gMSA Configuration

Group Managed Service Accounts (gMSA) provides the same functionalities as **managed service accounts** but they extend its capabilities to host **group** levels. This feature was first introduced with Windows Server 2012. It uses Microsoft Key Distribution **Service**(KDC) to create and manage the passwords for the gMSA.

Created the account by using the following commands:

PS C:\Users\Administrator> Add-KdsRootKey –EffectiveTime ((get-date).addhours(-10))

Guid

0bcb8044-4708-ba00-8a5c-e6b5425f1a92

PS C:\Users\Administrator> New-ADServiceAccount -Name gmsa01

cmdlet New-ADServiceAccount at command pipeline position 1

Supply values for the following parameters:

DNSHostName: gmsa01.ad.bmc.com

PS C:\Users\Administrator> Get-ADServiceAccount

cmdlet Get-ADServiceAccount at command pipeline position 1

Supply values for the following parameters:

(Type !? for Help.)

Filter: *

DistinguishedName : CN=gmsa01,CN=Managed Service Accounts,DC=ad,DC=bmc,DC=com

Enabled : True

Name : gmsa01

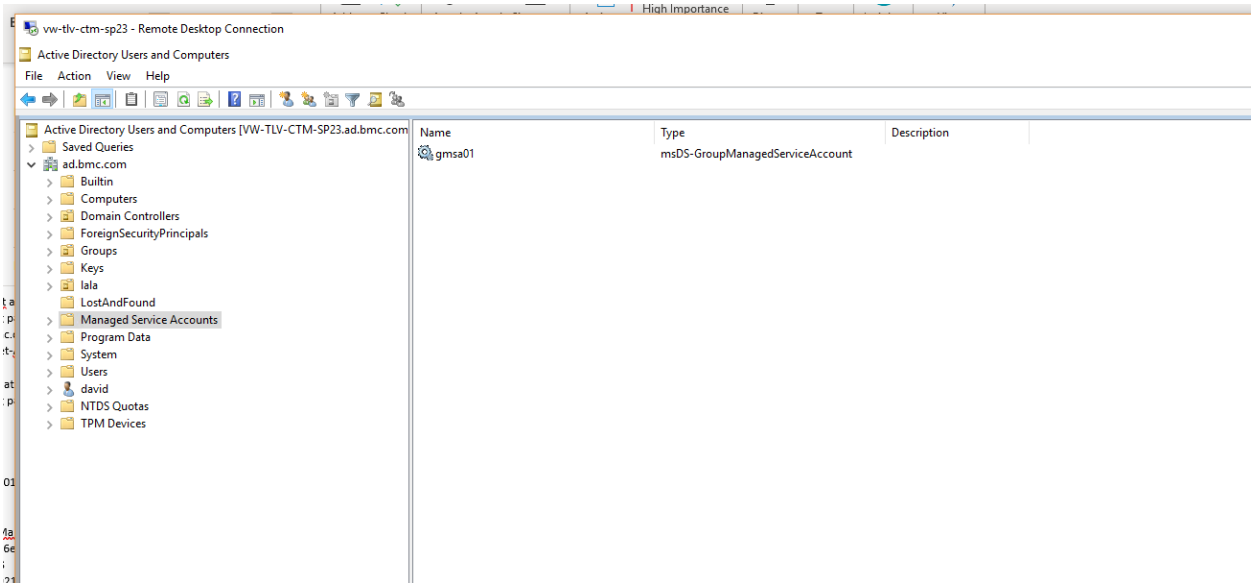
ObjectClass : msDS-GroupManagedServiceAccount

ObjectGUID : bc963a64-5d6e-4562-b3c9-3fe93b3b1634

SamAccountName : gmsa01$

SID : S-1-5-21-4187989210-2745887710-1304445342-1122

UserPrincipalName :



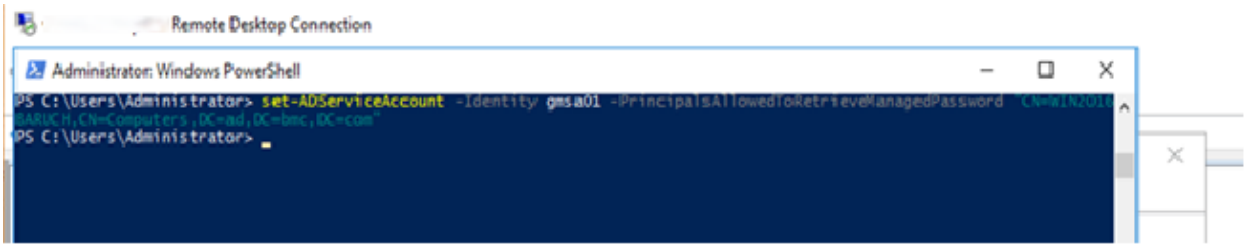
Now you need to configure the Computer Name where you will allow the use of this “gmsa01” service account

What is the computer name? Host: Win2016Baruch

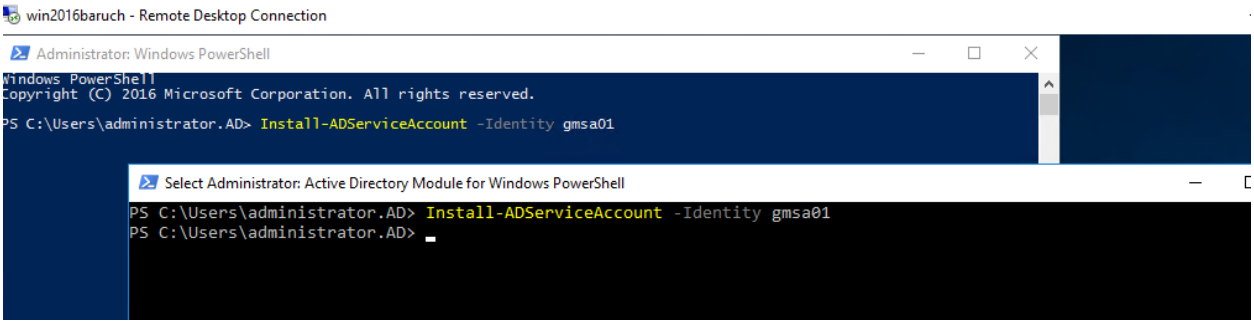
It must be on that same domain

Win2016Baruch will be configured to use the managed service account “gmsa01”

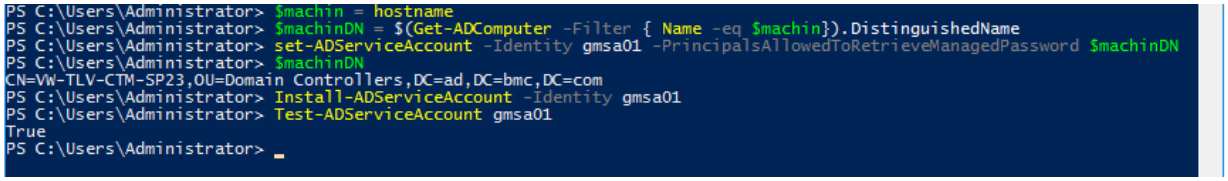
On the DC: (you will need to know the DistinguishedName)



On Win2016Baruch



Can be done by using PowerShell on the DC



PS C:\Users\Administrator> $machin = hostname

PS C:\Users\Administrator> $machinDN = $(Get-ADComputer -Filter { Name -eq $machin}).DistinguishedName

PS C:\Users\Administrator> set-ADServiceAccount -Identity gmsa01 -PrincipalsAllowedToRetrieveManagedPassword $machinDN

PS C:\Users\Administrator> $machinDN

CN=VW-TLV-CTM-SP23,OU=Domain Controllers,DC=ad,DC=bmc,DC=com

PS C:\Users\Administrator> Install-ADServiceAccount -Identity gmsa01

PS C:\Users\Administrator> Test-ADServiceAccount gmsa01

True

Now you should be able to configure the service to login as user:

You basically need the service account with the $ and NOT to enter any password

```
PS C:\Users\Administrator> Get-ADServiceAccount -Identity gmsa01


DistinguishedName : CN=gmsa01,CN=Managed Service Accounts,DC=ad,DC=bmc,DC=com
Enabled           : True
Name              : gmsa01
ObjectClass       : msDS-GroupManagedServiceAccount
ObjectGUID        : bc963a64-5d6e-4562-b3c9-3fe93b3b1634
SamAccountName    : gmsa01$
SID               : S-1-5-21-4187989210-2745887710-1304445342-1122
UserPrincipalName :
```

Now you can associate the new MSA with your service(s).

The GUI way:

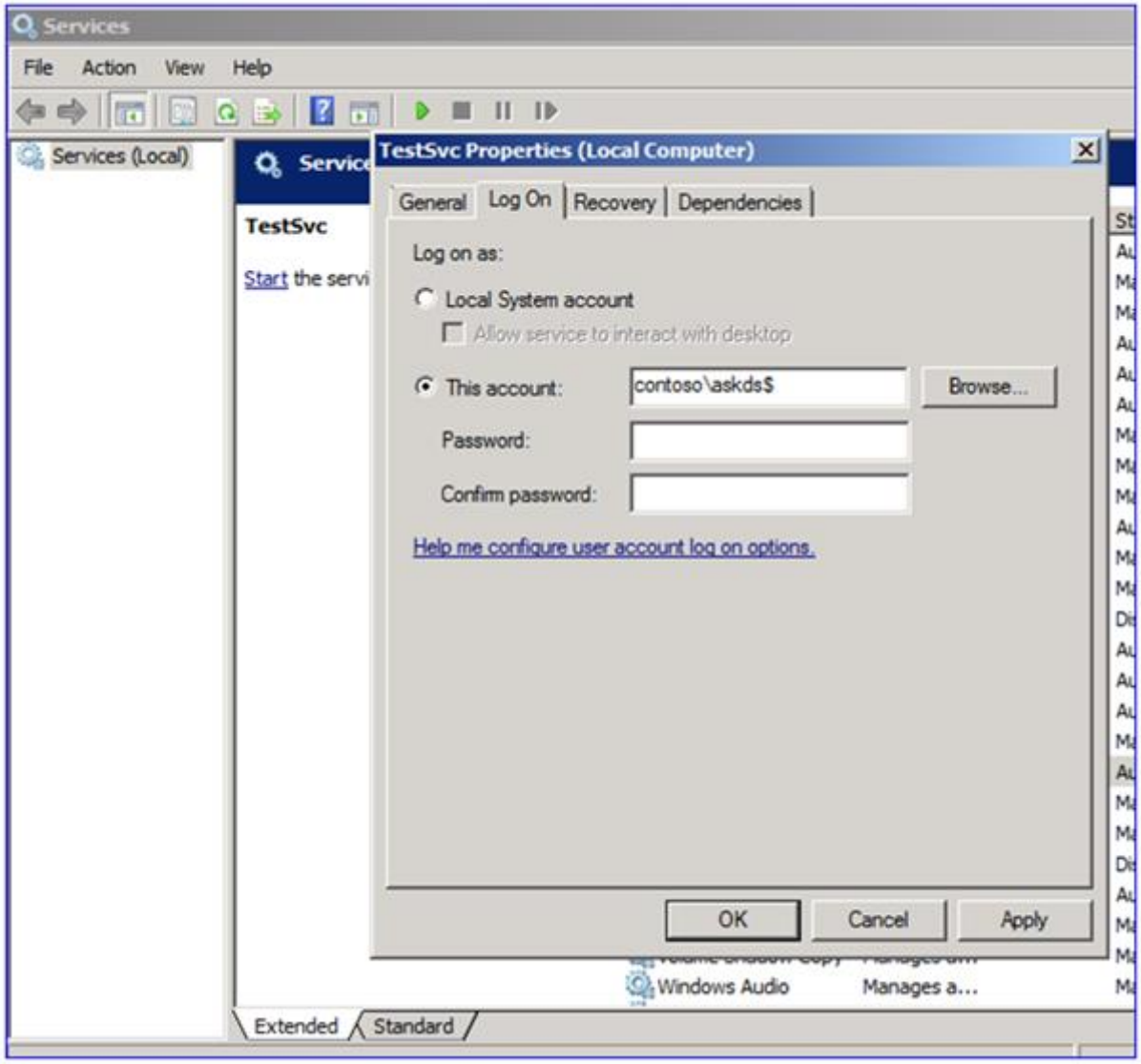
a. Start services.msc.

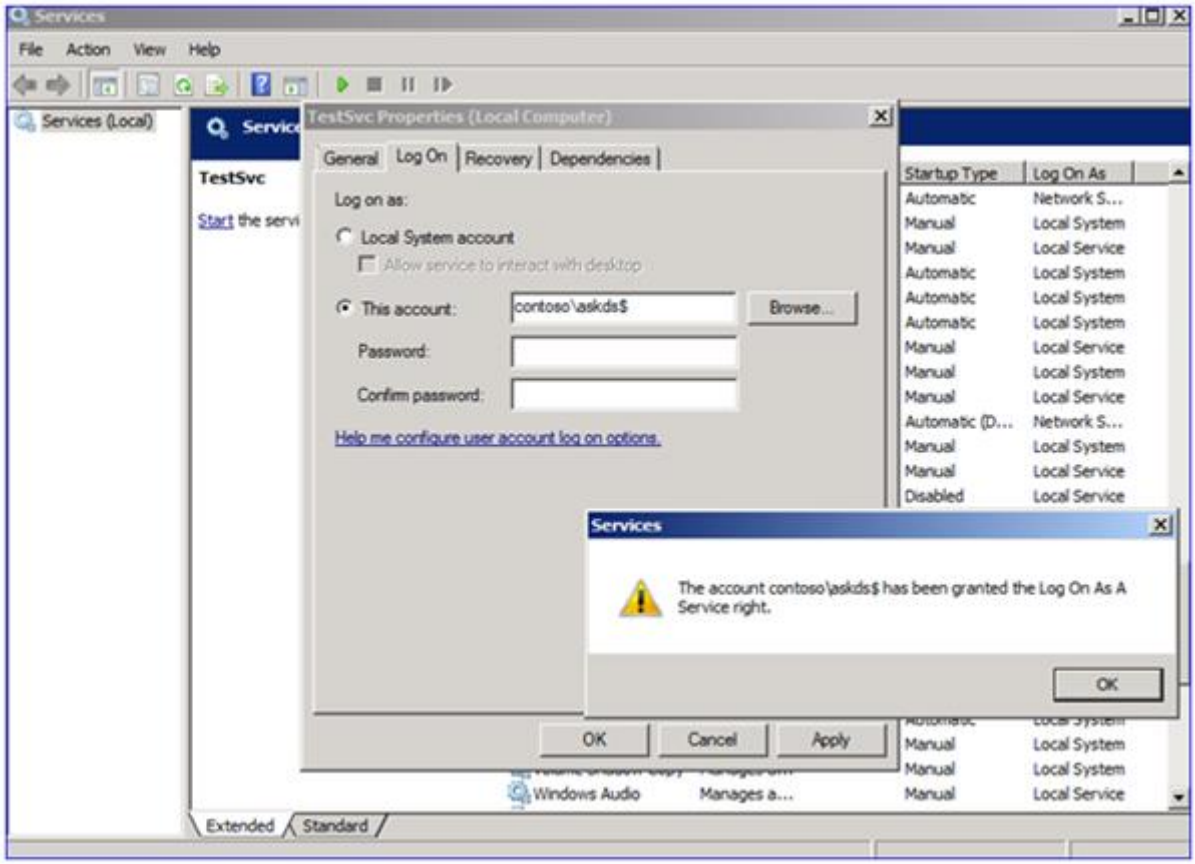
b. Edit your service properties.

c. On the Log On tab, set “This Account” to the domainname$ of your MSA. So if your MSA was called “AskDS” in the “contoso.com” domain, it would be:

`contosoaskds$`

d. Remove all information from Password and Confirm password – they should not contain *any* data:


Services
File
Action
View
Help
Services (Local)
TestSvc
Start the servi
TestSvc Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
contoso\askds$
Browse...
Password:
Confirm password:
Help me configure user account log on options.
OK
Cancel
Apply
Windows Audio
Manages a...
Extended
Standard



Start the service. It should run without errors.

Note: From: http://www.rebeladmin.com/2018/02/step-step-guide-work-group-managed-service-accounts-gmsa-powershell-guide/

Uninstall Service Account

If there is a need to remove the managed service account, it can be done by executing the following:

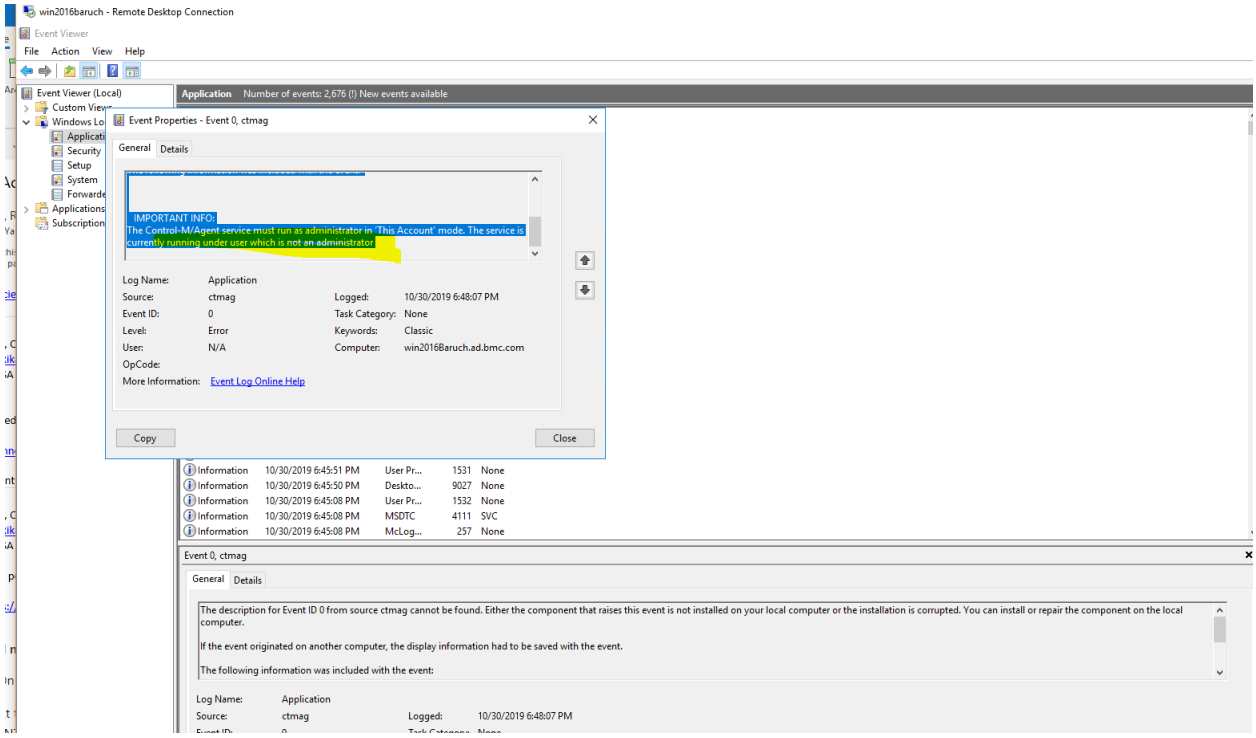
Remove-ADServiceAccount -identify “Mygmsa1”

Above command will remove Mygsmsa1 account

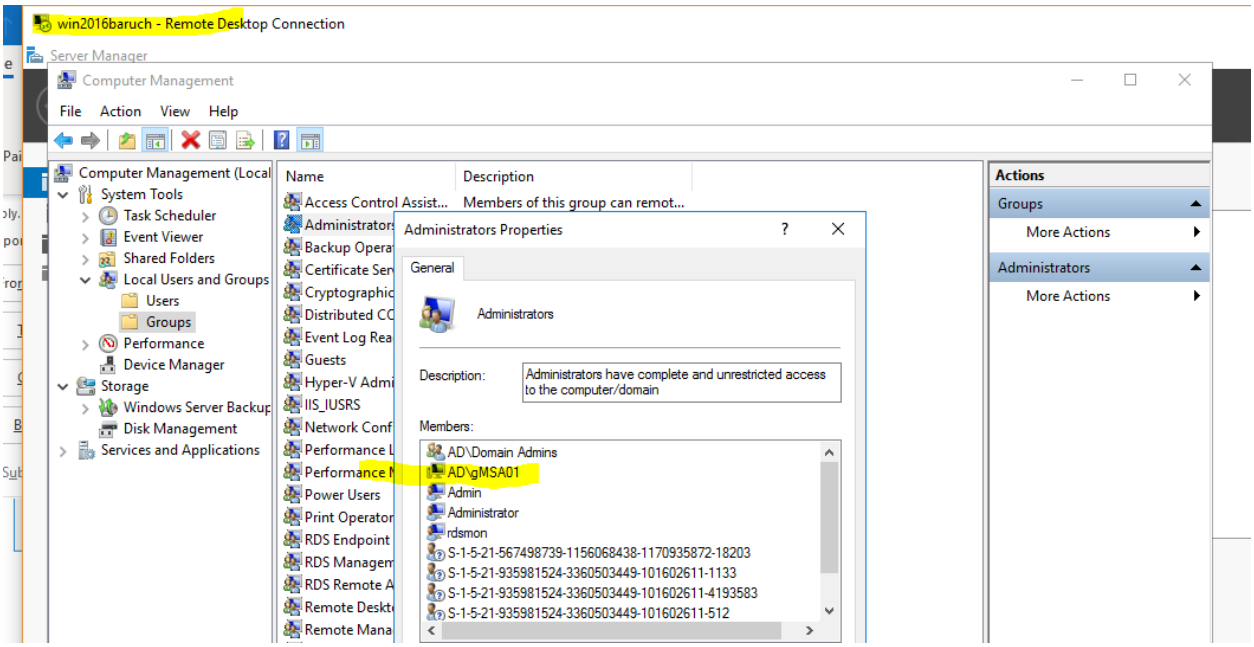
The “Install-AdserviceSccount -identity dmsa01 must be installed on the server that runs the service

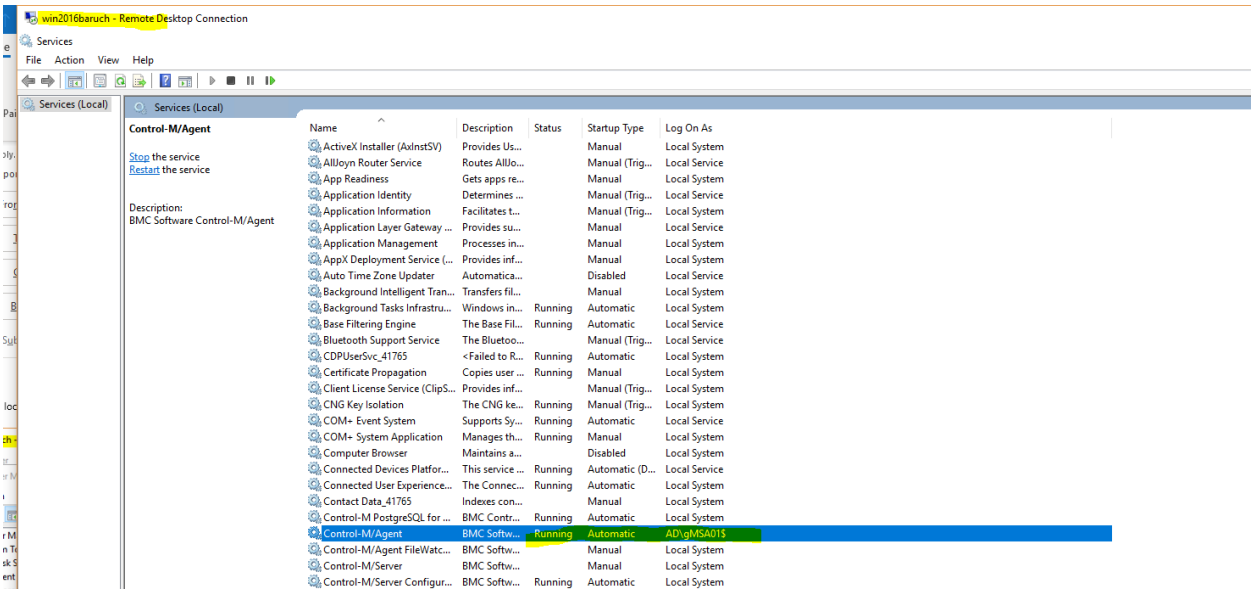
```
PS C:\Users\Administrator> Get-ADServiceAccount -Identity gmsa01 -Properties * |fl PrincipalsAllowedToRetrieveManagedPassword

PrincipalsAllowedToRetrieveManagedPassword : {CN=WIN2016BARUCH,CN=Computers,DC=ad,DC=bmc,DC=com}

PS C:\Users\Administrator>
```

Encountered an issue:



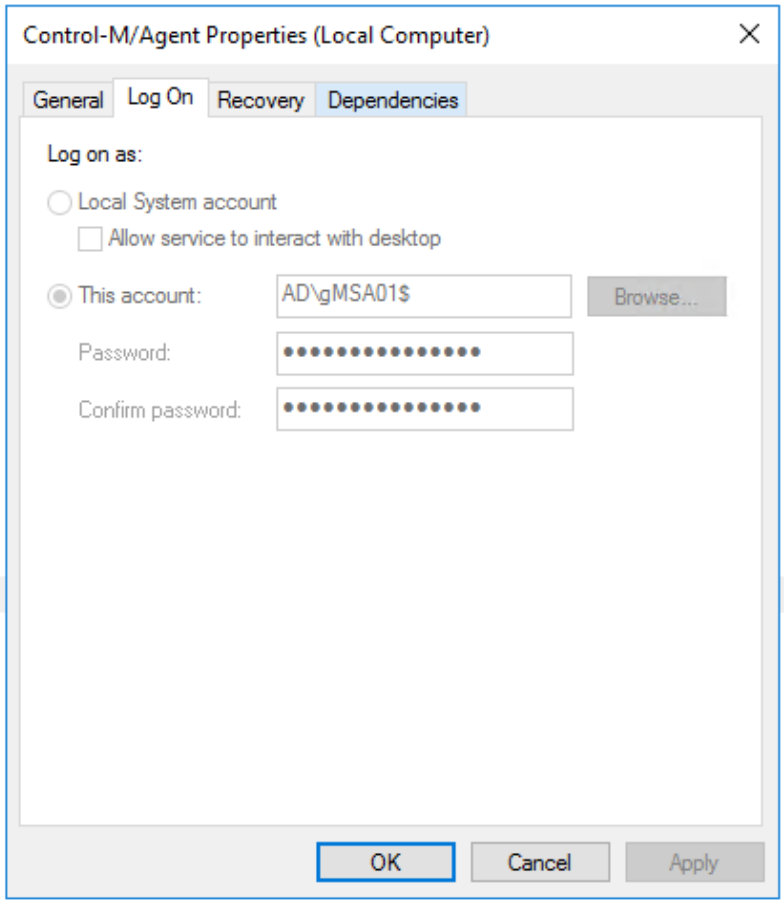
It is added to the local administrator group:





A gMSA will change the logon of the service to GRAY and therefore no one can change it (from the GUI).

Local System



Local System
Local System
Local System
Local System
Local System
Local System

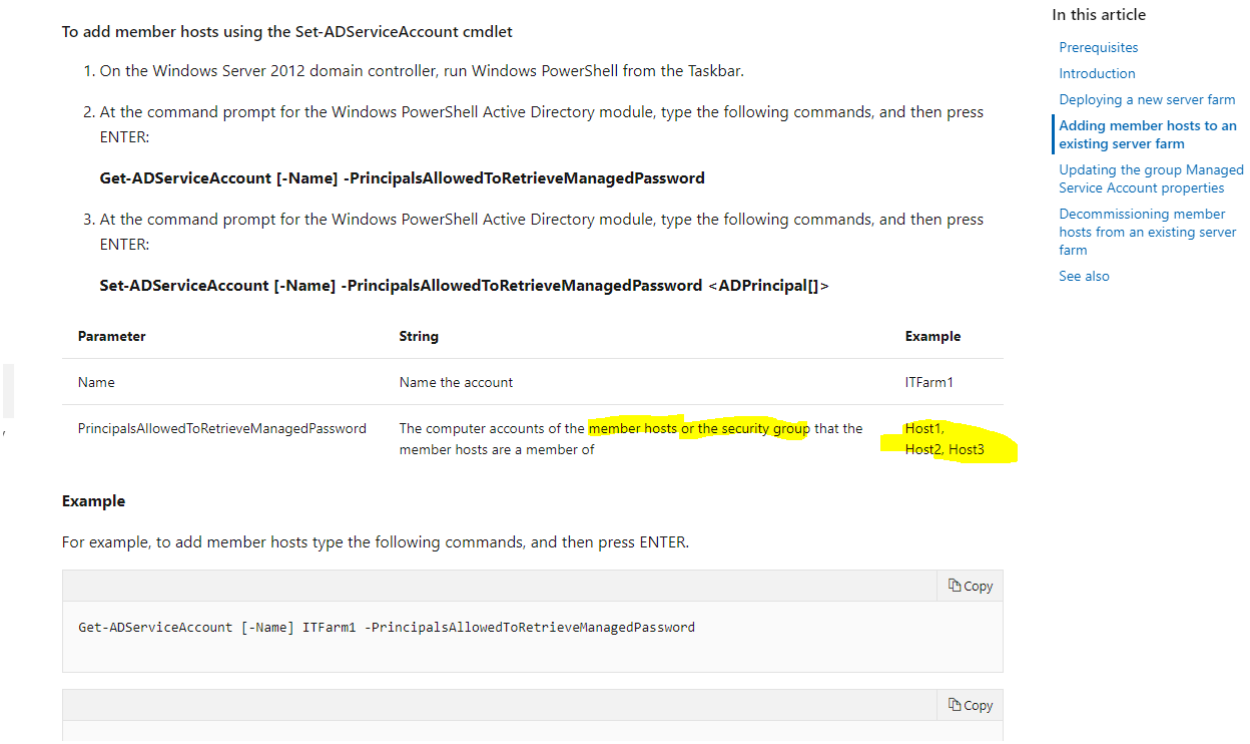
If there is a need to change it to a regular account:

Follow the steps below:

https://www.wojcieh.net/change-windows-service-log-on-as-user-from-msagmsa-to-normal-account/

sc config ctmag obj= ad\Administrator password=<PASSWORD>

With gMSA there is an option to use the same account on multiple hosts:
https://docs.microsoft.com/en-us/windows-server/security/group-managed-service-accounts/getting-started-with-group-managed-service-accounts#BKMK_DeployNewFarm



In this article

To add member hosts using the Set-ADServiceAccount cmdlet

1. On the Windows Server 2012 domain controller, run Windows PowerShell from the Taskbar.
2. At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

   Get-ADServiceAccount [-Name] -PrincipalsAllowedToRetrieveManagedPassword
3. At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

   Set-ADServiceAccount [-Name] -PrincipalsAllowedToRetrieveManagedPassword <ADPrincipal[]>

Parameter	String	Example
Name	Name the account	ITFarm1
PrincipalsAllowedToRetrieveManagedPassword	The computer accounts of the member hosts or the security group that the member hosts are a member of	Host1, Host2, Host3

Example

For example, to add member hosts type the following commands, and then press ENTER.

Copy

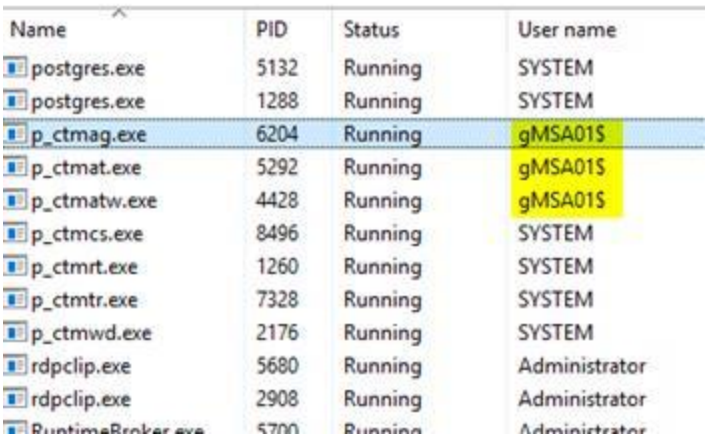
```
Get-ADServiceAccount [-Name] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword
```

Copy

Testing configuration:

AG to SRV and SRV to AG communication is working

AG process run as gMSA01 user



Name	PID	Status	User name
postgres.exe	5132	Running	SYSTEM
postgres.exe	1288	Running	SYSTEM
p_ctmag.exe	6204	Running	gMSA01$
p_ctmat.exe	5292	Running	gMSA01$
p_ctmatw.exe	4428	Running	gMSA01$
p_ctmcs.exe	8496	Running	SYSTEM
p_ctmrt.exe	1260	Running	SYSTEM
p_ctmtr.exe	7328	Running	SYSTEM
p_ctmwd.exe	2176	Running	SYSTEM
rdpclip.exe	5680	Running	Administrator
rdpclip.exe	2908	Running	Administrator
RuntimeBroker.exe	5700	Running	Administrator

One more test that should be done is to have multiple endpoints (multiple Control-M/Agents) and to configure that same gMSA to be used on all of them.

To add member hosts using the Set-ADServiceAccount cmdlet

1. On the Windows Server 2012 domain controller, run Windows PowerShell from the Taskbar.
2. At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

   Get-ADServiceAccount [-Name] -PrincipalsAllowedToRetrieveManagedPassword
3. At the command prompt for the Windows PowerShell Active Directory module, type the following commands, and then press ENTER:

   Set-ADServiceAccount [-Name] -PrincipalsAllowedToRetrieveManagedPassword <ADPrincipal[]>

Parameter	String	Example
Name	Name the account	ITFarm1
PrincipalsAllowedToRetrieveManagedPassword	The computer accounts of the member hosts or the security group that the member hosts are a member of	Host1, Host2, Host3

Example

For example, to add member hosts type the following commands, and then press ENTER.

Copy

```
Get-ADServiceAccount [-Name] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword
```

Copy

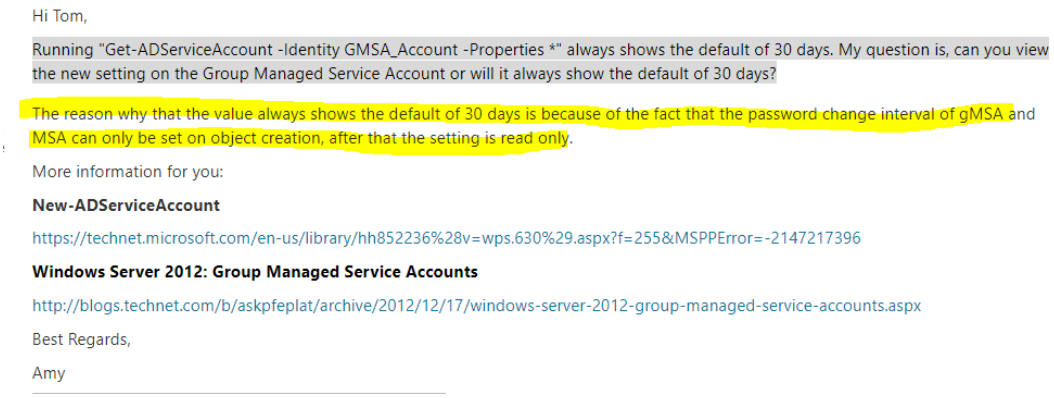
```
Set-ADServiceAccount [-Name] ITFarm1 -PrincipalsAllowedToRetrieveManagedPassword Host1,Host2,Host3
```

Ye
In this
Prerec
Introd
Deplo
Addin
existi
Updat
Servic
Decor
hosts
farm
See al

Automatic password change

We cannot change an existing gMSA account password once the user is already created.

To do that, we will need to create a new account and configure that setting at the creation time of the account.



Hi Tom,

Running "Get-ADServiceAccount -Identity GMSA_Account -Properties *" always shows the default of 30 days. My question is, can you view the new setting on the Group Managed Service Account or will it always show the default of 30 days?

The reason why that the value always shows the default of 30 days is because of the fact that the password change interval of gMSA and MSA can only be set on object creation, after that the setting is read only.

More information for you:

New-ADServiceAccount

https://technet.microsoft.com/en-us/library/hh852236%28v=wps.630%29.aspx?f=255&MSPPError=-2147217396

Windows Server 2012: Group Managed Service Accounts

http://blogs.technet.com/b/askpfeplat/archive/2012/12/17/windows-server-2012-group-managed-service-accounts.aspx

Best Regards,

Amy

Changing an automatic password daily:

The account name is: **gMSA02dailypass**

On the DC machine:

New-ADServiceAccount -Name gMSA02dailypass -DNSHostName gMSA02dailypass.ad.bmc.com -ManagedPasswordIntervalInDays 1

set-ADServiceAccount -Name gMSA02dailypass -PrincipalsAllowedToRetrieveManagedPassword "CN=WIN2016BARUCH,CN=Computers,DC=ad,DC=bmc,DC=com"

On the client win2016Baruch:

INSTALL-ADSERVICEACCOUNT -IDENTITY gMSA02dailypass