CHAPTER 6

Configuring SSH

This chapter describes how to configure Secure Shell Protocol (SSH) on Nexus 1000V.

This chapter includes the following sections:

Information About SSH

This section includes the following topics:

SSH Server

You can use the SSH server to enable an SSH client to make a secure, encrypted connection to a Nexus 1000V. SSH uses strong encryption for authentication. The SSH server in the Nexus 1000V can interoperate with publicly and commercially available SSH clients.

TACACS+ user authentication and locally stored usernames and passwords is supported for SSH.

Send document comments to nexus1k-docfeedback@cisco.com.

SSH Client

The SSH client feature is an application that runs over the SSH protocol to provide device authentication and encryption. The SSH client enables Nexus 1000V to make a secure, encrypted connection to any device that runs the SSH server. This connection provides an encrypted outbound connection. With authentication and encryption, the SSH client produces secure communication over an insecure network.

The Nexus 1000V SSH client works with publicly and commercially available SSH servers.

SSH Server Keys

SSH requires server keys for secure communication. You can use SSH server keys for the following SSH options:

- SSH version 2 using Rivest, Shamir, and Adelman (RSA) public-key cryptography
- SSH version 2 using the Digital System Algrorithm (DSA)

Be sure to have an SSH server key-pair with the correct version before enabling the SSH service. Generate the SSH server key-pair according to the SSH client version used. The SSH service accepts two types of key-pairs for use by SSH version 2:

- The **dsa** option generates the DSA key-pair for the SSH version 2 protocol.
- The **rsa** option generates the RSA key-pair for the SSH version 2 protocol.

By default, an RSA key using 1024 bits is generated.

SSH supports the following public key formats:

- OpenSSH
- IETF Secure Shell (SECSH)
- Public Key Certificate in Privacy-Enhanced Mail (PEM)

Caution If you delete all of the SSH keys, you cannot start the SSH services.

Prerequisites for SSH

SSH has the following prerequisite:

- You have configured IP on a Layer 3 interface, out-of-band on the mgmt 0 interface, or inband on an Ethernet interface.
- Before enabling the SSH server, obtain the SSH key.

Guidelines and Limitations

- Nexus 1000V supports only SSH version 2 (SSHv2).
- SSH is enabled by default.

Note Be aware that the Nexus 1000V commands might differ from the Cisco IOS commands.

Send document comments to nexus1k-docfeedback@cisco.com.

Configuring SSH

This section includes the following topics:

Generating SSH Server Keys

Use this procedure to generate an SSH server key based on your security requirements.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- The default SSH server key is an RSA key that is generated using 1024 bits.

SUMMARY STEPS

1. **config t**
2. **no ssh server enable**
3. **ssh key** {**dsa** [**force**] | **rsa** [*bits* **[force**]]}
4. **ssh server enable**
5. **exit**
6. **show ssh key**
7. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**no ssh server enable** **Example:** `n1000v(config)# no ssh server enable`	Disables SSH.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 3	**ssh key** {**dsa** [**force**] | **rsa** [*bits* [**force**]]} **Example:** n1000v(config)# ssh key dsa force	Generates the SSH server key. The *bits* argument is the number of bits used to generate the key. The range is from 768 to 2048 and the default value is 1024. Use the **force** keyword to replace an existing key.
Step 4	**ssh server enable** **Example:** n1000v(config)# ssh server enable	Enables SSH.
Step 5	**exit** **Example:** n1000v(config)# exit n1000v#	Exits Global Configuration mode and returns you to EXEC mode.
Step 6	**show ssh key** **Example:** n1000v# show ssh key	(Optional) Displays the SSH server keys.
Step 7	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Example:

```
n1000v# config t
n1000v(config)# no ssh server enable
XML interface to system may become unavailable since ssh is disabled
n1000v(config)# ssh key dsa force
generating dsa key(1024 bits).....
.
generated dsa key
n1000v(config)# exit
n1000v# show ssh key
*************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*************************************
```

Configuring a User Account with a Public Key

Use this procedure to configure an SSH public key to log in using the SSH client without being prompted for a password. You can specify the SSH public key in one of three different formats:

- OpenSSH format
- IETF SECSH format
- Public Key Certificate in PEM format

Configuring an OpenSSH Key

Use this procedure to specify the SSH public keys in OpenSSH format for user accounts.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already generated an SSH public key in OpenSSH format.
- The user account already exists in Nexus 1000V.

SUMMARY STEPS

1. **config t**
2. **username** *username* **sshkey** *ssh-key*
3. **exit**
4. **show user-account**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**config t** **Example:** n1000v# config t n1000v(config)#	Places you in the CLI Global Configuration mode.
Step 2	**username** *username* **sshkey** *ssh-key*	Configures the SSH public key in OpenSSH format with an exiting user account. To create a user account use the following command: **username** *name* **password** *pwd*

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
	Example: `n1000v(config)# username user1 sshkey ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyK cb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5aw fVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8 QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuD YSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby /ZWx/clTYiXQR1X1VfhQ==`	

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits Global Configuration mode and returns you to EXEC mode.

Step 4	**show user-account**	(Optional) Displays the user account configuration.

	Example:
	`n1000v# show user-account`
	`user:admin`
	`this user account has no expiry date`
	`roles:network-admin`
	`user:user1`
	`this user account has no expiry date`
	`roles:network-operator`
	`ssh public key: ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdH Ha/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6 /n3FVroyRwupMki6mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EI r/0XIP1mqTsrqTsmjZ2vLk+fFzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m 9R+s6AZPuljVQbGfxPrahEu4GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1Vf hQ==`	

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Configuring IETF or PEM Keys

Use this procedure to specify the SSH public keys in IETF SECSH or PEM format for user accounts.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already generated an SSH public key in one of the following formats:
  - IETF SECSH format
  - Public Key Certificate in PEM format

SUMMARY STEPS

1. **copy** *server-file* **bootflash:***filename*
2. **config t**
3. **username** *username* **sshkey file bootflash:***filename*
4. **exit**

Send document comments to nexus1k-docfeedback@cisco.com.

5. **show user-account**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose
Step 1	**copy** *server-file* **bootflash:***filename*	Downloads the file containing the SSH key from a server. The server can be FTP, secure copy (SCP), secure FTP (SFTP), or TFTP.

Example:
```
n1000v# copy tftp://10.78.1.10/secsh_file.pub bootflash:secsh_file.pub vrf management
Trying to connect to tftp server......
Connection to server Established.
|
TFTP get operation was successful
n1000v#
```

Step 2	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 3	**username** *username* **sshkey file bootflash:***filename* **Example:** `n1000v(config)# username User1 sshkey file bootflash:secsh_file.pub`	Configures the SSH public key.

Step 4	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits Global Configuration mode and returns you to EXEC mode.

Step 5	**show user-account**	(Optional) Displays the user account configuration.

Example:
```
n1000v# show user-account
user:admin
        this user account has no expiry date
        roles:network-admin
user:user2
        this user account has no expiry date
        roles:network-operator
        ssh public key: ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXKfVhHbX2a+V0cm7CC
LUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6
mWoM6UwaGID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4GVc6sMJN
U1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==
```

Step 6	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Send document comments to nexus1k-docfeedback@cisco.com.

Starting SSH Sessions

Use this procedure to start SSH sessions using IP to connect to remote devices.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- You have already obtained the hostname and, if needed, the username, for the remote device.
- The SSH server is already enabled on the remote device.

SUMMARY STEPS

1. **ssh** [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]
   ssh6 [*username*@]{*hostname* | *username*@*hostname*} [**vrf** *vrf-name*]

DETAILED STEPS

	Command	Purpose

Step 1	**ssh** [root@]{*ip address* | *hostname*} [**vrf** *vrf-name*]
	
	Example:
	`n1000v(config)# ssh root@172.28.30.77`
	`root@172.28.30.77's password:`
	`Last login: Sat Jul 26 11:07:23 2008 from 171.70.209.64`
		Creates an SSH IP session to a remote device using IP. The default VRF is the default VRF.

Clearing SSH Hosts

Use this procedure to clear from your account the list of trusted SSH servers that were added when you downloaded a file from a server using SCP or SFTP, or when you started an SSH session to a remote host.

BSUMMARY STEPS

1. **clear ssh hosts**

DETAILED STEPS

	Command	Purpose
Step 1	**clear ssh hosts** **Example:** `n1000v# clear ssh hosts`	Clears the SSH host sessions.

Send document comments to nexus1k-docfeedback@cisco.com.

Disabling the SSH Server

Use this procedure to disable the SSH server to prevent SSH access to the switch.By default, the SSH server is enabled.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- If you disable SSH, to reenableit you mustfirst generate an SSH server key.

  See the "Generating SSH Server Keys" procedure on page 6-3.

SUMMARY STEPS

1. **config t**
2. **no ssh server enable**
3. **exit**
4. **show ssh server**
5. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**no ssh server enable**
	
	Example:
	`n1000v(config)# no ssh server enable`
	`XML interface to system may become`
	`unavailable since ssh is disabled`
	`n1000v#`
		Disables the SSH server. The default is enabled.

Step 3	**exit**
	
	Example:
	`n1000v(config)# exit`
	`n1000v#`
		Exits Global Configuration mode and returns you to EXEC mode.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose

Step 4	**show ssh server**
	
	Example:
	`n1000v# show ssh server`
	`ssh is not enabled`
	`n1000v#`
		(Optional) Displays the SSH server configuration.

Step 5	**copy running-config startup-config** **Example:** `n1000v# copy running-config startup-config`	(Optional) Copies the running configuration to the startup configuration.

Deleting SSH Server Keys

Use this procedure to delete SSH server keys after you disable the SSH server.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.
- If you disable SSH, to reenableit you mustfirst generate an SSH server key.

  See the "Generating SSH Server Keys" procedure on page 6-3.

SUMMARY STEPS

1. **config t**
2. **no ssh server enable**
3. **no ssh key** [**dsa** | **rsa**]
4. **exit**
5. **show ssh key**
6. **copy running-config startup-config**

DETAILED STEPS

	Command	Purpose

Step 1	**config t**
	
	Example:
	`n1000v# config t`
	`n1000v(config)#`
		Places you in the CLI Global Configuration mode.

Step 2	**no ssh server enable** **Example:** `n1000v(config)# no ssh server enable`	Disables the SSH server.
Step 3	**no ssh key** [**dsa** | **rsa**] **Example:** `n1000v(config)# no ssh key rsa`	Deletes the SSH server key. The default is to delete all the SSH keys.

Send document comments to nexus1k-docfeedback@cisco.com.

	Command	Purpose
Step 4	**exit** **Example:** n1000v(config)# exit n1000v#	Exits Global Configuration mode and returns you to EXEC mode.
Step 5	**show ssh key** **Example:** n1000v# show ssh key	(Optional) Displays the SSH server key configuration.
Step 6	**copy running-config startup-config** **Example:** n1000v# copy running-config startup-config	(Optional) Copies the running configuration to the startup configuration.

Example:

```
n1000v# config t
n1000v(config)# no ssh server enable
n1000v(config)# no ssh key rsa
n1000v(config)# exit
n1000v# show ssh key
*************************************
rsa Keys generated:Sun Jul 27 15:18:46 2008

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAQEAyKcb7Nv9Ki1OOId9/tdHHa/ngQujlvK5mXyL/n+DeOXK
fVhHbX2a+V0cm7CCLUkBh+BvZRmpmOVTmU/5awfVhVxMKXMiPOPBc+A6/n3FVroyRwupMki6mWoM6Uwa
GID5gsVPqFjFNSgMWtbhjo97XVKhgjFW+wOVt8QoAcrEtnwEfsnQk1EIr/0XIP1mqTsrqTsmjZ2vLk+f
FzTGYAxMvYZI+BrN47aoH2ywS7CpnODjCDXJuDYSPbc3PA8t0ghU/60m9R+s6AZPuljVQbGfxPrahEu4
GVc6sMJNU1JxmqDJkodhMArObB4Umzj7E3Rdby/ZWx/clTYiXQR1X1VfhQ==

bitcount:2048
fingerprint:
fd:ca:48:73:b9:ee:e7:86:9e:1e:40:46:f1:50:1d:44
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTC1WPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
*************************************
mcs-srvr43(config)# no ssh key rsa
mcs-srvr43(config)# show ssh key
*************************************
could not retrieve rsa key information
*************************************
dsa Keys generated:Sun Jul 27 15:20:12 2008

ssh-dss AAAAB3NzaC1kc3MAAACBALpdxLjXNS/jcCNY+F1QZV9HegxBEb0DMUmq9bSq2N+KAcvHllEh
GnaiHhqarOlcEKqhLbIbuqtKTCvfa+Y1hBIAhWVjg1UR3/M22jqxnfhnxL5YRc1Q7fcesFax0myayAIU
nXrkO5iwv9XHTu+EInRc4kJ0XrG9SxtLmDe/fi2ZAAAAFQDbRabAjZa6GfDpwjXw5smRhrElJwAAAIEA
r50yi3hHawNnb5qgYLXhN+KA8XJF753eCWHtMw7NR8fz6fjQ1R2J97UjjGuQ8DvwpGeNQ5S+AuIo0rGq
```

Send document comments to nexus1k-docfeedback@cisco.com.

```
svdg7TTecBcbgBOnR7Fs2+W5HiSVEGbvj1xaeK8fkNE6kaJumBB343b8Rgj0G97MP/os1GfkEqmX9glB
0IOM2mgHHyoAAACAfRir27hHy+fw8CxPlsK0R6cFhxYyd/qYYogXFKYIOPxpLoYrjqODeOFThU7TJuBz
aS97eXiruzbffHwzUGfXgmQT5o9IMZRTClWPA/5Ju4O9YABYHccUghf0W+QtgGOT6FOSvBh8uOV0kcHC
GMJAP8omphauZJlc+wgFxhnkyh4=

bitcount:1024
fingerprint:
44:91:32:1f:7a:d1:83:3c:f3:5e:db:53:0a:2d:ce:69
************************************
mcs-srvr43(config)# no ssh key dsa
mcs-srvr43(config)# show ssh key
************************************
could not retrieve rsa key information
************************************
could not retrieve dsa key information
************************************
no ssh keys present. you will have to generate them
************************************
n1000v#
```

Clearing SSH Sessions

Use this procedure to clear SSH sessions from the device.

BEFORE YOU BEGIN

Before beginning this procedure, you must know or do the following:

- You are logged in to the CLI in EXEC mode.

SUMMARY STEPS

1. **show users**
2. **clear line** *vty-line*
3. **show users**

DETAILED STEPS

	Command	Purpose
Step 1	**show users** **Example:** `n1000v# show users`	Displays user session information.
Step 2	**clear line** *vty-line* **Example:** `n1000v# clear line 0`	Clears a user SSH session.
Step 3	**show users** **Example:** `n1000v# show users`	Displays user session information.

Send document comments to nexus1k-docfeedback@cisco.com.

```
Example:
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/0        Jul 28 09:49 00:02       28556 (10.21.148.122)
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
n1000v# clear line 0
n1000v# show users
NAME     LINE         TIME         IDLE          PID COMMENT
admin    tty1         Jul 25 19:13  old         2867
admin    pts/1        Jul 28 09:46   .         28437 (::ffff:10.21.148.122)*
mcs-srvr43(config)#
```

Verifying the SSH Configuration

To display the SSH configuration information, use one of the following commands:

Command	Purpose
show ssh key [dsa | rsa]	Displays SSH server key-pair information.
show running-config security [**all**]	Displays the SSH and user account configuration in the running configuration. The **all** keyword displays the default values for the SSH and user accounts.
show ssh server	Displays the SSH server configuration.

```
Example:
n1000v# show ssh key rsa
**************************************
rsa Keys generated:Mon Jul 28 09:49:18 2008

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAGEAv0a4p6VulQMW4AMgoPfApB2KegF3QTojCzed51iVQnEkNglnM7A/oEIZAtlVLY
k/PEzt+ED7lPal/8pomaqjgRxHSeK2gw1cJKSDbcYH5na8uox1Hr50eK0q2+ZfvMqV

bitcount:768
fingerprint:
76:6c:a0:5c:79:a6:ae:3d:cb:27:a1:86:62:fa:09:df
**************************************
```

SSH Example Configuration

To configure SSH with an OpenSSH key, follow these steps:

Step 1 Disable the SSH server.

```
n1000v# config t
n1000v(config)# no ssh server enable
```

Step 2 Generate an SSH server key.

```
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
.generated rsa key
```

Send document comments to nexus1k-docfeedback@cisco.com.

Step 3 Enable the SSH server.

```
n1000v(config)# ssh server enable
```

Step 4 Display the SSH server key.

```
n1000v(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007

ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=

bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*************************************
could not retrieve dsa key information
*************************************
```

Step 5 Specify the SSH public key in OpenSSH format.

```
n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
```

Step 6 Save the configuration.

```
n1000v(config)# copy running-config startup-config
```

Example:

```
n1000v# config t
n1000v(config)# no ssh server enable
n1000v(config)# ssh key rsa
generating rsa key(1024 bits).....
n1000v(config)# ssh server enable
n1000v(config)# show ssh key
rsa Keys generated:Sat Sep 29 00:10:39 2007
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAvWhEBsF55oaPHNDBnpXOTw6+/OdHoLJZKr+MZm99n2U0
ChzZG4svRWmHuJY4PeDWl0e5yE3g3EO3pjDDmt923siNiv5aSga60K36lr39HmXL6VgpRVn1XQFiBwn4
na+H1d3Q0hDt+uWEA0tka2uOtXlDhliEmn4HVXOjGhFhoNE=
bitcount:1024
fingerprint:
51:6d:de:1c:c3:29:50:88:df:cc:95:f0:15:5d:9a:df
*************************************
could not retrieve dsa key information
*************************************

n1000v(config)# username User1 sshkey ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAy19oF6QaZl9G+3f1XswK3OiW4H7YyUyuA50rv7gsEPjhOBYmsi6PAVKui1nIf/
DQhum+lJNqJP/eLowb7ubO+lVKRXFY/G+lJNIQW3g9igG30c6k6+XVn+NjnI1B7ihvpVh7dLddMOXwOnXHYshXmSiH
3UD/vKyziEh5S4Tplx8=
n1000v(config)# copy running-config startup-config
[########################################] 100%
n1000v(config)#
```

Send document comments to nexus1k-docfeedback@cisco.com.

Default Settings

The following table lists the default settings for SSH.

Parameters	Default
SSH server	Enabled.
SSH server key	RSA key generated with 1024 bits.
RSA key bits for generation	1024.

Additional References

For additional information related to implementing RBAC, see the following sections:

- Related Documents, page 6-15
- Standards, page 6-15

Related Documents

Related Topic	Document Title
CLI	*Cisco Nexus 1000V Getting Started Guide, Release 4.0(4)SV1(1)*
Telnet	Chapter 7, "Configuring Telnet"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

Feature History for SSH

This section provides the SSH release history.

Feature Name	Releases	Feature Information
SSH	4.0	This feature was introduced.

Send document comments to nexus1k-docfeedback@cisco.com.