



Access & Permissions

Module 2



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:

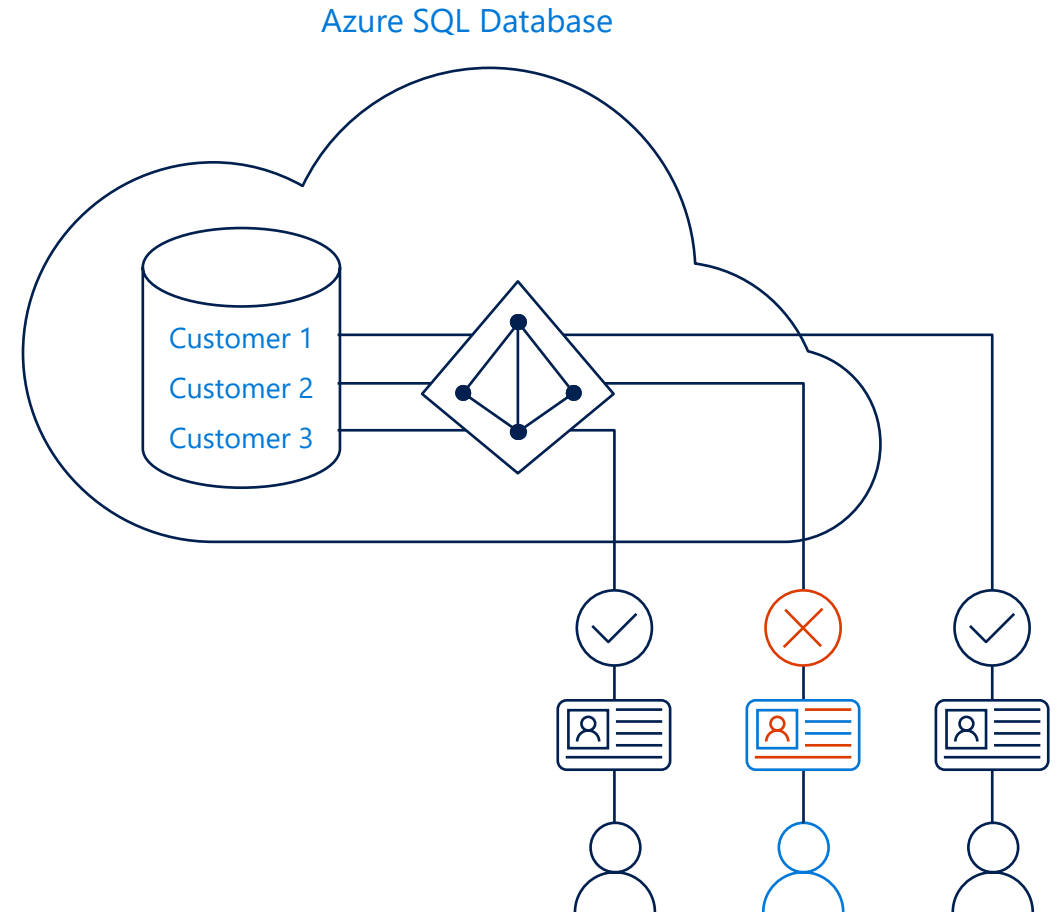
- Know how to leverage Entra ID security for authenticating connections to an Azure SQL Database.



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



Types of Entra ID Authentication

The screenshot shows the 'Connect to Server' dialog box with the following fields and options:

- Server type:** Database Engine
- Server name:** sqlcentral.database.windows.net
- Authentication:** A dropdown menu is open, showing the following options:
 - Microsoft Entra MFA (highlighted)
 - Windows Authentication
 - SQL Server Authentication
 - Microsoft Entra MFA (highlighted)
 - Microsoft Entra Password
 - Microsoft Entra Integrated
 - Microsoft Entra Service Principal
 - Microsoft Entra Managed Identity
 - Microsoft Entra Default
- User name:** (empty field)

At the bottom of the dialog, there are four buttons: **Connect**, **Cancel**, **Help**, and **Options >>**.

Benefits of Entra Authentication

Centrally manage user permissions.

Alternative to SQL Server authentication.

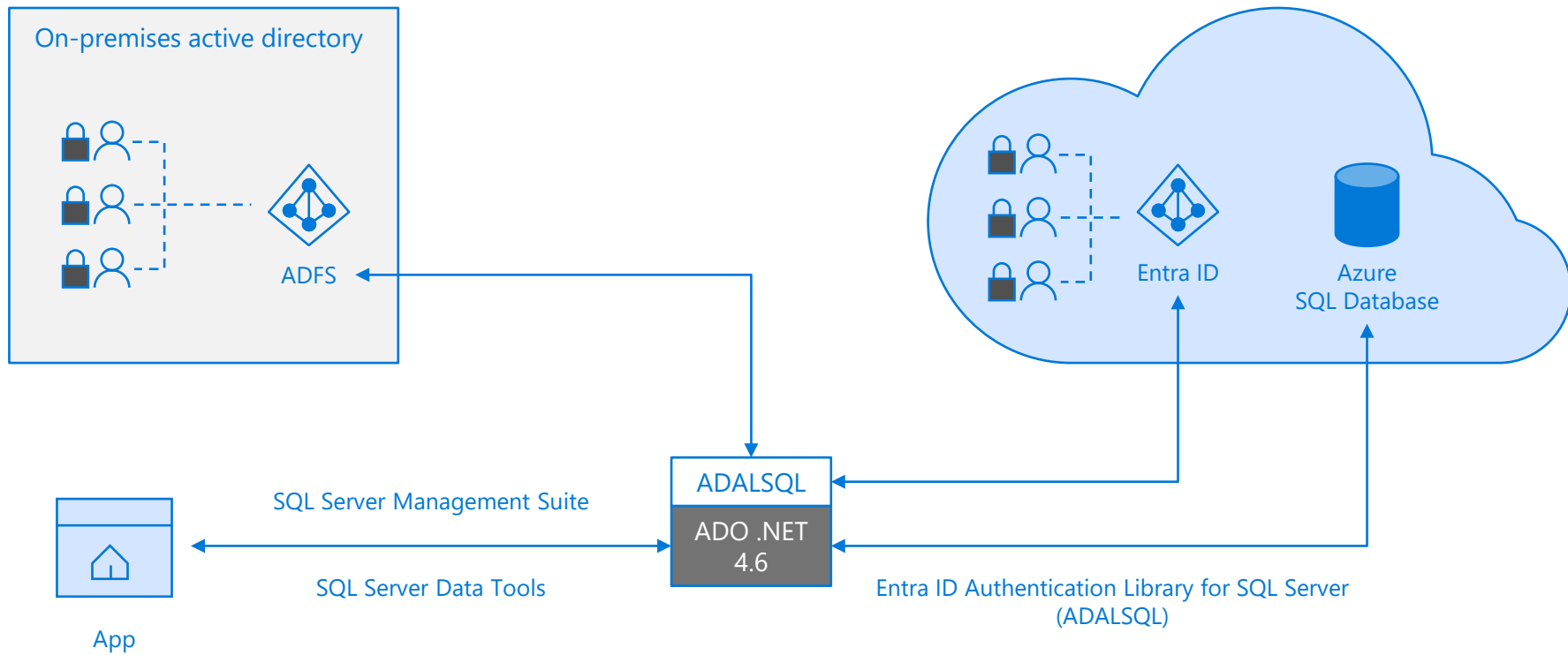
Allows password rotation in a single place.

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

Entra ID and Azure SQL Database



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

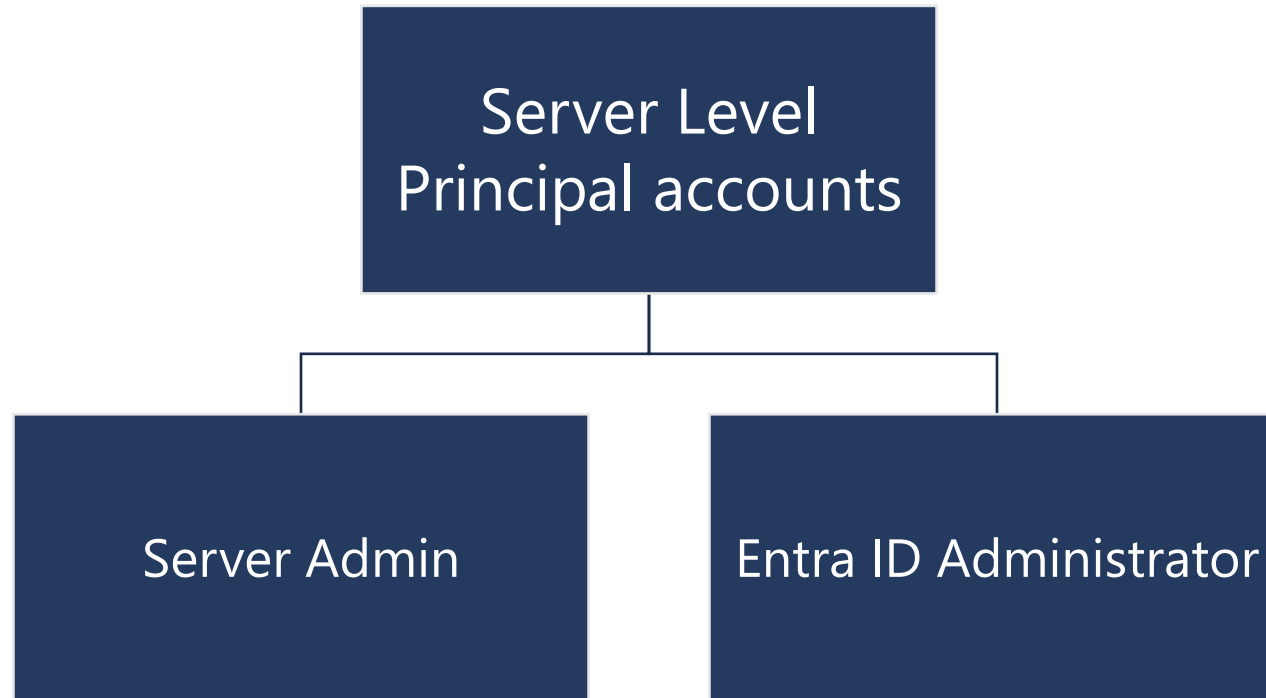
Objectives

After completing this learning, you will be able to:

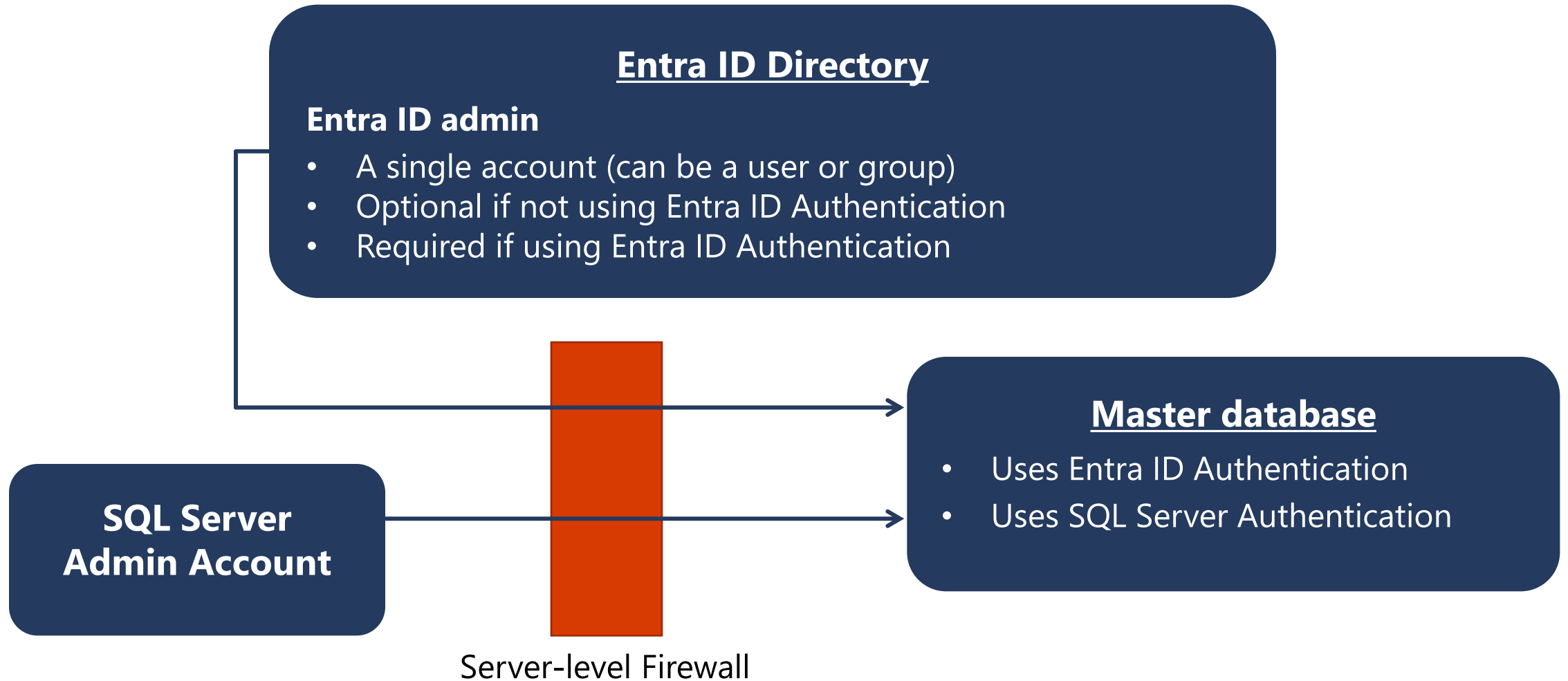
- Manage logins within Azure SQL Database.



Unrestricted Administrative Accounts



Administrator Access Path



Additional Special Roles

Database Creators

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

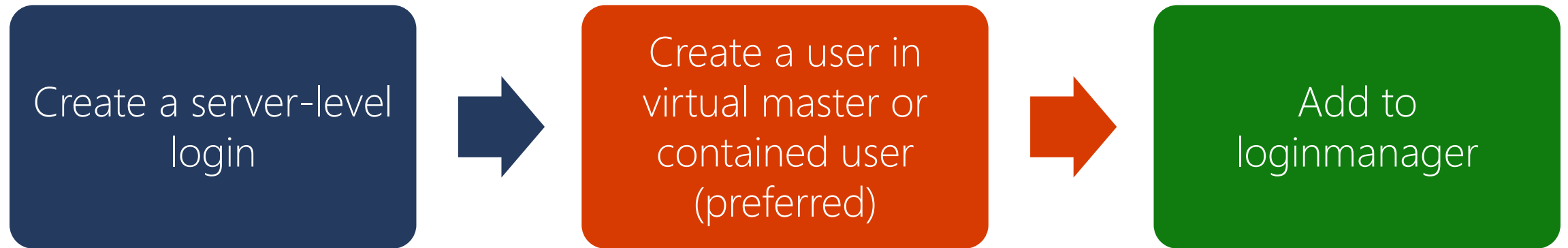


*dbmanager is a database role in virtual master database.

Additional Special Roles (continued)

Login Managers

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



*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.

Roles

Server Roles

- Fixed server roles
- User-defined server roles

Database Roles

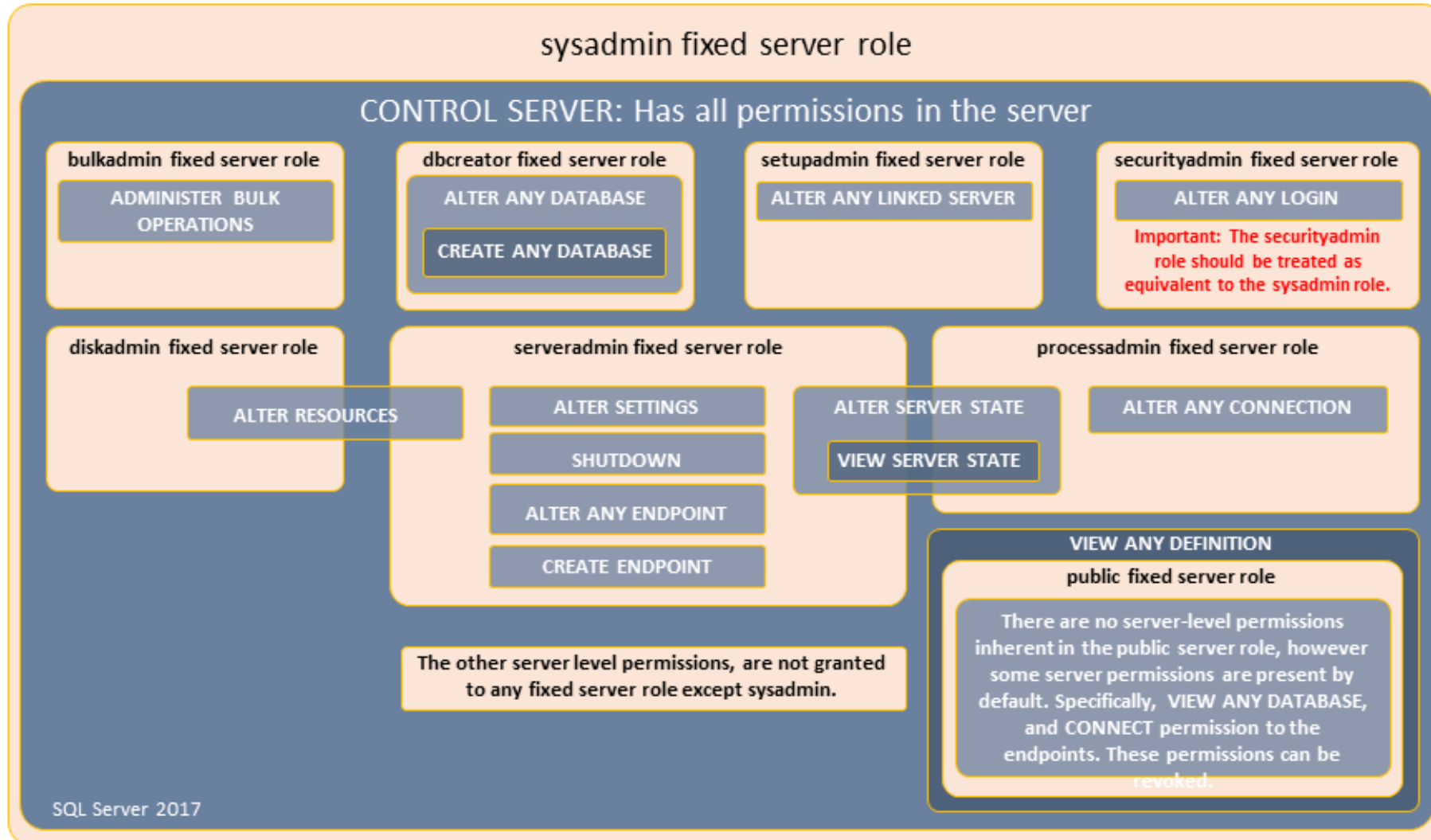
- Fixed database roles
- User-defined database roles

Application roles

- Assign rights to applications instead of users

Fixed Server Level Roles and Permissions

SERVER LEVEL ROLES AND PERMISSIONS: 9 fixed server roles, 34 server permissions



Fixed Server Level Roles and Permissions



Role	Description	Server-level Permission
sysadmin	Perform any activity	CONTROL SERVER (with GRANT option)
dbcreator	Create and alter databases	ALTER ANY DATABASE
diskadmin	Manage disk files	ALTER RESOURCES
serveradmin	Configure server-wide settings	ALTER ANY ENDPOINT, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS, SHUTDOWN, VIEW SERVER STATE
securityadmin	Manage and audit server logins	ALTER ANY LOGIN
processadmin	Manage SQL Server processes	ALTER ANY CONNECTION ALTER SERVER STATE
bulkadmin	Run the BULK INSERT statement	ADMINISTER BULK OPERATIONS
setupadmin	Configure replication and linked servers	ALTER ANY LINKED SERVER

New Server Level Roles introduced in SQL Server 2022

Server-level role	Description
##MS_DatabaseConnector##	Connect to any database without requiring a database User-account.
##MS_LoginManager##	Create, delete and modify logins. Cannot GRANT.
##MS_DatabaseManager##	Create and delete databases.
##MS_ServerStateManager##	Same as the ##MS_ServerStateReader## role, but also has the ALTER SERVER STATE permission.
##MS_ServerStateReader##	Read all dynamic management views (DMVs) and functions that are covered by VIEW SERVER STATE .
##MS_ServerPerformanceStateReader##	Read all dynamic management views (DMVs) and functions that are covered by VIEW SERVER PERFORMANCE STATE
##MS_ServerSecurityStateReader##	Read all dynamic management views (DMVs) and functions that are covered by VIEW SERVER SECURITY STATE
##MS_DefinitionReader##	Read all catalog views that are covered by VIEW ANY DEFINITION
##MS_PerformanceDefinitionReader##	Read all catalog views that are covered by VIEW ANY PERFORMANCE DEFINITION .
##MS_SecurityDefinitionReader##	Read all catalog views that are covered by VIEW ANY SECURITY DEFINITION .

Listing Server Level Permissions

```
SELECT * FROM sys.fn_builtin_permissions('SERVER')  
ORDER BY permission_name;
```

<div><div> Results</div><div> Messages</div></div>						
	class_desc	permission_name	type	covering_permission_name	parent_class_desc	parent_covering_permission_name
1	SERVER	ADMINISTER BULK OPERATIONS	ADBO	CONTROL SERVER		
2	SERVER	ALTER ANY AVAILABILITY GROUP	ALAG	CONTROL SERVER		
3	SERVER	ALTER ANY CONNECTION	ALCO	CONTROL SERVER		
4	SERVER	ALTER ANY CREDENTIAL	ALCD	CONTROL SERVER		
5	SERVER	ALTER ANY DATABASE	ALDB	CONTROL SERVER		
6	SERVER	ALTER ANY ENDPOINT	ALHE	CONTROL SERVER		
7	SERVER	ALTER ANY EVENT NOTIFICATION	ALES	CONTROL SERVER		

Public Role



Public is a special role that is at the server and database level.



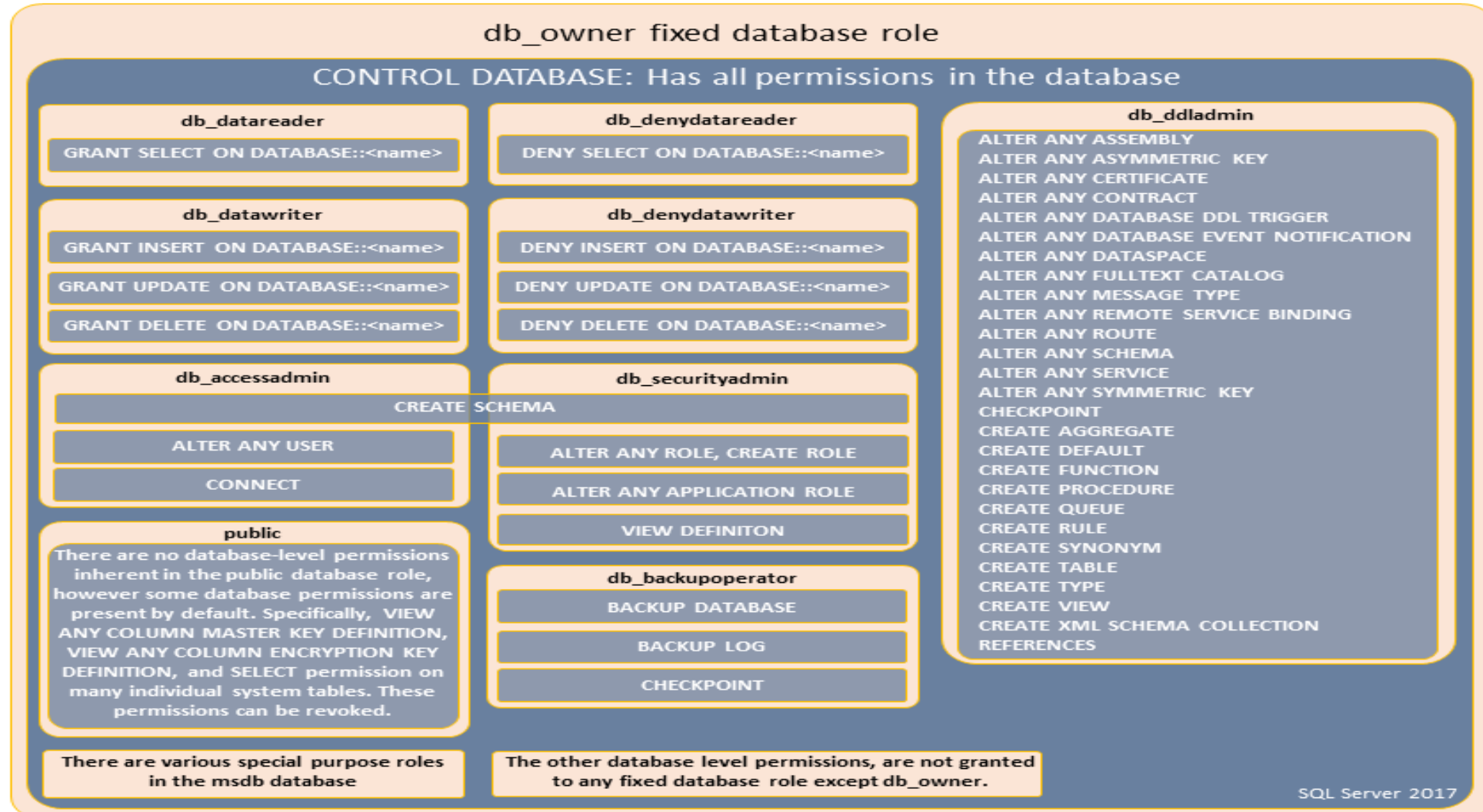
Every SQL Server login and user belongs to the Public role



Care must be taken when granting permissions to Public server role especially when granting server-level **permissions**.

Fixed Database Level Roles and Permissions

DATABASE LEVEL ROLES AND PERMISSIONS: 11 fixed database roles, 77 database permissions



Fixed Database Level Roles and Permissions

Role	Description
db_owner	Perform any configuration and maintenance activities on the DB and can drop it
db_securityadmin	Modify role membership and manage permissions
db_accessadmin	Add or remove access to the DB for logins
db_backupoperator	Back up the DB
db_ddladmin	Run any DDL command in the DB
db_datawriter	Add, delete, or change data in all user tables
db_datareader	Read all data from all user tables
db_denydatawriter	Cannot add, delete, or change data in user tables
db_denydatareader	Cannot read any data in user tables

Listing Database level permissions

```
SELECT * FROM sys.fn_builtin_permissions('Database')  
ORDER BY permission_name;
```

Results		Messages				
	class_desc	permission_name	type	covering_permission_name	parent_class_desc	parent_covering_permission_name
1	DATABASE	ALTER	AL	CONTROL	SERVER	ALTER ANY DATABASE
2	DATABASE	ALTER ANY APPLICATION ROLE	ALAR	ALTER	SERVER	CONTROL SERVER
3	DATABASE	ALTER ANY ASSEMBLY	ALAS	ALTER	SERVER	CONTROL SERVER
4	DATABASE	ALTER ANY ASYMMETRIC KEY	ALAK	ALTER	SERVER	CONTROL SERVER
5	DATABASE	ALTER ANY CERTIFICATE	ALCF	ALTER	SERVER	CONTROL SERVER
6	DATABASE	ALTER ANY COLUMN ENCRYPTION KEY	ALCK	ALTER	SERVER	CONTROL SERVER
7	DATABASE	ALTER ANY COLUMN MASTER KEY	ALCM	ALTER	SERVER	CONTROL SERVER

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)

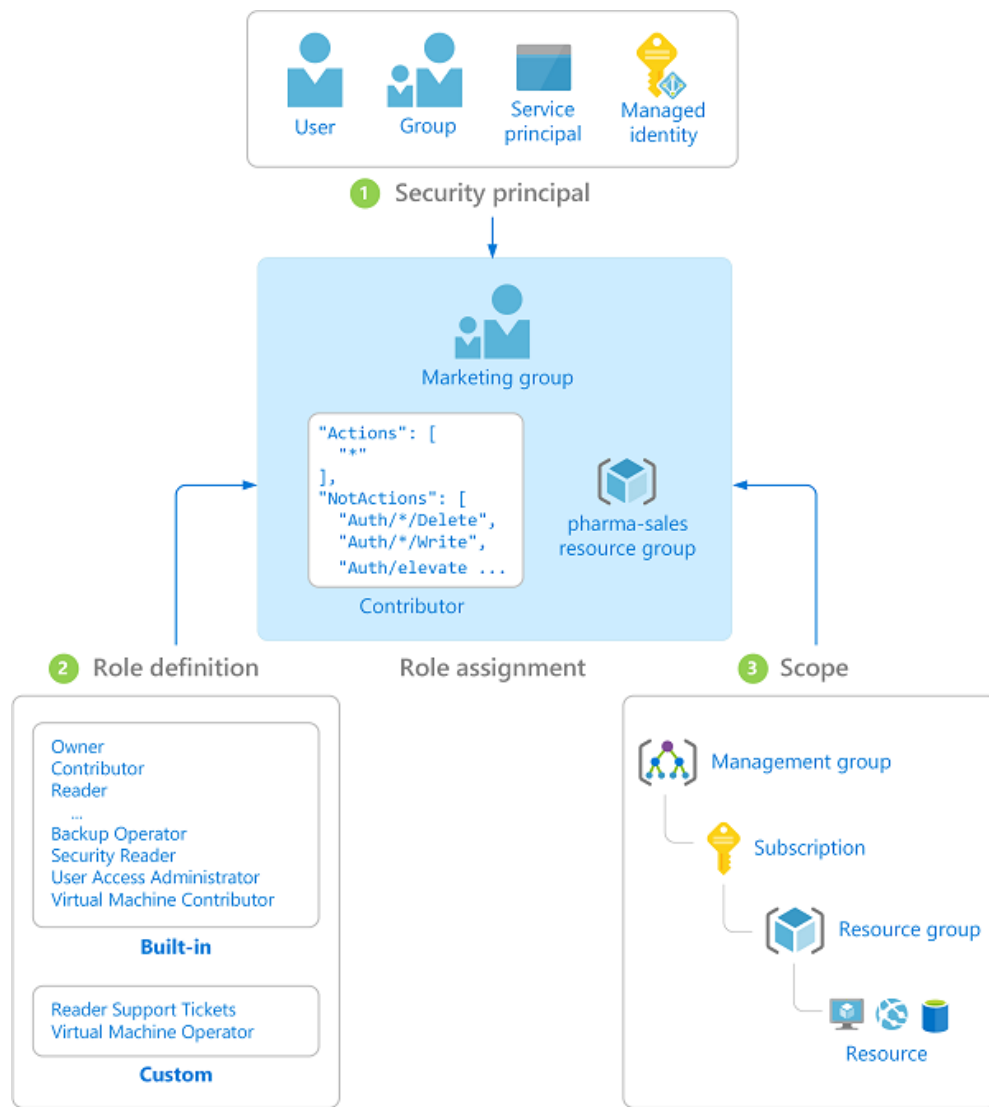
What is Azure Role-Based Control (RBAC)

- 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

- An individual who has a profile in Entra ID. You can also assign roles to users in other tenants.

Group

- A set of users created in Entra ID. When you assign a role to a group, all users within that group have that role.

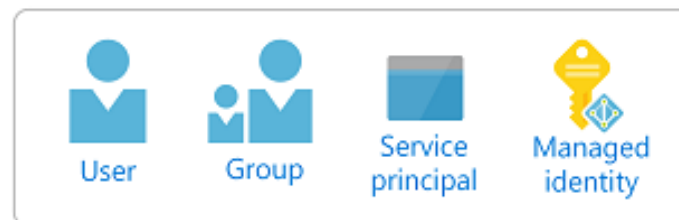
Service principal

- 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

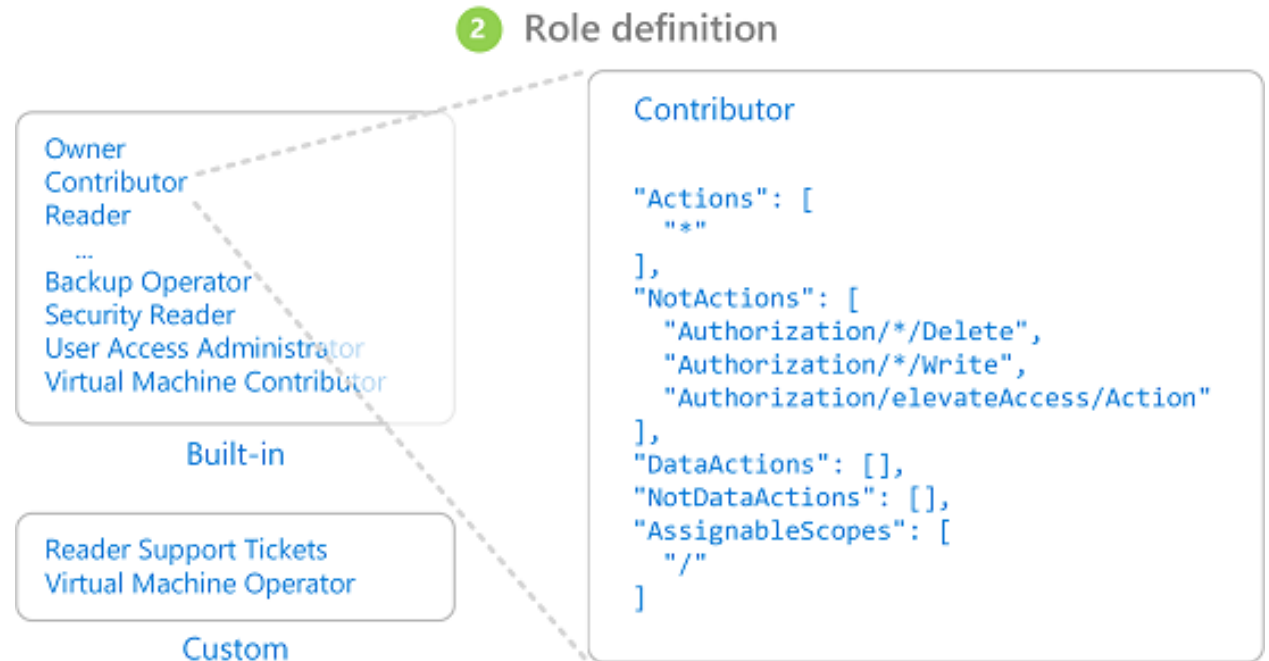
- An identity in Entra ID that is automatically managed by Azure. You typically use managed identities when developing cloud applications to manage the credentials for authenticating to Azure services.

1 Security principal



Azure RBAC – Role Definition

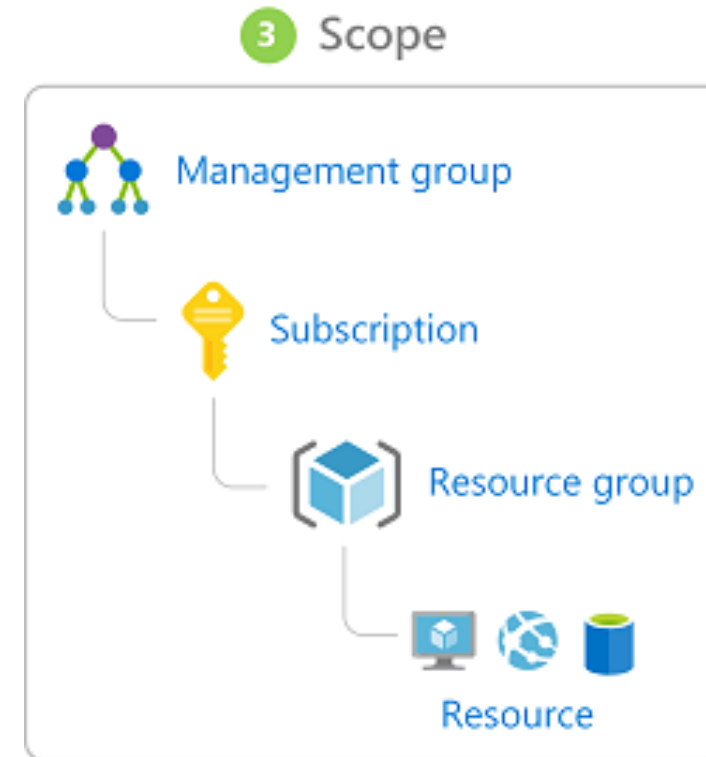
A role definition is a collection of permissions. It's sometimes just called a role. A role definition lists the operations that can be performed, such as read, write, and delete. Roles can be high-level, like owner, or specific, like virtual machine reader.



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

- 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.

User Access Administrator

- 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

