✓ 100 XP

Implement role-based access control

3 minutes

Secure access management for cloud resources is critical for businesses that operate in the cloud. Role-based access control (RBAC) is a mechanism that can help you manage who can access your Azure resources. RBAC lets you determine what operations specific users can do on specific resources, and control what areas of a resource each user can access.

Azure RBAC is an authorization system built on Azure Resource Manager. Azure RBAC provides fine-grained access management of resources in Azure.

Things to know about Azure RBAC

Here are some things you can do with Azure RBAC:

- Allow an application to access all resources in a resource group.
- Allow one user to manage VMs in a subscription, and allow another user to manage virtual networks.
- Allow a database administrator (DBA) group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as VMs, websites, and subnets.

Azure RBAC concepts

The following table describes the core concepts of Azure RBAC.

Concept	Description	Examples
Security principal	An object that represents something that requests access to resources.	User, group, service principal, managed identity
Role definition	A set of permissions that lists the allowed operations. Azure RBAC comes with built-in	Some built-in role definitions: *Reader*,

Concept	Description	Examples
	role definitions, but you can also create your own custom role definitions.	*Contributor*, *Owner*, *User Access Administrator*
Scope	The boundary for the requested *level* of access, or "how much" access is granted.	Root, management group, subscription, resource group, resource
Assignment	An **assignment** attaches a **role definition** to a **security principal** at a particular **scope**. Users can grant the access described in a role definition by creating (attaching) an assignment for the role.	- Assign the *User Access Administrator* role to an admin group scoped to a management group - Assign the *Contributor* role to a user scoped to a subscription

Things to consider when using Azure RBAC

As you think about how you can implement roles and scope assignments within your organization, consider these points:

- **Consider your requestors**. Plan your strategy to accommodate for all types of access to your resources. Security principals are created for anything that requests access to your resources. Determine who are the requestors in your organization. Requestors can be internal or external users, groups of users, applications and services, resources, and so on.

- **Consider your roles**. Examine the types of job responsibilities and work scenarios in your organization. Roles are commonly built around the requirements to fulfill job tasks or complete work goals. Certain users like administrators, corporate controllers, and engineers can require a level of access beyond what most users need. Some roles can be defined to provide the same access for all members of a team or department for specific resources or applications.

- **Consider scope of permissions**. Think about how you can ensure security by controlling the scope of permissions for role assignments. Outline the types of permissions and levels of scope that you need to support. You can apply different scope levels for a single role to support requestors in different scenarios.

- **Consider built-in or custom definitions**. Review the built-in role definitions in Azure RBAC. Built-in roles can be used as-is, or adjusted to meet the specific requirements for your organization. You can also create custom role definitions from scratch.

Next unit: Create a role definition

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆