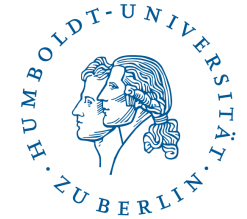


IT-Workshop des CMS am 20.04.2015

Anschluss an CMS-Dienste

Winfried Naumann, ZE CMS

Agenda



- Bestandsaufnahme:
Installationen + Anforderungen der Einrichtungen
- Dienste des CMS und deren Anforderungen
- Technische Möglichkeiten der Anbindung
an CMS-Dienste
- Der nächste Schritt.. ?

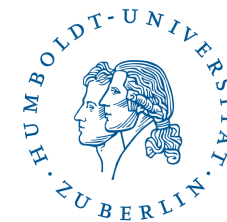
Bestandsaufnahme:

Installationen in den Einrichtungen



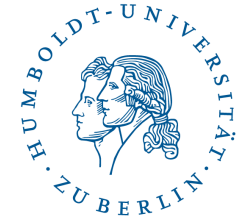
- eigene Filedienste (Samba, Windows)
- eigene Benutzerverwaltung – eigene Accounts
- DNS-Server
- Mail-Server
- Web-Server, Wikis, Blogs, Groupware, Virtualisierungs-Hosts, ownCloud, ..

Warum eigene Dienste? (1)



- historisch gewachsen:
 - in der Aufbruchstimmung nach der Wende
 - als Alternative zu Banyan VINES ,
später als Alternative zu Windows-Servern
 - eigene Benutzerverwaltung (durch eigene Dienste)
 - Windows- u.a. Filedienste im CMS erst ab 2003
 - Unix-Wissen der Admins, Unix-/Linux-Umgebung
 - Open Source (kostenlos)

Warum eigene Dienste? (2)



- historisch gewachsen (Fortsetz.):
 - zentrale Accountverwaltung im CMS erst ab 2003
- eigene Dienste sind flexibler
 - schneller anzupassen
 - Betrieb nach eigenen Regeln

Probleme (1)



- CMS-Dienste können mit eigenen Accounts nicht benutzt werden (v.a. die, die mit dem Active Directory authentifizieren)
 - öffentliche Computer-Arbeitsplätze (ÖCAP) in den Bibliotheken
 - der Dienst „Software as a Service“ (SaaS)
 - Filedienste anderer Einrichtungen im HU-Windows-Netz (interdisziplinäre Zusammenarbeit)

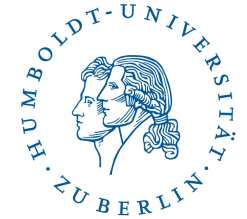
Bestandsaufnahme:

Probleme (2)



- Schwierigkeiten der Benutzer mit mehreren Accounts
- der Aufwand mit eigener Benutzerverwaltung, v.a. Zugriffsrechte für Studierende für eigene Dienste
- Probleme mit dem Betrieb der eigenen Dienste

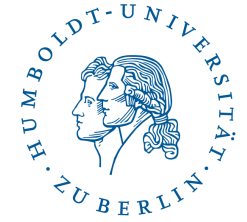
Anforderungen (1)



- sichere, stabile, schnelle Dienste
- einfache Administration dieser Dienste
- flexible, einfache, kurzfristige Anpassung der Nutzung an die Anforderungen der Einrichtung
- Nutzung der eigenen Dienste mit (zentralen) HU-Accounts und eigenen Accounts
- eigene Accounts notwendig:
für Gäste, Veranstaltungen, ..

Bestandsaufnahme:

Anforderungen (2)



- Anbindung von Linux- und Windows-Clients
- eigene E-Mail-Accounts (-Adressen)

Ergänzungen?

Korrekturen?

Diskussions-Pause!

Dienste des CMS (1)



von Accounts im Active Directory abhängig:

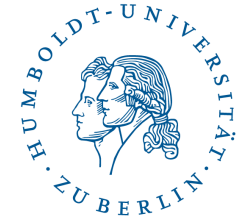
- öffentliche Computer-Arbeitsplätze (ÖCAP)
v.a. in den Bibliotheken
- „Software as a Service“ (SaaS)
- Filedienste im HU-Windows-Netz
- Webfiles (mobiler Zugang zu Filediensten)
- Terminal Services im HU-Windows-Netz

Dienste des CMS (2)



- weitere Dienste werden über LDAP authentifiziert
- einige Einrichtungen pflegen einen eigenen Zweig im zentralen LDAP

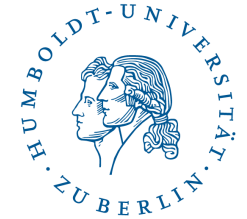
Dienste des CMS (3)



Vorteile

- Ausfallsicherheit (mehrere Standorte)
- Klimatisierung
- Skalierung
- Personal (Vertretung, Spezial-Wissen, Weiterbildung)

Accounts im Active Directory (1)



Zwei Möglichkeiten für Benutzer von Einrichtungen außerhalb des HU-Windows-Netzes:

1. Account in einer OU der Domäne user.hu-berlin.de
 - begrenzt auf 5 Accounts pro Einrichtung
 - noch mehr Accounts: müssen selbst administriert werden
 - geplant: Selbstbedienung über eine Webseite

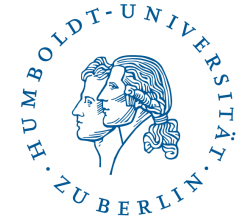
Accounts im Active Directory (2)



2. Aleph-Account der Unibibliothek

- erzeugt nach erstmaliger Passwort-Änderung automatisch einen Account in der User-Domäne

Accounts im Active Directory (3)



- nur ein Home-Verzeichnis, keine weiteren Leistungen
- Support durch die Benutzerberatung, nicht durch wintech
- für Beschäftigte damit Zugang zu ÖCAP und SaaS
- weitere Dienstleistungen würden Support durch die Einrichtung erfordern ..

Technische Möglichkeiten

für die Anbindung an CMS-Dienste



(alle Komponenten stehen unter Open-Source-Lizenz)

- sssd
- Samba + LDAP
- Samba + winbind
- Samba + sssd
- FreeIPA
- ...

sssd (1)



- System Security Services Daemon
- aus dem FreeIPA-Projekt (Red Hat)
- direkte Integration von Linux-Systemen
- außer einem Directory Service sind keine zusätzlichen Komponenten nötig
- Anbindung an FreeIPA oder Active Directory möglich

sssd (2)



- in Distributionen teilweise sehr alte Versionen
- besteht aus dem Daemon sssd, Providern für verschiedene Datenquellen und Modulen für NSS und PAM
- eigener Cache
- kann dadurch Benutzer auch offline authentifizieren (mobile Geräte!)

sssd (3)



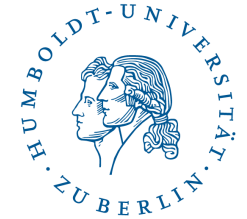
- Integration in mehrere Domänen möglich
- Unterstützung verschiedener Sicherheits-Mechanismen (StartTLS, LDAPS, SASL/GSSAPI (im Windows-Umfeld))
- für Integration ins Active Directory:
LDAP-Provider (sssd-ldap) und Kerberos-Provider (sssd-krb5) bzw. AD-Provider (sssd-ad)

sssd (4)



- sssd-ad:
ID-Mapping für die schnelle Integration,
Linux-IDs werden aus der Windows-SID generiert
- Nachteile:
für Anmeldeberechtigungen über Gruppen muss für
den LDAP-Provider noch einmal alles konfiguriert
werden, was im AD-Provider schon enthalten ist
(aufwendig, umständlich)

Samba (1)



- CIFS- (und Druck-)Server
- als File Server und Anmeldeserver (Domain Controller) integriert er sich gut in Unix-/Linux-Umgebungen
 - integriert die Windows-Clients
 - erspart Lizenzkosten und Windows-Administration
- kann Windows-Server (z.T.) vollständig ersetzen

Samba (2)



- Samba 3 (2003):
Windows-NT4-kompatibler Domain Controller
- Samba 4 (2012):
Active Directory-kompatibler Domain Controller
(ab Windows 2000)

Samba (3)

- aktuelle stabile Version: 4.2.1
- Release-Zweig 3.x:
kein Support mehr seit 04.03.2015 !
- Release-Zweig 4.0.x:
nur noch mit Sicherheits-Updates versorgt,
letztes Release 4.0.26 steht unmittelbar bevor !
- für jeden Release-Zweig:
9 Monate Full Support + 9 Monate Maintenance,
+ 9 Monate Security Fixes only

Samba (4)



- siehe „Samba Release Planning“
https://wiki.samba.org/index.php/Samba_Release_Planning
- die Versionen sind wichtig für die Kompatibilität zu Active Directory und die Funktionen und Sicherheits-Einstellungen der neuen Windows-Versionen (!)

Samba 4 (1)

- deutlich bessere Unterstützung der aktuellen Windows-(Client-)Versionen 7 und 8.1 und -Server-Versionen bis Windows 2012 R2 (Sicherheit, Geschwindigkeit, Kommunikation)
- SMB 3.0
- integrierter oder externer DNS-Server (bind 9)
- Kerberos-Server (KDC)

Samba 4 (2)



- eigene Registry, kann die smb.conf ersetzen
- für die Administration auf der Kommandozeile: samba-tool
- Administration mit Windows-Werkzeugen möglich bzw. teilweise sogar empfehlenswert
- DFS-Unterstützung, Gruppenrichtlinien

Samba 4 (3)



- noch keine Dateisystem-Replikation; die ist aber wichtig für das SYSVOL-Share (Richtlinien, Logon-Skripte), kann z.B. mit rsync realisiert werden;
- noch keine Multidomain-Unterstützung, nur alleinstehende Samba-Domänen, d.h. noch keine Integration in einen Forest wie das HU-Windows-Netz möglich

Samba 4 (4)

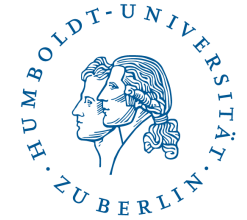


- in den Distributionen sind teilweise veraltete Samba-Pakete enthalten
- empfehlenswert:
Verwendung der Packages von SerNet
unter <http://enterprisesamba.com/>
(für Debian 7, Red Hat und SuSE Enterprise)

Samba + winbind

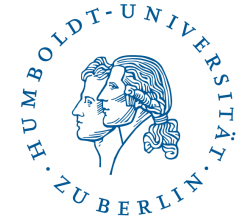
- winbind ist im Samba-Paket enthalten
- konfigurierbar, aus welcher Domäne Benutzer sich anmelden dürfen
- einfache Integration eines Samba File Servers in eine Domäne
- kein Cache, kein Offline-Authentifizierung

FreeIPA (1)



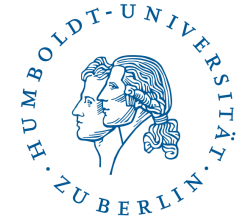
- vereint mehrere Open-Source-Komponenten unter einem Dach:
 - Kerberos-Server (MIT)
 - DNS (Bind 9), externer DNS möglich
 - LDAP-Server (389-DS aus dem Fedora-Projekt)
 - NTP-Server (ISC)
 - Zertifikatssystem (dogtag)

FreeIPA (2)



- Replicas möglich (Ausfallsicherheit)
- 2 native Programme für Linux-Clients:
 - System Security Services Daemon (sssd)
 - certmonger (für das Zertifikats-Management)

FreeIPA (3)



- 2 Varianten für die Anbindung an das AD:
 - Replikation der Objekte aus dem AD in den FreeIPA-Directory Server
 - Vertrauensstellung zwischen AD und FreeIPA-Domäne

Anbindung an das Active Directory



aktuelle Beispiele im HU-Netz:

- nur für die Nutzung von ÖCAP und SaaS:
eigene OU (*Mathematik*)
- Verwaltung der Accounts des Samba-File Servers:
eigene OU (*Chemie*)
- Windows-Filedienste und Samba File Server:
eigene Domäne bzw. eigene OU (*Psychologie u.a*)

Der nächste Schritt .. ?



- Beratungen in den Einrichtungen?
(genaue Bestandsaufnahme, eigene Vorhaben)
- Planung eines Lehrgangs?

Danke für Ihre Aufmerksamkeit!

*Weitere Fragen bitte an
w.naumann@cms.hu-berlin.de*

Quellen: sssd (1)



- Projekt:
SSSD - System Security Services Daemon
- Mark Pröhl, Fremde Welten. Mit Linux via SSSD ins Active Directory
iX Kompakt 3/2014 – Administration (Heise Zeitschriften Verlag)
- Sumit Bose,
ID Mapping of Active Directory users with sssd (.pdf),
auch als Audio-Datei (.mp3)
Vortrag auf der Konferenz SambaXP, Göttingen 2014

Quellen: sssd (2)

- Jakub Hrozek, The SSSD Active Directory provider
Teil 1, Teil 2
- Samba-Wiki:
Local user management and authentication/sssds
- ubuntu Wiki: [sssds](#)
- sssds versus winbind
Kap. 7.4 in: S. Kania, Samba 4
(siehe auch unter Quellen zu Samba 4)

Quellen: FreeIPA (1)



- Projekt:
http://www.freeipa.org/page/Main_Page
- Thorsten Scherf, Identity-Management mit FreeIPA
Vortrag auf der 7. SLAC 2104
- Alexander Bokovoy,
Trusting Active Directory with FreeIPA: a story beyond Samba
auch als [Audio-Datei \(.mp3\)](#)
Vortrag auf der Konferenz SambaXP, Göttingen 2014

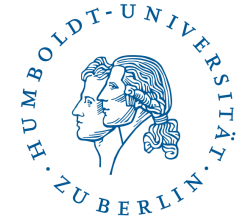
Quellen: FreeIPA (2)



- Thorsten Scherf,
 - Einlasskontrolle. Einführung in das freie Identity-Management-Framework (FreeIPA-Tutorial I)
 - Viele Köpfe. Client-Setup und Policy-Management (FreeIPA-Tutorial II)
 - Verschiedene Ansichten. Linux- und Windows-Welt verbinden (FreeIPA-Tutorial III)

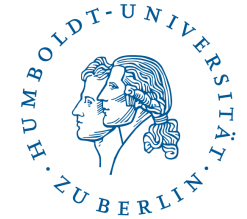
iX Kompakt 3/2014 – Administration (Heise Zeitschriften Verlag)

Quellen: FreeIPA (3)



- Thomas Drilling, [Zusammengeschweißt](#). Active Directory mit freier Software
in: [ADMIN-Magazin 01/2014](#), S. 52 ff.
- Thorsten Scherf, [Gemeinsame Sache](#) Workshop: Linux-Systeme in Active Directory-Domänen integrieren
in: [IT Administrator 07/2014](#), S. 42 ff.

Quellen: Samba (1)



- Samba Projekt
<https://www.samba.org/>
- Samba Release Planning
https://wiki.samba.org/index.php/Samba_Release_Planning
- Samba News
- Samba Release History
- Samba Security Releases
- Samba Features added/changed (by release)
- Roadmap

Quellen: Samba (2)



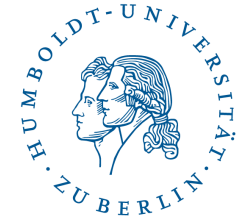
- Samba-Wiki: <https://wiki.samba.org/>
- User Documentation:
https://wiki.samba.org/index.php/User_Documentation
- Presentations
<https://wiki.samba.org/index.php/Presentations>
- Download Samba:
<https://www.samba.org/samba/download/>
- Samba on Enterprise Linux:
u.a. mit den Samba4-Paketen von SerNet
<http://enterprisesamba.com/>

Quellen: Samba (3)



- Michael Adam,
Present And Future File Serving With Samba (Oktober 2014)

Quellen: Samba 4



- Stefan Kania,
[Samba 4. Das Praxisbuch für Administratoren](#) (mit E-Book)
Bonn: Rheinwerkverlag GmbH 2014
- Volker Lendecke, [Samba 4.2](#)
Vortrag auf dem [GUUG-Frühjahrsfachgespräch](#), März 2015