5.4.3 Kerberos in ApacheDS 1.5.5

ApacheDS 1.5.5

This site was updated for ApacheDS 1.5.5.

Overview

This page shows how to activate and setup the KDC server of ApacheDS 1.5.5 (build from trunk 2009-08-04). This is a very simple setup (host: localhost, realm: EXAMPLE.COM). Need to check the setup for other hosts and realms...

Activate Kerberos

Acivate the keyDerivationInterceptor and the kdcServer. Also set saslHost and saslPrincipal to localhost. Add entries for users **not** before you have activated those elements, otherwise the krb5Key won't be created!

server.xml

```
<spring:beans ...>
  <defaultDirectoryService ...>
    ...
    <interceptors>
      ...
      <keyDerivationInterceptor/>
      ...
    </interceptors>
  </defaultDirectoryService>
   ...

  <!--
  +============================================================+
  | Kerberos server configuration                              |
  +============================================================+
  -->
  <kdcServer id="kdcServer" searchBaseDn="ou=Users,dc=example,dc=com">
    <transports>
      <tcpTransport port="60088" nbThreads="4" backLog="50"/>
      <udpTransport port="60088" nbThreads="4" backLog="50"/>
    </transports>
    <directoryService>#directoryService</directoryService>
  </kdcServer>

  ...

  <ldapServer ...
            saslHost="localhost"
            saslPrincipal="ldap/localhost@EXAMPLE.COM"
            searchBaseDn="ou=users,dc=example,dc=com"
            ...>
  ...

</spring:beans>
```

Here is a complete server.xml: server.xml

Optional: Logging

Configure debug level logging in log4j.properties:

```
log4j.logger.org.apache.directory.server.kerberos=DEBUG
```

Restart the Server

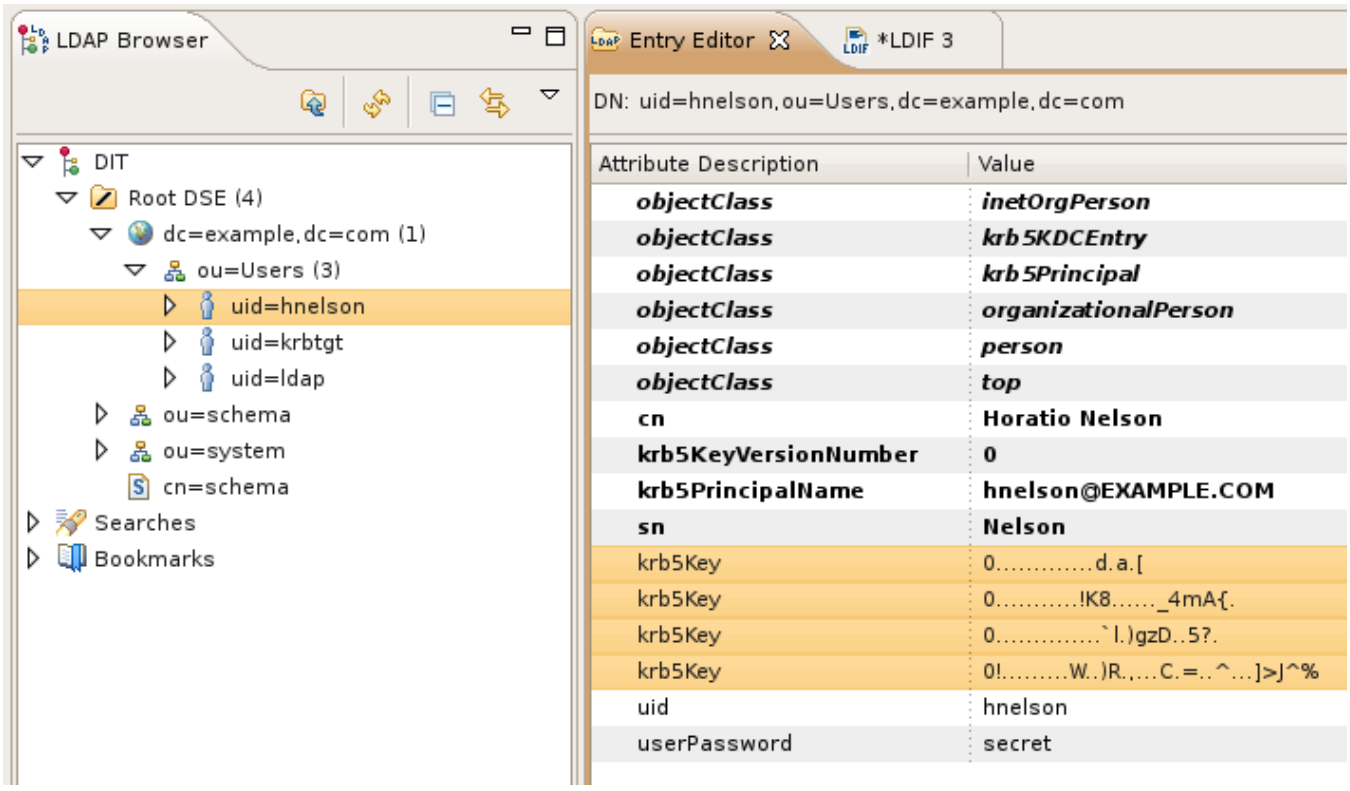
Restart the server, you should see the following output:

```
Starting the Kerberos server
           _                          _          _  __  ____    ___
          / \   _ __    ___  ___| |__   ___| |/ /|  _ \ / __|
         / _ \ | '_ \ / _ |/ __| '_ \ / _ \ ' / | | | / /
        / ___ \| |_) | (_| | (__| | | |  __/ . \ | |_| \ \__
       /_/   \_\ .__/ \__,_|\___|_| |_|\___|_|\_\|____/ \___|
               |_|

[19:28:03] INFO [org.apache.directory.server.kerberos.kdc.KdcServer] - Kerberos service started.
Kerberos service started.
Kerberos server started
```

Load User Data

Load the following data into the server, e.g. using Apache Directory Studio: kdc-data.ldif

Note: The activated keyDerivationInterceptor automatically creates the krb5Key attributes:



Authenticate using kinit (Unix/Linux)

Make sure kinit is installed.

A minimal /etc/krb5.conf file looks as follows (make sure the port matches!):

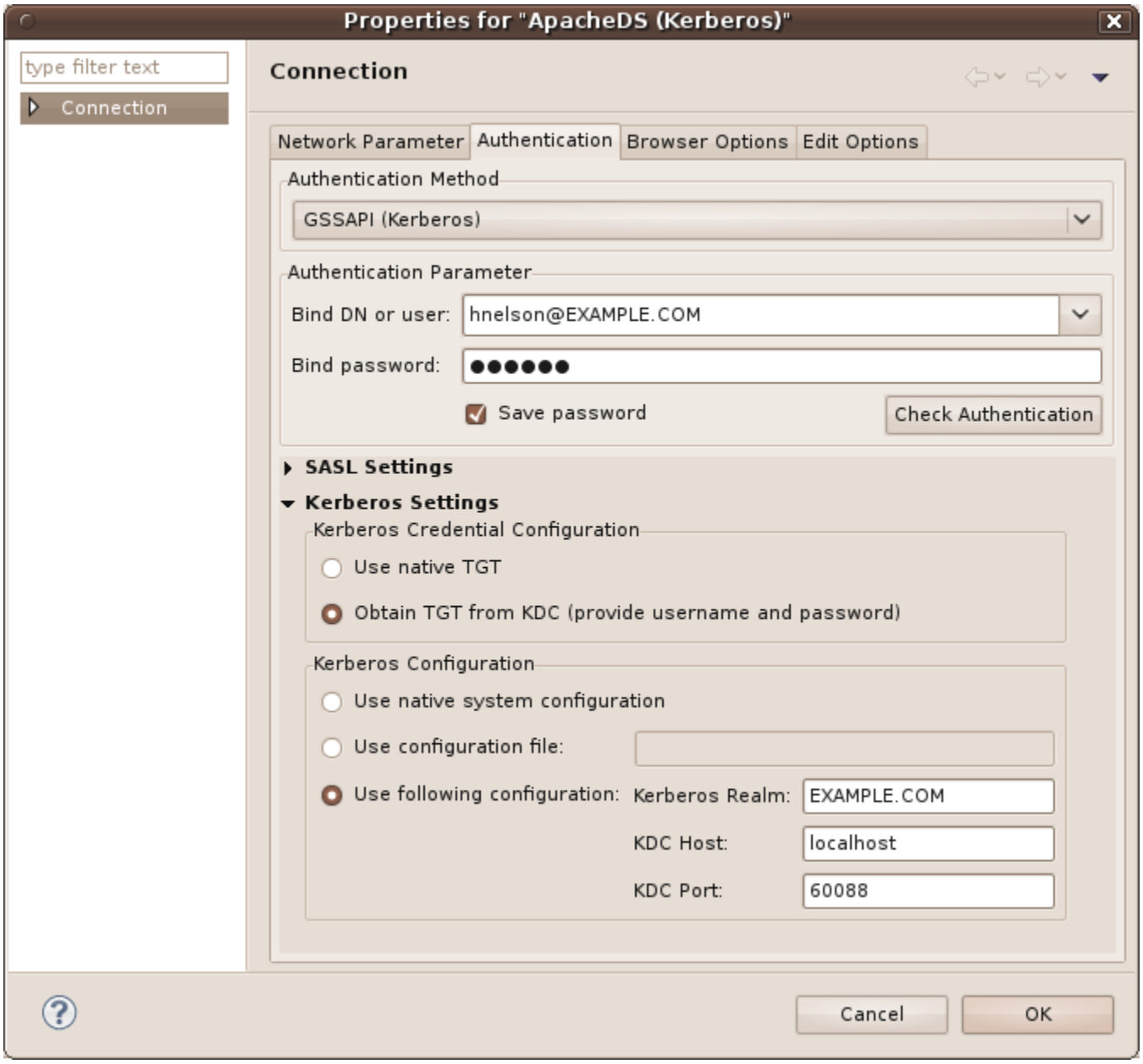
```
[libdefaults]
        default_realm = EXAMPLE.COM

[realms]
        EXAMPLE.COM = {
                kdc = localhost:60088
        }

[domain_realm]
        .example.com = EXAMPLE.COM
        example.com = EXAMPLE.COM

[login]
        krb4_convert = true
        krb4_get_tickets = false
```

Then try to authenticate, password is 'secret':

```
stefan@r61:~$ kinit hnelson@EXAMPLE.COM
Password for hnelson@EXAMPLE.COM:

stefan@r61:~$ klist
Ticket cache: FILE:/tmp/krb5cc_1000
Default principal: hnelson@EXAMPLE.COM

Valid starting     Expires            Service principal
08/04/09 19:54:22  08/05/09 19:54:21  krbtgt/EXAMPLE.COM@EXAMPLE.COM


Kerberos 4 ticket cache: /tmp/tkt1000
klist: You have no tickets cached
```

Authenticate using Apache Directory Studio

You can also configure Apache Directory Studio to use Kerberos (GSSAPI) for authentication. If you use the following authentication parameters you don't need to configure any Kerberos settings in your native operating system.


Properties for "ApacheDS (Kerberos)"
type filter text
Connection
Connection
Network Parameter
Authentication
Browser Options
Edit Options
Authentication Method
GSSAPI (Kerberos)
Authentication Parameter
Bind DN or user:
hnelson@EXAMPLE.COM
Bind password:
Save password
Check Authentication
SASL Settings
Kerberos Settings
Kerberos Credential Configuration
Use native TGT
Obtain TGT from KDC (provide username and password)
Kerberos Configuration
Use native system configuration
Use configuration file:
Use following configuration:
Kerberos Realm:
EXAMPLE.COM
KDC Host:
localhost
KDC Port:
60088
Cancel
OK