## Inhalt

WS IT-Solutions

1.	Automation durch Benutzer mit statischen Kennwörtern	1
	Scheduled-Tasks	1
	Services	2
	Wo ist das Problem?	3
2.	Was sind gMSA?	4
	Definition	4
	Wie funktioniert ein gMSA?	4
3.	Administration mit gMSA-Accounts ohne mein Script	5
	Einrichtung eines gMSA	5
	Konfiguration eines Services mit gMSA	6
	Konfiguration eines Scheduled-Tasks mit gMSA	7
	Das Problem	8
4.	Einsatz des gMSA-Admin-Scriptes	10
	Die Lösung	10
	Einrichtung eines gMSA mit Vorbereitung der Domäne	11
	Konfiguration eines Scheduled-Tasks mit gMSA	13
	Konfiguration eines Services mit gMSA	14
	Konfiguration von Berechtigungen eines gMSA	15
	Der aMSA benötiat höhere Rechte? Kein Problem:	15
	Zusammenfassung	15

# 1. Automation durch Benutzer mit statischen Kennwörtern

## **Scheduled-Tasks**

Um wiederkehrende Aufgaben zu automatisieren bieten sich geplante Aufgaben an. Diese müssen in einem Sicherheitskontext ausgeführt werden. Für viele Aufgaben genügt der lokale Systemkontext. Aber wenn eine Aufgabe rechnerübergreifend arbeiten muss oder auf bestimmte Services zugreifen soll, dann muss ein Benutzeraccount verwendet werden. Dieser wird dann etwa so aussehen:



Active Directory Users and Com	puters					_
File Action View Help	i 🛯 🔒 🔽 🗖	1 % 🗽 🎦 🔻 🛛	2 🗽			
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Adatum.com</li> <li>AdminArea</li> </ul>	Name Service-admint service-user	ask service-admintask Pr	Type User User		Description	7 ×
Builtin     Gomputers     Tovelopment     S     Dovelopment     S     Domain Controllers     S     ForeignSecurityPrincipal-		Member Of Remote control General Address	Dial-in Remote Account	Env Desktop Se Profile	ironment ervices Profile Telephones	Sessions COM+ Organization
<ul> <li>G IT</li> <li>Managed Service Accour</li> <li>Managers</li> <li>Marketing</li> <li>Research</li> <li>Sales</li> <li>Users</li> </ul>		User logon name: service-admintask User logon name (pre ADATUM\ Logon Hours	-Windows 200 Log On 1	@Adatu 00): service- 10	um.com admintask	~
		Unlock account				
		User must chan User annot ch Password never	nge password hange passwor er expires d using reversit	at next logo d	n	<b>^</b>
< >>		Account expires Never End of:	Tuesday ,	December	5, 2017	

In der Aufgabenplanung wird der Benutzer dann mit seinem Passwort hinterlegt:

🕑 Task Scheduler							-	
File Action View Help								
🗢 🄿 🙍 🖬 🖬								
🕑 Task Scheduler (Local)	Name	Status	Triggers	Next Run Time	Last Run Tin	Act	ions	
> 🔀 Task Scheduler Library	AdminTask	Ready	At system startup		11/30/1999	Tas	k Scheduler Library	
	CreateExplorerSh	Running	When the task is created or modified		10/23/2017	1	Create Basic Task	
						•	Create Task	
							Import Task	
							Display All Running Tasks	
	<				>		Disable All Tasks History	
	General Triggers Ac	tions Co	aditions Settings History			1	New Folder	
	Name Admin		View					
	Name: Aumin	lask				Q	Refresh	
	Location:					?	Help	
	Author: ADATUM\Administrator						Selected Item	
	Description:					•	Run	
						10	End	
						+	Disable	
							Export	
	Security options					e	Properties	
	When running the t	ask, use the	following user account:			×	Delete	
	service-admintask					?	Help	
	Run only when user is logged on					1		
	😑 Run whether use	r is logged	on or not					
	Do not store	password.	The task will only have access to local	resources		L		
	🖉 Run with highest	t privileges						
	Hidden Co	onfigure fo	r: Windows Vista <sup>ms</sup> , Windows Server <sup>ms</sup>	2008				

Das Kennwort darf nicht einfach ablaufen und ungültig werden, da eine geplante Aufgabe sonst nicht mehr ausgeführt wird...

#### **Services**

Mit Diensten ist es meist genauso. Wenn ein Benutzerkontext der Domäne benötigt wird, findet man eben solche Benutzer im AD:



Active Directory Users and Com	puters					- 0	×
File Action View Help							
		a   42 🐁 🏎 📼 🖂	1 6.				
		💩 🚳 💷 🦷 🖉					
Active Directory Users and Com	Name		Type		Description		
> Caved Queries	🕹 service-admint	ask	User				
<ul> <li>Adatum.com</li> <li>Admin0.com</li> </ul>	🕹 service-user		User				
Builtin		service-user Propertie	s			? >	<
> Computers							
> 💼 Development		Member Of	Dial-in	Envi	ironment	Sessions	_
> 🛅 Domain Controllers		General Address	Account	Profile	Telephones	Organization	n .
> ForeignSecurityPrincipal:		General Address	1 IOODUIN	TIONE	relephones	organizatio	·
> 🛅 IT		User logon name:					
Managed Service Accourt Managerr		service-user		@Adatu	um.com	~	
Marketing		User logon name (pre	Windows 200	0):			
> 🖬 Research		ADATUM\		service	user		
> 📓 Sales							
> 🧮 Users		Logon Hours	Log On T	0			
		_					
		Unlock account					
		Assessment antisensu					
		Account options.					
		User must chan	ige password a	at next logo	n	î	
		Password neve	ange passwor r evpires	a			
		Store password	usina reversih	le encryptic	n		
						4	
4		Account expires					
		Never					
		O End of:	Tuesday , [	December	5, 2017		

Und in der Dienstekonsole wird dieser Benutzer dann hinterlegt:

🍓 Services								
File Action View	Help							
(+ +) 📰 🔯	2 🕞 🛛 📷 🕨 🔲 II 🕪							
🔍 Services (Local)	Services (Local)							
	Storage Tiers Management	Name	Description Status Startup Type	Log On As				
	Start the service	System Events Broker System Event Notification S Sync Host 45bf5	Coordinates Running Automatic (T Monitors sy Running Automatic This service Running Automatic (D	Local System Local System Local System				
	Description: Optimizes the placement of data in storage tiers on all tiered storage spaces in the system.	Superfetch Storage Tiers Management	Maintains a Manual Optimizes t Manual Provides en Running Manual (Trig	Local System Local System Local System				
	spaces in the system.	Image Acquisition Events         State Repository Service         SSDP Discovery         Spot Verifier         Special Administration Con	Storage Tiers Management Properties (Local Computer) General Log On Recovery Dependencies Log on as:					
		🥨 Software Protection 🍓 SNMP Trap 🧠 Smart Card Removal Policy	Allow service to interact with deskto     This account: service-user@Ac	P datum.com Browse				
		<ul> <li>Smart Card Device Enumera</li> <li>Smart Card</li> <li>Smart Card</li> </ul>	Password:					
		Server Sensor Service Sensor Monitoring Service Sensor Data Service	s Confirm password:	]				

Kommt euch das etwa bekannt vor?

#### Wo ist das Problem?

Es liegt auf der Hand: ein Benutzer im AD mit statischem Kennwort (der zumeist auch nicht überprüft wird) ist für Angreifer eine lohnende Beute. Kapert er einmal dessen Anmeldeinformationen, dann kann er sie nahezu endlos verwenden.

Für jeden anderen Benutzer im AD würde eine Kennwortrichtlinie vorschreiben, dass dessen Kennwort regelmäßig geändert wird. Nur wie will man das mit den vielen Service-Usern unternehmensweit vornehmen? Meist weiß nach Monaten niemand mehr, wo der Useraccount eingesetzt wird.

Ebenso habe ich auch schon oft (genug) verwaiste Service-User gefunden, die nirgends mehr eingesetzt wurden. Dennoch traute sich niemand, den Service-User zu löschen. Wer weiß schon, ob er nicht doch noch eingesetzt wird??

Und wenn dann die Benutzerkonten noch erhöhte Rechte haben, dann ist das Durchfallen beim nächstem Pentest fast garantiert:





# 2. Was sind gMSA?

### **Definition**

Group Managed Service Accounts – kurz gMSA – sind die Lösung für diese Probleme. Es sind Benutzerkonten-ähnliche Objekte im Active Directory, die durch Gruppenmitgliedschaften berechtigt werden können. Deren Kennwort wird aber regelmäßig geändert!

Dafür braucht ihr "nur" ein AD mit der Funktionsebene WindowsServer2012 (ohne R2 genügt). Den Vorgänger "Managed Service Account" beleuchte ich hier nicht, denn das war leider nix…

### Wie funktioniert ein gMSA?

Es sind folgende Arbeitsschritte notwendig:

- 1. Das AD muss einmalig vorbereitet werden. Neben der richtigen Domänen-Funktionsebene ist ein KDS-RootKey erforderlich. Dieser wird von den DCs benötigt, um die Kennworte zu generieren und zu schützen. Dazu gleich mehr!
- 2. Dann kann der erste gMSA erstellt werden. Leider gibt es auch mit Windows Server 2016 keine Möglichkeit, dies über die grafische Oberfläche zu erledigen. Es bleibt nur die PowerShell. Beim Erstellen des gMSA wird angegeben, welche Domänen-Computer den Account verwenden dürfen.
- 3. Auch Gruppenmitgliedschaften können über die PowerShell konfiguriert werden.
- 4. Zuletzt wird der Account als Service-User oder als Task-User auf den Zielservern eingesetzt.

Doch wie funktioniert nun der Kennwortaustausch?

- 1. Beim Erstellen eines gMSA vergibt der DC ein komplexes Kennwort.
- 2. Wird ein gMSA auf einem Server eingesetzt, der berechtigt ist, diesen gMSA zu verwenden, dann erfragt der Server über den SecureChannel beim DC das aktuelle Kennwort und speichert es.
- 3. Der DC überwacht das Kennwortalter aller gMSA. Läuft von einem gMSA das Kennwort aus, dann wird der DC dieses ändern.
- 4. Verliert danach auf einem Server das TGT (Ticket Granting Ticket) des eingesetzten gMSA seine Gültigkeit, dann wird der Server dessen Anmeldung erneuern. Dabei kontaktiert er den DC über den SecureChannel und erfährt das neue Kennwort.

So einfach ist die Idee. 🕹

Ein gMSA kann von einem oder von mehreren AD-Computern verwendet werden. Ebenso kann ein AD-Computer einen oder mehrere gMSA verwenden.

# 3. Administration mit gMSA-Accounts ohne mein Script

## Einrichtung eines gMSA

**VS IT-Solutions** 

Zunächst muss das AD vorbereitet werden:

Active Directory Users and Comp	outers		- 0
File Action View Help			
🗢 🏟  📅 🛅 📋 🖾 🖻	) 🛛 🗊 🗏 🐮 🛅 🍸 💆 🐍		
<ul> <li>Active Directory Users and Com</li> <li>Saved Queries</li> <li>Adatum.com</li> <li>AdminArea</li> <li>Builtin</li> <li>Computers</li> <li>Development</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>IT</li> <li>Managed Service Accour</li> <li>Marketing</li> <li>Research</li> <li>Sales</li> <li>Users</li> </ul>	Name Name AdminArea Builtin Computers Computers Development Raise domain functional level Current domain functional levet: Current domain functional levet: Vindows Server 2012 R2 Select an available domain functional lev Windows Server 2016	Type Organizational builtinDomain Container Organizational	Description Default container for up.
> 🎦 Users	After you raise the domain functiona reverse it. For more information on c	al level, it is possible that you domain functional levels, clic	u may not be able to k Help.

Es wird ein KDS-RootKey benötigt. Dieser kann mit der PowerShell erstellt und geprüft werden. Ist kein Key vorhanden, dann bleibt die PS-Ausgabe leer:



Einen neuen Key kann man in LAB-Umgebungen von seiner Gültigkeit her zurückdatieren. In Produktionsumgebungen würde ich den Parameter EffectiveImmediately empfehlen und abwarten, bis der Key repliziert wurde:



Ist das AD bereit, dann kann man den ersten gMSA erstellen. Dabei muss neben dessen Namen auch mindestens ein Server angegeben werden, der das Kennwort abfragen darf:

```
$Domain = (Get-ADDomain).dnsroot
1
2
    $gMSA
               gMSA-Tasks
3
   $MemberServer = 'LON-DC1', 'LON-SVR4' | Get-ADComputer
4
5
    New-ADServiceAccount
        -Name $gMSA
6
        -DNSHOSTNAME "$gMSA.$Domain"
7
        -PrincipalsAllowedToRetrieveManagedPassword $MemberServer
8
```

In Zeile 1 frage ich die aktuelle Domain ab. Zeile 2 speichert den Namen des neuen Accounts. Zeile 4 ermittelt die Computerkonten von 2 Servern. Und Zeile 5++ erstellt den gMSA. Hier sieht man das Ergebnis in dsa.msc:

WS IT-Solutions

# WSHowTo – Group Managed Service Accounts mit gMSA-Admin 2017-11-06 Windows Server 2012,2012R2,2016

Active Directory-Benutzer und -Co	omputer		
Datei Aktion Ansicht ?			
🗢 🔿 🖄 📊 🔏 📋  🎇	1 🖬 🚺 📾	🕹 🗽 🛅 🍸 🗾 🍇	
<ul> <li>Active Directory-Benutzer und -</li> <li>Gespeicherte Abfragen</li> <li>Adatum.com</li> <li>Builtin</li> <li>Computers</li> <li>Development</li> <li>Domain Controllers</li> <li>ForeignSecurityPrincipal:</li> <li>IT</li> <li>Keys</li> <li>LostAndFound</li> <li>Kanaged Service Accour</li> <li>gMSA-Tasks</li> <li>Managers</li> <li>Marketing</li> <li>Program Data</li> <li>Sales</li> <li>System</li> <li>Users</li> <li>NTDS Quotas</li> <li>TDM Devices</li> </ul>	Name Rigenschafter Allgemein O Attribut accountNa aCSPolicyl adminDesc adminDisp altSecurity assistant attributec audio badPassw badPwdCc	Image: Second	Beschreibung erviceA
	c <	<nicht festgelegt=""> <nicht festgelegt=""></nicht></nicht>	>
	Bearbeite	n	Filter
	[	OK Abbrechen	Dbernehmen Hilfe

Jede Änderung wird über die PowerShell vorgenommen: in der MMC gibt es dafür keine Funktionen... Selbst der Attributeditor ist nur bedingt hilfreich.

## Konfiguration eines Services mit gMSA

Wie bekomme ich nun den Account als Service-User eingetragen? In der klassischen Services.msc gibt es die Option "Anmelden":



Das Kennwort ist nicht bekannt, denn das wird ja vom KDC verwaltet. Der Trick in der MMC besteht darin, das Kennwortfeld leer zu lassen. Eine Erweiterung der Berechtigung später ist der Account bereit:

WS IT-Solutions

# WSHowTo – Group Managed Service Accounts mit gMSA-Admin 2017-11-06 Windows Server 2012,2012R2,2016

		Dienste	×				
		Dem Konto ADATUM\gMSA-Tasks\$ wurde die Berei Anmelden als Dienst zugewiesen.	chtigung zum				
			ОК				
🤹 Dienste	iek+ 2					-	
	) 🕞 🔽 🥽 🕨 🖬 🖬 🖬						
🤐 Dienste (Lokal)	O Dienste (Lokal)						
	Storage Tiers Management	Name	Beschreibung	Status	Starttyp	Anmelden als	
	Den Dienst <u>starten</u>	Sicherheitskonto-Manager Smartcard	Durch den Sta… Verwaltet den …	Wird au	Automa Deaktivi	Lokales System Lokaler Dienst	
	Beschreibung:	Smartcard-Geräteaufzählungsdienst SMMP-Trap	Erstellt Softwa Empfängt Tra	Wird au	Manuell Manuell	Lokales System Lokaler Dienst	
	den Speicherstufen in allen	Software Protection	Aktiviert das	Wird au	Automa	Netzwerkdienst	
	mehrstufigen Speicherplätzen im	Speicherdienst	Stellt Unterstü	Wird au	Manuell	Lokales System	
	System.	SSDP-Suche	Sucht nach N		Deaktivi	Lokaler Dienst	
		Standardsammlungsdienst des Microsoft/R)-	Standardsam		Manuell	Lokales System	
		Standortübergreifender Messagingdienst	Ermöalicht de…	Wird au	Automa	Lokales System	
		StateRepository-Dienst	Bietet die erfo	Wird au	Manuell	Lokales System	
		🏟 Storage Tiers Management	Optimiert die		Manuell	ADATUM\gMSA-Tasks	\$
		🏟 Stromversorgung	Verwaltet die E	Wird au	Automa	Lokales System	
		🆏 Superfetch	Verwaltet und		Manuell	Lokales System	
		🆏 Synchronisierungshost_48a9d	Dieser Dienst s	Wird au	Automa	Lokales System	
		🆏 Systemereignissebroker	Koordiniert di	Wird au	Automa	Lokales System	
		🖾 TCP/IP-NetBIOS-Hilfsdienst	Bietet Unterst	Wird au	Manuell	Lokaler Dienst	

### Konfiguration eines Scheduled-Tasks mit gMSA

Diese Änderung ist deutlich schwerer, denn die MMC findet den Benutzeraccount nicht:

🕑 Aufgabenplanung			
Datei Aktion Ansicht ?			
🗢 🔿 🙋 📰 🚺			
Aufgabenplanung (Lokal)	Narr	Bigenschaften von AdminTask (Lokaler Computer)	× Ergebni
	<u>е</u> А С	Benutzer, Dienstkonto oder Gruppe auswählen X	Die Auf Die Auf
		Objekttyp:	
		Benutzer, Dienstkonto, Gruppe oder Integriertes Sicherheitsprinzipal Objekttypen	
	<	Suchpfad:	
	Allg	Gesamtes Verzeichnis Pfade	
	Na	<u>G</u> eben Sie die zu verwendenden Objektnamen ein ( <u>Beispiele</u> ):	
	Sne	gMSA-Tasks Namen überprüfen	
	Aut		
	Bes	Benutzer, Dienstkonto oder Gruppe auswanien	
		Ein Objekt (Benutzer, Dienstkonto, Gruppe oder Integriertes Sicherheitsprinzipal)	
		Adminis and the second	
		Nur     Inchtig eingegeben haben, oder entfernen Sie dieses Ubjekt aus der Liste.	
		● Unal Schließen	
	— Si	Mit höchsten Privilegien ausführen	
	В	Ausgeblendet Konfigurieren für: Windows Vista <sup>™</sup> , Windows Server <sup>™</sup> 2008	
	Α		
	9	OK Abbrechen	1
		onconengig ton act octaversities and a savanter.	

Da hilft nur die PowerShell:

1	<pre>\$action = New-ScheduledTaskAction "c:\scripts\test-\$gMSA.bat"</pre>
2	<pre>\$trigger = New-ScheduledTaskTrigger -AtStartup</pre>
3	<pre>\$principal = New-ScheduledTaskPrincipal -UserID "\$Domain\\$gMSA\$" -LogonType Password</pre>
4	Register-ScheduledTask
5	-TaskName "Test-\$gMSA"
6	-Action Saction
7	-Trigger Strigger
8	-Principal Sprincipal
9	-ErrorAction SilentlyContinue
10	Out-Null
11	
12	New-Item -Path "c:\scripts" -ItemType directory -ErrorAction SilentlyContinue   Out-Null
13	"whoami > c:\Scripts\Protokoll-\$gMSA.txt"
14	Out-File -FilePath "c:\scripts\test-\$gMSA.bat" -Encoding default

Dieser Code erstellt eine neue Aufgabe, die von dem gMSA-Account beim Systemstart ein Script startet. Das Script wird samt Verzeichnis ab Zeile 12 erstellt:

🕑 Aufgabenplanung					— C	×		🖣 📙 🖛 🛛 se	ripts		
Datei Aktion Ansicht	?						Datei	Start	Freigeb	en Ansicht	
🗢 🄿 🖄 📰 🚺							← →	· · ^	« Lok	aler > scripts	~ ē
+ + 2 III 2 III O Aufgabenplanung (Loka ) Aufgabenplanungsb	Name AdminTask CreateExplorerShe TastgMSA-Tasks Callgemein Trigger Name: Speicherort: Autor: Beschreibung: Sicherheitsoptione Beim Ausführen d SMSA-Tasks Unabhängig vu Linghängig vu Li	Aktionen Test-gMSA- ) n er Aufgaben , wenn der Brout nicht speiche Jerechtigung	Status Bereit Wird ausgeführt Bereit Bedingungen Ein Tasks folgendes Benutze enutzer angemelde teranmeldung aus m. Die Aufgabe gr en ausführen	Trigger Beim Systemstart Beim Systemstart stellungen Verlauf stellungen Verlauf	N Zierung	lachste Lauf		A 1 chnellzugriff Desktop Downloads Dokumente Bilder Desktop Dokumente Desktop Dokumente Downloads Musik Videos Lokaler Date Allfiles (E:) letzwerk	<ul> <li>« Lok</li> <li>ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب ب</li></ul>	isler > scripts Name	v đ
	Ausgeblendet	Konfigurie	ren für: Windows	s ® 7, Windows Server™ 2008 R2							

Beim manuellen Start der Aufgabe wird dann die batch-Datei ein whoami in eine Textdatei umleiten. Und hier sieht man den aktiven gMSA:

🕘 Aufgabenplanung				- 0	×	📕   🛃 📕 🖛   scri	ipts			_	
Datei Aktion Ansicht	?					Datei Start F	reigeber	n Ansicht			
🗢 🏟 🖄 📰 🛙 🖬						← → ~ ↑	« Loka	ler > scripts	v Ö	"scripts" durch	hsuch
<ul> <li>Aufgabenplanung (Lok:</li> <li>Aufgabenplanungst</li> </ul>	Name AdminTask CreateExplorerShel TestcgMSAcTask Allgemein Trigge Name: Speicherort: Autor: Beschreibung:	Status Bereit IlUnelevat Wird ausgefül Ausführen Beenden Deaktivieren Exportieren Eigenschaften Löschen	Trigger Beim Systemstart nt Bei Aufgabenerstellung oder - it Beim Systemstart instellungen Verlauf	Ns modifizierung	ichste Lauf	<ul> <li>Schnellzugriff</li> <li>Desktop</li> <li>Downloads</li> <li>Dokumente</li> <li>Bilder</li> <li>Dieser PC</li> <li>Bilder</li> <li>Desktop</li> <li>Dokumente</li> <li>Downloads</li> <li>Musik</li> <li>Videos</li> </ul>	1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1	Name Protokoll-gMS test-gMSA-Ta Protokoll- Datei Bearbe adatum\gms	gMSA gmSA iten Forma a - tasks \$	- 🗆	Ande 06.11 06.11

#### **Das Problem**

Das passt doch soweit. Wo ist nun die Problematik? Ganz einfach:

• ändert doch einmal den Benutzer des Services:



🤹 Dienste Datei Aktion Ans	icht ?		
	à 📑   🛛 📷   🕨 🔳 II IV		
🔍 Dienste (Lokal)	Oienste (Lokal)		
	Storage Tiers Management	Name	Beschreibung Status Starttyp Anmelden als
	Den Dienst <u>starten</u> Beschreibung: Optimiert die Verteilung der Daten in den Speicherstufen in allen mehrstufigen Speicherplätzen im System.	Sicherheitskonto-Manager     Smartcard     Smartcard-Geräteaufzählungse     Smartcard-Geräteaufzählungse     Software Protection     Software Protection     Software Protection     Software Protection     Standardsammlungsdienst de:     Standardsammlungsdienst     Starge Tiers Management     Systemereignissebroker     Systemereignissebroker     TCP/IP-NetBIOS-Hilfsdienst     Telefondienst     Diberwachung verteilter Verkn(     Uberstützung in der Systemst     Sudae Orchestrator Service fö	Eigenschaften von Storage Tiers Management (Lokaler Computer) ×          Allgemein       Anmelden         Wiederherstellung       Abhängigkeiten         Anmelden als:
	Enweitert / Standard /		OK Abbrechen Obernehmen
			UK Abbrechen Übernehmen

### Der Dialog kann nicht erneut aufgerufen werden!!!

### ändert doch einmal die Aufgabe:

🕒 Aufg	gabenplanu	ng									_	_		$\times$
Date 🍳	🖻 Eigenscha	ften von '	Test-gMSA-	Tasks (Lokaler	Comput	ter)					$\times$			
A	Allgemein Beim Erste	Trigger llen einer	Aktionen Aufgabe kö	Bedingungen innen Sie die B	edingun	ellungen gen angeb	Verlauf en, die die	Aufgabe a	auslösen.				Nächs	te Lauf
	Trigger		Details						St	atus		ung		_
	Beim Sta	rt	Beim S	ystemstart					А	ktiviert				
	Neu	В	earbeiten	Aufgaben Geben Sie Aufgabe e Benutzern Kennwort:	planung Benutzerl in. ame: nn der B	kontoinform	ationen zun A-Tasks\$ OK gemeldet i	? n Ausführer	× n dieser	Abbrec	chen			>

Das Kennwort kann eben NICHT leergelassen werden:



Aufgabenplanung	×
Die Änderungen können von der Aufgabenplanungnicht über Das Benutzerkonto ist unbekannt, das Kennwort ist falsch ode besitzt keine Berechtigung zum Ändern der Aufgabe.	nommen werden. <sup>,</sup> das Benutzerkonto
	ОК

Änderungen sind also nur durch die PowerShell möglich... Und das schließt auch die Erweiterung der Server mit Passwortleserecht und die Änderung der Gruppenmitgliedschaften mit ein.

#### So wird das bestimmt nichts mit gMSA!!!

# 4. Einsatz des gMSA-Admin-Scriptes

### Die Lösung

Ich habe für genau diese Aufgabenstellung ein kleines PowerShell-Script geschrieben. Dieses beinhaltet die erforderlichen Funktionen zur gMSA-Administration:

- Erstellen eines gMSA
- Löschen eines gMSA
- Änderung der Server f
  ür die gMSA-Verwendung (hinzuf
  ügen und entfernen)
- Änderung der Gruppenmitgliedschaft eines gMSA
- Konfiguration einer bestehenden Aufgabe für gMSA
- Konfiguration eines bestehenden Services für gMSA inklusive Entfernen des gMSA
- Vorbereitung des AD
- Testen eines gMSA (erstellt eine Aufgabe, bindet den gMSA ein startet die Aufgabe und löscht sie wieder)

Und das ganze mit grafischer Oberfläche! So wird es gestartet:



Und das ist die GUI:



gMSA-Admin		-	×
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:	
erstelle gMSA lösche gMBA	weiterer Server entferne Server teste gMSA	weitere Gruppe entferne Gruppe	
vorhandene Tasks:	vorhandene Services:		
lese alle Server setze gMSA ein	lese alle Server setze gMSA ein zurücksetzen		

### Einrichtung eines gMSA mit Vorbereitung der Domäne

Sollte die Funktionsebene der Domäne niedriger sein als Windows Server 2012, dann wird das Script nachfragen, ob es die Erhöhung durchführen darf.



Sollte das Script keinen KDS-Rootkey finden, dann wird es fragen, ob es einen erstellen darf:

Prüfung der gMSA-Voraussetzungen	×
Im AD wurde kein KDSRootKey gefunden. Soll ein Key erstellt werde	en?
Ja Nein	

Wenn die Voraussetzungen nicht erfüllt sind, dann bleiben alle Schalter deaktiviert.

Über den Schalter "neuer gMSA" kann mit 2 Eingaben ein neuer gMSA erzeugt werden:



드 gMSA-Admin			_	$\times$
gMSA-Admin  vorhandene gMSA:   restelle gMSA  Pische gMSA  vorhandene Tasks:	zugehörige Server:	zugehörige Gruppen: × OK tere Gruppe enfferne Gruppe		×
🖕 gMSA-Admin			-	×
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:		

	neuer gMSA Geben Sie eine <mark>Beschreibung</mark> ein	X
erstelle gMSA lösche git BA vorhandene Tasks:	Abb	rech ere Gruppe entferne Gruppe

Ist der Account erzeugt, dann wird er direkt ausgewählt. Zu dem selektierten gMSA werden alle weiteren Felder aktualisiert:

드 gMSA-Admin		- 🗆 ×
vorhandene gMSA:	zugehörige Server:	zugehörige Gruppen:
(pMSA-Test1 (Testaccount)		direkte Gruppen Donänencomputer Jeder Prä-Windows 2000 kompatibler Zugriff Benutzer Zertifikatdienst-DCDM-Zugriff Authentifizierte Benutzer Diese Organisation Vom Dienst bestätigte ID Mittlere gehobene Verbindlichkeitsstufe
erstelle gMSA lösche gMSA	weiterer Server entferne Berver teste gM6A.	weitere Gruppe entferne Gruppe
vorhandene Tasks:	vorhandene Services:	



Nun können Server an den gMSA gebunden werden:

🖕 gMSA-Admin		- 🗆 X
vorhandene gMSA: (#MSA-Test) (Testaccourt)	zugehörige Server:	zugehörige Gruppen: drekte Gruppen Domänencomputer Jeder Y Prä-Windows 2000 kompatibler Zugriff Benutzer Zerlifk-adiensi-DCDM-Zugriff Authenhitizerte Benutzer
	LON-DC1	Vom Dienst bestätigte ID Mittlere gehobene Verbindlichkeitsstufe
erstelle gMSA lösche gMSA vorhandene Tasks:	weiterer Server         entferme Server         teste.gMSA,           vorhandene Services:	weitere Gruppe entreme Gruppe

Für den ausgewählten Server wird dann ein Powershell-Remoting versucht. Ist dieses erfolgreich, dann werden in den unteren Boxen alle Aufgaben und Dienste des Servers angezeigt:

erstelle gMSA lösche gMSA	weiterer Server entferne Server teste gMSA weitere Gruppe entferne Gruppe
vorhandene Tasks:	vorhandene Services:
LON-DC1 \Admin Task (Administrator) LON-DC1 \CreateExplorerShellUnelevatedTask (Administrator)	LON-DCTV4DVS - C: Windows'ADWS'\MicrosoftActiveDirectory.WebServices.exe [LocalSystem]     LON-DCTV4DVS - C: Windows'System32Valg.exe (NT AUTHORITY'LocalService)     LON-DCTV4DVS - C: Windows'System32Valg.exe (NT AUTHORITY'LocalService)     LON-DCTVDVS - C: Windows'System32VDFSR: exe [LocalSystem]     LON-DCTVDFSR - C: Windows'System32Valses exe [LocalSystem]     LON-DCTVSR - C: Windows'System32Valses exe [LocalSystem]     LON-DCTVR SPC - C: Windows'System32Valse
lese alle Server setze gMSA ein	lese alle Server seize gMBA ein zurücksetzen

### Konfiguration eines Scheduled-Tasks mit gMSA

Eine fertige Aufgabe in der Aufgabenplanung kann nun einfach ausgewählt werden. Mit dem Schalter "setze gMSA ein" wird dann der gewählte gMSA auf dem gewählten Server aus Account für die gewählte Aufgabe geschrieben. Wenn das funktioniert wird der Erfolg mitgeteilt:

orhandene Tasks:	vorhandene Services:
LON-DE1VAdminTask (pMSA-Test1\$) _DN-DE1VCreateExplorerShellUnelevatedTask (Administrator)	LON-DCTVADY Erfolg LON-DCTVALG LON-DCTVALG LON-DCTVALG LON-DCTVALG LON-DCTVALG LON-DCTVALG LON-DCTVALG Der Task wurde umgertellt! LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB LON-DCTVAB
lese alle Server setze gMSA ein	lese elle Gerver setze gMDA: ein zurücksetzen



In der Aufgabenplanung kann das Ergebnis geprüft werden:

🕑 Aufgabenplanung						- 0	×
Datei Aktion Ansicht ?							
🗢 🏟 🖄 📰 🚺							
Aufgabenplanung (Lokal) > Aufgabenplanungsbibliot	Name AdminTask CreateExplorerShe <	Status Bereit IIUn Wird ausgeführt Aktionen Bedingunge	Trigger Beim Systemstart Bei Aufgabenerstellung oder -modifizierung	Nächste Laufzeit	Letzte Laufzeit 30.11.1999 00:00:00 06.11.2017 11:53:06	Ergebnis der I Die Aufgabe v Die Aufgabe v	etzten / wurde r wird mc >
	Name:	AdminTask					
	Autor: Beschreibung:	ADATUM\Administrator					
	Sicherheitsoptione Beim Ausführen d gMSA-Test15 Nur ausführen, Unabhängig vo Lennwort r Mit höchsten E Ausgeblendet	n er Aufgaben folgendes B wenn der Benutzer ange on der Benutzeranmeldur nicht speichern. Die Aufg ierechtigungen ausführer Konfigurieren für:	enutzerkonto verwenden: meldet ist 1g ausführen abe greift nur auf lokale Ressourcen zu. 1 ndows © 7, Windows Server™ 2008 R2				~
< >>	J.						

Wenn eine Aufgabe verändert werden muss, dann trägt man temporär einen Benutzer als Konto ein, ruft den gMSA-Admin auf und überschreibt den User mit dem passenden gMSA. ③

### Konfiguration eines Services mit gMSA

Dienste können ebenso leicht modifiziert werden: such den Service aus der Liste aus und klicke auf "setze gMSA ein". Der Dienst wird danach in der Liste nach oben einsortiert:

erstelle gMSA lösche gMSA	weiterer Server entferne Server teste gMSA weitere Gruppe entferne Gruppe
vorhandene Tasks:	vorhandene Services:
LON-DC1VAdminTask. (gMSA-Test1\$) LON-DC1VCreateExplorerShellUnelevatedTask (Administrator)	LDN-DC1X1tethplBprg252cortee         CAWindows/suptem32X1ieringEngineService.exe (ADATUM/sMISA8Text)           LDN-DC1X4DW3 - C.Windows/ADWS/Microsoft.ActiveDirectory.WebServices.exe (LocalSystem)         LDN-DC1X4DW3 - C.Windows/System32Xalg.exe (INT AUTHORITYLcoalService)           LDN-DC1VeFsv - C.Windows/System32Xalg.exe (INT AUTHORITYLcoalService)         LDN-DC1Versv - C.Windows/System32Xalg.exe (INT AUTHORITYLcoalService)           LDN-DC1VeFsv - C.Windows/System32Xalg.exe (INT AUTHORITYLcoalService)         LDN-DC1VeFsv - C.Windows/System32Xalfinost.exe /Processid (ID2048)F1FD88-11D1-960D-00805FC79235) (Loc UN-DC1V)FS - C.Windows/System           LDN-DC1VeFsv - C.Windows/System         Erfolg           LDN-DC1VeFsv - C.Windows/System         Der Service, wurde neu gestartet!           LDN-DC1VsS-VC.Windows/System         Der Service, wurde neu gestartet!           LDN-DC1VsSVersv - C.Windows/System         Der Service, wurde neu gestartet!           LDN-DC1VsSV - C.Windows/System         Der Service, wurde neu gestartet!           LDN-DC1Vsefsv - C.Windows/System         Der Service, wurde neu gestartet!           LDN-DC1Vsefsv - C.Windows/System         Der Service, Wurde           LDN-DC1Vsefsv - C.Windows/System32Vmsiewsc.exe / (LocalSystem)         Service)           LDN-DC1Vseffsv - C.Windows/System32Vmsiewsc.exe / (LocalSystem)         Service)           LDN-DC1Vseffvard C.Windows/System32Vsass.exe (LocalSystem)         Service)           LDN-DC1Vseffvard C.Windows/System32Vsass.exee (Loc
lese alle Server setze gMSA ein	lese die Gerver setze gMSA ein zurücksetzen

Keine Lust mehr auf gMSA? Dann wähle den Service aus und klicke auf Zurücksetzen:

erstelle gMSA lösche gMSA	weiterer Server entferme Server teste gMSA weitere Gruppe entferme Gruppe	
orhandene Tasks:	vorhandene Services:	
DN-DC1VAdminTask (gMSA-Test1\$) DN-DC1VCreateExplorerShellUnelevatedTask (Administrator)	LDN-DC1VMSDTC - C.Windows/System32/snsitec.exe (NT AUTHORITY/NetworkService) LDN-DC1Vmiserver - C.Windows/system32/snsitec.exe // LocalSystem) LDN-DC1VMstop - C.Windows/System32/snsite.exe (LocalSystem) LDN-DC1VHT05 - C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VHT05 - C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VSepTevo - C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VSepter - C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1VwattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Snsite.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe (LocalSystem) LDN-DC1WattSv C.Windows/System32/Wats.exe	
lese alle Server setze gMSA ein	lese die Server setze gMSA ein zurücksetzen	

## Konfiguration von Berechtigungen eines gMSA

Der gMSA benötigt höhere Rechte? Kein Problem:

gMSA-Admin					-		>
vorhandene gMSA:		zugehörige Server:		zugehörige Gruppen:			
gl GSA-Test1 (Testaccount) G G	VSA in Gruppe aufnehmen ieben Sie den Namen der Gruppe ein Domänen-Admins	Adatum.com X OK Abbrech		direkte Gruppen Domänencomputer Jeder Prä-Windows 2000 kompatibler Zugriff Benutzer Zetrifikatdienst-DCDM-Zugriff Authentitizierte Benutzer Diese Organisation Vom Dienst-bestätigte ID Mittlere gehobene Verbindlichkeitsstufe			
erstelle gMSA lösche gMSA	weitere	Server entferne Server	teste gMSA	weitere Gruppe			
.ON-DC1\AdminTask (gMSA-Test1\$) .ON-DC1\CreateExplorerShellUneleva	atedTask (Administrator) LON-DC1 LON-DC1 LON-DC1	\MSDTC - C:\Windows\Systen \msiserver - C:\Windows\syste \Netlogon - C:\Windows\syster \NTDS - C:\Windows\System?	n32\msdtc.exe (NT AL) m32\msiexec.exe /V (I m32\lsass.exe (LocalS) 22\lsass.exe (LocalSus)	ITHORITY'\NetworkService) LocalSystem) ystem) tem)	^		
gMSA-Admin					-		
vorhandene gMSA:	zugehörig	zugehörige Server:		zugehörige Gruppen:			
gMSA-Test1 (Testaccount)	LON-DC	Adəlum com		- diekte Gruppen Domärear-Admiss 			
erstelle gMSA lösche gMSA	weitere	r Server entferne Server	teste gMSA.	weitere Gruppe entferne Gruppe			
vorhandene Tasks:	vorhande	ne Services:					
LON-DC1\AdminTask (gMSA-Test1\$)	atedTask (Administrator)	\MSDTC - C:\Windows\System	m32\msdtc.exe (NT Al	JTHORITY'NetworkService)	^	]	

## <u>Zusammenfassung</u>

Das Script steht für euch in der ersten Generation bereit und wurde bereit in mehreren Produktionsumgebungen getestet. Nun gibt es keine Ausreden mehr! Viel Spaß beim Evaluieren!!!