Login

Idle SSH Connections are Broken After 10-15 Minutes

If you find that idle SSH connections tend to be dropped after 10 to 15 minutes and your are using a router or other device that implements Network Address Translation (NAT), such as a DSL router, you may want to enable the ServerAliveInterval parameter in your ~/.ssh/config.

The issue is that some devices that implement NAT will drop information from their state tables if a TCP connection has been idle for just a few minutes. In such cases, it may be necessary to ensure that the connection is never truly idle for an extended period.

The ServerAliveInterval parameter (supported in OpenSSH 3.8 and later) causes the SSH client to periodically send an encrypted query to determine if the server is still responsive. The packets will make the connection appear to be active and can prevent the NAT state table entry for the connection from timing out.

For example, adding the following to your ~/.ssh/config will cause an encrypted query to be sent every five minutes:

```
ServerAliveInterval 5m
```

TIP: You may need to experiment with the length of the interval to determine an appropriate value to prevent your connection from being broken. If you use the NAS config template, ServerAliveInterval is set to 10 minutes.

SSH Connection is Periodically Broken Even When Connection is Active

During an SSH session, the client and server will re-negotiate the keys used to encrypt the session every so often. Very old versions of OpenSSH did not implement this feature, which can cause a problem when connected to the SFEs. Your connection may appear to hang or may abort with an error message such as the following:

```
Dispatch protocol type 20
```

If you encounter this issue, you will need to upgrade to a newer version of OpenSSH. Note: Other implementations that were derived from the OpenSSH distribution, such as SUN Secure Shell, are likewise known to exhibit this problem.

Slow Performance Transferring Data

While OpenSSH performs reasonably for local data transfers, the performance will tend to be reduced due to the latency of long-haul network connections.

Depending on the severity of the impact you may have several options to improve this situation.

Upgrade to OpenSSH 4.7 or Later

If you are using a version of OpenSSH that is older than 4.7, you may see an improvement in file transfer performance by upgrading to OpenSSH 4.7 or later. This is due to the use of a larger channel buffer introduced in that version.

Read File Transfer Tips for more recommendations.

Use the information in this section to help troubleshoot any problems you encounter when logging into NAS systems.

SSH Known-Hosts Error

A successful host verification indicates that your Secure Shell (SSH) client has established a secure connection with the SSH server, and that no intermediate machines have access to that connection. The identity of the remote host is verified by checking the host public key of the remote host, which is stored in one of the following locations:

- The system-wide /etc/ssh/ssh_known_hosts file (for some systems, /etc/ssh_known_hosts)
- The ~/.ssh/known_hosts file on your local system

There are three ways SSH can respond to an unrecognized or changed SSH host key, based on the value of the StrictHostKeyChecking variable in either your ~/.ssh/config file or in the /etc/ssh/ssh_config (or /etc/ssh_config) file on your local system. The possible values are:

StrictHostKeyChecking=no
: This is the most insecure setting as it will blindly connect to the server. It will add the server's key if it's not present locally, and if the key has changed it will add the key without asking.

StrictHostKeyChecking=ask
: With this setting, if you have no host key for the server, it will show you the fingerprint and ask you to confirm. If you connect and the key does not match, it will prevent you from logging in, and will tell you where to find the conflicting key inside the known_hosts file.

StrictHostKeyChecking=yes
: This is the most secure setting. If you have no host key for this server, then it will prevent you from logging in at all.

If you receive an SSH known-hosts error message the first time you log into an SFE, and the StrictHostKeyChecking variable is set to yes, you can resolve the problem by adding -o "stricthostkeychecking=ask" to your SSH command. For example:

SSH Known-Hosts Error Example

your_local_system% ssh sfe*6*.nas.nasa.gov

```
WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
SHA256:IKccVJBCXNjEEJ0Gq2XWKNfWtzimfyGEMu64asz5bwM.
Please contact your system administrator.
Add correct host key in /Users/userid/.ssh/known_hosts2 to get rid
of this message.
Offending key in /etc/ssh_known_hosts2:24
RSA host key for sfe6.nas.nasa.gov has changed and you have
requested strict checking.
No RSA host key is known for sfe6.nas.nasa.gov and you have
requested strict checking.
Host key verification failed.
```

SSH Known-Hosts Error: Solution

Add -o "stricthostkeychecking=ask" to your SSH command. For example:

your_local_system% ssh -o "stricthostkeychecking=ask" sfe*6*.nas.nasa.gov

```
---------------------------------------------------------------------
The authenticity of host 'sfe6.nas.nasa.gov (198.9.4.40)'
can't be established.
RSA key fingerprint is
SHA256:IKccVJBCXNjEEJ0Gq2XWKNfWtzimfyGEMu64asz5bwM.
Are you sure you want to continue connecting (yes/no)? yes
---------------------------------------------------------------------
Warning: Permanently added 'sfe6.nas.nasa.gov,198.9.4.40' (RSA) to
the list of known hosts.

---------------------------------------------------------------------
Plugin authentication
Enter PASSCODE: type your passcode
```

Common RSA SecurID Passcode Problems

Incorrect Passcode or Locked Token

Each RSA SecurID tokencode can be used only once. If you try to use a single tokencode multiple times, you will be prompted again

to enter a new passcode. If you do not provide a correct passcode in a few consecutive attempts, your RSA SecurID token will be temporarily disabled and you will need to contact the NAS Control Room at (800) 331-8737 or (650) 604-4444 to unlock the token.

Note: If you have an RSA SecurID hard token (fob), the passcode is your PIN + the tokencode. If you have anRSA SecurID soft token (mobile app), the passcode is the tokencode only.

Incomplete PIN Setup (Hard Token Only)

If you have a hard token (fob) and you cannot log into NAS systems after you first create your PIN, it is possible that you did not successfully complete the new-PIN process. For example, you might have used a special character in your PIN, which is not supported.

In this case, try logging into an SFE again. You will be prompted to complete the new-PIN process, as shown below.

Note: Your PIN must consist of exactly 8 alphanumeric characters, with at least 1 letter and at least 1 number, and no special characters.

your_local_system% ssh sfe*6*
user@sfe*6*'s password:
Authenticated with partial success.
Plugin authentication
Enter PASSCODE:
Plugin authentication
You may create your own PIN or accept a server assigned PIN.
Would you like to create your own new PIN (yes/no)? *yes*
Plugin authentication
Enter a new PIN of 8 alphanumeric characters:
Re-enter new PIN to confirm:
Enter PASSCODE:
Plugin authentication
Enter PASSCODE:
Permission denied, please try again.
user@sfe*6*'s password:
Permission denied, please try again.
user@sfe*6*'s password:
Permission denied ().

Common NASA PIV Problems

PIN Always Prompted when Connecting to SFEs

NASA-supported laptops attempt to use PIV by default when a NASA badge is in an attached card reader. To avoid having to enter your NASA PIV PIN every time you log in, set up SSH Passthrough. Alternatively, you can disable the NASA PIV as discussed below.

Too Many Authentication Failures

The hook that allows SSH to use NASA PIV authentication may attempt to utilize all of the certificates on a NASA badge instead of just the one needed for authentication. This can cause more authentication failures than are allowed on NAS systems. In this case, you can disable PIV in one of the following ways.

- Disable PIV on the command line each time you log in:

  ssh -oPKCS11Provider=none *username*@sfeX.nas.nasa.gov

- Disable PIV by permanently modifying your SSH configuration in the ~/.ssh/config file by adding the following line (in the section of the file related to SFE configuration):

  PKCS11Provider none

Alternatively, if you want to continue using NASA PIV, sometimes a different provider is available on the systems (such as NASA-supported laptops) using:

ssh -oPKCS11Provider=/usr/lib/ssh-keychain.dylib *username*@sfeX.nas.nasa.gov

(or in the ~/.ssh/config file):

PKCS11Provider /usr/lib/ssh-keychain.dylib

Common Passthrough Problems

If you have previously set up SSH passthrough correctly, when you log into a NAS host you should be prompted only for your RSA SecurID passcode before you are "passed through" directly to the host you requested. If this does not happen, see the following common problems and solutions.

Authentication Failure

If authentication fails when you enter the passcode, it is possible that your username for your local system is not the same as your username for the NAS systems, and your .ssh/config file does not contain your NAS username. To solve this problem, add your NAS username to your .ssh/config file, as follows:

- If you use the .ssh/config file to connect to multiple computer sites, then add your NAS username to the ProxyCommand lines for corresponding NAS hosts. For example:

  Host lfe
  ProxyCommand ssh *username*@sfe*6*.nas.nasa.gov /*usr*/local/bin/ssh-proxy lfe

  In this case, you will still need to include your NAS username when you run the ssh command, as shown in the following example, in order to avoid being prompted for a password:

  %ssh *your_nas_username*@lfe

- If you use the .ssh/config file to connect only to NAS, then you can simply add the following line at the beginning of your .ssh/config file:

  User your_nas_username

  In this case, you do not need to add your NAS username to the ProxyCommand lines. Additionally, you can run the ssh command without your NAS username in the command line, and you will not be prompted for a password. For example:

  %ssh lfe

Password Prompt After Entering Passcode

If you are prompted for a password in addition to the passcode, there are several possible causes:

- Your local system username is different from your NAS system username. To solve this problem, see the previous section, **Authentication Failure**.
- Either your home directory or the .ssh/authorized_keys file under your NAS account specifies write permission for group or others. You must ensure that write permission is specified only for you.
- One or both of the following:
  - You have not run ssh-key-init on *sfeX*.
  - The .ssh/authorized_keys file of the NAS host that you want to connect to is missing.

Passphrase Prompt After Entering Passcode

If you are prompted for your passphrase in addition to the passcode, the most likely reason is that you did not run following commands to forward your private key before you issued the ssh command:

- ssh-agent
- ssh-add ~/.ssh/id_rsa

See Setting Up SSH Passthrough for more information about these commands.

Password Expiration

Your NAS password is valid for 60 days. Before it expires, you will receive an email notification reminding you to change your password. If your password expires you will still be able to log into NAS systems, but you will not be able to proceed until you follow the prompt to change it.

Account Expiration or Deactivation

Your NAS account is active as long as you have a valid project and a valid account request form on file at NAS. If your account expires, it will be removed from the NAS database and from the /etc/passwd files, and you will not be able to log in.

To maintain a valid account, you must submit a new account request form each year. You will receive an email notification when it is time to submit a new one.

If you violate NAS security rules such as those listed in the NAS Systems Environment Rules of Behavior, your account can be deactivated.

Error Connecting to a Cloud SFE

The cloud SFE updates new PIV credentials once every 24 hours. If you receive the following error when trying to connect to create a mesh key, your new PIV card credentials may not yet have been added to the cloud SFE:

WARNING: Your password has expired.
Password change required but no TTY available.

The solution is to wait 24 hours and try again.