

Using Roles:

A blurred screenshot of the AWS IAM console interface, showing various settings and options in a purple-themed layout.

What Is an IAM Role?

A role is an identity you can create in IAM that has specific permissions. A role is similar to a user, as it is an AWS identity with permission policies that determine what the identity can and cannot do in AWS.

Roles Are Temporary

A role does not have standard long-term credentials the same way passwords or access keys do. Instead, when you assume a role, it provides you with temporary security credentials for your role session.



What Else Can Roles Do?

Roles can be assumed by people, AWS architecture, or other system-level accounts.

Roles can allow cross-account access. This allows one AWS account the ability to interact with resources in other AWS accounts.

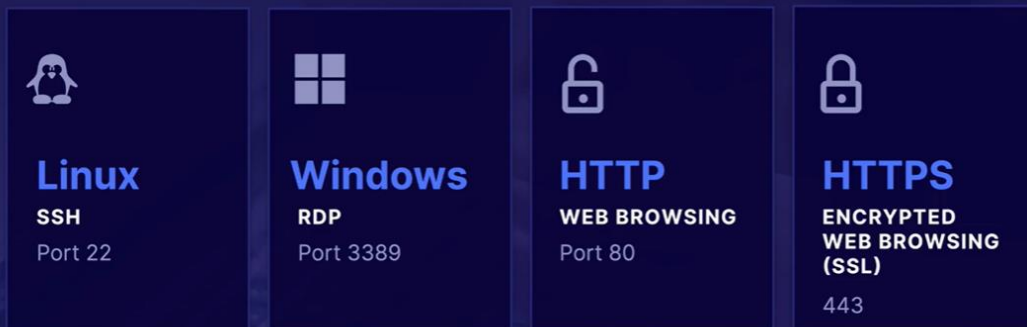


What to Remember When Using Roles

- 1 The Preferred Option**
Roles are preferred from a security perspective.
- 2 Avoid Hard-Coding Your Credentials**
Roles allow you to provide access without the use of access key IDs and secret access keys.
- 3 Policies**
Policies control a role's permissions.
- 4 Updates**
You can update a policy attached to a role, and it will take immediate effect.
- 5 Attaching and Detaching**
You can attach and detach roles to running EC2 instances without having to stop or terminate those instances.

Security Groups:

How Computers Communicate



Security Groups

Security groups are **virtual firewalls for your EC2 instance**. By default, everything is blocked.

TO LET EVERYTHING IN: 0.0.0.0/0

In order to be able to **communicate to your EC2 instances via SSH/RDP/HTTP**, you will need to **open up the correct ports**.



Bootstrap Scripts

A script that runs when the instance first runs

```
#!/bin/bash
yum install httpd -y
#installs apache
yum service httpd start
#starts apache
```

Adding these tasks at boot time **adds to the amount of time it takes to boot the instance.** However, it allows you to **automate the installation** of applications.

Security Groups Exam Tips

- ✓ **Tip 1:** Changes to security groups take effect immediately.
- ✓ **Tip 2:** You can have any number of EC2 instances within a security group.
- ✓ **Tip 3:** You can have multiple security groups attached to EC2 instances.
- ✓ **Tip 4:** All inbound traffic is blocked by default.
- ✓ **Tip 5:** All outbound traffic is allowed.

💡 STUDY TIP

Bootstrap Scripts

A bootstrap script is **a script that runs when the instance first runs.** It passes user data to the EC2 instance and can be used to install applications (like web servers and databases), as well as do updates and more.

EC2 Metadata:



WHAT IS EC2 METADATA?

EC2 metadata is simply data about your EC2 instance.

This can include information such as private IP address, public IP address, hostname, security groups, etc.

User Data vs. Metadata

- ✓ User data is simply bootstrap scripts.
- ✓ Metadata is data about your EC2 instances.
- ✓ You can use bootstrap scripts (user data) to access metadata.

Networking with EC2:

Networking with EC2

You can attach 3 different types of **virtual networking cards** to your EC2 instances

ENI

Elastic Network Interface

For basic, day-to-day networking

EN

Enhanced Networking

Uses single root I/O virtualization (SR-IOV) to provide high performance

EFA

Elastic Fabric Adapter

Accelerates High Performance Computing (HPC) and machine learning applications

An **ENI** is simply a virtual network card that allows:



Private IPv4 Addresses



Public IPv4 Address



Many IPv6 Addresses



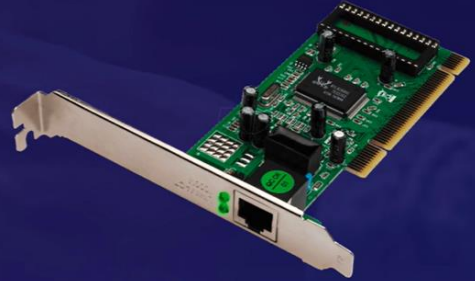
MAC Address



1 or More Security Groups

Common **ENI** Use Cases

- ✓ Create a management network.
- ✓ Use network and security appliances in your VPC.
- ✓ Create dual-homed instances with workloads/roles on distinct subnets.
- ✓ Create a low-budget, high-availability solution.



What Is Enhanced Networking?

For High-Performance Networking between 10 Gbps - 100 Gbps

SINGLE ROOT I/O VIRTUALIZATION (SR-IOV)

SR-IOV provides higher I/O performance and lower CPU utilization

PERFORMANCE

Provides higher bandwidth, higher packet per second (PPS) performance, and consistently lower inter-instance latencies

Depending on your instance type, enhanced networking can be enabled using:

**ELASTIC
NETWORK
ADAPTER
(ENA)**

OR

**INTEL 82599
VIRTUAL FUNCTION
(VF) INTERFACE**

Supports network speeds of up to 100 Gbps for supported instance types.

Supports network speeds of up to 10 Gbps for supported instance types. Typically used on older instances.

What Is an **EFA**?

Elastic Fabric Adapter



A network device you can attach to your Amazon EC2 instance to accelerate High Performance Computing (HPC) and machine learning applications.



Provides lower and more consistent latency and higher throughput than the TCP transport traditionally used in cloud-based HPC systems.



EFA CAN USE OS-BYPASS

It makes it a lot **faster** with
much lower latency.

OS-bypass enables HPC and machine learning applications to bypass the operating system kernel and communicate directly with the EFA device. Not currently supported with Windows — only Linux.

For different scenarios on the exam, choose the correct networking device.

1

ENI

For basic networking. Perhaps you need a separate management network from your production network or a separate logging network, and you need to do this at a low cost. In this scenario, use multiple ENIs for each network.

2

Enhanced Networking

For when you need speeds between 10 Gbps and 100 Gbps. Anywhere you need reliable, high throughput.

3

EFA

For when you need to accelerate High Performance Computing (HPC) and machine learning applications or if you need to do an OS-bypass. If you see a scenario question mentioning HPC or ML and asking what network adapter you want, choose EFA.