Assign an Azure role for access to blob data

- 7 contributors

Contributors to this article

- 
  jimmart-dev
- 
  tamram
- 
  stevenmatthew
- 
  laurabren
- 
  v-alje
- 
  animeshdas11
- 
  shawnweisfeld
-

In this article

Azure Active Directory (AAD) authorizes access rights to secured resources through Azure role-based access control (Azure RBAC). Azure Storage defines a set of Azure built-in roles that encompass common sets of permissions used to access blob data.

When an Azure role is assigned to an Azure AD security principal, Azure grants access to those resources for that security principal. An Azure AD security principal may be a user, a group, an application service principal, or a managed identity for Azure resources.

To learn more about using Azure AD to authorize access to blob data, see Authorize access to blobs using Azure Active Directory.

Note

This article shows how to assign an Azure role for access to blob data in a storage account. To learn about assigning roles for management operations in Azure Storage, see **Use the Azure Storage resource provider to access management resources**.

Assign an Azure role

To access blob data in the Azure portal with Azure AD credentials, a user must have the following role assignments:

- A data access role, such as **Storage Blob Data Reader** or **Storage Blob Data Contributor**
- The Azure Resource Manager **Reader** role, at a minimum

To learn how to assign these roles to a user, follow the instructions provided in Assign Azure roles using the Azure portal.

The Reader role is an Azure Resource Manager role that permits users to view storage account resources, but not modify them. It does not provide read permissions to data in Azure Storage, but only to account management resources. The **Reader** role is necessary so that users can navigate to blob containers in the Azure portal.

For example, if you assign the **Storage Blob Data Contributor** role to user Mary at the level of a container named **sample-container**, then Mary is granted read, write, and delete access to all of the blobs in that container. However, if Mary wants to view a blob in the Azure portal, then the **Storage Blob Data Contributor** role by itself will not provide sufficient permissions to navigate through the portal to the blob in order to view it. The additional permissions are required to navigate through the portal and view the other resources that are visible there.

A user must be assigned the **Reader** role to use the Azure portal with Azure AD credentials. However, if a user has been assigned a role with **Microsoft.Storage/storageAccounts/listKeys/action** permissions, then the user

can use the portal with the storage account keys, via Shared Key authorization. To use the storage account keys, Shared Key access must be permitted for the storage account. For more information on permitting or disallowing Shared Key access, see Prevent Shared Key authorization for an Azure Storage account.

You can also assign an Azure Resource Manager role that provides additional permissions beyond than the **Reader** role. Assigning the least possible permissions is recommended as a security best practice. For more information, see Best practices for Azure RBAC.

Note

Prior to assigning yourself a role for data access, you will be able to access data in your storage account via the Azure portal because the Azure portal can also use the account key for data access. For more information, see **Choose how to authorize access to blob data in the Azure portal**.

Keep in mind the following points about Azure role assignments in Azure Storage:

- When you create an Azure Storage account, you are not automatically assigned permissions to access data via Azure AD. You must explicitly assign yourself an Azure role for Azure Storage. You can assign it at the level of your subscription, resource group, storage account, or container.
- If the storage account is locked with an Azure Resource Manager read-only lock, then the lock prevents the assignment of Azure roles that are scoped to the storage account or a container.
- If you have set the appropriate allow permissions to access data via Azure AD and are unable to access the data, for example you are getting an "AuthorizationPermissionMismatch" error. Be sure to allow enough time for the permissions changes you have made in Azure AD to replicate, and be sure that you do not have any deny assignments that block your access, see Understand Azure deny assignments.

Note

You can create custom Azure RBAC roles for granular access to blob data. For more information, see **Azure custom roles**.