Overview of Anvil

Jingchao Zhang

September 5, 2017
What is Anvil?

• **Anvil** is the Holland Computing Center's cloud computing resource, based on the OpenStack software

• Anvil was created to address the needs of NU's research community that are not well served by a traditional batch-scheduled Linux cluster environment

Examples of use cases that are well suited to Anvil include:

• A highly interactive environment, especially GUI applications
• Research requiring root-level access, such as kernel modification or virtualization work
• Alternate operating systems, such as Windows or other distributions of Linux
• Test cluster environments for various software frameworks, such as Hadoop or Spark
• Cluster applications that require a persistent resource, such as a web or database server
Steps for Anvil access

1. **Connect to the Anvil VPN** *
2. Create SSH keys
3. **Create an Anvil Linux CentOS 6 instance**
4. **Connect to the Linux instance** *

* These are the only steps you will have to repeat in the future to connect to your instance.
1. Connect to the Anvil VPN (virtual private network)

- The Anvil web portal is accessible from the Internet in general
- For security reasons, the Anvil instances are not
- In order to access the Anvil instance from on and off-campus, you will need to first connect to the Anvil VPN
- If you've already connected to the UNL VPN service before, you'll already have the Cisco AnyConnect client installed and can use it to connect to Anvil VPN
- Otherwise, please click the following link, https://vpn.unl.edu/
1. Connect to the Anvil VPN

- Cisco AnyConnect client:
  - Click on https://vpn.unl.edu/
  - Group = Full
  - Enter your Blackboard/Canvas username/password, NOT your HCC username/password
  - Click on the Login button
1. Connect to the Anvil VPN

- Cisco AnyConnect client:
1. Connect to the Anvil VPN

- **Cisco AnyConnect client:**
  - Save the file in a convenient location
  - Open the file and follow the installation steps
1. Connect to the Anvil VPN

• Open the "Cisco AnyConnect Secure Mobility Client" and connect to anvil-vpn.unl.edu
1. Connect to the Anvil VPN

• Login with your **HCC username and password**
1. Connect to the Anvil VPN

- Login with Duo

<table>
<thead>
<tr>
<th>Type</th>
<th>To</th>
</tr>
</thead>
<tbody>
<tr>
<td>push</td>
<td>Push a login request to your phone. Just review the request and tap &quot;Approve&quot; to log in.</td>
</tr>
<tr>
<td>phone</td>
<td>Authenticate via phone callback.</td>
</tr>
<tr>
<td>sms</td>
<td>Get a new batch of SMS passcodes.</td>
</tr>
<tr>
<td>A passcode</td>
<td>Log in using a passcode, either generated with Duo Mobile, or your YubiKey</td>
</tr>
</tbody>
</table>
2. Create SSH keys

- OpenStack uses SSH key pairs to identify users and control access to the VMs themselves, as opposed to the traditional username/password combination.

- SSH key pairs consist of two files, a public key and a private key:
  - The public file can be shared freely; this file will be uploaded to OpenStack and associated with your account.
  - The private key file should be treated the same as a password.
  - Treat the private key file the same as you would a password.
  - Keep your private key in a secure location and do not share it with anyone.
2. Create SSH keys

Anvil Instance  Public Key  Private Key

Don’t forget to attach your public key to your Anvil instance when you are creating the instance.
2. Create SSH keys

- From your web browser, navigate to
  https://anvil-beta.unl.edu
- Enter your HCC username
- If you have a Yubikey, in the password window, type your HCC password first, add a comma, then press Yubikey.
2. Create SSH keys

• Connect to the Anvil VPN - ✔

• Log into the Anvil web dashboard at anvil-beta.unl.edu using your HCC credentials - ✔

• On the left-hand side navigation menu, click Access & Security
2. Create SSH keys

• Choose the **Key Pairs** tab in the main window section:

![Access & Security](image)

• On the right-hand side, click the **Create Key Pair** button:
2. Create SSH keys

- Fill the **Key Pairs Name** with a name to your instance, then click **Create Key pair**:

  - The Key Pair should be downloaded automatically.
2. Create SSH keys

- You should then see an entry with the saved key (the fingerprint value will be different than the example below)

### Access & Security

<table>
<thead>
<tr>
<th>Key Pair Name</th>
<th>Fingerprint</th>
<th>Actions</th>
</tr>
</thead>
</table>

- The key pair can now be associated with any newly created instances
  - You can use the same key pair with multiple instances
2. Create SSH keys (Windows user only)

- One more step for windows users. The .pem file cannot be recognized by PuTTY. It needs to be transformed into .ppk format.

- To make the file format transfer, use PuTTYgen.

- If you downloaded PuTTY before, then you already have PuTTYgen. Otherwise download PuTTY first. (direct download [link](#))
2. Create SSH keys (Windows user only)

Step 1

- Choose to generate a new key pair.
- Click on "Generate".
- Select the key type (e.g., RSA, DSA, ECDSA).
- Specify the number of bits for the key.
- Click on "Save public key" and "Save private key".

Step 2

- Load the generated private key into PuTTYgen.
- Click on "Load".
- Select the key type and upload the private key file.
- After import, click on "OK".
- Use the "Save private key" command to save the key in PuTTY's own format.
2. Create SSH keys (Windows user only)

**Step 3**

*PuTTY Key Generator*

- **File**
  - Key: Generate a public/private key pair
  - Load an existing private key file
  - Save the generated key
  - Save public key

- **Key**
  - Key fingerprint
  - Key comment
  - Key passphrase
  - Confirm passphrase

- **Actions**
  - Generate a public/private key pair
  - Load an existing private key file  
  - Save the generated key

- **Parameters**
  - Type of key to generate: RSA, DSA, ECDSA, ED25519, SSH-1 (RSA)
  - Number of bits in a generated key: 2048

**Step 4**

*PuTTY Key Generator*

- **Key**
  - Public key for pasting into OpenSSH authorized_keys file

- **Warning**
  - Are you sure you want to save this key without a passphrase to protect it?

- **Actions**
  - Generate a public/private key pair
  - Load an existing private key file
  - Save the generated key

- **Parameters**
  - Type of key to generate: RSA, DSA, ECDSA, ED25519, SSH-1 (RSA)
  - Number of bits in a generated key: 2048
3. Create an Anvil Linux CentOS 6 instance

• Connect to the Anvil VPN - ✅

• Log into the Anvil web dashboard at **anvil-beta.unl.edu** using your HCC credentials - ✅

• On the left-hand side navigation menu, click **Images**
3. Create an Anvil Linux CentOS 6 instance

- Choose **CentOS 6.8**
- Click on **Launch Instance**
3. Create an Anvil Linux CentOS 6 instance

- A pop-up box will appear with additional details about the instance
- There are 5 tabs: Details, Access & Security, Networking, Post-Creation, Advanced Options
- In the Details tab, enter a name for the instance and select `general.small` from the drop-down menu under Flavor

![Launch Instance form with selected options]
3. Create an Anvil Linux CentOS 6 instance

• Click the **Access & Security** tab

• Under **Key Pair**, select your SSH key pair from the drop-down menu

• Under **Security Groups**, check the default box
3. Create an Anvil Linux CentOS 6 instance

- Click the **Networking** tab
- Under **Available networks**, click the small *blue '+' icon* in the *Cluster Interface* box
- This will add *Cluster Interface* to the **Selected networks**
3. Create an Anvil Linux CentOS 6 instance

• Click the **Launch** button to start the instance

• It may take several minutes for the instance to complete
4. Connect to the Linux CentOS instance

• After an instance has been created, you can connect (login) and begin using it.

• Connecting is done via SSH or X2Go for Linux instances and via Remote Desktop (RDP) for Windows instances. We use Linux instance for this workshop.

• Windows:
  • Using PuTTY

• Mac:
  • Using Terminal
4. Connect to the Anvil Linux instance (Mac user)

1. Change the permission of your .pem file. Command is ‘chmod 600 ~/Downloads/YourPemFileName’
2. ssh to your VM using Terminal. Command is ‘ssh -i ~/Downloads/YourPemFileName centos@10.71.106.58’
3. Note, **username** to access Centos Linux instance is always ‘centos’.

More instructions: https://hcc-docs.unl.edu/display/HCCDOC/Connecting+to+Linux+Instances+from+Mac
4. Connect to the Anvil Linux instance (Windows user)

More instructions: https://hcc-docs.unl.edu/display/HCCDOC/Connecting+to+Linux+instances+from+Windows
4. Connect to the Anvil Linux instance (Windows user)

User name is ‘centos’ for all CentOS instance

More instructions: https://hcc-docs.unl.edu/display/HCCDOC/Connecting+to+Linux+instances+from+Windows
1. Connect to the Anvil VPN
2. Create SSH keys
3. Create an Anvil Linux CentOS 6 instance
4. Connect to the Linux instance

Try exiting all programs and connecting to your instance again