Joget SSO to Active Directory with Kerberos

Introduction

This article describes the single sign-on (SSO) setup between Joget and Microsoft Active Directory using Kerberos and SPNEGO.

Kerberos is a network authentication protocol designed by the Massachusetts Institute of Technology (MIT) for SSO in client-server environments, while SPNEGO (Simple and Protected GSS-API Negotiation Mechanism) extends Kerberos SSO to web applications.

Test Environment

- Joget Server: Joget Workflow v6 Enterprise on Apache Tomcat 8 and Java 8
- Windows Server: Windows Server 2012 R2 Datacenter (running on VirtualBox within a NAT Network, downloaded from https://www.microsoft.com/en-us/evalcenter/evaluate-windows-server-2012-r2)
- Windows Client PC: IE11 on Windows 10 (running on VirtualBox within a NAT Network, downloaded from https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/)

Test Settings

- Windows Server COMPUTER NAME is WIN-TKDH9LCHUUO
- WINDOWS DOMAIN is windows.local
- DOMAIN USER is joget
- JOGET DOMAIN is joget.windows.local

- This article assumes familiarity with the basics of Windows Server and Windows 10 system and network administration
- This setup is tested within a local VirtualBox environment. Actual setup on a different environment should be adapted accordingly.

Kerberos SSO Setup Configuration

1. Setup Windows Server Kerberos Key Distribution Center (KDC):

1.1 Install DNS Server

1. Go to Server Manager > Add roles and features to install the DNS Server.

   blocked URL
2. In the Network and Sharing Center, configure the network adapter so that the Preferred DNS server is 127.0.0.1.

   blocked URL
3. In the DNS Manager, right click on the server name and Configure a DNS Server to create a forward lookup zone for windows.local.

   blocked URL

1.2 Add Joget Domain Name into the Windows Server DNS

1. In the windows.local DNS zone, add an A record for joget to point to the Joget server IP.

   blocked URL
2. Test ping to ensure that joget.windows.local resolves to the correct IP.

   blocked URL

1.3 Create a Windows Domain User for the Service

1. In Active Directory Users and Computers, create a domain user joget. This is the user account to be mapped to the service name used by the Joget server.

   blocked URL

1.4 Register Service Principal Name (SPN)

1. In PowerShell, execute: setspn -s HTTP/{JOGET DOMAIN} {DOMAIN USER} e.g.

   ```
   setspn -s HTTP/JOGET.WINDOWS.LOCAL joget
   ```

blocked URL

In PowerShell, check that the SPN has been registered

```
setspn -L joget
```

should display

```
Registered ServicePrincipalNames for CN=Joget,CN=Users,DC=windows,DC=local:
     HTTP/JOGET.WINDOWS.LOCAL
```

2. Setup Joget Server for Kerberos

2.1 Add Windows Domain to Hosts File

1. Edit /etc/hosts (Linux or macOS) or C:\Windows\System32\drivers\etc\hosts (Windows) and add the server IP e.g.

```
192.168.56.102        windows.local win-tkdh9lchuuo win-tkdh9lchuuo.windows.local
```

> NOTE: This step is not required if the Joget Server is using the Windows Server as the DNS server.

2.2 Create Kerberos Identification (Keytab) File

Using Windows

1. In PowerShell on the Windows Server, generate a keytab file using the Ktpass tool:

```
ktpass -out joget.keytab -mapuser joget@WINDOWS.LOCAL  -pass Pass@word1  -crypto all -ptype
KRB5_NT_PRINCIPAL  -princ HTTP/joget.windows.local@WINDOWS.LOCAL
```

   blocked URL
2. Copy the generated joget.keytab file into the Joget server e.g. at C:\Joget-v6-Enterprise\wflow\joget.keytab

3. Java 8 may be required for the Kerberos authentication to work with the ktpass generated keytab. Download and install JDK 8, and edit the tomcat-run.bat startup script to update the JAVA_HOME path accordingly.

4. Create a krb5.ini file under C:\Windows folder with these configurations:

```
[libdefaults]
default = WINDOWS.LOCAL
default_realm = WINDOWS.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true

[realms]
   WINDOWS.LOCAL = {
       kdc = WIN-TKDH9LCHUUO.WINDOWS.LOCAL:88
       default_domain = WINDOWS.LOCAL
   }

[domain_realm]
   .windows.local = WINDOWS.LOCAL
   windows.local = WINDOWS.LOCAL
```

Using Linux

1. Install the krb5-user package

```
sudo apt-get install krb5-user
```

   and configure the realm as WINDOWS.LOCAL and the KDC as WIN-TKDH9LCHUUO.WINDOWS.LOCAL:88

2. In a terminal, run

```
kinit joget@WINDOWS.LOCAL
```

> IMPORTANT NOTE: The domain must be UPPER CASE

The command should run without error

3. Confirm the configuration in /etc/krb5.conf

```
[libdefaults]
default = WINDOWS.LOCAL
default_realm = WINDOWS.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true

[realms]
   WINDOWS.LOCAL = {
       kdc = WIN-TKDH9LCHUUO.WINDOWS.LOCAL:88
       default_domain = WINDOWS.LOCAL
   }

[domain_realm]
   .windows.local = WINDOWS.LOCAL
   windows.local = WINDOWS.LOCAL
```

> IMPORTANT NOTE: The domain must be UPPER CASE

4. In a terminal, generate a keytab file using:

```
ktutil
ktutil: add_entry -password -p HTTP/JOGET.WINDOWS.LOCAL@WINDOWS.LOCAL -k 1 -e arcfour-hmac-md5
Password for HTTP/JOGET.WINDOWS.LOCAL@WINDOWS.LOCAL:
ktutil: wkt /etc/joget.keytab
```

5. List the SPNs in the keytab using:

```
ktutil
ktutil: rkt /etc/joget.keytab
ktutil: list
```

Using macOS

1. In a terminal, run

```
kinit joget@WINDOWS.LOCAL
```

IMPORTANT NOTE: The domain must be UPPER CASE

The command should run without error, or just a warning "Encryption type arcfour-hmac-md5(23) used for authentication is weak and will be deprecated"

2. Edit /etc/krb5.conf

```
[libdefaults]
default = WINDOWS.LOCAL
default_realm = WINDOWS.LOCAL
dns_lookup_realm = true
dns_lookup_kdc = true

[realms]
   WINDOWS.LOCAL = {
       kdc = WIN-TKDH9LCHUUO.WINDOWS.LOCAL:88
       default_domain = WINDOWS.LOCAL
   }

[domain_realm]
    .windows.local = WINDOWS.LOCAL
    windows.local = WINDOWS.LOCAL
```

IMPORTANT NOTE: The domain must be UPPER CASE

3. In a terminal, generate a keytab file using:

```
ktutil -k joget.keytab add -p HTTP/JOGET.WINDOWS.LOCAL@WINDOWS.LOCAL -e arcfour-hmac-md5 -V 1
```

4. List the SPNs in the keytab using:

```
ktutil -k joget.keytab list
```

5. Keep a copy of the generated joget.keytab file e.g. in /etc/joget.keytab

3. Configure Kerberos Directory Manager Plugin

3.1 Upload Kerberos Directory Manager Plugin

1. Download the Kerberos Directory Manager plugin from the Joget Marketplace and upload it in Settings > Manage Plugins.

   blocked URL

3.2 Configure Kerberos Directory Manager Plugin

1. In Settings > Directory Manager, select the Kerberos Directory Manager plugin, and key in the appropriate values in the configuration:

   - Service Principal: HTTP/JOGET.WINDOWS.LOCAL
   - Path to Keytab File: /etc/joget.keytab (Linux) or C:/Joget-v6-Enterprise/wflow/joget.keytab (Windows)
   - Debug Enabled: View debugging messages in the logs

blocked URL

> ⚠ Please remember to configure the LDAP Directory Manager as external directory manager to retrieve users from Active Directory.

3.3 Configure API Domain Whitelist

1. In Settings > General Settings, set the API Domain Whitelist to * to allow SSO requests to the Kerberos Directory Manager.

   blocked URL

4. Setup Client PC for SSO

4.1 Add Client PC to Windows Domain

1. Ensure that the Windows Server is reachable on the network from the Client PC.
2. Set the DNS server to the IP address of the Windows Server.

   blocked URL
3. Ping the windows domain name to test.

   blocked URL
4. Click on File Explorer, right click on the This PC and choose Properties. Click on Change Settings next to the computer name. Click on Change and set the Domain e.g. windows.local, keying in the domain administrator login when prompted. Restart after joining the domain is successful, and login as a domain user.

   blocked URL

4.2 Setup Browser for Windows Authentication

1. In IE, click on Internet Options > Security > Local intranet site > Advanced and add the Joget domain e.g. http://joget.windows.local

   blocked URL

4.3 Test the SSO

1. Using the Kerberos Directory Manager plugin approach, access http://joget.windows.local/jw/web/json/plugin/org.joget.plugin.kerberos.KerberosDirectoryManager/service to SSO.

   > ⓘ Please note that for the SSO to work properly:
   >
   > - the client PC and Joget server must reside on different machines
   > - the Windows server and client PC must reside on the same Windows domain

Resources

Introduction to Kerberos and SPNEGO

- http://thekspace.com/home/component/content/article/54-kerberos-and-spnego.html
- https://developer.ibm.com/answers/questions/246107/what-is-the-difference-between-kerberos-and-spnego.html?lnk=hm
- http://web.mit.edu/kerberos/www/index.html

Configuring Kerberos on Windows Server

- https://technet.microsoft.com/en-us/library/hh831553(v=ws.11).aspx
- https://msftplayground.com/2009/08/configure-kerberos-authentication/
- https://technet.microsoft.com/en-us/library/cc731241(v=ws.11).aspx
- https://technet.microsoft.com/en-us/library/hh831553(v=ws.11).aspx
- https://msftplayground.com/2009/08/configure-kerberos-authentication/

Kerberos with Java and Spring

- https://venkatsadasivam.com/2009/08/29/single-sign-on-in-java-platform/
- http://docs.spring.io/spring-security-kerberos/docs/1.0.1.RELEASE/reference/htmlsingle/
- http://projects.spring.io/spring-security-kerberos/
- https://tomcat.apache.org/tomcat-8.0-doc/windows-auth-howto.html
- http://docs.oracle.com/javase/jndi/tutorial/ldap/security/gssapi.html
- http://docs.oracle.com/javase/8/docs/technotes/guides/security/jgss/lab/part1.html#PART1
- https://docs.oracle.com/cd/E23943_01/web.1111/e13707/sso.htm#SECMG481
- https://stackoverflow.com/questions/25289231/using-gssmanager-to-validate-a-kerberos-ticket

Tips

- Kerberos Auto Redirection From External Navigation