

ISE SFTP RSA密钥身份验证超时错误

目录

问题

配置了RSA密钥身份验证的SFTP存储库在一个ISE节点(ise1)上成功运行，但在运行ISE 3.4的另一个ISE节点(ise2)上失败。在故障节点上，SSH握手和服务器验证成功完成，但公钥身份验证未完成，并且SFTP会话超时，并显示“sftp_select Error:超时！”错误消息。

当尝试在受影响的ISE节点上使用show repository SFTP命令列出SFTP存储库内容时，会发生以下错误序列：

```
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
```

这会阻止从受影响的ISE节点使用SFTP存储库执行关键ISE功能，例如备份操作。

环境

- 思科身份服务引擎(ISE)3.4.0版
- 具有至少两个节点 (ise1和ise2) 的多节点ISE部署
- 使用RSA密钥身份验证配置的SFTP存储库
- 使用RSA私钥(/home/admin/.ssh/id_rsa)进行基于SSH密钥的身份验证
- 可访问SFTP服务器

- 已禁用密码身份验证(-oPasswordAuthentication=no)

分辨率

工程小组目前正在调查此案。已针对根日志分析上报问题，以确定受影响的ISE节点上SFTP超时的根本原因。

根据调试输出，执行以下各节中描述的故障排除步骤以收集更多信息。

步骤 1：验证节点之间的SFTP存储库配置的一致性

比较两个ISE节点上的SFTP存储库配置，确保它们相同。

步骤 2：检查SSH密钥文件权限和所有权

验证SSH私钥文件(/home/admin/.ssh/id_rsa)在受影响的节点上具有正确的权限和所有权。

步骤 3：测试网络连通性

确认受影响的ISE节点可以到达端口22上的SFTP服务器，并且不存在网络级阻止问题。

步骤 4：启用其他调试

启用更详细的SSH/SFTP调试，以捕获有关身份验证失败的详细信息。

从受影响的节点CLI:

1. — 使用以下命令启用这些调试：

- debug copy 7
- debug transfer 7

2. — 启用调试后，请使用show repository xxxxx命令捕获更多信息。

步骤 5：比较SSH密钥指纹

验证SFTP服务器上的SSH公钥是否与受影响ISE节点使用的私钥匹配。

通过识别用于在SPAN节点上生成RSA密钥的正确密码并重新配置存储库设置以与有效凭证保持一致，问题得以解决。

临时解决方法

建议在CLI上使用ssh-keygen -y -f /home/admin/.ssh/id_rsa手动验证密码，以确认哪个密码已成功解锁私钥，然后再在GUI中重新应用存储库配置。

重新生成RSA密钥的步骤：

1. — 打开受影响的节点CLI。
2. — 使用crypto key delete rsa命令删除旧的RSA密钥。
3. — 使用crypto key generate rsa passphrase XXXXXXXXXXXX命令生成具有所需密码的新RSA密钥。



注意：密码必须是13个或更多字符。

-
4. — 使用show crypto key命令获取要导入到其他系统的新RSA公钥。

原因

用户错误/配置错误。调查确定辅助节点上的存储库身份验证失败是由预期密码短语与用于保护存储的RSA私钥的密码短语不匹配引起的。这阻止了加密子系统成功解密密钥以签署SSH身份验证质询。

相关内容

- [思科技术支持和下载](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。