**Creating a Kerberos service principal and keytab file that is used by the WebSphere Application Server SPNEGO TAI (deprecated)**

**Procedure**

1. Create a user account in the Microsoft Active Directory for the WebSphere Application Server.

Click **Start->Programs->Administrative Tools->Active Directory Users and Computers**

##Create a service account or admin account on the same domain of the server.

**Important:** Select Password do not expire (service accounts)

Do not select User must change password at next logon

1. Login to any of the server in the same domain. Use the **setspn** command to map the Kerberos service principal name, HTTP/<host name>, to a Microsoft user account.

**Open Command prompt:**

*Setspn -A HTTP/<server name> <Account name>*

***e.g.:*** *Setspn -A http/WinSrv01.contoso.com User1*

*Setspn -A SAP/ User1 User1*

Make sure that you do not have the same SPNs mapping to more than one Microsoft user account. If you map the same SPN to more than one user account, the web browser client can send a NTLM instead of SPNEGO token to WebSphere Application Server.

**Note:** There may already be some SPNs related to the Microsoft Windows hosts that have been added to the domain. You can display those that exist by using the setspn -L command, but you still have to add an HTTP SPN for WebSphere Application Server. For example, setspn -L myappserver would list the SPNs

E.g.: Setspn -L User1

For deleting any additional SPNs mapped or duplicates use the below command to delete the unwanted.

setspn -D HTTP/myappserver.austin.ibm.com myappserver

Eg: *Setspn -D http/ WinSrv01.contoso.com User1*

1. Create the Kerberos keytab file and make it available to WebSphere Application Server. Use the ktpass command to create the Kerberos keytab file (krb5.keytab)

C:\>ktpass -princ <HTTP/www.example.com@EXAMPLE.COM> -mapuser <krbsrv@example.com> -crypto <RC4-HMAC-NT> -ptype KRB5\_NT\_PRINCIPAL -pass <krbPass!> -out <c:\temp\krb5.keytab>

Eg.: **ktpass -princ** HTTP/ *WinSrv01.contoso.com* @*contoso.com* **-mapuser** User1@*contoso.com* **-crypto** ALL **-ptype** KRB5\_NT\_PRINCIPAL **-pass** \*\*\*\*\*\*\*\*\*\*\*\*\*\*\* **-out** C:\Keytab\User1\_ALL.keytab

*\*\* Replace the “\*\*\*” with the account password.*

*-out <location> mention the location where the keytab file to be created.*

*-Crypto --- instead of* <RC4-HMAC-NT> provide ALL, it will enable all possible encryption (RC4, DES, 128 bit, 256 bit)

*References:*

1. [*https://docs.oracle.com/cd/E41633\_01/pt853pbh1/eng/pt/tsec/task\_GeneratingtheKeytabFileandMappingtheServicePrincipalName-8371d4.html*](https://docs.oracle.com/cd/E41633_01/pt853pbh1/eng/pt/tsec/task_GeneratingtheKeytabFileandMappingtheServicePrincipalName-8371d4.html)
2. [*https://www.ibm.com/support/knowledgecenter/en/SS7JFU\_8.5.5/com.ibm.websphere.express.doc/ae/tsec\_SPNEGO\_config\_dc.html*](https://www.ibm.com/support/knowledgecenter/en/SS7JFU_8.5.5/com.ibm.websphere.express.doc/ae/tsec_SPNEGO_config_dc.html)
3. [*https://blogs.technet.microsoft.com/pie/2018/01/03/all-you-need-to-know-about-keytab-files/*](https://blogs.technet.microsoft.com/pie/2018/01/03/all-you-need-to-know-about-keytab-files/)

*Short:*

*Commands to run from Wintel Side*

*1) Setspn -A http/* *WinSrv01.contoso.com User1*

*2) Setspn -A SAP/User1 User 1*

*3) ktpass -princ HTTP/ WinSrv01.contoso.com @contoso.com -mapuser User1@contoso.com -crypto ALL -ptype KRB5\_NT\_PRINCIPAL -pass \*\*\*\*\*\*\*\*\*\*\*\*\*\*\* -out C:\Keytab\User1\_ALL.keytab*