5. IAM, ACCOUNTS AND AWS ORGANISATIONS

Created	@August 22, 2022 6:10 PM
Class	
Type	
Materials	
Reviewed	☐
Property	
Date	

IAM Policies

default deny policy will work

it will always take deny first and then go for allow

for example at the below code deny policies will take effect at first and then other

lets for example user is in 2 policy and also he is member of group

collect all of the statements and evaluate them and applied all together but there is explicit deny then its deny or explicit allow then allow

deny allow deny

if none of the apply then its default deny

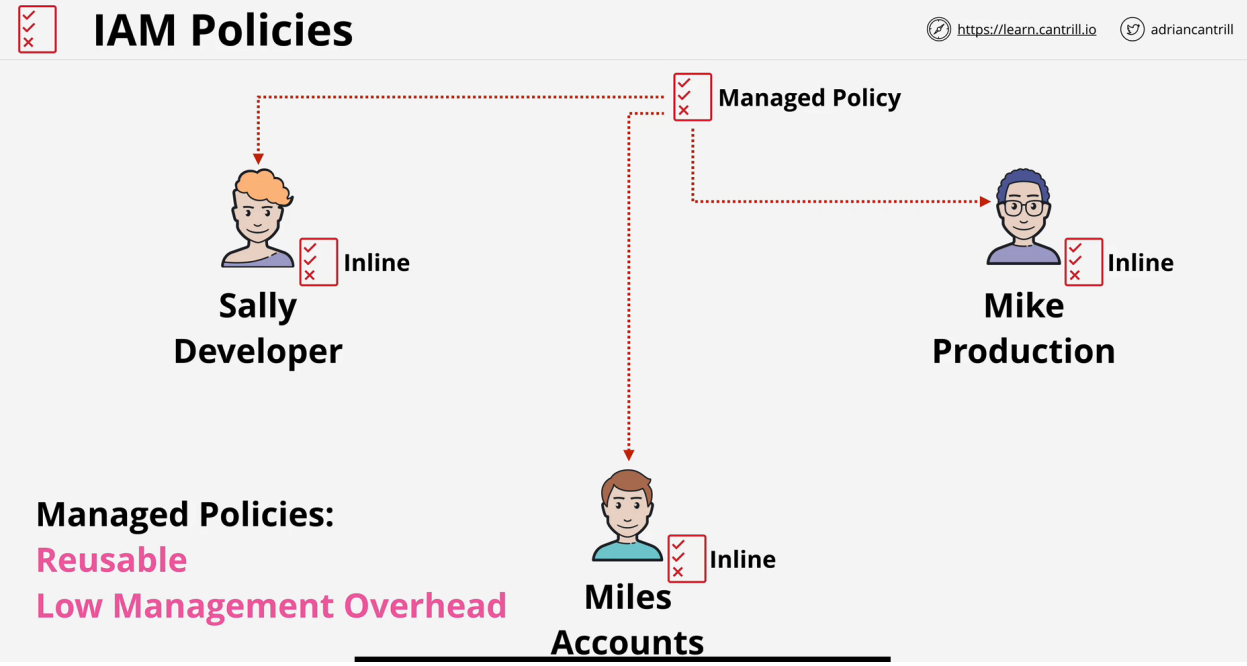
1. Inline policy type

where you can separate assign policy using JSON but not the best practice

incase of exception we use inline

for ex blocking of access to that particular user

2. Managed policy



1.AWS managed policy

2. Customer managed policy

Demo on IAM Users where we created IAM user using cloudFormation template and then explicitly allowed and denied some of the policies using upload template for sally

we tested this by login into sally and username(inside IAMadmin) then tested everything

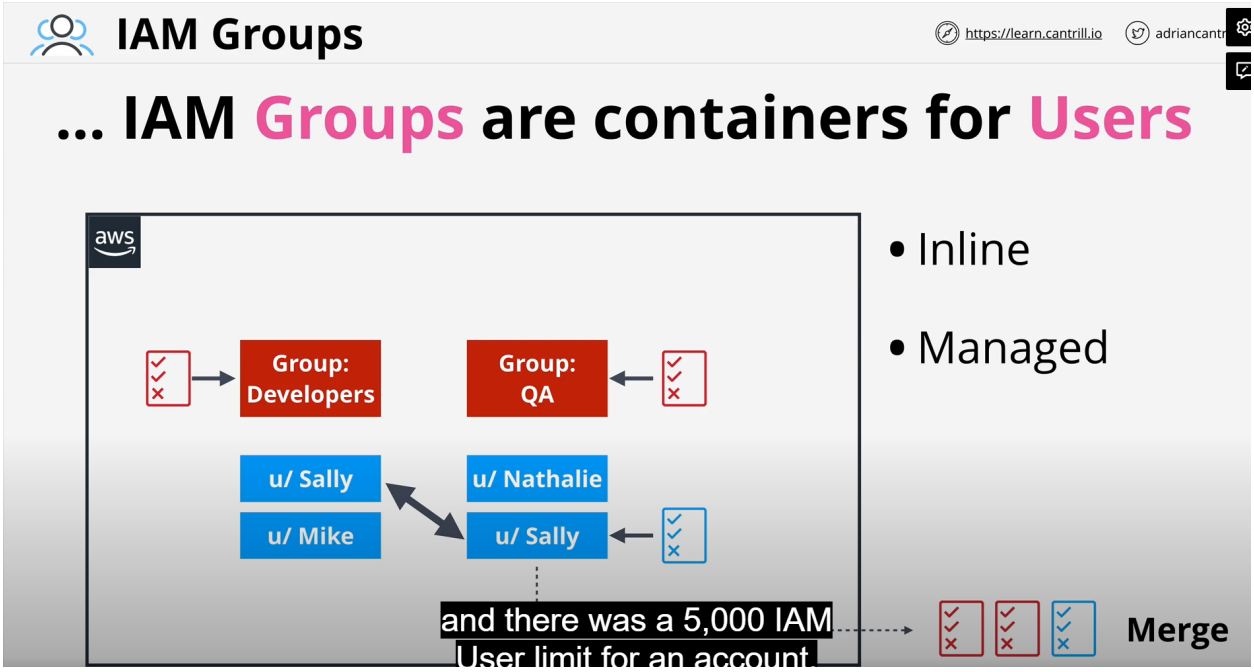
then we tested inline policy by explicitly denying some s3 access and then we deleted the cloudformation stack

to delete stack make sure to delete the objects from s3 bucket first

IAM Groups:

It is not user its container so you cannot login to groups

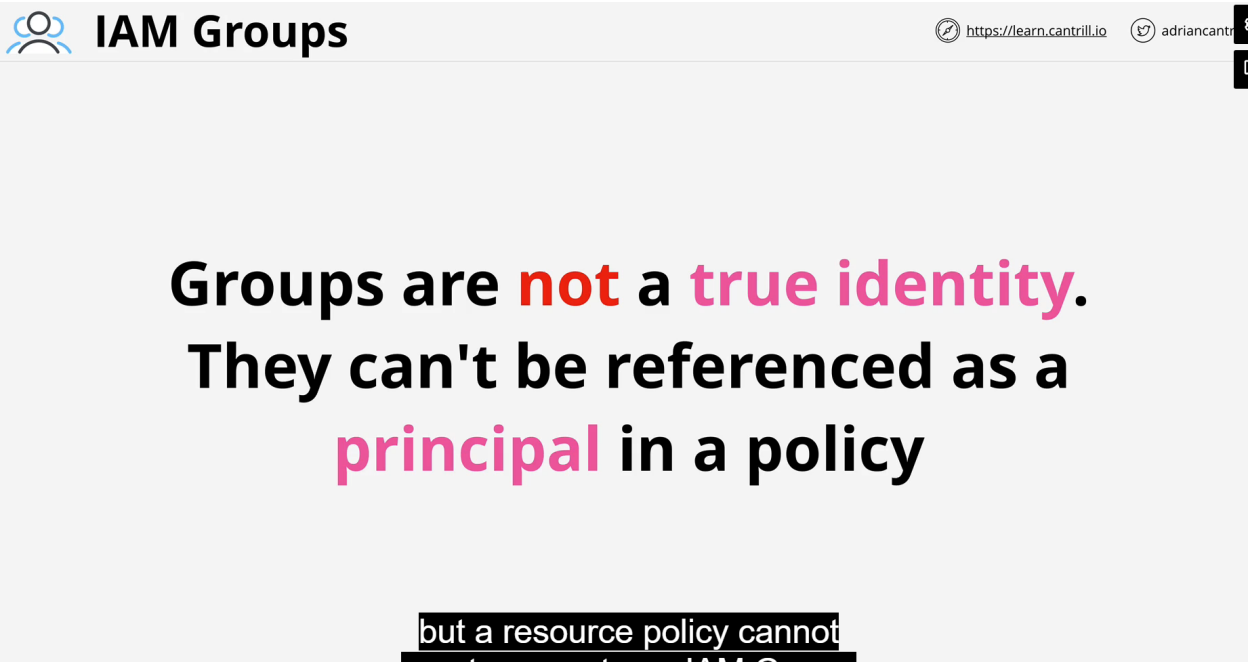
its used to manage Iam users

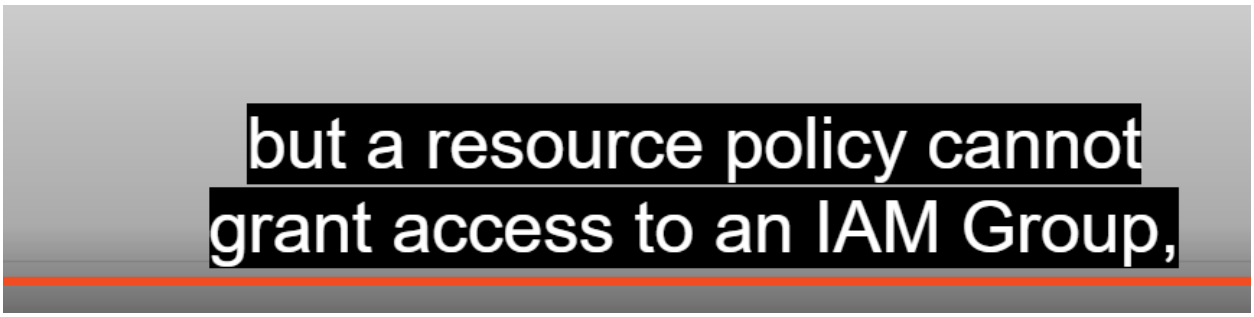


▼ IAM user restriction:

Can be memeber of 10 group

and 5000 IAM user limit for a single account





IAM Groups are a feature of IAM which you need to know about for the exam.

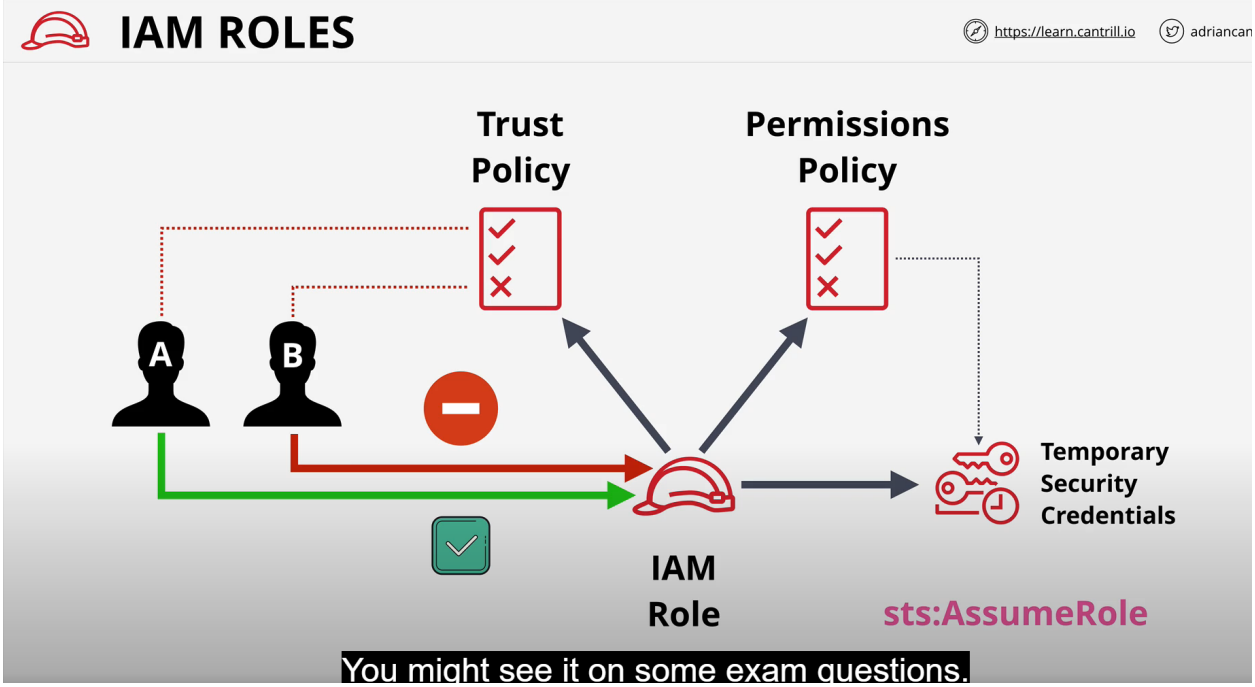
They are an admin or container feature.

You can add IAM users to groups, and add permissions to Groups

Groups are NOT real identities ... can't be used from resource policies and have no credentials to login with.

IAM Roles

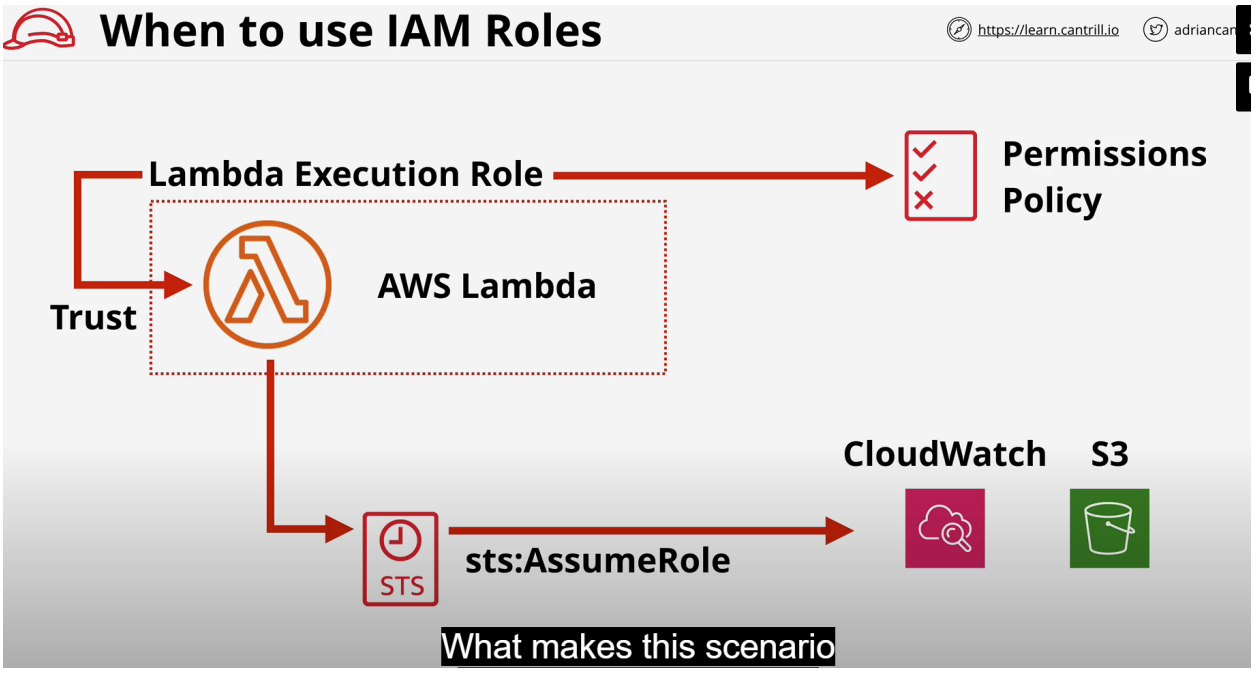
Principle: Is the physical person, identity, process or application which wants to authenticate with AWS



When to use IAM Roles:

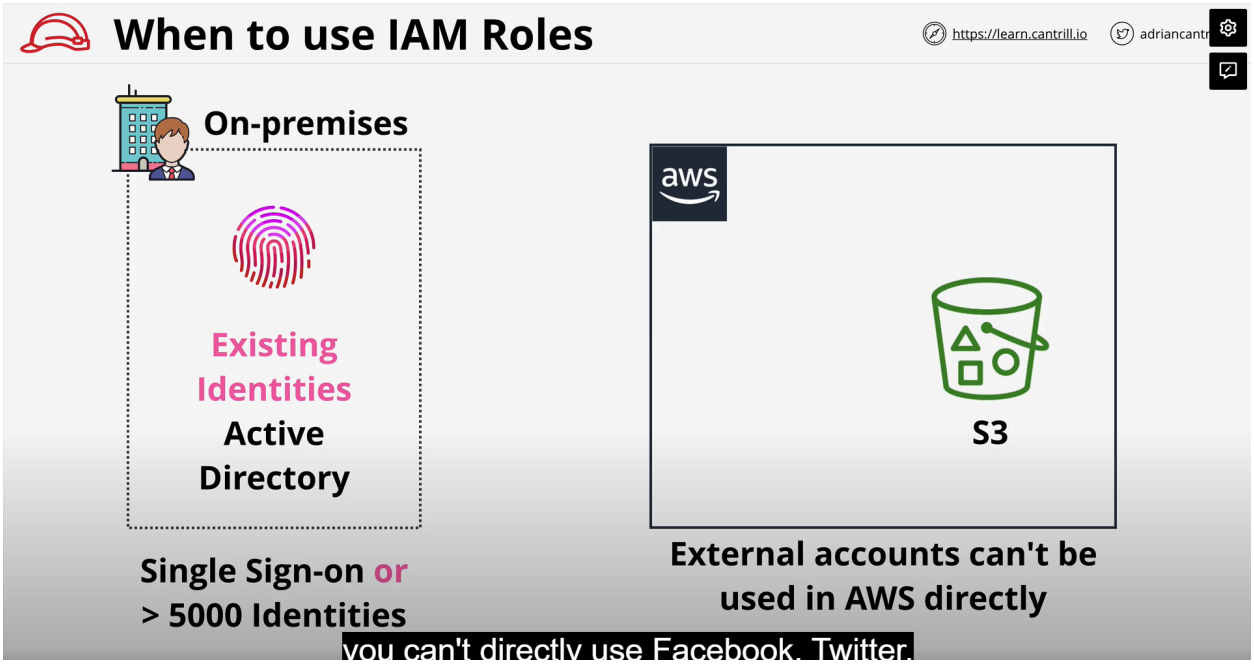
To prevent from hardcoding roles and authentication information into any function such as for example in lambda function we use IAM Roles which gives temporary access to the function using sts:AssumeRole and once the execution is done access can be revoked.

also we dont know how many functions will be running on runtime so its better to have IAM roles assigned

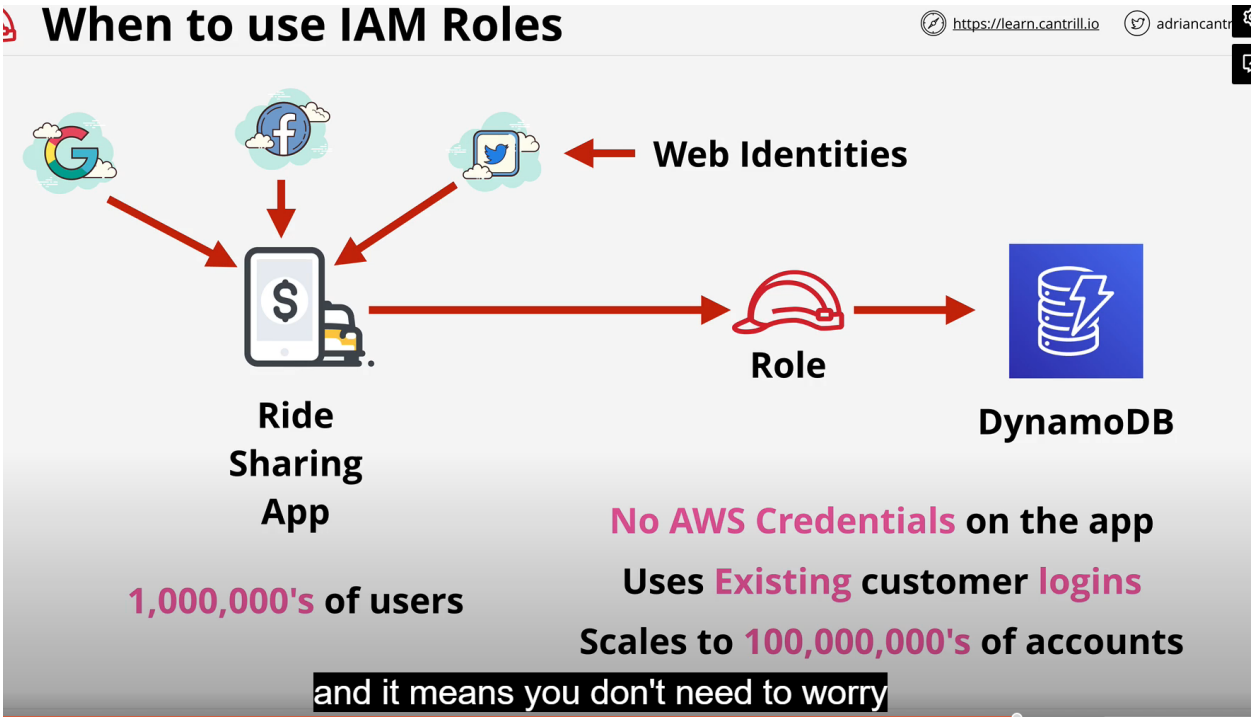


Another use of IAM Roles is when on-premises for example Active directory allows them to login

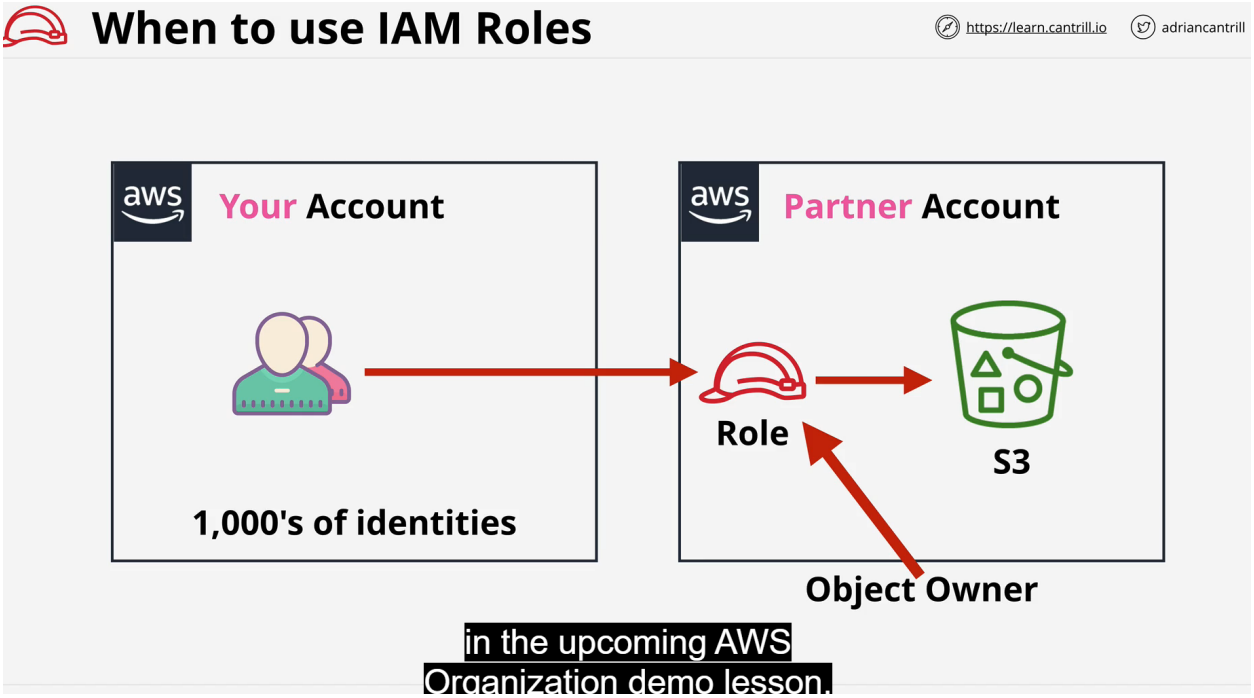
external accounts or entities cannot be used to access aws account



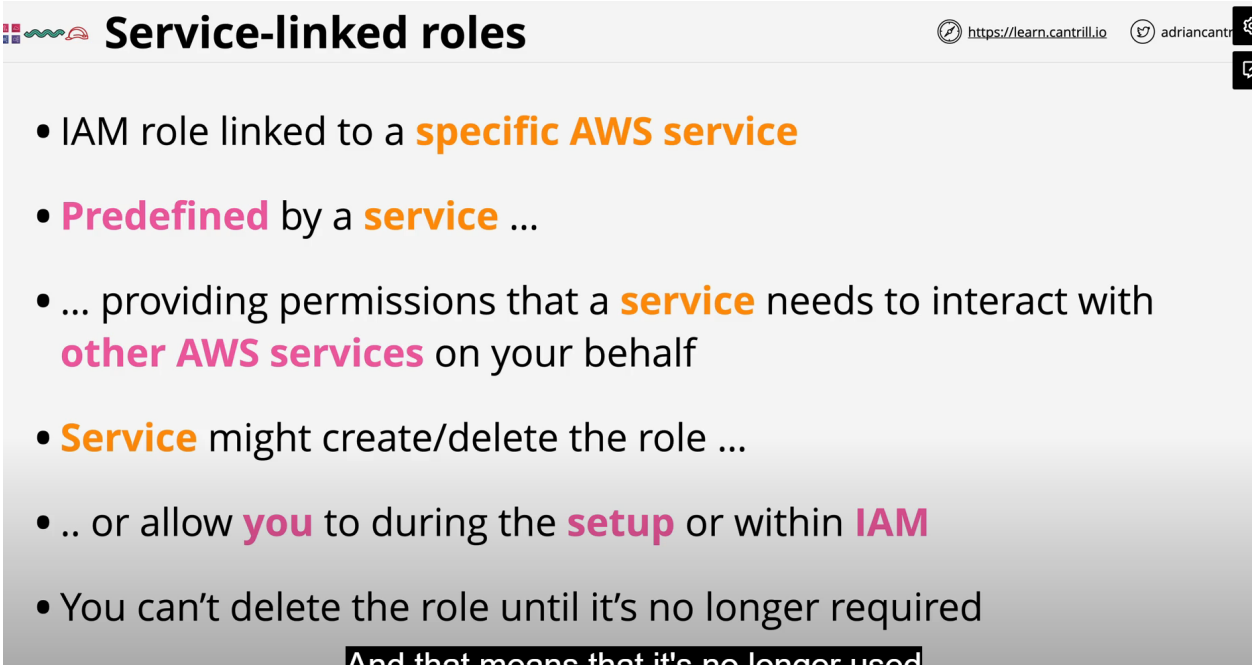
max 5k IAM roles



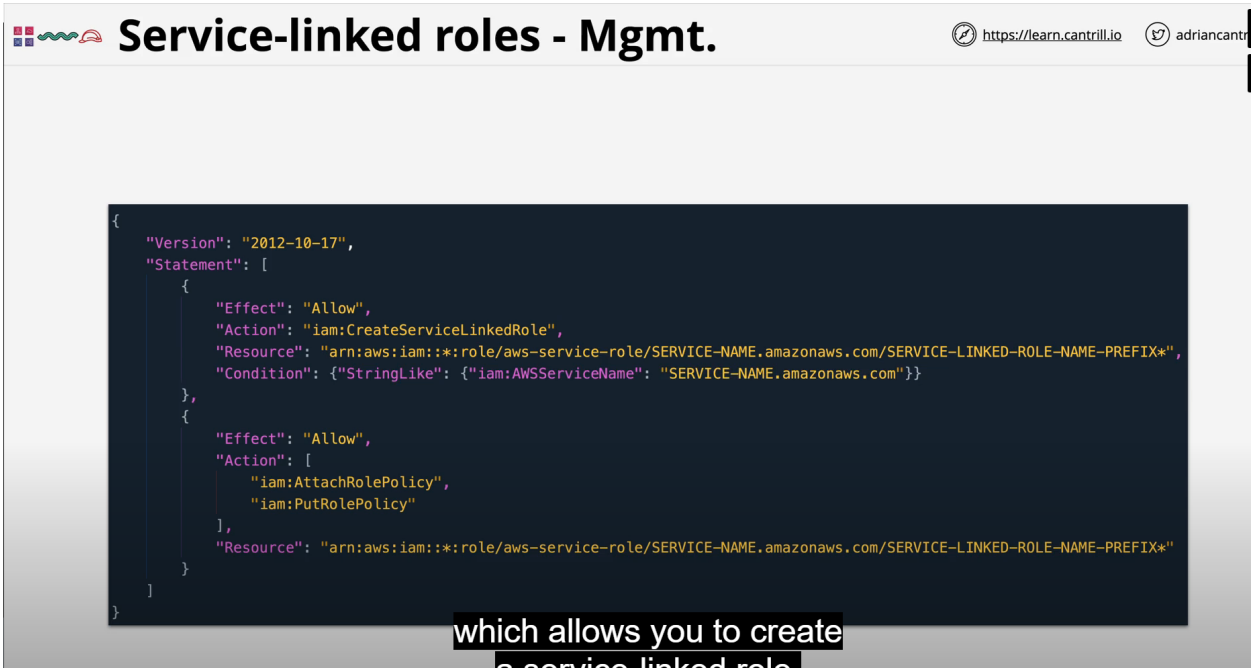
lets say my 1k user wants to access and use s3 from another account we can apply **IAM roles**



Server Linked roles:



Example of policy which allows service linkes role:



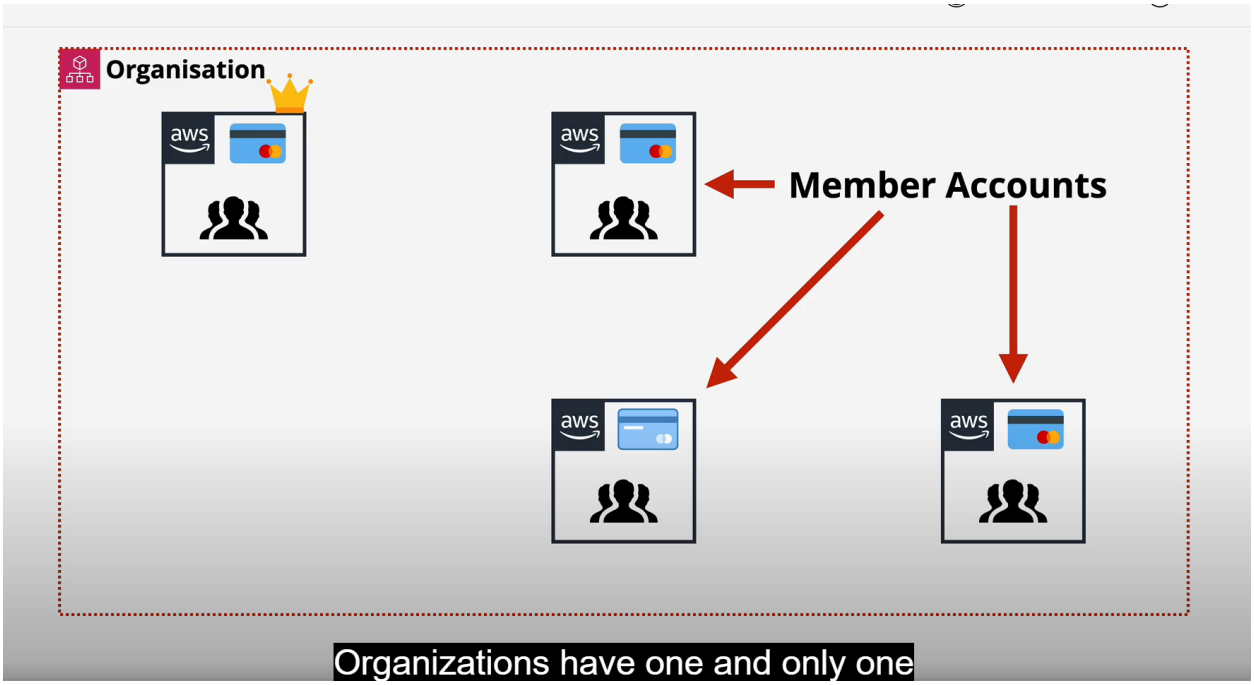
Passrole is role in aws which allows to give role separation in aws

AWS organization:

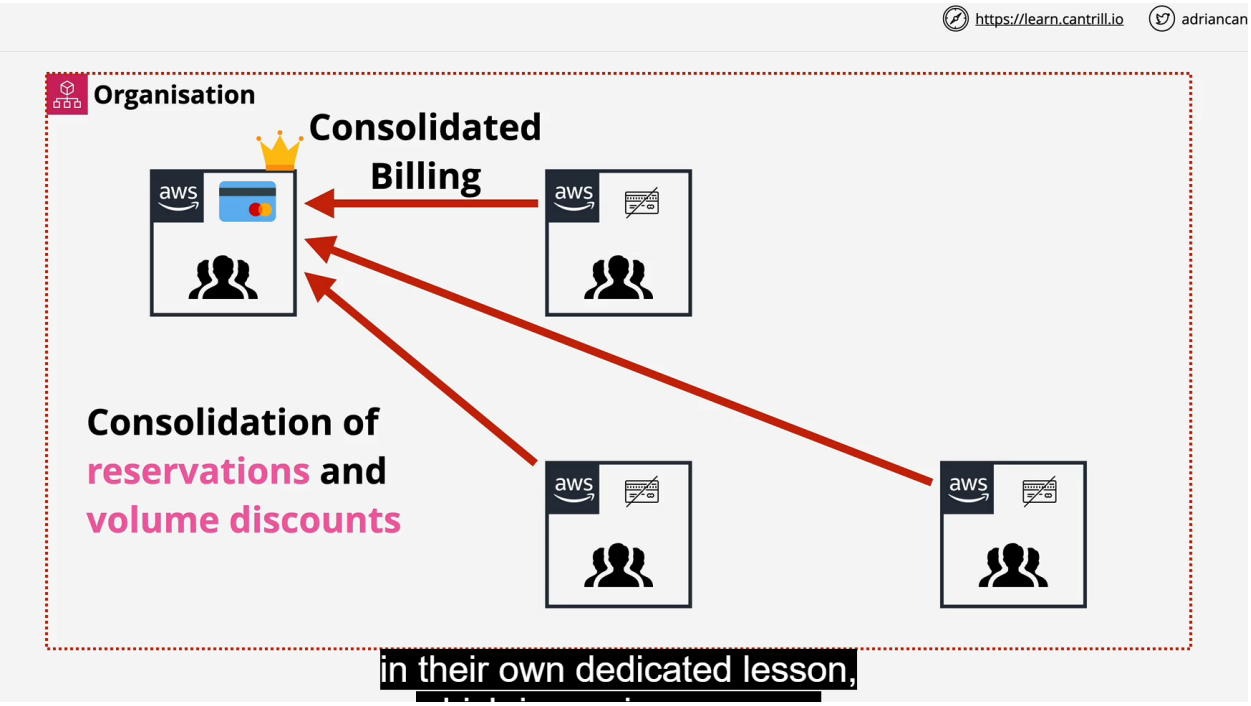
Without aws organization we have to manage hundreds of accounts

standard accounts are account which are not part of aws organization

but when they accept the invite of organization account they are no longer standard account but a member accounts.



with AWS organization we get consolidated billing and get volume discount along the same



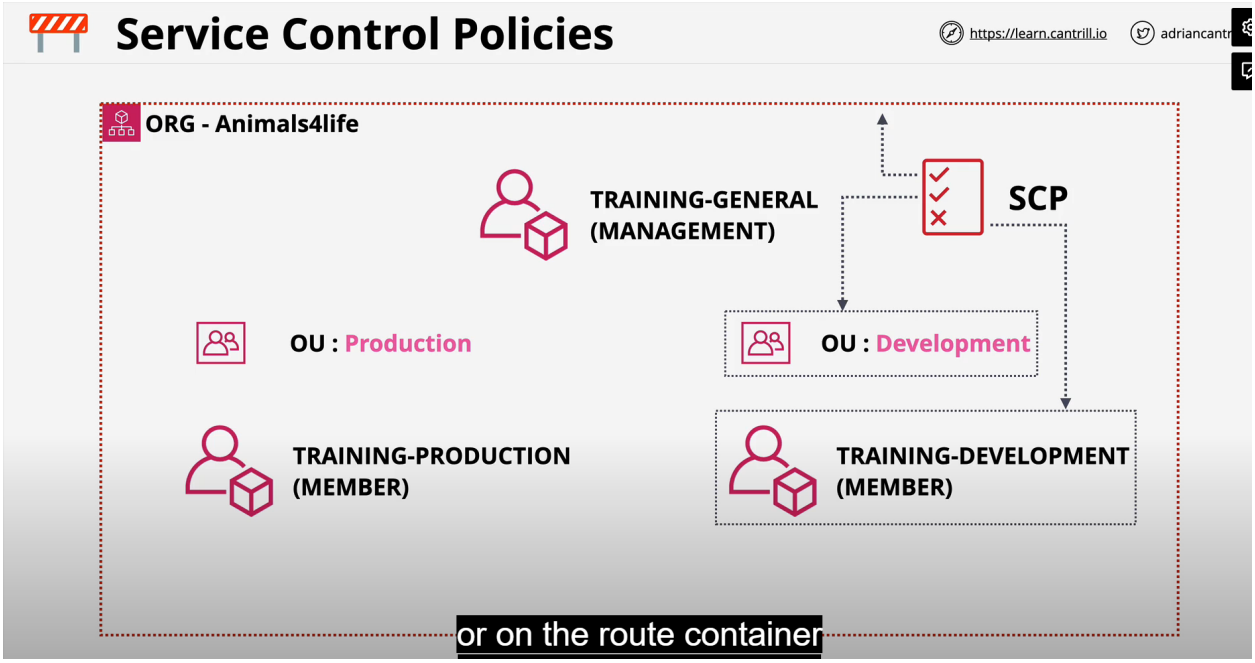
Service Control policy

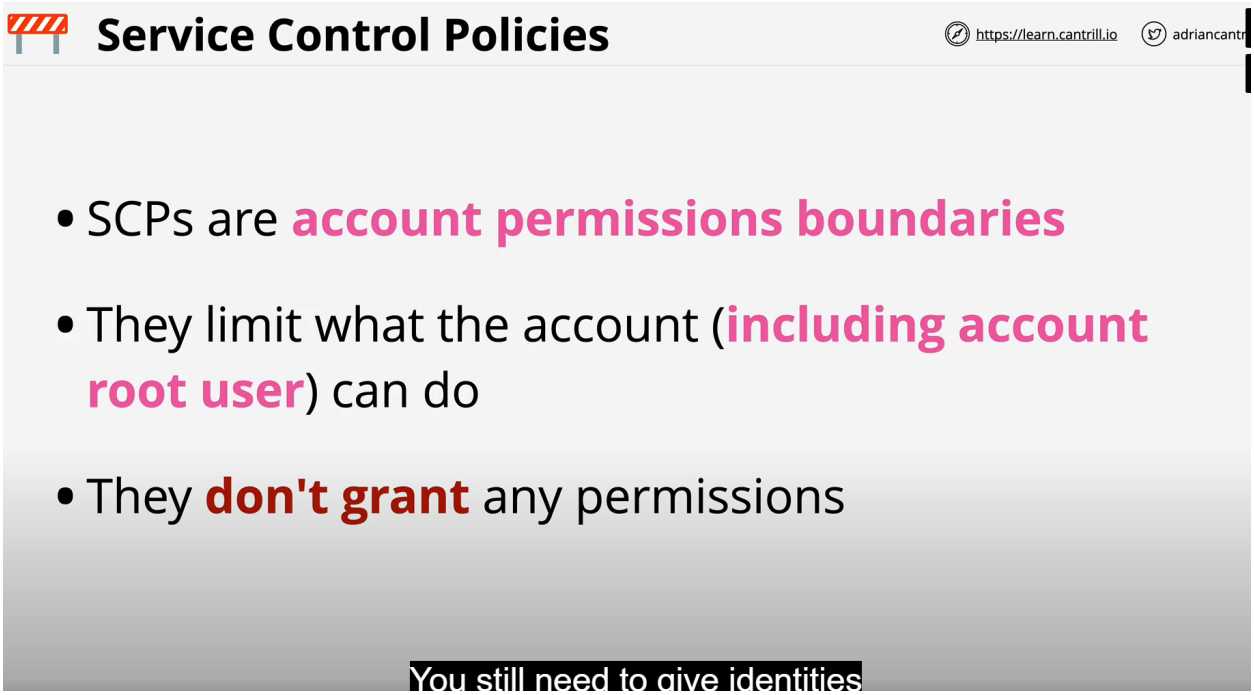
default is deny

its basically firewall with default block as aws being aws for security

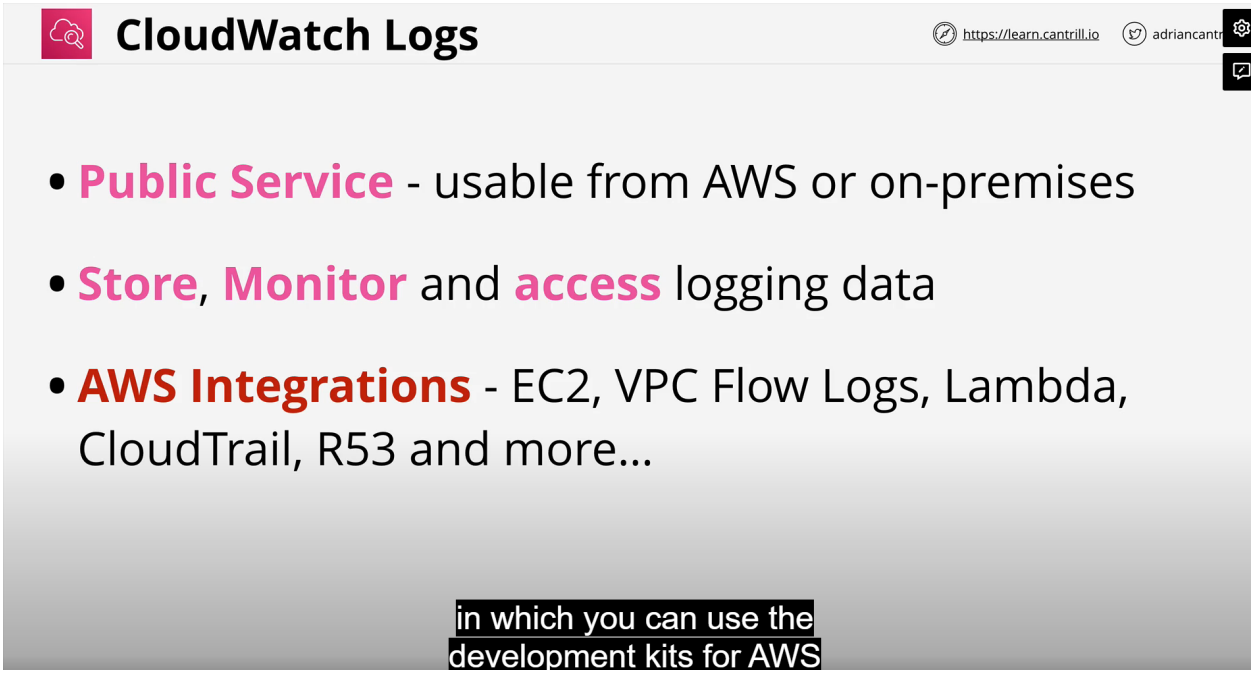
Service Control policy: its basically limitor to account on what it can do

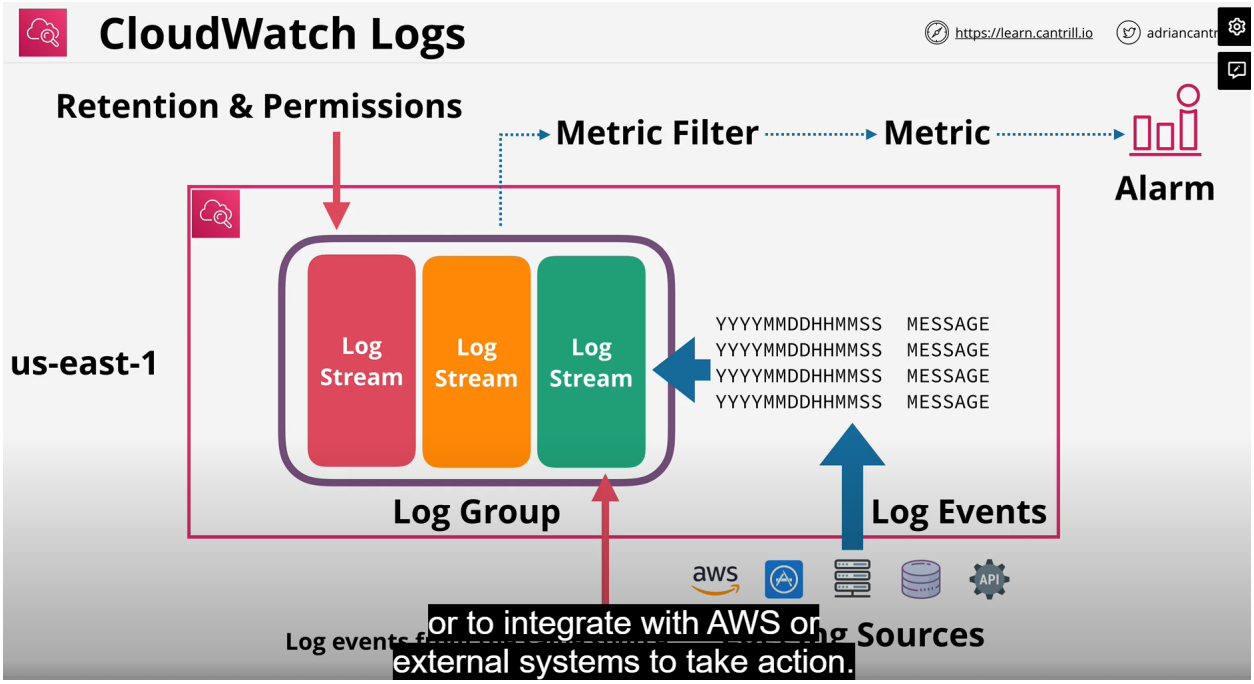
You cannot restrict management aka aws account





CloudWatch Logs:





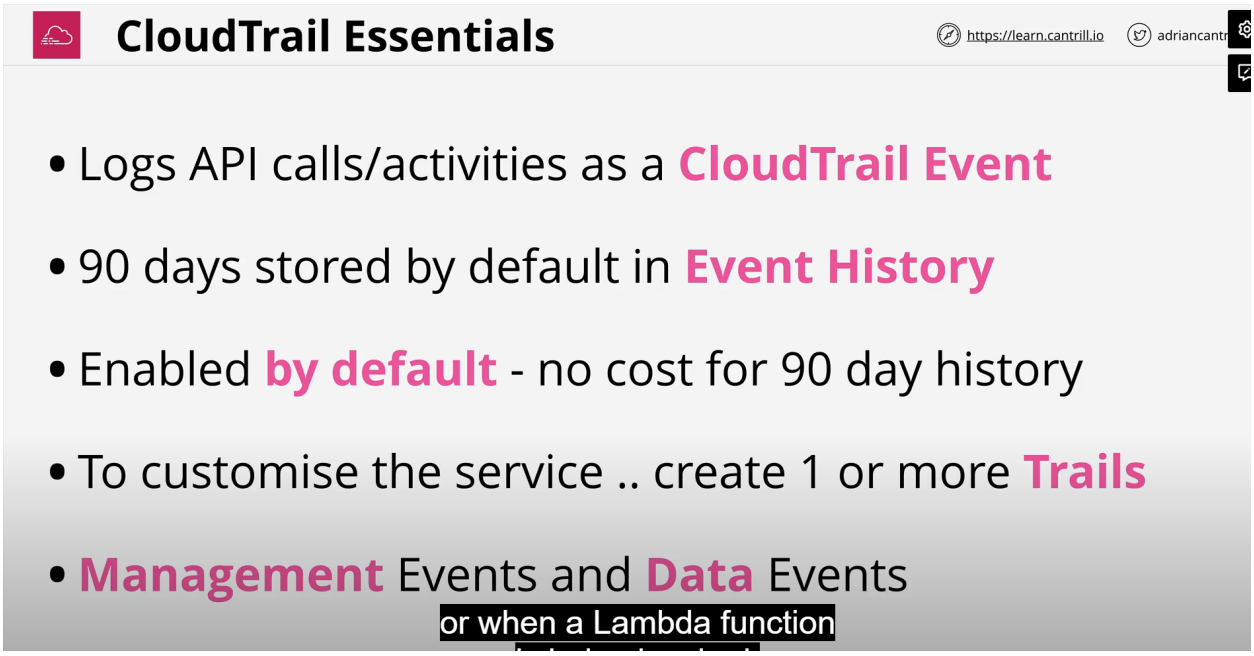
CloudTrail: Uses cloudwatch logs

CloudTrail:

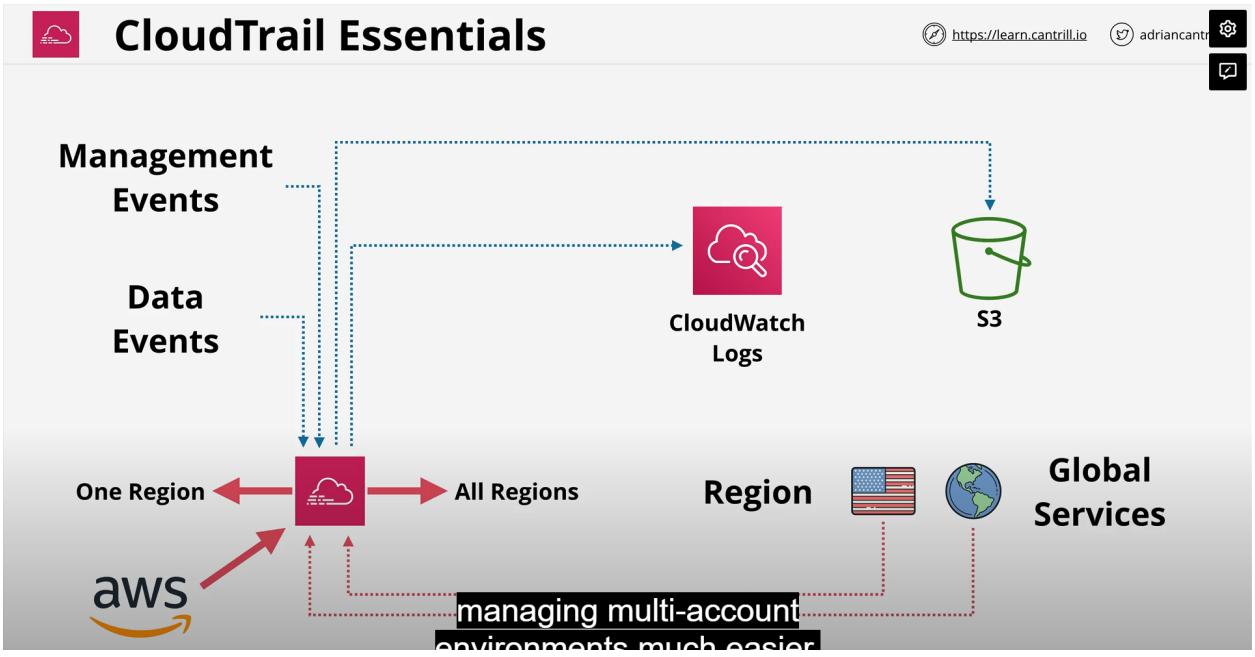
Uses Clooudwatch for taking logs

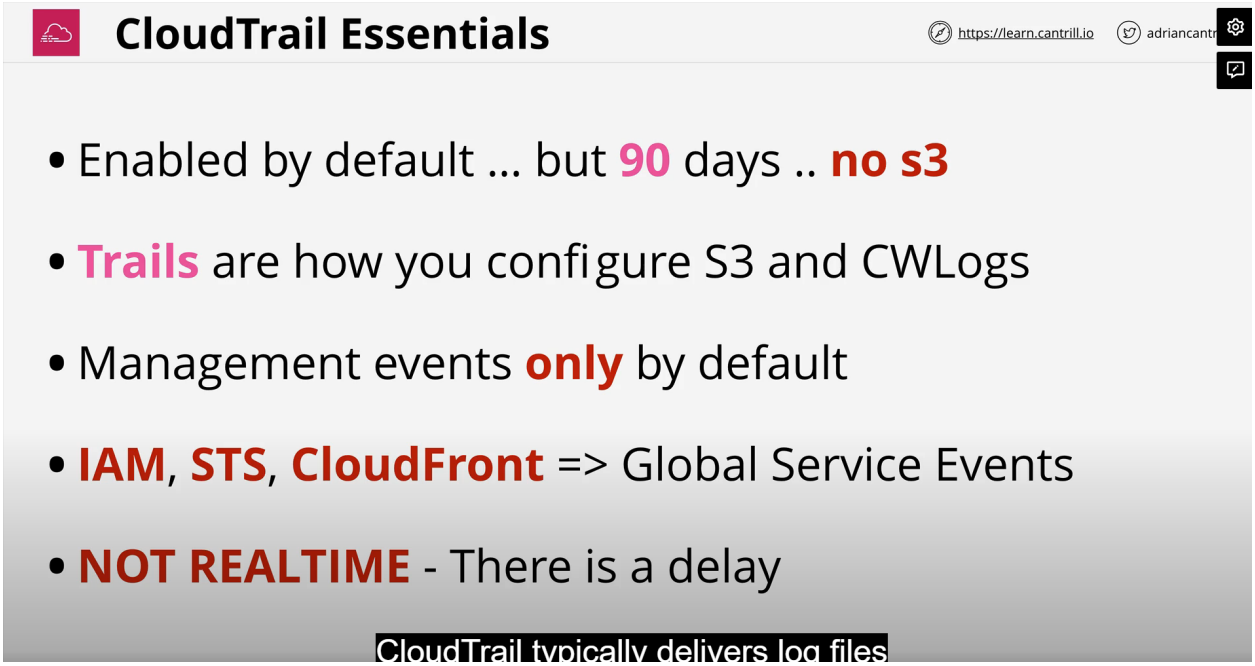
90 days free event logs

by default it only logs management events to reduce the log list



cloudtrail is regional service to get logs of global region it has to be enabled first





IAM STS n Cloudfront stores data on global services and to use them they have to be enabled first

Not real-time 15-20 min

also stores data on s3 bucket in json format

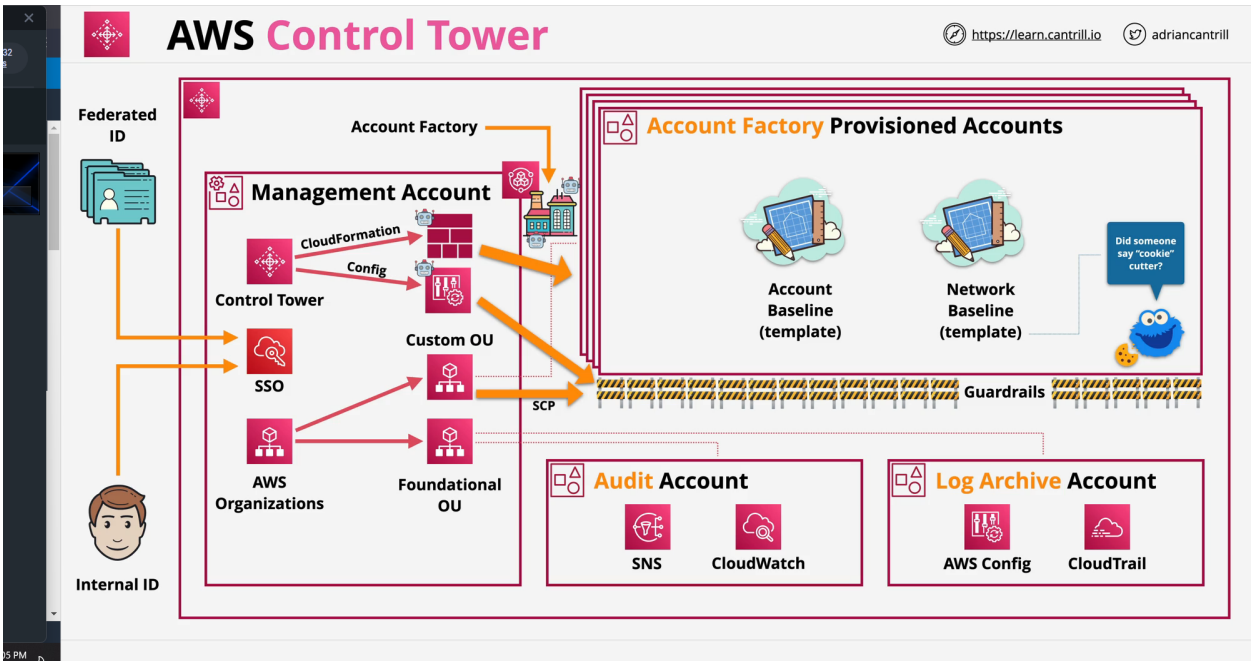
AWS Control Tower:

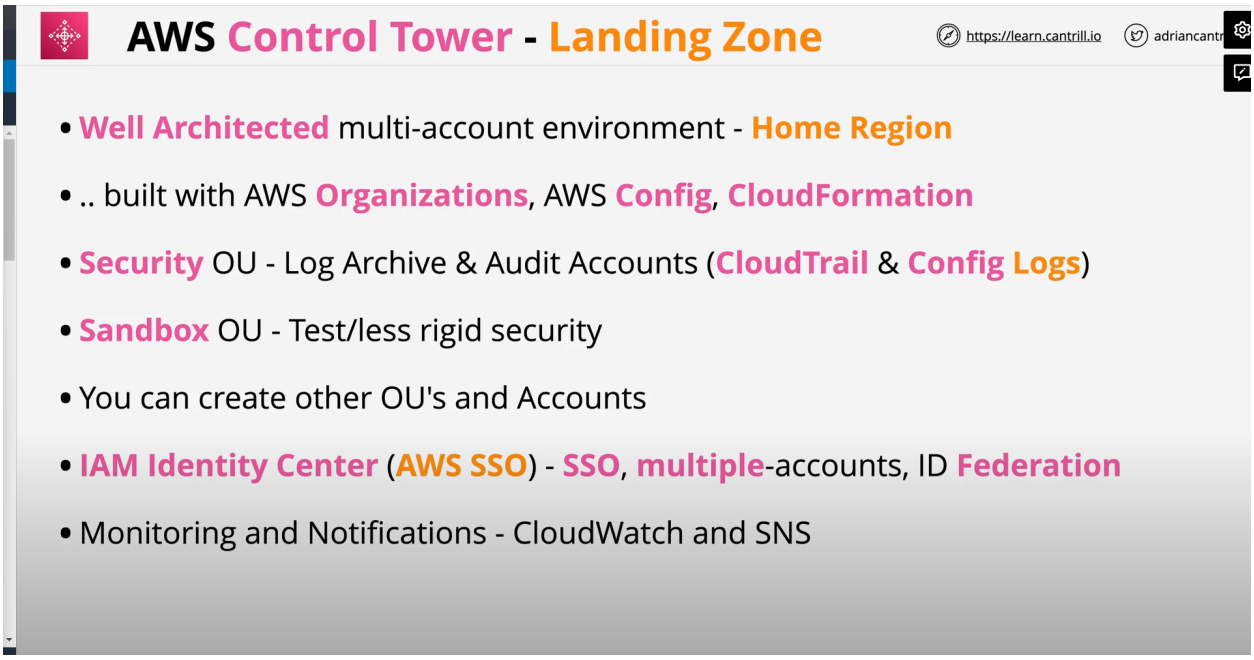
AWS Control Tower

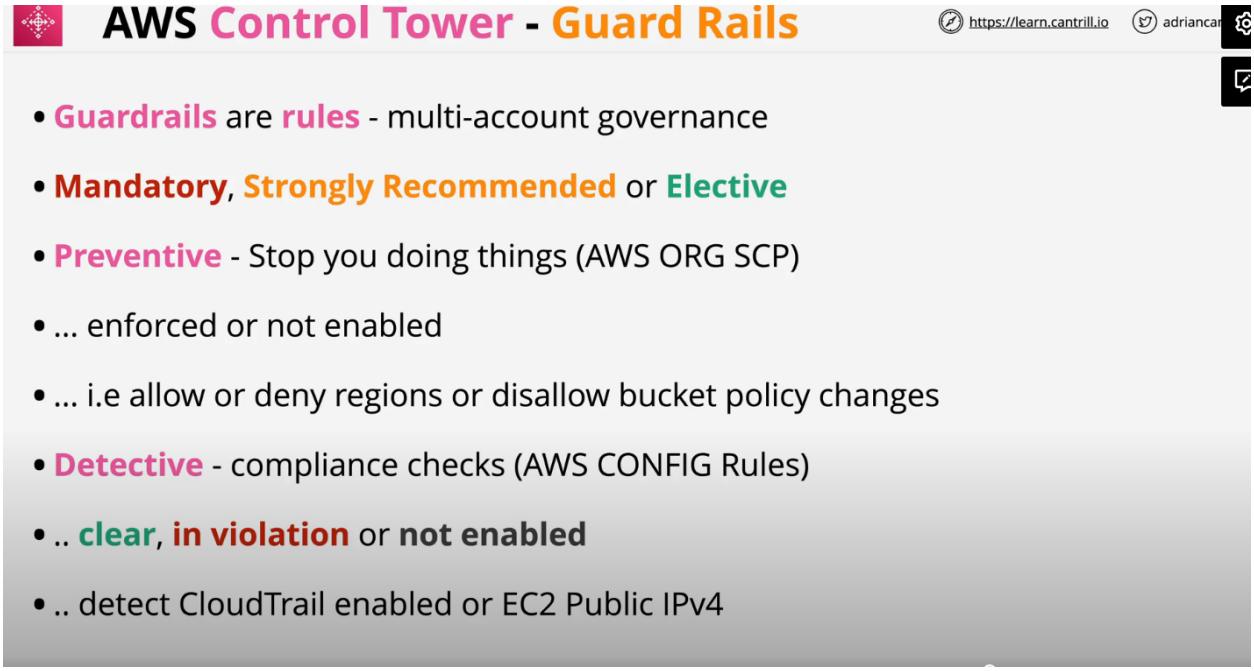
https://learn.cantrill.io adriancantrill

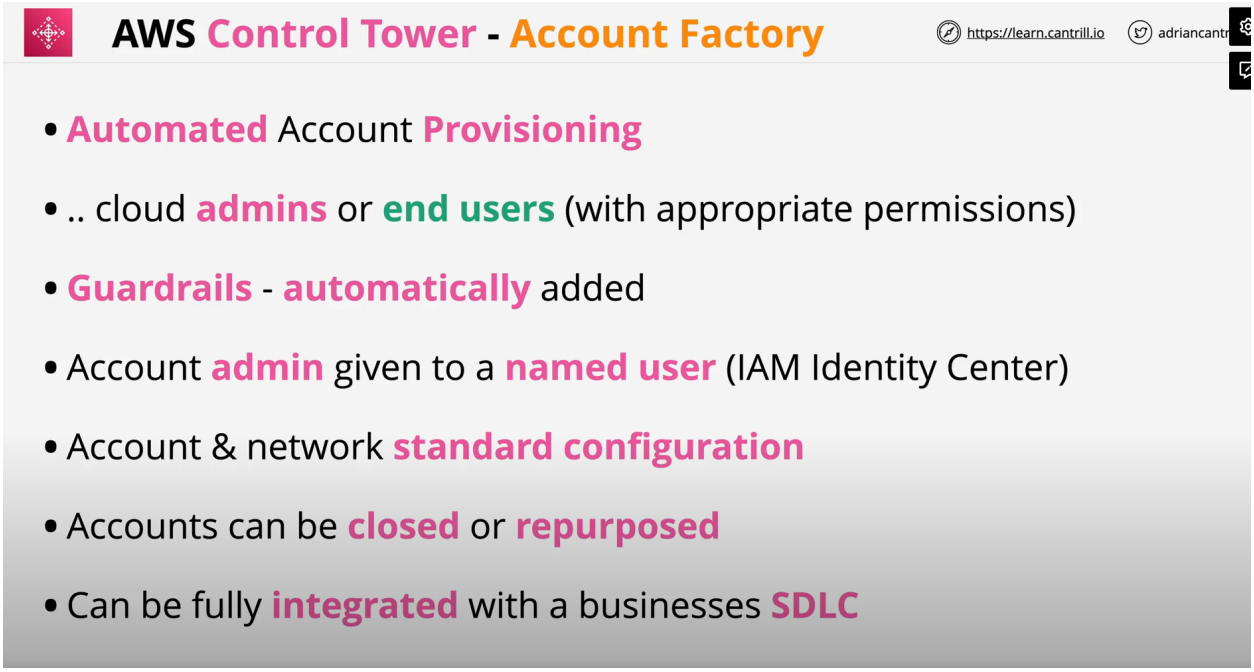
- **Quick** and **Easy** setup of **multi-account** environment
- **Orchestrates** other **AWS** services to provide this functionality.
- Organizations, IAM Identity Center, CloudFormation, Config and more....
- **Landing Zone** - **multi-account** environment
- ... SSO/ID Federation, Centralised Logging & Auditing
- **Guard Rails** - **Detect**/**Mandate** rules/standards across all accounts
- **Account Factory** - **Automates** and **Standardises** new account creation.
- **Dashboard** - single page oversight of the entire environment

better version of amazon organization




AWS Control Tower - Landing Zone
https://learn.cantrill.io
adriancantr
• Well Architected multi-account environment - Home Region
• .. built with AWS Organizations, AWS Config, CloudFormation
• Security OU - Log Archive & Audit Accounts (CloudTrail & Config Logs)
• Sandbox OU - Test/less rigid security
• You can create other OU's and Accounts
• IAM Identity Center (AWS SSO) - SSO, multiple-accounts, ID Federation
• Monitoring and Notifications - CloudWatch and SNS


AWS Control Tower - Guard Rails
https://learn.cantrill.io
adriancan
• Guardrails are rules - multi-account governance
• Mandatory, Strongly Recommended or Elective
• Preventive - Stop you doing things (AWS ORG SCP)
• ... enforced or not enabled
• ... i.e allow or deny regions or disallow bucket policy changes
• Detective - compliance checks (AWS CONFIG Rules)
• .. clear, in violation or not enabled
• .. detect CloudTrail enabled or EC2 Public IPv4


AWS Control Tower - Account Factory
https://learn.cantrill.io
adriancantr
• Automated Account Provisioning
• .. cloud admins or end users (with appropriate permissions)
• Guardrails - automatically added
• Account admin given to a named user (IAM Identity Center)
• Account & network standard configuration
• Accounts can be closed or repurposed
• Can be fully integrated with a businesses SDLC