

EC2 Instances

As a Cloud Architect and Consultant for Advanced Accounting LLC., I have been discussing steps for migrating to the cloud with owner Jessica Smith. We have decided on a measured, methodical migration process. While the company is eager to begin using and learning about their cloud infrastructure, we have chosen to start with spinning up Compute instances for each employee to use. Although it is a simple start to establishing a cloud infrastructure, it allows us to set proper inbound and outbound rules for security groups, and set network access controls for a solid security framework.

Although this is a project with real world scenarios and use cases, I still need to use the free tier to demonstrate the project. Because the employees are familiar with Microsoft Windows, we chose Windows Server 2022, as our machine image which is the underlying operating system used on the Compute instance to run any programs.

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Q Search our full catalog including 1000s of application and OS images

AMI from catalog

Recents

Quick Start

Name

Microsoft Windows Server 2022 Base

Description

Microsoft Windows 2022 Datacenter edition.
[English]

Image ID

ami-07cc1bbe145f35b58

Catalog

Published

Architecture

Virtualization

Root device type

ENA Enabled

Quick Start AMIs

2024-08-14T05:45:31.00

x86_64

hvm

ebs

Yes

Verified provider

Free tier eligible

Q

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

When adding new instances a key pair must be created or an existing key pair may be used. While I did create a key pair, for security reasons the actual key pair is not displayed in the screenshot.

▼ Key pair (login) Info

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

Select ▼

Create new key pair

For Windows instances, you use a key pair to decrypt the administrator password. You then use the decrypted password to connect to your instance.

In order to minimize the attack surface of our EC2 instances and help protect against threats like ransomware, we have established inbound rules using AWS security groups to restrict traffic only to RDP and SSH traffic from the local IP addresses. Because the security groups are stateful all other inbound traffic is denied by default. It is also possible to disable SSH and RDP completely and use the Session Manager for instance management.

Type Info	Protocol Info	Port range Info
rdp ▼	TCP	3389
Source type Info	Name Info	Description - optional Info
My IP ▼	<input type="text" value="Add CIDR, prefix list or security"/>	RDP Access

Type Info	Protocol Info	Port range Info
ssh ▼	TCP	22
Source type Info	Name Info	Description - optional Info
My IP ▼	<input type="text" value="Add CIDR, prefix list or security"/>	SSH Access

In order to further protect against attacks like ransomware, we will restrict our outbound traffic to necessary traffic on port 443 and disable the default outbound rule that allows all traffic. We will also employ Endpoint Protection to detect and prevent ransomware and will employ data loss protection to prevent data exfiltration. Finally,

we will use an AWS Web Application Firewall to protect against web exploits that could be used to inject ransomware.

Outbound rules [Info](#)

Security group rule ID	Type Info	Protocol Info	Port range Info	Destination Info	Description - optional Info
-	HTTPS ▼	TCP	443	Any... ▼ 0.0.0.0/0 ✕	<input type="text"/> <input type="button" value="Delete"/>

Now that our rules are set we can launch our instances!

▼ Summary

Number of instances [Info](#)

When launching more than 1 instance, [consider EC2 Auto Scaling](#)

Software Image (AMI)
Microsoft Windows Server 2022 ...[read more](#)
ami-07cc1bbe145f35b58

Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 30 GiB

Our instances are now up and running!

Instances (14) Info							
Last updated less than a minute ago			Refresh	Connect	Instance state	Actions	Launch instances
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>					All states	< 1 >	
<input type="checkbox"/>	Name ↗	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability
<input type="checkbox"/>	Microsoft Win...	i-0e548d388f45a2489	Running	t2.micro	Initializing	View alarms +	us-east-1b
<input type="checkbox"/>	Microsoft Win...	i-0484bc4636fb7dfe1	Running	t2.micro	Initializing	View alarms +	us-east-1b
<input type="checkbox"/>	Microsoft Win...	i-0ef41b63baf203c3c	Running	t2.micro	Initializing	View alarms +	us-east-1b
<input type="checkbox"/>	Microsoft Win...	i-06056fcc40952d371	Running	t2.micro	Initializing	View alarms +	us-east-1b
<input type="checkbox"/>	Microsoft Win...	i-0410117f-8f01-7	Running	t2.micro	Initializing	View alarms +	us-east-1b

In my future projects I will create storage including a database and web server for hosting documents and files for use by the company. I will also delve deeper into security policies and frameworks like Identity and Access Management. Stay Tuned!