

Erro de Tempo Limite de Autenticação de Chave RSA SFTP do ISE

Contents

Problema

Um repositório SFTP configurado com a autenticação de chave RSA funciona com êxito em um nó ISE (ise1), mas falha em outro nó ISE (ise2) executando o ISE 3.4. No nó com falha, o handshake SSH e a validação do servidor são concluídos com êxito, mas a autenticação de chave pública não é concluída e a sessão SFTP expira com um erro "sftp_select Error: timeout!" mensagem de erro.

Ao tentar listar o conteúdo do repositório SFTP usando o comando show repository SFTP no nó ISE afetado, esta sequência de erros ocorre:

```
device/admin# show repository SFTP
6 [4005534]:[info] transfer: cars_xfer.c[333] [system]: sftp dir of repository SFTP requested
6 [4005534]:[info] transfer: cars_xfer_util.c[2654] [system]: Server validation successful 10.50.60.200
7 [4005534]:[debug] transfer: sftp_handler.c[1295] [system]: Running sftp command: 10.50.60.200 will.ki
6 [4005534]:[info] transfer: sftp_handler.c[695] [system]: DEBUG: local user: admin UID: 0 sftp_run_par
7 [4005534]:[debug] transfer: sftp_handler.c[705] [system]: fd is:7
7 [4005535]:[debug] transfer: sftp_handler.c[327] [system]: Executing SFTP command: 0 admin /usr/bin/sf
3 [4005534]:[error] transfer: sftp_handler.c[417] [system]: sftp_select Error: timeout!
7 [4005534]:[debug] transfer: sftp_handler.c[1136] [system]: sftp parent status -999
% Failure occurred during request
```

Isso impede o uso do repositório SFTP do nó afetado do ISE para funções críticas do ISE, como operações de backup.

Ambiente

- Cisco Identity Services Engine (ISE) versão 3.4.0
- Implantação do ISE de vários nós com pelo menos dois nós (ise1 e ise2)

- Repositório SFTP configurado com autenticação de chave RSA
- Autenticação baseada em chave SSH usando chave privada RSA (/home/admin/.ssh/id_rsa)
- Servidor SFTP acessível
- Autenticação de senha desabilitada (-oPasswordAuthentication=no)

Resolução

Este caso está sendo investigado pela equipe de engenharia. O problema foi escalado para a análise do registro raiz para determinar a causa subjacente do tempo limite de SFTP no nó ISE afetado.

Com base na saída da depuração, execute as etapas de solução de problemas descritas nas próximas seções para coletar informações adicionais.

Passo 1: Verificar a consistência da configuração do repositório SFTP entre nós

Compare a configuração do repositório SFTP em ambos os nós do ISE para garantir que sejam idênticos.

Passo 2: Verificar Permissões e Propriedade do Arquivo de Chave SSH

Verifique se o arquivo de chave privada SSH (/home/admin/.ssh/id_rsa) tem as permissões e a propriedade corretas no nó afetado.

Passo 3: Testar a conectividade da rede

Confirme se o nó ISE afetado pode acessar o servidor SFTP na porta 22 e se não há problemas de bloqueio em nível de rede.

Passo 4: Habilitar Depuração Adicional

Ative a depuração mais detalhada SSH/SFTP para capturar informações detalhadas sobre a falha de autenticação.

Na CLI do nó afetado:

1.- Ative essas depurações com comandos:

- debug copy 7
- debug transfer 7

2.- Use o comando show repository xxxxx depois de habilitar depurações para capturar mais informações.

Passo 5: Comparar impressões digitais da chave SSH

Verifique se a chave pública SSH no servidor SFTP corresponde à chave privada que está sendo usada pelo nó ISE afetado.

O problema foi resolvido identificando a senha correta usada para gerar a chave RSA no nó SPAN e redefinindo as configurações do repositório para alinhar com as credenciais válidas.

Solução temporária

Você é recomendado verificar manualmente a senha usando `ssh-keygen -y -f /home/admin/.ssh/id_rsa` na CLI para confirmar qual senha desbloqueou com êxito a chave privada antes de reaplicar a configuração do repositório na GUI.

Etapas para regenerar a chave RSA:

1.- Abra a CLI do nó afetado.

2.- Exclua a chave RSA antiga com o comando `crypto key delete rsa`.

3.- Gere uma nova chave RSA com a senha desejada com o comando `crypto key generate rsa` `passphrase XXXXXXXXXXXXXXXXX`.



Note: A senha deve ter 13 caracteres ou mais.

4.- Obtenha a nova chave pública RSA para importar para o outro sistema com o comando `show crypto key`.

Causa

Erro de usuário / Erro de configuração. A investigação determinou que a falha de autenticação do repositório no nó secundário foi causada por uma incompatibilidade entre a senha esperada e a senha usada para proteger a chave privada RSA armazenada. Isso impediu o subsistema criptográfico de descriptografar com êxito a chave para assinar o desafio de autenticação SSH.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

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.