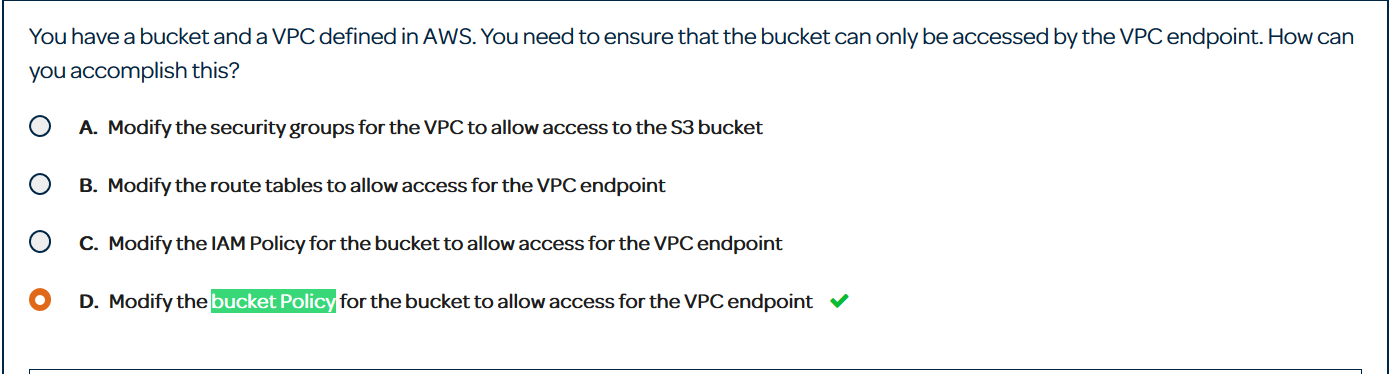
Policies in AWS

In AWS you use policies to control what identities have access to what. There are actually 5 different types of policies in AWS. I suggest you research about all of these before you sit your exam.

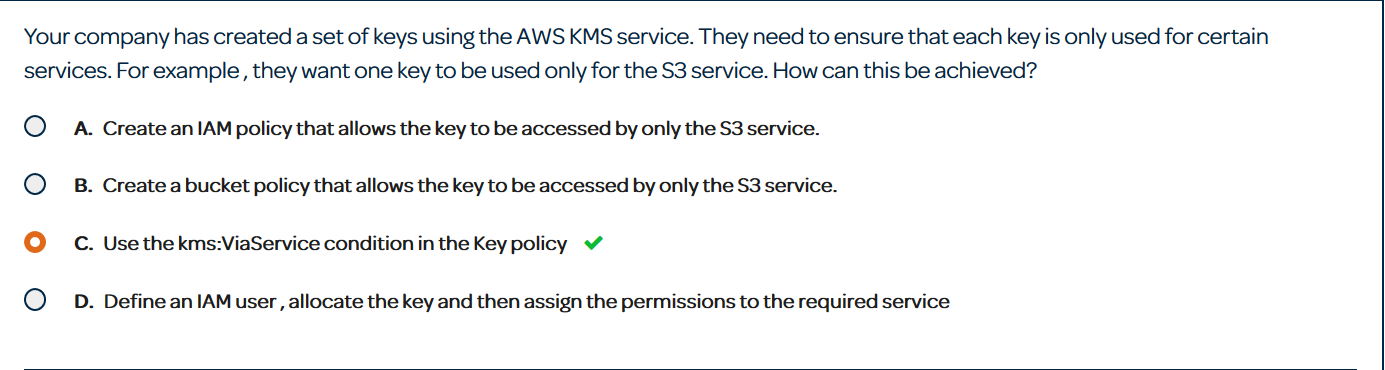
**Identity Policies-** These are your basic policies attached to users, groups, or roles.

Answering questions around identity policies usually involve reading them and figuring out what they do. Questions around every other policy type tend to be more niche around conditions and troubleshooting why they might not be working.

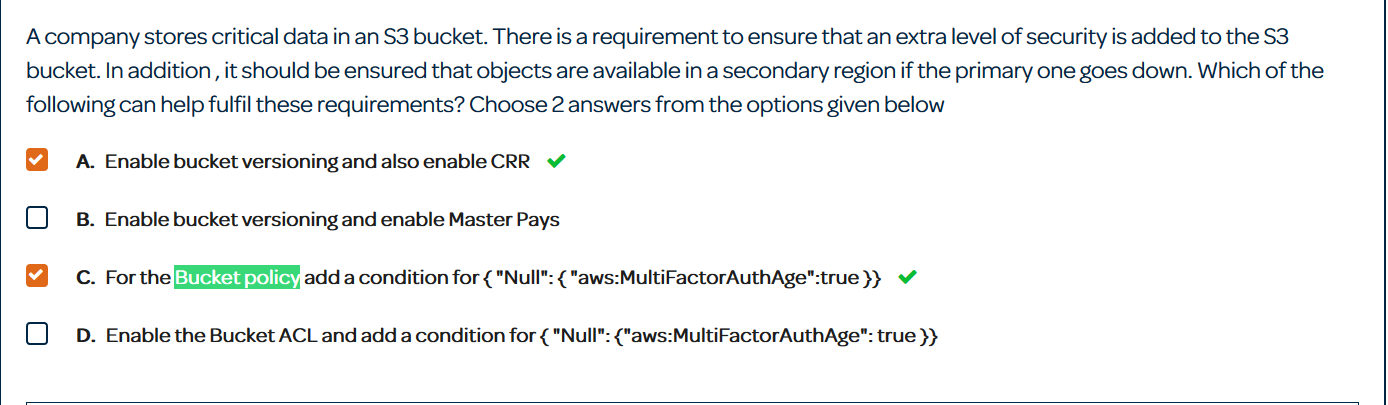
**Resource Policies-** These policies are attached to resource and delegate access via the resource itself. A few different types of resource policies are bucket policies, CMK key policies, and Lambda function policies.



A lot of bucket policy questions will be based around restricting access to a bucket via conditions.

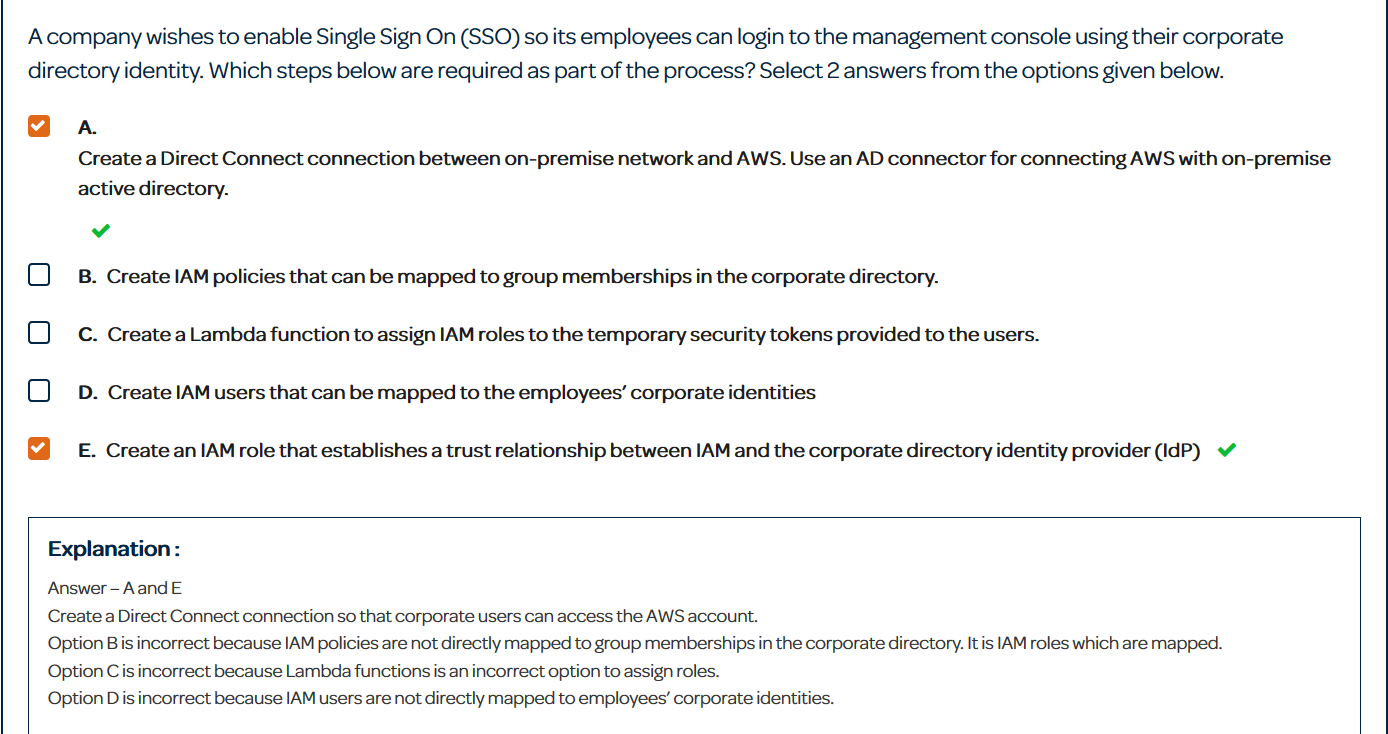


Same with key policies. From my experience the condition keys are pretty self-explanatory.

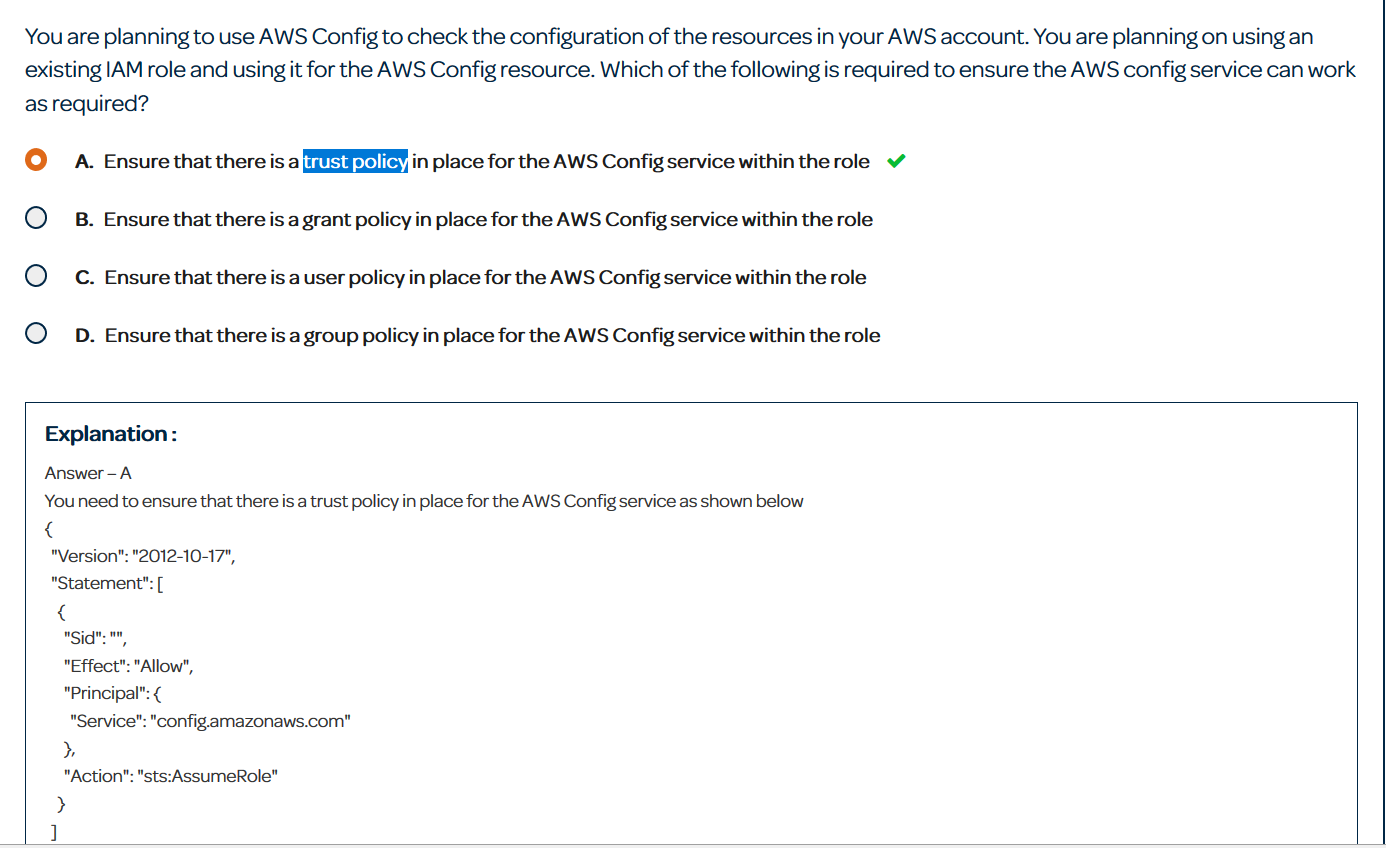


This condition the aws:MultiFactorAuthAge will add MFA to a bucket.

**Trust Policies-** This is only a feature within IAM roles and a trust policy defines who or what can assume that role. The trust policy can specify and account or a service.



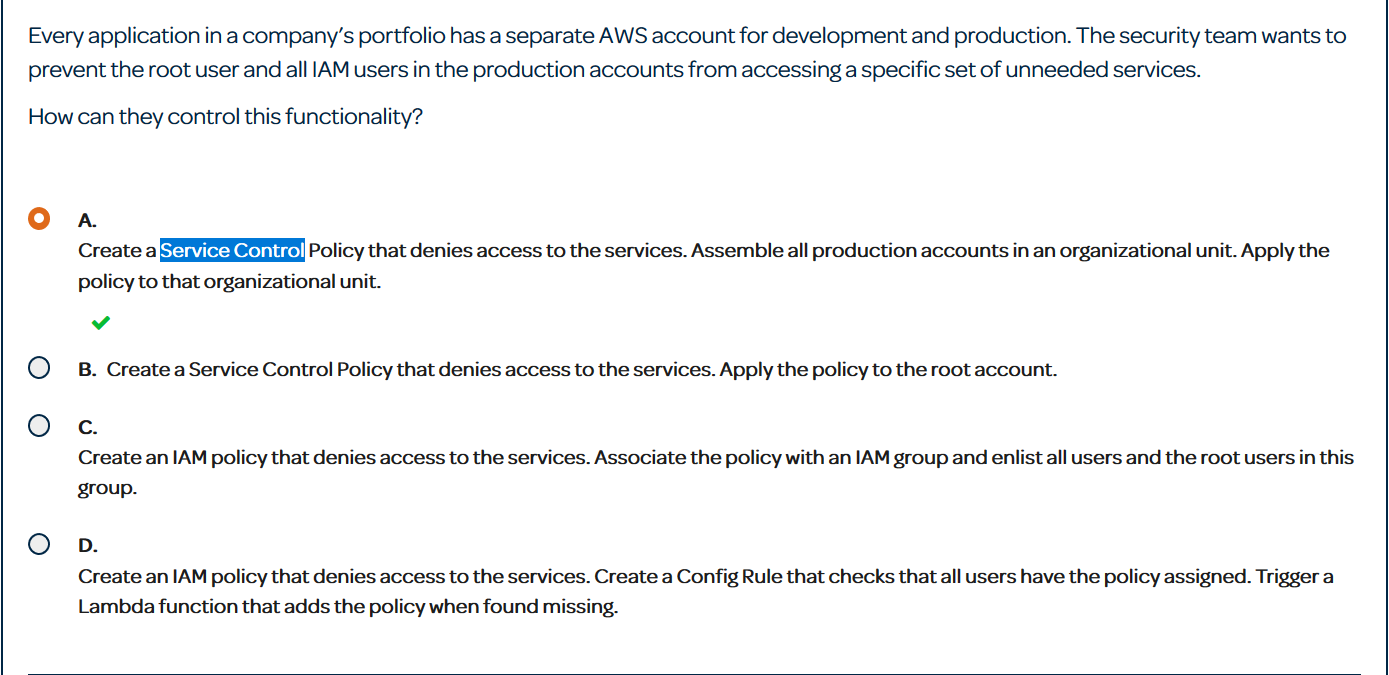
A trust policy must allow the entity trying to assume a role its trust. Weather that be in id federation, across accounts, or a service trying to assume a role.



A trust policy has the syntax in the explanation of the question. If it is suppose to trust a service it allows that service to do the sts:AssumeRole action.

**Permission Boundaries-** Permission boundaries put a cap on the services you are allowed to use. They do not grant extra permissions but instead define the only service you are allowed to use in their policy. For example, if the permissions boundary allowed only S3, but your user identity policy allowed full access, that user would only be able to use S3. Permissions boundaries can be applied to users and roles.

**Service Control Policies-** These are applied in AWS Organizations and are the only policy type that can actually restrict root users. To be clear in an Organization you have a master account and child accounts. Those child accounts can have the root user restricted but not the master account.



In this example you want to apply a service control policy to only affect your production account. In order to do that you must make separate organizational units and you must apply the service control to the production OU.