OPENNTF WEBINARS

September 21, 2023 OpenNTF Webinar
Domino SSL Implementation and Renewal, A Survivor's Guide
AGENDA

• Welcome
• Presentation
  Avery Shaffer
• Q and A
THANKS TO THE OPENNTF SPONSORS

• HCL made a contribution to help our organization
  • Funds these webinars!
  • Events, Community interaction on Discord
  • Running the organization
• Prominic donates all IT related services
  • Cloud Hosting for OpenNTF
  • Infrastructure management for HCL Domino Servers
  • System Administration for day-to-day operation
COMMUNITY – WE ARE ALL OPENNTF

- Participate – we all learn from each other
- We are all volunteers
- No effort is too small
- If your idea is bigger than you can do on your own, we can connect you to a team to work on it
- Test or help or modify an existing project
- Write guides or documentation
- Add reviews on projects / stars on Snippets
AUTUMN 2023 COMMUNITY EVENT

• Blogathon!
  • Dust off your Blog, or create a new one, or a video, or a wiki
    • OpenNTF can host your post if you don’t have a Blog
  • Share what you know with the Community
    • You never know what might happen
  • All blog posts will be featured on the OpenNTF Discord server (#blogathon) and in Collaboration Today
  • Get an OpenNTF Badge!
  • Helps with consideration as an HCL Ambassador
JOIN US ON DISCORD
UPCOMING EVENTS

• OpenNTF Repair Café
  • Admin topics
  • Next week! Thursday, Sep 28 @ 11:00AM EDT / 5:00PM CEST

• Dev and Admin topics each month
NEXT WEBINAR

October: HCL Domino Leap with Marty Lechleider

November: Sametime v12 with Erick Schwalb & Herwig Schauer

December: Annual Holiday Community Celebration
Domino SSL Implementation and renewal,
A Survivor's Guide

Presentation by Avery Shaffer
About Me

- Senior Systems Administrator at Prominic.NET and primary certificate handler
- Domino Administrator since 2012
- Local fire performer of Champaign/Urbana
Why Are SSLs Such A Pain Now?
SSL Certificate Renewal Reduced To One Year

Why?
- Higher security with frequently changing certificates
- Newly released security features are updated faster (i.e. SHA1 to SHA2)
- Exposed or compromised key chains removed quicker
- The “correct” theory that if we keep changing the certificates, the site can't be hacked

Who?
- In 2015 the CA/Browser Forum voted to reduce certificate validity from 5 years to 3 years.
- In 2019 they voted again to reduce certificate validity to 1 year but the vote failed.
- Apple decided independently to only allow 1 year SSL validation for Safari browsers, everyone following suite.

Future Change
- Google is pushing for maximum 90 day SSL key expiration by the end of 2024
Uniformity is important as the entry is in several critical places:

- Internet Site Documents, Internet Ports, SMTP, LDAP, IMAP, etc.
- Yearly .kyr name change can cause outages if an entry is missed.
SSL Purchase and Renewal
Let's Encrypt VS Paid Certificate

Let's Encrypt

Pro

● Free!
● Updates Automatically
● Generates .kyr format. No need to convert (certmgr does not use .kyr!)
● Set Up and Go
● Wildcard supported (experience has varied)

Cons

● No warranty protection
● DV (domain validation) level certificate only
● Incomplete chain issues with certain Java applications
● Requires port 80 open
Paid Certificate

**Pro**
- Higher Validation Levels offered (OV EV)
- Warranty
- Full Certificate Chain Provided
- Site Seal to reassure visitors
- No port validation needed

**Cons**
- Cost $$$
- Must convert to .kyr or .pem manually
- Only valid one year and requires manual validation via email or DNS
Purchased SSL
Where to buy SSL keys

- DNS Registrar
  - Can install keys for you if site is hosted by them
  - Generates the .csr and .key for you

- SSL Specialty Sites
  - Can purchase multi-year for cheaper (SSL still expires in one year)
  - Can pay extra for installation assistance

- Managed Hosting Providers
  - Handles the whole process for extra cost
  - Receive certificates in all formats needed
  - Can Install on Domino environment for you
Generating your .csr and .key

Server Certificate Administration
- Does not support key size above 2048
- Keyfile.key buried in Domino server
- Template not available on modern Domino installations

OpenSSL
- Continuously updated
- Supports key size 4096
- Can generate .kyr as well as convert certs to .pfx .p12 etc
- Knowledgebase article:
  - https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0073175
Consistent Validation

- Stop the headache of single user validation
- People leave, emails change
- Streamline validation with a generic email and mail-in database

Level 2 Generic Domain E-Mail Addresses

- admin@trainingwheels.lol
- administrator@trainingwheels.lol
- hostmaster@trainingwheels.lol
- postmaster@trainingwheels.lol
- webmaster@trainingwheels.lol

SSL
dominolearn-2.trainingwheels.lol/trainingwheels
mail/SSL.nsf
admin@trainingwheels.lol
Notes 9.0.1.3 to 11 can utilize the keyring/kyrtool
-  https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0073172

- Command line tool to view, create and import certificates to .kyr format
- Kyrtool installs with Notes 11 out of the box
- Notes/Domino 12 switch to Certificate Manager!
Certificate Manager – No More .kyr!

- Certificate Manager can import .pem, .p12 and .pfx formatted keys
- Simple as copy/pasting certificates in .pem format on a notepad and upload
- Replicated DOMAIN WIDE! Huge deal for when 90 day keys are implemented for wildcard certificates

-----BEGIN RSA PRIVATE KEY-----
(Private Key: domain_name.key contents)
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
(Primary SSL certificate: domain_name.crt contents)
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
(Intermediate certificate: certChainCA.crt contents)
-----END CERTIFICATE-----
Let’s Encrypt
Automated certificate management for Domino 10 and 11
Two part streamlined installation on OS and Domino
- Supports Linux and Windows OS
- DSAPI filter entry required on Internet Site document
Requires program document and http restart to update certificate chain
Certificates stored in data directory as .kyr/.sth
Server restart usually clears any renewal errors
Test connection with staging setting before automating
- Certificate requests are limited and you will get timed out!
Certificate Manager

- Native automated certificate management for Domino 12
- One line Administrator command for installation
  - “load certmgr”
  - DSAPI filter entry required on Internet Site document (No longer when upgrading to 12.0.1!)
- Requires a server task entry to ensure the task runs on startup
  - Set config ServerTasks=Replica,Router,Update,Amgr,Adminp,Sched,CalConn,RnRMgr,HTTP,LDAP,Certmgr
- Replicated DOMAIN WIDE! Huge deal for if 90 day keys are implemented
  - Note: TLS credentials cannot be exported. The .key is encrypted
  - Workaround in Domino V12 Certificate Management slides linked at the end
Cipher Security by Domino Version
- Fantastic free tool for testing your site security
- Use it to check:
  - Certificate Chain
  - TLS Protocols Enabled
  - Ciphers
  - Handshake Simulation
- Be sure to check “Do not show results on the boards
- [https://www.ssllabs.com/ssltest](https://www.ssllabs.com/ssltest)
Domino 9.0.1 FP3 – Support for TLS 1.2 is implemented
Domino 9.0.1 FP3 IF2 – Ability to disable TLS 1.0
  SSL_DISABLE_TLS_10=1
- Updated cipher suite to include 256
- Weak ciphers are NOT removed automatically
  - Ciphers set in previous versions stay selected
  - New ciphers are not selected
Domino 12.0.2 Cipher Security

- Domino 12.0.2 deprecated most weak/outdated ciphers
  - Domino 12 disables TLS 1.0 by default!
- Check your cipher lists!
How to Achieve an A+

- You have made all changes but still receiving an A in SSL Labs
- HSTS is the answer!
- This protocol is used to prevent man-in-the-middle attacks, downgrade attacks and cookie hijacking
- HTTP_ENABLE_HSTS=1
- HTTP_HSTS.Include_SUBDOMAINS=1
- Seeing a “Too Short” warning? Add the following notes.ini - HTTP_HSTS_MAX_AGE=63072000
- Too short can cause the browser to ignore the request for HTTPS connection and use HTTP
● TLS 1.3 is currently not supported by any version of Domino
● HCL has stated it is on the roadmap, no current release date
Bonus Tips!
Cipher errors present even after cleaning up Internet Site Documents
Invalid Cipher Errors on HTTP Startup

- Hidden views strike again!

- Configuration → Current Server Document to disable Internet Site Documents then save

- Ports → Internet Ports → TLS Ciphers

- To achieve an A+ in SSL Labs disable all but the top four
Cipher List Not Updating After Domino Update

- Domino Version under Configuration → All Documents only updated by names.nsf admin server. Is it correct?

- No? Update the Administrator server on the names.nsf and restart server

- Be sure to refresh the design template of names.nsf as well
Certmgr – Port 80 Error

- Certmgr auto renewal requires port 80 to be open
- Settings that redirect traffic to 443 will break this process
- Setting Anonymous access to no will also break auto renewal unless you update your notes.ini

HTTPPUBLICURLS=/iwaredir.nsf/*/well-known/acme-challenge/*
As of Domino 12.0.1FP1, HCL Nomad can be installed directly on the Domino server instance.

During the initial set up, Nomad will look for/install Certmgr and create a nomad.<yourdomain>.com entry.

To utilize your own purchased certificate, install Certmgr and set up nomad.<yourdomain>.com prior to installation.

- This is not a requirement just a way to skip the extra step of having to modify/recreate the entry.
If no matter what you change your Domino ciphers to does not reflect in SSL Labs, Check for proxy and passthru servers in the environment that may be handling Encrypting the traffic.
Redirect Rules can interfere with certmgr renewal, throwing a port 80 connection error.

Workaround – Temporarily disable Internet Site Documents → restart http → re-run the renewal.

Yes, this will break the auto-renew feature while the redirect is in place.
Bonus Tip

- Type in a command and realize you want to copy in the email path?
- You still can! Though a CTRL + V will replace the line, a Right Click + Paste will insert your clipboard at the end of the line!
- Domino V12 Certificate Management
  - HCL Academy, by Daniel Nashed
    - https://blog.nashcom.de/presentations/openntf2021_domino_certmgr.pdf
- Let’s Encrypt for Domino V10/11
  - https://www.midpoints.de/de-solutions-LE4D