AWS Organizations

With your first foray into the AWS Cloud, you most likely will start with one AWS account and have everything reside in there. Most people start this way, but as your company grows or even begins their cloud journey, it's important to have a separation of duties.

For example, you want your developers to have access to development resources, have your accounting staff able to access billing information, or even have business units separate so that they can experiment with AWS services without effecting each other.

When you create an organization, AWS Organizations automatically creates a **root**, which is the parent container for all the accounts in your organization.

In AWS Organizations, you can **centrally control permissions for the accounts** in your organization by using **service control policies (SCPs)**. SCPs enable you to place restrictions on the AWS services, resources, and individual API actions that users and roles in each account can access. In other words, you can apply service control policies (SCPs) to the **organization root, an individual member account, or an organizational unit (OU)**.

An **SCP affects all IAM users**, groups, and roles within an account, **including the AWS account root user**. You can apply IAM policies to IAM users, groups, or roles, but you **cannot apply an IAM policy to the AWS account root user.**

Organizational units

In AWS Organizations, you can implement hierarchical groupings of your group accounts into organizational units (OUs) to make it easier to manage accounts with similar business or security requirements (kind of like business units). **When you apply a policy to an OU, all the accounts in the OU automatically inherit the permissions** specified in the policy.

By organizing **separate accounts into OUs**, you can more easily isolate workloads or applications that have specific security requirements. For instance, if your company has accounts that can access only the AWS services that meet certain regulatory requirements, you can put these accounts into one OU. Then, you can **attach a policy to the OU** that blocks access to all other AWS services that do not meet the regulatory requirements.

AWS Artifact

Depending on your company’s industry, you may need to **uphold specific standards**. An audit or inspection will ensure that the company has met those standards. For example, you could be audited for taxes to see that you have run the back office correctly and have followed the law. You rely on documentation, records and inspections to pass audits and compliance checks as they come along. You'll need to devise a similar way to meet compliance and auditing in AWS.

AWS complies with a **long list of assurance programs** that you can find online. This means that segments of your compliance have already been completed, and you can focus on meeting compliance within your own architectures that you build on top of AWS.

**AWS Artifact Agreements**

Suppose that your company needs to **sign an agreement with AWS** regarding your use of certain types of information throughout AWS services. You can do this through **AWS Artifact Agreements**.

In AWS Artifact Agreements, you can review, accept, and manage agreements for an individual account and for all your accounts in AWS Organizations. Different types of agreements are offered to address the needs of customers who are subject to specific regulations, such as the Health Insurance Portability and Accountability Act (**HIPAA**). Another example is that if you run software that deals with consumer data in the EU, You would need to make sure that you're in compliance with GDPR.

**AWS Artifact Reports**

Next, suppose that a member of your company’s development team is building an application and needs more information about their responsibility for complying with certain regulatory standards. You can advise them to access this information in **AWS Artifact Reports**.

AWS Artifact Reports provide **compliance reports from third-party auditors**. These auditors have **tested and verified that AWS is compliant** with a variety of global, regional, and industry-specific security standards and regulations. AWS Artifact Reports remains up to date with the latest reports released. You can **provide the AWS audit artifacts to your auditors or regulators as evidence of AWS security controls**.

Customer Compliance Centre

The **Customer Compliance Centre** contains resources to help you learn more about AWS compliance.

In the Customer Compliance Centre, you can read customer compliance stories to discover how companies in regulated industries have solved various compliance, governance, and audit challenges. You can also access compliance whitepapers and documentation on topics such as:

 AWS answers to key compliance questions

 An overview of AWS risk and compliance

 An auditing security checklist

To know if you are compliant in AWS, please remember that we follow a shared responsibility. The underlying platform is secure and **AWS can provide documentation on what types of compliance requirements they meet**, through services like AWS Artifact and whitepapers.

Denial-of-service attacks

Customers can call the coffee shop to place their orders. After answering each call, a cashier takes the order and gives it to the barista.

However, suppose that a prankster is calling in multiple times to place orders but is never picking up their drinks. This causes the cashier to be unavailable to take other customers’ calls. The coffee shop can attempt to stop the false requests by blocking the phone number that the prankster is using.

In this scenario, the prankster’s actions are similar to a **denial-of-service attack**.

A **denial-of-service (DoS) attack** is a deliberate attempt to make a website or application unavailable to users.

AWS Shield

AWS Shield is a service that protects applications against DDoS attacks. AWS Shield provides two levels of protection: Standard and Advanced.

**AWS Shield Standard** automatically protects all AWS customers **at no cost**. It protects your AWS resources from the most common, frequently occurring types of DDoS attacks.

As network traffic comes into your applications, AWS Shield Standard uses a variety of analysis techniques (e.g. security groups) to detect malicious traffic in real time and automatically mitigates it.

**AWS Shield Advanced** is a **paid** service that provides detailed attack diagnostics and the ability to detect and mitigate sophisticated DDoS attacks.

It also integrates with other services such as Amazon CloudFront, Amazon Route 53, and Elastic Load Balancing. Additionally, you can **integrate AWS Shield with AWS WAF** by writing custom rules to mitigate complex DDoS attacks.

For the