





S3 - Set up permissions

Go to AWS and go to IAM

1. Go to IAM > Roles > aws-s3-access
2. Select aws-s3-access-progamatic
3. Select S3
4. Select the Json and modify the policy
5. Add the name of the bucket permissions
6. Bucket should have correct permission.

Check that the instance has the aws-s3-access permission policy attached to it.

<input type="checkbox"/>	Policy name 🔗	Type	Attached entities
<input type="checkbox"/>	 AmazonEKSWorker...	AWS managed	3
<input type="checkbox"/>	 aws-s3-access-console	Customer managed	10
<input type="checkbox"/>	 aws-s3-access-progra...	Customer managed	10
<input type="checkbox"/>	 SecretsManagerRe...	AWS managed	5

If not create a new role and select AWS service under trusted entity type
Select EC2 under use case

Select trusted entity [Info](#)

Trusted entity type

☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2

Choose a use case for the specified service.
Use case

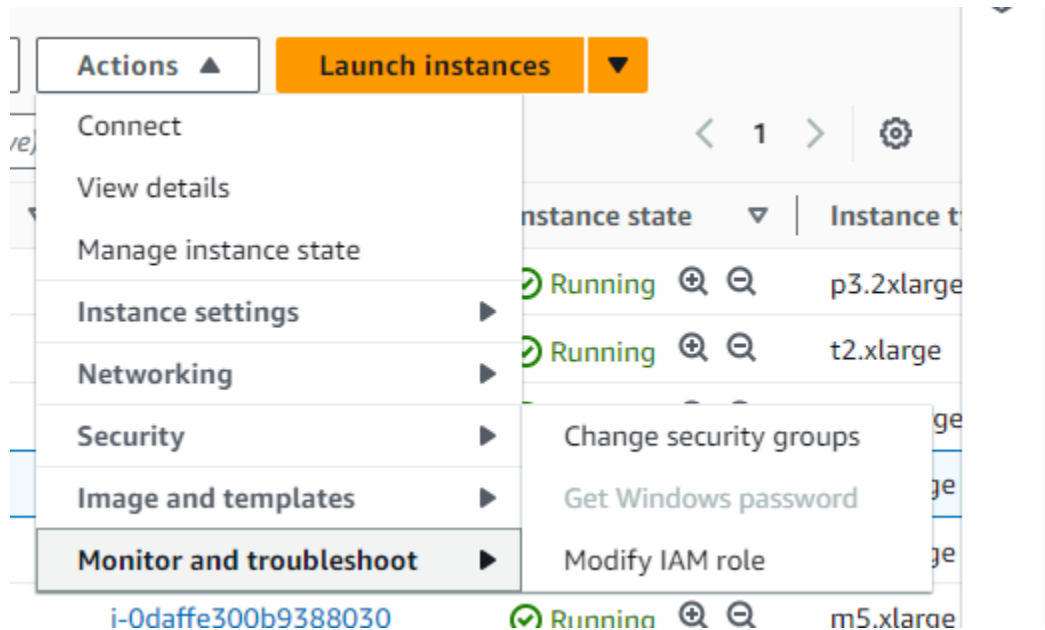
☒ **EC2**
Allows EC2 instances to call AWS services on your behalf.

☐ **EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

☐ **EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

Add aws-s3-access-progamatic permissions and secretsManager to the role
Click Next and create the role.

1. Go back to Instances
2. Select the specific instance.
3. Click Actions.
4. Click Security from the dropdown.



5. Select Modify IAM role and add the role that was just created

