100 XP

Compare Azure roles to Azure Active Directory roles

2 minutes

Three types of roles are available for access management in Azure:

- Classic subscription administrator roles
- Azure role-based access control (RBAC) roles
- Azure Active Directory (Azure AD) administrator roles

To better understand how these different roles are defined and implemented in Azure, it helps to know some of the history.

When Azure was initially released, access to resources was managed with just three administrator roles: *Account Administrator*, *Service Administrator*, and *Co-Administrator*. Access was controlled by assigning admin roles to subscriptions.

Later, role-based access control (RBAC) for Azure resources was added. Azure RBAC is a newer authorization system that provides fine-grained access management to Azure resources. RBAC includes many built-in roles that can be assigned at different scopes. The Azure RBAC model also lets you create your own custom roles.

In addition to Classic subscription admin roles and Azure RBAC roles, Azure AD provides built-in administrator roles to manage Azure AD resources like users, groups, and domains.

Tip

If you're considering using Classic administrator roles, use Azure Resource Manager roles instead. The following table highlights differences between Azure RBAC roles and Azure AD administrator roles.

	Azure RBAC roles	Azure AD admin roles
Access management	Manages access to Azure resources	Manages access to Azure AD resources
Scope assignment	Scope can be specified at multiple levels, including management groups, subscriptions, resource groups, and resources	Scope is specified at the tenant level
Role definitions	Roles can be defined via the Azure portal, the Azure CLI, Azure PowerShell, Azure Resource Manager templates, and the REST API	Roles can be defined via the Azure admin portal, Microsoft 365 admin portal, and Microsoft Graph Azure AD PowerShell

Next unit: Apply role-based access control

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆