100 XP

Create a role assignment

2 minutes

A role assignment is the process of scoping a role definition to limit permissions for a requestor, such as a user, group, service principal, or managed identity.

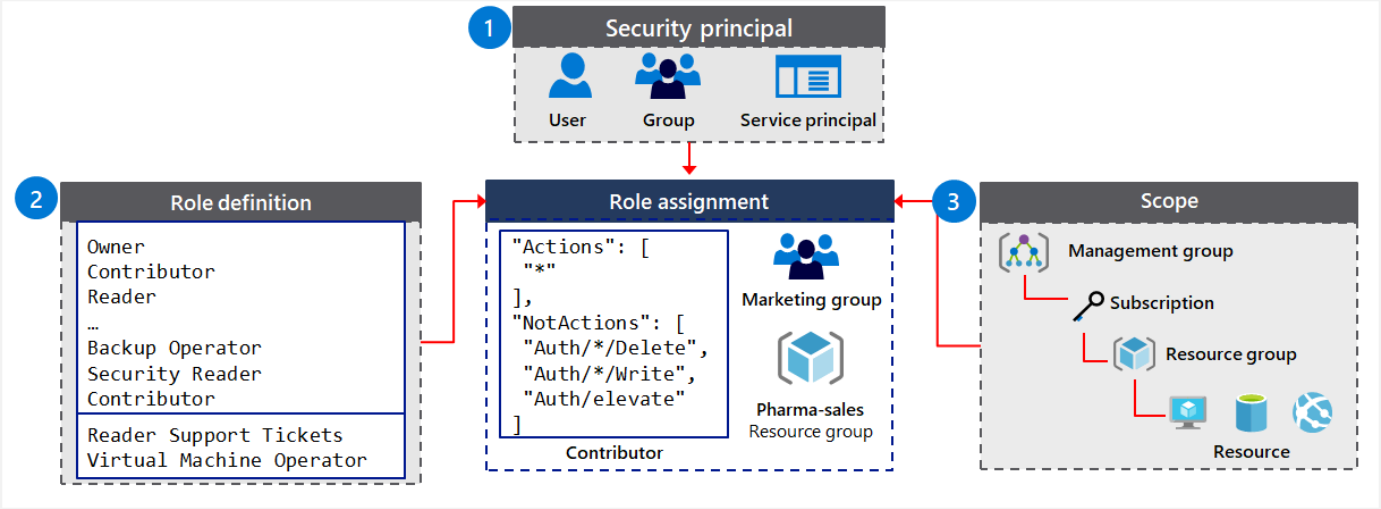
Things to know about role assignments

Review the following characteristics of role assignments:

- The purpose of a role assignment is to control access.
- The scope limits which permissions defined for a role are available for the assigned requestor.
- Access is revoked by removing a role assignment.
- A resource inherits role assignments from its parent resource.
- The effective permissions for a requestor are a combination of the permissions for the requestor's assigned roles, and the permissions for the roles assigned to the requested resources.

Things to consider when assigning scope levels for roles

The following diagram shows an example of how scopes can be applied for a role to grant varying levels of access for different users. Think about how you can implement scopes for your roles to create meaningful assignments for your organization.



This scenario has the following access management configuration:

- Three security principals are supported: user, group, service principal.
- Six built-in roles are implemented, and two custom roles are defined: *Reader Support Tickets* and *Virtual Machine Operator*.
- The built-in *Contributor* role has two sets of permissions: *Actions* and *NotActions*.
- The *Contributor* role is assigned at different scopes to the Marketing group and Pharma-sales resource group:
  - Users in the Marketing group are granted access to create or manage any Azure resource in the Pharma-sales resource group.
  - Marketing users aren't granted access to resources outside the Pharma-sales resource group, unless they have another role assignment that grants them access to the resource group.

Next unit: Compare Azure roles to Azure Active Directory roles

Continue >

How are we doing? ☆ ☆ ☆ ☆ ☆