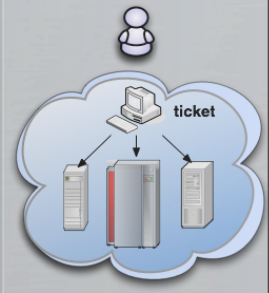
Warp9 IT-Sicherheit und Netzwerkmanagement

Single Sign-On (SSO)



Michael Buth - Warp9 GmbH - Münster

11/27/08

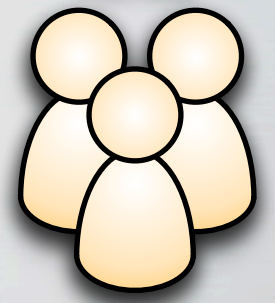
Michael Buth
warp9.de

Single Sign-On (SSO)

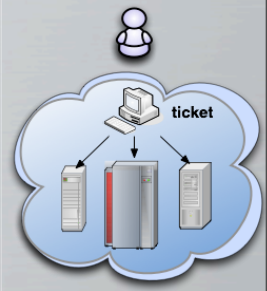
Warp9 GmbH, Münster

Warp9 GmbH

Kunde



Telekommunikationsbranche
Öffentliche Verwaltung
Pharmaindustrie
.....

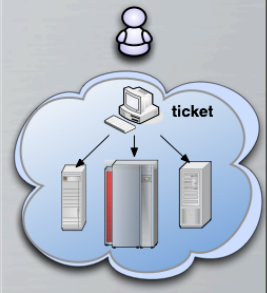


„Das Ganze ist mehr als die Summe seiner

Michael Buth
warp9.de

Definitionen: Single Sign-On (kurz: SSO)

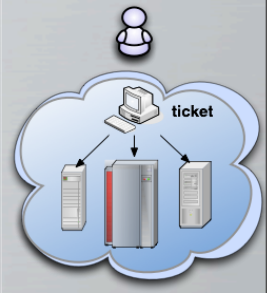
- Single Sign-On: nur einmal Anmelden
  - Jeder Benutzer besitzt immer **genau** eine einzige Identität.
  - SSO bietet einem Benutzer – nach einmaliger Authentifizierung – Zugriff auf alle Dienste, für die er berechtigt ist.
  - Erneute Anmeldungen sind somit hinfällig.



Michael Buth
warp9.de

Ziele: Single Sign-On (kurz: SSO)

- Benutzer identifizieren sich nur mittels eines Authentifizierungsverfahrens.
- Der SSO-Mechanismus übernimmt danach die Aufgabe, den User zu identifizieren.
- Single Sign-On sollte dabei niemals schwächer sein als das Authentifizierungsverfahren selbst.

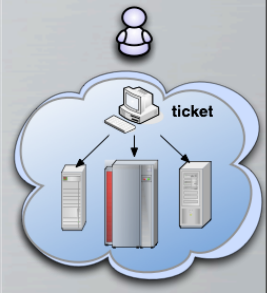


Michael Buth
warp9.de

Single Sign-On (SSO)

Vorteile: Single Sign-On (kurz: SSO)

- **Gewinn an Zeit:**
- Nur eine einzige Authentifizierung ist notwendig, um auf alle Systeme zugreifen zu können.
- Nur ein Benutzerkonto muss beim Entfernen oder Aktualisieren verwaltet werden.
- Kostenreduktion durch bessere Wartbarkeit von Zugangs- und Benutzerdaten

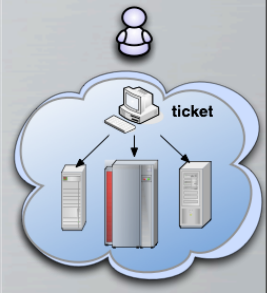


Michael Buth
warp9.de

Single Sign-On (SSO)

Vorteile: Single Sign-On (kurz: SSO)

- **Gewinn an Sicherheit:**
- Passwörter müssen nur einmal übertragen werden.
- Phishing wird erschwert, da UserID und Passwort nur an einer Stelle eingeben werden müssen.
- Benutzer müssen sich nur noch ein sicheres und komplexes Kennwort merken, das regelmäßig geändert werden muss.

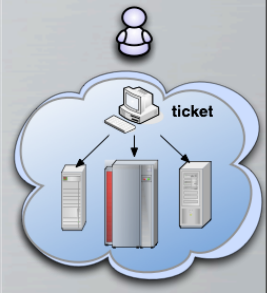


Michael Buth
warp9.de

Single Sign-On (SSO)

Nachteile: Single Sign-On (kurz: SSO)

- **Verlust an Sicherheit:**
- Sollte ein Angreifer an die Identität eines Benutzers gelangen, stehen ihm sofort alle Systeme, auf die dieser Benutzer Zugriff hat, zur Verfügung.
- Ein zentraler Anmeldevorgang kann in Bezug auf Sicherheitsprobleme und Lastverhalten ein Single Point of Failure sein.
- Die Verfügbarkeit von Systemen und Diensten hängt nicht mehr nur von deren eigener Verfügbarkeit ab, sondern auch von der Verfügbarkeit des Single-Sign-on-



Michael Buth
warp9.de

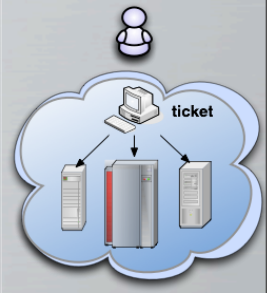
Lösungsansätze: Single Sign-On (kurz: SSO)

1. Portal

- Benutzerauthentifizierung und -autorisierung erfolgen erstmals an einem Portal.
- Bei webbasierten Portalen, kann das z.B. mittels HTTP-Cookies erfolgen.
- Über dieses Portal, das den Benutzer eindeutig ausweißt, erhält er Zugang zu mehreren Webanwendungen.

2. Lokal

- Installation eines Clients auf den Arbeitsplätzen.
- Loginmasken werden damit sofort automatisch mit dem korrekten Usernamen und dem passenden Passwort ausfüllt.
- Benutzernamen und Passwort können z.B. lokal in einer verschlüsselten Datei gespeichert werden.

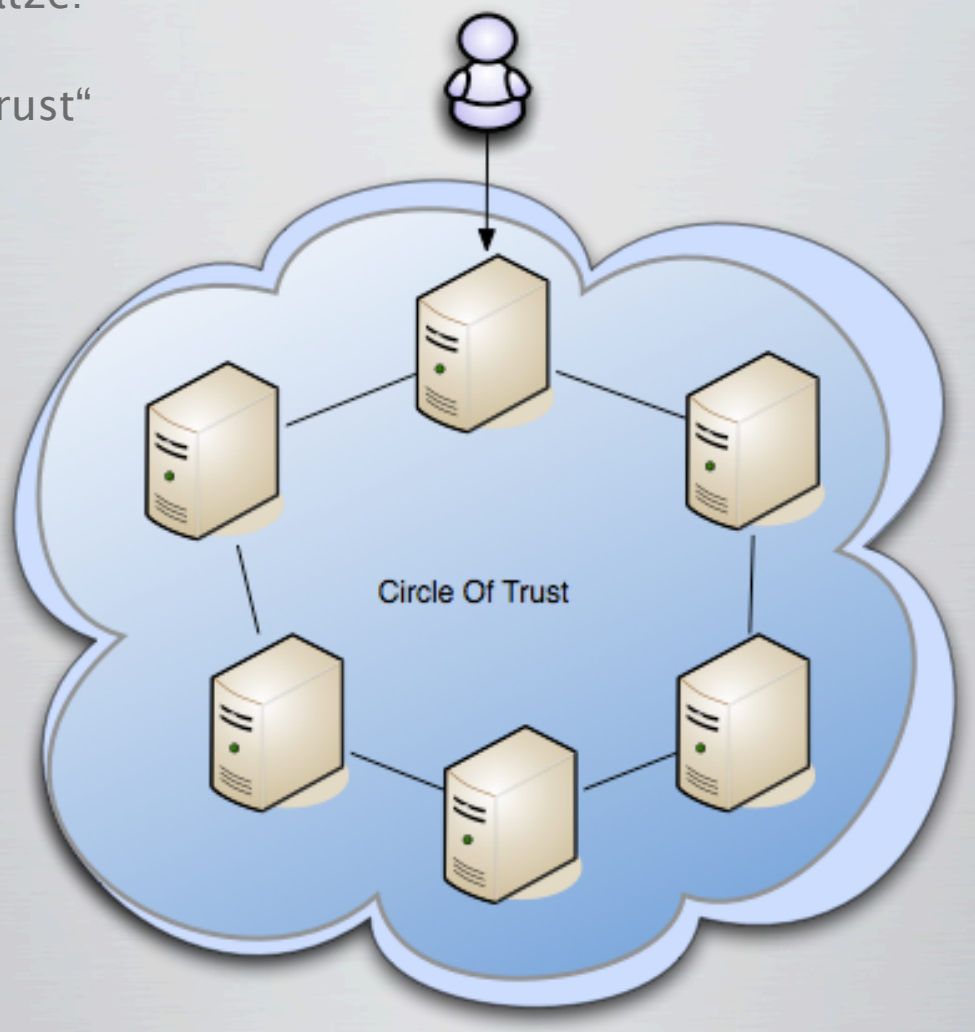


Michael Buth
warp9.de

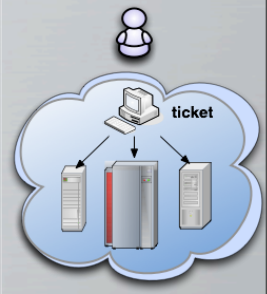
Lösungsansätze: 3. Ticketing System

Zwei Lösungsansätze:

- „Circle of Trust“



Single Sign-On (SSO)



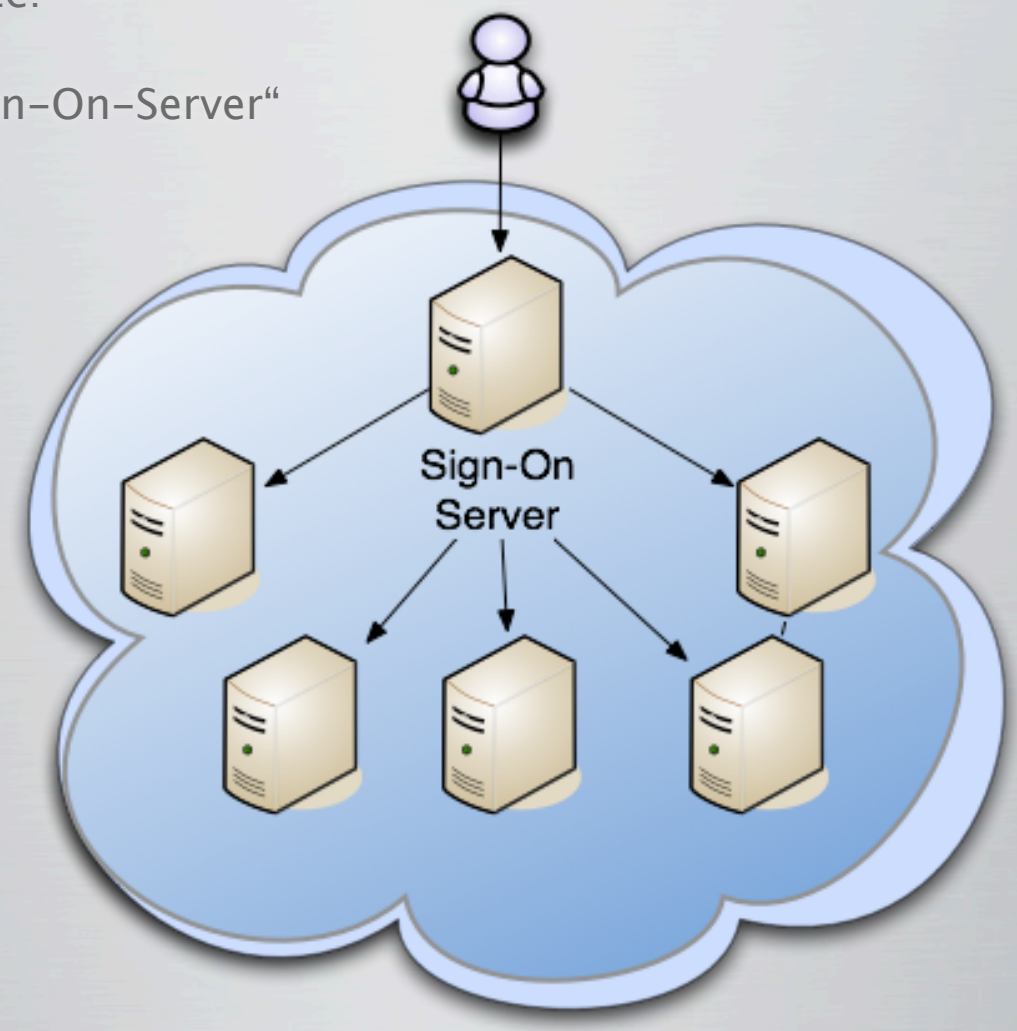
11/27/08

Michael Buth
warp9.de

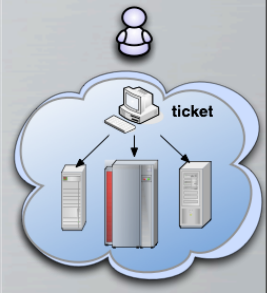
Lösungsansätze: 3. Ticketing System

Zwei Lösungsansätze:

- Zentraler „Sign-On-Server“



Single Sign-On (SSO)



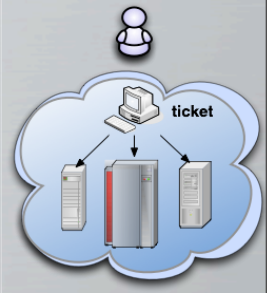
11/27/08

Michael Buth
warp9.de

Single Sign-On (SSO)

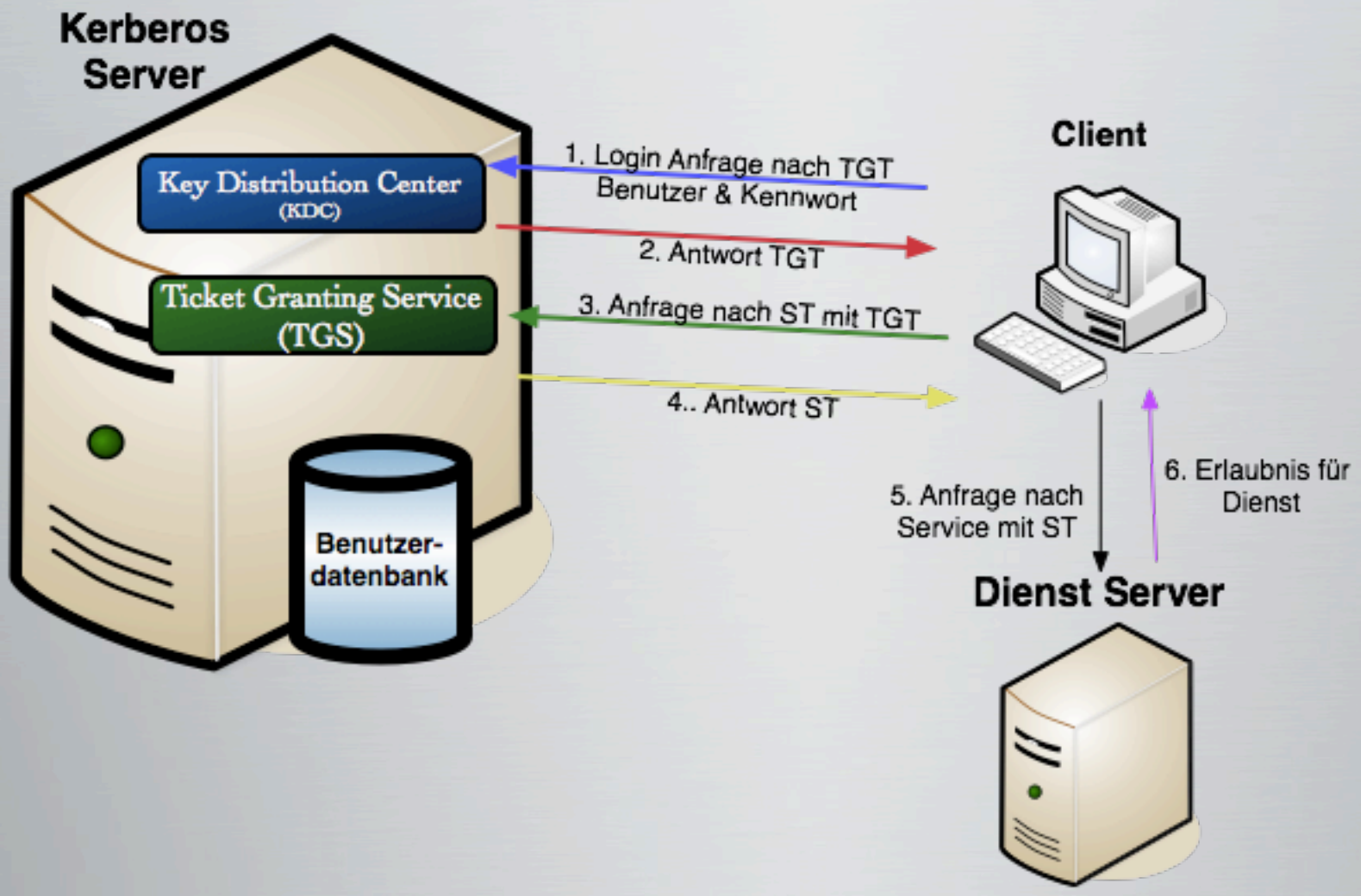
Definition: Kerberos

- Verteilter Authentifizierungsdienst (Netzwerkprotokoll), entwickelt vom Massachusetts Institute of Technology (MIT).
- Aktuelle Version ist Kerberos 5.
  - (definiert in RFC 1510 und RFC 4120)
- Das Verschlüsselungsverfahren verhindert das Abhören oder Verfälschen des Schlüssels oder der Daten.
- Bietet sichere und einheitliche Authentifizierung in einem TCP/IP-Netzwerk.
- Benutzer authentifizieren sich nur einmal beim zentralen Key Distribution Center (KDC), die weitere Authentifizierung gegenüber anderen Diensten erfolgt automatisch ohne Interaktion des Anwenders.

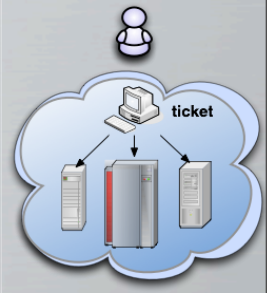


Michael Buth
warp9.de

Architektur: Kerberos



Single Sign-On (SSO)



11/27/08

Michael Buth
warp9.de

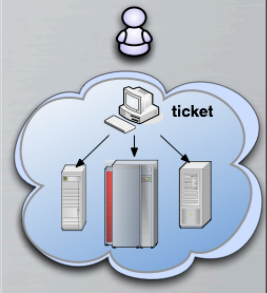
Single Sign-On (SSO)

Vorteile: Kerberos

- Sichere gegenseitige Authentifizierung
- Keine Verbindung zwischen Service und KDC notwendig
- Geringe Belastung des KDC
- Authentifizierung für jeden unterstützten Netzwerkdienst
- Autorisierung wird dem Dienst überlassen
- Plattform- und Systemunabhängig

Nachteile:

- Teilweise fehlende Clientunterstützung (keine kerberized Services)



Michael Buth
warp9.de

Single Sign-On (SSO)

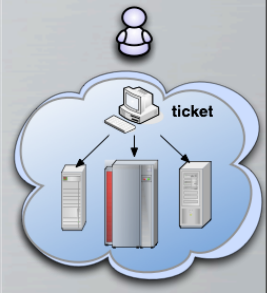
Implementierung: Kerberos

Microsoft:

- Implementierung seit Windows 2000
- Unterstützt nur Kerberos 5
- Unterstützt nur DES und RC4

Linux:

- Unterstützung von (3)DES, AES, RC4
- Weite Verbreitung
- Gute Unterstützung für viele Anwendungen

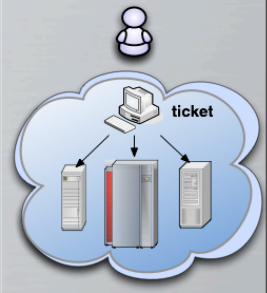


Michael Buth
warp9.de

Single Sign-On (SSO)

Problemstellung: Kerberos

- Rahmenbedingungen:
  - Active Directory
  - (S)NTP
  - (D)DNS
  - Kerberos 5
  - Samba 3
  - Squid 2.5 / 2.6
  - Apache 2

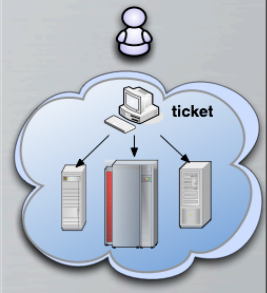


Michael Buth
warp9.de

Single Sign-On (SSO)

Problemstellung: Testscenario

- Ist-Zustand:
  - Netzwerkdienste befinden sich in einer heterogenen Umgebung.
  - Authentifizierung muss jeweils für jeden einzelnen Netzwerkdienst erfolgen.
  - Ablage der Benutzerdaten auf jedem der Dienstserver.
  - Dienste z. T. mit unverschlüsselter Übertragung von Benutzerdaten

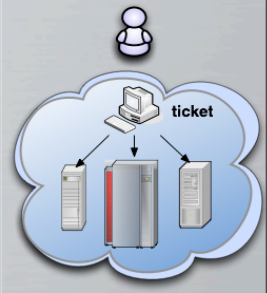


Michael Buth
warp9.de

Problemstellung: Testscenario

Single Sign-On (SSO)

- Soll-Zustand:
  - SSO
  - Zentrale Benutzerverwaltung (Active Directory)
  - Nur verschlüsselte Übertragung von Benutzerdaten.



11/27/08

Michael Buth
warp9.de

Konfiguration: Linux System

Systemzeit Synchronisation:

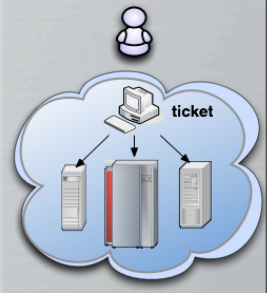
/etc/ntp.conf

```
server 0.W2K3-SSO.transwarp.intern
server 1.ptbtime1.ptb.de
server 2.ptbtime2.ptb.de

restrict 0.W2K3-SSO.transwarp.intern mask
    255.255.255.255 nomodify notrap noquery

restrict 1.ptbtime1.ptb.de mask 255.255.255.255
    nomodify notrap noquery

restrict 2.ptbtime2.ptb.de mask 255.255.255.255
    nomodify notrap noquery
```



Michael Buth
warp9.de

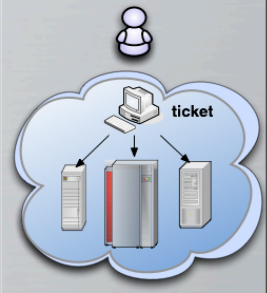
Konfiguration: Linux System

Samba Konfiguration: /etc/samba/smb.conf

```
[global]

workgroup = TRANSWARP
netbios name = Linux-SSO
realm = TRANSWARP.INTERN
security = ADS
encrypt passwords = yes
server string = Linux Samba Server
password server = W2K3-SSO
local master = no
os level = 17
preferred master = no
domain logons = no
idmap uid = 16777216-33554431
idmap gid = 16777216-33554431
template shell = /bin/false
winbind use default domain = yes
```

Single Sign-On (SSO)



11/27/08

Michael Buth
warp9.de

Single Sign-On (SSO)

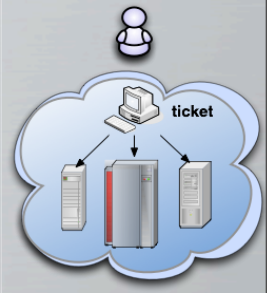
Konfiguration: Linux System

Windows Domain Controller in die Datei **/etc/krb5.conf** eintragen:

```
 [libdefaults]
default_realm = TRANSWARP.INTERN
dns_lookup_realm = false
dns_lookup_kdc = false

[realms]
TRANSWARP.INTERN = {
        kdc = W2K3-SSO:88
        admin_server = W2K3-SSO:749
        default_domain = TRANSWARP.INTERN
}

[domain_realm]
.transwarp.intern = TRANSWARP.INTERN
transwarp.intern = TRANSWARP.INTERN
```



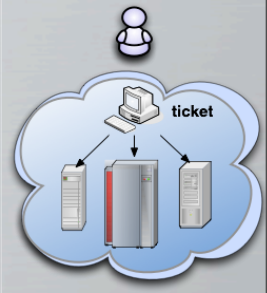
Michael Buth
warp9.de

Single Sign-On (SSO)

Konfiguration: Squid Proxy Linux System

- Der Squid Dienst selbst ist nicht kerberized. Er greift mittels NTLM auf Samba zu und erst Samba realisiert die Anbindung an das Active Directory mittels Winbind und Kerberos.

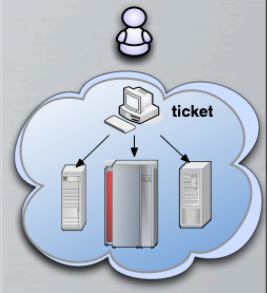
- **NTLM**
  - NTLM (NT LAN Manager) ist ein Authentifizierungsschema.
  - NTLM ist ein proprietärer Microsoft Standard.
  - Samba, Squid, Mozilla Firefox, cURL, Opera, Apache Web Server etc. unterstützen NTLM.



Michael Buth
warp9.de

Konfiguration: Squid Proxy Linux System

- **Winbind**
  - ist ein Bestandteil der Samba-Suite
  - einheitlichen Anmeldung
  - UNIX-Implementierung der Microsoft RPC-Aufrufe
  - Übernimmt die Authentifizierung der Benutzerbeglaubigung
  - Übernimmt die Auflösung der Identität



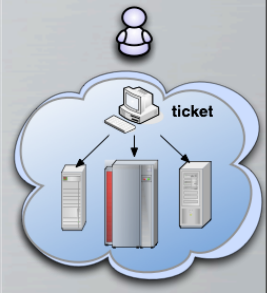
Michael Buth
warp9.de

Konfiguration: Squid Proxy Linux System

Single Sign-On (SSO)

/etc/squid/squid.conf:

```
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 30
# auth_param ntlm max_challenge_reuses 0
# auth_param ntlm max_challenge_lifetime 2 minutes
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
auth_param basic children 5
auth_param basic realm Squid AD
auth_param basic credentialsttl 2 hours
```



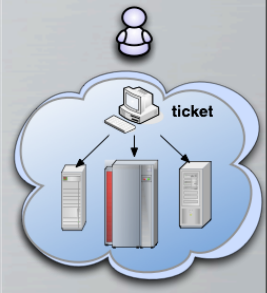
Michael Buth
warp9.de

Konfiguration: Squid Proxy Linux System

/etc/squid/squid.conf:

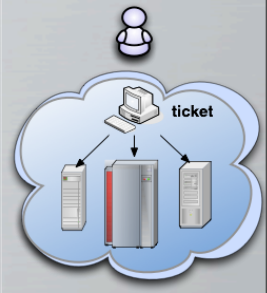
ACLs:

```
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl to_localhost dst 127.0.0.0/8
acl SSL_ports port 443 563
acl password proxy_auth REQUIRED
http_access allow manager localhost
http_access deny manager
http_access allow password
```



Michael Buth
warp9.de

Single Sign-On (SSO)



Konfiguration: Squid Proxy Linux System

Praxisbeispiel:

Das Surfen soll nur für bestimme Gruppen im Active Directory erlaubt werden:

```
auth_param ntlm program /usr/bin/ntlm_auth
  --helper-protocol=squid-2.5-ntlmssp --
  require-membership-of=TRANSWARP\
  \INTERNET

auth_param basic program /usr/bin/
  ntlm_auth --helper-protocol=squid-2.5-
  basic --require-membership-
  of=TRANSWARP\\INTERNET
```

11/27/08

Michael Buth
warp9.de

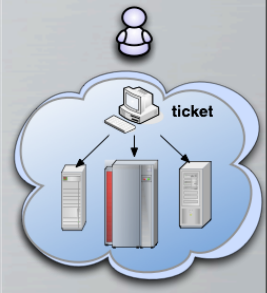
Single Sign-On (SSO)

Konfiguration: Squid Proxy Linux System

/etc/squid/squid.conf:

Weitere Log Parameter:

- log_fqdn on
  - Full Qualified Domain Name werden anstelle von IP Adressen in der Logdatei angezeigt.
- emulate_httpd_log on
  - Datum im Standardformat



Michael Buth
warp9.de

Single Sign-On (SSO)

Konfiguration: Squid Proxy Linux System

- **Linux-SSO zum AD hinzufügen:**

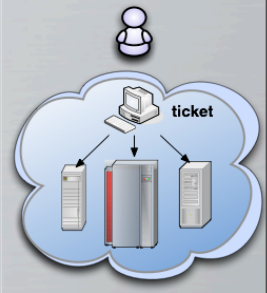
```
[root@linux-sso ~]# net ads join -U Administrator
Administrator's password:
Using short domain name -- TRANSWARP
Joined 'LINUX-SSO' to realm 'TRANSWARP.INTERN'
```

- **Die betroffenen Dienste starten:**

```
[root@linux-sso ~]# service winbind restart
[root@linux-sso ~]# chkconfig winbind on
[root@linux-sso ~]# chkconfig squid on
```

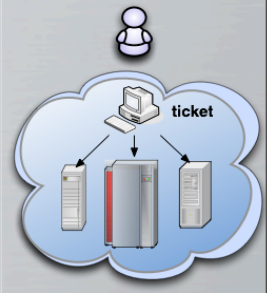
- **Änderung der Squid Berechtigung für NTLM:**

```
[root@linux-sso ~]# chgrp squid /var/cache/samba/winbindd_privileged/
```



Michael Buth
warp9.de

Single Sign-On (SSO)



Konfiguration: Squid Proxy Linux System

- **Überprüfung der NTLM Authentification:**

```
[root@linux-sso ~]# /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
```

user password

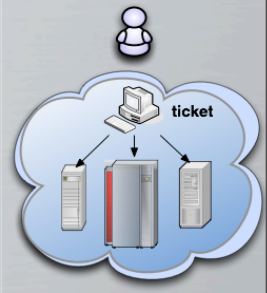
- **Squid Neustart:**

```
[root@linux-sso ~]# service squid restart
```

11/27/08

Michael Buth
warp9.de

Single Sign-On (SSO)

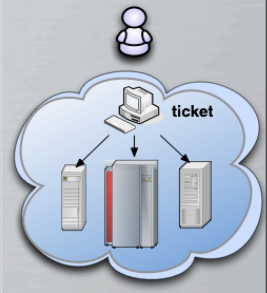


Konfiguration: Apache Linux System

- Der Schlüssel zur Kerberos Authentisierung ist das Modul **mod_auth_kerb**. Dieses Modul erlaubt es dem Benutzer, sich transparent mittels Browser zu authentifizieren, ohne dass eine weitere Kennworteingabe verlangt wird.
- Anlegen eines Benutzeraccounts für den Apache-Server
- Für jeden im AD angelegten Apache Account, muss nun mittels des **ktpass.Exe-Befehls** auf dem AD Controller

Michael Buth
warp9.de

Single Sign-On (SSO)



Konfiguration: Windows Server 2003 AD

- Benutzer für Apache im AD anlegen. Das Kennwort für diesen Account darf niemals ablaufen!
- Active Directory: (ktpass.exe / Support Tools)
- Service Key erzeugen:
  - c:\Programme\Support Tools>ktpass -princ HTTP/linux-sso.transwarp.intern@TRANSWARP.INTERN -mapuser TRANSWARP\apache -crypto DES-CBC-MD5 +DesOnly -pass test -ptype KRB5_NT_PRINCIPAL -out c:\temp\linux-sso.keytab
- Die erzeugte Service Key Datei muss nun z.B. mittels winscp auf Apache Server in das Verzeichnis /etc/httpd/conf kopiert werden.

Michael Buth
warp9.de

Single Sign-On (SSO)

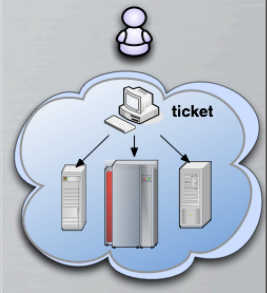
Konfiguration: Apache Linux System

- Kerberos Modul für Apache Webserver installieren:
  - [root@linux-sso ~]# yum install mod_auth_kerb

- **/etc/httpd/conf/httpd.conf**

```
LoadModule auth_kerb_module modules/
    mod_auth_kerb.so

<Location />
  AuthType Kerberos
  AuthName "Kerberos Login"
  KrbMethodNegotiate On
  KrbMethodK5Passwd On
  KrbAuthRealms TRANSWARP.INTERN
  Krb5KeyTab /etc/httpd/conf/linux-sso.keytab
  require valid-user
</Location>
```



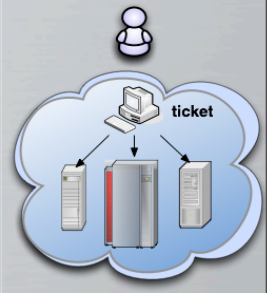
11/27/08

Michael Buth
warp9.de

Single Sign-On (SSO)

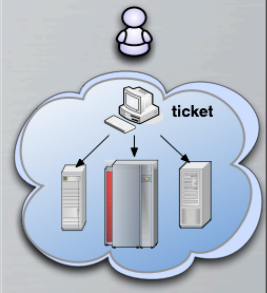
Weitere „kerberized“ Services:

- OpenLDAP
- Cyrus IMAP
- SSH
- Putty
- Telnet
- Apple Mail.app
- ...

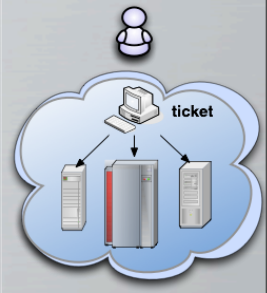


Michael Buth
warp9.de

Single Sign-On (SSO)



Vielen Dank für Ihre Aufmerksamkeit!



Impressum

Haftungshinweis:

Alle Warennamen werden ohne Gewährleistung der freien Verwendbarkeit benutzt und sind möglicherweise eingetragene Warenzeichen. Die Firma Warp9 GmbH richtet sich im Wesentlichen nach der Schreibweise der Hersteller. Andere hier genannte Produkte können Warenzeichen des jeweiligen Herstellers sein.

Warp9® und **Transwarp®** sind eingetragene Warenzeichen der Warp9 GmbH.

Warp9 GmbH, Scheibenstraße 109, 48153 Münster

Phone: +49 251 973 190 Fax: +49 251 973 192 9

E-Mail: kontakt@warp9.de Internet: http://warp9.de