How to Use SetSPN to Set Active Directory Service Principal Names

A common configuration step when establishing a Kerberos authentication method is the use of a **Service Principal Name**, or **SPN**, to identify a specific service. This article shows you how to specify a user or computer account to be identified with that specific service by using the **SetSPN** utility.

First things first: SetSPN is a built in utility with Windows Server 2008 and Server 2008 R2. You don't have to download SetSPN to use it. It's already part of your operating system on both workstations and servers.

Note: While SetSPN can be run from either a workstation or a server, don't run it from domain controllers. Use SetSPN from either a member server or a client system to assign Service Principal Names to a user or computer account.

We're talking about SetSPN, not to be confused with a Sit 'n Spin. (Image via Imremembering)

What Is an SPN?

An SPN is a reference to a specific service, for example, an instance of SQL or a web application run by IIS. Since SPNs are specific, they reference not only what the service is (such as an SQL server), but also which hostname runs the instance and on which port it's running (however, you don't have to specify the port if running on default ports).

Service Principal Names are already in use for every computer and user account. Though not usually seen, there is a default SPN established at the time of account creation which is identified as the SAMAccountName with a Dollar Sign appended to it. Therefore, JoeUser@contoso.com would have a Service Principal Name of Contoso\JoeUser$ which is referenced by the domain during authentication and ticket granting.

When Should You Set an SPN?

Service Principal Names are not always necessary. Again, using the SQL Server as an example, once the SQL instance is established, a web application that uses the databases in the instance may point directly at the server. In that case, an SPN is not required, because there is no confusion about where the authentication is going to take place or where the service is located. However, in some cases you do not reference the SQL Server by direct name.

Why R2? Storage Quality of Service

Another time that you may need to configure SPNs through the use of SetSPN is when using Kerberos to connect to a web application. In many cases, web applications running on IIS 7.5 will be using Kernel Mode authentication and will not require the use of SPNs to authenticate properly. But not all use cases can take advantage of Kernel Mode Authentication: SharePoint 2010 is an example of a web application that does not support Kernel Mode Authentication, even when running on IIS 7.5.

There are more use cases published by Microsoft that provide examples of when you will need to set a Service Principal Name with SetSPN.

How to Set an SPN for an Active Directory Account

The easiest way to set the Service Principal Name for an Active Directory account is by using the SetSPN utility. It's really easy to use once you know how, so here are some examples to show you what I mean:

```
SetSPN –a HTTP/myweb.contoso.com  contoso\MyWebAppPoolID
SetSPN –a HTTP/myweb   contoso\MyWebAppPoolId
```

This sets the SPN for a web application to the service account that is used for the Application Pool Identity. You need to include the hostname of the web application as well as the fully qualified domain name (FQDN) of the web application, so you'll insert two entries.

This next example shows how you will set it for a Configuration Manager Database server.

```
SetSPN –a MSSQLSvc/sccmdb1.contoso.com:4000 contoso\SQLService_SCCM
SetSPN –a MSSQLSvc/sccmdb1:4000 contoso\SQLService_SCCM
```

Just like the first example, it uses two entries: the NetBIOS name and the FQDN are both set as SPNs.

SetSPN.exe Switches and Syntax

You may have noticed the "-a" switch used on the previous examples. SetSPN can be used with no switch, but then it doesn't set an SPN, it displays them.

SetSPN contoso\SQLService_SCCM

This example displays all SPNs that have been set on the SQL service account. Here are the most common switches used with SetSPN:

-a Add an entry to an account (explicitly)
-s Add an entry to an account (only after checking for duplicates first)
-d Delete an entry from an account

-x Search the domain for duplicate SPNs
-q Query the domain for a specific SPN

There are also a few switches that specify whether an account is a computer or user (-c and –u), but if you omit those you're likely all right, as it will check for computers first and then check for users. If in your domain environment you have computers and users that share account names, then you will want to use the –u switch to modify user accounts.

But Wait... That's Not All!

Here are a few notes that may come in handy when dealing with Service Principal Names.

- SPNs should be unique within the domain. If you set an AD account to have an SPN, do not set it on another account. This goes for the SPN being set on multiple computers, multiple users; it will also not function properly if there is both a user and a computer account that have the same SPN.
- You can search for SPNs in the domain by using the –q switch. This will tell you if there is already an account that is using that SPN. For example:

```
SetSPN –q HTTP/MyWeb.contoso.com
```

- And if you need to troubleshoot a problem with an SPN, a good place to start is by verifying that there are no duplicate entries:

```
SetSPN –x
```