IBM Connections
Sicherheit & Administration

Christoph Stöttner – Fritz & Mazciol GmbH

Tags

active ad bash blackberry collaboration connections db2 directory domino g+ ibm ibmcnx iseries jython linux lotus ltpa microsoft notes on python sametime scripting sign single social speaker sql sso tdi twitter

Christoph Stoettner

IBM Software Consultant

cstoettner@fum.de

+49 (0) 89 4567858 90

Send Email | Download vCard

Recent Updates | **Contact Information** | Background

Name:	**Christoph Stoettner**
Company:	Fritz & Macziol Software und Computervertrieb GmbH
Department:	IBM Collaboration Solutions
Working Address:	Hörvelsinger Weg 17, 89081 Ulm, DE
Office number:	+49 (0) 89 4567858 90
Alternate email:	cstoettner@fum.de
Blog link:	http://www.stoeps.de
More Infos:	http://about.me/stoeps

Agenda

- **Einleitung**
- IBM HTTP Server
- WebSphere Application Server
- IBM Connections
- TDI
- DB2
- Troubleshooting

Einleitung

- “From Zero to Social Hero” - Frank Altenburg
- Projektgruppe definieren
- NICHT ausschließlich aus IT starten
- Erhöhung der Sicherheit und Performance
- PoC Installationen
  - Skalierbar planen
  - Mid-Size Deployment
  - DB und Shared Verzeichnis ins SAN

Agenda

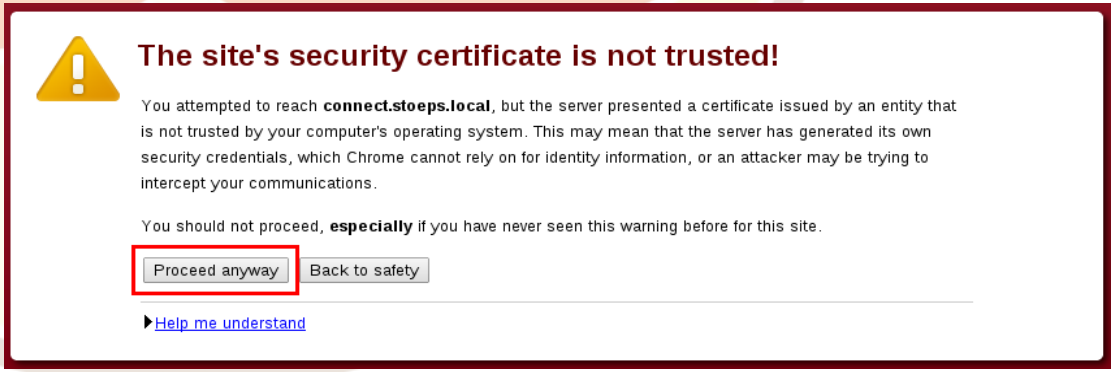
- Einleitung
- **IBM HTTP Server**
- WebSphere Application Server
- IBM Connections
- TDI
- DB2
- Troubleshooting

HTTP Server - Gefahren

- SSL Attacken durch
  - Men in the middle
  - Schwache Verschlüsselung
- Zugriff auf
  - Verzeichnisse
  - Index
  - Header
  - Interne Information

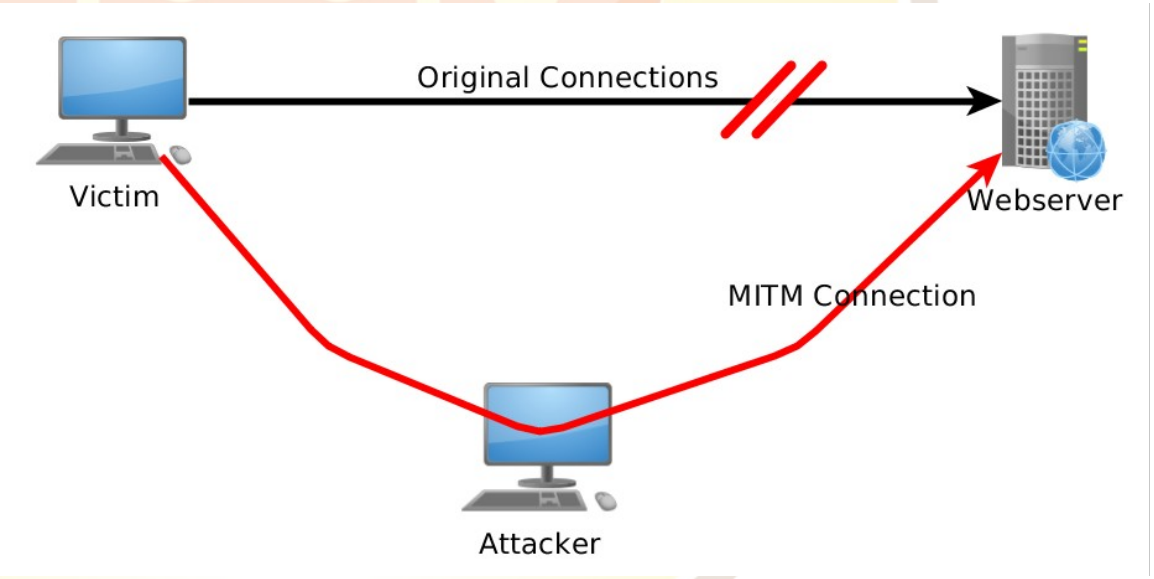
HTTP Server - SSL

- Selfsigned Keys
  - Nur mit automatischer Verteilung der ROOT CA KEYS!
  - Benutzer akzeptieren sonst alle Browser Warnungen
- Gekaufte SSL Keys
  - Im Browser automatisch anerkannt
  - Erfolgreiche Angriffe auf SSL Zertifikatssystem (DigiNotar)
    - Falsche Hostkeys
      - Google Mail
      - Yahoo
    - Falsche Herausgeberzertifikate (von Browsern akzeptiert)
      - 26: *.google.com
      - 22: *.skype.com
      - 14: *.torproject.org



SSL – Men in the Middle

- SSL Endpoint
  - Schiebt Browser falsches Zertifikat unter
  - User oder Browser müssen diesem vertrauen
- Schlüssellänge
  - Hostkey
    - 1024 – 4096 Bit
  - Sessionkey?
- SSL Protokoll
  - SSL v2
  - SSL v3
  - TLS v1.x



Session Verschlüsselung

Website cipher security against publicly known feasible attacks

Protocol version	Security[12][13]									
	3DES CBC	AES CBC	AES CCM	AES GCM	Camellia CBC	Camellia GCM	DES CBC	IDEA CBC	RC2 CBC	RC4
SSL 2.0	Insecure	N/A	N/A	N/A	N/A	N/A	Insecure	Insecure	Insecure	Insecure
SSL 3.0 [note 1]	Insecure [note 2][note 3][note 4]	N/A	N/A	N/A	N/A	N/A	Insecure	Insecure [note 2][note 3][note 4]	Insecure	Insecure [note 5][note 3][note 1]
TLS 1.0	Insecure [note 2][note 3][note 4]	Insecure [note 2][note 3][note 4]	N/A	N/A	N/A	N/A	Insecure	Insecure [note 2][note 3][note 4]	Insecure	Insecure [note 5][note 3][note 6]
TLS 1.1	Secure [note 3][note 4][note 6]	Secure [note 3][note 4][note 6]	N/A	N/A	N/A	N/A	Insecure	Secure [note 3][note 4][note 6]	Insecure	Insecure [note 5][note 3][note 6]
TLS 1.2	Secure [note 3][note 4][note 6]	Secure [note 3][note 4][note 6]	Secure [note 3][note 6]	Secure [note 3][note 7][13][note 6]	Secure [note 3][note 4][note 6]	Secure [note 3][note 6]	N/A	N/A	N/A	Insecure [note 5][note 3][note 6]

- SSL v2 deaktivieren
- Nur bestimmte Verschlüsselungsstandards zulassen
- Nicht nötig mit IHS > 8
  - SSLv2 deaktiviert
  - Cipher > 128 Bit
- SSLFIPSENABLE
  - ausschließlich TLS

```
Supported Server Cipher(s):
  Accepted  TLSv1  256 bits  AES256-SHA
  Accepted  TLSv1  168 bits  DES-CBC3-SHA
  Accepted  TLSv1  128 bits  AES128-SHA

Prefered Server Cipher(s):
  TLSv1  128 bits  AES128-SHA
```

Httpd.conf - SSL

```
<VirtualHost *:443>
   ServerName connect.stoeps.local
   RewriteEngine On
   RewriteRule A\/$ https://connect.stoeps.local/homepage [noescape,L,R]
   SSLEnable
   SSLProtocolDisable SSLv2
   SSLCipherSpec 3A
   SSLCipherSpec 34
   SSLCipherSpec 35
   SSLCipherSpec 2F
   SSLCipherSpec 35b

   #Only the specified MIME types will be compressed.
   SetOutputFilter DEFLATE
   AddOutputFilterByType DEFLATE application/*
   AddOutputFilterByType DEFLATE text/*

   # Ensures that images and executable binaries are not compressed
   SetEnvIfNoCase Request_URI \\.(?:gif|jpe?g|png|exe)$ no-gzip dont-vary

   # Ensure that proxies do not deliver the wrong content
   Header append Vary User-Agent env=!dont-vary
</VirtualHost>
```

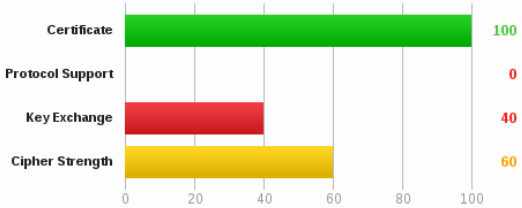
Test der Session Verschlüsselung (IHS 7)

- Default

Summary

Overall Rating

F



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	Yes
SSL 2 **INSECURE**	Yes

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

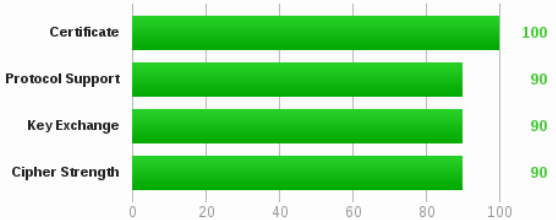
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_RC4_128_SHA (0x5)	128
TLS_RSA_WITH_RC4_128_MD5 (0x4)	128
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA (0x62) **WEAK**	56
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA (0x64) **WEAK**	56
TLS_RSA_EXPORT_WITH_RC4_40_MD5 (0x3) **WEAK**	40
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5 (0x6) **WEAK**	40
TLS_RSA_WITH_DES_CBC_SHA (0x9) **WEAK**	56
SSL_CK_DES_192_EDE3_CBC_WITH_MD5 (0x700c0) **INSECURE**	168

- Optimiert

Summary

Overall Rating

A



Protocols

TLS 1.2	Yes
TLS 1.1	Yes
TLS 1.0	Yes
SSL 3	Yes
SSL 2	No

Cipher Suites (SSL 3+ suites in server-preferred order, then SSL 2 suites where used)

TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	168
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)	128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)	256

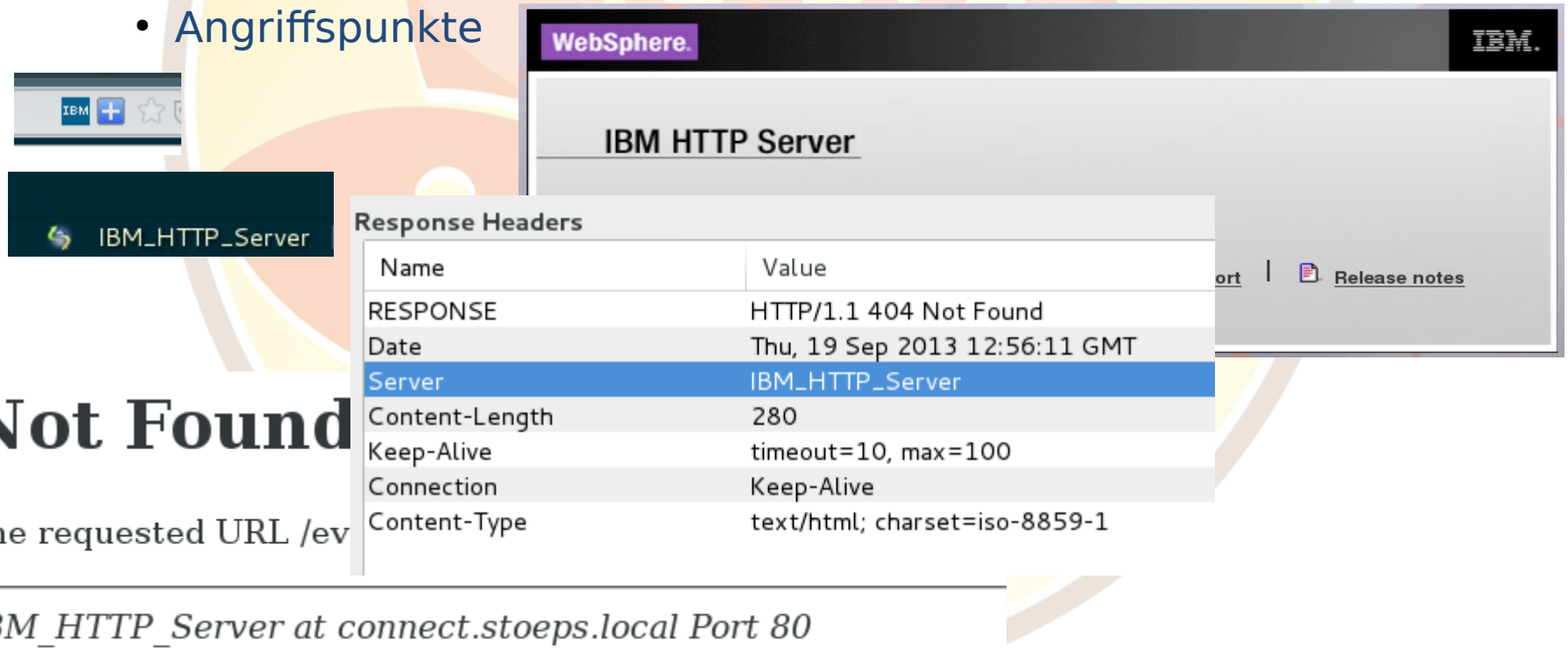
Test der Session Verschlüsselung (2)

- sslscan

```
root@kali-tester1:~# sslscan --no-failed connect.stoeps.local
                    _
           ___ ___| |___  ___ __ _ _ __
          / __/ __| / __|/ __/ _` | '_ \
          \__ \__ \ \__ \ (_| (_| | | | |
          |___/___/_|___/\___\__,_|_| |_|

                  Version 1.8.2
             http://www.titania.co.uk
        Copyright Ian Ventura-Whiting 2009

Testing SSL server connect.stoeps.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

  Prefered Server Cipher(s):
    SSLv3  168 bits  DES-CBC3-SHA
    TLSv1  168 bits  DES-CBC3-SHA
```

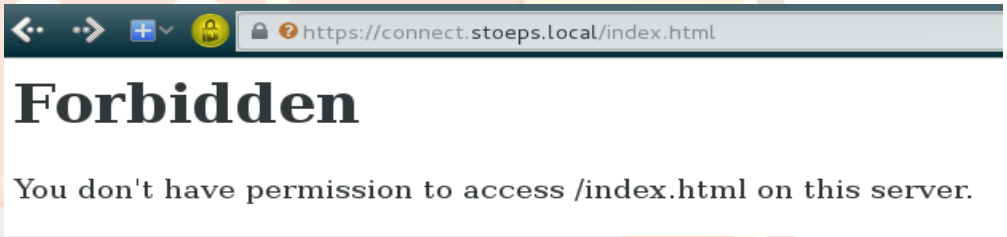
Zugriff auf HTTP Server einschränken

- Default Konfiguration läßt Directory Browsing zu
- Seiten in htdocs für Connections nicht benötigt
- Angreifer erhält
  - Zusätzliche Informationen
  - Angriffspunkte



Zugriff auf HTTP Server einschränken (2)

- Weitere Aliase und Directories definiert
- Zugriff verbieten oder auskommentieren
- Debug, MPM und Server-Status ausschalten
  - Wenn nicht benötigt
  - Oder benutzt
- Module ausschalten



Response Headers

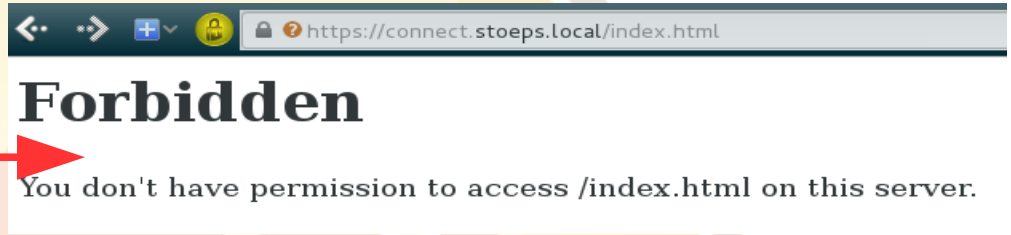
Name	Value
RESPONSE	HTTP/1.1 403 Forbidden
Date	Thu, 19 Sep 2013 13:01:20 GMT
Content-Length	212
Keep-Alive	timeout=5
Connection	Keep-Alive
Content-Type	text/html; charset=iso-8859-1

Forbidden

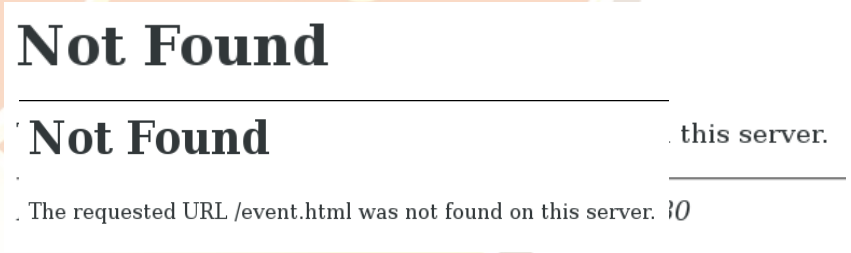
You don't have permission to access /event.html on this server.

Httpd.conf - Zugriffe

```
<Directory />
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
    FileETag All -INode
</Directory>


<Directory "/opt/IBM/HTTPServer/htdocs">
    Options None
    AllowOverride None
    Order deny,allow
    Deny from all
</Directory>
```




```
ServerSignature Off
```



Httpd.conf - Zugriffe

```
AddServerHeader Off
```

Response Headers

Name	Value
RESPONSE	HTTP/1.1 404 Not Found
Date	Thu, 19 Sep 2013 12:56:11 GMT
Server	IBM_HTTP_Server
Content-Length	280
Keep-Alive	timeout=10, max=100
Connection	Keep-Alive
Content-Type	text/html; charset=iso-8859-1

Response Headers

Name	Value
RESPONSE	HTTP/1.1 403 Forbidden
Date	Thu, 19 Sep 2013 13:01:20 GMT
Content-Length	212
Keep-Alive	timeout=5
Connection	Keep-Alive
Content-Type	text/html; charset=iso-8859-1

Unnötige Module

- Auskommentieren
- Mpmstats, whatkilledus, backtrace nur für Fehlersuche
- mod_proxy, mod_headers nur bei Bedarf

```
# LoadModule mpmstats_module modules/debug/mod_mpmstats.so
# <IfModule mod_mpmstats.c>
#       ReportInterval 600
#       TrackModules On
# </IfModule>

# Only activate for debug
# EnableExceptionHook On
# LoadModule whatkilledus_module
modules/debug/mod_whatkilledus.so
# LoadModule backtrace_module modules/debug/mod_backtrace.so
```

Performance

- Nur wenig Tuning notwendig
- Komprimierung aktivieren
  - http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+documentation#action=openDocument&res_title=Determining_which_files_to_compress_ic45&content=pdcontent
- Filezugriff auf Webserver auslagern
  - http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.5+documentation#action=openDocument&res_title=Configuring_file_downloads_through_the_HTTP_Server_ic45&content=pdcontent
  - Security bedenken!
    - IHS steht in DMZ
    - Zugriff auf Fileshare oder Freigabe notwendig
    - Zusätzlicher Port ins interne Netz benötigt
    - Share in DMZ -> Performance / Firewall ...

Bei vielen Benutzern

- Beobachten mit mod_status

	Default	Linux	Windows
KeepAliveTimeOut	10	5	5
ThreadLimit	25	25	2048
ThreadsPerChild		25	700
MaxRequestsPerChild	0	0	0
MaxKeepAliveRequests	100	0	0
StartServers	1	2	N/A
ServerLimit		80	N/A
MinSpareThreads		25	N/A
MaxSpareThreads		2000	N/A
MaxClients		2000	N/A

Agenda

- Einleitung
- IBM HTTP Server
- **WebSphere Application Server**
- IBM Connections
- TDI
- DB2
- Troubleshooting

WebSphere Security

- Stabile & sichere Plattform
  - Exploit DB
  - 1 Eintrag

DATE	Title	Summary
2005-02-24	allinurl:wps/portal/ login	**Pages containing login portals** Login to IBM WebSphere Portal.You may find portals using standard administrator user/password which gave you complete access to the application itself...

- ISC und Default Apps
  - Deaktivieren (Apps)
  - ISC nur intern erreichbar
- Zugriffe von Connections über WebSphere Plugin

Federated Repository

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Cell=cnxwas1Cell01, Profile=Dmgr01

Global security

Global security

Use this panel to configure administration and the default application security policy. This s
administrative functions and is used as a default security policy for user applications. Secu
the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Realm name
defaultWIMFileBasedRealm

Current realm definition
Federated repositories

Available realm definitions

Federated repositories | Configure... | Set as current

Federated Repository (2)

- 1 – nicht ändern
  - CCM
- 2 – Failover

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 consist of identities in the file-based repository that is built into 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

1

* Primary administrative user name
wasadmin

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

2

Repositories in the realm:

Add Base entry to Realm... | Use built-in repository | Remove

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
	o=defaultWIMFileBasedRealm	InternalFileRepository	File
	root	mail.stoeps.local	LDAP:DOMINO
Total 2			

Anmeldung über LDAPS

- Signer Zertifikat in ISC importieren
- Ablaufdatum beachten

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates

Manages signer certificates in key stores.

Preferences

Add | Delete | Extract | Retrieve from port

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
You can administer the following resources:				
	connect 2k	CN=connect.stoeps.local	6B:02:FA:E9:E6:A6:63:53:E3:6A:EC:AF:75:07:A7:7A:75:DE:91:68	Valid from Jul 29, 2013 to Jul 27, 2023.
	root	CN=cnxwas1.stoeps.local, OU=Root Certificate, OU=cnxwas1Cell01, OU=cnxwas1CellManager01, O=IBM, C=US	A3:22:32:E4:AC:7F:FA:3D:A5:92:46:25:75:09:DC:52:A5:8D:90:62	Valid from Jun 16, 2013 to Jun 12, 2028.
	selfsigned webserver1	CN=cnxwas1.stoeps.local, O=cnxwas1.stoeps.local	1B:B7:DB:37:69:1F:66:ED:AE:13:1E:31:80:B4:FD:84:C4:12:64:C8	Valid from Jun 17, 2013 to Jun 17, 2014.
	stoeps local	CN=mail.stoeps.local, O=Stoeps Inc., L=Rosenheim, ST=Bavaria, C=DE	33:0A:77:21:64:03:A5:E7:35:5C:6A:41:91:E9:6F:D5:9B:AB:33:10	Valid from Jun 12, 2013 to Jun 13, 2033.
	webserver	CN=connect.stoeps.local, C=DE	29:76:95:06:91:AD:E8:EA:4A:2A:68:14:6F:EF:B1:2A:2B:AF:EE:8F	Valid from Jul 26, 2013 to Jul 24, 2023.
Total 5				

Anmeldung über LDAPS (2)

Global security

Global security > Federated repositories > mail.stoeps.local

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

* Repository identifier
mail.stoeps.local

Repository adapter class name
com.ibm.ws.wim.adapter.ldap.LdapAdapter

LDAP server

* Directory type
IBM Lotus Domino

1

* Primary host name
mail.stoeps.local

Port
636

Failover server used when primary is not available:

Delete

Select	Failover Host Name	Port
None		

Add

3

Support referrals to other LDAP servers
ignore

Support for repository change tracking
none

Security

Bind distinguished name
CN=Bind LDAP,ou=users,o=stoeps

Bind password
•••••••

Login properties
uid;cn;mail

LDAP attribute for Kerberos principal name
krbPrincipalName

Certificate mapping
EXACT_DN

Certificate filter

Require SSL communications

2

Centrally managed

Domino LDAP für CNX Anmeldung

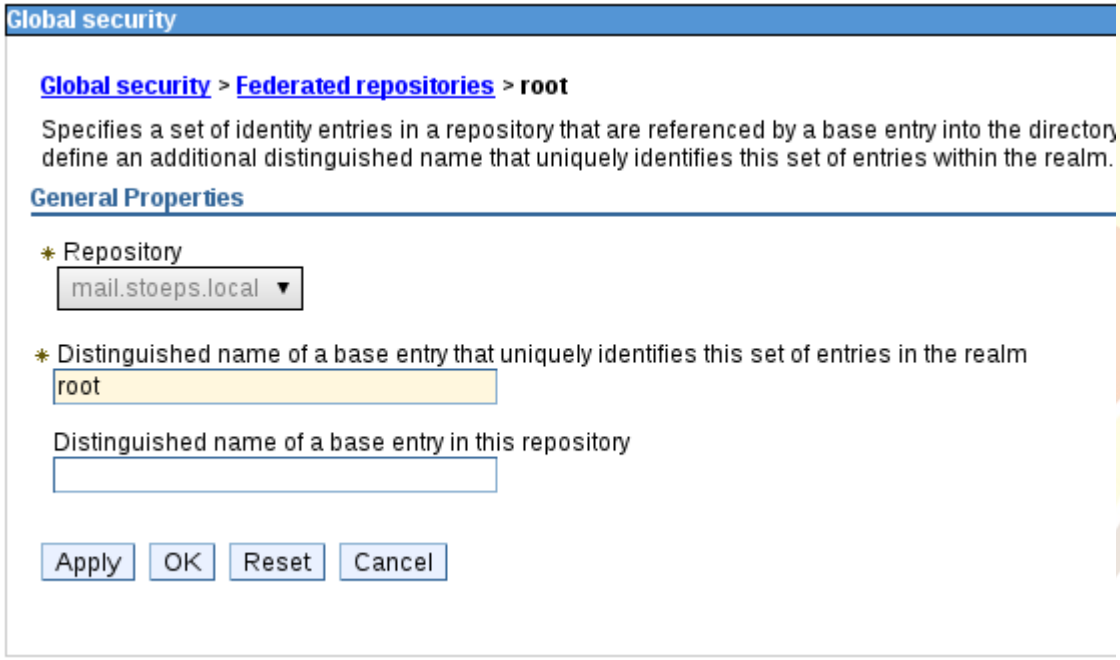
- Kein Bruteforce Schutz!
- Firewall oder Intrusion Prevention
- Passwort Hash > 8.0 problematisch
  - 50-100 Authentifizierungen / min
- Passwort Hash > 4.6
  - ca. 10.000 Authentifizierungen /min

Laufzeit ca. 50 min für 4000 Versuche

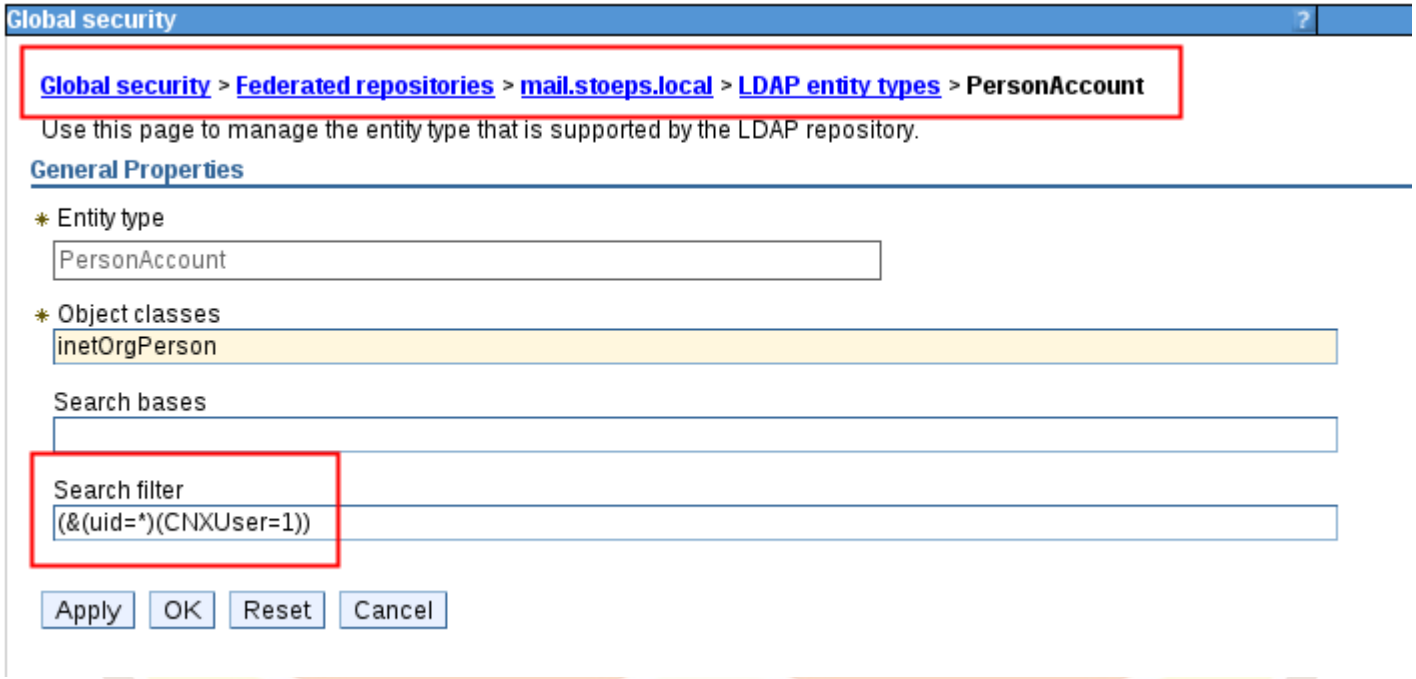
```
root@bt:~# hydra -l cs
Hydra v7.3 (c)2012 by

Hydra (http://www.thc.
[WARNING] Restorefile (./hydra.restore) from a previous session found, to prevent overwritin
g, you have 10 seconds to abort...
[DATA] 16 tasks, 1 server, 10001 login tries (l:1/p:10001), ~625 tries per task
[DATA] attacking service ldap3 on port 636
[STATUS] 89.00 tries/min, 89 tries in 00:01h, 9912 todo in 01:52h, 16 active
[STATUS] 85.00 tries/min, 255 tries in 00:03h, 9746 todo in 01:55h, 16 active
[STATUS] 84.00 tries/min, 588 tries in 00:07h, 9413 todo in 01:53h, 16 active
[STATUS] 80.53 tries/min, 1208 tries in 00:15h, 8793 todo in 01:50h, 16 active
[STATUS] 77.10 tries/min, 2390 tries in 00:31h, 7611 todo in 01:39h, 16 active
[STATUS] 76.40 tries/min, 3591 tries in 00:47h, 6410 todo in 01:24h, 16 active
[636][ldap] host: 192.168.110.15   login: cstoettner   password: lotusnotes
[STATUS] attack finished for domino.stoeps.local (waiting for children to finish)
1 of 1 target successfuly completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2013-02-15 18:28:34
```

Domino Gruppen benutzen

- ab WebSphere 7.0.0.22 direkt in ISC konfigurierbar
- Base Entry des LDAP Repositories
  - root



Anmeldung einschränken



Single Sign On

- LtpaToken / LtpaToken2
  - IBM / Lotus
  - Sametime / Domino
  - Voraussetzung:
    - Gleiche DNS Domäne (Vorplanung)
    - WebSphere Multi-Domain
    - Domino Support nur für eine Domain
- SPNEGO
  - Active Directory
  - Kerberos
  - Browser übergibt Windows Anmeldung

Single Sign On mit Domino / Sametime Proxy

- LtpaToken im WebSphere erstellen
- Import im Domino Web SSO Dokument
- Sametime Proxy verwendet den LtpaToken des Community Servers (Domino)
- Timeout in allen System gleich setzen!
- Immer beide Richtungen testen!

Single Sign On - Domino / Sametime Proxy (2)

WebSphere. software

Welcome AConnections Help | Logo

Cell=cnxwas1Cell01, Profile=Dmgr01

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Security
  - Global security (1)
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

Authentication

Authentication mechanisms and expiration

- (•) LTPA (3)
- ( ) Kerberos and LTPA

Kerberos configuration

Authentication cache settings

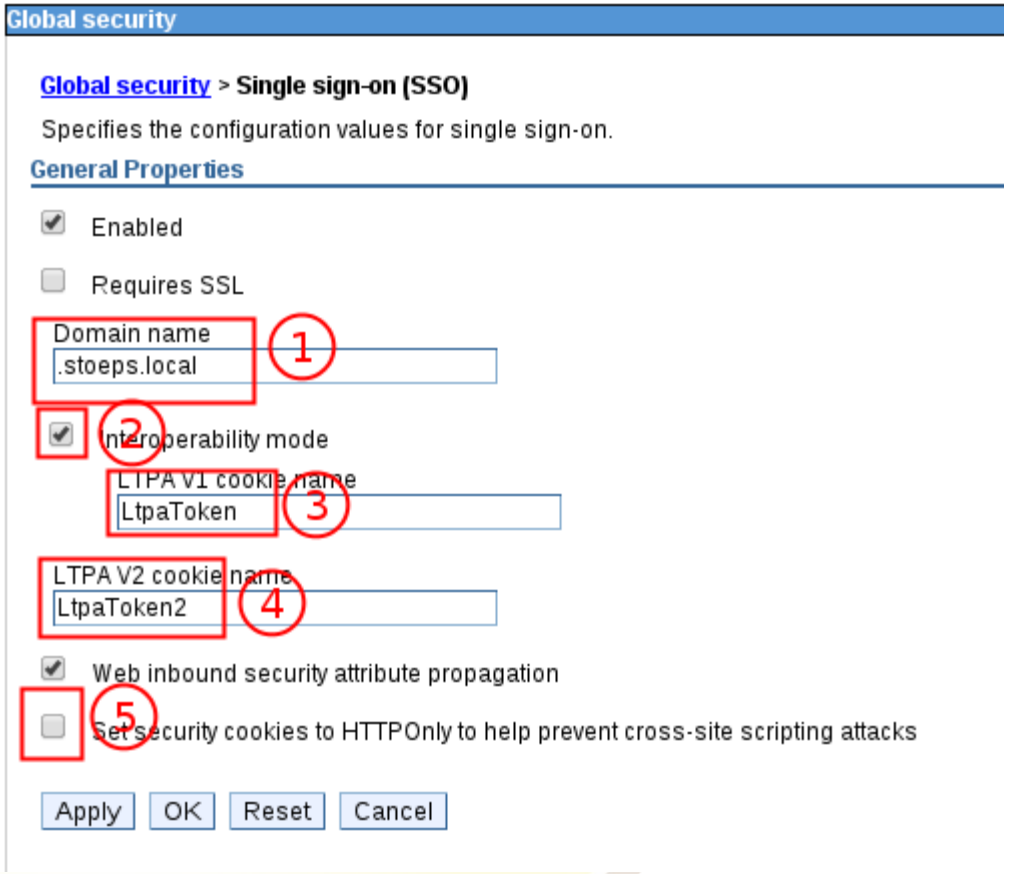
Web and SIP security

- General settings
- (2) Single sign-on (SSO)
- SPNEGO web authentication
- Trust association
- SIP digest authentication

RMI/IIOP security

Single Sign On - Domino / Sametime Proxy (3)

- Interop Mode für
  - Domino < 7



Single Sign On - Domino / Sametime Proxy (4)

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Security
  - Global security (1)
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Cell=cnxwas1Cell01, Profile=Dmgr01

Global security

Global security > LTPA

Encrypts authentication information so that the application server can send the data from one server to another in a secure manner. The encryption of authentication information that is exchanged between servers involves the LTPA mechanism.

Key generation

Authentication data is encrypted and decrypted by using keys that are kept in one or more key stores.

Key set group: CellLTPAKeySetGroup — Generate keys

- Key set groups

LTPA timeout

LTPA timeout value for forwarded credentials between servers: 240 minutes (2)

Cross-cell single sign-on

Single sign-on across cells can be provided by sharing keys and passwords. To share the keys and password, log on to one cell, specify a key file, and click Export keys. Then, log on to the other cell, specify the key file, and click Import keys.

* Password

* Confirm password

Fully qualified key file name (3)

Import keys — Export keys (4)

Single Sign On - Domino / Sametime Proxy (5)

Web SSO Configuration for : LtpaToken

Basics | Comments | Administration

Token Configuration

Configuration Name:	LtpaToken
Organization:	
DNS Domain:	.stoeps.local
Map names in LTPA tokens:	Disabled
Require SSL protected communication (HTTPS):	Disabled
Restrict use of the SSO token to HTTP/HTTPS:	Disabled

Token Expiration

Expiration (minutes):	240

Participating Servers

Domino Server Names:	domino1/srv/stoeps, sametime/srv/stoeps
Windows single sign-on integration (if available):	Disabled

WebSphere Information

Token Format:	LtpaToken and LtpaToken2 (compatible with all releases of Domino)
LDAP Realm:	defaultWIMFileBasedRealm
LTPA Version:	1.0

SPNEGO

- Voraussetzung
  - Connections Admin muss ein LDAP Benutzer sein
- Federated Repository
  - Active Directory
  - IBM Domino LDAP mit Name mapping
- Mailintegration / Sametime
  - AD Name in Notes Fullname oder Kerberos Namensfeld
- SPN für den Service Benutzer:
  - HTTP/wasserver.domain.tld@ADDOMAIN.TLD
  - HTTP/connections.domain.tld@ADDOMAIN.TLD
- Keytab-Files generieren
- Krb.conf mit wsadmin erstellen

SPNEGO (2)

WebSphere. software

Welcome AConnections Help | Log

Cell=cnxwas1Cell01, Profile=Dmgr01

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

Global security

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard | Security Configuration Report

Administrative security

☑ Enable administrative security

- Administrative user roles
- Administrative group roles
- Administrative authentication

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Realm name

defaultWIMFileBasedRealm

Current realm definition

Federated repositories

Authentication

Authentication mechanisms and expiration

- ◉ LTPA
- ○ Kerberos and LTPA
- Kerberos configuration

Authentication cache settings

Web and SIP security

- General settings
- Single sign-on (SSO)
- SPNEGO web authentication
- Trust association
- SIP digest authentication

RMI/IIOP security

Java Authentication and Authorization Service

☐ Enable Java Authentication SPI (JASPI)

Providers

☐ Use realm-qualified user names

SPNEGO (2)

Global security

Global security > **SPNEGO web authentication**

SPNEGO provides a way for web clients and the server to negotiate the web authentication protocol used to permit communications.

General Properties

- [ ] Use the alias host name for the application server
- [x] Dynamically update SPNEGO
- [x] Enable SPNEGO
  - [x] Allow fall back to application authentication mechanism

* Kerberos configuration file with full path

E:\IBM\WebSphere\AppServer\java\jre\lib\security\krb5.conf [Browse...]

Kerberos keytab file name with full path

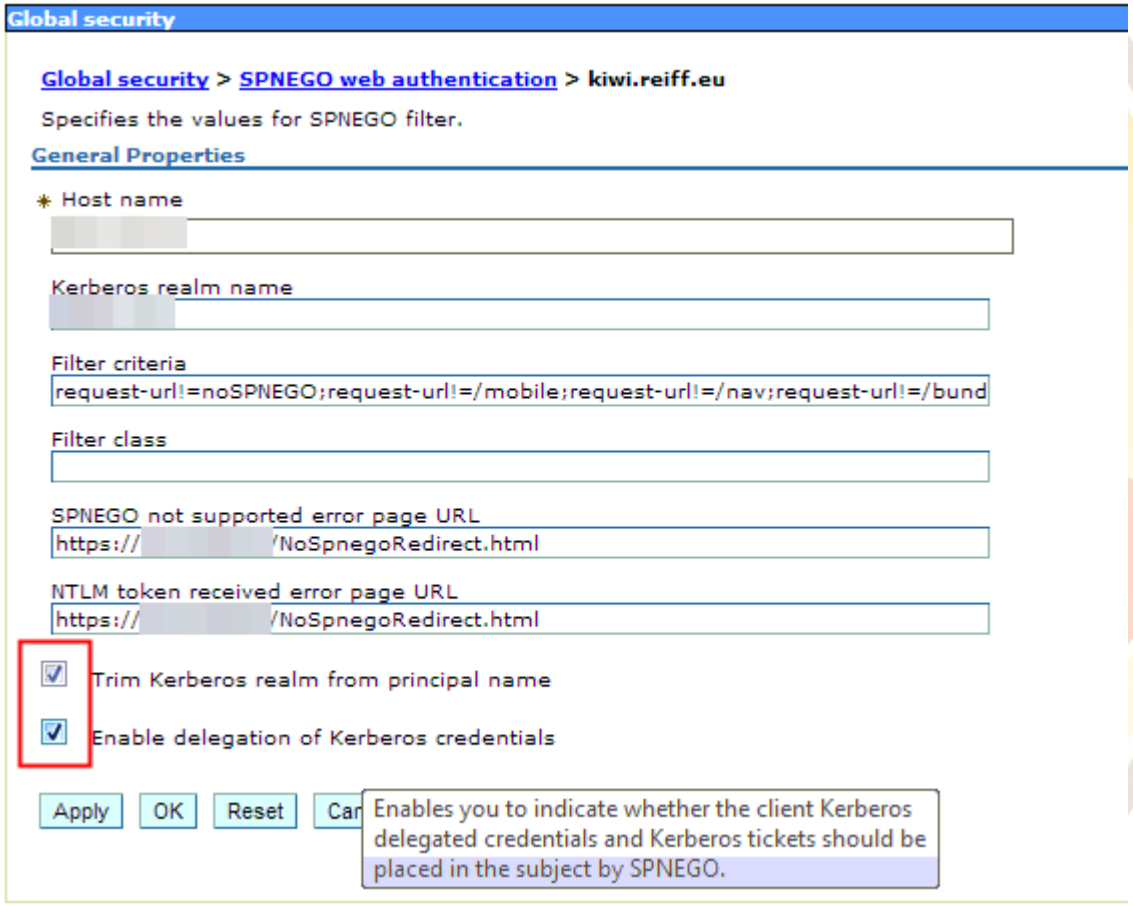
E:\IBM\WebSphere\SSO\ merged.keytab [Browse...]

SPNEGO Filters:

New... Delete

Select	Host Name	Kerberos Realm Name	Filter Criteria
You can administer the following resources:			
[ ]		.LOC	request-url!=noSPNEGO;request-url!=/mobile;request-url!=/nav;request-url!=/bundles/js;request-url!=/static;request-url!=/activities/oauth;request-url!=/blogs/oauth;request-url!=/dogear/oauth;request-url!=/communities/calendar/oauth;request-

SPNEGO (3)


Global security
Global security > SPNEGO web authentication > kiwi.reiff.eu
Specifies the values for SPNEGO filter.
General Properties
* Host name
Kerberos realm name
Filter criteria
request-url!=noSPNEGO;request-url!=/mobile;request-url!=/nav;request-url!=/bund
Filter class
SPNEGO not supported error page URL
https://
/NoSpnegoRedirect.html
NTLM token received error page URL
https://
/NoSpnegoRedirect.html
Trim Kerberos realm from principal name
Enable delegation of Kerberos credentials
Apply
OK
Reset
Car
Enables you to indicate whether the client Kerberos delegated credentials and Kerberos tickets should be placed in the subject by SPNEGO.

SPNEGO - Browser

- Konfiguration im Connections Wiki beschrieben
- Anmeldung immer mit dem lokalen Windows User
  - Workaround
    http://www-10.lotus.com/ldd/lcforum.nsf/55c38d716d632d9b8525689b005ba1c0/4041dfc93b83686185257bcc00315685?OpenDocument
- Browser die Kerberos nicht unterstützen öffen eine Redirect Seite -> Login Maske

Security Rollen / J2EE Rollen

- Absicherung der Connections Applikationen
- 21 Applikationen
  - Bis zu 12 Rollen (insgesamt 142)
  - 30 unterschiedliche Rollen
- Rollen mit gleichen Namen sollten gleich gesetzt sein

Überblick Rollen (1)

	Activities	Blogs	Common	Communities	connectionsProxy	Dogear	Files	FNCS	Forums	Homepage	Metrics	Mobile Admin	Mobile	Moderation	News	Profiles	Search	WebSphereOAuth20SP	WidgetContainer	Wikis
admin	x	x	x	x			x		x	x	x				x	x	x		x	x
administrator												x								
allAuthenticated			x		x										x	x			x	
Anonymous								x												
app-connector							x													
authenticated																		x		
Authenticated								x												
bss-provisioning-admin	x	x		x			x		x						x	x				x
client manager																		x		
community-creator				x																
community-metrics-run				x							x									
discussThis-user									x											
dsx-admin				x												x				
everyone	x	x	x	x	x	x	x		x	x	x	x	x		x	x	x		x	x

Überblick Rollen (2)

	Activities	Blogs	Common	Communities	connectionsProxy	Dogear	Files	FNCS	Forums	Homepage	Metrics	Mobile Admin	Mobile	Moderation	News	Profiles	Search	WebSphereOAuth20SP	WidgetContainer	Wikis
everyone-authenticated							x				x			x			x			x
files-owner							x													
global-moderator		x	x	x			x		x					x					x	
mail-user			x																x	
metrics-reader	x	x		x		x	x		x	x					x	x	x		x	x
metrics-report-run			x								x									
OAuthClient								x												
org-admin							x									x				
person	x	x	x	x	x	x	x		x	x	x		x	x	x	x	x		x	x
reader	x	x	x	x	x	x	x		x	x	x		x	x	x	x	x		x	x
search-admin	x	x		x		x	x		x						x	x	x			x
search-public-admin									x											
sharebox-reader															x					
trustedExternalApplication																			x	
widget-admin	x	x		x			x		x						x					x
wiki-creator																				x

Rollen Details

- admin
  - Administrative Rolle, je nach Modul mehr oder weniger Rechte
- community-creator
  - Berechtigung zum Anlegen neuer Communities
- communities-metric-run
  - Berechtigung zum Ansehen von Community Metriken
- discussThis-user
  - Forum Discuss This aus einem anderem Deployment
- dsx-admin
  - Account mit dem andere Applikationen in Profiles und Communities Benutzer- und Memberdaten auslesen

Rollen Details (2)

- everyone
  - Bereich der ohne Authentifizierung zu lesen sein soll (= Login Page)
- everyone-authenticated
  - Sollte zu AllAuthenticated in Application's Realm gemappt werden
- files-owner
  - Haben eine persönliche Library für den Upload von Dateien
- global-moderator
  - Berechtigung für die Content Moderation
- metrics-reader
  - Darf die Metriken der Applikation einsehen

Rollen Details (3)

- metrics-report-run
  - Zugriff auf globale Metriken (in Metrics Applikation)
- person
  - Darf in der Applikation lesen und schreiben
- reader
  - Darf in der Applikation grundsätzlich nur lesen
- search-admin
  - User greift zur Generierung der Suche auf den Content zu
- wiki-creator
  - Berechtigung zum Anlegen neuer Wikis außerhalb Communities
- widget-admin
  - User der berechtigt ist, von Communities aus in der Applikation administrative Befehle durchzuführen

Role Mapping

- Zu Rollen können hinzugefügt werden
  - User
  - Gruppen
- Special Subjects
  - None
  - AllAuthenticated in Application's Realm
  - AllAuthenticated in Trusted Realms
  - Everyone

Authentifizierung erzwingen

- reader Rolle
  - Default: everyone
- All Authenticated in Applications Realm
  - Anmeldung wird erzwungen
- everyone Rolle
  - muss auf everyone gemappt bleiben!
  - Anmeldemaske kann sonst nicht dargestellt werden

Rollen und Fixpacks

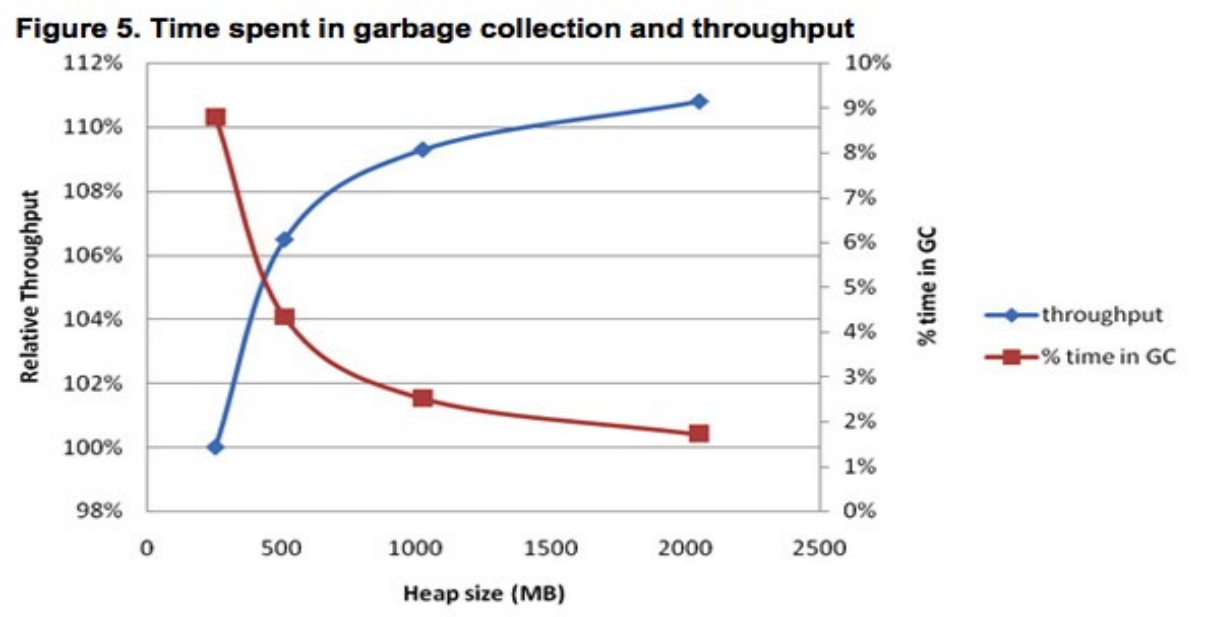
- Fixpack Installation setzt manchmal die Rollen auf Default
  - aufwändige Rekonstruktion
  - setzen dauert 30 – 45 min je nach Adminanzahl
- v.a. in Umgebungen mit erzwungener Authentifizierung gefährlich
  - Content öffentlich im Internet
  - Googlebot findet das in wenigen Minuten und beginnt zu indizieren
- Überprüfung
  - Google: “site:connectionshostname”
- Lösung:
  Track 1 Session 6 – Zeitsparen mit Skripting

Performance

- File Share für Connections shared directory
  - gleich als Share konfigurieren
  - weniger Aufwand bei 2. Node
  - NFS v4 oder CIFS/SMB
  - kein DFS (MS Distributed File System)
- Cognos auf eigene Maschine / Node auslagern
  - hoher I/O
  - hohe CPU
- Verzögerung beim Aufruf von Connections

WebSphere JVM Parameter

- JVM Heapsize
  - Richtige Größe zu finden oft aufwändig
  - Balance zwischen Garbage Collector und Speichergröße
- Verbose Garbage Collector aktivieren
  - Auswertung: Garbage Collection and Memory Visualizer



- http://www.ibm.com/developerworks/websphere/techjournal/0909_blythe/0909_blythe.html

Thread Pool / Connection Pool

- Analyse mit PMI
- WebContainer Thread Pools
  - initial 50
  - bis zu 100 notwendig
  - muss pro Application Server gesetzt werden
- JDBC Connection Pool
  - Einstieg: IBM Connections 4.0 Performance Tuning Guide
  - Weitere Analyse mit PMI
  - Default Werte sind z.B. bei Updates zu gering
    - http://www-10.lotus.com/ldd/lcforum.nsf/55c38d716d632d9b8525689b005ba1c0/676247a814058f1585257bc200456fc2?OpenDocument
    - Jdbc/search zu gering für Connections 4.5 CR1

PMI

WebSphere. software

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
  - Performance Monitoring Infrastructure (PMI)
  - Request metrics
  - Performance Viewer
- Troubleshooting
- Service integration
- UDDI

Cell=cnxwas1Cell01, Profile=Dmgr01

Performance Monitoring Infrastructure (PMI)

Performance Monitoring Infrastructure (PMI)

Use this page to configure Performance Monitoring Infrastructure (PMI)

Preferences

Maximum rows

20

Retain filter criteria

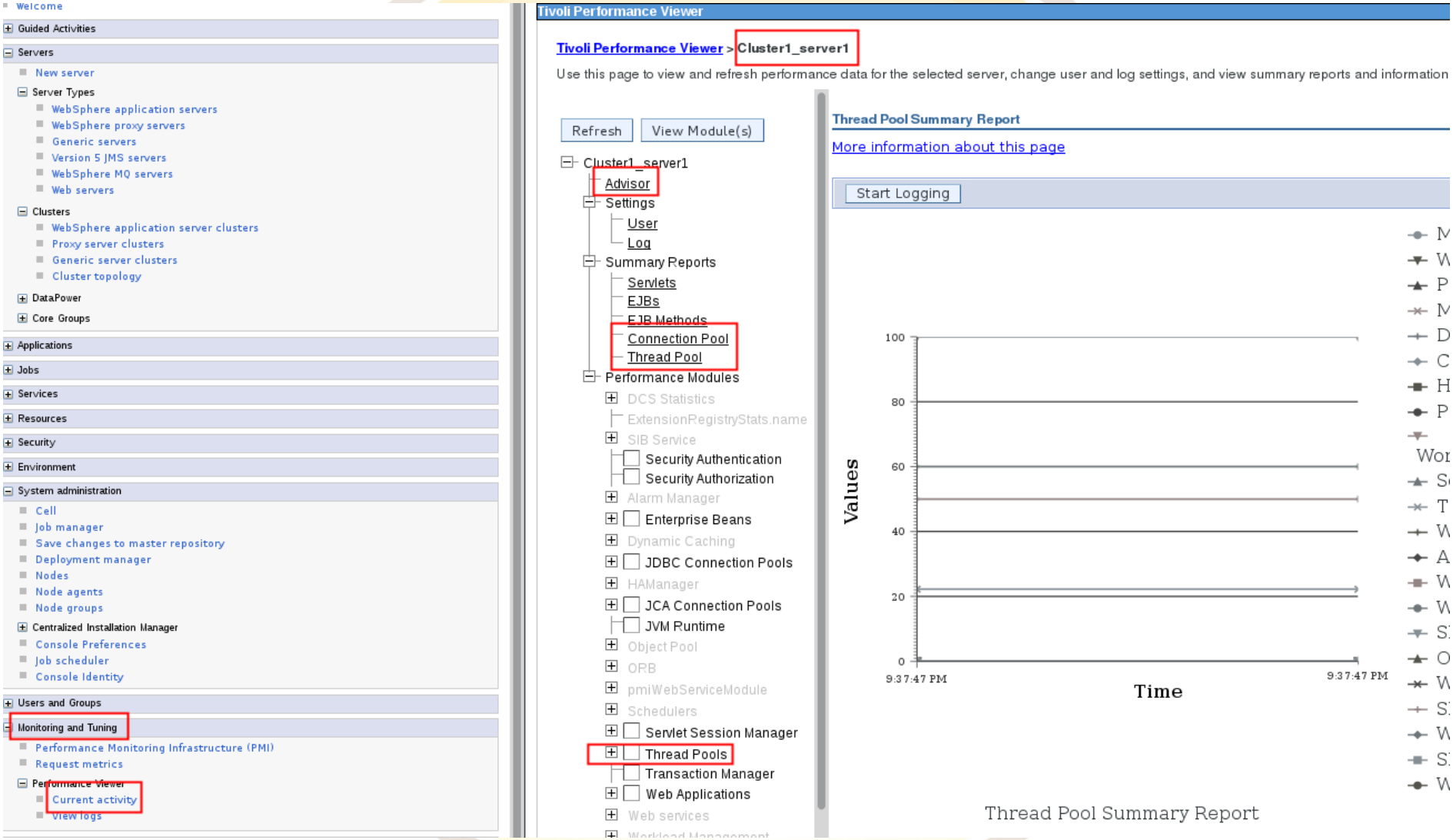
Show items at the following authorization group level:

All Roles

Apply Reset

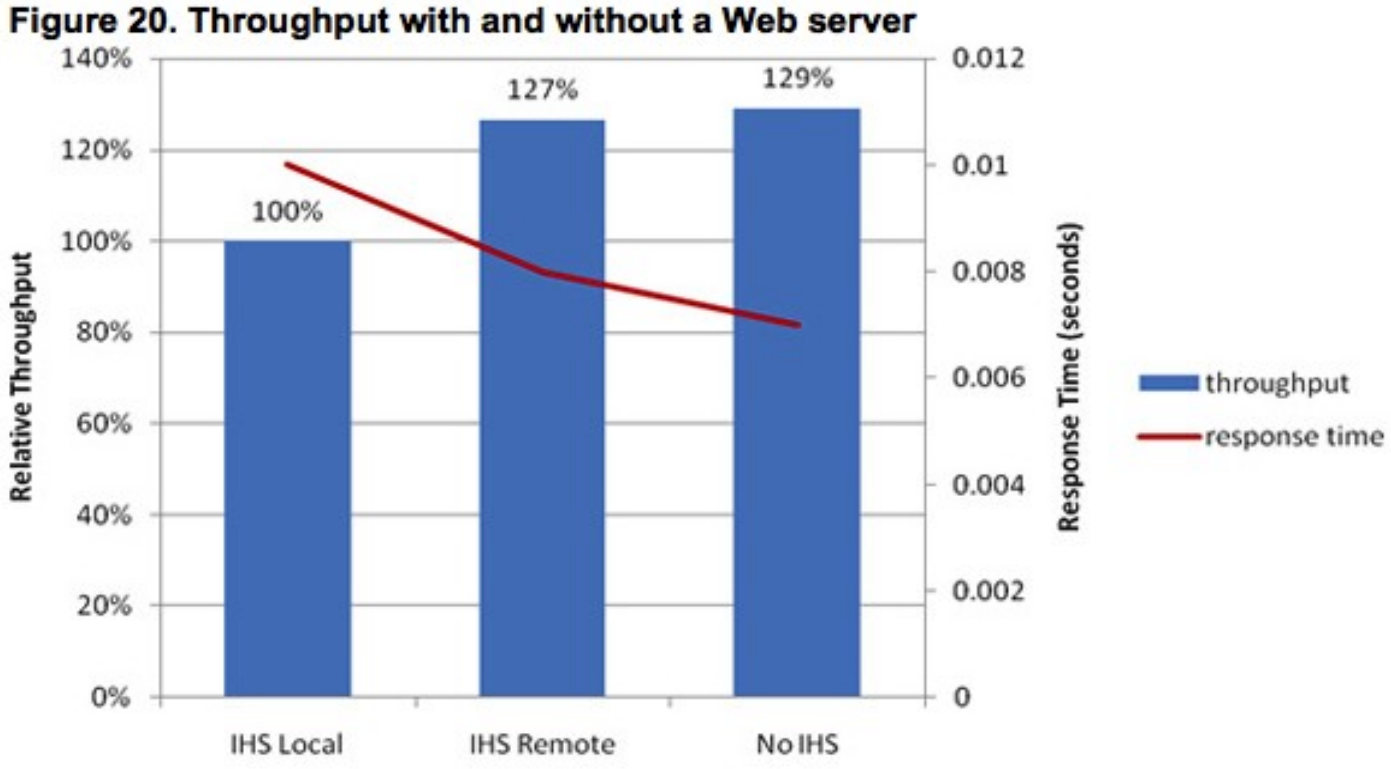
Select	Name	Node
You can administer the following resources:		
	Cluster1_server1	cnxwas1Node01
	Cluster2_server1	cnxwas1Node01
	ConvCL_server1	convNode01
	DocsCL_server1	DocsNode01

PMI


Welcome
Guided Activities
Servers
New server
Server Types
WebSphere application servers
WebSphere proxy servers
Generic servers
Version 5 JMS servers
WebSphere MQ servers
Web servers
Clusters
WebSphere application server clusters
Proxy server clusters
Generic server clusters
Cluster topology
DataPower
Core Groups
Applications
Jobs
Services
Resources
Security
Environment
System administration
Cell
Job manager
Save changes to master repository
Deployment manager
Nodes
Node agents
Node groups
Centralized Installation Manager
Console Preferences
Job scheduler
Console Identity
Users and Groups
Monitoring and Tuning
Performance Monitoring Infrastructure (PMI)
Request metrics
Performance Viewer
Current activity
View logs
Tivoli Performance Viewer
Tivoli Performance Viewer > Cluster1_server1
Use this page to view and refresh performance data for the selected server, change user and log settings, and view summary reports and information
Refresh
View Module(s)
Cluster1_server1
Advisor
Settings
User
Log
Summary Reports
Servlets
EJBs
EJB Methods
Connection Pool
Thread Pool
Performance Modules
DCS Statistics
ExtensionRegistryStats.name
SIB Service
Security Authentication
Security Authorization
Alarm Manager
Enterprise Beans
Dynamic Caching
JDBC Connection Pools
HAManager
JCA Connection Pools
JVM Runtime
Object Pool
ORB
pmiWebServiceModule
Schedulers
Servlet Session Manager
Thread Pools
Transaction Manager
Web Applications
Web services
Thread Pool Summary Report
More information about this page
Start Logging
Values
100
80
60
40
20
0
9:37:47 PM
9:37:47 PM
Time
Thread Pool Summary Report

Webserver auf eigener VM

- Extra Server hat erfahrungsgemäß gute Auswirkungen auf die Antwortzeit
- Beispiel aus WebSphere Tuning



Agenda

- Einleitung
- IBM HTTP Server
- WebSphere Application Server
- **IBM Connections**
- TDI
- DB2
- Troubleshooting

LDAP Benutzer vs. Lokaler wasadmin

- Tipp:
  - Installation von Connections **IMMER mit LDAP Benutzer**
- Voraussetzung für Integration von FileNet / CCM
- Nachträgliche Umstellung aufwändig / fehleranfällig
- User in J2EE Rollen eintragen
- Verschiedene Bugs in Connections traten nur mit lokalem Admin auf
  - Fehlende Thumbnails in Media Gallery

Admin Rolle

- Eigene Admin Accounts anlegen!

☐	admin	None	wasadmin aconnections	CNXAdmins

- Homepage
  - Aktivierung von Widgets
- Blogs
  - weitreichende Administration möglich
- Search
  - Übersicht der Suche
- Communities
  - Communities Catalog verwalten

Admin - Homepage

- Aktivierung von Widgets für “My Page”

Getting Started
I'm Following
Status Updates
My Notifications
Mentions
Action Required
Saved
Discover
My Page
Administration

Tips

New Administrator?

- Use the Administration page to enable and disable individual widgets, and edit their details.
- Enhance the functionality of the Home page by adding new widgets from your

Administrator's Home Page

Use this page to define the widgets that are available to Home page users.

My Page is currently Enabled ▾ Save

Refresh cache

Click a widget name to select it.

Enabled widgets

Enabled widgets appear on the Home page

Activities
Blogs
Bookmarks
Communities
Connections Embedded Experience
Connections Mail
Events
Files Share
Files Shared with Me
Latest Wikis
Microblogging Share
My Activities
My Bookmarks
My Communities
My Files

Disable Edit Remove

Disabled widgets

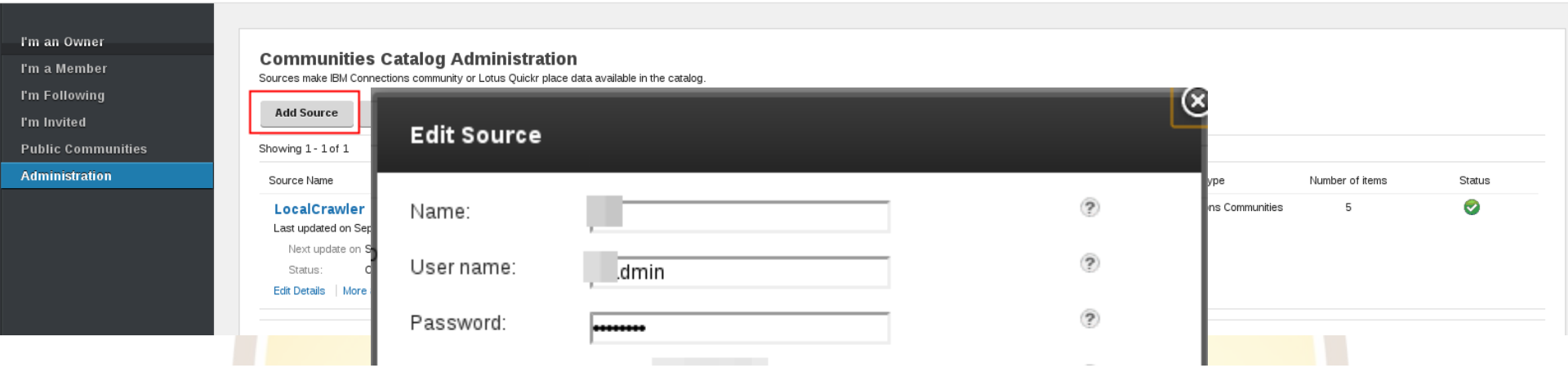
Disabled widgets do not appear on the Home page

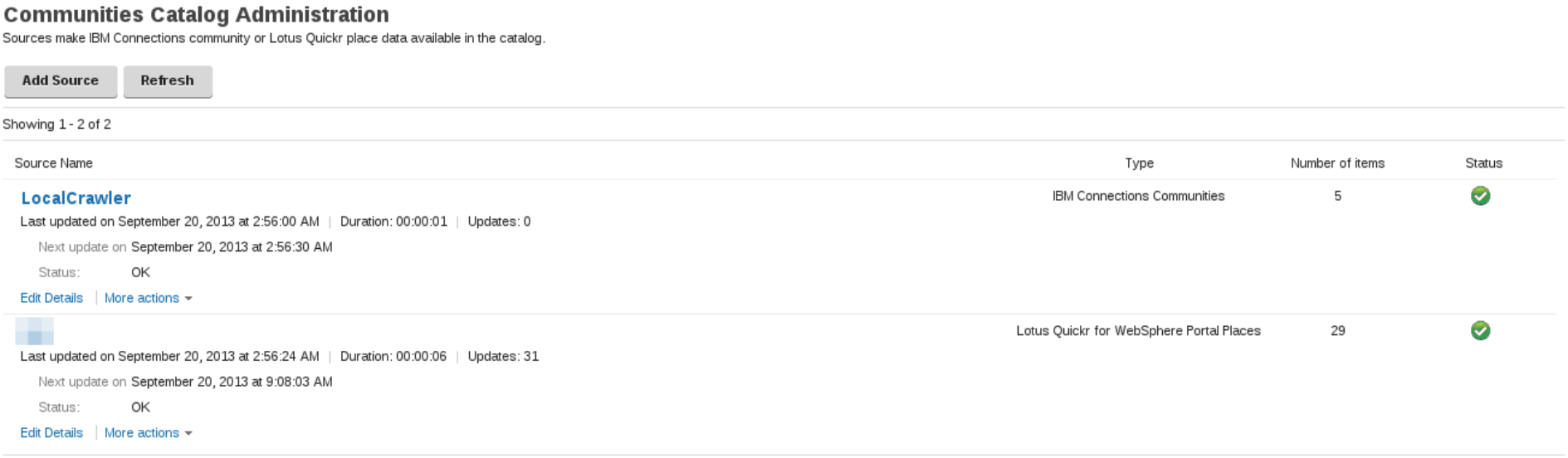
Enable Edit Remove

Communities Admin

- Communities Catalog verwalten
  - Crawler neustarten bei Anzeigeproblemen
  - More Actions – Collect Data
- Quickr oder andere Community Kataloge hinzufügen
  - Community Catalog Admin Rolle notwendig
  - URL (manuell setzen): https://{connectionsserver}/communities/seedlist/myserver?Source=Catalog
  - Standard-User -> not found
- Community Ansichten zeigen zusammengeführte Kataloge
- Keine Unterscheidung ausser Autorennamen!

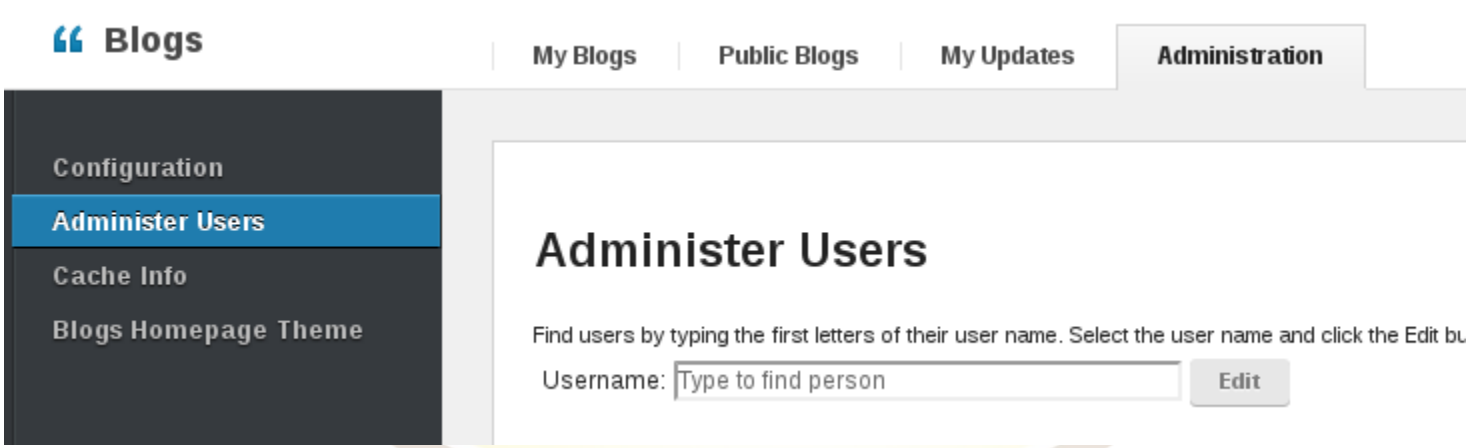
Communities Admin (2)





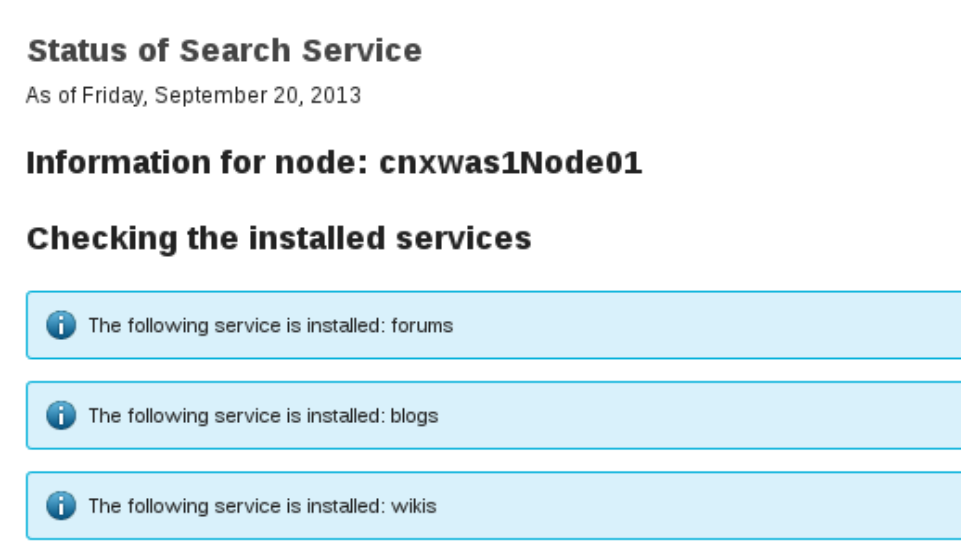
Blogs Admin

- Globale Einstellungen
  - File Upload
  - Maximale Dateigröße
  - Andere Module müssen das über wsadmin konfigurieren
- Veränderung von Einstellungen in User Blogs
  - Administer Users



Search Admin

- Aufruf des Search Status
  - https://{connectionsserver}/search/serverStatus
- Übersicht über installierte Module
- Seedlist Status
- WebSphere Variables
- Log Entries mit Bezug auf Suche



Active Content Filter

- Default (ausser Blogs, Wikis, Forums)
  - RTF Formatierung erlaubt, kein CSS
  - Javascript wird entfernt
  - Flash ist nicht erlaubt
- LotusConnections-config/extern
  - acf-config-{variable}.xml
  - {variable} 1-n
    - nf – No Forms, No Styles
    - ns – No Scripts
    - flash – No Flash
  - Beispiel acf-config-nf-ns-flash.xml
- Einbinden über LotusConnections-config.xml

```
<sloc:serviceReference acf_config_file="acf-config-nf.xml" bootstrapHost="" bootstrapPort="" clusterName="Cluster1" en
abled="true" person_card_service_name_js_eval="generalrs.label_personcard_activitieslink" person_card_service_url_pattern=
"/service/html/mainpage#dashboard%2Cmyactivities%2Cuserid%3D{userid}%2Cname%3D{displayName}" serviceName="activities" ssl_
enabled="true">
```

Agenda

- Einleitung
- IBM HTTP Server
- WebSphere Application Server
- IBM Connections
- **TDI**
- DB2
- Troubleshooting

Tivoli Directory Integrator

- Speichertuning
  - Linux: /opt/IBM/TDI/V7.1/ibmdisrv
    - "$TDI_JAVA_PROGRAM" **-Xms256M -Xmx1024M** $TDI_MIXEDMODE_FLAG **-Xnojit** -cp "$TDI_HOME_DIR/IDILoader.jar" "$LOG_4J" com.ibm.di.loader.ServerLauncher "$@" &
  - Windows: ibmdisrv.bat
    - "%TDI_JAVA_PROGRAM%" **-Xms256M -Xmx1024M -Xnojit** -classpath "%TDI_HOME_DIR%\IDILoader.jar" %ENV_VARIABLES% com.ibm.di.loader.ServerLauncher %*

TDI - Troubleshooting

- prüfen ob TDISOL/**sync_all_dns.lck** vorhanden
- TDISOL/logs/ibmdi.log
  - Log Datei zur Analyse von Importfehlern
- TDISOL/employee.error
  - Benutzernamen der Importfehler ($dn)
- map_dbrepos_from_source.properties
- profiles_functions.js
  - Erweiterbar um eigene Skripte
  - Fehlende Fullnames, Timezone

Agenda

- Einleitung
- IBM HTTP Server
- WebSphere Application Server
- IBM Connections
- TDI
- **DB2**
- Troubleshooting

DB2 Performance

- Planung
  - mehrere Instanzen
- I/O
  - Datenbanken auf eigene I/O Quelle auslagern
  - durch
    - ändern der DB Skripte (DB Wizard)
    - create database homepage on 'R:\'
    - globale Änderung
    - set dftdbpath
- Memory
  - unter 10.1 bisher unnötig
  - unter 9.7 STMP_HEAP_SZ

DB2 Performance

- Planung
  - mehrere Instanzen
- I/O
  - Datenbanken auf eigene I/O Quelle auslagern
  - durch
    - ändern der DB Skripte (DB Wizard)
    - create database homepage on 'R:\'
    - globale Änderung
    - set dftdbpath
- Memory
  - unter 10.1 bisher unnötig
  - unter 9.7 STMP_HEAP_SZ

DB2 – Datenbank Reorganisation

- Connections Wizards/connections.sql/<db>/db2/
  - reorg.sql
    - Empfehlung 1x wöchentlich
    - regelmäßige Ausführung über scheduled Tasks
    - reorganisation Tabellen und Indizes
    - merklicher Performancegewinn
  - clearScheduler.sql
    - Empfehlung vor Updates / Fixpack Installation
    - leert die Scheduler von WebSphere

DB2 Security

- Administrationsbenutzer nur für
  - Create DB
  - Backup
  - Restore
- LCUSER für die Verbindung von WAS zu DB2
  - Skripte setzen genau die benötigten Rechte (appGrants.sql)
- konsistent auch bei Systemmigration
  - default Windows Admin: db2admin
  - default Linux/AIX: db2inst1
- Keine speziellen OS Rechte notwendig

Agenda

- Einleitung
- IBM HTTP Server
- WebSphere Application Server
- IBM Connections
- TDI
- DB2
- **Troubleshooting**

Troubleshooting - Logs

- System Requirements!
  - ist das System supportet?
  - Tipp:
    - nicht von den Requirements abweichen!
    - WebSphere Fixes nicht vergessen
- Komponente identifizieren, Logdatei finden
  - IHS
    - /opt/IBM/HTTPServer/logs/error.log
    - c|d|e:\IBM\HTTPServer\logs\error.log
  - WebSphere Applikation
    - /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs
      - InfraCluster/SystemOut.log
      - Cluster1/SystemOut.log
      - Cluster2/SystemOut.log

Troubleshooting – Logs (2)

- WebSphere Plugins
  - /opt/IBM/WebSphere/Plugins/logs/<server/http_plugin.log
  - Zertifikatsprobleme (HTTP Cert im WAS nicht bekannt)
- Datenbank DB2
  - /home/dbinst1/sqllib/db2dump/db2diag.log
  - Lizenz eingespielt?
- TDI (Benutzersynchronisation)
  - TDISOL/logs/ibmdi.log
  - meist fehlende Felder und falsche Inhalte im LDAP

Fragen?

Danke für die Aufmerksamkeit!