# SNTT : Using Active Directory To Authenticate Web Users

**Sean Cull 10 March 2011 21:24:59**

## Introduction

This article describes how you can use Active Directory via LDAP and Directory Assistance to authenticate your web users. This is particularly useful in our case where we have an XPages based application running in on a black boxed appliance in a MS shop.
The example uses a Windows Server 2008 R2 for AD and Domino 8.5.2 running on Linux. The scheme is simple enough but I struggled to piece the bits together so I thought a write up would be useful.

## Useful tools

I found that the Apache Directory Studio was really useful. This allows you to explore the Active Directory LDAP feed and get a feel for its structure.

## Useful debugging parameters

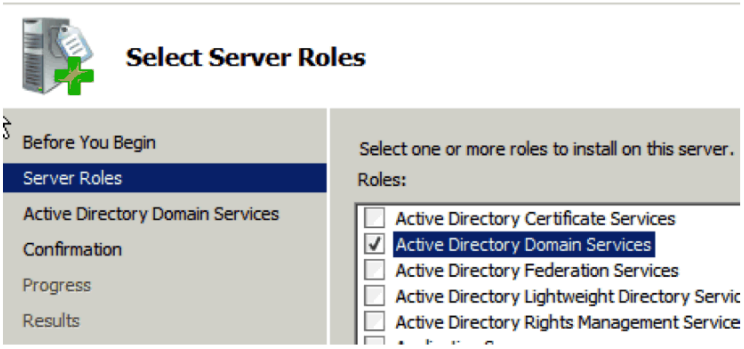
I found the following two parameters very useful because you can see the structures of the names and groups in AD as they are queried by Domino - these settings are for temporary use only as they create overhead and also show users passwords on the console in plain text ( somewhat disconcerting )

Webauth_verbose_trace=1
LDAPDEBUG=1

## Setting up an AD test environment

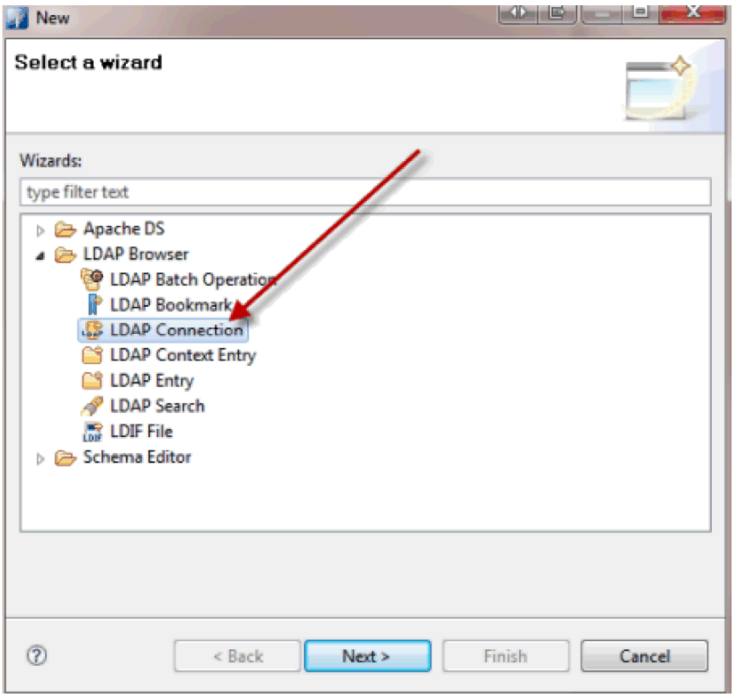
This was very straight froward. I installed a 2008 R2 server as a VM and used the Server

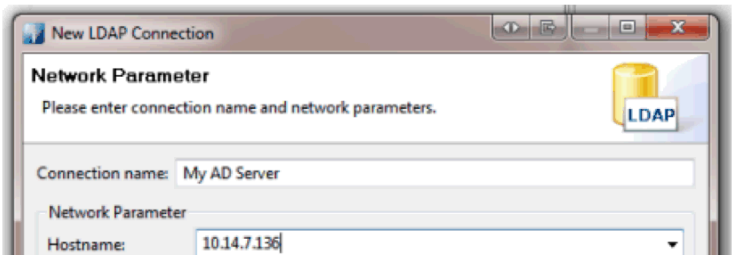
Roles Manager wizard to install Active Directory accepting the defaults and dependencies. I then created a new user ( joe bloggs ) and used that account to authenticate the LDAP feed.

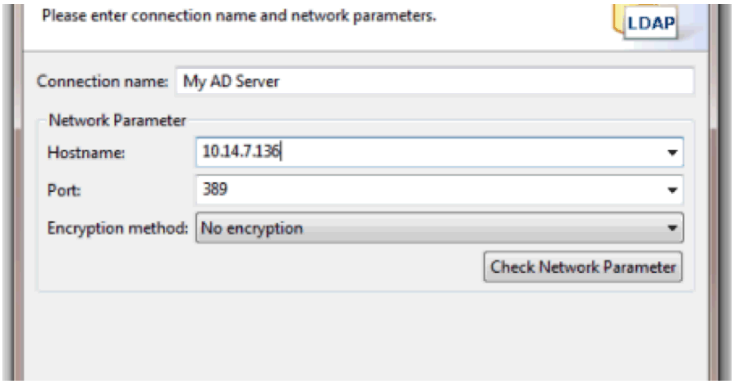


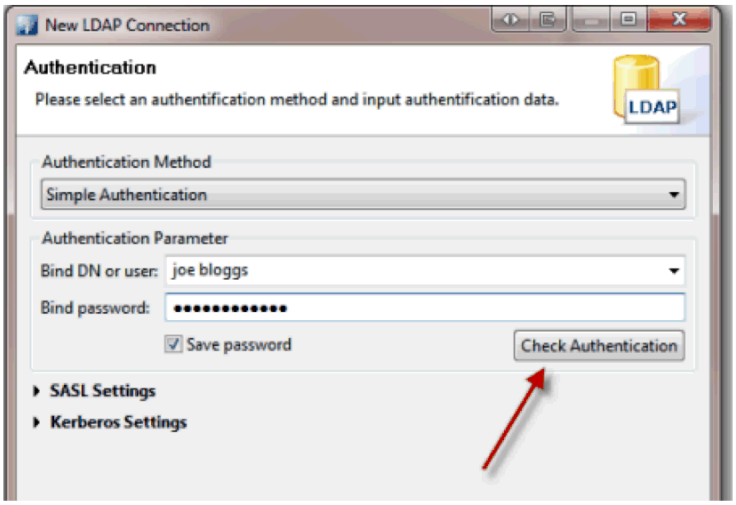

## Exploring the LDAP Feed with Apache Directory Studio

Use File New and then choose LDAP Connection



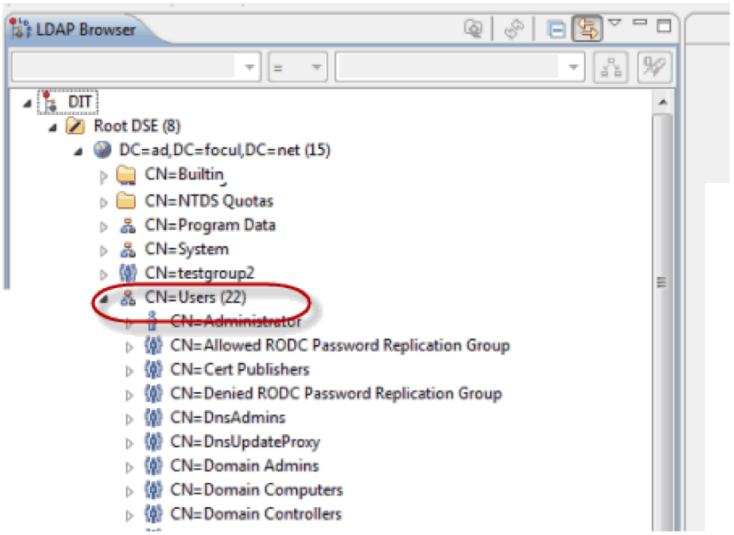





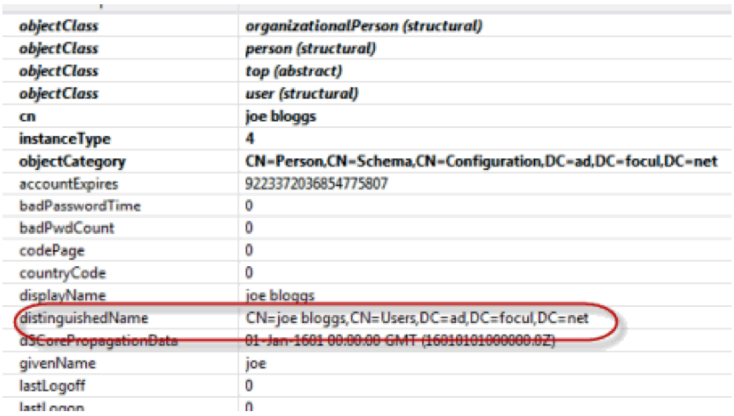

Press the check Authentication button and all should be well

Next you can browse the LDAP tree and see information on the users and groups



The equivalent "Notes name" as used in an ACL would be

CN=joe bloggs/CN=Users/DC=ad/DC=focul/DC=net

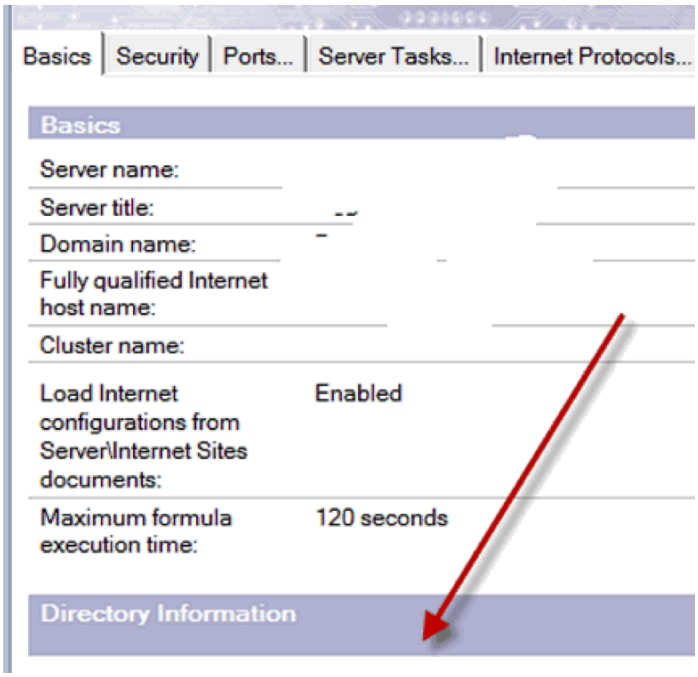


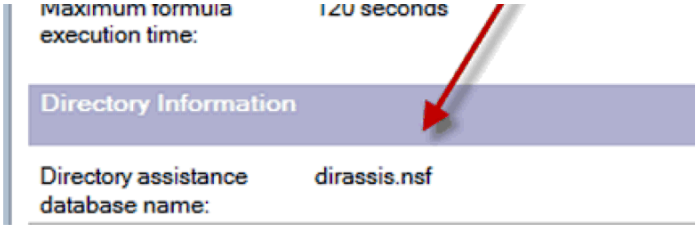
| | |
|---|---|
| ***objectClass*** | ***organizationalPerson (structural)*** |
| ***objectClass*** | ***person (structural)*** |
| ***objectClass*** | ***top (abstract)*** |
| ***objectClass*** | ***user (structural)*** |
| **cn** | **joe bloggs** |
| **instanceType** | **4** |
| **objectCategory** | **CN=Person,CN=Schema,CN=Configuration,DC=ad,DC=focul,DC=net** |
| accountExpires | 9223372036854775807 |
| badPasswordTime | 0 |
| badPwdCount | 0 |
| codePage | 0 |
| countryCode | 0 |
| displayName | joe bloggs |
| distinguishedName | CN=joe bloggs,CN=Users,DC=ad,DC=focul,DC=net |
| dSCorePropagationData | 01-Jan-1601 00:00:00 GMT (16010101000000.0Z) |
| givenName | joe |
| lastLogoff | 0 |
| lastLogon | 0 |

## Configuring Domino to use the Active Directory LDAP

You need to create a Directory Assistance Database and then list this in the server record
The directory assistance template is an advanced template called called Directory Assistance ( da.ntf )

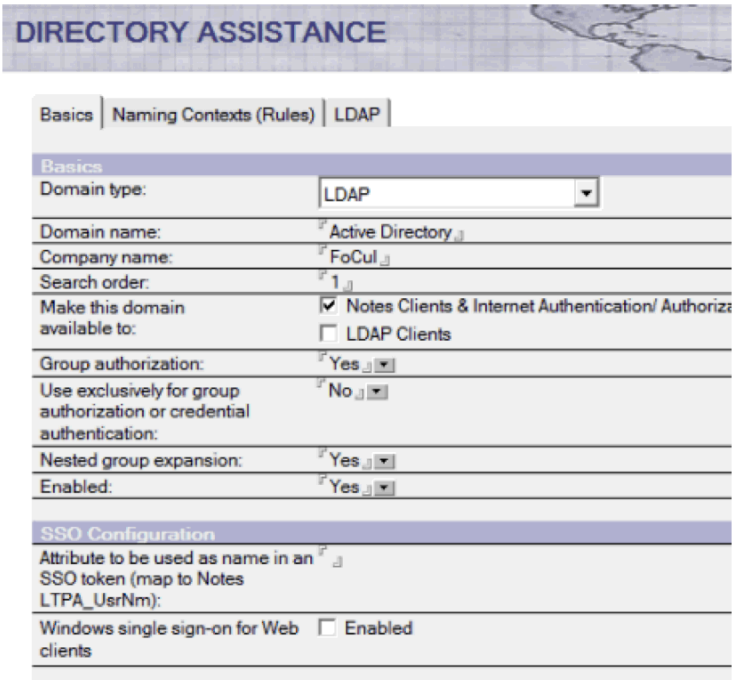
The server document entry looks like this

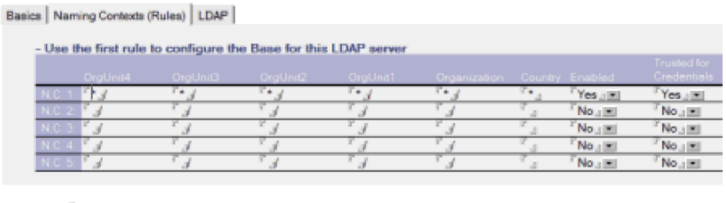





In the Directory Assistance Database create a record as follows.

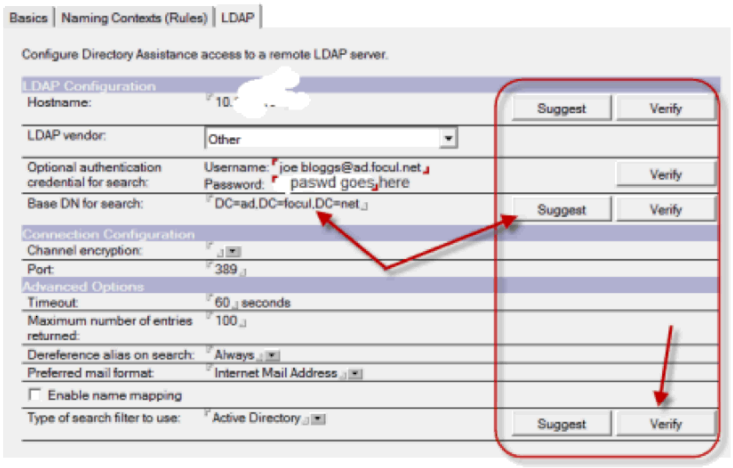
**Note that Gabriella Davis and Marie Scott on page 20 of their very useful presentation One DirectoryTo Rule Them All, Yes suggests encrypting the LDAP configuration document - not sure how to do that just yet.**




Note that the suggest and verify buttons are very useful, particularly for the Base DN for

search




## Testing Authentication

Start with the most basic example you can.
With a test database set anaonymous access to No Access and Default Access to reader or higher.

Open the URL and attempt to login - in my case as Joe Bloggs. In the console you will see something similar to this :

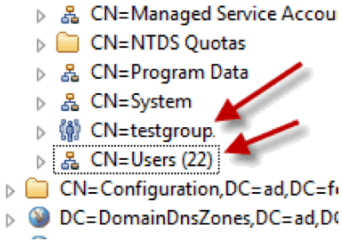
```
35,90 [26083:00005-2808085392] <LDAP GW> Searching LDAP host='[10.14.7.136]:389' with name='joe bloggs@
35,90 [26083:00005-2808085392] <LDAP GW>   Attr: FullName
35,90 [26083:00005-2808085392] <LDAP GW>   Attr: userPassword  (mapped from Item=HTTPPassword)
35,90 [26083:00005-2808085392] <LDAP GW>   Attr: MailServer

  |... deleted fro brevity

35,91 [26083:00005-2808085392] <LDAP GW>   Attr: AltFullNameLanguage
35,91 [26083:00005-2808085392] <LDAP GW>   Attr: CN
35,91 [26083:00005-2808085392] <LDAP GW>   Base: DC=ad,DC=focul,DC=net
35,91 [26083:00005-2808085392] <LDAP GW>   Scope: 2
35,91 [26083:00005-2808085392] <LDAP GW>   Filter: (|(cn=joe bloggs)(|(&(sn=joe)(givenname=bloggs))(&(s
35,91 [26083:00005-2808085392] <LDAP GW>   Timeout: 60 secs
35,91 [26083:00005-2808085392] <LDAP GW> SEARCH returned '1' match(es).
35,91 [26083:00005-2808085392] <LDAP GW> ldap_search returned matched DN='CN=joe bloggs/CN=Users/DC=ad/
```

Your authentication is working.

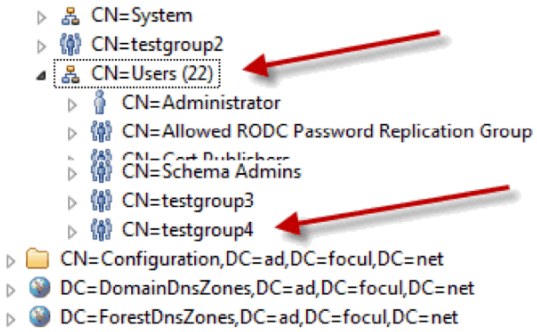
You can now test it with a specific name. You can see the shape of the name from the console output

The AD name CN=joe bloggs,CN=Users,DC=ad,DC=focul,DC=net gets mapped to CN=joe bloggs/CN=Users/DC=ad/DC=focul/DC=net for use in the ACL
Groups also work but note that if you put a group into the AD as a peer of "Users" the group

name construct includes "Builtin" as in CN=testgroup/CN=Builtin/DC=ad/DC=focul/DC=net so it is better to put the groups within the users branch.




In our case the group name is CN=testgroup4/CN=Users/DC=ad/DC=focul/DC=net




## Further Integration

This OpenNTF Active directory name picker project and search by Rishi Sahi looks really interesting. He also has some good blog articles on LDAP integration

## Other useful presentations

As mentioned above I found Gabriella Davis and Marie Scott's presentation very useful - One DirectoryTo Rule Them All, Yes

I also attended Warren Elsmore's Directory Integration session at ILUG which was very useful. You can download all of the ILUG slides here => http://www.ilug2010.org/ilug/ilug2010.nsf.

## A mild rant

In pulling this material together I have come to the conclusion that it is a real shame that IBM has not published the slide decks from lotussphere 2011.

It would make it a lot easier for developers to make the IBM products more popular if IBM as **an organisation** was a good citizen of the community in that respect.

I have huge admiration for many individuals within IBM that do their best despite IBM in this regard. I also think it is unfair to expect the community to contribute to the IBM Wikis when they are sitting on hundreds of excellent presentations by the world experts in this area - experts who gave up thousands of hours to prepare those slide decks.

Its hardly what I would describe as a good example of a Social Business.

Admin Tips Appliance Dev Tips Show-n-Tell Thursday Active Directory LDAP Lotus

Please leave a comment