Subversion Plugin HTTPS Kerberos authentication

Introduction

If the Subversion SCM of your build needs access to a repository on a Web server which is configured to accept only a Kerberos authentication. Typically servers in a company network using the domain accounts to grant the access to the hosted resources.

This setup was tested with a MS Active Directory 2008 R2 but should also work with other Directory servers. As Web front-end an Apache 2.4 with mod_auth_kerb 5.4 on Linux was used. The Jenkins slaves were running on Windows 10 and Linux - the required configuration you'll find below.

For Windows two different setups are explained: a slave which is member of a domain and a standalone slave without domain membership. The second configuration is about the same as for Linux.

Prerequisites

- A working Jenkins instance - has been tested on Linux RHEL 7 and Open SUSE 42 with Jenkins 2.32.3
- Subversion plugin 2.7.2 has been tested
- Oracle JRE 1.8 with JCE installed - details below
- Kerberos V5 installation and configuration on the master or slave were the jobs with Subversion will run - only MIT Kerberos has been tested on Linux, for Windows no dedicated setup is required
- A domain account that has access to your Subversion server/repository
- For testing a native Subversion 1.8 client is recommended

Configure the Oracle JRE with Java Cryptography Extension (JCE)

Oracles Java runtime does not include encryption algorithms required by Kerberos due to U.S. export regulations. You must download the JCE extension and install it manually. Follow the instructions in the package which are the same for Linux and Windows.

The same applies to the JRE/JDK from IBM and the Open JDK, downloads are available.

Server certificates

For HTTPS communication the Apache server is using a certificate. Make sure that the Certificate Authority (CA) of the server certificates is trusted by Java. As an alternative add the CA in the Subversion servers, parameter: ssl-authority-files.

Prepare and test the domain account

Important: The password for the domain account should never expire/changed, otherwise a keytab must be re-created.

Linux

That the domain account is not compromised because the credentials are saved in clear text somewhere in the file system Kerberos is using a keytab file. In this file the domain credentials are stored encrypted. The keytab can be created by your domain administrator. When you have the password for the account you also can create the keytab by yourself. Here is the procedure:

```
$ ktutil
ktutil: addent -password -p JenkinsAccount@DOMAIN.ORG -e RC4-HMAC -k 1
Password for JenkinsAccount@DOMAIN.ORG: xxxxxx
ktutil: wkt JenkinsAccount.keytab
ktutil: q
```

Let's have a look to the content of the keytab:

```
$ klist -kte JenkinsAccount.keytab
Keytab name: FILE: JenkinsAccount.keytab
KVNO Timestamp           Principal
---- ------------------- ------------------------------------------------------
   1 03/18/2017 18:38:28 JenkinsAccount@DOMAIN.ORG (arcfour-hmac)
```

Use the keytab file to test the authentication, run the following command:

```
$ kinit -kt JenkinsAccount.keytab JenkinsAccount@DOMAIN.ORG
```

When the run was successful (no output) let's have a look to the created TGT:

```
$ klist
Ticket cache: DIR::/run/user/1000/krb5cc/tkt
Default principal: JenkinsAccount@DOMAIN.ORG

Valid starting       Expires              Service principal
03/19/2017 15:59:30  03/20/2017 01:59:30  krbtgt/DOMAIN.ORG@DOMAIN.ORG
        renew until 03/20/2017 15:59:30
```

Test the access to the Subversion repository with a native Subversion client.

If no TGT is available run:

```
$ kinit -kt JenkinsAccount.keytab JenkinsAccount@DOMAIN.ORG
```

Try to get the repository info:

```
$ svn info https://svn.organization.org/repos/HelloWorld/trunk
Path: trunk
URL: https://svn.organization.org/repos/HelloWorld/trunk
Relative URL: ^/trunk
Repository Root: https://svn.organization.org/repos/HelloWorld
Repository UUID: bd8deff7-301f-404f-b90d-11f05c129706
Revision: 309
Node Kind: directory
Last Changed Author: JenkinsAccount@DOMAIN.ORG
Last Changed Rev: 309
Last Changed Date: 2016-11-13 18:52:10 +0100 (Sun, 13 Nov 2016)
```

Windows - domain member

For the slave on a domain computer just try to login to the build machine. Run a svn info to check the access to the repository and that the certificate is accepted.

TGT accessibility
By default, Windows does not allow the session key of a TGT to be accessed. Please add the following registry key on the client side, so that the session key for TGT is accessible and Java can use it to acquire additional service tickets.

When this is not compliant with the security regulation of your company configure the build client in the same way like the standalone client.

For Windows XP and Windows 2000, the registry key and value should be:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos
Value Name: allowtgtsessionkey
Value Type: REG_DWORD
Value: 0x01
```

For Windows 2003 and Windows Vista, the registry key and value should be:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
Value Name: allowtgtsessionkey
Value Type: REG_DWORD
Value: 0x01
```

Windows - standalone

The keytab should be created by the domain admin. Run the following commands to test the validity of the file. Both programs are part of the Java Runtime, do not use the klist program of Windows.

```
> klist -kt C:\Jenkins\etc\JenkinsAccount.keytab
Key tab: C:\Jenkins\etc\JenkinsAccount.keytab, 1 entry found.

[1] Service principal: JenkinsAccount@DOMAIN.ORG
         KVNO: 1

> kinit -t C:\Jenkins\etc\JenkinsAccount.keytab JenkinsAccount@DOMAIN.ORG
New ticket is stored in cache file C:\Users\Jenkins\krb5cc_Jenkins
```

Setup of the Java Kerberos configuration file

Java needs some settings that Kerberos authentication works and they are placed in a file, e.g. JenkinsAccount.conf and this is the content.

Linux and Windows standalone client:

```
com.sun.security.jgss.krb5.initiate {
     com.sun.security.auth.module.Krb5LoginModule required
     useKeyTab=true
     keyTab="/home/jenkins/etc/JenkinsAccount.keytab"
     principal="JenkinsAccount@DOMAIN.ORG"
     debug=false
     ;
};
```

You must replace the path for the keyTab file and the name for the principal. On Windows use a path like this: “C:/Jenkins/etc/JenkinsAccount.keytab”. Additional parameters should be not required.

Windows domain client:

```
com.sun.security.jgss.krb5.initiate {
     com.sun.security.auth.module.Krb5LoginModule required
     renewTGT=true
     doNotPrompt=true
     refreshKrb5Config=true
     useTicketCache=true
     debug=false
     ;
};
```

Configure the master/slave

The following parameters must be added to the JRE configuration:

```
-Djava.security.krb5.conf=/where-ever/krb5.conf
-Dsun.security.krb5.debug=false
-Djavax.security.auth.useSubjectCredsOnly=false
-Djava.security.auth.login.config=/home/jenkins/etc/JenkinsAccount.conf
```

On Linux the first parameter is only required when the file is in another location than the default of your system. For Windows it must be specified all the time.

The debug parameter is optional, set to true for troubleshooting.

Replace the path of the last parameter by your file name.

For the Jenkins master these parameters must be added to the Jenkins configuration. For a slave add them to the JVM Options under Advanced in the node configuration page.

Restart the master/slave.

Configure your Jenkins job

Under Source Code Management -> Subversion add just the URL of your repository and leave the credential empty.

Note for master: when you move the text pointer out of the text field, you will immediately see a red error message, in case your configuration does not work.

Note for slave: the authentication test every time will return an error. It looks like that this test is initiated on the master and not on the slave. Just run a job on the slave and check the log.

Troubleshooting

- First make sure that the Kerberos authentication is woking with a native Subversion client. The client needs no special configuration. On Linux use only a client which is part of the distribution. Third party clients normally do not support Kerberos, e.g. CollabNet Linux packages.
- You may try turning on debugging - use the debug parameter in the Java configuration file and sun.security.krb5.debug. Disable both after the issue is solved - the log files will grow rapidly.
- For a job running on the master check the Jenkins log file.
- For jobs running on a slave check the log of the slave and of the job.

Some hints

- This setup works only when all jobs on the master or on a slave are using the same domain account for Subversion access. When different accounts are required it should be applicable to configure a slave for each domain account, even on the same computer. On a master this is not possible.
- This setup has not been tested on a Jenkins master running on Windows.
- This setup has not been tested with VisualSVN.