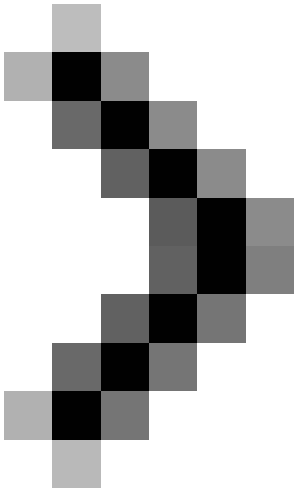
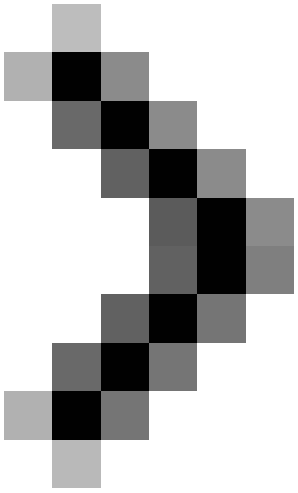
Troubleshoot problems with Kerberos in SharePoint - Part 3

In this third part, we will introduce you to Kerberos authorization and when to configure this trust.



Troubleshoot problems with Kerberos in SharePoint - Part 1



Troubleshoot problems with Kerberos in SharePoint - Part 2
Jesper M. Christensen

Network Administration - In this part of the series, we will introduce Kerberos authorization and when to configure this trust.

Introduce

We will start this section by explaining what Kerberos Delegation is and when it is necessary to configure it. In the previous articles of this series, we have introduced the configuration steps, but the delegation is not always needed because it depends on the application scenario or design and security requirements.

Kerberos Delegation can give a valid account across multiple servers using personalization. This problem is often known as double jump and you can feel it when using some services such as Excel Calculation Services (ECS). When configuring trust for credentials and using user account credentials, we must ensure that access levels are maintained properly throughout the system. Another example can be seen when a user requests data from a web application. The web application will create a query to the SQL database on another physical server and therefore must use personalization. If delegation and personalization are used, the SQL server only returns data that the user accesses.

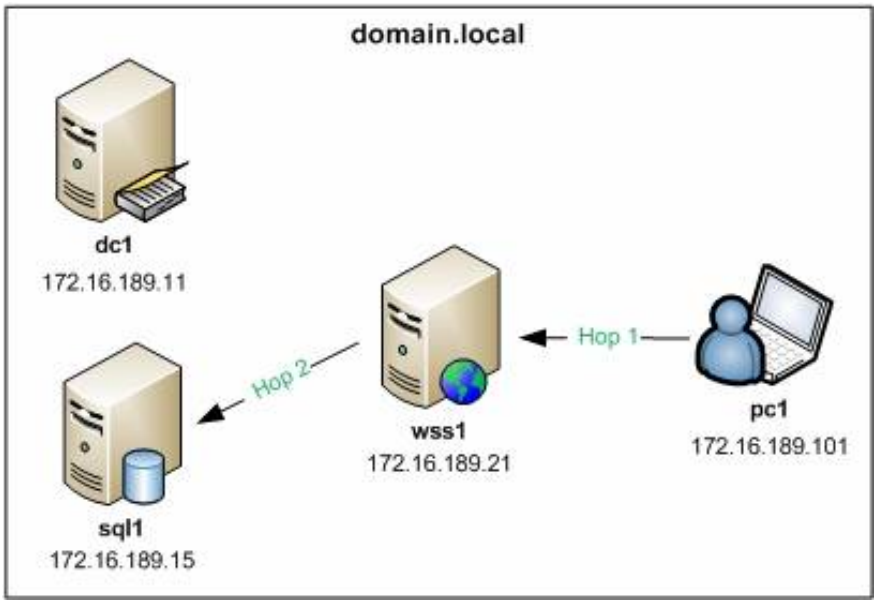


Figure 22: Two physical hops create double jump problems

We will set up a test environment for this issue and see what kinds of errors occur if the credentials are not properly configured. We have a page. The aspx is working and displaying data from a regular database on SQL server.

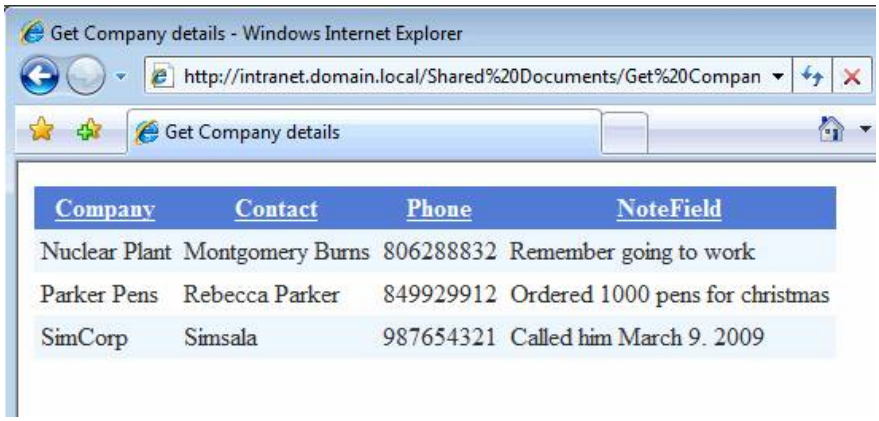


Figure 23: Query to SQL server

Kerberos Delegation has been properly configured in our demo environment, but let's see what happens if we remove the trust for some credentials for the Application Pool accounts; SPContentPoolAcct. Figure 24 shows the current configuration for this account.

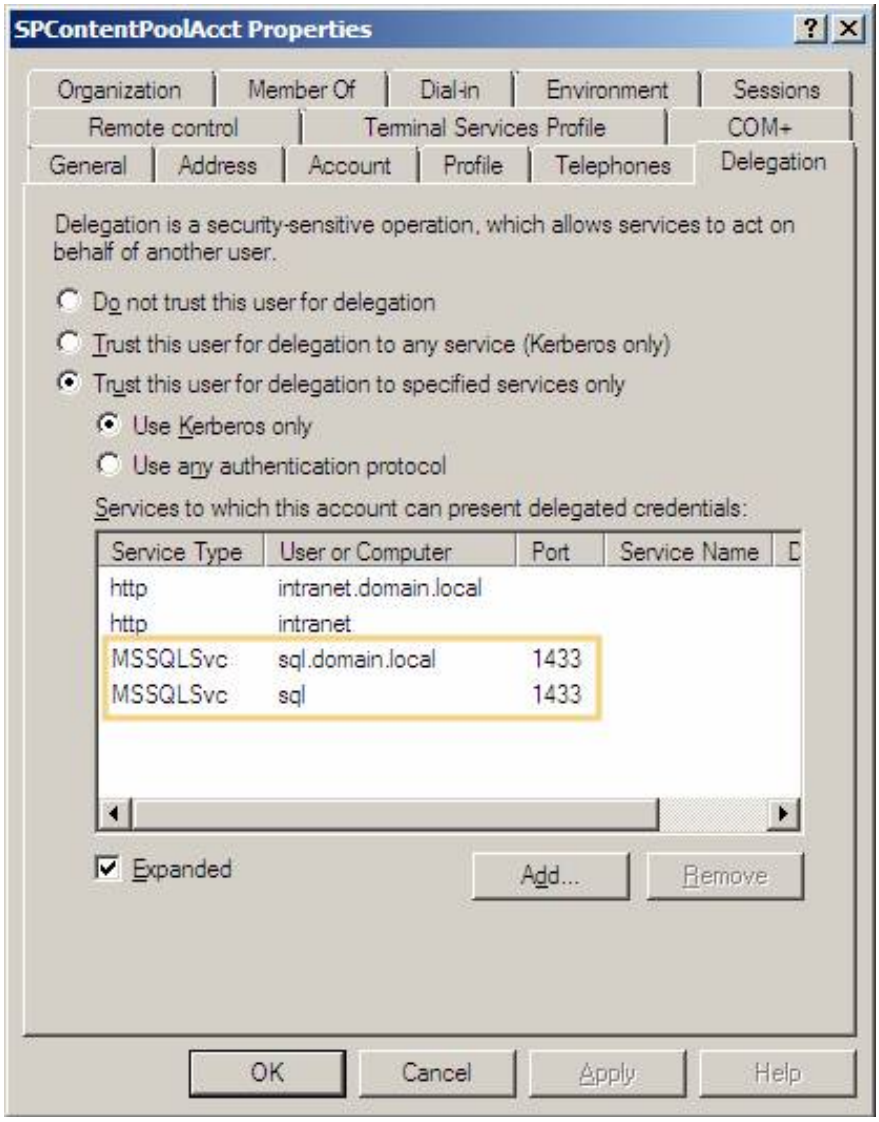


Figure 24: Modifying the proxy settings

We will try to remove the trusted permissions for the MSSQLSvc service highlighted in yellow in the figure and perform an IISRESET / NOFORCE on the SharePoint server WSS1. Without the necessary permissions, the SPContentPoolAcct account may not personalize user standards and display that to SQL server. Now the user will encounter the standard Microsoft SharePoint error as shown in Figure 25.

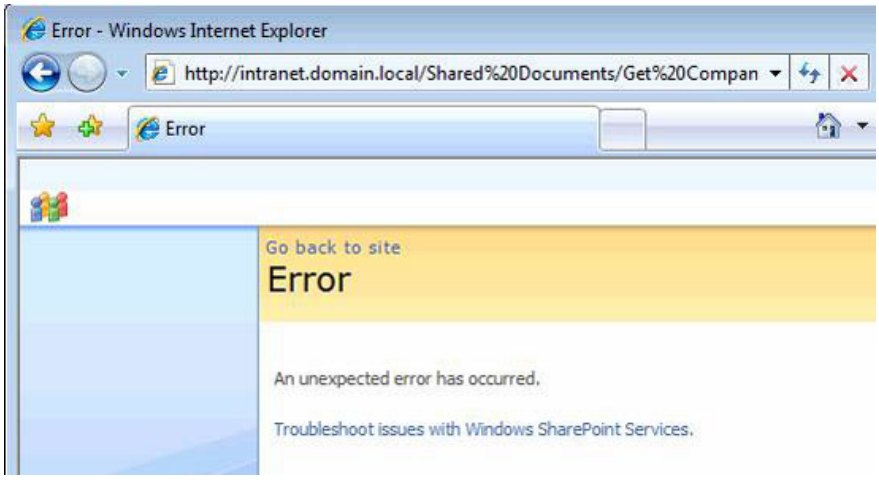


Figure 25: SharePoint site is returning a standard error message

First of all, we can't do much with this error message. If you are an administrator, you will be able to disable the *web.config* file in the file system of Microsoft SharePoint Web FrontEnd server (WFE).

The test environment is located here: *C: inetpubwwwrootwssVirtualDirectoriesintranet.domain.local80*

Disable error messages in Microsoft SharePoint

Note: This can be done on any Microsoft SharePoint WFE server

1. Create a copy with the web.config file before editing it (make sure in worse cases)
2. Open it with a text editor such as Notepad.
3. Search and change into
4. Search *CallStack = "true"* and change to *CallStack = "false"*
5. Restart Internet Information Server (IIS) with the IISRESET / NORFORCE command

Now let's go over this page.

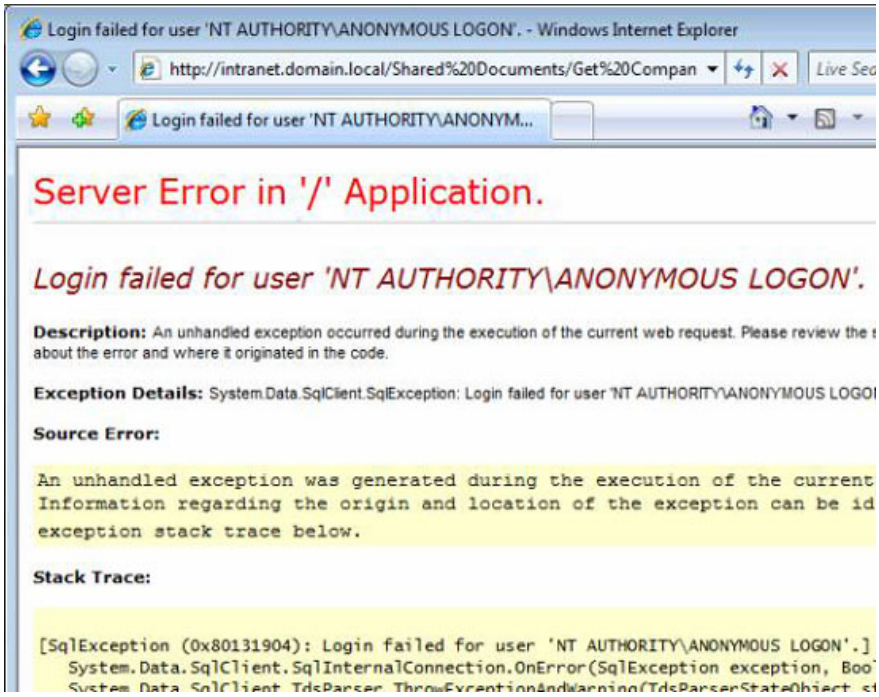


Figure 26: SharePoint page returns detailed error messages

This error message gives us a lot of information about the problem and the page clearly indicates that the problem lies with the SQL client login error with the message: *System.Data.SqlClient.SqlException: Login failed for user 'NT AUTHORITYANONYMOUS LOGON '*

Anonymous login has been done with .NET code and so the user's account (DOMAINAdministrator is logged into the client and trying to load the page) is not used in this process. For more information on this issue, you can see in the application event log at the SharePoint server (We only have one scenario, but if you have multiple WFE servers in Network Load balanced Network (NLB) then you need to check each server one by one to find your error messages.

In Event Viewer on WSS1 we will find a warning event:

Warning, ASP.NET 2.0.50727.0, Event ID: 1039, Category: Web Event
Event code: 3005
Event message: An unhandled exception has occurred
.
.
User: DOMAINAdministrator
Is authenticated: True
Authentication Type: Negotiate
Thread account name: DOMAINspcontentpoolacct

Thread information:
Thread ID: 4
Thread account name: DOMAINspcontentpoolacct

Is impersonating: False

.

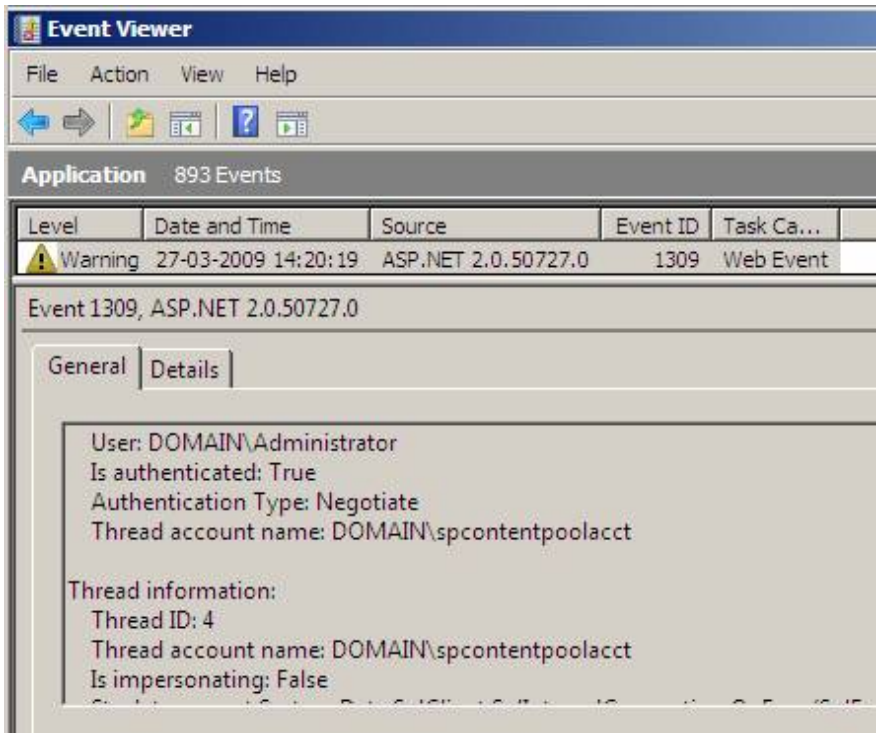


Figure 27: Warning from event log on WSS1 SharePoint WFE

The information in the event viewer shows us that the .NET code generated a web alert event. The user who created that is the authenticated user (DOMAINAdministrator) and the error account is DOMAINspcontentpoolacct. It also shows us that the user causing the error is not personalizing the real user account. Therefore personalization is not used for .NET code and this has caused problems.

Kerberos credential configuration will include:

- Service name (SPN) in Active Directory
  - Service type (MSSQLSvc)
  - Server name (SQL and SQL.DOMAIN.LOCAL)
  - Port if used (1433)
  - Registered account (DOMAINSQLSvcAcct because it is configured to run SQL Server service)
- Configure authorization for the application account (DOMAINSPContentPoolAcct to be allowed to pass standards to the SPN service, port and account).
- .Net code (Appraisal must be established and use personalization)

Note: Note that we have omitted the proxy configuration in DOMAINSPContentPoolAcct. However, it's simple, you can add information and start IIS services on a SharePoint WFE server.

Kerberos for Shared Service Provider (SSP)

Before the Infrastructure Update (July 2008) for Microsoft Office Servers servers was released, Kerberos authentication was not fully supported for SSH. This has caused some problems with many SSP and search functions. Therefore, we recommend that you install the upgrade on the systems if you haven't done so already. Microsoft has announced a number of updates later on including this infrastructure upgrade, so check out the Microsoft website to get the latest upgrade path. You can find a link to those links at the end of this section.

In the Infrastructure Update, Microsoft added the Service Principal Name format (SPN): **MSSP //** .

To get the configuration details for the SSP using this new SSP format, go to the TechNet website mentioned in the link section of this section. We have briefly summarized the Kerberos configuration steps as mentioned in a TechNet article about Shared Services Provider.

Shared Services Provider (SSP)

- Register Shared Service Provider SPN in Active Directory
- Change the SSP to use Kerberos authentication with the STSADM command-line tool
- Create a change in the registry on all MOSS 2007 servers to use the new SPN format for SSP.
- Confirm that Kerberos authentication works for root and access to virtual directory shared web services.

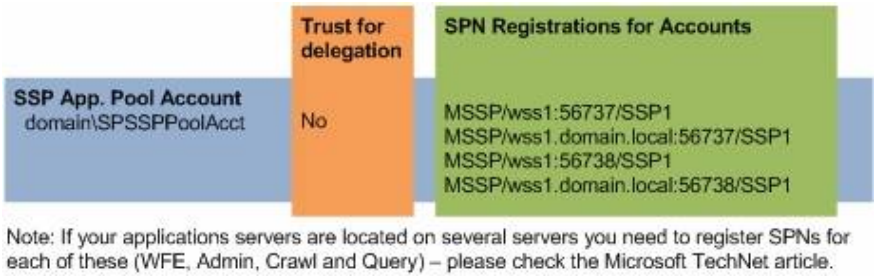


Figure 28: Register service name for SSP

Add some issues and notes

SharePoint service users and accounts

Check if the user or SharePoint account is locked in the domain or has an expired password. A company policy can be enforced in your environment in this case.

Secure connection of computer account

Some clients and servers fail to establish a secure connection to the domain but Kerberos is built on this type of secure infrastructure. If that happens, you need to reset and rebuild this relationship.

If the server and client are duplicated, then you need to create a new security ID (SID) and the recommended way to do it is to run the sysprep utility. Another possible way is to use Sysinternals, NewSID.

Problems with the size of MTU

Network packets sent through the wiring often have a certain length. If an account is a member of some large groups, this may be obvious. Another way to deal with the MTU issue is to enforce Kerberos using TCP. You can find information on this issue in Microsoft's KB244474 article.

Web applications with different authentication methods

Disable agreements on web applications if they are not needed or use Kerberos authentication. If you have multiple web applications on the same server and use Kerberos on some web applications and NTLM then you can feel this problem. Especially if web applications use the same server name and use other application accounts, it usually takes you a few hours to troubleshoot the systems.

We introduce some guidelines for web applications.

- **Use unique host-headers**
  such as intranet.domain.local instead of server name for SharePoint server
- **Use unique IP addresses for host-header**
  - This makes it easier to balance the load later
- **Use other application accounts for web applications**
  For security purposes, please create your own accounts. If using a NETWORK SERVICE account, the computer account is the account used by the web application to identify the SPN.
- **Use Network Load Balancing (NLB) network balancing for WFE servers**
  You will have better tolerance and better performance
- **Activate the agreement when using Kerberos. Disable it when using NTLM**
  Check your web application with the adsutil.vbs command line tool

Check if Kerberos is configured for the web application

Start the command prompt.

cd c: inetpubadminscripts
cscript adsutil.vbs get w3svc // root / NTAuthenticationProviders
(you will find the ID for the website via IIS Management in the identifier)

With Kerberos the result will be: *NTAuthenticationProviders: (STRING) "Negotiate, NTLM"*
With NTLM the result will be: *NTAuthenticationProviders: (STRING) 'NTLM'*
Configure the IIS website with another method (in this example with Kerberos) using the following command:
cd c: inetpubadminscripts
cscript adsutil.vbs set w3svc // root / NTAuthenticationProviders 'Negotiate, NTLM'

This is required on every SharePoint frontend server

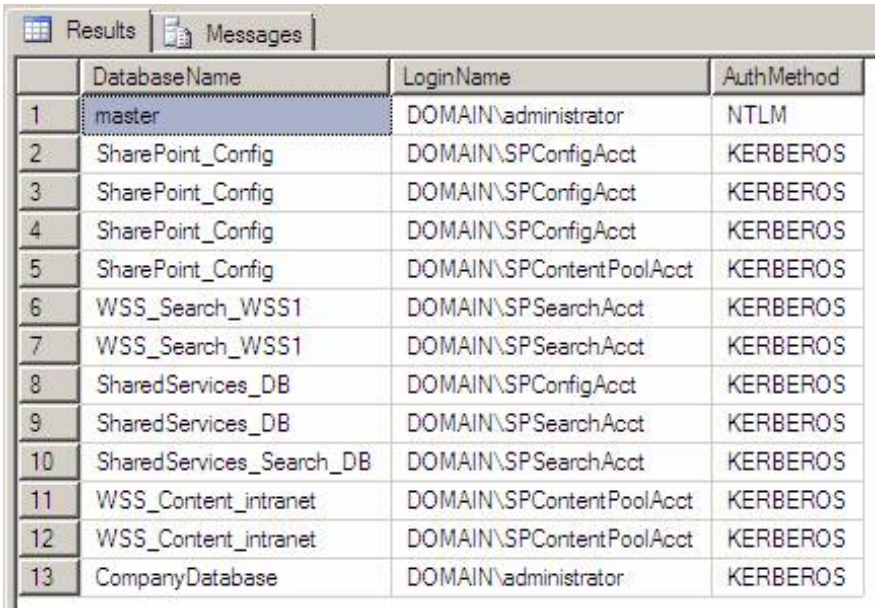
SQL Server 2005 script to test

We introduce an SQL script to check what type of authentication method is used for the database. This is useful when you need to make sure everything works as expected.

```
SELECT DB_NAME (dbid) AS DatabaseName, loginame AS LoginName,
sys.dm_exec_connections.auth_scheme as AuthMethod
```

FROM sys.sysprocesses
JOIN sys.dm_exec_connections
ON sys.sysprocesses.spid = sys.dm_exec_connections.session_id
WHERE dbid> 0
GROUP BY dbid, loginame, spid, sys.dm_exec_connections.auth_scheme

The output of the script in our test environment (with the CompanyDatabase example above) is shown in Figure 29 below.



Results | Messages

	DatabaseName	LoginName	AuthMethod
1	master	DOMAIN\administrator	NTLM
2	SharePoint_Config	DOMAIN\SPConfigAcct	KERBEROS
3	SharePoint_Config	DOMAIN\SPConfigAcct	KERBEROS
4	SharePoint_Config	DOMAIN\SPConfigAcct	KERBEROS
5	SharePoint_Config	DOMAIN\SPContentPoolAcct	KERBEROS
6	WSS_Search_WSS1	DOMAIN\SPSearchAcct	KERBEROS
7	WSS_Search_WSS1	DOMAIN\SPSearchAcct	KERBEROS
8	SharedServices_DB	DOMAIN\SPConfigAcct	KERBEROS
9	SharedServices_DB	DOMAIN\SPSearchAcct	KERBEROS
10	SharedServices_Search_DB	DOMAIN\SPSearchAcct	KERBEROS
11	WSS_Content_intranet	DOMAIN\SPContentPoolAcct	KERBEROS
12	WSS_Content_intranet	DOMAIN\SPContentPoolAcct	KERBEROS
13	CompanyDatabase	DOMAIN\administrator	KERBEROS

Figure 29: Output of the script in SQL Management Studio

Conclude

In this section, we introduced the delegation in Kerberos, the personalization and configuration of Shared Service Provider (SSP). In addition, we also introduced notes and scripts to check the authentication method used - this can be used with SharePoint as well as other configurations.

Kerberos configuration and especially troubleshooting different issues can be very complicated. However, our task in this series is to provide you with some important information in the technologies so that you can find the reasons for the problems and then solve them. We hope you will find success after this series.

You finished reading the article "**Troubleshoot problems with Kerberos in SharePoint - Part 3**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.