NetOps
by Broadcom

SOLUTION BRIEF

DX NETOPS BY BROADCOM

Accelerate Triage and Troubleshooting through Contextual Access to Syslog

KEY BENEFITS

- Up to 5x improvement in the mean time to triage by totally automating the retrieval of Syslog data in the context of alarms
- Reduced learning curve for network operators getting direct access to Syslog without leaving DX NetOps Portal
- Leverage the existing investments in popular log management platforms such as Splunk and Elastic to enhance network troubleshooting
- Zero additional license and storage costs for managing Syslog in DX NetOps

Business Challenges

Efficient triaging of issues is paramount to maintaining reliable network operations and minimizing downtime. Syslog plays a pivotal role in this process by providing centralized logging that offers insights into network devices, systems, applications, and security events.

However, despite its importance, gaining access to Syslog data poses significant challenges for Network Operations Center (NOC) teams, introducing delays in identifying the source of issues and ultimately impacting the Mean Time to Resolution (MTTR). This includes:

- **Limited access.** Level 1 operators often lack direct access to log management tools such as Splunk or Elastic, delaying the retrieval of critical Syslog information.
- **Manual handovers.** Manual processes for obtaining and correlating Syslog data introduce errors and increase the risk of losing context during handovers between teams.
- **Context fragmentation.** Level 2 engineers struggle with maintaining a comprehensive view of network issues, as they need to switch between tools for accessing Syslog data, performance metrics, and alarms.

These challenges associated with manual intervention highlight the importance of implementing streamlined and automated processes for accessing and viewing Syslog data within the NOC environment.

Solution Overview

DX NetOps by Broadcom seamlessly integrates with Splunk and Elastic, significantly enhancing NOC efficiency by automating the retrieval of relevant Syslog data in the context of alarms or network devices. This approach enables operators to access Syslog insights alongside performance metrics, flow data, and user experience information, all within the context of network faults, thereby streamlining the troubleshooting process of network issues.

When operators engage in issue triaging through the DX NetOps Portal's alarms view, the integration seamlessly retrieves Syslog data from log management servers based on the alarm's occurrence time. Additionally, optional filtering capabilities are available to refine searches based on specific message patterns. In situations where troubleshooting involves a specific device, the integration efficiently fetches Syslogs for designated timeframes and presents the logs directly on the device's context page.

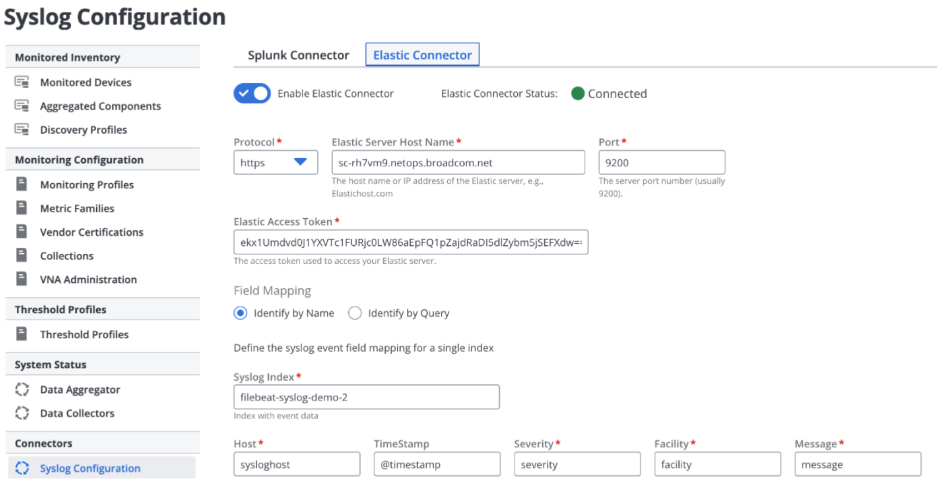
The DX NetOps integration with Splunk and Elastic not only reduces manual efforts but also optimizes time-consuming activities and collaboration within the NOC. As a result, the solution helps expedite issue-triaging processes, facilitating the rapid identification and resolution of network problems. With such streamlined and automated processes, network teams can overcome the challenges associated with poor Syslog access, and improve the reliability of network services.

KEY CAPABILITIES

- Transparent integration with Splunk and Elastic log management solutions
- Single-page display of Syslog data within the context of devices or alarms
- Search and filter across Syslog data for faster triage
- Central configuration for connecting to Splunk and Elastic repositories
- Export relevant Syslog data in CSV and PDF format
- Display and export queries automatically generated for retrieving contextual Syslog data

NetOps
by Broadcom

Central Configuration



Enable Elastic Connector: on
Elastic Connector Status: ● Connected

Protocol*: https
Elastic Server Host Name*: sc-rh7vm9.netops.broadcom.net
The host name or IP address of the Elastic server, e.g., Elastichost.com
Port*: 9200
The server port number (usually 9200).

Elastic Access Token*: ekx1Umdvd0J1YXVTc1FURjc0LW86aEpFQ1pZajdRaDI5dlZybm5jSEFXdw==
The access token used to access your Elastic server.

Field Mapping
● Identify by Name ○ Identify by Query

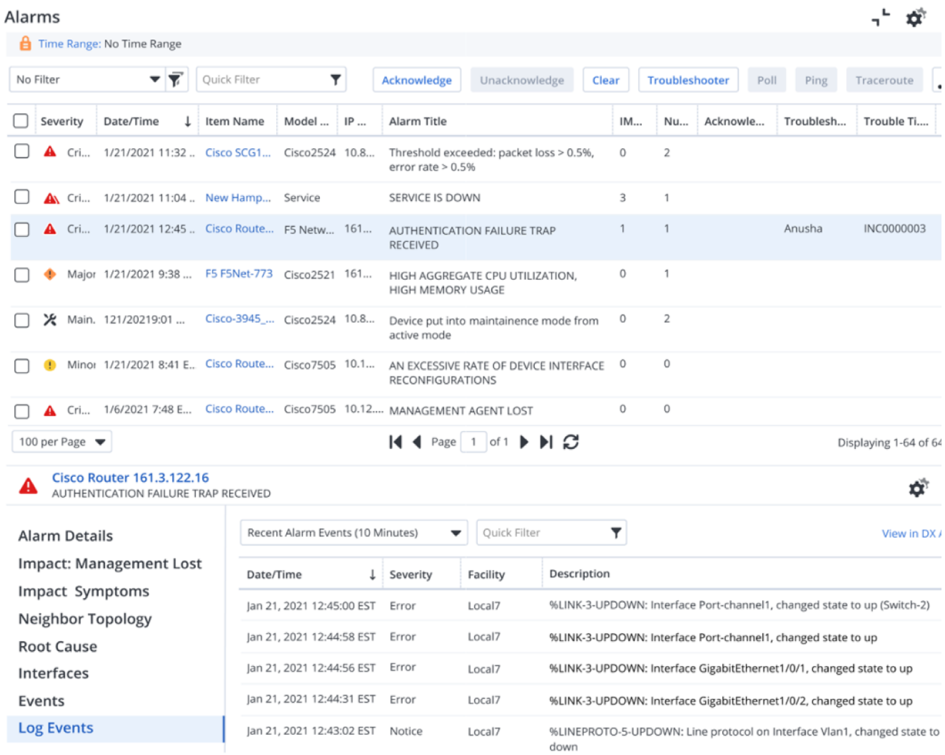
Define the syslog event field mapping for a single index

Syslog Index*: filebeat-syslog-demo-2
Index with event data

Host*	TimeStamp	Severity*	Facility*	Message*
sysloghost	@timestamp	severity	facility	message

DX NetOps uses a central configuration to connect and generate a query for retrieving Syslog data from the log management tools. The integration also allows the acquisition of Syslog data based on specific requirements, such as multiple indexes or source types, using a custom query.

Single-Page Triage



□	Severity	Date/Time	Item Name	Model ...	IP ...	Alarm Title	IM...	Nu...	Acknowle...	Troublesh...	Trouble Ti....
□	Cri...	1/21/2021 11:32 ..	Cisco SCG1...	Cisco2524	10.8...	Threshold exceeded: packet loss > 0.5%, error rate > 0.5%	0	2			
□	Cri...	1/21/2021 11:04 ..	New Hamp...	Service		SERVICE IS DOWN	3	1			
□	Cri...	1/21/2021 12:45 ..	Cisco Route...	F5 Netw...	161...	AUTHENTICATION FAILURE TRAP RECEIVED	1	1		Anusha	INC0000003
□	Major	1/21/2021 9:38 ...	F5 F5Net-773	Cisco2521	161...	HIGH AGGREGATE CPU UTILIZATION, HIGH MEMORY USAGE	0	1			
□	Main.	121/20219:01 ...	Cisco-3945_...	Cisco2524	10.8...	Device put into maintainence mode from active mode	0	2			
□	Minor	1/21/2021 8:41 E..	Cisco Route...	Cisco7505	10.1...	AN EXCESSIVE RATE OF DEVICE INTERFACE RECONFIGURATIONS	0	0			
□	Cri...	1/6/2021 7:48 E...	Cisco Route...	Cisco7505	10.12....	MANAGEMENT AGENT LOST	0	0			

100 per Page | Page 1 of 1 | Displaying 1-64 of 64

Cisco Router 161.3.122.16
AUTHENTICATION FAILURE TRAP RECEIVED

Date/Time	Severity	Facility	Description
Jan 21, 2021 12:45:00 EST	Error	Local7	%LINK-3-UPDOWN: Interface Port-channel1, changed state to up (Switch-2)
Jan 21, 2021 12:44:58 EST	Error	Local7	%LINK-3-UPDOWN: Interface Port-channel1, changed state to up
Jan 21, 2021 12:44:56 EST	Error	Local7	%LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to up
Jan 21, 2021 12:44:31 EST	Error	Local7	%LINK-3-UPDOWN: Interface GigabitEthernet1/0/2, changed state to up
Jan 21, 2021 12:43:02 EST	Notice	Local7	%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down

DX NetOps enables the display of alarms and contextual Syslog data on a single page, offering a comprehensive view of issues while removing the need to constantly switch between tools for triage and troubleshooting activities.

For more information, visit our website at: www.broadcom.com

DX-NetOps-Solutions-Brief_BC-NO-2024_CE-4376_v2b May 13, 2024