CHAPTER 1

定義済みの SAN 管理者ロールの使用方法

この章では、Cisco Nexus 5000 シリーズ デバイスでの定義済みの SAN 管理者（san-admin）ロールの使用方法について説明します。

この章の内容は、次のとおりです。

定義済みの SAN 管理者ロールに関する情報

Cisco Nexus 5000 シリーズ デバイスの最新のロールベース アクセス コントロール（RBAC）モデルでは、ルールに基づいたカスタム アクセス ロールを設定できます。ルールによって、特定の機能、インターフェイス、またはコマンドへのアクセスを許可または拒否できます。RBAC の詳細については、『*Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 5.x*』を参照してください。

リリース 5.2(1)N1(1) よりも前のリリースでは、RBAC の実装の制限により、定義済みの SAN 管理者ロールを作成する必要がありました。それらの制限は以下のとおりです。

- ルールの作成に使用できる一部の RBAC 機能が定義されていませんでした。この制限のため、ユーザは特定の機能へのアクセスを許可または拒否するために複数のルールを設定する必要がありました。
- 特定のストレージ エリア ネットワーク（SAN）機能に対する System Network Management Protocol（SNMP）オブジェクト ID と RBAC 機能間のマッピングが欠落していました。この制限のため、SNMP 管理を許可するようにロールが設定されている場合でも、SNMP 管理がブロックされていました。
- LAN 管理者と SAN 管理者の間にロールの区別がありませんでした。

SAN 管理者とローカル エリア ネットワーク（LAN）管理者間の責任を区別するために、san-admin と呼ばれる新しい定義済みの SAN 管理者ロールが作成されました。このロールは変更できません。ただし、自分の組織に適したカスタム定義のルールを設定した独自のカスタム ロールを作成するために使用できます。RBAC モデルも機能が拡張され、ルールの作成を容易にするいくつかの新しい RBAC 機能が定義されています。

SAN 管理者ロール

SAN 管理者（san-admin）ロールでは、SAN と LAN の管理作業を分離することができます。このロールでは、イーサネット機能に影響を与えることなく、SNMP またはコマンドライン インターフェイス（CLI）を使用して、ファイバ チャネル（FC）および Fibre Channel over Ethernet（FCoE）の設定作業のみ実行できます。

san-admin ロールでは、以下の作業を実行できます。

- すべてのインターフェイスを設定する。ファイバ チャネル（FC）インターフェイスのみに制限されません。
- ポートの作成または削除以外の FC 統合ポートのすべての属性を設定する
- データベースとメンバーシップを含む、仮想 SAN（VSAN）のすべての情報を設定する
- FCoE 用の定義済みの仮想 LAN（VLAN）を VSAN にマップする
- ゾーン分割を設定する
- 以下の SAN 機能を設定および管理する。
  - FC-SP
  - FC-PORT-SECURITY
  - FCoE
  - FCoE-NPV
  - FPORT-CHANNEL-TRUNK
  - PORT-TRACK
  - FABRIC-BINDING
- SNMP コミュニティと SNMP ユーザを除く、SNMP 関連のパラメータを設定する。
- FC/FCoE、イーサネット インターフェイス、および他のデフォルト以外の設定を含む、実行中の設定全体を保存する。
- その他すべての設定を表示する（読み取り専用権限）。

ロール機能マッピング

san-admin ロールでは、ロール機能マッピングを使用して、特定の機能へのアクセスを許可または拒否できます。マップできる機能は以下のとおりです。

- copy（copy 関連コマンド）
- trapRegEntry（SNMP トラップ レジストリ コマンド）
- snmpTargetAddrEntry（SNMP トラップ ターゲット コマンド）
- snmpTargetParamsEntry（SNMP トラップ ターゲット パラメータ コマンド）
- fcfe（FC fe 関連コマンド）
- fcoe（FCoE 関連コマンド）
- trunk（FC ポート チャネル トランク関連コマンド）
- fcmgmt（FC 管理関連コマンド）
- port-track（Port-track 関連コマンド）
- port-security（FC ポート セキュリティ関連コマンド）

- fabric-binding（ファブリック バインディング コマンド）

例

以下の項の例は、SAN 管理者ロールのさまざまな作業の実行方法を示しています。

SAN 管理者ロールを備えたユーザの設定

この例は、「mynewuser」という新しいユーザ ID を作成して、そのユーザを san-admin ロールに割り当てる方法を示しています。

```
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
```

SAN 管理者ロールの設定の確認

この例は、「mynewuser」SAN 管理者ロールの確認方法を示しています。また、デフォルトのコマンド リストと比較した、このユーザの制限されたコマンド リストを示しています。

```
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
```

SAN 管理者ユーザに対する FCoE 機能のイネーブル化

この例は、「mynewuser」SAN 管理者ユーザに対して FCoE 機能をイネーブルにする方法を示しています。（SAN 管理者ユーザ ロールに対する FC 関連機能のみイネーブルにできます）。

```
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
```

SAN 管理者のデフォルト ロールの変更

san-admin ロールは、定義済みのシステムベースのロールであり、変更することはできません。ただし、モデルとして使用し、新しい SAN 管理者ロールを作成することができます。

この例は、「newsan-admin」という新しい SAN 管理者ロールを作成し、このロールを変更して以下の機能を許可する方法を示しています。

- Cisco NX-OS システムおよびキックスタート イメージのアップグレードとダウングレード。
- イーサネットまたはネイティブ FC タイプ向けの 5548UP ベース ポートの設定。（ポート タイプの割り当てを変更するには、モジュールをリロードする必要があります）。

```
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
```

新しい SAN 管理者ロールの設定の確認

この例では、「newsanadmin」という新規ユーザが作成され、newsan-admin ロールが割り当てられていると想定しています。この例は、newsanadmin ユーザを使用して、newsan-admin RBAC ロールを確認する方法を示しています。

```
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".
```

ユーザ ロールの設定の表示

この例は、ユーザ ロールとそれぞれの設定の表示方法を示しています。

```
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
  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
```