Troubleshoot SSH Public Key Authentication StarOS

Contents

Introduction

This document describes how to troubleshoot SSH/SFTP public key authentication configuration from the packet gateway to external servers in StarOS.

Problem

If warning or failure messages appear after public key generation and configurations, then check the next section for possible remedies.

Solution

- ### Are SSH client keys present?

Check for SSH Public key using Exec CLI “show ssh client key”. If keys are not present, generate them using set of CLIs present in section "Generating SSH Keys" of reference document in the reference section below.

And then, authenticate the keys to be pushed to remote server using Exec CLI “push ssh-key <hostname> user <username> [context <contextname>].

- ### Have you pushed Client SSH key?

If Client SSH public key is not present in remote server’s authorized list, then push public key to remote server using Exec CLI “push ssh-key <hostname> user <username> [context <contextname>].

- ### Does remote server supports Public Key Authentication?

Make sure remote server supports public key authentication by checking remote server’s SSHD configuration file. Make sure “PubkeyAuthentication yes” parameter is present in SSHD configuration file.

If there are any changes in parameters/values in the SSHD configuration file, to be effective, the SSHD server needs to be restarted.

- **Are you seeing any warning or failure messages?**

“Warning: Could not find ID file”:

This indicates that SSH Client Keys ID files are missing due to internal error or manual deletion of files. Actions to recover are as follows.

- If o/p of Exec CLI “show ssh client key [type v2-rsa]” is showing v2-rsa public key in “hex” and “bubble-babble” format and additionally giving failure message “Failure: Unable to find ssh public key file”, then,
    1. Obtain/grep the SSH client key (ssh key <key> len <keylen> type v2-rsa) from SSH client configuration (“client ssh”) section of Exec CLI “show configuration” o/p.
    2. Reconfigure same SSH key value by entering into “config-ssh” CLI mode.
    3. Example:

```
<#root>

[local]swch#

show ssh client key type v2-rsa


v2-rsa public key:
    ximal-hyges-hovul-vonuk-lacyl-pezuk-nifad-lulon-raviv-cypal-vyxox
    60:75:d1:c5:7a:7e:e7:67:86:7a:7d:69:0e:27:5d:9b:78:e1:69:7e
"Failure: Unable to find ssh public key file"

[local]swch#

show configuration



config


    ….


client ssh




ssh key +KEYVALUE len KEYLEN type v2-rsa




#exit



…

[local]swch61#

configure


[local]swch61(config)#

client ssh
```

```
[local]swch61(config-ssh)#
```

```
ssh key +KEYVALUE len KEYLEN type v2-rsa
```

```
[local]swch61(config-ssh)#
```

```
end
```

If you see these warnings, contact Cisco Technical Support.

```
“Warning: Failed to add ID file argument”
“Warning: Failed to add ciphers argument”
“Warning: Failed to add preferred authentication argument”
“Failure: Failed to add ssh options”
```

Reference:

VPC-DI System Administration Guide, StarOS Release 21.28