

I AWS Accounts:

Isolate Risk:

(Isolated Billing Account)

Identity Store & Permission

root user is a principal that can authenticate to the account and is the only one auth to do so

(Access key-pair)
(auth)

Fault isolation entities → AZ

storage & content-distribution

Edge

(cant deploy EC2, RDS in e)

HA v/s FT v/s DR

Not remove
But recover
from fault/
disaster

(Continue service)

(AutoScaling)

multi-AZ

(highly Resilient)

(will be disruption)

Redundancy

((active-active))

(Survive failure)

(parallel)

\$ ↑

New working
for critical data

Applⁿ layer LB has all 7

Netw layer has lower 3 //

RPO/RTO : Point / Time

(Time b/w last recoverable copy and Disaster) ((rec. Time objective))

RTO: when disaster occurred and when system can be restored

to operational state,

(Not standby devices)

Data Persistence:

Instance store, ElastiCache
(temp. key-value)

Super-fast & ephemeral

Persistent:

Start, Stop, Restart

Transient:

Queue

II ACCOUNTS

IAM: → access resources & services

Authenticate → Users & PW

Access Key

ID

Secret
Access Key

Long-Term
access credentials

SSH key
HTTP key

Code Commit

User & Roles

Real
Identities

① No access

② Implicit DENY

③ DENY over ALLOW

5000 IAM users

To get around used
identity provider

Group ← contains users
↑ can't login as group

(★ Credential Report)

Effect Action Resource

S3 resource?

AWS ↑

arn:aws:s3:::*

use managed policy

not inline

Condition: { "StringLike": { "s3:prefix": ["testuser/*"] }

IAM Variables **

((User & Resource policies are evaluated))

((Principal ← req. in resource policy))

((To many different identities))

all identities access to a resource,

Role: Trust policy
who can assume
this role

Permission policy
what access?

Cannot revoke/expire
current tokens

bucket-owner-full-control

condition ↑

S3 Access logs: Using ACL

Every object can be changed
by owner. Bucket v/s Obj owner

III) Organizations

All Features

Consolidated
Billing

SCP's

Root account
↓
JSON doc → OU
↓
Account

↓ downwards

(Only Allow/DENY
not Grant access)

Cannot operate in master account
don't keep resources

Nobody including
account root user



(Service)
Account Limits:

Trusted Advisors

Core checks:

Business / Enterprise

(Support API)

(proactive
programs)

in Enterprise

Well Archi,

Infra Event Mgmt