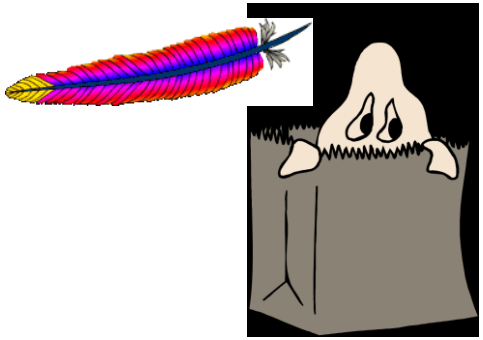
MindWorks UK



Hiding Tomcat behind Apache

Joe Doupnik

MindworksUK and Novell

jrd@netlab1.net

Hiding ports 8080/8443/9443/etc

Example applications: Vibe, SSPR/PWM, Filr

By default users are asked to contact Vibe on ports 8080, 8443 or Filr admin 9443…

Ports and https are nusances, add detail to be remembered

Best would be *http://example.com/foo*, easy to remember, let computers do translations

The official way

The Novell documentation recommends using IPtables to remap ports, say from 80 to 8080 and 443 to 8443.

That unnecessairly clobbers Apache

Tomcat listens on these 8xxx ports and provides little to no access controls, plus doubts about strength against attacks

The user friendly strategy

Redirect browser to https, if desired
Detect user friendly URL prefix
Redirect URL to app specific prefix

Detect app specific prefix on ports 80/443
Proxy into tomcat on its ports (8080,8443,9009 etc)

SSL is between client and Apache, simplifying certs

Vibe's login, a difficult case

Vibe invokes its login screen under two conditions:

	`http(s)://host:port/`	**no path at all (doc root)**
or	`http(s)://host:port/ssf/a`	**an arcane path**

`port` **is 8080 or 8443**

The first results in Vibe itself returning an HTTP redirect to the second form `/ssf/a`

We prefer a `/foo` **prefix to invoke Vibe, no interference with DocumentRoot and other areas**

Friendly Vibe login, first clause

```
<Location /foo>
Options +FollowSymLinks
RewriteEngine on
RewriteRule (.*) https://%{HTTP_HOST}/ssf/a [R]
</Location>
```

This does two things:

ensures usage of HTTPS

steers the browser to a particular path (`/ssf/a`)

***Rule* redirects the browser to resend the request to `https://host/ssf/a` rather than use `http(s)://host/foo`**

(Thus far, no mention of ports)

[R] means send a "301 redirect" to the browser, not just rewrite what the destination sees.

`Options +FollowSymLinks` is needed for this redirect.

Alternative forms

Replace this much:

```
<Location /foo>
Options +FollowSymLinks
RewriteEngine on
RewriteRule (.*) https://%{HTTP_HOST}/ssf/a [R]
</Location
```

with this: (no <Location>, no frills)

```
RewriteEngine on
RewriteCond %{REQUEST_URI} /foo
RewriteRule (.*) https://%{HTTP_HOST}/ssf/a [R]
```

or with this: (no <Location>, hard coded, no frills)

```
RedirectPermanent /foo https://host.address.here/ssf/a
```

Second clause (/ssf), proxying

```
<Location /ssf>
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}/%{REQUEST_URI} [QSA,R]

ProxyPass   ajp://localhost:8009/ssf
ProxyPassReverse   ajp://localhost:8009/ssf
</Location>
```

The majority of Vibe traffic uses the `/ssf` pathway

Ensure use of HTTPS:// via a browser redirect
Proxy into tomcat on its particular port

Clauses 3 & 4 (/ssr, /ssfs)

```
<Location /ssr>
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}/%{REQUEST_URI} [QSA,R]

ProxyPass   ajp://localhost:8009/ssr
ProxyPassReverse   ajp://localhost:8009/ssr
</Location>
```

For Vibe SOAP connections

/ssfs is for Vibe WebDAV

```
<Location /ssfs>
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}/%{REQUEST_URI} [QSA,R]

ProxyPass   ajp://localhost:8009/ssfs
ProxyPassReverse   ajp://localhost:8009/ssfs
</Location>
```

Apache proxy commands

```
<Location /ssf>
RewriteEngine on
RewriteCond %{HTTPS} off
RewriteRule (.*) https://%{HTTP_HOST}/%{REQUEST_URI} [QSA,R]

ProxyPass   ajp://localhost:8009/ssf
ProxyPassReverse  ajp://localhost:8009/ssf
</Location>
```

What the user sends as path prefix

Prefix for Tomcat

Two sections:
If HTTP:// then redirect browser to HTTPS://
This is optional

[QSA,] means keep query strings (?xxx) intact. QSA greatly reduces busy work for [R]edirects

The interesting part is the ProxyPass pair

ProxyPass

```
ProxyPass   ajp://localhost:8009/ssf
ProxyPassReverse   ajp://localhost:8009/ssf
```

ProxyPass has syntax of

```
ProxyPass /userprefix  method://host:port/newprefix
```

`/userprefix` **is what to detect from incoming (say** `/ssf or /foo`**).**

Omit `/userprefix` **if within a <Location> clause because <Location> supplies it.**
`userprefix` **is replaced by** `newprefix` **and the entire string is sent to the application.**

Method: is `http:, https:, ajp:, or balancer:.`

`http(s):` **sends regular HTTP request to destination //host:port.**
`ajp:` **does similarly, but to an ajp listener. Quicker than http.**
`balancer:` **used for load balanced multiple destinations**

Notes on load balancing

The Apache documents show how to distribute connections across two or more worker web servers. This uses the proxy "balancer" feature.

(copying from that documentation, plus my last two lines)

<Proxy balancer://*mycluster*>

BalancerMember http://192.168.1.50:80

BalancerMember http://192.168.1.51:80

</Proxy>

ProxyPass /test balancer://*mycluster*

ProxyPassReverse /test balancer://*mycluster*

(Omit the /test item if doing this within a <Location> clause

Notes on load balancing

The notion is define a cluster of workers within a <proxy> clause. Each worker can be reached by http/https/ajp, mix and match as you wish

In each regular proxypass command pair reference balancer:*cluster-name* rather than a given host name

To make this work we need to add proxy_balancer to the list of installed Apache modules

See the docs about balance scheduling and more

ProxyPassReverse

```
ProxyPass   ajp://localhost:8009/ssf
ProxyPassReverse   ajp://localhost:8009/ssf
```

ProxyPassReverse has the same syntax as ProxyPass
It rewrites headers of replies to simulate them coming from Apache (hiding Tomcat+application details)

ProxyPass and ProxyPassReverse directives should be used as a pair, and look alike

Cleverly, these examples use localhost, but any host will do, even one far far away, plus load balancer clusters

Summary thus far

Detect `/foo` and redirect to `/ssf/a` for Vibe login
Detect `/ssf`, `/ssr`, `/ssfs` and proxy them into Tomcat
[ProxyPass has the port information]
Optionally enforce HTTPS for all

`<Location /ssf>`, `/ssr` and `/ssf` are similar
`<Location /ssfs>` is used for Vibe WebDAV
`<Location /ssr>` is for certain Vibe client SOAP requests, ShareOnVibe uses it

There remains discovering which ports are used by Tomcat, and what URIs are needed by an application

Part of Tomcat server.xml file

```
<!-- A "Connector" using the shared thread pool-->
  <Connector executor="tomcatThreadPool"
            port="8080" protocol="HTTP/1.1"
            connectionTimeout="20000"
            redirectPort="8443"
            URIEncoding="UTF-8" />

   <!-- Define a SSL HTTP/1.1 Connector on port 8443
        This connector uses the JSSE configuration, when using APR, the connector should be using
the OpenSSL
        style configuration described in the APR documentation -->

   <Connector port="8443" protocol="HTTP/1.1" SSLEnabled="true" maxThreads="200"
scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="conf/.keystore"
keystorePass="changeit" keyAlias="tomcat" URIEncoding="UTF-8"/>

   <!-- Define an AJP 1.3 Connector on port 8009 -->
   <Connector port="8009" protocol="AJP/1.3" maxThreads="200" redirectPort="8443"
URIEncoding="UTF-8" tomcatAuthentication="false"/>
```

ajp on 8009 and http on 8080 steer internally to the https 8443 handler for SSL connections

Tomcat listeners

We see that Tomcat in this Vibe example listens on

http://host:8080
https://host:8443
ajp://host:8009

ajp covers both bases. Thus we use method ajp to port 8009

We could have used `ProxyPass http://localhost:8080/ssf` **but ajp is cleaner**

What does the application want?

Observe a web browser when going to an application in the offical “documented” manner. Note the URLs and port numbers etc

That shows what the application wants. We do the proxy work to offer users what they find convenient

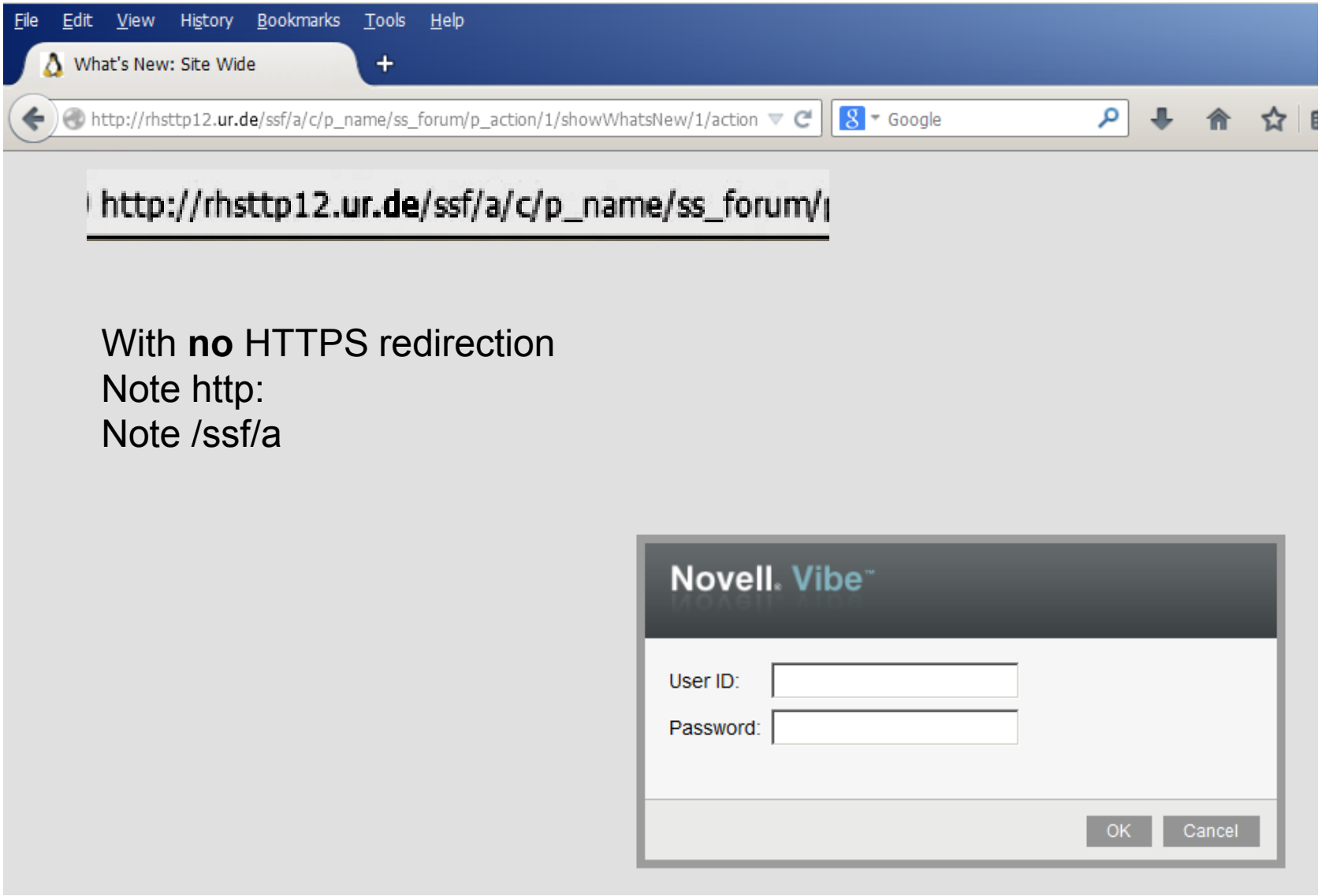
While proxying we can do selective access controls, plus do standard logging via Apache

Apache runs, with our other applications

We do not need (nor want) IPtables port redirection

MindWorks UK

http://rhsttp12.ur.de/foo



With **no** HTTPS redirection
Note http:
Note /ssf/a

http://rhsttp12.ur.de/foo

With HTTPS redirection
Note https:
Note /ssf/a

Wireshark, incoming https://

No.	Time	Source	Destination	Protocol	Length	Info
19	3.78189800	82.70.37.218	132.199.249.55	TCP	68	49875 > https [SYN] Seq=0 Win=8192 Len=0 MSS=14
20	3.78193000	132.199.249.55	82.70.37.218	TCP	68	https > 49875 [SYN, ACK] Seq=0 Ack=1 Win=14600 L
21	3.82933200	82.70.37.218	132.199.249.55	TCP	62	49875 > https [ACK] Seq=1 Ack=1 Win=66560 Len=0
22	3.83024800	82.70.37.218	132.199.249.55	TLSv1	573	Client Hello
23	3.83027500	132.199.249.55	82.70.37.218	TCP	56	https > 49875 [ACK] Seq=1 Ack=518 Win=15744 Len=
24	3.83068300	132.199.249.55	82.70.37.218	TLSv1	201	Server Hello, Change Cipher Spec, Encrypted Hanc
25	3.87836400	82.70.37.218	132.199.249.55	TLSv1	115	Change Cipher Spec, Encrypted Handshake Message
26	3.87871000	82.70.37.218	132.199.249.55	TLSv1	418	Application Data, Application Data
27	3.87875300	132.199.249.55	82.70.37.218	TCP	56	https > 49875 [ACK] Seq=146 Ack=939 Win=16768 Le
28	3.87912900	132.199.249.55	82.70.37.218	TLSv1	732	Application Data, Application Data, Application
29	3.92779100	82.70.37.218	132.199.249.55	TLSv1	482	Application Data, Application Data
30	3.92801700	127.0.0.1	127.0.0.1			
31	3.92954000	127.0.0.1	127.0.0.1	MySQL	89	Request Query
32	3.92967700	127.0.0.1	127.0.0.1	MySQL	79	Response OK
33	3.92973300	127.0.0.1	127.0.0.1	TCP	68	43663 > mysql [ACK] Seq=22 Ack=12 Win=4481 Len=(
34	3.93056400	127.0.0.1	127.0.0.1	MySQL	79	Request Query
35	3.93061900	127.0.0.1	127.0.0.1	MySQL	79	Response OK
36	3.93068900	127.0.0.1	127.0.0.1	MySQL	89	Request Query
37	3.93074000	127.0.0.1	127.0.0.1	MySQL	79	Response OK
38	3.93113400	127.0.0.1	127.0.0.1	MySQL	89	Request Query

Browser speaks HTTPS:// to Apache
Apache speaks plain-text ajp: to tomcat

Thus only Apache's SSL certificate is involved

Apache module setup

In file /etc/sysconfig/apache2, add three items to section APACHE_MODULES=

rewrite, proxy_ajp, proxy_http

Apache application specific files, such as vibe.conf, go into /etc/apache2/conf.d

Add lines

```
include /etc/apache2/conf.d/*.conf
DocumentIndex index.html
```

within the <virtualHost> clause of file /etc/apache2/vhosts.d/vhost-ssl.conf

Another example: NetIQ SSPR, PWM

File /etc/apache2/conf.d/sspr.conf

```
# NetIQ SSPR password recovery application
<Location /sspr>
        Order allow,deny
        allow from all
        ProxyPass  ajp://localhost:9009/sspr
        ProxyPassReverse  ajp://localhost:9009/sspr
</Location>
```

Above I have started on Apache restriction controls (the frills stuf)
SSPR runs behind OES11 tomcat on port 9009, wants path /sspr

OES11 SP2 /var/opt/novell/tomcat5/conf/server.xml snippet:

```
<!-- Define a Coyote/JK2 AJP 1.3 Connector on port
9009 -->
    <Connector port="9009"
               enableLookups="false"
redirectPort="443"
```

URLs embedded in app responses

Network Information

Specify how you want Novell Vibe to communicate on the network.

You must specify a valid fully qualified domain name (FQDN) in order for remote clients and services to connect to your Vibe site.

If installing in a clustered environment, it is important to enter identical set of network information for all the Vibe nodes that are members of the cluster. You must enter the DNS name that end users use to access Vibe services rather than the DNS name of the individual Vibe node.

User's #'s

Host:	rhsttp12.ur.de
HTTP Port:	80
Secure HTTP port:	443

Tomcat #'s

Listen port:	8080
Secure listen port:	8443
Shutdown port:	8005
Session timeout	240
Keystore file	

Some apps send fully qualified URLs within a response body

Some allow them to be tailored

Host name is stated
The user-side port numbers are stated

Vibe permalinks & WebDAV

Permalink	https://rhsttp12.ur.de/ssf/a/c/p_name/ss_forum/p_action/1/binderId/44/action/view_permalink/entityType/folder/vibeonprem_url/1
WebDAV URL	https://rhsttp12.ur.de/ssfs/files/library/Home Workspace/Personal Workspaces/admin (admin)/Files

Both links reference the named host, with /ssf or /ssfs

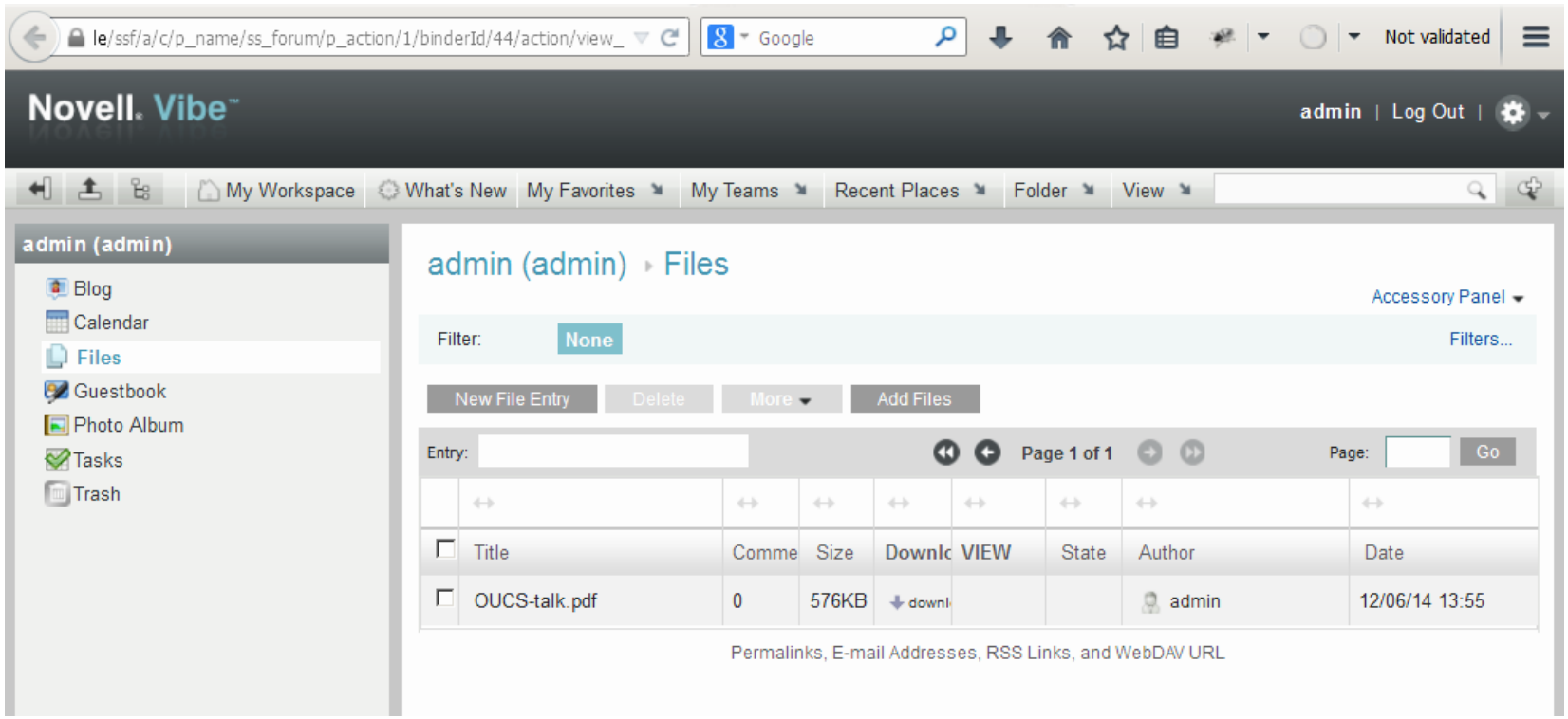
WebDAV requires path prefix /ssfs

Thus four <Location> clauses: /foo, /ssf, /ssr, /ssfs

MindWorks UK

Using the permalink for a file

https://rhsttp12.ur.de/ssf/a/c/p_name/ss_forum/p_action/1/binderId/44/action/view_permalink/entityType/folder/vibeonprem_url/1



MindWorks UK

Using the Vibe WebDAV link

https://rhsttp12.ur.de/ssfs/files/library/Home Workspace/Personal Workspaces/admin (admin)/Files

File Edit View History Bookmarks Tools Help

Files | Directory listing for /files/libra... | Files

https://rhsttp12.ur.de/ssfs/files/library/Home Workspace/Personal Workspaces/admin (admin)/Files

Google

Not validated

Directory listing for /files/library/Home Workspace/Personal Workspaces/admin (admin)/Files

Up To /files/library/Home Workspace/Personal Workspaces/admin (admin)

Filename	Size	Last Modified
OUCS-talk.pdf	575.9 kb	Thu, 12 Jun 2014 13:55:34 GMT

Jakarta Slide 2.2 — Thu, 12 Jun 2014 14:12:39 GMT

ShareOnVibe, it works

File Edit View History Bookmarks Tools Help

Netlab1.net Home Page

http://netlab1.net/

Back
Forwards
Quick Share Page
Share Plus
Share Plus Again
Share Thought
History
Open Vibe Folder
Configure ShareOnVibe
Reload
Bookmark This Page
Save Page As...
View Background Image
Select All
View Page Source
View Page Info
Inspect Element (Q)
Inspect Element with Firebug

rhsttp12.ur.de - Files

other interesting material

Novell a

Novell te

Info and joining Archives (log

https://rhsttp12.ur.de/ssf/a/c/p_name/ss_forum/p_action/1/binderId

Novell. Vibe

My Workspace | What's New | My Favorites | My Teams | Recent Places | Folder | View

admin (admin)
Blog
Calendar
Files
Guestbook
Photo Album
Tasks
Trash

admin (admin) ▸ Files

Filter: None

New File Entry | Delete | More | Add Files

Entry: Page 1 of 1

Title	Comme	Size	Downlc	VIEW	State	Author
OUCS-talk.pdf	0	576KB	downl			admin

Permalinks, E-mail Addresses, RSS Links, and WebDAV URL

SOV wants https:// on the client side (can't handle HTTP redirects)

Filr, fix "port 8443" user path

```
<Location /filr>
        Options +FollowSymLinks
        RewriteEngine On
        RewriteRule (.*) https://%{HTTP_HOST}/ssf/a [QSA,R]
</Location>
```

Redirect to /ssf/a for login

```
<Location /ssf>
        RewriteEngine On
        RewriteCond %{HTTPS} off
        RewriteRule (.*) https://%{HTTP_HOST}/%{REQUEST_URI} [QSA,R]

        ProxyPass ajp://82.70.37.215:8009/ssf
        ProxyPassReverse ajp://82.70.37.215:8009/ssf
</Location>
```

Proxy /ssf to remote Filr

Appliance config path (port 9443) uses a separate java web server (jetty), no prefix.
We cannot readily proxy this with other items.

Filr configuration detail

Network

Specify how you want Novell Filr to communicate on the network.

You must specify a valid fully qualified domain name (FQDN) in order for remote clients and services to c

If installing in a clustered environment, it is important to enter identical set of network information for all t end users use to access Filr services rather than the DNS name of the individual Filr node.

☐ Port Redirection

HTTP Port: 8080 ☑ Enabled ☐ Force Secure Connection

Secure HTTP Port: 8443

AJP Port: 8009 ☑ Enabled

Session Timeout: 240

Keystore File:

Forward Proxy Host Name (optional):

Forward Proxy Port (optional): 80

OK Cancel

None

Filr configuration detail

Reverse Proxy

The Host name is used to build some of the URLs that are sent in notifications. It should reflect the host

Host: filr.jrdresearch.net

Reverse Proxy HTTP Port: 80

Reverse Proxy Secure HTTP Port: 443

NetIQ Access Manager Integration

Configure the following settings if using Novell Filr with NetIQ Access Manager.

Select Enable Access Gateway when user access to the Novell Filr server is provided through Access

Access Gateway address(es) is a comma separated list of IP addresses using the Access Gateway(s

Logout URL is the URL of the Access Gateway for the purpose of simultaneous logout.
Examples: http:///AGLogout or http:///:/AGLogout

☐ Enable Access Gateway

Access Gateway address(es):

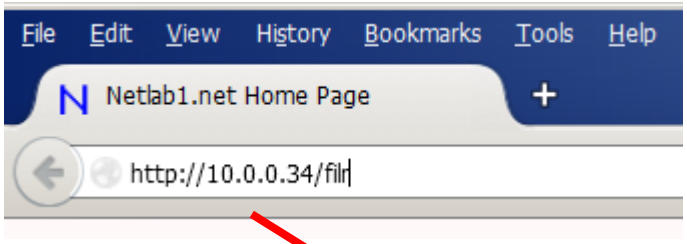
Logout URL:

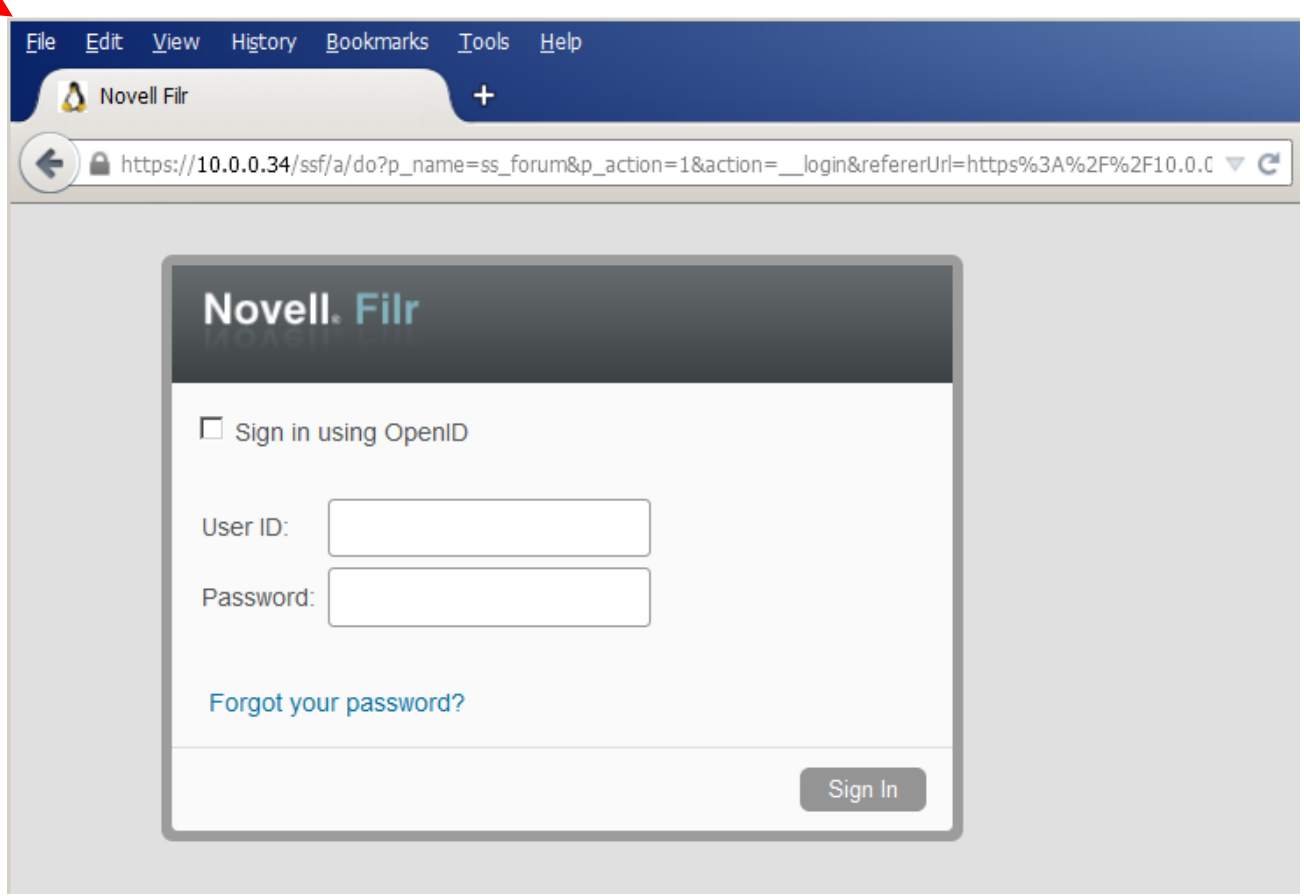
OK Cancel

What users will employ from embedded URLS

Leave unchecked unless really using Access Manager

Log into Filr via proxy (/filr)





Checking Filr offered links

Permalinks

Permalink https://10.0.0.34/ssf/a/c/p_name/ss_forum/p_action/1/action/view_permalink/entityType/folderEntry/entryId/19/novl_url/1

File Download Permalink https://10.0.0.34/ssf/s/readFile/folderEntry/19/d2c6a55746d3677e0146d37710ae0c02/1377794206000/lastView/drums2.html

File Edit View History Bookmarks Tools Help

novttp novttp

https://10.0.0.34/ssf/a/c/p_name/ss_forum/p_action/1/action/view_permalink/entityType/folderEntry

Novell. Filr

My Files Shared with Me Shared by M

drums2.html

drums2.html 1 KB

/Home Workspace/Net Folders/novttp

File Sync Agent 25-Jun-2014 15:38

More

File Edit View History Bookmarks Tools Help

novttp New Tab

tps://10.0.0.34/ssf/s/readFile/folderEntry/19/d2c6a55746d3677e0146d37710ae0c02/1377794206000/lastVi

Opening drums2.html

You have chosen to open:

drums2.html

which is: Firefox HTML Document (523 bytes)

from: https://10.0.0.34

What should Firefox do with this file?

Open with Firefox (default)

Save File

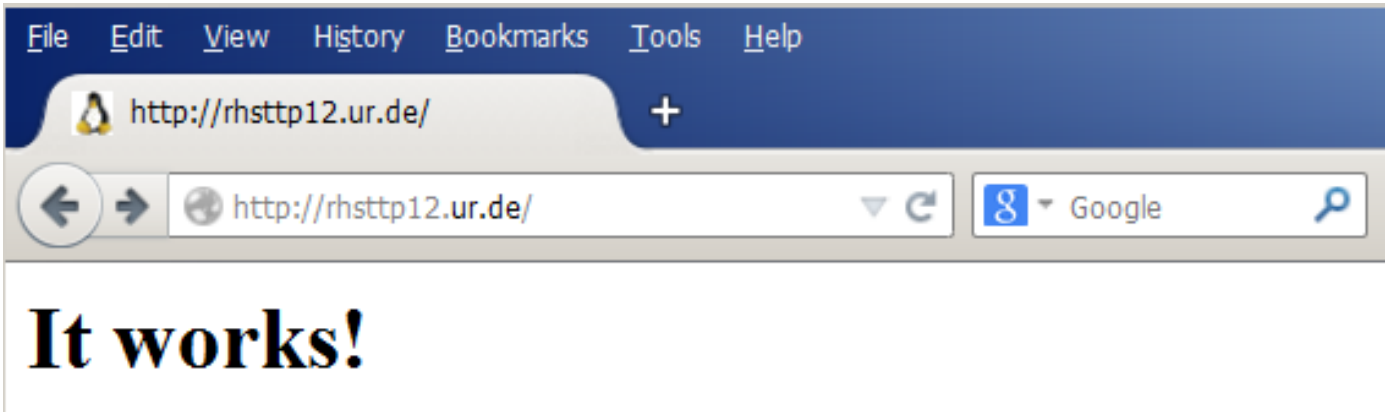
Do this automatically for files like this from now on.

OK Cancel

IP 10.0.0.34 is the proxy machine

Document root, preserved

http(s)://host/



Summary

Apache may be retained for diverse server issues, including access controls and good logging

Knowledge by users is minimised by removing traces of 8443 and obscure paths; use our own paths

Users can start with http://.../foo
SSL redirection can be forced automatically

The work is done in short ordinary Apache configuration files