NiFi Server Build Out With Active Directory Authentication

# Overview

In order to have multiple developers using the same NiFi server, we must allow multi-tenancy. There are several ways to do this, but in our environment, we’ll use Active Directory. The basic steps are:

1. Build Server

2. Install Pre-requisites

3. Download and Install NiFi software

4. Install TLS Toolkit Software and Create AD Service Account

5. Configure NiFi for TLS communication

6. Configure Initial Admin Account

7. Configure LDAP Authentication

8. Configure User Accounts

# Detailed Process

## 1. Build Server

The first step is to build a CentOS server. We are just using a standard CentOS 6.7 template in VMWare. Since all the NiFi configuration files and working directories are in /opt, it may be a good idea to mount /opt on a separate virtual disk.

### Operating System Configuration

#### SELinux

It’s easiest to put SELinux in permissive mode, but if enforcing is required, testing will have to be done.

vi /etc/sysconfig/selinux (command **getenforce** to verify changes)

#### Firewall

For the firewall, you need port 9443 and 8080 open for http and https. For testing purposes we turned the firewall off.

iptables -I INPUT 1 -i eth0 -p tcp --dport 8080 -j ACCEPT

iptables -I INPUT 1 -i eth0 -p tcp --dport 9443 -j ACCEPT

## 2. Install Prerequisites

You must first make sure that you have the latest Java installed. You can grab the latest from the Spacewalk server:

**wget** [**http://spacewalk.radon.mil/cobbler/repo\_mirror/oracle\_JDK/jdk-8u112-linux-x64.rpm**](http://spacewalk.radon.mil/cobbler/repo_mirror/oracle_JDK/jdk-8u112-linux-x64.rpm)

**rmp –ivh jdk-8u112-linux-x64.rpm**

## 3. Download and Install NiFi Bundle

Once the OS is stable and connectivity is verified, download the NiFI bundle, which includes the TLS Toolkit and preconfigured configuration files.

**cd /opt**

**wget** [**http://spacewalk.radon.mil/cobbler/repo\_mirror/nifi/nifi\_full\_setup.tar.gz**](http://spacewalk.radon.mil/cobbler/repo_mirror/nifi/nifi_full_setup.tar.gz)

**tar –xzvf nifi\_full\_setup.tar.gz**

At this point you should have two new directories under /opt **(nifi-1.3.0** and **nifi-toolkit-1.3**). You can now start NiFi and verify you have proper web functionality.

**/opt/nifi-1.3.0/bin/nifi.sh start** (you can do a **status** to ensure its running)

## 4. Install the TLS Toolkit and Create AD Service Account

In order for the NiFi server to ask for authentication you must first have TLS communication enabled (https). To do this you must installed the TLS toolkit.

If you used the NiFi bundle in step 3, then you have the *already extracted* TLS toolkit under **/opt/nifi-toolkit-1.3.0**

Once the toolkit is installed you need to create an Active Directory service account that has access to query AD (or use one that is already in place)

Once you have that account created, you need to pull the exact DN from AD for configuration. The best way to do this is to open Active Directory Users and Computers and select View 🡪 Advanced Features as shown below

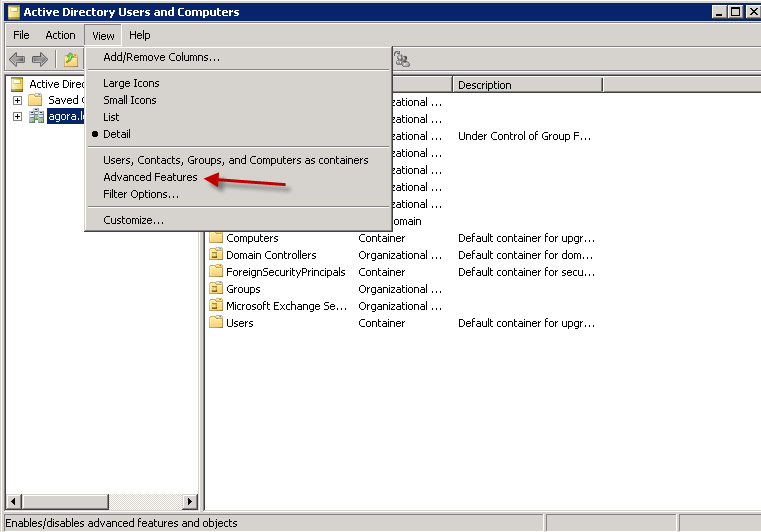


Figure - AD View Advanced Features

Then navigate the directory tree to the new service account you created (you **can’t** use **find** for this) and **right click** and view **properties,** then select **attribute editor**, then scroll down to DN, then highlight and click **View**. You can then copy this into the buffer.

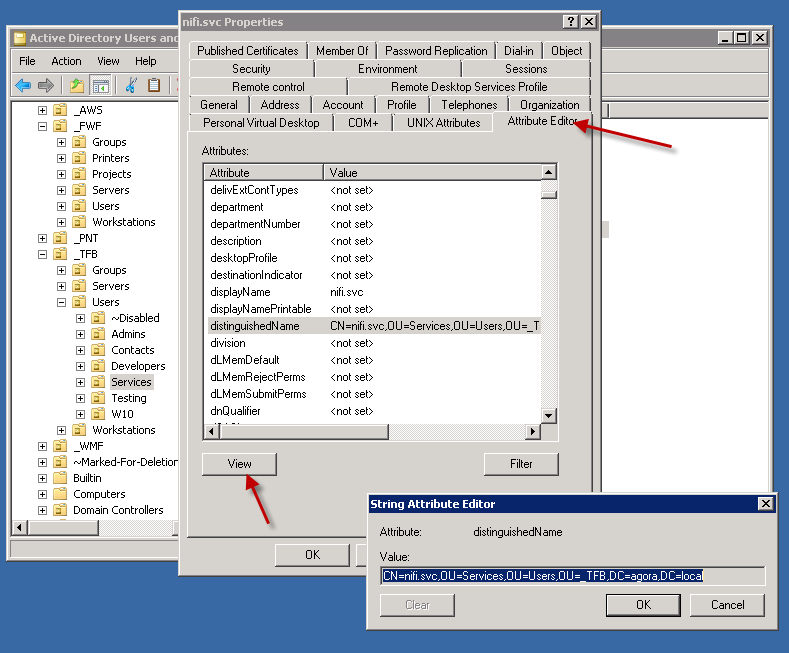


Figure - Attribute Editor for DN Name

## 5. Configure NiFi for TLS Communications

Once you have the TLS Toolkit installed do the following:

**cd /opt/nifi-toolkit-1.3.0**

**./bin/tls-toolkit.sh standalone -n 'fwf-rd-pd-nifi-01' -C 'CN=nifi.svc,OU=Services,OU=Users,OU=\_TFB,DC=agora,DC=local' -O -o ./certs**

***NOTE: In the above command you need to replace the hostname and DN with your new information.***

At this point, you will have a cert directory under your /opt/nifi-toolkit-1.3.0 directory. You now need to move the contents of this directory to your conf directory. You must first remove any files currently in the conf directory

**cd /opt/nifi-1.3.0/conf/certs**

**rm –rf \***

**cd /opt/nifi-toolkit-1.3.0/certs**

**cp –r \* /opt/nifi-1.3.0/conf/certs/**

Now, you have the newly generated certs in the proper directory. You need to save the original nifi.properties file and replace with the new one generated by the TLS toolkit.

**cd /opt/nifi-1.3.0/conf**

**mv nifi.properties nifi.properties.orig**

**cp /opt/nifi-toolkit-1.3.0/conf/certs/fwf-rd-pd-nifi-01/nifi.properties /opt/nifi-1.3.0/conf/**

The next step is to edit the nifi.properties file to point to the correct cert locations as shown below

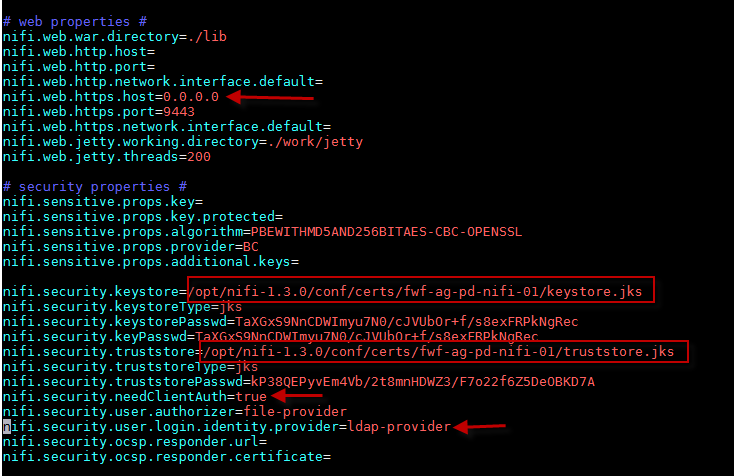


Figure - nifi.properties file changes

You will also see that we added options to the **nifi.security.needClientAuth** and **nifi.security.user.login.identity.provider**. These are for the LDAP configuration below. Also, you should change the **nifi.web.https.host** option to 0.0.0.0 to accept connections from all subnets.

At this point you should only be able to access the nifi page via https. The URL should be something like <https://fwf-rd-pd-nifi-01.radon.mil:9443/nifi>. You should see a page that says unknown user or something. This is normal because you haven’t set up your admin account yet. That is the next step.

## 6. Configure Initial Admin Account

The way NiFi handles the administrative user is to validate via a browser cert that is validated against an authorizers.xml config file. You don’t create an admin user, you add the user DN that was configured with your cert to the /opt/nifi-1.3.0/conf/authorizers.xml file. You then import that cert into your browser. When you connect to the TLS version of the NiFi server it will log you in with admin rights.

In section 5, above, we created the certs using the service account **nifi.svc** with a DN of **CN=nifi.svc,OU=Services,OU=Users,OU=\_TFB,DC=agora,DC=local**

We need to add this user to the **/opt/nifi-1.3.0/conf/authorizers.xml** file as shown below

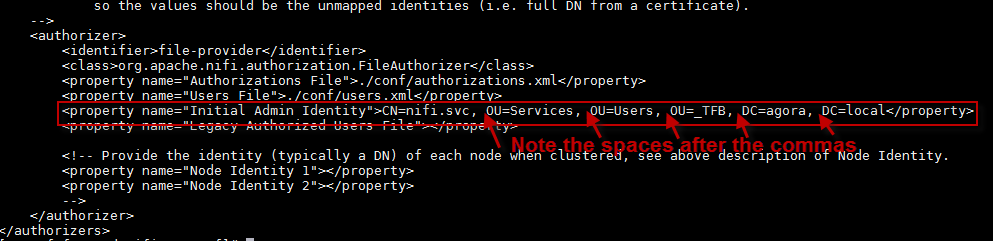


Figure - Authorizers.xml File

No**te that even though we don’t have spaces in the true DN name pulled from Active Directory, we DO need to insert them in this file. (I’m not sure why that is).**

### Import Cert in Browser for Admin Access

The next step is to import the certificate that was created in Step 5 into your browser. You need to download the p12 certificate from **/opt/nifi-1.3.0/conf/certs/**. In Firefox, you go **to Settings 🡪 Advanced 🡪 Certificates 🡪 View Certificates 🡪 Import** then find the .p12 file you grabbed from the server.

When prompted for the password, you must use the password provided by the TLS toolkit under **/opt/nifi1.3.0/conf/certs** as shown below. (Just do a **more** or **cat** this file)

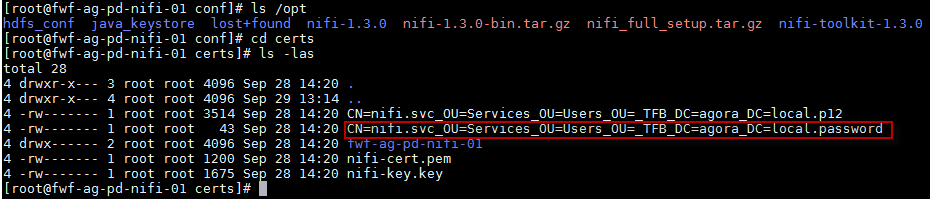


Figure - pk12 Cert Password for Browser

You need to restart the nifi server to force the changes to take effect.

**/opt/nifi-1.3.0/bin/nifi.sh restart**

After this, you should be able to log into the URL and see the main screen as shown below

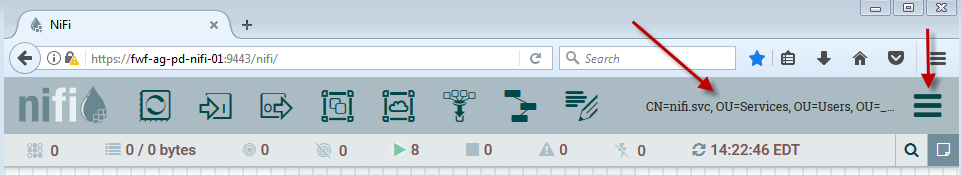


Figure - Admin Login Screen

You should see the CN displayed and the “hamburger menu” should be displayed to the right of it. If you can see this, TLS is configured and you have Admin access.

## 7. Configure Active Directory (LDAP) Authentication

The next step in the process is to configure multi-tenancy login via Active Directory. To do this, you need to tell the nifi server to use LDAP, then configure the LDAP section in the conf directory.

The two files you will modify are **nifi.properties** and **login –identity-providers.xml**

First, in the **nifi.properties** file, add the words **ldap-provider** and **true** as shown below.

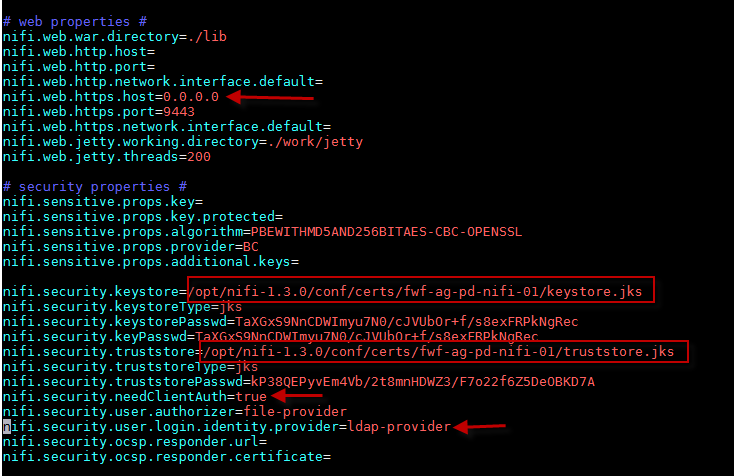


Figure - LDAP Provider

Next, you need to configure the ldap-provider section by editing the **login-identity-providers.xml** file with your AD connection information. An example is shown below.

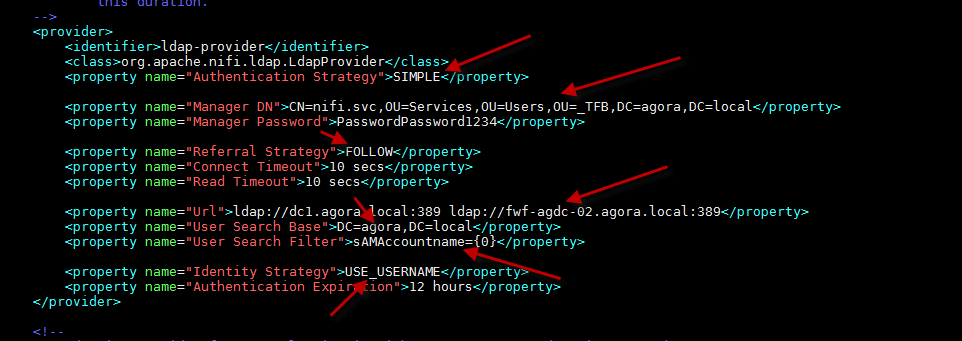


Figure - LDAP Provider Configuration

**NOTE: If you did not use the bundle but set this up from scratch, you will have to uncomment the line above and below this section.**

You will need to restart the nifi server again for these changes to take effect.

**/opt/nifi-1.3.0/bin/nifi.sh restart**

## 8. Configure User Accounts

Even though you are now using AD to authenticate, you still need to authorize the specific accounts for whatever role you want. This is done through the NiFi GUI.

First add the user accounts and make sure they match their AD name as shown below.

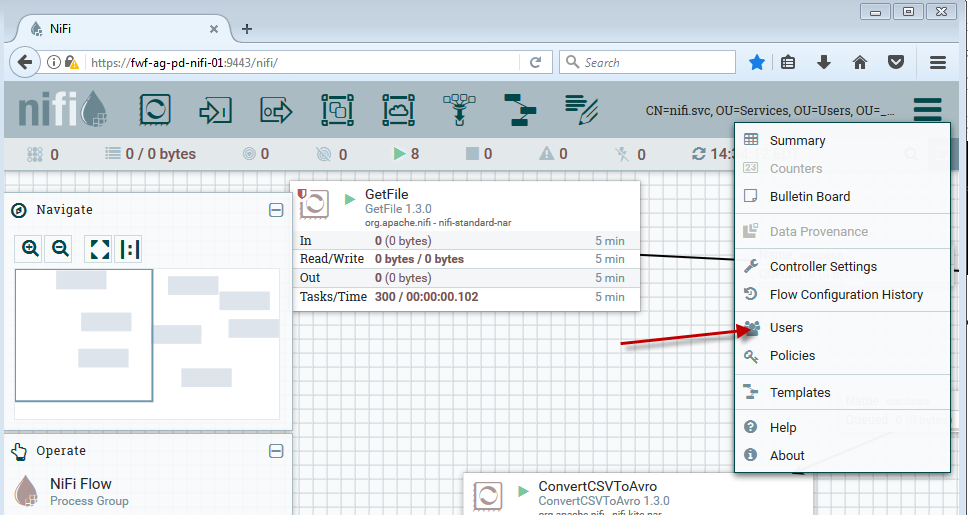


Figure - Add Users

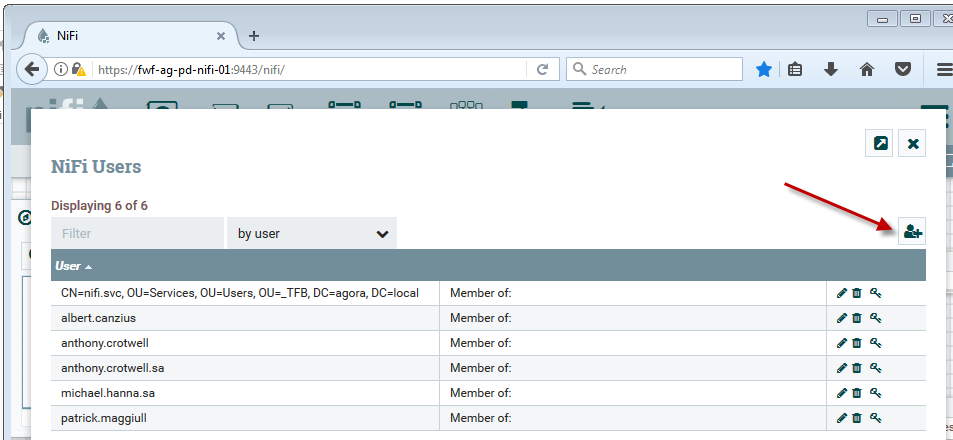


Figure - Add Users Cont...

Once you have your users added, you need to assign roles to them and the the first thing is to allow flow create for your users. To do this click on the “key” symbol on the left **Operate pane** as shown below.

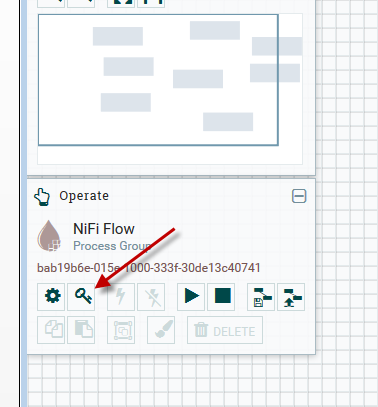


Figure - Assign Privileges for Workflow

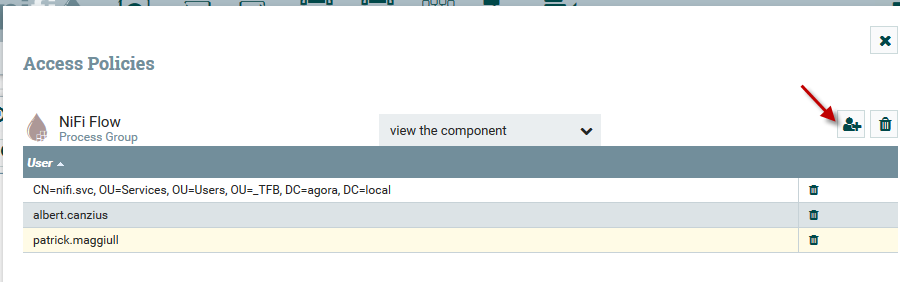


Figure - Flow Control Users Cont....

Lastly, you need to assign roles to your users for other functionality by using the “Hamburger Menu” on the far right as shown below.

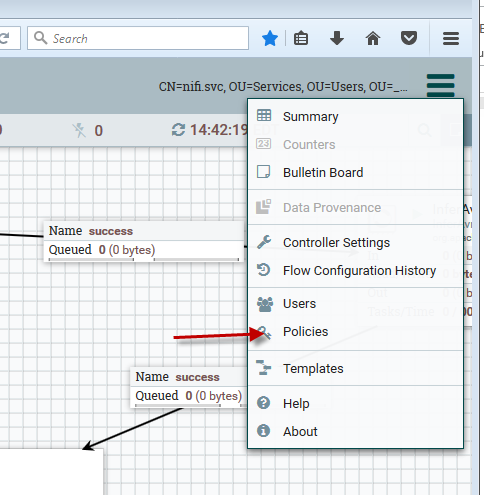


Figure - Assign Policies

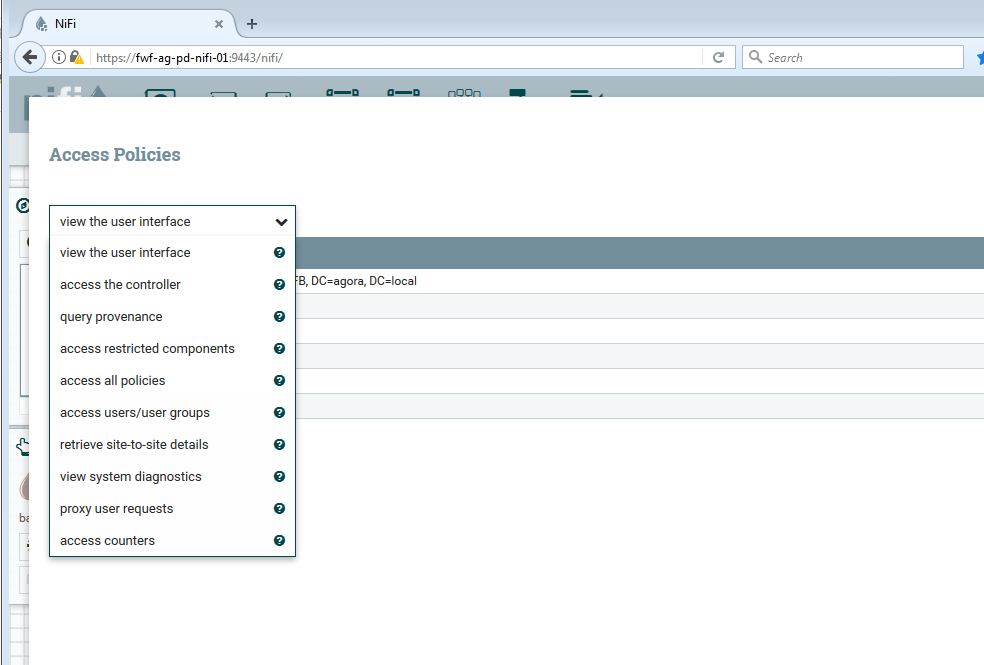


Figure - Assign Policies Cont....

# Misc Notes

If you use the CentOS template, you will need to modify a few files.

## SSH

vi the /etc/ssh/sshd\_config and change MaxrAuthTries to 10 instead of 1

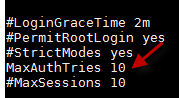


Figure - SSH Config Change

## SUDO

You will need to add admin users to the sudoers file /etc/sudoers then vi /etc/nsswitch.conf and add the word files on the sudo line.

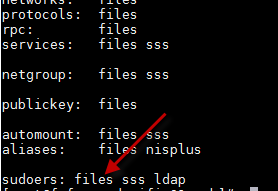


Figure - NSSwitch.conf SUDOERS Change