Single Sign-On Configuration

DATE: 28th September 2018

Author: Vijay Bhaskar Reddy Gurrala
Review One: Naveen Kumar Reddy
Review Two: Kamalakar Sagiri
INDEX
Introduction ................................................................................................................................. 3
What is Single Sign-On? ................................................................................................................ 3
Steps involved in SSO Configuration ............................................................................................. 4
About Author ................................................................................................................................ 12
Introduction

Single Sign-On (SSO) is becoming more attractive for all the SAP applications due to its security, cost saving and simplicity. With the introduction of Kerberos and SPNEGO as authentication methods, users from different software applications are getting logged in to SAP applications without giving credentials. Further advantages to the authentication methods are the increasing ease of installation process. This SSO Configuration is helped by simple Secure Network Communication (SNC) authentication methods to follow SAP GUI and web-based applications.

This document briefs about the SSO 3.0 Configuration for the SAP ABAP Application server using SNC Kerbros method.

What is Single Sign-On?

Single Sign-On (SSO) Overview

SAP Single Sign-On (SSO) is a SAP software product and it provides a secure authentication and encryption when the users are accessed to SAP and Non-SAP applications with single password. It is intended to improve enterprise security and simplicity by providing access to applications across all systems.

By default SAP Authentication, user can enter username and password for every application server, SAP Single sign-on (SSO) SNC method provides a security authentication encryption within the network and it provides an authentication without username and password by default login to SAP with Active Directory logins.

ADVANTAGES:

Security

- Secure authentication with one strong password no need of additional factors
- All passwords are stored in central place and protected.

Cost saving

- Higher productivity due to reduced efforts to manual reset for user logon.
- Reduce the helpdesk interaction.

Simplicity

- It is generating more productivity and gaining more satisfied users with improved authentication.
- It helps to reduce the time taken by business users to log in to multiple applications.
- With simplicity, it reduces efforts to reset and manage password for multiple SAP Applications.
The following diagram is shown step by step workflow and communication in between different components:

➢ When user click on SAP GUI connection, The Secure Login Client retrieves the SNC name (User Principal Name of the service user) of the respective SAP server system.
➢ The Secure Login Client starts at the Ticket Granting Service a request for a Kerberos Service token.
➢ The Secure Login Client receives the Kerberos Service token
➢ The Secure Login Client provides the Kerberos Service token for SAP single sign-on and secure communication between SAP Client and SAP server.
➢ The user is authenticated, and the communication is secured.

Steps involved in SSO Configuration

<table>
<thead>
<tr>
<th>Step. No</th>
<th>Name of the activity</th>
<th>Owner</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Setup the AD Service account</td>
<td>Network Team</td>
</tr>
<tr>
<td>2</td>
<td>Setup the Service principle name for Service account.</td>
<td>Network Team</td>
</tr>
<tr>
<td>3</td>
<td>Upgrade the SAP Crypto lib version to 8.5</td>
<td>BASIS Team</td>
</tr>
<tr>
<td>4</td>
<td>SAP Note - 2304831 implementation</td>
<td>BASIS Team</td>
</tr>
<tr>
<td>5</td>
<td>Set the profile parameters for SNC in the t-code SNCWIZARD</td>
<td>BASIS Team</td>
</tr>
<tr>
<td>6</td>
<td>Restart the SAP Application server to affect the SNC parameters</td>
<td>BASIS Team</td>
</tr>
<tr>
<td>7</td>
<td>Create or validate the key tab for Kerberos based SNC in the t-code SNCWIZARD</td>
<td>BASIS Team</td>
</tr>
<tr>
<td>8</td>
<td>Mapping windows domain user ID to SAP User ID Using t-code SU01</td>
<td>Security team</td>
</tr>
<tr>
<td>9</td>
<td>Install Secure login client and setup the SNC Settings in the SAP GUI in the client machines</td>
<td>Network Team</td>
</tr>
</tbody>
</table>

Landscape details.

Netweaver 7.4 SP08
Single Sign On 3.0 SP02.
Step 1: Create one service account in the Windows domain controller.

We recommend the format is Kerberos<SID>.

Note: We recommend that you do not use SAP Service<SID> because the Password Never Expires option is not set for this account by default. If the password for this account expires, single sign-on fails.

- Go to Windows AD and create service account as SSA_SNC_SPNEGO

Enable the Password Never Expires option for this account.

Click on finish.

Step 2: Register the Service Principal Name (SPN) for Service account.

Register the Service Principal Names (SPNs) for the service account for the host name of the SAP NetWeaver AS for ABAP and all AS ABAP aliases.

Ensure that all SPNs are unique. Use the setspn -X SPN Name.

Go to Active Directory Users and computers and right click on Service account properties and assign SPN name as per below steps.
In Attribute Editor, edit the SPN and set the required SPN for service account.

In screenshot, we have set **SAP/FQDN of SAP Server** and **HTTP/FQDN of SAP Server**.
Once the Service Principle Name is set, click on Apply and Ok.

**Step 3:** Upgrade the SAP Crypto lib version to 8.5 and restart the Application server.

**Step 4:**
Execute SNCWIZARD T- code in SAP. It will throw an error “**SAPCRYPTOLIB too old**”.
As a solution apply SAP Note – **2304831**.
Download the SAP Note using transaction SNOTE.
Select the SNOTE and execute it.

**Note:** SPNEGO and SNCWIZARD Transactions can work only SAP NetWeaver AS for ABAP 7.4 SPS08 or higher.

Enter the transport request.

![Image of Note Assistant: Note Browser](image)

Implement the automatic correction instructions

![Image of Implementation State](image)

SAP Note is successfully implemented.

**Step 5:** Set the profile parameters for SNC in the t-code SNCWIZARD
Click on continue.

Keep default value and continue.

List the profile values to be set in the system and continue for next step.

Click on Complete and make sure Application server is restarted to affect the parameter values.
Step 6: Create or validate the key tab for Kerberos based SNC in the t-code SPNEGO

Continue for next step and then enter the Service User ID

Click on Service Principal Names tab, it will show SPN names we assigned for service user account.

In below screenshot, user principal uniqueness and Token checks are marked in green. That implies there are no issues found in SPNs.
Click on continue.

Click on Complete and close this wizard.

**Step 7**: Mapping windows domain user ID to SAP User ID Using t-code SU01.

**Step 8**: Install secure Login in client machines.
Step 9: Set the SNC name in SAP GUI properties under Secure Network Settings.

Logon to the application server with SSO with AD logins.

Here we can choose the client and click on user tab.

Then it will logon to the system with AD logins.

With this, the customers who wanted to configure SSO, can make use of this document.
About Author

Vijay Bhaskar Reddy Gurrala has been associated with MOURI Tech for the past 3 years and is having a vast experience across all the products of SAP applications and he has been administrating various flavours of SAP applications, databases and operating systems. Vijay had utilized various sources to build a successful SSO 3.0 authentication methods in a client environment.

********** END OF DOCUMENT**********