Lab Information ×

AWS Console Information

Region

us-west-2

Contents

aws training and certification

Lab 2: Building your Amazon VPC Infrastructure

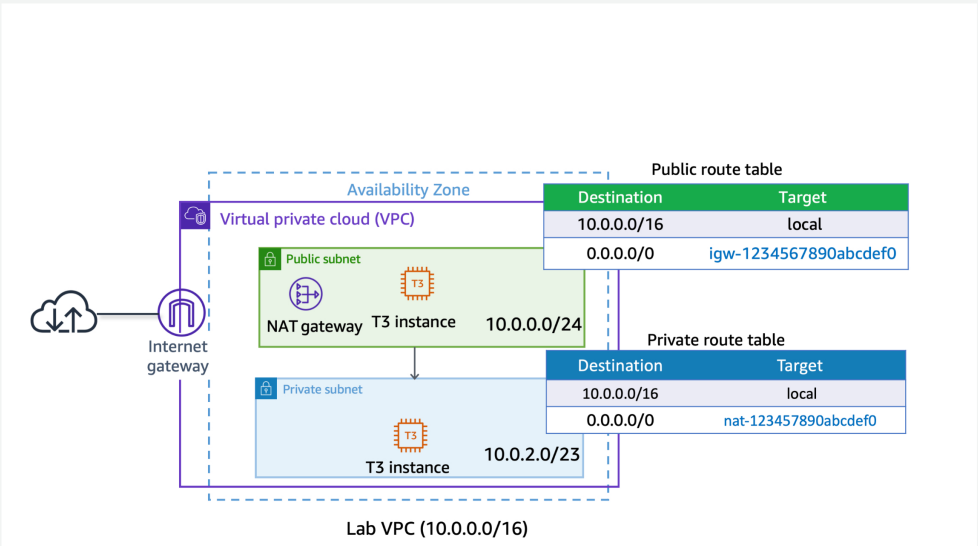
Note: Do not include any personal, identifying, or confidential information into the lab environment. Information entered may be visible to others.

Corrections, feedback, or other questions? Contact us at *AWS Training and Certification* .

Lab overview

As an AWS solutions architect, it is important that you understand the overall functionality and capabilities of Amazon Web Service (AWS) and the relationship between the AWS networking components. In this lab, you create an Amazon Virtual Private Cloud (Amazon VPC), a public and a private subnet in a single Availability Zone, public and private routes, a NAT gateway, and an internet gateway. These services are the foundation of networking architecture inside of AWS. This architecture design covers concepts of infrastructure, design, routing, and security.

The following image shows the final architecture for this lab environment:



OBJECTIVES

After completing this lab, you should know how to do the following:

- Create an Amazon VPC.
- Create public and private subnets.
- Create an internet gateway.
- Configure a route table and associate it to a subnet.
- Create an Amazon Elastic Compute Cloud (Amazon EC2) instance and make the instance publicly accessible.
- Isolate an Amazon EC2 instance in a private subnet.
- Create and assign security groups to Amazon EC2 instances.
- Connect to Amazon EC2 instances using Session Manager, a capability of AWS Systems Manager.

DURATION

This lab requires up to 45 minutes to complete.

ICON KEY

Various icons are used throughout this lab to call attention to different types of instructions and notes. The following list explains the purpose for each icon:

- **Command:** A command that you must run.
- **Expected output:** A sample output that you can use to verify the output of a command or edited file.
- **Note:** A hint, tip, or important guidance.
- **Learn more:** Where to find more information.
- **Security:** An opportunity to incorporate security best practices.
- **Caution:** Information of special interest or importance (not so important to cause problems with the equipment or data if you miss it, but it could result in the need to repeat certain steps).
- **WARNING:** An action that is irreversible and could potentially impact the failure of a command or process (including warnings about configurations that cannot be changed after they are made).

Start lab

1. To launch the lab, at the top of the page, choose Start lab .

You must wait for the provisioned AWS services to be ready before you can continue.

2. To open the lab, choose **Open Console** .

You are automatically signed in to the AWS Management Console in a new web browser tab.

Do not change the Region unless instructed.

COMMON SIGN-IN ERRORS

Error: You must first sign out

If you see the message, **You must first log out before logging into a different AWS account:**

- Choose the **click here** link.
- Close your **Amazon Web Services Sign In** web browser tab and return to your initial lab page.
- Choose **Open Console** again.

Error: Choosing Start Lab has no effect

In some cases, certain pop-up or script blocker web browser extensions might prevent the **Start Lab** button from working as intended. If you experience an issue starting the lab:

- Add the lab domain name to your pop-up or script blocker's allow list or turn it off.
- Refresh the page and try again.

SCENARIO

Your team has been tasked with prototyping an architecture for a new web-based application. To define your architecture, you need to have a better understanding of public and private subnets, routing, and Amazon EC2 instance options.

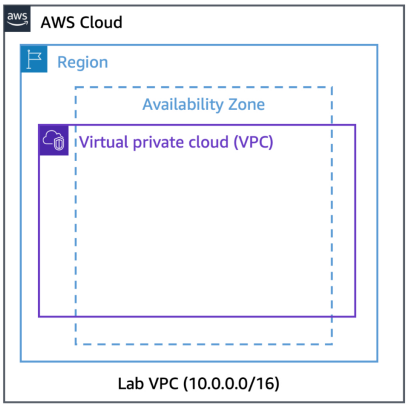
AWS SERVICES NOT USED IN THIS LAB

AWS services not used in this lab are deactivated in the lab environment. In addition, the capabilities of the services used in this lab are limited to only what the lab requires. Expect errors when accessing other services or performing actions beyond those provided in this lab guide.

Task 1: Creating an Amazon VPC in a Region

In this task, you create a new Amazon VPC in the AWS Cloud.

Learn more: With Amazon VPC, you can provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define. You have complete control over your virtual networking environment, including selection of your own IP address ranges, creation of subnets, and configuration of route tables and network gateways. You can also use the enhanced security options in Amazon VPC to provide more granular access to and from the Amazon EC2 instances in your virtual network.



3. At the top of the AWS Management Console, in the search bar, search for and choose VPC .

Caution: Verify that the Region displayed in the top-right corner of the console is the same as the **Region** value on the left side of this lab page.

Note: The VPC management console offers a VPC Wizard, which can automatically create several VPC architectures. However, in this lab you create the VPC components manually.

4. In the left navigation pane, choose **Your VPCs** .

The console displays a list of your currently available VPCs. A default VPC is provided so that you can launch resources as soon as you start using AWS.

5. Choose **Create VPC** and configure the following:

- **Resources to create:** Choose *VPC only*.

- **Name tag - *optional*:** Enter `Lab VPC`
- **IPv4 CIDR:** Enter `10.0.0.0/16`

6. Choose **Create VPC** .

A **You successfully created vpc-xxxxxxxxx / Lab VPC** message is displayed on top of the screen.

The **VPC Details** page is displayed.

7. Verify the state of the **Lab VPC** .

Expected output: It should display the following:

- **State:** Available

The lab VPC has a Classless Inter-Domain Routing (CIDR) range of **10.0.0.0/16** , which includes all IP addresses that start with **10.0.x.x** . This range contains over 65,000 addresses. You later divide the addresses into separate subnets.

8. From the same page, choose **Actions** and choose **Edit VPC settings** .

The **Edit VPC settings** page is displayed.

9. From the **DNS settings** section, select **Enable DNS hostnames** .

This option assigns a friendly Domain Name System (DNS) name to Amazon EC2 instances in the VPC, such as the following:

ec2-52-42-133-255.us-west-2.compute.amazonaws.com

10. Choose **Save** .

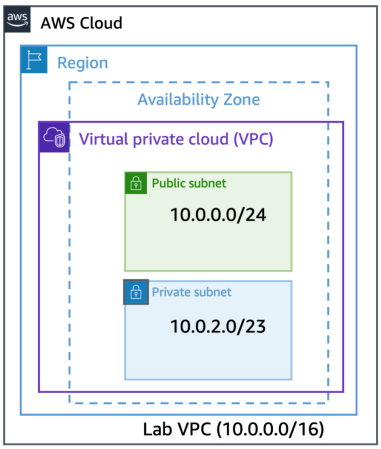
A **You have successfully modified the settings for vpc-xxxxxxxxx / Lab VPC.** message is displayed on top of the screen.

Any Amazon EC2 instances launched into this Amazon VPC now automatically receive a DNS hostname. You can also create a more meaningful DNS name (for example, *app.company.com*) using records in Amazon Route 53.

Congratulations! You have successfully created your own VPC and now you can launch the AWS resources in this defined virtual network.

Task 2: Creating public subnets and private subnets

In this task, you create a public subnet and a private subnet in the lab VPC. To add a new subnet to your VPC, you must specify an IPv4 CIDR block for the subnet from the range of your VPC. You can specify the Availability Zone in which you want the subnet to reside. You can have multiple subnets in the same Availability Zone.



Note: A *subnet* is a sub-range of IP addresses within a network. You can launch AWS resources into a specified subnet. Use a *public subnet* for resources that must be connected to the internet, and use a *private subnet* for resources that are to remain isolated from the internet.

TASK 2.1: CREATING YOUR PUBLIC SUBNET

The public subnet is for internet-facing resources.

11. In the left navigation pane, choose **Subnets** .

12. Choose **Create subnet** and configure the following:

- **VPC ID:** Select **Lab VPC** from the dropdown menu.
- **Subnet name:** Enter `Public Subnet` .
- **Availability Zone:** Select the **first** Availability Zone in the list. (Do **not** choose *No Preference.*)
- **IPv4 CIDR block:** Enter `10.0.0.0/24` .

13. Choose **Create subnet** .

A **You have successfully created 1 subnet: subnet-xxxxxx** message is displayed on top of the screen.

14. Verify the state.

Expected output: It should display the following:

- **State:** Available

Note: The VPC has a CIDR range of **10.0.0.0/16** , which includes all **10.0.x.x** IP addresses. The subnet you just created has a CIDR range of **10.0.0.0/24** , which includes all **10.0.0.x** IP addresses. These ranges might look similar, but the subnet is smaller than the VPC because of the **/24** in the CIDR range.

Now, configure the subnet to automatically assign a public IP address for all instances launched within it.

15. Select **Public Subnet** .

16. Choose **Actions** and choose **Edit subnet settings** .

The **Edit subnet settings** page is displayed.

17. From the **Auto-assign IP settings** section, select **Enable auto-assign public IPv4 address** .

18. Choose **Save** .

A **You have successfully changed subnet settings:** Enable auto-assign public IPv4 address message is displayed on top of the screen.

Note: Even though this subnet is named **Public Subnet** , it is not yet public. A public subnet must have an internet gateway and route to the gateway. You create and attach the internet gateway and route tables in this lab.

TASK 2.2: CREATING YOUR PRIVATE SUBNET

The private subnet is for resources that are to remain isolated from the internet.

19. Choose **Create subnet** , and then configure the following:

- **VPC ID:** Select **Lab VPC** from the dropdown menu.
- **Subnet name:** Enter `Private Subnet` .
- **Availability Zone:** Select the **first** Availability Zone in the list. (Do **not** choose *No Preference*.)
- **IPv4 CIDR block:** Enter `10.0.2.0/23` .

20. Choose **Create subnet** .

A You have successfully created 1 subnet: subnet-xxxxxx message is displayed on top of the screen.

21. Verify the state.

Expected output: It should display the following:

- **State:** Available

Note: The CIDR block of **10.0.2.0/23** includes all IP addresses that start with **10.0.2.x** and **10.0.3.x** . This is twice as large as the public subnet because most resources should be kept private, unless they specifically need to be accessible from the internet.

Your VPC now has two subnets. However, these subnets are isolated and cannot communicate with resources outside the VPC. Next, you configure the public subnet to connect to the internet through an internet gateway.

Congratulations! You have successfully created a public subnet and a private subnet in the lab VPC.

Task 3: Creating an internet gateway

In this task, you create an internet gateway so that internet traffic can access the public subnet. To grant access to or from the internet for instances in a subnet in a VPC, you create an internet gateway and attach it to your VPC. Then you add a route to your subnet's route table that directs internet-bound traffic to the internet gateway.

Learn more: An internet gateway serves two purposes: To provide a target in your VPC route tables for internet-bound traffic, and to perform network address translation (NAT) for instances that have been assigned public IPv4 addresses.

22. In the left navigation pane, choose **Internet gateways** .

23. Choose **Create internet gateway** and configure the following:

- **Name tag:** Enter `Lab IGW` .

24. Choose **Create internet gateway** .

A The following internet gateway was created: igw-xxxxxx - Lab IGW. You can now attach to a VPC to enable the VPC to communicate with the internet. message is displayed on top of the screen.

You can now attach the internet gateway to your Lab VPC.

25. From the same page, choose **Actions** and choose **Attach to VPC** .

26. For **Available VPCs** , select **Lab VPC** from the dropdown menu.

27. Choose **Attach internet gateway** .

A Internet gateway igw-xxxxx successfully attached to vpc-xxxxx message is displayed on top of the screen.

28. Verify the state.

Expected output: It should display the following:

- **State:** Attached

The internet gateway is now attached to your Lab VPC. Even though you have created an internet gateway and attached it to your VPC, you must also configure the route table of the public subnet to use the internet gateway.

Congratulations! You have successfully created an internet gateway so that internet traffic can access the public subnet.

Task 4: Routing internet traffic in the public subnet to the internet gateway

In this task, you create a route table and add a route to the route table to direct internet-bound traffic to your internet gateway and associate your public subnets with your route table. Each subnet in your VPC must be associated with a route table; the table controls the routing for the subnet. A subnet can only be associated with one route table at a time, but you can associate multiple subnets with the same route table.

Learn more: A route table contains a set of rules, called routes, that are used to determine where network traffic is directed. To use an internet gateway, your subnet's route table must contain a route that directs internet-bound traffic to the internet gateway. You can scope the route to all destinations not explicitly known to the route table (0.0.0.0/0 for IPv4 or ::/0 for IPv6), or you can scope the route to a narrower range of IP addresses. If your subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet.

29. In the left navigation pane, choose **Route tables** .

There is currently one default route table associated with the VPC, **Lab VPC** . This routes traffic locally. You now create an additional route table to route public traffic to your internet gateway.

30. Choose **Create route table** , and then configure the following:

- **Name - *optional*:** Enter `Public Route Table` .
- **VPC:** Select **Lab VPC** from the dropdown menu.

31. Choose **Create route table** .

A Route table rtb-xxxxxxx | Public Route Table was created successfully. message is displayed on top of the screen.

32. Choose the **Routes** tab in the lower half of the page.

Note: There is one route in your route table that allows traffic within the 10.0.0.0/16 network to flow within the network, but it does not route traffic outside of the network.

You now add a new route to permit public traffic.

33. Choose **Edit routes** .

34. Choose Add route , and then configure the following:

- **Destination:** Enter `0.0.0.0/0` .
- **Target:** Choose **Internet Gateway** in the dropdown menu, and then choose the displayed internet gateway ID.

35. Choose **Save changes** .

A **Updated routes for rtb-xxxxxxx / Public Route Table successfully** message is displayed on top of the screen.

36. Choose the **Subnet associations** tab.

37. Choose Edit subnet associations .

38. Select **Public Subnet**

39. Choose **Save associations** .

A **You have successfully updated subnet associations for rtb-xxxxxxx / Public Route Table.** message is displayed on top of the screen.

Note: The subnet is now *public* because it has a route to the internet through the internet gateway.

Congratulations! You have successfully configured the route table.

Task 5: Creating a public security group

In this task, you create a security group so that users can access your Amazon EC2 instance. Security groups in a VPC specify which traffic is allowed to or from an Amazon EC2 instance.

Learn more: You can use Amazon EC2 security groups to help secure instances within an Amazon VPC. By using security groups in a VPC, you can specify both inbound and outbound network traffic that is allowed to or from each Amazon EC2 instance. Traffic that is not explicitly allowed to or from an instance is automatically denied.

Security: It is recommended to use *HTTPS* protocol to improve web traffic security. However, to simplify this lab, only *HTTP* protocol is used.

40. In the left navigation pane, choose **Security groups** .

41. Choose **Create security group** , and then configure the following:

- **Security group name:** Enter `Public SG` .
- **Description:** Enter `Allows incoming traffic to public instance` .
- **VPC:** Select the **X** to clear the text box and then select **Lab VPC** from the dropdown menu.

42. In the **Inbound rules** section, choose Add rule and configure the following:

- **Type:** Select **HTTP** from the dropdown menu.
- **Source:** Select **Anywhere-IPv4** from the dropdown menu.

43. In the **Tags -** *optional* section, choose Add new tag and configure the following:

- **Key:** Enter `Name` .
- **Value:** Enter `Public SG` .

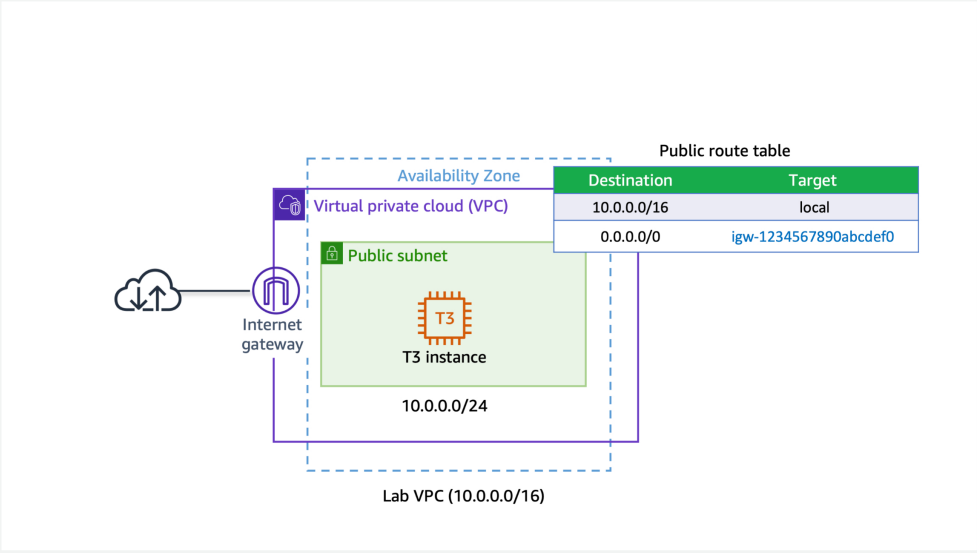
44. Choose **Create security group** .

A **Security group (sg-xxxxxxx | Public SG) was created successfully** message is displayed on top of the screen.

Congratulations! You have successfully created a security group that allows HTTP traffic. You need this in the next task when you launch an Amazon EC2 instance in the public subnet.

Task 6: Launching an Amazon EC2 instance into a public subnet

In this task, you launch an Amazon EC2 instance into a public subnet. To activate communication over the internet for IPv4, your instance must have a public IPv4 address that's associated with a private IPv4 address on your instance. By default, your instance is only aware of the private (internal) IP address space defined within the VPC and subnet.



Learn more: The internet gateway that you created logically provides the one-to-one NAT on behalf of your instance. So when traffic leaves your VPC subnet and goes to the internet, the reply address field is set to the public IPv4 address or Elastic IP address of your instance, and not its private IP address.

45. At the top of the AWS Management Console, in the search bar, search for and choose `EC2` .

The **Amazon EC2 Management Console** is displayed.

TASK 6.1: BEGINNING THE INSTANCE CONFIGURATION

46. From the console navigation menu on the left, choose **EC2 Dashboard** .

47. From the **Launch instances** section, choose the **Launch instances** dropdown menu.

The **Launch an instance** page is displayed.

TASK 6.2: ADDING TAGS TO THE INSTANCE

You can use tags to categorize your AWS resources in different ways, such as by purpose, owner, or environment. You can apply tags to most AWS Cloud resources. Each tag consists of a *key* and a *value*, both of which you define. One use of tags is for when you must manage many resources of the same type. You can quickly search for and identify a specific resource by the tag you have applied to it.

In this task, you add a tag to the Amazon EC2 instance.

48. Locate the **Name and tags** section.

49. In the **Name** field, enter `Public Instance` .

Note: No additional instance tags are required for this lab.

TASK 6.3: SELECTING AN AMI

In this task, you choose an Amazon Machine Image (AMI). The AMI contains a copy of the disk volume used to launch the instance.

50. Locate the **Application and OS Images (Amazon Machine Image)** section.

51. Ensure that **Amazon Linux** is selected as the OS.

52. Ensure that **Amazon Linux 2023 AMI** is selected in the dropdown menu.

TASK 6.4: CHOOSING THE AMAZON EC2 INSTANCE TYPE

Each instance type allocates a specific combination of virtual CPUs (vCPUs), memory, disk storage, and network performance.

For this lab, use a **t3.micro** instance type. This instance type has 2 vCPUs and 1 GiB of memory.

53. Locate the **Instance type** section.

54. From the **Instance type** dropdown menu, choose **t3.micro** .

TASK 6.5: CONFIGURING KEY PAIR FOR LOGIN

55. Locate the **Key pair (login)** section.

56. From the **Key pair name -** *required* dropdown menu, choose `Proceed without a key pair (Not recommended)` .

TASK 6.6: CONFIGURING INSTANCE NETWORKING

57. Locate the **Network settings** section.

58. Choose `Edit` .

59. Configure the following settings from the dropdown menus:

- **VPC -** *required:* Select **Lab VPC** .
- **Subnet:** Select **Public Subnet** .
- **Auto-assign public IP:** Select **Enable** .

TASK 6.7: CONFIGURING INSTANCE SECURITY GROUPS

You can use security groups to define both the allowed/denied and the inbound/outbound traffic for the elastic network interface. The network interface is attached to an Amazon EC2 instance. Port 80 is the default port for HTTP traffic, and it is necessary for the web server you launch in this lab to work correctly.

60. For **Firewall (security groups)** , choose `Select existing security group` .

61. From the **Common security groups** dropdown menu, choose the security group that has a name like **Public SG** .

TASK 6.8: ADDING STORAGE

You can use the **Configure storage** section to modify ephemeral instance storage and add additional Amazon Elastic Block Store (Amazon EBS) disk volumes attached to the instance. The EBS volumes can be configured in both their size and performance.

In this lab, the default storage settings are all that is needed. No changes are required.

TASK 6.9: CONFIGURING USER DATA

62. Locate and expand the **Advanced details** section.

63. From the **IAM instance profile** dropdown menu, select the role that has a name like **EC2InstProfile** .

Note: To install and configure the new instance as a web server, you provide a user data script that automatically runs when the instance launches.

64. In the **User data -** *optional* section, copy and paste the following:

```
#!/bin/bash
# To connect to your EC2 instance and install the Apache web server with PHP
yum update -y
yum install -y httpd php8.1
systemctl enable httpd.service
systemctl start httpd
cd /var/www/html
wget  https://us-west-2-tcprod.s3.amazonaws.com/courses/ILT-TF-200-ARCHIT/v7.6.1.prod-8310d0c0/lab-2-VPC/scripts/instanceData.zip
unzip instanceData.zip
```

The remaining settings on the page can be left at their default values.

TASK 6.10: REVIEWING THE INSTANCE LAUNCH

Take a moment to review that the configuration for the Amazon EC2 instance you are about to launch is correct.

65. Locate the **Summary** section.

66. Choose **Launch instance** .

The **Launch an instance** page is displayed.

Your Amazon EC2 instance is now launched and configured as you specified.

67. Choose **View all instances** .

The **Amazon EC2 console** is displayed.

68. Occasionally choose the console refresh button and wait for **Public Instance** to display the **Instance state** as Running and wait for Status check to pass 2/2 checks passed .

Note: The Amazon EC2 instance named Public Instance is initially in a *Pending* state. The instance state then changes to Running indicating that the instance has finished booting.

Congratulations! You have successfully launched an Amazon EC2 instance into a public subnet.

Task 7: Connecting to a public instance through HTTP

In this task, you connect to the public instance and launch the basic Apache web server page. The inbound rules added earlier that allow HTTP access (port 80) allow you to connect to the web server running Apache.

69. In the left navigation pane, choose **Instances** .

70. Select **Public Instance** .

71. Choose the **Networking** tab in the lower pane.

Note: If you need to make any section of the console larger, you can resize the horizontal edges of the containers displayed on the console.

72. Locate the **Public IPv4 DNS** value.

73. Copy the public DNS value. Do not choose the open address option, because HTTPS is not set up for this lab environment.

74. Open a new browser tab and paste the public DNS value for *Public Instance* in the URL address bar.

The web page hosted on the Amazon EC2 instance is displayed. The page displays the instance ID and the AWS Availability Zone where the Amazon EC2 instance is located.

75. Close the browser tab and return to the console.

Congratulations! You have successfully launched an Apache web server in the public subnet and tested the HTTP connection. You can safely close the tab and return to the console.

Task 8: Connecting to the Amazon EC2 instance in the public subnet through Session Manager

In this task, you connect to your Amazon EC2 instance in the public subnet using Session Manager.

Learn more: Session Manager is a fully managed AWS Systems Manager capability that you use to manage your Amazon EC2 instances through an interactive one-click browser-based shell or through the AWS Command Line Interface (AWS CLI). You can use Session Manager to start a session with an Amazon EC2 instance in your account. After starting the session, you can run bash commands as you would through any other connection type.

76. At the top of the AWS Management Console, in the search bar, search for and choose EC2 .

77. In the left navigation pane, choose **Instances** .

78. Select **Public Instance** and choose Connect .

The **Connect to instance** page is displayed.

79. Choose the **Session Manager** tab.

Learn more: With Session Manager, you can connect to Amazon EC2 instances without needing to expose the SSH port on your firewall or Amazon VPC security group. For more information, see AWS Systems Manager Session Manager .

80. Choose **Connect** .

A new browser tab or window opens with a connection to the **Public Instance** .

Note: The Session Manager service is not updated in real time. If you experience errors with Session Manager connecting to an Amazon EC2 instance you just launched, ensure that you have given the instance a few minutes to launch, pass health checks, and communicate with the Session Manager service before trying to open a session connection again.

81. **Command:** Enter the following command to change to the home directory (/home/ssm-user/) and test web connectivity using the cURL command:

```
cd ~
curl -I https://aws.amazon.com/training/
```

Expected output:

```
HTTP/2 200
content-type: text/html;charset=UTF-8
server: Server
date: Wed, 19 Apr 2023 14:43:47 GMT
x-amz-rid: 6HVPS1JY1XW2S1K34Q3Z
set-cookie: aws-priv=eyJ2IjoxLCJldSI6MCwic3QiOjB9; Version=1; Comment="Anonymous cookie for privacy regulations"; Domain=.aws.amazon.com; Max-Age=31536000; Expires=Thu,
set-cookie: aws_lang=en; Domain=.amazon.com; Path=/
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
strict-transport-security: max-age=63072000
x-content-type-options: nosniff
x-amz-id-1: 6HVPS1JY1XW2S1K34Q3Z
last-modified: Thu, 30 Mar 2023 15:58:02 GMT
content-security-policy-report-only: default-src *; connect-src *; font-src * data:; frame-src *; img-src * data:; media-src *; object-src *; script-src *; style-src 'u
vary: accept-encoding,Content-Type,Accept-Encoding,User-Agent
x-cache: Miss from cloudfront
via: 1.1 88c333921d5c405e037b84bb8c2dc33e.cloudfront.net (CloudFront)
x-amz-cf-pop: GRU3-P1
x-amz-cf-id: 89R1wtM9vYV0kIQXrEVkcoNzg_C3UfQJIEVkC5BA3xiIH3FD0nVnYw==
```

Congratulations! You have successfully connected to your public instance using Session Manager. You can safely close the tab and return to the console.

Task 9: Creating a NAT gateway and configuring routing in the private subnet

In this task, you create a NAT gateway and then create a route table to route non-local traffic to the NAT gateway. You then attach the route table to the private subnet. You can use a NAT gateway to allow instances in a private subnet to connect to the internet or other AWS services, but prevent the internet from initiating a connection with those instances.

Note: To create a NAT gateway, you must specify the public subnet in which the NAT gateway should reside. You must also specify an Elastic IP address to associate with the NAT gateway when you create it. You cannot change the Elastic IP address after you associate it with the NAT gateway. After you've created a NAT gateway, you must update the route table associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This allows instances in your private subnets to communicate with the internet.

82. Return to the AWS Management Console browser tab.

83. At the top of the AWS Management Console, in the search box, search for and choose VPC .

84. In the left navigation pane, choose **NAT gateways** .

85. Choose **Create NAT gateway** and configure the following:

- **Name - *optional*:** Enter Lab NGW .
- **Subnet:** Select **Public Subnet** from the dropdown menu.
- For **Elastic IP allocation ID** , choose **Allocate Elastic IP** .

86. Choose **Create NAT gateway** .

A NAT gateway nat-xxxxxxx | Lab NGW was created successfully. message is displayed on top of the screen.

In the next step, you create a new route table for a private subnet that redirects non-local traffic to the NAT gateway.

87. In the left navigation pane, choose **Route tables** .

88. Choose **Create route table** and configure the following:

- **Name - *optional*:** Enter Private Route Table .
- **VPC:** Select **Lab VPC** from the dropdown menu.

89. Choose **Create route table** .

A Route table rtb-xxxxxxx | Private Route Table was created successfully. message is displayed on top of the screen.

The private route table is created and the details page for the private route table is displayed.

90. Choose the **Routes** tab.

There is currently one route that directs all traffic *locally*.

You now add a route to send internet-bound traffic through the NAT gateway.

91. Choose **Edit routes** .

92. Choose **Add route** and then configure the following:

- **Destination:** Enter 0.0.0.0/0 .
- **Target:** Choose **NAT Gateway** in the dropdown menu, and then choose the displayed NAT Gateway ID.

93. Choose **Save changes** .

A **Updated routes for rtb-xxxxxxx / Private Route Table successfully** message is displayed on top of the screen.

94. Choose the **Subnet associations** tab.

95. Choose **Edit subnet associations** .

96. Select **Private Subnet** .

97. Choose **Save associations** .

A You have successfully updated subnet associations for rtb-xxxxxxx / Private Route Table. message is displayed on top of the screen.

This route sends internet-bound traffic from the private subnet to the NAT gateway that is in the same Availability Zone.

Congratulations! You have successfully created the NAT gateway and configured the private route table.

Task 10: Creating a security group for private resources

In this task, you create a security group that allows incoming HTTPS traffic from resources assigned to the public security group.

Learn more: When you specify a security group as the source for a rule, traffic is allowed from the network interfaces that are associated with the source security group for the specified port and protocol. Incoming traffic is allowed based on the private IP addresses of the network interfaces that are associated with the source security group (and not the public IP or Elastic IP addresses). Adding a security group as a source does not add rules from the source security group.

98. In the left navigation pane, choose **Security groups** .

99. Choose **Create security group** , and then configure the following:

- **Security group name:** Enter Private SG .
- **Description:** Enter Allows incoming traffic to private instance using public security group .
- **VPC:** Select the **X** to clear the text box, and then choose **Lab VPC** from the dropdown menu.

100. In the **Inbound rules** section, choose **Add rule** and configure the following:

- **Type:** Select *HTTP*.
- **Source:** Select *Custom*.
  - In the box to the right of Custom, type sg .
  - Choose **Public SG** from the list.

101. In the **Tags - *optional*** section, choose **Add new tag** and configure the following:

- **Key:** Enter Name .
- **Value:** Enter Private SG .

102. Choose **Create security group** .

A **Security group (sg-xxxxxxx | Private SG) was created successfully** message is displayed on top of the screen.

Congratulations! You have successfully created the private security group.

Task 11: Launching an Amazon EC2 instance into a private subnet

In this task, you launch an Amazon EC2 instance into a private subnet.

Learn more: Private instances can route their traffic through a NAT gateway or a NAT instance to access the internet. Private instances use the public IP address of the NAT gateway or NAT instance to traverse the internet. The NAT gateway or NAT instance allows outbound communication but doesn't allow machines on the internet to initiate a connection to the privately addressed instances.

103. At the top of the AWS Management Console, in the search bar, search for and choose EC2 .

The **Amazon EC2 console** is displayed.

TASK 11.1: BEGINNING THE INSTANCE CONFIGURATION

104. Choose **EC2 Dashboard** from the console navigation menu on the left.

105. Choose the **Launch instance** dropdown menu from the **Launch instance** section.

106. Select **Launch instance** from the list.

The **Launch an instance** page is displayed. In this task, you add a tag to the Amazon EC2 instance.

107. Locate the **Name and tags** section.

108. Enter `Private Instance` in the **Name** field.

Note: No additional instance tags are required for this lab.

TASK 11.3: SELECTING AN AMI

In this task, you choose an AMI. The AMI contains a copy of the disk volume used to launch the instance.

109. Locate the **Application and OS Images (Amazon Machine Image)** section.

110. Ensure that **Amazon Linux** is selected as the OS.

111. Ensure that **Amazon Linux 2023 AMI** is selected in the dropdown menu.

TASK 11.4: CHOOSING THE AMAZON EC2 INSTANCE TYPE

Each instance type allocates a specific combination of vCPUs, memory, disk storage, and network performance.

For this lab, use a **t3.micro** instance type. This instance type has 2 vCPUs and 1 GiB of memory.

112. Locate the **Instance type** section.

113. Choose **t3.micro** from the **Instance type** dropdown menu.

TASK 11.5: CONFIGURING KEY PAIR FOR LOGIN

114. Locate the **Key pair (login)** section.

115. Choose **Proceed without a key pair (Not recommended)** from the **Key pair name - *required*** dropdown menu.

TASK 11.6: CONFIGURING INSTANCE NETWORKING

116. Locate the **Network settings** section.

117. Choose **Edit** and configure the following settings from the dropdown menus:

- **VPC - *required:*** Select **Lab VPC** .
- **Subnet:** Select **Private Subnet** .
- **Auto-assign public IP:** Select **Disable** .

TASK 11.7: CONFIGURING INSTANCE SECURITY GROUPS

118. For **Firewall (security groups)** , choose **Select existing security group**

119. Choose the security group that has a name like **Private SG** from the **Common security groups** dropdown menu.

TASK 11.8: ADDING STORAGE

You use the **Configure storage** section to modify ephemeral instance storage and to add additional Amazon EBS disk volumes attached to the instance. You can configure the EBS volumes in size and performance.

In this lab, the default storage settings are all that is needed. No changes are required.

TASK 11.9: CONFIGURING IAM INSTANCE PROFILE

120. Locate and expand the **Advanced details** section.

121. Choose the **EC2InstProfile** role from the **IAM instance profile** dropdown menu.

The remaining settings on the page can be left at their default values.

TASK 11.10: REVIEWING THE INSTANCE LAUNCH

Take a moment to review that the configuration for the Amazon EC2 instance you are about to launch is correct.

122. Locate the **Summary** section.

123. Choose **Launch instance** .

The **Launch an instance** page is displayed.

Your Amazon EC2 instance is now launched and configured as you specified.

124. Choose **View all instances** .

The **Amazon EC2 console** is displayed.

The Amazon EC2 instance name Private Instance is initially in a *Pending* state. The state then changes to *Running*, indicating that the instance has finished booting.

125. Occasionally choose the console refresh button and wait for the **Instance state** to change to Running .

Congratulations! You have successfully launched an Amazon EC2 instance into a private subnet.

Task 12: Connecting to the Amazon EC2 instance in the private subnet

In this task, you connect to the Amazon EC2 instance in the private subnet using Session Manager.

126. In the left navigation pane, choose **Instances** .

127. Select **Private Instance** and choose **Connect**

127. Select **Private Instance** and choose Connect.

The **Connect to instance** page is displayed.

128. Choose the **Session Manager** tab.

129. Choose **Connect**.

A new browser tab or window opens with a connection to the **Private Instance**.

Note: The Session Manager service is not updated in real time. If you experience errors with Session Manager connecting to an Amazon EC2 instance you just launched, ensure that you have given the instance a few minutes to launch, pass health checks, and communicate with the Session Manager service before trying to open a session connection again.

130. **Command:** Enter the following command to change to the home directory (/home/ssm-user/) and test web connectivity using the cURL command:

```
cd ~
curl -I https://aws.amazon.com/training/
```

Expected output:

```
HTTP/2 200
content-type: text/html;charset=UTF-8
server: Server
date: Wed, 19 Apr 2023 14:59:09 GMT
x-amz-rid: AZPXJ57K93ERATZV588Z
set-cookie: aws-priv=eyJ2IjoxLCJldSI6MCwic3QiOjB9; Version=1; Comment="Anonymous cookie for privacy regulations"; Domain=.aws.amazon.com; Max-Age=31536000; Expires=Thu,
set-cookie: aws_lang=en; Domain=.amazon.com; Path=/
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
strict-transport-security: max-age=63072000
x-content-type-options: nosniff
x-amz-id-1: AZPXJ57K93ERATZV588Z
last-modified: Thu, 30 Mar 2023 15:58:02 GMT
content-security-policy-report-only: default-src *; connect-src *; font-src * data:; frame-src *; img-src * data:; media-src *; object-src *; script-src *; style-src 'u
vary: accept-encoding,Content-Type,Accept-Encoding,User-Agent
x-cache: Miss from cloudfront
via: 1.1 fb6a4eca9caced7b791557c24b8c6606.cloudfront.net (CloudFront)
x-amz-cf-pop: GRU3-P1
x-amz-cf-id: Tjphb1UhSXmtyHvybuq4QIFwzTurEI0g_saLB2nLjlYRiBbHbqn85Q==
```

131. Close the Session Manager tab and return to the console.

Congratulations! You have successfully connected to a private instance using Session Manager.

(Optional) Task 1: Testing connectivity to the private instance from the public instance

In this optional task, you use the Internet Control Message Protocol (ICMP) to validate a private instance's network reachability from the public instance.

Note: This task is **optional** and is provided in case you have lab time remaining. You can complete this task or skip to the end of the lab.

132. Return to the AWS Management Console browser tab.

133. In the left navigation pane, choose **Instances**.

134. Select **Private Instance**.

135. On the **Details** tab, copy the value of **Private IPv4 addresses** to your clipboard.

Note: To copy the private IPv4 address, hover over it and choose the copy icon.

136. Unselect **Private Instance**.

137. Select **Public Instance**.

138. Choose Connect.

The **Connect to instance** page is displayed.

139. Choose the **Session Manager** tab.

140. Choose **Connect**.

A new browser tab or window opens with a connection to the **Public Instance**.

141. **Command:** Copy the following command to your notepad. Replace **PRIVATE_IP** with the value of the **Private IPv4 address**:

```
ping PRIVATE_IP
```

142. **Command:** Copy and paste the updated command in your terminal and press **Enter**.

This is a sample command only. Do not use the following command.

```
ping 10.0.2.131
```

143. After a few seconds, stop the ICMP ping request by pressing CTRL+C.

The ping request to the private instance fails. Your challenge is to use the console and figure out the correct *inbound rule* required in the **Private SG** to be able to successfully ping the private instance.

If you have trouble completing the optional task, refer to the Optional Task Solution section at the end of the lab.

(Optional) Task 2: Retrieving instance metadata

In this optional task, you run instance metadata commands on AWS CLI using a tool such as cURL. Instance metadata is available from your running Amazon EC2 instance. This can be helpful when you write scripts to run from your Amazon EC2 instance.

Note: This task is **optional** and is provided in case you have lab time remaining. You can complete this task or skip to the end of the lab.

144. Return to the browser tab with the AWS Management Console open.

145. In the left navigation pane, choose **Instances** .

146. Select **Public Instance** .

147. Choose **Connect** .

The **Connect to instance** page is displayed.

148. Choose the **Session Manager** tab.

149. Choose **Connect** .

A new browser tab or window opens with a connection to the **Public Instance** .

150. **Command:** To view all categories of instance metadata from within a running instance, run the following command:

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" -H "X-aws-ec2-metadata-token-ttl-seconds: 21600"` \
&& curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/
```

151. **Command:** Run the following command to retrieve the public-hostname (one of the top-level metadata items that were obtained in the preceding command):

```
curl -H "X-aws-ec2-metadata-token: $TOKEN" -v http://169.254.169.254/latest/meta-data/public-hostname
```

Note: The IP address 169.254.169.254 is a link-local address and is valid only from the instance.

You have successfully learned how to retrieve instance metadata from your running Amazon EC2 instance.

Conclusion

Creating a VPC with both public and private subnets provides you the flexibility to launch tasks and services in either a public or private subnet. Tasks and services in the private subnets can access the internet through a NAT gateway.

Congratulations! You now have successfully:

- Created an Amazon VPC.
- Created public and private subnets.
- Created an internet gateway.
- Configured a route table and associated it to a subnet.
- Created an Amazon EC2 instance and made the instance publicly accessible.
- Isolated an Amazon EC2 instance in a private subnet.
- Created and assigned security groups to Amazon EC2 instances.
- Connected to Amazon EC2 instances using Session Manager.

End lab

Follow these steps to close the console and end your lab.

152. Return to the **AWS Management Console** .

153. At the upper-right corner of the page, choose **AWSLabsUser** , and then choose **Sign out** .

154. Choose **End lab** and then confirm that you want to end your lab.

Additional resources

- What is Amazon VPC?
- Subnets for Your VPC
- Connect to the internet using an internet gateway
- Configure route tables
- Control traffic to resources using security groups
- NAT gateways
- Public IPv4 addresses
- Understanding the basics of IPv6 networking on AWS

Optional task solution

155. Return to the AWS Management Console browser tab.

156. At the top of the AWS Management Console, in the search box, search for and choose `EC2` .

157. In the left navigation pane, choose **Security Groups** .

158. Select **Private SG** .

159. Choose **Actions** and then choose **Edit inbound rules** .

160. On the **Edit inbound rules** page, in the **Inbound rules** , choose **Add rule** and configure the following:

- **Type:** Select *Custom ICMP - IPV4*.
- **Source:** Select *Custom*.
  - In the box to the right of **Custom** , type `sg` .
  - Choose **Public SG** from the list.

161. Choose **Save rules** .

162. Select the Optional Task link to go to the **Optional Task** and re-run the steps. The *Public Instance* should now be able to successfully ping *Private Instance*.

For more information about AWS Training and Certification, see *https://aws.amazon.com/training/* .

Your feedback is welcome and appreciated.
If you would like to share any feedback, suggestions, or corrections, please provide the details in our *AWS Training and Certification Contact Form* .