Manage Role Based Access Control (RBAC)

Mike Pfeiffer
Microsoft Azure MVP

Manage Role Based Access Control

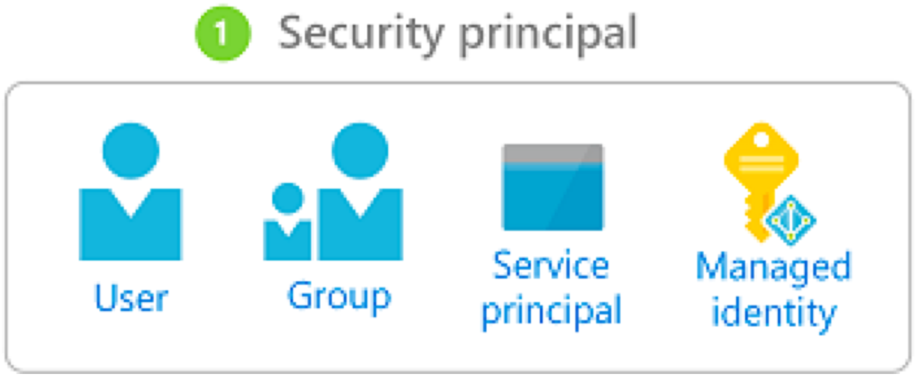
- Create a custom role
- Provide access to Azure resources by assigning roles
  - Subscriptions
  - Resource groups
  - Resources (VM, disk, etc.)
- Interpret access assignments
- Manage multiple directories

What Can I do with RBAC?

- Allow one user to manage virtual machines in a subscription and another user to manage virtual networks
- Allow a DBA group to manage SQL databases in a subscription
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets
- Allow an application to access all resources in a resource group

RBAC: Security Principal

A security principal is an object that represents a user, group, service principal, or managed identity that is requesting access to Azure resources.



RBAC: Security Principal

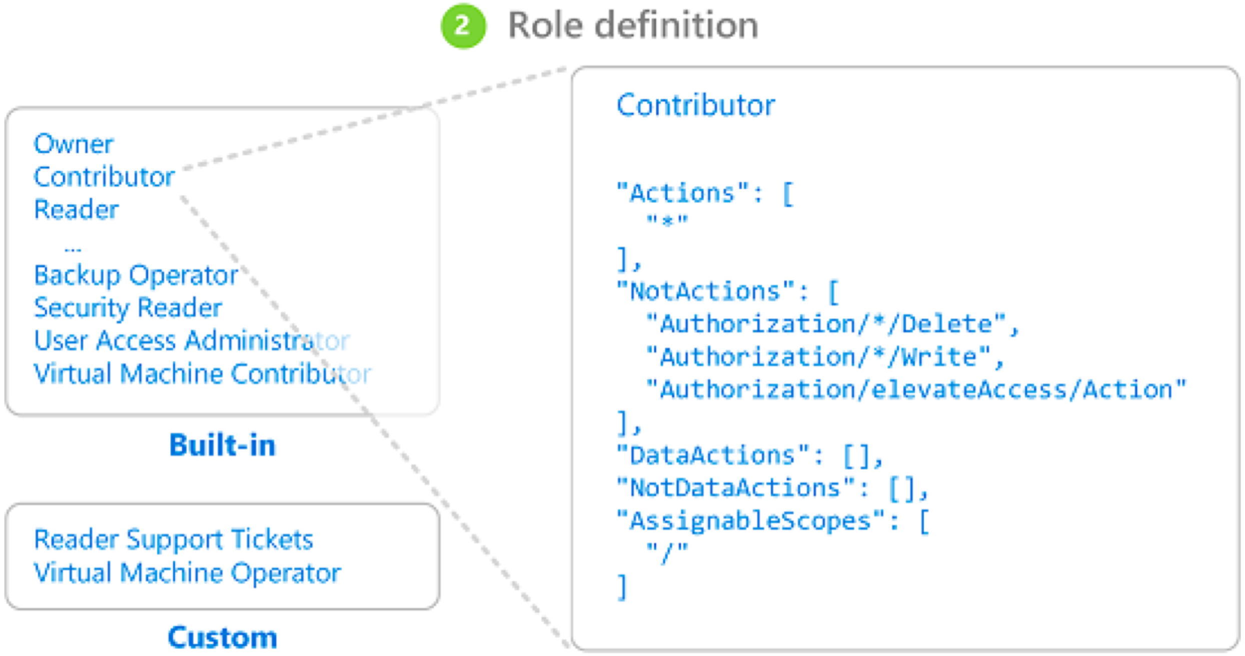
- **User** - An individual who has a profile in Azure Active Directory. You can also assign roles to users in other tenants. For information about users in other organizations, see Azure Active Directory B2B.
- **Group** - A set of users created in Azure Active Directory. When you assign a role to a group, all users within that group have that role.
- **Service principal** - A security identity used by applications or services to access specific Azure resources. You can think of it as a user identity (username and password or certificate) for an application.
- **Managed identity** - An identity in Azure Active Directory that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services.

RBAC: Role Definition

A role definition is a collection of permissions.

It's typically just called a role.

A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.



2 Role definition

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

Contributor

```
"Actions": [
  "*"
],
"NotActions": [
  "Authorization/*/Delete",
  "Authorization/*/Write",
  "Authorization/elevateAccess/Action"
],
"DataActions": [],
"NotDataActions": [],
"AssignableScopes": [
  "/"
]
```

RBAC: Role Definition

Azure includes several built-in roles that you can use. The following lists four fundamental built-in roles. The first three apply to all resource types.

- **Owner** - Has full access to all resources including the right to delegate access to others.
- **Contributor** - Can create and manage all types of Azure resources but can't grant access to others.
- **Reader** - Can view existing Azure resources.

The rest of the built-in roles allow management of specific Azure resources. For example, the Virtual Machine Contributor role allows a user to create and manage virtual machines.

If the built-in roles don't meet the specific needs of your organization, you can create your own custom roles for Azure resources.

RBAC: Scope

Scope is the set of resources that the access applies to.

When you assign a role, you can further limit the actions allowed by defining a scope. This is helpful if you want to make someone a Website Contributor, but only for one resource group.

In Azure, you can specify a scope at multiple levels:

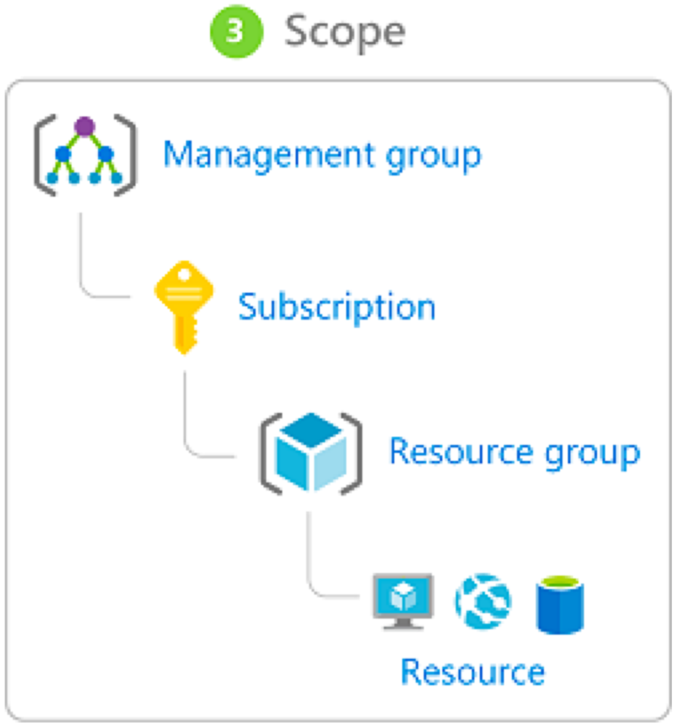
- Management group
- Subscription
- Resource group
- Resource

Scopes are structured in a parent-child relationship.

RBAC: Scope

When you grant access at a parent scope, those permissions are inherited to the child scopes.

- If you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions in the management group.
- If you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource in the subscription.
- If you assign the Contributor role to an application at the resource group scope, it can manage resources of all types in that resource group, but not other resource groups in the subscription.

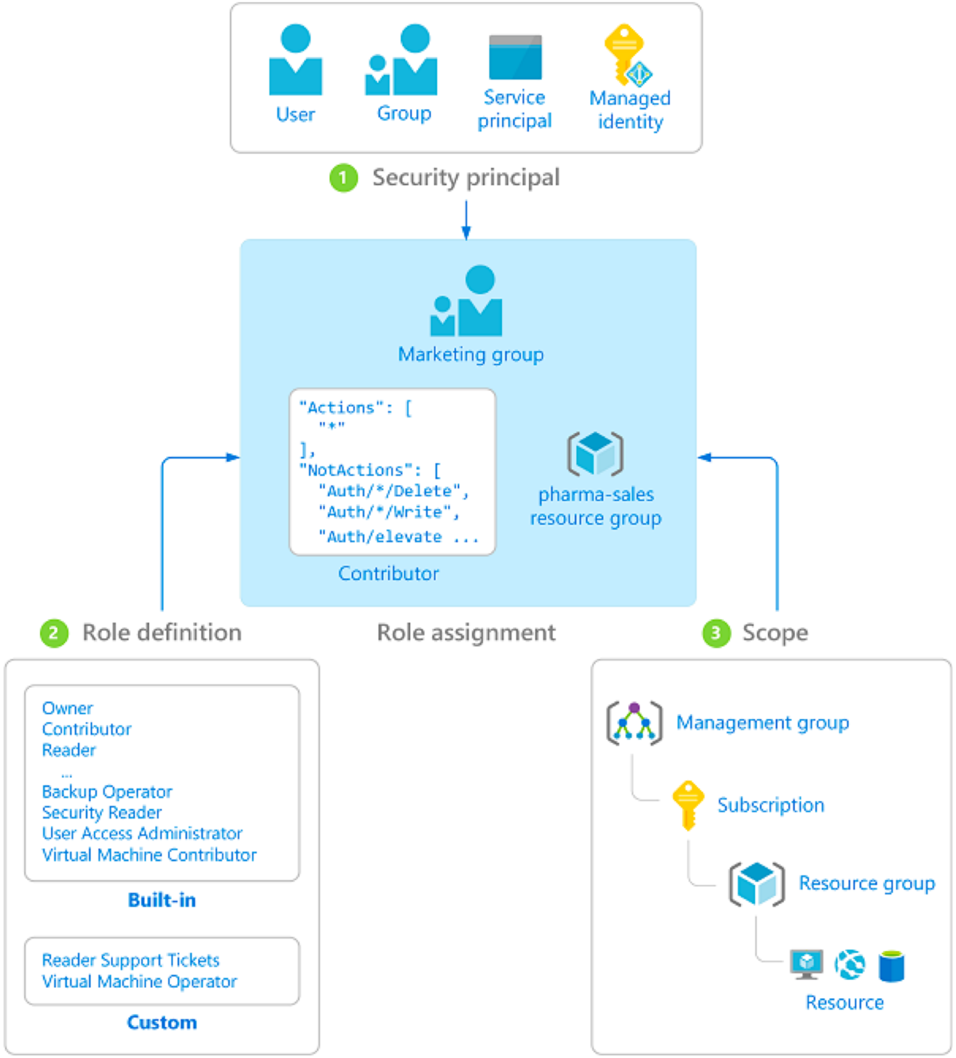


RBAC: Role Assignments

A role assignment is the process of attaching a role definition to a **user**, **group**, **service principal**, or **managed identity** at a particular scope for the purpose of granting access.

Access is granted by creating a role assignment, and access is revoked by removing a role assignment.

RBAC: Role Assignments



User

Group

Service principal

Managed identity

1 Security principal

Marketing group

```
"Actions": [
  "*"
],
"NotActions": [
  "Auth/*/Delete",
  "Auth/*/Write",
  "Auth/elevate ...
```

Contributor

pharma-sales resource group

2 Role definition

Role assignment

3 Scope

Owner
Contributor
Reader
...
Backup Operator
Security Reader
User Access Administrator
Virtual Machine Contributor

Built-in

Reader Support Tickets
Virtual Machine Operator

Custom

Management group

Subscription

Resource group

Resource

RBAC: Multiple Role Assignments

RBAC is an **additive model**, so your effective permissions are the sum of your role assignments.

- Consider a scenario where a user is granted the Contributor role at the subscription scope and the Reader role on a resource group.

- The sum of the Contributor permissions and the Reader permissions is effectively the Contributor role for the resource group. Therefore, in this case, the Reader role assignment has no impact.

RBAC: Deny Statements

Similar to a role assignment, a deny assignment attaches a set of deny actions to a user, group, or service principal at a particular scope for the purpose of denying access.

Deny assignments block users from performing specific Azure resource actions even if a role assignment grants them access.

Deny assignments are created and managed by Azure to protect resources. Azure Blueprints and Azure managed apps use deny assignments to protect system-managed resources. Azure Blueprints and Azure managed apps are the only way that deny assignments can be created. **You can't directly create your own deny assignments**.

How RBAC determines if a user has access to a resource

1. A user (or service principal) acquires a token for Azure Resource Manager.
2. The token includes the user's group memberships (including transitive group memberships).
3. The user makes a REST API call to Azure Resource Manager with the token attached.
4. Azure Resource Manager retrieves all the role assignments and deny assignments that apply to the resource upon which the action is being taken.
5. Azure Resource Manager narrows the role assignments that apply to this user or their group and determines what roles the user has for this resource.
6. Azure Resource Manager determines if the action in the API call is included in the roles the user has for this resource.
7. If the user doesn't have a role with the action at the requested scope, access is not granted. Otherwise, Azure Resource Manager checks if a deny assignment applies.
8. If a deny assignment applies, access is blocked. Otherwise access is granted.

Manage Role Based Access Control

- Create a custom role
- Provide access to Azure resources by assigning roles
  - Subscriptions
  - Resource groups
  - Resources (VM, disk, etc.)
- Interpret access assignments
- Manage multiple directories