

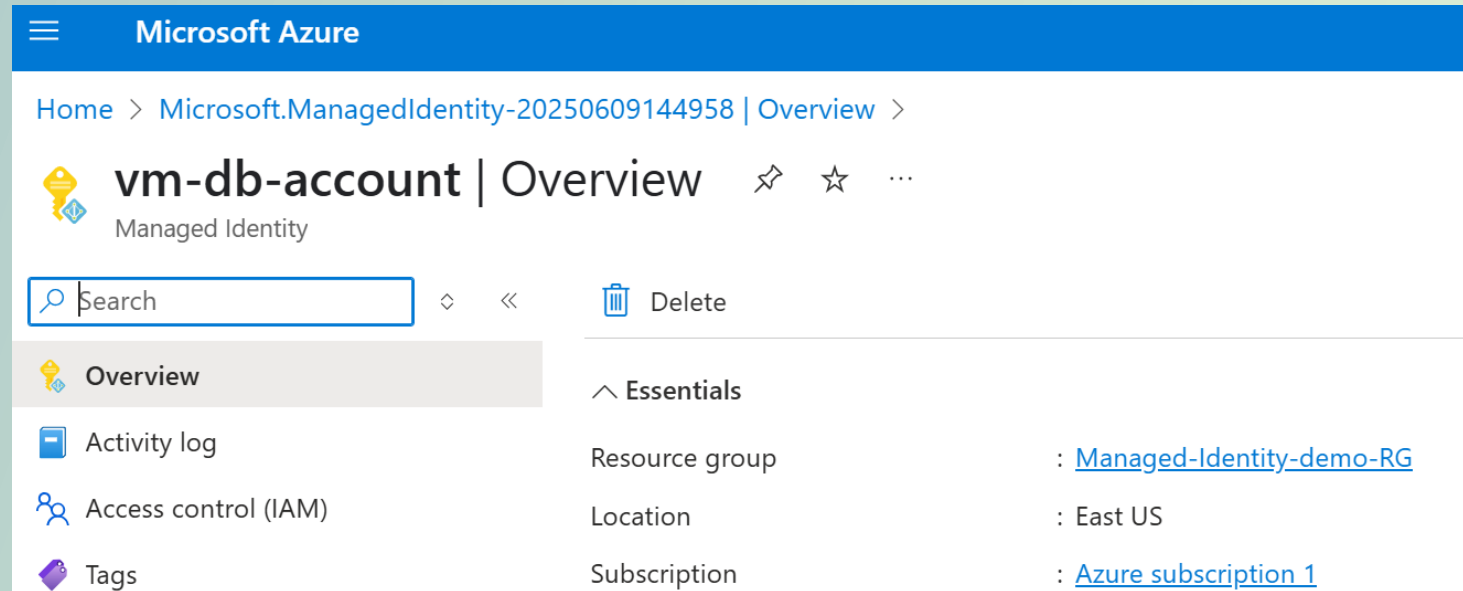


Secure Azure Access Using Managed Identity (No Passwords Needed)

Learn how to use Managed Identity to securely connect an Azure VM to a SQL Database — no secrets, no passwords. A real-world security demo using Microsoft Entra and RBAC.

Managed Identity Types

- **System-assigned** (1:1)
- **User-assigned** (Reusable)



The screenshot displays the Microsoft Azure portal interface. At the top, the header bar is blue with the 'Microsoft Azure' logo. Below the header, the breadcrumb trail reads 'Home > Microsoft.ManagedIdentity-20250609144958 | Overview >'. The main title is 'vm-db-account | Overview', with 'Managed Identity' as a subtitle. A search bar and a 'Delete' button are visible. On the left, a sidebar lists navigation options: 'Overview' (selected), 'Activity log', 'Access control (IAM)', and 'Tags'. The main content area, titled 'Essentials', shows three key details: 'Resource group' linked to 'Managed-Identity-demo-RG', 'Location' set to 'East US', and 'Subscription' linked to 'Azure subscription 1'.

Essentials	
Resource group	: Managed-Identity-demo-RG
Location	: East US
Subscription	: Azure subscription 1



Assign Managed Identity to Azure VM

To securely access other Azure resources, we assign both:

- “System-assigned identity for 1:1 resource access”
- “User-assigned identity (vm-db-account) for shared, scalable access across multiple services”

These identities allow the VM to authenticate securely without storing passwords or secrets.

VM1 | Identity ☆ ...
Virtual machine

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied have to store any credentials in code.

Save Discard Refresh Got feedback?

Status ⓘ
Off On

Add user assigned managed identity ✕

Select a subscription *

Azure subscription 1

User assigned managed identities

vm-db-

☒ **vm-db-account**
Resource Group: Managed-Identity-demo-RG

Selected identities:

vm-db-account
Resource Group: Managed-Identity-demo-RG
Subscription: Azure subscription 1 Remove

Microsoft Azure Search resources, services, and docs (G+/)

Compute infrastructure | Virtual machines > VM1

VM1 | Identity ☆ ...
Virtual machine

Search

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security

System assigned **User assigned**

User assigned managed identities enable Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Similarly, a single user assigned managed identity can be shared across multiple resources (e.g. VM).

+ Add Remove Refresh Got feedback?

Name	Resource group
<input type="checkbox"/> vm-db-account	managed-identity-demo-rg

Identity
Microsoft Defender for Cloud

Add

Create SQL Database with Entra Authentication

WE DEPLOY A
SECURE SQL
DATABASE USING:

MICROSOFT
ENTRA-ONLY
AUTHENTICATION
(NO SQL LOGINS)

REGION AND
COMPUTE
SETTINGS
OPTIMIZED FOR
LAB USE

THIS PREPARES
THE DATABASE TO
ACCEPT
CONNECTIONS
FROM OUR VM VIA
**MANAGED
IDENTITY** — NO
SECRETS, NO
PASSWORDS.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > SQL databases >

Create SQL Database

Microsoft

Basics Networking Security Additional settings Tags Review + create

Product details

SQL database by Microsoft

Estimated cost per month

418.37 USD

Terms

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace of listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offer the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage transactional information with the provider(s) of the offering(s) for support, billing and other transactional act Microsoft does not provide rights for third-party offerings. For additional details see [Azure Marketplace Terms](#)

Basics

Subscription	Azure subscription 1
Resource group	Managed-Identity-demo-RG
Region	South Central US
Database name	sql-server-managed
Server	(new) perparim-sq101
Authentication method	Microsoft Entra-only authentication
Microsoft Entra Admin	PerparimAbdullahu@PerparimSC300lab.onmicrosoft.com
Compute + storage	General Purpose: Standard-series (Gen5), 2 vCores, 32 GB storage
Backup storage redundancy	Locally-redundant backup storage

Networking

Allow Azure services and resources to access this server	Yes
Add current client IP address	No
Private endpoint	None
Minimum TLS version	1.2
Connection Policy	Default

Create

< Previous

[Download a template for automation](#)

Microsoft Azure

Search resources, services, and docs (G+/)

Home > SQL databases >

Create SQL Database

Microsoft


Security

Identity	Not enabled
Transparent data encryption (Server level)	Service-managed key selected
Database level customer-managed key	Not configured
Database level user assigned managed identity	Not configured
Advanced data security	Start free trial
Always Encrypted with secure enclaves	Not configured
Sql Ledger(Database)	Disabled
Digest Storage	Disabled

Additional settings

Use existing data	Blank
Collation	SQL_Latin1_General_CP1_CI_AS
Maintenance window	System default (5pm to 8am)

Tags



Cost summary

General Purpose (GP, Gen5 2)	
Cost per vCore (in USD)	206.32
vCores selected	x 2
Cost per GB (in USD)	
Max storage selected (in GB)	x 41.6

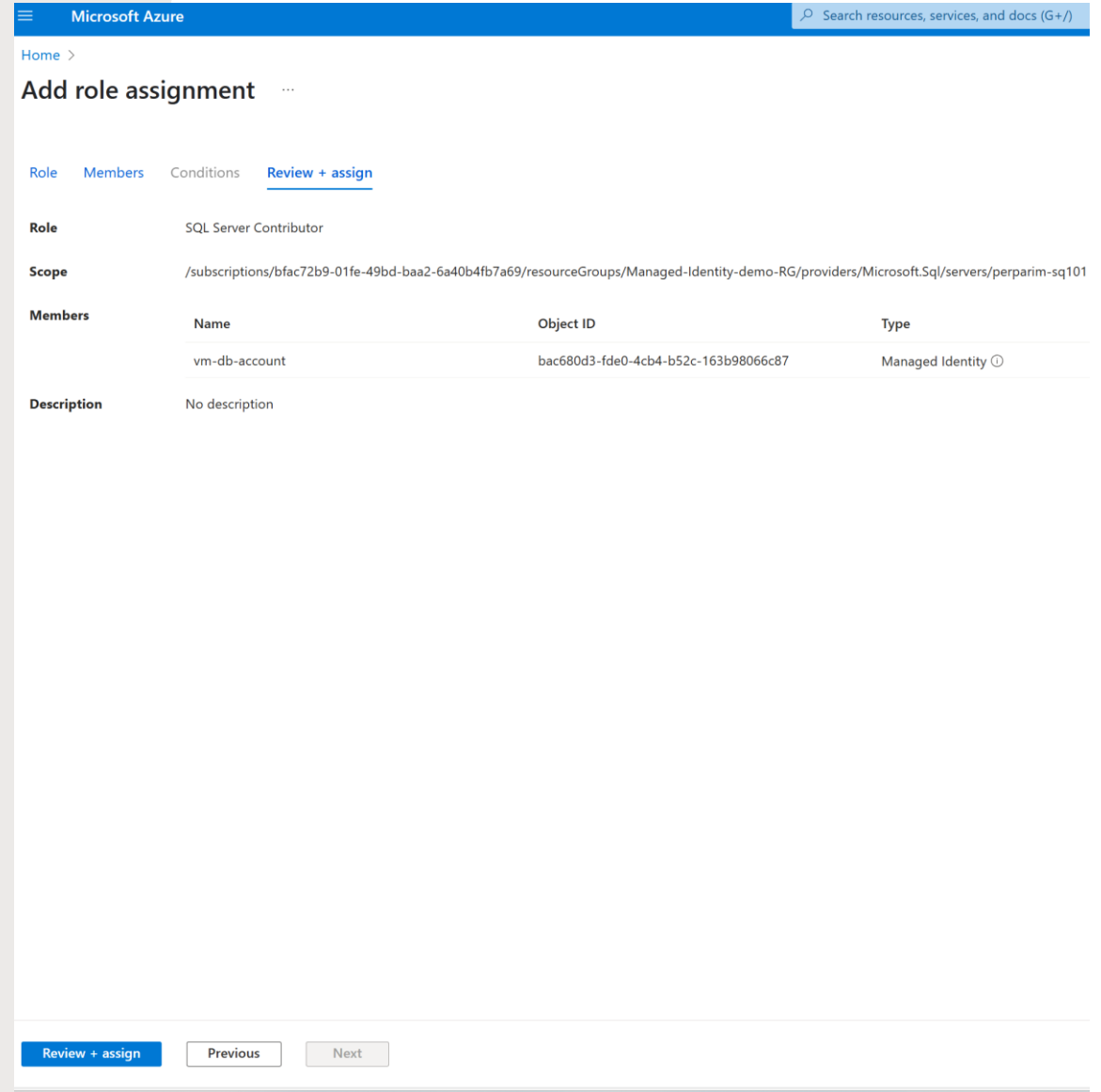
Create

< Previous

[Download a template for automation](#)

Grant Secure Access with RBAC

- We assigned the **SQL Server Contributor** role to our **user-assigned managed identity**. This lets the VM securely interact with the SQL Database — without using passwords or connection strings.
- Access is controlled using **Microsoft Entra + RBAC**, which allows precise permission management.



Microsoft Azure

Home >

Add role assignment

Role Members Conditions Review + assign

Role SQL Server Contributor

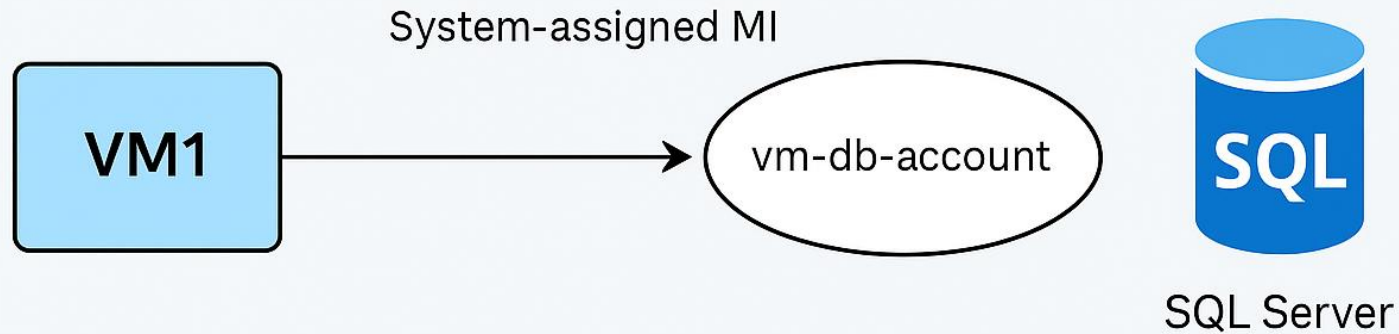
Scope /subscriptions/bfac72b9-01fe-49bd-baa2-6a40b4fb7a69/resourceGroups/Managed-Identity-demo-RG/providers/Microsoft.Sql/servers/perparim-sq101

Members	Name	Object ID	Type
	vm-db-account	bac680d3-fde0-4cb4-b52c-163b98066c87	Managed Identity ⓘ

Description No description

[Review + assign](#) [Previous](#) [Next](#)

Managed Identity Flow: No Secrets Needed



1. VM uses its managed identity to authenticate
2. Identity has RBAC access to SQL via SQL Server Contributor
3. No passwords, no connection strings –just identity-based trust



Built in #PerparimLabs using Microsoft Entra + Azure RBAC

Key Takeaways from This Lab



Enabled **System + User-assigned Managed Identity** on VM



Deployed Azure SQL with **Entra-only authentication**



Assigned SQL RBAC role to managed identity



VM can now access SQL securely — **no secrets needed**



Aligns with **SC-300**, Zero Trust, and real-world architecture