

Identificar e Solucionar Problemas de StarOS de Autenticação de Chave Pública SSH

Contents

[Introdução](#)

[Problema](#)

[Solução](#)

[As chaves do cliente SSH estão presentes?](#)

[Você empurrou a chave SSH do cliente?](#)

[O servidor remoto dá suporte à Autenticação de Chave Pública?](#)

[Você está vendo alguma mensagem de aviso ou falha?](#)

[Referência:](#)

Introdução

Este documento descreve como resolver problemas de configuração de autenticação de chave pública SSH/SFTP do gateway de pacotes para servidores externos no StarOS.

Problema

Se as mensagens de aviso ou falha aparecerem após a geração e as configurações de chave pública, verifique a próxima seção para possíveis soluções.

Solução

- As chaves do cliente SSH estão presentes?

Procure a chave pública SSH usando Exec CLI "show ssh client key". Se as chaves não estiverem presentes, gere-as usando um conjunto de CLIs presentes na seção "Gerando chaves SSH" do documento de referência na seção de referência abaixo.

Em seguida, autentique as chaves a serem enviadas para o servidor remoto usando Exec CLI "push ssh-key <hostname> user <username> [context <contextname>].

- Você empurrou a chave SSH do cliente?

Se a chave pública SSH do cliente não estiver presente na lista autorizada do servidor remoto, envie a chave pública para o servidor remoto usando Exec CLI "push ssh-key <hostname> user <username> [context <contextname>].

- O servidor remoto dá suporte à Autenticação de Chave Pública?

Verifique se o servidor remoto oferece suporte à autenticação de chave pública verificando o arquivo de configuração SSHD do servidor remoto. Verifique se o parâmetro "PubkeyAuthentication yes" está presente no arquivo de configuração SSHD.

Se houver alguma alteração nos parâmetros/valores no arquivo de configuração SSHD, para ser eficaz, o servidor SSHD precisa ser reiniciado.

- Você está vendo alguma mensagem de aviso ou falha?

"Aviso: não foi possível localizar o arquivo de ID":

Isso indica que os arquivos de ID das chaves do cliente SSH estão ausentes devido a um erro interno ou à exclusão manual dos arquivos. As ações a serem recuperadas são as seguintes.

- Se o/p do Exec CLI "show ssh client key [type v2-rsa]" estiver mostrando a chave pública v2-rsa no formato "hex" e "bubble-babble" e, além disso, apresentar a mensagem de falha "Failure: Unable to find ssh public key file" (Falha: não foi possível encontrar o arquivo de chave pública ssh),
 1. Obtenha/gere a chave do cliente SSH (ssh key <key> len <keylen> type v2-rsa) na seção de configuração do cliente SSH ("client ssh") do Exec CLI "show configuration" o/p.
 2. Reconfigure o mesmo valor de chave SSH entrando no modo CLI "config-ssh".
 3. Exemplo:

```
<#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 você vir esses avisos, entre em contato com o Suporte Técnico da 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”
```

Referência:

[Guia de administração do sistema VPC-DI, StarOS versão 21.28](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.