Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

What is IAM?

- **IAM** (Identity & **A**ccess **M**anagement) is where you manage your AWS users and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***IAM Access Policies***
  - ***Roles***

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- By default, any new users you create in the AWS account are created with ***NO*** access to any AWS services (except the ability to log in).

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

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines that recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility and efficiency.

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

- Those tasks include:
  - Delete your root access keys
  - Activate MFA on your root account
  - Create individual IAM users
  - User groups to assign permissions
  - Apply an IAM password policy

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

Activate MFA on your Root Account:

- What is **MFA**?
  - **MFA** is an abbreviation for **M**ulti-**F**actor **A**uthentication.
  - It is an additional layer of security on your root account that is provided by a 3rd party.
  - And it takes the form of a continually-changing, random six digit code that you will need to input (in addition to your password) when logging into your root account.

- How do I get the **MFA** code?
  - **Virtual MFA Device:**
    - Smartphone or tablet.
    - Commonly used app (iOS & Android): Google Authenticator.
  - **Hardware Key Fob:**
    - Small physical device with a display that you can attached to your keychain.
    - Order it directly from AWS.

Lesson Navigation

Start

What is IAM?

IAM Setup

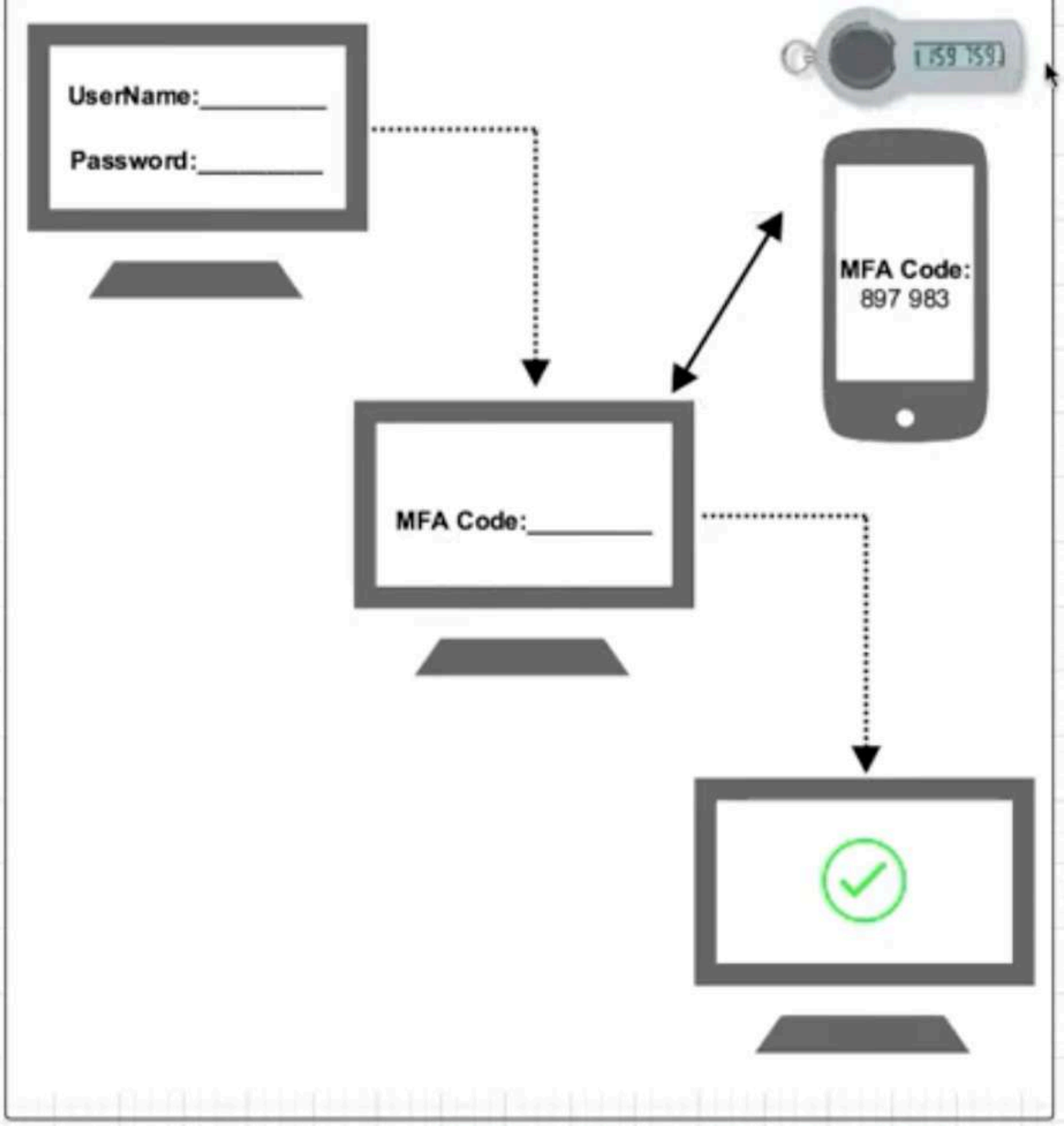
Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main



Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines that recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility, and efficiency.

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

- Those tasks include:
  - Delete your root access keys
  - Activate MFA on your root account
  - Create individual IAM users
  - User groups to assign permissions
  - Apply an IAM password policy

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

Create Individual IAM Users:

- AWS ***best practice*** is to **NEVER** use your root account for day-to-day use.
- If you want full admin access for yourself, create an IAM user and attach the "**AdministratorAccess**" policy to it.
- Then use that account as your daily driver.

Quick Reference

Current Section = *IAM*

MORE -> 1 2 3 4 5 6 7 8 9 10 11

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines that recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility and efficiency.

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

- Those tasks include:
  - Delete your root access keys
  - Activate MFA on your root account
  - Create individual IAM users
  - User groups to assign permissions
  - Apply an IAM password policy

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

Use Groups to Assign Permissions:

- It can often be more convenient and efficient to set up groups and assign permissions to the group rather than manage each user individually.

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines for recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility and efficiency.

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

- Those tasks include:
  - Delete your root access keys
  - Activate MFA on your root account
  - Create individual IAM users
  - User groups to assign permissions
  - Apply an IAM password policy

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

Apply an IAM Password Policy:

- A password policy dictates the format and expiration rules that must be followed when a user creates or modifies their password.

- These rules include password:
  - Length
  - Case requirements
  - Number requirements
  - Non-alphanumeric requirements
  - Password expiration
  - Password reuse
  - User rights to change their own password
  - Administrator reset requirements

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

IAM Initial Configuration:

- ***AWS Best Practices:*** Guidelines that recommend settings, configurations and architecture for the purpose of having a high level of security, accessibility and efficiency.

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

- Those tasks include:
  - Delete your root access keys
  - Activate MFA on your root account
  - Create individual IAM users
  - User groups to assign permissions
  - Apply an IAM password policy

Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

What is IAM?

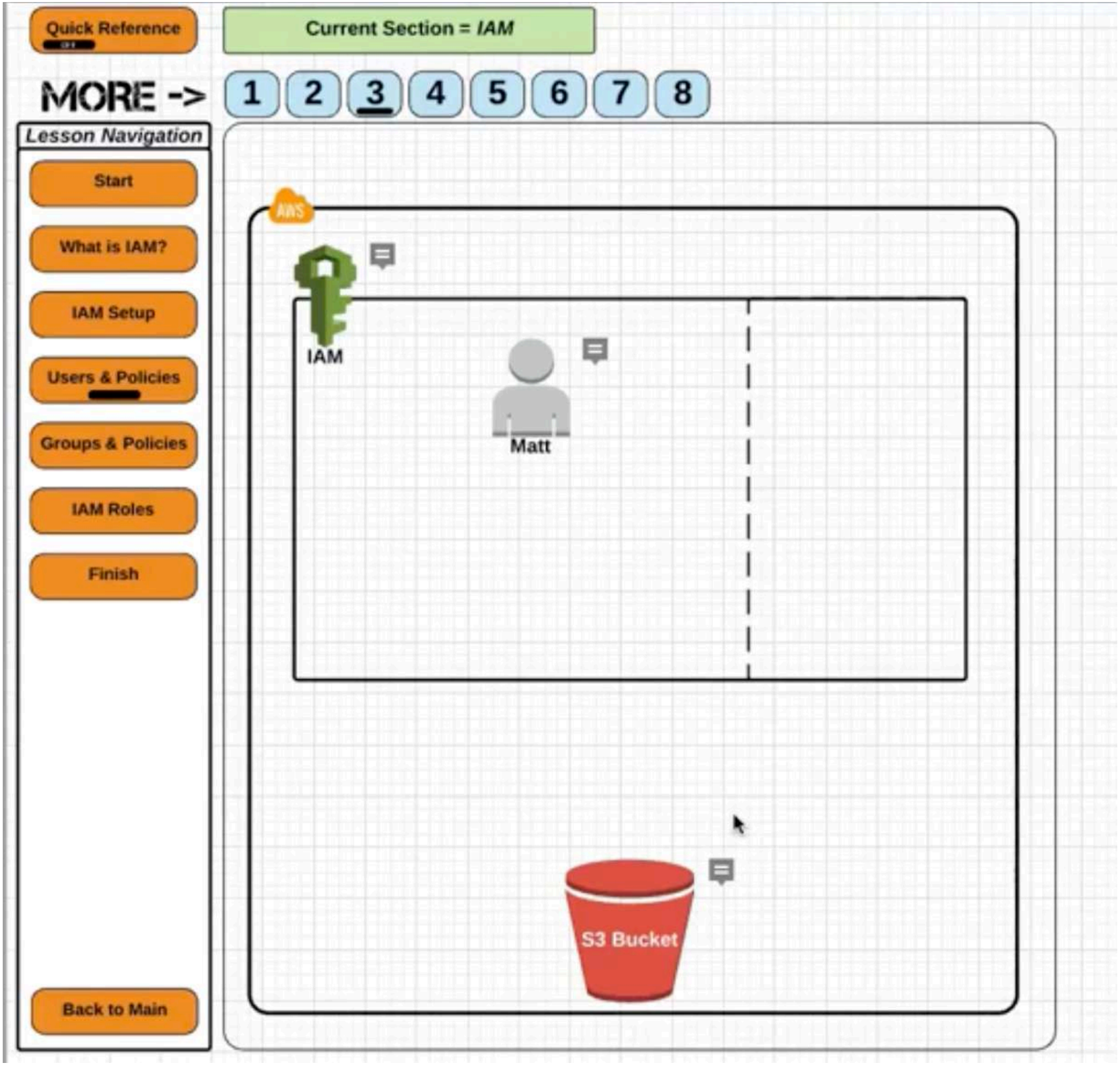
- **IAM** (Identity & **A**ccess **M**anagement) is where you manage your AWS users, and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - *Users*
  - ***Groups***
  - *IAM Access Policies*
  - ***Roles***

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- Any new or additional users you create in the AWS account are created with ***NO*** access to anything by default (except the ability to log in).


Quick Reference
Current Section = IAM
MORE ->
1
2
3
4
5
6
7
8
Lesson Navigation
Start
What is IAM?
IAM Setup
Users & Policies
Groups & Policies
IAM Roles
Finish
Back to Main
AWS
IAM
Matt
S3 Bucket

Quick Reference

Current Section = *IAM*

MORE ->

Lesson Navigation

Start

What is IAM?

IAM Setup

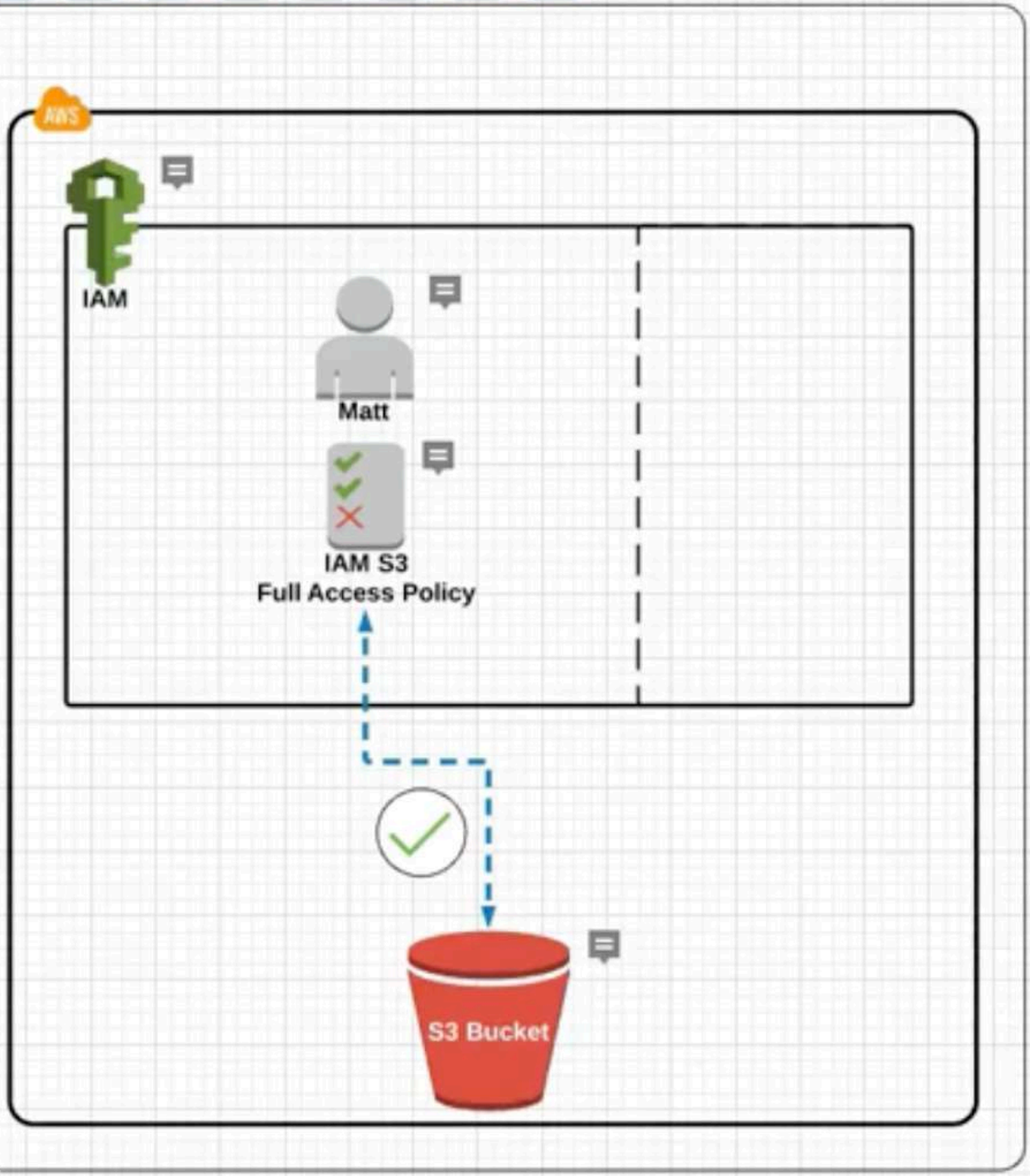
Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main



Quick Reference

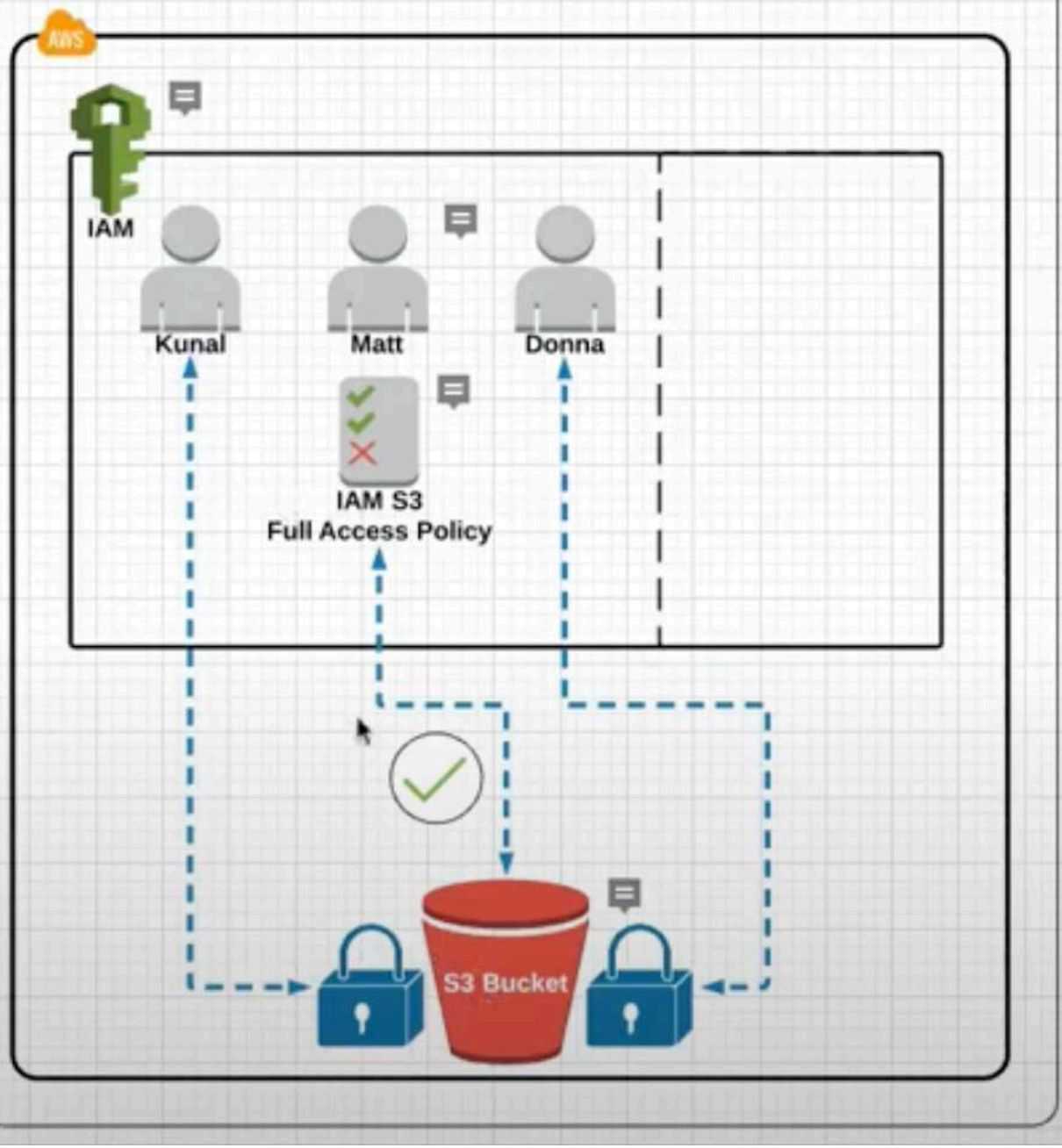
Current Section = *IAM*

MORE -> 1 2 3 4 5 6 7 8

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main



Quick Reference

Current Section = *IAM*

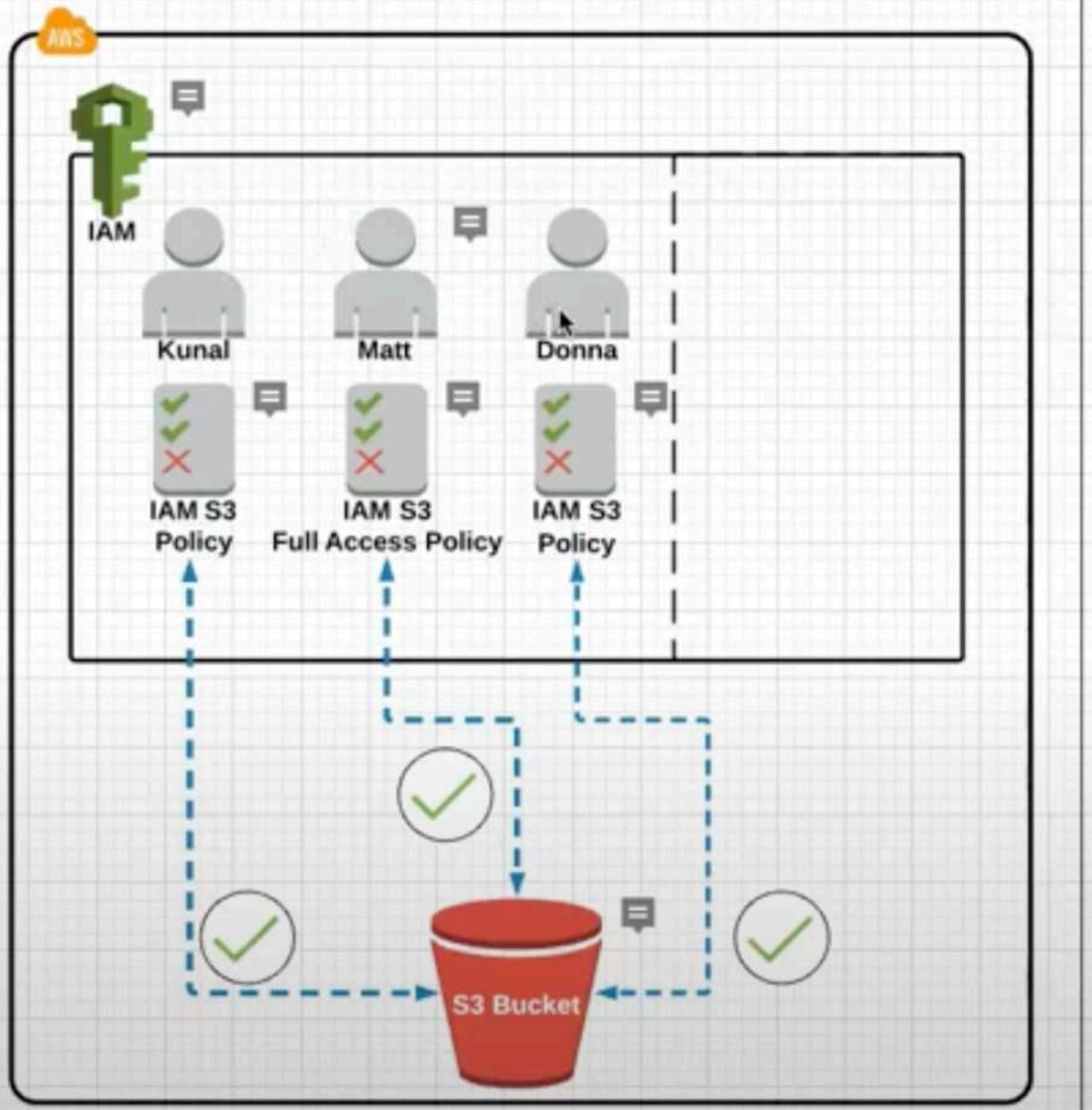
MORE ->

1 2 3 4 5 6 7 8

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main



Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main

What is IAM?

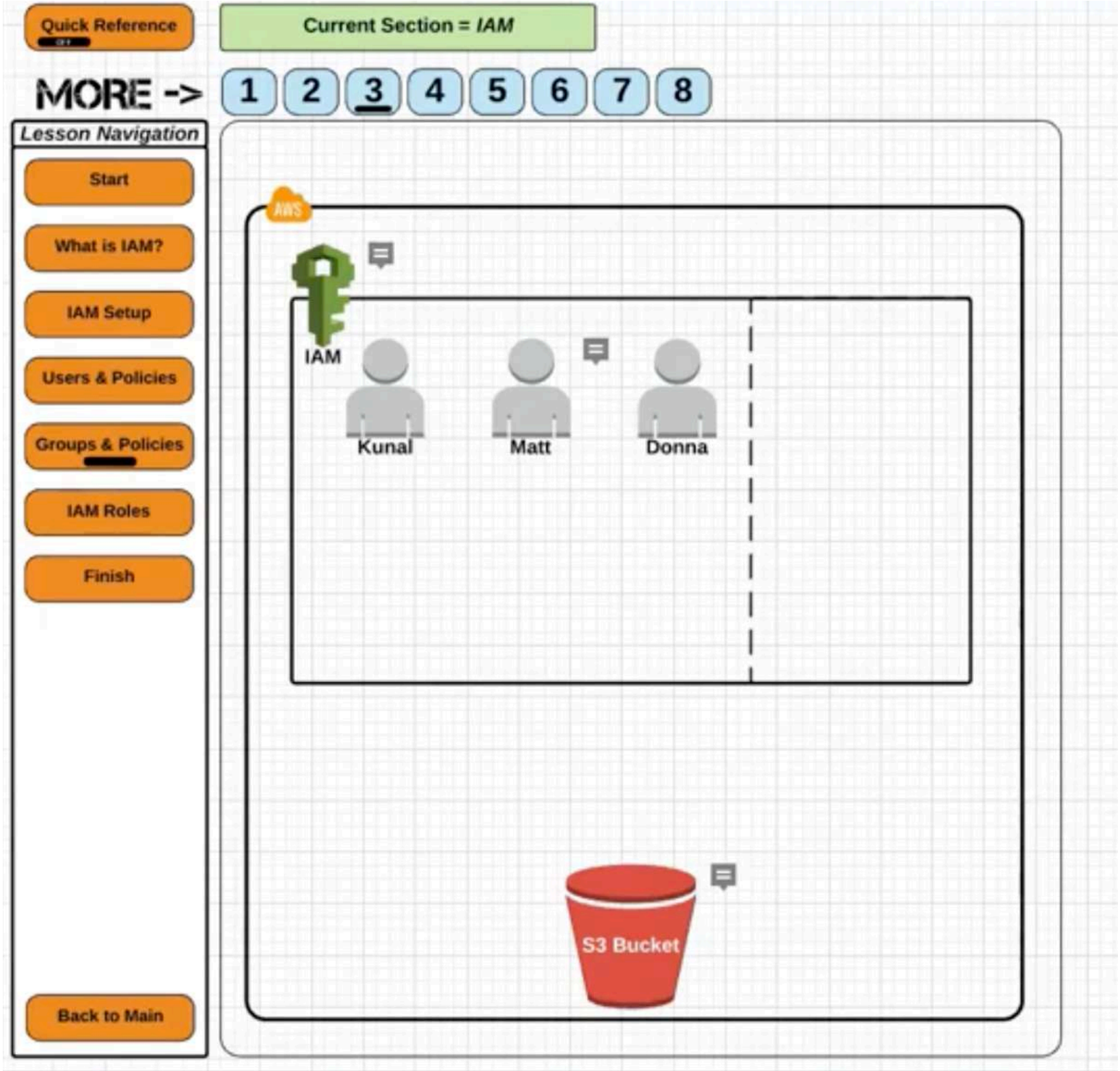
- **IAM** (Identity & **A**ccess **M**anagement) is where you manage your AWS users and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - ***Users***
  - *Groups*
  - *IAM Access Policies*
  - ***Roles***

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- Any new or additional users you create in the AWS account are created with ***NO*** access to anything by default (except the ability to log in).


Quick Reference
Current Section = IAM
MORE ->
1
2
3
4
5
6
7
8
Lesson Navigation
Start
What is IAM?
IAM Setup
Users & Policies
Groups & Policies
IAM Roles
Finish
Back to Main
AWS
IAM
Kunal
Matt
Donna
S3 Bucket

Quick Reference

Current Section = *IAM*

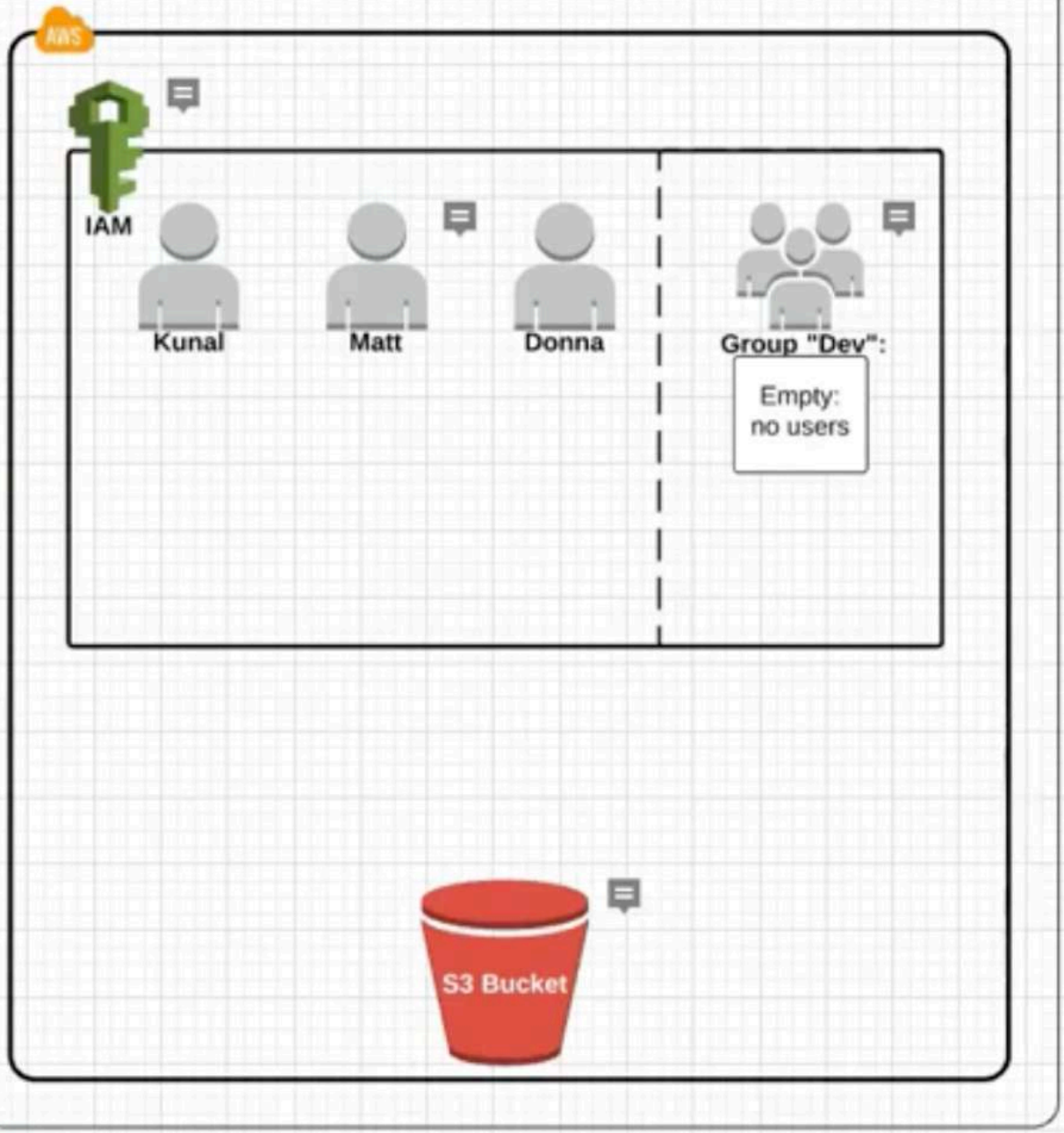
MORE ->

1 2 3 4 5 6 7 8

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main



Quick Reference

Current Section = *IAM*

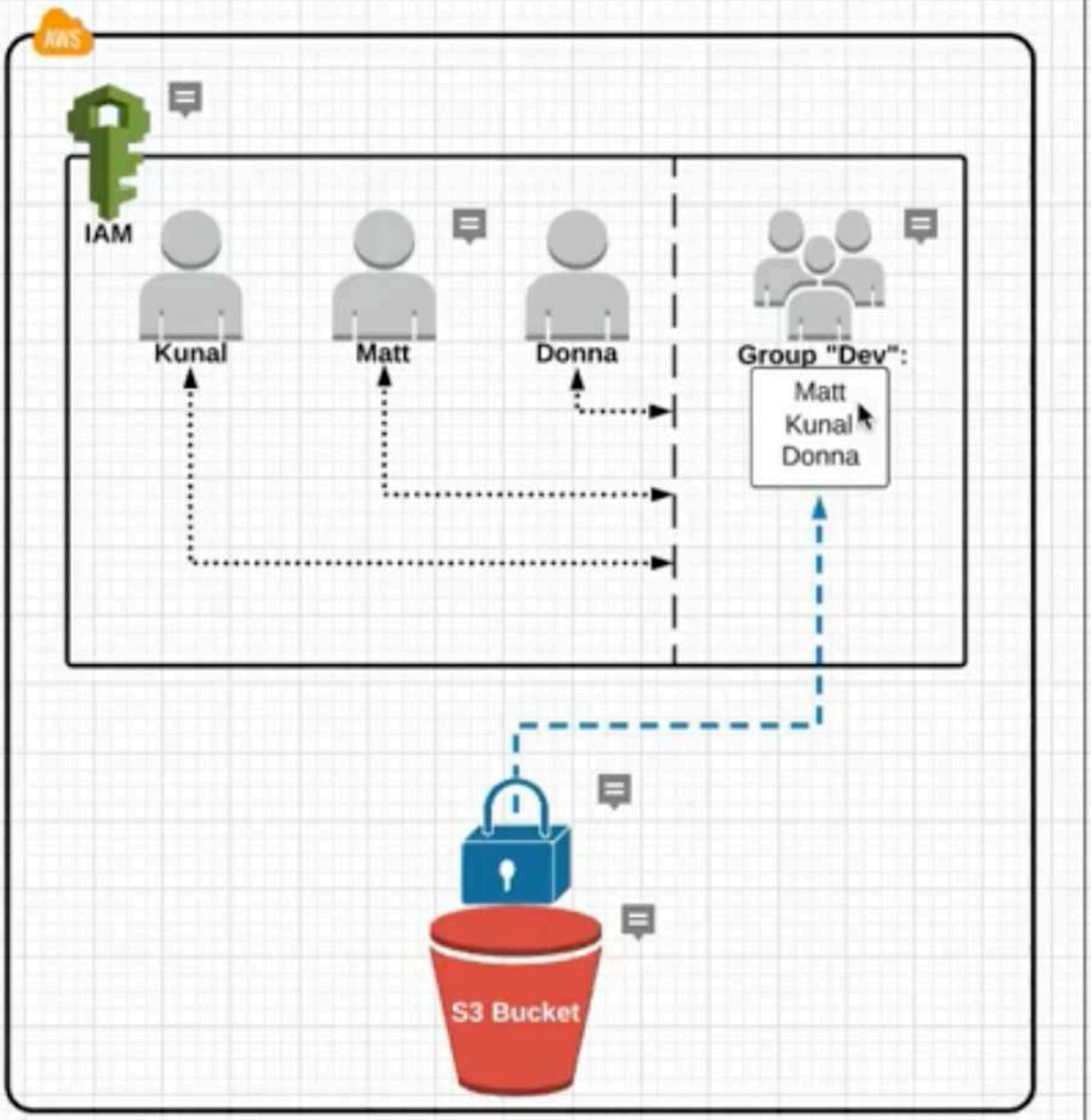
MORE ->

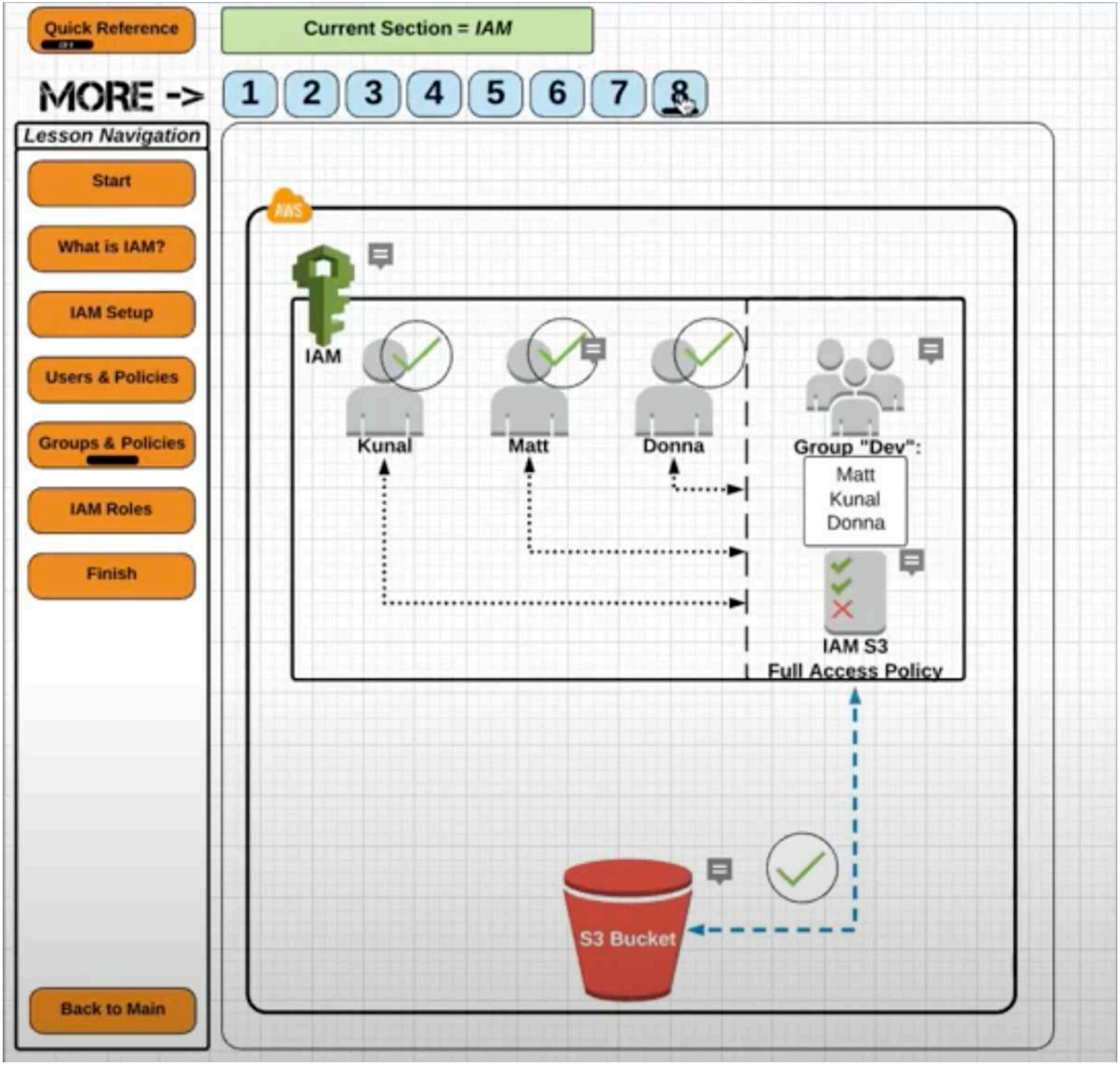
1 2 3 4 5 6 7 8

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main




Quick Reference
Current Section = IAM
MORE ->
1
2
3
4
5
6
7
8
Lesson Navigation
Start
What is IAM?
IAM Setup
Users & Policies
Groups & Policies
IAM Roles
Finish
Back to Main
IAM
Kunal
Matt
Donna
Group "Dev":
Matt
Kunal
Donna
IAM S3
Full Access Policy
S3 Bucket

Quick Reference

Current Section = *IAM*

MORE -> 1 2 3 4 5 6 7

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main

What is IAM?

- **IAM** (Identity & **A**ccess **M**anagement) is where you manage your AWS users and their access to AWS accounts and services.

- The common use of **IAM** is to manage:
  - ***Users***
  - ***Groups***
  - ***IAM Access Policies***
  - *Roles*

NOTE: The user created when you created the AWS account is called the "root" user.

- By default, the root user has ***FULL*** administrative rights and access to every part of the account.

- Any new or additional users you create in the AWS account are created with ***NO*** access to anything by default (except the ability to log in).

Quick Reference

Current Section = *IAM*

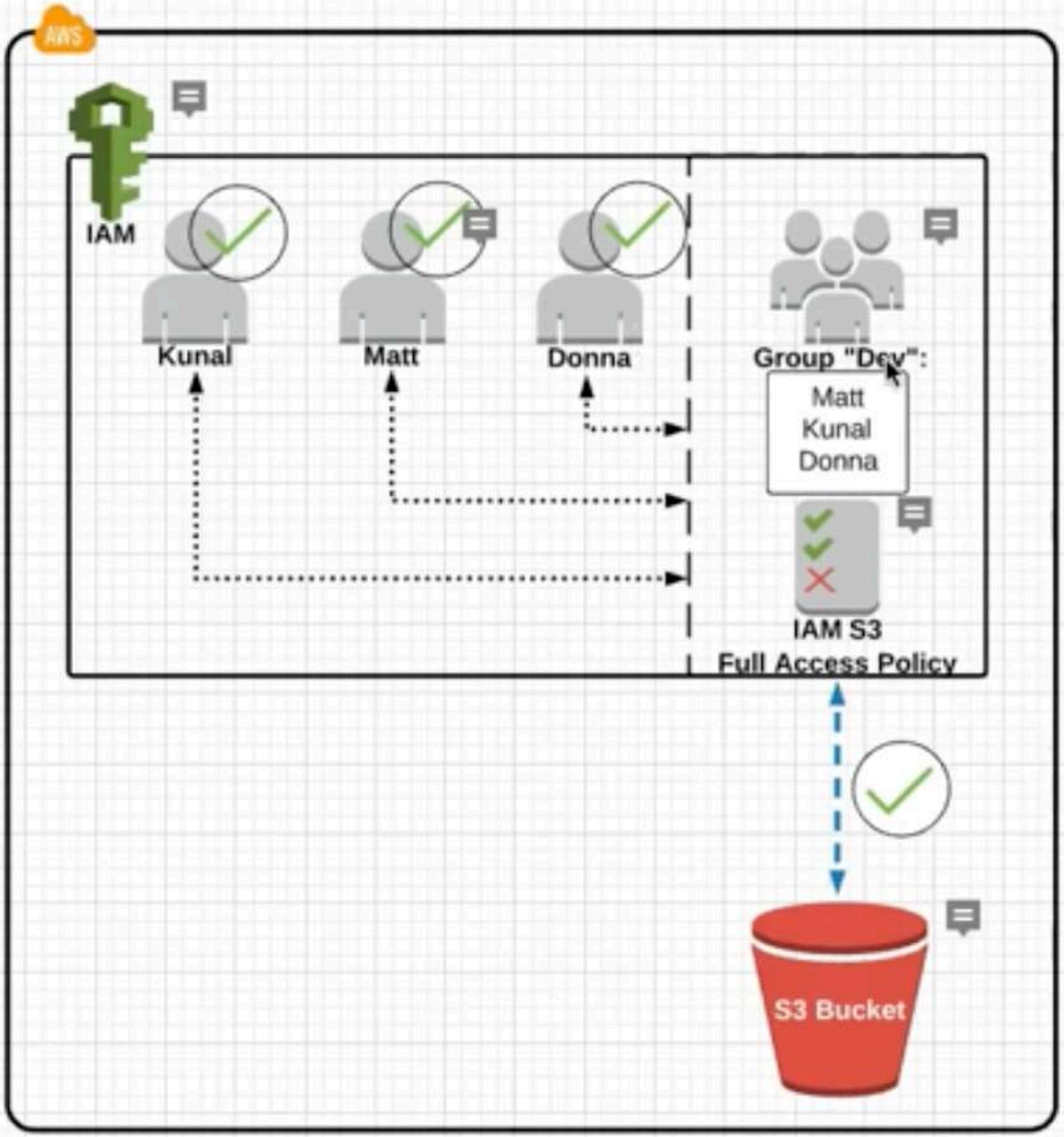
MORE ->

1 2 3 4 5 6 7

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish

Back to Main



Quick Reference

Current Section = *IAM*

MORE ->

Lesson Navigation

Start

What is IAM?

IAM Setup

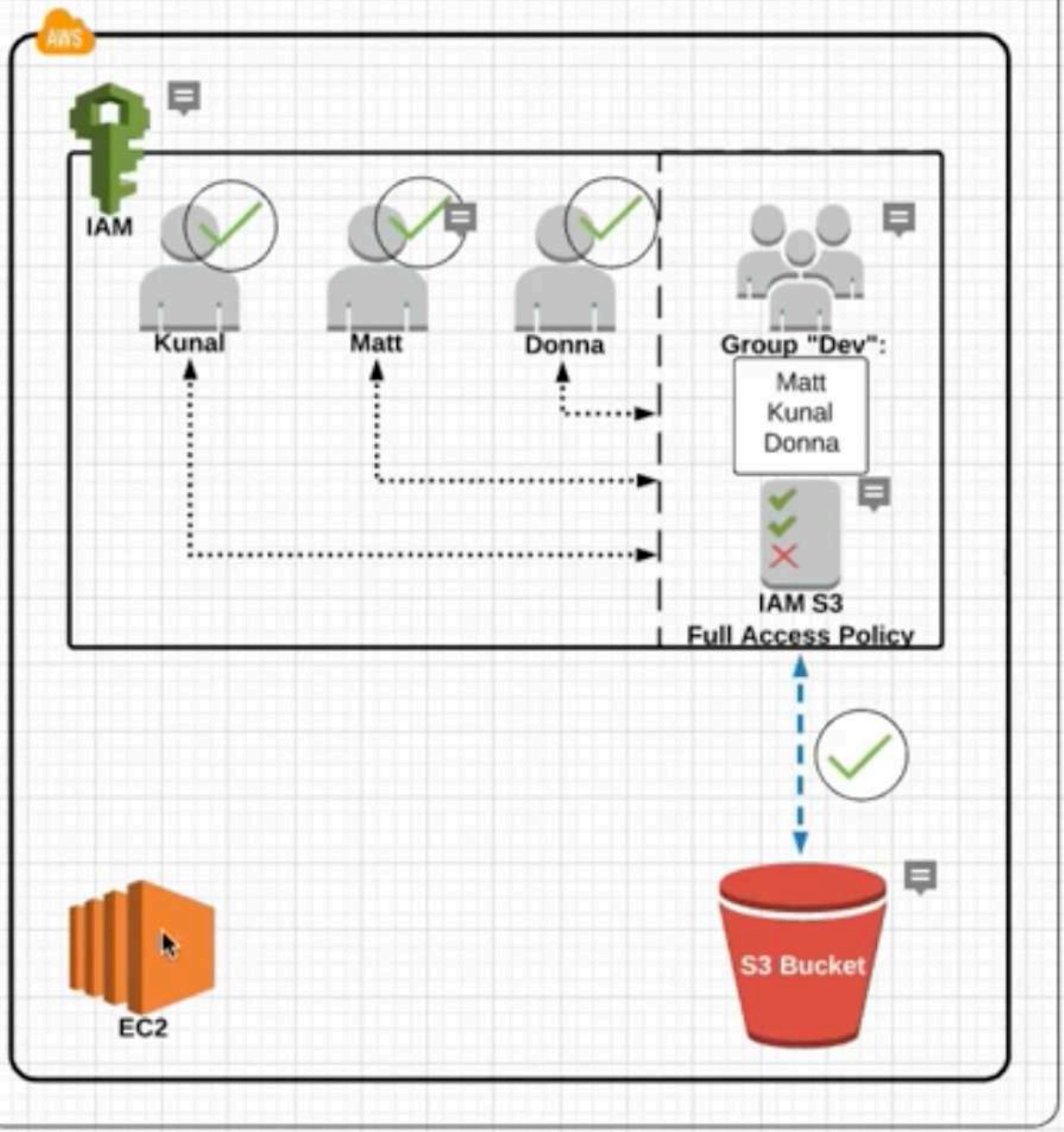
Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main



Lesson Navigation

Start

What is IAM?

IAM Setup

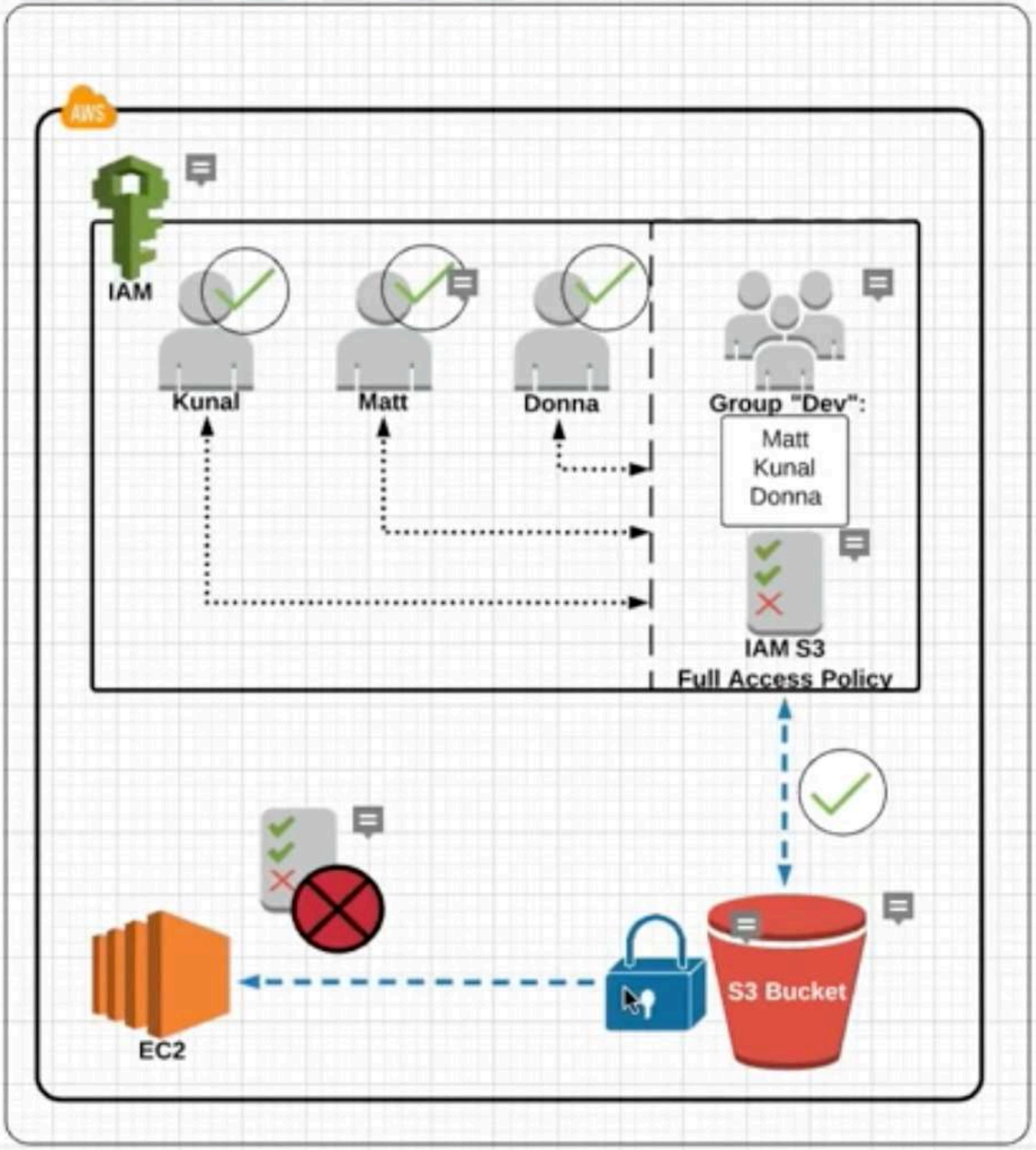
Users & Policies

Groups & Policies

IAM Roles

Finish

Back to Main



Quick Reference

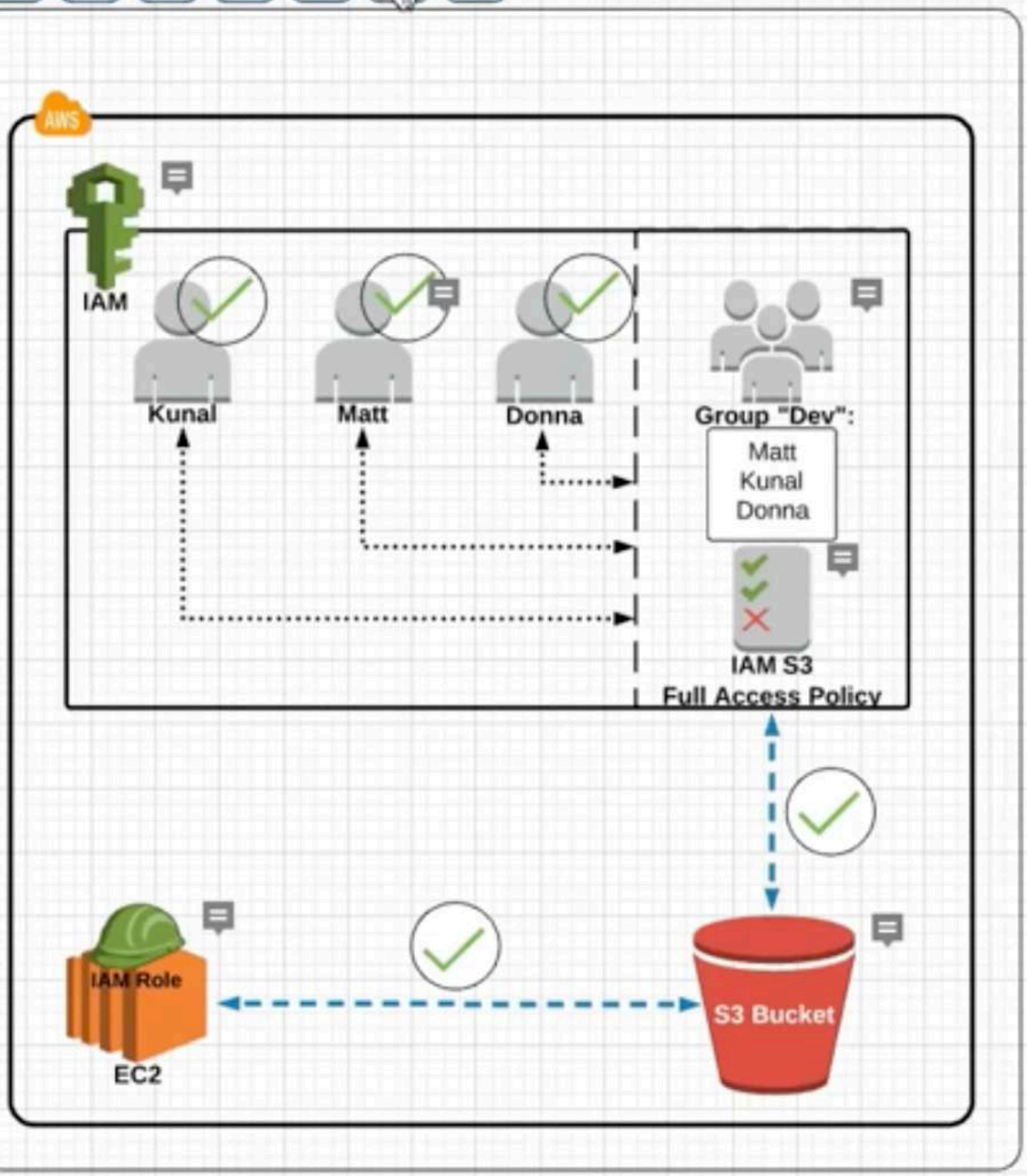
Current Section = *IAM*

MORE ->

1 2 3 4 5 6 7

Lesson Navigation

- Start
- What is IAM?
- IAM Setup
- Users & Policies
- Groups & Policies
- IAM Roles
- Finish
- Back to Main



Lesson Navigation

Start

What is IAM?

IAM Setup

Users & Policies

Groups & Policies

IAM Roles

Finish

PROJECT OMEGA

Have you completed the Project Omega infrastrucutre requirements for this section?

(1) ~~An AWS account~~

(2) User accounts for the development team with access to core AWS services:

-Three IAM user accounts, one for each member of the dev team.

-An IAM group for the dev team.

-IAM policies attached to the group - granting acess to S3, EC2, and RDS.

(3) Proper traffic routing into and out of our AWS Virtual Private Cloud (VPC).

(4) A location for bulk storage of files.

(5) Servers to host and run Project Omega.

(6) A databse to store and catalog data.

(7) A way to sent notifications (email or text messages) to Project Omega's team members based on events that may occur with Projects Omega's infrastructure.

(8) A way to internally monitor parts of Projects Omega's infrastructure.

(9) Automate the process of distributing incoming (external user) traffic evenly accross Projects Omega's AWS resources.

(10) Automate the process of scaling up or scaling down AWS resources based on traffic demand.

(11) Set up and configure a web domain that points to Project Omega's infrastructure.

(12) Test the possibiliy of using "serverless" technology for Project Omega.