

Cisco NAC Appliance (Clean Access) 4.x: Configure the Syslog Settings for Events

Document ID: 91899

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Interpreting Event Logs

- View Logs

- Event Log Example

- Limit the Number of Logged Events

- Configure Syslog Logging

- Log Files

Related Information

Introduction

This document describes how to configure the syslog settings in order to log the events to an external server in the Cisco Network Admission Control (NAC) Appliance, formerly known as Cisco Clean Access (CA).

Prerequisites

Requirements

This document assumes the Cisco Clean Access Manager (CAM) and Cisco Clean Access Servers (CAS) are installed and work properly.

Components Used

The information in this document is based on the Cisco NAC Appliance that runs software version 4.0 and later.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

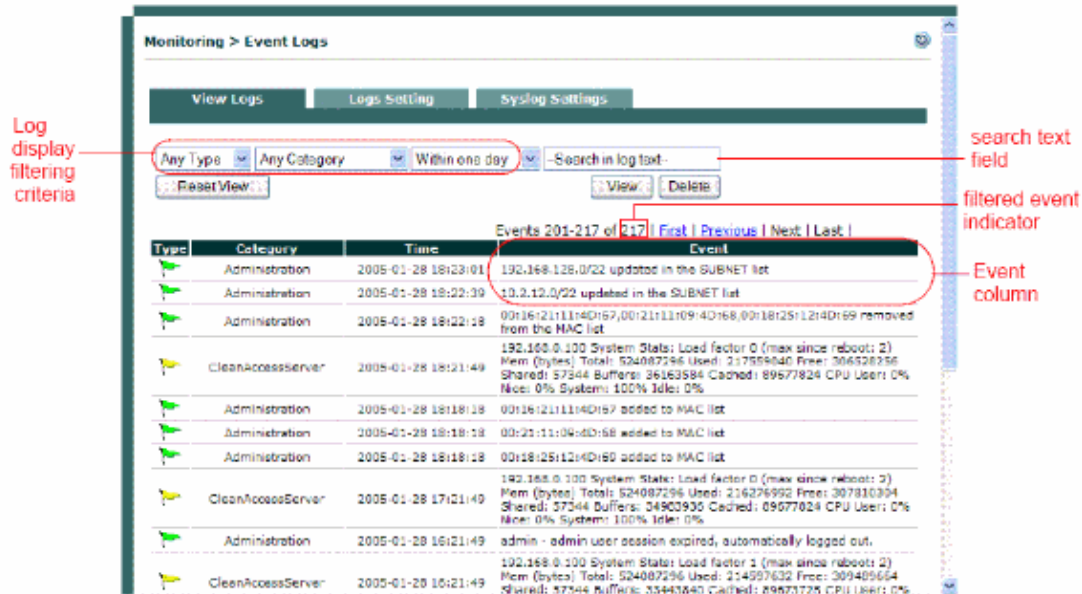
Interpreting Event Logs

Click the **Event Logs** link in the **Monitoring** module in order to view syslog-based event logs in the admin console. There are three Event Logs tabs:

- View Logs
- Logs Settings
- Syslog Settings

View Logs

Figure 1



The View Logs tab includes this information:

- System statistics for Clean Access Servers, which are generated every hour by default.
- User activity, with user logon times, log-off times, failed logon attempts, and more.
- Network configuration events, which include changes to the media access control (MAC) or IP passthrough lists, and addition or removal of Clean Access Servers.
- Switch management events for out-of-band (OOB), which include when linkdown traps are received, and when a port changes to the Auth or Access Virtual LAN (VLAN).
- Changes or updates to the Clean Access checks, rules, and Supported AntiVirus/AntiSpyware Product List.
- Changes to the Clean Access Server Dynamic Host configuration Protocol (DHCP) configuration.

System statistics are generated for each CAS managed by the Clean Access Manager every hour by default. See Configuring Syslog Logging in order to change how often system checks occur.

Note: The most recent events appear first in the Events column.

Table 1 describes the navigation, search capabilities, and actual syslog displayed on View Logs.

Column

Description

Navigation

First/Previous/Next/Last

These navigation links page through the event log. The most recent events appear first in the Events column. The **Last** link shows you the oldest events in the log. A maximum of 25 entries is displayed on a page.

Column

Click a column heading , such as Type or Category, in order to sort the Event log by that column.

Search criteria

Type

Search by these Type column criteria, and then click **View**:

- Any Type
- Failure
- Information
- Success

Category

Search by these Category column criteria, and then click **View**:

- Authentication ¹
- Administration
- Client
- Clean Access Server
- Clean Access
- SW_Management, if OOB is enabled
- Miscellaneous
- DHCP

Time

Search by these Time criteria, and then click **View**:

- Within one hour
- Within one day
- Within two days
- Within one week
- Anytime
- One hour ago
- One day ago
- Two days ago
- One week ago

Search in log text

Type the desired search text and click **View**.

Controls

View

After the desired search criteria is chosen, click **View** in order to display the results.

Reset View




If you click **Reset View**, it restores the default view, in which logs within one day are displayed.

Delete

If you click **Delete**, it removes the events filtered through the search criteria across the number of applicable pages. Delete removes filtered events from Clean Access Manager storage. Otherwise, the event log persists through system shutdown. Use the filter event indicator shown in Figure 1 in order to view the total number of filtered events that are subject to deletion.

Status Display

Type

- Red flag () = Failure indicates an error or otherwise unexpected event
- Green flag () = Success indicates a successful or normal usage event, such as successful login and configuration activity
- Yellow flag () = Information indicates system performance information, such as load information and memory usage

Category

Indicates the module or system component that initiated the log event. For a list, refer to **Category** under the Search criteria section. Note that, by default, system statistics are generated every hour for each Clean Access Server that is managed by the Clean Access Manager.

Time

Displays the date and time (hh:mm:ss) of the event, with the most recent events first in the list.

Event

Displays the event for the module, with the most recent events listed first. See Table 2 – Event Column Fields for an example of a Clean Access Server event.

Footnotes – Table 1

1. Authentication-type entries can include the item Provider: <provider type>, Access point: N/A, Network: N/A. In order to continue to provide support for the end-of-life (EOL) legacy wireless client, if present and pre-configured in the Manager, the Access point: N/A, Network: N/A fields provide access point (AP) MAC and service set identifier (SSID) information respectively for the legacy client.

Event Log Example

Table 2 explains the typical Clean Access Server health event example:

```
CleanAccessServer 2006-04-03 15:07:53 192.168.151.55 System Stats:  
Load factor 0 (max since reboot: 9) Mem Total: 261095424 bytes Used: 246120448  
bytes Free: 14974976 bytes Shared: 212992 bytes Buffers: 53051392 bytes Cached:
```

106442752 bytes CPU User: 0% Nice: 0% System: 97% Idle: 1%

Value

Description

CleanAccessServer

A Clean Access Server reports the event

2006-04-03 15:07:53

Date and time of the event

192.168.151.55

IP address of reporting Clean Access Server

Load factor 0

Load factor indicates the number of packets that wait to be processed by the Clean Access Server, that is, the current load that is handled by the CAS. When the load factor grows, it is an indication that packets wait in the queue to be processed. If the load factor exceeds 500 for any consistent period of time, such as five minutes, this indicates that the Clean Access Server has a steady high load of inbound traffic/packets. Be concerned if this number increases to 500 or higher.

(max since reboot: <n>)

The maximum number of packets in the queue at any one time. In other words, the maximum load handled by the Clean Access Server.

Mem Total: 261095424 bytes

These are the memory usage statistics. There are six numbers shown here:

- total memory
- used memory
- free memory
- shared memory
- buffer memory
- cached memory

Used: 246120448 bytes

Free: 14974976 bytes

Shared: 212992 bytes

Buffers: 53051392 bytes

Cached: 106442752 bytes

CPU User: 0%

These numbers indicate CPU processor load on the hardware, in percentages. These four numbers indicate time spent by the system in user, nice, system, and idle processes.

Note: Time spent by the CPU in system process is typically greater than 90 percent on a Clean Access Server. This indicates a healthy system.

Nice: 0%

System: 97%

Idle: 1%

Limit the Number of Logged Events

The event log threshold is the number of events to be stored in the Clean Access Manager database. The maximum number of log events kept on the CAM, by default, is 100,000. You can specify an event log threshold of up to 200,000 entries to be stored in the CAM database at a time. The event log is a circular log. The oldest entries are overwritten when the log passes the event log threshold.

In order to change the maximum number of events:

1. Click the **Logs Setting** tab in the **Monitoring > Event Logs** pages.
2. Enter the new number in the **Maximum Event Logs** fields.
3. Click **Update**.

Configure Syslog Logging

System statistics are generated every hour, by default, for each Clean Access Server that is managed by the Clean Access Manager. By default, event logs are written to the CAM. You can redirect CAM event logs to another server, such as your own syslog server.

Additionally, you can configure how often you want the CAM to log system status information. In order to do this, set the value in the **Syslog Health Log Interval** field. The default is **60** minutes.

In order to configure Syslog logging:

1. Choose **Monitoring > Event Logs > Syslog Settings**.
2. Enter the IP address of the syslog server in the **Syslog Server Address** field. The default is **127.0.0.1**.
3. Enter the port for the syslog server in the **Syslog Server Port** field. The default is **514**.
4. Enter how often you want the CAM to log system status information, in minutes, in the **System Health Log Interval** field. The default is **60** minutes. This setting determines how frequently CAS statistics are logged in the event log.
5. Click **Update** in order to save your changes.

Note: After you set up your syslog server in the CAM, you can test your configuration. In order to do this, log off and log back into the CAM admin console. This generates a syslog event. If the CAM event is not seen on your syslog server, make sure that the syslog server receives user datagram protocol (UDP) 514 packets and that they are not blocked elsewhere on your network.

Log Files

The Event Log is located in the Clean Access Manager database table and is named log_info table. lists other logs in the Clean Access Manager.

File	Description
<code>/var/log/messages</code>	Startup
<code>/var/log/dhcplog</code>	DHCP relay, DHCP logs
<code>/tmp/perfigo-log0.log.*</code>	Perfigo service logs for 3.5(4) and earlier ¹
<code>/perfigo/logs/perfigo-log0.log.*</code>	Perfigo service logs for 3.5(5) and later ^{1,2}
<code>/perfigo/logs/perfigo-redirect-log0.log.0</code>	Certificate-related CAM/CAS connection errors
<code>/var/nessus/logs/nessusd.messages</code>	Nessus plugin test logs
<code>/perfigo/control/apache/logs/*</code>	Secure sockets Layer (SSL) certificates, Apache error logs
<code>/perfigo/control/tomcat/logs/localhost*.</code>	Tomcat, redirect, JavaServer Pages (JSP) logs
<code>/var/log/ha-log</code>	High availability logs for CAM and CAS

Footnotes – Table 3

1. 0 instead of * shows the most recent log.

2. Switch Management events for notifications received by the CAM from switches are written only to the logs on the file system (`/perfigo/logs/perfigo-log0.log.0`). Furthermore, these events are written to disk only when the log level is set to INFO or finer.

Networking Professionals Connection is a forum for networking professionals to share questions, suggestions, and information about networking solutions, products, and technologies. The featured links are some of the most recent conversations available in this technology.

NetPro Discussion Forums – Featured Conversations for Security
Security: Intrusion Detection [Systems]
Security: AAA
Security: General
Security: Firewalling

Related Information

- [Cisco NAC Appliance Support Page](#)
- [Technical Support & Documentation – Cisco Systems](#)

All contents are Copyright © 2006–2007 Cisco Systems, Inc. All rights reserved. Important Notices and Privacy Statement.

Updated: Jun 11, 2007

Document ID: 91899
