

Stuff Andrew Thinks You Should Know

Performance, Security, and Single Sign-On... Mostly for Administrators, but developers should know this stuff too...



Before We Start

- English is the only (non-programming) language I know
- I will try to speak clearly, but if I am moving too quickly, or too slowly, please make some kind of sign, so I can adjust!
- Set All Phasers & Phones to Stun
 - We will all point at you
 - If you need to type on a laptop or iShiny move toward the back please

What's in this Presentation?

- Quick stability and crash resolution tips
- Quick Performance Tips
- Critical steps to better security
- A couple of quick How-To pages on SMTP Configuration and SSL Certificates
- A whole lot about SSO including SAML, OpenID, OAuth
 - But we're not going to talk specifically about Domino configuration
- A couple of useful tools you've never heard of

Who Am I?

- Andrew Pollack – President of NCT
- Administrator & Developer since version 2.0
- Products
 - NCT Search, NCT Compliance Search,
 - and NCT Simple Sign On, and Second Signal
- Services
 - Site Performance Reviews
 - Application Development
 - Administrative Overhaul
 - Security Review & Penetration Testing
- IBM Lotus Beacon Award Winner
- Structural Firefighter – Lieutenant of Engine Company 1 in Cumberland, Maine



Monie Sarkis

The background of the slide features a series of thin, vertical, slightly wavy lines in a light blue-grey color, set against a darker blue-grey gradient. A solid dark blue horizontal band spans the width of the slide, containing the title text. Below this band is a thin yellow horizontal line, and at the very bottom is a solid grey horizontal band.

Quick Stability & Crash Resolution Tips

First, Get Back To Good

- Completely Clean INI File
- Completely Clean Program Directory
 - No Fixpacks
 - No Debug Code
 - No Custom Libs or DLLs

Disable Other Server Programs

- Backup Software
 - Anti-Virus Software
 - FTP Server Software
 - Other Strange Things
-
- If it works, turn them on one at a time till it crashes again.

Disable Java Agents and XPages

- Poor Use of Recycle Kills Servers
- Errors Tend to Accumulate
 - Don't Show up in Test
- If this fixes things, re-enable and shut off agents one at a time

Disable Restricted LS Agents

- Restricted Access Required To
 - Load External Active-X, OLE, DDE
 - Access The File System
 - Load External DLL's or API Calls
 - Send Mail (less problematic for us)
- These Are All Things Which Can Cause Memory Issues or System Faults in some cases

The background of the slide features a series of thin, vertical, slightly wavy lines in a light blue-grey color against a darker grey background. A solid teal horizontal band spans the width of the slide, positioned below the patterned area. The text 'Quick Performance Tips' is centered within this teal band.

Quick Performance Tips

Disk I/O Tip #1 – Use More Disks

- Give These Things Their Own Disk If at all Possible
 - Transaction Logs
 - View Rebuild Temp Directories
 - DAOS File Store
- Note: A RAID Array only counts as one disk in this case!

Disk I/O Tip #2 – SERIOUSLY -- Use More Disks

- Give These Things Their Own Disk If at all Possible
 - Transaction Logs
 - View Rebuild Temp Directories
 - DAOS File Store
- Note: A RAID Array only counts as one disk in this case!

Disk I/O Tip #3 – Use Local Disks

- Local Disks Are Faster Than Your SAN
 - Don't argue with me. They are. Really.
 - SAN is probably OK for DAOS data
 - If it's a really good SAN
- Use cheaper SATA drives for low-risk data
 - Swap Memory
 - View Rebuild Temp Directory
 - OS Temp Directory
 - Web Server Cache?

Index Tip 1: @AllDescendants

- @IsResponseDoc includes ALL responses even if not visible in the view.
- Test DB with 30,000 Docs and 4 views
 - #1: No Responses w/ @IsResponseDoc
 - #2: No Responses w/ @AllDescendants
 - #3: 30k Responses w/ @IsResponseDoc
 - #4: 30k Responses w/ @AllDescendants

What's The Result?

- View #2 is 153 Times the Size of #1
 - And has the EXACT same content

Manage the views of this database

Use this tool to manage the views of this database.

Selected: Test View Index Count.nsf, 4 MB bytes

The view indexes of this database consume 17 MB of disk space, which is 410% of the entire space used by this database.

View name	Size	Owner	Refresh	Discard	NoteID
Test 1 Using AllDescendants	42,192	Andrew Pollack/thenorth	Automatic	If inactive for 45 da	0x16A
Test 1 Using Responses	6,055,892	Andrew Pollack/thenorth	Automatic	If inactive for 45 da	0x186
Test 2 Using AllDescendants	6,138,836	Andrew Pollack/thenorth	Automatic	If inactive for 45 da	0x18A
Test 2 Using Responses	6,055,892	Andrew Pollack/thenorth	Automatic	If inactive for 45 da	0x18E

Purge

Index Tip 2: Limit Sorted Columns

- Each Additional Sorted Column Can DOUBLE the size of the view index
- 5 Sorted Columns?
 - In our 30k Doc Example, Our 6mb View could become:
 - $6\text{mb} * 2 * 2 * 2 * 2 == 96\text{ mb}$

Index Tip 3: Hardcode Date Limits

- `Select Form="Request" & @Modified > [1/1/2005]`
- Yes, hard coding is bad most of the time
 - You can update this by agent monthly
 - Use a DB Script to notify if not updated
- DO NOT use `@Adjust(@Now;.....)`

Some very useful view indexing stats

- `Update.DeferredList`
 - Number of requests for view updating or full text indexing on the deferred queue
- `Update.DeferredList.Duplicates`
 - Number of requests for view updating or full text indexing avoided because they were already waiting on the deferred queue
- `Update.DeferredList.Max`
 - Maximum number of requests waiting for view updating or full text indexing on the deferred queue
- `Update.DeferredList.Processed.AllViews`
 - Number of all view updates processed from the deferred queue
- `Update.DeferredList.Processed.SingleViews`
 - Number of single view updates processed from the deferred queue
- `Update.FullTextList`
 - Number of requests on the full text index queue
- `Update.FullTextList.Duplicates`
 - Number of requests for full text indexing avoided because they were waiting on the full text index queue
- `Update.FullTextList.Max`
 - Maximum number of requests waiting for full text indexing
- `Update.FullTextList.Processed`
 - Number of full text indexing requests processed
- `Update.NAB.Updates`
 - Number of Domino Directory view updates processed
- `Update.PendingList`
 - Number of requests for view updating or full text indexing on the immediate queue
- `Update.PendingList.Max`
 - Maximum number of requests waiting for view updating or full text indexing on the immediate queue
- `Update.PendingList.Processed.AllViews`
 - Number of all view updates processed from the immediate queue

Some NOTES.INI tweaks

- COMMENT NOTES.INI Changes!
- Here's some that I use
 - MailLeaveSessionsOpen=1
 - For busy mail servers, can speed up delivery
 - Update_Fulltext_Thread=1
 - Move full text indexing to its own thread, distinct from the indexer – This is the closest to “runfaster” I have found
 - Ftg_use_sys_memory=1
 - Use memory outside the Domino server
 - HttpQueueMethod=2
 - According to Kerr, this is a must have for busy web servers
- Use These Together:
 - SERVER_NAME_LOOKUP_NO_UPDATE=1
 - Tells the server to use the old index while the new one catches up
 - DEBUG_ENABLE_UPDATE_FIX=8191
 - Fine tunes when the directory indexes get refreshed

Some hard core indexer control options

- **UPDATE_NOTE_MINIMUM**
 - Proactively update views when the number of notes that have been updated has reached this threshold.
 - Increasing this MAY reduce the view indexer load – there are pros and cons, so consider carefully.
- **UPDATE_IDLE_TIME**
 - Decreasing lets the view indexers have more processor time
 - Increasing may improve server response but delay view updates
 - Default is 5 Seconds
- **UPDATE_IDLE_TIME_MS**
 - The same as “Update_Idle_time” but in Milliseconds

And of course... NSF_Buffer_Pool_Size_MB

- NSF_Buffer_Pool_Size_MB=
 - Very powerful, but very complex
 - Check the Lotus Notes Knowledge base
 - Starts at around 300
- Not as critical as it used to be
 - Documentation Says it is now set AUTOMATICALLY for non-partitioned Servers
 - My Testing Says it is also now set AUTOMATICALLY even for partitioned Servers in 8.5.x
- Check your success with this console command
 - `show stat database.database.b*`
- Don't check too soon after a change, its only valid over time

Notes 8 Client Tweak

- Edit the file: `jvm.properties`

- Located in the directory:

`{Notes}\framework\rcp\deploy\com.ibm.rcp.i2se.{Version}`

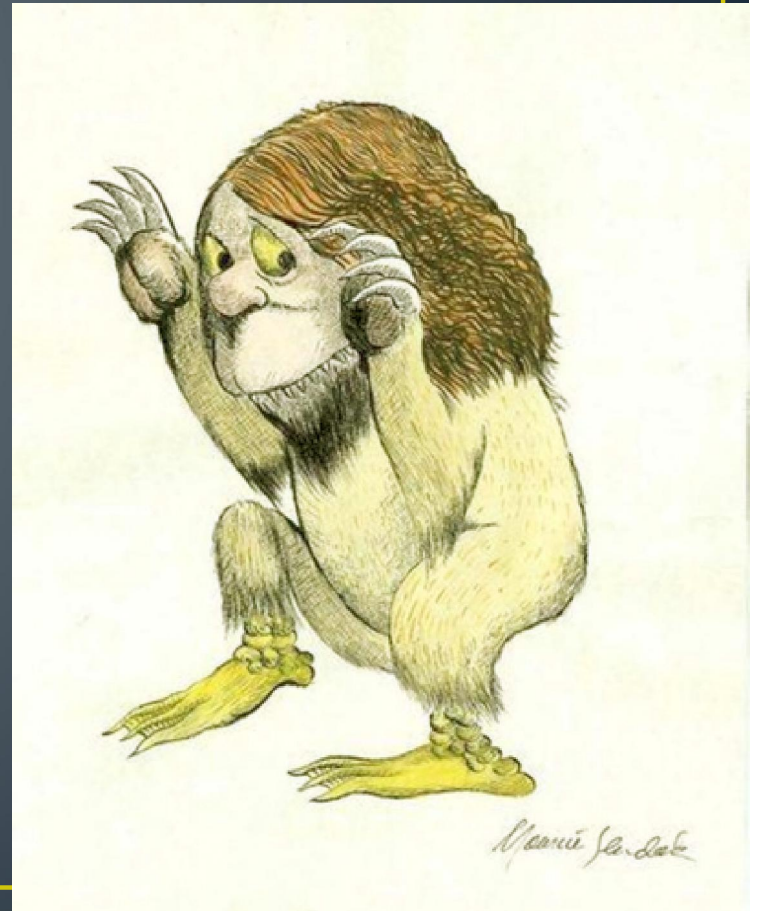
- Change the line: `vmarg.Xmx=-Xmx256m`
- So that it reads: `vmarg.Xmx=-Xmx512m`
- Note: You can set it higher, but aim for about half of your available RAM
- Readers on my blog overwhelmingly report fantastic results with this one

The background of the slide features a series of thin, vertical, slightly wavy lines in a light blue-grey color against a darker grey background. A solid teal horizontal band spans the width of the slide, positioned below the patterned area. The title text is centered within this band.

First Steps to Better Security

Where The Wild Things Are

- Most Security Problems Are Internal
- Administrators are Frequently Accused
 - Good Policies & Procedures
 - Protect You
- Outdated Data is Bad Data
- Developers ARE out to get you



First Things First

- UPDATE YOUR SERVERS AND YOUR OS
 - And keep up with updates and patches fairly quickly
- Work with your network team and firewall off what you don't need open
- Shut down services that aren't needed
- If you think you don't have to, talk to anyone who has been in Paul Mooney's "Ethical Hacker" day class.
 - Or better yet, go take that class as soon as you can.

Control Your Certifiers & ID Files

- Use the CA Process
- NO MORE ID FILE NETWORK SHARES
- Move to ID Vault
- Update Certificates

Control HTTP Password Fields

- Don't Use Them? Yes, You Do!
 - Many contain the original default password
- Used by *MANY* tasks on the server
 - And by Java agents or external apps
- Spammers Routinely Dictionary Test This
 - Because we don't read the SMTP logs

Get Serious About ECLs

- Use Code Signing IDs
- DIFFERENT Code Signing IDs for Agents
- Use SPECIFIC Code Signing IDs for Critical Applications

Protect Your Administrators

- Log and report EVERY use of “Full Access Administrator”
 - Using DDM to capture the event from the console
 - Immediately send a report of the occurrence to an operations center or other such resource which is not on the same server
- Do not let Administrator ID files be the same as user ID files even for administrators. Make them switch.
 - No access to administrator mail files while using your admin id unless you go into full access admin mode
- Administrators are frequently accused of reading users' mail files. This is the only way to protect yourself from that accusation

Understand What's On The Server

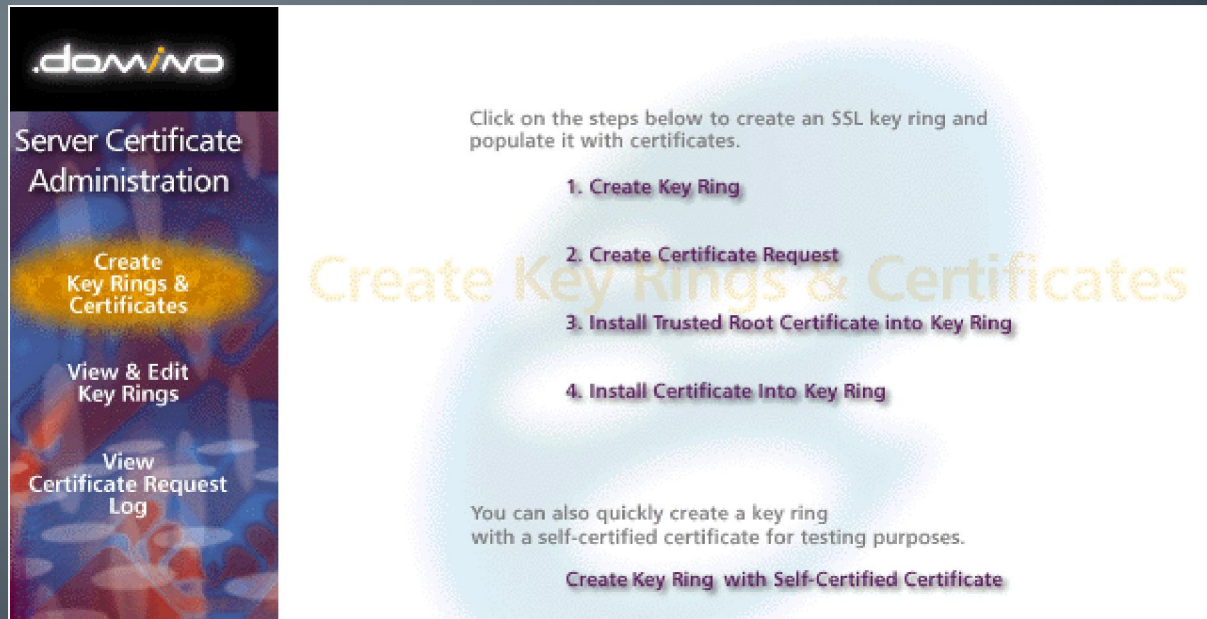
- For Every Database (EVERY)
 - Who Owns It
 - Who Supports It
 - Do you have a contact number?
 - Privacy / Security Rating
 - You don't have a rating scale?
- Review This Data Every 6 Months

Understand Your Group Hierarchy

- Do users have access to more than you think?
- Do you remove users from groups when they change jobs?
- Consider using a database to track “group” ownership
 - Make group owners acknowledge that they’ve reviewed the group every six months (at most), indicating that the group is still needed, and it’s membership is still accurate.

Creating an SSL Certificate

<http://bit.ly/10rgnGd>



.domivo

Server Certificate Administration

- Create Key Rings & Certificates
- View & Edit Key Rings
- View Certificate Request Log

Click on the steps below to create an SSL key ring and populate it with certificates.

1. Create Key Ring
2. Create Certificate Request
3. Install Trusted Root Certificate into Key Ring
4. Install Certificate Into Key Ring

You can also quickly create a key ring with a self-certified certificate for testing purposes.

Create Key Ring with Self-Certified Certificate

Multiple SSL Certs on One Server

- Yes! It Can Be Done
- EVERY Web Site Definition *MUST* be bound to a **UNIQUE IP** address -- NOT bound to DNS Name
- That's all it takes

SMTP Routing in a Nutshell

- Server Documents except the server that will route smtp
 - Set "SMTP Listener" to Disabled
 - Set "Routing Tasks" to "Mail Routing" – but not "SMTP Mail Routing"
- Create a "Foreign SMTP Domain" Domain Document
 - Route *.* to "OurFakeName"
- Create a Connection Document
 - Type: SMTP
 - Source Server: The domino server with smtp
 - Destination Server: MAKE UP a name
 - Destination Domain: "OurFakeName"
 - Routing Task: SMTP Mail Routing

The background of the slide is a dark blue-grey color with a pattern of thin, vertical, light blue-grey lines of varying thicknesses, creating a textured, rain-like effect.

Single Sign On & Shared Authentication

SSO & Shared Authentication Topics

- What's the difference?
- Specific Security Concerns
- Creating your own simple specification
- Emerging Standards
 - SAML (Security Assertion Markup Language)
 - OpenID
 - OAuth
- A Real World Example

What's the Difference?

Single Sign On

- Enter Credentials Once and you are signed in at multiple sites
- Wikipedia lists dozens of projects
 - <http://bit.ly/WRaxPq>

Shared Authentication

- May need to re-enter the same credentials at each site
- LDAP
- Domino HTTP Password Sync with Notes ID

Specific Security Concerns

- Authentication is not Authorization
 - Who you are does not tell us what you can do
- How much do you trust the credential provider?
 - Their security weaknesses are now yours
 - Can you protect your administrative logins?
- Can cookies or URL parameters be captured and re-used, or even altered?
- Can a session be universally revoked by the credential provider?

Opportunities to add some control

- Consider putting all SSO logins in a specific “organization” or “Organizational Unit”
 - Prevents the credentials from using your admin accounts
 - “SSOName/SSO” or “SSOName/SSO/MyOrg”
- Make full use of the “Maximum Internet Name and Password” ACL setting

Creating Your Own – What You Need

- **Minimum Requirements**
 - A way to know that the credentials came from the provider and were not counterfeited
 - A way to know when the credentials were last authorized by the provider
- **Additional Requirements**
 - User meta data
 - Authorization Criteria

Example of Custom SSO Specification

- URL Parameter “PACKET”
 - Packet is encrypted with a standard encryption method (e.g. blowfish) or signed using x.509
 - Packet contains userid and timestamp

OpenID Overview

- Useful for low security public facing sites like blog comments and discussion boards
- Because OpenID is so open, the level of trust you can place in credentials is very limited.
- Many well known OpenID providers
 - Google, Yahoo! LiVE JOURNAL, Blogger, Aol
- You can create your own provider
 - But not all sites that accept OpenID will use it
 - Many sites just use specific buttons to authenticate using known OpenID providers
- Not directly supported by the Domino Web Server
 - But it can be done
- For more: <http://openid.net/>

OAuth Overview

- Complementary to OpenID
- OpenID provides Authentication while OAuth provides for Authorization
- OAuth works like a “valet key”, authorizing third party applications to do things under your credentials on a site.
- Major split between version 1 and version 2
 - Original author no longer involved
 - Version 2 implementations “unlikely to be compatible” with each other.

OAuth Terminology

- Resource Owner: Who's Content Is it?
- Client: Who wants to access the content?
- Server: Where does the content live?

OAuth Credential Types

- Client Credentials
 - Typically the user's server login
- Temporary Credentials
 - May be used to track the authorization request between the client and the server
- Token Credentials
 - Issued by the server to the client as a stand-in for the client credentials without giving those away
 - Can usually be revoked at the server by the resource owner (e.g. Remove this application's authorization)

OAuth Request Types

- Two Legged Request
 - Where the Client and the Resource Owner are the same
- Three Legged Request
 - Where the Client is a third party (like an app) acting with authorization from the Resource Owner
- N-Legged Request
 - Used when “re-delegation” is allowed (works like a three legged request)

OAuth Use Cases

- Third party web site apps
 - E.g. Facebook Games
- RSS Feed Aggregators
- Third Party Client Software
 - E.g. Twitter Applications
- Notes 9
 - Integration with Connections

SAML Terminology

- Security Assertion Markup Language
- IdP – Identity Provider
- SP – Service Provider
- Assertion – What the IdP tells the SP

SAML Overview

- SAML is a very rich and detailed spec which provides for passing identity along with meta data between an Identity Provider and one or more Service Providers
- Data is passed in XML packages
 - Generally using http protocols, but not necessary always. The XML can be passed almost any way.
- Packaged XML can be signed, encrypted, both, or neither
- Communication can be made directly between the SP and the IdP or the XML packages can be passed by the requesting client.

SAML Benefits/Use Cases

- A single trusted, authoritative source is used to authenticate users who then need access to resources on multiple servers – often outside the control sphere of the authoritative source.
- Allows third parties to provide services to your user community, while management of that community remains centralized.
- Highly flexible security and meta data capabilities allow a wide range of interoperability

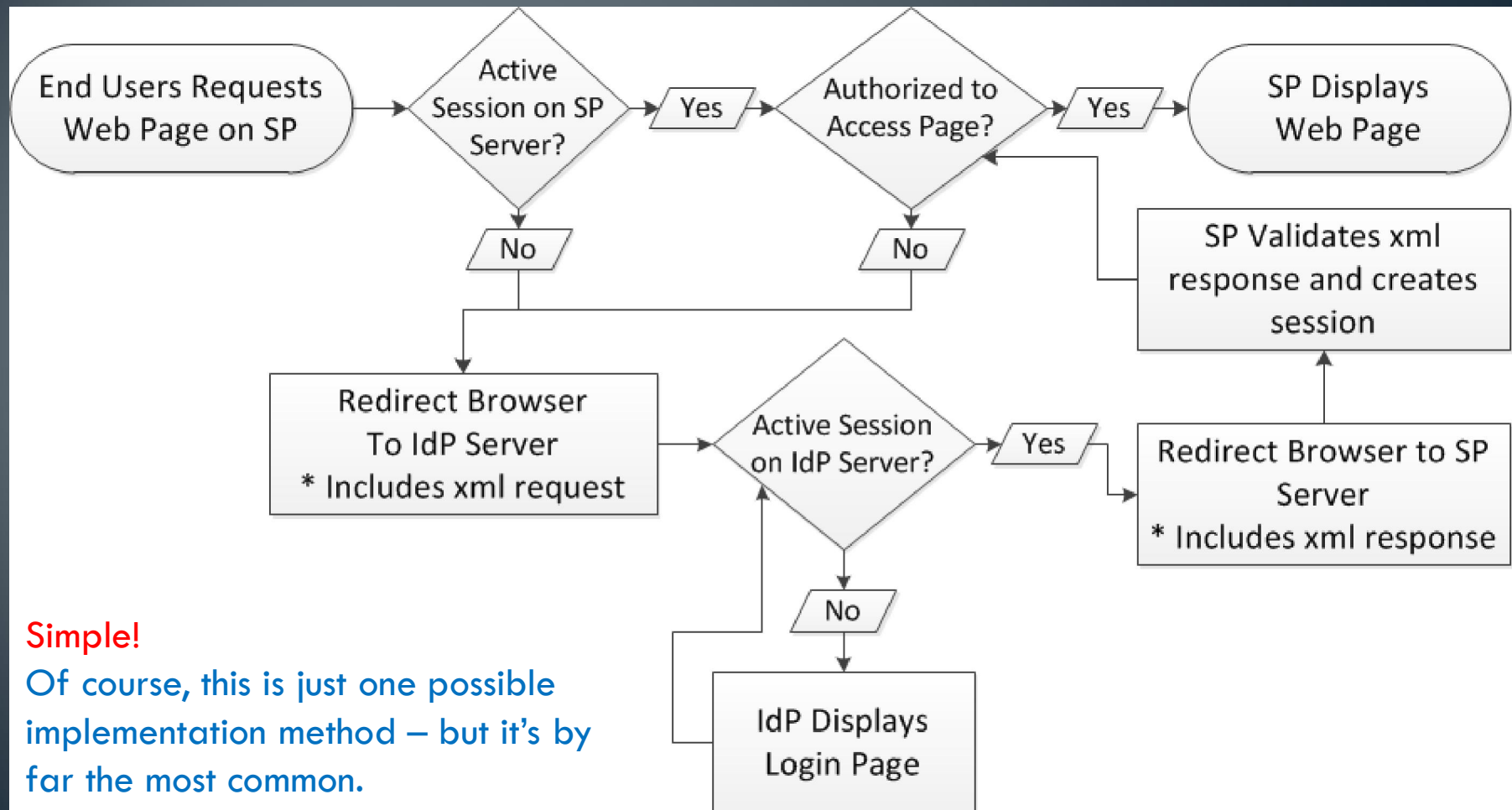
SAML Setup

- The IdP and the SP MUST establish a trust relationship for exchanging credentials and keys outside this process – typically by exchanging official x509 certificates to be used for signature validation and decryption
 - Public keys are commonly also transferred inside the xml transactions, however these cannot be trusted unless the SP and IdP servers are in direct, verified, secure communication
- The IdP provides set up information in the form of an IdP.xml file
 - Contains the resource locations, Identifiers, requirements and defined services for all future transactions between the IdP and the SP
- The SP imports that data and responds with an SP.XML file
 - Contains the SP identifier, resource locations, and defined services for this service provider

The Assertion is The Heart of SAML

- The IdP “Asserts” specific information to the SP
 - The UserID and other metadata attributes
 - The format of the userid and each attribute
 - The timespan in which the assertion is valid
 - Other conditions placed on this use of this info
 - Audience Restriction, One Time Use, Proxy Use, etc.
 - Assertions are usually signed and may be encrypted as well

Typical SAML Process Flow



Simple!

Of course, this is just one possible implementation method – but it's by far the most common.

SAML in Domino 9

- Still In Beta Cycle as of this presentation's creation date
 - Released now but I haven't done a set up with it
- Acts as an SP only, not an IdP
- Currently only supports two IdP Products
 - Microsoft Active Directory
 - Tivoli Federated Identity Manager
- There are reports of it working with others
 - Most common IdP I've seen is Oracle Federated Identity (add on to Oracle Identity Manager)
- Requires a Notes ID and Person Document for all federated Notes Client users but not necessarily browser access users
- Requires the use of ID Vault if used for Notes Client federated login

The background features a complex pattern of thin, vertical, slightly wavy lines in various shades of blue and grey. These lines are set against a light grey background. A solid dark blue horizontal band spans the width of the image, containing the text. Below this band is a thin yellow horizontal line, followed by a solid grey horizontal band at the bottom.

Add On Tools

Xlight FTP Server

- SFTP & FTP
- LDAP Authentication Can Authenticate with Domino
- Individual Or Group Based “Home” Directories
- Event Notifications Trigger Domino Agents

EchoVNC

- Remote VNC Through Most Firewalls
- Partly Open Source
- Very Inexpensive
- Great for End User Support

Game Over

Thank you for playing
Insert .25 to Continue

Contact me:

andrewp@thenorth.com

@FireFighterGeek

<http://www.thenorth.com>