Microsoft Azure Fundamentals
Training Bootcamp

Azure RBAC Fundamentals 101

Azure RBAC Overview

- RBAC is an authorization system built on Azure Resource Manager that you can use to provide granular access to Azure resources

- RBAC helps you manage WHO has access to Azure resources, WHAT they can do with those resources and WHAT areas they have access to

- Best practice ! – grant minimum permissions (least privilege) to users or services in order to perform their job

Azure RBAC - Common Use Cases

- Allow a user to manage VMs (or some Azure resource) in a subscription
- Allow an application to access all resources in a RG
- Allow a user to manage all resources in a RG, such as virtual machines, websites and subnets
- Allow the databases team to manage (only) the SQL databases in a subscription

Azure RBAC – How it works

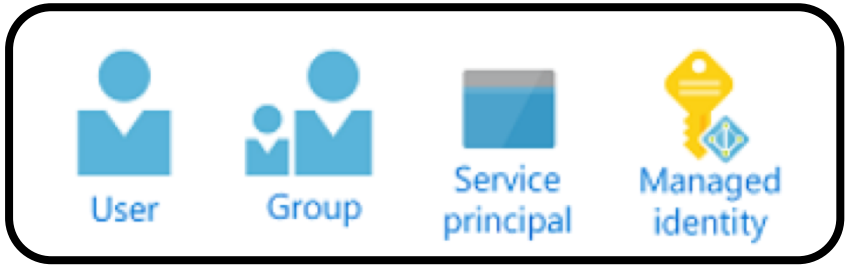
- With RBAC, you can control access to resources using role assignments - it's how permissions are enforced

- A role assignment consists of three elements:
  - Security principal
  - Role definition
  - Scope

- First, we will define each of the components and last we will see how all fit together and talk about role assignments

Azure RBAC – Security Principal

- A security principal is an object that is requesting access to Azure resources - user, group, service principal or managed identity
- User - individual who has a profile in Azure AD
- Group – a set of users in Azure AD
- Service Principal – security identity of an app or service
- Managed Identity – identity in Azure AD, Azure managed



Azure RBAC – Role Definition

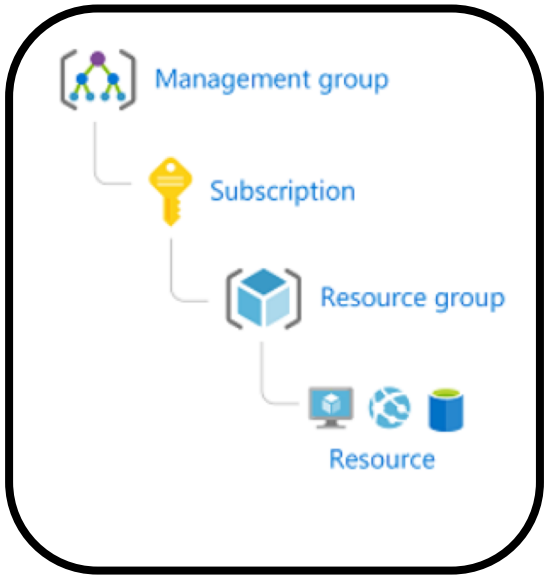
- A role definition, or simply just role, is a collection of permissions (operations permitted: read, write and delete)

- Azure includes custom roles and built-in roles :
  - Owner – Full admin permissions
  - Contributor - create and manage any Azure resources, but can't grant access to others
  - Reader - can view existing Azure resources

- Other built-in roles are available, targeting specific Azure resources; e.g. Virtual Machine Contributor

Azure RBAC – Scope

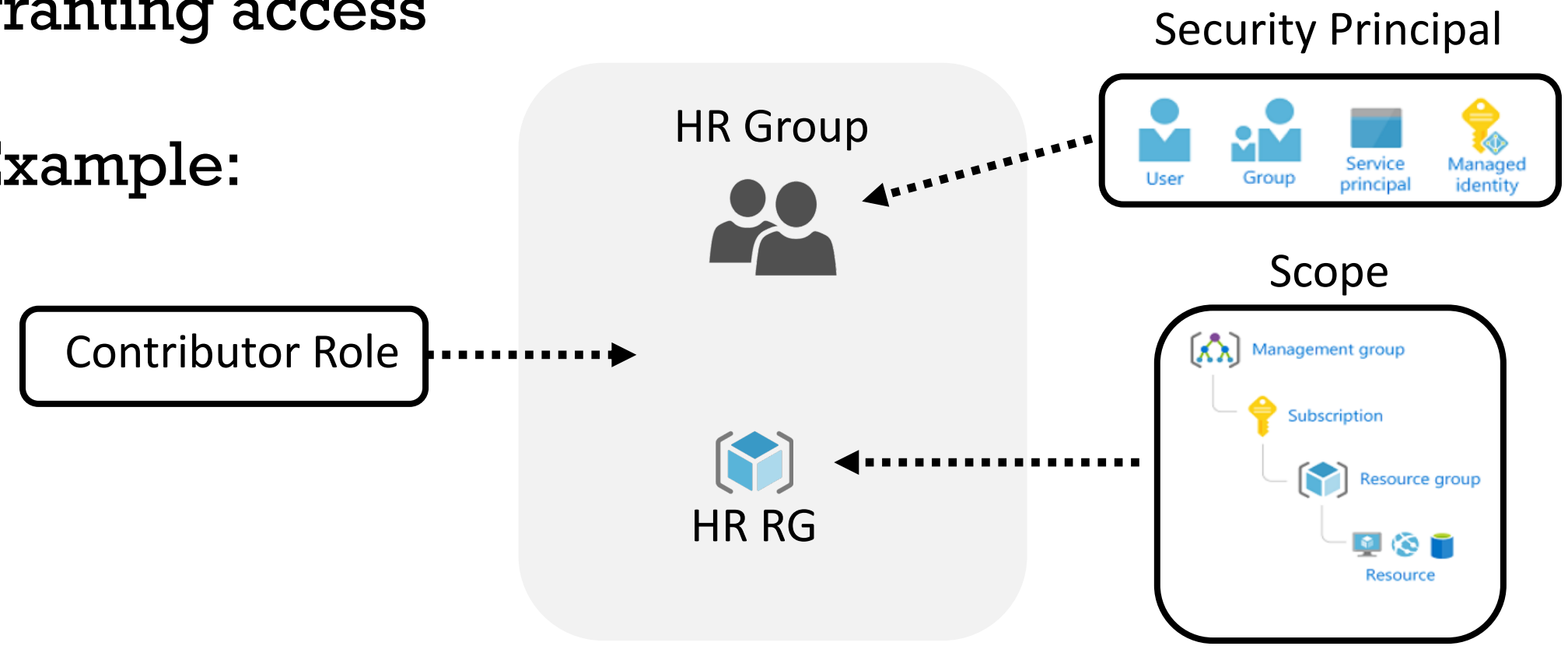
- Scope is the set of resources that the access applies to
- When you assign a role, you can further limit the actions allowed by defining a scope; e.g. VM Contributor for a specific Resource Group
- You can specify scope at multiple levels; structured in a parent-child relationship
- When you grant access at a parent scope, permissions are inherited to the child scopes



Azure RBAC – Role Assignment

- A role assignment is the process of attaching a role definition to a security principal, at a particular scope, for the purpose of granting access

- Example:



Microsoft Azure Fundamentals
Training Bootcamp

Thank you