Configuring Integrated Windows Authentication for IBM WebSphere with SAS 9.2 Web Applications

Copyright Notice

Table of Contents

Chapter 1 — Integrated Windows Authentication

Overview of Integrated Windows Authentication

Integrated Windows Authentication (IWA) is a Microsoft technology that is used in an intranet environment where users have Windows domain accounts. With IWA, the credentials (user name and password) are hashed before being sent across the network. The client browser proves its knowledge of the password through a cryptographic exchange with your Web application server.

The key components of IWA include an Active Directory Controller machine (either Windows 2000 or higher server), Kerberos Key Distribution Center (KDC) in a Domain Controller machine, a machine with a client browser, and a Web application server.

When used in conjunction with Kerberos, IWA enables the delegation of security credentials. Kerberos is an industry-standard authentication protocol that is used to verify user or host identity. The Kerberos protocol uses strong cryptography so that a client can prove its identity to a server (and vice versa) across an insecure network connection. After a client and server has used Kerberos to provide their identity, they can also encrypt all of their communications to assure privacy and data integrity.

If Active Directory is installed on a Domain Controller running Windows 2000 or higher server, and the client browser supports the Kerberos authentication protocol, Kerberos authentication is used. Note that IWA does not work over HTTP proxy connections.

Use of the Kerberos protocol is guided by the following requirements:

- The client must have a direct connection to Active Directory
- Both the client and the server must have a trusted connection to a Key Distribution Center (KDC) and be Active Directory-compatible
- Service Principal Names (SPNs) are required for multiple worker processes.

Integrated Windows Authentication for WebSphere

When IWA is configured, HTTP clients use Windows login user name to access the SAS Web applications deployed in the WebSphere application server without any authentication challenge.

To configure IWA for WebSphere and create a single sign-on for HTTP requests using the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO), the following requirements should be met:

- SAS 9.2 or the October 2009 release of SAS 9.2 is installed.
- Web authentication is configured.

- An Active Directory Controller machine. Typically, this is a Microsoft Windows 2000 or Windows 2003 Server running the Active Directory Domain Controller and associated Kerberos Key Distribution Center (KDC).
- Machine with a client browser. This is a Microsoft Windows 2000 (or higher) domain member that has a browser client and supports the SPNEGO authentication mechanism. Microsoft Internet Explorer Version 7.0 or later qualifies as the client.
- The Microsoft Windows 2000 (or higher) active directory domain should include the domain controller, client workstation, and users who can log into the client workstation
- WebSphere should be running and SAS Web applications should be deployed. Users on the active directory must have access to WebSphere. WebSphere should be enabled for application security, and configured to use the Active Directory as the user registry.
- The clock on all three machines should be synchronized to within five minutes.

Installing, Configuring, and Deploying SAS 9.2

Install SAS 9.2 with WebSphere. Follow the instructions provided in the **Instructions.html** file to complete the SAS 9.2 installation and verify the Web applications. An initial installation of SAS 9.2 uses the Metadata Server to authenticate users who log into SAS Web applications.

Stopping SAS Web Infrastructure Platform Applications and the Web Application Server

Stop the SAS Web Infrastructure Platform applications and WebSphere Application Server.

Configuring Web Authentication

An initial SAS 9.2 installation uses the Metadata Server to authenticate users who log into SAS Web applications. You must configure the WebSphere application server to use Web authentication. When Web authentication is configured, users who access SAS Web applications are presented with a dialog box with a log in prompt. The credentials supplied by the users are authenticated in the Active Directory by the Domain controller.

For instructions on configuring Web authentication for WebSphere, see "Configuring IBM WebSphere Application Server 9.2 for Web Authentication with SAS 9.2 Web Applications."

Configuration Tasks on the Active Directory Domain Controller Machine

To perform tasks on the Microsoft Active Directory domain controller machine, you should be familiar with Active Directory Users and Computer on a Windows server. This task is required to process single sign on browser requests to the WebSphere application server and the SPNEGO trust association interceptor (TAI).

For instructions on how to use the Active Directory Users and Directory, refer to the product's online Help. Complete the following tasks on the Microsoft Active Directory domain controller machine.

Create a Group in the Microsoft Active Directory

Create an organizational unit or group for user accounts in the Active Directory on the Windows server. The process by which WebSphere creates a query to the Active Directory requires that all user accounts reside within an organizational unit or group.

Create a User Account in the Microsoft Active Directory

1. (Optional). On the domain controller machine, run the following command to find the principals for all users:
   dsquery user
2. Create a user account within the Active Directory Users and Directory window, and add this user account to the group that you created. This user account will be mapped to the Kerberos service principal name (SPN). IBM's convention is to use the host name of the WebSphere server for the user name. For example, if the WebSphere server was running redwood2.sas.com, use the ID redwood2. Make sure that the following options are selected when you create the user:
   User cannot change password
   Password never expires.
   Note the password you defined when creating the user account. You will need it later.
3. Configure the new user account to comply with the Kerberos protocol.
4. Right-click the name of the user account in the Users tree in the left pane and select Properties.
5. In the Properties dialog box for the user, click **Account** tab.
6. Under Account Options, select the following:
   Password never expires
   Use DES Encryption types for this Account
   Do not require Kerberos preauthentication

   Selection **"Do not require Kerberos preauthentication"** is optional.

7. Setting the encryption type might corrupt the password. Therefore, reset the user password by right-clicking the name of the user account, selecting Reset Password, and re-entering the same password specified earlier.
8. Add the user to the group that you created.

Configure Kerberos SPN for WebSphere Application Server

The Microsoft Active Directory provides support for service principal names (SPN), which are a key component in Kerberos authentication. SPNs are unique identifiers for services running on servers. Every service that uses Kerberos authentication needs to have an SPN set for it so that clients can identify the service on the network. An SPN usually looks something like name@YOUR.REALM. You need to define an SPN to represent your WebSphere Server in the Kerberos realm. If an SPN is not set for a service, clients have no way of locating that service. Without correctly set SPNs, Kerberos authentication is not possible.

1. On the Active Directory Controller, access the command prompt window to use the **setspn** commands.
2. Before executing the **setspn** commands, verify that there are no additional mappings already configured for the users:

   ```
   setspn -l HTTP/fully-qualified-host
   ```

   No Service Principal Names should be presented.
3. Enter the following commands for SPNs by using correct capitalization of letters and substituting the host name and user name that you created earlier:

   ```
   setspn -a HTTP/fully-qualified-host-name username
   ```

   Here is an example of the use of the **setspn** command:

   ```
   setspn -a redwood2.abc.sas.com redwood2
   ```

4. Run the **setspn** command to view the SPNs you created:

   ```
   setspn -l username
   ```

   This is an important step. If the same service is linked to different accounts in the Active Directory server, the client will not send a Kerberos ticket to the server.

Create the Kerberos Keytab File Used by SPNEGO

Keytab files are the mechanism for storing the SPNs. Keytab files are copied to the WebSphere Server domain and are used in the login process. For each service (like WebSphere), there must also be a service key known only to Kerberos and the service. On the Kerberos server, the service key is stored in the Kerberos database. On the server host, the service key is stored in a key table called a keytab. This service key is the equivalent of the service's password, and must be kept secure. Data that is meant to be read only by the service is encrypted using this key.

1. Create the Kerberos keytab file for SPNEGO and make it available to the WebSphere application server. Use the **ktpass** command to create a user mapping and the Kerberos keytab file:

   ```
   ktpass -out C:\hostname.host.keytab -mapuser username -princ HTTP/fully-qualified-
   domain-name@URL address -pass password -ptype KRB5_NT_PRINCIPAL
   ```

   The **ktpass** command creates the **hostname.host.keytab** file.

   Here is an example of the use of the **ktpass** command and the options which create the **redwood2.host.keytab** file:

   ```
   ktpass -out C:\redwood2.host.keytab -mapuser redwood2 -princ
   HTTP/redwood2.abc.sas.com@ABC.SAS.COM -pass password-of-logged-user -ptype
   KRB5_NT_PRINCIPAL
   ```

   The following table explains the options used with the **ktpass** command.

Option	Explanation
-out	The key is written to this output file.
-mapuser	The key is mapped to this user.
-princ	Principal name.
-pass	This option denotes the password for the user ID.
-ptype KRB5_NT_PRINCIPAL	This option specifies the KRB5_NT_PRINCIPAL principal value. Specify this option to avoid warning messages.

The ktpass command offers many options. Use the command with the help option, `ktpass /?`, to view these options.

The Kerberos keytab file is created for use with SPNEGO. Next, you will make the keytab file available to the WebSphere application server by copying the Kerberos keytab file from the Domain Controller machine to WebSphere.

Configuration Tasks on WebSphere

To enable the use of SPNEGO for WebSphere, the Kerberos configuration must be completed. Configuration tasks on WebSphere include copying the keytab file to the appropriate directory, and creating the Kerberos configuration files, **krb5.ini** (on Windows) and **krb5login.conf** (on UNIX).

- Configure Lightweight Third Party Authentication (LTPA)
- Enable trust association and configure the SPNEGO Trust Association Interceptor (TAI)
- Enable the SPNEGO TAI
- Install the Kerberos keytab file on the WebSphere host
- Create a Kerberos configuration file
- Verify the Kerberos Authentication

Configure Lightweight Third Party Authentication

To configure LTPA, see IBM's documentation on "Configuring the Lightweight Third Party Authentication mechanism."

Enable the Trust Association and Configure the SPNEGO TAI

Perform the following steps to enable the SPNEGO Trust Association Interceptor:

1. In the WebSphere administration console, navigate to **Security** > **Security administration, applications, and infrastructure** > **Web security** > **Trust association**.
2. Enable the **Enable trust association** check box, and click **OK**.
3. Return to the **Trust association** page and click **Interceptors**.
4. Click **com.ibm.ws.security.spnego.TrustAssociationInterceptorImpl** (the first link in the list).
5. On the target page, click **Custom properties**.
6. Add a new property named `com.ibm.ws.security.spnego.SPN1.hostName`, and use the fully qualified domain name of the WebSphere host as the value. For example, `redwood2.sas.com`. Then, click **OK**.

This is the minimum level of configuration. The interceptor supports many other properties that you might choose to configure. For a list of the properties, see the IBM documentation for "SPNEGO TAI custom properties configuration."

Two properties that are especially useful are:

`com.ibm.ws.security.spnego.SPN1.filterClass`
`com.ibm.ws.security.spnego.SPN1.filter`.

By default, the SPNEGO TAI intercepts all HTTP requests. You can change this by modifying the following property

from:

`com.ibm.ws.security.spnego.SPN1.filterClass`

to:

`com.ibm.ws.security.spnego.HTTPHeaderFilter`

Then specify `com.ibm.ws.security.spnego.SPN1.filter` to an expression built by using information in the HTTP headers of a request and the operators listed in the IBM documentation for "SPNEGO TAI custom properties configuration."

Enable the SPNEGO TAI

To enable SPNEGO TAI that you just configured, complete these steps:

1. In the WebSphere administration console, navigate to **Servers** > **Application servers** > ***server-name*** > **Java and Process Management** > **Process Definition** > **Java Virtual Machine** > **Custom properties**.
2. Create a new custom property: `com.ibm.ws.security.spnego.isEnabled` and set a value of `true`.
3. Click **OK**.

Install the Keytab File

Copy the keytab file you created earlier from the Domain Controller to the WebSphere host, and put it in a known location such as the `C:\WINNT` directory.

Create a Kerberos Configuration File

Create a Kerberos configuration file, **krb5.ini** by following the instructions in the topic "Kerberos Configuration File" at the IBM website.

Your **krb5.ini** file should resemble the content in the following example:

```
[libdefaults]
      default_realm = SAS.COM
      default_keytab_name = FILE:c:\winnt\krb5.ini
      default_tkt_enctypes = des-cbc-md5 rc4-hmac
      default_tgs_enctypes = des-cbc-md5 rc4-hmac
      kdc_default_options = 0x54800000
#     forwardable  = true
#     proxiable  = true
#     noaddresses = true
[realms]
      ABC.SAS.COM = {
            kdc = redwood2.abc.sas.com:88
            default_domain = abc.sas.com
      }
[domain_realm]
      .ABC.SAS.com = ABC.SAS.COM
```

If you have a Windows 2000 server, the rc4-hmac encryption is not supported. For Windows 2000 server, do not specify the rc4-hmac encryption. The default encryption will be used.

Note: The machine `redwood2.abc.sas.com` is the Domain Controller.

At the end of this step, restart WebSphere.

Verify the Kerberos Authentication

A Ticket Granting Ticket (TGT) could expire or get lost from the cache. To ensure that a valid TGT is available in the system, use the kinit command. The kinit command obtains and caches the Kerberos ticket-granting tickets.

1. Bring up a command prompt window, and go to the Java directory where the kinit utility resides (for example, C:\jdk1.5.0.19\bin directory).
2. On Windows, run the kinit utility to make a Kerberos request. Substitute the name of the keytab filename, URL address and domain name:

   ```
   kinit -k -t C:\krb5.keytab\redwood2.host.keytab HTTP/redwood2.abc.sas.com@ABC.SAS.COM
   ```

   It is important that the following message displays at the end of the output:

   "New ticket is stored in cache file C:\Documents and settings…"

Configuring the Client Browser to Use SPNEGO

Complete the following steps on the machine with the client browser application to ensure that your Microsoft Internet Explorer browser is enabled to perform SPNEGO authentication.

Configure Local Intranet Domains

1. In the Internet Explorer window, select **Tools** > **Internet Options** > **Security**.
2. Under Local Intranet, click **Sites**.
3. Verify that the checkboxes are selected for the following options:
   Include all local (Intranet) sites not listed in other zones
   Include all sites that bypass the proxy server
4. Add your domain name to the list of websites to ensure that Internet Explorer recognizes any site with your domain name as the intranet.

Configure Intranet Authentication

1. In the Internet Explorer window, select **Tools** > **Internet Options** > **Security**.
2. Under Local Intranet, click **Sites**.
3. On the **Security** tab, select Local Intranet and click **Custom Level**.
4. In the Security Settings – Local Intranet Zone, under **User Authentication**, select **Automatic Logon only in Intranet Zone** and click **OK**.

Verify the Proxy Settings

1. In the Internet Explorer window, select **Tools** > **Internet Options** > **Connections** .
2. Click **LAN Settings**.
3. Verify that the proxy server address and port number are correct.
4. Click **Advanced**.
5. In the **Proxy Settings** dialog box, ensure that all desired domain names are entered in the **Exceptions** field.
6. Click **OK** to close the **Proxy Settings** dialog box.

Specify Integrated Authentication for Internet Explorer

1. On the Internet Options window, click the **Advanced** tab and scroll to **Security settings**. Verify that the checkbox is selected for **Enable Integrated Windows Authentication**.
2. Click **OK**. Restart your Microsoft Internet Explorer to activate this configuration.

Testing SPNEGO Support From a Domain Client PC

SPNEGO testing can be done with the sec_con tool, if it is available on the WebLogic machine. You can access the sec_con tool from a domain client PC by specifying the URL address in the browser application. To obtain the sec_con tool, contact SAS Technical Support.

Following is an example of a URL address used to access the sec_con tool:

http://redwood2.abc.sas.com:7501/sec_con/sec_con_03wls.jsp

Verifying IWA

Log on to SAS Web applications to confirm that no prompt is presented for logon credentials, and that the applications load with the current Windows user logged into the application.

Recommended Reading

IBM Corporation. 2007. *Configuring the client browser to use SPNEGO*. IBM Information Center. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_SPNEGO_config_web.html.

IBM Corporation. 2007. *Configuring the Lightweight Third Party Authentication mechanism. IBM Information Center*. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/tsec_ltpa.html.

IBM Corporation. 2007. *Kerberos configuration file*. IBM Information Center. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/rsec_SPNEGO_config_krb5.html.

IBM Corporation. 2007. *SPNEGO TAI custom properties configuration*. IBM Information Center. Available at http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=/com.ibm.websphere.nd.multiplatform.doc/info/ae/ae/rsec_SPNEGO_tai_attribs.html.

SAS Institute, Inc., 2009. *SAS 9.2 Intelligence Platform: Security Administration Guide*. Cary, NC. SAS Institute, Inc. Available at http://support.sas.com/92administration.

SAS Institute, Inc., 2009. *Configuring IBM WebSphere Application Server 6.1 for Web Authentication with SAS 9.2 Web Applications*. Available at http://support.sas.com/resources/thirdpartysupport/v92m2/appservers/webspheredoc.html.

Massachussetts Institute of Technology., 2009. *Kerberos: The Network Authentication Protocol*. Available at http://web.mit.edu/Kerberos

support.sas.com

SAS is the world leader in providing software and services that enable customers to transform data from all areas of their business into intelligence. SAS solutions help organizations make better, more informed decisions and maximize customer, supplier, and organizational relationships. For more than 30 years, SAS has been giving customers around the world The Power to Know®. Visit us at **www.sas.com**.