Manage access to your Azure environment with role-based access controls

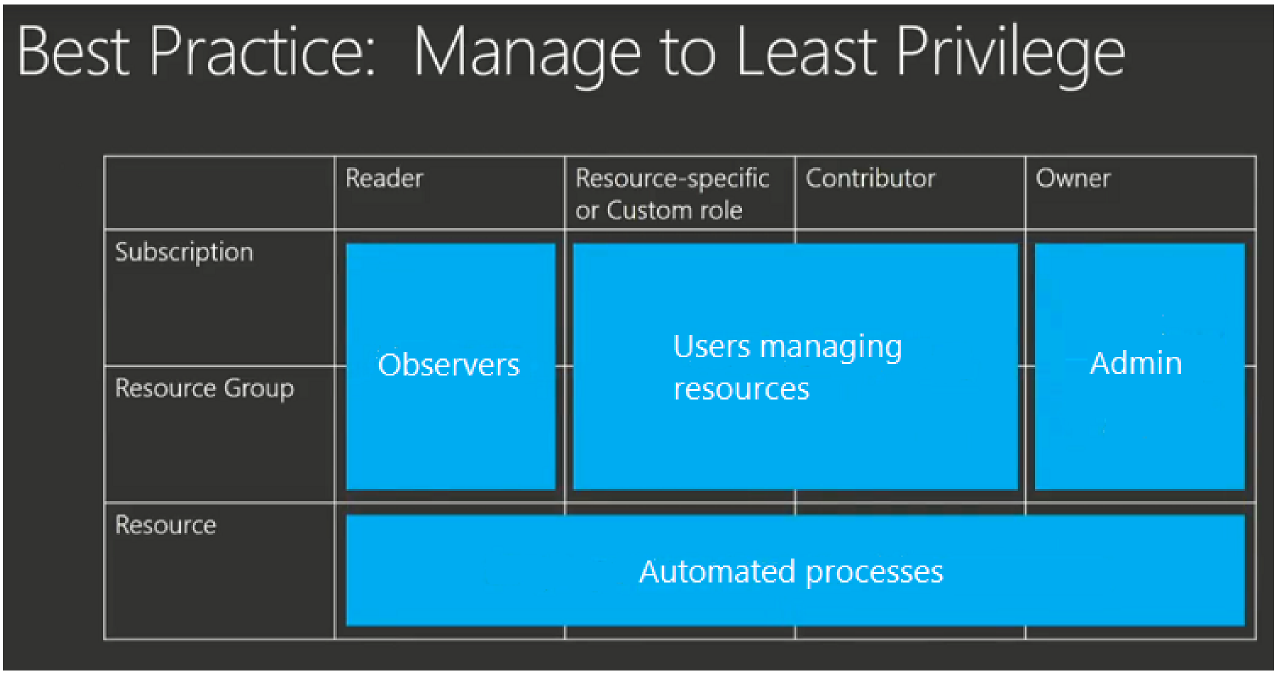
04/09/2019 • 2 minutes to read • Contributors

In this article

Managing who can access your Azure resources and subscriptions is an important part of your Azure governance strategy. Role-based access control (RBAC) is the primary method of managing access in Azure.

RBAC provides detailed access management of resources in Azure. It helps you manage who has access to Azure resources, what they can do with those resources, and what scopes they can access.

When planning your access control strategy, grant users the least privilege required to get their work done. The following image shows a suggested pattern for assigning RBAC.



Best Practice: Manage to Least Privilege

Reader

Resource-specific or Custom role

Contributor

Owner

Subscription

Resource Group

Resource

Observers

Users managing resources

Admin

Automated processes

When you plan your access control methodology, we recommend you work with people in your organizations with the following roles: security and compliance, IT administration, and enterprise architect.

Grant resource group access

To grant a user access to a resource group:

1. Go to Resource groups.
2. Select a resource group.
3. Select **Access control (IAM)**.
4. Select **+Add** > **Add role assignment**.
5. Select a role, then assign access to a user, group, or service principal.

Grant subscription access

To grant a user access to a subscription:

1. Go to Subscriptions
2. Select a subscription.
3. Select **Access control (IAM)**.
4. Select **+Add** > **Add role assignment**.
5. Select a role, then assign access to a user, group, or service principal.

Learn more

To learn more, see What is role-based access control (RBAC)?