

Microsoft Azure Developer: Implement Secure Cloud Solutions

IMPLEMENT MANAGED IDENTITIES FOR AZURE RESOURCES



Reza Salehi

CLOUD CONSULTANT

@zaalion



Overview



Implement Managed Identities for Azure resources

Demo: Managed Identities (formerly MSI)



Implement Managed Identities for Azure Resources



Managed Identity



Managed Identity



Managed Identity



Don't hardcode service credentials in the client app settings



The configuration file can get compromised or checked into the source control



Azure Key Vault is more secure, but the you need to use AAD App Registration id and secret to authenticate



Use Managed Identities to eliminate the need to hardcode credentials in the client code



Azure AD Managed Identities

Provides Azure services with an automatically managed identity. use this identity to authenticate to any service that supports Azure AD authentication.



Services That Support Managed Identities

Client Services

Azure Virtual Machines and Scale Sets

Azure App Service, Functions Apps

Logic Apps

Azure Cognitive Search

Azure Data Factory V2

Azure Container Instances

Azure API Management

Target Services

Azure Key Vault

Azure SQL

Azure Service Bus, Azure Event Hubs

Azure Storage (blobs & queues)

Azure Data Lake

Azure Resource Manager

Azure Analysis Services



Managed Identity Support

<https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities>



Types of Managed Identities

system-assigned

Enabled directly on the Azure service instance

One per each Azure service instance

Gets cleaned up if Azure service instance is deleted

Widely supported by Azure resources

user-assigned

Created as a standalone Azure resource

Can be assigned to one or more Azure service instances

Its lifecycle is separate from the lifecycle of Azure service to which it's assigned

Might be in preview for some resources



Configuring Managed Identities

Create Identity

Create system-assigned or user-assigned identity (authentication)

Give Permission

In the target Azure service, assign permissions to the client identity (authorization)



func-az303-demo01 - Microsoft

portal.azure.com/#@zaalion.com/resource/subscriptions/19969c81-e8ff-4585-8c2f-3f196b588227/resourceGroups/rg-ps-az303/providers/Microsoft.Web/sites/func-az303-demo01/msi

zaalion@outlook.com
ZAALION (DEFAULT DIRECTORY)

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

Azure Active Directory

Resource groups

Machine Learning

Search services

Bot Services

Cognitive Services

Function App

Stream Analytics jobs

SQL databases

Azure Cosmos DB

Logic apps

Blueprints

App Services

Home > Function App > func-az303-demo01

func-az303-demo01 | Identity

Function App

Search (Ctrl+ /)

Deployment Center

Settings

Configuration

Authentication / Authorization

Application Insights

Identity

Backups

Custom domains

TLS/SSL settings

Networking

Scale up (App Service plan)

Scale out

Push

Properties

System assignedUser assigned

A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. [Learn more about Managed identities.](#)

SaveDiscardRefreshGot feedback?

Status ⓘ

OffOn

vm-az303-demo01 - Microsoft A

portal.azure.com/#@zaalion.com/resource/subscriptions/19969c81-e8ff-4585-8c2f-3f196b588227/resourceGroups/rg-ps-az303/providers/Microsoft.Compute/virtualMachines/vm-az303-demo01/managedserviceidentity

zaalion@outlook.com
ZAALION (DEFAULT DIRECTORY)

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

Function app

Stream Analytics jobs

SQL databases

Azure Cosmos DB

Logic apps

Blueprints

App Services

Policy

Storage accounts

Key vaults

Automation Accounts

Cost Management + Billi...

Virtual machines

All services > Virtual machines > vm-az303-demo01

vm-az303-demo01 | Identity

Virtual machine

Search (Ctrl+ /)

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Security

Advisor recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

System assigned

User assigned

A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. [Learn more about Managed identities.](#)

Save

Discard

Refresh

Got feedback?

Status ⓘ

Off

On

logic-az303-psdemo01 - Microsc

portal.azure.com/#@zaalion.com/resource/subscriptions/19969c81-e8ff-4585-8c2f-3f196b588227/resourceGroups/rg-ps-az303/providers/Microsoft.Logic/workflows/logic-az303-psdemo01/msiSettings

zaalion@outlook.com
ZAALION (DEFAULT DIRECTORY)

Microsoft Azure

Search resources, services, and docs (G+)

Create a resource

Home

Dashboard

All services

FAVORITES

Function app

Stream Analytics jobs

SQL databases

Azure Cosmos DB

Logic apps

Blueprints

App Services

Policy

Storage accounts

Key vaults

Automation Accounts

Virtual machines

Cost Management + Billi...

Home > Logic apps > logic-az303-psdemo01

logic-az303-psdemo01 | Identity

Logic app

Search (Ctrl+ /)

Quick start guides

Release notes

Settings

Workflow settings

Authorization

Access keys

Identity

Properties

Locks

Monitoring

Alerts

Metrics

Diagnostic settings

Logs

System assigned

User assigned

A system assigned managed identity enables Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. Once enabled, all necessary permissions can be granted via Azure role-based-access-control. The lifecycle of this type of managed identity is tied to the lifecycle of this resource. Additionally, each resource (e.g. Virtual Machine) can only have one system assigned managed identity. [Learn more about Managed identities.](#)

Save

Discard

Refresh

Got feedback?

Status ⓘ

Off

On

Creating a Managed Identity only
takes care of the authentication.



Configuring Managed Identities

Create Identity

Create system-assigned or user-assigned identity (authentication)

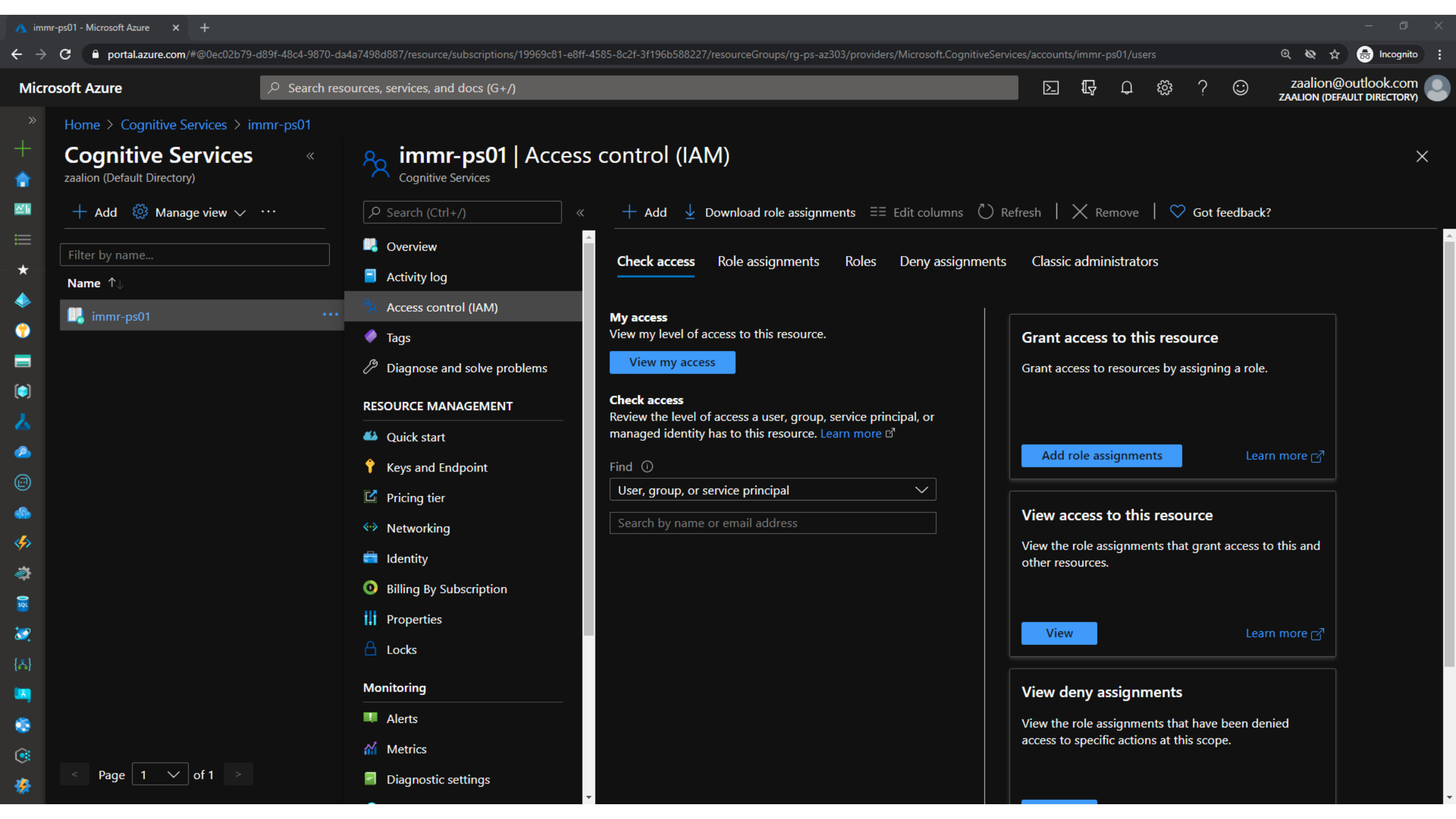
Give Permission

In the target Azure service, assign permissions to the client identity (authorization)



You still need to grant target service access to the new identity.





Microsoft Azure

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

zaalion@outlook.com
ZAALION (DEFAULT DIRECTORY)

Home > Cognitive Services > immr-ps01

Cognitive Services

zaalion (Default Directory)

+ Add

Manage view

Filter by name...

Name

↑↓

immr-ps01

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

RESOURCE MANAGEMENT

Quick start

Keys and Endpoint

Pricing tier

Networking

Identity

Billing By Subscription

Properties

Locks

Monitoring

Alerts

Metrics

D diagnostic settings

immr-ps01 | Access control (IAM)

Cognitive Services

Search (Ctrl+ /)

+ Add

Download role assignments

Edit columns

Refresh

Check access

Role assignments

Roles

Deny assignments

CL

My access

View my level of access to this resource.

View my access

Check access

Review the level of access a user, group, service principal, or managed identity has to this resource. [Learn more](#)

Find

User, group, or service principal

Search by name or email address

Add role assignment

Role

Cognitive Services Contributor

Assign access to

User, group, or service principal

Select

func

func-managedidentitydemo

Selected members:

func-identity-kv-demo02

Remove

Save

Discard

Page 1 of 1

immr-ps01 - Microsoft Azure

portal.azure.com/#@0ec02b79-d89f-48c4-9870-da4a7498d887/resource/subscriptions/19969c81-e8ff-4585-8c2f-3f196b588227/resourceGroups/rg-ps-az303/providers/Microsoft.CognitiveServices/accounts/immr-ps01/users

Microsoft Azure

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

Incognito

zaalion@outlook.com
ZAALION (DEFAULT DIRECTORY)

Home > Cognitive Services > immr-ps01

Cognitive Services

zaalion (Default Directory)

+ Add

⚙️ Manage view

⋮

Filter by name...

Name

↑↓

immr-ps01

immr-ps01 | Access control (IAM)

Cognitive Services

Search (Ctrl+ /)

⋮

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

RESOURCE MANAGEMENT

Quick start

🔑 Keys and Endpoint

📊 Pricing tier

🔗 Networking

👛 Identity

🕒 Billing By Subscription

📋 Properties

🔒 Locks

Monitoring

📢 Alerts

📈 Metrics

🔧 Diagnostic settings

+ Add

⬇️ Download role assignments

⋮ Edit columns

🔄 Refresh

✖ Remove

📖 Got feedback?

Check access

Role assignments

Roles

Deny assignments

Classic administrators

Number of role assignments for this subscription

102000

Search by name or email






Type : All

Role : All

Scope : All scopes

Group by : Role

9 items (8 Unknown, 1 Managed Identities)

<input type="checkbox"/>	Name	Type	Role	Scope
Cognitive Services Contributor				
<input type="checkbox"/>	 func-identity-kv-demo02/subscriptions/19969c8...	App Service or Function App	Cognitive Services Contributor ⓘ	This resource
Contributor				
<input type="checkbox"/>	 Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ	Subscription (Inherited)
<input type="checkbox"/>	 Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ	Subscription (Inherited)
<input type="checkbox"/>	 Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ	Subscription (Inherited)
<input type="checkbox"/>	 Identity not found. ⓘ Unable to find identity.	Unknown	Contributor ⓘ	Subscription (Inherited)

Page 1 of 1

At this point you don't need to provide Key Vault credentials in your Function App code.



Activity

Provision both system-assigned and user-assigned Managed Identities for a Function App.



Activity

Configure an Azure Key Vault instance to use Managed Identity for authentication.



Demo



Using Managed Identities with

- Azure Cognitive Search and Azure Blob Storage



Demo



Creating a user-assigned Managed Identity



Summary



Implement Managed Identities for Azure resources

Demo: Managed Identities (formerly MSI)

