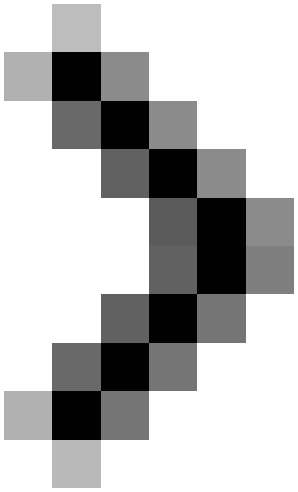
Troubleshoot problems with Kerberos in SharePoint - Part 2

In this part 2, I will show you how to configure SPN, Duplicate Service Principal Names, and dislocation in DNS configuration.



Troubleshoot problems with Kerberos in SharePoint - Part 1
Jesper M. Christensen

Network Administration - In this part 2, I will show you how to configure SPN, Duplicate Service Principal Names, and dislocation in DNS configuration.

In the first part of this series, we discussed the date and time issues, application accounts, and the basic Service Principal Name (SPN) configuration. In this section, we will introduce the following topics:

- Configure SPN - for IIS 7
- Duplicate Service Principal Names
- Incompatibility DNS Configuration

Configure SPN - for IIS 7

In the previous section of this article, there are a number of issues we mentioned that cannot use websites that work with Kerberos if they use Internet Information Server 7 on Windows Server 2008. Application accounts and SPN registrations correct configuration, but this error message still appears in the system event log - Windows System Event Log: KRB_AP_ERR_MODIFIED.

This problem occurs because kernel mode authentication is enabled by default. You should normally use a SharePoint server and register the SPN to the NETBIOS servers. However, in a web system, you need to disable authentication in Kernel mode or configure the application to be able to use permissions from the application.

Let's take a closer look at our environment from part 1 used as an example.

Information about IP addresses:

172.16.189.11 is the domain controller (and KDC) **DC1**
172.16.189.15 is SQL Server (and KDC) **SQL1**
172.16.189. Is the website **http:///intranet.domain.local**
172.16.189.21 is SharePoint Server **WSS1**
172.16.189.22 is SharePoint Server **WSS2**
172.16.189.101 is **PC1** computer accessing website

We have disabled the kernel authentication mode in our environment for this test, you can enable it again (as its default mode) in Internet Information Manager 7:

1. In IIS 7 Manager, select 'Sites / 'and select' Authentication '.

Figure 7

2. Select 'Windows Authentication' and click 'Advanced Settings'

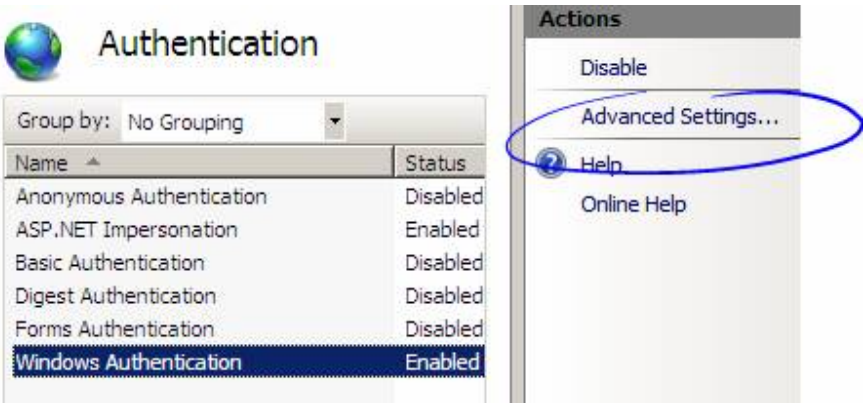


Figure 8

3. Check the 'Enable Kernel-mode authentication' checkbox, which is also the default setting

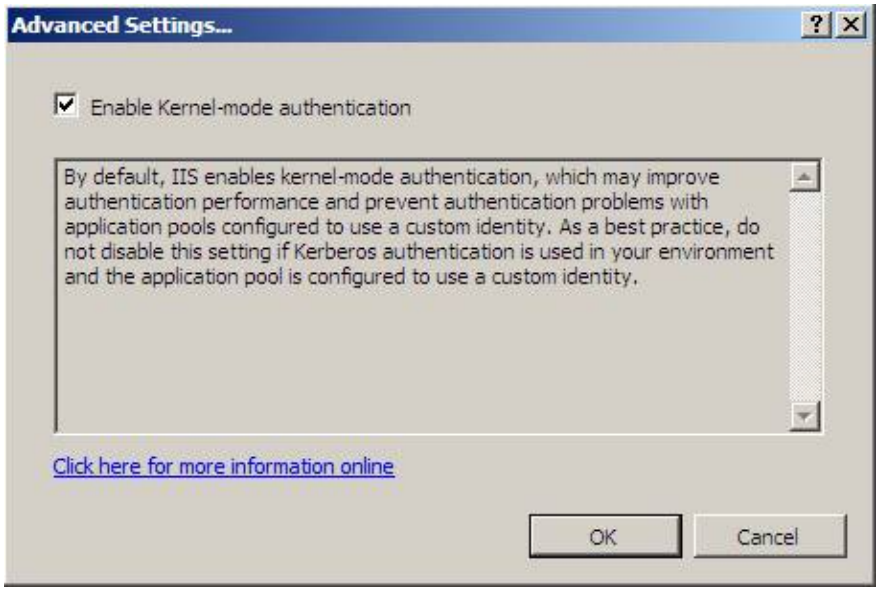


Figure 9

4. Then reset IIS using the command: **IISRESET / NOFORCE**

We want to see more details about the package, so before you access the website, you need to launch Wireshark, this is a network protocol analysis on DC1 and PC1 so we can study it. Kerberos errors on. We recommend setting up a filter to display only Kerberos packages:

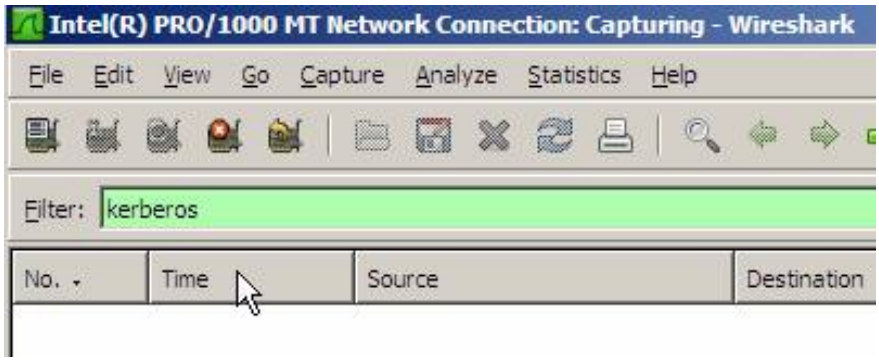


Figure 10

Now we will access the website: **http:///intranet.domain.local** - here, we will see a registration box because the login attempt failed. The first step is to check the event log on the computer accessing the website. This is an event from the Windows System Event Log on the computer accessing the website that was checked on PC1:

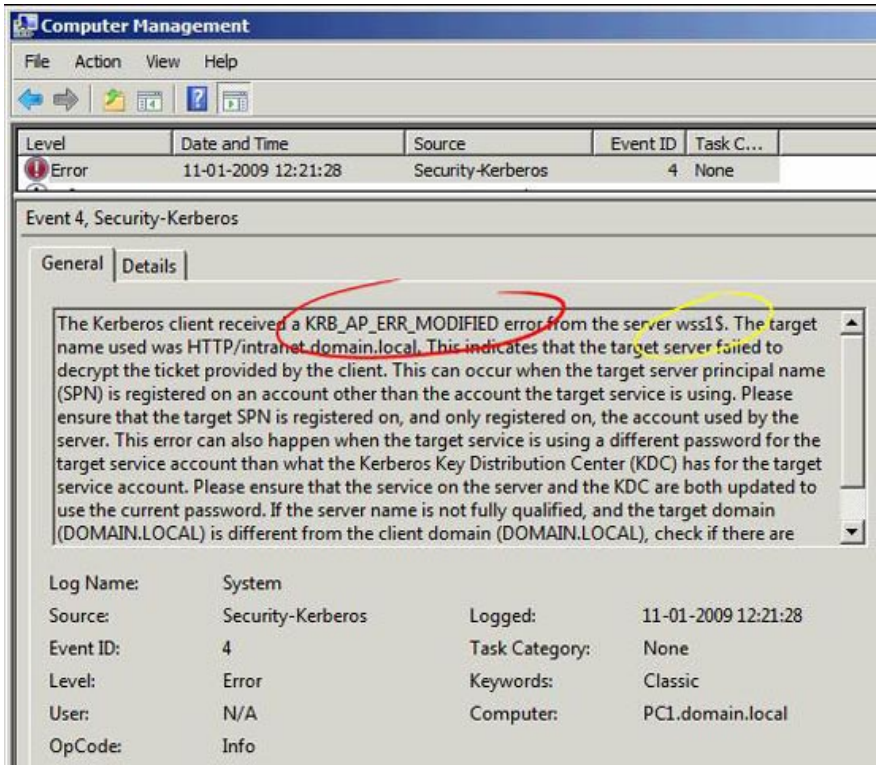


Figure 11

If you look at the packets and errors captured on PC1 with Wireshark, we will see the same errors:

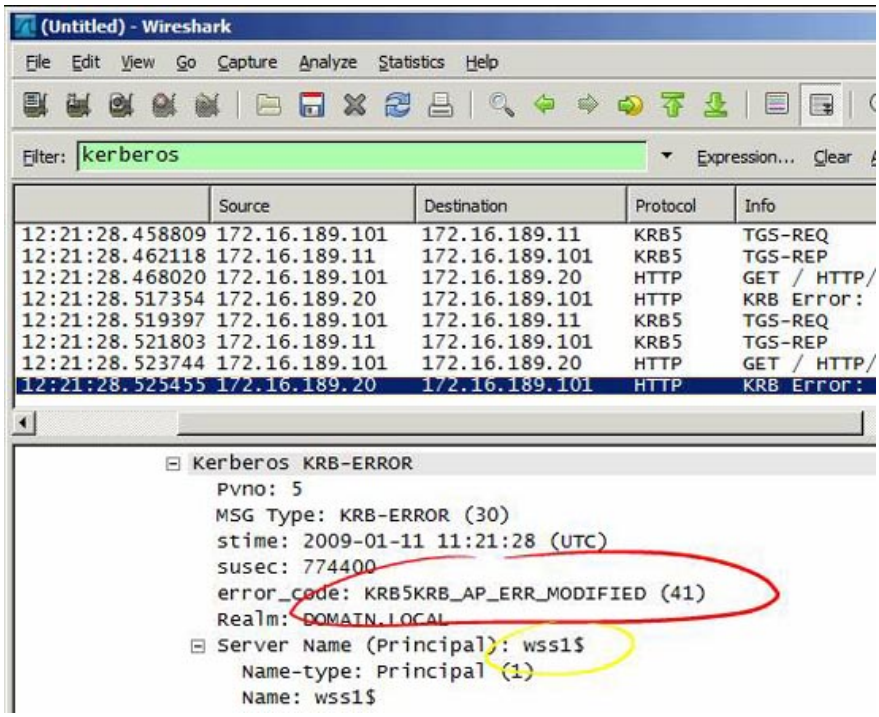


Figure 12

What we can see, in both the event log and captured packets, is to indicate the KRB_AP_ERR_MODIFIED error code and the responding account is wss1 $. Know that the WSS1 server reports this error when we access the website. We can also see that from the IP address if we look at the source and destination IP address information in Wireshark. Please observe on this server. KRB_AP_ERR_MODIFIED means that the computer assumes that the Client / Service exchange package seems to be changed and the parameters checked are the date, IP address, hostname and decryption key whether or not to work. Quickly check date / time, IP addresses and hostnames (see DNS configuration section) and assume the truth is correct. Encryption and decryption keys are determined by SPN account mapping. This account must be an IIS website account on the currently used WSS1 server.
We will check that issue with the following command:

Figure 13

The Service Principal Name maps the domain account SPContentPoolAcct and allows us to check the IIS Application Pool that the website uses. In the IIS manager, navigate to the Application Pool used in the IIS Website. Then check Advanced Settings - Figure 14 shows the account is properly configured.

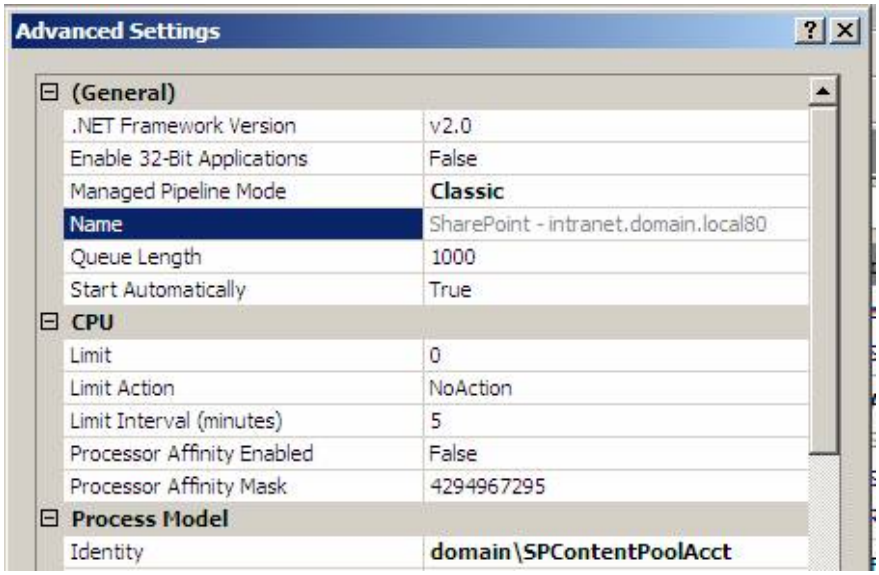


Figure 14

Because the new structure in IIS 7 on Windows Server 2008 should be used only if Kernel mode authentication is disabled or the master configuration is changed.
We check and edit the configuration file using this method:

1. First open the configuration file on the SharePoint server: **% WinDir% System32inetsrvconfigApplicationHost.config**
2. Then check that the useAppPoolCredentials setting is present. Otherwise we need to add the same attributes as in the example highlighted by the green below.

   useAppPoolCredentials = "true" />

3. Finally, reset Internet Information Server from the command prompt:
   IISRESET / NOFORCE

Now we can access the website again without prompting for login or event log errors. With the log, we only include the details of the protocol captured from the **PC1** client:

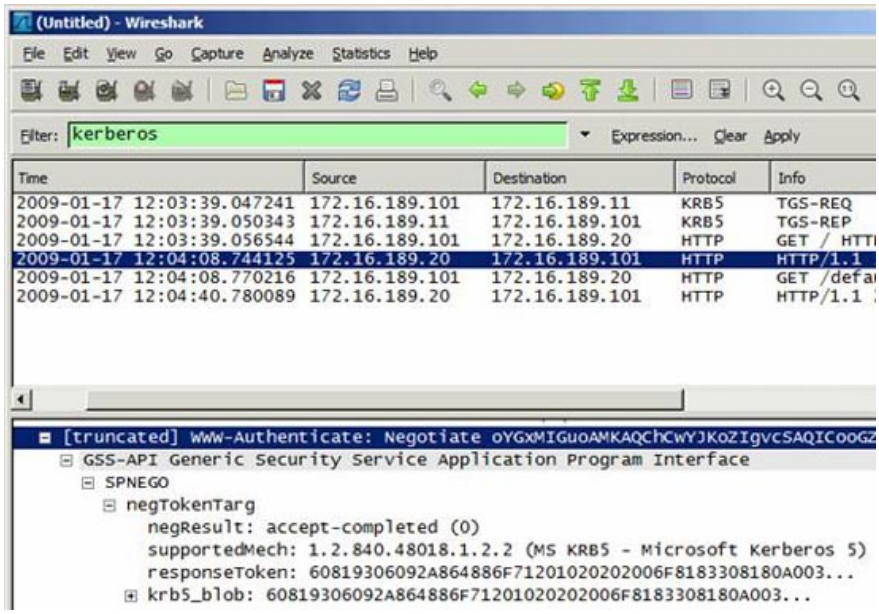


Figure 15

Check the Service Principal Names replication

It's easy to create a replicated SPN in Active Directory unless you use setspn.exe with the '-S' or '-F' switch (only applies to setspn.exe in Windows Server 2008 or higher). For a better understanding of how Service Principal Names are saved and how the KDC blocks SPN-based accounts. We have shown by the diagram in Figure 16. The example of a replicated SPN registered in SPWrongAcct is highlighted in red.

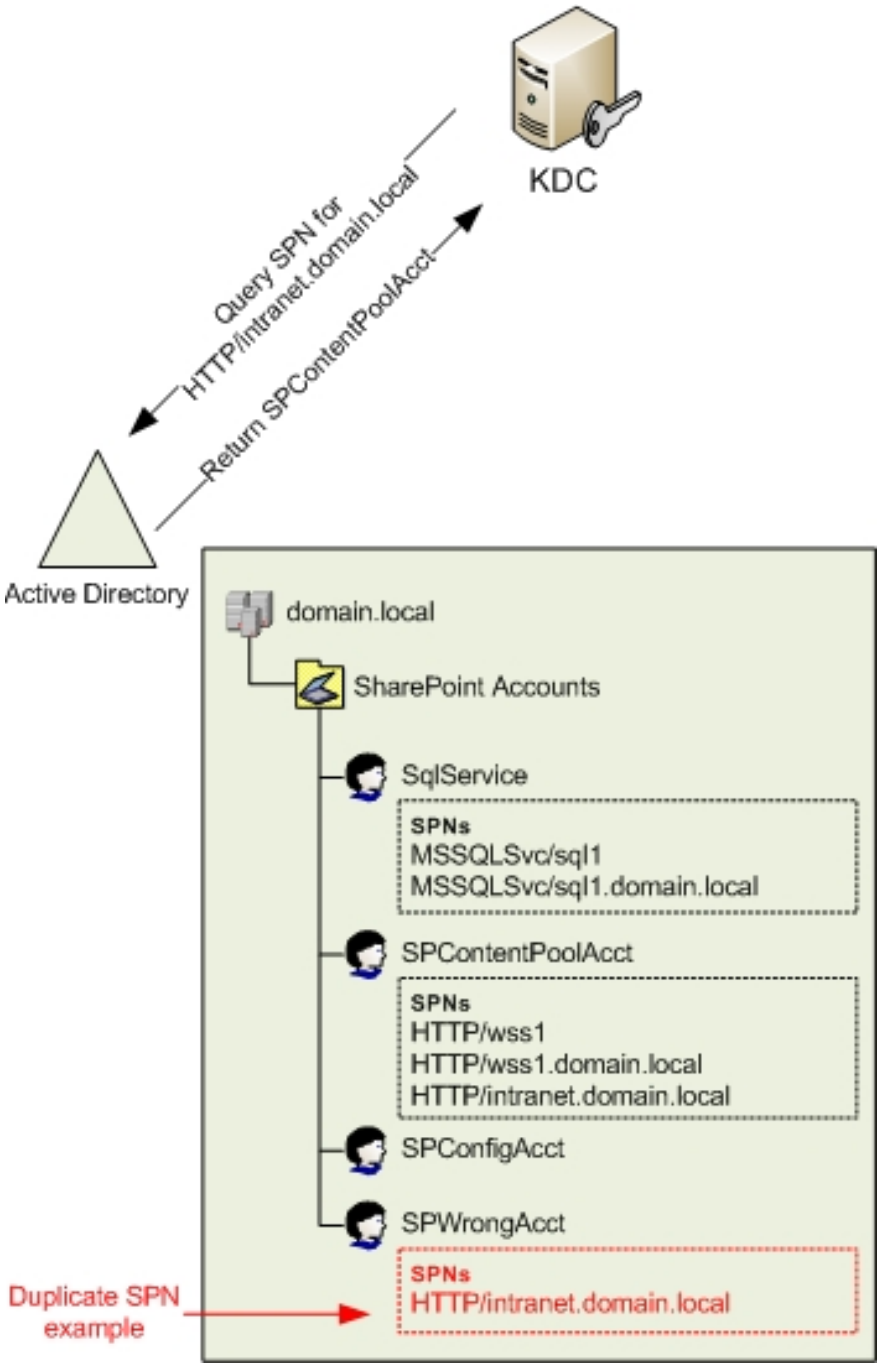


Figure 16

The SPN replication can make the intermittent error messages indicate KRB_AP_ERR_MODIFIED, because KDC can encrypt the service tag with the public key of the SPN account - possibly another account that the application uses to decode. data package. Checking for duplicate SPNs is recommended in any environment and can be done in several ways.

- ldifde - extract the SPN directly and filtered from Active Directory.

?ang l?y tài kho?n ? khi HTTP SPNs ???c xác ??nh:
ldifde -d "dc = domain, dc = local" -r "servicePrincipalName = http *" -p subtree -l "dn, servicePrincipalName" -f output.txt

Getting accounts where the MSSQLSvc SPNs is defined:
ldifde -d "dc = domain, dc = local" -r "servicePrincipalName = mssqlsvc *" -p subtree -l "dn, servicePrincipalName" -f output.txt

- setspn.exe - on Windows Server 2008 can check the mirror

  Getting the account where a HTTP SPN is defined:
  setspn.exe –Q http / intranet.domain.local

  Hãy ki?m tra cho m?t ph?n m?m HTTP ???c ??ng vào nhi?u các tài kho?n (duplicate SPNs):
  setspn.exe –X http / intranet.domain.local

- ADSIEdit - usually enters through user accounts and computers in turn and checks that the value does not exist on multiple accounts. This method is difficult so we choose one of the other methods.

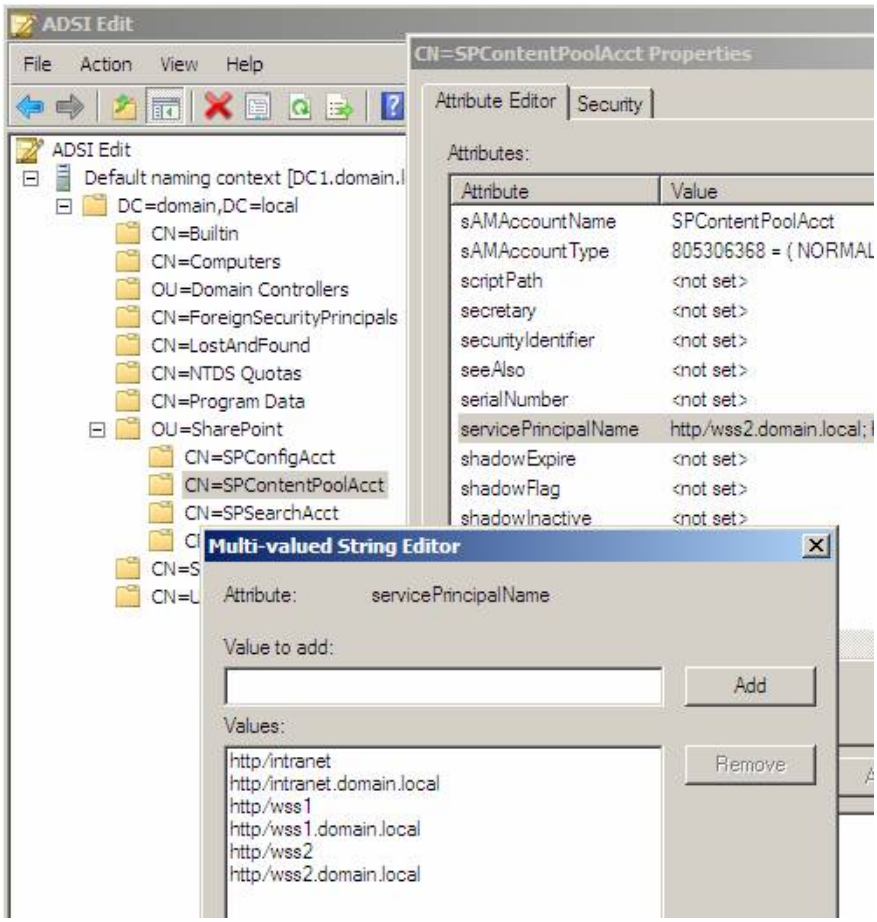


Figure 17

The thing to look for in the output of any of the above procedures is that SPN (such as HTTP / intranet.domain.local) is not listed on other accounts (only one account). The account itself may have multiple SPNs listed without problems (see Figure 17).

We recommend using the following commands if running Windows Server 2008:

- ' **setspn.exe –S** ' for registering an SPN on an account and checking for domain replication
- ' **setspn.exe –F -S** ' for registering SPNs on an account and checking for duplicates in the forest.

We have used images in the process of checking duplicates and configuring the Service Principal Name (Figure 18) for the DOMAINSPContentPoolAcct account

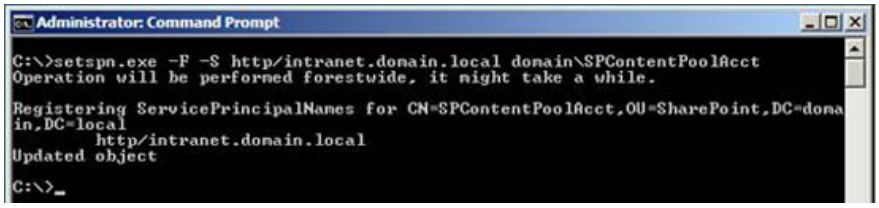


Figure 18

The next figure shows an action to create a replicated SPN. setspn.exe in this replication is shown in Figure 19 and it also tells you which Active Directory object it conflicts with.

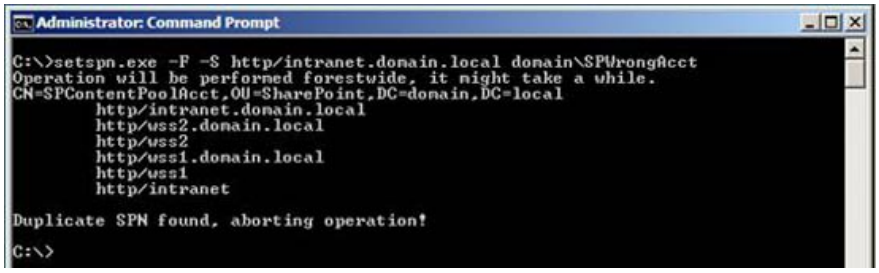


Figure 19

Configure DNS

A solid DNS configuration must be compatible with all domains today and when using Kerberos, this is not an exception. All hostnames must be created in reverse lookup zones and no duplicates on hostname or IP address are acknowledged. In the forward lookup zone, the records need to be created as A-records - also the host header names that point to the servers. If CNAME is sometimes used then Kerberos will construct tags using the wrong hostname - basically a rule to practice in configuring DNS to make sure it works.

Information sent and received will be checked by both forward and reverse lookup areas. We will test our configuration first to see if the DNS responds properly to our hostname.

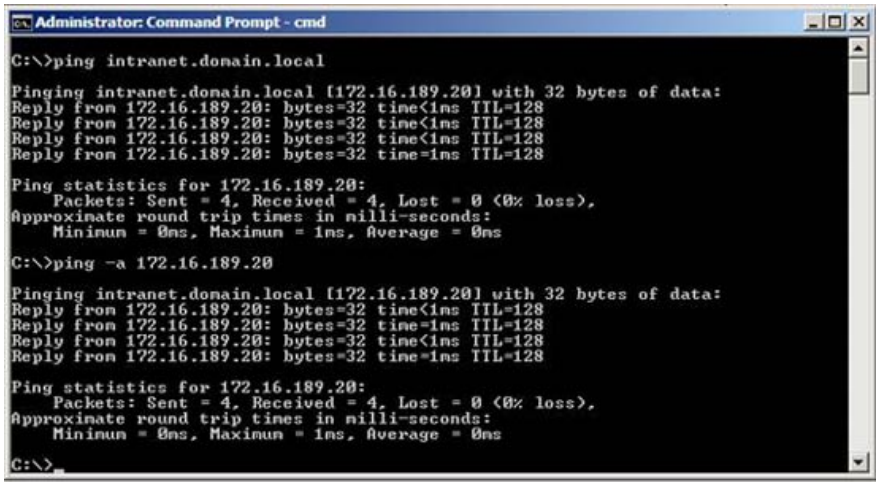


Figure 20

Both commands need to return the correct host-name and IP address - but the best idea is to manually check the DNS configuration. You need to ensure that all hostnames in the installation (servers DC1, SQL1, WSS1 and PC1) and used host-headers (intranet.domain.local) are created and unique. Below are the images from the DNS configuration process shown in Figure 21 and 22.
The lookup zone is convenient for domain.local:

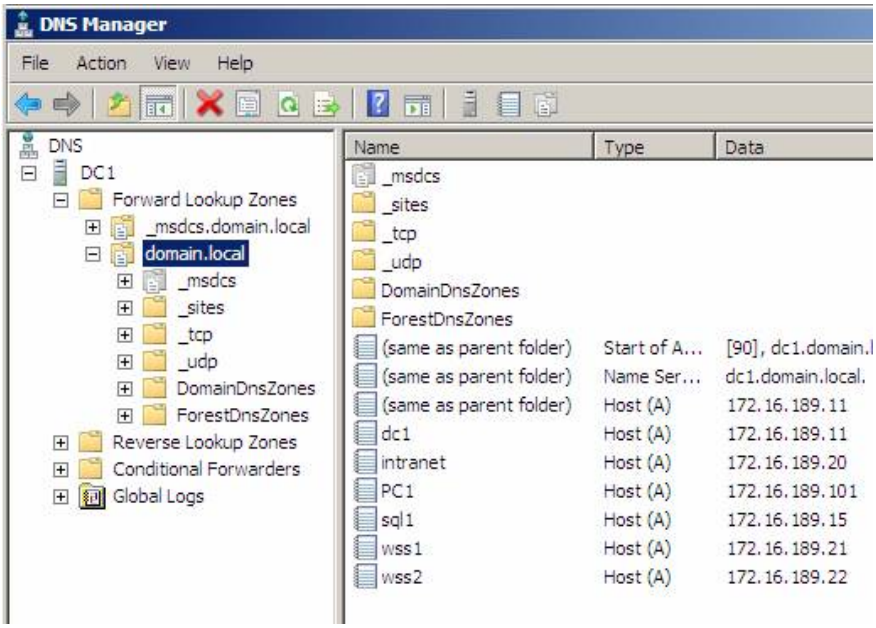


Figure 21

The reverse lookup zone for domain.local:

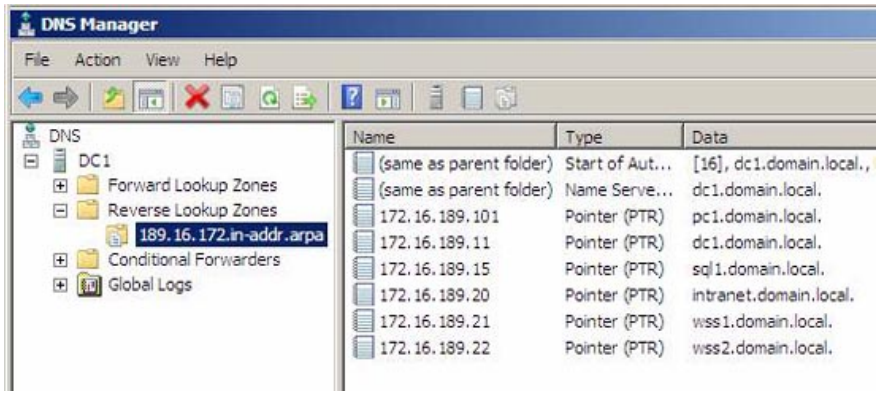


Figure 22

Conclude

So far, we have covered most of the components of typical errors in SharePoint and Kerberos such as DNS configuration, replication of SPN and IIS 7 on Windows Server 2008. In the third part of this series We will introduce more about the tags and see what information we can use from there. We also introduced the delegation and Shared Service Provider according to how it works, creating errors and analyzing and then correcting errors.