Credit: https://wallpapercave.com/w/wp2169364

AWS Security Best Practices

@linux_girl

10/31/2020

DISCLAIMER

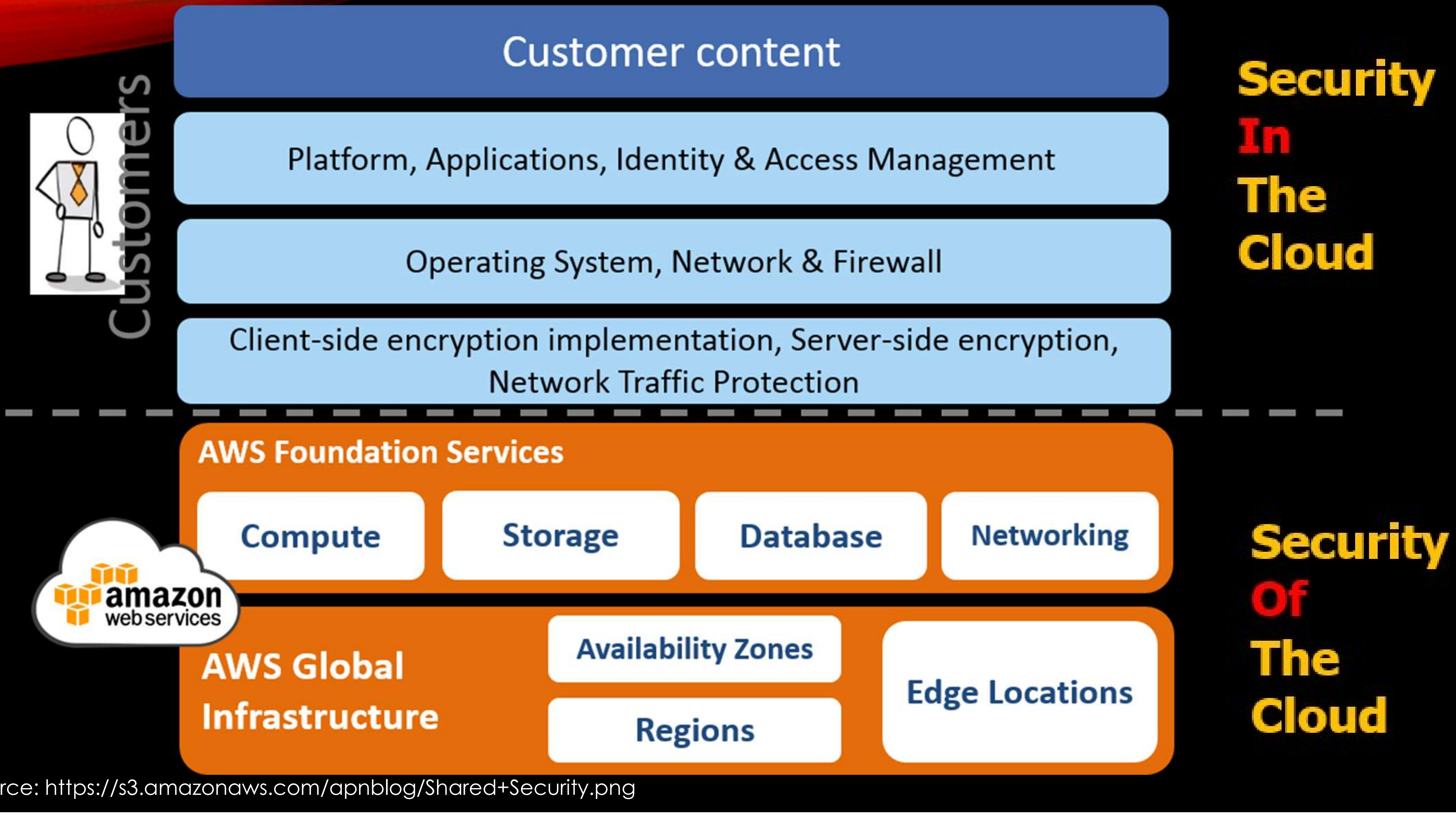
The views, thoughts and opinions expressed in this presentation belong solely to the author and not necessarily to the author’s employer, organization, committee or other group or individual

OH, YOU USE CLOUD COMPUTING?
YOUR WORK MUST BE SO SECURE

“By 2023, **75%** of security failures will result from mismanagement of IAM privileges”

Gartner, 2020

AWS SHARED RESPONSIBILITY MODEL



Customers

Customer content

Platform, Applications, Identity & Access Management

Operating System, Network & Firewall

Client-side encryption implementation, Server-side encryption, Network Traffic Protection

Security In The Cloud

AWS Foundation Services

Compute

Storage

Database

Networking

amazon web services

AWS Global Infrastructure

Availability Zones

Regions

Edge Locations

Security Of The Cloud

Source: https://s3.amazonaws.com/apnblog/Shared+Security.png

AWS IDENTITY ACCESS MANAGEMENT (IAM)

User Identity System

Which Users Can Access

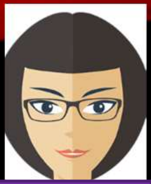
What Type Of Actions

Objects

1. Users
2. Group
3. Roles
4. Policies or
5. Permissions

Source: https://pixabay.com/

ABOUT AWS IAM OBJECTS



User:
Janet

User:
Service

#root
User:

Group: Engineering

Policies/Permissions

Role:
Developer

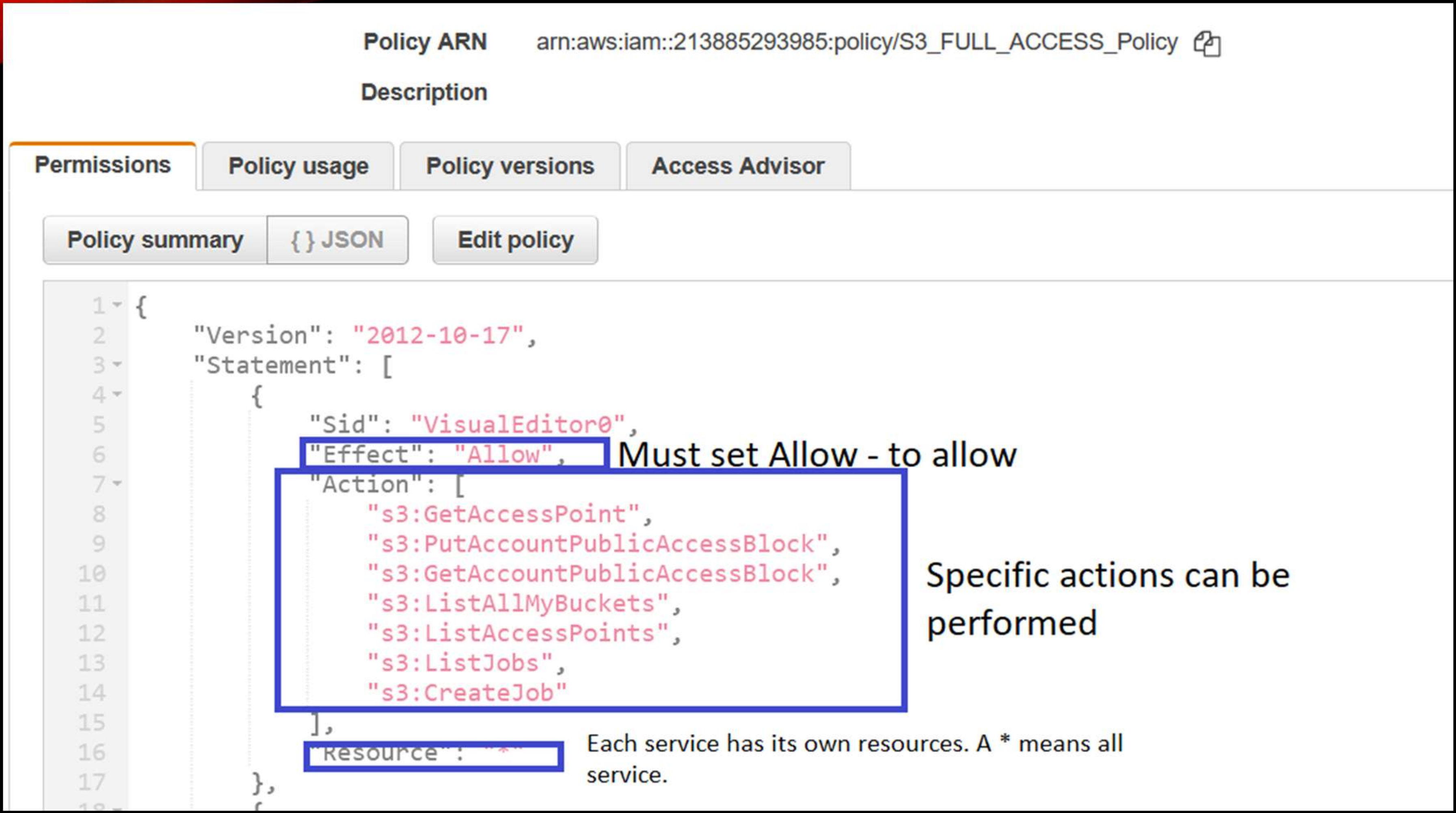
Resources
and Services

Role:
Manager

Resources
and Services

Source: http://www.geek-tips.com/wp-content/uploads/2015/01/AWS_Services.gif

EXAMPLE OF AN AWS JSON POLICY



Policy ARN arn:aws:iam::213885293985:policy/S3_FULL_ACCESS_Policy

Description

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:GetAccessPoint",
                "s3:PutAccountPublicAccessBlock",
                "s3:GetAccountPublicAccessBlock",
                "s3:ListAllMyBuckets",
                "s3:ListAccessPoints",
                "s3:ListJobs",
                "s3:CreateJob"
            ],
            "Resource": "*"
        },
        {
```

Must set Allow - to allow

Specific actions can be performed

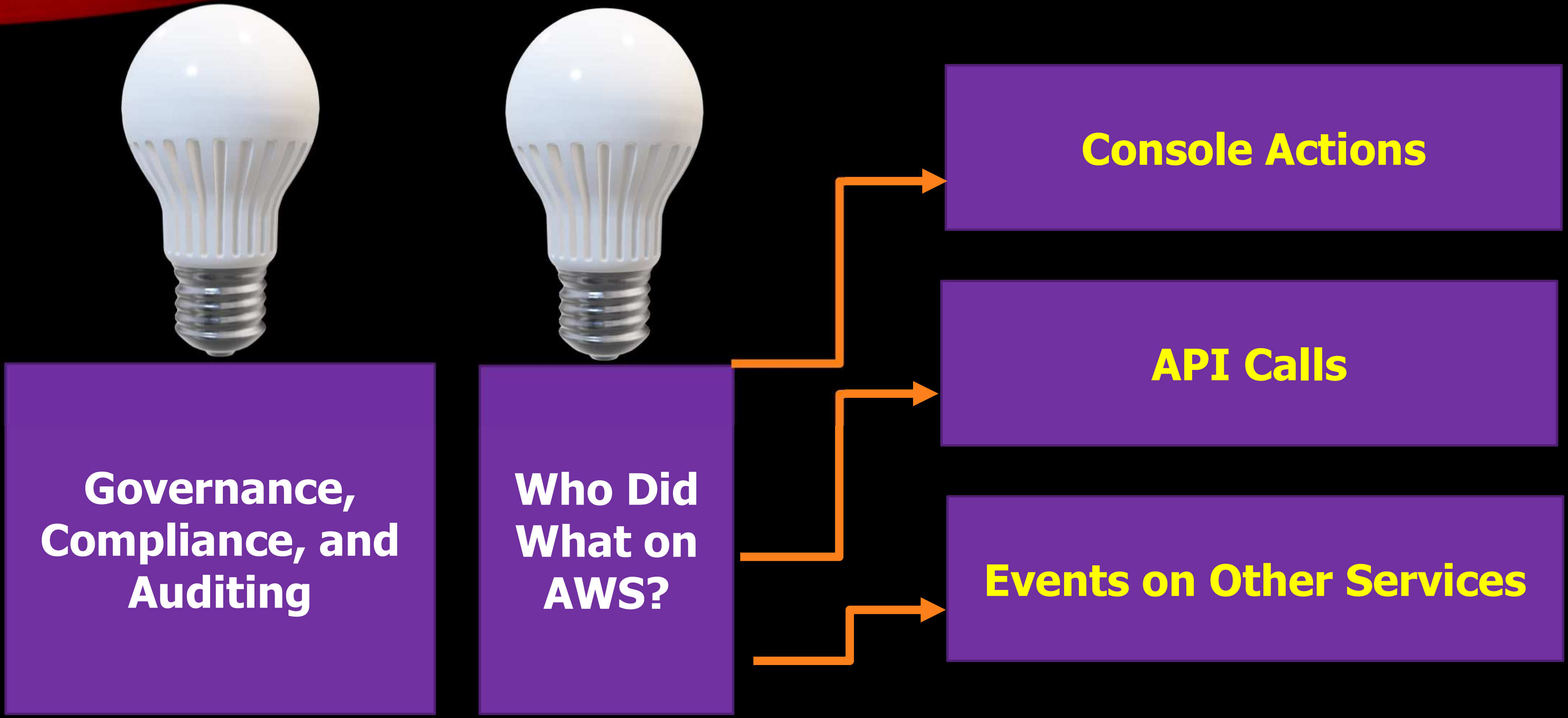
Each service has its own resources. A * means all service.

IAM BEST PRACTICES

- Enforce Strong Passwords
- Use Multifactor Authentication (MFA) is a MUST
- Don’t Use Privileged Accounts
- Never Embed Keys into Code
- Remove the Unnecessary IAM Users
- Audit Access to Resources

Source: https://i0.wp.com/quickreadbuzz.com/wp-content/uploads/2017/10/Best_Practice.jpg

AWS CLOUDTRAIL



Governance, Compliance, and Auditing

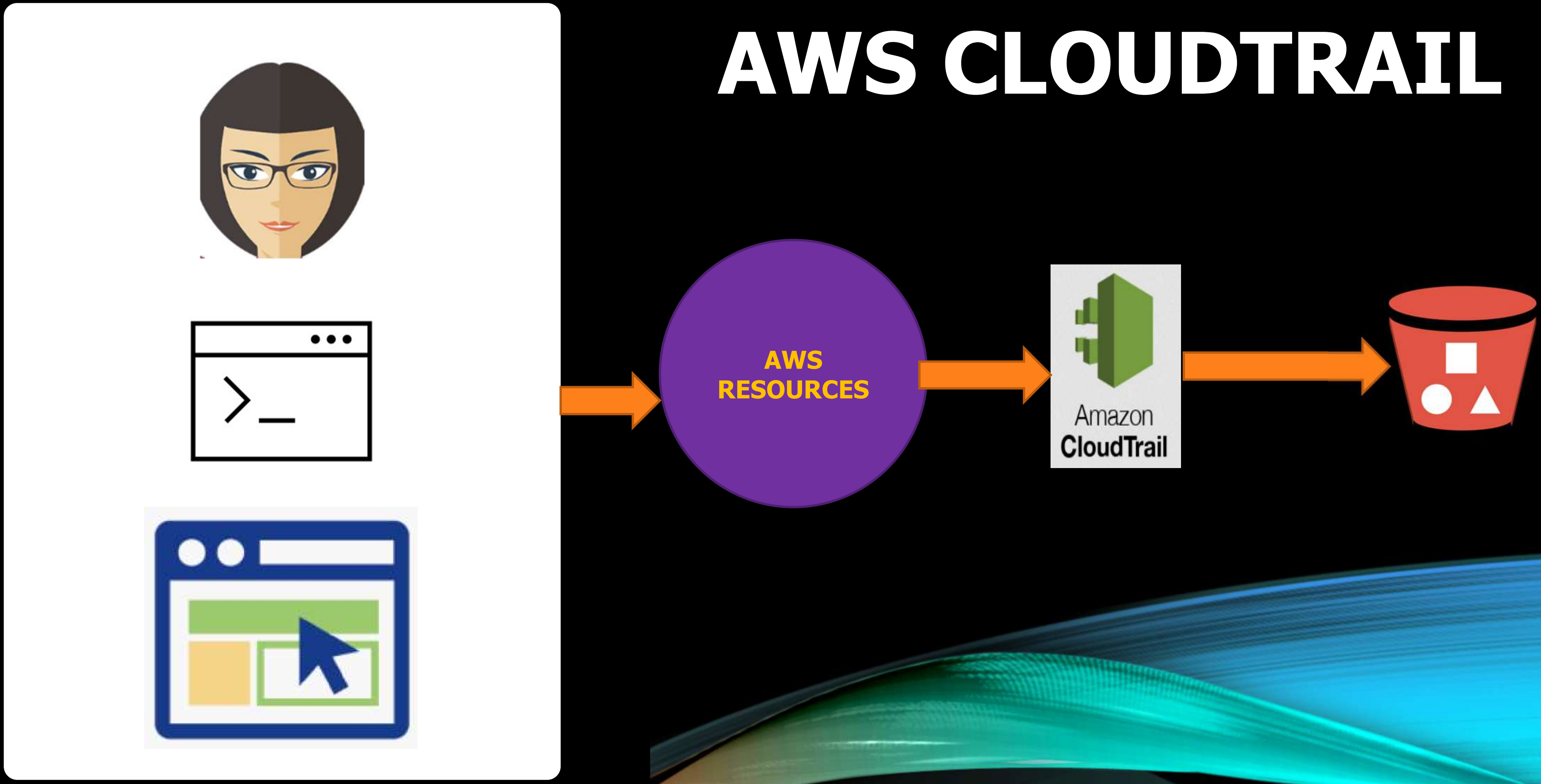
Who Did What on AWS?

Console Actions

API Calls

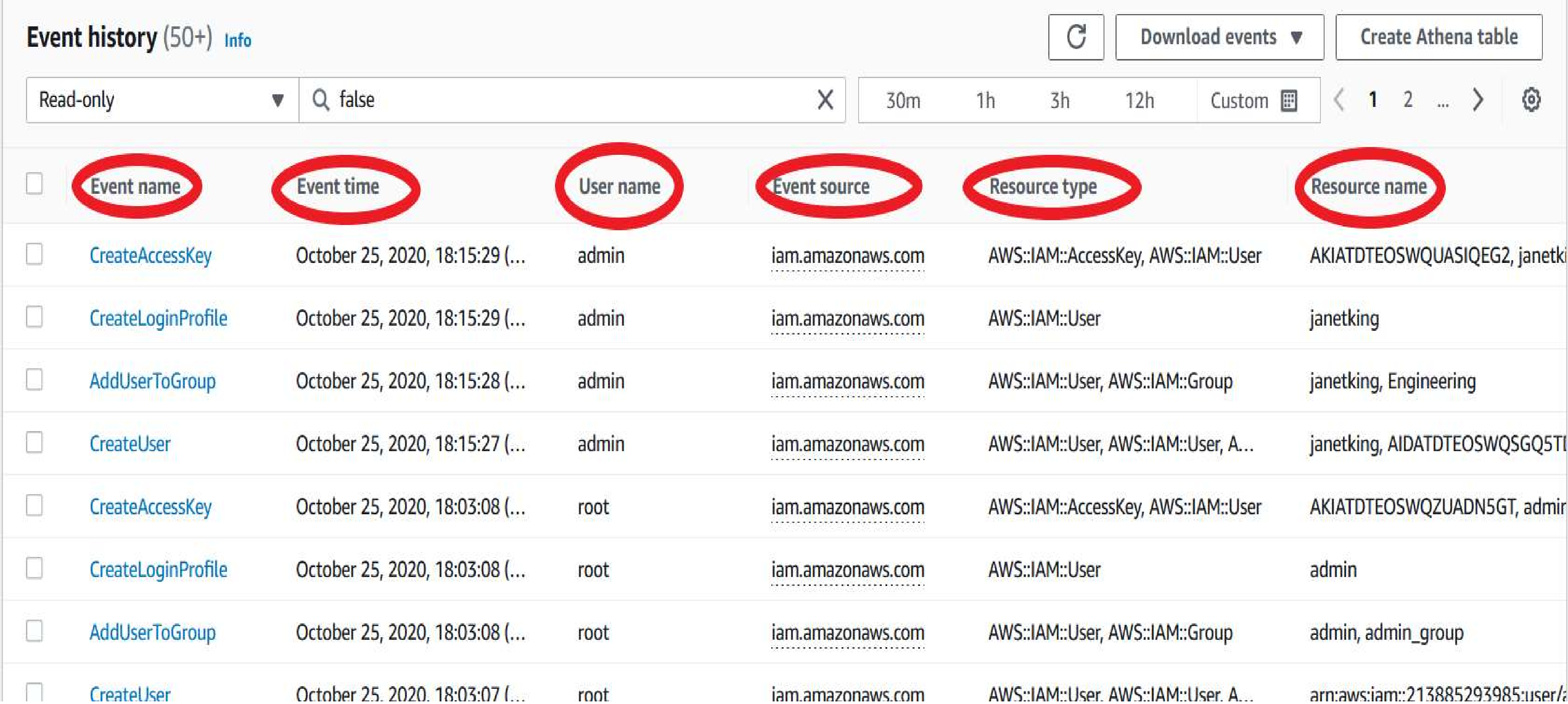
Events on Other Services

AWS CLOUDTRAIL



Source: https://imgix.datadoghq.com/img/aws-integrations/amazon_cloudtrail.png

EXAMPLE OF CLOUDTRAIL EVENTS



Event history (50+)

Read-only ▼ | false

□	Event name	Event time	User name	Event source	Resource type	Resource name
□	CreateAccessKey	October 25, 2020, 18:15:29 (...	admin	iam.amazonaws.com	AWS::IAM::AccessKey, AWS::IAM::User	AKIATDTEOSWQUASIQEG2, janetki
□	CreateLoginProfile	October 25, 2020, 18:15:29 (...	admin	iam.amazonaws.com	AWS::IAM::User	janetking
□	AddUserToGroup	October 25, 2020, 18:15:28 (...	admin	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::Group	janetking, Engineering
□	CreateUser	October 25, 2020, 18:15:27 (...	admin	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User, A...	janetking, AIDATDTEOSWQSGQ5TI
□	CreateAccessKey	October 25, 2020, 18:03:08 (...	root	iam.amazonaws.com	AWS::IAM::AccessKey, AWS::IAM::User	AKIATDTEOSWQZUADN5GT, admir
□	CreateLoginProfile	October 25, 2020, 18:03:08 (...	root	iam.amazonaws.com	AWS::IAM::User	admin
□	AddUserToGroup	October 25, 2020, 18:03:08 (...	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::Group	admin, admin_group
□	CreateUser	October 25, 2020, 18:03:07 (...	root	iam.amazonaws.com	AWS::IAM::User, AWS::IAM::User, A...	arn:aws:iam::213885293985:user/a

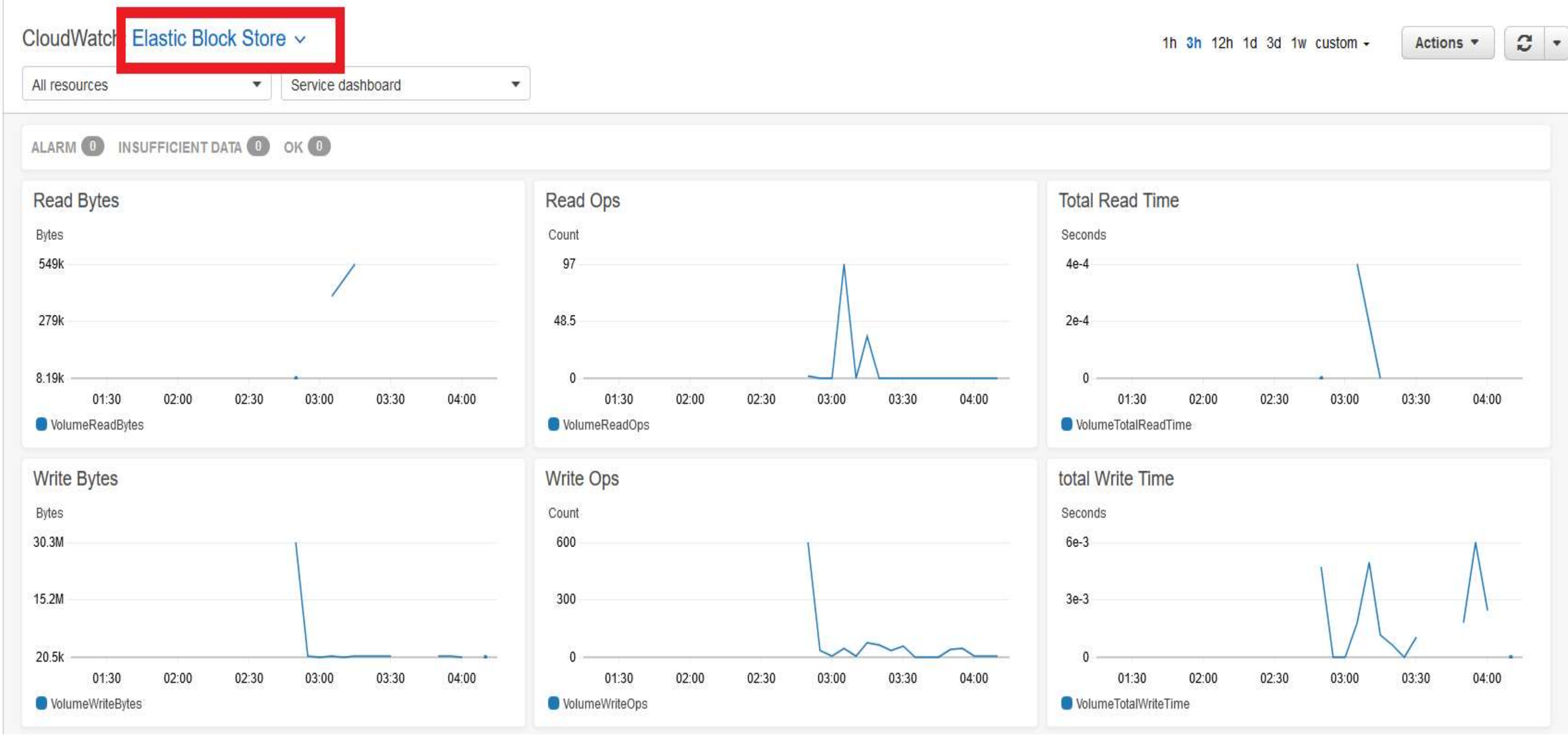
AWS CLOUDWATCH

Monitoring AWS Resources and Applications

- Track Metrics
- Collect and Monitor Logs
- Set Alarm

- Resource Utilization
- Application Performance
- Operational Health

EXAMPLE OF AN AWS CLOUDWATCH – EC2 SERVICE DASHBOARD



AWS SECURITY BEST PRACTICES

- AWS Shared Responsibility Model
- Define and Categorize Assets
- AWS Accounts, IAM Users, Groups and Roles
- Continuous Monitoring and Logging

Source: https://www.rednightconsulting.com/wp-content/uploads/2018/09/best_practices.jpg

Source: https://pixabay.com/illustrations/thank-you-letters-140227/

Source: https://pixabay.com/illustrations/question-ques[illegible]k-request-63916/

ABSTRACT

Do you use Amazon Web Services (AWS)? It's okay if you don't use it and use another cloud provider. I'm going to discuss three important AWS security services and also which security controls are AWS's responsibility and which are yours.

In this talk you will learn:

. An overview of the AWS Shared Responsibility Model

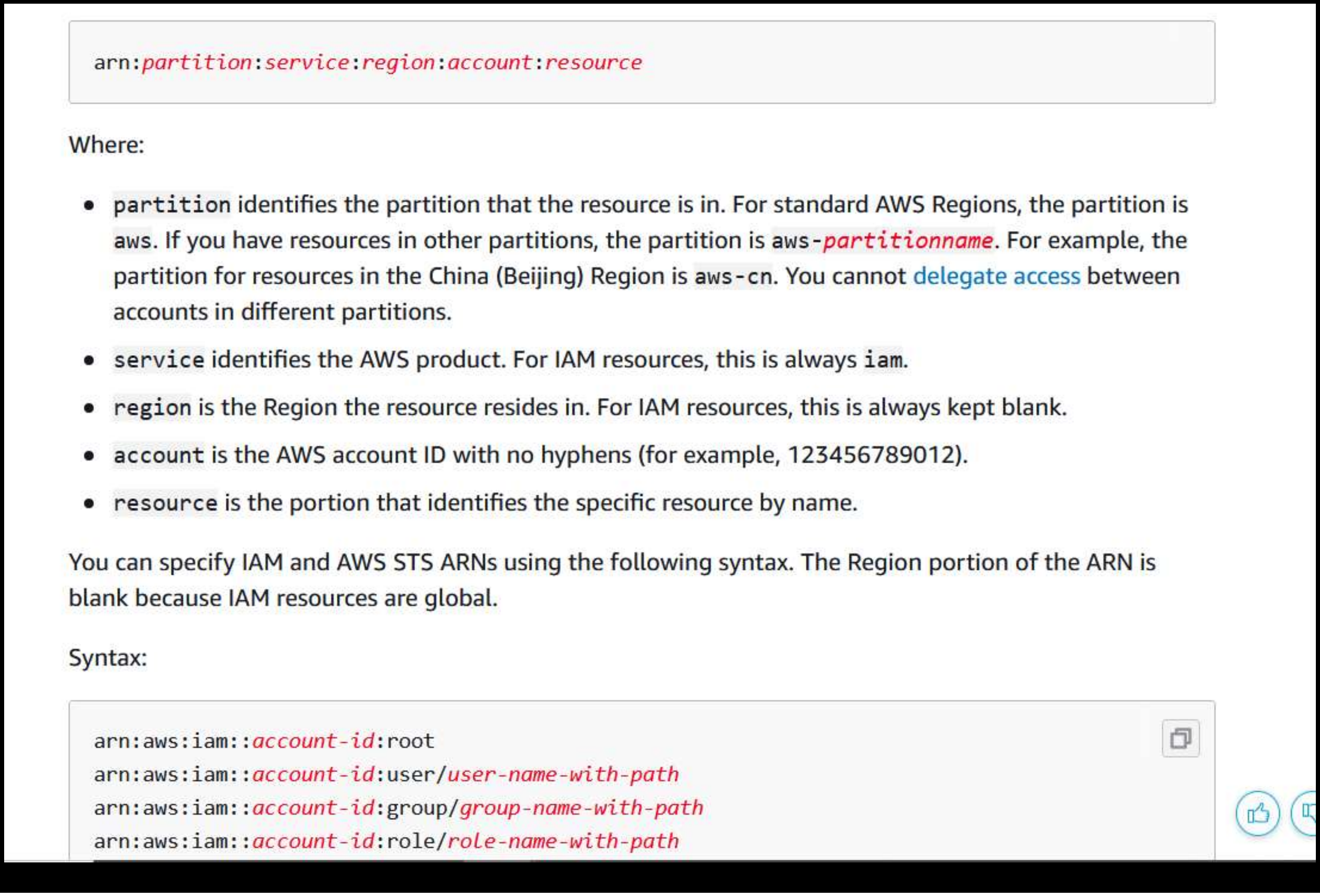
. Security best practices in AWS Identity Access Management (IAM)

. Using AWS CloudTrail and CloudWatch for logging and auditing purposes

Finally, we'll dive in to how you might benefit from implementing other AWS security practices.

BACKUP

IAM AMAZON RESOURCE NAMES (ARN)



```
arn:partition:service:region:account:resource
```

Where:

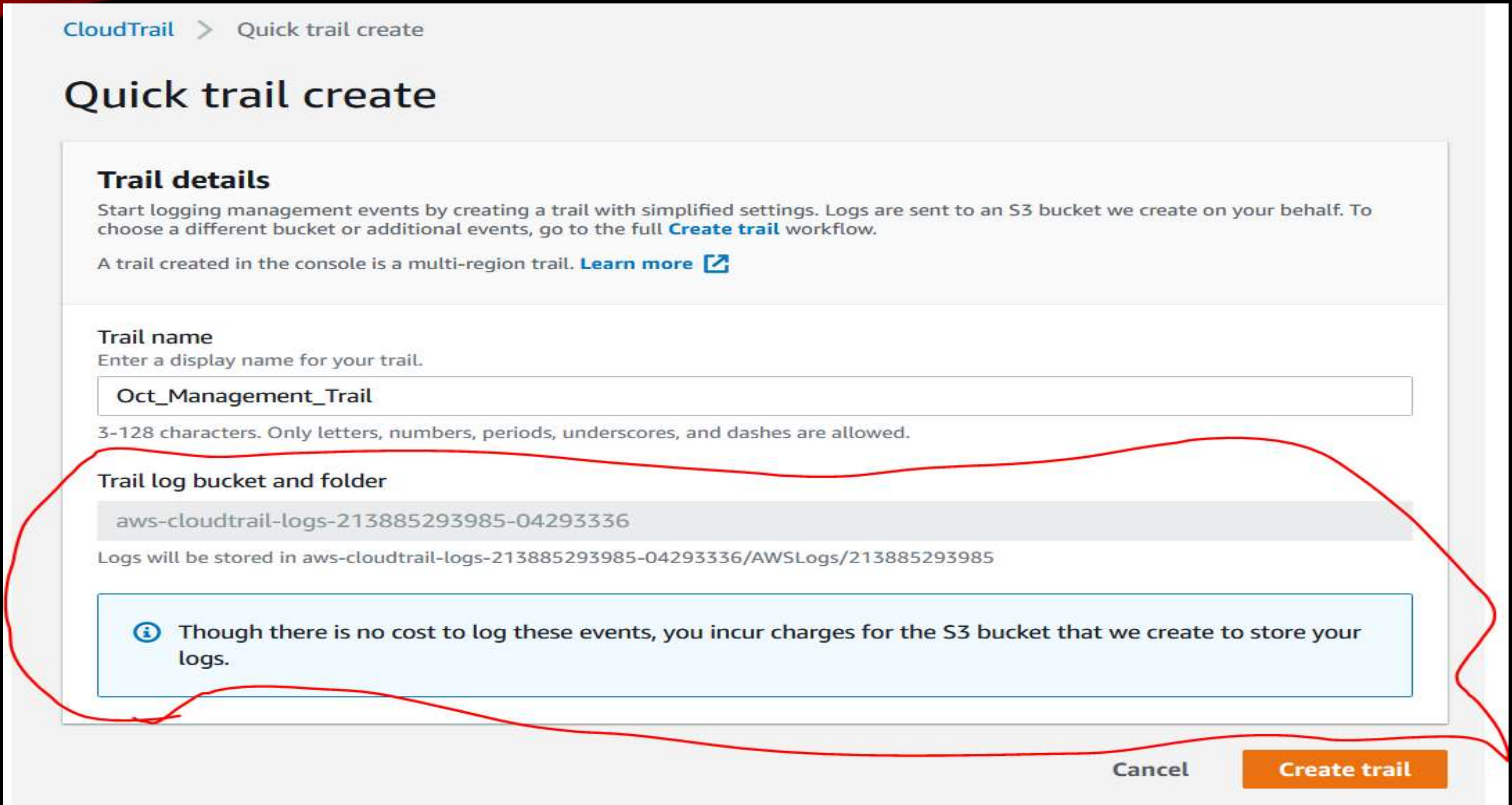
- `partition` identifies the partition that the resource is in. For standard AWS Regions, the partition is `aws`. If you have resources in other partitions, the partition is `aws-partitionname`. For example, the partition for resources in the China (Beijing) Region is `aws-cn`. You cannot delegate access between accounts in different partitions.
- `service` identifies the AWS product. For IAM resources, this is always `iam`.
- `region` is the Region the resource resides in. For IAM resources, this is always kept blank.
- `account` is the AWS account ID with no hyphens (for example, 123456789012).
- `resource` is the portion that identifies the specific resource by name.

You can specify IAM and AWS STS ARNs using the following syntax. The Region portion of the ARN is blank because IAM resources are global.

Syntax:

```
arn:aws:iam::account-id:root
arn:aws:iam::account-id:user/user-name-with-path
arn:aws:iam::account-id:group/group-name-with-path
arn:aws:iam::account-id:role/role-name-with-path
```

SETTING UP CLOUDTRAIL



CloudTrail > Quick trail create

Quick trail create

Trail details

Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full **Create trail** workflow.

A trail created in the console is a multi-region trail. **Learn more**

Trail name

Enter a display name for your trail.

Oct_Management_Trail

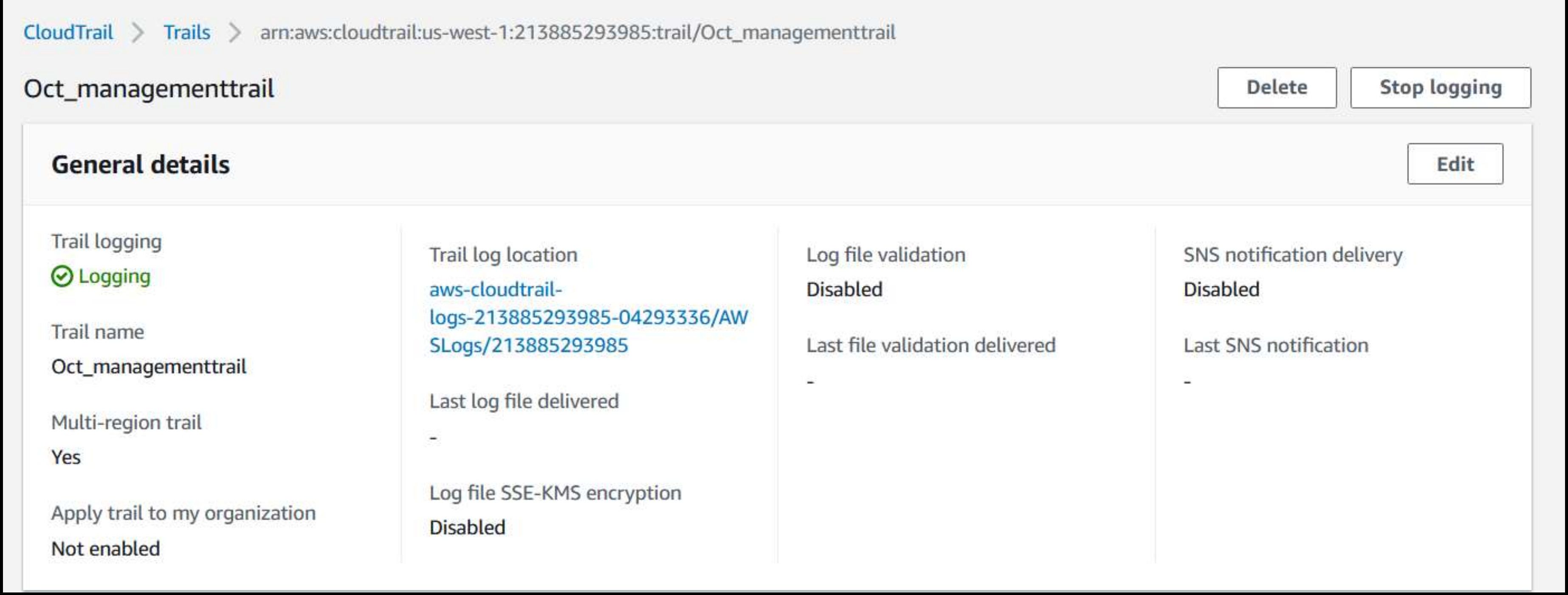
3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Trail log bucket and folder

aws-cloudtrail-logs-213885293985-04293336

Logs will be stored in aws-cloudtrail-logs-213885293985-04293336/AWSLogs/213885293985

ⓘ Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.



CloudTrail > Trails > arn:aws:cloudtrail:us-west-1:213885293985:trail/Oct_managementtrail
Delete
Stop logging
Edit

Oct_managementtrail

General details

Trail logging
✓ Logging

Trail name
Oct_managementtrail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
aws-cloudtrail-logs-213885293985-04293336/AWSLogs/213885293985

Last log file delivered
-

Log file SSE-KMS encryption
Disabled

Log file validation
Disabled

Last file validation delivered
-

SNS notification delivery
Disabled

Last SNS notification
-