

Reliable and secure CIRCABC



circa-support.eu



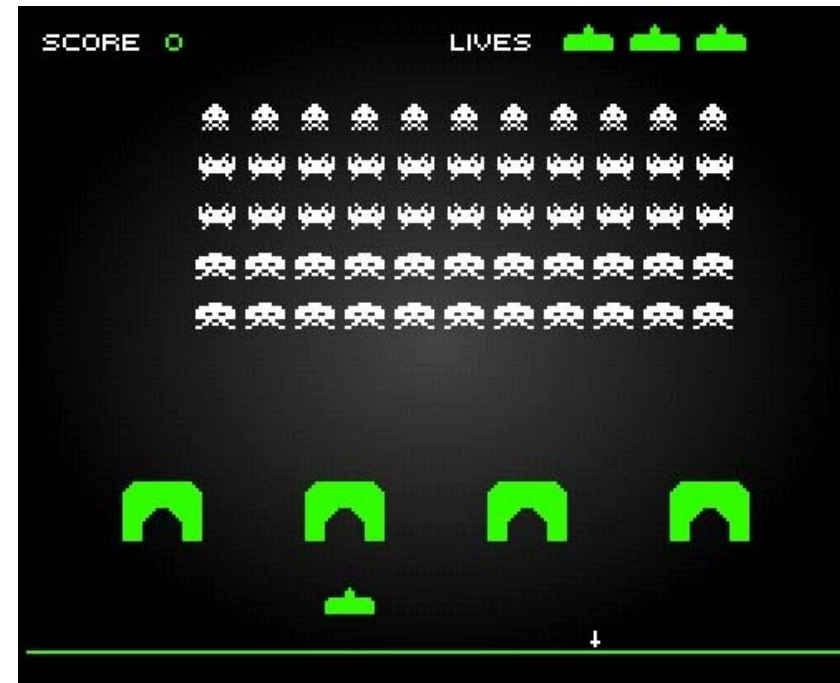
nidbs CIRCABC
Conference
23.04.2010
Jan Büren

Tactical Overview, Sir!



circa-support.eu

- ✓ CIRCABC architecture
- ✓ Network analysis
- ✓ Management pitfalls
- ✓ Recommendations
- ✓ Optional Stuff



Simplify it: components



circa-support.eu

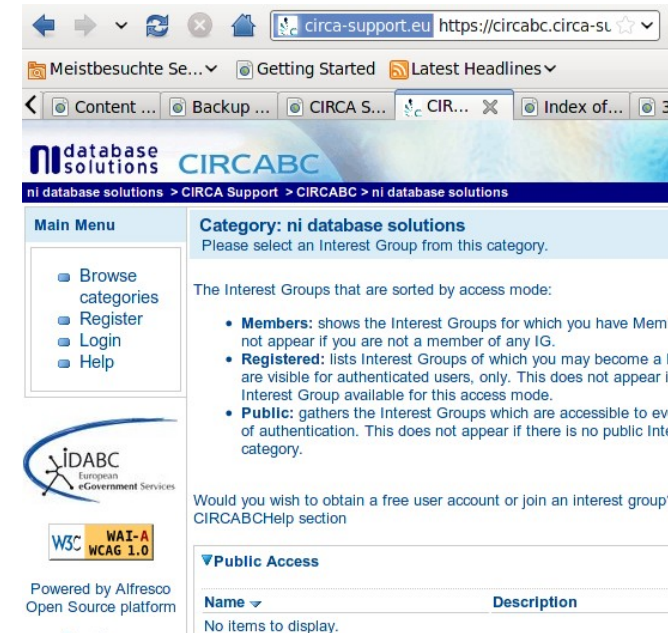
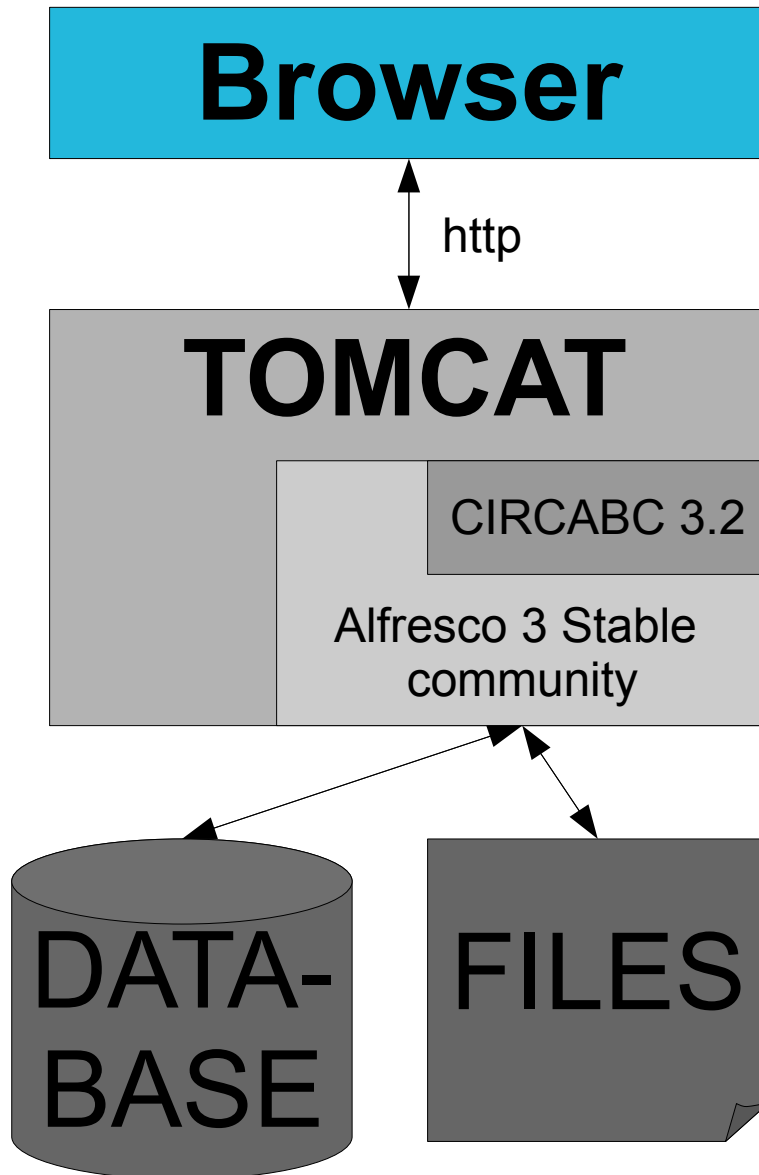
CIRCABC 3.2

Alfresco 3 Stable
community

Still simple: deliver pretty pages



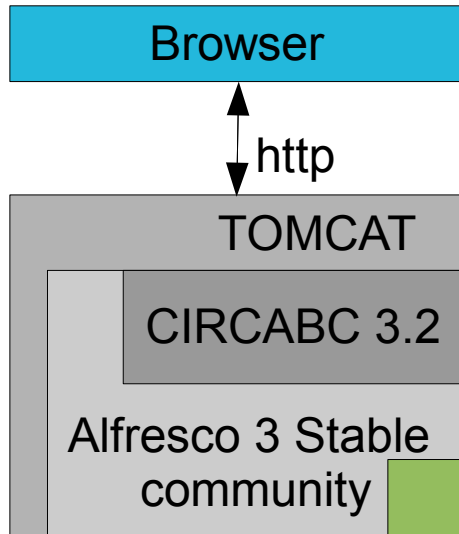
circa-support.eu



All Gaul is occupied by ~~romans~~ http

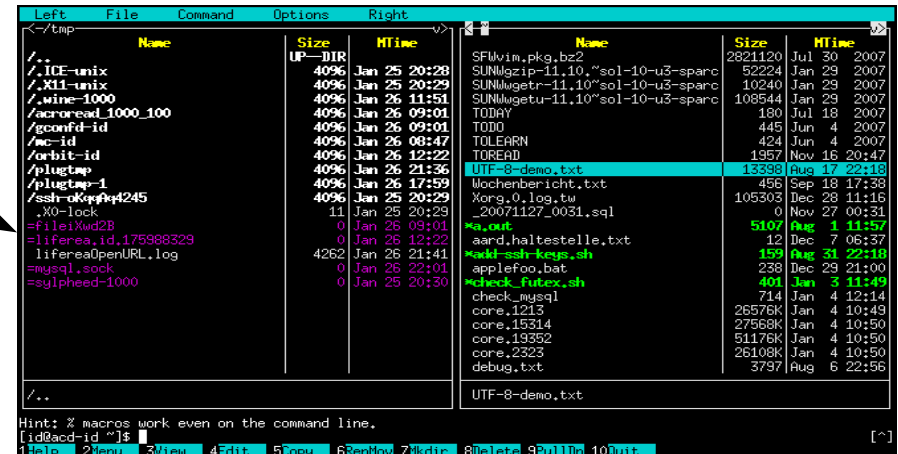
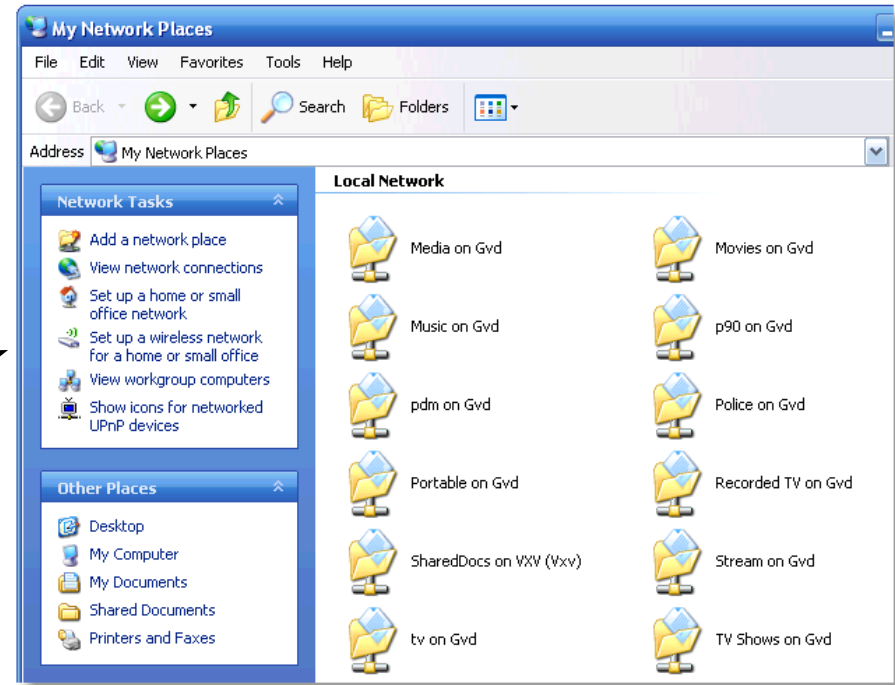


circa-support.eu



CIFS

FTP



external port scan



circa-support.eu

```
Interesting ports on 172.16.1.1:
```

```
Not shown: 994 closed ports
```

```
PORT      STATE SERVICE
21/tcp    open  ftp
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
8009/tcp  open  ajp13
8080/tcp  open  http-proxy
50500/tcp open  unknown
```

→ **FTP**

→ **CIFS**

→ **HTTP**

→ **RMI**

How hard do they knock?



circa-support.eu

CIFS-Interface:

10 seconds

11 unsuccessful logins

```
17 Jun 2009 11:04:35 1432750319 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, db2admin
17 Jun 2009 11:04:36 1432751611 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, db2admin
17 Jun 2009 11:04:37 1432752535 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, db2admin
17 Jun 2009 11:04:37 1432752880 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, db2admin
17 Jun 2009 11:04:38 1432753775 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, db2admin
17 Jun 2009 11:04:40 1432755984 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
17 Jun 2009 11:04:41 1432756888 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
17 Jun 2009 11:04:42 1432757820 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
17 Jun 2009 11:04:43 1432758805 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
17 Jun 2009 11:04:44 1432759650 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
17 Jun 2009 11:04:45 1432760853 WARN [org.alfresco.filesys.auth.cifs.EnterpriseCifsAuthenticator]:2172 User does not exist, administrator
```

They knock with dictionaries!



circa-support.eu

User does not exist, DiVX

User does not exist, serveur ftp

User does not exist, box1

User does not exist, Administrador'

User does not exist, Administrateur

User does not exist, Administrada

User does not exist, billgates

The knock with force!



circa-support.eu

```
grep "User does not exist" /opt/circabc/logs/tomcat/catalina.out | wc -l
```

350202 login attempts

Installation: 20.3.2009

First attack: 26.4.2009

Last attack: 01.2.2010

(RMI?) + (RTFM!) == JMX

JMX: Java Management Extensions

The screenshot shows the J2SE 5.0 Monitoring & Management Console. The title bar indicates the connection URL: `service:jmx:rmi:///jndi/rmi://localhost:50500/alfresco/jmxrmi`, which is circled in red. The console is displaying the MBeans tab for the connection. On the left, a tree view shows the hierarchy of MBeans, with `RepoServerMgmt` selected. The main area shows a table of MBeans with columns for Name and Value. The table lists `ReadOnly` (false), `SingleUserOnly`, `TicketCountAll`, and `TicketCountNonExpired`. Below the table, there are two line charts: one for `UserCountAll` and one for `UserCountNonExpired`. Both charts show a step function that rises from 0 to 1 at 10:57. A red arrow points from the circled URL to the text `jmx:rmi:localhost:50500` overlaid on the right side of the image.

Name	Value
ReadOnly	false
SingleUserOnly	
TicketCountAll	
TicketCountNonExpired	

jmx:rmi:localhost:50500

Speak friend and Enter

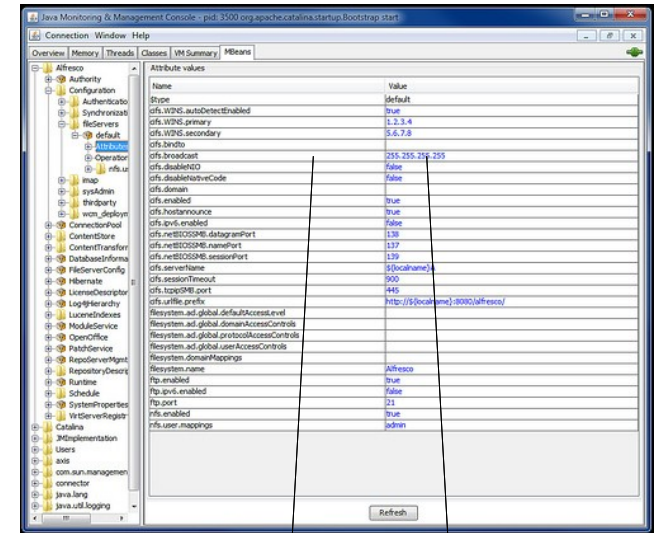


circa-support.eu



Alfresco 3.2 JMX monitoring

JMX tools can (...) stop, re-configure and restart subsystems without shutting down Alfresco.

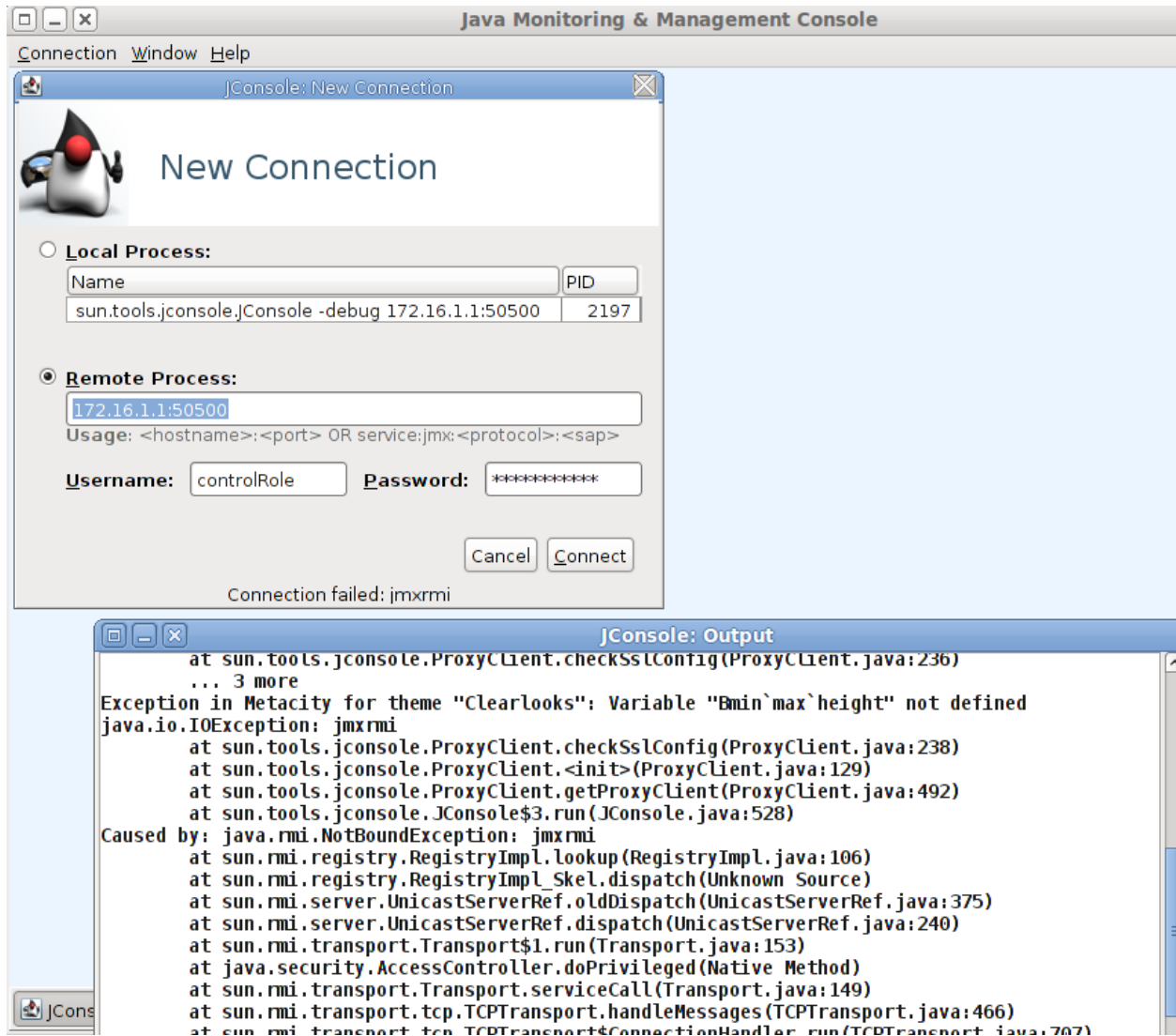


CIFS enabled **true**

Luckily, I couldn't make it ...



circa-support.eu



```
#!/# sed -i 's/change_asap/SECURE/g' webapps/ROOT/WEB-INF/classes/alfresco/alfresco-jmxrmi.password
```

<http://jared.ottleys.net/alfresco/tunneling-debug-and-jmx-for-alfresco>

More default (http) entry points



circa-support.eu



Apache Tomcat/5.5.28

- ✓ JBOSS Administration
- ✓ Tomcat Administration
- ✓ Hidden admin URLs



If you'

As you ma
filesystem

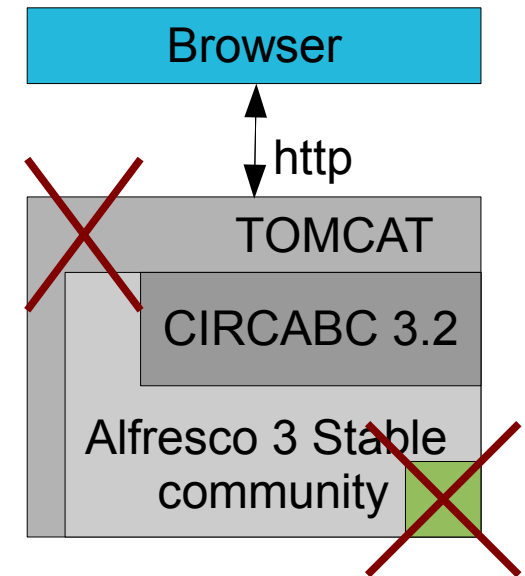
```
# aptitude purge tomcat5.5-admin tomcat5.5-webapps
```

Simple advice: just pretty pages



circa-support.eu

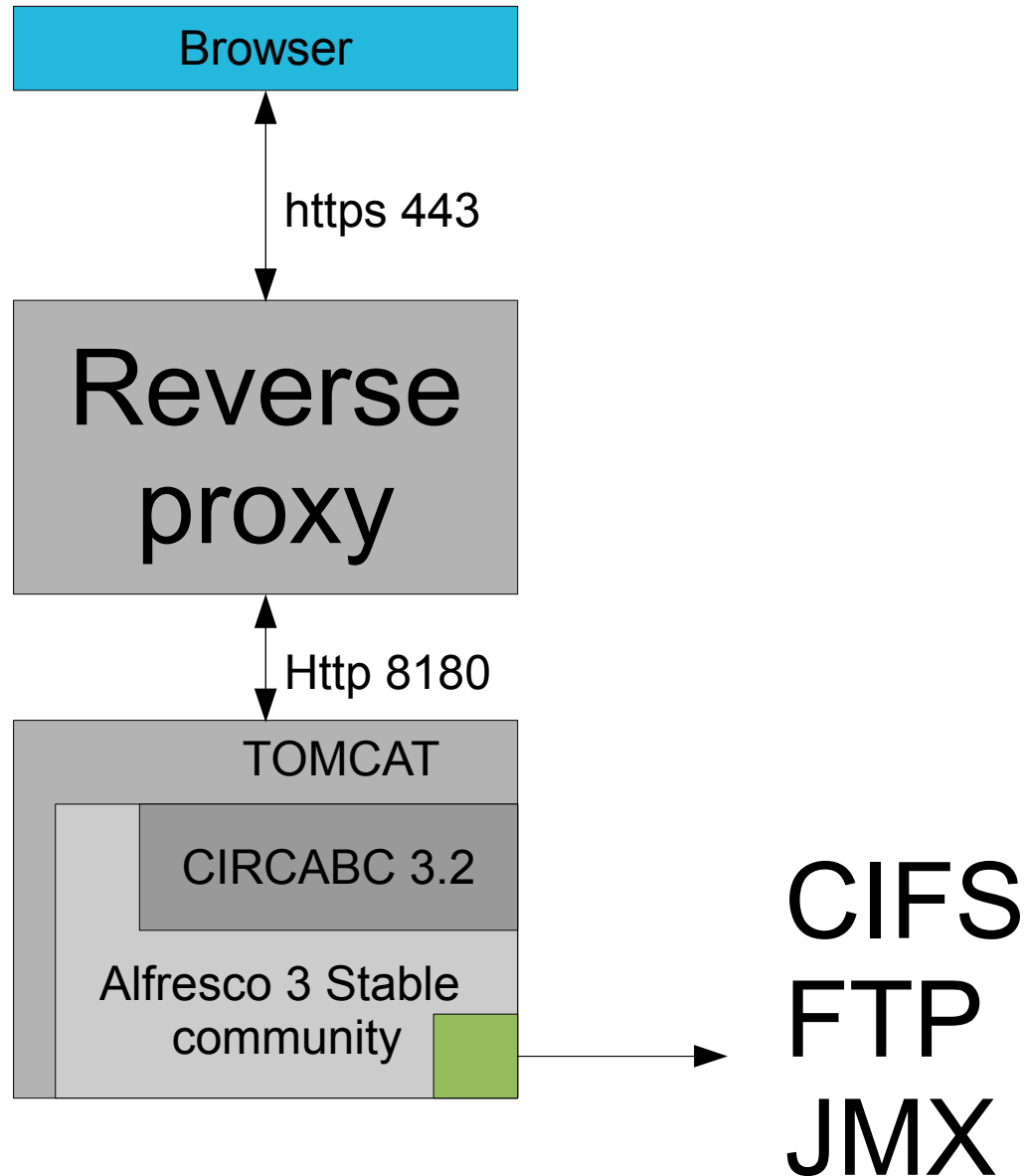
- **Disable CIFS / FTP**
- **Disable Tomcat Admin**
- **Bind services on localhost**
- **Change default passwords**



advanced advice: proxy it!



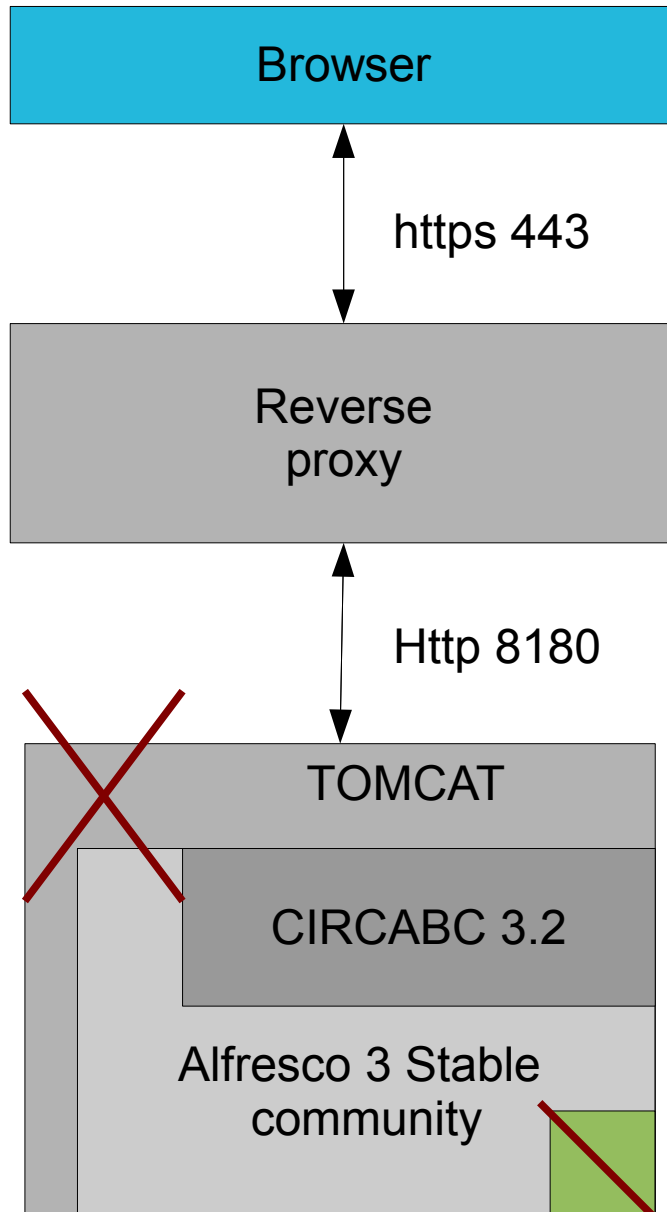
circa-support.eu



Combine simple and advanced



circa-support.eu



```
Not shown: 997 closed ports
PORT      STATE  SERVICE
22/tcp    open   ssh
443/tcp   open   https
1720/tcp  filtered H.323/Q.931
```

don't do what they told ya!

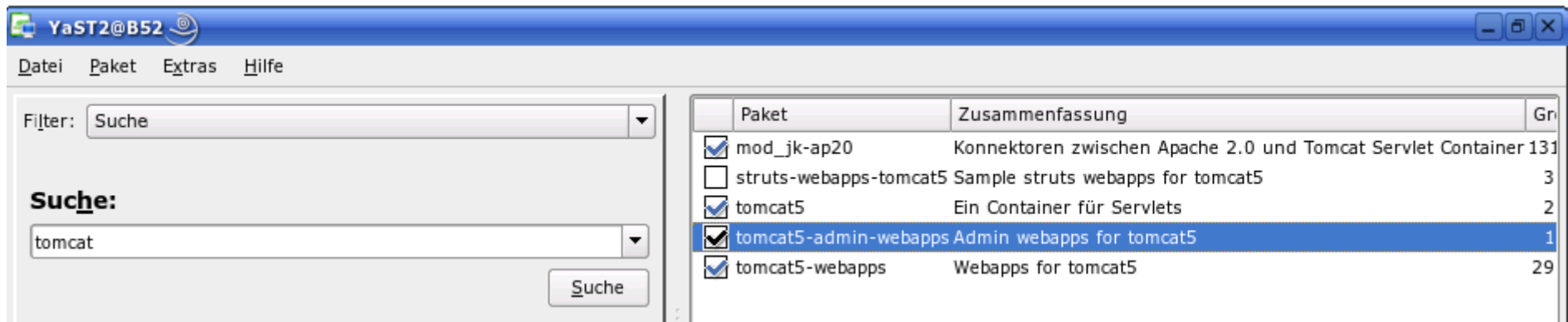
➤ ~~Download the corresponding distribution:~~

~~The tar.gz binary distribution file is available at the following address:~~

~~<http://tomcat.apache.org/download-55.cgi>~~

Please use your distribution's package:

```
# aptitude install tomcat5.5
```



The screenshot shows the aptitude package manager interface. The search filter is set to 'tomcat'. The search results are as follows:

Paket	Zusammenfassung	Gr
<input checked="" type="checkbox"/> mod_jk-ap20	Konnektoren zwischen Apache 2.0 und Tomcat Servlet Container	131
<input type="checkbox"/> struts-webapps-tomcat5	Sample struts webapps for tomcat5	3
<input checked="" type="checkbox"/> tomcat5	Ein Container für Servlets	2
<input checked="" type="checkbox"/> tomcat5-admin-webapps	Admin webapps for tomcat5	1
<input checked="" type="checkbox"/> tomcat5-webapps	Webapps for tomcat5	29

Things I didn't manage ...

- Disabling JMX
- Bind JMX ONLY localhost
- Use jconsole with CIRCABC

```
$ nmap -p1-65535 circabc.circa-support.eu
```

```
8114/tcp open unknown
49353/tcp open unknown
50501/tcp open unknown
50502/tcp open unknown
50503/tcp open unknown
50504/tcp open unknown
50505/tcp open unknown
50506/tcp open unknown
```

... if you can, write to: support@circa-support.eu

Legal issues



circa-support.eu

Quotations were taken from:

- Rage against the machine
- Lord of the Rings

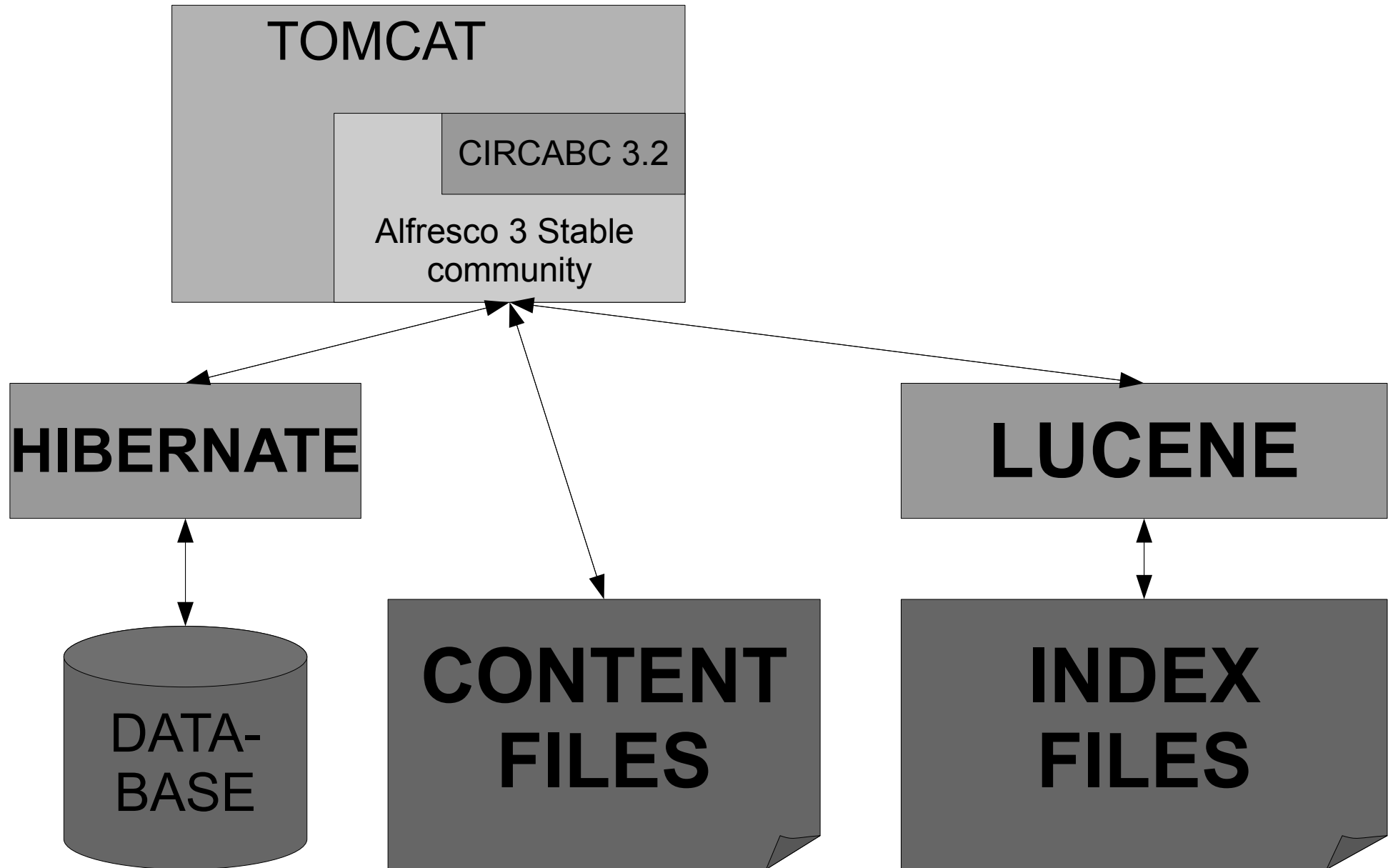
Pretty Pictures from:

- freebsd-image-gallery.netcode.pl
- kendgame.bridigum.com

Backup considerations



circa-support.eu



- STOP CIRCABC
- DATABASE DUMP
- BACKUP FILES AND DUMPS
- START CIRCABC

- DATABASE DUMP
- BACKUP FILES
(EXCEPT LUCENE-INDEXES!)
AND DUMPS

Incremental backup considerations



circa-support.eu

- USE checksums
- Do not RELY on size or timestamp