Nclose
ADVANCED CYBER SECURITY

LSM – Guide

Procedures around LSMs

Stephen Heger

11/13/2024

Johannesburg
1st floor, Building 1, DQ Office Park
Cnr William Nicol & Leslie Drives
Fourways, Sandton

Cape Town
2nd floor, Old Warehouse Building
Black River Park, 2 Fir Street
Observatory, Cape Town

info@nclose.com
0860 625 673
www.nclose.com

Nclose
ADVANCED CYBER SECURITY

Table of Contents

LSM investigation

Steps to investigate.

A LSM stands for Log Source Missing this occurs when logs have stopped ingesting after a certain time. It will then trigger an operational alert; this will then be investigated by the engineer to confirm if it is 1 of the 3 possible situations. False positive, True Positive, Infrequent log source.

How to analyse a log source and find the needed information.

- Look at observable in the hive.
- Take observable and search in Kibana in the correct client's index and place the observable as such : log_src:"observable" in a time frame of 1 hour.
- If no logs are seen, expand the time frame to 24 hours and keep expanding till the log source is found.
- Once log is found filter the index the log source type example : ClientName_Windows
- Note : Do not search a wide index with a vague observable in a large time frame, that will cause a high resource usage and may cause Kibana to break or slow down.

False positives

A false positive is when a LSM is trigged however the logs are ingesting normally that can be marked as read with a proper reason. Causes for a false positive are the following.

- Logs are ingesting normally after the time frame it fired.
- Lag is causing the LSM alert to trigger.
- Log source was informed to be decommissioned.
- Log source is used from time to time but only for updates.
- The log source is in a pair system so 1 might stop and the other is still ingesting.

True Positives

A true positive is when a LSM is trigged, and no logs are busy ingesting. These are imported and either the client or infrastructure are alerted on. Causes for a true positive are the following.

- Log source has stopped ingesting from the standard rate it's supposed to.
- Log source is ingesting but the name is not unique, so a git needs to be logged.
- A parsing issue was found, and a git will need to be logged with infrastructure after approval.
- Log type turns out to be a scanner that needs to be excluded or fixed on infrastructure side.

Infrequent log source

A monthly infrequent log source (ILS) is a log source that does not ingest often due to a low log count or only ingest if certain conditions are met. These are imported and given the standard LSM – Month, Year, ILS title.
Causes for an ILS are the following.

- Log type will be dormant or not in use, but a scanner picks it up causing it to ingest logs every set number of days.
- Log type ingests a low number of events and causes the time frame of a LSM to fire do to ingesting 1-2 events a day.
- Functionally of the log type for example dark trace only being used when it discovers something malicious
- Log type often appears as LSM however it ingests normally but you want to create a case to keep track of how often it fires.

Additional Notes

Keep the following in mind when doing an LSM.

- If a WEC/WEF stops ingesting, ask deployments team if they can restart it 1st.
- If a firewall stops ingesting, make sure it’s in a High Availability pair and confirm if the other device is not ingesting before any action is taken.
- Confirm if the device was renamed or confirmed in previous cases.
- Not all DNS servers are going to have a windows server with them.
- Check Zabbix for ports of a log type for remediating
- Check Zabbix to confirm if a client is lagging before sending alerts.
- Ask deployments team after a client has done basic remediation steps for follow up process if logs are still not ingesting.
- Ask deployments team if you are uncertain about a log source or action.
- Do not mark as read without being 100% certain of the reason.
- If a large amount of LSM’s triggerd for a client regarding a specific log source confirm with deployments team.

Log types and how they ingest

Windows.

Windows will be ingested into an MDR server in the following 2 methods.

- Winlogbeat is used when the server is sending logs directly to the MDR server.

- WinRM, this is used when logs are going to another device called a WEF(windows event forwarder). The WEF will then transport logs gathered from the windows server to the Nview server.

To identify how we observe if the server is using Winlogbeat or WinRM we would need to check in Kibana and review the log source named field and match it with the agent or beat name field. Examples of the 2 are below,

Winlogbeat is in use due to log_src and beat.name are matching.

Time	log_src	beat.name	tags
Dec 1, 2023 @ 13:09:56.962	DR-INT-DC01.intembeko.com	DR-INT-DC01	windows
Dec 1, 2023 @ 13:09:56.945	DR-INT-DC01.intembeko.com	DR-INT-DC01	windows
Dec 1, 2023 @ 13:09:55.944	DR-INT-DC01.intembeko.com	DR-INT-DC01	windows
Dec 1, 2023 @ 13:09:51.936	DR-INT-DC01.intembeko.com	DR-INT-DC01	windows

WinRM is in use due to log_src and angent.name not matching.

Time	log_src	agent.name	tags
Dec 1, 2023 @ 13:05:32.670	MXHQPRDMPDC04.bayportfinance.com	ZADCPRDMNVS01	windows
Dec 1, 2023 @ 13:05:30.237	MXHQPRDMPDC04.bayportfinance.com	ZADCPRDMNVS01	windows
Dec 1, 2023 @ 13:05:28.611	MXHQPRDMPDC04.bayportfinance.com	ZADCPRDMNVS01	windows
Dec 1, 2023 @ 13:05:27.591	MXHQPRDMPDC04.bayportfinance.com	ZADCPRDMNVS01	windows
Dec 1, 2023 @ 13:05:27.374	MXHQPRDMPDC04.bayportfinance.com	ZADCPRDMNVS01	windows

The basic remediation for Winlogbeat is the following.

- Please ensure that the server is online and the Winlogbeat service is running, restart the services if possible.
- Please start the service if it is not running.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

The basic remediation for WinRM is the following.

- Please ensure that the WinRM service is running on this host. Start the service if stopped.
- Please restart the service if it is currently running.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

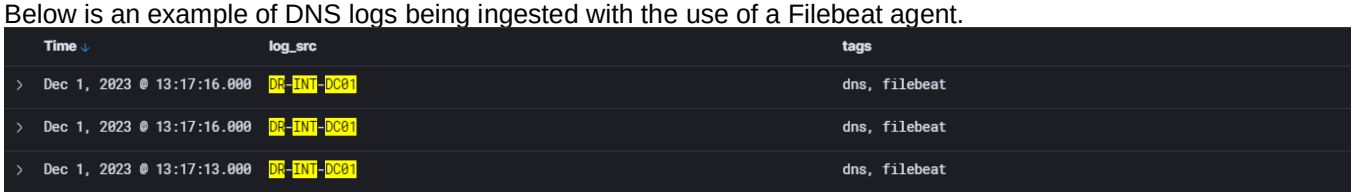
DNS

DNS logs will be ingested into an Nview server in the following method.

- Filebeat is used when the server is sending logs directly to the Nview server.

DNS servers are normally associated to a windows server check to confirm both log types are ingesting however, there are exceptions where windows won't be ingesting.

Below is an example of DNS logs being ingested with the use of a Filebeat agent.



The basic remediation for Filebeat is the following.

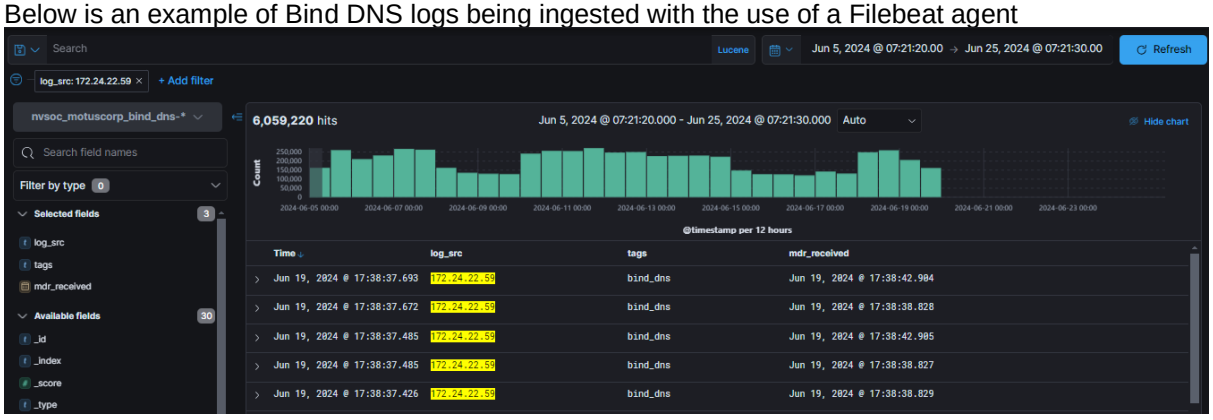
- Please confirm whether the Filebeat Service is running on the host. If already running, please restart the service if possible.
- If the Filebeat Service is stopped on the host, please start the service.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

Bind DNS

Bind DNS logs will be ingested into an Nview server in the following method.

- Unlike DNS which is associated with the windows server. Bind DNS uses a Linux server that's configured to send syslogs directly to the Nview server

Below is an example of Bind DNS logs being ingested with the use of a Filebeat agent



The basic remediation is the following:

- Please ensure that device is currently switched on and the syslog service is running.
- Please ensure that the device is configured to send syslog to the Nview server (**Nview server IP**) over port (**Port client uses**).
- The config file should reside in the below location which then you can check if the syslog is configured, and the services should be running.

“/etc/bind/named.conf”

“/etc/rsyslog.conf”

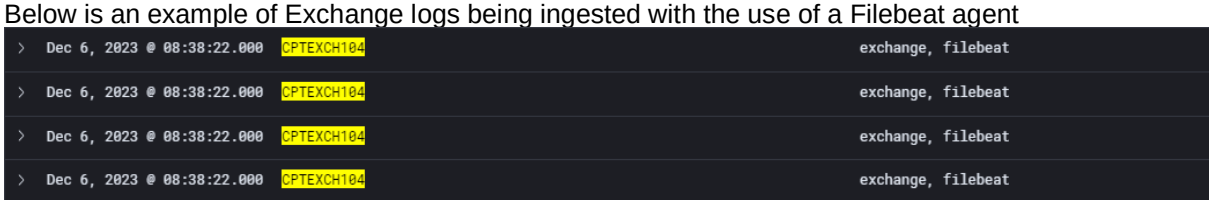
Exchange

Exchange logs will be ingested into an Nview server in the following method.

- Filebeat is used when the server is sending logs directly to the Nview server

Exchange servers are normally straightforward and do not impact other log sources.

Below is an example of Exchange logs being ingested with the use of a Filebeat agent



The basic remediation for Filebeat is the following.

- Please confirm whether the Filebeat Service is running on the host. If already running, please restart the service if possible.
- If the Filebeat Service is stopped on the host, please start the service.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

Sysmon

Sysmon will be ingested into a Nview server in the following 2 methods.

- Sysmon service + Winlogbeat is used, and this is when Sysmon logs are sent directly to the Nview Server and these are non-Domain joined.

- Sysmon service + WinRM is used, this is used when logs are going to another device called a WEF(windows event forwarder). The WEF will then transport logs gathered from the Sysmon server to the Nview server these are Domain joined servers.

To identify which method the the Sysmon is ingesting we must observe if the server is using Winlogbeat or WinRM we would need to check in Kibana and review the log source named field and match it with the agent or beat name field. Examples of the 2 ways it ingests are below,

Winlogbeat is in use with the Sysmon service due to the log_src name and beat.name matching.

Time	log_src	beat.name	tags
Dec 1, 2023 @ 13:43:18.522	INT-AXWAY-UAT	INT-AXWAY-UAT	sysmon
Dec 1, 2023 @ 13:42:18.399	INT-AXWAY-UAT	INT-AXWAY-UAT	sysmon
Dec 1, 2023 @ 13:41:48.319	INT-AXWAY-UAT	INT-AXWAY-UAT	sysmon
Dec 1, 2023 @ 13:41:18.236	INT-AXWAY-UAT	INT-AXWAY-UAT	sysmon

WinRM is in use with the Sysmon service due to the log_src name and agent.name not matching.

The basic remediation for Sysmon + Winlogbeat is the following .

- Please ensure that the Winlogbeat and Sysmon service is running on this host. Start the service if stopped.
- Please restart the service if it is currently running.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

The basic remediation for Sysmon + WinRM is the following.

- Please ensure that the Sysmon and WinRM service are started on these hosts.
- If the above service are already running, please restart it on the respective hosts if possible.
- If possible, automate the restarting of the service upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

Firewall

Firewall logs will be ingested into a Nview server in the following 2 methods

- Firewall is set to send logs straight to Nview server this will include port number + Nview node IP
- Firewall is set to send logs to Firewall collector which will send to the Nview server with the port number + Nview node IP.

To identify which method the Firewall is ingesting we must observe if the firewall sends directly to the Nview server or if it is configured to send to a firewall collector and then the collector being sent to the Nview server. To confirm this, we would need to check Kibana and observe if the log_src matches the device field.
Examples of the 2 ways it ingests are below.

Firewall logs are being sent directly to the Nview server observed by the **log_src** and **Device** fields matching.

Time	log_src	Device	tags
Dec 1, 2023 @ 14:44:22.000	Adams_PA-850	Adams_PA-850	paloalto
Dec 1, 2023 @ 14:44:22.000	Adams_PA-850	Adams_PA-850	paloalto
Dec 1, 2023 @ 14:44:22.000	Adams_PA-850	Adams_PA-850	paloalto
Dec 1, 2023 @ 14:44:22.000	Adams_PA-850	Adams_PA-850	paloalto

Firewall logs are being sent to the Firewall collection and then forwarded to the Nview server observed by the **log_src** and **Device** fields not matching.

Time	log_src	Device	tags
Dec 1, 2023 @ 14:40:56.000	DXB25-FW02A	DXB01-B2-Panorama-01.me.hcnet.biz	paloalto
Dec 1, 2023 @ 14:40:56.000	DXB25-FW02A	DXB01-B2-Panorama-01.me.hcnet.biz	paloalto
Dec 1, 2023 @ 14:40:56.000	DXB25-FW02A	DXB01-B2-Panorama-01.me.hcnet.biz	paloalto
Dec 1, 2023 @ 14:40:56.000	DXB25-FW02A	DXB01-B2-Panorama-01.me.hcnet.biz	paloalto

The basic remediation for firewall logs being sent to Nview server is the following.

- Ensure that your event logging on your (**Firewall name**) device is set to send events through syslog to the NView server (**Nview Server IP**) via port (**Port client uses**)

The basic remediation for firewall logs being sent to the Firewall collector to Nview server.

- Ensure that the Firewall is switched on.
- Please confirm if the **(Firewall name eg PaloAlto)** Firewall is configured to send syslog to the **(collector type**) through port **XXXX**(Port client uses)+(Name of the Firewall collector).

API

API will ingest into an Nview server in the following method.

API refers to “Application Programming Interface” this is used when the log source can’t forward logs to the Nview server without the help of an API. API is a folder we set up in the client environment that will pull the required information from the log source with requirements set in the API folder. Examples of this are

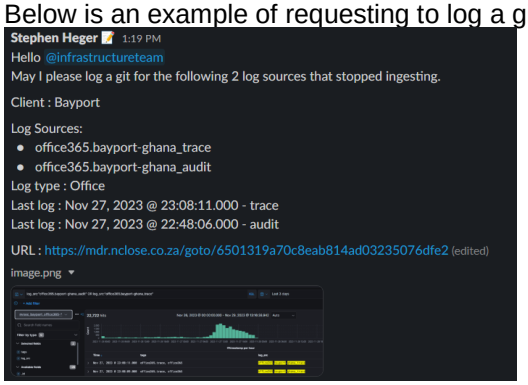
- **Office365,**
- **Mimecast,**
- **Crowdstrike,**
- **vSphere,**
- **Cloudtrail,**
- **Darktrace,**
- **Cyberark**.
- **Netskope**

Should there not be ILS, these are normally escalated to infrastructure in the slack channel and tagging the infrastructure team with all relevant information and confirmation for a git will be required. There are cases where we need to contact the client of the missing log source, however this will be confirmed with infrastructure and the request of what needs to be done.

When posting in infrastructure basic details on the log are needed, which include.
Client :

- Log Source
- Log Type
- Last log
- Kibana URL
- Snapshot :

Below is an example of requesting to log a git.



WEB

Web logs are sent to the Nview server with the Microsoft IIS feature enabled with the Filebeat service. These are normally sent directly to the Nview server.

Below is an example of web log being sent to the Nview server with the use of a Filebeat agent.

Time	log_src	agent.type	tags
Dec 1, 2023 @ 15:14:53.000	ITTAWeb01	filebeat	web, filebeat
Dec 1, 2023 @ 15:14:44.000	ITTAWeb01	filebeat	web, filebeat
Dec 1, 2023 @ 15:14:35.000	ITTAWeb01	filebeat	web, filebeat
Dec 1, 2023 @ 15:14:32.000	ITTAWeb01	filebeat	web, filebeat

The basic remediation for WEB logs being sent to Nview server is the following.

- Please ensure that the that the Microsoft IIS feature is enabled and the Filebeat services are running, restart the services if possible.
- If possible, automate the restarting of the services upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.
- Please confirm if the host is configured to send logs to the Nview server (**IP**) over port (**Client's port)**

DXL

So DXL is used to ingest macfee and trellix logs. This is sent to the epos box on Ncloses side before being sent to the Nview Server. There are 2 sets of DXL services dxlcompliance and dxlthreatevents. Normal response engineers can not confirm what epos box it which are Macaffee and Trellix

Below is an example of a DXL threatserver being sent to the epos on the macfee box

The basic remediation for the DXL logs are the following.

- Check the getting to know our client documentation to see who is the engineer handling DXL for the client.
- Reach out and inform the engineer if it stopped ingesting with the standard information.
- There are 2 sets of DXL Epos boxs which is used to ingest macfee or trellix, this will be confirmed with the engineer handling DXL logs.
- Ask the engineer to restart the Epos box to start ingesting logs.

If the logs do not ingest after the restart.

- Informing the engineer and ask them for the next steps we can take to help.

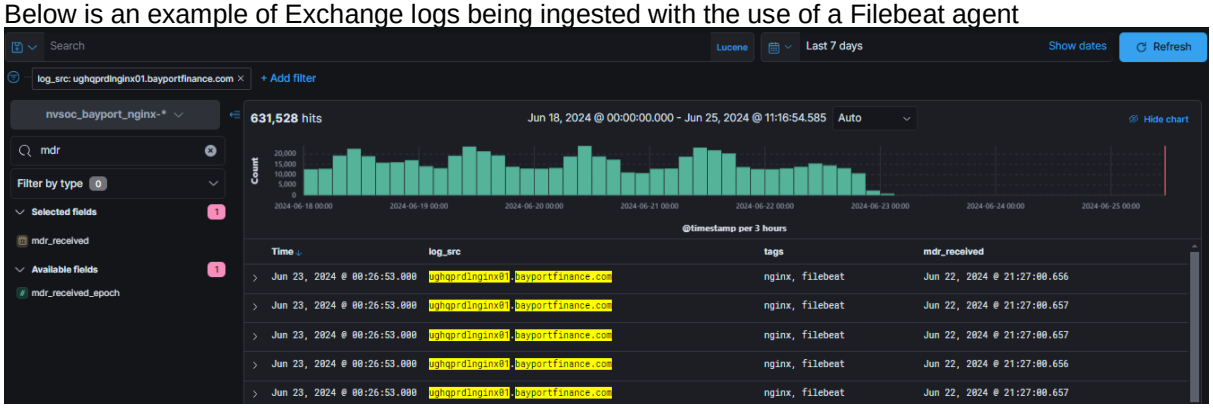
Ngnix

Ngnix logs will be ingested into an Nview server in the following method.

- Filebeat is used when the server is sending logs directly to the Nview server

Ngnix servers are Linux hosts and normally straightforward and do not impact other log sources

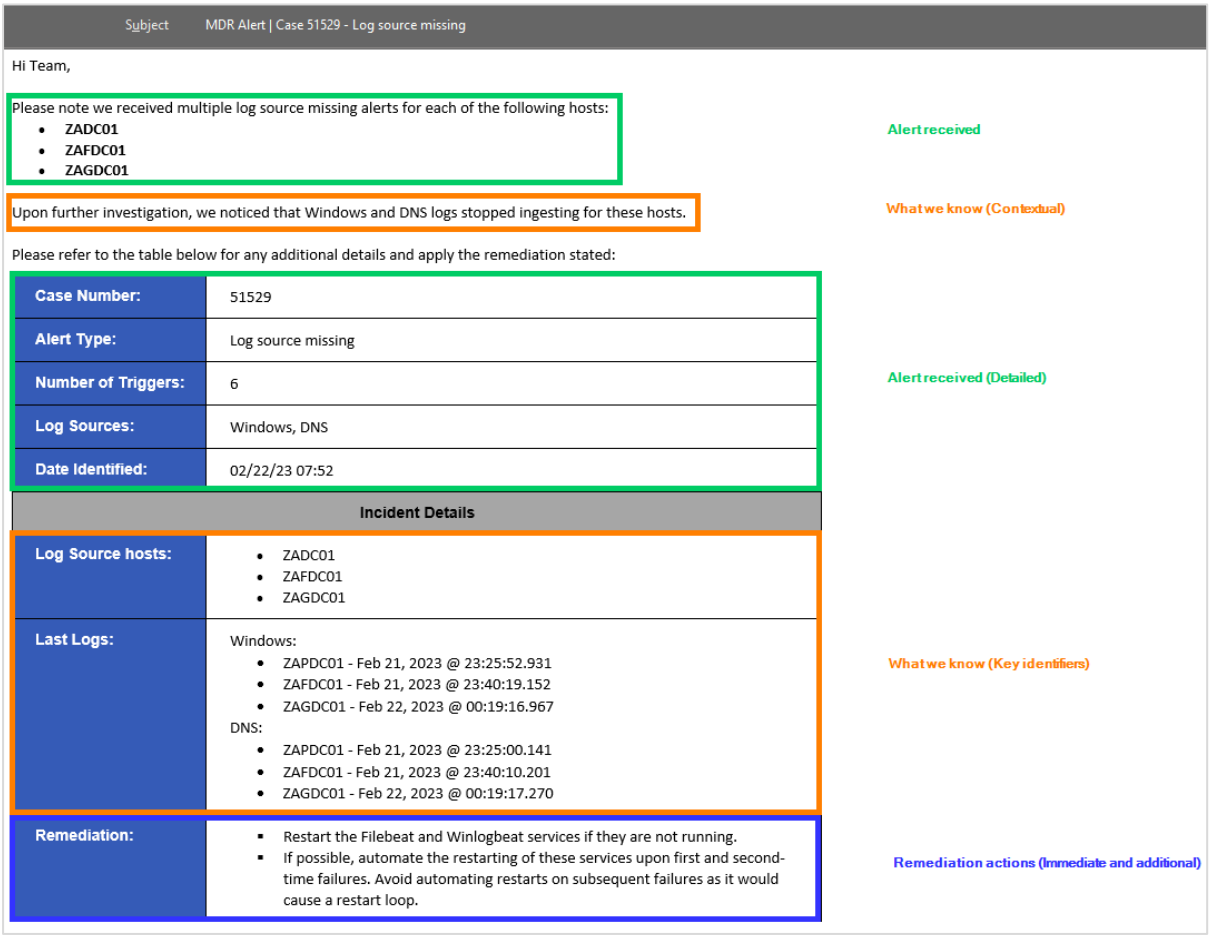
Below is an example of Exchange logs being ingested with the use of a Filebeat agent



The basic remediation for the Ngnix logs are the following.

- Please confirm whether the Filebeat Services are running on the hosts. If already running, please restart the services if possible.
- Please confirm that the latest date stamp on the log file in this location **/var/log/nginx/*.log.**
- If the Filebeat Services have stopped on the hosts, please start the services.
- If possible, automate the restarting of the services upon first- and second-time failures. Please avoid automating restarts on subsequent failures as it would cause a restart loop.

Log Source Missing alert example.



Subject MDR Alert | Case 51529 - Log source missing

Hi Team,

Please note we received multiple log source missing alerts for each of the following hosts:

- **ZADC01**
- **ZAFDC01**
- **ZAGDC01**

Alert received

Upon further investigation, we noticed that Windows and DNS logs stopped ingesting for these hosts.

What we know (Contexdual)

Please refer to the table below for any additional details and apply the remediation stated:

Case Number:	51529
Alert Type:	Log source missing
Number of Triggers:	6
Log Sources:	Windows, DNS
Date Identified:	02/22/23 07:52

Alert received (Detailed)

Incident Details	
Log Source hosts:	• ZADC01 • ZAFDC01 • ZAGDC01
Last Logs:	Windows: • ZAPDC01 - Feb 21, 2023 @ 23:25:52.931 • ZAFDC01 - Feb 21, 2023 @ 23:40:19.152 • ZAGDC01 - Feb 22, 2023 @ 00:19:16.967 DNS: • ZAPDC01 - Feb 21, 2023 @ 23:25:00.141 • ZAFDC01 - Feb 21, 2023 @ 23:40:10.201 • ZAGDC01 - Feb 22, 2023 @ 00:19:17.270
Remediation:	▪ Restart the Filebeat and Winlogbeat services if they are not running. ▪ If possible, automate the restarting of these services upon first and second-time failures. Avoid automating restarts on subsequent failures as it would cause a restart loop.

What we know (Key identifiers)

Remediation actions (Immediate and additional)

Log Source Missing alert layout - detailed.

Section:	Details:
Subject:	MDR Alert | Case # - Log Source Missing
Body:	Alert received. What we know (Based on facts, provides key identifiers)
Table:	• Case number • Alert received • Number of triggers • Date triggered • Log source • Log source name/host • Last logs • Remediation actions

Log Source Follow Up’s

This is a general rule for doing a case follow up.

- After 3 days a follow, up will be made to a client if the log source has still not ingested.
- If you have made more then 2 follow ups and a client has not responded back escalate to a senior for advice
- If it is multiple log sources or an entire index field, you will follow up daily.
- When following up you will include the following.
    - Log Source.
    - Last log ingested.
    - Any additional information
    - Remediation.

Documentation

Kibana URL :
Log source :
Log type :
Last log :

Details: The details will include if the log is infrequent but being monitored or if the logs have stopped ingesting and a git was logged.

If the logs have stopped ingesting
You will confirm and write the action taken and why.

Examples are :
Client was notified do to logs stopped ingesting
Client was not notified for investigation is occurring on log source.
A GIT request was logged + adding the GIT number.

Note: When closing a case out besides it being decommissioned make sure logs are ingesting.

Thank you

Johannesburg
1st floor, Building 1, DQ Office Park
Cnr William Nicol & Leslie Drives
Fourways, Sandton

Cape Town
2nd floor, Old Warehouse Building
Black River Park, 2 Fir Street
Observatory, Cape Town

info@nclose.com
0860 625 673
www.nclose.com