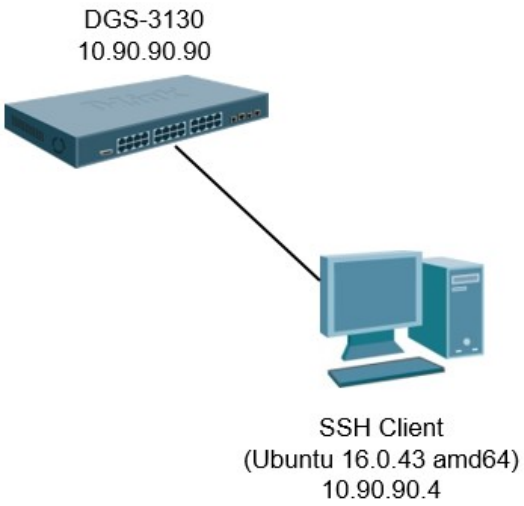
How to use SSH host-based key authentication on DGS-3130

[Topology]



[Overview]

1) İnstall OpenSSH Server on Ubuntu 16.0.43 OS
2) Copy SSH host-based key to Switch
3) Configure SSH on Switch
4) Access to Switch via SSH Client

[Configure]

Step 1. Install Open SSH Server on Ubuntu 16.0.43 OS

1. Install openssh server on ubuntu 16.0.43

```
root@ubuntu:~# apt-get install openssh-server
Do you want to continue? [Y/n] Y
```

[Note.]
After installing open ssh server successfully, it will auto generate a SSH host key in the openssh folder.

```
root@ubuntu:~# cd /etc/ssh/
root@ubuntu:/etc/ssh# ls
moduli              ssh_host_dsa_key.pub
ssh_host_ed25519_key.pub
ssh_config          ssh_host_ecdsa_key      ssh_host_rsa_key
sshd_config         ssh_host_ecdsa_key.pub  ssh_host_rsa_key.pub
ssh_host_dsa_key    ssh_host_ed25519_key    ssh_import_id
```

2. Modify ssh config file and enable ssh host-based authentication.

```
root@ubuntu:/etc/ssh# vim /etc/ssh/ssh_config
PasswordAuthentication yes
HostbasedAuthentication yes
PubkeyAuthentication yes
EnableSSHKeysign yes
PubkeyAcceptedKeyTypes=+ssh-dss
```

3. Restart ssh function

```
root@ubuntu:/etc/ssh# service ssh restart
```

Step 2. Copy SSH host-based key to Switch

1. Copy ssh host key to Desktop

```
root@ubuntu:~# cd /etc/ssh/
root@ubuntu:/etc/ssh# ls
moduli              ssh_host_dsa_key.pub
ssh_host_ed25519_key.pub
ssh_config          ssh_host_ecdsa_key      ssh_host_rsa_key
sshd_config         ssh_host_ecdsa_key.pub  ssh_host_rsa_key.pub
ssh_host_dsa_key    ssh_host_ed25519_key    ssh_import_id

root@ubuntu:/etc/ssh# cp ssh_host_rsa_key.pub ~james/Desktop/
```

2. Copy ssh host key to switch via tftp server

```
copy tftp: //10.90.90.7/ssh_host_rsa_key.pub flash:
ssh_host_rsa_key.pub
```

Step 3. Configure SSH on Switch

Configure switch's ssh host-based authentication commands

```
DGS-3130 commands:
############################################################

config t
username james privilege 15
ssh user james authentication-method hostbased
c:/ssh_host_rsa_key.pub host-name ubuntu 10.90.90.4
exit
crypto key generate rsa
768
config t
ip ssh server

############################################################
```

Note. The host-name "ubuntu" should be the same as

Host name of SSH-client. (E.g. root@**ubuntu**:~#)

Step 4. Access to Switch via SSH Client

Connected as topology, and setup ssh session via Ubuntu 16.0.43

```
root@ubuntu:/etc/ssh# logout
james@ubuntu:~$ ssh -v james@10.90.90.90
```

[Result]

It can be successful to login Switch CLI via SSH host based authentication session.

===LOG=====================================

```
root@ubuntu:~# ssh -v james@10.90.90.90
OpenSSH_7.2p2 Ubuntu-4ubuntu2.2, OpenSSL 1.0.2g  1 Mar 2016
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Connecting to 10.90.90.90 [10.90.90.90] port 22.
debug1: Connection established.
debug1: key_load_private_cert: No such file or directory
debug1: key_load_private_cert: No such file or directory
debug1: key_load_private_cert: No such file or directory
debug1: key_load_private_cert: No such file or directory
debug1: permanently_set_uid: 0/0
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_rsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_rsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_dsa type -1
debug1: key_load_public: No such file or directory
```

```
debug1: identity file /root/.ssh/id_dsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /root/.ssh/id_ed25519-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2
debug1: Remote protocol version 2.0, remote software version OpenSSH_6.8
debug1: match: OpenSSH_6.8 pat OpenSSH* compat 0x04000000
debug1: Authenticating to 10.90.90.90:22 as 'james'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ssh-rsa
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit>
compression: none
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit>
compression: none
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ssh-rsa
SHA256:6qIY8FqRQ16kMqt49Amv9TsPlFaJchSID5h2Jye46+4
debug1: Host '10.90.90.90' is known and matches the RSA host key.
debug1: Found key in /root/.ssh/known_hosts:1
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS received
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: hostbased
debug1: Next authentication method: hostbased
```

```
debug1: userauth_hostbased: trying hostkey ecdsa-sha2-nistp256
SHA256:3CMGv5woFKV32H6AjfGC8AOxcBI85xN7uNe/VWca/DE

get_socket_address: getnameinfo 8 failed: Temporary failure in name resolution

debug1: Authentications that can continue: hostbased

debug1: userauth_hostbased: trying hostkey ssh-ed25519
SHA256:66LHoiVrzy69wqi0gU+ppMTu/7x4UG1wAffVuOD2eo8

get_socket_address: getnameinfo 8 failed: Temporary failure in name resolution

debug1: Authentications that can continue: hostbased

debug1: userauth_hostbased: trying hostkey ssh-rsa
SHA256:bD4f4b/0BwNCNgbGdUuvC/PC4uPze6USWPXX6BiC9eM

get_socket_address: getnameinfo 8 failed: Temporary failure in name resolution

debug1: Authentication succeeded (hostbased).

Authenticated to 10.90.90.90 ([10.90.90.90]:22).

debug1: channel 0: new [client-session]

debug1: Requesting no-more-sessions@openssh.com

debug1: Entering interactive session.

debug1: pledge: network

debug1: client_input_global_request: rtype hostkeys-00@openssh.com want_reply 0


                DGS-3130-54PS Gigabit Ethernet Switch


                        Command Line Interface

                          Firmware: 1.01.B009

          Copyright(C) 2016 D-Link Corporation. All rights reserved.


Switch#


Switch#

Switch#configure t
```

==========

[Attached file]

1) SSH Client Log:

Ubuntu16.0.4_log.txt

2) Switch Log:

DUT setup log .txt

3) SSH Host key file:

ssh_host_rsa_key.pub

4) Switch config file:

ssh_config