



Užitečné rady pro administrátory

IBM Domino/Notes



Radim Turoň
©2015

Úvod



- Podkladem této prezentace jsou přednášky uveřejněné na konferencích Lotusphere a ConnectED 2012-2015, přednášky a webové konference Paula Mooneyho, Daniela Nasheda, technických týmů IBM a také jsem čerpal přímo z technické dokumentace k systému IBM Notes.
- Vybral a upravil jsem pro vás některé tipy a triky z těchto přednášek a dokumentů a doplnil je dalšími poznatky z naší technické dílny.



Tip #1 Nová verze ODS52

- K dispozici ve verzi R9.0.1
- Nastavení nového formátu
 - V serverovém notes.ini nastavte **Create_R9_Databases=1**
 - Pro změnu stávající ODS na novou ODS52 na databázi, proveďte kompaktaci databáze copy stylem (load compact -c ...)
 - ...nebo kompaktaci bez zamknutí databáze s parametrem -REPLICA (load compact -REPLICA)
- Nový formát opravuje
 - Porušení dokumentů ve středně a silně šifrovaných databázích
 - Porušení dokumentů s přílohami většími než 2GB
- Více v tomto odkazu
<http://blog.nashcom.de/nashcomblog.nsf/dx/details-about-ods-52-shipped-with-notesdomino-9.0.1.htm>



Tip #2 Internet Password Lockout

- Ochrana proti brute-force útokům na přístup přes internetové heslo
- Po nastaveném počtu neúspěšných autentizací zamyká přístup pro daného neúspěšně se autentizujícího uživatele
- Volitelně je možno logovat pokusy o neúspěšnou autentizaci a zamknutí přístupu (datum a čas, IP adresa, jméno uživatele)
- Nastavuje se v Configuration settings dokumentu → záložka Security
- Nevýhodou je možné zneužití - zamknutí uživatele „z legrace“
- Doporučuji všem nastavit!



Tip #3 Traveler - úklid neplatných zařízení, uživatelů

- Postupem času se v lotustraveler.nsf shromažďují nastavení pro již nepoužívaná mobilní zařízení
- Procházejte periodicky databázi traveler.nsf a sledujte, zda obsahuje jen záznamy pro aktuální zařízení (podle doby poslední synchronizace)
- Neplatné záznamy mažte příkazem:
tell traveler delete **Device_ID** „CN=Jméno Uživatele/O=Organizace“
 - kde **Device_ID** naleznete na záznamu neplatného mobilního zařízení

Device Name	samsung GT-P7510
Device ID	Android_ce87e44140ffdb36
Connection State	Disconnected



Tip #4 Database User Activity

- Loguje aktivitu uživatelů v databázi
- Maximálně 1440 záznamů
- Povoluje se ve vlastnostech databáze, standardně zapnuto na všech databázích
- NOTES.INI proměnná NO_FORCE_ACTIVITY_LOGGING=X
 - X=0 -(default) statlog task zapíná logování aktivity na všech databázích na serveru
 - X=1 -statlog task vypíná logování aktivity na všech databázích na serveru
- Activity is confidential - log uvidí pouze uživatelé s přístupem Designer a vyšší

Date/Time	Reads	Adds	Updates	Deletes	User
25. 01. 2013 01:01:29	0	0	6	3	Orion/TCL-DigiTrade
24. 01. 2013 15:56:06	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:55:29	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:55:04	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:54:24	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:54:14	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:53:33	4	0	0	0	Radim Turon/TCL-DigiTrade
24. 01. 2013 15:53:32	4	0	0	0	Radim Turon/TCL-DigiTrade

	Total	Uses	Reads	Adds	Updates	Deletes
Last Day	0	0	0	0	0	0
Last Week	8	2	15	5	0	0
Last Month	18	5	22	8	0	0
Last 849 Days	1400	7399	963	2213	313	0

Record activity Activity is confidential Copy to clipboard OK Cancel



Tip #5 Database User Activity – co se loguje?

- Do verze ODS48



- ODS48 a vyšší



User Activity

Date/Time	Reads	Writes	User
23. 05. 2015 14:46:02	2	0	Merkur/TCL-DigiTrade
23. 05. 2015 14:26:44	1	0	Radim Turon/TCL-DigiTrade
23. 05. 2015 14:16:41	1	0	Radim Turon/TCL-DigiTrade
23. 05. 2015 14:16:30	4	2	Orion/TCL-DigiTrade
23. 05. 2015 14:15:56	1	0	Merkur/TCL-DigiTrade
23. 05. 2015 14:15:26	4	2	Orion/TCL-DigiTrade
23. 05. 2015 14:14:41	4	2	Orion/TCL-DigiTrade
23. 05. 2015 12:44:57	1	0	Merkur/TCL-DigiTrade

Record activity Activity is confidential Copy to clipboard OK Cancel

User Activity

Date/Time	Reads	Adds	Updates	Deletes	User	Total	Uses	Reads	Adds	Updates	Deletes
23. 05. 2015 05:40:05	1	0	0	0	Merkur/TCL-DigiTrade						
23. 05. 2015 05:09:57	1	0	8	0	Merkur/TCL-DigiTrade	Last Day	6	6	0	17	0
23. 05. 2015 02:00:01	1	0	0	0	Orion/TCL-DigiTrade	Last Week	78	94	5	119	0
23. 05. 2015 02:00:01	1	0	0	0	Orion/TCL-DigiTrade	Last Month	502	922	42	627	29
23. 05. 2015 01:30:43	2	0	1	0	Merkur/TCL-DigiTrade	Last 82 Days	1400	2483	105	1620	130
23. 05. 2015 01:01:33	0	0	8	0	Orion/TCL-DigiTrade						
22. 05. 2015 05:36:48	1	0	0	0	Merkur/TCL-DigiTrade						
22. 05. 2015 05:06:40	1	0	8	0	Merkur/TCL-DigiTrade						

Record activity Activity is confidential Copy to clipboard OK Cancel



Tip #6 Compact Replication

- Nová varianta replikace od verze R8.5.3.3
- Pro spuštění se zadává parametr `-replica`
load compact -replica *volitelné.parametry* jmeno_db
- Používá se např. v případě, že při copy-style replikaci databáze vypisuje chyby „Insufficient memory“ nebo „Unable to extent an ID table – insufficient memory“
- Reorganizuje ID Table, vhodné použít pro databáze, kde je historicky ID tabulka velmi fragmentována nebo hrozí její zaplnění
- Nenahrazuje copy-style replikaci, spíše ji doplňuje
- Bližší info naleznete zde
<http://www-01.ibm.com/support/docview.wss?uid=swg27039379>



Tip #7-1 Anatomie NoteID

- UNID (Universal Note ID)

Identifikuje dokument ve všech replikách - nemění se při modifikaci dokumentu.
Pokud se vytvoří nová kopie databáze, UNID dokumentu se změní!

ID: OF0000039D:3836C29F-ON85255DC9:0056FB94
SD00255DF4:0057B8FA-SN00000003
DB85255CD9:00567287-NT0000C092

- OID (Originator ID)

Identifikuje konkrétní revizi dokumentu nezávisle na databázi.
Mění se s každou modifikací dokumentu (mění se pouze SD a SN).

ID: OF0000039D:3836C29F-ON85255DC9:0056FB94
SD00255DF4:0057B8FA-SN00000003
DB85255CD9:00567287-NT0000C092



Tip #7-2 Anatomie NoteID

- NID (Note ID)

Identifikuje konkrétní dokument v dané databázi.

Neobsahuje informaci o databázi.

Nemění se při modifikaci dokumentu.

ID: OF0000039D:3836C29F-ON85255DC9:0056FB94

SD00255DF4:0057B8FA-SN00000003

DB85255CD9:00567287-NT0000C092

- GNID (Global Note ID)

Database ID + Note ID.

Identifikuje konkrétní dokument v konkrétní databázi.

Každá replika dokumentu bude mít jiné GNID.

Nemění se při modifikaci dokumentu.

ID: OF0000039D:3836C29F-ON85255DC9:0056FB94

SD00255DF4:0057B8FA-SN00000003

DB85255CD9:00567287-NT0000C092



Tip #7-3 Anatomie NoteID

- IID (Instance ID)
Identifikuje konkrétní revizi dokumentu v dané databázi.
Neobsahuje informaci o databázi.
Mění se při modifikaci dokumentu.

- GIID (Global Instance ID)
Identifikuje konkrétní revizi dokumentu v konkrétní databázi.
Obsahuje informaci o databázi.
Mění se při modifikaci dokumentu.



Tip #7-4 Anatomie NoteID

- K čemu slouží jednotlivé položky Note ID:
 - UNID a OID
Replikace dat.
 - NID
Identifikuje dokument v databázi.
Pozice dokumentu v souboru.



Tip #8 Logování status baru na klientovi

- Užitečné při řešení problémů na klientovi
- Nastavte do NOTES.INI klienta proměnnou **LogStatusBar=1**
- Vše, co se objeví ve status baru, je logováno do log.nsf na klientovi

Miscellaneous Events:

```
25.05.2014 17:28:19 Status Msg: Prompting for password
25.05.2014 17:28:32 Status Msg: Using application on Local
25.05.2014 17:28:46 Status Msg: Note item not found
25.05.2014 17:28:47 Status Msg: 1 document selected
25.05.2014 17:28:50 Status Msg: Background replication/sync request submitted
25.05.2014 17:28:54 Status Msg: 2 documents selected
25.05.2014 17:28:54 Dynamic Client Configuration started
25.05.2014 17:28:54 Initializing Dynamic Client Configuration
```



Tip #9 Prevence náhodného smazání složky v poště

- Vyskytuje se velmi zřídka, ale již jsem zaznamenal několik případů
- Klient klávesou DEL smaže složku, na kterou je v navigátoru přepnut, v domněnání, že maže mail
- Nastavte do NOTES.INI klienta proměnnou **DisableDelKeyForNavigator=1**



Tip #10 Hromadné změny ACL mail databází

- Volně stažitelný nástroj Paula Mooneyho
 - www.pmooney.net/resources
- Vynikající v případě, že potřebujete změnit ve všech mailových databázích přístup vlastníka z Manager na Editor
- Poslední verze je 0.4 updatovaná Sebastianem Beckerem



Tip #11 Čištění databáze Rezervace prostředků

- Databáze „Rezervace prostředků“ je velká a obsahuje spoustu historických rezervací
- Problém mnoha dlouho používaných databází tohoto typu
- Zapněte agenta pro periodické čištění databáze od starých záznamů
- Agent maže všechny dokumenty starší než 2 dny

Name	Alias	Type
(Delete User Reservations)	Delete User R...	LotusScript
(DeletedResourceNotice)		LotusScript
(DeletePendingReservations)		LotusScript
(DeleteSelectedReservations)		LotusScript
(DisableBusytimeDetails)		LotusScript
(EnableBusytimeDetails)		LotusScript
(Update AllowBusyAccess)	Update Allo...	LotusScript
(wAppointmentOpen)		LotusScript
(wAppointmentSave)		LotusScript
(wEmptyTrash)		LotusScript
(wSiteOpen)		LotusScript
✘ Autoremind		LotusScript
Export do iCAL vybraných polož		LotusScript
✓ Purge Documents (Auto)		LotusScript
✘ RenameReservations and SendM	Rename	LotusScript
Show UNID		LotusScript
✘ Update Blocker Documents		LotusScript



Tip #12 NSF_DBCache_Maxentries

- Domino standardně uchovává ve své cache paměti 25 databází
- Přístup k těmto databázím je pak o mnoho rychlejší
- Pokud máme na serveru dostatek paměti, můžeme zvětšit počet databází uchovávaných v cache paměti
- V server NOTES.INI nastavte proměnnou **NSF_DBCache_Maxentries=X** ...kde X je počet databází uchovávaných v cache
- Statistická proměnná database.dbcache.hits zobrazuje, jak často byl požadavek nalezen v cache paměti
- Hodnota database.dbcache.hits by měla být vysoká, pokud je nízká, zvyšte počet databází v cache paměti



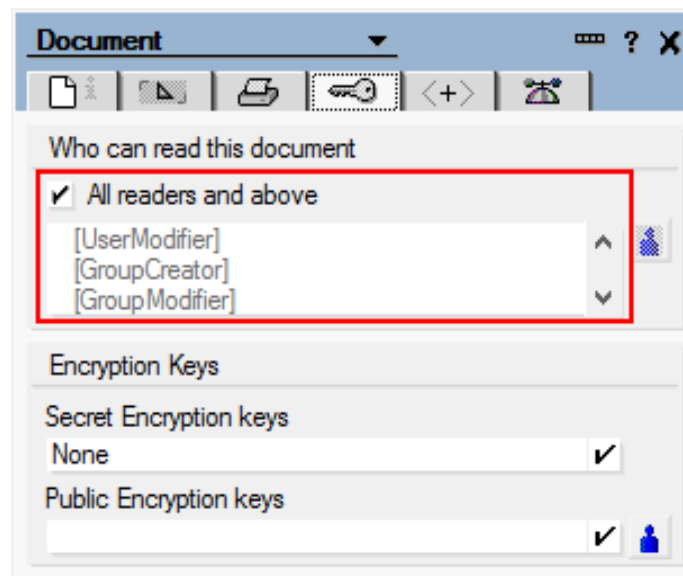
Tip #13 PIRC - Purge Interval Replication Control

- Novinka – od verze R8.5.3
- Pokud replikujeme databázi, u níž je datum poslední replikace daleko v minulosti, může dojít k přenesení již smazaných dokumentů ze staré neaktuální repliky zpět do aktuální repliky databáze (uživatel odcestuje pryč, po roce se vrátí a zreplikuje)
- Jak funguje PIRC – pokud je dokument starší než xx dnů, nereplikuj ho
- Události PIRC, které nastanou při replikaci naleznete v DDM
- Jak nastavit
 - Replication->Option for this Application->Space Savers->Enable Purge Interval Replication Control
 - load compact -PIRC On
 - IBM Administrator->záložka Files->vybrat jednu nebo více databází->pravé tlačítko myši a z menu vybrat „Advanced Properties“->položka „Purge interval replication control“
- Podrobnosti naleznete zde
<http://www-01.ibm.com/support/docview.wss?uid=swg21501675>



Tip #14 Viditelnost pohledů v Domino names.nsf

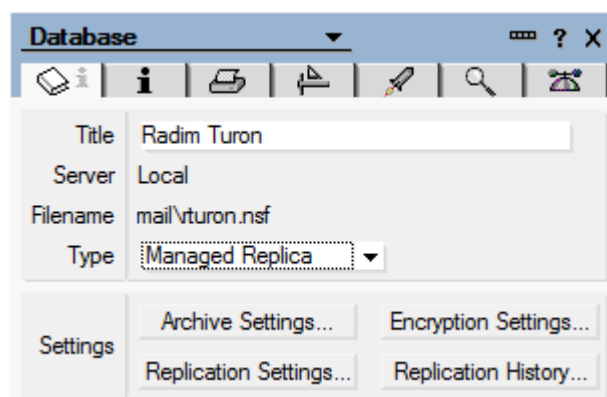
- Uživatelé používají adresní knihu organizace pro vyhledávání
- Bohužel také standardně vidí i konfigurační dokumenty (server dokument, connection dokumenty atd.)
- Skryjte tyto dokumenty





Tip #15 Managed Mail Replica

- Používejte pro lokální repliky, přináší spoustu výhod
 - Automatické doručování emailu, uživatel nemusí replikovat
 - Uživatel vždy pracuje s lokální replikou
 - Failover v clusteru
 - Automatické opětovné vytvoření v případě porušení
 - Nastavovaná a řízená politikou – skvělé pro administraci





Tip #16 DAOS a systémové databáze

System Database File	Should DAOS be enabled on this database?	Comments
NAMES.NSF	No	
LOG.NSF	No	
ADMIN4.NSF	No	
MAIL.BOX	Yes	If you want to use DAOS and not transaction log mailbox bodies you can use the following in 8.51. NSF_DONT_LOG_MAILBOX_BODY=1 RM_NO_LOG_LARGE_OBJECTS=1 RM_NO_LOG_OBJECTS_IN_MAILBOX=1
DBDIRMAN.NSF	No	
CLUBUSY.NSF	No	
DDM.NSF	No	
STATREP.NSF	No	
STATMAIL.NSF	No	
CLBDBDIR.NSF	No	
WEBADMIN.NSF	No	
CLBDBDIR.NSF	No	
BUSTIME.NSF	No	
EVENTS4.NSF	No	
STATLOG.NSF	No	
REPORTS.NSF	No	
MTSTORE.NSF	No	
ACTIVITY.NSF	No	



Tip #17 Posílání mailu na skupiny v BCC

- Pokud se posílá mail, ve kterém jsou v BCC uvedeny skupiny (s mnoha uživateli), znamená to velkou zátěž pro Domino
- Domino rozbíjí a upravuje zprávu, příjemce vidí své jméno v BCC
- Nastavte do server NOTES.INI proměnnou **DISABLE_BCC_GROUP_EXPANSION=1**
- Menší zátěž pro server, příjemce nevidí své jméno v BCC



Tip #18 AMgr a kompaktace

- Občas dochází ke konfliktu na databázi mezi Agent Managerem a právě běžící kompaktací (AMgr chce spustit agenta na právě kompaktované databázi)
- Takový agent je vyřazen z fronty plánovaných agentů (přestane běžet v plánovaných intervalech) až do
 - restartu Agent Managera
 - půlnoční refreshe AMgr cache
- Od verze 8.5.2FP3 je možno zadáním proměnné do notes.ini předejít výpadku v běhu agenta (agent se opět spustí v následujícím plánovaném intervalu)

DEBUG_AMGR_ENABLE_RETRY_ON_COMPACT=1



Tip #19 Vypnutí TXN logování systémových db

- Transakční (TXN) logování některých systémových databází vytěžuje server (mnoho zápisů na disk)
- Vyřadte je z transakčního logování proměnnými v notes.ini
 - MailBoxDisableTXNLogging=1** (pro mail.box)
 - Log_DisableTXNLogging=1** (pro log.nsf)
 - Schedule_DisableTXNLogging=1** (pro clubusy.nsf nebo busytime.nsf)
- POZOR: Pokud používáte DAOS, nezakazujte transakční logování pro Mailbox!



Tip #20 Program dokument - rozšíření

- Od verze R9 je možno do pole **Server to run on:** zadávat jména skupin (musí být typu Servers only)

Program: compact

Basics | Administration

Basics

Program name: compact

Command line: -c mail

Server to run on: MailServersGroup

Comments:

- V tomto poli můžeme také použít konvenci zápisu názvu serverů se znaky ? a *
 - Server??/ACME (Server00/ACME, Server01/ACME, Server03/ACME ...)
 - Server*/ACME (ServerMail/ACME, ServerBackup/ACME, ServerTraveler/ACME ...)



Tip #21 Directory Assistance - doporučení

- Při nastavování adresní knihy do DA nepoužívejte link, raději použijte přímé vypsání jména souboru

Basics | Naming Contexts (Rules) | Domino

Replicas

Application links: ~~✗~~

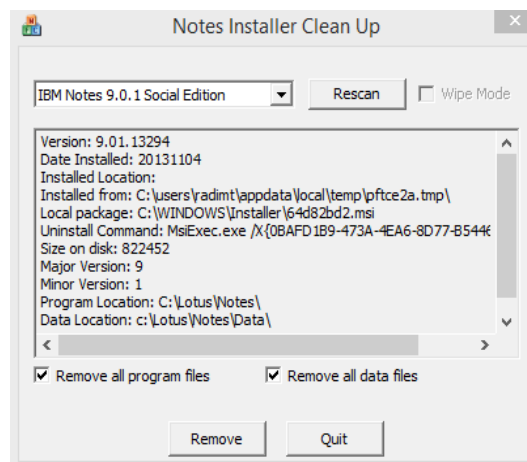
OR

	Server Name	Domino Directory Filename	Enabled
Replica1:	*	klienti.nsf	Yes
Replica2:			No
Replica3:			No
Replica4:			No
Replica5:			No



Tip #22 Notes Install Cleanup Executable Tool (NICE)

- Používá se v případě problému s instalací, odinstalací nebo opětovnou instalací klienta Lotus Notes verze R6 a vyšší
- Čistí OS od nastavení a souborů klienta LN „dočista dočista“ ;-)
(soubory klienta, nastavení, registry, uživatelská data)



- Stahujte zde: <http://www-01.ibm.com/support/docview.wss?uid=swg21459714>



Tip #23 DDM probe - jak monitorovat agenty

- Často se stává, že vinou kódu v agenetch nebo i jinými vlivy, agenti neúměrně vytěžují Domino server (dlouhý běh, vytěžování CPU, paměti) nebo nefungují dle očekávání
- Pro monitoring agentů nastavte DDM probe typu „Application Code“
- Můžete monitorovat agenty spouštěné v úlohách Amgr a HTTP na tyto události:
 - Agent behind schedule - monitoring agentů, kteří se nespustili v určeném čase
 - Agents evaluated by CPU usage - monitoring agentů, kteří vytěžují CPU
 - Agents evaluated by memory usage - monitoring agentů náročných na paměť
 - Long running agents - monitoring dlouho běžících agentů



Tip #24 Chráněné skupiny v adresní knize

- Ochrňte kriticky důležité skupiny v adresní knize proti náhodnému smazání!
Pro design DD R9 a výše.

Domino Directory Profile

File Edit View Create Actions Tools Window Help Basics

Open [Icons]

Domino Directory

- People
 - by Organization
 - by Client Version
 - Alternate Language
 - Certificate Expiration
- Policies
- Groups
- Configuration

Apply Delegation to All Selected

Edit Directory Profile

Edit Administration ECL

Set Secure Internet Passwords

Add Admin Roles to Access

Remove Directory Profile

Update Auto Dialer Schedule

Recertify Selected People

Add Internet Certificate to Selected

Rename Selected People

Set Password Fields

Upgrade to More Secure Internet

Edit Document

Domino Directory Configuration Profile

Domain defined by this Domino Directory: Iris

Note: This setting is obsolete as of Domino 8.5.1. It is used for compatibility with prior versions only:

Condensed server directory catalog for domain:

Sort all new groups by default: No

Auto-populated group Members update interval: 30 minutes

Use more secure Internet Passwords: Yes - Password verification compatible with Notes/Domino release 4.6 or greater

Allow the creation of Alternate Language Information documents: Yes

List of administrators who are allowed to create Cross Domain Configuration documents in the Administration Process Requests database:

Prevent deletion of these groups: LocalDomainAdmins, LocalDomainServers, OtherDomainServers, Iris Servers

Comments:



Tip #25 CentOS 7 a Domino server

- CentOS 7 je novou verzí bezplatného linuxového operačního systému, vycházejícího z komerční verze OS Redhat Enterprise Linux Server 7 (RHEL 7)
- Nahrazuje řadu CentOS 6, která je populární alternativou k OS Microsoft Windows pro provoz Domino serveru
- Oficiální podpora IBM pro provoz Domino serveru na RHEL7 (a tím také neoficiálně i pro CentOS7) je pro Domino server od verze **9.0.1FP2**, viz.:
<http://www-10.lotus.com/ldd/fixlist.nsf/8d1c0550e6242b69852570c900549a74/7ff6a78cb16153d085257d2b0062d7b8?OpenDocument>





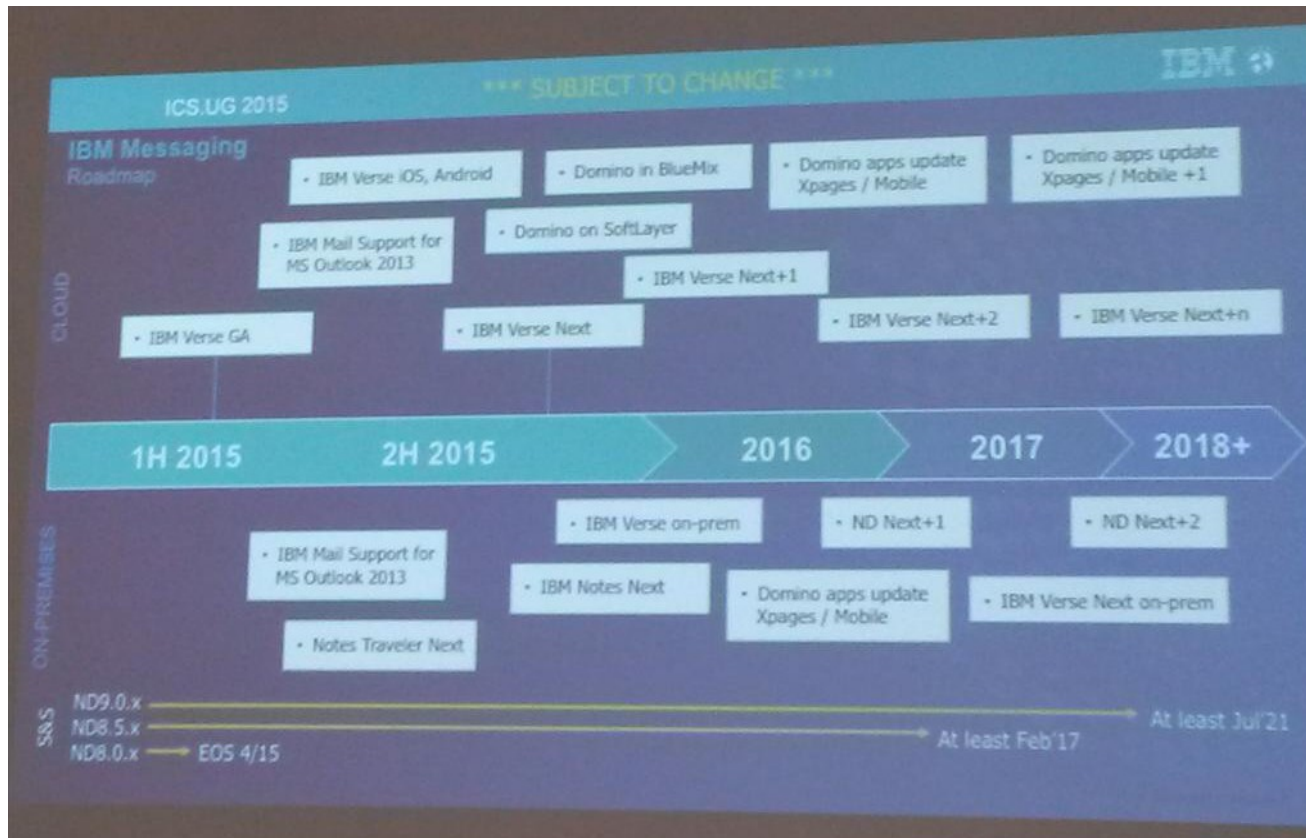
Tip #26 CentOS 7 a Domino 9.0.1 - start/stop skript

- V CentOS 7 byl proces sysvinit (system and service manager) nahrazen procesem systemd
- Přineslo to problém se stávajícími skripty pro spouštění/ukončování Domino serveru, např. od Daniela Nasheda:
<http://www.nashcom.de/nshweb/pages/startscript.htm>
- Při ukončování Domino serveru je místo provedení „shutdown“ proveden „kill“
- Řešením je upravený skript:
http://www-10.lotus.com/ldd/dominowiki.nsf/dx/Starting_and_Stopping_Domino_-with-_the_Server_OS_automatically_with_systemd



Tip #27 Konec podpory Lotus Domino/Notes R8

- K datu 30. dubna 2015 byla ukončena podpora pro verzi Lotus/Domino R8
- V současnosti zůstávají podporovány verze R8.5, R9 a R9.0.1





Tip #28 Mail File Delivery Failover

- Od verze Domino R9 umožňuje router doručovat zprávy na repliky poštovní schránky v clusteru v případě, že je home/mail replika poštovní schránky nedostupná z důvodu:
 - Kompaktace copy-stylem
 - Fixupu
 - Chybějícího souboru pošty v datovém adresáři Domina
- V serverovém NOTES.INI nastavte proměnnou:
MailFileEnableDeliveryFailover=1



Tip #29 Silent failover

- Potlačuje na klientovi hlášku o přepnutí na jinou repliku v clusteru při failoveru
- Pouze pro klienta 8.5.2 a výše
- V NOTES.INI klienta nastavte proměnnou:
FailoverSilent=1
- Je možno nastavit uživatelům pomocí Desktop Policy dokumentu
(Desktop Settings -> Mail -> Client Settings)
- Výhodou je, že automaticky přepíná uživatele zpět, pokud je původní nedostupný server opět v provozu

Client Settings

Auto-retrieve document setting: Disable

Enable server to poll for new mail and trigger replication on notification of new mail: Disable

Enable silent failover when a server goes down: Enable

Enable upgrade of all local NSF's to latest ODS version: Disable



Tip #30-1 Optimalizace HTTP pro Traveler

- HTTP task musí mít dostatek vláken k obsluze požadavků z mobilních zařízení přistupujících na Traveler skrze HTTP
- Pokud je počet vláken nedostačující, mobilní uživatelé uvidí tyto hlášky:
 - Zařízení Apple - "Cannot connect to server" nebo velmi pomalé odezvy
 - Ostatní zařízení - hlášky „error 503 (Server busy)“ nebo velmi pomalé odezvy až selhání synchronizace
 - Na Traveler serveru neúměrně naroste zatížení CPU a vytížení paměti
- Pokud máte tyto problémy, nastavte v Server dokumentu pole „Number active threads“ na vyšší hodnotu

Basics	Security	Ports...	Server Tasks...	Internet Protocols...	MT
HTTP	Domino Web Engine	DIIOIP	LDAP		
Basics					
Host name(s):	servera.cosmos.com				
Bind to host name:	Disabled				
DNS lookup:	Disabled				
DNS lookup cache:	Enabled				
DNS lookup cache size:	256				
DNS lookup cache found timeout:	120 seconds				
DNS lookup cache not found timeout:	240 seconds				
Number active threads:	100				



Tip #30-2 Optimalizace HTTP pro Traveler

- Defaultní hodnoty pro počet HTTP vláken, tak jak je nastavuje Traveler při instalaci
 - Domino 32bit - 100 vláken
 - Domino 64bit - 400 vláken
- Kalkulace kolik vláken je skutečně potřebných
 - Příkazem *Tell Traveler stat show push.devices.total** zjistíme, kolik je celkem registrovaných zařízení pro synchronizaci
 - Výsledek vynásobíme číslem 1,2 a dostaneme skutečně potřebný počet HTTP vláken



Tip #30-3 Optimalizace HTTP pro Traveler

- POZOR! Alokováním příliš velkého počtu HTTP vláken, může dojít k zabránění velkého množství operační paměti na serveru
- Kalkulace kolik operační paměti je potřeba pro HTTP vlákna
 - 64bit – 1 vlákno zabírá přibližně 4MB paměti
 - 32bit – 1 vlákno zabírá přibližně 1MB paměti
- Vynásobíme počet nastavených vláken číslem 4 (pro 64bit) nebo 1 (pro 32bit) a dostaneme velikost zabrané paměti pro HTTP vlákna v MB



Tip #31 Optimalizace paměti Javy pro Traveler

- Proces Traveleru je napsán v Javě, proto je nutné pro ni správně alokovat paměť
- Standardní nastavení alokace paměti pro Javu v Traveleru:
 - Domino 32bit – 512MB
 - Domino 64bit - 1024MB
- Velikost alokované paměti pro Javu závisí také na počtu připojených zařízení
- Využití paměti zjistíme příkazem *Tell Traveler Mem Show*

Basics Security Ports... Server Tasks... Internet Protocols... MTAs... Miscellaneous Transactional Logging Shared Mail DAOS IBM Traveler	
Basics	
Maximum Memory Size:	『 1024 』 MB
IPC Socket Ports:	『 50125 』 『 50126 』
External Server URL:	『 http://servera.acme.com/traveler 』



Tip #32 Optimalizace cache paměti pro Traveler

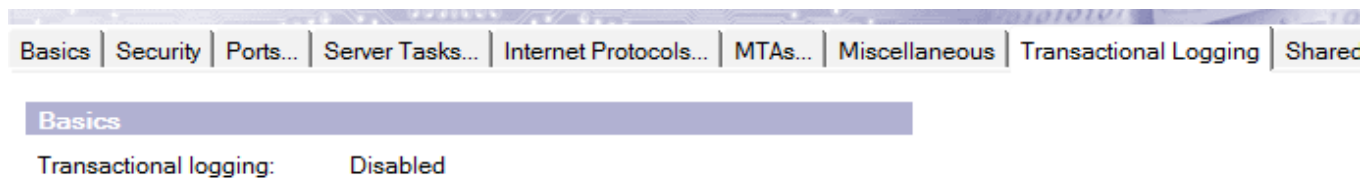
- Pole „Maximum cached users“ se používá k nastavení cache, ve které se uchovává uživatelské jméno, heslo a příslušnost ke skupinám pro autentizované uživatele
- Pokud počet autentizovaných uživatelů překročí nastavenou hodnotu, můžeme zvětšením hodnoty pole zvýšit výkon Traveler serveru
- Aktuální hodnoty zjistíme příkazem *show stat Domino.Cache.User**
Domino.Cache.User Cache.Count = 86
Domino.Cache.User Cache.MaxSize = 64
- Nastavení naleznete na Server dokumentu v záložce Internet Protocols -> Domino Web Engine

Memory Caches	
Maximum cached designs:	128
Maximum cached users:	64
Cached user expiration interval:	120 seconds



Tip #33 Transakční logování a Traveler

- Traveler server není typický Domino server a nedochází na něm k většímu počtu zápisů do databází
- Není proto nutné používat transakční logování





Tip #34 Defragmentace Derby databáze

- Traveler používá relační databázi Derby pro uchování stavových informací o zařízeních a s nimi spojených synchronizacích
- Pro optimalizaci výkonu Traveleru je dobré tuto databázi periodicky defragmentovat
- Plánovanou defragmentaci je možno nastavit v NOTES.INI proměnnou:

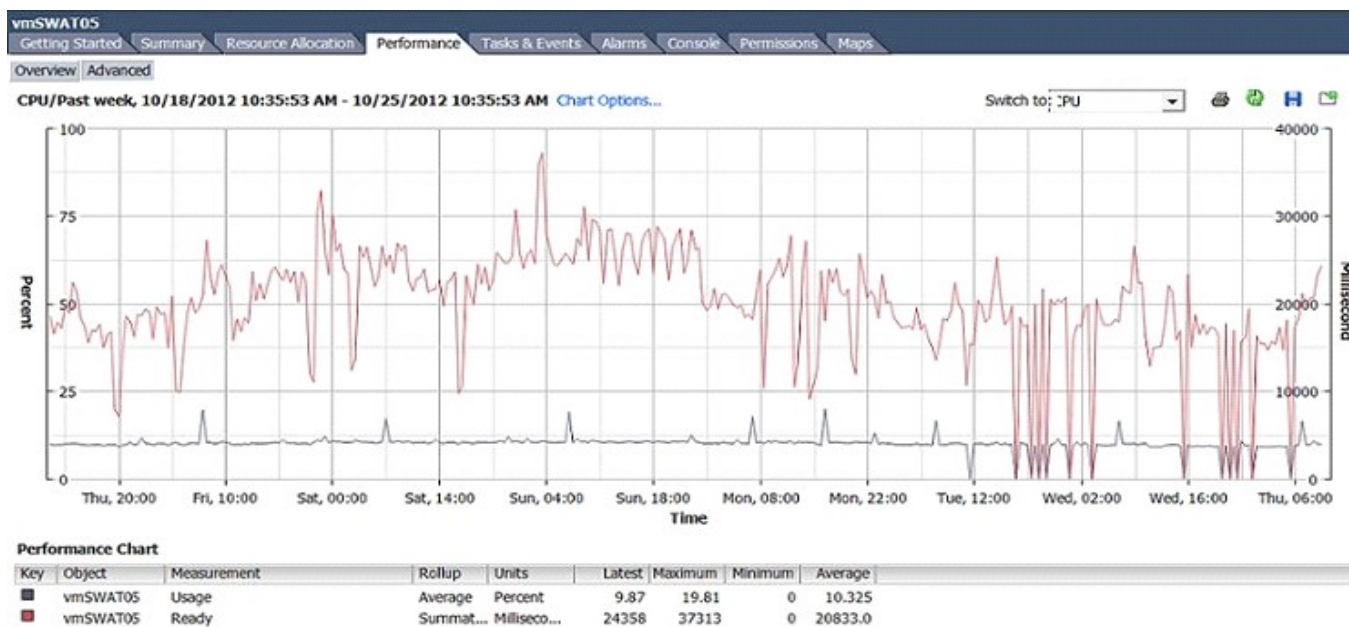
NTS_DEFRAG_INTERVAL_DAYS=XX (XX je počet dnů)

- pokud je doba od poslední defragmentace větší než XX, po restartu Traveleru proved' automaticky defragmentaci
- Je také možno provést ruční defragmentaci z Domino konzoly příkazy:
tell traveler quit
tell http quit
load traveler -defrag



Tip #35 Traveler ve virtualizovaném prostředí

- Je doporučeno alokovat HW prostředky pro Traveler staticky, pokud je host nastaven na dynamickou alokaci a server je vytěžován i jinými aplikacemi, může dojít k degradaci výkonu Traveleru





Tip #36 Traveler a logování dat mobilních zařízení

- V Server dokumentu na Traveler serveru povolte logování HTTP komunikace pomocí databáze domlog.nsf (založky Internet Protocols->HTTP, pole Domlog.nsf)
- Zároveň ze šablony domlog.ntf vytvořte v rootu datového adresáře Domina databázi domlog.nsf a restartujte HTTP task
- V databázi domlog.nsf si vytvořte nový pohled pro filtraci Traveler komunikace, s následující selection formulí:
@Contains(Request,"/servlet/traveler") & AuthenticatedUser!="-"
 - Pak si vytvořte v tomto vašem novém pohledu sloupce dle své potřeby
- I pokud si výše uvedený pohled nevytvoříte, standardně v databázi domlog.nsf uvidíte podrobné informace o komunikaci s mobilními zařízeními



Tip #37 Stop informacím o HTTP serveru

- Bezpečnostní doporučení pro Domino HTTP server
- Přidejte do serverového NOTES.INI proměnnou **HTTPDisableServerHeader=1**
- Domino již nebude zveřejňovat podrobnosti o své verzi HTTP serveru

```
HTTP/1.1 400 Bad Request
Date: Mon, 25 May 2015 15:33:44 GMT
Connection: close
Pragma: no-cache
Cache-Control: no-cache
Expires: Mon, 25 May 2015 15:33:44 GMT
Content-Type: text/html
Content-Length: 161
```



Tip #38 SSL, TLS a jejich zranitelnost

- SSL a TLS jsou kryptografické protokoly, poskytující možnost zabezpečené komunikace po internetu pro služby jako jsou el. pošta, WWW apod.
- Po dlouhou dobu byl hromadně používán protokol SSL 3.0 i když existovaly a byly připraveny i jeho dokonalejší nástupci - protokoly TLS 1.0, 1.1, 1.2
- POODLE - útok který změnil svět kryptované komunikace na internetu
 - **SSL 3.0 již není bezpečný!**
 - **Přejděte urgentně na TLS!**
- Na konci roku 2014 se objevil POODLE útok na určité implementace protokolu TLS
 - **POZOR, některé verze Domina jsou tímto zasaženy, více zde:**
<https://www-01.ibm.com/support/docview.wss?uid=swg21692502>



Tip #39 Podpora protokolu TLS v Domino/Notes

- Podpora TLS 1.2
 - Domino 9.0.1Fix Pack 3 Interim Fix 2
 - Domino 8.5 - nebude zavedeno
 - Notes 9.0.1Fix Pack 3 Interim Fix 3
- Podpora TLS 1.0
 - Domino 9.0.1 Fix Pack 2 Interim Fix 3
 - Domino 9.0 Interim Fix 7
 - Domino 8.5.3 Fix Pack 6 Interim Fix 6
 - Domino 8.5.2 Fix Pack 4 Interim Fix 3
 - Domino 8.5.1 Fix Pack 5 Interim Fix 3
- Výše uvedené Interim Fixy zabezpečují proti oběma POODLE útokům
http://www-10.lotus.com/ldd/dominowiki.nsf/dx/IBM_Domino_TLS_1.0



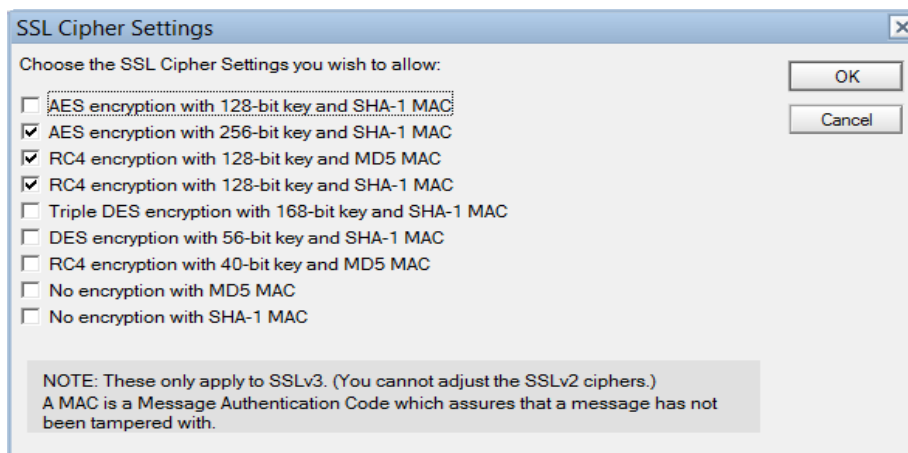
Tip #40 Notes.ini proměnné pro SSL a TLS

- `DISABLE_SSLV3=1`
 - Zakazuje používání protokolu SSL 3.0
- `SSL_DISABLE_TLS_10`
 - Zakazuje používání protokolu TLS 1.0
 - Od Domino 9.0.1FP3IF2



Tip #41 Nastavení typů šifrování na Domino

- Specifikace typu šifrování pro SSL/TLS se provádí na Server nebo Internet Site dokumentu (pole SSL ciphers)
 - Nastavení na Server/Internet Sites dokumentu nastavuje typ šifry **pouze** pro HTTP protokol
 - Jsou ale i nové typy šifer, které v seznamu nevidíme, jelikož nový seznam bude až s novou verzí šablony adresní knihy (9.0.2)





Tip #42 SSLCipherSpec

- Notes.ini proměnná, která specifikuje používané typy šifer pro všechny typy protokolů, nejen pro HTTP
 - Každá šifra je reprezentována dvouciferným hexadecimálním číslem
SSLCipherSpec=0405
04 = SSL_RSA_WITH_RC4_128_MD5
05 = SSL_RSA_WITH_RC4_128_SHA
- Aktuální doporučený typ šifrování pro TLS 1.2
SSLCipherSpec=9D9C3D3C352F0A9F9E6B3967

DHE_RSA_WITH_AES_256_GCM_SHA384 (9F)	DHE_RSA_WITH_AES_128_GCM_SHA256 (9E)
DHE_RSA_WITH_AES_256_CBC_SHA256 (6B)	DHE_RSA_WITH_AES_256_CBC_SHA (39)
DHE_RSA_WITH_AES_128_CBC_SHA256 (67)	DHE_RSA_WITH_AES_128_CBC_SHA (33)
RSA_WITH_AES_256_GCM_SHA384 (9D)	RSA_WITH_AES_128_GCM_SHA256 (9C)
RSA_WITH_AES_256_CBC_SHA256 (3D)	RSA_WITH_AES_256_CBC_SHA (35)
RSA_WITH_AES_128_CBC_SHA256 (3C)	RSA_WITH_AES_128_CBC_SHA (2F)
RSA_WITH_3DES_EDE_CBC_SHA (0A)	RSA_WITH_RC4_128_SHA (05)
- IBM vydává s novými FP/IF i aktualizovaný seznam podporovaných šifer
http://www-10.lotus.com/ldd/dominowiki.nsf/dx/TLS_Cipher_Configuration



Tip #43 Nástroj na testování SSL

- V poslední době velmi vytěžovaný ;-)
 - Test pro servery
<https://www.ssllabs.com/ssltest/>
 - Test pro klienty
<https://www.ssllabs.com/ssltest/viewMyClient.html>
- Výsledkem je bezpečnostní status testovaného serveru nebo klienta
 - Výsledek testu oznamuje známkou od A do F (A je nejlepší)
 - Vypíše používané verze SSL, TLS protokolu a používané šifry

Děkuji za pozornost

