AWS Security Baseline Playbook

OVERVIEW

Security baseline playbook is the minimum security control every customer should implement, this address the following

- Auditability
- Network behaviour Analysis
- Governance & Compliance, Inventory & Configuration Visibility
- Audit Access Management
- Organization & Account level controls
- Threat Intelligence
- Vulnerability & Patch Management
- Centralised Alert/Event Management

DOCUMENT PURPOSE

This is the minimum security baseline setup for any size of account, this document is a self service resource. All the controls step by step configuration are provided. This is not limited to setup baseline, it also open threads on Log management, threat Management, Incident playbook creation & building forensic muscles.

AUDITABILITY: AWS IS COLLECTION OF THOUSANDS OF API, CLOUDTRAIL HELPS YOU ENABLE GOVERNANCE, COMPLIANCE, AND OPERATIONAL AND RISK AUDITING OF YOUR AWS ACCOUNT. ACTIONS TAKEN BY A USER, ROLE, OR AN AWS SERVICE ARE RECORDED AS EVENTS IN CLOUDTRAIL. EVENTS INCLUDE ACTIONS TAKEN IN THE AWS MANAGEMENT CONSOLE, AWS COMMAND LINE INTERFACE, AND AWS SDKS AND APIS.

USE CASES:

- Operational troubleshooting & RCA
- Enhance security analysis
- Monitor data exfiltration risks
- Simplify compliance workflow

1. ENABLE CLOUDTRAIL

Enable cloud trail by creating a trail using CloudTrail console. Follow the steps as per below link.

*If you have already enabled a trail in a Region, please proceed to Step-2

https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-create-a-trail-using-the-console-first-time.html#creating-a-trail-in-the-console

- Sign in to the AWS Management Console and open the CloudTrail console at https://console.aws.amazon.com/cloudtrail/.
- Choose the region where you want the trail to be created.
- Choose **Get Started Now**. If you do not see **Get Started Now**, choose **Trails**, and then choose **Create trail**.
- On the **Create Trail** page, for **Trail name**, type a name for your trail.
- For **Apply trail to all regions**, choose **Yes**
- For **Management events**, leave as default.
- For **Data events**, leave as default.
- For **Storage location**, for **Create a new S3 bucket**, choose **Yes**
- For **S3 bucket**, type a name for the bucket you want to designate for log file storage.
- leave **Advanced** setting as default.
- Choose **Create**.
- The new trail appears on the **Trails** page. The **Trails** page shows the trails in your account from all regions.

Question: How to Analyze CloudTrail Logs?

- Download logs from S3 manually & do the traditional grep - very primitive does not help much
- Use Athena on S3 to run SQL queries on CloudTrail
- CloudTrail logs are pushed to ElasticSearch for correlation & Monitoring
- CloudTrail Logs pushed to SIEM
- CloudTrail Logs are pushed to a 3rd Party log analysis system
- Use CloudWatch Logs Insights - built in SQL query engine

Configure CloudWatch Logs for CloudTrail

- Go back to your Trail
- Go to the Section **CloudWatch Logs**
- Click on **Configure**
- **New or existing log group,** leave default
- Click **Continue**
- Click **Allow**

Question: What to look for in CloudTrail Logs

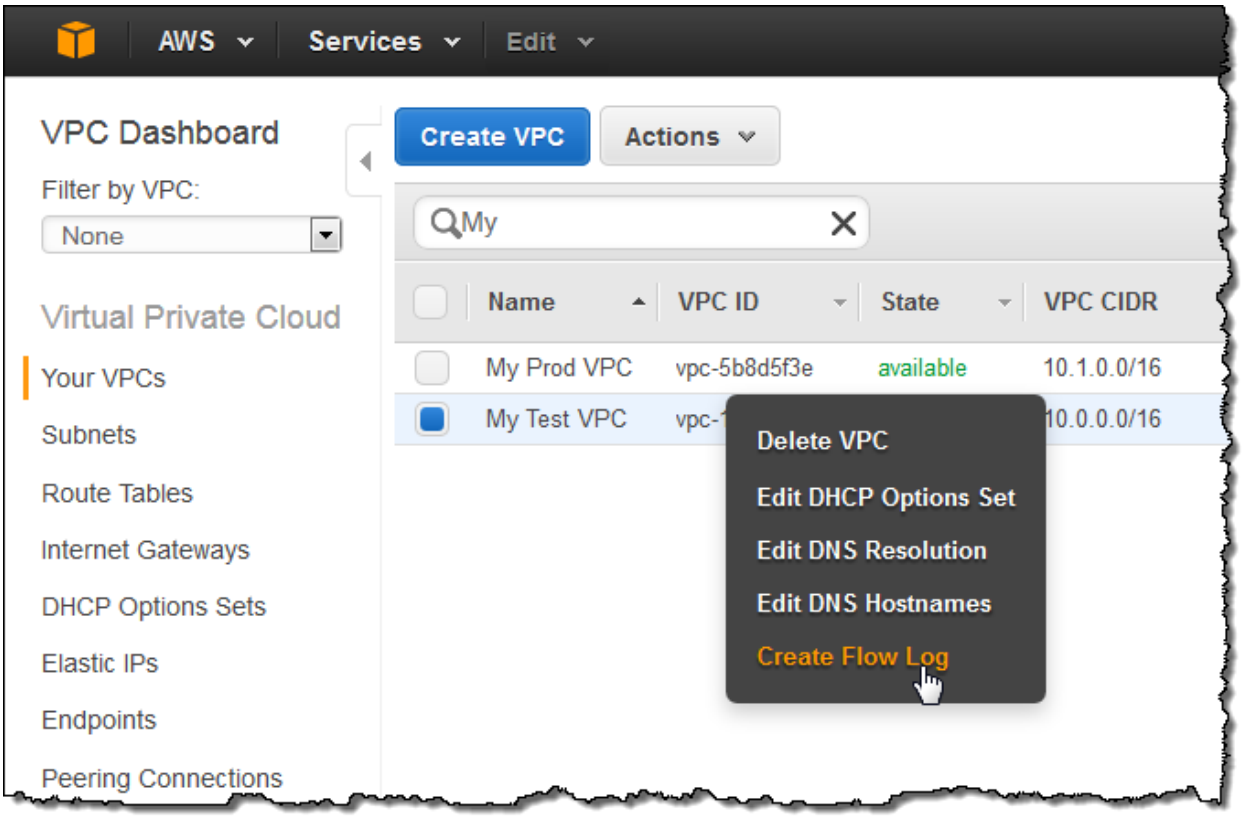
CloudTrail logs could be used to get information on events generated for configuration changes, security misconfigurations & Indicators of Compromise (Some examples)

- Configuration changes
- Anomalies in Privileges user account activity
- Geo irregularities
- Console login red flags

2. Setup Network & Access Behaviour analysis

VPC Flow Logs for Amazon Virtual Private Cloud enables you to capture information about the IP traffic going to and from network interfaces in your VPC. Flow Logs data can be published to Amazon CloudWatch Logs or Amazon Simple Storage Service (S3).

Enabling VPC Flow Logs
You can enable VPC Flow Logs from the AWS Management Console or the AWS Command Line Interface (CLI), Here's how you would enable them for a VPC:



Consideration: Understand Flow logs basics, formats & meta data: VPC Flow log basics

USE CASES:

- Troubleshooting connectivity issues across your VPCs
- Intrusion detection,
- Anomaly detection
- Archival for compliance purposes

Question: What to look for in VPC Flow Logs

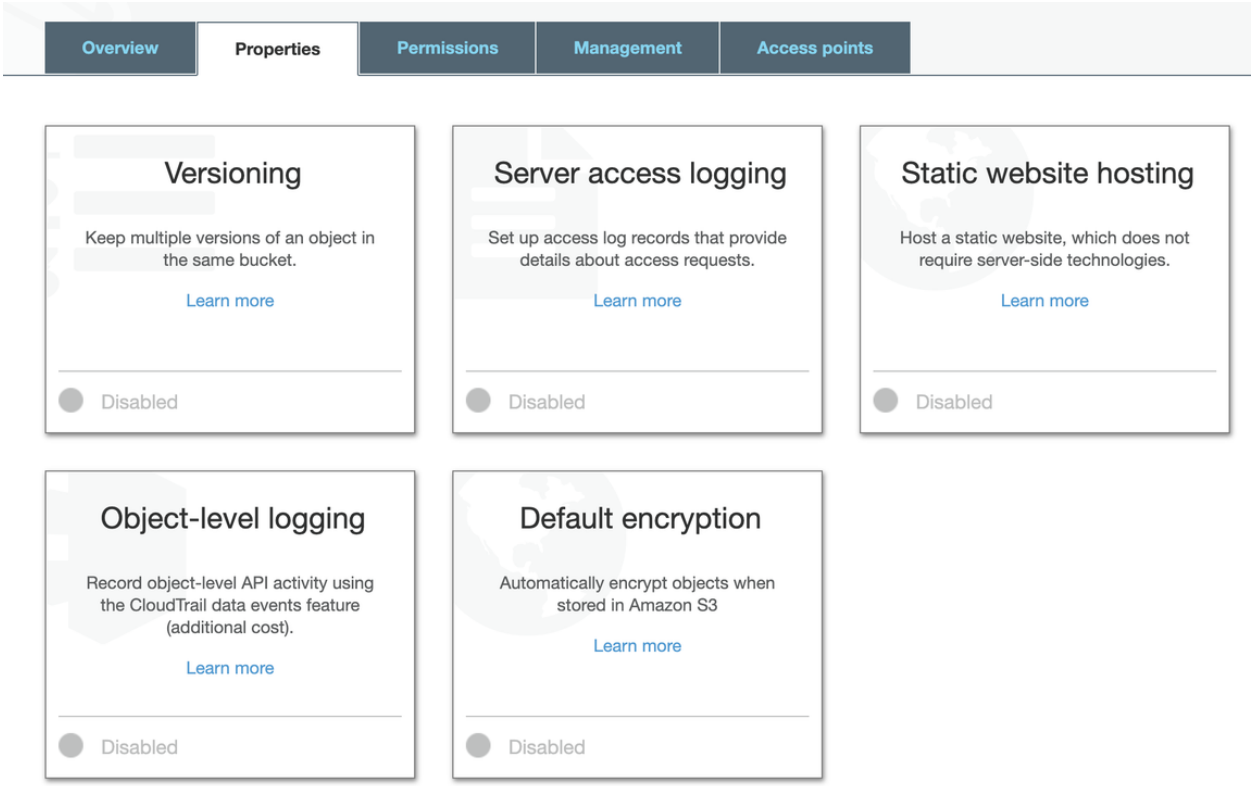
- Unusual outbound network traffic
- HTML response size
- Mismatched port & application traffic
- Signs of DDoS activity

Additional: Want to go deeper at header level: Consider VPC Traffic Mirroring

Question: How do you analyze VPC Flow logs

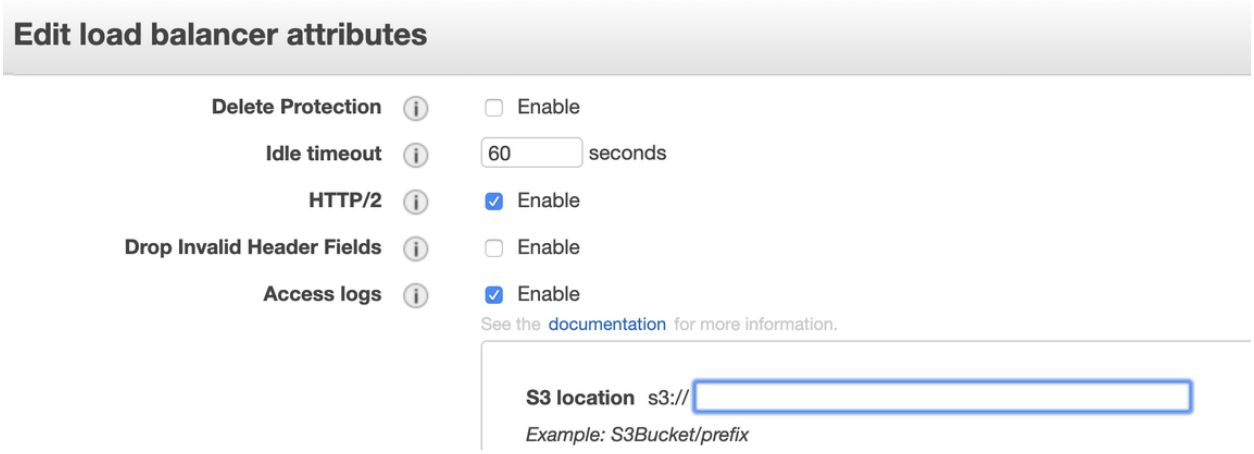
S3 ACCESS LOGS

Each access log record provides details about a single access request, such as the requester, bucket name, request time, request action, response status, and an error code, if relevant.



ALB ACCESS LOGS

Each log contains information such as the time the request was received, the client's IP address, latencies, request paths, and server responses. You can use these access logs to analyze traffic patterns and troubleshoot issues.



3. Account Access Audit

Who get **Access** to **What? AAA(Authentication, Authorization & Audit)**

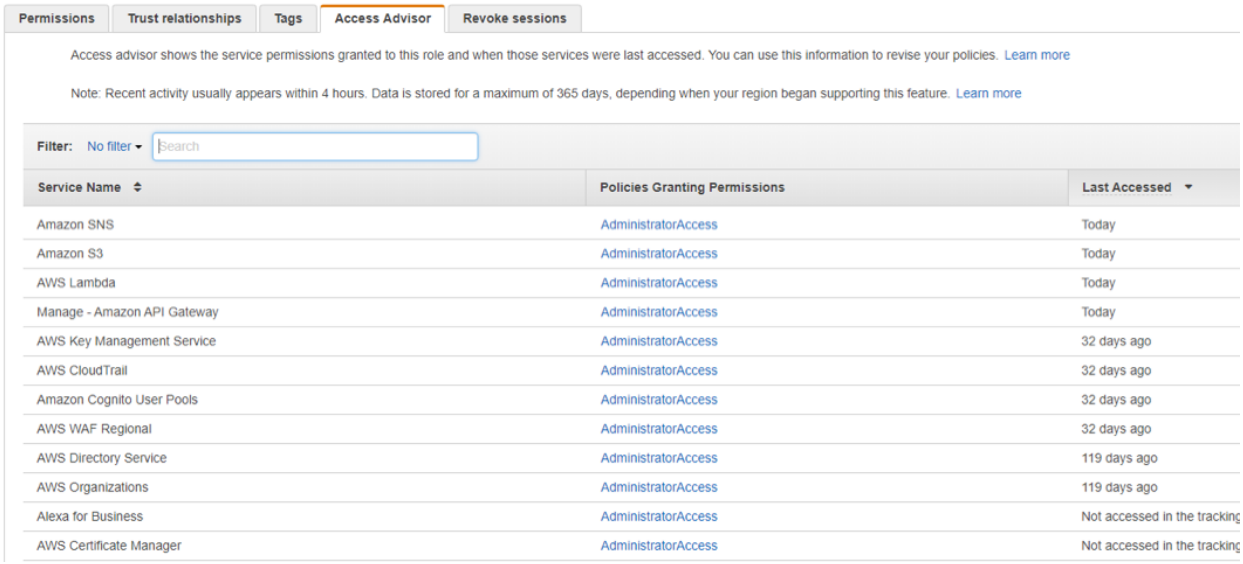
Identity & Access Management provides access to AWS resources, primarily through Users or Roles(in case of SSO, identity Federation etc.)

<u>Strive for Least Privilege Access - AWS Access Advisor</u>

Provides service last accessed information for services allowed through permissions, Available for IAM entities (users, roles, groups & IAM policies)

Determine services access record & restrict services not in use

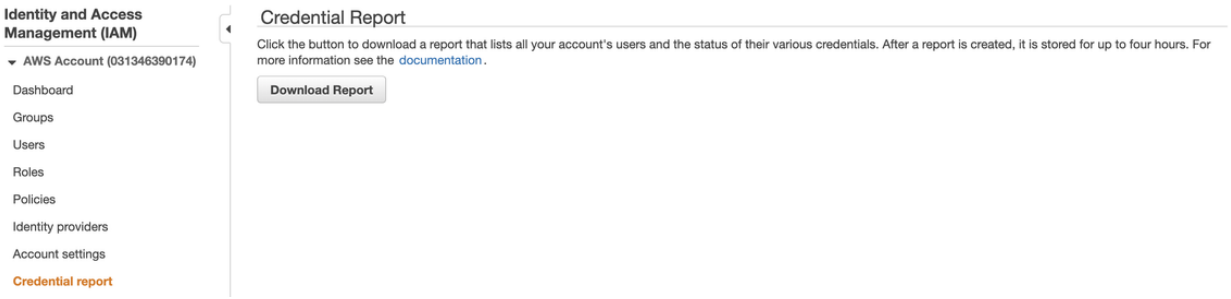
- Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam
- Choose Role or User in the left pane: click on Role or User
- Choose **Access Advisor** tab to check **Last Accessed**
- Remove unwanted service permissions from your policies



To Check users adhere to organization standards like: MFA, Password complexity

Credential Management

Check for MFA enforcement, Password policy enforcement & Key rotation



Access Analyzer

Access Analyzer is new feature that enables security team to continuously ensure that your policies only provide intended public & cross-account access to your resources such as S3, KMS Keys or Lambda functions.

- Sign in to the AWS Management Console and open the IAM console at https://console.aws.amazon.com/iam
- Choose Access Analyzer

Access Analyzer

Monitor access to resources

Create analyzer

How it works

1 Create an analyzer

The scope for the analyzer is your AWS account, which is your zone of trust. The analyzer scans all of the supported resources within your zone of trust.

2 Review active findings

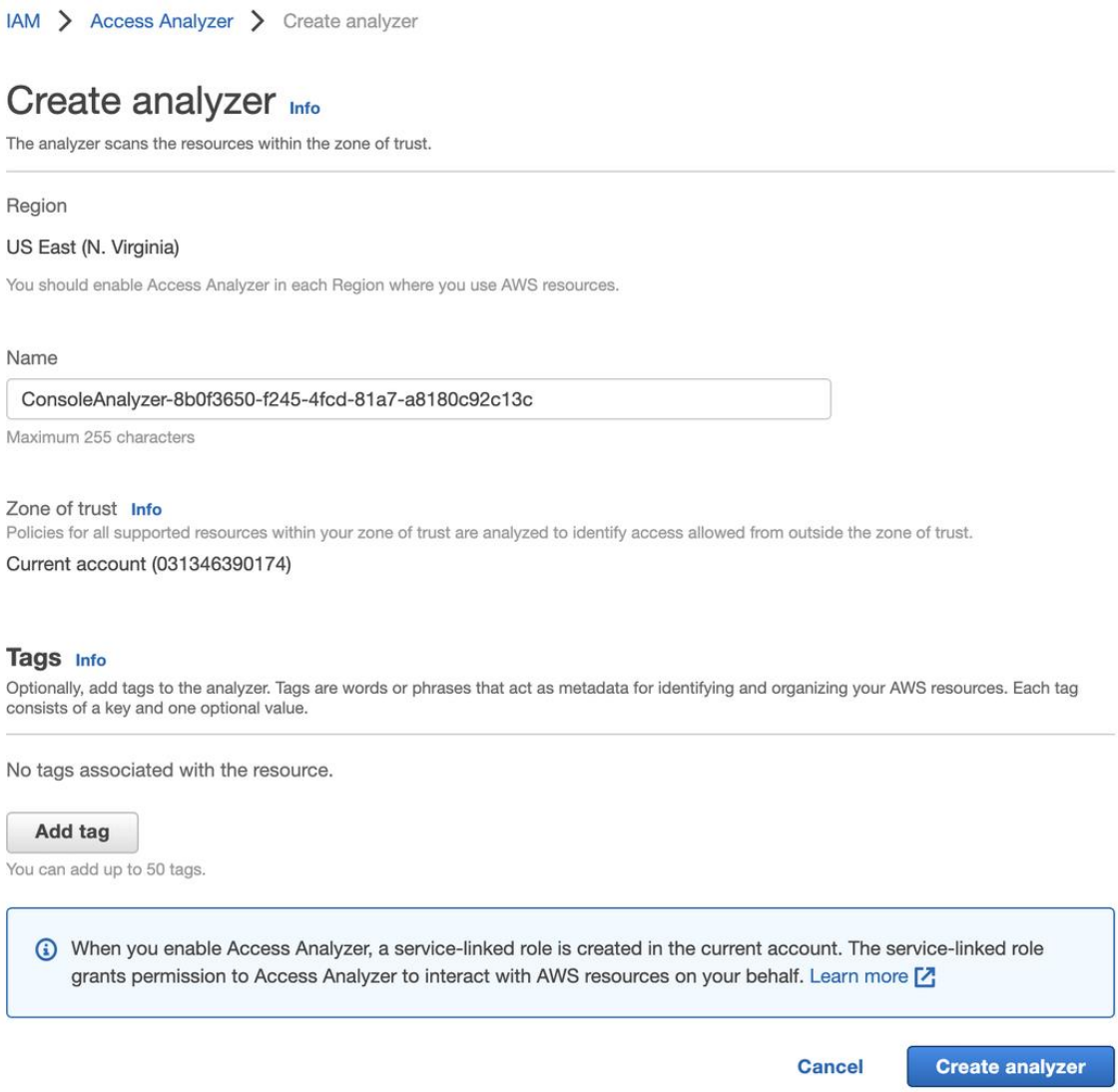
When Access Analyzer finds a policy that allows access to a resource from outside of your zone of trust, it generates an active finding. Findings include details about the access so that you can take action.

3 Take action

If the access is intended, you can archive the finding so that you can focus on reviewing active findings. If the access is not intended, you can resolve the finding by modifying the policy to remove access to the resource.

Getting started

- What is Access Analyzer?
- Access Analyzer User Guide



4. Governance, Regulation & Compliance

Starting point in security is visibility, visibility of environment configuration, configuration changes, Governance control & Compliance status

Enable AWS config

- Sign in to the AWS Management Console and open the AWS Config console in your desired region https://console.aws.amazon.com/config/.
- Choose **Get Started Now**.
- On the **Settings** page, for **Resource types to record**, under **All resources**
- Select **Record all resources supported in this region**
- Select **Include global resources**

- For **Amazon S3 Bucket**, select **Create a new bucket** – For **Bucket Name** there will be pre populated bucket either leave that as it is or type a name for your Amazon S3 bucket.
- Jump to **AWS Config Role**
- For **AWS Config role**, choose **Create AWS Config service-linked role** – AWS Config creates a role that has the required permissions. Select **NEXT**
- On **AWS Config rules page** it will show various rules, we can skip this for now select **SKIP**
- Click on **Review** AWS Config displays the **Config Dashboard** page as of now there will be no Resources or Rules
- AWS config is configured now.

USE CASES TO BE SOLVED

- **Resource Inventory**: Get resource inventory

Resources

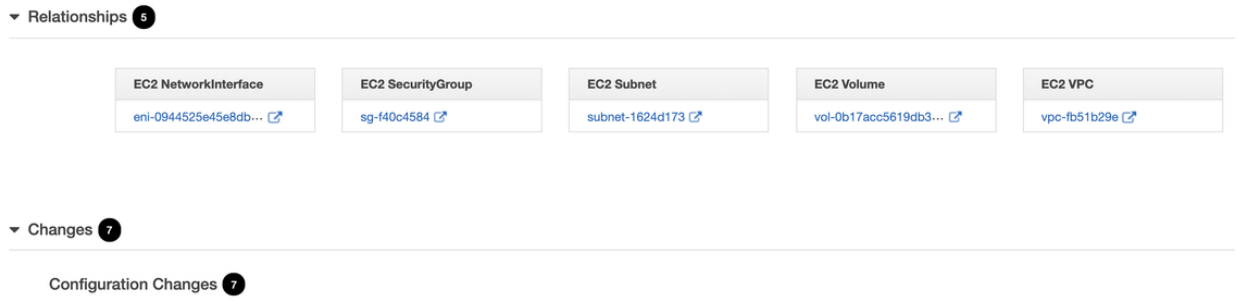
Total resource count	467

Top 10 resource types	Total
IAM Role	138
IAM Policy	48
EC2 SecurityGroup	41
Lambda Function	29
S3 Bucket	28
EC2 NetworkInterface	26
EC2 Subnet	22
EC2 Instance	17
EC2 Volume	17
EC2 RouteTable	14

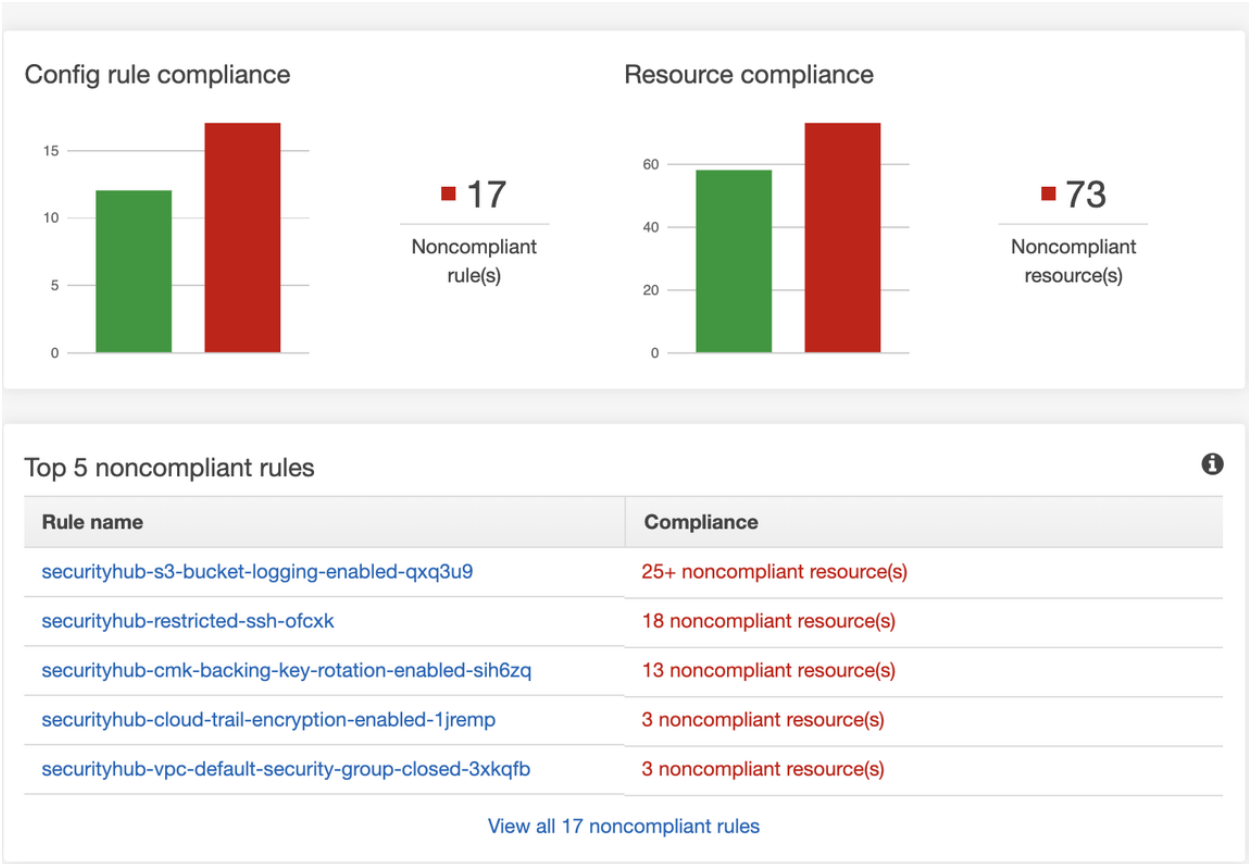
View all 467 resources

Run advanced queries against your resource configuration data.

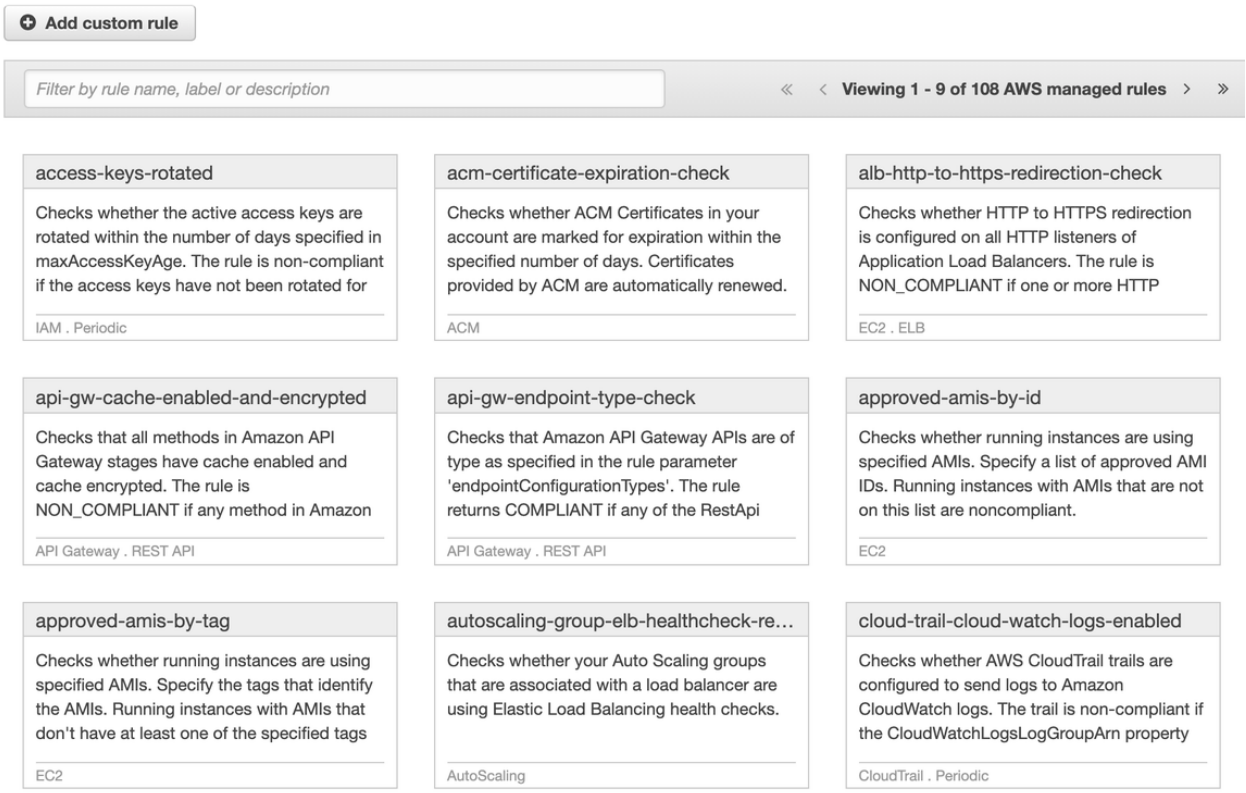
2. Resource Relationship Mapping & Configuration changes



3. **Compliance time line & Dashboard**

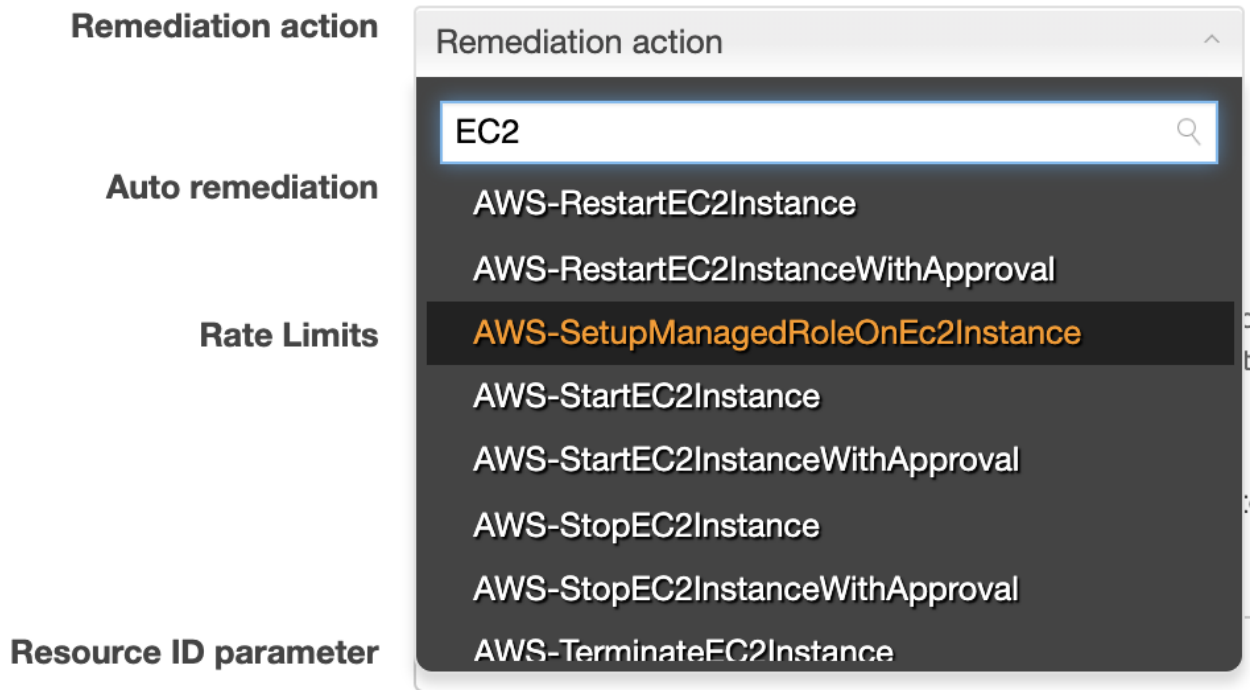


4. **Managed Rules for Compliance**



Also, you could write your own Rules or else just implement prewritten rules: https://github.com/awslabs/aws-config-rules/tree/master/python

5. On Non-compliance define **Remediation** action right from Config console



One of the lesser known but powerful feature of AWS Config is "**Advanced Query** " that helps to audit for compliance, manage cost & evaluate security. **Advanced Query** does not have additional cost.

Advanced Query offers query capabilities across your recourses using SQL Select statements

Sample SQL Queries
List all EC2 instances with AMI ID "ami-2a69aa47"
List all resources that are related to security group "sg-12345"
List all IAM users created between date "2018-12-01T00:00" and date "2019-10-10T00:00"
List all RDS DB Instances that are publicly accessible
List all S3 buckets where versioning is disabled

Example: To determine all running instances in an account

```sql
SELECT
    resourceId,
    resourceName,
    resourceType,
    configuration.instanceType,
    tags,
    availabilityZone,
    configuration.state.name
WHERE
    resourceType = 'AWS::EC2::Instance'
    AND configuration.state.name = 'running'
```

You can write your own SQL queries using the config schema https://github.com/awslabs/aws-config-resource-schema

5. Organization & Account level controls

Organizations helps you to centrally manage billing; control access, compliance, and security; and share resources across your AWS accounts.

IMPLEMENT AND ENFORCE CORPORATE SECURITY, AUDIT, AND COMPLIANCE POLICIES

Use AWS Organizations to implement Service Control Policy (SCP) permission guardrails to ensure that users in your accounts can only perform actions that meet your corporate security and compliance policy requirements. Additionally, you can configure central logging of all actions performed across your organization using AWS CloudTrail and centrally aggregate data for rules that you've defined using AWS Config, enabling you to audit your environment for compliance and react quickly to changes.

Service Control Policies: SCPs offer central control over the maximum available permissions for all accounts in your organization, allowing you to ensure your accounts stay within your organization's access control guidelines.

This helps in avoiding over engineering, look at some of the examples of SCP that are required by most of the customers

- Example 1: Prevent Users from Disabling AWS CloudTrail
- Example 2: Prevent Users from Disabling Amazon CloudWatch or Altering Its Configuration
- Example 3: Prevent Users from Deleting Amazon VPC Flow Logs
- Example 4: Prevent Users from Disabling AWS Config or Changing Its Rules
- Example 5: Prevent Any VPC That Doesn't Already Have Internet Access from Getting It
- Example 6: Denies Access to AWS Based on the Requested Region
- Example 7: Prevent IAM Principals from Making Certain Changes
- Example 8: Prevent IAM Principals from Making Certain Changes, with Exceptions for Admins
- Example 9: Require Encryption on Amazon S3 Buckets
- Example 10: Require Amazon EC2 Instances to Use a Specific Type
- Example 11: Require MFA to Stop an Amazon EC2 Instance
- Example 12: Restrict Access to Amazon EC2 for Root User

6. Threat Intelligence

Amazon GuardDuty is a threat detection service that continuously monitors for malicious activity and unauthorized behavior to protect your AWS accounts and workloads.

GuardDuty identifies threats by continuously monitoring the network activity and account behavior within the AWS environment. Amazon GuardDuty comes integrated with up-to-date threat intelligence feeds from AWS, CrowdStrike, and Proofpoint. Threat intelligence coupled with machine learning and behavior models help you detect activity such as crypto-currency mining, credential compromise behavior, communication with known command-and-control servers, or API calls from known malicious IPs.

Enable AWS GuardDuty

- In the AWS Management Console click on **Services** and go to GuardDuty https://console.aws.amazon.com/guardduty/.
- Choose **Get Started Now**. This will display Welcome to GaurdDuty
- Click on **Enable GaurdDuty**
- You will be taken to Findings Screen, GuardDuty is Configured

GuardDuty works on 3 data sources: CloudTrail Logs, VPC Flow Logs & DNS Query Logs

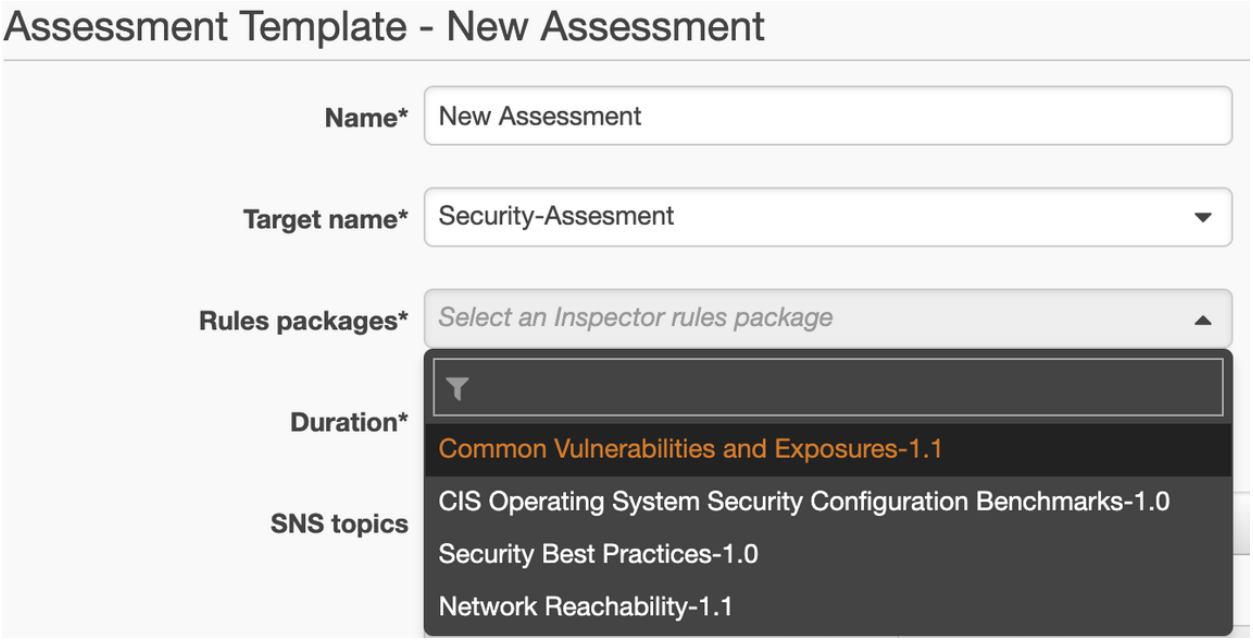
GuardDuty Finding Types: As of now there are 56 findings of the following types

- Backdoor Finding Types
- Behavior Finding Types
- CryptoCurrency Finding Types
- PenTest Finding Types
- Persistence Finding Types
- Policy Finding Types
- PrivilegeEscalation Finding Types
- Recon Finding Types
- ResourceConsumption Finding Types
- Stealth Finding Types
- Trojan Finding Types
- Unauthorized Finding Types

7. Vulnerability & Patch Management

Amazon Inspector is a security vulnerability assessment service that helps improve the security and compliance of applications deployed on Amazon EC2. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices, and then produces a detailed list of security findings prioritized by level of severity. Amazon Inspector includes a knowledge base of hundreds of rules mapped to common security standards and vulnerability definitions that are regularly updated by AWS security researchers.

Select Rule Package



Inspector offers EC2 host assessment & Network Reachability assessment

Inspector uses SSM agent for EC2 host assessment, Network Reachability has two modes

Agentless network assessments
Find externally accessible EC2 instances (internet, VPN, peering), ex. SSH open to internet

Enhanced - with agent
Using Agent, will get information about software listening on the ports

******Inspector is not available in Singapore region as of January 2020, use AWS Marketplace options like Qualys Nessus

PATCH MANAGEMENT

AWS Systems Manager Patch Manager automates the process of patching managed instances with both security related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications.

How it works

1. Use default patch baselines, or create your own
2. Organize instances into patch groups (optional)
3. Automate the patching schedule by using Maintenance Windows
4. Monitor patch status to ensure compliance

Benefits and features

Automate Patching

Automate patching to ensure that your instances stay up to date.

Create patch baselines

Create custom patch baselines for each operating system, or use Systems Manager default patch baselines.

Define approval rules

Create rules to specify which patches are approved for deployment.

Monitor compliance

View reports to determine whether any instances are not in compliance with the current patch baseline.

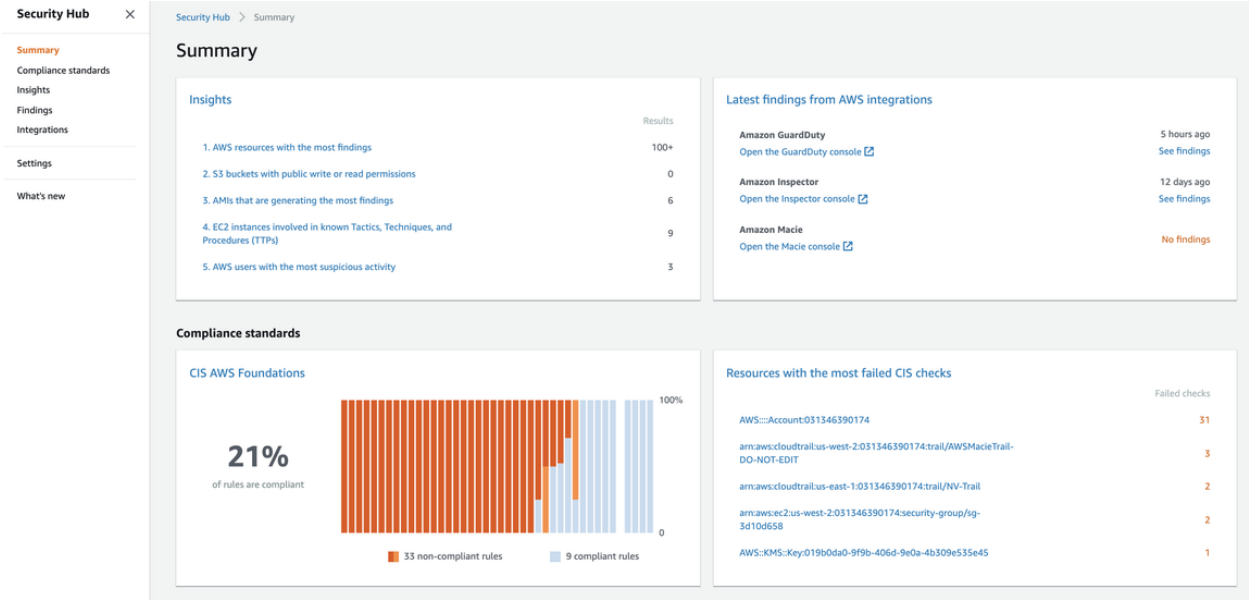
[Simplify Security Assessment Setup Using Amazon EC2 Systems Manager and Amazon Inspector]

8. Centralized Alert & Event Management: Bringing it all together

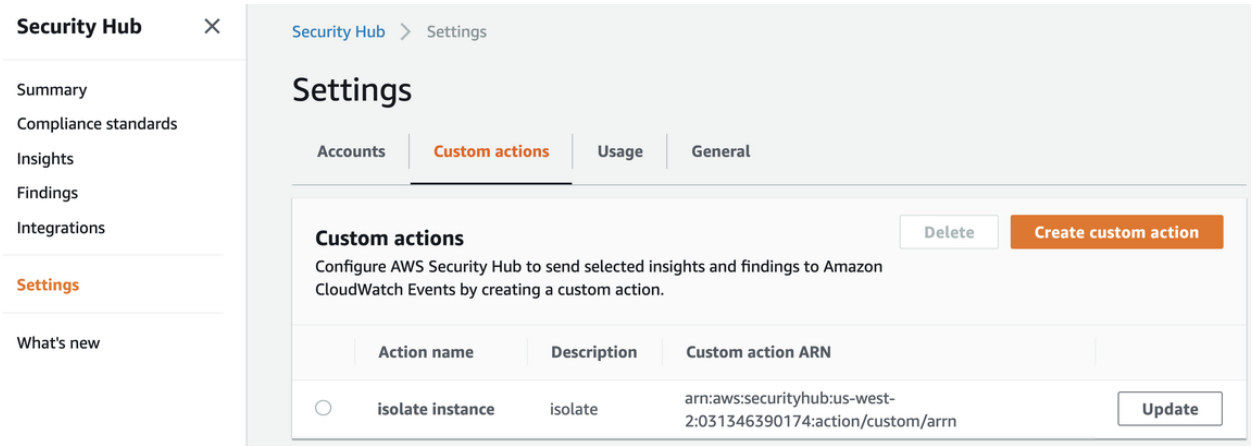
AWS Security Hub gives a comprehensive view of high-priority security alerts and compliance status across AWS accounts. With Security Hub, you now have a single place that aggregates, organizes, and prioritizes your security alerts, or findings, from multiple AWS services, such as Amazon GuardDuty, Amazon Inspector, and Amazon Macie, as well as from AWS Partner solutions. Your findings are visually summarized on integrated dashboards with actionable graphs and tables. You can also continuously monitor your environment using automated compliance checks based on the AWS best practices and industry standards your organization follows. Get started with AWS Security Hub in just a few clicks in the Management Console and once enabled, Security Hub will begin aggregating and prioritizing findings.

Enable AWS Security Hub

- In the AWS Management Console click on **Services** and go to GuardDuty https://console.aws.amazon.com/securityhub/
- Choose **Get Started Now**. This will display Welcome to GaurdDuty
- Click on **Enable Security Hub**



Create Custom Actions from Security Hub like isolate instance



Integrate your existing Security solutions with Security Hub