

Apache als Reverse Proxy

für iNotes und für Applikationen

Dateien kopieren

- USB Stick
- Fileshare



Stephan Kopp

- Fritz & Macziol Group
- Dabei seit Notes 4.5
- Admin & Entwickler
- <http://stephankopp.net>
- @KoppStephan
- skopp@fum.de



Agenda

- Einführung
- Vorbereitung der Testumgebung
- Szenario 1: 1x Apache + 1x Domino
- Szenario 2: 1x Apache + 2x Domino
- Szenario 3: 1x Apache + 2x Domino + Kosmetik + Sicherheit
- Szenario 4: Komplexe Umgebung inkl. RSA, Kerberos, IBM Docs...

Die Problemstellung

- ich habe mehrere Domino Server
- ich möchte den Anwendern einen einfachen Zugang zu iNotes oder Browser Applikationen bieten (intern und/oder extern)
- ich habe ein Domino Cluster und möchte auch für iNotes ein Failover haben
- ich möchte nicht ständig auf allen Domino Servern irgendwelche SSL Bugs beheben
- Zugriffe von extern sollen evtl. über 2-Factor Authentifizierung laufen

Eine Lösung: Apache Reverse Proxy

- entweder als direkter reverse Proxy in der DMZ
- oder als reverse Proxy zwischen DMZ und Domino
- auch sinnvoll für rein interne Verwendung
- ideale Vorbereitung für IBM Verse

Demo Umgebung

- 1x Windows VM (Virtual Box)
- 2x Domino Server
- 1x Apache Server
- 1x Notes/Admin Client
- *Windows Passwort: AdminCamp15*

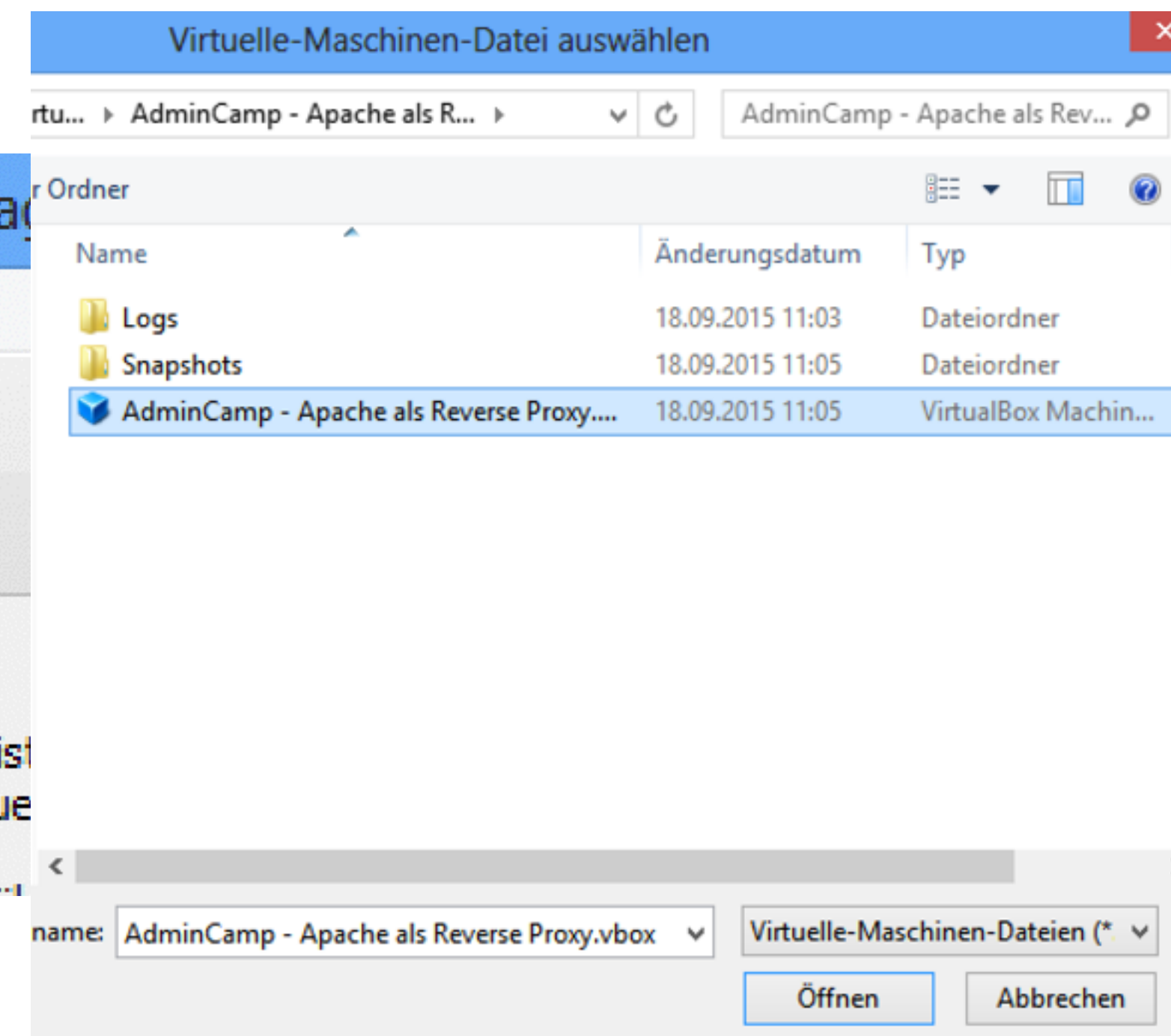
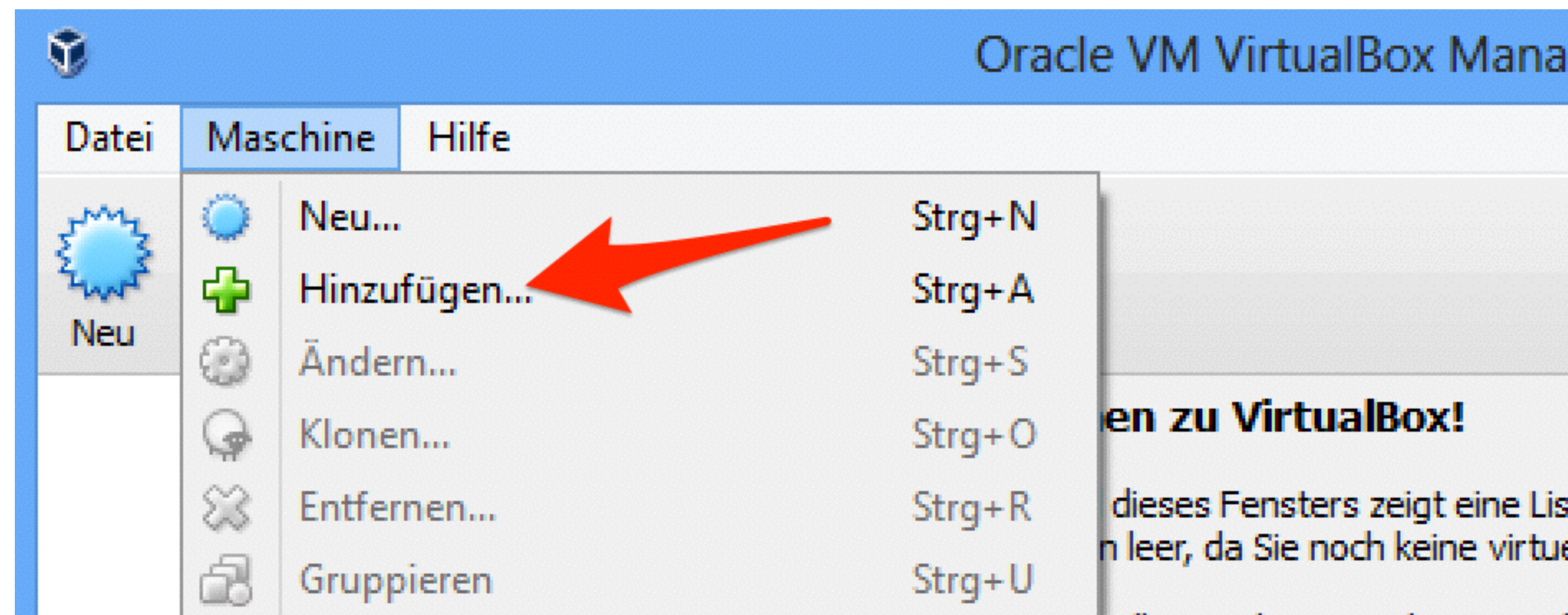
Vorbereitung

- Dateien kopieren
- Virtual Box installieren
- virtuelle Maschine in Betrieb nehmen
- Host Datei und IP Konfig überprüfen

- Ziel:
 - <http://domino1.hands-on.local> erreichbar
 - Anmeldung mit „Test User1“ und „AdminCamp15“ funktioniert
 - <http://domino2.server.lokal> erreichbar
 - Anmeldung mit „Test User2“ und „AdminCamp15“ funktioniert

Virtual Box installieren

- Virtual Box installieren (VirtualBox-5.0.0-101573-Win.exe)
- Den Ordner „AdminCamp - Apache als Reverse Proxy“ auf die lokale Platte kopieren
- Virtual Box starten und Virtuelle Maschine hinzufügen



- Virtuelle Maschine starten

IP Adressen & Hostnamen

- 3 Netzwerkkarten mit diesen IP Adressen:

192.168.56.101

192.168.56.102

192.168.56.103

- Hosts Datei (C:\Windows\System32\Drivers\hosts)

192.168.56.101 domino1 domino1.hands-on.local

192.168.56.102 domino2 domino2.server.lokal

192.168.56.103 apache apache.hands-on.local

Apache installieren

- Installation schon erledigt (next, next, finish)
- Grundkonfiguration (NICHT FÜR DEN PRODUKTIVEN EINSATZ)
- was wurde an der httpd.conf schon geändert?
 - IP Adresse

Vorbereitung abgeschlossen

- <http://domino1.hands-on.local> erreichbar
 - Anmeldung mit „Test User1“ und „AdminCamp15“ funktioniert
- <http://domino2.server.lokal> erreichbar
 - Anmeldung mit „Test User2“ und „AdminCamp15“ funktioniert
- <http://apache.hands-on.local/> erreichbar
 - Service „Apache2.4“ manuell starten



Szenario 1

Ein Apache in der DMZ und ein Domino Server (oder ein Cluster)

Reverse Proxy Konfiguration

- httpd.conf anpassen (C:\Apache24\conf\httpd.conf):
 - ➔ LoadModule proxy_module modules/mod_proxy.so
 - ➔ LoadModule proxy_balancer_module modules/mod_proxy_balancer.so
 - ➔ LoadModule proxy_connect_module modules/mod_proxy_connect.so
 - ➔ LoadModule proxy_http_module modules/mod_proxy_http.so
 - ➔ LoadModule slotmem_shm_module modules/mod_slotmem_shm.so
 - ➔ Include conf/active/*.conf

Szenario1.conf

(C:\Apache24\conf\active\szenario1.conf)

```
<VirtualHost *:80>
```

```
ServerName apache.hands-on.local
```

```
ServerAdmin webmaster@localhost
```

```
LogLevel info
```

```
ErrorLog "C:\Apache24\logs\schritt1_error.log"
```

```
CustomLog "C:\Apache24\logs\schritt1_access.log" common
```

```
ProxyRequests off
```

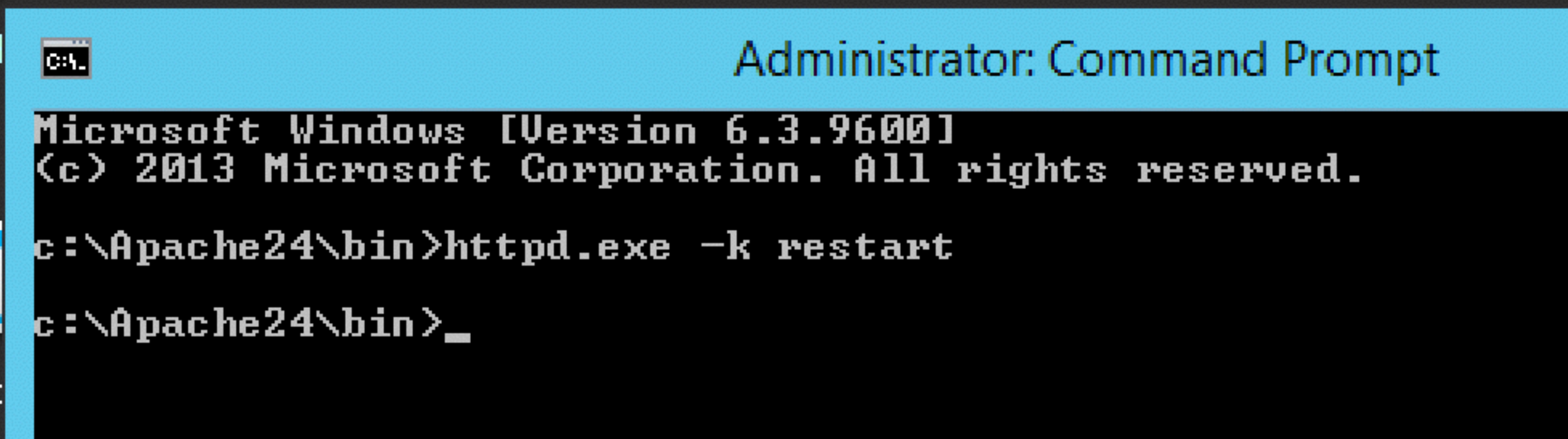
```
ProxyPass / http://domino1.hands-on.local/
```

```
ProxyPassReverse / http://domino1.hands-on.local/
```

```
</VirtualHost>
```


Apache Befehle

- Commandline öffnen
- Pfad sollte C:\Apache24\bin sein
- httpd -k restart



```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\Apache24\bin>httpd.exe -k restart
c:\Apache24\bin>_
```


Domino Konfiguration

- Web Konfig überprüfen (im Server Dokument „Domino1/AdminCamp“)
 - Internet Sites = disabled
 - HTTP hostname = domino1.hands-on.local
 - Bind to hostname = enabled
 - Homepage = /iwaredir.nsf

Server: Domino1/AdminCamp domino1.hands-on.local

Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail | DAOS |

HTTP | Domino Web Engine | DIIOP | LDAP |

| Basics | Mapping |
|---|-------------------------------|
| Host name(s): domino1.hands-on.local | Home URL: /iwaredir.nsf |
| Bind to host name: Enabled | HTML directory: domino\html |
| DNS lookup: Disabled | Icon directory: dominolicons |
| DNS lookup cache: Enabled | Icon URL path: /icons |
| DNS lookup cache size: 256 | CGI directory: dominolcgi-bin |
| DNS lookup cache found 120 seconds timeout: | CGI URL path: /cgi-bin |

Domino Konfiguration

- iNotes Redirect DB öffnen (iwaredir.nsf auf Domino1)
 - Redirection Type: Fixed
 - Reverse Proxy: <http://apache.hands-on.local>

IBM iNotes Redirect configuration

Save & Exit

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

Please select the Redirection type

Fixed
Dynamic
MailServer

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

<http://apache.hands-on.local>

If you wish to force the PATH, please enter it here
(Leave blank to disable)

Help

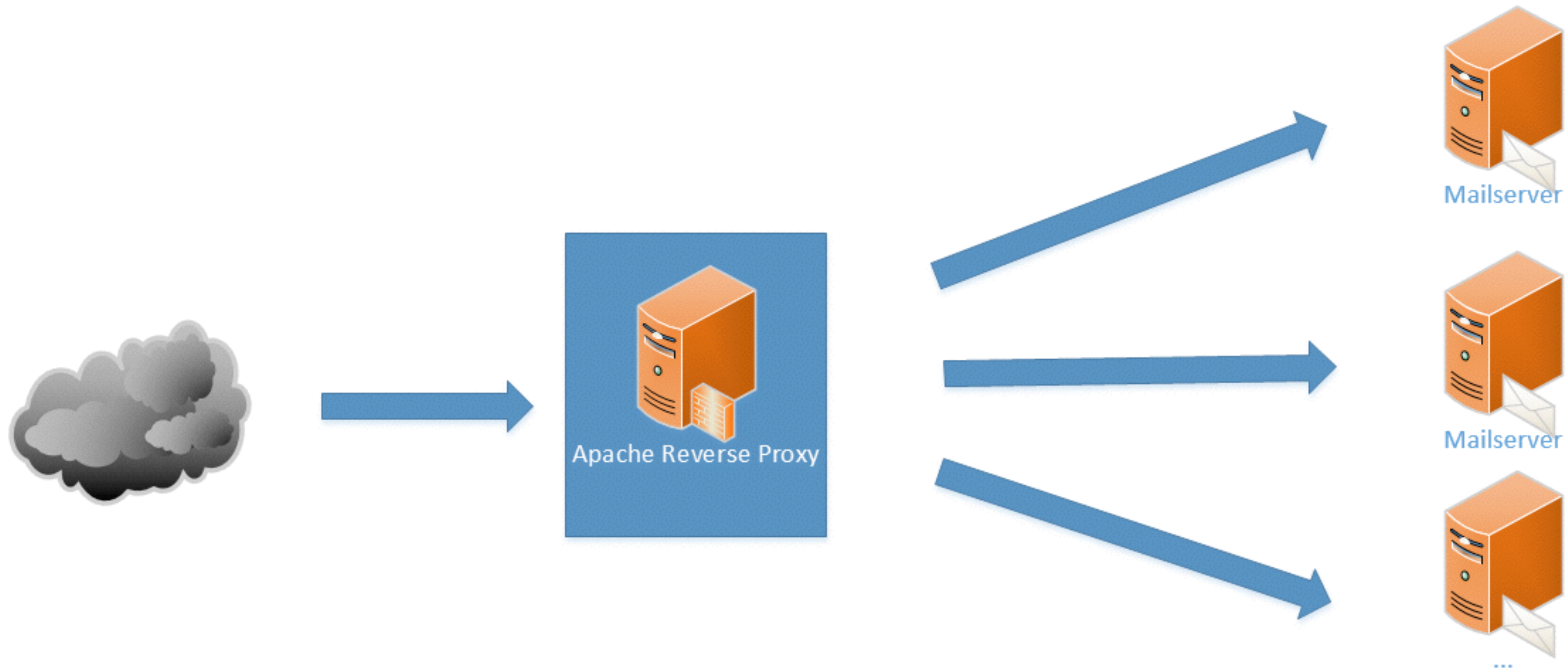
notes.ini

- iNotes_WA_CalOverlay=1
- iNotes_WA_UseRelativeUrl=1

| Add Configuration Edit Configuration Delete Configuration | |
|---|--|
| Server Name | Parameters |
| * - [All Servers] | iNotes_WA_UseRelativeUrl=1 iNotes_WA_CalOverlay=1 |

Ziel

- <http://apache.hands-on.local> erreichbar
- Anmeldung (Test User1) funktioniert und iNotes wird angezeigt
- Ich kann auf iNotes zugreifen, aber auf (fast) nichts anderes



Szenario 2

Ein Apache in der DMZ und mehrere Domino Server

Domino Konfiguration ändern

- Server Dokumente umstellen auf „Internet Sites“ (beide Server)

Server: Domino1/AdminCamp domi

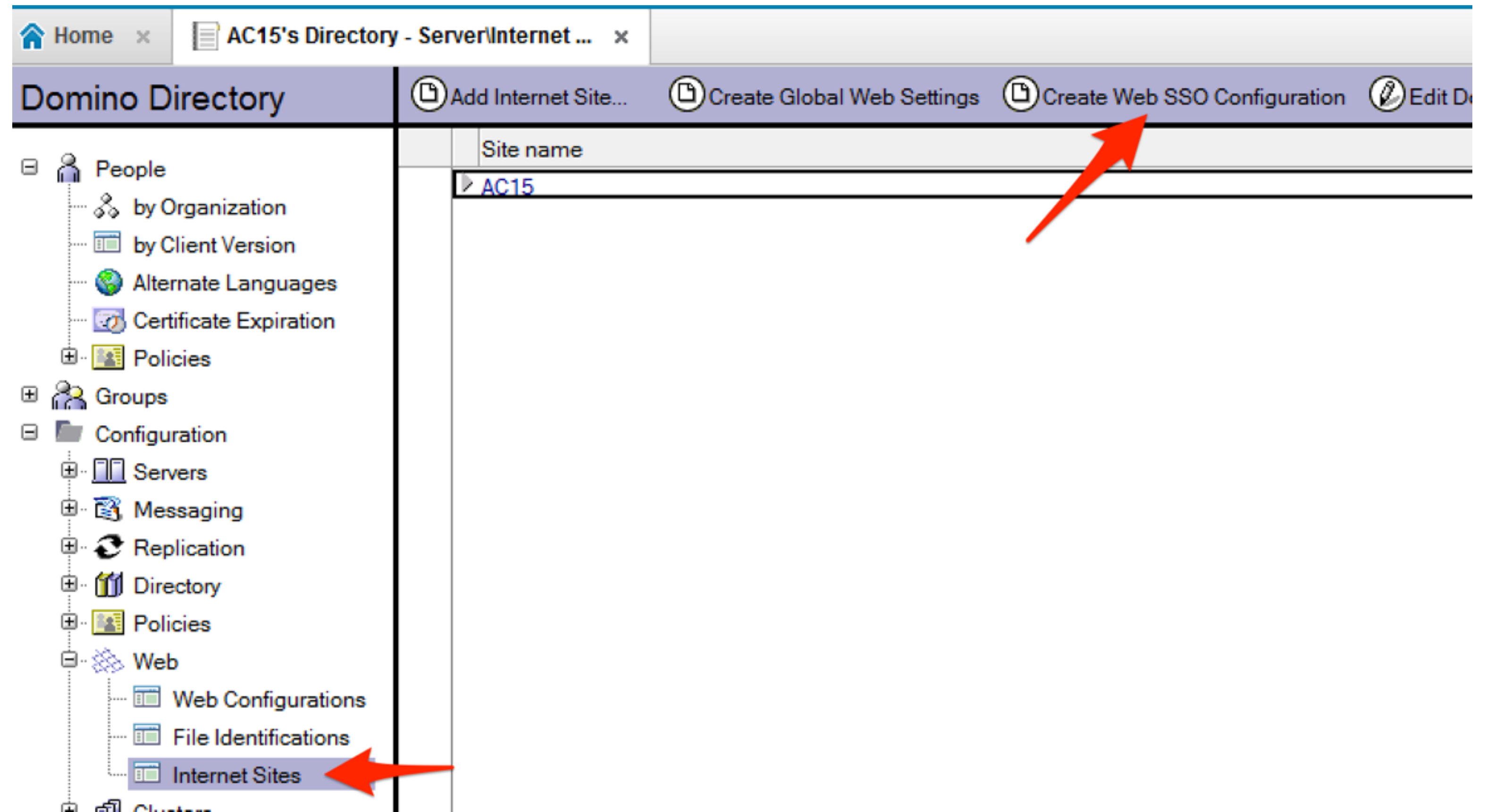
Basics | Security | Ports... | Server Tasks... | Internet Protoco

Basics

| | |
|--|------------------------|
| Server name: | Domino1/AdminCamp |
| Server title: | |
| Domain name: | AC15 |
| Fully qualified Internet host name: | domino1.hands-on.local |
| Cluster name: | |
| Load Internet configurations from Server/Internet Sites documents: | Enabled |

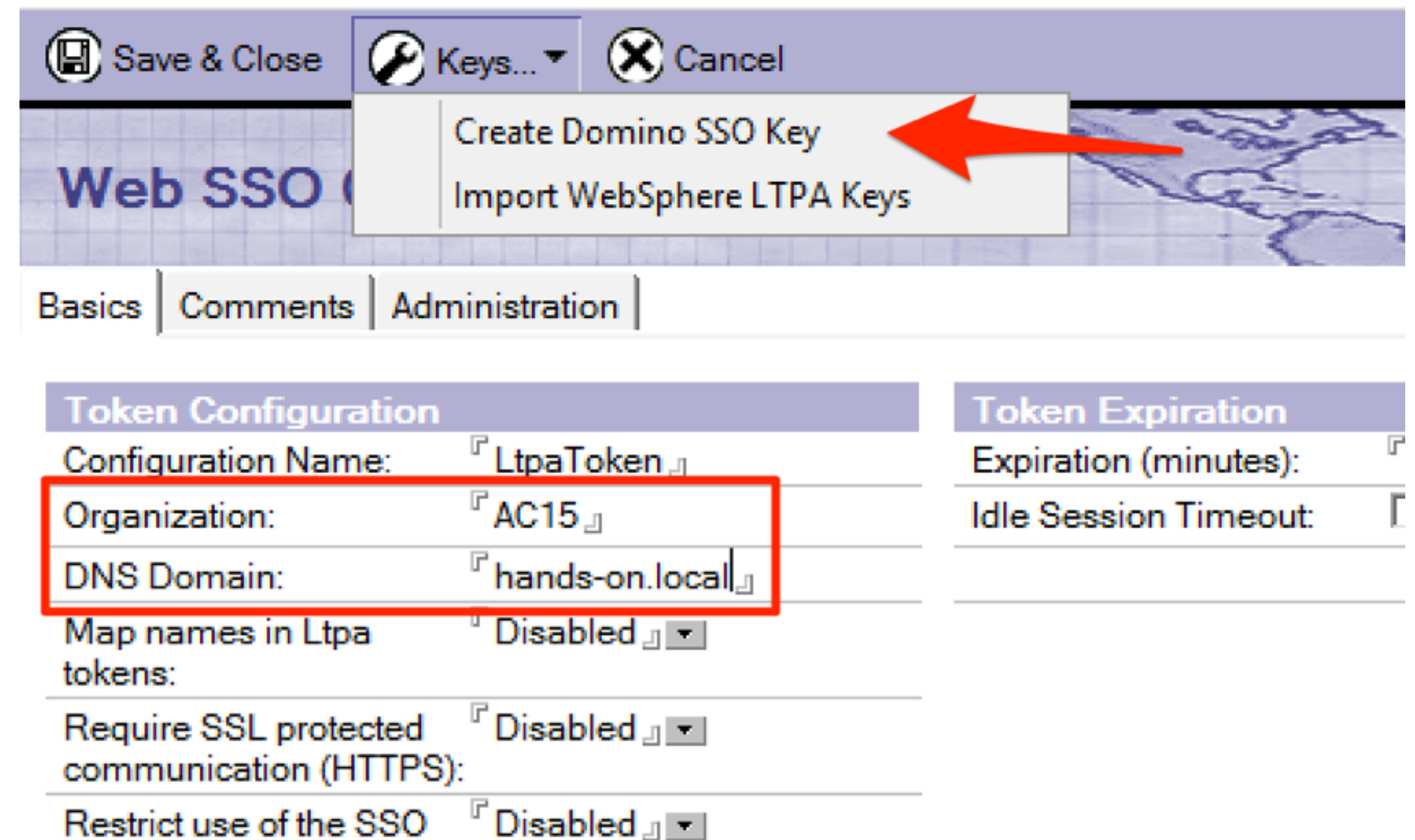
Domino Konfiguration ändern

- SSO Dokument erstellen



Domino Konfiguration ändern

- Create Domino SSO Key
- Organization: AC15
- DNS Domain: hands-on.local



Save & Close Keys... Cancel

Web SSO

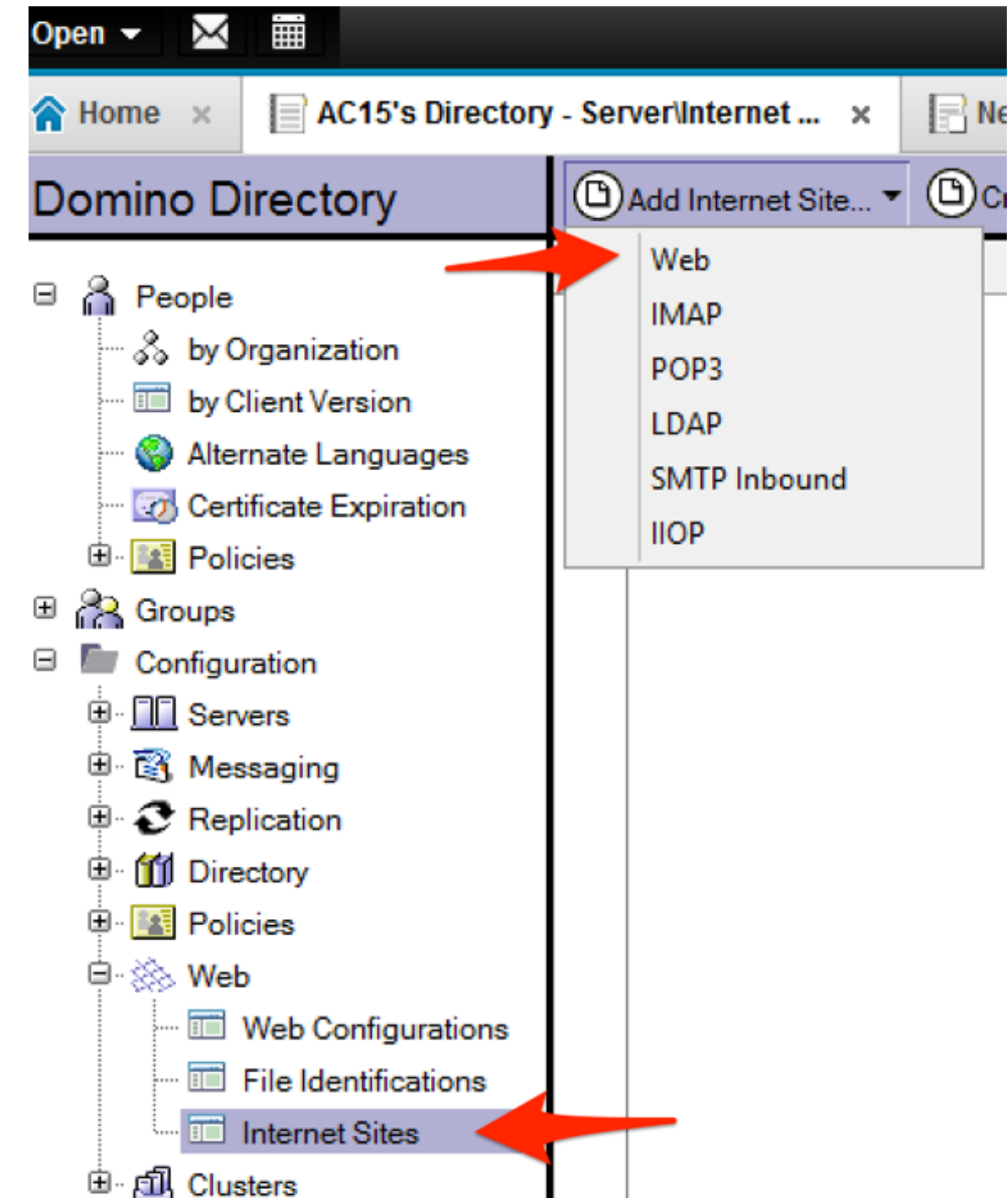
Create Domino SSO Key
Import WebSphere LTPA Keys

Basics | Comments | Administration

| Token Configuration | | Token Expiration | |
|--|----------------|-----------------------|--|
| Configuration Name: | LtpaToken | Expiration (minutes): | |
| Organization: | AC15 | Idle Session Timeout: | |
| DNS Domain: | hands-on.local | | |
| Map names in Ltpa tokens: | Disabled | | |
| Require SSL protected communication (HTTPS): | Disabled | | |
| Restrict use of the SSO | Disabled | | |

Domino Konfiguration ändern

- Internet Site Dokument erstellen



Domino Konfiguration ändern

- Name: iNotes
- Organization: AC15
- Host names:
domino1.hands-on.local
domino2.hands-on.local

The screenshot shows the 'Web Site iNotes' configuration dialog box. The title bar includes 'Web Site...', 'Save & Close', and 'Cancel' buttons. The main title is 'Web Site iNotes'. Below the title is a tabbed interface with tabs for 'Basics', 'Configuration', 'Domino Web Engine', 'Security', 'Comments', and 'Admin'. The 'Basics' tab is selected, showing the 'Site Information' section. The 'Descriptive name for this site:' field is set to 'iNotes'. The 'Organization:' field is set to 'AC15'. The 'Use this web site to handle requests which cannot be mapped to any other web sites:' checkbox is checked, with a note: 'Note: only one web site should be set to Yes'. The 'Host names or addresses mapped to this site:' field is set to 'domino1.hands-on.local' and 'domino2.hands-on.local'. The 'Domino servers that host this site:' field is set to '*'. Red boxes highlight the 'iNotes', 'AC15', and the host names fields.

Web Site... Save & Close Cancel

Web Site iNotes

Basics | Configuration | Domino Web Engine | Security | Comments | Admin

Site Information

Descriptive name for this site: iNotes

Organization: AC15

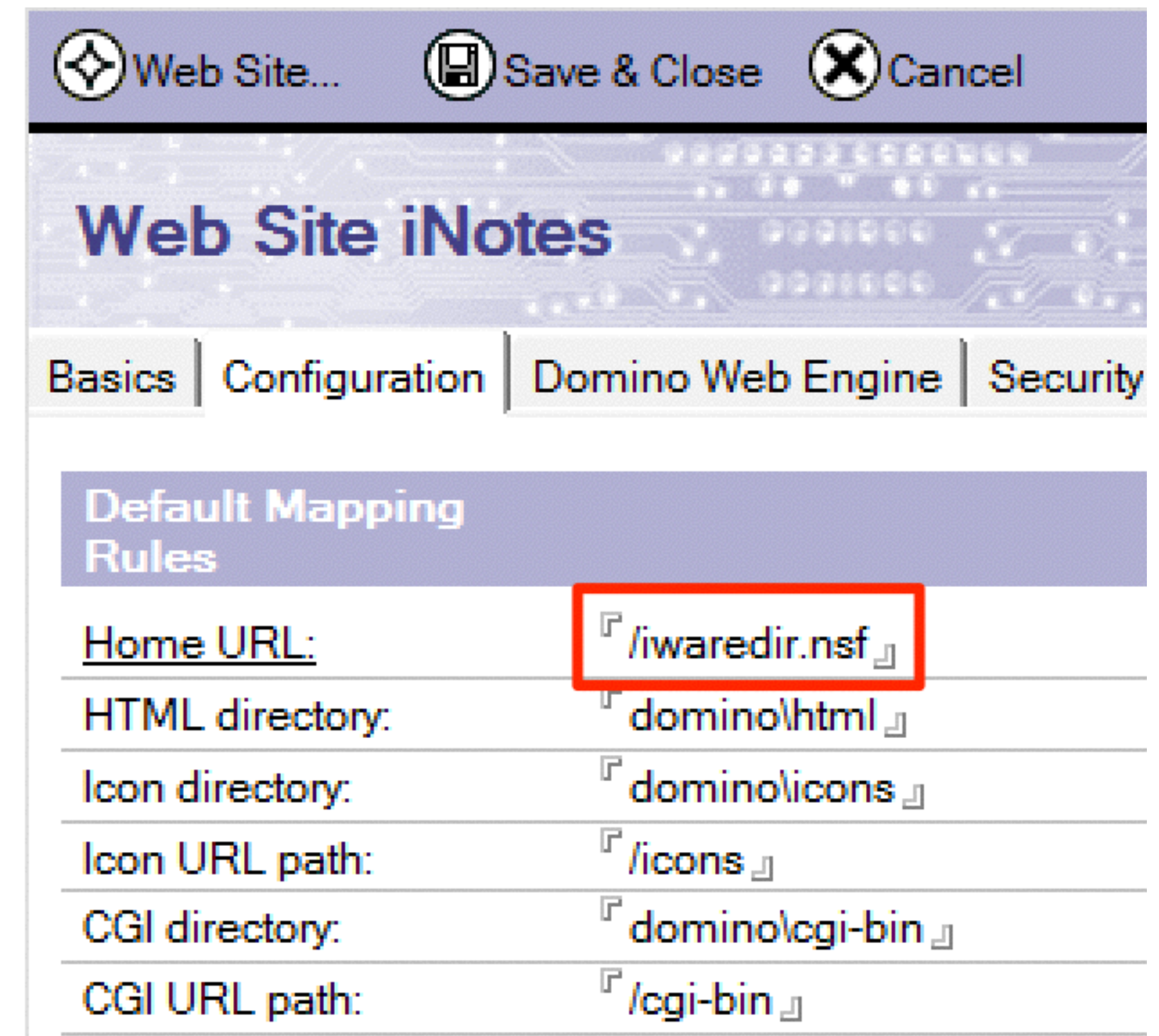
Use this web site to handle requests which cannot be mapped to any other web sites: Yes No
Note: only one web site should be set to Yes

Host names or addresses mapped to this site: domino1.hands-on.local
domino2.hands-on.local

Domino servers that host this site: *

Domino Konfiguration ändern

- Homepage: /iwaredir.nsf



Domino Konfiguration ändern

- Session authentication:
Multiple Servers (SSO)
- Web SSO Configuration:
LtpaToken



Web Site... Save & Close Cancel

Web Site iNotes

Basics | Configuration | Domino Web Engine | Security | Comr

HTTP Sessions

Session authentication: Multiple Servers (SSO) ▾

Web SSO Configuration: LtpaToken ▾

Force login on SSL: No ▾

When overriding session authentication, generate session cookie: Yes ▾

Domino Konfiguration ändern

- iNotes Redirect DB öffnen (iwaredir.nsf auf Domino1)
 - Redirection Type: MailServer
 - Reverse Proxy: <http://apache.hands-on.local>

IBM iNotes Redirect configuration

Save & Exit

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

Please select the Redirection type

Fixed
Dynamic
MailServer

Please enter a valid TCP/IP domain for the mailserver

Help

Please enter a valid Reverse Proxy server to use
i.e., <http://mail.lotus.com> (or use https:// to use SSL)

Help

http://apache.hands-on.local

Domino Konfiguration ändern

- Domino1 mit Domino2 replizieren
- Beide Server neu starten

DNS Alias

- Hosts Datei anpassen (C:\Windows\System32\drivers\etc\hosts)

192.168.56.102 domino2 domino2.server.lokal domino2.hands-on.local

```
# localhost name resolution is handled within DNS itself.
#       127.0.0.1       localhost
#       ::1            localhost
192.168.56.101 domino1 domino1.hands-on.local
192.168.56.102 domino2 domino2.server.lokal domino2.hands-on.local
192.168.56.103 apache apache.hands-on.local|
```

Apache Konfiguration erweitern

- C:\Apache24\conf\szenario1.conf löschen oder umbenennen
- httpd.conf anpassen (C:\Apache24\conf\httpd.conf):
 - ➔ LoadModule rewrite_module modules/mod_rewrite.so
 - ➔ LoadModule lbmethod_byrequests_module modules/mod_lbmethod_byrequests.so
 - ➔ LoadModule slotmem_plain_module modules/mod_slotmem_plain.so

Szenario2.conf

```
<VirtualHost *:80>
```

```
ServerName apache.hands-on.local
```

```
ServerAdmin webmaster@localhost
```

```
LogLevel info
```

```
#LogLevel Debug
```

```
ErrorLog "C:\Apache24\logs\szenario2_error.log"
```

```
CustomLog "C:\Apache24\logs\szenario2_access.log" common
```

```
ProxyRequests off
```

```
RewriteEngine On
```

Szenario2.conf

```
#~~~~~#  
# Rule 0 : If Cookie is set and user logs out, remove the cookie  
RewriteCond %{HTTP_COOKIE} ^.*iNotesServer=.*  
RewriteCond %{QUERY_STRING} ^Logout  
RewriteRule ^/.* - [R=301,CO=iNotesServer:INVALID::-1]  
  
# Rule 1 : Read domino server name from first access to the mail directory,  
# save it to the cookie and redirect to the mail server  
RewriteCond %{REQUEST_URI} ^/(.*)/mail  
RewriteRule /(.*)/mail/(.*) /mail/$2 [QSD,R,L,CO=iNotesServer:$1:hands-on.local]  
  
# Rule 2 : If cookie is set, use it to rewrite rules for iNotes generated URLs  
# and non mail DBs for the server definde in the cookie iNotesServer  
RewriteCond %{REQUEST_URI} ^/domjs [OR]  
RewriteCond %{REQUEST_URI} ^/domjava [OR]  
RewriteCond %{REQUEST_URI} ^/iNotes [OR]  
RewriteCond %{REQUEST_URI} ^/icons [OR]  
RewriteCond %{REQUEST_URI} ^/mail [OR]  
RewriteCond %{REQUEST_URI} ^/archive [OR]  
RewriteCond %{REQUEST_URI} ^/download [OR]  
RewriteCond %{REQUEST_URI} ^/dwa(.*)  
RewriteCond %{HTTP_COOKIE} ^.*iNotesServer=(^[^;]+)  
RewriteRule /(.*). balancer://%1/$1 [P]
```

Szenario2.conf

Rule 3 : if no cookie set -> on first access on the iNotes iwaredir.nsf

```
RewriteCond %{REQUEST_URI} ^/favicon.ico [OR]
```

```
RewriteCond %{REQUEST_URI} ^/domcfg.nsf [OR]
```

```
RewriteCond %{REQUEST_URI} ^/iwaredir(.*) [OR]
```

```
RewriteCond %{REQUEST_URI} ^/names.nsf [OR]
```

```
RewriteCond %{REQUEST_URI} ^/redirect(.*)
```

```
RewriteRule /(.*). balancer://DEFAULT/$1 [P]
```

Rule 4 : everything else should be redirected to the original link

```
RewriteCond %{REQUEST_URI} ^/
```

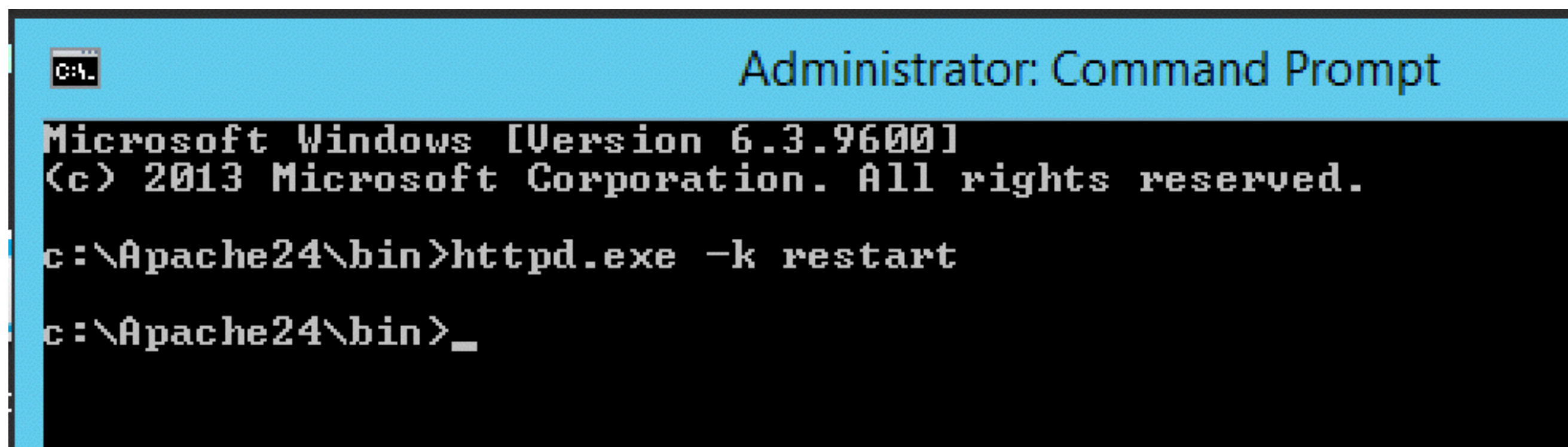
```
RewriteRule / balancer://DEFAULT/ [P]
```

Szenario2.conf

```
### SERVER KONFIGURATION ###  
<Proxy balancer://DEFAULT>  
    BalancerMember http://domino1.hands-on.local:80  
</Proxy>  
  
<Proxy balancer://domino1>  
    BalancerMember http://domino1.hands-on.local:80  
</Proxy>  
  
<Proxy balancer://domino2>  
    BalancerMember http://domino2.hands-on.local:80  
</Proxy>  
  
ProxyPass / balancer://DEFAULT  
ProxyPassReverse / balancer://DEFAULT  
ProxyPass / balancer://domino1  
ProxyPassReverse / balancer://domino1  
ProxyPass / balancer://domino2  
ProxyPassReverse / balancer://domino2  
  
</VirtualHost>
```

Apache Neustart

- Commandline öffnen
- Pfad sollte C:\Apache24\bin sein
- httpd -k restart

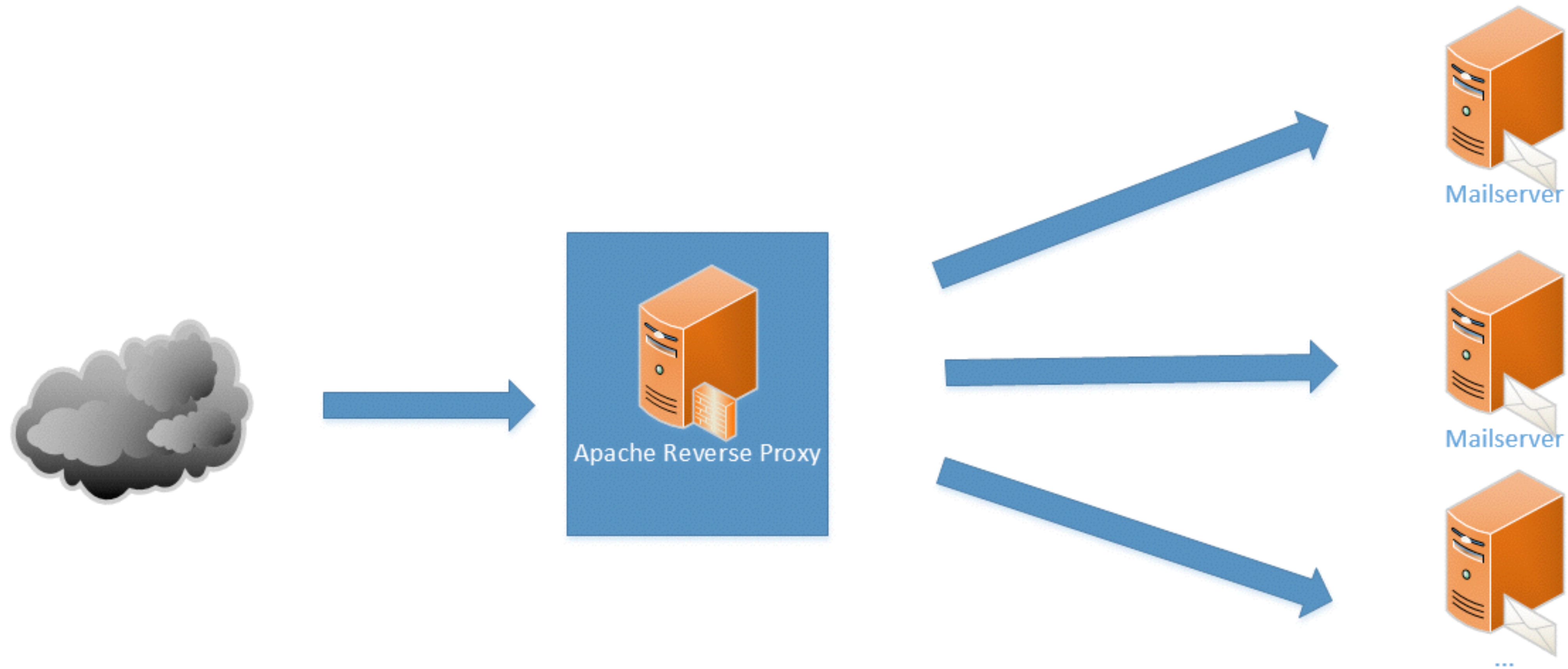


```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\Apache24\bin>httpd.exe -k restart
c:\Apache24\bin>_
```

Ziel

- Anmeldung mit User: „Test User1“ an <http://apache.hands-on.local>
- Anmeldung mit User: „Test User2“ an <http://apache.hands-on.local>
- Beide Domino Server sind über die selbe URL erreichbar



Szenario 3

die Feinheiten

Die Feinheiten

- SSL zumindest von extern bis zum Apache
- URL Maskierung
- Zugriff auf Attachments verhindern
- Zugriff auf weitere Applikationen und Systeme

SSL Aktivierung

- httpd.conf
 - LoadModule ssl_module modules/mod_ssl.so
- SSL Zertifikate sind schon vorhanden
 - es sollten natürlich offizielle verwendet werden

Szenario3.conf

(Szenario2.conf in Szenario3.conf umbenennen)

<VirtualHost *:443>

ServerName apache.hands-on.local

ServerAdmin webmaster@localhost

LogLevel info

#LogLevel Debug

ErrorLog "C:\Apache24\logs\szenario3_error.log"

CustomLog "C:\Apache24\logs\szenario3_access.log" common

ProxyRequests off

RewriteEngine On

#~~~~~#

SSLEngine On

SSLProxyEngine On

SSLCertificateFile "\${SRVROOT}/conf/ssl/server.crt"

SSLCertificateKeyFile "\${SRVROOT}/conf/ssl/server.key"

Szenario3.conf

```
<VirtualHost *:80>  
ServerName apache.hands-on.local  
ErrorLog "C:\Apache24\logs\szenario3_error.log"  
CustomLog "C:\Apache24\logs\szenario3_access.log" common
```

```
ProxyRequests off  
RewriteEngine On  
RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]  
</VirtualHost>
```

```
<VirtualHost *:443>  
ServerName apache.hands-on.local  
ServerAdmin webmaster@localhost
```

```
LogLevel info  
#LogLevel Debug
```

```
ErrorLog "C:\Apache24\logs\szenario3_error.log"  
CustomLog "C:\Apache24\logs\szenario3_access.log" common
```

Domino

- iNotes Redirect öffnen (iwaredir.nsf)
- Reverse Proxy URL auf https ändern

IBM iNotes Redirect configuration

Save & Exit

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

Please select the Redirection type

Fixed
Dynamic
MailServer

Please enter a valid TCP/IP domain for the mailserver

Help

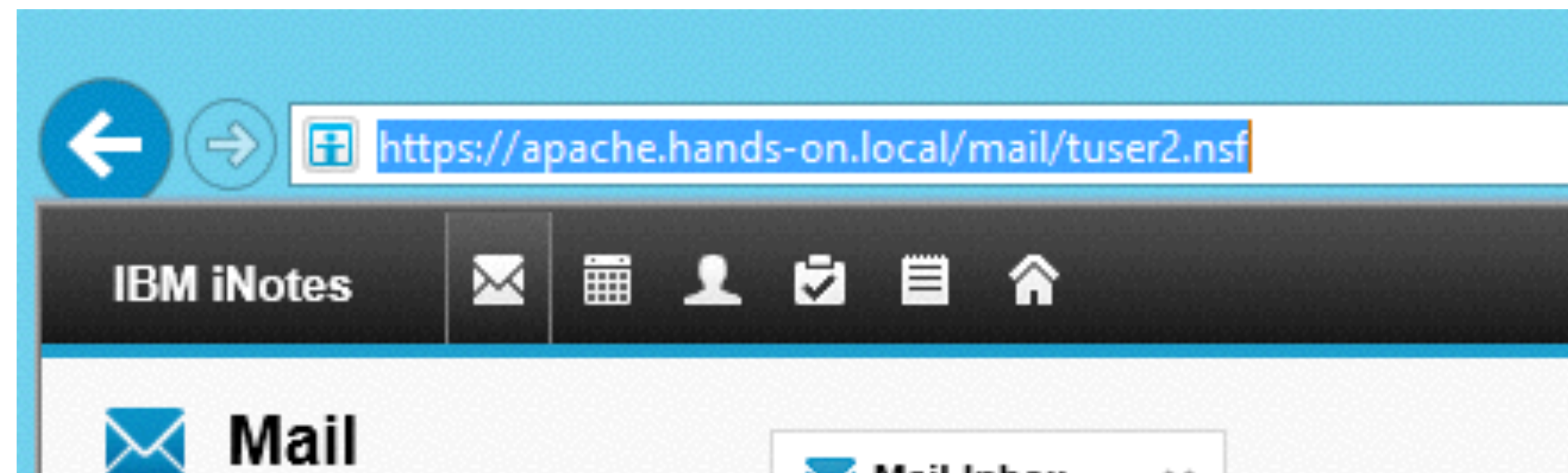
Please enter a valid Reverse Proxy server to use
i.e., <http://mail.lotus.com> (or use https:// to use SSL)

Help

https://apache.hands-on.local

URL Maskierung

- relative Pfade in der URL können manchmal nicht erwünscht sein
- es könnte bei Umzügen der Anwender auf andere Server Probleme geben, wenn diese URLs z.B. als Bookmark gesetzt waren
- Abhilfe: Wir speichern zusätzlich zum Domino Server auch den Pfad in einem Cookie



Szenario3.conf

```
#~~~~~#
SSLEngine On
SSLProxyEngine On
SSLCertificateFile "${SRVROOT}/conf/ssl/server.crt"
SSLCertificateKeyFile "${SRVROOT}/conf/ssl/server.key"

#~~~~~#
SSLProxyVerify none
SSLProxyCheckPeerCN off
SSLProxyCheckPeerName off
SSLProxyCheckPeerExpire off

RewriteCond %{REQUEST_URI} ^/webmail?
RewriteCond %{HTTP_COOKIE} ^.*iNotesPath=([^;]+)
RewriteRule ^/.*/%1 [P]

#~~~~~#
# Rule 0 : If Cookie is set and user logs out, remove the cookie
RewriteCond %{HTTP_COOKIE} ^.*iNotesServer=.*
RewriteCond %{QUERY_STRING} ^Logout
RewriteRule ^/.*/ - [R=301,CO=iNotesServer:INVALID;:-1]

# Rule 1 : Read domino server name from first access to the mail directory,
# save it to the cookie and redirect to the mail server
RewriteCond %{REQUEST_URI} ^/(.*)/mail
#RewriteRule /(.*)/mail/(.*) /mail/$2 [QSD,R,L,CO=iNotesServer:$1:hands-on.local]
RewriteRule ^/(.*)/(mail.*\.\nsf) /webmail? [QSD,R,L,CO=iNotesServer:$1:hands-on.local,CO=iNotesPath:$2:hands-on.local]

# Rule 2 : If cookie is set, use it to rewrite rules for iNotes generated URLs
# and non mail DBs for the server definde in the cookie iNotesServer
```


Zugriff auf Attachments verhindern

- kann man entweder über einen notes.ini Parameter, oder über die URL
- notes.ini verhindert Zugriffe immer, über den Apache können wir z.B. nur externe Zugriffe beschränken

Szenario3.conf

```
#~~~~~#  
# Rule 0 : If Cookie is set and user logs out, remove the cookie  
RewriteCond %{HTTP_COOKIE} ^.*iNotesServer=.*  
RewriteCond %{QUERY_STRING} ^Logout  
RewriteRule ^/.* - [R=301,CO=iNotesServer:INVALID::-1]  
  
# Rule 1 : Read domino server name from first access to the mail directory,  
# save it to the cookie and redirect to the mail server  
RewriteCond %{REQUEST_URI} ^/(.*)/mail  
RewriteRule ^/(.*)/(mail.*\nspf) /webmail?OpenDatabase&ra=0 [QSD,R,L,CO=iNotesServer:$1:hands-on.local,CO=iNotesPath:$2:hands-on.local]  
  
# Rule 2 : If cookie is set, use it to rewrite rules for iNotes generated URLs  
# and non mail DBs for the server define in the cookie iNotesServer
```

Weitere Applikationen

- Im Moment können wir nur auf iNotes zugreifen
- Wir wollen aber den Proxy auch für weitere Applikationen verwenden

Applikation erstellen

- Neue Datenbank auf dem DOMINO1 erstellen
- Template = Discussion Notes & Web
- Pfad = web_app.nsf

Szenario3.conf

```
# Rule 3 : if no cookie set -> on first access on the iNotes iwaredir.nsf
RewriteCond %{REQUEST_URI} ^/favicon.ico [OR]
RewriteCond %{REQUEST_URI} ^/domcfg.nsf [OR]
RewriteCond %{REQUEST_URI} ^/iwaredir.* [OR]
RewriteCond %{REQUEST_URI} ^/names.nsf [OR]
RewriteCond %{REQUEST_URI} ^/redirect.*
RewriteRule /(.* ) balancer://DEFAULT/$1 [P]
```

Application Rule

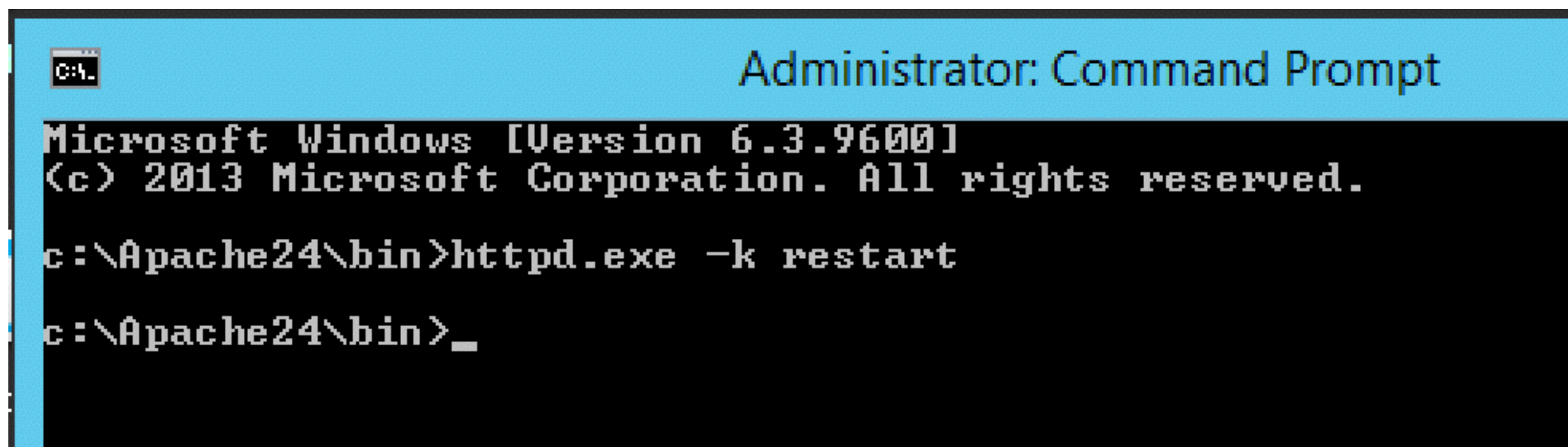
```
RewriteCond %{REQUEST_URI} ^/myApp
RewriteRule / balancer://domino1/web_app.nsf [P]
```

```
RewriteCond %{REQUEST_URI} ^/web_app.nsf [OR]
RewriteCond %{REQUEST_URI} ^/domjava [OR]
RewriteCond %{REQUEST_URI} ^/xsp
RewriteRule ^/(.*) balancer://domino1/$1 [P]
```

```
# Rule 4 : everything else should be redirected to the original link
RewriteCond %{REQUEST_URI} ^/
RewriteRule / balancer://DEFAULT/ [P]
```

Apache Neustart

- Commandline öffnen
- Pfad sollte C:\Apache24\bin sein
- httpd -k restart

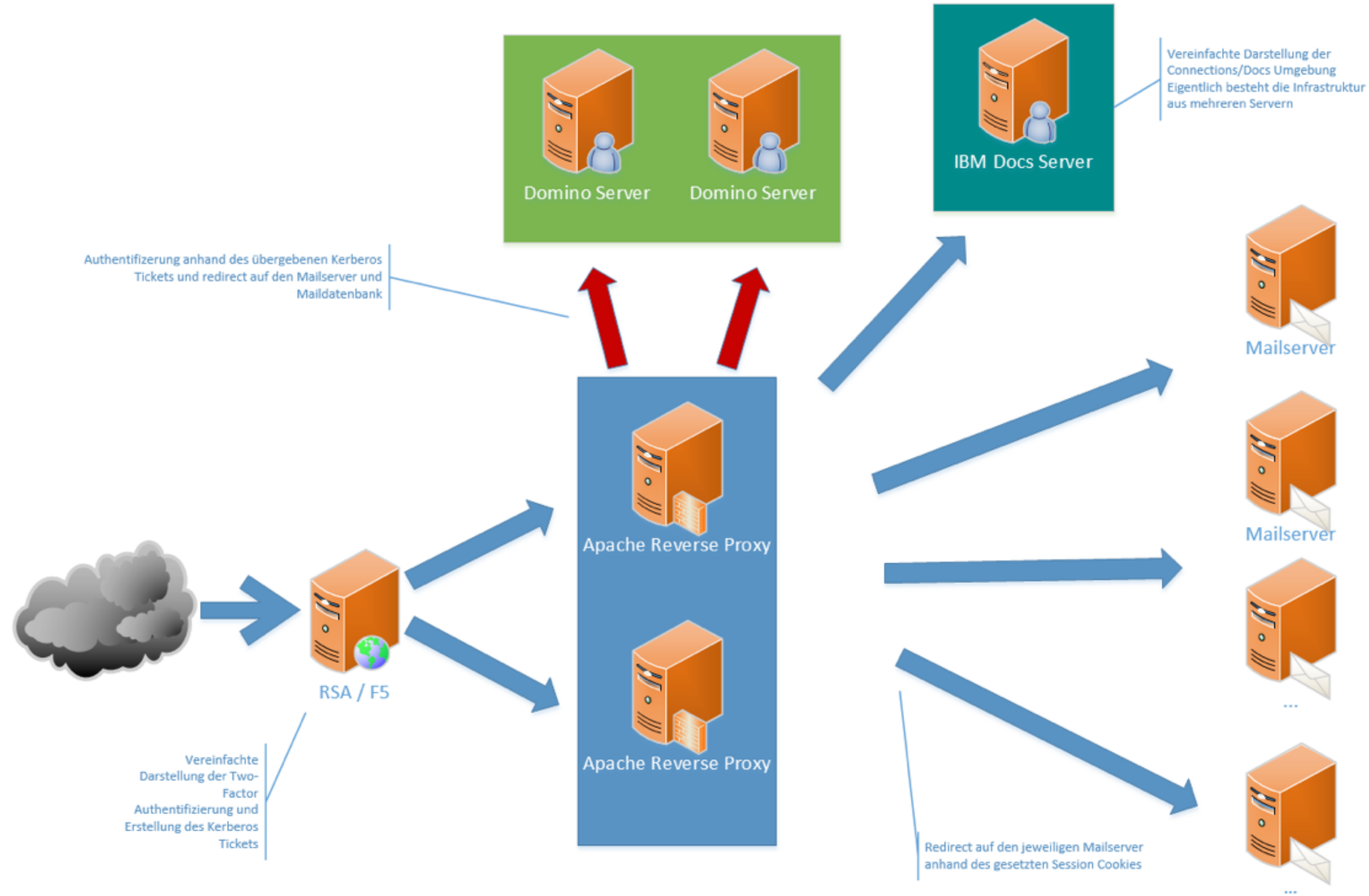


```
Administrator: Command Prompt
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

c:\Apache24\bin>httpd.exe -k restart
c:\Apache24\bin>_
```


Ziel

- Zugriffe laufen immer über SSL
<https://apache.hands-on.local>
- URL für Zugriffe auf iNotes ist mit „webmail“ maskiert
- Ich kann im iNotes keine Anhänge öffnen
- Ich kann auf mein Applikation über /myApp zugreifen
<https://apache.hands-on.local/myApp>



Szenario 4

RSA 2-Factor Authentication, Load Balancer, zwei Apache, Kerberos Authentication, IBM Docs und mehrere interne Domino Server

Fragen?

- <http://stephankopp.de>
- @KoppStephan
- skopp@fum.de

