The Iam Lotus User Group

One Directory To Rule Them All, Yes!

Gabriella Davis ▪ Turtle Partnership
Marie Scott ▪ Virginia Commonwealth University

Agenda

- Two Directories, One Name
- Directories, Types and Choices
- Domino as LDAP
- Secondary Directories
- Security Implications
- Setting Up
- Adding Automation with TDI
- Our One Directory

Two Directories, One Name

- Directory “nice to haves”
  - Looking up the mail address of a user from an external system
  - Authenticating users from other external systems
- Most advanced Lotus Software products now require you to use an LDAP directory as a single point of reference

- What are we trying to achieve today
  - Single login
  - Single password
  - Possible removal of HTTP password
  - Single point of Administration

Directories, Types and Choices

- Let's back up a bit and talk about "Directories"
  - We have a lot of choice in choosing what to use and how to use it
  - Understanding those options helps us decide when to store vs lookup info
- Domino's Proprietary Directory Format
- LDAP as a 'Standard'
  - Schemas vs Design
  - Attributes vs Fields
- LDAP Servers
  - Active Directory
  - Novell eDirectory
  - Tivoli Directory
  - Sun One

Domino as LDAP

- **Domino can act as an LDAP itself**
  - It can make itself available to any LDAP client
  - It can allow LDAP clients to search its directory (names.nsf)
  - You can select which additional directories outside of names.nsf are available to LDAP clients
- **LDAP Task on the Domino server**
  - Handles enquiries from LDAP clients
  - Translates between Domino format and LDAP when serving up requests
  - Honors server and db (names.nsf) security
  - Is limited by settings in the global configuration document
    - More on this in a bit!

Can I Do Without A Domino Directory Entirely?

- **No**

  but we can definitely cut down what user information is held in there

- **You'll always need**
  - **Server and configuration documents that tell Domino how to behave**
  - **At least one administration account that can access Domino if all else fails**

- **You could - and we often do - have no other person documents in the names.nsf**

Why would I have additional Domino Directories?

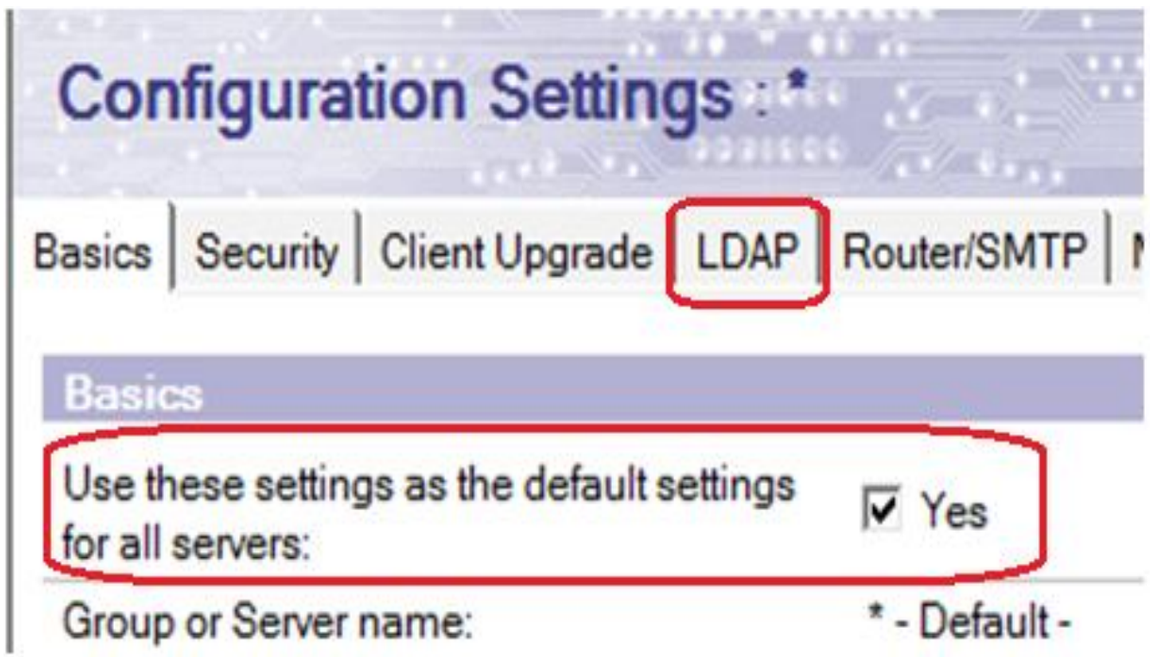
- **Customer / Supplier email addresses**
  - You want all your users to be able to email your customers or suppliers from their mail clients.
- **Shared address books**
  - You want users to store contact information in a shared address book on the server so it can be seen by others. You control rights to see specific contacts via reader fields
- **Web Application authentication**
  - You have a public website where you want people to register themselves for access

Why would I use additional LDAP directories?

- Authenticating people to your environment who are only registered in external (non Domino) directories
- Sending mail to people registered in external directories
  - Notes is an LDAP client, this means it can query LDAP directories
  - For example, there are public LDAP directories that are set up by default in your client
  - You can search any directory that has made itself available to an LDAP Client
- Retrieving information that is held externally for your users from other systems
- LDAP Directory information isn't imported into Domino format - it's always accessed live off the LDAP servers
  - This is important as it affects security, server and user performance.
    - More about this in a bit!

Configuring Domino as a LDAP Server

- **Configuring Domino as an LDAP Server**
  - You don't need to do this for our single login task here
    - but your environment may require a combination of things we're showing you today
  - Start Task by adding LDAP to server notes.ini or "Load LDAP"
  - Create a global configuration document
    - That's a configuration document that's set to "All Servers"



Using Domino as an LDAP Server

LDAP Attribute Types:	Domino Fields:
AltFullName	AltFullName
altServer	altServer
attributeTypes	attributeTypes
authorityRevocationList	authorityRevocationList
c	OfficeCountry
certificateRevocationList	certificateRevocationList
cn	cn

Allow LDAP users write access:	(•) Yes ( ) No
Timeout:	0 seconds
Maximum number of entries returned:	0
Minimum characters for wildcard search:	1
Allow Alternate Language Information processing:	( ) Yes (•) No
Rules to follow when this directory is the primary directory, and there are multiple matches on the distinguished name being compared/modified:	( ) Don't modify any (•) Modify first match ( ) Modify all matches
Automatically Full Text Index Domino Directory?	(•) Yes ( ) No
Enforce schema?	(•) Yes ( ) No
DN Required on Bind?	( ) Yes (•) No
Encode results in UTF8 for LDAPv2 clients?	(•) Yes ( ) No
Maximum number of referrals:	1
Activity Logging truncation size:	4096
Allow dereferencing of aliases on search requests?	( ) Yes (•) No

Reviewing the Domino Schema

- **When you enable LDAP on your Admin server it will create the first instance of schema.nsf**
  - **If you don't have a working schema.nsf that is accessible from your LDAP server, the LDAP task can't run**
  - **You should not need to open it but it's a very good reference for seeing how Domino maps attributes and fields**

LDAP OID	LDAP Name	LDAP Aliases	Notes Name
LDAP AttributeTypes			
0.9.2342.19200300.100.1.1	uid	userid	ShortName
0.9.2342.19200300.100.1.10	manager		manager
0.9.2342.19200300.100.1.11	documentIdentifier		documentIdentifier
0.9.2342.19200300.100.1.12	documentTitle		documentTitle
0.9.2342.19200300.100.1.13	documentVersion		documentVersion
0.9.2342.19200300.100.1.14	documentAuthor		documentAuthor
0.9.2342.19200300.100.1.15	documentLocation		documentLocation
0.9.2342.19200300.100.1.2	textEncodedOrAddress		textEncodedOrAddress
0.9.2342.19200300.100.1.20	homePhone	homeTelephoneNumber	PhoneNumber
0.9.2342.19200300.100.1.21	secretary		Assistant
0.9.2342.19200300.100.1.22	otherMailbox		otherMailbox
0.9.2342.19200300.100.1.23	lastModifiedTime		lastModifiedTime
0.9.2342.19200300.100.1.24	lastModifiedBy		lastModifiedBy
0.9.2342.19200300.100.1.25	dc	domainComponent	dc
0.9.2342.19200300.100.1.26	dnsRecord		dnsRecord
0.9.2342.19200300.100.1.3	mail	rfc822Mailbox	InternetAddress

How to set up Secondary Directories

- Create a Directory Assistance database based upon the template da.ntf (Directory Assistance)
- Set up a Directory Assistance document for any directories you want this server to use
- In Domino Administrator choose “Set Directory Assistance Information” whilst having the server document selected
  - Complete the name of the database created in the first step

How Directories Behave

- All directories enabled in Directory Assistance for mail routing will appear as other directory choices when addressing mail
  - And type ahead will search each of those directories as well as local and server based names.nsf
- All directories enabled for searching by LDAP clients will be searched by the LDAP task during queries
- All directories trusted for credentials will be authenticated and trusted equally to users in names.nsf
- Directory Assistance doesn't run as a separate server task
  - It will reload settings automatically on 8.5x Domino versions

Directory Options and Settings

- Domino Type - Notes (Domino db) / LDAP (remote server)
- Domain Name can be any unique name
- Search Order
- Make Domain Available to Notes and / or LDAP clients
- Use for authentication only
  - Make sure you select “Yes” on the 2nd tab, trusted for credentials
- Use for mail routing only
- Add details of directory location
  - Database link for Notes directories
  - Server and filename for Notes directories
  - Settings for LDAP directories

Server Performance

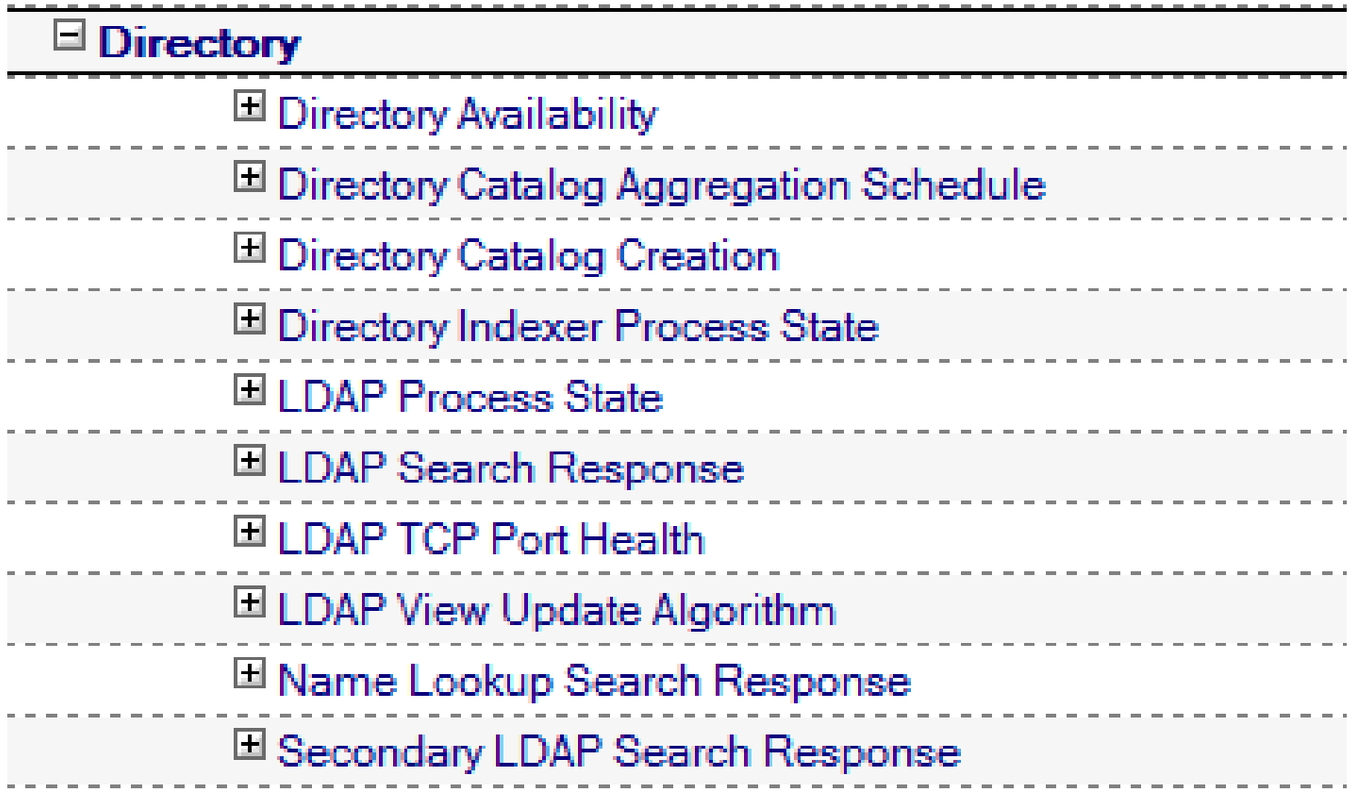
- Domino prioritises indexing and maintenance of the directories highly in terms of allocating resources
- Directory information is cached for performance
- Performing a lookup or doing type-ahead utilises all server based directories
  - The server you use for lookup is set in your location document in Notes. The directories it uses are defined in its Directory Assistance document
- When authenticating, all directories are used to validate a login
- Poor directory performance (type ahead, sending mail, web login) will be noted by your users as “Notes being slow”

Things to watch out for

- Sh XDir shows a list of configured directories and where they are
  - If you pasted in a Domino db link and then replicated the directory, the link could be pointing to a database on a different server
  - If you configured LDAP then the DNS resolution for that FQHN from the server itself is critical
- Ensure your indexer task isn't constantly overloaded
  - Domino spawns a specific thread
- If we're making a secondary directory critical to our infrastructure then we need to monitor it
  - LDAP directories tend to be outside our control

DDM Probes

- **Use Directory DDM probes to monitor performance and response times**
  - **These are critical to your environment and to your user's perception**
  - **Found in events4.nsf. All you have to do is enable what you need**



Additional Troubleshooting Tools

- **Use the following Notes.ini parms to assist with LDAP or authentication troubleshooting:**
  - **Webauth_verbose_trace=1 (shows web authentication responses)**
  - **LDAPDebug (if you're using Domino LDAP)**
    - **1 = Show Query Information**
      2 = Show Result Information
      3 = 1 & 2
      4 = Authentification Information
      5 = 1 & 4
      6 = 2 & 4
      7 = All of the above
      8 = Even more verbose information (no details known)
      9 - 15 = Summaries of the above

Security Implications

- What happens to Domino when I set up a secondary directory for authentication
  - Unique names
  - Common passwords (Sametime users)
  - Other tasks - SMTP, IMAP, POP3, DIIOP, Traveler
- What happens to Domino when I run the LDAP task and make it available as an LDAP directory
  - What fields / information are you sharing?
  - Use an LDAP browser (Softerra's free ldapbrowser is good) to check your own security
  - Secure your servers and only publish what you need

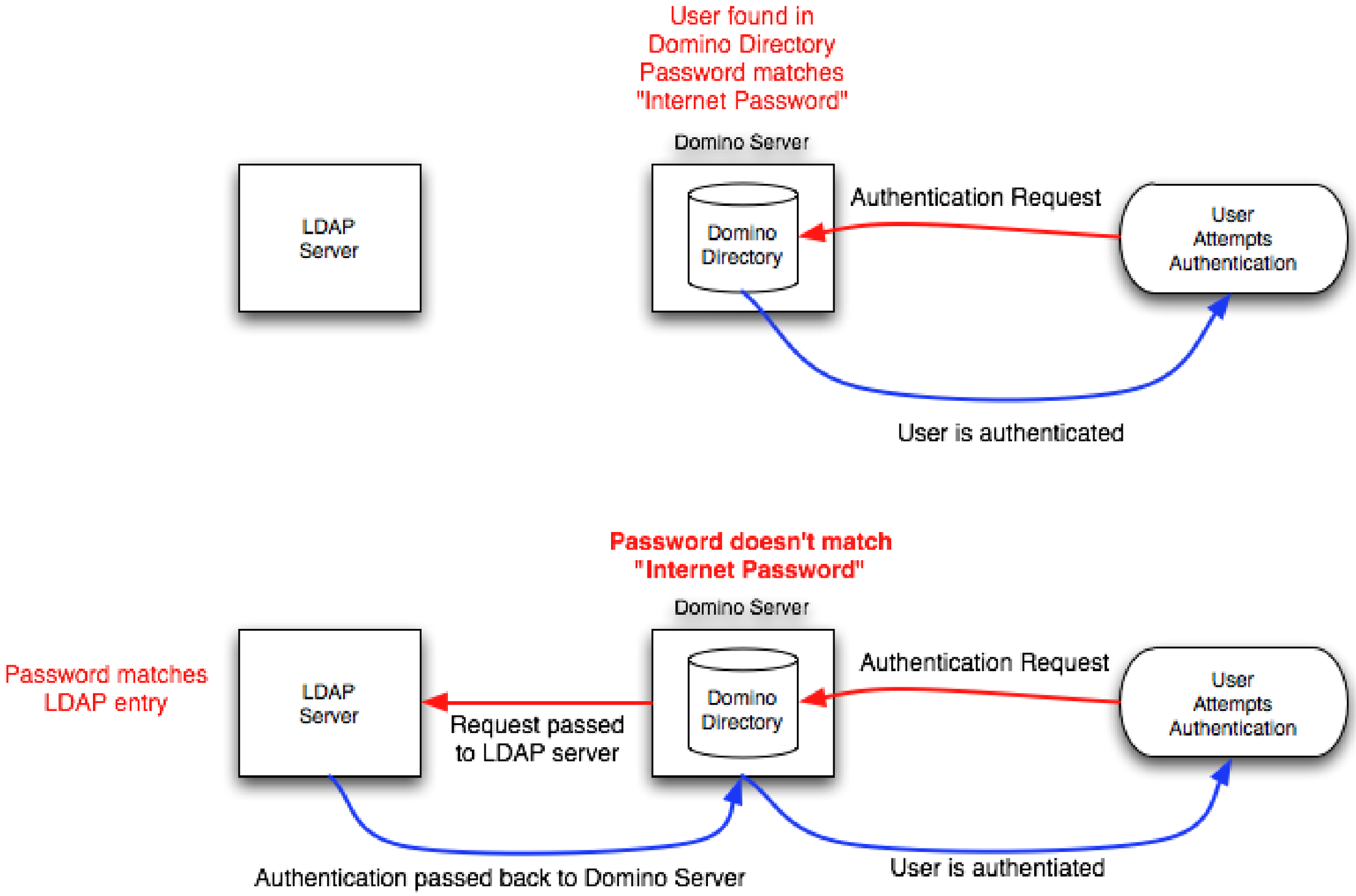
Using LDAP Servers For Authentication

- SSL - impacts performance slightly but guarantees you are talking to the right server
- DNS resolving to the right address / DNS resolving at all
- Security imposed by LDAP administrators (or lack of)
- Be wary of LDAP directories that allow anonymous access
- Encrypt your directory assistance document if it contains bind credentials for LDAP
- Only use bind credentials with the minimum access you need (in most cases, reader)

Two Directories, One Name

- **What we're configuring today**
  - **Single login**
  - **Single password**
  - **Possible removal of HTTP password**
  - **Single point of Administration**

How It Will Work



Setting Up Single Directory - Step by Step

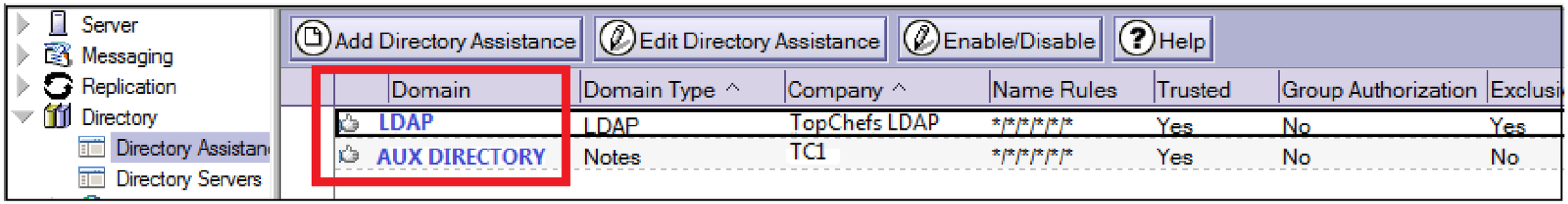
- Create Directory Assistance database in Domino
- Create a Directory Assistance document pointing to a LDAP source (such as Active Directory)
  - You'll need bind credentials (hopefully!)
  - You'll use SSL (also hopefully!)
  - If you use bind credentials without SSL you are sending those in clear text
- Configure your server to use the new Directory Assistance database
  - Restart server if possible
- Test your Directory Assistance works by creating a Domino database with -Default- access set to 'Reader' and Anonymous set to "No Access"
  - Try accessing that database via a URL and logging in using the "name" and password from the LDAP source
  - Until you can successfully login you haven't completed the LDAP setup correctly

Setting Up Single Directory - Step by Step

- **For this next bit you need to charm your LDAP administrator!**
  - **You may want to buy them a coffee first**

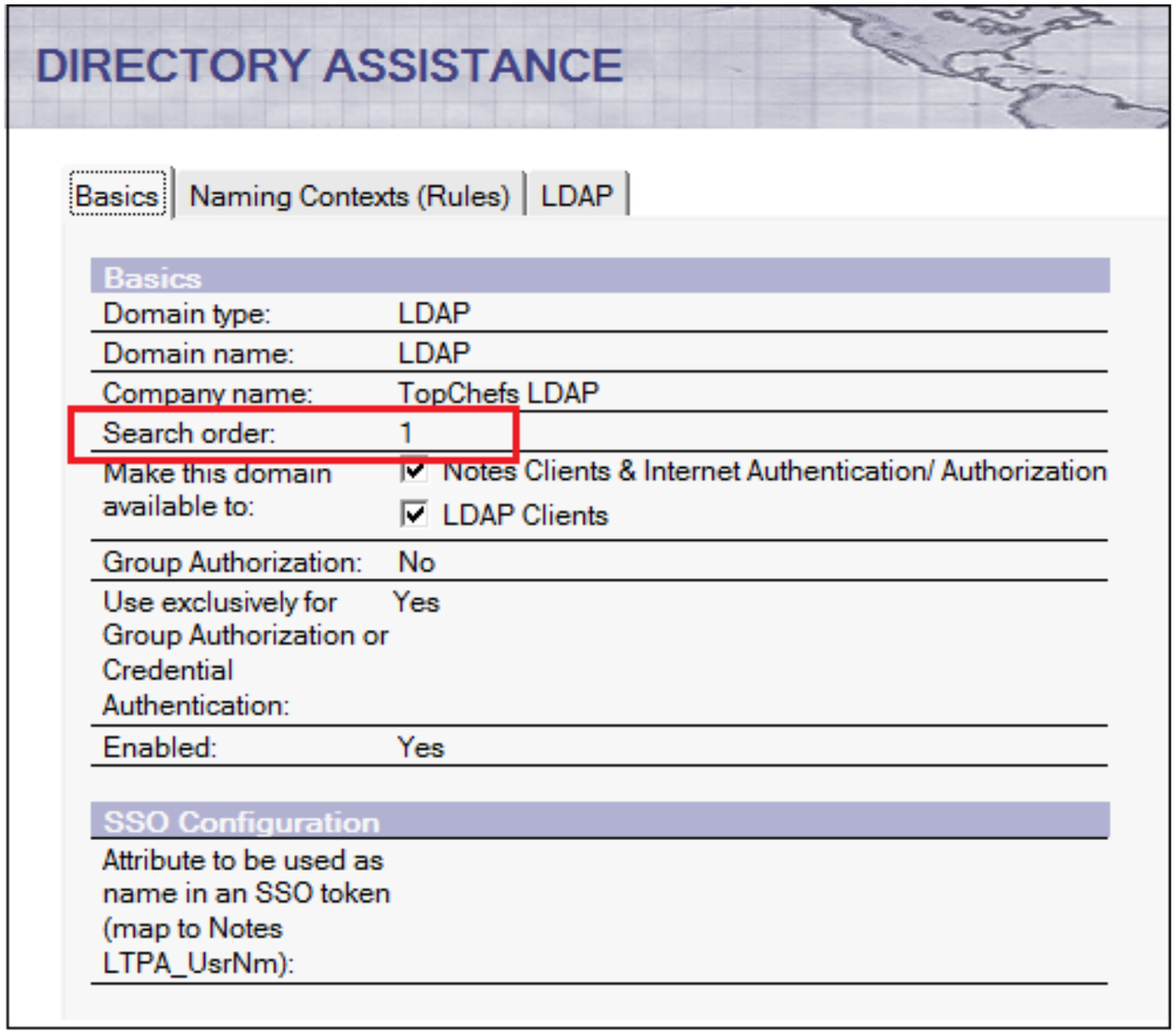
Directory Assistance Configuration Example

- **LDAP server is first listed – as you want this to be primary lookup (outside of your Domino Directory)**



DA Basics Configuration

- LDAP server should be first in search order
- Don't include primary Domino Directory in DA



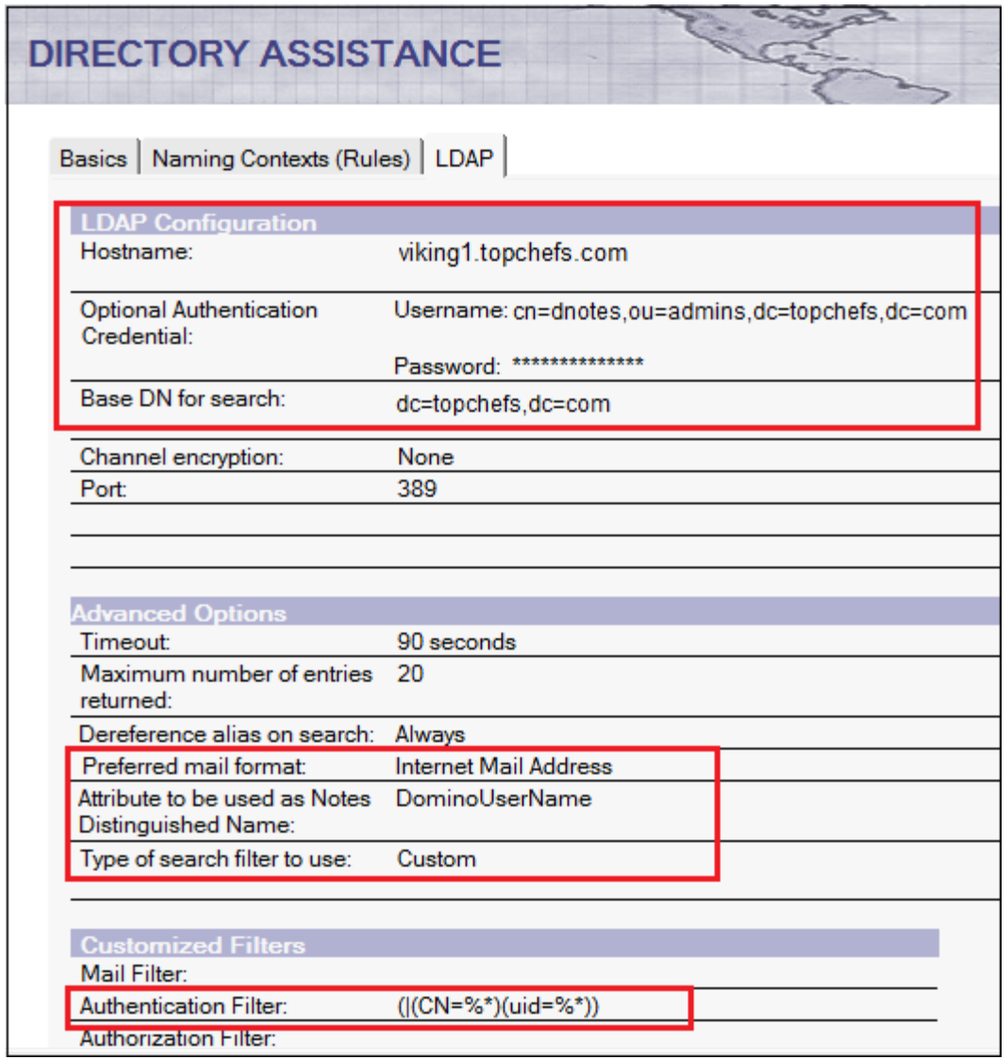
Directory Assistance LDAP Configuration

- **Ensure an attribute in their LD Schema contains, as a minimum, the full hierarchical Notes name of your users**
  - **The LDAP administrators will need to tell you which attribute to use**
  - **You can verify it is configured correctly using an LDAP browser**
  - **It doesn't matter what attribute they give you so long as it's dedicated to that purpose**
    - **If the LDAP distinguished names are the same as your Domino hierarchical names then you don't need to do this**
      - ***eg CN=Gabriella Davis/O=Turtle and LDAP name of CN=Gabriella Davis, O-Turtle***
- **Ensure the attribute value you use to key on is unique**

Directory Assistance LDAP Configuration

Set up connection to LDAP server

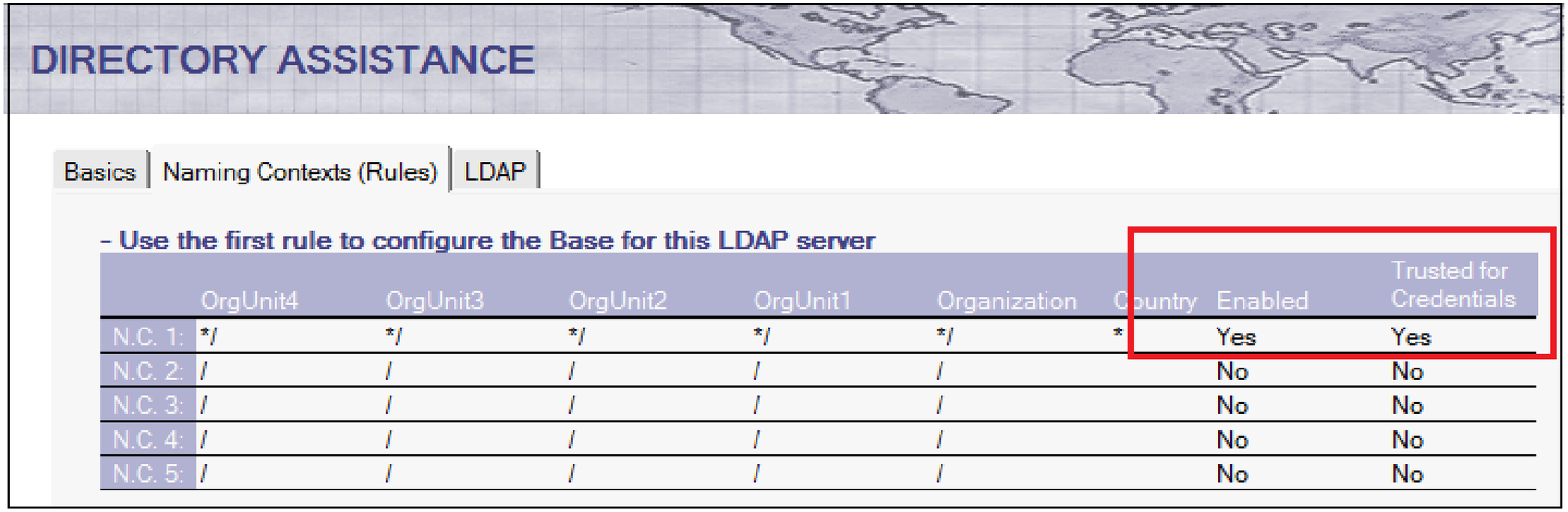
Decide if you should use custom filters



Decide what attribute is to be used as Notes Distinguished Name for lookups

DA Naming Context Configuration

- **Configure to "Trusted for Credentials" as you're going to use this LDAP source for authentication**



	OrgUnit4	OrgUnit3	OrgUnit2	OrgUnit1	Organization	Country	Enabled	Trusted for Credentials
N.C. 1:	*/	*/	*/	*/	*/	*	Yes	Yes
N.C. 2:	/	/	/	/	/		No	No
N.C. 3:	/	/	/	/	/		No	No
N.C. 4:	/	/	/	/	/		No	No
N.C. 5:	/	/	/	/	/		No	No

Now let's test!

- Using the test database we created earlier (-Default- = Reader, Anonymous=No Access)
  - Make sure you close down all browser windows between each test so the credentials don't cache
  - Attempt to open the database via a browser and login using
    - Your Notes name and HTTP password
    - Your Notes name and LDAP password
    - Your LDAP name and LDAP password
  - Have the Internet Access setting on your Domino server document as "Fewer name variations wtih higher security"
    - Add an additional LDAP alias to the "Full Name" field on a person document (eg. LDAP nickname or shortname)
      - *You should now be able to login using either your HTTP or LDAP password using that too*

Our One Directory

- Authentication works for Sametime and other protocols
- If there is no HTTP password (in the Domino Person document) then only the LDAP password is validated for the user
- The HTTP and LDAP passwords don't have to be kept in sync, both will work
  - if that's what you want....
- If you use TDI you can keep the hierarchical name updated automatically (for example after a name change)
  - You can also sync other information to the LDAP directory that other systems may find useful
    - including password syncing

What is IBM Tivoli® Directory Integrator®?

"Tivoli Directory Integrator (TDI) is a graphical integration toolkit for accessing and detecting changes in practically any type of system, data store, protocol, or API. It also lets you transform, filter, and validate this data before driving it to the output targets of your choosing."

Source: Redpaper IBM Lotus Domino Integration Using IBM Tivoli Directory Integrator

- **Use for migration**
- **Use for integration**
- **Use for synchronization**

So why should you use Tivoli Directory Integrator?

- "Free" tool for integration of data sources
- Works great with directories – like Domino, Active Directory, LDAP
- Includes plug-ins for Password Sync – if you're interested!
- Comprised of Project – AssemblyLine, Connector, Attributes, Data Feed, Data Flow.
- Runs on multiple platforms; doesn't have to be installed on Domino server.

TDI is fantastic for working with directories…

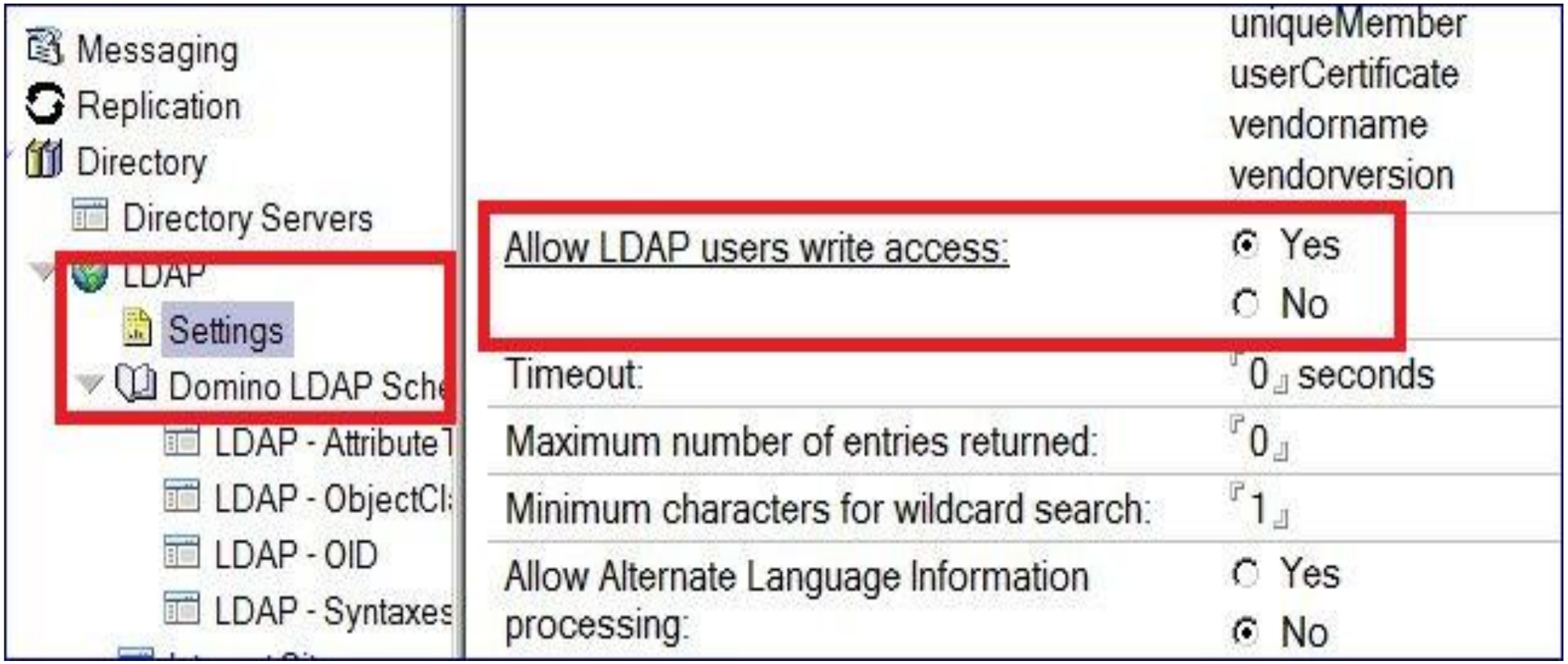
- **Connectors already included for Directory work:**
  - **LDAP Connector:**
    - **Use to connect to LDAP directories (including AD & Domino)**
  - **Domino Change Detection Connector**
    - **Detects changes on objects in a Notes database (add, modify, delete). Includes actions on the names.nsf.**
  - **Active Directory Change Detection Connector**
    - **Detects changes on AD objects.**
  - **Domino Users Connector**
    - **Use when you want to create, delete or modify Notes user information (in names.nsf or admin4.nsf). Can be used to create or delete Notes accounts.**

A few words about LDAP and TDI…

- **Rule #1: Love your LDAP or AD Administrator because they will need to "Love" you.**
  - They will need to grant you access to LDAP or AD to update records
  - They may need to add attributes to the LDAP or AD schema
    - Especially if you're going to add custom attributes
  - Ask for access to the Test system first!
    - So you can demonstrate you're not going to "blow up" the LDAP or AD directory!

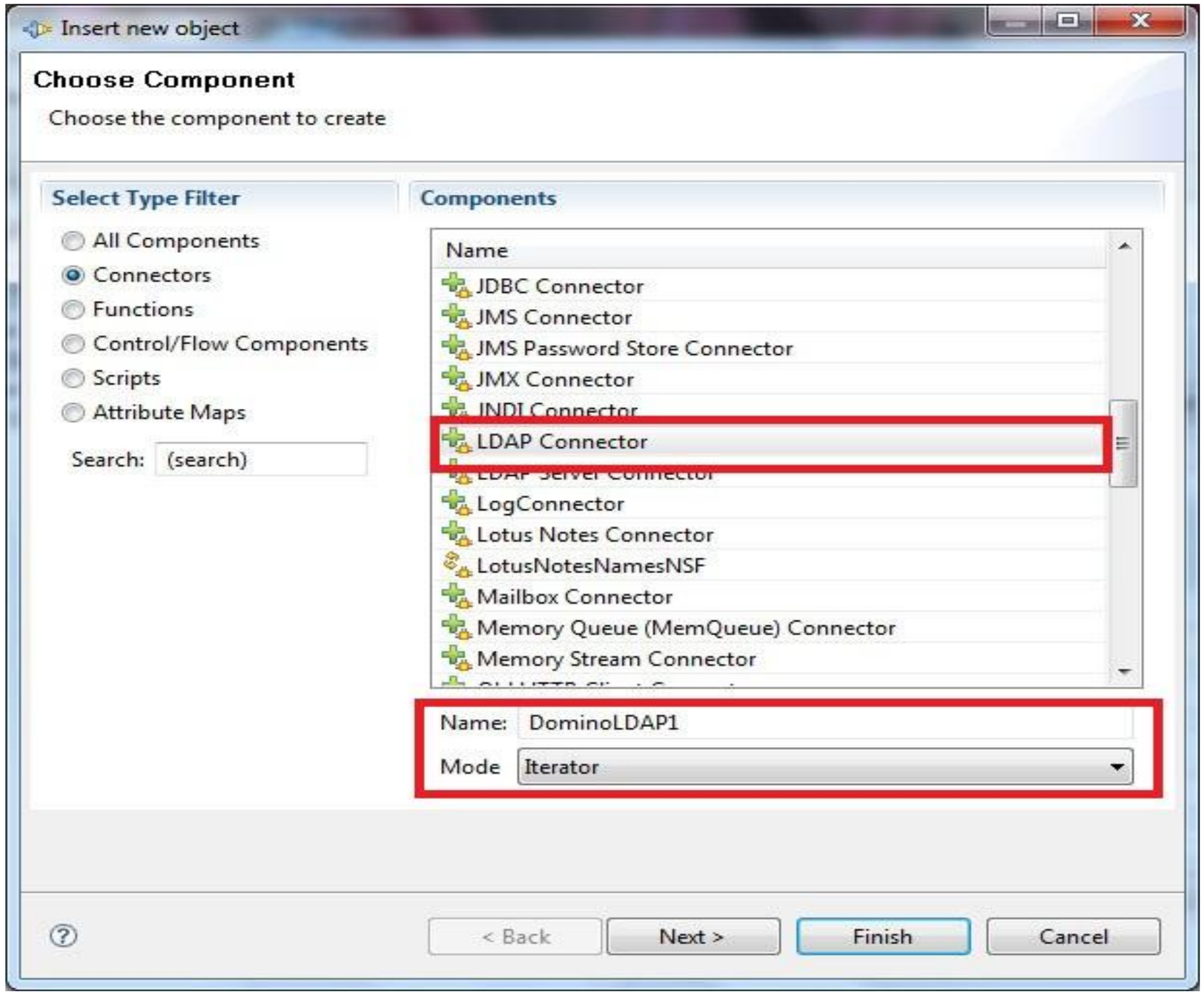
A little Domino LDAP config check:

- Confirm that domain configuration document has the following set on the LDAP tab.
- You can control security via Security settings.



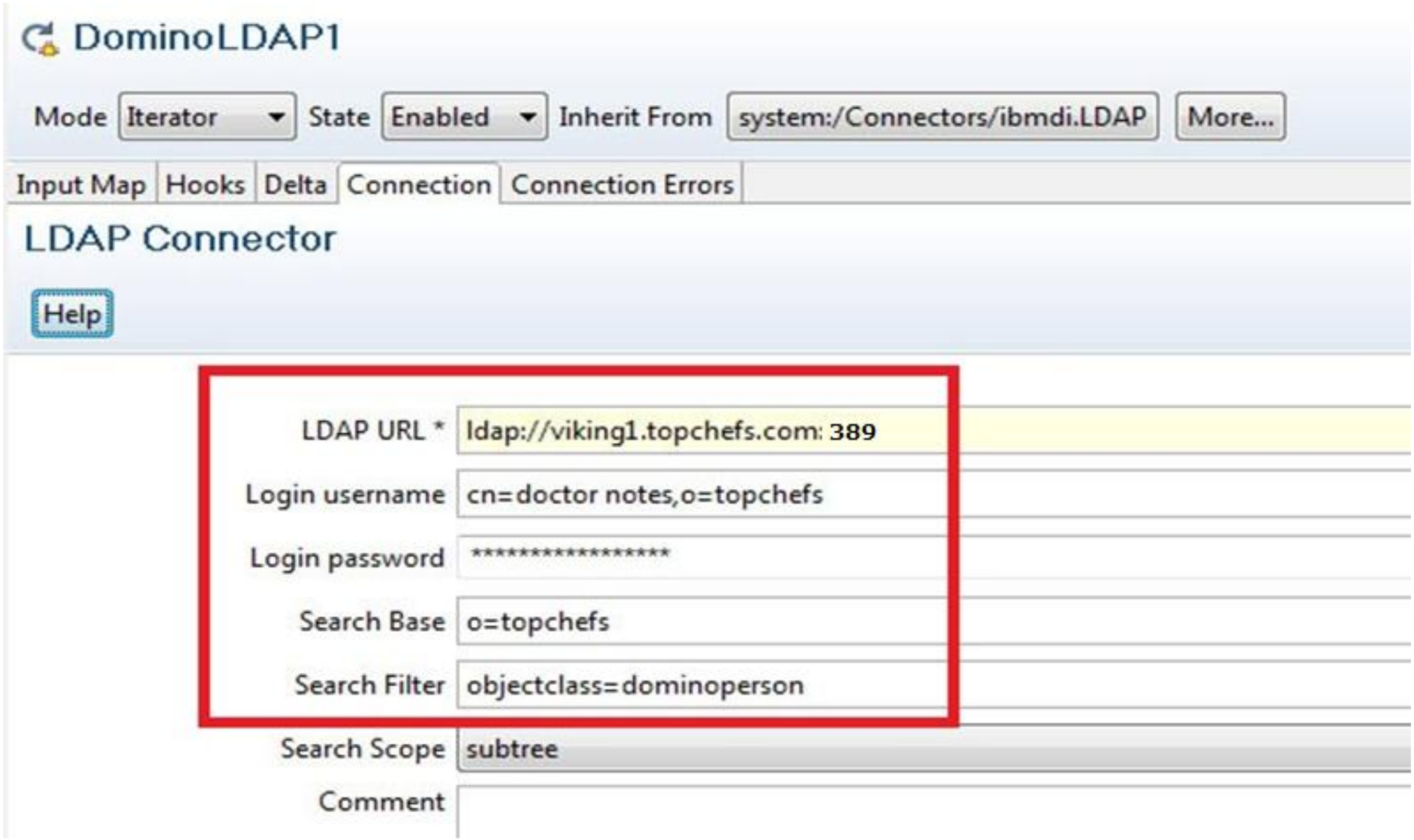
Create Domino LDAP Connector

- Create a connector for Domino – using base LDAP Connector
- Create in Iterator Mode



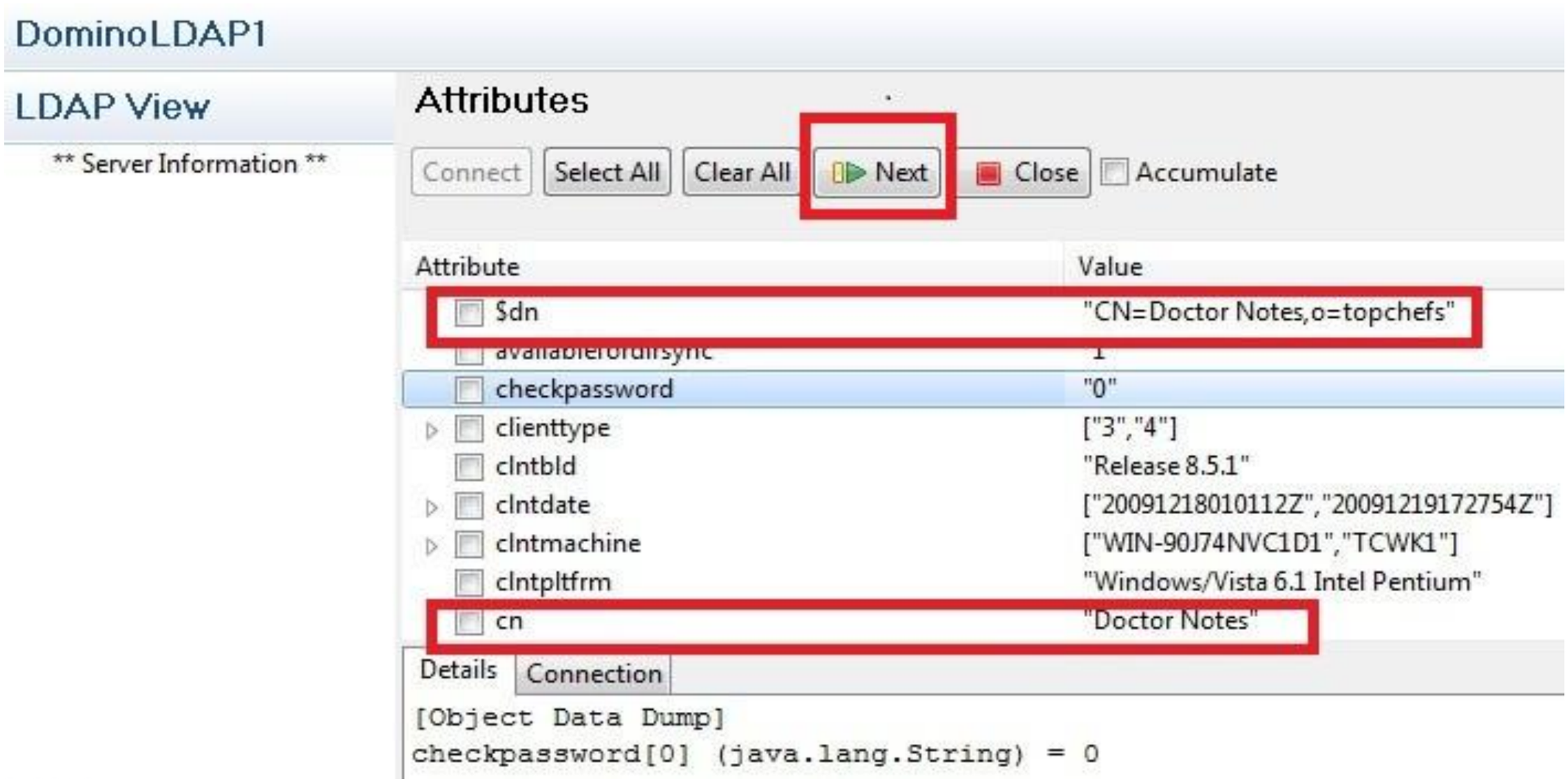
Configure the Domino LDAP Connector

- Add the specifics for your Domino LDAP connection (Connector Tab)



Browsing Domino Directory Data

- Allows you to see the actual Domino Directory data in LDAP format
- Click Next to cycle through records in the names.nsf
- Helps you determine if you need to make any editing changes in your AssemblyLine



Example: Add Domino Attributes to LDAP Directory

LDAP Attribute	Example Value
DominoUserName	cn=doctor notes/ou=admins/o=topchefs
DominoUserAbbrev	doctor notes/admins/topchefs
MailFile	mail1/dnotes.nsf
MailServer	cn=viking1/o=topchefs
SametimeServer	cn=sametime1/o=topchefs

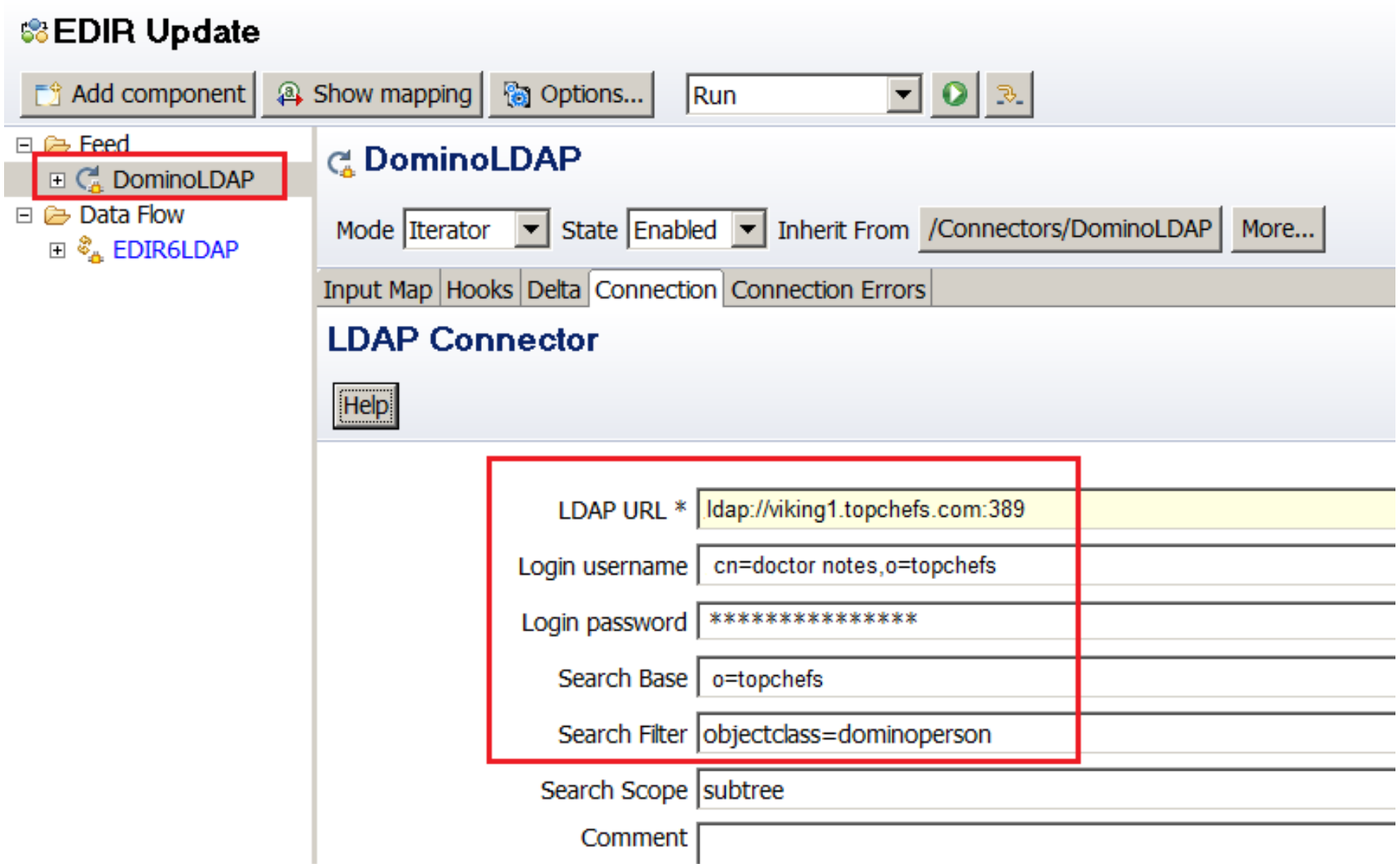
- **DominoUserName**
  - **Allows you to specify the format Domino expects canonical names to be in vs. LDAP format.**
- **DominoUserAbbrev**
  - **Allows you to specify the user name in Abbreviated Name format (use for custom Directory lookups)**
- **MailFile**
  - **Allows you specify the mail file path of the user's mail file – useful for centralized web authentication.**
- **MailServer**
  - **Allows you to specify the name of the user's primary mail server – useful for centralized web authentication.**
- **SametimeServer**
  - **Allows you to specify the canonical name of the Sametime Server – especially important if you have multiple ST servers.**

So how do you get this data from Domino to LDAP or AD?

- **Set up a TDI AssemblyLine**
  - Create an LDAP connector to Domino LDAP server
    - Modify Domino fields with javascript to change from LDAP format to Domino format, e.g., commas to slashes
  - Create an LDAP connector to LDAP or AD Server
  - Data Feed = Domino LDAP Connector
  - Data Flow = LDAP/AD Connector

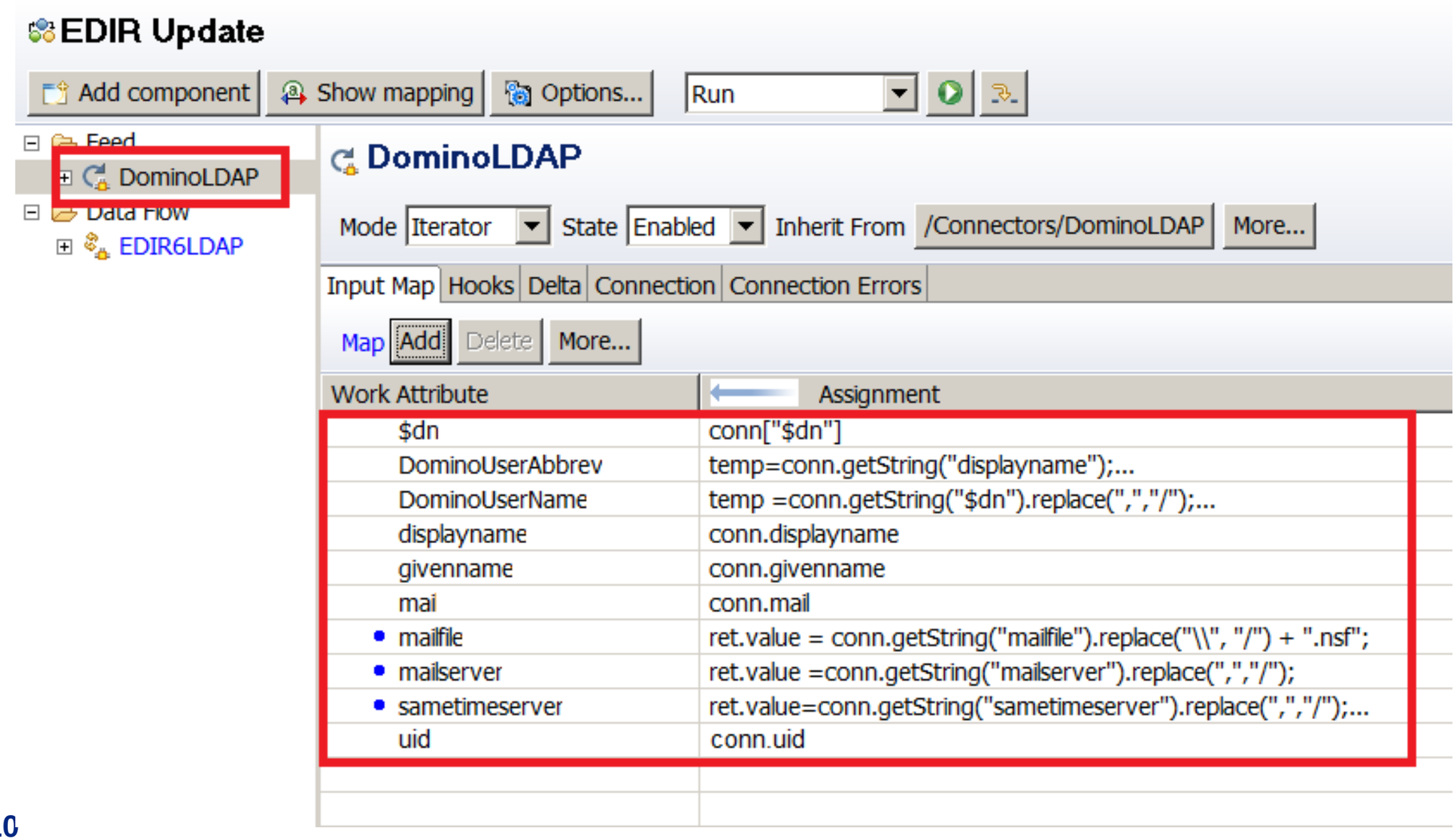
Domino LDAP Connector

- Iterator mode (cycles through records one at a time)
- Search Filter is important to limit the scope of search – you don't need Server documents, etc., included in the search.



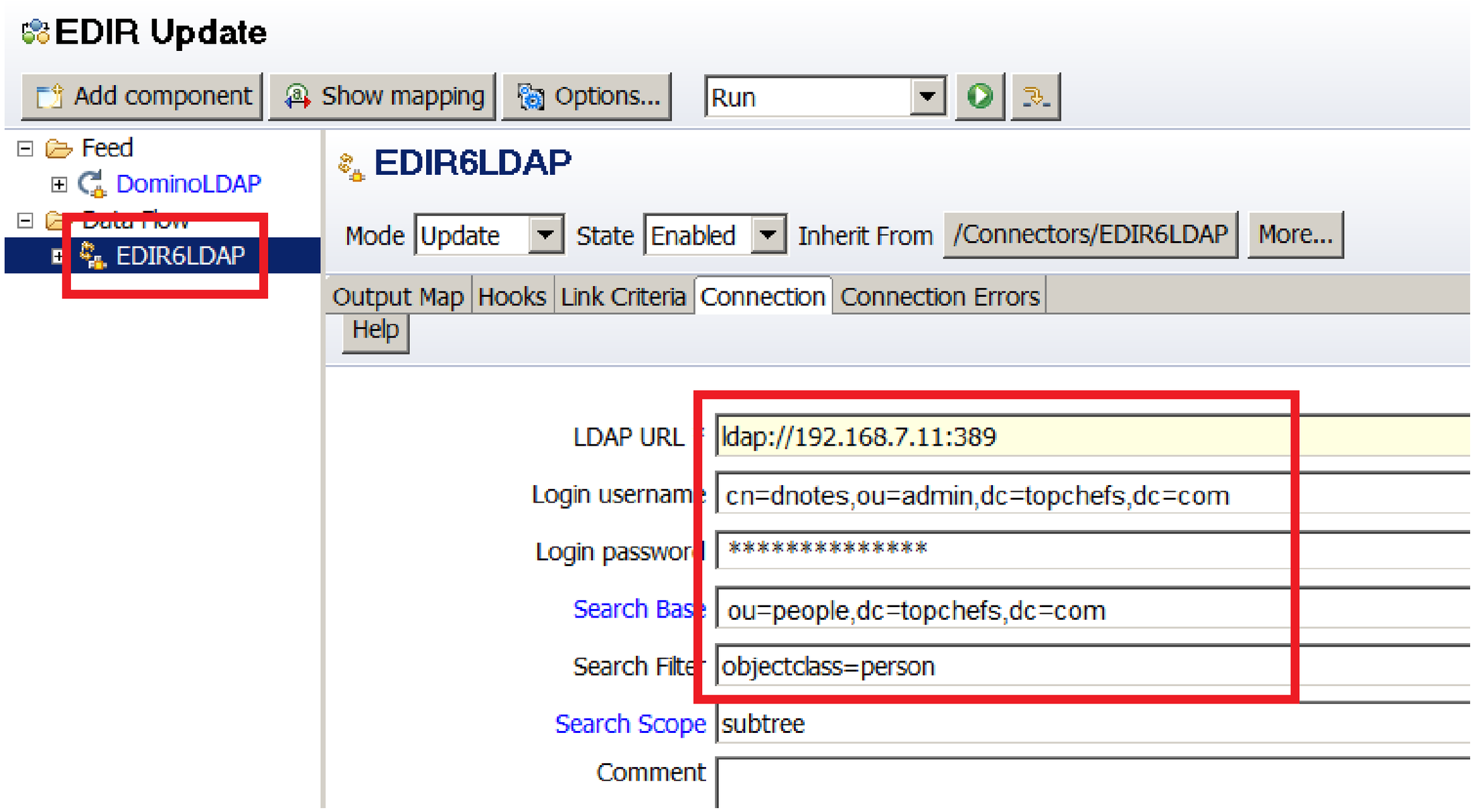
Data Feed: Use Domino LDAP Connector

- Input Map – make any “editing” changes to the Work Attribute
- In this example – removing commas and changing to forward slashes



LDAP Connector

- **Search Filter – only include those objects you want to include in the search**



Data Flow: LDAP Connector

- Work Mode is “Update” as you’re updating attribute values

EDIR Update

Add component | Show mapping | Options... | Run

- Feed
  - DominoLDAP
- Data Flow
  - EDIR6LDAP

EDIR6LDAP

Mode: Update | State: Enabled | Inherit From: /Connectors/EDIR6LDAP | More...

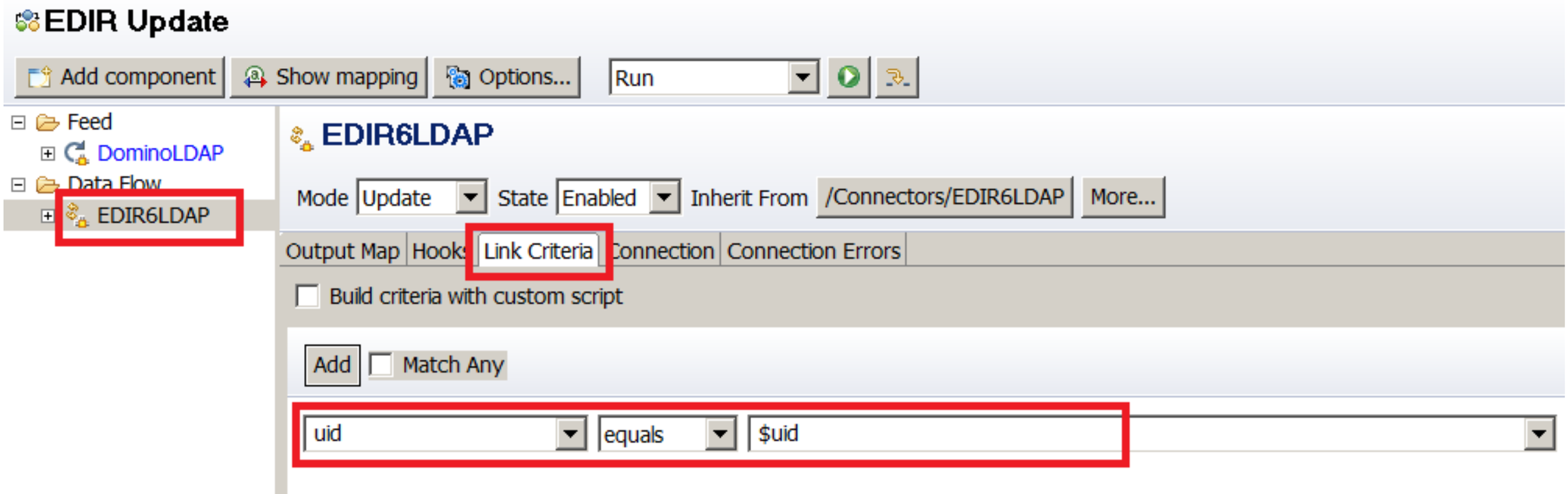
Output Map | Hooks | Link Criteria | Connection | Connection Errors

Map | Add | Delete | More...

Assignment	Add	Mod	Component
ret.value="uid=" + work.getString("uid") + ",ou=people,dc=topchefs,dc=com"	false	false	$dn
ret.value = work.getString("DominoUserAbbrev");	false	true	DominoUserAbbrev
ret.value = work.getString("DominoUserName");	false	true	DominoUserName
ret.value=work.getString("MailFile");...	false	true	MailFile
ret.value =work.getString("MailServer");...	false	true	MailServer
ret.value = work.getString("sametimeserver");	false	true	SametimeServer
work.givenname	false	false	givenname
work.uid	false	false	uid

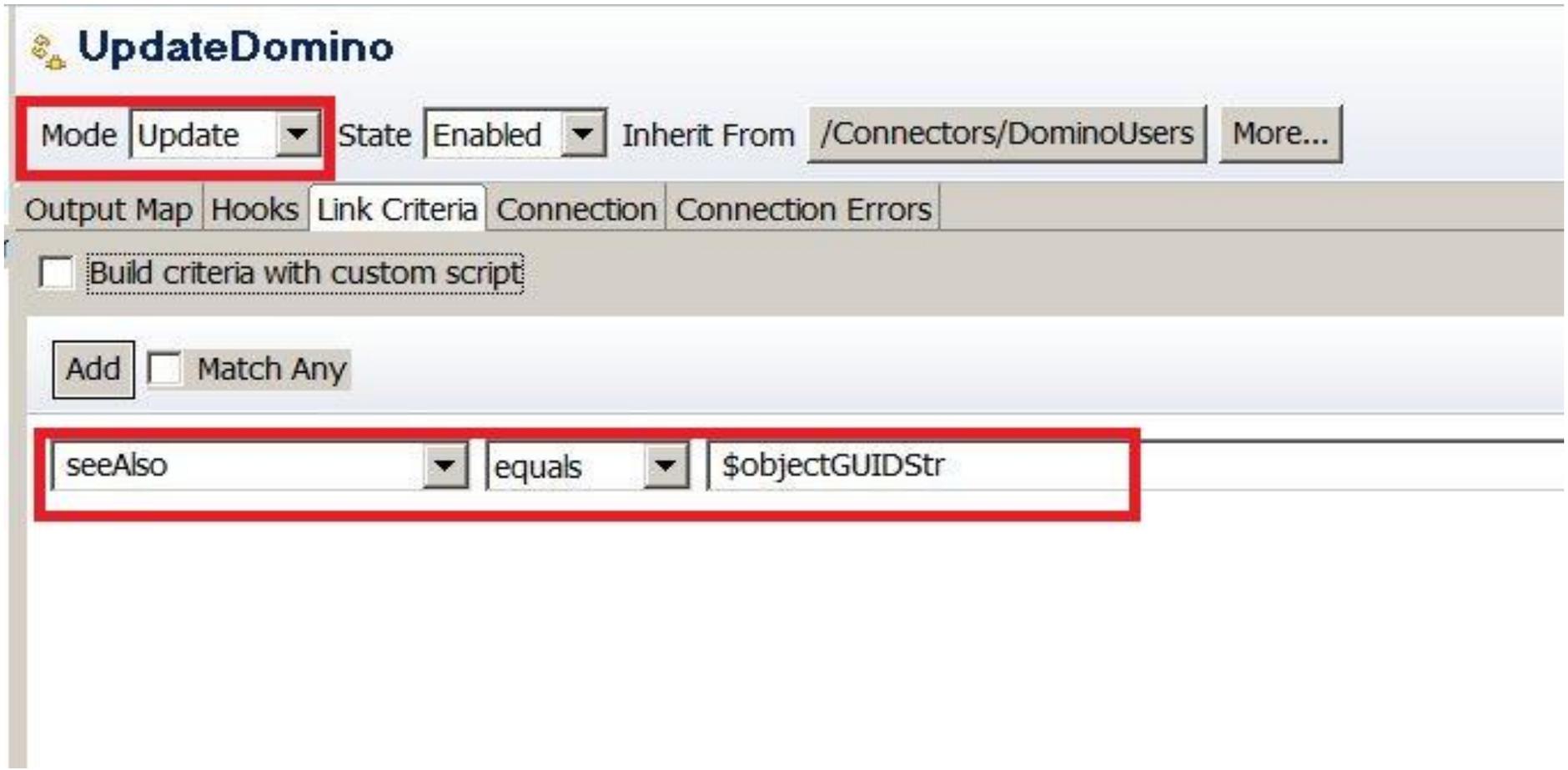
Data Flow: Link Criteria

- Create Link Criteria to indicate what are the unique keys that must have the same value before the update will take place
- UID (LDAP) equals $UID (Domino) – if not true record's attributes won't be updated



Create UpdateDomino Link Criteria

- **Link Criteria includes fields used to detect account changes.**



Example: Update Corporate Data in Domino from AD

- **Create an AssemblyLine**
  - Create a Active Directory Change Detection Connector
  - Create a Domino Users Connector
  - Data Feed = Active Directory Change Detection Connector
  - Data Flow = Domino Users Connector
  - Include logic that will delete records in Names.nsf if AD userids are deleted.
  - Include logic to update corporate info: phone, office location, title, department in person record in Names.nsf

SyncAD_to_Domino Final AssemblyLine

SyncAD_to_Domino

Add component | Show mapping | Options... | Run

- Feed
  - ADChanges
- Data Flow
  - IF: IF delete
    - DeleteDomino
  - ELSE: ELSE add or modify
    - UpdateDomino
      - Before Modify

Map | Add | Delete | Browse Data

Work Attribute	Assignment	Component Attribute
ADChanges	←	[Source]
*	(Map all Attributes)	*
DeleteDomino	←	[Source]
	[Empty map - double click to ac	
UpdateDomino	→	[Target]
Department	work.Department	Department
sAMAccountName	work.sAMAccountName	EmployeeID
givenName	work.givenName	FirstName
	Person	Form [Add]
getString	ret.value = "cn=" + work.getSt	FullName
mai	work.mail	InternetAddress
title	work.title	JobTitle
sn	work.sn	LastName
Location	[work.Location, work["$dn"]]	Location
cn	{work.cn}/TOPCHEFS	MailAddress
department	work.department	OU
getString	ret.value = "cn=" + work.getSt	Owner [Add]
telephoneNumber	work.telephoneNumber	PhoneNumber
sAMAccountName	work.sAMAccountName	ShortName [Add]
description	work.description	Title
	Person	Type [Add]
objectGUIDStr	work.objectGUIDStr	seeAlso

Isn’t Domino Already Doing Directory Integration ?

- Active Directory plug-in
- IBM / Lotus plans for directory integration
- Single Notes Logon
  - Client Shared Login
- SPNEGO!

SPNEGO

- Windows sign on for HTTP clients
- Once you have logged into Windows, you are automatically authenticated to Domino and Sametime
- Requires a Windows based Domino server
  - Configured for multi server SSO, this can be an invisible “point of entry” for clients into your environment
- Requires Active Directory 2003 and higher
- Users must login to an Active Directory domain
- Your ‘entry’ Domino server logs in as a user to Active Directory

Resources

- **Domino Directory**
  - **Domino Directory FAQs (notes.net)**
    - http://www-10.lotus.com/ldd/nd6forum.nsf/0/5c4bf25f844b9ac785256e4c005998b7
    - Includes technotes about LDAP (general), Directory Assistance, Domino LDAP schema and tons more!
  - **Domino Directory Wiki**
    - http://www-10.lotus.com/ldd/dominowiki.nsf/xpViewCategories.xsp?lookupName=Domino%20directory
- **Tivoli Directory Integrator Resources**
  - IBM Tivoli Directory Integrator Users group – http://www.tdi-users.org
  - Consultant in Your Pocket Webcasts: TDI Admin Perspective & TDI Developer Perspective: http://consultantinyourpocket.com/ciyp/ciyp.nsf/

Questions or Comments?

- **Gabriella Davis**
  - Blog: http://blog.turtleweb.com
  - Twitter: gabturtle
  - Email: gabriella@turtlepartnership.com

- **Marie Scott**
  - Blog: http://www.bleedyellow.com/blogs/crashtestchix
  - Twitter: marie_scott
  - Email: mlscott@vcu.edu