DIRECTORY INTEGRATION: USING ACTIVE DIRECTORY FOR AUTHENTICATION

Gabriella Davis
The Turtle Partnership

In This Session

- Review possible use cases for multiple directories
- Understand security implications of having multiple directories
- Configure authentication using a Domino user id and a LDAP password
- Learn what your options for Single Sign On are

Agenda

- Directory Assistance
- Domino as LDAP
- Secondary Directories and Security
- Our One Directory
- Setting Up “One Directory”
- Other Single Sign – On
- Wrap Up

Single Sign On vs Single Password

- Many people ask for "SSO" but is that what they actually want?
  - SSO means that the user is never prompted for another password as they move from server to server
  - The key thing about SSO is that all servers involved must be sharing a single internet domain
    - www.turtlepartnership.com and quickr.turtlepartnership.com can share a SSO configuration and will not prompt the user to re-enter a password
    - Sametime.turtleweb.com is a different domain and cannot share a SSO configuration with the turtlepartnership.com servers
- Often people will settle for there being a single password, so if users are prompted to login more than once, they at least have only one set of credentials to use everywhere
- Both SSO and single password have security implications

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 Directory Language
  - Schemas translate Design
  - Attributes vs Fields
- LDAP Servers
  - Active Directory
  - Novell eDirectory
  - Tivoli Directory
  - Sun One

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

What We'll Cover

- Directory Assistance
- Domino as LDAP
- Secondary Directories and Security
- Our One Directory
- Setting Up "One Directory"
- Other Single Sign – On
- Wrap Up

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!

Domino as LDAP

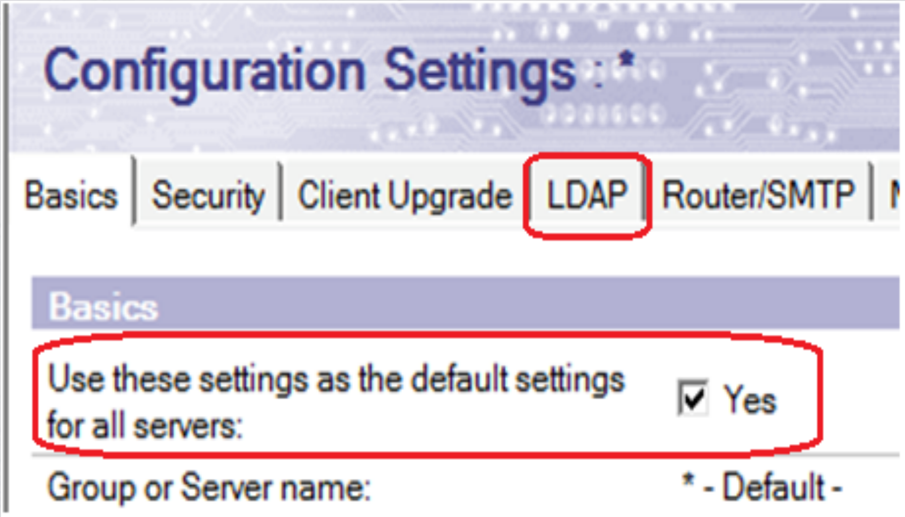
- Domino can act as an LDAP itself
  - It can make itself available to any LDAP client
  - It can allow LDAP clients to search its directory (names.nsf)
  - You can select which additional directories outside of names.nsf are available to LDAP clients

Domino as LDAP

- 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!

Domino as LDAP

- 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” 9



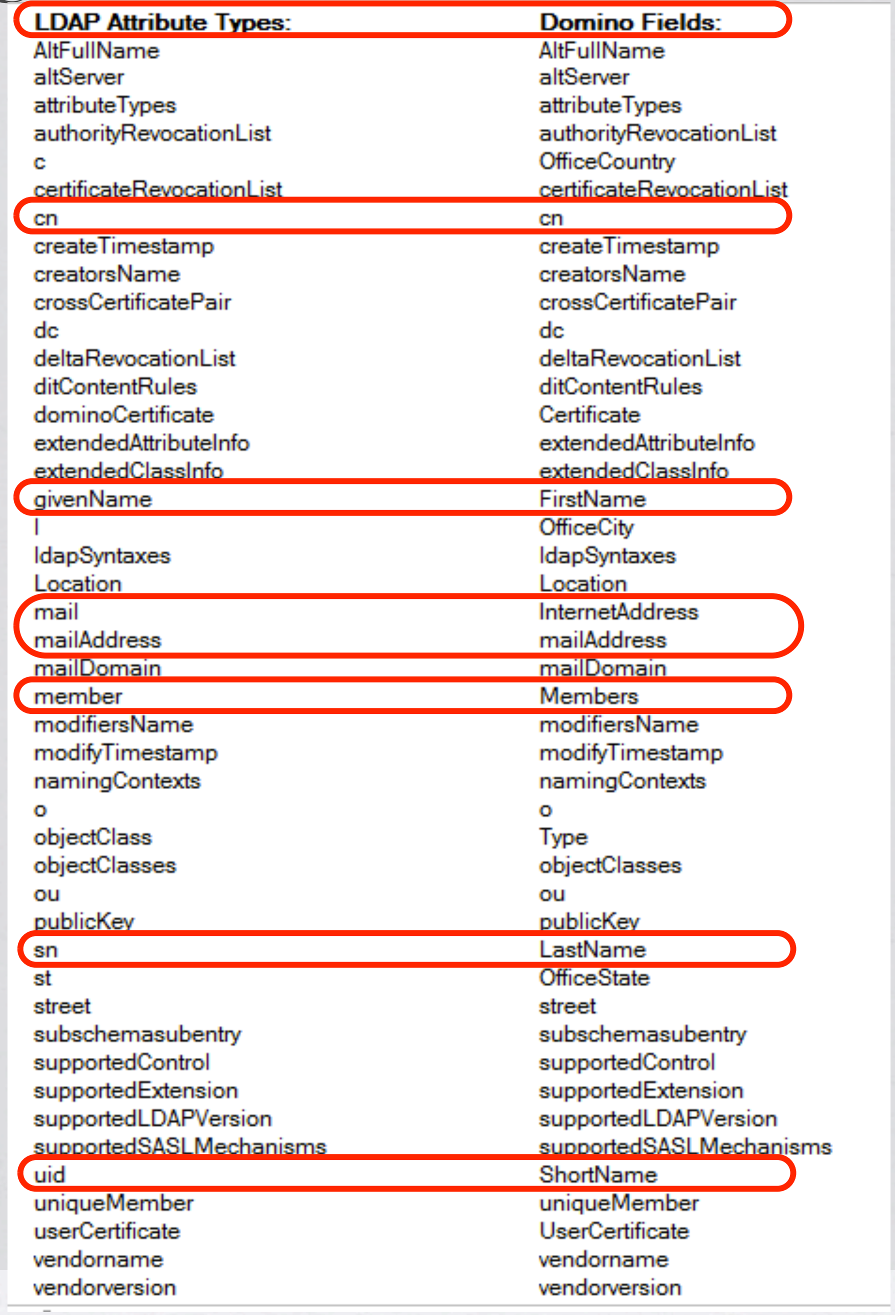
Configuration Settings : *

Basics

Use these settings as the default settings for all servers: ☑ Yes

Group or Server name: * - Default -

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
createTimestamp	createTimestamp
creatorsName	creatorsName
crossCertificatePair	crossCertificatePair
dc	dc
deltaRevocationList	deltaRevocationList
ditContentRules	ditContentRules
dominoCertificate	Certificate
extendedAttributeInfo	extendedAttributeInfo
extendedClassInfo	extendedClassInfo
givenName	FirstName
l	OfficeCity
ldapSyntaxes	ldapSyntaxes
Location	Location
mail	InternetAddress
mailAddress	mailAddress
mailDomain	mailDomain
member	Members
modifiersName	modifiersName
modifyTimestamp	modifyTimestamp
namingContexts	namingContexts
o	o
objectClass	Type
objectClasses	objectClasses
ou	ou
publicKey	publicKey
sn	LastName
st	OfficeState
street	street
subschemasubentry	subschemasubentry
supportedControl	supportedControl
supportedExtension	supportedExtension
supportedLDAPVersion	supportedLDAPVersion
supportedSASLMechanisms	supportedSASLMechanisms
uid	ShortName
uniqueMember	uniqueMember
userCertificate	UserCertificate
vendorname	vendorname
vendorversion	vendorversion

LDAP Options Affecting Domino Performance

- Allow LDAP users write access
  Do you want LDAP clients to be able to make change to your Domino Director(ies) ? This doesn't override directory ACL or roles.

- Timeout
  How many seconds before a search is cancelled. Don't leave it as zero which means indefinite.

- Maximum number of entries returned
  When doing an LDAP search against a large directory you can restrict the number of results returned

- Minimum characters for wildcard search
  Do you really want people searching for the letter "S" if they are looking for "Smith" or even "Sm"

- Allow Alternate Language Information processing

- 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?

LDAP Options Affecting Domino Performance

- Automatically Full Text Index Domino Directory?
  Improves performance of searches against Domino Directory but only use if you are performing high demand searches against a large Directory

- Enforce schema?
  If the LDAP user has write access to the Domino Directory can they write or change attributes that aren't defined in the Domino schema

- DN Required on Bind?
  Require fully distinguished name for security

- Encode results in UTF8 for LDAPv2 clients?
  If you really care it's about the formatting of results for older LDAP client queries

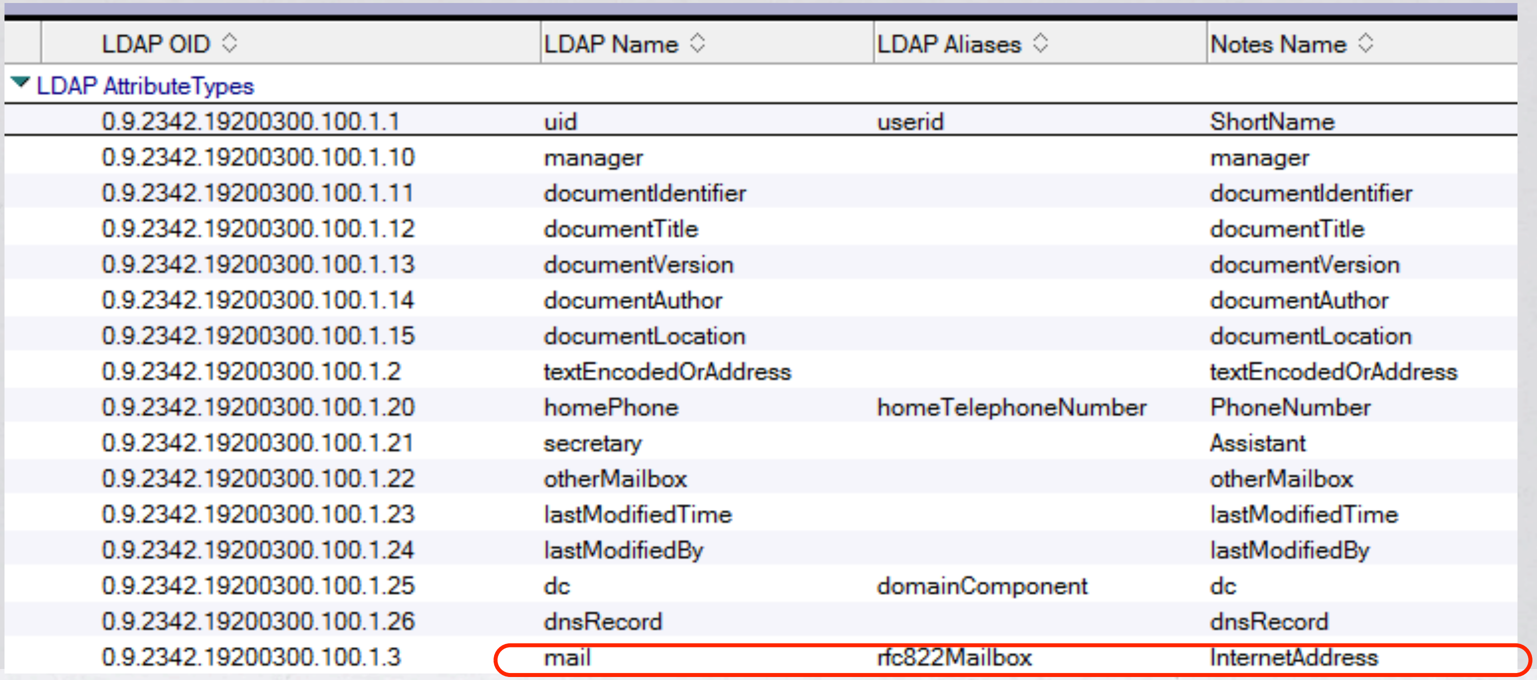
- Maximum number of referrals:

- Activity Logging truncation size:

- Allow dereferencing of aliases on search requests?
  Instructing Domino to return search values that correspond to aliases matched by a search?

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

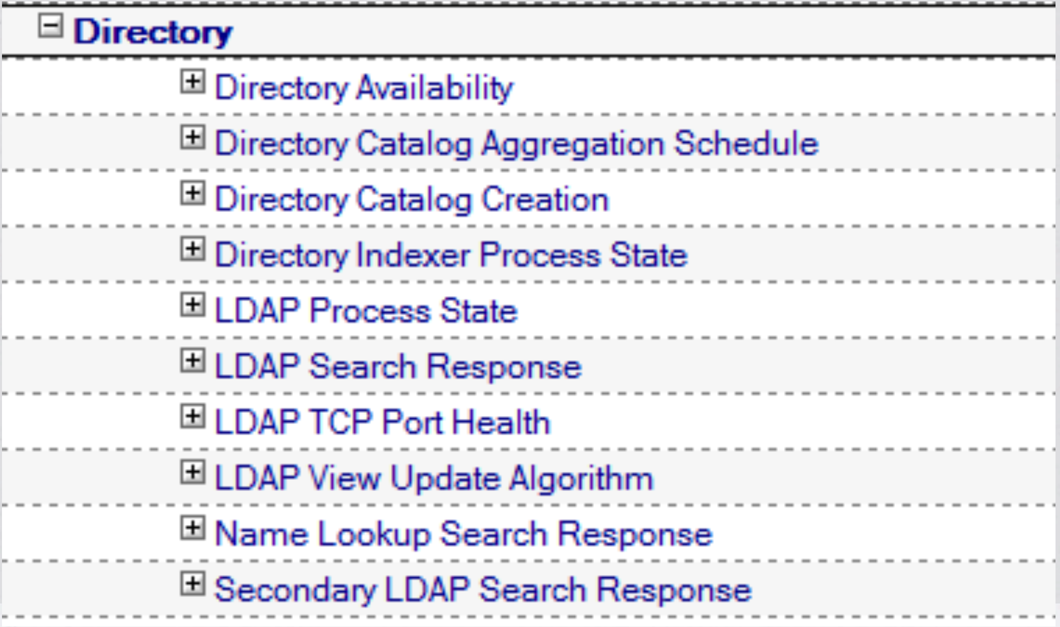
- Domino prioritises indexing and maintenance of the directories highly in terms of allocating resources
- Directory information is cached for performance
- Performing a lookup or doing type-ahead utilises all server based directories
    - The server you use for lookup is set in your location document 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



⊟ Directory

⊞ Directory Availability

⊞ Directory Catalog Aggregation Schedule

⊞ Directory Catalog Creation

⊞ Directory Indexer Process State

⊞ LDAP Process State

⊞ LDAP Search Response

⊞ LDAP TCP Port Health

⊞ LDAP View Update Algorithm

⊞ Name Lookup Search Response

⊞ Secondary LDAP Search Response

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

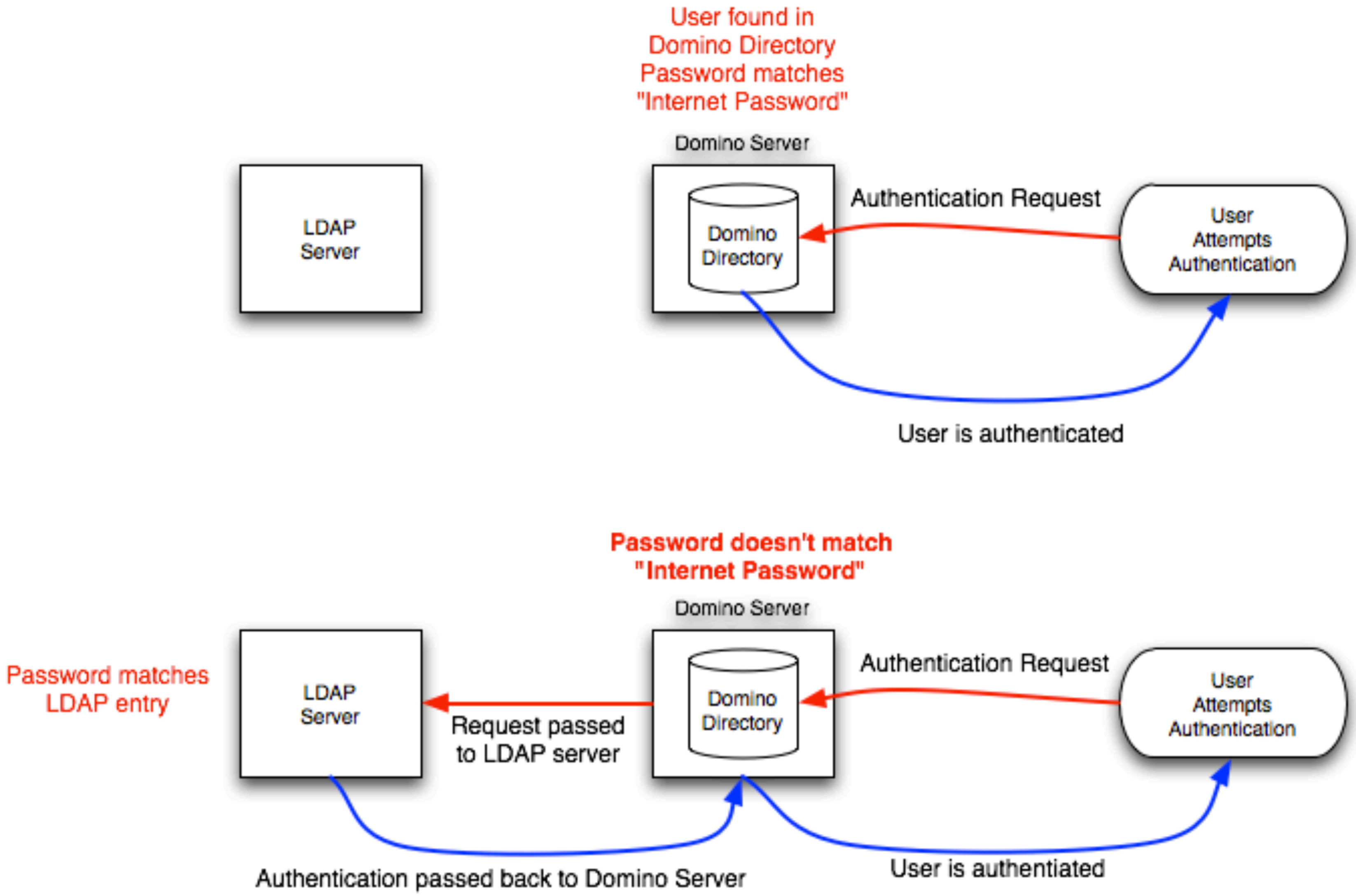
Using LDAP Servers For Authentication

- 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



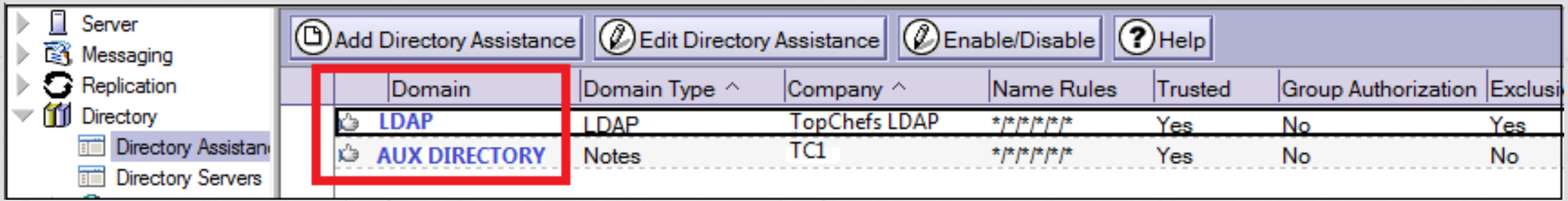
Setting Up Single Directory – Step by Step

1. Create Directory Assistance database in Domino
2. 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
3. Configure your server to use the new Directory Assistance database
   - Restart server if possible
4. 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

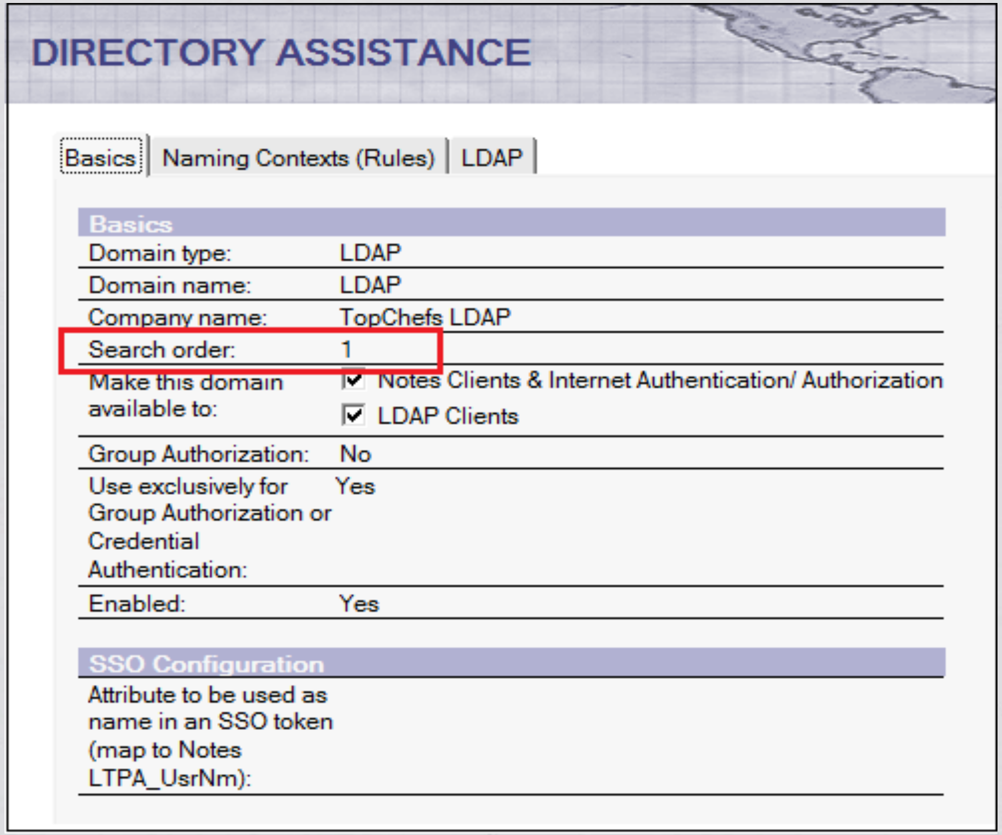


Domain	Domain Type ^	Company ^	Name Rules	Trusted	Group Authorization	Exclusi
LDAP	LDAP	TopChefs LDAP	*/*/*/*/*	Yes	No	Yes
AUX DIRECTORY	Notes	TC1	*/*/*/*/*	Yes	No	No

- 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 (names.nsf) in DA



DIRECTORY ASSISTANCE

Basics

Domain type:	LDAP
Domain name:	LDAP
Company name:	TopChefs LDAP
Search order:	1
Make this domain available to:	☑ Notes Clients & Internet Authentication/ Authorization ☑ LDAP Clients
Group Authorization:	No
Use exclusively for Group Authorization or Credential Authentication:	Yes
Enabled:	Yes

SSO Configuration

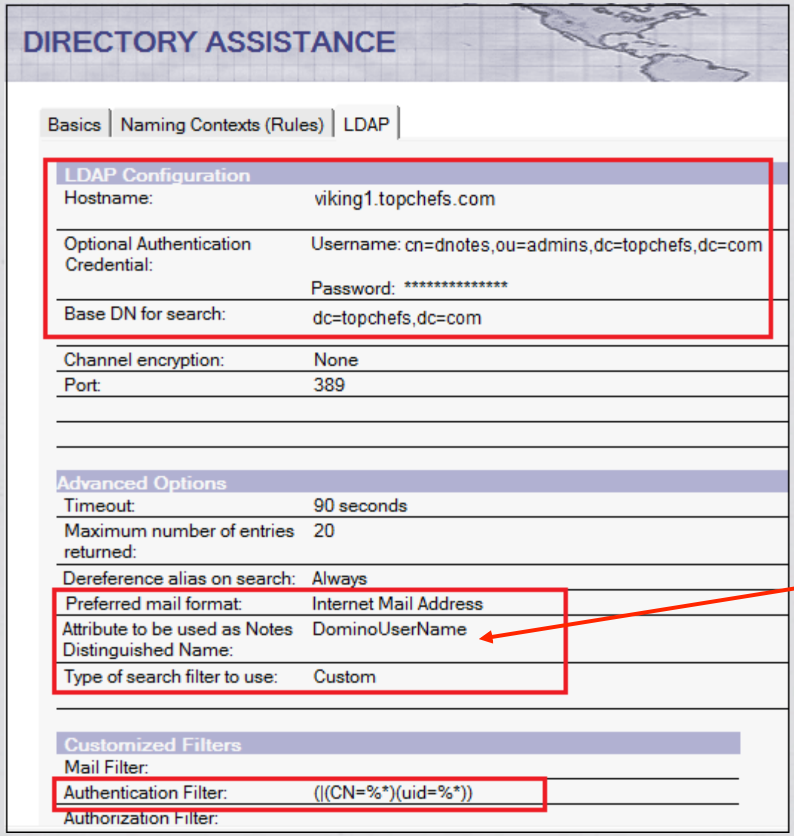
Attribute to be used as name in an SSO token (map to Notes LTPA_UsrNm):	

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



DIRECTORY ASSISTANCE

LDAP Configuration

Hostname:	viking1.topchefs.com
Optional Authentication Credential:	Username: cn=dnotes,ou=admins,dc=topchefs,dc=com Password: **************
Base DN for search:	dc=topchefs,dc=com
Channel encryption:	None
Port:	389

Advanced Options

Timeout:	90 seconds
Maximum number of entries returned:	20
Dereference alias on search:	Always
Preferred mail format:	Internet Mail Address
Attribute to be used as Notes Distinguished Name:	DominoUserName
Type of search filter to use:	Custom

Customized Filters

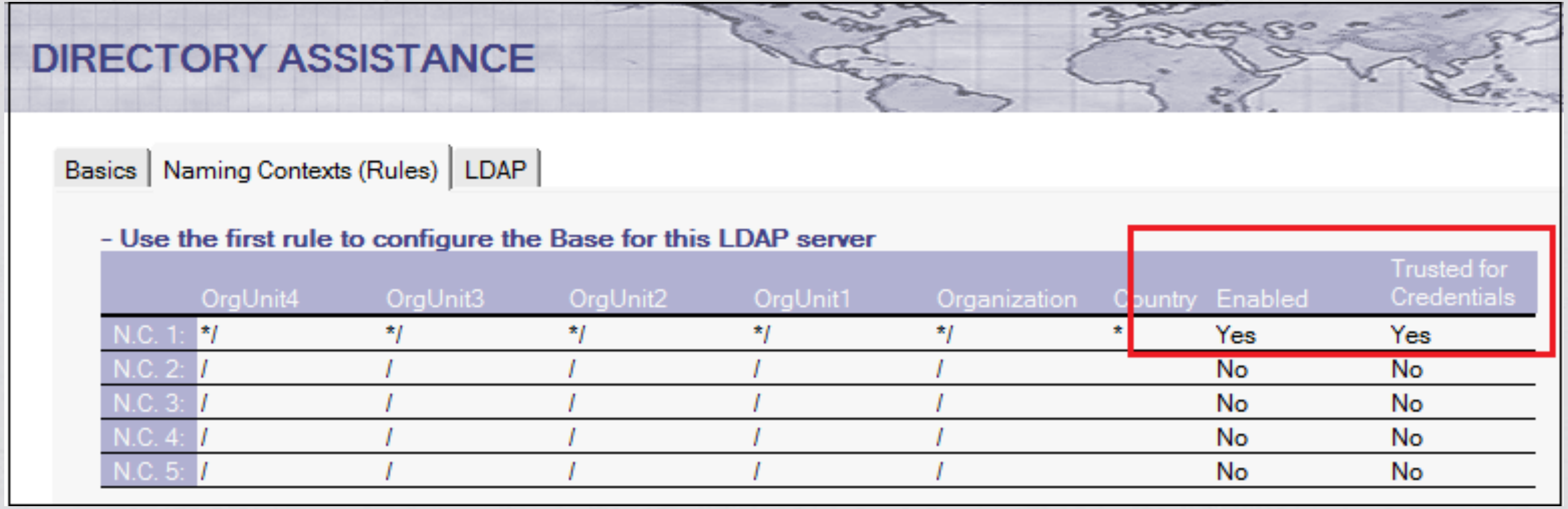
Mail Filter:	
Authentication Filter:	(|(CN=%*)(uid=%*))
Authorization Filter:	

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

Decide if you should use custom filters

DA Naming Context Configuration

- Configure to “Trusted for Credentials” as you’re going to use this LDAP source for authentication



DIRECTORY ASSISTANCE

- Use the first rule to configure the Base for this LDAP server

	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

Storing The Unique Name

- The LDAP directory must contain the hierarchical name of the user in the Domino Directory in an attribute
- How do you keep that in sync
    - Manually?
    - TDI?

Tivoli Directory Integrator

- Licensed for use as long as your source or destination directory is Domino
- TDI can monitor a source directory for changes and trigger activity in a destination directory.
    - This behaviour is detailed in an Assemblyline, a logical flow chart built in TDI that specifies what to monitor and what to do when triggered
- TDI doesn't ship with pre-built Assemblylines for syncing your Domino data to your AD data BUT it does ship with monitoring programs designed to spot changes in either Directory source
    - All you have to do is decide what action you want to take when a change occurs
    - At its simplest you can configure TDI to monitor Domino for changes and update the hierarchical name of a Domino user into an attribute in their matching AD record so you don't have to do that manually.

Isn’t Domino Already Doing Directory Integration?

- Active Directory plug-in
  - Client side administrator install
  - Allows person entries to be created in AD as they are created in Domino
- IBM / Lotus plans for directory integration
  - Still very much in the planning stage

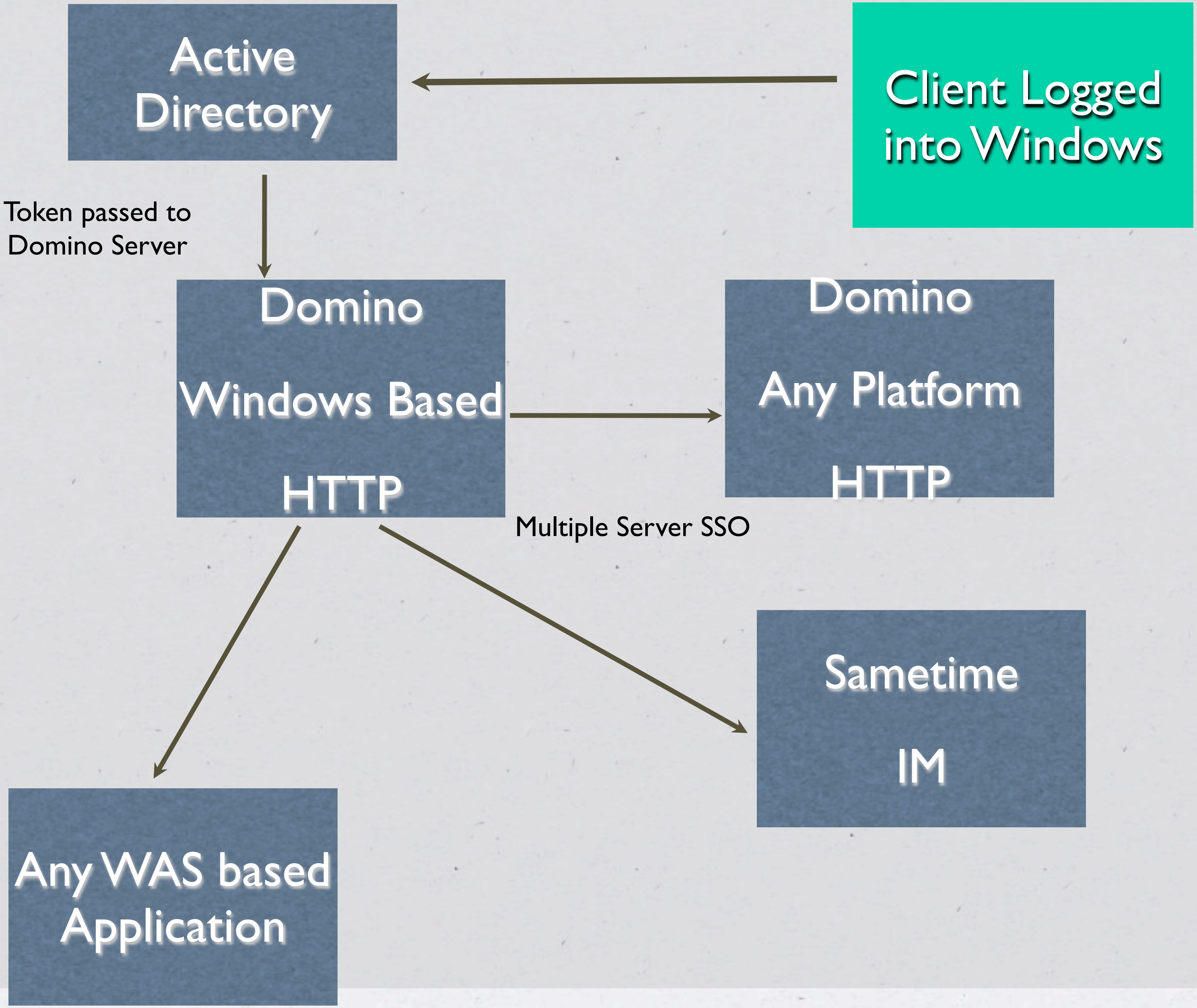
Notes Single Logon

- Notes Single Logon
    - Removal of password from the Notes ID which is then encrypted with a key generated by the user’s windows login and the machine name it appears on
        - Good for users who belong to a single machine
        - Not good for roaming users due to lack of security
        - Replaces Client Shared Login and requires that to be uninstalled from the client

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

SPNEGO



Active Directory

Client Logged into Windows

Token passed to Domino Server

Domino

Windows Based

HTTP

Domino

Any Platform

HTTP

Multiple Server SSO

Sametime

IM

Any WAS based Application

Summary

- SSO may be what you're asked to provide, but your existing server naming or configuration may make that impossible
- Dirlint
- Single password is often a good solution as it balances security with usability
- If you're going to have a single password then make it very secure
- If you use secondary directories in Domino, especially external LDAP directories, be aware you are exposing your Domino security to level of security applied on that external directory
- Set up DDM probes if you use external directories to monitor their performance and that of your DNS server, both become critical to Domino performance
- Configuring AD or any LDAP source to validate your users with their passwords is a simple, neat solution requiring no 3rd party plugins or tools
- SPNEGO is effective if all your users authenticate into Active Directory each day, but it's not usable by remote users who don't login to AD