Troubleshoot problems with Kerberos in SharePoint - Part 1

In this section we will create a test environment to show which error message comes from which configuration causes.

Jesper M. Christensen

Network Administration - In this section we will create a test environment to show which error message comes from which configuration problems.

Introduce

If you haven't read the article with the Kerberos title in a Sharepoint environment, here's an article about Kerberos configuration and login process, please read through this article to get a better understanding of what happens when access to the website and basic configuration issues.

It is very difficult to accurately point out the meaning of the error messages that appear and you can spend a lot of time searching for help on the internet. So in this section we will create a test environment to help improve those tasks for you.

This is not a guide that can show all Kerberos related errors, but we create a test environment and create different problems to show which problems come from. Besides, the error messages in the server event log seem to be quite obvious, but sometimes larger investments are needed.

Setting

Demo-lab has the following computers:
DC1 Domain Controller (KDC)
SQL1 SQL Server 2008
WSS1 Windows Sharepoint Services 3.0 SP1 (+ infrastructure upgrade)
PC1 Windows Vista

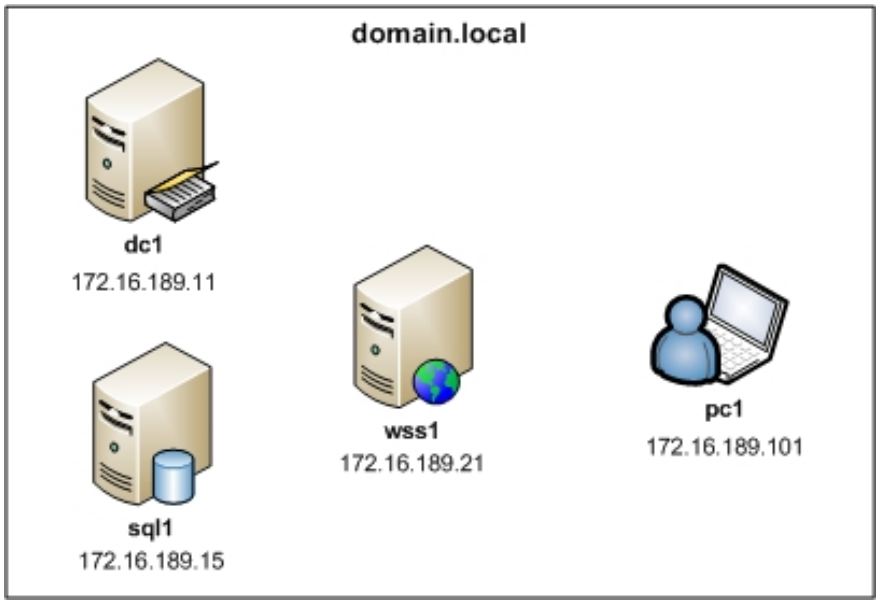

Figure 1

Service Principal Names (SPN) and delegation are configured as below.

	Trust for delegation	SPN Registrations for Accounts
Computer Accounts		
WSS1	Yes	
SQL1	Yes	
App. Pool Account		
domain\SQLServiceAcct	Yes	MSSQLSvc/sql1 MSSQLSvc/sql1.domain.local
App. Pool Account		
domain\SPContentPoolAcct	Yes	HTTP/wss1 HTTP/wss1.domain.local HTTP/intranet.domain.local

Figure 2

Where is the toolbox?

When troubleshooting errors, we must have a set of tools. In this series we will only use some of those tools, but for your convenience, here we recommend some troubleshooting tools.

- Windows server and client login events
- IIS log files are on frontend servers, SQL servers, and Domain Controllers
- SharePoint log files

- Command line tools
  - **setspn** (of the toolkit for Windows Server, Windows Server 2008 also has this default toolkit)
  - **ldifde**
  - **KList** (of the toolkit for Windows Server, Windows Server 2008 also has default)
- GUI tools
  - **KerbTray** (of Windows 200 Server, works with all versions of Windows)
  - **ADSIEdit**
  - **Network Monitor**
  - **WireShark** network data **analyzer**

Some useful commands to use when testing the clarity of commands:

- DNS cache: Ipconfig / flushdns
- NetBIOS cache you type in: Nbtstat -R
- Kerberos tickets: Klist purge

When analyzing the login procedure in Kerberos you need to follow the actions in the following table.

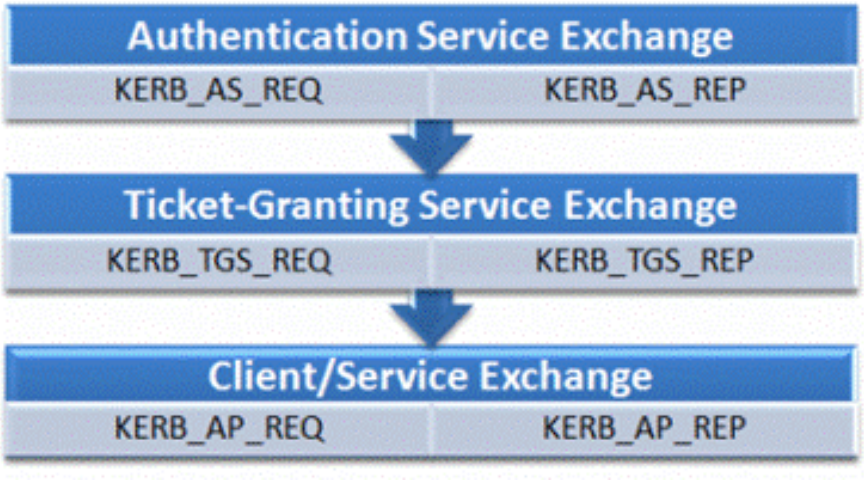

Figure 3

The issues need to be studied carefully

There are a number of common problems on servers and here is a list of issues that will be introduced in the article:

- Time and date
- Application account
- Configure SPN

In this section we will show you what you can see in Windows event log files and the network data analyzer for each of the problems we create.

Time and date

The date and time are a very important part of the Kerberos authentication mechanism because the cards used by the Key Distribution Center (KDC) are only valid for a limited period of time. If the client and server are not synchronized, the validation of the cards will fail because this is part of the security structure. Therefore, it is important to check all servers and clients with the right time zone and regional settings. In this example, we will introduce the date and time issues.

Time differences on SharePoint servers

We configure the SharePoint server WSS1 to be unique after 24 hours and errors appear in the Windows System event log of

Warning, W32Time, Event ID: 52, Category: None
D?ch v? th?i gian có ??t th?i gian v?i offset -86391 seconds

Usually servers will synchronize time automatically and these errors will not be encountered. That's just the case in our experiment so there's no need for administrators to intervene.

However, sometimes domain controllers may have synchronization issues. We tested it by changing the time on the domain controller and Kerberos announced the LSASRV event id 40960 in the system event log.

Warning, LSASRV, Event ID: 40960, Category: SPNEGO (Negotiator)
H? th?ng b?o v? tìm th?y l?i xác th?c cho máy ph?c v? MSSQLSvc / sql1.domain.local: 1433. Mã l?i khi th?c hi ?n Kerber giao th?c ?ã xác ??nh là th?i gian ? các Ph?n m?m chính h?c không ph?i là th?i gian th?i gian t?i các Domain Backup ho?c máy ph?c v? c?a quá l?n. (0xc0000133) '.

Time errors are quite easy and bug fixes - just adjust the time or open the required ports in the firewall if the sync packets on time fail. In virtual environments, time synchronization problems can cause more serious problems, as the virtual hardware clock of the virtual machine may be different from other virtual servers.

Application accounts

IIS websites for web applications are automatically configured by SharePoint and when creating them you need to select or add Application Pools. The web application will run in this block and with its configured identity (user).

Change application account yourself

Websites run in IIS application blocks and are not meant to be configured themselves. If an administrator changes the identity of the application block to a wrong account, this can cause the website to become unavailable. Then you need to adjust what users change.

We try to change the application block account to domainspwrongacct for http:///intranet.domain.local.

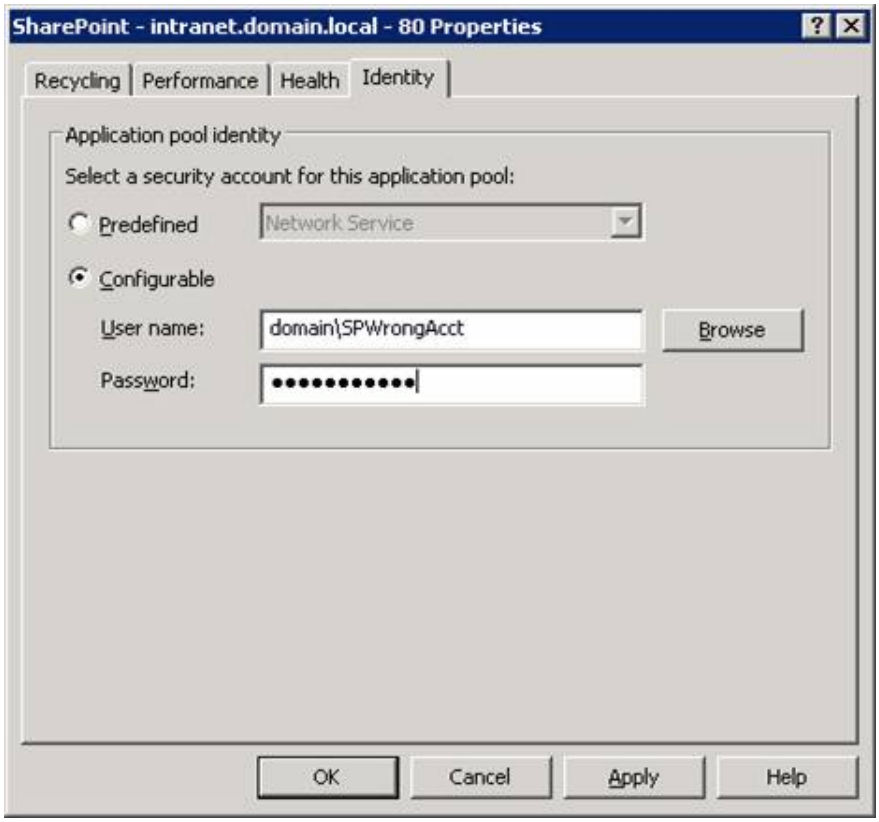

Figure 4

This will cause errors in the Windows System event log on the SharePoint server.

Warning, W3SVC, Event ID: 1012, Category: None
The identity of application pool, 'SharePoint - intranet.domain.local - 80' is invalid. N?u nó không h?p l? khi yêu c?u ??u tiên cho ?ng d?ng ???c x? lý, ?ng d?ng pool s? ???c disabled. Tr??ng d? li?u ch?a s? l?i.

Warning, W3SVC, Event ID: 1057, Category: None
The identity of application pool 'SharePoint - intranet.domain.local - 80' is invalid, so the World Wide Web Publishing Service cannot create a worker process to serve the application pool. Therefore, the application pool has been disabled.

Error, W3SVC, Event ID: 1059
A l?i ?ã b? khi khi khi kh?i ??ng ?ng d?ng d?ch v? ???ng d?n "SharePoint - intranet.hendriksen.dk80 '. Application pool has ???c disabled.

and the error on the client computer accessing the website will be: **Service Unavailable**

To fix the above error, change the account to an account that is configured in SharePoint configuration and start the application block again from the IIS management interface. If you need to change the user / password in the SharePoint configuration, follow the steps described in the Microsoft article.

Service Principle Name configuration (SPN)

The configuration of SPN is also important for Kerberos authentication to work. First, we summarize how they are used between the server and the client.

1. User types a URL in Internet Explorer (eg: http:///intranet.domain.local)
2. The client browser will create an SPN that includes the host name and service type (SPN: http / intranet.domain.local - Service type: HTTP Name: intranet.domain.local)
3. The client will send a request to KDC to get a card for this SPN
4. The KDC server will encrypt the card with the public key of the registered accounts (domainspcontentpoolacct) and send this card to the client.
5. The client will authenticate with the SharePoint server (frontend) by sending a card
6. The SharePoint server decrypts the card with the application account (its identity) and checks the contents.
7. An authenticated user or an error message will be sent to the event log or client browser record.
8. If the user fails to authenticate Kerberos, then NTLM authentication will be performed.

Error of SPN for web application

We will try to see what happens if the client cannot get the card from the KDC by removing the SPN mapping to the account.

Delete the wrong account : SETSPN –D HTTP / intranet.domain.local domainspwrongpoolacct
Then we access the website from PC1, http:///intranet.domain.local, and go to the default page of the website. - but how to do the assessment?

If we check the event log on the client, we will not be able to see any entries. In the Windows security event log on a SharePoint server, we see the following components:

Audit Success, Event ID: 4624, Category: Logon

.
Logon process: NtLmSsp
Authentication Package: NTLM
.

Therefore, Kerberos has failed to log in and authenticate with NTLM because it overcomes that phenomenon. We need to study billions of why it happens and we can add more Kerberos and client and server logs or use network analytics packages. Most of the time we use network analytics packages called Wireshark and start by installing and running on the client. We will get the output when capturing the process above:

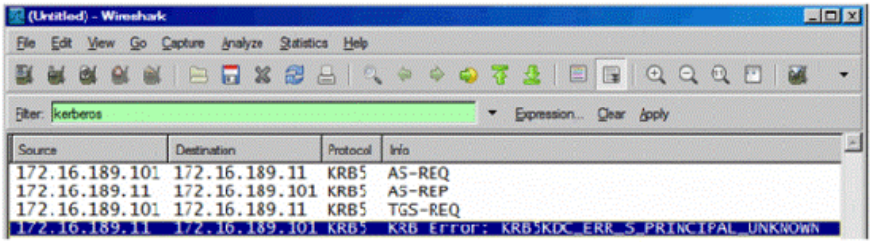

Figure 5

When the SPN is lost, Active Directory will send a KDC_ERR_S_PRINCIPAL_UNKNOWN. This is a message saying that the Active Directory cannot find a matching SPN for this website.

Configure the error account in Active Directory for SPN

If the decryption key does not match step 6, this means that the encryption key comes from another account and the configuration has an error somewhere. Let's configure the SPN to use the error account and see their results.

Delete the account correct : SETSPN –D HTTP / intranet.domain.local domainspcontentpoolacct

Add the wrong account : SETSPN -A HTTP / intranet.domain.local domainspwrongpoolacct

If we analyze data packets from a SharePoint server, we will see communication when we perform *iisreset / noforce* and access the web application.

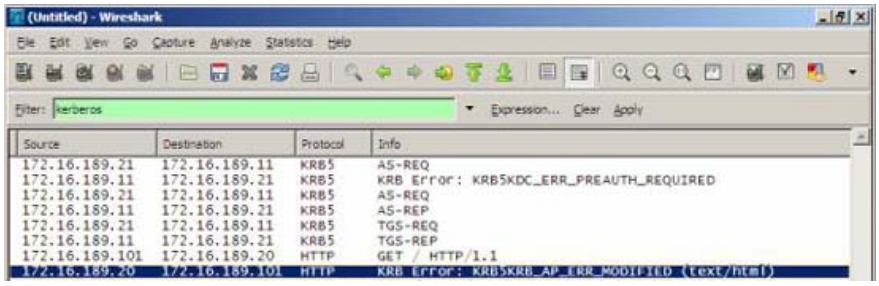

Figure 6

SharePoint server will receive Kerberos information from KDC and use it to decrypt the card. If it does not match, it will generate an error message to be sent to the client.

In the Windows System event log of the client, we will get the following error:

Error, Event ID: 4, Category: None
Ng??i dùng Kerberos ?ã nh?n m?t KRB_AP_ERR_MODIFIED error from the server wss1 $. The target name used was HTTP / intranet.domain.local. Không rõ m?t máy ph?c v? ?ích vào decrypt th? m?c ???c cung c?p c?a máy ph?c v?. Không th? th?c hi?n này khi tên c? s? d? li?u chính sách (SPN) ???c ??ng nh?p vào m?t tài kho?n khác có ng??i dùng c?a thi?t b? tài kho?n ???c dùng. Hãy xác ??nh các SPN ?ích ???c ??ng nh?p, và ch? ??ng nh?p, tài kho?n ???c dùng b?i máy ph?c v?. L?i này không th? thay ??i khi m?t d?ch v? ?ích ???c s? d?ng m?t m?t kh?u khác cho tài kho?n d?ch v? này, không bi?t s? ??nh v? l?i Kerberos Key Center (KDC) có cho thi?t b? d?ch v?. Hãy ki?m tra ??t d?ch v? trên máy ch? và KDC ???c c?p nh?t ?? s? d?ng m?t kh?u hi?n th?i. If the name server is not fully qualified, and the target domain (DOMAIN.LOCAL) is different from the domain client (DOMAIN.LOCAL), check if there is identically ???c ??ng nh?p máy ph?c v? trong hai các tr??ng nào, ho?c s? d?ng fully-qualified name to identify the server.

When the front-end server tries to decrypt the service card, the lock fails because it is encrypted using the SPN account key (domainspcontentpoolacct) but is decrypted with the private key of the application block accounts (domainspwrongacct). The KRB_AP_ERR_MODIFIED error will be sent to the client and appear in the Windows System event log.

The environment is properly reconfigured into a domainspcontentpoolacct account:

Delete the wrong account : SETSPN –D HTTP / intranet.domain.local domainspwrongpoolacct
Add the correct account : SETSPN -A HTTP / intranet.domain.local domainspcontentpoolacct

Note: The KRB_AP_ERR_MODIFIED error is also caused by a configuration error.

Conclude

We have set up a test environment, found several tools to use and caused error messages to help us find some date / time answers, accounts in applications. and configure SPN.

In the next parts of this series, we will introduce some typical problems like:

- Duplicate Service Principal Names
- Error of DNS configuration type
- Delegation when used and how to check it
- Shared Service Provider (SSP)
- Research more with the data analyzer in the network