

# Gobernanza Integral de infraestructura cloud

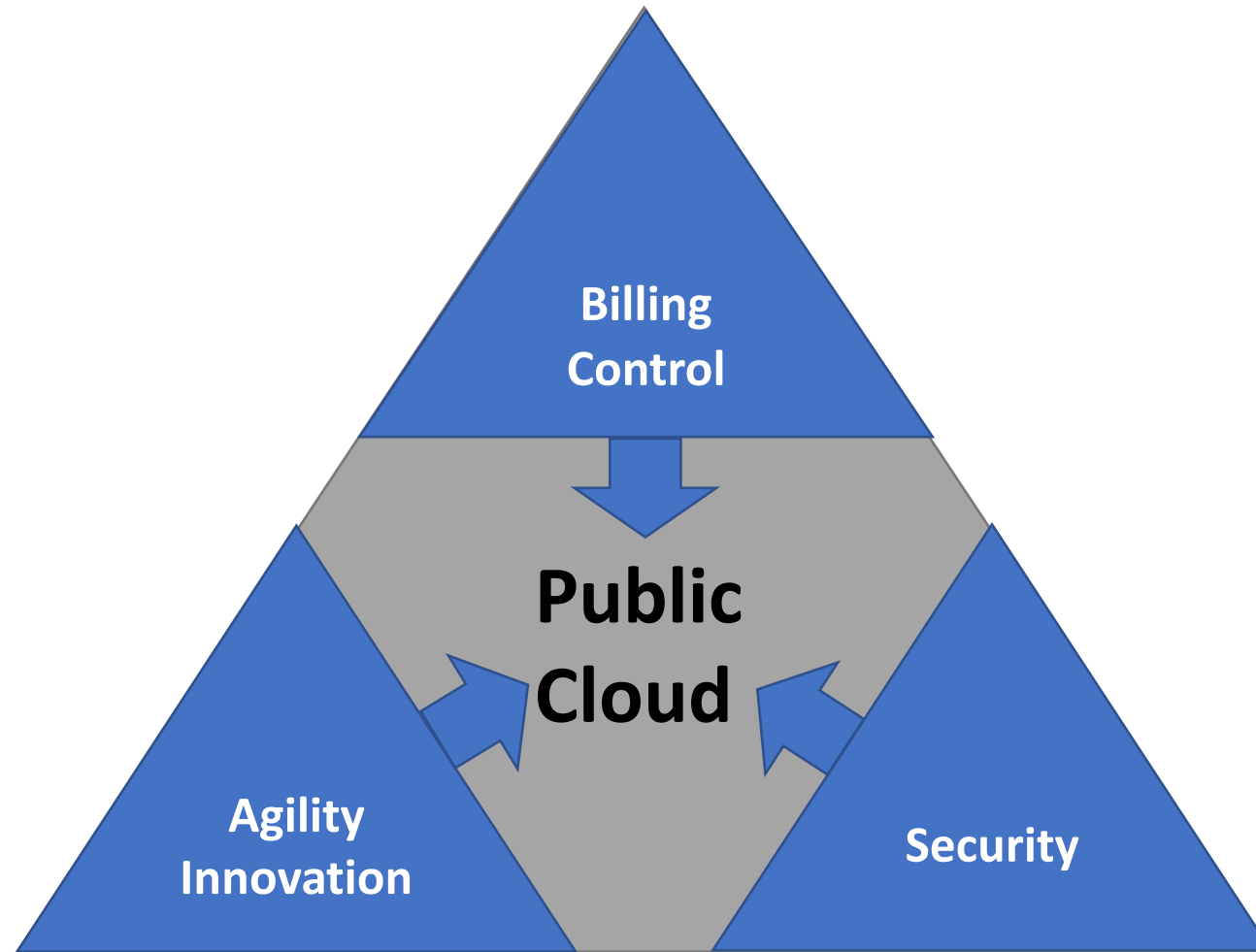


UNIVERSITAT POLITÈCNICA  
DE CATALUNYA  
BARCELONATECH



# Generic Concepts

# Control vs. Innovation/Agility WITH security



# Landing Zone – Cloud Foundations

- BUZZWORD



# AWS Account

- What is an AWS Account?

Pues yo nunca me  
había preguntado eso

g2

g2

# Why Multiaccount

Cost

Policies

Limits

Strict controls  
and Classified  
Data

Different IT  
model

Limit Blast  
Radius

# Why Multiaccount

A solid orange square with the word "Cost" centered inside it in white text.

Cost

# Associate Costs

- Associate costs to a given cost center, be it a Business Unit, a project, an environment, or a product line.
- It's the simpler approach to group costs



# Why Multiaccount



Policies

# Policies

- Each account can implement its own policies for deployable resource types and supported regions.
- Example: Environment have different permissions
  - Sandbox/Test: access to most AWS resources
  - Dev: usually granted most permissions to try and experiment
  - Int/UAT: access to the required teams for validating
  - PRO: only the MSP managing the application has access

# Why Multiaccount



Limits

# Limits

- Accounts have limits for different resource types.
  - For example, the *number of virtual networks* in an account is limited.
- When an account approaches its **hard limit** (one that even the Public Cloud Vendor can not modify), it will be necessary to create another account and deploy new resources there.
- In case of **soft limits**, the CSP can modify the value after the organization requests it via a support case.

# Why Multiaccount

Strict controls  
and Classified  
Data

# Strict Controls

- Impose strict controls and isolation to sensitive or classified data.
- PCI environments

# Why Multiaccount

Different IT  
model

# Different IT models

- Support different IT operating models.
  - Different providers accessing only this application
  - External/third party components accessing the application
  - Tooling that require installing components with high privileges



# Why Multiaccount

Limit Blast  
Radius

# Limit Blast Radius

- Limit the blast radius of an issue impacting other workloads.

# Why Multiaccount

Cost

Policies

Limits

Strict controls  
and Classified  
Data

Different IT  
model

Limit Blast  
Radius

# Keep it controlled

- The more Accounts=>The more complex
  - Permissions
  - Networking
  - Debugging
  - Require centralizing metrics, logs, and traces.
  - Security

## Automatize and apply IaC to control complexity





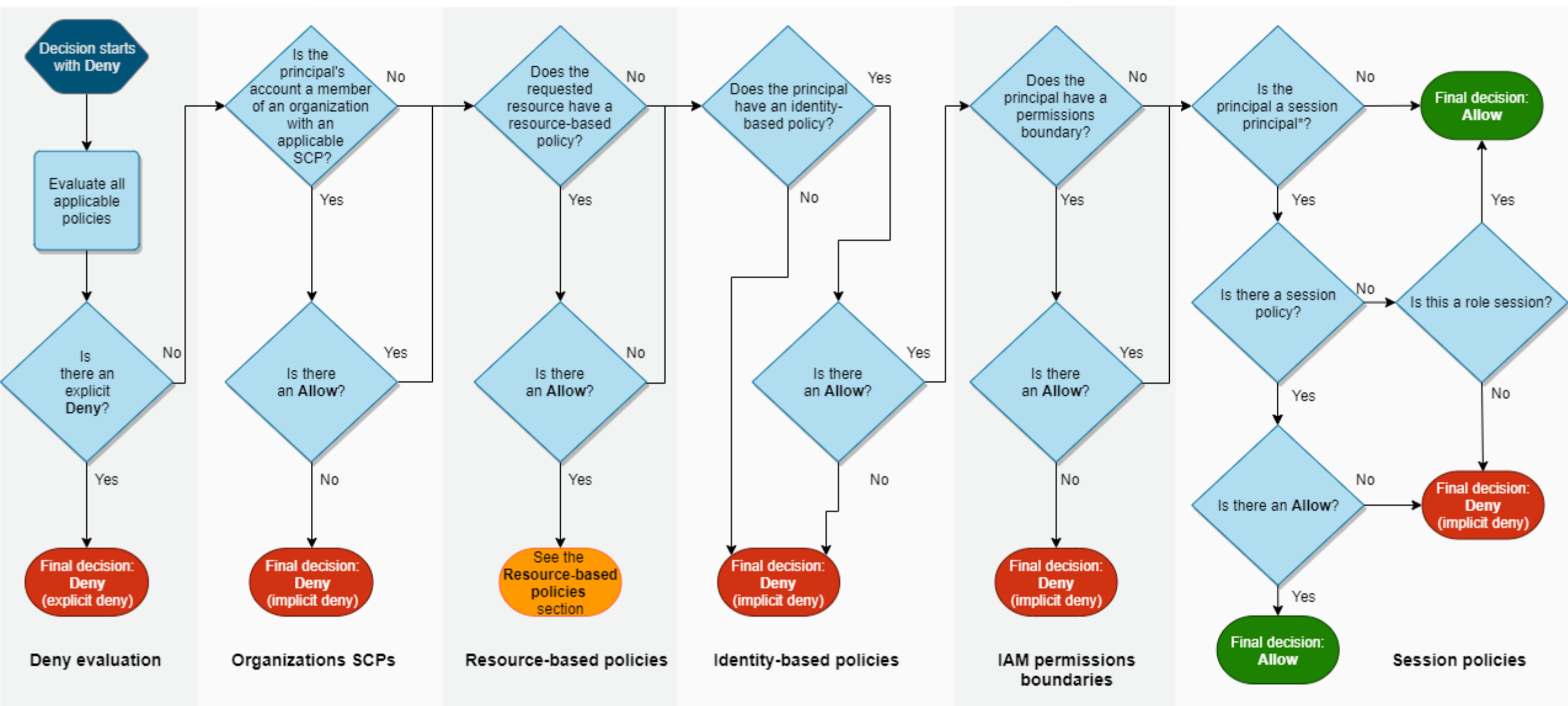
AWS IAM





# AWS IAM Policies

- Service Control Policies (SCP)... wait until the end of the section
- Resource Based Policies *Already known, right?*
- Identity Based Policies *Already known, right?*
- Permissions Boundary *Next slides*
- Session Policies *Already known, right?*

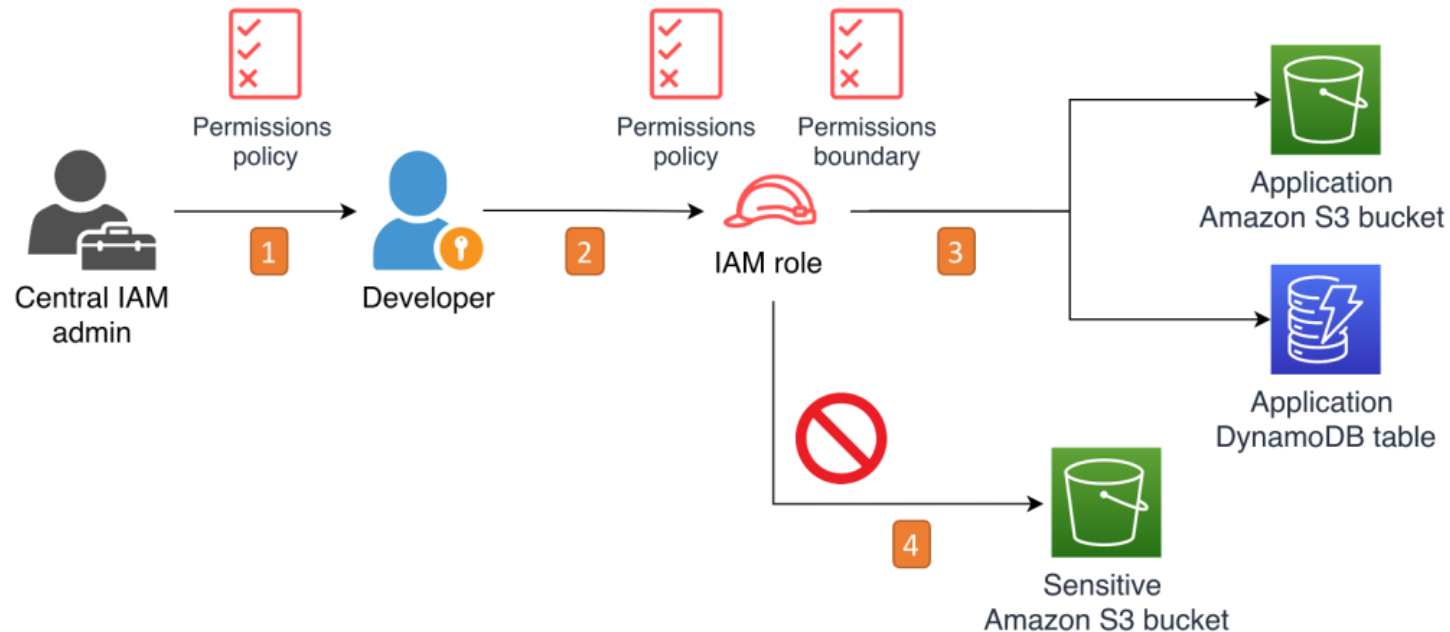


\*A session principal is either a role session or an IAM federated user session.



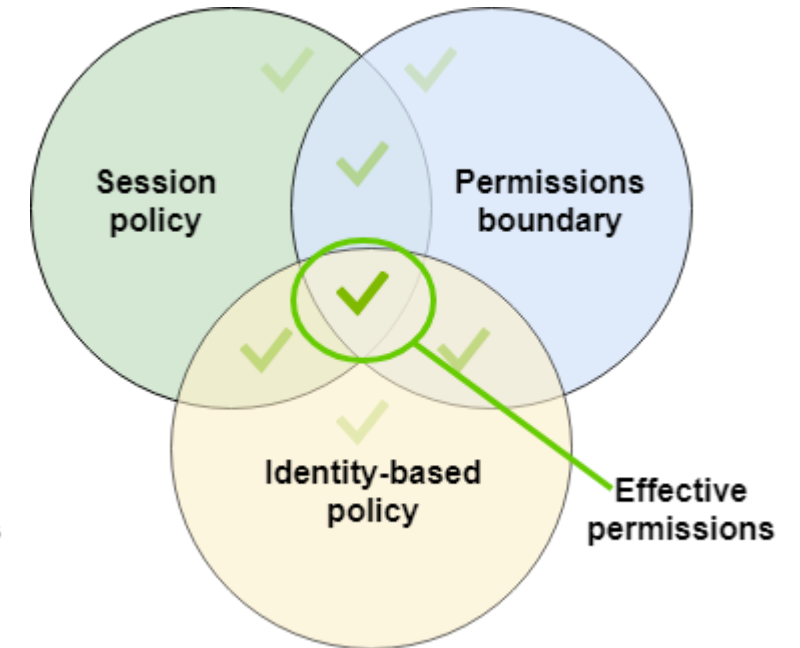
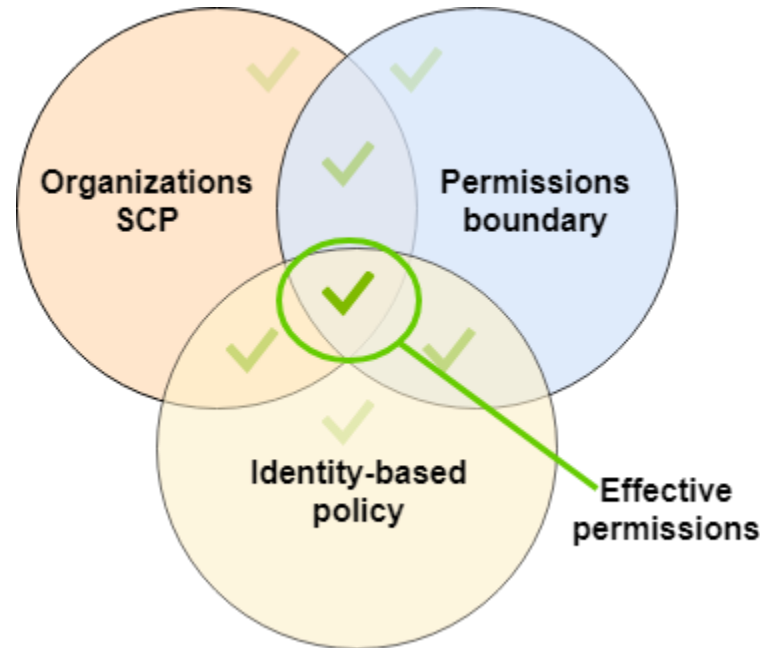
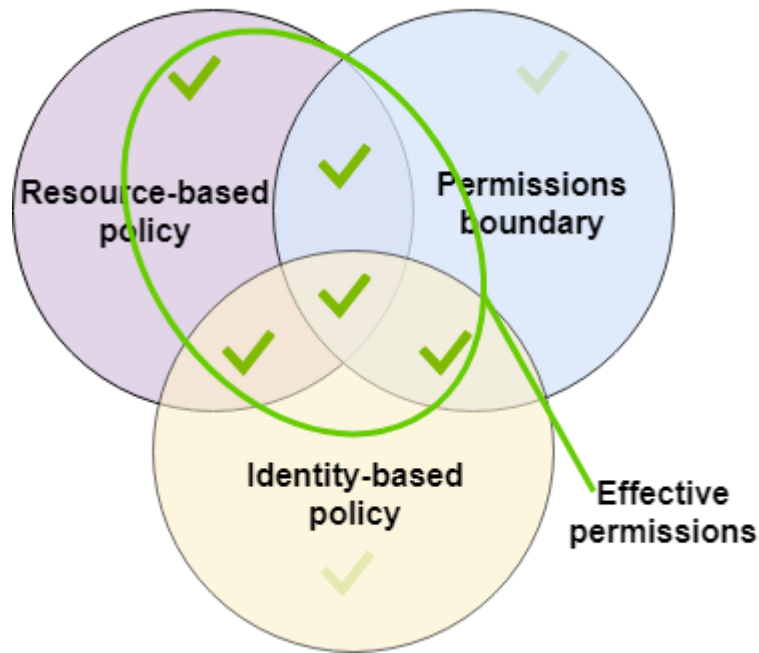
# Permissions Boundaries

- Give agility with control
  - The only tool to delegate the creation of policies and IAM elements with limits (boundaries)



# Boundaries

- Permissions boundaries set the limit of allowed permissions
- DO NOT GRANT permissions



# Avoid security breaches

- Permissions Boundary policy must have a condition: to force including the permissions boundary in the newly created IAM policies to avoid escalating privileges by using the **Condition** element:

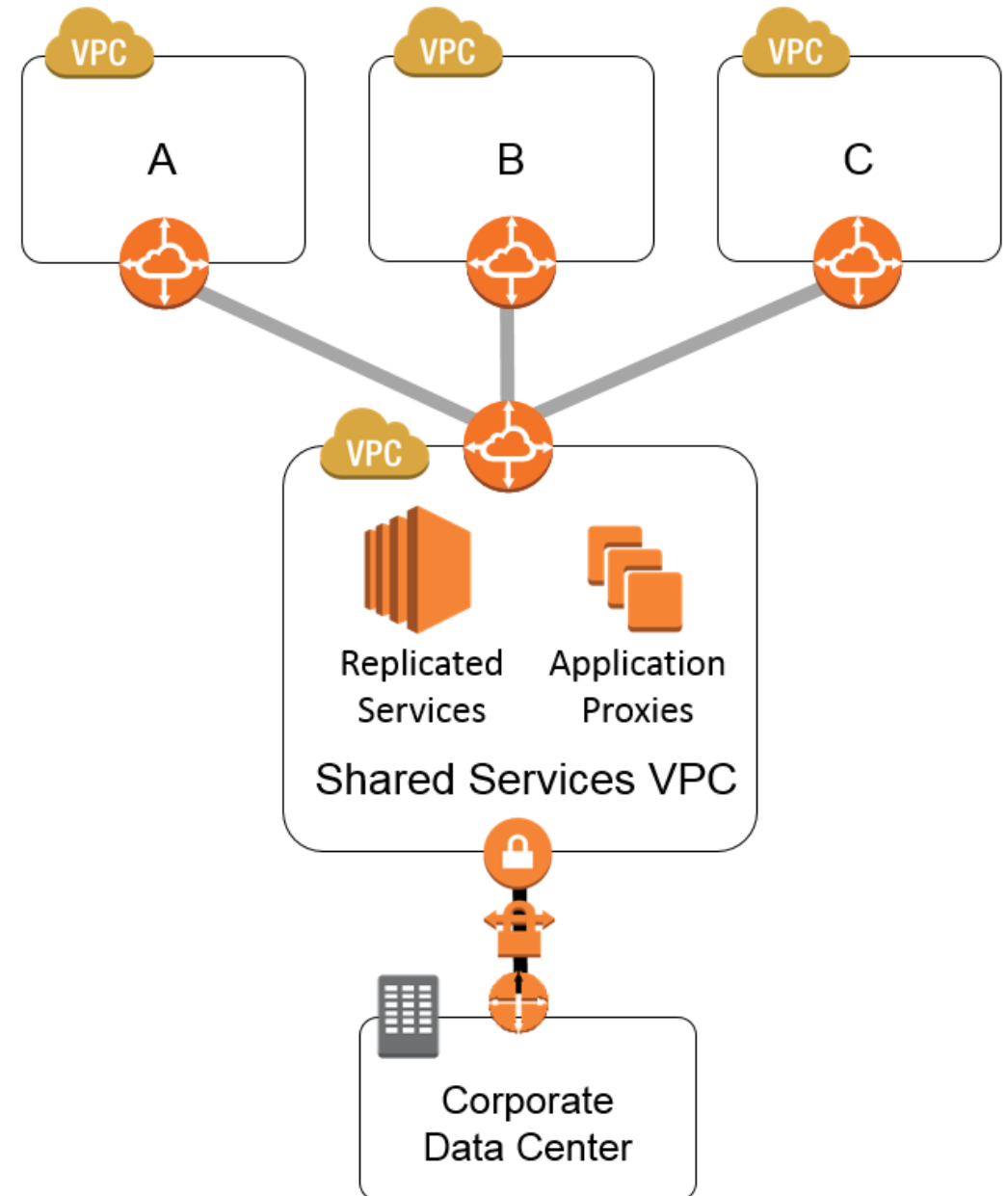
```
"Condition": {  
  "StringEquals": {  
    "iam:PermissionsBoundary": [  
      "arn:aws:iam::<YourAccount_ID>:policy/PermissionsBoundaryFunctionA",  
      "arn:aws:iam::<YourAccount_ID>:policy/PermissionsBoundaryFunctionB"  
    ]  
  }  
}
```



Networking

# Hub And Spoke

- Central Networking Hub  
interconnecting to outside world
  - Central point terminating VPNs and Direct Connect
  - Peering/Transit GW/VPNs connecting to the rest of AWS Accounts

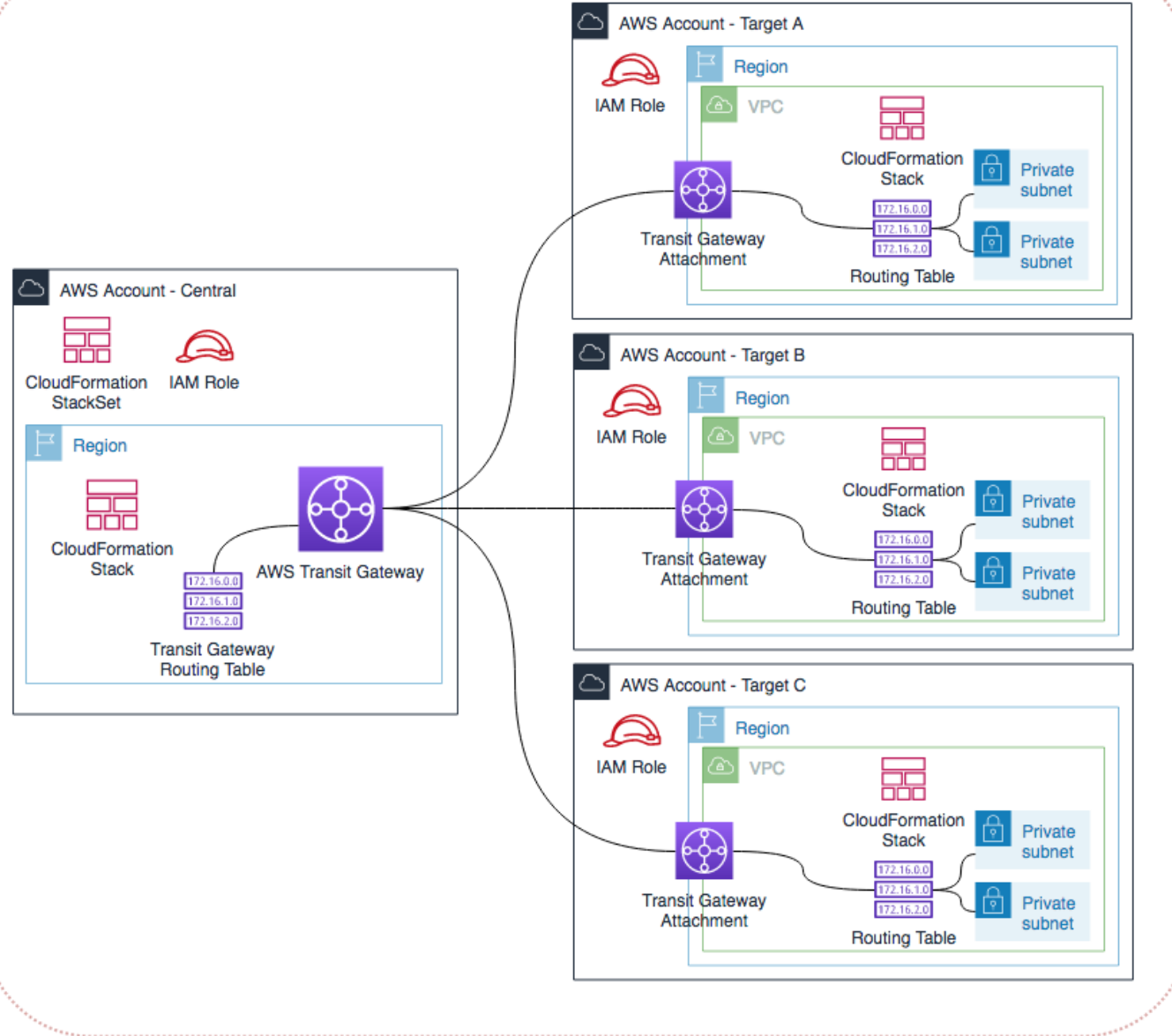


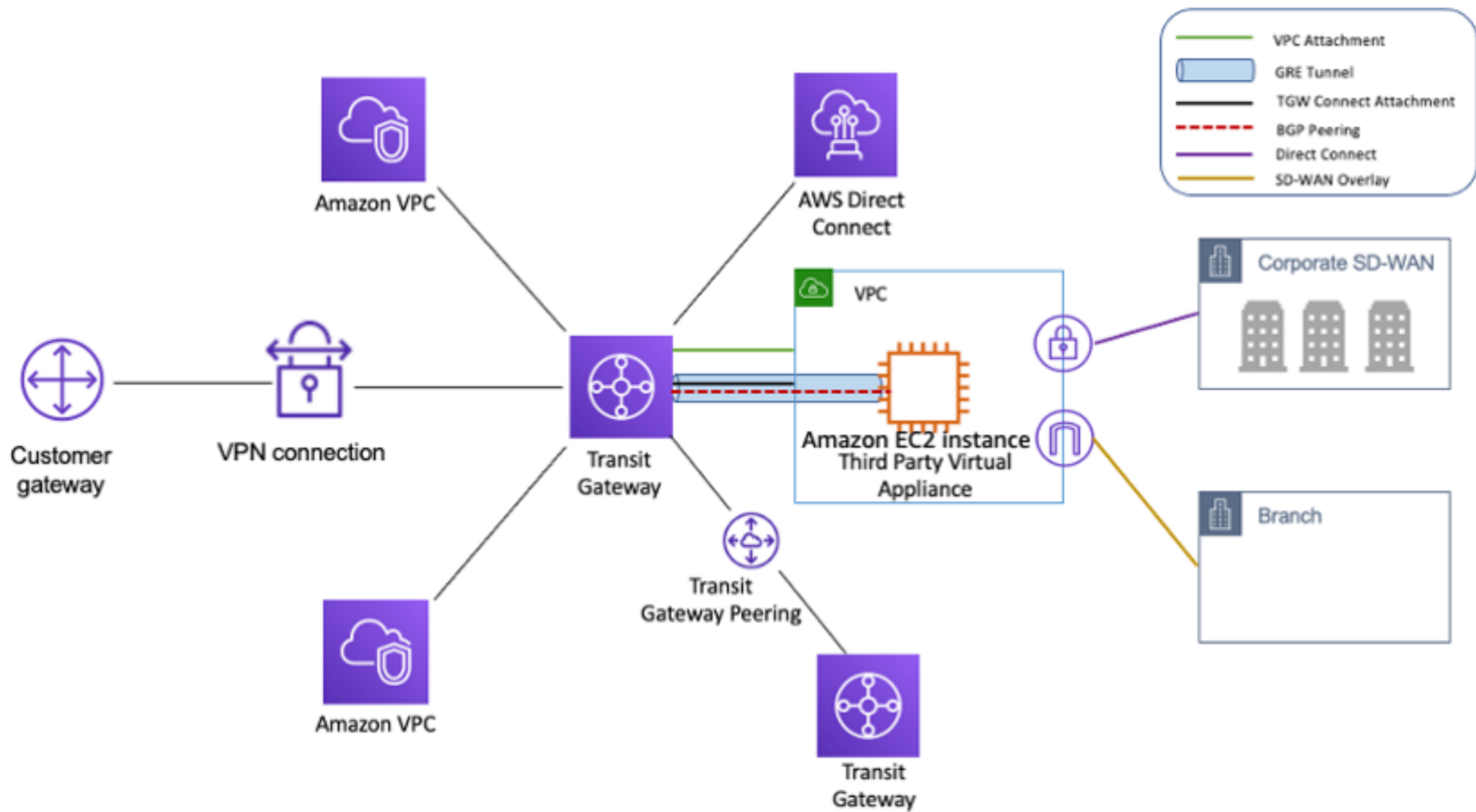
# Advanced Topologies

- Transit GW with VPCs for:
  - Egress
    - Reduce the number of NAT GWS
    - Apply controls to outbound flows
  - Ingress
    - Exposing only required public endpoints
    - Use native services like WAF
  - Inspection
    - Apply AWS Firewall or NVAs for traffic filtering and inspection

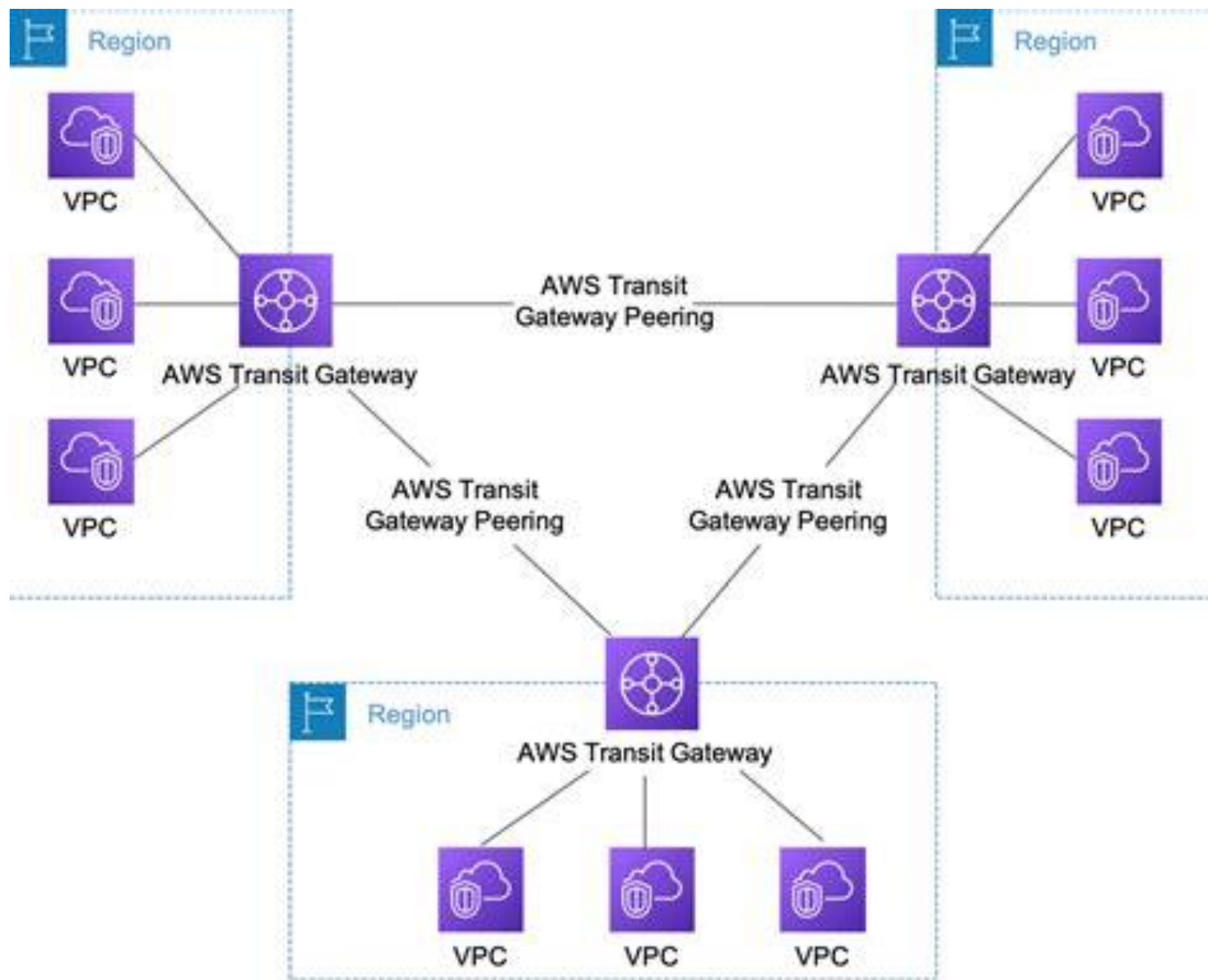


AWS Organization

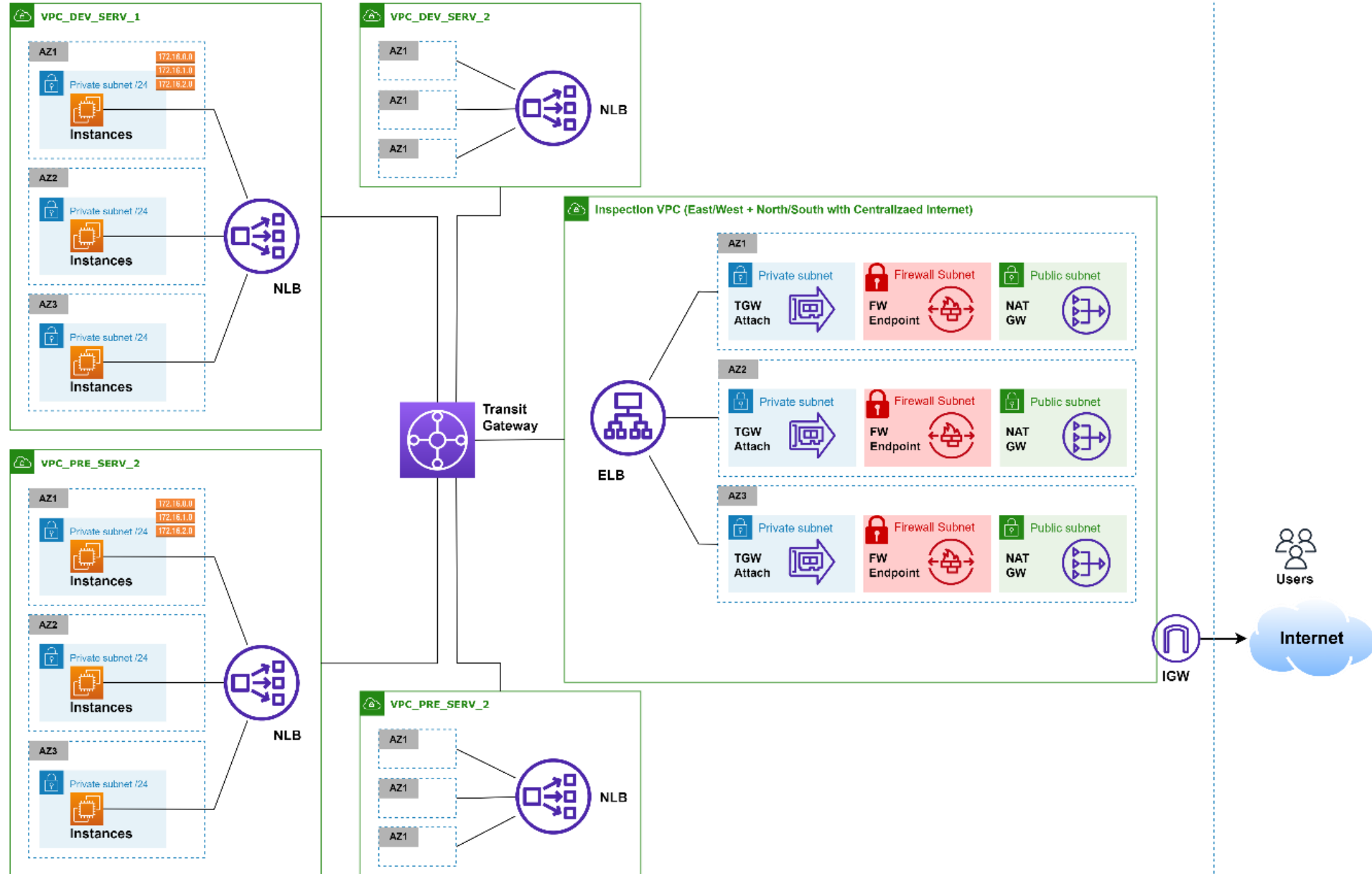








Region: Europe (Ireland) eu-west-1





AWS Config

# AWS Config

- Dynamic CMDB that discovers AWS resources in accounts and registers all configuration changes.
- Rules can then be applied to the CMDB to discover compliant and non compliant components
- Configuration changes are recorded in S3 buckets and can be streamed to SNS or Cloudwatch.
- Compliance information can be summarized under a Dashboard

# AWS Config - features

- AWS Config can be applied to one or several accounts and be visualized separately or aggregated on only one account.
- Same rules or different can be applied to the accounts
- Not all resources are currently supported by AWS Config. Supported list in <https://docs.aws.amazon.com/config/latest/developerguide/resource-config-reference.html>
- New AWS regions and their components can be automatically discovered when added by AWS

# Dynamic CMDB

## Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for supported global resources in this region.

### All resources

- ☐ Record all resources supported in this region ⓘ
- ☐ Include global resources (e.g., AWS IAM resources) ⓘ

### Specific types

No resource types have been selected.

### Data retention period

### Amazon S3 bucket

Your bucket receives configuration history and configuration snapshots, which contain details for the resources that AWS Config records.

☐ Create a bucket

#### ACM

Certificate

#### AutoScaling

AutoScalingGroup









LaunchConfiguration

ScalingPolicy

ScheduledAction

AWS config will record all components and the actions (delete/add/update) on all the supported components or specific type mentioned.

# Dynamic CMDB

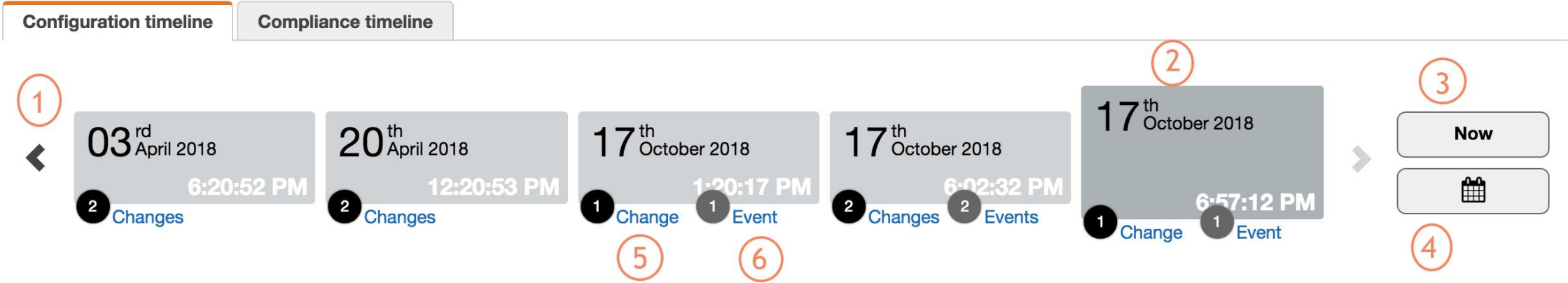
Resources	
Total resource count	50
Top 10 resource types	Total
 EC2 SecurityGroup	13
 EC2 Subnet	12
 EC2 RouteTable	9
 EC2 VPC	4
 EC2 NetworkAcl	4
 EC2 InternetGateway	2
 EC2 Instance	1
 AutoScaling LaunchConfiguration	1

- CMDB shows all the components (resources) that have been discovered by Config
- All the components will be evaluated against matching rules
- Modifications done on those components will be dynamically reflected

# S3 Bucket bucketname

on October 18, 2018 3:21:50 PM Pacific Daylight Time (UTC-07:00)

Manage resource



Configuration Details

View Details

Amazon Resource Name	arn:aws:s3:::bucketname	Owner ID	abcd1234abcd1234abcd1234abcd1234abcd1234
Resource type	AWS::S3::Bucket	Requester pays	false
Resource ID	bucketname	Access control list	<a href="#">View bucket ACL</a>
Resource name	bucketname	Bucket policy	<a href="#">View bucket policy</a>
Availability zone	Regional	CORS	null

Relationships

4

Changes

4



# Rules

- AWS provides ~326 managed rules but custom rules can be defined to match specific cases.
- Rule examples:
  - Component should have at least the tags “cost” and “owner”
  - Volumes should be encrypted
- Rules are periodically applied to CMDB components (frequency can be defined) or when their configuration changes
  - Configuration changes
  - Periodic
  - Hybrid
- Rules are evaluated using type of resource (ej: EC2) or tag value (ej: owner=Samuel) as matching criterias.

# Rules – Evaluation modes

- **Proactive**

- Actively evaluate resources that are not yet deployed.

<https://aws.amazon.com/about-aws/whats-new/2022/11/aws-config-rules-support-proactive-compliance/>

- **Detective**

- “Standard” scheduled or periodic resource evaluation

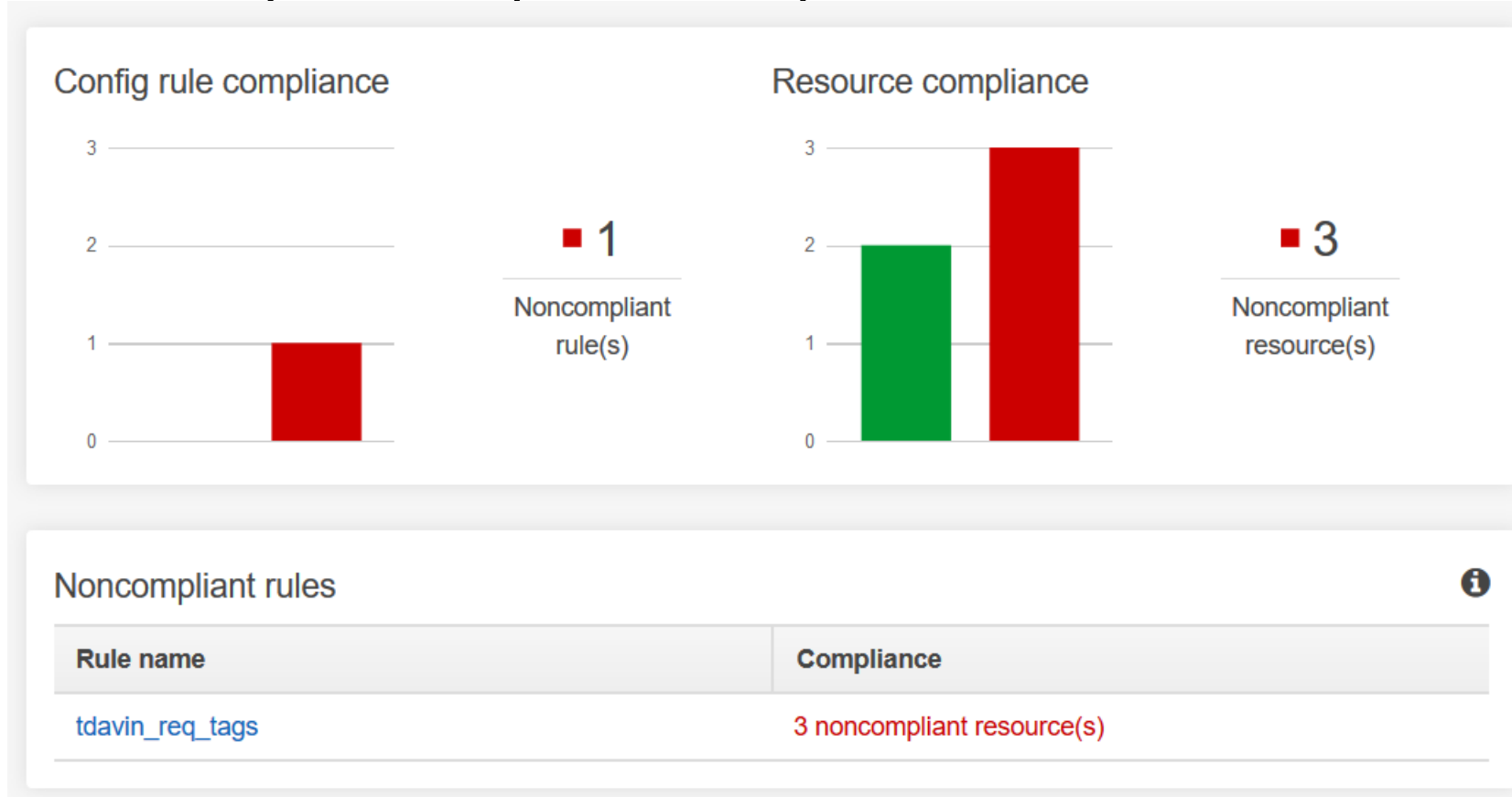
# Conformance Packs

- Collection of AWS Config Rules that follows best practices and recommendations.
- Provided by AWS or custom created (YAML file containing list of rules)

<https://docs.aws.amazon.com/config/latest/developerguide/conformancepack-sample-templates.html>

# Compliance Dashboard

- AWS provides a simple dashboard stating the number of compliant rules and components (resources)



# Configuration changes storage

- S3 bucket is always required to store configuration changes
- As an option, configuration changes can be streamed:
  - SNS Topic
  - Cloudwatch event

## Amazon SNS topic

---

- ☐ Stream configuration changes and notifications to an Amazon SNS topic.

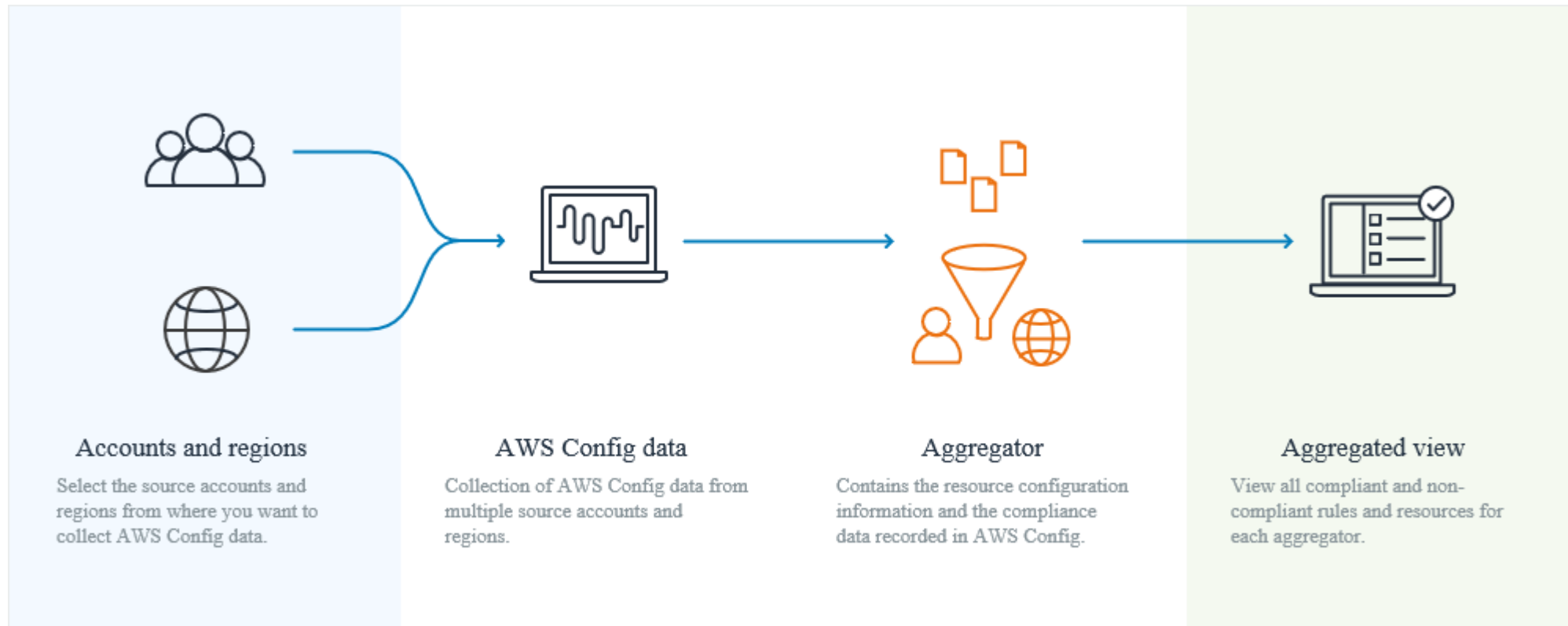
## Amazon CloudWatch Events rule

---

AWS Config sends detailed information about the configuration changes and notifications to Amazon CloudWatch Events. To create rules, visit the [Step 1: Create Rule](#) page in the Amazon [CloudWatch Events](#) console.

# Aggregated views - multiaccount

- Allows to aggregate Configuration changes from several accounts



# Aggregated views - multiaccount

- Accounts can be part of an AWS organization or can be named one by one
- CMDB will record components of all accounts, apply specific account rules on each account and display the results
- Config and rule definition can be parametrized using cloudformation so that every account gets the same

# Costs

- \$0.003 per configuration item recorded in an AWS account per AWS Region. No added fees for maintaining the CMDB
- Charged based on the number of evaluations of Config Rules:

AWS Config rules evaluations	Price
First 100,000 rule evaluations	\$0.001 per rule evaluation per region
Next 400,000 rule evaluations (100,001-500,000)	\$0.0008 per rule evaluation per region
500,001 and more rule evaluations	\$0.0005 per rule evaluation per region

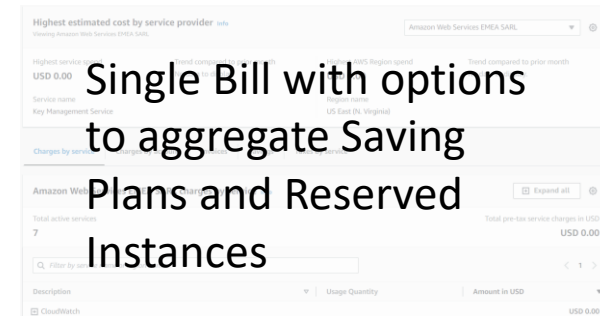
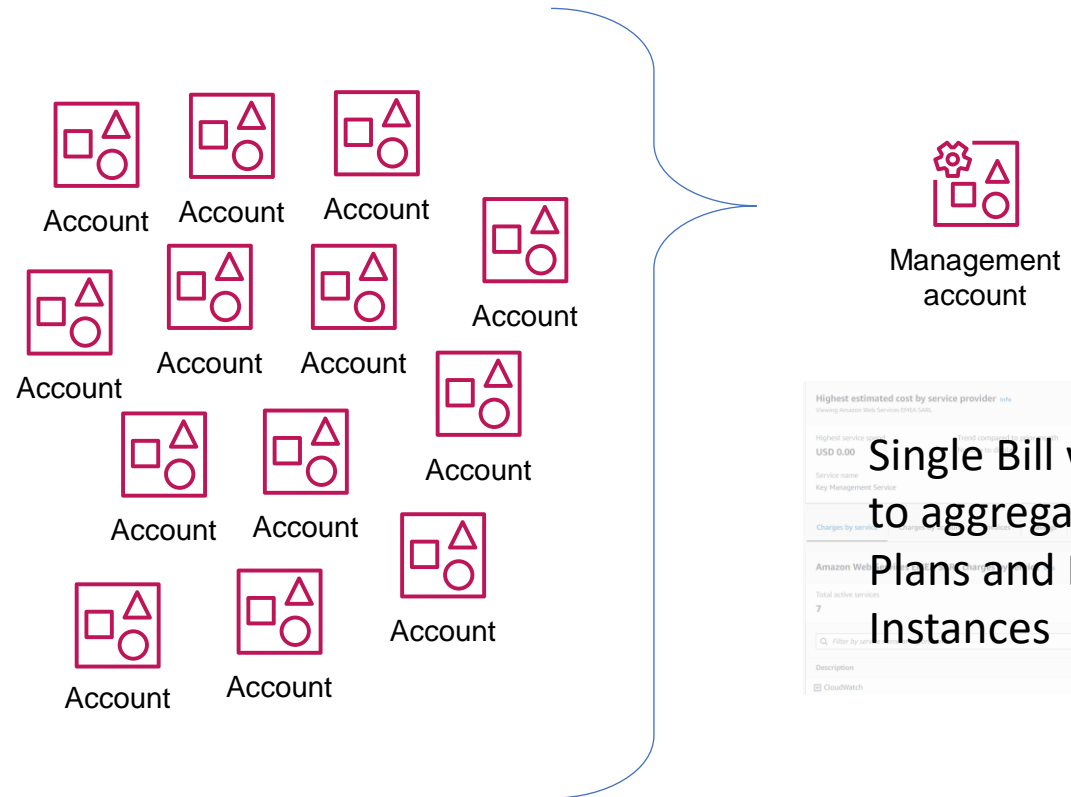




# AWS Organizations

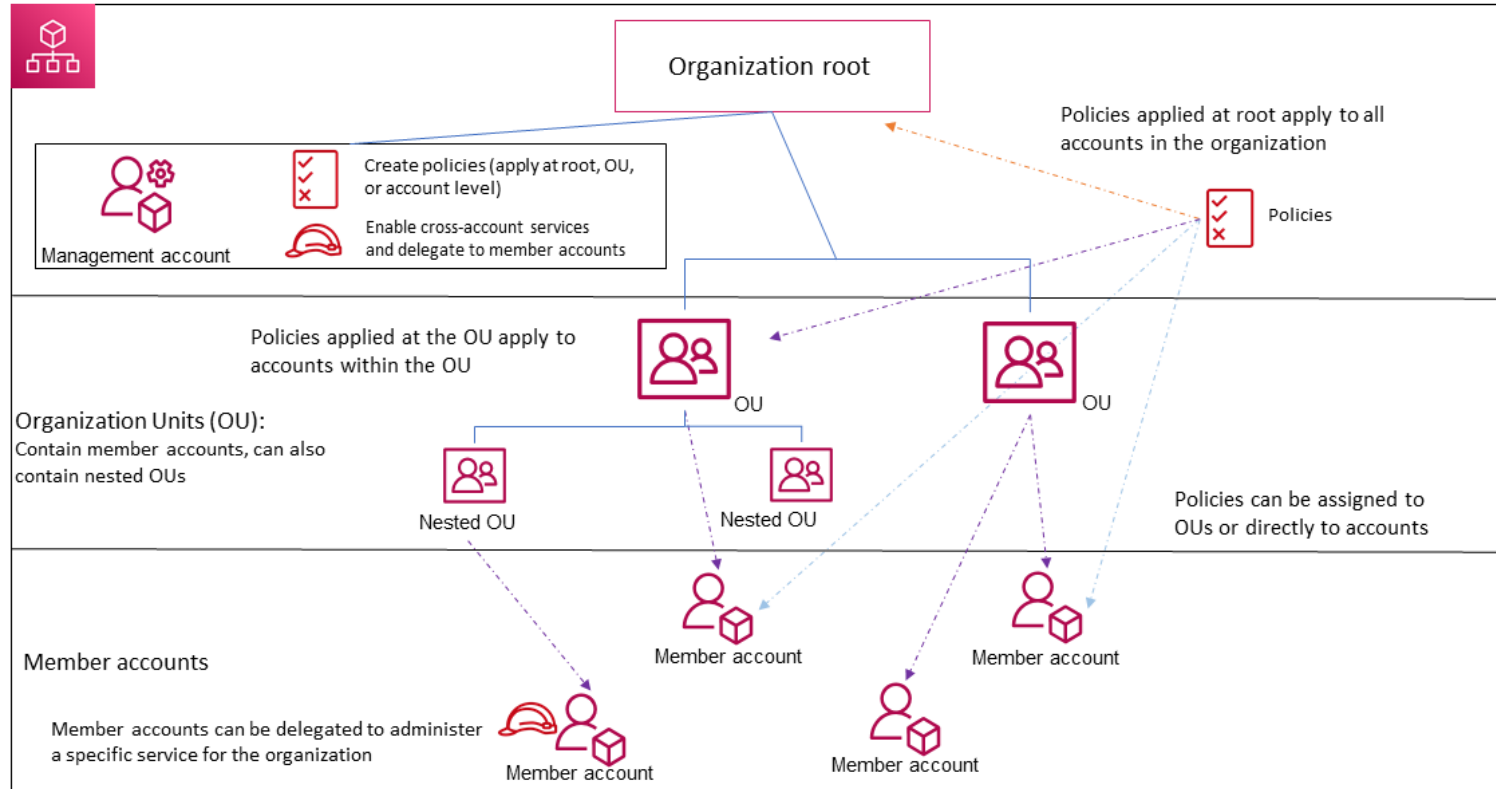
# AWS Organizations

- **Centralized billing**
- Account hierarchy
  - Organizational Units (OUs)
- Policies
  - Service Control Policies (SCP)
  - Tag
  - Backup
  - AI



# AWS Organizations

- Centralized billing
- **Account hierarchy**
  - Organizational Units (OU)
- Policies
  - SCP
  - Tag
  - Backup
  - AI



# OUs

- Limits: 5 nested OUS under the root
  - Recommend to keep it between 2 or 3 to limit complexity (inheritance and maintaining effective policies and permissions)

# AWS Organizations

- Centralized billing
- Account hierarchy
  - OUs
- **Policies**
  - SCP
  - Tag
  - Backup
  - AI

Supported policy types	
Policy type	Status
<b>AI services opt-out policies</b> Artificial Intelligence (AI) services opt-out policies enable you to control whether AWS AI services can store and use your content. <a href="#">Learn more</a>	⊖ Disabled
<b>Backup policies</b> Backup policies enable you to deploy organization-wide backup plans to help ensure compliance across your organization's accounts. Using policies helps ensure consistency in how you implement your backup plans. <a href="#">Learn more</a>	✔ Enabled
<b>Service control policies</b> 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. <a href="#">Learn more</a>	✔ Enabled
<b>Tag policies</b> Tag policies help you standardize tags on all tagged resources across your organization. You can use tag policies to define tag keys (including how they should be capitalized) and their allowed values. <a href="#">Learn more</a>	⊖ Disabled

# SCPs

- Why?
  - Central management of policies along the whole organization
  - **Affect to root IAM user of AWS Accounts**



Products

Solutions

Resources

Plans & Pricing

Schedule

Join

Host ▾

User: arn:aws:iam::[REDACTED]user/web\_user is not authorized to perform: dynamodb:Query on resource: arn:aws:dynamodb:us-east-1:[REDACTED]:table/us06\_ZMWEB\_OAUTH\_APPROVAL with an explicit deny in a service control policy (Service: AmazonDynamoDBv2; Status Code: 400; Error Code: AccessDeniedException; Request ID: SABH7J7J5UK4I4L8EHTG90JPMNVV4KQNSO5AEMVJF66Q9ASUAAJG; Proxy: null) (-1)

- Some organizations, but few, have a mirror-like Ous/subscriptions hierarchy to try changes, because there is no audit or “what-if” test scenario provided by AWS: **changes are automatically applied.**

# SCP best practices

- General examples
  - Deny access to AWS based on the requested AWS Region
  - Prevent IAM users and roles from making certain changes
  - Prevent IAM users and roles from making specified changes, with an exception for a specified admin role
  - Require MFA to perform an API action
  - Block service access for the root user
  - Prevent member accounts from leaving the organization
- Example SCPs for Amazon CloudWatch
  - Prevent users from disabling CloudWatch or altering its configuration
- Example SCPs for AWS Config
  - Prevent users from disabling AWS Config or changing its rules
- Example SCPs for Amazon Elastic Compute Cloud (Amazon EC2)
  - Require Amazon EC2 instances to use a specific type
- Example SCPs for Amazon GuardDuty
  - Prevent users from disabling GuardDuty or modifying its configuration
- Example SCPs for AWS Resource Access Manager
  - Preventing external sharing
  - Allowing specific accounts to share only specified resource types
  - Prevent sharing with organizations or organizational units (OUs)
  - Allow sharing with only specified IAM users and roles
- Example SCPs for Amazon Route 53 Application Recovery Controller
  - Prevent users from updating Route 53 ARC routing control states

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DenyAllOutsideEU",
      "Effect": "Deny",
      "NotAction": [
        "acm:*",
        "aws-marketplace-management:*",
        "aws-marketplace:*",
        "aws-portal:*",
        "budgets:*",
        "cc:*",
        "chime:*",
        "cloudfront:*",
        "config:*",
        "cur:*",
        "directconnect:*",
        "ec2:DescribeRegions",
        "ec2:DescribeTransitGateways",
        "ec2:DescribeVpnGateways",
        "es:*",
        "globalaccelerator:*",
        "health:*",
        "iam:*",
        "importexport:*",
        "iis:*",
        "mobileanalytics:*",
        "networkmanager:*",
        "organizations:*",
        "pricing:*",
        "route53:*",
        "route53-recovery-cluster:*",
        "route53-recovery-control-config:*",
        "route53-recovery-readiness:*",
        "s3:GetAccountPublic*",
        "s3:ListAllMyBuckets",
        "s3:ListMultiRegionAccessPoints",
        "s3:PutAccountPublic*",
        "shield:*",
        "sts:*",
        "support:*",
        "trustedadvisor:*",
        "waf-regional:*",
        "waf:*",
        "wafv2:*",
        "wellarchitected:*"
      ],
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": [
            "eu-central-1",
            "eu-west-1"
          ]
        }
      },
      "ArnNotLike": {
        "aws:PrincipalARN": [
          "arn:aws:iam::*:role/RoletAllowedToBypassThisSCP",
          "arn:aws:iam::*:role/RoletAllowedToBypassThisSCP"
        ]
      }
    }
  ]
}
```

WHY?

```
"Resource": "*",
"Condition": {
  "StringNotEquals": {
    "aws:RequestedRegion": [
      "eu-central-1",
      "eu-west-1"
    ]
  }
},
```

# SCP in real life

- Limitation of 5 SCP attached to an OU
  - Recommended to review policy JSON to group permissions into the same file.

Policy type	Minimum attached to an entity	Maximum attached to root	Maximum attached per OU	Maximum attached per account
Service control policy	1 — Every entity must have <i>at least</i> one SCP attached at all times. You can't remove the last SCP from an entity.	5	5	5
AI services opt-out policy	0	5	5	5
Backup policy	0	10	10	10
Tag policy	0	10	10	10



# Delegation of permissions

- AWS Organization Manage Account must be exclusively used only when required

## **Selected Timeline of Relevant Releases**

- 2006: AWS began offering IT infrastructure services.
- May 2011: AWS launched Identity and Access Management (IAM).
- February 2017: AWS Organizations generally available.
- October 2020: Amazon GuardDuty Delegated Administrator.
- February 2021: CloudFormation StackSets delegated administration.
- November 2022: Delegated Administrator via Delegation Policies Release.

[https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_integrate\\_services\\_list.html?icmpid=docs\\_orgs\\_console](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_integrate_services_list.html?icmpid=docs_orgs_console)



# AWS Organizations pricing

- AWS Organization is a **Free** service, only incurring **costs of auxiliary resources** like S3 buckets or AWS Config evaluations.



# Greenfield vs. Brownfield

- “It’s possible to include (*invite*) existing accounts into an AWS Organization **BUT**
  - Be careful with resources dependencies, policies being applied, and network topology
  - In order to provide a reliable and secure environment, usually **take-over entails creating new Organizations Accounts and redeploying resources** (most times it’s a good opportunity to apply the latest IaC processes and technologies as well as clean-up).

# Lab Time

- Align OUs and accounts
- Apply SCPs to OUs



# AWS Control Tower

# Control Tower

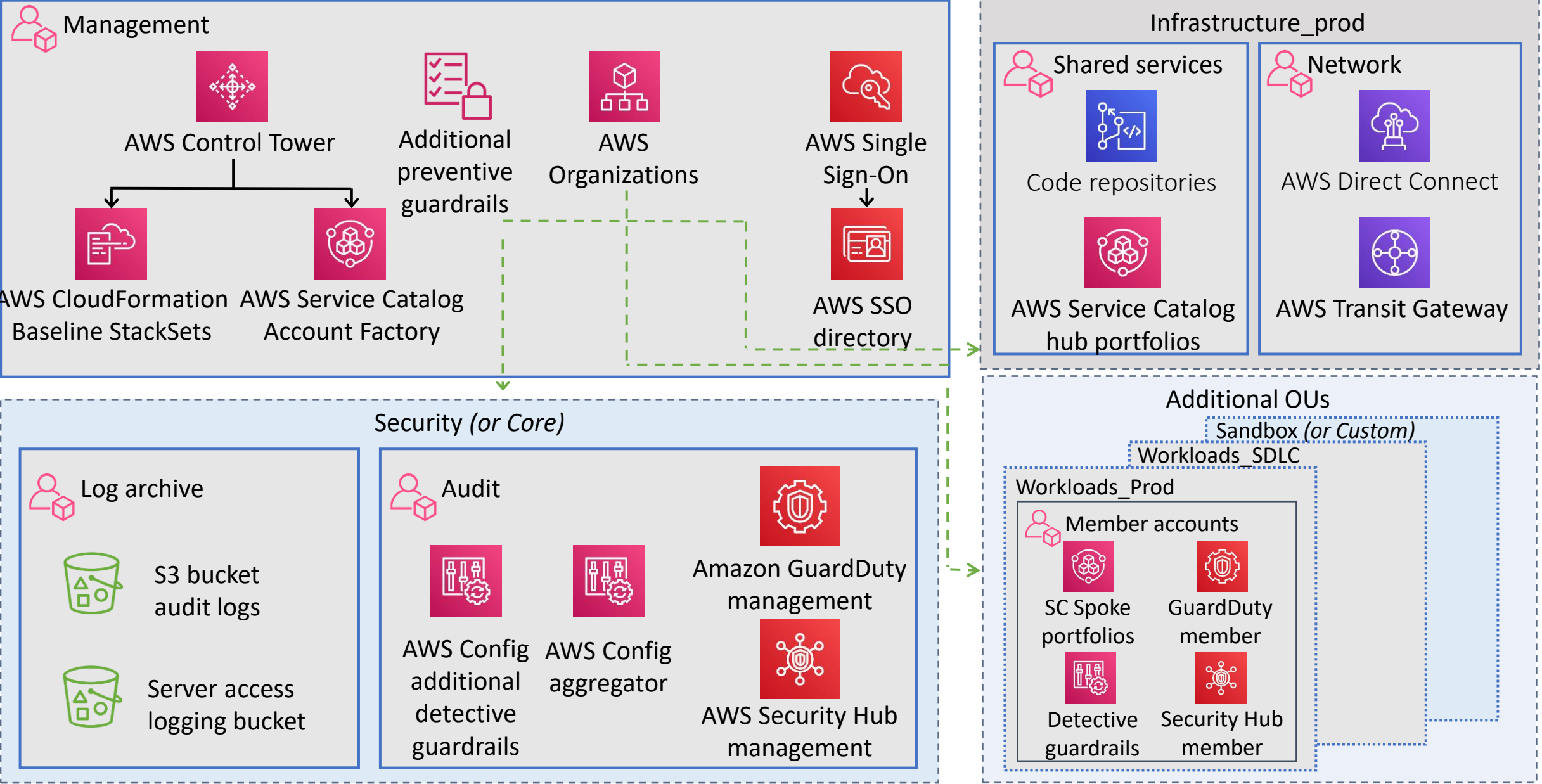
- Service leveraging AWS Organizations, SCPs, and AWS Config
- Applies best practices from industry
  - Account Structure
  - Guardrails and controls
- Cross Account permissions already setup
  - Centralize logging from AWS CloudTrail, and
  - AWS Config stored in Amazon Simple Storage Service (Amazon S3).
- Account Creation factory
- Dashboard presenting
  - Provisioned accounts
  - Controls enabled
  - Noncompliant resources

# Best practices for AWS Account

- Root account with no resources deployed
  - Those minimum that can not be delegated
- An account for audit purposes
- An account for centralizing network interconnection
- An account for shared services like AD, monitoring, CI/CD...

Control Tower Creates an OU *Security* with two Accounts *Log Archive*, and *Audit*. Optionally it can create a *Sandbox* OU.

# Landing zone reference architecture





# AWS Recommended OUs



## AWS Organization OUs



Sandbox



Workloads



Policy  
Staging



Suspended



Individual  
Business  
Users



Exceptions



Deployments



Transitional



Business  
Continuity

### Foundational OUs



Security



Infrastructure

# Control type (Guardrails)

Preventive

Detective

Proactive

# Preventive Controls (Guardrails)

- A preventive control ensures that your accounts **maintain compliance**, because it disallows actions that lead to policy violations. The status of a preventive control is either **enforced** or **not enabled**. Preventive controls are supported in all AWS Regions.
- Usually implemented as **SCP**

# Detective Controls (Guardrails)

- A detective control **detects noncompliance** of resources within your accounts, such as policy violations, and provides alerts through the dashboard. The status of a detective control is either **clear**, **in violation**, or **not enabled**. Detective controls apply only in those AWS Regions supported by AWS Control Tower.
- Usually implemented via **AWS Config Rules**

# Proactive Controls (Guardrails)

- A proactive control **scans your resources before they are provisioned** and makes sure that the resources are compliant with that control. Resources that are not compliant will not be provisioned.
- Proactive controls are implemented by means of AWS **CloudFormation hooks**, and they apply to resources that would be provisioned by AWS CloudFormation. The status of a proactive control is PASS, FAIL, or SKIP.



# Example Proactive Controls

- Amazon API Gateway controls
- AWS Certificate Manager controls
- Amazon CloudFront controls
- AWS CloudTrail controls
- AWS CodeBuild controls
- AWS Database Migration Service (AWS DMS) controls
- Amazon DynamoDB controls
- DynamoDB Accelerator controls
- AWS Elastic Beanstalk controls
- Amazon Elastic Compute Cloud (Amazon EC2) controls
- Amazon Elastic Compute Cloud (Amazon EC2) Auto Scaling controls
- Amazon Elastic Container Registry controls
- Amazon Elastic Container Service controls
- Amazon Elastic File System controls
- Elastic Load Balancing controls
- Amazon GuardDuty controls
- AWS Identity and Access Management (IAM) controls
- AWS Key Management Service (AWS KMS) controls
- Amazon Kinesis controls
- AWS Lambda controls
- AWS Network Firewall controls
- Amazon OpenSearch controls
- Amazon Relational Database Service (Amazon RDS) controls
- Amazon Redshift controls
- Amazon Simple Storage Service (Amazon S3) controls
- Amazon SageMaker controls
- Amazon Simple Queue Service (Amazon SQS) controls
- AWS WAF regional controls
- AWS WAF controls
- AWS WAFV2 controls

- [https://aws.amazon.com/about-aws/whats-new/2023/05/aws-control-tower-new-proactive-controls /](https://aws.amazon.com/about-aws/whats-new/2023/05/aws-control-tower-new-proactive-controls/)

- [CT.AUTOSCALING.PR.1] Require an Amazon EC2 Auto Scaling group to have multiple Availability Zones
- [CT.AUTOSCALING.PR.2] Require an Amazon EC2 Auto Scaling group launch configuration to configure Amazon EC2 instances for IMDSv2
- [CT.AUTOSCALING.PR.3] Require an Amazon EC2 Auto Scaling launch configuration to have a single-hop metadata response limit
- [CT.AUTOSCALING.PR.4] Require an Amazon EC2 Auto Scaling group associated with an AWS Elastic Load Balancing (ELB) to have ELB health checks activated
- [CT.AUTOSCALING.PR.5] Require that an Amazon EC2 Auto Scaling group launch configuration does not have Amazon EC2 instances with public IP addresses
- [CT.AUTOSCALING.PR.6] Require any Amazon EC2 Auto Scaling groups to use multiple instance types
- [CT.AUTOSCALING.PR.8] Require an Amazon EC2 Auto Scaling group to have EC2 launch templates configured

# AWS Control Tower controls

- Control Tower provide human readable controls and groups them depending on the recommendation:

Mandatory

Strongly  
Recommended

Elective

# Mandatory Controls (Guardrails)

- **Mandatory** controls are always enforced in your landing zone. You **cannot turn them off** for any OU.

An orange square graphic with the word "Mandatory" written in white text inside it.

Mandatory



# Mandatory Controls

- Disallow Changes to Encryption Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive
- Disallow Changes to Logging Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive
- Disallow Changes to Bucket Policy for AWS Control Tower Created Amazon S3 Buckets in Log Archive
- Disallow Changes to Lifecycle Configuration for AWS Control Tower Created Amazon S3 Buckets in Log Archive
- Disallow Changes to Amazon CloudWatch Logs Log Groups set up by AWS Control Tower
- Disallow Deletion of AWS Config Aggregation Authorizations Created by AWS Control Tower
- Disallow Deletion of Log Archive
- Detect Public Read Access Setting for Log Archive
- Detect Public Write Access Setting for Log Archive
- Disallow Configuration Changes to CloudTrail
- Integrate CloudTrail Events with Amazon CloudWatch Logs
- Enable CloudTrail in All Available Regions
- Enable Integrity Validation for CloudTrail Log File
- Disallow Changes to Amazon CloudWatch Set Up by AWS Control Tower
- Disallow Changes to Tags Created by AWS Control Tower for AWS Config Resources
- Disallow Configuration Changes to AWS Config
- Enable AWS Config in All Available Regions
- Disallow Changes to AWS Config Rules Set Up by AWS Control Tower
- Disallow Changes to AWS IAM Roles Set Up by AWS Control Tower and AWS CloudFormation
- Disallow Changes to AWS Lambda Functions Set Up by AWS Control Tower
- Disallow Changes to Amazon SNS Set Up by AWS Control Tower
- Disallow Changes to Amazon SNS Subscriptions Set Up by AWS Control Tower
- Detect whether shared accounts under the Security organizational unit have AWS CloudTrail or CloudTrail Lake enabled



```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GRCLOUDTRAILENABLED",
      "Effect": "Deny",
      "Action": [
        "cloudtrail:DeleteTrail",
        "cloudtrail:PutEventSelectors",
        "cloudtrail:StopLogging",
        "cloudtrail:UpdateTrail"
      ],
      "Resource": ["arn:aws:cloudtrail:*:*:trail/aws-controltower-*"],
      "Condition": {
        "ArnNotLike": {
          "aws:PrincipalARN": "arn:aws:iam::*:role/AWSControlTowerExecution"
        }
      }
    }
  ]
}
```

# Strongly recommended Controls (Guardrails)


- **Strongly recommended** controls are designed to enforce some common best practices for well-architected, multi-account environments. These controls apply at the OU level, for all accounts in that OU.



Strongly  
Recommended

# Strongly recommended Controls

- Disallow Creation of Access Keys for the Root User
- Disallow Actions as a Root User
- Detect Whether Encryption is Enabled for Amazon EBS Volumes Attached to Amazon EC2 Instances
- Detect Whether Unrestricted Incoming TCP Traffic is Allowed
- Detect Whether Unrestricted Internet Connection Through SSH is Allowed
- Detect Whether MFA for the Root User is Enabled
- Detect Whether Public Read Access to Amazon S3 Buckets is Allowed
- Detect Whether Public Write Access to Amazon S3 Buckets is Allowed
- Detect Whether Amazon EBS Volumes are Attached to Amazon EC2 Instances
- Detect Whether Amazon EBS Optimization is Enabled for Amazon EC2 Instances
- Detect Whether Public Access to Amazon RDS Database Instances is Enabled
- Detect Whether Public Access to Amazon RDS Database Snapshots is Enabled
- Detect Whether Storage Encryption is Enabled for Amazon RDS Database Instances
- Detect whether an account has AWS CloudTrail or CloudTrail Lake enabled



```
AWSTemplateFormatVersion: 2010-09-09
Description: Configure AWS Config rules to require MFA for root access to accounts
Parameters:
  ConfigRuleName:
    Type: 'String'
    Description: 'Name for the Config rule'
  MaximumExecutionFrequency:
    Type: String
    Default: 24hours
    Description: The frequency that you want AWS Config to run evaluations for the rule.
    AllowedValues:
      - 1hour
      - 3hours
      - 6hours
      - 12hours
      - 24hours
Mappings:
  Settings:
    FrequencyMap:
      1hour : One_Hour
      3hours : Three_Hours
      6hours : Six_Hours
      12hours : Twelve_Hours
      24hours : TwentyFour_Hours
Resources:
  CheckForRootMfa:
    Type: AWS::Config::ConfigRule
    Properties:
      ConfigRuleName: !Sub ${ConfigRuleName}
      Description: Checks whether the root user of your AWS account requires multi-factor authentication for console sign-in.
      Source:
        Owner: AWS
        SourceIdentifier: ROOT_ACCOUNT_MFA_ENABLED
      MaximumExecutionFrequency:
        !FindInMap
        - Settings
        - FrequencyMap
        - !Ref MaximumExecutionFrequency
```

# Elective Controls (Guardrails)

- **Elective** controls enable you to track or lock down actions that are commonly restricted in an AWS enterprise environment. These controls apply at the OU level, for all accounts in that OU.

A solid yellow square graphic located in the bottom right corner of the slide.

Elective

# Elective Controls

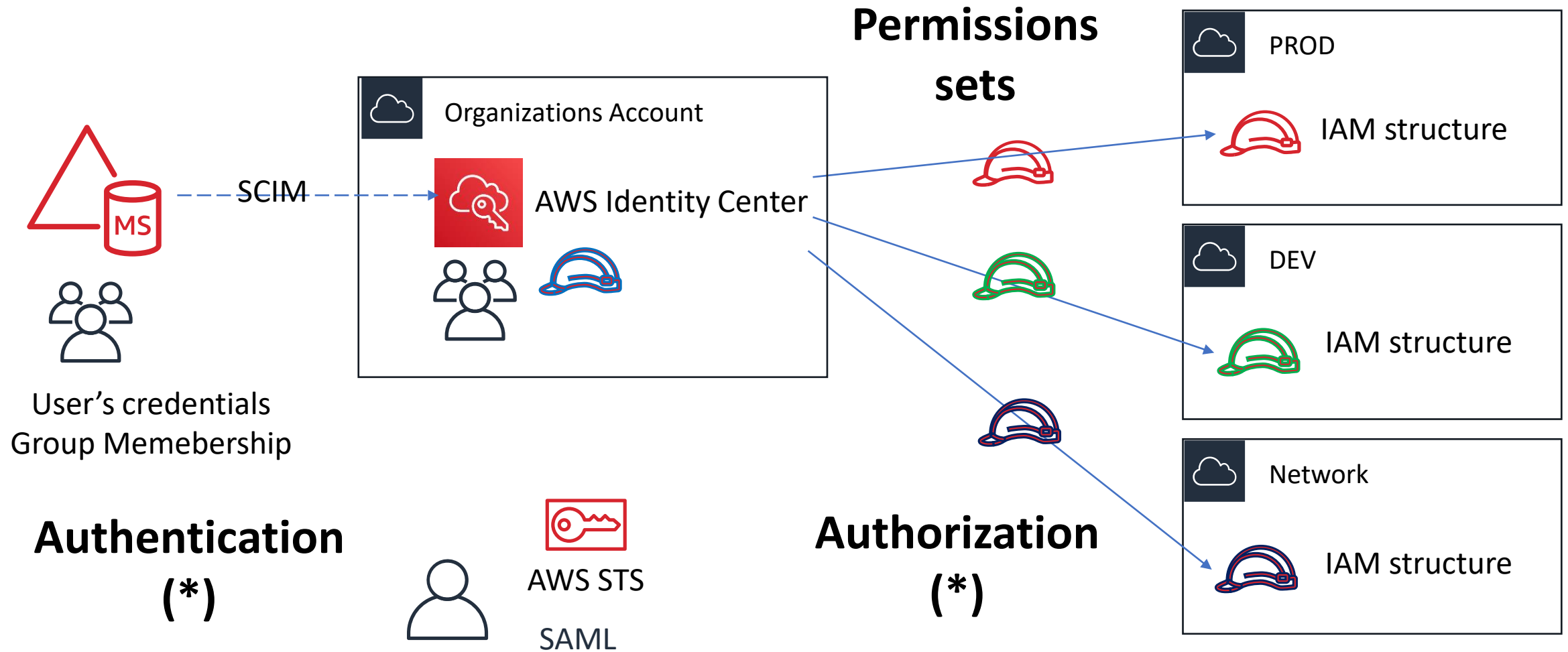
- [Disallow Changes to Encryption Configuration for Amazon S3 Buckets \[Previously: Enable Encryption at Rest for Log Archive\]](#)
- [Disallow Changes to Logging Configuration for Amazon S3 Buckets \[Previously: Enable Access Logging for Log Archive\]](#)
- [Disallow Changes to Bucket Policy for Amazon S3 Buckets \[Previously: Disallow Policy Changes to Log Archive\]](#)
- [Disallow Changes to Lifecycle Configuration for Amazon S3 Buckets \[Previously: Set a Retention Policy for Log Archive\]](#)
- [Disallow Changes to Replication Configuration for Amazon S3 Buckets](#)
- [Disallow Delete Actions on Amazon S3 Buckets Without MFA](#)
- [Detect Whether MFA is Enabled for AWS IAM Users](#)
- [Detect Whether MFA is Enabled for AWS IAM Users of the AWS Console](#)
- [Detect Whether Versioning for Amazon S3 Buckets is Enabled](#)
- [Disallow management of resource types, modules, and hooks within the AWS CloudFormation registry](#)

# AWS SSO->AWS IAM Identity Center

CHANGED the name to *AWS IAM Identity Center*

- Integration with Control Tower
- Permissions Sets
- Link to external Identity Providers (Azure AD, Okta,...)

# AWS Identity Center



# Account Factory

- Integrated into AWS Service Catalog
- <https://github.com/aws-samples/aws-account-vending-machine>
- Mention AFT Account Factory for Terraform  
<https://docs.aws.amazon.com/controltower/latest/userguide/aft-overview.html>



# Integrated with other AWS services

- Increasing number of AWS services that are integrated within Control Tower:

▼ Integrated services

AWS CloudFormation

CloudTrail

CloudWatch

AWS Config

IAM

AWS Key Management  
Service

AWS Lambda

AWS Organizations

Amazon S3

**Security Hub**

Service Catalog

IAM Identity Center

Amazon SNS

Step Functions

# Open Ideas

- Have you work with Control Tower?
  - Painpoints?
  - Stories?

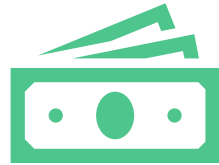


# Key Takeaways

# Key takeaway



**Keep complexity  
under control,  
provide agility and  
promote innovation**



**Group and  
centralize billing  
and accounting**

Cost allocation Tags



**Apply policies  
centrally to the  
whole organization**

[illegible]