Day 11 – Cloud IAM Foundations

Today's vision is to clear conceptual things ,so day 11 is all about Understanding ,how linux IAM maps to cloud IAM, how to be able to explain IAM in interviews. We have to think like a cloud security analyst , not a cloud user .

Phase 1 – Big Picture (Understand this first)

Core truth:

Cloud security is equal to identity security. This means in the cloud we do not have physical walls, access is granted based on your (user login) so therefore if you protect user identity it means you are protecting the entire cloud environment.

In cloud networks, the perimeter is weak because resources are accessible over the internet.A attacker can often bypass the network, so we can not rely on simple line defense.

Identity and access management(IAM) is our strongest ,powerful defense because it acts like a bouncer or a gatekeeper that protects every single file and service. If an attacker gets access for getting into the network ,IAM will stop from touching data unless they have full authority.

There are three main reasons for cloud breaching:

Over-permissioned Identities:

This only happens when we provide more access to users than they actually need for their job. If by chance a user gets hacked ,the attacker gets all that power.

Stolen Credentials:
This is simply when a hacker gets a username, password, or access key. Because the cloud trusts that 'ID card,' the hacker can walk right in looking like a real employee.

No Logging:
If we don't record what is happening (logging), we are flying blind. We won't know a hacker is inside, and we won't be able to fix the problem after they leave.

Phase 2 – Linux IAM → Cloud IAM Mapping

The Professional Mapping:

Linux Concept (What you did)	Cloud Equivalent (The Future)	Why it matters for an Interview
User	**IAM User**	Just like a person on Linux, an IAM User is a digital identity for a human or a service in the Cloud.

Group	**IAM Groups**	We put users into Groups (like 'Devs' or 'Admins') to manage permissions for many people at once.
sudo	**Privileged Role**	In Linux, you use sudo for power. In Cloud, you "Assume a Role" to get temporary high-level permissions only when needed.
File Permissions	**Resource Permissions**	Instead of chmod on a file, we use "Bucket Policies" or "Key Policies" to control who can see specific cloud data.
/var/log/auth.log	**CloudTrail / Sign-in Logs**	In Linux, auth.log catches hackers. In the Cloud, **CloudTrail** records every single click and action for security auditing.
Least Privilege	**Least Privilege**	This rule never changes: Only give a user the **minimum** access they need to do their job.

Phase 3 – Cloud IAM Concepts

1️⃣ IAM User:(The Identity)

This is an individual "ID Card" for a specific person or a specific software. Remember this Every person gets their own ID, You never share IDs.
You only have to provide that id access to those who are working on these projects, roles but minimum permission.

2️⃣ IAM Group:(The Department)

This is a "List" or a "Folder" of people who do the same job.
Instead of giving keys to 50 different people one by one, you put all 50 people into a "Marketing Group" and give the keys to the group.
If a new person joins, you just drop them into the Group, and they automatically get the right keys.

3️⃣ IAM Role:(The Temporary Power)

This is like a "Special Uniform" or a "Visitor Badge" that you put on for a short time to do a specific task.
In Linux, you use (`sudo`) to become "Root" for a second. In the Cloud, you "Assume a Role" to get extra power for a short time.
It is safer because you do not have a permanent password in it ,once you remove the user the power is gone even if the attacker steals a role key because the key will expire very quickly.

Phase 4 – Security Failures (Think like a defender)

Write short answers:

1) Why is giving admin access to everyone dangerous?

The Answer: It increases the "blast radius." If every user has Admin power, one small mistake (like deleting a folder) or one hacked account can destroy the entire company's infrastructure.

3) Why are long-lived credentials risky?

The Answer: Because the longer a password or "Access Key" exists, the more time an attacker has to steal it. Permanent keys are "static targets."

4) Why does logging every login matter?

The Answer: Without logs, you are blind. You cannot stop an attack you cannot see, and you cannot learn how the hacker got in after they leave.

Knowledgeable Questions/answers:

1. Linux sudo misuse Giving every user Admin power in the cloud is like giving every Linux user (`sudo`) access; it only takes one person to run a wrong command and destroy the entire infrastructure.

2. Auth.log failures Operating a cloud environment without logging is like having a broken `auth.log` in Linux; you will have no evidence of who entered your system or what data was stolen during a breach.

3. Brute force attempts Permanent cloud keys are high-risk targets because, just like a Linux server facing a brute force attack, the longer a credential stays the same, the more time a hacker has to eventually guess it.

Phase 5 – Detection Mindset (SIEM bridge)

In cloud, you detect:

- *Failed logins*
- *Impossible travel*
- *Privilege escalation*
- *Role misuse*

This is the same thinking you used in Ubuntu logs.

1. Failed Logins

The Cloud Logic: *Monitoring for multiple wrong passwords in a short time.*

The Linux Bridge*: This is exactly like checking your* Ubuntu `auth.log` *for "Failed password" messages during a* Brute Force attempt.

2. Impossible Travel

The Cloud Logic: Detecting a login from New York at 10:00 AM and another login from Karachi at 10:05 AM for the same user.

The Linux Bridge: In Linux, you check the IP addresses in the logs. If a user usually logs in from a local IP but suddenly shows an IP from another country, it's a red flag.

3. Privilege Escalation

The Cloud Logic: A regular user suddenly tries to change the "Admin" settings or delete a database.

The Linux Bridge: This is like a normal user trying to use `sudo` when they are not in the sudoers list.