OPENNTF WEBINARS

Domino Security - not knowing is not an option

OpenNTF Webinar, March 2024

Darren Duke
Janitor Level 34
STS
Thanks to….

• OpenNTF
  • Bruce and Nathan, all those years ago
  • All the past and present board members, all the contributors, and the users, lurkers, posters
  • Roberto and Kim for inviting me present

• HCL
  • For giving Notes/Domino the development backing so sorely lacking in the latter years of IBM
  • For the most part, I have nothing but great things to say about what HCL development has done since the acquisition

• Lisa
  • She’s now a published author (and didn’t even force me to add this!)
• AKA my favorite slide
• Started with “Lotus Notes” in R3
• Yes, really….R3
• That means 1996
• Yes, really….1996
• Yes, I do still think I look like this picture →
• No, I don’t. But I still think I do
• Co-founder of STS in 2005
• Sometime blogger, ranting ex-Tweeter (or now ex-Xer?), ex-co-host of This Week In Lotus, Speaker
• [http://blog.darrenduke.net](http://blog.darrenduke.net)
• Twitter/X [@darrenduke](https://twitter.com/darrenduke) (for utter silence these days)
10,000 feet view

- What we’ll (hopefully) cover (in no particular order…sorry about that)
  - Server Security
  - User Security
  - Web
SERVER SECURITY
All security starts with Backup and Restore

• Native VSS Support in Windows
  • Added in 12.0.2
  • If your backup solution supports VSS, it now supports Domino on Windows
  • See https://blog.darrenduke.net/darren/ddbz.nsf/dx/domino-12.0.2-adds-vss-backup-support.htm
  • Also supports Veeam restores (a tad complicated though)

• Native Backup and Restore in Domino!!!!
  • Supports to-file-system, Veeam and S3 repositories as is
  • Added as server tasks, cross platform support
  • Opensource
  • See https://opensource.hcltechsw.com/domino-backup/
  • Intended as “middleware”
Security is also patching and updating

- **9.0.x and 10.x go end of support, June 1\(^{st}\), 2024**
  - If you are running those versions, you will be insecure on June 2\(^{nd}\)
    - Well, maybe not on June 2\(^{nd}\), but at some point you will be
  - Also Xwork EOS
  - Also LEI 9.0.x EOS

- 3 months from the date of this webinar

- 11.x and higher have no EOS date at time of writing

Speaking of patching - Fix Packs

• As a general rule, the higher the Domino version number, the more secure your server or client will be
  • And Traveler, and Nomad, and Leap….and…and

• Further to this rule, the higher the FP and the higher the IF, the more secure your server or client will be

• There is a new download site
  • I mean, who knew we’d all think FixCentral was actually not that bad?
    • Well, FlexNet made us long for FixCentral.
    • FlexNet
      • Truly. Abysmally. Awful. Beyond words
  • If you have a favorite deity, give it thanks, because…
  • New download site is https://my.hcltechsw.com/downloads
Server Security SSL/TLS/SHA2

• SSLv3 is dead (SSLv2 has been dead for a long time)
  • Unless you need it for some ancient SMTP STARTTLS compatibility
  • SSLv3 disabled by default since 9.0.1 FP9

• TLS is King, long live the King
  • TLS 1.2 is now the default
    • TLS 1.0 disabled by default in 12.0+, Domino never had TLS 1.1 support
  • Still no TLS 1.3 support in Domino
    • So sad, sad face goes here

• Here’s to hoping HCL don’t make the same mistake as IBM did with Poodle
  • They waited and waited on adding TLS support to Domino….then one day this happened:
Don’t forget Perfect Forward Secrecy

- In cryptography, **forward secrecy** (FS; also known as **perfect forward secrecy**, or PFS) is a property of key-agreement protocols ensuring that a session key derived from a set of long-term keys cannot be compromised if one of the long-term keys is compromised in the future. (via wikipedia)

- Domino supports FPS since 9.0.1 FP3 IF2/3
  - The data is secure even if the server private key is compromised in the future
  - This is a good thing. Use it
Server Security SSL/TLS/SHA2

• **SMTP with STARTTLS**
  • Rarely needed these days, but some problems fixed with….
  • Server notes.ini SSL_ENABLE_INSECURE_SSLV2_HELLO=1

• **Ciphers**
  • Domino server now dictates the preferred cipher list
  • No need to override with SSLCipherSpec notes.ini unless you really need to
  • Updated frequently, but you still must manually disable deprecated ones
    • Especially after server and/or NAB upgrade:
Speaking of STARTTLS and email…

• Your SMTP task should always be using STARTTLS
  • STARTTLS is encryption *only*
  • There is no in-built mechanism to verify the authenticity of the TLS certificate
  • Any TLS certificate is trusted when using STARTTLS
    • Even self signed
• Inbound and outbound configured in different places!
Email continued....DKIM

• **DomainKeys Identified Mail (DKIM)**
  • Tell the recipient server that the sender is cryptographically verified
    • Uses DNS and PKI
  • Outbound support added in 12.0.1
  • Inbound support added in 12.0.2

• DKIM, DMARC and SPF provide the basis of modern SMTP sender verification
  • Still not a perfect solution, but that’s not Domino’s fault

• Domino doesn’t support DMARC (yet?), so it can’t provide full protection for DKIM alignment rules.
  • Pile on to get it added:
Let’s Encrypt (LE) and CertMgr

• Added into Domino natively in 12.0
• LE does require port 80 open
  • May fail security audits
• New task and NSF added in 12, certmgr
  • Certmgr stands for….never mind, you found this webinar, you’re smarter than most
  • Automate requesting and renewing from certain trusted Internet CA’s
    • Very good if you are using one of the supported vendors.
    • Even without a supported CA, it is easier than kyrtool.exe
      • But 20 years to life in prison is easier than kyrtool.exe
• For versions prior to 12 there is LE4D from Midpoints
  • https://www.midpoints.de/de-solutions-LE4D
• You can still use kyrtool, and Gab Davis still has the most useful post for this
  • https://turtleblog.info/2015/06/22/creating-sha-2-4096-ssl-certificates-for-domino/
Reverse Proxies

•What is a Reverse Proxy?
  •In computer networks, a reverse proxy is a type of proxy server that retrieves resources on behalf of a client from one or more servers. These resources are then returned to the client as though they originated from the proxy server itself - Wikipedia
Reverse Proxies

• **Benefits**
  • You can handle more than one web server per proxy
    • Reduce (potential attack) surface area
  SSL offloading
    • Have the reverse proxy handle all your SSL/TLS
    • When security issue detected, one place to fix
    • Can use self-signed/internal CA certs on inside
  • **Security**
    • Hide version/platform/application from the browser
    • No direct access to backend servers
    • Restrict URL access to Domino for only required URLs for
      • iNotes/Verse/Nomad
      • Traveler
      • Domino web applications
• **Load balancing**
  • Provide HA for iNotes, Traveler, etc
Reverse Proxies

• The Real Reason to use a Proxy

<table>
<thead>
<tr>
<th></th>
<th>Date Spec Released</th>
<th>Date Domino Added</th>
<th>Time taken by IBM/HCL</th>
</tr>
</thead>
<tbody>
<tr>
<td>TLS 1.0</td>
<td>1999</td>
<td>2014</td>
<td>15</td>
</tr>
<tr>
<td>TLS 1.2</td>
<td>2008</td>
<td>2015</td>
<td>7</td>
</tr>
<tr>
<td>PFS</td>
<td>2011</td>
<td>2015</td>
<td>4</td>
</tr>
<tr>
<td>TLS 1.3</td>
<td>2018</td>
<td>Not - as of Mar 2024</td>
<td>6 and counting</td>
</tr>
</tbody>
</table>

• With a Proxy you may in the future avoid something like this:
Reverse Proxies

• The Proxies
  • NGINX (pronounced Engine X)
    • Most popular today, used by Netflix, Zappos, et al
    • Open source
    • Can do mail and other TCP connections, not just HTTP(S)
      • IMAP
      • SMTP (including STARTTLS)
  • Apache
    • Most famous
    • Open source
  • SafeLinx by HCL (nee LMC/IMC)
    • Used to be required for Nomad Web
    • Pretty complicated TBH
Reverse Proxies

• The Proxies
  • Anything else really, but usually big dollar:
    • BigIP F5
    • Citrix NetScaler
  • IBM HTTP Server
    • Keep away
    • No longer part of Domino install any more
BROWSER SECURITY
CORS – Cross Origin Resource Sharing

• The web is a dangerous place
  • Browsers add security to protect the user
  • Official CORS support in Domino added in 10.0.1 FP2
    • https://help.hcltechsw.com/domino/10.0.1/admin/conf_cors.html

• One of the easiest-to-digest examples
  • https://medium.com/@manrvaldez.92/what-is-cors-2330158ef227
  • https://lo-victoria.com/introduction-to-cross-origin-resource-sharing-cors
CSP – Content Security Policies

- Allows servers (via admins) to mitigate an array of attacks
  - Mainly XSS, but also packet sniffing
- Web Rules in Domino allow CSP headers to be added
- Browser side security, most have
  - Can verify here: https://content-security-policy.com/browser-test/

![Image of Web Site Rule interface]

- Description: HCL
- Type of rule: HTTP response headers
- HTTP response codes: 200, 206
- Expires header: Don’t add header, Add header only if application did not, Always add header (override application’s header)
- Custom headers: Content-security-policy, img-src ‘self’; date;
USER SECURITY
User Security

• There is a current security bulletin with certain internet passwords < 14.0

  • Details here
    https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0107585
  • CVSS v3.1 score of 5.2 (so “medium”)
  • If you are using “Add Person” (as opposed to “registering a user”) for server versions earlier than 14.0
    • New NAB templates
    • Update existing person docs
    • Protect new person docs
User Security

• **Strong Internet Passwords**
  • Changes how passwords are stored in the Domino Directory
    • A salted hash is created for each user
      • @Password has starts a hex digit ('0' - '9', 'A'-‘F’), with Domino 4.5
      • @Password2 hash starts with 'G', with Domino 4.6+
      • @Password3 hash starts with 'H', with Domino 8.5.1+
      • Obviously if you want ‘G’ or preferably ‘H’

• Go from this

![Enter Password](image1)

• To this

![Enter Password](image2)
User Security

- Strong Internet Passwords for new users
- Edit Domino Directory Profile
User Security

- **Strong Internet Passwords for existing users**
  - Select the users in the Domino Directory then Actions\Set Secure Internet Password
  - Then the top (8.0.1) option (but I think it started working in 8.5.1)
SAML

• Security Assertion Markup Language
• Allows Notes users to go password-less
  • This can be a huge selling point
• Can also be set up so that the Notes ID is never stored on the user’s PC
  • It gets downloaded and stored in memory each time the user starts Notes
• User NEVER has to enter password
• You need 9.0.1, ID Vault, patience
• No password = no post-it note with password written on it!
MFA for HTTP

• Two options:
  • Native
    • Added in 12.0
    • TOTP, no push
    • Per internet site setting
    • Also works in Verse Mobile (and maybe Nomad too now...maybe?)
    • Much easier than SAML
    • There are some improvements HCL could add to make this much, much more useful
      • See the M365 implementation for ideas
  • SAML
    • You can control the MFA provider
    • As stated previously, complicated
Internet Passwords – You have choices now

• Old way – two passwords:
  • Notes ID password
  • Internet Password stored in person document
  • Two to manage
  • Complicated
    • For admins, PITA
    • Users get aneurisms, two passwords manage
    • Lots of cludgy workarounds attempted to fix this

• New way – Shared Internet Password
  • New in 11.0
  • Allow Domino to use the Vaulted ID password
    • That’s right, the password on the ID in ID Vault can now be the users’ Internet Password
  • One password to rule them all
  • Much more simplified password management
    • Change in one, change in the other
Internet Passwords – You have choices now

• But there’s more…..

• ActiveDirectory Password Sync
  • Yes, I will repeat this…..ActiveDirectory Password Sync
  • The pot of gold at the end of the rainbow actually exists now
  • New in 12.0
  • Will provide a 1-way-sync of AD User password changes into ID Vault
    • And with Shared Internet Password, that could also mean HTTP passwords are now your AD password
  • Does required a Domino sever (non-running) to be installed on every writeable AD controller

![Network settings](image-url)
Internet Passwords – Prevent the Brute Force Attacks

• Internet lockouts
  • Extended in 12.0
  • Now able to block based on IP address
    • This is how hackers really work
      • They sit on an IP and spray user name and password combos at your server
      • Pre 12.0 all you could block was the same user name being used
      • Now you can block the IP doing the attack
  • Turn this on if you are >= 12.0 servers!
By default, Deny Access ONLY works for Notes client traffic

• Yeah, I know, weird right? Strange decision.
• You have to specifically choose to enforce deny access on other protocols (HTTP, LDAP, etc.)
  • Per server as well….grrrrr
• If not, you may deny a user access to Notes and email via a client, but that can still log into iNotes or Verse and send snoty emails about the management
• By default all protocols are set to “No”
• DLAU also highlights this now
OTHER SECURITY
Disable Things

• Anything you don’t use, disable. Anything you don’t need, disable
• Need POP3 or IMAP? No?
  • Not having it in the Notes.ini will not start those tasks… BUT…
  • They can still be started manually
    • `load pop3`
  • This is not sufficient, disable it in the Domino Directory
    • Now `load pop3` won’t actually load anything
Enable Things - Notes/Domino Port Encryption

• For Domino server to server or Notes client to server communication
  • Turn on at one end, works at both
  • AES and PFS are available, set in ini file on server or pushed do to client via policy
  • See https://help.hcltechsw.com/domino/11.0.1/admin/conf_port_encryption_t.html
• WAN accelerators don’t link this (or port compression)
• Test via a trace in the Notes Client or the Server console (debug ini settings help)
  • See https://blog.darrenduke.net/darren/ddbz.nsf/dx/9.0.1-fp7-and-how-to-enable-the-new-port-encryption-settings.htm
NOT SECURITY (?)
Antivirus Settings (OS)

• Domino Server Exclusions
  • Transaction Logs
  • Domino Data
  • DAOS repository
  • View Rebuild Dir folder
  • Directory Links

• Notes Client Exclusions
  • Notes\framework
  • Notes\data\workspace\.config\org.eclipse.osgi
  • JAR files

• See https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0093046
Antivirus Settings (OS)

- But Darren, what about when my users click on a virus infested email attachment?

- **HCL Notes and Attachments**
  - All Notes attachments are saved to %TEMP% on Windows
  - So long as the OS AV has real time scanning of %TEMP% you are covered
  - Remember, %TEMP% could be different per user
Knowledge is Power

• Forewarned is forearmed and there are resources that allow you to be pro-active.
  • US CERT weekly email
  • Be afraid, be very afraid (especially of Flash, Acrobat, AIR and Java)
  • See https://www.us-cert.gov/ to sign up

## High Vulnerabilities

<table>
<thead>
<tr>
<th>Primary Vendor – Product</th>
<th>Description</th>
<th>Published</th>
<th>CVSS Score</th>
<th>Source &amp; Patch Info</th>
</tr>
</thead>
</table>
Testing

• So you *think* you’re secure? OK…..
• Testing is what elevates belief to evidence
• QualSYS SSL Labs test site for web sites
  • [https://www.ssllabs.com/ssltest/](https://www.ssllabs.com/ssltest/)
  • Scan a server, get a grade
  • Will take a few minutes
  • Also lists potential remediation
  • Tons of useful information
  • If you get a A- or higher you’re good
  • Scan every quarter or so. Things change!
  • Use on sites other that your own
    • Be scared. Be real scared.
Testing

- Here is my Domino Blog server behind an Apache Reverse Proxy

**SSL Report: blog.darrenduke.net (199.103.7.9)**

Assessed on: Thu, 21 Mar 2024 08:51:34 UTC | HIDDEN | Clear cache

**Summary**

**Overall Rating**

A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »
Testing

- Test SMTP STARTTLS at CheckTLS.com
  - [https://www.checktls.com/testreceiver.html](https://www.checktls.com/testreceiver.html)
  - Test both send and receive

- Receive example:
Testing

- Send
  - You send email with a code in it, CheckTLS then replies to you with the transaction

```plaintext
Your email was successfully sent securely using TLS.

A transcript of the email SMTP session is below:

---> this would be a line from your email system to our test
<-- and this would be a line to your email system from our test

If TLS was negotiated, a line is added:

  === TLS negotiation successful (cypher: option1, client cert: certinfo)

Everything after that line is secure (encrypted), as indicated by:

  --> commands from your system then have wiggly lines
  <-- and responses from our system do too

Any errors that the test notices are noted in the log by asterisk boxes:

  *****************************************************
  *** Error Note ****************************************
  *** The error message would be here
  *****************************************************

---TRANSCRIPT BEGINS ON THE NEXT LINE---

<-- 220 t33.checktls.com CheckTLS TestSender Mon, 17 Aug 2015 14:14:03 -0400
<-- EHLO smtp.
<-- 250-t33.checktls.com Hello smtp2.250-enhanced.letsencrypt.org, pleased to meet you
<-- 250-ENHANCEDSTATUSCODES
<-- 250-SMTPHIME
<-- 250-STARTTLS
<-- 250 HELP
--> STARTTLS
<-- 220 Ready to start TLS

  === TLS negotiation successful (cypher: AES256-SHA, client cert: Subject Name: undefined/Issuer Name: undefined)

--> EHLO smtp2
<-- 250-t33.checktls.com Hello smtp2.250-enhanced.letsencrypt.org, pleased to meet you
<-- 250-ENHANCEDSTATUSCODES
<-- 250-SMTPHIME
<-- 250 HELP
```
Securing LDAP

• Using DA to AD for internet passwords?
  • Also secure this otherwise your users AD passwords are going from Domino to AD in **plain text**
  • Just checking the box in DA.NSF **is not** sufficient!!!!

• You also need to import your AD server SSL certificate in your server.id file
Securing LDAP

- I see a shocking amount of Domino LDAP servers NOT using LDAPS
  - LDAPS is over port 636 by default
  - Provided Domino has been set up for SSL, enable LDAPS
  - If your LDAP clients supports LDAPS, USE IT!
Securing LDAP

• Potential LDAPS issues
  • Your LDAP client (copier, spam gateway, etc) may not support newer ciphers
    • DEBUG_SSL_ALL=3 is your friend when testing this
    • Usually, a firmware update will address this
      • Usually
      • Or a new copier ;)
  • Also enabling deprecated ciphers in Domino can help
    • Debug first to ensure you need too