

ISE SFTP RSAキー認証タイムアウトエラー

内容

問題

RSAキー認証を使用して設定されたSFTPリポジトリは、1つのISEノード(ise1)では正常に動作しますが、ISE 3.4を実行している別のISEノード(ise2)では失敗します。障害が発生したノードでは、SSHハンドシェイクとサーバ検証は正常に完了していますが、公開キー認証が完了せず、SFTPセッションが「sftp_select Error: timeout!」エラーメッセージでタイムアウトします。

該当するISEノードでshow repository SFTPコマンドを使用してSFTPリポジトリの内容を一覧表示しようとする、次のエラーシーケンスが発生します。

```
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
```

これにより、バックアップ操作などの重要なISE機能のために、影響を受けるISEノードからのSFTPリポジトリが使用されなくなります。

環境

- Cisco Identity Services Engine(ISE)バージョン3.4.0
- 少なくとも2つのノード (ise1とise2) を含むマルチノードISE導入
- RSAキー認証で設定されたSFTPリポジトリ

- RSA秘密キー(/home/admin/.ssh/id_rsa)を使用したSSHキーベース認証
- SFTPサーバにアクセス可能
- パスワード認証が無効です(-oPasswordAuthentication=no)

解決方法

このケースは現在、エンジニアリングチームによって調査中です。この問題は、影響を受けるISEノードでのSFTPタイムアウトの根本的な原因を特定するために、ルートログ分析のためにエスケーションされました。

デバッグ出力に基づいて、次の項で説明するトラブルシューティング手順を実行し、追加情報を収集します。

ステップ1：ノード間でのSFTPリポジトリ設定の一貫性の確認

両方のISEノードのSFTPリポジトリ設定を比較して、それらが同一であることを確認します。

ステップ2:SSHキーファイルの権限と所有権を確認する

SSH秘密キーファイル(/home/admin/.ssh/id_rsa)に、影響を受けるノードの正しい権限と所有権があることを確認します。

ステップ3：ネットワーク接続をテストする

影響を受けるISEノードがポート22のSFTPサーバに到達できること、およびネットワークレベルのブロッキングの問題がないことを確認します。

ステップ4：追加のデバッグの有効化

より詳細なSSH/SFTPデバッグを有効にして、認証の失敗に関する詳細情報を取得します。

影響を受けるノードのCLIで次のコマンドを実行します。

1. – 次のコマンドを使用して、これらのデバッグを有効にします。

- デバッグコピー7
- デバッグ転送7

2. – デバッグを有効にしてさらに多くの情報をキャプチャした後で、show repository xxxxxコマンドを使用します。

ステップ5:SSHキーフィンガープリントの比較

SFTPサーバのSSH公開キーが、影響を受けるISEノードで使用されている秘密キーと一致することを確認します。

この問題は、SPANノードでRSAキーを生成するために使用される正しいパスフレーズを特定し、有効なクレデンシャルに合わせてリポジトリ設定を再設定することで解決されました。

暫定回避策

GUIでリポジトリ設定を再適用する前に、CLIでssh-keygen -y -f /home/admin/.ssh/id_rsaを使用してパスフレーズを手動で確認し、秘密キーのロック解除に成功したパスワードを確認することをお勧めします。

RSAキーを再生成する手順：

1. – 影響を受けるノードのCLIを開きます。

2.- crypto key delete rsaコマンドを使用して、古いRSAキーを削除します。

3.- crypto key generate rsa passphrase XXXXXXXXXXXXXXXXコマンドを使用して、目的のパスフレーズで新しいRSAキーを生成します。



注：パスフレーズは13文字以上にする必要があります。

4.- show crypto keyコマンドを使用して、新しいRSA公開キーを取得して他のシステムにインポートします。

原因

ユーザエラー/設定エラー。調査の結果、セカンダリノードでのリポジトリ認証の失敗は、格納されているRSA秘密キーを保護するために使用するパスフレーズと予期されるパスフレーズの不一致が原因であったことが判明しました。これにより、暗号化サブシステムがSSH認証チャレンジに署名するキーを正常に復号化できなくなりました。

関連コンテンツ

- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。