Highlight Note

Access Controls and Permissions

As with any cloud resource, you need to ensure that only authorized users can access and work with assets in an Azure Machine Learning workspace.

For the most part, access to Azure Machine Learning workspace resources is managed through Azure Active Directory (AAD) role-based access control (RBAC). Typically, a user (or a service principal for an application) is authenticated by Azure Active Directory and receives an access token, this token is then used to request access to individual resources, and access is granted (or denied) based on membership of roles that have permission to perform specific actions. The default roles defined for an Azure Machine Learning workspace, and some of their most important permissions, are shown in the following table – but you can add custom roles and set custom permissions.

Permission	Owner	Contributor	Reader
Create workspace	X	X	
Share workspace	X		
Create compute target	X	X	
Attach compute target	X	X	
Attach data stores	X	X	
Run experiments	X	X	
View runs / metrics	X	X	X
Register model	X	X	
Create image	X	X	
Deploy web service	X	X	
View models / images	X	X	X
Call web service	X	X	X

Some resources within an Azure Machine Learning workspace support alternative access methods. For example, compute resources (which we'll explore later) can be configured to allow access via secure shell (SSH); and when you deploy a machine learning model as a service (which again, we'll explore later), you can enable access using an AAD token or by specifying an access key.