SEEDUbuntu 16.04 AWS setup instructions

Steve Cole (svcole@wustl.edu)

Washington University in St. Louis

Last modified 9/16/2020

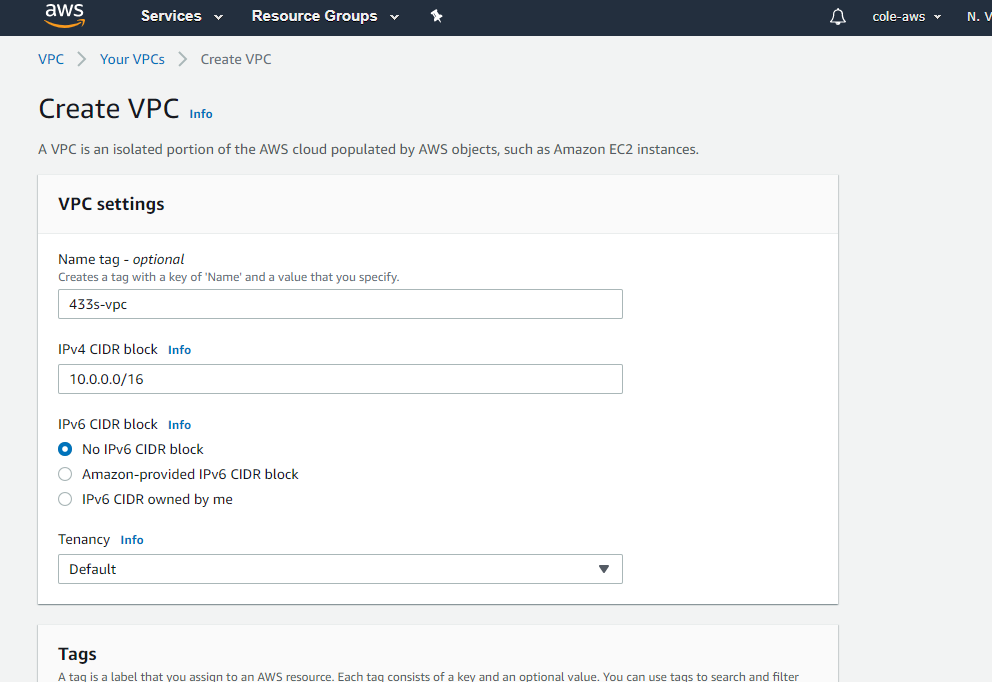
I have created an AWS AMI (Amazon Machine Image) derived from the [SEEDUbuntu-16.04-32bit](file:///C:\Users\coles\Documents\Custom%20Office%20Templates) .vmdk image provided on the [SEED Lab setup page](https://seedsecuritylabs.org/lab_env.html). The original image has been augmented with extra software packages and configurations to make it AWS friendly. The configurations allow remote GUI access to an instance launched from the AMI and strengthen the security of the instance in the public-accessibility context.

*Note:* The AMI is currently available as a “community” AMI in the us-east-1, us-west-1, and ap-east-1 regions under the name “SEEDUbuntu-aws.”

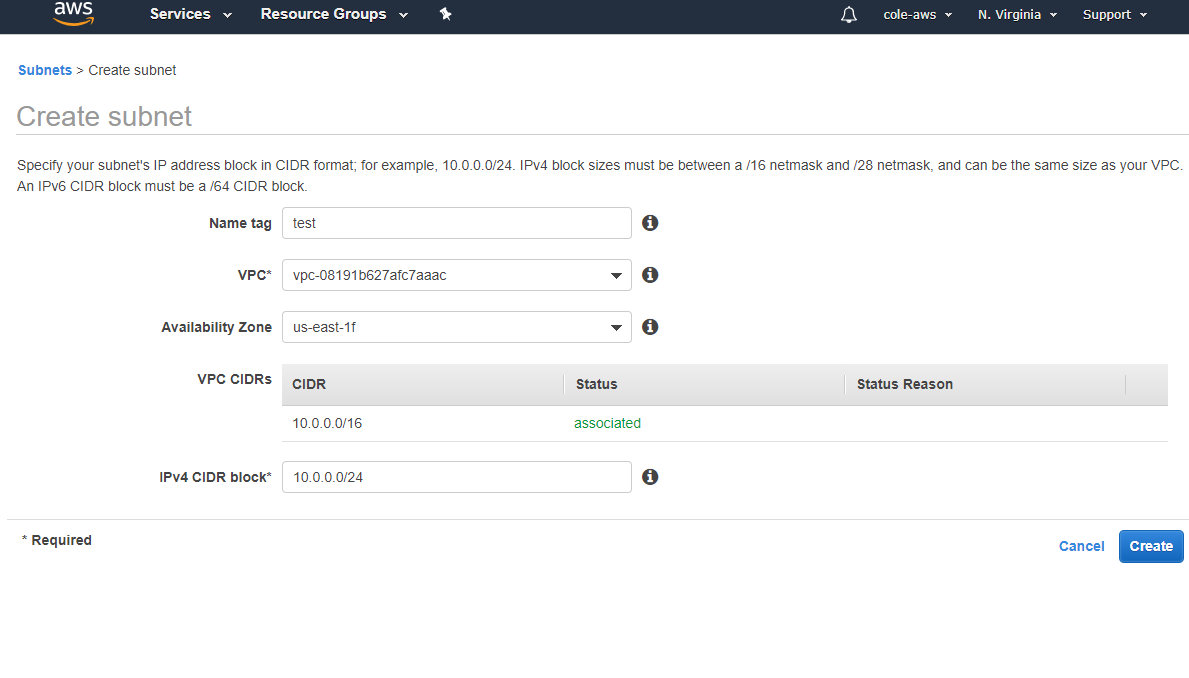
**How to Launch SEEDUbuntu VM:**

*Note: Steps 1-2 are only needed for setting up multiple SEEDUbuntu instances on the same local (virtual) subnet. For setting up a single SEEDUbuntu instance, these steps may be skipped.*

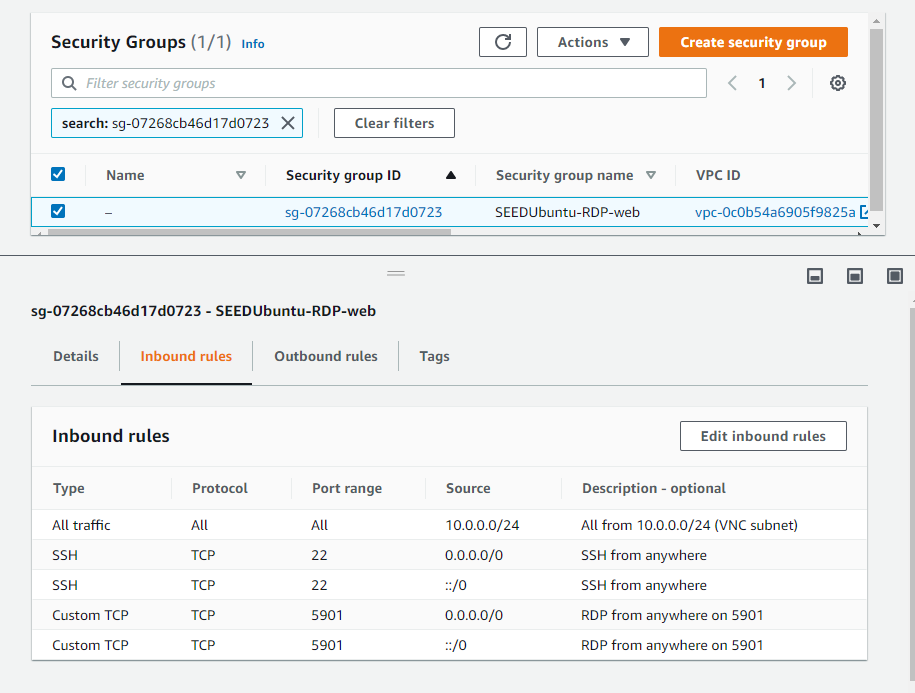
1. Create a new VPC (under Services -> VPC in AWS; VPCs are distinct from EC2). Set the CIDR block to 10.0.0.0/16.

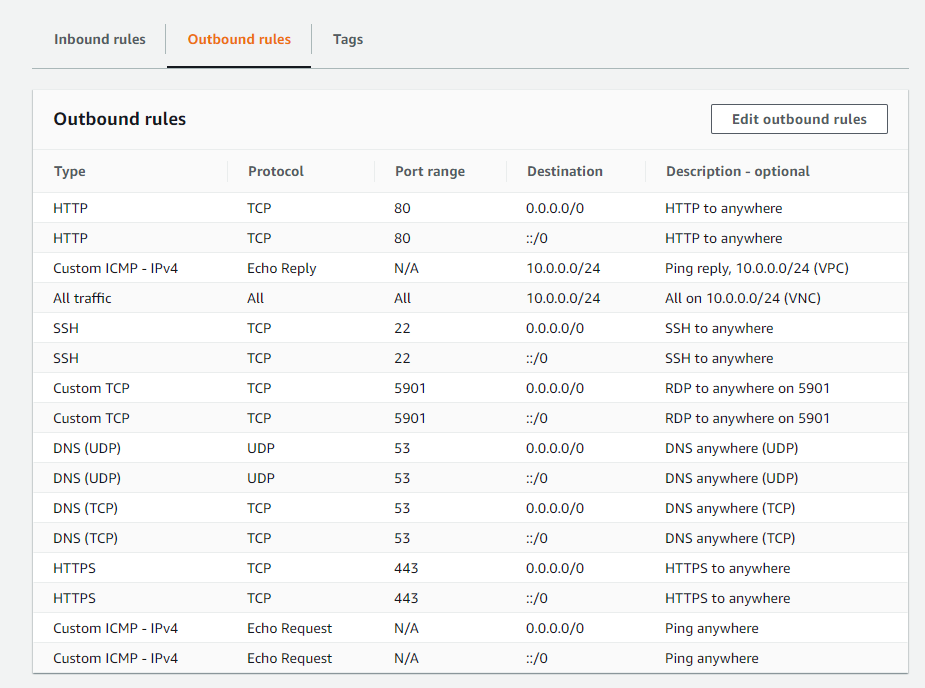


1. Create a new VPC subnet in the region in which the custom AMI image is available (currently us-east-1f). Be sure to select the VPC just created in the previous step. Give the subnet the CIDR block 10.0.0.0/24.



1. Create a security group with the following rules:
   1. Inbound: allow  TCP ports 22 (for SSH access) and 5901 (for remote desktop access via xrdp on custom port), (any traffic from local subnet (10.0.0.0/24) if using multiple machines only)
   2. Outbound: allow TCP ports 22 (SSH), 5901 (xrdp on custom port), 80, and 443 (so we can access the Internet from inside the SEED machine), ICMP for pings anywhere, UDP anywhere for DNS, (any traffic to local subnet (10.0.0.0/24) if using multiple machines only)





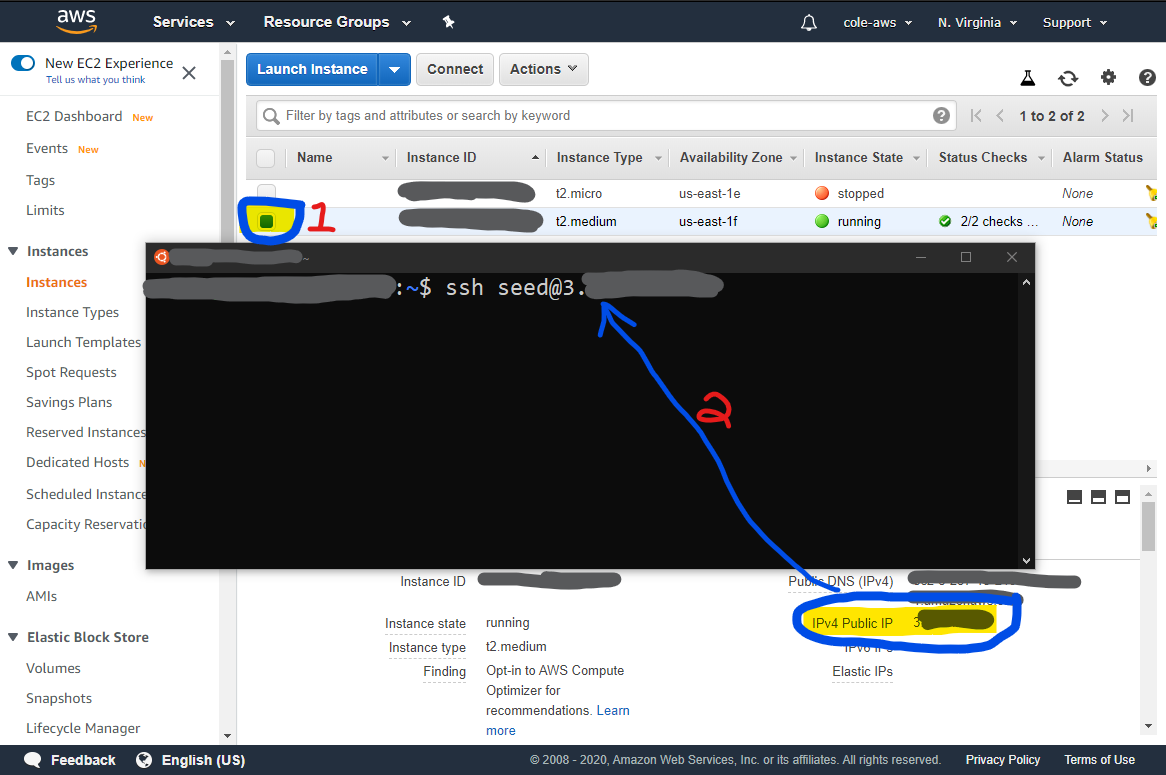
1. Launch a new instance with a configuration that includes the following:

* the custom AMI, which can be found by searching for “SEEDUbuntu-aws” in the “Community” section of AMI options. NOTE: this AMI is currently available in the regions us-east-1, us-west-1, and ap-south-1 . If you would like to create an instance in a different region, please contact Steve Cole.
* a suitable instance type (t4.medium recommended to give 4GB RAM and is the only instance tested so far, but smaller instances may be fine)
* the security group you created in Step 3
* the VPC subnet you created in Step 2 (*if setting up multiple machines on same local subnet)*.

**First Access to SEEDUbuntu Instance:**

Once an instance is launched with the above configuration, do the following:

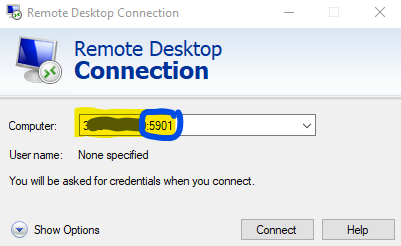
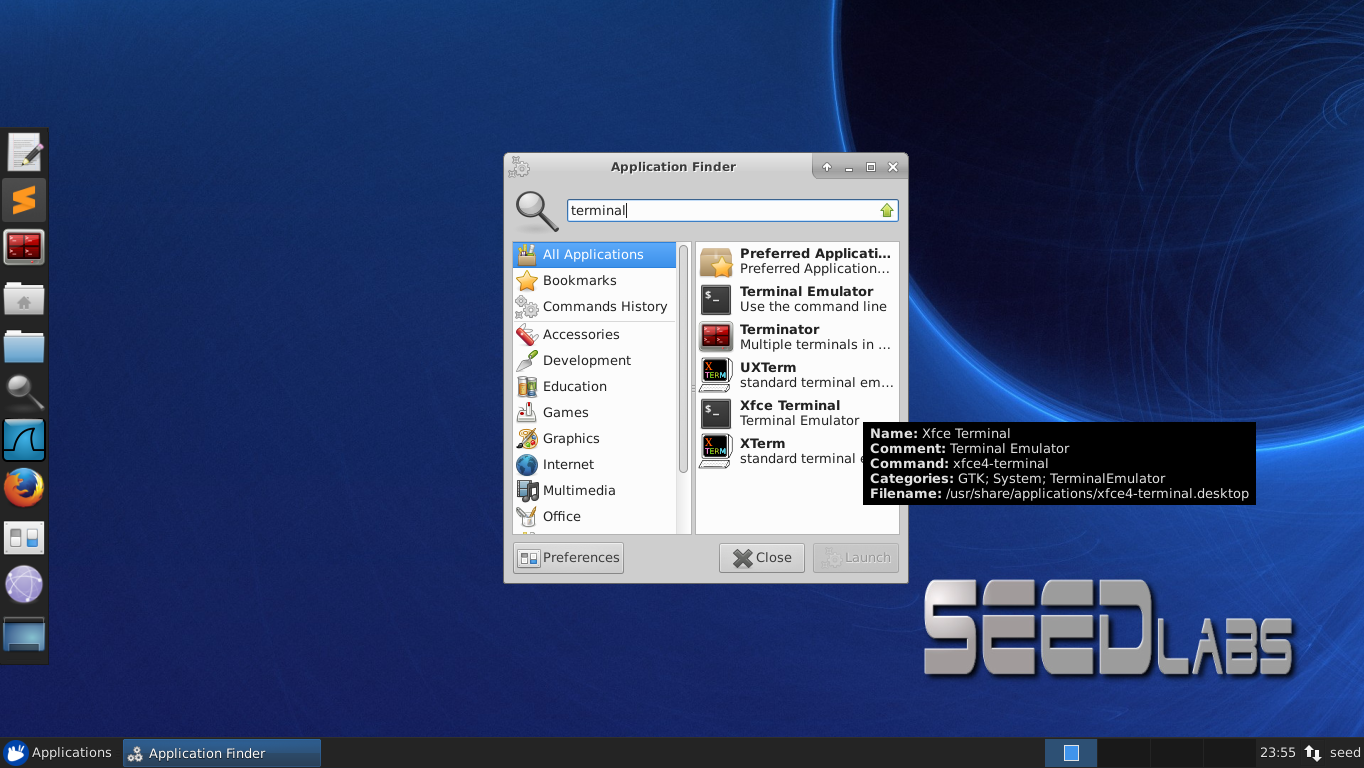
1. SSH to the instance using the AWS public IP assigned to the instance; e.g., “ssh [seed@3.4.5.6](mailto:seed@3.4.5.6)” .

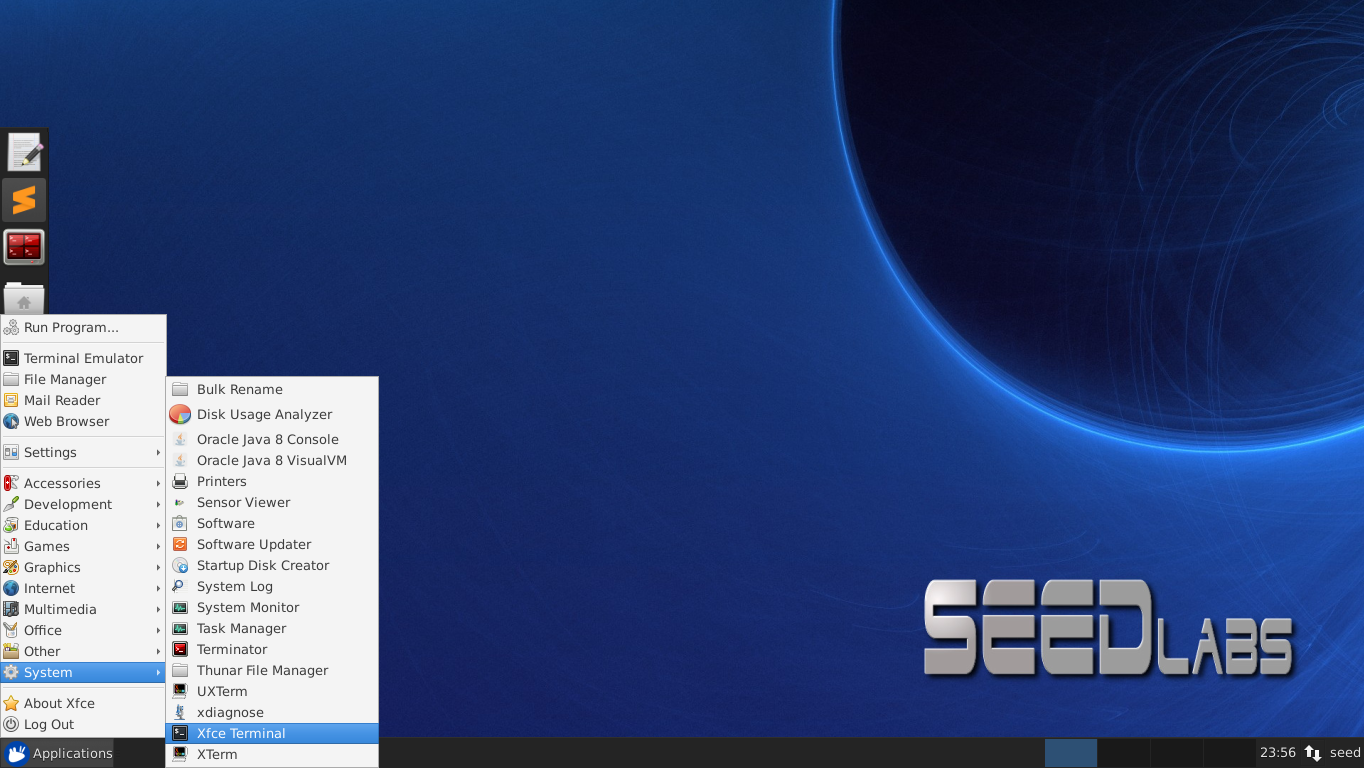


1. Enter the updated default password when prompted (NOT the same as the default password in the original SEEDUbuntu image!). The password is “**5sFr7%93#PJY**” (without the quotes).
2. Follow prompts to choose a new password. Note that the system will automatically log you out if the password is successfully changed.
3. Log in again using your new password to verify that it works.
4. You can now log in via SSH for command-line access or RDP for GUI Desktop access.

**Remote Desktop Access to SEEDUbuntu Instance:**

Note: you must complete initial login via SSH according to instructions above BEFORE logging in via RDP.

1. Open a remote desktop client that can use RDP (e.g. “Remote Desktop Connection” in Windows or “Microsoft Remote Desktop” on a Mac).
2. Instantiation a new connection to the IP address of the AWS image at port 5901; e.g., 3.4.5.6:5901 . Note the syntax: IP address followed by “:5901” .  
   
3. Log in as the “seed” user with your new password.
4. Note that the first time you log in, you may see an error and be immediately disconnected. If this happens, connect again and your login should succeed.
5. You should see the SEEDUbuntu desktop as usual, with a few slight changes due to using xfce4 as the desktop manager rather than the default Ubuntu desktop manager:  
   
   1. The “Terminal” application does not appear in the sidebar. You can either use the “Terminator” app in the sidebar, or open “Applications -> System” and select one of the terminal emulators from the list, or search for “terminal” in the application search tool in the toolbar (represented by the magnifying glass) and select a terminal emulator.  
      



**Testing local network configuration for SEED Labs (*if setting up multiple machines on same subnet*):**

1. Create 2 instances according to the above instructions and log in either via ssh or RDP.
2. Open a terminal on each instance and run “ifconfig -a” . You should see an interface with IPv4 address 10.0.0.x for some (unique) x for each machine.
3. Run “ping –c 5 10.0.0.x” from each machine, using the other machine’s IP address found in the previous step. You should see 5 results printing on the terminal one per second; if so, then the ping was successful.