Wifi / Password

Wifi name:
TDPK-WIFI

Username:
AWS-Workshop-1
AWS-Workshop-2
AWS-Workshop-3

Password
Welcome@2022

https://github.com/TIDC-PS-Inter/AWS-Workshop

Part 1

AWS Workshop Series

Day 2: Security on AWS

Taking Enterprise Beyond the Cloud by TrueIDC

Mr. Athiwat Itthiwatana

Cloud & Solution Consultant

Presented by

- Athiwat Itthiwatana (HAM)
- Cloud & Solution Consultant, TrueIDC
- AWS Specialist
- SAP Basis Specialist
- athiwat.itt@ascendcorp.com

aws certified
Solutions Architect
PROFESSIONAL

aws certified
SAP on AWS
SPECIALTY

aws certified
Security
SPECIALTY

Agenda

- Introduction to Security on Cloud
- IAM Service
- CloudTrail Service
- VPC Flowlog
- Lab: CloudTrail

Source: AWS Immersion day

Introduction to Security

Before…

Move fast OR Stay secure

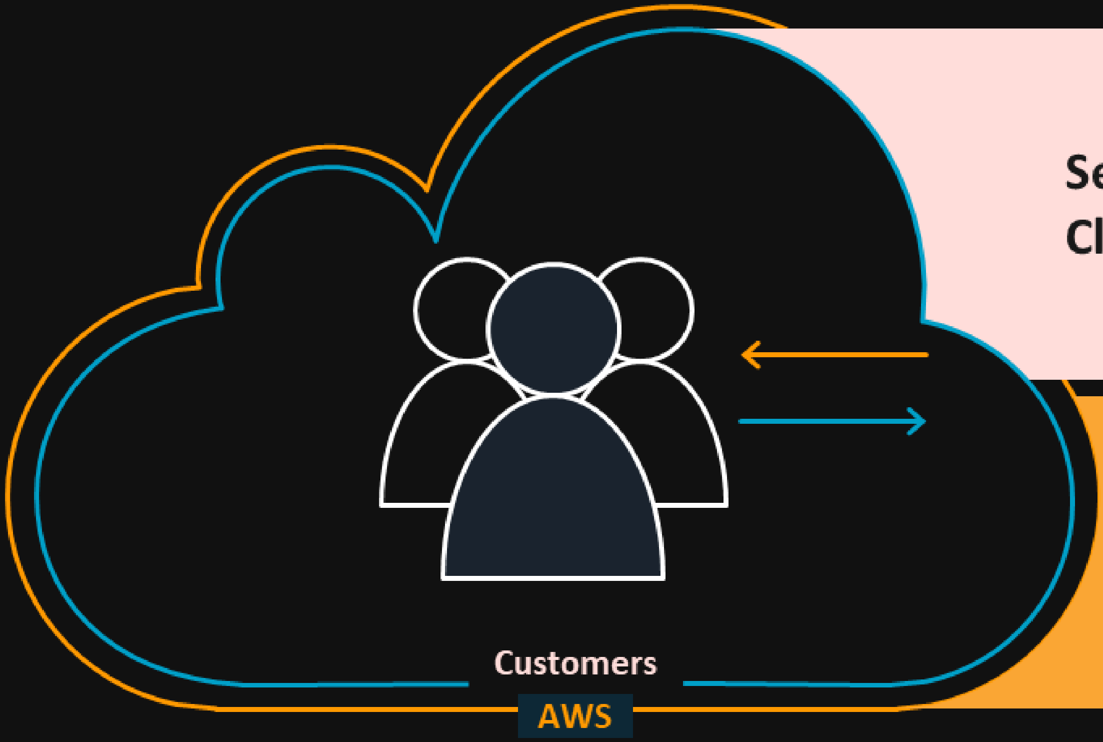
Source: AWS Immersion day

Now !!

Move fast AND Stay secure

Source: AWS Immersion day

Shared responsibility model



Security IN the Cloud

Customer responsibility is determined by the AWS Cloud services a customer selects.

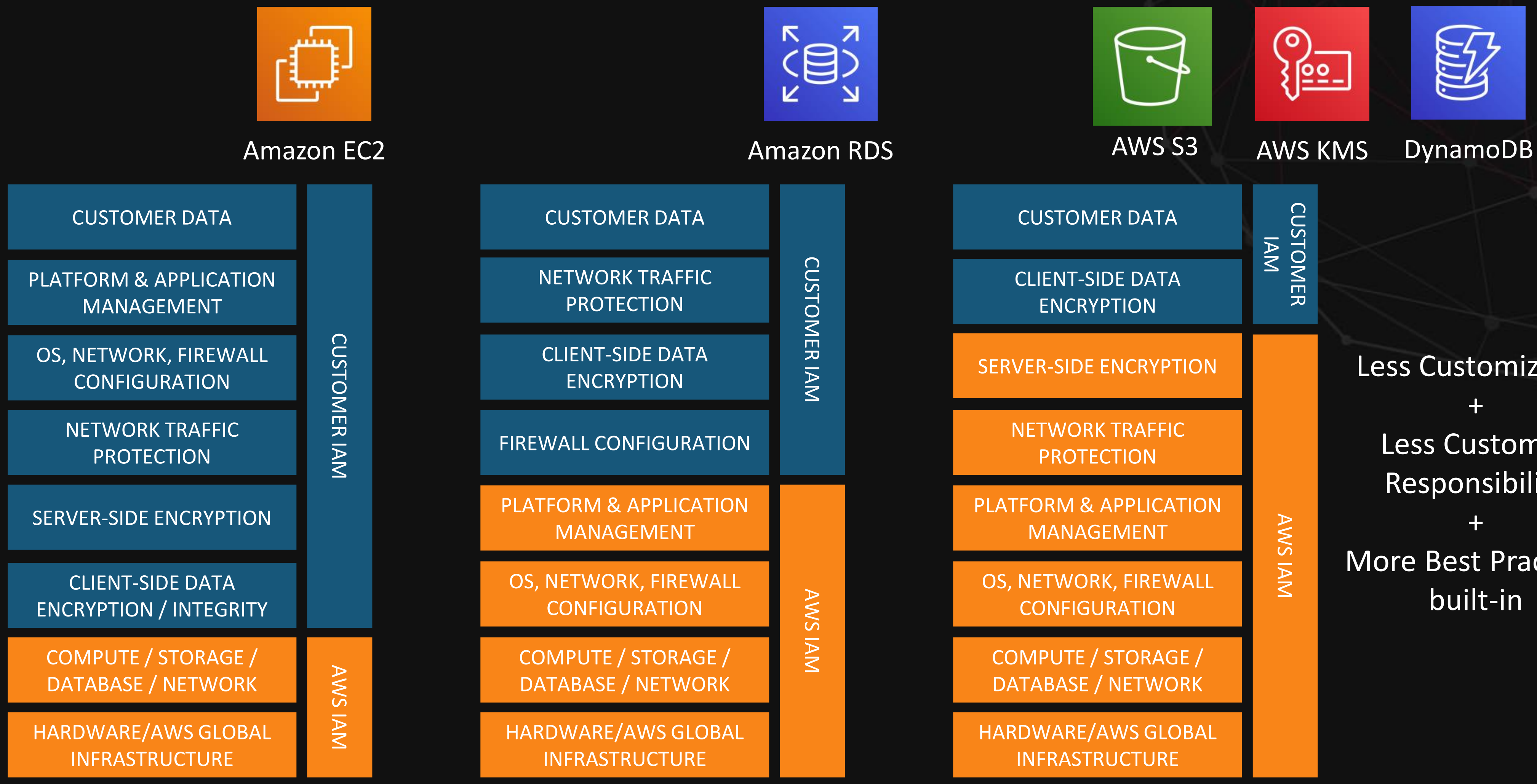
Security OF the Cloud

AWS is responsible for protecting the infrastructure that runs all the services offered in the AWS Cloud.

Source: AWS Immersion day

The Line Varies ...

More Customizable
+
More Customer
Responsibility



Amazon EC2

CUSTOMER DATA

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

NETWORK TRAFFIC PROTECTION

SERVER-SIDE ENCRYPTION

CLIENT-SIDE DATA ENCRYPTION / INTEGRITY

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

Infrastructure Services

Amazon RDS

CUSTOMER DATA

NETWORK TRAFFIC PROTECTION

CLIENT-SIDE DATA ENCRYPTION

FIREWALL CONFIGURATION

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

Container Services

AWS S3 AWS KMS DynamoDB

CUSTOMER DATA

CLIENT-SIDE DATA ENCRYPTION

SERVER-SIDE ENCRYPTION

NETWORK TRAFFIC PROTECTION

PLATFORM & APPLICATION MANAGEMENT

OS, NETWORK, FIREWALL CONFIGURATION

COMPUTE / STORAGE / DATABASE / NETWORK

HARDWARE/AWS GLOBAL INFRASTRUCTURE

CUSTOMER IAM

AWS IAM

Abstracted Services

Less Customizable
+
Less Customer
Responsibility
+
More Best Practices
built-in

Source: AWS Immersion day

AWS Security, Identity, and Compliance Solutions

Identity and access management

- AWS Identity and Access Management (IAM)
- AWS Single Sign-On
- AWS Organizations
- AWS Directory Service
- Amazon Cognito
- AWS Resource Access Manager

Detective controls

- AWS Security Hub
- Amazon GuardDuty
- Amazon Inspector
- Amazon CloudWatch
- AWS Config
- AWS CloudTrail
- VPC Flow Logs
- AWS IoT Device Defender

Infrastructure protection

- AWS Firewall Manager
- AWS Network Firewall
- AWS Shield
- AWS WAF
- Amazon VPC
- AWS PrivateLink
- AWS Systems Manager

Data protection

- Amazon Macie
- AWS Key Management Service (KMS)
- AWS CloudHSM
- AWS Certificate Manager
- AWS Secrets Manager
- AWS VPN
- Server-Side Encryption

Incident response

- Amazon Detective
- Amazon EventBridge
- AWS Backup
- AWS Security Hub
- AWS Elastic Disaster Recovery

Privacy and Compliance

- AWS Artifact
- AWS Audit Manager
- Amazon CloudWatch
- AWS CloudTrail
- AWS Config
- AWS Security Hub
- AWS Systems Manager

Source: AWS Immersion day

Identity and access management

Define, enforce, and audit user permissions across AWS services, actions, and resources

AWS Identity and Access Management (IAM) Day 2 ✓

Securely manage access to AWS services and resources

AWS Single Sign-On (SSO) Day 6 ✓

Centrally manage SSO access to multiple AWS accounts and business apps

AWS Directory Service

Managed Microsoft Active Directory in AWS

Amazon Cognito Day 5 ✓

Add user sign-up, sign-in, and access control to your web and mobile apps

AWS Organizations Day 6 ✓

Policy-based management for multiple AWS accounts

AWS Resource Access Manager

Simple, secure service for sharing AWS resources

aws

Source: AWS Immersion day

trueIDC

Detective controls

Gain the visibility you need to spot issues before they impact your business, improve your security posture, and reduce the risk profile of your environment

AWS Security Hub

Centrally view and manage security alerts & automate compliance checks. Day 6 ✓

Amazon GuardDuty

Intelligent threat detection and continuous monitoring to protect your AWS accounts and workloads. Day 2 ✓

Amazon Inspector

Automates security assessments to help improve the security and compliance of applications deployed on AWS.

Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes. Day 2 ✓

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis. Day 6 ✓

AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational and risk auditing of your AWS account. Day 2 ✓

VPC Flow Logs

Capture info about the IP traffic going to and from network interfaces in your VPC. Flow log data is stored using Amazon CloudWatch Logs. Day 2 ✓

Source: AWS Immersion day

Infrastructure protection

Reduce surface area to manage and increase privacy for and control of your overall infrastructure on AWS

AWS Firewall Manager

Centrally configure and manage AWS WAF rules across accounts and applications

AWS Network Firewall

Deploy network security across your Amazon VPCs with just a few clicks

AWS Shield

Managed DDoS protection service that safeguards web applications running on AWS

Day 2 ✓

AWS WAF—Web Application Firewall

Protects your web applications from common web exploits ensuring availability and security

Day 2 ✓

Amazon Virtual Private Cloud

Provision a logically isolated section of AWS where you can launch AWS resources in a virtual network that you define

Day 2 ✓

AWS PrivateLink

Access services hosted on AWS easily and securely by keeping your network traffic within the AWS network

AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure OSs

Source: AWS Immersion day

Data protection

In addition to using automatic data encryption and management services,
you can employ more features for data protection
(including data management, data security, and encryption key storage)

Amazon Macie

Discover and protect your sensitive data at scale

AWS Key Management Service (AWS KMS)

Day 2 ✓

Easily create and control the keys used to encrypt your data

AWS CloudHSM

Managed hardware security module on the AWS Cloud

AWS Certificate Manager

Easily provision, manage, and deploy SSL/TLS certificates for use with AWS services

AWS Secrets Manager

Easily rotate, manage, and retrieve database credentials, API keys, and other secrets through their lifecycle

AWS VPN

Extend your on-premises networks to the cloud and securely access them from anywhere

Server-Side Encryption

Day 2 ✓

Flexible data encryption options using AWS service managed keys, AWS managed keys via AWS KMS, or customer managed keys

Source: AWS Immersion day

Incident response

During an incident, containing the event and returning to a known good state are important elements of a response plan. AWS provides the following tools to automate aspects of this best practice.

Amazon Detective

Analysis and visualization of security data to get to the root cause of potential security issues quickly

Amazon EventBridge

Serverless event bus that makes it easier to build event-driven applications to scale your programmed, automated response to incidents

Day 5 ✓

AWS Backup

Centrally manage and automate backups across AWS services to simplify data protection at scale

AWS Security Hub

Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows

Day 6 ✓

AWS Elastic Disaster Recovery

Fast, automated, cost-effective disaster recovery

aws

Source: AWS Immersion day

trueIDC

Privacy and Compliance

AWS supports security standards and compliance certifications to help you satisfy the requirements of virtually every regulatory agency around the globe.

AWS Artifact

No-cost, self-service portal for on-demand access to AWS compliance reports

AWS Audit Manager

Continuously audit your AWS usage to simplify how you assess risk and compliance

Amazon CloudWatch

Complete visibility of your cloud resources and applications to collect metrics, monitor log files, set alarms, and automatically react to changes

Day 2 ✓

AWS CloudTrail

Track user activity and API usage to enable governance, compliance, and operational and risk auditing of your AWS account

Day 2 ✓

AWS Config

Record and evaluate configurations of your AWS resources to enable compliance auditing, resource change tracking, and security analysis

AWS Security Hub

Out-of-the-box integrations with ticketing, chat, SIEM, SOAR, threat investigation, incident management, and GRC tools to support your security operations workflows

Day 6 ✓

AWS Systems Manager

Easily configure and manage Amazon EC2 and on-premises systems to apply OS patches, create secure system images, and configure secure OSs

aws

Source: AWS Immersion day

trueIDC

IAM Identity and Access Management

AWS identity management – Who

Workforce identity

- AWS Single Sign-On (SSO)
- AWS Directory Service
- AWS Partner Identity Provider Federation

Consumer identity

- Amazon Cognito
- AWS Partner Identity Provider Federation

AWS Single Sign-On

AWS Directory Service

Amazon Cognito

Source: AWS Immersion day

AWS access management – Can access

Identity-based policies

Resource-based policies

Two AWS policy types shown

Policies define permissions

Source: AWS Immersion day

AWS resource management – What

At cloud scale for . . .

Hundreds of AWS accounts

Thousands of Amazon EC2 instances

Billions of Amazon S3 objects

Trillions of Amazon DynamoDB items

And thousands of workloads

Source: AWS Immersion day

IAM: Root account

Create by default.

Safeguard your root user

Credentials and don’t use

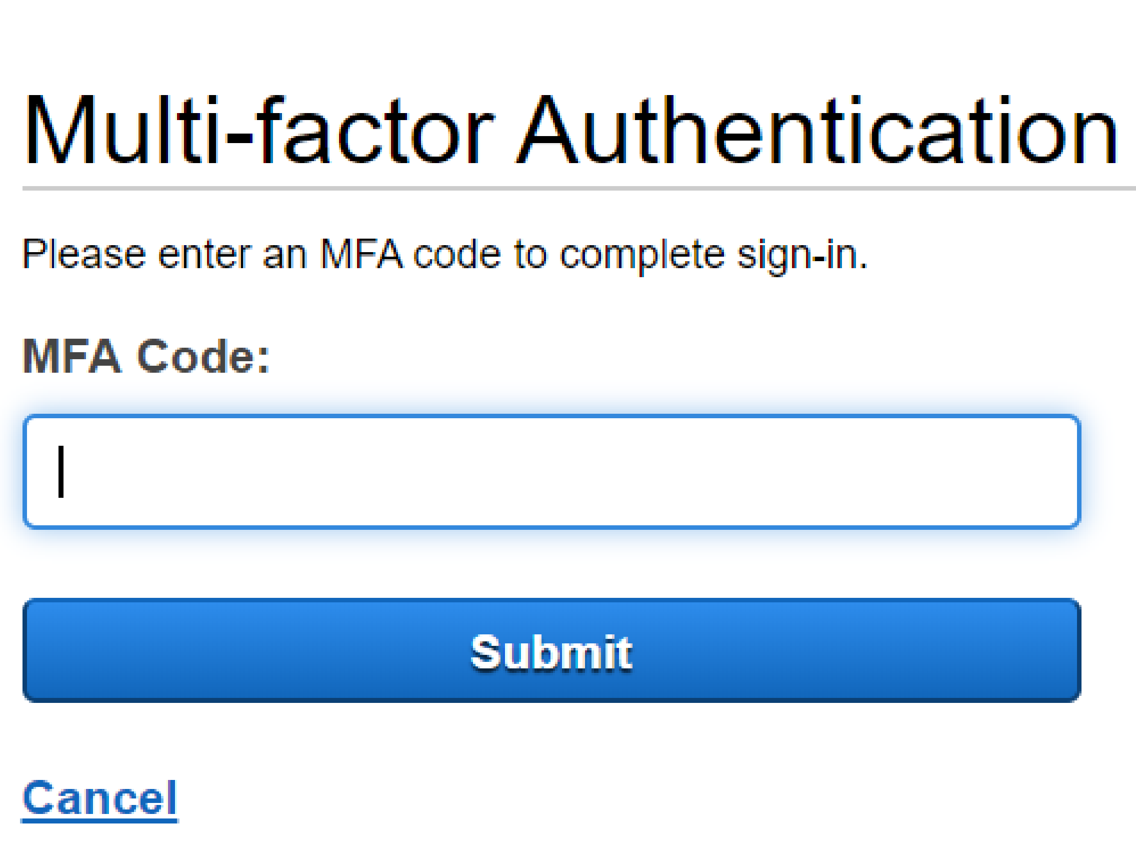
Them for everyday tasks

Source: AWS Immersion day

Multi-factor authentication (MFA)

1 Combine what you know with what you have

2 Apply to all humans accessing AWS resources



Multi-factor Authentication

Please enter an MFA code to complete sign-in.

MFA Code:

Source: AWS Immersion day

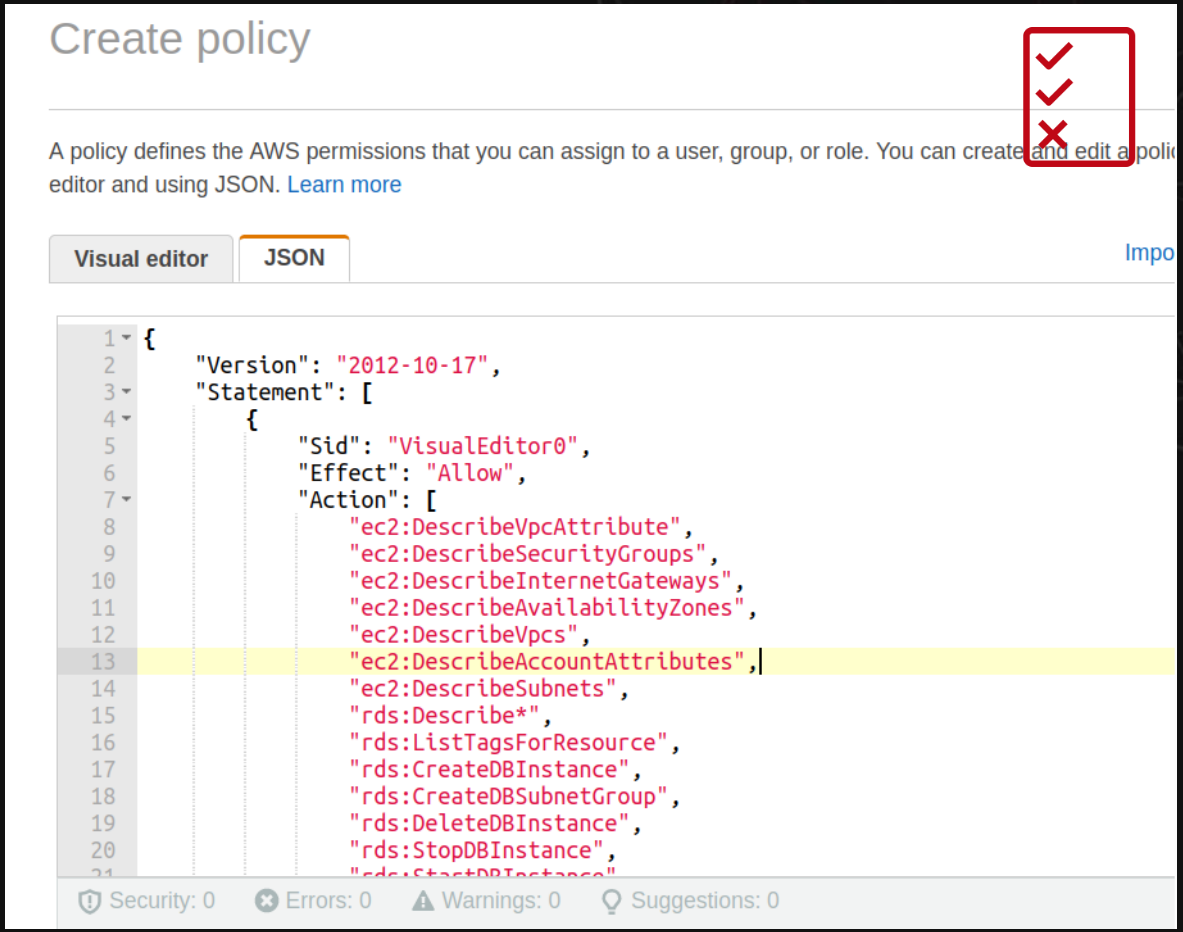
IAM Users & Group

- Users are people within your organization, and can be assign to IAM group
- Groups can only contain users
- User don’t have to belong to a group, multiple assign is allowed
- Group help you manage user easier

Source: AWS Immersion day

IAM Policy

- User or Groups can be assigned with IAM Policy
- Policy define the permissions for user or group
- Grant permission with least privilege principle
- Policy must be in JSON format



Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a polic
editor and using JSON. Learn more

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcAttribute",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeInternetGateways",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeVpcs",
                "ec2:DescribeAccountAttributes",
                "ec2:DescribeSubnets",
                "rds:Describe*",
                "rds:ListTagsForResource",
                "rds:CreateDBInstance",
                "rds:CreateDBSubnetGroup",
                "rds:DeleteDBInstance",
                "rds:StopDBInstance",
                "rds:StartDBInstance"
```

Source: AWS Immersion day

IAM Policy

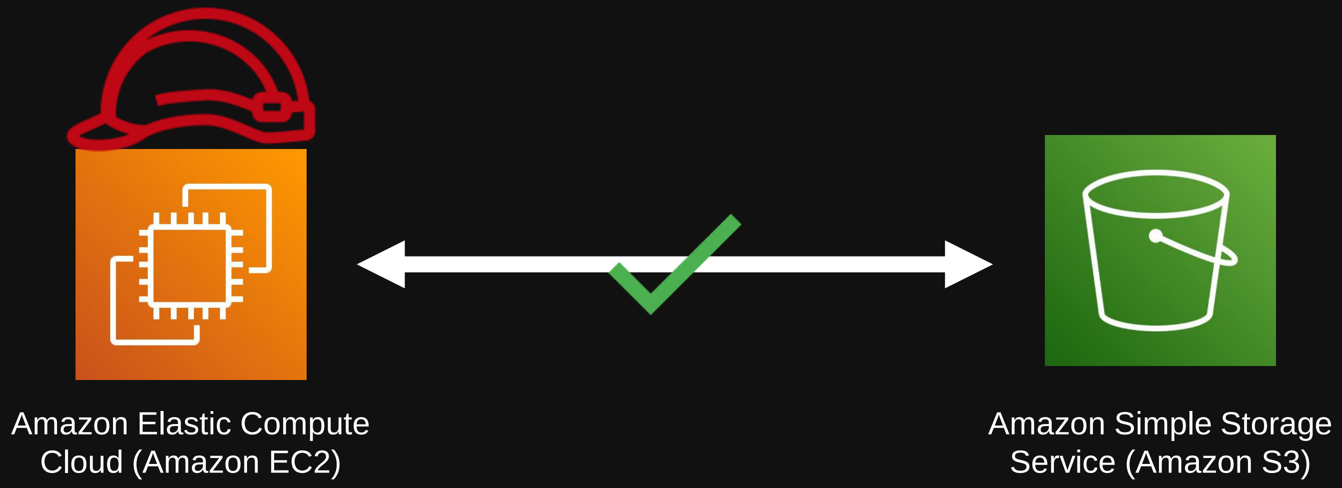
- **Managed Policy** - Standalone policies that you can attach to multiple users, groups, and roles in your AWS account. Managed policies apply only to identities (users, groups, and roles) – not resources.

- **Inline Policy** - Policies that you create and manage, and that are embedded directly into a single user, group, or role. Resource based policies are another form of inline policy.

Source: AWS Immersion day

IAM Role

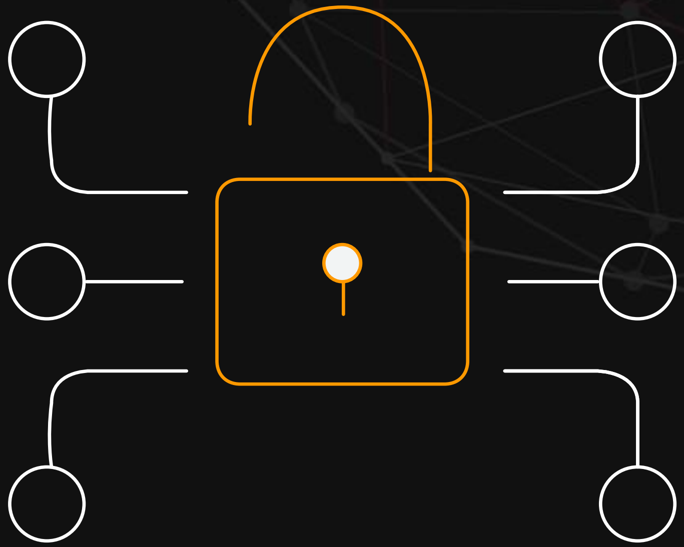
- A secure way to grant permissions to entities that you trust
- AWS services can only assign with IAM Role
- You can multiple assign IAM policies to IAM role


Amazon Elastic Compute Cloud (Amazon EC2)
Amazon Simple Storage Service (Amazon S3)

Source: AWS Immersion day

IAM Best Practices

- Protect the “root” account.
- Create the individual IAM user.
- Create and use groups.
- Set up a strong password policy.
- Use multifactor authentication.
- Use Roles/Instance profiles.
- Rotate credentials often.
- Monitor IAM activity.



Source: AWS Immersion day

CloudTrail

Visibility into what is happening in your environment is crucial

- Who is using my resource?
- Did they modify it?
- When did they access it?
- Where did they login from?
- Was it during my maintenance window?
- Who were active users during an incident?
- What events occurred during a time period?
- What actions did AWS take on my behalf?
- … and many more

AWS CloudTrail

Source: AWS Immersion day

AWS CloudTrail provides audit logs for AWS

- Capture and log user and resource activity across your AWS infrastructure and resources for governance and auditing.
- Enable compliance, operational and risk auditing.

Capture

Record activity as CloudTrail events

Store

Retain events logs in secure S3 bucket

Act

Trigger actions when important events are detected

Review

Analyze recent events and logs with Amazon Athena or CloudWatch Logs Insights

Source: AWS Immersion day

Components of CloudTrail

Audit Trails	• Configure recording events across all your AWS accounts and regions • Centralize logging across your AWS Organization • Create additional trails as needed for operations, support, and security needs • Configure trail to select relevant events for delivery by choosing management events (all, read, write, exclude KMS), and/or data events (all or specific S3 buckets and Lambda functions)
Event Delivery	• Deliver events to Amazon S3, Amazon CloudWatch Logs or Amazon EventBridge • Get SNS notifications when events are delivered • Enable encryption using SSE or KMS • Cryptographically validate whether log file was modified, deleted or unchanged
Search and Analytics	• Lookup recent (90-day) event history on Console or API • Leverage integration with CloudWatch Logs, or Amazon Athena to query events • Import logs to Amazon Elasticsearch Service, or AWS Partner Solutions for deeper analysis
CloudTrail Insights	• Identify unusual operational activity such as spikes in resource provisioning, or gaps in periodic maintenance activity • Enable automatic analysis of events to establish baseline for normal behavior and detect anomalous patterns. • Remediate operational issues using actionable information in Insights events.

Source: AWS Immersion day

Audit Trails

- Configure the events to be captured by the trails
- Includes Management Events, Data Events and Insight Events
- Easily configure multi-account and multi-region trails
- Narrow down the events by creating trails to capture write-only events, data events from specific S3 buckets, exclude read-only KMS events, etc
- Create additional trails as needed for operations, support, security and compliance needs

Tip: Create one ‘audit’ trail that logs all events across all regions

Source: AWS Immersion day

Event Delivery

- Deliver logs to S3, CloudWatch Logs or EventBridge
- Identify whether logs were modified, deleted or unchanged using cryptographic validation
- Leverage SNS notifications to take actions based on event delivery
- Receive logs within minutes of the event occurrence

Tip: Deliver events from all accounts to a central restricted-access logging bucket with multi-factor authentication delete

Source: AWS Immersion day

Search and Analytics

- Retrieve 90 day event history from CloudTrail console or API
- Narrow down to relevant time period, API operation, user name or resource
- Leverage integration with CloudWatch Logs to query audit logs alongside performance and monitoring logs
- 20+ partner integrations for operational and security solutions

Tip: Automatically create Athena tables from the CloudTrail console and enhance your analysis of AWS service activity

Source: AWS Immersion day

CloudTrail Insights

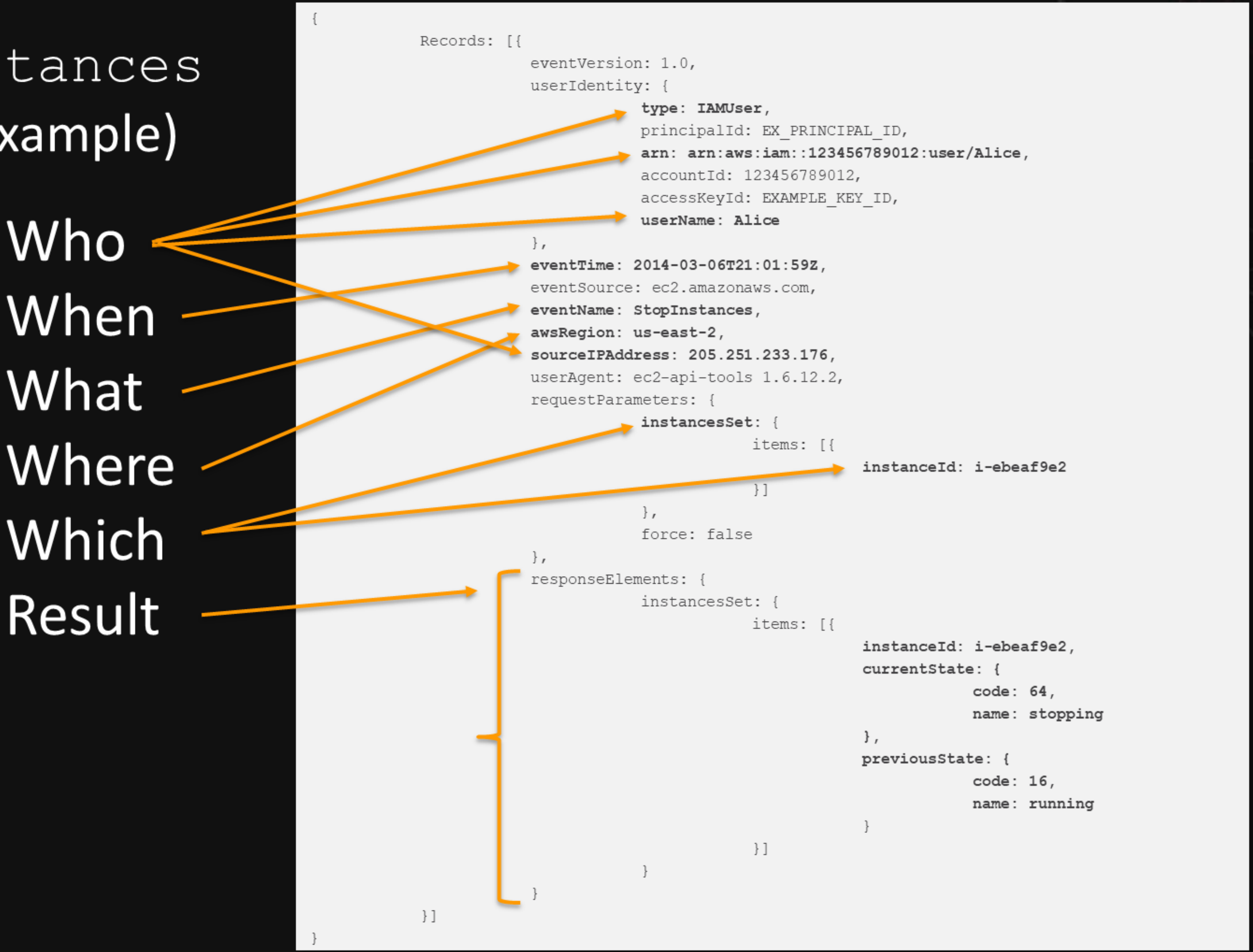
- Identify and respond to unusual operational activity
  - Unexpected spikes in resource provisioning
  - Bursts of IAM management actions
  - Gaps in periodic maintenance activity
- Automatic analysis of API calls and usage patterns
- Near real-time alerts when unusual activity is detected

Tip: Turn on Insights on your trails to save time sifting through logs and getting ahead of issues before they impact your business

Source: AWS Immersion day

Core Logs in AWS CloudTrail

StopInstances
API Call (Example)



```
{
        Records: [{
                eventVersion: 1.0,
                userIdentity: {
                        type: IAMUser,
                        principalId: EX_PRINCIPAL_ID,
                        arn: arn:aws:iam::123456789012:user/Alice,
                        accountId: 123456789012,
                        accessKeyId: EXAMPLE_KEY_ID,
                        userName: Alice
                },
                eventTime: 2014-03-06T21:01:59Z,
                eventSource: ec2.amazonaws.com,
                eventName: StopInstances,
                awsRegion: us-east-2,
                sourceIPAddress: 205.251.233.176,
                userAgent: ec2-api-tools 1.6.12.2,
                requestParameters: {
                        instancesSet: {
                                items: [{
                                        instanceId: i-ebeaf9e2
                                }]
                        },
                        force: false
                },
                responseElements: {
                        instancesSet: {
                                items: [{
                                        instanceId: i-ebeaf9e2,
                                        currentState: {
                                                code: 64,
                                                name: stopping
                                        },
                                        previousState: {
                                                code: 16,
                                                name: running
                                        }
                                }]
                        }
                }
        }]
}
```

Source: AWS Immersion day

VPC Flowlog

Amazon VPC Flow Logs

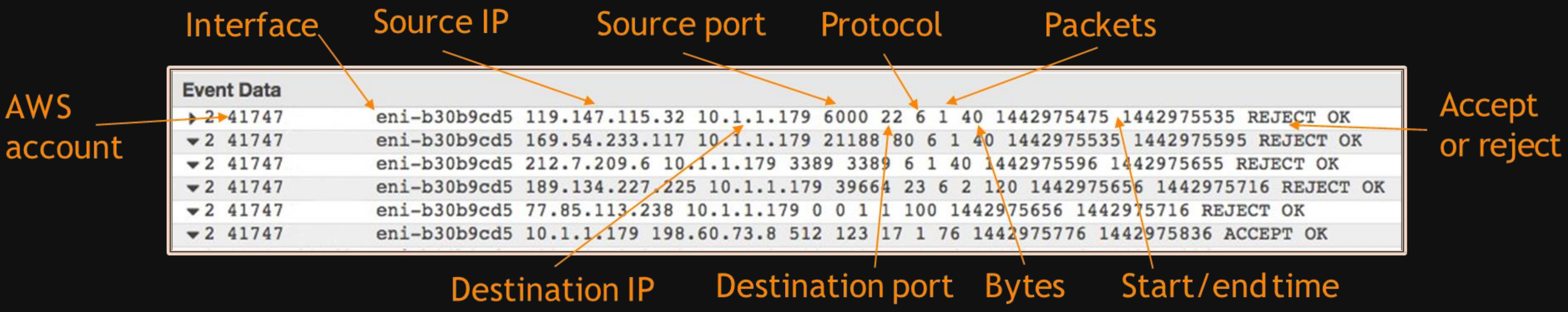
Stores logs in AWS CloudWatch Logs

- Can be enabled on
  - Amazon VPC, a subnet, or a network interface
  - Amazon VPC & subnet enables logging for all interfaces in the VPC/subnet
  - Each network interface has a unique log stream
- Flow logs do not capture real-time log streams for your network interfaces
- Filter desired result based on need
  - All, Reject, Accept
  - Troubleshooting or security related with alerting needs?
  - Think before enabling All on VPC, will you use it?

Source: AWS Immersion day

Amazon VPC Flow Logs

- Agentless
- Enable per ENI, per subnet, or per VPC
- Logged to AWS CloudWatch Logs
- Create CloudWatch metrics from log data
- Alarm on those metrics



```
Event Data
▸ 2 41747          eni-b30b9cd5 119.147.115.32 10.1.1.179 6000 22 6 1 40 1442975475 1442975535 REJECT OK
▾ 2 41747          eni-b30b9cd5 169.54.233.117 10.1.1.179 21188 80 6 1 40 1442975535 1442975595 REJECT OK
▾ 2 41747          eni-b30b9cd5 212.7.209.6 10.1.1.179 3389 3389 6 1 40 1442975596 1442975655 REJECT OK
▾ 2 41747          eni-b30b9cd5 189.134.227.225 10.1.1.179 39664 23 6 2 120 1442975656 1442975716 REJECT OK
▾ 2 41747          eni-b30b9cd5 77.85.113.238 10.1.1.179 0 0 1 1 100 1442975656 1442975716 REJECT OK
▾ 2 41747          eni-b30b9cd5 10.1.1.179 198.60.73.8 512 123 17 1 76 1442975776 1442975836 ACCEPT OK
```

Source: AWS Immersion day

https://github.com/TIDC-PS-Inter/AWS-Workshop

trueIDC

REGIONAL
DATA CENTER &
CLOUD SERVICE
PROVIDER