

ISE SFTP RSA Key Authentication Timeout Error

Contents

Issue

An SFTP repository configured with RSA key authentication works successfully on one ISE node (ise1) but fails on another ISE node (ise2) running ISE 3.4. On the failing node, the SSH handshake and server validation complete successfully, but public-key authentication does not finish and the SFTP session times out with an "sftp_select Error: timeout!" error message.

When attempting to list the SFTP repository contents using the **show repository SFTP** command on the affected ISE node, this error sequence occurs:

```
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
```

This prevents the use of the SFTP repository from the affected ISE node for critical ISE functions such as backup operations.

Environment

- Cisco Identity Services Engine (ISE) version 3.4.0
- Multi-node ISE deployment with at least two nodes (ise1 and ise2)
- SFTP repository configured with RSA key authentication
- SSH key-based authentication using RSA private key (/home/admin/.ssh/id_rsa)
- SFTP server accessible

- Password authentication disabled (-oPasswordAuthentication=no)

Resolution

This case is currently under investigation by the engineering team. The issue has been escalated for root log analysis to determine the underlying cause of the SFTP timeout on the affected ISE node.

Based on the debug output, perform the troubleshooting steps described in the next sections to gather additional information.

Step 1: Verify SFTP Repository Configuration Consistency between Nodes

Compare the SFTP repository configuration on both ISE nodes to ensure they are identical.

Step 2: Check SSH Key File Permissions and Ownership

Verify that the SSH private key file (/home/admin/.ssh/id_rsa) has the correct permissions and ownership on the affected node.

Step 3: Test Network Connectivity

Confirm that the affected ISE node can reach the SFTP server on port 22 and that there are no network-level blocking issues.

Step 4: Enable Additional Debugging

Enable more verbose SSH/SFTP debugging to capture detailed information about the authentication failure.

From the affected node CLI:

1.- Enable these debugs with commands:

- **debug copy 7**
- **debug transfer 7**

2.- Use the **show repository xxxxx** command after enabling debugs to capture more information.

Step 5: Compare SSH Key Fingerprints

Verify that the SSH public key on the SFTP server matches the private key being used by the affected ISE node.

The issue was resolved by identifying the correct passphrase used to generate the RSA key on the SPAN node and re-configuring the repository settings to align with the valid credentials.

Interim Workaround

You are advised to manually verify the passphrase using **ssh-keygen -y -f /home/admin/.ssh/id_rsa** on the CLI to confirm which password successfully unlocked the private key before re-applying the repository configuration in the GUI.

Steps to regenerate the RSA key:

- 1.- Open the affected node CLI.
- 2.- Delete the old RSA Key with the **crypto key delete rsa** command.
- 3.- Generate a new RSA key with the desired passphrase with the **crypto key generate rsa passphrase XXXXXXXXXXXXXXXX** command.



Note: Passphrase must be 13 or more characters.

- 4.- Get the new RSA public key to import to the other system with the **show crypto key** command.

Cause

User Error / Configuration Error. The investigation determined that the repository authentication failure on the secondary node was caused by a mismatch between the expected passphrase and the passphrase used to secure the stored RSA private key. This prevented the cryptographic subsystem from successfully decrypting the key to sign the SSH authentication challenge.

Related Content

- [Cisco Technical Support & Downloads](#)