1049 - Best and Worst Practices for Deploying IBM Connections

Christoph Stoettner – panagenda – 1. February 2016
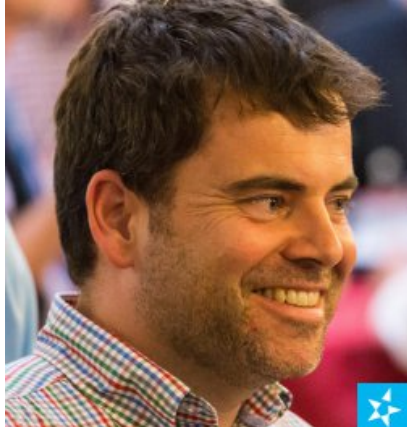
Connect 2016

The Premier Social Business and Digital Experience Conference

Make Every **Moment** Count

#ibmconnect

Christoph Stoettner

a @stoeps
j christoph-stoettner

IBM**CHAMPION**

*pan*agenda

- Senior Consultant – panagenda
  - IBM Notes / Domino since 1999
  - IBM Connections since version 2.5 / 2009
- Many years of experience in:
  - Migrations
  - Administration und installs
  - Performance analysis
- Joined panagenda in 2015 focusing in:
  - IBM Connections deployment und optimization
  - IBM Connections monitoring
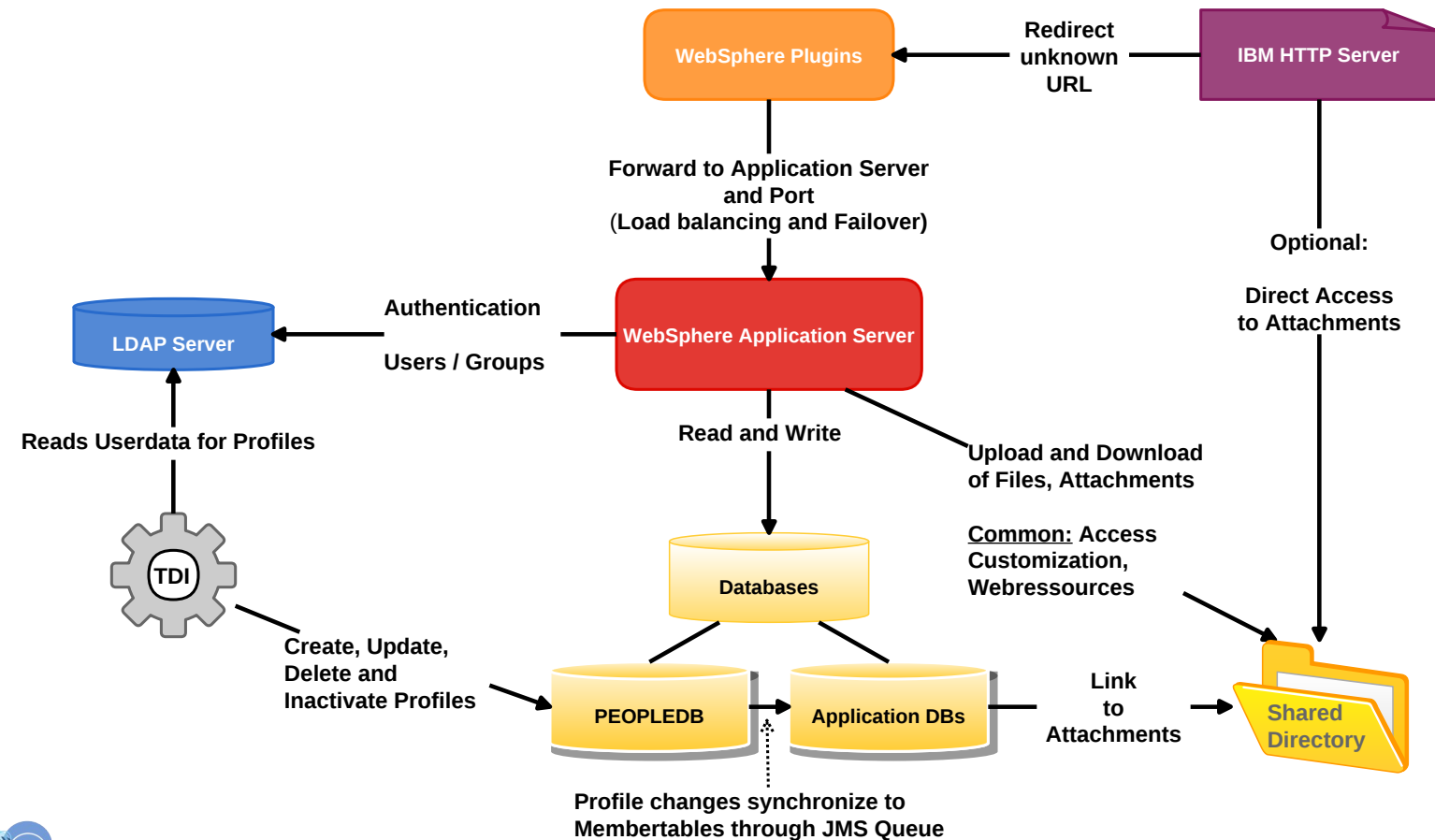- Husband of one & father of two, Bavarian

Make Every **Moment** Count

Agenda

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

Make Every **Moment** Count

Connect 2016

The Premier Social Business and Digital Experience Conference

WebSphere Plugins

IBM HTTP Server

Redirect unknown URL

Forward to Application Server and Port
(Load balancing and Failover)

Optional:

Direct Access to Attachments

WebSphere Application Server

Authentication

Users / Groups

LDAP Server

Reads Userdata for Profiles

Upload and Download of Files, Attachments

Common: Access Customization, Webressources

Read and Write

TDI

Create, Update, Delete and Inactivate Profiles

Databases

PEOPLEDB

Application DBs

Link to Attachments

Shared Directory

Profile changes synchronize to Membertables through JMS Queue

Installation & Requirements

Connect 2016

The Premier Social Business and Digital Experience Conference

Make Every **Moment** Count

#ibmconnect

System Requirements

- Regularly check requirement documents
- All versions
  - http://short.stoeps.de/vwzrv
- IBM Connections 5
  - http://short.stoeps.de/mspdi
- IBM Connections 5.5
  - http://short.stoeps.de/cnx55sysreq
- Check all notes, Download PDF

Connections 5.5 Connections 5.0 CR3

Connect 2016
The Premier Social Business and Digital Experience Conference

System Requirements

- Be careful with installation documents

  - Sometimes wrong dependencies mentioned

  - Supported statement does not mean it's licensed

    - http://www-01.ibm.com/support/docview.wss?uid=swg21683118

    - Supported: DB2 10.5 FP4 ->
      but Connections 5.0 License Agreement:

      IBM DB2 Enterprise Server Edition Version 10.1

      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

    - You will not find a DB2 10.5 license in your PA Account

Connect 2016

The Premier Social Business and Digital Experience Conference

Sizing

- Be prepared for future growth
- Do not overact
  - Some hundred users mostly won't need a large deployment
- I'm not a fan of multi-instance database machines
  - If I run in database performance issues I split the databases to different machines
  - Performance tuning guide
    - Multi-instance is best practice, **if you have enough resources**

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.

Sizing (2)

- A word to minimum requirements

  - 4 | 8 GB memory minimum is often too less, better starting with 10 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 (expensive with PVU license)

- Disk

  - Using network storage or virtualized servers
  - Easier to extend

Connections 5.6

Memory requirement for x86-32/64 and POWER Intel (x86-32 or x86-64 compatible server systems) and POWER systems Per IBM Connections node:

Application Node:
Two processor cores per server, 2.0 GHz CPU speed, or higher
Minimum 4 GB of memory for IBM Connections Server
- For enterprise-scale deployments, at least 16 GB of memory is recommended

Database server:
Two processor cores per server, 2.0 GHz CPU speed, or higher
Minimum 4 GB of memory
- For enterprise-scale deployment, at least 16 GB of memory is recommended

50 GB of available disk space after installation and configuration of the base operating system

Prepare your Installation

- Download all software packages
  - Check System Requirements!
- 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
  - If possible disable User Account Control (UAC)
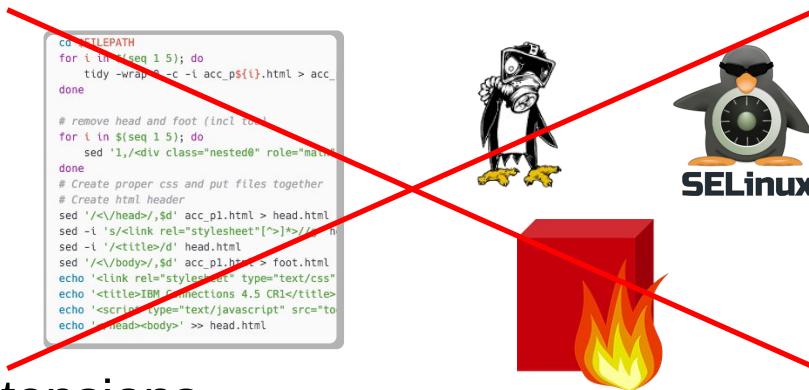 - Run all Installer and Scripts with option "Run As Administrator"

Make Every **Moment** Count

Connect 2016

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

Connect2016

Network

- Name lookup / DNS
  - All servers must be resolvable (hosts is not a suitable workaround)
  - Knowing 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
- Reverse Proxies / Proxies
  - Always test your deployment without proxies
  - Activate after successful testing

Connect 2016
The Premier Social Business and Digital Experience Conference
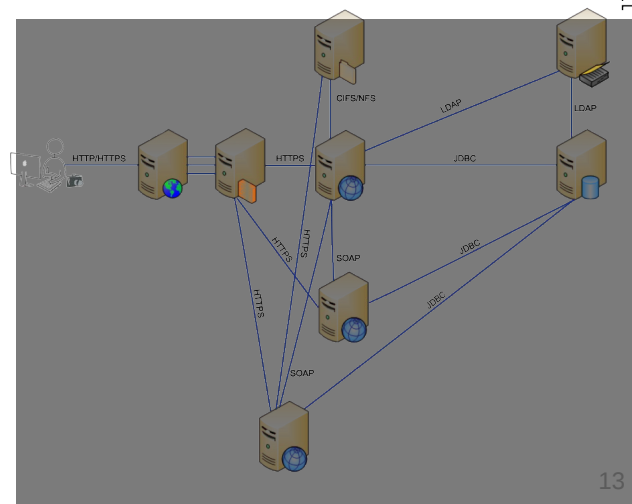
Operating system - Linux

- Different operating systems need special settings
- Always use the operating system where you have the best skills
- 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 (e.g. within bashrc)
  - 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

    - Enable "Password never expires"

    - Disable "Must change password on next login"

  - Default: LocalSystem has no network access

- Check access rights on Shared Directory

User name:	cnxtec
Full name:	IBMCNX Technicalaccount
Description:	Service Account WebSphere
Password:	••••••••
Confirm password:	••••••••

- ☐ User must change password at next logon
- ☐ User cannot change password
- ☑ Password never expires
- ☐ Account is disabled

Register a service to start WebSphere

- Services for Deployment Manager and NodeAgent(s)
  - 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>
                -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
```
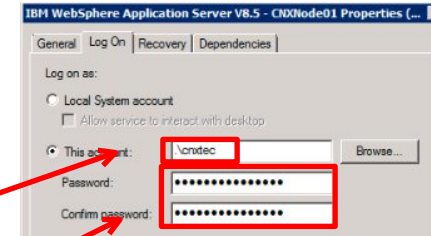
parsed to nodeAgent

stops AppServer

IBM WebSphere Application Server V8.5 - CNXNode01 Properties (...)

General | Log On | Recovery | Dependencies

Log on as:

○ Local System account
☐ Allow service to interact with desktop

● This account: .\cnxtec   Browse...

Password: ●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●

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

  - Increase Value at: HKEY_Local_Machine: SYSTEM\CurrentControlSet\Control\ WaitToKillServiceTimeout

Directories and Synchronization

- Prepare your LDAP

  - Better data within LDAP $\rightarrow$ better Profiles

- Switching Authentication directories is possible

  - Need some planning

- Dependencies

  - Quality of LDAP data

  - Plans to activate SPNEGO

  - Domino Mail Integration

Christoph Stoettner
Senior Consultant
panagenda
Heppenheim , Hessen , Germany
+49 6252 67939-
christoph.stoettner@panagenda.com
Local Time: 3:35 PM

Send Email   Download vCard

Recent Updates   **Contact Information**   Background

Name:	**Christoph Stoettner**
Office number:	+49 625
Mobile number:	+49 173
Fax number:	+49 625
Office email:	christoph.stoettner@panagenda.com
Job title:	Senior Consultant

Report-to Chain   ≡

- Henning Kunz
  - Christoph Stoettner

Full Report-to Chain
Same Manager

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 configuration)

The Premier Social Business and Digital Experience Conference

Set English for all Logs - WebSphere

- WebSphere
  - Add "-Duser.language=en –Duser.region=US" 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 ...)

Generic JVM arguments

```
-Xgcpolicy:gencon -Djava.awt.headless=true -Duser.language=en
-Duser.region=US
```
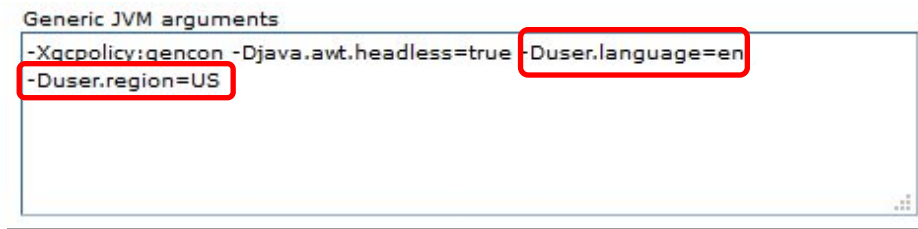
Set English for all logs - TDI

- TDI

  - edit ibmdisrv.bat|sh

  - add -Duser.language=en –Duser.region=US
    to LOG_4J variable

  - Linux:

```
# Log4j configuration file
LOG_4J="-Dlog4j.configuration=file:etc/log4j.properties -Duser.language=en -Duser.region=US"

"$TDI_JAVA_PROGRAM" $TDI_MIXEDMODE_FLAG -cp "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" com.ibm.di.loader.ServerLauncher "$@" &
```

  - Windows:

```
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%
```

Log rotate - WebSphere

- WebSphere Logs too small for Troubleshooting
  - Default: 5 Logs 1 MB each (SystemOut and SystemErr)
  - Better 5-10 Logs 20 MB each
    - Setting for each Application Server
    - remember Nodeagents and Dmgr

Log rotate - WebSphere

- IBM Connections 5.5

  - ■ Install.log

```
Update WebContainer Thread Pool settings:  [['maximumSize', 75], ['minimumSize', 50]]
Update SystemOut.log settings:  [['maxNumberOfBackupFiles', 30], ['baseHour', 24], ['rolloverSize', 10], ['rolloverPeriod', 24], ['rolloverType', 'TIME']]
Update SystemErr.log settings:  [['maxNumberOfBackupFiles', 30], ['baseHour', 24], ['rolloverSize', 10], ['rolloverPeriod', 24], ['rolloverType', 'TIME']]
```

  - ■ Result:

  - ■ So your logs are stored 30 days, independent of size

Rotate Logs – IBM HTTP Server

- Default: no max size for access_log and error_log
- Often some GB of Log files
    - Open with an Editor?
    - Disk size
- Search for this lines in httpd.conf:

CustomLog log/access_log common

ErrorLog logs/error_log

- Comment out:

CustomLog log/access_log common

ErrorLog logs/error_log

Rotate Logs – IBM HTTP Server

- Add:

```
Linux:
CustomLog "|/opt/IBM/HTTPServer/bin/rotatelogs /opt/IBM/HTTPServer/logs/access_log.%Y%m%d 86400" common
ErrorLog "|/opt/IBM/HTTPServer/bin/rotatelogs /opt/IBM/HTTPServer/logs/error_log.%Y%m%d 86400"

Windows:
CustomLog "|D:/IBM/HTTPServer/bin/rotatelogs.exe D:/IBM/HTTPServer/logs/access_log.%Y%m%d 86400" common
ErrorLog "|D:/IBM/HTTPServer/bin/rotatelogs.exe D:/IBM/HTTPServer/logs/error_log.%Y%m%d 86400"
```

- Delete Log Files older than x days

  - Linux

  - ```
    crontab -e
    # Delete logfiles older than 3 days in logs
    10 0 * * * find /opt/IBM/HTTPServer/logs/*_log.* -mtime +3 -exec rm -rf {} \;
    ```

  - Windows (Batch through Task Scheduler or Powershell)

    ```
    forfiles -p "D:\IBM\HTTPServer\logs" -s -m *_log.* -d -3 -c "cmd /c echo @file"
    ```

Rotate Logs – DB2

- db2diag.log
- Default: no maximum size
  - Default: %PROGRAMDATA%\IBM\DB2\instancename\DB2
  - Full C-Partition in Windows still hard to solve

```
[db2inst1@cnx-db2 ~]$ db2 get dbm cfg |grep -i diagsize
Size of rotating db2diag & notify logs (MB)  (DIAGSIZE) = 0

[db2inst1@cnx-db2 ~]$ db2 update dbm cfg using DIAGSIZE 1024
DB20000I  The UPDATE DATABASE MANAGER CONFIGURATION command completed successfully.

[db2inst1@cnx-db2 ~]$ db2 get dbm cfg |grep -i diagsize
Size of rotating db2diag & notify logs (MB)  (DIAGSIZE) = 1024
```

Connect 2016

The Premier Social Business and Digital Experience Conference

HTTP Server Keystore

- Several Reviews showed

    - Keystore of WebSphere Plugin used for IHS SSL Key

    - Why is this worse?

    - What would you c ... rors within Connections?

    Plug-in key store file name
    plugin-key.kdb

    Manage keys and certificates

    Copy to Web server key store directory

    - This overwrites plugin-key.kdb on your Webserver

    - SSL Key deleted

    - Backup?

Make Every **Moment** Count

Connect 2016
The Premier Social Business and Digital Experience Conference

HTTP Server Key store

- When you want to reuse Plugin Key store
  - Import SSL Key into CMSKeyStore
  - But never seen this in the wild

	CMSKeyStore	CMSKeyStore for web server webserver1.	(cell):cnxwin5Cell01: (node):cnxWebserver: (server):webserver1	${CONFIG_ROOT}/cells/cnxwin5Cell01/nodes/cnxWebserver/servers/webserver1/plugin-key.kdb

- BP: Create a separate key store for IHS
  - ikeyman will help you

Connect 2016

Default J2EE Roles

- Some Applications are publi[c]
  - Profiles
  - Communities
  - Blogs

- Check after Updates
  - Google: "Site:myconnections-host"
  - Should only show a login page

| Map Users... | Map Groups... | Map Special Subjects ▾ |

Select	Role	Special subjects	Mapped users	Mapped groups
☐	everyone	Everyone		
☐	reader	None	ldapconntest	ConnectionsTestUsersInternal
☐	person	None	ldapconntest	ConnectionsTestUsersInternal
☐	allAuthenticated	None	ldapconntest	ConnectionsTestUsersInternal
☐	metrics-reader	None	ldapconntest	ConnectionsTestAdmins
☐	admin	None	wasadmin ldapconntest	ConnectionsTestAdmins
☐	search-admin	None	wasadmin ldapconntest	ConnectionsTestAdmins
☐	dsx-admin	None	wasadmin ldapconntest	
☐	org-admin	None	wasadmin ldapconntest	
☐	bss-provisioning-admin	None		

Harden HTTP Server

- Disable SSLv2 / v3
  - Automatically disabled with 8.5.5.4
  - SSLProtocolDisable SSlv2 SSLv3
- Check with
  hydra, nmap or ssllabs.com/ssltest/
- Default httpd.conf uses:
  TLS_RSA_WITH_3DES_EDE_CBC_SHA

      # Ciphers TLS1.0, 1.1
      SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA
      SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA
      # Additional Ciphers TLS1.2
      SSLCipherSpec TLS_RSA_WITH_AES_128_GCM_SHA256
      SSLCipherSpec TLS_RSA_WITH_AES_256_GCM_SHA384
      SSLCipherSpec TLS_RSA_WITH_AES_128_CBC_SHA256
      SSLCipherSpec TLS_RSA_WITH_AES_256_CBC_SHA256


```
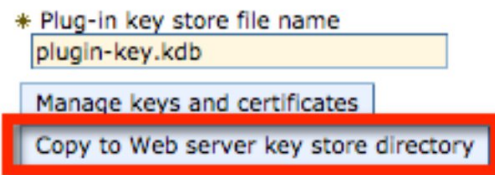1 root@kali ~ # nmap --script ssl-enum-ciphers -p 443 connections-
root@kali ~ # nmap --script ssl-enum-ciphers -p 443 connections-

Starting Nmap 7.01 ( https://nmap.org ) at 2016-01-07 04:47 EST
Nmap scan report for connections-test50.          .com (10.10.        )
Host is up (0.0029s latency).
rDNS record for 10.10.
PORT     STATE SERVICE
443/tcp open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Weak certificate signature: SHA1
|   TLSv1.1:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Weak certificate signature: SHA1
|   TLSv1.2:
|     ciphers:
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_GCM_SHA384 (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA256 (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA256 (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       Weak certificate signature: SHA1
|_  least strength: A

|_  least strength: C
```

Connect 2016

Harden HTTP Server

- If you use SSL Keys longer than 2048 bit, you must replace

  - Download and replace Java (unrestricted) policy files

  - https://www-01.ibm.com/marketing/iwm/iwm/web/reg/pick.do?source=jcesdk

  - Also needed if Domino (Mail Integration) or Sametime Proxy use longer keys

- Remove Server Information (HTTP Header, Error pages)

  - ServerSignature Off

  - ServerTokens Prod (DEFAULT)

  - AddServerHeader Off

Not Found

The requested URL /index2.html was not found on this server.

Not Found   Default

The requested URL /index2.html was not found on this server.

IBM_HTTP_Server at connections-   .com Port 443

Make Every **Moment** Count

Remove index.html

- Remove all Files except index.html from <IHS_ROOT>/htdocs

- Rename index.html (e.g. 0815.html)

  - echo 1 > 0815.html

  - For testing you can access the file

- Add robots.txt to exclude from Search engines

User-agent: *
Disallow: /
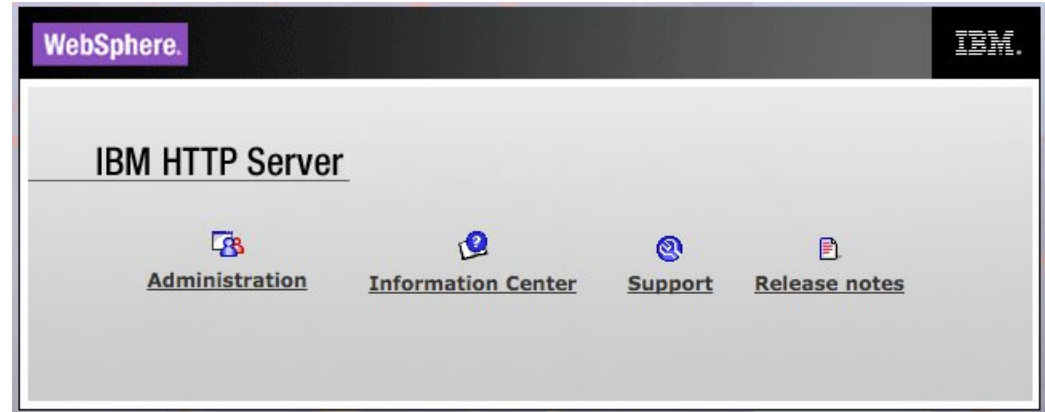
Tuning

Connect 2016

The Premier Social Business and Digital Experience Conference

#ibmconnect

Make Every **Moment** Count

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

LDAP
domino1.example.local

Authentication   UserSynchronisation

Web Server   WebSphere   Db2 /TDI
ihs.example.local   was1.example.local   db2.example.local
                                                        Freigabe

Make Every **Moment** Count

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
- counting 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

- Enable compression
    - Important
    - See Slides from [BP307 - IBM Connect 2014](#)
    - Save up to 70% network traffic
    - Minimal increase of CPU load
- Enable file download through IHS
    - Depend 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

Make Every **Moment** Count

Midsize Deployment - Files

- Often IHS positioned in the red zone (DMZ)

- Mostly No Access to SHARED DIRECTORY

  - Create a Cluster for Files

  - No Problem with Large Deployments

  - With Midsize you can add an additional Cluster during Setup
    (Looks different on Connections 5.5!)

		You can administer the following resources:				
☐	Cluster1_server1	cnxNode01	cnx-was.panastoeps.local	ND 8.5.5.3	Cluster1	➡
☐	Cluster2_server1	cnxNode01	cnx-was.panastoeps.local	ND 8.5.5.3	Cluster2	➡
☐	FilesCluster_server1	cnxNode01	cnx-was.panastoeps.local	ND 8.5.5.3	FilesCluster	➡
☐	InfraCluster_server1	cnxNode01	cnx-was.panastoeps.local	ND 8.5.5.3	InfraCluster	➡
Total 4						

- http://www-01.ibm.com/support/docview.wss?uid=swg21317658

Connect 2016

The Premier Social Business and Digital Experience Conference

Activate Synchronous File transfer

- Servers -> Application Servers -> serverName -> Web Container Settings -> Web Container -> Custom Properties

  - com.ibm.ws.webcontainer.channelwritetype=sync

Enhance User experience

Happy admins with happy users

Connect 2016

The Premier Social Business and Digital Experience Conference

Make Every **Moment** Count

#ibmconnect

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) as a reverse proxy to access iNotes

Connect 2016

Single Sign On - SPNEGO

- Requirements

  - Windows 2003 / 2008 / 2012 Active Directory

- Configure use documentation and http://de.slideshare.net/david_hay/dave-hay-deskto signon-in-an-active-directory-world?related=1

- Real additional 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

- Use IBM HTTP Server as reverse proxy to access iNotes

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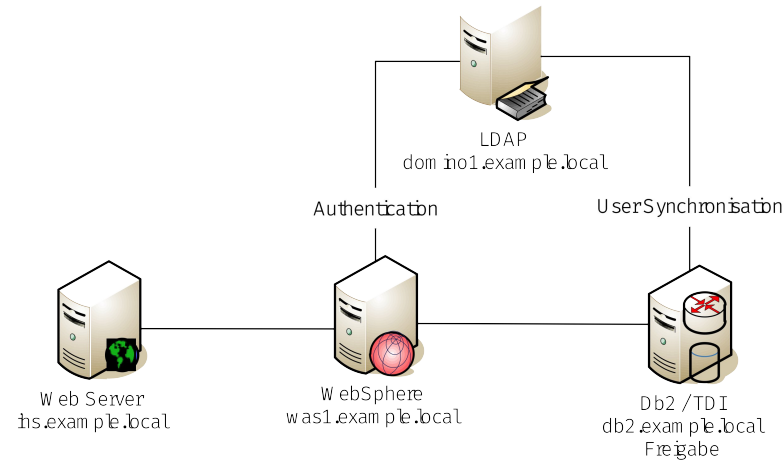LoadModule rewrite_module modules/mod_rewrite.so
<IfModule mod_ibm_ssl.c>
      Listen 0.0.0.0:1443
      <VirtualHost *:1443>
                  ServerName connections.example.com
                  SSLEnable
                  RewriteEngine on
                  ProxyRequests Off
                  ProxyPass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

Connect 2016

The Premier Social Business and Digital Experience Conference

iNotes Web Mail Redirect

Socialmail-config.xml

- When you use reverse proxy to access iNotes
  - Mail integration works only when you use http or https
  - Add UseConfiguredProtocol to your configuration
- 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>
```

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)

- Or:

  - http://tdiblog.anderIs.com/2015/02/adding-user-active-directory.html

  - Thanks Andreas Artner (He attends SocCNX, so bring him a beer)

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

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
- Use a LDAP user for connectionsAdmin
- Be prepared for scaling
    - Shared directory on UNC path
    - No small deployment installations
- Tune your environment

Don'ts

- Use multiple instances 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 IE
- Test with only one language

Connect2016

Installation Checklist

- WebSphere Application Server
    - Configure Federated Repository
    - LtpaToken, enable security
- WebSphere Application Server Supplements (IHS, Plugins)
- DB2 (or other DBM)
- TDI
- Add Webserver to Dmgr (use configurewebserver.bat)
- Enable SSL on IHS
- Import IHS Root Key within WebSphere cell trust keystore (retrieve from port)
- Configure CCM

Documentation of your environments

- Create valid documentation and keep it up-to-date

- 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_installation.dita

- Use a Microsoft Excel version of this at (Kudos to Keith Brooks)

  - http://blog.vanessabrooks.com/p/downloads.html

- Asciidoc is a possible way to automate your documentation

Tools

- Browser
  - Firefox (portable) / Firefox ESR
  - Chrome
  - IE (download vm with different versions)
    - https://www.modern.ie
- Network analyzer
  - Wireshark
  - tcpdump
- Unzip / Unarchiver
  - 7-zip

- Editor with syntax highlighting
  - vim, geany
  - notepad++
- Tail
  - baretail
  - multitail
  - mtail
- Proxy
  - Fiddler (often asked from Support)
  - Burpsuite (intercept proxy)

Connect 2016

The Premier Social Business and Digital Experience Conference

Links

- [IBM Connections Requirements](#)

- [Official Documentation Connections family](#)

- [Connections 5 Documentation](#)

- [Tuning Guide 4.0](#)

- [Tuning Guide Addendum 4.5](#)

- [Tuning Guide 5.0CR1](#)

Blogs with IBM Connections stuff

http://www.stoeps.de

http://scripting101.org

http://meisenzahl.org/

http://martin.leyrer.priv.at/

http://kbild.ch

http://dilf.me.uk/socialshazza

http://www.notesgoddess.net

http://notesbusters.com

http://ibmconnections.com

http://turtleblog.info

http://portal2portal.blogspot.de

https://www.urspringer.de

http://socialconnections.info

http://blog.robertfarstad.com

http://www.curiousmitch.com

http://www.ramsit.com/category/blog/

Connect 2016
The Premier Social Business and Digital Experience Conference

Acknowledgements and Disclaimers

Availability. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided AS-IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. Nothing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

Make Every **Moment** Count

Connect2016

The Premier Social Business and Digital Experience Conference

Acknowledgements and Disclaimers cont.

Make Every **Moment** Count

Connect 2016

The Premier Social Business and Digital Experience Conference