**AWS Security Fundamentals**

**Introduction.**

Design Principles - In the cloud, there are a number of principles that can help you strengthen your security. Use the principles described below to help guide your conversation around security and compliance.

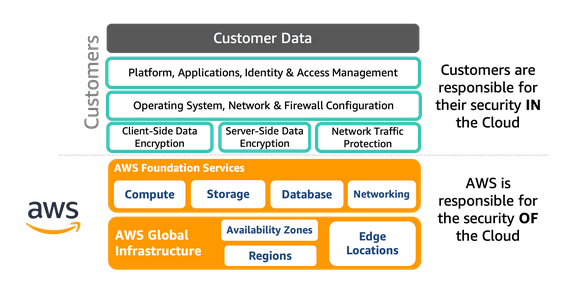
* Implement a strong identity foundation - Implement the principles of least privilege and enforce separation of duties with appropriate authorization for each interaction with your AWS resource.
* Enable traceability - Monitor, alert, and audit actions and changes to your environment in real time. Integrate logs and metrics with systems to automatically respond and take action.
* Apply security at all layers - Rather than just focusing on protection of a single outer layer, apply a defence-in-depth approach with other security controls.
* Automate security best practices - Automated software-based security mechanisms improve your ability to securely scale more rapidly and cost-effectively. Implement 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 where appropriate, use mechanisms like encryption and access control.
* Enforce the principles of least privilege - Access to data should only be granted to the people who really need that access. Start with denying access to everything and grant access when needed.
* Prepare for security events - Prepare for an incident by having an incident management process that aligns to your organisational requirements. Run incident response simulations and use tools with automation to increase your speed for detection, investigation, and recovery.

**AWS Shared Responsibility Model**

AWS is responsible for protecting the global infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure comprises the hardware, software, networking, and facilities that run AWS services.

As an AWS customer, you are responsible for securing your data, operating systems, networks, platforms, and other resources that you create in the AWS Cloud. You are responsible for protecting the confidentiality, integrity, and availability of your data and for meeting any specific business and/or compliance requirements for your workloads.

In this course, we will look at how AWS deals with security OF the cloud, and how you can take care of security IN the cloud.



**AWS Global Infrastructure -** Data Centres are grouped together as Availability Zones. These Data Centres are connected by high speed dedicated connections. An AWS Region is made up of multiple Availability Zones. The Availability Zones are completely independent of each other to provide redundancy.

AWS regions near to the customers makes sense to provide best service to customers, however, considerations have to be made as to compliance and storage of data vs processing. Also, cost across regions differs.

**Data Centre Security** - The AWS global infrastructure is designed and managed according to security best practices and a variety of security compliance standards. As an AWS customer, you can be assured that you are building solutions supported by one of the most secure computing infrastructures in the world.

* Perimeter - AWS data centre physical security starts at the perimeter layer.
  + Buildings - AWS data centers are housed in nondescript, undisclosed facilities
  + Least Privilege - AWS limits access to pre-approved areas and only provides data centre access and information to employees and contractors who have a legitimate business need for such privileges.
  + Employee scrutinisation - Only AWS employees who routinely need access are given permissions to relevant areas of the facility based on job function. If an employee doesn’t have an ongoing business need to be at a data centre, they have to go through the visitor process and have an escort assigned throughout the duration of their visit.
  + Surveillance - Professional security staff use video surveillance, intrusion detection, access log monitoring systems, and other electronic means. Entrances are secured with devices that sound alarms if a door is forced or held open
* Environmental - AWS carefully chooses their data center locations to mitigate environmental risks like flooding, extreme weather, and seismic activity.
  + Customers requiring high availability and performance can deploy their applications across multiple Availability Zones in the same region for fault tolerance and low latency.
  + To mitigate and prepare for the unexpected, AWS tests their Business Continuity Plan regularly with drills that simulate different scenarios.
  + Companies generally use 77% fewer servers, 84% less power, and tap into a 28% cleaner mix of solar and wind power in the AWS Cloud versus their own traditional data centers.
* Infrastructure Layer - Components like backup power equipment, the HVAC system, and fire suppression equipment are all part of the Infrastructure Layer and help protect servers and ultimately your data. Click each icon below for more information.
  + Fire Detection: Automatic fire detection and suppression equipment reduces the risk of fire-related accidents. Smoke detection sensors are in all data centre environments, mechanical and electrical spaces, chiller rooms, and generator equipment rooms.
  + Monitoring: AWS monitors electrical, mechanical, and life support systems. Preventive maintenance is regularly performed.
  + Climate Control: Used to maintain a constant temperature for servers and other hardware. Prevents overheating and reduces the possibility of service outages.
  + Power: Electrical systems are fully redundant and maintainable without impact to operations. UPS units provide backup power for critical and essential loads and generators provide power backup for the entire facility.
* Data Layer - Even though protecting your data is ultimately your responsibility in the cloud, AWS takes extra precautions to protect the media that your data lives on.
  + Storage devices are decommissioned by using NIST800-88 techniques to destroy customer data.
  + AWS is audited by external auditors who inspect our data centers and confirm that we are following established rules needed to obtain our security certifications.
  + AWS servers can notify employees of any attempts to remove data. In the unlikely event of a breach, the server is automatically disabled.

**Compliance and Governance -**  AWS communicates about its security and control environment to customers by:

* Obtaining industry certifications and independent third-party attestations.
* Publishing information about AWS security and control practices in whitepapers and website content.
* Providing certificates, reports, and other documentation directly to AWS customers under an NDA (as required).
* Providing security features and enablers, including compliance playbook and mapping documents for compliance programs.

Running your workloads on AWS does not automatically make the workload compliant. It is your responsibility to ensure that your workload meets all the requirements established in the compliance standard. However, AWS is already certified for its infrastructure, so you only have to certify the applications and architectures you create.



**AWS Artifact** - AWS Artifact is a no-cost, self-service portal for access to the AWS security and compliance reports and select online agreements. Reports available include our Service Organization Control (SOC) reports, Payment Card Industry (PCI) reports, and certifications from accreditation bodies across geographies and compliance verticals.

<https://aws.amazon.com/artifact/>

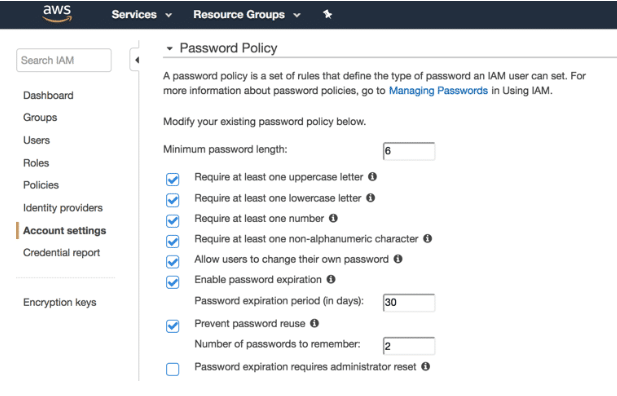
**Identity and Access Management**

**AWS IAM Users and Groups** - The careful management of access credentials is the foundation of how you will secure your resources in the cloud. As we saw in the previous video, every interaction you make with AWS is authenticated. When you open an AWS account, the identity you begin with has access to all AWS services and resources in that account. You use this identity to establish less-privileged users and role-based access in IAM. IAM is a centralized mechanism for creating and managing individual users and their permissions with your AWS account.

An IAM group is a collection of users. Groups allow you to specify permissions for similar types of users. For example, if you have a group named "Developers," you can give that group the types of permissions that developers typically need. This can be considered a form of role-based access control. Create groups that reflect organization roles, not technical commonality.

**Types of AWS Credentials**

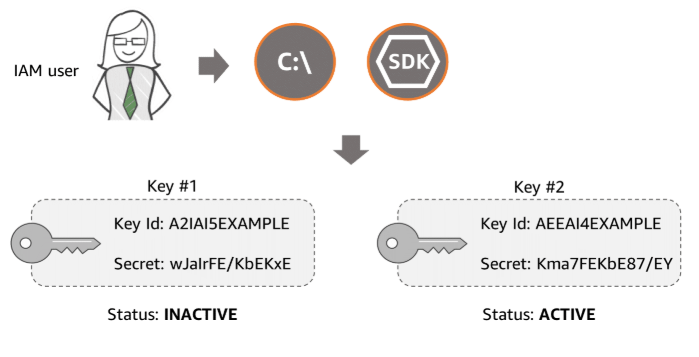
**Username and Password** - A password policy is a set of rules that define the type of password an IAM user can set. You should define a password policy for all of your IAM users to enforce strong passwords and regular changing of passwords. Password requirements are similar to those found in most secure online environments.



**Multi-Factor Authentication** - Multi-factor authentication (MFA) is an additional layer of security for accessing AWS services. With this authentication method, more than one authentication factor is checked before access is granted, which consists of a user name and password, and the single-use code from the MFA device. AWS CLI also supports MFA. Please click here for a list of supported MFA devices.

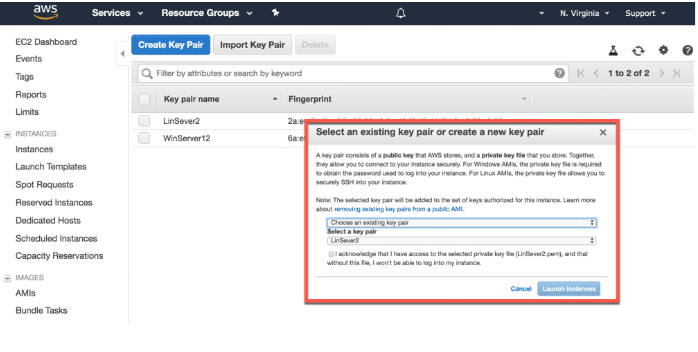


**User Access Keys** - Users need their own access keys to make programmatic calls to AWS using the AWS CLI, the AWS SDKs, or direct HTTPS calls using the APIs for individual AWS services. Access keys are used to digitally sign API calls made to AWS services. Each access key credential consists of an access key ID and a secret key. Each user can have two active access keys, which is useful when you need to rotate the user's access keys or revoke permissions.



**Amazon EC2 Key Pairs -** To enable SSH or RDP connections to an Amazon Elastic Cloud Compute (EC2) instance, AWS uses a public–key infrastructure to sign the login request. The public and private keys are known as a key pair. To log in to your instance, you must create a key pair, or use an existing key pair, and provide the private key when you connect to the instance. You can choose to have the EC2 key pairs generated by AWS or import your own set of keys.

EC2 key pairs do not provide accountability (as in who is using the keys); therefore, they are not recommended for routine usage. If you require daily access to the instance, AWS recommends that EC2 instances be part of a directory domain (Active Directory or LDAP) in order to enable federated access and provide accountability by tracking which user is logging into which instance.



*“The separation between Authentication and Authorization is important to optimize – having strong authentication methods (Active Directory integration, SAML, rotating credentials, MFA) is critical, but ensuring that each operator (human or machine) only has the authorization to do the tasks they need to do against only the objects they should be touching keeps the risk of accidental or malicious actions in a manageable scope. Humans can’t break it, if they can’t touch it.*

Blaine Sundrud - Senior AWS Instructional Designer

**Additional AWS Services for Identity and Access Management**

The AWS services listed below can also be used to protect credentials, allow for user federation, and centrally manage and secure multiple AWS accounts.

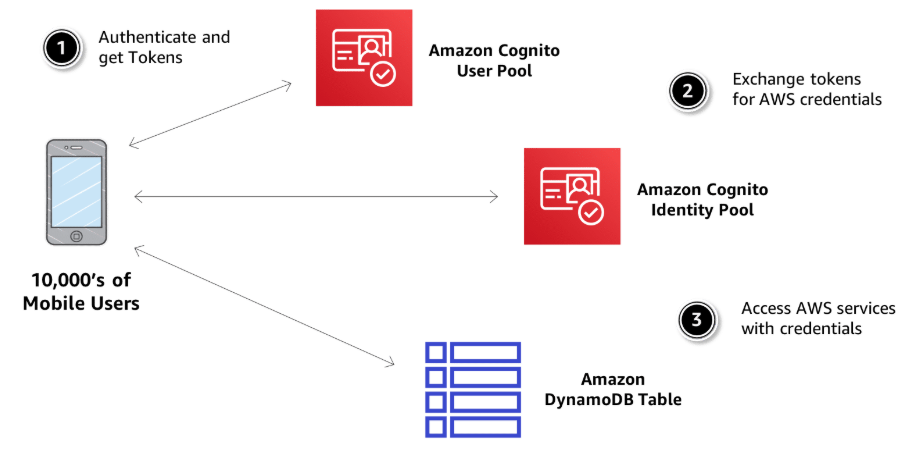
* **AWS Secrets Manager** - AWS Secrets Manager is designed to centrally manage secrets used to access resources on AWS, on-premises, and third-party services. Secrets can be database credentials, passwords, third-party API keys, and even arbitrary text. Secrets Manager enables you to replace hard coded credentials in your code with an API call to Secrets Manager to retrieve the secret programmatically. Also, you can configure Secrets Manager to automatically rotate the secret for you according to a schedule that you specify.
* **AWS Single Sign-On** - AWS Single Sign-On (SSO) is a cloud SSO service that allows for the central management of SSO access to multiple AWS accounts and business applications. It enables users to sign in to a user portal with their existing corporate credentials and access all of their assigned accounts and applications from one place. AWS SSO includes built-in SAML integrations to many business applications. AWS SSO may be integrated with Microsoft Active Directory, which means your employees can sign in to your AWS SSO user portal using their corporate Active Directory credentials.
* **AWS STS** - The AWS Security Token Service (STS) is a web service that enables you to request temporary, limited-privilege credentials for IAM users who are taking on a different role or for users who are being federated. A scenario in which someone, or something, needs access to your account to perform a specific task that is not done on a daily basis would be a great candidate for temporary credentials.
* **AWS Directory Service** - AWS Directory Service for Microsoft Active Directory, also known as AWS Managed Microsoft AD, enables your domain workloads and AWS resources to use managed Active Directory in the AWS Cloud. AWS Managed Microsoft AD is built on actual Microsoft Active Directory and does not require you to synchronize or replicate data from your existing Active Directory to the cloud.
* **AWS Organisations -** AWS Organizations lets you centrally manage and enforce policies for multiple AWS accounts. This service allows grouping accounts into organizational units and use service control policies to centrally control AWS services across multiple AWS accounts. With Organizations, you can also automate the creation of new accounts through APIs and simplify billing by allowing you to set up a single payment method for all the accounts in your organization through consolidated billing. Organizations are available to all AWS customers at no additional charge.

****

**AWS Service Spotlight**

**Amazon Cognito** - Amazon Cognito lets you add user sign-up, sign-in, and access controls to your web and mobile apps. You can define roles and map users to different roles so your app can access only the resources that are authorized for each user. User sign in can be done either by a third-party identity provider, or directly via Amazon Cognito.

An Amazon Cognito user pool is a user directory that manages the overhead of handling the tokens that are returned from social sign-in providers, such as Facebook, Google, and Amazon, and enterprise identity providers via SAML 2.0. After a successful user pool sign-in, your web or mobile app will receive user pool tokens from Amazon Cognito. These tokens can then be used to retrieve AWS credentials via Amazon Cognito identity pools. These credentials allow your app to access other AWS services and you don’t have to embed long-term AWS credentials in your app.

****

**Detective Controls**

**Capturing and Collecting Logs**

Detective controls are an essential part of governance frameworks and can be used to identify a potential security threat or incident. In AWS, there are a number of approaches to consider when addressing detective controls. AWS CloudTrail records API calls made on your account. This information helps you track changes made to your AWS resources, troubleshoot operational issues, and ensure compliance with internal policies and regulatory standards.

**AWS CloudTrail logs -**  AWS CloudTrail is enabled by default on your AWS account. You can use the AWS API call history produced by CloudTrail to track changes to AWS resources, including creation, modification, and deletion of AWS resources. Here we have an example of the type of information found in a CloudTrail log file.

Who made the request:



The log file example that we are analyzing shows that an IAM user named Alice performed some kind of action. You can verify the user's account ID and access key ID.

When and from where?



If we scroll down a bit, we can verify the date of the request and the source IP address from where the request was made. Also available here is the eventName, or the action that was requested, and what was used to send the request in the userAgent field. Here we can see that Alice called the Amazon EC2 StopInstances action by using the AWS CLI. Now let's see which Amazon EC2 instance was involved in this request.

What happened?



Scrolling further down, we can see which resource was affected. Here we see that an Amazon EC2 instance of Id "i-ebeaf9e2" was the resource in this request. The previous and current state of the instance tells us that the call was successful.

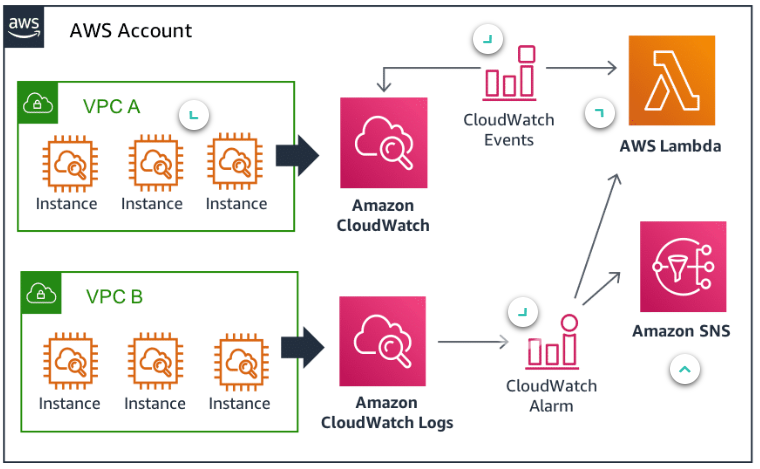
*“Keeping every CloudTrail log in its immutable form is part of proving your compliance. The best suggestion is to have every log file copied to a different account with a non-penetrable access wall. For example, if account A is tracking all actions using CloudTrail, all logs are copied to account B. No user from account A has access to B, and vice versa. That way, any event forensics can prove that no one person, even a human with “admin access,” has the ability to cover their own tracks.”*

Blaine Sundrud - Senior AWS Instructional Designer

**Monitoring and Notifications**

It's not uncommon for organizations to integrate security alerts into their operations and platforms. It's essential to be able to detect change, determine whether a change was appropriate, and then route this information to the correct remediation workflow.

In AWS, you use Amazon CloudWatch to route events and information reflecting potentially unwanted changes into a proper workflow. CloudWatch can be used to monitor resources and logs, send notifications, and trigger automated actions for remediation. Take a moment to review the Amazon CloudWatch architecture below to learn more about this service.



**CloudWatch Agent** - Install the CloudWatch agent to allow communication between the Amazon EC2 instance and CloudWatch. This is also true when OS and application logs are being sent from instances and on-premises servers to Amazon CloudWatch Logs for monitoring and analysis.

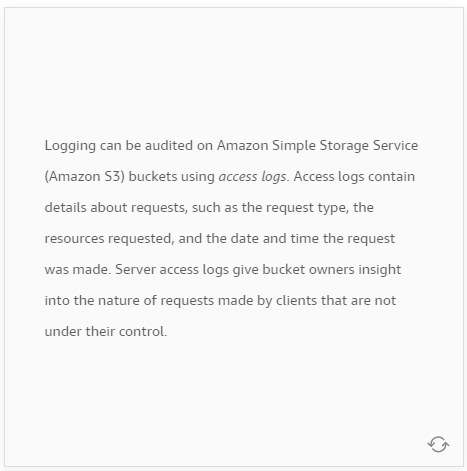
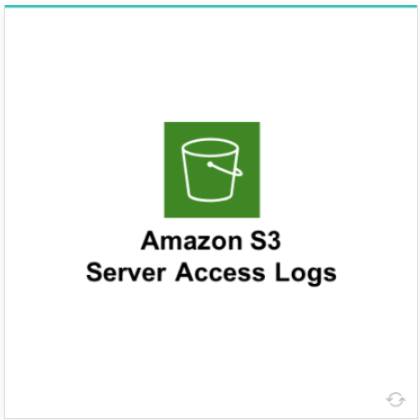
**CloudWatch Events** - Amazon CloudWatch Events delivers a near real-time stream of system events to AWS resources. For example, creating a new snapshot of an Amazon EBS volume qualifies as an event. By using simple rules, you can match events and route them to one or more targets for processing. CloudWatch Events lets you process both AWS-provided events and custom events, or those that you create and inject yourself.

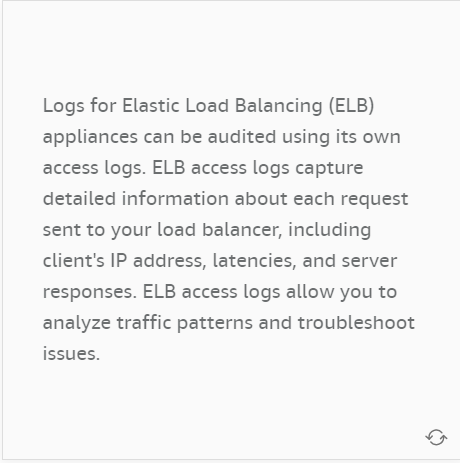
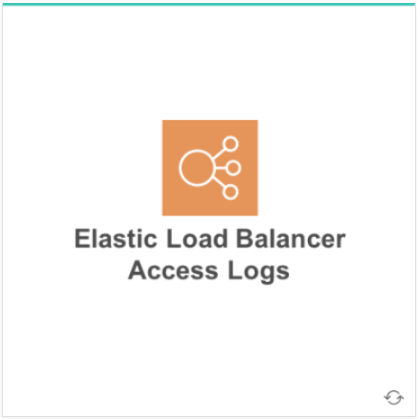
**AWS Lambda for Remediation** - Once an event meets a certain rule, such as a failed security check, an AWS Lambda function is triggered to remedy the situation. Lambda lets you run code without provisioning or managing servers. You pay only for the compute time you consume. There is no charge when your code is not running.

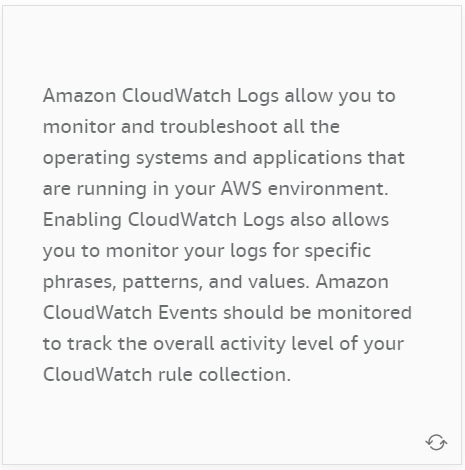
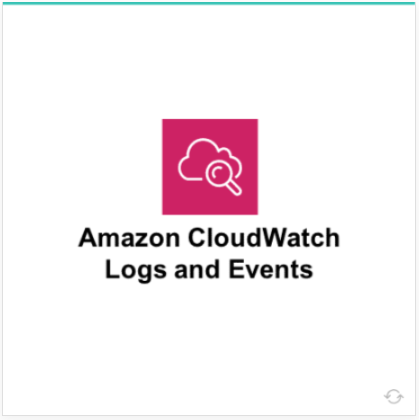
**CloudWatch Alarms** - CloudWatch alarms can be triggered through changes in metrics to send notifications or automatically make changes to resources you are monitoring. For example, a CloudWatch alarm monitoring an EC2 instance can automatically recover the instance via a Lambda function if a system’s status check fails due to loss of network connectivity. When an alarm is triggered and the recovery action is initiated, you can be notified by Amazon Simple Notification Service (Amazon SNS).

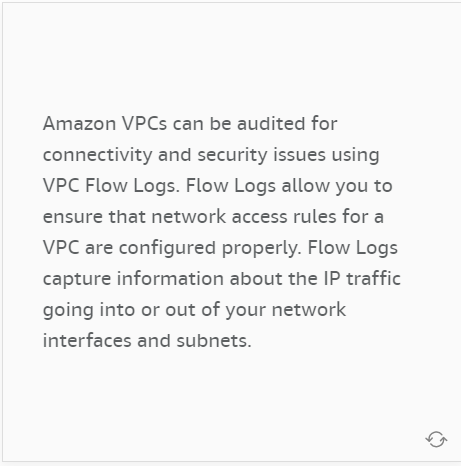
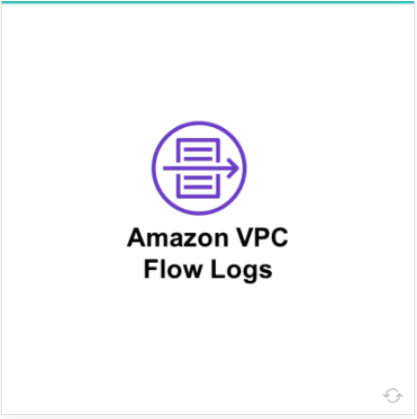
**Amazon SNS for Notifications** - Amazon Simple Notification Service (Amazon SNS) is a flexible, fully managed messaging and mobile notification service for coordinating the delivery of messages to subscribing endpoints and clients. With Amazon SNS, you can fan out messages to a large number of subscribers, and mobile devices. Subscribers may consist of an Amazon SQS queue, web servers, email addresses, SMS text message, mobile devices, or Lambda functions.

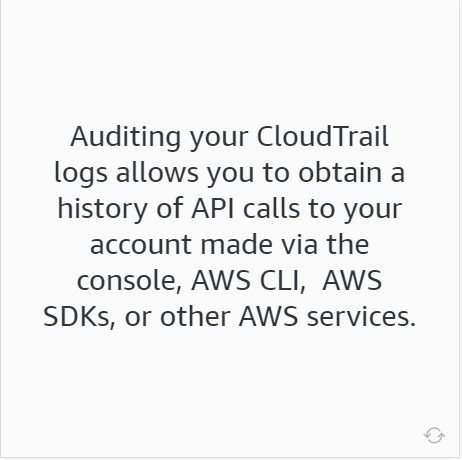
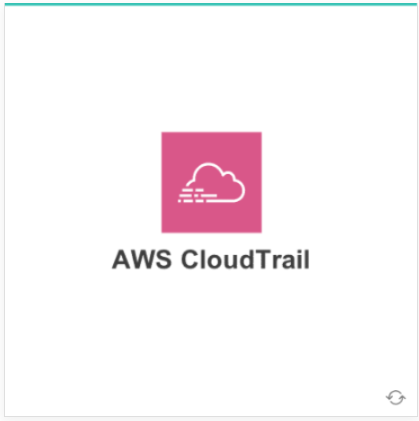
**Auditing on AWS -** The AWS Management Console, along with the AWS CLI, can produce powerful results for auditors across multiple regulatory, standards, and industry authorities. The key services to audit include Amazon S3, Elastic Load Balancing, Amazon CloudWatch, AWS CloudTrail, and Amazon VPC. View each flashcard below for more information.









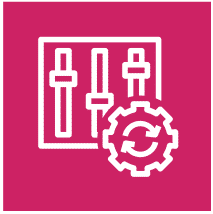


**Additional AWS Services for Detective Controls**

When talking about monitoring and logging, AWS provides a variety of tools and services. Each of the AWS services listed below can be used in conjunction to provide optimal security.

* **Amazon Guard Duty** - an intelligent threat detection service that provides customers with a way to continuously monitor and protect their AWS accounts and workloads. GuardDuty identifies suspected attackers through integrated threat intelligence feeds and uses machine learning to detect anomalies in account and workload activity. It monitors for activity such as unusual API calls or unauthorized deployments that indicate that a customer’s accounts may have been compromised, as well as direct threats like compromised instances or reconnaissance by attackers.
* **AWS Trusted Advisor** - a service that draws upon best practices and inspects your AWS environment making recommendations for saving money, improving system performance, or closing security gaps. You can configure Trusted Advisor notifications to receive weekly emails about any changes. You can also subscribe to Business and Enterprise-level support to access the full suite of Trusted Advisor best-practice checks.
* **Amazon VPC Flow Logs** - Many AWS services provide built-in access control audit trails and logs. You can enable Amazon VPC Flow Logs to capture information about the IP traffic going to and from network interfaces in your VPC. VPC flow logs can help you with a number of tasks. For example, you can troubleshoot why specific traffic is not reaching an instance, which in turn helps you diagnose overly restrictive security group rules. You can also use flow logs as a security tool to monitor the traffic that is reaching your instance.
* **AWS Security Hub** - gives you a single pane of glass view of your high-priority security alerts and compliance status across AWS accounts. It provides you a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. This service is currently in a preview period at no cost to you.

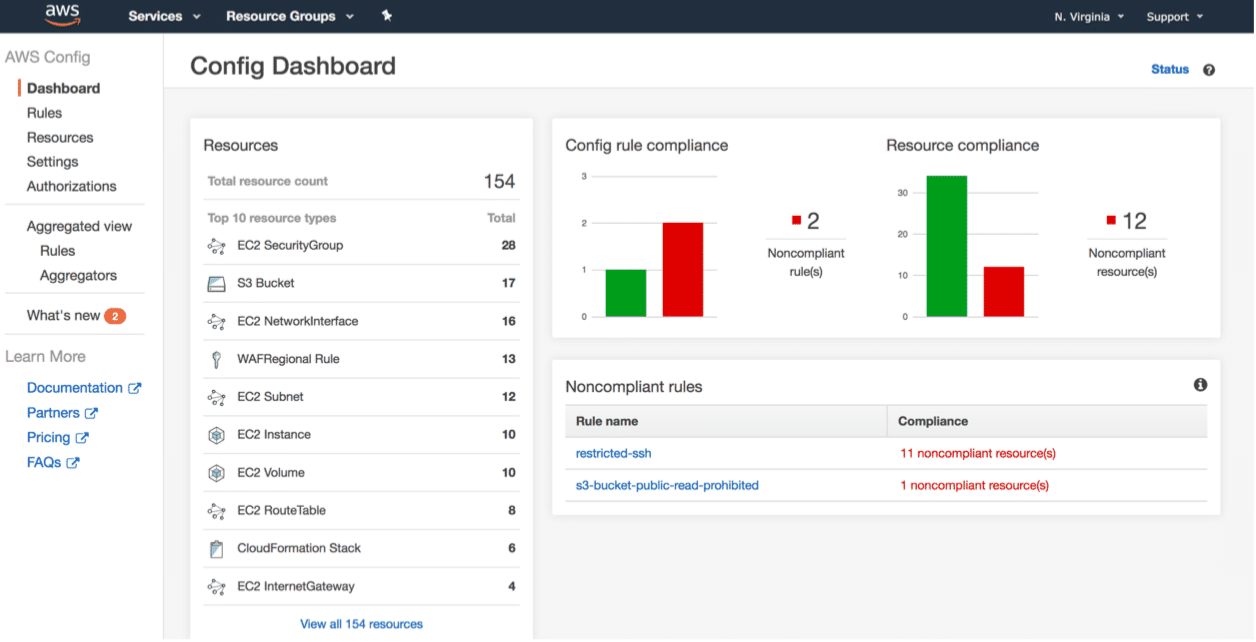




**AWS Config -** a continuous monitoring and assessment service that can help you detect non-compliance configurations almost in real time. You can view the current and historic configurations of a resource and use this information to troubleshoot outages and conduct security attack analyses.

<https://aws.amazon.com/config/>

**AWS Config Dashboard.**



With AWS Config rules, you can run continuous assessment checks on your resources to verify that they comply with your own security policies, industry best practices, and compliance standards. AWS provides several managed pre-built rules that require minimal to no configuration. For example, AWS Config provides a rule to ensure that encryption is turned on for all EBS volumes in your account. You can also write a custom AWS Config rule to essentially “codify” your own corporate security policies.

*“AWS Config is like a tattletale: You will know everything that happens in your AWS account.”*

Marcio Morales - Senior AWS Solution Architect

**Infrastructure Protection**

**Protection via Isolation -** Infrastructure protection ensures that systems and resources within your workloads are protected against unintended and unauthorized access, and other potential vulnerabilities. Amazon Virtual Private Cloud (Amazon VPC) allows you to isolate your AWS resources in the cloud. A VPC enables you to launch resources into a virtual network that you've defined and that closely resembles a traditional network that you'd operate in your own data center.

Here we have the most common VPC features that provide a defense-in-depth approach for your resources. Please review each item for more information.

* **Network ACLs** - To further add a layer of security within your VPC, you can configure network ACLs. A network access control list (ACL) is an optional layer of security for your VPC that acts as a firewall for controlling traffic at the subnet level. Your VPC automatically comes with a modifiable default ACL. By default, it allows all inbound and outbound IP traffic. To control traffic, you need to add ALLOW and DENY rules for specific IP addresses, protocols, and ports.
* **Security Group** - A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. When you launch an instance in a VPC, you must specify a security group for the instance. For each security group, you add one set of rules that control the inbound traffic to instances, and a separate set of rules that control the outbound traffic. Security groups are stateful: responses to allowed inbound traffic are allowed to flow outbound regardless of outbound rules, and vice versa. No inbound traffic is allowed until you configure inbound rules to your desired security group. Traffic can be restricted by IP, protocol, service, port, and source/destination IP address.
* **Subnet Routing** - Subnets enable you to group instances and AWS resources based on your security and operational needs. You can have all instances launched in a subnet receive a public IPv4 address, or an IPv6 address, or both. A subnet also allows you to configure routing for your network. With routing, you can specify targets for your resources and whether they can be reached via the Internet.

**Application and OS Security**

Securing your network and making sure that all your servers are hardened and properly patched are some of the tasks required in infrastructure security. AWS Systems Manager includes capabilities that help you automate management tasks such as collecting system inventory, applying operating system patches, maintaining up-to-date anti-virus definitions, and configuring operating systems and applications at scale. Systems Manager helps keep your systems compliant with your defined configuration policies.

**AWS Systems Manager Features**

Some of the features provided by the AWS Systems Manager:

* **Automation** - Safely automate common and repetitive IT operations and management tasks across AWS resources.
* **Inventory** - Collect information about your instances and the software installed on them, helping you understand your system configurations and installed applications. Collected data includes applications, files, network configurations, updates, and any other system properties.
* **Patch Manager** - Deploy software patches automatically across large groups of Amazon EC2 or on-premises instances.
* **Parameter Store** - A centralised store to manage your configuration data, whether plain-text data such as database strings or secrets such as passwords. This allows you to separate your secrets and your configuration data from your code.
* **Run Command** - Manage instances remotely at scale without logging into your servers. It provides a simple way of automating common administrative tasks across groups of instances such as registry edits, user management, and software and patch installations.
* **Session Manager** - Manage Windows and Linux EC2 instances via a browser-based interactive shell or CLI, without the need to open inbound ports, manage SSH keys, or you Bastion hosts.

*“AWS Systems Manager provides a tool to help with automating operations with things like patch deployment, deploying automation scripts to your instances, and a lot more. Doing these sorts of tasks manually, one instance at a time, is like inviting the elusive creatures that cause you to get paged at 3 AM directly into your metaphorical server room. Through the use of Systems Manager, you can push patches and scripts to be run on an instance, or group of instances, in an automated fashion to avoid logging directly into a production box to make those changes.”*

Morgan Willis - Senior AWS Technical Trainer

**Additional AWS Services for Infrastructure Protection**

Each of the AWS services listed below can be used to provide protection for your network and infrastructure:

* **AWS Firewall Manager** - a security management service that allows you to centrally configure and manage AWS WAF rules across your accounts and applications. Firewall Manager is able to bring new applications and resources into compliance with a common set of security rules from the start.
* **AWS Direct Connect** - a cloud service solution that is used to establish a dedicated and secure network connection from your premises to AWS. Using AWS Direct Connect, you can establish private connectivity between AWS and your data center, office, or colocation environment. In many cases, this can reduce your network costs, increase bandwidth throughput, and provide a more consistent network experience than internet-based connections.
* **AWS CloudFormation** - automates and simplifies the task of repeatedly creating and deploying AWS resources in a consistent manner. With AWS CloudFormation, you can ensure that all of your security and compliance controls are deployed along with your new environment.

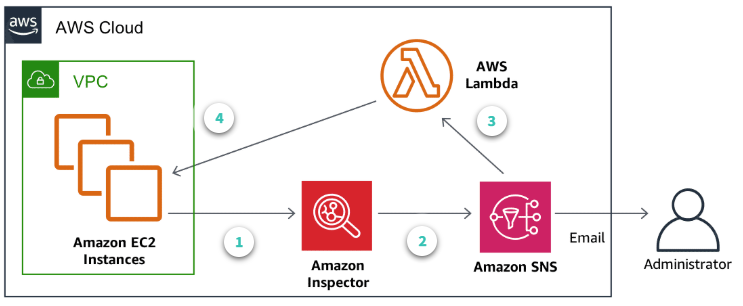




**Amazon Inspector**

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. It assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity.

<https://aws.amazon.com/inspector/>



1. **Findings** - Amazon Inspector runs assessments on a group of EC2 instances
2. **Notifications** - Security findings are then sent to an Amazon SNS to notify the administrator.
3. **AWS Lambda function** - A Lambda function is invoked by those same notifications. It examines the findings from Amazon Inspector.
4. **AWS Systems Manager** - The Lambda function uses AWS Systems Manager to patch the EC instances with the latest updates as a remediation to the findings.

Using Amazon Inspector with AWS Lambda allows you to automate certain security tasks. Combining these capabilities allows you to build event-driven security automation to help better secure your AWS environment in near real time. The diagram above illustrates a solution that automatically remediates findings generated by Amazon Inspector.

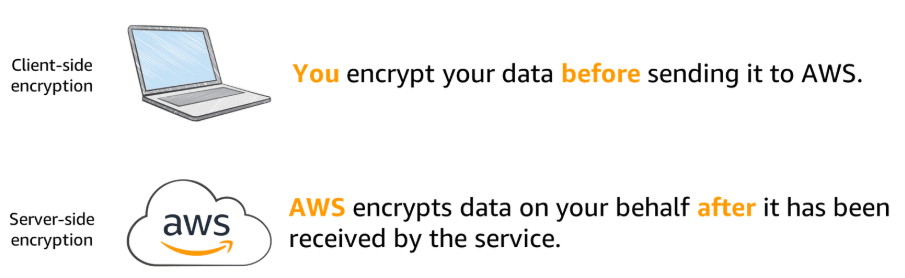
Additional information on this specific use case:

<https://aws.amazon.com/blogs/security/how-to-remediate-amazon-inspector-security-findings-automatically/>

**Data Protection**

**Protection at Rest**

Protecting data at rest has to do with encrypting data while using one of our storage services, including our database services. When it comes to Amazon S3, for example, there are two types of encryption options available:



The option you choose depends on who will be managing and/or providing the keys used in encryption.

**Protection in Transit**

Any data that gets transmitted from one system to another is considered data in transit. AWS recommends the following solutions and best practices to help you provide the appropriate level of protection for your data in transit, including the confidentiality and integrity of your application’s data.

* AWS services provide HTTPS endpoints using TLS for communication, thus providing end-to-end encryption when communicating with the AWS APIs.
* Use AWS to generate, deploy, and manage public and private certificates used for TLS encryption in web-based workloads.
* Use IPsec with VPN connectivity into AWS to facilitate encryption of traffic.

**Additional AWS Services for Data Protection**

Each of the AWS services listed below can be used to provide protection for your data:

* **AWS CloudHSM** - provides hardware security modules (HSM) in the AWS Cloud. An HSM is a computing device that processes cryptographic operations and provides secure storage for cryptographic keys. CloudHSM allows you to generate, store, import, export, and manage cryptographic keys, including symmetric keys and asymmetric key pairs.
* **Amazon S3 Glacier** - a storage service optimized for infrequently used data, also called cold data. This service provides durable and extremely low-cost storage with security features for data archiving and backup. Amazon S3 Glacier stores data as archives within vaults. You can enforce compliance controls for individual Amazon S3 Glacier vaults with a vault lock policy.
* **AWS Certificate Manager** - handles the complexity of creating and managing public SSL/TLS certificates for your AWS based websites and applications. ACM can also be used to issue private SSL/TLS X.509 certificates that identify users, computers, applications, services, servers, and other devices internally.
* **Amazon Macie** - uses machine learning to automatically discover, classify, and protect sensitive data in AWS. Macie recognizes sensitive data such as personally identifiable information (PII) or intellectual property. It provides you with dashboards and alerts that give visibility into how this data is being accessed or moved.





**AWS KMS**

AWS Key Management Service is a managed service that allows you to create and control the keys used in data encryption. If you want a managed service for creating and controlling encryption keys, but do not want or need to operate your own hardware security module (HSM), consider using AWS KMS. You can use the key management and cryptographic features directly in your applications or through AWS services that are integrated with AWS KMS, including AWS CloudTrail, which helps meet your auditing, regulatory, and compliance needs.

*“Let’s say you need to encrypt some data. You encrypt that data with a key to create a cipher text. Now it’s time to store the data key, but you need a way to encrypt it as well, so that not just anyone can decrypt your data. So you create another key, which you use to encrypt the data key. But what about the key you just created? You should probably encrypt that too. And what about the key used for that? This could go on for a while. What you really need is a place to store your master key so you know it’s safe. AWS KMS makes this process of storing and retrieving encryption keys significantly easier to manage.”*

Morgan Willis - Senior AWS Technical Trainer

**Incident Response**

There are obvious differences between environments built to run in the cloud and environments running on-premises. When it comes to incident response, the same can be said. Incident response in the AWS Cloud is faster, cheaper, more effective, and simpler to manage. Your ability to detect, react, and recover can be significantly enhanced with AWS. Let's take a look at some capabilities for investigation that are only possible by using AWS.

**The Power of APIs for Automation**

In AWS, you can use APIs to automate many of the routine tasks that need to be performed during incident response. For example, using a single command, you can isolate an instance by changing the security groups associated with the instance.

**Performing Forensics on Data Volumes**

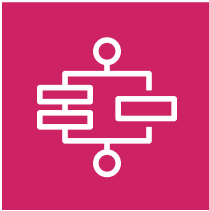
Forensics often requires capturing the disk image or "as-is" configuration of an operating system. You can use Amazon EBS snapshots and the Amazon EC2 APIs to capture the data and state of systems under investigation.

**Operating in a Clean Room**

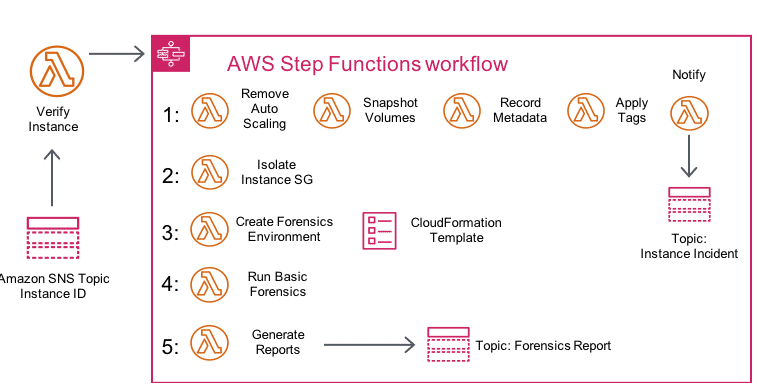
AWS CloudFormation can be used to quickly create a new, trusted environment in which to conduct deeper investigation. AWS CloudFormation can deploy preconfigured instances in an isolated environment that contains all the necessary tools forensic teams need to determine the cause of the incident.

*“The biggest vulnerability in any organization are humans. I’m not prejudiced against humans, some of my best friends are humans, but human beings have no business deploying infrastructure [when compared to AWS CloudFormation]. There are too many ways smart people can make mistakes. The “smart” part is irrelevant, it is the “people” part that will always let you down.”*

Blaine Sundrud - Senior AWS Instructional Designer



**AWS Step Functions**

AWS Step Functions lets you coordinate multiple AWS services into serverless workflows so you can build and update apps quickly. Workflows are made up of a series of steps, with the output of one step acting as the input into the next. Step Functions can be used to design and run workflows that stitch together services such as AWS Lambda and AWS CloudFormation to respond to an incident in the cloud.

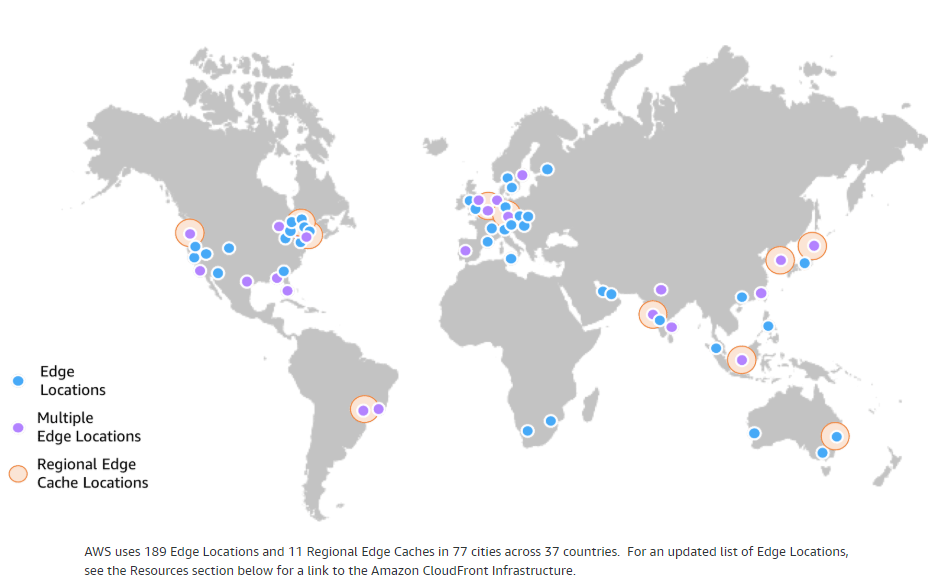
Here we have an example of how to respond to a compromised instance using AWS Step Functions, AWS Lambda, AWS CloudFormation, and Amazon SNS. We start with a script, or third-party tool, pushing instance IDs to an SNS topic. IDs are then verified by a Lambda function, and if compromised, a Step Function workflow is initiated.

1. The instance is removed from its auto scaling group, a snapshot is created of any attached EBS volume, instance metadata (like IP, AMI ID, subnets. etc.) is recorded, a quarantine resource tag is applied to the instance, and the team is notified.
2. The instance is isolated by removing all its previously associated security groups. Then, a new forensics security group is assigned to the instance with no ingress or egress permissions.
3. An AWS CloudFormation template is used to create a brand new environment, including a new VPC containing a forensics instance with prebuilt tools attached to a copy of any volumes from the snapshots.
4. A basic forensics investigation is performed on the attached volumes.
5. Reports are then generated with the results from the investigation and sent to the team via an SNS topic.

**DDoS Mitigation**

**Protection at the Edge**

A combination of AWS services may be used to implement a defense in depth strategy when it comes to DDoS attacks. These services are designed with an automatic response to DDoS attacks and can help minimize time to mitigate and reduce impact. AWS Edge locations provide an additional layer of network infrastructure that increases your ability to absorb DDoS attacks and to isolate faults while minimizing availability impact.



Edge locations are physical data centers located in key cities, that are different from Availability Zones. As access to certain data increases with time, this data is copied to an edge location near your customer base for better performance and latency. Threats can then be taken care of at these edge locations, away from your web applications, AWS resources, and the original data.

**AWS Services for Out-of-Region Protection**

The AWS services listed below work seamlessly together to create a flexible, layered security perimeter against multiple types of DDoS attacks. All of these services reside at the AWS Edge and provide a scalable, reliable, and high-performance security perimeter for your applications and content.

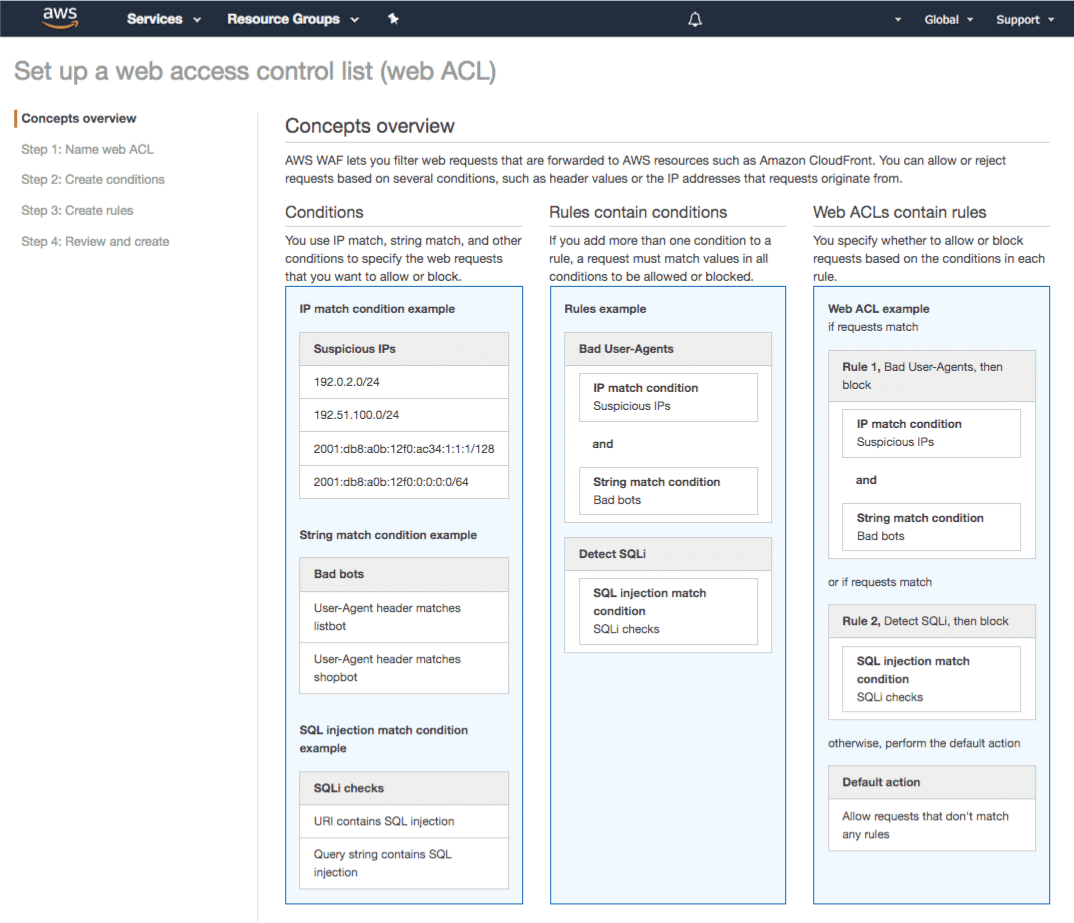
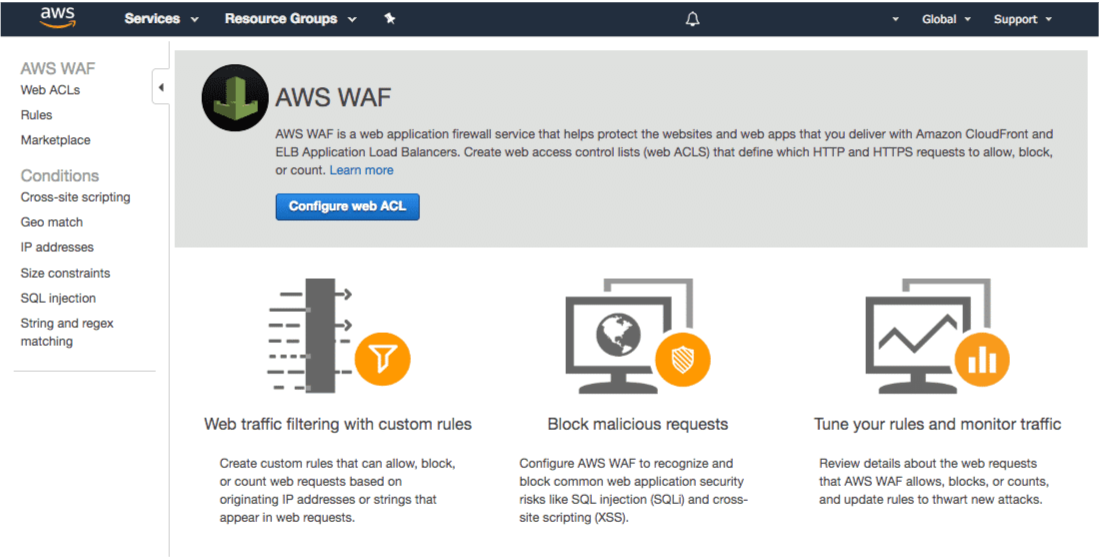
* **Amazon Route 53** - a highly available and scalable DNS service that can be used to direct traffic to your web application. It includes many advanced features like traffic flow, latency-based routing, weighted round-robin, Geo DNS, health checks, and monitoring. You can use these features to improve the performance of your web application and to avoid site outages. Route 53 is hosted at numerous AWS edge locations, creating a global surface area capable of absorbing large amounts of DDoS traffic.
* **Amazon CloudFront** - a content delivery network (CDN) service that can be used to deliver data, including your entire website, to end users. CloudFront only accepts HTTPS and HTTP well-formed connections to prevent many common DDoS attacks. These capabilities can greatly improve your ability to continue serving traffic to end users during larger DDoS attacks.
* **AWS Shield** - a managed DDoS protection service that safeguards web applications that run on AWS. AWS Shield provides always-on detection and automatic inline mitigations that minimize application downtime and latency.





**AWS WAF**

AWS Web Application Firewall (WAF) helps protect your web applications from common web exploits that could affect application availability, compromise security, or consume excessive resources. AWS WAF gives you control over which traffic to allow or block by defining customizable web security rules.



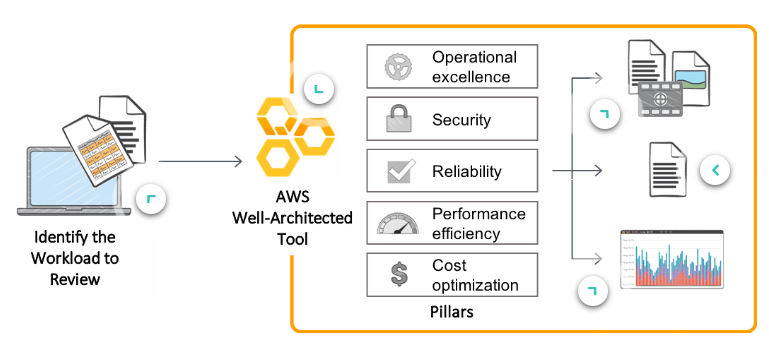
*“There really is no reason to not use a web application firewall this day in age. DDOS attacks are more common than ever and you should be taking every precaution you can to secure your environment from attacks. AWS WAF can help you create rules to protect your environment. These rules can be things like filtering HTTP traffic that is trying to use SQL injection, or filtering HTTP floods. Just about anyone can rent a bot army online to try to take down your servers, and that means you should be using AWS WAF and AWS Shield to protect your resources online.”*

Morgan Willis - Senior AWS Technical Trainer

**AWS Well-Architected Tool**

The AWS Well-Architected Tool is a self-service tool that is designed to help customers review AWS workloads at any time, without the need for an AWS Solutions Architect. By using this tool, you can review your workloads using a consistent process, understand potential risks in your workload architectures, and identify next steps for improvement.

**How it works**

****

* Define your workload - To define your workload, you must answer a series of questions regarding your architecture. A workload is the collection of resources and code that make up a cloud application.
* The Five Pillars - The tool will evaluate your responses against the five pillars of the Well-Architected Framework and provide an improvement plan with a prioritised list of issues for the workload. We recommend performing a workload review at major milestones in your development cycle.
* AWS Best Practices - Get videos and documentation related to AWS best practices and step-by-step guidance on how to build better workloads for the cloud.
* Reports - Generate a report that summarises your workload review. Use these reports to identify next steps for improvement, drive architectural decisions, and bring architecture considerations into your corporate governance process.
* Dashboard - View the results of workload reviews across your organisation in a single dashboard. Use the AWS Well-Architected Tool to support continuous improvement throughout the workload lifecycle.

First define your workload, then answer a set of questions across the five pillars of the Well Architected Framework: Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization. The AWS Well-Architected Tool then provides a plan describing the improvements that can be applied to the workload. There’s no charge for the AWS Well-Architected Tool; you pay only for any AWS resources that you consume. However, the tool is only available in select regions.

**Next Steps...**

Once you have completed this course, your next steps should be to attend the Architecting on AWS and Security Engineering on AWS instructor-led courses, in that order. The services and concepts that were introduced to you here will be discussed in more detail in these two courses.

**Course Objectives**

**Architecting on AWS**

* Make architectural decisions based on AWS architectural principles and best practices.
* Use AWS services to make your infrastructure scalable, reliable, and highly available.
* Use AWS Managed Services to enable greater flexibility and resiliency in an infrastructure.
* Make an AWS-based infrastructure more efficient to increase performance and reduce costs.
* Use the Well-Architected Framework to improve architectures with AWS solutions.

<https://www.aws.training/training/schedule?courseId=10002>

**Security Engineering on AWS**

* Assimilate and use the AWS shared security responsibility model.
* Architect and build AWS application infrastructures that are protected against the most common security threats.
* Protect data at rest and in transit with encryption.
* Apply security checks and analyses in an automated and reproducible manner.
* Configure authentication for resources and applications in the AWS Cloud.
* Gain insight into events by capturing, monitoring, processing, and analyzing logs.
* Perform security assessments to ensure that common vulnerabilities are patched and security best practices are applied.

<https://www.aws.training/training/schedule?courseId=10021>

**References:**

**AWS Services per Region** - Provides a table with all AWS services and their availability per AWS Region.

<https://aws.amazon.com/about-aws/global-infrastructure/regions_az/?p=ngi&loc=2>

**AWS Global Infrastructure** - Number of AWS Regions and Availability Zones, including AWS Regions that are coming soon.

<https://aws.amazon.com/about-aws/global-infrastructure/>

**AWS & Sustainability** - Information on our long-term commitment to achieve 100% renewable energy usage for our global infrastructure.

<https://aws.amazon.com/about-aws/sustainability/?p=gi>

**Cloud Adoption Framework - Security**

Provides guidance for coordinating the different parts of organizations migrating to cloud computing.

<https://d1.awsstatic.com/whitepapers/AWS_CAF_Security_Perspective.pdf>

**AWS Shared Responsibility Model**

Contains more information and details.

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

**Our Data Centres**

More information on the four data centre security layers.

<https://aws.amazon.com/compliance/data-center/data-centers/>

**AWS Artifact**

<https://aws.amazon.com/artifact/>

**AWS Compliance Programs**

Complete list of compliance certifications and attestations, laws and regulations, and compliance alignments and frameworks supported by AWS.

<https://aws.amazon.com/compliance/programs/>

**AWS Compliance Center**

Central location of country-specific regulatory requirements regarding the adoption of AWS Cloud services.

<https://www.atlas.aws/>

**Compliance Best Practices and Workbooks**

Provides a comprehensive list of compliance resources including whitepapers, guides, and privacy statements.

<https://aws.amazon.com/compliance/resources/>

**AWS CIS Foundations Benchmark**

Provides guidance for configuring security options for a subset of AWS services.

<https://d1.awsstatic.com/whitepapers/compliance/AWS_CIS_Foundations_Benchmark.pdf>

**AWS Service Endpoints**

Provides information about which regions and endpoints are supported for each service.

<https://docs.aws.amazon.com/general/latest/gr/rande.html#ct_region>

**Supported AWS Services per Region**

Supported services per region in a tabbed format.

<https://aws.amazon.com/about-aws/global-infrastructure/regional-product-services/>

**AWS Secrets Manager**

<https://aws.amazon.com/secrets-manager/>

**AWS SSO**

<https://aws.amazon.com/single-sign-on/>

**AWS STS**

<https://docs.aws.amazon.com/STS/latest/APIReference/Welcome.html>

**AWS AD**

<https://aws.amazon.com/directoryservice/>

**AWS Organisations**

<https://aws.amazon.com/organizations/>

**Amazon Cognito**

<https://aws.amazon.com/cognito/>

**AWS IAM in Practice**

Whitepaper on IAM guidelines and best practices to get started with AWS IAM.

<https://aws.amazon.com/answers/security/aws-iam-in-practice/>

**Password Policies for IAM Users**

Provides steps on configuring password policies for the AWS Management Console, AWS APIs, and AWS CLI.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_passwords_account-policy.html>

**IAM Best Practices**

List of recommendations and tips to secure your AWS resources with AWS IAM.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html>

**AWS Config**

<https://aws.amazon.com/config/>

**Amazon CloudWatch Events**

Tutorials on how to create CloudWatch Events rules for certain tasks and targets.

<https://docs.aws.amazon.com/AmazonCloudWatch/latest/events/CloudWatch-Events-Tutorials.html>

**Security at Scale: Logging in AWS**

Guide on using AWS CloudTrail to achieve compliance by logging API calls and changes to resources.

<https://d1.awsstatic.com/whitepapers/compliance/AWS_Security_at_Scale_Logging_in_AWS_Whitepaper.pdf>

**Introduction to Auditing the Use of AWS**

Whitepaper on auditing on AWS best practices.

<https://d0.awsstatic.com/whitepapers/compliance/AWS_Auditing_Security_Checklist.pdf>

**AWS System Manager**

<https://aws.amazon.com/systems-manager/features/>

**AWS Firewall Manager**

<https://aws.amazon.com/firewall-manager/>

**AWS Direct Connect**

<https://aws.amazon.com/directconnect/>

**AWS Could Formation**

<https://aws.amazon.com/cloudformation/>

**Amazon Inspector**

<https://aws.amazon.com/inspector/>

**Overview of AWS Security - Network**

Provides an overview of the different methods used by AWS to secure your workload in the cloud

<https://d1.awsstatic.com/whitepapers/Security/Networking_Security_Whitepaper.pdf>

**Securing Your EC2 Instance**

Outlines a number of best practices for helping you secure your instances

<https://aws.amazon.com/articles/tips-for-securing-your-ec2-instance/>

**Amazon Inspector Assessments**

Description of all available tests performed by Amazon Inspector during an assessment

<https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html>

**AWS Systems Manager Use Cases**

Lists common use cases and best practices for AWS Systems Manager capabilities

<https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-best-practices.html>

**AWS CloudHSM**

<https://aws.amazon.com/cloudhsm/>

**Amazon S3 Glacier**

<https://aws.amazon.com/glacier/>

**AWS Certificate Manager**

<https://aws.amazon.com/certificate-manager/>

**Amazon Macie**

<https://aws.amazon.com/macie/>

**AWS KMS**

<https://aws.amazon.com/kms/>

**Protecting Data in Amazon S3**

Provides an overview of the different ways to protect your data in Amazon S3

<https://docs.aws.amazon.com/AmazonS3/latest/dev/DataDurability.html>

**AWS Encryption Videos**

Contains a list of AWS videos related to data encryption from past Re:Invent sessions and AWS Summits

<https://www.youtube.com/user/AmazonWebServices/search?query=encryption>

**AWS KMS Cryptographic Details**

This whitepaper provides details on the cryptographic operations that are executed within AWS when you use AWS KMS

<https://d0.awsstatic.com/whitepapers/KMS-Cryptographic-Details.pdf>

**VPN Connections Overview**

List of different options for VPN connectivity from your data center to the AWS Cloud

<https://docs.aws.amazon.com/vpc/latest/userguide/vpn-connections.html>

**Amazon EBS**

<https://aws.amazon.com/ebs/>

**AWS CloudFormation**

<https://aws.amazon.com/cloudformation/>

**AWS Step Functions**

<https://aws.amazon.com/step-functions/>

**Building a Cloud-Specific Incident Response Plan**

An AWS blog post discussing an example of the steps required to build an incident response plan

<https://aws.amazon.com/blogs/publicsector/building-a-cloud-specific-incident-response-plan/>

**AWS Incident Response Videos**

Contains a list of AWS videos related to incident response on AWS from past Re:Invent sessions and AWS Summits

<https://www.youtube.com/user/AmazonWebServices/search?query=incident+response>

**Amazon Route 53**

<https://aws.amazon.com/route53/>

**Amazon CloudFront**

<https://aws.amazon.com/cloudfront/>

**AWS Shield**

<https://aws.amazon.com/shield/>

**AWS WAF**

<https://aws.amazon.com/waf/>

**AWS Best Practices for DDoS Resiliency**

Whitepaper on different mitigation techniques and information on how to reduce your attack surface

<https://d0.awsstatic.com/whitepapers/Security/DDoS_White_Paper.pdf>

**AWS Edge Locations**

Provides more information on AWS Edge locations, including a list of cities where Edge locations are hosted

<https://aws.amazon.com/cloudfront/features/>

**AWS Well-Architected Tool**

<https://console.aws.amazon.com/wellarchitected/>

**AWS Well-Architected Tool FAQ**

<https://aws.amazon.com/well-architected-tool/faqs/>

**AWS Well-Architected Tool User Guide**

Provides details on the AWS Well-Architected Framework and instructions on how to properly use the tool

<https://docs.aws.amazon.com/wellarchitected/latest/userguide/wellarchitected-ug.pdf>

**AWS News Blog by Jeff Barr**

An AWS blog that covers an example of the steps required to use the AWS Well-Architected Tool

<https://aws.amazon.com/blogs/aws/new-aws-well-architected-tool-review-workloads-against-best-practices/>

**Getting Started Video**

This video provides a demo on using the AWS Well-Architected Tool

<https://d3nn3d4w2aqyem.cloudfront.net/mp4/Getting_started_video.mp4>

**AWS Well-Architected Partners**

Provides a list of AWS partners who can help you with hands-on experience architecting, building, migrating, and optimizing architectures that follow the AWS Well-Architected Framework

<https://aws.amazon.com/architecture/well-architected/partners/>