Kerberos in Sharepoint environment

In this article, I will show you some basics to use Kerberos in a Sharepoint environment. You will find many configuration instructions for different scenarios and some tips here and we hope this article can provide you with an overview of your own environment.

Jesper M. Christensen

Network Administration - Microsoft Windows Sharepoint Services (WSS) 3.0 and Microsoft Office Sharepoint Server (MOSS) 2007 are designed to focus information and help team members collaborate effectively. Users can access all the information in individual accounts if allowed from the Sharepoint website.

In this article, I will show you some basics to use Kerberos in a Sharepoint environment. You will find many configuration instructions for different scenarios and some tips here and we hope this article can provide you with an overview of your own environment.

Using Kerberos in Sharepoint?

Kerberos is a secure protocol that allows tabbed authentication if the client request to the Key Distribution Center (KDC) has valid user certificates and service names - Service Principal Name (SPN) Invalid. Kerberos is the preferred type of authentication in Sharepoint because of its speed, more security and reduced number of errors with usernames and passwords than NTLM. If the Sharepoint website uses external data (located on servers other than your Sharepoint server) for the SQL database through the webpart, then the server needs Kerberos to delegate client certificates.

So what happens between the client and the server when you access a website that allows Kerberos? We have created an overview summary to show what will happen behind the script. This scenario shown in Figure 1 is created from Windows Sharepoint Services 3.0.

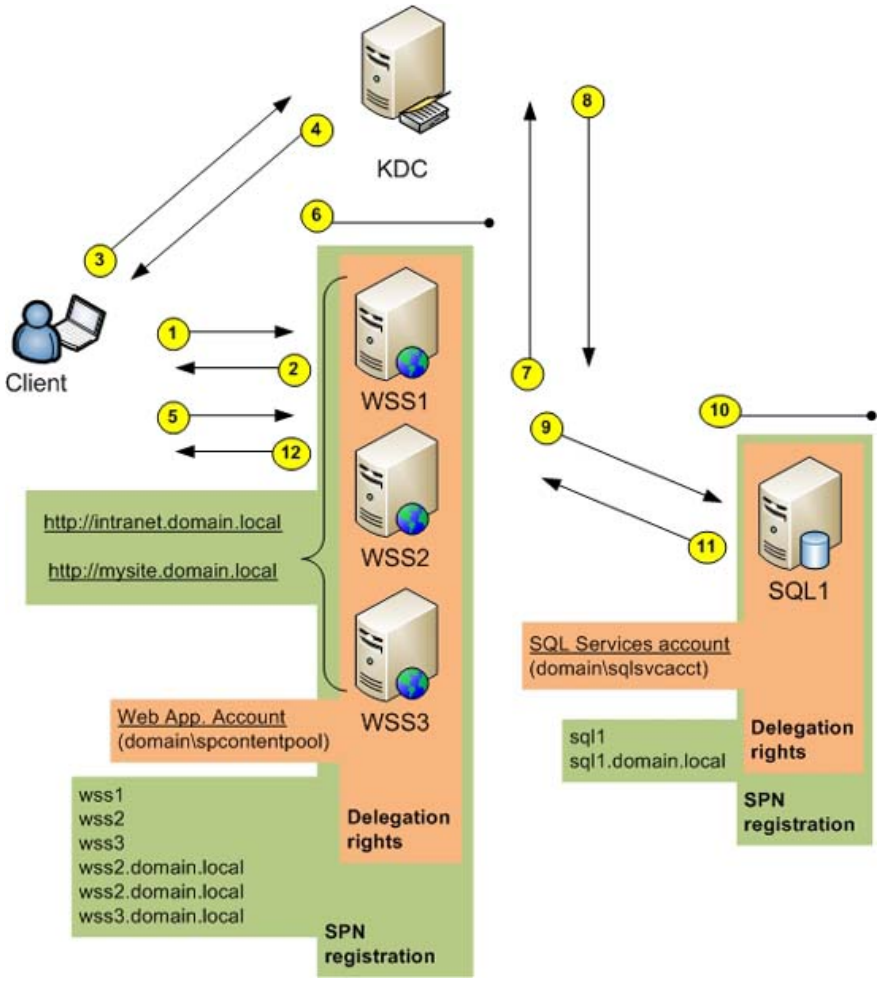

Figure 1: Kerberos in Sharepoint flow

1. The client accesses http:///intranet.domain.local with anonymous certificates
2. WSS Server returns an IIS error 401.2 error but also returns a WWWAuthenticate header.
3. The client requests the card for the SPN created by the internal Internet browser: HTTP / intranet.domain.local
4. KDC returns the card if the SPN is detected. This is encrypted with the account holder key registered for SPN (domainspcontentpool).
5. Client appraises with the card for the web application.
6. Web App account decodes the card and validates it.
7. Web App account requires card for SPN created by SQL Client: MSSqlSvc / sql1.domain.local: 1433.
8. KDC returns the card if the SPN is found. This is encrypted with the master key of the account registered for the SPN (domainsqlsvsacct).
9. Service appraisal web application with the QLS database with the web application account card and play the user with credentials.
10. SQL service account decodes the card and validates it.
11. SQL Server returns the requested data for WSS Server.
12. The WSS Server returns to the webpage.

If Kerberos is not configured for SQL communication, jump from step 6 to step 12. Remember that allowing the tag to happen only at the first login and until the timeout.

Configure Kerberos for Sharepoint

First we recommend that you create a test installation before reconfiguring the production environment. Knowing this problem will be difficult for you, but if you have virtual servers, you can build test servers quickly and easily. This also allows you to compare the final configuration if something does not work as expected.

Therefore, we need to remove NTLM on our web applications and configure it to use Kerberos. First you disable this communication protocol between frontend and backend servers. Then enable Kerberos between clients and separate web applications to manage authentication through Sharepoint servers (you can call it dual- or double-hop authentication).

Consider the list that needs to be done for these settings.

1. Collect the necessary information and create Sharepoint users
2. Enable Kerberos for SQL communications
3. Configure Service Principal Names (SPNs) in Active Directory
4. Configure 'trust trust' for computer and user accounts
5. Configure *Component Services* on Sharepoint servers
6. Enable Kerberos for web applications and Shared Service Provider (SSP)
7. Test Sharepoint environment

Collect the necessary information

To make it easy and harmless for operating systems, we need to have all the blocks ready. Suppose your environment is running Active Directory and each server has a unique IP address. This must be registered in the DNS server and no duplication exists in the forward and reverse lookup regions for Kerberos to work. In addition, all servers and clients must be set in time as Kerberos uses to validate tags and access for internal DNS servers.

Before installation, Sharepoint will create appropriate users in Active Directory. If you have created these necessary accounts, read the following sections.

This is a list of essential information for Kerberos setup in a Sharepoint environment.

1. Service class of SPN
2. (HTTP for WSS / MOSS web applications. MSSQLSvc for SQL Server by default)
3. Host name of SPN
4. Fully Qualified Domain Name (FQDN) for all wen applications and servers
5. Your port number or SPN (there are no ports for WSS and MOSS web applications. 1433 for SQL).
6. Active Directory accounts for SPNs (services and application accounts)

Enable Kerberos in SQL communications

Microsoft recommends taking this step before installing Microsoft Sharepoint to ensure that the SQL communication will work. The configuration database is located in the SQL server and if the connection is broken, you need to fix it before the Sharepoint sites are set up and run again. If you change the authentication after initial installation, you must turn off Sharepoint services to avoid losing data.

Enable Kerberos between Sharepoint frontend servers for your SQL server by:

1. Configure SPN
2. Configure trustworthiness for delegation if you need to act as a user in other services.

It is not necessary to enable Kerberos in SQL communications if you only need to authenticate clients for the frontend Sharepoint, without other services such as data connection, Excel Services / SQL Reporting.

Configure Service Principal Names (SPNs) in Active Directory

The Service Principal Name mapping is used by Kerberos to allow a service delegation to impersonate a user service account. An SPN includes Service Class, hostname and sometimes a port number. Some examples here are **HTTP / intranet.domain.local** and **MSSqlSvc / sql1.domain.local: 1433** . You should register both hostname and FQDN for your web applications even though they usually only use one of them.

To configure the Service Principal Name, you can use several tools. We use the SetSPN-tool component installed in Windows Server 2008 by default. For Windows Server 2003, this component can be found in the support tools section of the installation CD-ROM or in the resource kit section downloadable from Microsoft. You can also use ADSIedit to configure SPN, but this takes a bit of work to navigate through the Active Directory, editing the items and changing their *ServicePrincipalName* .

The command to register an SPN: **setspn.exe –A HTTP / intranet.domain.local DOMAINAccount**
The command lists the SPN for an account: **setspn.exe - L DOMAINAccount**
The command deletes an SPN: **setspn.exe –D HTTP / intranet.domain.local DOMAINAccount**

Use the tables in Figures 2 and 3 to see the necessary registrations for SQL in MOSS and WSS scenarios

	Trust for delegation	SPN registrations for Accounts (MOSS)
Computer Account WSS1	Yes	
Computer Account WSS2	Yes	
Computer Account WSS3	Yes	
Computer Account SQL1	Yes	
Service Account <SQL Server Service>	Yes	MSSQLSvc/sql1:1433 MSSQLSvc/sql1.domain.local:1433
Service Account <Farm Service>	Yes	HTTP/wss1 HTTP/wss2 HTTP/wss3 HTTP/wss1.domain.local HTTP/wss2.domain.local HTTP/wss3.domain.local
Application Pool Account <SSP Admin>	Yes	HTTP/sspadmin HTTP/sspadmin.domain.local
Application Pool Account <MySite>	Yes	HTTP/mysite HTTP/mysite.domain.local
Application Pool Account <Web app.>	Yes	HTTP/intranet HTTP/intranet.domain.local

Note: Only register the SPN to a single account, or you will get duplicate SPN registrations (no error is presented by either SetSPN.exe or ADSIEdit!)

Figure 2: Delegation and SPN for MOSS

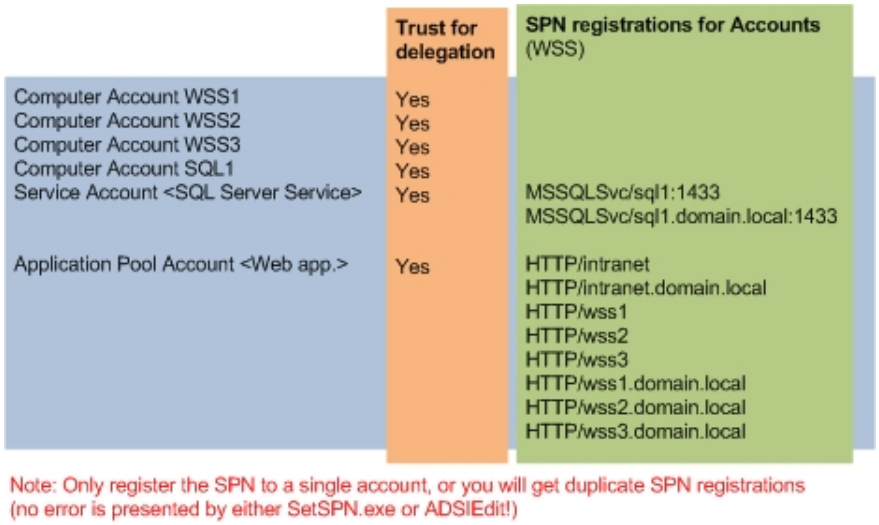

Figure 3: Delegation and SPN for WSS

Configure trust for credentials on computer and user accounts

Now you need to manage delegate rights in Active Directory. This can be done for computer and user accounts as you can see in the table above. In *Active Directory Users and Computers*, right-click on the account, select properties and check the trusted part of the delegation (see the information in Figure 4 and 5 below). Text or procedure may differ in versions of Windows Server.

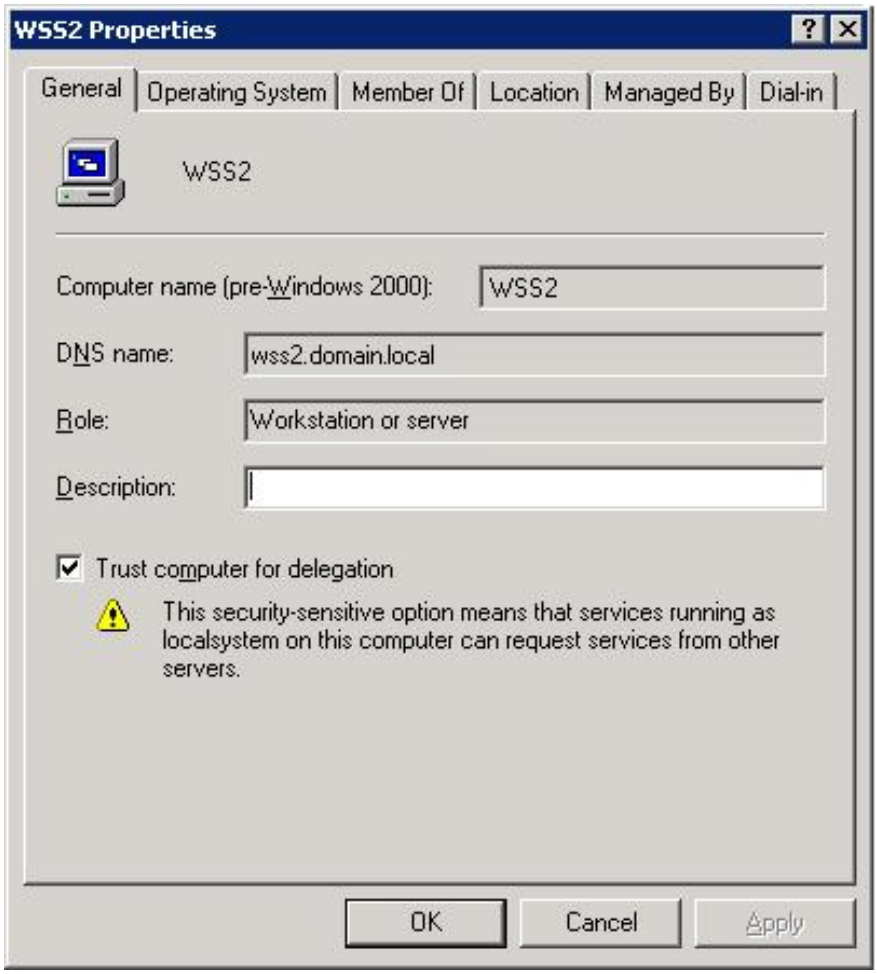

Figure 4: Delegation for computer account

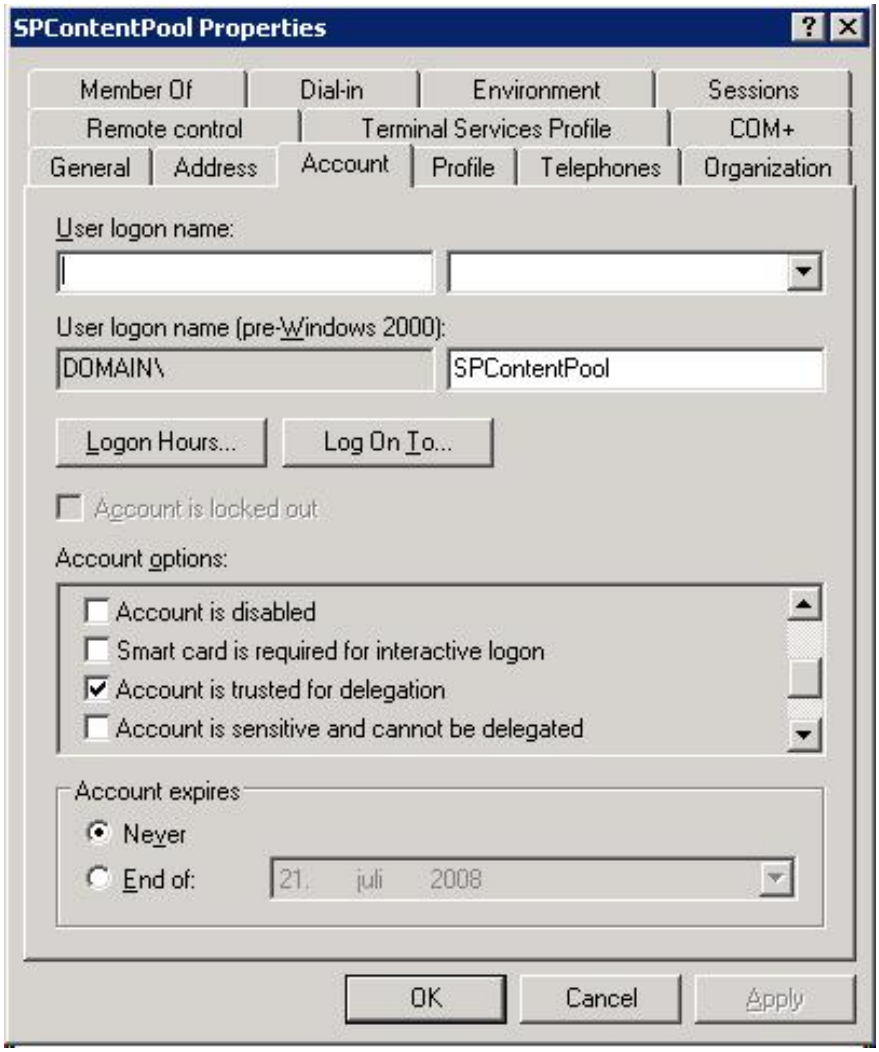

Figure 5: Delegation of user accounts

See Figure 2 and 3 for accounts for configuring criminal credentials in the script.

Configure component services on Sharepoint server

Web application accounts need to have legitimate rights or you will receive a DCOM error with the event code 10017 in your event log and described in Microsoft KB920783:

'The application-specific permissions settings do not grant Local Activation permissions for the COM Server application with CLSID {CLSID} to the user DomainNameUserName SID {SID}. ?ã có quy?n quy?n h?n này có th? ???c s? d?ng s? d?ng ph?n m?m c?a công c? ?i?u khi?n. '

With the appropriate security settings for the accounts, simply go to Control Panel, *Component Services* , Computers, My Computer, DCOM Config and edit the properties of 'IIS WAMReg Admin Service'. Edit 'Launch and Activate' in the Security tab and 'Local Activation' permissions for application accounts (see Figures 2 and 3).

When you are in Component Services, set 'Default Impersonation Level' to 'Delegate' by editing the properties of 'My Computer'.

Enable Kerberos for web applications and Shared Service Provider (SSP)

Your basic configuration will be done now. To use Kerberos you must enable it through the *Central Administration* for your web applications. We can choose between NTLM and Kerberos for separate web applications on the *Authentication Providers* page that you will find in the *Application Management* panel. Follow this path to configure:

1. Central Administration, Application Management, Authentication providers
2. Select your web application to use Kerberos for, for example:

1. Click 'Default'
2. Select or check the Kerberos option

Restart IIS with **iisreset / noforce** in the command prompt on your front end servers.
In MOSS, your Shared Service Provider must also be configured and you do so in a command prompt. The **SetSharedWebServiceAuthn** command **does** not exist in WSS. Navigate to the 12-hive directory (usually in *C: Program FilesCommon FilesMicrosoft Sharedweb server extensions12bin*) and run the command: **stsadm.exe -o SetSharedWebServiceAuthn -negotiate**

Test Sharepoint environment

Now go to the existing part of the activity: Make sure everything works as expected.

Check the security log for Kerberos login events. Domain account checking has been used. If the account has an error log, check the following:

1. The date and time are set correctly on all servers
2. The account is not locked in the domain
3. Service or application is working with the correct account
4. The credentials are configured correctly on computer and user accounts

5. The SPN is correctly configured in Active Directory
6. There is no duplication on servers that exist in DNS forward and reverse zones
7. The DNS server is properly assigned on all servers

Version issues for Internet Explorer

If you use non-default ports on your IIS Virtual server, make sure that the version of Internet Explorer you are using is Internet Explorer 6 or has been patched and configured to have ports in the SPN. *The Central Administration* will contain a non-default port number. Note here that you will not see an error message saying that this error is due to using an inappropriate version of Internet Explorer

Conclude

Microsoft Windows Sharepoint can be used in complex environments where secure authentication with Kerberos is needed. This article is provided to you in the hope of explaining some of the big Kerberos page problems in Sharepoint settings. Basic tools and configurations are available so you can start using the great features of Sharepoint with dual-hop authentication.