

The principle of least privilege

AWS SECURITY AND COST MANAGEMENT CONCEPTS



Dev Bhosale

Principal Data & Cloud Architect

What is the principle of least privilege?

- Separate access to employees by department and capabilities
- Grant the narrowest set of privileges
- Do not grant more privileges than necessary to perform job responsibilities



Jen

Accounting Department
Can read/write balance sheet data



Joe

Finance Department
Read-only access to balance sheet

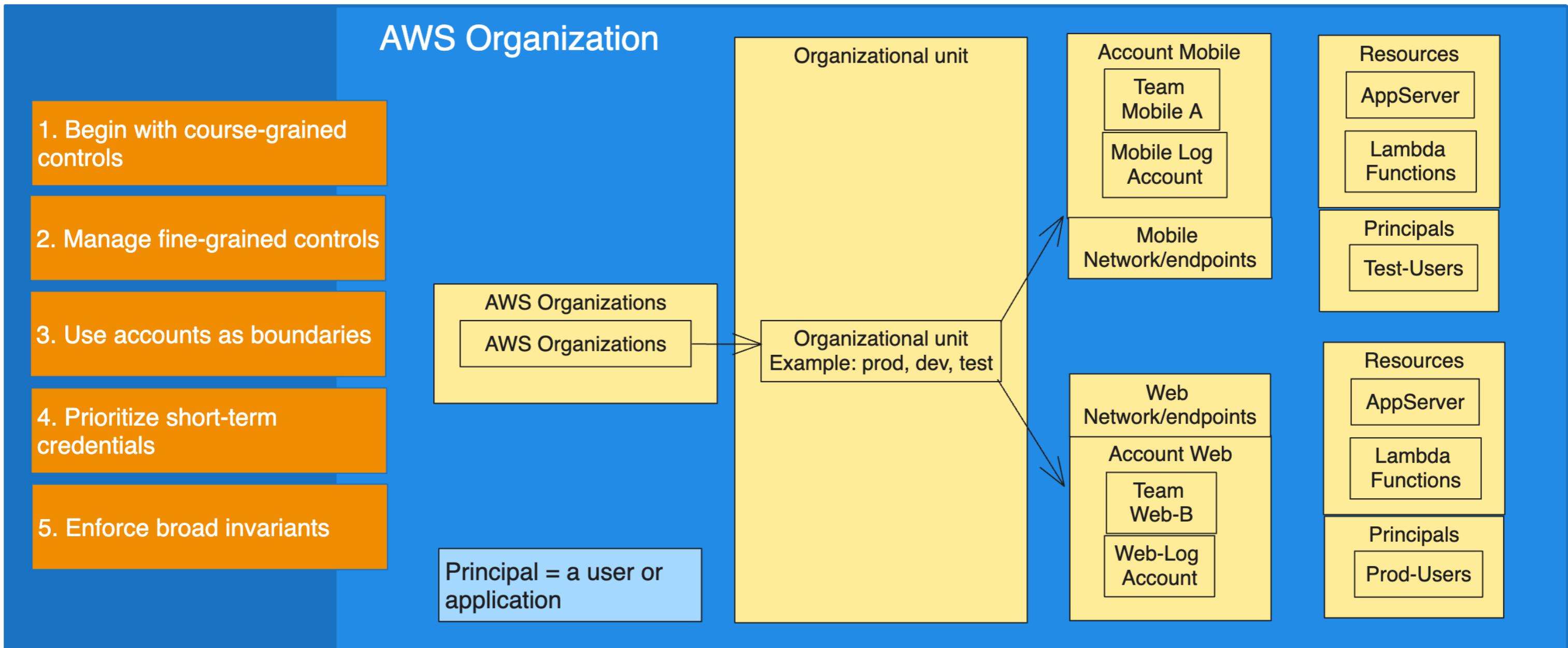
Balancing the goal

Balancing the goal

Things you don't want
Dangerous actions
Unaccountable teams
Expensive resources

Things you do want
Business to innovate
Agility to move quickly
Freedom for builders

Strategies for least privilege



Account security framework

- Root user security is critical
- grant least necessary privileges to users, groups, and computing resources
- Develop a process for credential sharing



Root user security



Password strength - %\$#%\$csnafkajhf!!#



MFA



Access keys



Group email



IAM

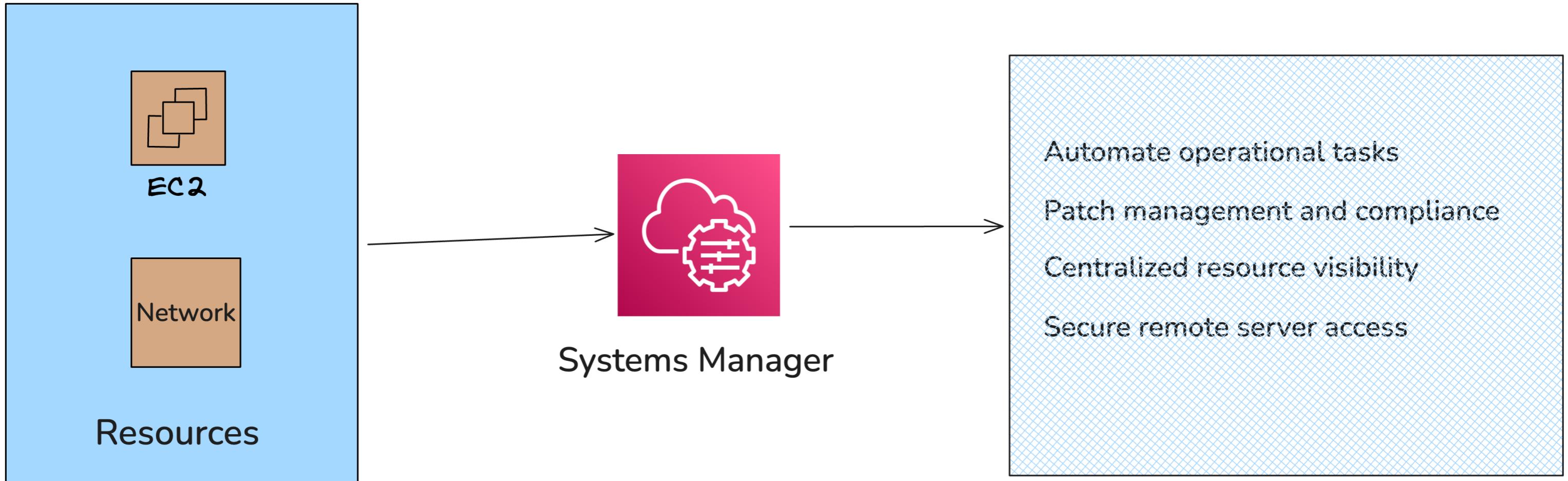
- Use a strong root user password
- Use multi-factor authentication
- Don't create access keys
- Use multi-person approval and group email

User and group security

- Enable MFA for all IAM users
- Use groups to assign permissions, not individuals
- Apply the principle of least privilege to all accounts
- Regularly rotate passwords and access keys

Resource security

- Improve visibility and control
- Maintain instance compliance against your patch, configuration, and custom policies
- Automate configuration and ongoing management of your applications



Credential security



- Manage database credentials securely
- Rotate secrets automatically
- Encrypt API keys
- Integrate with AWS services

Secrets Manager

Let's practice!

AWS SECURITY AND COST MANAGEMENT CONCEPTS

Identity and Access Management (IAM)

AWS SECURITY AND COST MANAGEMENT CONCEPTS



Dev Bhosale

Principal Data & Cloud Architect

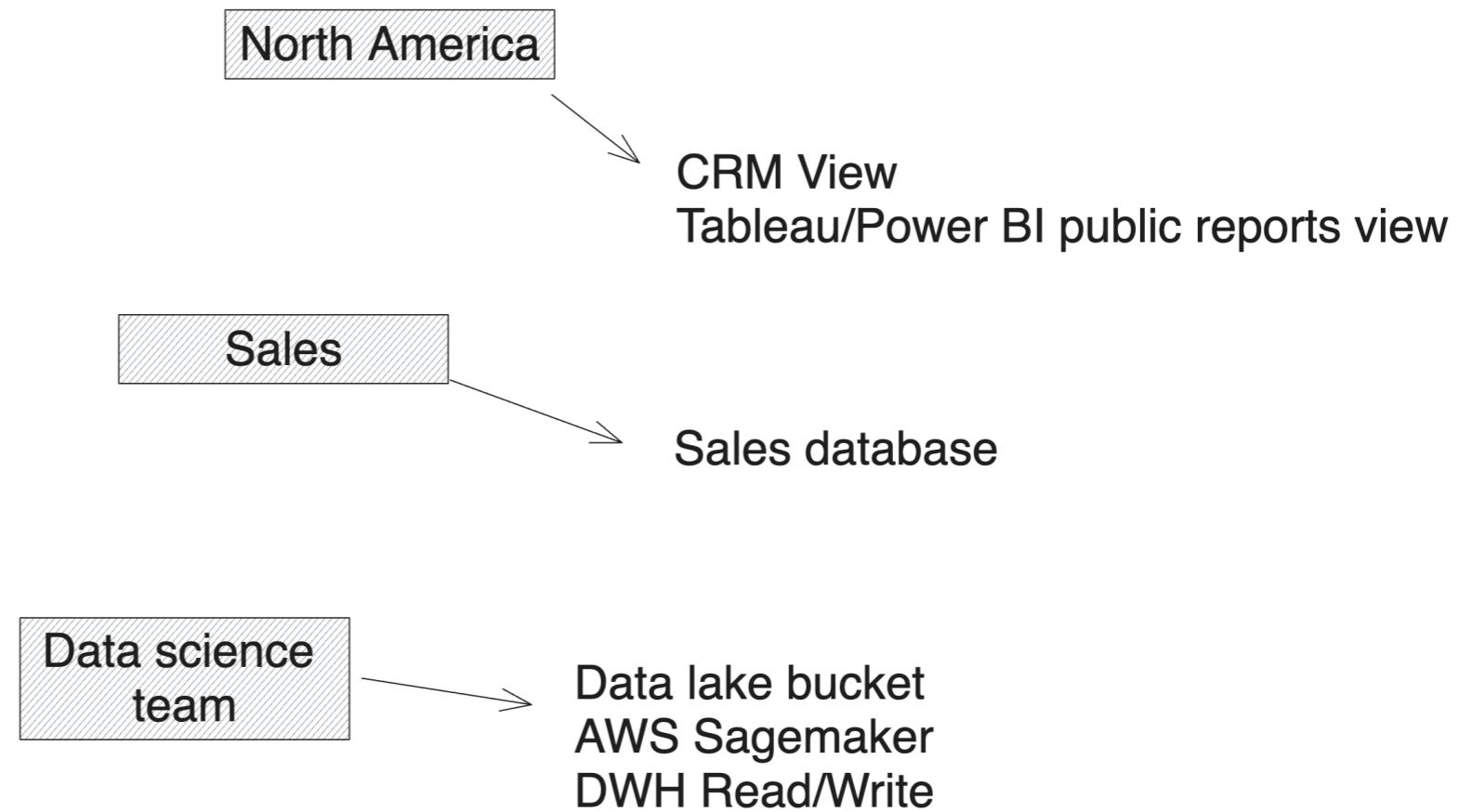
Why IAM?

Dee
A new data scientist
Sales department - North America

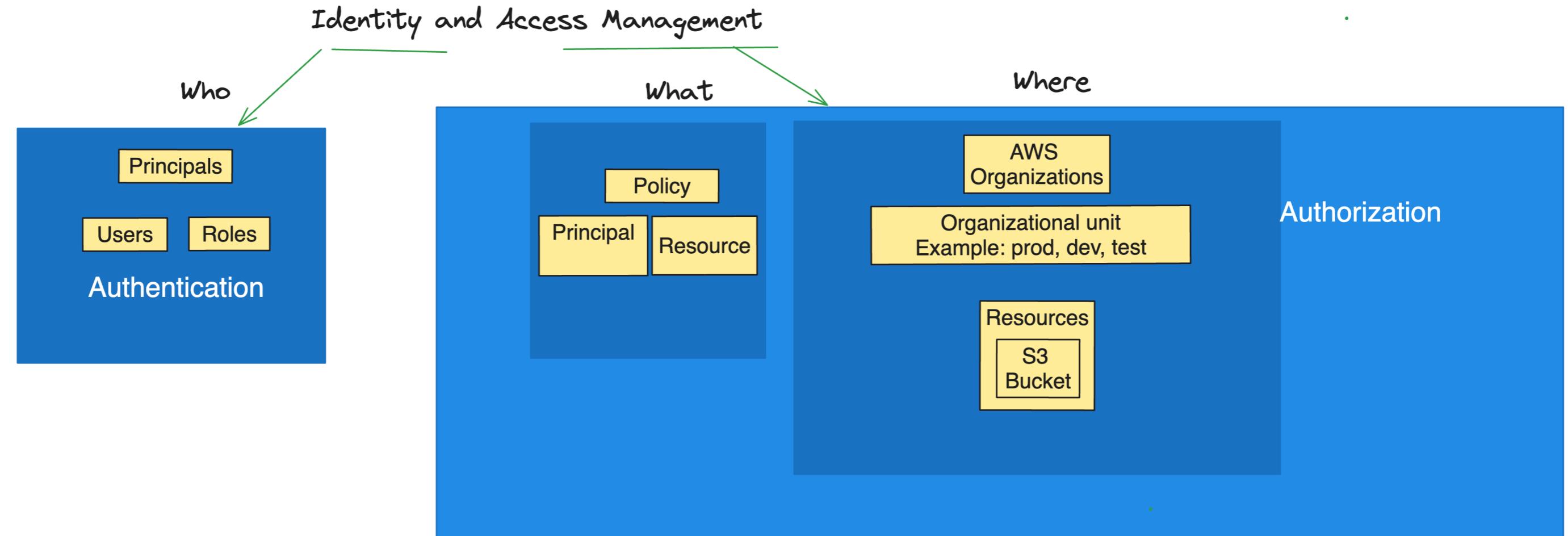


Access Request
Sales database
DWH Database
Production Read Access
CRM access
AWS console
Data lake bucket (read/write)
Tableau server
Power BI
AWS SageMaker

Simplified access management with organizational hierarchy



Who, what, and where?



Users vs. Roles

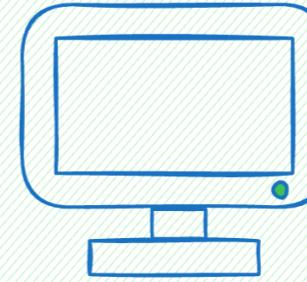
Users



Use long-term credentials

A user group is a collection of users

Roles



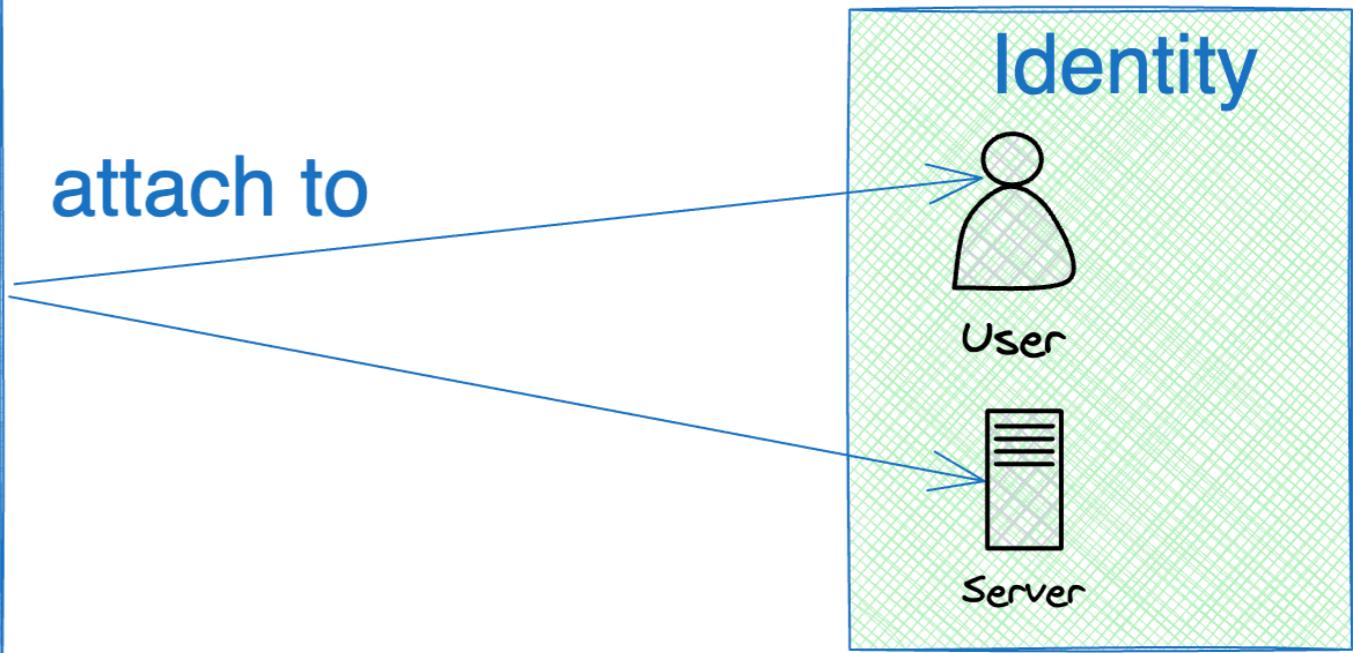
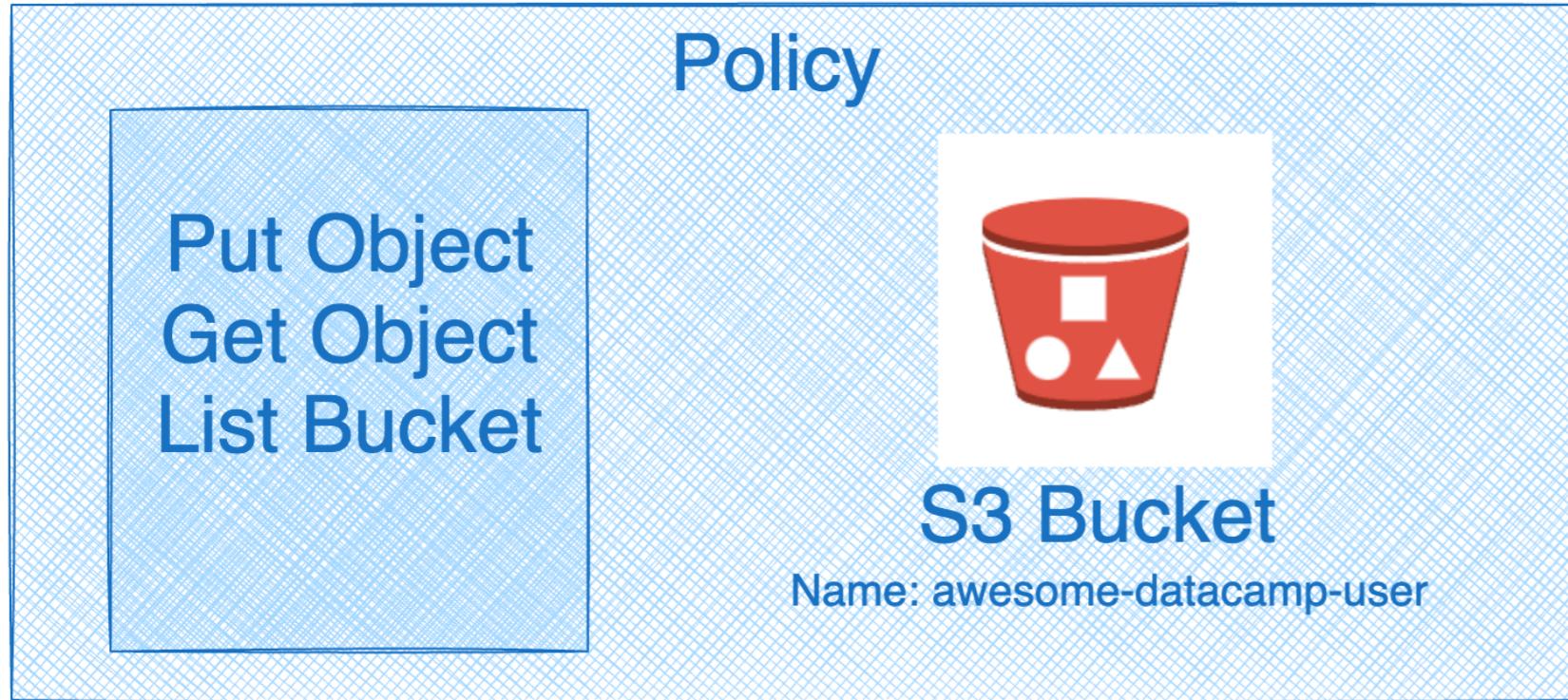
STS

Short-term credentials

Roles cannot be grouped

Assigned to machine

Policy



```
{  
  "Version": "2012-10-17",  
  "Statement": [  
    {  
      "Sid": "VisualEditor1",  
      "Effect": "Allow",  
      "Action": "s3:*",  
      "Resource": "arn:aws:s3:::awesome-datacamp-user"  
    }  
  ]  
}
```

Identity Center



- One tool to manage user access
- Create new account
- Connect to existing work accounts (e.g. Office 365, Google Apps)
- Grant access to multiple AWS accounts

AWS Identity Center

Let's practice!

AWS SECURITY AND COST MANAGEMENT CONCEPTS

Network Security in AWS

AWS SECURITY AND COST MANAGEMENT CONCEPTS

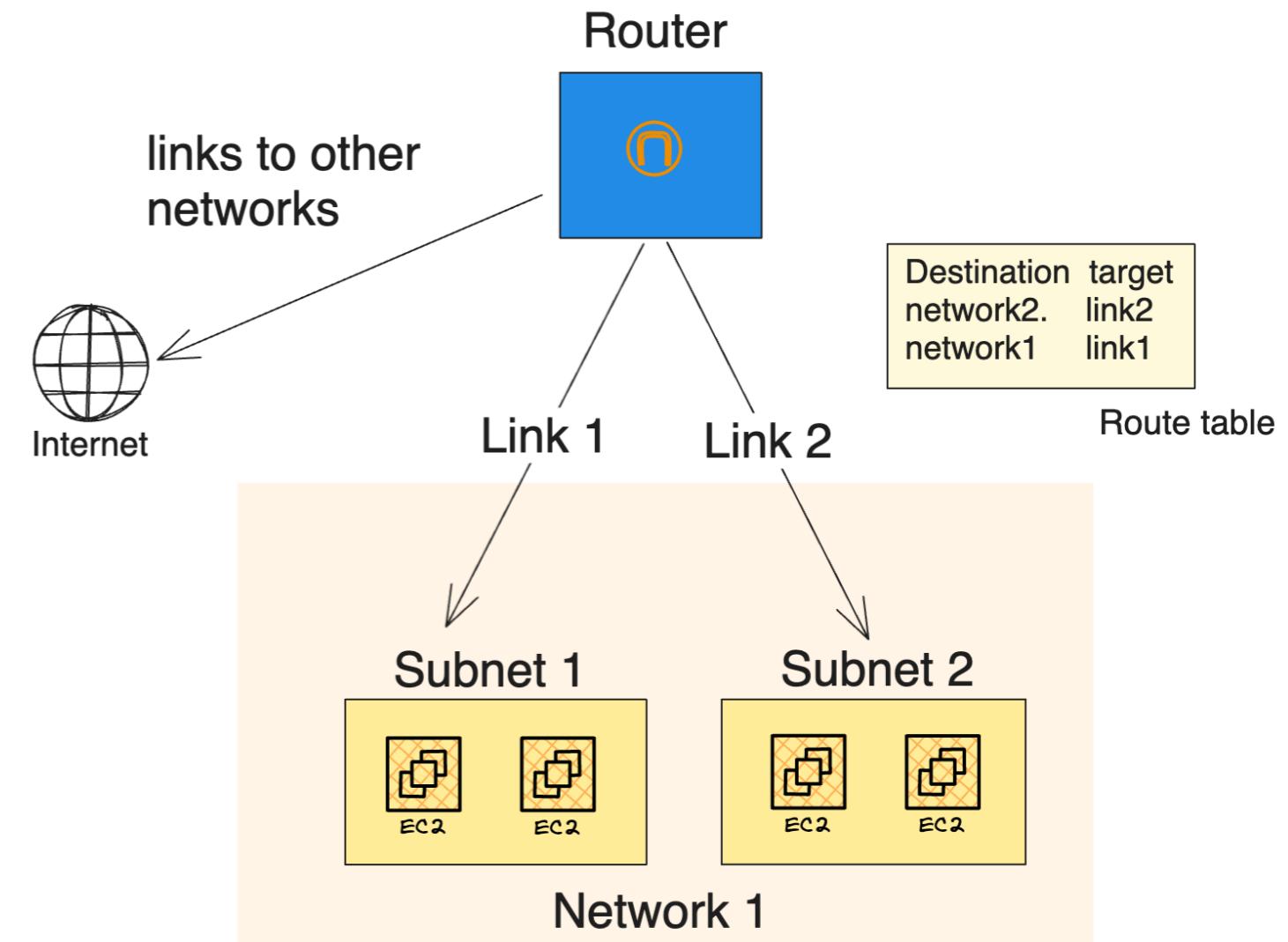


Dev Bhosale

Principal Data & Cloud Architect

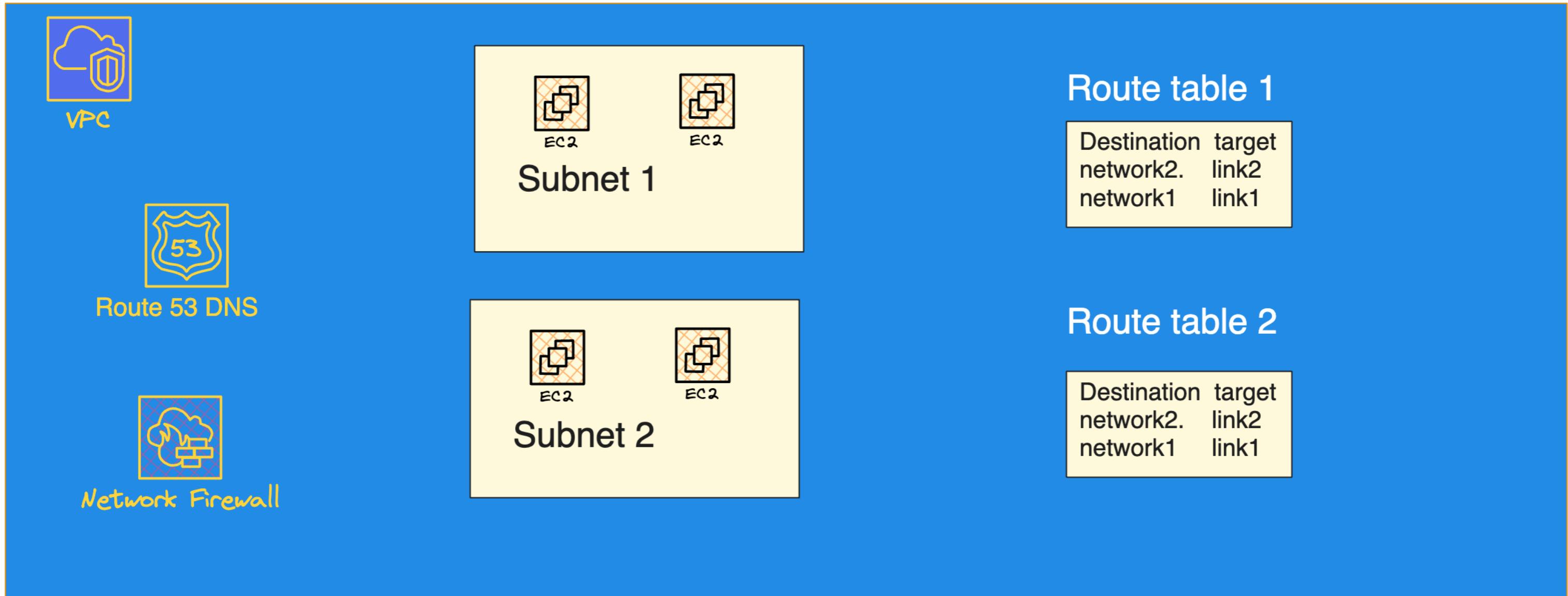
Networking basics

- A subnet contains multiple devices
- A network consists of multiple subnets
- A router routes traffic between networks using routing tables



Virtual private cloud

Components of a basic VPC



VPC security

Five steps to securing networks in AWS

- Subnet design
- Network Access Control Lists
- Firewall and WAF
- Security software

- 1 Design appropriate subnets
- 2 Isolate environments
- 3 Use Network ACLs (NACL)
- 4 Protect with a firewall
- 5 Monitor flow logs

NACL, firewall, and WAF

Feature	AWS Firewall	NACL	AWS WAF
Scope	Regional or VPC-level	Subnet-level	Application-level
Statefulness	Stateful	Stateless	Stateful
Default Rules	Managed rules available	Deny unless allowed	Allow, block, or count based on rules
Cost	Charged per usage	No additional cost	Charged per request & rules
Best for	High-level security control	Broad network control	Protecting web applications

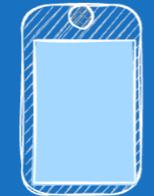
AWS Marketplace

What is AWS Marketplace?

Find, subscribe to, deploy, and govern - Software, data, and professional services



Broad product
selection



Fast, flexible
procurement



Easy deployment



Centralized governance

Let's practice!

AWS SECURITY AND COST MANAGEMENT CONCEPTS

Compute and data security

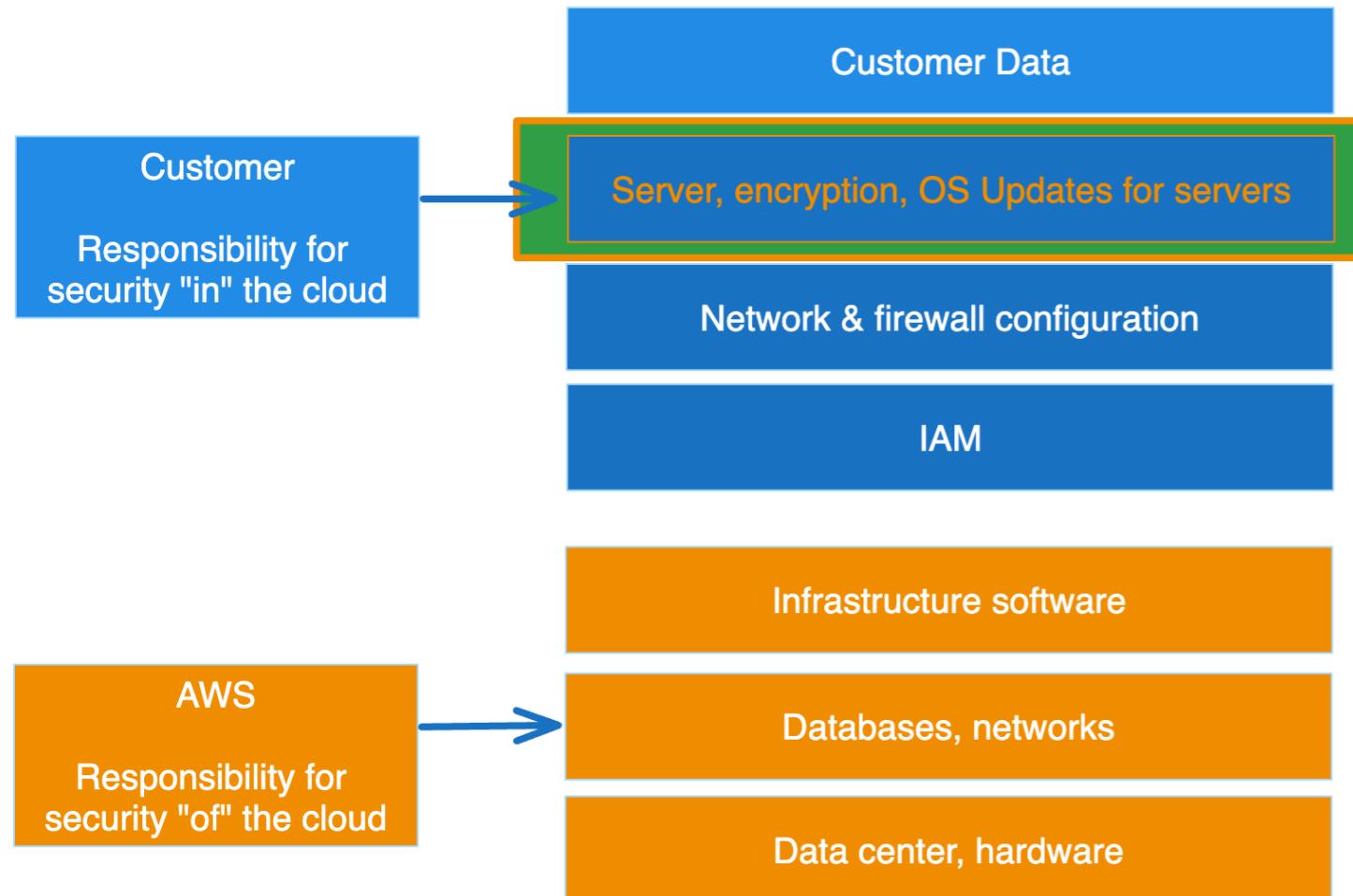
AWS SECURITY AND COST MANAGEMENT CONCEPTS



Dev Bhosale

Principal Data & Cloud Architect

Securing customer data



- Protection of customer data is a customer responsibility
- It is necessary to secure compute, network, and storage

Compute security strategies

- Use SSH keys instead of passwords
- Update OS with latest patches
- Control access to servers using security groups
- Use IAM roles instead of stored credentials
- Use security groups

Compute Security



Keep credentials secure



Update Operating System



Manage access
using security groups



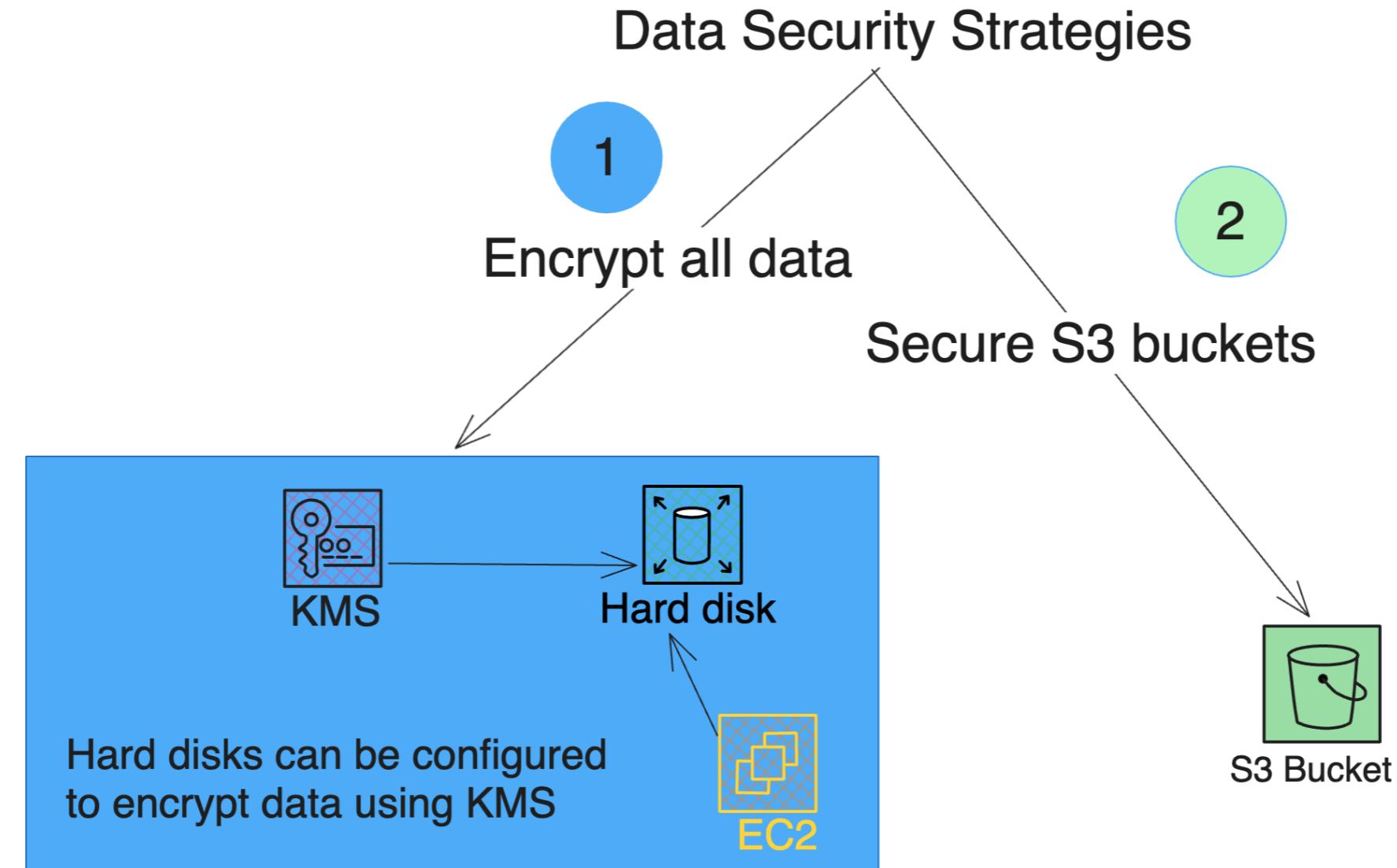
Use IAM Roles

Security groups



Feature	NACL (Network Access Control List)	Security Groups
Scope	Subnet-level	Instance-level
Statefulness	Stateless	Stateful
Default Rules	Denies all unless allowed	Allows outbound
Best for	Broad network layer control	Granular instance

Data security strategies



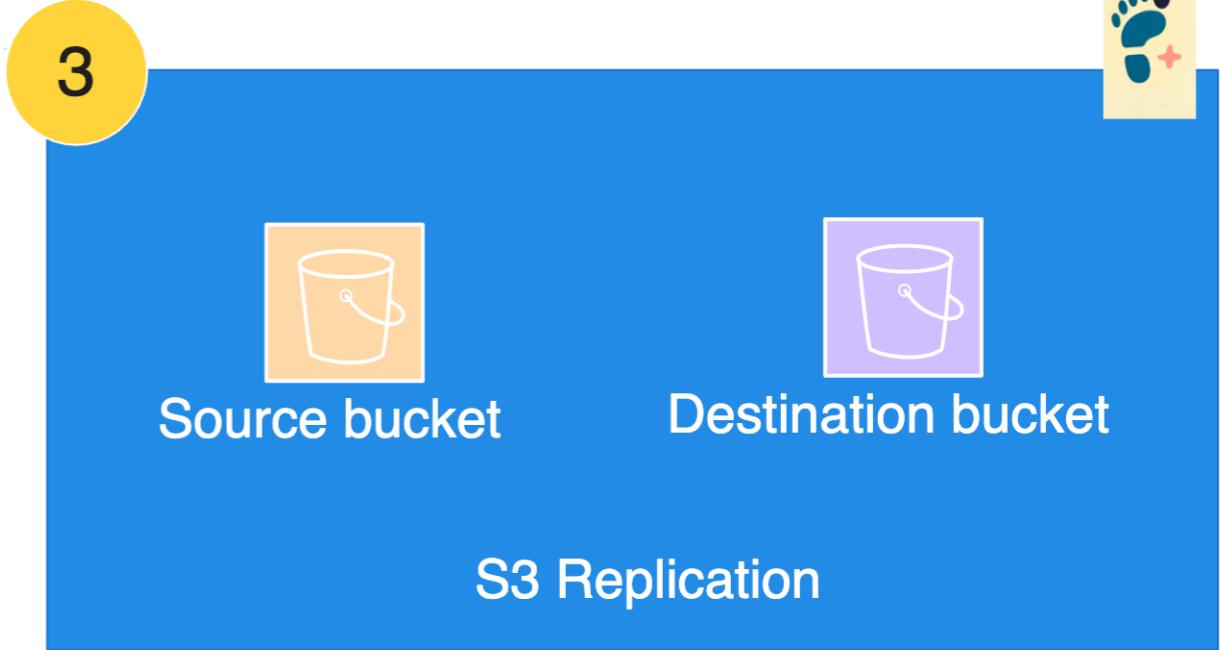
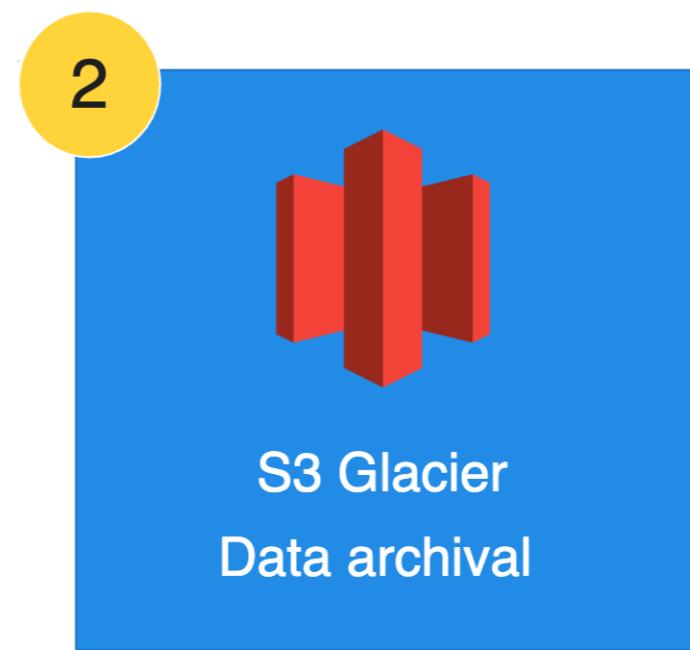
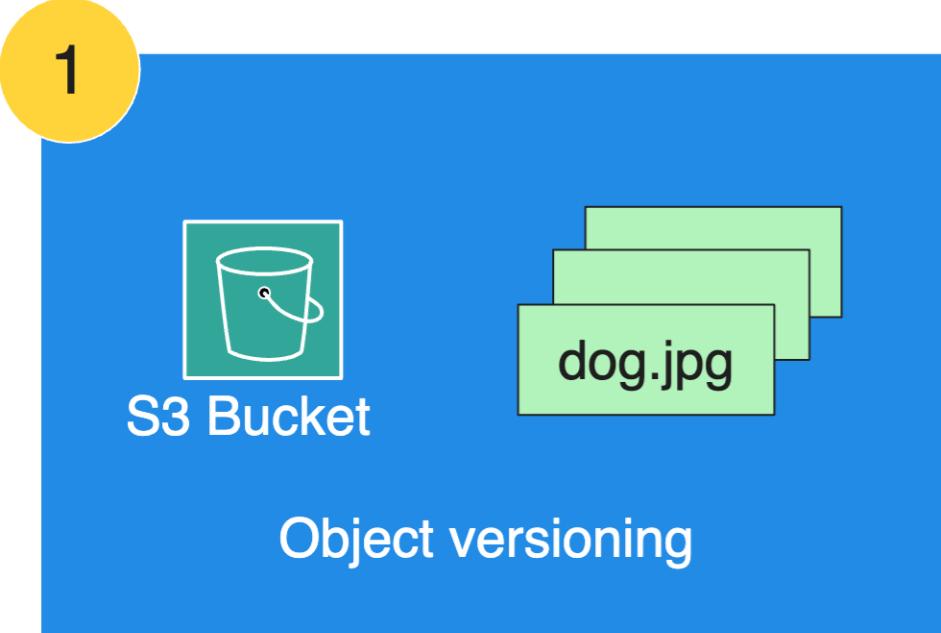
S3 public access and recovery

The screenshot shows the AWS S3 console interface. At the top left, the navigation path is "Amazon S3 > Buckets > awesome-datacamp-user". The main title is "awesome-datacamp-user" with an "Info" link. Below the title is a navigation bar with tabs: "Objects", "Properties", "Permissions" (which is highlighted with a blue border), "Metrics", and "Management". To the right of the tabs is a small yellow icon featuring a cartoon owl wearing a blue hard hat. The main content area is titled "Permissions overview". Under the "Access" section, the status "Bucket and objects not public" is displayed. A large button labeled "Block public access (bucket settings)" is prominently featured. Below this button, a detailed description explains that public access is granted through ACLs and bucket policies, and that turning on "Block all public access" will ensure applications work correctly. A "Learn more" link with a blue arrow icon is provided. At the bottom of the page, there is a link to "Block all public access".

- S3 public access enables anyone to read data
- Public access can be turned off using a setting

Encryption at-rest

- Automatic Encryption
- Customer-Controlled Keys
- Compliance & Security



Security resources



Security Resources

Articles and videos covering the most frequent questions and requests from AWS customers



Security blog

Deep-dive on security best practices, how-to guides, and customer stories



User guides, code samples, SDKs & toolkits, tutorials, API & CLI references



Security Hub

Collects security data across accounts, services, and supported third-party products and helps you analyze your security trends

Let's practice!

AWS SECURITY AND COST MANAGEMENT CONCEPTS