



SCAN ME

Managed Service Accounts Redux

Unveiling Best Practices And Security Measures To Reduce Risk And Impact



MC2MC
—CONNECT—

Introducing Me, Myself & I!



Jorge de Almeida Pinto Senior Incident Response Lead

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



<http://tiny.cc/JQFKblog>



<http://tiny.cc/JQFKtwitter>



<http://tiny.cc/JQFKgithub>



<http://tiny.cc/JorgeLinkedIn>



<https://www.semperis.com/>



The Sponsors Of MC2MC Connect...

2Pint



robopack

wortell

INGRAM MICRO®



The Collective

bechtle

lebon.IT

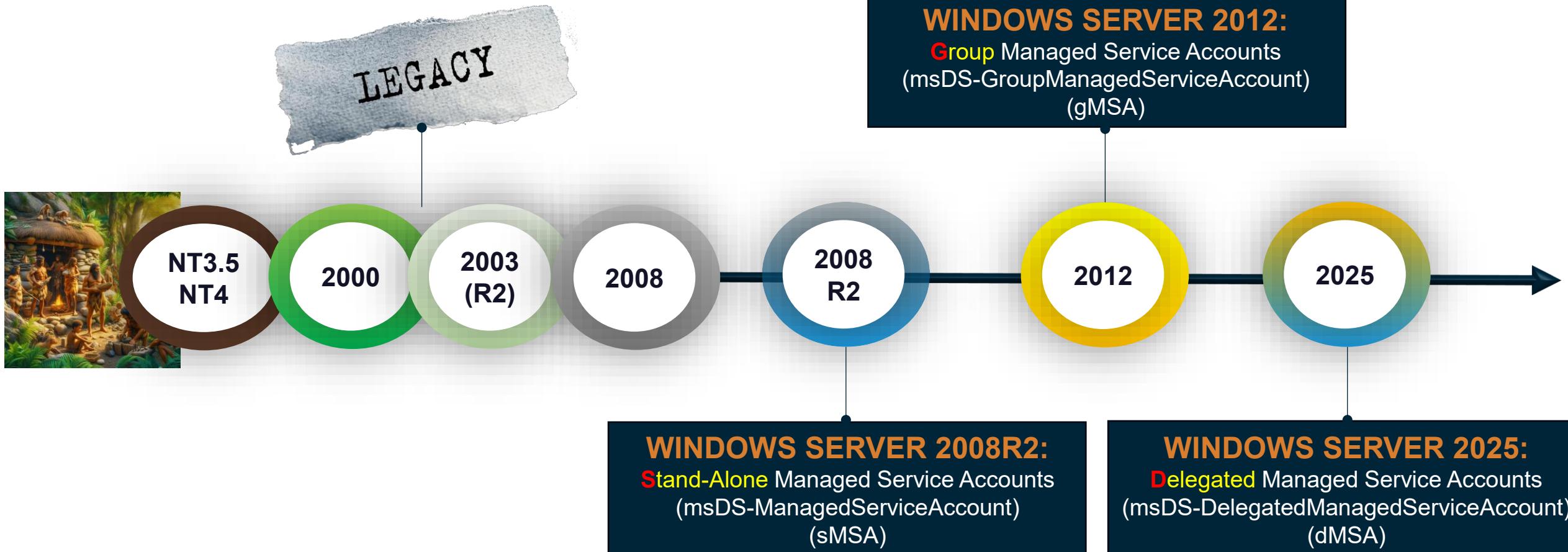


VirtualMetric

veeam

eVri

Evolution Of Service Accounts

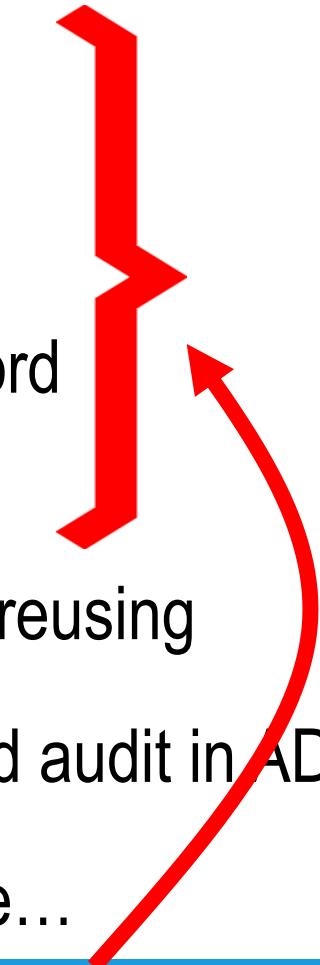


(Legacy) Service Accounts

Common Good, Bad And Ugly Reality



- Used for svcs, 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 many occasions no clear/unique/consistent naming convention + reusing
- No ownership/periodic recertification → hard to discover, secure and audit in AD
- Prime targets for attackers using the "*Kerberoasting Attack*" because...



(Legacy) Service Accounts vs xMSAs

Main benefits of sMSAs/gMSAs/dMSAs over (legacy) service accounts?

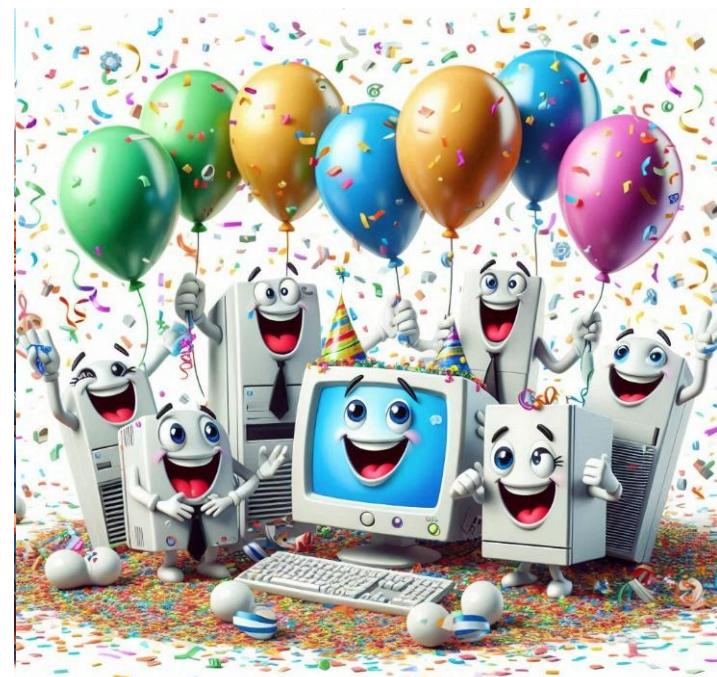
- Automatic, better & stronger credential management

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)

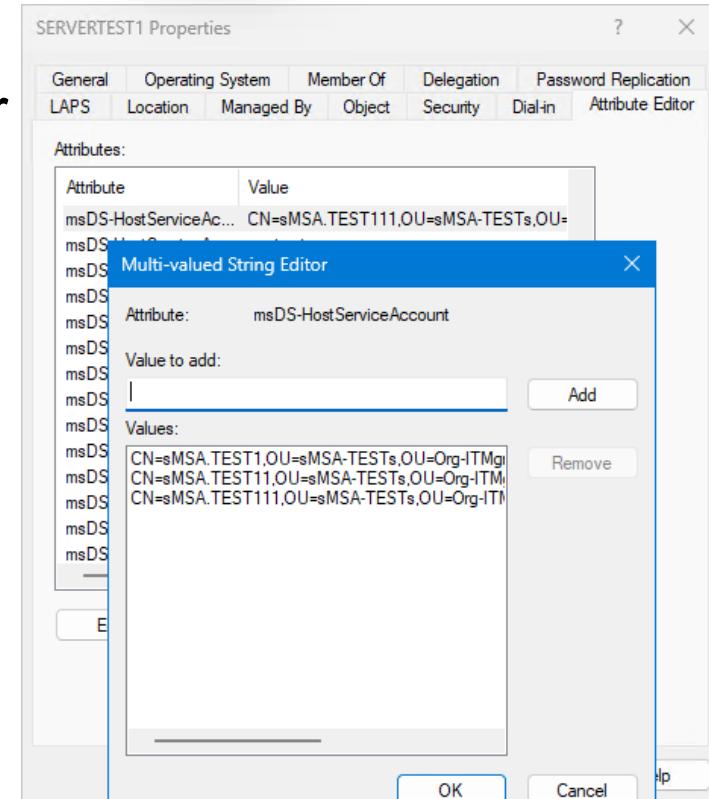


Managed Service Accounts

Stand-Alone (sMSA)

2008
R2

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



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)

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=GRP_R0_ALLOWCache-ROFSRODC1,OU=Group...
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-ROFSRODC1,OU=Group...
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=sMSA.TEST111,OU=sMSA-TESTs...	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=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
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,...}	{CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}

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-ManagedObjectId" and "msDS-ManagedObjectPreviousId"
 - "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 EF 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 1B 00 00 00 13 00 00 00 CE 38 D9 29 37 62 0F 40 CD 42 E4 EF 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...)

"The DS Managed/Resource" constructed attribute is a container object containing a PL-QD with

Two screenshots of Active Directory Manager showing the "dsCore" attribute for a gMSA:

Screenshot 1 (RWDC):

```

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;
uSNCchanged: 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))

Screenshot 2 (RODC):

```

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;
uSNCchanged: 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!).

Managed Service Accounts

Group (gMSA)

```
Administrator: Windows Pow + 
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 : 63b36db40c5cc43c86306e839f7a1c76
SecureCurrentPassword : System.Security.SecureString
PreviousPassword : f75c692672e5a1821b45c5073c5cec13
SecurePreviousPassword : System.Security.SecureString
QueryPasswordInterval : 14:32:51.4560834
UnchangedPasswordInterval : 14:27:51.4560834

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

AD PoSH

```
Administrator: Windows Pow + 
DistinguishedName: CN=GMSA_1DAY_001,OU=TEST,DC=ADTEC,DC=NET
SamAccountName: GMSA_1DAY_001$
```

DS Internals

```
# 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))"
```

DS Internals

```
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
```

Works With BOTH gMSA And dMSA

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



Managed Service Accounts

Group (gMSA)



- Get relevant data from all gMSAs (Group Managed Service Accounts) in AD Domain (<https://gist.github.com/zjorz/d1906ac04964a29d87bd377e0298eb21>)

CN=GMSA35B18	CurKDSRootKeyOrgRWDCDateTime	PrevKDSRootKeyGuid(+KeyCre...	PrevKDSRootKeyOrgRW...	PrincipalsAllowedToRetrieveManagedPasswordCONFIGURED	PrincipalsAllowedToRetrieveManagedPasswordEFFECTIVE	MemberOf
CN=GMSA35B18	09:13:46:52	DTCNTR01\R0FSRWDC2 (2025-06-10 20:07:30)	be3cf336-9db8-ef50-1efd-a28...	DTCNTR01\R0FSRWDC2 (2...	{SERVERTEST3\\$ (S-1-5-21-274783270-2712129839-3354909249-1...	(CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=GMSA35B18	09:13:46:52	DTCNTR01\R0FSRWDC3 (2025-06-10 12:42:38)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC3 (2...	{SERVERTEST3\\$ (S-1-5-21-274783270-2712129839-3354909249-1...	(CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=GMSA35B18	09:13:46:52	DTCNTR01\R0FSRWDC3 (2025-06-10 00:17:45)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC3 (2...	{SERVERTEST1\\$ (S-1-5-21-274783270-2712129839-3354909249-1...	(CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=GMSA35B18	09:13:46:52	DTCNTR01\R0FSRWDC1 (2025-06-10 12:40:47)	8f1ff2ec-6515-6624-ea89-44cb...	DTCNTR01\R0FSRWDC1 (2...	{SERVERTEST2\\$ (S-1-5-21-274783270-2712129839-3354909249-1...	(CN=Domain Admins,CN=Users,DC=ADTEC,DC=NET}
CN=GMSA35B18	24:12:20:55	46bb96e-5-a0d-408a-82b1-742ddf1e3359 (...)	29d938ce-6237-400f-cd42-e46...	46bb96e-5-a0d-408a-82b...	R0FSMBSV3\\$ (S-1-5-21-274783270-2712129839-3354909249-1...	(CN=Performance Log Users,CN=Builtin,DC=ADTEC...
CN=GMSA35B18	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-1-5-21-274783270-2712129839-3354909249-1...
CN=GMSA35B18	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=GMSA35B18	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-1-5-21-274783270-2712129839-3354909249-1...
CN=GMSA35B18	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-04-06 10:32:32)			CN=grp.gs.Tier0-Retrieve-Password-For-gmsa.t0.SQL,OU=G...	0
	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:23)			CN=GroupGMSA35B18EF6732,OU=TEST,DC=ADTEC,DC=NET	0
	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:24)			CN=GroupGMSA35B18EF6742,OU=TEST,DC=ADTEC,DC=NET	0
	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:25)			CN=GroupGMSA35B18EF6752,OU=TEST,DC=ADTEC,DC=NET	0
	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:26)			CN=GroupGMSA35B18EF6767,OU=TEST,DC=ADTEC,DC=NET	0
	24:12:20:55	DTCNTR01\R0FSRWDC1 (2023-06-12 20:31:28)			CN=GroupGMSA35B18EF6771,OU=TEST,DC=ADTEC,DC=NET	0

Managed Service Accounts

Delegated (dMSA)

Security descriptor - CN=gMSA.TEST11,OU=gMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET

Owner	ADTEC\Domain Admins
Group	ADTEC\Domain Admins
SD control	<input checked="" type="checkbox"/> SELF_RELATIVE <input type="checkbox"/> OWNER_DEFAULTED <input type="checkbox"/> GROUP_DEFAULTED

DACL (146 ACEs)

Type	Trustee	Rights	Flags
Allow	CREATOR OWNER	Extended write (Validated write to computer attributes.)	Inherit, Inherit only, Inherited (computer)
Deny	Everyone	Control access (Reset Password)	
Allow	Everyone	Read property (msDS-ManagedPassword)	
Allow	NT AUTHORITY\Authenticated Users	Read	Inherit, Inherited
Allow	NT AUTHORITY\Authenticated Users	Read property (Exchange Information)	Inherit, Inherited
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read property (tokenGroups)	Inherit, Inherit only, Inherited (computer)

gMSA

```
PowerShell
PS C:\Users\regular.user> Get-ADServiceAccount -LDAPFilter "(objectClass=msDS-GroupManagedServiceAccount)" | Measure-Object -Count
Count
-----
58
PS C:\Users\regular.user>
```

Add...
Delete
Edit...

DACL (163 ACEs)

Type	Trustee	Rights	Flags
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read property (tokenGroups)	Inherit, Inherit only, Inherited (user)
Allow	NT AUTHORITY\Authenticated Users	Read property (Exchange Information)	Inherit, Inherited
Deny	Everyone	Control access (Reset Password)	
Deny	Everyone	Read property (msDS-ManagedPassword)	
Allow	CREATOR OWNER	Extended write (Validated write to computer attributes.)	Inherit, Inherit only, Inherited (computer)

dMSA

```
PowerShell
PS C:\Users\regular.user> Get-ADServiceAccount -LDAPFilter "(objectClass=msDS-DelegatedManagedServiceAccount)" | Measure-Object -Count
Count
-----
0
PS C:\Users\regular.user>
```

Add...
Delete
Edit...

Add...
Delete
Edit...

DACL (163 ACEs)

Type	Trustee	Rights	Flags
Allow	NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read property (tokenGroups)	Inherit, Inherit only, Inherited (user)
Allow	NT AUTHORITY\Authenticated Users	Read property (Exchange Information)	Inherit, Inherited
Deny	Everyone	Control access (Reset Password)	
Deny	Everyone	Read property (msDS-ManagedPassword)	
Allow	CREATOR OWNER	Extended write (Validated write to computer attributes.)	Inherit, Inherit only, Inherited (computer)

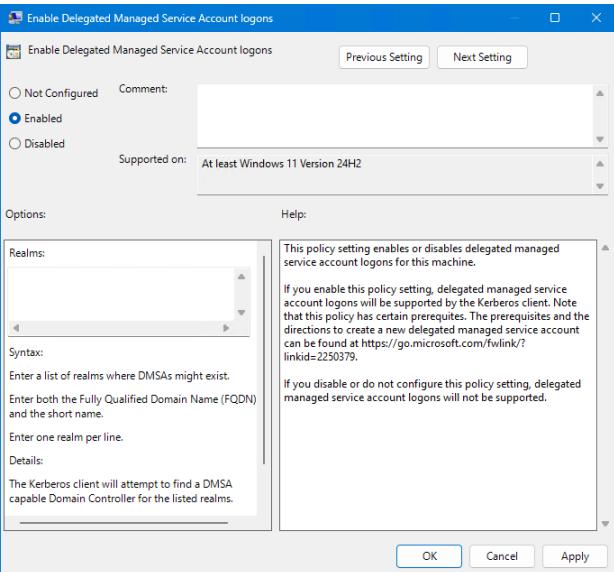
Managed Service Accounts

Delegated (dMSA)

- dMSA = gMSA with more steroids and more requirements! Key differences are:

- Unlike gMSA, with regards to a dMSA:

- 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 
 - MIGRATION dMSA supports ANY (legacy) service account!
- NOTE: dMSA creation and management is to be considered as Tier 0!



- 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) (AT LEAST: how it is intended! ;-))
 - "*msDS-SupersededManagedAccountLink - adminSDHolder DOES NOT follow link!*

Managed Service Accounts

Delegated (dMSA)



- Get relevant data from all dMSAs (Delegated Managed Service Accounts) in AD Domain (<https://gist.github.com/zjorz/62de8c4b5c8d10f7b3c1934c4332dfb8>)

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.TEST\$	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 12:00:00)
CN=dMSA.SQL,OU=...	dMSA.SQL\$	13612	dM...	dMSA.SQL,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 13:00:00)
CN=dMSA.AD LDS...	dMSA.AD LDSmi...	12949	dM...	dMSA.AD LDS...	dMSA F...	True	MigEnd (2)	CN=sVC.AD LDSmi...	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 13:00:00)
CN=dMSA.AD LDS1...	dMSA.AD LDS1\$	12941	dM...	dMSA.AD LDS...	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 13:00:00)
CN=dMSA.AD LDS2...	dMSA.AD LDS2\$	12943	dM...	dMSA.AD LDS...	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 13:00:00)
CN=dMSA.AD LDS...	dMSA.AD LDSmi...	12951	dM...	dMSA.AD LDS...	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 12:00:00)
CN=dMSA.AD LDSn...	dMSA.AD LDSnat...	12945	dM...	dMSA.AD LDS...	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 13:00:00)
CN=dMSA.AD LDSn...	dMSA.AD LDSnat...	12947	dM...	dMSA.AD LDS...	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 13:00:00)
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 12:00:00)
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 12:00:00)

Filter

+ Add criteria ▾

CN=dMSA.TEST	CurKDSRootKeyOrgRWDCDateTime	PrevKDSRootKeyGuid(+KeyCreation)	PrevKDSRootKeyOrgRWDCDateTime	PrincipalsAllowedToRetrieveManagedPassword	CONFIGURED	PrincipalsAllowedToRetrieveManagedPassword	EFFECTIVE	memberOf
DTNCNTR01\ROFSRWDC1 (2025-05-02 23:31:46)				CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST8,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=...	SERVERTEST\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC2 (2025-06-10 12:41:35)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTNCNTR01\ROFSRWDC2 (2025-06-10 12:41:35)		(CN=SERVERTEST2,OU=TEST2,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET, CN=SE...	{SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC2 (2025-06-10 20:00:29)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTNCNTR01\ROFSRWDC2 (2025-06-10 20:00:29)		CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDSmig1,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,...	{SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC1 (2025-06-10 20:01:14)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTNCNTR01\ROFSRWDC1 (2025-06-10 20:01:14)		(CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDS...	{ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500)			
DTNCNTR01\ROFSRWDC2 (2025-06-10 20:14:14)	8f1ff2ec-6515-6624-ea89-44cba14...	DTNCNTR01\ROFSRWDC2 (2025-06-10 20:14:14)		CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDS2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=...	SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC1 (2025-05-15 11:22:20)				CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDSmig2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,...	{SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC1 (2025-06-10 20:09:29)	be3cf336-9db8-ef50-1efd-a28b0ac...	DTNCNTR01\ROFSRWDC1 (2025-06-10 20:09:29)		(CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET, CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDS...	{ADM.TEC (S-1-5-21-274783270-2712129839-3354909249-500)			
DTNCNTR01\ROFSRWDC1 (2025-06-10 20:10:59)	8f1ff2ec-6515-6624-ea89-44cba14...	DTNCNTR01\ROFSRWDC1 (2025-06-10 20:10:59)		CN=grp.gs.Retrieve-Pwd-For-dMSA.AD LDSnat2,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=...	{SERVERTEST2\$ (S-1-5-21-274783270-2712129839-3354909249-000)			
DTNCNTR01\ROFSRWDC1 (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)			
DTNCNTR01\ROFSRWDC1 (2025-05-09 12:55:36)				CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET	SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-000)			[CN=GRP_R0_ALLOWCache]
DTNCNTR01\ROFSRWDC1 (2025-05-02 23:31:40)				CN=grp.gs.Retrieve-Pwd-For-dMSA.TEST8,OU=Groups,OU=Org-ITMgmt,DC=ADTEC,DC=NET	{SERVERTEST3\$ (S-1-5-21-274783270-2712129839-3354909249-000)			[CN=Domain Admins,CN=U]
DTNCNTR01\ROFSRWDC1 (2025-05-02 22:21:41)				CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET	SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-000)			[CN=Domain Admins,CN=U]
DTNCNTR01\ROFSRWDC1 (2025-05-03 23:11:23)				CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET	SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-000)			[CN=Domain Admins,CN=U]
DTNCNTR01\ROFSRWDC1 (2025-05-02 22:21:42)				CN=SERVERTEST1,OU=TEST1,OU=Servers,OU=Org-ITMgmt,DC=ADTEC,DC=NET	SERVERTEST1\$ (S-1-5-21-274783270-2712129839-3354909249-000)			[CN=Domain Admins,CN=U]

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 = [ADSJ]"LDAP://<RWDC FQDN>/RootDSE"
```

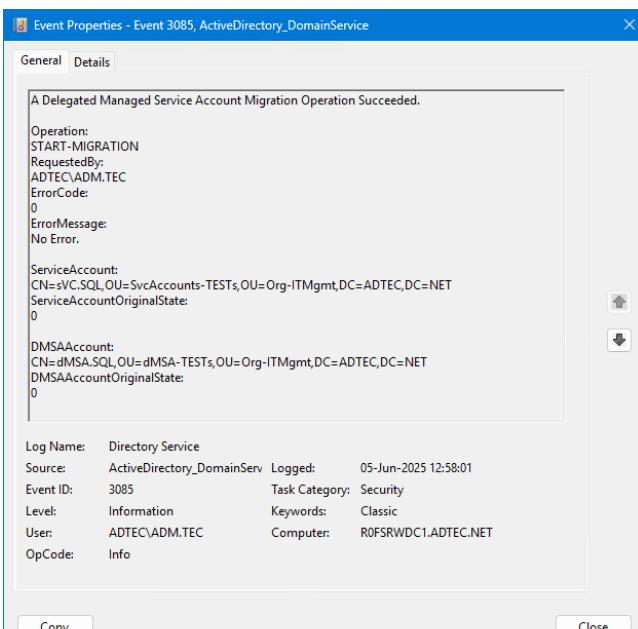
```
$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>:1")
```

```
$rootDSE.SetInfo()
```

```
Administrator: Windows Powershell + ▾

PS C:\> Get-ADUser -Identity "CN=sVC.SQL,OU=SvcAccounts-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET" -Properties "msDS-SupersededServiceAccountState", "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 :
Surname :
UserPrincipalName : sVC.SQL@ADTEC.NET
```

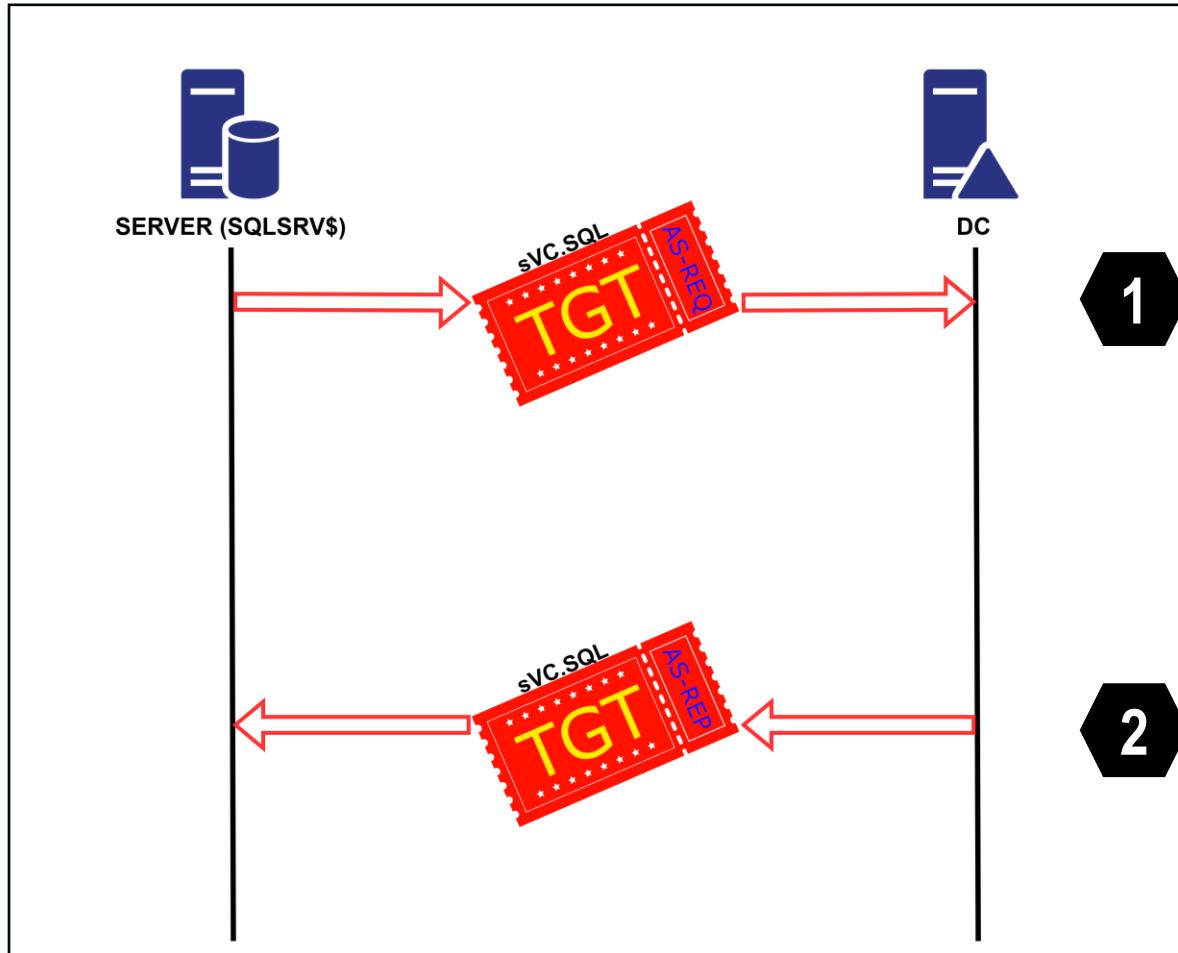


Migrating Service Accounts

Legacy → dMSA (Good Successor!)



Authentication BEFORE Migration State



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



Migrating Service Accounts

Legacy → dMSA (Good Successor!)



Authentication DURING Migration State (either force or take enough time!)

The figure shows a NetworkMiner capture interface with two main panes. The top pane displays Kerberos traffic, specifically a sequence of three messages (114, 117, 125) between source 10.1.4.41 and destination 10.1.4.1. The bottom pane displays LDAP traffic, specifically a sequence of messages (154, 155, 156, 157, 271, 273) between the same hosts. A red box highlights the Kerberos AS-REP message (117). A yellow box highlights the LDAP modifyRequest message (271). The left sidebar shows a detailed tree view of the LDAP message structure, including the GSS-API Generic Security Service Application Program Interface and its sub-components like LDAPPMessage, protocolOp, and modification. The right sidebar provides a hex dump of the modified message, with a yellow box highlighting the msDS-GroupMSAMembership modification. The status bar at the bottom right indicates the message was captured on 05-Jun-2025 13:53:09, category: Directory Service Changes, and user: ROFSRWDC1.ADTEC.NET.

Migrating Service Accounts

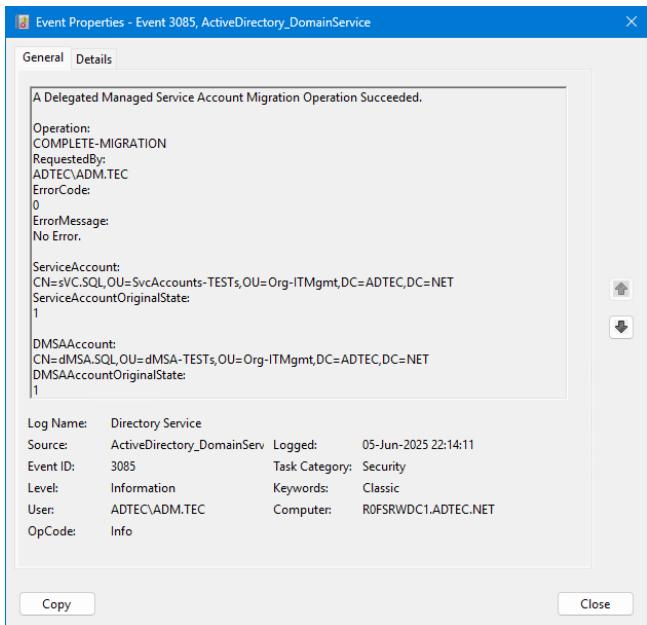
Legacy → dMSA (Good Successor!)



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 = [ADSJ]"LDAP://<RWDC FQDN>/RootDSE"

\$rootDSE.Put("migrateADServiceAccount", "<DN of dMSA>:<DN of Legacy Svc Account>:2")
\$rootDSE.SetInfo()

Allow	ADTEC\pVC.SQL	Write property (msDS-GroupMSAMembership)	Object inherit
Allow	ADTEC\pVC.SQL	Read	

Migrating Service Accounts

Legacy → dMSA (Good Successor!)

```
Administrator: Windows PowerShell -> PS C:\> Get-ADServiceAccount -Identity "dMSA.SQL$" -Properties "msDS-AllowedToActOnBehalfOfOtherIdentity", "msDS-AllowedToDelegateTo", "msDS-AssignedAuthnPolicy", "msDS-DelegatedMSAState", "msDS-ManagedAccountPrecededByLink", PrincipalsAllowedToRetrieveManagedPassword, 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-118b5-9a17-0df3e211a2a8
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.gs.SomeGroupForLegacyServiceAccounts,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

Administrator: Windows PowerShell -> PS C:\> Get-ADUser -Identity "sVC.SQL" -Properties memberOf, "msDS-AllowedToActOnBehalfOfOtherIdentity", "msDS-AllowedToDelegateTo", "msDS-AssignedAuthnPolicy", "msDS-SupersededServiceAccountState", "msDS-SupersededManagedAccountLink", servicePrincipalName, 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=NET}
msDS-SupersededManagedAccountLink : CN=dMSA.SQL,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET
msDS-SupersededServiceAccountState : 2
Name : sVC.SQL

```

During Migration!

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)

Migrating Service Accounts

Legacy → dMSA (Good Successor!)



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

kerberos

No.	Time	Source	Destination	Protocol	Length	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

Name Description

SQL Server (MSSQLSERVER) Provides

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 [...]: fa431b48b41f7d1240dab58fb87b9bf030ecfdc232292995c2371af63d74418e8f3919fe

> Derived strengthen-reply-key keytype 18 (id=304.3) (9f9cfca13...)

> 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 [...]: 3081aaa06330613029a003020112a12204200b4ad6bbe1ec6db

> PA-DATA pa-SUPPORTED-ETYPES

User

IntegratedManagedServiceAccount

Reassembled TCP (2140 bytes) | Krb5 FastRep (232 bytes) | Krb5 Ticket (1151 bytes) | Krb5 KDC-REP (454 bytes)

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

Profile: Default

padata-value (kerberos.padata_value), 173 bytes

semperis

Migrating Service Accounts

Legacy → dMSA (Good Successor!)



WARNING: Some applications/services may still require attention!!! → e.g., ADFS

BEFORE Start

```
Administrator: Windows PowerShell
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636
AuthorizationPolicy
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

AuthorizationPolicyReadOnly
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

PS C:\> |
```

Microsoft.IdentityServer.PolicyModel.Client.StorageAuthorizationException: ADMIN0120: The client is not authorized to access the endpoint net.tcp://localhost:1500/policy. The client process must be run with service administrative privileges.

Log Name: AD FS/Admin
Source: AD FS
Event ID: 102
Level: Error
User: ADTEC\dMSA.ADFS\$
OpCode: Info
Source: AD FS
Event ID: 102
Task Category: None
Keywords: AD FS
Computer: SERVE

AFTER Starting Mig BEFORE Completing

```
Administrator: Windows PowerShell
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636
AuthorizationPolicy
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13636"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

AuthorizationPolicyReadOnly
@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

PS C:\> |
```

AFTER Completing Migration

```
Administrator: Windows PowerShell
AllowedOnBehalfOfCallers SID
S-1-5-21-274783270-2712129839-3354909249-13636
AuthorizationPolicy
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true"); New Service Account

AuthorizationPolicyReadOnly
@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

@RuleName = "Permit Service Account"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid", Value == "S-1-5-21-274783270-2712129839-3354909249-13637"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", value = "true"); New Service Account

@RuleName = "Permit Local Administrators"
exists([Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Value == "S-1-5-32-544"])
=> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value = "true");

PS C:\> |
```

Removing OLD Service Account From AuthZ Rules

<https://github.com/microsoft/adfsToolbox/tree/master/serviceAccountModule>

Remove-AdfsServiceAccountRule -ServiceAccount "<Old Legacy Account>" [-SecondaryServers "<List Of Secondary Servers>"]

Adding NEW Service Account To AuthZ Rules

<https://github.com/microsoft/adfsToolbox/tree/master/serviceAccountModule>

Add-AdfsServiceAccountRule -ServiceAccount "<New dMSA Account>" [-SecondaryServers "<List Of Secondary Servers>"]

User: ADTEC\dMSA.ADFS\$ Computer: SERVERTEST1.ADTEC.NET
OpCode: Info

Migrating Service Accounts

Legacy → dMSA (*Bad Successor!*)



- **Bad Successor** = **WITHOUT PATCH** Aug 12, 2025 - KB5063878 - W2K25 DCs
 - Merging PAC (= Privilege Attribute Certificate) and getting hashes/keys of supported encryption types from targeted account, under the following minimal conditions
 - dMSA attribute "msDS-DelegatedMSAState" = 2
 - dMSA attribute "msDS-ManagedAccountPrecededByLink" = "<DN of some account, user/computer/sMSA/gMSA/dMSA>" (anything that can authenticate!)
Major Problem → Accounts with well-known DNs (default domain admin + KRBTGT)
 - Listed attributes ARE NOT protected from regular LDAP writes!
 - Wow! That's a LOT of EASY power! What could go wrong? 😱

Migrating Service Accounts

Legacy → dMSA (*Bad Successor!*)



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

[Bad-Successor-WRITE-DATA-v2.ps1](#)

[Bad-Successor-VIEW-DATA-v2.ps1](#)

```
# WRITE DATA INTO ATTRIBUTES "msDS-groupMSAMembership", "msDS-DelegatedMSAState", "msDS-ManagedAccountPrecededByLink" OF THE dMSA
$dMSADN = "CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET"
$objectState = 2
$accDN = "CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET" # = Renamed Default Domain Admin
$accAllowGetPwd = "ADTEC\bad.act0r"
$badSuccessorPatchInstalled = $false
```

```
Windows PowerShell

+++ dMSA ***
> Updating dMSA Object 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET' ...
# Attribute.....: 'msDS-DelegatedMSAState'
* Value.....: '2'

# Attribute.....: 'msDS-groupMSAMembership'
* Value.....: 'ADTEC\bad.act0r'

# Attribute.....: 'msDS-ManagedAccountPrecededByLink'
* Value (ADD).....: 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'

- SUCCESS

PS C:\Users\bad.act0r> | Renamed Default Domain Administrator (RID 500)
```

Migrating Service Accounts

*Legacy → dMSA (**Bad Successor!**)*



J the
MSA

```
1127) "<ROOT>" sasl  
21127) success
```

```
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ID: 512  
ttributes: 0x00000007  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ID: 518  
ttributes: 0x00000007  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ID: 519  
ttributes: 0x00000007  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ERSHIP:  
ID: 500  
ttributes: 0x00000007  
x00000020  
Key: 00000000000000000000000000000001  
WDC1
```

Migrating Service Accounts

Legacy → dMSA (*Patched Successor!*)



- **Patched Successor** = **WITH PATCH** Aug12, 2025 - KB5063878 - W2K25 DCs
 - Merging PAC (= Privilege Attribute Certificate) and getting hashes/keys of supported encryption types from targeted account, under the following minimal conditions
 - dMSA attribute "msDS-DelegatedMSAState" = 2
 - dMSA attribute "msDS-ManagedAccountPrecededByLink" = "<DN of some account, user/computer/sMSA/gMSA/dMSA>" (anything that can authenticate, except dMSAs!)
 - (legacy service) account attribute "msDS-SupersededServiceAccountState" = 2
 - (legacy service) account attribute "msDS-SupersededManagedAccountLink" = <DN of dMSA referencing the (legacy service) account>
 - Listed attributes ARE STILL NOT protected from regular LDAP writes!
 - In addition to controlling dMSA, control is also needed on target/referenced account!
 - Protected Accounts (secured by adminSDHolder) are now exempt from this attack.
But... what about over-permissioned non-protected accounts as the backdoor?

Migrating Service Accounts

Legacy → dMSA (*Patched Successor!*)



- Therefore, anyone controlling ANY Account + dMSA through:
 - Create Child (Specific to dMSA or generic)
 - Full Control (e.g., Account Operators)
 - Write DACL
 - Write Owner
 - Write Property
- Attack technique still valid!

[Bad-Successor-WRITE-DATA-v2.ps1](#)

[Bad-Successor-VIEW-DATA-v2.ps1](#)

```
# WRITE DATA INTO ATTRIBUTES "msDS-groupMSAMembership", "msDS-DelegatedMSAState", "msDS-ManagedAccountPrecededByLink" OF THE dMSA
# WRITE DATA INTO ATTRIBUTES "msDS-SupersededServiceAccountState", "msDS-SupersededManagedAccountLink" OF THE (LEGACY SERVICE) ACCOUNT
$dMSADN = "CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET"
$objectState = 2
$accDN = "CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET" # = Renamed Default Domain Admin
$accAllowGetPwd = "ADTEC\bad.act0r"
$badSuccessorPatchInstalled = $true
```

The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". It displays two sets of command-line output:

dMSA Patching Output:

```
+++ dMSA ***
> Updating dMSA Object 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'...
# Attribute.....: 'msDS-DelegatedMSAState'
* Value.....: '2'

# Attribute.....: 'msDS-groupMSAMembership'
* Value.....: 'ADTEC\bad.act0r'

# Attribute.....: 'msDS-ManagedAccountPrecededByLink'
* Value (ADD)....: 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'
- SUCCESS
Renamed Default Domain Administrator (RID 500)
```

Legacy Service Account Update Output:

```
+++ ACCOUNT ***
> Updating Account Object 'CN=ADM TEC,CN=Users,DC=ADTEC,DC=NET'...
# Attribute.....: 'msDS-SupersededManagedAccountLink'
* Value (ADD)....: 'CN=dMSA.weak,OU=dMSA-TESTs,OU=Org-ITMgmt,DC=ADTEC,DC=NET'

# Attribute.....: 'msDS-SupersededServiceAccountState'
* Value.....: '2'

- SUCCESS
```

PS C:\>

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
 - Applicable For BadSuccessor → Event ID 5136 - writes to "*msDS-DelegatedMSAState*" with value of "2" (not coming from 1) in combination with writes to "*msDS-ManagedAccountPrecededByLink*" on dMSA object (+not being DN of disabled user object), while also NOT writing anything to "*msDS-SupersededServiceAccountState*" and to "*msDS-SupersededManagedServiceAccountLink*" on the referenced account

Migrating Service Accounts

Legacy → dMSA (*Protections!*)



- Auditing (Continued)
 - Applicable For PatchedSuccessor → Event ID 5136 - writes to "msDS-DelegatedMSAState" with value of "2" (not coming from 1) in combination with writes to "msDS-ManagedAccountPrecededByLink" on dMSA object (+not being DN of disabled user object), while also writing "2" (not coming from 1) to "msDS-SupersededServiceAccountState" and to "msDS-SupersededManagedServiceAccountLink" on the referenced account
 - Event ID 2946 - Audit fetching passwords of dMSAs (unusual)
 - Event ID 4768 - Audit Success Of Kerberos Tickets Operations (*TGT Request by Account*) followed by Event ID 4769 - Audit Failure Of Kerberos Tickets Operations (*TGS Request by same Account*)
(When patched IS installed and BadSuccessor method, 2 attributes only, is used)

Migrating Service Accounts

Legacy → dMSA (Protections!)



From a non-High-Privileged Account perspective

model before intro of W2K25 DCs and enhance security

From a High-Privileged Account perspective

Y“

Left Window (Non-High-Privileged Account Perspective):

- Shows Active Directory Users and Computers interface.
- Focuses on the "Users" container under "ADTEC.NET".
- Red boxes highlight several accounts: ADM.IORG, ADM.TEC, krbtgt, and krbtgt_10503.
- Bottom pane shows the full path: OU=dMSA-TESTS,OU=Org-ITMgmt,DC=ADTEC,DC=NET.

Middle Window (Non-High-Privileged Account Perspective):

- Shows Active Directory Users and Computers interface.
- Focuses on the "Users" container under "ADTEC.NET".
- Red boxes highlight several accounts: ADM.TEC and AdminTiering.
- Bottom pane shows the full path: ADTEC.NET/Org-ITMgmt/dMSA-TESTS.

Right Window (High-Privileged Account Perspective):

- Shows Active Directory Users and Computers interface.
- Focuses on the "AdminTiering" container under "Users" in "ADTEC.NET".
- Red boxes highlight the "Tier0", "Tier1", and "Tier2" sub-containers.
- Bottom pane shows the full path: ADTEC.NET/Org-ITMgmt/dMSA-TESTS/AdminTiering/Tier0.

Bottom Table:

Object Type	Object Name	Delegation Type	Description	Attributes
organizationalUnit	ADTEC\BdActrADTEC3	GenericAll	All Descendant msDS-DelegatedMan...	All Attributes
organizationalUnit	ADTEC\BdActrADTEC10	WriteDacl	This Object Only	Not Applicable
organizationalUnit	ADTEC\BdActrADTEC11	WriteDacl	This Object And All Descendant Objects	Not Applicable
organizationalUnit	ADTEC\BdActrADTEC12	WriteDacl	All Descendant Objects	Not Applicable
organizationalUnit	ADTEC\BdActrADTEC2	GenericAll	All Descendant Objects	All Attributes
organizationalUnit	ADTEC\BdActrADTEC60	Owner Of...	Not Applicable	Not Applicable
organizationalUnit	ADTEC\BdActrADTEC0	GenericAll	This Object Only	All Attributes
organizationalUnit	ADTEC\BdActrADTEC1	GenericAll	This Object And All Descendant Objects	All Attributes
organizationalUnit	ADTEC\BdActrADTEC40	CreateChild	This Object Only (All Object Types)	All Attributes

Migrating Service Accounts

Legacy → dMSA (The Ultimate Block!)

- Block writing values into
 - “*msDS-ManagedAccountPrecededByLink*”
 - “*msDS-SupersededManagedServiceAccountLink*”
- Impacts regular LDAP writes & unfortunately also writes through PoSH CMDlets

ldap://R0FSRWDC1.ADTEC.DC=ADTEC,DC=NET

Link Attribute on a dMSA

Connection Browse View Options Utilities Help

Expanding base 'CN=ms-DS-Managed-Account-Preceded-By-Link' Getting 1 entries:

```
Dn: CN=ms-DS-Managed-Account-Preceded-By-Link,CN=Schema,CN=Configuration,DC=ADTEC,DC=N
adminDescription: This attribute is the forward link from a service account to a delegated managed service account object.; adminDisplayName: ms-DS-Managed-Account-Preceded-By-Link; attributeID: 1.2.840.113556.1.4.2375; attributeSyntax: 2.5.5.1 = ( DISTNAME ); cn: ms-DS-Managed-Account-Preceded-By-Link; distinguishedName: CN=ms-DS-Managed-Account-Preceded-By-Link; dSCorePropagationData: 0x0 = ( ); instanceType: 0x4 = ( WRITE ); isSingleValued: TRUE; IDAPDisplayName: msDS-ManagedAccountPrecededByLink; linkID: 2224; name: ms-DS-Managed-Account-Preceded-By-Link; objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=ADTEC,DC=N; objectClass (2): top; attributeSchema; objectGUID: a76328ae-ca34-47ec-aea8-0b3a1844de7a; oMObjectClass: \x2b0c0287731c00854a; oMSyntax: 127 = ( OBJECT ); schemaIDGUID: a0945b2b-57a2-43bd-b327-4d112a4e8b; searchFlags: 0x0 = ( ); showInAdvancedViewOnly: TRUE; systemOnly: FALSE; uSNChanged: 177359; uSNCreated: 9220; whenChanged: 02-Sep-2025 15:12:49 W. Europe Daylight Time; whenCreated: 17-Apr-2025 13:41:25 W. Europe Daylight Time;
```

ldap://R0FSRWDC1.ADTEC.DC=ADTEC,DC=NET

Link Attribute on any account

Connection Browse View Options Utilities Help

Expanding base 'CN=ms-DS-Superseded-Managed-Account-Link,CN=Schema,CN=Configuration,DC=ADTEC,DC=N' Getting 1 entries:

```
Dn: CN=ms-DS-Superseded-Managed-Account-Link,CN=Schema,CN=Configuration,DC=ADTEC,DC=N
adminDescription: This attribute is the forward link from a service account to a delegated managed service account object.; adminDisplayName: ms-DS-Superseded-Managed-Account-Link; attributeID: 1.2.840.113556.1.4.2373; attributeSyntax: 2.5.5.1 = ( DISTNAME ); cn: ms-DS-Superseded-Managed-Account-Link; distinguishedName: CN=ms-DS-Superseded-Managed-Account-Link,CN=Schema,CN=Configuration,DC=ADTEC,DC=N; dSCorePropagationData: 0x0 = ( ); instanceType: 0x4 = ( WRITE ); isSingleValued: TRUE; IDAPDisplayName: msDS-SupersededManagedAccountLink; linkID: 2222; name: ms-DS-Superseded-Managed-Account-Link; objectCategory: CN=Attribute-Schema,CN=Schema,CN=Configuration,DC=ADTEC,DC=N; objectClass (2): top; attributeSchema; objectGUID: c089c6fd-4eb1-4571-8bc9-75711c9084ac; oMObjectClass: \x2b0c0287731c00854a; oMSyntax: 127 = ( OBJECT ); schemaIDGUID: 3752e002-43be-48c8-b3ca-2cb2fffb08a1; searchFlags: 0x0 = ( ); showInAdvancedViewOnly: TRUE; systemOnly: FALSE; uSNChanged: 177359; uSNCreated: 9218; whenChanged: 02-Sep-2025 15:12:49 W. Europe Daylight Time; whenCreated: 17-Apr-2025 13:41:24 W. Europe Daylight Time;
```

Migrating Service Accounts

Legacy → dMSA (*More 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](#)
 - [\(2025-07-11\) How to Block BadSuccessor: The Good, Bad, and Ugly of dMSA Migration](#)
 - [\(2025-09-02\) From BadSuccessor To PatchedSuccessor](#)



Auditing KDS Root Key Access

Detecting Golden gMSA/dMSA Attacks

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

<https://www.semneris.com/blog/golden-msa-attack/>



Event 4662, Microsoft Windows security auditing.

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-ae62-4fe39fadfb9e)
(db2c48b2-d14d-ec4e-9f58-ad579d8b440e)
(8a800772-f4b3-154f-b41c-2e4271eff7a7)
(1702975d-225e-cb4a-b15d-0daea8b5e990)
(30b099d9-edfe-7549-b807-eba444da79e9)
(e338f470-39cd-4549-ab5b-f69f9e583fe0)
(615fa2a1-37e7-1148-a0dd-3007e09fcf81)
(26627c27-08a2-0a40-a1b1-8dcce85b42993) <- msKds-RootKeyData
(d5f07340-e6b0-1e4a-97be-0d3318bd9ab1)
(96400482-cf07-e94c-90e8-f2efc4f0495e)
(6cdc047f-f522-b74a-9a9c-d95ac8cdfda2)

Log Name: Security
Source: Microsoft Windows security
Event ID: 4662
Level: Information
User: N/A
OpCode: Info

Task Category: Directory Service Access
Keywords: Audit Success

Computer: R0FSRWDC1.ADTEC.NET

For Each KDS Root Key

Copy Close

Event Properties - Event 4662, Microsoft Windows security auditing.

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-ae62-4fe39fadfb9e)
(26627c27-08a2-0a40-a1b1-8dcce85b42993) <- msKds-RootKeyData
(aa02fd41-17e0-4f18-8687-b2239649736b)

Additional Information: Parameter 1: -
Parameter 2: -

Log Name: Security
Source: Microsoft Windows security
Event ID: 4662
Level: Information
User: N/A
OpCode: Info

Task Category: Directory Service Access
Keywords: Audit Success

Computer: R0FSRWDC1.ADTEC.NET

For Each KDS Root Key

Copy Update Close

Event Properties - Event 4662, Microsoft Windows security auditing.

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-ae62-4fe39fadfb9e)
(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
Event ID: 4662
Level: Information
User: N/A
OpCode: Info

Task Category: Directory Service Access
Keywords: Audit Success

Computer: R0FSRWDC1.ADTEC.NET

For Each KDS Root Key

Copy Close

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

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!



<https://jorgequestforknowledge.wordpress.com/2025/06/27/well-known-containers-in-an-ad-domain-how-to-restore-and-or-repair-as-needed/>

Managed Service Accounts Properties

General Object Security Attribute Editor

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

OK Cancel Apply Help

Managed Service Accounts Properties

General Object Security Attribute Editor

Attributes:

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

View Filter

OK Cancel Apply Help

Active Directory Administrative Center

ADTEC (local) > Deleted Objects

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 ...

Managed Service Accounts

Object class: Container Modified: 27-May-2025 9:12 PM

Description: Default container for managed service accounts

Tasks

- Managed Service Accounts
- Restore
- Restore To...
- Locate Parent
- Properties

Deleted Objects

- New
- Delete
- Search under this node
- Properties

WINDOWS POWERSHELL HISTORY

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

Policy Usage Resultant Policy

Display users and computers that meet the following criteria:

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

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 Object Types...

From this location:

ADTEC.NET Locations...

Enter the object names to select (examples):

Check Names

Advanced... OK Cancel

Object Types

Select the types of objects you want to find.

Object types

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>

- The Secure Way:
 - Remove account from “Allowed To Cache” list
 - Reset the password of the account (or wait in case of gMSA/dMSA)
- The Less Impactful Way (Also Less Secure):
 - Use PowerShell and the operational attribute “rODCPurgeAccount” against the RODC

Advanced Password Replication Policy for R0FSRODC1					
Policy Usage		Resultant Policy			
Display users and computers that meet the following criteria:					
Accounts whose passwords are stored on this Read-only Domain Controller					X
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	
gMSA RODC	ADTEC.NET/Org-ITM...	msDS-Gr...	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	

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>



ANY
QUESTIONS?
?

Please Fill In Feedback Form

Session feedback
available in home feed
of the app after the
session



THANK YOU!



MC2MC
—CONNECT—

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

