

# Troubleshooting de SSH Public Key Authentication StarOS

## Contenido

---

[Introducción](#)

[Problema](#)

[Solución](#)

[¿Están presentes las claves de cliente SSH?](#)

[¿Ha pulsado la clave SSH del cliente?](#)

[¿Admite el servidor remoto la autenticación de clave pública?](#)

[¿Aparece algún mensaje de error o advertencia?](#)

[Referencia:](#)

---

## Introducción

Este documento describe cómo resolver problemas de configuración de autenticación de clave pública SSH/SFTP desde el gateway de paquetes a los servidores externos en StarOS.

## Problema

Si aparecen mensajes de advertencia o de error después de la generación y configuración de claves públicas, consulte la siguiente sección para ver las posibles soluciones.

## Solución

- ¿Están presentes las claves de cliente SSH?

Verifique la clave pública SSH usando Exec CLI "show ssh client key". Si las claves no están presentes, génere las usando el conjunto de CLIs presentes en la sección "Generación de Llaves SSH" del documento de referencia en la sección de referencia a continuación.

Y luego, autentique las claves que se enviarán al servidor remoto usando Exec CLI "push ssh-key <hostname> user <username> [context <contextname>].

- ¿Ha pulsado la clave SSH del cliente?

Si la clave pública SSH del cliente no está presente en la lista autorizada del servidor remoto, inserte la clave pública en el servidor remoto mediante Exec CLI "push ssh-key <hostname> user <username> [context <contextname>].

- ¿Admite el servidor remoto la autenticación de clave pública?

Asegúrese de que el servidor remoto admite la autenticación de clave pública comprobando el archivo de configuración SSHD del servidor remoto. Asegúrese de que el parámetro "PubkeyAuthentication yes" esté presente en el archivo de configuración SSHD.

Si hay algún cambio en los parámetros/valores en el archivo de configuración SSHD, para ser efectivo, el servidor SSHD debe ser reiniciado.

- ¿Aparece algún mensaje de error o advertencia?

"Advertencia: no se pudo encontrar el archivo de ID":

Esto indica que faltan archivos de ID de claves de cliente SSH debido a un error interno o a la eliminación manual de archivos. Las acciones a recuperar son las siguientes.

- Si el comando o/p de la CLI de Exec "show ssh client key [type v2-rsa]" muestra la clave pública v2-rsa en formato "hex" y "bubble-balble" y además da el mensaje de falla "Failure: Cannot to find ssh public key file", entonces,
  1. Obtenga/grep la clave de cliente SSH (ssh key <key> len <keylen> type v2-rsa) de la sección de configuración de cliente SSH ("client ssh") de la CLI de Exec "show configuration" o/p.
  2. Vuelva a configurar el mismo valor de clave SSH ingresando en el modo CLI "config-ssh".
  3. Ejemplo:

```
<#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
```

Si ve estas advertencias, póngase en contacto con el soporte técnico de 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”
```

## Referencia:

[Guía de administración del sistema VPC-DI, StarOS versión 21.28](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).