CISCO Nexus Integrations

Overview

The Cisco Nexus integration allows users to monitor Errors and System Messages. The Cisco Nexus series switches are modular and fixed port network switches designed for the data center. All switches in the Nexus range run the modular NX-OS firmware/operating system on the fabric. NX-OS has some high-availability features compared to the well-known Cisco IOS. This platform is optimized for high-density 10 Gigabit Ethernet.

Use the Cisco Nexus integration to collect and parse data from Syslog and log files. Then visualize that data through search, correlation and visualization within Elastic Security.

Data streams

The Cisco Nexus integration collects one type of data: log.

Log consists of errors and system messages. See more details about errors and system messages

Requirements

Elastic Agent must be installed.

The minimum **kibana.version** required is **8.7.0**.

This module has been tested against the **Cisco Nexus Series 9000, 3172T and 3048 Switches**.

Setup

To collect data from Cisco Nexus, follow the below steps:

Logging System Messages to a File

You can configure the device to log system messages to a file. By default, system messages are logged to the file /logflash/log/*logfilename* .

	Command or Action	**Purpose**

Step 1	configure terminal
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[no] logging logfile *logfile-name severity-level* [| size *bytes*] Example: `switch(config)# logging logfile my_log 6`	Configures the nonpersistent log file parameters. *logfile-name* : Configures the name of the log file that is used to store system messages. Default filename is "message". *severity-level* : Configures the minimum severity level to log. A lower number indicates a higher severity level. Default is 5. Range is from 0 through 7: • 0 – emergency • 1 – alert • 2 – critical • 3 – error • 4 – warning • 5 – notification • 6 – informational • 7 – debugging size *bytes* : Optionally specify maximum file size. Range is from 4096 through 4194304 bytes.

Step 3	logging event {link-status | trunk-status} {enable | default}
	Example:
	`switch(config)# logging event link-status default`
		Logs interface events.
		• link-status —Logs all UP/DOWN and CHANGE messages.
		• trunk-status —Logs all TRUNK status messages.
		• enable —Specifies to enable logging to override the port level configuration.
		• default —Specifies that the default logging configuration is used by interfaces that are not explicitly configured.

Configuring Syslog Servers

Note: Cisco recommends that you configure the syslog server to use the management virtual routing and forwarding (VRF) instance. For more information on VRFs, see Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide.

You can configure up to eight syslog servers that reference remote systems where you want to log system messages.

Procedure

	Command or Action	Purpose

Step 1	configure terminal
	Example:
	`switch# configure terminal`
	`switch(config)#`
		Enters global configuration mode.

Step 2	[no] logging server *host* [*severity-level* [use-vrf *vrf-name*]]
	Example:
	`switch(config)# logging server 192.0.2.253`
	Example:
	`switch(config)# logging server 2001::3 5 use-vrf red`
		Configures a syslog server at the specified hostname, IPv4, or IPv6 address. You can specify logging of messages to a particular syslog server in a VRF by using the use-vrf keyword. The use-vrf *vrf-name* keyword identifies the default or management values for the VRF name. The default VRF is the management VRF, by default. However, the show-running command will not list the default VRF.
		Severity levels range from 0 to 7:
		• 0 – emergency
		• 1 – alert
		• 2 – critical
		• 3 – error
		• 4 – warning
		• 5 – notification
		• 6 – informational
		• 7 – debugging
		The default outgoing facility is local7.
		The no option removes the logging server for the specified host.
		The first example forwards all messages on facility local 7. The second example forwards messages with severity level 5 or lower to the specified IPv6 address in VRF red.

Step 3	logging source-interface loopback *virtual-interface* Example: `switch(config)# logging source-interface loopback 5`	Enables a source interface for the remote syslog server. The range for the *virtual-interface* argument is from 0 to 1023.

NOTE:

- Use the Timezone Offset parameter, if the timezone is not present in the log messages.

If you need further assistance, kindly contact our support at support@cytechint.com for prompt assistance and guidance.

Revision #2
Created 3 December 2024 05:25:29 by David Napoleon Romanillos
Updated 3 December 2024 05:38:21 by David Napoleon Romanillos