Von Fix Pack zu Feature Pack

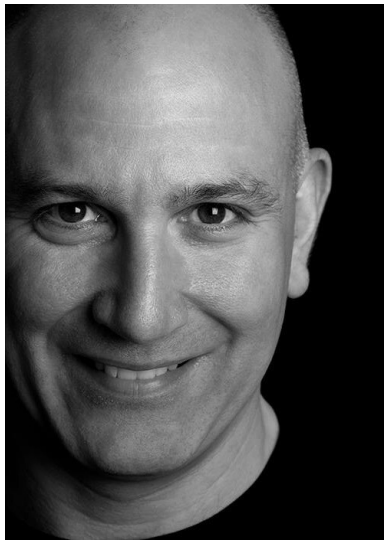
What's new in Domino

Daniel Nashed, Nash!Com

AdminCamp 2017 – Sept. 18-20 in Gelsenkirchen

Nash!Com
Communication Systems

Über den Referenten



- Nash!Com – IBM® Business Partner/ISV
- Mitglied The Penumbra group - An international consortium of selected Business Partners pooling their talent and resources
- Fokus: Cross-Platform C-API, IBM® Domino® Infrastruktur, Administration, Integration, Performance, Security, Troubleshooting und IBM® Traveler
- Platform Fokus: Microsoft® Windows®,Linux® und IBM AIX®
- DNUG Fachgruppenleiter: Verse/Notes/Domino
- Autor des Domino auf Linux®/UNIX® Start Scripts

IBM CHAMPION

Nash!Com
Communication Systems

Agenda

- Grundlegende Informationen zu „Fps“ und Strategie
- Was gibt es Neues in „Feature Pack 8“ und „Feature Pack 9“ in Notes und Domino
- Erfahrungen aus der Praxis und Best Practices
- Highlights aus dem letzten Fixpack 7
- Fragen und Anregungen – Jeder Zeit
- Bonus-Slides - Security Update TLS – Review des aktuellen Status

„FP“ - aus „FixPack“ wird „Feature Pack“

- Neue Strategie für die Auslieferung von neuen Features
  - 3-4 **Feature Packs** pro Jahr mit neuen Features im Notes Client und Domino Server
  - Template Änderungen werden separat bereitgestellt
  - „**FP**s“ enthalten Features und Bug-Fixes
  - Features werden so bereitgestellt, daß sie optional genutzt werden können
    - z.B. aktivierbar über Policies und notes.ini Einstellungen
- Schon in den letzten FPs wurden viele Funktionen neue Funktionen ausgeliefert
  - Besonders im Security-Bereich wurden in **FP**s und auch in **IF**s neue Funktionen implementiert
  - Aktueller Status und wichtigste Änderungen im Anhang der Präsentation

Notes Windows Feature Pack Candidates (Stand : IBM Connect 2017)

Notes Fix Pack 7

- Improved support in the Notes client for high resolution monitors including 4k monitors
- Support for TNEF based calendar invitations in Notes / Domino addressing parsing issues

Notes Feature Pack 8

- Support Java 8 runtime
- Ability to show internet address instead of Notes addresses in Mail / Calendar / Contacts and ToDo's
- Improvements in rendering forwarded MIME messages (read - only)
- Mail template update
- Policy support for Group By Messages and beginning of message

Notes Feature Pack 9

- Upgrade OSGi / Eclipse / SWT to support Java 8 compile time
- Ability to run rules on existing emails
- Support for persistent VDIs for Roaming and SAML configurations
- Support for Last Name / First Name mail addressing in Notes client providing consistent results
- Support auto refresh for delegated mail files

High Priority

- Support for STARTTLS protocol in Notes client
- Support for incremental overlay in federated calendars for ICS files
- Delegate Calendar and ToDo's option when delegating mail files
- Increase limit for junk mail in the Notes client
- Archiving with editor access for delegates
- Support for folder design upgrades for large number of folders
- Forward invitation as an invitation
- Support for Notes touch screen in Mail / Calendar / Contacts view

Nash!Com
Communication Systems

Domino / Application Development Feature Pack Candidates (Stand: IBM Connect 2017)

Domino Fix Pack 7

- Notes / Domino Port Encryption upgraded to AES

Domino Feature Pack 8

- Upgrade Java 1.8 (Run time only)
- Move Views outside of NSF for Increased data store in NSF
- Document encryption for XPages
- Backend LotusScript / JavaScript / Java Access to ID Vault
- Increase Document Summary limit from 64k to 16mb
- Domino Designer source control extension point for Swiper integration
- Pubnames template update
- Support ADFS 3.0
- New @ModifiedInThisFile , @AddedToThisFile

Domino Feature Pack 9

- Upgrade to Java 1.8 (Designer Compile time)
- Upgrade OSGi on Domino Server
- NIF – Concurrency Enhancements (inline view update)
- Domino policy to restrict mail from forwarding to an internet address
- Support RFC 2231 - this RFC is the current standard for specifying non -ASCII headers. It was first introduced over 15 years ago. It was not widely used for many years. It is now the default for many mail clients, e.g., Thunderbird

High Priority

- Performance and Scalabilty improvements from IBM Verse On Premises

Nash!Com
Communication Systems

Server Plattform Support – Neue Plattformen

- RHEL 7 Support seit 9.0.1 FP2
- SLES 12 Support seit 9.0.1 FP3 IF1
  - Ungewöhnlich, daß eine neue OS Major Version ab einem IF supportet wird
    - Der IF behebt ein Problem mit bindsock, daß durch eine Kernel-Änderung entstanden ist
      - Referenz: SPR# YXYX9RA56Z - HTTP server can't be started with "Error - Unable to Bind port 443 or 80" on SUSE12.
- Microsoft Windows 2016 Support ab Feature Pack 8
- IBM i 7.3 Support seit 9.0.1 Fix Pack 6
  - http://www.ibm.com/support/docview.wss?rs=463&uid=swg21977077

Strategische Plattformen

- **Windows 64bit** und **RHEL Linux 64 Bit** sind die strategischen Plattformen für alle neuen Produkte und Major Releases in der IBM Software Group

- Alle anderen Plattformen bleiben im 9.0.1 Code-Stream inkl. aller FPs voll supported!!

  - Verse on Prem und IMSMO sind die ersten Produkte, die von dieser Änderung betroffen sind
  - Bewertung pro Produkt, ob es auf einer Plattform angeboten und supportet wird nach Marktnachfrage und anderen Kriterien → Aktuell ist aber keine „Ausnahme“ in Sicht!
    - Diskussions-Punkte bei Kunden aktuell: SLES und iSeries

- Änderungen ab 9.0.1 FP8 für Domino

  - Wegfall von **Linux 32bit** und **AIX 32bit** für Domino → Migration auf 64bit ohnehin empfohlen

  - **Win 32bit** bleibt als einzige 32bit Plattform → u. A. für Sametime

Client Plattform Support

- Windows 10 Support seit 9.0.1 FP4
  - Windows 10 Pro (32-bit & 64-bit) und Windows 10 Enterprise (32-bit & 64-bit)
  - Notes, iNotes, Domino Designer, und Domino Administrator, Microsoft Edge Browser Support
  - http://www.ibm.com/support/docview.wss?uid=swg21963922
  - Citrix XenApp 7.7 Support ab 9.0.1 FP7
  - Citrix XenApp 7.8, 7.9, 7.11, 7.12 und 7.14 Support ab 9.0.1 FP9
- Ab Notes 9.0.1 FP8
  - Wegfall Linux Client :-(
  - Redhat und Ubuntu waren in 9.0.1 nach Wegfall von SLED die einzigen supporteten Distributionen
  - Laut IBM setzen den Client auf Linux recht wenige Kunden ein
  - Technisch gibt es einige Änderungen im Linux Code, die für den Notes Client besonders im Bereich Sametime Client schwierig sind

JVM Update Strategie – Bisher

- In „**FP**s“ können JVM Patches integriert sein
  - In der Regel werden mit einem FP die zu dem Zeitpunkt verfügbaren Versionen ausgeliefert
  - In **IF**s (im Grunde technisch Hotfixes) werden keine JVM Patches ausgeliefert
  - Kommt zwischenzeitlich eine neue JVM Version wird sie über einen separaten JVM Patch ausgeliefert
- Patches sind immer ein „diff“ zum Major Release

Java 1.8 ab Notes/Domino 9.0.1 FP8

- Funktionen in Java 1.8 werden von Entwicklern schon sehr lange erwartet
- Wird dringend für TLS 1.2 mit aktuellen ECDHE Ciphern benötigt
  - Beispiel/Test: Feed-Reader **ECDHE_RSA_WITH_AES_128_GCM_SHA256**
- Austausch der JVM – Kein Patch, wie normalerweise in „Fixpacks“
- In FP8 bleibt die Entwicklungsumgebung noch auf Java 1.6
  - Geplant für FP9 war ein Update inkluive Eclipse Umgebung → Wird für die neue JVM benötigt
    - **Verschoben auf FP10**
  - Für FP10 soll dann endlich voller JVM 1.8 Support für den Notes Designer Client kommen!

FP 7 vs FP 8 - TLS Verschlüsselung Notes/Domino Java

- Notes/Domino 9.0.1 FP7 → Java 1.6.0 SR16 FP30
- Bester Cipher für JVM 1.6 in Verbindungen mit der "Java Cryptography Extension":

  DHE_RSA_WITH_AES_256_CBC_SHA / 2048 bit key und **TLS 1.2** möglich!

  - Benötigt Patch zum Austausch der Java Security Policy Files"**Java Cryptography Extension**"
    - Weitere Informationen → http://blog.nashcom.de/nashcomblog.nsf/dx/higher-crypt-standards-with-notesdomino-and-jvm-1.6.htm

- **Ab Notes/Domino 9.0.1 FP8 → Java 1.8.0 SR3 FP22**

  - TLS 1.2 mit aktuellen ECDHE Ciphern!

Neue Java Security Issues auch für JVM 1.8

- „Multiple Vulnerabilities in the IBM SDK Java Technology Edition affect IBM Domino“
- Summary
  - „There are multiple vulnerabilities in IBM® SDK Java™ Technology Edition Version **6 SR16FP35** that affect IBM Domino. These issues were disclosed as part of the IBM Java SDK updates in Feb. 2017, fixed with Version **6 SR16FP41** and Version **8 SR4FP1**“
  - Betrifft JVM 1.6 und JVM 1.8
- Download-Beispiel Linux: JDK**1.8_SR4FP1**_Linux64_901.8_Server
- Jedes FP enthält die zu dieser Zeit aktuelle JVM
  - Zwischen den FPs werden neben IFs auch JVM patches bereitgestellt

Ref - Check Java Version - Fixpack 7

```
/opt/ibm/domino/notes/latest/linux/jvm/bin/java -version

java version "1.6.0"

Java(TM) SE Runtime Environment (build pxa6460sr16fp35-20161024_04(SR16 FP35))

IBM J9 VM (build 2.4, JRE 1.6.0 IBM J9 2.4 Linux amd64-64 jvmxa6460sr16fp35-20161012_322120
(JIT enabled, AOT enabled)

J9VM - 20161012_322120

JIT  - r9_20160630_120368

GC   - GA24_Java6_SR16_20161012_1548_B322120)

JCL  - 20161020_01
```

Ref - Check Java Version – Feature Pack 8

```
/opt/ibm/domino/notes/latest/linux/jvm/bin/java -version

java version "1.8.0"

Java(TM) SE Runtime Environment (build pxa6480sr3fp22-20161213_02(SR3 FP22))

IBM J9 VM (build 2.8, JRE 1.8.0 Linux amd64-64 Compressed References 20161209_329148 (JIT
enabled, AOT enabled)

J9VM - R28_20161209_1345_B329148

JIT  - tr.r14.java.green_20161207_128946

GC   - R28_20161209_1345_B329148_CMPRSS

J9CL - 20161209_329148)

JCL - 20161213_01 based on Oracle jdk8u111-b14
```

Ref - Check Java Version – Feature Pack 9

```
/opt/ibm/domino/notes/latest/linux/jvm/bin/java -version

java version "1.8.0"

Java(TM) SE Runtime Environment (build pxa6480sr4fp5-20170421_01(SR4 FP5))

IBM J9 VM (build 2.8, JRE 1.8.0 Linux amd64-64 Compressed References 20170419_344392 (JIT
enabled, AOT enabled)

J9VM - R28_20170419_1004_B344392

JIT  - tr.r14.java_20170419_344392

GC   - R28_20170419_1004_B344392_CMPRSS

J9CL - 20170419_344392)

JCL - 20170420_01 based on Oracle jdk8u131-b11
```

9.0.1 FP9 - SSLv3 ist per default deaktiviert

- SPR # DKENAKNSEG will affect all connection types that utilise the native Domino security stack such as HTTPS and secure DIIOP.

- Nicht in der Fixlist enthalten. Aber es gibt eine separate Technote
- Neuer notes.ini Parameter **ENABLE_SSLV3=1** zur Aktivierung, wenn nötig

- Die meisten Applikationen sollten mittlerweile mindestens TLS 1.0 unterstützen
  - Sinnvoller Default-Wert!

- Weitere Informationen zu TLS im Anhang

ADFS 3.0 Support ab 9.0.1 FP8

- ADFS 3.0 Support für
  - Notes Federated Login
  - Web Federated Login und Web SAML
- Die meisten Kunden haben mittlerweile ADFS 3.0 im Einsatz
  - ADFS 3.0 hat viele Verbesserungen z.B. verwendet ADFS 3.0 kein IIS mehr!
- Neue Dokumentation statt „Cookbook“
  - https://www.ibm.com/support/knowledgecenter/SSKTMJ_9.0.1/admin/secu_using_security_assertion_markup_language_saml_to_configure_federated_identity_authentication_t.html

NIFNSF – View/Folder Indize Auslagerung

- Separates **.NDX** File pro NSF
  - Entweder im selben Verzeichnis oder im separaten Verzeichnis mit gleicher Unterverzeichnis-Struktur
- Backup-Ersparnis (10% für Mail-Datenbanken ohne DAOS, 30% auf NSF nach DAOS)
- Größeres Datenbank Limit durch Auslagern des Index
  → Physisches NSF Limit immer noch 64 GB
- Performance-Gewinn durch weniger „locking“ der NSF Files
  - Erst ab 9.0.1 FP9 – **Wichtig: ODS 52 benötigt!**
    - SPR# SWAS96DSGG - Fixed concurrency issues between NIF & NSF on high usage shared databases. To realize this fix, databases must be ODS52 and Transaction logged.
    - SPR# SWASAKELQ8 - Fix a performance issue where when NIF/NSF is enabled on a database, the read time (returning more than a single entry) of views is up to 2 times the time for a database without NIF/NSF enabled.

NIFNSF - Aktivierung

- **Vorbereitung**
  - NIFNSF benötigt Transaktion Logging auf dem Server und der Datenbank!
  - **ODS 52** → notes.ini **CREATE_R9_DATABASES=1**
  - Notes.ini **NIFNSFEnable=1**
  - Optional: Verschieben der NDX Files in ein separates Verzeichnis
    - **Notes NIFBasePath=path**
      - Entweder a.) relativer Path im Data-Directory oder b.) absoluter Path
- **Aktivierung/Deaktivierung**
  - load compact -c -nifnsf **on** xyz.nsf
  - load compact -c -nifnsf **off** xyz.nsf

NIFNSF – Weitere Einstellungen und Commands

- Notes.ini **CREATE_NIFNSF_DATABASES=1**
  - Erstellt alle neuen Datenbanken mit NIFNSF aktiviert
- Server Console Commands
  - **show dir -nifnsfonly**
    - Zeigt alle Datenbanken an, die NIFNSF aktiviert haben
  - **show dir -nifnsf**
    - Zeigt alle Datenbanken an mit zusätzlich NIFNSF Informationen

NIFNSF Tuning

- NIFNSF braucht ein separates File-Handle für die NDX Datei
- Die NDX Datei ist mehr oder weniger eine Datenbank und braucht auch einen „Cache Entry“

- Default Max Cache-Entry Anzahl ~ NSF Buffer Pool in MB * 3 ~ 1024 * 3 ~ 3072
- Erhöhung für große Server via Notes.ini **NSF_DbCache_Maxentries=n**

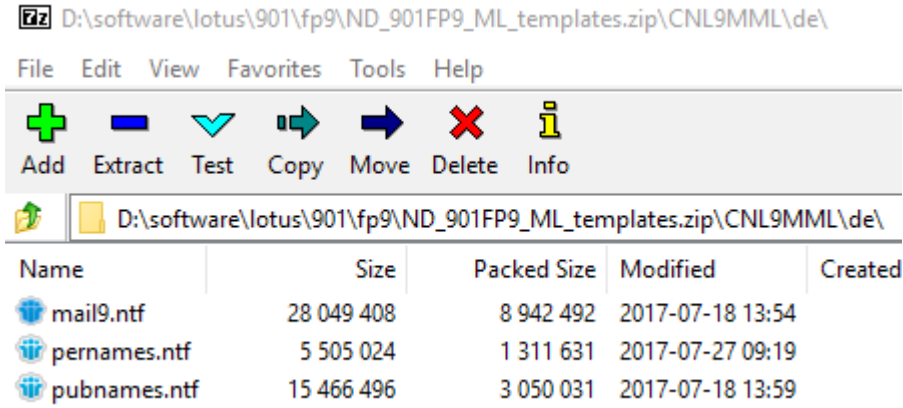
- Statistiken
  - Database.DbCache.**CurrentEntries** = 1173
  - Database.DbCache.**HighWaterMark** = 1189
  - Database.DbCache.**MaxEntries** = 3072
  - Database.DbCache.**OvercrowdingRejections** = 0 → sollte immer Null sein!

Large Summary Data

- Beschränkung für Summary Data eines Dokumentes bisher
  - Summary Data pro Dokument → **64 KB**
  - Summary Data pro Item → **32 KB**
- Erhöhung der Summary Data pro Dokument auf **16 MB**
- Voraussetzung: Aktivierung von **ODS 52**
  - Notes.ini → **Create_R9_Databases=1**
- Aktivierung über Compact
  - Load compact **-LargeSummary on** database.nsf
  - Load compact -ls on database.nsf

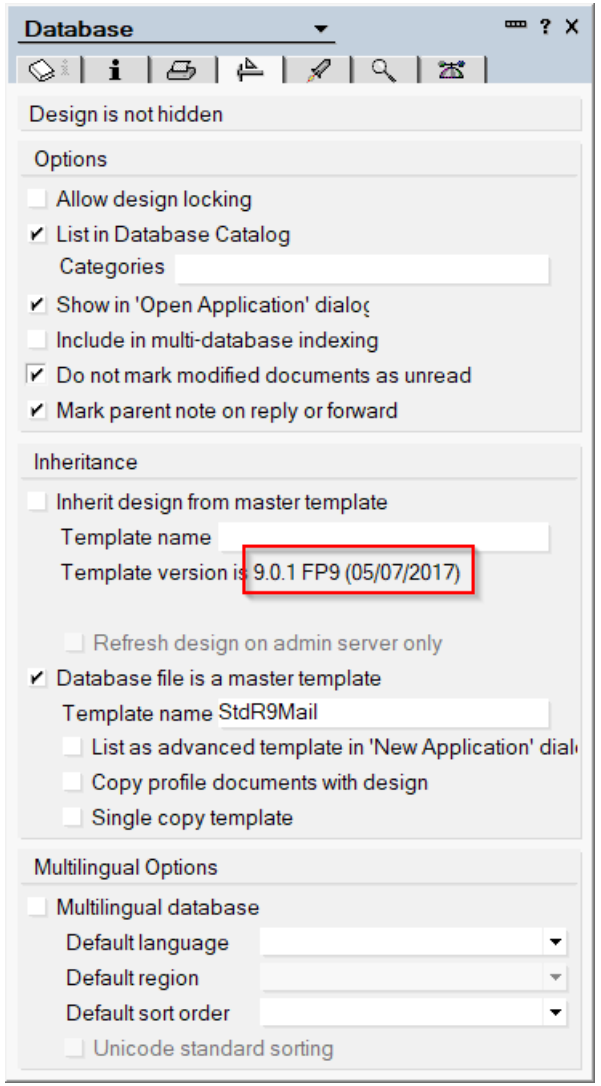
Template Änderungen in FP 8 / FP9

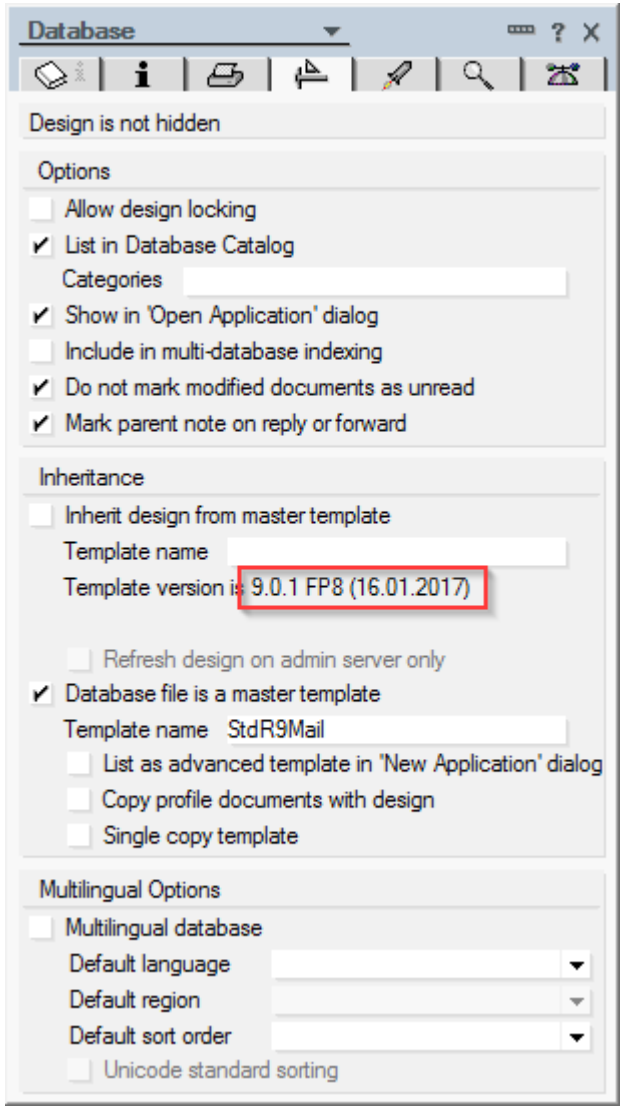
- Separate download für English und alle anderen Sprachen
  - 1 ZIP file für Englisch
  - 1 ZIP für alle anderen Sprachen mit Verzeichnis pro Sprache
  - **pubnames.ntf** und **mail9.ntf**
  - Seit FP9 auch **pernames.ntf**
    - pernames.ntf muß nach der Client-Installation ersetzt werden
    - Feature Pack Installer enthält kein Update für Templates
    - Bei Multi-User Client Installationen pro MUI Verzeichnis z.B.
      - C:\ProgramData\IBM\Notes\Data\Shared
      - C:\ProgramData\IBM\Notes\Data\Shared\mui\de
    - Multi-Language Templates via mlmerge.exe
      - Nicht wirklich empfohlen → Besser Templates separt ausrollen

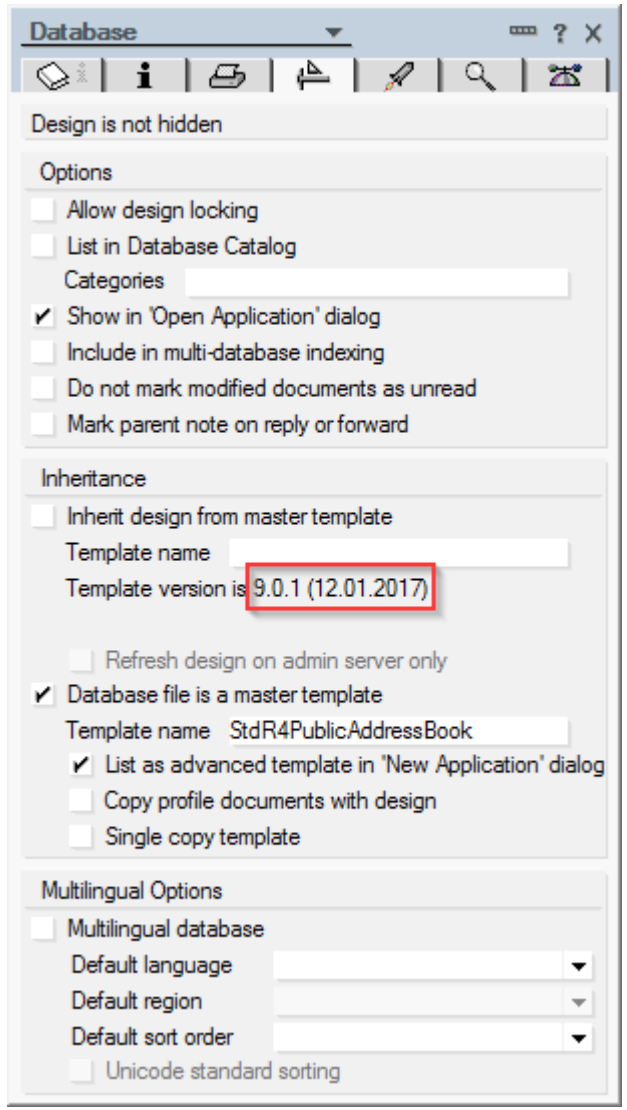


Nash!Com
Communication Systems

Design Namen / Versionen







Nash!Com
Communication Systems

Neue @Formulas in 9.0.1 FP8

- Zwei neue, sinnvolle @Formulas

- @ModifiedInThisFile
- @AddedToThisFile

- Verschiedene Einsatzmöglichkeiten
  - Wann ist ein Dokument in dieser Replik hinzugefügt worden ..
  - Wie lange hat es gedauert, bis ein Dokument in dieser Replik angekommen ist ..

Neue Funktionen Notes 9.0.1 FP8

- Anzeige von Internet Addressen in Typeahead
  - Benötigt 9.0.1 FP8 Mail Design
- Anzeigen der 100 Zeichen des Subject und Group bei Date aktivierbar über Policies
  - Bisherige Funktion, die jetzt per Policy verteilbar ist
- Read-only MIME Email Inhalt mit „Full Fidelity“ bei Reply/Forward
- Notes.ini Einstellung → **KeepReplyForwardMime=1**
  - In prior releases of Notes, the Notes editor would not maintain fidelity when a complex HTML MIME email message was prepared for Reply/Forward. Beginning in this release, when replying to or forwarding these types of MIME messages, the original message content is presented in read-only mode so that the recipient will see the content as originally received. This setting must be enabled by your administrator and is **not available in the Notes basic client**.

9.0.1 FP9 – Notes Client Windows High Resolution Support

- In 9.0.1 FP8 gab es die ersten Fixe für High Resolution Support
- Ab FP9: Voller High Resolution Support für Notes client

- Korrekte Skalierung für Text und Icons für High Resolution Displays (4K)
- Hilft auch mit angepaßten DPI-Einstellungen (z.B. 125 %)

Notes 9.0.1 FP9 – Verbesserter „Name Lookup“

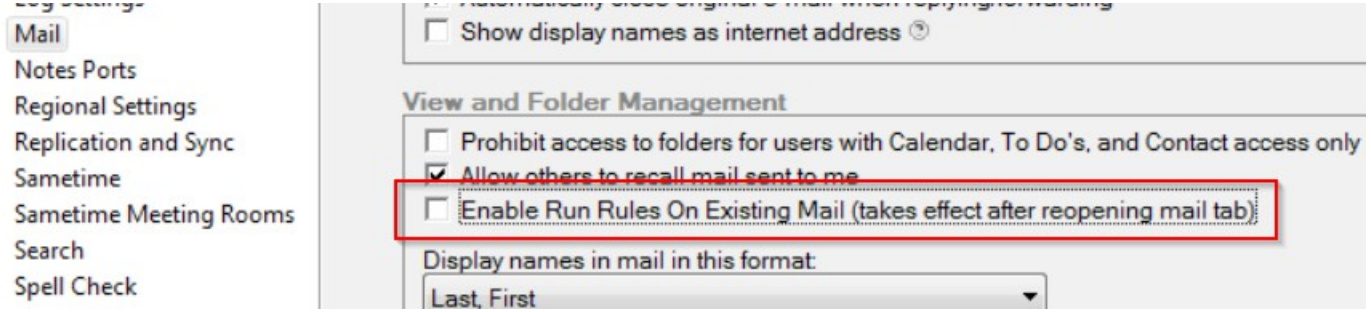
- Suche nach **<last name first name>** für Typeahead und im nicht eindeutigen Namen Dialog ergibt das selbe Ergebnis wie die Suche nach **<first name last name>**.
- Beispiel: Suche nach „**don smith**“ oder „**smith don**“ ergibt das selbe Ergebnis
  - Auch mit Varianten wie „**Donald, Donovan, Smithfield**“
- Benötigt neues 9.0.1 FP9 **pernames.ntf** und notes.ini **AllowWildcardLookup=1**

Notes 9.0.1 FP9 – Mobile Directory Catalog Änderung

- Auf Englisch belassener Text:
  - Improved support for Notes® addressing with mobile directory catalogs (SPR #SAPLAK8ANL)
  - The list of names that is shown when using typeahead to search a mobile directory catalog is now sorted according to the directory catalog configuration.
  - Names in local contacts follow this list.
  - In addition, the Search Directory for <characters> option is available at the end of the list to facilitate server lookup.
  - To enable this feature, add the notes.ini setting **$TypeAheadShowDircatFirst = 1** to the Notes® 9.0.1 FP9 client.

Notes 9.0.1 FP9 – Mail-Rules auf bestehende Dokumente

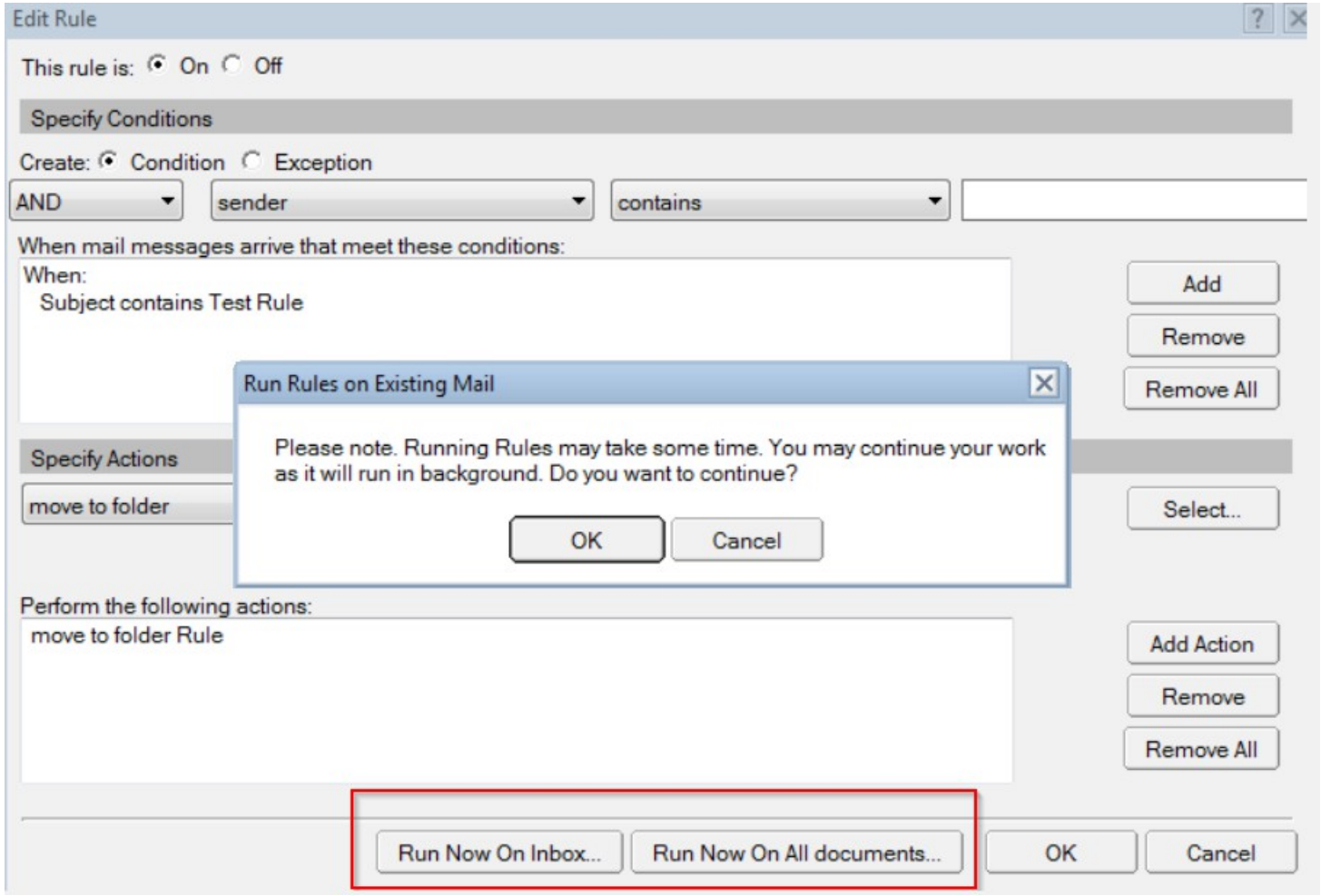
- Bisher wurden Mail-Rules nur auf neu eingehenden Mails ausgeführt
- SPR #BLIO8TGDUW
- Benötigt FP 9 Mail-Template!
- Aktivierung
  - File > Preferences > Mail / In Mail Options, „**Enable Run Rules On Existing Mail**“



Nash!Com
Communication Systems

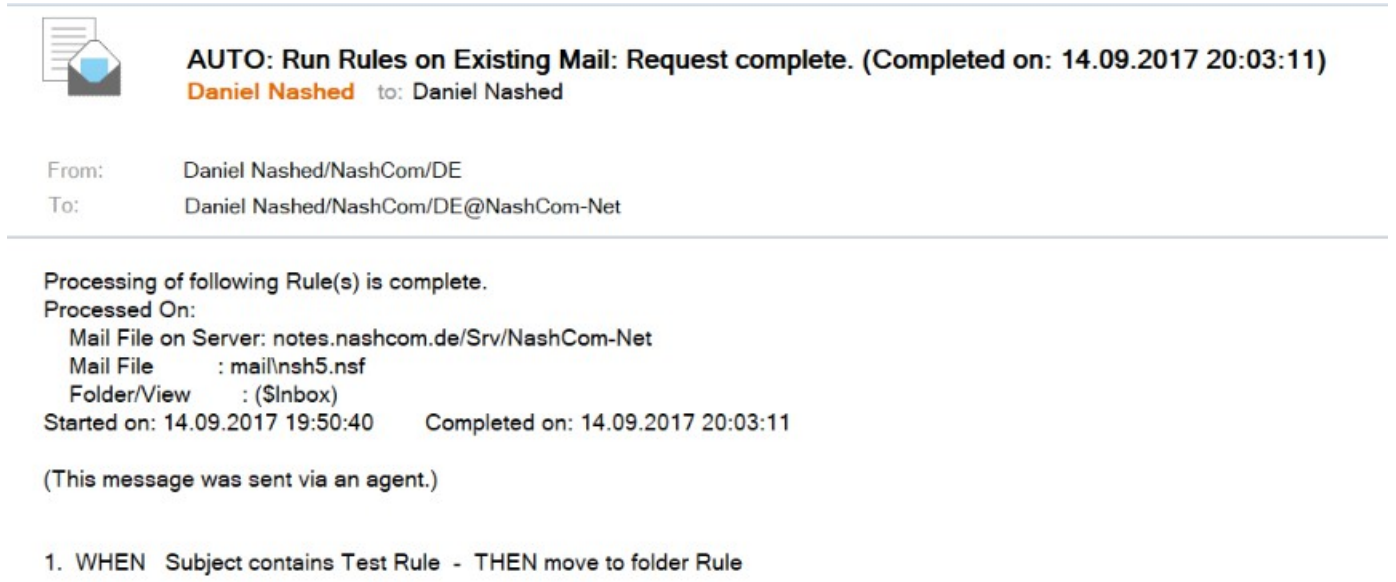
Notes 9.0.1 FP9 – Mail-Rules auf bestehende Dokumente

- Neue Optionen in der Regel selbst



Nash!Com
Communication Systems

Run Rules on Existing Mail Ergebnis per Mail



AUTO: Run Rules on Existing Mail: Request complete. (Completed on: 14.09.2017 20:03:11)
Daniel Nashed to: Daniel Nashed

From: Daniel Nashed/NashCom/DE
To: Daniel Nashed/NashCom/DE@NashCom-Net

Processing of following Rule(s) is complete.
Processed On:
Mail File on Server: notes.nashcom.de/Srv/NashCom-Net
Mail File : mail\nsh5.nsf
Folder/View : ($Inbox)
Started on: 14.09.2017 19:50:40 Completed on: 14.09.2017 20:03:11

(This message was sent via an agent.)

1. WHEN Subject contains Test Rule - THEN move to folder Rule

Run Rules Design Details

- Voraussetzungen, die im Design geprüft werden in der Hide-When Formel
  - Client muß mindestens 9.0.1 FP9 sein (oder Build 410..)
  - Datenbank ist kein Archiv
  - User muß mindestens Editor in der Datenbank sein
  - CalendarProfile muß RunRulesEnabled=1 haben
  - Rule muß aktiviert sein
  - Wird nicht auf dem online Mailfile in SmartCloudNotes supported
    - Calendar-Profile Check: **isMailDbOnCloud=1**
- Button startet einen Agenten der einen Agenten startet
  - ExRunRules → ExRunRules1

Font Problem mit 9.0.1 FP9

- Änderung in der Font-Generierung für SMTP Mail
- Jetzt
  - <span style=3D" **font-size:10pt;font-family:sans-serif**">Daniel Nashed
- Vorher
  - <**font size=3D2 face=3D"sans-serif**">Daniel Nashed

- Soll bessere Darstellung auf der Empfänger-Seite bringen
- Für Notes Clients (auch mit FP9) funktioniert das nicht sauber mit manchen Einstellungen
  - SanSerif wird als Serif dargestellt
  - Im Edit Modus und mit Einstellung: „Disable Embedded Browser for MIME mail“
  - Aktuell gibt es noch keine Lösung

9.0.1 FP 9 Problem – Private 1st Use Folder/View

- Private on first use View/Folder werden nicht mehr erstellt
- Laut einem Kunden ein Server und nicht ein Client Problem!
  - Leider ist das aus der Technote nicht ersichtlich
- SPR# JVEKAQSGCC / LO92948
  - SHARED, PRIVATE ON FIRST USE FOLDER NOT WORKING AS EXPECTED IN 9.0.1 FP9. IT IS NOT POSSIBLE TO VIEW THE FOLDER IN DESIGNER.

9.0.1 FP9 - Verbesserungen im C&S Compatibility Mode

- Neues Feature
  - „Before Feature Pack 9, a Notes user creating a repeating meeting with a non-Notes invitee encountered a dialog box warning of action limitations. With Feature Pack 9, that warning no longer appears."
  - With Feature Pack 9, if a Notes user wants to reschedule or cancel a meeting with a non-Notes invitee, all the options on the Change Repeating Entry are enabled.
  - Detailerte Beschreibung:
    - https://www.ibm.com/developerworks/collaboration/library/co-compatibility-mode-improvements-FP9/index.html
  - Neue Notes.ini Parameter zur Deaktivierung der neuen Optonen
    - CSDisableChairCompatOverride=1
    - CSDisableInviteeCompatOverride=1

Domino Designer 9.0.1 FP8

- Notes Client und Domino Designer laufen jetzt in einer 1.8 JVM
  - Aber wegen Eclipse Kompatibilitäts-Problemen ist das Compile Target noch 1.6 JVM
    - Geplant für FP9 → Eclipse Update und JVM 1.8 Compile Support
- Update CKEditor von 3.6.6.2 up to 4.5.3.2
- Update Dojo von 1.8.3 auf 1.9.7
- Neue URL Parameters im REST Calendar Service

What's new in IBM Domino Access Services Release 9.0.1 FP8

- Data API lowercasefields parameter
- Data API fields parameter
- Data API view entries limit – Wichtige Änderung, die Applikationen betreffen kann!
  - Prior to 9.0.1 FP8, the data API would return the specified number of entries (if available).
    As of 9.0.1 FP8, the data API will instead return HTTP 400 (Bad request)
  - IBM made this change to encourage paging through large views for better performance and scalability. However, if the change **breaks existing applications**, you can adjust the limit with a server notes.ini setting. For example, this setting increases the limit to 2000 entries:
  - Notes.ini **DataServiceMaxViewEntries=2000**
  - „IBM recommends keeping the limit as low as possible. Ideally, you want each view entries request to complete quickly and you want your Domino server to be able to handle many simultaneous requests."

What's new in IBM Domino Access Services Release 9.0.1 FP8

- Meeting updates with the Calendar API
- Calendar API sincenow and days parameters

- Core API statistics resource
  - /api/core/stats

- OpenAPI Specifications auf GitHub
  - https://github.com/OpenNTF/das-api-specs

- Referenz
  - https://www.lotus.com/ldd/ddwiki.nsf/dx/Whatsqos_new_in_IBM_Domino_Access_Services_Release_9.0.1_FP8

Domino 9.0.1 FP9 - Domino REST API enhancements

- Feature Pack 9 provides the following Domino REST API enhancements.
  For details on these enhancements, see the OpenNTF / das-api-specs repository.
  - **https://github.com/OpenNTF/das-api-specs**
- Improved attachment support
  - Previously, the data API returned all attachments inline with a document. Now, when reading a document, you can use the attachmentlinks=true parameter to get links to the attachments. Then you can read each attachment as a separate resource.
- Full-text search score
  - When you search within a view or across all documents, the data API returns a list of matching documents. Each item in the list now includes the relative search score. This helps a client rank search results.
- More granular administrator control of REST resources
  - When administrators enable an API, they can now use a server NOTES.INI setting to selectively disable a specific resource. For example, if administrators enable the data API but they don't want an application browsing the list of databases on the server, they can disable the database collection resource (**set config DAS_DATA_DB_COLLECTION=0**).
    See the OpenNTF / das-api-specs repository for a complete list of new NOTES.INI settings.

Domino 9.0.1 FP8 - Xpages

- Support for infinite scrolling (mobile "touch" scrolling) in Dataview control
- Improvements to the XPages mobile Date and Time control support in mobile themes
- Improvements to Xpages TypeAhead control support
- Support for Bootstrap responsive web design in Xpages
- Domino Designer with XPages in Bluemix support
- Document encryption and decryption in Domino using Xpages in combination with IDVault

Aktuelles Problem mit 9.0.1 FP8

- SPR #TPONAKFJLP / APAR #LO91828
  - After Upgrade To FP8, With Disclaimers Enabled, Pdf Attachments Have Content-transfer-encoding Of Binary And Can't Be Opened
  - If the mail is sent without disclaimers added, the Content-Transfer-Encoding is Base64 and the attachment can be opened.
  - Quelle: http://www.ibm.com/support/docview.wss?uid=swg22000468
  - Gefixed in 9.0.1 FP8 IF1
- Passiert auch mit anderen Attachments in Kombination mit „Disclaimern“
- Temporärer Workaround
  - Notes.ini **MIMEDisclaimersNoEncode=0** auf dem SMTP Outbound Server
    - Deaktiviert einen Fix, der für Google Calendar Probleme in FP8 enthalten ist und per default aktiviert ist

Wichtige SPRs gefixed in 9.0.1 FP9

- SPR# DKENA6RUGB - Performance improvement in SMIME processing
  - Eigentlicher Text: „Verifying S/MIME signatures is extremely slow when using AES algs for ID files“
- SPR# CEBS9B9RWE - Fixed a Traveler shutdown issue where the shutdown is causing a hang which results in QOS kills.
  - Wichtiger Fix für den sauberen Shutdown für Traveler Server
- SPR# MKINAJ8VB3 - Fixed an issue where the notes.ini TCPIP_ControllerTcpIpAddress is no longer ignored on Unix platforms.
  - Wichtig für partitionierte Domino Server unter Linux/AIX mit Server Controller

Wichtige SPRs in 9.0.1 FP9 für SMTP

- SPR# TMIZ6T6EB6 - Fixed an issue where the Inbound SMTP Internet Site document is not working with a Language Pack (All langugages except Kazakh and Hebrew)
  - Vorher gab es mit installiertem Language Pack Probleme bei Inbound SMTP Dokumenten!
- SPR# SAZR8MKH9Q - Add the ability to control SMTP the visible host name (EHLO param, greeting response, Received headers and Reporting-MTA in DSNs...) by these 2 controlled INI's **SMTPDisplayHostName** and **SMTPDisplayDomainName**
  - Neue Parameter zur Festlegung des SMTP Hostnames
  - Beispiel:

    SMTPDisplayHostName=myhost.mydomain.com

  - Vorher gab es nur den Parameter:
    - **SMTPGREETING**=domino.nashcom.de ESMTP Service ready at %s

SMTPDisplayHostName & SMTPDisplayDomainName

- Notes.ini **SMTPDisplayHostName=mysmtp.nashcom.de**
  - Outbound SMTPClient: CommandEHLO: **EHLO mysmtp.nashcom.de**
  - Inbound Server Responses:
    - **250-mysmtp.nashcom.de Hello st14p31im-asmtp003.me.com...**
  - Received Header:
    - **from st14p31im-asmtp003.me.com ([17.163.246.47]) by mysmtp.nashcom.de (IBM Domino Release 9.0.1FP9HF19) with ESMTP id 20170910180629 78-2 ; Sun, 10 Sep 2017 18:06:29 +0200 ...**
- Notes.ini **SMTPDisplayDomainName** funktioniert ähnlich, ändert aber nur den Domain-Namen und der Hostname bleibt bestehen
  - **SMTPDisplayHostName** überschreibt **SMTPDisplayDomainName**

9.0.1 FP9 - Agent Manger Queue

- Enhancement Request To Be Able To Increase The Amgr Queue Beyond 100 (SPR #RSTNA4SL7C APARID: LO87242)
  - The Agent Manager's Eligible queue is now able to change from the lowest value possible at 100, to 255 which is the highest value possible via an INI **AMGRMaxQueue**.
- Davor konnten nur 100 Agenten gleichzeitig gescheduled werden
- Der interne Wert ist als BYTE gespreichert und wurde leider nicht weiter erhöht
  - 255 sollte aber für die meisten Umgebungen reichen

SMTP Änderung und Bug

- SPR# TPON949L2M - Fixed an issue where encoded phrases may have embedded delimiters after decoding -- e.g., the comma (',') in Ziffle, Fred <fred.ziffle@zifflemail.com> causes an error for Notes. Fix is to unconditionally quote the decoded phrase: "Ziffle, Fred" <fred.ziffle@zifflemail.com>
  - Fix erzeugt ein Problem bei eingehenden Mails → Header enthalten Müllzeichen am Anfang des „From“ Headers und anderen Adress-Headern
- Wirkt sich bei unterschiedlichen Konfigurationen unterschiedlich aus
  - Müllzeichen im Header, SMTPVerifyAuthenticatedSender=1 geht nicht
  - SMTPSaveImportErrors=3 mit SMTPSaveFileFrom=sender funktioniert nicht mehr

Domino 9.0.1 FP9 IF1 (15.9.2017)

- SPR #JCARAQSJB6
  - SMTP regression issue in Domino 9.0.1FP9 can cause malformed headers & prevent Internet mail delivery with SMTPVerifyAuthenticatedSender=1 (technote 2008327)
  - http://www.ibm.com/support/docview.wss?uid=swg22008327
- SPR #KBRNAQKKK9
  - Domino agents crash in the backend in FP8 with a memory overwrite
- Linux64 Build is dieser Hotfix → 9.0.1 FP9 HF 63

Inline View Indexing

- Schnellere „Inline“ Indizierung von Indizes
- Muß pro View aktiviert werden

- Wenig Informationen in den Release-Notes
- Detailierte Beschreibung hier:

  https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/admn_inline_index_enabling.html

- Details auf den nächsten Folien (in Englisch)

Enabling inline view indexing with the Updall task

- Inline view indexes enabled with the Updall task are referred to as design-enabled inline view indexes.
- Procedure
  - Use the following command to use the Updall task to enable inline view indexing for a database. To enable inline view indexing for all views in a database, omit the view argument.
  - **load updall database -T view -inline on**
- Results
  - Inline indexing is enabled as a view is opened.
- Example
  - The following example enables inline view indexing for the By Author view in disc9.nsf:
    - load updall disc9.nsf -T "By Author" -inline on
  - The following example enables inline view indexing for all views in disc9.nsf:
    - load updall disc9.nsf -inline on

Enabling inline view indexing with INLINE_VIEW_INDEX setting

- Inline view indexes enabled with the INLINE_VIEW_INDEX setting are referred to as static-enabled inline view indexes.

- Procedure
  - Add the following NOTES.INI setting to the Domino® server.
  - INLINE_VIEW_INDEX=<database>,<database>

- Results
  - A server restart is not necessary. Inline view indexing is enabled as views are opened.

- Example

  - The following example enables inline view indexing for all views in sales.nsf and marketing.nsf:
  - INLINE_VIEW_INDEX=sales.nsf,marketing.nsf

Disabling inline view indexing

- load updall <database> -T <view> -Inline off
  - To disable indexing for a specific view, specify the view name. If you don't specify a view, all views in the database that use inline indexing are disabled.
- Notes.ini DISABLE_INLINE_INDEX=1
  - This NOTES.INI setting temporarily disables all inline view indexing on a server.
    A server restart is not necessary. Inline view indexing is disabled as views are opened.
- tell inlineindex disable <database> <view>
  - Temporarily disables inline view indexing in an active database.
  - To disable indexing for one view only, specify the view name.

Setting index expiration for inline view indexes

- Use NOTES.INI settings on a server to control when inline view indexes expire in:
  - inactive views in open databases
  - cached views in closed databases
- **INLINE_VIEW_INDEX_DESIGN_ACCESS_MIN**=<minutes>
  - Open database view expiration for design-enabled inline indexes
  - Default: no expiration.
- **INLINE_VIEW_INDEX_STATIC_ACCESS_MIN**=<minutes>
  - Open database view expiration for static-enabled inline indexes
  - Default: no expiration.
- **INLINE_VIEW_INDEX_DESIGN_CACHE_MIN**=<minutes>
  - Closed database view expiration for design-enabled inline indexes
  - Default: 5 minutes
- **INLINE_VIEW_INDEX_STATIC_CACHE_MIN**=<minutes>
  - Closed database view expiration for static enabled inline indexes
  - Default: 5 minutes

Inline View Index Commands

Command	Description
tell inlineindex show <database> <view>	Shows views in a database enabled for inline viewing indexing with Updall. Use <view> to see if specific view is enabled for inline indexing via Updall.
tell inlineindex disable	Temporarily disables inline view indexing for open databases.
tell inlineindex enable	Enables inline view indexing for open databases after temporarily disabling it.
tell inlineindex refresh	Refreshes all view indexes enabled for inline view indexing with Updall.
show dbs * inline	Shows the view expiration period for open databases enabled for inline view indexing. Lists all open databases with views that are enabled for inline view indexing and the number of views that are enabled in each database.
show dbs * inline views	Shows the same output as show dbs * inline, but adds information about each view that is enabled for inline view indexing.
dbcache show inline	Shows view expiration periods for closed databases enabled for inline view indexing. Lists closed databases with views enabled for inline view indexing.
dbcache show inline views	Shows the same output as dbcache show inline, but adds information about each view that is enabled for inline view indexing.
show stat database.inline*	Shows statistics for databases with views that use inline indexing.

9.0.1 FP9 & Verse On Prem (VOP) 1.0.2

- Verse on Prem benötigt 9.0.1 FP9
- Und andersrum 9.0.1 FP9 sollte nur mit VOP 1.0.2 verwendet werden
- Zuest FP9 und dann VOP 1.0.2 installieren!
- Notes 9.0.1 FP9 Mail template beinhaltet die benötigten Views für VOP
- Weitere Infos
  - https://www.ibm.com/support/knowledgecenter/en/SS4RQV_1.0.2/whats_new/wn_102.html

Überprüfung der Client Version aus der Applikation

- **Session.NotesVersion** gibt die volle Notes Version aus
- @Version gibt imer noch **405** aus.
- Ab FP 8 gibt es eine neue Option **@Version(1)**
- **Ausgabe: FP 8 = 8, FP 9 = 9**
- Wird im Mail-Template verwendet und ist mittlerweile dokumentiert in einer TN
- In älteren Versionen gibt **@Version(1)** den Wert **0** zurück
- Interessant: Im Design findet man auch eine Prüfung auf Build „410“ ...

Neue „Features“ in Fixpack 7 und früher

Linux 64Bit Fix

- Austausch aller Binaries in FP7
  - Neuere Linux Versionen liefern längere Thread-IDs, die nicht in die interne Struktur paßt
  - Neu-Compile nötig für eine interne Strukturänderung (SPR# KBRN9Q7EZW)
  - Crash in bestimmen Hochlast-Situationen
- Problem Linux 64bit Cluster Replicator Hang nach FP7 Installation
  - Nicht aller Code wurde durch den FP Installer ersetzt bei FP7
  - SPR# KBRN9Q7EZW → Fixed in Domino **9.0.1 FP7 IF1** und **FP8** (nur für Linux64)

Domino FP Größen auf Linux und FP Backup

- FP Installer sichern Binaries der Fixpacks im Binary Directory
- Beispiel /opt/ibm/domino/notes/latest/Linux
  - 431M 901FP5
  - 433M 901FP6
  - **516M 901FP7**
  - 293M 901FP8
  - 2.3M 901FP7HF92/
  - 110M 901FP5HF416/
  - 115M 901FP4HF423/
- Unter Windows gibt es nur einen Release901 Ordner mit IIB Files (ca. 400 MB)

- Größe oft problematisch wenn für /opt ein eigenes File-System verwendet wird
- Tip: Aufräumen der älteren FPs (+ Daten im „**data1_bck**“ Ordner)

Überblick / Zusammenfassung TLS Fixes

- Seit November 2014 Security Fixes in jedem Fixpack und vielen Interims Fixes
  - 9.0.1 FP2, 9.0, 8.5.3 FP6, 8.5.2 FP4, 8.5.1 FP5
  - Überblick der aktuellen Fixe im Anhang
- Aktuell TLS 1.2 mit aktuellen ECDHE Ciphern
  - Weitere Details siehe Anhang

9.0.1 FP7 - AES and SHA-2 Support for Network Port Encryption

- Braucht Client and Server muß FP7 oder höher sein

- 2 Neue Notes.ini Parameter

  - **PORT_ENC_ADV**

    - Kontrolliert den Level der Port-Verschlüsselung und aktiviert die Verwendung von AES Tickets
    - Muß auf dem Server aktiviert werden!

  - **TICKET_ALG_SHA**

    - Entscheidet welcer Crypto-Algorithmus verwendet wird um Tickets zu generieren.
    - HMAC-SHA 256 ist im Standard aktiviert

Notes.ini „PORT_ENC_ADV“

- **1** - Enable **HMAC-SHA256** integrity protection for the legacy **RC4** port encryption.
  - Only useful for resource constrained servers that cannot handle **AES** encryption.
- **2** - Enable **AES-128 CBC** rather than **RC4** for confidentiality and **HMAC-SHA256** for integrity.
  - At this time, IBM recommens using **AES-GCM** rather than **AES-CBC**.
- **4** - Enable **AES-128 GCM** for confidentiality and integrity.
  - Current industry best practices indicate that 128 bit symmetric keys are strong enough to guard against attacks based on the classical laws of physics.
- **8** - Enable **AES-256 GCM** for confidentiality and integrity.
  - 256 bit keys are expected to provide "128-bit level" protection against attacks based on quantum computing. If AES-256 GCM is enabled without Forward Secrecy, AES-128 GCM is used instead.
- **16** - Enable Forward Secrecy for port encryption using 2048 bit ephemeral Diffie-Hellman
- **64** - Enable AES tickets
  - Upgrades tickets from RC2-128 to AES-128. Performance impact is minimal.

Notes.ini „TICKET_ALG_SHA“

- Ticket Algorithmus
  - SHA 256 ist eine gute Wahl
  - Default, keine Konfiguration nötig

- Referenz:
  - **1** - HMAC-SHA 1
  - **256** - HMAC-SHA 256 (Enabled by default; no configuration needed.)
  - **384** - HMAC-SHA 384
  - **512** - HMAC-SHA 512

Best Practices / Performance

- **PORT_ENC_ADV=84 (Best Practice)**
  - (4) Enable AES-128 GCM for port encryption and transport integrity
  - (16) Forward Secrecy
  - (64) Enable AES tickets

- **PORT_ENC_ADV=88 (Maximum Security)**
  - (8) AES-256 GCM for port encryption and transport integrity
  - (16) Forward Secrecy
  - (64) AES tickets

- **PORT_ENC_ADV=65 (Minimum Overhead)**
  - (1) HMAC-SHA256 for transport integrity and continue to use 128-bit RC4 for network traffic.
  - (64) AES tickets

Port Encryption Logging

- **log_authentication=1**

- Neue Debug-Einstellung **DEBUG_PORT_ENC_ADV=1**

```
FP 6
Authenticate {1B3F0009}: CN=xyz/OU=Srv/O=NashCom-Net
T:RC2:128 E:1:  P:c:e S:RC4:128 A:4:1 L:N:N:N FS:


FP 7
Authenticate {1B3F0002}: CN=xzy/OU=Srv/O=NashCom-Net
T:AES:128 E:1:  P:c:e S:AES-GCM:256 A:2:1 L:N:N:N FS:DHE-2048
```

FP 7 - Neue Option zur Notes Verschlüsselung mit AES 128/256

- Neuer Parameter, der die aktuellen Regeln überschreibt
  - Anforderungen an Schlüssellänge, Einstellungen im Person-Doc wie FIPS Algorithmen
- Parameter zur Aktivierung der AES Verschlüsselung ohne spezielle Anforderungen
- Notes.init **PREFER_AES** auf der Maschine, die die Mail absendet
  - 128 oder 256 für AES 128 oder AES 256
- Verwendet für die Bulk Verschlüsselung – Symmetischer Key
- Wird nur für neue Verschlüsselungen verwendet.
  Keine automatische Neuverschlüsselung!

Bekannte Probleme in 9.0.1 FP7

- SPR # BBSZAEEK8C APAR #LO90429.: Notes User Id File Upload To Vault Failed If Port_enc_adv Parameter Is Enabled
  - Gefixed in FP 8
  - Workaround: Neue Verschlüsselung noch nicht auf dem ID-Vault-Server zu verwenden
- iNotes Probleme mit nicht US Locale → iNotes Fehler direkt beim Öffnen
  - Gerfixed in iNotes 901FP7IF2 und FP8

Bekannte Probleme in 9.0.1 FP7

- CD zu MIME Konvertierung auf dem Server erzeugt JavaScript Code
  - SPR #AJASAEHJKB - Reply Section Or Twistie In A Cd-mime Conversion Is Converted Incorrectly
  - Gefixed in FP8
  - Antwort des Entwicklers in meinem Blog:

    Sorry about that. This regression was caused by a change I made to browser.cnf to let sections work with the edge browser. I neglected to take the HAPI use case into consideration. A hotfix for this SPR is now available.
  - A workaround would be to edit browser.cnf as follows:

    Property DHTMLSections String Standard
    to
    Property DHTMLSections String None

FP6 – Soft Deletions

- Seit Domino 9 werden Soft-Deletions nur noch von der updall Task gelöscht
  - Nicht mehr wir in Domino 8.5.x bei jedem Datenbank Öffnen
- Neuer Notes.ini Parameter **CHECK_EXPIRED_SOFT_DELETES_ON_DBOPEN=1**
  - Bringt das 8.5.x Verhalten zurück
- Referenz: SPR# HYYH9DF5GR
  - Fixes situation where emails in trash are not removed even if "Permanently delete documents after X hours" is set.
    This fix introduced a new Notes.ini CHECK_EXPIRED_SOFT_DELETES_ON_DBOPEN=1.
    This is off be default.

FP6 - Keyrollover Fix für ID-Vault

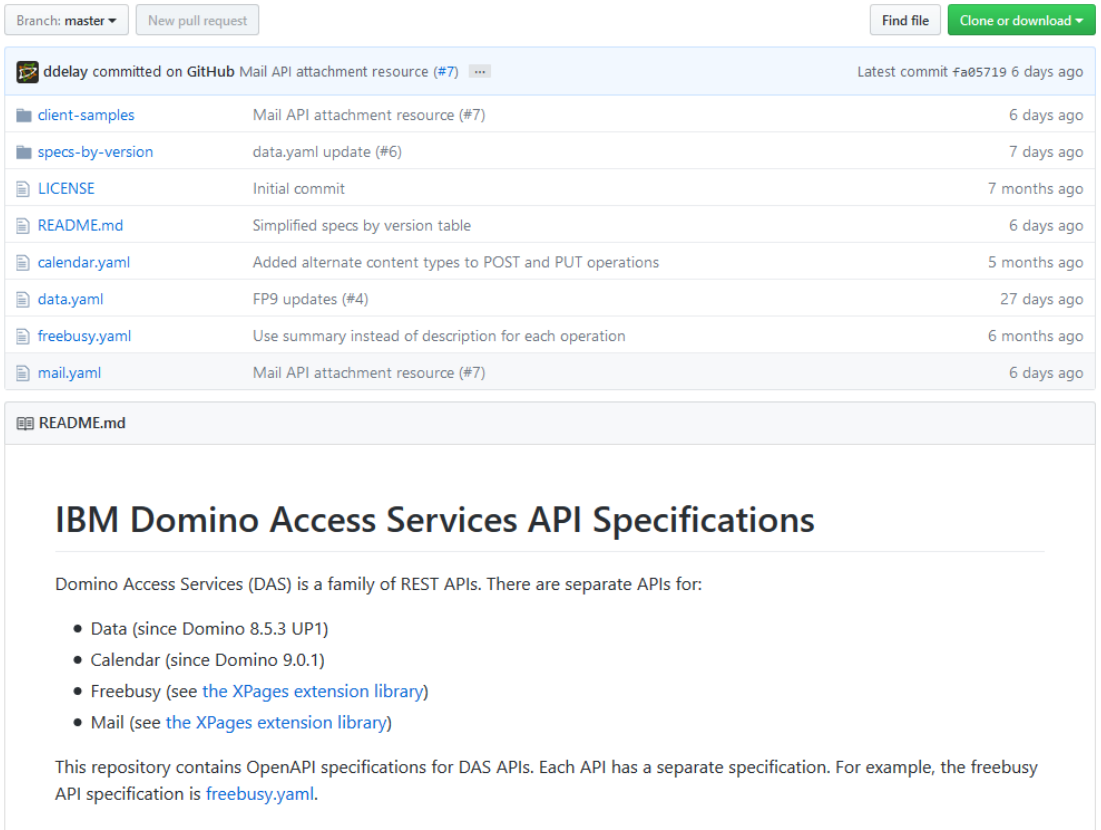
- Probleme mit Key-Rollover und ID Vault
- Der Fix ist aus Perfomance-Gründen deaktiviert
- Aktivieren über Notes.ini **IDV_RefreshCerts=1** auf den Vault-Servern
  - Sollte nur für Key-Rollover aktiviert sein
- Reference: SPR# KLYH9ZDQNC
  IDVault Key Rollover State Can Be Incorrect Due to Timing Issue

Notes/Domino 9.0.1 Feature Pack 8 Dokumentation

- Einstieg
  - http://www.lotus.com/ldd/fixlist.nsf/8d1c0550e6242b69852570c900549a74/26aa7417bb60f7df852580b40072af2d
- What's new in IBM Notes Feature Pack 8/9?
  - https://www.ibm.com/support/knowledgecenter/SSKTWP_9.0.1/fram_newFP8_r.html
  - https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/over_whats_new_in_fp9.html
- What's new in IBM Domino 9.0.1 Social Edition Feature Pack 8/9
  - https://www.ibm.com/support/knowledgecenter/SSKTMJ_9.0.1/admin/over_whats_new_in_fp8.html
  - https://www.ibm.com/support/knowledgecenter/en/SSKTMJ_9.0.1/admin/over_whats_new_in_fp9.html
- What's new in IBM Domino Designer 9.0.1 Social Edition Feature Pack 8?
  - https://www.ibm.com/support/knowledgecenter/SSKTWP_9.0.1/fram_newFP8_r.html

Wichtige OpenNTF Seite für das REST API

- OpenNTF / das-api-specs repository
  - https://github.com/OpenNTF/das-api-specs



Branch: master ▾ | New pull request | Find file | Clone or download ▾

ddelay committed on GitHub Mail API attachment resource (#7) ··· Latest commit fa05719 6 days ago

client-samples	Mail API attachment resource (#7)	6 days ago
specs-by-version	data.yaml update (#6)	7 days ago
LICENSE	Initial commit	7 months ago
README.md	Simplified specs by version table	6 days ago
calendar.yaml	Added alternate content types to POST and PUT operations	5 months ago
data.yaml	FP9 updates (#4)	27 days ago
freebusy.yaml	Use summary instead of description for each operation	6 months ago
mail.yaml	Mail API attachment resource (#7)	6 days ago

README.md

IBM Domino Access Services API Specifications

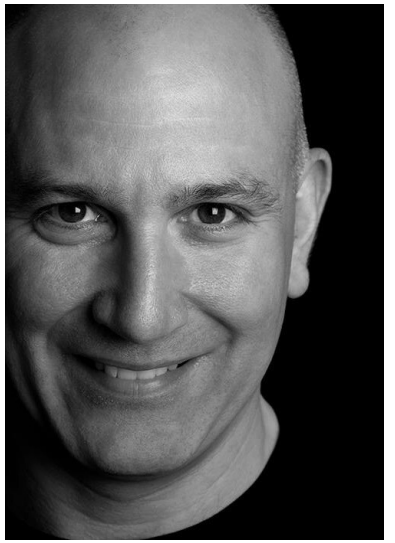
Domino Access Services (DAS) is a family of REST APIs. There are separate APIs for:

- Data (since Domino 8.5.3 UP1)
- Calendar (since Domino 9.0.1)
- Freebusy (see the XPages extension library)
- Mail (see the XPages extension library)

This repository contains OpenAPI specifications for DAS APIs. Each API has a separate specification. For example, the freebusy API specification is freebusy.yaml.

Fragen & Antworten

- Offene Fragen?
  - Jetzt oder später per Mail
  - Aktuelle Informationen in meinem Blog
- Feedback?
- Kontakt
  - nsh@nashcom.de
  - http://blog.nashcom.de



IBM CHAMPION

Nash!Com
Communication Systems

Domino Security Update

Nash!Com
Communication Systems

Referenz BSI Whitepaper – 11.2.2015

- **BSI TR-02102-1 "Kryptographische Verfahren: Empfehlungen und Schlüssellängen"**
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102_pdf
- Block Ciphers:
  - AES-128, AES-192, AES-256 with
    - Galois-Counter-Mode (**GCM**)
    - Cipher-Block Chaining (**CBC**)
    - Counter Mode (CTR)
- Asymmetric Encryption:
  - ECIES 224 (after 2015 at least 250), DLIES and RSA >= 2048 Bits (after 2016 at least >= 3072 bits)
- Hashing: SHA-224, SHA-256, SHA-512/256, SHA-384, SHA-512, SHA-512/224
  - **SHA1 nicht mehr für neue Certs** → Nach 2015 nur noch: SHA-256, SHA-384, SHA-512, SHA-512/256
- Key Exchange:Diffe-Hellma (**DHE_RSA**)/ EC Diffe-Hellman (**ECDHE_RSA**)

Apple Transport Security (ATS)

- Apple führt neuen Sicherheits-Standard (ATS) ein
- Wird bei iOS 9 und OSX 10.11 (El Capitan) verwendet

- Anforderungen
  - TLS 1.2
  - >= 2048 bit RSA Key
  - Mindestens SHA-256 Signierte Web-Server Zertifikate
  - **ECDHE** → PFS supported, moderne Cipher

- Bisher wird dieser Standard nur für Applikationen erzwungen
  - Wenn der Entwickler die Applikation nicht mit entsprechenden Ausnahmen compiled hat
  - Es ist aber zu erwarten, daß Apple in den nächsten Releases die Anforderungen weiter festzieht

Domino TLS Support!

- IBM hat aufgrund von Sicherheitsproblemen wie dem SSL V3 Bug „Poodle“ schrittweise neuere SSL/TLS Versionen eingeführt
  - „Poodle“ und andere Probleme haben den ursprünglichen Zeitplan, geändert
  - Funktionen wurden durch Fixpacks und Interims-Fixe bereitgestellt
- Aktuelle Version: Domino 9.0.1 FP7
  - Support für TLS 1.2 inklusive aktueller **DHE und ECDHE** Ciphers
  - Empfehlung: Update auf die aktuelle 9.0.1 Version mit FP und IF!!!
  - Domino 8.5.3 wird kein TLS 1.2 und kein SHA-256 supporten!

Aktuelle Änderungen

- TLS 1.2
  - Verwendet intern SHA-256 statt MD5/SHA-1
- Neue Cipher
  - **A**dvanced **E**ncrption **S**tandard (**AES**) **G**alois/**C**ounter **M**ode (**GCM**)
  - **P**erfect **F**orward **S**ecrecy (**PFS**) via
    - Ephemeral **D**iffie-**He**llman (**DHE**)
    - **E**lliptic **C**urve **D**iffie-**He**llman (**ECDHE**)
- Support für “Secure Renegotiation”
- HSTS (**H**ttp **S**trict **T**ransport **S**ecurity)
  - Header Information, daß der Browser über HTTPS zugreifen soll

Referenz - Aktueller Cipher Support – Teil 1

- Alle Cipher in der Reihenfolge ihrer Verwendung von Server-Seite
- **ECDHE** und **DHE** Cipher
  - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0x**c030**) ECDH 256 bits (eq. 3072 bits RSA)
  - TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0x**9f**) DH 2048 bits (p: 256, g: 1, Ys: 256)
  - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0x**c02f**) ECDH 256 bits (eq. 3072 bits RSA)
  - TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0x**9e**) DH 2048 bits (p: 256, g: 1, Ys: 256)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0x**c028**) ECDH 256 bits (eq. 3072 bits RSA)
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (0x**6b**) DH 2048 bits (p: 256, g: 1, Ys: 256)
  - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0x**c014**) ECDH 256 bits (eq. 3072 bits RSA)
  - TLS_DHE_RSA_WITH_AES_256_CBC_SHA (0x**39**) DH 2048 bits (p: 256, g: 1, Ys: 256)
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0x**c027**) ECDH 256 bits (eq. 3072 bits RSA)
  - TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (0x**67**) DH 2048 bits (p: 256, g: 1, Ys: 256)
  - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0x**c013**) ECDH 256 bits (eq. 3072 bits RSA)

Referenz - Aktueller Cipher Support – Teil 2

- RSA **AES GCM** Cipher
  - TLS_RSA_WITH_AES_256_GCM_SHA384 (0x**9d**)
  - TLS_RSA_WITH_AES_128_GCM_SHA256 (0x**9c**)
- RSA **AES CBS** Cipher
  - TLS_RSA_WITH_AES_256_CBC_SHA256 (0x**3d**)
  - TLS_RSA_WITH_AES_256_CBC_SHA (0x**35**)
  - TLS_RSA_WITH_AES_128_CBC_SHA256 (0x**3c**)
  - TLS_RSA_WITH_AES_128_CBC_SHA (0x**2f**)
- RSA **3DES** Cipher
  - TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x**a**)

Cipher manuell konfigurieren

- Der „Cipher Dialog“ im Server Dokument und Internet-Site Dialog wird bis zum nächsten Feature Release nicht mehr verwendet
- Per Default sind aktuell sichere Cipher konfiguriert
- Änderungen an der Cipher Liste erfolgt über einen notes.ini Eintrag für alle Protokolle

  notes.ini Eintrag **SSLCIPHERSPEC=...**

  - Enthält die Codes der Cipher aneinander gehängt
  - Vor 9.0.1 FP4 IF2 gab es nur 2 Octet Codes
  - Jetzt sollten 4 Octet Codes verwendet werden
- Beispiel mit gemischtem 2 / 4 Octet Format:

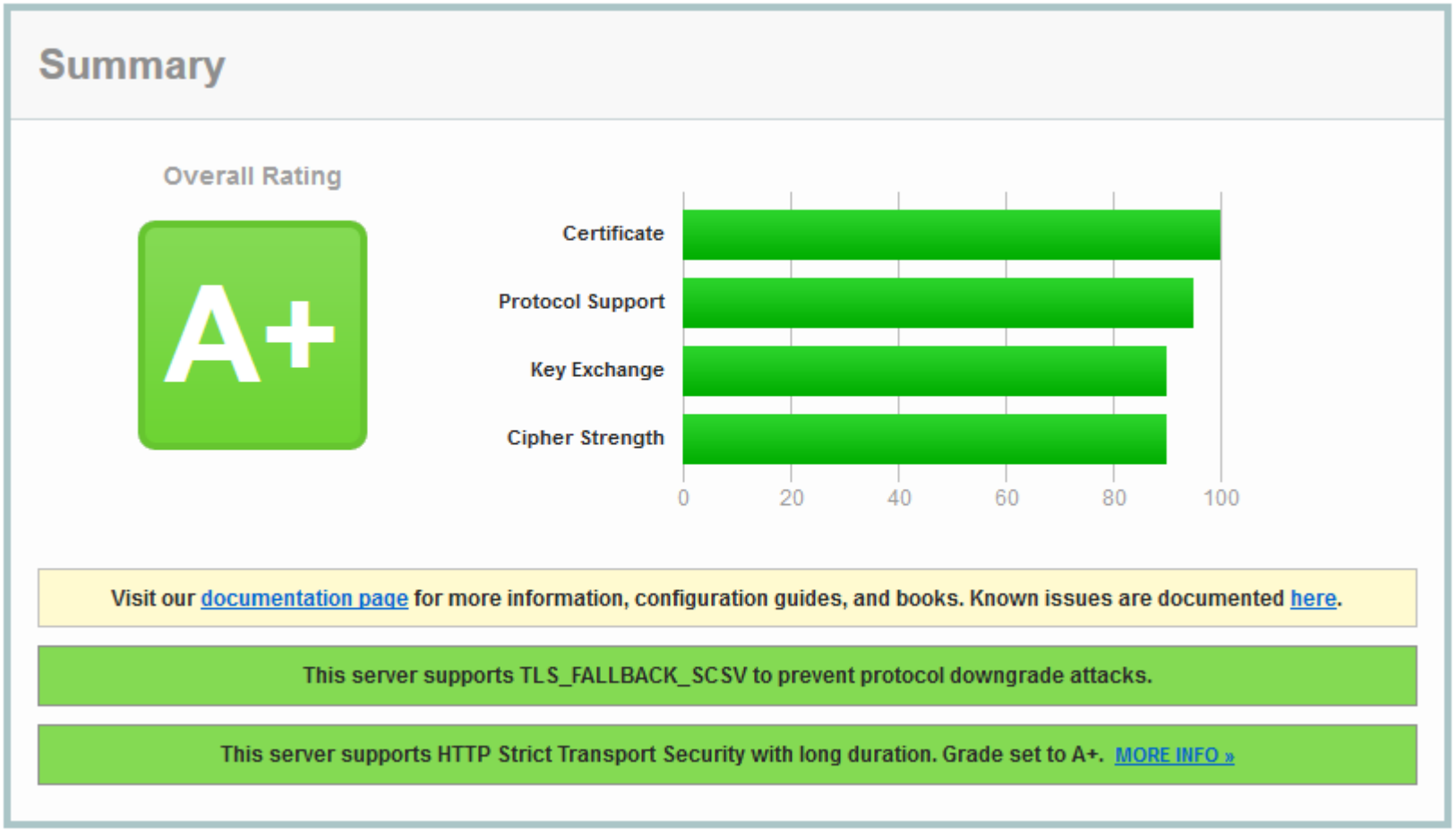
  - **SSLCIPHERSPEC**=9D9C**3D**3C352F0A39676B9E9F**C030**C02FC028C014C027C013

  - Blog-Eintrag: http://www.lotus.com/ldd/dominowiki.nsf/dx/TLS_Cipher_Configuration

Referenz - SSL Test Tools

- Eine der meist verwendeten SSL Test-Websites
  - Gibt einen guten Überblick über die SSL/TLS Sicherheit des eigenen Servers
  - Rating von "**A**" bis "**F**"
  - Detail Information über TLS Version und Cipher
    - „Simulation" welcher Cipher von welchem Client-Typ verwendet wird
- Server Test
  - https://www.ssllabs.com/ssltest/
- Client Test
  - https://www.ssllabs.com/ssltest/viewMyClient.html

Aktueller Status



Nash!Com
Communication Systems

Aktuelle SSL/TLS Parameter

- **DISABLE_SSLV3=1**
  - Empfohlen und wichtig: Deaktiviert SSL V3
- DEBUG_SSL_ALL=2
  - Oder nur **DEBUG_SSL_HANDSHAKE=2** und **DEBUG_SSL_CIPHERS=2**
- USE_WEAK_SSL_CIPHERS=1
  - Nicht empfohlen! IBM stellt sicher, daß aktuelle Cipher vorhanden sind
- SSL_ENABLE_INSECURE_RENEGOTIATE=1
  - Nicht empfohlen! Ist nur aus Compatibilitäts-Gründen noch vorhanden
- SSL_DISABLE_FALLBACK_SCSV=1
  - Nicht empfohlen! Deaktiviert TLS_FALLBACK_SCSV wenn Client es nicht (richtig) supporten
- SSL_USE_CLIENT_CIPHER_ORDER=1
  - Nicht empfohlen! Erlaubt Clients die Cipher Order anzugeben

Logging - SSL/TLS Fehler

- Neues Logging auch ohne Debug Einstellungen
  - Kann via notes.ini **SSL_LOGGING_DISABLE=1** deaktiviert werden
- Log-Beispiele:
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(1263) failed with server certificate chain requiring support for SHA384
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(3829) failed with no supported ciphers
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(3416) failed with rejecting incoming SSLv3 connection
  - TLS/SSL connection 1.2.3.4(443)-4.5.6.7(1263) failed with server certificate chain signature alogrithms NOT supported by client

Extended Master Secret Extension

- D 9.0.1 FP5 IF1 supportet das Extended Master Secret Extension with TLS 1.2
  - Recht neue RFC, die neben von Google und Microsoft supportet wird
  - Windows 2008 R2 supported nur TLS 1.0 aber sendet trotzdem die Extended Master Secret Extension in im Server Helo.
  - Domino kann sich nicht verbinden weil der Server die Extended Master Secret Extension verwenden will
  - Das Problem tritt zum Beispiel bei LDAP AD Anfragen via Directory Assistance auf
- Work-Around um das Microsoft-Problem zu umgehen
  - Deaktivierne via notes.ini **SSL_DISABLE_EXTENDED_MASTER_SECRET=1**
- Neuere Versionen supporten TLS 1.2 und haben das Problem nicht mehr
- Referenz & Details → http://www.ibm.com/support/docview.wss?uid=swg21987608

SHA-256 (SHA-2) Support

- Domino 9.0.x ohne die neuen Fixe supportet SHA-256 bereits in machen Bereichen
  - X.509 S/MIME Verschlüsselung und Signatur
  - HTTP Passwort Hashing (Intern)
  - Internet CA supportet SHA-256
- Domino >= 9.0.1 FP2 IF1 supportet SHA-2 Zertifikate für alle Internet Protokolle und für Keyring Files
  - SHA-2 Support: SHA-256, SHA-384 und SHA-512
  - **Kein Support für SHA-2 in Domino 8.5.3**
- Neues Keyring File Management Tool "**kyrtool**"

Referenz - Neues Keyring Tool - “kyrtool”

- Separater Download
  - Win32/64, Linux 32/64 Client & Server → einfach in das Notes/Domino Programmverzeichnis kopieren
- Importieren, Anzeigen show und Exportieren von Zertifikaten
  - Aber kann keine Keys erzeugen oder Zertifikate Anforderungen erstellen
- OpenSSL für das Erzeugen von Key-Paaren und Zertifikats-Anforderungen („CSR“)
  - Viele andere Tools können verwendet werden
  - Oder bestehende Zertifikate im PEM Format
- Importieren von „Trusted Roots“
  - Entweder alle zusammen aus einer PEM Datei in richtiger Reihenfolge (Key, cert, intermediates, Root)
  - Oder separater Import

Referenz - Beispiel: Zertifikat mit OpenSSL erstellen

- OpenSSL
  - Nativ auf Linux/Unix installiert
  - Oder auf Windows z. B. In einer cygwin Umgebung

- 1. Erstellen Private/Public Key
  - **openssl genrsa -out server.key 2048**

- 2. Erstellen des „Certificate Signing Request“ (CSR)
  - **openssl req -new -sha256 -key server.key -out server.csr**

- 3. Senden CSR zur CA
  - Oder erstellen eines “self signed” Zertifikates für eine Test-Umgebung
    - **openssl x509 -req -days 3650 -sha256 -in server.csr -signkey server.key -out server.pem**

  - **Resultat sollte immer im “PEM” Format sein**

Referenz - Verify Import File

- Inhalt einer PEM Datei sollte vor dem Import immer „verifiziert“ werden
  - Sicherstellen, daß die Zertifikates-Kette vollständig ist und aufeinander aufbaut
    - **Key, Cert, Intermediate Certs, Root Cert**
  - **Special Tip:** Anzeigen der Certs in einer Eingabe-Datei
    - Example: **kyrtool.exe show certs -i c:\domino\all.pem**

- **kyrtool.exe verify c:\domino\all.pem**
  - Successfully read 2048 bit RSA private key
  - INFO: Successfully read 4 certificates
  - INFO: Private key matches leaf certificate
  - INFO: IssuerName of cert 0 matches the SubjectName of cert 1
  - INFO: IssuerName of cert 1 matches the SubjectName of cert 2
  - INFO: IssuerName of cert 2 matches the SubjectName of cert 3
  - INFO: Final certificate in chain is self-signed

Referenz - Keyring File erstellen

- Erstellen des Keyring Files
  - **kyrtool create -k keyring.kyr -p password**
  - Beim Erstellen muß ein Passwort eingegeben werden
    - Alle anderen Commands lesen das Passwort aus der **“.sth” Datei**
- Importieren von Key, Certificate, Intermediates und Trusted Root
  - Kopieren von Key, Cert, Intermediates und Root Certificate in ein PEM file
  - **kyrtool import all -k keyring.kyr -i server.pem**
- Separates Importieren der unterschiedlichen Teile ist auch möglich
  - **Kyrtool import all|keys|certs|roots -k keyring.kyr -i server.pem**
  - Aber ist weitaus komplizierter und Fehler anfälliger

Referenz - Keyring “show” Command

- Wird verwendet um Informationen aus dem Domino Keyring File anzuzeigen

- **Kyrtool show certs -k keyfile.kyr**
  - Zeitgt die komplette Zertifikateskette inklusive es entsprechenden Root Certs
  - Tip: Dump aller Zertifikate und Überprüfung via „verify“

- **Kyrtool show keys -k keyfile.kyr**
  - Zeigt alle Keys im Keyring File

- **Kyrtool show roots -k keyfile.kyr**
  - Zeigt alle Trusted Roots im Keyring File

- Verbose Pption “-v” kann verwendet werden für mehr Informationen
  - Mehrere “-v”s bedeuten mehr Informationen

Referenz – Konvertierung von Formaten

- Kyrtool benötigt das “PEM” Format (Text basiert - BASE64 encoded DER format)
  - In vielen Fällen verwendet die CA binäre Formate (z.B. Microsoft CA)

- OpenSSL hilft bei der Konvertierung
  - Aber der Syntax ist nicht immer naheliegend

  - Konvertier PKCS#12 file (.pfx .p12) – Datei mit Keys und Certs
    - **openssl pkcs12 -in cert.pfx -out cert.pem -nodes**

  - Konvertiert das binäre DER Zertifikates-File in das (BASE64 kodierte) PEM Format
    - **openssl x509 -inform der -in server.cer -outform pem -out server.pem**

  - Konvertiert die binär DER kodierte Zertifikates-Kette in das (BASE64 kodierte) PEM Format
    - **openssl pkcs7 -print_certs -inform der -in certificate_chain.p7b -outform pem -out chain.pem**

Referenz – Hilfreiche OpenSSL Commands

- Connect Test HTTPS
  - **openssl s_client -connect www.acme.com:443**
- Connect Test SMTP TLS
  - **openssl s_client -connect mail.acme.com:25 -starttls smtp**
- Beide geben Information über Protokoll und Cipher etc aus
- Optionen um bestimmte SSL/TLS Versionen zu verwenden
  - **-tls1, -no_tls1, -no_ssl3**
- "wget"
  - Verwendet OpenSSL Libs und kann für HTTPS Anfagen verwendet werden
  - **wget.exe [--secure-protocol=TLSv1] --no-check-certificate https://www.acme.com**