

Alarms

- Introduction, on page 1
- Alarm Details, on page 2
- Related Documentation, on page 70
- Full Cisco Trademarks with Software License, on page 70

Introduction

This guide provides a comprehensive overview of alarm descriptions for Cisco Catalyst SD-WAN and SD-Routing. It covers alarms generated by Cisco IOS XE Catalyst SD-WAN devices and Cisco Catalyst SD-WAN Control Components.

Each alarm entry includes details on its meaning, severity level, and recommended steps for resolution, enabling you to effectively monitor and manage your network infrastructure.

Cisco SD-WAN Manager suppresses or does not clear alerts for issues that resolve within 30 seconds to avoid logging short-lived events and keep alerts relevant.

UTD Alarms

From Cisco Catalyst SD-WAN Manager Release 26.1.1.1, Cisco SD-WAN Manager no longer displays the UTD alarms listed below and instead provides their corresponding events:

- UTD IPS Alert
- UTD File Analysis Status Event
- UTD File Analysis Upload_Status
- UTD File Reputation Alert
- UTD File Reputation Retrospective Alert

Alarm Details

AAA Admin Password Change

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The AAA user admin changed the password on a Cisco IOS XE Catalyst SD-WAN device or Cisco Catalyst SD-WAN Control Components.

Clear the AAA Admin Password Change Alarm

Procedure

No clearing procedure.

AAA Password Expired

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The password age of any user expires.

AAA Password Expired

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The password age of any user expires.

AAA Password Expiry Warning

Default Severity: Major

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

For any user, password will expire soon.

Clear the AAA Password Expiry Warning Alarm

Procedure

No clearing procedure.

Acknowledgement File Not Uploaded

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The alarm triggers when the acknowledgement file is not uploaded after report generation for licensed devices.

Clear the Acknowledgement File Not Uploaded Alarm

Procedure

Upload the acknowledgment file to clear the alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Analytics Directory Usage

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Alarms of varying severity trigger when disk usage by analytics files increases.

Clear the Analytics Directory Usage Alarm

Procedure

Lower severity alarms clear the higher severity alarms.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Analytics Purge Completed

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

System deletes older files if disk usage exceeds the specified limit due to unsent files for analytics.

Clear the Analytics Purge Completed Alarm

Procedure

This notice confirms the completion of a file purge.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Analytics Token Status

Default Severity: Major/Medium/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

An alarm is triggered when cloud service tokens are expired or invalid and the system cannot refresh them, or an error occurs during token retrieval.

Clear the Analytics Token Status Alarm

Procedure

The alarm clears when the tokens become valid.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Analytics Upload Status

Default Severity: Major/Medium/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The alarm triggers at a medium level for uploads to analytics failure rate up to 20%. It triggers at a major level if more than 20% of uploads fail.

Clear the Analytics Upload Status Alarm

Procedure

The alarm clears when the upload rate improves.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

API Volume Monitor

Default Severity: Minor

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

API volume monitor alarms apply only when you enable monitoring for an API, such as when:

- The API has exceeded the Rate-per-Minute, or
- The API Rate-per-Minute is normal

Clear the API VOLUME MONITOR Alarm

Procedure

No clearing procedure.

AppQoE

Default Severity: Major/Critical/Medium/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The alarm triggers in any of the following cases:

- When the Proxy Signing CA expires or is missing
- When the CA bundle is missing, or
- When the TCP Proxy limit reaches its maximum.

Clear the AppQoE Alarm

Procedure

Fixing the Proxy Signing CA, CA bundle, or TCP connection limit automatically clears the alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AppQoE Service Node State

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Reachability issues or traffic exceeding its supported capacity bring the service node down.

Clear the AppQoE Service Node State Alarm

Procedure

This alarm clears when the service node is reachable and the traffic is reduced to a supported level.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

AppQoE Site ID Mismatch

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The service node with a certain site ID registers to a service controller of a different site ID.

Clear the AppQoE Site ID Mismatch Alarm

Procedure

Fix the site ID in the service node to clear the alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

BFD Node Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

All BFD sessions for a router are in the **Down** state, preventing any data traffic sending or transmission.

Clear the BFD Node Down Alarm

Procedure

No clearing procedure.

BFD Node Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

A BFD session for a router transitioned to the Up state.

Clear the BFD Node Up Alarm

Procedure

No clearing procedure.

BFD Scale Threshold

Default Severity: Minor and Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

When the number of BFD sessions drops below 90%, the device triggers three types of minor alarms:

- **Healthy**: BFD sessions are below 50%.
- **Notice**: BFD sessions are between 50% and 75%.
- **Warning**: BFD sessions are above 75% but below 90%.

When the number of BFD sessions exceeds 90%, the device triggers a critical alarm.

Clear the BFD Scale Threshold Alarm

SUMMARY STEPS

1. No clearing procedure.

DETAILED STEPS

Procedure

No clearing procedure.

BFD Site Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

All BFD sessions on all Cisco IOS XE Catalyst SD-WAN devices in a site are in the **Down** state, preventing data traffic transmission from or sending to that site.

Clear the BFD Site Down Alarm

Procedure

No clearing procedure.

BFD Site Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

A BFD session on a router in a site transitioned to the Up state.

Clear the BFD Site Up Alarm

Procedure

No clearing procedure.

BFD TLOC Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All BFD sessions for a TLOC (transport tunnel identified by a color) are in the **Down** state.

This means that no data traffic can be sent to or transmitted from that transport tunnel.

Clear the BFD TLOC Down Alarm

Procedure

No clearing procedure.

BFD TLOC Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

A BFD session for a TLOC transitioned to the **Up** state.

Clear the BFD TLOC Up Alarm

Procedure

No clearing procedure.

BGP Peer State Change

Default Severity: Major/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

This alarm indicates the BGP status between BGP peers. It triggers a major alarm when the peer goes down and a medium alarm when the peer is up.

Clear the BGP Peer State Change Alarm

Procedure

No clearing procedure.

BGP Router Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All BGP sessions on a router are in the **Down** state.

Clear the BGP Router Down Alarm

Procedure

No clearing procedure.

BGP Router Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A BGP session on a router transitioned to the **Up** state.

Clear the BGP Router Up Alarm

Procedure

No clearing procedure.

Certificate CRL Disabled

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The ID certificate is unrevoked from the CRL list.

Clear the Certificate CRL Has Been Disabled Alarm

Procedure

No clearance logic.

Certificate Expiration Status

Default Severity: Critical/Medium/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The ID, Proxy CA, Feature CA, or Syslog certificate is approaching or has surpassed its expiration date, with the following alarm levels:

- Minor: Expiry in < 6 months.
- Medium: Expiry in < 3 months but > 1 month
- Critical: Expiry in ≤ 1 month, ≤ 14 days, or if the certificate has expired

Clear the Certificate Expiration Status Alarm

Procedure

No clearing procedure.

Certificate Revoked

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The ID certificate is revoked from the CRL list.

Clear the Certificate Has Been Revoked Alarm

Procedure

No clearing procedure.

Cisco Secure Access

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device raises this alarm when configured tunnel credentials are incorrect, or when the Cisco SSE provider credentials are wrong.

Clear the Cisco Secure Access Alarm

Procedure

No clearing procedure.

Cisco SD-WAN Manager Node Latency State

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

Cisco SD-WAN Manager raises this alarm when it detects potential latency issues within the Cisco SD-WAN Manager cluster.

Clear the Cisco SD-WAN Manager Node Latency State

Procedure

When the latency issue resolves, Cisco SD-WAN Manager raises the same alarm in the "up" state to indicate the alarm is cleared.

Clear Installed Certificate

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All certificates on a controller or device, including the public and private keys and the root certificate are cleared. The device has returned to the factory-default state.

Clear the Clear Installed Certificate Alarm

Procedure

No clearing procedure.

Cloned vEdge Detected

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The network detects a duplicate router with the same chassis and serial numbers and the same system IP address.

Clear the Cloned Vedge Detected Alarm

Procedure

No clearing procedure.

Cloud OnRamp

Default Severity: Major

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN

The attempt to get the Cloud OnRamp status for a particular account failed.

Clear the Cloud OnRamp Alarm

Procedure

No clearing procedure.

Configuration Database Health State

Default Severity: Major/Critical/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Any config-db on the nodes is in an unhealthy state.

Clear the Configuration Database Health State Alarm

Procedure

The alarm clears when the node status is healthy.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Container Activate Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

IOX container app (e.g. UTD, TE) fails to activate.

Clear the Container Activate Failed Alarm

Procedure

No clearing procedure.

Container App Installation Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

IOX container app installation failure (e.g. TE, UTD)

Clear the Container App Installation Failed Alarm

Procedure

No clearing procedure.

Container Disk Usage

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The config-db/olap-db disk utilization crosses thresholds.

Clear the Container Disk Usage Alarm

Procedure

Release the disk space to clear the alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Container Reload failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

IOX container app reload fails.

Clear the Container Reload Failed Alarm

Procedure

No clearing procedure.

Container Reset Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

IOX container app reset fails.

Clear the Container Reset Failed Alarm

Procedure

No clearing procedure.

Container Upgrade Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

IOX container app upgrade procedure fails.

Clear the Container Upgrade Failed Alarm

Procedure

No clearing procedure.

Control All vSmart Down



Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control All vSmart Down** alarm appears as **Control All Controller Down**.

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

All control connections from Cisco Catalyst SD-WAN Controller in the overlay network are Down, preventing the overlay network from functioning.

Clear the Control All vSmart Down Alarm

Procedure

No clearing procedure.

Control vSmart Up



Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control vSmart Up** alarm appears as **Control Controller Up**.

Default Severity: Medium

Logical Object: Cisco Catalyst SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

All Cisco Catalyst SD-WAN Controller in the overlay network transition their control connections to the Up state.

Clear the Control vSmart Up Alarm

Procedure

No clearing procedure.

Control vManage Down

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control vManage Down** alarm appears as **Control Manager Down**.

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN

Cisco SD-WAN Manager has all control connections in the Down state.

Clear the Control vManage Down Alarm

Procedure

No clearing procedure.

Control vManage Up

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control vManage Down** alarm appears as **Control Manager Up**.

Default Severity: Medium

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN

Cisco SD-WAN Manager transitioned a control connection to the up state.

Clear the Control vManage Up Alarm

Procedure

No clearing procedure.

Control No Active vBond



Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control No Active vBond** alarm appears as **Control No Active Validator**.

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device/Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

When there is no connectivity from controllers or devices to a Cisco Catalyst SD-WAN Validator

Clear the Control No Active Validator Alarm

Procedure

The alarm automatically clears upon establishing connectivity to Cisco SD-WAN Validator.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Control Node Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device/Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All control connections for a Cisco vEdge device are in the **Down** state.

Clear the Control Node Down Alarm

Procedure

No clearing procedure.

Control Node Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device/Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

At least one control connection for a Cisco vEdge device transitioned to the **Up** State.

Clear the Control Node Up Alarm

Procedure

No clearing procedure.

Control Site Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All control connections from all Cisco Catalyst SD-WAN devices in a site are in the **Down** state. This prevents both control and data traffic from being sent to or transmitted from that site.

Clear the Control Site Down Alarm

Procedure

No clearing procedure.

Control Site Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A control connection from Cisco SD-WAN Manager and the Cisco Catalyst SD-WAN Validator in the site transitioned to the **Up** state.

Clear the Control Site Up Alarm

Procedure

No clearing procedure.

Control TLOC Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

All control connections for a TLOC are in the **Down** state.

Clear the Control TLOC Down Alarm

Procedure

No clearing procedure.

Control TLOC Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

At least one control connection for a TLOC is in the Up state.

Clear the Control TLOC Up Alarm

Procedure

No clearing procedure.

Control vBond State Change

Default Severity: Major/Critical

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **Control vBond State Change** alarm appears as **Control Validator State Change**.

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Alarm triggers when interfaces flap on devices.

Clear the Control vBond State Change Alarm

Procedure

Auto Clear

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CoR SaaS - Application Path Status

Default Severity: Major/Medium/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

CoR SaaS Application best path selection status:

- Major: CoR SaaS application is unreachable. This alarm is triggered with the path-status value set to ‘unreachable’ in the cloudexpress-application-change notification. CoR SaaS had a best path earlier and currently it no longer have any best path.
- Medium: CoR SaaS application is reachable. This alarm will be generated when CoR-SaaS recovers from the earlier lost best path and finds a working best path.

- Minor: CoR SaaS application is disabled. This alarm will be generated when CoR-SaaS is disabled in the IOS-XE edge device

Clear the CoR SaaS - Application Path Status Alarm

Procedure

Step 1 Triggering a medium alarm clears the major and minor alarms.

Step 2 Triggering a minor alarm clears the major and medium alarms.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CPU Usage

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The CPU load on a controller or device has reached a critical level, which may impair or shut down functionality, or a medium level, which could impair functionality.

Clear the CPU Usage Alarm

Procedure

Reboot your device or identify and close the process utilizing higher CPU cycles.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CPU Barrier

Default Severity: Major/Critical/Minor

Logical Object: Cisco Catalyst SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

Critical: The CPU load on a controller exceeds a high level, it may throttle further consumption of CPU resource.

Major: The CPU load on a controller exceeds a low level, it gives an early warning that the CPU load is a bit high.

Clear the CPU Barrier Alarm

Procedure

Reboot your device or identify and close the process utilizing higher CPU cycles.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Disk Barrier

Default Severity: Major/Critical/Minor

Logical Object: Cisco Catalyst SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

Critical: The disk usage on a controller exceeds a high level, it may throttle further consumption of disk resource.

Major: The disk usage on a controller exceeds a low level, it gives an early warning that the disk usage is a bit high.

Clear the Disk Barrier Alarm

Procedure

Reduce the disk utilization below the thresholds.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

DPI Status Alarm

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

This alarm shows a device's DPI status change for NBAR enable/disable, SDAVC enable/disable, traffic-category sync, and protocol sync operations.

Clear the DPI Status Alarm

Procedure

	Command or Action	Purpose
Step 1	This alarm auto-clears in most scenarios, if the alarm persists, reboot the device to clear the alarm.	

Memory Barrier

Default Severity: Major/Critical/Minor

Logical Object: Cisco Catalyst SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

Critical: The memory usage on a controller exceeds a high level, it may throttle further consumption of memory resource.

Major: The memory usage on a controller exceeds a low level, it gives an early warning that the memory usage is a bit high.

Clear the Memory Barrier Alarm

Procedure

Reduce the memory utilization below the thresholds.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

CRL Has Been Disabled

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The CRL setting is disabled.

Clear the CRL Has Been Disabled Alarm

Procedure

No clearing procedure.

CRL Has Been Enabled

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The CRL setting is enabled.

Clear the CRL Has Been Enabled Alarm

Procedure

No clearing procedure.

CRL Unreachable Or Invalid

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

With the CRL setting enabled, the Cisco SD-WAN Manager checks the CRL list on the server at regular intervals. The alarm activates if the server becomes unavailable or invalid either when first enabled or during periodic checks.

Clear the CRL Unreachable or Invalid Alarm

Procedure

No clearing procedure.

Data Policy Commit Failure

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

When Cisco SD-WAN Controller sends a centralized policy to a device, but the device fails to commit this configuration to the config DB (CDB) due to validation constraints or similar issues.

Clear the Data Policy Commit Failure Alarm

Procedure

No clearing procedure.

Default App List Update

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

When the default application or application family lists, which are used in application-aware routing policy, changes.

Clear the Default App List Update Alarm

Procedure

No clearing procedure.

Device Quarantine

Default Severity: Critical/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Two levels of alarms are raised:

1. Critical - CRL quarantine: The device certificate is quarantined based on the Certificate Revocation List (CRL).

2. Critical - Moved to staging certificate expiry: The device is moved to staging based on CRL and certificate quarantine settings.
3. Minor - Device unquarantined post certificate refresh: The device certificate is renewed or refreshed after being quarantined.

Clear the Device Quarantine Alarm

Procedure

If the certificate is staged, renew the device certificate to clear the Moved to Staging critical alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Device Activation Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Activation of a software image on a controller or device failed.

Clear the Device Activation Failed Alarm

Procedure

No clearing procedure.

Device Upgrade Failed

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The software upgrade on a router failed.

Clear the Device Upgrade Failed Alarm

Procedure

No clearing procedure.

DHCP Server State Change

Default Severity: Major

Logical Object: Cisco SD-WAN Control Components and Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The state of a DHCP server changed.

Clear the DHCP Server State Change Alarm

Procedure

No clearing procedure.

Disaster Recovery

Default Severity: Critical/Info/Warning/Error

Logical Object: Cisco SD-WAN Manager

Alarm Name	Summary	Severity
Export Data	Primary Successfully Exported	Info
Import Data	Secondary Successfully Imported	Info
Download Data	Replication payload successfully downloaded by secondary	Info
Export Data Fail	Primary Failed to export	Critical
Import Data Fail	Secondary Failed to import	Critical
Download Data Fail	Replication payload failed to download on secondary	Critical
Invalid Manager Creds	Invalid user credentials to access Manager. Please update the user credentials	Error
Arbitrator Down	The arbitrator is down	Critical

Primary Down	The primary is down	Critical
Secondary Down	The secondary is down	Critical
Switchover Success	Switchover successful	Info
Arbitrator Switchover	Switchover successful triggered by Arbitrator	Info
Switchover Warn	Not all vBonds are updated with new Manager list	WARNING
Switchover Fail	Switchover Failed	Critical
Link Failure Arbitrator	Failed to reach arbitrator	Critical
Link Failure Primary	Failed to reach primary cluster	Critical
Link Failure Secondary	Failed to reach secondary cluster	Critical
Vm Failure Primary	Majority of members in primary cluster are down	Critical
Vm Failure Secondary	Majority of members in secondary cluster are down	Critical
Deregistration Failure	DR De-registration Failure	Critical
Registration Failure	DR Registration Failure	Critical
vBond Down	vBond unreachable	Critical
Deregistration Success	DR De-registration Success	Info
Registration Success	DR Registration Success	Info
Read-replica Fall Behind	DR neo4j replication warning	Info
Pause Failure	DR Pause Failure	Critical

Clear the Disaster Recovery Alarm

Procedure

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Disk Read Speed

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Triggers Yellow, Orange, or Red alarms if the disk read speed for any path exceeds the corresponding thresholds.

Clear the Disk Read Speed Alarm

Procedure

A decrease in speed triggers a green alarm or clears the existing alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Disk Usage

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco Catalyst SD-WAN Control Components and Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

- Critical: The disk usage on a controller or device reaches a critical level, it may impair or shut down functionality.
- Medium: The disk usage on a controller or device reaches a medium level, it may impair functionality.

Clear the Disk Usage Alarm

Procedure

The alarm clears when disk utilization reduces below the thresholds.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Disk Write Speed

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Triggers yellow, orange, or red alarms when the disk write speed exceeds the set thresholds.

Clear the Disk Write Speed Alarm

Procedure

Reducing the speed triggers a green alarm or clears the existing alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Domain-ID Change

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A domain identifier in the overlay network changed.

Clear the Domain-ID Change Alarm

Procedure

	Command or Action	Purpose
Step 1	No clearing procedure.	

Edge Device Doesn't Support Umbrella CA Update

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The deployment of a new Umbrella root certificate to the device via Cisco SD-WAN Manager fails because it runs a version earlier than Cisco IOS XE Catalyst SD-WAN Release 17.9.1a.

Clear the Edge Device Doesn't Support Umbrella CA Update Alarm

Procedure

No clearing procedure.

Failed To Update Umbrella CA

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

Alarm triggers when the deployment of a new Umbrella Root Certificate to the device via Cisco SD-WAN Manager fails.

Clear the Failed to Update Umbrella CA Alarm

Procedure

No clearing procedure.

Geo Fence Alert Status

Default Severity: Major/Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

The device sends the following geo-fencing statuses to Cisco SD-WAN Manager:

- Device Location Inside: Major
- Device Location Lost: Major
- Device Location Update: Major
- Device Location Outside: Critical

Clear the Geo Fence Alert Status Alarm

Procedure

Step 1 The alarm clears in these scenarios:

- When the device is located inside, it clears the alarms raised from the device being outside or lost.
- When the device location is lost, the alarm auto-clears.
- When the device location updates, it clears the alarms raised from the device being lost.
- When the device location is outside, it clears the alarms raised from the device being lost.

Step 2 If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

High Direct Memory Usage

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The config-db direct memory usage reaches or exceeds 80% of the total direct memory.

Clear the High Direct Memory Usage Alarm

Procedure

No clearing procedure.

HTTP Proxy Unreachable

Default Severity: Critical

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The proxy is configured and the proxy server is unreachable.

Clear the HTTP Proxy Unreachable Alarm

Procedure

No clearing procedure.

Interface Admin State Change

Default Severity: Critical/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The administrative status of an interface in a controller or router changes from **Up** to **Down** (Critical) or **Down** to **Up** (Medium).

Clear the Interface Admin State Change Alarm

Procedure

No clearing procedure.

Interface State Change

Default Severity: Critical/Medium

Logical Object: Cisco SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The administrative or operational status of an interface changed.

Clear the Interface State Change Alarm

Procedure

No clearing procedure.

License Report Generation Failure

Default Severity: Critical

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The license report generation for a Virtual Account fails.

Clear the License Report Generation Failure Alarm

Procedure

The alarm clears when report generation for VA is successful.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Memory Usage

Default Severity: Major/Critical/Minor/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN deviceand Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The memory usage on a controller or device reaches a level that could critically impair or shut down functionality. A medium-level alarm triggers if the memory usage might impair functionality.

Clear the Memory Usage Alarm

Procedure

The alarm clears when the memory usage reduces.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Multicloud

Default Severity: Warning

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The alarrm is raised in the following scenarios:

- Alerts the user when a service name from GCP overlaps with an existing custom application in SD-AVC.
- Raises an alarm if a custom application has been deleted from GCP but is still being referenced in a policy.

Clear the Multicloud Alarm

Procedure

No clearing procedure.

MultiCloud License State Change

Default Severity: Critical/Medium

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN

Alerts the user if Megaport license state changes or expires.

Clear the MultiCloud License State Change Alarm

Procedure

The alarm clears when the license is renewed.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

NAT Update

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

The state of DIA routes changes:

1. When DIA goes **Down** (Major)
2. When DIA goes **Up** (Minor)

Clear the NAT Update Alarm

Procedure

No clearing procedure.

New CSR Generated

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A controller or router generates a certificate signing request (CSR).

Note In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, this alarm's severity value is Critical.

Clear the New CSR Generated Alarm

Procedure

No clearing procedure.

NHRP

Default Severity: Critical/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco SD-Routing

Raises critical severity alarms in the following conditions:

1. NextHopServer(NHS) State Change - When NHS connection is down
2. NextHopClient(NHC) State Change - When NHC connection is down
3. NHRP Control Packet Rate Limit - when control packet rate exceeds threshold

Clear the NHRP Alarm

Procedure

A medium severity alarm clears the critical severity alarms. A medium severity alarm is triggered in the following scenarios::

- When the NHS connection is up.
- When the NHC connection is up.
- When the device resets the limit every 10 seconds.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OMP Node Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All OMP connections for a Cisco IOS XE Catalyst SD-WAN device are in the **Down** state.

Clear the OMP Node Down Alarm

Procedure

The OMP Node up alarm automatically clears an OMP Node down alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OMP Node Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

At least one OMP connection for a Cisco vEdge device is in the **Up** state.

Clear the OMP Node Up Alarm

Procedure

No clearing procedure.

OMP Ribout Gen Failure

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

OMP Rib-out memory buffer reaches 100% capacity and Cisco SD-WAN Controller cannot generate anymore rib-outs.

Clear the OMP Ribout Gen Failure Alarm

Procedure

No clearing procedure.

OMP Ribout Usage

Default Severity: Critical/Major/Minor

Logical Object: Cisco SD-WAN Controller

Applicable for: Cisco Catalyst SD-WAN

Cisco SD-WAN Controller triggers this alarm when the OMP ribout memory buffer utilization exceeds the defined thresholds:

- Critical: When memory buffer usage is 75% or higher.
- Major: When memory buffer usage is 50% or higher.
- Minor: When memory buffer usage is below 50%.

Clear the OMP Ribout Usage Alarm

Procedure

The alarms clear in these conditions:

- When ribout usage drops below themajor threshold and reaches the minor threshold, Cisco SD-WAN Manager clears any pre existing major alarms.
- When ribout usage drops below the critical threshold and reaches the major threshold, Cisco SD-WAN Manager clears any pre existing critical alarms.

OMP Site Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All OMP connections to Cisco Catalyst SD-WAN Controller from all nodes in the site are in the Down state. This means that site cannot participate in the overlay network.

Clear the OMP Site Down Alarm

Procedure

The OMP site up alarm automatically clears the OMP site down alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

OMP Site Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

At least one OMP connection to Cisco Catalyst SD-WAN Controller from all nodes in the site is in the **Up** state.

Clear the OMP Site Up Alarm

Procedure

No clearing procedure.

OMP State Change

Default Severity: Critical/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The administration or operational state of an OMP session between a Cisco SD-WAN Controller and a Cisco vEdge device has changed, from **Up** to **Down** (Critical) or **Down** to **Up** (Medium).

Clear the OMP State Change Alarm

Procedure

A medium (Up) alarm automatically clears the critical (Down) alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Org Name Change

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The organization name used in the certificates for all overlay network devices changed.

Clear the Org Name Change Alarm

Procedure

No clearing procedure.

OSPF Neighbor State Change

Default Severity: Major/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Major: When the OSPF neighbor is down, deleted, or initialized.

Medium: When the OSPF neighbor is up.

Clear the OSPF Neighbor State Change Alarm

Procedure

The medium alarm automatically clears a major alarm.

OSPF Router Down

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

All OSPF connections on a router are in the **Down** state.

Clear the OSPF Router Down Alarm

Procedure

The OSPF Router Up Alarm automatically clears this alarm.

OSPF Router Up

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

An OSPF connection on a router transitioned to the **Up** state.

Clear the OSPF Router Up Alarm

Procedure

No clearing procedure.

PIM Interface State Change

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The state of a PIM interface changes from down to up or up to down.

Clear the PIM Interface State Change Alarm

Procedure

When the PIM interface state changes from down to up, it triggers an alarm.

Policy Enforcement Status

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Policy programming failed. Further policy pushes may not be successful.

Clear the Policy Enforcement Status Alarm

Procedure

Collect admin-tech and raise a support case. Schedule maintenance window and reboot the device to re-program policy

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Process Restart

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A process (daemon) on a device or any Cisco Catalyst SD-WAN Control Components restarted.

Clear the Process Restart Alarm

Procedure

No clearing procedure.

Pseudo Commit Status

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Cisco SD-WAN Manager has pushed a device configuration template to a controller or router. Cisco SD-WAN Manager pushes a tentative configuration (called the pseudo commit) to the device and starts the rollback timer. If with the new configuration, the control connections between the device and Cisco SD-WAN Manager come up, the tentative configuration becomes permanent. If the control connections do not come up, the tentative configuration is removed, and the device's configuration is rolled back to the previous configuration (that is, to the last known working).

Clear the Pseudo Commit Status Alarm

Procedure

No clearing procedure.

PxGrid Connection Notification

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Cisco Catalyst SD-WAN Control Components sends the alarm if the pxGrid account is not activated correctly during the ISE setup or when there is a connectivity loss to the ISE server for more than 12 hours.

Clear the PxGrid Connection Notification Alarm

Procedure

Fixing the mentioned scenarios prevents the device from raising this alarm. There is no explicit clearance logic for alarms that were raised previously.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

QFP Exmem Usage

Default Severity: Major/Critical/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The

```
show platform hardware qfp active infrastructure exmem statistics
```

CLI gives the output of QFP exmem information.

The device checks the QFP EXMEM DRAM information and, based on a threshold value, sends an alarm to SD-WAN Manager.

Clear the QFP exmem Usage Alarm

Procedure

The device alarm changes based on usage levels:

- The alarm indicates healthy usage when it is 80% or less.
- The alarm indicates a warning when usage is between 85% and less than 95%.
- The alarm indicates a critical state when usage is 95% or more.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Quarantine Monitoring Thread

Default Severity: Critical/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Quarantine Monitoring Thread starts on device quarantine feature enablement.

Two levels of alarms are raised:

1. Critical - When the monitoring thread fails in its processing, but only one alarm is raised in the case of consecutive failures.
2. Minor - When the monitoring thread successfully processes its task, but only if there was a past failure.

Clear the Quarantine Monitoring Thread Alarm

Procedure

A pass (minor) alarm automatically clears the fail (critical) alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RootCA Certificate Warning

Default Severity: Major/Critical/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

There are 3 levels for this alarm:

1. Minor: When a root certificate is renewed.
2. Major: When a root certificate is about to expire in the next 24 hours.
3. Critical: When a root certificate has expired.

Clear the RootCA Certificate Warning Alarm

Procedure

Renewing the root certificate clears the expiring (major) and expired (critical) alarms.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

RootCA Sync Failure

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Whenever root CA chain synchronization (e.g., certificate installation) fails.

Clear the RootCA Sync Failure Alarm

Procedure

No clearing procedure.

Root Certification Chain Installed

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Whenever root certification chain is installed (eg: on root ca chain modification, certificate install), a minor level alarm is raised per device.

The file containing the root certificate key chain was installed on a controller or router.

Note In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, this alarm's severity value is critical.

Clear the Root Certification Chain Installed Alarm

Procedure

No clearing procedure.

Root Certification Chain Uninstalled

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Whenever root certification chain is uninstalled (eg: on root ca chain invalidation), a minor level alarm is raised per device.

The file containing the root certificate key chain was removed from a controller or router.

Note In Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and earlier, this alarm's severity value is critical.

Clear the Root Certification Chain Uninstalled Alarm

Procedure

No clearing procedure.

SAML Security Rejection

Default Severity: Major

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 26.2.1

Cisco SD-WAN Manager raises this alarm when it rejects a SAML login response that may pose a security risk or cannot be validated. The alarm identifies the node that rejected the response and provides details such as the rejection reason, source IP address, endpoint, and payload size to help administrators investigate.

Conditions that can raise this alarm include:

- A DOCTYPE declaration
- An external XML entity declaration
- A parameter entity reference
- An XInclude directive
- An unusually large SAML response
- Malformed SAML XML
- An invalid SAML message
- A SAML security-validation failure
- Repeated qualifying SAML login-response failures from the same source IP address

The alarm may indicate a malicious login attempt, an incorrectly constructed SAML response, or an identity provider configuration problem.

Clear the SAML Security Rejection Alarm

Procedure

Review the rejection reason and source IP address in the alarm details. Check the Cisco SD-WAN Manager SSO log, audit log, alarm log, and syslog for additional information.

- If the request came from a trusted identity provider, correct its SAML configuration to send a valid and secure response.
- If the source is not trusted, block the source IP address or restrict its access, and investigate the activity as a potential security incident.

After resolving the underlying issue and confirming that the rejected requests have stopped, manually clear the alarm in Cisco SD-WAN Manager.

If the alarm does not clear, collect the relevant SSO, audit, alarm, and syslog information and contact Cisco TAC (1 800 553-2447).

SD-AVC Cloud Connector Credentials Error

Default Severity: Major

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN

The SD-AVC Cloud Connector is enabled, but the cloud connector credentials are expired.

Clear the SD-AVC Cloud Connector Credentials Error Alarm

Procedure

No clearing procedure.

SD-AVC Password Sync

Default Severity: Critical/Minor

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN

This alarm concerns the interaction between the SD-AVC component and Cisco SD-WAN Manager. The conditions are used for troubleshooting with TAC, including the in-sync (minor) and out-of-sync (critical) alarms.

Clear the SD-AVC Password Sync Alarm

Procedure

The minor alarm autoclears the critical alarm.

SD-AVC State Change

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN

This alarm shows a change in the status of the SD-AVC component. Statuses include unreachable (major), unknown (major), unconfigured (major), configured (major), connected (minor), and disconnected (major).

Clear the SD-AVC State Change Alarm

Procedure

Alarms are cleared in these scenarios:

- The unknown alarm clears the unreachable alarm.

- The unconfigure alarm clears the unreachable and unknown alarms.
- The configure alarm clears the unreachable, unknown, and the unconfigured alarms.
- The connected alarm clears the unreachable, unknown, unconfigured, configured, and disconnected alarms.
- The disconnected alarm clears the unreachable, unknown, unconfigured, and configured alarms

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

SD-AVC Troubleshooting

Cisco SD-WAN Manager alert

Default Severity: Critical

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN

The SD-AVC Troubleshooting alarm indicates that some information is out of sync between SD-AVC component and Cisco SD-WAN Manager. The information can relate to custom applications, Protocol Packs, cloud-sourced applications, or SaaS feeds.

Device alerts

Default Severity: Critical/Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

The SD-AVC Troubleshooting alarm indicates a device has an alert-type of Error or Warning. A device alert can have these alert states:

- NO_CONNECTIVITY: SD-AVC is not receiving connectivity packets from the device.
- NO_HTTPS_CONNECTIVITY: The device is not able to retrieve information from SD-AVC.
- NO_SOCKET_CACHE_EXPORT: The device is not sending IP + PORT cache entries.
- NO_L3_CACHE_EXPORT: The device is not sending DNS IP rule entries.
- NO_PD_EXPORT: The device is not exporting analytics data.
- PD_NOT_CONFIGURED: The device is not configured with protocol discovery on any interface.
- NO_RULE_PACK_UPDATE: The device is not able to load IP rule information provided by SD-AVC.
- NO_PPDK_UPDATE: The device is not loading external Protocol Pack Distribution Kit (PPDK) information.
- NO_DP_MEMORY: There is insufficient memory on the device, which may cause the Protocol Pack or PPDK to be blocked.

Clear the SD-AVC Troubleshooting alarm

Procedure

This alarm is automatically cleared when the error condition is not detected during the subsequent attempt to retrieve device details from SD-AVC.

Security Certificate Expired

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

When any Cisco Catalyst SD-WAN Control Components or Cisco IOS XE Catalyst SD-WAN device certificate expires.

Clear the Security Certificate Expired Alarm

Procedure

No clearing procedure.

Security Certificate Expiring

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A control component or device certificate is nearing its expiry date.

For Cisco IOS XE Catalyst SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Manager Release 20.12.1, you will receive the notification in this frequency:

- Once every month from 1 year to 6 months before expiry.
- Once every week from 6 months to 30 days before expiry.
- Once a day from 30 days to 1 week before expiry.
- Every 12 hours during the final week leading to expiry.

For Cisco IOS XE Catalyst SD-WAN Release 17.11.1a and Cisco SD-WAN Manager Release 20.11.1, you will receive the notification in this frequency:

- Once every week from 60 days to 1 week before expiry.

- Once a day during the final week before expiry.

Clear the Security Certificate Expiring Alarm

Procedure

No clearing procedure.

Site-ID Change

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The overlay network changed a site identifier.

Clear the Site-ID Change Alarm

Procedure

No clearing procedure.

SLA Violation

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

A BFD session changes its SLA Violation Packet Drop from one level to another.

Clear the SLA Violation Alarm

Procedure

No clearing procedure.

SLA Violation Packet Drop

Default Severity: Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

An Application-Aware Routing (AAR) Policy forwards traffic based on SLA criteria. When none of the tunnels meet the SLA and SLA strict is configured, the device drops the traffic and triggers this alarm.

This alarm is generated when a data or AAR policy is configured and a packet is dropped with the SdwanDataPolicyDrop QFP drop code, specifically when the FIA trace shows the "Tunnel Match Reason" as "MATCHED_NONE." This alarm may also occur intermittently when the system cannot find a route to the destination or when it fails to resolve and install the OMP route into the RIB due to the data plane or BFD session being down.

Clear the SLA Violation Packet Drop Alarm

Procedure

No clearing procedure.

Software out of compliance

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

An alarm is raised in the **Alarm Details** page in Cisco SD-WAN Manager when devices running versions older than N-2 are detected in the overlay. If the list of out-of-compliance devices contains five or fewer entries, the **Probable Causes** section displays the device hostnames. For more than five devices, the **Probable Causes** section displays only the count of out-of-compliance devices.

Clear the software out of compliance alarm

Procedure

This alarm automatically clears once all incompatible devices are upgraded to a compatible version.

SSL Certificate Warning

Default Severity: Major/Critical/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

This alarm triggers when the following events concerning certificates in IOS PKI occur.

- Certificate installation events:
  - CRYPTO_PKI_CERTIFICATE_INSTALL: Major
  - CRYPTO_PKI_CERTIFICATE_FAILURE: Critical
  - CRYPTO_PKI_CERTIFICATE_DELETE: Critical
  - CRYPTO_PKI_CERTIFICATE_EXPIRY (expiry after 7 days): Minor
- SCEP response to certificate enrollment requests:
  - CRYPTO_PKI_CERTIFICATE_SCEP_GRANTED: Minor
  - CRYPTO_PKI_CERTIFICATE_SCEP_REJECTED: Major
  - CRYPTO_PKI_CERTIFICATE_SCEP_PENDING: Major

Clear the SSL Certificate Warning Alarm

Procedure

No clearing procedure.

System IP Change

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The system IP address on Cisco Catalyst SD-WAN Control Components or Cisco IOS XE Catalyst SD-WAN device changed.

When a device's system IP changes multiple times, the site-based alarm filter shows only the latest system-ip-change alarm, hiding intermediate changes. Filtering by device hostname displays all system-ip-change alarms.

Clear the System IP Change Alarm

Procedure

No clearing procedure.

System IP Reuse

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device and Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

More than one device in the overlay network is using the same system IP address.

Clear the System IP Reuse Alarm

Procedure

No clearing procedure.

System License Mismatch

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A Cisco Catalyst 8000V Edge device (C800V) generates this alarm when spun up in AWS. When the PAYG UUID is selected in the bootstrap to bring up a C8000V Edge virtual machine in AWS, the corresponding C8000V Edge PAYG AMI must be used. If a BYOL C8000V UUID is used with a C8000V Edge PAYG AMI in AWS, the device raises a system-license-mismatch notification, and its bandwidth is limited to 10 Mbps.

Clear the System License Mismatch Alarm

Procedure

No clearing procedure.

System Reboot Issued

Default Severity: Critical/Medium

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device initiated a reboot on its own (Critical) or a user initiated the reboot (Medium).

Clear the System Reboot Issued Alarm

Procedure

No clearing procedure.

Template Rollback

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device failed to attach a configuration template to Cisco IOS XE Catalyst SD-WAN device within the configured rollback time, so it rolled back the configuration to the previous version instead of updating it.

Clear the Template Rollback Alarm

Procedure

No clearing procedure.

Tracker State Change

Default Severity: Major/Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

An endpoint tracker's state changes to Up (Medium) or Down (Major).

Clear the Tracker State Change Alarm

Procedure

The medium alarm autoclears the major alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

Umbrella CA has been Updated

Default Severity: Medium

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN

A new Umbrella root certificate is successfully deployed to a device using Cisco SD-WAN Manager.

Clear the Umbrella CA has been updated Alarm

Procedure

No clearing procedure.

Unsupported SFP Detected

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The hardware router detected an unsupported transceiver with its software.

Clear the Unsupported SFP Detected Alarm

Procedure

No clearing procedure.

UTD File Analysis Status Event

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable For: Cisco Catalyst SD-WAN and Cisco SD-Routing

The connectivity status to the AMP cloud for file analysis changes.

Clear the UTD File Analysis Status Event Alarm

Procedure

No clearing procedure.

UTD File Analysis Upload Status

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Displays the file upload status for file analysis updates.

Clear the UTD File Analysis Upload Status Alarm

Procedure

No clearing procedure.

UTD File Reputation Alert

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The AMP cloud issues a verdict of drop, allow, alert, or unknown for an uploaded file.

Clear the UTD File Reputation Alert Alarm

Procedure

No clearing procedure.

UTD File Reputation Retrospective Alert

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

AMP returns the cloud analysis results for a file uploaded in the past week.

Clear the UTD File Reputation Retrospective Alert Alarm

Procedure

No clearing procedure.

UTD File Reputation Status Event

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

This alarm provides the status of the device's connectivity to the AMP cloud.

Clear the UTD File Reputation Status Event Alarm

Procedure

No clearing procedure.

UTD IPS Alert

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Network traffic generates an IPS event with a status of unknown, drop, or alert.

Clear the UTD IPS Alert Alarm

Procedure

No clearing procedure.

UTD Notification

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The UTD engine status changes to green or red, or the device hits the maximum number of flows. It indicates that the engine may be down due to an IPS update.

Clear the UTD Notification Alarm

Procedure

This alarm functions as a notification. It indicates that the engine may be down due to an IPS update.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UTD Update

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The UTD signature or URL-F DB update results in a failure or a success. Investigate the reason in the event of a failure. Out-of-date signatures will impact the solution's efficacy.

Successful UTD update alarms are reported with Major severity in Cisco Catalyst SD-WAN Manager Release 20.15.x and Minor severity in Cisco Catalyst SD-WAN Manager Release 26.1.x and later.

Clear the UTD Update Alarm

Procedure

Investigate the reason in the event of failure. Out-of-date signatures will impact the solution's efficacy.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

UTD URL-F Connectivity Event

Default Severity: Major/Minor

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The URL-F connectivity to BrightCloud status changes to Down (Major) or Up (Minor).

Clear the UTD URL-F Connectivity Event Alarm

Procedure

No clearing procedure.

UTD Version Mismatch

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The UTD tar/ova version does not match the IOS-XE version.

Clear the UTD Version Mismatch Alarm

Procedure

Follow one of these methods to clear the alarm.

- Upgrade or downgrade the current UTD VMAN OVA/IOX TAR to match the IOS-XE version.
- Upgrade or downgrade the current IOS-XE version to match the UTD VMAN OVA/IOX TAR.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

vEdge Serial File Uploaded

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device uploads the WAN Edge serial number file to the Cisco SD-WAN Manager server. The Cisco SD-WAN Controller and Cisco SD-WAN Validator send an alarm when the vEdge serial file loads successfully, visible after you trigger "Send to Controllers" on the Configuration → Certificates → WAN Edges screen.

Clear the vEdge Serial File Uploaded Alarm

Procedure

No clearing procedure.

vManage Critical Space Usage

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vManage Critical Space Usage** alarm appears as **Manager Critical Space Usage**.

Default Severity: Critical/Medium

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A critical alarm is triggered when:

- Disk usage is greater than or equal to 80%.
- Free disk space is less than or equal to 10GB.

A medium alarm is triggered when a disk usage is less than 75%.

Clear the vManage Critical Space Usage Alarm

Procedure

The medium alarm autoclears the critical alarm.

vManage Node Reachability State

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vManage Node Reachability State** alarm appears as **Manager Node Reachability State**.

Default Severity: Major/Critical

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Cisco SD-WAN Manager detects that the Out-of-Band (OOB) interface of a remote Cisco SD-WAN Manager in the cluster is unreachable.

Clear the vManage Node Reachability State Alarm

Procedure

The alarm clears when reachability is restored.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

vManage Queue State

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vManage Queue State** alarm appears as **Manager Queue State**.

Default Severity: Major/Medium

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The event data collector queue fills up, indicating that no new device events will be consumed until the queue has space available again.

Clear the vManage Queue State Alarm

Procedure

No clearing procedure.

vManage Self Signed Certificate Out Of Sync

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vManage Self Signed Certificate Out Of Sync** alarm appears as **Manager Self Signed Certificate Out Of Sync**.

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The Root CA chain does not include the SD-WAN Manager self-signed certificate.

Clear the vManage Self Signed Certification Out Of Sync Alarm

Procedure

No clearing procedure.

vManage Service State



Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vManage Service State** alarm appears as **Manager Service State**.

Default Severity: Major/Critical/Medium

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

This alarm monitors the status of services like SD-AVC on Cisco SD-WAN Manager nodes.

- Critical: When a service, such as the configuration database or messaging server, is down or terminated.
- Medium: When a service like SD-AVC is moved from one Cisco SD-WAN Manager node to another.
- Major: When the service is restored to its normal state.

Clear the vManage Service State Alarm

Procedure

A major alarm autoclears the critical alarm.

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

vSmart/vManage Serial File Upload

Note From Cisco Catalyst SD-WAN Control Components Release 26.1.x, the **vSmart/vManage Serial File Upload** alarm appears as **Controller/Manager Serial File Upload**.

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

Cisco SD-WAN Manager uploads the file containing certificate serial numbers for Cisco SD-WAN Managers and Cisco Catalyst SD-WAN Controllers in the overlay network. The validator sends an alarm when it successfully loads the Cisco Catalyst SD-WAN Controllers file, visible after you trigger "Send to Validator" on the Configuration → Certificates → Control Components screen.

Clear the vSmart/vManage Serial File Upload Alarm

Procedure

No clearing procedure.

WebServer Certificate Warning

Default Severity: Critical

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A Web Server Certificate is about to expire in less than one month.

Clear the WebServer Certificate Warning Alarm

Procedure

No clearing procedure.

ZBFW Geo DB Notification

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The geo-location database file on your device was updated with a result of success or failure, indicating the file path on the device.

Clear the ZBFW Geo DB Notification Alarm

Procedure

No clearing procedure.

ZBFW Half Open Limit Hit

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The configured limit for half-open sessions reached its limit.

Clear the ZBFW Half Open Limit Hit Alarm

Procedure

The alarm clears when the session count falls below the half-open limit. limit

If the alarm does not clear, log into the Technical Support Website at https://www.cisco.com/c/en/us/support/index.html for more information or call Cisco TAC (1 800 553-2447).

ZBFW Policy Download Error

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The ZBFW policy download fails due to memory issues, configuration errors, classification problems, or internal errors.

Clear the ZBFW Policy Download Error Alarm

Procedure

No clearing procedure. We recommend immediate triage, as the firewall may be improperly configured or not operational.

ZBFW Session Maximum

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The firewall parameter map reached the maximum configured sessions.

Clear the ZBFW Session Maximum Alarm

Procedure

No clearing procedure.

ZBFW Session Rate Alert Off

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device detects that the rate of establishing half-open sessions falls below the configured low water mark for the specified time period.

Clear the ZBFW Session Rate Alert Off Alarm

Procedure

No clearing procedure.

ZBFW Session Rate Alert On

Default Severity: Major

Logical Object: Cisco IOS XE Catalyst SD-WAN device

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

The device detects that the rate of establishing half-open sessions rises above the configured threshold for the time period.

Clear the ZBFW Session Rate Alert On Alarm

Procedure

No clearing procedure.

Zscaler SSE Sublocation

Default Severity: Medium

Logical Object: Cisco SD-WAN Manager

Applicable for: Cisco Catalyst SD-WAN

API calls to Zscaler fail to create, update, or delete a sublocation.

Clear the Zscaler SSE Sublocation Alarm

Procedure

No clearing procedure.

ZTP Upgrade Failed

Default Severity: Critical

Logical Object: Cisco Catalyst SD-WAN Control Components

Applicable for: Cisco Catalyst SD-WAN and Cisco SD-Routing

A Cisco Catalyst SD-WAN Control Components failed to upgrade software using ZTP.

Clear the ZTP Upgrade Failed Alarm

Procedure

No clearing procedure.

Related Documentation

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17
- User Documentation for Cisco SD-WAN Release 20

Full Cisco Trademarks with Software License

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)