

Integrating Cisco Nexus OS EventTracker v7.x

About this Guide

This guide provides instructions to configure Cisco Nexus Operating System (NX-OS) to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, Cisco MDS, Nexus 2000 and later.

Audience

Cisco Nexus Operating System users, who wish to forward syslog messages to EventTracker manager.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

©2013 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Contents

About this Guide	1
Scope	1
Audience	1
Introduction	3
Pre-requisite	3
EventTracker Knowledge Pack (KP)	4
Import Cisco Nexus OS knowledge pack into EventTracker	8
To import Category	8
To import Alerts	8
Verify Cisco Nexus OS knowledge pack in EventTracker	9
Verify Cisco Nexus OS Categories	9
Verify Cisco Nexus OS Alerts	10

Introduction

NX-OS is a network operating system designed by Cisco Systems for their own Nexus-series Ethernet switches and MDS-series Fibre Channel storage area network switches. NX-OS is designed to support high performance, high reliability server access switches used in the data center.

The EventTracker Enterprise supports Cisco Nexus Operating System. It provides an additional level of support by enabling you to generate alerts, reports and run searches on data to improve your ability to manage your Cisco NX-OS activity.

Pre-requisite

- EventTracker 7.x should be installed
- Cisco MDS or Nexus 2000 later should be installed
- Proper access permissions to make configuration changes on the Nexus system.

Enabling Log settings

You must configure logging on the Cisco NX OS appliance, To configure a Cisco Device to send syslog data you will need to use the logging server command through the Cisco's CLI.

1. Login to Cisco Nexus using CLI
2. Type the following command to switch to configuration mode:
config t
3. Type the following commands:
logging server <IP address> <severity>

Where:

<IP address> is the IP address of your EventTracker machine's IP address.

<severity> is the severity level of the event messages, which range from 0-7.

For example,

logging server 200.100.10.1 6 forwards information level (6)
syslog messages to 200.100.10.1.

4. Type the following to configure the interface for sending syslog events:
logging source-interface loopback
5. Type the following command to save your current configuration as the start up configuration:
copy running-config startup-config

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker v7 to support Cisco NX-OS monitoring:

Categories:-

- **Cisco Nexus: ACLMGR commit failed** - This category based report provides information related to ACLMGR commit failed.
- **Cisco Nexus: ACLMGR service initialization failed** - This category based report provides information related to ACLMGR service initialization failed.
- **Cisco Nexus: ACLQOS operation failed** - This category based report provides information related to ACLQOS operation failed.
- **Cisco Nexus: Battery charging failure** - This category based report provides information related to battery charging failure.
- **Cisco Nexus: Boot configuration initialized** - This category based report provides information related to boot configuration initialized.
- **Cisco Nexus: Boot configuration updated** - This category based report provides information related to boot configuration updated.
- **Cisco Nexus: CDP daemon initialization failed** - This category based report provides information related to CDP daemon initialization failed.
- **Cisco Nexus: CDP disabled** - This category based report provides information related to CDP disabled.
- **Cisco Nexus: CDP enabled** - This category based report provides information related to CDP enabled.
- **Cisco Nexus: CFS service created** - This category based report provides information related to CFS service created.
- **Cisco Nexus: CLI library initialization failed** - This category based report provides information related to CLI library initialization failed.
- **Cisco Nexus: Control-plane protected** - This category based report provides information related to control-plane protected.
- **Cisco Nexus: Control-plane unprotected** - This category based report provides information related to control-plane unprotected.
- **Cisco Nexus: CoPP initialization failed** - This category based report provides information related to CoPP initialization failed.
- **Cisco Nexus: CTS SXP socket listen failed** - This category based report provides information related to CTS SXP socket listen failed.
- **Cisco Nexus: Database operation failed** - This category based report provides information related to database operation failed.

- **Cisco Nexus: Database unlock failure** - This category based report provides information related to database unlock failure.
- **Cisco Nexus: Debug infrastructure initialization failed** - This category based report provides information related to debug infrastructure initialization failed.
- **Cisco Nexus: DOT1X authentication failed** - This category based report provides information related to DOT1X authentication failed.
- **Cisco Nexus: Duplicate address detection failed** - This category based report provides information related to duplicate address detection failed.
- **Cisco Nexus: Expired user account deleted** - This category based report provides information related to expired user account deleted.
- **Cisco Nexus: Fan module failed** - This category based report provides information related to fan module failed.
- **Cisco Nexus: FDMI initialization failed** - This category based report provides information related to FDMI initialization failed.
- **Cisco Nexus: FIPS compliance test failed** - This category based report provides information related to FIPS compliance test failed.
- **Cisco Nexus: FIPS crypto-test failure** - This category based report provides information related to FIPS crypto-test failure.
- **Cisco Nexus: FIPS mode initialization failed** - This category based report provides information related to FIPS mode initialization failed.
- **Cisco Nexus: Global port index lookup failed** - This category based report provides information related to global port index lookup failed.
- **Cisco Nexus: Heap memory allocation failed** - This category based report provides information related to heap memory allocation failed.
- **Cisco Nexus: High availability operation failed** - This category based report provides information related to high availability operation failed.
- **Cisco Nexus: Hot standby port down** - This category based report provides information related to hot standby port down.
- **Cisco Nexus: Inband interface lif lookup failed** - This category based report provides information related to inband interface lif lookup failed.
- **Cisco Nexus: Interface database refresh failed** - This category based report provides information related to interface database refresh failed.
- **Cisco Nexus: LDP disabled** - This category based report provides information related to LDP disabled.
- **Cisco Nexus: LDP enabled** - This category based report provides information related to LDP enabled.
- **Cisco Nexus: Memory allocation failed** - This category based report provides information related to memory allocation failed.
- **Cisco Nexus: MTS operation failed** - This category based report provides information related to MTS operation failed.
- **Cisco Nexus: NetFlow feature disabled** - This category based report provides information related to NetFlow feature disabled.

- **Cisco Nexus: NetFlow feature enabled** - This category based report provides information related to NetFlow feature enabled.
- **Cisco Nexus: NVRAM failure** - This category based report provides information related to NVRAM failure.
- **Cisco Nexus: Pong manager disabled** - This category based report provides information related to pong manager disabled.
- **Cisco Nexus: Pong manager enabled** - This category based report provides information related to pong manager enabled.
- **Cisco Nexus: Post-initialization failed** - This category based report provides information related to post-initialization failed.
- **Cisco Nexus: PPF operation failed** - This category based report provides information related to PPF operation failed.
- **Cisco Nexus: PSS infrastructure initialization failed** - This category based report provides information related to PSS infrastructure initialization failed.
- **Cisco Nexus: PSS open failed** - This category based report provides information related to PSS open failed.
- **Cisco Nexus: PSS operation failed** - This category based report provides information related to PSS operation failed.
- **Cisco Nexus: QoS manager initialization failed** - This category based report provides information related to QoS manager initialization failed.
- **Cisco Nexus: RBACL enforcement failed** - This category based report provides information related to RBACL enforcement failed.
- **Cisco Nexus: SAP exchange failed** - This category based report provides information related to SAP exchange failed.
- **Cisco Nexus: Sensor mgr initialization failed** - This category based report provides information related to sensor manager initialization failed.
- **Cisco Nexus: TCAM resource exhausted** - This category based report provides information related to TCAM resource exhausted.
- **Cisco Nexus: Temperature sensor access failed** - This category based report provides information related to temperature sensor access failed.
- **Cisco Nexus: Thread creation failed** - This category based report provides information related to thread creation failed.
- **Cisco Nexus: Timer subsystem initialization failed** - This category based report provides information related to timer subsystem initialization failed.
- **Cisco Nexus: Translation port manager created** - This category based report provides information related to translation port manager created.
- **Cisco Nexus: User password changed** - This category based report provides information related to user password changed.
- **Cisco Nexus: VLAN ID association created** - This category based report provides information related to VLAN ID association created.
- **Cisco Nexus: VLAN ID association deactivated** - This category based report provides information related to VLAN ID association deactivated.

- **Cisco Nexus: VLAN ID association deleted** - This category based report provides information related to VLAN ID association deleted.


Alerts:-

- **Cisco Nexus: ACLMGR commit failed** - This alert is generated when ACLMGR commit failed.
- **Cisco Nexus: Battery charging failure** - This alert is generated when battery charging failure occurs.
- **Cisco Nexus: CDP disabled** - This alert is generated when CDP disabled.
- **Cisco Nexus: CLI library initialization failed** - This alert is generated when CLI library initialization failed.
- **Cisco Nexus: Control-plane unprotected** - This alert is generated when control-plane unprotected.
- **Cisco Nexus: Database operation failed** - This alert is generated when database operation failed.
- **Cisco Nexus: Database unlock failure** - This alert is generated when database unlock failure occurs.
- **Cisco Nexus: DOT1X authentication failed** - This alert is generated when DOT1X authentication failed.
- **Cisco Nexus: Expired user account deleted** - This alert is generated when expired user account deleted.
- **Cisco Nexus: Fan module failed** - This alert is generated when fan module failed.
- **Cisco Nexus: FIPS test failed** - This alert is generated when FIPS test failed.
- **Cisco Nexus: Heap memory allocation failed** - This alert is generated when heap memory allocation failed.
- **Cisco Nexus: License check out failure** - This alert is generated when license check out failure.
- **Cisco Nexus: Not enough free space left** - This alert is generated when not enough free space left.
- **Cisco Nexus: RBACL update failed** - This alert is generated when RBACL update failed.
- **Cisco Nexus: User password changed** - This alert is generated when user password changed.

Import Cisco Nexus OS knowledge pack into EventTracker

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**.
3. Click the **Import** tab.
4. **Import Category/ Alerts** as given below.

To import Category

1. Click **Category** option, and then click the browse  button.
2. Locate the [All Cisco Nexus OS group of categories.iscat](#) file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
EventTracker displays success message.

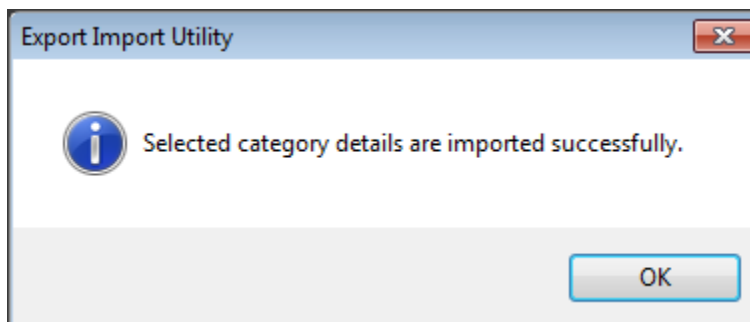



Figure 01

4. Click the **OK** button.
5. Click the **Close** button.

To import Alerts

1. Click **Alert** option, and then click the browse  button.
2. Locate the [All Cisco Nexus OS group of alerts.isalt](#) file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
EventTracker displays success message.

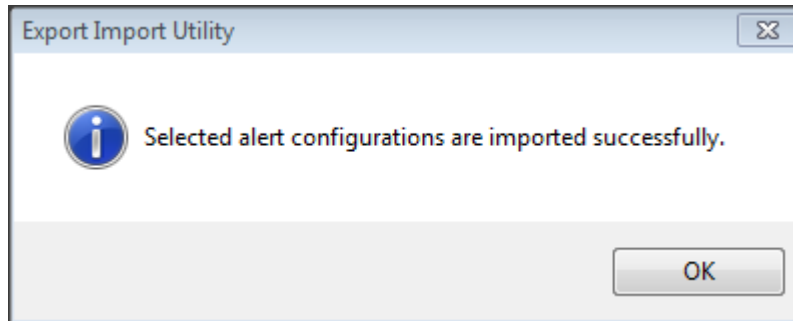


Figure 02

4. Click the **OK** button.
5. Click the **Close** button.

Verify Cisco Nexus OS knowledge pack in EventTracker

Verify Cisco Nexus OS Categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Categories**.
3. In the **Category Tree**, expand **Cisco Nexus OS** group folder to see the imported categories.

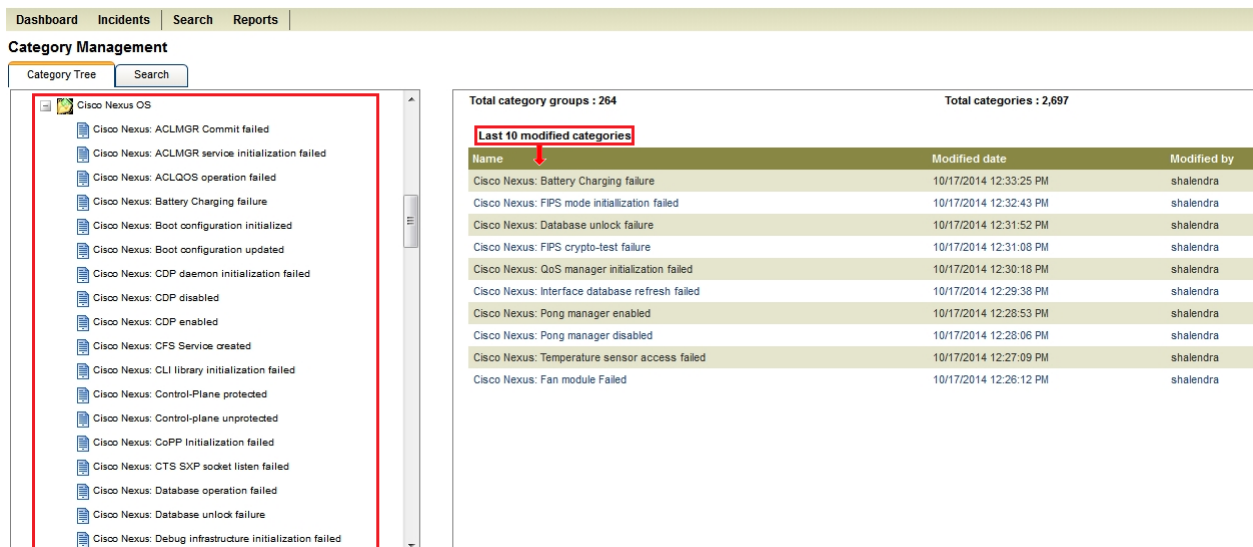


Figure 03

Verify Cisco Nexus OS Alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, type 'Cisco Nexus', and then click the **Go** button.
Alert Management page will display all the imported Cisco Nexus OS alerts.

Alert Name	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
Cisco Nexus: ACL/MGR commit failed	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: Battery charging failure	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: CDP disabled	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: CLI library initialization failed	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: Control-plane unprotected	High	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: Database operation failed	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000 and later
Cisco Nexus: Database unlock failure	Serious	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco MDS, Nexus 2000

***Click 'Activate Now' after making all changes

Figure 04

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

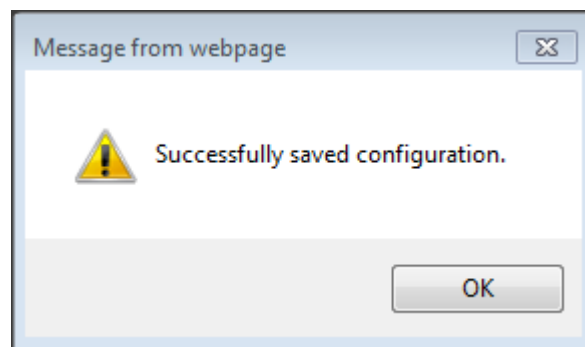


Figure 05

5. Click the **OK** button, and then click the **Activate now** button.
Note: You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.