✓ 100 XP

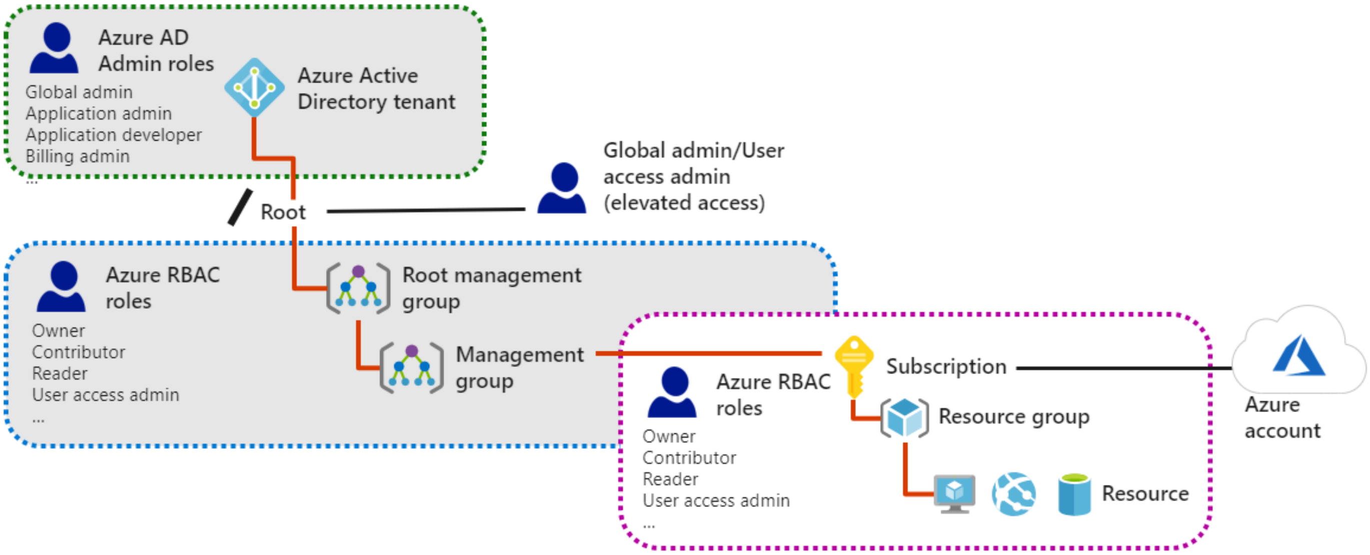
Apply role-based access control

2 minutes

Built-in role definitions in Azure RBAC are defined for several categories of services, tasks, and users. You can assign built-in roles at different scopes to support various scenarios, and build custom roles from the base definitions.

Azure Active Directory (Azure AD) also provides built-in roles to manage resources in Azure AD, including users, groups, and domains. Azure AD offers administrator roles that you can implement for your organization, such as *Global admin*, *Application admin*, and *Application developer*.

The following diagram illustrates how you can apply Azure AD administrator roles and Azure RBAC roles in your organization.



- **Azure AD admin roles** are used to manage resources in Azure AD, such as users, groups, and domains. These roles are defined for the Azure AD tenant at the root level of the configuration.
- **Azure RBAC roles** provide more granular access management for Azure resources. These roles are defined for a requestor or resource and can be applied at multiple levels: the root, management groups, subscriptions, resource groups, or resources.

Next unit: Review fundamental Azure RBAC roles

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆