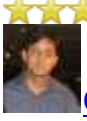
qUICKLY Explained: Managed Service Account

Rate This


Qasim Zaidi
24 Oct 2010 4:47 AM

- 2

Hi again, q here with more of the qUICKLY explained blog and this time how about we touch on user accounts in AD for the sole and exclusive purpose of running services on member servers and other devices on the network. These accounts are used for service isolation and provide a false sense of security while running these services. A big caveat is that these accounts are set with their passwords never to expire cause if the password expires, the service can no longer run and you would have to manually update the service using the now new password. This would cause a lot of maintenance work to prevent service outages not to mention that if someone has the account and password he can use it to logon interactively or gain access to resources. You will be surprised how many companies use user objects they call service accounts with password never expires set and membership of Domain Admins group.

Windows Server 2008 R2 provides a new class of accounts called **msDS-ManagedServiceAccount** or simply **Managed Service Account** (MSA). These class of accounts have automatic password management as well as other tasks such as Service Principal Names management. You can read about SPNs in my other blog of course qUICKLY Explained. So as I was saying MSAs do not require manual updates on the password and/or SPNs registered under the account. Now you are probably wondering, wow, cool, we can create a MSA for each type of service in the environment and assign these accounts to run those services, well, not quiet, cause while the purpose of MSA is exactly that, the current limitation is these accounts can only be installed and used on a single Windows Server 2008 R2 or Windows 7 machine. However, they still provide complete hassle-free password updating and SPN registration which means you as an administrator do not need to perform any action on them.

In order to use MSAs, your Domain Functional Level must be Windows Server 2008 R2 as these accounts are domain specific just like any user/machine accounts. This requirement is only for automatic SPN management so if your environment has Windows Server 2003 or Windows Server 2008, you can still use MSA but in this case only the password of the MSA will be managed automatically and not the SPN. So to take full advantage of MSA, make sure you have the following requirements met:

1. Domain Functional Level = Windows Server 2008 R2
2. Can only be used/installed on Windows Server 2008 R2 or Windows 7
3. Cannot be used/installed on more than one machine - no sharing allowed
4. Install Active Directory Module for Windows PowerShell (RSAT component of Windows Server 2008 R2 or Windows 7)
5. Microsoft .Net Framework 3.51

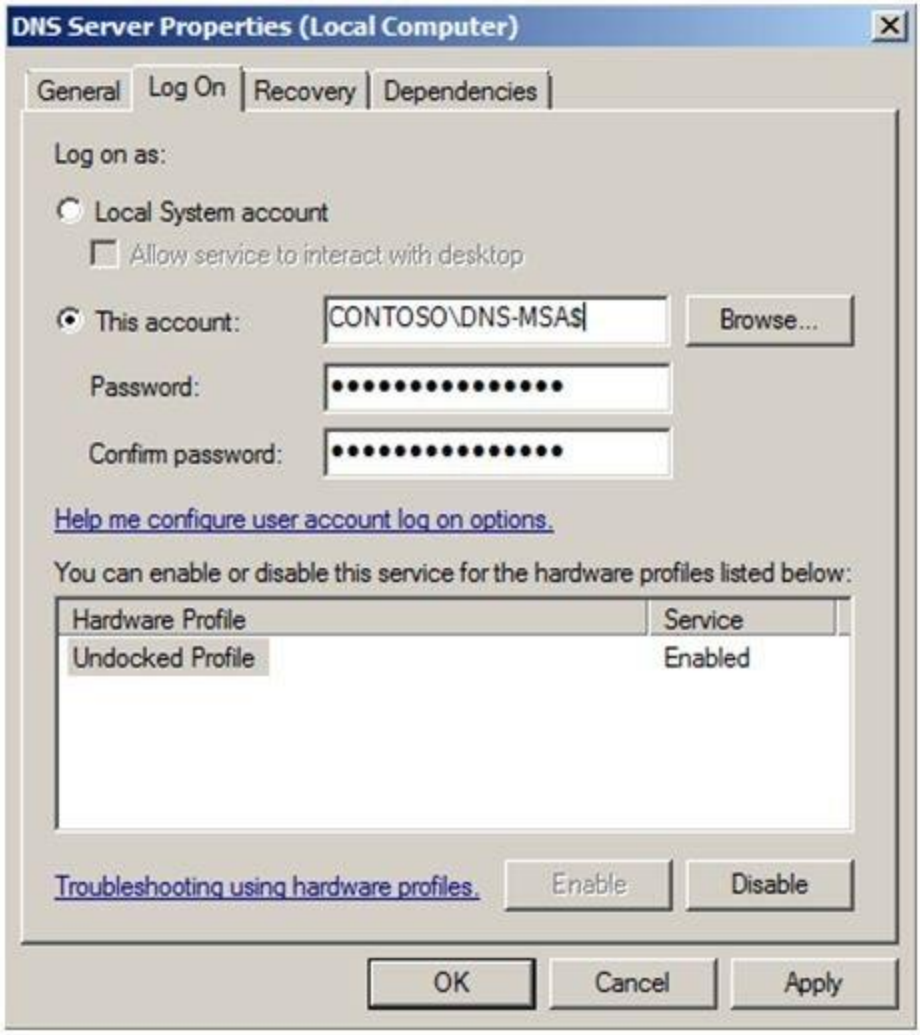
Windows PowerShell cmdlets should be used for creating, installing, resetting password, and uninstalling MSAs. To create an MSA, use **New-ADServiceAccount**. To install MSA on a member machine, use **Install-ADServiceAccount**. Use **Reset-ADServiceAccountPassword** to reset the password and **Remove-ADServiceAccount** to delete an MSA. Of course there are a lot of switches for these cmdlets for instance you can specify the -path parameter with New-ADServiceAccount <MSA_Name> to create MSA in a specific OU. By default all MSAs are created in "Managed Service Account" container.

Managed Service Account passwords are changed when either:

1. At the time the machine account password changes, 30 days default. This is defined via GPO "Domain Member: Maximum machine account password age" under "Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options".
The default is 30 days. The minimum supported value is 1 day.

2. Reset-ADServiceAccountPassword PS cmdlet is used or command nltest/sc_change_pwd:<domain> is used.

Once an MSA is created and installed on a member computer, you can use Services.msc to specify this account to run a service. Just remember to use a $ at the end of the MSA in the properties of the service.



-

[Managed Service Account], [MSA]