# Introduction to Instances in AWS

For many businesses and personal projects, maintaining a physical server is a costly endeavor with many security and recovery concerns. Instances are a cost-effective solution that is 100% virtual, secure, and remotely accessible. Amazon Web Services (AWS) is one of the best options for creating scalable instances based on your needs.

This guide will cover the basics of instances and why you should use AWS for instances. You will then learn how to use AWS to create, configure, and connect to a Windows Server instance. Only general knowledge of cloud computing and networking concepts like IP addresses, Remote Desktop Protocol (RDP), network traffic, and the command prompt is required to understand this guide.

## What is an instance?

An *instance* is a virtual computer that runs on the AWS Cloud. Instances look and act like any other computer; you can browse the internet, host servers, run applications, etc. They are even powered by virtual versions of physical hardware like CPUs and RAM.

The only difference between instances and physical computers is that instances are entirely virtual; you can connect to an instance from your own computer, even if it uses a different operating system!

### Types of instances

Not all instances are built the same, from the operating system to the virtual hardware specs. In AWS you can select an instance type that best suits your computational needs, and each type offers different instance families with various sizes and features. AWS offers six instance types:

* **General Purpose:** Balances computing, networking, and memory resources. Best for web servers and small application servers.
* **Compute Optimized:** Offers high computation power. Best for gaming servers and data models requiring high performance.
* **Memory Optimized:** Processes large datasets quickly for fast performance. Best for databases and analytics.
* **Accelerated Computing:** Uses hardware accelerators to efficiently process data. Best for graphics applications.
* **Storage Optimized:** Stores large volumes of data. Best for data warehousing.
* **HPC Optimized:** Affordable alternative for high-performance computing.

In this guide, you will create a t2.micro instance, a general-purpose instance from the T2 family. When creating an instance, t2.micro is normally the default selection because it’s free-tier eligible and has a baseline performance. For a detailed look at instance types and their different families, sizes, and specifications, see [Amazon EC2 Instance Types](https://aws.amazon.com/ec2/instance-types/).

**Note:** Free-tier eligibility means that, under the AWS free tier, you can run a t2.micro instance for 750 hours per month for the first 12 months after creating your AWS account. Once your instance passes the 750-hour mark, you will be charged by the hour that your instance is running. For more pricing details, see [Amazon EC2 Pricing](https://aws.amazon.com/ec2/pricing/?trk=36c6da98-7b20-48fa-8225-4784bced9843&sc_channel=ps&ef_id=Cj0KCQjwiZqhBhCJARIsACHHEH92ne1Qjwdj6EQgHboPctF88XLT_CfJm5ALRpWO5muybKSP_5pp26QaAkDxEALw_wcB:G:s&s_kwcid=AL!4422!3!536451475355!e!!g!!ec2%20pricing!11198711716!118263956828).

### Benefits of instances

On top of flexibility, instances offer a lot of benefits over physical servers and computers:

* **Cost-effective:** Instances eliminate the need to invest in hardware, staffing, or physical space to house a data center.
* **Scalable:** You can adjust capacity anytime, only paying for what you need. Physical data centers require guessing capacity, leading to spending too much money maintaining servers you don’t need, or not having enough servers.
* **Reliable:** In case of an outage, natural disaster, or other failures, instances are easily recoverable or replaceable as they're in the cloud. You can spend less time on maintenance and more on satisfying your customers.

## Why use AWS for instances?

AWS is a cloud computing service powered by Amazon. AWS uses the *Elastic Compute Cloud (EC2)* service to run and store instances. On top of instances, AWS offers a variety of free and paid cloud-computing products like VPCs, databases, APIs, and more.

Instances are the same as virtual machines offered by VMWare and the Google Cloud Platform (GCP). What makes AWS stand out is that it has more data centers around the globe, delivering greater accessibility and more storage and RAM. AWS is best for businesses looking to move away completely from physical data centers and legacy systems.

## Creating a Windows Server instance

You can create and configure instances through the *EC2 Dashboard.* You will create a t2.micro instance that uses the Windows Server operating system. *Windows Server* resembles the regular Windows OS but with additional features for server management. To create a Windows Server t2.microinstance:

1. Log in to the [AWS Console](https://us-east-2.console.aws.amazon.com/console/home?region=us-east-2).
2. Type **EC2** into the search bar. Click the **EC2** result that should be the first to appear under **Services**. You are now in the EC2 Dashboard.
3. Under the **Instances** dropdown on the left side menu, click **Instances**. This is where you'd see each of your instances listed as a row in a table.
4. Click **Launch instances**. Give your instance a name.
5. In the **Application and OS Images** section, select an operating system for your instance. Select **Windows** and keep the free-tier version that is already selected for you.
6. In the **Instance type** dropdown, select **t2.micro**. It may already be selected for you.
7. In the **Key pair (login)** section, click **Create new key pair**. Enter a name for your key pair and check the **.pem** radio box for the file format. Click **Create key pair**. Your key pair file will be downloaded to your computer.
8. Keep the remaining settings as their defaults and select **Launch instance**.

Your instance will now appear on the Instances page and should say it's running in the **Status** column. If not running, right-click anywhere on your instance row and click **Start instance**.

## Configuring security settings

AWS provides a lot of customization for an instance’s security settings. You can modify most of these settings by adding and editing rules in your instance’s security group. A *security group* is your instance’s firewall that controls inbound and outbound traffic. You can create your own security groups that you can assign to one or multiple instances, or let AWS create and assign one for you.

### Finding your instance’s security group

When you launched your first instance, you allowed AWS to assign it to a security group instead of creating your own. To find your instance’s security group:

1. On the Instances page of EC2, click on your instance. A panel will appear at the bottom showing your instance’s IP addresses, security, monitor checks, and other details.
2. Click the **Security** tab. Under **Security Groups** you will find your instance’s security group listed. It will probably be named something like **launch-wizard-1**.
3. Click your security group. This will redirect you to a page listing your security group’s details and allows you to edit its inbound and outbound rules.

### Adding an inbound rule

Let’s say you want your actual computer and your instance to be able to exchange data. Security groups block all inbound traffic by default, even if you could successfully connect to that instance. You can test this by pinging your instance’s public IP from your computer. Pinging tests the connection between two IP addresses.

To ping your instance from your computer, open your command prompt or terminal and type ping followed by the public IP address of your instance. The output will likely display Request timed out multiple times, meaning the instance IP is unreachable.

To fix this, you can add a rule in the security group’s inbound rules to allow pings from your computer/IP address. To add an inbound rule to your security group:

1. From the security group’s page, click the **Inbound rules** tab, then click **Edit inbound rules**. This will show a table listing your inbound rules.
2. Click **Add rule**. A new row/rule has been added.
3. Select the following options from the dropdowns in this rule:
   * **Type**: Custom ICMP – IPv4.
   * **Protocol**: Echo Request.
   * **Source**: My IP.
4. Click **Save rules**.

Ping your instance again. The output should now print Reply from followed by the instance’s public IP address and ping statistics and information. This is because the new inbound rule now allows traffic just from your IP.

**Note:** Editing outbound rules works just like editing inbound rules, but is instead done in the **Outbound rules** tab.

## Connecting to your instance

Now that your instance is running and security configured, you're now ready to connect to your instance. There are different ways to connect to a Windows instance, but the easiest way is to download the instance as a .rdp file and log into it using the password decrypted from the key pair file that you downloaded earlier. To connect to your instance:

1. Right-click your instance and select **Connect** (or click the **Connect** button at the top).
2. Select the **RDP client** tab, then click **Download remote desktop file**. A .rdp file with the same name as your instance will be downloaded to your computer.
3. Click **Get password**, and then click **Upload private key file**. Find and open the key-pair .pem file you downloaded in Launching an instance. The contents of your private key should appear in the textbox below.
4. Click **Decrypt password**, and your instance password now appears. Copy the password.
5. Open the .rdp file you downloaded earlier. The Remote Desktop Connection client may warn you that this remote connection can’t be identified. Click **Connect**.
6. Paste your instance password into the **Password** textbox and then click **OK**. Your instance will now open.

Your instance will resemble a Windows desktop, with the wallpaper displaying your instance details. Feel free to play around by browsing the internet, running an application, or hosting a server. When finished, click the **X** button in the title bar to close the instance.

**Caution:** To avoid being charged after the 750-hour mark, you can stop your instance from running by right-clicking your instance on the Instances page and selecting **Stop Instance**. This will change the value in the **Instance state** column to *Stopped*. To delete your instance, right-click your instance and select **Terminate Instance**.

## Conclusion

Instances are a great option for server hosting because they eliminate hardware costs and provide advanced network, configuration, and auto-recovery features. You now know the basics of instances and how to navigate AWS and EC2 to create, configure, and connect to an instance.

For your next step, see the [Amazon EC2 Windows Instance](https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/EC2Win_Infrastructure.html) user guide to learn more about Windows instance configuration. AWS also provides user guides for [Mac](https://aws.amazon.com/getting-started/hands-on/launch-connect-to-amazon-ec2-mac-instance/) and [Linux](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EC2_GetStarted.html) instances.  If you want to branch into other AWS services that can still be applied to instances, try learning about the virtual private cloud (VPC) through [AWS's introductory guide to VPCs](https://docs.aws.amazon.com/vpc/latest/userguide/what-is-amazon-vpc.html).

# Research

This document includes more information after additional research. Much of this research will appear sprinkled throughout the document, rather than as large sections of new information. Nonetheless, all the additions are important for the audience to understand not only AWS instances and their parts, but to also see the documentation available for further learning.

## Types of instances

The most notable addition is a new subsection called **Types of instances** in the **What is an** **instance?** section. This subsection lists the AWS instance types alongside their use cases and purpose. Understanding instance types and how their resources are managed demonstrates the different use cases, from web development to gaming.

The subsection also introduces *t2.micro*, the general-purpose instance that they will learn how to create. Here you can learn about t2.micro and why you will be creating it. If the reader wants to learn about more instance families, specifications, and sizes, the Amazon EC2 Instance Types page is linked at the end.

Additionally, in the section now called **Creating a Windows Server instance**, step 6 has been added to show where you’re specifically choosing to create a t2.micro instance, rather than it being implied in the last step where you’re keeping the remaining settings as-is.

## Free-tier instances

Through my research and personal experience with running an AWS instance, I learned how the AWS EC2 free tier works. The note at the end of Types of instances explains how the free-tier works, as t2.micro, is a free-tier eligible instance.

Because t2.micro is a small instance, many readers probably won’t use it for their business or large personal projects. Alongside readers who decide after reading this guide that they are no longer interested in AWS EC2, they probably don’t want to be charged because the instance they created just for this guide accidentally ran past the 750-hour mark.

A caution note is included at the end of **Connecting to your instance** reminding users that they will be charged if they leave the instance running too long and showing them how to stop or terminate their instance to prevent this. This prevents the guide from being at fault for the reader being charged and will save the reader a headache

## Windows Server and interface

AWS instances are primarily used for server hosting, so the operating systems used in instances will differ from the regular operating systems used on a normal PC. Rather than the regular Windows OS, AWS has the option to use Windows Server, an OS specifically designed for server management. Because Windows Server looks like regular Windows save for a few additional programs for server management, they will not need an in-depth introduction.

When the reader connects to their Windows Server instance, they will notice.

## Next steps

In the conclusion section, I added a short paragraph encouraging the reader to look deeper into instances and other AWS topics not covered in the document. Because the document only teaches you how to create a Windows Server instance, I added links to official AWS documentation that go into how to create Mac and Linux instances, as many readers may have a preference for their operating system.

For those who want to investigate other AWS concepts