U コマンド

この章では、U で始まる Cisco NX-OS セキュリティ コマンドについて説明します。

use-vrf

RADIUS、TACACS+、または LDAP サーバ グループの Virtual Routing and Forwarding（VRF; VPN ルーティングおよび転送）インスタンス名を指定するには、**use-vrf** コマンドを使用します。VRF 名を削除するには、このコマンドの **no** 形式を使用します。

use-vrf *vrf-name*

no use-vrf *vrf-name*

構文の説明

vrf-name	VRF 名。名前では、大文字と小文字が区別されます。

デフォルト

なし

コマンド モード

RADIUS サーバ グループ コンフィギュレーション
TACACS+ サーバ グループ コンフィギュレーション
LDAP サーバ グループ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	LDAP サーバ グループのサポートが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

サーバ グループに設定できるのは、1 つの VRF インスタンスだけです。

RADIUS サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server radius** コマンドを使用します。TACACS+ サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** コマンドを使用します。LDAP サーバ グループ コンフィギュレーション モードを開始するには、**aaa group server ldap** コマンドを使用します。

サーバを検索できなかった場合、**radius-server host** コマンド、**tacacs-server host** コマンド、または **ldap-server host** コマンドを使用してサーバを設定します。

（注） TACACS+ を設定する前に、**feature tacacs+** コマンドを使用するか、LDAP を設定する前に、**feature ldap** コマンドを使用する必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、RADIUS サーバ グループの VRF 名を指定する例を示します。

```
switch# config t
switch(config)# aaa group server radius RadServer
switch(config-radius)# use-vrf vrf1
```

次に、TACACS+ サーバ グループの VRF 名を指定する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# use-vrf vrf2
```

次に、TACACS+ サーバ グループから VRF 名を削除する例を示します。

```
switch# config t
switch(config)# feature tacacs+
switch(config)# aaa group server tacacs+ TacServer
switch(config-tacacs+)# no use-vrf vrf2
```

次に、LDAP サーバ グループの VRF 名を指定する例を示します。

```
switch# config t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# use-vrf vrf3
```

次に、LDAP サーバ グループから VRF 名を削除する例を示します。

```
switch# config t
switch(config)# feature ldap
switch(config)# aaa group server ldap LdapServer
switch(config-tacacs+)# no use-vrf vrf3
```

関連コマンド

コマンド	説明
aaa group server	AAA サーバ グループを設定します。
radius-server host	RADIUS サーバを設定します。
show ldap-server groups	LDAP サーバ情報を表示します。
show radius-server groups	RADIUS サーバ情報を表示します。
show tacacs-server groups	TACACS+ サーバ情報を表示します。

コマンド	説明
feature ldap	LDAP をイネーブルにします。
feature tacacs+	TACACS+ をイネーブルにします。
ldap-server host	LDAP サーバを設定します。
tacacs-server host	TACACS+ サーバを設定します。
vrf	VRF インスタンスを設定します。

user-certdn-match

検索クエリーを Lightweight Directory Access Protocol（LDAP）サーバに送信するために、証明書 DN 一致検索操作の属性名、検索フィルタ、ベース DN を設定するには、**user-certdn-match** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

user-certdn-match attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-certdn-match

構文の説明

attribute-name *attribute-name*	LDAP 検索マップの属性名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
search-filter *filter*	LDAP 検索マップ用のフィルタを指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
base-DN *base-DN-name*	LDAP 検索マップのベース指定名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

なし

コマンド モード

LDAP 検索マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、証明書 DN 一致検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-certdn-match attribute-name certificateDN
search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。

user-pubkey-match

検索クエリーを Lightweight Directory Access Protocol（LDAP）サーバに送信するために、公開キー一致検索操作の属性名、検索フィルタ、ベース DN を設定するには、**user-pubkey-match** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

user-pubkey-match attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-pubkey-match

構文の説明

attribute-name *attribute-name*	LDAP 検索マップの属性名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
search-filter *filter*	LDAP 検索マップ用のフィルタを指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
base-DN *base-DN-name*	LDAP 検索マップのベース指定名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

なし

コマンド モード

LDAP 検索マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、公開キー一致検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-pubkey-match attribute-name sshPublicKey
search-filter (&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。

user-switch-bind

検索クエリーを Lightweight Directory Access Protocol（LDAP）サーバに送信するために、ユーザスイッチグループ検索操作の属性名、検索フィルタ、ベース DN を設定するには、**user-switch-bind** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

user-switch-bind attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no user-switch-bind

構文の説明

attribute-name *attribute-name*	LDAP 検索マップの属性名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
search-filter *filter*	LDAP 検索マップ用のフィルタを指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
base-DN *base-DN-name*	LDAP 検索マップのベース指定名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

なし

コマンド モード

LDAP 検索マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、ユーザスイッチグループ検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# user-switch-bind attribute-name memberuid search-filter
(&(objectClass=posixGroup)(cn=dcgroup)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。

username

仮想デバイス コンテキスト（VDC）にユーザ アカウントを作成および設定するには、**username** コマンドを使用します。ユーザ アカウントを削除するには、このコマンドの **no** 形式を使用します。

username *user-id* [**expire** *date*] [**password** [**0** | **5**] *password*] [**role** *role-name*]

username *user-id* [**sshkey** {*key* | **file** *filename*}]

username *user-id* [**keypair generate** {**rsa** [*bits* [**force**]] | **dsa** [**force**]}]

username *user-id* [**keypair** {**export** | **import**} {**bootflash:***filename* | **volatile:***filename*} {**rsa** | **dsa**} [**force**]]

username *user-id* [**priv-lvl** *n*] [**expire** *date*] [**password** [**0** | **5**] *password*]

no username *user-id*

構文の説明

user-id	ユーザ アカウントのユーザ ID。*user-id* 引数は、最大 28 文字の英数字で、大文字と小文字が区別されます。詳細については、次の「使用上のガイドライン」を参照してください。 **（注）** Cisco NX-OS ソフトウェアでは、*user-id* 引数の文字列に特殊文字の _ . + = \ - を使用できます。
expire *date*	（任意）ユーザ アカウントが満了する日付を指定します。*date* 引数の形式は、YYYY-MM-DD です。
password	（任意）アカウントのパスワードを指定します。デフォルトでは、パスワードは設定されていません。
0	（任意）パスワードがクリア テキストであること指定します。クリア テキストのパスワードは、実行コンフィギュレーションに保存される前に暗号化されます。
5	（任意）パスワードが暗号化形式であること指定します。暗号化パスワードは、実行コンフィギュレーションに保存されるまで変更されません。
password	パスワードのストリング。パスワードは、英数字で指定します。大文字と小文字が区別され、最大文字数は 64 です。 **（注）** 出力可能なすべての ASCII 文字は、引用符で囲めば、パスワード文字列でサポートされます。
role *role-name*	（任意）ユーザ ロールを指定します。*role-name* 引数では、大文字と小文字が区別されます。
sshkey	（任意）ユーザ アカウントの SSH キーを指定します。
key	SSH キーの文字列。
file *filename*	SSH キーの文字列を含むファイル名を指定します。
keypair	SSH ユーザ キーを生成します。
generate	SSH キーペアを生成します。
rsa	RSA キーを生成します。
bits	キーの生成に使用するビット数。範囲は 1024 ～ 2048 で、デフォルト値は 1024 です。
force	以前のキーが存在する場合でも強制的にキーを生成します。
dsa	Digital System Algorithm（DSA）キーを生成します。

export	ブートフラッシュまたは揮発性ディレクトリにキーペアをエクスポートします。
import	ブートフラッシュまたは揮発性ディレクトリからキーペアをインポートします。
bootflash:*filename*	ブートフラッシュ ファイル名を指定します。
volatile:*filename*	リモート ファイル名を指定します。
priv-lvl ***n***	ユーザに割り当てる権限レベルを指定します。指定できる範囲は 0 ～ 15 です。

デフォルト

指定しない限り、ユーザ名には満了日、パスワード、または SSH キーが存在しません。

デフォルトの VDC では、作成するユーザに network-admin ロールがある場合、デフォルトのロールは network-operator で、作成するユーザに vdc-admin ロールがある場合、デフォルトのロールは vdc-operator です。

デフォルトでない VDC では、デフォルトのユーザ ロールは vdc-operator です。

デフォルトの管理ユーザ ロールは削除できません。また、デフォルトの管理ユーザ ロールの満了日の変更または network-admin ロールの削除はできません。

権限レベルを指定するには、**feature privilege** コマンドを使用して、TACACS+ サーバでのコマンド認可にロールの累積権限をイネーブルにする必要があります。デフォルトの特権レベルはありません。

このコマンドには、ライセンスは必要ありません。

コマンド モード

グローバル コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.1(1)	1024 ビット未満の RSA キーのサポートが削除されました。
5.0(2)	**keypair** キーワード オプションが追加されました。
5.0(2)	**priv-lvl** キーワード オプションが追加されました。
4.1(2)	**sshkey** キーワード オプションが追加されました。
4.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco NX-OS ソフトウェアは、admin および adminbackup の 2 つのデフォルト ユーザ アカウントを VDC に作成します。デフォルトでない VDC には、1 つのデフォルト ユーザ アカウント（admin）があります。デフォルト ユーザ アカウントを削除することはできません。

ユーザ アカウントは、VDC に対してローカルです。異なる VDC に同じユーザ ID を持つユーザ アカウントを作成できます。

注意 Cisco NX-OS ソフトウェアは、ユーザ名が TACACS+ または RADIUS によって作成されたのかローカルに作成されたのかに関係なく、すべて数字のユーザ名をサポートしていません。すべて数字の名前を持つローカル ユーザは作成できません。AAA サーバに数字だけのユーザ名が存在する場合、ログイン時に入力しても、そのユーザはログインできません。

Cisco NX-OS ソフトウェアは、**password strength-check** コマンドを使用してパスワードの強度の確認をイネーブルにした場合だけ、強力なパスワードを許可します。強力なパスワードは、次の特性を備えています。

- 長さが 8 文字以上である
- 複数の連続する文字（「abcd」など）を含んでいない
- 複数の同じ文字の繰返し（「aaabbb」など）を含んでいない
- 辞書に載っている単語を含んでいない
- 固有名詞を含んでいない
- 大文字および小文字の両方が含まれている
- 数字が含まれている

注意 ユーザ アカウントのパスワードを指定しない場合、そのユーザはアカウントにログインできない可能性があります。

このコマンドを使用するには、**feature privilege** コマンドを使用して、ロールの累積権限をイネーブルにする必要があります。

キーペアのエクスポートまたはインポート時には、パスフレーズが必要です。パスフレーズは、ユーザのエクスポートされた秘密キーを暗号化し、インポート時に復号化します。

このコマンドには、ライセンスは必要ありません。

例

次に、パスワードおよびユーザ ロールを持つユーザ アカウントを作成する例を示します。

```
switch# config t
switch(config)# username user1 password Ci5co321 role vdc-admin
```

次に、ユーザ アカウントの SSH キーを設定する例を示します。

```
switch# config t
switch(config)# username user1 sshkey file bootflash:key_file
```

次に、SSH 公開キーおよび秘密キーを生成し、それらをユーザの Cisco NX-OS デバイスのホーム ディレクトリに保存する例を示します。

```
switch# config t
switch(config)# username user1 keypair generate rsa
generating rsa key(2048 bits)......
generated rsa key
```

次に、公開キーおよび秘密キーを Cisco NX-OS デバイスのホーム ディレクトリからブートフラッシュ ディレクトリにエクスポートする例を示します。

```
switch# config t
switch(config)# username user1 keypair export bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# dir
.
.
.
951 Jul 09 11:13:59 2009 key_rsa
221 Jul 09 11:14:00 2009 key_rsa.pub
.
.
```

秘密キーは、指定したファイルとしてエクスポートされ、公開キーは、同じファイル名に .pub 拡張子を付けてエクスポートされます。

次に、エクスポートされた公開キーおよび秘密キーをブートフラッシュ ディレクトリから Cisco NX-OS デバイスのホーム ディレクトリにインポートする例を示します。

```
switch# config t
switch(config)# username user1 keypair import bootflash:key_rsa rsa
Enter Passphrase:
switch(config)# show username user1 keypair
**************************************
rsa Keys generated: Thu Jul 9 11:10:29 2009
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAxWmjJT+oQhIcvnrMbx2BmD0P8boZElTfJ
Fx9fexWp6rOiztlwODtehnjadWc6A+DE2DvYNvqsrU9TBypYDPQkR/+Y6cKubyFW
VxSBG/NHztQc3+QC1zdkIxGNJbEHyFoajzNEO8LLOVFIMCZ2Td7gxUGRZc+fbq
S33GZsCAX6v0=
bitcount:262144
fingerprint:
8d:44:ee:6c:ca:0b:44:95:36:d0:7d:f2:b5:78:74:7d
**************************************
could not retrieve dsa key information
**************************************
switch(config)#
```

秘密キーは指定したファイルとしてインポートされ、公開キーは同じファイル名に .pub 拡張子を付けてインポートされます。

次に、ユーザに権限レベル 15 を割り当てる例を示します。

```
switch# config t
switch(config)# feature privilege
switch(config)# enable secret 5 def456 priv-lvl 15
switch(config)# username user2 priv-lvl 15
```

関連コマンド

コマンド	説明
enable *level*	上位の特権レベルへのユーザの昇格をイネーブルにします。
enable secret priv-lvl	特定の権限レベルのシークレット パスワードをイネーブルにします。
feature privilege	TACACS+ サーバでのコマンド認可に対するロールの累積権限をイネーブルにします。
password strength-check	パスワードのセキュリティ強度を確認します。

コマンド	説明
show privilege	現在の特権レベル、ユーザ名、および累積権限サポートのステータスを表示します。
show user-account	ユーザ アカウントの設定を表示します。
show username	指定したユーザの公開キーを表示します。

userprofile

検索クエリーを Lightweight Directory Access Protocol（LDAP）サーバに送信するために、ユーザ プロファイル検索操作の属性名、検索フィルタ、ベース DN を設定するには、**userprofile** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

userprofile attribute-name *attribute-name* **search-filter** *filter* **base-DN** *base-DN-name*

no userprofile

構文の説明

attribute-name *attribute-name*	LDAP 検索マップの属性名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
search-filter *filter*	LDAP 検索マップ用のフィルタを指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。
base-DN *base-DN-name*	LDAP 検索マップのベース指定名を指定します。名前は、英数字で指定します。大文字と小文字が区別され、最大文字数は 128 です。

デフォルト

なし

コマンド モード

LDAP 検索マップ コンフィギュレーション

サポートされるユーザ ロール

network-admin
vdc-admin

コマンド履歴

リリース	変更箇所
5.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、LDAP をイネーブルにする必要があります。

このコマンドには、ライセンスは必要ありません。

例

次に、検索クエリーを LDAP サーバに送信するために、ユーザ プロファイル検索操作の属性名、検索フィルタ、ベース DN を設定する例を示します。

```
switch# conf t
switch(config)# ldap search-map s0
switch(config-ldap-search-map)# userprofile attribute-name description search-filter
(&(objectClass=inetOrgPerson)(cn=$userid)) base-DN dc=acme,dc=com
switch(config-ldap-search-map)#
```

関連コマンド

コマンド	説明
feature ldap	LDAP をイネーブルにします。
ldap search-map	LDAP 検索マップを設定します。
show ldap-search-map	設定された LDAP 検索マップを表示します。