排除SSH公鑰身份驗證StarOS故障

目錄

簡介

問題

解決方案

- 是否存在SSH客戶端金鑰？
- 您是否推送了客戶端SSH金鑰？
- 遠端伺服器是否支援公鑰身份驗證？
- 您是否看到任何警告或失敗消息？

參考資料：

簡介

本文檔介紹如何對StarOS中從資料包網關到外部伺服器的SSH/SFTP公鑰身份驗證配置進行故障排除。

問題

如果在公鑰生成和配置之後出現警告或失敗消息，則檢查下一部分是否有可能採取補救措施。

解決方案

- ### 是否存在SSH客戶端金鑰？

使用Exec CLI「show ssh client key」檢查SSH公鑰。如果不存在金鑰，則使用下面參考部分參考文檔的「生成SSH金鑰」部分中存在的一組CLI生成金鑰。

然後，使用Exec CLI "push ssh-key <hostname> user <username> [context <contextname>]對要推送到遠端伺服器的金鑰進行身份驗證。

- ### 您是否推送了客戶端SSH金鑰？

如果客戶端SSH公鑰不在遠端伺服器的授權清單中，則使用Exec CLI "push ssh-key <hostname> user <username> [context <contextname>]將公鑰推送到遠端伺服器。

- ### 遠端伺服器是否支援公鑰身份驗證？

通過檢查遠端伺服器的SSHD配置檔案，確保遠端伺服器支援公鑰身份驗證。確保SSHD配置檔案中存在「PubkeyAuthentication yes」引數。

如果SSHD配置檔案中的引數/值有任何更改，則需要重新啟動SSHD伺服器。

- 您是否看到任何警告或失敗消息？

"警告：找不到ID檔案":

這表示由於內部錯誤或手動刪除檔案，SSH客戶端金鑰ID檔案丟失。要恢復的操作如下。

- 如果Exec CLI的o/p「show ssh client key [type v2-rsa]」以「hex」和「bubble-babble」格式顯示v2-rsa公鑰，並且還顯示故障消息「Failure: Unable to find ssh public key file」，則，
    1. 從Exec CLI "show configuration" o/p的SSH客戶端配置("client ssh")部分獲取/grep SSH客戶端金鑰（ssh key <key> len <keylen>型別v2-rsa）。
    2. 通過進入「config-ssh」 CLI模式重新配置相同的SSH金鑰值。
    3. 範例：

<#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
```

如果您看到這些警告，請與Cisco技術支援聯絡。

```
“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”
```

參考資料：

[VPC-DI系統管理指南，StarOS版本21.28]

關於此翻譯
思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。