Configuring Kerberos Authentication For Laserfiche Search Integration 8.2 For SharePoint 2010

White Paper

October 2011

Laserfiche®

Table of Contents

About SharePoint Search Integration 8.2

Laserfiche SharePoint Search Integration 8.2 for SharePoint 2010 allows SharePoint Search to periodically index the contents of your Laserfiche repository. You can then create a SharePoint Search Center for users to search for documents in a Laserfiche repository from SharePoint.

When a SharePoint user submits a search request, the integration dynamically connects to the Laserfiche Server to check that user's Laserfiche security in order to exclude any Laserfiche documents or folders that the user should not be able to see. By default, the integration impersonates as the SharePoint user's Windows account when connecting to the Laserfiche Server. This method allows the integration to use an optimized method for retrieving the Laserfiche entry access rights for that user to determine what documents to display in the SharePoint search results.

To preserve a single sign-on experience, the search integration does not prompt the SharePoint user to provide their Windows user account and password. Instead, the integration relies on a Windows feature called the Claims to Windows Token Service (C2WTS) to generate a Windows security token for that user. When the integration and the Laserfiche Server are on the same computer, no additional configuration is required. But, when the integration and the Laserfiche Server are on different computers in the domain, you must allow protocol transition and Kerberos constrained delegation on the following service accounts in Active Directory:

- The Claims to Windows Token Service's (C2WTS) service account
- The **SharePoint Web Services Default** IIS application pools identity (the integration runs within this application pool)

Both service accounts must be trusted for delegation to the Laserfiche Server service account.

Note: If C2WTS or the SharePoint Web Services IIS application pool are running as Local System or Network Service, you must allow protocol transition and constrained delegation on the SharePoint computer in Active Directory.

SPN Registration for the Laserfiche Server service account

Before we configure constrained delegation to the Laserfiche server, first make sure that there are valid SPNs registered for the Laserfiche Server. SPN registration requires domain administrator privileges. Use the setspn.exe command-line utility.

1. As a domain administrator, click **Start** and click **Command Prompt**.

2. Type the following and press ENTER

   ```
   Setspn –s HTTP/LFServerName LFServerServiceAccount
   ```

   Where *LFServerName* is the name of your Laserfiche Server and *LFServerServiceAccount* (e.g., *mydomain\jdoe*) is the domain name of the user for the Laserfiche Server service.

3. Repeat the above step with:

   ```
   Setspn –s HTTP/FQDNLFServerName LFServerServiceAccount
   ```

   Where *FQDNLFServerName* is the fully-qualified domain name to your Laserfiche Server (e.g., *myServer.domain.com*).

To configure constrained delegation with protocol transition for the C2WTS service account

1. Click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**.

2. Do one of the following:

   - By default, C2WTS runs under Local System. If C2WTS is running as Local System, expand the item for your domain and select the **Computers** item. Locate the SharePoint server and view its properties.

   - If C2WTS is running under a custom service account, expand the item for your domain and select the **Users** item. Locate the appropriate user and view its properties..

3. On th**e Delegation** tab, select the **Trust this computer/user for delegation to specified services only** option.

4. Select the **Use any authentication protocol** option.

5. Click **Add** to open the **Add Services** dialog box.

6. In the **Add Services** dialog box, click **Users and Computers**.

7. In the **Select Users or Computers** dialog box, type the name of the service account for the Laserfiche Server service. If the Laserfiche Server is running under Local System, type the name of the computer hosting the Laserfiche Server. Click **OK**.

8. Back in the **Add Services** dialog box, select the Laserfiche Server SPN you would like to delegate to and click **OK**. The Service Type is **HTTP**.

To configure constrained delegation for the SharePoint Web Services Default Application Pool identity

1. Click **Start**, point to **Administrative Tools**, and click **Active Directory Users and Computers**

2. Do one of the following:

    - By default, the SharePoint Web Services Default application pool runs under Network Service. If the application pool is running as Network Service, expand the item for your domain and select the **Computers** item. Locate the SharePoint server and view its properties.

    - If the SharePoint Web Services Default application pool is running under a custom service account, expand the item for your domain and select the **Users** item. Locate the appropriate user and view its properties.

3. On th**e Delegation** tab, select the **Trust this computer/user for delegation to specified services only** option.

4. Select the **Use any authentication protocol** option.

5. Click **Add** to open the **Add Services** dialog box.

6. In the **Add Services** dialog box, click **Users and Computers**.

7. In the **Select Users or Computers** dialog box, type the name of the service account for the Laserfiche Server service. If the Laserfiche Server is running under Local System, type the name of the computer hosting the Laserfiche Server. Click **OK**.

8. Back in the **Add Services** dialog box, select the Laserfiche Server SPN you would like to delegate to and click **OK**. The Service Type is **HTTP**.

Troubleshooting Tips

When using the default user accounts for the SharePoint Web Services application pool identity (Network Service) and the Claims to Windows Token Service (Local System), the entire Kerberos configuration process is reduced to using the Active Directory Users and Computers snap-in to enable Kerberos constrained delegation on the SharePoint computer. When you use custom service accounts, additional prerequisites and best practices are required. The following section highlights common scenarios, best practices, and pitfalls.

The Delegation tab may not visible in the user's properties dialog box

By default, the Active Directory Users and Computers MMC snap-in does not automatically display the **Delegation** tab for all users. As a workaround, register a placeholder SPN for the user. For example:

```
Setspn –s FakeProtocol/AnyServerName UserAccount
```

Once registered, you can now view the **Delegation** tab to configure constrained delegation.

> **Note:** It is possible to manually edit a user's attributes to configure constrained delegation. For more information, see Microsoft documentation on the **msDS-AllowedToDelegateTo** attribute and the UserAccountControl attribute's **TRUSTED_TO_AUTHENTICATE_FOR_DELEGATION** bit.

Use the SharePoint 2010 Central Administration Web site to configure the service accounts for the SharePoint Web Services Default application pool or the Claims To Windows Token Service

Instead of using IIS Manager or the Services snap-in to change the process identities for the SharePoint Web Services Default application pool or C2WTS, use the SharePoint 2010 Central Administration site to streamline the configuration process. For example, C2WTS only accepts requests from domain accounts explicitly listed in its configuration file. By default, SharePoint adds the "WSS_WPG" local group to the configuration file. When you use Central Administration to modify the identity of the SharePoint Web Services Default IIS application pool, SharePoint will automatically add that account to the "WSS_WPG" group.

To register a managed account

1. Open the SharePoint 2010 Central Administration site.
2. Click **Security**.
3. Under **General Security**, click **Configure managed accounts**.
4. On the **Managed Accounts** page, click **Register Managed Account**.
5. Specify the desired Windows domain name and password and click **OK**.

To change the application pool identity

1. Open the SharePoint 2010 Central Administration site.
2. Under **Security**, click **Configure service accounts**.
3. In the top drop-down list, select the **Service Application Pool – SharePoint Web Services Default** option.
4. In the Select an account for the component drop-down list, select the desired account and click **OK**.

To change the Claims to Windows Token Service identity

1. Open the SharePoint 2010 Central Administration site.
2. Under **Security**, click **Configure service accounts**.
3. In the top drop-down list, select the **Windows Service – Claims to Windows Token Service** option.
4. In the Select an account for the component drop-down list, select the desired account and click **OK**.

The custom service account for C2WTS requires special local policy user rights on the SharePoint Server

By default, C2WTS runs under the Local System account. If you want C2WTS to run as a custom user account, be aware that the service account for C2WTS must have the following local policy user rights on the SharePoint Server:

- Act as part of the operating system
- Impersonate a client after authentication
- Log on as a service

Use the Local Security Policy MMC snap-in to add the account to listed rights.

1. Click **Start**, point to **Administrative Tools**, and click **Local Security Policy**.
2. Expand **Local Policies** and select User Rights Assignment.
3. Double-click **Act as part of the operating system**.

4. Click **Add User or Group** and specify the custom C2WTS service account.
5. Repeat the above steps with the **Impersonate a client after authentication** right and the **Log on as a service** right.

Removing Duplicate SPNs

A Service Principal Name (SPN) must be unique. Duplicate SPNs prevent Kerberos authentication from functioning. Use the setspn.exe command-line utility to identify and remove duplicate SPNs.

To identify duplicate SPNs

1. As a domain administrator, click Start and click Command Prompt.
2. Type the following and press ENTER to display duplicate SPNs:

```
Setspn –x
```

To remove an SPN

1. As a domain administrator, click **Start** and click **Command Prompt**.
2. Type the following and press ENTER to remove the specified SPN:

```
Setspn –d spn ServiceAccount
```

Resetting C2WTS to use Local System

The SharePoint Central Administration does not allow you to reset C2WTS to run as Local System.

Please see the following Microsoft TechNet article for details on using Windows PowerShell to reset the Claims to Windows Token Service back to using Local System.

http://technet.microsoft.com/en-us/library/gg502596.aspx

Impersonation Workaround

The Laserfiche SharePoint Search Integration includes a different method for connecting to the Laserfiche Server when checking Laserfiche entry access rights. You can configure the integration to log in to Laserfiche with the same Windows account that you specified in the Laserfiche SharePoint Search Configuration utility. In this scenario, the integration no longer attempts to impersonate the user running the search when connecting to the Laserfiche Server and Kerberos authentication is not necessary. However, be aware that the benefit of no longer needing to configure Kerberos comes at the expense of search performance.

To switch to this alternate login method, create a **UseC2WTS** DWORD value in the "HKEY_LOCAL_MACHINE\SOFTWARE\Laserfiche\SharePoint Integration\8.2" registry key.

To create the UseC2WTS registry value

1. Click Start and type the following into the search box:

   ```
   Regedit
   ```

2. Expand KEY_LOCAL_MACHINE.
3. Expand SOFTWARE.
4. Expand Laserfiche.
5. Expand SharePoint Integration
6. Expand 8.2.
7. Create a new DWORD value named:

   ```
   UseC2WTS
   ```

8. Set the value to 0 to configure the Search Integration to connect to the Laserfiche Server using a static account.

   Note: Configuring the Search Integration in this manner removes the need to configure Kerberos authentication, but introduces performance slowdowns. SharePoint searches of Laserfiche documents will take longer to return results and there is a greater chance of searches timing out.

Additional Resources

See the following Microsoft TechNet articles on Kerberos authentication for SharePoint 2010.

http://technet.microsoft.com/en-us/library/gg502594.aspx

The same set of articles is also available as a Microsoft Word document:

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=23176

Configuring Kerberos Authentication For Laserfiche Search Integration 8.2 For SharePoint 2010
October 2011

Author: Roger Wu
Technical Editor: Zhiyu Chen, Brian McKeever

Compulink Management Center, Inc.
Global Headquarters
3545 Long Beach Blvd.
Long Beach, CA 90807
U.S.A

Phone: +1.562.988.1688
www.laserfiche.com

Laserfiche makes every effort to ensure the accuracy of these contents at the time of publication. They are for information purposes only and Laserfiche makes no warranties, express or implied, as to the information herein.