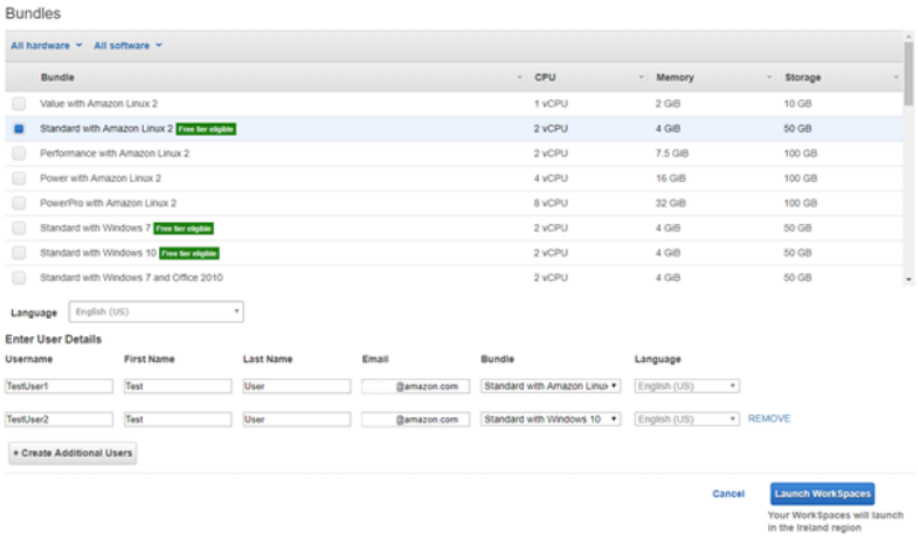
BAP207-Up and Running With Amazon Linux Workspaces Lab Guide

Launch Your Workspace and Directory

Note: This section assumes that you are using a new account and have never created WorkSpaces in this Account and/or Region. If that is not the case, jump to [Appendix 1: If you are using an Account that has already housed WorkSpaces in US-WEST-2.]

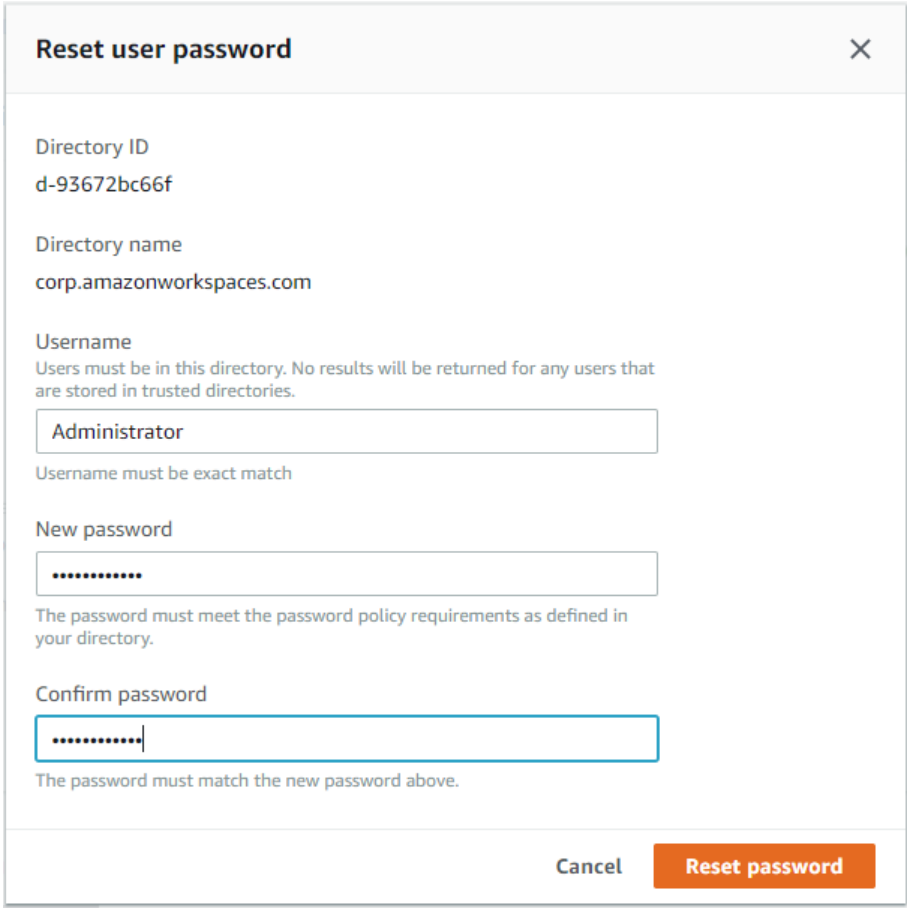
1. Browse to the Amazon Workspaces Service page, for Oregon, in your console
   https://us-west-2.console.aws.amazon.com/workspaces
2. Click Get Started Now
3. Next to Quick Setup Click **Launch**
4. Check **Standard with Amazon Linux 2**
5. Enter a Username and a valid E-Mail address
6. Click **+ Create Additional Users**
7. Enter a Username and the same E-Mail address
8. Change the bundle for your second user to **Standard with Windows 10**



9. Select **Launch WorkSpaces** *(This step will take approx. 20 minutes)*
10. Switch to the Directories page in the WorkSpaces Console and make note of the **Directory ID**
11. Switch to the Directory Services Page in the Amazon Console
    https://us-west-2.console.aws.amazon.com/directoryservicev2

NOTE: Wait for your Directory show Active under Status

12. Click on the Directory ID of the Directory you noted in Step 11
13. Click the **Reset user password** button in the upper right
14. Enter **Administrator** and a new password



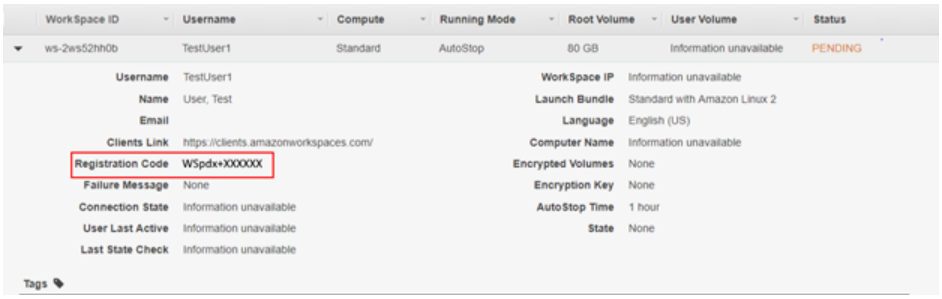
15. Click **Reset password**

Enable SSH between WorkSpaces

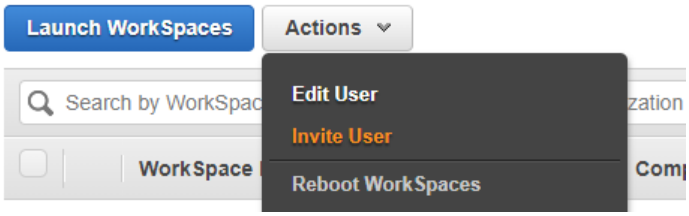
16. Go to the EC2 Security Groups Page by selecting the **Services** menu (https://us-west-2.console.aws.amazon.com/vpc/v2/home?region=us-west-2#securityGroups)
17. Select **EC2**
18. Select **Security Groups** from the Left Hand menu under **Network and Security**
19. There will be 2 Security Groups with Group Names that start with the Directory ID of the Directory you created. Find the one that ends with _workspacesMembers and select it

20. Change to the **Inbound** menu in the details section at the bottom of the page
21. Click the **Edit** button
22. Modify the blank rule to allow SSH access from member of the group

23. Click Save
24. Return to the WorkSpaces Service page
25. Expand one of the WorkSpaces and note the Registration Code (It should be



26. When your WorkSpaces are ready, you will receive emails to set the passwords for your newly created users and their Status will change to Available.
27. Check the radio box next to your first WorkSpace
28. Click **Actions**
29. Select **Invite User**



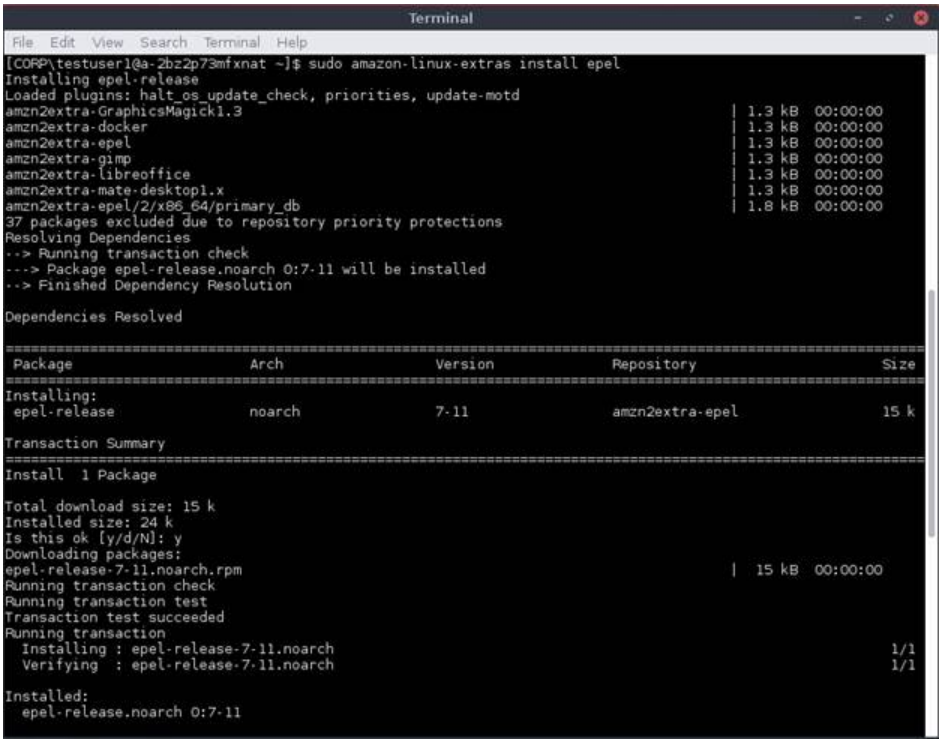
30. Find the Invite URL in the message body and copy it into your browser
31. Set a new password for your user
32. Repeat steps 27 thru 31 for your second WorkSpace
33. Open the WorkSpaces software client on your system and enter the registration code you noted in step 25

Setup your Linux WorkSpace

1. At the Login Prompt enter the Username and Password for your Linux user and click **Sign In**
2. Click the Terminal icon in the panel
3. Update the system by typing **sudo yum update** (press y when prompted)

Add EPEL from Amazon Linux Extras

4. Add the EPEL repository using Amazon Linux Extras by typing **sudo amazon-linux-extras install epel** (press y when prompted)



Setup your Developer Environment

5. Open Firefox using the shortcut in your panel
6. Browse to https://code.visualstudio.com
7. Click the .rpm download link
8. Copy the instructions for RHEL,Fedora and CentOS into your terminal one command at a time

```
sudo rpm --import https://packages.microsoft.com/keys/microsoft.asc
sudo sh -c 'echo -e "[code]\nname=Visual Studio Code\nbaseurl=https://packages.microsoft.com/yumrepos/vscode\nenabled=1\ngpgcheck=1\ngpgkey=https://packages.microsoft.com/keys/microsoft.asc" > /etc/yum.repos.d/vscode.repo'
```

9. Update your repository index by typing **sudo yum check-update**
10. Install VSCode by entering **sudo yum install code** (enter y when prompted)

Configure Admin Access

11. Open the access.conf file for editing in Pluma by typing **sudo pluma /etc/security/access.conf** in your terminal
12. Scroll down to find the entry for the assigned user and add **+:(corp\LinuxAdmins):ALL**

```
#
# All other users should be denied to get access from all sources.
#-:ALL:ALL
+:corp\testuser1,(corp\domain admins):ALL
+:(corp\LinuxAdmins):ALL
-:ALL:ALL
```

13. Exit Pluma and Save
14. In your terminal type in **sudo visudo**
15. Scroll to the bottom
16. Press **o**
17. Enter **%corp\\LinuxAdmins ALL=(ALL) ALL**

```
## Allows members of the users group to shutdown this system
# %users  localhost=/sbin/shutdown -h now
%corp\\LinuxAdmins ALL=(ALL) ALL
```

18. Press the Esc key
19. Enter **:wq!** and press Enter

Configure PCoIP Protocol Settings

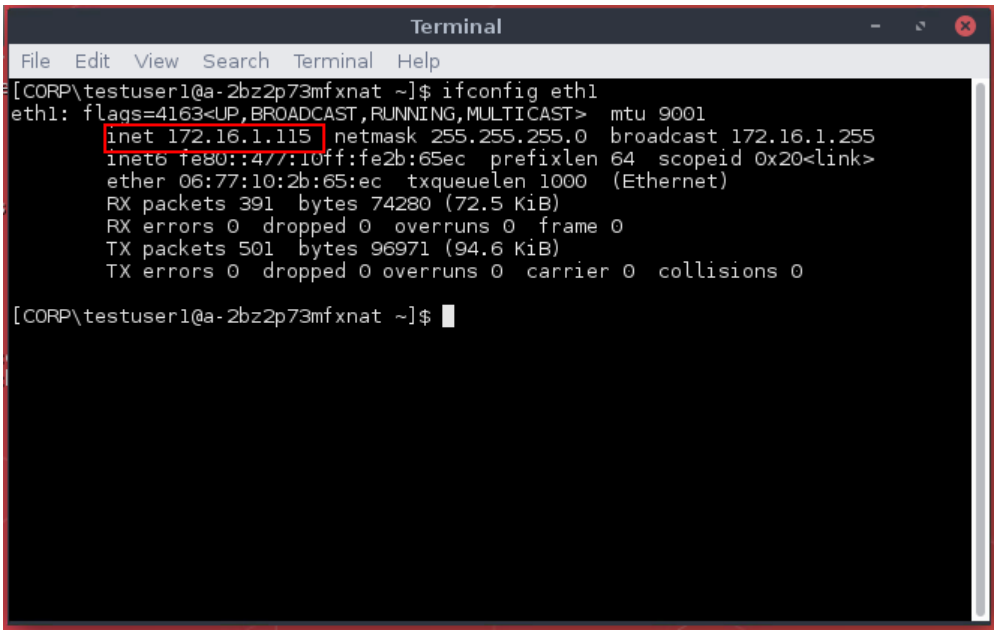
20. Open the PCoIP settings file for editing, in Pluma, by typing **sudo pluma /etc/pcoip-agent/pcoip-agent.conf**

Note: you can see all the available settings by looking at the Man entry. Just open a terminal and type man pcoip-agent.conf

21. For this lab we will configure verbose logging and ensure the clipboard is enabled in both directions

```
pcoip.event_filter_mode = 3
pcoip.desktop_session = mate
pcoip.server_clipboard_state =1
```

22. Exit Pluma and save when prompted
23. In your terminal find your WorkSpace IP by typing **ifconfig eth1** and make note of it (note: you can also find this in the WorkSpaces console by expanding the details of your WorkSpace)



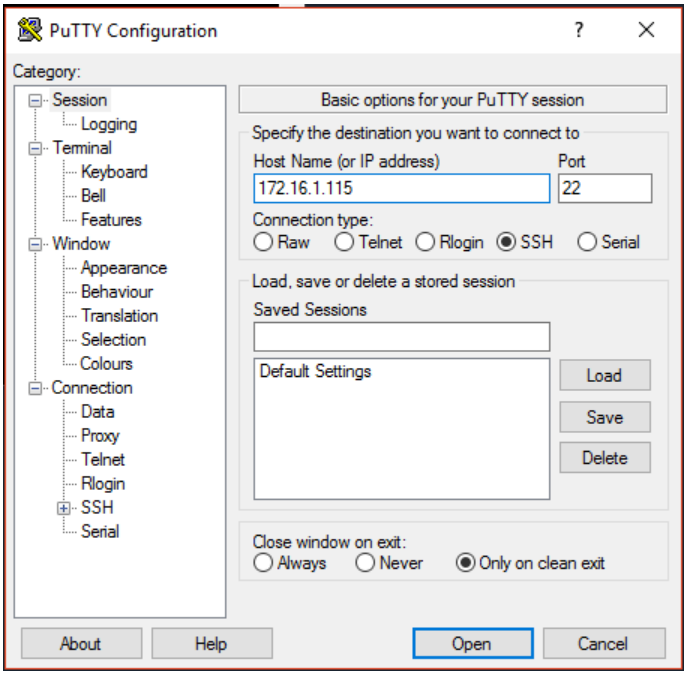
24. Disconnect from your Linux WorkSpace by selecting **Disconnect** from the **Connection** Menu

Setup your Active Directory Environment

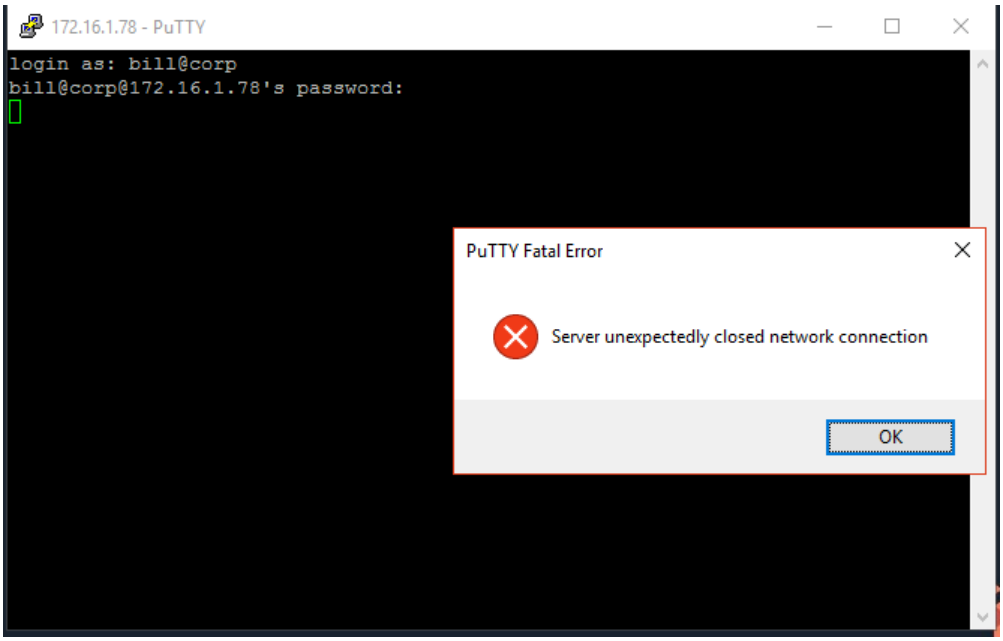
1. Enter the Username and Password for your Windows user and click **Sign In**
2. Open Firefox
3. Browse to https://www.putty.org
4. Click the link to Download Putty
5. Select the 64bit installer on the resulting page
6. Click Safe file when prompted
7. Click the Folder icon in the Windows Taskbar
8. Select Downloads from the quick Access Toolbar
9. Double click the Putty Installer
10. Click **Run**
11. Click **Next**, **Next**, **Install**
12. Select Yes at the UAC prompt
13. Click **Finish**

Verify you cannot SSH to your Linux System

14. Click Start
15. Type Putty
16. Click the match
17. Enter the IP you got in step 23, from the last section, in the **Host Name** field

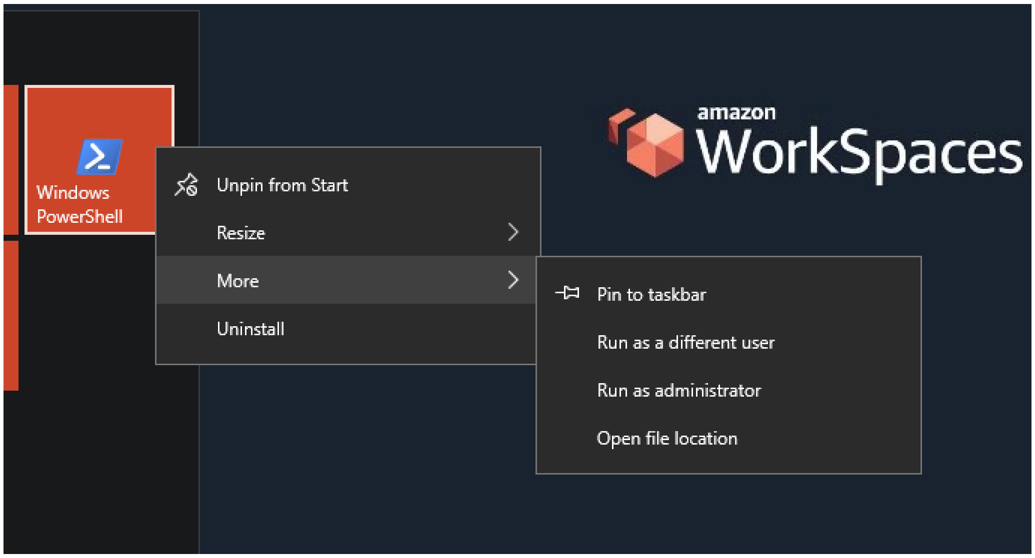


18. Click **Open**
19. Enter your Windows user's credentials in username@domain format
20. Enter your Windows user's password

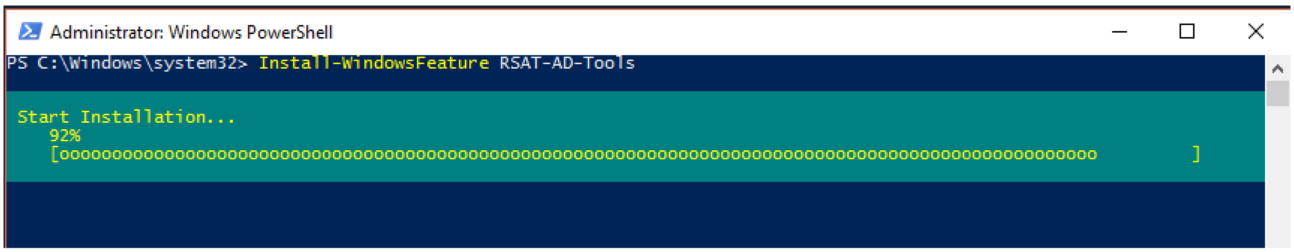


Add the user to your Linux Admins Group in AD

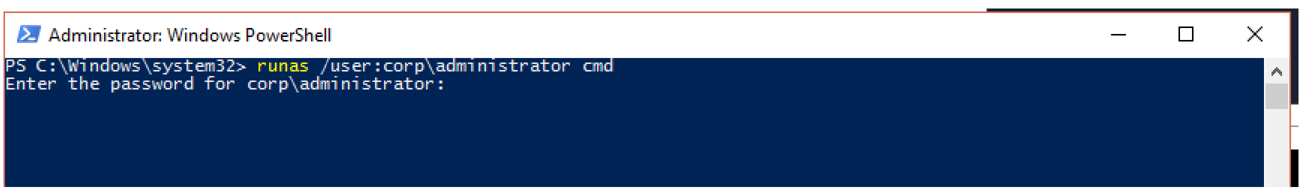
21. Click Start
22. Right click on the Windows PowerShell icon
23. Select More
24. Select Run as administrator



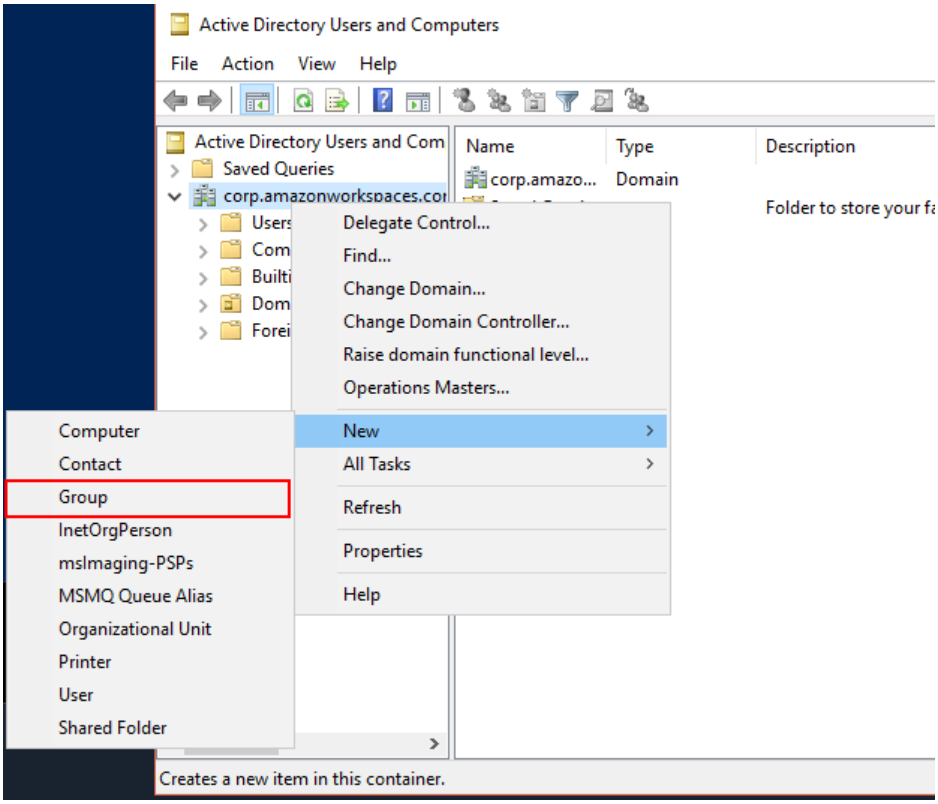
25. Select **Yes** at the UAC prompt
26. Enter **Install-WindowsFeature RSAT-AD-Tools** and press enter



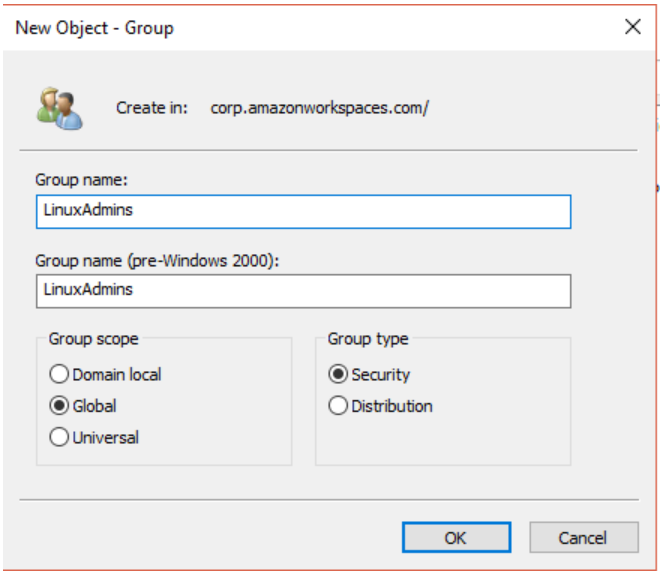
27. In the same prompt type **runas /user:corp\Administrator cmd** and press enter



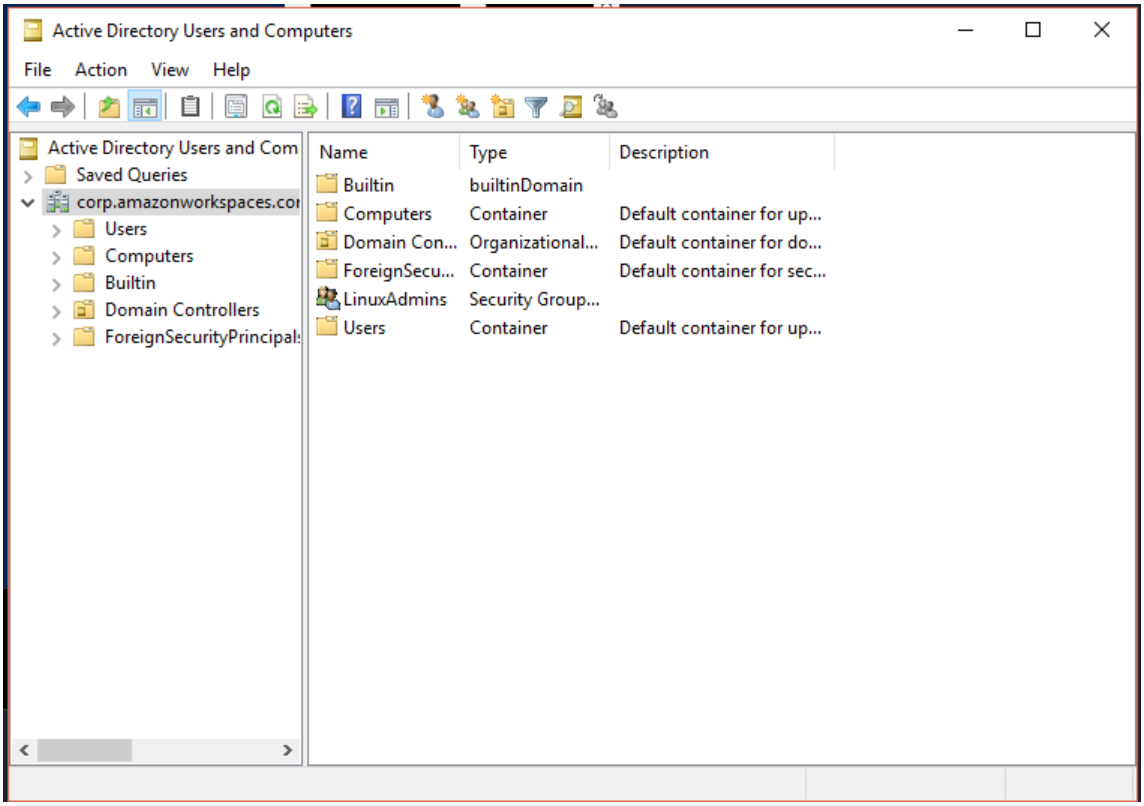
28. Enter the password you set for the Administrator user in step14
29. In the resulting prompt type dsa.msc (This will launch Active Directory Users and Computers as Administrator)
30. In the Active Directory Users and Computer window, right click **corp.amazonworkspaces.com**
31. Select New
32. Select Group



33. Create a **LinuxAdmins** group and click OK



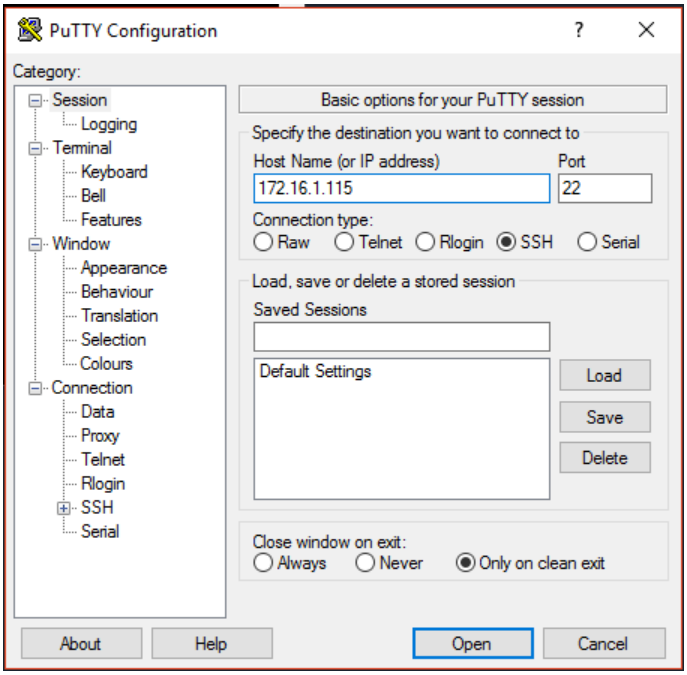
34. Double Click the newly created group in the DSA window



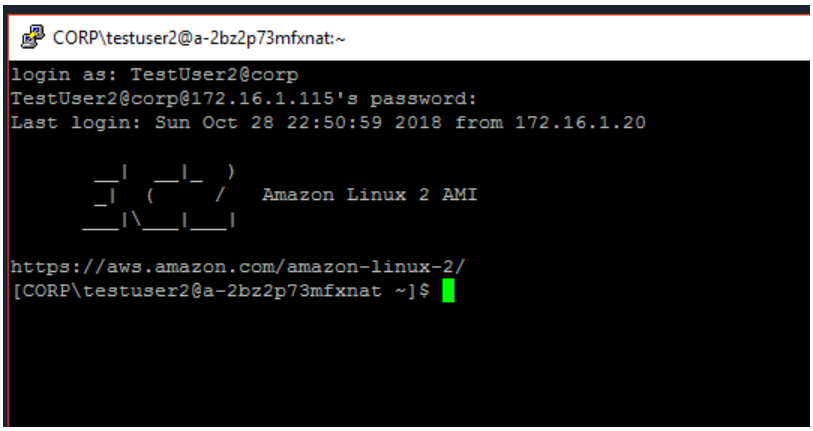
35. Select the **Members** Tab
36. Click **Add**
37. Enter the name of your Windows User
38. Click **Check Names**
39. Click **OK** twice
40. In the WorkSpaces **Connection** Menu, click **Disconnect**

Verify access

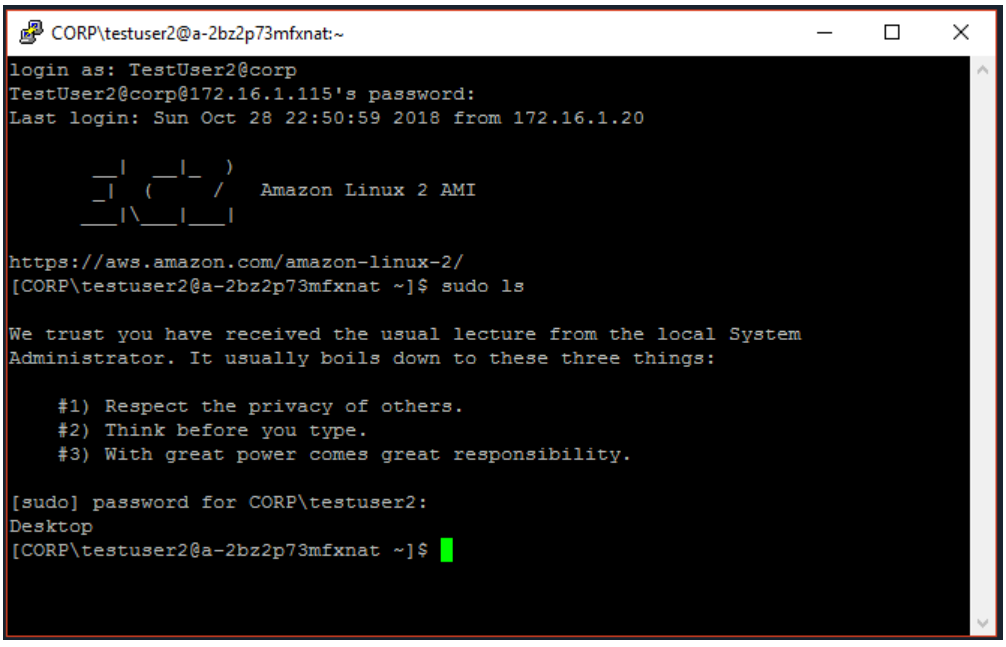
41. Disconnect from your Linux WorkSpace
42. Login as your Windows User again
43. Click Start
44. Type Putty
45. Click the match
46. Enter the IP you got in step 23, from the last section, in the **Host Name** field



47. Click **Open**
48. Enter your Windows user's credentials in username@domain format
49. Enter your Windows user's password



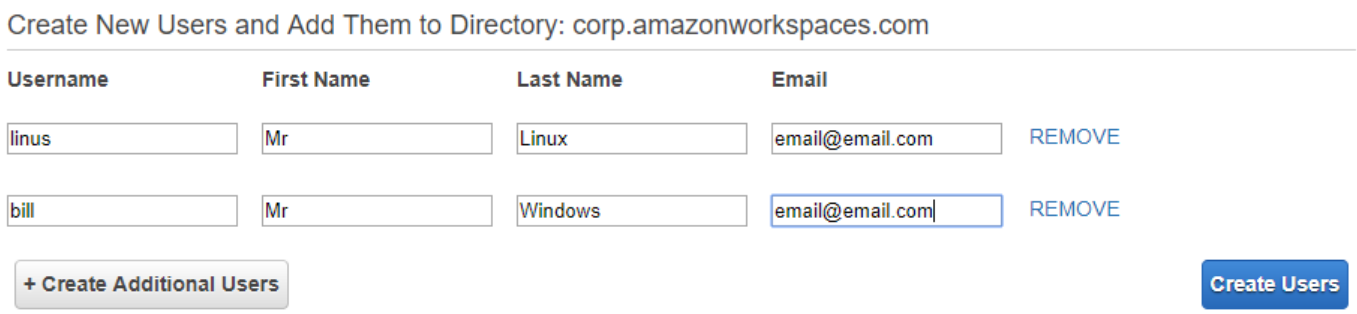
50. Verify you have sudo access by typing **sudo ls**



Appendix 1: If you are using an Account that has already housed WorkSpaces in US-WEST-2

Note: Ensure you are using a VPC that has internet access. Several steps in this Lab require your WorkSpaces download items from the internet.

1. Browse to the Amazon Workspaces Service page, for Oregon, in your console
   https://us-west-2.console.aws.amazon.com/workspaces
2. Select **Directories** from the left-hand menu
3. Click **Set up Directory**
4. Click **Create Simple AD**
5. Enter an **Organization name**, **Directory DNS**, and **Administrator password** (Make note of the Password. You will need it later)
6. Select a VPC and Subnets with Internet access (like your Default VPC) or create a new one
7. Click **Next Step**
8. Validate the details
9. Click **Create Simple AD** (This will take about 5 minutes)
10. Check the radio box next to your new directory
11. Click **Actions**
12. Select **Register**
13. Select **No** when prompted to enable WorkDocs
14. Select WorkSpaces from the left-hand menu
15. Click **Launch WorkSpaces**
16. Select your newly created Directory
17. Click Next Step
18. Create two user accounts



19. Click **Create Users**
20. Click **Next Step**
21. Modify the Bundle for your Windows user to **Standard with Windows 10**
22. Modify the bundle for your Linux user to **Standard with Amazon Linux 2**
23. Click Next Step
24. Leave the Defaults and click **Next Step**
25. Verify your settings and click **Launch WorkSpaces**
26. Go to **Enable SSH between WorkSpaces**