Openfire XMPP Server configuration on Windows Server 2008 R2 with SSO

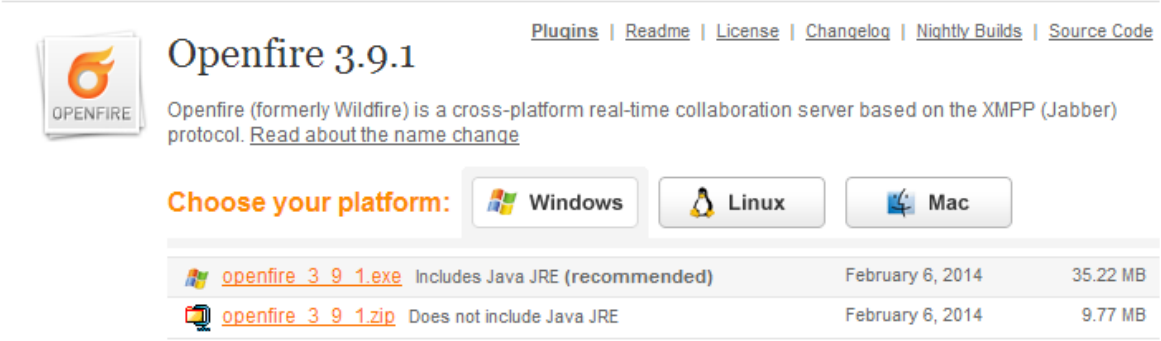
Prerequisites

Windows Server 2008 R2 SP1

Windows 7 64-bit SP1

Openfire 3.9.1.zip http://www.igniterealtime.org/downloads/download-landing.jsp?file=openfire/openfire_3_9_1.zip

Java Runtime Environment 1.6 or higher https://www.java.com/en/download/manual.jsp



Background

To test the configuration of Single Sign On (SSO) with Openfire, I built a small environment consisting of three virtual machines (VM's). This was necessary prior to deploying into a production environment, and being able to fully document the configuration required.

My three VM's were configured as the following:

1. AD.test.com 192.168.0.1 Active Directory Domain Controller, DNS
2. APP.test.com 192.168.0.2 Openfire Application Server
3. VM-1.test.com 192.168.0.3 Windows 7 64-bit client

The Active Directory (AD) domain had a functional domain level of 2008 R2.

Jonathan Murch jonathansmurch@gmail.com

Openfire XMPP Server configuration on Windows Server 2008 R2 with SSO

System Setup

1. Install Java onto the Openfire application server
2. Extract Openfire 3.9.1.zip, and copy and paste the *openfire* directory within to: *C:\Program Files*
3. Open a command prompt and change directory to: *C:\Program Files\openfire\bin*
4. Run command: *openfire-service /install* to install as a Windows service
5. Run command: *openfire-service /start* to start the installed service
6. Add the following value to the registry and reboot, this change allows Java to access the Windows Kerberos ticket cache:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
Value Name: AllowTGTSessionKey
Value Type: REG_DWORD
Value: 1
```

Account Configuration

7. Log on to the Domain Controller (DC) or Key Distribution Center (KDC) using a domain Administrator account
8. Open AD Users and Computers, and create a new user or service account with a user logon name of *xmpp-openfire* and set a secure password. The account only needs to be a member of the *Domain Users* group.
9. On the Account tab of the account, set the account options:
    - *User cannot change password*
    - *Password never expires*
    - *Do not require Kerberos preauthentication*
10. Open a command prompt and create two Kerberos XMPP Service Principal Name (SPN) for the *xmpp-openfire* account using the *setspn* utility
    http://technet.microsoft.com/en-us/library/cc731241.aspx

```
setspn -A xmpp/app.test.com@TEST.COM xmpp-openfire

setspn -A xmpp/app.test.com xmpp-openfire
```

Notes: *app.test.com* should be the Fully Qualified Domain Name (FQDN) of the Openfire application server and *TEST.COM* should be the name of your Kerberos realm which is usually the same as your Windows domain name but all capitalised in uppercase. *Updated object* indicates the account has been modified.

11. From the same command prompt use the *ktpass* utility to map the Kerberos XMPP SPN created in the previous step to the *xmpp-openfire* account

Jonathan Murch jonathansmurch@gmail.com

http://technet.microsoft.com/en-us/library/cc753771.aspx

```
ktpass -princ xmpp/ app.test.com@TEST.COM –mapuser

xmpp-openfire@test.com -pass * -ptype KRB5_NT_PRINCIPAL
```

Notes: *xmpp-openfire@test.com* is the full AD username of the account. If you do not put the name of the AD domain that the account was created in on the end, the utility may not be able to find the user account in AD and report an error. The *-pass* * parameter will indicate to the *ktpass* utility to prompt you for the password for the *xmpp-openfire* account.

Keytab Configuration

12. There are two ways two create the keytab file; by utilising the toolset within the Windows operating system (OS) or with Java. There has been mixed reviews on which is most successful. In my experience I focussed on generating a keytab with Windows. The commands for each can be found below.
    - The Java ktab utility is located in the jre\bin directory of your Java installation directory on the Openfire application server: *C:\Program Files (x86)\Java\jre7\bin*

```
ktab -k xmpp.keytab -a xmpp/app.test.com@TEST.COM
```

The ktab utility will prompt you for the password for the *xmpp-openfire* account.

- For Windows, on the DC open a command prompt:

```
ktpass -princ xmpp/app.test.com@TEST.COM -mapuser xmpp-
openfire@test.com -pass * -crypto RC4-HMAC-NT -ptype
KRB5_NT_PRINCIPAL -out c:\xmpp.keytab
```

The ktab utility will prompt you for the password for the xmpp-openfire account.

Notes: *xmpp-openfire@AD_domain.com* is the full AD name of the account. If you do not put the name of the AD domain that the account was created in on the end, the utility may not be able to find the user account in AD and report back an error.

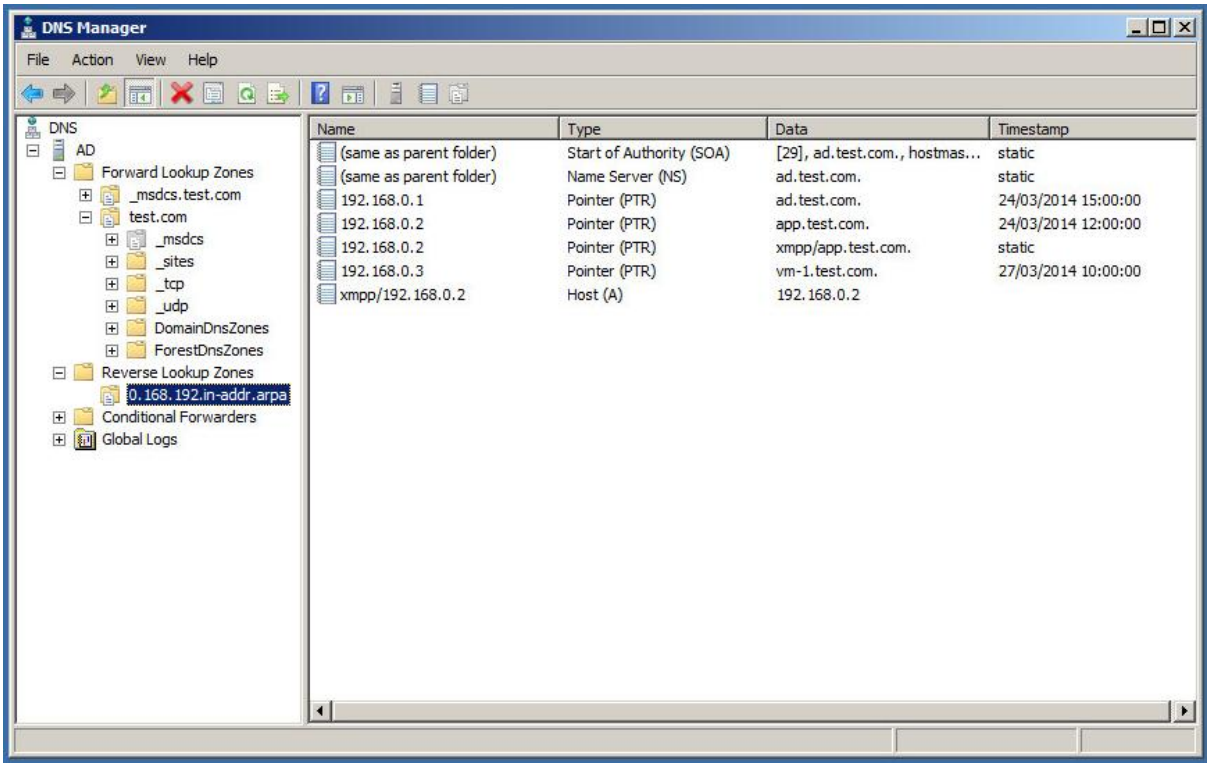
13. The ktab or ktpass utility will have created a file named *xmpp.keytab* , move this file to *C:\Program Files\openfire\resources* of the Openfire application server.

Group Policy

14. Set group policy to allow DES encryption types. To simplify things and conform to best practice use Group Policy and apply it to the Default Domain Policy.
    - Computer Configuration >Policy >Windows Settings >Security Settings >Local Policies >Security Options: Network Security: Configure encryption types allowed for Kerberos
    - Enable all encryption types including DES_CBC_CRC
      http://technet.microsoft.com/en-us/library/dd560670(v=ws.10).aspx

DNS

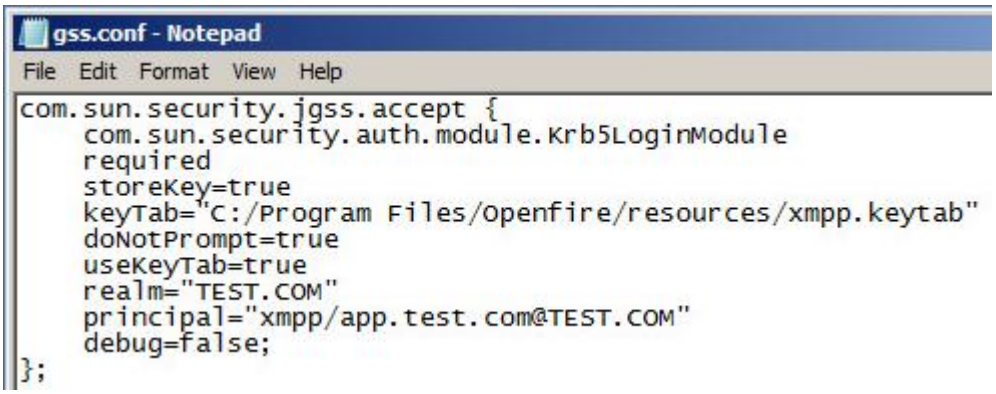
15. A Pointer (PTR) record for the Openfire server and SPN must be in the Reverse Lookup Zone or SSO will not work.



GSSAPI Configuration

16. On the Openfire server create a GSSAPI configuration file named *gss.conf* in the Openfire conf directory (C:\Program Files\Openfire\conf).
    Here's an example of what the gss.conf file should look like:

```
com.sun.security.jgss.accept {
     com.sun.security.auth.module.Krb5LoginModule
     required
     storeKey=true
     keyTab="C:/Program Files/Openfire/resources/xmpp.keytab"
     doNotPrompt=true
     useKeyTab=true
     realm="REALM.COM"
     principal="xmpp/servername.domain.com@REALM.COM"
     debug=true;
};
```

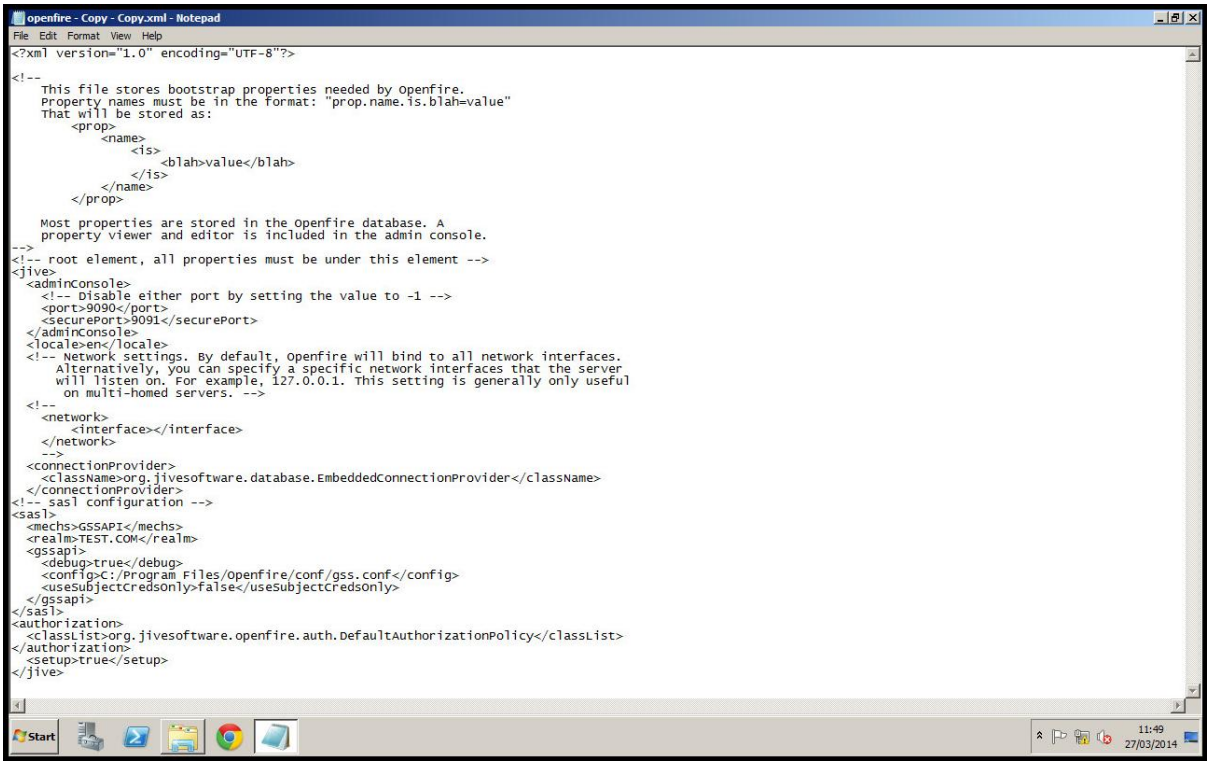


Notes: The last line of the gss.conf file *debug=true* will tell Openfire to debug and log any GSSAPI errors. This is useful while configuring SSO to track down any problems. Once you have confirmed everything is working you can set it to *debug=false*. Also, make sure you use / instead of \ in the keytab path, even on Windows.

17. Enable GSSAPI in Openfire by adding the following section to your *openfire.xml* configuration file found at *C:\Program Files\openfire\conf*:

```
<!-- sasl configuration -->
<sasl>
  <mechs>GSSAPI</mechs>
  <!-- Set this to your Keberos realm name which is usually your AD domain name in
all caps. -->
  <realm>REALM.COM</realm>
  <gssapi>
    <!-- You can set this to false once you have everything working. -->
    <debug>true</debug>
    <!-- Set this to the location of your gss.conf file created earlier -->
    <!-- "/" is used in the path here not "\" even though this is on Windows. -->
    <config>C:/Program Files/Openfire/conf/gss.conf</config>
    <useSubjectCredsOnly>false</useSubjectCredsOnly>
  </gssapi>
</sasl>

<authorization>
  <classList>org.jivesoftware.openfire.auth.DefaultAuthorizationPolicy</classList>
</authorization>
```



18. Start the Openfire service, and then check this configuration is reflected in the System Properties section on the Openfire administration web console.
19. Add the *xmpp.fqdn* property to the FQDN of your Openfire server.
20. Restart the Openfire server

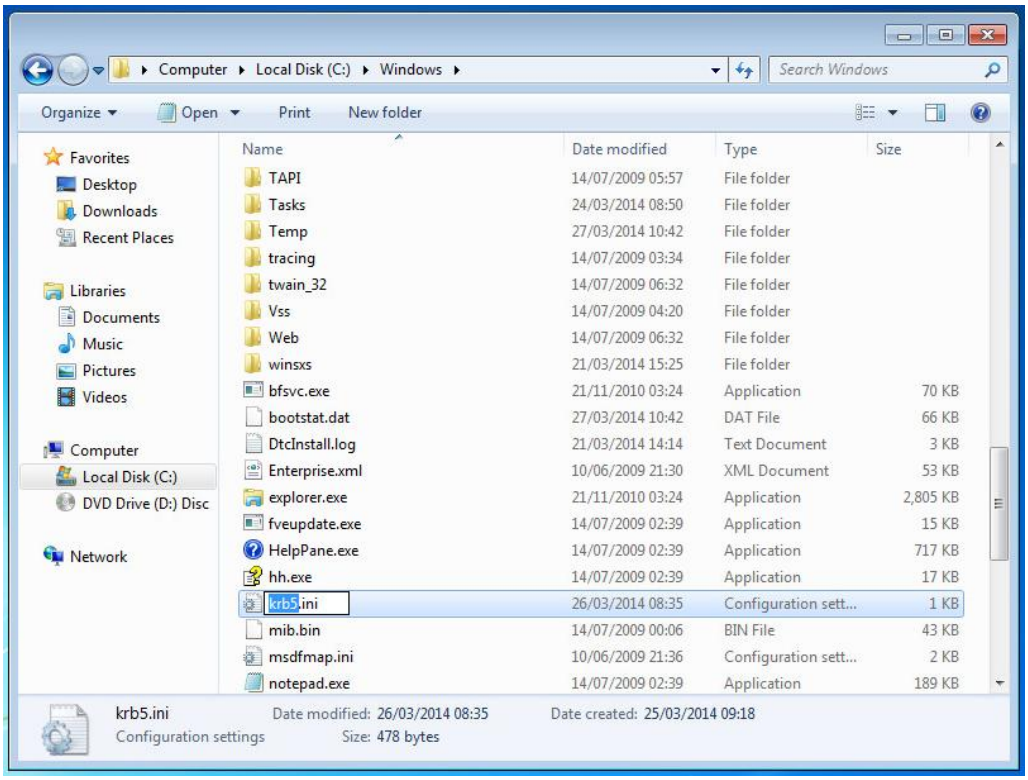
Kerberos Configuration

21. Create a Kerberos configuration file named *krb5.ini* in your Windows installation directory (C:\Windows). This file will also need to be copied to the same directory for each of the Spark clients. Here's an example of what the *krb5.ini* file should look like:

```
[libdefaults]
    default_realm = REALM.COM
    default_tkt_enctypes = rc4-hmac des3-cbc-sha1 des-cbc-crc des-cbc-md5
    default_tgs_enctypes = rc4-hmac des3-cbc-sha1 des-cbc-crc des-cbc-md5
    permitted_enctypes = rc4-hmac des3-cbc-sha1 des-cbc-crc des-cbc-md5

[realms]
    REALM.COM = {
        kdc = kdc1.domain.com
        admin_server = kdc1.domain.com
        default_domain = domain.com
    }

[domain_realms]
    domain.com = REALM.COM
    .domain.com = REALM.COM
```

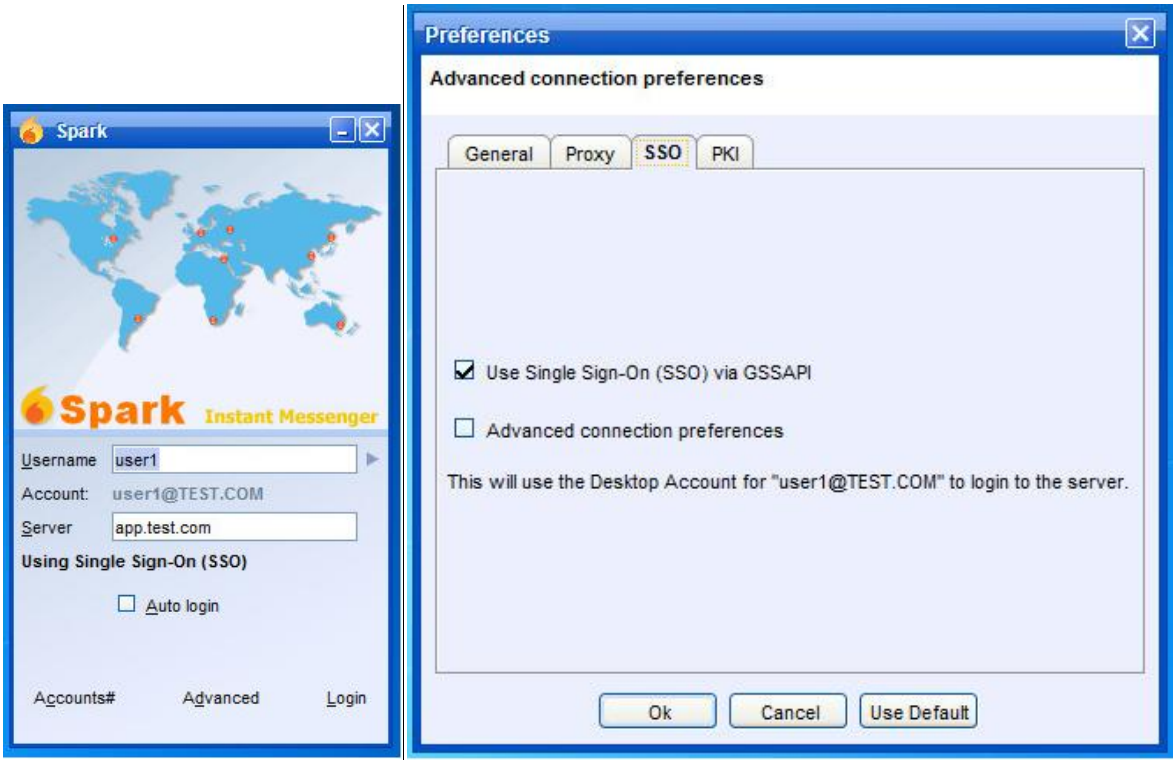


Windows 7 64-bit Spark client

22. Add the following value to the registry of each Spark client. This change allows Java to access the Windows Kerberos ticket cache:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\Kerberos\Parameters
Value Name: AllowTGTSessionKey
Value Type: REG_DWORD
Value: 1
```

23. Check that a copy of the *krb5.ini* is located at *C:\Windows*
24. Restart the Windows 7 client for the changes to take effect
25. Once the Windows 7 client is back up, log into the computer using a domain user account
26. Configure your Spark client and enable the SSO login option on the SSO tab. On the SSO tab Spark should report what username it will attempt to use when logging into the Openfire server. If it reports something about "Unable to find principal" then you've done something wrong. Go back over all the settings, checking carefully there are no typos!



Openfire XMPP Server configuration on Windows Server 2008 R2 with SSO

Terminology

There is a lot of terminology used in regards to SSO so here is a clear definition of what is being referred to:

Authentication - The process of verifying a user really is who the user claims to be.

Authorisation - The process of taking an authenticated user and granting access to particular resources.

SASL - Simple Authentication and Security Layer: This is the basic protocol used for authentication and authorization in the XMPP protocol.

SASL Mechanism - Sometimes just referred to as a "Mechanism", this is a particular method of authentication in SASL. Both the client and server need to agree on a mechanism for authentication to be successful.

Kerberos - The name of the protocol used to authenticate users.

Token - A special piece of information exchanged between two entities. A token will often have authentication and/or authorization information in it.

GSSAPI - Generic Security Service Application Program Interface: A generic way of passing tokens between applications. Kerberos is the primary user of GSSAPI, but not the only.

Username - This is an overly generic term for the name of a user. With SSO its ambiguous by itself, so whenever possible Ill try to clarify. In general Ill refer to the username as being the Openfire username, though.

Principal - The term we use for the username of the Kerberos account. Principals can refer to more than just people, however. Takes the form of username@REALM . Note that the username portion of a principal does not need to match the username of Openfire, but it will greatly simplify things if they do.

Service Principal - Exactly the same thing as a regular principal, but used to denote a service instead of an individual. Takes the form of service/hostname@REALM

Keytab - A keytab is a special file that contains the "password" for a service principal, or more than one service principal. These files contain sensitive information, so they need to be protected appropriately.