Microsoft

Introduction to Azure SQL

Module 1

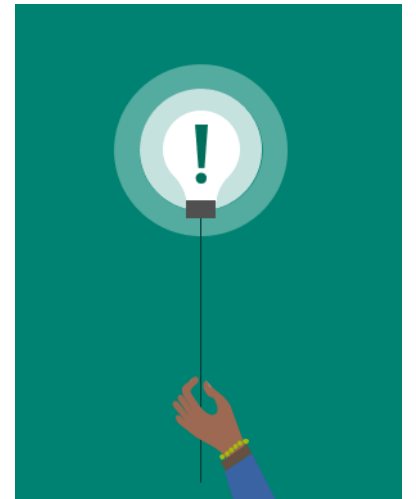# Learning Units covered in this Module

- Lesson 1: Implement Entra ID Security

- Lesson 2: Manage Logins in Azure SQL

- Lesson 3: Azure Role Based Access Control

Lesson 1: Implement Entra ID Security

Objectives

After completing this learning, you will be able to:

· Know how to leverage Entra ID security for authenticating connections to an Azure SQL Database.
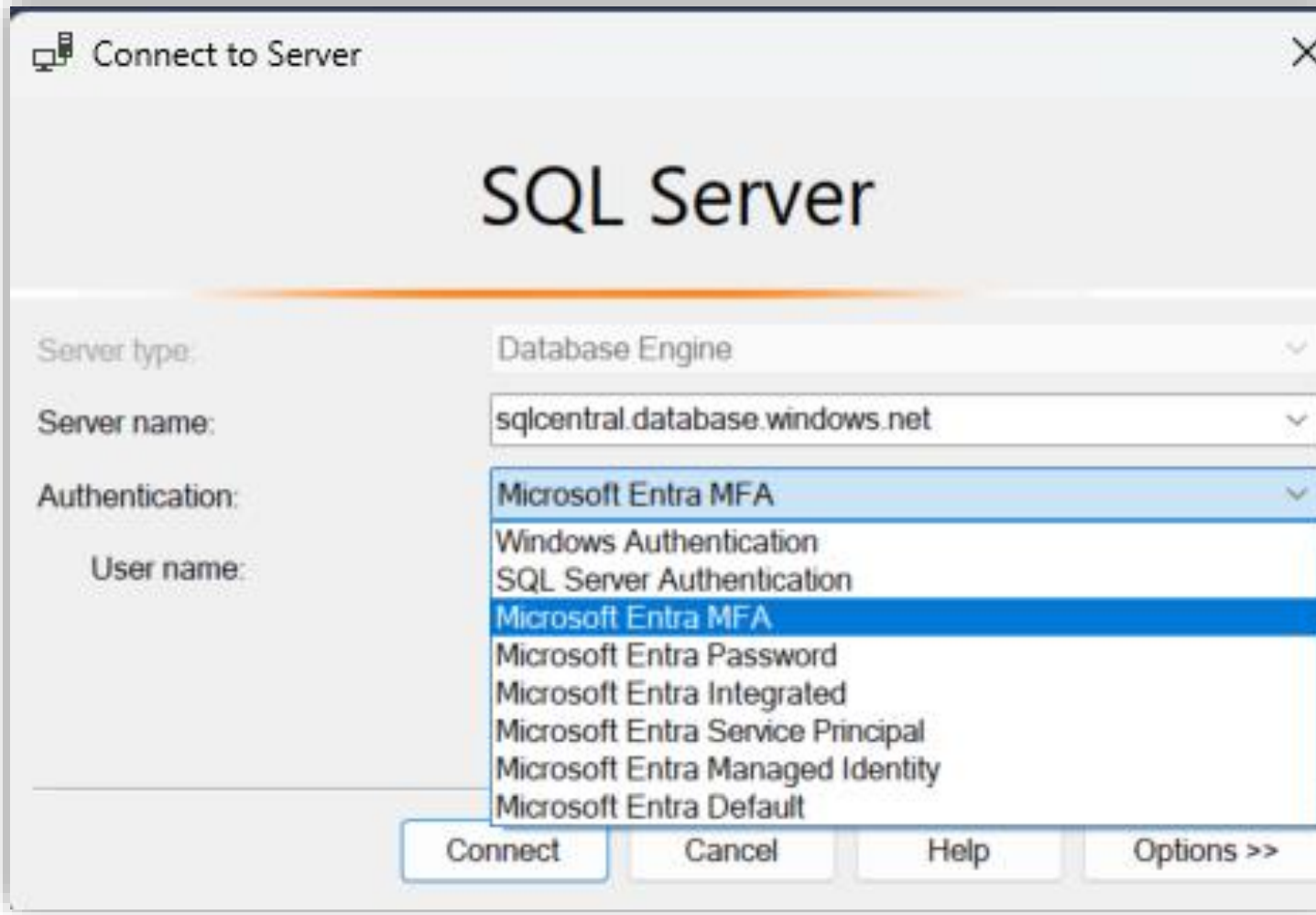
Entra ID Security

Azure Active Directory is now called Entra ID authentication.

Authentication is a mechanism of connecting to Microsoft Azure SQL Database by using identities in Entra ID

Azure SQL Database

Customer 1
Customer 2
Customer 3
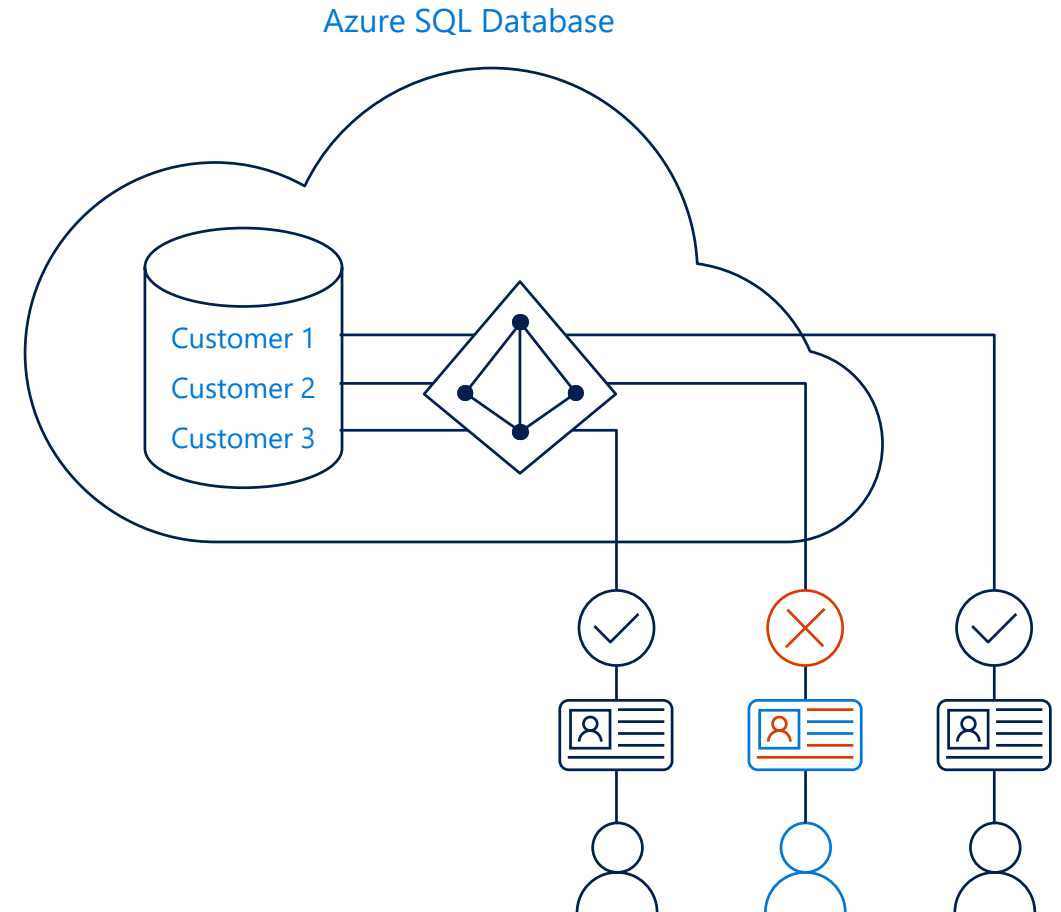
Types of Entra ID Authentication

Benefits of Entra Authentication

Centrally manage user permissions.

Alternative to SQL Server authentication.

Allows password rotation in a single place.

Enables management of database permissions using external Entra ID groups.

Stops password storing by using integrated Windows authentication and other forms of authentication supported by Entra ID.

Trust architecture
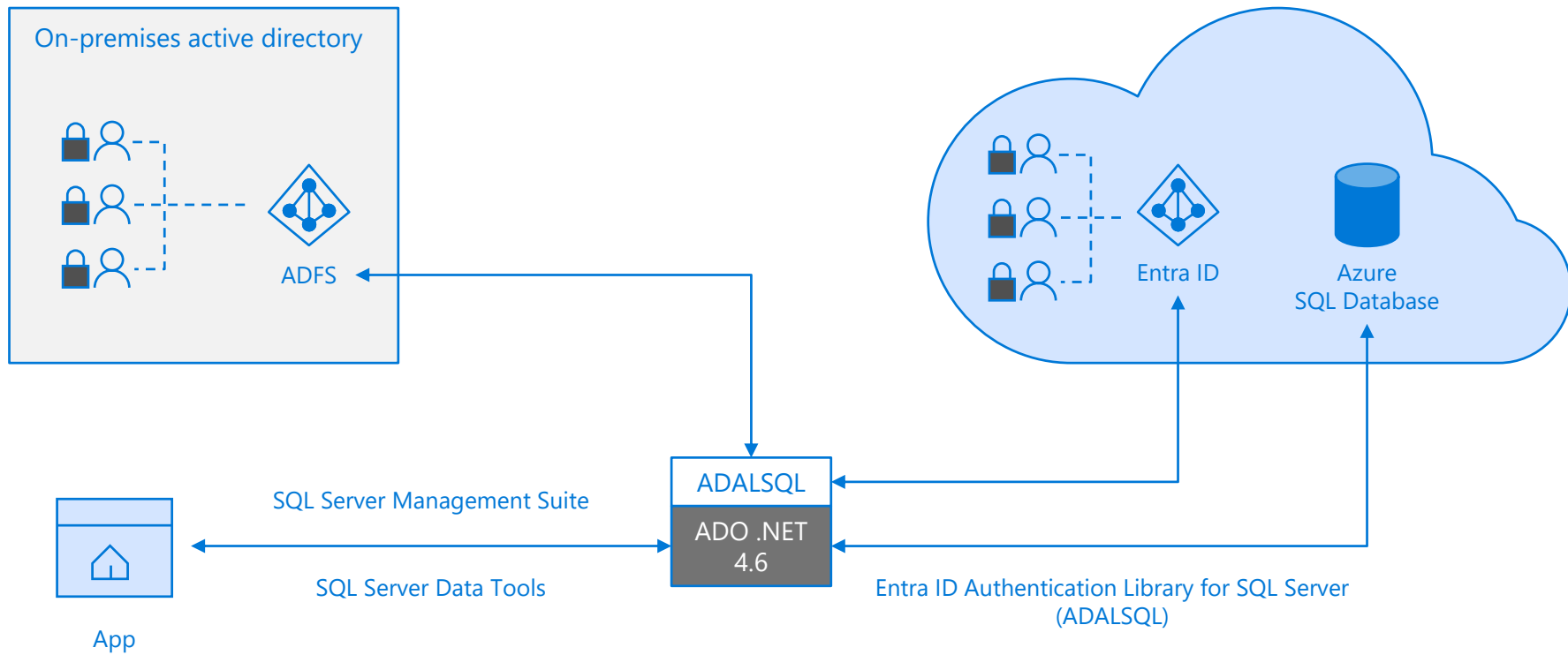
Demonstration

Implement Entra ID Authentication

- Connect to Entra ID.
- Connect to Azure SQL DB using SSMS through Entra ID authentication.

Questions?

Knowledge Check

List three benefits of Azure Activity Directory Authentication.

Can we use Windows authentication for Azure SQL Database?

Lesson 2: Manage Logins in Azure SQL Database

Objectives

After completing this learning, you will be able to:

· Manage logins within Azure SQL Database.

Unrestricted Administrative Accounts
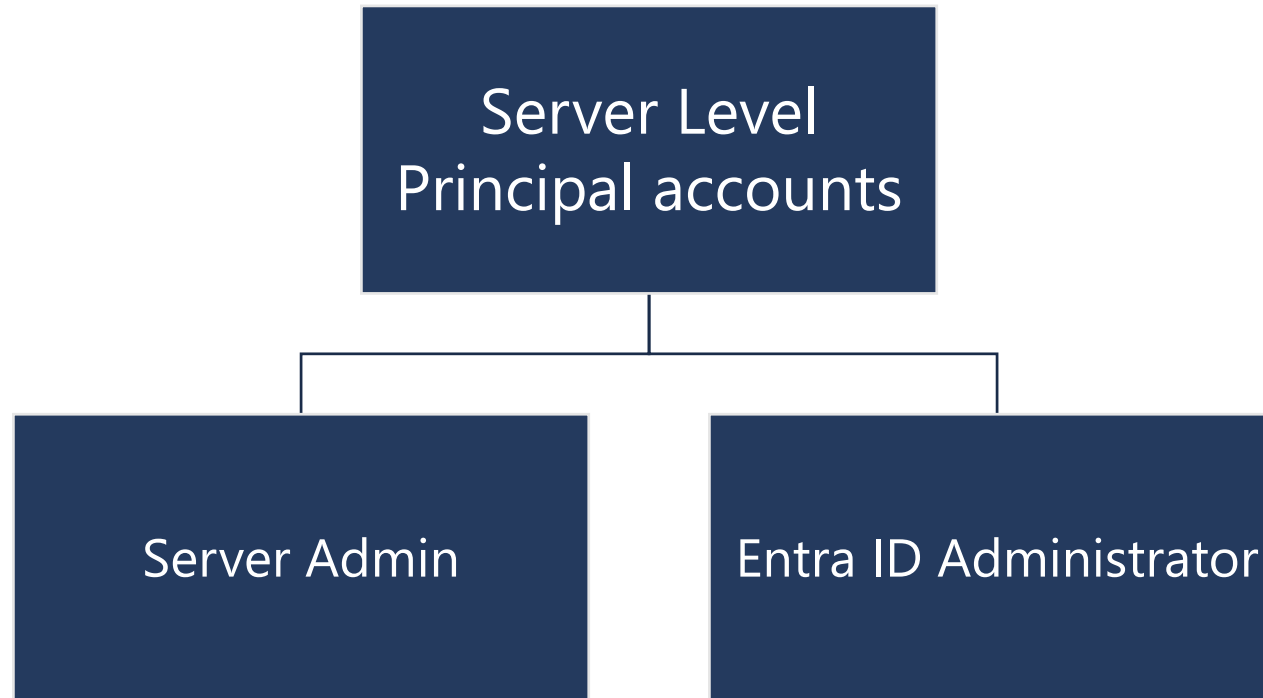
Administrator Access Path

Entra ID Directory

Entra ID admin
- A single account (can be a user or group)
- Optional if not using Entra ID Authentication
- Required if using Entra ID Authentication

SQL Server Admin Account

Server-level Firewall

Master database
- Uses Entra ID Authentication
- Uses SQL Server Authentication
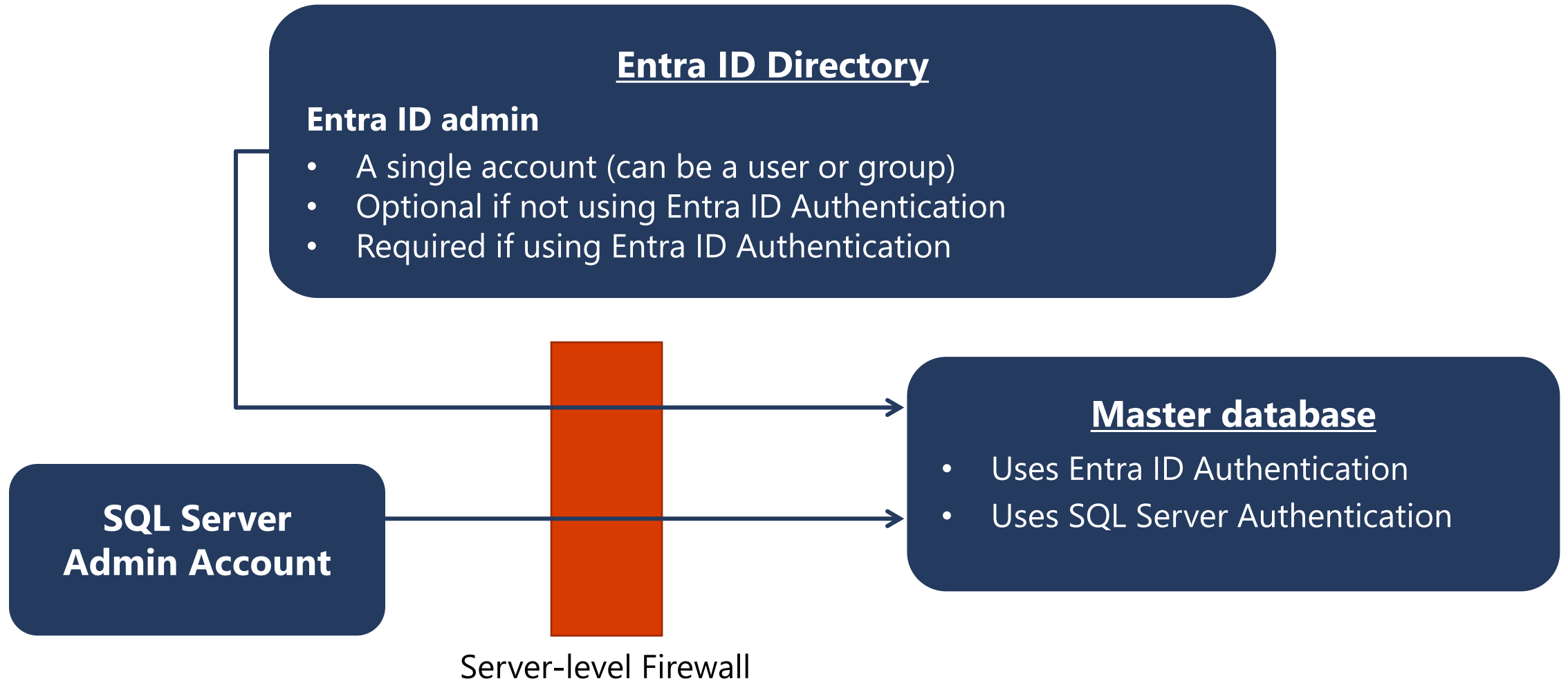
Additional Special Roles

Database Creators

· ALTER ROLE dbmanager* ADD MEMBER Mary;

· ALTER ROLE dbmanager* ADD MEMBER [mike@contoso.com];

Create a server-level login → Create a user in virtual master → Add to dbmanager

*dbmanager is a database role in virtual master database.

Additional Special Roles (continued)

Login Managers

- ALTER ROLE loginmanager* ADD MEMBER Mary;
- ALTER ROLE loginmanager* ADD MEMBER [mike@contoso.com];

Create a server-level login	→	Create a user in virtual master or contained user (preferred)	→	Add to loginmanager
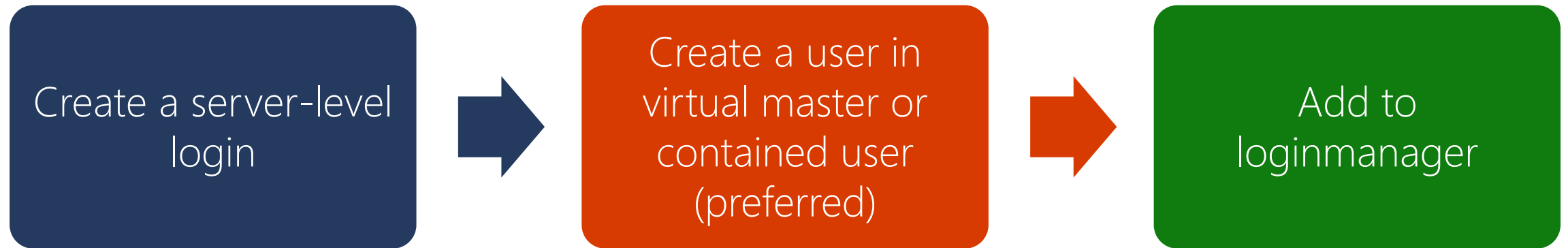
*loginmanager is a database role in virtual master database.

Non-administrator Users

- Generally, non-administrator accounts do not need access to the virtual master database.

- Create contained database users at the database level.

Options:

Entra ID authentication contained database user.	SQL Server authentication contained database user.	SQL Server authentication user based on a SQL Server authentication login.

Groups and Roles

Entra ID authentication

- Put Entra ID users into an Entra ID group.

- Create a contained database user for the group.

- Place one or more database users into a database role.

- Assign permissions to the database role.

SQL Server authentication

- Create contained database users in the database.

- Place one or more database users into a database role.

- Assign permissions to the database role.

Database Roles

The database roles can be the built-in roles such as:

db_owner	db_ddladmin	db_datawriter
db_datareader	db_denydatawriter	db_denydatareader

Naming Requirements

Certain usernames are not allowed for security reasons. You cannot use the following names:

admin

administrator

guest

root

sa

Demonstration

Connect to an Azure SQL DB using SQL Authentication

- Using SQL Login + SQL User.
- Using Contained Database User.

Questions?

Lesson 3: Azure Role Based Access Control (RBAC)

Azure Role-Based Access Control (RBAC)

What is Azure Role-Based Control (RBAC)

- Access management for cloud resources is a critical function for any organization that is using the cloud
- Role-based access control (RBAC) helps you manage who has access to Azure resources, what they can do with those resources, and what areas they have access to.

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

Azure RBAC Role Assignment
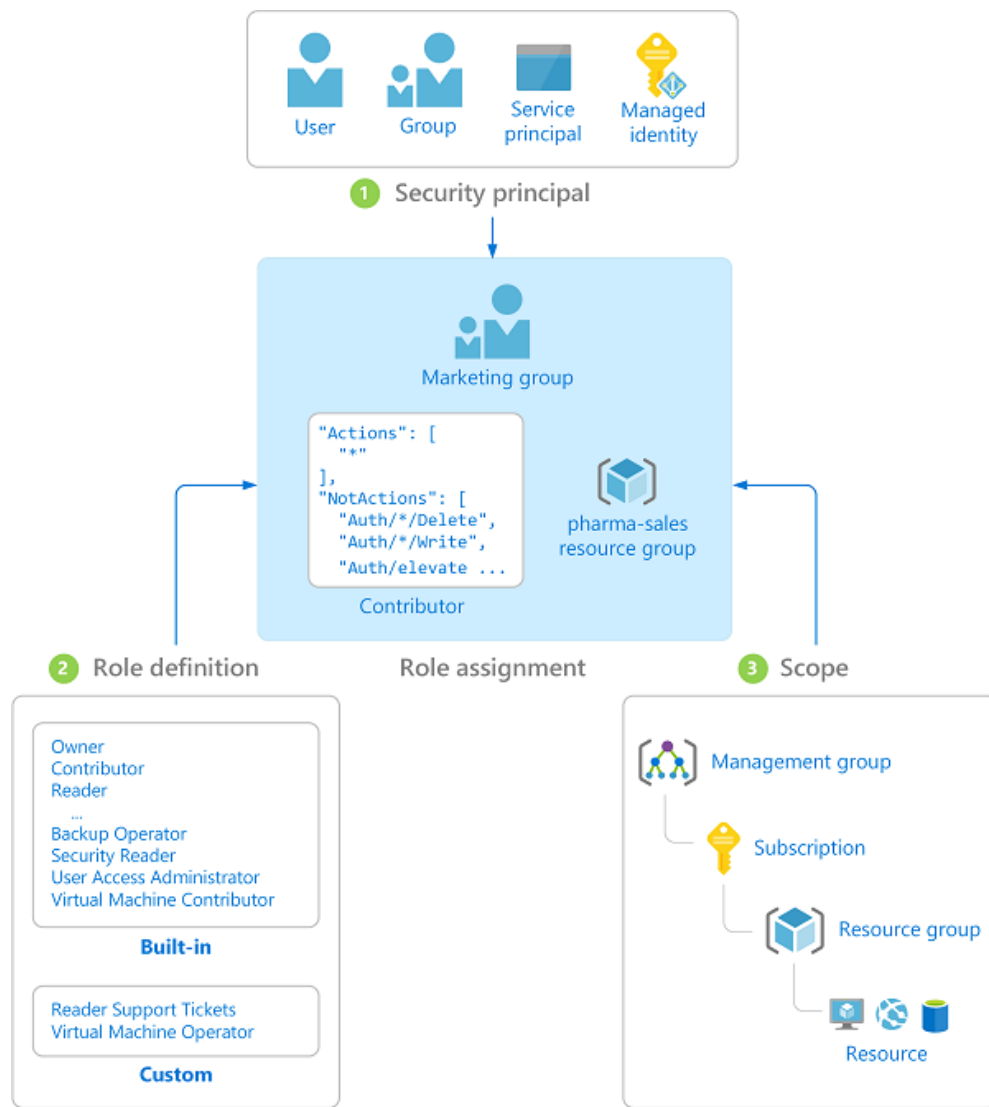
Azure RBAC – Security Principals

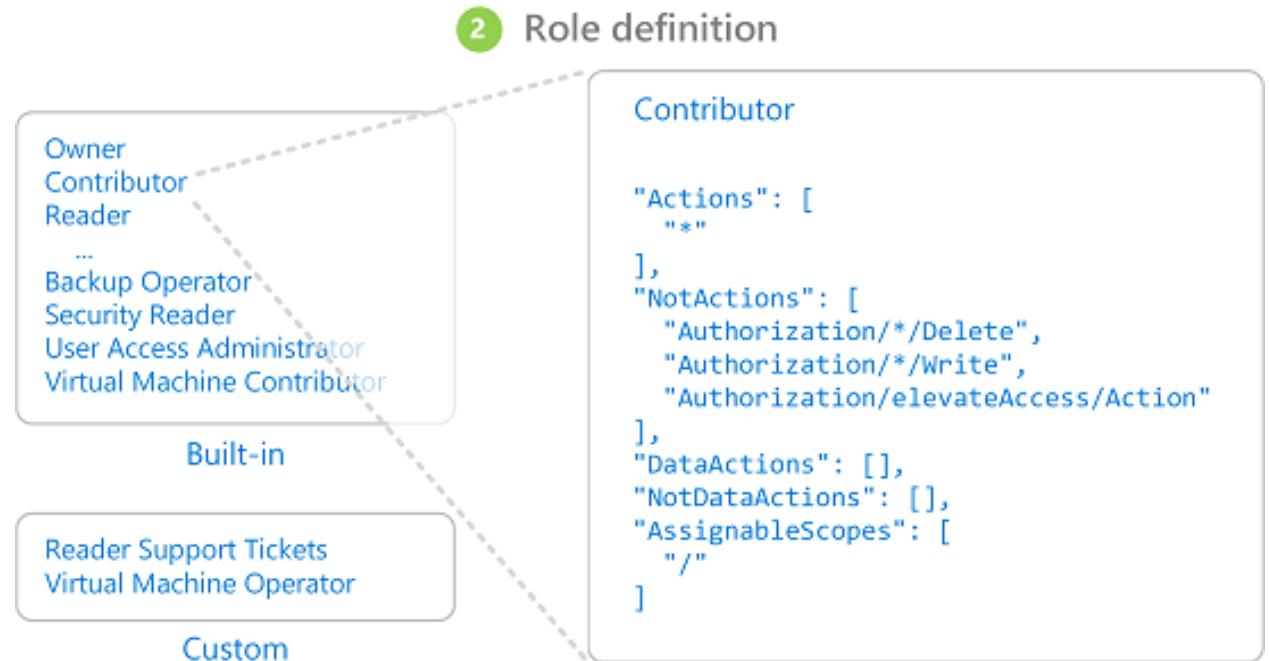| User	Group	Service principal	Managed identity
• An individual who has a profile in Entra ID. You can also assign roles to users in other tenants.	• A set of users created in Entra ID. When you assign a role to a group, all users within that group have that role.	• A security identity used by applications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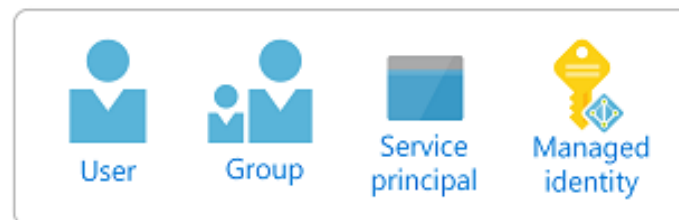
Azure RBAC – Role Definition

A role definition is a collection of permissions. It's sometimes 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": [
  "/"
]
```

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.

In Azure, you can specify a scope at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent-child relationship.
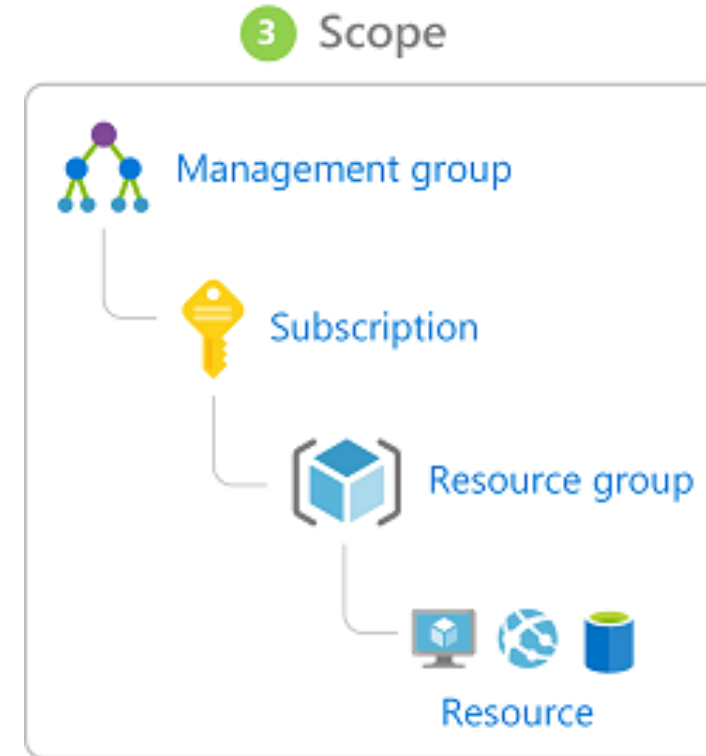
Azure Built-In Roles

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

Azure SQL Database Roles

Roles	Rights
SQL Server Contributor	Allows for managing SQL servers and databases but not access to the data within them.
SQL Database Contributor	Permits management of SQL databases, including creating and deleting databases, but does not grant access to the data.
SQL Security Manager	Enables management of SQL security policies and auditing settings.
SQL Managed Instance Contributor	Allows for managing SQL Managed Instances, including creating and deleting instances, but not access to the data.
SQL Backup Contributor	Grants permissions to manage backup operations on SQL database

Azure RBAC Limits

Resource	Limit
Role assignments for Azure resources per Azure subscription	2000
Role assignments for Azure resources per management group	500
Custom roles for Azure resources per tenant	5000