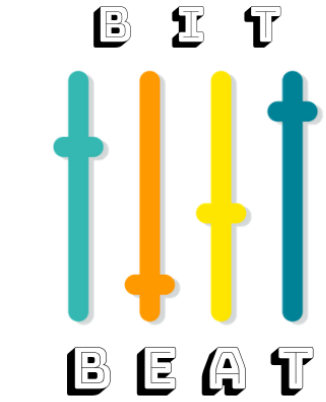
READ ME



World Domination One Beat At A Time

BitBeat is a new startup that is planning to take the record industry and the world by storm with its new product **BitBanger,** a web-based music mixer app.

As a new member of the **BitBeat** infrastructure team, you will need a variety of skills to assist in the growth of the startup. As the startup grows, the need for employees to work remotely also increases.

A new remote employee has just been hired. You have been asked to support their onboarding by creating a virtual server. You need to ensure the new hire can successfully SSH (Secure Shell) into the machine. SSH enables two computers to establish a secure and direct connection within a potentially unsecure network, such as the internet. It is important that you can successfully perform this task and that, in alignment with business requirements, you also train employees on how to do this for themselves.

BEFORE GETTING STARTED

Here's some important information to know before starting this hands-on activity.

Activity time: 60 minutes

Requirements: You must have an AWS Educate account.

Getting help: If you experience any issues as you complete this activity, please ask your instructor for assistance.

DID YOU KNOW

A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance. Amazon EC2 stores the public key, and you store the private key. You use the private key, instead of a password, to securely access your instances. Anyone who possesses your private key can connect to your instances, so it's important that you store your private keys in a secure place.

Task overview

In this hands-on activity, you are going to build a cloud webserver, create a key pair, and SSH into the Amazon Elastic Compute Cloud (EC2) instance.

Anyone who possesses your private key can connect to your instances, so it's important that you store your private keys in a secure place. When you launch an instance, you are prompted for a key pair. If you plan to connect to the instance using SSH, you must specify a key pair. You can choose an existing key pair or create a new one. When your instance boots for the first time, the public key content is placed on your Linux instance in an entry within `~/.ssh/authorized_keys`. When you connect to your Linux instance using SSH, you must specify the private key that corresponds to the public key content to log in.

Task objectives:

- Build a cloud webserver
- Create a key pair
- SSH into the Amazon Elastic Compute Cloud (EC2) instance

Learning outcomes

Provision and launch an EC2 instance, set up a sample webpage, create a key pair, and SSH into the virtual machine you create.

Let's get started!

Launch an EC2 instance

Follow these steps to launch an EC2 instance:

1. In the **AWS Management Console,** find and select the EC2 Dashboard.
2. From the **EC2 Dashboard**, click **Launch Instances.**
3. Notice the variety of AMIs located on the AMI page. These are different templates for different types of machines. Select the **Amazon Linux 2 AMI** (HVM).
4. Notice the variety of instance types available. Select the **t2.micro instance**.
5. Select **Next: Configure Instance Details**.
6. Accept the default settings for the **Step 3: Configure Instance Details** page and scroll down to the bottom to see the **Advanced Details** section.
    a. Expand Advanced Details. A field for **User data** will appear.
    b. Copy the following commands and paste them into the **User Data** field:

Important info

- This is referred to as "*bootstrapping*," providing code that runs when a computer starts up. Make sure you don't insert additional characters or spaces at the end of your code.

```
#!/bin/bash
yum-y install httpd
systemctl enable httpd
systemctl start httpd
echo '<html><h1>Hey Guru, You have mad Cloud
skills! </h1></html>' >/var/www/html/index.html
```

Here's what this bash script does; see if you can identify which actions each line of script executes:

i. Installs, enables, and starts the Apache HTTP Server
ii. Creates an index.html page with a message

Let's add some storage to our instance, tags and security groups:

7. Click **Next: Add Storage** (You will not need another EBS volume).
8. Click **Next: Add Tags.**
9. Click **Add tag** then configure:
    a. **Key:** Name **Value**: SSH Practice Server
    b. **Key:** Department **Value**: Development
10. Click **Next: Configure Security Group.**
11. Configure a **new** security group as follows:
    1. **Security Group** Name: SSH Practice SG.
    2. **Description:** This security group is for SSH practice and training.
    3. By default, the Type SSH with Port 22 has been added.
    4. Click **Review and Launch.**
12. Review the details, scroll down, and click **Launch**.
13. The key pair modal displays. In the dropdown, select **Create a new key pair,** in the **Key pair** name box, name your key pair My_SSH_Key and then click **Download Key Pair**. Save to your desktop.
14. After you have downloaded your key pair to your desktop, click **Launch Instances.**
15. On the **Launch Status** page, scroll to the bottom and click **View Instances.** You'll be taken to the Instances page.

Wait for your new EC2 **Instance State** to display as running.

DID YOU KNOW

SSH enables two computers to establish a secure and direct connection within a potentially unsecure network, such as the internet. This is necessary so that third parties cannot access the data stream, which would result in sensitive data falling into the wrong hands. SSH encrypts the connection between two computers and enables a second one to be operated from one computer.

SSH not only provides an encrypted connection, but also ensures that only connections are established between the **designated** computers and that the corresponding data cannot be manipulated on its way to the recipient.

SSH has many different areas of application including:

- Managing servers that cannot be accessed locally
- Securing transmission of files
- Securing creation of backups
- Connecting between two computers with end-to-end encryption
- Remote maintenance from other computers

Now that your Amazon EC2 instance is running:

1. Select your SSH Practice Server Instance and Copy the **IPV4 Public IP** address located near the bottom of your screen to your clipboard.
2. Paste the **IPv4 Public IP** address into a new browser window and observe the results.

Did your webpage load properly? If not, what might be the reason why?

_____

_____

Troubleshooting EC2

You successfully launched your SSH Practice Server but when you tried to access the Public IP address, there was an error: *This site cannot be reached*. You won't be able to access the application if you can't reach the webserver. You need to figure out how to fix this issue. Review the previous steps and read about security groups.

Are you allowing normal web traffic (Port 80) to access your webserver? Did you configure this properly?

Update your security group

1. Keep the web browser open and go back to the **EC2 Management Console** tab.
2. In the left navigation pane, under **Network & Security,** click **Security Groups**.
3. Select the SSH Practice SG or the security group you created when launching your EC2 instance.
4. Expand the **Security Group** info pane at the bottom of the screen and click the **Inbound** tab. Notice the Security Group currently has **no HTTP rules**.

Create a rule

Create a rule in the **Inbound** tab.

1. Click **Edit inbound rules.**
2. Click **Add Rule** and then configure the following settings:

   - **Type**: HTTP
   - **Source**: Anywhere
   - Click **Save rules**

The new **Inbound HTTP** rule will create an entry for both IPV4 IP address (0.0.0.0/0) as well as IPV6 IP address (::/0).

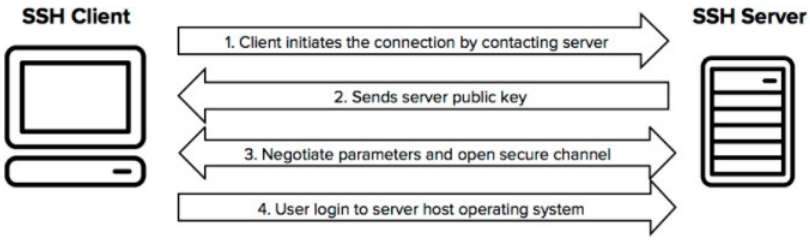
Test your rule

1. Return to the tab you previously opened with the Webserver Public IP address.
2. Refresh the browser page.

You should see the message: **Hey Guru, you have mad Cloud skills!**

DID YOU KNOW

SSH Factoid: The most common tool to connect to Linux servers is Secure Shell (**SSH**). It was created in 1995 and is now installed by default on almost every Linux distribution. When connecting to hosts via SSH, SSH key pairs are often used to individually authorize users. As a result, organizations have to store, share, manage access for, and maintain these SSH keys. Some organizations also maintain bastion hosts, which help limit network access into hosts by the use of a single jump point. They provide logging and prevent rogue SSH access by adding an additional layer of network obfuscation.



The above presents a simplified setup flow of a secure shell connection.

Test your SSH

Now that you have successfully launched an Amazon EC2 with a bootstrap script, configured the security group correctly utilizing both the SSH / HTTP ports, and tested the Port 80 HTTP port, check to make sure you can SSH into the EC2 instance.

1. Navigate to the EC2 Dashboard and click on **Running Instances**.
2. Click and highlight your SSH Practice Server.
3. Write down the IPv4 Public IP address. You will need this address momentarily.

Now let's SSH into the EC2 instance using **PuTTyGen** and **PuTTy**. Refer to the accompanying PuTTy instructions for detailed instructions.

If you don't already have PuTTYGen and PuTTY already installed navigate to:

PuttyGen
https://www.puttygen.com/#Download_PuTTYgen_on_Windows

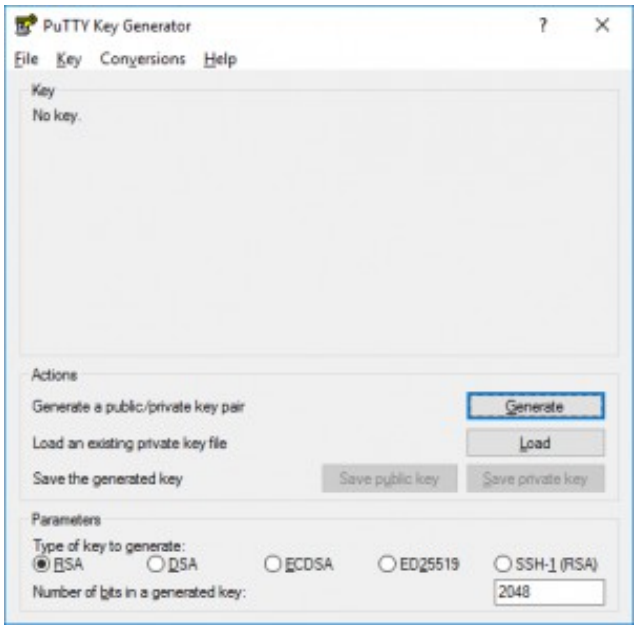
PuTTY
https://www.puttygen.com/download-putty#PuTTY_for_windows

After installation, review the PuTTYGen and PuTTY instructions for this activity:

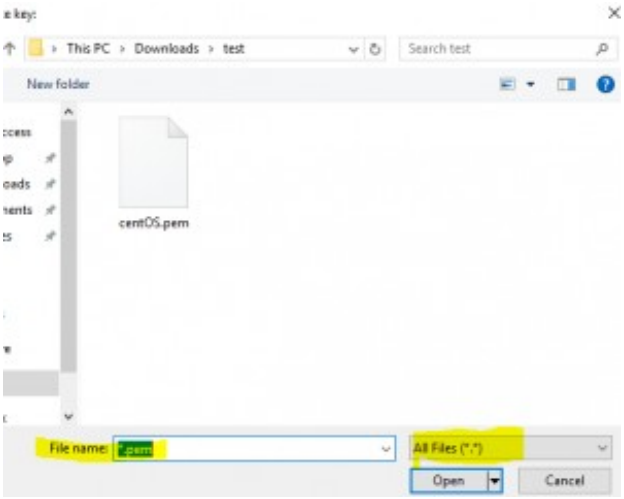
Converting .pem to .ppk on Windows

1. Click on **Start** menu> ***Search*** > **PuTTYgen.**

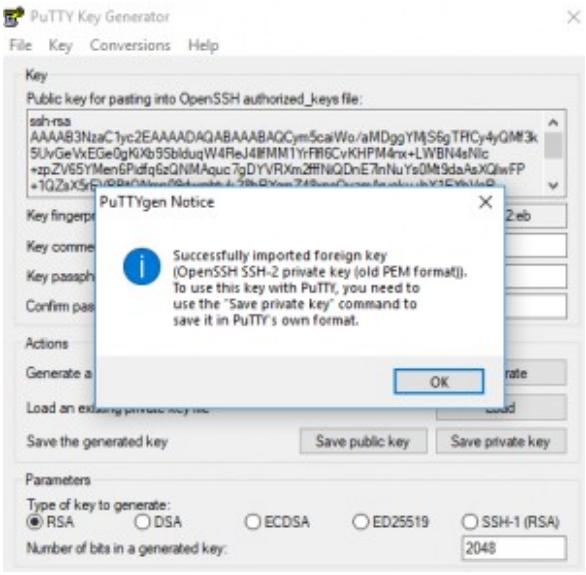
2. The following window will present options on the type of key a user wants to generate. Select the option '**RSA**' (Rivest–Shamir–Adleman). RSA is a public-key cryptosystem that is commonly used to transmit data securely.



3. Next, click on the option '**Load**.'
(As PuTTY supports its native file format, it will only show files that have .ppk file extension. Therefore, users have to choose the '**All Files**' option from the drop-down bar. It will display all key files included the .pem file.)

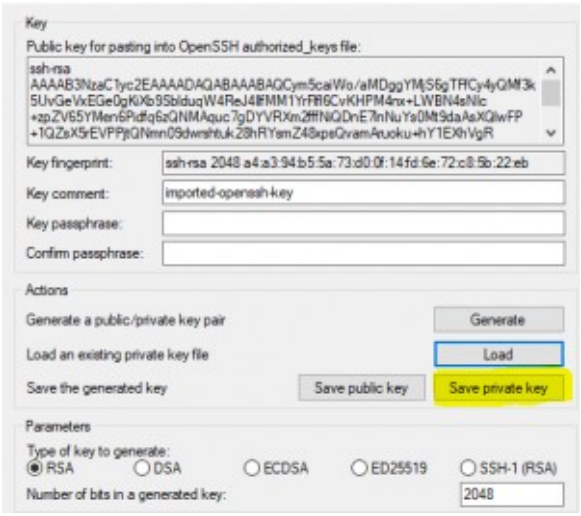


4. Now, select the .pem file that you want to convert *(My_SSH_Key.pem).* That PuTTYgen is used for SSH connectivity, so it is critical for users to select the specific file that they plan to convert and click 'Open.' To confirm, click on 'OK.'



5. In the resultant window, click on 'Save private key,' which will convert and save the key file in PuTTY compatible format.

6. PuTTYgen will prompt a warning of saving the key without a passphrase. Hit **Yes**.



7. Now, give the name to your file and PuTTYgen will automatically add .ppk file extension *(My_SSH_Key).*
8. Close PuTTyGen.

SSH Using PuTTY Instructions

1. Locate and launch PuTTY on your PC like you did with PuTTYGen, then locate the **Host Name (or IP address)** field in the PuTTY Configuration window.
2. In the EC2 management console, highlight your SSH Practice Server and towards the bottom of the screen, locate the IPv4 Public IP address of the EC2 instance within the AWS Console and copy/paste it into **Host Name (or IP address) field**.
3. In the left-hand navigation of PuTTY within the **Category** box, scroll down and locate **SSH**.
4. Expand the SSH option then locate the **Auth** option and highlight.
5. Click on the **Browse** option and locate the .ppk file on your computer that you generated using the PuTTyGen instructions *(My_SSH_Key.ppk).*
6. Select the .ppk file and click **Open.** Then click **Open** again.
7. This will launch a PuTTY SSH window that will allow you to log into the EC2 instance associated with the IP from the EC2 instance within the AWS Console.
8. Click **YES** on the PuTTY Security Alert window that might pop up
9. Log in with **ec2-user.**
10. At the command prompt, type **pwd** and enter.
11. You should see that you're in the **/home/ec2-user directory.**
12. Close your PuTTY login screen and confirm you want to exit the session.

Important info
Passphrases provide extra protection, but it can become cumbersome, as each time a user copies files, they have to enter the passphrase. Thus, it entirely depends on the user if they wish or don't wish to add the extra layer of protection. Once the file is converted to a PuTTY compatible format, users can connect their local machine with remote servers.

Congratulations! You have successfully connected to your SSH Practice Server via the command line.

DID YOU KNOW

Fun Factoid: You've launched your EC2 instance using a script inserted into your **User Data** field in the **Advanced Details** section. You can retrieve and view the user data information from within a running instance using the following URL: *http://169.254.169.254/latest/user-data*. Type *curl http://169.254.169.254/latest/user-data,* after you've used SSH to gain access to your instance. You can retrieve your instances user data.

Cost Effectiveness

Stop Your EC2 Instance

You used a t2.micro Instance but what are some other ways that you can save on cost for the startup? Cloud computing services use a **utility-based pricing** model. Basically, if you leave your light on, there is an associated cost that will show up in your electricity bill. If the development team only works on Mondays through Fridays between the hours of 6 AM and 6 PM, you can minimize cost by turning off the **Windows Practice Server** when you aren't using it.

1. In the **EC2 Management Console**, click **Instances** in the left navigation.
2. Select your running instance and then at the top of the screen click **Actions** > **Instance State** > **Stop**.
3. Your instance will do a normal shutdown and then will stop running.

Resize your instance

1. In the **Actions** menu, select **Instance Settings** > **Change Instance Type**
2. Then configure the following:
    1. **Instance Type:** t2.small
    2. Click **Apply.**

Start the resized instance

1. In the left navigation pain, click **Instances**.
2. In the Actions menu, select **Instance State > Start**.
3. Click **Yes, Start** in the modal.
4. Copy and paste the **new** EC2 Public IP address from the EC2 Details.
5. Open up a browser tab and enter the address.

Can you SSH into your new t2:small instance using the same key pair and SSH commands you used before? Hint: Remember to use the new t2:small IPv4 Public IP address and not the t2micro IP.

Great job!

Let's review

In this activity, as a member of the **BitBeat** infrastructure team, you built a cloud webserver, created a key pair, and gained access to the Amazon EC2 instance using SSH, PuTTYGen, and PuTTY.

In this activity you:

- Launched an Amazon EC2 Instance.
- Created user-data (bootstrapping) instructions for your Amazon EC2 Instance.
- Configured security group settings.
- Created a key pair.
- Connected to your instance via SSH.
- Resized an existing Amazon EC2 instance.
- Demonstrated ways to minimize cost.

DID YOU KNOW

RDP (Remote Desktop Protocol) is a network communication protocol developed by Microsoft, which allows users to remotely connect to another computer. **RDP** is secure, interoperable, and enables network terminals. **RDP** creates secure connections between clients and servers/virtual machines, and virtual desktops are encrypted. **RDP** works across different **Windows** operating systems and devices, and enables strong physical security through remote data storage. The most common tool to connect to Linux servers is Secure Shell (**SSH**), but RDP using port 3389 can be used to access Window servers.

Test your knowledge

- ☐ What is a key pair and what is it used for?

  _____
- ☐ Who stores the public portion of the key pair? _____
- ☐ Who stores the private portion of the key pair? _____
- ☐ What is an Amazon tag? Explain some uses for tags.

  _____
- ☐ What is SSH? What is it used for? _____
- ☐ What is RDP What is it used for?

  _____
- ☐ What is the port number for RDP? _____
- ☐ What is the URL to access EC2 user data information?

  _____

  _____

Bonus activity

In this lab, you have successfully completed many tasks. Let's explore a few more things before you practice good cloud hygiene and clean up your environment. **DO NOT** change any of your configurations or modify your current settings.

1. In the **EC2 Management Console**, click **Instances** in the left navigation and highlight your SSH Practice Server.
2. Click the **Actions** button and review all the options that are available.
3. Under each of the options where there is an additional drop-down options menu, take a moment to review the additional options that are available. Take note how you can do many things under the **Instance Settings** options.

Clean up your environment

The development team has fully deployed and tested their software in a development setting. You are requested to terminate the testing machine you created.

1. Find and select your **SSH Practice Server.**
2. Select Actions>Instance State>Terminate.
3. Delete your SSH Practice SG security group by navigating to the **Security Groups** option in the left-hand navigation within the Network and Security category. Ensure there is a check mark in the box next to your Security Group name – Actions – delete security group.
4. You may also want to delete your My_SSH_Key by navigating to the **Key Pairs** option in the left-hand navigation within the Network and Security category. Ensure there is a checkmark in the box next to your Key Pair Name – click the Actions dropdown box – click Delete – confirm deletion by typing *Delete* in the field – click Delete.

Resources

https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/connecting_to_windows_instance.html
https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-key-pairs.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/instancedata-data-retrieval.html
https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/concepts.html