

Event Analytics for SAN Fabrics, Release 4.2.1

Table of Contents

New and changed information . . . 1
Alarms . . . 2
- Alarms Raised . . . 2
- Alarms Cleared . . . 3
- Enable alarm policies . . . 4
  - Forward alarms to registered SNMP listeners . . . 4
  - Managing alarm policies . . . 5
  - Create new alarm policies . . . 7

Events . . . 13
- Event Setup . . . 14

Accounting . . . 18
Remote Clusters . . . 19
Copyright . . . 20

New and changed information

The following table provides an overview of the significant changes up to this current release. The table does not provide an exhaustive list of all changes or of the new features up to this release.

Release Version	Feature	Description
Nexus Dashboard 4.2.1	There were no major changes from the previous release.	

Alarms

This tab displays the alarms that are generated for various categories. This tab displays information such as **ID** (optional), **Severity**, **Failure Source**, **Name**, **Category**, **Acknowledged**, **Creation Time**, **Last Updated** (optional), **Policy**, and **Message**. You can specify the **Refresh Interval** in this tab. You can select one or more alarms and then acknowledge or unacknowledge their status using the **Change Status** drop-down list. In addition, you can select one or more alarms and then click the **Delete** button to delete the alarms.

A default alarm policy, **pm_optics_predict**, is available so that when optics values exceed the default threshold as defined on the switch, alert notifications are sent out automatically. The **pm_optics_predict** raised alarms are listed on the **Analyze > Event Analytics > Alarms > Alarms Raised** page.

For more information, see the section "Viewing Performance Information for Optics" in Add Interfaces for SAN Fabrics.

Alarms Raised

1. Navigate to **Analyze > Event Analytics > Alarms**.
2. Click the **Alarms Raised** tab to view the alarm policies that were triggered by an alarm.
3. Double-click on the link in the **ID** column to open the **Alarm ID** page for the selected alarm ID.

   This page displays more details about the selected alarm ID and also provides a history of the alarms raised for the associated source.

   A default alarm policy, **pm_optics_predict**, is available so that when optics values exceed the default threshold as defined on the switch, alert notifications are sent out automatically. The **pm_optics_predict** raised alarms are listed on the **Analyze > Event Analytics > Alarms > Alarms Raised** page.

   For more information, see the section "Viewing Performance Information for Optics" in Add Interfaces for SAN Fabrics.

   The following table describes the fields that appear on the **Alarms Raised** tab.

Field	Description
ID	Specifies the ID of the alarm.
Severity	Specifies the severity of the alarm.
Source	Specifies the name of the source.
Name	Specifies the name of the alarm.
Message	Displays the message.
Category	Specifies the category of the alarm.
Creation Time	Specifies the time at which the alarm was created.
Updated Time	Specifies the time at which the alarm was updated.
Policy	Specifies the policy of the alarm.

Field	Description
Ack User	Displays the username who acknowledged the alarm.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on the **Alarms Raised** tab.

Action Item	Description
Acknowledge	Select one or more alarms and choose **Acknowledge**. Allows you to bookmark the alarms and adds ack user name to the **Acknowledged** column.
Unacknowledge	Select one or more alarms and choose **Unacknowledge** to remove the bookmarked alarms.  Only acknowledged alarms can be unacknowledged.
Clear	Select one or more alarms and choose **Clear** to clear the alarm policy manually. The cleared alarms will be moved to the **Alarms Cleared** tab.
Delete Alarm	Select one or more alarms and choose **Delete** to delete the alarm.

Alarms Cleared

1. Navigate to **Analyze > Event Analytics > Alarms > Alarms Cleared**.

   The **Alarms Cleared** tab has the list of alarms that are cleared in the **Alarms Raised** tab. This tab displays information such as **ID**, **Severity**, **Failure Source**, **Name**, **Category**, **Acknowledged**, **Creation Time**, **Cleared At**, **Cleared By**, **Policy**, and **Message**. You can view the cleared alarm details for a maximum of 90 days.

2. You can choose one or more alarms and click **Actions > Delete** to delete the alarms.

   The following table describes the fields that appear on the **Alarms Cleared** tab.

Field	Description
ID	Specifies the ID of an alarm.
Status	Indicates the status of the alarm as **Cleared**.
Source	Specifies the IP address of the source alarm.
Name	Specifies the name of the alarm.
Message	Specifies the CPU utilization and other details of alarm.
Category	Specifies the category of the alarm.
Creation Time	Specifies the time at which the alarm was created.
Cleared Time	Specifies the time at which the alarm was cleared.
Cleared By	Specifies the user who cleared the alarm.

Field	Description
Policy	Specifies the policy of the alarm. A default alarm policy, **pm_optics_predict**, is available so that when optics values exceed the default threshold as defined on the switch, alert notifications are sent out automatically. When small form-factor pluggable (SFP) thresholds come back to normal or are below the specified threshold, the raised optic alerts or alarms are cleared automatically and are listed on the **Analyze > Event Analytics > Alarms > Alarms Raised** page. For more information, see the section "Viewing Performance Information for Optics" in Add Interfaces for SAN Fabrics.
Ack User	Specifies the acknowledged user role name.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on the **Alarms Cleared** tab.

Action Item	Description
Delete Alarm	Select an alarm and choose **Delete** to delete the cleared alarm.

Enable alarm policies

Follow these steps to enable alarm policies.

1. Navigate to **Analyze > Event Analytics > Alarms > Alarm Policies**.
2. Ensure that you check the **Enable external alarms** checkbox in **Admin > System Settings > Fabric Management > Alarms**.

   You must restart the Nexus Dashboard server for this change to take effect.

Forward alarms to registered SNMP listeners

Follow these steps to forward alarms to registered SNMP listeners.

1. Choose **Admin > System Settings > Fabric Management > Alarms**, and ensure that you check the **Enable external alarms** checkbox. You must restart the Nexus Dashboard server for this change to take effect.
2. Choose **Admin > System Settings > Fabric Management > Alarms**, and enter an external port address in the **alarm.trap.listener.address** field.
3. Click **Apply Changes** and restart the Nexus Dashboard.



Ensure that you check the **Forwarding** checkbox in the **Alarm Policy creation** dialog box to enable forwarding alarms to external SNMP listeners.

These fields appear on the **Analyze > Event Analytics > Alarms > Alarms Policies** page.

Field	Description
Name	Specifies the name of the alarm policy These default policies are available for triggering an alarm when zone, FCNS, and FLOGI scale percentages on a switch exceed the defined threshold of 80%. · **Zone_alarm** · **Fcns_alarm** · **Flogi_alarm** Nexus Dashboard runs a nightly scan at midnight for determining if a zone, FCNS, and FLOGI scale limitation is triggered for raising an alarm. You can export or import a **Zone_alarm**, **Fcns_alarm**, and a **Flogi_alarm** policy as a .txt file, update the scale percentage values, and wait for the nightly scan to see the raised alarms on the **Analyze > Event Analytics > Alarms > Alarms Raised** page.
Description	Specifies the description of the alarm policy
Status	Specifies the status of the alarm policy. · **Activated** · **Deactivated**
Policy type	Specifies the type of the policy. · Device Health Policy · Interface Health Policy · Syslog Alarm Policy · SAN Insights Anomaly · External
Devices	Specifies the devices to which the alarm policy is applied.
Interfaces	Specifies the interfaces.
Details	Specifies the details of the policy.
External	Specifies if the policy type is a default policy or if it is auto-generated by Nexus Dashboard.

Managing alarm policies

You can manage alarm policies for your fabric using the action items available in the **Actions** drop-down list on the **Analyze > Event Analytics > Alarms > Alarms Policies** page.

These action items are available in the **Actions** drop-down list.

Action Item	Description
Create new alarm policy	Choose **Create new alarm policy** to create a new alarm policy. For more information, see Create new alarm policies.
Edit	Check the checkbox next to a policy name and choose **Edit** to modify the alarm policy.
Delete	Check the checkbox next to a policy and choose **Delete** to remove the alarm policy.
Activate	Check the checkbox next to a policy and choose **Activate** to activate and apply the alarm policy.
Deactivate	Check the checkbox next to a policy and choose **Deactivate** to disable and deactivate the alarm policy.
Import	Check the checkbox next to a specific alarm policy, then choose **Import** to upload alarm policy from a .txt file.
Export	• Click the box next to a specific alarm policy, then click **Export** to download that alarm policy as a .txt file. • Check or uncheck all the checkboxes next to the alarm policies, then click **Export** to download all the alarm policies as a .txt file.

You can add these types of alarm policies.

Policy	Description
Device Health Policy	Device health policies enable you to create alarms when Device SNMP Unreachable, or Device SSH Unreachable or when the device peripherals are unavailable. Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.
Interface Health Policy	Interface health policies enable you to monitor Up or Down, Packet Discard, Error, Bandwidth details of the interfaces. By default, all interfaces are monitored.
Syslog Alarm Policy	A syslog alarm policy defines a pair of syslog messages formats; one which raises the alarm, and one which clears the alarm.
SAN Insights Anomaly Policy	A SAN Insights anomaly policy enables you to create customized alarms to identify issues in the fabric using SAN Insight data.
pm_optics_predict	An external **pm_optics_predict** alarm policy is available so that when optics values exceed the default threshold as defined on the switch, alert notifications are sent out automatically. You cannot modify the **pm_optics_predict** alarm policy. For more information, see the section "Viewing Performance Information for Optics" in Add Interfaces for SAN Fabrics.

You can modify or activate or use data of pre-provisioned SAN Insights anomaly policies that are in **Not Active** state by default.

Create new alarm policies

You can add new alarm policies for these types of policies.

- Device Health Policy
- Interface Health Policy
- Syslog Alarm Policy
- SAN Insights Anomaly Policy

After you create a new alarm policy in the **Analyze > Event Analytics > Alarms > Alarm Policies** tab, click **Refresh** to view the newly-created alarm policy.

Device Health Policy

Device health policies enable you to create alarms when certain conditions are met. By default, all devices are monitored.

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: Check the checkbox to forward alarms to registered SNMP listeners inNexus Dashboard. From the Nexus Dashboard UI, choose Admin > System Settings > Fabric Management > Events.



You must check the **Forwarding** checkbox while configuring alarm policies to ensure alarms are forwarded to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. In Nexus Dashboard UI, choose **Admin > System Settings > Fabric Management > Events**. Configure the SMTP parameters, click **Save**, and restart Nexus Dashboard services.
- Specify the CPU utilization parameters, memory utilization parameters, and environmental temperature parameters.
- **Device Availability**: Device health policies enable you to create alarms for these situations.
  - **Device Access**: When device SNMP or device SSH is unnreachable.
  - **Peripherals**: When fan, power supply, or module is unnreachable.

    For detailed trap OID definitions, refer to https://snmp.cloudapps.cisco.com/Support/SNMP/do/BrowseOID.do.

Also, these policies enable you to monitor chassis temperature, CPU, and memory usage.

Choose the devices for which you want to create policies. Specify the policy name, description, CPU Utilization parameters, Memory Utilization parameters, Environment Temperature parameters, device availability, and device features.

Interface Health Policy

Interface health policies enable you to monitor the interface status, packet discards, errors, and utilization details of the interfaces. By default, all interfaces are monitored.

Choose the devices for which you want to create policies and then specify the following parameters:

- **Policy Name**: Specify a name for the policy. It must be unique.
- **Description**: Specify a brief description for the policy.
- **Forwarding**: Check the checkbox to forward alarms to registered SNMP listeners in Nexus Dashboard after configuring sender and recepient email addresses in **Admin > System Settings > Fabric Management > Alarms** tab.



You must check the **Forwarding** checkbox while configuring alarm policies to ensure alarms are forwarded to an external SNMP listener.

- **Email**: You can forward alarm event emails to recipients when an alarm is created, cleared or when the severity is changed. From Nexus Dashboard UI, navigate to **Admin > System Settings > General > Email**, configure the SMTP parameters and restart Nexus Dashboard services.
- **Linkstate**: Choose linkstate option to check for the interface link status. You can generate an alarm whenever a link is down and clear the alarms when the link is up.
- **Bandwidth (In/Out)**: Allows you to set the maximum bandwidth allowed in inbound and outbound directions. The system generates alarms when the bandwidth exceeds the specified values.
- **Interface Power (Rx/Tx)**: Allows you to configure low warning thresholds for Tx Power and Rx Power. The system generates alarms when the threshold values drop below the configured values. The interfaces are monitored every 15 minutes.
- **Interface Current**: Allows you to configure low warning thresholds for current. The system generates alarms when the threshold values drop below the configured values. The interfaces are monitored every 15 minutes.
- **Interface Voltage**: Allows you to configure low warning thresholds for voltage. The system generates alarms when the threshold values drop below the configured values. The interfaces are monitored every 15 minutes.
- **Inbound Errors**: Allows you to set thresholds for the number of inbound errors that are discarded after which it generates an alarm.
- **Outbound Errors**: Allows you to set thresholds for the number of outbound errors that are discarded after which it generates an alarm.
- **Inbound Discards**: Allows you to set thresholds for the number of inbound packets that are discarded after which it generates an alarm.
- **Outbound Discards**: Allows you to set thresholds for the number of outbound packets that are discarded after which it generates an alarm.

Default interface health policies

You can create default interface health policies for Hosts, ISLs, and Storage Devices to monitor port utilization. For example, you can create **HostUtilization**, **ISLUtilization**, and **StorageUtilization** policies to monitor the port performance. When the port utilization exceeds the threshold value of 80%, Nexus Dashboard triggers critical alarms and sends alert notifications. You can edit the threshold values for these policies, see Managing alarm policies for more information.

Syslog Alarm Policy

Syslog Alarm Policy defines a pair of Syslog messages formats; one which raises the alarm, and one

which clears the alarm.

Choose the devices for which you want to create policies and then specify these parameters.

- Devices: Define the scope of this policy. Choose individual devices or all devices to apply this policy.
- Policy Name: Specify the name for this policy. It must be unique.
- Description: Specify a brief description for this policy.
- Forwarding: You can forward alarms to registered SNMP listeners in Nexus Dashboard. From Web UI, choose **Admin > System Settings > Fabric Management > Events**.



You must check the **Forwarding** checkbox while configuring alarm policies to ensure alarms are forwarded to an external SNMP listener.

- **Email**: Check the checkbox to forward alarm event emails to recipients when alarm is created, cleared, or severity is changed. From Nexus Dashboard UI, choose **Admin > System Settings > Fabric Management > Events**. Configure the SMTP parameters, click **Save**, and restart Nexus Dashboard services.
- **Severity**: Choose a severity level from the severity drop-down list. The severity options are; Critical, Major, Minor, and Warning.
- **Identifier**: Specify the identifier portions of the raise & clear messages.
- **syslogRaise**: Define the format of a syslog raise message. Use Facility-Severity-Type: Message syntax to define the message format.
- **syslogClear**: Define the format of a syslog clear message. Use Facility-Severity-Type: Message synax to define the message format.

The Regex definitions are simple expressions but not a complete regex. Variable regions of text are noted using $(LABEL) syntax. Each label represents a regex capture group (.+), which corresponds to one or more characters. The variable texts found in both raise and clear messages are used to associate the two messages. An Identifier is a sequence of one or more labels that appear in both messages. An Identifier is used to match a clear syslog message to the syslog message that raised the alarm. If the text appears only in one of the messages, it can be noted with a label and exclude it from the identifier.

Example: A policy with "Value" : "ID1-ID2",

```
"syslogRaise" : "SVC-5-DOWN: $(ID1) module $(ID2) is down $(REASON)"
"syslogClear" : "SVC-5-UP: $(ID1) module $(ID2) is up."
```

In the example, ID1 and ID2 labels can be marked as an identifier to find the alarm. This identifier will be found in corresponding syslog messages. Label "REASON" is in the raise but not in the clear message. This label can be excluded from the identifier, as it has no impact on the syslog message to clear the alarm.

Example 1

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_ADMIN_UP: Interface Ethernet15/1 is admin up.
Clear Regex	ETHPORT-5-IF_DOWN_NONE: Interface Ethernet15/1 is down (Transceiver Absent)

In the above example, the regex expressions are part of the syslog messages that appear in the terminal monitor.

Example 2

Identifier	ID1-ID2
Raise Regex	ETH_PORT_CHANNEL-5-PORT_DOWN: $(ID1): $(ID2) is down
Clear Regex	ETH_PORT_CHANNEL-5-PORT_UP: $(ID1): $(ID2) is up

Example 3:

Identifier	ID1-ID2
Raise Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning
Clear Regex	ETHPORT-5-IF_SFP_WARNING: Interface $(ID1), High Rx Power Warning cleared

SAN Insights Anomaly Policy

You can customize the SAN Insights anomaly policy type to identify issues. You can also create an alarm policy based on the specific flows to retain per interval data for analysis. If the selected flow matches an alarm policy, maintain the flow based on the parameters defined by the policy.

1. Choose **Analyze > Event Analytics > Alarms**.
2. Choose **Alarm Policies** in the **Alarms** tab.
3. Choose **Actions > Create new alarm policy**.
4. Click the **SAN Insights Anomaly Policy** radio button.
5. Enter the necessary field values as described in the following table.

Field	Description
Policy Name	Specify the name for the alarm policy. It must be unique.
Description	Specify a brief description of the alarm policy.
Forwarding	Check this checkbox to enable forwarding of alarms to an external Simple Network Management Protocol (SNMP) listener.
Email	Check this checkbox to send email updates on this alarm policy to an email id.

Field	Description
Capture Time	Click the time in hours from the drop-down list to define **Capture Time**. Specifies the length of time to capture per-interval data for each flow matching the given alarm policy.
Retention Time	Choose the time from the drop-down list to define the **Retention Time**. Specifies the length of time to keep the data before it is deleted.
Analysis Level	Click the interval from the drop-down list to define the **Analysis Level**. Specifies which aggregation of flow data must be checked for the given policy. Policy types such as abort or failures should have logic to catch these failures instantly, so you can select the analysis level as an interval. Some data policy types can be considered as anomaly only when the anomaly is sustained above the threshold value for a specific amount of time. For example, a momentary Exchange Completion Time (ECT) or Data Access Latency (DAL) spike in level is not alarming, but if that same spike level is continued for a period (five minutes or one hour), then it must be investigated.
Severity	Click the severity level from the drop-down list to define the **Severity** of the alarm policy.

Field	Description
Match Rules	Click **Add new rule** to define a new match rule. You need one or more match rules to describe the matching traffic. You can compare any of the telemetry data fields to another field or to a value that you define. Each flow matching all of the match rules generates an alarm (up to the limit defined in **Admin > System Settings > Fabric Management**).  • You can define one or more new rules and match criteria to identify a flow and create a new policy. • All policies are matched against each ITL/ITN flow record streamed to the receiver from the switches.
Compare Source	Click a type of telemetry data for comparison from the drop-down list for matching rules. For example, if you want to check for a read ECT value of a particular host enclosure in a switch, if the ECT value is more than a particular value, create a SAN Insights alarm to monitor the value. You can monitor one particular parameter, and you can create a corresponding alarm if the traffic matches the rule you created.
Operator	Click an operator from the drop-down list for comparing the telemetry data.
Compare To	Click **Custom Value** if you want to compare telemetry data to a custom value that you define.
Compare Value	Enter a comparison value if you clicked **Custom Value**.

6. You can view the created alarms in the **Alarms** tab.
7. Click **Create SAN Insights Anomaly Policy** to create the alarm policy.

Events

This tab displays the events that are generated for the switches. This tab displays information such as Ack, Acknowledged user, Group, Switch, Severity, Facility, Type, Count, Last Seen, and Description. You can select one or more events and then acknowledge or unacknowledge their status using the Change Status drop-down list. In addition, you can select one or more alarms and then click the Delete button to delete them. If you want to delete all events, click the Delete All button.

The following table describes the fields that appear on **Analyze > Event Analytics > Events**.

Field	Description
Group	Specifies the Fabric
Switch	Specifies the hostname of the switch
Severity	Specifies the severity of the event
Facility	Specifies the process that creates the events. The event facility includes two categories: - Nexus Dashboard facility represents events generated by Nexus Dashboard internal services and SNMP traps generated by switches. - Syslog facility represents the machine process that created the syslog messages.
Type	Specifies how the switch/fabric are managed
Count	Specifies the number of times the event has occurred
Creation Time	Specifies the time when the event was created
Last Seen	Specifies the time when the event was run last
Description	Specifies the description provided for the event
Ack	Specifies if the event is acknowledged or not

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Analyze > Event Analytics > Events**.

Action Item	Description
Acknowledge	Select one or more events from the table and choose **Acknowledge** icon to acknowledge the event information for the fabric. After you acknowledge the event for a fabric, the acknowledge icon is displayed in the Ack column next to the Group.
Unacknowledge	Select one or more events from the table and choose **Unacknowledge** icon to acknowledge the event information for the fabric.
Delete	Select an event and choose **Delete** to delete the event.
Add Suppressor	Select an event and choose **Add Suppressor** to add a rule to the event. You can provide name to the rule. Using the **Scope** options, you can add this rule to all the Fabrics, or particular elements or all elements.
Event Setup	Allows you to setup new event. For more information, see Event Setup.

Event Setup

To setup an event using the Cisco Nexus Dashboard UI, perform the following steps:

1. Choose **Analyze > Event Analytics** and click on the **Events** tab.
2. From the **Actions** drop-down list, choose **Event Setup**. The **Receiver** tab displays the following details:
   - **Syslog Receiver enabled**: Displays the status of the syslog server.
   - **SNMP Trap Receiver**: Displays the details of SNMP traps received, processed and dropped.
   - **Syslog Receiver**: Displays the details of syslog messages received, processed and dropped.



- Ensure that you allow access to the SMTP service from the cisco-ndfc-dcnm-syslog-trap interface for forwarding of event email notifications. The cisco-ndfc-dcnm-syslog-trap interface also provides access to the switches for SNMP queries. For more information, see the section "Configuring Persistent IPs" in Nexus Dashboard Infrastructure Management.
- The cisco-ndfc-dcnm-syslog-trap interface also provides access to the switches for SNMP. Ensure that you allow access to the SNMP destination port 161 on the switches for the cisco-ndfc-dcnm-syslog-trap interface. For more information, see the section “Communication Ports” in Cisco Nexus Dashboard and Services Deployment and Upgrade Guide.
- The Nexus Dashboard Fabric Controller cannot forward events as syslogs to a syslog server.
- SMTP servers with Start Transport Layer Security (STARTTLS) are not supported.
- SMTP authentication must be enabled only when the target SMTP server requires SMTP AUTH. If SMTP authentication is enabled for an SMTP server that does not require or support it, event email notifications can fail.

3. Perform the following steps to enable switches to automatically configure syslog and to send syslog messages to the Nexus Dashboard server:
   a. Ensure that Cisco Fabric Services (CFS) is disabled on all the switches.
   b. In Cisco Nexus Dashboard, choose **Admin > System Settings > Fabric Management**.
   c. Click on the **Events** tab and check the **Auto Registration of syslogs on Switch** check box.

      By default, this feature is disabled. You can view the syslog messages in the **Analyze > Event Analytics > Events** page. Nexus Dashboard collects syslog messages from the server every 5 mins.

4. Navigate to the **Sources** tab, to view a list of fabrics and its associated switches. The **Sources** tab displays all the fabrics and the associated switches in tabular format. It also displays if traps and syslogs have been configured on the switches.
5. Perform the following steps to create rules for forwarding email notifications or traps for events:

Cisco Nexus Dashboard Web UI forwards fabric events through email or SNMPv1 or SNMPv2c traps. Some SMTP servers require SMTP authentication parameters, while others do not support or require SMTP AUTH. Enable SMTP authentication in Nexus Dashboard only when the target SMTP server requires it. If SMTP authentication is enabled for a server that does not require or support it, event email notifications can fail.

a. Ensure that you have configured SMTP parameters before configuring rules for forwarding event notifications through emails. To verify SMTP configuration, navigate to **Admin > System Settings > General > Email** and verify that you have configured the required fields.

b. To enable events forwarding, choose **Admin > System Settings > Fabric Management > Events** and configure the fields as described in the following table.

Configure Events Forwarding

Field	Description
Enable Event forwarding	Check the checkbox to enable events forwarding feature.
Email Forwarding From Email List	Specifies the email address from which the forwarding messages arrive.
Snooze Event Forwarding	Snoozes an event from forwarding for the given time range.
Maximum Number of Repeats in Event Forwarding	Stops forwarding an event after the specified time. 0 indicates unlimited time.
Maximum Number in Events/Traps/Syslog Queue	Specifies the maximum number in the queue before dropping the incoming events/traps/syslog.

c. To configure rules, choose **Analyze > Event Analytics**.

d. Navigate to the **Forwarding** tab and choose **Actions > Add Rule** and configure the fields as described in the following table.

Configure Rules

Field	Description
Forwarding Method	Choose one of the forwarding methods: · **E-Mail** · **Trap**
Email Address	This field appears if you choose **E-mail** as the forwarding method. Enter an email address for forwarding the event notifications.
Address	This field appears if you choose **Trap** as the forwarding method. Enter the IP address of the SNMP trap receiver. You can either enter an IPv4 or IPv6 address or a DNS server name.

Field	Description
Port	Enter the port to which the traps are forwarded.
Forwarding Scope	Maximum number in queue before dropping the incoming events/traps/syslog messages.
Fabric	Choose **All Fabrics** or a specific fabric for notification.
VSAN Scope	For SAN Installer, choose the VSAN scope. You can either choose **All** or **List**.
VSAN List	If you chose **List**, provide the list of VSANs for notification.
Source	Choose **DCNM** or **Syslog**. If you chose **DCNM**, do the following: 1. From the **Type** drop-down list, choose an event type. 2. Check the **Storage Ports Only** check box to choose only the storage ports. This check box is enabled only for port related events. If you chose **Syslog**, do the following: 1. In the **Facility** list, choose the syslog facility. 2. In the **Type** field, enter the syslog type. 3. In the **Description Regex** field, enter a description that matches with the event description.

e. From the **Minimum Severity** drop-down list, choose the severity level of the messages to receive.

The traps that are transmitted by Cisco Nexus Dashboard correspond to the severity type. A text description is also provided with the severity type.

```
trap type(s) = 40990 (emergency)
40991 (alert)
40992 (critical)
40993 (error)
40994 (warning)
40995 (notice)
40996 (info)
40997 (debug)
textDescriptionOid = 1, 3, 6, 1, 4, 1, 9, 9, 40999, 1, 1, 3, 0
```

f. Click **Add Rule**.

6. Perform the following steps to create rules for suppressing events:

   Nexus Dashboard allows you to suppress specified events based on user-specified rules. Such events will not be displayed on the Nexus Dashboard Web UI and SAN Client. The events will neither be added to the Nexus Dashboard database, nor forwarded via email or as SNMP traps.

   You can view, add, modify, and delete rules from the table. You can create a rule from the existing events. Choose an existing event as the template and open the **Add Rule** page by navigating to **Analyze > Event Analytics > Events** page, choose the event and choose **Actions > Add Suppresor**. The details are automatically ported from the event you chose in the events table to the fields of the **Add Rule** page.

   a. In the **Name** field, enter a name for the rule.

   b. In the **Scope** field, choose one of the following options - **SAN**, **Port Groups** or **Any**.

      In the **Scope** field, the LAN/SAN groups and the port groups are listed separately. For SAN and LAN, choose the scope of the event at the fabric or group or switch level. You can only choose groups for port group scope. If use choose **Any** as the scope, the suppression rule is applied globally.

   c. In the **Facility** field, enter the name or choose from the SAN/LAN switch event facility list.

      If you do not specify a facility, a wildcard is applied.

   d. In the **Type** field, enter the event type.

      If you do not specify the event type, wildcard is applied.

   e. In the **Description Matching** field, specify a matching string or regular expression.

      The rule matching engine uses regular expression that is supported by Java Pattern class to find a match against an event description text.

   f. Check the **Active Between** check box and choose a valid time range during which the event is suppressed.

      By default, the time range is not enabled.

      

      In general, you must not suppress accounting events. Suppression rule for Accounting events can be created only for certain situations where accounting events are generated by actions of Nexus Dashboard or switch software. For example, 'sync-snmp-password' AAA syslog events are automatically generated during the password synchronization between Nexus Dashboard and managed switches. To suppress accounting events, navigate to **Analyze > Event Analytics > Events** page, choose the event and choose **Actions > Add Suppressor**.

   g. Click **Add Rule**.

Accounting

You can view the accounting information on Cisco Nexus Dashboard Web UI.

The following table describes the fields that appear on **Analyze > Event Analytics > Accounting**.

Field	Description
Source	Specifies the source
User Name	Specifies the user name.
Time	Specifies the time when the event was created
Description	Displays the description.
Group	Specifies the name of the group.

The following table describes the action items, in the **Actions** menu drop-down list, that appear on **Analyze > Event Analytics > Accounting**.

Action Item	Description
Delete	Select a row and choose **Delete** to delete accounting information from the list.

Remote Clusters

This tab displays the clusters and the number of Fabrics in each cluster in your setup.

Click on the Cluster Name to see the summary information. You can click on the launch icon to view the detailed summary of the Cluster.

Copyright

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.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

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/go/trademarks. 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. (1110R)

© 2017-2026 Cisco Systems, Inc. All rights reserved.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

USA
https://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883