Risoluzione dei problemi di autenticazione StarOS con chiave pubblica SSH

Sommario

Introduzione

Problema

Soluzione

- Sono presenti chiavi client SSH?
- È stata inserita la chiave SSH del client?
- Il server remoto supporta l'autenticazione con chiave pubblica?
- Vengono visualizzati messaggi di avviso o di errore?

Riferimento:

Introduzione

In questo documento viene descritto come risolvere i problemi relativi alla configurazione dell'autenticazione a chiave pubblica SSH/SFTP dal packet gateway ai server esterni di StarOS.

Problema

Se dopo la generazione e la configurazione della chiave pubblica vengono visualizzati messaggi di avviso o di errore, vedere la sezione successiva per informazioni sulle possibili soluzioni.

Soluzione

- ### Sono presenti chiavi client SSH?

Verificare la presenza di una chiave pubblica SSH usando Exec CLI "show ssh client key". Se le chiavi non sono presenti, generarle utilizzando il set di CLI presente nella sezione "Generating SSH Keys" del documento di riferimento nella sezione di riferimento riportata di seguito.

Quindi, autenticare le chiavi da inviare al server remoto utilizzando Exec CLI "push ssh-key <nomehost> user <nomeutente> [context <nomecontesto>].

- ### È stata inserita la chiave SSH del client?

Se la chiave pubblica SSH del client non è presente nell'elenco delle chiavi autorizzate del server remoto, eseguire il push della chiave pubblica nel server remoto utilizzando Exec CLI "push ssh-key <nomehost> user <nomeutente> [context <nomecontesto>].

- ### Il server remoto supporta l'autenticazione con chiave pubblica?

Verificare che il server remoto supporti l'autenticazione a chiave pubblica verificando il file di configurazione SSHD del server remoto. Verificare che il parametro "PubkeyAuthentication yes" sia presente nel file di configurazione SSHD.

In caso di modifiche ai parametri/valori nel file di configurazione SSHD, per rendere effettive le modifiche è necessario riavviare il server SSHD.

- Vengono visualizzati messaggi di avviso o di errore?

"Avviso: impossibile trovare il file di ID":

Ciò indica che i file ID delle chiavi client SSH non sono presenti a causa di un errore interno o dell'eliminazione manuale dei file. Le azioni da recuperare sono le seguenti.

- Se l'o/p di Exec CLI "show ssh client key [type v2-rsa]" visualizza la chiave pubblica v2-rsa in formato "hex" e "bubble-babble" e visualizza inoltre il messaggio di errore "Failure: Unable to find ssh public key file", allora,
    1. Ottenere/Grep della chiave del client SSH (chiave ssh <key> len <keylen> tipo v2-rsa) dalla sezione della configurazione del client SSH ("client ssh") in Exec CLI "show configuration" o/p.
    2. Riconfigurare lo stesso valore della chiave SSH immettendo la modalità "config-ssh" nella CLI.
    3. Esempio:

<#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
```

Se vengono visualizzati questi avvisi, contattare il supporto tecnico 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”
```

Riferimento:

[Guida all'amministrazione del sistema VPC-DI, StarOS release 21.28]

Informazioni su questa traduzione
Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).