U Commands

- user-certdn-match, page 2
- username, page 4
- userprofile, page 9
- user-pubkey-match, page 11
- user-switch-bind, page 13
- use-vrf, page 15

user-certdn-match

To configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-certdn-match** command. To disable this configuration, use the **no** form of this command.

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

no user-certdn-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the certificate DN match search operation in order to send a search query to the LDAP server:

```
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)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

username

To create and configure a user account in a virtual device context (VDC), use the **username** command. To remove a user account, use the **no** form of this command.

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*]

username *user-id* [**ssh-cert-dn** *dn-name*{**rsa**}]

no username *user-id*

Syntax Description

user-id	User identifier for the user account. The *user-id* argument is a case-sensitive, alphanumeric character string with a maximum length of 28 characters. For more information, see the usage guidelines section below. **Note** The Cisco NX-OS software allows these special characters in the *user-id* argument text string: (_ . + = \ -).
expire *date*	(Optional) Specifies the expire date for the user account. The format for the *date* argument is YYYY-MM-DD.
password	(Optional) Specifies a password for the account. The default is no password.
0	(Optional) Specifies that the password is in clear text. Clear text passwords are encrypted before they are saved to the running configuration.
5	(Optional) Specifies that the password is in encrypted format. Encrypted passwords are not changed before they are saved to the running configuration.
password	Password string. The password is alphanumeric, case sensitive, and has a maximum of 64 characters. **Note** All printable ASCII characters are supported in the password string if they are enclosed in quotation marks.
role *role-name*	(Optional) Specifies the user role. The *role-name* argument is case sensitive.

sshkey	(Optional) Specifies an SSH key for the user account.
key	SSH key string.
file *filename*	Specifies the name of a file that contains the SSH key string.
keypair	Generates SSH user keys.
generate	Generates SSH key-pairs.
bits	Number of bits used to generate the key. The range is from 1024 to 2048, and the default value is 1024.
force	Forces the generation of keys even if previous ones are present.
rsa	Generates Rivest, Shamir, and Adelman (RSA) keys.
export	Exports key-pairs to the bootflash or volatile directory.
import	Imports key-pairs from the bootflash or volatile directory.
ssh-cert-dn	Specifies an SSH X.509 certificate distinguished name RSA algorithm to use for authentication for an existing user account.
dn-name	Specifies the distinguished name, which can be up to 512 characters and must follow the Open SSL format.
bootflash:*filename*	Specifies the bootflash filename.
volatile:*filename*	Specifies the remote filename.
priv-lvl *n*	Specifies the privilege level to which the user is assigned. The range is from 0 to 15.

Command Default

Unless specified, usernames have no expire date, password, or SSH key.

In the default VDC, the default role is network-operator if the creating user has the network-admin role, or the default role is vdc-operator if the creating user has the vdc-admin role.

In nondefault VDCs, the default user role is vdc-operator.

You cannot delete the default admin user role. Also, you cannot change the expire date or remove the network-admin role for the default admin user role.

To specify privilege levels, you must enable the cumulative privilege of roles for command authorization on TACACS+ servers using the **feature privilege** command. There is no default privilege level.

This command does not require a license.

Command Modes

Global configuration

Command History

Release	Modification
8.0(1)	Added the **ssh-cert-dn** keyword option.
5.1(1)	Removed support for RSA keys less than 1024 bits.
5.0(2)	Added the **keypair** keyword option.
5.0(2)	Added the **priv-lvl** keyword option.
4.1(2)	Added the **sshkey** keyword option.
4.0(1)	This command was introduced.

Usage Guidelines

The Cisco NX-OS software creates two default user accounts in the VDC: admin and adminbackup. The nondefault VDCs have one default user account: admin. You cannot remove a default user account.

User accounts are local to the VDCs. You can create user accounts with the same user identifiers in different VDCs.

Caution The Cisco NX-OS software does not support all numeric usernames, whether created with TACACS+ or RADIUS, or created locally. Local users with all numeric names cannot be created. If an all numeric user name exists on an AAA server and is entered during login, the user is not logged in.

The Cisco NX-OS software accepts only strong passwords when you have password-strength checking enabled using the **password strength-check** command. The characteristics of a strong password include the following:

- At least eight characters long
- Does not contain many consecutive characters (such as “abcd”)
- Does not contain many repeating characters (such as “aaabbb”)
- Does not contain dictionary words
- Does not contain proper names
- Contains both uppercase and lowercase characters
- Contains numbers

Caution If you do not specify a password for the user account, the user might not be able to log in to the account.

To use this command, you must enable the cumulative privilege of roles using the **feature privilege** command.

A passphrase is required when you export or import the key-pair. The passphrase encrypts the exported private key for the user and decrypts it during import.

This command does not require a license.

Examples

This example shows how to create a user account with a password and a user role:

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

This example shows how to configure the SSH key for a user account:

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

This example shows how to generate the SSH public and private keys and store them in the home directory of the Cisco NX-OS device for the user:

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

This example shows how to export the public and private keys from the home directory of the Cisco NX-OS device to the bootflash directory:

```
switch# configure 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
.
.
```

The private key is exported as the file that you specify, and the public key is exported with the same filename followed by a .pub extension.

This example shows how to import the exported public and private keys from the bootflash directory to the home directory of the Cisco NX-OS device:

```
switch# configure 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)#
```

The private key is imported as the file that you specify, and the public key is imported with the same filename followed by a .pub extension.

This example shows how to assign privilege level 15 to the user:

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

This example shows how to configure X.509v3 certificate-based SSH authentication.

```
switch# configure terminal
switch(config)# username jsmith password 4Ty18Rnt
switch(config)# username jsmith ssh-cert-dn "/O = ABCcompany, OU = ABC1,
emailAddress = jsmith@ABCcompany.com, L = Metropolis, ST = New York, C = US, CN = jsmith"
rsa
switch(config)# crypto ca trustpoint tp1
switch(config-trustpoint)# crypto ca authenticate tp1
switch(config-trustpoint)# crypto ca crl request tp1 bootflash:crl1.crl
switch(config-trustpoint)# exit
switch(config)# exit
```

Related Commands

Command	Description
enable *level*	Enables a user to move to a higher privilege level.
enable secret priv-lvl	Enables a secret password for a specific privilege level.
feature privilege	Enables the cumulative privilege of roles for command authorization on TACACS+ servers.
password strength-check	Checks the password security strength.
show privilege	Displays the current privilege level, username, and status of cumulative privilege support.
show user-account	Displays the user account configuration.
show username	Displays the public key for the specified user.

userprofile

To configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **userprofile** command. To disable this configuration, use the **no** form of this command.

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

no userprofile

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user profile search operation in order to send a search query to the LDAP server:

```
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)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-pubkey-match

To configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-pubkey-match** command. To disable this configuration, use the **no** form of this command.

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

no user-pubkey-match

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the public key match search operation in order to send a search query to the LDAP server:

```
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)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

user-switch-bind

To configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the Lightweight Directory Access Protocol (LDAP) server, use the **user-switch-bind** command. To disable this configuration, use the **no** form of this command.

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

no user-switch-bind

Syntax Description

attribute-name *attribute-name*	Specifies the attribute name of the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
search-filter *filter*	Specifies the filter for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.
base-DN *base-DN-name*	Specifies the base designated name for the LDAP search map. The name is alphanumeric, case sensitive, and has a maximum of 128 characters.

Command Default

None

Command Modes

LDAP search map configuration

Command History

Release	Modification
5.0(2)	This command was introduced.

Usage Guidelines

To use this command, you must enable LDAP.

This command does not require a license.

Examples

This example shows how to configure the attribute name, search filter, and base-DN for the user-switchgroup search operation in order to send a search query to the LDAP server:

```
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)#
```

Related Commands

Command	Description
feature ldap	Enables LDAP.
ldap search-map	Configures an LDAP search map.
show ldap-search-map	Displays the configured LDAP search maps.

use-vrf

To specify a virtual routing and forwarding instance (VRF) name for a RADIUS, TACACS+, or LDAP server group, use the**use-vrf** command. To remove the VRF name, use the **no** form of this command.

use-vrf *vrf-name*

no use-vrf *vrf-name*

Syntax Description

vrf-name	VRF name. The name is case sensitive.

Command Default

None

Command Modes

RADlUS server group configurationTACACS+ server group configurationLDAP server group configuration

Command History

Release	Modification
5.0(2)	Added support for LDAP server groups.
4.0(1)	This command was introduced.

Usage Guidelines

You can configure only one VRF instance for a server group.

Use the **aaa group server radius** command to enter RADIUS server group configuration mode, the **aaa group server tacacs+** command to enter TACACS+ server group configuration mode, or the **aaa group server ldap** command to enter LDAP server group configuration mode.

If the server is not found, use the **radius-server host** command, the **tacacs-server host** command, or the **ldap-server host** command to configure the server.

Note You must use the **feature tacacs+** command before you configure TACACS+ or the **feature ldap** command before you configure LDAP.

This command does not require a license.

Examples

This example shows how to specify a VRF name for a RADIUS server group:

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

This example shows how to specify a VRF name for a TACACS+ server group:

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

This example shows how to remove the VRF name from a TACACS+ server group:

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

This example shows how to specify a VRF name for an LDAP server group:

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

This example shows how to remove the VRF name from an LDAP server group:

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

Related Commands

Command	Description
aaa group server	Configures AAA server groups.
radius-server host	Configures a RADIUS server.
show ldap-server groups	Displays LDAP server information.
show radius-server groups	Displays RADIUS server information.
show tacacs-server groups	Displays TACACS+ server information.
feature ldap	Enables LDAP.
feature tacacs+	Enables TACACS+.
ldap-server host	Configures an LDAP server.
tacacs-server host	Configures a TACACS+ server.
vrf	Configures a VRF instance.