

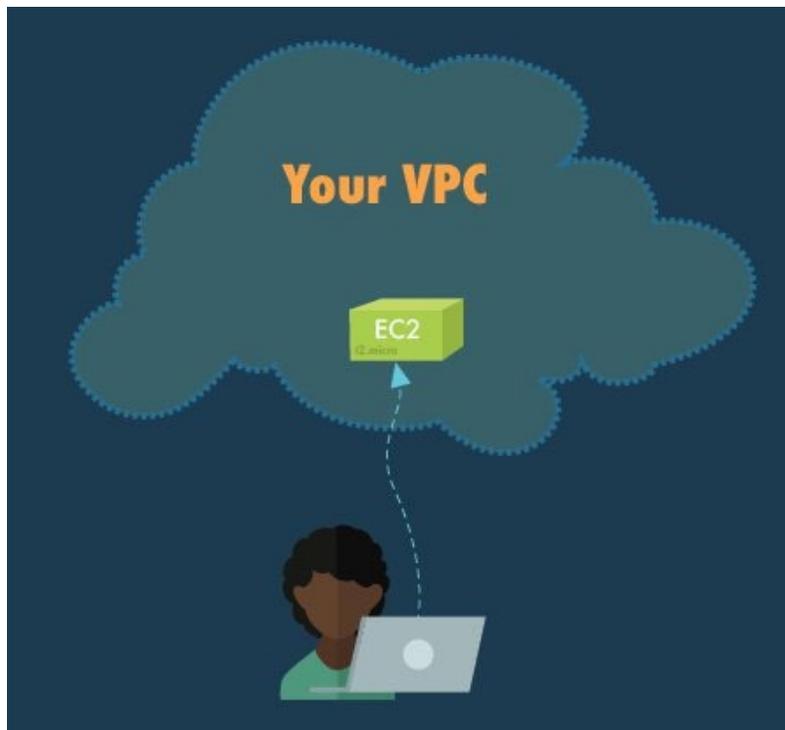
Tutorial 2: Creating a VPC and Active Directory for Your Studio

Estimated Time to Complete: 1 hour

Review of: [Tutorial 1: Getting Started with AWS Virtual Workstations](#)

In our first tutorial, we introduced you to the AWS Console. We also talked about EC2 instances and led you through an exercise where you started, connected to, and then terminated your own EC2 Windows instance.

Hopefully you found that using a virtual workstation is much like using hardware that is physically at your desk, except it could be miles away in a data center...a data center that you don't have to maintain or manage...so that you can concentrate on creating content and not on installing or upgrading hardware.



Overview of this Tutorial

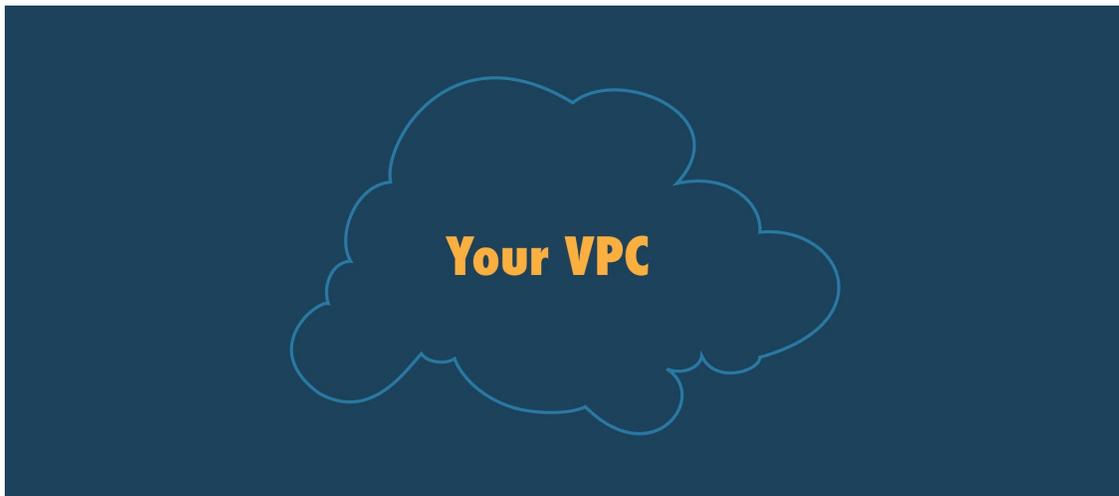
This tutorial will cover creating the basic infrastructure for your Studio in the Cloud. We'll set up

your own network, connect it to the internet and configure some options to handle security and user accounts. At the end of the tutorial, you'll launch an instance in your studio and login using your studio's administrator account.

Creating Your Own VPC

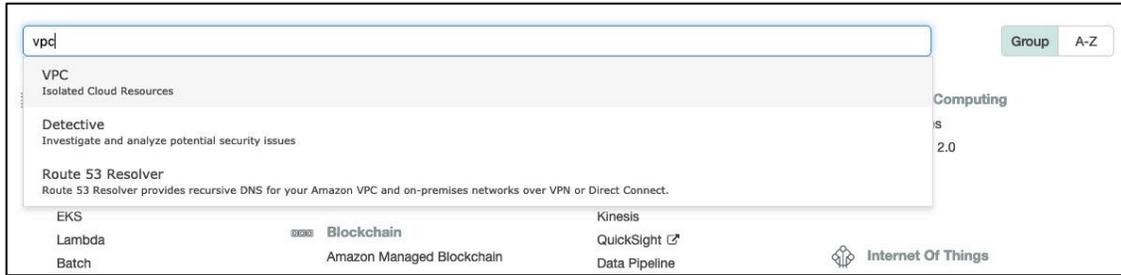
The Virtual Private Cloud (VPC) will be the backbone of your cloud-based studio. It's a virtual network that is dedicated to your AWS account. It is isolated from other virtual networks on AWS. You can think of your VPC as the container in which your Studio in the Cloud resides, including workstations for all your users, shared file storage and your render farm. It enables your users to share resources while also keeping your data secure.

Each AWS account already has a default VPC that has been created in each region that AWS serves. In the starter exercise from our first tutorial, you launched an EC2 instance in the default VPC for your region. But for your Studio in the Cloud, we'll need to customize things a bit. We'll begin with creating a VPC of your own.



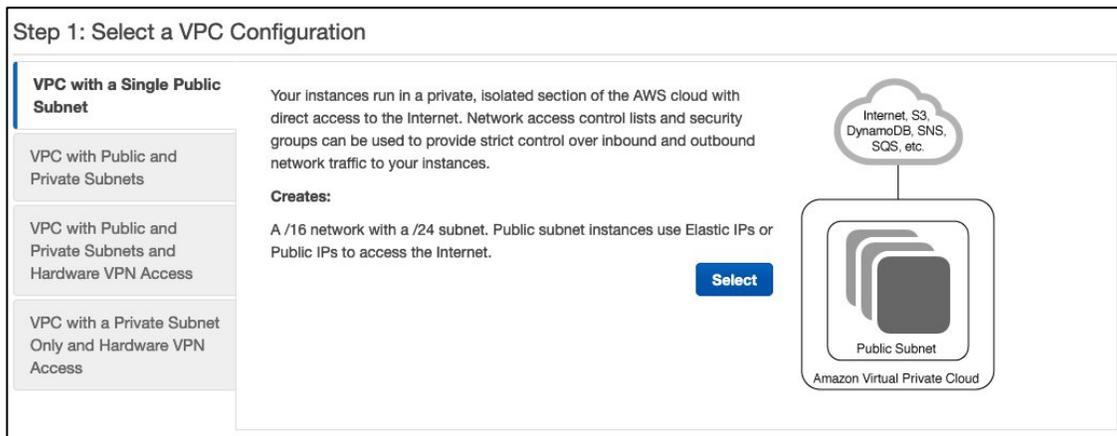
Launch the VPC

- Log in to the AWS Console using your AWS account information, if you haven't already.
- Check that your Region is set correctly. You may have already set your Region as part of the starter exercise in the last tutorial. For a refresher on how to set your Region, please go to the Set Your Region section of Tutorial 1.
- Once you've set your Region, go to the **Services** dropdown menu and in the **Networking & Content Delivery** section choose **VPC** (or search for VPC in the search bar at the top of the page).



- Click **Launch VPC Wizard**.
- Choose **VPC with a Single Public Subnet**. A subnet represents a portion of the addresses in your network. Having more than one subnet allows you to divide your network into different sections based on usage and for security. By default, the launch wizard creates a subnet with IP addresses from 10.0.0.0 to 10.0.0.255. We'll be creating a second subnet for your VPC in the next section.

⚠ Note: We are using a public subnet here for initial setup and testing purposes. After completing the tutorials, we recommend using a private subnet before using your setup for production content requiring a higher level of security. We will publish an add-on tutorial in the future on how to add extra layers of security to your Studio in the Cloud.



- Click **Select**.
- Fill out the next page, **Step 2: VPC with a Single Public Subnet** (unless otherwise stated, leave as default values).
 - **VPC name:** Give your VPC a descriptive name. If you want to pick a name for your studio, you can use it to name your VPC (e.g., My-Studio-VPC). If you'd like to use our example name of "My-Studio", that's fine too. *Either way, be sure to write down your studio name and VPC name in the [Important Information Cheat Sheet](#) so you can refer to them later.*
 - **Availability Zone:** Choose the 'a' Availability Zone for your Region (e.g., us-west-2a).

- Note: If the Availability Zones you have access to don't include 'a', just set it to one of the other zones.
- **Subnet name:** Set this to **Public Subnet A** (you'll add another public subnet next).

Step 2: VPC with a Single Public Subnet

IPv4 CIDR block: 10.0.0.0/16 (65531 IP addresses available)

IPv6 CIDR block: No IPv6 CIDR Block
 Amazon provided IPv6 CIDR block

VPC name: My-Studio-VPC

Public subnet's IPv4 CIDR: 10.0.0.0/24 (251 IP addresses available)

Availability Zone: us-west-1a

Subnet name: Public Subnet A
You can add more subnets after AWS creates the VPC.

Service endpoints
Add Endpoint

Enable DNS hostnames: Yes No

Hardware tenancy: Default

Cancel and Exit Back Create VPC

- Click **Create VPC**.



A Note on Naming

Throughout the tutorials, you'll need to name various components of your studio, such as the VPC above. A good rule of thumb is to avoid any spaces or special characters, except for hyphens (-). While some components have more relaxed naming restrictions, some, like directory DNS names, are more restrictive. For that reason, we recommend erring on the side of caution. Each time you need to choose a name for something, we'll provide an example for you that follows the correct naming convention. Feel free to use our example naming or if you chose your own studio name, you can replace any instance of "My-Studio" with your studio's name instead.

Create a Second Subnet

- Click on **Subnets** in the left side panel

- Click **Create Subnet**
- Name tag: **Public Subnet B**
- VPC: Choose the one you just created (e.g., My-Studio-VPC)
- Availability Zone: Choose the **'b'** availability zone for your region (e.g., us-west-2b)
- IPv4 CIDR block: **10.0.1.0/24**
 - The **"/24"** in the CIDR block notation above specifies a range of IPv4 addresses for your subnet. In this case, we are specifying that your second subnet will have 24 bits allocated for the network prefix, and the remaining 8 bits for host addressing, resulting in IP addresses that range from 10.0.1.0 to 10.0.1.255.

Subnets > Create subnet

Create subnet

Specify your subnet's IP address block in CIDR format; for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC*

VPC CIDRs	CIDR	Status	Status Reason
	10.0.0.0/16	associated	

Availability Zone

IPv4 CIDR block*

* Required Cancel Create

- Click **Create**
- Click **Close**

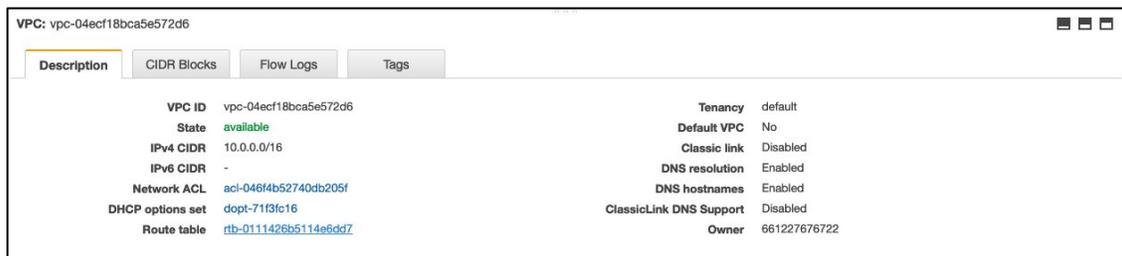


Internet Gateway

Now that you have your own VPC, you'll need to edit the internet gateway. What's that? An internet gateway allows for communication between your VPC and the greater internet. You'll need access to the internet in order to access the virtual workstations that we'll create later on.

Edit the Internet Gateway

- Click on **Your VPCs** in the left side panel
- Select the VPC that you created in the last step
- Under the **Description Tab** in the bottom panel click on the **Route Table** item



VPC: vpc-04ecf18bca5e572d6

Description | CIDR Blocks | Flow Logs | Tags

VPC ID	vpc-04ecf18bca5e572d6	Tenancy	default
State	available	Default VPC	No
IPv4 CIDR	10.0.0.0/16	Classic link	Disabled
IPv6 CIDR	-	DNS resolution	Enabled
Network ACL	acl-046f4b52740db205f	DNS hostnames	Enabled
DHCP options set	dopt-71f3c16	ClassicLink DNS Support	Disabled
Route table	rtb-0111426b5114e6dd7	Owner	661227676722

- This will show you the Route Table associated with your VPC. By default it doesn't have a name. To make it easier to identify your Route Table in the future, it's a good idea to name it.
- Hover over the blank field under **Name** in the list of Route Tables until you see the **pencil icon**.



Create route table | Actions

Route Table ID : rtb-0111426b5114e6dd7 | Add filter

Name	Route Table ID	Explicit subnet association
	rtb-0111426b5114e6dd7	-

- Click the icon, and then name your Route Table something that helps you identify it (e.g. My-Studio-Route-Table).



Create route table | Actions

Route Table ID : rtb-0111426b5114e6dd7 | Add filter

Name	Route Table ID	Explicit subnet association
My-Studio-Route-Table	rtb-0111426b5114e6dd7	-

- Make sure the Route Table you just named is selected, then click on the **Routes** tab down below.
- Click **Edit Routes**
 - Click **Add route**
 - Under **Destination** add **0.0.0.0/0**
 - For **Target** choose **Internet Gateway** and pick the item that appears.

Route Tables > Edit routes

Edit routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-01081c2fe99c43c34		No

Add route

* Required **Cancel** **Save routes**

- Click **Save Routes**
- Click **Close**

Route Table: rtb-0111426b5114e6dd7

Summary **Routes** Subnet Associations Edge Associations Route Propagation Tags

Edit routes

View All routes

Destination	Target	Status	Propagated
10.0.0.0/16	local	active	No
0.0.0.0/0	igw-01081c2fe99c43c34	active	No

- Make sure your Route Table is selected again, and click on **Subnet Associations** tab down below.
 - If there are no associations listed in the first table, click **Edit subnet associations**

Summary Routes **Subnet Associations** Route Propagation Tags

Edit subnet associations

<< None found >>

Subnet ID	IPv4 CIDR	IPv6 CIDR
You do not have any subnet associations.		

- Select **ALL** of the subnets

Route Tables > Edit subnet associations

Edit subnet associations

Route table: rtb-0111426b5114e6dd7 (My-Studio-Route-Table)

Associated subnets: subnet-042d148fed239b8ff | subnet-023d70e801c011c42

Filter by attributes or search by keyword

<input type="checkbox"/>	Subnet ID	IPv4 CIDR	IPv6 CIDR	Current Route Table
<input checked="" type="checkbox"/>	subnet-023d70e801c011c42 Public Su...	10.0.0.0/24	-	rtb-0da748f9f6ad0a14a
<input checked="" type="checkbox"/>	subnet-042d148fed239b8ff Public Subn...	10.0.1.0/24	-	Main

* Required

Cancel Save

- Click **Save**
- You now have your own VPC, which contains two public subnets and is connected to the Internet through your Internet Gateway:

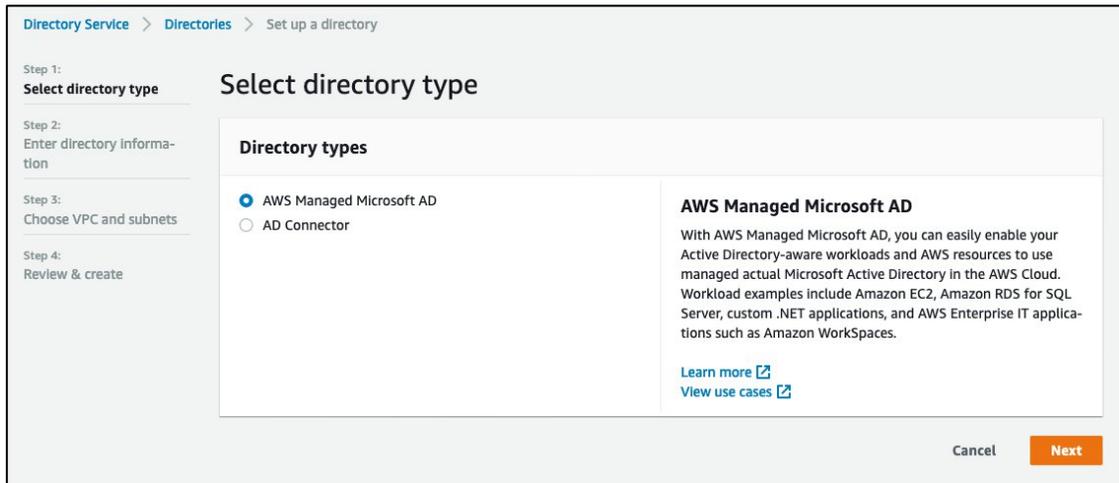


Active Directory

When you created an instance and connected to it in the first [tutorial](#), you logged in as Administrator. This is fine for a quick test, but for your studio you will want to have artists log in with their own accounts. In order to manage the different artists and users in your studio you'll set up a **Managed Microsoft Active Directory**. This allows for the storing of user profiles and settings that can follow users from virtual machine to virtual machine. In the next tutorial, we'll be adding users to Active Directory for your artists, but for now we'll just be doing some initial setup.

Set up your Active Directory

- Go to the **Services** drop down menu and search for **Directory Service**
- Click the **Set up directory** button
- Choose **AWS Managed Microsoft AD** and click **Next**



- Set the **Directory Information**
 - Edition: **Standard Edition**
 - Set the Directory DNS Name to **<your studio name>.com** (e.g., mystudio.com). Since DNS names are not case-sensitive, we suggest setting your DNS Name to the name of your studio, but in all lowercase letters. You'll also be typing this in a lot in later steps, so it's also easier to type! *Write this down in the [Important Information Cheat Sheet](#).*
 - Set the directory **NetBIOS** name (e.g., mystudio). Again it's not case-sensitive, so all lowercase here. *Note this in the cheat sheet as well.*
 - Set a description if you like.

- Set a unique Administrator password. *Make sure to put this on the cheat sheet as you will be using this password frequently.*

Enter directory information

Directory information

A managed Microsoft Active Directory domain based on Windows Server 2012 R2. [Info](#)

Directory type
Microsoft AD

Edition Info
Microsoft AD is available in the following two editions:

<input checked="" type="radio"/> Standard Edition Best for small to medium sized businesses. <ul style="list-style-type: none">• 1GB of storage for directory objects• Optimized for up to 30,000 objects ~USD 97.9200/mo (USD 0.1360/hr)* * Includes two domain controllers, USD 48.9600/mo for each additional domain controller.	<input type="radio"/> Enterprise Edition Best for large businesses. <ul style="list-style-type: none">• 17GB of storage for directory objects• Optimized for up to 500,000 objects ~USD 313.9200/mo (USD 0.4360/hr)* * Includes two domain controllers, USD 156.9600/mo for each additional domain controller.
---	--

Directory DNS name
A fully qualified domain name. This name will resolve inside your VPC only. It does not need to be publicly resolvable.

Directory NetBIOS name - *Optional*
A short identifier for your domain. If you do not specify a NetBIOS name, it will default to the first part of your Directory DNS name.

Maximum of 15 characters, can't contain the following characters: ` / : * ? " < > | ` . It must not start with ` ` .

Directory description - *Optional*
Descriptive text that appears on the details page after the directory has been created.

Maximum of 128 characters, can only contain alphanumerics, and the following characters: ` _ @ # % * + = : ? . / 1 - ` . It may not start with a special character.

Admin password
The password for the default administrative user named Admin.

Passwords must be between 8 and 64 characters, not contain the word "admin", and include three of these four categories: lowercase, uppercase, numeric, and special characters.

Confirm Password

This password must match the Admin password above.

- Click Next
- Set up the Networking

- Choose the **VPC** you just setup earlier (e.g., My-Studio-VPC) *You can find this on the cheat sheet.*
- Choose **Subnets** (A, then B - important to keep them in order)

Choose VPC and subnets

Networking
The VPC that contains your directory. If you do not have a VPC with at least two subnets, you must create one.

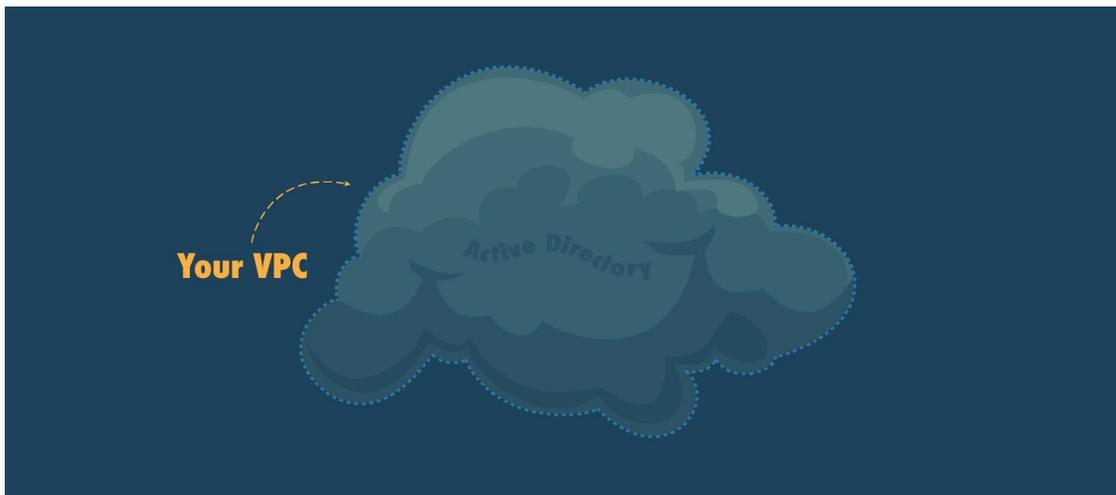
VPC Info
My-Studio-VPC | vpc-04ecf18bca5e572d6 (10.0.0.0/16)

[Create new VPC](#)

Subnets Info
Public Subnet A | subnet-023d70e801c011c42 (10.0.0.0/24, us-we...
Public Subnet B | subnet-042d148fed239b8ff (10.0.1.0/24, us-wes...

[Create new subnet](#)

- Click **Next**
- **Review**
 - Review the information you entered in the steps above.
 - If all looks good, click **Create directory**
 - This will take some time, about 20-40 minutes. While it is creating, move on to the next step!



IAM Role

AWS Identity and Access Management (IAM) helps you control access to AWS resources. We will use an IAM role to allow access to the services that your users need and restrict access to things that they don't. In this case, we'll be creating an IAM role to allow access to the Active Directory we just created. Without access to your Active Directory, your artists won't be able to login to instances using the unique usernames and passwords that we'll be creating for them in the next tutorial.

Create IAM Role for Launching Instances

Let's create an IAM Role that we can use when launching virtual workstation instances!

- Go to the **Services** dropdown menu and search for **IAM**
- In the lefthand column, click **Roles**
- Click **Create role**
- Under **Select type of trusted entity**, choose **AWS service**.
- Under **Choose the service that this role will use**, choose **EC2** and then choose **Next: Permissions**.

Select type of trusted entity

 AWS service EC2, Lambda and others	 Another AWS account Belonging to you or 3rd party	 Web identity Cognito or any OpenID provider	 SAML 2.0 federation Your corporate directory
---	--	--	---

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2 Allows EC2 instances to call AWS services on your behalf.
Lambda Allows Lambda functions to call AWS services on your behalf.

- In the list of policies, select the **AmazonSSMDirectoryServiceAccess** and **AmazonSSMManagedInstanceCore** policies. (To filter the list, type **SSM** in the search box.)

Create role 1 2 3 4

▼ **Attach permissions policies**

Choose one or more policies to attach to your new role.

Filter policies Showing 13 results

	Policy name	Used as
<input type="checkbox"/>	▶ AmazonEC2RoleforSSM	None
<input type="checkbox"/>	▶ AmazonSSMAutomationApproverAccess	None
<input type="checkbox"/>	▶ AmazonSSMAutomationRole	None
<input checked="" type="checkbox"/>	▶ AmazonSSMDirectoryServiceAccess	Permissions policy (1)
<input type="checkbox"/>	▶ AmazonSSMFullAccess	None
<input type="checkbox"/>	▶ AmazonSSMMaintenanceWindowRole	None
<input checked="" type="checkbox"/>	▶ AmazonSSMManagedInstanceCore	Permissions policy (1)
<input type="checkbox"/>	▶ AmazonSSMReadOnlyAccess	None

- Click **Next: Tags**
- For **Key** enter **Studio** and for **Value** enter the name of your studio from above (e.g., My-Studio). Then click **Next: Review**

Create role 1 2 3 4

Add tags (optional)

IAM tags are key-value pairs you can add to your role. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this role. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Studio"/>	<input type="text" value="My-Studio"/>	<input type="button" value="✕"/>
<input type="text" value="Add new key"/>	<input type="text"/>	

- For **Role name**, enter **EC2DomainJoin**
- (Optional) For **Role description**, enter a description

Create role

1
2
3
4

Review

Provide the required information below and review this role before you create it.

Role name*

Use alphanumeric and '+=,@_-' characters. Maximum 64 characters.

Role description

Allows EC2 instances to call AWS services on your behalf.

Maximum 1000 characters. Use alphanumeric and '+=,@_-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies

- [AmazonSSMDirectoryServiceAccess](#) ↗
- [AmazonSSMManagedInstanceCore](#) ↗

Permissions boundary Permissions boundary is not set

The new role will receive the following tag

Key	Value
Studio	My-Studio

- Choose **Create role**

Security Groups

Next, you'll create a new security group. Since your VPC is connected to the Internet, you need some way of controlling the inbound and outbound traffic. In the security group you will define rules to allow only certain kinds of traffic into your VPC. This helps keep your VPC and your data secure. In our tutorials, we'll be creating different security groups for different functions.

The first security group we'll create will be to allow Remote Desktop connections, which we'll be using throughout these tutorials for connecting to EC2 instances. Later on, we'll create more security groups to allow for other things such as connecting to Linux instances and connecting to render farm management software.

Create a Remote Desktop Security Group

- Go to **Services** → **EC2**
- Check that your region is still set correctly by looking at the region dropdown menu in the top right of the page.
- Select **Security Groups** in the left side panel under Network & Security
- Click **Create Security Group**
- Choose a name for your security group (e.g., My-Studio-Remote-Desktop-SG)

- Set the Description to **Allows for Remote Desktop Connection**
- Set the **VPC** to the VPC you created above (e.g. My-Studio-VPC). *You can also find this information on the cheat sheet.*
- Next, we'll tell the security group which ports are going to be open for *incoming* connections (located in the **Inbound rules** block).
 - Notice at first there are no rules for incoming connections. This means that nobody can connect to this machine from anywhere. We want to allow your local computer to be able to connect, thus we need to open the port that specifically allows that connection.
 - Click **Add Rule**
 - Under **Type**: choose **RDP**
 - Notice that it automatically set the port range to **3389** - this is the default incoming port for RDP (Remote Desktop Protocol) connections.
 - Set the **Source**

 *Note:* By default, we'll be setting the source to "Anywhere", which allows any computer to attempt Remote Desktop connections to your instances. This is probably acceptable during the initial setup of your studio, but before creating production content, you will want to limit the source to **just the computers** your artists will be using to access your studio. Your network administrator can help you determine the correct range of source IP addresses to enter here.

- If you do not wish to limit which IP addresses can connect at this time, then you can set the Source to **Anywhere**. It will automatically add the IP addresses 0.0.0.0/0, and ::/0.
 - Set the **Description** to **Remote Desktop**

EC2 > Security Groups > Create security group

Create security group [Info](#)

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name [Info](#)

Name cannot be edited after creation.

Description [Info](#)

VPC [Info](#)

Inbound rules [Info](#)

Type	Protocol	Port range	Source	Description - optional
RDP	TCP	3389	Anywhere	Remote Desktop
			0.0.0.0/0	
			::/0	

[Add rule](#)

Outbound rules [Info](#)

Type	Protocol	Port range	Destination	Description - optional
All traffic	All	All	Custom	
			0.0.0.0/0	

[Add rule](#)

Cancel [Create security group](#)

- Click **Create security group**
- You will now be placed in the details page for the newly created security group.
- Look at the **Inbound rules** tab and you should see the following rules. Note: Even though you added one rule above, you will see two separate rules (one with source 0.0.0.0/0 and one with source ::/0). Don't worry, that's normal.

Inbound rules | Outbound rules | Tags

[Edit inbound rules](#)

Type	Protocol	Port range	Source	Description - optional
RDP	TCP	3389	0.0.0.0/0	Remote Desktop
RDP	TCP	3389	::/0	Remote Desktop

- Please take a moment to enter the Remote Desktop Security Group's name and ID on the [Important Information Cheat Sheet](#). You can find the ID to the right of the name in the list of security groups. It will look like: sg-928th290koqj8214r.

Add a Tag to Your Security Group

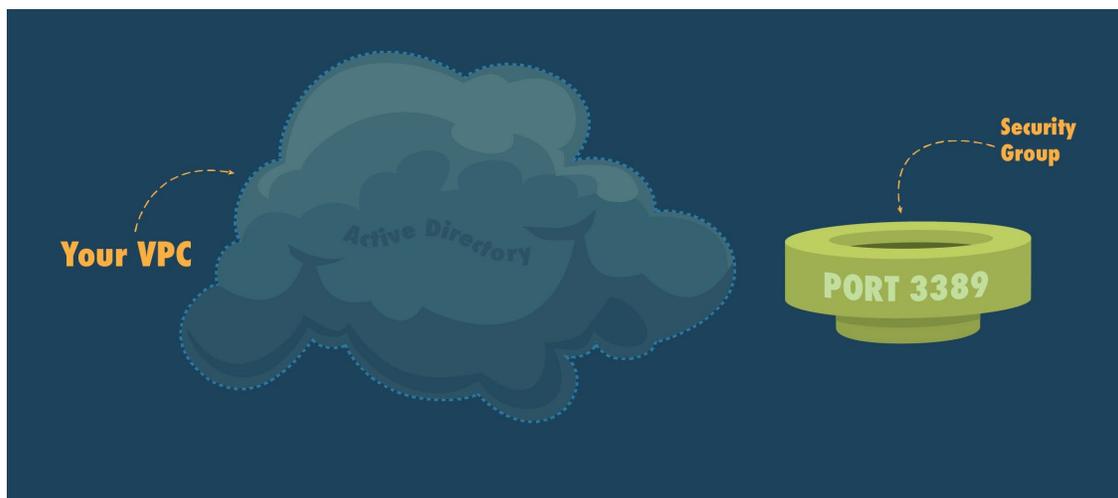
Next, we're going to add a tag to identify this security group as part of your studio. A tag is just a label that you can assign to an AWS resource. They make it easier to manage, search for and

filter resources. They can also be used as cost allocation tags to help you understand the cost of running various aspects of the studio.

- Make sure your new security group is selected
- On the **Tags** tab in the bottom panel, click on the **Add/Edit Tags** button
- In the **Add/Edit Tags** popup window, click the **Create Tag** button
- For **Key** enter **Studio**
- For **Value** enter the name you picked for your studio (e.g., My-Studio). *Refer to your studio name in the cheat sheet if needed.*
- When you're done, click the **Save** button

Key	Value
Studio	My-Studio

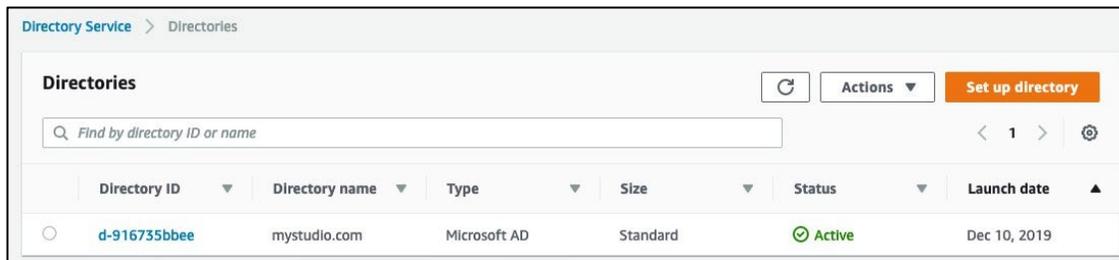
We'll be adding this same Studio:My-Studio tag to each of the resources you'll be creating for your studio in the cloud. That will make it super easy to find everything if you need to later on.



Exercise: Test Your Setup So Far

Congratulations, you've completed the basic setup for your Studio in the Cloud! Now you're going to launch a virtual workstation and test that Active Directory is working. This instance will be used later to manage your users. We'll call it the **User Management** instance.

Note: Before moving on to this step, make sure that Active Directory has finished creating by going to **Services** → **Directory Service**. When it's done, the status will change from **Creating** to **Active**.



Sometimes the status may not update automatically. If you've already waited 20-40 minutes and the status is still listed as **Creating**, you can click the **Refresh** button, located near the top of the page, to the left of the white "Actions" pull down and orange "Set up directory" button.

Create an EC2 Instance

- Go to **Services** → **EC2** and select **Instances** in the left side panel
- Click **Launch Instance**
- Search for **Windows**
- Select: **Microsoft Windows Server 2019 Base**
- Choose the instance type **m5.xlarge**, then click **Next: Configure Instance Details**

<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes

- Configure Instance Details:
 - Network: **<VPC you created>** (e.g., My-Studio-VPC) *Refer to the VPC name you wrote down in the cheat sheet.*
 - Subnet: **Public Subnet A**

- Auto-assign Public IP: **Enable**

Network *i* vpc-04ecf18bca5e572d6 | My-Studio-VPC ↕ [Create new VPC](#)

Subnet *i* subnet-023d70e801c011c42 | Public Subnet A | us ↕ [Create new subnet](#)
251 IP Addresses available

Auto-assign Public IP *i* **Enable** ↕

- Domain join directory: **<your Active Directory DNS name>** (e.g., mystudio.com)
You can also find this on the cheat sheet.
- IAM role: **EC2DomainJoin**

Domain join directory *i* mystudio.com (d-916735bbee) ↕ [Create new directory](#)
This directory is in a different VPC from the instance you are launching. Ensure that networking is setup between these two VPCs. [Learn more](#)

IAM role *i* EC2DomainJoin ↕ [Create new IAM role](#)
For Domain join to succeed select an IAM role that has an AmazonEC2RoleforSSM policy attached

- Monitoring: **Enable CloudWatch detailed monitoring**

Shutdown behavior *i* Stop ↕

Stop - Hibernate behavior *i* Enable hibernation as an additional stop behavior

Enable termination protection *i* Protect against accidental termination

Monitoring *i* Enable CloudWatch detailed monitoring
[Additional charges apply.](#)

- Click **Next: Add Storage**
- Add Storage:
 - Leave the storage size at the default value of **30 GB**.

Step 4: Add Storage
Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type <i>i</i>	Device <i>i</i>	Snapshot <i>i</i>	Size (GiB) <i>i</i>	Volume Type <i>i</i>	IOPS <i>i</i>	Throughput (MiB/s) <i>i</i>	Delete on Termination <i>i</i>	Encryption <i>i</i>
Root	/dev/sda1	snap-00708ab38ae2495bc	30	General Purpose SSD (gp2) ↕	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted ⌵

[Add New Volume](#)

- Click **Next: Add Tags**
- Add Tags
 - Add a tag with the key **Name** and the value **User Management**

- Add another tag with the key **Studio** and the value the name of your studio you've used in other steps (e.g., My-Studio)

Step 5: Add Tags
 A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webservers.
 A copy of a tag can be applied to volumes, instances or both.
 Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances ⓘ	Volumes ⓘ	
Name	User Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Studio	My-Studio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Add another tag (Up to 50 tags maximum)

- Click **Next: Configure Security Group**
- **Configure Security Group**
 - Choose **Select existing security group**
 - Choose the security group that you created earlier (e.g., My-Studio-Remote-Desktop-SG). Selecting that security group allows for Remote Desktop connections to your instance. For now that is all we need, but in later tutorials we'll be adding more security groups to allow other types of connections as well. *Refer to the Remote Desktop Security Group Name and ID your entered on the cheat sheet if necessary.*

Step 6: Configure Security Group
 A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group
 Select an existing security group

Security Group ID	Name	Description	Actions
<input type="checkbox"/> sg-0469b547302b78a18	default	default VPC security group	Copy to new
<input checked="" type="checkbox"/> sg-0c0efc81a52047acb	My-Studio-Remote-Desktop-SG	Allows for Remote Desktop Connection	Copy to new

- Click **Review and Launch**
- Click **Launch**
- Create a new key pair if you want, or use one that you already have. If you completed the Starter Exercise from Tutorial 1, we recommend re-using the key pair that you already created (e.g., mystudio-keypair.pem). *If you don't remember the name of the key pair you created, you can find it at the bottom of the Tutorial 1 section of the cheat sheet.*

- Check the box next to the acknowledgement that you have access to the selected key pair.

Select an existing key pair or create a new key pair ✕

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair ⌵

Select a key pair

mystudio-keypair ⌵

I acknowledge that I have access to the selected private key file (mystudio-keypair.pem), and that without this file, I won't be able to log into my instance.

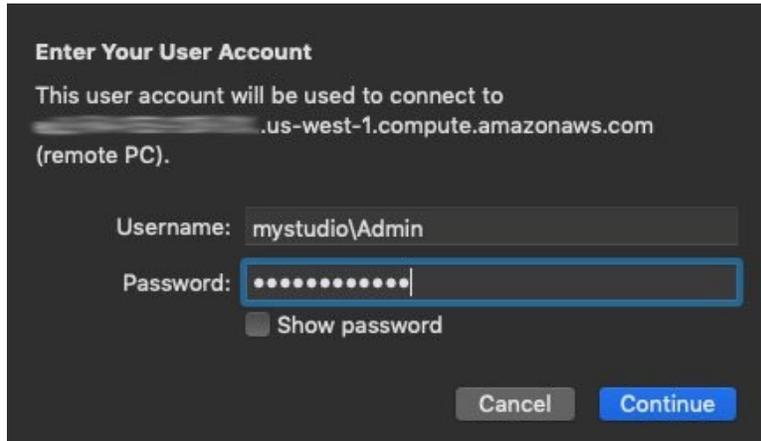
Cancel Launch Instances

- Click **Launch Instances**
- Note: If you are trying to launch in a new region, you may get a "Launch Failed" screen after attempting to launch. If that happens, just wait a few minutes and try again.
- Click the **View Instances** button at the bottom right of the screen to go to the list of running instances.
- Logging in
 - After a few minutes, when the instance is ready (its state says running and the status checks say 2/2 Status Checks Complete), select it and hit **Connect**

Launch Instance		Connect	Actions				
Name	Instance Type	Instance State	Status Checks	Launch Time	Owner		
User Management	m5.xlarge	running	2/2 checks ...	December 10, 2019 at 9:35:...	6612276722		

- Click **Download the Remote Desktop File**
- Open Remote Desktop
- A window asking for the Administrator password will pop up, but this time we're going to use the credentials you created when you set up your Active Directory. Instead, click **More choices** near the bottom of the popup, then click **Use a different account**

- For **User name**: use the <Active Directory NetBios name>\Admin. For example: **mystudio\Admin** *You can find the Active Directory NetBios name on the cheat sheet.*
- The password will be what you entered above when you set up your Active Directory. *This password can also be found on the cheat sheet.*
- Click **OK**



Enter Your User Account

This user account will be used to connect to
[redacted].us-west-1.compute.amazonaws.com
(remote PC).

Username: mystudio\Admin

Password: [masked password]

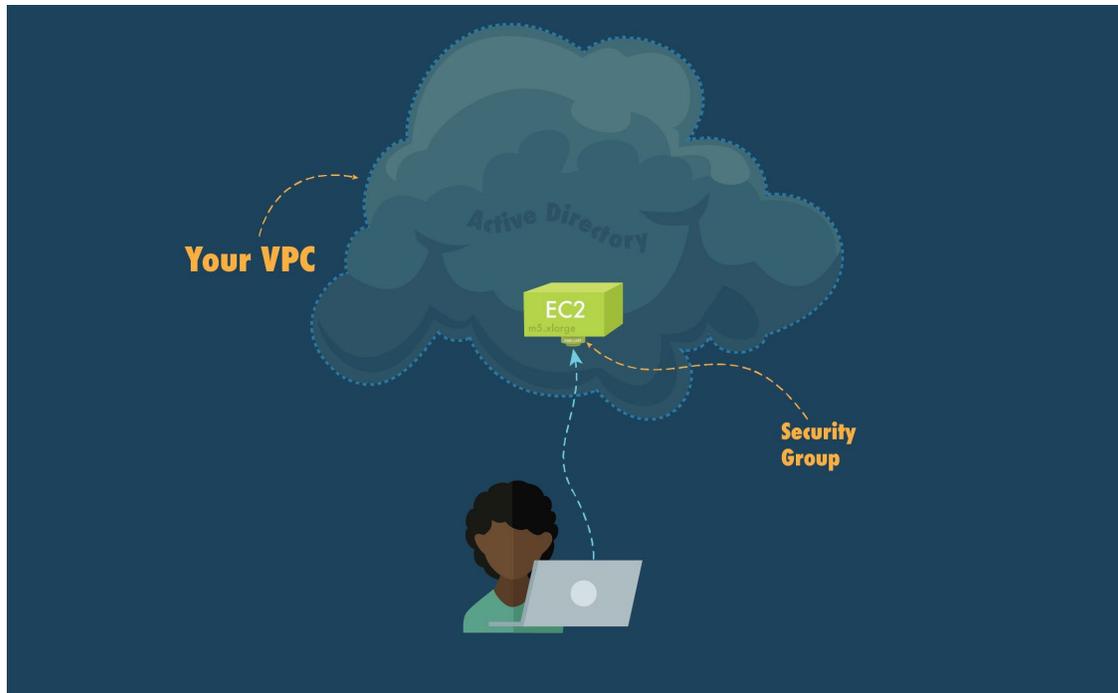
Show password

Cancel Continue

- Click **Yes** in the next popup window
- If all goes well, you should connect to the desktop of your virtual workstation with the Active Directory administrator account!

Your Studio in the Cloud VPC So Far

Let's review what we've done up to this point. Here's an illustration of the current state of your VPC:



You've got your custom VPC and inside it are one Active Directory serving two subnets. And inside Public Subnet A you have one EC2 instance currently running, connected to your local machine through an Internet gateway with the traffic controlled by your security group.

In our next tutorial, we'll continue building on the parts that you've already put in place and add new ones. Our next task is to create a shared file system and set up accounts for your users.

If you'll be moving immediately to the next tutorial, you can stay logged in to your User Management instance and go directly to: [Tutorial 3: Setting Up an FSx File System and User Accounts](#)

However, if you will be continuing your setup on another day, you'll want to disconnect from and temporarily stop your instance to save resources (and money!).

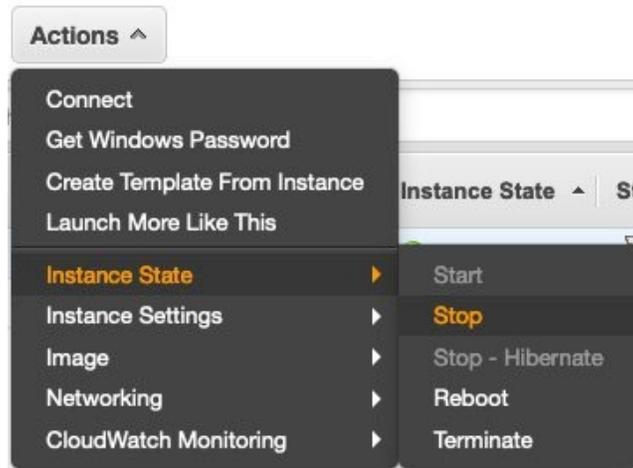
Shut Down Notes

At the moment you only have one instance running for user management, so the shut down notes for this tutorial will be short and sweet. The procedure is almost identical to the steps you used to terminate the instance you created in the starter exercise in Tutorial 1, except this time instead of terminating your instance you'll be stopping it instead. This way, you'll be able to easily start it up again when you're ready to continue.

Stopping an Instance

- In the Remote Desktop session for your instance, disconnect by going to **Start Menu**→**Power**→**Disconnect**

- In the AWS Console go to **Services**→**EC2**
- Near the top of the page, click **Running Instances**
- Select your **User Management** instance from the list
- Click on the **Actions** button, then select **Instance State**→**Stop**



Link to next tutorial: [Tutorial 3: Setting Up an FSx File System and User Accounts](#)

Appendix

Tutorial Table of Contents

- [Tutorial 1: Getting Started with AWS Virtual Workstations](#)
- [Tutorial 2: Creating a VPC and Active Directory for Your Studio - *this page*](#)
- [Tutorial 3: Setting Up an FSx File System and User Accounts](#)
- [Tutorial 4: Building a Render Scheduler with AWS Thinkbox Deadline](#)
- [Tutorial 5: Installing Applications and Creating a Workstation AMI](#)
- [Tutorial 6: Setting Up a Linux Farm Worker and Spot Fleet Request](#)
- [Tutorial 7: Onboarding New Artists and Sample Workflow](#)

Links to AWS Documentation

- [What Is Amazon VPC?](#)
- [Internet Gateways](#)
- [Security Groups for Your VPC](#)
- [Active Directory Prerequisites](#)
- [What is IAM?](#)

- [Seamlessly Join a Windows EC2 Instance](#)

Downloads

- [Important Information Cheat Sheet](#)