**How SPN’s (servicePrincipalName) work with SCOM**

*You are here:* [*Home*](http://www.culham.net) */ How SPN's (servicePrincipalName) work with SCOM*

August 12, 2013

***Categories:*** [*SCOM*](http://www.culham.net/category/scom/)

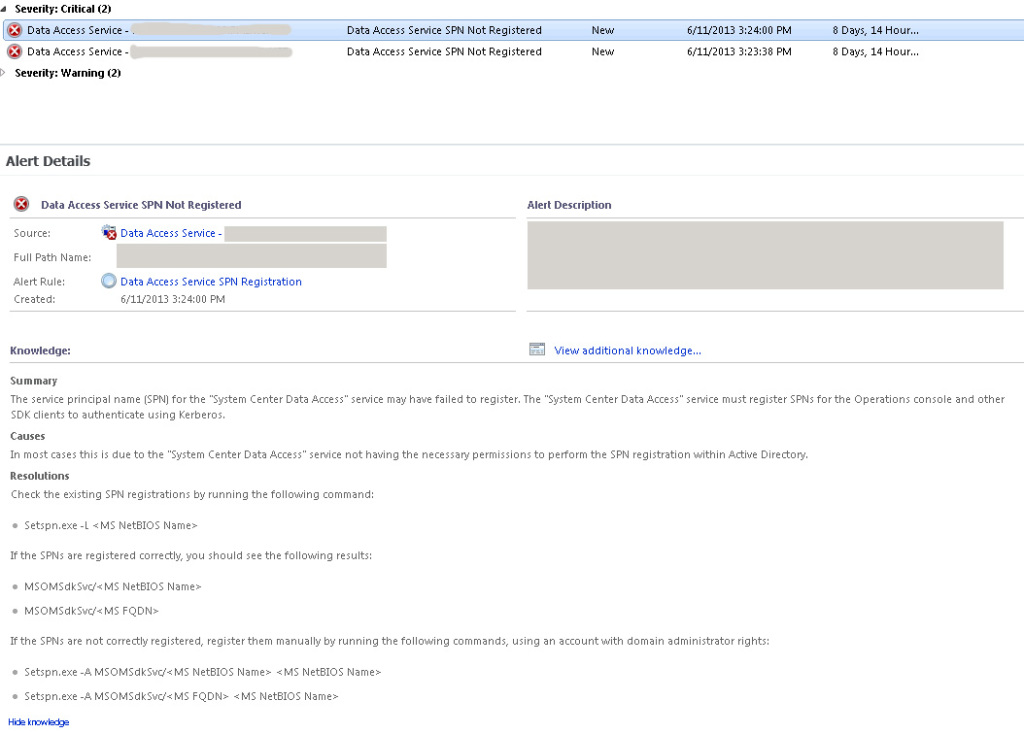
***Tags:*** [*Registered*](http://www.culham.net/tag/registered/)*,* [*ServicePrincipalName*](http://www.culham.net/tag/serviceprincipalname/)*,* [*SPN*](http://www.culham.net/tag/spn/)

Active directory User and Computer accounts and Groups are simply objects that exist in the Active Directory Database. These objects have attributes. Attributes can be things like “First Name”, “Last Name”, “Description”, “Telephone Number” and so on.

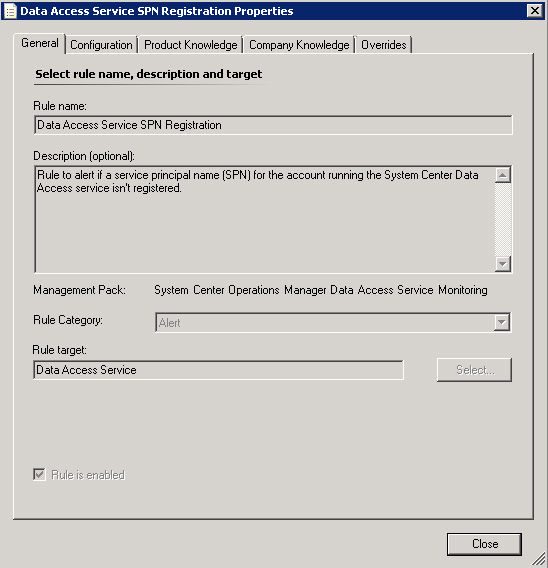
Computer and User accounts are rather similar in the way they operate on a Windows domain and they both share an attribute called servicePrincipalName (SPN). An account object can have multiple ServicePrincipalName attributes defined. Where SCOM is concerned, the job of the setspn.exe tool is simply to modify this ServicePrincipalName attribute for the Data Access Service (SDK) account.

So to illustrate how this affects SCOM, let’s assume that NO SPN’s have been registered for our SCOM Server server01.

This will result in the following Rule (Data Access Service SPN Registration) trigger an Alert in the SCOM console.

[](http://www.culham.net/wp-content/uploads/2013/08/SPN11-e1410148815109.jpg)

The rule is from the “System Center Operations Manager Data Access Service Monitoring” Management Pack.

[](http://www.culham.net/wp-content/uploads/2013/08/SPN21.jpg)

**Why SCOM complains without an SPN registered**

1. When a client wants to connect to a SCOM Management Server it asks a domain controller for a kerberos ticket to “MSOMSdkSvc/server01.thescomlab.com”
2. The domain controller looks in the Active Directory Database for the account object who’s ServicePrincipalName is “MSOMSdkSvc/server01.thescomlab.com”
3. The Active Directory Database in this case has no account objects with that servicePrincipalName (because it hasn’t been registered).
4. So the domain controller looks in the Active Directory Database again for the account object who’s servicePrincipalName is SERVER01/server01.thescomlab.com“
5. All computer accounts have, by default servicePrincipalName attributes set to: HOST/[computername] and HOST/[computername].[domain]
6. So the Active Directory Database replies to the domain controller: With the Computer Account object that has that servicePrincipalName of server01.thescomlab.com.
7. The Domain Controller now creates a Kerberos Ticket that only the computer account of server01.thescomlab.com can read. That ticket is given to the Client requesting it.
8. The client goes to the DAS (SDK) service on server01.thescomlab.com and presents the ticket which allows it to authenticate.
9. The DAS service will attempt to read the ticket. The problem is, the SCOM DAS service is not running under the computer account; it is running under a domain service account (unless the DAS Service is using Local System). It cannot read the ticket; the ticket is only intended for the computer account of server01.thescomlab.com. Authentication fails (and falls back to NTLM authentication until the issue is resolved).

**So we need to Register the SPN to fix this problem**

So the commands that would need to execute for SCOM are as follows:

setspn -a MSOMSdkSvc/server01 thescomlab\s-scomdas  
setspn -a MSOMSdkSvc/server01.thescomlab.com thescomlab\s-scomdas

\* where (s-scomdas is the name of your das/sdk account)  
\*\* We run this command twice so that we’re able to access the server using the hostname and the FQDN.  
\*\*\* These commands will need to be run under Domain Admin Credentials.

On a Windows 2012 Server, we’ll use -S instead.

setspn -S MSOMSdkSvc/server01 thescomlab\s-scomdas  
setspn -S MSOMSdkSvc/server01.thescomlab.com thescomlab\s-scomdas

**This will now work with an SPN Registered**

Now if we run through the scenario again, this time the Domain Controller will return a ticket that the Data Access Service (DAS/SDK) Account on the Management Server can read.

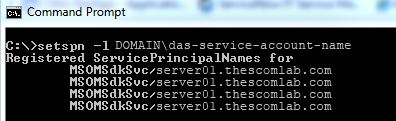
This is why we need to set the SPN attribute on the Account that runs a given service in order for authentication to work properly.  Of course if the service runs under the local NetworkService or LocalSystem account then everything will just work because these local accounts represent the computer account in active directory.

**How do we verify that an SPN is Registered?**

We can run the following command:

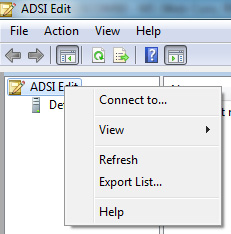
setspn –l domainaccount

\* This does not require Domain Admin credentials to run this command as we’re not modifying anything.

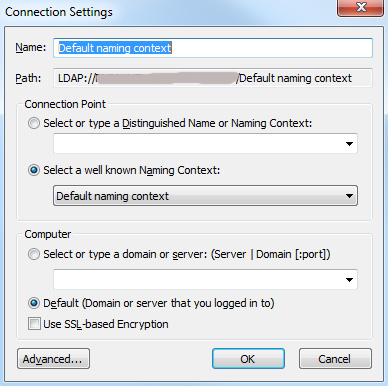
[](http://www.culham.net/wp-content/uploads/2013/08/SPN31.jpg)

 We can also verify this using the ADSI Edit utility.

Run ADSI Edit and right click on “ADSI Edit” and choose “Connect to”

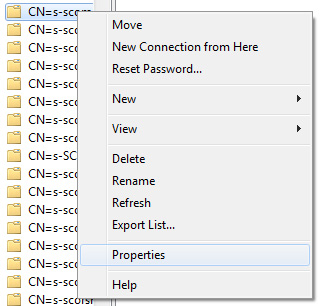
[](http://www.culham.net/wp-content/uploads/2013/08/SPN41.jpg)

 We can connect to the default naming context or a specific name if applicable.

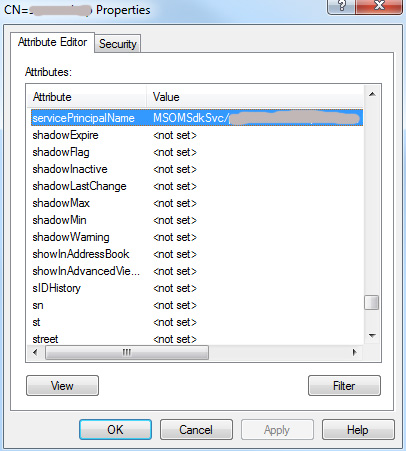
[](http://www.culham.net/wp-content/uploads/2013/08/SPN51.jpg)

We’ll need to locate the appropriate object. A hint, you’ll find where the object is stored if you look at the output of the setspn –l command…it will show you the Distinguished Name…we’ll read from Right to Left so we’ll navigate through the Domain (DC), OU’s and locate the object from its Common Name (CN).

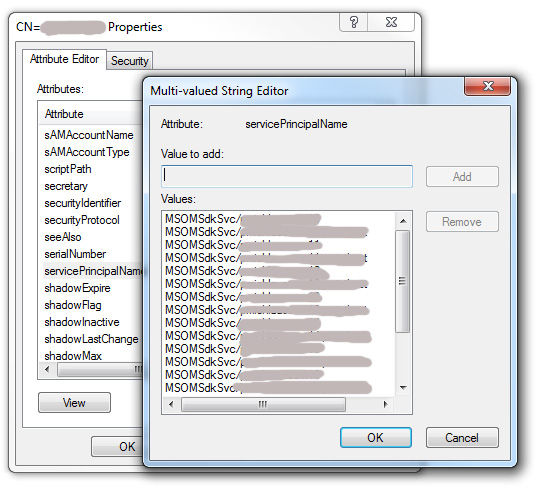
We’ll right click on the service account and choose “Properties”.

[](http://www.culham.net/wp-content/uploads/2013/08/SPN61.jpg)

Locate the ‘servicePrincipalName’ attribute and click the “View” button:

[](http://www.culham.net/wp-content/uploads/2013/08/SPN71.jpg)

And you can see the registered values:

[](http://www.culham.net/wp-content/uploads/2013/08/SPN81.jpg)

So if these values are not correct or servers are missing, you’ll need to go back and add them using the setspn command (with the appropriate Domain Admin credentials of course).

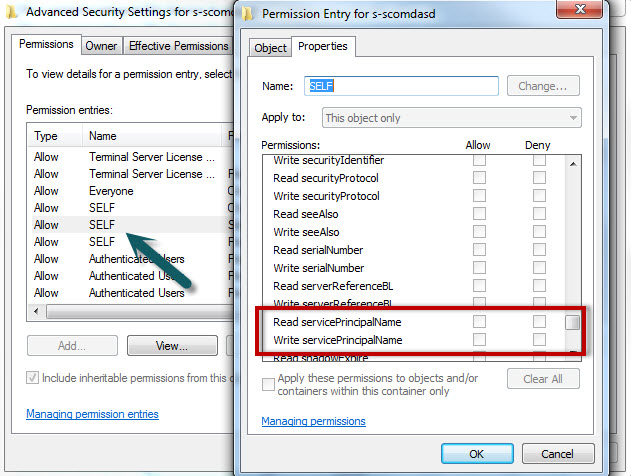
Note:

On the subject of SPN’s…check out Kevin Holman’s blog where he discusses SPN’s where System Center Operations Manager SDK service failed to register an SPN.

<http://blogs.technet.com/b/kevinholman/archive/2007/12/13/system-center-operations-manager-sdk-service-failed-to-register-an-spn.aspx>

<http://blogs.technet.com/b/kevinholman/archive/2011/08/08/opsmgr-2012-what-should-the-spn-s-look-like.aspx>

If you’re getting this error you might wish to grant permission for your DAS-Service-Account to read/write the servicePrincipalName attribute in AD. You can use Active Directory Users and Computers and locate the DAS-Service-Account object and grant SELF to have Full Control. Or you can use ADSI Edit for this (with the appropriate Domain Admin credentials) and set the specific permissions directly on the DAS-Service-Account.

[](http://www.culham.net/wp-content/uploads/2013/08/Read-Write-servicePrincipalName1.jpg)