#### 

#### **How can you create a new security group in AWS?**

You can create a new security group in AWS by going to the EC2 console, selecting the “Security Groups” link in the sidebar, and then clicking the “Create Security Group” button.

#### **What is an AWS Security Group?**

A security group is a virtual firewall that controls the inbound and outbound traffic for your EC2 instances. When you launch an instance, you associate one or more security groups with the instance. You add rules to each security group that control the traffic that is allowed to reach your instance.

#### **What’s the best way to assign multiple IP addresses to a single instance using security groups?**

You can use Amazon’s EC2 security groups to allow multiple IP addresses to access a single instance. To do this, you will need to create a security group and add each IP address that you want to allow access to the group. You can then assign the security group to your instance.

#### **Can you give me some examples of situations where it makes sense to use separate security groups for different instances?**

There are a few reasons you might want to use separate security groups for different instances. One reason is if you want to have different security policies for different types of instances – for example, you might want to have a more restrictive security policy for database servers than for web servers. Another reason is if you want to isolate different parts of your infrastructure for security purposes – for example, you might want to put all of your database servers in one security group so that they can communicate with each other, but you might want to put your web servers in a different security group so that they can’t directly access your database servers.

#### **Are there any limitations on the number of security groups that can be created per region or account? If yes, then what are they?**

Yes, there are limitations on the number of security groups that can be created per region or account. The maximum number of security groups that can be created per region is 100, and the maximum number of security groups that can be created per account is 500.

#### **What happens if two security groups have conflicting rules for a single port?**

If two security groups have conflicting rules for a single port, then the security group with the more restrictive rule will take precedence.

#### **When creating a new rule in an AWS security group, which among these parameters is mandatory: source, destination, or protocol?**

The protocol parameter is mandatory when creating a new rule in an AWS security group. The source and destination parameters are not mandatory, but they are recommended in order to help specify the traffic that is allowed by the rule.

#### **Is it possible to add more than one CIDR block as a source IP address for a security group?**

Yes, it is possible to add more than one CIDR block as a source IP address for a security group. You can do this by creating multiple inbound rules, each with a different CIDR block as the source.

#### **How long does it take for changes made to a security group to get reflected in terms of network traffic?**

The changes made to a security group are usually reflected within a few minutes. However, it can take up to an hour for the changes to be fully propagated.

#### **What’s the default limit on the number of security groups that can be used by each instance?**

The default limit on the number of security groups that can be used by each instance is 5.

**Terraform**

Provisioners are **used to execute scripts on a local or remote machine as part of resource creation or destruction**. Provisioners can be used to bootstrap a resource, cleanup before destroy, run configuration management, etc.

**What is the difference between remote-exec provisioner and local-exec?**

Provisioners should be used only as a last resort. **The remote-exec provisioner will run a script on the remote machine through WinRM or SSH, and local-exec will run a script on our local machine**.

### **What are the various levels of Sentinel enforcement?**

Sentinel has three enforcement levels - advisory, soft mandatory, and hard mandatory.

* Advisory - Logged but allowed to pass. An advisory is issued to the user when they trigger a plan that violates the policy.
* Soft Mandatory - The policy must pass unless an override is specified. Only administrators have the ability to override.
* Hard Mandatory - The policy must pass no matter what. This policy cannot be overridden unless it is removed. It is the default enforcement level in Terraform.

### **What are the key features of Terraform?**

Terraform helps you manage all of your infrastructures as code and construct it as and when needed. Here are its key main features:

* A console that allows users to observe functions
* The ability to translate HCL code into JSON format
* A configuration language that supports interpolation
* A module count that keeps track of the number of modules applied to the infrastructure.

### 

### **Is Terraform usable for an on-prem infrastructure?**

Yes, Terraform can be used for on-prem infrastructure. As there are a lot of obtainable providers, we can decide which suits us the best. All that we need is an API.

### **Define Resource Graph in Terraform.**

A resource graph is a visual representation of the resources. It helps modify and create independent resources simultaneously. Terraform establishes a plan for the configuration of the graph to generate plans and refresh the state. It creates structure most efficiently and effectively to help us understand the drawbacks.

### **Can you provide a few examples where we can use for Sentinel policies?**

Sentinels are a powerful way to implement a variety of policies in Terraform. Here are a few examples:

* Enforce explicit ownership in resources
* Restrict roles the cloud provider can assume
* Review an audit trail for Terraform Cloud operations
* Forbid only certain resources, providers, or data sources
* Enforce mandatory tagging on resources
* Restrict how modules are used in the Private Module Registr