DEV-1269:
Best and Worst Practices for Deploying IBM Connections

Christoph Stoettner, panagenda

Connect
2017

IBM

Notices and disclaimers

- Copyright © 2017 by International Business Machines Corporation (IBM). No part of this document may be reproduced or transmitted in any form without written permission from IBM.

- **U.S. Government Users Restricted Rights — Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**

- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IN NO EVENT SHALL IBM BE LIABLE FOR ANY DAMAGE ARISING FROM THE USE OF THIS INFORMATION, INCLUDING BUT NOT LIMITED TO, LOSS OF DATA, BUSINESS INTERRUPTION, LOSS OF PROFIT OR LOSS OF OPPORTUNITY. IBM products and services are warranted according to the terms and conditions of the agreements under which they are provided.

- IBM products are manufactured from new parts or new and used parts. In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."

- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**

- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.

- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.

- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.

- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. IBM EXPRESSLY DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.

- IBM, the IBM logo, ibm.com, Aspera®, Bluemix, Blueworks Live, CICS, Clearcase, Cognos®, DOORS®, Emptoris®, Enterprise Document Management System™, FASP®, FileNet®, Global Business Services ®, Global Technology Services ®, IBM ExperienceOne™, IBM SmartCloud®, IBM Social Business®, Information on Demand, ILOG, Maximo®, MQIntegrator®, MQSeries®, Netcool®, OMEGAMON, OpenPower, PureAnalytics™, PureApplication®, pureCluster™, PureCoverage®, PureData®, PureExperience®, PureFlex®, pureQuery®, pureScale®, PureSystems®, QRadar®, Rational®, Rhapsody®, Smarter Commerce®, SoDA, SPSS, Sterling Commerce®, StoredIQ, Tealeaf®, Tivoli®, Trusteer®, Unica®, urban{code}®, Watson, WebSphere®, Worklight®, X-Force® and System z® Z/OS, are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml.

Christoph Stoettner

 @stoeps
in linkedin.com/in/christophstoettner
Ⓦ www.stoeps.de
Ⓢ christophstoettner
☐ +49 173 8588719
christoph.stoettner@panagenda.com

- Senior Consultant – panagenda
  - IBM Notes / Domino since 1999
  - IBM Connections since version 2.5 / 2009
- Experience in:
  - Migrations
  - Administration and Install
  - Performance Analysis
- Focusing in:
  - IBM Connections deployment und optimization
  - IBM Connections monitoring
- Husband of one & father of two, Bavarian
- Beer or Wine? … Depends
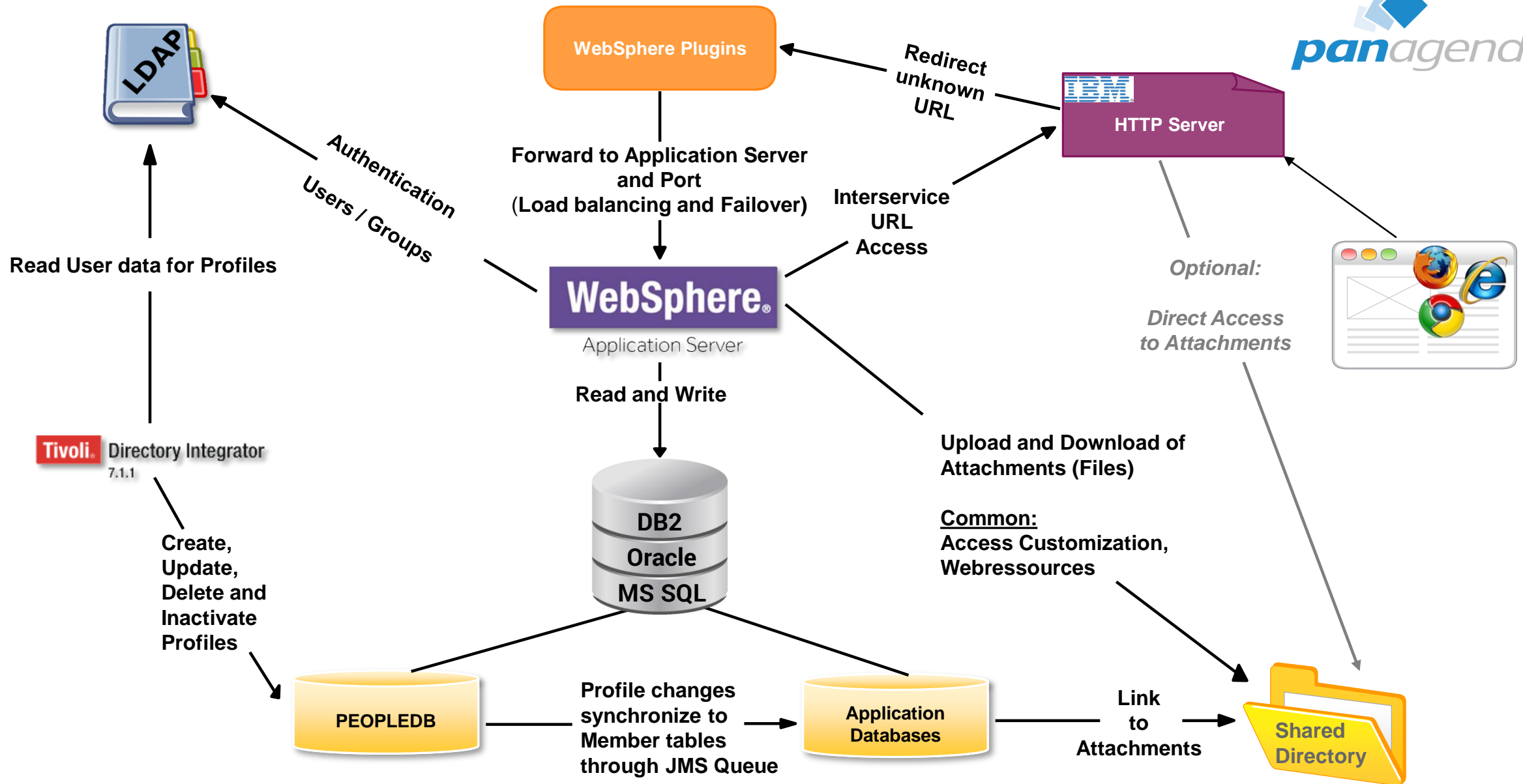
Installation Preparation – System Requirements

- ## Check System Requirements regularly

Deployment Unit	8.5.5	8.5.5.1	8.5.5.2	8.5.5.3	8.5.5.4	8.5.5.5	8.5.5.6	8.5.5.7	8.5.5.8	8.5.5.9	8.5.5.10
Server	❌	❌	❌	❌	❌	❌	✅ (1)	✅ (1)	✅ (1)	✅ (1)	❌

  - https://www-01.ibm.com/support/docview.wss?uid=swg27012786
  - Check all Notes
  - Download PDF (Documentation)

- ## Be careful with all other documents
  - Update strategy for IBM Connections 5.0

    DB2 Enterprise Server Edition Version 10

	DB2 Enterprise Server Edition Version 10	
	Minimum	Supported
CR1	10.1 FP4 (10.0.1.4)	10.1 FP4 (10.0.1.4)
CR2 (and above)	10.1 FP4 (10.0.1.4)	10.5 FP4 (10.5.0.4)

    - http://www-01.ibm.com/support/docview.wss?uid=swg21683118
  - Supported does not mean licensed
  - Connections 5.0 License Agreement

    The following are Supporting Programs licensed with the Program:
    IBM DB2 Enterprise Server Edition Version 10.1
    TDI Identity Edition V7.1.1
    IBM MQEveryplace 2.0.2.13
    IBM Tivoli Directory Server 6.3
    IBM Lotus Expeditor 6.2.1
    IBM solidDB 7.0
    IBM WebSphere Application Server Network Deployment v8.5.5
    IBM Cognos Business Intelligence
    IBM Cognos Business Intelligence Transformer
   IBM Support Assistant Lite
    EditLive! For IBM Connections
    IBM Forms Experience Builder 8.5.1

Official Documentation

- Product documentation
  - https://www.ibm.com/support/knowledgecenter/SSYGQH
- Performance Tuning Guides
  - 4.0
    - http://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM_Connections_4.0_Performance_Tuning_Guide
  - 4.5 Addendum
    - http://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM_Connections_4.5_Performance_Tuning_Guide_Addendum
  - 5.0 CR1
    - http://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM_Connection_V5_CR1_Tuning_guide
  - 5.5
    - https://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM_Connections_V5.5_Tuning_guide
- Read everything carefully
- Check and understand dependencies

Example 1: Slow Large Deployment

- Customer showed me a system with following infrastructure
- WebSphere
  - Large deployment
  - 16 GB RAM
  - 4 Cores
- DB2
  - 12 instances
  - 8 GB RAM
  - 4 Cores
- Just a few users without issues
- Connections restart took **22 minutes**
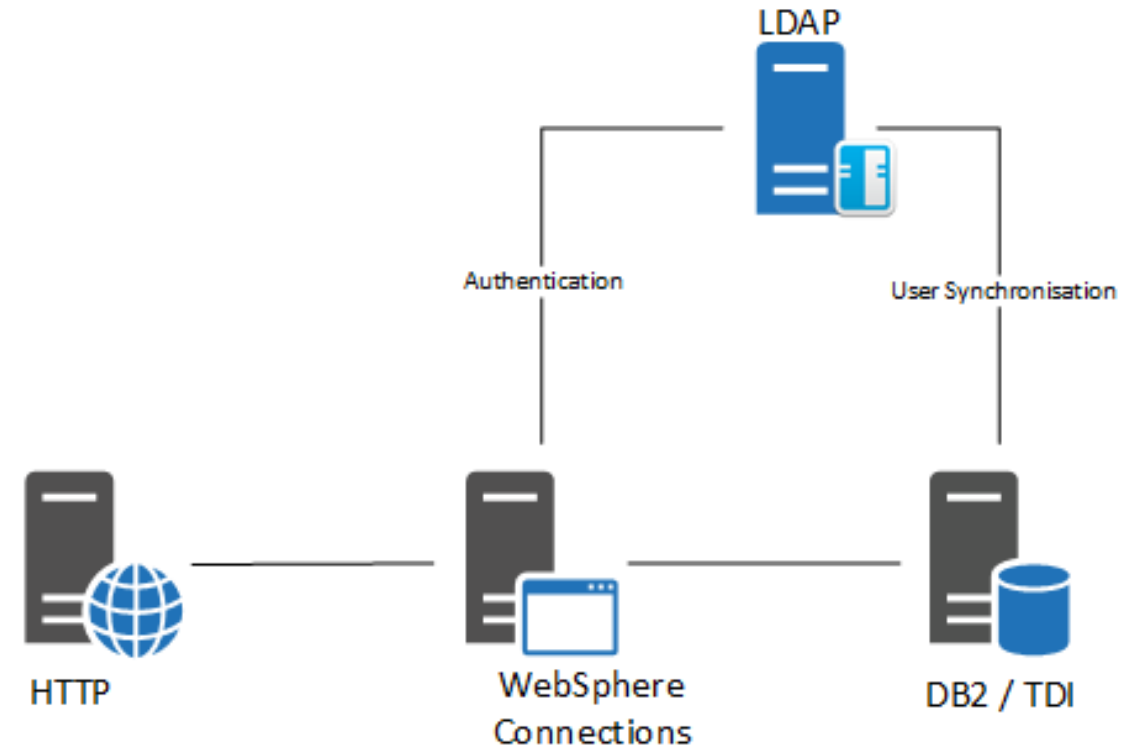
Example 1: Solving this

- Large deployment means about 15 JVM on the machine
  - Restart shows 15 min 100% CPU usage
  - Adding 4 cores and restart time got down to 7 minutes
  - Other option would be a medium size deployment → New install required
- Java Heap Sizes set to default
  - Useful default values can be found in the Tuning guides
  - No real boost after this change
- Performance Tuning Guide says:
  - Use multi instance for databases
  - So why wasn't it fast?

Key points: If possible, deploy the databases used by IBM® Connections Version 5.0 on 64-bit hardware, with each database deployed in its own database instance, if sufficient physical memory is available.

Performance Tuning Guide 5CR1 – page 10

Example 1: Solution

- Data Source connection pool sizes were set to default 1/10
  - Increase this values to the proposals in the guide and …
  - Restart time comes down to under 3 minutes
- **Key point**: read the complete guide
- Tip: Monitor Connection Pool sizes
  - Performance Monitoring Infrastructure (PMI)

Data Source	DB2	
	JDBC Pool (min/max)	Statement Cache Size
activities	1/50	100
blogs	1/250	100
dogear (Bookmarks)	1/150	100
CCM FNOSDS	75/200	100
CCM FNOSDSXA	25/75	100
CCM FNGCDDS	default	default
CCM FNGCDDSXA	default	default
communities	10/200	100
files	10/100	100

Example 2: Small Deployment

- Customer showed me a system with following infrastructure
- WebSphere
  - Small Deployment
  - 10 GB RAM
  - 4 Cores
- DB2
  - 1instance
  - 4 GB RAM
  - 2 Cores
- Log with few wait messages
- Access problems when 300 users access Wikis at the same time
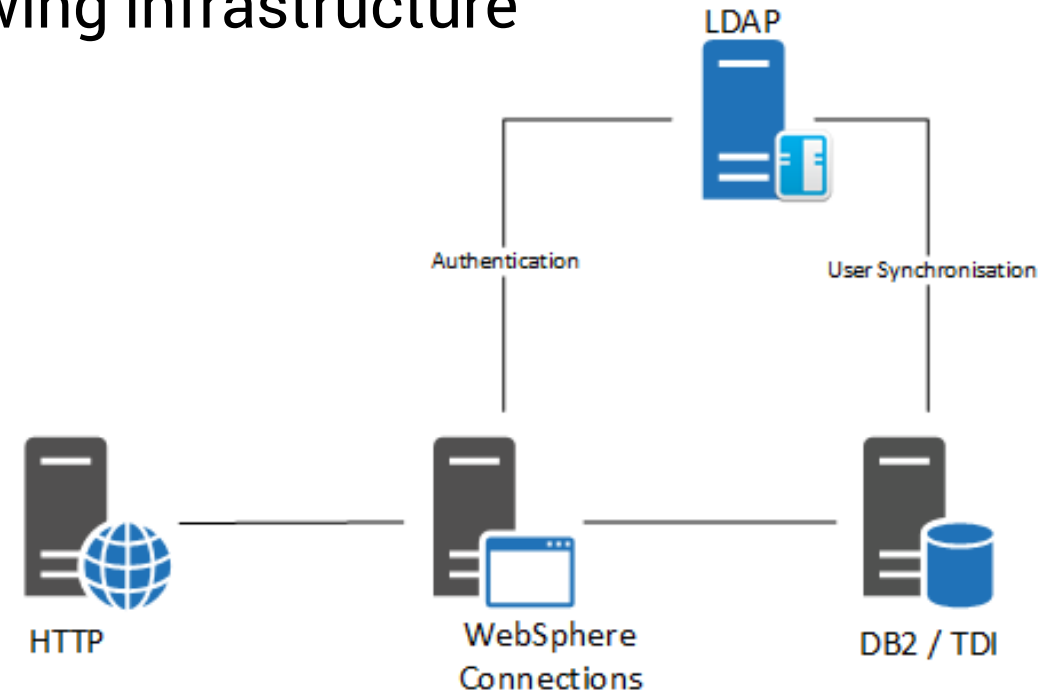
Example 2: Investigation & Solution

- Adding CPU → not successful
  - Small Deployment → Just 1 JVM → needs 100% of one CPU
- Problem mainly occurred when lots of users connected
  - Simulate with jmeter or other stress test software
- Check PMI
  - We found Average Wait time for database connection of 85 seconds
  - Like in Example 1, Connection Pool sizes too small, Default Minimum = 1
  - Extending the DB Pool sizes and rerun test → Average Wait time = 0
- Check HTTP Server /server-status
  - All threads occupied (Default: 600)
  - Browser push notification uses long polling which causes bigger amount of threads (Connections 5.5)
  - We increased the threads

Sizing and Deployment Options

- **I often start with three servers (easy to extend)**
  - HTTP Server
  - WebSphere / IBM Connections
  - DB2 / Tivoli Directory Integrator
- **Be prepared for future growth**
  - Build a easy extendable topology
  - POC License is often restricted to Small Deployment
    - Going live will need a new installation of Connections
- **Do not overact**
  - Some hundred users won't need a Large Deployment
- **Starting with Medium Deployment fits mostly**

LDAP

Authentication

User Synchronisation

HTTP

WebSphere Connections

DB2 / TDI

(Virtual) Hardware
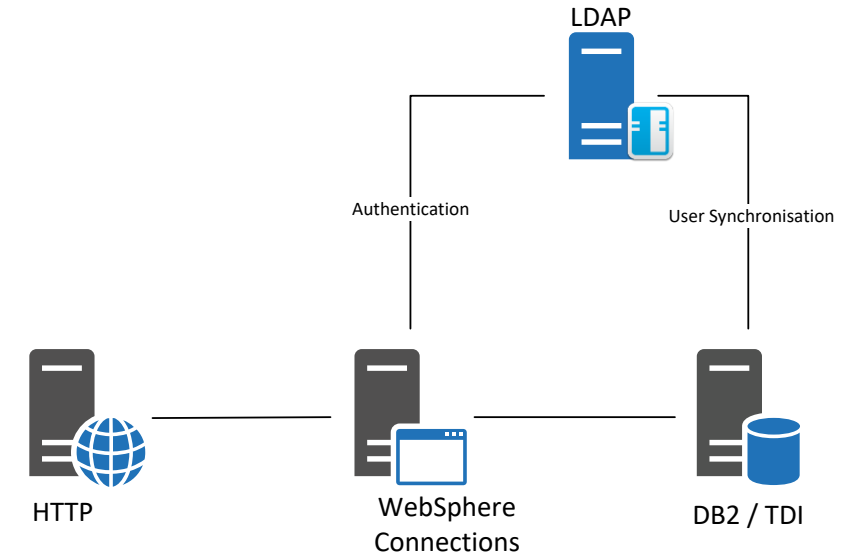
- Requirements tells us
  - "Two processor cores per server", "Enterprise-scale deployments, at least 4 CPU"
  - "8 GB memory", "16 GB for enterprise-scale"
- I assume that Enterprise-scale uses the "Large Deployment" option
  - Around 15-20 JVM on one machine (DMGR, Node Agents, AppServer)
  - This means that 4 JVM share one Core
  - Which is too less, my prefered calculation is:
    - 0.5 * JVM-Count or 1 * JVM-Count
    - So PVU License option can be pricy
- Memory of 8 GB is very low, calculate a minimum of 10-12 GB
  - Always be aware that insufficient memory results in swapping
  - Swapping kills all your tuning efforts
  - A high JVM count need more memory overhead

Operating System

- Always use the Operating System you like most
  - No real performance differences
  - I assume you have the best knowledge on systems you like
- Easier to troubleshoot
- IBM Docs Conversion (mandatory for Docs and Viewer) needs Windows Server OS

Directory and User Synchronization

- Prepare your LDAP

  – Better data within LDAP $\longrightarrow$ better Profiles

- Switching Authentication directories is possible
  – Needs some planning
  – Ask before you start and avoid duplicate profiles

- Dependencies
  – Quality of LDAP data
  – Plans to activate SPNEGO
  – Domino Mail Integration

Prepare Installation

- Download all software
- Extract to a central place
- Do not use spaces in paths
  - Neither source or target paths
- Disable all "Security stuff" during install and testing
  - SELinux
  - AppArmor
  - AntiVirus
  - Firewalls
  - Self developed scripts, OS extensions / optimizations
    - Example: Script which deletes unknown folder, network stack optimizations …
- After successful testing, you can re-enable them step-by-step

Example 3: Round Robin

- All prerequisites installed
- Domino LDAP
  - LDAP Installation User
- 2 Domino Servers configured with a central DNS Name ldap.example.com
  - Federated Repository with 1 LDAP Server entry (ldap.example.com)
- Both Domino Servers with 2 NIC
  - ldap.example.com resolves to 4 IP Addresses
- Only 25% of Connections Applications installed successfully
- What happened?

- Round robin DNS works
  - Each namelookup got one of the 4 IPs
- Domino Server configuration (notes.ini)
  - LDAPSERVER=LDAP://192.168.1.1:389
  - So LDAP listens only on one of two IPs
  - Each second DNS request resolves an IP without LDAP Service
- Federated Repository without Failover Server
  - No additional authentication request when a connection is not successful
- So two problems
  - LDAP Configuration
  - Round Robin

Network and Name Lookup

- ## Name lookup / DNS
  - All servers must be resolvable (hosts is not a suitable workaround)
  - Understanding the protocol
    - Avoid Round Robin
    - No Authentication failover in WebSphere with Round Robin!
- ## Network storage (file locking is important)
  - NFS v4 / SMB|CIFS
  - No DFS (http://www-01.ibm.com/support/docview.wss?uid=swg21614197)
- ## Reverse Proxies / Proxies
  - Always test your deployment without proxies
  - Activate after successful testing

Example 4: The SSL Key store

- I got a call that Connections can't be accessed
- Log showed SSL errors
- What would you do?
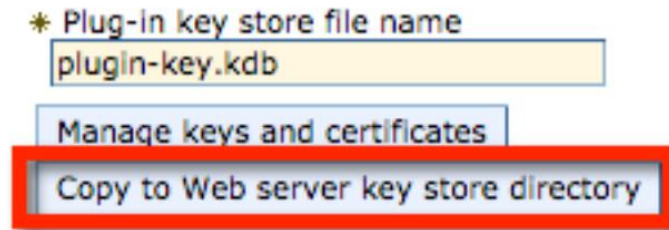
- The result: A overwritten plugin-key.kdb
- Installer registered HTTP Server SSL Key into the Plugin Key store
  - So now the key is deleted
  - Good chance to test your backup and restore strategy

HTTP Server Key store

- ## Best Practice - Create a separate key store for IHS
    - iKeyman will help you
    - It's possible to use a wildcard certificate
        - Then you can just copy it to use on dev / test machines
    - Backup the key store before changing it
    - Don't activate "Expiration time"
    - "Stash password to a file"
        - Creates a cnx-key.sth file
        - Which is used by IHS to open key store

HTTP Server is important
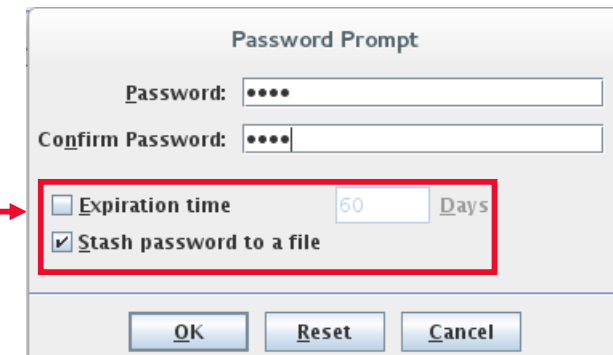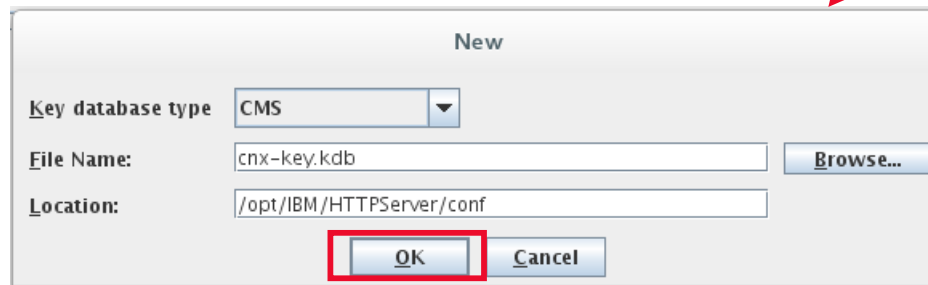
- **Check SSL Protocols**
  - Be careful with TLS 1.2 only
  - Double check with
    - https://ssllabs.com/ssltest
    - sslscan, openssl … (https://www.owasp.org/index.php/Testing_for_SSL-TLS_(OWASP-CM-001))
    - nmap (https://nmap.org/nsedoc/scripts/ssl-enum-ciphers.html)
- **Enable only fast and secure ciphers**
- **Enable compression**
- **Remove Server Information**
  - ServerSignature Off
  - ServerTokens Prod
  - AddServerHeader Off

Create and Follow Checklists

- Create a test plan
- Test in multiple languages
  - There were several issues which only appear in some languages
- Test with multiple Browsers
- Don't test SSO with Chrome

Test Environment

OH: Everybody has a testing environment.
Some people are lucky enough to have a totally separate environment to run production in
#DevOps

— Stephan H. Wissel (@notessensei)

Clean Test Environment

- You should have a test environment
- Testing issues
- Check if something is a bug or works as designed
- Customization
- Configuration Changes
- Migration
  – Data
  – Customization
- Updates
  – Deployment
  – Possible problems
- Use virtual environment
  – Snapshot

Troubleshooting

- Learn from White Hat Hackers
- Use tools like
  - Burpsuite
    - Intercept Proxy
    - Check data sent and received from Webserver
  - Fiddler
    - IBM Support will ask you for traces in PMR
    - Like Burpsuite you see header and received data
  - Apache JMeter
    - Create simple or detailed test plans
    - Simulate some hundred users (or use different hosts and some thousands)
  - PMI
- Check Server responses

Installation Checklist

1. WebSphere Application Server
2. DB2
   1. Import DB2 license
3. HTTP Server
   1. Configure
   2. Enable Compression
   3. Enable SSL
4. WebSphere Plugins
   1. Create Plugin Configuration
5. Tivoli Directory Integrator
   1. TDI Fixpack

6. Connections Wizard
   1. Create Databases
   2. Populate Profiles
7. IBM Connections
8. Ephox Editors
9. Surveys
10. Mail Integration
11. Configuration *-config.xml
12. J2EE Security Roles
13. Test
14. Apply customization

Migration Checklist

1. Follow Step 1- 13 of Installation Checklist
2. Apply customizations
   1. Do not copy
3. Test everything[1]
4. Enable Firewalls, Proxies, Reverse Proxies
5. Test again[1]
6. Drop databases and recreate them
7. Clean Shared Directory
8. Import Data
9. Test again[1]

[1] I prefer a non-admin test person! Favorite choice: Femke Goedhart
You should plan more time to test, she will always find something

Test Checklist

- Security checks:
  - Internal / external access
  - Access over LAN/Wifi/mobile
  - Access by other applications
- Third party apps & integration
  - Check app support for adding and extensions
  - Check widgets that display Connections data in other applications (intranet, portal)
  - Verify any custom applications
- Create a script per Connections app to:
  - Verify whether all of your data exists
  - Access existing data (read)
  - Create new data (write)
  - Change/update existing data (update)
  - Interact with existing data (comment or like)
- Additional:
  - Check notifications
  - Check logging

What to Backup

- Using an example Connections installation guide rarely explains backups
  - These guides normally do not mention backup, or what to back up
  - Disk crash means data loss
- Database backups through file backup are not supported and mostly not restorable
- Important!!!
  - Database Backup through Online Backups can be taken when Connections is up
  - Offline backups are also possible
- Ensure the file system & DB backup are run at the same time of the day
  - DB and Filesystem data will stay in sync – if you take your DB backup at midnight and the file system at midday they will be out of sync

Backup

- Most important (minimum daily)
  - Databases (offline or online)
  - Shared content
- Important
  - Configuration
    - WebSphere Application Server
    - Connections
    - IBM HTTP Server
    - TDI Solution
- Test if restore is possible!!!!
  - Several issues with WebSphere restores, where binaries weren't on the tape
  - HINT for TSM:
    - dsm.opt
      - SNAPSHOTPROVIDERFS vss

Version Control Systems

- Some data within your deployment are great to manage with
  - SVN
  - GIT
- TDISolution Directory
- LotusConnections-config
- IBMDocs-config
- Customization
- Only check-in working code, so you can revert on errors
- Learn branching

Documentation

- Everyone hates writing documentation
- BUT – make notes as you go, it doesn't need to be a full step by step guide with screenshots
- Document all customizations
- Any additional changes made
- Anything of note that deviates from the guides
- Lessons learnt or how you solved issues
- Use scripts to output some of it

General Checklist

Do

- Read the documentation
- Tune your environment
- Be prepared for scaling
- Create a documentation
- Test with all used languages

Don't

- Use unstable file shares
- Use Server IE (even without extended Security)
- Install on single machine
- Use Small Deployment
- Copy customizations to newer versions

Thank you

Christoph Stoettner
Senior Consultant

panagenda GmbH – Make Your Data Work for You

Lahnstr. 17 ● 64646 Heppenheim (Germany)

Skype: christophstoettner ● Cell: +49 173 8588 719

Office: +49 6252 67939-87 ● E-Mail: christoph.stoettner@panagenda.com