1 Table of Contents

1.1 Revision History

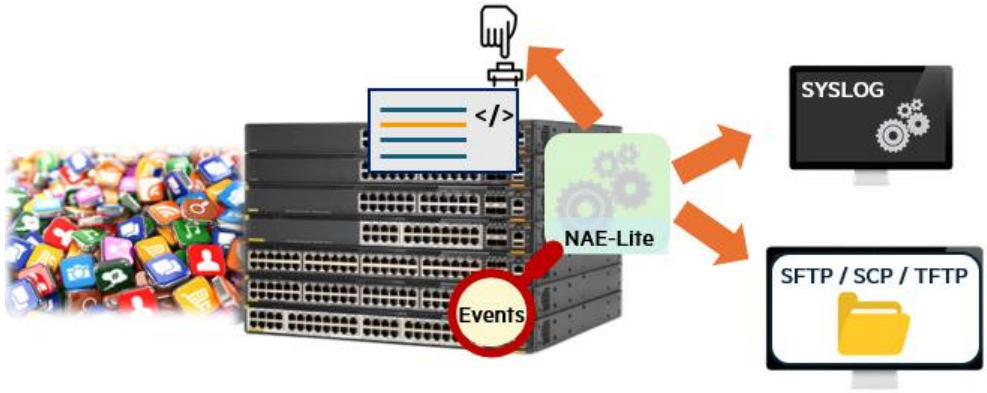
DATE	VERSION	EDITOR	CHANGES
19 Mar 2025	0.1	Ariya Parsamanesh	Initial creation
06 Apr 2025	0.2	Ariya Parsamanesh	Added the second use case
22 Apr 2025	0.3	Ariya Parsamanesh	Added the Aruba Central section

2 Aruba CX Switch Automation with Network Analytics Engine Lite

In this technote we will explore simple automation with CX switches that do not require any knowledge of scripting. You might know about Network Analytics Engine (NAE) which is part of most of the CX switches. NAE is a unique built-in analytics framework that is used for network assurance and remediation. The NAE agents are provided by HPE Aruba and are basically python scripts with the aim of monitoring switch resources and protocol state.

We will be using NAE Lite, a command-line interface (CLI) based framework. Our goal is to define the event you want to monitor, specify the conditions for this event, and outline the actions to be taken when these conditions are met. This feature does not require any licenses or additional software/collectors, and it can be used without any knowledge of programming languages like Python.

You can use these NAE Lite agents to monitor availability, security and troubleshooting events.



NAE Lite is very flexible and you can use it to monitor the CPU and memory usage of the CX switch. You can also check for system daemon crash events and gather additional debugging outputs.

You can use it to check the availability of authentication server, frequent mac address moves, spanning tree changes, BGP and OSPF state changes, VSX and VSF changes, etc. Basically, you can monitor anything that there is an event/syslog for which is almost all the processes.

This is also applicable to VSX based switches as well like 8XXX, 64XX and 542X CX series switches.

2.1 Things you need

We need the following.

- 2x CX switch, here I am using CX 6200 switch running 10.15.1010 (minimum version CX10.10.x)
- SYSLOG server
- Optional TFTP server

3 NAE Lite Use Cases

Aruba CX switches support over 7000 event IDs that can be monitored. All the events are documented in the Event Log Message Reference Guide which can be downloaded from HPE Networking Support Portal. I am using the event log reference guide for AOS-CX 10.15.

To start with, NAE lite has the following three parts.

1. Events you want to monitor.
2. Some conditions that should be met.
3. Action to be performed when those conditions are met.

You can configure NAE Lite agents to watch any of the events that are listed in Event Log Message Reference Guide and here are some of the interesting events.

- Radius-server (any server) that is not reachable.
- IPSLA, icmp-echo and https-server.
- Static route that is deleted.
- Interface flaps.
- Routing state changes .
- Spanning tree events and topology changes.

And the supported actions for a given condition are (refer to the user guide for the examples)

- Generate and send SYSLOG message to a SYSLOG server.
    - You can customise the facility and severity of the SYSLOG message.
- Execute multiple CLI commands.
- Redirect the output of the CLI commands to TFTP server or to a local file on the flash.
- Generate custom SNMP trap and send it to the SNMP server.
- Execute a configured job CLI commands at the specific time. (schedule jobs)

Note that I am using 6200 switch which supports a maximum of 10 NAE or NAE-Lite agents. You can use the HPE Aruba Networking Switch Feature Navigator to check the maximum supported agents for your switch model.

3.1 LACP Monitoring Use Case

In this use case, we'll check the state change for interface that is part of a LACP LAG. The "Event Log message reference guide" has a section for LACP. It lists all the possible LACP events that are generated. Here I'll be using Event ID: 1321 that is generated when there is a change in the LACP state.

The following screenshot is directly from the guide.

Event ID: 1321

Message	LAG <*lag_id*> State change for interface <*intf_id*>: Actor state: <*actor_state*>, Partner state <*partner_state*>
Category	LACP
Severity	Information
Description	Logs that capture changes to LACP state for LAG interface.

Before we start creating our NAE-lite agent we need to see the generated event 1321 message to give us a better idea. I have configured the switch to send SYSLOG messages to my SYSLOG server.

The following 3x events were generated when I connected the LACP interfaces to another CX switch.

```
2025-03-31T08:45:06.606172+11:00 6200-Core lacpd 3237 - - Event|1321|LOG_INFO|CDTR|1|LAG 256 State change for interface 1/1/14: Actor state: ALFNC, Partner state ALFNC
2025-03-31T08:45:06.623688+11:00 6200-Core lacpd 3237 - - Event|1321|LOG_INFO|CDTR|1|LAG 256 State change for interface 1/1/14: Actor state: ALFNCD, Partner state ALFNC
2025-03-31T08:45:06.635825+11:00 6200-Core lacpd 3237 - - Event|1321|LOG_INFO|CDTR|1|LAG 256 State change for interface 1/1/14: Actor state: ALFNCD, Partner state ALFNCD
```

Here when we see ALFNCD it means that one of the LACP interfaces is up. The event also mentions the “Actor state” and “Partner state”. We’ll make use of those as well. And finally, if the flag is ALFO, then one of the LACP interfaces is down.

Below is my configuration and my SYSLOG server is 192.168.1.100

```
nae-agent lite lacp_interface_watch_agent
  watch lacp_DOWN event-log 1321
  watch lacp_UP event-log 1321
  set-condition watch event-log lacp_DOWN include any "Actor state: ALFO","Partner
state ALFO"
     status critical
     syslog "LACP Interface is down"
     cli show lacp interfaces
     clear-condition watch event-log lacp_UP include all "Actor state:
ALFNCD","Partner state ALFNCD"
          syslog "LACP Interface is up"
          cli show interface lag256 brief\n show lacp interfaces
!
nae-agent lite lacp_interface_watch_agent activate
!
Loggin 192.168.1.100
!
```

Here is the description of this NAE-lite agent and what it is configured to do

- The agent has two watchers “lacp-DOWN” and “lacp-UP” both watching the same SYSLOG event 1321 that indicates a change in LACP status.
- Next, we’ll configure the conditions to indicate when a LACP interface is down. This is done by matching the event content with any of these two texts "Actor state: ALFO", "Partner state ALFO".
- If that condition is met, then we sent a critical syslog message saying “LACP Interface is down" and run a CLI command “sh lacp interfaces”.
- We then check if there is another event 1321 message but this time with two conditions that both should be met, "Actor state: ALFNCD" and "Partner state ALFNCD". This indicates that the previous interface that was down is now back up. And that’s our clear-condition.
- We then run two CLI commands.
- And finally, we will activate the NAE-lite agent.

3.1.1 Testing

As always, we need to establish a baseline before we start the testing. The current status of the LACP interfaces is shown below.

```
6200Core(config)# sh lacp int

State abbreviations :
A - Active        P - Passive       F - Aggregable I - Individual
```

```
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/1/13     lag256     14    1     ALFNCD  94:60:d5:da:5a:20 65534  256  up
1/1/14     lag256     15    1     ALFNCD  94:60:d5:da:5a:20 65534  256  up


Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/1/13     lag256     14    1     ALFNCD  ec:67:94:d4:79:c0 65534  256
1/1/14     lag256     15    1     ALFNCD  ec:67:94:d4:79:c0 65534  256

6200Core(config)#
```

Checking the NAE-lite agent we just configured.

```
6200Core(config)# sh nae-agent lacp_interface_watch_agent
Script Name       : lacp_interface_watch_agent
Version           : 1.0
Origin            : generated
Disabled          : false
Status            : NORMAL
Time Series Count : 0
Alerts Count      : 0
Rules             : 0
Error             : NONE
Alert Description : NONE
Recent alerts     :
        No alerts found

6200Core(config)#
```

Here is the output of “show interface lag256 brief” that indicates the speed of the LACP is 2Mbps because I am using two 1GE interfaces in my lag256 interface.

```
6200Core(config)# sh int lag256 brief
------------------------------------------------------------------------------------------
---------
Port           Native  Mode   Type           Enabled Status  Reason                  Speed
Description
               VLAN                                                                  (Mb/s)
------------------------------------------------------------------------------------------
---------
lag256         1       trunk  --             yes     up      --                      2000
--

6200Core(config)#
```

Now that I have established the baseline, I’ll disconnect one of the interfaces that is part of lag256 and using LACP. This generates the following SYSLOG messages that are sent to my SYSLOG server.

Time	IP	Host	Facility	Priority	Tag	Message
Mar 31 09:29:50	192.168.1.249	1	local7	info		2025-03-31T09:29:49.933226+11:00 6200-Core intfd 840 - - Event|404|LOG_INFO|UKWN|1|Link status for interface 1/1/13 is down
Mar 31 09:29:50	192.168.1.249	1	local7	info		2025-03-31T09:29:49.969841+11:00 6200-Core lacpd 3237 - - Event|1321|LOG_INFO|CDTR|1|LAG 256 State change for interface 1/1/13: Actor state: ALFO, Partner state ALF
Mar 31 09:29:50	192.168.1.249	1	local7	info		2025-03-31T09:29:50.214243+11:00 6200-Core hpe-policyd 63842 - - Event|5507|LOG_INFO|AMM|-|LACP Interface is down
Mar 31 09:29:51	192.168.1.249	1	local7	info		2025-03-31T09:29:51.603737+11:00 6200-Core hpe-policyd 63842 - - Event|6901|LOG_INFO|AMM|-|An action has been triggered by the NAE agent lacp_interface_watch_ager
Mar 31 09:31:35	192.168.1.249	1	local7	info		2025-03-31T09:31:35.321436+11:00 6200-Core lldpd 3286 - - Event|106|LOG_INFO|CDTR|1|LLDP neighbor ec:67:94:d4:79:c0 deleted on 1/1/13

Here the first highlighted message is sent by the NAE-agent. “LACP interface is down”

Now we can check the NAE lite agent alerts with this command.

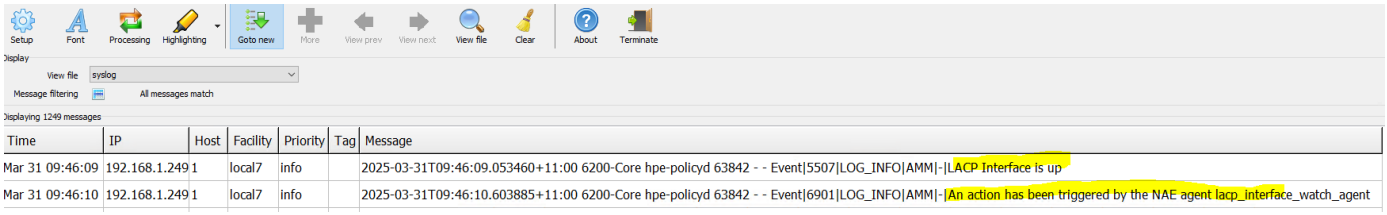
```
6200Core(config)# sh nae-agent lacp_interface_watch_agent alerts

<1> 2025-03-31 09:29:50 An action has been triggered by NAE agent
lacp_interface_watch_agent

6200Core(config)#
```

I want to see the details of the alert and the output of the CLI commands that were part of the Nae-Lite agent.

```
6200Core(config)# sh nae-agent lacp_interface_watch_agent alerts details

Alert message       : 2025-03-31 09:29:50 An action has been triggered by NAE agent
lacp_interface_watch_agent
Action(s) Performed : Alert(1), Syslog(1), CLI(1)

Action Details
======================
Action Alert        : Alert Level Changed to CRITICAL
Action Syslog       :
                      [local] LACP Interface is down
Action CLI          :

<1> CLI command(s)
---------------------
show lacp interfaces
---------------------
Output
---------------------
6200Core# show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
------------------------------------------------------------------------------
1/1/13     lag256                                                     down
1/1/14     lag256     15    1     ALFNCD  94:60:d5:da:5a:20 65534  256  up

Partner details of all interfaces:
------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
------------------------------------------------------------------------------
1/1/13     lag256
1/1/14     lag256     15    1     ALFNCD  ec:67:94:d4:79:c0 65534  256

---------------------
Only the action Alert, action Syslog, and action CLI details are displayed in this
command. Please refer to the Web UI for other action details.
```

```
6200Core(config)#
```

So, the agent worked as expected. Next, I'll reconnect the down interface and that should bring up the LACP interface. Here is the message that was received by my SYSLOG server.



Now we will look at the second alert.

```
6200Core(config)# sh nae-agent lacp_interface_watch_agent alerts

<1> 2025-03-31 09:46:09 An action has been triggered by NAE agent
lacp_interface_watch_agent
<2> 2025-03-31 09:29:50 An action has been triggered by NAE agent
lacp_interface_watch_agent

6200Core(config)#
```

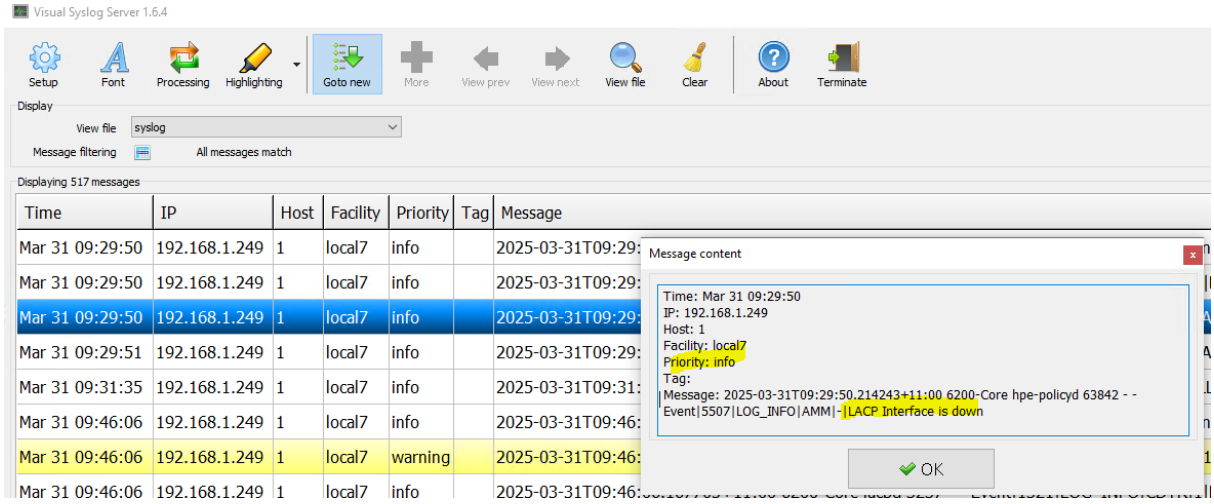
Let's check the details, note that we are matching the latest alert.

```
6200Core(config)# sh nae-agent lacp_interface_watch_agent alerts details 1

Alert message       : 2025-03-31 09:46:09 An action has been triggered by NAE agent
lacp_interface_watch_agent
Action(s) Performed : Alert(1), Syslog(1), CLI(1)

Action Details
======================
Action Alert        : Alert Level Changed to None
Action Syslog       :
                      [local] LACP Interface is up
Action CLI          :

<1> CLI command(s)
---------------------
show interface lag256
show lacp interfaces
---------------------
Output
---------------------
6200Core# show interface lag256

Aggregate lag256 is up
 Admin state is up
 Description :
 MAC Address                  : 94:60:d5:da:5a:20
 Aggregated-interfaces        : 1/1/13 1/1/14
 Aggregation-key              : 256
 Aggregate mode               : active
 Speed                        : 2000 Mb/s
 qos trust none
 VLAN Mode: native-untagged
 Native VLAN: 1
 Allowed VLAN List: 1,5,10-13,16,20,100,110,120,130,140,150,160,192
 L3 Counters: Rx Disabled, Tx Disabled

 Statistic                          RX                    TX                Total
```

```
---------------- -------------------- -------------------- --------------------
Packets                          1661                21681                23342
  Unicast                        1178                   14                 1192
  Multicast                       376                 4176                 4552
  Broadcast                       107                17491                17598
Bytes                           200292              2757079              2957371
Jumbos                               0                    0                    0
Dropped                              0                    0                    0
Pause Frames                         0                    0                    0
Errors                               0                    0                    0
  CRC/FCS                            0                  n/a                    0
  Collision                        n/a                    0                    0
  Runts                              0                  n/a                    0
  Giants                             0                  n/a                    0

6200Core#  show lacp interfaces

State abbreviations :
A - Active        P - Passive      F - Aggregable I - Individual
S - Short-timeout L - Long-timeout N - InSync     O - OutofSync
C - Collecting    D - Distributing
X - State m/c expired              E - Default neighbor state

Actor details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr Forwarding
           Name       Id    Pri                             Pri    Key  State
-------------------------------------------------------------------------------
1/1/13     lag256     14    1     ALFNCD  94:60:d5:da:5a:20 65534  256  up
1/1/14     lag256     15    1     ALFNCD  94:60:d5:da:5a:20 65534  256  up

Partner details of all interfaces:
-------------------------------------------------------------------------------
Intf       Aggr       Port  Port  State   System-ID         System Aggr
           Name       Id    Pri                             Pri    Key
-------------------------------------------------------------------------------
1/1/13     lag256     14    1     ALFNCD  ec:67:94:d4:79:c0 65534  256
1/1/14     lag256     15    1     ALFNCD  ec:67:94:d4:79:c0 65534  256

---------------------
Only the action Alert, action Syslog, and action CLI details are displayed in this
command. Please refer to the Web UI for other action details.

6200Core(config)#
```

This too worked as expected and this time we have 2x CLI commands that were executed. Note that we made use of "\n" as a separator between the two CLI commands.

Going back to the time I disconnected one of the LACP interfaces, I noticed that the SYSLOG message that the agent sent to my SYSLOG server had the severity of "info" as shown below.



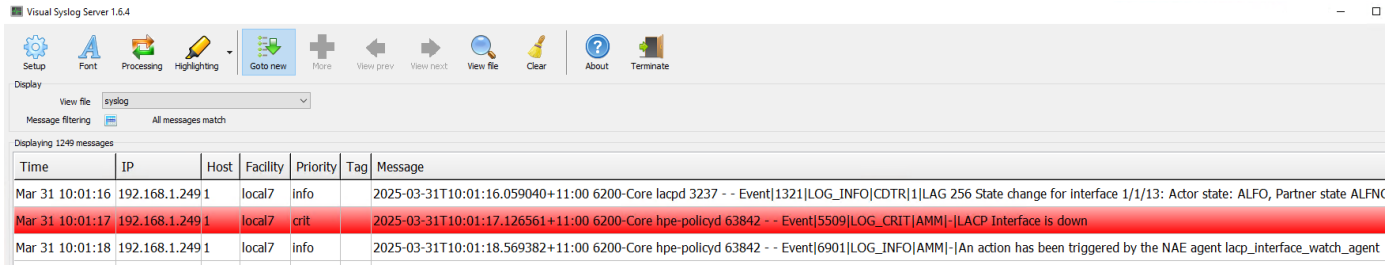
I am going to change that severity to be “critical” so I can easily see the event as my SYSLOG server will display it in a different colour. To do that I’ll modify the configuration and add the highlighted commands.

```
nae-agent lite lacp_interface_watch_agent
    watch lacp_DOWN event-log 1321
    watch lacp_UP event-log 1321
    set-condition watch event-log lacp_DOWN include any "Actor state: ALFO","Partner
state ALFO"
        status critical
        syslog "LACP Interface is down" severity crit
        cli show lacp interfaces
        clear-condition watch event-log lacp_UP include all "Actor state:
ALFNCD","Partner state ALFNCD"
            syslog "LACP Interface is up"
            cli show interface lag256 brief \n show lacp interfaces
```

Note that when you make any changes to an already activated NAE-Agent, you need to reactivate it so that the changes take effect. This is shown below.

```
6200Core(config)# no nae-agent lite lacp_interface_watch_agent activate
6200Core(config)#
6200Core(config)# nae-agent lite lacp_interface_watch_agent activate
6200Core(config)#
```

Now I’ll disconnect one of the LACP interfaces again and this will generate the syslog of severity critical as shown below in red.



3.2 Offline backup of Switch Configuration Use Case

Here is another use case in which the aim is when a configuration of the switch is saved, a copy of the configuration file will be sent to the TFTP server along with the audit for the last 20x commands that were run on the switch. The audit trail log will have us find out what were the changes and who made those changes.

Here we’ll use event ID 6801 which generate the following SYSLOG message

```
Event|6801|LOG_INFO|AMM|-|Copying configs from: running-config to: startup-config
```

So basically, the above event is generated when we execute a “write memory”. And here is our NAE-lite agent

```
nae-agent lite ConfigChange_agent
    watch config_change event-log 6801
    watch tftp_transfer event-log 6801
    set-condition watch event-log config_change include any "Copying configs from: running-
config"
        status minor
        syslog "TFTP configuration updated" severity warning
        cli copy running-config tftp://192.168.1.100/confign-core.txt cli\n
        clear-condition watch event-log tftp_transfer include any "URL: tftp:"
            syslog "TFTP xfer completed"
            cli show accounting log last 20 | redirect tftp://192.168.1.100/acctlog.txt
```

Now we'll activate the agent and check all the NAE-lite agents that we have configured so far.

```
6200Core(config)#nae-agent lite ConfigChange_agent activate

6200Core(config)#sh nae-agent
-------------------------------------------------------------------------------
-------------------------------------------------------------------------
Agent Name                          Script Name                    Version   Origin
Disabled  Status    Time Series Count   Alerts Count   Rules     Error
-------------------------------------------------------------------------------
ConfigChange_agent                  ConfigChange_agent             1.0
generated false     NORMAL    0                  0              0         NONE
interface_watch_agent               interface_watch_agent          1.0
generated false     NORMAL    0                  4              0         NONE
lacp_interface_watch_agent          lacp_interface_watch_agent     1.0
generated false     CRITICAL  0                  1              0         NONE
system_resource_monitor.default     system_resource_monitor        1.5       system
false     NORMAL    10                 0              6         NONE

6200Core(config)#
```

3.2.1 Testing

You can also clear the NAE-data with this command

```
6200Core(config)# clear nae-data
This action will delete NAE data monitored so far.
Do you want to continue (y/n)? y

6200Core(config)#
```

Let's display the agent we just configured.

```
6200Core(config)# sh nae-agent ConfigChange_agent
Script Name       : ConfigChange_agent
Version           : 1.0
Origin            : generated
Disabled          : false
Status            : NORMAL
Time Series Count : 0
Alerts Count      : 2
Rules             : 0
Error             : NONE
Alert Description : NONE
Recent alerts     :
        No alerts found

6200Core(config)#
```

We are ready to test our new NAE-lite agent, and we do that by executing "write memory" command and check the SYSLOG and TFTP servers.

```
6200Core(config)# wr mem
Copying configuration: [Success]

6200Core(config)#
```

This will generate the event we are looking for. Remember that the latest alert will be <1> and so on.

```
6200Core(config)# show nae-agent ConfigChange_agent
Script Name       : ConfigChange_agent
Version           : 1.0
```

```
Origin            : generated
Disabled          : false
Status            : NORMAL
Time Series Count : 0
Alerts Count      : 2
Rules             : 0
Error             : NONE
Alert Description : NONE
Recent alerts     :
        <1> 2025-04-05 17:07:27 An action has been triggered by NAE agent
ConfigChange_agent
        <2> 2025-04-05 17:07:21 An action has been triggered by NAE agent
ConfigChange_agent

6200Core(config)#
```

Let's check the details as we have 2x alerts, the alert #2 is for the configuration changes that was triggered by "write mem" and the action is to copy the configuration to TFTP server

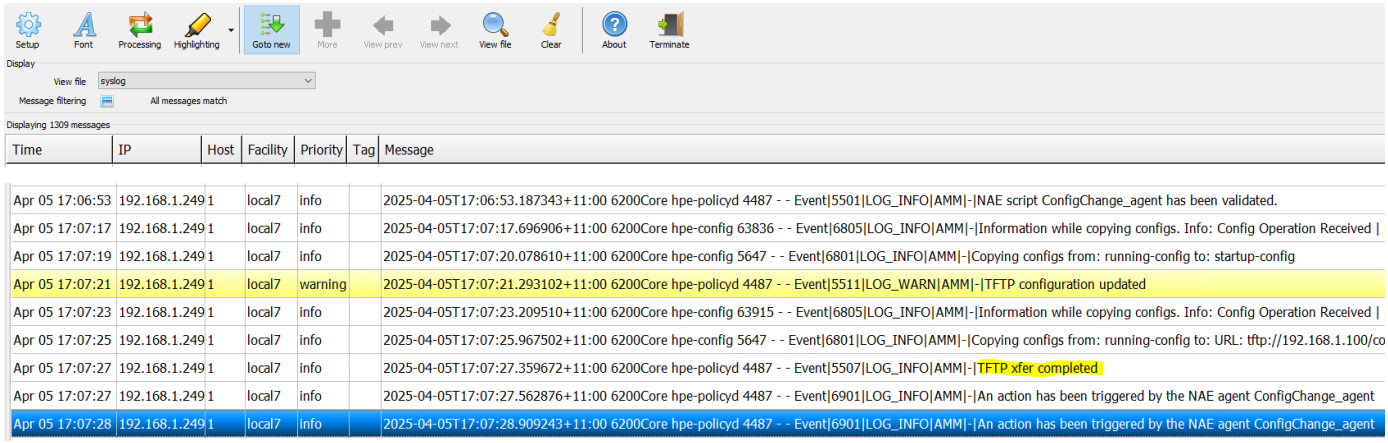
```
6200Core(config)# show nae-agent ConfigChange_agent alerts details 2
Alert message       : 2025-04-05 17:07:21 An action has been triggered by NAE agent
ConfigChange_agent
Action(s) Performed : Alert(1), Syslog(1), CLI(1)

Action Details
======================
Action Alert        : Alert Level Changed to MINOR
Action Syslog       :
                      [local] TFTP configuration updated
Action CLI          :

<1> CLI command(s)
----------------------
copy running-config tftp://192.168.1.100/configN-core.txt cli

----------------------
Output
----------------------
6200Core# copy running-config tftp://192.168.1.100/configN-core.txt cli
Copying configuration: [Success]

6200Core#
----------------------
Only the action Alert, action Syslog, and action CLI details are displayed in this
command. Please refer to the Web UI for other action details.

6200Core(config)#
```

Alert #1 is when for the clear-condition of this watch event. So basically, when the copying the configuration to TFTP server is finished successfully, this condition will be triggered. Here we use a SYSLOG message "TFTP xfer completed" and a CLI action.

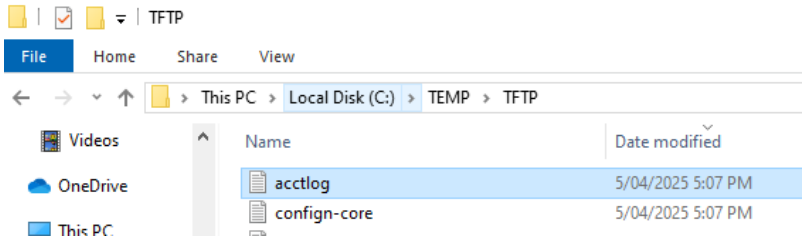
```
6200Core(config)# show nae-agent ConfigChange_agent alerts details 1
Alert message       : 2025-04-05 17:07:27 An action has been triggered by NAE agent
ConfigChange_agent
Action(s) Performed : Alert(1), Syslog(1), CLI(1)

Action Details
======================
Action Alert        : Alert Level Changed to None
Action Syslog       :
                      [local] TFTP xfer completed
Action CLI          :
```

```
<1> CLI command(s)
---------------------
show accounting log last 20 | redirect tftp://192.168.1.100/acctlog.txt
---------------------
Output
---------------------
6200Core# show accounting log last 20 | redirect tftp://192.168.1.100/acctlog.txt

---------------------
Only the action Alert, action Syslog, and action CLI details are displayed in this
command. Please refer to the Web UI for other action details.

6200Core(config)#
```

Here, the SYSLOG server shows SYSLOG message “TFTP configuration updated” with severity = warning.



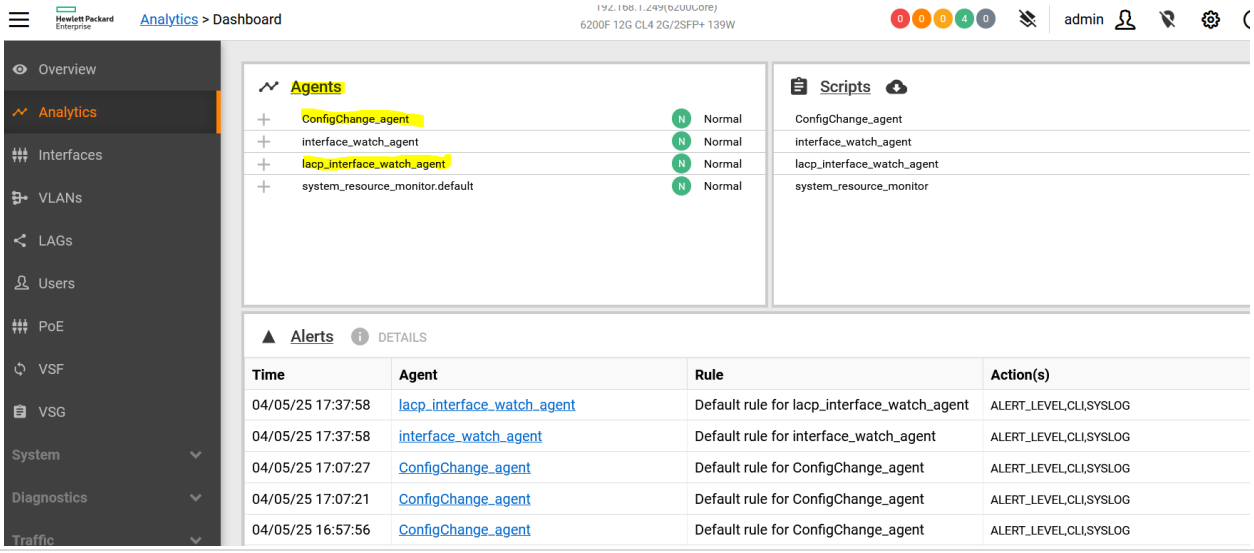
And here are the files that were transfer to our TFTP server.



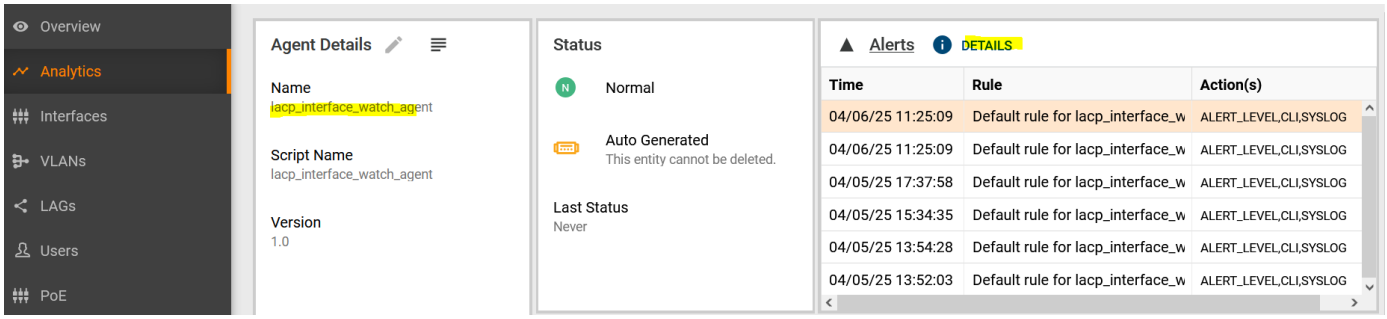
Note that NAE lite with CX firmware 10.15.x now supports TFTP/SFTP/SCP for redirection of any show command.

3.3 Analytics Switch Dashboard

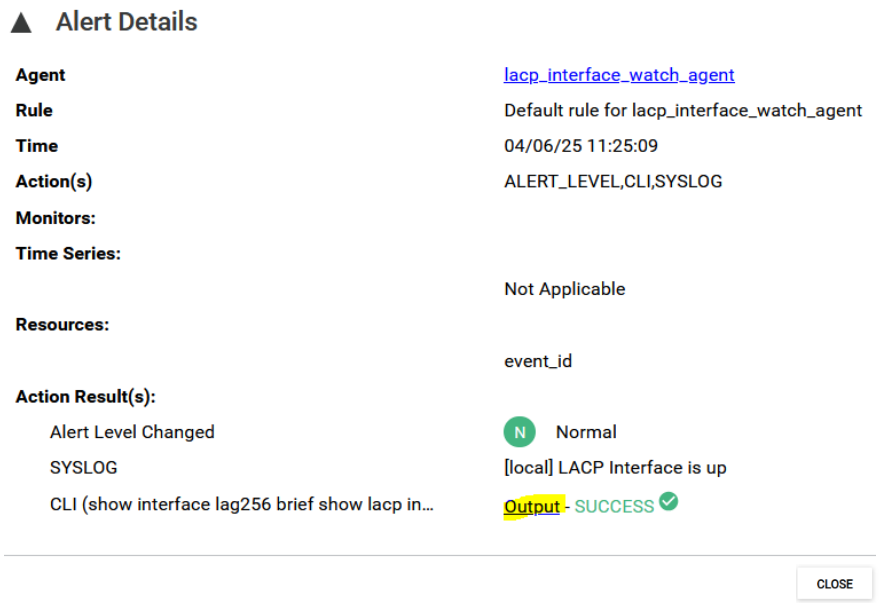
In addition to the CLI, you can also use the WebUI of the CX switch to see the outputs of NAE-Lite agents.



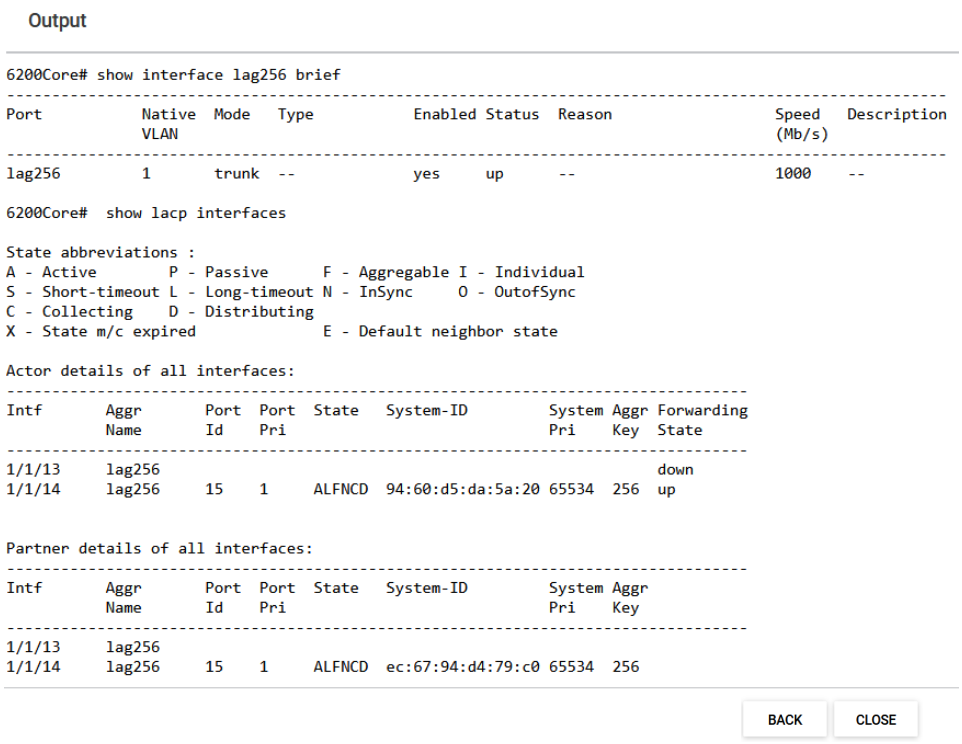
Here you'll see that I have 4x agents running, one of the is the system default "system_resource_monitor" and the rest are my NAE lite agents. I'll click on the LACP agent.



We notice that there has been a recent alert, and I'll click on the latest one and then "Details"



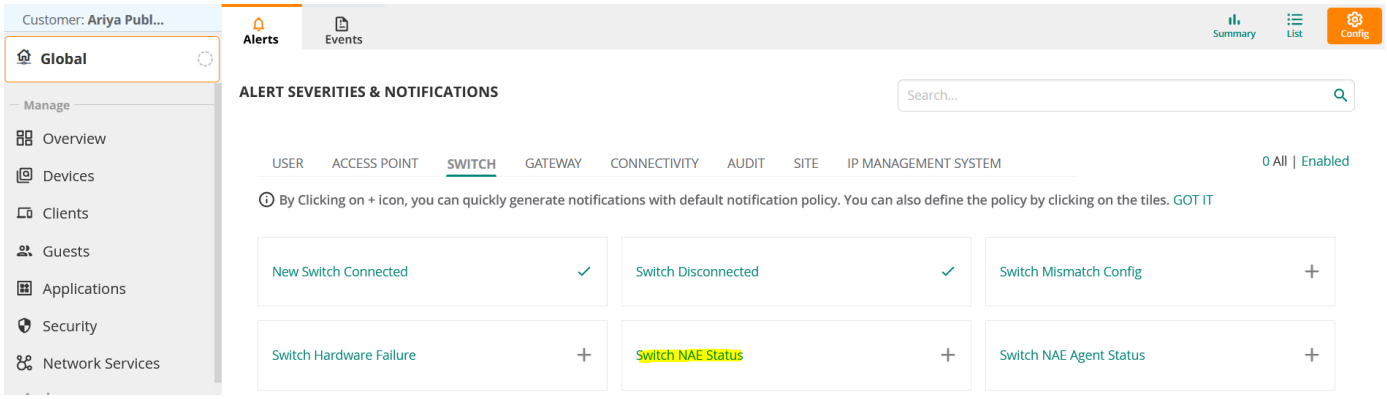
And when we click on the output we see the out of the CLI command that was part of this alert.



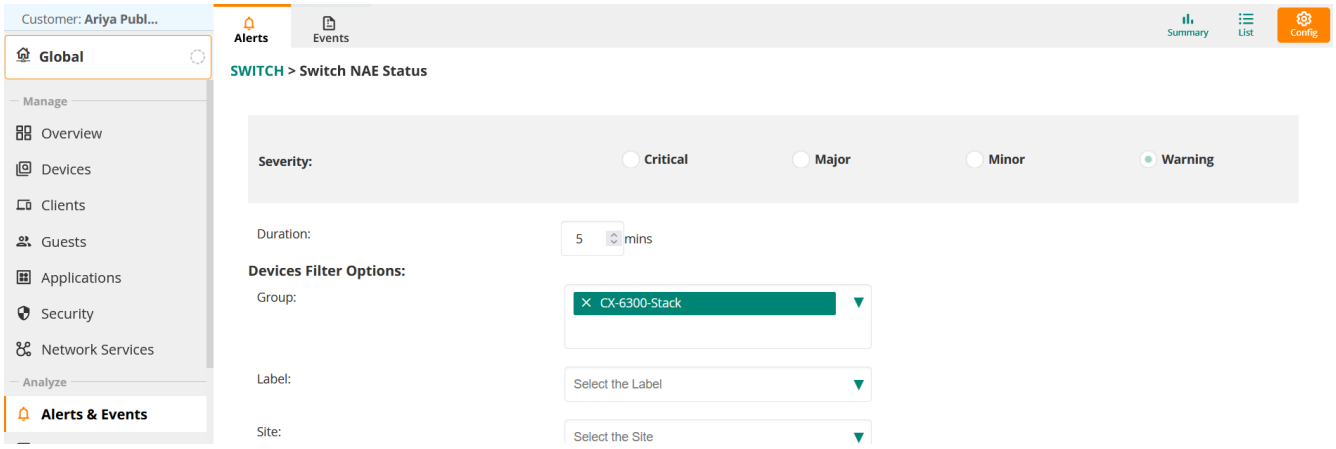
4 NAE Lite and Aruba Central

You should be able to see the alerts and event details for NAE lite agents in Aruba Central if you have those switches under the management of Aruba Central.

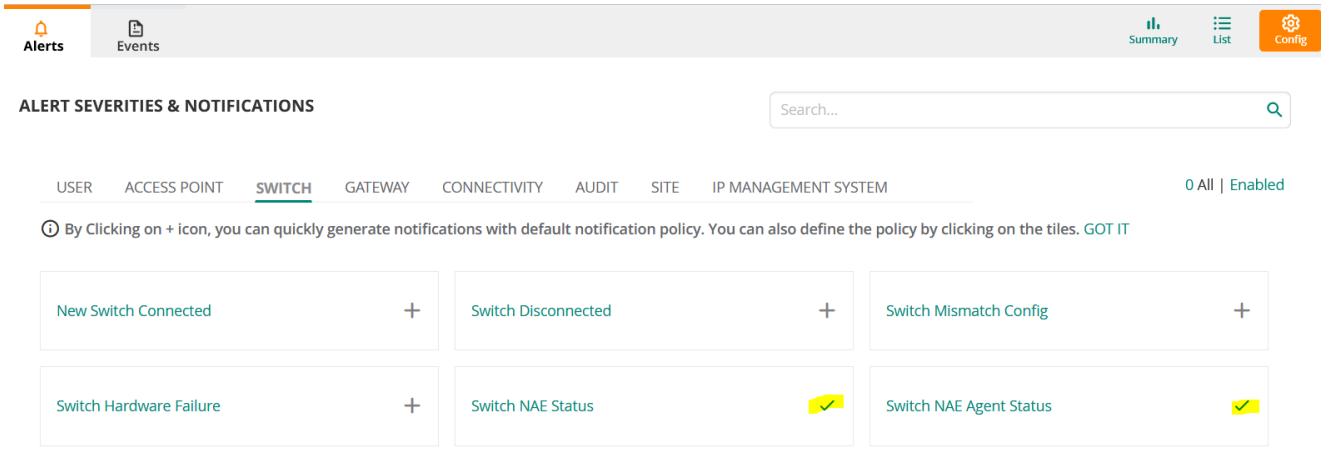
You need to enable NAE status alerts, as they are disabled by default.



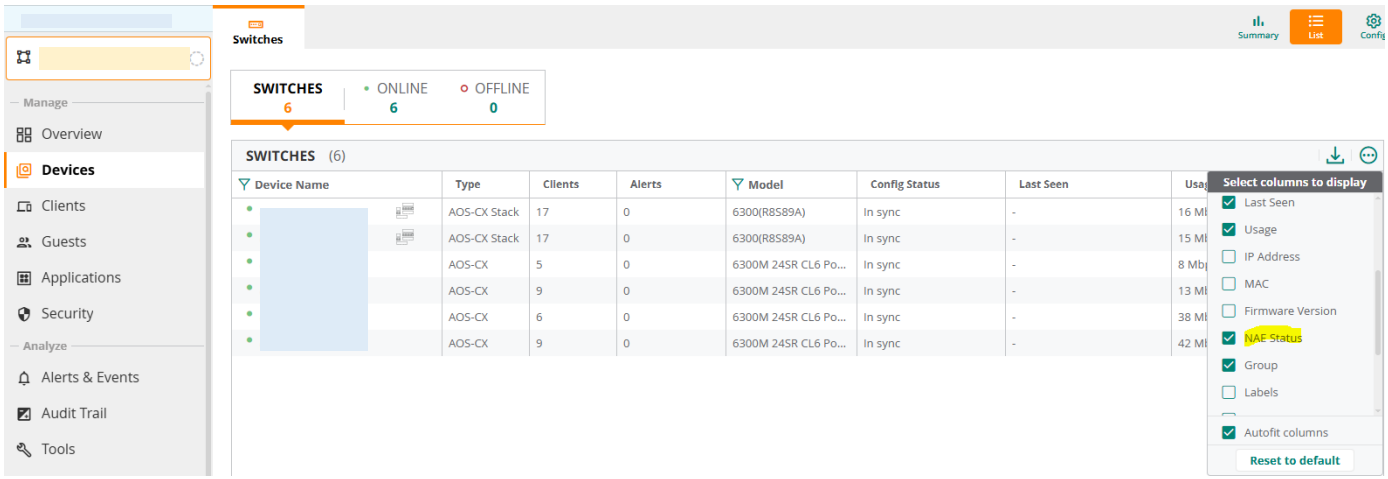
Here you can select the severity level that you want and then enable it for the group/site/device you need.

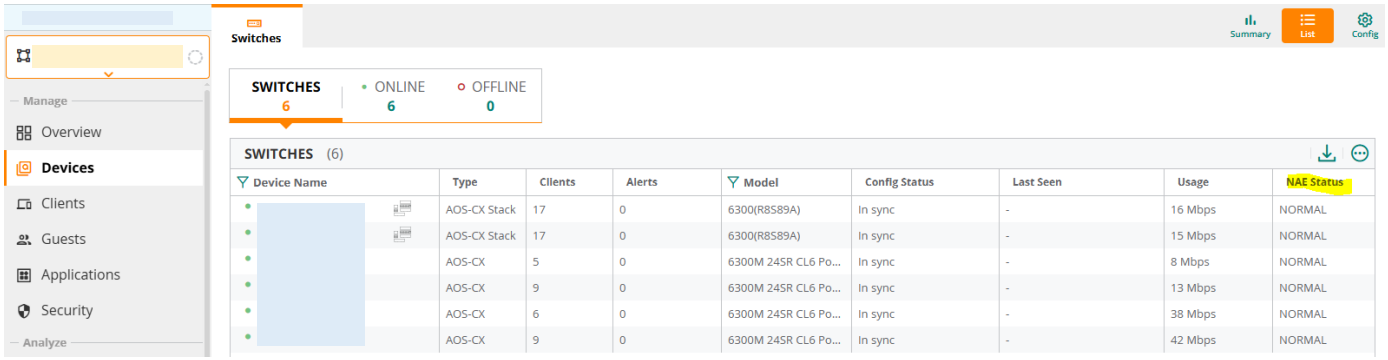


You do the same for the “Switch NAE Agent Status” as well.

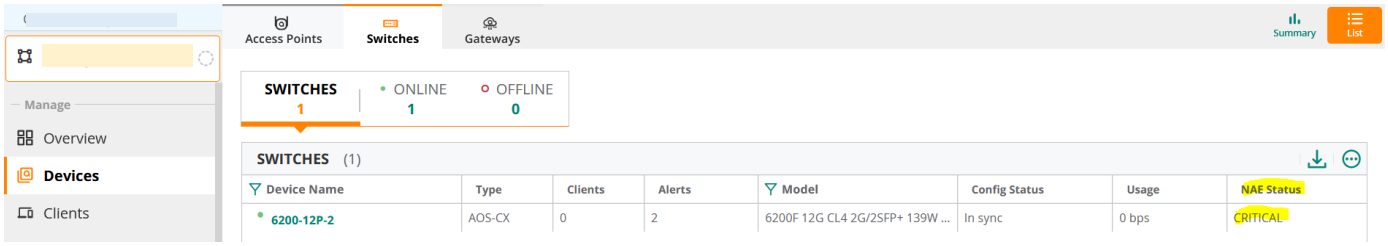


Once this is done, in the Classic Central you can see the NAE status from the group/global level where you need to select the NAE status column as shown below.



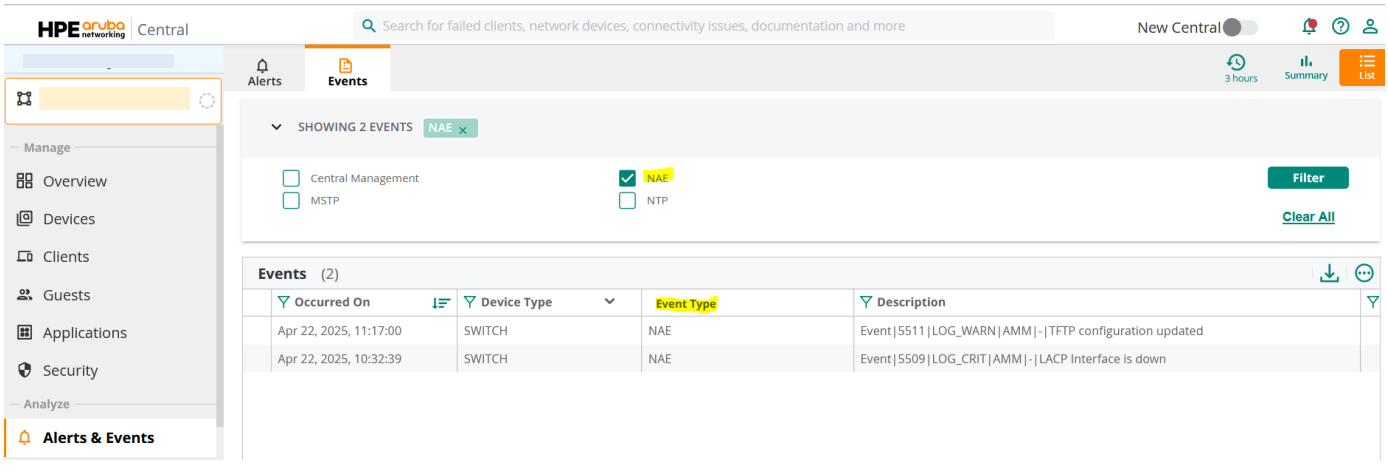


When the NAE Lite agents generate events, we should be able to see in two places. First, we should see it in the group context as shown below using NAE status column.

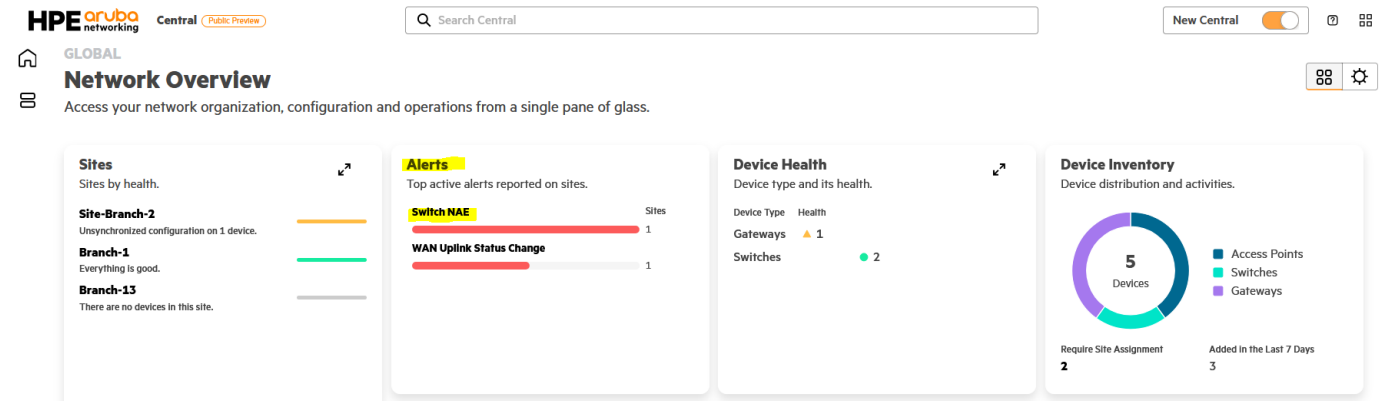


Remember that we had change the severity of the NAE lite agent to Critical that's why it is shown as critical in the screen shot above.

The second place is under events where you can filter on NAE to see just those alerts. Here you can see the two events that were generated for our NAE Lite scripts.



Now, we slide the bar to New Central and in the Network Operation Centre (NOC) view, we see that the alert section lists NAE as one of the high severity alerts.



Here I'll click on "Switch NAE" we get the following, where we can click on Branch1 to go to that site. This is particularly useful if you have a few sites. This way you can quickly view alerts based on severity across all your sites.

Once I click on "Branch-1" , I see that there are two NAE alert. This is because we had configured and tested two NAE Lite scripts. The alerts also display the agent name that generated the alert.