Integrating Cisco NAC Appliance Clean Access Manager

EventTracker v7.x

Publication Date: April 29, 2013

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Abstract

This guide helps you in configuring **Cisco NAC Appliance - Clean Access Manager**, and EventTracker to receive Cisco NAC Appliance - Clean Access Manager events. You will find the detailed procedures required for monitoring Cisco NAC Appliance.

Intended audience

Administrators who are assigned the task to monitor and manage events using EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise version 7.x**, and **Cisco Network Access Control (NAC) 3300 Series** and later.

Table of Contents

Cisco NAC Appliance - Clean Access Manager

The Cisco Network Admission Control (NAC) Appliance (formerly known as Cisco Clean Access) is a powerful, easy-to-use admission control and compliance enforcement solution. With comprehensive security features, In-Band or Out-of-Band deployment options, user authentication tools, and bandwidth and traffic filtering controls, Cisco NAC Appliance is a complete solution for controlling and securing networks.

Overview

To monitor Cisco NAC Appliance in EventTracker, configure Cisco NAC Appliance to send all events as Syslog to the EventTracker system.

Prerequisites

- EventTracker v7.x should be installed.
- Cisco NAC Appliance should be installed.

Configure Cisco NAC Appliance - Clean Access Manager to forward all the logs to EventTracker

Configure Syslog logging

1. Go to **Monitoring > Event Logs > Syslog Settings.**

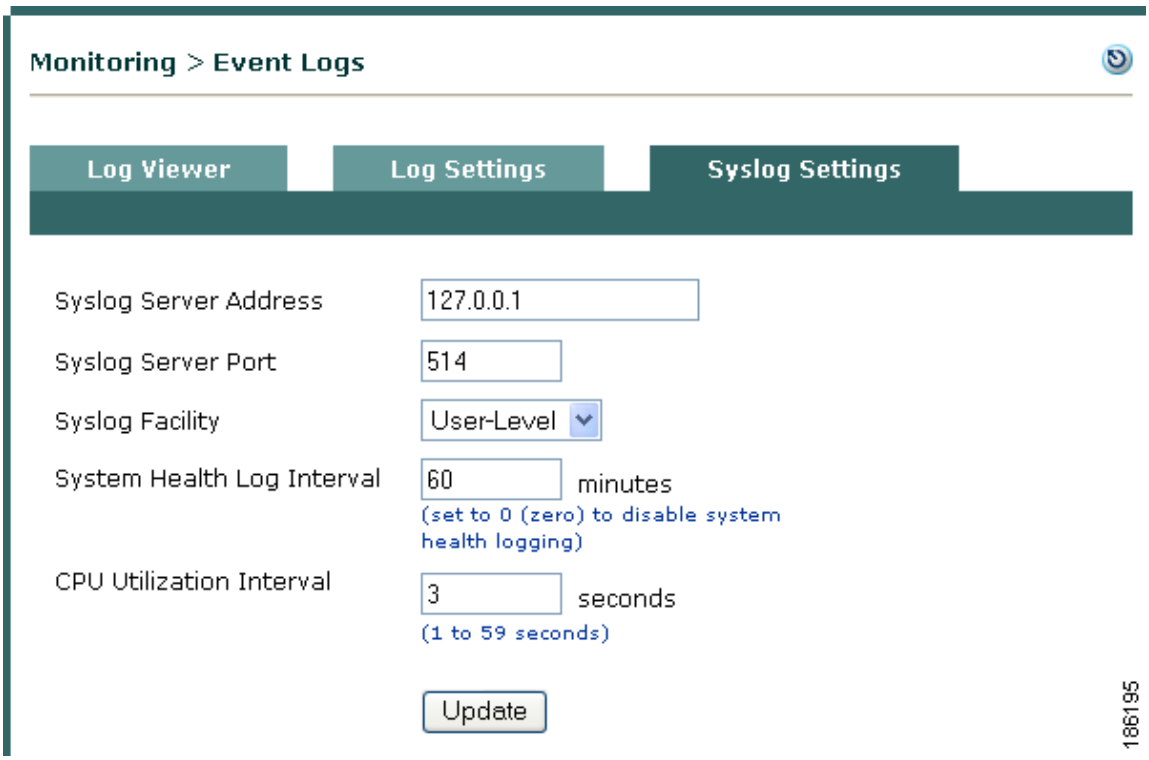

Figure 1

2. In the **Syslog Server Address** field, type the IP address of the Syslog server (default is 127.0.0.1).

3. In the **Syslog Server Port** field, type the port 514 for the Syslog server (default is 514 only).

4. Specify a **Syslog Facility** from the dropdown list.

   This setting enables you to optionally specify a different Syslog facility type for Syslog messages originating from the CAM. You can use the default 'User-Level' facility type, or

you can assign any of the 'local use' Syslog facility types defined in the Syslog RFC ('Local use 0' to 'Local use 7'). This feature gives you the ability to differentiate Cisco NAC Appliance Syslog messages from other 'User-Level' Syslog entries you may already generate and direct to your Syslog server from other network components.

5. In the **System Health Log Interval** field, specify how often you want the CAM to log system status information, in minutes (default is 60 minutes). This setting determines how frequently CAS statistics are logged in the event log.

6. In the **CPU Utilization Interval** field, specify how often, in seconds, you want the CAM to record CPU utilization statistics. You can configure the CAM to record CPU status information up to nearly every minute and the default is every 3 seconds.

7. Click the **Update** button to save your changes.

Import Cisco NAC Appliance - Clean Access Manager Knowledge pack in EventTracker

1. Launch EventTracker Control Panel.
2. Double click on the **Export/Import Utility**. Click the **Import** tab.

   Import Category/Alert as given below.

To import Category

1. Click **Category** option, and then click the **browse** button.
2. Locate all Cisco nac group of categories **.iscat** file, and then click the **Open** button.
3. Click the **Import** button to import the categories.
4. Click **OK**, and then click the **Close** button.

To import Alerts

1. Click **Alert** option, and then click the **browse** button.
2. Locate all Cisco nac group of alerts **.isalt** file, and then click the **Open** button.
3. Click the **Import** button to import the alerts.
4. Click **OK**, and then click **Close** button.

Verify Cisco NAC Appliance - Clean Access ManagerKnowledge pack in EventTracker

Verify Cisco NAC categories

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

Verify Cisco NAC alerts

1. Logon to EventTracker Enterprise.
2. Click the **Admin** dropdown, and then click **Alerts**.
3. In the **Search** field, type 'Cisco nac', and then click the **Go** button.

   Alert Management page will display all the imported Cisco nac alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

   EventTracker displays message box.

Types of Event logs monitored

1. Admin User activity
2. Wired and Wireless user activity
3. System activity
4. Network activity