

AOS-CX 10.09 Usability Enhancements

Steve Bartlett

Technical Marketing Engineer AOS-CX
Switching

steve.bartlett@hpe.com



Agenda

1	Firmware Distribution	All platforms
2	Log Buffer Notification	Feature specific, check platform
3	Admin Access to the log file	6200,6300,6400
4	Locked out Users	All platforms
5	Prefer statement on NTP Server	All platforms
6	IPv6 RA Guard (without ND Guard)	8325
7	'sh ip ospf interface' improvement	All ospv2 platforms
8	'sh spanning tree' improvement	All platforms
9	'sh mac-address' improvement	All platforms

Usability

Firmware Distribution - REST
All switch platforms

Firmware Site Distribution - REST

AO-CX Firmware site distribution feature supports a switch and image to be used as a local image distributor.

Supported by any CX Switch with 10.09 or later

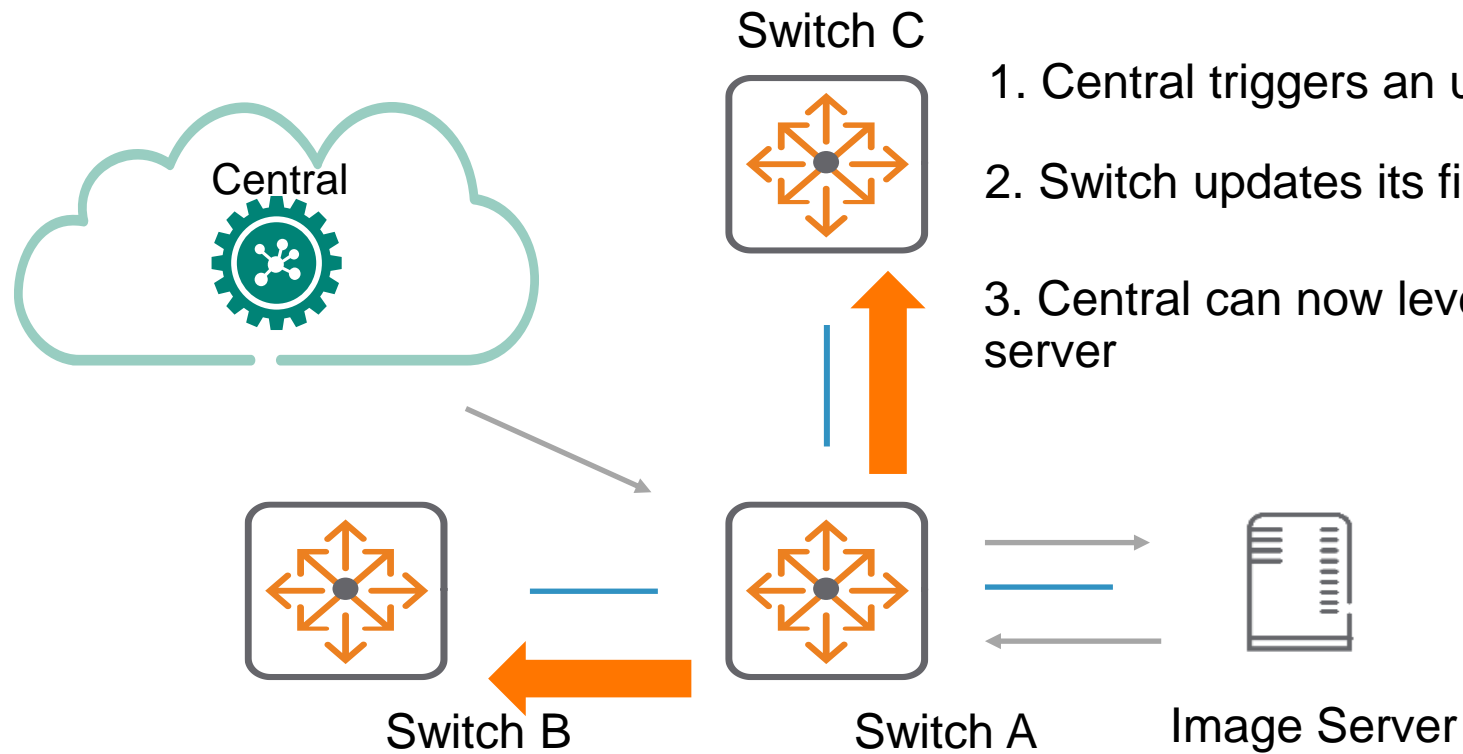
Uses the same existing Firmware REST API

No cross-family image distribution between switches

Process is to

- Upgrade switch image slot in a switch (optionally reboot)
- Then use the switch image as a local image distributor

Example



1. Central triggers an upgrade request on the desired switch
2. Switch updates its firmware image via the target image server
3. Central can now leverage the Switch as the distribution server

The Central functionality to provide the orchestration will be present in the next release

(*anticipated release 2.5.5)

Usability

Log Buffer notification - Notify when logs exceed threshold

Problem Statement

Some features inadvertently fill the partition with logs in the /var/log directory and when the log-buffer 'wraps', the older logs are overwritten with no user warning or notification.

A method is required to ensure that the Network Administrator has the option of copying log files prior to the overwrite and is notified via rmon traps and an event log raised whenever the log buffer or var/log directory size exceeds its threshold limit.

Solution Overview

Generate an event log as well as a rmon trap whenever the log buffers exceeds its limit.

Log buffer notification supported below log buffers

- Event logs
- Auth logs
- Audit logs
- **Security logs (Applicable to 6200, 6300 and 6400 platforms).**

Platform support [event log/audit/auth log]

4100i, 6100, 6200, 6300, 6400, 8320, 8325, 8360, 8400

Security log platform support - new

6200/6300/6400

Design detail

Log buffer monitoring :

The log buffer is split into manageable 'chunks'.

The size and the number of 'chunks' may vary based on the platform.

Whenever one chunk is full, it will be archived and a new chunk is created for storing new logs.

When the max limit for the last chunk number is reached, the chunk is archived & the oldest chunk will be deleted.

The *log buffer almost full* event and snmp RMON trap is raised whenever the number of chunks reaches one less than the max limit.

User can collect the needed logs before they get rotated.

The *log buffer overwritten* event and snmp RMON trap is raised whenever the max limit is hit resulting in rotating the oldest chunk.

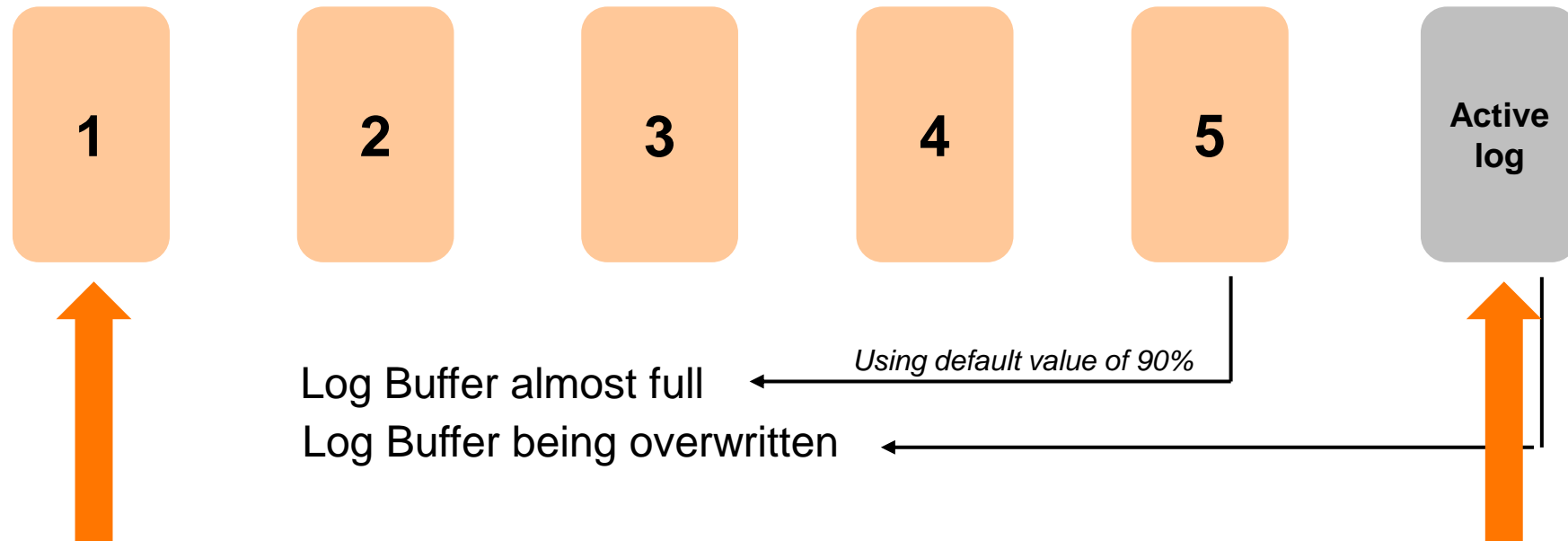
Uses the logrotate functionality to notify log-mgmt, whenever log buffers are reaching to their threshold and about to rotate/wrapped.

The log-mgmt will trigger the event/trap notification as appropriate

Example – 6300 platform

Log Buffer chunks of 16mb each

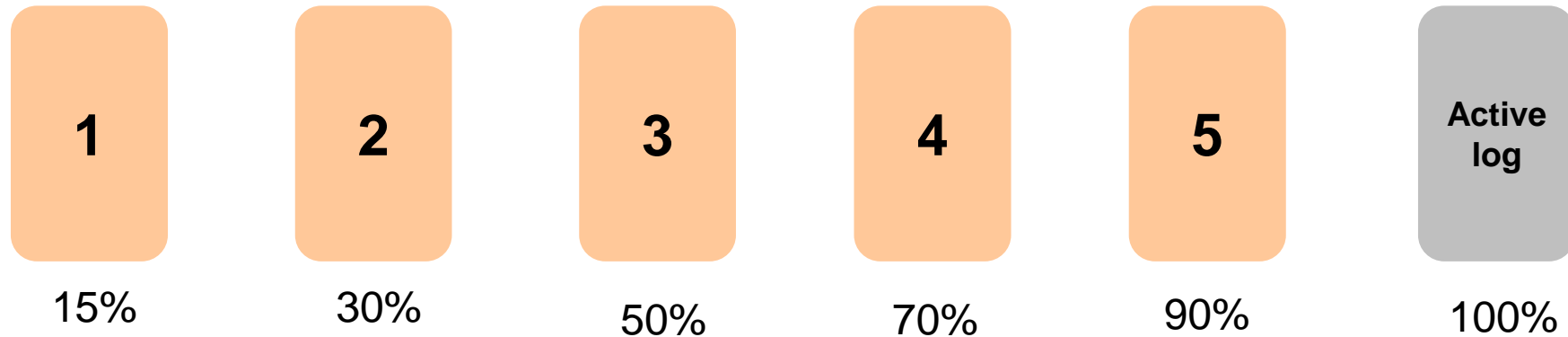
When 5 chunks are consumed , a log buffer almost full event with snmp RMON trap is triggered



1. When one chunk is full, it is archived and a new chunk is created.
2. When 5 chunks (80 mb) is consumed , the log buffer almost full event and snmp RMON trap is triggered
3. When 6 chunks are consumed, the log buffer full event and snmp RMON trap is triggered.
4. When the max limit is reached on the number of chunks, the oldest chunk is deleted.
5. The log buffer almost full event and snmp RMON trap is raised whenever the number of chunks reaches one less than the max limit.

Example Log threshold CLI

Log Buffer chunks of 16mb each – 6300 (chunk size will vary for each platform)
% values indicates the log buffer chunk is full



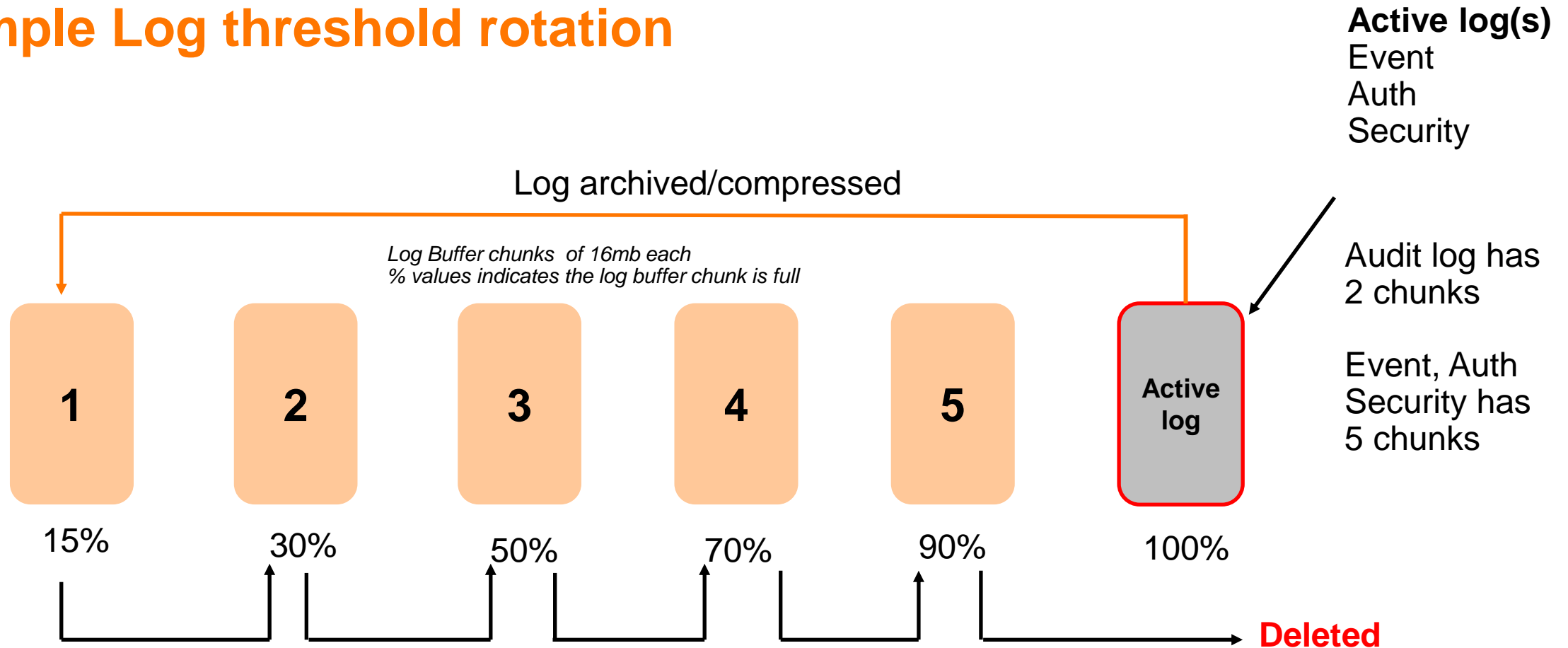
Syntax :

```
[no] log-threshold { event-log | security-log | audit-log | auth-log } <15 | 30 | 50 | 70 | 90 | 100>
```

Default threshold-limit : 90

*Avoid changing the default threshold higher than 90%

Example Log threshold rotation



Whenever one chunk is full, it will be archived and a new chunk is created for storing the new logs

When we hit the max limit for the number of chunks, the oldest chunk will be deleted.

Log archive and retrieval

```
6405-BLDG03# start-shell
```

Start shell from cli prompt

```
6405-BLDG03:~$ sudo bash
```

Shell commands

```
6405-BLDG03:/home/admin#
```

```
6405-BLDG03:/home/admin#
```

```
6405-BLDG03:/home/admin# cd /var/log
```

```
6405-BLDG03:/var/log# ls audit.log*
```

Rotated audit log file 'chunk1'

```
audit.log.1.gz
```

```
6405-BLDG03:/var/log# ip netns exec swns  
bash
```

Allow apps that are network namespace unaware
to be run outside of the default network namespace

```
6405-BLDG03:/var/log# sftp  
admin@10.80.2.118
```

Run SFTP commands to destination host server

Commands

```
switch(config)# log-threshold event-log 30
switch(config)# log-threshold auth-log 50
switch(config)# log-threshold audit-log 70
switch(config)# log-threshold security-log 50
switch(config)# no log-threshold event-log
switch(config)# no log-threshold auth-log
switch(config)# no log-threshold audit-log
switch(config)# no log-threshold security-log
```

`no log-threshold' command restores the log default value

Platform storage capacity

Platform	Flash size/type
6100	16GB eMMC
6200	16GB eMMC
4100i	32GB eMMC
6300	32GB eMMC
6400	32GB eMMC
8360	32GB eMMC
8320	64GB SSD
8325	64GB SSD
8400	100GB SSD
10000	64GB SSD

eMMC = embedded multimedia card

SSD = solid state drive

*SSD will be considerably faster when transferring data compared to an eMMC storage device

Summary

All platforms have 6 'chunks' for event, auth and Security logs

All platforms have 2 'chunks' for audit logs

The size of the platform 'chunk' will vary depending on platform, some platforms are 'lightweight'.

Usability

Admin access to the logfile
(security log) 6200/6300/6400

Admin Access to the security logfile – 6200,6300,6400 series

A new log file is available for security logging as part of the security logging framework

The security logging is a framework to log events generated by daemons, process and plugins running within the switch software which are of a sensitive nature or related to authentication and authorisation.

The Security logging framework captures these generated security-logs into a secure file.

A local user group can be given privileges for viewing and copying the security logs to a remote location.

This privilege can only be granted by members of the 'administrators' user group.

The group that obtains the security permission behaves like a security user group or security auditor group.

Although members of the 'administrators' group can grant this privilege, they themselves are not permitted to execute the commands.

Security User and built in groups

A security user is a user having access to only security log related commands and no other access on the switch.

Administrators are advised to configure a user group permitting only security log commands.

A security user can be created to similar to a local-user and can be given privilege to execute security-log related commands which are not available to any built-in-users.

It is advised that when such a security-user group is created no other commands apart from the security related commands are added to the group.

The 3 default built in roles: Administrators, operators , auditors are not permitted to execute the following CLI commands:

```
show security-logs  
clear security-logs  
copy security-logs
```

Only a **local user-group** created and permitted to execute these commands by the users of the 'administrators' group have the required privilege.

Creating a security user group and user

```
user-group security-audit
```

```
20 permit cli command "clear security-logs*"
```

```
30 permit cli command "show security-logs*"
```

```
40 permit cli command "copy security-logs*"
```

← Security commands assigned to user group

```
user-group security-audit
```

```
user security-user group security-audit password  
plaintext xxxxxxxxx
```

← local user assignment to group membership
security-audit

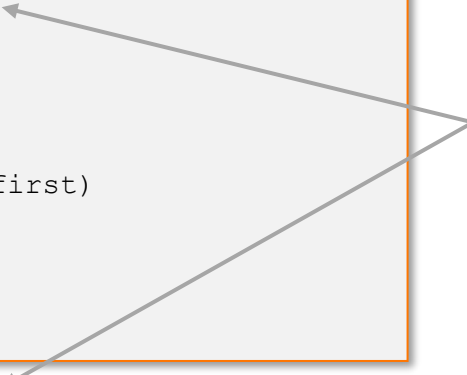
**The assignment user groups and cli permissions are not new.
The security-log and association events to the security-user is new*

sh security-logs

```
6200-BLDG02-F1# sh security-logs
```

- a Display event logs from previous and current boots
- c Display event logs for specified event category
- d Display event logs for specified daemon
- n Display the specified number of event logs
- r Display event logs in reverse order (most recent first)
- s Display event logs as per specified severity

Users assigned to security-user group only have access to the assigned security cli commands

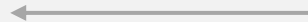



```
6200-BLDG02-F1# 6200-BLDG02-F1# sh security-logs -c user-mgmt -n 2 -r -s
```

- alert Display logs with severity 'alert(6)' and above
- crit Display logs with severity 'critical(5)' and above
- debug Display logs with all severities
- emer Display logs with severity 'emergency(7)' only
- err Display logs with severity 'error(4)' and above
- info Display logs with severity 'info(1)' and above
- notice Display logs with severity 'notice(2)' and above
- warn Display logs with severity 'warning(3)' and above

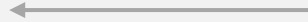

Security-log commands access

```
6200-BLDG02-F1# sh security-logs  
Permission denied. User cannot execute this command.
```



Users with admin privileges cannot access the security commands that are specific to users assigned to the security-group

```
6200-BLDG02-F1# sh running-config  
Cannot execute command. Command not allowed.
```



Users with security-group privileges cannot access other commands only the allocated [security] commands.



```
user-group security-audit  
20 permit cli command "clear security-logs*"  
30 permit cli command "show security-logs*"  
40 permit cli command "copy security-logs*"
```

Summary

```
sh security-logs  
clear security-logs [separate logfile]  
copy security-log sftp://root@10.80.2.118/securelog vrf mgmt  
copy security-log scp://root@10.80.2.118/securelog vrf mgmt  
copy security-log tftp://root@10.80.2.118/securelog vrf mgmt
```

3 new commands

security-user group is supported with AAA configurations and standard RBAC features with Radius and Tacacs

The security user role is not 'in built' and has to be configured

Security user roles are created by the user-group administrators

Administrators cannot execute the associated security log commands (x3)

Only assigned users to the security-group can access the security log commands (the recommendation is to restrict to the security related commands only – and no other commands)

EVENT-IDs Security logging - 1

Event Name	ID	Description	Severity	Event Catagory
INTERFACE_LINK_MACSEC_PFC_INCOMPAT	408	Log when interface is down due to incompatible MACsec and PFC configutration	LOG_WARN	INTERFACE
AAA_CONFIG	2301	Logs AAA Authentication/Authorization/Accounting/fail-through	LOG_INFO	AAA
TACACS	2302	Logs TACACS+ server update, server group update and global default update	LOG_INFO	AAA
RADIUS	2303	Logs RADIUS server update, server group update and global default update	LOG_INFO	AAA
RADIUS_TRACKING	2304	Logs changes in RADIUS server reachability status	LOG_INFO	AAA
TACACS_TRACKING	2305	Logs changes in TACACS server reachability status	LOG_INFO	AAA
RADIUS_SERVER_ROUTE_REACHABILITY	2306	Logs changes in RADIUS server route reachability status	LOG_INFO	AAA
SELFTEST_BEGIN	4501	logs the start of selftest on a particular subsystem	LOG_INFO	SELFTEST
SELFTEST_END	4502	logs the completion of selftest on a particular subsystem	LOG_INFO	SELFTEST
CARD_SELFTEST_FAILURE	4503	logs the selftest failure of a particular subsystem	LOG_ERR	SELFTEST
PORT_SELFTEST_FAILURE	4504	logs the port selftest failure on a given subsystem	LOG_ERR	SELFTEST
AUTZ_FAILURE	4506	logs a failed authorization attempt of a user via REST	LOG_ERR	SELFTEST

EVENT-IDs Security logging -2

Event Name	ID	Description	Severity	Event Catagory
AUTZ_SUCCESS	4607	logs a successful authorization attempt of a user via REST	LOG_INFO	RESTD
AUTZ_ALLOWED	4608	logs an allowed authorization attempt of a user via REST	LOG_INFO	RESTD
USER_PASSWORD_CHANGE_SUCCESS	4611	logs a successful password change for a user via REST	LOG_INFO	RESTD
USER_PASSWORD_CHANGE_FAILURE	4612	logs an unsuccessful password change for a user via REST	LOG_WARN	RESTD
USER_PASSWD_CHANGE	4703	Logs a message when a user changes his/her password	LOG_INFO	USER-MGMT
USER_PASSWD_CHANGE_FAIL	4704	Logs a message when a user fails to change his/her password	LOG_ERR	USER-MGMT
PASSWD_EXPORT	4705	Logs a message when a user sets export password	LOG_INFO	USER-MGMT
NO_PASSWD_EXPORT	4706	Logs a message when a user restores default export password	LOG_INFO	USER-MGMT
DEFAULT_EXP_PASSWD_USED	6501	Warns the user that export password file was corrupted and default passwd was used instead.	LOG_WARN	CREDMGR
CHASSIS_SECRET_CORRUPTED	6502	Warns the user that the chassis secret has been corrupted.	LOG_ALERT	CREDMGR
SS_CERT_CREATED	6504	Logs a message when the self-signed cert is created by credmgr.	LOG_INFO	CREDMGR
SVOS_ADMIN_PW_CHANGED	6505	Logs a message when a user changes admin password from ServiceOS	LOG_INFO	CREDMGR

EVENT-IDs Security logging -3

Event Name	ID	Description	Severity	Event Catagory
AUTH_KEY_CREATED	6506	Logs a message when SSH authorized keys are added for a user	LOG_INFO	CREDMGR
AUTH_KEY_FAILED	6507	Logs a message after a failure to write SSH authorized keys for a user	LOG_ERR	CREDMGR
AUTH_KEY_DELETED	6508	Logs a message afte deleting SSH authorized keys for a user	LOG_INFO	CREDMGR
AUTH_KEY_INVALID	6509	Logs a message when SSH authorized key fails validation chack	LOG_ERR	CREDMGR
ACL_LOG_STATS	1000 2	ACL log statistics	LOG_INFO	ACL
ACL_APPLICATION_FAILURE	1000 3	ACL application failure	LOG_ERR	ACL

The background features a solid red circle in the top-left corner and a large, dark blue shape with a white dotted pattern that occupies the right and bottom portions of the frame.

Usability

locked out users

All platforms

locked out users

Login attempts can be limited with two new authentication commands impacting ssh vty access and console access.

```
6200-BLDG02-F1(config)# aaa authentication
    allow-fail-through      Allow AAA fail-through
    console-login-attempts Limit user console failed login attempts
    limit-login-attempts    Limit user failed login attempts
    login                   Switch login
    port-access             Configure Port Based Network Access.
```

```
6200-BLDG02-F1(config)# aaa authentication limit-login-attempts 5 lockout-time 60
```

```
6200-BLDG02-F1(config)# aaa authentication console-login-attempts 5 console-lockout-time 60
```

Values

login-attempts <1-10> Max retries

lockout-time <1-360> [seconds] Timeout max lockout hr

Locked out user example

```
6200-BLDG02-F1# sh user-list
```

USER	GROUP

admin	administrators
contractor	administrators
security-user	security-audit

```
6200-BLDG02-F1# sh authentication locked-out-users
```

USER	GROUP

contractor	administrators

← New command

Summary

	console-login-attempts	limit-login-attempts	console	SSH , REST & Telnet
Scenario 1	Enabled	Disabled	User locked out when configured console-limit-login threshold is exceeded	The locked out user can still access the switch through SSH, REST and Telnet interface
Scenario 2	Disabled	Enabled	The locked out user can access the switch through the console login	User is locked out of SSH, REST and Telnet when configured limit-login threshold is exceeded
Scenario 3	Enabled	Enabled	User will be locked Out from all interfaces when console-limit-login threshold is exceeded	User is locked out of all interfaces when configured limit-login threshold is exceeded

Caveats

If remote authentication using RADIUS/TACACS+ is configured on any channel (eg: ssh, https-server, console, telnet, default) then the console login attempts and lockout feature cannot be configured.

If console login attempts and lockout is configured, then remote authentication using RADIUS/TACACS+ cannot be configured on any channel.

Console login attempts configuration is only applied to console channel (not applied to SSH, TELNET and REST).

No timestamp available

Usability

Prefer statement on a NTP server

IPv4 IPv6

All AOS-CX switch platforms

NTP Server preference

```
BLDG01-AGG02(config)# ntp server time2.google.com

burst      NTP Association use burst mode
iburst     NTP Association use iburst mode
key-id     NTP Key ID
maxpoll    NTP maximum poll time to use configuration
minpoll    NTP minimum poll time to use configuration
prefer    NTP Association preference configuration
version    NTP Association version configuration
```

```
ntp server 10.80.2.219 iburst prefer
ntp server time.google.com
ntp server time1.google.com
ntp enable
```

```
ip dns domain-name tmlab.net
ip dns server-address 10.80.2.219
```

Note when using multiple servers with the same stratum setting a preferred server is recommended.

Setting a preferred server, NTP will attempt to keep the preferred server the primary NTP connection.

If a preferred server is not manually set and NTP is enabled the configured server with the lowest stratum will automatically be set as the preferred server.

Prefer selection of servers with same stratum (if not manually selected) may change on reboot or reconfiguration.

Supported with IPv4 and IPv6 addressing

Summary & Caveats

IPv4 & IPv6 NTP services are supported.

If no manual preference is configured, an 'auto' preference is applied based on the configured server with the lowest stratum. This will automatically be set as the preferred server.

A manual preferred server is highly recommended, especially when using multiple servers with the same stratum setting

DHCP options can be used to configure up to 2 NTP servers

AOS-CX switches 4100i, 6100,6200,6300,6400v1,v2 & 10000 using DHCP option (42) after the 'erase all zeroize' command.

DHCP uses the OBM port to get its Ip addresses and at the same time receive the DHCP NTP server detail

NTP is set to use the default VRF and using this method cannot access the NTP server to mark it as 'preferred'

Work around is to use the mgmt. vrf for NTP `'ntp vrf mgmt'`

After connectivity via the mgmt. VRF , the default VRF can be used.

Does not impact 8400 & 8325 series

Usability

IPv6 RA guard without ND guard
AOS-CX 8325 Series

IPv6 RA Guard

Routers periodically multicast Router Advertisement (RA) messages to announce their availability and convey information to neighboring nodes that enable them to be automatically configured on the network.

Hosts listen for RA messages for IPv6 address autoconfiguration and discovery of link-local addresses of the neighboring routers, and can also send a Router Solicitation (RS) message to request immediate advertisements

RA messages are unsecured, which makes them susceptible to attacks on the network that involve the spoofing (or forging) of link-layer addresses.

RA guard can be applied to filter router advertisements, either block or permit RAs based on trust or untrusted ports

The RA guard feature is now available on the 8325 series platform

IPv6 RA Guard – Configuration notes

ND Snooping

The ND snooping feature is used in Layer 2 switching networks.

It learns the source MAC addresses, source IPv6 addresses, input interfaces, VLANs of arriving ND messages and data packets to build the ND snooping table.

ND snooping entries can be used by ND detection to prevent spoofing attacks.

ND detection processes the ND messages received on ND trusted and untrusted interfaces a

RA Guard

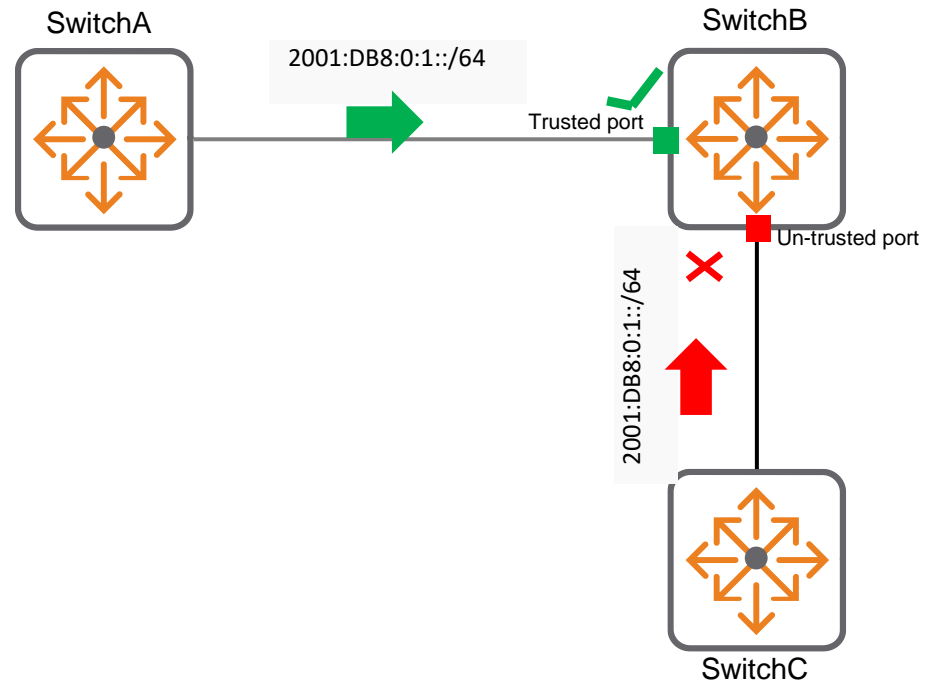
RA guard is applied to a VLAN

ND-Snooping must enabled at a global level and at the desired VLAN level

When enabled, ingress RA (Router Advertisement) and RR (Router Redirect) packets are blocked and dropped on untrusted ports

RA/RR packets are forwarded if received on trusted ports

IPv6 RA Guard feature - 8325 series



Configuration

RA guard applied to a VLAN

```
SERV-AGG02(config)# nd-snooping enable
```

nd-snooping enabled globally

```
SERV-AGG02(config)# vlan 101
```

```
SERV-AGG02(config-vlan-101)# nd-snooping ra-guard log
```

nd-snooping with ra-guard

```
SERV-AGG02(config)# interface 1/1/5
```

```
SERV-AGG02(config-if)# no routing
```

```
SERV-AGG02(config-if)# vlan access 101
```

```
SERV-AGG02(config-if)# nd-snooping trust
```

*nd-snooping trust [interface/lag]

*nd-snooping trust [interface/lag]

Ingressing RA (Route Advertisements) RR (Router Redirect) packets are blocked/dropped on untrusted ports

Useful commands

```
SERV-AGG02# sh nd-snooping  
statistics    Show ND Snooping statistics  
vlan          Show ND Snooping configuration for the specific VLAN  
vsx-peer      Displays VSX peer switch information
```

```
SERV-AGG02# sh nd-snooping vlan 101
```

ND Snooping Information

=====

ND Snooping : Enabled

MAC Address Check : Enabled

RA Guard : Enabled

PORT	TRUST
------	-------

lag69	No
-------	----

lag256	No
--------	----

1/1/5	Yes
-------	-----

Usability

sh ip ospf interface

All platform support for OSPFv2

OSPF Passive interface

Either in the ospf context or per interface

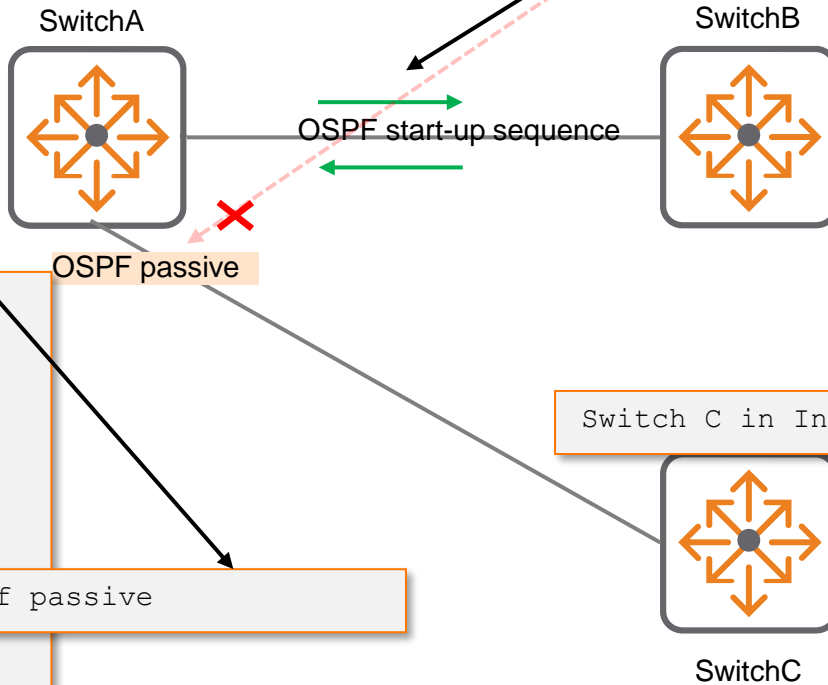
```
router ospf 1
router-id 10.69.253.4
```

~~passive-interface default~~

Remove

```
interface 1/1/1
no shutdown
ip mtu 9192
ip address 10.69.0.17/31
ip ospf 1 area 0.0.0.0
no ip ospf passive
ip ospf network point-to-point
```

ip ospf passive



Init - Ospf hello packets

Exstart - Peer relationship established

Exchange - Dbase synchronization

Loading - Link state updates between peers

Full - fully functional neighbor adjacency

sh ip ospf interface 10.09 enhancement

```
VTEP2# sh ip ospf interface

Codes: DR - Designated router  BDR - Backup Designated router

Interface 1/1/49 is up, line protocol is up
-----

VRF          : default          Process          : 1
IP Address    : 192.168.2.3/31   Area             : 0.0.0.0
Status        : Up              Network Type     : Point-to-point
Hello Interval : 10      sec     Dead Interval    : 40      sec
Transit Delay  : 1        sec     Retransmit Interval : 5        sec
BFD            : Disabled        Link Speed       : 100000 Mbps
Cost Configured : NA            Cost Calculated  : 1
State/Type     : Point-to-point Router Priority    : n/a
DR             : No              BDR              : No
Link LSAs      : 0              Checksum Sum     : 0
Authentication : No              Passive          : No
```





Usability

sh spanning-tree

All switch platforms

sh spanning-tree

```
6405-BLDG03# sh spanning-tree

Spanning tree status      : Enabled Protocol: MSTP

MST0

  Root ID    Priority    : 32768

          MAC-Address: 90:20:c2:dc:47:00

          This bridge is the root

          Hello time(in seconds):2   Max Age(in seconds):20

          Forward Delay(in seconds):15

  Bridge ID  Priority    : 32768

          MAC-Address: 90:20:c2:dc:47:00

          Hello time(in seconds):2   Max Age(in seconds):20

          Forward Delay(in seconds):15
```

From Disabled/Blocking
To Disabled/Down

Port	Role	State	Cost	Priority	Type	BPDU-Tx	BPDU-Rx	TCN-Tx	TCN-Rx
1/3/1	Disabled	Down	20000	128	P2P	0	0	0	0
1/3/3	Disabled	Down	20000	128	P2P	0	0	0	0
1/3/4	Disabled	Down	20000	128	P2P	0	0	0	0





Usability

Show mac-address improvement
All switch platforms

show mac-address table port - adding Interface for port alias

Prior to 10.09

```
SwitchB# sh mac-address-table

address    Show a specific MAC address
count      Number of MAC addresses
detail     Show Layer 2 MAC address table detail information
dynamic    Show learnt MAC addresses
hsc        Show MAC addresses learnt by the Hardware Switch Controller
port       Show MAC addresses learnt on port
static     Show static MAC address information
vlan       Show MAC addresses learnt on VLANs
vsx-peer   Displays VSX peer switch information
```

'sh mac-address-table port' command will be deprecated

```
SwitchB# sh mac-address-table port 1/1/1

MAC age-time          : 300 seconds
Number of MAC addresses : 1

MAC Address      VLAN    Type                Port
-----
00:50:56:8e:fb:12  30      dynamic             1/1/1
```

10.09

```
SwitchA# sh mac-address-table

address    Show a specific MAC address
count      Number of MAC addresses
detail     Show Layer 2 MAC address table detail information
dynamic    Show learnt MAC addresses
hsc        Show MAC addresses learnt by the Hardware Switch Controller
interface Show MAC addresses learnt on interface
port      Show MAC addresses learnt on port
static     Show static MAC address information
vlan       Show MAC addresses learnt on VLANs
vsx-peer   Displays VSX peer switch information
```

Replaced with 'sh mac-address-table interface' command

```
SwitchA# sh mac-address-table interface 1/1/1

MAC age-time          : 300 seconds
Number of MAC addresses : 1

MAC Address      VLAN    Type                Interface
-----
00:50:56:8e:62:1d  20      dynamic             1/1/1
```


Thank you

Contact information