



Security Essentials

Yasser Quraishi, AWS Solutions Architect –
yquraish@amazon.com

Jeff Hosley, AWS Account Manager – jhosley@amazon.com



Overview

Overview of the AWS cloud security concepts such as the AWS Security Center, Shared Responsibility Model, and Identity and Access Management.



AWS Security

At AWS, cloud security is our highest priority.

Gain access to a world-class security team

Where would some of the world's top security people like to work? At scale on huge challenges with huge rewards

So AWS has **world-class security and compliance** teams watching your back!

Every customer benefits from the tough scrutiny of other AWS customers



Broad Accreditations & Certifications

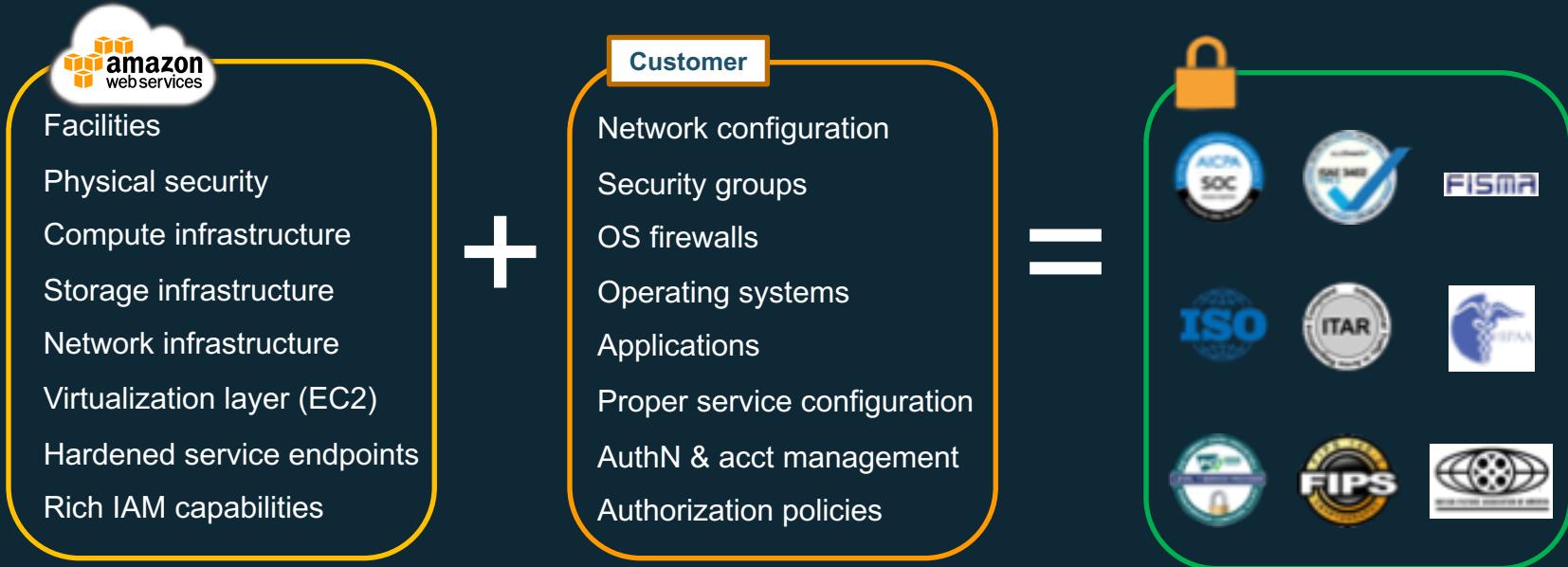


See <https://aws.amazon.com/compliance/programs/> for full list



Shared
Responsibility Model

AWS Shared Responsibility Model



- Scope of responsibility depends on the type of service offered by AWS:
Infrastructure, Container, Abstracted Services
- Understanding who is responsible for what is critical to ensuring your AWS data and systems are secure!

Shared Responsibility Model

Customer

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall Configuration

Client-side Data
Encryption

Server-side Data
Encryption

Network Traffic
Protection

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

AWS Global
Infrastructure

Availability Zones

Regions

Edge Locations

Customers are responsible for their security and compliance **IN** the Cloud

AWS is responsible for the security **OF** the Cloud

Meet your own security objectives

Customer

Your own accreditation



Your own certifications



Your own external audits



Customer scope and effort is reduced

Better results through focused efforts

AWS

AWS Foundation Services

Compute

Storage

Database

Networking

Built on AWS consistent baseline controls

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

AWS Responsibilities

Physical Security of Data Center

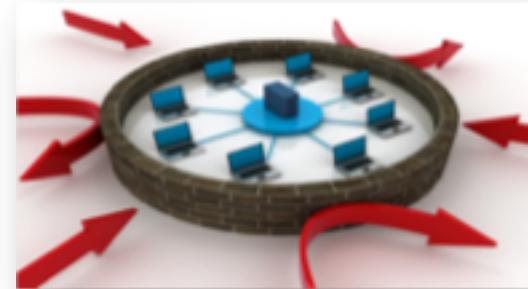
- Amazon has been building large-scale data centers for many years.
- Important attributes:
 - Non-descript facilities
 - Robust perimeter controls
 - Strictly controlled physical access
 - Two or more levels of two-factor authentication
- Controlled, need-based access.
- All access is logged and reviewed.
- Separation of Duties
 - Employees with physical access don't have logical privileges.



AWS Responsibilities

EC2 Security

- **Host (hypervisor) operating system**
 - Individual SSH keyed logins via bastion host for AWS admins
 - All accesses logged and audited
- **Guest (EC2 Instance) operating system**
 - Customer controlled (customer owns root/admin)
 - AWS admins cannot log in
 - Customer-generated key-pairs
- **Stateful firewall**
 - Mandatory inbound firewall, default deny mode
 - Customer controls configuration via Security Groups



Network Security

- IP Spoofing prohibited at host OS level.
- Unauthorized Port Scanning a violation of TOS and is detected/blocked.
- Inbound ports blocked by default.

AWS Responsibilities

Configuration Management

- Most updates are done in such a manner that they will not impact the customer.
- Changes are authorized, logged, tested, approved, and documented.
- AWS will communicate with customers, either via email, the AWS Service Health Dashboard (<http://status.aws.amazon.com/>), or the AWS Personal Health Dashboard (<https://phd.aws.amazon.com/>) when there is a potential for service being affected.

Built for “Continuous Availability”

- **Scalable, fault tolerant services.**
- **All availability zones (AZs) are always on.**
 - There is no “Disaster Recovery Datacenter”
 - All managed to the same standards
- **Robust Internet connectivity**
 - Each AZ has redundant, Tier 1 ISP Service Providers
 - Resilient network infrastructure

Service Health Dashboard

aws SERVICE HEALTH DASHBOARD

Amazon Web Services > Service Health Dashboard
Get a personalized view of AWS service health
[Open the Personal Health Dashboard.](#)

Current Status - Aug 2, 2019 PDT

Amazon Web Services publishes our most up-to-the-minute information on service availability in the table below. Check back here any time to get current status information, or subscribe to an RSS feed to be notified of interruptions to each individual service. If you are experiencing a real-time operational issue with one of our services that is not described below, please inform us by clicking on the "Contact Us" link to submit a service issue report. All dates and times are Pacific Time (PST/PDT).

Region	Service	Status	Action
North America	Alexa for Business (N. Virginia)	Service is operating normally	Details RSS
North America	Amazon API Gateway (Montreal)	Service is operating normally	Details RSS
North America	Amazon API Gateway (N. California)	Service is operating normally	Details RSS
North America	Amazon API Gateway (N. Virginia)	Service is operating normally	Details RSS
North America	Amazon API Gateway (Ohio)	Service is operating normally	Details RSS
North America	Amazon API Gateway (Oregon)	Service is operating normally	Details RSS
North America	Amazon AppStream 2.0 (N. Virginia)	Service is operating normally	Details RSS
North America	Amazon AppStream 2.0 (Oregon)	Service is operating normally	Details RSS
North America	Amazon Athena (Montreal)	Service is operating normally	Details RSS
North America	Amazon Athena (N. Virginia)	Service is operating normally	Details RSS
North America	Amazon Athena (Ohio)	Service is operating normally	Details RSS
North America	Amazon Athena (Oregon)	Service is operating normally	Details RSS
South America			
Europe			
Asia Pacific			
Middle East			
Contact Us			

Personal Health Dashboard

AWS Services Edit Support name @ 123456789012 🔍

Personal Health Dashboard

Dashboard

Set up notifications with CloudWatch Events 🔍

4 Open issues Past 7 days | 4 Scheduled changes | 3 Other notifications Past 7 days

Issues that might affect your AWS infrastructure. 2 issues were closed in the past 24 hours.

See all Issues ?

Filter: 🔍 Helper Text

Event type	Status	Region/AZ ⓘ	Start time	End time
Direct Connect Maintenance Sch..	Ongoing	ap-northeast-1	November 16, 2016 at 8:10:..	November 20, 2016 at 8:10:..
EC2 Dedicated Host Power Mainte...	Ongoing	ap-northeast-1	November 16, 2016 at 8:10:..	November 22, 2016 at 8:10:..
RDS Maintenance Scheduled	Ongoing	ap-northeast-1	November 17, 2016 at 8:10:..	November 23, 2016 at 8:10:00 P..
VPN Maintenance Scheduled	Upcoming	us-west-2	November 24, 2016 at 8:10:..	November 25, 2016 at 8:10:..

All events

© 2019

Feedback English

aws

© 2008 - 2016, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

AWS Responsibilities

Disk Management

- Proprietary disk management prevents customers from accessing each other's data.
- Disks wiped prior to use.
- Disks can also be encrypted by the customer for additional security.

Storage Device Decommissioning

- All storage devices go through process using techniques from:
 - DoD 5220.22-M ("National Industrial Security Program Operating Manual").
 - NIST 800-88 ("Guidelines for Media Sanitization").
- Ultimately devices are:
 - Degaussed.
 - Physically destroyed.

Under the AWS Shared Responsibility Model

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Preventing packet sniffing at the hypervisor level

Patching the operating system with the latest security patches

Shredding disk drives before they leave a datacenter

Securing the internal network inside the AWS datacenters

Installing camera systems to monitor the physical datacenters

Toggling on the Server-side encryption feature for S3 buckets

Under the AWS Shared Responsibility Model

AWS Responsibility? or Customer Responsibility?

Configuring the Security Group rules that determine which ports are open on the EC2 Linux instance

Patching the operating system with the latest security patches

Installing camera systems to monitor the physical datacenters

Preventing packet sniffing at the hypervisor level

Shredding disk drives before they leave a datacenter

Toggling on the Server-side encryption feature for S3 buckets

Securing the internal network inside the AWS datacenters



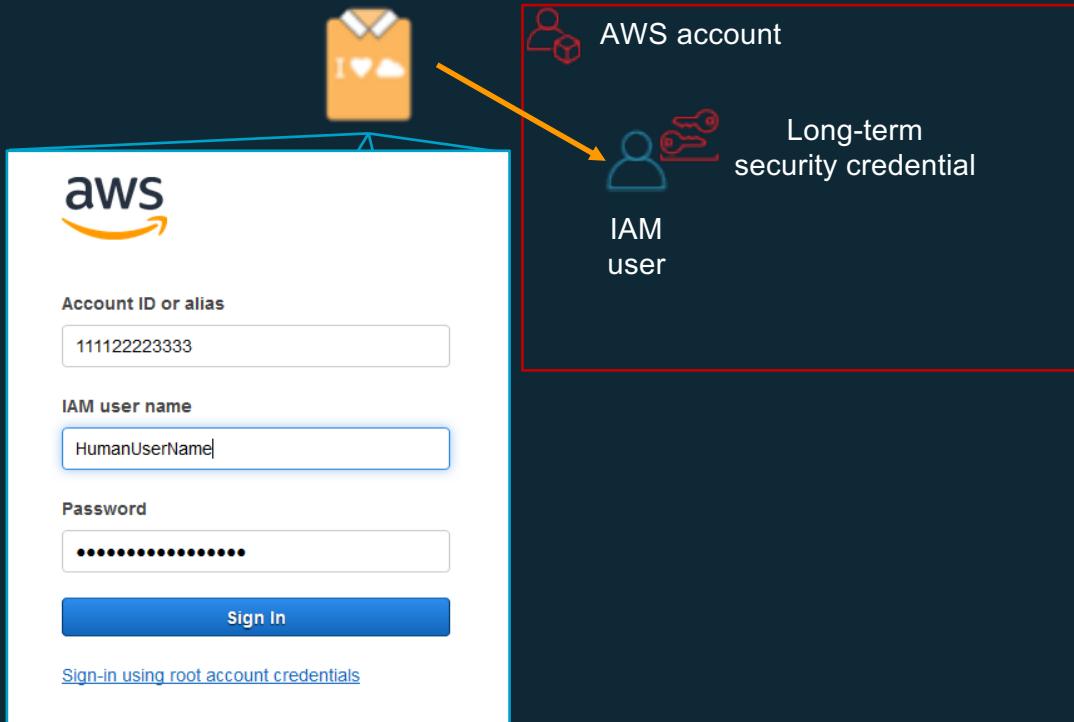
Identity and Access Management

AWS IAM

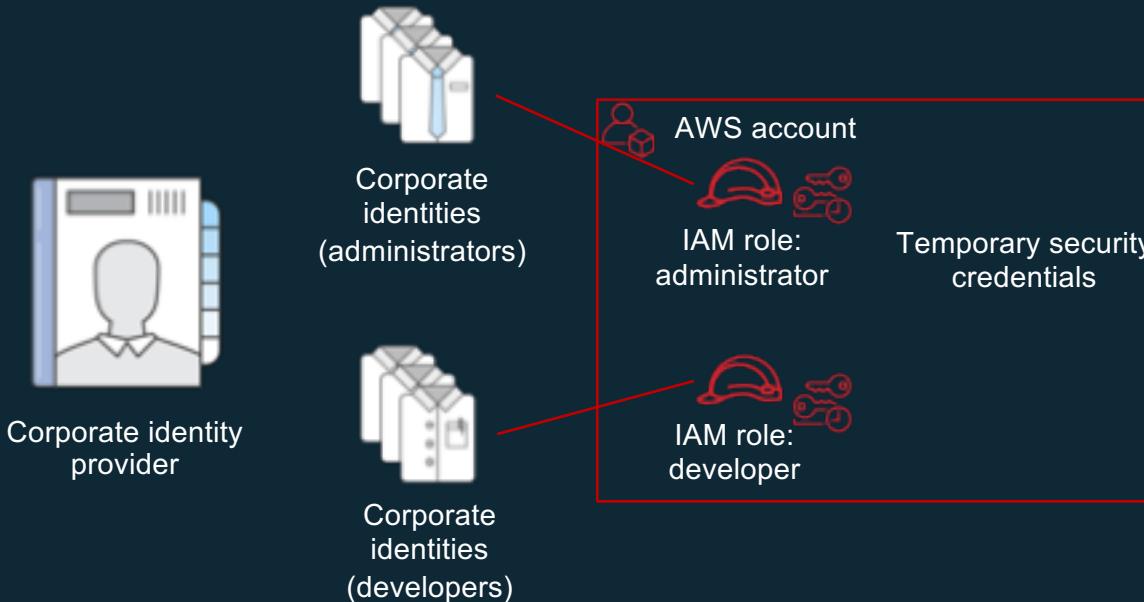


- **What it is**
 - I – Authentication: Support for human and application caller identities
 - AM – Authorization: Powerful, flexible permissions language for controlling access to cloud resources
- **Why it matters to you:** Every AWS service uses IAM to authenticate and authorize API calls
- **What builders need to know**
 - How to make authenticated API calls to AWS from IAM identities
 - Basic fluency in IAM policy language
- **Where to find and how to understand service-specific authorization**

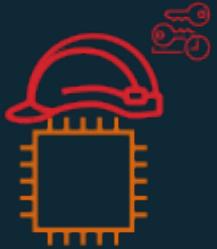
AWS identities for human callers: IAM users



AWS identities for human callers: Federated identities



AWS identities for non-human callers



Amazon
EC2
instance



AWS Lambda
function



Amazon
SageMaker
notebook



AWS Glue
crawler



Amazon ECS
task

...and many others

Creating a role in the AWS Management Console

Role for your
non-human process

Role for federated
(human) identities

Choose the type of entity you want to grant access to.

1 Selected entity

2 **Role for your non-human process**

3 **Role for federated (human) identities**

4 **Role for cross-account access**

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role.

EC2
Allows EC2 instances to call AWS services on your behalf.

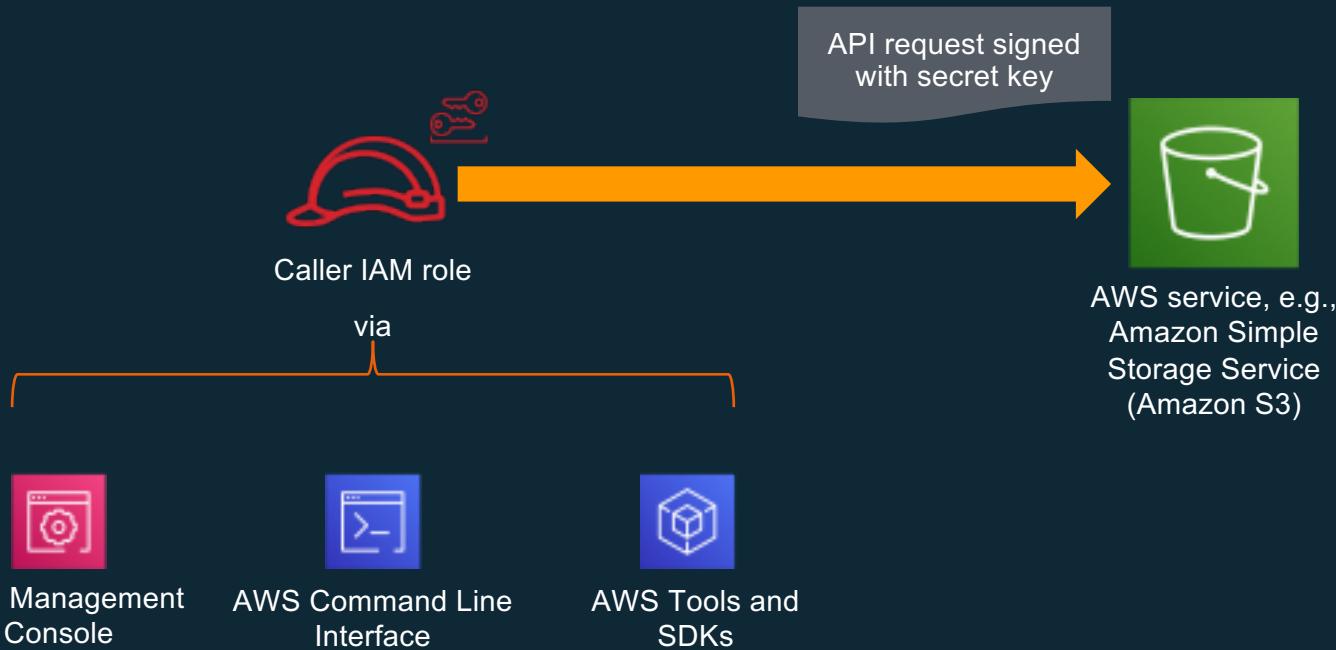
Lambda
Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeDeploy	CloudFront	Kinesis	S3
AWS Backup	Comprehend	EMR	Lambda	SMS
AWS Support	Config	ElastiCache	Lex	SNS
Amplify	Connect	Elastic Beanstalk	License Manager	SWF
AppSync	DMS	Elastic Container Service	Machine Learning	SageMaker

* Required

Cancel **Next: Permissions**

How an authentication works in AWS



AWS-managed policies for common sets of permissions

Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy

Filter policies ▾ Search

AWS pre-defines some IAM policies for common tasks

Showing 512 results

	Policy name ▾	Used as	Description
<input type="checkbox"/>	AdministratorAccess	Permissions policy (1)	Provides full access to AWS services a...
<input type="checkbox"/>	AlexaForBusinessDeviceSetup	None	Provide device setup access to AlexaF...
<input type="checkbox"/>	AlexaForBusinessFullAccess	None	Grants full access to AlexaForBusines...
<input type="checkbox"/>	AlexaForBusinessGatewayExecution	None	Provide gateway execution access to ...
<input type="checkbox"/>	AlexaForBusinessNetworkProfileServicePolicy	None	This policy enables Alexa for Business ...
<input type="checkbox"/>	AlexaForBusinessReadOnlyAccess	None	Provide read only access to AlexaForB...
<input type="checkbox"/>	AmazonAPIGatewayAdministrator	None	Provides full access to create/edit/delet...

Reading and writing IAM policy

```
{  
  "Version": "2012-10-17"  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "dynamodb:*"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

Allow or deny?

What can (or can't) you do?

What can (or can't) you do it to?

In English: Allowed to take all Amazon DynamoDB actions

Reading and writing IAM policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "dynamodb:BatchGetItem",  
        "dynamodb:GetItem",  
        "dynamodb:Query"  
      ],  
      "Resource": "*"  
    }  
  ]  
}
```

In English: Allowed to take only a few specific Amazon DynamoDB actions

Reading and writing IAM policy

```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": [  
        "dynamodb:BatchGetItem",  
        "dynamodb:GetItem",  
        "dynamodb:Query",  
      ],  
      "Resource": [  
        "arn:aws:dynamodb:us-east-2:111122223333:table/MyTableName",  
        "arn:aws:dynamodb:us-east-2:111122227773:table/MyTableName/index/*"  
      ]  
    }  
  ]  
}
```

In English: Allowed to take specific Amazon DynamoDB actions on a specific table and its indexes

This is an Amazon Resource Name (ARN);
All AWS services use them, and they follow this format

Reading and writing IAM policy

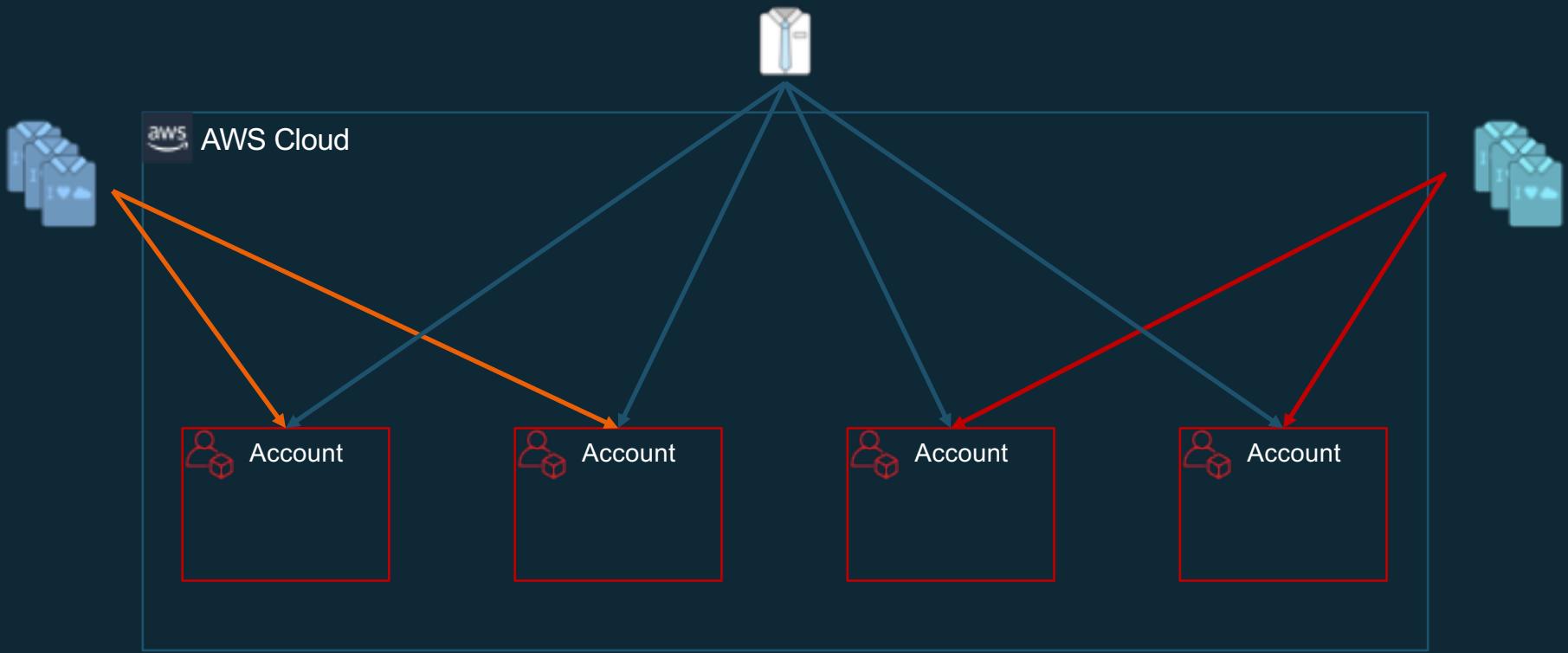
```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Effect": "Allow",  
      "Action": "secretsmanager:GetSecretValue",  
      "Resource": "*",  
      "Condition": {  
        "StringEquals": {  
          "secretsmanager:ResourceTag/Project": "${aws:PrincipalTag/Project}"  
        }  
      }  
    }  
  ]  
}
```

Attribute-based access control
(ABAC)

In English: You can read secrets whose project tag matches your own

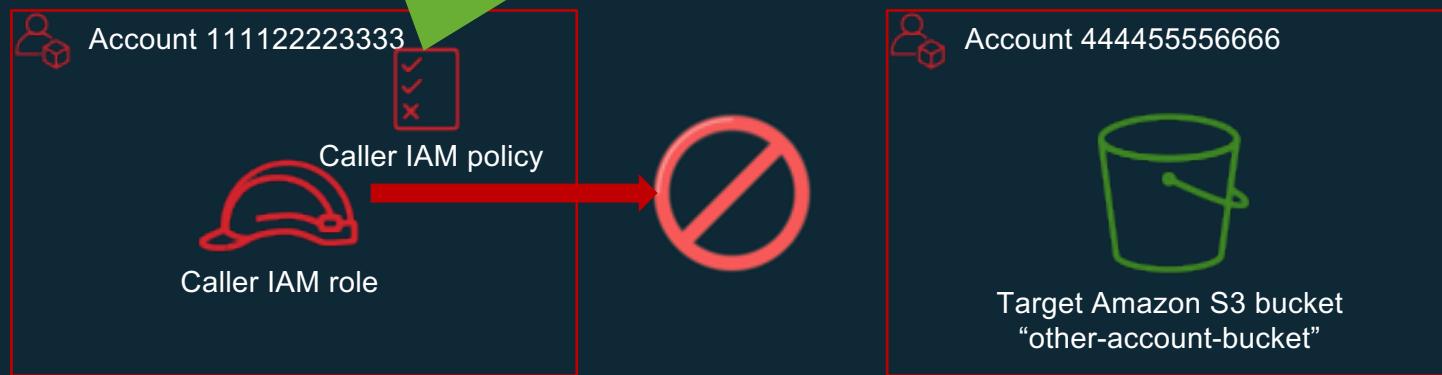


IAM in an AWS enterprise environment



Working across AWS account boundaries

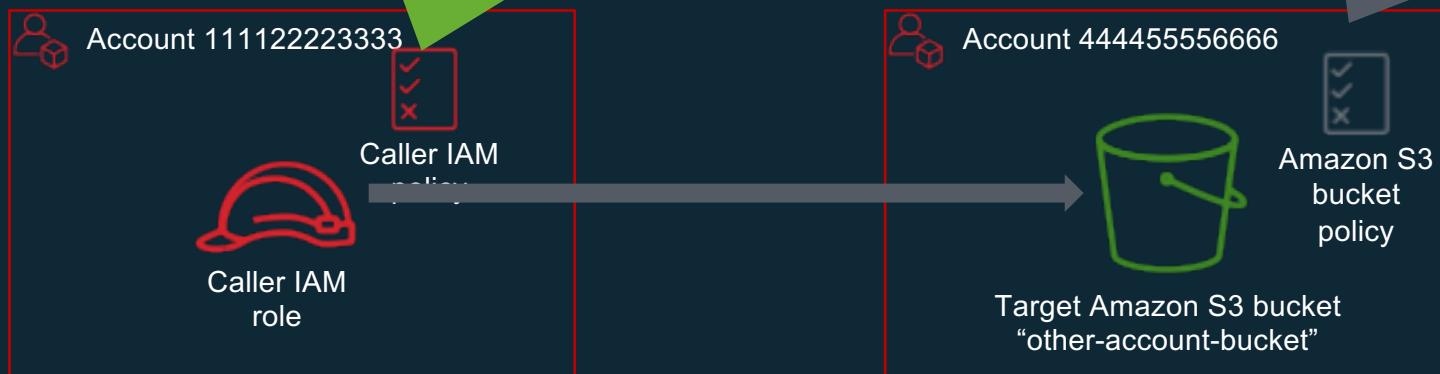
```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::other-account-bucket/*"
```



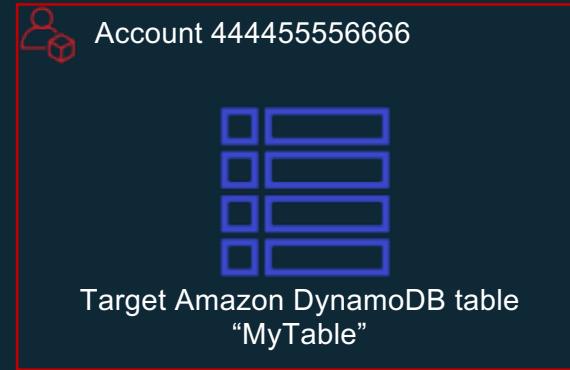
Working across AWS account boundaries

```
{  
    "Effect": "Allow",  
    "Action": "s3:GetObject",  
    "Resource": "arn:aws:s3:::other-account-bucket/*"
```

```
{  
    "Effect": "Allow",  
    "Principal": {  
        "AWS": "arn:aws:iam::111122223333:root"  
    }  
    "Action": "s3:GetObject",  
    "Resource": "arn:aws:s3:::other-account-bucket/*"
```

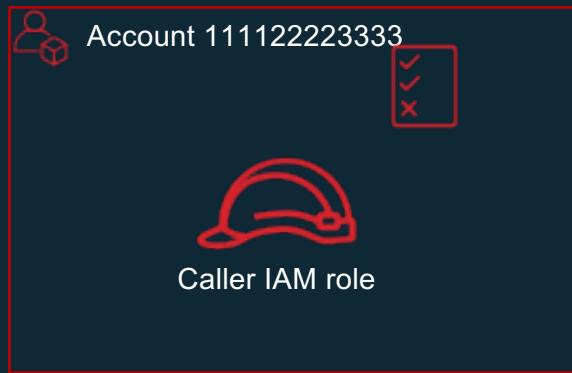


Working across AWS account boundaries



Working across AWS account boundaries

```
{  
    "Effect": "Allow",  
    "Action": "dynamodb:GetItem",  
    "Resource": "arn:aws:dynamodb:us-west-  
2:444455556666:table/MyTable"  
}
```

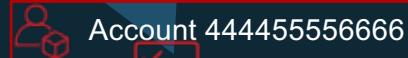


Working across AWS account boundaries

```
{  
    "Effect": "Allow",  
    "Action": "dynamodb:GetItem",  
    "Resource": "arn:aws:dynamodb:us-west-  
2:444455556666:table/MyTable"  
}
```



```
{  
    "Effect": "Allow",  
    "Action": "sts:AssumeRole",  
    "Principal": {  
        "AWS": "arn:aws:iam::111122223333:root"  
    }  
}
```



Working across AWS account boundaries

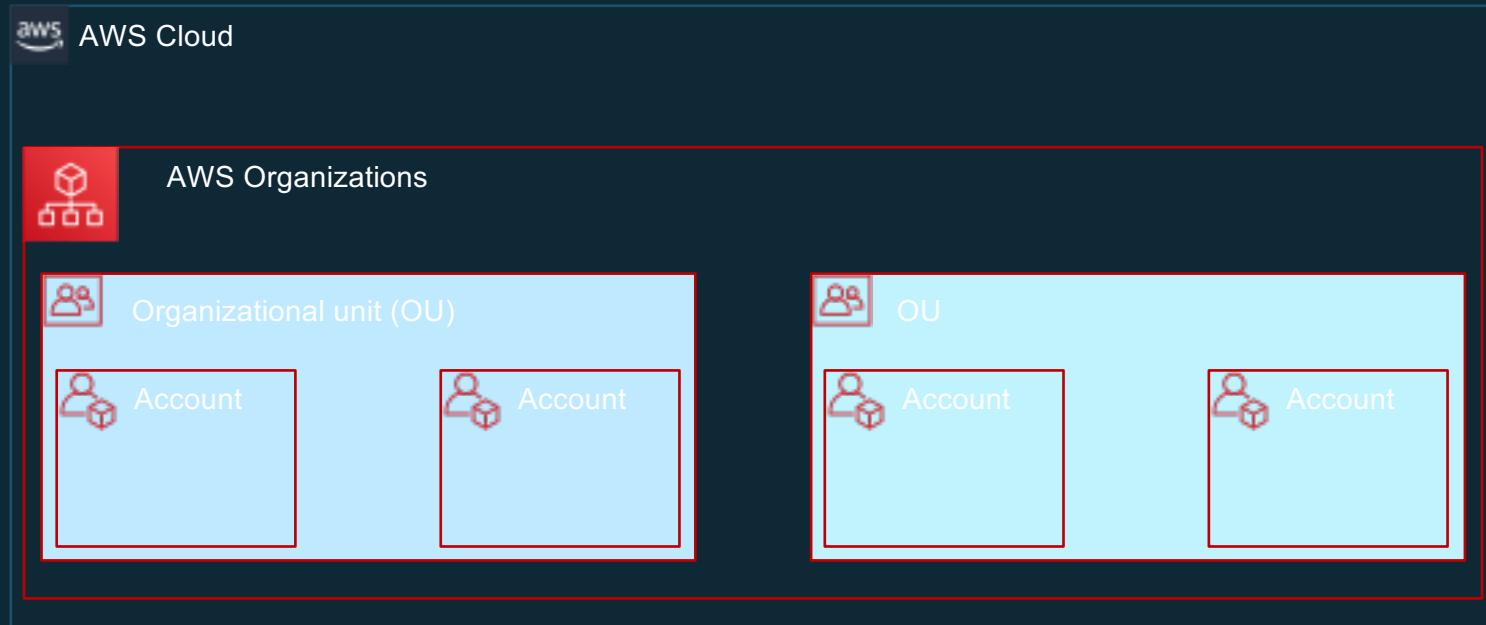
```
{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Resource": "arn:aws:iam::444455556666:role/CrossAccountAccess"  
}
```

```
{  
  "Effect": "Allow",  
  "Action": "dynamodb:GetItem",  
  "Resource": "arn:aws:dynamodb:us-west-  
2:444455556666:table/MyTable"
```



```
{  
  "Effect": "Allow",  
  "Action": "sts:AssumeRole",  
  "Principal": {  
    "AWS": "arn:aws:iam::111122223333:root"  
  }  
}
```

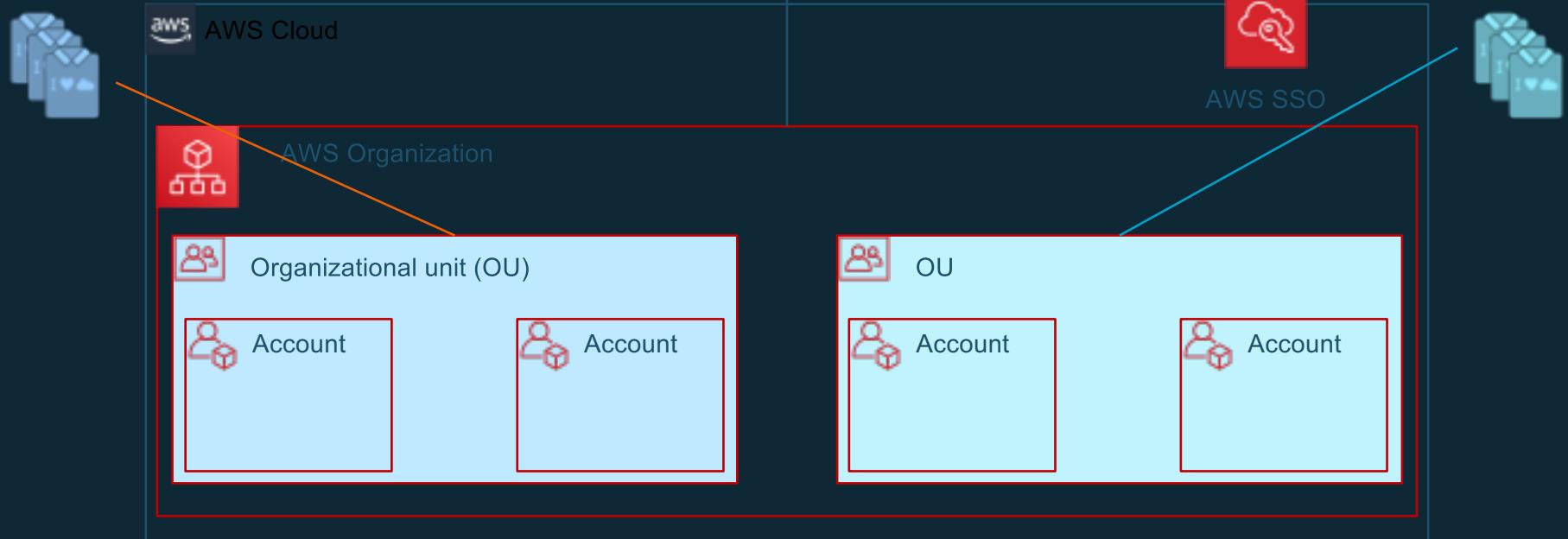
Managing multi-account environments with AWS Organizations



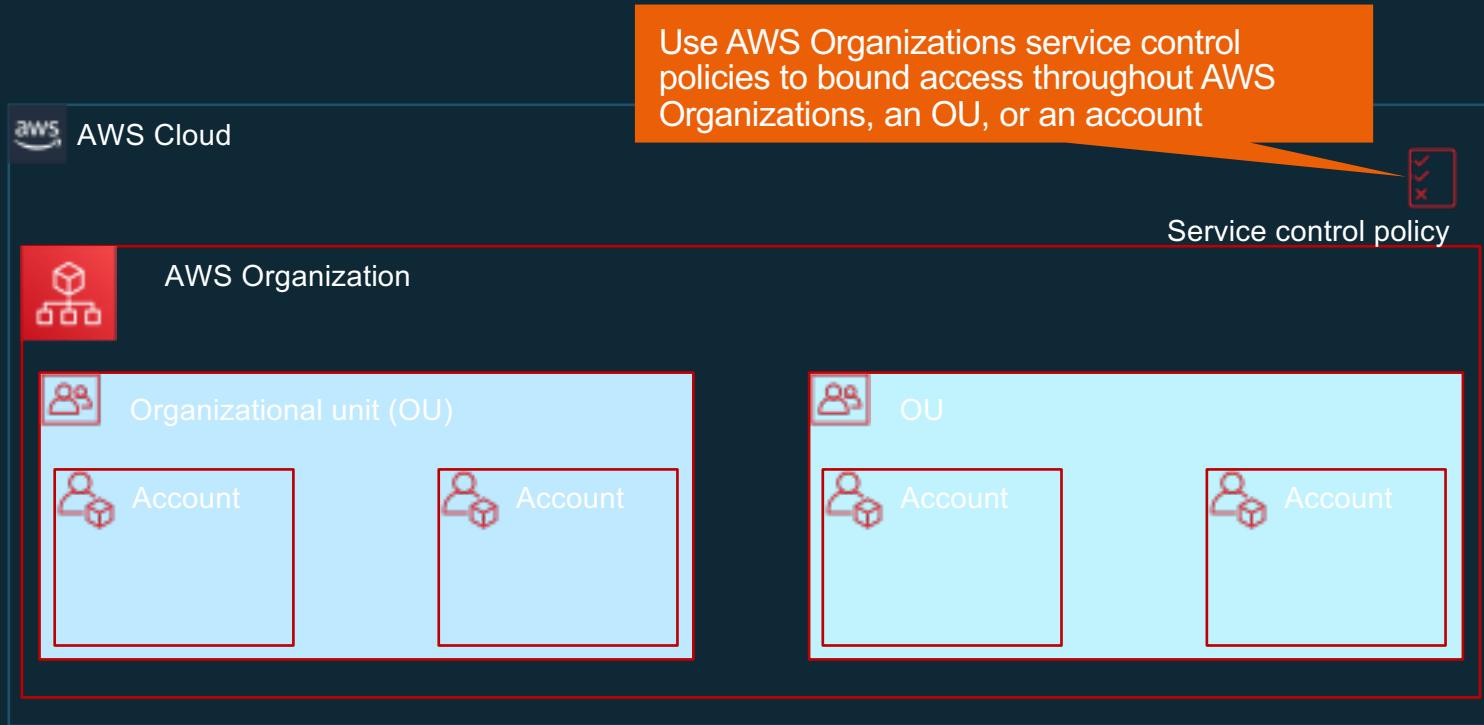
Managing multi-account environments with AWS Organizations



Use AWS Single Sign-On (AWS SSO) to map human users to accounts (or your own federation provider)



AWS Organizations provides guardrails for IAM





4

Encryption

How are you currently encrypting your data?

The mechanics of an AWS KMS key

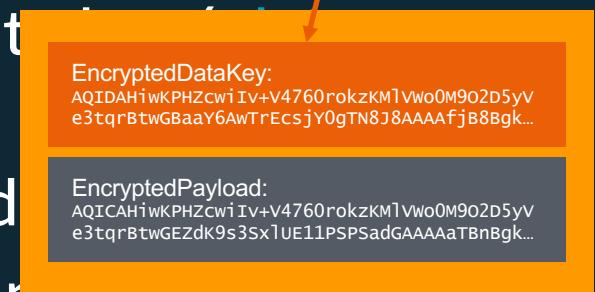


For encrypting individual pieces of data (<=4KB)

- KMS.Encrypt("hello world") → AQICAHiwKPHZcwlv....
- KMS.Decrypt("AQICAHiwKPHZcwlv....") → "hello world"

For encrypting application data, use envelope encryption

- KMS.GenerateDataKey → symmetric data and **encrypted**
- Use **plaintext** data key to encrypt your data
- Store **encrypted** data key alongside your data
- To decrypt



Why you didn't need to understand that:

AWS services manage the AWS KMS mechanics for you

Encrypting the easy way with AWS service integrations

The screenshot shows the 'Create bucket' wizard in progress, specifically the 'Configure options' step (step 2). The interface includes tabs for 'Name and region' (marked with a checkmark), 'Configure options', 'Set permissions', and 'Review'. In the 'Configure options' tab, there are sections for 'Tags', 'Object-level logging', and 'Default encryption'. The 'Default encryption' section contains a checked checkbox for 'Automatically encrypt objects when they are stored in S3.' Below this, two radio button options are shown: 'AES-256' (selected) and 'AWS-KMS' (disabled). A large orange callout bubble points from the text 'Amazon S3 manages the encryption key' to the 'AES-256' option. At the bottom of the screen, a search bar shows the text 'aws/s3'.

Amazon S3 manages the encryption key

Create bucket

① Name and region ② Configure options ③ Set permissions ④ Review

Tags
You can use tags to track project costs. [Learn more](#)

Object-level logging
 Record object-level API activity using AWS CloudTrail for an additional charge

Default encryption
 Automatically encrypt objects when they are stored in S3. [Learn more](#)

AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

Type to search

aws/s3

Advanced

arn:aws:kms:us-east-1:XXXXXXXXXX:key/84d3eb0c-b920-4f21-b316-4d27b85f07a9

aws/s3

CloudWatch

Encrypting the easy way with AWS service integrations

An AWS KMS key in your account is used for encryption: Customer master key (CMK)

Create bucket

① Name and region ② Configure options ③ Set permissions ④ Review

Tags
You can use tags to track project costs. [Learn more](#)

Object-level logging
 Record object-level API activity using AWS CloudTrail for an additional fee.

Default encryption

Automatically encrypt objects when they are stored in S3. [Learn more](#)

AES-256
Use Server-Side Encryption with Amazon S3-Managed Keys (SSE-S3)

AWS-KMS
Use Server-Side Encryption with AWS KMS-Managed Keys (SSE-KMS)

aws/s3

Type to search

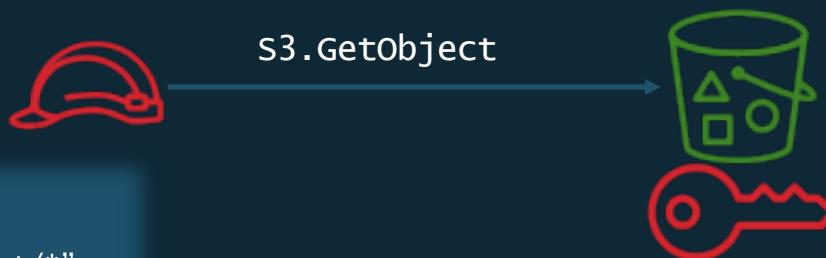
Management

CloudWatch

IAM permissions for AWS KMS keys

Question: What happens here?

```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::my-bucket/*"  
}
```



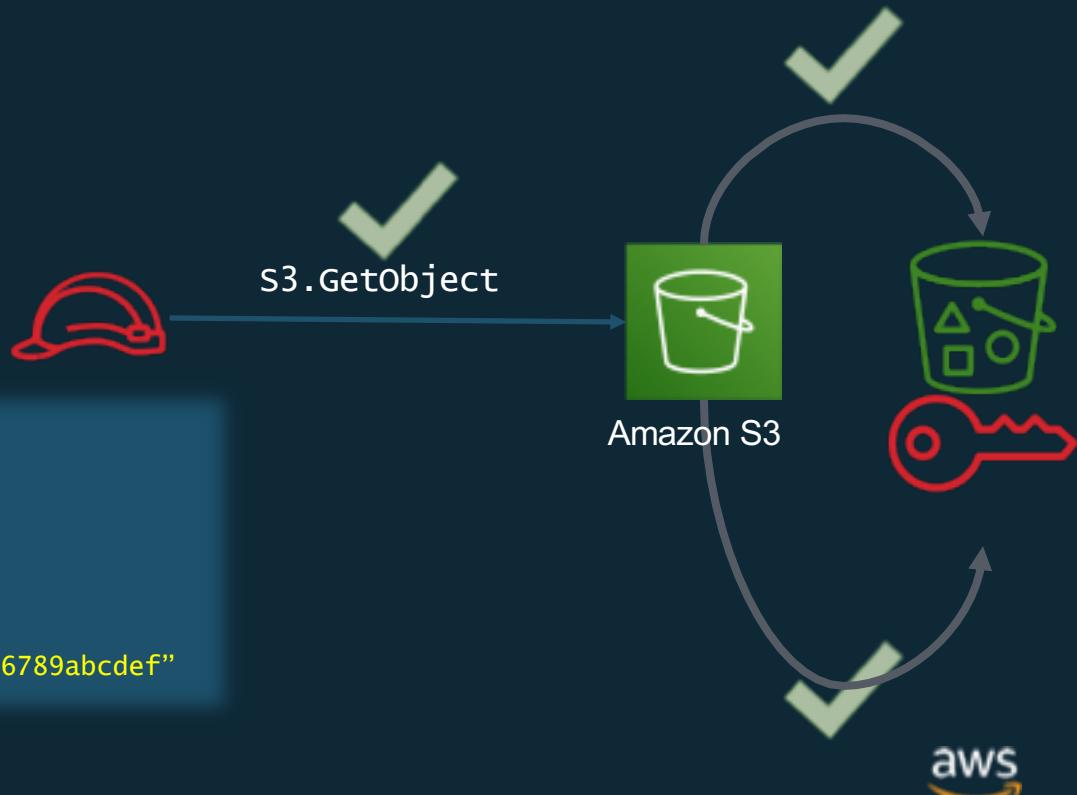
IAM permissions for AWS KMS keys

```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::my-bucket/*"  
}
```



IAM permissions for AWS KMS keys

```
{  
  "Effect": "Allow",  
  "Action": "s3:GetObject",  
  "Resource": "arn:aws:s3:::my-bucket/*"  
},  
{  
  "Effect": "Allow",  
  "Action": "kms:Decrypt",  
  "Resource": "arn:aws:kms:us-east-  
2:111122223333:key/01234567-89ab-cdef-0123-456789abcdef"  
}
```





Configuration Management

Amazon Inspector

- Vulnerability Assessment Service
 - Built from the ground up to support DevSecOps
 - Automatable via APIs
 - Integrates with CI/CD tools
 - On-Demand Pricing model
 - Static & Dynamic Rules Packages
 - Generates Findings



AWS WAF



Web Traffic Filtering with Custom Rules

Create custom rules that can block, allow or monitor requests based on IP address, HTTP headers, or a combination of both.



Malicious Request Blocking

AWS WAF can recognize and block common web application security risks like SQL injection (SQLi) and cross-site scripting (XSS).



Active monitoring & tuning

Monitor and configure the requests that are being blocked and allowed by the Web ACL rules.

AWS CloudTrail

Web service that records AWS API calls for your account and delivers logs.

Who?	When?	What?	Where to?	Where from?
Bill	3:27pm	Launch Instance	us-west-2	72.21.198.64
Alice	8:19am	Added Bob to admin group	us-east-1	127.0.0.1
Steve	2:22pm	Deleted DynamoDB table	eu-west-1	205.251.233.176

```
{
  "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",
        "sessionContext": {
          "attributes": {
            "mfaAuthenticated": "false",
            "creationDate": "2014-03-25T18:45:11Z"
          }
        }
      },
      "eventTime": "2014-03-25T21:08:14Z",
      "eventSource": "iam.amazonaws.com",
      "eventName": "AddUserToGroup",
      "awsRegion": "us-east-1",
      "sourceIPAddress": "127.0.0.1",
      "userAgent": "AWSConsole",
      "requestParameters": {
        "userName": "Bob",
        "groupName": "admin"
      },
      "responseElements": null
    },
    ...additional entries
  ]
}
```

AWS CloudWatch

Monitoring services for AWS Resources and AWS-based Applications.

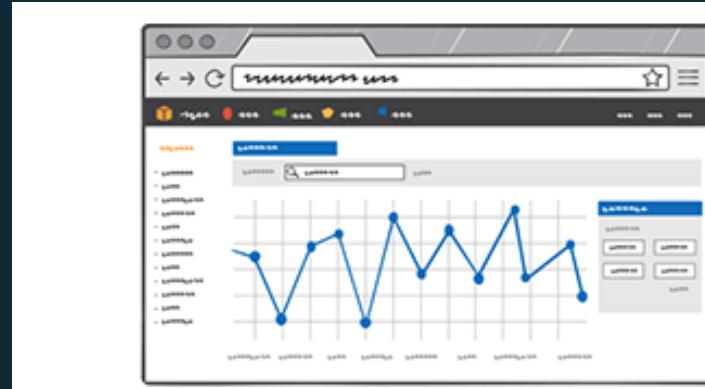
What does it do?

Collect and Track Metrics

Monitor and Store Logs

Set Alarms (react to changes)

View Graphs and Statistics



How can you use it?

Monitor CPU, Memory, Disk I/O, Network, etc.

CloudWatch Metrics

React to application log events and availability

CloudWatch Logs / CloudWatch Events

Automatically scale EC2 instance fleet

CloudWatch Alarms

View Operational Status and Identify Issues

CloudWatch Dashboards

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

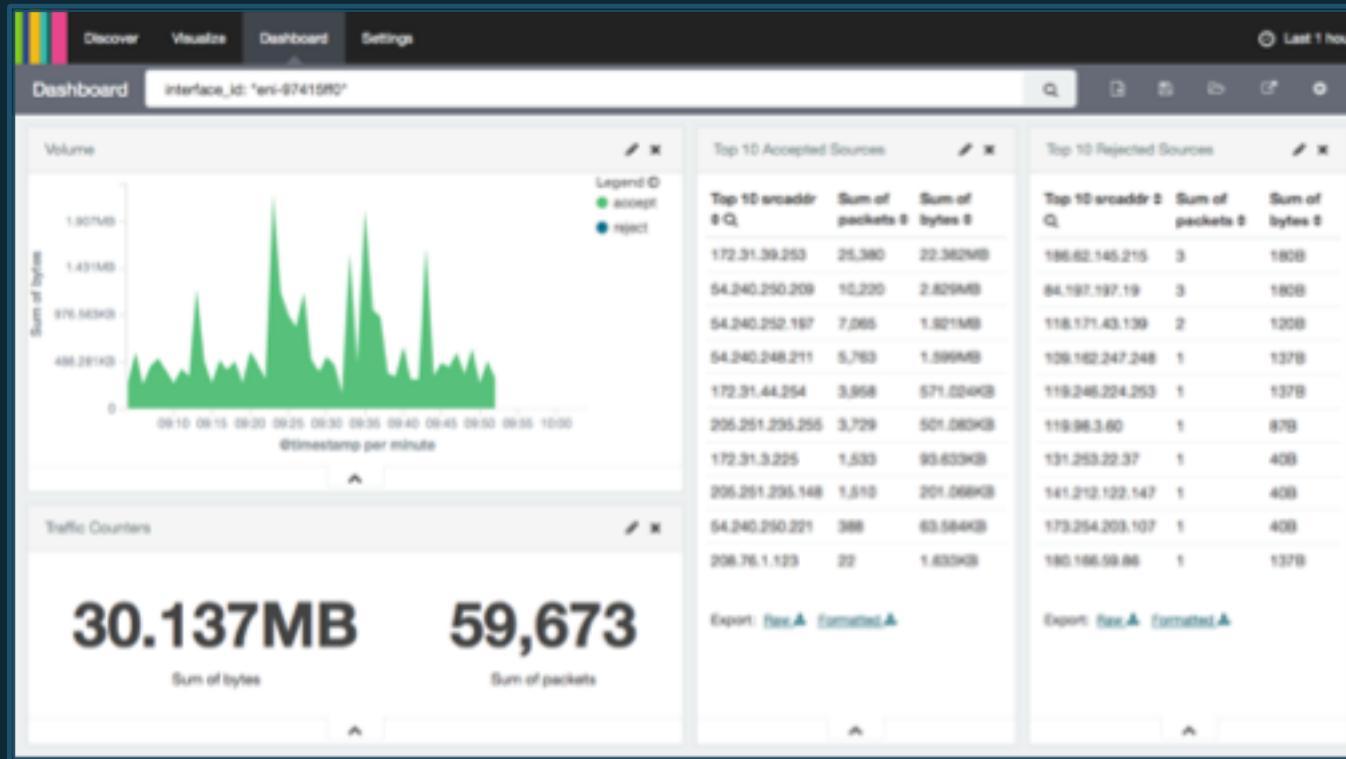
The diagram illustrates the structure of VPC Flow Log data as it appears in AWS CloudWatch Logs. The data is presented in a table format with the following columns:

Event Data	Interface	Source IP	Source port	Protocol	Packets	Destination IP	Destination port	Bytes	Start/end time	Accept or reject
▼ 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

Annotations with arrows point to specific columns and rows:

- An arrow labeled "AWS account" points to the first column.
- Arrows labeled "Interface", "Source IP", "Source port", "Protocol", "Packets", "Destination IP", "Destination port", "Bytes", and "Start/end time" point to their respective columns.
- An arrow labeled "Accept or reject" points to the last column.

VPC Flow Logs



- Amazon Elasticsearch Service
- Amazon CloudWatch Logs subscriptions

AWS Config

Managed service for tracking AWS inventory and configuration, and configuration change notification.



Security Analysis

Audit Compliance

Change Management

Troubleshooting

Discovery



Additional Best Practices

AWS Trusted Advisor

Leverage Trusted Advisor to analyze your AWS resources for best practices for availability, cost, performance and security.

Trusted Advisor Dashboard

Welcome to the AWS Trusted Advisor console! For more information, see [Meet AWS Trusted Advisor](#).

Cost Optimization



2 ✓ 5 ▲ 0 !
0 excluded items
\$331.20
Potential monthly savings

Performance



6 ✓ 2 ▲ 0 !
0 excluded items

Security



4 ✓ 1 ▲ 4 !
1 excluded items

Fault Tolerance



8 ✓ 3 ▲ 2 !
0 excluded items

[Download](#)   

Security

 4 ✓ 1 ▲ 4 !
1 excluded items

[View](#) [All checks](#)  

Security Checks

 Security Groups - Specific Ports Unrestricted Checks security groups for rules that allow unrestricted access (0.0.0.0/0) to specific ports. 44 of 124 security group rules allow unrestricted access to a specific port.	Updated: Dec 22, 2014 6:32 AM	 
 Security Groups - Unrestricted Access Checks security groups for rules that allow unrestricted access to a resource. 47 of 124 security group rules have a source IP address with a /0 suffix. 1 items have been excluded.	Updated: Dec 22, 2014 6:24 AM	 
 Amazon S3 Bucket Permissions Checks buckets in Amazon Simple Storage Service (Amazon S3) that have open access permissions.	Updated: Dec 22, 2014 6:24 AM	 

Amazon Macie

Leverage Amazon Macie to help prevent data loss in AWS.

The screenshot shows the Amazon Macie interface. On the left, a sidebar includes links for ALERTS, DASHBOARD (selected), REPORTS, RESEARCH, SETTINGS, and INTEGRATIONS. The main dashboard area displays the following metrics:

- Critical Assets: 2 (Risk level 8 to 10)
- Total Events: 681k
- Total User Sessions: 147k (4 unique users)
- Total users (44): 4 (blue), 3 (yellow), 23 (grey), 14 (red)

Below these metrics is a section titled "Minimum Risk: 6" with a slider. To the right, there's a "Total Matching Themes" section showing 11 unique risky themes. A donut chart at the bottom indicates the distribution of data types across time ranges: All Data (blue), Range - 0 - 6 months ago (orange), and Range - beyond 6 months ago (light blue).

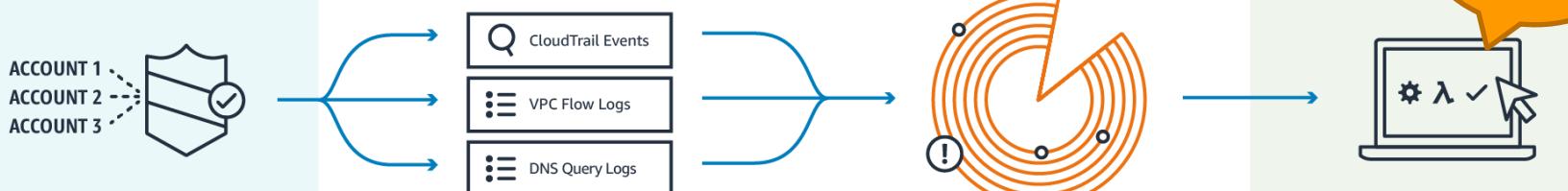
On the right side of the dashboard, a sidebar lists categories: ALERTS (selected) and DASHBOARD. Other categories include Admin (2), Audit (3), Device (2), Identity (2), Login (2), S3 (1), S3 (2), S3 (3), Location Anomaly (2), Anonymous Proxy (2), Malicious Location (2), S3 (4), Behavioral Anomaly (1), Custom Alert (200), and Predictive (2).

The interface also displays a list of alerts:

- S3 Bucket uses IAM policy to grant read rights to Everyone (100, CUSTOM_ALERT, S3, 11 minutes ago, 0 comments, 0 events)
- S3 Bucket uses IAM policy to grant read rights to Everyone (100, CUSTOM_ALERT, S3, 21 minutes ago, 0 comments, 0 events)
- Access Denied In Secure Account (50, CUSTOM_ALERT, S3, 46 minutes ago, 0 comments, 0 events)

Amazon GuardDuty

Intelligent Threat Detection and Notification



Enable GuardDuty

With a few clicks in the console, monitor your AWS accounts without additional security software or infrastructure to deploy or manage

Continuously analyze

Automatically analyze network and account activity at scale providing broad, continuous monitoring of your AWS accounts and workloads

Intelligently detect threats

Utilize managed rule-sets, integrated threat intelligence, anomaly detection, and machine learning to intelligently detect malicious or unauthorized behavior

Leverage actionable alerts

Review detailed findings in the console, integrate into event management or workflow systems, or trigger AWS Lambda for automated remediation or prevention

AWS Marketplace Security Partners

Infrastructure Security



Logging & Monitoring



Identity & Access Control



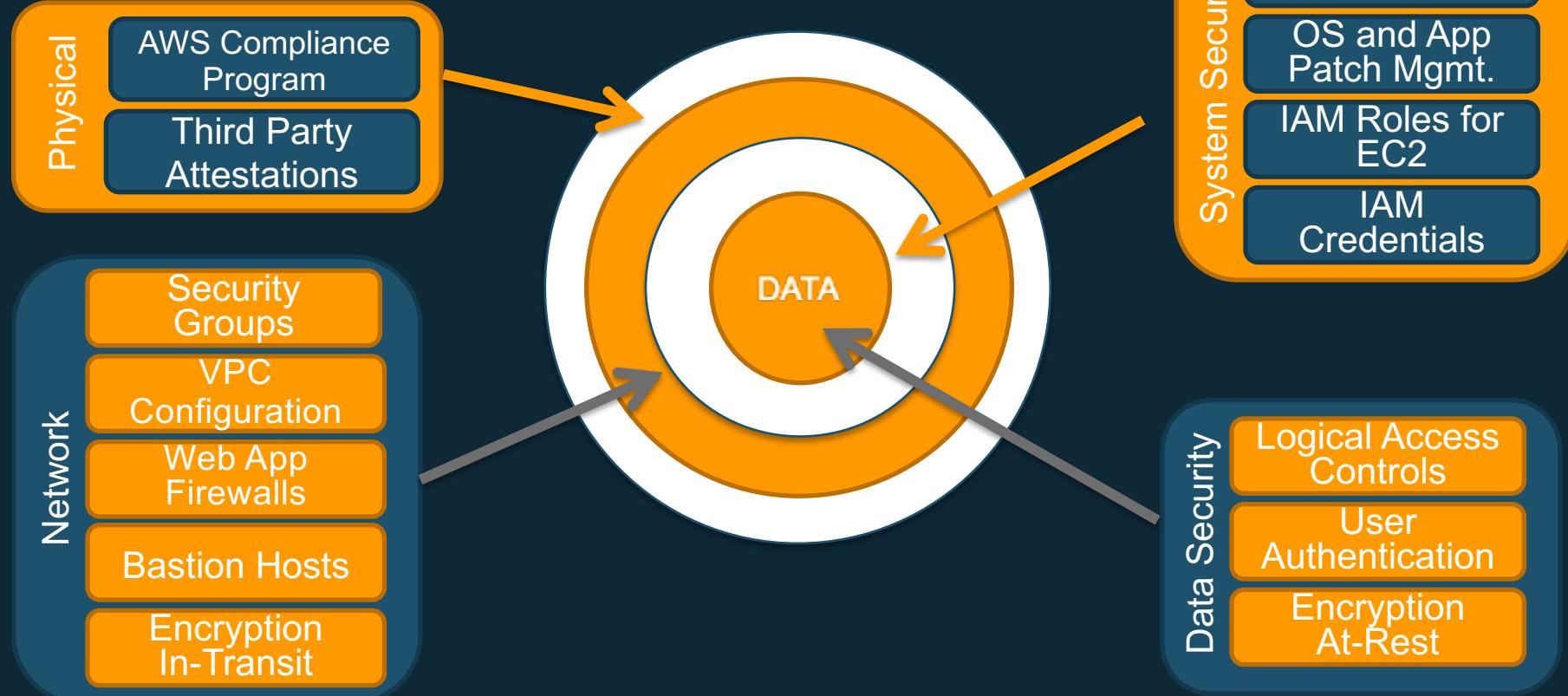
Configuration & Vulnerability Analysis



Data Protection



Defense-in-Depth





AWS Security Center

AWS Security Center

Comprehensive security portal to provide a variety of security notifications, information and documentation.

<http://aws.amazon.com/security>



The screenshot shows the AWS Security Center homepage. The top navigation bar includes links for Products, Solutions, Software, Pricing, More, English, My Account, and Sign In to the Console. On the left, there's a sidebar with sections for About AWS (AWS Security Center, Security Resources, Vulnerability Reporting, Penetration Testing, Report Suspicious Emails, Security Bulletins) and Related Links (AWS Compliance, AWS Architecture Center, AWS Security Blog). The main content area features a heading "AWS Security Center" and a paragraph about the secure cloud computing environment. Below that is a section titled "World-Class Protection" with a detailed description of AWS's infrastructure and security measures. At the bottom, there's a testimonial from JD Sherry, VP of Technology at Trend Micro, and a video play button.

Security Whitepapers

- Overview of Security Process
- AWS Risk and Compliance
- AWS Security Best Practices

Security Bulletin

Security Resources

Vulnerability Reporting

Penetration Testing

Requests

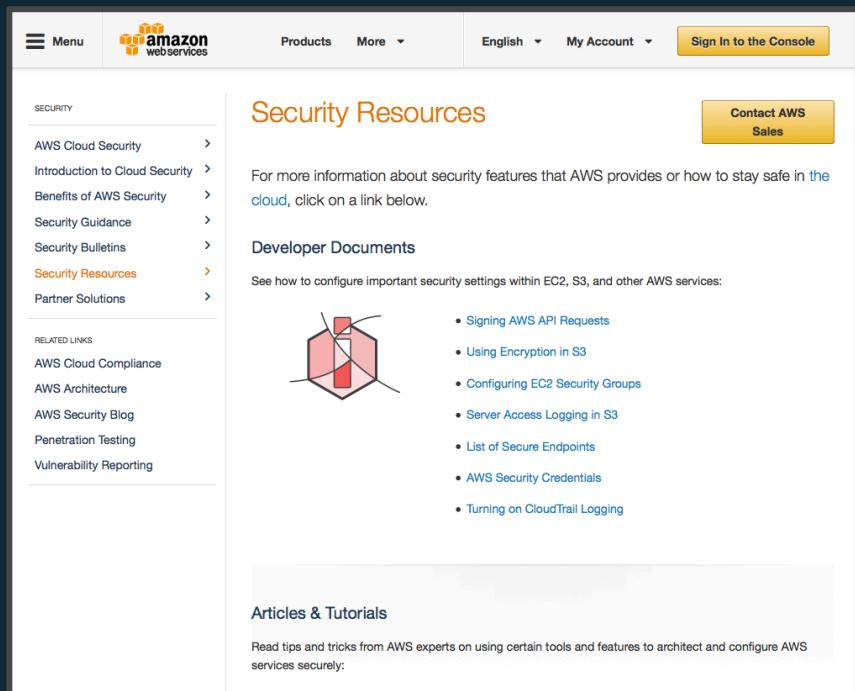
Report Suspicious Emails



Security Resources

<http://aws.amazon.com/security/security-resources/>

Developer Information, Articles and Tutorials,
Security Products, and Whitepapers

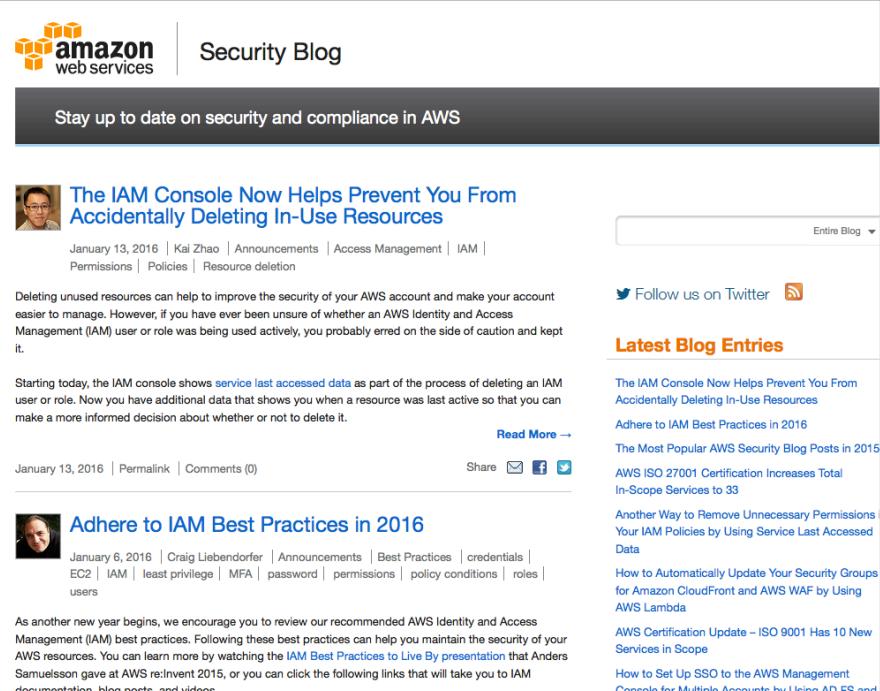


The screenshot shows the AWS Security Resources page. At the top, there's a navigation bar with 'Menu', the Amazon logo, 'Products', 'More', 'English', 'My Account', and a 'Sign In to the Console' button. Below the navigation, a sidebar on the left lists 'SECURITY' categories: AWS Cloud Security, Introduction to Cloud Security, Benefits of AWS Security, Security Guidance, Security Bulletins, Security Resources (which is selected and highlighted in orange), and Partner Solutions. Under 'RELATED LINKS', it lists AWS Cloud Compliance, AWS Architecture, AWS Security Blog, Penetration Testing, and Vulnerability Reporting. The main content area has a title 'Security Resources' with an orange background. It contains a paragraph about security features and a 'Contact AWS Sales' button. Below this is a section titled 'Developer Documents' with a sub-section 'See how to configure important security settings within EC2, S3, and other AWS services:' followed by a list of items like 'Signing AWS API Requests', 'Using Encryption in S3', etc. At the bottom, there's an 'Articles & Tutorials' section with a sub-section 'Read tips and tricks from AWS experts on using certain tools and features to architect and configure AWS services securely:'.

AWS Security Blog

<http://blogs.aws.amazon.com/security/>

Subscribe to the blog – it's a great way to stay up-to-date on AWS security and compliance.



The screenshot shows the AWS Security Blog page. At the top, there's the Amazon logo and the text 'Security Blog'. Below this is a dark banner with the text 'Stay up to date on security and compliance in AWS'. The main article is titled 'The IAM Console Now Helps Prevent You From Accidentally Deleting In-Use Resources' by Kai Zhao, published on January 13, 2016. It includes a small profile picture of Kai Zhao. The article discusses how the IAM console now shows service last accessed data when deleting resources. Below the article is a 'Read More →' link, the publication date, and sharing options. To the right, there's a sidebar with a 'Follow us on Twitter' button and a 'Latest Blog Entries' section listing several recent posts. The first entry in the sidebar is 'Adhere to IAM Best Practices in 2016' by Craig Liebendorfer, published on January 6, 2016.



Questions