



Lotusphere2011

IBM Software

BP108

Admin for the Developer -- Build and Secure Your Own IBM Lotus Domino Server Playground in One Hour!

Jess Stratton | IBM Lotus Domino Consultant, Solace





Who is this Jess person and why should we listen to her? Jess...

- Does Lotus® Domino® consulting, ongoing and project-based.
- Has worked with Lotus Notes®/Domino since R4.x, ~10 years.
- Speaks at The View's Admin and Developer conferences.
- Has written articles for Group Computing/E-Pro Magazine.
- Hosts the group blog at LotusUserGroup.org (blog with me!)
- Has submitted apps to OpenNTF.org.
- Co-hosts the 1352 Report podcast on industry news.
- **AND – I'm an administrator AND a developer!**

A great thing about developing and administrating together:

You can write agents to do all your Administration tasks!





The Problem:

- You're going independent and want to set up a server at home to work with...OR...
- You want to set up a developing playground at the office...
- BUT...
- All the servers you've ever developed for have been installed and are in place already!
- I guess you could just install the server software out of the box, but do you really want to put it live on a network like that?
 - Here's some great news though – ND8 > is REALLY secure out of the box.



The Solution, and the Expectation:

We're going to do a full walkthrough of a Lotus Domino server install and configuration.



- WHEN YOU LEAVE, YOU'LL BE ABLE TO:
 - Have a one-server Domino playground at your home or office and sleep easily knowing that it is secure and maintained, and independent of other servers.



- WHEN YOU LEAVE, YOU WON'T BE ABLE TO:
 - Regularly maintain and run a large, multi-server mail and web environment with clustering and thousands of users.



Agenda

- Install server software
- Launch/install setup file
- Configure the newly installed Lotus Domino server
- Start Domino
- Install and configure the Administrator client
- Secure and further tweak the Domino server
- Setup a firewall for external access to the Domino server
- Register our test subjects. I mean, er, users



Table of Contents

- Installing Lotus Domino
- Administrator Client setup
- Configuring Domino
- Configuring a firewall for external access
- Registering users
- Addendum: Playing safe with existing (production) servers



Installing Lotus Domino 8.5



Installing Domino 8.5...

PREREQUISITES

- Hardware/Software requirements
 - Where to Find: They are always in the Release Notes which can be found at developerWorks. Unless it's a beta, and then you can find the Release Notes with the rest of the beta download.
- Server/Client OS communication
 - Always test this FIRST.
 - Basic PING test is fine, but make sure they can TALK!
 - If using Virtual PC/VMware, do ping test between host and client.

```
C:\>ping 192.168.1.100

Pinging 192.168.1.100 with 32 bytes of data:

Reply from 192.168.1.100: bytes=32 time=3ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```





Installing Lotus Domino...

- **THE EASY PART:**
- Download from Passport Advantage, double-click!
- OK to accept Program Files directory name, or change. It's your call!
 - I always change it to “C:\Lotus\Domino”. I don't like something as important as a Domino server being buried in a file system.
- If you ever want to use as a partitioned server, just re-install server software and CHECK the box “install Domino Partitioned Servers”.
- The server setup type selection will depend on what license you have and what services will be installed by default.
 - Click “customize” to turn on services you will need, such as DECS.
 - *(though you can add them later, too.)*



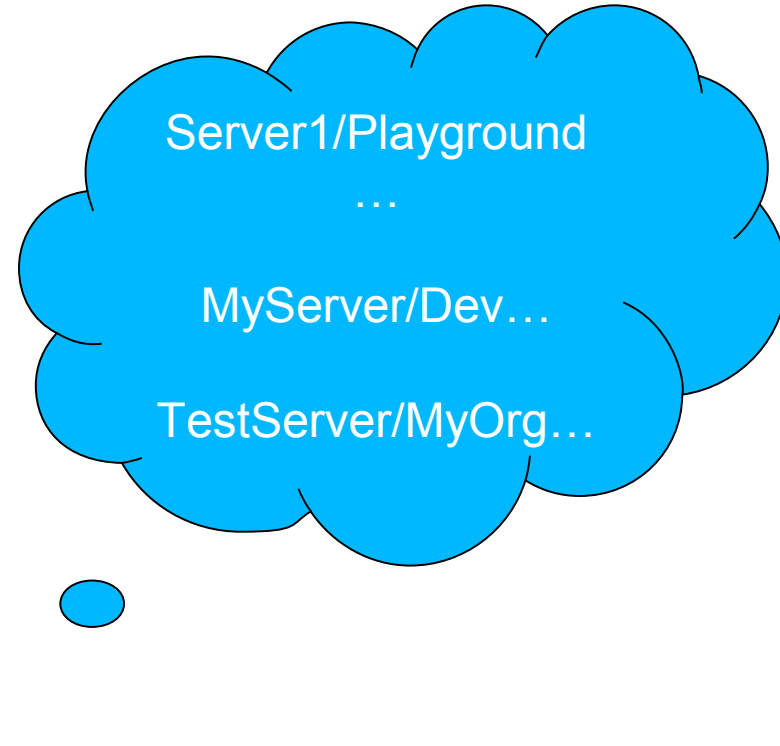
Lotus Domino as a service?

- If you install Domino as a service, don't forget!
 - You won't see the console on the desktop as it will be running in the background!
 - When you turn it on, you could have a fully-functional web or SMTP server that you may not know about.



Launch & Configure “Lotus Domino Server” Icon

- Things to decide in advance:
- **Server Name**
 - Server 1, Dev, Playground, Test, etc.
- **Organization Name**
 - /Dev, /Playground, /MyOrg, etc.
- **Domain Name**
 - @Playground, @MyDomain, etc.
- **Putting it together:**
 - Server1/Playground@Test, etc.





A note about Naming conventions...

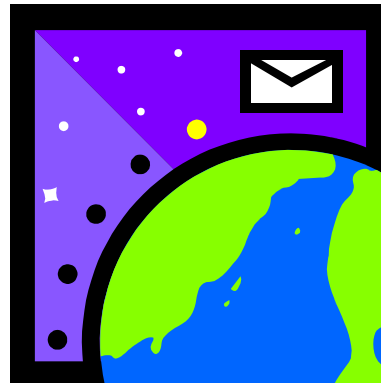
- A Lotus Domino domain is NOT an Internet domain.
 - No .com, .org, etc. necessary (though possible, it WILL obfuscate and make troubleshooting more difficult)
 - Can be the same as the Org name.
- If this is in addition to a production server already in place, do NOT use the same Organization or Domain!
 - All servers in the same Domino domain share key elements, such as the Domino Directory!
- This server should **clearly** be identified as a playground environment.





Configuring Lotus Domino for the first time

- This is a one-time setup dialog the first time you click the icon.
- Set up Lotus Domino as a first server.
 - Enter Server name, i.e.. Server1
 - Enter Organization name, i.e.. Playground
 - Enter Domain name, i.e.. MyDomain





Finalizing the initial config...

- CONGRATULATIONS!
- Your server is now identified as **Server1/Playground@MyDomain**
- Set up network ports and services you want to use, and click “Setup” when done.
- Domino will now create databases, and you’re ready to launch the server!





Start Lotus Domino!


- Double click the icon, and start 'er up!
- The first time Domino starts, it creates databases, starts services, and checks *stuff* like host names.
- It may take a few minutes, and log a few errors. Just let it start! For example, it may be trying to start services whose partner databases haven't been created yet.
- Once it's settled down (and the server stops sounding like a percolating coffee maker) type 'q' to bring down the server, and then start it up again.

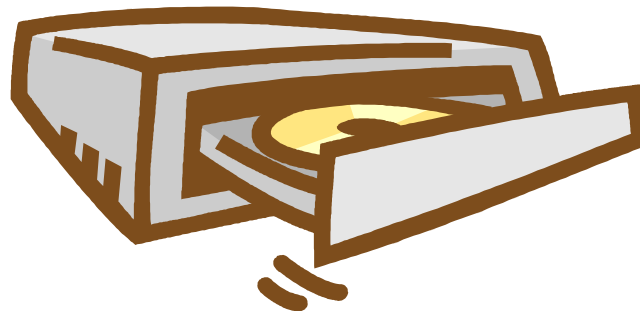


Lotus Domino Administrator Client Setup



Installing the Lotus Domino Administrator Client...

- The Easy Part – Download from Passport Advantage, install!
- Don't install this on the server. 
- During client setup, don't forget to install ALL the clients...
 - Notes, Designer, Administrator





Launch the Lotus Notes client FIRST.

- Set up the Lotus Notes client with your new ID file before launching the Administrator client.
- Put in the Administrator name you used and the Domino server name when you registered.
- If you forgot the server name, go back to the console of the server!
 - The title bar of the DOS window is the server name.
 - We won't tell anyone. Promise.





A note on client configuration...

- If you already have a Lotus Notes client on a machine you want to use, use Location/Connection documents for your Playground server.
- Configure your Location document to automatically switch to your Playground ID file.
- So never the twain shall meet – Configure the Connection document to only work for THAT ID file and location document.

SERVER CONNECTION: Tas192.168.1.100

Basics | Comments | **Advanced**

Advanced

Only from Location(s): Solace

Only for user: Jessica Stratton/Solace

Usage priority: Normal ▾



Configuring Lotus Domino

(using the Domino Administrator Client)



Securing Lotus Domino

- Launch that Administrator client!
- Verify your name is in the LocalDomainAdmins group.
 - People & Groups Tab --> Groups
- Verify you are using more secure Internet Passwords.
 - Actions-->Edit Directory Profile, make sure this field is on “Yes”.
- Verify ACL of Domino Directory (names.nsf).
 - File-->Application-->Access Control, Advanced tab.
 - Maximum Internet name and password should be 'Reader', unless you want to use Web Admin, and then it should be 'Editor'.



We begin with the Server document...

- Configuration tab->Server->All Server Documents



BASICS tab

- Routing Tasks
 - Mail Routing
 - Select SMTP routing if this is going to be an SMTP server.
- If creating an SMTP server, also enable the SMTP listener task.
 - Check the status anyway - shut it off if you aren't using SMTP.
- Enter the Fully Qualified Internet Host name if it's empty.
 - If unknown, you can put the server name or leave blank.
- Load Internet configurations from Server\Internet Sites documents
 - Enabled (We will make the site documents later!)



SECURITY tab – recommended settings

- Full Access Administrators:
 - Put your name explicitly in the field.
- Administrators:
 - LocalDomainAdmins
- Run unrestricted methods, Sign agents to run on behalf of someone else, Sign agents to run on behalf of invoker, Sign script libraries:
 - Put your name explicitly in the field, or the Xpages builder!





SECURITY tab - recommended settings

- Compare public keys:
 - Enforce key checking for all users
- Allow Anonymous Lotus Notes connections:
 - No! (It's the default anyway)
- Check passwords on Notes IDs:
 - Enabled.
- Access server:
 - Users listed in Trusted directories AND server name, AND LocalDomainServers
 - You can also just put in */YourCertifier, ie. */Playground.
- Don't forget – if you ever lock yourself out:
 - Administration-->Full Access Administration!



SECURITY tab recommended settings...

- Create databases & templates, Create new replicas, Create Master templates:
 - You'll make judgment calls here, just as long as your name is in there somehow. You are a developer! Use your name explicitly, or LocalDomainAdmins.
 - *NOTE: I have had trouble by not putting in LocalDomainServers before, so I do it out of habit now.*
- Allowed to use monitors:
 - LocalDomainAdmins



SECURITY tab – XPages additions in 8.5.1

- Sign or run unrestricted methods and operations
 - XPages builder should be listed here!
- See “Controlling agents and XPages that run on a server” in Domino Administrator 8.5.1 Help for detailed information.



Ports tab settings...

- Make sure the Net Address of your Lotus Notes Network is a reachable network name, i.e.. Computer name, host name, or IP address.
 - This is a common gotcha for mail agents not working!





Server Tasks tab settings...

- Domain Catalog tab->Domain Catalog:
 - Enabled. The Domain Catalog is mind-bogglingly useful.
- Remote Debug Manager->Allow remote debugging on this server:
 - Enabled. This IS a playground, right?



Internet Protocols tab settings...

- HTTP tab->Hostname(s):
 - Enter the hostname. If unknown, the server will use the computer's host name.
- Enable Logging To:
 - Log files: Enabled
 - Domlog.nsf: Enabled
- NOTE: You must create Domlog.nsf!
 - Create a new database called Domlog.nsf based off the “Domino Web Server Log” (domlog.ntf) template in the Advanced Templates list.
- Save and close the Server doc!
 - There are other settings you CAN tweak, but these are the settings you MUST tweak.





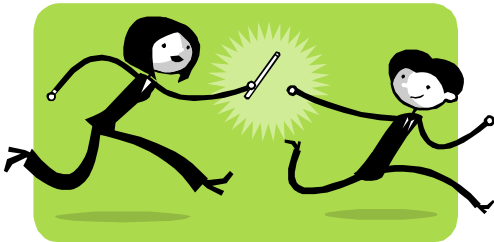
Edit the Configuration document...

- Configuration tab->Servers->Configurations->Edit Configuration



The Router/SMTP tabs

- If your playground is for a home server, and you have to send outbound SMTP through your ISP.
- Relay Host for messages leaving the local internet domain:
 - Add your outgoing SMTP mail server here.
 - *(The same that you use for your home ISP mail accounts)*
 - In Restrictions and Controls/SMTP Inbound Controls tab:
 - Remove * from ‘Deny messages to be sent to the following external internet domains’.
 - Add your Domino server IP address in “Allow messages only from the following internet hosts to be sent to external internet domains”.





MIME tab settings...

- Conversion Options tab, Inbound tab
- Field “Use character set auto-detection if message has no character set information.”
 - Set this to “Yes”. One little setting can solve so many potential problems!

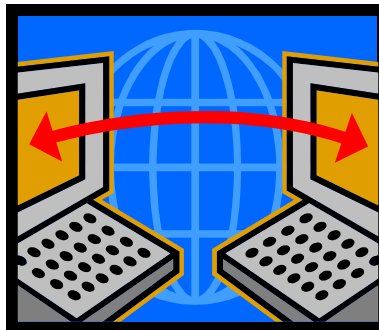


- Save & close the configuration document.
 - After making any other changes you like, of course. But these are what you NEED.
- Refresh the server with the new settings.
 - At the Domino console, type “tell router update config”.



Encrypting port traffic

- Server tab->Status->Ports (on the right!)->Setup
- Click “Encrypt network data” on all used ports:
 - TCPIP
 - LAN0tcpip
- This only needs to be done once, and one-way (you don't have to do it on any clients that connect to this server)!

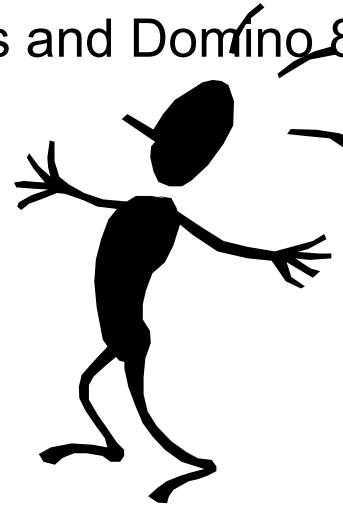




Lastly, we need to lock down some ACLs.

- Names.nsf
 - Set Default to 'no access'
 - Add Anonymous with 'no access'
 - Give LocalDomainAdmins all Roles, or check and make sure you are in explicitly.

- It must be said again! Lotus Notes and Domino 8.x > out of the box security is GREAT!





Create a Global Domain document

- Configuration tab->Messaging->Domains->Add Domain



BASICS tab

- Domain type: Global Domain
- Global domain name: “Demo”, or “Playground”.
 - This is also not to be confused with an *Internet* domain, ie. '.com'. It's “Playground”, not “Playground.com”.
 - This can be the same name as your Certifier and Lotus Domino domain.
- Global domain role: R5/R6/R7/R8 Internet Domains...



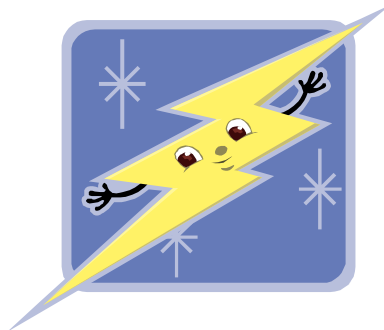
RESTRICTIONS and CONVERSIONS tab

- Lotus Domino domains and aliases: Enter your Domino domain here.
- Local primary Internet domain: Enter any Internet domains (ie. '.com' email addresses you are using with this Domino server).
- Save and close the document.



Performance Tweaks for Lotus Domino...

- The two major performance tweaks:
 1. Using program documents to schedule maintenance for top performance, AND
 2. Shutting off unnecessary server tasks.





Creating Program documents

- Configuration tab->Server->Programs
- Three program documents, scheduled to go off tiered (2AM, 3AM, 4AM, etc.):

1. Fixup (program name)



- -L (command line. This will log all processed files to log.nsf.)
- *Fixup isn't recommended nightly (or even at all unless there is a problem) for large organizations, but for a playground server I do it.*

2. Updall (program name)

3. Compact (program name)

- -s 10 B (command line. This will only compact those documents whose unused space is greater than 10%. The 'B' is case sensitive, and will use file size reduction.)



Other ways to schedule maintenance...

- Notes.ini
 - ServerTasksAt1
 - ServerTasksAt2, etc.
- Program documents are WAY easier!

```
DefaultMailTemplate=mail6.ntf
ServerTasks=Replica, Router, Update, AMgr, Adminp, sched, CalConn, HTTP
ServerTasksAt1=Catalog
ServerTasksAt2=UpdAll
ServerTasksAt5=Statlog
TCPDIP-TCP 0 15 0
```



Shut off those pesky unused server tasks...

- What's running, anyway? They're pesky if I'm not using them!
 - And, using up valuable CPU resources.
- Server tab->Status->Server Tasks
 - This gives you a complete list of everything running RIGHT NOW!
- Common tasks you may not need!
 - DOMWS Convert AddIn (new with R7 and needed if you are using Common Mail and Calendar portlets from Websphere Portal.)
 - HTTP (if not running web server)
 - SMTP (if not running SMTP server)
 - LDAP
 - IMAP
 - Design (if you don't want your templates updated automatically)



How do I disable them?

- Take them out of the ServerTasks lines in the Notes.ini file
 - Edit Notes.ini manually, or
 - Use Notes.ini params in the configuration file, or
 - Edit Notes.ini WHILE the server is running on the web with Webadmin.nsf!
- Some tasks can only be disabled by adding Notes.ini parameters.
 - If you only have one server, disable the Cluster replicator task for better performance:
 - DISABLE_CLUSTER_REPLICATOR=1
 - If you never plan on using LDAP:
 - DisableLDAPOnAdmin=1.



Identifying basic server tasks...

- The Administrator Help File contains a list of all server tasks in the section titled “Domino server tasks”.



Creating Internet Site Documents

- You can create Site documents for Web, POP3, LDAP, SMTP Inbound, and IIOP.
- In our case, we're setting one up for SMTP Inbound, and Web.
 - You can have multiple site documents for each web site the Domino server is hosting, but only ONE site document for each mail protocol (SMTP, POP3).
- To get to Sites:
- Configuration Tab->Web->Internet Sites
 - “Add Internet Site”
 - “Web”



SMTP Inbound Site

- **Add Internet Site-->SMTP Inbound**
- Give name and description.
- Organization should be your Certifier name.
- “Hostnames or addresses mapped to this site”:
 - This is the incoming DNS mapping that emails will use to get to the server.
 - If using a POP forwarder, such as PopWeasel, enter ‘localhost’ here.
 - If your emails already have an “MX” record, enter that IP address or hostname here.
- Save and Close.





Web Site configuration

- **Add Internet Site-->Web**
- Give name and description.
- “Hostnames or addresses mapped to this site”:
 - This is the incoming hostname or IP address that is used to get to the site.
 - If using SSL, this must be an IP address!
 - *(To set up SSL, see the Domino Administrator Help File, “Setting Up SSL on a Domino Server”.)*





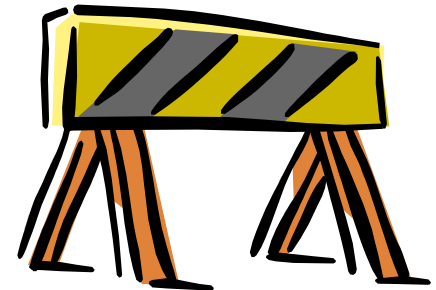
Configuration Tab (Web site)

- Home URL:
 - This is the default URL of the database to go to when the hostname or IP address you put in the previous field is entered into a browser.
 - Examples:
 - `portal.nsf/Welcome?OpenForm`
 - `Mail/mymailfile.nsf`



Lotus Domino Web Engine tab (Web Site)

- Session Authentication:
 - Single Server (enables cookies for a single server for logon use).
- Save and Close.
- A note about home office playgrounds and web servers...
 - Many ISPs block incoming port 80. You can change the default port from '80' to something like '8081':
 - Server document->Ports tab->Internet Ports tab->Web:
 - TCP/IP Port Number: Change 80 to 8081.
 - Issue console command "Tell http restart"





Customizing the Login Form:

- To customize the login form for Single Server authentication, create the Domino Web Configuration database.
 - File->database->New
 - Template server: Your playground server (show advanced templates)
 - Use template: Domino Web Server Configuration
 - Title the database “Domino Web Configuration”, with the filename “Domcfg.nsf”. (these aren’t negotiable 😊)
 - Make sure the ACL contains an entry for Anonymous with Reader access.
- To create your own custom form, Add ‘Sign-In Form Mapping’:
 - Change target database and form.
 - Or, simply modify the existing CustomLoginForm.

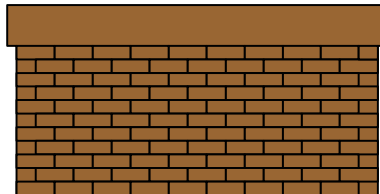


Configuring a Firewall for External Access



Prerequisites (things to have handy):

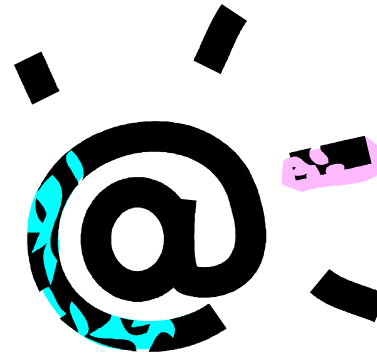
- The IP address of the Domino server.
- The Username and passwords to get into the Firewall or Router.
- The ports of the server tasks you have open.
 - Easiest way is to go to the Server Tasks view and in Activity, look at “Listen for connect requests on TCP Port:80”...
 - You don't have to do this if they aren't accessible outside your internal network.





Common Ports:

- POP3: 110
- SMTP: 25
- Notes Client: 1352
- HTTP: 80
- HTTPS (SSL): 443
- LDAP: 389
- Sametime: 1516





Enabling Port Forwarding on the Firewall

- Log into your router or firewall.
 - Web interface, commonly 192.168.1.1
- Look for “Port Range Forwarding” or “Port Forwarding”
 - Give your forwarders clear names, such as “DominoWeb”, “DominoSMTP”.
 - Set the Start and End range (they can be the same).
 - Set the IP address to the IP address of the Domino Server.
 - Do this for each port/service you need!



Registering Users



Lots of users – Use a text file!

- A text file can help you mass register lots of users at once.
 - In Administrator Help, See “Registering users from a text file”.
- For time restraints, we are not going to create mail files along with our test users.
 - It takes a lot longer to register users!
 - And, it will take up a lot of hard drive space too, if this is a home machine.
 - You can always create one and link it later to a person doc!
- Remember, the Golden Rule of Geek Test Subjects:
 - The more obscure reference the test names, the cooler you will appear to your colleagues! 😊



Some good sources for test names:

- Comic book characters.
- Cancelled 80's TV shows.
- Hitchhiker's Guide characters.

Why? Because
cool names = cool playground =
people will think you're cool. 😊





Excel tips for quick “test subjects” ...

- Online D&D character name generator results can be cut and pasted into Excel columns.
 - Seriously!!
 - Create an Excel spreadsheet with two columns:
 - first name and last name.
- We will end up with a total of four columns.
 - First name, last name, password, and ID file name.
- To concatenate first letter of first name and last name in a column:
 - Use the cell formula `=LEFT(A1,1)&B1` in a new column.
 - Paste the values all the way down the entire column. Instant passwords!
 - Use `=LEFT(A1,1)&B1&1` to add ‘1’ if a number is required.
 - For the name of the ID file, use `=LEFT(A1,1)&B1&”.id”`



Creating the Text file, continued...

- Save your Excel file as .CSV
- Rename the extension to .TXT
- Open the text file (in Notepad).
- Find and replace all ',' with ';'.
• Our text file is complete!

The screenshot shows an Excel spreadsheet with the following data:

	A	B	C	D	E	F	G
1	Shushnai	llasiel			Sllasiel		Sllasiel.id
2	Chiddect	Indatrian			CIndatrian		CIndatrian.id
3	Yijichi	llcil			Yllcil		Yllcil.id
4	Shuddichi	Eriel			SEriel		SEriel.id
5	Benaja	Filyon			BFilyon		BFilyon.id
6	Chonakra	Quarmol			CQuarmol		CQuarmol.id
7	Yirkeni	Ealyon			YEalyon		YEalyon.id
8	Shujesh	llenon			Sllenon		Sllenon.id



Registering users...

- People & Groups tab->People->Register (toolbar on the right)
- Choose cert.id
- Click 'Advanced'
- Mail System field: Choose 'none'.
 - We will create mail files when needed.
- Create and choose your directory if necessary for storing ID files.
 - Local to the Lotus\Notes directory!
 - Choose the directory!
- Click 'Import Text File'
- Click "Register All"





Addendum: Playing safe with existing (production) servers



How Domino servers can be connected:

- On the same Domino Domain
 - This means they share ONE Domino Directory (names.nsf)
 - Connection documents are normally not needed here...
- On the same Notes Named Network
 - Connection documents aren't needed here, either.
- On the same Domino Domain, but different NNN
 - Connection documents must be in place!
- On different Domino Domains
 - The servers must be cross-certified, and connection documents must be in place.
 - For mail routing scenarios, Adjacent Domain documents are needed, too.

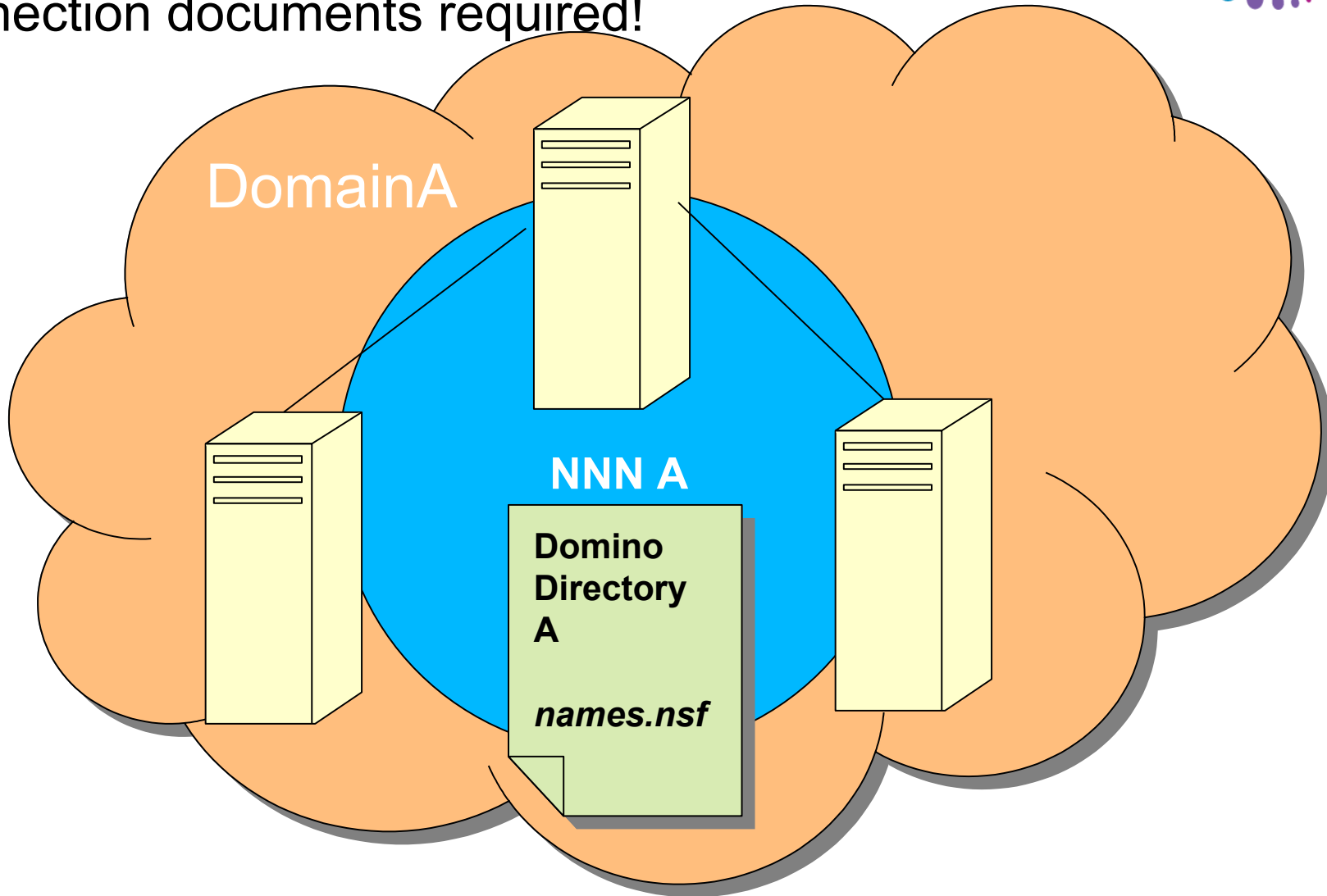


Domino servers in a domain share the following files:

- The Domino Directory:
 - Names.nsf
- The Administration Process
 - Admin4.nsf
- The Certification Log
 - Certlog.nsf
- All Domino servers in the same domain share these databases that gets replicated around to each server.
 - Most likely, these are exactly the databases you'll be modifying when you start "Playing".

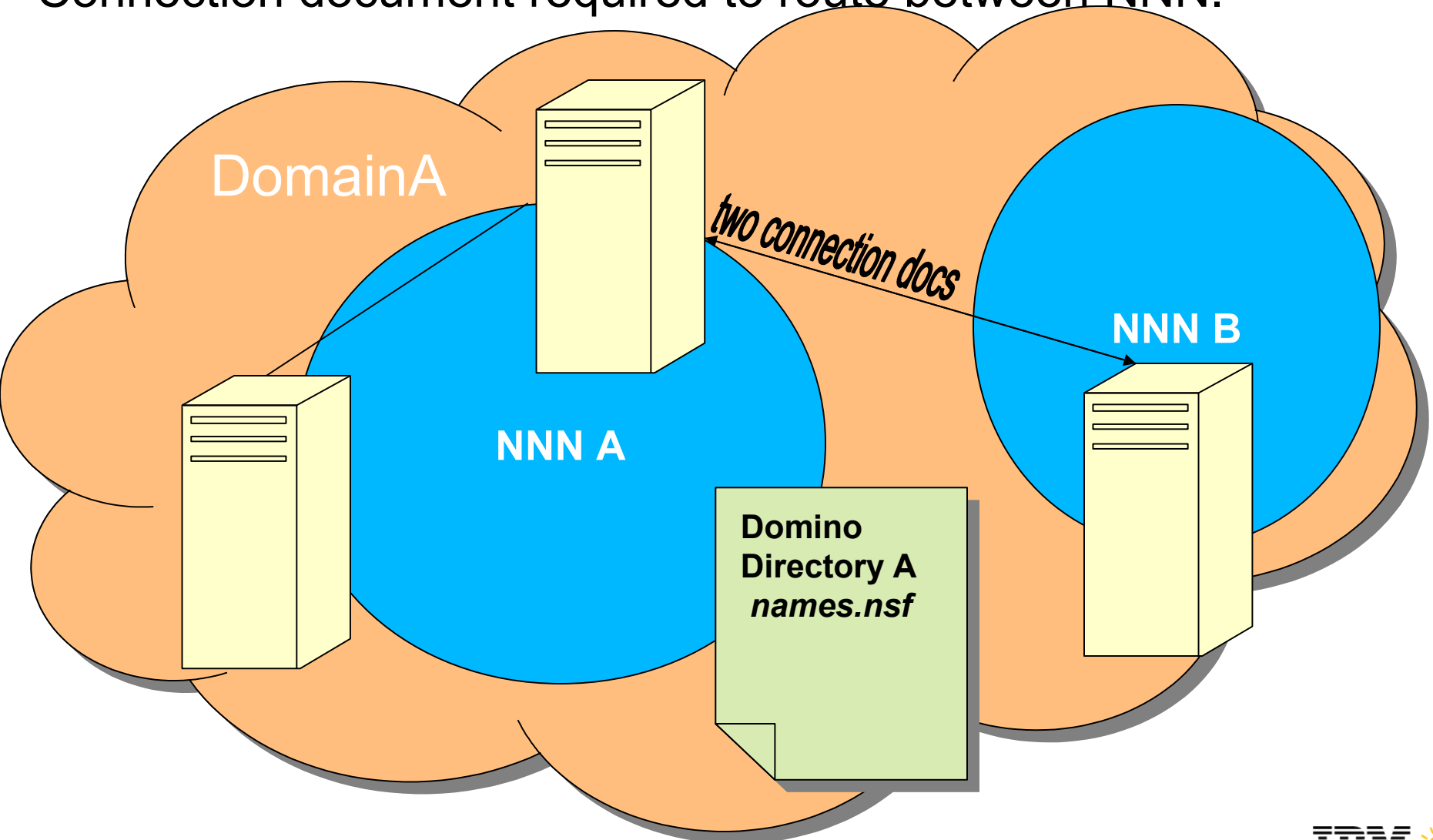


One domain, same NNN
No connection documents required!





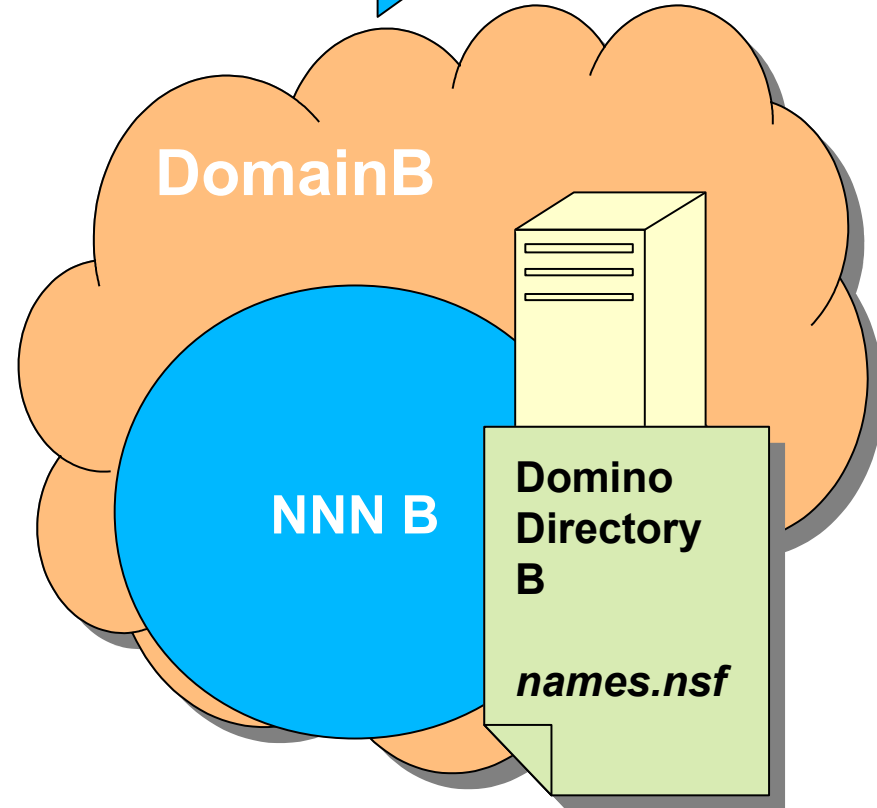
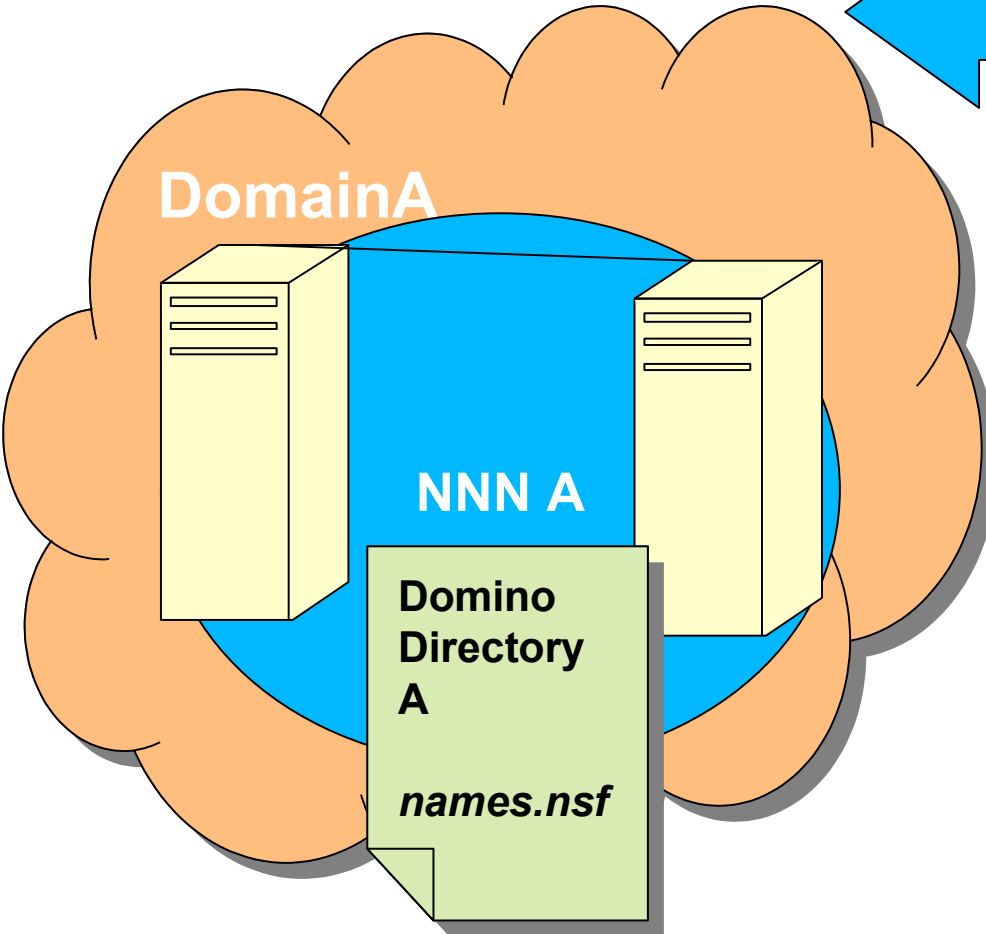
One domain, two Notes Networks:
Connection document required to route between NNN.





Two domains, two NNN.

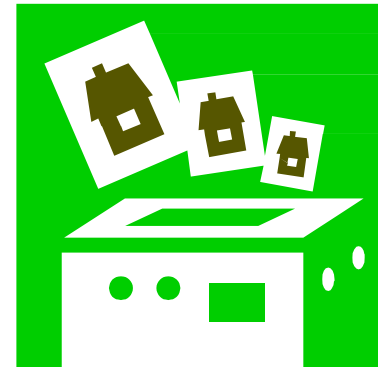
Cross-certification & connection docs required





How do I play safely with existing databases I want to change?

- Bring COPIES, *not* replicas over to your playground server of production databases you want to start playing with.
- Make sure your server is on a different:
 - Domain
 - Certifier
 - Notes Named Network





Contact me with questions! (good jokes always accepted graciously, too)

JESS STRATTON

SOLACE

EMAIL: jstratton@solacelearning.com

BLOG 1: www.mattandjess.net

BLOG 2: www.momelettes.com

Twitter: [@NerdGirlJess](https://twitter.com/NerdGirlJess)





Your turn!





Legal Disclaimer

© IBM Corporation 2011. All Rights Reserved.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.

IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

• All references to Solace refer to a fictitious company and are used for illustration purposes only.