

4) bucket permissions for public access,
Security groups with unrestricted ports.

Fault Tolerance:

EBS snapshots age, availability zone
balance.

ASG Multi-AZ, RDS Multi-AZ, ELB
Config.

Service Limits.

IAM Section *

IAM: Identity and Access Management,
Global Service

Root account created by default.

Groups only contain users and not other
groups.

Permissions: Users / Groups can be assigned JSON
documents called policies. (they define the
permissions of the users).

- Apply least privilege principle
- A user can be in more than one group.
- IAM Policies structure consists of: Version, Id, Statement, Sid, Effect, Principal, Action, Resource, Condition.

- Multi-Factor Authentication (MFA): To protect Root Accounts & IAM Users

- MFA = Password you know + Security device you own.

- MFA device options in AWS:

1) Virtual MFA device:
 Google Authenticator (phone only) } Support for multiple tokens on a single device
 Authy (multi-device)

2) Universal 2nd factor (U2F) Security Key:
 Yubikey by Yubico (3rd party): Support for multiple root & IAM users using a single security key.

3) Hardware Key Fob MFA device: Provided by Gemalto (3rd Party).

4) Hardware Key Fob MFA device for AWS Gov Cloud (US) - Provided by SurePass ID (3rd Party).

- How can users access AWS?

1) AWS Management Console: Password + MFA

2) CLI - Protected by access keys

3) SDK - Protected by access keys

- Access keys are generated by AWS console.

- AWS SDK - Language specific APIs (set of libraries), access and manage AWS services programmatically.

1) IAM security tools:
- IAM Credentials Report (account level)
A report that lists all your account's

users and the status of their various credentials.
2) IAM Access advisor (user-level).
Shows the service permissions granted to a user.

We use this info to review your policies.
Assign users to groups and assign permissions to groups.

Roles are for EC2 instances or other AWS services

Audit: IAM Credentials Report & IAM Access advisor.

→ How to choose an AWS Region?

- 1) Compliance
- 2) Proximity
- 3) Available Services
- 4) Pricing.

→ AWS Global Services:

- 1) IAM
- 2) Route 53 (DNS Service)
- 3) CloudFront (Content Delivery Network)
- 4) WAF (Web Application Firewall)

Region - Scoped services.

EC2 (IaaS)

1) Elastic Beanstalk (PaaS)

Lambda (FaaS)

Recognition (SaaS).