

# Passwordless Azure Authentication using Managed Identities

- Jan Vidar Elven
- Senior Architect @ Skill
- Twitter @JanVidarElven
- MVP Enterprise Mobility



Official sponsors



RECAST SOFTWARE

# NORDIC

— VIRTUAL SUMMIT —

# Agenda

1

**Defining  
Passwordless**

**Managed Identity**

2

3

**Using Managed  
Identities**

**Azure Serverless  
and Managed  
Identities**

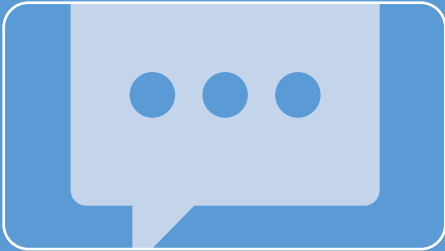
4

1

# What does Passwordless mean?

From Password-based Authentication to Passwordless

# From Password-based to Passwordless Authentication



## Password-based Authentication

- Something you know
- Single-factor authentication

### Azure solutions:

- Client ID + Secret
- DB Connectionstring
- Keys, ..



## Password+Factor Authentication

- Something you know + something you have
- 2FA
- Multi-Factor Authenticon

### Azure solutions:

- Client ID + Certificate
- IP, VNet Integration
- ..



## Passwordless Authentication

- Something you have + Something you are

### Azure solution:

- Managed Identity!

# Challenges in Azure Services Authentication

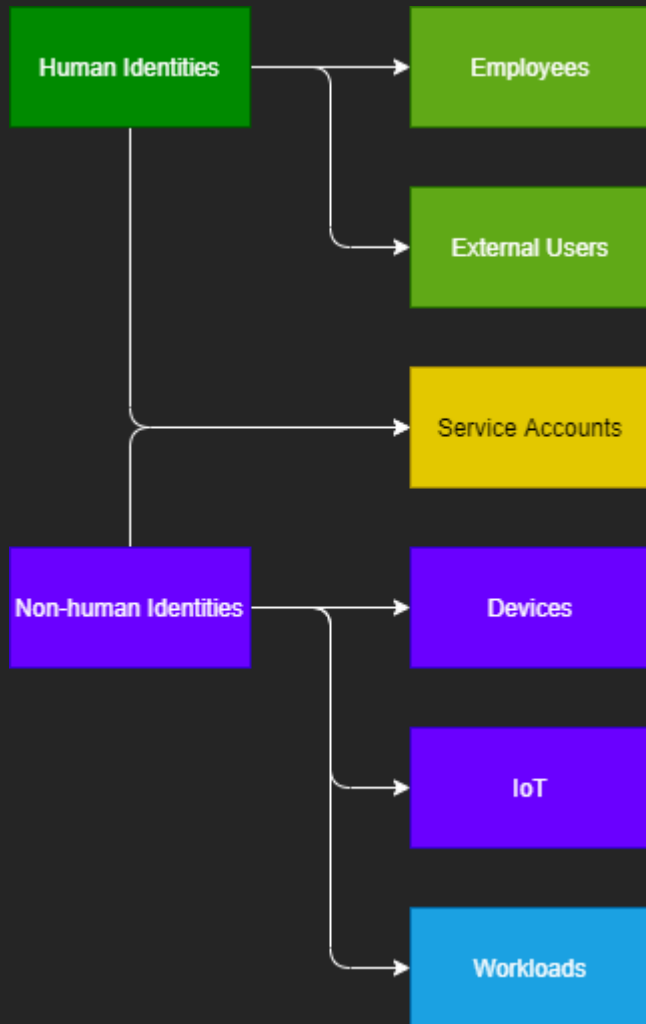
## Development

- Managing Secrets and Credentials between Components in a Solution
- Lifecycle challenges
- Example: App Service needs to access Azure SQL, Storage Account, Key Vault etc.

## Operations

- Using Accounts, Credentials and Secrets for Automation or Management Operations
- Policy exemptions & monitoring security breach
- Overprivilege, permission gap
- Example: Logic App needs to Start or Stop a VM

# What are Service/Workload Identities?



## Service Accounts

- A User Account created with Privileges
- Often Single-Factor Auth
- Used for Legacy/Basic Auth

## Service Principals

- Application identities and Managed identities
- Modern Authentication for Services that Support Azure AD
- Represented as an Enterprise Application in Azure AD

1

2

# Managed Identity

Definition and Use Case

# “Managed Identity is an Identity Connected to your Azure Service”

- Can be Used for Connecting to any Resources that support Azure Active Directory (Azure AD) Authentication



# Benefits of Managed Identities

No Credential Management



Any Azure AD Authentication



No Additional Cost



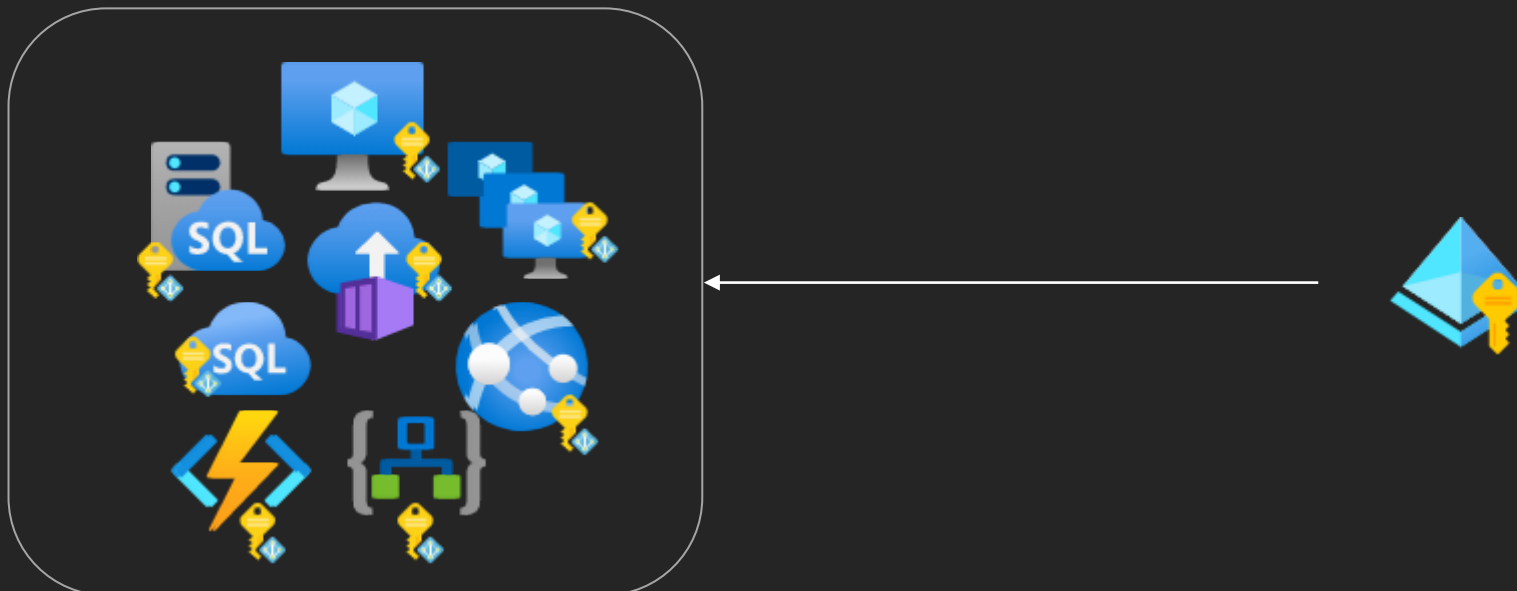
# Types of Managed Identities

## System-Assigned

- Part of specific resource
- Lifecycle follows resource
- Cannot be shared

## User-Assigned

- Standalone Azure resource
- Independent lifecycle
- Shared between Azure resources



# I can use Managed Identities when...

## 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!

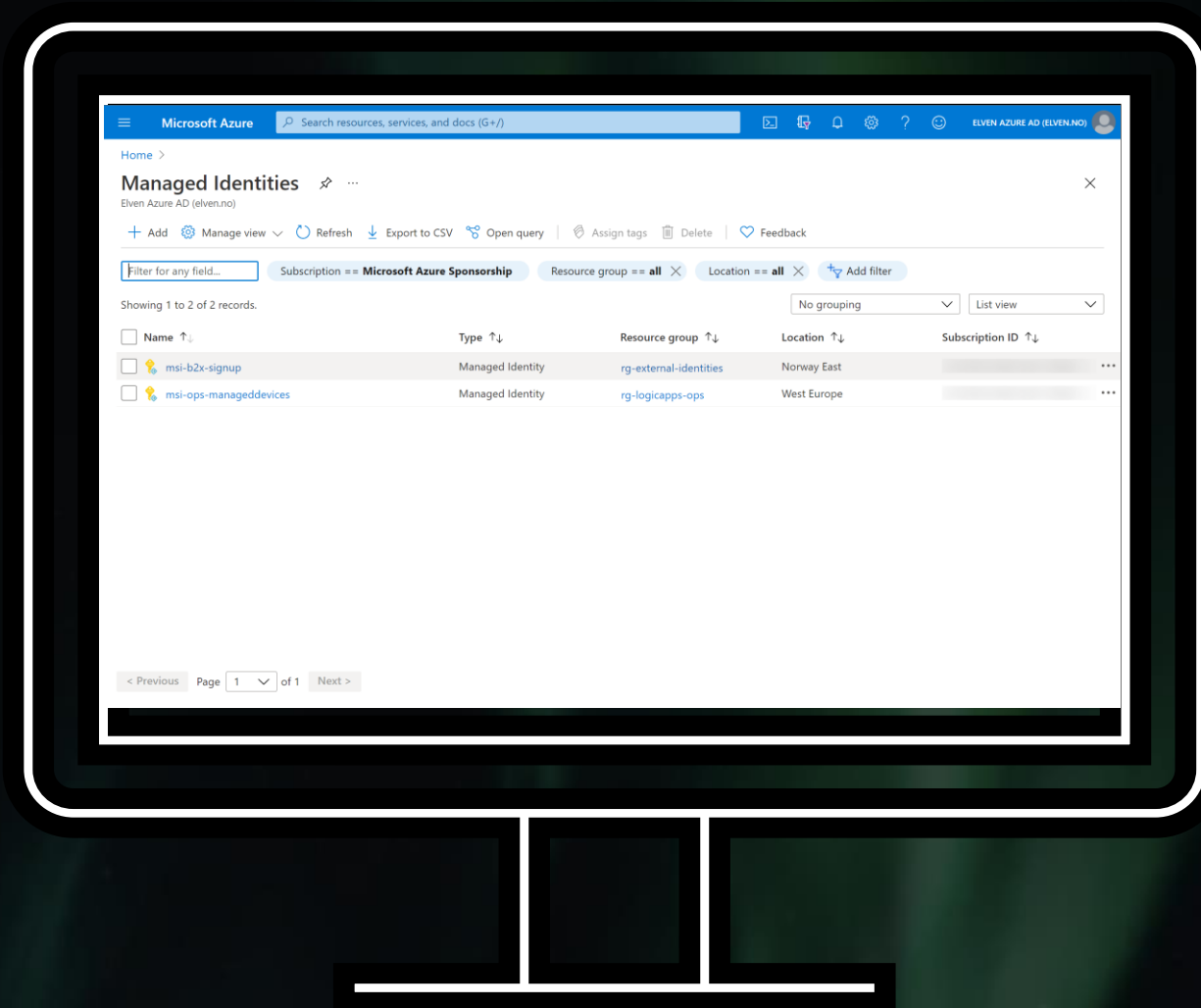
As a Developer, I  
want to build an  
application using

**..not only  
Developers,  
also IT Ops  
and Sec Ops**

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

# DEMO

## Azure Managed Identity





1

2

3

# Using Managed Identity

How Azure Services Use Managed Identities

# Start with Quickstart Samples & Tutorials at Docs

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

## ▼ Quickstarts

- ▼ Use a VM managed identity to access Azure Resource Manager

Windows VM

Linux VM

## ▼ Tutorials

› Windows VM/VMSS

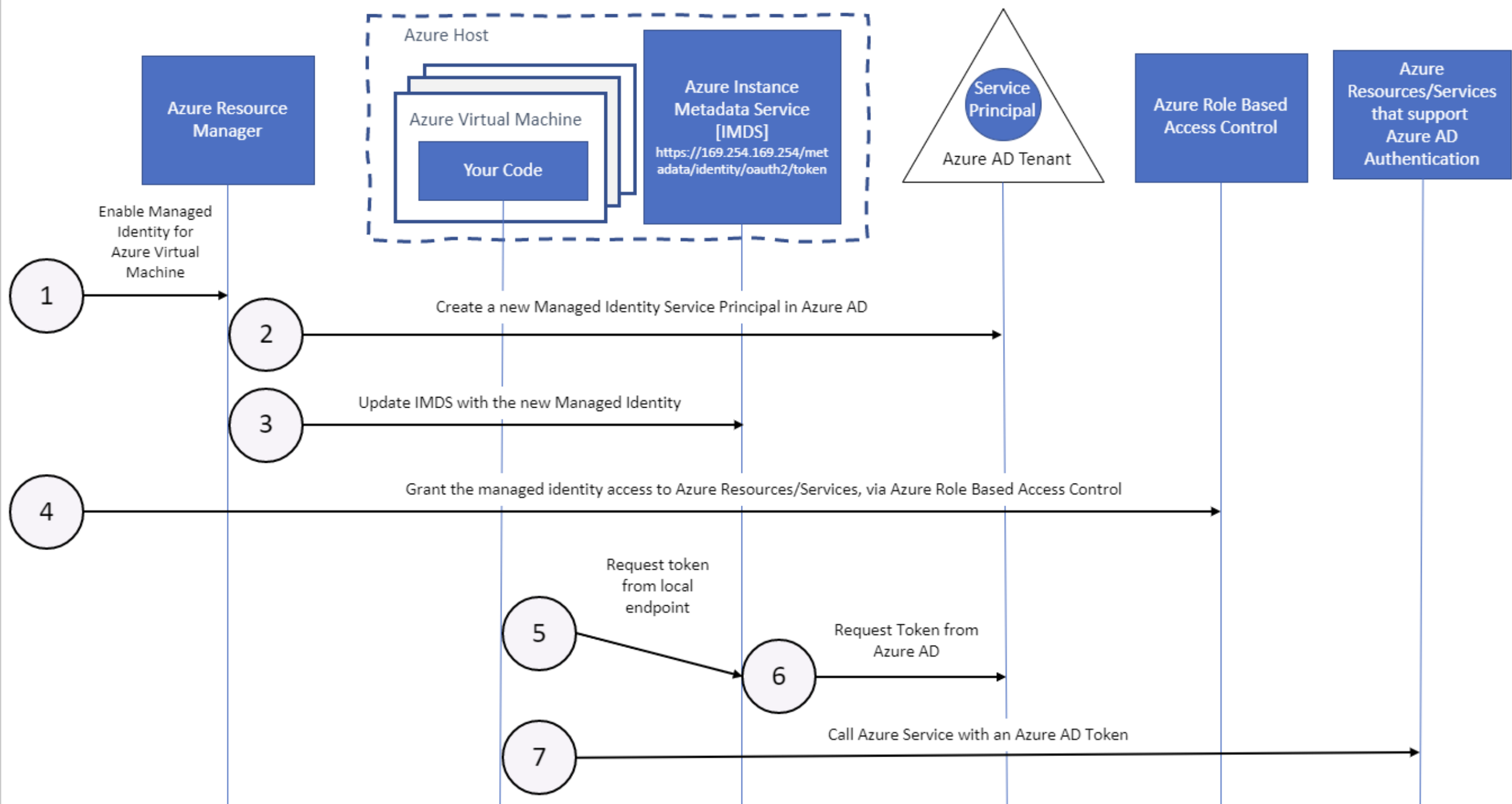
› Linux VM/VMSS

Azure Service Bus

Azure App Service and Functions

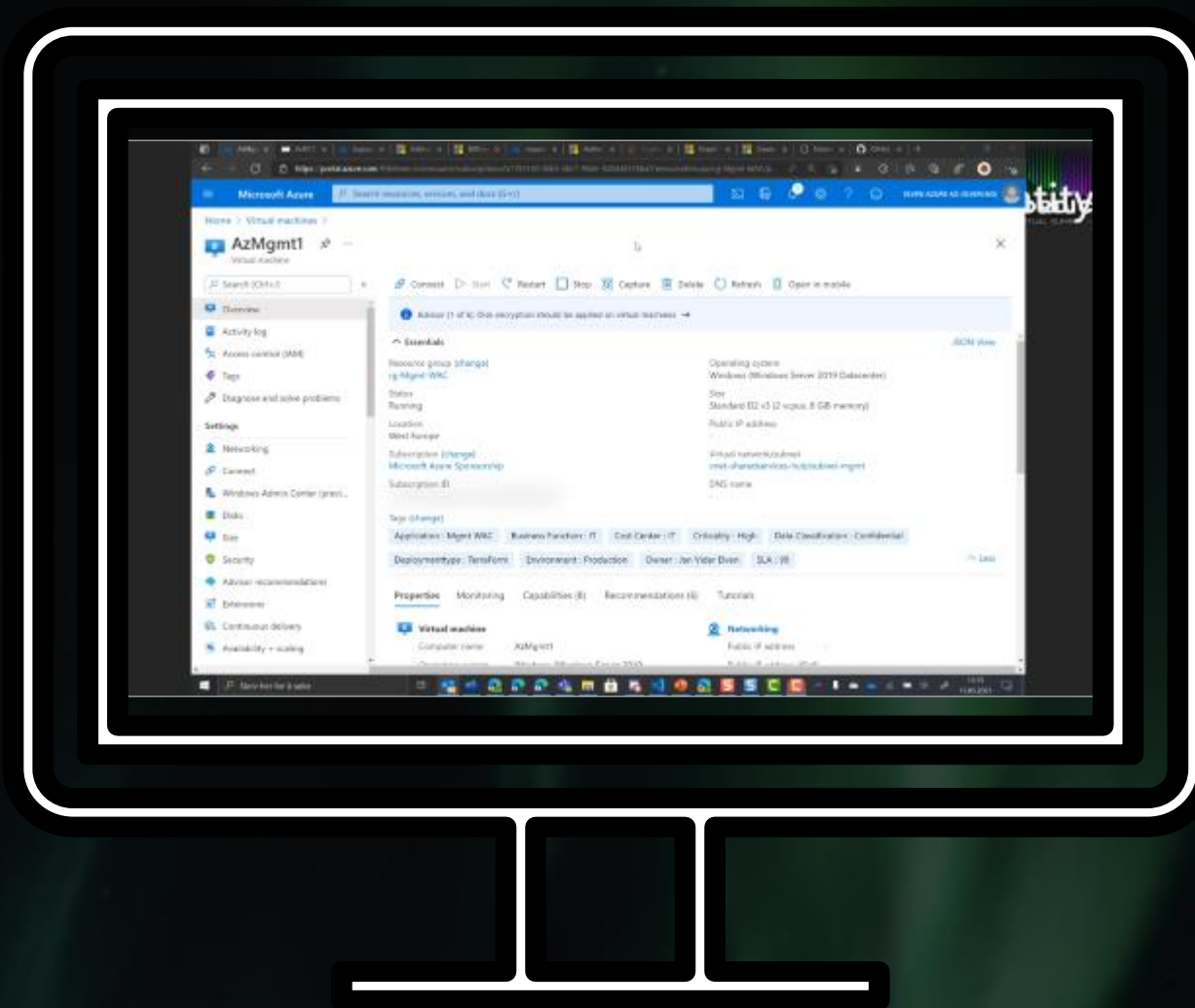
Azure Event Hubs

Azure Container Instances



# DEMO

Managed Identity for  
Azure VM





 **AzMgmt1**    
Virtual machine

&lt;&lt;

 Connect
  Start
  Restart
  Stop
  Capture
  Delete
  Refresh
  Open in mobile

 Advisor (1 of 6): Disk encryption should be applied on virtual machines →

[JSON View](#)

Operating system  
Windows (Windows Server 2019 Datacenter)

Size  
Standard D2 v3 (2 vcpus, 8 GiB memory)

Public IP address  
-

Virtual network/subnet  
vnet-sharedservices-hub/subnet-mgmt

DNS name

Application : Mgmt WAC      Business Function : IT      Cost Center : IT      Criticality : High      Data Classification : Confidential

Deploymenttype : TerraForm      Environment : Production      Owner : Jan Vidar Elven      SLA : 99

^ Less

## Tutorials

 **Networking**

Public IP address -

Public IP address (IPv6)



1

2

3

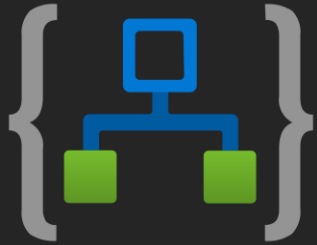
4

# Azure Serverless and Managed Identities

Usage Scenarios for Serverless and Managed Identities

# Managed Identity with Serverless Management and Automation Solutions

## Azure Logic Apps



- Supports Managed Identity for Connector and Actions
- HTTP Action

## Azure Functions



- Supports Managed Identity via Function Code
- Can be used against any API protected by Azure AD

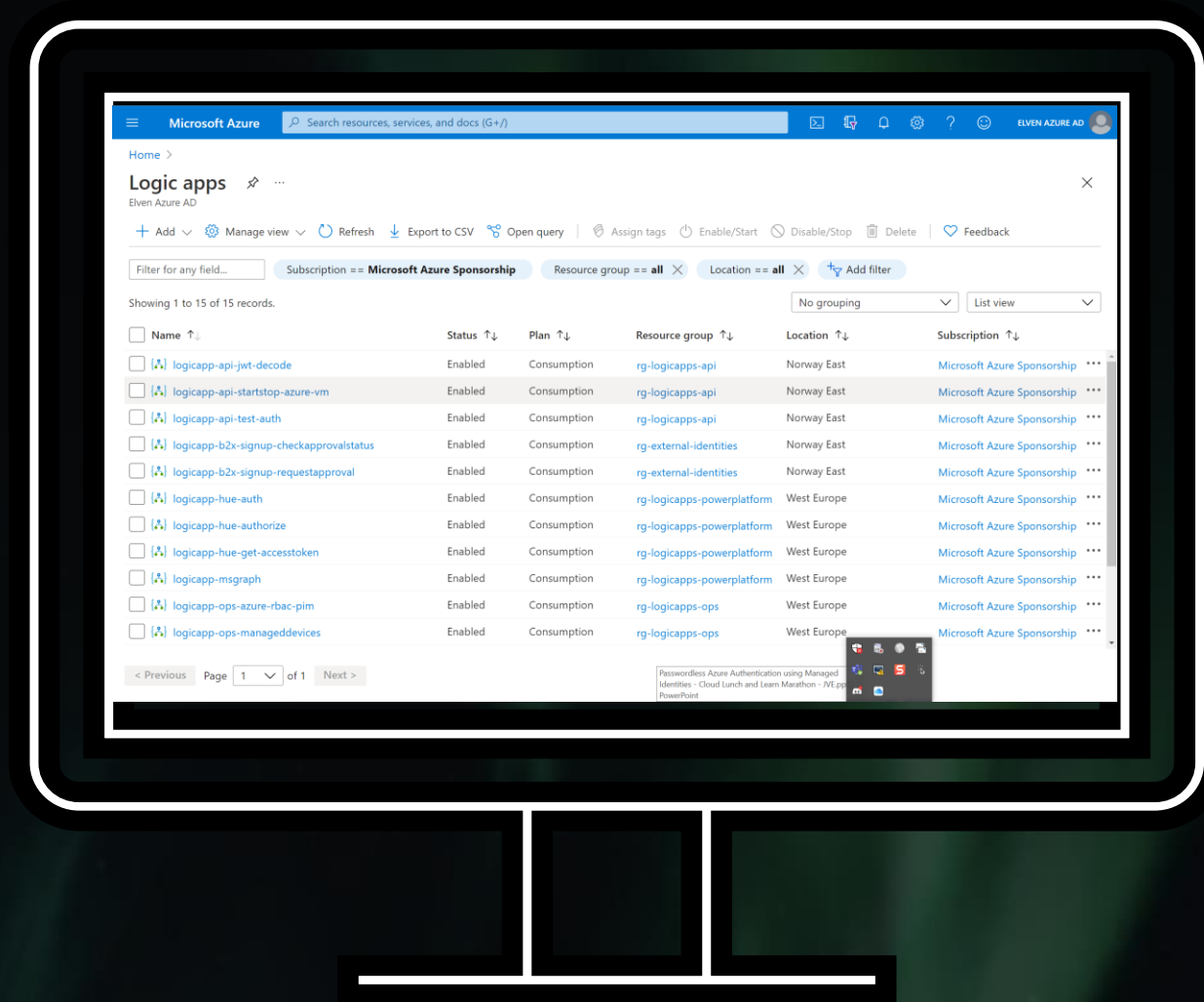
## Azure Automation



- Support Managed Identity for Runbook automation
- <https://docs.microsoft.com/en-us/azure/automation/enable-managed-identity-for-automation>
- [PS! AutoWarp!](#)

# DEMO

## Managed Identity for Azure Serverless



# Resources

- Docs:
  - <https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview>
- Samples & Blog Posts from my own Community Contributions:
  - <https://github.com/JanVidarElven/ProtectAzureServerLessWithAzureAD>
  - <https://gotoguy.blog/2022/03/15/add-graph-application-permissions-to-managed-identity-using-graph-explorer/>
  - <https://gotoguy.blog/2020/12/31/protect-logic-apps-with-azure-ad-oauth-part-1-management-access/>
  - <https://gotoguy.blog/2021/12/22/creating-an-azure-ad-protected-api-in-azure-in-a-school-hour/>

# A big thanks to our sponsors



**RECAST SOFTWARE**

# Thank you!

**Please remember to fill out the evals!**

**<https://stream.nordicvirtualsummit.com/feedback>**

