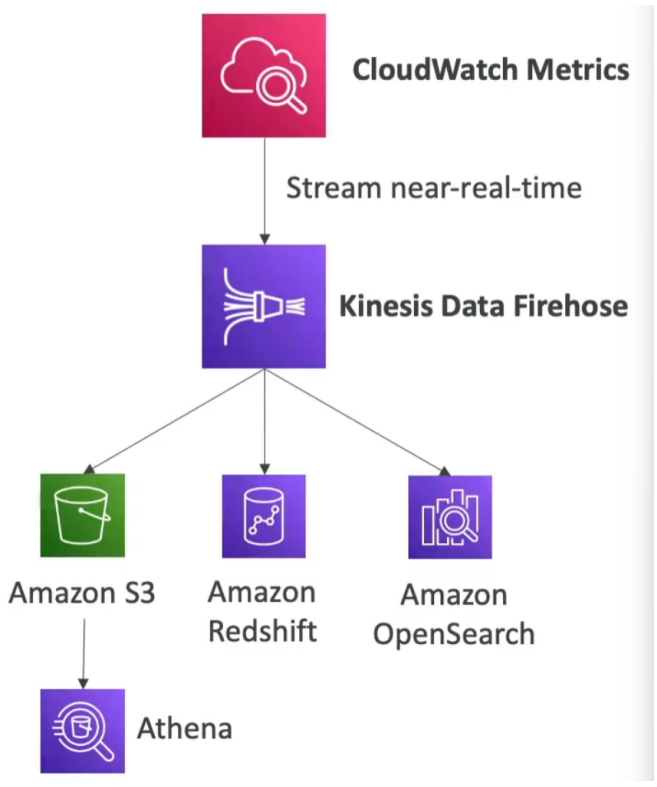
SAA-8

Amazon CloudWatch Metrics

- CloudWatch provides metrics for every services in AWS
- **Metric** is a variable to monitor (CPUUtilization,NetworkIn...)
- Metrics belong to **namespaces**
- **Dimension** is an attribute of a metric (instance id, environment,ect ...)
- Up to 10 dimensions per metric
- Metrics have **timestamps**
- Can create CloudWatch dashboards of metrics
- Can create **CloudWatch Custom Metrics** (for the RAM for example)

CloudWatch Metric Streams

- Continually stream CloudWatch metrics to a destination of your choice, with **near-real-time** delivery and low latency
  - Amazon Kinesis Data Firehose (and then its destinations)
  - 3rd party service provider: Datadog,Dynatrace, New Relic,Splunk, Sumo Logic ...
- Option to **filter metrics** to only stream a subset of them



CloudWatch Logs

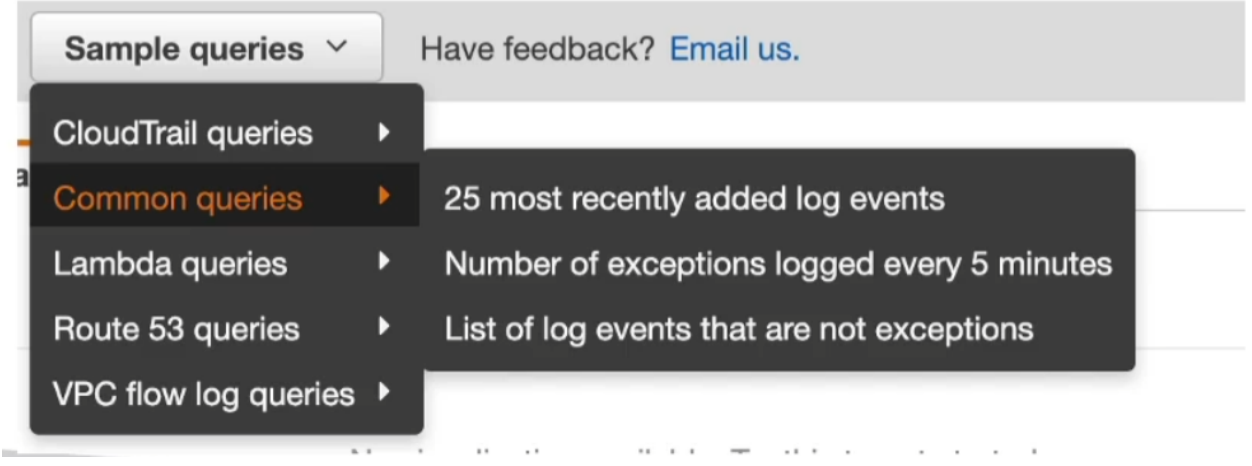
- **Log groups:** arbitrary name, usually representing an application
- **Log stream**: instances within application / log files / containers
- Can define log expiration policies (never expire, 30 days, etc ...)
- **CloudWatch Logs can send logs to:**
  - Amazon S3 (exports)
  - Kinesis Data Streams
  - Kinesis Data Firehose
  - AWS Lambda
  - ElasticSearch

CloudWatch Logs - Sources

- SDK, CloudWatch Logs Agent, CloudWatch Unified Agent
- Elastic Beanstalk: collection of logs from application
- ECS: collection from containers
- AWS Lambda: collection from function logs
- VPC Flow Logs: VPC specific logs
- API Gateway
- CloudTrail based on filter
- Route53: Log DNS queries

CloudWatch Logs Metric Filter & Insights

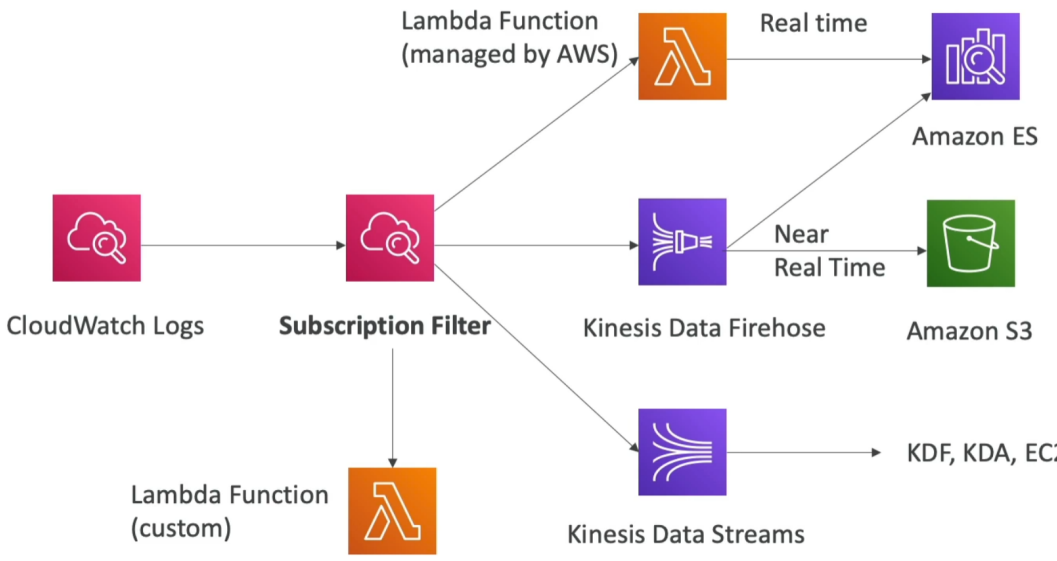
- CloudWatch Logs can use filter expressions
  - For example, find a specific IP inside of a log
  - Or count occurrences of "ERROR" in your logs
- Metric filters can be used to trigger CloudWatch alarms
- CloudWatch Logs Insights can be used to query logs and add queries to CloudWatch Dashboards



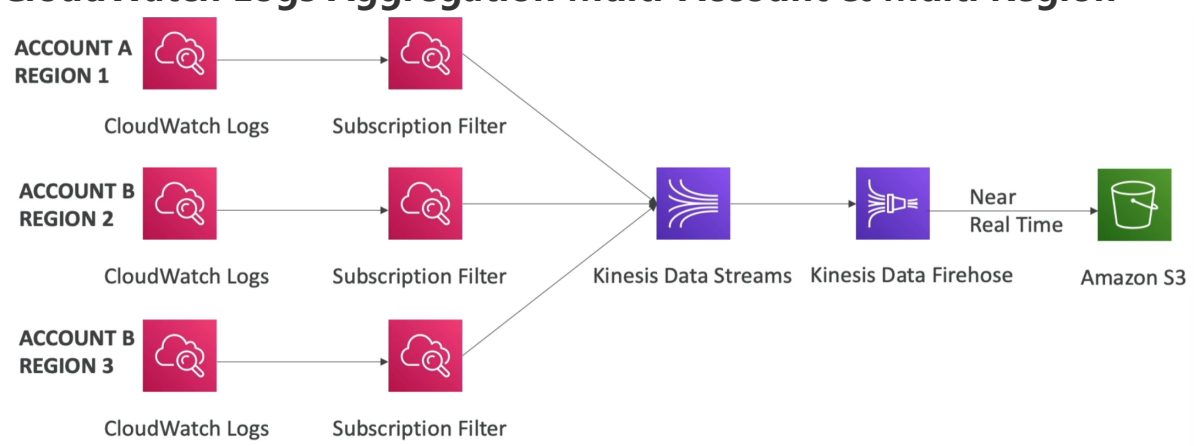
CloudWatch Logs - S3 Export

- Log data can take **up to 12 hours** to become available for export
- The API call is **CreateExportTask**
- Not near-real time or real-time... use Logs Subscriptions instead

CloudWatch Logs Subscriptions

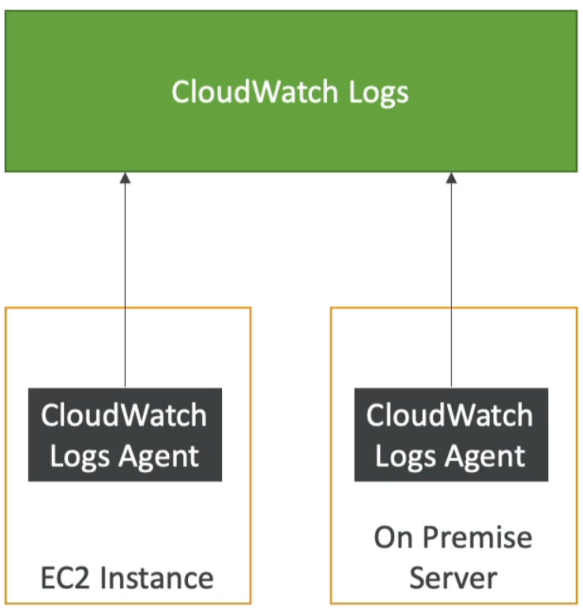


CloudWatch Logs Aggregation Multi-Account & Multi Region



CloudWatch Logs for EC2

- By default, no logs from your EC2 machine will go to CloudWatch
- You need to run a CloudWatch agent on EC2 to push the log files you want
- Make sure IAM permissions are correct
- The CloudWatch log agent can be setup on-premises too



CloudWatch Logs Agent & Unified Agent

- For virtual servers (EC2 instances,on-premise servers ...)
- **CloudWatch Logs Agent**
  - Old version of the agent
  - Can only send to CloudWatch Logs
- **CloudWatch Unified Agent**
  - Collect additional system-level metrics such as RAM, processes, etc ...
  - Clollect logs to send to CloudWatch Logs
  - Centralized configuration using SSM Parameter Store

CloudWatch Unified Agent - Metrics

- Collected directly on your Linux server / EC2 instance

- **CPU** (active, guest, idle, system, user, steal)
- **Disk metrics** (free,used,total), Disk IO (writes,reads,bytes,iops)
- **RAM** (free, inactive, used, total, cached)
- **Netstat** (number of TCP and UDP connections,net packets,bytes)
- **Processes** (total,dead, bloqued,idle,running, sleep)
- **Swap Space** (free, used, used %)

- Reminder: out-of-the box metrics for EC2 - disk, CPU, network (high level)

CloudWatch Alarms

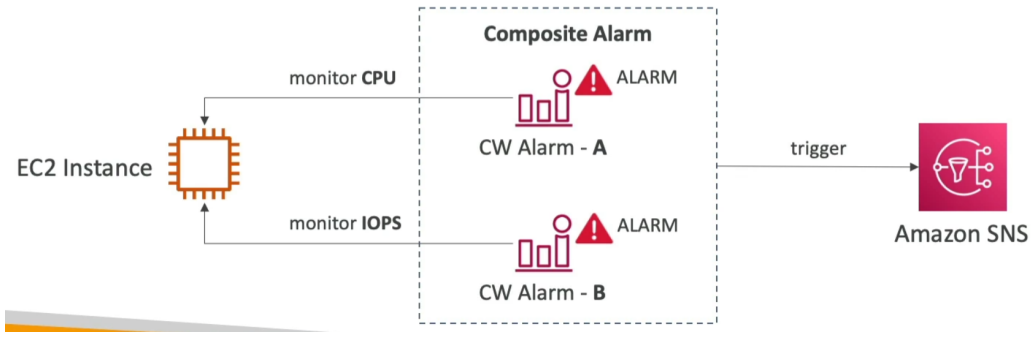
- Alarms are used to trigger notifications for any metric
- Various options (sampling, %,max,min,ect ...)
- Alarm States:
  - OK
  - INSUFFICIENT_DATA
  - ALARM
- Period
  - Length of time in seconds to evaluate the metric
  - High resolution custom metrics: 10 sec, 30 sec or multiples of 60 sec

CloudWatch Alarm Targets

- Stop, Terminate, Reboot, or Recover an EC2 Instance
- Trigger Auto Scaling Action
- Send notification to SNS (from which you can do pretty much anything)

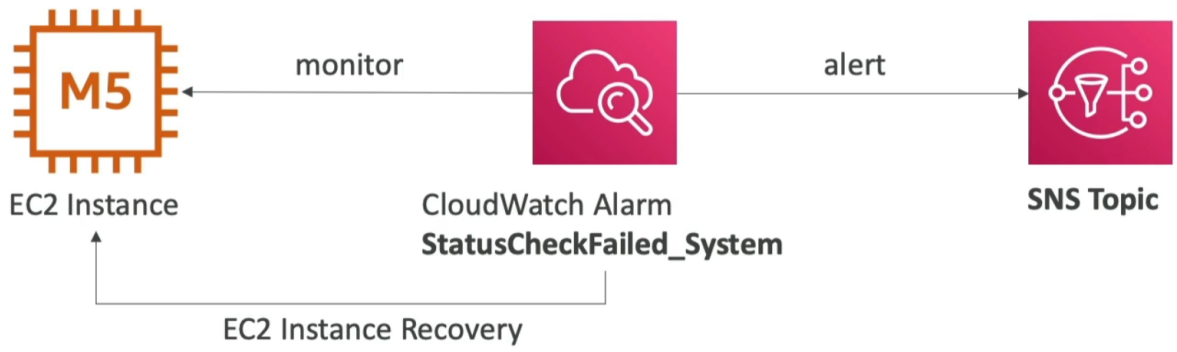
CloudWatch Alarms - Composite Alarms

- CloudWatch Alarms are on a single metric
- **Composite Alarms are monitoring the states of multiple other alarms**
- AND and OR conditions
- Helpful to reduce "alarm noise" by creating complex composite alarms



EC2 Instance Recovery

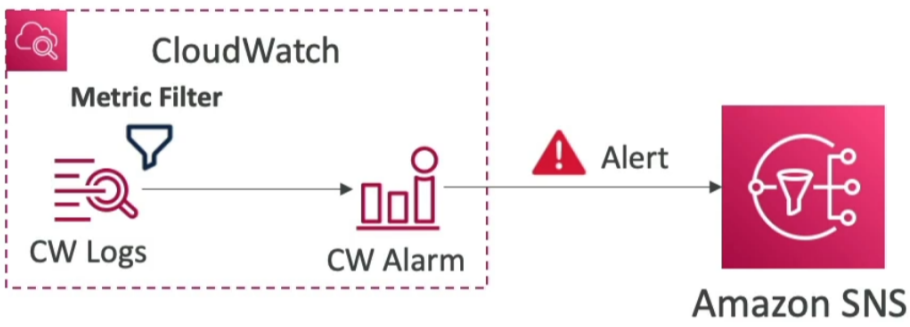
- Status Check:
  - Instance status = check the EC2 VM
  - System status = check the underlying hardware



- **Recovery**: Same Private,Public, Elastic IP, metadata,placement group

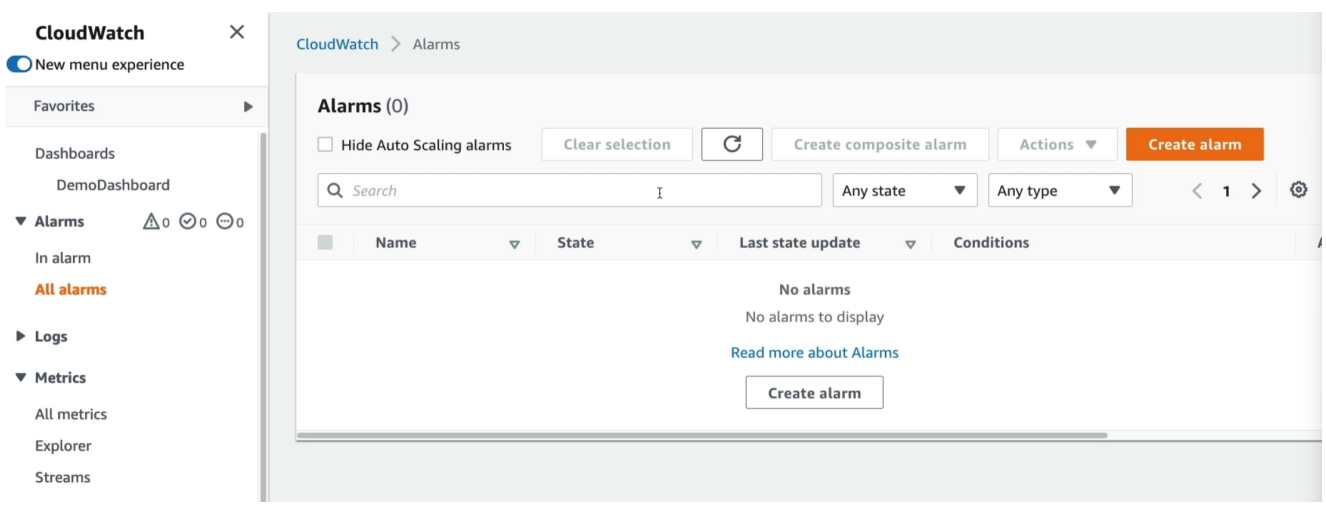
CloudWatch Alarm: good to know

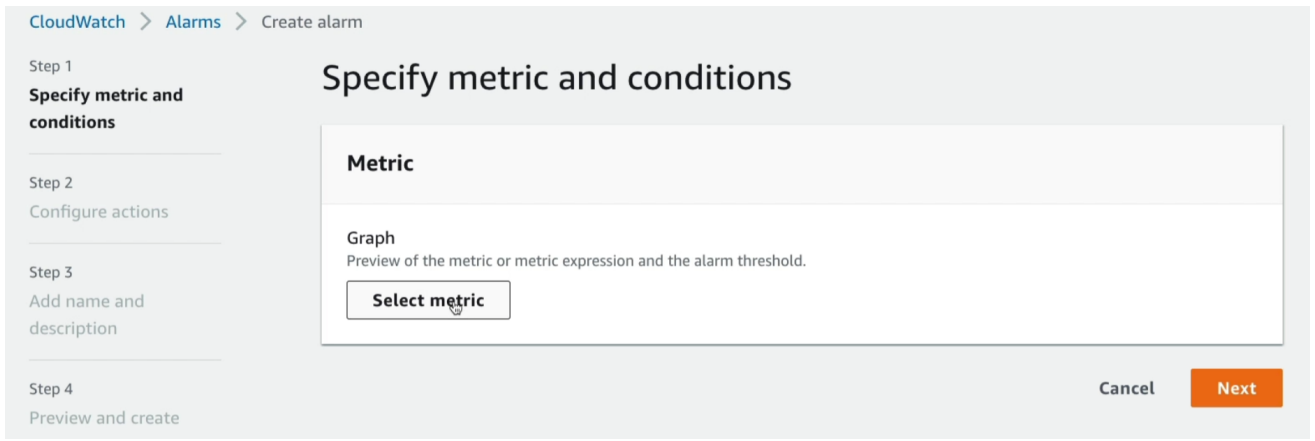
- Alarms can be created based on CloudWatch Logs Metrics Filters

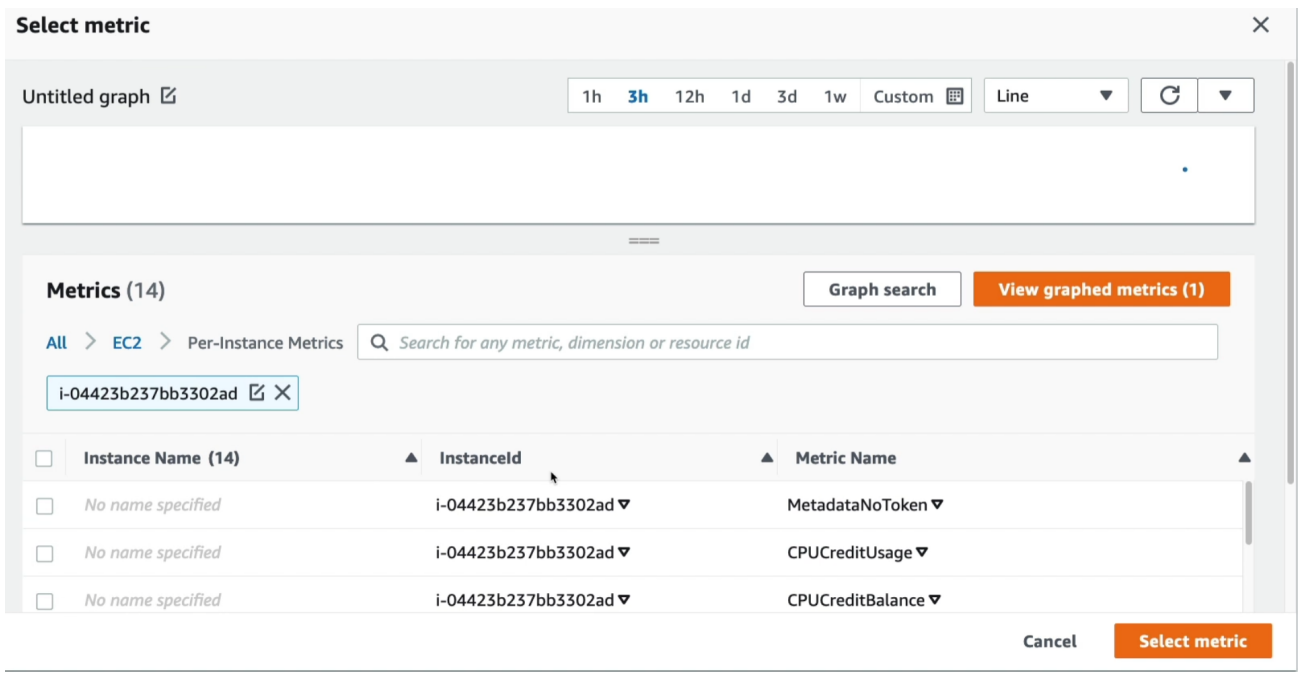


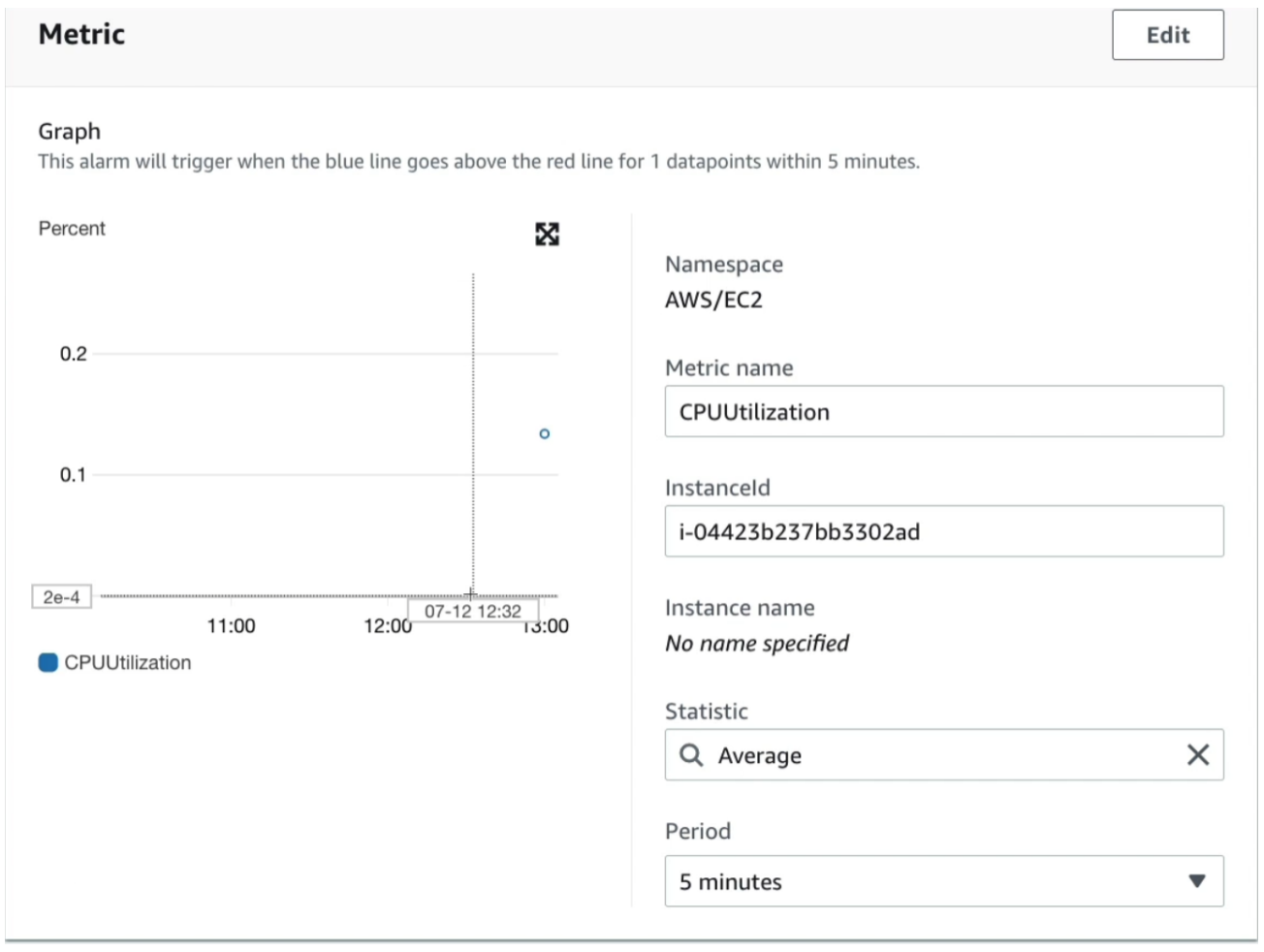
- To test alarms and notifications, set the alarm state to Alarm using CLI **aws cloudwatch set-alarm-state --alarm-name "myalarm" -- state-value ALARM --state-reason "testing purposes"**

Hands On




CloudWatch > Alarms > Create alarm
Step 1
Specify metric and conditions
Step 2
Configure actions
Step 3
Add name and description
Step 4
Preview and create
Specify metric and conditions
Metric
Graph
Preview of the metric or metric expression and the alarm threshold.
Select metric
Cancel
Next


Select metric
Untitled graph
1h 3h 12h 1d 3d 1w Custom
Line
Metrics (14)
Graph search
View graphed metrics (1)
All > EC2 > Per-Instance Metrics
Search for any metric, dimension or resource id
i-04423b237bb3302ad
Instance Name (14)
InstanceId
Metric Name
No name specified
i-04423b237bb3302ad
MetadataNoToken
No name specified
i-04423b237bb3302ad
CPUCreditUsage
No name specified
i-04423b237bb3302ad
CPUCreditBalance
Cancel
Select metric


Metric
Edit
Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.
Percent
0.2
0.1
2e-4
11:00
12:00
07-12 12:32
CPUUtilization
Namespace
AWS/EC2
Metric name
CPUUtilization
InstanceId
i-04423b237bb3302ad
Instance name
No name specified
Statistic
Average
Period
5 minutes

Conditions

Threshold type

- (•) **Static**
  Use a value as a threshold
- ( ) **Anomaly detection**
  Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

- (•) **Greater**
  > threshold
- ( ) **Greater/Equal**
  >= threshold
- ( ) **Lower/Equal**
  <= threshold
- ( ) **Lower**
  < threshold

than...
Define the threshold value.

95

Must be a number

▼ **Additional configuration**

Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.

3 out of 3

Missing data treatment
How to treat missing data when evaluating the alarm.

Treat missing data as missing

EC2 action

Alarm state trigger
Define the alarm state that will trigger this action.

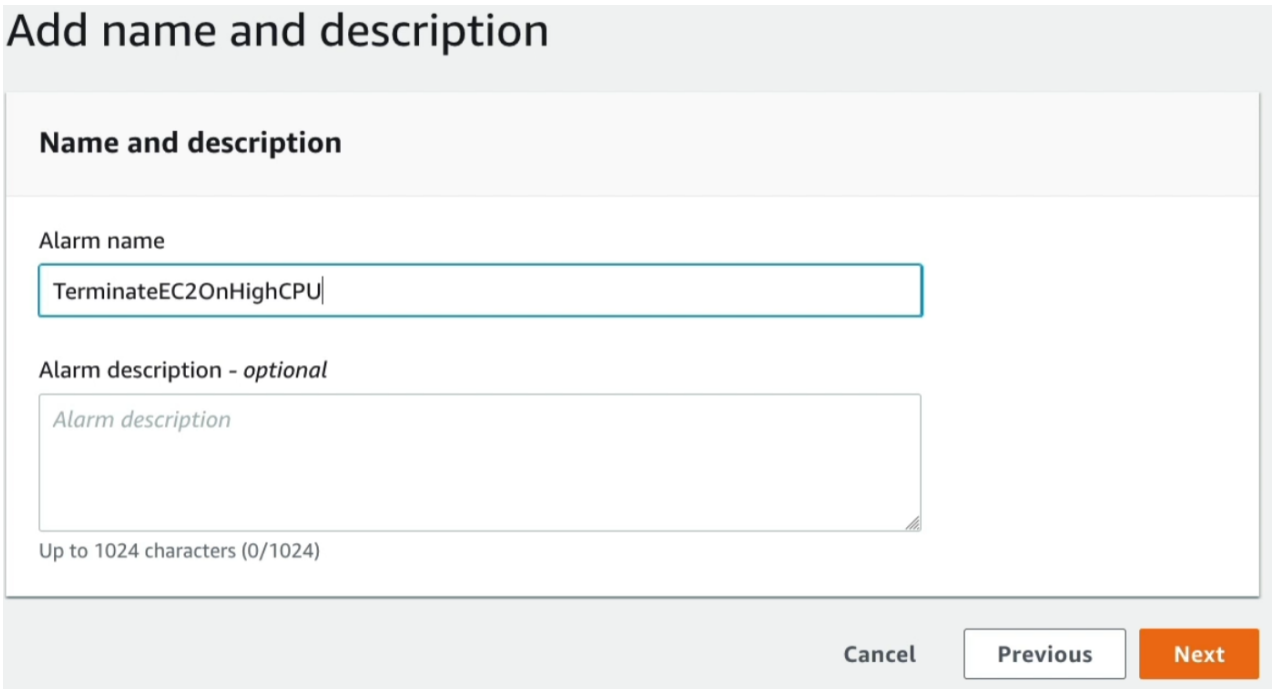
Remove

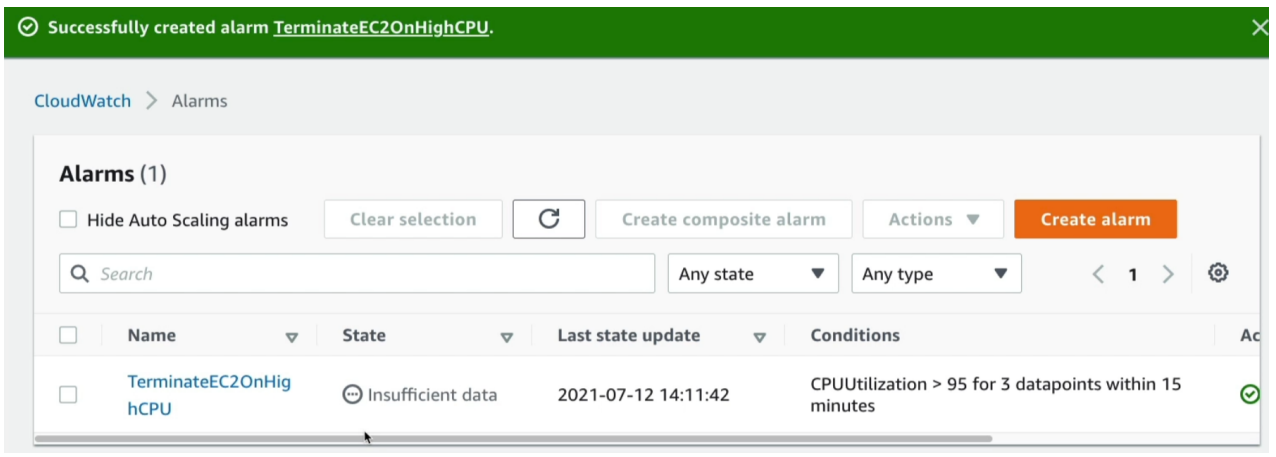
- (•) **In alarm**
  The metric or expression is outside of the defined threshold.
- ( ) **OK**
  The metric or expression is within the defined threshold.
- ( ) **Insufficient data**
  The alarm has just started or not enough data is available.

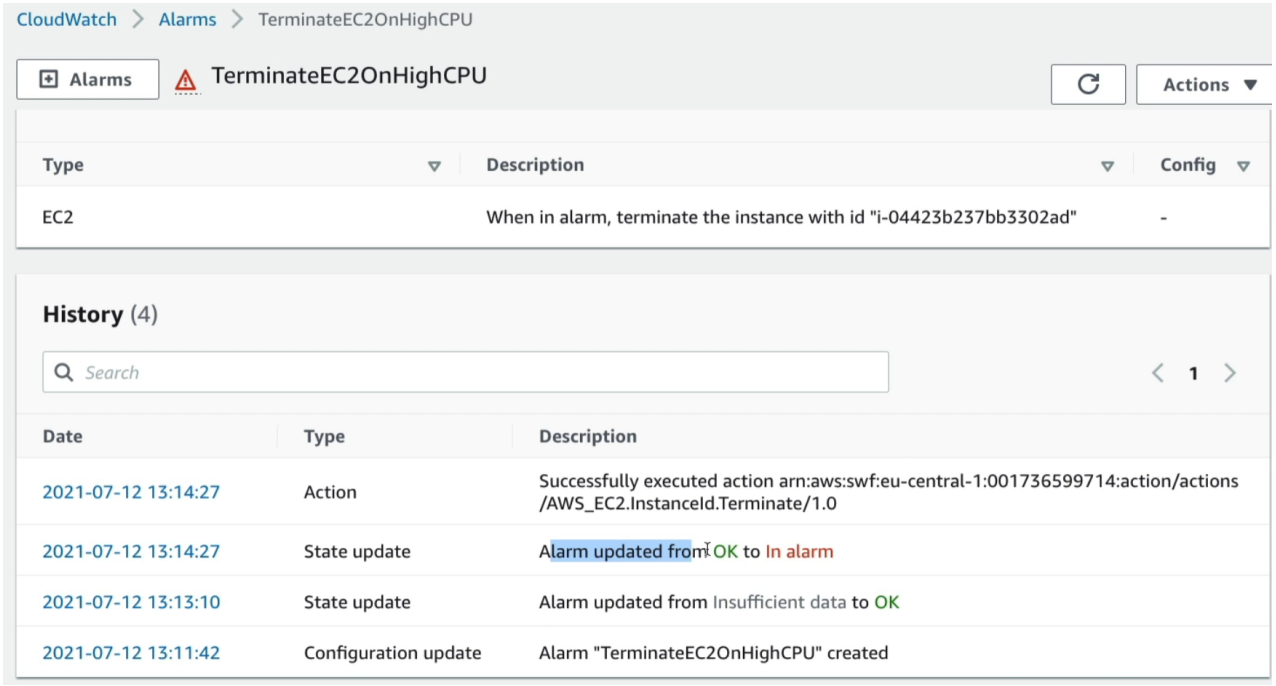
Take the following action...
Define what will happen to the EC2 instance with the Instance ID i-04423b237bb3302ad when this alarm is triggered.

- ( ) Recover this instance
  You can only recover certain EC2 instance types. See documentation
- ( ) **Stop this instance**
  You can only stop an instance if it is backed by an EBS volume. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document
- (•) **Terminate this instance**
  You will not be able to terminate this instance if termination protection is enabled. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document
- ( ) **Reboot this instance**
  An instance reboot is equivalent to an operating system reboot. AWS will use the existing Service Linked Role (AWSServiceRoleForCloudWatchEvents) to perform this action. Show IAM policy document

Add EC2 action

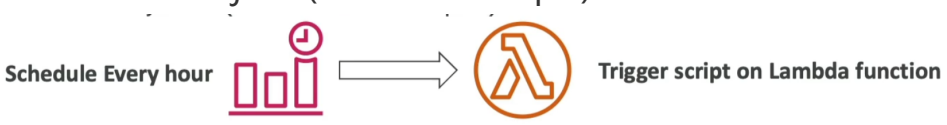




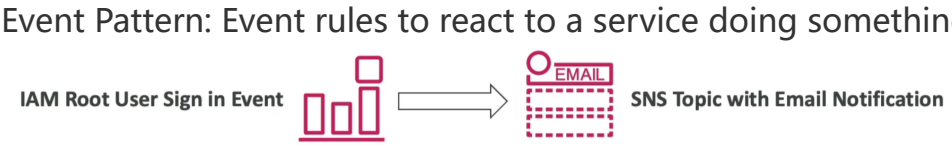


Amazon EventBridge (formerly CloudWatch Events)

- Schedule: Cron jobs (scheduled scripts)

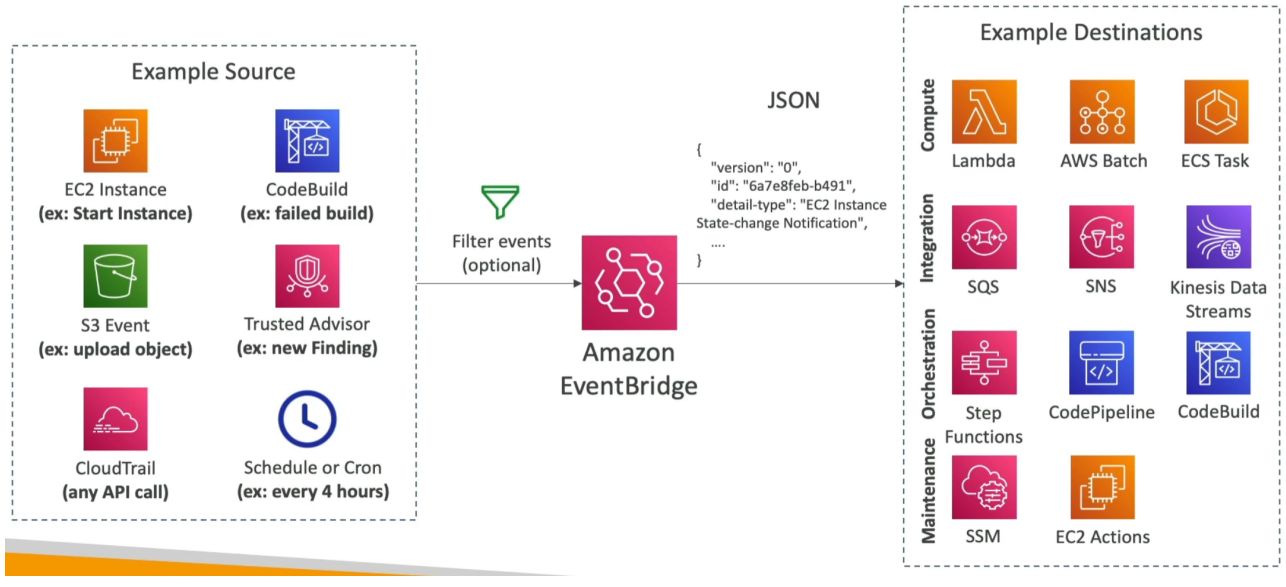


- Event Pattern: Event rules to react to a service doing something



- Trigger Lambda functions,send SQS/SNS messages...

Amazon EventBridge Rules

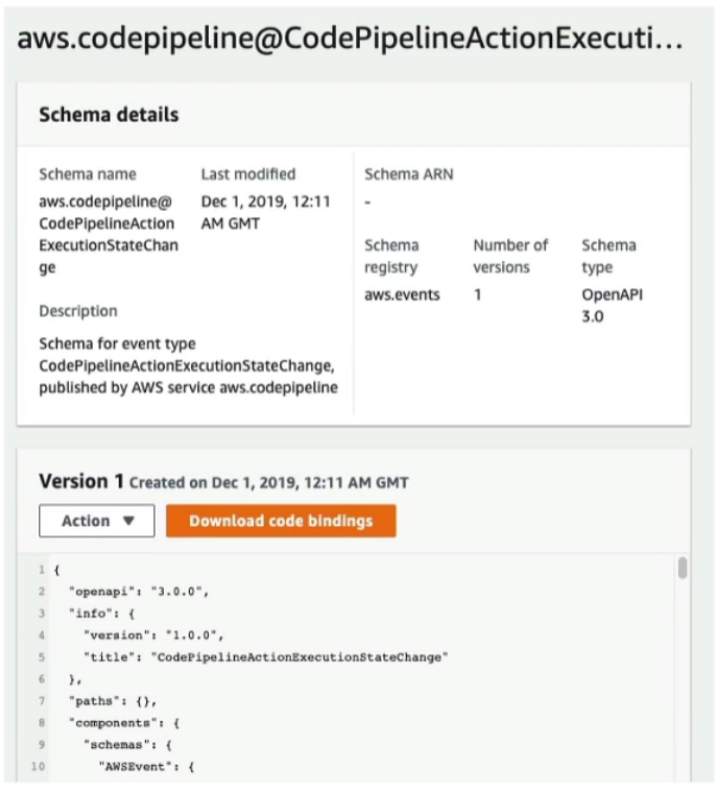


Amazon EventBridge

- Event buses can be accessed by other AWS accounts using Resource-based Policies
- You can **archive events** (all/filter) sent to an event bus (indefinitely or set period)
- Ability to **replay archived events**

Amazon EventBridge - Schema Registry

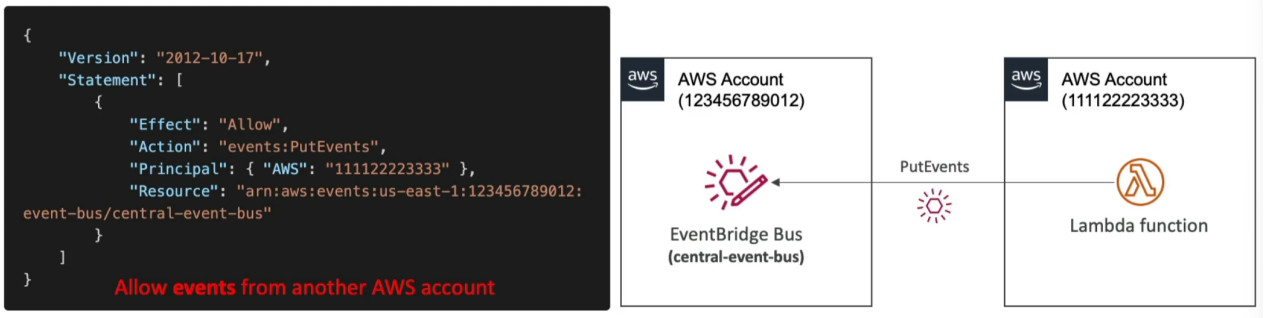
- EventBridge can analyze the events in your bus and infer the **schema**
- The **Schema Registry** allows you to generate code for your application, that will know in advance how data is structured in the event bus
- Schema can be versioned



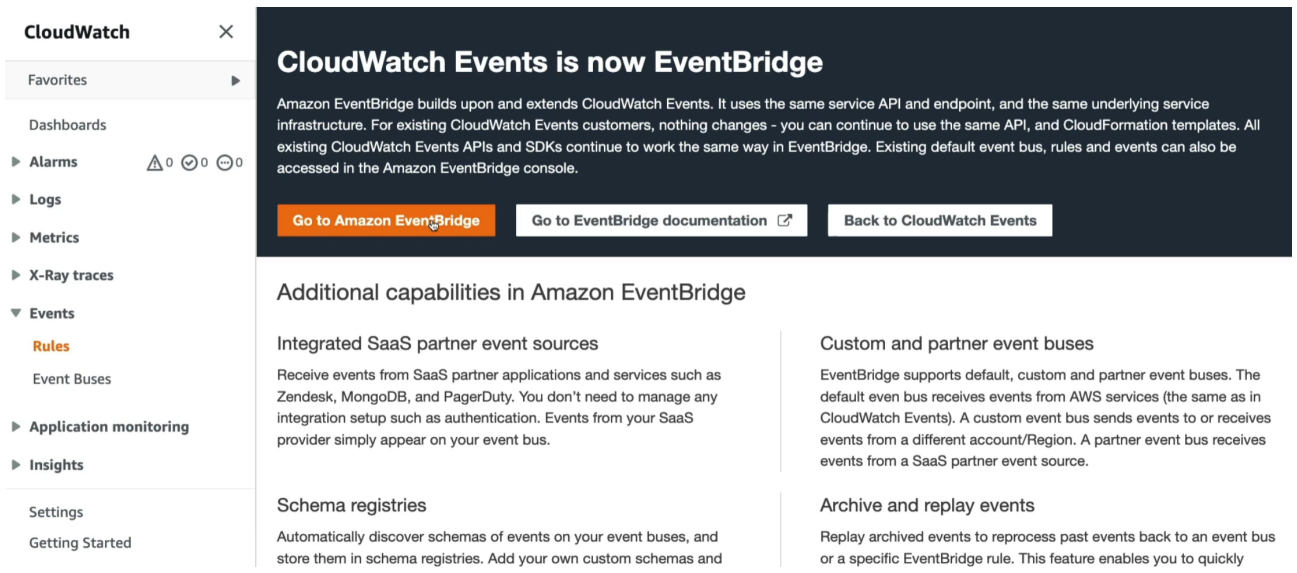
Amazon EventBridge - Resource-based Policy

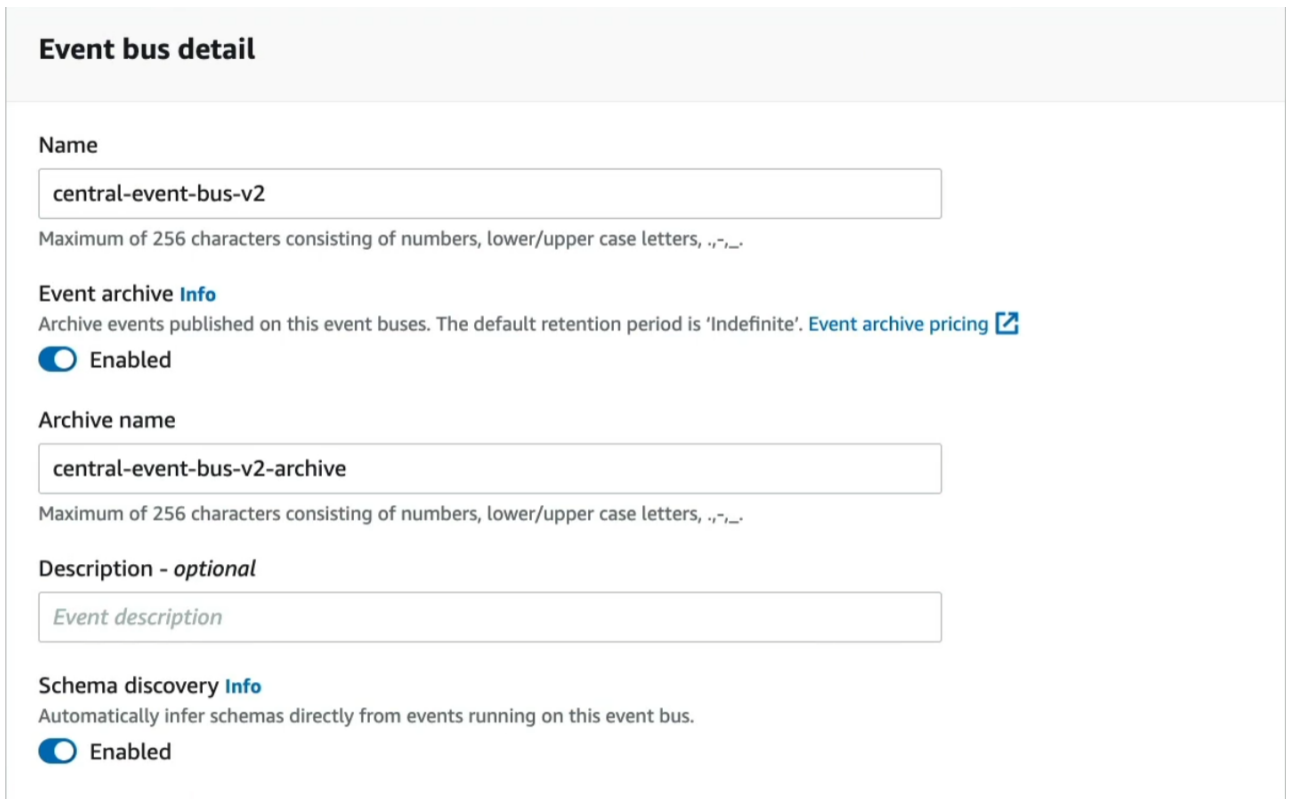
- Manage permissions for a specific Event Bus
- Example: allow/ deny events from another AWS account or AWS region

- Use case: aggregate all events from your AWS Organization in a single AWS account or AWS region

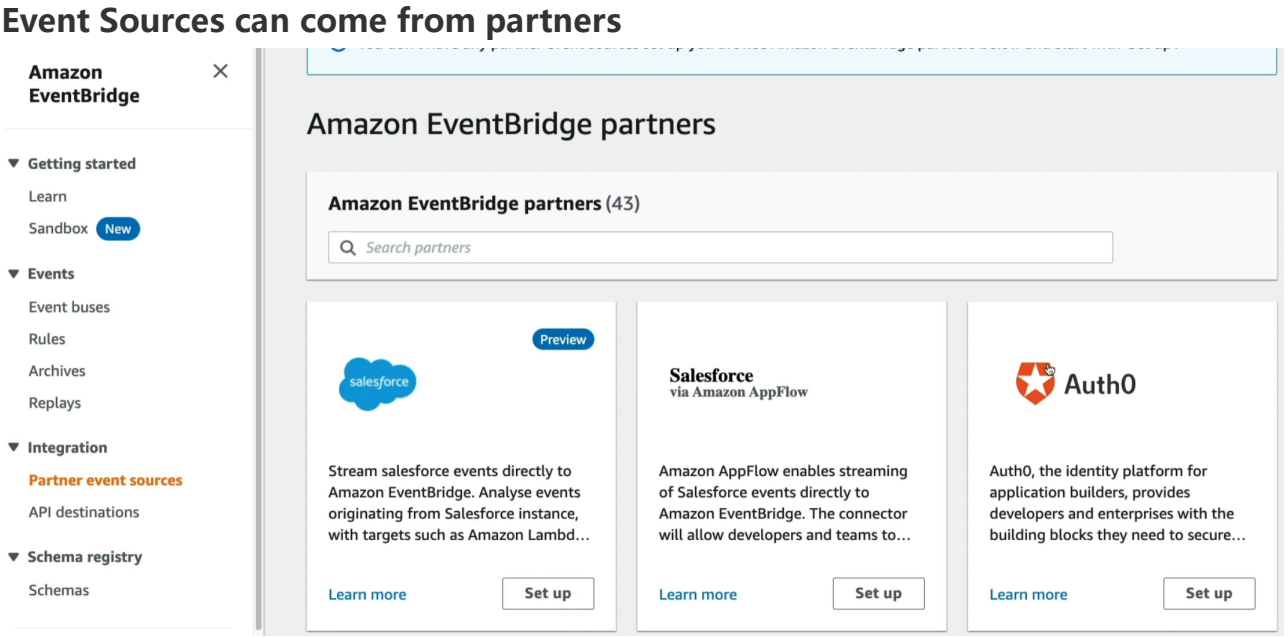


Hands on

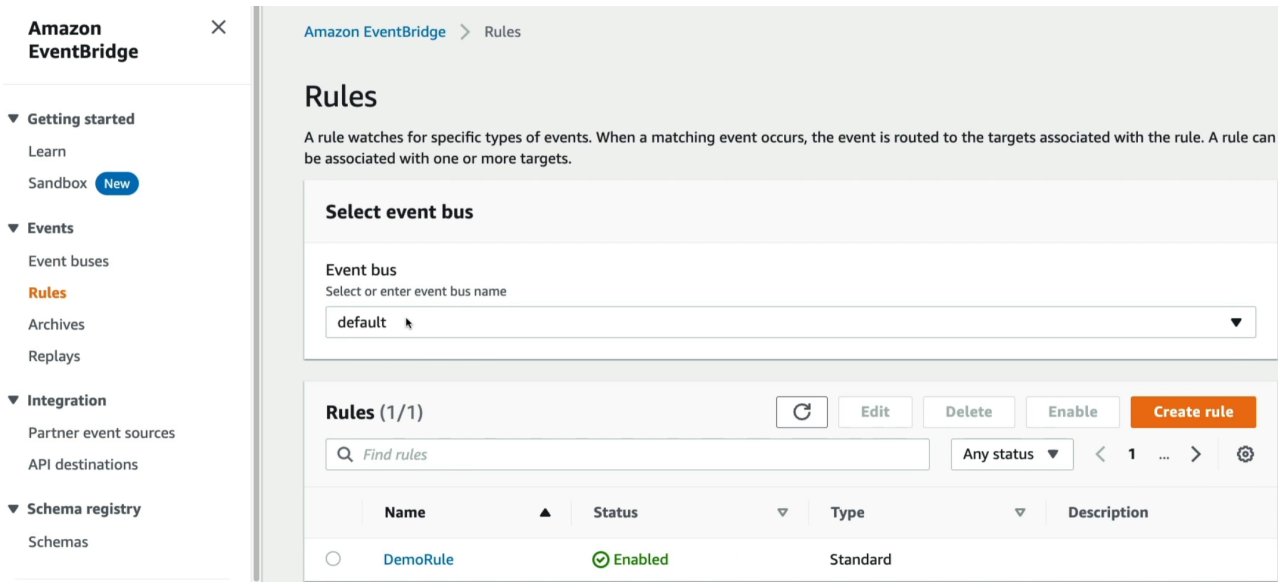


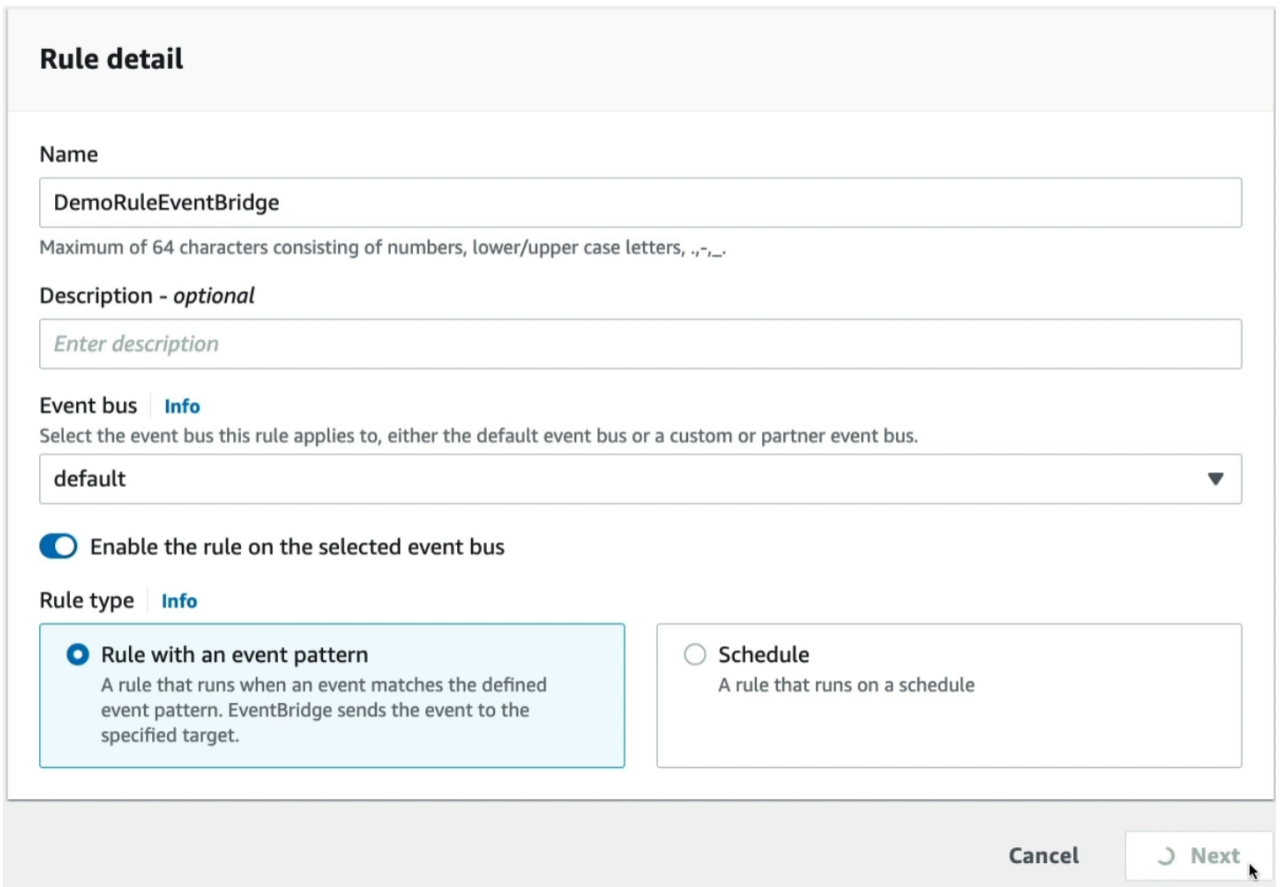


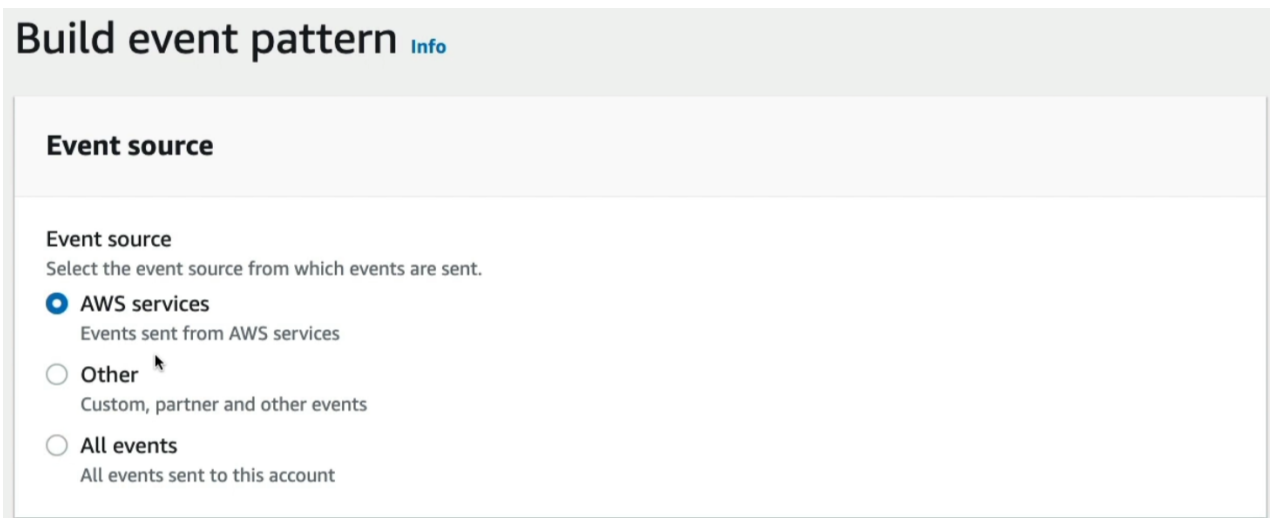
Event Sources can come from partners



Create Rules


Amazon EventBridge
Getting started
Learn
Sandbox New
Events
Event buses
Rules
Archives
Replays
Integration
Partner event sources
API destinations
Schema registry
Schemas
Amazon EventBridge > Rules
Rules
A rule watches for specific types of events. When a matching event occurs, the event is routed to the targets associated with the rule. A rule can be associated with one or more targets.
Select event bus
Event bus
Select or enter event bus name
default
Rules (1/1)
Edit
Delete
Enable
Create rule
Find rules
Any status
1
...
Name
Status
Type
Description
DemoRule
Enabled
Standard


Rule detail
Name
DemoRuleEventBridge
Maximum of 64 characters consisting of numbers, lower/upper case letters, .,-,_.
Description - optional
Enter description
Event bus Info
Select the event bus this rule applies to, either the default event bus or a custom or partner event bus.
default
Enable the rule on the selected event bus
Rule type Info
Rule with an event pattern
A rule that runs when an event matches the defined event pattern. EventBridge sends the event to the specified target.
Schedule
A rule that runs on a schedule
Cancel
Next


Build event pattern Info
Event source
Event source
Select the event source from which events are sent.
AWS services
Events sent from AWS services
Other
Custom, partner and other events
All events
All events sent to this account

Sample events

Filter by event source and type or by keyword.

EC2 Instance State-change Notification | Sample event 4

```
{
  "version": "0",
  "id": "651d5f8b-947c-4c0f-acb7-5ac4e41a1b8a",
  "detail-type": "EC2 Instance State-change Notification",
  "source": "aws.ec2",
  "account": "123456789012",
  "time": "2015-11-11T21:33:19Z",
  "region": "us-east-1",
  "resources": ["arn:aws:ec2:us-east-1:123456789012:instance/i-abcd3333"],
  "detail": {
    "instance-id": "i-abcd3333",
    "state": "stopped"
  }
}
```

JSON is valid

Copy | Prettify JSON

Event pattern Info — Event pattern form | Custom patterns (JSON editor)

Event source

The name of the AWS service as the event source.

EC2

Event type

The type of events as the source of the matching pattern

EC2 Instance State-change Notification

- Any state
- Specific state(s)

stopped ✕ terminated ✕

- Any instance
- Specific instance Id(s)

Event pattern

Event pattern, or filter to match the events

```
{
  "source": ["aws.ec2"],
  "detail-type": ["EC2 Instance State-change Notificati
  "detail": {
    "state": ["stopped", "terminated"]
  }
}
```

Copy | Test pattern | Edit pattern

Cancel | Previous | Next

Target 1

Target types

Select an EventBridge event bus, EventBridge API destination (SaaS partner), or another AWS service as a target.

- EventBridge event bus
- EventBridge API destination
- AWS service

Select a target Info

Select target(s) to invoke when an event matches your event pattern or when schedule is triggered (limit of 5 targets per rule)

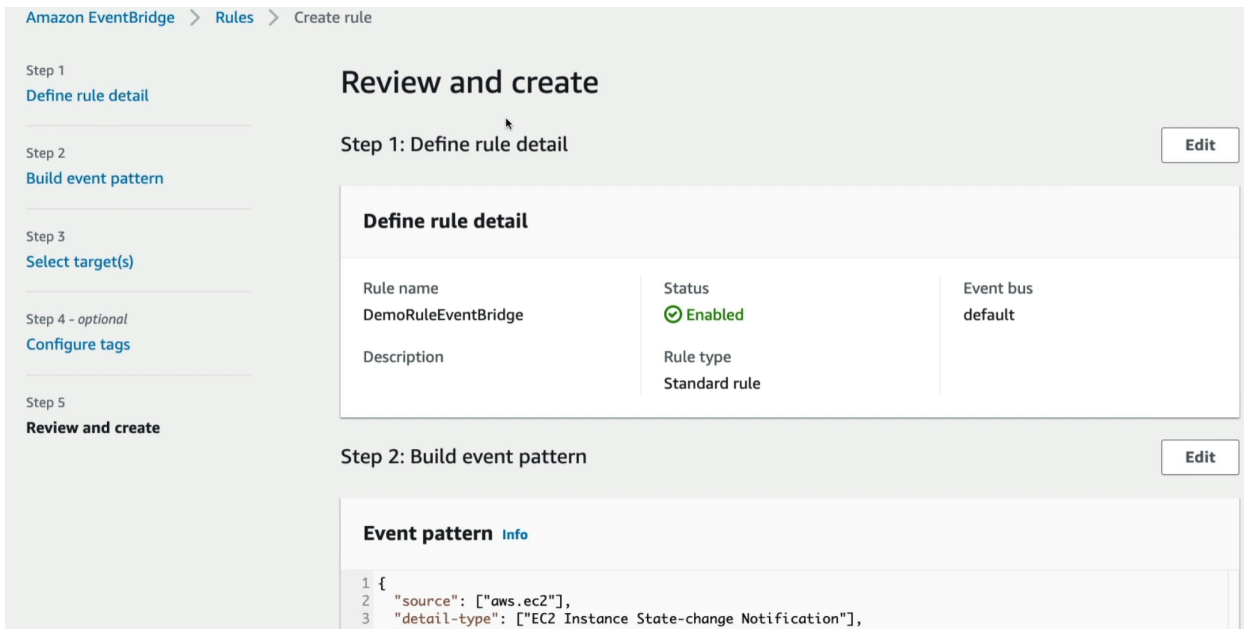
SNS topic

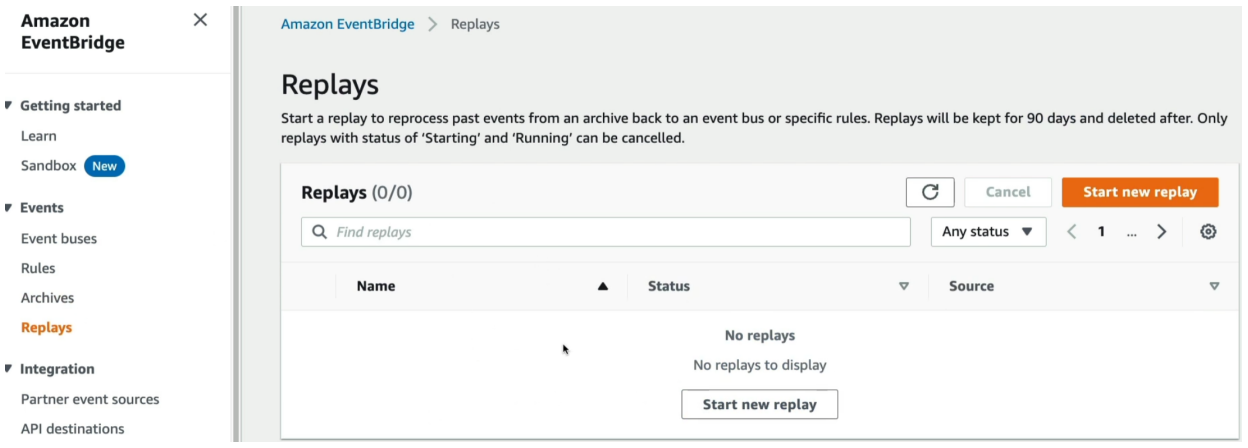
Topic

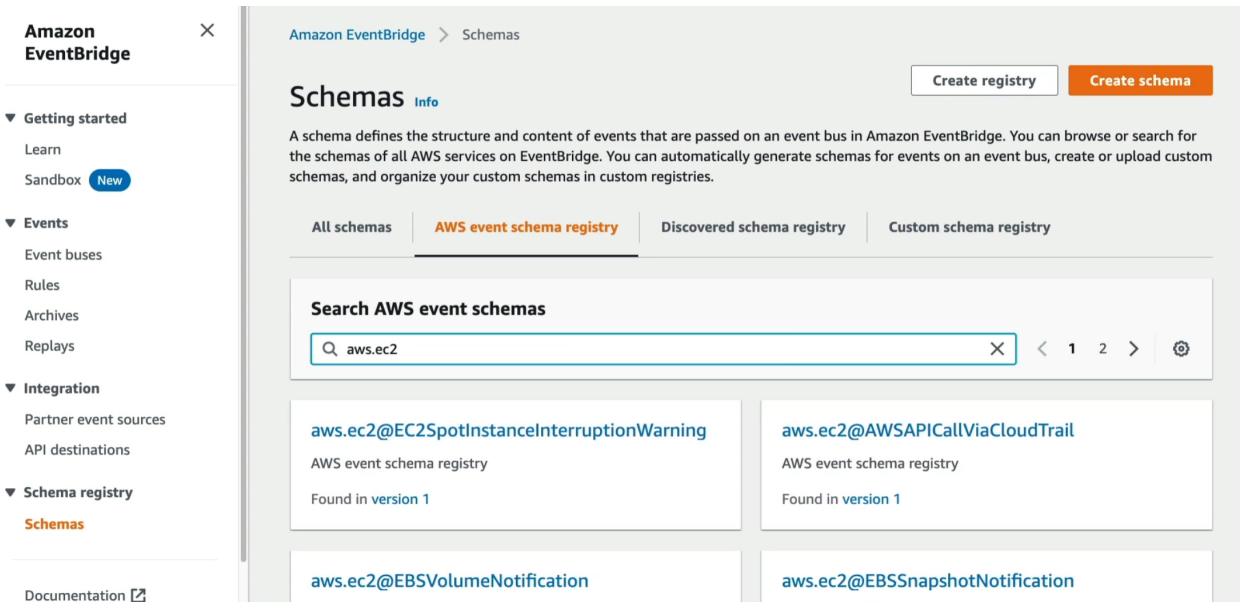
demo-topic

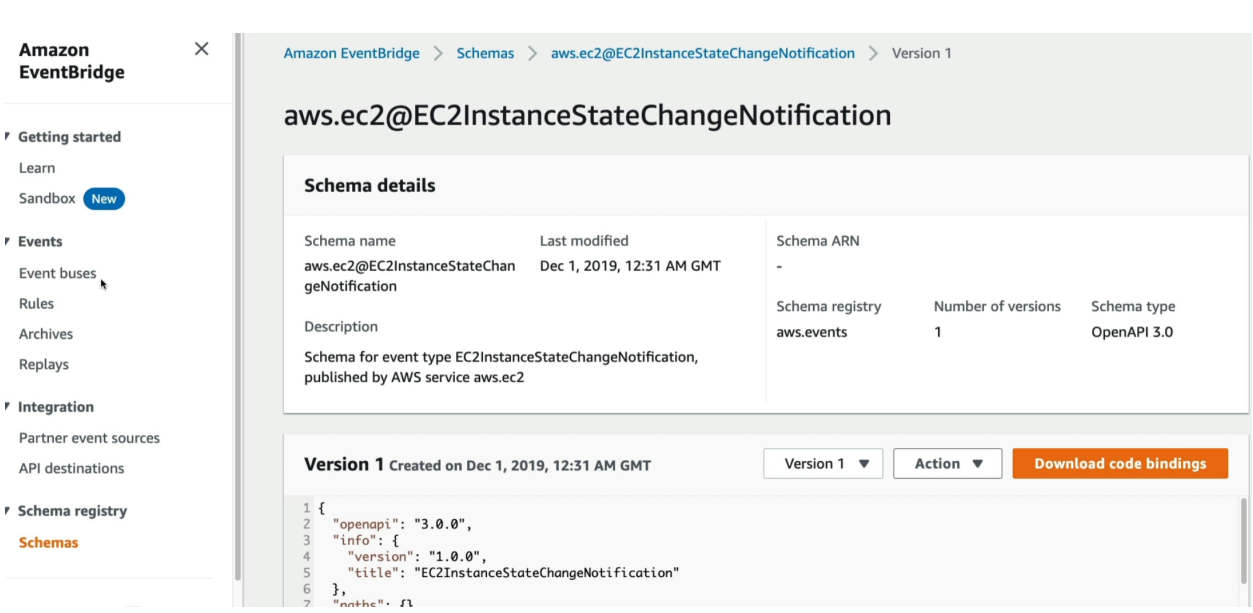
▶ Additional settings

Add another target | Cancel | Previous | Next





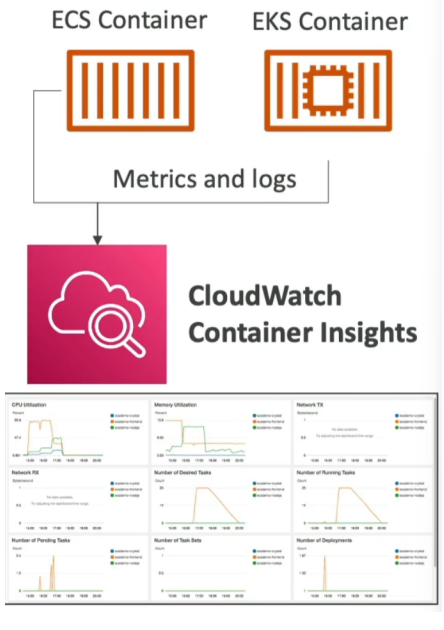




CloudWatch container Insights

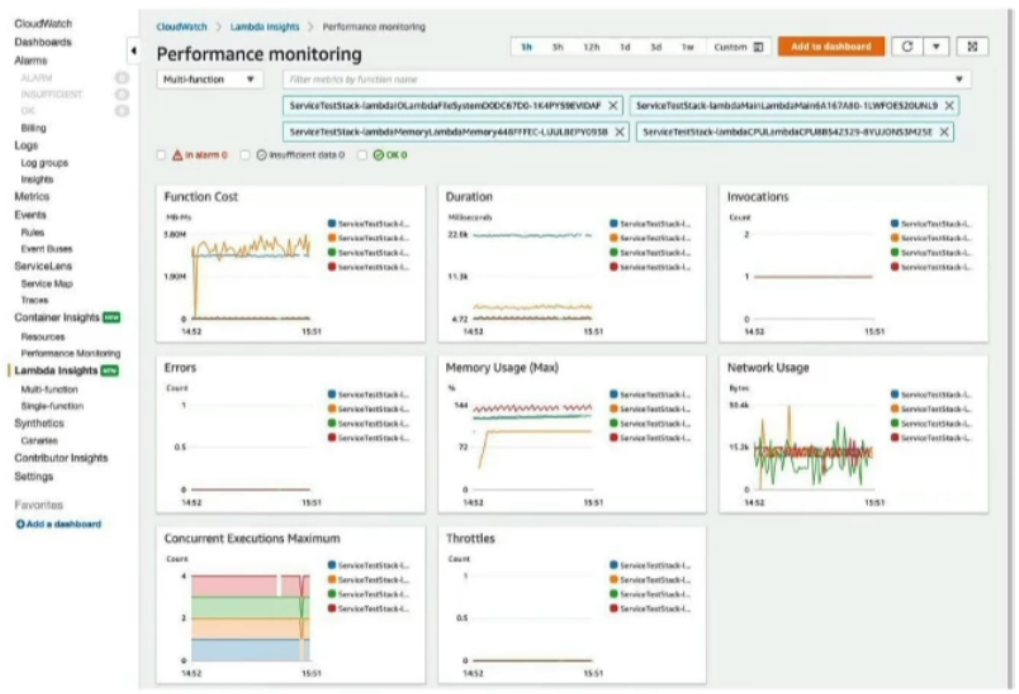
- Collect, aggregate, summarize **metrics and logs** from aontainers
- Available for containers on ...
  - Amazon Elastic Container Service (Amazon ECS)
  - Amazon Elastic Kubernetes Services (Amazon EKS)
  - Kubernetes paltforms on EC2

    - Fargate (both for ECS and EKS)
- **In Amazon EKS and Kubernetes, CloudWatch Insights is using a containerized version of the CloudWatch Agent to discover containers**



CloudWatch Lambda Insights

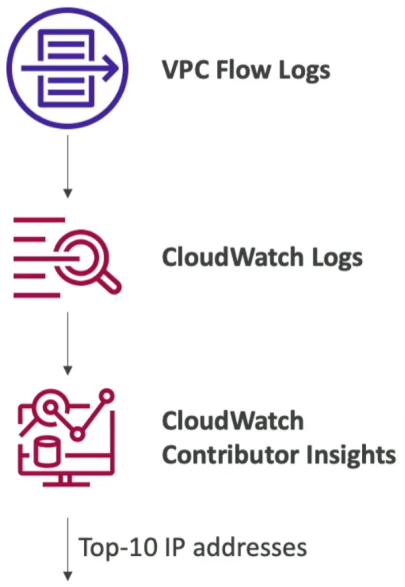
- Monitoring and troubleshooting solution for serverless applications running on AWS Lambda
- Collects, aggregates, and summarizes system-level metrics including CPU time, memory, disk,and network
- Collects, aggregates, and summarizes diagnostic information such as cold starts and Lambda worker shutdowns
- Lambda Insights is provided as a Lambda Layer



CloudWatch Contributor Insights

- Analyze log data and create time series that display contributor data
    - **See metrics about the top-N contributors**
    - The total number of unique contributors, and their usage.
- This helps you find top talkers and understand who or what is impacting system performance.
- Works for any AWS-generated logs (VPC, DNS,etx...)
- For example, you can find bad hosts, **identify the heaviest network users**, or find the URLs that generate the most errors
- You can build your rules from scrach, or you can also use sample rules that AWS has created - **leverages your CloudWatch Logs**

- CloudWatch also provides built-in rules that you can use to analyze metrics from other AWS services.



CloudWatch Application Insights

- **Provides automated dashboards that show potential problems with monitored applications, to help isolate ongoing issues**
- Your applications run on Amazon EC2 Instances with select technologies only (Java, .NET, Microsoft IIS Web Server, databases...)
- And you can use other AWS resources such as Amazon EBS, RDS, ELB, ASG,Lambda,SQS, DynamoDB, S3 bucket, ECS, EKS, SNS, API Gateway...

- Powered by SageMaker
- Enhanced visibility into your application health to reduce the time it will take you to troubleshoot and repair your applications
- Findings and alerts are sent to Amazon EventBridge and SSM OpsCenter

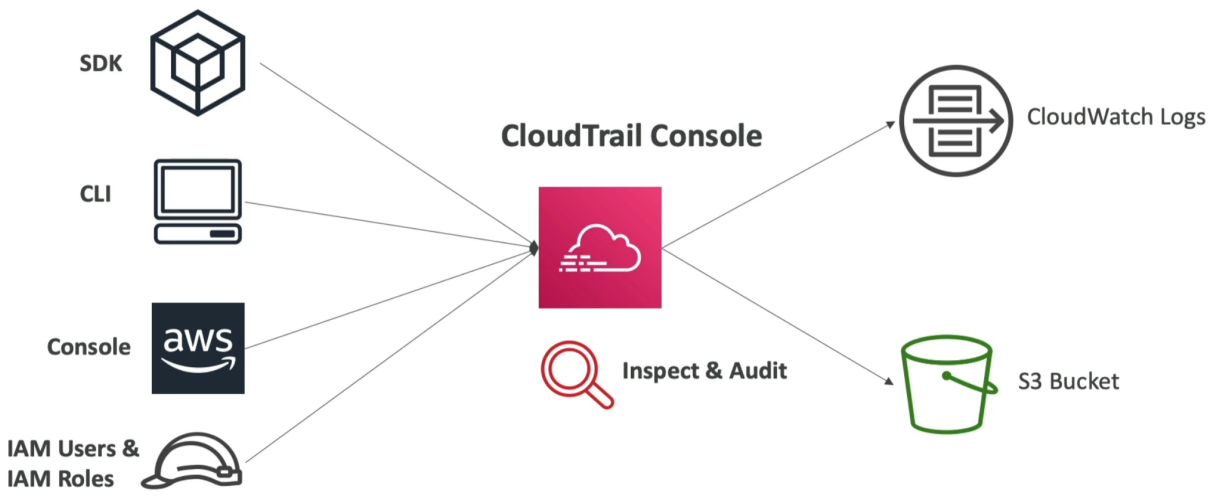
CloudWatch insights and Operational Visibility

- **CloudWatch Container Insights**
  - ECS, EKS, Kubernetes on EC2, Fargate, needs agent for Kubernetes
  - Metrics and logs
- **CloudWatch Lambda Insights**
  - Detailed metrics to troubleshoot serverless applications
- **CloudWatch Contributors Insights**
  - Find "Top-N" Contributors through CloudWatch Logs
- **CloudWatch Application Insights**
  - Automatic dashboard to troubleshoot your application and related AWS services

AWS CloudTrail

- **Provides governance, compliance and audit for your AWS Account**
- CloudTrail is enabled by default !
- Get **an history of events / API calls made within your AWS Account** by:
  - Console
  - SDK
  - CLI
  - AWS Services
- Can put logs from CloudTrail into CloudWatch Logs or S3
- **A trail can be applied to All Regions (default) or a single Region.**
- If a resource is deleted in AWS, investigate CloudTrail first !

CloudTrail Diagram

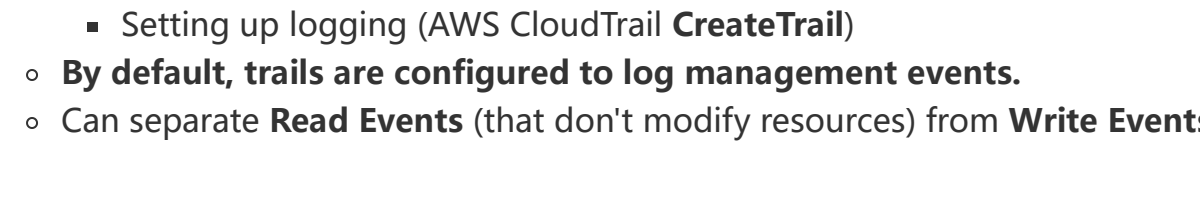


CloudTrail Events

- **Management Events:**
  - Operations that are performed on resources in your AWS account
  - Examples:
    - Configuring security (IAM **AttachRolePolicy**)
    - Configuring rules for routing data (Amazon EC2 **CreateSubnet**)
    - Setting up logging (AWS CloudTrail **CreateTrail**)
  - **By default, trails are configured to log management events.**
  - Can separate **Read Events** (that don't modify resources) from **Write Events** (that may modify resources)

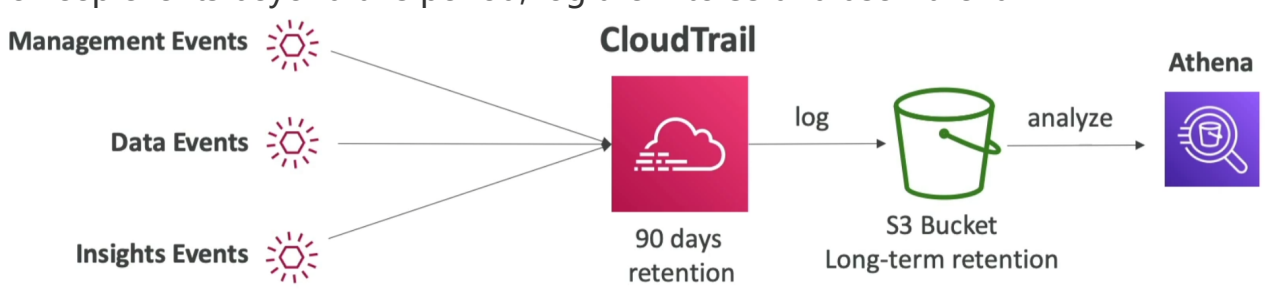
- **Data Events:**
  - B**y default, data events are not logged (because high volume operations)**
  - Amazon S3 object-level activity (ex: **GetObject, DeleteObject, PutObject**): can separate Read and Write Events
  - AWS Lambda function execution activity (the **Invoke** API)

CloudTrail Insights

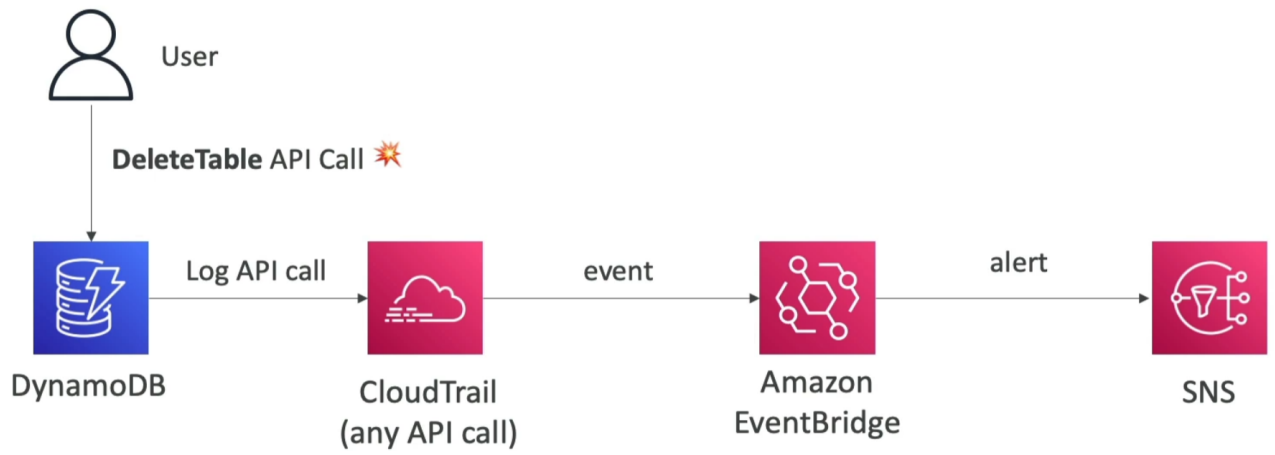
- Enable **CloudTrail Insights to detect unusual activity** in your account:
  - inaccurate resource provisioning
  - hitting service limits
  - Bursts of AWS IAM actions
  - Gaps in periodic maintenance activity
- CloudTrail Insights analyzes normal management events to create a baseline
- And then **continuously analyzes write events to detect unusual patterns**
  - Anomalies appear in the CloudTrail console
  - Event is sent to Amazon S3
  - An EventBridge event is generated(for automation needs)
- 

CloudTrail Events Retention

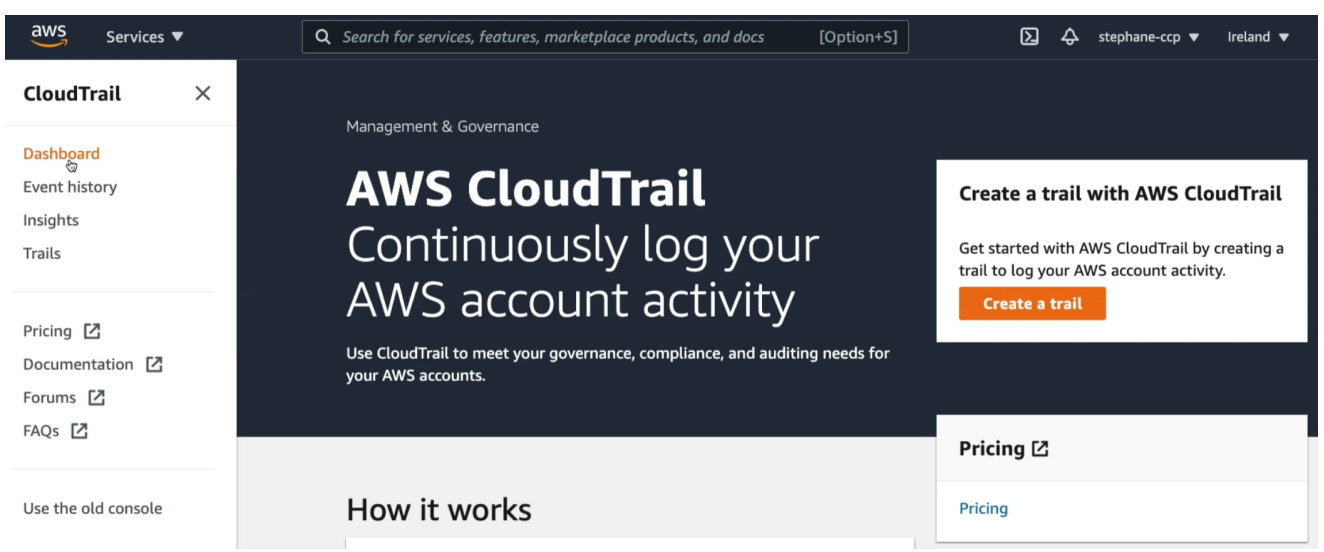
- Events are stored for 90 days in CloudTrail
- To keep events beyond this period, log them to S3 and use Athena

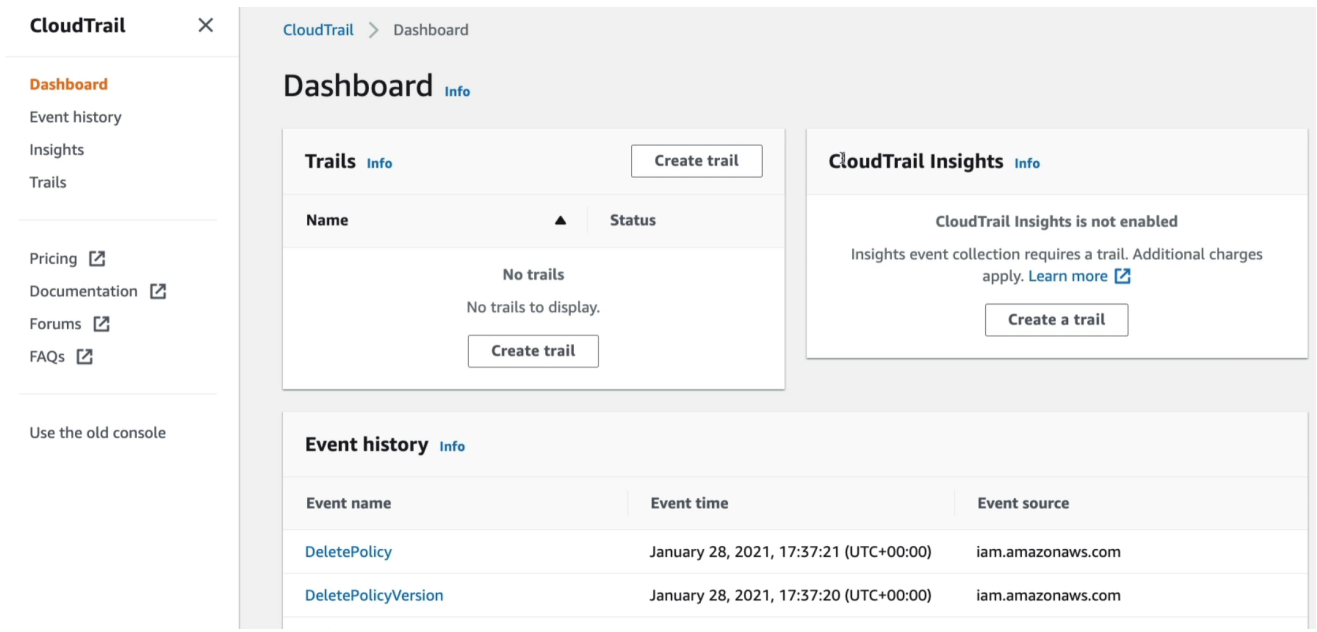


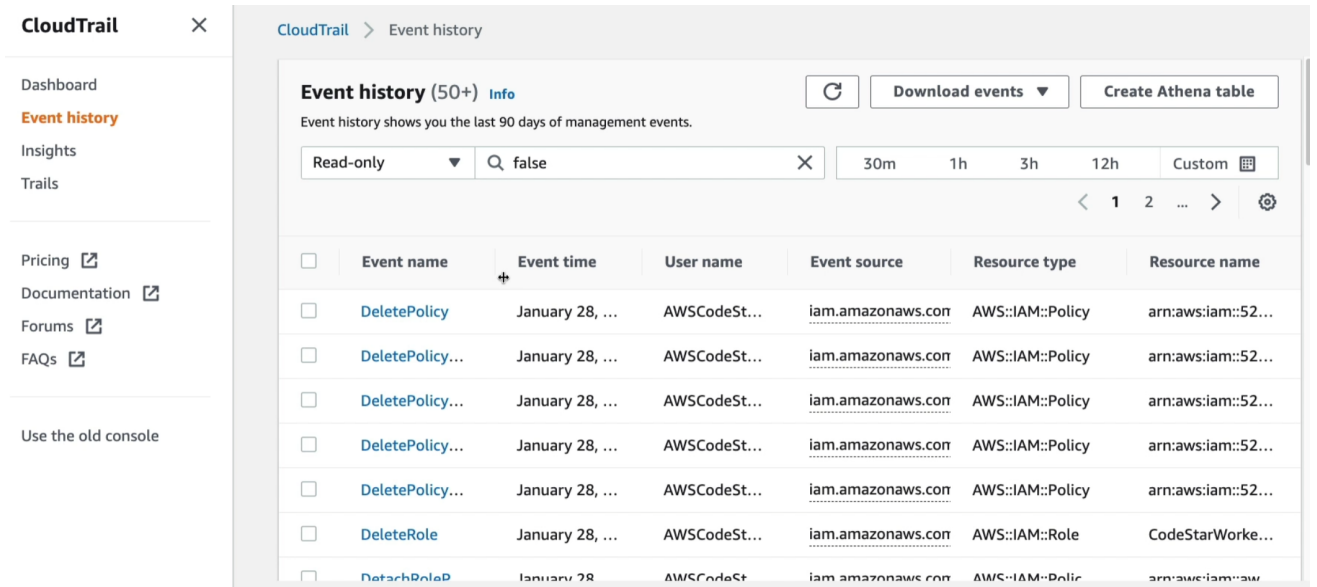
Amazon EventBridge - Intercept API Calls

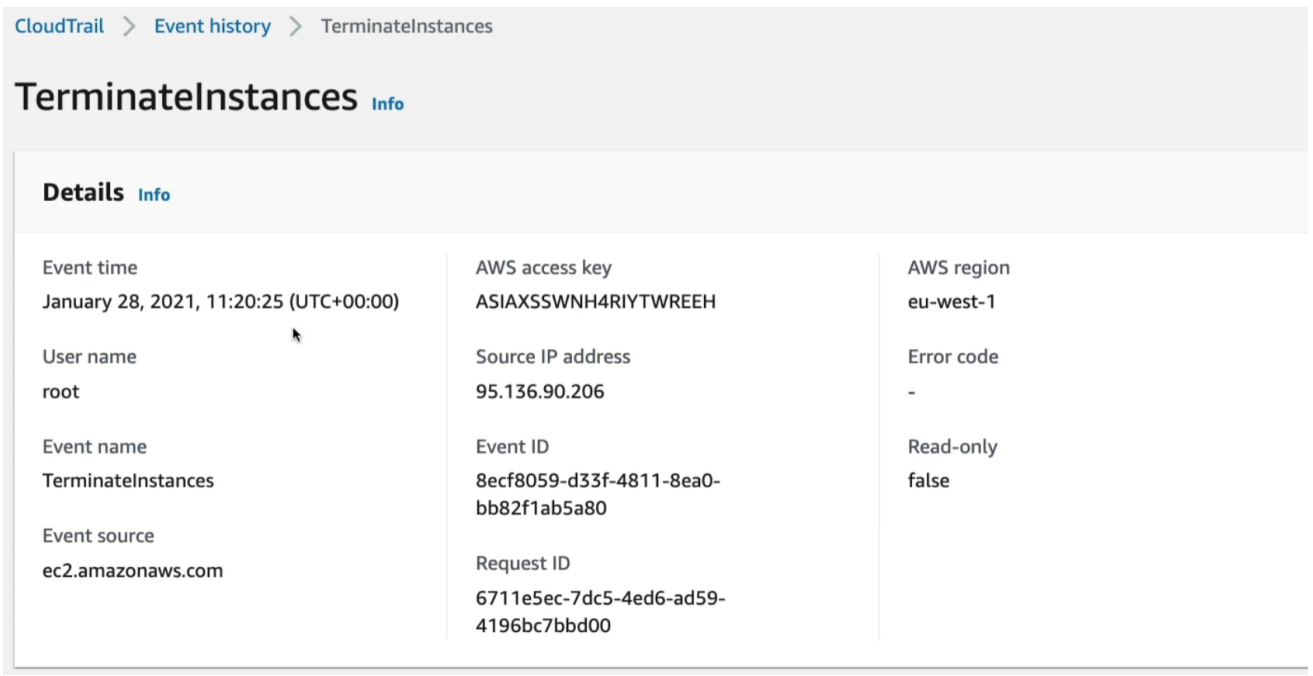

User
DeleteTable API Call
Log API call
event
alert
DynamoDB
CloudTrail
(any API call)
Amazon
EventBridge
SNS

Hands on

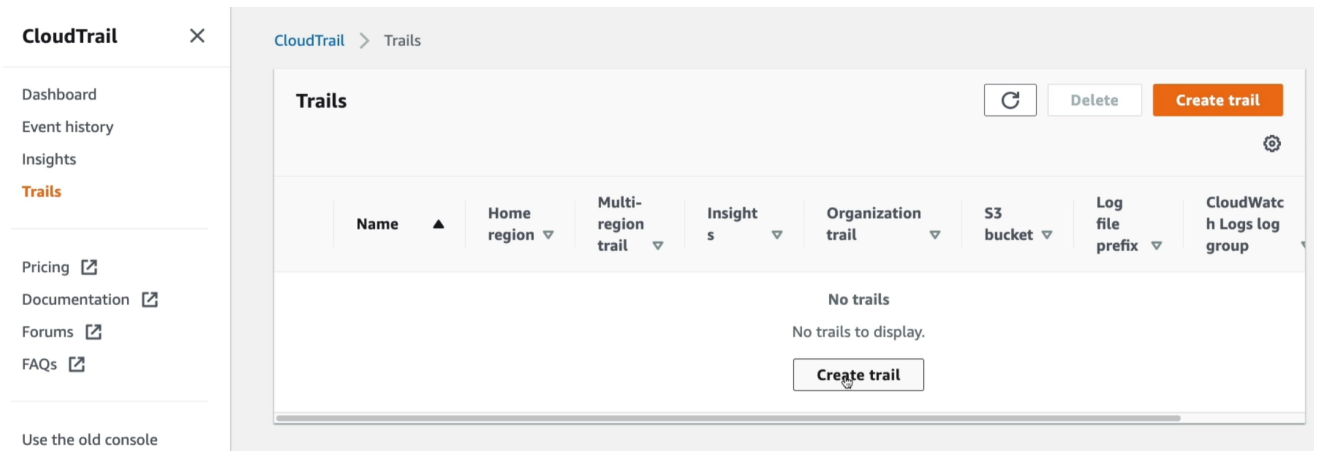

aws
Services
Search for services, features, marketplace products, and docs
[Option+S]
stephane-ccp
Ireland
CloudTrail
Dashboard
Event history
Insights
Trails
Pricing
Documentation
Forums
FAQs
Use the old console
Management & Governance
AWS CloudTrail
Continuously log your AWS account activity
Use CloudTrail to meet your governance, compliance, and auditing needs for your AWS accounts.
Create a trail with AWS CloudTrail
Get started with AWS CloudTrail by creating a trail to log your AWS account activity.
Create a trail
Pricing
Pricing
How it works

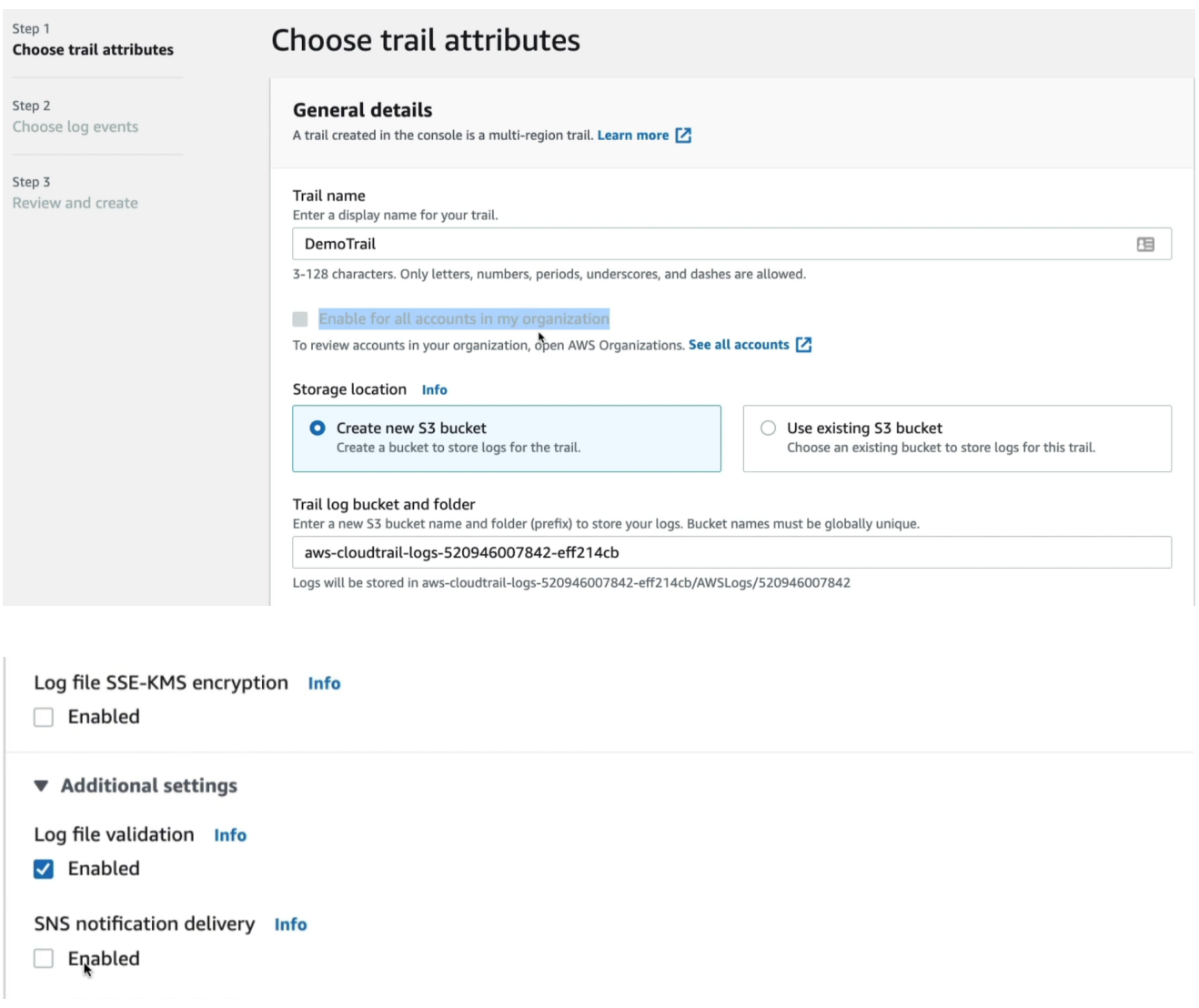

CloudTrail
Dashboard
Event history
Insights
Trails
Pricing
Documentation
Forums
FAQs
Use the old console
CloudTrail > Dashboard
Dashboard Info
Trails Info
Create trail
Name
Status
No trails
No trails to display.
Create trail
CloudTrail Insights Info
CloudTrail Insights is not enabled
Insights event collection requires a trail. Additional charges apply. Learn more
Create a trail
Event history Info
Event name
Event time
Event source
DeletePolicy
January 28, 2021, 17:37:21 (UTC+00:00)
iam.amazonaws.com
DeletePolicyVersion
January 28, 2021, 17:37:20 (UTC+00:00)
iam.amazonaws.com


CloudTrail
Dashboard
Event history
Insights
Trails
Pricing
Documentation
Forums
FAQs
Use the old console
CloudTrail > Event history
Event history (50+) Info
Download events
Create Athena table
Event history shows you the last 90 days of management events.
Read-only
false
30m
1h
3h
12h
Custom
1
2
...
Event name
Event time
User name
Event source
Resource type
Resource name
DeletePolicy
January 28, ...
AWSCodeSt...
iam.amazonaws.com
AWS::IAM::Policy
arn:aws:iam::52...
DeletePolicy...
DeleteRole
AWS::IAM::Role
CodeStarWorke...



Create Trail





CloudWatch Logs - *optional*

Configure CloudWatch Logs to monitor your trail logs and notify you when specific activity occurs. Standard CloudWatch and CloudWatch Logs charges apply. **Learn more**

CloudWatch Logs **Info**

☑ Enabled

Log group **Info**

◉ New
○ Existing

Log group name

aws-cloudtrail-logs-520946007842-e71cefab

1-512 characters. Only letters, numbers, dashes, underscores, forward slashes, and periods are allowed.

IAM Role **Info**

AWS CloudTrail assumes this role to send CloudTrail events to your CloudWatch Logs log group.

◉ New
○ Existing

Role name

CloudTrailRoleForCloudWatchLogs_{trail-name}

▶ **Policy document**

Choose log events

Events **Info**

Record API activity for individual resources, or for all current and future resources in AWS account. **Additional charges apply**

Event type

Choose the type of events that you want to log.

☑ Management events

Capture management operations performed on your AWS resources.

☑ Data events

Log the resource operations performed on or within a resource.

☑ Insights events

Identify unusual activity, errors, or user behavior in your account.

Management events **Info**

Management events show information about management operations performed on resources in your AWS account.

ⓘ No additional charges apply to log management events on this trail because this is your first copy of management events.

API activity

Choose the activities you want to log.

☑ Read ☑ Write

☑ Exclude AWS KMS events

Data events **Info**

Additional charges apply Data events show information about the resource operations performed on or within a resource.

ⓘ **Advanced data event selectors**
Advanced data event selectors give you more control over the events that are captured by your trail. Advanced data event selectors offer fine-grained controls on the following fields within an event: eventName, eventSource, readOnly, eventCategory, resources.type, and resources.ARN. These new controls can help you control costs by limiting the data events that are important to you.

Switch to advanced event selectors

Data event: S3 **Info** — **Remove**

Data event source

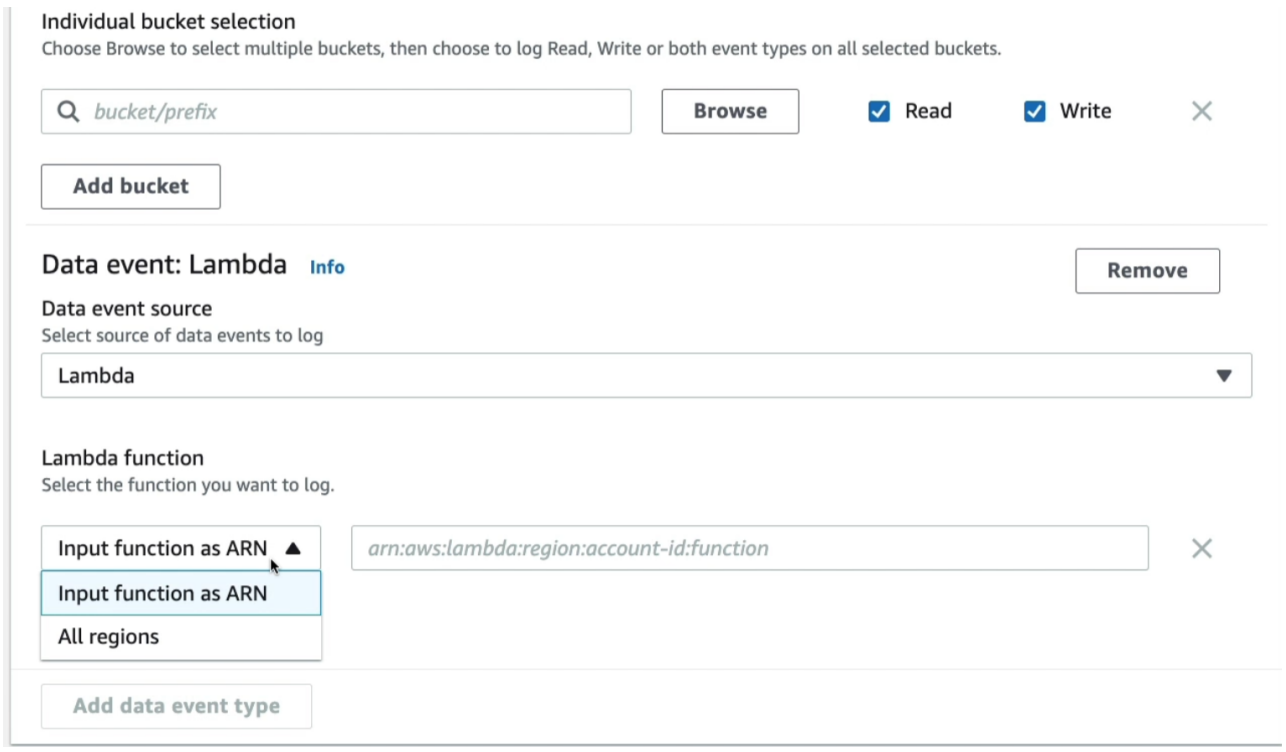
Select source of data events to log

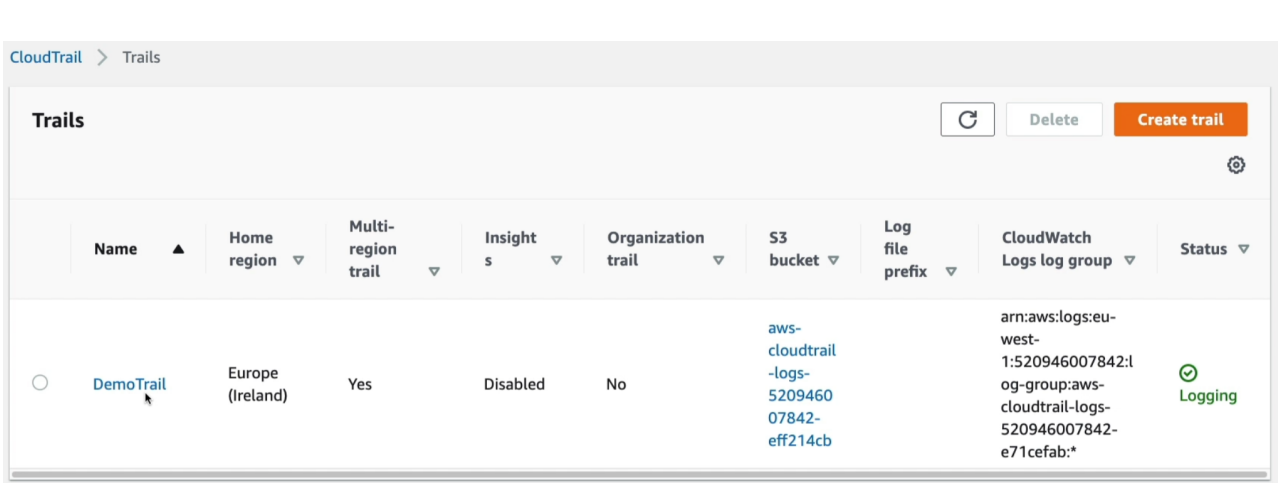
S3

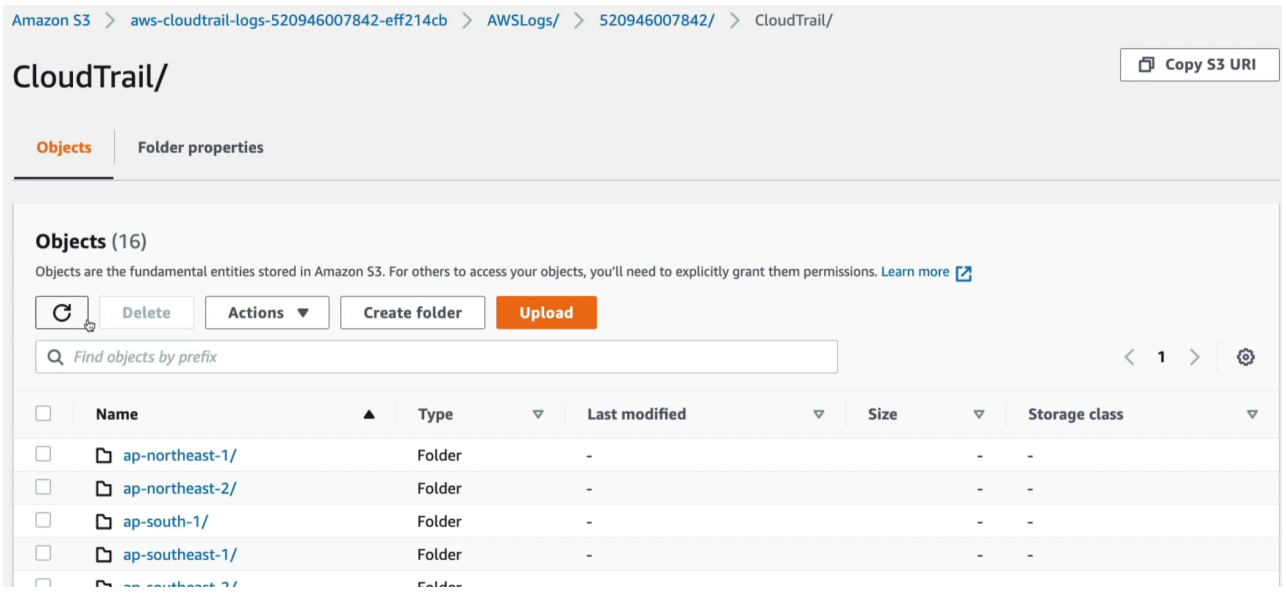
S3 bucket

You can choose to log read and/or write events for all buckets. You can also choose individual buckets.

All current and future S3 buckets ☑ Read ☑ Write







AWS Config

- Helps with auditing and recording **compliance** of your AWS resources
- Helps record configurations and changes over time
- Questions that can be solved by AWS Config:
  - Is there unrestricted SSH access to my security group?
  - Do my buckets have any public access?
  - How has my ALB configuration changed over time?
- You can receive alerts (SNS notifications) for any changes
- AWS Config is a per-region service
- Can be aggregated across regions and accounts
- Possibility of storing the configuration data into S3 (analyzed by Athena)

Config Rules

- Can use AWS managed config rules (over 75)
- Can make custom config rules (must be defined in AWS Lambda)

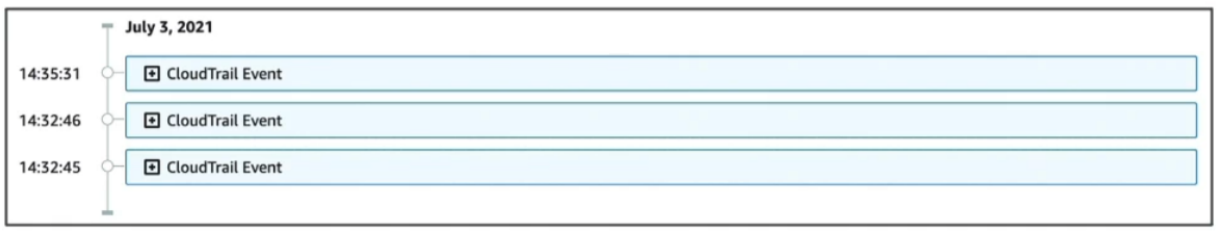
    - Ex: evaluate if each EBS disk is of type gp2
    - Ex: evaluate if each EC2 instance is t2.micro
- Rules can be evaluated / triggered:
    - For each config change
    - And / or: at regular time intervals
- **AWS Config Rules does not prevent actions from happening (no deny)**
- Pricing: no free tier,$0.003 per configuration item recorded per region, $ 0.001 per config rule evaluation per region

AWS Config Resource

- View compliance of a resource over time

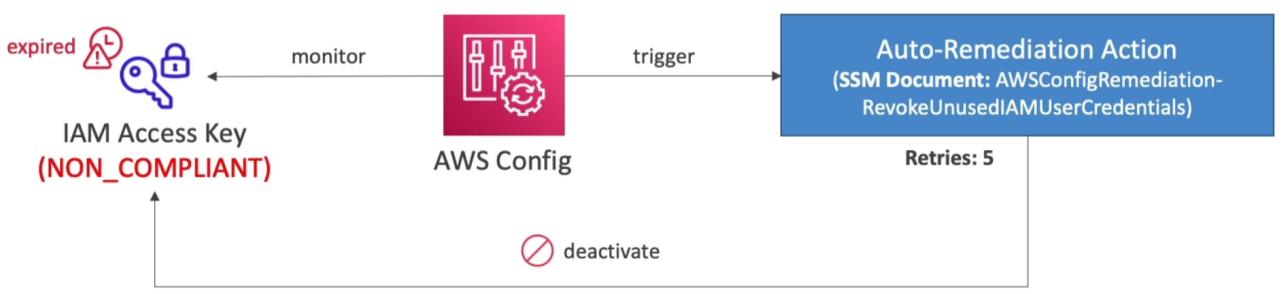
- View configuration of a resource over time

- View CloudTrail API calls of a resource over time



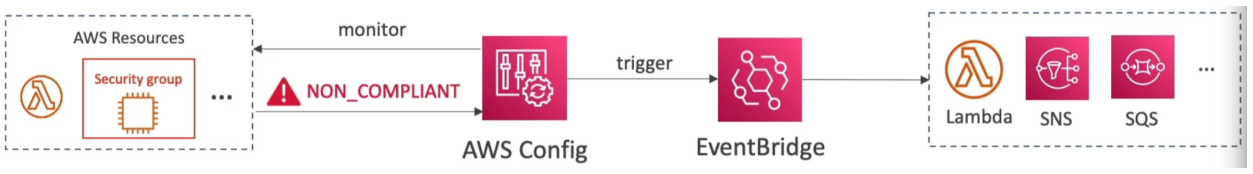
Config Rules - Remediations

- Automate remediation of non-compliant resources using SSM Automation Documents
- Use AWS-Managed Automation Documents or create custom Automation Documents
    - Tip: you can create custom Automation Documents that invokes Lambda function
- You can set **Remediation Retries** if the resource is stil non-compliant after auto-remediation

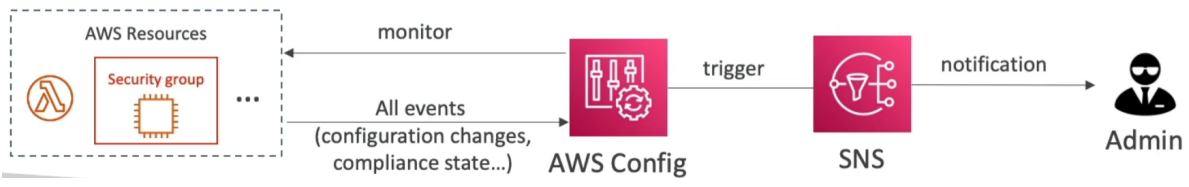


Config Rules - Notifications

- Use EventBridge to trigger notifications when AWS resources are non-compliant



- Ability to send configuration changes and compliance state notifications to SNS (all events - use SNS Filtering or filter at client-side)



Hands on

AWS Config > Set up AWS Config

Step 1
Settings

Step 2
Rules

Step 3
Review

Settings

General settings

Resource types to record

- (•) Record all resources supported in this region
- ( ) Record specific resource types

To learn more, see Supported Resource Types .

[x] Include global resources (e.g., AWS IAM resources)
Supported global resource types are IAM users, groups, roles, and customer managed polices.

AWS Config role

- (•) Create AWS Config service-linked role
- ( ) Choose a role from your account

Delivery method

Amazon S3 bucket

- (•) Create a bucket
- ( ) Choose a bucket from your account
- ( ) Choose a bucket from another account

Ensure appropriate permissions are available in this S3 bucket's policy. Learn more .

S3 bucket name

nfig-bucket-001736599714 | Prefix (optional) | /AWSLogs/001736599714/Config/eu-central-1

Amazon SNS topic

[ ] Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. Learn more .

Cancel **Next**

AWS Config > Set up AWS Config

Step 1
Settings

Step 2
Rules

Step 3
Review

Review

Review your AWS Config setup details. You can go back to edit changes for each section. Choose **Confirm** to finish setting up AWS Config.

General settings

Resource types to record
All resources (including global resources)

AWS Config role
AWSServiceRoleForConfig

Delivery method

S3 bucket name
config-bucket-001736599714

▸ **AWS Config rules (0)**

Cancel | Previous | Confirm

AWS Config > Rules

Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the compliance results.

Rules

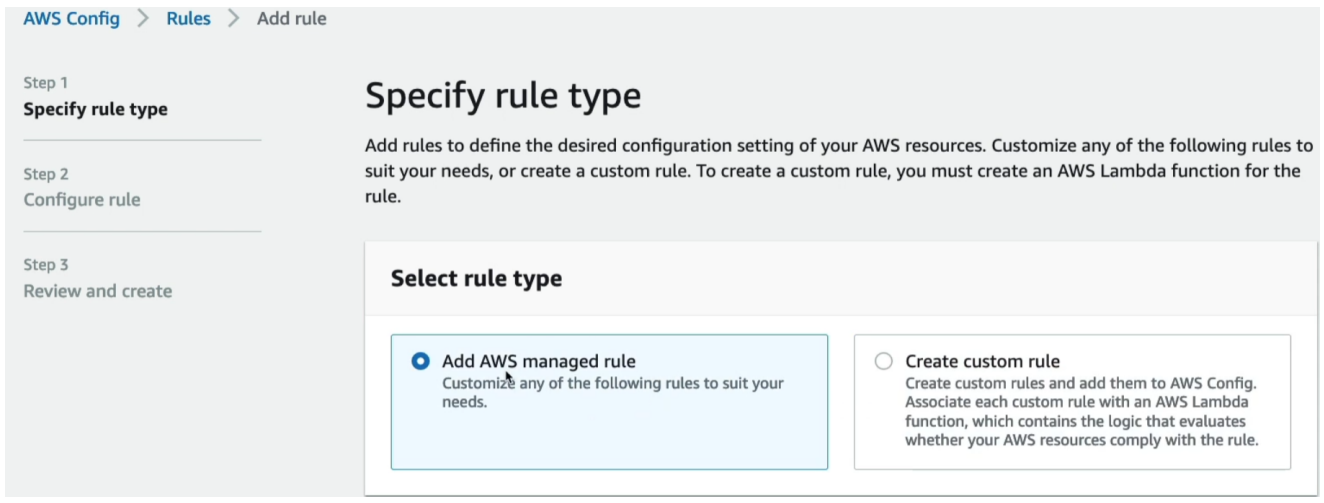
View details | Edit rule | Actions | Add rule

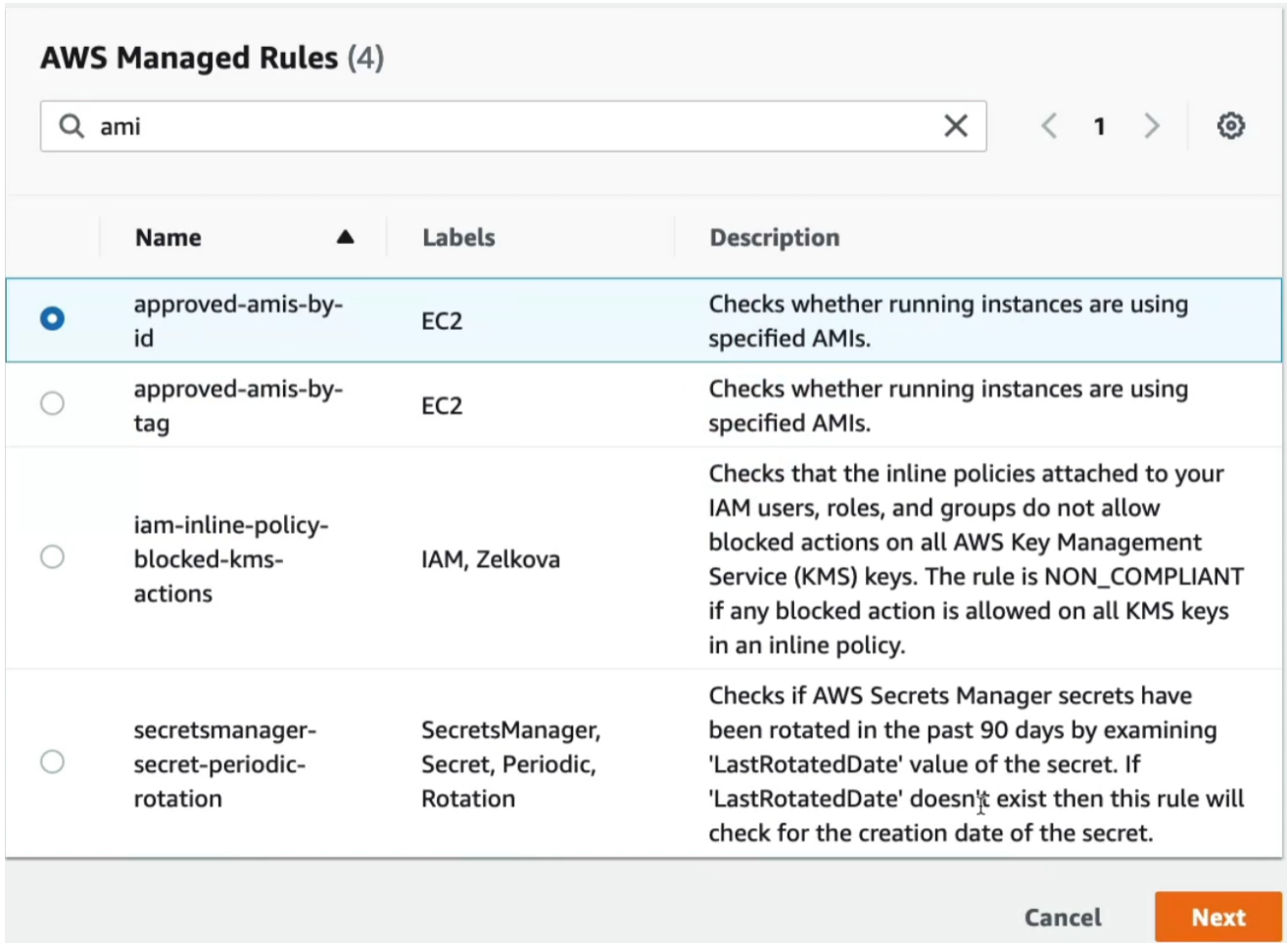
Any status

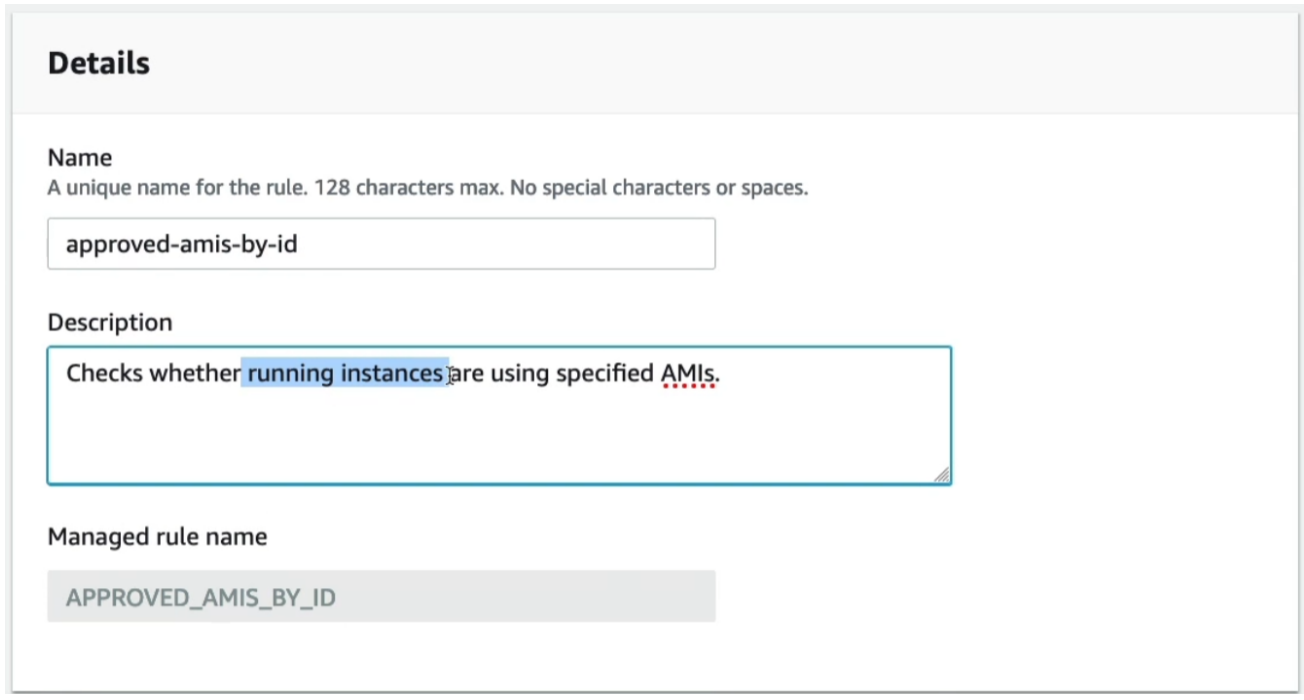
1

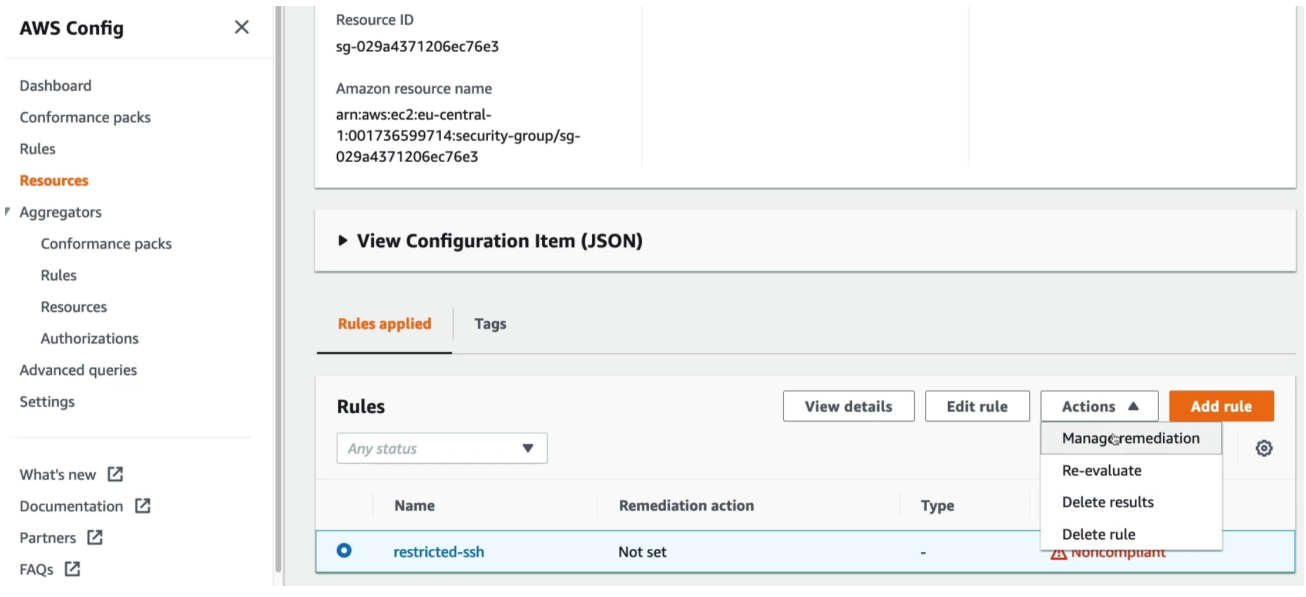
Name	Remediation action	Type	Compliance

No rules found.
Add rule


AWS Config > Rules > Add rule
Step 1
Specify rule type
Step 2
Configure rule
Step 3
Review and create
Specify rule type
Add rules to define the desired configuration setting of your AWS resources. Customize any of the following rules to suit your needs, or create a custom rule. To create a custom rule, you must create an AWS Lambda function for the rule.
Select rule type
Add AWS managed rule
Customize any of the following rules to suit your needs.
Create custom rule
Create custom rules and add them to AWS Config. Associate each custom rule with an AWS Lambda function, which contains the logic that evaluates whether your AWS resources comply with the rule.


AWS Managed Rules (4)
ami
1
Name
Labels
Description
approved-amis-by-id
EC2
Checks whether running instances are using specified AMIs.
approved-amis-by-tag
EC2
Checks whether running instances are using specified AMIs.
iam-inline-policy-blocked-kms-actions
IAM, Zelkova
Checks that the inline policies attached to your IAM users, roles, and groups do not allow blocked actions on all AWS Key Management Service (KMS) keys. The rule is NON_COMPLIANT if any blocked action is allowed on all KMS keys in an inline policy.
secretsmanager-secret-periodic-rotation
SecretsManager, Secret, Periodic, Rotation
Checks if AWS Secrets Manager secrets have been rotated in the past 90 days by examining 'LastRotatedDate' value of the secret. If 'LastRotatedDate' doesn't exist then this rule will check for the creation date of the secret.
Cancel
Next


Details
Name
A unique name for the rule. 128 characters max. No special characters or spaces.
approved-amis-by-id
Description
Checks whether running instances are using specified AMIs.
Managed rule name
APPROVED_AMIS_BY_ID



CloudWatch vs CloudTrail vs Config

- CloudWatch
  - Performance monitoring (metrics, CPU, network, etc...) & dashboards
  - Event & Alerting
  - Log Aggregation & Analysis
- CloudTrail
  - Record API calls made within your Account by Everyone
  - Can define trails for specific resources
  - Global Service
- Config
  - Record configuration changes
  - Evaluate resources against compliance rules
  - Get timeline of changes and compliance

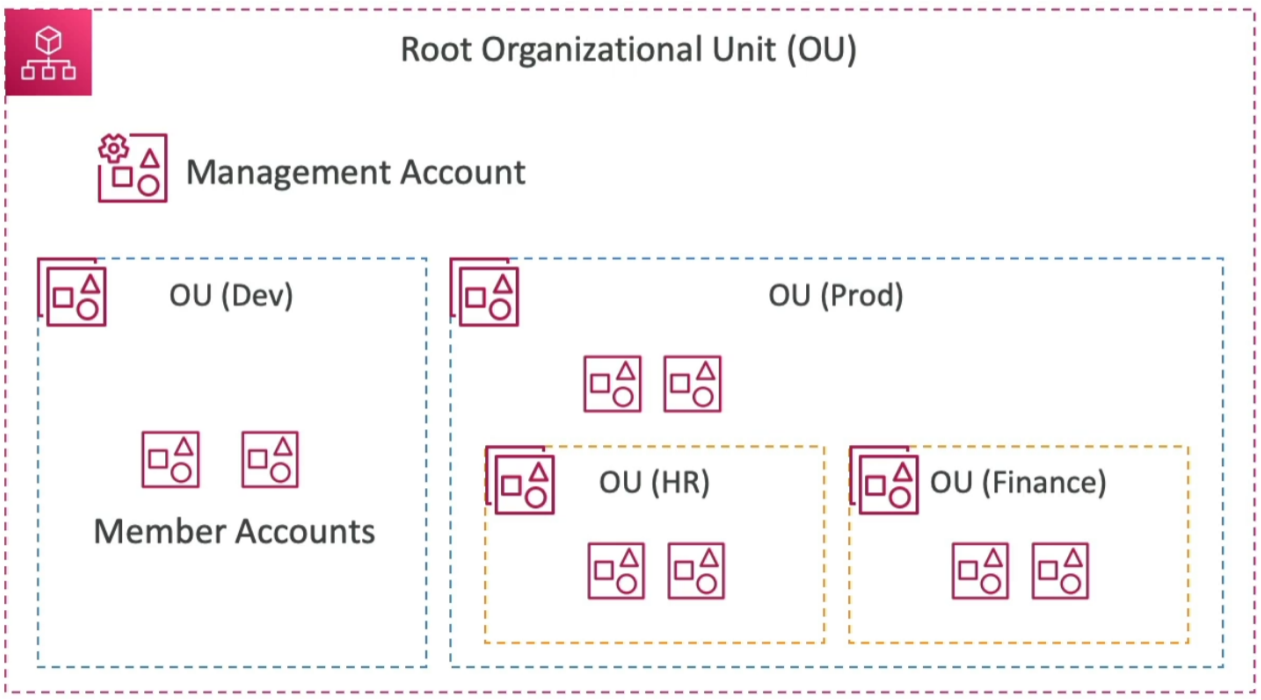
For an Elastic Load Balancer

- CloudWatch:
  - Monitoring Incoming connections metric
  - Visualize error codes as a % over time
  - Make a dashboard to get an idea of your load balancer performance
- Config:
  - Track security group rules for the Load Balancer
  - Track configuration changes for the Load Balancer
  - Ensure an SSL certificate is always assigned to the Load Balancer (compliance)
- CloudTrail:
  - Track who made any changes to the Load Balancer with API calls

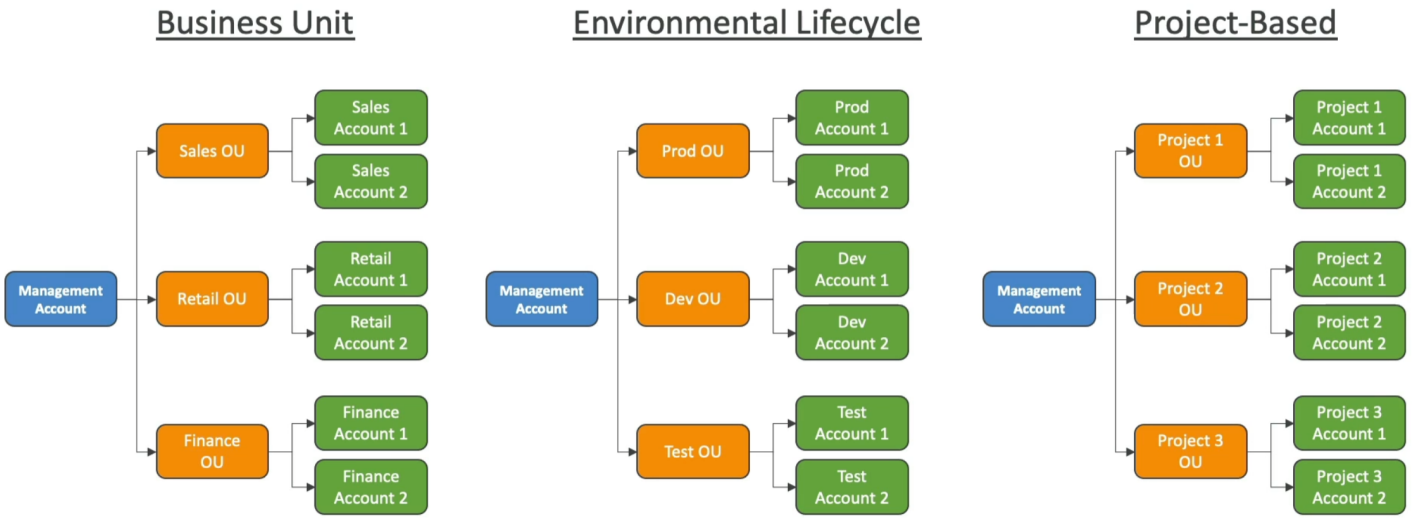
AWS Organizations

- Global service
- Allows to manage multiple AWS accounts
- The main account is the management account
- Other accounts are member accounts
- Member accounts can only be part of one organization
- Consolidated Billing across all accounts - single payment method
- Pricing benefits from aggregated usage (volume discount for EC2, S3...)
- **Shared reserved instances and Savings Plans discounts across accounts**

- API is available to automate AWS account creation



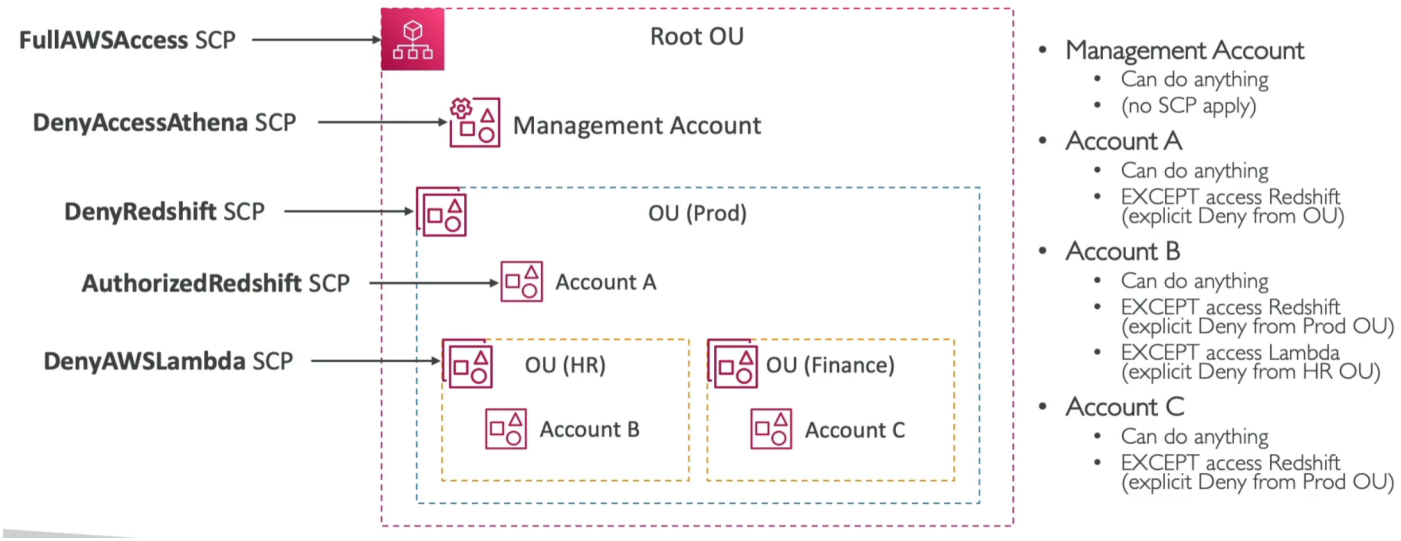
Organizational Units (OU) - Examples



AWS Organizations

- **Advantages**
  - Multi Account vs One Account Multi VPC
  - Use tagging standars for billing purposes
  - Enable CloudTrail on all accounts, send logs to central S3 account
  - Send CloudWatch Logs to central logging account
  - Establish Cross Account Roles for Admin purposes
- **Security: Service Control Policies (SCP)**
  - IAM policies **applied to OU or Accounts** to restrict Users and Roles
  - They do not apply to the management account (fully admin power)
  - Must have an explicit allow (does not allow anything by default - like IAM)

SCP Hierarchy



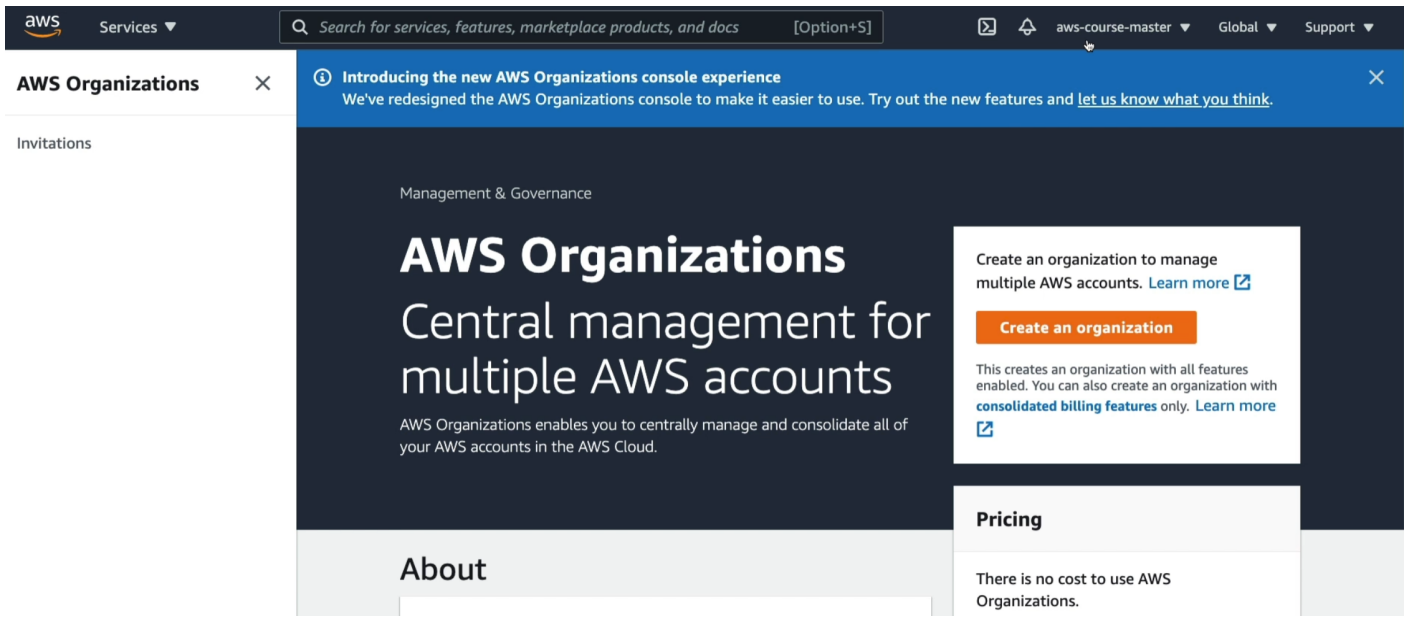
SCP Examples

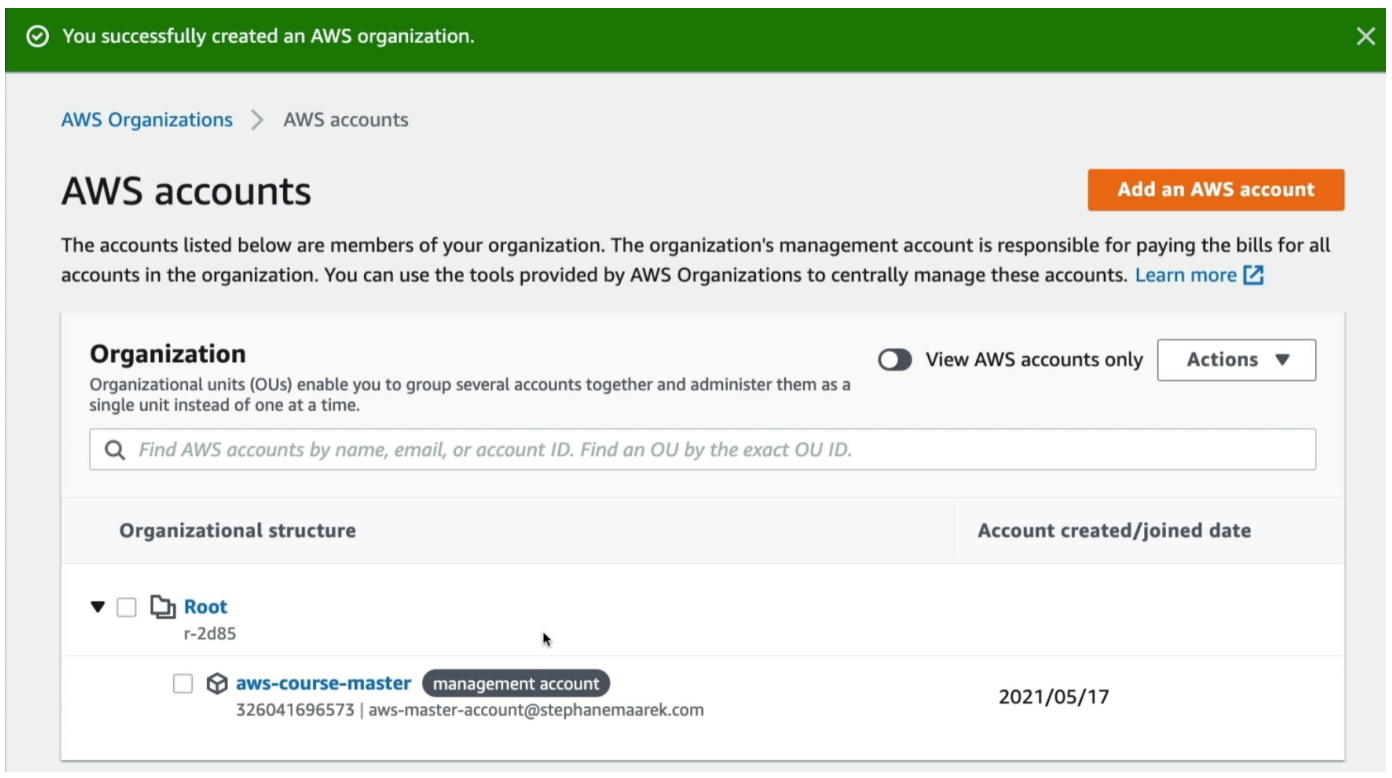
Blocklist and Allowlist strategies

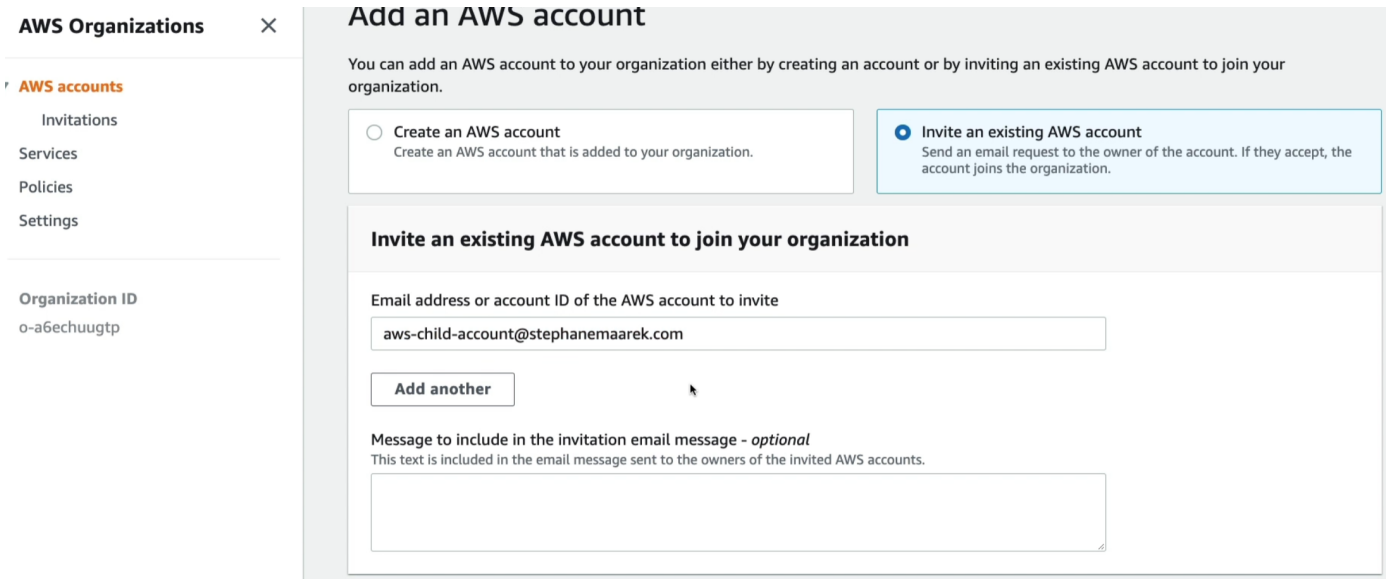
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowsAllActions",
            "Effect": "Allow",
            "Action": "*",
            "Resource": "*"
        },
        {
            "Sid": "DenyDynamoDB",
            "Effect": "Deny",
            "Action": "dynamodb:*",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

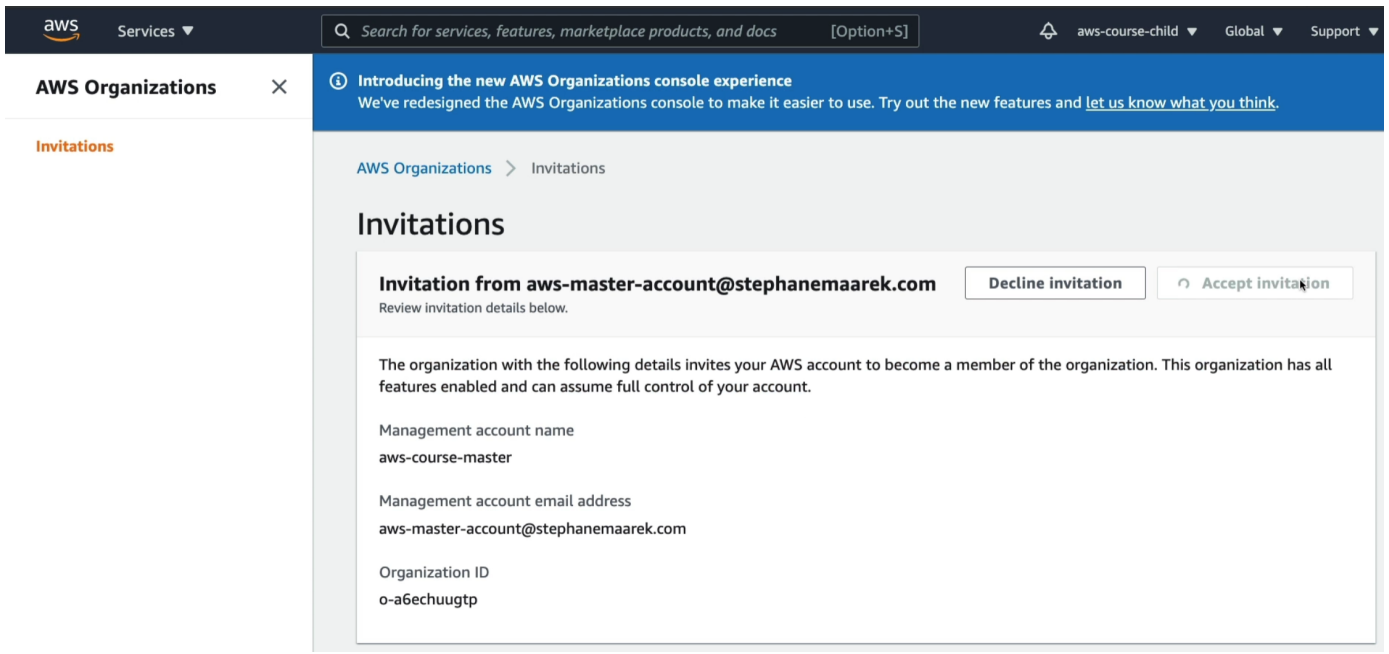
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:*",
                "cloudwatch:*"
            ],
            "Resource": "*"
        }
    ]
}
```

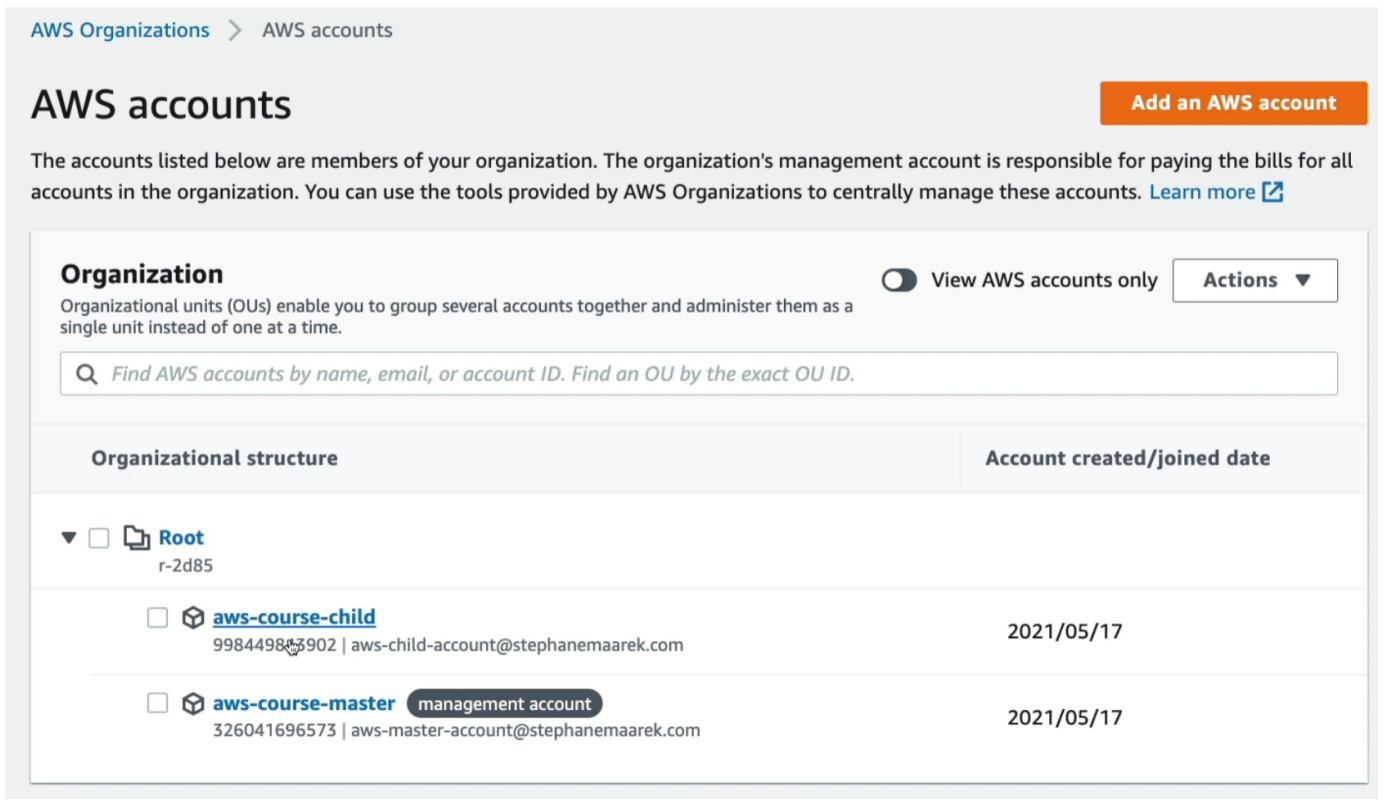
Hnads on






AWS Organizations
AWS accounts
Invitations
Services
Policies
Settings
Organization ID
o-a6echuugtp
Add an AWS account
You can add an AWS account to your organization either by creating an account or by inviting an existing AWS account to join your organization.
Create an AWS account
Create an AWS account that is added to your organization.
Invite an existing AWS account
Send an email request to the owner of the account. If they accept, the account joins the organization.
Invite an existing AWS account to join your organization
Email address or account ID of the AWS account to invite
aws-child-account@stephanemaarek.com
Add another
Message to include in the invitation email message - optional
This text is included in the email message sent to the owners of the invited AWS accounts.


aws
Services
Search for services, features, marketplace products, and docs
[Option+S]
aws-course-child
Global
Support
AWS Organizations
Invitations
Introducing the new AWS Organizations console experience
We've redesigned the AWS Organizations console to make it easier to use. Try out the new features and let us know what you think.
AWS Organizations > Invitations
Invitations
Invitation from aws-master-account@stephanemaarek.com
Review invitation details below.
Decline invitation
Accept invitation
The organization with the following details invites your AWS account to become a member of the organization. This organization has all features enabled and can assume full control of your account.
Management account name
aws-course-master
Management account email address
aws-master-account@stephanemaarek.com
Organization ID
o-a6echuugtp


AWS Organizations > AWS accounts
AWS accounts
Add an AWS account
The accounts listed below are members of your organization. The organization's management account is responsible for paying the bills for all accounts in the organization. You can use the tools provided by AWS Organizations to centrally manage these accounts. Learn more
Organization
Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.
View AWS accounts only
Actions
Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.
Organizational structure
Account created/joined date
Root
r-2d85
aws-course-child
9984498[redacted]3902 | aws-child-account@stephanemaarek.com
2021/05/17
aws-course-master
management account
326041696573 | aws-master-account@stephanemaarek.com
2021/05/17

Go into Root

ARN

arn:aws:organizations::326041696573:root/o-a6echuugtp/r-2d85

Enabled policy types (**manage policy types**)

-

Children | Tags | Policies

Children

These are organizational units and AWS accounts attached directly to Root.

Actions

- Organizational unit
  - Create new
  - Rename
  - Delete
- AWS account
  - Move
  - Remove from organization

Organizational structure	Ac
aws-course-child 998449843902 | aws-child-account@stephanemaarek.com	20
aws-course-master management account 326041696573 | aws-master-account@stephanemaarek.com	20

Create organizational unit in Root

An organizational unit (OU) can contain both accounts and other OUs. This enables you to create an inverted tree hierarchy. The structure has a root at the top and branches of OUs that reach down. The branches end in accounts that act as the leaves of the tree. Learn more

Details

Organizational unit name

Dev

An OU name can be up to 128 characters.

Tags

Tags are key-value pairs that you can add to AWS resources to help identify, organize, and secure your AWS resources.

No tags are associated with the resource.

Add tag

You can add 50 more tags.

Cancel | Create organizational unit

Organizational structure	Account created/joined date
Root r-2d85	
Dev ou-2d85-bbsxn9eg	
This resource is empty	
Prod ou-2d85-w88cuurs	
Finance ou-2d85-y7g174ph	
HR ou-2d85-8ysq05u4	
Test ou-2d85-7k5vpz5i	
aws-course-child 998449843902 | aws-child-account@stephanemaarek.com	2021/05/17
aws-course-master management account 326041696573 | aws-master-account@stephanemaarek.com	2021/05/17

Move account

Organizational structure	Account created/joined date
Root r-2d85	
Dev ou-2d85-bbsxn9eg	
Prod ou-2d85-w88cuurs	
Finance ou-2d85-y7g174ph	
aws-course-child 998449843902 | aws-child-account@stephanemaarek.com	2021/05/17
HR ou-2d85-8ysq05u4	
Test ou-2d85-7k5vpz5i	
aws-course-master management account 326041696573 | aws-master-account@stephanemaarek.com	2021/05/17

AWS Organizations

- AWS accounts
- Services
- Policies
- Settings

Organization ID
o-a6echuugtp

Introducing the new AWS Organizations console experience
We've redesigned the AWS Organizations console to make it easier to use. Try out the new features and let us know what you think.

AWS Organizations > Policies > Service control policies

Service control policies

Disable service control policies

Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. Learn more

Available policies

Actions | Create policy

Name	Kind	Description
FullAWSAccess	AWS managed policy	Allows access to every operation

Create new service control policy

A service control policy (SCP) specifies the maximum permissions that can be used by users and roles in your organization's accounts. An SCP doesn't grant permissions. You must still use IAM permission policies or resource policies to grant permissions. Learn more

Details

Policy name

DenyAccessS3

A policy name can be up to 128 characters and can include the following characters: a-z, A-Z, 0-9, and .,*=@_-

Policy description - *optional*

e.g Sandbox

A description can have up to 512 characters and can include the following characters: a-z, A-Z, 0-9, and .,*=@_-

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "DenyS3",
            "Effect": "Deny",
            "Action": [
                "s3:*"
            ],
            "Resource": ["*"]
        }
    ]
}
```

Edit statement
DenyS3
Remove

1. Add actions

Choose a service

s3

Included

S3

Available

S3 Object Lambda

S3 Outposts

Successfully created the policy named 'DenyAccessS3'.

AWS Organizations > Policies > Service control policies

Service control policies

Disable service control policies

Service control policies (SCPs) enable central administration over the permissions available within the accounts in your organization. This helps ensure that your accounts stay within your organization's access control guidelines. Learn more

Available policies

Actions | Create policy

Name	Kind	Description
DenyAccessS3	Customer managed policy	-
FullAWSAccess	AWS managed policy	Allows access to every operation

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

View AWS accounts only | Actions

Find AWS accounts by name, email, or account ID. Find an OU by the exact OU ID.

Organizational structure | Account created/joined date

- Root
  r-2d85
  - Dev
    ou-2d85-bbsxn9eg
  - Prod
    ou-2d85-w88cuurs
    - Finance
      ou-2d85-y7g174ph
    - HR
      ou-2d85-8ysq05u4
  - Test
    ou-2d85-7k5vpz5i

Children | Tags | Policies

You have enabled the following policy type out of the 4 available to the organization.

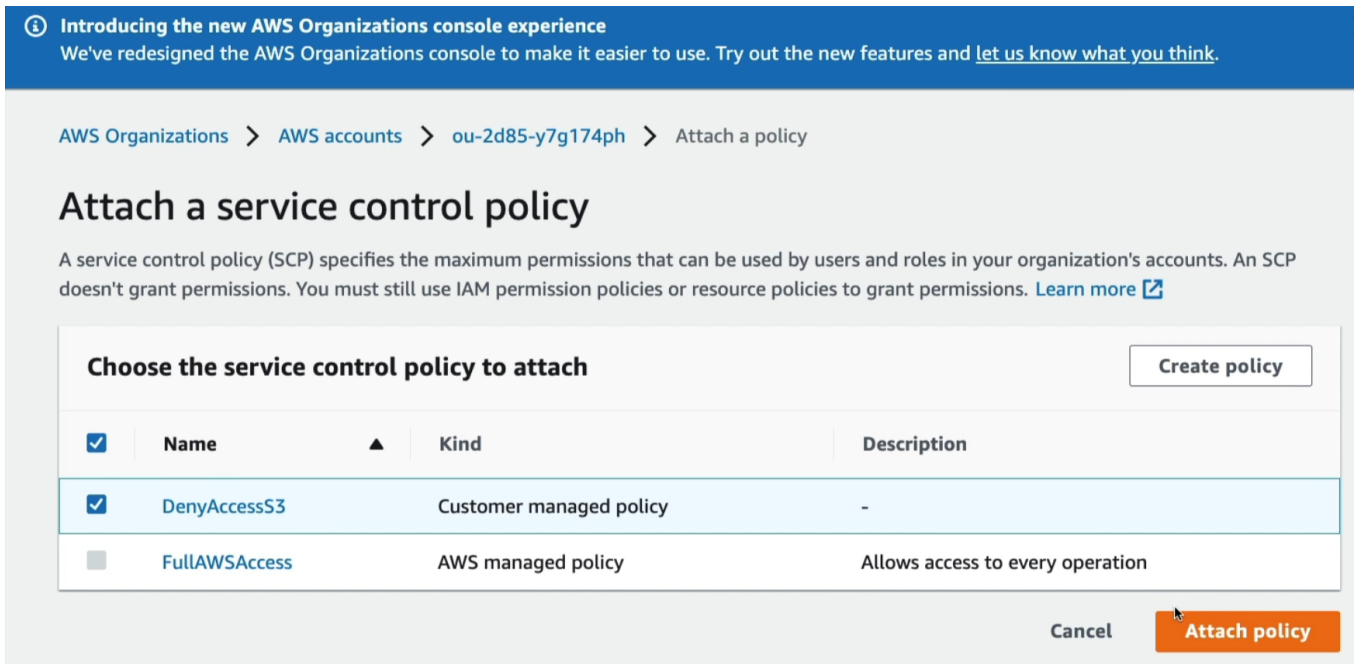
Service control policies

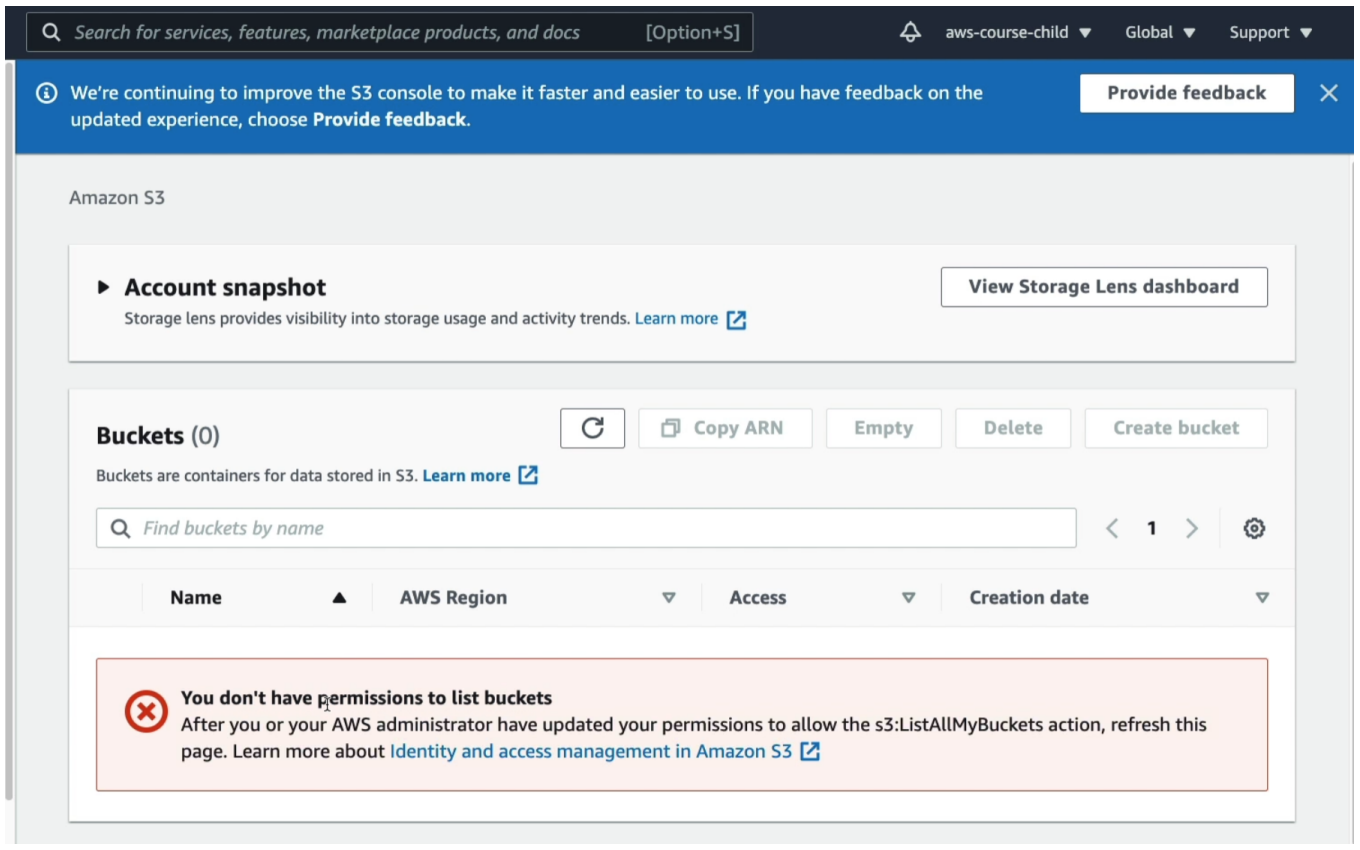
Service control policies (SCPs) enable central administration of the permissions available within the accounts in your organization. Policies attached to the root or to OUs can be inherited by child OUs and accounts. Learn more

Applied policies (3)

Detach | Attach

Name	Source	Description
FullAWSAccess (AWS managed policy)	Attached directly	Allows access to every operation
FullAWSAccess (AWS managed policy)	Inherited from Prod	Allows access to every operation
FullAWSAccess (AWS managed policy)	Inherited from Root	Allows access to every operation





IAM Conditions

aws:SourceIp
restrict the client IP **from**
which the API calls are being made

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": "*",
            "Resource": "*",
            "Condition": {
                "NotIpAddress": {
                    "aws:SourceIp": ["192.0.2.0/24", "203.0.113.0/24
                }
            }
        }
    ]
}
```

aws:RequestedRegion
restrict the region the
API calls are made **to**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": ["ec2:*", "rds:*", "dynamodb:*"],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestedRegion": ["eu-central-1", "eu-west-1"]
                }
            }
        }
    ]
}
```

ec2:ResourceTag
restrict based on **tags**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["ec2:startInstances", "ec2:StopInstances"],
            "Resource": "arn:aws:ec2:us-east-1:123456789012:instance/*",
            "Condition": {
                "StringEquals": {
                    "ec2:ResourceTag/Project": "DataAnalytics",
                    "aws:PrincipalTag/Department": "Data"
                }
            }
        }
    ]
}
```

aws:MultiFactorAuthPresent
to force **MFA**

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "ec2:*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": ["ec2:StopInstances", "ec2:TerminateInstances"],
            "Resource": "*",
            "Condition": {
                "BoolIfExists": {
                    "aws:MultiFactorAuthPresent": false
                }
            }
        }
    ]
}
```

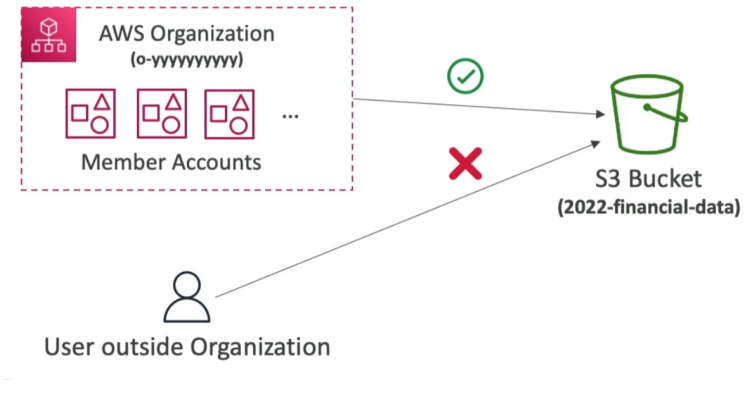
IAM for S3

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:ListBucket"],
            "Resource": "arn:aws:s3:::test"
        },
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "s3:GetObject",
                "s3:DeleteObject"
            ],
            "Resource": "arn:aws:s3:::test/*"
        }
    ]
}
```

- s3:ListBucket permission applies to arn:aws:s3:::test
- => bucket level permission
- s3:GetObject,s3:PutObject,
- s3:DeleteObject applies to arn:awn:s3:::test/*
- => object level permission

Resource Policies & aws:PrincipalOrgID

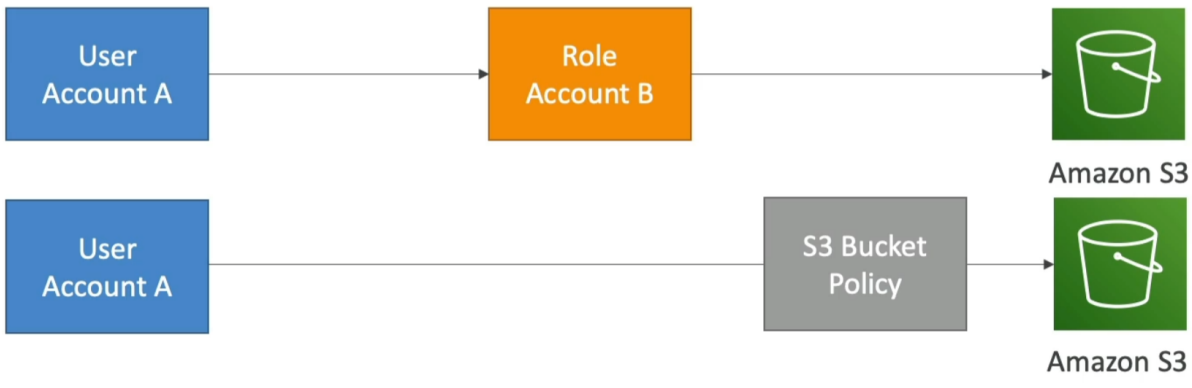
- **aws:PrincipalOrgID** can be used in any resource policies to restrict access to accounts that are member of an AWS Organization




```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": ["s3:PutObject", "s3:GetObject"],
            "Resource": "arn:aws:s3:::2022-financial-data/*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": ["o-yyyyyyyyyy"]
                }
            }
        }
    ]
}
```

IAM Roles vs Resource Based Policies

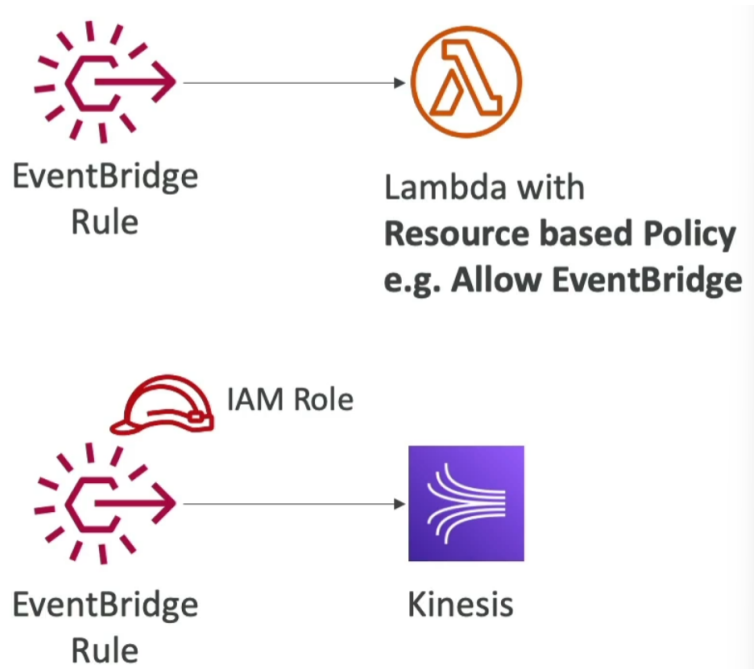
- Cross account:
  - attaching a resource-based policy to a resource (example: S3 bucket policy)
  - OR using a role as a proxy



- **When you assume a role (user,application or service), you give up your original permissions and take the permissions assigned to the role**
- When using a resource-based policy, the principal doesn't have to give up his permissions
- Example: User in account A needs to scan a DynamoDB table in Account A and dump it in an S3 bucket in Account B
- Supported by: Amazon S3 buckets, SNS topics, SQS queues, etc...

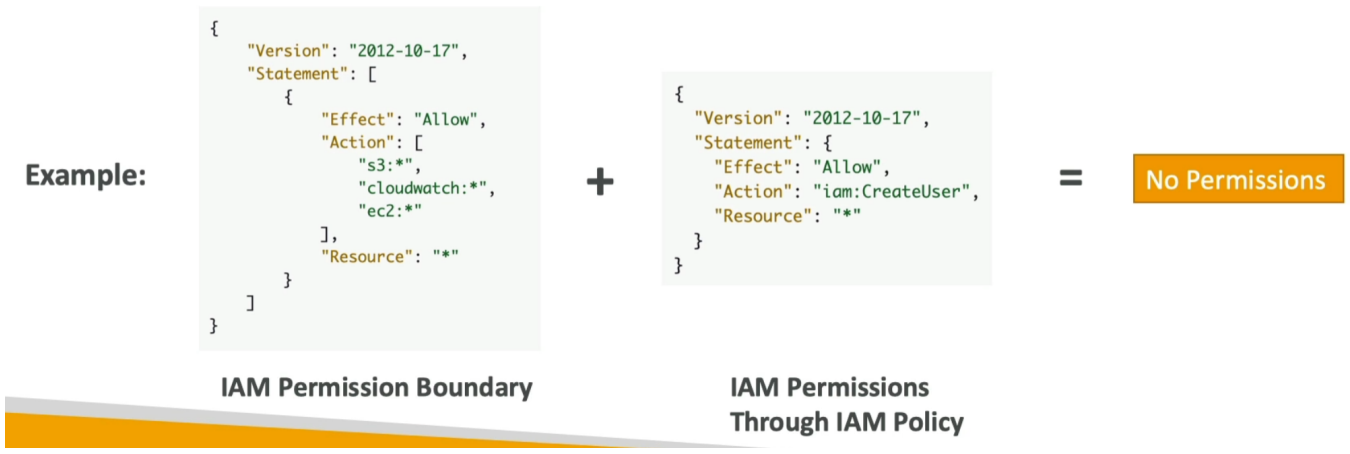
Amazon EventBridge - Security

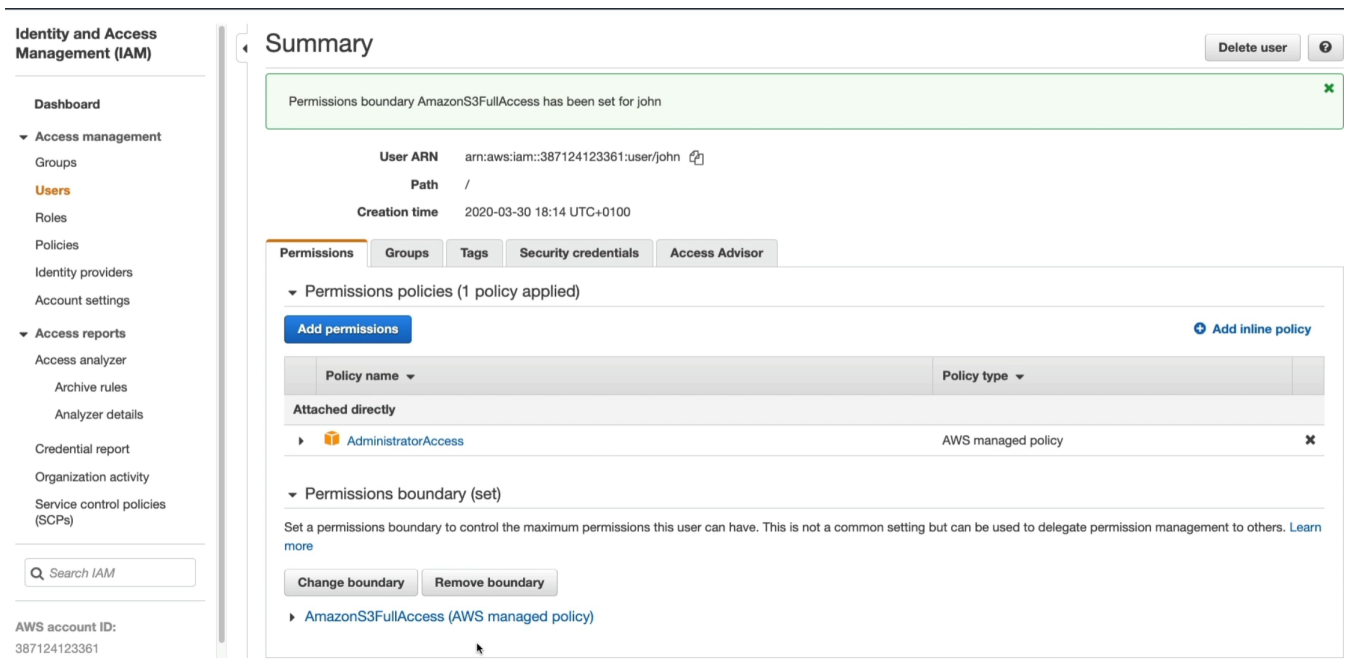
- When a rule runs, it needs permissions on the target
- Resource-based policy: Lambda, SNS, SQS, CloudWatch Logs, API Gateway...
- IAM role: Kinesis stream, Systems Manager Run Command, ECS task ...



IAM Permission Boundaries

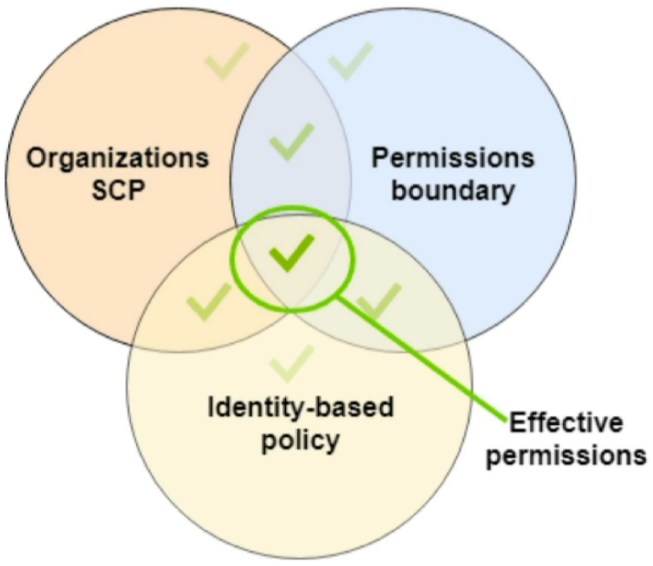
- IAM Permission Boundaries are supported for users and roles (not groups)
- Advanced feature to use a managed policy to set the maximum permissions an IAM entity can get



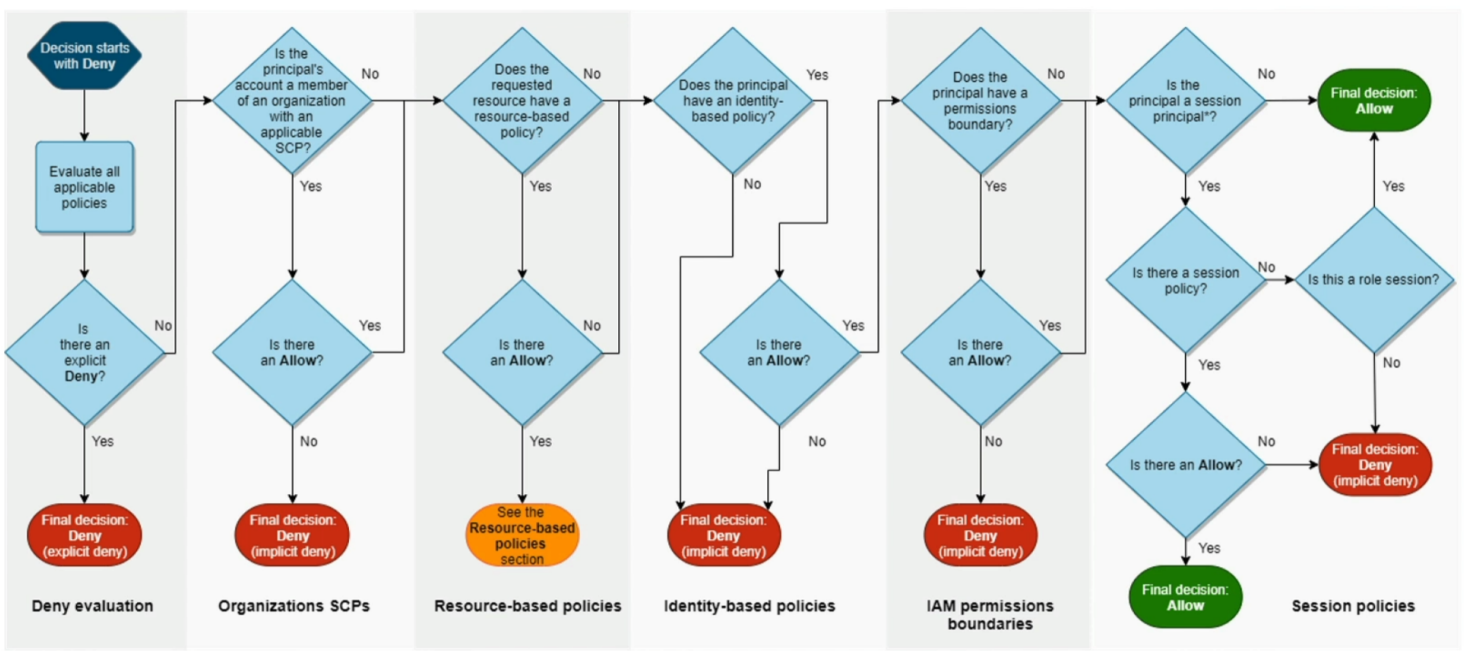


- Can be used in combinations of AWS Organizations SCP
- Use cases
  - Delegate responsibilities to non administrators within their permission boundaries, for example create new IAM users
  - Allow developers to self-assign policies and manage their own permissions, while making sure they can't "escalate" their privileges (= make themselves admin)

- Useful to restrict one specific user(instead of a whole account using Organizations & SCP)



IAM Policy Evaluation Logic



Example IAM Policy

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

- Can you perform sqs: CreateQueue? No
- Can you perform sqs: DeleteQueue? No
- Can you perform ec2: DescribeInstances? Yes

Amazon Cognito

- Give users an identity to interact with our web or mobile application
- **Cognito User Pools:**
  - Sign in functionality for app users
  - Integrate with API Gateway & Application Load Balancer

- **Cognito Identity Pools (Federated Identity):**

    - Provide AWS credentials to users so they can access AWS resources directly
    - Integrate with Cognito User Pools as an identity provider

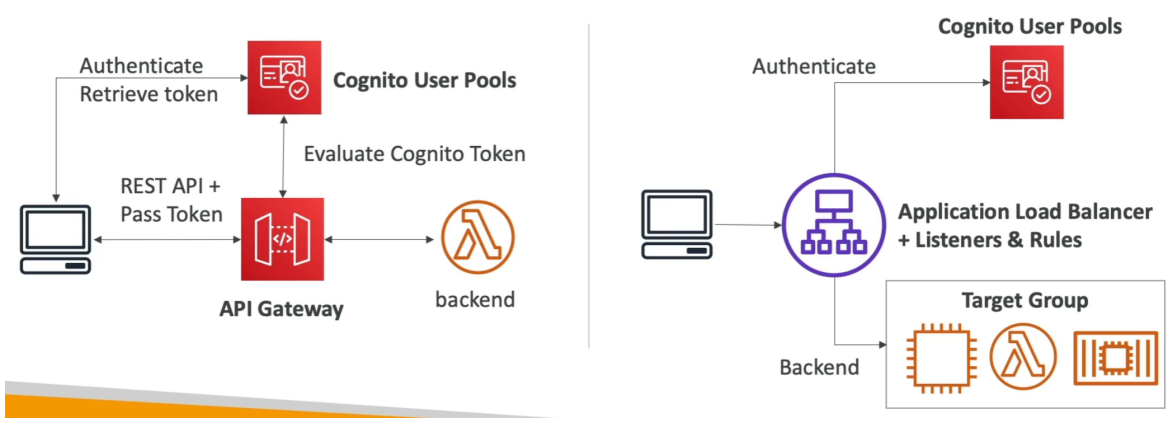
- **Cognito vs IAM:** "hundreds of users", "mobile users", "authenticate with SAML"

Cognito User Pools (CUP) - User Features

- **Create a serverless database of user for your web & mobile apps**
- Simple login: Username (or email) / password combination
- Password reset
- Email & Phone Number Verification
- Multi-factor authentication(MFA)
- Federated Identities: users from Facebook, Google, SAML ...

Cognito User Pools (CUP) - Integrations

- CUP integrates with **API Gateway** and **Application Load Balancer**

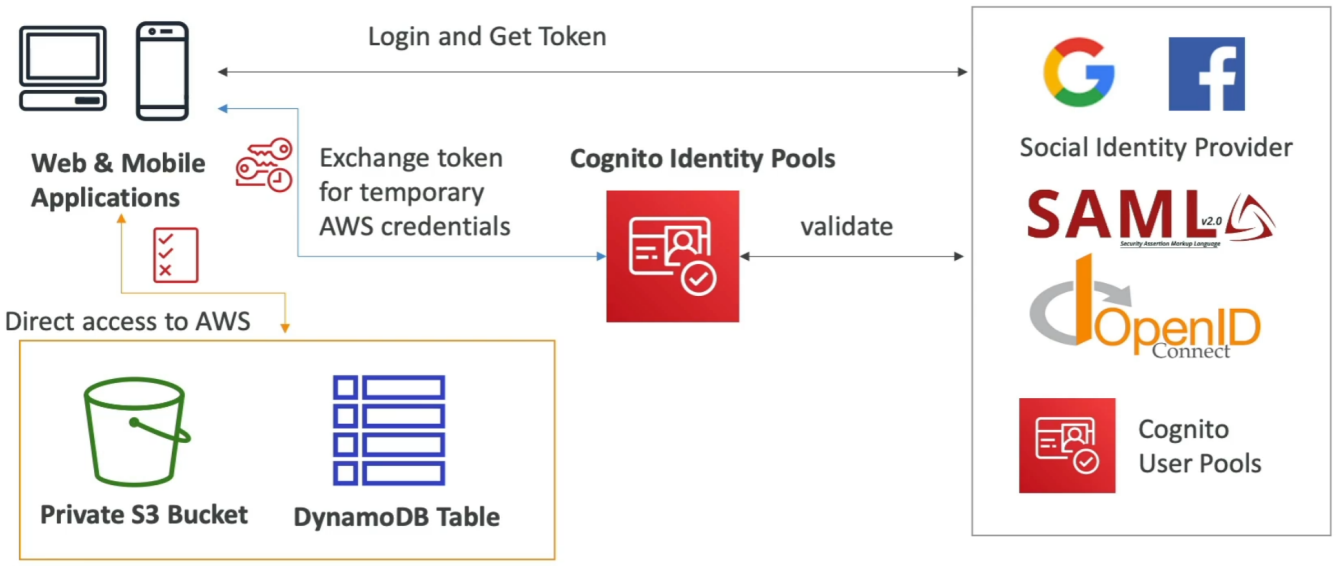


Cognito Identity Pools (Federated Identities)

- **Get identities for "users" so they obtain temporary AWS credentials**
- Users source can be Cognito User Pools, 3rd party logins, etc...

- **Users can then access AWS services directly or through API Gateway**
- The IAM policies applied to the credentials are defined in Cognito
- They can be customized based on the user_id for fine grained control
- **Default IAM roles** for authenticated and guest users

Cognito Identity Pools - Diagram



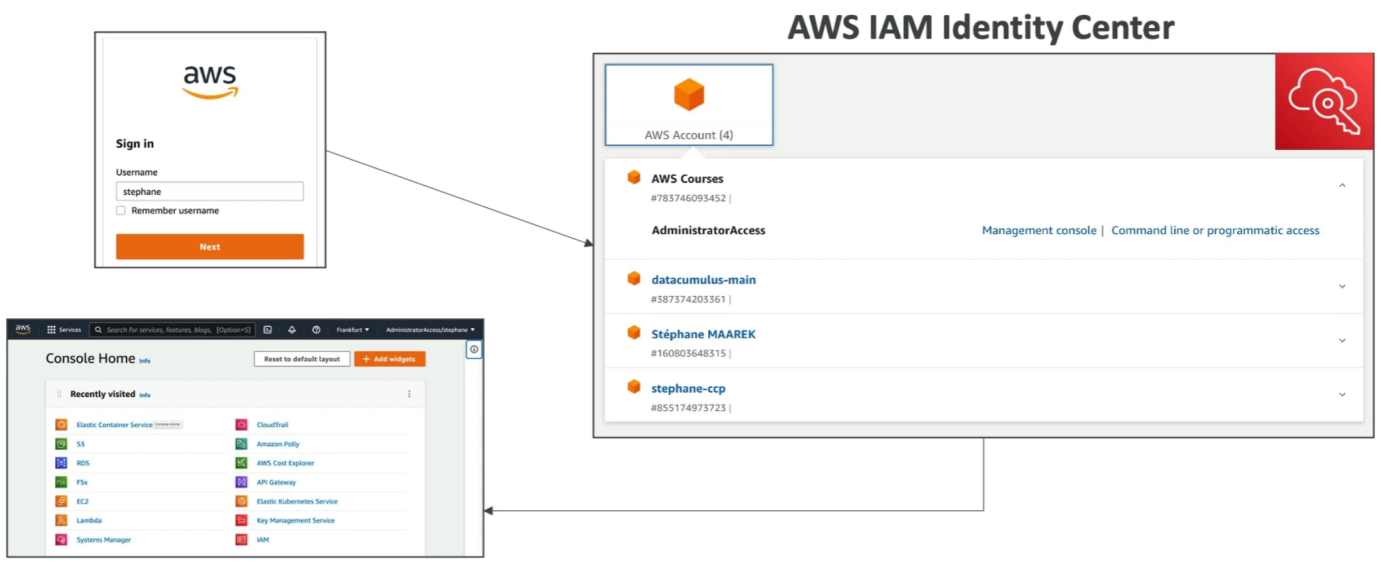
Cognito Identity Pools Row Level Security in DynamoDB

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "dynamodb:GetItem", "dynamodb:BatchGetItem", "dynamodb:Query",
                "dynamodb:PutItem", "dynamodb:UpdateItem", "dynamodb:DeleteItem",
                "dynamodb:BatchWriteItem"
            ],
            "Resource": [
                "arn:aws:dynamodb:us-west-2:123456789012:table/MyTable"
            ],
            "Condition": {
                "ForAllValues:StringEquals": {
                    "dynamodb:LeadingKeys": [
                        "${cognito-identity.amazonaws.com:sub}"
                    ]
                }
            }
        }
    ]
}
```

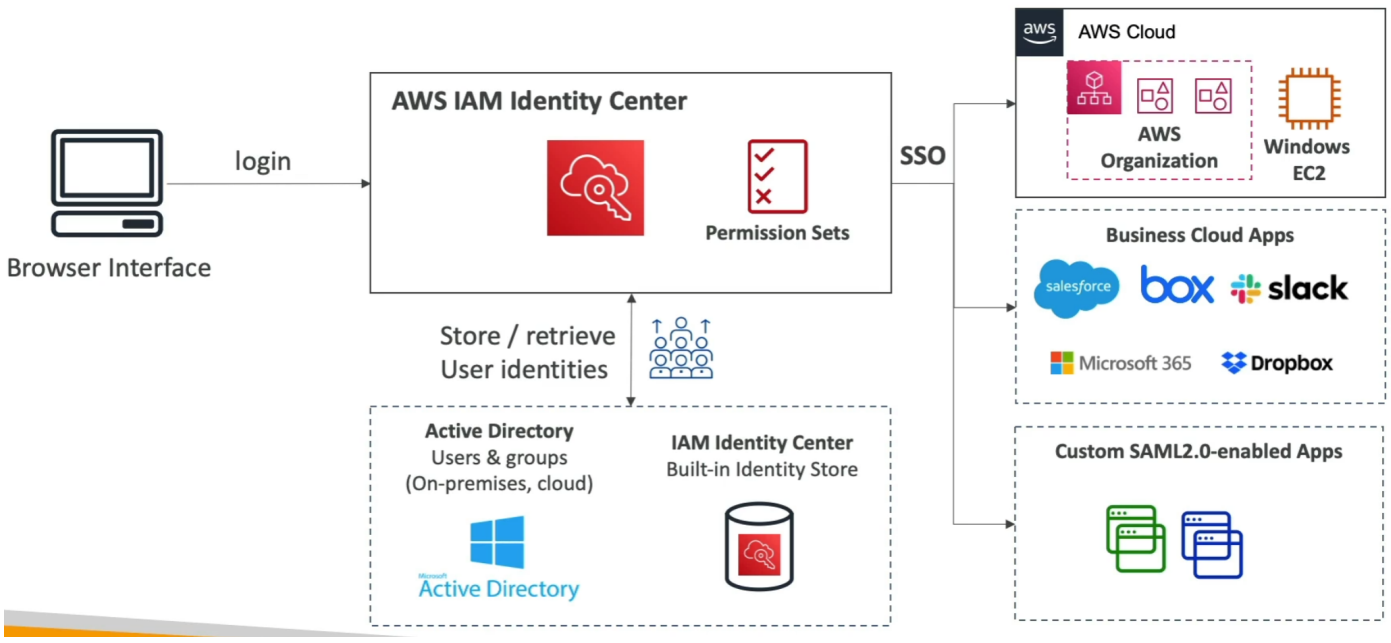
AWS IAM Identity Center (successor to AWS Single Sign-On)

- One login (single sign-on) for all your
  - **AWS accounts in AWS Organizations**
  - Business cloud applications (e.g., Salesforce, Box, Microsoft 365, ...)
  - SAML2.0-enables applications
  - EC2 Windows Instances
- Identity providers
  - Built-in identity store in IAM Identity Center
  - 3rd party: Active Directory (AD), OneLogin, Okta ...

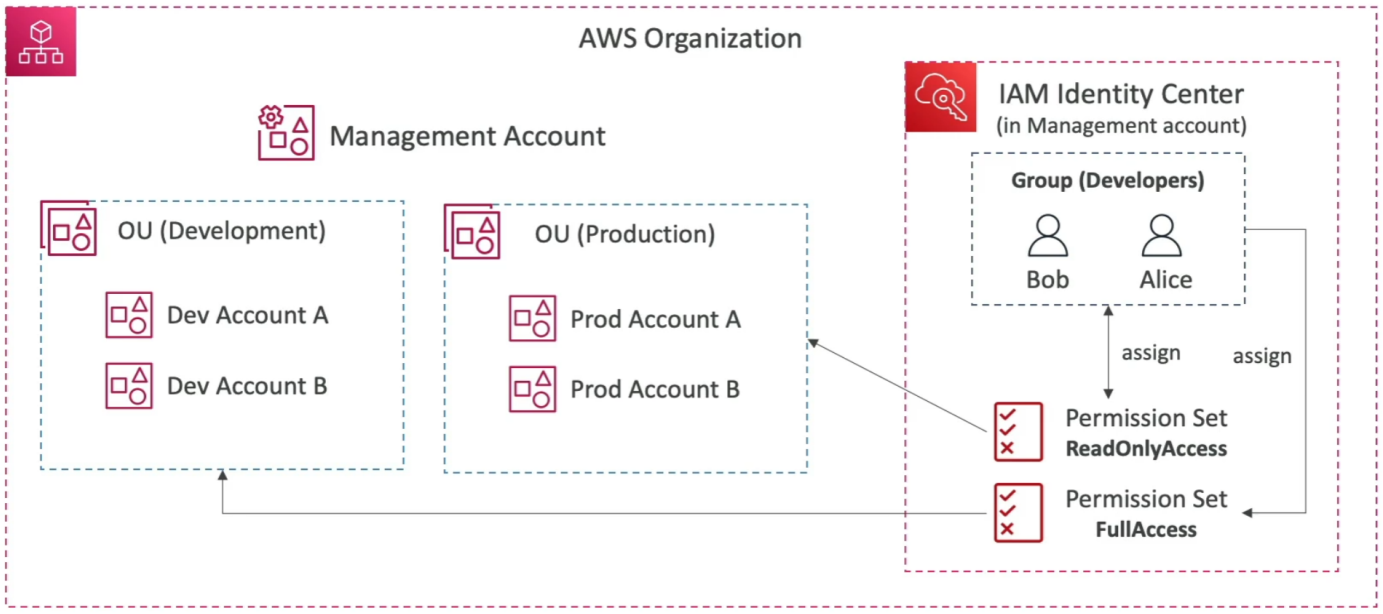
AWS IAM Identity Center - Login Flow



AWS IAM Identity Center



IAM Identity Center

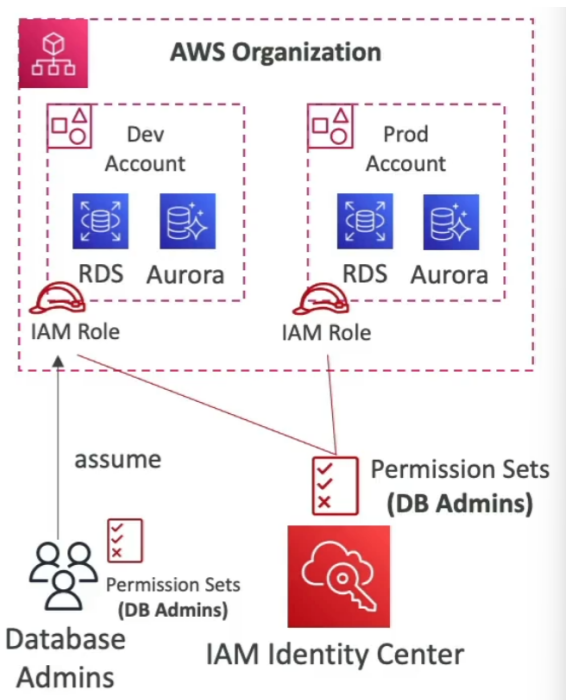


AWS IAM Identity Center Fine-grained Permissions and Assignments

- **Multi-Account Permissions**
  - Manage access across AWS accounts in your AWS Organization
  - Permission Sets - a collection of one or more IAM Policies assigned to users and groups to define AWS access

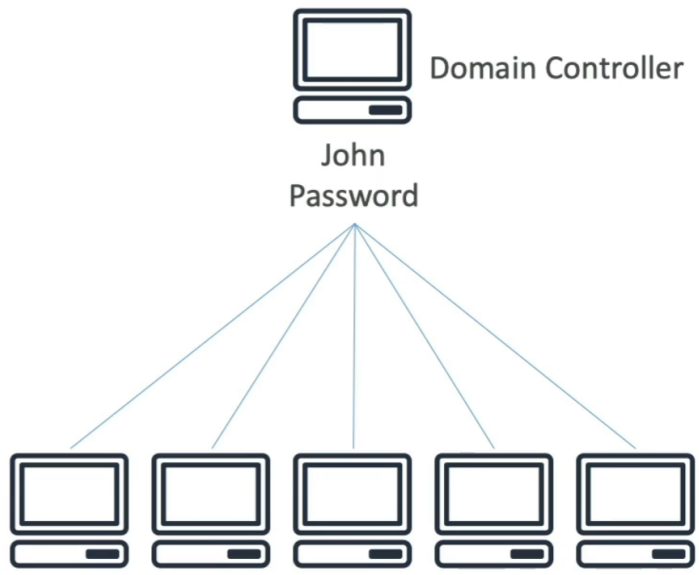
- **Application Assignments**
  - SSO access to many SAML 2.0 business applications (Saleforce, Box, Microsoft 365, ...)
  - Provide required URLs, certificates, and metadata

- **Attribute-Based Access Control (ABAC)**
  - Fine-grained permissions based on users' attributes stored in IAM Identity Center Identity Store
  - Example: cost center, title, locale, ...
  - Use case: Define permissions once, then modify AWS access by changing the attributes



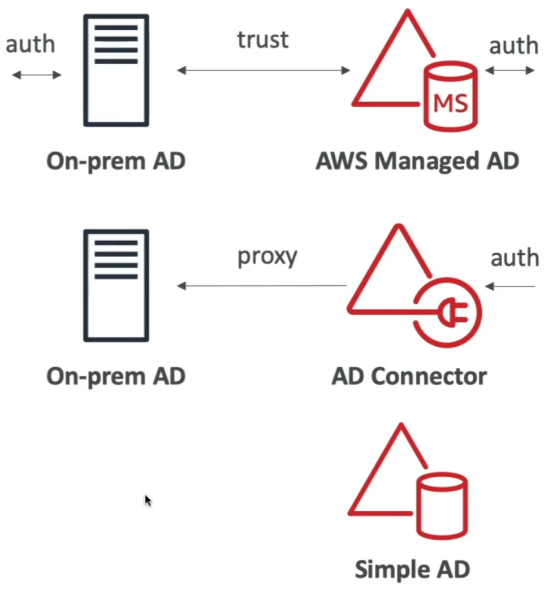
What is Microsoft Active Directory (AD)

- Found on any Windows Server with AD Domain Services
- Database of objects: User Accounts, Computers, Printers, File Shares, Security Groups
- Centralized security management, create account, assign permissions
- Objects are organized in **trees**
- A group of trees is a **forest**



AWS Directory Services

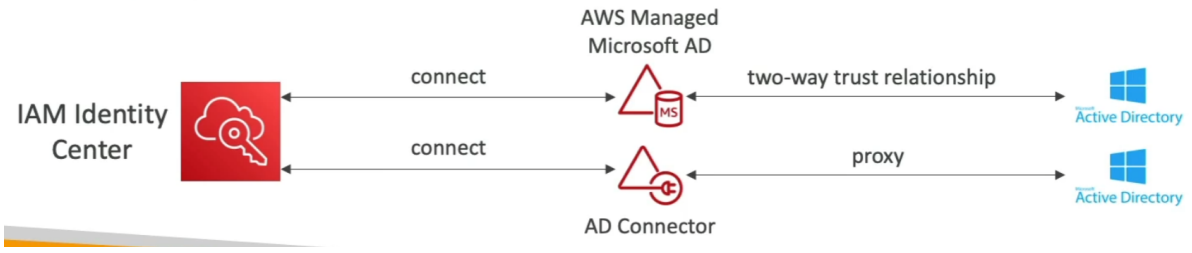
- **AWS Managed Microsoft AD**
  - Create your own AD in AWS, manage users locally, supports MFA
  - Establish "trust" connections with your on-premise AD
- **AD Connector**
  - Directory Gateway(proxy) to redirect to on-premise AD, supports MFA
  - Users are managed on the on-premise AD
- **Simple AD**
  - AD-compatible managed directory on AWS
  - Cannot be joined with on-premise AD



IAM Identity Center - Active Directory Setup

- **Connect to an AWS Managed Microsoft AD (Directory Service)**
  - Integration is out of the box

- **Connect to a Self-Managed Directory**
  - Create Two-way Trust Relationship using AWS Managed Microsoft AD
  - Create an AD Connector



AWS Control Tower

- Easy way to **set up and govern a secure and compliant multi-account AWS environment** based on best practices
- AWS Control Tower uses AWS Organizations to create accounts
- Benefits:
  - Automate the set up of your environment in a few clicks
  - Automate ongoing policy management using guardrails
  - Detect policy violations and remediate them
  - Monitor compliance through an interactive dashboard

AWS Control Tower - Guardrails

- Provides ongoing governance for your Control Tower environment (AWS Accounts)
- **Preventive Guardrail - using SCPs** (e.g., Restrict Regions across all your accounts)
- **Detective Guardrail - using AWS Config** (e.g., identify untagged resources)