

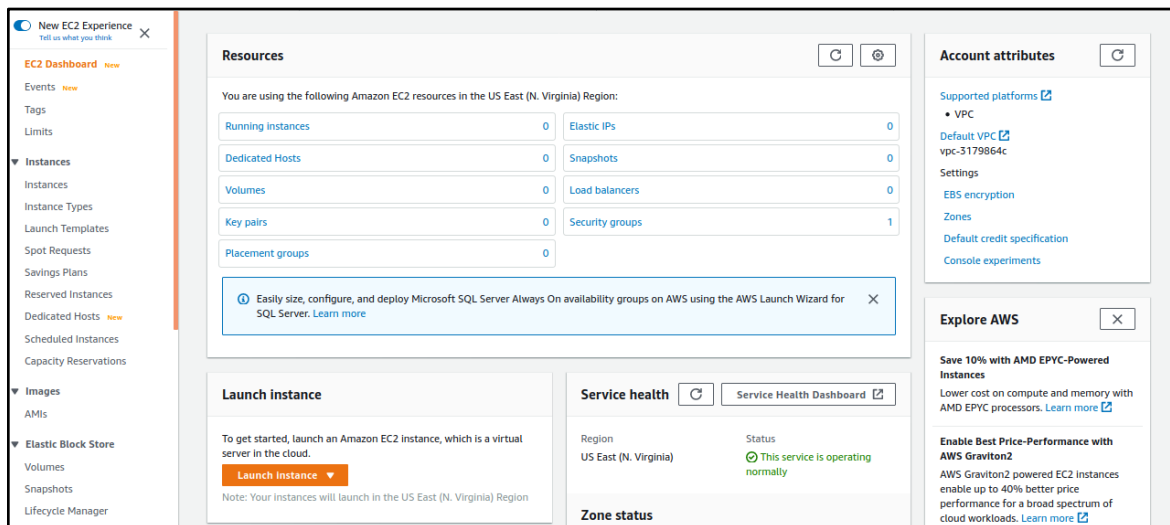
Course-End Project: Setting up a Website on Cloud

This section will guide you to:

1. Create an EC2 instance
2. Install a web server (IIS) role
3. Create a static website and check on a localhost
4. Create an image of the machine and save the AMI
5. Create a new instance using the AMI you have saved
6. Create a Load Balancer and attach the instances mentioned above
7. Check the DNS name on the browser

Step 1: Create an EC2 instance

- On the **Services** menu, click on **EC2**
- On the EC2 dashboard, click on **Launch Instance**



- Under **Amazon Machine Image (AMI)** select the **Windows Server 2012 R2 Base** image

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 1: Choose an Amazon Machine Image (AMI)

Cancel and Exit

Windows Free tier eligible	Microsoft Windows Server 2016 with SQL Server 2019 Standard - ami-0c6b5ca726ff8c706 Microsoft Windows 2016 Datacenter edition, Microsoft SQL Server 2019 Standard. [English] Root device type: ebs Virtualization type: hvm EBS Enabled: Yes	Select 64-bit (x86)
Windows	Microsoft Windows Server 2016 with SQL Server 2019 Enterprise - ami-08615379f14965117 Microsoft Windows 2016 Datacenter edition, Microsoft SQL Server 2019 Enterprise. [English] Root device type: ebs Virtualization type: hvm EBS Enabled: Yes	Select 64-bit (x86)
Windows	Microsoft Windows Server 2012 R2 Base - ami-0a11ca1795668bd94 Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English] Root device type: ebs Virtualization type: hvm EBS Enabled: Yes	Select 64-bit (x86)
Windows Free tier eligible	Microsoft Windows Server 2012 R2 with SQL Server 2016 Standard - ami-08403a8aec8d3c5fb Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Standard edition. [English] Root device type: ebs Virtualization type: hvm EBS Enabled: Yes	Select 64-bit (x86)
Windows Free tier eligible	Microsoft Windows Server 2012 R2 with SQL Server 2016 Enterprise - ami-02926206ca981994e Microsoft Windows Server 2012 R2 Standard edition, 64-bit architecture, Microsoft SQL Server 2016 Enterprise edition. [English] Root device type: ebs Virtualization type: hvm EBS Enabled: Yes	Select 64-bit (x86)
Linux	Amazon Linux 2 LTS with SQL Server 2017 Standard - ami-087a6127ba9676bb6 Microsoft SQL Server 2017 Standard edition on Amazon Linux 2 LTS. The AMI also comes pre-installed with .NET Core 2.0 and PowerShell 6.0.	Select 64-bit (x86)

- Choose the instance type as **t2.micro**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: All instance types Current generation Show/Hide Columns

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GiB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t3a.nano	2	0.5	EBS only	Yes	Up to 5 Gigabit	Yes
<input type="checkbox"/>	General purpose	t3a.micro	2	1	EBS only	Yes	Up to 5 Gigabit	Yes

Cancel Previous **Review and Launch** Next: Configure Instance Details

- On the **Configure Instance Details** page, specify the following settings:
 - Network: **Default VPC**
 - Subnet: **No Preference**
 - Auto-assign public IP: **Enabled**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances [View Spot Instance Prices](#)

Network [Create new VPC](#)

Subnet [Create new subnet](#)

Auto-assign Public IP

Placement group ☐ Add instance to placement group

Capacity Reservation

Domain join directory [Create new directory](#)

IAM role [Create new IAM role](#)

Shutdown behavior

Stop - Hibernate behavior ☐ Enable hibernation as an additional stop behavior

Enable termination protection ☐ Protect against accidental termination

Monitoring ☐ Enable CloudWatch detailed monitoring

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

- Click on **Next: Add storage**
- Accept the default storage details and click on **Next: Tag Instance**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/sda1	snap-063df574a9934f5a0	30	General Purpose SSD (gp2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Tags](#)

- In the **Value** box, type EC2VM and click on **Next: Configure Security Group**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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)	Instances (i)	Volumes (i)
Name	EC2VM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

[Add another tag](#) (Up to 50 tags maximum)

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Configure Security Group](#)

- In this step, you will configure a security group that will allow you to access the EC2VM instance by using an RDP connection. On the **Configure Security Group** page, use the following values:
 - Assign a security group:** Click on **Create a new security group** option
 - Security group name:** **RDP Access**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

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:

Description:

Type (i)	Protocol (i)	Port Range (i)	Source (i)	Description (i)
RDP	TCP	3389	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning
Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Previous](#) [Review and Launch](#)

- Click on **Review and Launch**
- On the **Review Instance Launch** page, review the configuration of your instance and then click on **Launch**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

AMI Details

Microsoft Windows Server 2012 R2 Base - ami-0a11ca1795e68bd94
 Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
 Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1
 Description: launch-wizard-1 created 2020-09-13T21:03:23.895+05:30

Type	Protocol	Port Range	Source	Description
RDP	TCP	3389	0.0.0.0/0	

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

[Cancel](#) [Previous](#) [Launch](#)

- Under **Select an existing key pair or create a new key pair**, enter the name of the key pair, accept, and click on **Download Key Pair**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

AMI Details

Microsoft Windows Server 2012 R2 Base - ami-0a11ca1795e68bd94
 Microsoft Windows 2012 R2 Standard edition with 64-bit architecture. [English]
 Root Device Type: ebs Virtualization type: hvm

If you plan to use this AMI for an application that benefits from Microsoft License Mobility, fill out the [License Mobility Form](#). Don't show me this again

Instance Type [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)
t2.micro	Variable	1	1

Security Groups [Edit security groups](#)

Security group name: launch-wizard-1
 Description: launch-wizard-1 created 2020-09-13T21:03:23.895+05:30

Type	Protocol
RDP	TCP

Instance Details [Edit instance details](#)

Storage [Edit storage](#)

[Cancel](#) [Previous](#) [Launch](#)

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](#).

Create a new key pair

Key pair name:

[Download Key Pair](#)

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

- Once it's downloaded, click on **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](#).

Create a new key pair

Key pair name:

[Download Key Pair](#)

You have to download the **private key file** (*.pem file) before you can continue. **Store it in a secure and accessible location.** You will not be able to download the file again after it's created.

[Cancel](#) [Launch Instances](#)

- On the **Launch Status** page, click on **View Instances**

Launch Status

Your instances are now launching

The following instance launches have been initiated: i-0593373e6f088ca94 [View launch log](#)

Get notified of estimated charges

Create [billing alerts](#) to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click **View Instances** to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

▼ Here are some helpful resources to get you started

- [How to connect to your Windows instance](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: User Guide](#)
- [Amazon EC2: Microsoft Windows Guide](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

- [Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)
- [Create and attach additional EBS volumes](#) (Additional charges may apply)
- [Manage security groups](#)

View Instances

- Find the EC2 instance created successfully

New EC2 Experience

EC2 Dashboard

Events

Tags

Limits

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Scheduled Instances

Capacity Reservations

Images

AMIs

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Launch Instance

Connect

Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public IP	IPv6 IPs
EC2VM	i-0becdb6218a84c430	t2.micro	us-east-1d	running	Initializing	None	ec2-3-93-49-239.comp...	3.93.49.239	-

Instance: i-0becdb6218a84c430 (EC2VM)

Public DNS: ec2-3-93-49-239.compute-1.amazonaws.com

Description

Status Checks

Monitoring

Tags

Instance ID

Instance state

Instance type

Finding

Optimizer

Public DNS (IPv4)

IPv4 Public IP

IPv6 IPs

Elastic IPs

i-0becdb6218a84c430

running

t2.micro

You may not have permission to access AWS Compute Optimizer.

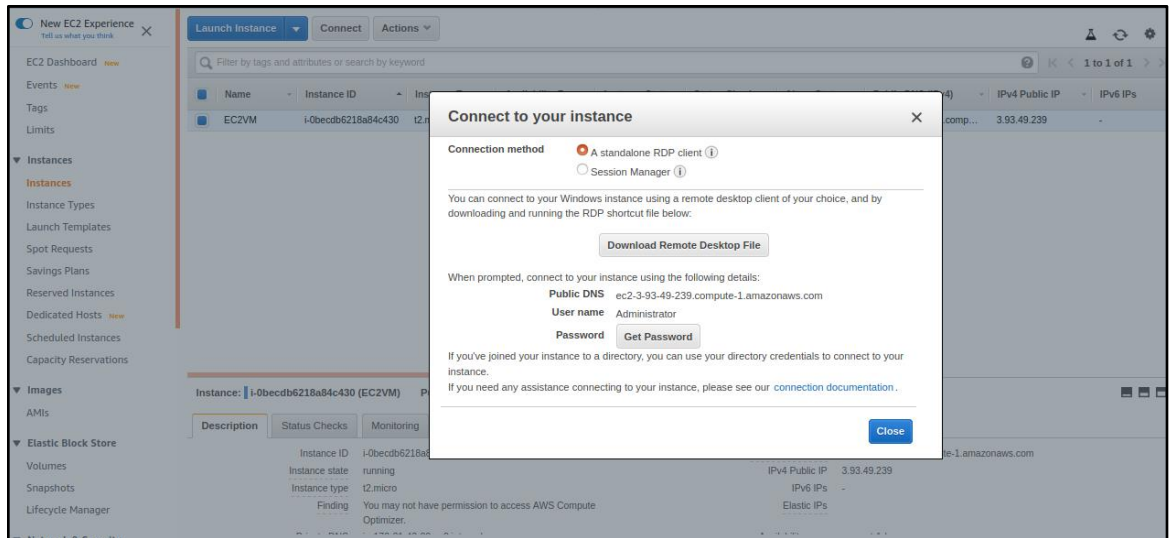
ec2-3-93-49-239.compute-1.amazonaws.com

3.93.49.239

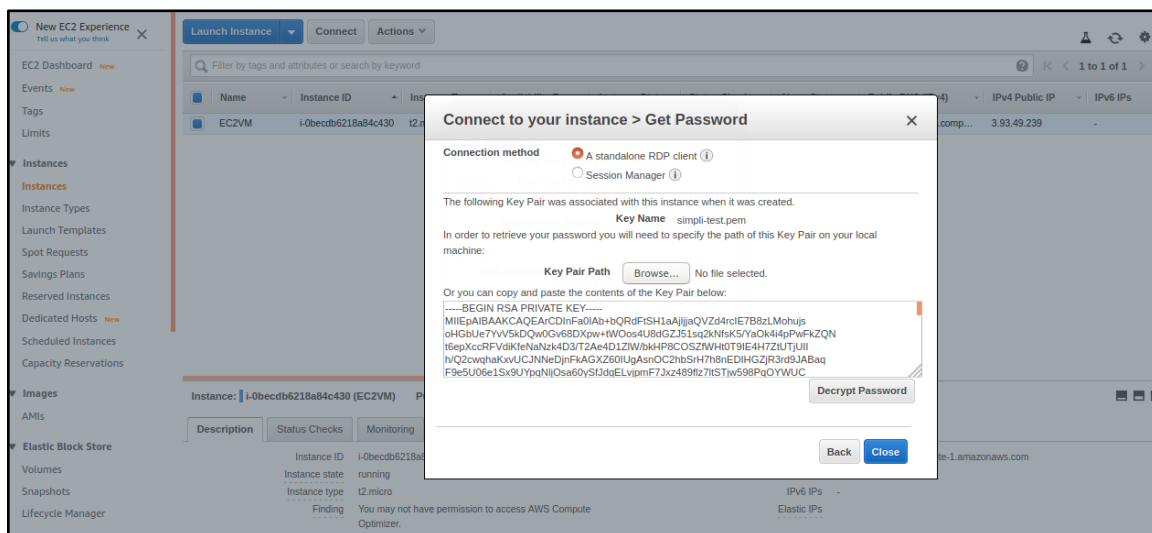
-

-

- Click on the **Connect** button, and a new window pops up for you to decrypt the password using the **pem** key downloaded
- Click on **Get password**

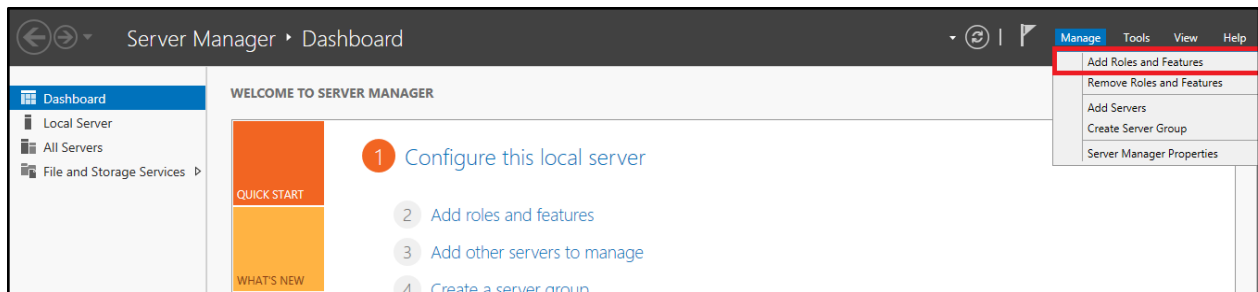


- Click on **Choose File** and select the file you have downloaded
- Click on **Decrypt Password** to get the system password
 - Please note the password file and download the remote desktop file to log in to the EC2 instance

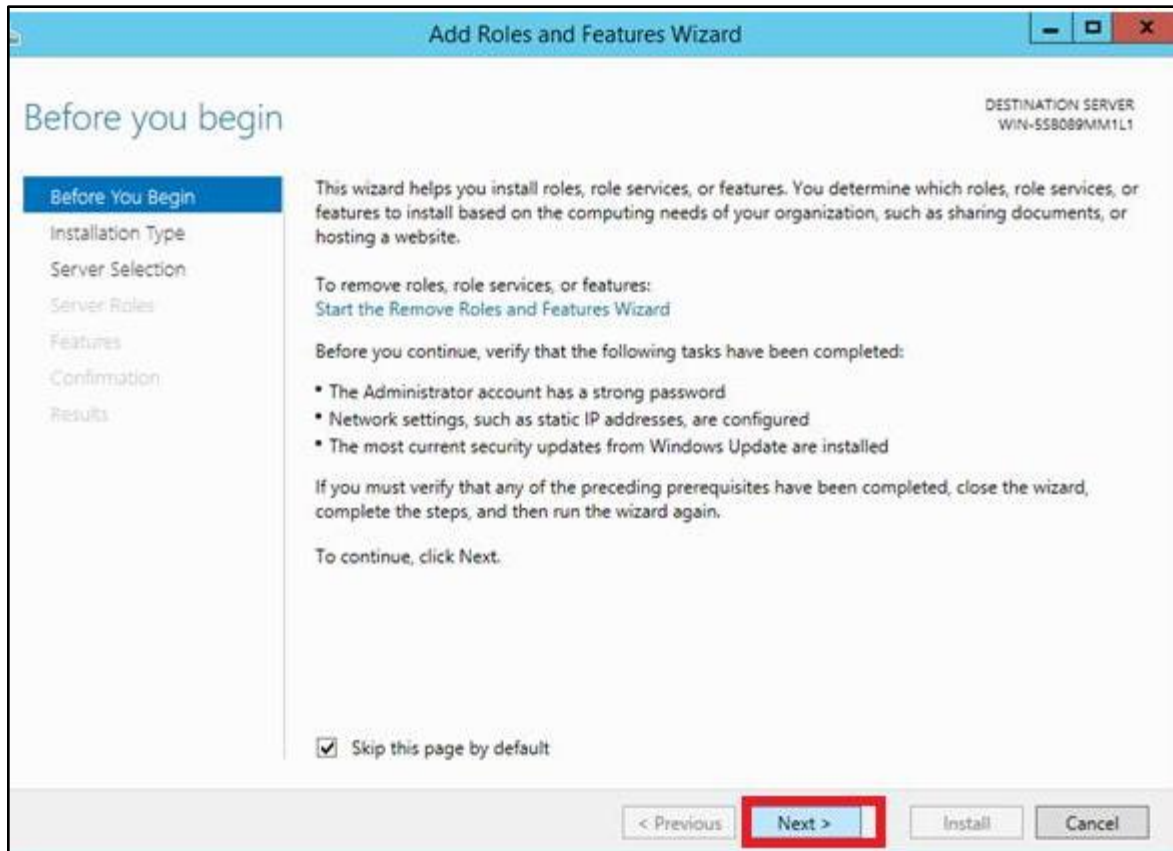


Step 2: Install a web server for IIS role

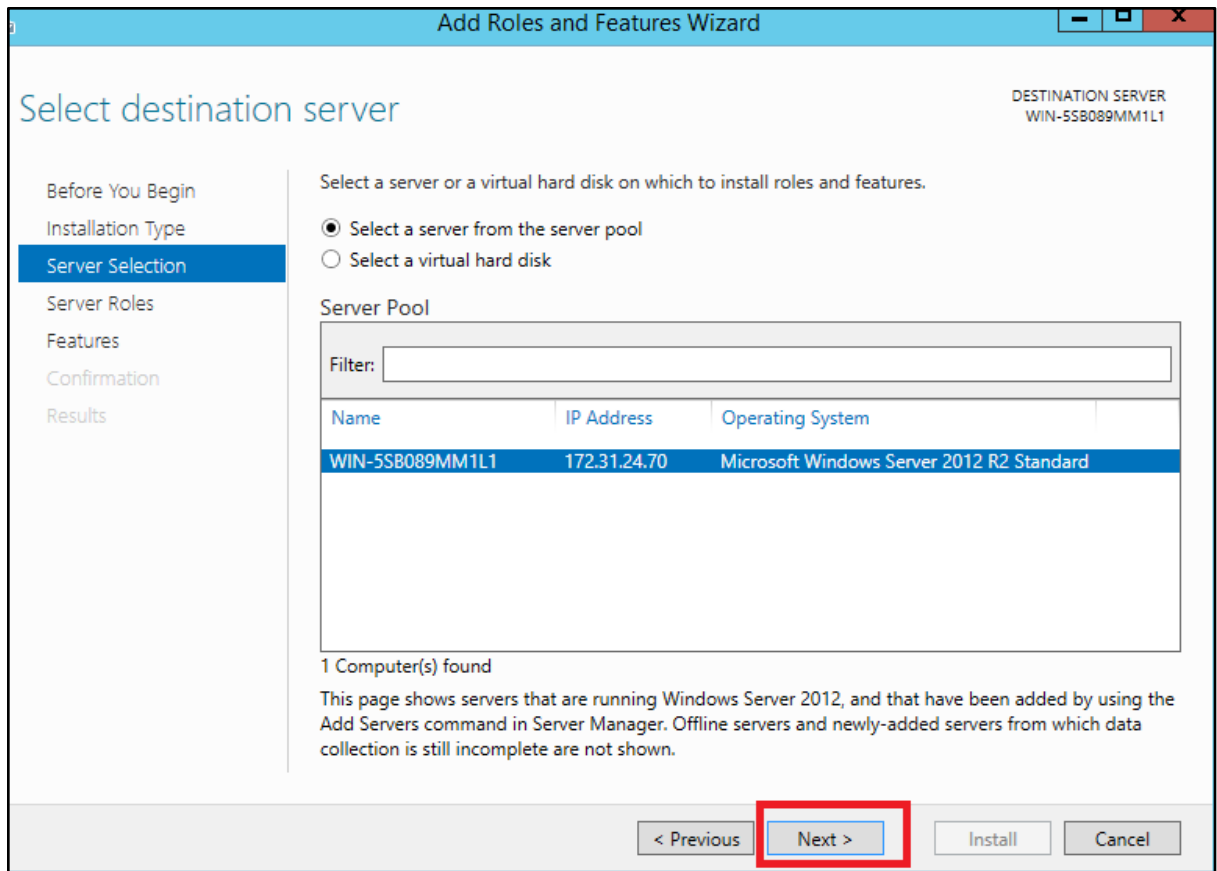
- After logging in to the instance, click on the **Server Manager** and then on **Manage**
- Select **Add Roles and Features**



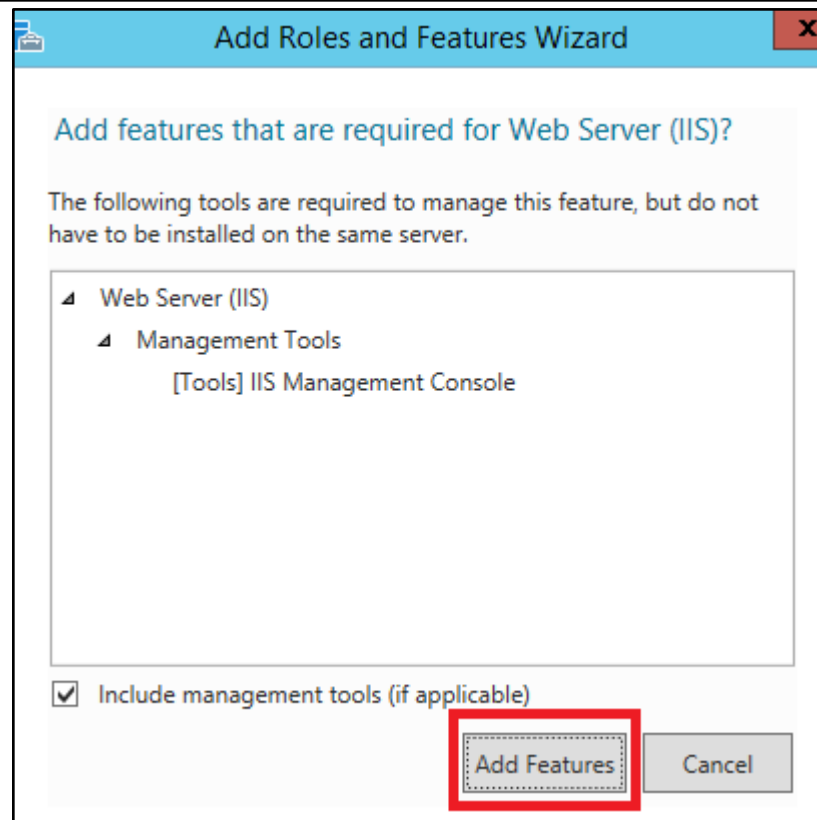
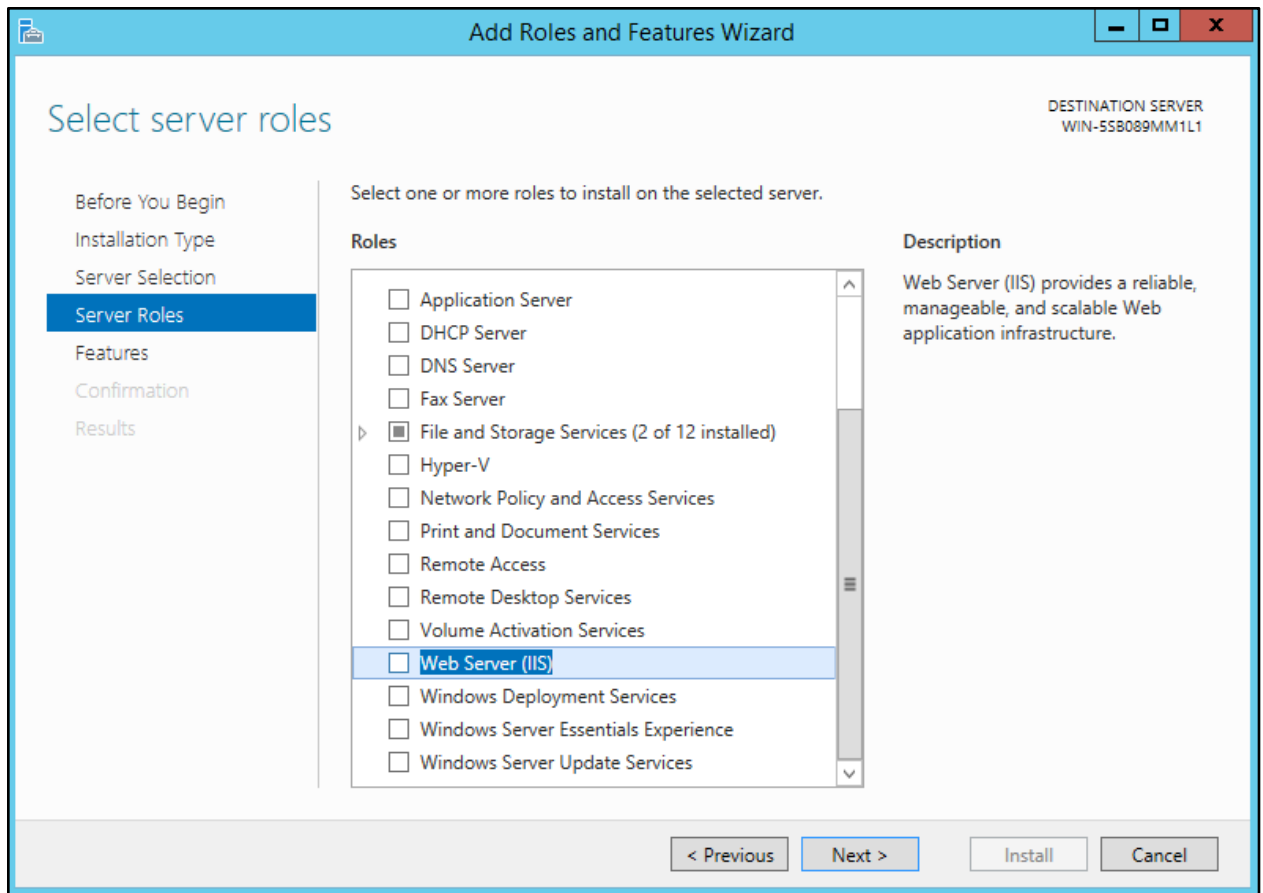
- In the **Before you begin** page, click on **Next**



- Click on **Next** on the **Select destination server** page



- On the **Select server roles** page, select **Web Server (IIS)**, and a window pops up showing the additional features required for the Web Server (IIS)
- Click on **Add Features** and then on **Next**



Add Roles and Features Wizard

DESTINATION SERVER
WIN-5SB089MM1L1

Select destination server

[Before You Begin](#)
[Installation Type](#)
[Server Selection](#)
[Server Roles](#)
[Features](#)
[Confirmation](#)
[Results](#)

Select a server or a virtual hard disk on which to install roles and features.

☒ Select a server from the server pool
☐ Select a virtual hard disk

Server Pool

Filter:

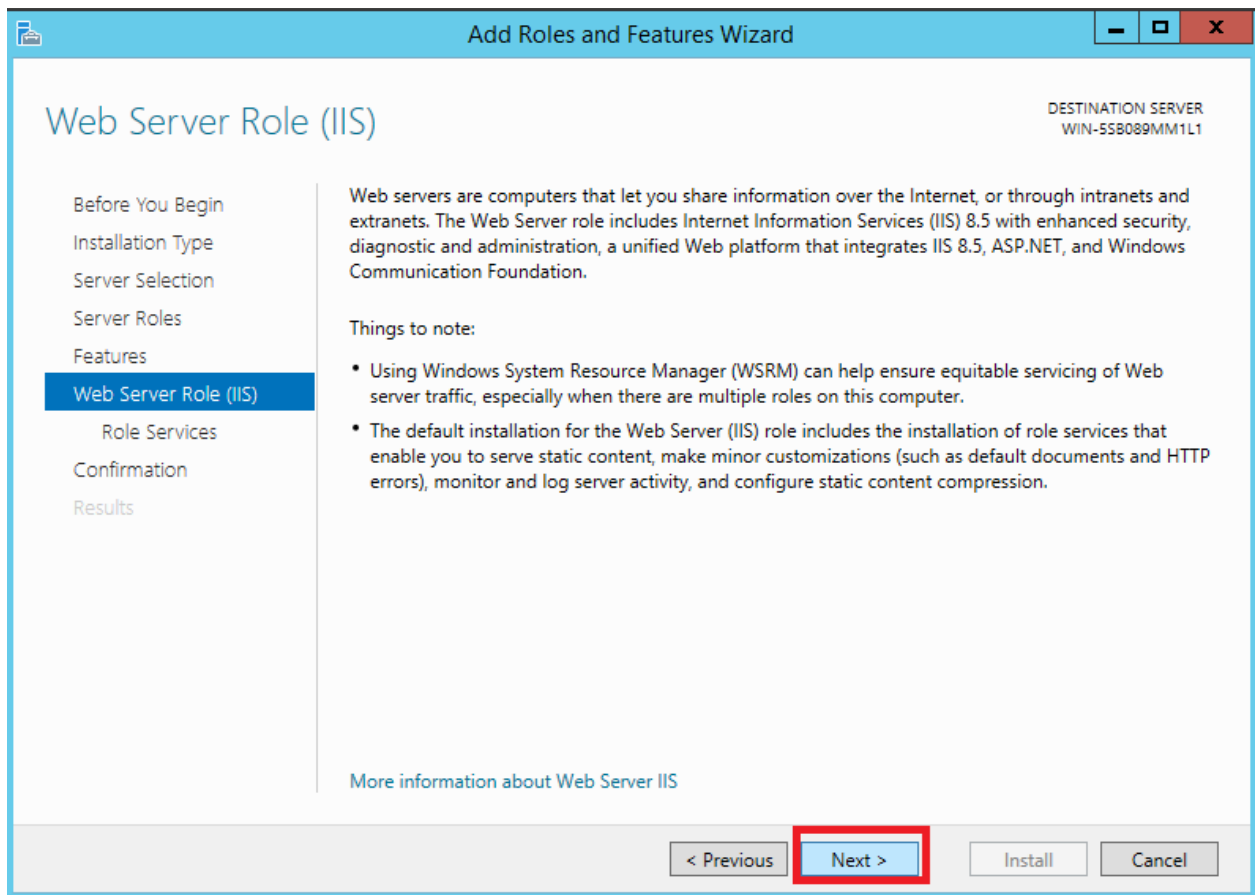
Name	IP Address	Operating System
WIN-5SB089MM1L1	172.31.24.70	Microsoft Windows Server 2012 R2 Standard

1 Computer(s) found

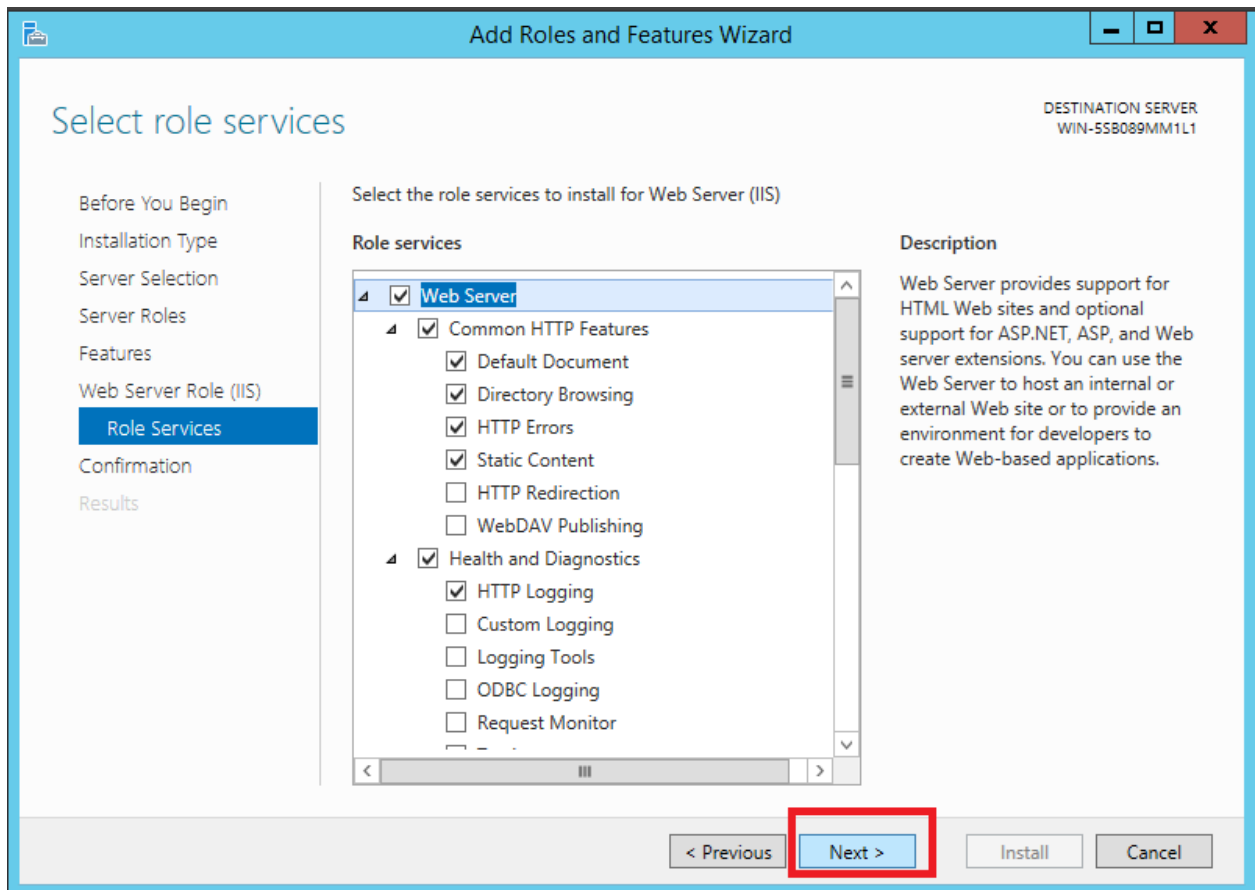
This page shows servers that are running Windows Server 2012, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

[< Previous](#) **[Next >](#)** [Install](#) [Cancel](#)

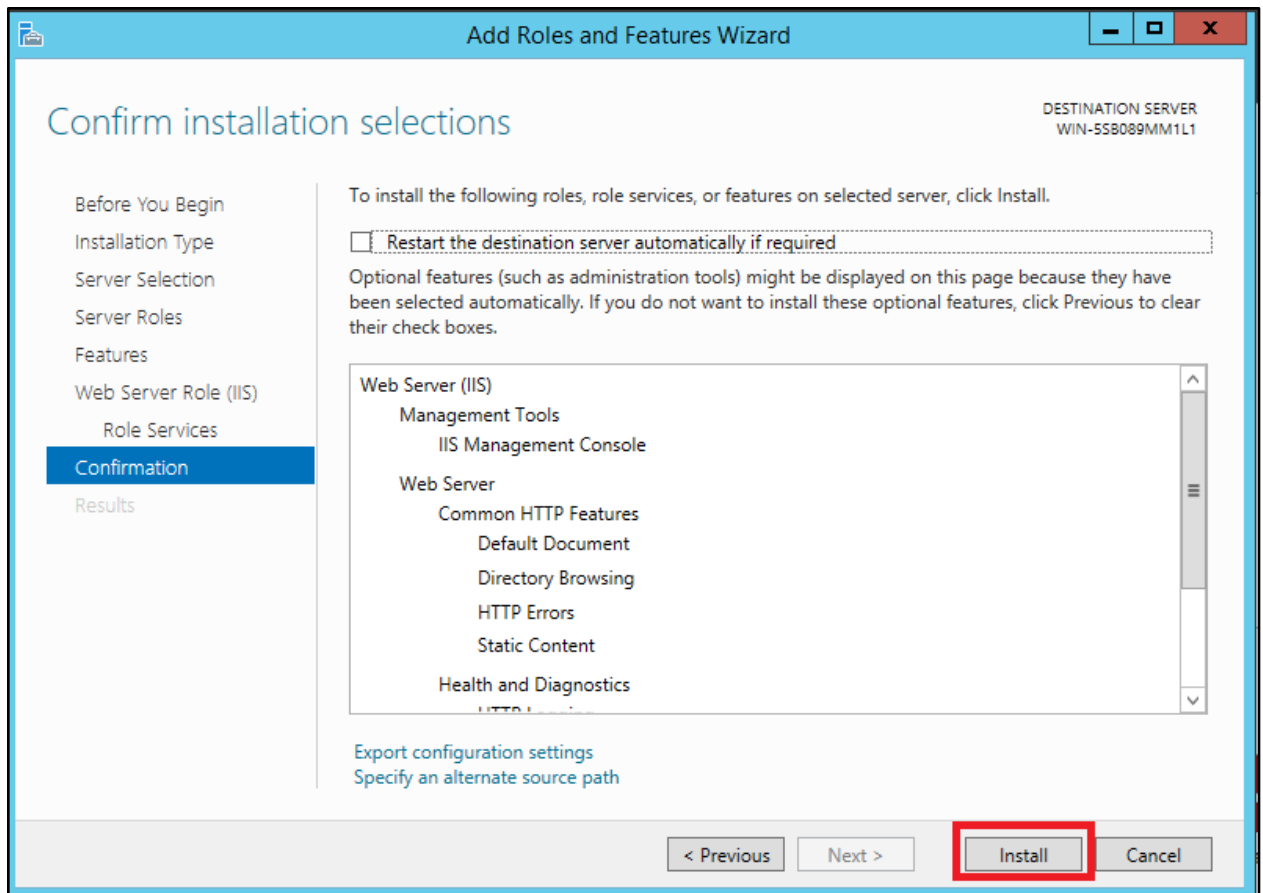
- On the **Web Server Role (IIS)** page, click on **Next**



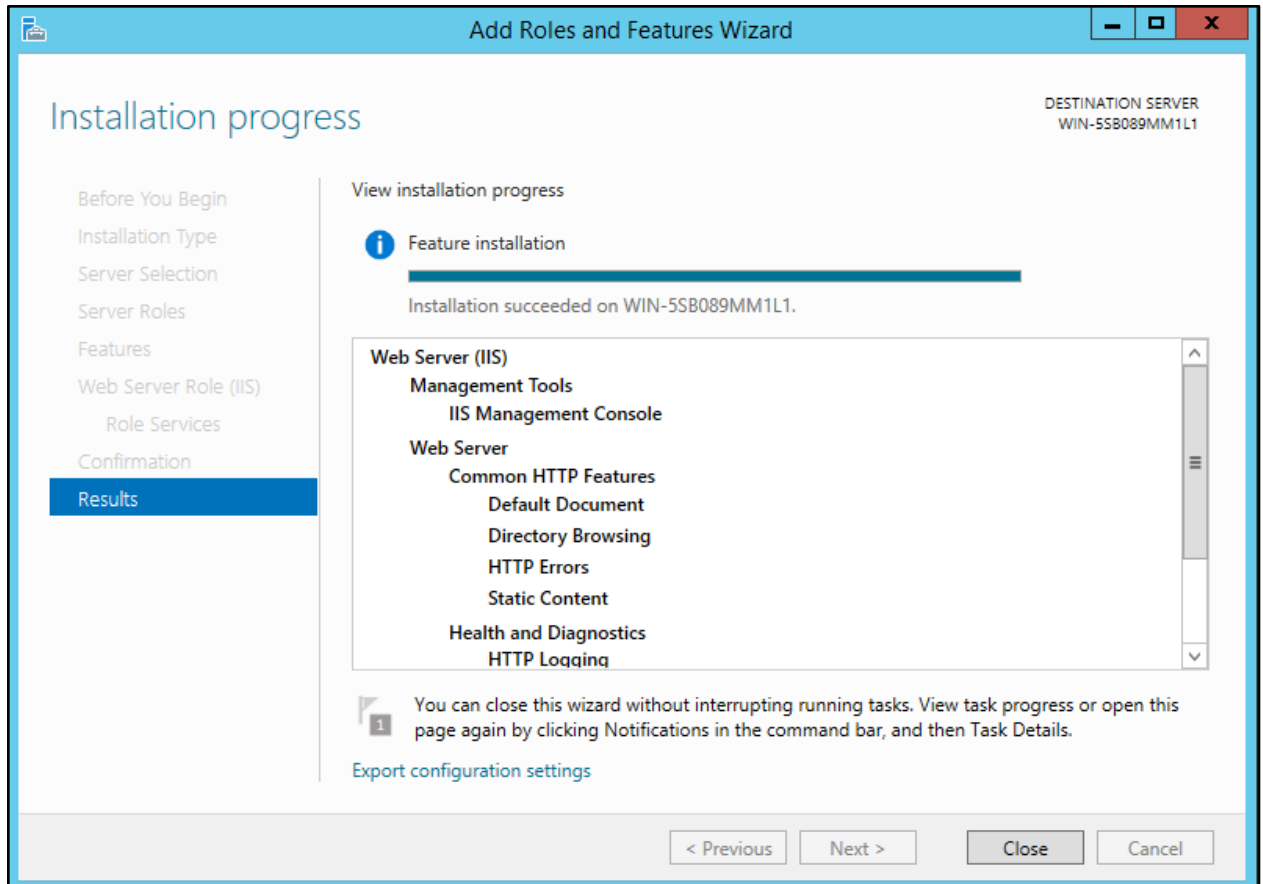
- In **Role services**, keep the default selection and click on **Next**



- On the **Confirm installation selections** page, click on **Install**

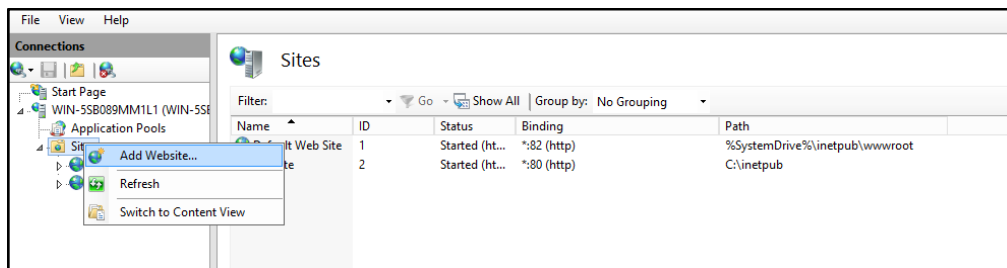


- After a couple of minutes, the IIS role will be installed successfully



Step 3: Create a static website and check on a localhost

- Add website using the screenshots given below:



Add Website

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Website immediately

Sites

Filter: Show All Group by: No Grouping

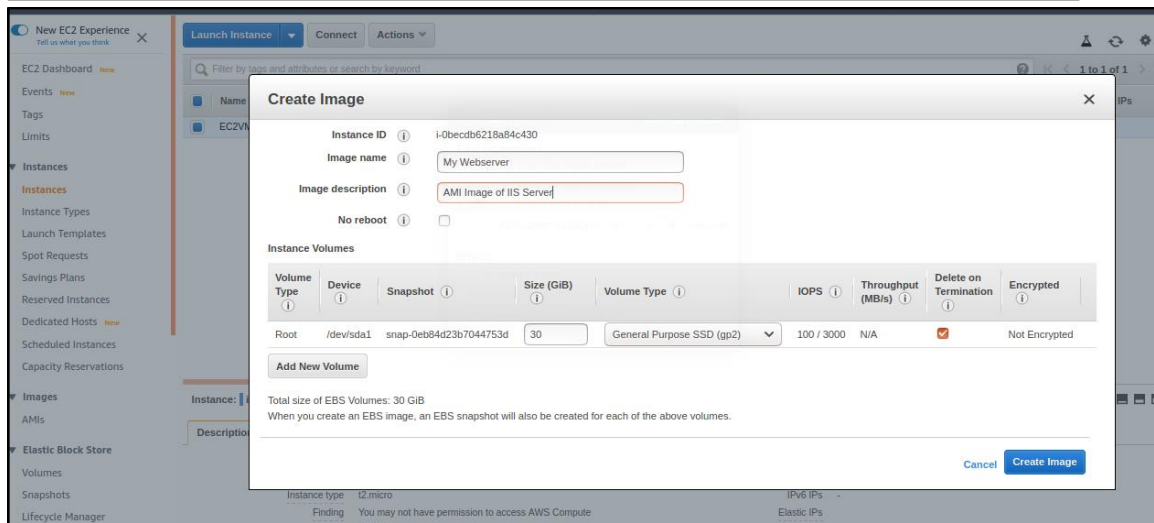
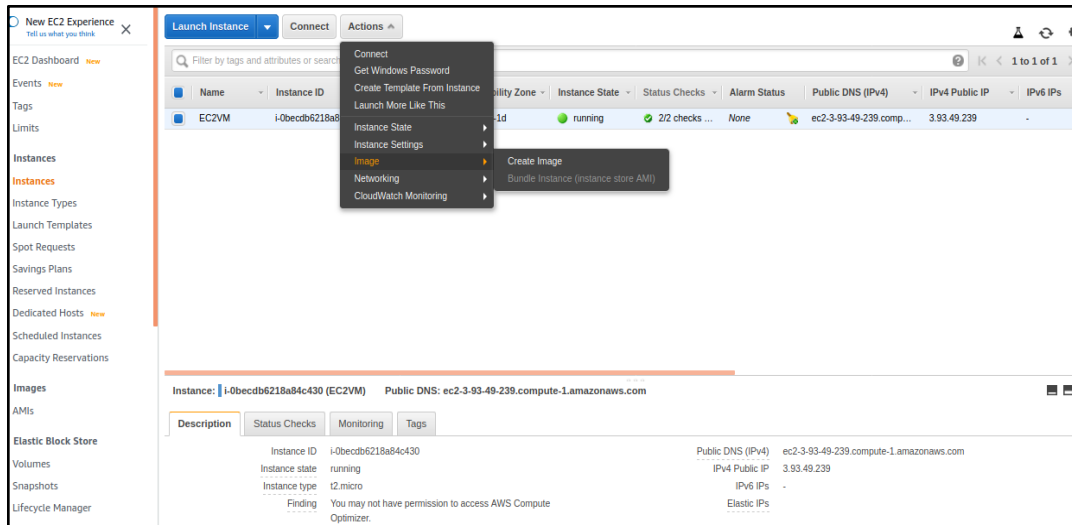
Name	ID	Status	Binding	Path
Default Web Site	1	Started (ht...	*:82 (http)	%SystemDrive%\inetpub\wwwroot
Website	2	Started (ht...	*:80 (http)	C:\inetpub

Actions

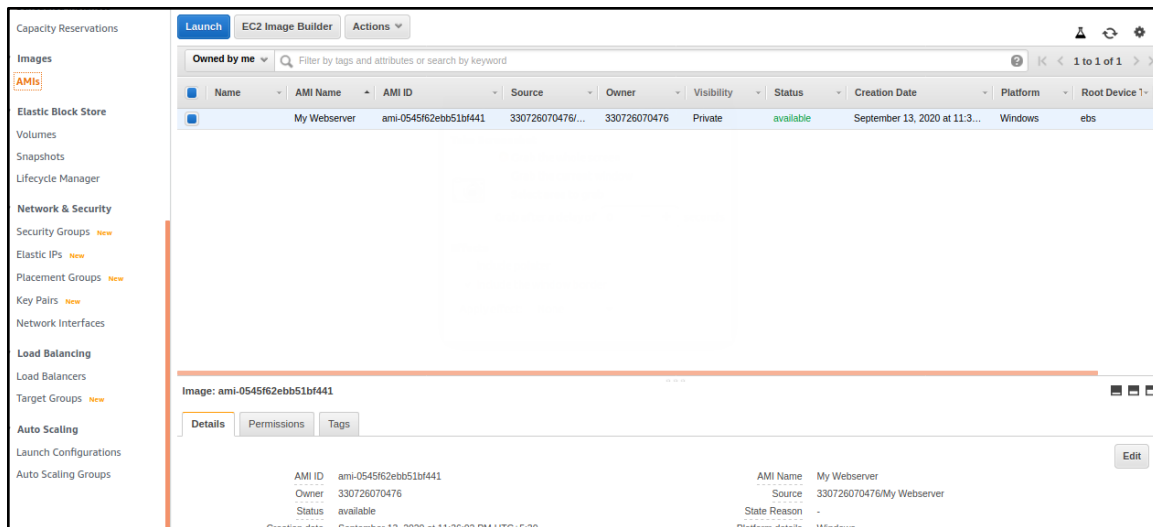
- Add Website...
- Set Website Defaults...
- Edit Site**
- Bindings...
- Basic Settings...
- Explore
- Edit Permissions...
- Remove
- Rename
- View Applications
- View Virtual Directories
- Manage Website**
- Restart
- Start
- Stop
- Browse Website**
- Browse *:80 (http)
- Advanced Settings...
- Configure
- Limits...
- Help

Step 4: Create an image of the machine and save the AMI

- Go to EC2 instance and select the **instance**
- Go to the drop-down option named **Actions>Image>select Create Image**

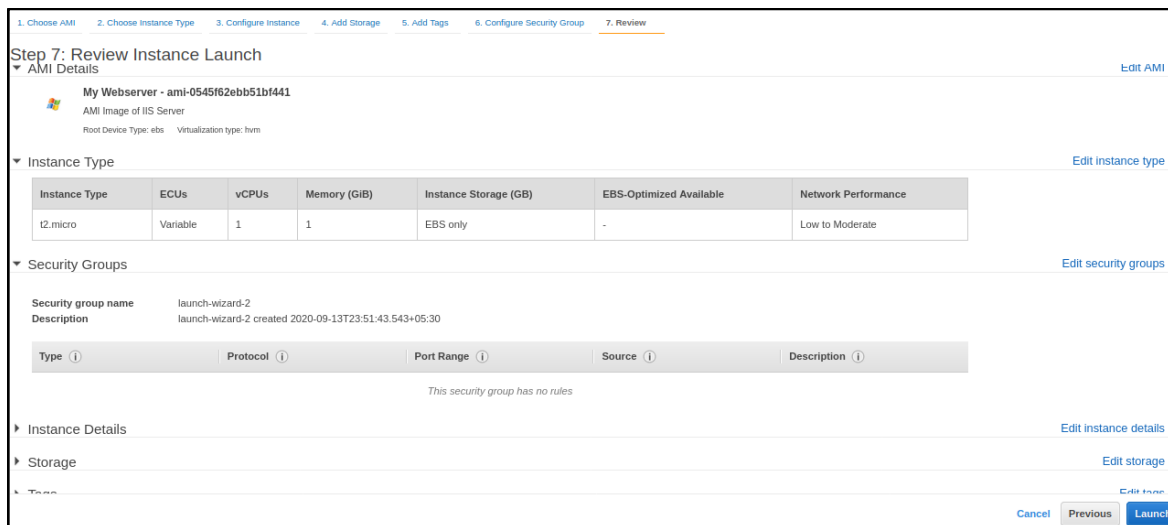


- Go to the new image and check its status
- See the new AMI under **Images/AMI**
 - Reuse this image whenever you want to provide a similar instance, which will save time while installing application binaries.
 - We can reuse such custom AMIs during auto-scaling and provisioning instances using Elastic Beanstalk.



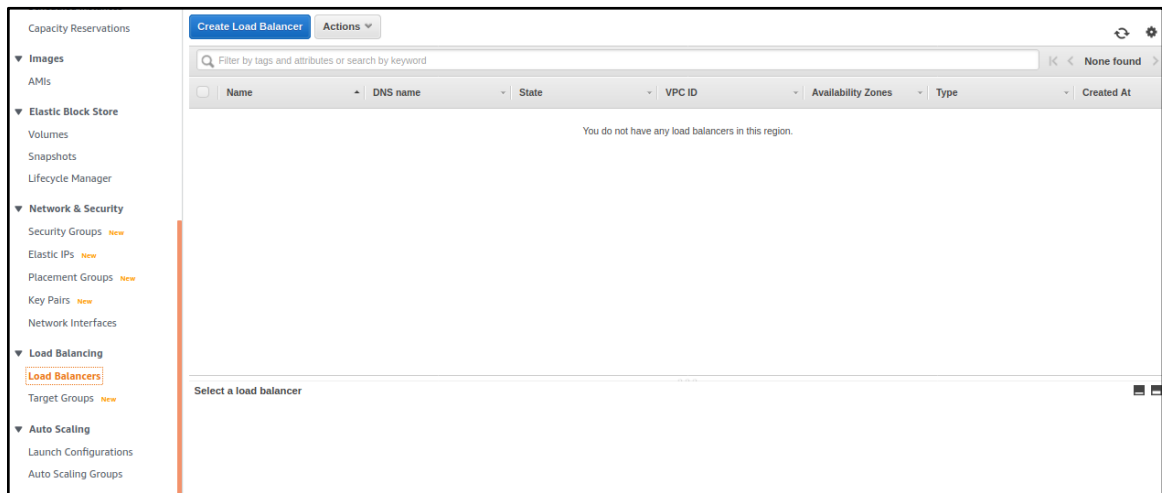
Step 5: Create a new instance using the AMI you have saved

- To launch the instance, select the AMI and click on **Launch**



Step 6: Create a Load Balancer and attach the instances mentioned above

- On the navigation pane, select a Load Balancer under **Load balancing**



- Type a name for your Load Balancer, and select **Next: Configure Security Settings**

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 1: Configure Load Balancer

Basic Configuration

To configure your load balancer, provide a name, select a scheme, specify one or more listeners, and select a network. The default configuration is an Internet-facing load balancer in the selected network with a listener that receives HTTP traffic on port 80.

Name ⓘ WebLoadBalancer

Scheme ⓘ ☒ Internet-facing
☐ Internal

IP address type ⓘ IPv4

Listeners

A listener is a process that checks for connection requests, using the protocol and port that you configured.

Load Balancer Protocol	Load Balancer Port
HTTP	80

[Add listener](#)

Availability Zones

Specify the Availability Zones to enable for your load balancer. The load balancer routes traffic to the targets in these Availability Zones only. You can specify only one subnet per Availability Zone. You must specify subnets from at least two Availability Zones to increase the availability of your load balancer.

[Cancel](#) [Next: Configure Security Settings](#)

- Create a new security group to allow RDP access and select **Next: Configure Routing**

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 3: Configure Security Groups

A security group is a set of firewall rules that control the traffic to your load balancer. On this page, you can add rules to allow specific traffic to reach your load balancer. First, decide whether to create a new security group or select an existing one.

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

Security group name:

Description:

Type	Protocol	Port Range	Source
RDP	TCP	3389	Custom 0.0.0.0/0:::0

Add Rule

Cancel Previous Next: Configure Routing

- Keep the default security settings

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 4: Configure Routing

☐ Lambda function

Protocol:

Port:

Health checks

Protocol:

Path:

Advanced health check settings

Port: ☒ traffic port
☐ override

Healthy threshold:

Unhealthy threshold:

Timeout: seconds

Interval: seconds

Success codes:

Cancel Previous Next: Register Targets

- Review the configuration and select **Create**
 - ELB is created successfully
 - Check the ELB settings and status of the instance

1. Configure Load Balancer 2. Configure Security Settings 3. Configure Security Groups 4. Configure Routing 5. Register Targets 6. Review

Step 6: Review

Please review the load balancer details before continuing

▼ Load balancer

Name WebLoadBalancer

Scheme internet-facing

Listeners Port:80 - Protocol:HTTP

IP address type ipv4

VPC vpc-3179864c

Subnets subnet-ec49ea8a, subnet-8ea108af

Tags

▼ Security groups

Security groups RDP Access

▼ Routing

Target group New target group

Target group name WEB

Port 80

Target type instance

Protocol HTTP

Health check protocol HTTP

Path /

Health check port traffic port

Healthy threshold 5

Unhealthy threshold 2

Timeout 5

Cancel Previous Create

Load Balancer Creation Status

✓ **Successfully created load balancer**

Load balancer **WebLoadBalancer** was successfully created.

Note: It might take a few minutes for your load balancer to be fully set up and ready to route traffic, and for the targets to complete the registration process and pass the initial health checks.

Suggested next steps

- Discover other services that you can integrate with your load balancer. Visit the [Integrated services](#) tab within **WebLoadBalancer**.
- Consider using AWS Global Accelerator to further improve the availability and performance of your applications. [AWS Global Accelerator console](#)

Close

Limits

INSTANCES

Instances

Spot Requests

Reserved Instances

Dedicated Hosts

IMAGES

AMIs

Bundle Tasks

ELASTIC BLOCK STORE

Volumes

Snapshots

NETWORK & SECURITY

Security Groups

Elastic IPs

Placement Groups

Key Pairs

Network Interfaces

Create Load Balancer Actions

Filter: Search Load Balancers

Load Balancer Name	DNS name	Port Configuration	Availability Zones	Instance Count	Health Check
webserverloadbalancer	webserverloadbalancer-20112...	80 (HTTP) forwarding to 80 (...)	ap-south-1b, ap-south-1a	2 Instances	HTTP: 80/
WebLoadbalancer	WebLoadbalancer-120404246...	80 (HTTP) forwarding to 80 (...)	ap-south-1b, ap-south-1a	2 Instances	HTTP: 80/index.html

Edit Instances

Instance ID	Name	Availability Zone	Status	Actions
i-0a96c5391ee7d902d	EC2VM1	ap-south-1a	InService	Remove from Load Balancer
i-0511ff929290c2fbf	EC2VM	ap-south-1a	InService	Remove from Load Balancer

Step 7: Check the DNS name on the browser

- Copy the DNS Name in the address bar of your browser

Create Load Balancer

Actions

Filter: Search

<input type="checkbox"/>	Name	DNS name	State	VPC ID
<input type="checkbox"/>	WebLoadbalancer	WebLoadbalancer-2097435...		vpc-dc9250b5
<input checked="" type="checkbox"/>	WebLoadBalancerVM	WebLoadBalancerVM-16753...		vpc-dc9250b5

Basic Configuration

Name:

WebLoadBalancerVM

* DNS name:

WebLoadBalancerVM-1675300082.ap-south-1.elb.amazonaws.com (A Record)

Scheme:

Internet-facing

webloadbalancervm-1675300082.ap-south-1.elb.amazonaws.com

