ADMINISTERING MANAGED AD

Abstract

In this lab, you will deploy a management server in your VPC and install the Active Directory tools to manage your AWS Managed Microsoft AD. You will also experience the seamless domain join feature. This feature automatically joins the new management server to AD as a domain member when you deploy it.

Introduction

AWS Managed Microsoft AD lets you run Microsoft Active Directory (AD) as a managed service. When you launch AWS Managed Microsoft AD, AWS creates a highly available pair of domain controllers connected to your virtual private cloud (VPC).

Since the Domain Controllers (DC's) are managed by AWS, you cannot login to the DC's using Remote Desktop Protocol (RDP). In order to manage the data within the AWS Managed Microsoft AD (e.g. users, computers, group policy, sites, sitelinks, DNS etc), you need to create a management server and perform all the domain management operations from this server. This management server can be placed anywhere on the network as long as necessary network connectivity exist between the Domain Controllers and the management server. Typically, this management server is placed network-wise close to the Domain Controllers.

For more information on AWS Directory service, please visit our developers guide.

Prerequisites

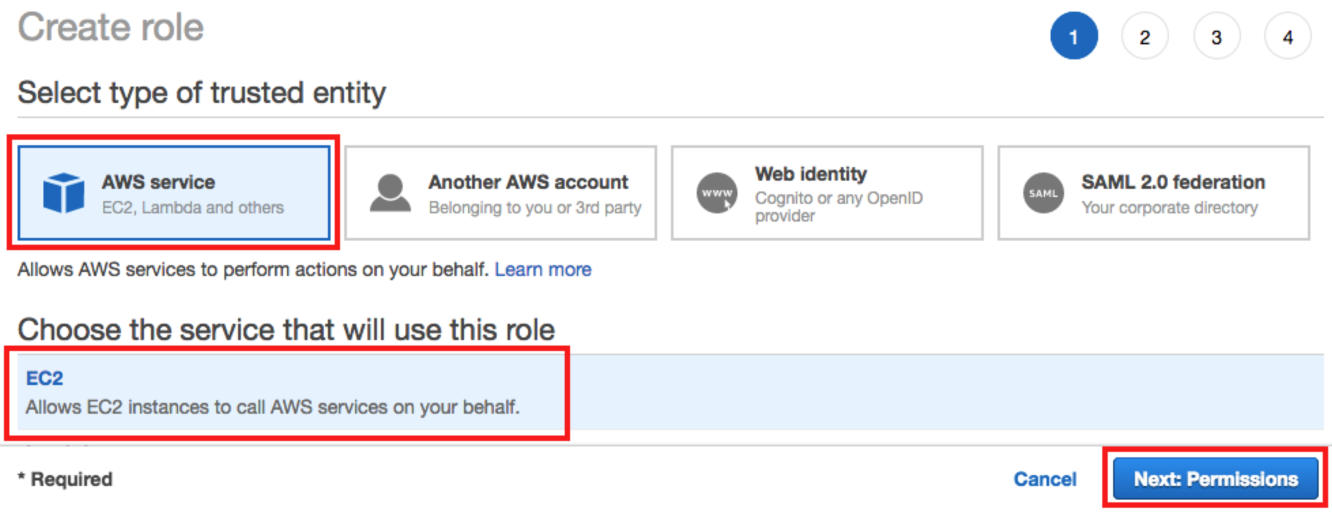
To setup the management server for use with AWS Managed AD, you need the following:

- Please complete the previous Lab 2 sections.

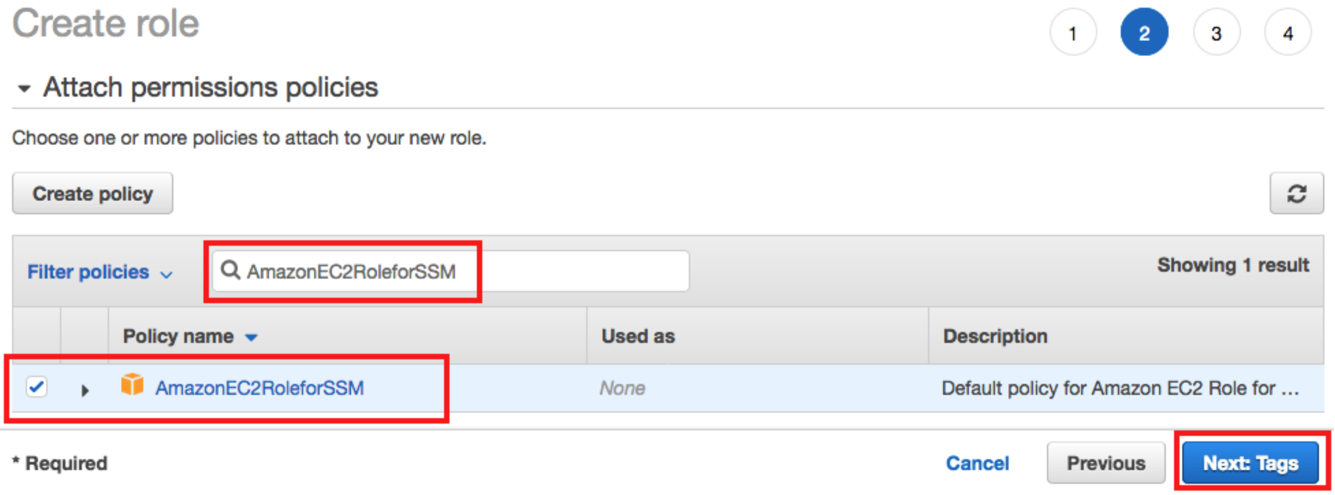
- An AWS account with an AWS IAM user / role with privileges to Elastic Compute Cloud (EC2) service.
- If you plan to login to the management server from the Internet, you need to deploy the management server in a public subnet in your VPC.
- All the necessary Active Directory TCP & UDP ports that are required for communication between DC's and the management server should be open.

Section 1: Create IAM role for seamless domain join

1. Login to your AWS Account. In the find services field, search for **IAM** service
2. Under Roles, click on "**Create Role**".
3. Select the **AWS service**.
4. Select **EC2** as shown below and click on **"Next: Permissions"**.


Create role
1
2
3
4
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.
* Required
Cancel
Next: Permissions

5. Under policies, search for "**AmazonEC2RoleforSSM**", select this policy and click **"Next: Tags"**.



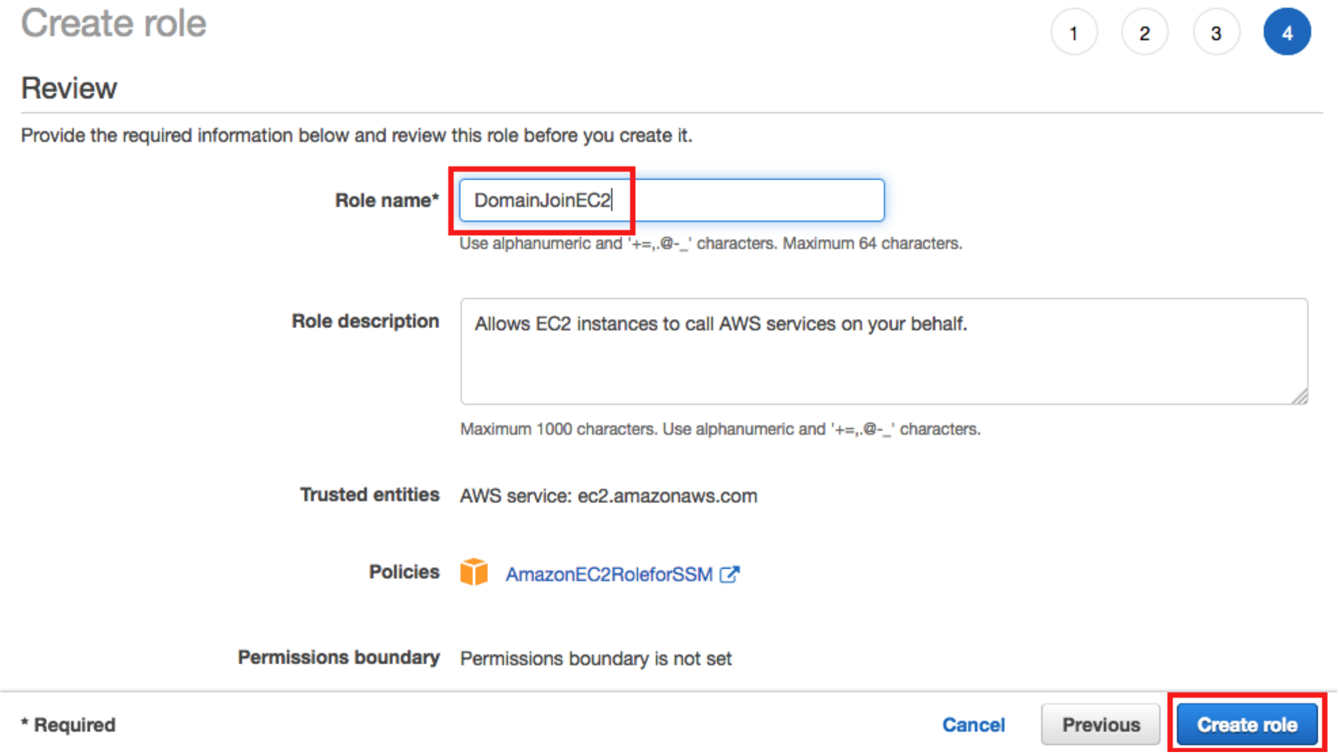
Attach permissions policies

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

Search: AmazonEC2RoleforSSM

☑		Policy name	Used as	Description
☑	▸	AmazonEC2RoleforSSM	None	Default policy for Amazon EC2 Role for …

6. Enter **“CreatedBy”** for the Key and for value, enter your name. Tags are great resource to help you organize and keep track of AWS resources. Before deploying a large AWS implementation, you should design a Tag strategy for your company. Click **“Next: Review”.**
7. For the role name, use **“DomainJoinEC2”** and click on **“Create Role”** to complete the role creation.



Review

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

Role name* DomainJoinEC2

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.

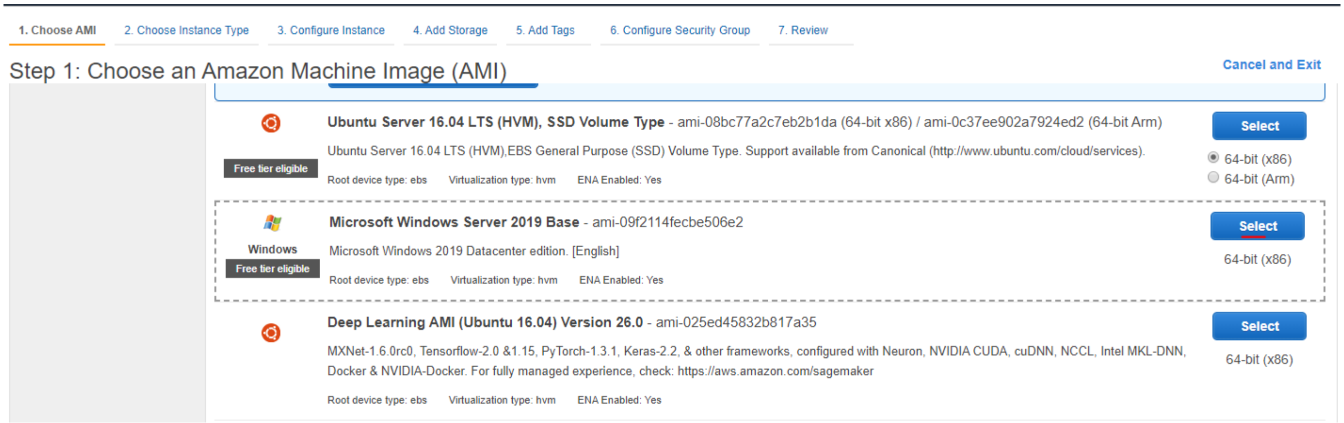
Trusted entities: AWS service: ec2.amazonaws.com

Policies: AmazonEC2RoleforSSM

Permissions boundary: Permissions boundary is not set

Section 2: Deploying the Management Server

1. Login to the AWS Console. In the find services search box, type **EC2**.
2. Before you begin the lab, make sure you are in the "**N. Virginia**" region (check the upper right hand corner of the screen). For this lab, you will deploy the management server in the same VPC as Managed AD.
3. Click on "**Launch Instance**".
4. For the Amazon Machine Image (AMI), search for the newest Microsoft Windows Server base image (e.g. Microsoft Windows Server 2019 Base) and press **Select**.



Step 1: Choose an Amazon Machine Image (AMI)

Ubuntu Server 16.04 LTS (HVM), SSD Volume Type - ami-08bc77a2c7eb2b1da (64-bit x86) / ami-0c37ee902a7924ed2 (64-bit Arm)

Ubuntu Server 16.04 LTS (HVM),EBS General Purpose (SSD) Volume Type. Support available from Canonical (http://www.ubuntu.com/cloud/services).

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

● 64-bit (x86)
○ 64-bit (Arm)

Microsoft Windows Server 2019 Base - ami-09f2114fecbe506e2

Microsoft Windows 2019 Datacenter edition. [English]

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

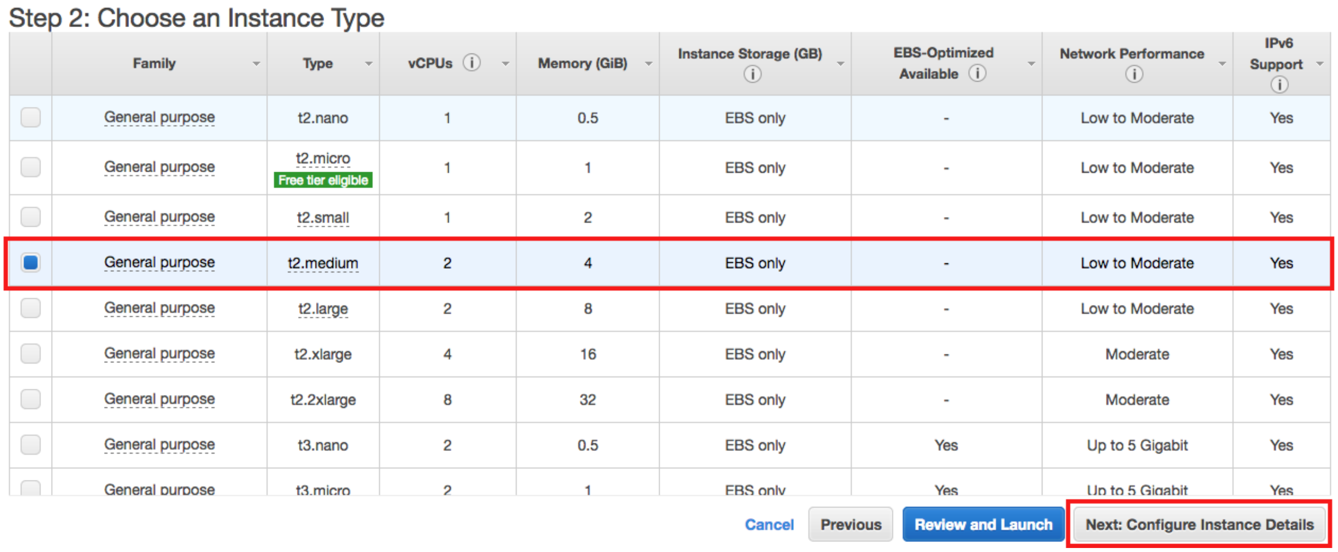
Deep Learning AMI (Ubuntu 16.04) Version 26.0 - ami-025ed45832b817a35

MXNet-1.6.0rc0, Tensorflow-2.0 &1.15, PyTorch-1.3.1, Keras-2.2, & other frameworks, configured with Neuron, NVIDIA CUDA, cuDNN, NCCL, Intel MKL-DNN, Docker & NVIDIA-Docker. For fully managed experience, check: https://aws.amazon.com/sagemaker

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

64-bit (x86)

5. For the Instance type, please select **"t2.medium"** for the management server. Click **"Next: Configure Instance Details"** after you select the instance type.



Step 2: Choose an Instance Type

	Family	Type	vCPUs ⓘ	Memory (GiB)	Instance Storage (GB) ⓘ	EBS-Optimized Available ⓘ	Network Performance ⓘ	IPv6 Support ⓘ
□	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
☑	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
□	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
□	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
□	General purpose	t3.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
□	General purpose	t3.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

6. For the Instance configuration,

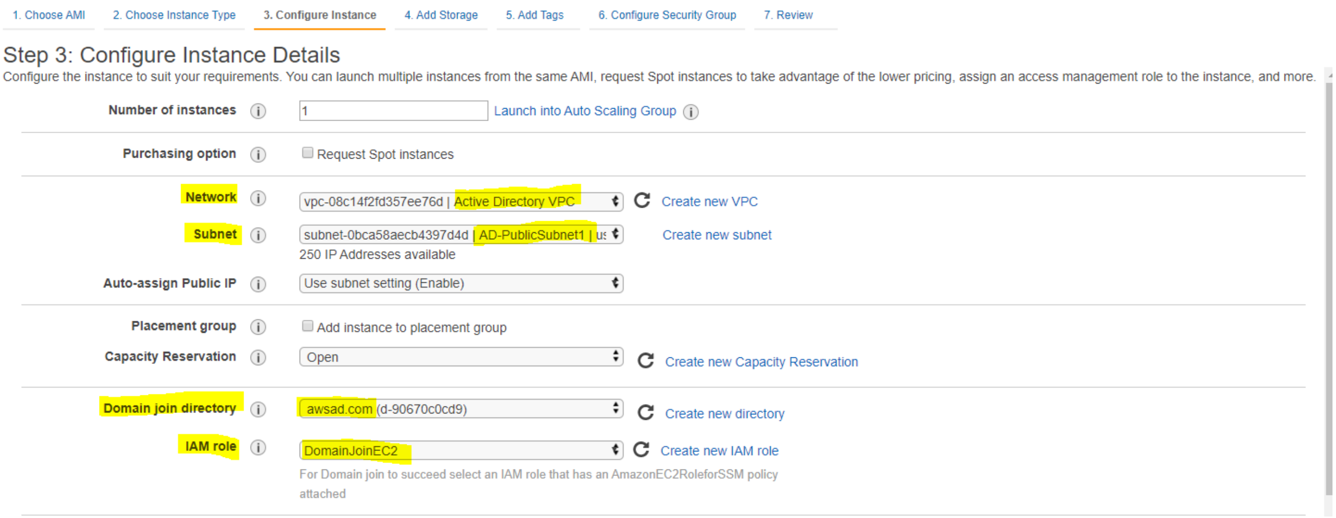
   a. For Network, select your **Active Directory VPC**

   b. For Subnet, select **AD-PublicSubnet1**.

   c. For Domain join directory, select **awsad.com**.

   d. For IAM role, select **DomainJoinEC2**.

   e. Click **“Next: Add Storage”.**



Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 Launch into Auto Scaling Group

Purchasing option: □ Request Spot instances

Network: vpc-08c14f2fd357ee76d | Active Directory VPC — Create new VPC

Subnet: subnet-0bca58aecb4397d4d | AD-PublicSubnet1 | us — Create new subnet

250 IP Addresses available

Auto-assign Public IP: Use subnet setting (Enable)

Placement group: □ Add instance to placement group

Capacity Reservation: Open — Create new Capacity Reservation

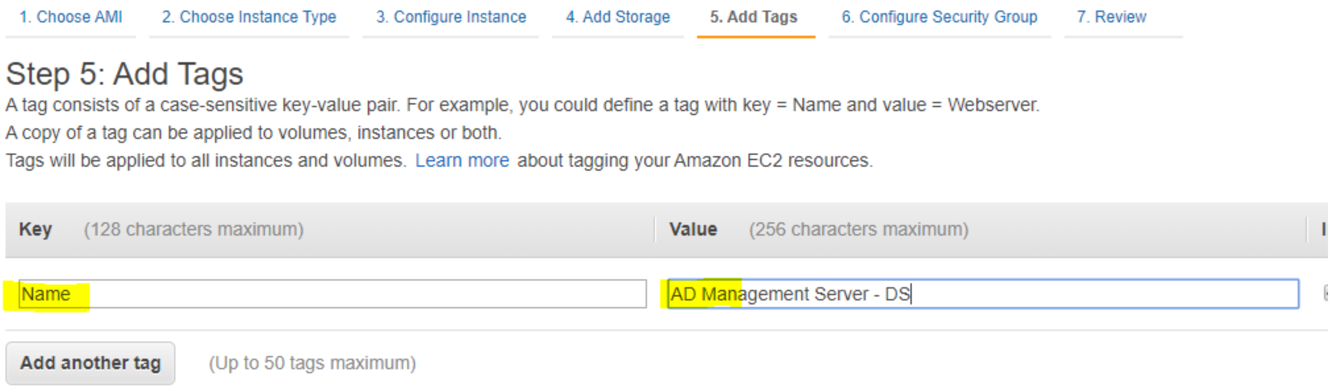
Domain join directory: awsad.com (d-90670c0cd9) — Create new directory

IAM role: DomainJoinEC2 — Create new IAM role

For Domain join to succeed select an IAM role that has an AmazonEC2RoleforSSM policy attached

7. Leave all the values in the storage page as default. Click **“Next: Add Tags”.**

8. Click on **“Add tag”** and enter **“Name”** for the key and **“AD Management Server - <initials>”** for the value. For EC2 instances, the name field is important to set since this name field value is used to identify the server in the list of EC2 instances. Click **“Next: Configure Security Group”.**



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 = Webserver.
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)
Name	AD Management Server - DS

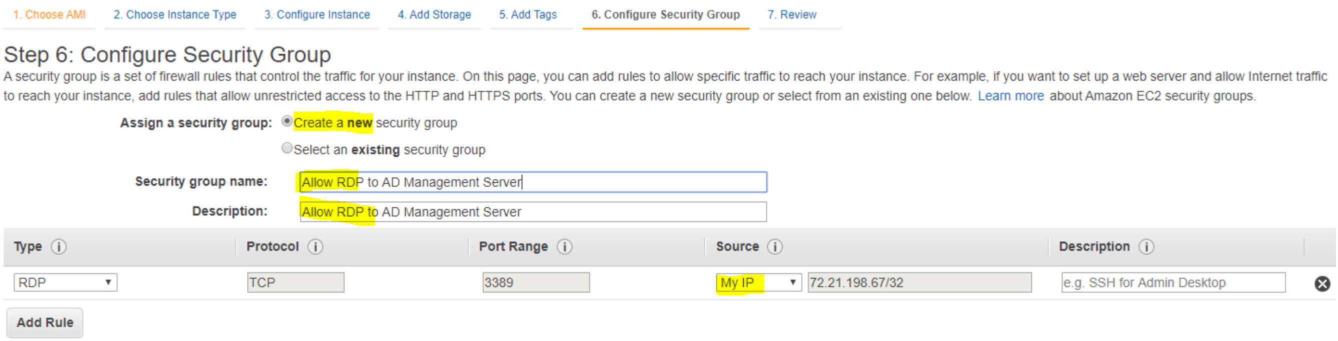
Add another tag (Up to 50 tags maximum)

9. Click on **"Create a new security group".**

   a. For Security Group name, enter **"Allow RDP to AD Management Server"**.

   b. For Description, enter a description of the security group usage.

   c. For the rule, go to the **Source** dropdown and select "**My IP**." Before this change, the security group would allow RDP access from anywhere in the Internet. This is not recommended. Try to limit the IP addresses which you will allow RDP access into your public server. Another option is to use System Manager Session Manager.



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 name: Allow RDP to AD Management Server

Description: Allow RDP to AD Management Server

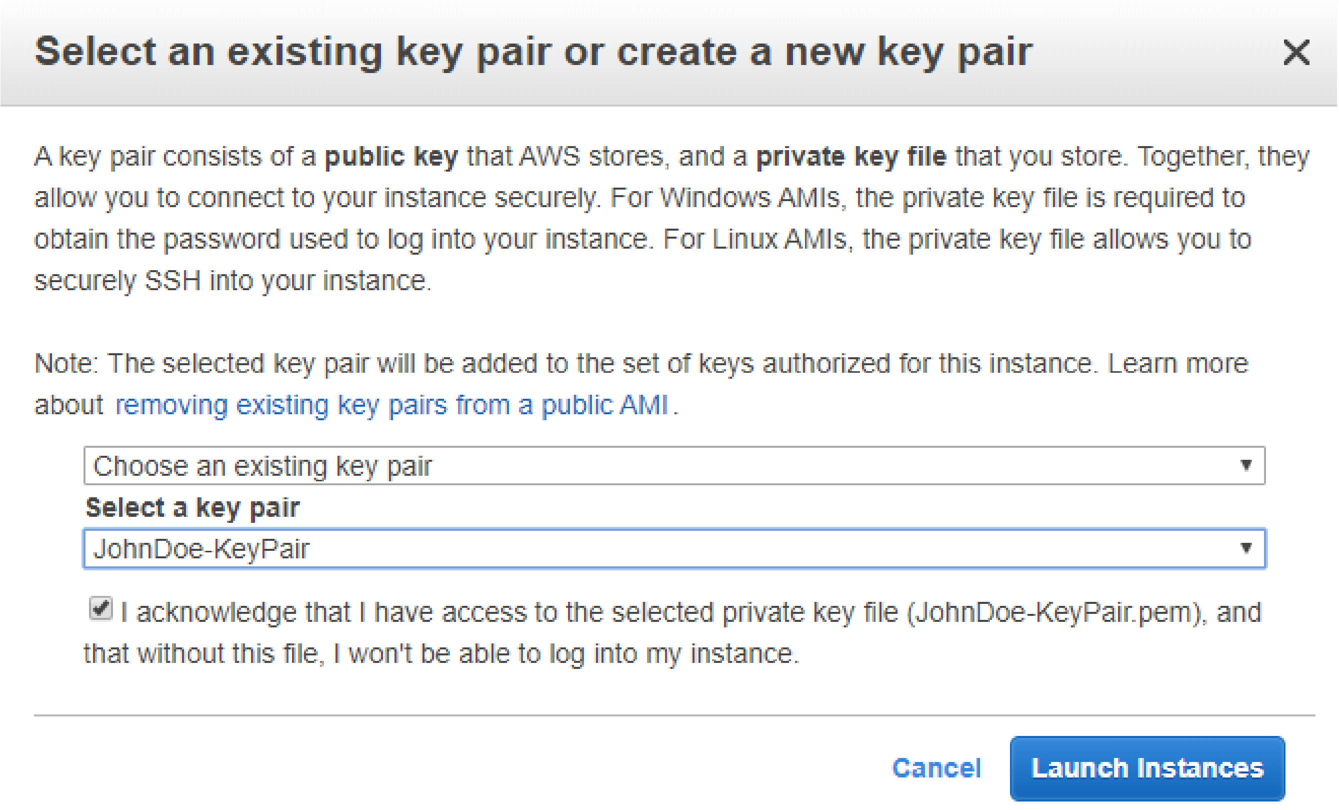
Type	Protocol	Port Range	Source		Description
RDP	TCP	3389	My IP	72.21.198.67/32	e.g. SSH for Admin Desktop

10. Review the configuration, and click on **"Review and Launch"**.

11. Review the settings, and click **"Launch Instances".**

12. If you have a key pair which you created in an earlier lab, select "**Choose an existing key pair**". If you didn't create a key pair earlier, then you will need to select "**Create a new key pair**." In the picture below, I selected the key pair that I created in an earlier lab.

13. Click "**Launch Instances**"



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

JohnDoe-KeyPair

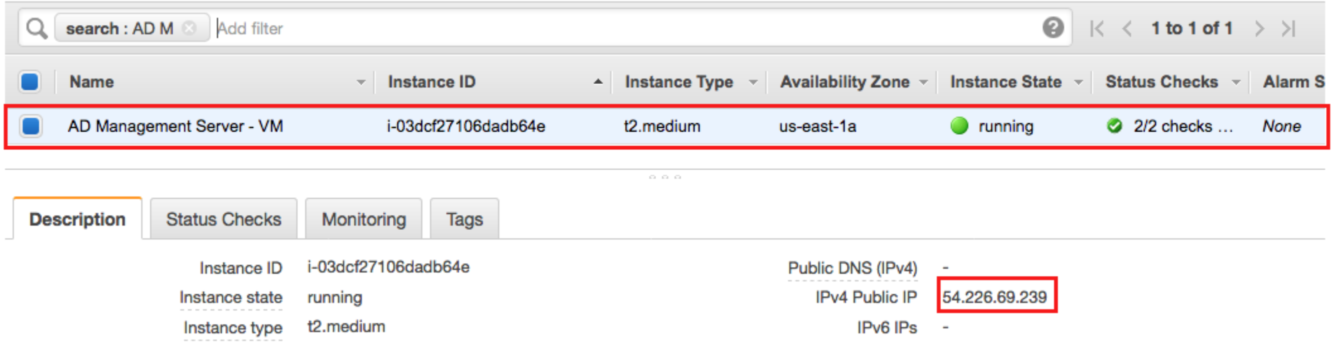
☑ I acknowledge that I have access to the selected private key file (JohnDoe-KeyPair.pem), and that without this file, I won't be able to log into my instance.

14. Click “**View Instances**”

Section 3: Installing the Active Directory Tools

You will next login to the management server using Remote Desktop Protocol (RDP) and install the Active Directory Tools. If you are connecting from a Windows computer, you should have the RDP tool. If you are using a Mac, please download the RDP client here.

1. Log in to the AWS Console and go to Elastic Compute Cloud (EC2) console.
2. Look for the server that you just created by looking at the Name column. You should see the server based upon the Name tag that you set.
3. Identify the public IP / DNS name of your management server by selecting the server in the list and reviewing the Description tab below it. Copy the IPv4 public IP to your clipboard.

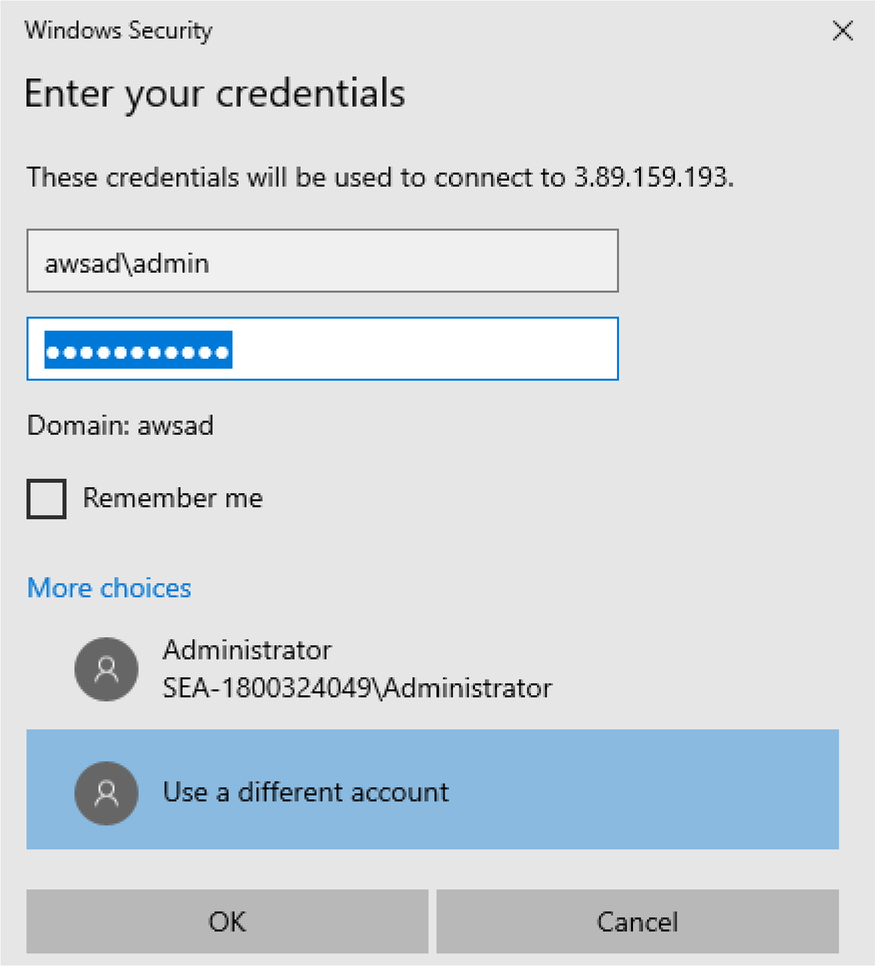


	Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm S
■	AD Management Server - VM	i-03dcf27106dadb64e	t2.medium	us-east-1a	● running	✓ 2/2 checks ...	None

Instance ID i-03dcf27106dadb64e
Instance state running
Instance type t2.medium

Public DNS (IPv4) -
IPv4 Public IP 54.226.69.239
IPv6 IPs -

4. RDP to the server. Click the **Connect** button. Click the "**Download Remote Desktop File**" to download the RDP file. Click the downloaded RDP file.
5. Since our instance is already domain joined to the AWS Managed AD, we can directly login to our instance with our admin credentials. Select **More Choices** and **Use a different account**. For the user name use **"awsad\admin"**. For the password, enter the password that you specified when you created the AWS Managed Microsoft AD.



Windows Security

Enter your credentials

These credentials will be used to connect to 3.89.159.193.

awsad\admin

●●●●●●●●●●●

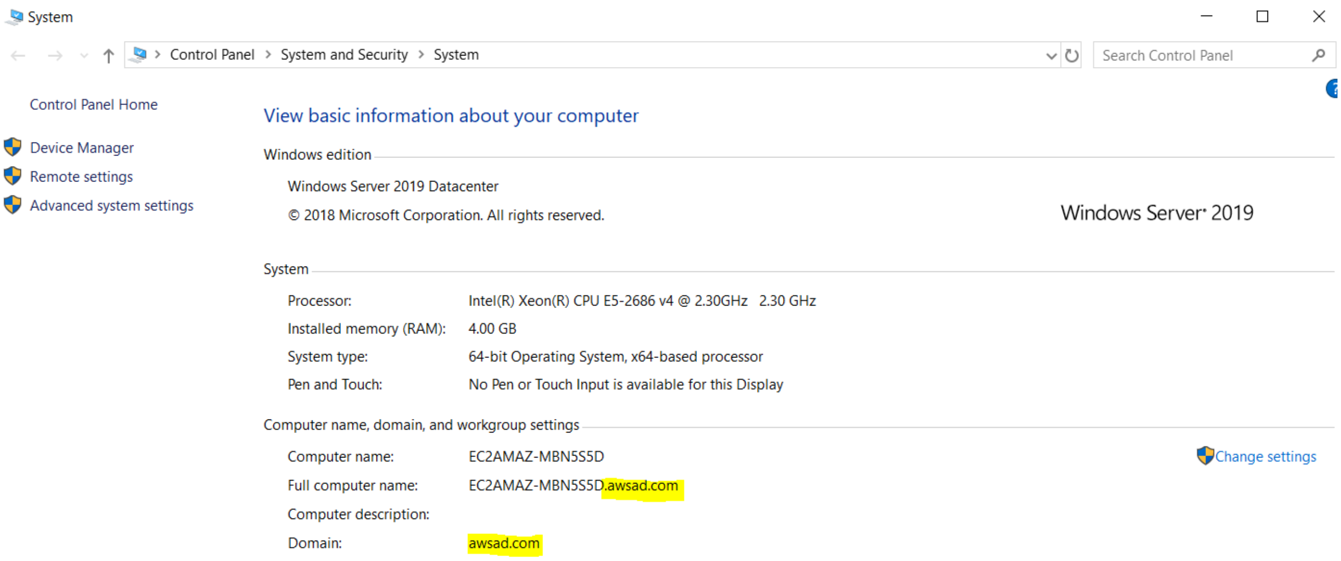
Domain: awsad

□ Remember me

Administrator
SEA-1800324049\Administrator

Use a different account

6. Notice that you are able to login with an AD domain account. Open a Windows Explorer window. Right click "**This PC**" and select **Properties**. Notice that the computer has been joined to the AWS Managed Microsoft AD that you created earlier.



View basic information about your computer

Windows edition

Windows Server 2019 Datacenter

© 2018 Microsoft Corporation. All rights reserved.

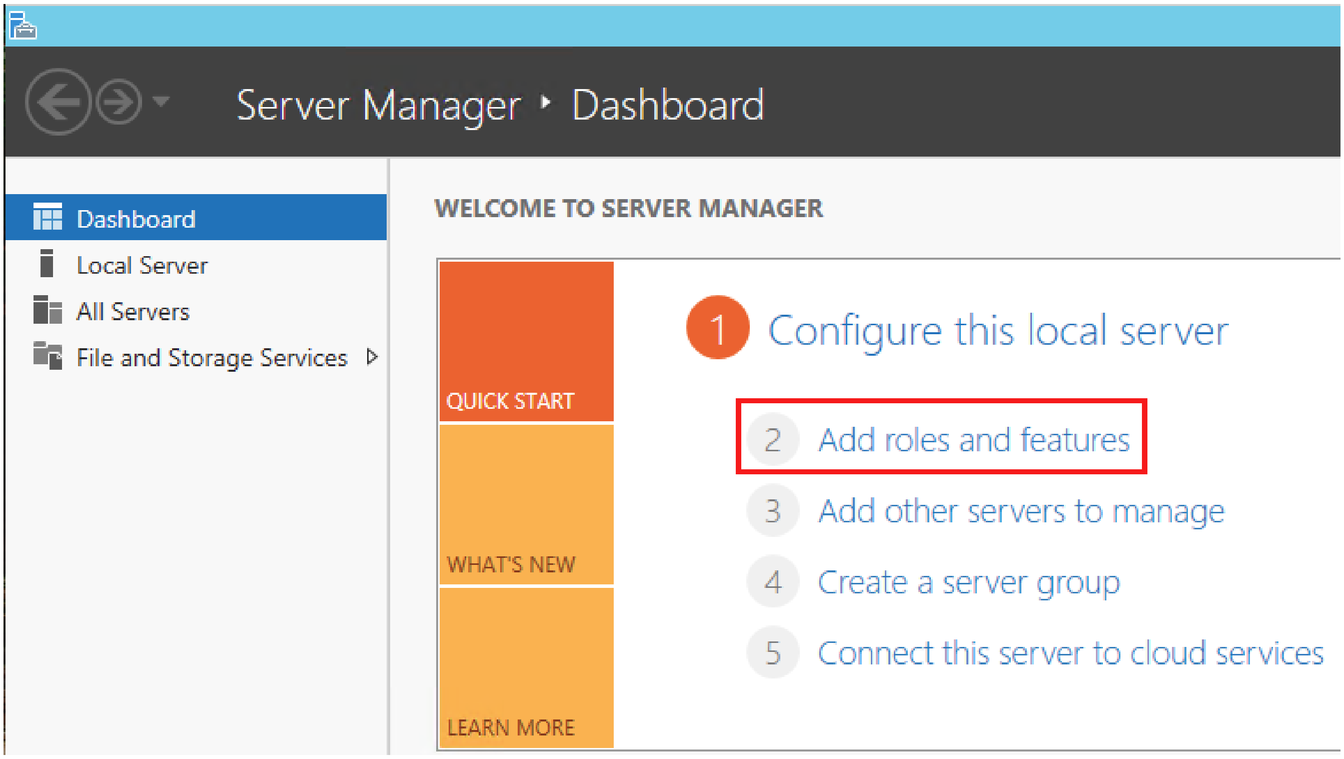
System

Processor:	Intel(R) Xeon(R) CPU E5-2686 v4 @ 2.30GHz 2.30 GHz
Installed memory (RAM):	4.00 GB
System type:	64-bit Operating System, x64-based processor
Pen and Touch:	No Pen or Touch Input is available for this Display

Computer name, domain, and workgroup settings

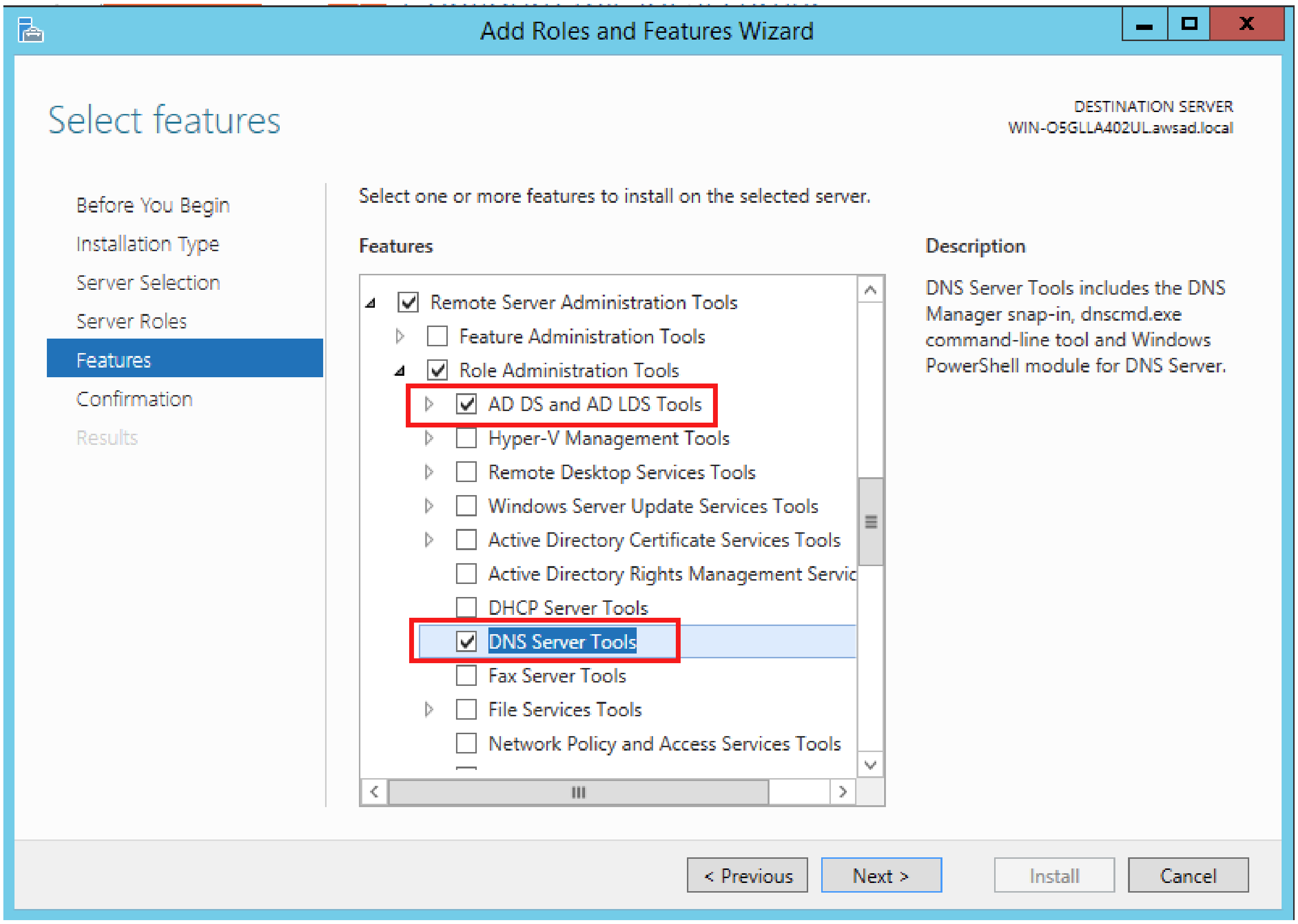
Computer name:	EC2AMAZ-MBN5S5D
Full computer name:	EC2AMAZ-MBN5S5D.awsad.com
Computer description:	
Domain:	awsad.com

7. Go to the Windows icon in the lower left corner, type "**Server Manager**" to open the **"Server Manager Dashboard"**. Click **"Add roles and features"**.



Server Manager ▸ Dashboard
Dashboard
Local Server
All Servers
File and Storage Services
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services

8. Click **"Next"** (4 times) till you get to the Features screen. Select the "**Remote Server Administration Tools"**. In the Role Administration Tools, also select "**DNS Server Tools"**. Click **"Next"** a couple times, and click **"Install"** to start the install.



Select features

DESTINATION SERVER
WIN-O5GLLA402UL.awsad.local

Select one or more features to install on the selected server.

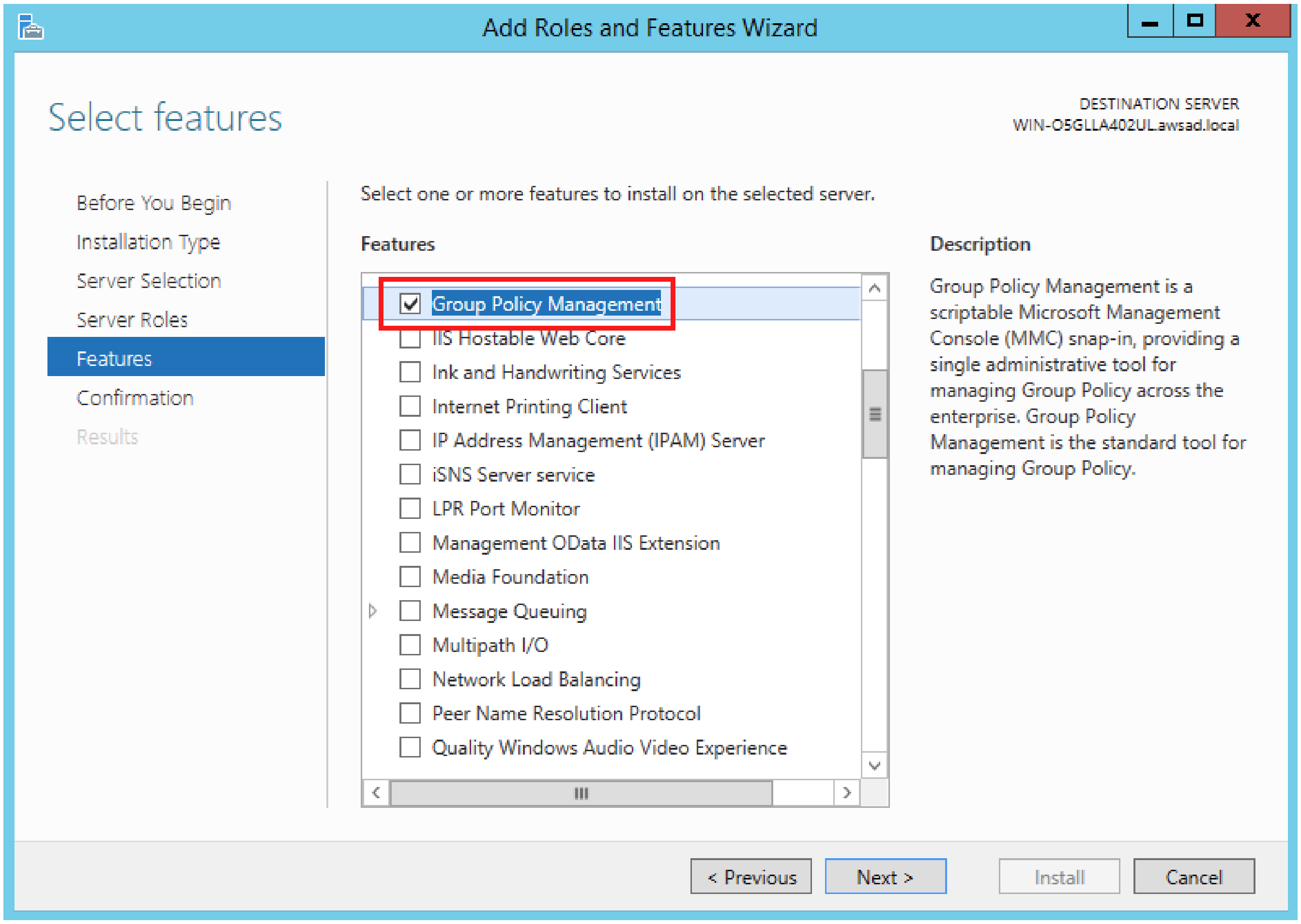
Features

- ☑ Remote Server Administration Tools
  - □ Feature Administration Tools
  - ☑ Role Administration Tools
    - ☑ AD DS and AD LDS Tools
    - □ Hyper-V Management Tools
    - □ Remote Desktop Services Tools
    - □ Windows Server Update Services Tools
    - □ Active Directory Certificate Services Tools
    - □ Active Directory Rights Management Servic
    - □ DHCP Server Tools
    - ☑ DNS Server Tools
    - □ Fax Server Tools
    - □ File Services Tools
    - □ Network Policy and Access Services Tools

Description

DNS Server Tools includes the DNS Manager snap-in, dnscmd.exe command-line tool and Windows PowerShell module for DNS Server.

9. Once you finish installing the AD and DNS tools, follow the same process to install the **Group Policy Management** tool as shown.



Add Roles and Features Wizard

Select features

DESTINATION SERVER
WIN-O5GLLA402UL.awsad.local

Select one or more features to install on the selected server.

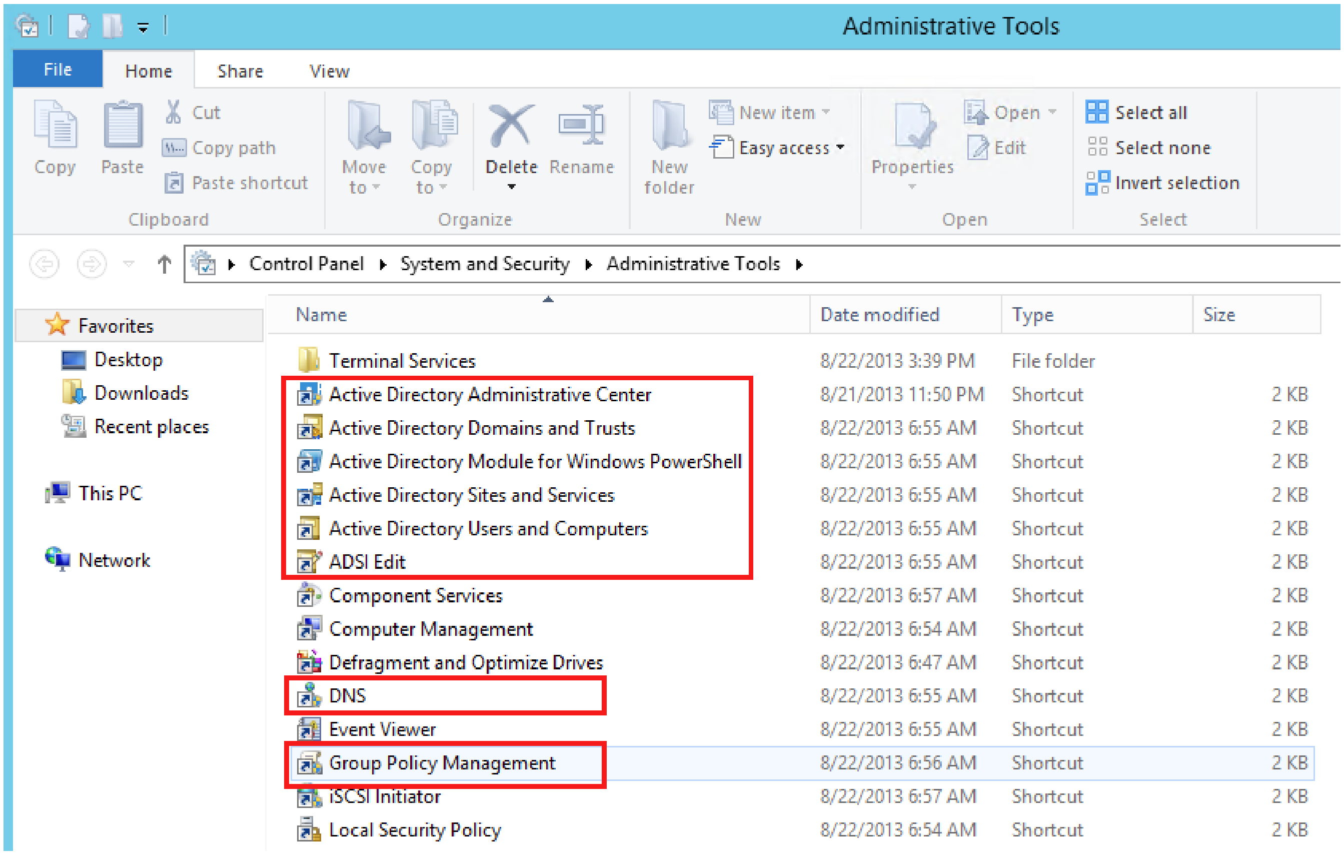
Features

- ☑ Group Policy Management
- □ IIS Hostable Web Core
- □ Ink and Handwriting Services
- □ Internet Printing Client
- □ IP Address Management (IPAM) Server
- □ iSNS Server service
- □ LPR Port Monitor
- □ Management OData IIS Extension
- □ Media Foundation
- □ Message Queuing
- □ Multipath I/O
- □ Network Load Balancing
- □ Peer Name Resolution Protocol
- □ Quality Windows Audio Video Experience

Description

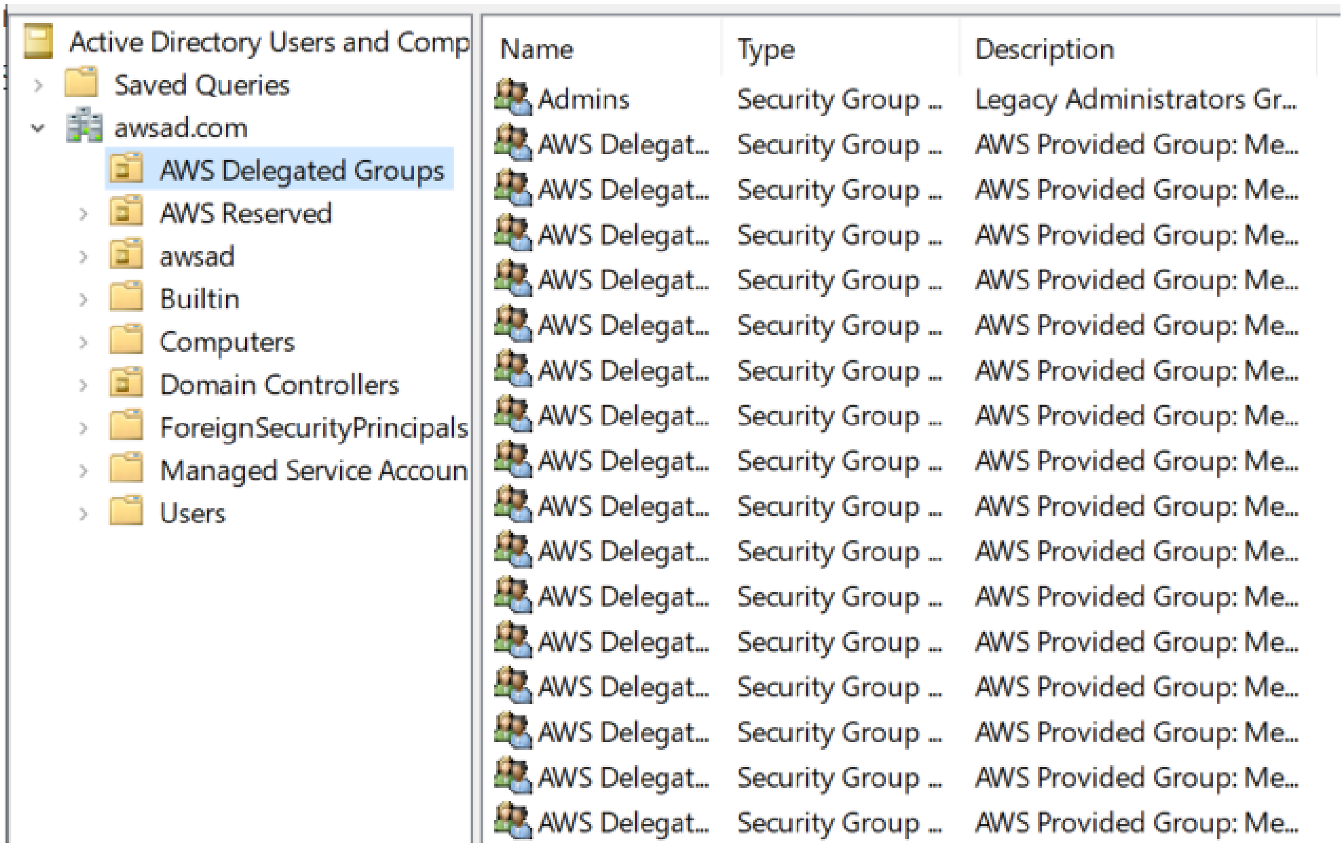
Group Policy Management is a scriptable Microsoft Management Console (MMC) snap-in, providing a single administrative tool for managing Group Policy across the enterprise. Group Policy Management is the standard tool for managing Group Policy.

10. Once the installation is completed, you can close the Server Manager. The Active Directory tools can be found under **Control Panel -> System and Security -> Administrative Tools** as follows. You can open any of these Active Directory tools and start administering your AWS Managed AD. Windows uses the logged on user to determine the permissions for running these tools. If you want to use a different user, either use “runas” or login to the server with different credentials



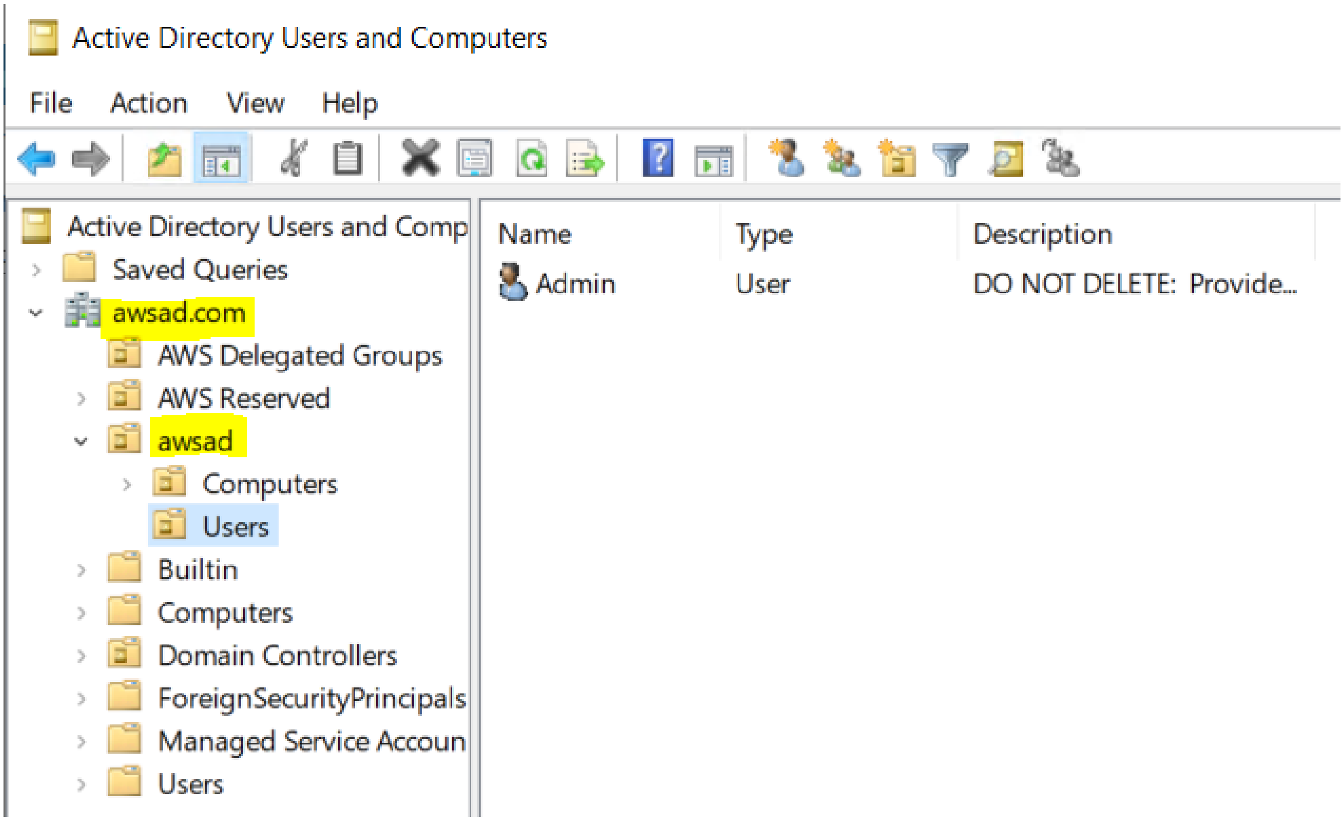
Name	Date modified	Type	Size
Terminal Services	8/22/2013 3:39 PM	File folder	
Active Directory Administrative Center	8/21/2013 11:50 PM	Shortcut	2 KB
Active Directory Domains and Trusts	8/22/2013 6:55 AM	Shortcut	2 KB
Active Directory Module for Windows PowerShell	8/22/2013 6:55 AM	Shortcut	2 KB
Active Directory Sites and Services	8/22/2013 6:55 AM	Shortcut	2 KB
Active Directory Users and Computers	8/22/2013 6:55 AM	Shortcut	2 KB
ADSI Edit	8/22/2013 6:55 AM	Shortcut	2 KB
Component Services	8/22/2013 6:57 AM	Shortcut	2 KB
Computer Management	8/22/2013 6:54 AM	Shortcut	2 KB
Defragment and Optimize Drives	8/22/2013 6:47 AM	Shortcut	2 KB
DNS	8/22/2013 6:55 AM	Shortcut	2 KB
Event Viewer	8/22/2013 6:55 AM	Shortcut	2 KB
Group Policy Management	8/22/2013 6:56 AM	Shortcut	2 KB
iSCSI Initiator	8/22/2013 6:57 AM	Shortcut	2 KB
Local Security Policy	8/22/2013 6:54 AM	Shortcut	2 KB

11. Open the **Active Directory Users and Computers** tool. Note the domain name for the AD forest. Also note that there is an OU called **AWS Delegated Groups**. When you use AWS Managed Microsoft Active Directory, the admin account that you are given is not an AD domain administrator. AWS creates a set of AD groups that have been delegated administrative rights to perform certain tasks. These groups are listed in this OU.



Name	Type	Description
Admins	Security Group ...	Legacy Administrators Gr...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...
AWS Delegat...	Security Group ...	AWS Provided Group: Me...

12. Also note that there is an OU with the same name as the NetBIOS name of the AD forest (e.g. awsad). Go to this OU and explore its contents. This OU is where you can create your users and create additional sub-OU’s.



Name	Type	Description
Admin	User	DO NOT DELETE: Provide...

Congratulations!

You have successfully launched a management server that you can use to administer your AWS Managed Microsoft AD. For high availability purposes, you can launch multiple management servers in different availability zones as required. If you are done with the lab, you can cleanup all the resources that you deployed in this lab to stop accruing AWS charges.