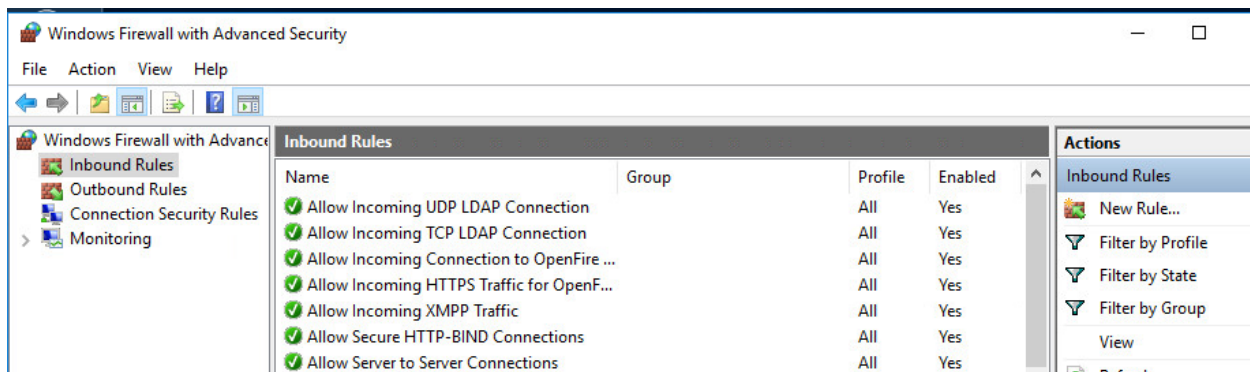
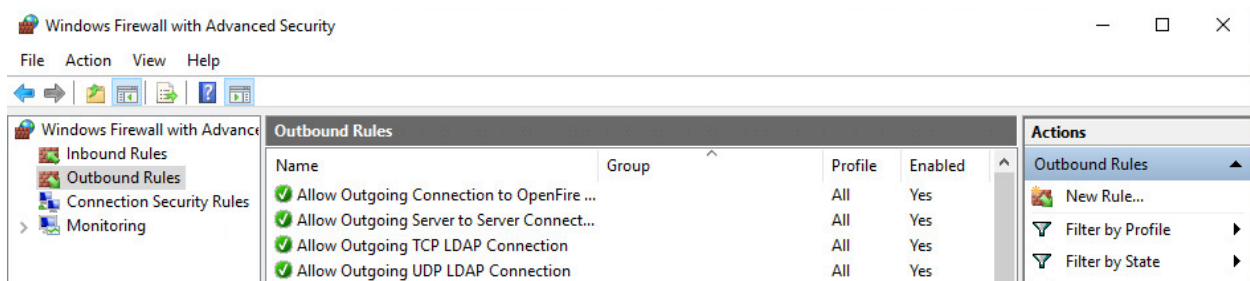


# Openfire Server Setup

Author: Benjamin Dreher

## Firewall Configuration

- **Incoming**
  - Opened TCP port 5222 for incoming XMPP client connections.
  - Opened TCP 9090 (HTTP) and TCP 9091 (HTTPS) ports for remotely connecting to admin console.
  - Opened HTTP-BIND TCP 7443 port.
  - Opened TCP 5269 port for server to server connections (only used for remote server connections, not really necessary in this instance).
  - Opened TCP and UDP 389 port for LDAP connection to ad01.
  - Opened TCP 5432 port for connection to the PostgreSQL database.
- **Outgoing**
  - Opened TCP and UDP 389 port for LDAP connection to ad01.
  - Opened TCP 5269 port for server to server connections (only used for remote server connections, not really necessary in this instance).
  - Opened TCP 5432 port for connection to the PostgreSQL database.



## Openfire Setup

Openfire Setup: Server Settings X

127.0.0.1:9090/setup/setup-host-settings.jsp

Openfire 4.3.2

openfire

Setup

Setup Progress

✓ Language Selection

▶ Server Settings

Database Settings

Profile Settings

Admin Account

### Server Settings

Below are network settings for this server.

XMPP Domain Name:

triplethreat.local

?

Server Host Name (FQDN):

openfire.triplethreat.local

?

Admin Console Port:

9090

?

Secure Admin Console Port:

9091

?

Property Encryption via:

?

☐ Blowfish

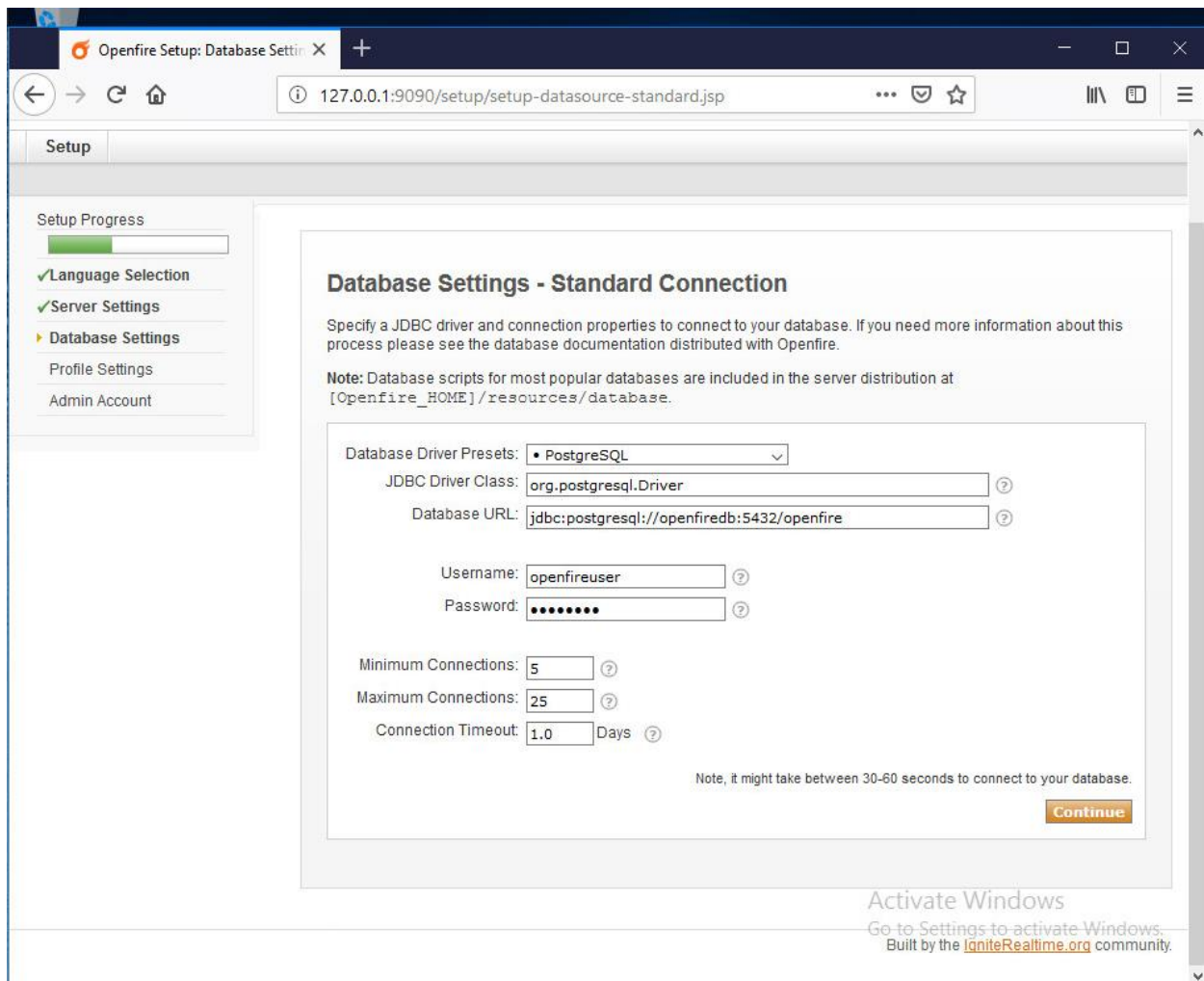
☒ AES

Property Encryption Key:

?

Continue

Built by the [IgniteRealtime.org](https://www.ignite-realtime.org/) community.



**Note:** Connections has nothing to do with how many users can connect at a time, because they don't connect to the DB, they connect to the OpenFire app. This just means how many connections OpenFire will use to the DB.

- 'openfiredb' is the database server hostname
- 5432 is the PostgreSQL port connection
- 'openfire' is the database
- 'openfireuser' is a PostgreSQL user that owns the openfire database

Below is an error that occurred during the database setup. I had to edit the PostgreSQL pg\_hba.conf configuration file on the openfireadb database server to include all databases for all users on all IPs with md5 encryption method (for simplicity sake only, not to be used on a production server for security reasons). I tried only including the openfire host, but it still gave me the same error (although I don't believe I entered the FQDN). I also made sure the postgresql.conf configuration file had listening on all IP addresses in order for the openfire application server to connect.

Suppressed: org.postgresql.util.PSQLException: FATAL: no pg\_hba.conf entry for host "141.210.25.10", user "openfireuser", database "openfire", SSL off

```
pg_hba - Notepad
File Edit Format View Help

#
# This file is read on server startup and when the server receives a
# SIGHUP signal. If you edit the file on a running system, you have to
# SIGHUP the server for the changes to take effect, run "pg_ctl reload",
# or execute "SELECT pg_reload_conf()".
#
# Put your actual configuration here
# -----
#
# If you want to allow non-local connections, you need to add more
# "host" records. In that case you will also need to make PostgreSQL
# listen on a non-local interface via the listen_addresses
# configuration parameter, or via the -i or -h command line switches.


# TYPE DATABASE USER ADDRESS METHOD
# IPv4 local connections:
host all all 127.0.0.1/32 md5
host all all 0.0.0.0/0 md5
# IPv6 local connections:
host all all ::1/128 md5
# Allow replication connections from localhost, by a user with the
# replication privilege.
host replication all 127.0.0.1/32 md5
host replication all ::1/128 md5
```

```
postgresql - Notepad
File Edit Format View Help

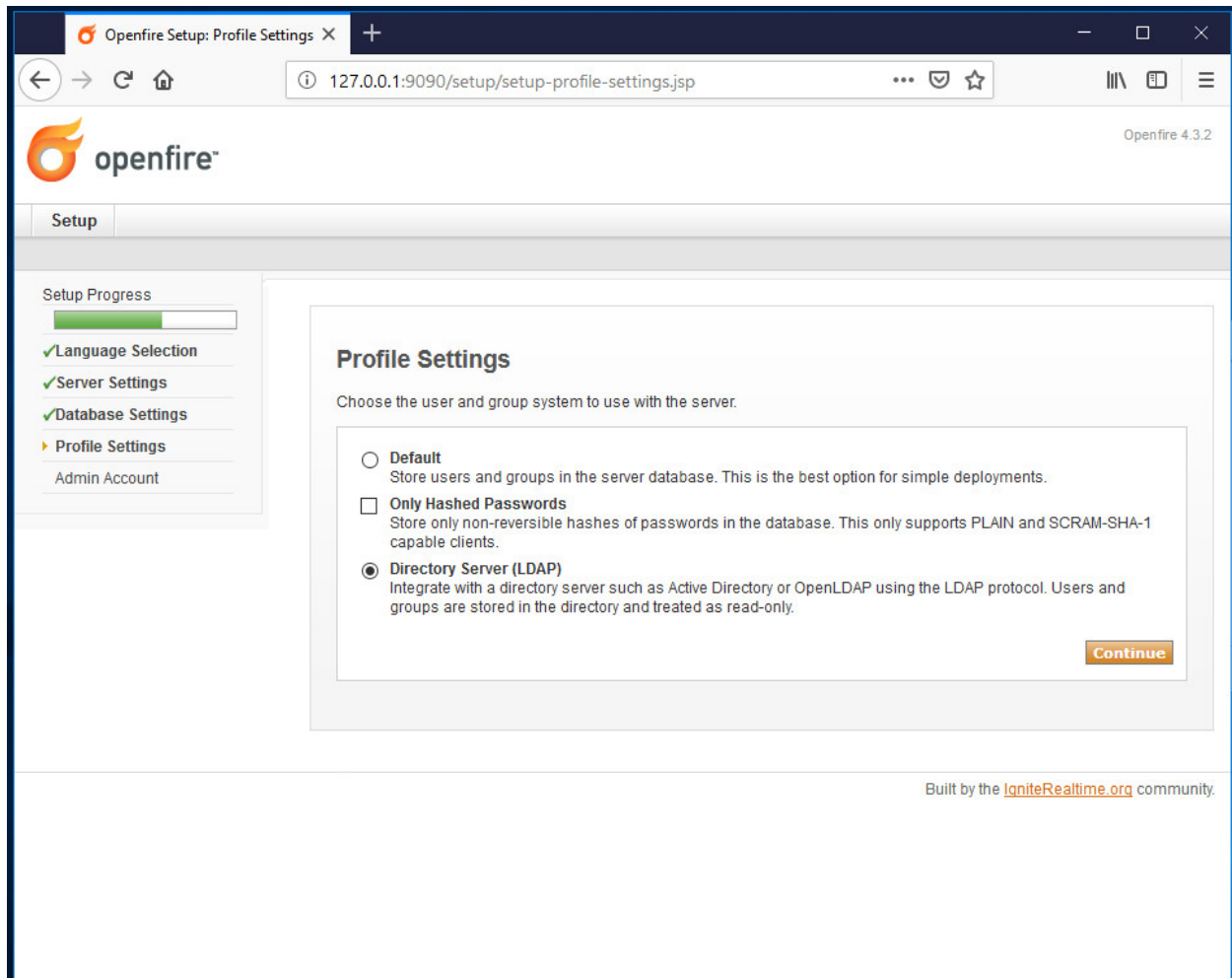
# (change requires restart)

# If external_pid_file is not explicitly set, no extra PID file is written.
#external_pid_file = ''
# write an extra PID file
# (change requires restart)

# -----
# CONNECTIONS AND AUTHENTICATION
# -----

# - Connection Settings -
listen_addresses = '*' # what IP address(es) to listen on;
# comma-separated list of addresses;
# defaults to 'localhost'; use '*' for all
# (change requires restart)
port = 5432 # (change requires restart)
max_connections = 100 # (change requires restart)
#superuser_reserved_connections = 3 # (change requires restart)
#unix_socket_directories = '' # comma-separated list of directories
# (change requires restart)
#unix_socket_group = '' # (change requires restart)
#unix_socket_permissions = 0777 # begin with 0 to use octal notation
# (change requires restart)
#bonjour = off # advertise server via Bonjour
# (change requires restart)
#bonjour_name = '' # defaults to the computer name
```

After I made those changes mentioned above, I restarted the openfiredb database server and the connection was successful. Below is the LDAP setup:



### Settings are as follows:

- Server Type: Active Directory (Openfire supports OpenLDAP as well)
- Hostname: ad01
- Port: 389 (LDAP protocol)
- Base Distinguished Name: CN=Users,DC=triplethreat,DC=local (where Openfire pulls group and user profile information, read only)
- Administrator Distinguished Name: CN=svc\_openfire,CN=User,DC=triplethreat,DC=local (svc\_openfire is a service account for Openfire and is a copy of Administrator)

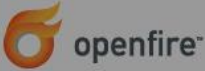
The screenshot shows the Openfire Setup: Profile Settings window. The browser address bar shows the URL `127.0.0.1:9090/setup/setup-ldap-server.jsp`. The Openfire logo and version (4.3.2) are visible in the top right. The Setup Progress bar on the left indicates the following steps: Language Selection (checked), Server Settings (checked), Database Settings (checked), Profile Settings (active), and Admin Account. The main content area is titled "Profile Settings: Connection Settings" and shows three tabs: 1. Connection Settings, 2. User Mapping, and 3. Group Mapping. The "Step 1 of 3: Connection Settings" section contains the following fields:

- LDAP Server:**
  - Server Type: Active Directory (dropdown menu)
  - Host: ad01
  - Port: 389
  - Base DN: CN=Users,DC=triplethreat,DC=local
- Authentication:**
  - Administrator DN: CN=svc\_openfire,CN=User,DC=triplethreat,DC=local
  - Password: (masked with dots)

At the bottom of the form, there are two buttons: "Test Settings" and "Save & Continue". A watermark for "Activate Windows" is visible in the bottom right corner.

Openfire Setup: Profile Settings

127.0.0.1:9090/setup/setup-ldap-server.jsp

Openfire 4.3.2

Setup

Setup Progress

✓Language Selection

✓Server Settings

✓Database Settings

▶Profile Settings

Admin Account

Profile Settings: Connection Settings

1. Connection Settings

2. User Mapping

3. Group Mapping

Step 1 of 3: Connection Settings

Configure connection settings for your LDAP directory below. All fields are required; if you need additional

Test: Connection Settings

Close

Status: Success!

A connection was successfully established to the LDAP server using the settings above. Close this test panel and continue to the next step.

Authentication:

Administrator DN: CN=svc\_openfire,CN=Users,DC=triplethreat,DC=local

Password:

Advanced Settings

Test Settings

Save & Continue

Activate Windows  
Go to Settings to activate Windows.

Openfire Setup: Profile Settings

127.0.0.1:9090/setup/setup-ldap-user.jsp?serverType=activedirect...

Openfire 4.3.2

Setup

Setup Progress

Language Selection

Server Settings

Database Settings

Profile Settings

Admin Account

Profile Settings: User Mapping

1. Connection Settings

2. User Mapping

3. Group Mapping

Step 2 of 3: User Mapping

Configure how the server finds and loads users from your LDAP directory. If you need additional information about a field, hover your mouse over the corresponding help icon.

User Mapping

Username Field: sAMAccountName

Advanced Settings

User Profiles (vCard)

Use the form below to specify the LDAP fields that match the profile fields. Fields that are left empty will not be mapped. Values enclosed in {} will be replaced with actual LDAP content.


Store avatar in database if not provided by LDAP

Profile Field	Value
Name	{cn}
Email	{mail}
Full Name	{displayName}
Nickname	
Birthday	



Openfire Setup: Administrator

127.0.0.1:9090/setup/setup-admin-settings.jsp

Openfire 4.3.2

Setup

Setup Progress

✓Language Selection

✓Server Settings

✓Database Settings

✓Profile Settings

Admin Account

Administrator Account

Choose one or more users from your LDAP directory to be administrators by entering their usernames.

Add Administrator:

Administrator	Test	Remove
bdreher		<input type="checkbox"/>
kkurkowski		<input type="checkbox"/>
meshiner		<input type="checkbox"/>


Built by the [igniteRealtime.org](https://ignite realtime.org) community.

Activate Windows

Go to Settings to activate Windows.

Openfire Setup: Administrator

127.0.0.1:9090/setup/setup-admin-settings.jsp

Openfire 4.3.2

Setup

Setup Progress

✓Language Selection

✓Server Settings

✓Database Settings

✓Profile Settings

Admin Account

Administrator Account

Choose one or more users from your LDAP directory to be administrators by entering their usernames.

Add Administrator:

Add

Administrator

Test

Remove

Remove

Continue

Test: Administrator Settings

Close

Status: Authentication Successful!

Specified username and password are valid. Close this test panel to continue.

Test: Administrator Settings

Close

Status: Authentication Successful!

Specified username and password are valid. Close this test panel to continue.


Built by the [igniteRealtime.org](https://ignite-realtime.org) community.

Activate Windows

Go to Settings to activate Windows.

Openfire Setup: Setup Complet

127.0.0.1:9090/setup/setup-finished.jsp

Openfire 4.3.2

Setup

Setup Progress

✓Language Selection

✓Server Settings

✓Database Settings

✓Profile Settings

✓Admin Account

Setup Complete!

This installation of Openfire is now complete. To continue:

Login to the admin console

Built by the [igniteRealtime.org](https://ignite realtime.org) community.

Activate Windows

Go to Settings to activate Windows.

## DNS SRV Record Error reported in the Openfire Admin Console:

### DNS SRV Record verification

 No DNS SRV records for this host are found.

To compose the information on this page, a DNS SRV query has been made, using the value of `triplethreat.local`, which is the XMPP domain name that is configured for Openfire. Any resulting records are inspected for a match against the value of `openfire.triplethreat.local`, which is the fully qualified domain name of the server that is running Openfire, as [configured here](#).

#### Current DNS Configuration Evaluation

There appear to be no DNS SRV records at all for this XMPP domain. With the current configuration of Openfire, it is recommended that DNS SRV records are created for this server.

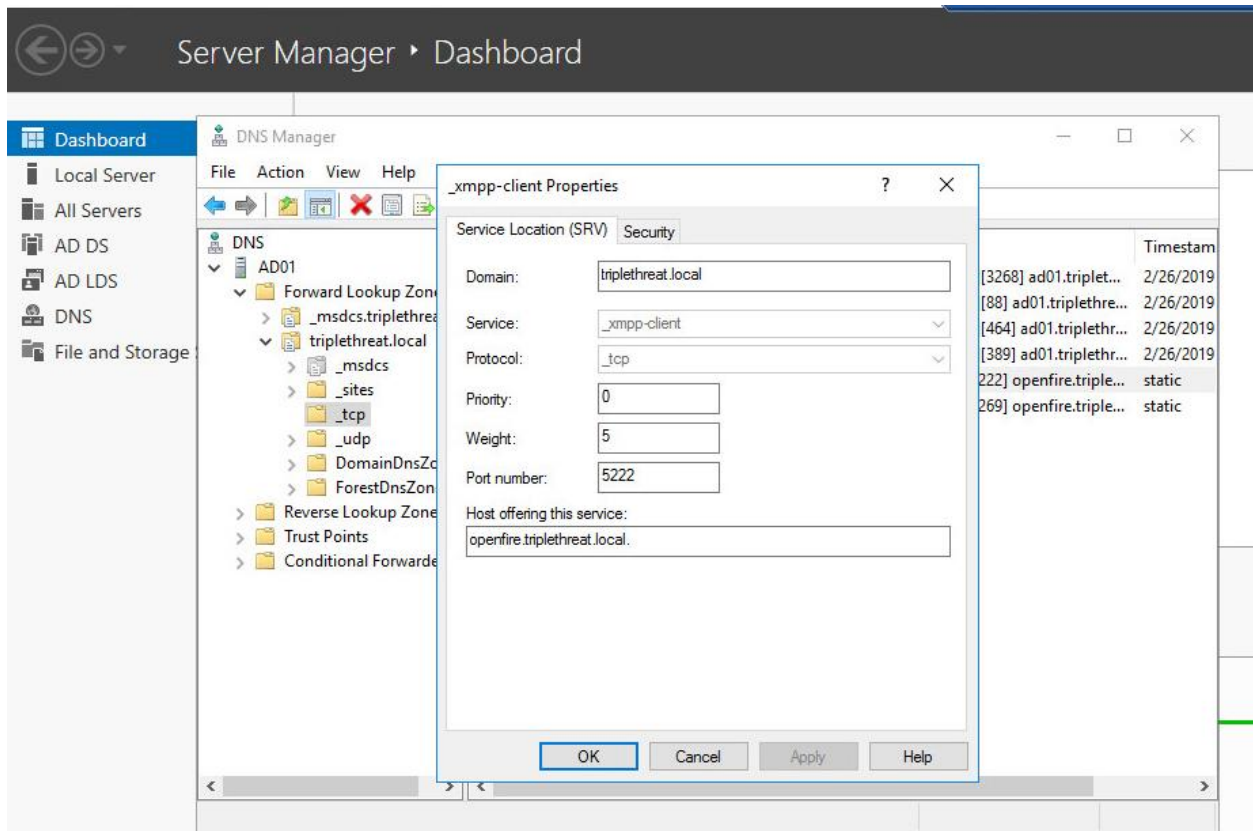
Without a valid DNS SRV record, clients are likely to have trouble connecting to your server. Even when clients provide a manual connect host, it is likely that they provide a different value than the fully qualified domain name that is configured for your server, which will cause problems with certain authentication mechanisms. It is recommended to have a DNS SRV record for this XMPP domain that matches the fully qualified domain name of the server on which you are running this instance of Openfire.

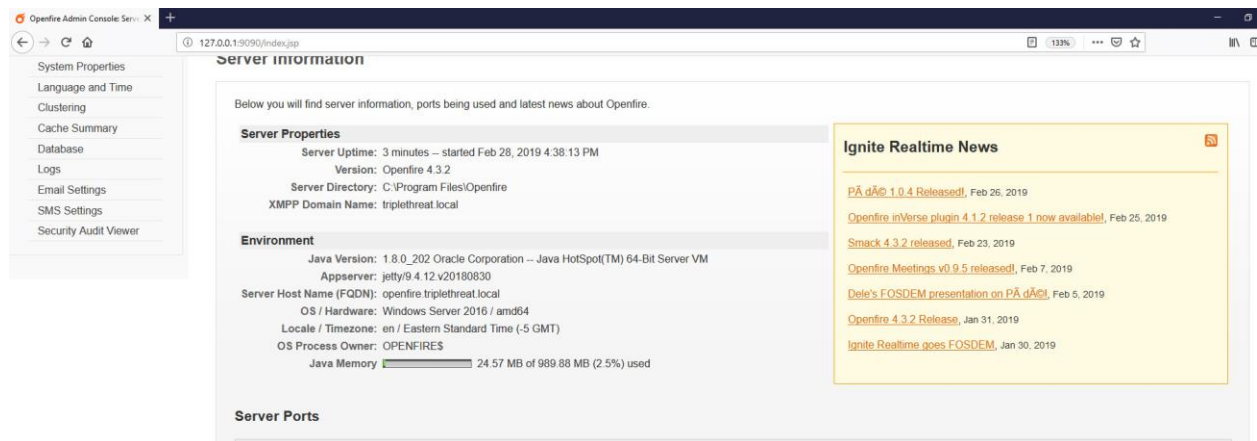
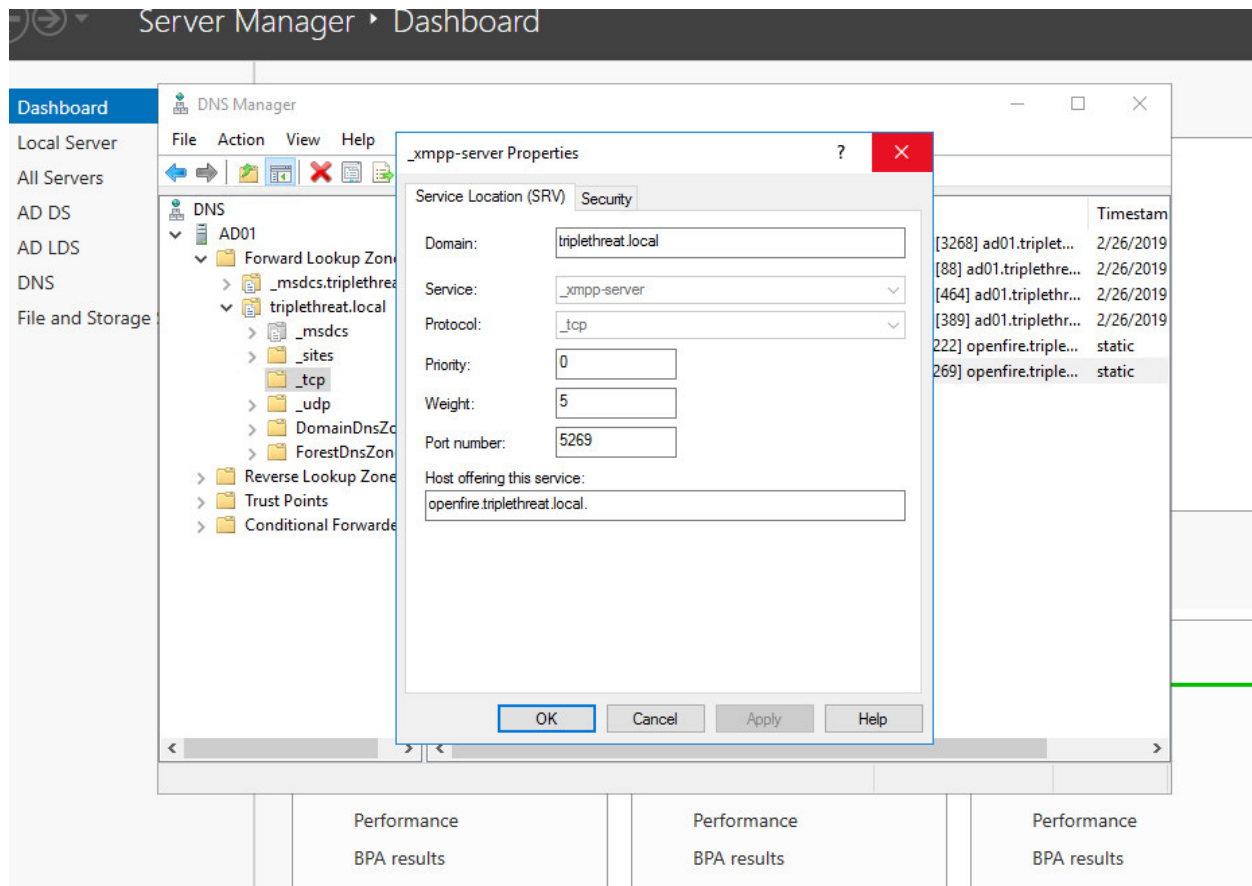
It is expected that your DNS configuration has at least two SRV records, which are similar to this (values like TTL, priority and weight are examples, and might be different in your configuration):

- `_xmpp-client._tcp.triplethreat.local. 86400 IN SRV 0 5 5222 openfire.triplethreat.local.`
- `_xmpp-server._tcp.triplethreat.local. 86400 IN SRV 0 5 5269 openfire.triplethreat.local.`

Note that changes that have been applied to DNS configuration might take a while to propagate. It might take some time for Openfire to be able to see the changes that were made to your DNS configuration.

Fixed the DNS SRV Record error issue by going into ad01, going into DNS manager, going under Forward Lookup Zones, right clicking the domain (triplethreat.local), and adding 'Other Record', in this case DNS SRV record for the Openfire application server. Please see record additions below.





Once I restarted both servers, I went into the Openfire Admin Console and there was no error notification. This SRV record notifies clients that the Openfire application in the triplethreat.local domain is located on openfire.triplethreat.local server and is servicing XMPP client requests on port 5222.

References:

- <http://download.igniterealtime.org/openfire/docs/latest/documentation/install-guide.html>
- [https://en.wikipedia.org/wiki/SRV\\_record](https://en.wikipedia.org/wiki/SRV_record)