VMware SD-WAN Orchestrator Deployment and Monitoring Guide

VMware SD-WAN 4.5

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

VMware SD-WAN Orchestrator Deployment and Monitoring Guide

1

The VMware SD-WAN™ Orchestrator Deployment and Monitoring Guide includes the following sections listed below.

This chapter includes the following topics:

Overview of the VMware SD-WAN Orchestrator Deployment and Monitoring Guide

The VMware SD-WAN Orchestrator Deployment and Monitoring Guide provides guidance on how to install, run, and monitor the VMware SD-WAN Orchestrator.

The SD-WAN Orchestrator Deployment and Monitoring Guide provides the following information:

- How to install the SD-WAN Orchestrator
- How to setup Disaster Recovery
- How to upgrade the SD-WAN Orchestrator
- How to back up the SD-WAN Orchestrator application Data
- How to monitor the SD-WAN Orchestrator application
- How to tune various system properties (depending on the scale of the deployment)

Install SD-WAN Orchestrator

This section describes SD-WAN Orchestrator installation.

Prerequisites

This section describes the prerequisites that must be met before installing the SD-WAN Orchestrator.

Instance Requirements

VMware recommends installation of the Orchestrator and Gateway applications as a virtual machine (i.e. guest instance) on an existing hypervisor.

The SD-WAN Orchestrator requires the following minimal guest instance specifications:

- 8 Intel vCPU's at 2.5 Ghz or higher
- 64 GB of memory
- Required Minimum IOPS: 5,000 IOPS
- SD-WAN Orchestrator requires 4 SSD based persistent volumes (expandable through LVM if needed)
  - 128GB x 1 - Root
  - 1TB x 1 - Store
  - 500GB x 1 - Store2
  - 1TB x 1 - Store3
- 1 Gbps NIC
- Ubuntu x64 server VM compatibility
- Single public IP address (Can be made available through NAT)

Upstream Firewall Configuration

The upstream firewall needs to be configured to allow inbound HTTP (TCP/80) as well as HTTPS (TCP/443). If a stateful firewall is in place, established connections that are outbound originated should also be allowed to facilitate upgrades and security updates.

External Services

The SD-WAN Orchestrator relies on several external services. Before proceeding with an installation, ensure that licenses are available for each of the services.

Google Maps

Google Maps is used for displaying Edges and data centers on a map. No account needs to be created with Google to utilize the functionality. However, Internet access must be available to the SD-WAN Orchestrator instance in order for the service to be available.

The service is limited to 25,000 map loads each day, for more than 90 consecutive days. VMware does not anticipate exceeding these limits for nominal use of the SD-WAN Orchestrator. For more information, see Google Maps.

Twilio

Twilio is used for SMS-based alerting to enterprise customers to notify them of Edge or link outage events. An account needs to be created and funded at http://www.twilio.com.

The account can be provisioned in the SD-WAN Orchestrator through the Operator Portal's **System Properties** page. The account will be provisioned through a system property, as described later in the guide. See Twilio for more information.

MaxMind

MaxMind is a geolocation service. It is used to automatically detect Edge and Gateway locations and ISP names based on IP address. If this service is deactivated, then geolocation information will need to be updated manually. The account can be provisioned in the SD-WAN Orchestrator through the Operator Portal's **System Properties** page. See MaxMind for more information.

Installation Procedures

This section describes installation.

Cloud-init Preparation

This section describes how to use the cloud-init package to handle the early initialization of instances.

About cloud-init

Cloud-init is a Linux package responsible for handling the early initialization of instances. If available in the distributions, it allows for configuration of many common parameters of the instance directly after installation. This creates a fully functional instance that is configured based on a series of inputs.

Cloud-init's behavior can be configured via user-data. User-data can be given by the user at instance launch time. This is typically done by attaching a secondary disk in ISO format that cloud-init will look for at first boot time. This disk contains all early configuration data that will be applied at that time.

The SD-WAN Orchestrator supports cloud-init and all essential configurations can be packaged in an ISO image.

Create the cloud-init meta-data File

The final installation configuration options are set with a pair of cloud-init configuration files. The first installation configuration file contains the metadata. Create this file with a text editor and label it `meta-data`. This file provides information that identifies the instance of SD-WAN Orchestrator being installed. The `instance-id` can be any identifying name, and the `local-hostname` should be a host name that follows your site standards, for example:

```
instance-id: vco01
local-hostname: vco-01
```

Additionally, you can specify network interface information (if the network is not configured via DHCP, for example):

```
instance-id: vco01
local-hostname: vco-01
network-interfaces: |
  auto eth0
  iface eth0 inet static
  address 10.0.1.2
  network 10.0.1.0
  netmask 255.255.255.0
  broadcast 10.0.1.255
  gateway 10.0.1.1
```

Create the cloud-init user-data File

The second installation configuration option file is the user data file. This file provides information about users on the system. Create it with a text editor and call it `user-data`. This file will be used to enable access to the installation of SD-WAN Orchestrator. The following is an example of what the `user-data` file will look like:

```
#cloud-config
            password: Velocloud123
            chpasswd: {expire: False}
            ssh_pwauth: True
            ssh_authorized_keys:
              - ssh-rsa AAA...SDvz user1@yourdomain.com
              - ssh-rsa AAB...QTuo user2@yourdomain.com
            vco:
              super_users:
                list: |
                  user1@yourdomain.com:password1
                remove_default_users: True
              system_properties:
                 list: |
                    mail.smtp.port:34
                    mail.smtp.host:smtp.yourdomain.com
                    service.maxmind.enable:True
                    service.maxmind.license:todo_license
                    service.maxmind.userid:todo_user
                    service.twilio.phoneNumber:222123123
                    network.public.address:222123123
            write_files:
               - path: /etc/nginx/velocloud/ssl/server.crt
                 permissions: '0644'
                 content: "-----BEGIN CERTIFICATE-----\nMI….ow==\n-----END CERTIFICATE-----\n"
               - path: /etc/nginx/velocloud/ssl/server.key
                 permissions: '0600'
                 content: "-----BEGIN RSA PRIVATE KEY-----\nMII...D/JQ==\n-----END RSA
PRIVATE KEY-----\n"
               - path: /etc/nginx/velocloud/ssl/velocloudCA.crt
```

This `user-data` file enables the default user, vcadmin, to login either with a password or with an SSH key. The use of both methods is possible, but not required. The password login is enabled by the `password` and `chpasswd` lines.

- The `password` contains the plain-text password for the vcadmin user.
- The `chpasswd` line turns off password expiration to prevent the first login from immediately prompting for a change of password. This is optional.

Note If you set a password, it is recommended that you change it when you first log in because the password has been stored in a plain text file.

The `ssh_pwauth` line enables SSH login. The `ssh_authorized_keys` line begins a block of one or more authorized keys. Each public SSH key listed on the `ssh-rsa` lines will be added to the vcadmin `~/.ssh/authorized_keys` file.

In this example, two keys are listed. For this example, the key has been truncated. In a real file, the entire public key must be listed. Note that the `ssh-rsa` lines must be preceded by two spaces, followed by a hyphen, followed by another space.

The `vco` section specifies configured SD-WAN Orchestrator services.

`super_users` contains list of VMware Super Operator accounts and corresponding passwords.

The `system_properties` section allows to customize Orchestrator System Properties. See System Properties for details regarding system properties configuration.

The `write_files` section allows to replace files on the system. By default, SD-WAN Orchestrator web services are configured with self-signed SSL certificate. If you would like to provide different SSL certificate, the above example replaces the `server.crt` and `server.key` files in the `/etc/nginx/velocloud/ssl/` folder with user-supplied files.

Note The `server.key` file must be unencrypted. Otherwise, the service will fail to start without the key password.

Create an ISO file

Once you have completed your files, they need to be packaged into an ISO image. This ISO image is used as a virtual configuration CD with the virtual machine. This ISO image, called `vco01-cidata.iso`, is created with the following command on a Linux system:

```
genisoimage -output vco01-cidata.iso -volid cidata -joliet -rock user-data meta-data
```

Transfer the newly created ISO image to the datastore on the host running VMware.

Install on VMware

VMware vSphere provides a means of deploying and managing virtual machine resources. This section explains how to run the SD-WAN Orchestrator using the VMware vSphere Client.

Deploy OVA Template

Note This procedure assumes familiarity with VMware vSphere and is not written with reference to any specific version of VMware vSphere.

1 Log in to the vSphere Client.

2 Select **File > Deploy OVF Template**.

3 Respond to the prompts with information specific to your deployment.

Field	Description
Source	Type a URL or navigate to the OVA package location.
OVF template details	Verify that you pointed to the correct OVA template for this installation.
Name and location	Name of the virtual machine.
Storage	Select the location to store the virtual machine files.
Provisioning	Select the provisioning type. "thin" is recommended for database and binary log volumes.
Network mapping	Select the network for each virtual machine to use. **Important** Uncheck **Power On After Deployment**. Selecting it will start the virtual machine and it should be started later after the cloud-init ISO has been attached.

4 Click **Finish**.

Note Depending on your network speed, this deployment can take several minutes or more.

Attach ISO Image as a CD/DVD to Virtual Machine

1 Right-click the newly-added SD-WAN Orchestrator VM and select **Edit Settings**.

2 From the **Virtual Machine Properties** window, select **CD/DVD Drive**.

3 Select the **Use an ISO image** option.

4 Browse to find the ISO image you created earlier (we called ours `vco01-cidata.iso`), and then select it. The ISO can be found in the datastore that you uploaded it to, in the folder that you created.

5 Select **Connect on Power On**.

6 Click **OK** to exit the **Properties** screen.

Run the SD-WAN Orchestrator Virtual Machine

To start up the SD-WAN Orchestrator virtual machine:

1 Click to highlight it, then select the **Power On** button.

2 Select the **Console** tab to watch as the virtual machine boots up.

Note If you configured SD-WAN Orchestrator as described here, you should be able to log into the virtual machine with the user name vcadmin and password that you defined when you created the cloud-init ISO.

Install on KVM

This section explains how to run the SD-WAN Orchestrator using the libvirt. This deployment was tested in Ubuntu 18.04 LTS.

Images

For KVM deployment, VMware will provide the SD-WAN Orchestrator in four qcow images.

- ROOTFS
- STORE
- STORE2
- STORE3

The images are thin provisioned on deployment.

Start by copying the images to the KVM server. In addition, you must copy the cloud-init iso build as described in the previous section.

XML Sample

Note For the images in the `images/vco` folder, you will need to edit from the XML.

```
<domain type='kvm' id='49'>
  <name>vco</name>
  <uuid>b0ff25bc-72b8-6ccb-e777-fdc0f4733e05</uuid>
  <memory unit='KiB'>12388608</memory>
  <currentMemory unit='KiB'>12388608</currentMemory>
  <vcpu>2</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
  <type>hvm</type>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
    <cpu mode='custom' match='exact'>
    <model fallback='allow'>SandyBridge</model>
    <vendor>Intel</vendor>
    <feature policy='require' name='vme'/>
    <feature policy='require' name='dtes64'/>
    <feature policy='require' name='invpcid'/>
```

```
    <feature policy='require' name='vmx'/>
    <feature policy='require' name='erms'/>
    <feature policy='require' name='xtpr'/>
    <feature policy='require' name='smep'/>
    <feature policy='require' name='pbe'/>
    <feature policy='require' name='est'/>
    <feature policy='require' name='monitor'/>
    <feature policy='require' name='smx'/>
    <feature policy='require' name='abm'/>
    <feature policy='require' name='tm'/>
    <feature policy='require' name='acpi'/>
    <feature policy='require' name='fma'/>
    <feature policy='require' name='osxsave'/>
    <feature policy='require' name='ht'/>
    <feature policy='require' name='dca'/>
    <feature policy='require' name='pdcm'/>
    <feature policy='require' name='pdpe1gb'/>
    <feature policy='require' name='fsgsbase'/>
    <feature policy='require' name='f16c'/>
    <feature policy='require' name='ds'/>
    <feature policy='require' name='tm2'/>
    <feature policy='require' name='avx2'/>
    <feature policy='require' name='ss'/>
    <feature policy='require' name='bmi1'/>
    <feature policy='require' name='bmi2'/>
    <feature policy='require' name='pcid'/>
    <feature policy='require' name='ds_cpl'/>
    <feature policy='require' name='movbe'/>
    <feature policy='require' name='rdrand'/>
  </cpu>
<clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/bin/kvm-spice</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/images/vco/rootfs.qcow2'/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/ images/vco/store.qcow2'/>
      <target dev='hdb' bus='ide'/>
      <alias name='ide0-0-1'/>
      <address type='drive' controller='0' bus='0' target='0' unit='1'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/ images/vco/store2.qcow2'/>
      <target dev='hdc' bus='ide'/>
      <alias name='ide0-0-2'/>
```

```
      <address type='drive' controller='0' bus='1' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' />
      <source file='/images/vco/store3.qcow2' />
      <target dev='hdd' bus='ide' />
      <alias name='ide0-0-3' />
      <address type='drive' controller='0' bus='1' target='0' unit='1' />
    </disk>
    <disk type='file' device='cdrom'>
      <driver name='qemu' type='raw'/>
      <source file='/ images/vco/seed.iso'/>
      <target dev='sdb' bus='sata'/>
      <readonly/>
      <alias name='sata1-0-0'/>
      <address type='drive' controller='1' bus='0' target='0' unit='0'/>
    </disk>
    <controller type='usb' index='0'>
      <alias name='usb0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
    </controller>
    <controller type='pci' index='0' model='pci-root'>
      <alias name='pci.0'/>
    </controller>
    <controller type='ide' index='0'>
      <alias name='ide0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
    </controller>
    <interface type='direct'>
      <source dev='eth0' mode='vepa'/>
    </interface>
    <serial type='pty'>
      <source path='/dev/pts/3'/>
      <target port='0'/>
      <alias name='serial0'/>
    </serial>
    <console type='pty' tty='/dev/pts/3'>
      <source path='/dev/pts/3'/>
      <target type='serial' port='0'/>
      <alias name='serial0'/>
    </console>
    <memballoon model='virtio'>
      <alias name='balloon0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </memballoon>
  </devices>
  <seclabel type='none' />
<!--  <seclabel type='dynamic' model='apparmor' relabel='yes'/> -->
</domain>
```

Create the VM

To create the VM using the standard virsh commands:

```
virsh define vco.xml
virsh start vco.xml
```

Install on AWS

This section describes how to install SD-WAN Orchestrator on AWS.

Minimum Instance Requirements

See the first section of the SD-WAN Orchestrator Installation, titled Instance Requirements, and select an AWS instance type matching these requirements. Both CPU and Memory requirements must be satisfied. Example: use c4.2xlarge or larger; r4.2xlarge or larger

Request an AMI Image

Request an AMI ID from VMware. It will be shared with the customer account. Have an Amazon AWS account ID ready when requesting AMI access.

Installation

1 Launch the EC2 instance in AWS cloud.

   Example: http://docs.aws.amazon.com/efs/latest/ug/gs-step-one-create-ec2-resources.html

2 Configure the security group to allow inbound HTTP (TCP/80) as well as HTTPS (TCP/443).

3 After the instance is launched, point the web browser to the Operator login URL:

   `https://<name>/operator`

Initial Configuration Tasks

Complete the following initial configuration tasks:

- Configure system properties
- Set up initial operator profile
- Set up operator accounts
- Create gateways
- Setup gateway pools
- Create customer account / partner account

Install an SSL Certificate

This section describes how to install an SSL certificate.

To install an SSL certificate:

1 Login into the SD-WAN Orchestrator CLI console through SSH. If you configured the SD-WAN Orchestrator as described here, you should be able to log into the virtual machine with the user name `vcadmin` and password that you defined when you created the cloud-init ISO.

2 Generate the SD-WAN Orchestrator private key.

Note Do not encrypt the key. It must remain unencrypted on the SD-WAN Orchestrator system.

```
openssl genrsa -out server.key 2048
```

3 Generate a certificate request. Customize `-subj` according to your organization information.

```
openssl req -new -key server.key -out
server.csr -subj "/C=US/ST=California/L=Mountain View/O=Velocloud Networks
Inc./OU=Development/CN=vco.velocloud.net"
```

Description of Subject fields:

Field	Description
C	country
ST	state
L	locality (city)
O	company
OU	department (optional)
CN	SD-WAN Orchestrator fully qualified domain name

4 Send `server.csr` to a Certificate Authority for signing. You should get back the SSL certificate (`server.crt`). Ensure that it is in the PEM format.

5 Install the certificate (which requires root access). SD-WAN Orchestrator SSL certificates are located in `/etc/nginx/velocloud/ssl/`.

```
cp server.key server.crt /etc/nginx/velocloud/ssl/
chmod 600 /etc/nginx/velocloud/ssl/server.key
```

6 Restart nginx.

```
systemctl restart nginx
```

Configure System Properties

This section describes how to configure System Properties, which provide a mechanism to control the system-wide behavior of the VMware SD-WAN.

System Properties can be set initially using the cloud-init config file. For more information, see Cloud-init Preparation. The following properties need to be configured to ensure proper operation of the service.

System Name

Enter a fully qualified VMware domain name in the `network.public.address` system property.

Google Maps

Google Maps is used for displaying edges and data centers on a map. Maps may fail to display without a license key. The Orchestrator will continue to function properly, but browser maps will not be available in this case.

1 Login into https://console.developers.google.com.

2 Create a new project, if one is not already created.

3 Locate the button **Enable API**. Click under the **Google Maps APIs** and enable both **Google Maps JavaScript API** and **Google Maps Geolocation API**.

4 On the left side of the screen, click the **Credentials** link.

5 Under the Credentials page, click **Create Credentials**, then select **API key**. Create an API key.

6 Set the `service.client.googleMapsApi.key` VMware system property to API key.

7 Set `service.client.googleMapsApi.enable` to “true.”

Twilio

Twilio is a messaging service that allows you to receive VMware alerts via SMS. It is optional. The account details can be entered into the VMware through the Operator Portal's **System Properties** page. The properties are called:

- `service.twilio.enable` allows the service to be deactivated in the event that no Internet access is available to the VMware
- `service.twilio.accountSid`
- `service.twilio.authToken`
- `service.twilio.phoneNumber` in `(nnn)nnn-nnnn` format

Obtain the service at https://www.twilio.com.

MaxMind

MaxMind is a geolocations service. It is used to automatically detect Edge and Gateway locations and ISP names based on an IP address. If this service is deactivated, then geolocation information will need to be updated manually. The account details can be entered into the VMware through the Operator Portal's **System Properties page**. You can configure:

- `service.maxmind.enable` allows the service to be deactivated in the event that no Internet access is available to the VMware

- `service.maxmind.userid` holds the user identification supplied by MaxMind during the account creation
- `service.maxmind.license` holds the license key supplied by MaxMind

Obtain the license at: https://www.maxmind.com/en/geoip2-precision-city-service.

Email

Email services can be used for both sending the Edge activation messages as well as for alarms and notifications. It is not required, but it is strongly recommended that you configure this as part of VMware operations. The following system properties are available to configure the external email service used by the Orchestrator:

- `mail.smtp.auth.pass` - SMTP user password.
- `mail.smtp.auth.user` - SMTP user for authentication.
- `mail.smtp.host` - relay server for email originated from the VMware.
- `mail.smtp.port` - SMTP port.
- `mail.smtp.secureConnection` - use SSL for SMTP traffic.

Upgrade SD-WAN Orchestrator

This section describes how to upgrade the SD-WAN Orchestrator.

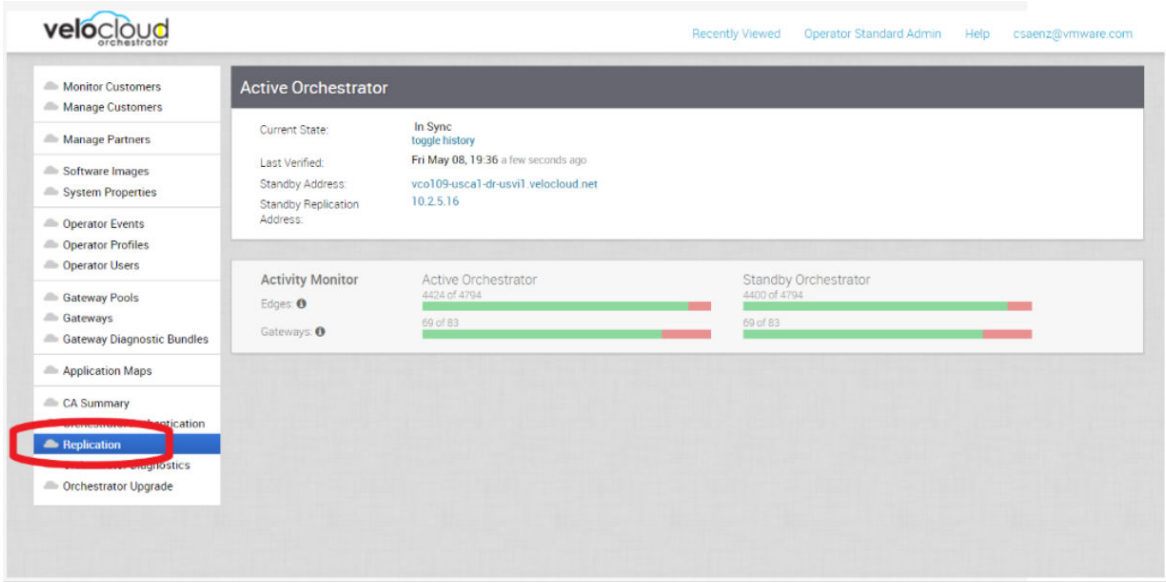
To upgrade the SD-WAN Orchestrator:

1 VMware SD-WAN by VeloCloud Support will assist you with your upgrade. Collect the following information prior to contacting Support.

   - Provide the current and target SD-WAN Orchestrator versions, for example: current version (ie 2.5.2 GA-20180430), target version (3.3.2 p2).

     Note For the current version, this information can be found on the top, right corner of the SD-WAN Orchestrator by clicking the **Help** link and choosing **About**.

   - Provide a screenshot of the replication dashboard of the SD-WAN Orchestrator as shown below.



- Hypervisor Type and version (ie vSphere 6.7)
- Commands from the SD-WAN Orchestrator:

  Note Commands must be run as root (e.g. ‘sudo <command>’ or ‘sudo -i’).

  - LVM layout
    - pvdisplay -v
    - vgdisplay -v
    - lvdisplay -v
    - df -h
    - cat /etc/fstab
  - Memory information
    - free -m
    - cat /proc/meminfo
    - ps -ef
    - top -b -n 2
  - CPU Information
    - cat /proc/cpuinfo
  - Copy of /var/log
    - tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log

- From the Standby Orchestrator:
  - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'
- From the Active Orchestrator:
  - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'

2 Contact VMware SD-WAN Orchestrator Support at https://kb.vmware.com/s/article/53907 with the above-mentioned information for assistance with the SD-WAN Orchestrator upgrade.

Expand Disk Size (VMware)

All storage volumes are configured as LVM devices. They can be resized online by providing the underlying virtualization technology to support online disk expansion. Disks are expanded automatically via cloud-init when the VM boots.

To expand disks after boot:

1 Login into the SD-WAN Orchestrator system console.

2 Identify the physical disks that support the database volume.

```
vgs -o +devices store
```

Example:

```
root@vco:~# vgs -o +devices db_data
   \  VG      #PV #LV #SN Attr   VSize   VFree   Devices
     store   1   1   0 wz--n- 500.00g 125.00g /dev/sdb(0)
```

3 Identify the physical disk attachment.

```
lshw -class volume
```

Example:

```
/dev/sdb is attached to scsi@2:0.1.0 (Host: scsi2 Channel: 00 Id: 01 Lun: 00)
```

```
root@vco:~# lshw -class volume
  *-volume
       description: EXT4 volume
       vendor: Linux
       physical id: 1
       bus info: scsi@2:0.0.0,1
       logical name: /dev/sda1
       logical name: /
       version: 1.0
       serial: 9d212247-77c4-4f98-a5c2-7f8470fa2da8
       size: 10239MiB
       capacity: 10239MiB
```

```
       capabilities: primary bootable journaled extended_attributes large_files huge_files
dir_nlink recover extents ext4 ext2 initialized
       configuration: created=2016-02-22 20:49:38 filesystem=ext4 label=cloudimg-
rootfs lastmountpoint=/ modified=2016-02-22 21:18:58 mount.fstype=ext4
mount.options=rw,relatime,data=ordered mounted=2016-10-06 23:22:04 state=mounted
  *-disk:1
       description: SCSI Disk
       physical id: 0.1.0
       bus info: scsi@2:0.1.0
       logical name: /dev/sdb
       serial: v5V2zm-Lvbh-Mfx3-W8ki-COI9-DAtP-RXndhu
       size: 500GiB
       capacity: 500GiB
       capabilities: lvm2
       configuration: sectorsize=512
  *-disk:2
       description: SCSI Disk
       physical id: 0.2.0
       bus info: scsi@2:0.2.0
       logical name: /dev/sdc
       serial: fTQFJ2-giAV-WsXL-1Wha-V305-oQkV-qqS3SA
       size: 100GiB
       capacity: 100GiB
       capabilities: lvm2
       configuration: sectorsize=512
```

4 On the hypervisor host, locate the disk attached to the VM using bus information. Example: `SCSI(0:1)`

5 Extend the virtual disk. For instructions, see VMware KB article 1004047: http://kb.vmware.com/kb/1004047

6 Re-login into the SD-WAN Orchestrator system console.

7 Re-scan the block device for the resized physical volume. Example:

```
echo 1 > /sys/block/$DEVICE/device/rescan
```

Example:

```
echo 1 > /sys/block/sdb/device/rescan
```

8 Resize the LVM physical disk.

```
pvresize /dev/sdb
```

9 Determine the amount of free space in the database volume group.

```
vgdisplay store |grep Free
```

Example:

```
root@vco:~# vgdisplay store |grep Free
Free  PE / Size       34560 / 135.00 GiB
```

10 Extend the database logical volume.

```
lvextend -r -L+#G /dev/store/data
```

Example:

```
root@vco1:~# lvextend -r -L+1G /dev/store/data
  Size of logical volume store/data changed from 400.00 GiB (102400 extents) to 401.00 GiB
(102656 extents).
  Logical volume store/data successfully resized.
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/mapper/store-data is mounted on /store; on-line resizing required
old_desc_blocks = 50, new_desc_blocks = 51
The filesystem on /dev/mapper/store-data is now 105119744 (4k) blocks long.
```

11 View the new size of the volume.

```
df -h /dev/store/data
```

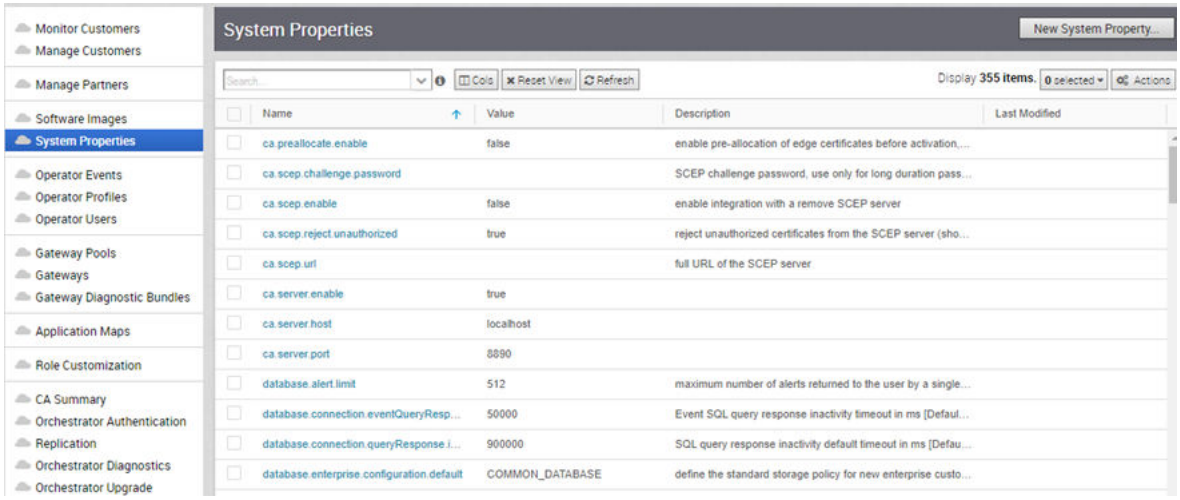
Example:

```
root@vco:~# df -h /dev/store/data
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/store-data  379G  1.2G  359G   1% /store
```

System Properties

VMware provides System Properties to configure various features and options available in the Orchestrator portal.

In the Operator portal, navigate to the **System Properties** page, which lists the available pre-defined system properties. See List of System Properties, which lists some of the system properties that you can modify as an Operator.



To configure the system properties:

1 Click **New System Property** to add a new property.

2 In the **New System Property** window, enter a name for the new property and choose the **Data Type** from the drop-down list.

3 Enter the **Value** for the property according to the data type.

4 Enter a description for the property.

5 Click **Save**.

6 To modify the values of a property, click the link to the property or select the property and click **Actions > Modify System Property**.

7 To remove a property, select the property and click **Actions > Delete System Property**.

You can use the **Search** field to find a specific system property. See the section titled, "List of System Properties" in the VMware SD-WAN Orchestrator Deployment and Monitoring Guide, which lists some of the system properties that you can modify as an Operator.

Note It is recommended to contact VMware Support before making changes to the system properties.

List of System Properties

As an Operator, you can add or modify the values of the system properties.

The following tables describe some of the system properties. As an Operator, you can set the values for these properties.

- Table 1-1. Alert Emails
- Table 1-2. Alerts
- Table 1-4. Certificate Authority
- List item.

Table 1-1. Alert Emails

System Property	Description
vco.alert.mail.to	When an alert is triggered, a notification is sent immediately to the list of Email addresses provided in the Value field of this system property. You can enter multiple Email IDs separated by commas. If the property does not contain any value, then the notification is not sent. The notification is meant to alert VMware support / operations personnel of impending issues before notifying the customer.
vco.alert.mail.cc	When alert emails are sent to any customer, a copy is sent to the Email addresses provided in the Value field of this system property. You can enter multiple Email IDs separated by commas.
mail.*	There are multiple system properties available to control the Alert Emails. You can define the Email parameters like SMTP properties, username, password, and so on.

Table 1-2. Alerts

System Property	Description
vco.alert.enable	Globally activates or deactivates the generation of alerts for both Operators and Enterprise customers.
vco.enterprise.alert.enable	Globally activates or deactivates the generation of alerts for Enterprise customers.
vco.operator.alert.enable	Globally activates or deactivates the generation of alerts for Operators.

Table 1-3. Bastion Orchestrator Configuration

System Property	Description
session.options.enableBastionOrchestrator	Enables the Bastion Orchestrator feature. For more information, see *Bastion Orchestrator Configuration Guide* available at https://docs.vmware.com/en/VMware-SD-WAN/index.html.
vco.bastion.private.enable	Enables the Orchestrator to be the Private Orchestrator of the Bastion pair.
vco.bastion.public.enable	Enables the Orchestrator to be the Public Orchestrator of the Bastion pair.

Table 1-4. Certificate Authority

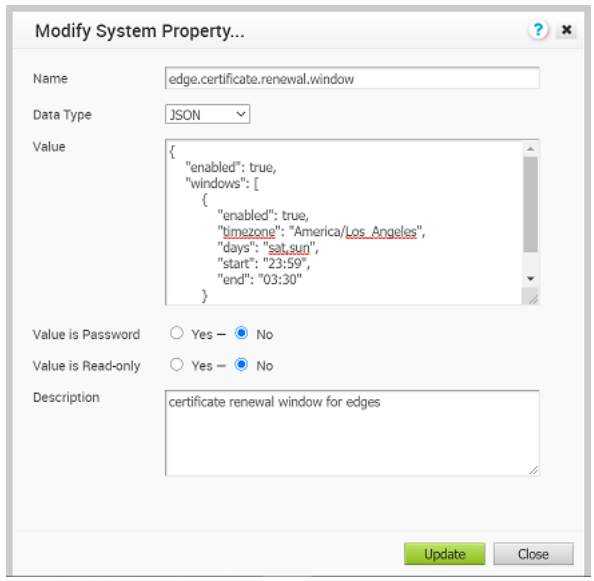
System Property	Description
edge.certificate.renewal.window	This optional system property allows the Operator to define one or more maintenance windows during which the Edge certificate renewal is enabled. Certificates scheduled for renewal outside of the windows will be deferred until the current time falls within one of the enabled windows. Enable System Property: To enable this system property, type "true" for "enabled" in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of the first part of this system property when it is enabled is shown below. Operators can define multiple windows to restrict the days and hours of the day during which Edge renewals are enabled. Each window can be defined by a day, or a list of days (separated by a comma), and a start and end time. Start and end times can be specified relative to an Edge's local time zone, or relative to UTC. See image below for an example.  **Note** If attributes are not present, the default is enabled "false." When defining window attributes, adhere to the following: ■ Use IANA time zones, not PDT or PST (e.g. America/Los_Angeles) See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for more information. ■ Use UTC for days (e.g. SAT, SUN). ■ Separated by comma. ■ Days in three letters in English. ■ Not case sensitive. ■ Use Military 24 hour time format only (HH:MM) for start times (e.g. 01:30) and end times (e.g. 05:30). If the above-mentioned values are missing, the attribute defaults in each window definition are as follow: ■ If enabled is missing, the default value = false.

Table 1-4. Certificate Authority (continued)

System Property	Description
	■ If timezone is missing, the default = 'local.' ■ If one of either 'days' or end and start times are missing, the defaults are as follows: ■ If 'days' is missing, the start/end is applied to each day of the week (mon, tue, wed, thu, fri, sat, sun). ■ If end and start times are missing, then any time in the specified day will match (start = 00:00 and end = 23:59). ■ NOTE: One of either 'days' or end and start times must be present. However, if they are missing, the defaults will be as indicated above. Deactivate System Property: This system property is deactivated by default, which means the certificate will automatically renew after it expires. "Enabled" will be set to "false in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of this property when it is deactivated is shown below. { "enabled": false, "windows": [{ NOTE: This system property requires that PKI be enabled.
gateway.certificate.renewal.window	This optional system property allows the Operator to define one or more maintenance windows during which the Gateway certificate renewal is enabled. Certificates scheduled for renewal outside of the windows will be deferred until the current time falls within one of the enabled windows. Enable System Property: To enable this system property, type "true" for "enabled" in the first part of the **Value** text area in the **Modify System Property** dialog box. See image below for an example. Operators can define multiple windows to restrict the days and hours of the day during which edge renewals are enabled. Each window can be defined by a day, or list of days (separated by a comma), and a start and end time. Start and end times can be specified relative to an edge's local timezone, or relative to UTC. See image below for an example.

Table 1-4. Certificate Authority (continued)

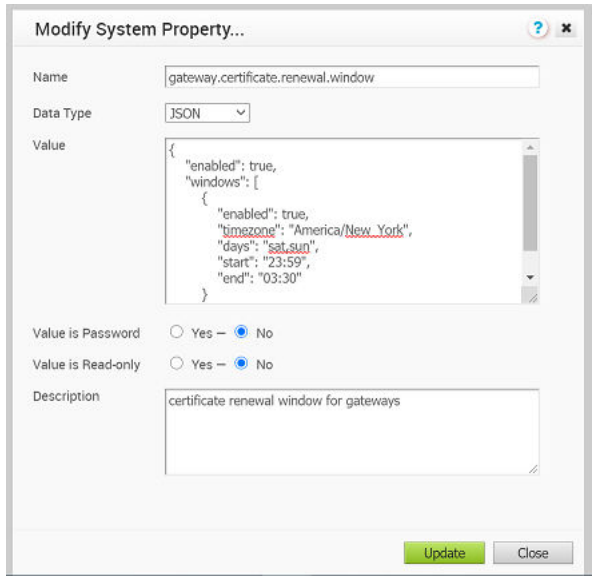
System Property	Description
	 **Note** If attributes are not present, the default is enabled "false." When defining window attributes, adhere to the following: ■ Use IANA time zones, not PDT or PST (e.g. America/Los_Angeles) See https://en.wikipedia.org/wiki/List_of_tz_database_time_zones for more information. ■ Use UTC for days (e.g. SAT, SUN). ■ Separated by comma. ■ Days in three letters in English. ■ Not case sensitive. ■ Use Military 24 hour time format only (HH:MM) for start times (e.g. 01:30) and end times (e.g. 05:30). If the above-mentioned values are missing, the attribute defaults in each window definition are as follow: ■ If enabled is missing, the default value = false. ■ If timezone is missing, the default = 'local." ■ If one of either 'days' or end and start times are missing, the defaults are as follows: ■ If 'days' is missing, the start/end is applied to each day of the week (mon, tue, wed, thu, fri, sat, sun). ■ If end and start times are missing, then any time in the specified day will match (start = 00:00 and end = 23:59). ■ NOTE: One of either 'days' or (end and start) must be present. However, if they are missing, the defaults will be as indicated above. Deactivate System Property: This system property is deactivated by default, which means the certificate will automatically renew after it expires. "Enabled" will be set to "false in the first part of the **Value** text area in the **Modify System Property** dialog box. An example of this property when it is deactivated is shown below.

Table 1-4. Certificate Authority (continued)

System Property	Description
	{ "enabled": false, "windows": [{ NOTE: This system property requires that PKI be enabled.

Table 1-5. Data Retention

System Property	Description
retention.highResFlows.days	This system property enables Operators to configure high resolution flow stats data retention anywhere between 1 and 90 days.
retention.lowResFlows.months	This system property enables Operators to configure low resolution flow stats data retention anywhere between 1 and 365 days.
session.options.maxFlowstatsRetentionDays	This property enables Operators to query more than two weeks of flows stats data.

Table 1-6. Edges

System Property	Description
edge.offline.limit.sec	If the Orchestrator does not detect a heartbeat from an Edge for the specified duration, then the state of the Edge is moved to OFFLINE mode.
edge.link.unstable.limit.sec	When the Orchestrator does not receive link statistics for a link for the specified duration, the link is moved to UNSTABLE mode.
edge.link.disconnected.limit.sec	When the Orchestrator does not receive link statistics for a link for the specified duration, the link is disconnected.
edge.deadbeat.limit.days	If an Edge is not active for the specified number of days, then the Edge is not considered for generating Alerts.
vco.operator.alert.edgeLinkEvent.enable	Globally activates or deactivates Operator Alerts for Edge Link events.
vco.operator.alert.edgeLiveness.enable	Globally activates or deactivates Operator Alerts for Edge Liveness events.

Table 1-7. Edge Activation

System Property	Description
edge.activation.key.encode.enable	Base64 encodes the activation URL parameters to obscure values when the Edge Activation Email is sent to the Site Contact.
edge.activation.trustedIssuerReset.enable	Resets the trusted certificate issuer list of the Edge to contain only the Orchestrator Certificate Authority. All TLS traffic from the edge are restricted by the new issuer list.
network.public.certificate.issuer	Set the value of **network.public.certificate.issuer** equal to the PEM encoding of the issuer of Orchestrator server certificate, when **edge.activation.trustedIssuerReset.enable** is set to True. This will add the server certificate issuer to the trusted issuer of the Edge, in addition to the Orchestrator Certificate Authority.

Table 1-8. Monitoring

System Property	Description
vco.monitor.enable	Globally activates or deactivates monitoring of Enterprise and Operator entity states. Setting the Value to **False** prevents SD-WAN Orchestrator from changing entity states and triggering alerts.
vco.enterprise.monitor.enable	Globally activates or deactivates monitoring of Enterprise entity states.
vco.operator.monitor.enable	Globally activates or deactivates monitoring of Operator entity states.

Table 1-9. Notifications

System Property	Description
vco.notification.enable	Globally activates or deactivates the delivery of Alert notifications to both Operator and Enterprises.
vco.enterprise.notification.enable	Globally activates or deactivates the delivery of Alert notifications to the Enterprises.
vco.operator.notification.enable	Globally activates or deactivates the delivery of Alert notifications to the Operator.

Table 1-10. Password Reset and Lockout

System Property	Description
vco.enterprise.resetPassword.token.expirySeconds	Duration of time, after which the password reset link for an enterprise user expires.
vco.enterprise.authentication.passwordPolicy	Defines the password strength, history, and expiration policy for customer users. Edit the JSON template in the Value field to define the following: **strength** ■ **minlength:** Minimum password character length. The default minimum password length is 8 characters. ■ **maxlength:** Maximum password character length. The default maximum password length is 32 characters. ■ **requireNumber:** The password must contain at least one numeric character. Numeric requirement is enabled by default. ■ **requireLower:** The password must contain at least one lowercase character. Lowercase requirement is enabled by default. ■ **requireUpper:** The password must contain at least one uppercase character. Uppercase requirement is not enabled by default. ■ **requireSpecial:** The password must contain at least one special character (for example, _@!). The special character requirement is not enabled by default. ■ **excludeTop:** Password must not match a list of the most used passwords. Default value is 1000, representing the top 1000 most used passwords, and is configurable to a maximum of 10,000 of the most used passwords. ■ **maxRepeatingCharacters:** Password must not include a configurable number of repeated characters. For example, if maxRepeatingCharacters is set to ‘2’ then the Orchestrator would reject any password with 3 or more repetitive characters, like “Passwordaaa”. The default value of -1 signifies that this feature is not enabled. ■ **maxSequenceCharacters:** Password must not include a configurable number of sequential characters. For example, if maxSequenceCharacters is set to ‘3’ then the Orchestrator would reject any password where 4 or more characters which are sequential, like “Password1234”. The default value of -1 signifies that this feature is not enabled.

Table 1-10. Password Reset and Lockout (continued)

System Property	Description
	■ **disallowUsernameCharacters:** Password must not match a configurable portion of the user's ID. For example, if disallowUsernameCharacters is set to 5, if a user with username username@domain.com attempts to configure a new password that includes ‘usern’ or ‘serna’, or any five-character string that matches a section of the user’s username, that new password would be rejected by the Orchestrator. The default value of -1 signifies that this feature is not enabled. ■ **variationValidationCharacters:** New password must vary from the old password by a configurable number of characters. The Orchestrator uses the Levenshtein distance between two words to determine the variation between the new and old password. The Levenshtein distance is the minimum number of single-character edits (insertions, deletions, or substitutions) required to change one word into another. ■ If variationValidationCharacters is set to 4, then the Levenshtein distance between the new and old password must be 4 or greater. In other words, the new password must have 4 or more variations from the old password. For example, if the old password used was "kitten" and the new password is "sitting", the Levenshtein distance for these is 3, since it requires only three edits to change kitten into sitting: ■ kitten → sitten (substitution of "s" for "k") ■ sitten → sittin (substitution of "i" for "e") ■ sittin → sitting (insertion of "g" at the end). Since the new password only varies by 3 characters from the old, “sitting” would be rejected as a new password to replace “kitten”. The default value of -1 signifies that this feature is not enabled. **expiry**: ■ **enable**: Set this to **true** to enable automatic expiry of customer user passwords. ■ **days**: Enter the number of days that an customer password may be used before forced expiration.

Table 1-10. Password Reset and Lockout (continued)

System Property	Description
	history: ■ **enable**: Set this to **true** to enable recording of customer users' previous Passwords. ■ **count**: Enter the number of previous Passwords to be saved in the history. When a customer user tries to change the password, the system does not allow the user to enter a password that is already saved in the history.
enterprise.user.lockout.defaultAttempts	Number of times the enterprise user can attempt to login. If the login fails for the specified number of times, the account is locked.
enterprise.user.lockout.defaultDurationSeconds	Duration of time, for which the enterprise user account is locked.
enterprise.user.lockout.enabled	Activates or deactivates the lockout option for the enterprise login failures.
vco.operator.resetPassword.token.expirySeconds	Duration of time, after which the password reset link for an Operator user expires.

Table 1-10. Password Reset and Lockout (continued)

System Property	Description
vco.operator.authentication.passwordPolicy	Defines the password strength, history, and expiration policy for Operator users. Edit the JSON template in the Value field to define the following: **strength** ■ **minlength:** Minimum password character length. The default minimum password length is 8 characters. ■ **maxlength:** Maximum password character length. The default maximum password length is 32 characters. ■ **requireNumber:** The password must contain at least one numeric character. Numeric requirement is enabled by default. ■ **requireLower:** The password must contain at least one lowercase character. Lowercase requirement is enabled by default. ■ **requireUpper:** The password must contain at least one uppercase character. Uppercase requirement is not enabled by default. ■ **requireSpecial:** The password must contain at least one special character (for example, _@!). The special character requirement is not enabled by default. ■ **excludeTop:** Password must not match a list of the most used passwords. Default value is 1000, representing the top 1000 most used passwords, and is configurable to a maximum of 10,000 of the most used passwords. ■ **maxRepeatingCharacters:** Password must not include a configurable number of repeated characters. For example, if maxRepeatingCharacters is set to '2' then the Orchestrator would reject any password with 3 or more repetitive characters, like "Passwordaaa". The default value of -1 signifies that this feature is not enabled. ■ **maxSequenceCharacters:** Password must not include a configurable number of sequential characters. For example, if maxSequenceCharacters is set to '3' then the Orchestrator would reject any password where 4 or more characters which are sequential, like "Password1234". The default value of -1 signifies that this feature is not enabled. ■ **disallowUsernameCharacters:** Password must not match a configurable portion

Table 1-10. Password Reset and Lockout (continued)

System Property	Description
	of the user's ID. For example, if disallowUsernameCharacters is set to 5, if a user with username username@domain.com attempts to configure a new password that includes 'usern' or 'serna', or any five-character string that matches a section of the user's username, that new password would be rejected by the Orchestrator. The default value of -1 signifies that this feature is not enabled. ■ **variationValidationCharacters:** New password must vary from the old password by a configurable number of characters. The Orchestrator uses the Levenshtein distance between two words to determine the variation between the new and old password. The Levenshtein distance is the minimum number of single-character edits (insertions, deletions, or substitutions) required to change one word into another. ■ If variationValidationCharacters is set to 4, then the Levenshtein distance between the new and old password must be 4 or greater. In other words, the new password must have 4 or more variations from the old password. For example, if the old password used was "kitten" and the new password is "sitting", the Levenshtein distance for these is 3, since it requires only three edits to change kitten into sitting: ■ kitten → sitten (substitution of "s" for "k") ■ sitten → sittin (substitution of "i" for "e") ■ sittin → sitting (insertion of "g" at the end). Since the new password only varies by 3 characters from the old, "sitting" would be rejected as a new password to replace "kitten". The default value of -1 signifies that this feature is not enabled. **expiry**: ■ **enable**: Set this to **true** to enable automatic expiry of Operator user passwords. ■ **days**: Enter the number of days that an Operator password may be used before forced expiration. **history**: ■ **enable**: Set this to **true** to enable recording of Operator users' previous Passwords.

Table 1-10. Password Reset and Lockout (continued)

System Property	Description
	■ **count**: Enter the number of previous Passwords to be saved in the history. When a Operator user tries to change the password, the system does not allow the user to enter a password that is already saved in the history.
operator.user.lockout.defaultAttempts	Number of times the Operator user can attempt to login. If the login fails for the specified number of times, the account is locked.
operator.user.lockout.defaultDurationSeconds	Duration of time, for which the Operator user account is locked.
operator.user.lockout.enabled	Activates or deactivates the lockout option for the Operator login failures.

Table 1-11. Rate Limiting APIs

System Property	Description
vco.api.rateLimit.enabled	Allows Operator Super users activate or deactivate the rate limiting feature at the system level. By default, the value is **False**. **Note** The rate-limiter is not enabled in earnest, that is, it will not reject API requests that exceed the configured limits, unless the **vco.api.rateLimit.mode.logOnly** setting is deactivated.
vco.api.rateLimit.mode.logOnly	Allows Operator Super user to use rate limit in a **LOG_ONLY** mode. When the value is set as **True** and if a rate limit exceeds, this option logs only the error and fires respective metrics allowing clients to make requests without rate limiting. When the value is set to **False**, the request API is restricted with defined policies and HTTP 429 is returned.

Table 1-11. Rate Limiting APIs (continued)

System Property	Description
vco.api.rateLimit.rules.global	Allows to define a set of globally applicable policies used by the rate-limiter, in a JSON array. By default, the value is an empty array. Each type of user (Operator, Partner, and Customer) can make up to 500 requests for every 5 seconds. The number of requests is subject to change based on the behavior pattern of the rate limited requests. The JSON array consists of the following parameters: **Types**: The type objects represent different contexts in which the rate limits are applied. The following are the different type objects that are available: ■ **SYSTEM**: Specifies a global limit shared by all the users. ■ **OPERATOR_USER**: A limit that can be set in general for all the Operator users. ■ **ENTERPRISE_USER**: A limit that can be set in general for all the Enterprise users. ■ **MSP_USER**: A limit that can be set in general for all the MSP users. ■ **ENTERPRISE**: A limit that can be shared between all users of an Enterprise and is applicable to all the Enterprises in the network. ■ **PROXY**: A limit that can be shared between all users of a Proxy and is applicable to all proxies. **Policies**: Add rules to the policies to apply the requests that match the rule, by configuring the following parameters: ■ **Match**: Enter the type of requests to be matched: ■ **All**: Rate-limit all requests matching one of the type objects. ■ **METHOD**: Rate-limit all requests matching the specified method name. ■ **METHOD_PREFIX**: Rate-limit all requests matching the specified method group. ■ **Rules**: Enter the values for the following parameters: ■ **maxConcurrent**: Number of jobs that can be performed at the same time. ■ **reservoir**: Number of jobs that can be performed before the limiter stops performing jobs. ■ **reservoirRefreshAmount**: Value to set the reservoir to when **reservoirRefreshInterval** is in use. ■ **reservoirRefreshInterval**: For every millisecond of **reservoirRefreshInterval**, the **reservoir** value will be automatically updated to the value of **reservoirRefreshAmount**. The **reservoirRefreshInterval** value should be a multiple of 250 (5000 for Clustering).

Table 1-11. Rate Limiting APIs (continued)

System Property	Description
	Enabled: Each type limit can be activated or deactivated by including the **enabled** key in **APIRateLimiterTypeObject**. By default, the value of **enabled** is True, even if the key is not included. You need to include **"enabled": false** key to deactivate the individual type limits. The following example shows a sample JSON file with default values: `[{ "type": "OPERATOR_USER", "policies": [{ "match": { "type": "ALL" }, "rules": { "reservoir": 500, "reservoirRefreshAmount": 500, "reservoirRefreshInterval": 5000 } }] }, { "type": "MSP_USER", "policies": [{ "match": { "type": "ALL" }, "rules": { "reservoir": 500, "reservoirRefreshAmount": 500, "reservoirRefreshInterval": 5000 } }] }, { "type": "ENTERPRISE_USER", "policies": [{ "match": { "type": "ALL" }, "rules": { "reservoir": 500, "reservoirRefreshAmount": 500, "reservoirRefreshInterval": 5000 } }]`

Table 1-11. Rate Limiting APIs (continued)

System Property	Description

	<pre>}
	]</pre>
	Note It is recommended not to change the default values of the configuration parameters.

vco.api.rateLimit.rules.enterprise.default	Comprises the default set of Enterprise-specific policies applied to newly created Customers. The Customer-specific properties are stored in the Enterprise property **vco.api.rateLimit.rules.enterprise**.
vco.api.rateLimit.rules.enterpriseProxy.default	Comprises the default set of Enterprise-specific policies applied to newly created Partners. The Partner-specific properties are stored in the Enterprise proxy property **vco.api.rateLimit.rules.enterpriseProxy**.

For more information on Rate limiting, see Rate Limiting API Requests.

Table 1-12. Remote Diagnostics

System Property	Description
network.public.address	Specifies the browser origin address/DNS hostname that is used to access the SD-WAN Orchestrator UI.
network.portal.websocket.address	Allows to set an alternate DNS hostname/address to access the SD-WAN Orchestrator UI from a browser, if the browser address is not the same as the value of `network.public.address` system property. As remote diagnostics now uses a WebSocket connection, to ensure web security, the browser origin address that is used to access the Orchestrator UI is validated for incoming requests. In most cases, this address is same as the `network.public.address` system property. In rare scenarios, the Orchestrator UI can be accessed using another DNS hostname/address that is different from the value set in the `network.public.address` system property. In such cases, you can set this system property to the alternate DNS hostname/address. By default, this value is not set.
session.options.websocket.portal.idle.timeout	Allows to set the total amount of time (in seconds) the browser WebSocket connection is active in an idle state. By default, the browser WebSocket connection is active for 300 seconds in an idle state.

Table 1-13. Segmentation

System Property	Description
enterprise.capability.enableSegmentation	Activates or deactivates the segmentation capability for Enterprise users.
enterprise.segments.system.maximum	Specifies the maximum number of segments allowed for any Enterprise user. Ensure that you change the value of this system property to 128 if you want to enable 128 segments on SD-WAN Orchestrator for an Enterprise user.
enterprise.segments.maximum	Specifies the default value for the maximum number of segments allowed for a new or existing Enterprise user. The default value for any Enterprise user is 16. **Note** This value must be less than or equal to the number defined in the system property, enterprise.segments.system.maximum. It is not recommended for you to change the value of this system property if you want to enable 128 segments for an Enterprise user. Instead, you can enable **Customer Capabilities** in the **Customer Configuration** page to configure the required number of segments. For instructions, refer to the "Configure Customer Capabilities" section in the VMware SD-WAN Operator Guide available at VMware SD-WAN Documentation.
enterprise.subinterfaces.maximum	Specifies the maximum number of sub-interfaces that can be configured for an Enterprise user. The default value is 32.
enterprise.vlans.maximum	Specifies the maximum number of VLANs that can be configured for an Enterprise user. The default value is 32.
session.options.enableAsyncAPI	When the segment scale is increased to 128 segments for any Enterprise user, to prevent UI timeouts, you can enable Async APIs support on the UI by using this system property. The default value is true.
session.options.asyncPollingMilliSeconds	Specifies the Polling interval for Async APIs on the UI. The default vaue is 5000 milliseconds.
session.options.asyncPollingMaxCount	Specifies the maximum number of calls to getStatus API from the UI. The default value is 10.
vco.enterprise.events.configuration.diff.enable	Activates or deactivates configuration diff event logging. Whenever the number of segments for an Enterprise user is greater than 4, the configuration diff event logging will be deactivated. You can enable configuration diff event logging using this system property.

Table 1-14. Self-service Password Reset

System Property	Description
vco.enterprise.resetPassword.twoFactor.mode	Defines the mode for the second level for password reset authentication, for all the Enterprise users. Currently, only the SMS mode is supported.
vco.enterprise.resetPassword.twoFactor.required	Activates or deactivates the two-factor authentication for password reset of Enterprise users.
vco.enterprise.selfResetPassword.enabled	Activates or deactivates self-service password reset for Enterprise users.
vco.enterprise.selfResetPassword.token.expirySeconds	Duration of time, after which the self-service password reset link for an Enterprise user expires.
vco.operator.resetPassword.twoFactor.required	Activates or deactivates the two-factor authentication for password reset of Operator users.
vco.operator.selfResetPassword.enabled	Activates or deactivates self-service password reset for Operator users.
vco.operator.selfResetPassword.token.expirySeconds	Duration of time, after which the self-service password reset link for an Operator user expires.

Table 1-15. Two-factor Authentication

System Property	Description
vco.enterprise.authentication.twoFactor.enable	Activates or deactivates the two-factor authentication for Enterprise users.
vco.enterprise.authentication.twoFactor.mode	Defines the mode for the second level authentication for Enterprise users. Currently, only SMS is supported as the second level authentication mode.
vco.enterprise.authentication.twoFactor.require	Defines the two-factor authentication as mandatory for Enterprise users.
vco.operator.authentication.twoFactor.enable	Activates or deactivates the two-factor authentication for Operator users.
vco.operator.authentication.twoFactor.mode	Defines the mode for the second level authentication for Operator users. Currently, only SMS is supported as the second level authentication mode.
vco.operator.authentication.twoFactor.require	Defines the two-factor authentication as mandatory for Operator users.

Table 1-16. VNF Configuration

System Property	Description

edge.vnf.extraImageInfos	Defines the properties of a VNF Image.
	You can enter the following information for a VNF Image, in JSON format in the **Value** field:
	`[ { "vendor": "Vendor Name", "version": "VNF Image Version", "checksum": "VNF Checksum Value", "checksumType": "VNF Checksum Type" } ]`
	Example of JSON file for Check Point Firewall Image:
	`[ { "vendor": "checkPoint", "version": "r80.40_no_workaround_46", "checksum": "bc9b06376cdbf210cad8202d728f1602b79cfd7d", "checksumType": "sha-1" } ]`
	Example os JSON file for Fortinet Firewall Image:
	`[ { "vendor": "fortinet", "version": "624", "checksum": "6d9e2939b8a4a02de499528c745d76bf75f9821f", "checksumType": "sha-1" } ]`

edge.vnf.metric.record.limit	Defines the number of records to be stored in the database
enterprise.capability.edgeVnfs.enable	Enables VNF deployment on supported Edge models.
enterprise.capability.edgeVnfs.securityVnf.checkPoint	Enables Check Point Networks Firewall VNF
enterprise.capability.edgeVnfs.securityVnf.fortinet	Enables Fortinet Networks Firewall VNF
enterprise.capability.edgeVnfs.securityVnf.paloAlto	Enable Palo Alto Networks Firewall VNF
session.options.enableVnf	Enables VNF feature
vco.operator.alert.edgeVnfEvent.enable	Activates or deactivates Operator alerts for Edge VNF events globally
vco.operator.alert.edgeVnfInsertionEvent.enable	Activates or deactivates Operator alerts for Edge VNF Insertion events globally

Table 1-17. VPN

System Property	Description
vpn.disconnect.wait.sec	The time interval for the system to wait before disconnecting a VPN tunnel.
vpn.reconnect.wait.sec	The time interval for the system to wait before reconnecting a VPN tunnel.

Configure SD-WAN Orchestrator Disaster Recovery

This section provides disaster recovery (DR) instructions for SD-WAN Orchestrator.

SD-WAN Orchestrator Disaster Recovery Overview

The SD-WAN Orchestrator Disaster Recovery (DR) feature prevents the loss of stored data and resumes SD-WAN Orchestrator services in the event of system or network failure.

SD-WAN Orchestrator DR involves setting up an active/standby SD-WAN Orchestrator pair with data replication and a manually-triggered failover mechanism.

- The recovery time objective (RTO), therefore, is dependent on explicit action by the operator to trigger promotion of the standby.
- The recovery point objective (RPO), however, is essentially zero, regardless of the recovery time, because all configuration is instantaneously replicated. Monitoring data that would have been collected during the outage is cached on the edges and gateways pending promotion of the standby.

Note DR is mandatory. For licensing and pricing, contact the VMware sales team for support.

Active/Standby Pair

In a SD-WAN Orchestrator DR deployment, two identical SD-WAN Orchestrator systems are configured as an active / standby pair. The operator can view the state of DR readiness through the web UI on either of the servers. Edges and gateways are aware of both SD-WAN Orchestrators, and while they receive configuration changes only from the active SD-WAN Orchestrator, they periodically send DR heartbeats to both systems to report their view of both servers and to query the DR system status. When the operator triggers a failover, the edges and gateways are informed of the change in their next DR heartbeat.

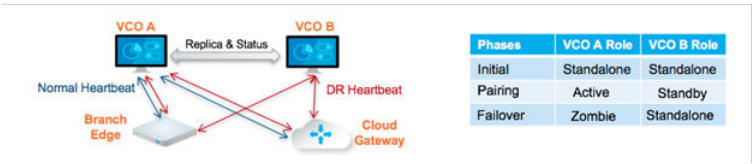
DR States

From the view of an operator, and of the edges and gateways, a SD-WAN Orchestrator has one of four DR states:

DR State	Description
Standalone	No DR configured.
Active	DR configured, acting as the primary SD-WAN Orchestrator server.
Standby	DR configured, acting as an inactive replica SD-WAN Orchestrator server.
Zombie	DR formerly configured and active but no longer acting as the active or standby.

Run-time Operation

When DR is configured, the standby server runs in a limited mode, blocking all API calls except those related to the DR status and the DR heartbeats. When the operator invokes a failover, the standby is promoted to become fully operational as a Standalone server. The server that was formerly active is automatically transitioned to a Zombie state if it is responsive and visible from the promoted standby. In the Zombie state, management configuration services are blocked and any contact from edges and gateways that have not transitioned to the new active SD-WAN Orchestrator are redirected to the promoted server.



Phases	VCO A Role	VCO B Role
Initial	Standalone	Standalone
Pairing	Active	Standby
Failover	Zombie	Standalone

Set Up SD-WAN Orchestrator Replication

Two installed SD-WAN Orchestrator instances are required to initiate replication.

- The selected standby is put into a `STANDBY_CANDIDATE` state, enabling it to be configured by the active server.
- The active server is then given the address and credentials of the standby and it enters the `ACTIVE_CONFIGURING` state.

When a `STANDBY_CONFIG_RQST` is made from active to standby, the two servers synchronize through the state transitions.

The two Orchestrators on which Disaster Recovery (DR) need to be established must have same time. Before you initiate SD-WAN Orchestrator replication, ensure you check the following NTP configurations:

- The Gateway time zone must be set to **Etc/UTC**. Use the following command to view the NTP time zone.

```
vcadmin@vcg1-example:~$ cat /etc/timezone
Etc/UTC
vcadmin@vcg1-example:~$
```

If the time zone is incorrect, use the following commands to update the time zone.

```
echo "Etc/UTC" | sudo tee /etc/timezone
sudo dpkg-reconfigure --frontend noninteractive tzdata
```

- The NTP offset must be less than or equal to 15 milliseconds. Use the following command to view the NTP offset.

```
sudo ntpqvcadmin@vcg1-example:~$ sudo ntpq -p
     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*ntp1-us1.prod.v 74.120.81.219    3 u  474 1024  377   10.171   -1.183   1.033
 ntp1-eu1-old.pr .INIT.          16 u    - 1024    0    0.000    0.000   0.000
vcadmin@vcg1-example:~$
```

If the offset is incorrect, use the following commands to update the NTP offset.

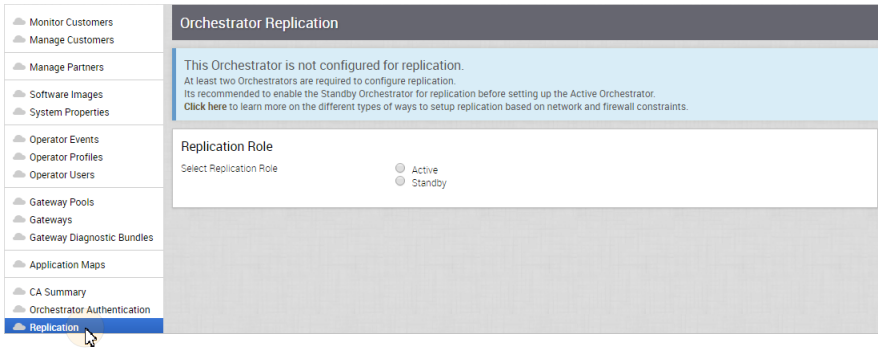
```
sudo systemctl stop ntp
sudo ntpdate <server>
sudo systemctl start ntp
```

- By default, a list of NTP Servers are configured in the `/etc/ntpd.conf` file. The Orchestrators on which DR need to be established must have Internet to access the default NTP Servers and ensure the time is in sync on both the Orchestrators. Customers can also use their local NTP server running in their environment to sync time.

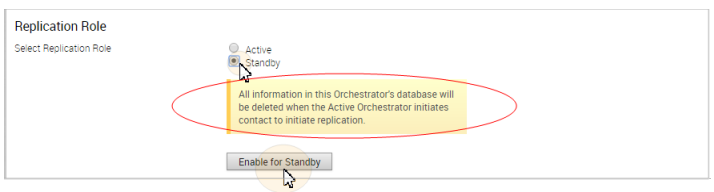
Set Up the Standby Orchestrator

To set up SD-WAN Orchestrator replication, perform the following steps:

1 Click **Replication** from the Navigation panel to display the **Orchestrator Replication** screen.

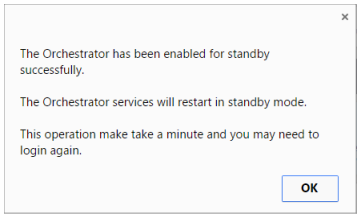


2 Enable the Standby Orchestrator by selecting the **Standby (Replication Role)** radio button.

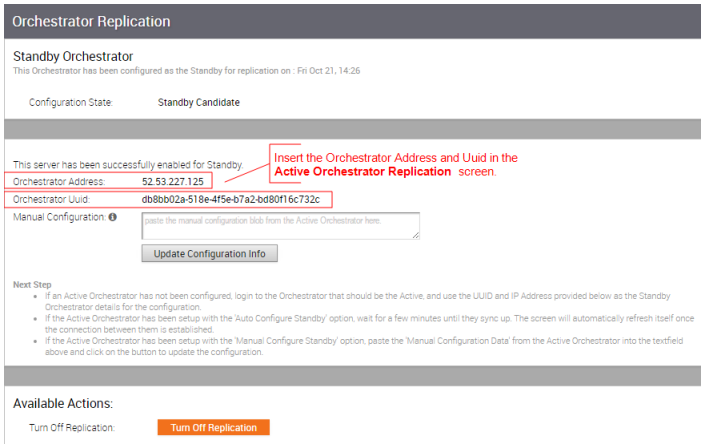


3 Click the **Enable for Standby** button.

The **Orchestrator Success** dialog box appears, indicating that the Orchestrator has been enabled for Standby, and that the Orchestrator will restart in Standby mode.



4 Click **OK**.



After the Standby Orchestrator has been configured for replication, configure the Active Orchestrator according to the instructions below.

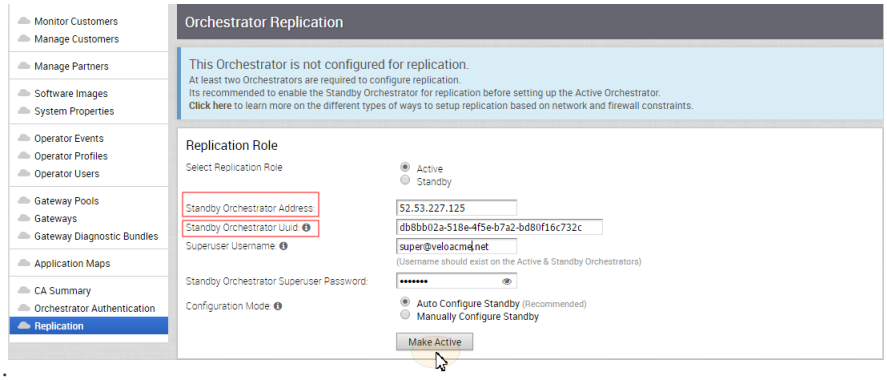
Set Up the Active Orchestrator

To configure the second SD-WAN Orchestrator to be the Active Orchestrator:

1 Click **Replication** from the Navigation panel. The **Orchestrator Replication** screen appears.

2 Choose the **Active Replication Role**.

3 Type in the **Standby Orchestrator Address** and the **Standby Orchestrator Uuid**. The Orchestrator Address and Uuid are displayed in the **Standby Orchestrator** screen.

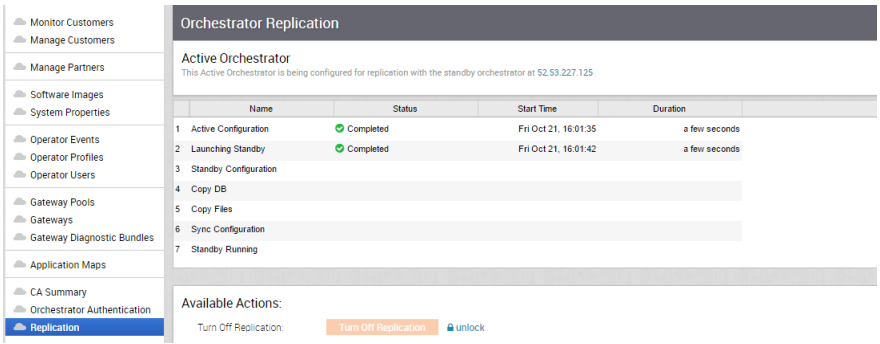


4 Type in the username and password for the Orchestrator Superuser to be used for replication.

Note This Superuser should already exist on both systems.

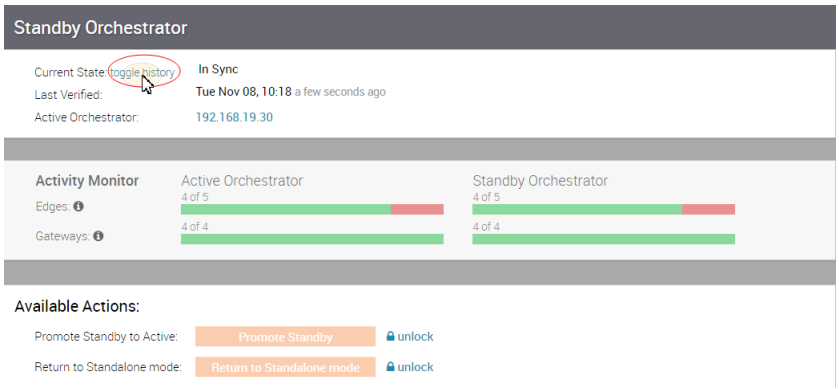
5 Click the **Make Active** button.

The **Active Orchestrator** screen displays showing a status of the current state.

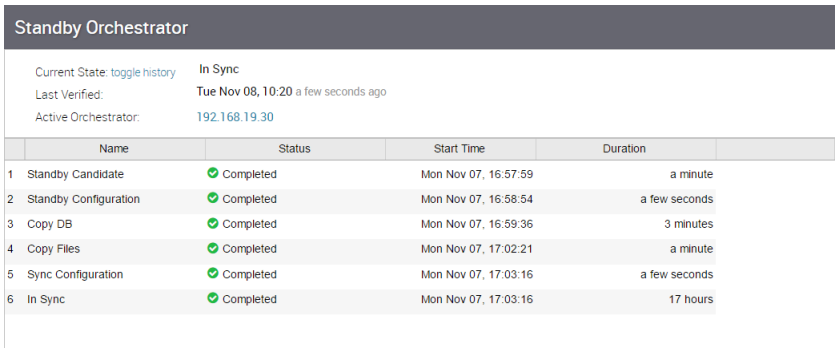


When configuration is complete, both Orchestrators (Standby and Active) will be in sync.

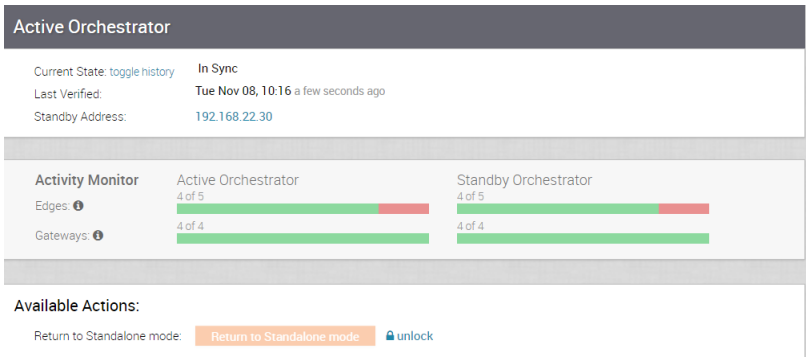
Standby Orchestrator in Sync



You can click the **toggle history** link to view the status of each state.



Active Orchestrator in Sync



Test Failover

The following testing failover scenarios are forced failovers for example purposes. You can perform these actions in the **Available Actions** area of the **Active** and **Standby** screens.

Promote a Standby Orchestrator

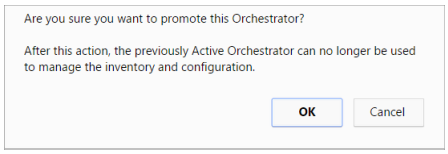
This section describes how to promote a Standby Orchestrator.

To promote a Standby Orchestrator

1 Click the **unlock** link.

2 Click the **Promote Standby** button in the **Available Actions** area on the Standby Orchestrator screen.

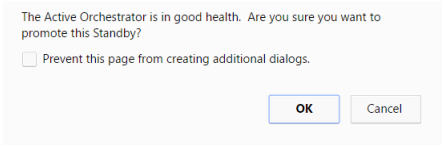
The following dialog box appears, indicating that when you promote your Standby Orchestrator, administrators will no longer be able to manage the SD-WAN Orchestrator using the previously Active Orchestrator.



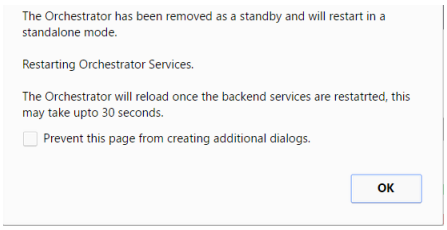
3 Click the **OK** button to promote the Standby Orchestrator.

Another message dialog box appears to verify your request to promote the Standby Orchestrator. This message will appear only if the Standby Orchestrator perceives the Active Orchestrator to be in good health, meaning the Standby is communicating with the Active and duplicating data.

4 Click **OK** to promote the Orchestrator.

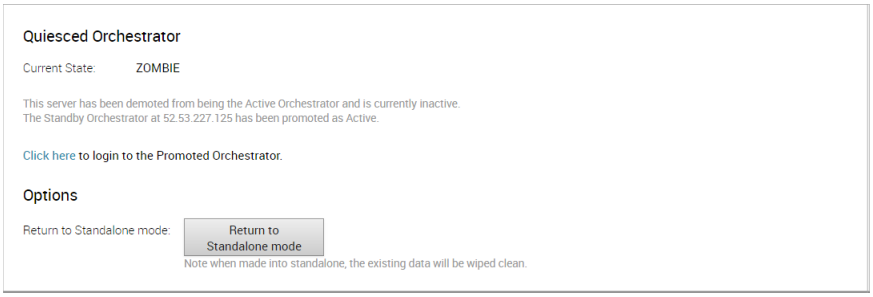


A final dialog box appears indicating that the Orchestrator is no longer a Standby and will restart in Standalone mode.



When you promote a Standby Orchestrator, it restarts in Standalone mode.

If the Standby can communicate with the formerly Active Orchestrator, it will instruct that Orchestrator to enter a Zombie state. In Zombie state, the Orchestrator communicates with its clients (edges, gateways, UI/API) that it is no longer active, and that they must communicate with the newly promoted Orchestrator. If the promoted Standby cannot communicate with the formerly Active Orchestrator, the operator should, if possible, manually demote the formerly Active Orchestrator.



Return to Standalone Mode

To return the Zombie to standalone mode, click the **Return to Standalone Mode** button in the **Available Actions** area on the **Active Orchestrator** or **Standby Orchestrator** screens.

Note The Orchestrator can be returned to the Standalone mode from the Zombie state after the time specified in the system property "vco.disasterRecovery.zombie.expirySeconds," which is defaulted to 1800 seconds.

Troubleshooting SD-WAN Orchestrator DR

This section describes the failure states of the system. These are also listed in the UI, along with a more detailed description of the failure. Additional information is available in the VMware log.

Recoverable Failures

The following errors are recoverable failures that can occur after SD-WAN Orchestrator DR reaches an in sync state. If the problem causing these failures is corrected, SD-WAN Orchestrator DR will automatically return to normal operation.

- `FAILURE_SYNCING_FILES`
- `FAILURE_GET_STANDBY_STATUS`
- `FAILURE_MYSQL_ACTIVE_STATUS`
- `FAILURE_MYSQL_STANDBY_STATUS`

Unrecoverable Failures

The following failures can occur during configuration of the SD-WAN Orchestrator DR. SD-WAN Orchestrator DR will not automatically recover from these failures.

- `FAILURE_ACTIVE_CONFIGURING`
- `FAILURE_LAUNCHING_STANDBY`
- `FAILURE_STANDBY_CONFIGURING`
- `FAILURE_COPYING_DB`
- `FAILURE_COPYING_FILES`
- `FAILURE_SYNC_CONFIGURING`
- `FAILURE_GET_STANDBY_CONFIG`
- `FAILURE_STANDBY_CANDIDATE`
- `FAILURE_STANDBY_UNCONFIG`
- `FAILURE_STANDBY_PROMOTION`
- `FAILURE_ACTIVE_DEMOTION`

Upgrade SD-WAN Orchestrator with DR Deployment

This section describes how to upgrade the SD-WAN Orchestrator with DR deployment.

SD-WAN Orchestrator Upgrade Overview

The following steps are required to upgrade a SD-WAN Orchestrator.

For SD-WAN Orchestrator Disaster Recovery, see " Set Up DR in the VMware" and " Upgrade the DR Setup."

1 Step 1: Prepare for the Orchestrator Upgrade

2 Step 2: Send Upgrade Announcement

3 Step 3: Proceed with the Orchestrator upgrade

4 Step 4: Complete the Orchestrator Upgrade

Upgrade an Orchestrator

This section describes how to upgrade an Orchestrator.

Step 1: Prepare for the Orchestrator Upgrade

Contact the VMware Support team to prepare for the Orchestrator upgrade as described in this section.

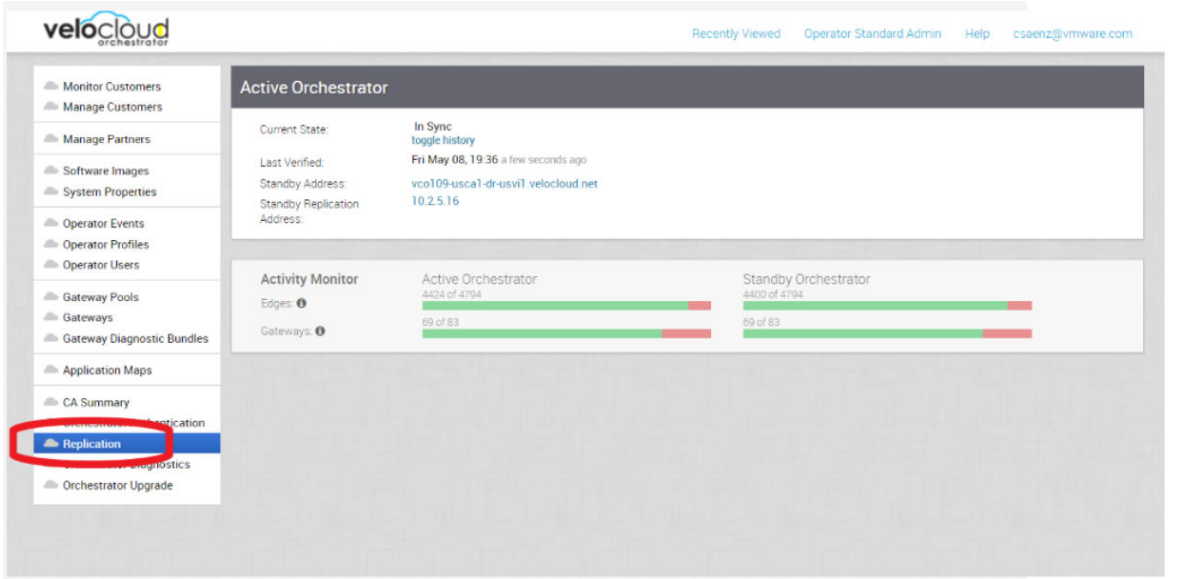
To upgrade SD-WAN Orchestrator:

1 VMware Support will assist you with your upgrade. Collect the following information prior to contacting Support.

- Provide the current and target Orchestrator versions, for example: current version (ie 2.5.2 GA-20180430), target version (3.3.2 p2).

  Note For the current version, this information can be found on the top, right corner of the Orchestrator by clicking the **Help** link and choosing **About**.

- Provide a screenshot of the replication dashboard of the Orchestrator as shown below.



- Hypervisor Type and version (ie vSphere 6.7)

- Commands from the Orchestrator:

  Note Commands must be run as root (e.g. ‘sudo <command>’ or ‘sudo -i’).

  - Run the script /opt/vc/scripts/vco_upgrade_check.sh to check:
    - LVM layout
    - Memory Information
    - CPU Information
    - Kernel Parameters
    - Some system properties
    - ssh configurations
    - Mysql schema and database sizes
    - File_store locations and sizes
  - Copy of /var/log
    - tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
  - From the Standby Orchestrator:
    - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'
- From the Active Orchestrator:
  - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'

2 Contact VMware Support at https://kb.vmware.com/s/article/53907 with the above-mentioned information for assistance with the Orchestrator upgrade.

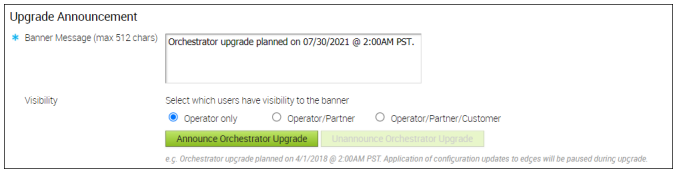
Step 2: Send Upgrade Announcement

The **Upgrade Announcement** area enables you to configure and send a message about an upcoming upgrade. This message will be displayed to all users the next time they login to the SD-WAN Orchestrator.

To send an upgrade announcement:

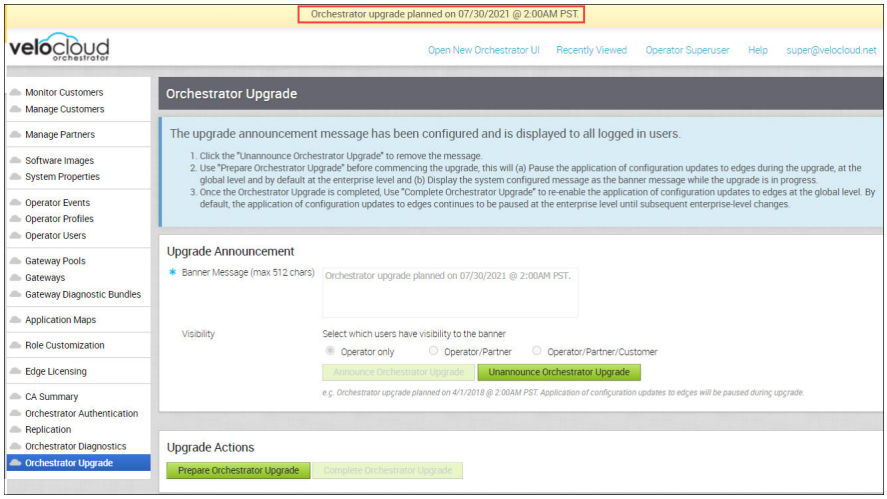
1 From the SD-WAN Orchestrator, select **Orchestrator Upgrade** from the navigation panel.

2 In the **Upgrade Announcement** area, type in your message in the **Banner Message** text box.



3 Click the **Announce Orchestrator Upgrade** button.

A popup message appears indicating that you have successfully created your announcement, and that your banner message displays at the top of the SD-WAN Orchestrator.



4 (Optional) You can remove the announcement from the SD-WAN Orchestrator by clicking the **Unannounce Orchestrator Upgrade** button. A popup message will appear indicating that you have successfully unannounced the Orchestrator upgrade. The announcement that was displayed at the top of the SD-WAN Orchestrator will be removed.

Step 3: Proceed with the Orchestrator Upgrade

Contact VMware Support at https://kb.vmware.com/s/article/53907 for assistance with the Orchestrator upgrade.

Step 4: Complete the Orchestrator Upgrade

After you have completed the Orchestrator upgrade, click the **Complete Orchestrator Upgrade** button. This re-enables the application of the configuration updates of Edges at the global level.

To verify that the status of the upgrade is complete, run the following command to display the correct version number for all the packages:

```
dpkg -l|grep vco
```

When you are logged in as an Operator, the same version number should display at the bottom right corner of the SD-WAN Orchestrator.

Upgrade VMware SD-WAN Orchestrator from version 3.3.2 or 3.4 to version 4.0

This document provides and overview and best practices on how to upgrade the VMware SD-WAN Orchestrator from the 3.3.2 or 3.4 release to the 4.0 release. However, please contact VMware Support to asssit you with the 3.3.2 or 3.4 to 4.0 upgrade at https://kb.vmware.com/s/article/53907

Only 3.3.2 and 3.4 Orchestrators can be upgraded to the 4.0 release. If you are running a 3.3.1 or lower version of the Orchestrator, you must upgrade to at least the 3.3.2 version before upgrading to the 4.0 version.

Consider the following when upgrading:

- This upgrade work does not modify any existing APIs.
- Just like other releases, there are schema changes with the 4.0 release. However, these changes will not impact the upgrade process.

The OS for the SD-WAN Orchestrator virtual appliance and the underlying data stores that store the configuration and statistics data are being upgraded. The specific upgrades include the following:

- The OS version is changing from Ubuntu 14.04 to 18.04.
- The Config store is moving to MySQL 8.0.
- The Stats store is moving to ClickhouseDB.

Note The Orchestrator OS, database, and several other dependent components currently in use have reached their end of life, and will no longer be supported.

The benefits to upgrading to the 4.0 release are as follows:

- A better scale overall in terms of number of Edges, flows, and UI.
- Faster query performance for statistics, longer retention out of the box for flow stats.
- Faster initial Disaster Recovery (DR) setup performance.
- Lower resource utilization - Disk, CPU, RAM.
- Better security due to components with active LTS.

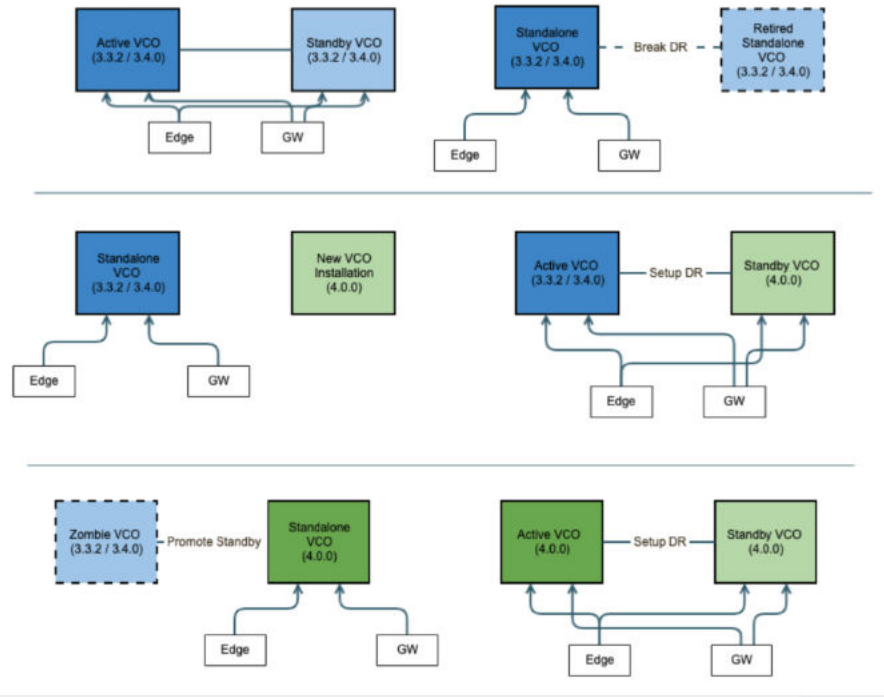
Best Practices/Recommendations:

Listed below are some upgrade best practices:

- From the System Properties page in the Orchestrator, make a note of the value of the edge.heartbeat.spread.factor system property. Then, change the heartbeat spread factor to a relatively high value for a large Orchestrator (e.g. 20, 40, 60). This will help reduce the sudden spike of the resource utilization (CPU, IO) on the system. Make sure to verify that all Gateways and Edges are in a connected state before restoring the previous edge.heartbeat.spread.factor value from the System Property page in the Orchestrator.
- Leave the demoted SD-WAN Orchestrator up for a few hours before complete shutdown or decommission.
- Freeze configuration modifications to avoid any additional configuration changes until the upgrade process is completed.

Upgrade Procedure Overview

This document provides the steps required to upgrade 3.3.2 or 3.4 release to the 4.0 release. The SD-WAN Orchestrator OS and Disaster Recovery upgrade have some of the same steps as the Disaster Recovery procedures as found in the Configure SD-WAN Orchestrator Disaster Recovery. However, follow the steps in Upgrade Procedures section in this document to complete the 3.3.2 or 3.4 release to the 4.0 release upgrade process. The image below depicts an illustration of the upgrade process. See the Upgrade Procedures below.



Upgrade Procedures

Please contact VMware Support to assist you with the 3.3.2 or 3.4 to 4.0 upgrade at https://kb.vmware.com/s/article/53907

SD-WAN Orchestrator Disaster Recovery

This section describes how to set up and upgrade disaster recovery in the SD-WAN Orchestrator.

Set Up DR in the VMware

To set up disaster recovery in the SD-WAN Orchestrator:

1 Install a new SD-WAN Orchestrator whose version matches the version of the VMware that is currently the Active SD-WAN Orchestrator.

2 Set the following properties on the Active and Standby SD-WAN Orchestrator, if necessary.

   - `vco.disasterRecovery.transientErrorToleranceSecs` to a non-zero value (Defaults to 900 seconds in version 3.3 and later, zero in earlier versions). This prevents any transient errors from resulting in an Edge/Gateway management plane update.
   - `vco.disasterRecovery.mysqlExpireLogsDays` (Defaults to 1 day). This is the amount of time the Active SD-WAN Orchestrator keeps the mysql binlog data.

3 Set up the `network.public.address` property on the Active and Standby to the address contacted by the Edges (Heartbeats).

4 Set up DR by following the usual DR Setup procedure that is described in *SD-WAN Orchestrator Disaster Recovery*.

Upgrade the DR Setup

To upgrade a DR-enabled SD-WAN Orchestrator pair, follow the steps below.

To upgrade a DR-enabled VCO pair:

Note If the Orchestrator upgrade is from 2.X -> 3.2.X, run dr-standby-schema.sh on the Standby before starting the upgrade.

1 Prepare for the Upgrade. For instructions, go to Step 1: Prepare for the Orchestrator Upgrade of the section titled, Upgrade an Orchestrator with DR Deployment.

2 Proceed with the Orchestrator Upgrade. For instructions, go to Step 3: Proceed with the Orchestrator Upgrade of the section titled, Upgrade an Orchestrator with DR Deployment.

Troubleshooting SD-WAN Orchestrator

This section describes SD-WAN Orchestrator troubleshooting.

Orchestrator Diagnostics

This section describes Orchestrator Diagnostics.

SD-WAN Orchestrator Diagnostics Overview

The SD-WAN Orchestrator Diagnostics bundle is a collection of diagnostic information that is required for Support and Engineering to troubleshoot the SD-WAN Orchestrator. For Orchestrator on-prem installation, Operators can collect the SD-WAN Orchestrator Diagnostic bundle from the Orchestrator UI and provide it to the VMware Support team for offline analysis and troubleshooting.

SD-WAN Orchestrator Diagnostics includes the following two diagnostic bundles:

- Diagnostic Bundles Tab: Request and download a diagnostic bundle. This information can be found in the VMware SD-WAN Orchestrator Deployment and Monitoring Guide. See the section titled, "Diagnostic Bundle Tab."

- Database Statistics Tab: Provides a read-only access view of some of the information from a diagnostic bundle. This information can be found in the VMware SD-WAN Orchestrator Deployment and Monitoring Guide. See the section titled, "Database Statistics Tab."

Diagnostics Bundle Tab

Users can request and download a diagnostic bundle in the **Diagnostics Bundle** tab.

Columns in the Diagnostics Bundle Tab

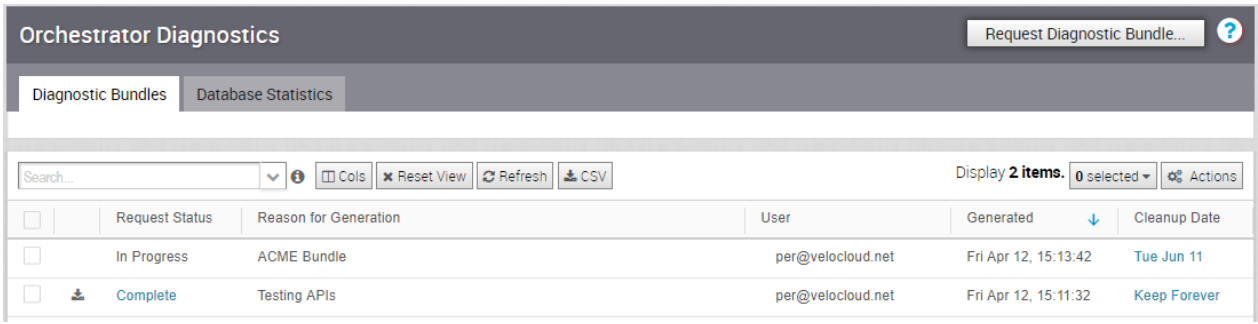
The Orchestrator Diagnostics table grid includes the following columns:

Column Name	Description
Request Status	There are two types of status requests: ■ Complete ■ In Progress If a bundle has not completed the download, the **In Progress** status appears.
Reason for Generation	The specific reason given for generating a diagnostic bundle. Click the **Request Diagnostic Bundle** button to include a description of the bundle.
User	The individual logged into the SD-WAN Orchestrator.
Generated	The date and time when the diagnostic bundle request was sent.
Cleanup Date	The default **Cleanup Date** is three months after the generated date, when the bundle will be automatically deleted. If you need to extend the Cleanup date period, click the **Cleanup Date** link located under the **Cleanup Date** column. For more information, see *Updating Cleanup Date*.

Request a Diagnostic Bundle

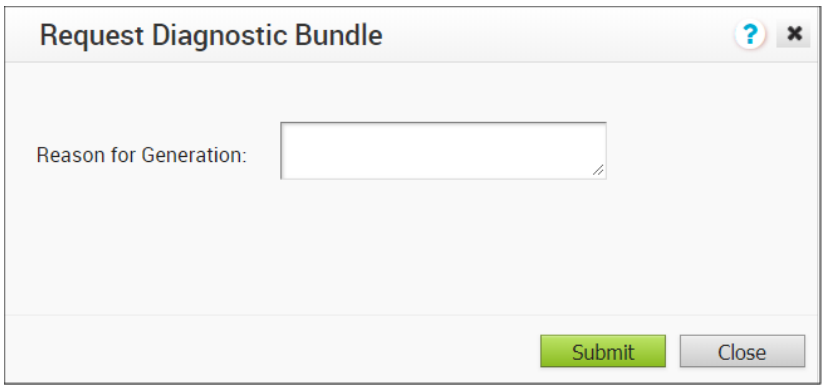
To request a diagnostic bundle:

1 From the SD-WAN Orchestrator navigation panel, click **Orchestrator Diagnostics** .



2 From the **Request Diagnostic Bundle** tab, click the **Request Diagnostic Bundle** button.

3 In the **Request Diagnostic Bundle** dialog, enter the reason for the request in the appropriate area.



4 Click **Submit**. The bundle request you created displays in the grid area of the **Diagnostic Bundle** screen with an **In Progress** status.

5 Refresh your screen to check the status of diagnostic bundle request. When the bundle is ready for download, a **Complete** status appears.

Download a Diagnostic Bundle

To download a diagnostic bundle:

1 Select a diagnostic bundle you want to download.

2 Click the **Actions** button, and choose **Download Diagnostic Bundle**. You can also click the **Complete** link to download the diagnostics bundle.

The diagnostics bundle downloads.

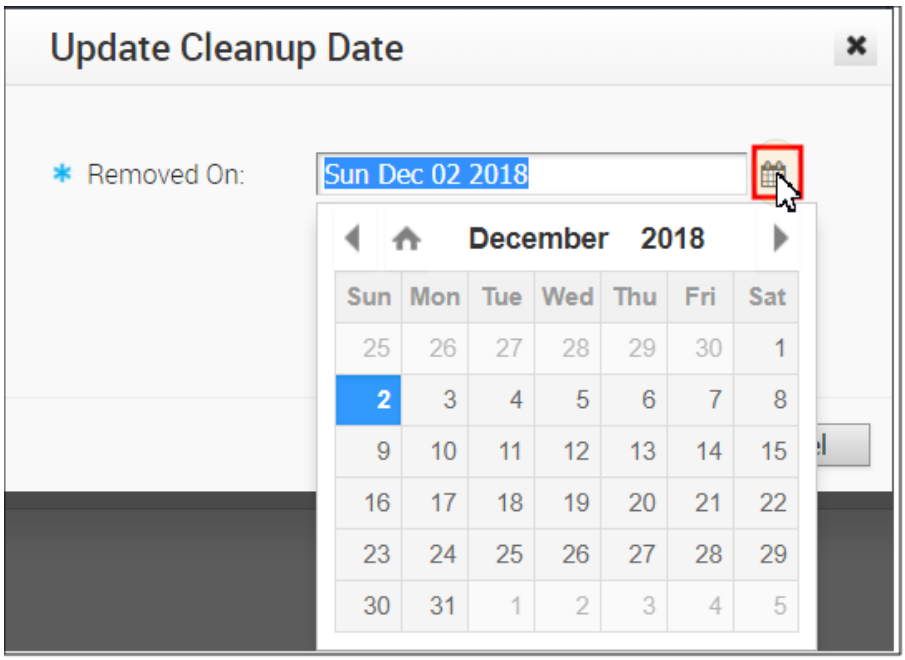
Update the Cleanup Date

The Cleanup date represents the date when the generated bundle will be automatically deleted, which by default is three months after the Generated date. You can change the Cleanup date or choose to keep the bundle indefinitely.

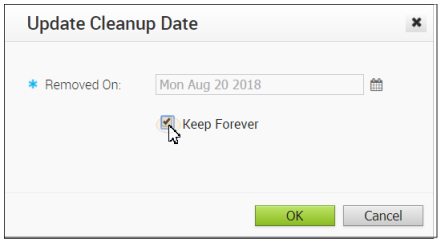
To update the Cleanup date:

1 From the **Cleanup Date** column, click the **Cleanup Date** link of your chosen Diagnostic Bundle.

2 From the **Update Cleanup Date** dialog, click the **Calendar** icon to change the date.

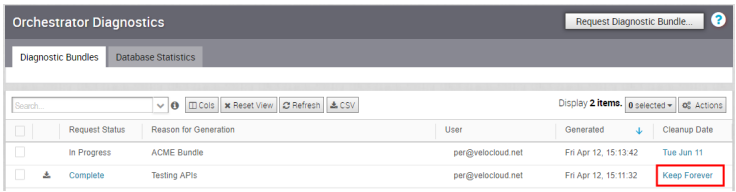


3 You can also choose to keep the bundle indefinitely by checking the **Keep Forever** checkbox.



4 Click **OK**.

The Orchestrator Diagnostics table grid updates to reflect the changes to the Cleanup Date.

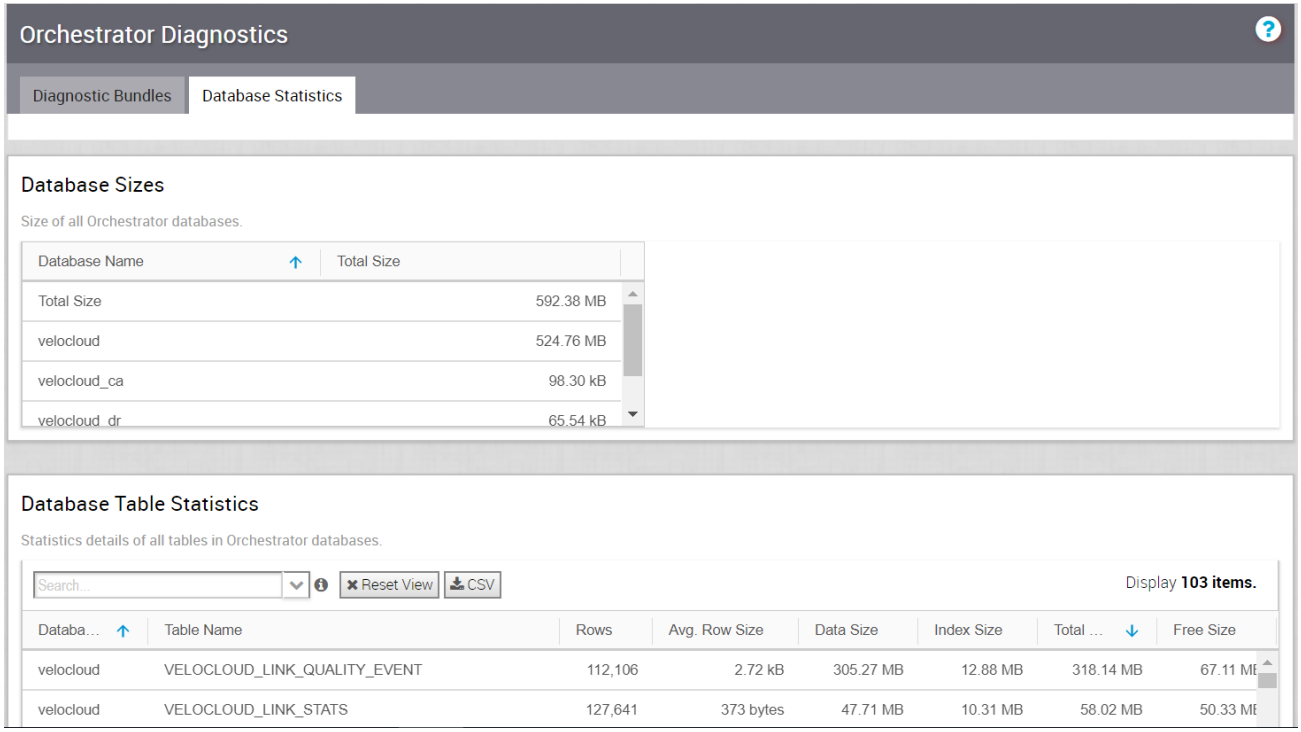


Database Statistics Tab

The **Database Statistics** tab provides a read-only access view of some of the information from a diagnostic bundle.

If you require additional information, go to the **Diagnostic Bundles** tab, request a diagnostic bundle, and download it locally. For more information, see *Request Diagnostic Bundle*.

The **Database Statistics** tab displays the following information:



Field	Description
Database Sizes	Sizes of the Orchestrator databases.
Database Table Statistics	Statistical details of all tables in the Orchestrator database.
Database Storage Info	Storage details of the mounted locations.
Database Process List	The top 20 records of long-running SQL queries.
Database Status Variable	The status variables of the MySQL server.
Database System Variable	System variables of the MySQL server.
Database Engine Status	The InnoDB engine status of the MySQL server.

System Metrics Monitoring

This section describes System Metrics Monitoring on the Orchestrator.

Orchestrator System Metrics Monitoring Overview

The Orchestrator comes with a built-in system metrics monitoring stack, which includes a metrics collector and a time-series database. With the monitoring stack, you can easily check the health condition and the system load for the Orchestrator.

To enable the monitoring stack, run the following command on the orchestrator:

```
sudo /opt/vc/scripts/vco_observability_manager.sh enable
```

To check the status of the monitoring stack, run:

```
sudo /opt/vc/scripts/vco_observability_manager.sh status
```

To deactivate the monitoring stack, run:

```
sudo /opt/vc/scripts/vco_observability_manager.sh disable
```

The Metrics Collector

Telegraf is used as the Orchestrator system metrics collector, which includes plugins to collect system metrics. The following metrics are enabled by default.

Metric Name	Description
inputs.cpu	Metrics about CPU usage.
inputs.mem	Metrics about memory usage.
inputs.net	Metrics about network interfaces.
inputs.system	Metrics about system load and uptime.
inputs.processes	The number of processes grouped by status.
inputs.disk	Metrics about disk usage.
inputs.diskio	Metrics about disk IO by device.
inputs.procstat	CPU and memory usage for specific processes.
inputs.nginx	Nginx's basic status information (ngx_http_stub_status_module).
inputs.mysql	Statistic data from the MySQL server.
inputs.clickhouse	Metrics from one or many ClickHouse servers.
inputs.redis	Metrics from one or many redis servers.
inputs.filecount	The number and total size of files in specified directories.
inputs.ntpq	Standard NTP query metrics (requires ntpq executable).
Inputs.x509_cert	Metrics from a SSL certificate.

To activate more metrics or deactivate some enabled metrics, edit the Telegraf configuration file on the Orchestrator by the following:

- sudo vi /etc/telegraf/telegraf.d/system_metrics_input.conf
- sudo systemctl restart telegraf

The Time-series Database

Prometheus is used to store the system metrics collected by Telegraf. The metrics data will be kept in the database for three weeks at the most. By default, Prometheus listens on port 9090. If you have an external monitoring tool, provide the Prometheus database as a source, so that you can view the Orchestrator system metrics on your monitoring UI.

Rate Limiting API Requests

When there are too many API requests sent at a time, it affects the performance of the system. You can enable Rate Limiting, which enforces a limit on the number of API requests sent by each user.

The SD-WAN Orchestrator makes use of certain defence mechanisms that curb API abuse and provides system stability. API requests that exceed the allowed request limits are blocked and returned with HTTP 429 (Too many Requests). The system needs to go through a cool down period before making the requests again.

The following types of Rate-Limiters are deployed on SD-WAN Orchestrator:

- **Leaky bucket limiter** – Smooths the burst of requests and only allows a pre-defined number of requests. This limiter takes care of limiting the number of requests allowed in a given time window.
- **Concurrency limiter** – Limits the number of requests that occur in parallel which leads to concurrent requests fighting for resources and may result in long running queries.

The following are the major reasons that lead to rate limiting of the API requests:

- Large number of active or concurrent requests.
- Sudden spikes in request volume.
- Requests resulting in long running queries on the Orchestrator holding system resources for long being dropped.

Developers that rely on the API can adopt the following measures to improve the stability of their code when the VCO rate-limiting capability is enabled.

- Handle HTTP 429 response code when requests exceed rate limits.
- The penalty time duration is 5000 ms when the rate limiter reaches the maximum allowed requests in a given period. If blocked, the clients are expected to have a cool down period of 5000 ms before making requests again. The requests made during the cool down period of 5000 ms will still be rate limited.
- Use shorter time intervals for time series APIs which will not let the request to expire due to long running queries.

- Prefer batch query methods to those that query individual Customers or Edges whenever possible.

Note Operator Super users configure Rate limits discretely based on the environment. For any queries on relevant policies, contact your Operator.

Configure Rate Limiting Policies using System Properties

You can use the following system properties to enable Rate Limiting and define the default set of policies:

- vco.api.rateLimit.enabled
- vco.api.rateLimit.mode.logOnly
- vco.api.rateLimit.rules.global
- vco.api.rateLimit.rules.enterprise.default
- vco.api.rateLimit.rules.enterpriseProxy.default

For more information on the system properties, see Table 1-11. Rate Limiting APIs.

Configure Rate Limiting Policies using APIs

It is recommended to configure the rate limiter policies as global rules using the system properties, as this approach produces the best possible API performance, facilitates troubleshooting, and ensures a consistent user experience across all Partners and Customers. In rare cases, however, Operators may determine that global policies are too lax for a particular tenant or user. For such cases, VMware supports the following operator-only APIs to set policies for specific partners and enterprises.

- **enterpriseProxy/insertOrUpdateEnterpriseProxyRateLimits** – Used to configure Partner-specific policies.
- **enterprise/insertOrUpdateEnterpriseRateLimits** – Used to configure Customer-specific policies.

For more information on the APIs, see https://code.vmware.com/apis/1037/velocloud-sdwan-vco-api.

Enterprise Deployment & Operations for SD-WAN Orchestrator

This section provides information about the available options to monitor, backup, and upgrade Enterprise On-Premises deployments in a two-day operation scenario.

Overview

Even though the enterprise on-premises model has some unique advantages and features, there are considerations that the service provider or customer managing the solution must understand. Some of these considerations are as follows:

- Isolation of the solution: The VMware Cloud Operations team will not have access to apply hotfixes and upgrades.
- Restrictions on change management limit the frequency of patching and upgrades.
- Inadequate or insufficient solution monitoring: This situation may happen due to a lack of personnel capable of managing the infrastructure, resulting in functional issues, slower resolution of problems, and customer dissatisfaction.

This approach always requires a significant investment in people and time to manage, operate, and patch properly. The table below outlines some of the elements that must be considered when managing a system on-premises.

Table 1-18. VMware Hosted Responsibility vs On-Premises Responsibility

System	Description	VMware Hosted Responsibility	On-Premises Responsibility
SD-WAN Orchestration	Application QoS and link steering policy	Yes	Yes
	Security policy for apps and SD-WAN appliances	Yes	Yes
	SD-WAN appliance provisioning and troubleshooting	Yes	Yes
	Handling of SD-WAN alerting & events	Yes	Yes
	Link performance and capacity monitoring	Yes	Yes
Hypervisor	Monitoring / alerting	No	Yes
	Compute and memory resourcing	No	Yes
	Virtual networking and storage	No	Yes
	Backup	No	Yes
	Replication	No	Yes
Infrastructure	CPU, memory, compute	No	Yes
	Switching and routing	No	Yes
	Monitoring & management systems	No	Yes

Table 1-18. VMware Hosted Responsibility vs On-Premises Responsibility (continued)

System	Description	VMware Hosted Responsibility	On-Premises Responsibility
	Capacity planning	No	Yes
	Software upgrades/ patching	No	Yes
	Troubleshooting application/infrastructure issues	No	Yes
Backup and Infrastructure DR	Backup infrastructure	No	Yes
	Regular testing of backup regime	No	Yes
	DR infrastructure	No	Yes
	DR testing	No	Yes

Two-day operation scenarios for Enterprise On-Premises deployments are explained in the two sections below, respectively (Day One Operations and Day Two Operations).

Day One Operations

Subscribe to Security Advisories

VMware Security Advisories document remediation for security vulnerabilities that are reported in VMware products. Please subscribe to the link below to receive an alert if an action is required in an on-prem component.

https://www.vmware.com/security/advisories.html

Deactivate Cloud-init on the SD-WAN Orchestrator

The data-source contains two sections: meta-data and user-data. Meta-data includes the instance ID and should not change during the lifetime of the instance, while user-data is a configuration applied on the first boot (for the instance ID in meta-data).

After the first boot up, it is recommended to deactivate the cloud-init file to speed up the SD-WAN Orchestrator boot sequence. To deactivate cloud-init, run:

```
./opt/vc/bin/cloud_init_ctl -d
```

It is not recommended to "purge" the cloud-init file with the command "apt purge cloud-init" (this procedure does not cause issues in the VMware SD-WAN Controller). Purging the cloud-init file also erases some essential SD-WAN Orchestrator tools and scripts (for instance, the upgrade and backup scripts). In case the "purge" command was used, you can restore the files using the following commands:

- Go to the folder /opt/vcrepo/pool/main/v/vco-tools

- Install the SD-WAN Orchestrator tool package from the folder: “sudo dpkg -i vco-tools_3.4.1-R341-20200423-GA-69c0f688bf.deb”. The vco-tools package name may change depending on your release. Please check the correct file name with the command "ls vco-tools."

NTP Timezone

The SD-WAN Orchestrator and Gateway timezone must be set to "Etc/UTC."

```
vcadmin@vco1-example:~$ cat /etc/timezone
Etc/UTC
vcadmin@vco1-example:~$
```

If the timezone is incorrect, it can be corrected by executing the following commands:

```
echo "Etc/UTC" | sudo tee /etc/timezone
sudo dpkg-reconfigure --frontend noninteractive tzdata
```

NTP Offset

The expectation is that the NTP offset is <= 15 milliseconds.

```
vcadmin@vco1-example:~$ sudo ntpq -p
     remote           refid      st t when poll reach   delay   offset
jitter
==============================================================================
*ntp1-us1.prod.v 74.120.81.219    3 u  474 1024  377   10.171   -1.183   1.033
ntp1-eu1-old.pr .INIT.          16 u    - 1024    0    0.000    0.000   0.000
vcadmin@vco1-example:~$
```

If the offset is incorrect, it can be corrected by executing the following commands:

```
sudo service ntp stop
sudo ntpdate <server>
sudo service ntp start
```

VMware SD-WAN Orchestrator Storage

When the SD-WAN Orchestrator is initially deployed, three partitions are created: /, /store, /store2., /store3 (version 4.0 and onwards). The partitions are created with default sizes. Please follow the instructions in the section titled, "Increasing Storage in the SD-WAN Orchestrator" for guidance in modifying the default sizes to match the design.

Additional Tasks

The SD-WAN Orchestrator requires further configuration after its implementation via the following steps:

1 Configure System Properties.

2 Set up the initial Operator Profile.

3 Set up Operator accounts.

4 Create SD-WAN Gateways.

5 Setup SD-WAN Orchestrator.

6 Create the customer account/partner account.

The configurations in the list above are out of this document's scope and can be found in the deployment guides in the VMware documentation. Detailed instructions can be found in the VMware SD-WAN Orchestrator Deployment and Monitoring Guide, section titled, "Install SD-WAN Orchestrator."

Day Two Operations

SD-WAN Orchestrator Backup

This section provides the available mechanisms to periodically backup the SD-WAN Orchestrator database to recover from Operator errors or catastrophic failure of both the Active and Standby Orchestrator.

Remember that the Disaster Recovery feature or DR is the preferred recovery method. It provides a Recovery Point Objective of nearly zero, as all configurations on the Active Orchestrator is instantly replicated. For more details on the Disaster recovery feature, refer to the next section.

Backup Using the Embedded Script

The SD-WAN Orchestrator provides an in-built configuration backup mechanism to periodically Backup the configuration to recover from Operator errors or catastrophic failure of both the Active and Standby Orchestrator. The mechanism is script-driven and is located at /opt/vc/scripts/db_backup.sh.

The script essentially takes a database dump of the configuration data and events, while excluding some of the large monitoring tables during the database dump process. Once the script is executed, backup files are created in the local directory path provided as input to the above script.

The Backup consists of two .gzs files, one containing the database schema definition and the other one containing the actual data without definition. The administrator should ensure that the backup directory location has enough disk space for the Backup.

Best Practices

- Mount a remote location and configure the backup script to it. The remote location should have the same storage as /store if flows are also being Backup.
- Before using the Backup Script, check the Disaster Recovery (DR) replication status from the SD-WAN Orchestrator replication page. They should be in sync, and no errors should be present.
- Additional to this, execute a MySQL query and check the replication lag.
  - SHOW SLAVE STATUS \G

- In the above query, look at the field seconds_behind_master. Ideally, it should be zero, but under 10 would be sufficient as well.
- For the large SD-WAN Orchestrators, it is recommended to use the Standby for the Backup script execution. There will be no difference in the Backup that is generated from both SD-WAN Orchestrators.

Caveats

- The Script only takes a backup of the configuration; flow stats or events are not included.
- Restoring the configuration requires assistance from the Support/Engineering team.

Frequently Asked Questions

1 How long does the Script take to run?

The duration of the Backup depends on the scale of the actual customer configuration. Since the monitoring tables are excluded from the Backup operation, it is expected that the configuration Backup operation will complete quickly. For a large SD-WAN Orchestrator with thousands of SD-WAN Edge and lots of historical events, it could take up to an hour, while a smaller SD-WAN Orchestrator should be completed within a few minutes.

2 What is the recommended frequency to run the Backup script?

Depending on the size and time it takes to complete the initial backup, the Backup operation frequency can be determined. The Backup operation should be scheduled to run during off-peak hours to reduce the impact on SD-WAN Orchestrator resources.

3 What if the root filesystem doesn't have enough space for the backup?

It is recommended that other mounted volumes are used to store the backup. Note, it is not a best practice to use the root filesystem for the backup.

4 How does one verify if the Backup operation completed successfully?

The script stdout and stderr should be sufficient to determine the success or failure of the Backup operation. If the script invocation is automated, the exit code can determine the Backup operation's success or failure.

5 How is the configuration recovered?

Currently, VMware requires that the customer work with VMware Support to recover the configuration data. VMware Support will help to recover the customer's configuration. Customers should refrain from making any additional configuration changes until the configuration is restored.

6 What is the exact impact of executing this Script?

Even though a backup of the configuration should have little impact on performance, there will be an increase in resource utilization for the MySQL process. It is recommended that the Backup be run during off-peak hours.

7 Are any configuration changes allowed during the run of the Backup operation?

It is safe to make configuration changes while the Backup operation is running. However, to ensure up-to-date backups, it is recommended that no configuration operations are done while the Backup is running.

8 Can the configuration be restored on the original SD-WAN Orchestrator, or does it require a new SD-WAN Orchestrator?

Yes, the configuration can, and ideally should, be restored on the same SD-WAN Orchestrator if it is available. This will ensure that the monitoring data is utilized after the Restore operation is completed. If the original SD-WAN Orchestrator cannot be recovered and the Standby SD-WAN Orchestrator is down, the configuration can be restored on a new SD-WAN Orchestrator. In this instance, the monitoring data will be lost.

9 What actions should be taken in case the configuration needs to be restored to a new SD-WAN Orchestrator?

Please contact VMware Support for the recommended set of actions on the new SD-WAN Orchestrator as the steps vary depending on the actual deployment.

10 DoSD-WAN Edges have to re-register on the newly restored SD-WAN Orchestrator?

No, SD-WAN Edges are not required to register on the new SD-WAN Orchestrator, as all needed information is preserved as part of the Backup.

SD-WAN OrchestratorDisaster Recovery

TheSD-WAN Orchestrator Disaster Recovery (DR) feature prevents the loss of stored data and resumes SD-WAN Orchestrator services in the event of system or network failure. SD-WAN OrchestratorDR involves setting up an Active/Standby SD-WAN Orchestrator pair with data replication and a manually-triggered failover mechanism.

Note DR is mandatory. For licensing and pricing, contact the VMware SD-WAN Sales team for support.

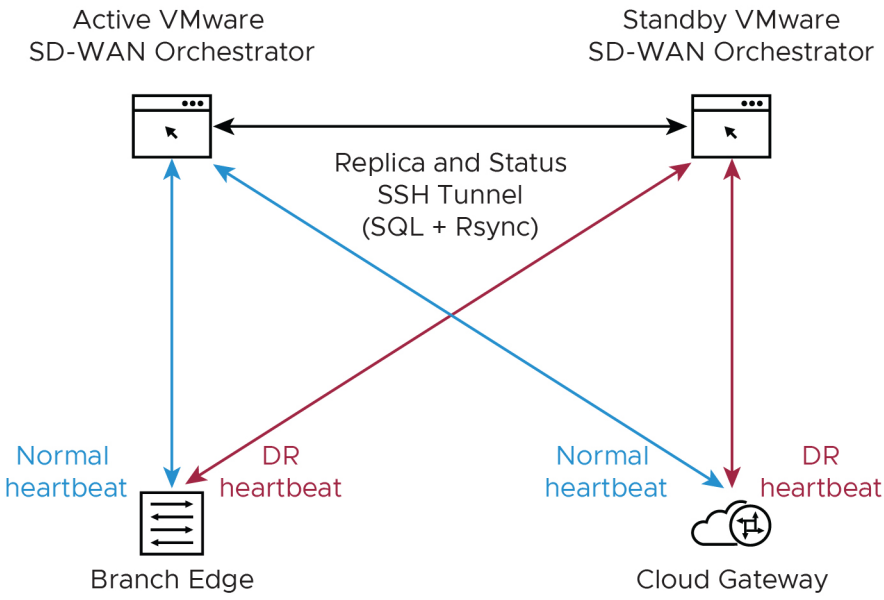
States

From the view of an Operator, and of the SD-WAN Edges and SD-WAN Gateways, a SD-WAN Orchestrator has one of four DR states:

- Standalone (no DR configured)
- Active (DR configured, acting as the primary SD-WAN Orchestrator server)
- Standby (DR configured, acting as an inactive replica SD-WAN Orchestrator server)
- Zombie (DR formerly configured and Active, but no longer working as the Active or Standby)

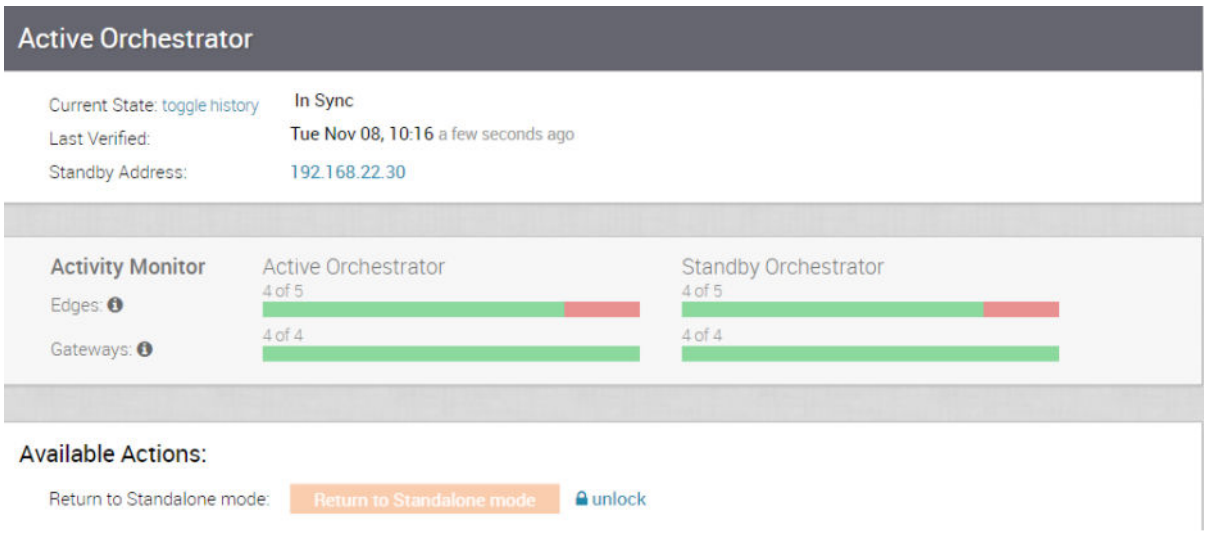
Table 1-19. Table 2: Instance Minimal Requirements for On-Prem SD-WAN Orchestrator

Phases	SD-WAN Orchestrator A Role	SD-WAN Orchestrator B Role
Initial	Standalone	Standalone
Pairing	Active	Standby
Failover	Zombie	Standalone



Best Practices

- Locate the SD-WAN Orchestrator DR in a geographically separate datacenter.
- Before promoting a Standby SD-WAN Orchestrator as Active, confirm that the DR replication Status is in Sync. The previously Active SD-WAN Orchestrator will no longer be able to manage the inventory and configuration.



- If the Standby can communicate with the formerly Active Orchestrator, it will instruct that Orchestrator to enter a Zombie state. In the Zombie state, the SD-WAN Orchestrator communicates with its clients (SD-WAN Edges, SD-WAN Gateways, UI/API) that it is no longer Active, and they must communicate with the newly promoted SD-WAN Orchestrator.
- If the promoted Standby cannot communicate with the formerly Active Orchestrator, the Operator should, if possible, manually demote the previously Active.
- Detailed instructions can be found in the official SD-WAN Orchestrator documentation docs.vmware.com under "Configure SD-WAN Orchestrator Disaster Recovery."

Upgrade Procedure for the SD-WAN Orchestrator

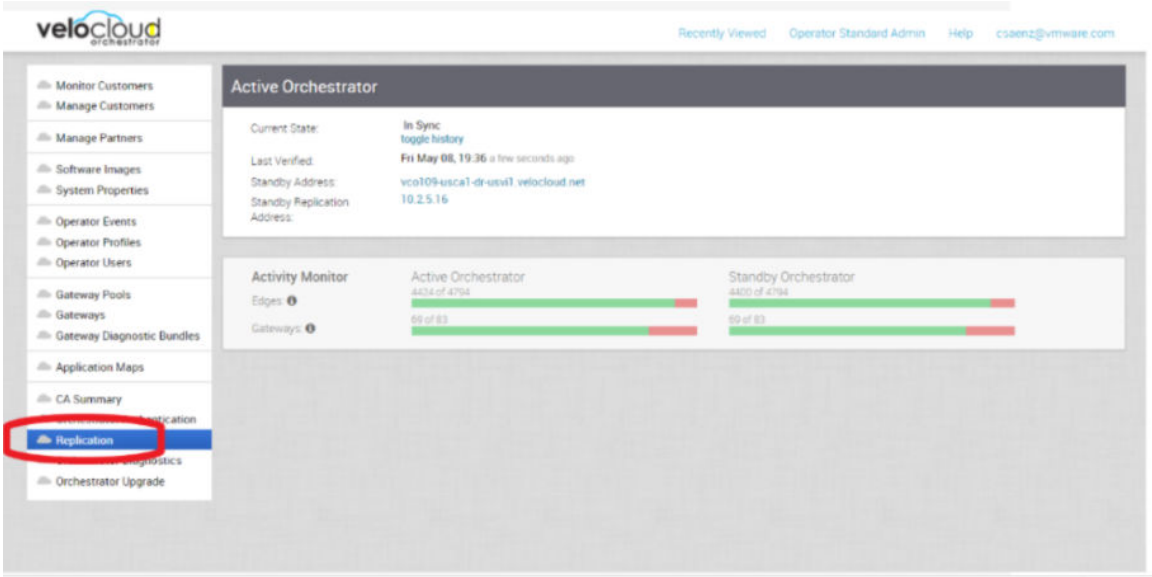
For Enterprise on-prem deployments, contact the VMware Support team to prepare for the SD-WAN Orchestrator upgrade as described below:

1 VMware Support will assist with the upgrade. Collect the following information before contacting VMware Support.

   - Provide the current and target SD-WAN Orchestrator versions, for example, the current version (i.e., 3.4.2), target version (3.4.3).

     Note For the current version, this information can be found on the top, right corner of the SD-WAN Orchestrator by clicking the Help link and choosing About.

   - Provide a screenshot of the replication dashboard of the SD-WAN Orchestrator, as shown below.



- Hypervisor Type and version (i.e., vSphere 6.7)
- Commands from the SD-WAN Orchestrator (Commands must be run as root (e.g. 'sudo <command>' or 'sudo -i').):
  - LVM layout
    - pvdisplay -v
    - vgdisplay -v
    - lvdisplay -v
    - df -h
    - cat /etc/fstab
  - Memory information
    - free -m
    - cat /proc/meminfo
    - ps -ef
    - top -b -n 2
  - CPU Information
    - cat /proc/cpuinfo
  - Copy of /var/log
    - tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
  - From the Standby Orchestrator:
    - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'

- From the Active Orchestrator:
  - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'

2 Contact VMware SD-WAN Orchestrator Support at https://kb.vmware.com/s/article/53907 with the above-mentioned information for assistance with the SD-WAN Orchestrator upgrade.

3 ESXi Snapshot guidelines are provided in the next section in case the customer wants a quick rollback solution after an upgrade.

ESXi Snapshot

The ESXi snapshot capability can be used before the SD-WAN Orchestrator upgrades to provide a quick rollback to the previous SD-WAN Orchestrator version.

ESXi Snapshot Best Practices

Before reviewing the step-by-step process, check the following best practices and guidelines about the feature:

- Standby and Active SD-WAN Orchestrator must be powered off before performing or restoring from the Snapshot to avoid any database inconsistencies.
- All Snapshot-related tasks must be done in the Standby and Active SD-WAN Orchestrator to avoid any database inconsistencies.
- It is essential to consolidate the Snapshot if the upgrade process was successful. The snapshot file continues to grow when it is retained for a more extended period. This can cause the snapshot storage location to run out of space and impact the system performance.
- Deactivate alerting in the SD-WAN Orchestrator while creating snapshots to avoid false alarms.
- Do not use a single snapshot for more than 72 hours.
- It is not recommended to use Snapshots as backups.
- Feature validation was done with ESXi 6.7 and SD-WAN Orchestrator version 3.4.4.

VMware Snapshot best practices can be found in the following kb article: https://kb.vmware.com/s/article/1025279

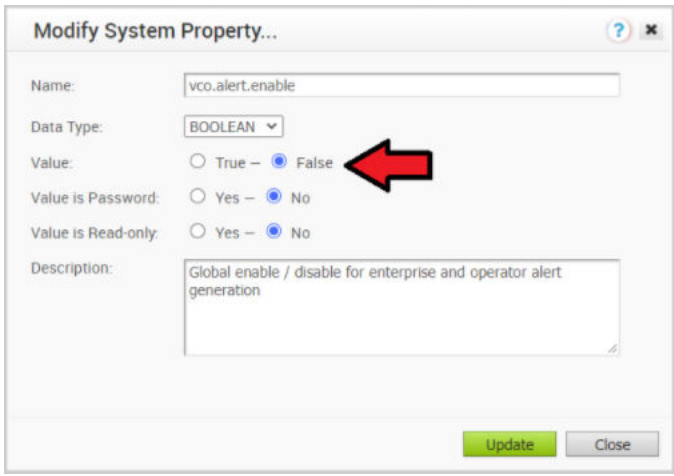
Create ESXi Snapshot

Follow the instructions below to create an ESXi Snapshot.

1 Deactivate alert, notification, and monitoring System Properties on the Active SD-WAN Orchestrator. The approximate duration is 10 Minutes.

   a In the Operator portal, click **System Properties**. Change the following System Properties to false.
      - vco.alert.enable
      - vco.notification.enable

- vco.monitor.enable



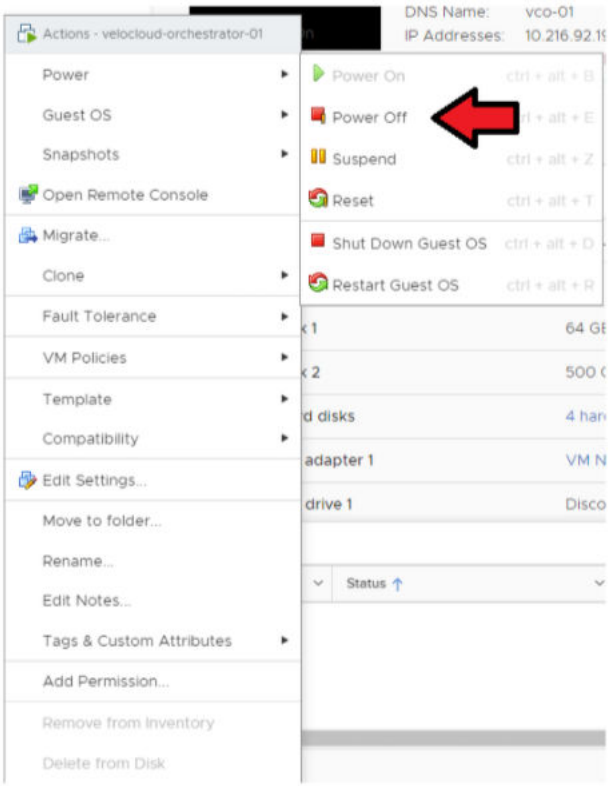
2 Deactivate alert, notification, and monitoring System Property on the Standby SD-WAN Orchestrator.

a Change the following System Properties to false.

- vco.alert.enable
- vco.notification.enable
- vco.monitor.enable

3 Power off the Active SD-WAN Orchestrator.

Go to ESXi/vCenter → SD-WAN Orchestrator VM → Actions → Power → Power Off.

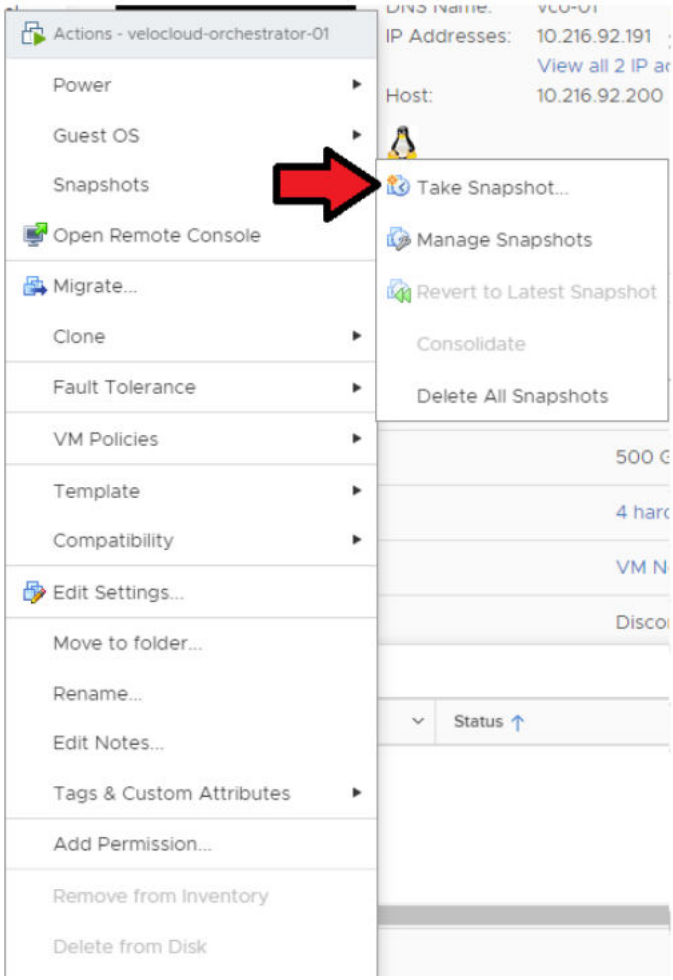


4 Power off the Standby SD-WAN Orchestrator.

Go to ESXi/vCenter → SD-WAN Orchestrator VM → Actions → Power → Power Off

5 Take a Snapshot of the Active SD-WAN Orchestrator. Confirm that the VM is powered off before performing this step.

Go to ESXi → SD-WAN Orchestrator VM → Actions → Power → Snapshots → Take Snapshot.



6 Take a Snapshot of Standby SD-WAN Orchestrator. Confirm that the VM is powered off before performing this step.

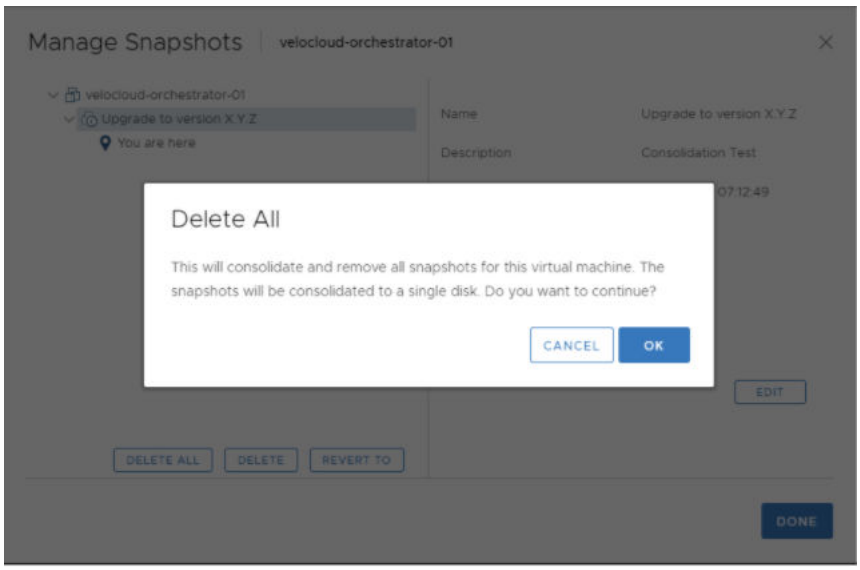
   Go to ESXi → SD-WAN Orchestrator VM → Actions → Power → Snapshots → Take Snapshot.

Consolidation of the ESXi Snapshot

Use the following instructions if you have a successful upgrade. An increased CPU usage of about 5 percent is expected while conducting the consolidation process. The approximate duration is 10 Minutes.

1 After confirming a successful upgrade on the Active and Standby Orchestrators, you can consolidate the Snapshots starting with the Active SD-WAN Orchestrator.

   Go to ESXi → SD-WAN Orchestrator VM → Actions → Snapshots → Snapshot Manager → Delete All.



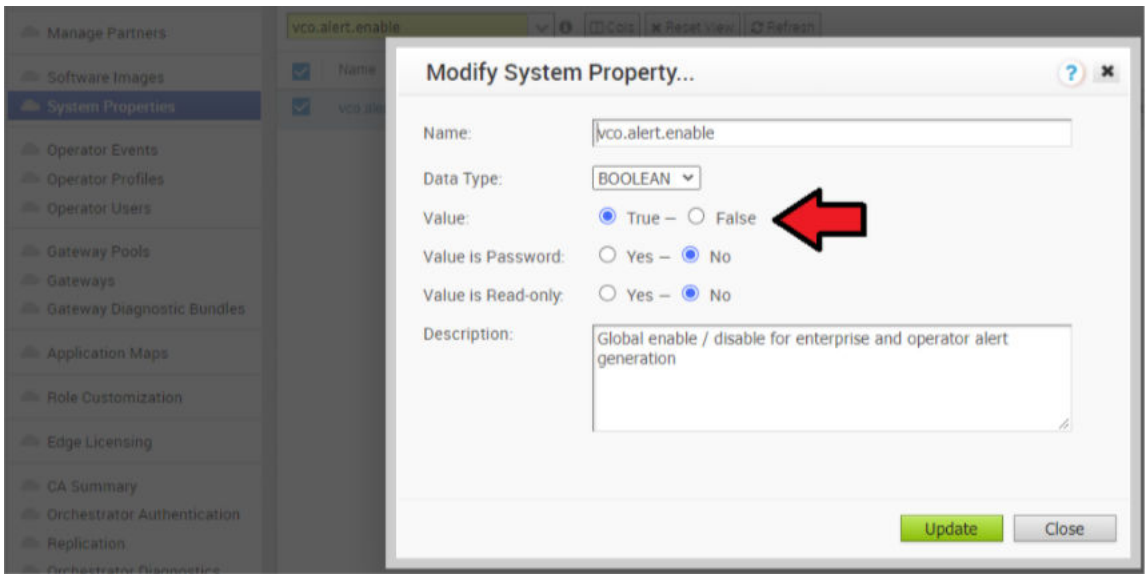
2 Consolidate the Snapshot in the Standby SD-WAN Orchestrator.

Go to ESXi → SD-WAN Orchestrator VM → Actions → Snapshots → Snapshot Manager → Delete All.

3 Re-enable alert, notification, and monitoring System Properties on the Active SD-WAN Orchestrator and the Standby SD-WAN Orchestrator.

In the Operator portal, click **System Properties**. Change the following system properties to true.

- vco.alert.enable
- vco.notification.enable
- vco.monitor.enable



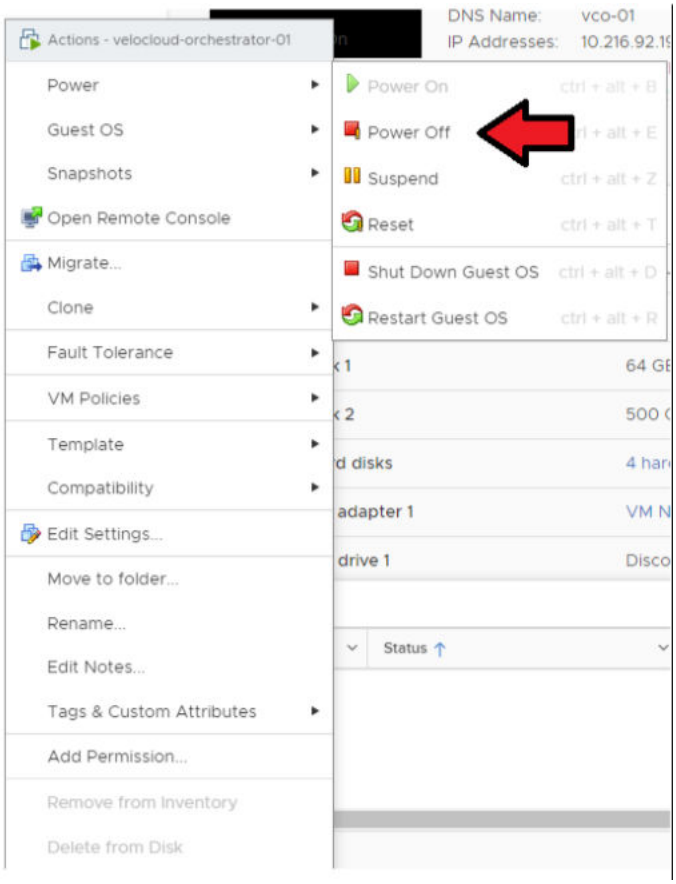
4 If the Delete All snapshots do not work with vSphere 6.x/7.x, you can try to Consolidate Snapshots. For more information, see the Consolidate Snapshots section in the vSphere Product Documentation.

Restore from the ESXi Snapshot

Perform the instructions below if you want to perform a rollback to the previous SD-WAN Orchestrator version. The approximate duration is 10 Minutes

1 Power off the Active SD-WAN Orchestrator.

Go to ESXi/vCenter → SD-WAN Orchestrator VM → Actions → Power → Power Off.



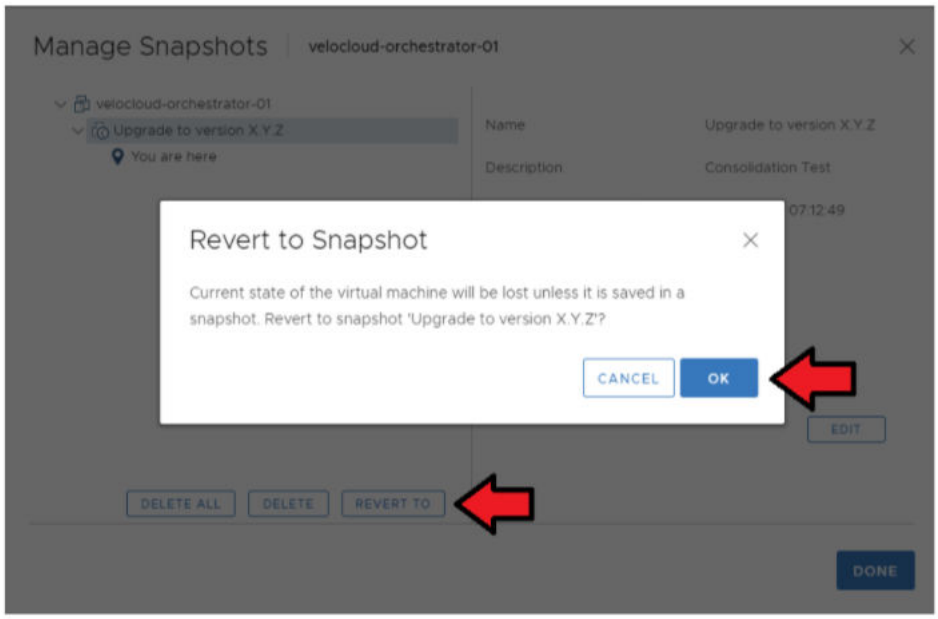
2 Power off the Standby SD-WAN Orchestrator.

Go to ESXi/vCenter → SD-WAN Orchestrator VM → Actions → Power → Power Off.

3 Restore the Snapshot of the Active SD-WAN Orchestrator.

Go to ESXi → SD-WAN Orchestrator VM → Actions → Power → Snapshots → Manage Snapshots.

Select the Snapshot you want to restore the VM → Revert to (see image below).



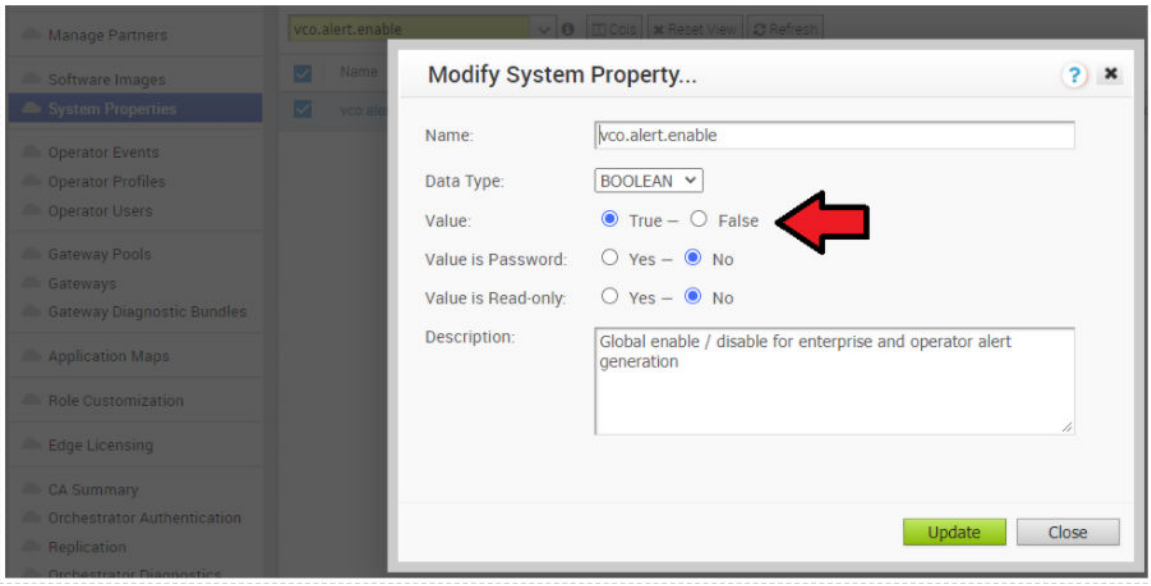
4 Restore the Snapshot of Standby SD-WAN Orchestrator.

Go to ESXi → VCO VM → Actions → Power → Snapshots → Manage Snapshots.

Select the Snapshot you want to restore the VM → Revert to.

5 Re-enable the alert, notification, and monitoring System Properties on the Active SD-WAN Orchestrator and the Standby SD-WAN Orchestrator. In the Operator portal, click **System Properties**. Change the following System Properties to true.

- vco.alert.enable
- vco.notification.enable
- vco.monitor.enable



Controller Minor Software Upgrade (Ex. from 3.3.2 P3 to3.4.4)

The software upgrade file contains Gateway and system updates. Do NOT run 'apt-get update && apt-get –y upgrade.'

Before proceeding with the VMware SD-WAN Controller's upgrade, ensure that the SD-WAN Orchestrator was upgraded before to the same or a higher version.

To upgrade an SD-WAN Controller:

1 Download the SD-WAN Controller update package.

2 Upload the image to the SD-WAN Controller storage (using, for example, the SCP command). Copy the image to the following location on the system: /var/lib/velocloud/software_update/vcg_update.tar.

3 Connect to the SD-WAN Controller console and run:

sudo /opt/vc/bin/vcg_software_update

Example:

```
root@VCG:/var/lib/velocloud/software_update# wget -O 'vcg_update.tar' <image location>
Resolving ftpsite.vmware.com (ftpsite.vmware.com)...
Connecting to ftpsite.vmware.com (ftpsite.vmware.com)| <ip address>|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: unspecified [application/octet-stream]
Saving to: 'vcg_update.tar'
    [                                <=>  ] 325,939,200 3.81MB/s   in 82s
2020-05-23 21:59:27 (3.79 MB/s) - 'vcg_update.tar' saved [325939200]
root@VCG:/var/lib/velocloud/software_update# sudo /opt/vc/bin/vcg_software_update
=========== VCG upgrade: Sat May 23 22:08:15 UTC 2020
Upgrading gateway version 3.4.0-106-R340-20200218-GA-c57f8316dd to 3.4.1-39-R341-20200428-
GA-44354-44451-596496a88a
Ign file: trusty InRelease
Ign file: trusty Release.gpg
Get: 1 file: trusty Release [2,668 B]
Ign file: trusty/main Translation-en_US
Ign file: trusty/main Translation-en
(...)
Writing extended state information...
Reading package lists...
Building dependency tree...
Reading state information...
Reading extended state information...
Initializing package states...
update-initramfs: Generating /boot/initrd.img-3.13.0-176-generic
Reboot is required. Reboot? (y/n) [y]:
```

Controller major software upgrade (Ex from 3.3.2 or 3.4 to 4.0)

In version 4.0, multiple changes are included:

- A new system disk layout based on LVM to allow more flexibility in volume management
- A new kernel version

- New and upgraded base OS packages
- Improved security hardening based on the Center for Internet Security benchmarks

Due to these changes, the standard upgrade procedure which uses the upgrade script does not work. A particular upgrade procedure is required. It is in the product manual below. This procedure is to replace the 3.3.2 or 3.4 Gateway VM with the new 4.0 Gateway VM. Refer to the following document: VMware SD-WAN Partner Gateway Upgrade and Migration 3.3.2 or 3.4 to 4.0

This upgrade procedure requires SD-WAN Orchestrator system property configuration, which only SD-WAN Orchestrator Operator accounts can run. Please create a support ticket with the VMware Support team to request the System Property change.

Monitoring

One of the customer's responsibilities on enterprise On-Prem deployments is to monitor the solution. Monitoring gives customer's the visibility required to be one step ahead of possible issues.

- SD-WAN Controller Monitoring

  You can monitor the status and usage data of Controllers available in the Operator portal.

  The procedure is as follows:

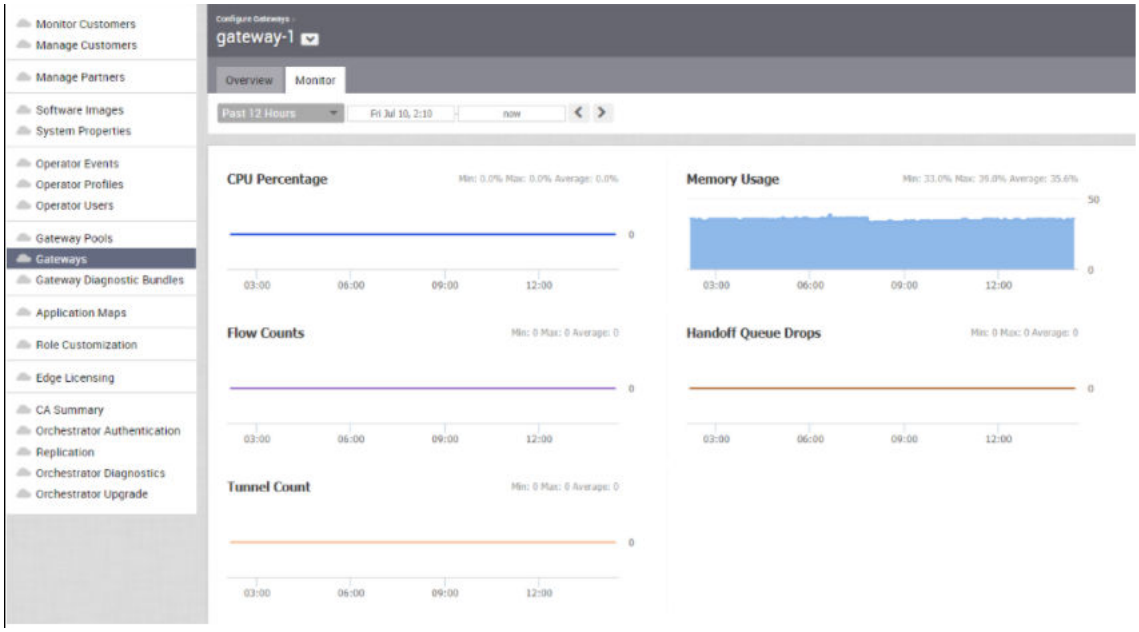
1 In the Operator portal, click **Gateways**.

2 The **Gateways** page displays the list of available Controllers.

3 Click the link to a Gateway. The details of the selected Controller displays.

4 Click the Monitor tab to view the usage data of the selected Controller.

The Monitor tab of the selected Controller displays the following details as shown in the image below.



You can choose a specific period to view the Controller's details for the selected duration at the top of the page.

The page displays a graphical representation of usage details of the following parameters for the period of selected time duration, along with the minimum, maximum, and average values.

Table 1-20. Usage Details

Usage	Description
CPU Percentage	Percentage of usage of CPU
Memory Usage	Percentage of usage of memory
Flow Counts	Count of traffic flow
Handoff Queue Drops	Count of packets dropped due to queued handoff
Tunnel Count	Count of tunnel sessions

- SD-WAN Gateway Controller Recommended Values to Monitor

  The following list shows values that should be monitored and their thresholds. The list below is given as a start point, and it is not exhaustive. Some deployments may require assessing additional components such as flows, packet loss, etc.

Whenever a warning threshold is reached, it is recommended to review the current device scale configuration and add more resources if required. When a critical alarm is triggered, it is crucial to contact VMware Support representatives to check the solution and provide further advice.

Table 1-21. Recommended Values to Monitor

Service Check	Service Check Description	Warn Threshold	Critical Threshold
CPU Load	Check System Load.	60	80
Memory	Checks the memory utilization buffer, cache, and used memory.	70	80
Tunnels	Number of tunnels from connected SD-WAN Edges.	60% of max Scale	80% of max Scale Note: A sudden loss of all tunnels or an abnormal low quantity should also be a concern.
Handoff Drops	Due to the busy nature of traffic through a Controller, occasional drops are expected.	Consistent drops in specific queues may indicate a capacity problem.	
Disk Space	Current disk utilization	40% Free	20% Free
Controller NTP	Check for Time offset	Offset of 5 Seconds	Offset of 10 Seconds

- SD-WAN Orchestrator Integration with Monitoring Stacks

The SD-WAN Orchestrator comes with a built-in system metrics monitoring stack, which can attach to an external metrics collector and a time-series database. With the monitoring stack, you can quickly check the health condition and the system load for the SD-WAN Orchestrator.

Before getting started, set up a time-based database and a dashboard/alerting agent. After this is complete, you can enable telegraf in the SD-WAN Orchestrator.

- To enable the monitoring stack, run the following command on the orchestrator:

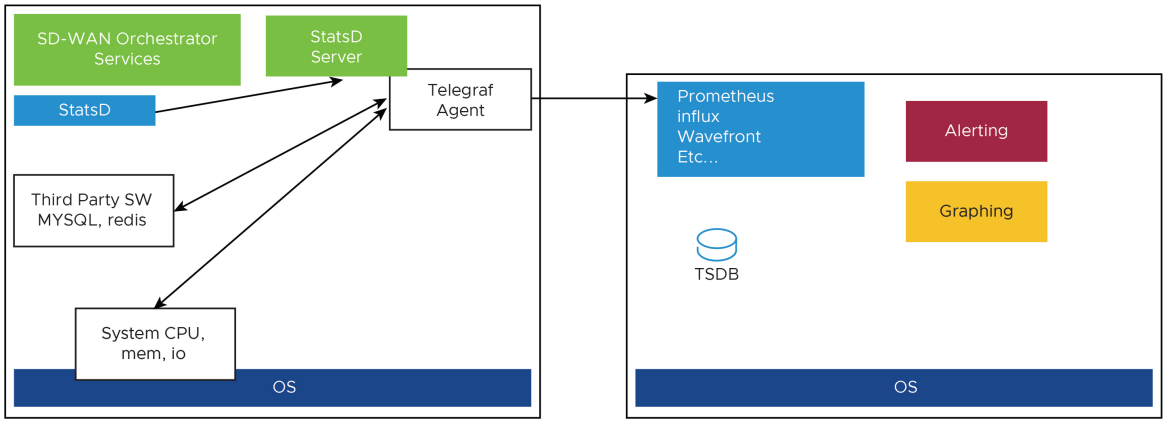
  sudo /opt/vc/scripts/vco_observability_manager.sh enable

- To check the status of the monitoring stack, run:

  sudo /opt/vc/scripts/vco_observability_manager.sh status

- To deactivate the monitoring stack, run:

```
sudo /opt/vc/scripts/vco_observability_manager.sh disable
```



- The Metrics Collector

  Telegraf is used as the SD-WAN Orchestrator system metrics collector, which has plenty of plugins to collect different system metrics. The following metrics are enabled by default.

  Table 1-22. Metrics Collector

Metric Name	Description	Supported in Version
inputs.cpu	Metrics about CPU usage.	3.4/4.0
inputs.mem	Metrics about memory usage.	3.4/4.0
inputs.net	Metrics about network interfaces.	4.0
inputs.system	Metrics about system load and uptime.	4.0
inputs.processes	The number of processes grouped by status.	4.0
inputs.disk	Metrics about disk usage.	4.0
inputs.diskio	Metrics about disk IO by device.	4.0
inputs.procstat	CPU and memory usage for specific processes.	4.0
inputs.nginx	Nginx's basic status information (ngx_http_stub_status_module).	4.0
inputs.mysql	Statistic data from MySQL server.	3.4/4.0
inputs.redis	Metrics from one or many redis servers.	3.4/4.0
inputs.statds	API and system metrics.	3.4/4.0 (additional metrics are included in 4.0)
inputs.filecount	The number and the total size of files in specified directories.	4.0

Table 1-22. Metrics Collector (continued)

Metric Name	Description	Supported in Version
inputs.ntpq	Standard NTP query metrics, requires ntpq executable.	4.0
Inputs.x509_cert	Metrics from a SSL certificate.	4.0

To activate more metrics or deactivate some enabled metrics, you can edit the Telegraf configuration file on the SD-WAN Orchestrator by:

sudo vi /etc/telegraf/telegraf.d/system_metrics_input.conf

sudo systemctl restart telegraf

- The Time-series Database

  A time Series Database can be used to store the system metrics collected by Telegraf. A time-series database (TSDB) is a database optimized for time series data.

- Dashboard and Alerting Agent

  The Dashboard and Alerting Agent allows you to query, visualize, alert, and explore the data stored in the TSDB. The image is an example of a dashboard using Telegraph (a TSDB and a dashboard engine) that can be created to monitor the solution.

- Time-series Database Setup

  Follow the instructions below to setup the time-series database.

1 Add the iptables entry to allow for external monitoring systems to access to telegraf port. The source IP address should be specified for security reasons.

  a Example. The IP address of the external monitoring system is 191.168.0.200 Add "-A INPUT -p tcp -m tcp --source 191.168.0.200 --dport 9273 -m comment --comment "allow telegraf port" -j ACCEPT" to /etc/iptables/rules.v4

```
vcadmin@vco-01:~$ cat /etc/iptables/rules.v4
*filter
:INPUT ACCEPT [0:0]
-A INPUT -p tcp -m tcp --source 191.168.0.200 --dport 9273 -m comment --comment "allow telegraf port" -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "allow established" -j ACCEPT
-A INPUT -p udp -m udp --source 127.0.0.1 --dport 161 -m comment --comment "allow SNMP port" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m comment --comment "nginx HTTP" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m comment --comment "nginx HTTPS" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m comment --comment "ssh port" -j ACCEPT
-A INPUT -p udp -m udp --sport 123 -m state --state ESTABLISHED -m comment --comment "NTP port" -j ACCEPT
-A INPUT -i lo -m comment --comment "allow local connections" -j ACCEPT
-A INPUT -m comment --comment "block everybody else" -j DROP
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
COMMIT
vcadmin@vco-01:~$
```

b Restart iptables.

sudo service iptables-persistent restart (SD-WAN Orchestrator 3.4.x)

sudo systemctl restart netfilter-persistent (SD-WAN Orchestrator 4.x)

c Make sure the iptables entry is added.

```
vcadmin@vco-01:~$ sudo iptables -S
-P INPUT ACCEPT
-P FORWARD ACCEPT
-P OUTPUT ACCEPT
-A INPUT -s 191.168.0.200/32 -p tcp -m tcp --dport 9273 -m comment --comment "allow telegraf port" -j ACCEPT
-A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -m comment --comment "allow established" -j ACCEPT
-A INPUT -s 127.0.0.1/32 -p udp -m udp --dport 161 -m comment --comment "allow SNMP port" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 80 -m comment --comment "nginx HTTP" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 443 -m comment --comment "nginx HTTPS" -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -m comment --comment "ssh port" -j ACCEPT
-A INPUT -p udp -m udp --sport 123 -m state --state ESTABLISHED -m comment --comment "NTP port" -j ACCEPT
-A INPUT -i lo -m comment --comment "allow local connections" -j ACCEPT
-A INPUT -m comment --comment "block everybody else" -j DROP
vcadmin@vco-01:~$
```

2 Add the time-series database details in the telegraf configuration. Create an output configuration file. Example with prometheus is as follows:

/etc/telegraf/telegraf.d/prometheus_out.conf

```
###############################################################################
#                            OUTPUT PLUGINS                                   #
###############################################################################

# # Configuration for the Prometheus client to spawn
[[outputs.prometheus_client]]
#   ## Address to listen on
#   listen = ":9273"
#
#   ## Metric version controls the mapping from Telegraf metrics into
#   ## Prometheus format.  When using the prometheus input, use the same value in
#   ## both plugins to ensure metrics are round-tripped without modification.
#   ##
#   ##   example: metric_version = 1; deprecated in 1.13
#   ##            metric_version = 2; recommended version
#   # metric_version = 1
  metric_version =2
#
#   ## Use HTTP Basic Authentication.
#   # basic_username = "Foo"
#   # basic_password = "Bar"
#
#   ## If set, the IP Ranges which are allowed to access metrics.
#   ##   ex: ip_range = ["192.168.0.0/24", "192.168.1.0/30"]
#   # ip_range = []
#
#   ## Path to publish the metrics on.
#   # path = "/metrics"
#
#   ## Expiration interval for each metric. 0 == no expiration
#   # expiration_interval = "60s"
#
#   ## Collectors to enable, valid entries are "gocollector" and "process".
#   ## If unset, both are enabled.
#   # collectors_exclude = ["gocollector", "process"]
#
#   ## Send string metrics as Prometheus labels.
#   ## Unless set to false all string metrics will be sent as labels.
#   # string_as_label = true
#
#   ## If set, enable TLS with the given certificate.
#   # tls_cert = "/etc/ssl/telegraf.crt"
#   # tls_key = "/etc/ssl/telegraf.key"
#
#   ## Set one or more allowed client CA certificate file names to
#   ## enable mutually authenticated TLS connections
#   # tls_allowed_cacerts = ["/etc/telegraf/clientca.pem"]
#
#   ## Export metric collection time.
#   # export_timestamp = false
```

- SD-WAN Orchestrator Recommended Values to Monitor

  The following list shows a list of values that should be monitored and their thresholds. The list below is given as a starting point, as it is not exhaustive. Some deployments may require assessing additional components such as database transactions, automatic backups, etc.

  Whenever a warning threshold is reached, it is recommended to review the current device scale configuration and add more resources if required. When a critical alarm is triggered, it is crucial to contact the VMware Support representatives to check the solution and give further advice.

Table 1-23. Monitor Values and Thresholds

Service Check	Service Check Description	Warn Threshold	Critical Threshold
CPU Load	Check System Load – Telegraf input plugin: inputs.cpu.	60	70
Memory	Checks the memory utilization buffer, cache, and used memory – Telegraf input plugin: inputs.memory.	70	80
Disk Usage	Disk Utilization in the different SD-WAN Orchestrator partitions, /, /store, /store2 and /store3 (version 4.0 and onwards) – Telegraf input plugin: inputs.disk (version 4.0 and onwards).	40% Free	20% Free
MySQL Server	Checks MySQL Connections -Telegraf input plugin: inputs.mysql.		Above 80% of max connection define in mysql.conf(/etc/mysql/my.cnf)
SD-WAN Orchestrator Time	Check for Time offset -Telegraf input plugin: inputs.ntpq (version 4.0 and onwards).	Offset of 5 Seconds	Offset of 10 Seconds
SD-WAN Orchestrator SSL Certificate	Checks Certificate Expiration - Telegraf input plugin: inputs.x509_cert (version 4.0 and onwards).	60 Days	30 Days
SD-WAN Orchestrator Internet (not applicable for MPLS only topologies)	Check for Internet access.	Response time > 5 secs	Response time > 10 secs
SD-WAN Orchestrator HTTP	Make sure HTTP on localhost is responding.		The localhost is not responding.

Table 1-23. Monitor Values and Thresholds (continued)

Service Check	Service Check Description	Warn Threshold	Critical Threshold
SD-WAN Orchestrator Total Cert Count	Check Total – Example mysql query: SELECT count(id) FROM VELOCLOUD_EDGE_CERTIFICATE WHERE validFrom <= NOW() AND validTo >=NOW()', 'SELECT count(id) FROM VELOCLOUD_GATEWAY_CERTIFICATE WHERE validFrom <= NOW() AND validTo >=NOW()	CRL	When Total Cert count exceeds 5000
DR Replication Status	Confirm the Standby SD-WAN Orchestrator is up-to-date.	Review that the DR SD-WAN Orchestrator is no more than 1000 seconds behind the Active SD-WAN Orchestrator. Seconds_Behind_Master: from mysql command: show slave STATUS\G;	
DR Replication SD-WAN Edge Gateway delta	Confirm that SD-WAN Edges and SD-WAN Gateways can talk to the DR SD-WAN Orchestrator. Different values between the Active and the Standby SD-WAN Orchestrators can be due to a difference in the timezone in SD-WAN Edges and SD-WAN Gateways.	The same amount of SD-WAN Edges talking with the Active SD-WAN Orchestrator should be able to reach the Standby SD-WAN Orchestrator. This value can be checked on the "replication" tab or via the API.	

API Best Practices

The VMware SD-WAN Orchestrator powers the management plane in the VMware SD-WAN solution. It offers a broad range of configuration, monitoring, and troubleshooting functionality to service providers and enterprises. The main web service with which users interact to exercise this functionality is called the SD-WAN Orchestrator Portal.

- The SD-WAN Orchestrator Portal

  The SD-WAN Orchestrator Portal allows network administrators (or scripts and applications acting on their behalf) to manage network and device configuration and query the current or historical network and device state. API clients may interact with the Portal via a JSON-RPC interface or a REST-like interface. It is possible to invoke all of the methods described in this document using either interface. There is no Portal functionality for which access is constrained exclusively to either JSON-RPC clients or REST-like ones.

Both interfaces accept exclusively HTTP POST requests. Both also expect that request bodies, when present, are JSON-formatted -- consistent with RFC 2616, clients are furthermore likely to formally assert where this is the case using the Content-Type request header, e.g., Content-Type: application/json.

More information about the VMware SD-WAN API can be found here:

https://code.vmware.com/apis/1000/velocloud-sdwan-vco-api

- Best Practices for enterprises and service providers Using APIs

  Some of the best practices while using APIs are:

  - Wherever possible, aggregate API calls should be preferred to enterprise-specific ones. e.g., a single call to monitoring/getAggregateEdgeLinkMetrics may be used to retrieve transport stats across all SD-WAN Edges concurrently.
  - VMware requests that clients limit the number of API calls in flight at any given time to no more than a handful (i.e., <2-4). If a user feels there is a compelling reason to parallelize API calls, VMware requests that they contact VMware Support to discuss alternative solutions.
  - We ordinarily don't recommend polling the API for stats data more frequently than every 10 min. New stats data arrives at the SD-WAN Orchestrator every 5 minutes. Due to jitter in reporting/processing, clients polling every 5 minutes might observe "false-positive" cases where stats aren't reflected in API calls' results. Users tend to find the best result using request intervals of 10 minutes or greater in duration.
  - Avoid querying the same information twice.
  - Use sleep between APIs.
  - For complex software automations, run your scripts and evaluate the CPU/Memory impact. Then adjust as required.

SD-WAN Orchestrator Syslog Configuration

The VMware SD-WAN Orchestrator Syslog capability can be configured independently for the following Orchestrator processes: portal, upload, and backend.

A short description of each process is listed below:

- Portal: The Portal process runs as an internal HTTP server downstream from NGINX. The Portal service handles incoming API requests, either from the SD-WAN Orchestrator web interface or from an HTTP/SDK client, primarily in a synchronous fashion. These requests allow authenticated users to configure, monitor, and manage the various services provided by the SD-WAN Orchestrator.

  This log is very useful for AAA activities as it has all actions taken by users in the SD-WAN Orchestrator.

  Log files: /var/log/portal/velocloud.log (Logs all info, warn, and error logs)

- Upload: The Upload process runs as an internal HTTP server downstream from NGINX. The Upload service handles incoming requests from SD-WAN Edges and SD-WAN Gateways, either synchronously or asynchronously. These requests primarily consist of activations, heartbeats, flow statistics, link statistics, and routing information sent by SD-WAN Edges and SD-WAN Gateways.

  Log files: /var/log/upload/velocloud.log (Logs all info, warn, and error logs)

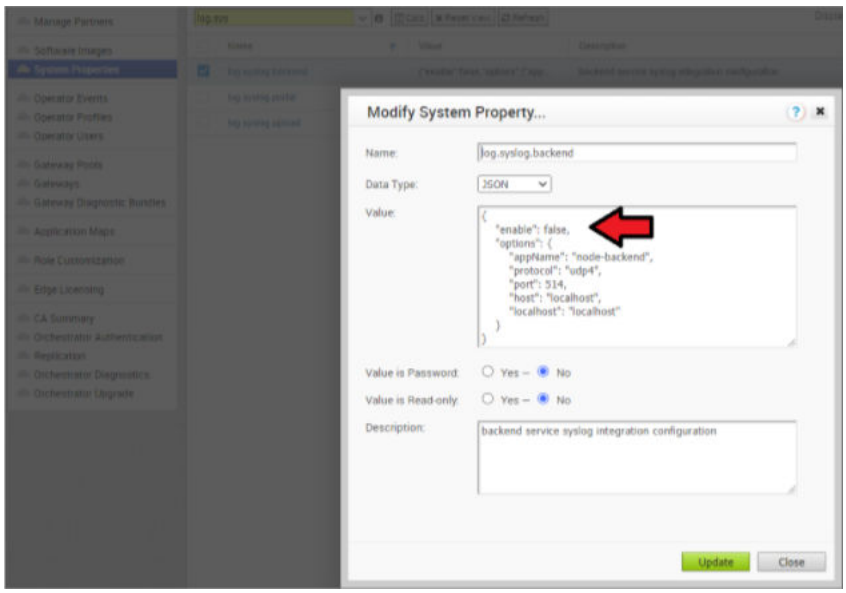
- Backend: Job runner that primarily runs scheduled or queued jobs. Scheduled jobs consist of cleanup, rollup, or status update activities. Queued jobs consist of processing link and flow statistics.

  Log files: /var/log/backend/velocloud.log (Logs all info, warn, and error logs)

Orchestrator Syslog Configuration

1 Navigate to System Properties in the SD-WAN Orchestrator, log.syslog.<server> (eg log.syslog.portal). Go to SD-WAN Orchestrator → System Properties → type “log.syslog” in the search bar

2 Change the “enable”:false value to true for one or more of the servers. Change the Host IP and port accordingly to your implementation.



Increasing Storage in the SD-WAN Orchestrator

Detailed instructions to increase the Storage in the SD-WAN Orchestrator can be found in the SD-WAN Orchestrator

documentation at https://docs.vmware.com/ under "Install SD-WAN Orchestrator" and "Expand Disk Size (VMware)"

- Best Practices:
  - Make sure that the same LVM distribution is applied to the Standby SD-WAN Orchestrator.

- It is not recommended to reduce the size of the volumes once they were increased. Use thin provisioning instead.
- In 3.4, when increasing the disk size, the following percentage/value distribution may be used:
  - “/” Volume: This volume is used for the operative system. Production SD-WAN Orchestrators are usually set to 140GBs and have from 40% to 60% usage.
  - /store and /Store2: The proportion applied in production SD-WAN Orchestrators is close to 85% for /Store and 15% for /Store2.
- The following guidelines in the table below should be used in the 4.x release and onwards.

Instance Size	/store	/store2	/store3	/var/log
Small (5000 SD-WAN Edges)	2 TB	500GB	8TB	15GB
Medium (10000 SD-WAN Edges)	2 TB	500GB	12TB	20GB
Large (15000 SD-WAN Edges)	2 TB	500GB	16TB	25GB

Managing Certificates in the SD-WAN Orchestrator

The SD-WAN Orchestrator uses a built-in certificate server to manage the overall PKI lifecycle of all SD-WAN Edges and SD-WAN Controllers. X.509 certificates are issued to the devices in the network.

Detailed instructions to configure the CA can be found in the official SD-WAN Orchestrator documentation at https://docs.vmware.com/ under "Install SD-WAN Orchestrator" and "Install an SSL Certificate."

Certificates issued by the CA are used only for the authentication of the following:

- Management plane TLS 1.2 tunnels between the SD-WAN Orchestrator and SD-WAN Edge SD-WAN Controller.
- Control and Data plane IKEv2/IPsec tunnels between SD-WAN Edges and between SD-WAN Edgeand SD-WAN Controller.

Certificate Revocation List

On Controllers with PKI enabled, revoked certificates are stored in a Certificate Revocation List ("CRL"). If this list grows too long (generally due to an issue with the SD-WAN Orchestrator's Certificate Authority), the Controller's performance will be impacted. The CRL should be less than 4,000 entries long.

```
vcadmin@vcg1-example:~$ openssl crl -in /etc/vc-public/vco-ca-crl.pem -text | grep 'Serial
Number' | wc -l
14
vcadmin@vcg1-example:~
```

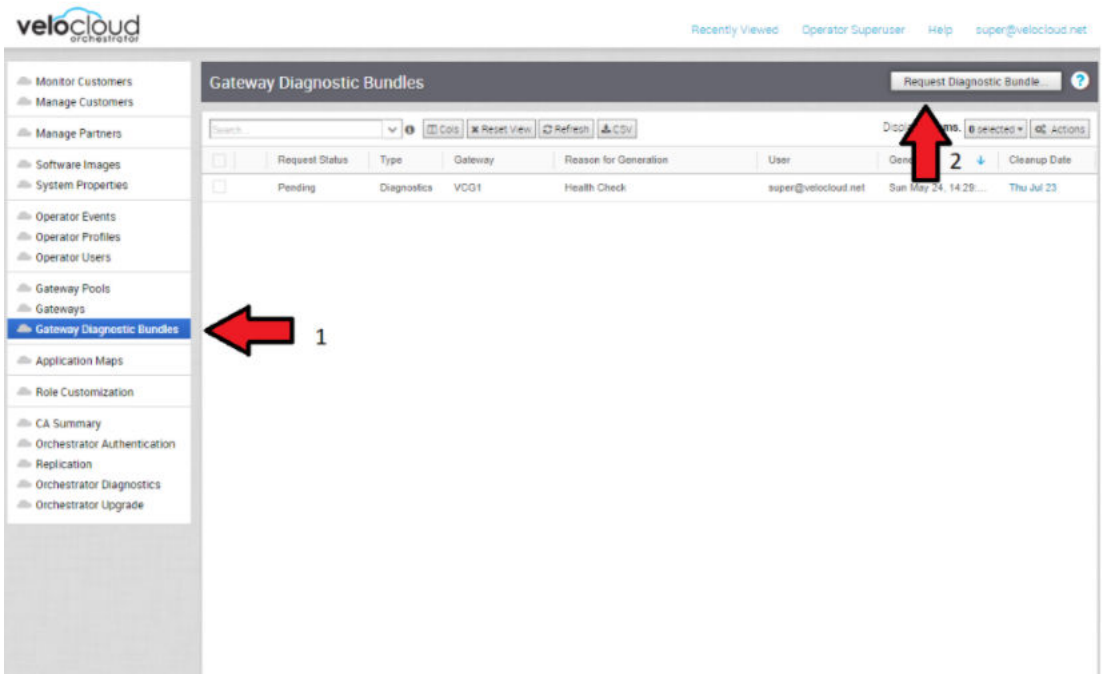
Support Interaction

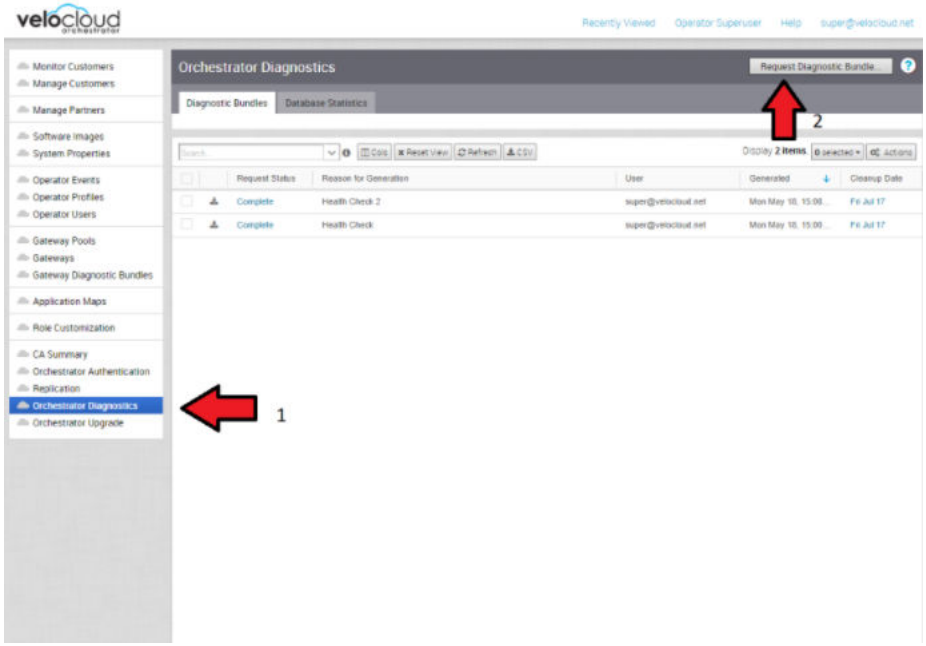
Our Customer Support organization provides 24x7x365 world-class technical assistance and personalized guidance to VMware SD-WAN customers.

This section provides some guidelines to interact with the VMware Support team.

- Diagnostic Bundles

  While investigating an incident, a diagnostic bundle of the SD-WAN Orchestrator and SD-WAN Controller can be created. The resulting file will assist the VMware Support team to further analyze the events around an issue.





- Share Access with Support

  On occasion assistance from VMware Support representatives for the SD-WAN Orchestrator and SD-WAN Controllers may be required.

  Some common ways to grant access are:

  - Remote sessions with Support: The customer would either grant remote control to the SSH jump server or follow the Support representative's instructions.
  - Creating an account for the Support team in the SD-WAN Orchestrator. This helps the Support team gather logs without customer interaction.
  - Through the Bastion Host: SSH permissions and keys can be configured to allow the Support engineers to access the on-premises SD-WAN Orchestrator and SD-WAN Controller using a Bastion Host.

  When contacting VMware SD-WAN Support to assist triaging an issue, include the data described in the table below.

  More information can be found in the following link: https://kb.vmware.com/s/article/53907

Required	Suggested
Partner Case Number	Issue Start/Stop
Partner Return Email/Phone	Impacted Flow SRC/DST IP
SD-WAN Orchestrator URL	Impacted Flow SRC/DST Port
Customer Name in SD-WAN Orchestrator	Flow Path (E2E, E2GW, Direct)
Customer Impact (High/Med/Low)	SD-WAN Gateway Name(s)

Required	Suggested
SD-WAN Edge Name(s)	Link to PCAP in the SD-WAN Orchestrator
Link to Diagnostic Bundle in SD-WAN Orchestrator	
Short Problem Statement	
Analysis & Requested Assistance	