Fehlerbehebung bei SSH Public Key Authentication StarOS

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Konfiguration der SSH/SFTP-Authentifizierung mit öffentlichem Schlüssel vom Paket-Gateway zu externen Servern in StarOS beschrieben.

Problem

Wenn nach der Generierung und Konfiguration des öffentlichen Schlüssels Warn- oder Fehlermeldungen angezeigt werden, finden Sie im nächsten Abschnitt mögliche Abhilfemaßnahmen.

Lösung

- Sind SSH-Clientschlüssel vorhanden?

Suchen Sie mithilfe der Exec-CLI "show ssh client key" nach einem öffentlichen SSH-Schlüssel. Wenn keine Schlüssel vorhanden sind, generieren Sie diese mithilfe der CLIs, die im Abschnitt x des Referenzdokuments im folgenden Referenzabschnitt enthalten sind.

Authentifizieren Sie anschließend die Schlüssel, die per Push an den Remote-Server übertragen werden sollen, mithilfe der Exec-CLI "push ssh-key <hostname> user <username> [context <contextname>].

- Haben Sie den Client SSH-Schlüssel gedrückt?

Wenn der öffentliche Client SSH-Schlüssel nicht in der Liste der autorisierten Server des Remote-Servers vorhanden ist, drücken Sie den öffentlichen Schlüssel mithilfe der Exec-CLI "push ssh-key

<Hostname> user <Benutzername> [context <Kontextname>] auf den Remote-Server.

- Unterstützt der Remoteserver die Authentifizierung mit öffentlichem Schlüssel?

Stellen Sie sicher, dass der Remote-Server die Public-Key-Authentifizierung unterstützt, indem Sie die SSHD-Konfigurationsdatei des Remote-Servers überprüfen. Stellen Sie sicher, dass der Parameter "PubkeyAuthentication yes" in der SSHD-Konfigurationsdatei vorhanden ist.

Wenn Parameter/Werte in der SSHD-Konfigurationsdatei geändert werden, muss der SSHD-Server neu gestartet werden.

- Werden Warn- oder Fehlermeldungen angezeigt?

"Warnung: ID-Datei nicht gefunden":

Dies weist darauf hin, dass SSH-Clientschlüssel-ID-Dateien aufgrund eines internen Fehlers oder des manuellen Löschens von Dateien fehlen. Die Maßnahmen zur Wiederherstellung sind wie folgt.

- Wenn o/p der Exec-CLI "show ssh client key [type v2-rsa]" den öffentlichen v2-rsa-Schlüssel im "hex"- und "babblebabble"-Format anzeigt und zusätzlich die Fehlermeldung "Failure: Cannot find ssh public key file" (Fehler: konnte öffentliche SSH-Schlüsseldatei nicht finden) ausgibt,
    1. Rufen Sie den SSH-Client-Schlüssel (ssh key <key> len <keylen> type v2-rsa) im Abschnitt zur SSH-Client-Konfiguration ("client ssh") der Exec-CLI "show configuration" o/p ab.
    2. Konfigurieren Sie denselben SSH-Schlüsselwert neu, indem Sie in den CLI-Modus "config-ssh" wechseln.
    3. Beispiel:

<#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
```

Wenn diese Warnungen angezeigt werden, wenden Sie sich an den technischen Support von Cisco.

```
“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”
```

Referenz:

VPC-DI System-Administrationshandbuch, StarOS Release 21.28

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.