MSA a gMSA účty pro běh SQL Serveru

Marek Chmel
Sr. Cloud Solutions Architect – Data & AI @ Microsoft CEE
Azure Solutions Architect Expert | AWS Certified Solutions Architect | CEH | MCSE & MCT
marekchmel@outlook.com

Motivation

- Installing SQL Server requires an account or set of accounts to be used for various SQL Server services available on your system. There's a myriad of options to choose from which have security impacts and different complexity for deployment.

- The Theory
  - Be able to use SQL Server without traditional user accounts.
  - Use AD features to control this
  - Needs Windows AD – so not vetted out on SQL on Linux only environment (or containers since they don't work nicely with AD) - Yet

Service Accounts

- Service accounts used to start and run SQL Server can be
  - domain user accounts
  - local user accounts
  - managed service accounts
  - virtual accounts (default for current version of SQL Server)
  - built-in system accounts

- Most common ? – domain user account
  - Password challenges
  - Scale-out challenges
  - SPN challenges

Overview

- gMSA in Windows Server 2012 inherits the benefits of sMSA from Windows Server 2008 R2:
  - Automatic password and Service Principal Name (SPN) management without service disruption
  - Password not disclosed
  - Account cannot be used for interactive logon
- gMSA in Windows Server 2012 addresses key limitations of sMSA:
  - Multiple authorized hosts can share the same gMSA allowing a server farm to appear as the same service to clients
  - Supports mutual authentication protocols running on multiple member hosts

Standalone Managed Service Accounts

- Designed to provide services and tasks their own domain accounts
- Automates
  - Password management
  - SPN management
  - Delegation
- Windows 2008 R2 and Windows 7 – introduced
- Limited to 1 server

- Is a user and a computer at the same time

Standalone Managed Service Accounts

- MSA – like a quasi-computer object and uses same password management mechanism used by computer objects
- Updated every 30 days by default
- Use a complex, auto generated password
  - 240 bytes
  - 120 characters
  - Cryptographically random
- Cannot be locked out
- Cannot login interactively
- Can manually set pwd – no justifiable reason for this
- Show up in AD
- Managed via PowerShell

Standalone Managed Service Accounts

- Automatically maintain server principal names (cover in more detail later)
- Linked to 1 computer at a time
- Support delegation
- Can add to AD groups!
- Can use multiple MSAs on a server
  - SQL server services options
    - 1 MSA for all
    - 1 MSA per service

Group Managed Service Accounts

- Similar to the MSAs, but provides functionality to multiple servers
- Manages the synchronizing of password between service instances
- Failover clusters do not support gMSAs
  - Services on top of the cluster can se sMSA and gMSA
- Windows Server 2012 + defaults to gMSA instead of sMSA when setting up
  - Use –RestrictToSingleComputer to setup a sMSA

gMSA Deployment Requirements

- Operating system requirements for authentication to work with services using gMSA:
  - Shared service member hosts: Windows Server 2012 or 2012 R2
  - Member host's domain controllers (DCs): RFC-compliant Key Distribution Center (KDC) (all currently supported Windows Server stock-keeping units (SKUs) that can run Active Directory Domain Services - AD DS)
  - gMSA account's DCs: Enough Windows Server 2012 or newer DCs to support the additional password retrieval traffic
- Active Directory Requirements:
  - Windows Server 2012 Schema update in gMSA domain's forest
  - KDS root key created in the forest hosting the gMSA
  - gMSA account provisioned

How gMSA Works: Simplified

1. An admin creates a gMSA object in Active Directory Domain Services (AD DS) and assigns it to one or more member host computers
2. A DC assigns that gMSA account a password using its Microsoft KDS
3. An admin configures an application service to use the gMSA account
4. The service running on those computers retrieves its password and logs on as that account
5. After a set period, computers hosting services running as the gMSA automatically contact the DC to retrieve the next password for the account. The DC generates a new password for the gMSA
6. The services retrieve and use the new password

Typical Errors

- 1069: service did not start due to logon failure
  - MSA disabled
- Duplicate backlink
  - Trying to link MSA that is already used by another computer (sMSA)
- Enter a valid password
  - Left old password info in logon properties of service
- Account name invalid or does not exist – password invalid for account name specified
  - Did not put the $ at the end of the account name (or typo)

Q & A

Marek Chmel

Sr. Cloud Solutions Architect – Data & AI @ Microsoft CEE

Azure Solutions Architect Expert | AWS Certified Solutions Architect | CEH | MCSE & MCT

marekchmel@outlook.com