JAAS
Lounge

LDAPLogin Module 0.3.0

Configuration for Tomcat 5.x
on Linux & Windows

1. Pre-Requirements

Application Server: Tomcat 5.x
Operating System: Linux or Windows
JaasLounge version : 0.3.0

2. Kerberos Configuration

The LADPLogin Module use Kerberos for the authentication against the AD Domain controller.

Configuration File:

Linux: */etc/krb5.conf*

Windows : *c:\windows\system32\krb5.conf*

Add this lines to the configuration file, for authentication against the domain **"SAMPLE.ORG"** with the authentication host in this domain **"HOST".**

krb5.conf

```
[libdefaults]
     default_realm = SAMPLE.ORG
     default_tgs_enctypes = des-cbc-md5
     default_tkt_enctypes = des-cbc-md5

[realms]
SAMPLE.ORG = {
     kdc = HOST. SAMPLE.ORG:88
     kpasswd = HOST. SAMPLE.ORG
}

[domain_realm]
     . sample.org = SAMPLE.ORG
```

3. LDAP Module Configuration

Add this lines to the Jaaslounge configuration file.

jaas.conf

```
AD_Realm {
org.jaaslounge.ldaplm.LDAPLoginModule required
LDAPServerURL="ldap://168.244.10.1:389"
LDAPSuperUserContext="DC=SAMPLE,DC=ORG"
LDAPInitialContextFactory="com.sun.jndi.ldap.LdapCtxFactory"
debug=true;
};

Kerberos2 {
com.sun.security.auth.module.Krb5LoginModule required client=false useTicketCach
e=false useSubjectCredsOnly=true useKeyTab=false;
};
```

PARAMETER	DESCRIPTION
AD_REALM	The name of the Realm
LDAPServerURL	The Ip-Adress or name of the authentication server
LDAPSuperUserContext	Domain name e.g. SAMPLE.ORG
Kerberos2	The name of the realm for the Kerberos authentication

4. Set Jaaslounge Configuration file

There are many ways to set the configuration for tomcat.

You can set a global environment variable in /etc/profile and export the variable.

profile

```
# Jaas Config File for Tomcat
CATALINA_OPTS="Djava.security.auth.login.config=/srv/www/tomcat5/base/conf/jaas.conf"
export CATALINA_OPTS
```

or you can add the configuration file into the java security file "java.security" under the section Default login configuration file.

java.security

```
# Default login configuration file
#
#login.config.url.1=file:${user.home}/.java.login.config
```

or add the variable into the tomcat start up script **/usr/shared/tomcat5/bin/catlina.sh**

catlina.sh

```
# Jaas Config File for Tomcat
CATALINA_OPTS="-Djava.security.auth.login.config=/srv/www/tomcat5/base/conf/jaas.conf"
export CATALINA_OPTS
```

5. Config Realm for Tomcat

Add this lines into the **/srv/www/tomcat5/base/conf/server.xml** file.

server.xml

```
<Realm className="org.apache.catalina.realm.JAASRealm"
       appName="AD_Realm"
       roleClassNames="org.jaaslounge.GroupPrincipal"
       userClassNames="org.jaaslounge.UserPrincipal"
       debug="99"
       useContextClassLoader="false"/>
```

Please uncomment all other relams in this configuration file.

6. Web Application

Set the xml file for the Tomcat application
/srv/www/tomcat5/base/conf/Catalina/localhost

jaaslounge.xml

```xml
<?xml version='1.0' encoding='utf-8'?>
<Context workDir="work/Catalina/localhost/jaaslounge" path="/jaaslounge" docBase="jaaslounge">
  <Logger className="org.apache.catalina.logger.FileLogger"
directory="/srv/www/tomcat5/base/webapps/jaaslounge/log" verbosity="0" prefix="jaaslounge"
timestamp="true"/>
</Context>
```

Create directory /srv/www/tomcat5/base/webapps/jaaslounge/WEB-INF for the Web
Application and add this Test Files.

web.xml

```xml
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE web-app
    PUBLIC "-//Sun Microsystems, Inc.//DTD Web Application 2.3//EN"
    "http://java.sun.com/j2ee/dtds/web-app_2_3.dtd">

<web-app>
    <servlet>
        <servlet-name>More</servlet-name>
        <servlet-class>CMore</servlet-class>
    </servlet>

    <servlet-mapping>
        <servlet-name>More</servlet-name>
        <url-pattern>/monatsrechnung</url-pattern>
    </servlet-mapping>

    <security-constraint>
        <display-name>Es</display-name>
        <web-resource-collection>
            <web-resource-name>testl</web-resource-name>
            <url-pattern>/*</url-pattern>
        </web-resource-collection>
        <auth-constraint>
            <role-name>pdf</role-name>
        </auth-constraint>
        <user-data-constraint>
            <transport-guarantee>NONE
            </transport-guarantee>
        </user-data-constraint>
    </security-constraint>
    <error-page>
        <error-code>404</error-code>
        <location>/monatsrechnung.html</location>
    </error-page>

 <login-config>
  <auth-method>FORM</auth-method>
  <realm-name>Tomcat Server Configuration Form-Based Authentication Area</realm-name>
  <form-login-config>
   <form-login-page>/login.html</form-login-page>
   <form-error-page>/bad_login.html</form-error-page>
  </form-login-config>
 </login-config>

 <!-- Security roles referenced by this web application -->
 <security-role>
  <description>
   The role that is required to log in to the Administration Application
  </description>
```

```
  <role-name>pdf</role-name>
 </security-role>
</web-app>
```

The blue highlighted defines the groupe membership of the authenticated user.
The logon user must into this group to access the page.

7. SSL Connector Configuration

7.1. Default Connector

File: server.xml

PARAMETER	DESCRIPTION
port	The connector port
redirectPort	The redircet port for ssl connection.
debug	Debug level

Bsp.:

```
<Connector port="8080"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
redirectPort="8443"
acceptCount="100"
debug="0"
connectionTimeout="20000"
disableUploadTimeout="true" />
```

7.2. SSL Connector

Datei: server.xml

PARAMETER	DESCRIPTION
port	The connector port.
debug	Debug level
keystoreFile	Keystorefile for ssl connection
keystorePass	Keystorepassword for the keystore file

Bsp.:

```
<Connector port="8443"
maxThreads="150"
minSpareThreads="25"
maxSpareThreads="75"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100"
debug="0"
scheme="https"
secure="true"
clientAuth="false"
sslProtocol="TLS"
keystoreFile="/srv/www/tomcat5/base/conf/keystore"
keystorePass="changeit" />
```

8. Troubleshooting