HORIZON
SECURED

Active Directory - gMSA

Creation Guide

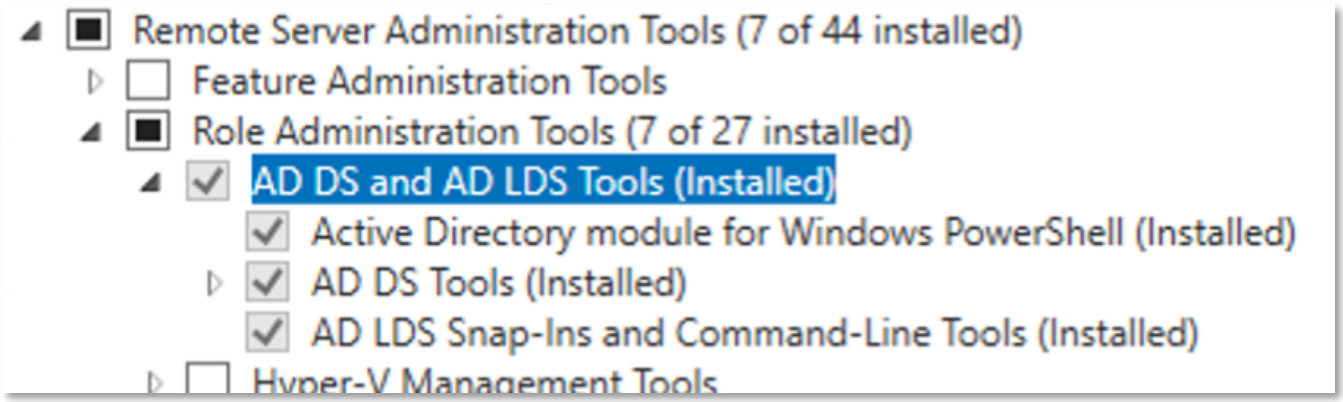
Procedure:

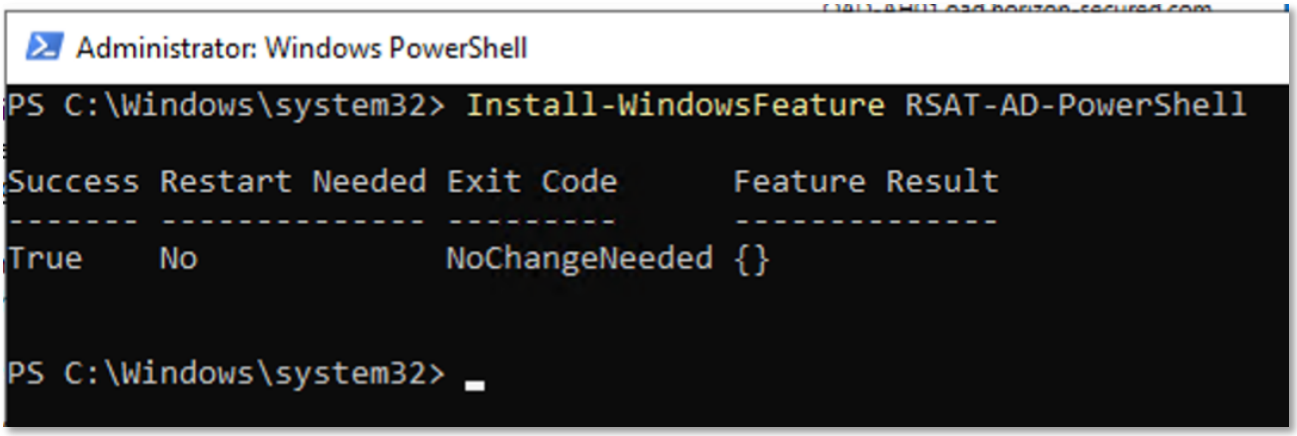
0. Develop a Sysmon configuration baseline
1. Download and install Sysmon
2. GPO installation
3. Verify the installation
4. Continuously work on the configuration baseline

For more details

1. First, we need to install Remote Server Administration Tools (RSAT):

    - *Open servermanager.exe*
    - *Go to Add Roles and Features*
    - *Under Features, select the following:*
        - *AD DS and AD LDS Tools*
    - *Or use PowerShell*
        - *Install-WindowsFeature RSAT-AD-PowerShell*





2. Now we might need to create new KdsRootKey. You might already have one, you can verify with:

- *Get-KdsRootKey*

```
PS C:\Windows\system32> Get-KdsRootKey
PS C:\Windows\system32>
```

As you can see, I don't have one, so let's create one:

- *$a = Get-Date*
- *$b = $a.AddHours(-10)*
- *Add-KdsRootKey -EffectiveTime $b*

```
PS C:\Windows\system32> $a = Get-Date
PS C:\Windows\system32> $b = $a.AddHours(-10)
PS C:\Windows\system32> Add-KdsRootKey -EffectiveTime $b

Guid
----
06505a26-4dd5-1173-501e-f3df88e2ff4d
```

3. Now to the creation of the gMSA itself. Let's say I am creating a service account for **OAD-AH01 server** and I have Security Baselies implemented. It is very straightforward and it is done, again, with PowerShell:

   - *New-ADServiceAccount -Name gMSA_TST01 -DNSHostName gMSA_TST01.oad.horizon-secured.com -Enabled $true -PrincipalsAllowedToRetrieveManagedPassword **OAD-AH01$** -KerberosEncryptionType AES128,AES256*
     - *Note **the encryption types**. This is important because you might end up with generic error when installing the gMSA account, if you are using Security Baselines or hardening of Kerberos Encryption types*

```
PS C:\Windows\system32> New-ADServiceAccount -Name gMSA_TST01 -DNSHostName gMSA_TST01
.oad.horizon-secured.com -Enabled $true -PrincipalsAllowedToRetrieveManagedPassword O
AD-AH01$ -KerberosEncryptionType AES128,AES256
```

4. Last part is installing the gMSA on the target device, in our case **OAD-AH01$.** Steps are as follows:

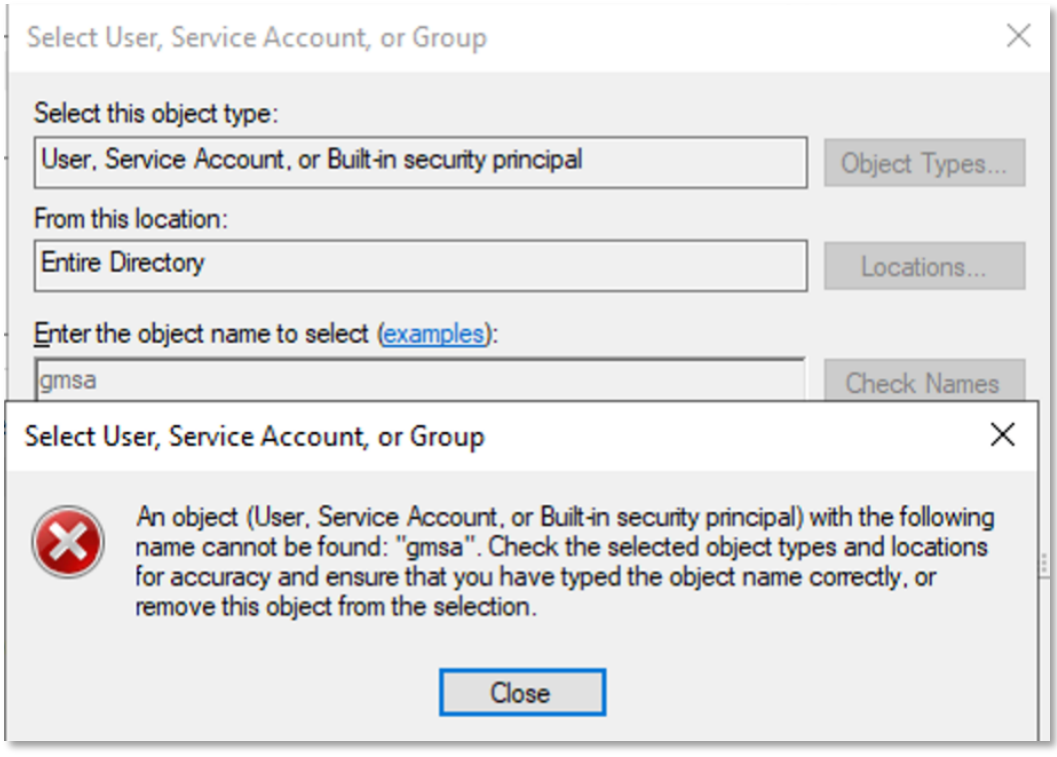
    - *Install RSAT AD tools:*
        - *Install-WindowsFeature RSAT-AD-PowerShell*
    - *Install the gMSA:*
        - *Install-ADServiceAccount gMSA_TST01*
            - *I found out that this is not always needed. You can verify if it's needed by using:*
                - *Test-ADServiceAccount gMSA_TST01*
                    i. *If it says True, you are ready to proceed.*

```
PS C:\Windows\system32> Install-ADServiceAccount gMSA_TST01
PS C:\Windows\system32> _
```

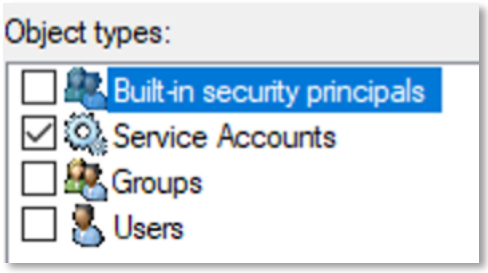
```
PS C:\Windows\system32> Test-ADServiceAccount gMSA_TST01
True
```

5. What happens next depends on the use-case which you have for your gMSA (app, service, task, …,) For this demonstration I chose Task Scheduler as my use-case, because it is, well, interesting:

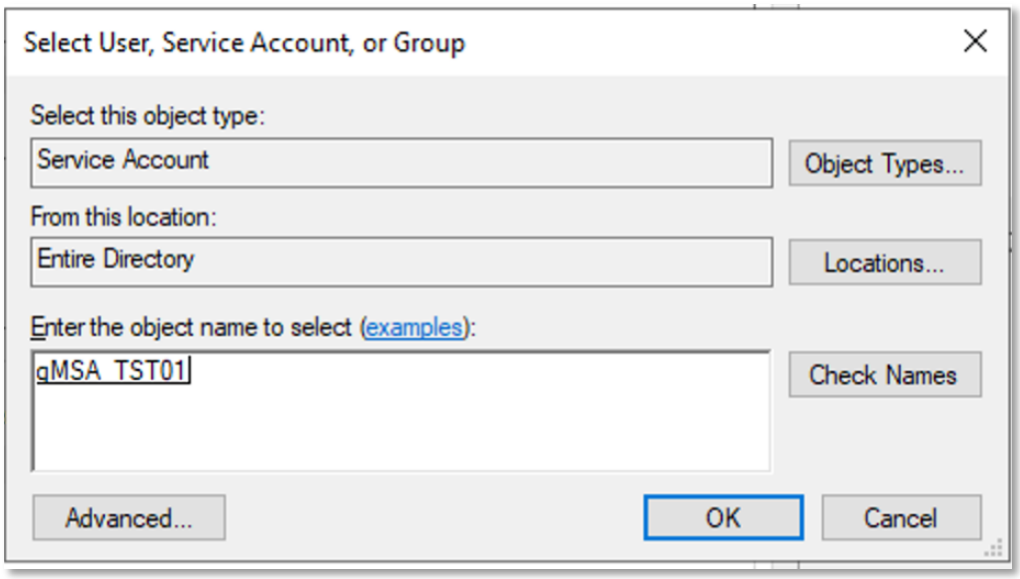
- *Open Task Scheduler (taskschd.msc)*
- *Create a task*
- *In the General tab choose Change User or Group*
- *Now click Locations*
  - *Select your Entire Directory*
- *Now click Object Types*
  - *Add Service Account*
- *And search for the gMSA account*
  - *And….Nothing, error*



- *This is very interesting bug. What you must do, is to uncheck all but Service Account Object Type:*



- *And you should be able to search for it now:*



  - *Funny, right?*

6. Now you should be able to use your gMSA account wherever needed. Of course you need to assign required permissions and privileges to it. Same way you would create just MSA, but I tent to always use gMSA, just in case. The difference is you can use gMSA on multiple target devices by specifying multiple targets in the parameter *PrincipalsAllowedToRetrieveManagedPassword*

7. **IMPORTANT**: If you are replacing service account with gMSA/MSA, which has been already used on some target device as a Service, there is still secret of the old service account stored in registry – you are able to extract the password in plaintext.

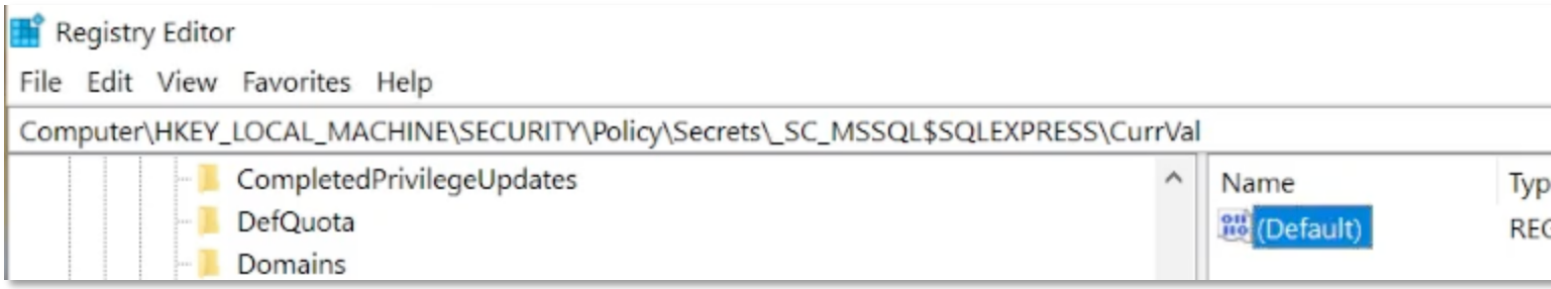
You can demo it with CQSecretsDumper.exe tool from CQURE company (run as System account):

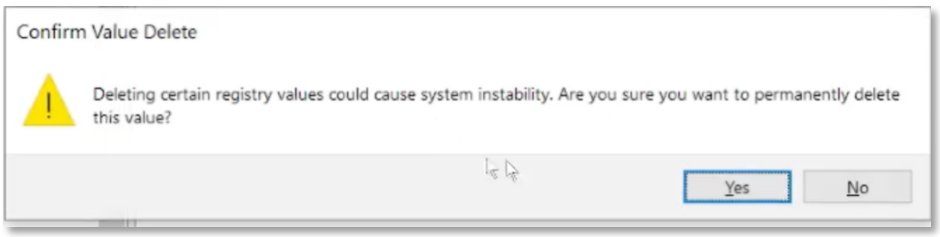
```
C:\Tools>CQSecretsDumper.exe /service MSSQL$SQLEXPRESS
Dumping data for: _SC_MSSQL$SQLEXPRESS
43 00 6F 00 6D 00 70 00 6C 00 65 00 78 00 2E 00   C.o.m.p.l.e.x...
50 00 61 00 73 00 73 00 31 00 32 00 33 00 2A 00   P.a.s.s.1.2.3.*.
```

- *As you can see there is a password visible, and it would be there, even if the service account is replaced in Services with the gMSA/MSA.*

You can remove the password. Again, you need to open Registry as System account and go to:

- *Computer\HKEY_LOCAL_MACHINE\SECURITY\Policy\Secrets_SC_MSSQL$SQLEXPRESS\CurrVal*
  - *Replace with your Service Name*
- *And delete the (default) REG_SZ there:*





🔒 Enjoyed This Resource?

I share real-world tactics for securing Windows infrastructure and Active Directory — no fluff, just what works.

Grab More Free Content:

📩 CyberSec Sunday Newsletter

Get a curated digest of the week's most important cybersecurity news, tools, and developments—all with my own insights.

➡️ https://horizon-secured.com/newsletter/

📚 Free Windows Security Resources

A growing collection of security guides, courses, tools and more !

➡️ https://academy.horizon-secured.com/