PUBLIC
SAP Single Sign-On 3.0 SP02
Document Version: 1.1 – 2020-03-17

Single Sign-On Extensions Library

THE BEST RUN SAP

Content

1 Single Sign-On Extensions Library

Currently, SAP Single Sign-On contains the following extension library:

- Extension for Kerberos Constrained Delegation

Related Information

Extension for Kerberos Constrained Delegation Implementation Guide [page 3]

1.1 Extension for Kerberos Constrained Delegation Implementation Guide

This library provides support for Kerberos constrained delegation.

The functionality consists of the following extensions:

- Service-for-User-to-Self (S4U2Self) extension - AS Java obtains a service ticket for itself on behalf of the currently-authenticated user.
- Service-for-User-to-Proxy (S4U2Proxy) extension - AS Java obtains a service ticket for a target system on behalf of the currently-authenticated user.

> **i Note**
>
> The library currently supports only the `RC4-HMAC` encryption algorithm.

1.1.1 Installation

This section explains the requirements and the procedure for the installation of the extension for Kerberos constrained delegation.

Related Information

System Requirements [page 4]
Installation Steps [page 4]

1.1.1.1 System Requirements

You can install the extension for Kerberos constrained delegation on SAP Netweaver Application Server (AS) Java 7.30 or higher.

1.1.1.2 Installation Steps

Procedure

1. Go to the SAP Software Download Center.
2. Go to the tab *Support Packages & Patches*.
3. Expand *By Alphabetical Index (A-Z)*, and navigate to the *S* section.
4. Navigate as follows: *SAP Single Sign-On* > *SAP Single Sign-On 3.0* > *Comprised Software Component Versions* > *SSO EXTENSION LIBRARY 3.0*.
5. Download `SSOEXTLIB<release>.sca`.
6. Deploy the SCA to the AS Java.

1.1.2 Configuration

The library uses the service user credentials (shared key) to obtain a Ticket Granting Ticket (TGT) from the Key Distribution Center (KDC). The TGT is needed for the S4U2-related communication with the KDC.

The settings for the different realms come from the SPNego configuration in *NetWeaver Administrator* and from a `krb5.conf` file.

The following table gives an overview of the configuration properties: where they are retrieved from and which Kerberos protocol messages they are used in:

Configuration Properties

Property	Source	Usage
KDC host and port (*kdc*)	`krb5.conf`	AS-REQ (obtain TGT) TGS-REQ (S4U2Self) TGS-REQ (S4U2Proxy)
Shared key	SPNego configuration	AS-REQ (obtain TGT)
Service principal name (*spn*)	`krb5.conf`	TGS-REQ (S4U2Self)

Property	Source	Usage
Client name (*cname*)	`krb5.conf`	AS-REQ (obtain TGT) TGS-REQ (S4U2Self) TGS-REQ (S4U2Proxy)

The library implements caches for the configuration and for the Kerberos tickets. The TGT cache is a global cache on VM level while the service tickets are cached in the user sessions. The settings for these caches are maintained as application properties of the *ssoext_krb5* application.

The configuration cache and the global TGT cache are invalidated when one of the following events occurs:

- SPNego configuration is modified.
- Application properties of *ssoext_krb5* are modified.
- Application *ssoext_krb5* is restarted.

Related Information

Configure Kerberos Trust With Key Distribution Center [page 5]
Configure Extension for Kerberos Constrained Delegation [page 6]

1.1.2.1 Configure Kerberos Trust With Key Distribution Center

Context

To configure Kerberos trust between an AS Java and a KDC, you need to do the following:

Procedure

1. Configure the KDC as described in Configuring Key Distribution Center.
2. Enable delegation for the AS Java service user created in the previous step.

> **Example**
>
> If you are using Microsoft Windows Server as a Windows Domain Controller (Kerberos KDC), there are two configuration options for the delegation:
>
> - Kerberos Only
>   With this option, the constrained delegation is allowed only when SPNego is used for authenticating users to AS Java.

> **Note**
>
> The support for this option is implemented only for certain Support Packages (SPs) of SAP NetWeaver AS for Java. See SAP Note 1925450 for the supported SPs.

- Any Authentication Protocol
  With this option, the constrained delegation is allowed regardless of what authentication mechanism is used for authenticating users to AS Java.

As part of the delegation settings in the domain controller, you can maintain a list of systems to which the AS Java service user is allowed to perform constrained delegation.

3. Start the SPNego configuration application as described in Starting the SPNego Configuration Application.

   Choose the *Enable SPNEGO Support* pushbutton and follow the steps of the configuration wizard.

1.1.2.2 Configure Extension for Kerberos Constrained Delegation

Context

The configuration includes the following:

Procedure

- Realm-specific configuration in `krb5.conf` file

  The realm-specific configuration has to be described in a `krb5.conf` file. The syntax of this file follows the MIT specification. Place the file in the `security` subdirectory of the system global share.

  > **Example**
  >
  > `\\centralhost\sapmnt\<SID>\SYS\global\security\krb5.conf`

  > **Note**
  >
  > The configuration in `krb5.conf` is loaded and cached when first used. To reload the configuration settings from the `krb5.conf` file, restart the *ssoext_krb5* application.

  Describe the realms for which constrained delegation is used under the *[realms]* section of the `krb5.conf` file.

Each realm entry has to contain the following properties:

- *kdc*
  This property specifies the host name of the KDC. It may contain a port. If the port is omitted, the default port 88 is used.
- *spn*
  This property specifies a service principal name (SPN) of the SAP NetWeaver AS for Java system. If multiple SPNs were assigned to the AS Java service user during the Configure Kerberos Trust With Key Distribution Center [page 5] step, include all of them in the `krb5.conf` file.
- *cname*
  This property specifies the name of the AS Java service user created in the Configure Kerberos Trust With Key Distribution Center [page 5] step.

Example

Example 1

```
[realms]
    COMPANY.COM = {
        kdc = dc.company.com
        cname = jee-epp
        spn = HTTP/portal.company.com
    }
```

Example

Example 2 (non-default KDC port and several SPNs)

```
[realms]
    COMPANY.COM = {
        kdc = dc.company.com:8888
        cname = jee-epp
        spn = HTTP/portal.company.com
        spn = HTTP/epp.company.com
    }
```

Example

Example 3 (multiple realms)

```
[realms]
    COMPANY.COM = {
        kdc = dc.company.com
        cname = jee-epp
        spn = HTTP/portal.company.com
    }
    ACME.COM = {
        kdc = dc.acme.com
        cname = jee-portal
        spn = HTTP/portal.acme.com
    }
```

- Global Configuration

  The global configuration is done using the application properties of the *ssoext_krb5* application. To maintain those properties, use the *Java System Properties* plug-in in SAP NetWeaver Administrator (NWA).

Go to *NWA* > *Configuration* > *Infrastructure* > *Java System Properties* > *Applications*. Find the application with the name *ssoext_krb5* and modify its properties.

The following properties are defined:

- *enabled*
  This property is used to enable and disable the functionality for Kerberos constrained delegation.

  > **i Note**
  >
  > To activate the constrained delegation functionality, set this property to *true*.

- *tgt.lifetime*
  This property specifies a time period in minutes. The value of this property will be set in the `AS-REQ` messages when ticket granting tickets are requested.
- *service.ticket.lifetime*
  This property specifies a time period in minutes. The value of this property will be set in the `TGS-REQ` messages when service tickets are requested.
- *cached.ticket.expiration*
  This property specifies a time period in minutes. A cached Kerberos ticket is considered expired if its remaining lifetime is less than the value of this property.

1.1.3 Usage

The functionality for Kerberos constrained delegation integrates with the destination service for the AS Java releases described in SAP Note 1924321. In addition, the library provides an API to programmatically obtain Kerberos tokens for single sign-on to the target systems. For example, this API can be used by applications running on older AS Java releases or applications that do not use the destination service.

Related Information

Declarative Usage Using a Destination Service [page 8]
Programmatic Usage [page 9]

1.1.3.1 Declarative Usage Using a Destination Service

You can configure existing HTTP destinations to send an SPNego token as a credential.

Procedure

1. In the *NetWeaver Administrator*, choose the *Configuration* tab.

2. Open *Security* > *Destinations*.
3. Select the destination you want to configure.
4. Choose the *Edit* button.
5. Choose the *Logon Data* tab.
6. From the *Authentication* dropdown list, choose *SPNego*.
7. Save your configuration.

1.1.3.2 Programmatic Usage

The library exposes an API that allows you to obtain Kerberos or SPNego tokens for other systems on behalf of the currently-authenticated user.

For more details, see the *SAP Single Sign-On* section at Javadocs Index of SAP Help Portal. To use the API, your application must define a reference to the *ssoext_krb5* application in the `application-j2ee-engine.xml` deployment descriptor.

```
<reference reference-type="hard">
    <reference-target target-type="application" provider-
name="sap.com">ssoext_krb5</reference-target>
</reference>
```

Example

Example Code of Adding an SPNego token to an HTTP URL Connection from a Destination:

```
import javax.naming.Context;
import javax.naming.InitialContext;
import com.sap.security.core.server.destinations.api.DestinationException;
import com.sap.security.core.server.destinations.api.DestinationService;
import com.sap.security.core.server.destinations.api.HTTPDestination;
import com.sap.security.ssoext.krb5.api.Krb5TokenServiceFactory;
import com.sap.security.ssoext.krb5.api.Krb5TokenService;
...
Context ctx = new InitialContext();
DestinationService dstService = (DestinationService)
ctx.lookup(DestinationService.JNDI_KEY);
  if (dstService == null) {
    throw new NamingException("Destination Service not available");
  }
HTTPDestination httpDestination = (HTTPDestination)
dstService.getDestination("HTTP", "dest-1");
HttpURLConnection httpConnection = httpDestination.getURLConnection();
Krb5TokenServiceFactory.getKrb5TokenService().addHttpSPNegoToken(httpConnectio
n);
```

Example

Example Code of Obtaining an SPNego Token and Setting the Token as an “Authorization” Header:

```
import java.net.URL;
import java.net.HttpURLConnection;
import com.sap.security.ssoext.krb5.api.Krb5TokenServiceFactory;
import com.sap.security.ssoext.krb5.api.Krb5TokenService;
...
URL url = new URL("http://server.company.com");
```

```
byte[] spnegoTokenBytes =
Krb5TokenServiceFactory.getKrb5TokenService().getHttpSPNegoToken(url.getHost()
);
String spnegoToken = Base64.encode(spnegoTokenBytes);
HttpURLConnection connection = (HttpURLConnection) url.openConnection();
connection.setRequestProperty("Authorization", "Negotiate " + spnegoToken);
```

1.1.4 Troubleshooting

This section can help you solve problems with the configuration or usage of the extension for Kerberos constrained delegation.

Related Information

Trace Locations [page 10]
Collecting Traces Using the Troubleshooting Wizard [page 10]
Support Component [page 11]

1.1.4.1 Trace Locations

The library writes traces to the following trace locations:

- `com.sap.security.ssoext.krb5`
- `com.sap.security.krb5`

1.1.4.2 Collecting Traces Using the Troubleshooting Wizard

Context

To collect traces for Kerberos constrained delegation using the Troubleshooting Wizard, proceed as follows:

Procedure

1. Open the standalone Security Troubleshooting Wizard by accessing `https://<host>:<port>/tshw`

2. Create an incident for the Kerberos constrained delegation and add the trace locations as described in Managing Incidents.
3. Collect traces for this incident as described in Collecting Traces for Troubleshooting Security Problems.

1.1.4.3 Support Component

The support component for Kerberos constrained delegation is `BC-IAM-SSO-FED`.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon  : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon  : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

www.sap.com/contactsap

THE BEST RUN SAP