Understanding IAM Permissions

Questions	Notes
Roles	• Roles define access permissions and are temporarily assumed by an IAM user or service • you asssume a role to perform a task in a single session • assumed by any user or service that needs it • access is assigned using policies • you grant users in one aws account access to ressources in another aws account • **In the real world:** ◦ Attach a role to an EC2 instance for access to s3 : you can attach a role to an instance that provides privileges (uploading files to s3) to applications running on the instance. Roles help you avoid sharing long-term credentials like access keys and protect your instances from Unauthorized access
policies	• You manage permissions for IAM users, groups , and roles by creating a policy document in JSON format and attaching it
best practices for IAM	1. **Enable MFA for privileged users**: you should enable multi-factor athentication (MFA) for the root user and other administrative users 2. **Implement strong password policies:** you should require IAM users to change their passwords after a specified period of time, prevent users from reusing previous password , and rotate security credntials regularly 3. Create Individual users instead of using root: you souldn't use the root user daily task 4. use roles fro amazon ec2 instances: you should use roles for applications that run on ec2 instnances instead of long-term credentials like access keys
IAM Credential Report	• The IAM credential report: The IAM credential report lists all users in your account and the status of thier various credentials ◦ Lists all users and status of passwords , access keys, and MFA devices ◦ Used for auditing and compliance
review time	• roles: define access permissions and are temporarily assumed by an IAM user or service • Policies:you manage permissions for IAM users, groups, and roles by creating a policy document in JSON format and attaching it • Cresential Report: The IAM crdential report lists all users in your account and the status of thier various credentials