Cloud Infrastructure

Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage** to **Cisco Catalyst SD-WAN Manager**, **Cisco vAnalytics** to **Cisco Catalyst SD-WAN Analytics**, **Cisco vBond** to **Cisco Catalyst SD-WAN Validator**, **Cisco vSmart** to **Cisco Catalyst SD-WAN Controller**, and **Cisco Controllers** to **Cisco Catalyst SD-WAN Control Components**. See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Cisco Cloud-Hosted Controller Snapshots

Cisco takes regular snapshots of the cloud hosted Cisco SD-WAN Manager controller managed by Cisco, based on the snapshot frequency. The snapshot frequency is set by default to once every day, typically midnight of the region of deployment, and the last 10 snapshots are retained. The snapshot frequency can be configured from once a day, to upto once in 4 days. For more information on Snapshots, see Information About Snapshots.

You can open a Cisco TAC support case with the Cisco CloudOps team to review the current snapshot setting or change it on the Cisco Catalyst SD-WAN Portal. You can retain only a maximum of last 10 periodic snapshots. The Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Validator are stateless and therefore snapshots are not taken. It is recommended that their configurations can be done via templates on Cisco SD-WAN Manager for disaster recovery.

You cannot download the snapshots as snapshots are stored within the Cisco cloud account. However, you can download the config-db backup file from Cisco SD-WAN Manager and save the configurations including templates using command request nms configuration-db backup path.

Note Since, Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller are stateless, snapshots are not captured. Use Cisco SD-WAN Manager template to configure and save Cisco SD-WAN Validator and Cisco Catalyst SD-WAN Controller Configuration settings.

Take an On-demand Snapshot

Note The on-demand snapshot process is applicable only for overlays with Cisco-hosted, cloud-based, dedicated, single tenant controllers. This is not applicable if you have a shared tenant overlay.

For any major planned change windows for Cisco SD-WAN Manager, You can take on-demand snapshot using Cisco Catalyst SD-WAN Portal. This can be requested via opening a Cisco TAC support case with the Cisco CloudOps team. You need to freeze the configuration changes and allocate up to eight hours prior to the change window to allow the on-demand snapshot to be taken and completed. We can store up to one on-demand snapshot. We can store this on-demand snapshot for a period of 3 months from the date of creation of the snapshot. Also, each time a new on-demand snapshot is taken, the previous one, if present, is automatically removed and replaced with the new one.

Cisco Catalyst SD-WAN Analytics

Refer to Cisco Catalyst SD-WAN Analytics.

Pen Test

Customers with overlay controllers in AWS can conduct their own pen tests for the Cisco Catalyst SD-WAN solution without approval using:

- https://aws.amazon.com/security/penetration-testing/

Customers with overlay controllers in Azure can conduct their own pen tests for the Cisco Catalyst SD-WAN solution without approval using:

- https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement

Mandatory Maintenance of Cloud-Hosted Controllers

The Cisco CloudOps team sends email notices to customers for mandatory reboot of a specific cloud-hosted controller managed by Cisco, only when hosted in AWS. Sometimes, maintenance is required on the instances and rebooting the instances prior to the cloud provider's maintenance window. It allows you to move them from the current hardware node requiring maintenance, to a new healthy hardware node, to avoid disruption of service.

The Cisco CloudOps team then sends notifications to the registered email address of the customer, which is a single email address registered for an overlay within the Cisco CloudOps system. Note that this registered

email address is configured initially using the original Sales Order's **End Customer Email Address** field and can be updated anytime by logging into the Cisco Catalyst SD-WAN Portal (link to https://ssp.sdwan.cisco.com). This registered email address is not derived from Cisco SD-WAN Manager Settings page.

You can reschedule to update the change window, as long as the requested date and time is before the cloud provider's maintenance window time. The amount of advance notice is not guaranteed and depends on the severity of the issue on the hardware node on cloud provider side.

Cisco Catalyst SD-WAN Disaster Recovery Guidelines

- Cisco Catalyst SD-WAN disaster recovery is based on Cisco SD-WAN Manager disk volume snapshots or configuration database backups.
- These configuration database backups and volume snapshots are taken each daily, typically around midnight time of the location of the Cisco SD-WAN Manager instance and securely stored on cloud.
- For Cisco SD-WAN Release 20.3.x and later, you can turn off configuration database backup feature, if desired, and take own backups and make them available to CloudOps when needed for recovery of the service.
- Cisco SD-WAN Manager disk volume snapshots are taken every night and sometimes on-demand for customer request or at start of major change windows. Each Cisco SD-WAN Manager has two or more disks and a snapshot of each of the volumes is taken at the exact same time to form an overall backup of the Cisco SD-WAN Manager instance. The snapshots, once completed, in the region where the Cisco SD-WAN Manager is running, are then copied over to the designated backup region, usually a different geographic region.

  For example, Cisco SD-WAN Manager may be running in US-East and backup region may be designated as US-West. The backup region is essentially the same region, where the second Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller are already running.
- Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller are stateless services and have a CLI-managed configuration or Cisco SD-WAN Manager provide configuration and hence they aren't backed up.
- There's no standby or active Cisco SD-WAN Manager service in a backup region. Three or six node cluster offers high availability of Cisco SD-WAN Manager, running within the same availability zone and region.
- Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller services are deployed in primary and backup regions. Both Cisco Catalyst SD-WAN Validator and Cisco Catalyst SD-WAN Controller work in active mode. The device and policy information is pushed to both the instances from Cisco SD-WAN Manager. When one region fails, Cisco Catalyst SD-WAN Controller and Cisco Catalyst SD-WAN Validator continue to function fine in the backup region.
- Cisco Catalyst SD-WAN is designed for the data plane to continue to function even if all the controllers fail. GR (Graceful Restart) timer configuration enables the high availability of the data plane. GR timer is configured to hold on to the routes advertised by Cisco Catalyst SD-WAN Controllers, by default for 12hrs. We recommend Cisco Catalyst SD-WAN customers to choose GR timer value judiciously to allow controllers to be back up in case of failures, and at the same time be able to learn the new routes from changed network configurations.
- Configuration database-based recovery method when used, allows only templates and policies to be restored. Volume-based recovery is used to include the stats data collected as well.

Volume Snapshot based Recovery Process

- Once determined that the Cisco SD-WAN Manager instance needs to be replaced with a backup, we can initiate the Disaster Recovery (DR) process.
- For DR at same region, Cisco pick the same region and same datacenter as the existing Cisco SD-WAN Manager instance location.

  We also specify the time/date of the snapshot set to use, based on requirement and availability.
- Once DR triggers, the system first shuts down the existing Cisco SD-WAN Manager instance.
- System then uses the volume snapshots to create a new cloud instance with the same set of disks, same instance size specifications, same private subnets, same security access-list, same isolated environment as that of the original Cisco SD-WAN Manager. Once the instance is up, the system swaps the public IPs from the old shutdown Cisco SD-WAN Manager instance to the new Cisco SD-WAN Manager instance.
- Overall, the new running Cisco SD-WAN Manager instance has the same public IPs, but new private IPs and have the same software version, same configuration, same data, as that present at the time when snapshot is taken.
- Cisco SD-WAN Manager has the necessary information to join the fabric. You can use the same FQDN/URL to log in into the Cisco SD-WAN Manager instance as before.
- For DR to the backup region, in the unlikely case where the primary region of Cisco SD-WAN Manager has failed and unavailable, we use the exact same process, except that the backup cloud region is selected.
- The difference with DR to backup region is that, once the new Cisco SD-WAN Manager instance is running in backup region, there's no swapping of public IPs from old region to new region. Cloud regions have a specific public IP pool per region and can't be assigned to instances across regions.

  Therefore, the new DR Cisco SD-WAN Manager instance in backup region, has new public IPs. The system updates the FQDN/DNS with the new public IP of the Cisco SD-WAN Manager.

  In this case, you may need to update the enterprise end firewall with the new public IP of the Cisco SD-WAN Manager.

Configuration Database backup by Cisco CloudInfra System

- Prior to Cisco vManage Release 20.3.1, the configuration database was backed up only if:
  - Monitoring is enabled in Cisco CloudInfra system. If 'viptelatac' user is unusable on the Cisco SD-WAN Manager for any reason, monitoring gets disabled, and customers are notified with request for correction.
  - The 'viptelatac' user must be usable on the Cisco SD-WAN Manager.
  - The configuration database size is lesser than 4GB.
- Cisco vManage Release 20.3.1 and later, the configuration database is backed up only if:
  - Monitoring is enabled in Cisco CloudInfra system.

Note In Cisco SD-WAN Manager, if the cloud service is disabled for any reasons, then monitoring gets disabled on Cisco CloudInfra system and customers are notified with request for correction.

- From the Cisco SD-WAN Manager menu, choose **Adminstration** > **Settings**, and enable Cloud Services and vMonitoring along with OTP added in the same section.
- In the Cisco SD-WAN Manager CLI, the **`nms configuration-db daily-backup`** service is enabled.
- The configuration database size is lesser than 4GB.

Configuration Database based Recovery Process

- If volume snapshot is not viable for DR for any reasons, then Cisco uses the configuration database recovery process. Cisco creates a brand new Cisco SD-WAN Manager instance and use the configuration database backup to restore the original configuration files. With this method, the statistics database of the original Cisco SD-WAN Manager instance is not restored. This method restores your templates and policies configuration. The new Cisco SD-WAN Manager instance in this case has both new public IPs and new private IPs.
- We update the FQDN/DNS of the Cisco SD-WAN Manager to use the new public IP of the new instance.
- In this case, you may need to update the enterprise end firewall with the new public IP of the Cisco SD-WAN Manager.
- The process for using disaster recovery method using configuration database backup remains same for both same region and backup region recovery.
- For process details, see Troubleshooting TechNotes.