

IBM Software

ConnectED2015

BP203: Best and Worst Practices Deploying IBM® Connections™

Christoph Stoettner, Fritz & Macziol GmbH



This presentation mentions the following Copyrights and Trademarks

- IBM®
- Notes®
- Domino®
- Connections™
- WebSphere®
- DB2®
- AIX®
- Tivoli®
- Linux®
- Java®
- Microsoft® Windows®
- Microsoft® Excel®
- Red Hat® Linux®
- Twitter®
- Skype®

Notices and Disclaimers

Copyright © 2015 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.

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.

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, BrassRing®, Connections™, Domino®, Global Business Services®, Global Technology Services®, SmartCloud®, Social Business®, Kenexa®, Notes®, PartnerWorld®, Prove It!®, PureSystems®, Sametime®, Verse™, Watson™, WebSphere®, Worklight®, 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.

About Me - Christoph Stoettner

IBM **CHAMPION** 
Thanks Martin Leyrer for your
comments and ideas

- Consultant at FRITZ & MACZIOL GmbH Germany
- Working with ICS products since 15 years
- Specialized in IBM Connections and IBM Domino Infrastructure
- Bavarian, Linux and Scripting Lover, Blogger
- www.stoeps.de / scripting101.org
- Speaker at:



Agenda

- Installation and Requirements
- Tuning
- Enhance the user experience
- Backup
- Checklists
- Resources

INSTALLATION & REQUIREMENTS

System Requirements

- Regularly check requirement documents

- Check all notes

- All versions

- <http://www-01.ibm.com/support/docview.wss?g27012786>

- IBM Connections 5

- <http://www-01.ibm.com/support/docview.wss?g27042395>

- Remember to add TLS fixes

Product support for prerequisite maintenance levels, current and future →

Deployment Unit	8.5.5	8.5.5.1	8.5.5.2	8.5.5.3	8.5.5.4	→
Server	✗	✓ (1)	✓ (2)	✗	✗	✗

Notes:

(1)

(2)

All notes

**** NEW Please Read** Connections Security Bulletin:**

<http://www.ibm.com/support/docview.wss?uid=swg21690640>

**Upgrade to IBM Connections 5.0 CR1 and WAS Fix Pack 8.5.5.2;
then apply WAS APAR PI28920**

SYSTEM REQUIREMENTS DOCUMENTATION (for 8.5.5.2 support)

PI15998 - Fix Central iFix for PI15998 - Hanging in the EJB deploy process due to a dead lock in

Sizing

- Be prepared for future growth
- Do not overact
 - Some hundred users mostly won't need a large deployment
 - Except you plan big and frequent file downloads
- I'm not a fan of multiinstance database machines
 - If i run in database performance issues i split the databases to different machines
 - Performance tuning guide
 - Multiinstance is best practice, if you **have enough resources**

Sizing (2)

- A word to minimum requirements
 - 4 GB memory minimum is too less, better starting with 8 or 12 GB
 - **Memory swapping kills all tuning efforts**
- CPU cores
 - 2 cores minimum only on small deployments
 - Thumb rule: calculate one core for each jvm
- Disk
 - Using network storage or virtualized servers
 - Easier to extend

Prepare your Installation

- Download all software packages
- All paths shouldn't contain spaces
 - No spaces in source and destination folders
- Use a dedicated administration user
 - Especially on Windows avoid users with applied group policies

Security Extensions

- During installation you should disable all "Security" Software
 - SELinux
 - AppArmor
 - Antivirus
 - Firewalls
 - Self developed scripts and extensions
- It's not fun, when a script deletes databases, because you forgot to add the directory to the script exclusions

Network

- Name lookup / DNS
 - All servers must be resolvable
 - Knowing the protocol
 - Avoid round robin
- Network storage (file locking is important)
 - NFS v4 / smb|cifs
 - No DFS
- Reverse Proxies / Proxies
 - Test your deployment without proxies
 - When everything works -> enable them

Operating System

- Different operating systems need special settings
- Connections supports
 - Linux
 - Windows Server
 - AIX
 - IBM i
- Always use the operating system where you have the best skills
- Saves time during troubleshooting
- Don't forget your virtualization platform

Operating system - Linux

- `/etc/security/limits.conf`
- Increase `nofile` and `nproc` (see tuning guides)
- Example from tuning guide
 - `root soft nproc 2047`
 - `root hard nproc 16384`
 - Default `nproc` (max number of processes) for user `root` 2047
 - You can extend the `nproc` with `ulimit -p up to 16384`
 - Within `.bashrc`
 - Service definition `/etc/init.d`
 - Or set soft and hard limit to equal sizes, avoids additional changes with profile

Operating system - Windows

- Always use UNC path as Shared Directory
 - Easier to add additional WebSphere Nodes for failover or load balancing
- WebSphere services
 - Technical user account
 - Password never expires
 - Must change password on next login
 - Default: LocalSystem has no network access
- Check access rights on Shared Directory



The screenshot shows the Windows User Accounts control panel window for a user named 'cnxtec'. The 'Full name' is 'IBMCNX Technicalaccount' and the 'Description' is 'Service Account WebSphere'. The 'Password' and 'Confirm password' fields are both masked with dots. Below the password fields, there are four checkboxes: 'User must change password at next logon' (unchecked), 'User cannot change password' (unchecked), 'Password never expires' (checked), and 'Account is disabled' (unchecked).

User name:	cnxtec
Full name:	IBMCNX Technicalaccount
Description:	Service Account WebSphere
Password:	••••••••
Confirm password:	••••••••
<input type="checkbox"/>	User must change password at next logon
<input type="checkbox"/>	User cannot change password
<input checked="" type="checkbox"/>	Password never expires
<input type="checkbox"/>	Account is disabled

Register a service to start WebSphere

- Service for Deployment Manager and NodeAgent(s) are enough
- wasservice.bat/sh
- Map service to a technical user
 - Any Active Directory User is possible
 - Allowed to read / write network share with Shared Content
- Service can parse commands to nodeagent
 - -stopArgs "<NA commands>"
- Configure monitoring policy

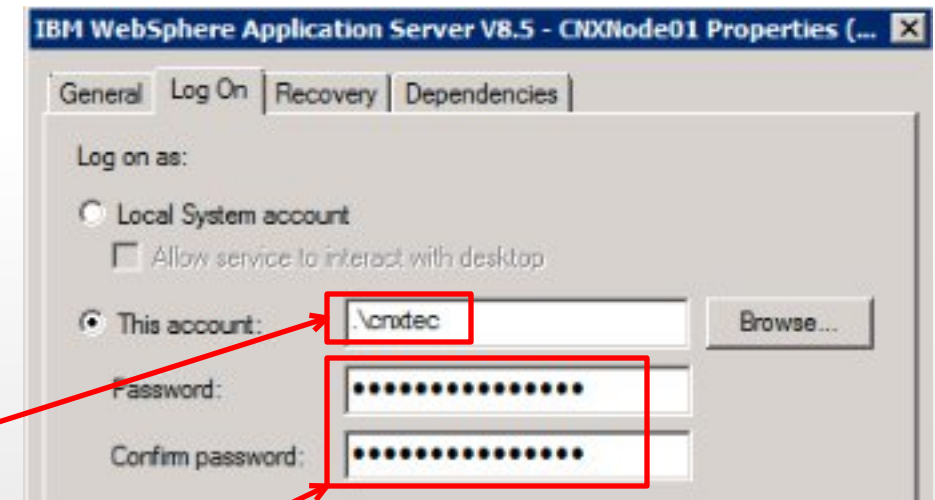
```
Usage: stopNode [options]
options:
  -stopservers [-saveNodeState]
  -quiet
  -logfile <filename>
  -replacelog
  -trace
  -timeout <seconds>
  -statusport <portnumber>
  -conntype <connector type>
  -port <portnumber>
  -username <username>
  -password <password>
  -profileName <profile>
  -help
```


WasService.bat/sh – Register service

```
cd D:\IBMCNX\WebSphere\AppServer\bin
```

```
WASService.exe
```

```
-add CnxNode01  
-serverName nodeagent  
-profilePath d:\ibmcnx\websphere\appserver\profiles\CNXNode01  
-stopArgs "-username wasadmin -password password -stopservers"  
-userid cnxtec -password password  
-encodeParams  
-restart true  
-startType automatic
```



parsed to nodeAgent
stops AppServer

IBM WebSphere Application Server V8.5 - CNXNode01	Controls th...	Started	Automatic	.\cnxtec
IBM WebSphere Application Server V8.5 - CNXNode02	Controls th...	Started	Automatic	.\cnxtec
IBM WebSphere Application Server V8.5 - cnxwin5CellManager01	Controls th...	Started	Automatic	.\cnxtec

Monitoring Policy

- Each Application Server
 - Change Node restart state to "RUNNING"
- Large deployment on Windows
 - Default timeout for service shutdown = 20 seconds
 - HKEY_Local_Machine:
SYSTEM\CurrentControlSet\Control\WaitToKillServiceTimeout



[Application servers](#) > [Cluster1_server1](#) > [MonitoringPoli](#)

Use this page to configure policy settings for performance mon

Configuration

General Properties

* Maximum startup attempts
3 attempts

Ping interval
60 seconds

* Ping timeout
300 seconds

☒ Automatic restart

* Node restart state
RUNNING

STOPPED
✓ RUNNING
PREVIOUS

Apply OK Reset Cancel

Directories and Synchronization

- Prepare your LDAP
 - Better data within LDAP, better Profiles
- Switching Authentication directories is possible, but must be planned
- Dependencies
 - Quality of LDAP data
 - Plans to activate SPNEGO
 - Domino Mail integration

Federated Repositories - Best Practices

- I normally leave the file based wasadmin with WebSphere Application Server
 - Fallback if LDAP Bind Credentials changed
 - Solving problems with Federated Repositories
- Default does not allow this (you have to disable security to change config)

☒ Allow operations if some of the repositories are down

Global security

[Global security](#) > **Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can be configured to use the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name

Server user identity

☒ Automatically generated server identity
☐ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

☒ Ignore case for authorization

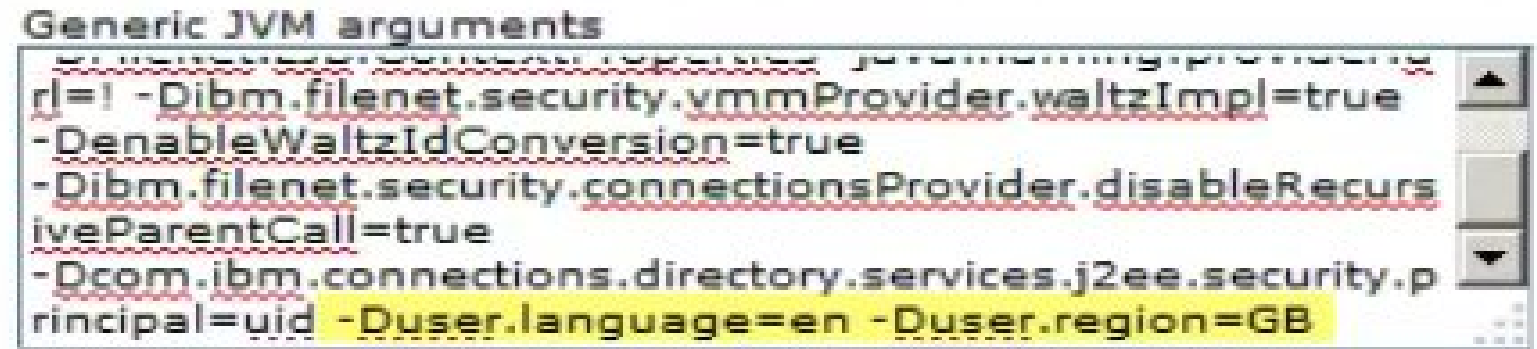
☐ Allow operations if some of the repositories are down

Repositories in the realm:

Set English for all logs

■ WebSphere

- Add "-Duser.language=en -Duser.region=GB" to **Generic JVM arguments** of
 - Each application server (Process definition – Java Virtual Machine)
 - dmgr (System Administration – Deployment Manager – Process Definition ...)
 - nodeagents (System Administration – Node agents – nodeagent – Process Def ...)



■ TDI

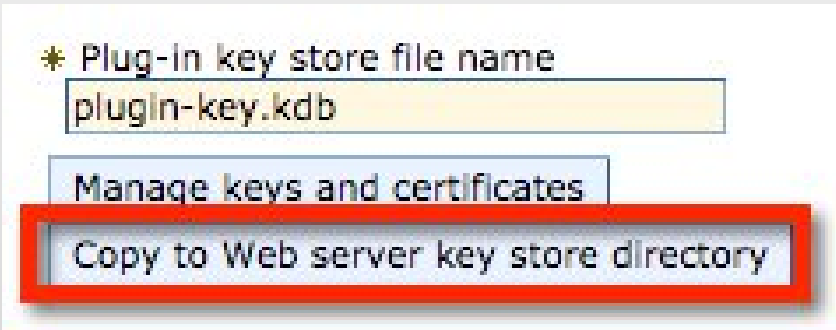
- Edit ibmdisrv.bat/sh
- Add -Duser.language=en -Duser.region=GB to LOG_4J variable

Example:

```
41 rem Take the supported env variables and pass them to Java program  
42 set LOG_4J=-Dlog4j.configuration="file:etc\log4j.properties" -Duser.language=en -Duser.region=GB  
43 set ENV_VARIABLES=%LOG_4J%
```

HTTP Server Keystore

- Several installations i had to review used the Plugin Keystore to hold the IHS SSL key
- Why is this worse? What do you do when SSL errors with Plugins appear?



- plugin-key.kdb at IHS Site is overwritten -> you loose the keys
- Except you imported the keys to CMSKeyStore (never seen this)

<input type="checkbox"/>	CMSKeyStore	CMSKeyStore for web server webserver1.	(cell):cnxwin5Cell01: (node):cnxWebserver: (server):webserver1	\${CONFIG_ROOT}/cells/cnxwin5Cell01/nodes/cnxWebserver/servers/webserver1/plugin-key.kdb
--------------------------	-----------------------------	--	--	--

- Better create a separate Keystore for your Webserver(s)

Security – Disable SSLv3

- Install WebSphere Application Server and Connections Fixes

Product Version	Remediation
IBM Connections 5.0	Upgrade to IBM Connections 5.0 CR1 and WAS Fix Pack 8.5.5.2 ; then apply WAS APAR PI28920
IBM Connections 4.5	Upgrade to IBM Connections 4.5 CR5 and WAS Fix Pack 8.0.0.8 ; then apply WAS APAR PI29575
IBM Connections 4.0	Upgrade to IBM Connections 4.0 CR4 and WAS Fix Pack 7.0.0.35 ; then apply WAS APAR PI28439
IBM Connections 3.0.1.1	Upgrade to IBM Connections 3.0.1.1 CR3 and WAS Fix Pack 7.0.0.35 ; then apply WAS APAR PI28439
IBM Connections 3.0.1 and earlier releases	Either upgrade to IBM Connections 5.0 CR1 and WAS Fix Pack 8.5.5.2 ; then apply WAS APAR PI28920 or upgrade to IBM Connections 3.0.1.1 CR3 and WAS Fix Pack 7.0.0.35 ; then apply WAS APAR PI28439

- <http://ibmconnections.com/news/poodle-in-the-repeat/> (thanks Sjaak Ursinus)
- PI28920 does not work in one of my environments too, so I applied [PI28437](#)
- Install Fix to all WebSphere components (WAS, HTTP, Plugins, WCT)

- HTTPServer/conf/httpd.conf

- SSLProtocolDisable SSLv3 SSLv2

Security – Configure WebSphere to use TLS

- ISC – Security – SSL certificate and key management – SSL configurations

CellDefaultSSLSettings	(cell):cnxwin5Cell01
NodeDefaultSSLSettings	(cell):cnxwin5Cell01:(node):cnxwin5Node01
NodeDefaultSSLSettings	(cell):cnxwin5Cell01:(node):cnxwin5Node02
XDADefaultSSLSettings	(cell):cnxwin5Cell01

[SSL certificate and key management](#) > [SSL configurations](#) > [CellDefaultSSLSettings](#) > **Quality of protection (QoP) settings**

Specifies the security level, ciphers, and mutual authentication settings.

General Properties

Client authentication
None

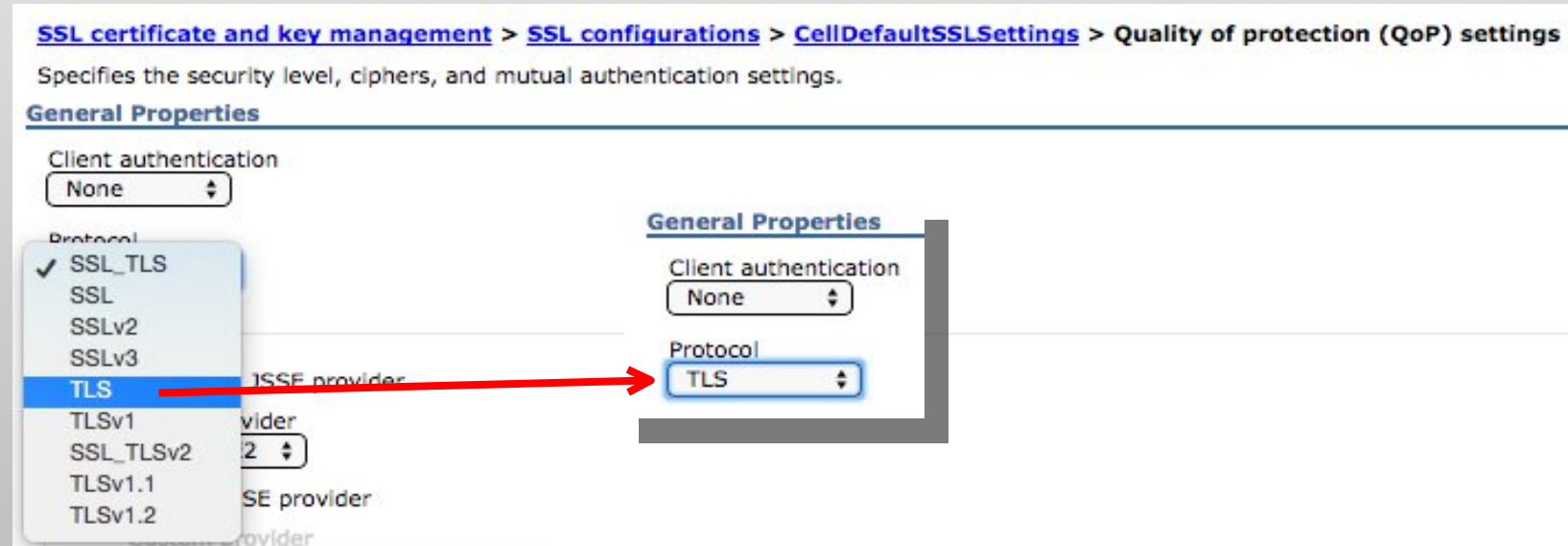
Protocol
SSL_TLS
SSL
SSLv2
SSLv3
TLS
TLSv1
SSL_TLSv2
TLSv1.1
TLSv1.2

SSLSE provider
provider
2
SE provider
provider

General Properties

Client authentication
None

Protocol
TLS

A screenshot of the WebSphere administrative console showing the 'Quality of protection (QoP) settings' for 'CellDefaultSSLSettings'. The 'General Properties' section is visible, showing 'Client authentication' set to 'None'. A dropdown menu for 'Protocol' is open, showing options: SSL_TLS, SSL, SSLv2, SSLv3, TLS (highlighted), TLSv1, SSL_TLSv2, TLSv1.1, and TLSv1.2. A red arrow points from the 'TLS' option in the dropdown to the 'Protocol' dropdown in the 'General Properties' section, which currently shows 'TLS'. Other partially visible options include 'SSLSE provider', 'provider', '2', 'SE provider', and 'provider'.

Checking Supported SSL Protocols

- `ssllscan --no-failed <connectionserver/webserver>`

without "SSLProtocolDisable SSLv3"

Testing SSL server cnxwin5.stoepe.local on port 443

Supported Server Cipher(s):

Accepted	SSLv3	256 bits	AES256-SHA
Accepted	SSLv3	168 bits	DES-CBC3-SHA
Accepted	SSLv3	128 bits	AES128-SHA
Accepted	SSLv3	128 bits	RC4-SHA
Accepted	SSLv3	128 bits	RC4-MD5
Accepted	TLSv1	256 bits	AES256-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Accepted	TLSv1	128 bits	AES128-SHA
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5

Preferred Server Cipher(s):

SSLv3	128 bits	AES128-SHA
TLSv1	128 bits	AES128-SHA

SSLProtocolDisable SSLv3

```
root@kali:~# ssllscan --no-failed cnxwin5.stoepe.local
```



Version 1.8.2

<http://www.titania.co.uk>

Copyright Ian Ventura-Whiting 2009

Testing SSL server cnxwin5.stoepe.local on port 443

Supported Server Cipher(s):

Accepted	TLSv1	256 bits	AES256-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Accepted	TLSv1	128 bits	AES128-SHA
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5

Preferred Server Cipher(s):

TLSv1	128 bits	AES128-SHA
-------	----------	------------

Check SSL Protocols on WebSphere

- `sslsan -no-failed <wasserver:9043>` (your ISC host)
- `sslsan -no-failed <wasserver:9444>` (your WebSphere host)

Testing SSL server cnxwin5.stoepe.local on port 9043

Supported Server Cipher(s):

Accepted	TLSv1	168 bits	EDH-RSA-DES-CBC3-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Accepted	TLSv1	128 bits	DHE-RSA-AES128-SHA
Accepted	TLSv1	128 bits	AES128-SHA
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5

Preferred Server Cipher(s):

TLSv1 168 bits EDH-RSA-DES-CBC3-SHA

Testing SSL server cnxwin5.stoepe.local on port 9444

Supported Server Cipher(s):

Accepted	TLSv1	168 bits	EDH-RSA-DES-CBC3-SHA
Accepted	TLSv1	168 bits	DES-CBC3-SHA
Accepted	TLSv1	128 bits	DHE-RSA-AES128-SHA
Accepted	TLSv1	128 bits	AES128-SHA
Accepted	TLSv1	128 bits	RC4-SHA
Accepted	TLSv1	128 bits	RC4-MD5

Preferred Server Cipher(s):

TLSv1 168 bits EDH-RSA-DES-CBC3-SHA

- Check SystemOut.logs if InterService can access all applications

```
executeWithRetry I/O exception (javax.net.ssl.SSLHandshakeException) caught when processing request: Received fatal alert: handshake_failure
executeWithRetry Retrying request
executeWithRetry I/O exception (javax.net.ssl.SSLHandshakeException) caught when processing request: Received fatal alert: handshake_failure
```

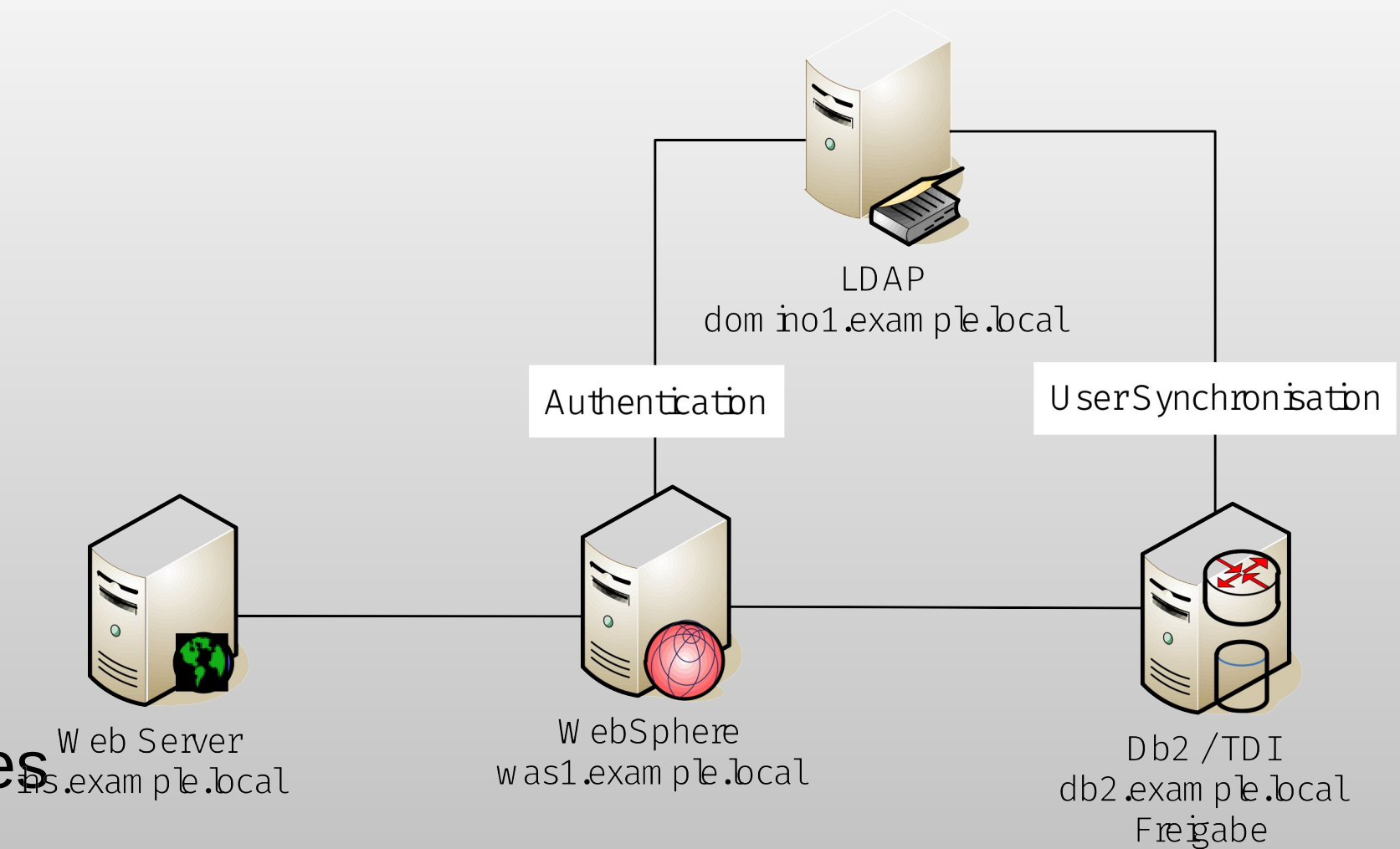
TUNING

Performance Tuning Guide

- 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
- Read everything carefully
- Check and understand dependencies

Worst practice example – Tuning

- Customer showed me a system with following infrastructure
- WebSphere
 - Large deployment
 - 16 GB RAM
 - 4 Cores
- DB2
 - 12 instances
 - 8 GB RAM
 - 4 Cores
- Connections restart: 22 minutes

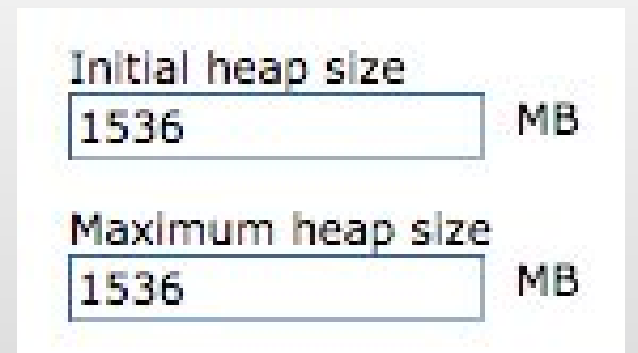


Solving this

- Large deployment means about 15 JVM on the machine
 - Restart shows 15 min 100% CPU usage
 - Adding 4 cores and restart time get down to 7 minutes
 - Other option would be midsize deployment, but then you have to reinstall Connections
- Java Heap Sizes set to default (256 MB and 768 MB) -> increase to 1.5 – 2.5 GB
- Perf Guide mentions that multiple instances on DB2 only increase performance with enough resources
 - But that was not the real problem
- DataSource connectionPool Sizes are set to Default 1/10
 - Increase this values to the proposals in the guide and ...
 - Restart time comes down under 3 minutes
- Key point: read the complete guide

Java Heap Size

- Default Java Heap Sizes on Midsize Deployment: 2506 MB / application server
- Large Deployment depends on application: 0.5 to 2.5 GB
- Main part in memory tuning
 - Never exceed the system memory
 - **SWAPPING KILLS ALL YOUR TUNING EFFORTS**
- Summing the JVM Heap sizes is not enough
 - Maximum heap is not the maximum amount of memory the jvm uses!
 - Libraries, jars and so on count additional to memory usage
 - JVM memory usage may be 3 * JVM maximum Heap
- Initial and Maximum Heap Size should be equalized



Initial heap size
1536 MB

Maximum heap size
1536 MB

IBM HTTPServer

- Activate Rotatelog to get your access.log and error.log manageable
 - access.log often gets up to some GB of size
 - only few editors can open this sizes, hard to troubleshoot then
 - Comment out:
 - # CustomLog logs/access.log common
 - Rollover by size (after 500MB create new log):
 - CustomLog "|D:/IBM/HTTPServer/bin/rotatelog.exe D:/IBM/HTTPServer/logs/access-%Y%m%d.log 500M" common
 - Rollover by time (new log each day):
 - CustomLog "|D:/IBM/HTTPServer/bin/rotatelog.exe logs/access-%Y%m%d.log 86400" common
 - You have to create a script to delete old logfiles!

IBM HTTPServer (2)

- Enable compression
 - Important
 - See Slides from [BP307 - IBM Connect 2014](#)
 - Saves up to 70% network traffic
 - Minimal increase of CPU load
- Enable file download through IHS
 - Depends on your deployment
 - Often security forbids storage access from DMZ
- If you have no access to file share from IHS -> Files should be installed in a separate Cluster

ENHANCE USER EXPERIENCE

Happy admins with happy users

User Synchronization

- IBM provides some great batch files and assembly lines
- TDI Solution Best Practices
 - Do not use tdisol from Wizards Archive
 - I often find scheduler which links directly to the used wizard folder
 - Never seen updates applied to these folders
- Updated archives can be found in <connections root>\tdisol
- With 4 and 4.5 often special TDISOL Update packages on Fixcentral
 - You should deploy them
 - Do not copy files between old and new configuration
 - Use diff and change needed values

Be aware of sync_updates_hash_field

- Possible values
 - uid (default)
 - guid
 - email
- Value is used to find matching persons between LDAP and peopleDB
- Possible problems
 - User renaming
 - Shortname reuse (retired and newly hired users)
- What happens when you rename a Domino user?
 - email address changes
 - shortname (uid) is added on first places

What can happen

- sync_updates_hash_field=uid
 - User is renamed
 - Normally no problem, because in Domino Shortname can store multivalues
 - User retires
 - Inactivated or deleted user within Profiles
 - User hires again
 - User is reactivated
 - Other User with same UID hires
 - Will get all data from old user account (picture, tags, community membership)
 - Splitting of this content is not possible

What can happen

- sync_updates_hash_field=email
 - User is renamed
 - On first TDI run the user gets inactivated
 - New profile will be created
 - Or you get Duplicate Login value errors, because UID still exists
 - No content available -> you must manually map the content to the new account
 - User retires
 - Inactivated or deleted user within Profiles
 - User hires again
 - User is reactivated
 - Other User with same mail address hires
 - Will get all data from old user account (picture tags community membership)

What can happen

- sync_updates_hash_field=guid
 - User is renamed
 - All data synchronize with LDAP
 - User retires
 - Inactivated or deleted user within Profiles
 - Within Domino the person document is deleted
 - User hires again
 - Newly registered user has new guid
 - New profile
 - Duplicate login data -> no new profile
 - you can use `populate_from_dn_file.bat/collect.dns` to sync this, because this always uses the UID for hashing

Single Sign On - LtpaToken

- Single Sign On within IBM portfolio
- Domino only supports one domain per Web SSO Document
 - You can copy & paste Web SSO Documents and change Domain names (see e.g. [Paul Mooney - AdminBlast 2012 – Tip #4](#))
 - DNS Domain is multi value (works until Domino 8.5.x, but not with Domino 9.x)
 - Servers with mixed Internet Site and Non-Internet Site usage: copy & paste too!
- Often internal servers use local domains, when Connections is external accessible SSO needs workaround
 - Adding additional hostnames to domino
 - You can use IHS (IBM HTTP Server) or nginx as a reverse proxy to access iNotes

Mail integration





- Use IBM HTTP Server as reverse proxy to access iNotes

```
LoadModule rewrite_module modules/mod_rewrite.so
<IfModule mod_ibm_ssl.c>
    Listen 0.0.0.0:1443
    <VirtualHost *:1443>
        ServerName connections.example.com
        SSLEnable
        RewriteEngine on
        ProxyRequests Off
        ProxyPass /
http://inotes.example.local/
        ProxyPassReverse /
http://inotes.example.local/
    </VirtualHost>
</IfModule>
```


iNotes WebMail Redirect

IBM iNotes Redirect configuration

Save & Exit

 Server Settings  UI Setup  Ultra-light/Mobile Settings  Application Setup

Please select the Redirection type

 Help

Fixed
Dynamic
MailServer

Please enter the server name to use
i.e., <http://mail.lotus.com> (or use https:// to use SSL) `https://connections.example.com:1443`

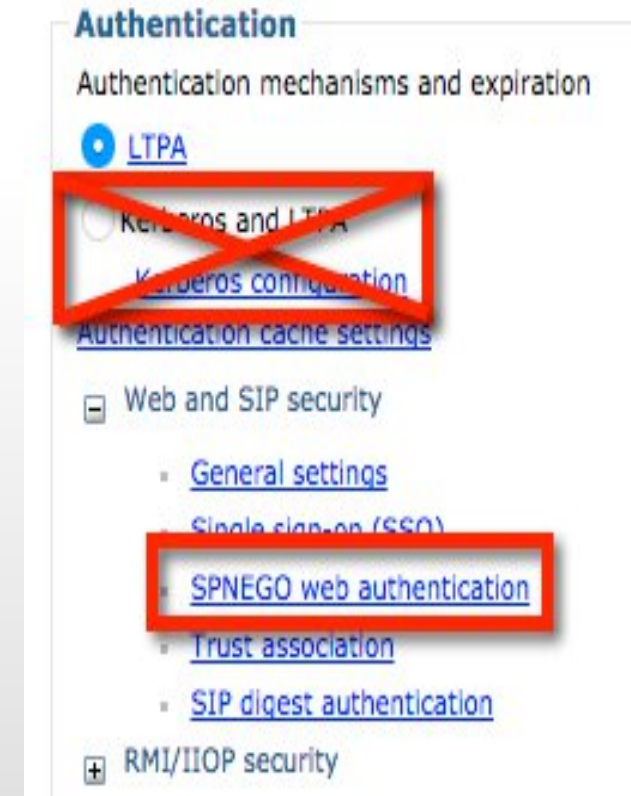
Socialmail-config.xml

- When you use reverse proxy to access iNotes
 - Mail integration works only when you use http or https
 - Remember to add UseConfiguredProtocol to your config
- Problem when you need to access multiple iNotes Servers

```
<ServerConfig name="domino-redirect">
  <ConfigType>REDIRECT</ConfigType>
  <RedirectURL>https://connections.example.com:1443/iwaredir.nsf</RedirectURL>
  <MailPattern type="example.com" />
</ServerConfig>
<GadgetConfig>
  <GadgetPreference id="UseConfiguredProtocol">true</GadgetPreference>
</GadgetConfig>
```

Single Sign On - SPNEGO

- Requirements
 - Windows 2003 / 2008 Active Directory
 - Websphere Service must start as Domain User
 - connectionsAdmin j2c Alias must be a LDAP User
- Configure use documentation and http://de.slideshare.net/david_hay/dave-hay-desktop-single-signon-in-an-active-directory-world?related=1
- Real value for users
- Easy to deploy, when you have the rights and clue what to do
- Do not test Browser Single Sign On with Chrome, because process does not end when you close the last window



Mail integration and SPNEGO

- LtpaToken contains AD \$DN
- Lookup in Domino Directory with this DN -> user is not allowed to open mail
- Solution
 - Add AD \$DN to ACL
 - Or add AD \$DN to Domino Fullname (AD DN contains , as delimiter between ou)
- Good to work on your TDI skills

BACKUP

Backup - Overview

- I got several calls from customers which installed Connections with installation guides
 - These guides normally do not mention backup
 - 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
 - There are some posts on DB2 Online Backups on
 - Klaus Bild Blog <http://kbild.ch>

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

Checklist

Do's

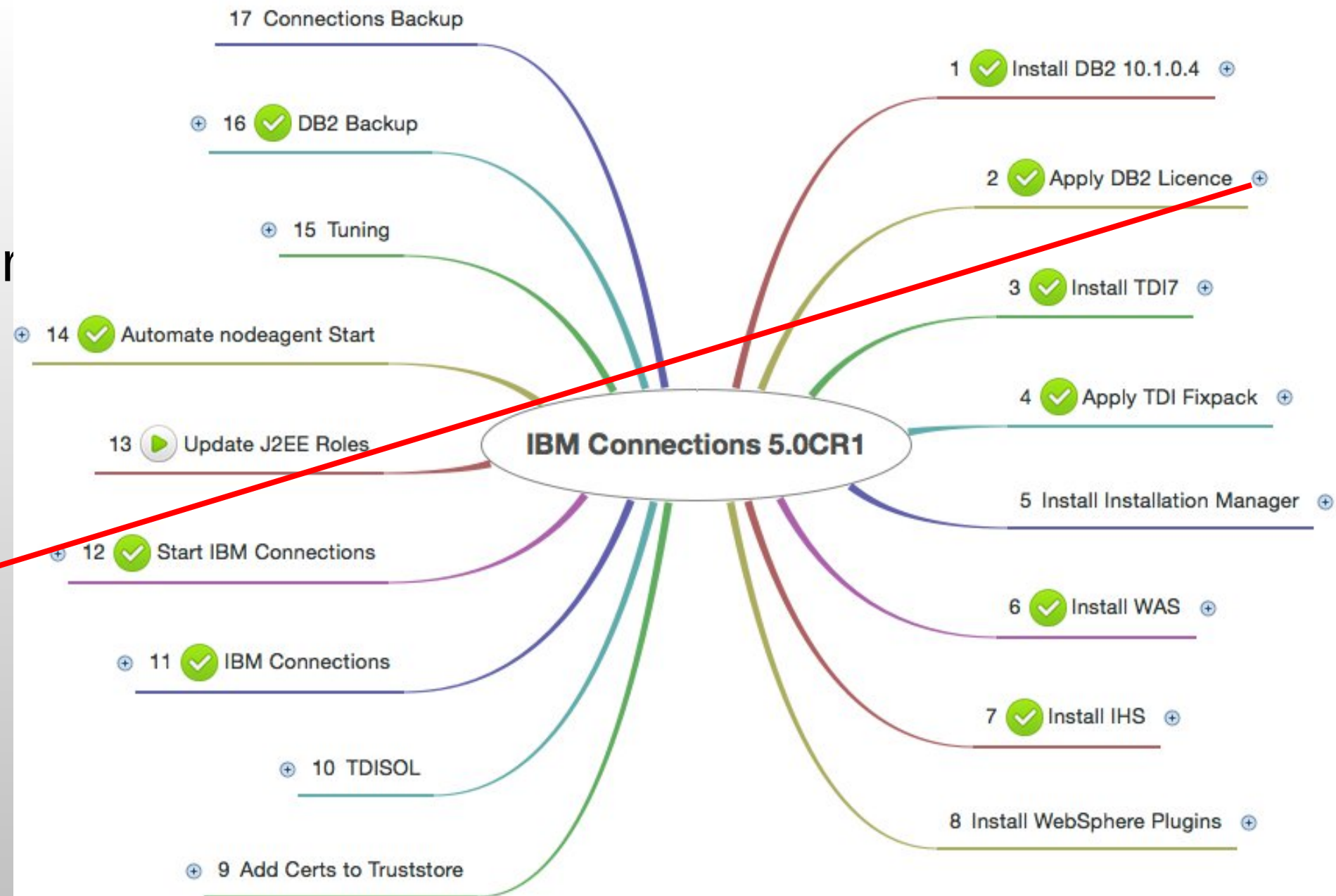
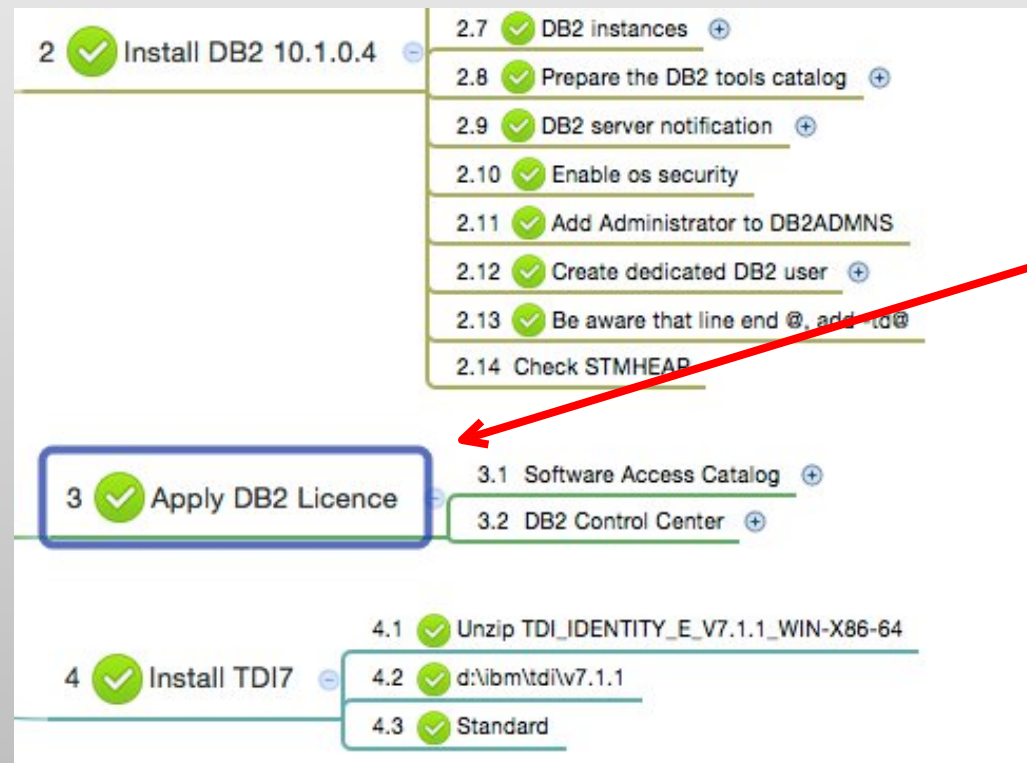
- Create a documentation of all installation steps
 - Documentation sometimes confusing, because all OS within one document
- Be prepared for scaling
 - Shared directory on UNC path
 - No small deployment installations
- Tune your environment
- Deactivate Antivirus
- Deactivate "Security" Tools during installation & SELinux / AppArmor

Don'ts

- Use multiinstance DB2 with small resources
- Install on a single machine
- Copy customizations to newer versions
 - jsp, ftl copy will break something
- Use unstable file shares
- Test deployment with Server Internet Explorer
- Test with only one (english) language
- Unzip with Windows Explorer built-in tool
- Untar with AIX tar

Installation Checklist

- Create a checklist or mindmap
- Add all steps you want or need to do



Documentation of your environments

- Create valid documentation and keep it up-to-date
 - Nobody likes creating documentations (except Sharon)
- Good overview for troubleshooting and migrations
- Nobody needs long text versions or hundreds of screenshots
- Use the Sheet provided within the documentation
 - http://www-01.ibm.com/support/knowledgecenter/SSYGQH_5.0.0/admin/plan/r_worksheet_in_stallation.dita
- Or download a Microsoft Excel version of this at (Thanks to Keith Brooks)
 - <http://blog.vanessabrooks.com/p/downloads.html>

Tools

- Editor with syntax highlighting
 - vim, geany
 - notepad++
- Tail
 - baretail
 - multital
 - mtail
- Proxy
 - Fiddler
(often asked by IBM Support too)
 - Burpsuite (intercept proxy)
- Browser
 - Firefox (portable) / Firefox ESR
 - Chrome
 - IE (download vm with different versions)
 - <https://www.modern.ie/en-us/virtualization-tools>
- Network analyzer
 - Wireshark
 - tcpdump
- Unzip / Unarchiver
 - 7-zip

Links

- [IBM Connections Requirements](#)
- [Official Documentation Connections family](#)
- [Connections 5 Documentation](#)
- [Tuning Guide 4.0](#)
- [Tuning Guide Addendum 4.5](#)
- [Tuning Guide 5.0CR1](#)
- **POODLE Fix (IMPORTANT):**
 - <http://ibmconnections.com/news/poodle-in-the-repeat/>
 - <http://www-01.ibm.com/support/docview.wss?uid=swg21690640>
 - <http://www-01.ibm.com/support/docview.wss?uid=swg21688357>
 - <http://www-01.ibm.com/support/docview.wss?uid=swg21687173>
 - <http://www-01.ibm.com/support/docview.wss?uid=swg21687172>

Blogs with IBM Connections stuff

- <http://www.stoeps.de>
- <http://scripting101.org>
- <http://martin.leyrer.priv.at/>
- <http://kbild.ch>
- <http://dilf.me.uk/socialshazza>
- <http://www.notesgoddess.net>
- <http://ibmconnections.com>
- <http://notesbusters.com>
- <http://wannes.rams.be>
- <http://turtleblog.info>
- <http://portal2portal.blogspot.de>
- <https://www.urspringer.de>
- <http://meisenzahl.org/>
- <http://blog.robertfarstad.com>
- <http://www.curiousmitch.com>
- <http://socialconnections.info>
- Have a look at Planetlotus.org

QUESTIONS

Engage Online

- **SocialBiz User Group** socialbizug.org
 - Join the epicenter of Notes and Collaboration user groups
- **Social Business Insights blog** ibm.com/blogs/socialbusiness
 - Read and engage with our bloggers
- **Follow us on Twitter**
 - [@IBMConnect](https://twitter.com/IBMConnect) and [@IBMSocialBiz](https://twitter.com/IBMSocialBiz)
- **LinkedIn** <http://bit.ly/SBComm>
 - Participate in the IBM Social Business group on LinkedIn
- **Facebook** <https://www.facebook.com/IBMConnected>
 - Like IBM Social Business on Facebook