

Deploying Virtual Machines within the Amazon Elastic Compute Cloud

The Virtual Machine (VM) is a software-based imitation that duplicates the functions and capabilities found in physical computing devices. This duplication allows for running tasks, applications, and processes in a way that is both isolated from, and insulated against, the underlying hardware infrastructure, providing a layer of abstraction that offers both versatility and efficiency. Deploying a VM within the Amazon Elastic Compute Cloud (EC2) is a prime example of virtualization technology at work, offering up scalability, flexibility, and control over computing resources in a cloud-based setting.

Creating a VM

A VM is created through a process known as **virtualization**. In this process, specialized software (a hypervisor) allocates and manages resources from the physical host to forge and sustain a VM. Each VM functions as if in its own virtual bubble, equipped with an array of virtualized hardware components such as CPUs, memory, storage, and network interfaces that mirror the structure of a physical computer.

Deploying a VM on EC2

Do the following to deploy a VM on EC2:

1. Initiate the EC2 instance:
 - a. Create an Amazon Web Services (AWS) account.
 - b. Go to the EC2 dashboard within the AWS Management Console.
 - c. Click **Launch Instance** to launch the EC2 instance.

2. Select an Amazon Machine Image (AMI). The AMI acts as the blueprint for the VM. This blueprint encompasses the operating system, application server and applications, along with bundled configurations.

Attention: The AMI selection is critical, as the AMI lays the groundwork for the VM.

3. Specify the instance type to determine the virtualized hardware resource allocation (for example, CPU, memory, and so forth) for the VM. EC2 offers a wide array of instance types, catering to various use cases and performance needs, each with its own set of complexities.
4. Adjust any additional settings relevant to the VM, such as:
 - The number of instances
 - The network and subnet configurations
 - The assignment of an Identity and Access Management (IAM) role, among others
5. Append extra storage volumes to the VM beyond the default storage provisioned by the AMI.

Attention: This step is critical for applications that require significant data storage and throughput capabilities.

6. Tag the instance. Assign key-value pairs to the VM for easier identification, organization, and management within the AWS ecosystem.
7. Configure security groups. Security groups act as virtual firewalls that control the traffic allowed to and from the VM. This ensures the security and integrity of the VM's operational environment.
8. Review and verify the configurations and settings specified previously.
9. Click **Launch** to launch the VM.