Security On the Cloud - Design Principles

Learn about the five best practice areas for security in the cloud: a) Identity and Access Management b) Detective Controls c) Infrastructure Protection d) Data Protection e) Incident Response

The security pillar includes the ability to protect information, systems, and assets while delivering business value through risk assessments and mitigation strategies. The security pillar provides an overview of design principles, best practices, and questions

Design Principles

There are six design principles for security in the cloud:

Implement a strong identity foundation:

Implement the principle of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resources. Centralize privilege management and reduce or even eliminate reliance on long term credentials.

Enable traceability:

Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.

Apply security at all layers:

Rather than just focusing on protecting a single outer layer, apply a defense-in-depth approach with other security controls. Apply to all layers, for example, edge network, virtual private cloud (VPC), subnet, load balancer, every instance, operating system, and application.

Automate security best practices:

Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost effectively. Create secure architectures, including the implementation of controls that are defined and managed as including the implementation of controls that are defined and managed as code in version-controlled templates.

Protect data in transit and at rest:

Classify your data into sensitivity levels and use mechanisms, such as encryption and tokenization where appropriate. Reduce or eliminate direct human access to data to reduce risk of loss or modification.

Prepare for security events:

Prepare for an incident by having an incident management process that aligns to your organizational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

Definition There are five best practice areas for security in the cloud:

1. Identity and Access Management
2. Detective Controls
3. Infrastructure Protection
4. Data Protection
5. Incident Response

Before you architect any system, you need to put in place practices that influence security. You will want to control who can do what. In addition, you want to be able to identify security incidents, protect your systems and services, and maintain the confidentiality and integrity of data through data protection.

You should have a well-defined and practiced process for responding to security incidents. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

The AWS Shared Responsibility Model enables organizations that adopt the cloud to achieve their security and compliance goals. Because AWS physically secures the infrastructure that supports our cloud services, as an AWS customer you can focus on using services to accomplish your goals.

Best Practices Identity and Access Management

Identity and access management are key parts of an information security program, ensuring that only authorized and authenticated users are able to access your resources, and only in a manner that is intended. For example,

you should define principals (users, groups, services, and roles that take action in your account), build out policies aligned with these principals, and implement strong credential management.

These privilege-management elements form the core concepts of authentication and authorization. In AWS, privilege management is primarily supported by the AWS Identity and Access Management (IAM) service, which allows you to control user access to AWS services and resources. You should apply granular policies, which assign permissions to a user, group, role, or resource. You also have the ability to require strong password practices, such as complexity level, avoiding re-use, and using multi-factor authentication (MFA).

You can use federation with your existing directory service. For workloads that require systems to have access to AWS, IAM enables secure access through instance profiles, identity federation, and temporary credentials. The following questions focus on identity and access management considerations for security

SEC 1: How are you protecting access to and use of the AWS account root user credentials?

SEC 2: How are you defining roles and responsibilities of system users to control human access to the AWS Management Console and API?

SEC 3: How are you limiting automated access to AWS resources (for example, applications, scripts, and/or third-party tools or services)?

It is critical to keep root user credentials protected, and to this end AWS recommends attaching MFA to the root user and locking the credentials with the MFA in a physically secured location. IAM allows you to create and manage other non-root user permissions, as well as establish access levels to resources.

Detective Controls:

You can use detective controls to identify a potential security incident. These controls are an essential part of governance frameworks and can be used to support a quality process, a legal or compliance obligation, and for threat identification and response efforts. There are different types of detective controls.

For example, conducting an inventory of assets and their detailed attributes promotes more effective decision making (and lifecycle controls) to help establish operational baselines. Or you can use internal auditing, an examination of controls related to information systems, to ensure that practices meet policies and requirements and that you have set the correct automated alerting notifications based on defined conditions. These controls are important reactive factors that can help your organization identify and understand the scope of anomalous activity.

In AWS, you can implement detective controls by processing logs, events, and monitoring that allows for auditing, automated analysis, and alarming. CloudTrail logs, AWS API calls, and CloudWatch provide monitoring of metrics with alarming, and AWS Config provides configuration history. Service-level logs are also available, for example, you can use Amazon Simple Storage Service (Amazon S3) to log access requests. Finally, Amazon Glacier provides a vault lock feature to preserve mission-critical data with compliance controls designed to support auditable long-term retention.

The following question focuses on detective controls considerations for security.

SEC 4: How are you capturing and analyzing logs? Log management is important to a well-architected design for reasons ranging from security or forensics to regulatory or legal requirements.

It is critical that you analyze logs and respond to them so that you can identify potential security incidents. AWS provides functionality that makes log management easier to implement by giving you the ability to define a data-retention lifecycle or define where data will be preserved, archived, or eventually deleted. This makes predictable and reliable data handling simpler and more cost effective.

Infrastructure Protection

Infrastructure protection includes control methodologies, such as defense in depth and MFA, which are necessary to meet best practices and industry or depth and MFA, which are necessary to meet best practices and industry or regulatory obligations. Use of these methodologies is critical for successful

ongoing operations either in the cloud or on-premises. In AWS, you can implement stateful and stateless packet inspection, either by using AWS-native technologies or by using partner products and services available through the AWS Marketplace.

You should use Amazon Virtual Private Cloud (Amazon VPC) to create a private, secured, and scalable environment in which you can define your topology—including gateways, routing tables, and public and private subnets. The following questions focus on infrastructure protection considerations for security.

Infrastructure protection includes control methodologies, such as defense in depth and MFA, which are necessary to meet best practices and industry or regulatory obligations. Use of these methodologies is critical for successful ongoing operations either in the cloud or on-premises. In AWS, you can implement stateful and stateless packet inspection, either by using AWS-native technologies or by using partner products and services available through the AWS Marketplace.

You should use Amazon Virtual Private Cloud (Amazon VPC) to create a private, secured, and scalable environment in which you can define your topology—including gateways, routing tables, and public and private subnets. The following questions focus on infrastructure protection considerations for security.

SEC 5: How are you enforcing network and host-level boundary protection?

SEC 6: How are you leveraging AWS service-level security features?

SEC 7: How are you protecting the integrity of the operating system?

Multiple layers of defense are advisable in any type of environment. In the case of infrastructure protection, many of the concepts and methods are valid across cloud and on-premises models. Enforcing boundary protection, monitoring points of ingress and egress, and comprehensive logging, monitoring, and alerting are all essential to an effective information security plan.

AWS customers are able to tailor, or harden, the configuration of an Amazon

AWS customers are able to tailor, or harden, the configuration of an Amazon Elastic Compute Cloud (Amazon EC2), Amazon EC2 Container Service (Amazon

ECS) container, or AWS Elastic Beanstalk instance, and persist this configuration to an immutable Amazon Machine Image (AMI). Then, whether triggered by Auto Scaling or launched manually, all new virtual servers (instances) launched with this AMI receive the hardened configuration.

Data Protection

Before architecting any system, foundational practices that influence security should be in place. For example, data classification provides a way to categorize organizational data based on levels of sensitivity, and encryption protects data by rendering it unintelligible to unauthorized access. These tools and techniques are important because they support objectives such as preventing financial loss or complying with regulatory obligations.

In AWS, the following practices facilitate protection of data:

As an AWS customer you maintain full control over your data.

AWS makes it easier for you to encrypt your data and manage keys, including regular key rotation, which can be easily automated by AWS or maintained by you. Detailed logging that contains important content, such as file access and changes, is available. AWS has designed storage systems for exceptional resiliency. For example, Amazon S3 is designed for 11 nines of durability. (For example, if you store 10,000 objects with Amazon S3, you can on average expect to incur a loss of a single object once every 10,000,000 years.)

Versioning, which can be part of a larger data lifecycle management process, can protect against accidental overwrites, deletes, and similar harm. AWS never initiates the movement of data between Regions. Content placed in a Region will remain in that Region unless you explicitly enable a feature or leverage a service that provides that functionality. The following questions focus on data protection considerations for security.

SEC 8: How are you classifying your data?

SEC 9: How are you encrypting and protecting your data at rest?

SEC 10: How are you managing keys?

SEC 11: How are you encrypting and protecting your data in transit?

AWS provides multiple means for encrypting data at rest and in transit. AWS build features into our services that make it easier to encrypt your data. For example, AWS has implemented server-side encryption (SSE) for Amazon S3 to make it easier for you to store your data in an encrypted form. You can also arrange for the entire HTTPS encryption and decryption process (generally known as SSL termination) to be handled by Elastic Load Balancing (ELB).

Incident Response

Even with extremely mature preventive and detective controls, your organization should still put processes in place to respond to and mitigate the potential impact of security incidents. The architecture of your workload will strongly affect the ability of your teams to operate effectively during an incident to isolate or contain systems and to restore operations to a known-good state.

Putting in place the tools and access ahead of a security incident, then routinely practicing incident response, will make sure the architecture is updated to accommodate timely investigation and recovery. In AWS, the following practices facilitate effective incident response:

Detailed logging is available that contains important content, such as file access and changes. Events can be automatically processed and trigger scripts that automate runbooks through the use of AWS APIs.

You can pre-provision tooling and a “clean room” using AWS CloudFormation. This allows you to carry out forensics in a safe, isolated environment. The following question focuses on incident response considerations for security

SEC 12: How do you ensure that you have the appropriate incident response?

Ensure that you have a way to quickly grant access for your InfoSec team, and automate the isolation of instances as well at the capturing of data and state for forensics.

Key AWS Services

The AWS service that is essential to security is IAM, which allows you to securely control access to AWS services and resources for your users. The following services and features support the five areas in security:

following services and features support the five areas in security:

Identity and Access Management:

IAM enables you to securely control access to AWS services and resources. MFA adds an extra layer of protection on top of your user name and password.

Detective Controls:

AWS CloudTrail records AWS API calls, AWS Config provides a detailed inventory of your AWS resources and configuration, and Amazon CloudWatch is a monitoring service for AWS resources.

Infrastructure Protection:

Amazon VPC lets you provision a private, isolated section of the AWS Cloud where you can launch AWS resources in a virtual network.

Data Protection:

Services such as ELB, Amazon Elastic Block Store (Amazon EBS), Amazon S3, and Amazon Relational Database Service (Amazon RDS) include encryption capabilities to protect your data in transit and at rest. Amazon Macie automatically discovers, classifies, and protects sensitive data, while AWS Key Management Service (AWS KMS) makes it easy for you to create and control keys used for encryption.

Incident Response: IAM should be used to grant appropriate authorization to incident response teams. AWS CloudFormation can be used to create a trusted environment for conducting investigations.