May 31 – June 2, Oslo Spektrum

10th anniversary

Azure Authentication using Managed Identities vs. Service Principals

Jan Vidar Elven
Tech Lead Cloud Platform & Security Skill
MVP Enterprise Mobility

Martin Ehrnst
Lead Architect Platform
Vipps
MVP Azure

1

Moving to the passwordless era..

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 Authenticaton

Azure solutions:
- Client ID + Certificate
- IP, VNet Integration
- ..

Passwordless Authentication

- Something you have + Something you are

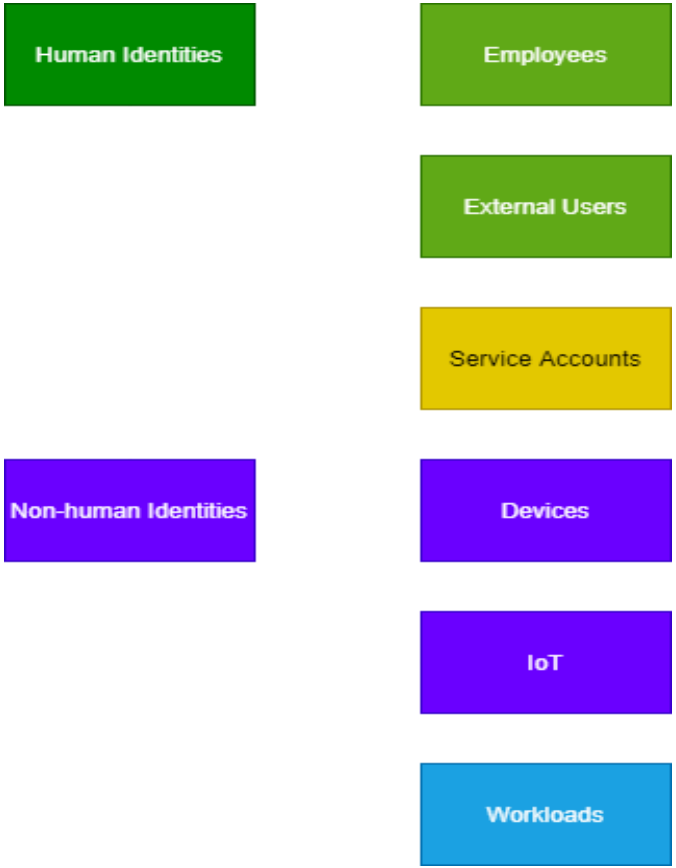
Azure solution:
- Managed Identity!

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

2

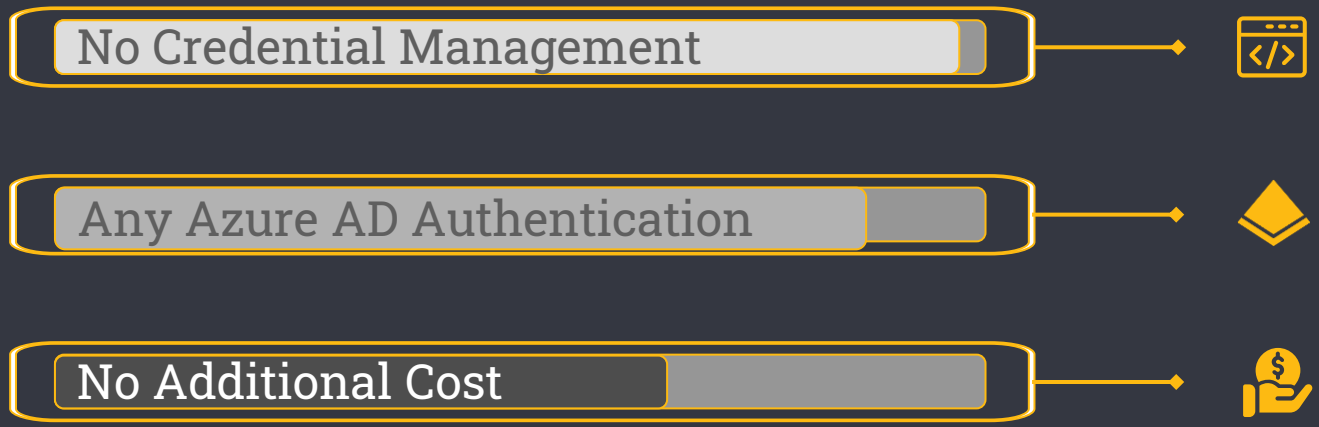
Managed Identity

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



Types of Managed Identites

- 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…

As a Developer, I want to build an application using

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

Source:

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

that accesses

Target:

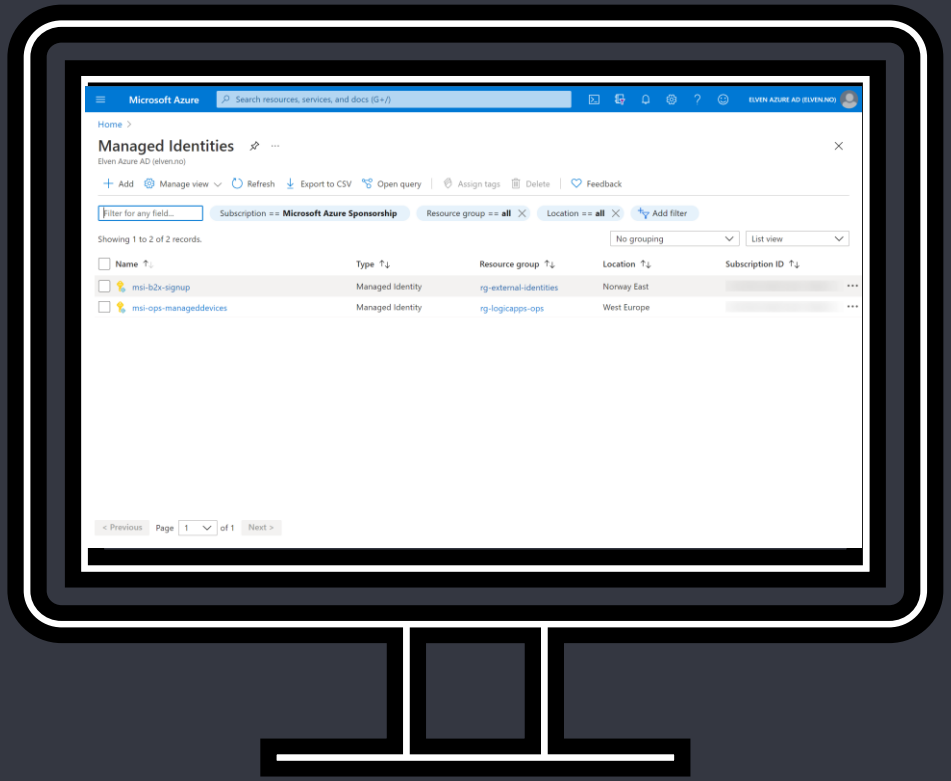
Any target that supports Azure Active Directory Authentication:
- **Your applications**
- **Azure Services:**
  - Azure Key Vault
  - Azure Storage
  - Azure SQL…

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.

DEMO

Azure Managed Identity



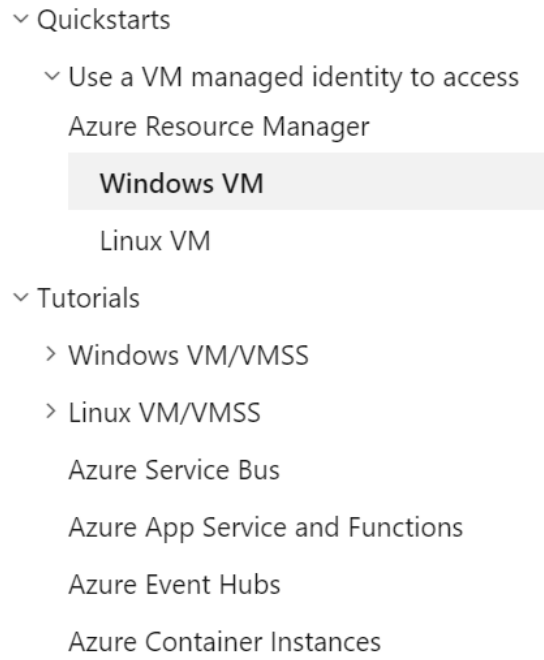
3

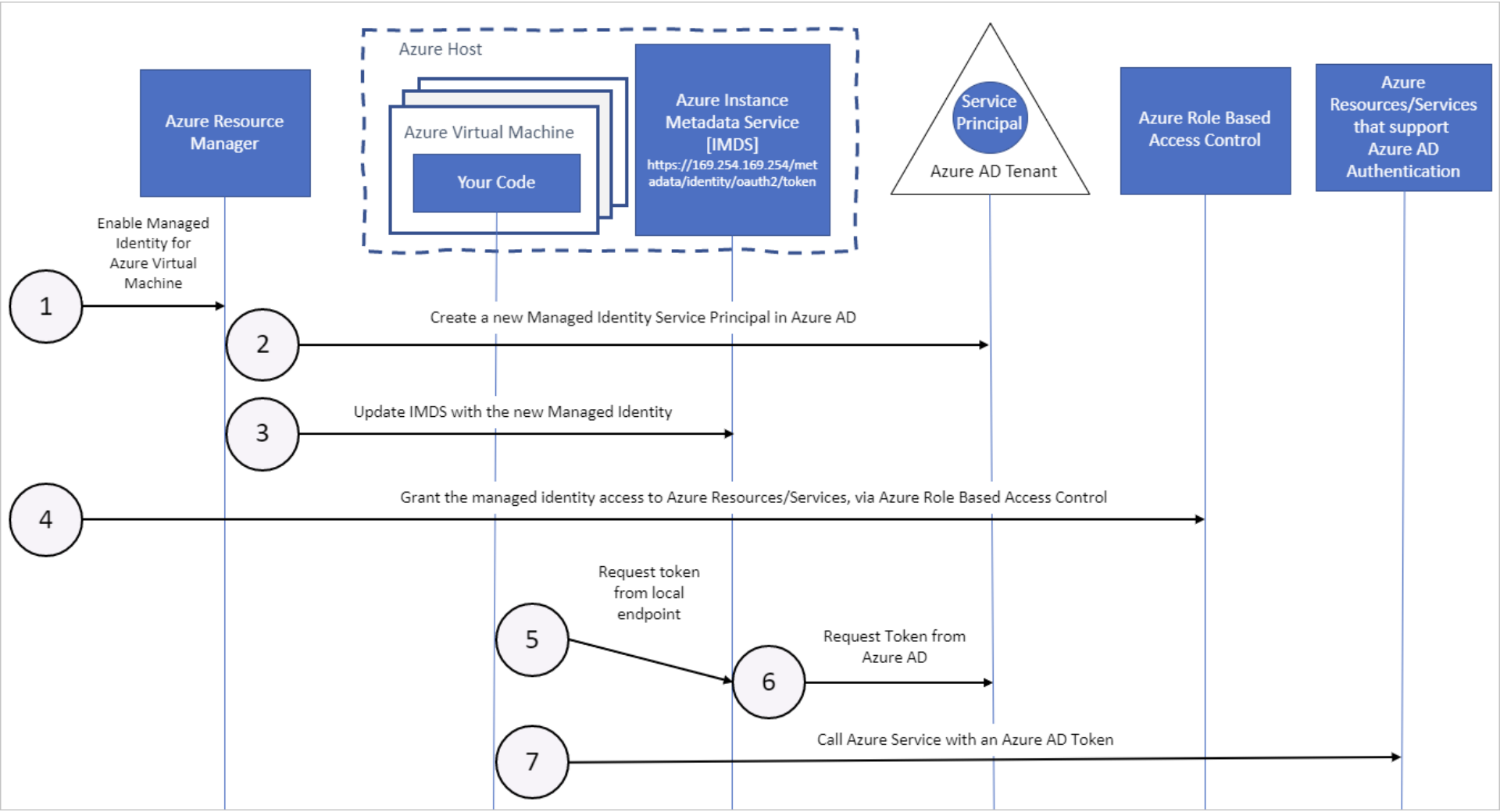
Using Managed Identity

How Azure Services Use Managed Identities

Start with Quickstart Samples & Tutorials at Docs

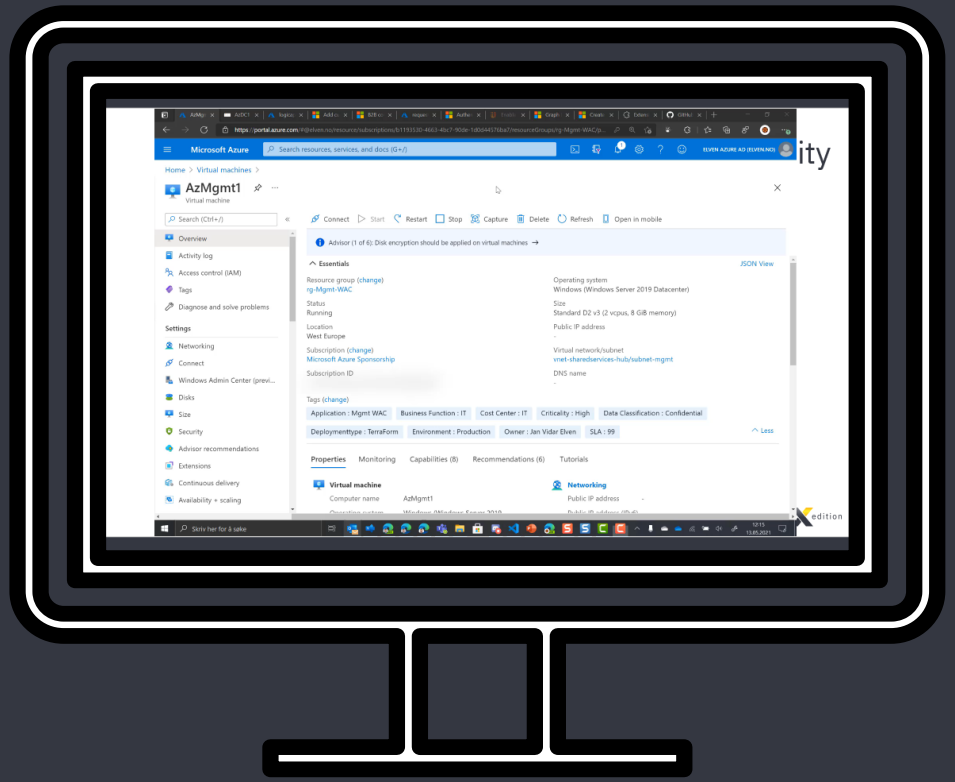
- https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/

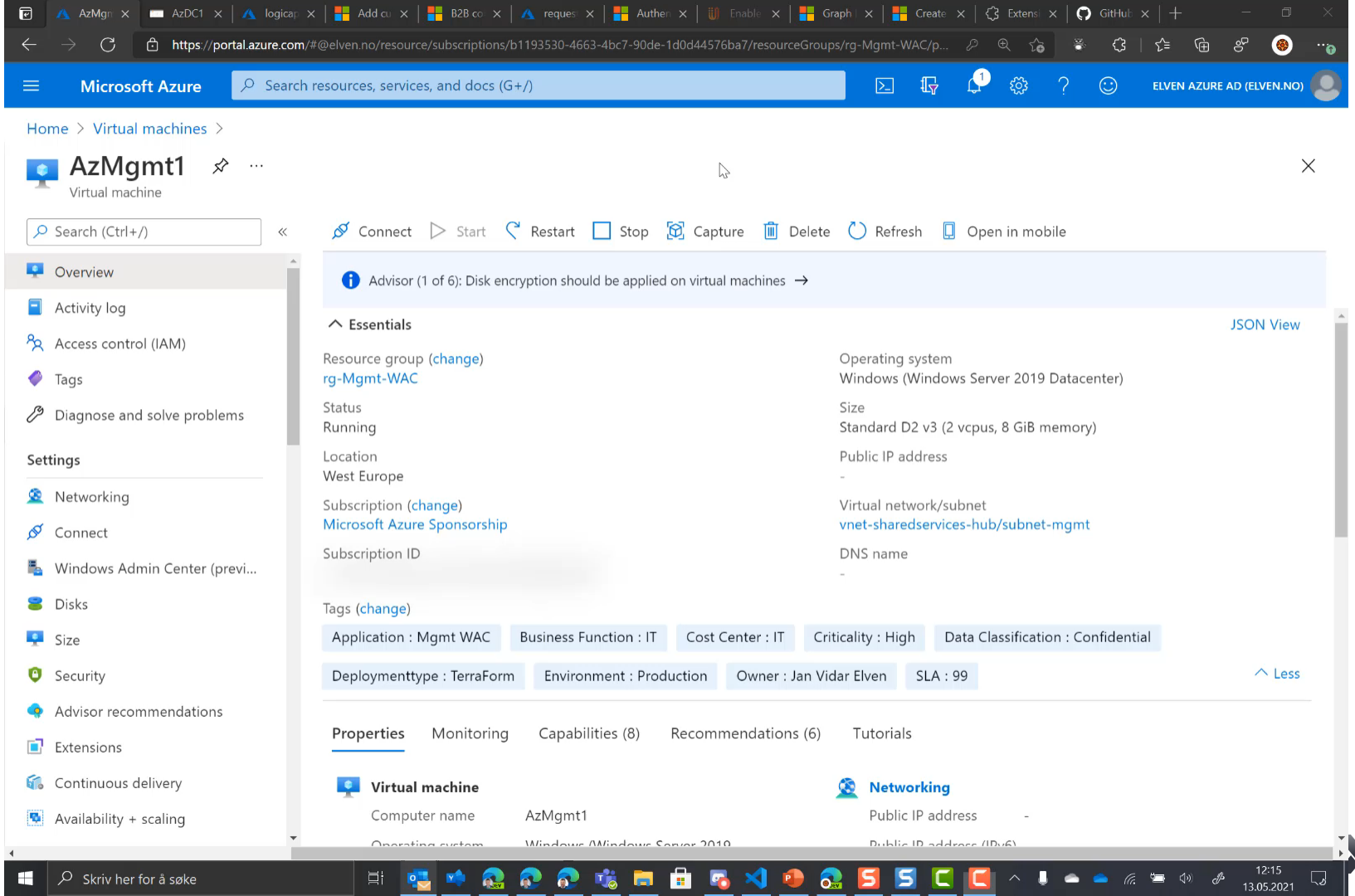



Azure Host
Azure Virtual Machine
Your Code
Azure Instance Metadata Service [IMDS]
https://169.254.169.254/metadata/identity/oauth2/token
Azure Resource Manager
Service Principal
Azure AD Tenant
Azure Role Based Access Control
Azure Resources/Services that support Azure AD Authentication
Enable Managed Identity for Azure Virtual Machine
1
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
Request token from local endpoint
5
6
Request Token from Azure AD
7
Call Azure Service with an Azure AD Token

DEMO

Managed Identity for Azure VM




https://portal.azure.com/#@elven.no/resource/subscriptions/b1193530-4663-4bc7-90de-1d0d44576ba7/resourceGroups/rg-Mgmt-WAC/p...
Microsoft Azure
Search resources, services, and docs (G+/)
ELVEN AZURE AD (ELVEN.NO)
Home > Virtual machines >
AzMgmt1
Virtual machine
Search (Ctrl+/)
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Settings
Networking
Connect
Windows Admin Center (previ...
Disks
Size
Security
Advisor recommendations
Extensions
Continuous delivery
Availability + scaling
Connect
Start
Restart
Stop
Capture
Delete
Refresh
Open in mobile
Advisor (1 of 6): Disk encryption should be applied on virtual machines →
Essentials
JSON View
Resource group (change)
rg-Mgmt-WAC
Status
Running
Location
West Europe
Subscription (change)
Microsoft Azure Sponsorship
Subscription ID
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
-
Tags (change)
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
Properties
Monitoring
Capabilities (8)
Recommendations (6)
Tutorials
Virtual machine
Computer name
AzMgmt1
Networking
Public IP address
-

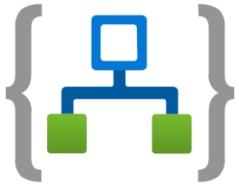
4

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

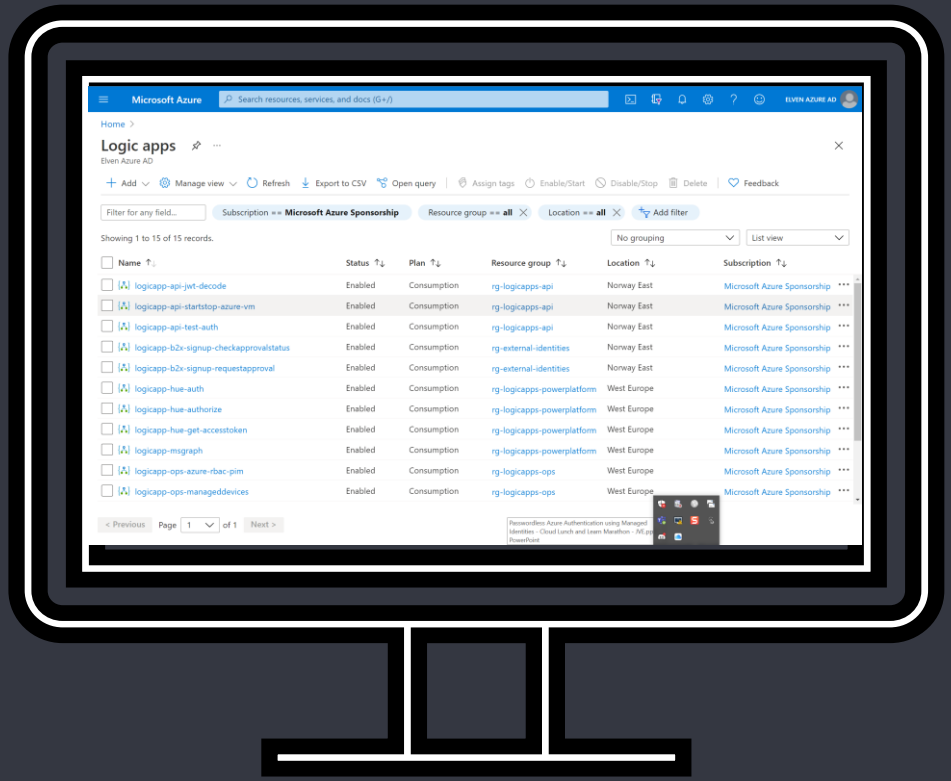
- Supports Managed Identity via Function Code
- Can be used against any API protected by Azure AD

Azure Automation

- Support Managed Identity for Runbook automation
- PS! AutoWarp!

DEMO

Managed Identity for Azure Serverless



nicX edition

Resources

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

- Samples & Blog Posts from Community Contributions:
  - https://github.com/JanVidarElven/ProtectAzureServerLessWithAzureAD
  - https://adatum.no/azure/azure-active-directory/azure-application-registrations-enterprise-app-managed-identities
  - 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/

Connect

Jan Vidar Elven | Martin Ehrnst

@JanVidarElven | @ehrnst

gotoguy.blog | adatum.no

Slides and demos from the conference will be available at

https://github.com/nordicinfrastructureconference/2022