Managed Identities for Azure Resources

Global Azure Bootcamp

Speaker Intro

- Joonas Westlin
- Developer / Architect @ Zure
- Azure MVP
- Global #1 on Stack Overflow for Azure AD answers
- Blog: https://joonasw.net
- Twitter: @JoonasWestlin

Problems with secrets

- Most services use shared secrets/passwords
- Have to:
  - Protect
  - Manage
  - Rotate
  - Revoke
- Often blanket access to e.g. whole Storage account
- Cannot tie access to single service

Managed Identities for Azure resources

- Previously known as Managed Service Identity
- Features
  - Automatic service identity creation
  - Key management and rotation
  - Identity lifecycle management
- Azure services can use their managed identity to access services with no credentials stored in code or configuration
- Price: free

Managed Identities for Azure resources

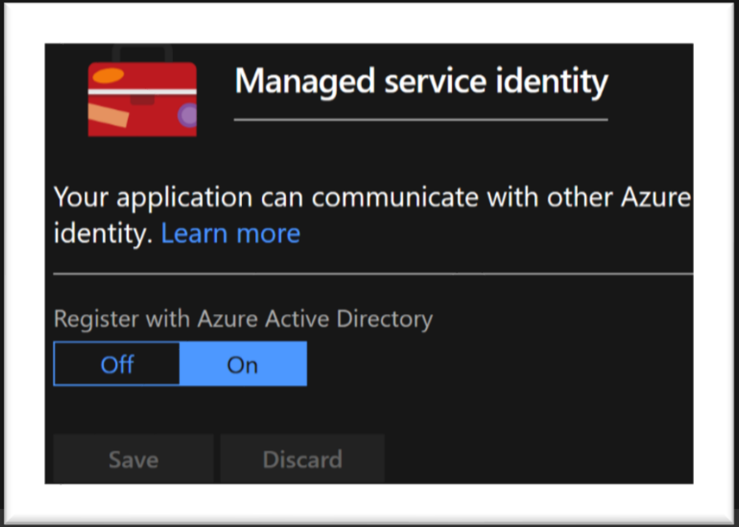
- Two types of managed identities assignable to services
- System-assigned identity
  - Tied to service
- User-assigned identity
  - Multiple services can share
- Check service support: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities

Why do we do this?

- No secrets to worry about in code or configuration
- No key rotation to remember
- More granular access for apps
- Auditable
- Revocation can be done very quickly

Basic Principles

- Managed Identity creates a *service principal* in AAD
- This principal must be granted access to the target service
- Access can be assigned at AAD or service level

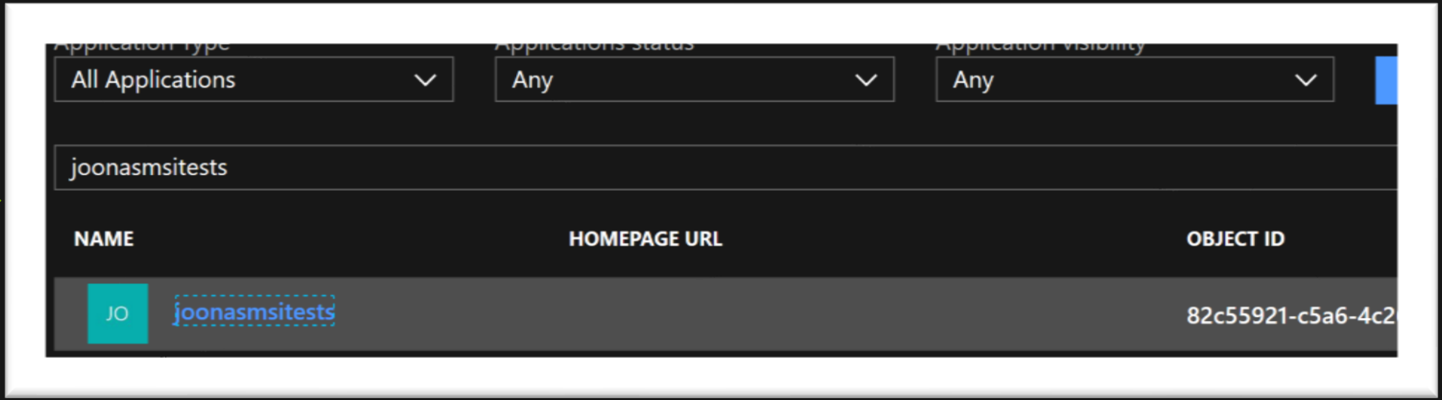


Managed service identity

Your application can communicate with other Azure identity. Learn more

Register with Azure Active Directory

Off [✓ On]



Application type	Applications status	Application visibility
All Applications	Any	Any

joonasmsitests

NAME	HOMEPAGE URL	OBJECT ID
JO joonasmsitests		82c55921-c5a6-4c2

Services supporting Azure AD auth

- ARM API
- Key Vault
- Data Lake
- SQL DB
- Storage
- Service Bus
- Event Hubs
- *Any service that supports application permission-based authentication*
- Ref: https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/services-support-managed-identities#azure-services-that-support-azure-ad-authentication

Demo

https://joonasmsitests.azurewebsites.net/

ZURE