Manage access to an Azure Machine Learning workspace

Article • 09/29/2022 • 14 minutes to read

In this article, you learn how to manage access (authorization) to an Azure Machine Learning workspace. Azure role-based access control (Azure RBAC) is used to manage access to Azure resources, such as the ability to create new resources or use existing ones. Users in your Azure Active Directory (Azure AD) are assigned specific roles, which grant access to resources. Azure provides both built-in roles and the ability to create custom roles.

Tip

While this article focuses on Azure Machine Learning, individual services that Azure ML relies on provide their own RBAC settings. For example, using the information in this article, you can configure who can submit scoring requests to a model deployed as a web service on Azure Kubernetes Service. But Azure Kubernetes Service provides its own set of Azure roles. For service specific RBAC information that may be useful with Azure Machine Learning, see the following links:

- **Control access to Azure Kubernetes cluster resources**
- **Use Azure RBAC for Kubernetes authorization**
- **Use Azure RBAC for access to blob data**

⚠ Warning

Applying some roles may limit UI functionality in Azure Machine Learning studio for other users. For example, if a user's role does not have the ability to create a compute instance, the option to create a compute instance will not be available in studio. This behavior is expected, and prevents the user from attempting operations that would return an access denied error.

Default roles

Azure Machine Learning workspaces have a five built-in roles that are available by default. When adding users to a workspace, they can be assigned one of the built-in roles described below.

Role	Access level
AzureML Data Scientist	Can perform all actions within an Azure Machine Learning workspace, except for creating or deleting compute resources and modifying the workspace itself.
AzureML Compute Operator	Can create, manage and access compute resources within a workspace.

Role	Access level
Reader	Read-only actions in the workspace. Readers can list and view assets, including datastore credentials, in a workspace. Readers can't create or update these assets.
Contributor	View, create, edit, or delete (where applicable) assets in a workspace. For example, contributors can create an experiment, create or attach a compute cluster, submit a run, and deploy a web service.
Owner	Full access to the workspace, including the ability to view, create, edit, or delete (where applicable) assets in a workspace. Additionally, you can change role assignments.

You can combine the roles to grant different levels of access. For example, you can grant a workspace user both **AzureML Data Scientist** and **Azure ML Compute Operator** roles to permit the user to perform experiments while creating computes in a self-service manner.

> **Important**
>
> Role access can be scoped to multiple levels in Azure. For example, someone with owner access to a workspace may not have owner access to the resource group that contains the workspace. For more information, see **How Azure RBAC works**.

Manage workspace access

If you're an owner of a workspace, you can add and remove roles for the workspace. You can also assign roles to users. Use the following links to discover how to manage access:

- Azure portal UI
- PowerShell
- Azure CLI
- REST API
- Azure Resource Manager templates

Use Azure AD security groups to manage workspace access

You can use Azure AD security groups to manage access to workspaces. This approach has following benefits:

- Team or project leaders can manage user access to workspace as security group owners, without needing Owner role on the workspace resource directly.
- You can organize, manage and revoke users' permissions on workspace and other resources as a group, without having to manage permissions on user-by-user basis.
- Using Azure AD groups helps you to avoid reaching the subscription limit on role assignments.

To use Azure AD security groups:

1. Create a security group.
2. Add a group owner. This user has permissions to add or remove group members. Note that the group owner isn't required to be group member, or have direct RBAC role on the workspace.
3. Assign the group an RBAC role on the workspace, such as AzureML Data Scientist, Reader or Contributor.
4. Add group members. The members consequently gain access to the workspace.

Create custom role

If the built-in roles are insufficient, you can create custom roles. Custom roles might have read, write, delete, and compute resource permissions in that workspace. You can make the role available at a specific workspace level, a specific resource group level, or a specific subscription level.

> **Note**
>
> You must be an owner of the resource at that level to create custom roles within that resource.

To create a custom role, first construct a role definition JSON file that specifies the permission and scope for the role. The following example defines a custom role named "Data Scientist Custom" scoped at a specific workspace level:

`data_scientist_custom_role.json` :

JSON

```
{
    "Name": "Data Scientist Custom",
    "IsCustom": true,
    "Description": "Can run experiment but can't create or delete compute.",
    "Actions": ["*"],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/*/delete",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/delete",
        "Microsoft.Authorization/*/write"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>/resourceGroups/<resource_group_name>/providers
/Microsoft.MachineLearningServices/workspaces/<workspace_name>"
    ]
}
```

> **Tip**

You can change the `AssignableScopes` field to set the scope of this custom role at the subscription level, the resource group level, or a specific workspace level. The above custom role is just an example, see some suggested **custom roles for the Azure Machine Learning service**.

This custom role can do everything in the workspace except for the following actions:

- It can't create or update a compute resource.
- It can't delete a compute resource.
- It can't add, delete, or alter role assignments.
- It can't delete the workspace.

To deploy this custom role, use the following Azure CLI command:

Azure CLI

```
az role definition create --role-definition data_scientist_role.json
```

After deployment, this role becomes available in the specified workspace. Now you can add and assign this role in the Azure portal.

For more information on custom roles, see Azure custom roles.

Azure Machine Learning operations

For more information on the operations (actions and not actions) usable with custom roles, see Resource provider operations. You can also use the following Azure CLI command to list operations:

Azure CLI

```
az provider operation show -n Microsoft.MachineLearningServices
```

List custom roles

In the Azure CLI, run the following command:

Azure CLI

```
az role definition list --subscription <sub-id> --custom-role-only true
```

To view the role definition for a specific custom role, use the following Azure CLI command. The `<role-name>` should be in the same format returned by the command above:

Azure CLI

```
az role definition list -n <role-name> --subscription <sub-id>
```

Update a custom role

In the Azure CLI, run the following command:

Azure CLI

```
az role definition update --role-definition update_def.json --subscription <sub-id>
```

You need to have permissions on the entire scope of your new role definition. For example if this new role has a scope across three subscriptions, you need to have permissions on all three subscriptions.

> **Note**
>
> Role updates can take 15 minutes to an hour to apply across all role assignments in that scope.

Use Azure Resource Manager templates for repeatability

If you anticipate that you'll need to recreate complex role assignments, an Azure Resource Manager template can be a significant help. The machine-learning-dependencies-role-assignment template shows how role assignments can be specified in source code for reuse.

Common scenarios

The following table is a summary of Azure Machine Learning activities and the permissions required to perform them at the least scope. For example, if an activity can be performed with a workspace scope (Column 4), then all higher scope with that permission will also work automatically. Note that for certain activities the permissions differ between V1 and V2 APIs.

> **Important**
>
> All paths in this table that start with `/` are **relative paths** to `Microsoft.MachineLearningServices/` :

Activity	Subscription-level scope	Resource group-level scope	Workspace-level scope

Activity	Subscription-level scope	Resource group-level scope	Workspace-level scope
Create new workspace [1]	Not required	Owner or contributor	N/A (becomes Owner or inherits higher scope role after creation)
Request subscription level Amlcompute quota or set workspace level quota	Owner, or contributor, or custom role allowing `/locations/updateQuotas/action` at subscription scope	Not Authorized	Not Authorized
Create new compute cluster	Not required	Not required	Owner, contributor, or custom role allowing: `/workspaces/computes/write`
Create new compute instance	Not required	Not required	Owner, contributor, or custom role allowing: `/workspaces/computes/write`
Submitting any type of run (V1)	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/*/read", "/workspaces/environments/write", "/workspaces/experiments/runs/write", "/workspaces/metadata/artifacts/write", "/workspaces/metadata/snapshots/write", "/workspaces/environments/build/action", "/workspaces/experiments/runs/submit/action", "/workspaces/environments/readSecrets/action"`
Submitting any type of run (V2)	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/*/read", "/workspaces/environments/write", "/workspaces/jobs/*", "/workspaces/metadata/artifacts/write", "/workspaces/metadata/codes/*/write", "/workspaces/environments/build/action", "/workspaces/environments/readSecrets/action"`
Publishing pipelines and endpoints (V1)	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/endpoints/pipelines/*", "/workspaces/pipelinedrafts/*", "/workspaces/modules/*"`

Activity	Subscription-level scope	Resource group-level scope	Workspace-level scope
Publishing pipelines and endpoints (V2)	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/endpoints/pipelines/*"`, `"/workspaces/pipelinedrafts/*"`, `"/workspaces/components/*"`
Attach an AKS resource [2]	Not required	Owner or contributor on the resource group that contains AKS	
Deploying a registered model on an AKS/ACI resource	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/services/aks/write"`, `"/workspaces/services/aci/write"`
Scoring against a deployed AKS endpoint	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/services/aks/score/action"`, `"/workspaces/services/aks/listkeys/action"` (when you are not using Azure Active Directory auth) OR `"/workspaces/read"` (when you are using token auth)
Accessing storage using interactive notebooks	Not required	Not required	Owner, contributor, or custom role allowing: `"/workspaces/computes/read"`, `"/workspaces/notebooks/samples/read"`, `"/workspaces/notebooks/storage/*"`, `"/workspaces/listStorageAccountKeys/action"`, `"/workspaces/listNotebookAccessToken/read"`
Create new custom role	Owner, contributor, or custom role allowing `Microsoft.Authorization/roleDefinitions/write`	Not required	Owner, contributor, or custom role allowing: `/workspaces/computes/write`
Create/manage online endpoints and deployments	Not required	Not required	Owner, contributor, or custom role allowing `Microsoft.MachineLearningServices/workspaces/onlineEndpoints/*`

Activity	Subscription-level scope	Resource group-level scope	Workspace-level scope
Retrieve authentication credentials for online endpoints	Not required	Not required	Owner, contributor, or custom role allowing `Microsoft.MachineLearningServices/workspaces/onlineEndpoints/token/action` and `Microsoft.MachineLearningServices/workspaces/onlineEndpoints/listkeys/action`.

1: If you receive a failure when trying to create a workspace for the first time, make sure that your role allows `Microsoft.MachineLearningServices/register/action`. This action allows you to register the Azure Machine Learning resource provider with your Azure subscription.

2: When attaching an AKS cluster, you also need to the Azure Kubernetes Service Cluster Admin Role on the cluster.

Differences between actions for V1 and V2 APIs

There are certain differences between actions for V1 APIs and V2 APIs.

Asset	Action path for V1 API	Action path for V2 API
Dataset	Microsoft.MachineLearningServices/workspaces/datasets	Microsoft.MachineLearningServices/workspaces/datasets/versions
Experiment runs and jobs	Microsoft.MachineLearningServices/workspaces/experiments	Microsoft.MachineLearningServices/workspaces/jobs
Models	Microsoft.MachineLearningServices/workspaces/models	Microsoft.MachineLearningServices/workspaces/models/verstions
Snapshots and code	Microsoft.MachineLearningServices/workspaces/snapshots	Microsoft.MachineLearningServices/workspaces/codes/versions
Modules and components	Microsoft.MachineLearningServices/workspaces/modules	Microsoft.MachineLearningServices/workspaces/components

You can make custom roles compatible with both V1 and V2 APIs by including both actions, or using wildcards that include both actions, for example Microsoft.MachineLearningServices/workspaces/datasets/*/read.

Create a workspace using a customer-managed key

When using a customer-managed key (CMK), an Azure Key Vault is used to store the key. The user or

service principal used to create the workspace must have owner or contributor access to the key vault.

Within the key vault, the user or service principal must have create, get, delete, and purge access to the key through a key vault access policy. For more information, see Azure Key Vault security.

User-assigned managed identity with Azure ML compute cluster

To assign a user assigned identity to an Azure Machine Learning compute cluster, you need write permissions to create the compute and the Managed Identity Operator Role. For more information on Azure RBAC with Managed Identities, read How to manage user assigned identity

MLflow operations

To perform MLflow operations with your Azure Machine Learning workspace, use the following scopes your custom role:

MLflow operation	Scope
(V1) List, read, create, update or delete experiments	`Microsoft.MachineLearningServices/workspaces/experiments/*`
(V2) List, read, create, update or delete jobs	`Microsoft.MachineLearningServices/workspaces/jobs/*`
Get registered model by name, fetch a list of all registered models in the registry, search for registered models, latest version models for each requests stage, get a registered model's version, search model versions, get URI where a model version's artifacts are stored, search for runs by experiment ids	`Microsoft.MachineLearningServices/workspaces/models/*/read`
Create a new registered model, update a registered model's name/description, rename existing registered model, create new version of the model, update a model version's description, transition a registered model to one of the stages	`Microsoft.MachineLearningServices/workspaces/models/*/write`
Delete a registered model along with all its version, delete specific versions of a registered model	`Microsoft.MachineLearningServices/workspaces/models/*/delete`

Example custom roles

Data scientist

Allows a data scientist to perform all operations inside a workspace **except**:

- Creation of compute
- Deploying models to a production AKS cluster

- Deploying a pipeline endpoint in production

`data_scientist_custom_role.json` :

JSON

```
{
    "Name": "Data Scientist Custom",
    "IsCustom": true,
    "Description": "Can run experiment but can't create or delete compute or deploy pro-
duction endpoints.",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/*/read",
        "Microsoft.MachineLearningServices/workspaces/*/action",
        "Microsoft.MachineLearningServices/workspaces/*/delete",
        "Microsoft.MachineLearningServices/workspaces/*/write"
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/delete",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/delete",
        "Microsoft.Authorization/*",
        "Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/services/aks/write",
        "Microsoft.MachineLearningServices/workspaces/services/aks/delete",
        "Microsoft.MachineLearningServices/workspaces/endpoints/pipelines/write"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

Data scientist restricted

A more restricted role definition without wildcards in the allowed actions. It can perform all operations inside a workspace **except**:

- Creation of compute
- Deploying models to a production AKS cluster
- Deploying a pipeline endpoint in production

`data_scientist_restricted_custom_role.json` :

JSON

```
{
    "Name": "Data Scientist Restricted Custom",
    "IsCustom": true,
    "Description": "Can run experiment but can't create or delete compute or deploy pro-
duction endpoints",
```

```
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/*/read",
        "Microsoft.MachineLearningServices/workspaces/computes/start/action",
        "Microsoft.MachineLearningServices/workspaces/computes/stop/action",
        "Microsoft.MachineLearningServices/workspaces/computes/restart/action",
        "Microsoft.MachineLearningServices/workspaces/computes/applicationaccess/action",
        "Microsoft.MachineLearningServices/workspaces/notebooks/storage/write",
        "Microsoft.MachineLearningServices/workspaces/notebooks/storage/delete",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/write",
        "Microsoft.MachineLearningServices/workspaces/experiments/write",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/submit/action",
        "Microsoft.MachineLearningServices/workspaces/pipelinedrafts/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/snapshots/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/artifacts/write",
        "Microsoft.MachineLearningServices/workspaces/environments/write",
        "Microsoft.MachineLearningServices/workspaces/models/*/write",
        "Microsoft.MachineLearningServices/workspaces/modules/write",
        "Microsoft.MachineLearningServices/workspaces/components/*/write",
        "Microsoft.MachineLearningServices/workspaces/datasets/*/write",
        "Microsoft.MachineLearningServices/workspaces/datasets/*/delete",
        "Microsoft.MachineLearningServices/workspaces/computes/listNodes/action",
        "Microsoft.MachineLearningServices/workspaces/environments/build/action"
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/computes/write",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/delete",
        "Microsoft.MachineLearningServices/workspaces/delete",
        "Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/listKeys/action",
        "Microsoft.Authorization/*",
        "Microsoft.MachineLearningServices/workspaces/datasets/registered/profile/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/registered/preview/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/unregistered/profile/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/unregistered/preview/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/registered/schema/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/unregistered/schema/read",
        "Microsoft.MachineLearningServices/workspaces/datastores/write",
        "Microsoft.MachineLearningServices/workspaces/datastores/delete"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

MLflow data scientist

Allows a data scientist to perform all MLflow AzureML supported operations **except**:

- Creation of compute
- Deploying models to a production AKS cluster
- Deploying a pipeline endpoint in production

`mlflow_data_scientist_custom_role.json` :

JSON

```
{
    "Name": "MLFlow Data Scientist Custom",
    "IsCustom": true,
    "Description": "Can perform azureml mlflow integrated functionalities that includes
mlflow tracking, projects, model registry",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/experiments/*",
        "Microsoft.MachineLearningServices/workspaces/jobs/*",
        "Microsoft.MachineLearningServices/workspaces/models/*"
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/delete",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/write",
        "Microsoft.MachineLearningServices/workspaces/computes/*/delete",
        "Microsoft.Authorization/*",
        "Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/services/aks/write",
        "Microsoft.MachineLearningServices/workspaces/services/aks/delete",
        "Microsoft.MachineLearningServices/workspaces/endpoints/pipelines/write"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

MLOps

Allows you to assign a role to a service principal and use that to automate your MLOps pipelines. For example, to submit runs against an already published pipeline:

`mlops_custom_role.json` :

JSON

```
{
    "Name": "MLOps Custom",
    "IsCustom": true,
    "Description": "Can run pipelines against a published pipeline endpoint",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/read",
        "Microsoft.MachineLearningServices/workspaces/endpoints/pipelines/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/artifacts/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/snapshots/read",
        "Microsoft.MachineLearningServices/workspaces/environments/read",
        "Microsoft.MachineLearningServices/workspaces/metadata/secrets/read",
        "Microsoft.MachineLearningServices/workspaces/modules/read",
        "Microsoft.MachineLearningServices/workspaces/components/read",
        "Microsoft.MachineLearningServices/workspaces/datasets/*/read",
        "Microsoft.MachineLearningServices/workspaces/datastores/read",
        "Microsoft.MachineLearningServices/workspaces/environments/write",
```

```
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/read",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/write",
        "Microsoft.MachineLearningServices/workspaces/experiments/runs/submit/action",
        "Microsoft.MachineLearningServices/workspaces/experiments/jobs/read",
        "Microsoft.MachineLearningServices/workspaces/experiments/jobs/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/artifacts/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/snapshots/write",
        "Microsoft.MachineLearningServices/workspaces/metadata/codes/*/write",
        "Microsoft.MachineLearningServices/workspaces/environments/build/action",
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/computes/write",
        "Microsoft.MachineLearningServices/workspaces/write",
        "Microsoft.MachineLearningServices/workspaces/computes/delete",
        "Microsoft.MachineLearningServices/workspaces/delete",
        "Microsoft.MachineLearningServices/workspaces/computes/listKeys/action",
        "Microsoft.MachineLearningServices/workspaces/listKeys/action",
        "Microsoft.Authorization/*"
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

Workspace Admin

Allows you to perform all operations within the scope of a workspace, **except**:

- Creating a new workspace
- Assigning subscription or workspace level quotas

The workspace admin also cannot create a new role. It can only assign existing built-in or custom roles within the scope of their workspace:

`workspace_admin_custom_role.json` :

JSON

```
{
    "Name": "Workspace Admin Custom",
    "IsCustom": true,
    "Description": "Can perform all operations except quota management and upgrades",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/*/read",
        "Microsoft.MachineLearningServices/workspaces/*/action",
        "Microsoft.MachineLearningServices/workspaces/*/write",
        "Microsoft.MachineLearningServices/workspaces/*/delete",
        "Microsoft.Authorization/roleAssignments/*"
    ],
    "NotActions": [
        "Microsoft.MachineLearningServices/workspaces/write"
    ],
    "AssignableScopes": [
```

```
        "/subscriptions/<subscription_id>"
    ]
}
```

Data labeling

Data labeler

Allows you to define a role scoped only to labeling data:

`labeler_custom_role.json` :

JSON

```
{
    "Name": "Labeler Custom",
    "IsCustom": true,
    "Description": "Can label data for Labeling",
    "Actions": [
        "Microsoft.MachineLearningServices/workspaces/read",
        "Microsoft.MachineLearningServices/workspaces/labeling/projects/read",
        "Microsoft.MachineLearningServices/workspaces/labeling/projects/summary/read",
        "Microsoft.MachineLearningServices/workspaces/labeling/labels/read",
        "Microsoft.MachineLearningServices/workspaces/labeling/labels/write"
    ],
    "NotActions": [
    ],
    "AssignableScopes": [
        "/subscriptions/<subscription_id>"
    ]
}
```

Troubleshooting

Here are a few things to be aware of while you use Azure role-based access control (Azure RBAC):

- When you create a resource in Azure, such as a workspace, you're not directly the owner of the resource. Your role is inherited from the highest scope role that you're authorized against in that subscription. As an example if you're a Network Administrator, and have the permissions to create a Machine Learning workspace, you would be assigned the Network Administrator role against that workspace, and not the Owner role.
- To perform quota operations in a workspace, you need subscription level permissions. This means setting either subscription level quota or workspace level quota for your managed compute resources can only happen if you have write permissions at the subscription scope.
- When there are two role assignments to the same Azure Active Directory user with conflicting

sections of Actions/NotActions, your operations listed in NotActions from one role might not take effect if they are also listed as Actions in another role. To learn more about how Azure parses role assignments, read How Azure RBAC determines if a user has access to a resource

- To deploy your compute resources inside a VNet, you need to explicitly have permissions for the following actions:
  - `Microsoft.Network/virtualNetworks/*/read` on the VNet resources.
  - `Microsoft.Network/virtualNetworks/subnets/join/action` on the subnet resource.

  For more information on Azure RBAC with networking, see the Networking built-in roles.
- It can sometimes take up to 1 hour for your new role assignments to take effect over cached permissions across the stack.

Next steps

- Enterprise security overview
- Virtual network isolation and privacy overview
- Tutorial: Train and deploy a model
- Resource provider operations