Using sshproxy

NUG Monthly Webinar
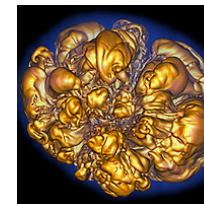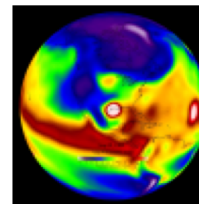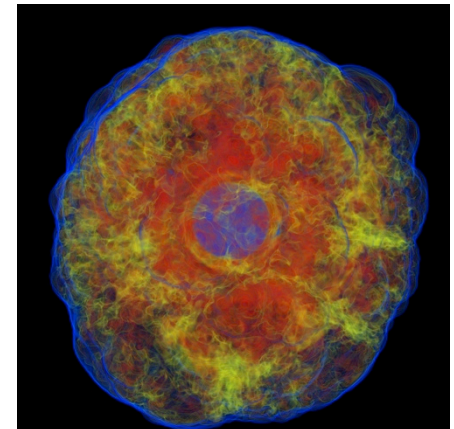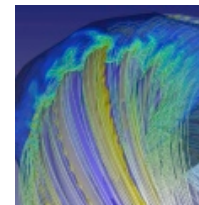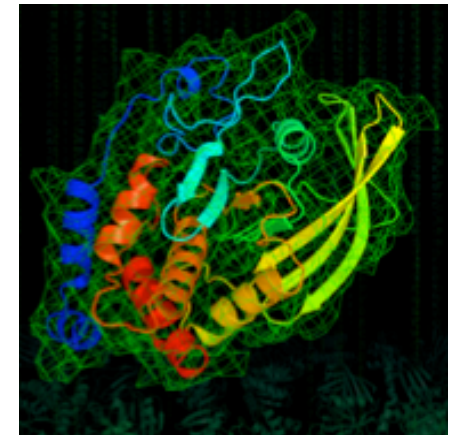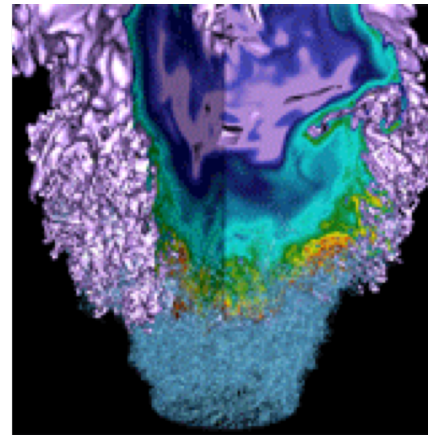
Woo-Sun Yang
NERSC User Engagement Group

August 23, 2019

SSH authentication

- **Assuming that you have correctly configured a MFA token on an authenticator app on your smartphone, tablet, laptop, …**
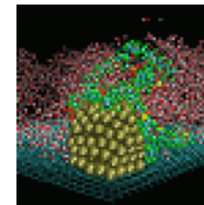 - https://www.nersc.gov/users/connecting-to-nersc/mfa/#toc-anchor-2

- **SSH authentication**
  - Password authentication

```
laptop$ ssh elvis@cori.nersc.gov
...
Password + OTP:
```

  - Enter password and OTP every time you open a new ssh session (tedious)

  - SSH key authentication
    - This is what we are going to cover mostly today

Old way for using SSH key authentication at NERSC

- **Generate a ssh key pair (public and private) with 'ssh-keygen' on your desktop/laptop**
  - For additional security, you can set a passphrase when generating a key pair
  - Keys never expire

```
laptop$ ls -l ~/.ssh
...
-rw-------    1 elvis  80609    3434 Jul  1  2019 id_rsa
-rw-------    1 elvis  80609     748 Jul  1  2019 id_rsa.pub
...
```

- **Copy the public key to NIM**

- **When you login to your desktop/laptop account, ssh-add the private key to ssh's "authentication agent"**

- **Subsequent ssh sessions from there do not ask for authentication ("password-less" or "passphrase-less" ssh)**

- **Not allowed any more at NERSC**

sshproxy: <u>new</u> way for SSH certificate authentication

- **sshproxy generates a key pair along with a signed certificate for you and they are downloaded to your desktop/laptop**

- **You authenticate with password+OTP when requesting for NERSC-generated ssh keys**

- **Certificate has an expiration time (default: 24 hours)**

- **For subsequent ssh sessions, you are NOT prompted for password+OTP, if the valid keys are used**

- **The only practical difference from the old way from the user's perspective is that users now have to generate keys once in 24 hours**

  – For users who hadn't used key authentication before, connecting to NERSC hosts has become almost a trivial matter!

What to do on linux-like desktop/laptop

- **Download sshproxy.sh to your desktop/laptop**

```
laptop$ scp elvis@cori.nersc.gov:/project/projectdirs/mfa/NERSC-MFA/sshproxy.sh .
```

- **Run the script on your desktop/laptop once a day**
  - Authenticate with password+OTP
  - Ssh key files are downloaded to ~/.ssh directory

```
laptop$ ./sshproxy.sh
Enter the password+OTP for elvis:
Successfully obtained ssh key /Users/elvis/.ssh/nersc
Key /Users/elvis/.ssh/nersc is valid: from 2019-08-23T09:24:00 to 2019-08-24T09:25:32

laptop$ ls -l ~/.ssh
...
-rw-------    1 elvis  80609   3179 Aug 23 09:25 nersc
-rw-------    1 elvis  80609   1501 Aug 23 09:25 nersc-cert.pub
-rw-------    1 elvis  80609    381 Aug 23 09:25 nersc.pub
...
```

What to do on linux-like desktop/laptop (cont'd)

- **Use the keys for subsequent ssh sessions**
  - Method 1: Specify the key in ssh command

```
laptop$ ssh -i ~/.ssh/nersc elvis@cori.nersc.gov
...
cori$                    # You're on cori
```

  - Method 2 (better): Configure local ssh to use the keys

```
laptop$ cat ~/.ssh/config
...
Host cori*.nersc.gov dtn*.nersc.gov
    IdentityFile ~/.ssh/nersc
    IdentitiesOnly yes
    ForwardAgent yes
...
```

   Your ssh command needs less typing:

```
laptop$ ssh elvis@cori.nersc.gov
...
cori$                        # You're on cori
```

sshproxy miscellany on linux-like desktop/laptop

- **Check the expiration time:**

```
laptop$ ssh-keygen -L -f ~/.ssh/nersc-cert.pub | grep Valid
    Valid: from 2019-08-23T09:24:00 to 2019-08-24T09:25:32
```

- **If your NERSC username doesn't match the one on your desktop/laptop, use the –u flag:**

```
laptop$ ./sshproxy.sh -u elvis        # NERSC username is 'elvis'
```

- **If you want to set the name of the NERSC-generated keys differently:**

```
laptop$ ./sshproxy.sh -o different_name
```

- **Display all sshproxy.sh options:**

```
laptop$ ./sshproxy.sh -h
```

- **NX now supports ssh key authentication**
  - https://docs.nersc.gov/connect/nx/#creating-a-connection-to-nersc-with-sshproxy

sshproxy for Windows

- **sshproxy supports PuTTY, a popular Windows SSH tool**

- **It can generate a ssh key in the PPK (PuTTY Private Key) format**

- **The key can be used with PuTTY or tools that support that format**

- **Install PuTTY on your desktop/laptop from https://www.putty.org/ (or, eventually, https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html)**

What to do on Windows desktop/laptop

- **Using your favorite scp/sftp tool, download sshproxy.exe from NERSC's /project/projectdirs/mfa/NERSC-MFA/ directory to your desktop/laptop**
  - Let's say that you downloaded it to C:\Users\elvis\Documents
- **Open 'Command Prompt,' the command-line interpreter**
- **Run sshproxy.exe on your desktop/laptop once a day**
  - Specify NERSC username with –u flag
  - Authenticate with password+OTP
  - A ssh key file is downloaded to the current folder

```
C:\Users\elvis\Documents> dir
...
08/23/2019  09:20 AM         8,160,768 sshproxy.exe
...

C:\Users\elvis\Documents> sshproxy.exe –u elvis
Enter the password+OTP for elvis: **************
Key was written to nersckey.ppk.
Run "pageant nersckey.ppk" to load the key.
Then run putty instances like this: putty —agent elvis@cori.nersc.gov

C:\Users\elvis\Documents> dir
...
08/23/2019  09:25 AM             1,438 nersckey.ppk
```
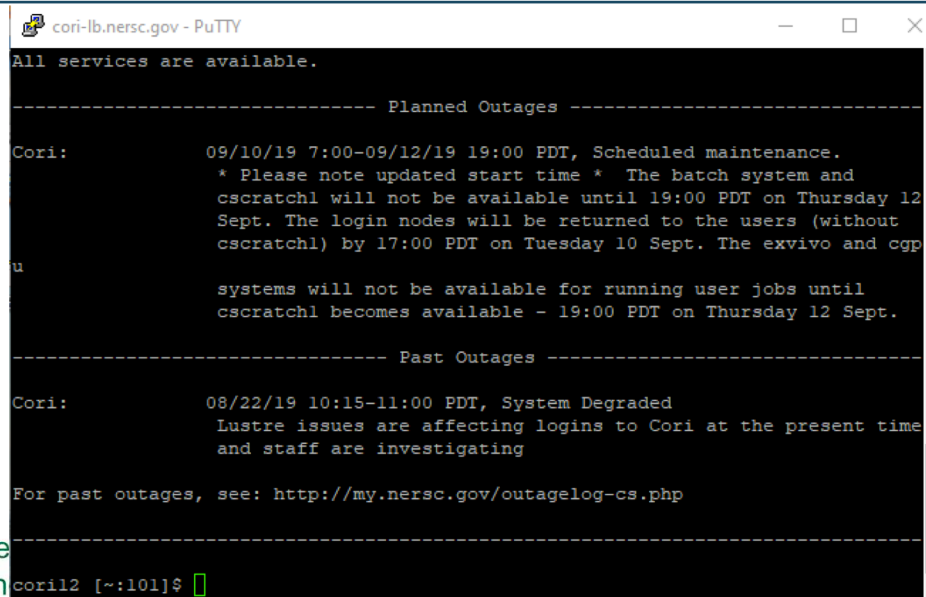
What to do on Windows desktop/laptop (cont'd)

- ## Use the key with PuTTY for subsequent ssh sessions
  - Method 1: As suggested:
    - Load the key into Pageant, PuTTY's ssh authentication agent (similar to Unix's ssh-agent)
    - Then, run the putty command to ssh to a NERSC host

```
C:\Users\elvis\Documents> pageant nersckey.ppk

C:\Users\elvis\Documents> putty -agent elvis@cori.nersc.gov
```

What to do on Windows desktop/laptop (cont'd)

- Method 2 (better): Configure to use the key in PuTTY tool
  - In the '**Host Name (or IP address)**' field, enter *username*@cori.nersc.gov
  - Select '**Connection** > **SSH** > **Auth**' menu in the left frame
  - Click the '**Browse...**' button in the '**Private key file for authentication**' field to select the PPK file you downloaded
  - Go back to the '**Session**' category in the left frame
  - Put a name in the '**Saved Sessions**' field (e.g., cori) and click the '**Save**' button
  - When you want to login to Cori next time, load the configuration from the '**Saved Sessions**' menu and click '**Open**'
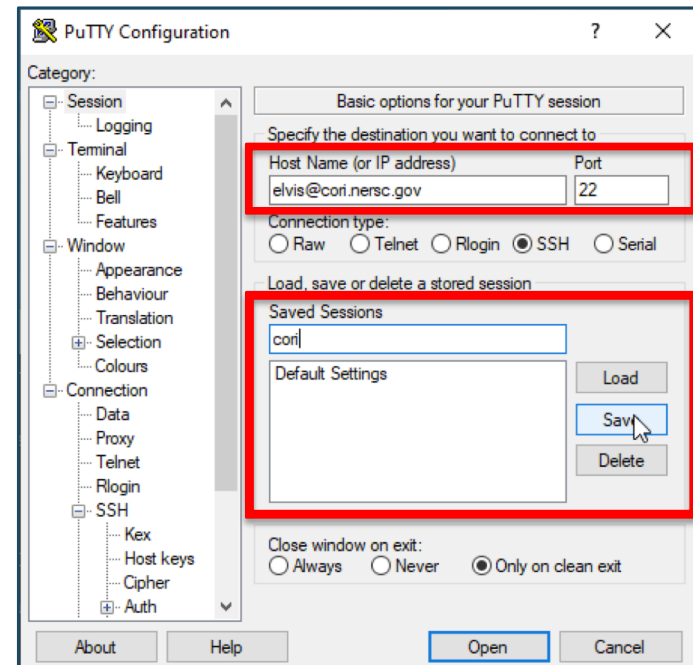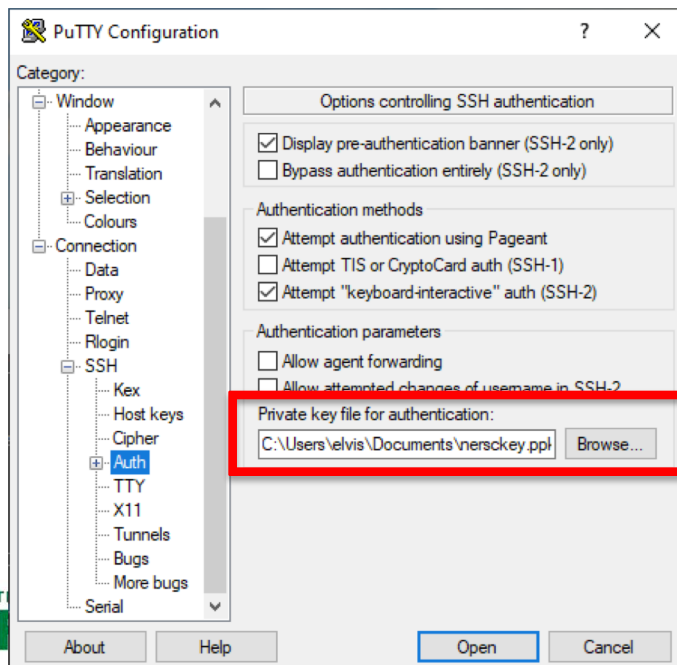
sshproxy miscellany on Windows desktop/laptop

- **<u>Always</u> use the –u flag with NERSC username**

```
C:\Users\elvis\Documents> sshproxy.exe –u elvis
```

- **If you want to set the name of the NERSC-generated keys differently:**

```
C:\Users\elvis\Documents> sshproxy.exe –o different_name
```

- **Display all sshproxy.sh options:**

```
C:\Users\elvis\Documents> sshproxy.exe –h
```

- **NX does not support ssh key authentication with a PPK key**
  - Use password+OTP
  - https://docs.nersc.gov/connect/nx/#creating-a-connection-to-nersc-without-sshproxy

U.S. DEPARTMENT OF **ENERGY** | Office of Science

BERKELEY LAB
Lawrence Berkeley National Laboratory

Some Q/A's

- **(Q) Can I get long-term ssh keys?**
  - You can make a request from NERSC online help (https://help.nersc.gov), but your request will be reviewed
- **(Q) I want to use tool _X_ that requires authentication to a NERSC host...**
  - Check the tool's documentation to see whether it supports ssh key authentication
  - If it does, try to make it use ssh keys generated by sshproxy
  - If it doesn't, you're out of luck - authenticate with password+OTP
- **(Q) I have my personal (permanent) ssh public key in GitHub, GitLab, a 3rd party host ..., how can I access there from Cori without being prompted to authenticate?**
  - Try to use the old way with the key (see slide #3)
    - Set 'ForwardAgent yes' for Cori in desktop/laptop's ~/.ssh/config
    - ssh-add the key on your desktop/laptop
    - Check if the key has been forwarded on Cori ('ssh-add –L') after ssh'ing to Cori
  - Some people say that this doesn't work for them, however
- **For more:**
  - https://www.nersc.gov/users/connecting-to-nersc/mfa/

National Energy Research Scientific Computing Center