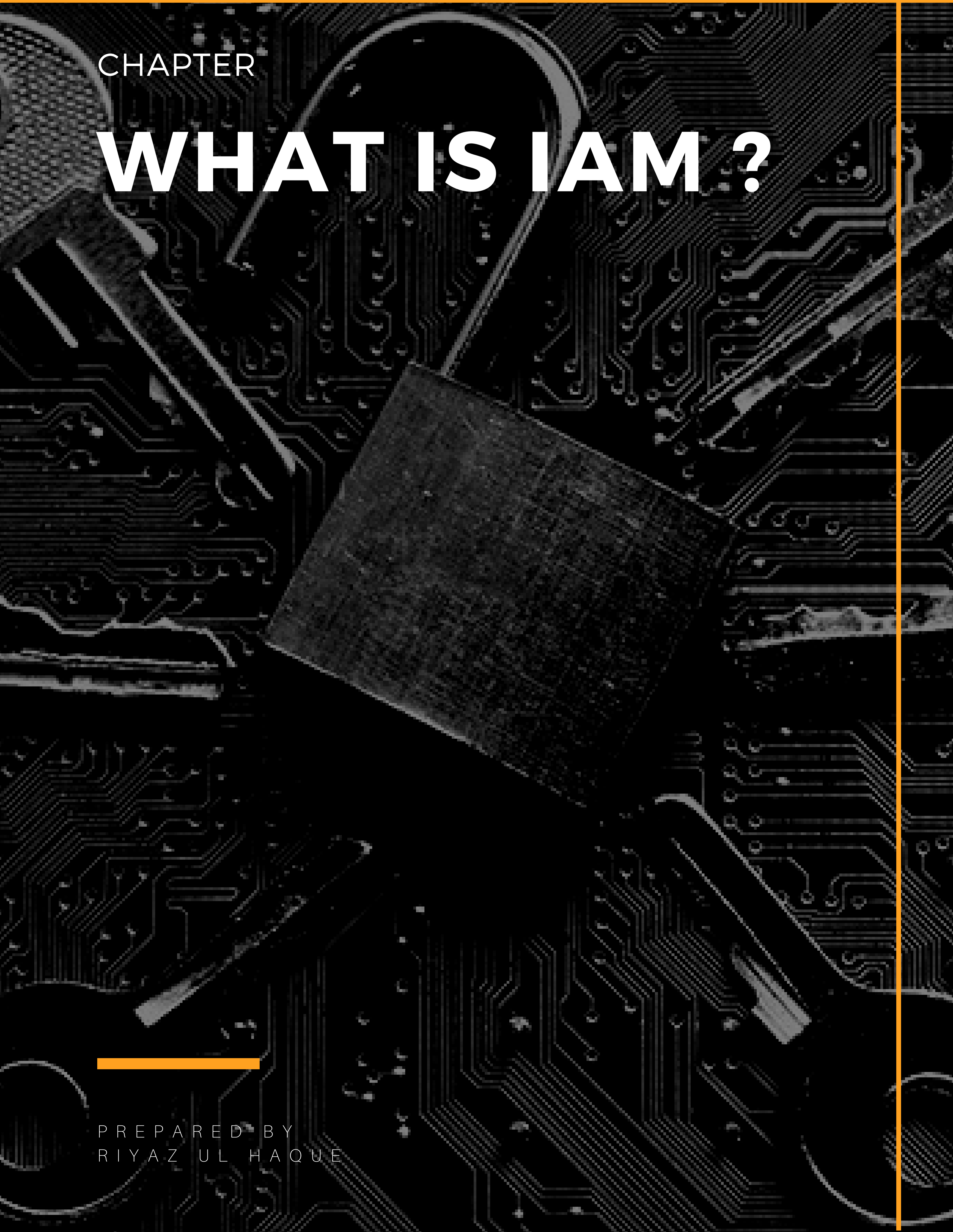
EXPLORING THE CLOUD WITH aws

IAM

PROPOSED
BY RIYAZ UL HAQUE

2018 | CONSULTADD



CHAPTER

WHAT IS IAM ?

PREPARED BY
RIYAZ UL HAQUE

DEFINITION

AWS Identity and Access Management (IAM) is a web service that helps the user to securely control their access to AWS accounts and resources. Moreover, you use IAM to control who is authenticated (signed in) and authorized (has permissions) to use resources.

Common Uses:

- Users
- Groups
- IAM Access Policies
- Roles

Root User
When you first create an Amazon Web Services (AWS) account, you begin with a single sign-in identity that has complete access to all AWS services and resources in the account.
In simple, The user created when you created the AWS account is called the 'Root User".

For all the user (besides the root user), permission must be given that grant access to AWS services

IAM FEATURES

IAM gives you the following features:

- Shared access to your AWS account.
- Granular permissions.
- Secure access to AWS resources for applications that run on Amazon EC2.
- Multi-factor authentication (MFA).
- Identity Federation.
- Identity information for assurance.
- PCI DSS Compliance.
- Integrated with many AWS services.
- Eventually Consistent.
- Free to use.

ACCESSING IAM

You can work with AWS Identity and Access Management in any of the following ways.

- AWS Management Console.
- AWS Command Line Tools.
- AWS SDKs.
- IAM HTTPS API.

IAM INITIAL CONFIGURATION AND SETUP

When a new AWS root account is created, it is "best practice" to complete the task listed in IAM under "Security Status".

Security Status Include:

- Delete your root access key.
- Activate MFA on your root account.
- Create Individual IAM user.
- Use groups to assign permissions.
- Apply an IAM password policy.

IAM BEST PRACTICES

IAM is the guidelines that recommend settings, configurations, and architecture for the purpose of having a high level of security, accessibility, and efficiency.

WHAT IS MULTI FACTOR AUTHENTICATION

PASSWORD
?
username
••••••••
Login
+
PROOF
Is that you?
=
ACCESS
Success!

fig:01

Multi-factor authentication (MFA) is a method of confirming a user's claimed identity in which a user is granted access only after successfully presenting 2 or more pieces of evidence (or factors) to an authentication mechanism.

When you name MFA , AWS ask

> - ONE TIME PASSCODE TO SIGN IN
>
> - HARDWARE OR VIRTUAL MFA DEVICE
>
> - AWS ADMIN MUST ENABLE MFA

MFA - MOTIVATION, BENEFITS & CHALLENGES

- MOTIVATION

There are typically three primary motivations for why people and organizations use MFA:

- Usability,
- Compliance and
- Security.

- BENIEFITS

The benefits for MFA align very closely to the motivations for having multi-factor authentication.

- Improve Security
- Achieve Compliance
- Increase Flexibility and Productivity

- CHALLENGES

While there are well-known benefits for MFA, as with any technology, there will be potential challenges as well. Below we have listed common sticking points for MFA.

- Cost
- Usability
- Backup Options
- Lack of Bandwidth
- Technical Gaps
- Complexity

HOW IAM WORKS ?

Before you create users, you should understand how IAM works. IAM provides the infrastructure necessary to control authentication and authorization for your account. The IAM infrastructure includes the following elements.

- Principal
- Request
- Authentication
- Authorization
- Actions
- Resources

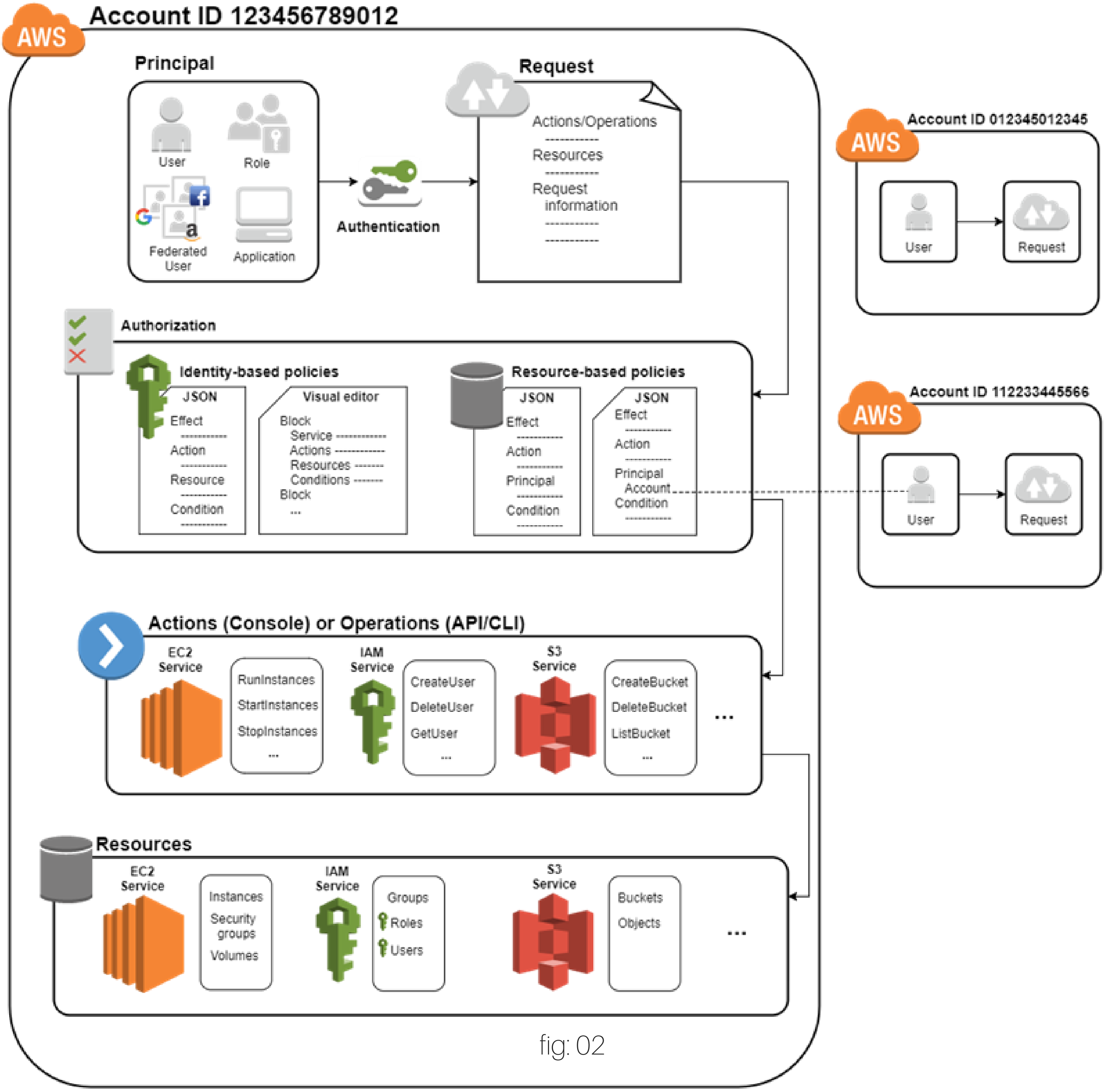


fig: 02

KEY POINTS TO REMEMBER

- Centralized control of your AWS account
- Shared access to your AWS account
- Granular permission
- Identity Federation
- Multifactor Authentication
- Provide temporary access to users/devices and services where necessary
- Integrates with different AWS services
- Allows you to setup your own password rotation policy

CRITICAL TERMS

1- USER: End Users (Think of people)

2- GROUPS: A collection of users under one set of permission

3- ROLES: You create roles and can then assign to AWS resources

4- POLICIES: A document that defines one or more permissions