

A Commands

- 1G-speed-mode, on page 3
- 10G-speed-mode (FC ports), on page 4
- 10G-speed-mode (IP Storage Ports), on page 5
- 16G-speed-mode, on page 6
- aaa accounting default, on page 7
- aaa accounting logsize, on page 8
- aaa authentication dhchap default, on page 9
- aaa authentication iscsi default, on page 10
- aaa authentication login, on page 11
- aaa authentication login ascii-authentication, on page 13
- aaa authentication login chap enable, on page 15
- aaa authentication login mschapv2 enable, on page 16
- aaa authorization, on page 17
- aaa authorization ssh-certificate, on page 19
- aaa authorization ssh-publickey, on page 20
- aaa group server, on page 21
- aaa user default-role, on page 23
- abort, on page 24
- absolute-timeout, on page 25
- action cli, on page 26
- action counter, on page 27
- action event-default, on page 29
- action exception log, on page 30
- action forceshut, on page 32
- action overbudgetshut, on page 33
- action policy-default, on page 34
- action reload, on page 35
- action snmp-trap, on page 36
- action syslog, on page 37
- active equals saved, on page 39
- add-session vsan, on page 40
- add-step dynamic, on page 41
- add-step static, on page 42

- add-tgt vsan, on page 43
- add-vi vsan, on page 44
- alert-group, on page 46
- analytics port-sampling, on page 49
- analytics query, on page 51
- analytics type, on page 56
- arp, on page 58
- attach, on page 59
- attachpriv, on page 60
- attribute-admin, on page 61
- attribute failover auto, on page 63
- attribute qos, on page 64
- attributes (DMM job configuration submode), on page 65
- authentication (IKE policy configuration submode), on page 66
- authentication, on page 68
- auth-mechanism plain, on page 69
- autonomous-fabric-id (IVR service group configuration), on page 70
- autonomous-fabric-id (IVR topology database configuration), on page 72
- autonomous-fabric-id database, on page 74
- auto-volgrp, on page 76
- autozone, on page 77

1G-speed-mode

To configure 1 Gbps link speed on an IP storage interface on the Cisco MDS 24/10 port SAN Extension Module, use the **1G-speed-mode** command.

1G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
7.3(0)DY(1)	This command was introduced.

Usage Guidelines

This command will only be accepted for an interface range of whole IPStorage port groups because all interfaces in an IPStorage port group must have the same link speed. IPStorage interface port groups are as follows:

- Cisco MDS 9250i Switch: 1-2
- Cisco MDS 24/10 port SAN Extension Module: 1-4, 5-8

Examples

The following example shows how to configure 1 Gbps link speed on an IP storage interface on Cisco MDS 24/10 port SAN Extension Module:

```
switch# config terminal
switch(config)# interface IPStorage 5/1-4
switch(config-if)# 1G-speed-mode
This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on selected IPStorage
ports.If FCIP tunnels are configured please make sure max-bw <= 1000 Mbps and tcp-connections
 set to 2.
Do you wish to continue(y/n)? [n]
switch(config-if)# end
```

Related Commands

Command	Description
10G-speed-mode	Configures 10 Gbps link speed on an IP storage interface.
show ips status	Displays the operational speed of the IP storage interface.

10G-speed-mode (FC ports)

To enable 10 gig speed mode, use the 10G-speed-mode command. To disable this feature, use the no form of the command.

10G-speed-mode
no 10G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
5.x	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the 10 Gig speed mode:

```
switch# config terminal
switch(config-if)# 10G-speed-mode
switch(config-if)#
```

Related Commands

Command	Description
show interface fc x/y brief	Displays the interface brief information.
show running-config interface fc **x/y**	Displays the running configuration of the interface.

10G-speed-mode (IP Storage Ports)

To configure 10 Gbps link speed on an IP storage interface on the Cisco MDS 24/10 port SAN Extension Module, use the **10G-speed-mode** command.

10G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
7.3(0)DY(1)	This command was introduced.

Usage Guidelines

This command will only be accepted for an interface range of whole IPStorage port groups because all interfaces in an IPStorage port group must have the same link speed. IPStorage interface port groups are as follows:

- Cisco MDS 9250i Switch: 1-2
- Cisco MDS 24/10 port SAN Extension Module: 1-4, 5-8

Examples

The following example shows how to configure 10 Gbps link speed on an IP storage interface on Cisco MDS 24/10 port SAN Extension Module:

```
switch# config terminal
switch(config)# interface IPStorage 5/5-8
switch(config-if)# 10G-speed-mode
This speed change will disrupt FCIP/iSCSI traffic for 60 seconds on select IPStorage ports.
Do you wish to continue(y/n)? [n]
switch(config-if)# end
```

Related Commands

Command	Description
1G-speed-mode	Configures 1 Gbps link speed on an IP storage interface.
show ips status	Displays the operational speed of the IP storage interface.

16G-speed-mode

To enable 2, 4, 8 and 16G speed mode, use the 16G-speed-mode command. To disable this feature, use the no form of the command.

16G-speed-mode
no 16G-speed-mode

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled.

Command Modes

Interface Configuration mode.

Command History

Release	Modification
6.x	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable the 16 Gig speed mode:

```
switch# config terminal
switch(config-if)# 16G-speed-mode
switch(config-if)#
```

Related Commands

Command	Description
show interface fc x/y brief	Displays the interface brief information.
show running-config interface fc **x/y**	Displays the running configuration of the interface.

aaa accounting default

To configure the default accounting method, use the aaa accounting default command. To revert to the default local accounting, use the **no** form of the command.

aaa accounting default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}
no aaa accounting default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group authentication method. The group name is a maximum of 127 characters.
none	(Optional) No authentication, everyone permitted.
local	Specifies the local authentication method.

Command Default

Local accounting.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables accounting to be performed using remote TACACS+ servers which are members of the group called TacServer, followed by the local accounting method:

```
switch# config t
switch(config)# aaa accounting default group TacServer
```

The following example turns off accounting:

```
switch(config)# aaa accounting default none
```

The following example reverts to the local accounting (default):

```
switch(config)# no aaa accounting default group TacServer
```

Related Commands

Command	Description
show aaa accounting	Displays the configured accounting methods.

aaa accounting logsize

To set the size of the local accounting log file, use the aaa accounting logsize command to set the size of the local accounting log file. To revert to the default log file size of 250000 bytes, use the **no** form of the command.

aaa accounting logsize *integer*
no aaa accounting logsize

Syntax Description

logsize	Configures local accounting log file size (in bytes).
integer	The size limit of the local accounting log file in bytes from 0 to 250000.

Command Default

25,0000.

Command Modes

Configuration mode.

Command History

Release	Modification
1.0(2)	This command was introduced.
2.0	This command was deprecated.

Usage Guidelines

None.

Examples

The following example shows the log file size configured at 29000 bytes:

```
switch# config terminal
switch(config)# aaa accounting logsize 29000
```

Related Commands

Command	Description
show accounting logsize	Displays the configured log size.
show accounting log	Displays the entire log file.

aaa authentication dhchap default

To configure DHCHAP authentication method, use the **aaa authentication dhchap default** command in configuration mode. To revert to factory defaults, use the **no** form of the command.

aaa authentication dhchap default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}
no aaa authentication dhchap default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group name authentication method. The group name is a maximum of 127 characters.
none	(Optional) Specifies no authentication.
local	Specifies local user name authentication (default).

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all DHCHAP authentication to be performed using remote TACACS+ servers which are members of the group called TacServers, followed by the local authentication:

```
switch# config terminal
switch(config)# aaa authentication dhchap default group TacServer
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication dhcahp default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication iscsi default

To configure the iSCSI authentication method, use the **aaa authentication iscsi default** command in configuration mode. To negate the command or revert to factory defaults, use the **no** form of this command.

aaa authentication iscsi default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}
no aaa authentication iscsi default {**group** {*group-name* [**none**] | **none**} | **local** [**none**] | **none**}

Syntax Description

group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
none	(Optional) Specifies no authentication.
local	Specifies local user name authentication (default).

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

The **local** option disables other authentication methods and configures local authentication to be used exclusively.

Specify the currently configured command preceded by a **no** in order to revert to the factory default.

Examples

The following example enables all iSCSI authentication to be performed using remote TACACS+ servers which are members of the group called TacServers, followed by the local authentication:

```
switch# config terminal
switch(config)# aaa authentication iscsi default group TacServer
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication iscsi default group TacServer
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login

To configure the authentication method for a login, use the **aaa authentication login** command in configuration mode. To revert to local authentication, use the **no** form of the command.

aaa authentication login { { **default** | **oauth** | **fallback** | **error** | **local** | **group** *group-name* [**none**] | **none** | **local** [**none**] | **none** } | **console** { {**fallback** | **error** | **local** | *group-name* [**none**] | **none**} | **local** [**none**] | **none** | **error-enable** | **mschap enable**}}
no aaa authentication login { {**default** | **oauth** | **fallback** | **error** | **local** | **group** *group-name* [**none**] | **none** | **local** [**none**] | **none**} | **console** { {**fallback** | **error** | **local** | *group-name* [**none**] | **none**} | **local** [**none**] | **none** | **error-enable** | **mschap enable**}}

Syntax Description

default	Specifies the default method.
fallback	Specifies the fallback mechanism configuration error.
error	Specifies the authentication error. The maximum size is 32 characters.
local	Specifies the fallback to local authentication.
group *group-name*	Specifies the group name. The group name is a maximum of 127 characters.
none	(Optional) Sets no authentication; everyone is permitted.
local	Specifies the local authentication method.
console	Configures the console authentication login method.
error-enable	Enables login error message display.
mschap enable	Enables MS-CHAP authentication for login.

Command Default

Local user name authentication.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	Added fallback, error, and local keywords to the syntax description.
1.3(1)	This command was introduced.
3.0(1)	Added the **mschap** option.

Usage Guidelines

Use the **console** option to override the console login method.

Specify the currently configured command preceded by a **no** to revert to the factory default.

Examples

The following example shows how to configure a default method:

```
switch# config t
switch(config)# aaa authentication login default fallback error local
switch(config)#
```

The following example shows how to configure a console method:

```
switch# config t
switch(config)# aaa authentication login console fallback error local
switch(config)#
```

The following example enables all login authentication to be performed using remote TACACS+ servers, which are members of the group called TacServer, followed by the local login method:

```
switch# config t
switch(config)# aaa authentication login default group TacServer
```

The following example enables console authentication to use the group called TacServer, followed by the local login method:

```
switch(config)# aaa authentication login console group TacServer
```

The following example turns off password validation:

```
switch(config)# aaa authentication login default none
```

The following example reverts to the local authentication method (default):

```
switch(config)# no aaa authentication login default group TacServer
```

The following example enables MS-CHAP authentication for login:

```
switch(config)# aaa authentication login mschap enable
```

The following example reverts to the default authentication method for login, which is the Password Authentication Protocol (PAP):

```
switch(config)# no aaa authentication login mschap enable
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

aaa authentication login ascii-authentication

To enable ASCII authentication, use the aaa authentication login ascii-authentication command. To disable this feature, use the no form of the command.

aaa authentication login ascii-authentication
no aaa authentication login ascii-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.1(3a)	aaa authentication login password-aging enable command changed to aaa authentication login ascii-authentication.

Usage Guidelines

Password aging notification is initiated when the user authenticates to a Cisco MDS 9000 switch with a TACACS+ account. The user is notified when a password is about to expire or has expired. If the password has expired, the user is prompted to change the password.



Note As of Cisco MDS SAN-OS Release 3.2(1), only TACACS+ supports password aging notification. If you try to use RADIUS servers by enabling this feature, RADIUSs will generate a SYSLOG message and authentication will fall back to the local database. Cisco ACS TACACS+ server must have chpass enabled as well.

- Password change—You can change your password by entering a blank password.
- Password aging notification—Notifies password aging. Notification happens only if the AAA server is configured and MSCHAP and MSCHAPv2 is disabled.
- Password change after expiration—Initiates password change after the old password expires. Initiation happens from the AAA server.



Note Password aging notification fails if you do not disable MSCHAP and MSCHAPv2 authentication.

Examples

The following example shows how to enable ASCII authentication:

```
switch(config)# aaa authentication login ascii-authentication
switch#(config)#
```

Related Commands

Command	Description
show aaa authentication login ascii-authentication	Displays the configured ASCII authentication method.

aaa authentication login chap enable

To enable CHAP authentication for login, use the aaa authentication login chap enable command. To disable CHAP authentication, use the no form of the command.

aaa authentication login chap enable
no aaa authentication login chap enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 5.0(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to enable CHAP authentication for login:

```
switch(config)# aaa authentication login chap enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login CHAP	Displays CHAP authentication for login.

aaa authentication login mschapv2 enable

To enable MS-CHAPv2 authentication for login, use the aaa authentication login mschapv2 enable command. To disable MS-CHAPv2 authentication, use the no form of the command.

aaa authentication login mschapv2 enable
no aaa authentication login mschapv2 enable

Syntax Description

This command has no arguments or keywords.

Command Default

None.

Command Modes

Configuration mode.

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

MS-CHAPv2 cannot be configured when MS-CHAP or ASCII authentication is configured and also when a TACACS group is configured for authentication.

Examples

The following example shows how to enable MS-CHAPv2 authentication for login:

```
switch(config)# aaa authentication login mschapv2 enable
switch(config)#
```

Related Commands

Command	Description
show aaa authentication login mschapv2	Displays MS-CHAPv2 authentication for login.

aaa authorization

To configure authorization for a function, use the aaa authorization command. To disable authorization for a function, use the no form of the command.

aaa authorization {**commands** | **config-commands**} **default** { {[**group** *group-name*] | [**local**]} | {[**group** *group-name*] | [**none**]}}
no aaa authorization {**commands** | **config-commands**} **default** { {[**group** *group-name*] | [**local**]} | {[**group** *group-name*] | [**none**]}}

Syntax Description

commands	Specifies authorization for all exec-mode commands.
config-commands	Specifies authorization for all commands under config mode L2 and L3.
default	Specifies the default methods.
group **group-name**	(Optional) Specifies the server group and group name..
local	(Optional) Specifies the local username authentication.
none	(Optional) Specifies no authorization.

Command Default

Authorization is disabled for all actions (equivalent to the method keyword none). If the aaa authorization command for a particular authorization type is entered without a specifies named method list. The default method list is automatically applied to all interfaces or lines (where this authorization type applies for except those that have a named method list explicitly defined. A defined method list overrides the default method list if no default method list is defined, then no authorization takes place.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 4.2(1)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure authorization for a configuration command function:

```
switch(config)# aaa authorization config-commands default group tac1 local
switch(config)#
```

The following example shows how to configure authorization for a command function:

```
switch(config)# aaa authorization commands default group tac1 local none
switch(config)#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

aaa authorization ssh-certificate

To configure SSH certificate authorization, use the aaa authorization ssh-certificate command. To disable this feature, use the no form of the command.

aaa authorization ssh-certificate default [**group** | **local**]

Syntax Description

default	Specifies default SSH methods.
group	Specifies server groups.
local	Specifies local user name authentication.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1)	This command was introduced.

Usage Guidelines

None

Examples

```
The following example shows how to use local user name authentication:
switch(config)# aaa authorization ssh-certificate default local
switch(config)#
The following example shows how to specify server groups:
switch(config)# aaa authorization ssh-certificate default group ldap1
switch#
```

Related Commands

Command	Description
show aaa authorization all	Displays all authorization information.

aaa authorization ssh-publickey

To configure SSH public key authorization, use the aaa authorization ssh-publickey command. To disable this feature, use the no form of the command.

aaa authorization ssh-publickey default [**group** | **local**]
no aaa authorization ssh-publickey default [**group** | **local**]

Syntax Description

default	Specifies default SSH methods.
group	(Optional) Specifies server groups.
local	(Optional) Specifies local user name authentication.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1)	This command was introduced.

Usage Guidelines

None

Examples

```
The following example shows how to use local user name authentication:
switch(config)# aaa authorization ssh-publickey default local
switch(config)#
The following example shows how to specify server groups:
switch(config)# aaa authorization ssh-publickey default group ldap1
switch#
```

Command	Description
show aaa authorization all	Displays all authorization information.

aaa group server

To configure one or more independent server groups, use the **aaa group server** command in configuration mode. To remove the server group, use the **no** form of this command to remove the server group.

aaa group server {**radius** | **tacacs**+ | **ldap**} *group-name* **server** *server-name* **no server** *server-name* **no aaa group server** {**radius** | **tacacs**+ | **ldap**} *group-name* **server** *server-name* **no server** *server-name*

Syntax Description

radius	Specifies the RADIUS server group.
tacac**s+**	Specifies the TACACS+ server group.
ldap	Specifies LDAP server group name.
group-name	Identifies the specified group of servers with a user-defined name. The name is limited to 64 alphanumeric characters.
no server *server-name*	Specifies the server name to add or remove from the server group.

Command Default

The command is by default set to do **cert-dn-match** for ldap.

Command Modes

Sub configuration mode

Command History

Release	Modification
NX-OS 5.0(1)	Added ldap keyword to the syntax description.
1.3(1)	This command was introduced.

Usage Guidelines

You can configure these server groups at any time but they only take effect when you apply them to a AAA service using the **aaa authentication login** or the **aaa accounting** commands.

LDAP groups cannot be used for AAA accounting commands.

Examples

The following example shows how to configure an LDAP server group with adding servers to and deleting servers from the group:

```
switch# config terminal
switch(config)# aaa group server tacacs+ TacacsServer1
switch(config-tacacs+)# server ServerA
switch(config-tacacs+)# exit
switch(config)# aaa group server radius RadiusServer19
switch(config-radius)# server ServerB
switch(config-radius)# no server ServerZ
```

Related Commands

Command	Description
show aaa groups	Displays all configured server groups.
show radius-server groups	Displays configured RADIUS server groups.
show tacacs-server groups	Displays configured TACACS server groups.

aaa user default-role

To allow remote users who do not have a user role to log in to the Cisco NX-OS device through a remote authentication server using a default user role, use the **aaa user default-role** command. To disable default user roles for remote users, use the **no** form of this command.

aaa user default-role
no aaa user default-role

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

When you disable the AAA default user role feature, remote users who do not have a user role cannot log in to the device.

This command does not require a license.

Examples

This example shows how to enable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# aaa user default-role
```

This example shows how to disable default user roles for AAA authentication of remote users:

```
switch# configure terminal
switch(config)# no aaa user default-role
```

Related Commands

Command	Description
show aaa user default-role	Displays the status of the AAA default user role feature.

abort

To discard a Call Home configuration session in progress, use the **abort** command in Call Home configuration submode.

abort

Syntax Description

This command has no other arguments or keywords.

Command Default

None

Command Modes

Call Home configuration submode

Command History

Release	Modification
2.0(1b)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to discard a Call Home configuration session in progress:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# callhome
switch(config-callhome)# abort
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination.
show callhome	Displays configured Call Home information.

absolute-timeout

To set the interval for closing the connection, use the **absolute-timeout** command in line configuration mode. To restore the default, use the **no** form of this command.

absolute-timeout *minutes*
no absolute-timeout

Syntax Description

minutes	Number of minutes after which the user session will be terminated. The range is from 0 to 10000 minutes.

Command Default

No timeout interval is automatically set.

Command Modes

Line configuration

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

Use the **absolute-timeout** command to configure the EXEC to terminate when the configured number of minutes occurs on the virtual terminal (vty) line. The **absolute-timeout** command terminates the connection after the specified time period has elapsed, regardless of whether the connection is being used at the time of termination. You can specify an absolute-timeout value for each port. The user is given 20 seconds notice before the session is terminated. You can use this command along with the **logout-warning** command to notify users of an impending logout.

Examples

The following example sets an interval of 60 minutes on line 5:

```
switch# configure terminal
switch(config)# line vty 5
switch(config-line)# absolute-timeout 60
```

Related Commands

Command	Description
logout-warning	Sets and displays a warning for users about an impending forced timeout.

action cli

To configure a VSH command string to be executed when an Embedded Event Manager (EEM) applet is triggered, use the **action cli** command. To disable the VSH command string, use the no form of the command.

action number [**.number2**] **cli command1** [**command2...**] [**local**]
no action number [**.number2**] **cli command1** [**command2...**] [**local**]

Syntax Description

number	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
local	(Optional) Specifies the action that is to be executed in the same module on which the event occurs.

Command Default

None.

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure a CLI command:

```
switch# configure terminal
switch(config)# event manager applet cli-applet
switch(config-applet)# action 1.0 cli "show interface e 3/1"
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action counter

To specify a setting or modify a named counter when an Embedded Event Manager (EEM) applet is triggered, use the **action counter** command. To restore the default value to the counter, use the no form of the command.

action number [**.number2**] **counter name counter value val op** {**dec** | **inc** | **nop** | **set**}
no action number [**.number2**] **counter name counter value val op** {**dec** | **inc** | **nop** | **set**}

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
name name	The counter name can be any case-sensitive, alphanumeric string up to 32 characters.
value val	Specifies the value of the counter. The value can be an integer from 0 to 2147483647 or a substituted parameter.
op {dec | inc | nop | set}	The following operations can be performed: • dec—Decrement the counter by the specified value. • inc—Increment the counter by the specified value. • nop—Only print the specified value. • set—Set the counter to the specified value.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to set or modify the counter when the EEM counter applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet counter-applet
switch(config-applet)# action 2.0 counter name mycounter value 20 op
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action event-default

To execute the default action for the associated event, use the action event-default command. To disable the default action, use the no form of the command.

action number [**.number2**] **event-default**
no action number [**.number2**] **event-default**

Syntax Description

number . number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.2(1)	Added a note.
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

If you want to allow the triggered event to process any default actions, you must configure the EEM policy to allow the event default action statement. For example, if you match a CLI command in a match statement, you must add the event-default action statement to the EEM policy or EEM will not allow the CLI command to execute.

Examples

The following example shows how to specify that the default action of the event be performed when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.0 event-default
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action exception log

To log an exception if the specific conditions are encountered when an Embedded Event Manager (EEM) applet is triggered, use the action exception log command.

action number [**.number2**] **exception log module module syserr error devid id errtype type errcode code phylayer layer ports list harderror error** [**desc string**]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module module	Records an exception for the specified module. Enter a module word.
syserr error	Records an exception for the specified system error. Enter an error word.
devid id	Records an exception for the specified device ID. Enter an ID word.
errtype type	Records an exception for the specified error type. Enter a type word.
errcode code	Records an exception for the specified error code. Enter a code word.
phylayer layer	Records an exception for the specified physical layer. Enter a layer word.
ports list	Records an exception for the specified ports. Enter a list word.
harderror error	The reset reason is a quoted alphanumeric string up to 80 characters.
desc string	(Optional) Describes the exception logging condition.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to log an EEM applet exception:

```
switch# configure terminal
switch(config)# event manager applet exception-applet
switch(config-applet)# action 1.42 exceptionlog module 1 syserr 13 devid 1 errtype fatal
errcode 13 phylayer 2 ports 1-42 harderror 13 desc “fatal exception logging”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action forceshut

To configure a forced shutdown of a module, a crossbar, ASCII, or the entire switch when an Embedded Event Manager (EEM) applet is triggered, use the action forceshut command.

action number [**.number2**] **forceshut** [**module slot** | **xbar xbar-number**] **reset-reason string**

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot	(Optional) Specifies slot range. The range is from 1 to 10, or a substituted parameter.
xbar xbar-number	(Optional) Specifies an xbar number. The range is from 1 to 4 or a substituted parameter.
reset-reason string	Specifies reset reason. The reason is an alphanumeric string up to 80 characters.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to log an EEM applet exception:

```
switch# configure terminal
switch(config)# event manager applet exception-applet
switch(config-applet)# action 1.0 forceshut module 2 reset-reason “flapping links”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action overbudgetshut

To configure the shutdown of a module or the entire switch due to an overbudget power condition when an Embedded Event Manager (EEM) applet is triggered, use the action overbudgetshut command.

action number [.*number2*] **overbudgetshut** [**module slot** [– *slot*]]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot -slot	(Optional) Specifies the slot range: • For 6slot the range is from 1 to 6. • For 9slot the range is from 1 to 9. • For 13slot the range is from 1 to 13.

Command Default

None

Command Modes

Embedded Event Manager

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure a power overbudget shutdown of module 3-5 when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet overbudget-applet
switch(config-applet)# action 1.0 overbudgetshut module 3-5
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action policy-default

To enable the default actions of the policy being overridden, use the action policy-default command.

action number [**.number2**] **policy-default**

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to enable the default action of a policy being overridden when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.0 policy-default
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action reload

To configure the reloading or to reload the switch software when an Embedded Event Manager (EEM) applet is triggered, use the action reload command. To remove the software reload configuration, use the no form of this command.

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
module slot -slot	(Optional) Specifies the slot range. The range is from 1 to 10, or a substituted parameter.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to enable the default action of a policy being overridden when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet default-applet
switch(config-applet)# action 1.0 policy-default
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action snmp-trap

To specify the generation of a Simple Network Management Protocol (SNMP) trap when an Embedded Event Manager (EEM) applet is triggered, use the action snmp-trap command. To disable the SNMP trap, use the no form of this command.

action number [**.number2**] **snmp-trap** [**intdata1 integer** [**intdata2 integer**] [**strdata string**]]
no action number [**.number2**] **snmp-trap** [**intdata1 integer** [**intdata2 integer**] [**strdata string**]]

Syntax Description

number .number2	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
intdata1 integer	(Optional) Specifies an integer to be sent in the SNMP trap message to the SNMP agent.
intdata2 integer	(Optional) Specifies a second integer to be sent in the SNMP trap message to the SNMP agent.
strdata string	(Optional) Specifies a string to be sent in the SNMP trap message to the SNMP agent. If the string contains embedded blanks, enclose it in double quotation marks.

Command Default

None

Command Modes

Embedded Event Manager mode.

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to specify an SNMP trap to generate when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet snmp-applet
switch(config-applet)# action 1.0 snmp-trap strdata “temperature problem”
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

action syslog

To configure a syslog message to generate when an Embedded Event Manager (EEM) applet is triggered, use the action syslog command. To disable the syslog message, use the no form of this command.

action number [**.number2**] **syslog** [**priority prio-val**] **msg error-message**
no action number [**.number2**] **syslog** [**priority prio-val**] **msg error-message**

Syntax Description

number	Number can be any number up to 16 digits. The range for number2 is from 0 to 9.
priority prio-val	(Optional) Specifies the priority level of the syslog messages. If this keyword is not selected, all syslog messages are set at the informational priority level. If this keyword is selected, the priority level argument must be defined. There are three ways of defining the priority level: • Define the priority level using one of these methods: – 0—System is unusable. – 1—Immediate action is needed. – 2—Critical conditions. – 3—Error conditions. – 4—Warning conditions. – 5—Normal but significant conditions. – 6—Informational messages. This is the default. – 7—Debugging messages. • Enter the priority by selecting one of the priority keywords: –emergencies—System is unusable. – alerts—Immediate action is needed. – critical—Critical conditions. – errors—Error conditions. – warnings—Warning conditions. – notifications—Normal but significant conditions. – informational—Informational messages. This is the default. – debugging—Debugging messages.
msg error message	Specifies the error message. The message can be any quoted alphanumeric string up to 80 characters.

Command Default

None

Command Modes

Embedded Event Manager mode

Command History

Release	Modification
NX-OS 4.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure a syslog message to save when an EEM applet is triggered:

```
switch# configure terminal
switch(config)# event manager applet syslog-applet
switch(config-applet)# action 1.0 syslog priority notifications msg "cpu high"
switch(config-applet)#
```

Related Commands

Command	Description
event manager applet	Displays an applet with the Embedded Event Manager.

active equals saved

To automatically write any changes to the block, prohibit or port an address name to the IPL file, use the **active equals saved** command. To disable the configuration or to revert to factory defaults, use the **no** form of the command.

active equals saved
no active equals saved

Syntax Description

This command has no other arguments or keywords.

Command Default

Disabled.

Enabled (when a FICON VSAN is configured).

Command Modes

FICON configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.

Usage Guidelines

Enabling **active equals saved** ensures that you do not have to perform the **copy running-config startup-config** command to save the FICON configuration as well as the running configuration. If your switch or fabric consists of multiple FICON-enabled VSANs, and one of these VSANs has **active equals saved** enabled, changes made to the non-FICON configuration causes all FICON-enabled configurations to be saved to the IPL file.

The following example enables the automatic save feature for a VSAN:

```
switch(config)# ficon vsan 2
switch(config-ficon)# active equals saved
```

The following example disables the automatic save feature for this VSAN:

```
switch(config-ficon)# no active equals saved
```

Related Commands

Command	Description
copy running-config startup-config	Saves the running configuration to the startup configuration.
ficon vsan	Enables FICON on the specified VSAN.
show ficon	Displays configured FICON details.

add-session vsan

To add sessions to a job, use the add-session vsan command in configuration mode.

add-session vsan *vsan-id* {**pwwn** *tgt-pwwn* **all-luns** | **lun** *lun-id* **algorithm** *name-id*}

Syntax Description

vsan-id	Specifies the VSAN ID of the target.
pwwn tgt-pwwn	Specifies the pWWN of the target.
all-luns	Specifies all of the LUNs in the Secure Erase session.
lun lun-id	Specifies the LUN ID of the Secure Erase session.
algorithm name/id	Specifies the algorithm that should be used for the session.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None.

Examples

The following example shows how to add a VI to a specific Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-session vsan 1 pwwn 20:04:00:a0:b8:16:92:18 all-luns algorithm
RCMP
```

Related Commands

Command	Description
add-session job	Adds sessions to the job.

add-step dynamic

To add a dynamic pattern step to a specific algorithm, use the add-step dynamic command in configuration mode.

add-step dynamic [**0** | **1**]

Syntax Description

0	(Optional) Specifies that the pattern is generated using a random number generator.
1	(Optional) Specifies that the pattern is complimentary to the previous pattern.

Command Default

None

Command Modes

Configuration Secure Erase algorithm submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to add a dynamic pattern step to a specific algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 algorithm 0
switch(config-se-algo)#
switch(config-se-algo)# add-step dynamic 0
```

Related Commands

Command	Description
add-step static	Adds static pattern step to a specific algorithm.

add-step static

To add a static pattern step to a specific algorithm, use the add-step static command in configuration mode.

add-step static pattern

Syntax Description

pattern	Specifies the static pattern step. The pattern is to write ranges from 1 to 512 bytes and can consist of only characters 0 to 9 and A to F.

Command Default

None

Command Modes

Configuration Secure Erase algorithm submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to add a static step to a specific algorithm:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 algorithm 0
switch(config-se-algo)#
switch(config-se-algo)# add-step static 1
```

Related Commands

Command	Description
add-step dynamic	Adds a dynamic pattern step to a specific algorithm.

add-tgt vsan

To define target enclosure and add multiple target ports for a specific Secure Erase job, use the add-tgt vsan command in configuration mode.

add-tgt vsan vsan-id pwwn target port pwwn

Syntax Description

vsan-id	Specifies the VSAN ID of the target port added to a Secure Erase job.
pwwn target port pwwn	Specifies the port world-wide name (pWWN) of the target port.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

The target ports added to a specific job can be part of a different VSAN. The Secure Erase application creates VIs in a specific VSAN.

Note VIs and targets from different VSANs can be added to a job. A storage array may have multiple storage ports belonging to a different VSAN. You can create one job for one storage array.

Examples

The following example shows how to define a target enclosure and add multiple target ports for a specific Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-tgt vsan 1 pwwn 20:04:00:a0:b8:16:92:18
```

Related Commands

Command	Description
add-session vsans	Adds sessions to a job.
add-VI job	Adds a VI to a specific Secure Erase job.
secure-erase create job	Creates a Secure Erase job.

add-vi vsan

To add a VI to a specific Secure Erase job, use the add-vi vsan command in configuration mode.

{**add-vi vsan vsan-id all** | **pwwn VI pwwn**}

Syntax Description

vsan-id	Specifies the VSAN ID of the target where a VI exists.
all	Adds all the VSAN IDs of the target.
pwwn VI pwwn	Adds a specific VI in a given VSAN to the job.

Command Default

None

Command Modes

Configuration Secure Erase job submode

Command History

Release	Modification
6.2(1)	This command was deprecated.
3.3(1a)	This command was introduced.

Usage Guidelines

You must add at least one VI in each VSAN where a Secure Erase target is present.

All VIs that are part of the same job and the VSAN must have same target view. The same set of targets and LUNs must be exposed for all VIs in the same VSAN.



Note VI-CPP can not be added to a job. To know the WWN of the VI-CPP, please run the show isapi virtual-nport database command on SSM module.

Examples

The following example shows how to add all VIs to a given Secure Erase job:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-vi vsan 1 all
The following example shows how to add a VI to a given Secure Erase job:
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# secure-erase module 2 job 1
switch(config-se-job)# add-vi vsan 1 pwwn 2c:0d:00:05:30:00:43:64
```

Related Commands

Command	Description
add-session job	Adds sessions to the job.

Command	Description
add-VI job	Adds a VI to a specific Secure Erase job.
secure-erase create job	Creates a Secure Erase job.

alert-group

To override the default data attached to a Call Home message, use the **alert-group** command in Call Home configuration submode. To remove the customization, use the **no** form of the command.

alert-group { **All** | **Cisco-TAC** | **Crash** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **RMON permit event-id** *id* | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test** } { **script-name** *script.tar* | **user-def-cmd** *commands* }
no alert-group { **All** | **Cisco-TAC** | **Crash** | **Environmental** | **Inventory** | **License** | **Linecard-Hardware** | **RMON permit event-id** *id* | **Supervisor-Hardware** | **Syslog-group-port** | **System** | **Test** } { **script-name** *script.tar* | **user-def-cmd** *commands* }

Syntax Description

All	Specifies an alert group consisting of events from all the Call Home messages.
Cisco-TAC	Specifies an alert group consisting of events that are meant only for Cisco TAC.
Crash	Specifies an alert group consisting of events that are meant only for software crashes.
Environmental	Specifies an alert group consisting of power, fan, and temperature-related events.
Inventory	Specifies an alert group consisting of inventory status events.
License	Specifies an alert group consisting of license status events.
Linecard-Hardware	Specifies an alert group consisting of module-related events.
RMON	Specifies an alert group consisting of RMON status events.
permit	Specifies to permit only specific RMON alert event IDs and ranges.
event-id *id*	Specifies the RMON event IDs to be permitted. This can be single event id or multiple event ids and ranges. If the RMON alert is permitted then the RMON alert will generate a Call Home event. If the RMON alert is not permitted then the RMON alert will not generate a Call Home event. By default, when the RMON alert group is specified all event IDs are permitted.
Supervisor-Hardware	Specifies an alert group consisting of supervisor-related events.
Syslog-group-port	Specifies an alert group consisting of syslog port group status events.
System	Specifies an alert group consisting of software-related events.
Test	Specifies an alert group consisting of user-generated test events.
script-name *script.tar*	Maps a script to the alert group that should trigger it.
user-def-cmd *command*	Configures a CLI command for an alert-group. The maximum size is 512.

Command Default

Events from all the Call Home alert groups are permitted.

Command Modes

Call Home configuration submode (config-callhome)

Command History

Release	Modification
8.5(1)	Added the **permit event-id** *id* option for RMON alert group.
8.1(1)	Added the **Crash** keyword.
7.3(1)DY(1)	Added the **script-name** keyword.
3.0(1)	This command was introduced.

Usage Guidelines

The **user-def-cmd** argument allows you to define a command whose outputs should be attached to the Call Home message being sent. Only **show** commands can be specified and they must be associated with an alert group. Five commands can be specified per alert group. Invalid commands are rejected.

Caution The script-name option is only for use by certain customers. Do not configure it if you are not approved by Cisco to use it.

Note Make sure the destination profiles for the non-Cisco-TAC alert group, with a predefined show command, and the Cisco-TAC alert group are not the same.

Examples

The following example shows how to define a set of commands to be used for the supervisor-hardware alert group:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show version
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show environment power
switch(config-callhome)# alert-group supervisor-hardware user-def-cmd show cores
```

The following example shows how to configure RMON Call Home event alerts for event IDs 9, 15, and 33 to 89:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# alert-group RMON permit event-id 9,15,33-89
```

The following example shows how to configure a script for all Call Home alerts:

```
switch# configure terminal
switch(config)# callhome
switch(config-callhome)# alert-group all script-name m9700.tar
```

Related Commands

Command	Description
callhome	Configures the Call Home function.
callhome test	Sends a dummy test message to the configured destination(s).
show callhome	Displays configured Call Home information.

analytics port-sampling

To enable port sampling on a module, use the **analytics port-sampling** command. To disable port sampling on the module and go back to the default mode of monitoring all analytics enabled ports with a configured streaming interval, use the **no** form of this command.

analytics port-sampling module *number* **size** *number***interval** *seconds*

no analytics port-sampling module *number*

Syntax Description

module *number*	Specifies a module number.
size *number*	Specifies the number of ports to be sampled.
interval *seconds*	Specifies the port sampling interval.

Command Default

No ports are sampled.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

The Port Sampling feature is useful when the network processing unit (NPU) load is high and you cannot reduce the number of ports being monitored on a module. In such a situation, the load on the NPU can be reduced by sampling a subset of the monitored ports at a specified port sampling interval. Use the **show analytics port-sampling module** *number* command to check the NPU load.

Examples

This example shows how to enable port sampling on a module with port sampling interval of 35 seconds:

```
switch# configure terminal
switch(config)# analytics port-sampling module 2 size 12 interval 35
```

This example shows how to disable port sampling on a module and go back to the default mode of monitoring all analytics enabled ports with the configured streaming interval:

```
switch# configure terminal
switch(config)# no analytics port-sampling module 2
```

Related Commands

Command	Description
analytics query	Installs a push analytics query.
analytics type	Enables the SAN Analytics feature on an interface or a range of interfaces.

Command	Description
clear analytics	Resets all flow metrics for a view instance.
feature analytics	Enables the SAN Analytics feature on a switch.
purge analytics	Deletes a view instance and its associated flow metrics.
show analytics flow	Displays the SAN analytics type.
show analytics port-sampling	Displays the SAN analytics port sampling information.
show analytics query	Displays the SAN analytics query information.
ShowAnalytics	Displays the SAN analytics information in a tabular format.

analytics query

To install a push analytics query, use the **analytics query** command. To remove the push analytics query, use the **no** form of this command.

analytics query *"query_string"* **name** *query_name* **type periodic** [**interval** *seconds*] [**clear**] [**differential**]
no analytics query *"query_string"* **name** *query_name* **type periodic** [**interval** *seconds*] [**clear**] [**differential**]
no analytics name *query_name*

Syntax Description

"query_string"	Query syntax.
name *query_name*	Query name.
type	Analytics query type.
periodic	Periodic fetch.
interval *seconds*	Specifies the time interval when the specified metrics in the *"query_string"* should be refreshed, in seconds.
clear	Clears all the minimum, maximum, and peak flow metrics after the streaming interval.
differential	Streams only the ITL flow metrics that have changed between streaming intervals.

Command Default

None.

Command Modes

Configuration mode (config)

Command History

Release	Modification
8.3(1)	This command was modified. This command has changed from **analytics query** *"query_string"* **type timer** *timer_val* to **analytics query** *"query_string"* **name** *query_name* **type periodic** [**interval** *seconds*] [**clear**] [**differential**].
8.2(1)	This command was introduced.

Usage Guidelines

You can remove a query name using one of the following commands:

- **no analytics name** *query_name*
- **no analytics query** *"query_string"* **name** *query_name*

The **analytics query** command is a configuration of push query that periodically extracts the flow metrics. The **show analytics query** *query_name* **result** command is used to extract the recently refreshed flow metrics for a specified push query name.

The *"query_string"* is a query syntax where you can specify query semantics such as **select**, **table**, **limit**, and so on. For example, *"select all from fc-scsi.port"*. For more information, see the "Cisco MDS 9000 Series NX-OS SAN Analytics and Telemetry Configuration Guide."

Only one push query using a specific *"query_string"* is allowed at a time. Maximum of eight push queries can be installed. If you try to configure a duplicate push query (query with the same *"query string"*), the query name of the already configured push query is returned with a message indicating that the current configuration is a duplicate.

Examples

This example shows how to configure a push query when the duration to refresh the flow metrics is set to the default duration of 30 seconds:

```
switch# configure
switch(config)# analytics query 'select all from fc-scsi.scsi_initiator_itl_flow' name
inititl type periodic
```

This example shows how to display the list of configured push queries that were installed on a switch:

```
switch(config)# show analytics query all
Total queries:7
============================
Query Name :init
Query String :select all from fc-scsi.scsi_initiator
Query Type :periodic, interval 30
Query Name :targettl
Query String :select all from fc-scsi.scsi_target_tl_flow
Query Type :periodic, interval 30
Query Options :differential clear
Query Name :port
Query String :select all from fc-scsi.logical_port
Query Type :periodic, interval 30
Query Name :targetit
Query String :select all from fc-scsi.scsi_target_it_flow
Query Type :periodic, interval 30
Query Name :targetitl
Query String :select all from fc-scsi.scsi_target_itl_flow
Query Type :periodic, interval 30
Query Options :differential clear
Query Name :inititl
Query String :select all from fc-scsi.scsi_initiator_itl_flow
Query Type :periodic, interval 30
Query Name :initit
Query String :select all from fc-scsi.scsi_initiator_it_flow
Query Type :periodic, interval 30
```

This example shows an output of the push analytics query that was configured in the previous example (query name inititl):

```
switch(config)# show analytics query name inititl result
{ "values": {
        "1": {
                "port": "fc1/6",
                "vsan": "10",
                "app_id": "255",
                "initiator_id": "0xe800a0",
                "target_id": "0xd601e0",
                "lun": "0000-0000-0000-0000",
```

```
        "active_io_read_count": "0",
        "active_io_write_count": "7",
        "total_read_io_count": "0",
        "total_write_io_count": "1008608573",
        "total_seq_read_io_count": "0",
        "total_seq_write_io_count": "1",
        "total_read_io_time": "0",
        "total_write_io_time": "370765952314",
        "total_read_io_initiation_time": "0",
        "total_write_io_initiation_time": "52084968152",
        "total_read_io_bytes": "0",
        "total_write_io_bytes": "2065630357504",
        "total_read_io_inter_gap_time": "0",
        "total_write_io_inter_gap_time": "16171468343166",
        "total_time_metric_based_read_io_count": "0",
        "total_time_metric_based_write_io_count": "1008608566",
        "total_time_metric_based_read_io_bytes": "0",
        "total_time_metric_based_write_io_bytes": "2065630343168",
        "read_io_rate": "0",
        "peak_read_io_rate": "0",
        "write_io_rate": "16070",
        "peak_write_io_rate": "32468",
        "read_io_bandwidth": "0",
        "peak_read_io_bandwidth": "0",
        "write_io_bandwidth": "32912384",
        "peak_write_io_bandwidth": "66494976",
        "read_io_size_min": "0",
        "read_io_size_max": "0",
        "write_io_size_min": "2048",
        "write_io_size_max": "2048",
        "read_io_completion_time_min": "0",
        "read_io_completion_time_max": "0",
        "write_io_completion_time_min": "111",
        "write_io_completion_time_max": "9166",
        "read_io_initiation_time_min": "0",
        "read_io_initiation_time_max": "0",
        "write_io_initiation_time_min": "36",
        "write_io_initiation_time_max": "3265",
        "read_io_inter_gap_time_min": "0",
        "read_io_inter_gap_time_max": "0",
        "write_io_inter_gap_time_min": "100",
        "write_io_inter_gap_time_max": "1094718",
        "peak_active_io_read_count": "0",
        "peak_active_io_write_count": "23",
        "read_io_aborts": "0",
        "write_io_aborts": "0",
        "read_io_failures": "0",
        "write_io_failures": "0",
        "read_io_timeouts": "0",
        "write_io_timeouts": "0",
        "read_io_scsi_check_condition_count": "0",
        "write_io_scsi_check_condition_count": "0",
        "read_io_scsi_busy_count": "0",
        "write_io_scsi_busy_count": "0",
        "read_io_scsi_reservation_conflict_count": "0",
        "write_io_scsi_reservation_conflict_count": "0",
        "read_io_scsi_queue_full_count": "0",
        "write_io_scsi_queue_full_count": "0",
        "sampling_start_time": "1529993232",
        "sampling_end_time": "1529993260"
},
"2": {
        "port": "fc1/6",
        "vsan": "10",
```

```
"app_id": "255",
"initiator_id": "0xe800a1",
"target_id": "0xd601e1",
"lun": "0000-0000-0000-0000",
"active_io_read_count": "0",
"active_io_write_count": "8",
"total_read_io_count": "0",
"total_write_io_count": "1004271260",
"total_seq_read_io_count": "0",
"total_seq_write_io_count": "1",
"total_read_io_time": "0",
"total_write_io_time": "370004164726",
"total_read_io_initiation_time": "0",
"total_write_io_initiation_time": "51858511487",
"total_read_io_bytes": "0",
"total_write_io_bytes": "2056747540480",
"total_read_io_inter_gap_time": "0",
"total_write_io_inter_gap_time": "16136686881766",
"total_time_metric_based_read_io_count": "0",
"total_time_metric_based_write_io_count": "1004271252",
"total_time_metric_based_read_io_bytes": "0",
"total_time_metric_based_write_io_bytes": "2056747524096",
"read_io_rate": "0",
"peak_read_io_rate": "0",
"write_io_rate": "16065",
"peak_write_io_rate": "16194",
"read_io_bandwidth": "0",
"peak_read_io_bandwidth": "0",
"write_io_bandwidth": "32901632",
"peak_write_io_bandwidth": "33165824",
"read_io_size_min": "0",
"read_io_size_max": "0",
"write_io_size_min": "2048",
"write_io_size_max": "2048",
"read_io_completion_time_min": "0",
"read_io_completion_time_max": "0",
"write_io_completion_time_min": "114",
"write_io_completion_time_max": "9019",
"read_io_initiation_time_min": "0",
"read_io_initiation_time_max": "0",
"write_io_initiation_time_min": "37",
"write_io_initiation_time_max": "3158",
"read_io_inter_gap_time_min": "0",
"read_io_inter_gap_time_max": "0",
"write_io_inter_gap_time_min": "101",
"write_io_inter_gap_time_max": "869035",
"peak_active_io_read_count": "0",
"peak_active_io_write_count": "19",
"read_io_aborts": "0",
"write_io_aborts": "0",
"read_io_failures": "0",
"write_io_failures": "0",
"read_io_timeouts": "0",
"write_io_timeouts": "0",
"read_io_scsi_check_condition_count": "0",
"write_io_scsi_check_condition_count": "0",
"read_io_scsi_busy_count": "0",
"write_io_scsi_busy_count": "0",
"read_io_scsi_reservation_conflict_count": "0",
"write_io_scsi_reservation_conflict_count": "0",
"read_io_scsi_queue_full_count": "0",
"write_io_scsi_queue_full_count": "0",
"sampling_start_time": "1529993232",
"sampling_end_time": "1529993260"
```

```
        }
}}
```

This example shows how to remove an installed query name:

```
switch(config)# no analytics name inititl
```

Related Commands

Command	Description
analytics port-sampling	Enables port sampling on a module.
analytics type	Enables the SAN Analytics feature on an interface or a range of interfaces.
clear analytics	Resets all flow metrics for a view instance.
feature analytics	Enables the SAN Analytics feature on a switch.
purge analytics	Deletes a view instance and its associated flow metrics.
show analytics port-sampling	Displays the SAN analytics port sampling information.
show analytics query	Displays the SAN analytics query information.
show analytics type	Displays the SAN analytics type.
ShowAnalytics	Displays the SAN analytics information in a tabular format.

analytics type

To enable the SAN Analytics feature on an interface or a range of interfaces, use the **analytics type** command. To disable this feature, use the **no** form of this command.

analytics type {**fc-all** | **fc-nvme** | **fc-scsi**}
no analytics type {**fc-all** | **fc-nvme** | **fc-scsi**}

Syntax Description

fc-all	All analytics types.
fc-nvme	Non-Volatile Memory Express (NVMe) analytics type.
fc-scsi	Fibre Channel Small Computer Systems Interface (SCSI) analytics type.

Command Default

This feature is disabled by default.

Command Modes

Interface configuration submode (config-if)

Command History

Release	Modification
8.4(1)	Added the **fc-all** and **fc-nvme** keywords.
8.2(1)	This command was introduced.

Usage Guidelines

To use the SAN Analytics feature on an interface, you must first enable the SAN Analytics feature on the respective switch.

Examples

This example shows how to enable the SAN Analytics feature on an interface for the SCSI analytics type:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# analytics type fc-scsi
```

This example shows how to disable the SAN Analytics feature on an interface for the SCSI analytics type:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# no analytics type fc-scsi
```

This example shows how to enable the SAN Analytics feature on an interface for the SCSI analytics type when the NVMe analytics type is already enabled:

- This example displays that the NVMe analytics type is already enabled:

```
switch# show running-config analytics
```

```
!Command: show running-config analytics
!Running configuration last done at: Wed Mar 13 09:01:56 2019
!Time: Wed Mar 13 09:02:52 2019

version 8.4(1)
feature analytics

interface fc1/1
    analytics type fc-nvme
```

- This example displays how to enable the SCSI analytics type on a single port:

```
switch# configure terminal
switch(config)# interface fc 1/1
switch(config-if)# analytics type fc-scsi
```

- This example displays that the SCSI analytics type is enabled:

```
switch# show running-config analytics

!Command: show running-config analytics
!Running configuration last done at: Wed Mar 13 09:01:56 2019
!Time: Wed Mar 13 09:02:52 2019

version 8.4(1)
feature analytics

interface fc1/1
    analytics type fc-scsi
    analytics type fc-nvme
```

Related Commands

Command	Description
analytics port-sampling	Enables port sampling on a module.
analytics query	Installs a push analytics query.
clear analytics	Resets all flow metrics for a view instance.
feature analytics	Enables the SAN Analytics feature on a switch.
purge analytics	Deletes a view instance and its associated flow metrics.
show analytics flow	Displays the SAN analytics type.
show analytics port-sampling	Displays the SAN analytics port sampling information.
show analytics query	Displays the SAN analytics query information.
ShowAnalytics	Displays the SAN analytics information in a tabular format.

arp

To enable the Address Resolution Protocol (ARP) for the switch, use the arp command.To disable ARP for the switch, use the no form of the command.

arp *hostname*
no arp *hostname*

Syntax Description

hostname	Specifies the name of the host. Maximum length is 20 characters.

Command Default

Enabled

Command Modes

Configuration mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

None.

Examples

The following example disables the Address Resolution Protocol configured for the host with the IP address 10.1.1.1:

```
switch(config)# no arp 10.1.1.1
switch(config)#
```

Related Commands

Command	Description
clear arp	Deletes a specific entry or all entries from the ARP table.
show arp	Displays the ARP table.

attach

To connect to a specific module, use the attach command in EXEC mode.

attach module *slot-number*

Syntax Description

module *slot-number*	Specifies the slot number of the module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
1.0(2)	This command was introduced.

Usage Guidelines

You can use the attach module command to view the standby supervisor module information, but you cannot configure the standby supervisor module using this command.

You can also use the attach module command on the switching module portion of the Cisco MDS 9216 supervisor module, which resides in slot 1 of this two-slot switch.

To disconnect, use the **exit** command at the module-number# prompt, or type **$.** to forcibly terminate the attach session.

Examples

The following example connects to the module in slot 2. Note that after you connect to the image on the module using the attach module command, the prompt changes to module-number#:

```
switch# attach module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
switch#
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attachpriv

To connect to a specific ILC line card as a privilege, use the attachpriv command in EXEC mode.

attachpriv module *slot-number*

Syntax Description

module *slot-number*	Specifies the slot number of the module.

Command Default

None

Command Modes

EXEC mode

Command History

Release	Modification
3.1(3)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to connect to a specific ILC line card as a privilege:

```
switch# attachpriv module 1
Attaching to module 1 ...
To exit type 'exit', to abort type '$.'
module-1# exit
```

Related Commands

Command	Description
exit	Disconnects from the module.
show module	Displays the status of a module.

attribute-admin

To create a user with a custom role that is equivalent to the network-admin role, using which the user can modify other users' accounts (role or password), use the **attribute-admin** command. To revert to the default, use the **no rule** *rule-number* **attribute-admin** command.

This command has no arguments and keywords.

Command Default

Disabled

Command Modes

Configuration Role

Command History

Release	Modification
8.3(1)	This command was introduced.

Usage Guidelines

Note

- The **attribute-admin** rule is mutually exclusive with an existing rule. Remove the existing rule to configure the new **attribute-admin** rule.
- The Role-distribute feature will not fail while configuring the **attribute-admin** command, if an unsupported software image is present in the fabric. Instead it gets accepted, and shows as an Invalid rule for the rule which is not supported.
- The Role-distribute feature will not fail for mutually exclusive configs if an unsupported software image is present in the fabric.
- Loading Dplug does not work when the **attribute-admin** privilege.
- The **show system internal kernel memory global detail** command output under the **show tech-support details** command fails for users with the **attribute-admin** privilege.

Example: Configuring Custom Roles

The following example shows how to configure a custom role:

```
switch# configure terminal
switch(config)# role name techdocs
switch(config-role)# rule 1 attribute-admin
switch(config-role)# end
```

Create a user and associate it with the custom role.

```
switch# configure terminal
switch(config)# username user1 role techdocs password xxxxxxx
switch(config-role)# end
```

The following example shows sample output for the **show user-account** command:

```
switch# show user-account user1

user:user1
```

```
        this user account has no expiry date
        roles:techdocs
         rule 1 attribute-admin
no password set. Local login not allowed
Remote login through RADIUS is possible
```

The following example shows sample output to verify the **attribute-admin** command configuration:

```
switch# show run | sec techdocs

role name techdocs
  rule 1 attribute-admin
```

Command	Description
show tech-support details	Displays information useful to technical support when reporting a problem.
show user-account	Displays configured information about user accounts.

attribute failover auto

To configure an automatic fallback failover for a virtual device, use the attribute failover auto command. To revert to the default, use the **no** form of the command.

attribute failover auto [**fallback**]
no attribute failover auto [**fallback**]

Syntax Description

fallback	(Optional) Enables a switchback with an automatic failover.

Command Default

Disabled

Command Modes

Virtual device submode

Command History

Release	Modification
NX-OS 4.1(1b)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure an automatic failover for a specific virtual device:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name vdev1 vsan 1
switch#(config-sdv-virt-dev)# attribute failover auto
switch#(config-sdv-virt-dev)#
```

The following example shows how to configure an attribute of a virtual device:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# sdv virtual-device name vdev1 vsan 1
switch#(config-sdv-virt-dev)# attribute failover auto fallback
```

switch(config-sdv-virt-dev)#

attribute qos

To configure a QoS attribute, use the **attribute qos** command in Inter-VSAN Routing (IVR) zone configuration submode. To disable this feature, use the **no** form of this command.

attribute qos {**high** | **low** | **medium**}
no attribute qos {**high** | **low** | **medium**}

Syntax Description

high	Configures frames matching zone to get high priority.
low	Configures frames matching zone to get low priority (default).
medium	Configures frames matching zone to get medium priority.

Command Default

Disabled

Command Modes

IVR zone configuration submode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example shows how to configure an IVR zone QoS attribute to low priority:

```
switch# config terminal

Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# ivr zone name IvrZone

switch(config-ivr-zone)# attribute qos priority low
```

Related Commands

Command	Description
show ivr zone	Displays IVR zone configuration.

attributes (DMM job configuration submode)

To set the attributes of a data migration job, use the **attributes** command in DMM job configuration submode. To remove the attributes of a data migration job, use the no form of the command.

attributes job_type {**1** | **2**} **job_mode** {**1** | **2**} **job_rate** {**1** | **2** | **3** | **4**} **job_method** {**1** | **2**}
no attributes job_type {**1** | **2**} **job_mode** {**1** | **2**} **job_rate** {**1** | **2** | **3** | **4**} **job_method** {**1** | **2**}

Syntax Description

job_type 1 | 2	Specifies the job type. Specify 1 for a server type job and 2 for a storage type job.
job_mode 1 | 2	Specifies the job mode. Specify 1 for an online job and 2 for an offline job.
job_rate 1 | 2 | 3 | 4	Specifies the job rate. Specify 1 for the default rate, 2 for a slow rate, 3 for a medium rate, and 4 for a fast rate.
job_method 1|2	Specifies the job method. Specify 1 for Method 1 and 2 for Method 2.

Command Default

None

Command Modes

DMM job configuration submode

Command History

Release	Modification
3.3(1a)	This command was introduced.

Usage Guidelines

None

Examples

The following example sets the job type to storage, the job mode to online, and the job rate to fast:

```
switch# config t
Enter configuration commands, one per line. End with CNTL/Z.
switch(config)# dmm module 3 job 1 create
Started New DMM Job Configuration.
Do not exit sub-mode until configuration is complete and committed
switch(config-dmm-job)# attributes job_type 2 job_mode 1 job_rate 4 job_method 1
switch(config-dmm-job)#
```

Related Commands

Command	Description
show dmm job	Displays job information.
show dmm srvr-vt-login	Displays server VT login information.

authentication (IKE policy configuration submode)

To configure the authentication method for an IKE protocol policy, use the **authentication** command in IKE policy configuration submode. To revert to the default authentication method, use the **no** form of the command.

authentication {**pre-share** | **rsa-sig**}
no authentication {**pre-share** | **rsa-sig**}

Syntax Description

pre-share	Configures the preshared key as the authentication method.
rsa-sig	Configures RSA signatures as the authentication method.

Command Default

Preshared key.

Command Modes

IKE policy configuration submode.

Command History

Release	Modification
3.0(1)	This command was introduced.

Usage Guidelines

To use this command, enable the IKE protocol using the **crypto ike enable** command. In addition, you must configure the identity authentication mode using the fully qualified domain name (FQDN) before you can use RSA signatures for authentication. Use the **identity hostname** command for this purpose.

Examples

The following example shows how to configure the authentication method using the preshared key:

```
switch# config terminal
switch(config)# crypto ike domain ipsec
switch(config-ike-ipsec)# policy 1
switch(config-ike-ipsec-policy)# authentication pre-share
```

The following example shows how to configure the authentication method using the RSA signatures:

```
switch(config-ike-ipsec-policy)# authentication rsa-sig
```

The following example shows how to revert to the default authentication method (preshared key):

```
switch(config-ike-ipsec-policy)# no
authentication rsa-sig
```

Related Commands

Command	Description
crypto ike domain ipsec	Enters IKE configuration mode.
crypto ike enable	Enables the IKE protocol.
identity hostname	Configures the identity for the IKE protocol.

Command	Description
show crypto ike domain ipsec	Displays IKE information for the IPsec domain.

authentication

To change the authentication behavior, use the authentication command. To disable this feature, use the no form of the command.

authentication {**compare** [**password-attribute password-attribute**] | **bind-first** [**append-with-baseDN string**]}
no authentication {**compare** [**password-attribute password-attribute**] | **bind-first** [**append-with-baseDN string**]}

Syntax Description

compare	Specifies the compare option to be used for authentication.
password-attribute password-attribute	(Optional) Overides the default password attribute.The maximum length is 128 characters.
bind-first	Specifies that the client use bind and search instead of search and bind.
append-with-baseDN string	(Optional) Overrides the default string appended with baseDN.

Command Default

userPassword.

append-with-baseDN default value is (cn=$userid).

Command Modes

Configuration submode

Command History

Release	Modification
NX-OS 5.0(1)	This command was introduced.

Usage Guidelines

The password-attribute keyword provdes a method for chaning the attribute type of password.

Examples

```
The following example shows how to change the default attribute:
switch(config-ldap)# authentication compare password-attribute 1
switch(config-ldap)#
```

Related Commands

Command	Description
show aaa authentication	Displays the configured authentication methods.

auth-mechanism plain

To set the authentication mechanism as plain, use the auth-mechanism plain command in configuration mode. To disable this feature, use the no form of the command.

auth-mechanism plain
no auth-mechanism plain

Syntax Description

This command has no arguments or keywords.

Command Default

Plain.

Command Modes

Configuration mode

Command History

Release	Modification
NX-OS 5.0(1)	This command was introduced.

Usage Guidelines

None.

Examples

```
The following example shows how to set the authentication mechanism as plain:
switch(config-ldap)# auth-mechanism plain
switch(config-ldap)#
```

Related Commands

Command	Description
show ldap-server groups	Displays the configured LDAP server groups.

autonomous-fabric-id (IVR service group configuration)

To configure an autonomous fabric ID (AFID) into an IVR service group, use the autonomous-fabric-id command in IVR service group configuration submode. To remove the autonomous fabric ID, use the **no** form of the command.

autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*
no autonomous-fabric-id *afid* **vsan-ranges** *vsan-id*

Syntax Description

afid	Specifies the AFID to the local VSAN.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the service group. The range is 1 to 4093.

Command Default

None

Command Modes

IVR service group configuration submode

Command History

Release	Modification
2.1	This command was introduced.

Usage Guidelines

Before configuring an IVR service group, you must enable the following:

- IVR using the **ivr enable** command
- IVR distribution using the **ivr distribute** command
- Automatic IVR topology discovery using the **ivr vsan-topology auto command**

To change to IVR service group configuration submode, use the **ivr service-group activate command.**

Examples

The following command enters the IVR service group configuration submode and configures AFID 10 to be in IVR service group serviceGroup1:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr distribute
switch(config)# ivr vsan-topology auto
switch(config)# ivr ?
  abort                 Flushes cached data without commiting and releases the lock
  commit                Commits cached data (of all msg types) and releases the lock
  distribute            Enables/disables fabric distribution using cfs.
  enable                Enable/Disable IVR
  nat                   Enable FCID address translation (NAT) for IVR traffic
  service-group         Configure IVR servive group
  virtual-fcdomain-add  Add IVR virtual domain(s) to fcdomain list
  vsan-topology         Configure or activate VSAN topology for inter-VSAN routing
  zone                  Configure a inter vsan zone
  zoneset               Configure inter vsan routing zoneset
switch(config)# ivr service-group name serviceGroup1
switch(config-ivr-sg)# ?
```

```
service grp. membership cmds:
  afid  Enter Autonomous Fabric ID
  do    EXEC command
  exit  Exit from this submode
  no    Negate a command or set its defaults
switch(config-ivr-sg)# <TBD - Information Needed>
switch(config-ivr-sg)# afid ?
  <1-64>  Enter an autonomous fabic ID
switch(config-ivr-sg)# afid 10 ?
  vsan-ranges  Enter VSANs within this afid
switch(config-ivr-sg)# afid 10 vsan 1-4 ?
  ,     Comma
  <cr>  Carriage Return
switch(config-ivr-sg)# autonomous-fabric-id 10 vsan 1-4
IVR service group is used only when VSAN Topology is in AUTO mode
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr service-group name	Configures an IVR service group and changes to IVR service group configuration submode.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id (IVR topology database configuration)

To configure an autonomous fabric ID (AFID) into the Inter-VSAN Routing (IVR) topology database, use the autonomous-fabric-id command. To remove the fabric ID, use the **no** form of the command.

autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*
no autonomous-fabric-id *fabric-id* **switch-wwn** *swwn* **vsan-ranges** *vsan-id*

Syntax Description

fabric-id	Specifies the fabric ID for the IVR topology. **Note** For Cisco MDS SAN-OS images prior to Release 2.1(1a), the *fabric-id value is limited to 1.* For Releases 2.1(1a) and later images, the *fabric-id* range is 1 to 64.
switch-wwn *swwn*	Configures the switch WWN in dotted hex format.
vsan-ranges *vsan-id*	Configures up to five ranges of VSANs to be added to the database. The range is 1 to 4093.

Command Default

None

Command Modes

IVR topology database configuration submode

Command History

Release	Modification
1.3(1)	This command was introduced.
2.1(1a)	Modified range for *fabric-id.*

Usage Guidelines

The following rules apply to configuring AFIDs to VSANs:

- The default AFID of a VSAN is 1.
- Each VSAN belongs to one and only one AFID.
- A switch can be a member of multiple AFIDs.
- AFIDs at a switch must not share any VSAN identifier (for example, a VSAN at a switch can belong to only one AFID).
- A VSAN identifier can be reused in different AFIDs, without merging the VSANs, as long as those AFIDs do not share a switch.

You can have up to 64 VSANs (or 128 VSANs for Cisco MDS SAN-OS Release 2.1(1a) or later) in an IVR topology. Specify the IVR topology using the following information:

- The switch WWNs of the IVR-enabled switches.
- A minimum of two VSANs to which the IVR-enabled switch belongs.
- The autonomous fabric ID (AFID), which distinguishes two VSANs that are logically and physically separate, but have the same VSAN number. Cisco MDS SAN-OS Release 1.3(1) and NX-OS Release 4.1(1b) supports only one default AFID (AFID 1) and does not support non-unique VSAN IDs in the network. As of Cisco MDS SAN-OS Release 2.1(1a), you can specify up to 64 AFIDs.

Note Two VSANs with the same VSAN number but different fabric IDs are counted as two VSANs out of the 128 total VSANs allowed in the fabric.

Examples

The following command enters the configuration mode, enables the IVR feature, enters the VSAN topology database, and configures the pWWN-VSAN association for VSANs 2 and 2000:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# ivr enable
switch(config)# ivr vsan-topology database
switch(config-ivr-topology-db)# autonomous-fabric-id 1 switch 20:00:00:00:30:00:3c:5e
vsan-ranges 2,2000
```

Related Commands

Command	Description
ivr enable	Enables the Inter-VSAN Routing (IVR) feature.
ivr vsan-topology database	Configures a VSAN topology database.
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

autonomous-fabric-id database

To configure an autonomous fabric ID (AFID) database, use the autonomous-fabric-id database command. To remove the fabric AFID database, use the **no** form of the command.

autonomous-fabric-id database
no autonomous-fabric-id database

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Configuration mode

Command History

Release	Modification
2.1(1a)	This command was introduced.

Usage Guidelines

You must configure the IVR VSAN topology to auto mode, using the **ivr vsan-topology auto** command, before you can use the **autonomous-fabric-id database** command to modify the database. The **autonomous-fabric-id database** command also enters AFID database configuration submode.

Note In user-configured VSAN topology mode, the AFIDs are specified in the IVR VSAN topology configuration itself and a separate AFID configuration is not needed.

Examples

The following example shows how to create an AFID database and enters AFID database configuration submode:

```
switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# autonomous-fabric-id ?
  database  Configure autonomous fabric identifier (AFID) database
switch(config)# autonomous-fabric-id database ?
  <cr>  Carriage Return
switch(config)# autonomous-fabric-id database
AFID database is used only when VSAN Topology is in AUTO mode
switch(config-afid-db)#
```

Related Commands

Command	Description
ivr vsan-topology auto	Configures a VSAN topology for Inter-VSAN Routing (IVR) to auto configuration mode.
switch-wwn	Configures a switch WWN in the autonomous fabric ID (AFID) database

Command	Description
show autonomous-fabric-id database	Displays the contents of the AFID database.
show ivr	Displays IVR feature information.

auto-volgrp

To configure the automatic volume grouping, use the auto-volgrp command. To disable this feature, use the no form of the command.

auto-volgrp
no auto-volgrp

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Cisco SME cluster configuration submode

Command History

Release	Modification
3.2(2)	This command was introduced.

Usage Guidelines

If Cisco SME recognizes that the tape's barcode does not belong to an existing volume group, then a new volume group is created when automatic volume grouping is enabled.

Examples

The following example enables automatic volume grouping:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

The following example disables automatic volume grouping:

```
switch# config t
switch(config)# sme cluster c1
switch(config-sme-cl)# auto-volgrp
switch(config-sme-cl)#
```

Related Commands

Command	Description
show sme cluster	Displays Cisco SME cluster information.

autozone

To create zones and a zoneset for all edge devices currently logged on VSAN 1 and schedule a timer to automatically add new device logins, use the **autozone --enable** command. To disable this feature, use the **autozone --disable** command.

autozone

Syntax Description

--enable	Enables Autozone. New devices logged in be zoned automatically. This option was added to enable Autozone explicitly. Prior to Cisco MDS NX-OS Release 8.4(1), Autozone was enabled via the **autozone** command with no options. From Cisco MDS NX-OS Release 8.4(1), the **--enable** option is required to enable Autozone.
--enableautosave	Enables automatically saving of the running-configuration to the startup-configuration after making a zoning change.
--delete	Deletes zone and zoneset configurations created by Autozone for VSAN 1. **Note** This option can be used even when Autozone is disabled.
--disable	Disables Autozone. New devices logged in will not be zoned automatically. No changes will be made in the existing configuration.
--disableautosave	Disables automatically saving of the running-configuration to the startup-configuration after making a zoning change.
-help, *--help*	Provides information about the list of available keywords and arguments. **Note** This option can be used even when Autozone is disabled.
--show	Displays all possible zone configurations with the currently logged-in devices. **Note** This option can be used even when Autozone is disabled.
--showpending	Displays only pending zone configurations that are yet to be applied to the switch. **Note** This option can be used even when Autozone is disabled.
--update	Computes and applies any pending zone configurations to switch for VSAN 1. **Note** This option can be used even when Autozone is disabled.

Command Default

The Autozone feature is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
8.4(1)	Added the **--enable**, **--enableautosave** and **--disableautosave** options.
8.3(1)	This command was introduced.

Usage Guidelines

See the "Guidelines and Limitations for Autozone" section in the Cisco MDS 9000 Series NX-OS Fabric Configuration Guide.

Note If you run only the **autozone** command, you will receive a message requesting you to provide a valid argument.

Examples

The following example shows how to create zones and a zoneset on VSAN 1 automatically:

```
switch# autozone --enable
This command will create and activate single-initiator and single-target zones for all
end-devices are already logged-in automatically; that may lead to more tcam entries and
also RSCN load on network. Please use AutoZone judiciously.

AutoZone feature is enabled

Device with pwwn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or Target.
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
                AUTOZONE_JPG21190082_1

Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

The following example shows how to run the Autozone feature one time to zone all unzoned devices logged in on VSAN 1 and add them to the active zoneset of VSAN 1 without creating the Autozone scheduler job. A device without a suitable FC4 type is detected and not included in the zone configuration.

```
switch# autozone --update
Device with pwwn 10:00:00:de:fb:74:e8:31 is not registered with FC4-type Init or Target.
Hence, it will be ignored for AutoZone configuration.
Configuring zones for vsan 1
                AUTOZONE_JPG21190082_1
                AUTOZONE_JPG21190082_2
                AUTOZONE_JPG21190082_3
                AUTOZONE_JPG21190082_4
Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

The following example shows how to disable Autozone so that newly logged in devices are not zoned while still retaining the existing zone configuration:

```
switch# autozone --disable
This will disable the AutoZone feature. Do you wish to continue? [y/n]|y: y

AutoZone feature disabled successfully.
```

The following example shows how to automatically save the running-configuration to the startup-configuration after autozone makes a zoning change:

```
switch# autozone --enableautosave
```



Note Autozone must be enabled before enabling the automatic save of the Autozone configurations option.

The following example shows how to disable automatically saving of the running-configuration to the startup-configuration after autozone makes a zoning change:

```
switch# autozone --disableautosave
```

The following example shows how to delete the Autozone and zoneset created for VSAN 1:

```
switch# autozone --delete
Checking if zoneset name AUTOZONESET present on switch...[Found]
Checking if AutoZone is enabled on switch...[Disabled]

This option will only delete the zone/zoneset configurations done by AutoZone feature.
Do you wish to continue? [n]|y: y
Deleting zoneset name AUTOZONESET and all zones for vsan 1 configured by AutoZone
Deleting following zones -
   AUTOZONE_JPG21190082_1
   AUTOZONE_JPG21190082_2
   AUTOZONE_JPG21190082_3
   AUTOZONE_JPG21190082_4
Deactivating zoneset for vsan 1.
Deactivated zoneset for vsan 1.
```

The following example displays the Autozone status, the zones already created, as well as uncreated (pending) zones, by Autozone:

```
switch# autozone --show
Feature AutoZone : Enabled
AutoSave Configuration : Enabled
The possible zone/zoneset configuration with AutoZone feature for currently logged-in devices
 is :
zoneset name AUTOZONESET vsan 1
        zone name AUTOZONE_JPG21190082_1 vsan 1
                member pwwn 20:00:00:11:0d:97:00:01
                member pwwn 20:01:00:11:0d:97:01:01
        zone name AUTOZONE_JPG21190082_2 vsan 1
                member pwwn 20:00:00:11:0d:97:00:01
                member pwwn 20:01:00:11:0d:97:01:00
        zone name AUTOZONE_JPG21190082_3 vsan 1
                member pwwn 20:00:00:11:0d:97:00:00
                member pwwn 20:01:00:11:0d:97:01:01
        zone name AUTOZONE_JPG21190082_4 vsan 1
```

```
                member pwwn 20:00:00:11:0d:97:00:00
                member pwwn 20:01:00:11:0d:97:01:00
```

The following example shows how to first check what zoning Autozone would create for any unzoned devices and then apply those changes. In this example, Autozone is disabled so that zoning is updated only one time and there is no periodic zoning by Autozone.

```
switch# autozone --showpending
Feature AutoZone : Disabled
zoneset name AUTOZONESET vsan 1
        zone name AUTOZONE_JPG21190082_1 vsan 1
                member pwwn 20:00:00:11:0d:97:00:00
                member pwwn 20:01:00:11:0d:97:01:00
switch# autozone --update
Configuring zones for vsan 1
               AUTOZONE_JPG21190082_1
Configuring zoneset for vsan 1
Activating the zoneset. Please wait...
Configured zoneset AUTOZONESET for vsan 1 successfully.
```

The following example displays how to get help about the **autozone** command:

```
switch# autozone --help
usage: autozone.py [-h] [--enable] [--disable] [--update] [--delete] [--show]
                   [--showpending] [--enableautosave] [--disableautosave]

Enables AutoZone feature for vsan 1

optional arguments:
  -h, --help         show this help message and exit
  --enable           Enables AutoZone feature for vsan 1. New devices logging
                     in will be zoned automatically. No changes will be done
                     for existing configuration.
  --disable          Disables AutoZone feature for vsan 1. New devices logging
                     in will not be zoned automatically. No changes will be
                     done for existing configuration.
  --update           Computes and applies any pending AutoZone configuration
                     to switch for vsan 1
  --delete           Deletes zoneset and zones configured by AutoZone for vsan
                     1
  --show             Displays zoning configuration that will be applied if
                     autozone is enabled or if the --update option is
                     executed.
  --showpending      Displays only zoning configuration that is pending and
                     not yet applied on the switch.
  --enableautosave   Enables Auto Saving of configurations to startup.
  --disableautosave  Disables Auto Saving of configurations to startup. To
                     save these changes to startup you need to manually do
                     "copy r s ".
```

Related Commands

Command	Description
show scheduler configuration	Displays scheduler configuration information.
show scheduler schedule	Displays scheduler schedule.
show vsan	Displays information about configured VSANs.

Command	Description
show zone	Displays zone information.
show zoneset	Displays the configured zone sets.