

Single-Sign-On am AD mit Apache und mod_auth_kerb

Ziel: Geschützte Seiten auf einem Apache-Webserver sollen ohne Passwortabfrage für Benutzer zugänglich sein, die sich bereits an der Windows-Domäne (Active Directory) angemeldet haben.

Konvention: Windows-Domänen-Namen und Kerberos-Realms werden GROß geschrieben!

AD-Maschine:

```
AD-Name: HALLOWELT.LOCAL
FQDN:    sbs.hw-intranet.biz
OS:      Windows Server 2003 für Small Business Server Service Pack 2 32-bit
```

Im AD wird ein Benutzer "kerbdummy" angelegt.

Wir benötigen das MS-Tool `ktpass.exe`. Dieses findet sich in z. B. in den *Windows Server 2003 Service Pack 2 32-bit Support Tools*.

Wir verwenden hier `ktpass.exe` aus der Datei `support.cab` von <http://www.microsoft.com/downloads/details.aspx?familyid=96A35011-FD83-419D-939B-9A772EA2DF90&displaylang=en>
(Beschreibung auf <http://support.microsoft.com/?kbid=926027>)

Apache-Webserver:

```
FQDN: ivm2.hw-intranet.biz
OS:   Ubuntu 8.04 LTS (krb5-config krb5-user libapache2-mod-auth-kerb libkrb53)
```

Wichtig: Beide Server müssen den jeweils anderen mit dessen FQDN erreichen (z. B. anpingen) können! Die Systemzeit darf nicht mehr als 5 Minuten abweichen!

Editieren der Datei `/etc/krb5.conf` (minimalistisch, aber funktioniert!):

```
[libdefaults]
    default_realm = HALLOWELT.LOCAL

[realms]
    HALLOWELT.LOCAL = {
        kdc = sbs.hw-intranet.biz
        admin_server = sbs.hw-intranet.biz
    }
```

Die irreführende Fehlermeldung "*Cannot find KDC for requested realm while getting initial credentials*" kann auf DNS-Probleme hinweisen, die evtl. durch Hinzufügen von

```
[domain_realm]
    hw-intranet.biz = HALLOWELT.LOCAL
    .hw-intranet.biz = HALLOWELT.LOCAL
```

behooben werden.

Test der Authentifizierung:

```
root@ivm2:~# kinit -VV kerbdummy@HALLOWELT.LOCAL
Password for kerbdummy@HALLOWELT.LOCAL:
Authenticated to Kerberos v5
```

Damit ist bereits eine große Hürde genommen!

Auf AD Keytab erzeugen:

Wichtig: Zur Verwendung mit dem IE **muss** der Principal Name mit „HTTP/“ beginnen!*

Auf Windows Server 2003 R2 (starke RC4-Verschlüsselung):

```
C:\>ktpass -princ HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL -mapuser
kerbdummy@HALLOWELT.LOCAL -crypto rc4-hmac-nt -ptype KRB5_NT_SRV_HST -pass
hallowelt -out c:\http.keytab
Targeting domain controller: sbs2003.HALLOWELT.LOCAL
Using legacy password setting method
Successfully mapped HTTP/ivm2.hw-intranet.biz to kerbdummy.
WARNING: pType and account type do not match. This might cause problems.
Key created.
Output keytab to c:\http.keytab:
Keytab version: 0x502
keysize 76 HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL ptype 3 (KRB5_NT_SRV_HST)
vno 3 etype 0x17 (RC4-HMAC) keylength 16 (0x0da8467ddcafe7ead260a8a76546c4f3)
```

Auf Windows Server 2003 (beherrscht nur DES-Verschlüsselung):

```
C:\>ktpass -princ HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL -mapuser
kerbdummy@HALLOWELT.LOCAL -crypto DES-CBC-MD5 -ptype KRB5_NT_PRINCIPAL -mapop
set +desonly -pass hallowelt -out c:\http.keytab
```

(Ausgabe ähnlich wie oben; etwaige Fehlermeldungen und vno beachten!)

Die Datei c:\http.keytab auf den Webserver kopieren und für Apache lesbar machen.

Auf dem Webserver diese testen:

```
root@ivm2:~# kinit -VV -k -t ./http.keytab HTTP/ivm2.hw-intranet.biz
Authenticated to Kerberos v5
```

```
root@ivm2:~# kvno HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL
HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL: kvno = 3
```

Die Key Version Number (hier: **3**) muss mit der Ausgabe von ktpass.exe übereinstimmen!

Erhaltene Tickets können wie folgt abgerufen werden:

```
root@ivm2:~# klist -e
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL

Valid starting      Expires            Service principal
07/30/08 16:28:54  07/31/08 02:28:54  krbtgt/HALLOWELT.LOCAL@HALLOWELT.LOCAL
        renew until 07/31/08 16:28:54, Etype (skey, tkt): ArcFour with HMAC/md5,
ArcFour with HMAC/md5
07/30/08 16:29:43  07/31/08 02:28:54  HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL
        renew until 07/31/08 16:28:54, Etype (skey, tkt): ArcFour with HMAC/md5,
ArcFour with HMAC/md5

Kerberos 4 ticket cache: /tmp/tkt0
klist: You have no tickets cached
```

Mittels `kdestroy` können vorhandene Tickets wieder gelöscht werden.

Jetzt kann eigentlich nichts mehr schiefgehen!

Schützen eines Verzeichnisses per `mod_auth_kerb`:

Wir schützen ein Verzeichnis, indem wir eine Datei namens `.htaccess` darin ablegen. Damit diese gelesen wird, muss in der Apache-Konfiguration der Wert `AllowOverride AuthConfig` gesetzt sein.

```
root@ivm2:~# cat /var/www/.htaccess
```

```
AuthType Kerberos
KrbAuthRealms HALLOWELT.LOCAL
KrbServiceName HTTP
Krb5Keytab /root/http.keytab
KrbMethodNegotiate on
KrbMethodK5Passwd off
require valid-user
```

(Erklärung `mod_auth_kerb`-Parameter: <http://modauthkerb.sourceforge.net/configure.html>)

Client-Seite (Client am AD angemeldet; hier Internet Explorer 7)

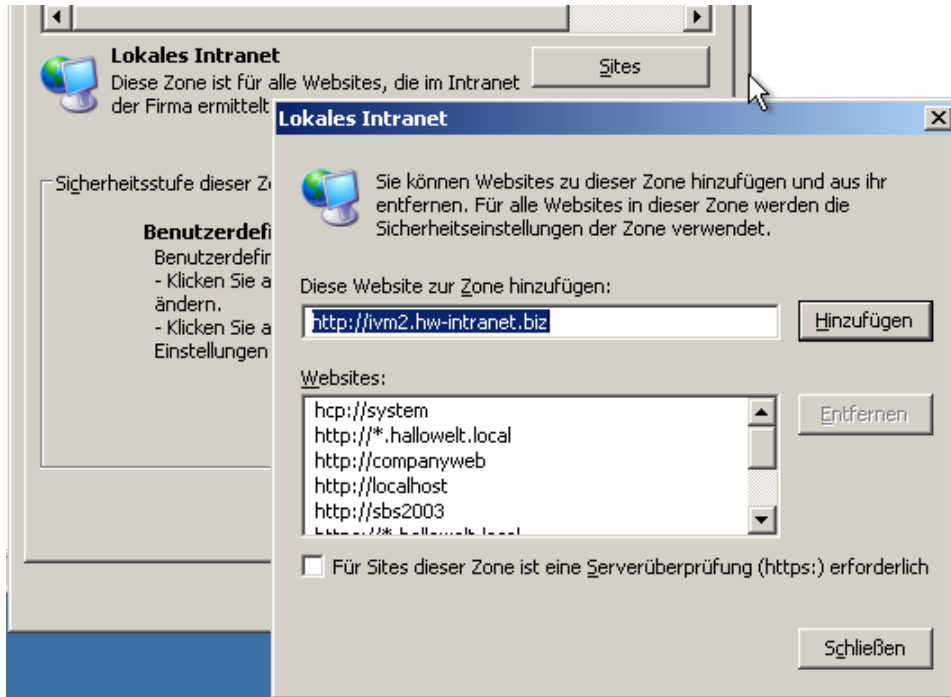
Wenn die Seite `http://ivm2.hw-intranet.biz` vom IE als zum Intranet gehörig erkannt wird, ist bei Default-Einstellung nichts weiter zu tun.

→ Der Zugriff sollte dann bereits ohne Passworteingabe funktionieren!

Ansonsten muss die Seite <http://ivm2.hw-intranet.biz> noch der Intranet-Zone hinzugefügt werden:

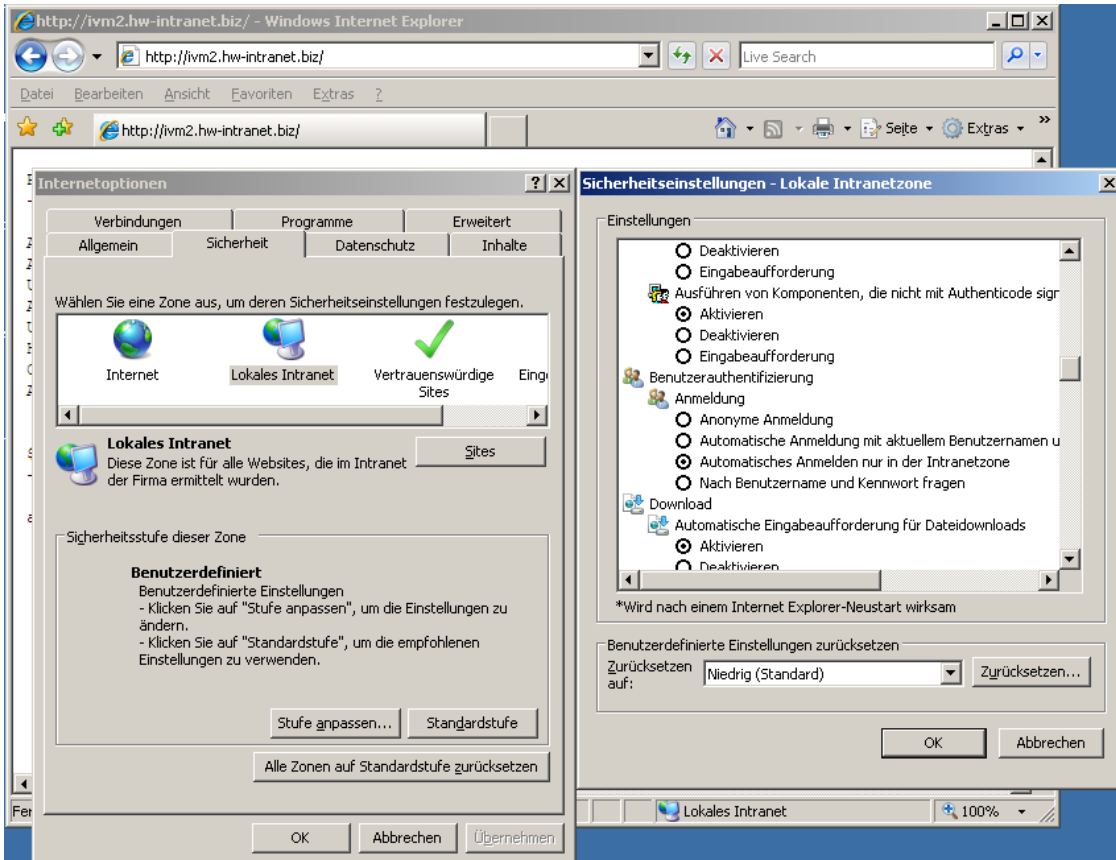
Extras → *Internetoptionen* → *Sicherheit* → *Lokales Intranet* → *Sites*:

„<http://ivm2.hw-intranet.biz>“ eingeben und auf „*Hinzufügen*“ klicken.



Sollte Single-Sign-On noch immer nicht funktionieren, muss evtl. noch „Automatisches Anmelden“ für die Intranet-Zone aktiviert werden:

Extras → *Internetoptionen* → *Sicherheit* → *Lokales Intranet* → *Stufe anpassen...*:



Unter „*Benutzerauthentifizierung*“ den Punkt „*Automatisches Anmelden nur in der Intranetzone*“ aktivieren.

Herzlichen Glückwunsch. Es ist vollbracht!

Wichtige Links:

There's a lot of stuff in the krb5.conf and kdc.conf files. What does it all mean, and what do I really need?

<http://www.faqs.org/faqs/kerberos-faq/general/section-38.html>

Using mod_auth_kerb and Windows 2000/2003 as KDC

<http://grolmsnet.de/kerbtut/>

Kerberos Module for Apache: Directives

<http://modauthkerb.sourceforge.net/configure.html>

* "HTTP/..." is a de-facto standard for Internet Explorer

<http://mailman.mit.edu/pipermail/kerberos/2005-November/008773.html>

Troubleshooting:

1. Sollte beim Test des Keytab-Files nicht „*Authenticated to Kerberos v5*“ erscheinen, sollte das Ereignisprotokoll auf dem AD-Server nach Fehlermeldungen durchsucht werden.

Bei folgender Fehlermeldung sollten beispielsweise zuerst die entsprechenden ServerPrincipalNames aus dem AD gelöscht werden:

```
Ereignistyp: Fehler
Ereignisquelle: KDC
Ereigniskategorie: Keine
Ereigniskennung: 11
Datum: 03.12.2008
Zeit: 10:49:47
Benutzer: Nicht zutreffend
Computer: SDC00103
Beschreibung:
Es sind mehrfache Konten vom Typ DS_USER_PRINCIPAL_NAME mit dem Namen
HTTP/ivm2.hw-intranet.biz@HALLOWELT.LOCAL vorhanden.
```

2. Der Principal Name muss bei der Verwendung des Internet Explorers (also in 99% aller Fälle) immer mit dem Service Name „HTTP“ beginnen!

3. Der HTTP-Fehler 400 Bad Request „Size of a request header field exceeds server limit.“ lässt sich durch den Eintrag LimitRequestFieldSize 16384 im Kontext Serverkonfiguration der httpd.conf lösen.