May 5th – 7th, 2022

#GlobalAzure

• BY COMMUNITY • FOR COMMUNITY •

#GLOBALAZURE

2022

May 7th, 2022

BY COMMUNITY • FOR COMMUNITY

IN VIETNAM

#GLOBALAZURE

2022

organized by

DEV CAFE

Connect and share

#Vietnam

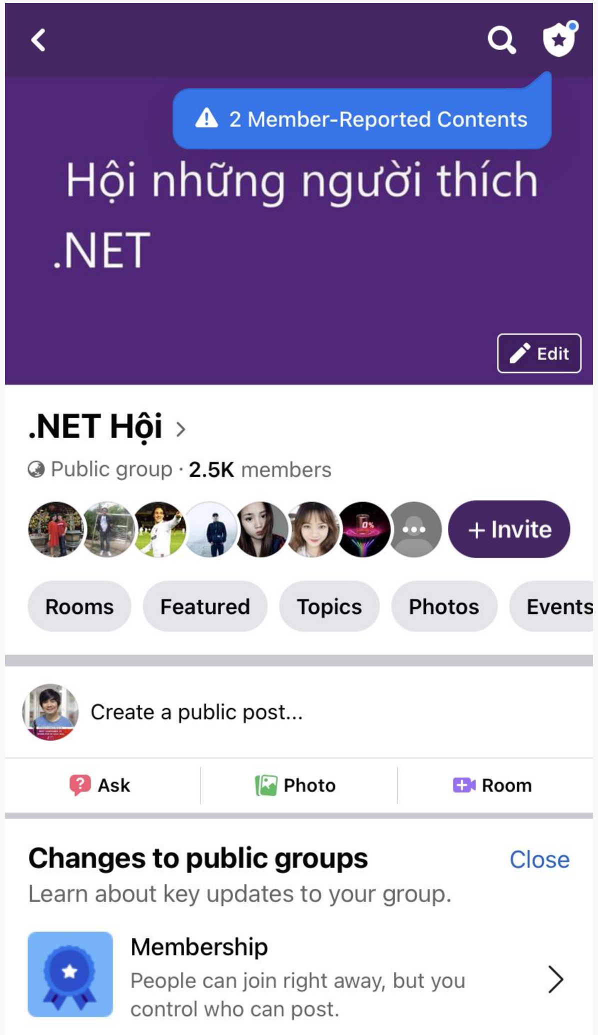
Managed Identities for Azure resources

Thien Nguyen

About me

https://www.facebook.com/groups/dotnetvn

https://github.com/thiennn



Hội những người thích .NET

.NET Hội >

Public group · 2.5K members

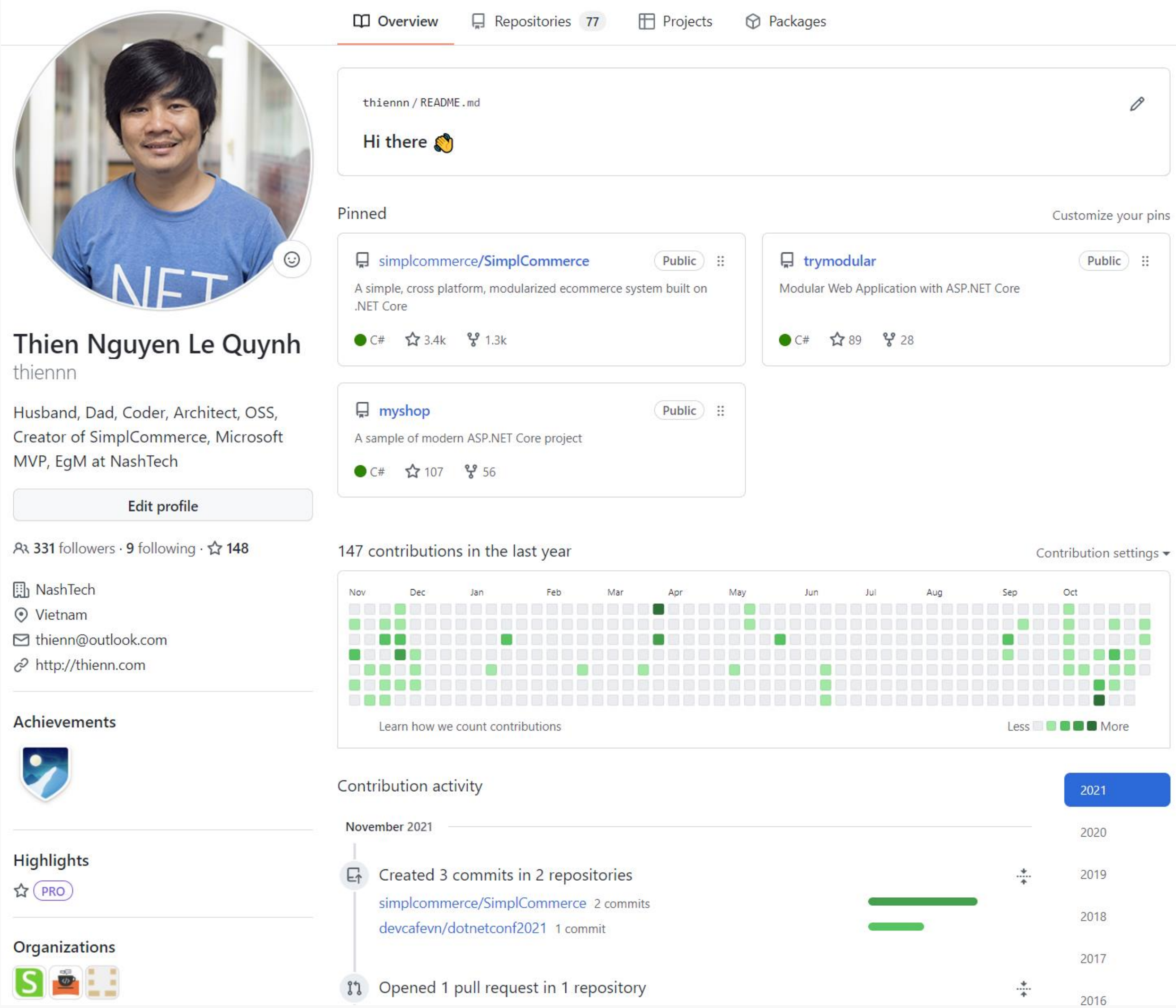
Create a public post...

Changes to public groups

Learn about key updates to your group.

Membership

People can join right away, but you control who can post.



Thien Nguyen Le Quynh

thiennn

Husband, Dad, Coder, Architect, OSS, Creator of SimplCommerce, Microsoft MVP, EgM at NashTech

331 followers · 9 following · 148

NashTech

Vietnam

thienn@outlook.com

http://thienn.com

Achievements

Highlights

PRO

Organizations

thiennn / README.md

Hi there 👋

Pinned

simplcommerce/SimplCommerce Public
A simple, cross platform, modularized ecommerce system built on .NET Core
C# 3.4k 1.3k

trymodular Public
Modular Web Application with ASP.NET Core
C# 89 28

myshop Public
A sample of modern ASP.NET Core project
C# 107 56

147 contributions in the last year

Learn how we count contributions

Contribution activity

November 2021

Created 3 commits in 2 repositories

simplcommerce/SimplCommerce 2 commits

devcafevn/dotnetconf2021 1 commit

Opened 1 pull request in 1 repository

Headache on managing service accounts

- Accidentally checked into source control
- Leaked/Stolen
- Expired
- Auto-rotation
- Clean up

Managed Identity come to rescue

- You don't need to manage credentials. Credentials aren’t even accessible to you.
- It’s free

I can use Managed Identities when…

As a developer, I want to build an application using

Source:

Azure Resources
Azure VMs
Azure App Services
Azure Functions
Azure Container instances
Azure Kubernetes Service
Azure Logic Apps
Azure Storage
….

that accesses

Target:

Any target that supports Azure Active Directory Authentication:

- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL…

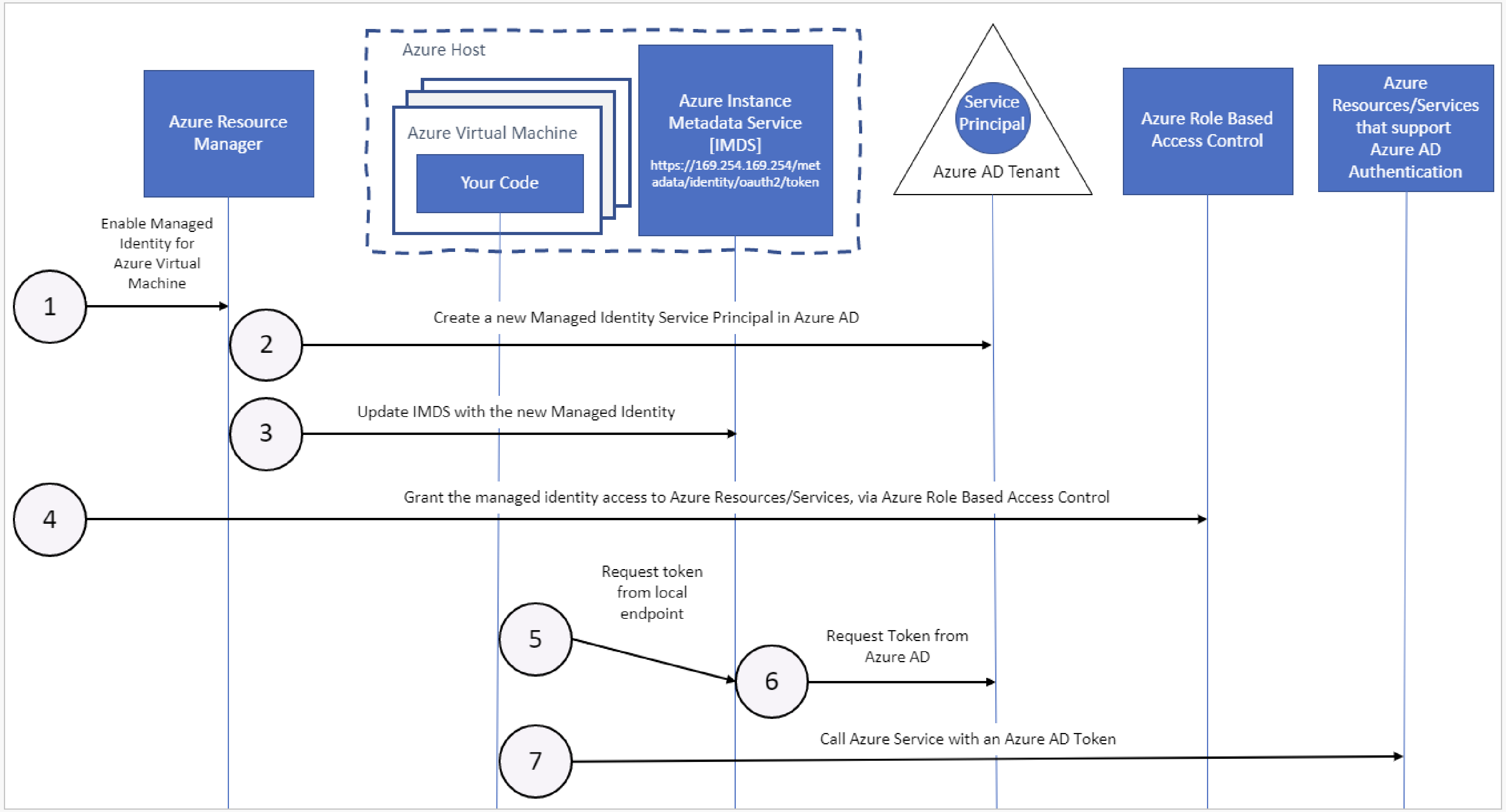
without having to manage any credentials!

For example, I want to build an application using ***Azure App Services*** that accesses **Azure Storage** without having to manage any credentials.

Managed identity types

- System-assigned: The identity is only used by a service instance and tied to the lifecycle of that service instance
- User-assigned: user-assigned managed identities managed by you, can be assigned to one or more service instances

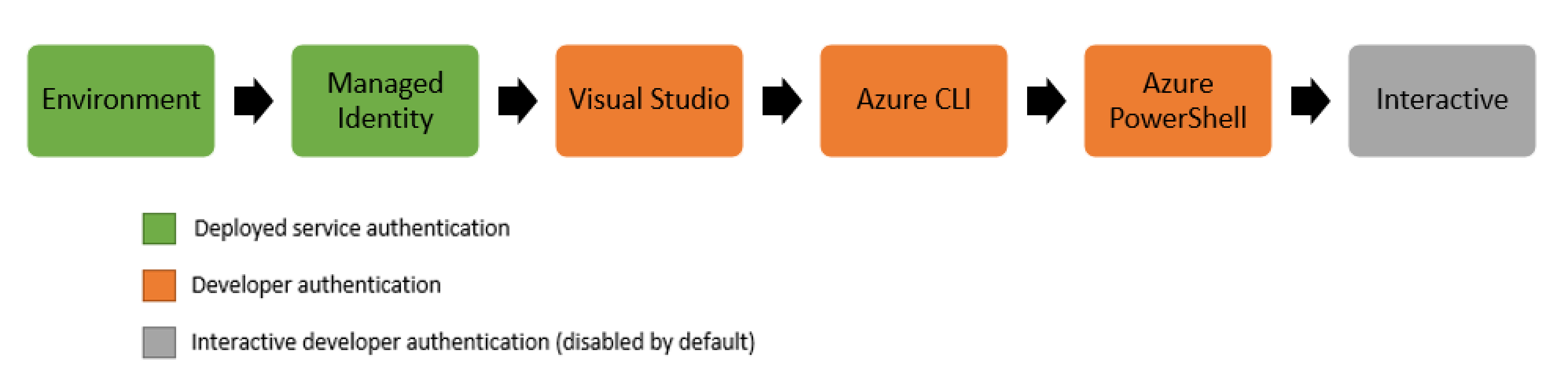
How it works (VM)



Azure Host
Azure Resource Manager
Azure Virtual Machine
Your Code
Azure Instance Metadata Service [IMDS]
https://169.254.169.254/metadata/identity/oauth2/token
Service Principal
Azure AD Tenant
Azure Role Based Access Control
Azure Resources/Services that support Azure AD Authentication
1
Enable Managed Identity for Azure Virtual Machine
2
Create a new Managed Identity Service Principal in Azure AD
3
Update IMDS with the new Managed Identity
4
Grant the managed identity access to Azure Resources/Services, via Azure Role Based Access Control
5
Request token from local endpoint
6
Request Token from Azure AD
7
Call Azure Service with an Azure AD Token

Azure Identity client library for .NET

The DefaultAzureCredential will attempt to authenticate via the following mechanisms in order.



Environment → Managed Identity → Visual Studio → Azure CLI → Azure PowerShell → Interactive

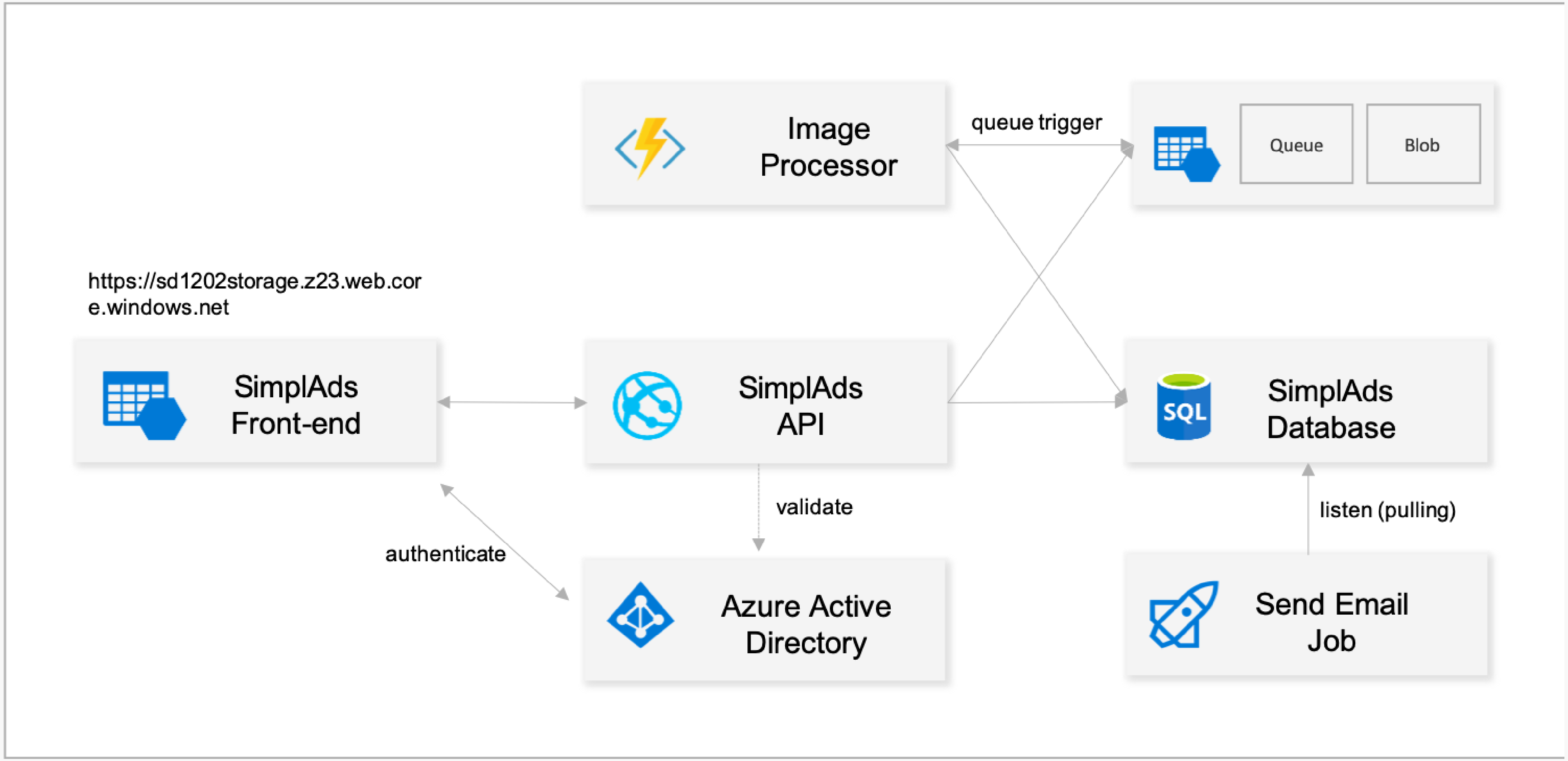
🟩 Deployed service authentication

🟧 Developer authentication

⬜ Interactive developer authentication (disabled by default)

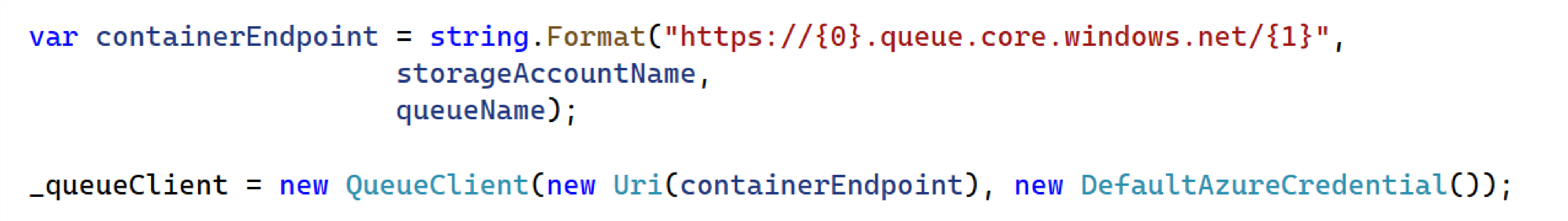
https://docs.microsoft.com/en-us/dotnet/api/overview/azure/identity-readme

Demo

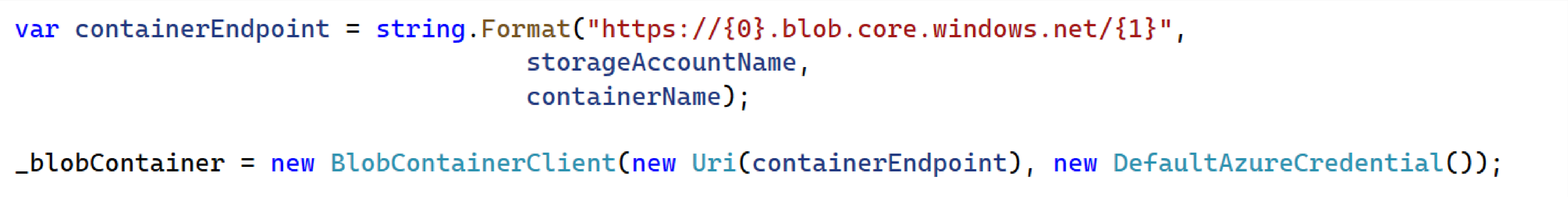


https://dev.azure.com/thienn/SimplAds

Storage - Code

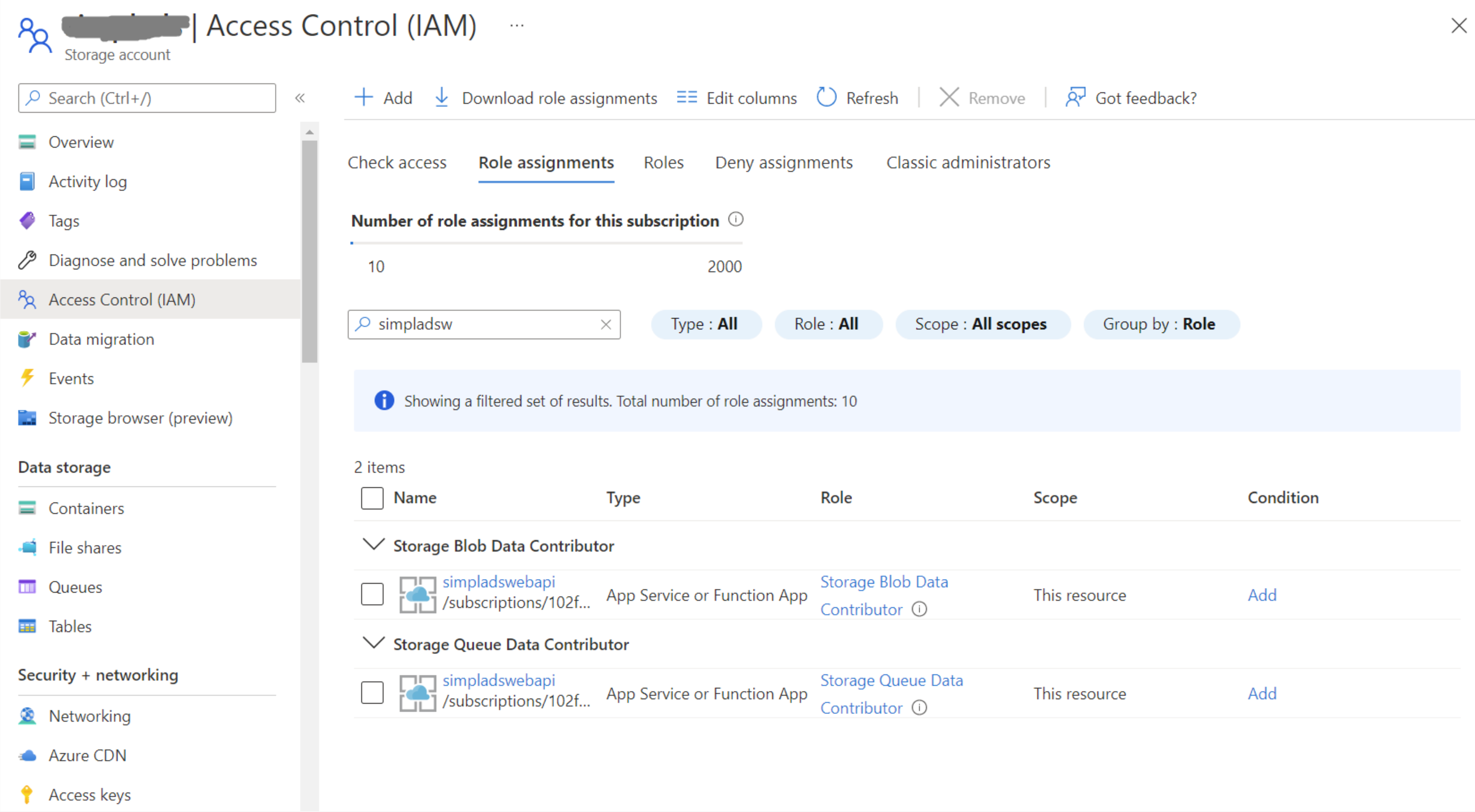


```
var containerEndpoint = string.Format("https://{0}.queue.core.windows.net/{1}",
                      storageAccountName,
                      queueName);

_queueClient = new QueueClient(new Uri(containerEndpoint), new DefaultAzureCredential());
```



```
var containerEndpoint = string.Format("https://{0}.blob.core.windows.net/{1}",
                                  storageAccountName,
                                  containerName);

_blobContainer = new BlobContainerClient(new Uri(containerEndpoint), new DefaultAzureCredential());
```

Storage – Add Access Control



[redacted] | Access Control (IAM)

Number of role assignments for this subscription

10 2000

simpladsw

Type : **All** Role : **All** Scope : **All scopes** Group by : **Role**

Showing a filtered set of results. Total number of role assignments: 10

2 items

Name	Type	Role	Scope	Condition
Storage Blob Data Contributor				
simpladswebapi /subscriptions/102f...	App Service or Function App	Storage Blob Data Contributor	This resource	Add
Storage Queue Data Contributor				
simpladswebapi /subscriptions/102f...	App Service or Function App	Storage Queue Data Contributor	This resource	Add

Azure SQL Database

Add permission for system-assigned identity

```
CREATE USER [<app-name>] FROM EXTERNAL PROVIDER;
ALTER ROLE db_datareader ADD MEMBER [<app-name>];
ALTER ROLE db_datawriter ADD MEMBER [<app-name>];
ALTER ROLE db_ddladmin ADD MEMBER [<app-name>];
```

Add permission for user-assigned identity

```
CREATE USER [<identity-name>] FROM EXTERNAL PROVIDER;
ALTER ROLE db_datareader ADD MEMBER [<identity-name>];
ALTER ROLE db_datawriter ADD MEMBER [<identity-name>];
ALTER ROLE db_ddladmin ADD MEMBER [<identity-name>];
```

Azure SQL Database – EF Core

Install-Package Microsoft.Data.SqlClient

Update connection string

"Server=tcp:<server-name>.database.windows.net;Database=<database-name>;Authentication=Active Directory Default;TrustServerCertificate=True"

"Server=tcp:<server-name>.database.windows.net;Database=<database-name>;Authentication=Active Directory Default;User Id=<client-id-of-user-assigned-identity>;TrustServerCertificate=True"

Managed identities token

- Managed identity tokens are cached per resource URI for around 24 hours
- Refresh token is handled by the client sdk

References

- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview
- https://www.youtube.com/watch?v=rC1TV0_sIrM
- https://docs.microsoft.com/en-us/dotnet/api/overview/azure/identity-readme
- https://github.com/Azure/azure-sdk-for-net/tree/main/sdk/identity/Azure.Identity
- https://github.com/Azure/azure-sdk-for-net/blob/main/sdk/core/Azure.Core/src/Pipeline/BearerTokenAuthenticationPolicy.cs
- https://blog.jongallant.com/2021/08/azure-identity-101/
- https://dev.to/stratiteq/managed-identity-how-it-works-behind-the-scenes-co4
- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-status
- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identities-faq
- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/managed-identity-best-practice-recommendations

Thanks for joining !

DEV CAFE

Connect and share

https://www.facebook.com/devcafevn