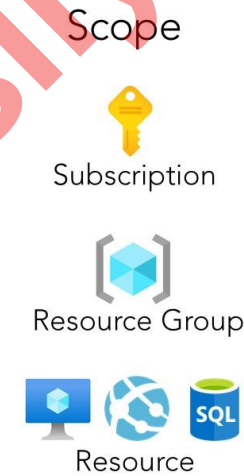


Azure Role-Based Access Control (RBAC)

Azure Role-Based Access Control

- ✓ Component of Azure's identity and access management system
- ✓ Defines who can do what with Azure resources



Role Definition



Security Principal



Azure Role-Based Access Control (RBAC)

Main Components of RBAC

Security Principal:

- ✓ Represents a user, group, service principal, or managed identity that is requesting access to Azure resources ✓

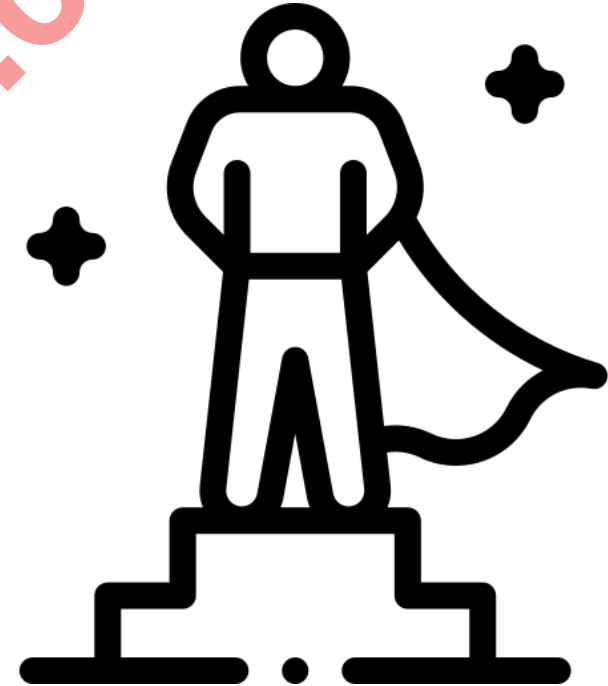


Azure Role-Based Access Control (RBAC)

Main Components of RBAC

Role Definition:

- ✓ Collection of permissions
- ✓ Built-in roles, such as Owner, Contributor, and Reader. Custom roles can also be created ✓

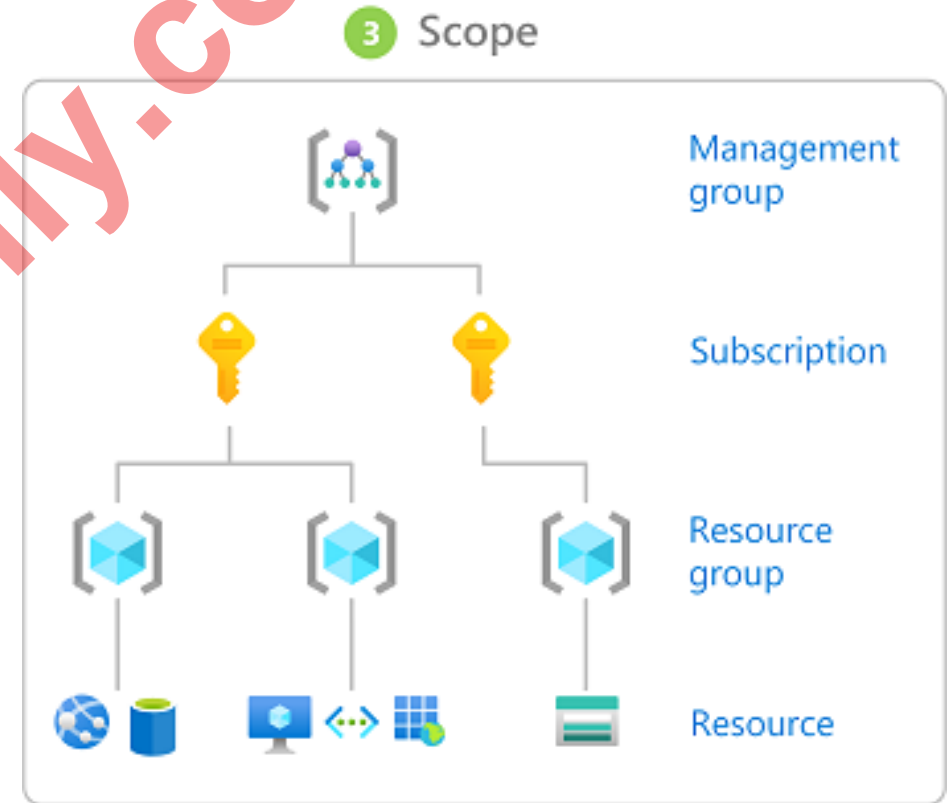


Azure Role-Based Access Control (RBAC)

Main Components of RBAC

Scope:

- ✓ Set of resources that the access applies to
- ✓ Specify a scope at four levels: management group, subscription, resource group, or resource.
- ✓ Scopes are structured in a parent-child relationship. ✓

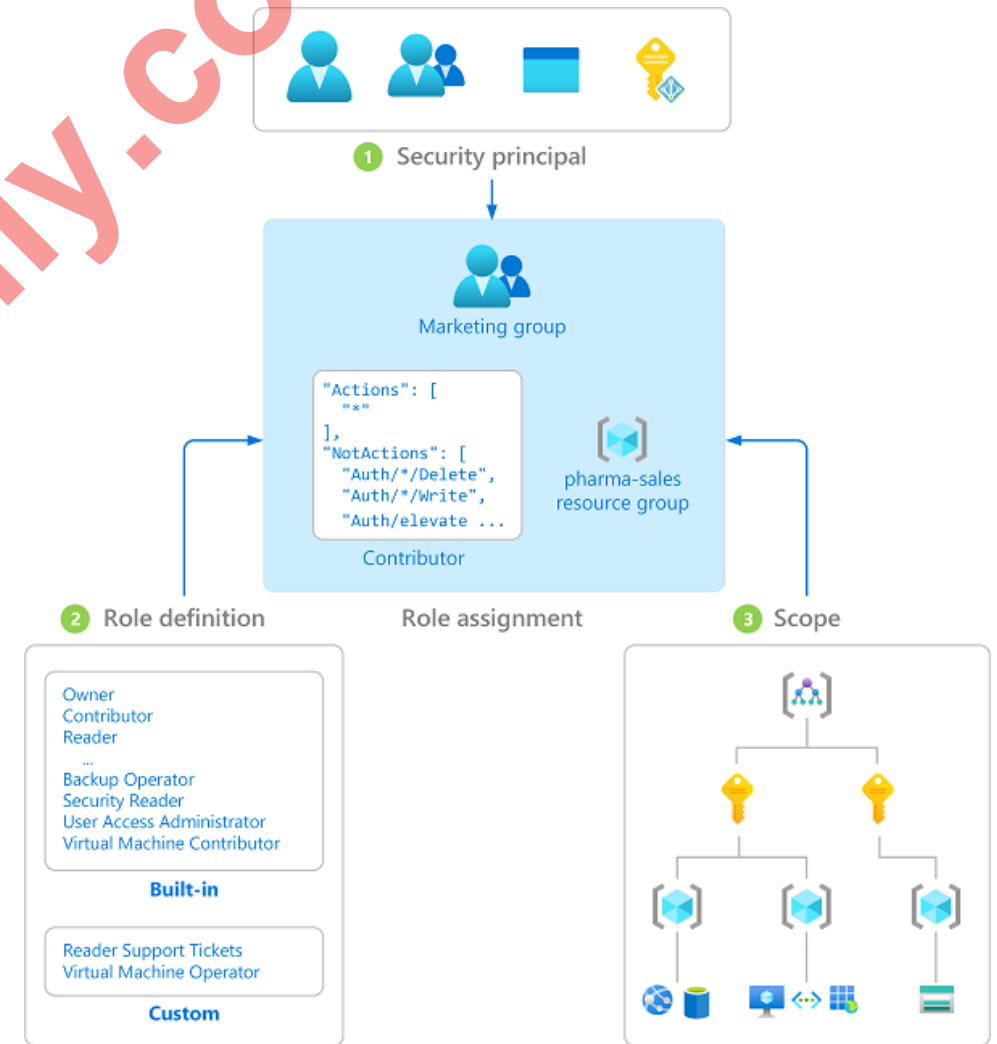


Azure Role-Based Access Control (RBAC)

Main Components of RBAC

Role assignments:

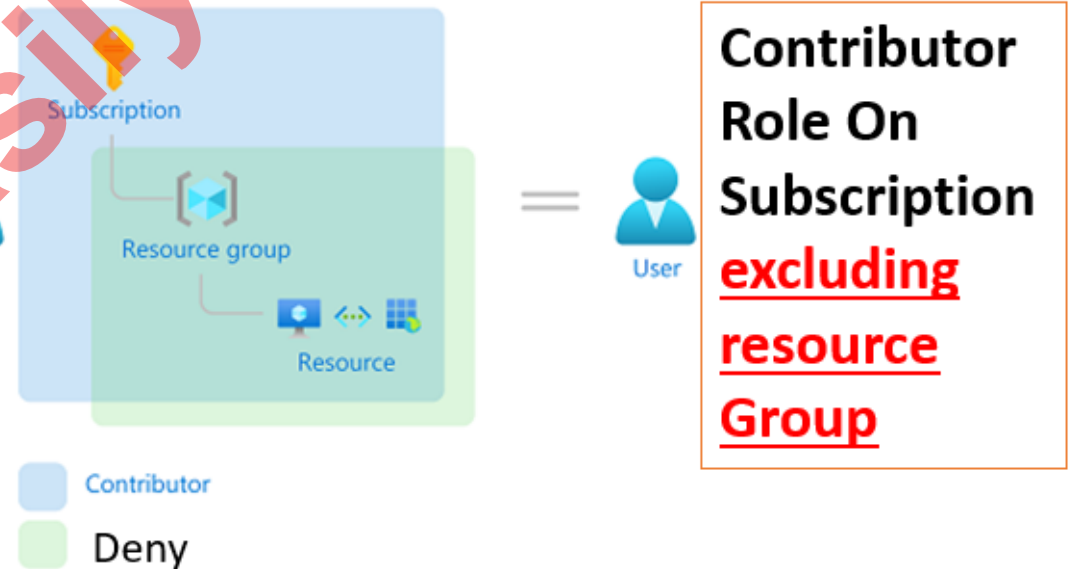
- ✓ Process of attaching a role definition to a user, group, service principal, or managed identity at a particular scope for the purpose of granting access. ✓



Azure Role-Based Access Control (RBAC)

In Case Of Overlapping Role Assignments

- ✓ Azure RBAC is an additive model, so your effective permissions are ones that has higher scope and higher permission
- ✓ Deny assignments take precedence over role assignments ✓



Azure Role-Based Access Control (RBAC)

Azure Built-In Roles

- ✓ **Owner:** Full access to all resources, including the ability to delegate access.
- ✓ **Contributor:** Full access to all resources, but without the ability to delegate access.
- ✓ **Reader:** View-only access to resources.
- ✓ **User Access Administrator:** Manage user access to resources.
- ✓ **Security Reader:** View security-related configurations.
- ✓ **Network Contributor:** Manage network-related configurations.



Azure Role-Based Access Control (RBAC)

Common Use Cases

- ✓ Enabling developers to **manage resources within their resource groups.**
- ✓ Allowing a security team to **audit resource configurations.**
- ✓ Providing **read-only access to auditors.**
- ✓ **Assigning specific roles** for managing virtual machines, databases, or storage accounts.
- ✓ Where only **authorized users** should access and manage **Azure resources.** ✓

