Hello, Cloud Gurus and welcome to this lecture.

And this lecture is called identity access management 101.

And IAM is the best place to start with AWS because it's all

about setting up your users and granting those users access to the

AWS console. So what is IAM? Well,

essentially,

IAM allows you to manage users and also manage their level of

access to the AWS console.

And it's really important to understand IAM and how it works,

both for the exam and for administrating a company's AWS account in

real life. So what does IAM give you?

It gives you centralized control over your AWS account.

It also gives you shared access to your AWS account.

It gives you granular permissions.

So this means you can enable different levels of access to different users

within your organization. It enables identity federation.

So this means that it can enable users to log in using credentials stored in

active directory, Facebook, or LinkedIn.

It allows multifactor authentication.

And this is where a user is granted access only after successfully completing

multiple independent authentication mechanisms.

So for example,

providing a username and password as one authentication mechanism,

and then providing a software token.

So that could be via a token generator like Google authenticator as

the second authentication mechanism.

It also provides temporary access for users or devices and services

as necessary. So for example,

if you developed a web or mobile phone application,

you can configure identity access management to enable users to have temporary

access to AWS resources within your account.

For example,

to enable access to store or retrieve data located in an S3

bucket or within a DynamoDB database.

It allows you to set up your own password rotation policy.

It integrates with many different AWS services and it

supports PCI DSS compliance for any applications

associated with the payment card industry.

So there are some core concepts that you need to understand before going into

the exam. So first of all, we have users,

so this is the end users and just think people.

So these are the people logging in to the AWS console and also

interacting with AWS by running API commands.

We then have groups which are collections of users grouped together with a

common set of permissions. So for example,

your marketing team might need access to read and write certain files

stored in an S3 bucket, and that might be logos or images,

et cetera.

And they're going to need a specific set of permissions to allow them to do

this.

So it makes sense to create a group with the required permissions.

And then all you need to do is add the relevant users into that group.

And they will all have permissions to read your S3 bucket. And similarly,

you might have a database administrations team and they need to create DynamoDB

tables and run queries on the database. So in that case,

you can create a group with the relevant permissions for DynamoDB,

and then add all of your database admins into that group.

And we also have roles.

Now you can create roles and then assign them to AWS resources.

So a role is used to define a set of permissions, for example,

S3 bucket access.

And then that role can be assumed by either users or AWS services

such as EC2.

So you might have an EC2 instance which needs to query a database or access

files in S3, and you can configure that using a role. And finally,

we have policies and a policy is a document that defines either one or

more permissions. And a policy can be attached to either a user,

a group, or a role. And when we attach a policy, the user, group,

or role will then have the permissions defined within that policy.

And it's possible for a user, group, and role to all share the same policy.

So the quickest way to learn identity access management is actually to start

using it. And that's what we're going to do right now. So if you've got time,

please join me in the next lecture, which is an identity access management lab.

Thank you.