SPNego Kerberos Authentication

SPNego for Kerberos Authentication on the Netweaver Application Server Java

SAP NetWeaver Application Server (AS) Java supports Kerberos authentication for Web-based access with the Simple and Protected GSS API Negotiation Mechanism (SPNego). SPNego enables you to use Kerberos authentication without an intermediary web server and independently of the underlying operating system (OS) of the SAP NetWeaver host.

The following image and steps provide an overview of the communication flow and the systems involved in Kerberos authentication with SAP NetWeaver AS Java (source: help.sap.com)

1. The Web client accesses an AS Java resource with a GET request.
2. The AS Java returns a 401 response code (unauthorized) with a request to initiate SPNego authentication.
3. The Web client recognizes that the host of the AS Java is a member of the Kerberos realm and procures a ticket from the KDC.
4. The Web client then sends the ticket to the AS Java wrapped as a SPNego token.
5. The SPNegoLoginModule reads the token and authenticates the user.

AS Java SPNego versions
Legacy SPNego

The original or as commonly referred to, ‘old’ or ‘legacy’ implementation of SPNego for Kerberos authentication was introduced with J2EE Engine 640 SP 15 and made use of the Krb5LoginModule from SUN/Oracle. Due to a limitation in the JDK only Data Encryption Standard (DES) was supported in the legacy SPNego implementation. Part of the authentication process required direct communication between the AS Java and the Kerberos Distribution Centre.

(New) SPNego

The ‘new’ implementation of SPNego for Kerberos authentication supports DES and RC4-HMAC (and AES in 7.20 and above) and was introduced with the following release and SP levels:

- SAP NetWeaver Web AS 2004 (6.40) SP27
- SAP NetWeaver Web AS 2004S (7.00) SP23
- SAP NetWeaver Web AS 2004S EhP1 (7.01) SP08
- SAP NetWeaver Web AS 2004S EhP2 (7.02) SP06
- SAP NetWeaver Web AS 710 SP15
- SAP NetWeaver Web AS 711 EhP1 (7.11) SP10
- SAP NetWeaver Web AS 720 SP2
- SAP NetWeaver Web AS 730 SP1
- SAP NetWeaver Web AS 731 SP1
- SAP NetWeaver Web AS 740 SP1

During client authentication no communication between the AS Java and the KDC takes place.

If a system is updated to one of the above SP levels and it was previously using legacy SPNego, migration of the configuration to the new SPNego implementation is possible.

The new SPNego implementation offers more user resolution flexibility and is considerably easier to configure than the legacy version. It can also be disabled using a request parameter.

For more information on the new SPNego implementation refer to SAP note 1488409 - New SPNego Implementation and the guide attached to it.

SPNego add-on

To allow 6.40 and 7.0x systems not yet updated to SP levels where the New SPNego was available to support RC4-HMAC the so called SPNego add-on was made available via SAP note 1457499 - SPNego add-on as a deployable solution.

SPNego Configuration

Legacy SPNego

SAP Help Portal: Using Kerberos Authentication for Single Sign-On 7.00 7.01 7.02

SAP Help Portal: Legacy SPNego Configuration for Kerberos Authentication 7.2 7.3 7.31 7.4

Holger Bruchelt's SCN blogs on Configuring and troubleshooting SPNego Part 1 Part 2 Part 3 and Configuring SPNego with ABAP datasource Part 1 Part 2

SAP Note 994791 - SPNego Wizard
SPNego

SAP note 1488409 - New SPNego Implementation. Refer to the guide attached to the note for information configuring the new SPNego implementation and migrating existing configuration.

SAP Help Portal: Using Kerberos Authentication 7.2 7.30 7.31 7.4

SAP Note 762419 - Multi-Domain Logon Using Microsoft Active Directory

SAP Note 1794551 - Add-On for Accepting Kerberos V5 Tokens without an SPNego Envelope

SAP Note 2029432 - Spnego wizard walkthrough for 7.3/7.4 netweaver versions

Wiki SPNego, Creating and adding the keytab file

SPNego add-on

SAP note 1457499 - SPNego add-on

Troubleshooting

SAP Community Network Security place

SAP Help Portal: Troubleshooting 7.00 7.01 7.02 7.30 7.31

SAP Note 1296330 - Security Troubleshooting Guide For NetWeaver J2EE 640/700

SAP KBA 1938645 - Troubleshooting kerberos authentication user resolution issues (New SPNego, Add-on)

SAP KBA 1649110 - SPNego for Kerberos Authentication: NTLM token received in authorization header

SAP Note 934138 - IE browser sends NTLM token instead of Kerberos

SAP Note 1313880 - SPNego with DNS aliases

SAP Note 2037052 - Disbale SPNego and SAML 2.0 With HTTP Header

SAP KBA 1794140 - How to test a key tab file

SAP Note 1708850 - User is authenticated even though change password fails

SAP Note 1639133 - Not able to login after new spnego failed due to NegoEx

SAP Note 1159129 - Password reset not possible in SPNego scenario

SAP Note 1680500 - Error message on logon page after logoff and spnego

SAP KBA 1853759 - SPNEGO does not work after upgrade from NW70x to NW73x

SAP Note 1649251 - new SPNego UserstoreException: Could not refresh user

SAP Note 1546290 - Client names in ticket and authenticator do not match

Holger Bruchelt's SCN blogs on Configuring and troubleshooting SPNego Part 1 Part 2 Part 3 (Legacy but much of the troubleshooting techniques are applicable to the new implementation)

Holger Bruchelt's SCN blog SSO with SPNego not working on Windows 7 / Windows 2008 R2 (Legacy only)

SAP Note 1082560 - SAP AS Java can not start after running SPNego wizard (Legacy only)

SAP Note 1641301 - KDC has no support for encryption type (Legacy only)