Monitoring

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.

Monitor the Cisco Catalyst SD-WAN Cloud-Hosted Controllers

Cloud hosted controller monitoring covers the following:

- Infrastructure monitoring of the following:
  - CPU and data disk utilization.
  - Loss of connectivity to network interfaces.
  - Failure to reach instances.
- Service monitoring of the following:
  - Expiration of controller SSL certificates.
  - Availability of the Cisco SD-WAN Manager web server.
  - Loss of control connection to the controllers.

Health Monitoring of Overlays with Cisco SD-WAN Manager Version below 20.3.x

The cloud monitoring is performed as a part of the Cisco Catalyst SD-WAN cloud-hosting services to ensure the availability of the Cisco SD-WAN Controllers. By default, Cisco SD-WAN Manager is configured with a user called `viptelatac` with `operator` privileges. Cisco uses this user to login to Cisco SD-WAN Manager and to collect and monitor the health of Cisco Catalyst SD-WAN.

The Cisco SD-WAN Manager audit log displays periodic logins from the monitoring system using the `viptelatac` user. The monitoring service uses RestAPIs to collect health information from Cisco SD-WAN Manager.

In case you want to disable the Cisco cloud monitoring system, you can open a Cisco TAC case with the Cisco Catalyst SD-WAN Cloud Infra team, requesting to disable the cloud monitoring. Once the monitoring is disabled, you can also remove the configured `viptelatac` user from the Cisco SD-WAN Manager.

Cisco Cloud Infra team will also use the `viptelatac` user to login to the Cisco SD-WAN Manager to do additional health checks, triage issues in response to internally generated alerts, as well as to assist with customer opened TAC cases.

Health Monitoring of Overlays with Cisco SD-WAN Manager Version Running at or above 20.3.x

From Cisco SD-WAN Release 20.3.1 release onwards, push based model is used.

In this model, the monitoring architecture uses Cisco SD-WAN Manager to authenticate with the system to send the health data. Cisco SD-WAN Manager pushes the data instead of monitoring system logging into the Cisco SD-WAN Manager with the `viptelatac` user. In order for this to work, you need to explicitly provide consent on the Cisco SD-WAN Manager settings page, as well as configure a One Time Password (OTP). The `viptelatac` user is not needed once Cisco SD-WAN Manager is upgraded to 20.3.1 or above.

You can login to Cisco SD-WAN Manager and perform the follwing steps:

1. Go to **Settings** > **Cloud Services** > **Enable**
2. Enter the OTP value. You can request the token from the Cisco CloudOps team by opening a Cisco TAC Support case.
3. Leave the Cloud Gateway URL blank.
4. Check the **vMonitoring** to enable monitoring.
5. Approve permission to collect the data regarding health status of the overlay from Cisco SD-WAN Manager.

For version 20.3.x and above, Cisco Cloud Infra team will use the `ciscotacro` and `ciscotacrw` user to login to the Cisco SD-WAN Manager to do additional health checks, triage issues in response to internally generated alerts, as well as to assist with the customer opened TAC cases. The same user will also be used to perform automated infrastructure upgrades and certain software updates based on pre-notified changes to the customer contacts for the overlay.

The `ciscotacro` user has read-only *operator* group privilege while `ciscotacrw` has read-write *netadmin* group privilege. For certain enhanced debugging, cloud infrastructure upgrades and management, Cisco Cloud Infra team needs to use the `ciscotacrw` user.

Only specific Cisco support teams have the ability to login via these users and they are based on a token challenge and token response based password mechanism i.e., the two users are not based on static passwords.

In case, you want to disable this access on any of the Cisco Catalyst SD-WAN fabric controllers, you can remove the user from the configuration at any time. However, this will limit Cisco ability to triage the issues.

Alert Notifications by CloudOps

CloudOps team manages the infrastructure of the cloud hosted instances and help with the monitoring and backend infrastructure maintenance. However, CloudOps team does not make changes or manage the running software version or configuration of the instances.

CloudOps team may send alert notifications to customers, based on any issues seen, which may indicate either software issue or misconfiguration or some features overutilizing the capacity, which CloudOps team is not aware of. Customers may be running their own tests, changes, or configuration updates, that the team is not aware of.

CloudOps team will therefore, only notify the customers instead of taking direct action on the hosted controller instances, and request customer to open a Cisco TAC support case for assistance and evaluation as needed. Once the customer has a TAC case open, Cisco TAC and thereafter, CloudOps team, can work together with the customer, to resolve the issue as needed.

Update Overlay Contact for Receiving Alert Notifications

- Every Cisco provisioned cloud-hosted overlay has a single customer contact email address registered as the owner, to receive CloudOps Alert notifications.
- By default, the contact email address provided on the Cisco Sales Order's End Customer details has been used as the owner contact.
- Customers can open a Cisco TAC case to review or update the contact at any time.
- For Cisco-hosted, cloud-based, dedicated, single tenant controllers, you can directly update the owner contact email address through the Cisco Catalyst SD-WAN Portal.
- We support only one email address contact as the owner contact and hence it is recommended that you provide a group mailing list email address.