CHAPTER 1

Using the Predefined SAN Administrator Role

This chapter describes how to use the predefined SAN administrator (san-admin) role on the Cisco Nexus 5000 Series devices.

This chapter includes the following sections:

Information About the Predefined SAN Administrator Role

The current Role-Based Access Control (RBAC) model in the Cisco Nexus 5000 Series device allows you to configure custom access roles that are based on rules. A rule can permit or deny access to a certain feature, interface, or command. For more information about RBAC, see the *Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.x*.

Limitations with the RBAC implementation previous to Release 5.2(1)N1(1) prompted the creation of a predefined SAN administrator role. These limitations were as follows:

- Some RBAC features that could be used for rule creation were not defined. This restriction caused the user to have to configure multiple rules for permitting or denying access to a certain feature.
- Mapping between the System Network Management Protocol (SNMP) object ID and the RBAC feature was missing for certain storage-area network (SAN) features. This restriction blocked SNMP management even if the role was configured to allow it.
- There was no role separation between LAN and SAN administrators.

To allow separation between SAN and local-area network (LAN) administrator responsibility, a new predefined SAN administrator role, called san-admin, has been created. You cannot modify this role, but you can use it to create your own custom role with custom defined rules that are appropriate for your specific organization. The RBAC model has also been enhanced and some new RBAC features have been defined to make rule creation easier.

SAN Administrator Role

The SAN administrator (san-admin) role allows a separation of SAN and LAN administrative tasks. With this role you can perform only Fibre Channel (FC) and Fibre Channel over Ethernet (FCoE) configuration tasks using SNMP or the command line interface (CLI), without impact any Ethernet capabilities.

With the san-admin role, you can do the following tasks:

- Configure all interfaces. There is no restriction to only Fibre Channel (FC) interfaces.
- Configure all attributes of FC unified ports other than creating or deleting ports
- Configure all virtual SAN (VSAN) information, including database and membership
- Map preconfigured virtual LANs (VLANs) for FCoE to VSANs
- Configure zoning
- Configure and manage the following SAN features:
  - FC-SP
  - FC-PORT-SECURITY
  - FCoE
  - FCoE-NPV
  - FPORT-CHANNEL-TRUNK
  - PORT-TRACK
  - FABRIC-BINDING
- Configure SNMP-related parameters, except SNMP community and SNMP users.
- Save the entire running configuration, including FC/FCoE, Ethernet interface, and other non-default configurations.
- View all other configurations (read-only privileges).

Role-Feature Mapping

The san-admin role has role-feature mapping capabilities that you can used to permit or deny access to that feature. The features that can be mapped are as follows:

- copy (copy-related commands)
- trapRegEntry (SNMP trap registry command)
- snmpTargetAddrEntry (SNMP trap target command)
- snmpTargetParamsEntry (SNMP trap target parameters command)
- fcfe (FC fe related commands)
- fcoe (FCoE related commands)
- trunk (FC port channel trunk related commands)
- fcmgmt (FC management related commands)
- port-track (Port-track related commands)
- port-security (FC port security related commands)
- fabric-binding (Fabric binding commands)

Examples

The examples in the following sections show you how to perform various tasks for the SAN administrator role:

- Configuring a User with the SAN Administrator Role, page 1-3

Configuring a User with the SAN Administrator Role

This example shows how to create a new user-id called “mynewuser” and assign that user to the san-admin role.

```
switch# configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# username mynewuser role san-admin password cisco123
switch(config)# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:mynewuser
        this user account has no expiry date
        roles:san-admin
```

Verifying the SAN Administrator Role Configuration

This example shows how to verify the “mynewuser” SAN administrator role. It also shows this user’s restricted command list, compared with the default command list.

```
Nexus 5000 Switch
login: mynewuser
Password:
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# ?
  clear      Reset functions
  configure  Enter configuration mode
  copy       Copy from one file to another
  debug      Debugging functions
  show       Show running system information
  end        Go to exec mode
  exit       Exit from command interpreter
```

Enabling the FCoE Feature for the SAN Administrator User

This example shows how to enable the FCoE feature for the “mynewuser” SAN administrator user. (You can enable only FC-related features for a SAN administrator user role.)

```
switch# configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# feature ?
  fcoe      Enable/Disable FCoE/FC feature
  fcoe-npv  Enable/Disable FCoE NPV feature
switch(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
Enabled FCoE QoS policies successfully
```

Modifying the SAN Administrator Default Role

The san-admin role is a predefined system-based role that cannot be modified. However, you can use it as a model to create a new SAN administrator role.

This example shows how to create a new SAN administrator role, called “newsan-admin” and modify the role to allow the following capabilities:

- Upgrade and downgrade of the Cisco NX-OS system and kickstart image.
- Configuration of the 5548UP base ports to Ethernet or native FC type. (A reload of the module is still required to change the port-type assignment.)

```
switch# configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# role name newsan-admin
switch(config-role)# rule 1 permit read-write feature snmp
switch(config-role)# rule 2 permit read-write feature snmpTargetParamsEntry
switch(config-role)# rule 3 permit read-write feature snmpTargetAddrEntry
switch(config-role)# rule 4 permit read-write feature trapRegEntry
switch(config-role)# rule 5 permit read-write feature interface
switch(config-role)# rule 6 permit read-write feature fabric-binding
switch(config-role)# rule 7 permit read-write feature vsanIfvsan
switch(config-role)# rule 8 permit read-write feature vsan
switch(config-role)# rule 9 permit read-write feature wwnm
switch(config-role)# rule 10 permit read-write feature zone
switch(config-role)# rule 11 permit read-write feature span
switch(config-role)# rule 12 permit read-write feature fcns
switch(config-role)# rule 13 permit read-write feature fcsp
switch(config-role)# rule 14 permit read-write feature fdmi
switch(config-role)# rule 15 permit read-write feature fspf
switch(config-role)# rule 16 permit read-write feature rscn
switch(config-role)# rule 17 permit read-write feature rmon
switch(config-role)# rule 18 permit read-write feature copy
switch(config-role)# rule 19 permit read-write feature port-security
switch(config-role)# rule 20 permit read-write feature fcoe
switch(config-role)# rule 21 permit read-write feature port-track
switch(config-role)# rule 22 permit read-write feature fcfe
switch(config-role)# rule 23 permit read-write feature fcmgmt
switch(config-role)# rule 24 permit read-write feature trunk
switch(config-role)# rule 25 permit read-write feature rdl
switch(config-role)# rule 26 permit read-write feature fcdomain
```

```
switch(config-role)# rule 27 permit read-write feature install
switch(config-role)# rule 28 permit command configuration terminal; slot 1
switch(config-role)# rule 29 permit read
```

Verifying the New SAN Administrator Role Configuration

This example assumes that a new user was created called “newsanadmin” and it was assigned the newsan-admin role. This example shows how to verify the newsan-admin RBAC role using the newsanadmin user:

```
Nexus 5000 Switch
login: newsanadmin
Password:
Bad terminal type: "xterm-256color". Will assume vt100.
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
switch# configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
switch(config)# slot 1
switch(config-slot)# port 16-32 type fc
switch(config-slot)# copy running-config startup-config
[########################################] 100%
Copy complete, now saving to disk (please wait)...
switch(config-slot)# install all kickstart
bootflash:n5000-uk9-kickstart.5.2.1.N1.0.211.bin system
bootflash:n5000-uk9.5.2.1.N1.0.211.bin

Verifying image bootflash:/n5000-uk9-kickstart.5.2.1.N1.0.211.bin for boot variable
"kickstart".
[####################] 100% -- SUCCESS

Verifying image bootflash:/n5000-uk9.5.2.1.N1.0.211.bin for boot variable "system".
```

Displaying the User Role Configurations

This example shows how to display the user roles and their configurations:

```
switch# show role

Role: network-admin
  Description: Predefined network admin role has access to all commands
  on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: network-operator
```

Examples


```
  Description: Predefined network operator role has access to all read
  commands on the switch
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: vdc-admin
  Description: Predefined vdc admin role has access to all commands within
  a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read-write

Role: vdc-operator
  Description: Predefined vdc operator role has access to all read commands
  within a VDC instance
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  1       permit  read

Role: san-admin
  Description: Predefined system role for san administrators. This role
  cannot be modified.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ------------------------------------------------------------------
  27      permit  read
  26      permit  read-write  feature             fcdomain
  25      permit  read-write  feature             rdl
  24      permit  read-write  feature             trunk
  23      permit  read-write  feature             fcmgmt
  22      permit  read-write  feature             fcfe
  21      permit  read-write  feature             port-track
  20      permit  read-write  feature             fcoe
  19      permit  read-write  feature             port-security
  18      permit  read-write  feature             copy
  17      permit  read-write  feature             rmon
  16      permit  read-write  feature             rscn
  15      permit  read-write  feature             fspf
  14      permit  read-write  feature             fdmi
  13      permit  read-write  feature             fcsp
  12      permit  read-write  feature             fcns
  11      permit  read-write  feature             span
  10      permit  read-write  feature             zone
  9       permit  read-write  feature             wwnm
  8       permit  read-write  feature             vsan
  7       permit  read-write  feature             vsanIfvsan
  6       permit  read-write  feature             fabric-binding
  5       permit  read-write  feature             interface
  4       permit  read-write  feature             trapRegEntry
  3       permit  read-write  feature             snmpTargetAddrEntry
  2       permit  read-write  feature             snmpTargetParamsEntry
  1       permit  read-write  feature             snmp

Role: priv-14
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
```

```
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------
  1       permit  read-write

Role: priv-13
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-12
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-11
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-10
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-9
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-8
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-7
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-6
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
```

```
Role: priv-5
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-4
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-3
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-2
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-1
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)

Role: priv-0
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
  10      permit  command                         traceroute6 *
  9       permit  command                         traceroute *
  8       permit  command                         telnet6 *
  7       permit  command                         telnet *
  6       permit  command                         ping6 *
  5       permit  command                         ping *
  4       permit  command                         ssh6 *
  3       permit  command                         ssh *
  2       permit  command                         enable *
  1       permit  read

Role: priv-15
  Description: This is a system defined privilege role.
  vsan policy: permit (default)
  Vlan policy: permit (default)
  Interface policy: permit (default)
  Vrf policy: permit (default)
  ----------------------------------------------------------------------
  Rule    Perm    Type        Scope               Entity
  ----------------------------------------------------------------------
```

```
permit  read-write
```