

Module 5. The AWS Shared Responsibility Model

This module covers the following subjects:

- **Understanding the Shared Responsibility Model:** This part of the module introduces you to the overall definition of the Shared Responsibility model.
- **Amazon Responsibilities:** This section provides examples of Amazon's responsibilities for security in your AWS implementation.
- **Client Responsibilities:** This section provides examples of client responsibilities for securing the resources in AWS.

Whereas some organisations are hesitant to move to the cloud due to sometimes false fears that their security will suffer, other organizations embrace the opportunities for greatly enhanced security. One major reason this is a reality is the existence of the AWS Shared Responsibility model. This model helps us fully understand the security environment when we operate in AWS. This module, designed to be straightforward and easy to follow, makes this subject simple and provides excellent examples of the various parts of the model, ensuring you feel at ease and comfortable with the learning process.

FOUNDATION TOPICS

UNDERSTANDING THE SHARED RESPONSIBILITY MODEL

The AWS Shared Responsibility model is straightforward and clear. It divides the security responsibilities between two parties—the AWS customer (you!) and Amazon (AWS). The fact that you are no longer responsible for a massive portion of the security required for scalable data centres is a huge advantage. You can leverage Amazon's massive budgets and intense expertise, knowing exactly what your role is in the security of your AWS implementation.

The following two sections of this module provide examples of responsibilities in each part of the model. For now, Amazon's responsibilities include the host operating system and virtualisation layer and the physical security of the facilities in which the service operates. Your (the customer's) responsibility is to secure the guest operating system (including updates and security patches), application software, and the AWS network security group firewall. Be aware that the client's responsibilities will vary depending on the client's chosen services. The client responsibilities further vary based on the level of integration of AWS services consumed and their IT infrastructure. Laws and regulations that must be followed will also vary.

As shown in Figure 5-1, AWS is considered “security of the cloud”, and the customer's responsibility is considered “security in the cloud.”

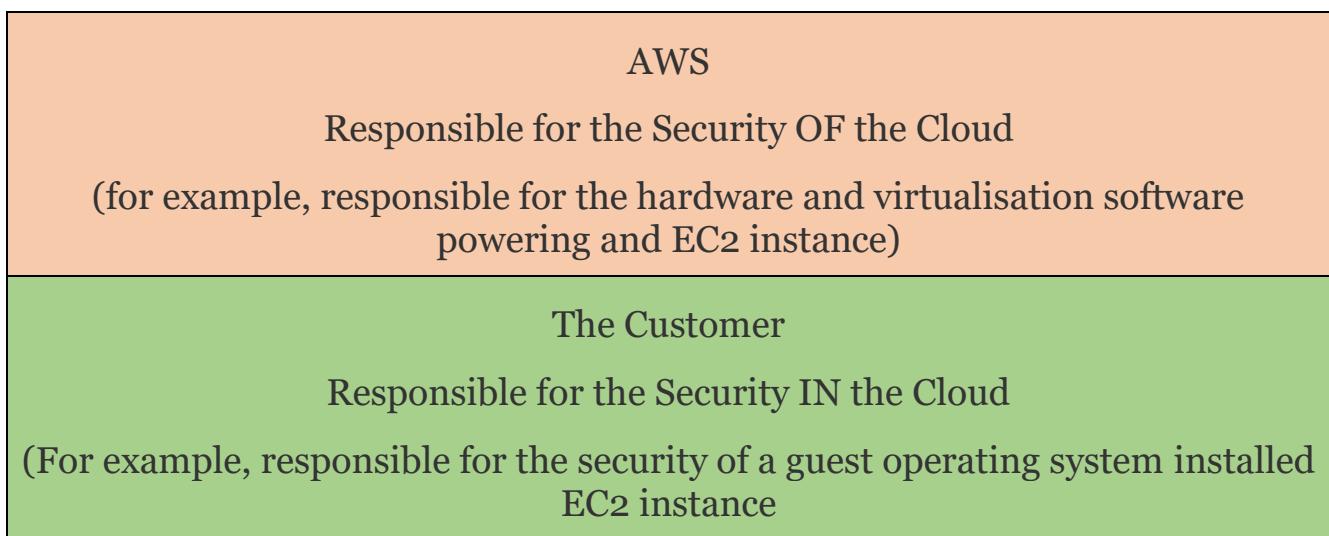


Figure 5-1 The AWS Shared Responsibility Model

In addition to partitioning the operational security concerns between the AWS client and AWS themselves, the Shared Responsibility model also applies to IT controls that are in use. Amazon categorizes these controls into three categories:

- **Inherited controls:** These are security controls the customer fully inherits from AWS. Perfect examples are the physical and environmental security controls used by Amazon.
- **Shared controls:** These are controls that apply to both the infrastructure layer of Amazon and the customer responsibilities. Note that these shared controls apply to each domain in completely separate contexts or perspectives. AWS provides the requirements for the infrastructure, and then the client must provide their own control implementation within their use of the services. A great example is Identity and Access Management (IAM). The IAM service must be secured, meet regulatory compliance, and function as intended, whereas the customer should create well-crafted policies.
- **Customer-specific controls:** These are security controls the customer is solely responsible for, and they vary based on the services the customer selects, of course. A great example would be when you apply specific patches to one of your operating systems on an EC2 instance.

AMAZON RESPONSIBILITIES

Remember, Amazon is considered responsible for security *of* the cloud. AWS is responsible for protecting the infrastructure that runs the services chosen. This includes the hardware and software required to power the AWS service as well as the networking and facilities used.

Specific Amazon responsibilities would include the following:

- Cloud software, including compute, storage, networking, and database software
- Hardware
- AWS Global Infrastructure, including regions, Availability Zones, and Edge Locations

CLIENT RESPONSIBILITIES

Remember, the client is considered responsible for security *in the cloud*. The specific services selected will cause variations in the client responsibilities. For example, if you are relying heavily on Simple Storage Service (S3) for storage, you will be responsible for knowledge and proper configuration of the security permissions for your resources. Another example would be if the client chooses to use EC2 and run an operating system like Windows Server 2016. The client is required to keep the operating system updated and patched and is also responsible for the application software they require on this guest operating system. The client is responsible for the appropriate security group configuration for the EC2 instance as well.

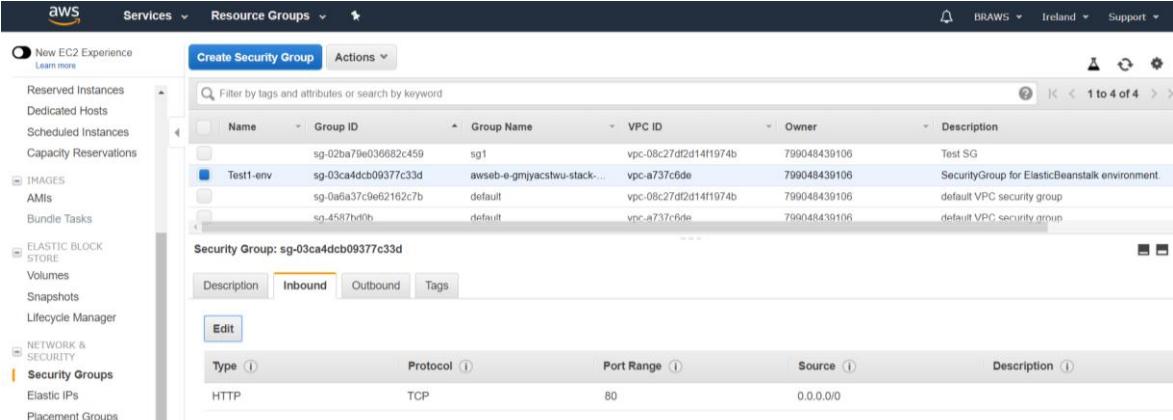
Specific examples of client responsibilities would include the following:

- Customer data
- Platform, applications, IAM
- Guest operating systems
- Network and firewall configurations
- Client-side data encryption
- Server-side encryption (file system and/or data)
- Networking traffic protection (encryption, integrity, and identity)

Figure 5-2 shows an example of a customer checking the security group settings that would apply to an EC2 instance. This is a perfect example of client responsibilities. AWS is responsible for ensuring the security group functions as intended, but the client must configure it correctly.

See:

<https://aws.amazon.com/compliance/shared-responsibility-model/>



The screenshot shows the AWS EC2 Service dashboard with the 'Resource Groups' section selected. On the left, a sidebar lists various AWS services like Reserved Instances, Dedicated Hosts, and Security Groups. The 'Security Groups' section is expanded, showing a list of existing security groups. One group, 'Test1-env', is selected and its details are shown in the main pane. The 'Inbound' tab is active, displaying a single rule: Type: HTTP, Protocol: TCP, Port Range: 80, and Source: 0.0.0.0/0.

Figure 5-2 Checking the Security Group Settings for an EC2 Instance

EXAM PREPARATION TASKS

- REVIEW ALL TOPICS
- DEFINE ALL KEY TERMS AND CHECK ANSWERS IN THE GLOSSARY.
- DO THE QUIZ – REPEAT UNTIL YOU PASS IT (100% PASSMARK).

DEFINE KEY TERMS

Define the following key terms from this module and check your answers in the Glossary:

The AWS Shared Responsibility model

security of the cloud

security in the cloud

Q&A

1. What would be an example of IT security controls that a customer inherits from Amazon?

2. Provide at least three examples of client responsibilities under the AWS Shared Responsibility model.

3. Provide at least two examples of Amazon responsibilities under the AWS Shared Responsibility model.