ELO IndexServer SSO

W. Imig

19.05.2009

Abstract

Single Sign On enabled applications do not force users to enter passwords for authentication. They use the credentials hold in the session of the operating system to verify the user's identity.

E. g. via the Integrated Windows Authentication, the Internet Explorer can access protected resources published by IIS without prompting for the user's password.

ELO IndexServer client applications can use the HTTP authentication mechanisms NTLM and SPNEGO to logon users to ELO, provided that the operating system users are configured in ELO with the same name – the password might be different.

Configuring NTLM is much easier than SPNEGO but can only be used, if IndexServer is running on a Windows server. Using SPNEGO requires Java 6.0 on the server and a somewhat error-prone Kerberos configuration.

This documentation only shows how to implement SPNEGO in environments that use a Windows Active Directory.

1 Requirements

- IndexServer 7.00.002
- EloixClient.jar resp. EloixClientCS.dll from IndexServer_Programming 7.00.002

2 Configure NTLM for IndexServer on Windows

The required modules for NTML authentication can be found in the folder "NTLM Authentication" in the IndexServer download package.

2.1 Requirements

- Server must run on a Windows operating system.
- Tomcat must run under Local System account or an account with SeTcbPrivilege "Act as part of the operating system".
- Java Runtime on the server must be 5.0 or newer.
- Java client applications must run on Java 5.0 Update 8 or newer.

2.2 Configuration

- Copy "IndexServer.zip/NTLM Authentication/Win32/EloixNtlmAuth.dll" resp. "…Win64…" into the Tomcat\bin folder
- Copy "IndexServer.zip/NTLM Authentication/eloixntlmauth.jar" into the Tomcat5.5\shared\lib resp. Tomcat6\lib folder.
- Restart Tomcat

- On Windows 2003 clients, add the server name to the trusted sites in the local intranet area.

2.3 Verify Configuration

Open the Internet Explorer and navigate to the IndexServer:

http://srvt02:8080/ix-elo70/ixlogin?streamversion=7.00.000.000

- Replace srvt02:8080 with your server name and port number (do not use localhost as server name)
- Replace elo70 with your archive name

The browser should not ask for name and password. The result should look like Abbildung 1, ixlogin response.

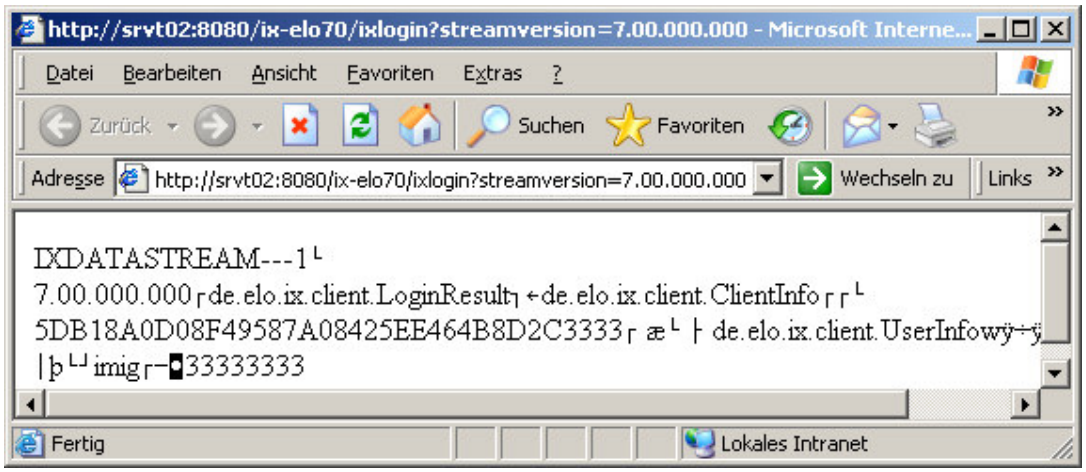

Abbildung 1, ixlogin response

3 Configure SPNEGO

SPNEGO uses the Kerberos protocol which has become an industry standard over the last years.

3.1 Requirements

- Java Runtime on the server must be 6.0 or newer.
- Java client applications must run on Java 6.0 newer.

First of all, a Kerberos principal has to be created for the HTTP service in the Key Distribution Center (KDC).

The following description uses SRVT02 as the server name where the IndexServer (resp. Tomcat) is running and the password “elo” for the user associated to the principal. “ELO.LOCAL” is used for the Kerberos realm (domain name) .

3.2 Provide Kerberos Principal and Keytab-File: java.keytab

- Create a domain user e.g. krb_SRVT02
- Use the ktpass command from the Windows Resource Kit to map the service principal name to the domain user and to generate a Keytab-File. This file contains a private key in order to decrypt incoming request and should not be visible to others than the administrator and the

Tomcat service account.

```
ktpass -princ HTTP/SRVT02.ELO.LOCAL@ELO.LOCAL
-pass elo -mapuser krb_SRVT02@ELO.LOCAL
-ptype KRB5_NT_PRINCIPAL
-out C:\java.keytab
-mapOp set
```

Notes:

- *Use always upper case letters in the domain name.*
- *A good place for this file is the directory <eloserverinstdir>/config/kerberos*

3.3 Provide Kerberos Configuration File for Java: jaas-krb5.conf

For using Kerberos with Java, you have to supply a configuration file for the JAAS portion of the Java runtime. The IndexServer needs a configuration file that looks like this:

```
IndexServer {
  com.sun.security.auth.module.Krb5LoginModule required
  debug=false
  useKeyTab=true
  storeKey=true
  keyTab="g:/ELOprofessional/config/kerberos/java.keytab"
  principal="http/SRVT02.ELO.LOCAL@ELO.LOCAL";
};
```

Notes:

- *Use always upper case letters in the domain name.*
- *A good place for this file is the directory <eloserverinstdir>/config/Kerberos/jaas-krb5.conf*
- *If the debug parameter is set to true, the Kerberos layer of the Java VM prints verbose information into Tomcat's stdout*.log file.*

3.4 Configure SPNEGO for IndexServer

The IndexServer configuration must be extended by some entries in the config.xml file, which is located in the directory <eloserverinstdir>/config/ix-<archivename> by default.

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
<comment>parameters for this web application</comment>
<entry key="jdbcurl">jdbc:sqlserver://srvt02:1433</entry>
<entry key="dbdriver">com.microsoft.sqlserver.jdbc.SQLServerDriver</entry>
<entry key="dbpwd">81-41-181-112-57-23-24-141</entry>
<entry key="schema"/>
<entry key="database">elo70</entry>
<entry key="dbuser">elodb</entry>
<entry key="kerberos.jaas.conf">g:/ELOprofessional/config/jaas-krb5.conf</entry>
<entry key="kerberos.login">IndexServer</entry>
<entry key="kerberos.kdc">NEGRIL.ELO.LOCAL</entry>
<entry key="kerberos.realm">ELO.LOCAL</entry>
</properties>
```

Property name	Description
kerberos.jaas.conf	Location of the jaas-krb5.conf file. Mandatory.
kerberos.login	This value corresponds to the first symbol in the jaas-krb5.conf file. Optional, defaults to IndexServer.
kerberos.kdc	Computer name of the Kerberos Key Distribution Center (Active Directory Server). Optional, see 3.5, Provide a Kerberos Configuration File.
kerberos.realm	Kerberos realm (Windows domain name). Optional, see 3.5, Provide a Kerberos Configuration File.

3.5 Provide a Kerberos Configuration File

Usually, the Kerberos Key Distribution Center and realm is common for all (Java) applications on a computer. Thus, it may be more convenient to define this attributes in a global accessible file rather than specifying it for each application.

The Java runtime accepts Kerberos configuration parameters in a file named krb5.ini in the %SystemRoot% directory (krb5.conf in non-Windows operating systems) .

The file looks like this:

```
[libdefaults]
  default_realm = ELO.LOCAL
[realms]
  ELO.LOCAL = {
    kdc = NEGRIL.ELO.LOCAL
  }
```

3.6 Enable Kerberos Authentication for Java Applications on Windows

On the server computer and on all client PCs that should run Kerberos enabled Java applications, a special registry key has to be set.

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
```

See also: http://java.sun.com/javase/6/docs/technotes/guides/security/kerberos/jgss-windows.html

3.7 Configure Integrated Windows Authentication on Windows Client PCs

In order to use the Kerberos authentication for HTTP (SPNEGO) on Windows clients, follow the steps listed in this document: http://technet.microsoft.com/en-us/library/cc779070.aspx.

The Web site to be added there looks like http://SRVT02.ELO.LOCAL.

3.8 Verify Configuration

Open the Internet Explorer and navigate to the IndexServer:

http://SRVT02.ELO.LOCAL:8080/ix-elo70/ixlogin?streamversion=7.00.000.000

- Replace SRVT02.ELO.LOCAL:8080 with your server principal name and port number
- Replace elo70 with your archive name

The browser should not ask for name and password. The result should look like Abbildung 1, ixlogin response.

Notes:

- *Use always the Kerberos principal name for the server name in the URL: SRVT02.ELO.LOCAL instead of SRVT02. Otherwise authentication fails and the debug output in stdout*.log shows a "Checksum failed" error.*

4 Writing Client Applications that use SSO via NTLM or SPNEGO

4.1 Microsoft .NET Platform

The following code fragment logs in via SSO:

```
ClientInfo ci = …
IXConnFactory connFact = …
IXConnection ix = connFact.CreateSso(ci, "mycomputer");
```

4.1.1 .NET on Windows Vista, Windows 7, Windows 2008

Since .NET 2.0 does not support the latest authentication protocols, set registry key HKLM\SYSTEM\CurrentControlSet\Control\Lsa\LMCompatibilityLevel=1
http://technet.microsoft.com/en-us/library/cc960646.aspx

4.2 Java 6.0 Platform

The following code fragment logs in via SSO:

```
ClientInfo ci = …
IXConnFactory connFact = …
IXConnection ix = connFact.createSso(ci, "mycomputer");
```