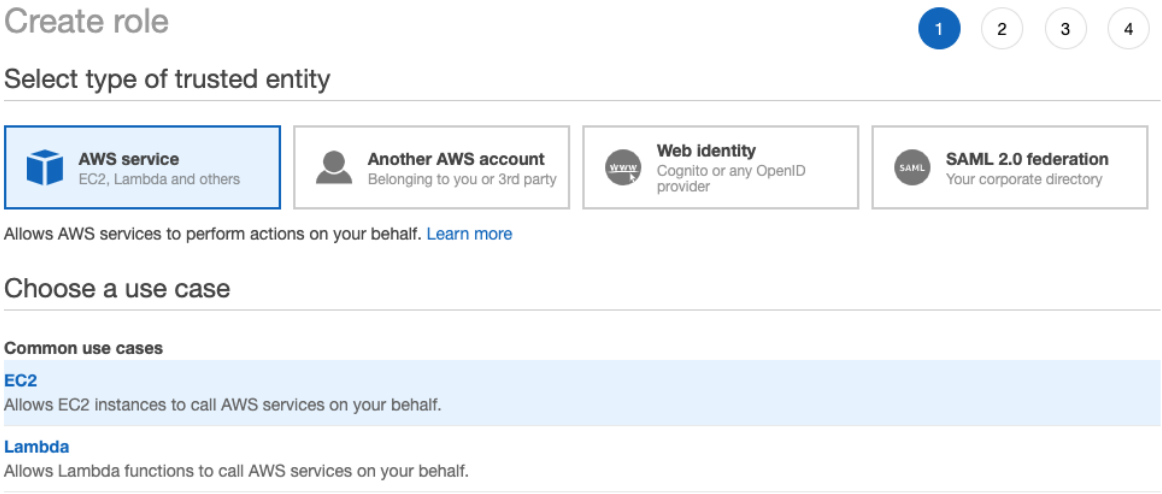
Solution: IAM Role Exercise

An IAM Role is an IAM identity similar to IAM user. Instead of uniquely associating with a person, a role is designed for anyone who needs to assume it. This is an excellent fit for a service or a server-to-server identity.

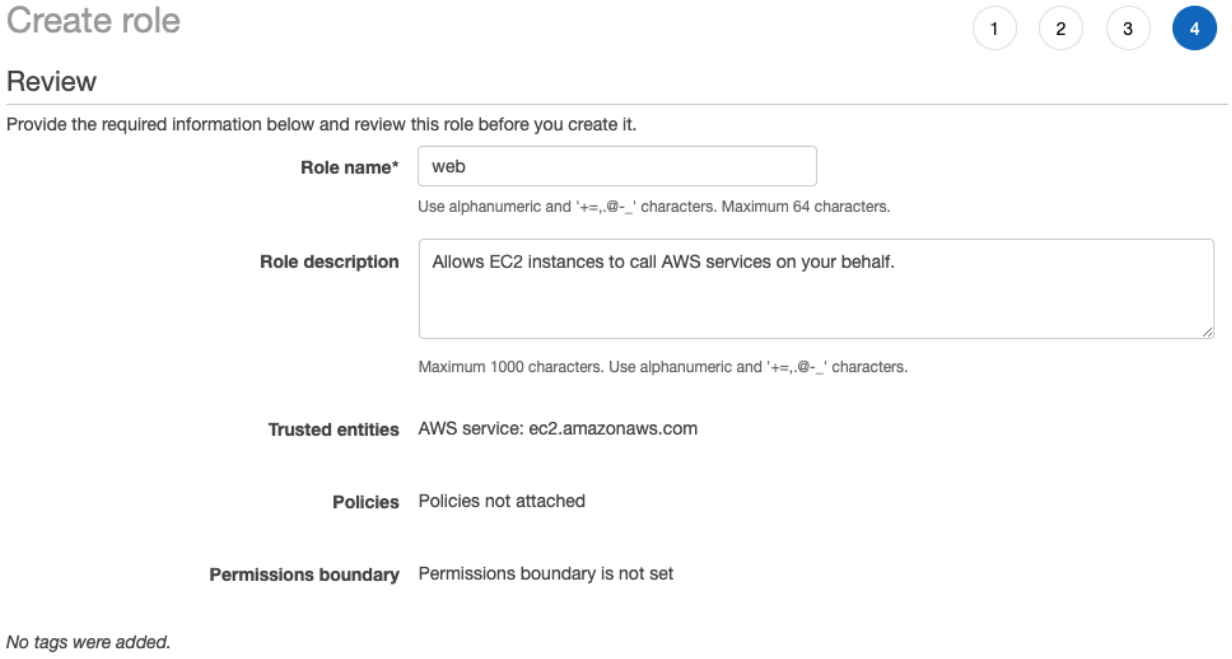
A role is more secure than the long-lived credentials of an IAM user because when the role is assumed it provides temporary security credentials that expire and renew every 15 minutes

Create the IAM Role

1. Navigate to the **IAM console**
2. Click **Roles** on the sidebar menu
3. Click on the **Create Role** button
4. Since we intended to use the role on an EC2 in the next exercise, choose **EC2** as the use case, and click on **Next: Permissions** button



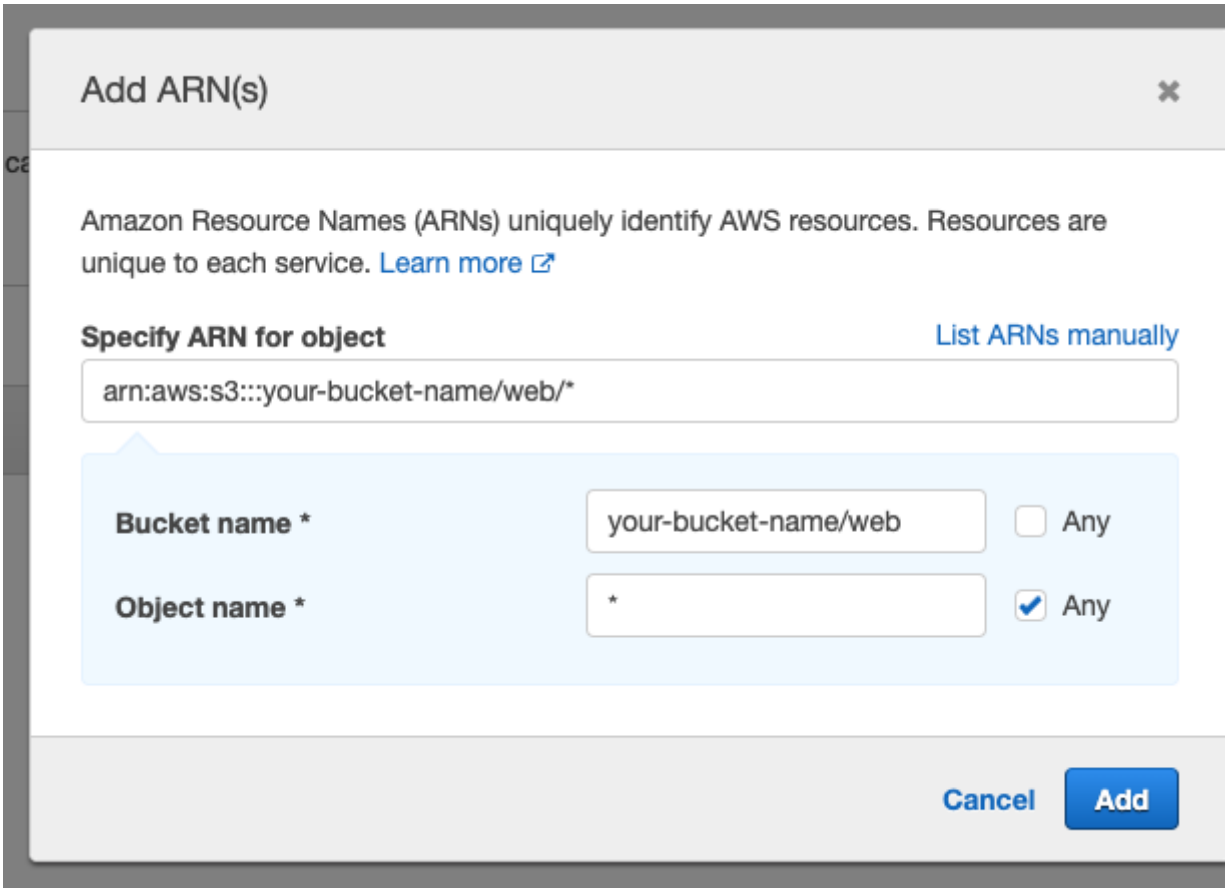
5. If we were to click on the **Create Policy** button, the role creation would be canceled, so instead click on **Next** until you get to the review page
6. Name the role **web** and click on the **Create Role** button

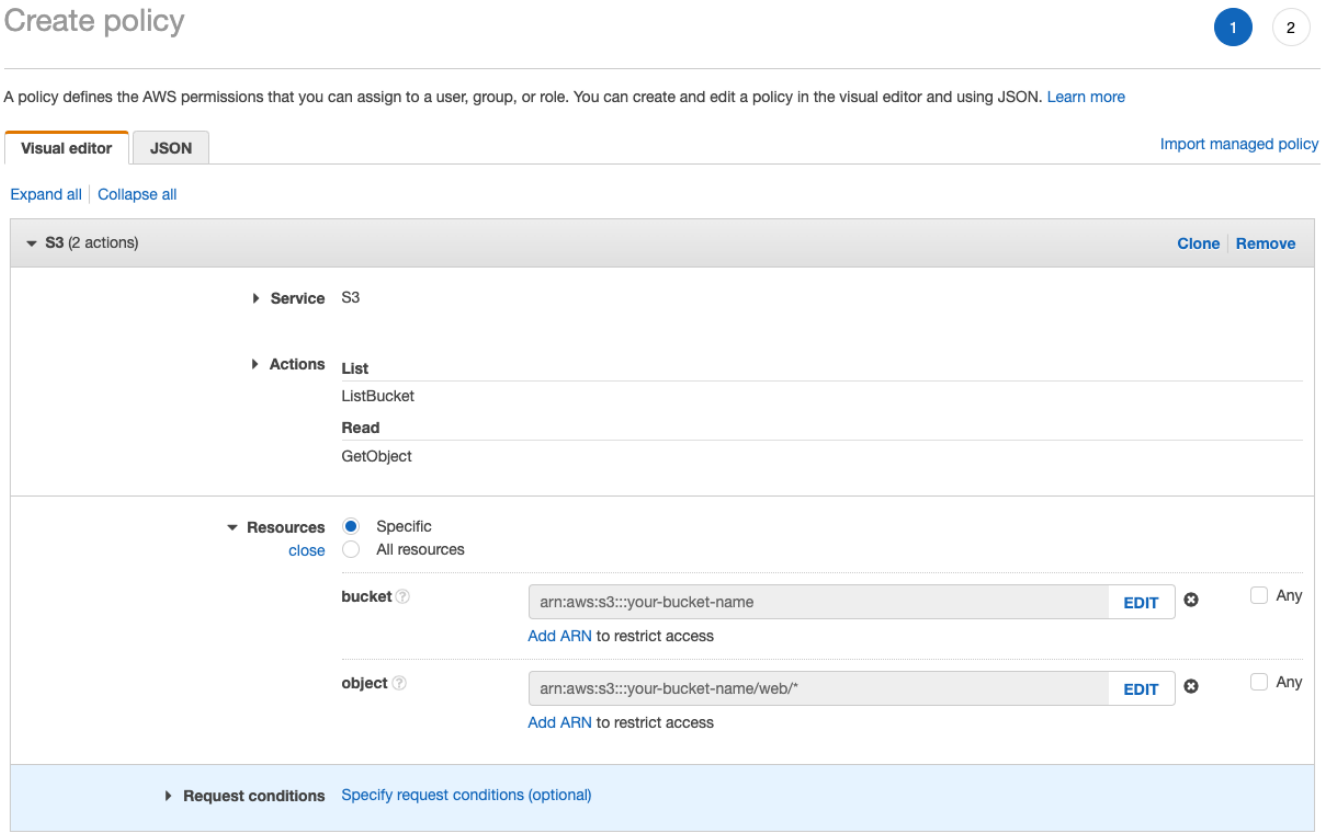


Creating and Attaching an IAM Policy to the Role

Now that we have a role, let's create an IAM policy so that it can access our S3 bucket.

1. From the sidebar menu click on **Policies** and then click on the **Create Policy** button
2. Select **S3** for the service
3. On the **Actions** field select **ListBucket** and **GetObject**
4. Click on Resources, while it is set to **specific** click the **Add ARN** for the **bucket** and add your bucket name
5. Click on the **Add ARN** for the object, set the **bucket name** again to your bucket name and set the **object name** to "web/*"



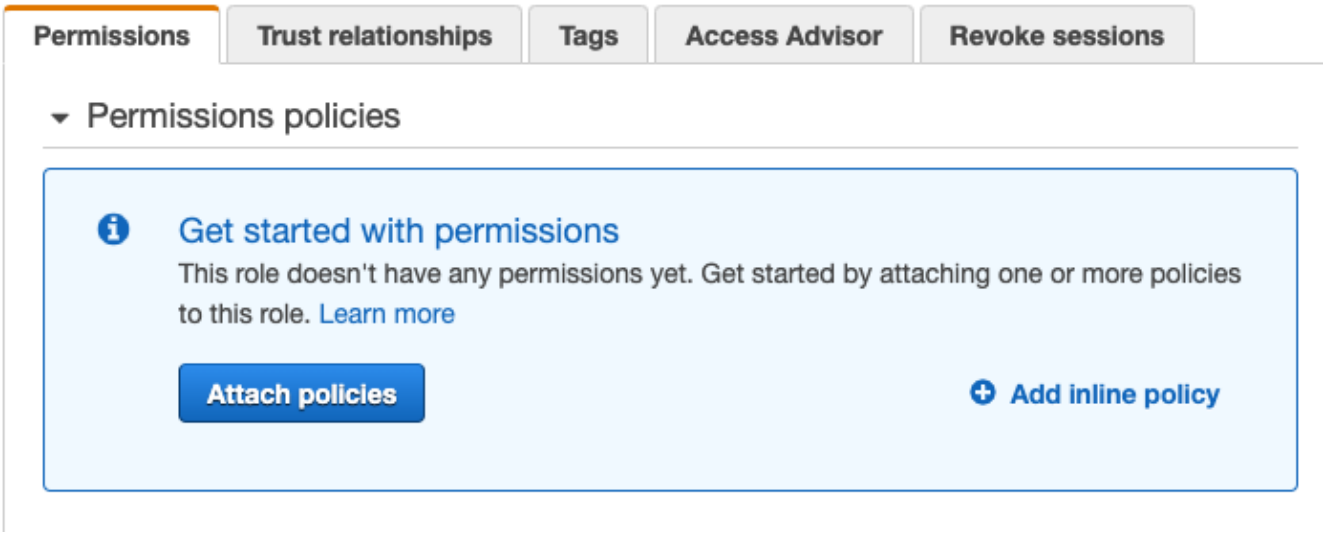


7. Click on the **Review policy** button, set a name (for example, "ec2_web_s3_access") and click the **Create policy** button

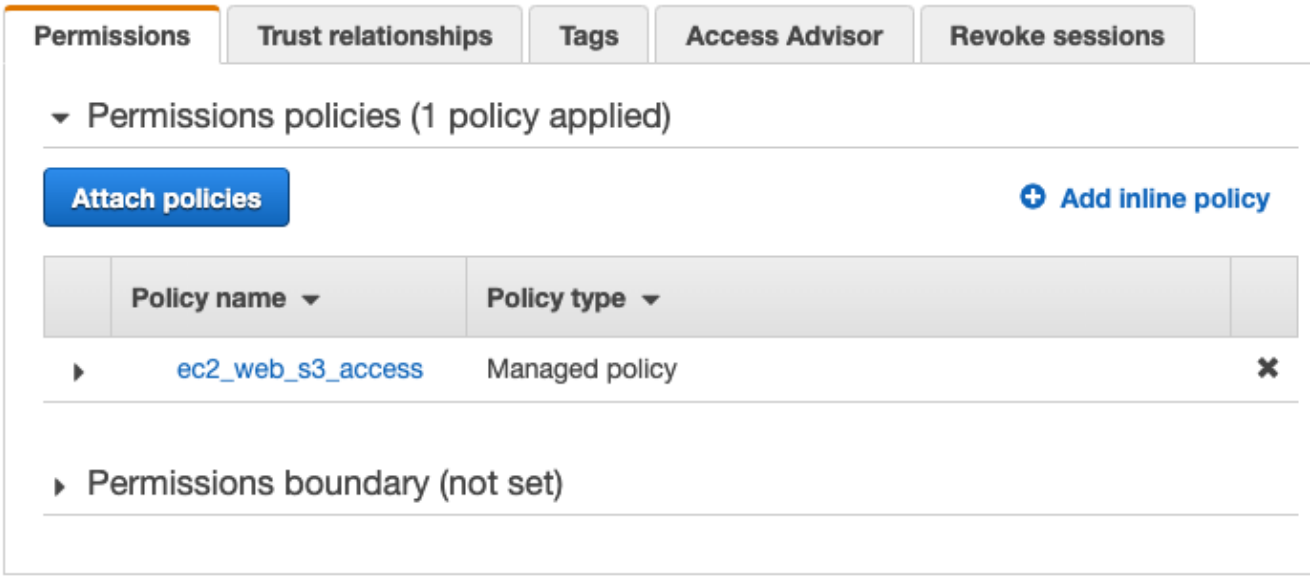
Attaching the Policy to the IAM Role

1. Click on the **Roles** on the sidebar menu of the IAM console
2. Search for the role "web"

3. Click on the role name to edit the role
4. Click on the **Attach policies** button



5. Search for "web" to find the policy you just created
6. Select it and click the **Attach policies** button


Permissions
Trust relationships
Tags
Access Advisor
Revoke sessions
Permissions policies (1 policy applied)
Attach policies
Add inline policy
Policy name
Policy type
ec2_web_s3_access
Managed policy
Permissions boundary (not set)