Einbinden einer Kerberos-Umgebung in openLDAP

Stefan Kania

6. Juni 2013

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Kerberos? openLDAP? Fragen über Fragen

- Warum Kerberos?
- Warum openLDAP?
- Warum Kerberos in openLDAP integrieren?
- Wie muss der openLDAP-Server vorbereitet werden?
- Wie wird die Kerberos-Datenbank umgewandelt?
- Wie wird Kerberos in den openLDAP eingebunden?
- Wie können die Daten einfach verwaltet werden?
- Und wie geht das Ganze in der Praxis?

Vorteile von Kerberos

- zentrale Verwaltung der Passwörter
- Replikation zur Ausfallsicherheit möglich
- von vielen Diensten nutzbar
- Einrichtung von single-sign-on

Vorteile von Kerberos

- zentrale Verwaltung der Passwörter
- Replikation zur Ausfallsicherheit möglich
- von vielen Diensten nutzbar
- Einrichtung von single-sign-on

Vorteile von Kerberos

- zentrale Verwaltung der Passwörter
- Replikation zur Ausfallsicherheit möglich
- von vielen Diensten nutzbar
- Einrichtung von single-sign-on

Vorteile von Kerberos

- zentrale Verwaltung der Passwörter
- Replikation zur Ausfallsicherheit möglich
- von vielen Diensten nutzbar
- Einrichtung von single-sign-on

Nachteile von Kerberos

- eine zusätzliche Datenbank
- komplizierte Verwaltung
- zusätzlicher administrativer Aufwand
- Zeitkritisch

Nachteile von Kerberos

- eine zusätzliche Datenbank
- komplizierte Verwaltung
- zusätzlicher administrativer Aufwand
- Zeitkritisch

Nachteile von Kerberos

- eine zusätzliche Datenbank
- komplizierte Verwaltung
- zusätzlicher administrativer Aufwand
- Zeitkritisch

Nachteile von Kerberos

- eine zusätzliche Datenbank
- komplizierte Verwaltung
- zusätzlicher administrativer Aufwand
- Zeitkritisch

Kerberos unter Kontrolle bringen

- /etc/krb5.conf für den Client
- /etc/krb5kdc/kdc.conf für den Server
- /etc/krb5kdc/kadm5.acl für die Zugriffsrechte
- /var/lib/krb5kdc/prinicipal die Datenbank

Kerberos unter Kontrolle bringen

- /etc/krb5.conf für den Client
- /etc/krb5kdc/kdc.conf für den Server
- /etc/krb5kdc/kadm5.acl für die Zugriffsrechte
- /var/lib/krb5kdc/prinicipal die Datenbank

Kerberos unter Kontrolle bringen

- /etc/krb5.conf für den Client
- /etc/krb5kdc/kdc.conf für den Server
- /etc/krb5kdc/kadm5.acl für die Zugriffsrechte
- /var/lib/krb5kdc/prinicipal die Datenbank

Kerberos unter Kontrolle bringen

- /etc/krb5.conf für den Client
- /etc/krb5kdc/kdc.conf für den Server
- /etc/krb5kdc/kadm5.acl für die Zugriffsrechte
- /var/lib/krb5kdc/prinicipal die Datenbank

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Aufgaben von openLDAP

- zentrale Ressourcenverwaltung
- zentrale Gruppen und Benutzerverwaltung
- speichern der Anmeldedaten der Benutzer
- Ausfallsicherheit der Authentifikation durch Replikation
- Viele Dienste können LDAP zur Authentifikation nutzen
- Vereinfachung der Anmeldung der Benutzer

Konfigurationsdateien von openLDAP

- /etc/ldap/ldap.conf für den Client
- /etc/ldap/slapd.conf für den Server
- das Verzeichnis /var/lib/ldap für die Datenbanken

Konfigurationsdateien von openLDAP

- /etc/ldap/ldap.conf für den Client
- /etc/ldap/slapd.conf für den Server
- das Verzeichnis /var/lib/ldap für die Datenbanken

Konfigurationsdateien von openLDAP

- /etc/ldap/ldap.conf für den Client
- /etc/ldap/slapd.conf für den Server
- das Verzeichnis /var/lib/ldap für die Datenbanken

Gemeinsam sind sie stark

- Alle Datenbanken werden zusammengefasst
- Nur noch eine Replikation des openLDAP nötig
- Verwaltung aller Benutzerdaten über grafische Tools
- Zentrale Sicherung aller Daten

Gemeinsam sind sie stark

- Alle Datenbanken werden zusammengefasst
- Nur noch eine Replikation des openLDAP nötig
- Verwaltung aller Benutzerdaten über grafische Tools
- Zentrale Sicherung aller Daten

Gemeinsam sind sie stark

- Alle Datenbanken werden zusammengefasst
- Nur noch eine Replikation des openLDAP nötig
- Verwaltung aller Benutzerdaten über grafische Tools
- Zentrale Sicherung aller Daten

Gemeinsam sind sie stark

- Alle Datenbanken werden zusammengefasst
- Nur noch eine Replikation des openLDAP nötig
- Verwaltung aller Benutzerdaten über grafische Tools
- Zentrale Sicherung aller Daten

Immer wieder diese Schemata

- Schema für Kerberos in slapd.conf eintragen
- ```
  # Schema and objectClass definitions
  include  /etc/ldap/schema/core.schema
  include  /etc/ldap/schema/cosine.schema
  include  /etc/ldap/schema/nis.schema
  include  /etc/ldap/schema/inetorgperson.schema
  include  /etc/ldap/schema/kerberos.schema
  ```
  ```

Immer wieder diese Schemata

- Schema für Kerberos in slapd.conf eintragen
- ```
  # Schema and objectClass definitions
  include  /etc/ldap/schema/core.schema
  include  /etc/ldap/schema/cosine.schema
  include  /etc/ldap/schema/nis.schema
  include  /etc/ldap/schema/inetorgperson.schema
  include  /etc/ldap/schema/kerberos.schema
  ```
  ```

Jetzt auch noch ACLs

- ACLs für Kerberos in slapd.conf eintragen
  - `limits dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `limits dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `access to dn.sub="ou=users,dc=example,dc=net" by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write by * break`
  - `access to dn.sub="ou=kerberos ,dc=example,dc=net" by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write by * break`

Jetzt auch noch ACLs

- ACLs für Kerberos in slapd.conf eintragen
  - `limits dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `limits dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - ```
    access to dn.sub="ou=users,dc=example,dc=net"
        by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write
        by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write
        by * break
    ```
  - ```
    access to dn.sub="ou=kerberos ,dc=example,dc=net"
        by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write
        by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write
        by * break
    ```

Jetzt auch noch ACLs

- ACLs für Kerberos in slapd.conf eintragen
  - `limits dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `limits dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `access to dn.sub="ou=users,dc=example,dc=net" by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write by * break`
  - `access to dn.sub="ou=kerberos,dc=example,dc=net" by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write by * break`

Jetzt auch noch ACLs

- ACLs für Kerberos in slapd.conf eintragen
  - `limits dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - `limits dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" size=unlimited time=unlimited`
  - ```
    access to dn.sub="ou=users,dc=example,dc=net"
        by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write
        by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write
        by * break
    ```
  - ```
    access to dn.sub="ou=kerberos ,dc=example,dc=net"
        by dn.exact="cn=kdc,ou=kerberos,dc=example,dc=net" write
        by dn.exact="cn=kadmin,ou=kerberos,dc=example,dc=net" write
        by * break
    ```

Endlich die benötigten Objekte

- LDIF-Datei für die benötigten Objekte
  - dn: ou=kerberos,dc=example,dc=net
    ou: kerberos
    objectClass: organizationalUnit
    objectClass: top
  - dn: cn=kdc,ou=kerberos,dc=example,dc=net
    cn: kdc
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}2vOrDsINZTpwNhj9wUrhiqBCvpTAQi02
  - dn: cn=kadmin,ou=kerberos,dc=example,dc=net
    cn: kadmin
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}9Xpeg17kacCnHQe5JiVEsUpTH2VYlFnq

Endlich die benötigten Objekte

- LDIF-Datei für die benötigten Objekte
  - dn: ou=kerberos,dc=example,dc=net
    ou: kerberos
    objectClass: organizationalUnit
    objectClass: top
  - dn: cn=kdc,ou=kerberos,dc=example,dc=net
    cn: kdc
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}2vOrDsINZTpwNhj9wUrhiqBCvpTAQi02
  - dn: cn=kadmin,ou=kerberos,dc=example,dc=net
    cn: kadmin
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}9Xpeg17kacCnHQe5JiVEsUpTH2VYlFnq

Endlich die benötigten Objekte

- LDIF-Datei für die benötigten Objekte
  - dn: ou=kerberos,dc=example,dc=net
    ou: kerberos
    objectClass: organizationalUnit
    objectClass: top
  - dn: cn=kdc,ou=kerberos,dc=example,dc=net
    cn: kdc
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}2vOrDsINZTpwNhj9wUrhiqBCvpTAQi02
  - dn: cn=kadmin,ou=kerberos,dc=example,dc=net
    cn: kadmin
    objectClass: organizationalRole
    objectClass: simpleSecurityObject
    userPassword: {SSHA}9Xpeg17kacCnHQe5JiVEsUpTH2VYlFnq

Kerberos hört auf seinen neuen Herrn

- Umstellung der Datei krb5.conf
  - [realms]
    EXAMPLE.NET = {
    admin_server = ldapserver.example.net
    database_module = ldapconf
    }
  - [dbmodules]
    ldapconf = {
    db_library = kldap
    ldap_kerberos_container_dn = "ou=kerberos,dc=example,dc=net"
    ldap_kdc_dn = "cn=kdc,ou=kerberos,dc=example,dc=net"
    ldap_kadmind_dn = "cn=kadmin,ou=kerberos,dc=example,dc=net"
    ldap_service_password_file = "/etc/krb5kdc/service.keyfile"
    ldap_servers = "ldap://ldapserver.example.net"
    ldap_conns_per_server = 5
    }

Kerberos hört auf seinen neuen Herrn

- Umstellung der Datei krb5.conf
  - [realms]
    EXAMPLE.NET = {
    admin_server = ldapserver.example.net
    database_module = ldapconf
    }
  - [dbmodules]
    ldapconf = {
    db_library = kldap
    ldap_kerberos_container_dn = "ou=kerberos,dc=example,dc=net"
    ldap_kdc_dn = "cn=kdc,ou=kerberos,dc=example,dc=net"
    ldap_kadmind_dn = "cn=kadmin,ou=kerberos,dc=example,dc=net"
    ldap_service_password_file = "/etc/krb5kdc/service.keyfile"
    ldap_servers = "ldap://ldapserver.example.net"
    ldap_conns_per_server = 5
    }

Kerberos hört auf seinen neuen Herrn

- Umstellung der Datei krb5.conf
  - [realms]
    EXAMPLE.NET = {
    admin_server = ldapserver.example.net
    database_module = ldapconf
    }
  - [dbmodules]
    ldapconf = {
    db_library = kldap
    ldap_kerberos_container_dn = "ou=kerberos,dc=example,dc=net"
    ldap_kdc_dn = "cn=kdc,ou=kerberos,dc=example,dc=net"
    ldap_kadmind_dn = "cn=kadmin,ou=kerberos,dc=example,dc=net"
    ldap_service_password_file = "/etc/krb5kdc/service.keyfile"
    ldap_servers = "ldap://ldapserver.example.net"
    ldap_conns_per_server = 5
    }

Jetzt wird es ernst

- Sichern der lokalen Kerberos-Datenbank
  - `root@ldapserver:~# kdb5_util dump /root/example.net`
- Löschen der lokalen Kerberos-Datenbank
  - ```
    root@ldapserver:~# kdb5_util destroy
    Deleting KDC database stored in '/var/lib/krb5kdc/principal', are you sure?
    (type 'yes' to confirm)? yes
    OK, deleting database '/var/lib/krb5kdc/principal'...
    ** Database '/var/lib/krb5kdc/principal' destroyed.
    ```
    ```

Jetzt wird es ernst

- Sichern der lokalen Kerberos-Datenbank
  - `root@ldapserver:~# kdb5_util dump /root/example.net`
- Löschen der lokalen Kerberos-Datenbank
  - ```
    root@ldapserver:~# kdb5_util destroy
    Deleting KDC database stored in '/var/lib/krb5kdc/principal', are you sure?
    (type 'yes' to confirm)? yes
    OK, deleting database '/var/lib/krb5kdc/principal'...
    ** Database '/var/lib/krb5kdc/principal' destroyed.
    ```
    ```

Jetzt wird es ernst

- Sichern der lokalen Kerberos-Datenbank
  - `root@ldapserver:~# kdb5_util dump /root/example.net`
- Löschen der lokalen Kerberos-Datenbank
  - ```
    root@ldapserver:~# kdb5_util destroy
    Deleting KDC database stored in '/var/lib/krb5kdc/principal', are you sure?
    (type 'yes' to confirm)? yes
    OK, deleting database '/var/lib/krb5kdc/principal'...
    ** Database '/var/lib/krb5kdc/principal' destroyed.
    ```
    ```

Jetzt wird es ernst

- Sichern der lokalen Kerberos-Datenbank
  - `root@ldapserver:~# kdb5_util dump /root/example.net`
- Löschen der lokalen Kerberos-Datenbank
  - ```
    root@ldapserver:~# kdb5_util destroy
    Deleting KDC database stored in '/var/lib/krb5kdc/principal', are you sure?
    (type 'yes' to confirm)? yes
    OK, deleting database '/var/lib/krb5kdc/principal'...
    ** Database '/var/lib/krb5kdc/principal' destroyed.
    ```
    ```

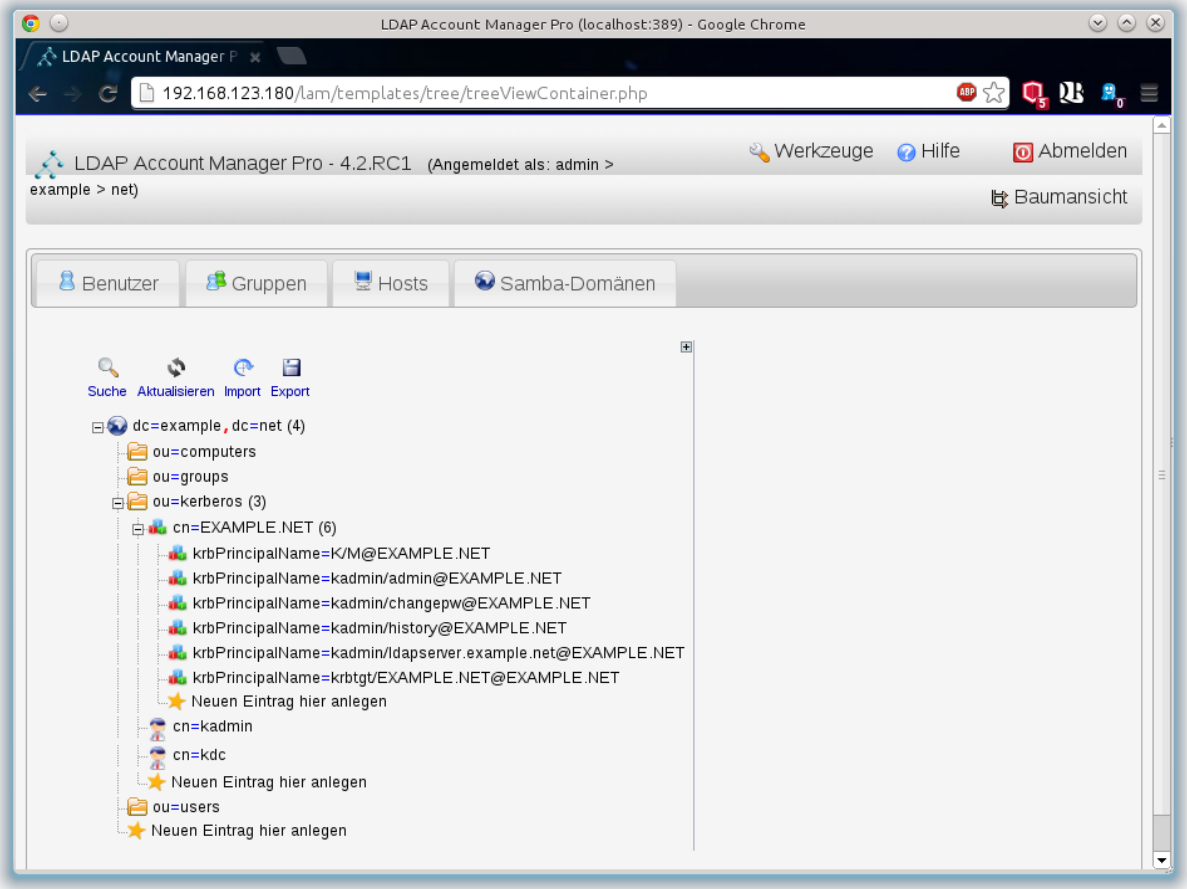
OpenLDAP ein schönes neues Zuhause

- Erstellung der Standard Kerberos-Principals
  - ```
    root@ldapserver:~# kdb5_ldap_util create -D cn=admin,dc=example,dc=net \
        -r EXAMPLE.NET -s -sscope sub

    Password for "cn=admin,dc=example,dc=net":
    Initializing database for realm 'EXAMPLE.NET'
    You will be prompted for the database Master Password.
    It is important that you NOT FORGET this password.
    Enter KDC database master key:
    Re-enter KDC database master key to verify:
    ```
    ```

Ein erstes Bild: Kerberos im openLDAP

- Alle Standardcontainer und Objekte



Einzug ins neu Zuhause für den Kerberos

- Passwort für den KDC und kadmin festlegen
  - `root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net \ -f /etc/krb5kdc/service.keyfile cn=kadmin,ou=kerberos,dc=example,dc=net`

    ```
    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    ```

  - `root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net \ -f /etc/krb5kdc/service.keyfile cn=kdc,ou=kerberos,dc=example,dc=net`

    ```
    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    ```

Einzug ins neu Zuhause für den Kerberos

- Passwort für den KDC und kadmin festlegen
  - ```
    root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net\
     -f /etc/krb5kdc/service.keyfile cn=kadmin,ou=kerberos,dc=example,dc=net

    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    ```
  - ```
    root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net\
     -f /etc/krb5kdc/service.keyfile cn=kdc,ou=kerberos,dc=example,dc=net
    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    ```

Einzug ins neu Zuhause für den Kerberos

- Passwort für den KDC und kadmin festlegen
  - `root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net \ -f /etc/krb5kdc/service.keyfile cn=kadmin,ou=kerberos,dc=example,dc=net`

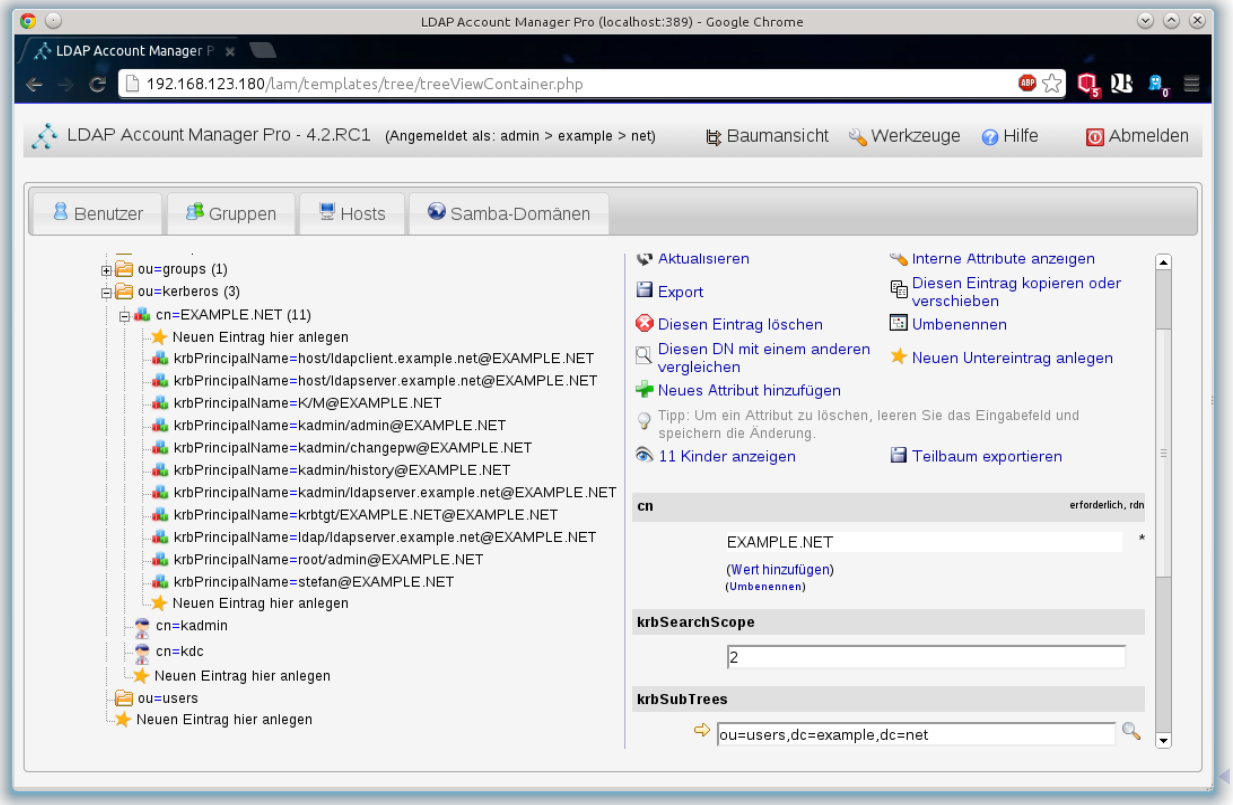
    ```
    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kadmin,ou=kerberos,dc=example,dc=net":
    ```

  - `root@ldapserver:~# kdb5_ldap_util stashsrvpw -D cn=admin,dc=example,dc=net \ -f /etc/krb5kdc/service.keyfile cn=kdc,ou=kerberos,dc=example,dc=net`

    ```
    Password for "cn=admin,dc=example,dc=net":
    Password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    Re-enter password for "cn=kdc,ou=kerberos,dc=example,dc=net":
    ```

Einzug ins neue Zuhause für den Kerberos

- Backup einspielen
  - `root@ldapserver:~# kdb5_util -update load example.net`
- Kerberos-Daten nach dem Recover



Kann der Kerberos schon zugreifen?

- Authentifizieren klappt schon für lokale Benutzer

```
root@ldapserver:~# kinit stefan
Password for stefan@EXAMPLE.NET:

root@ldapserver:~# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: stefan@EXAMPLE.NET

Valid starting     Expires            Service principal
27.05.2013 13:37:40  27.05.2013 23:37:40  krbtgt/EXAMPLE.NET@EXAMPLE.NET
        renew until 28.05.2013 13:37:37
```

- Aber die LDAP-Benutzerkonten fehlen noch
- Dem Kerberos den Weg zu den Benutzern im LDAP zeigen durch hinzufügen eines Subtrees

```
root@ldapserver:~# kdb5_ldap_util modify -D cn=admin,dc=example,dc=net \
                   -r EXAMPLE.NET -subtrees ou=users,dc=example,dc=net

Password for "cn=admin,dc=example,dc=net":
```

Kann der Kerberos schon zugreifen?

- Authentifizieren klappt schon für lokale Benutzer
- ```
  root@ldapserver:~# kinit stefan
  Password for stefan@EXAMPLE.NET:

  root@ldapserver:~# klist
  Ticket cache: FILE:/tmp/krb5cc_0
  Default principal: stefan@EXAMPLE.NET

  Valid starting     Expires            Service principal
  27.05.2013 13:37:40  27.05.2013 23:37:40  krbtgt/EXAMPLE.NET@EXAMPLE.NET
          renew until 28.05.2013 13:37:37
  ```
- Aber die LDAP-Benutzerkonten fehlen noch
- Dem Kerberos den Weg zu den Benutzern im LDAP zeigen durch hinzufügen eines Subtrees
- ```
  root@ldapserver:~# kdb5_ldap_util modify -D cn=admin,dc=example,dc=net \
                     -r EXAMPLE.NET -subtrees ou=users,dc=example,dc=net

  Password for "cn=admin,dc=example,dc=net":
  ```

Kann der Kerberos schon zugreifen?

- Authentifizieren klappt schon für lokale Benutzer
- ```
  root@ldapserver:~# kinit stefan
  Password for stefan@EXAMPLE.NET:

  root@ldapserver:~# klist
  Ticket cache: FILE:/tmp/krb5cc_0
  Default principal: stefan@EXAMPLE.NET

  Valid starting     Expires            Service principal
  27.05.2013 13:37:40  27.05.2013 23:37:40  krbtgt/EXAMPLE.NET@EXAMPLE.NET
          renew until 28.05.2013 13:37:37
  ```
- Aber die LDAP-Benutzerkonten fehlen noch
- Dem Kerberos den Weg zu den Benutzern im LDAP zeigen durch hinzufügen eines Subtrees
- ```
  root@ldapserver:~# kdb5_ldap_util modify -D cn=admin,dc=example,dc=net \
                     -r EXAMPLE.NET -subtrees ou=users,dc=example,dc=net

  Password for "cn=admin,dc=example,dc=net":
  ```

Kann der Kerberos schon zugreifen?

- Authentifizieren klappt schon für lokale Benutzer
- ```
  root@ldapserver:~# kinit stefan
  Password for stefan@EXAMPLE.NET:

  root@ldapserver:~# klist
  Ticket cache: FILE:/tmp/krb5cc_0
  Default principal: stefan@EXAMPLE.NET

  Valid starting     Expires            Service principal
  27.05.2013 13:37:40  27.05.2013 23:37:40  krbtgt/EXAMPLE.NET@EXAMPLE.NET
          renew until 28.05.2013 13:37:37
  ```
- Aber die LDAP-Benutzerkonten fehlen noch
- Dem Kerberos den Weg zu den Benutzern im LDAP zeigen durch hinzufügen eines Subtrees
- ```
  root@ldapserver:~# kdb5_ldap_util modify -D cn=admin,dc=example,dc=net \
                     -r EXAMPLE.NET -subtrees ou=users,dc=example,dc=net

  Password for "cn=admin,dc=example,dc=net":
  ```

Kann der Kerberos schon zugreifen?

- Authentifizieren klappt schon für lokale Benutzer
- ```
  root@ldapserver:~# kinit stefan
  Password for stefan@EXAMPLE.NET:

  root@ldapserver:~# klist
  Ticket cache: FILE:/tmp/krb5cc_0
  Default principal: stefan@EXAMPLE.NET

  Valid starting     Expires            Service principal
  27.05.2013 13:37:40  27.05.2013 23:37:40  krbtgt/EXAMPLE.NET@EXAMPLE.NET
          renew until 28.05.2013 13:37:37
  ```
- Aber die LDAP-Benutzerkonten fehlen noch
- Dem Kerberos den Weg zu den Benutzern im LDAP zeigen durch hinzufügen eines Subtrees
- ```
  root@ldapserver:~# kdb5_ldap_util modify -D cn=admin,dc=example,dc=net \
                     -r EXAMPLE.NET -subtrees ou=users,dc=example,dc=net

  Password for "cn=admin,dc=example,dc=net":
  ```

Schau an, ein Neuer im Baum

- Ein Benutzer ohne Kerberos-Eigenschaften
  - `root@ldapserver:~# ldapsearch -LLL "(uid=ktom)"`

```
dn: cn=Kater Tom,ou=users,dc=example,dc=net
objectClass: posixAccount
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
homeDirectory: /home/KTom
loginShell: /bin/bash
uid: KTom
cn: Kater Tom
uidNumber: 10000
gidNumber: 10000
sn: Tom
givenName: Kater
```

Jetzt soll der Neue auch Kerberos können

- Kerberos-Eigenschaften hinzufügen

```
kadmin:  add_principal -x dn="uid=ktom,ou=users,dc=example,dc=net" \
         -pw geheim ktom

WARNING: no policy specified for ktom@EXAMPLE.NET; defaulting to no policy
Principal "ktom@EXAMPLE.NET" created.
```

Jetzt soll der Neue auch Kerberos können

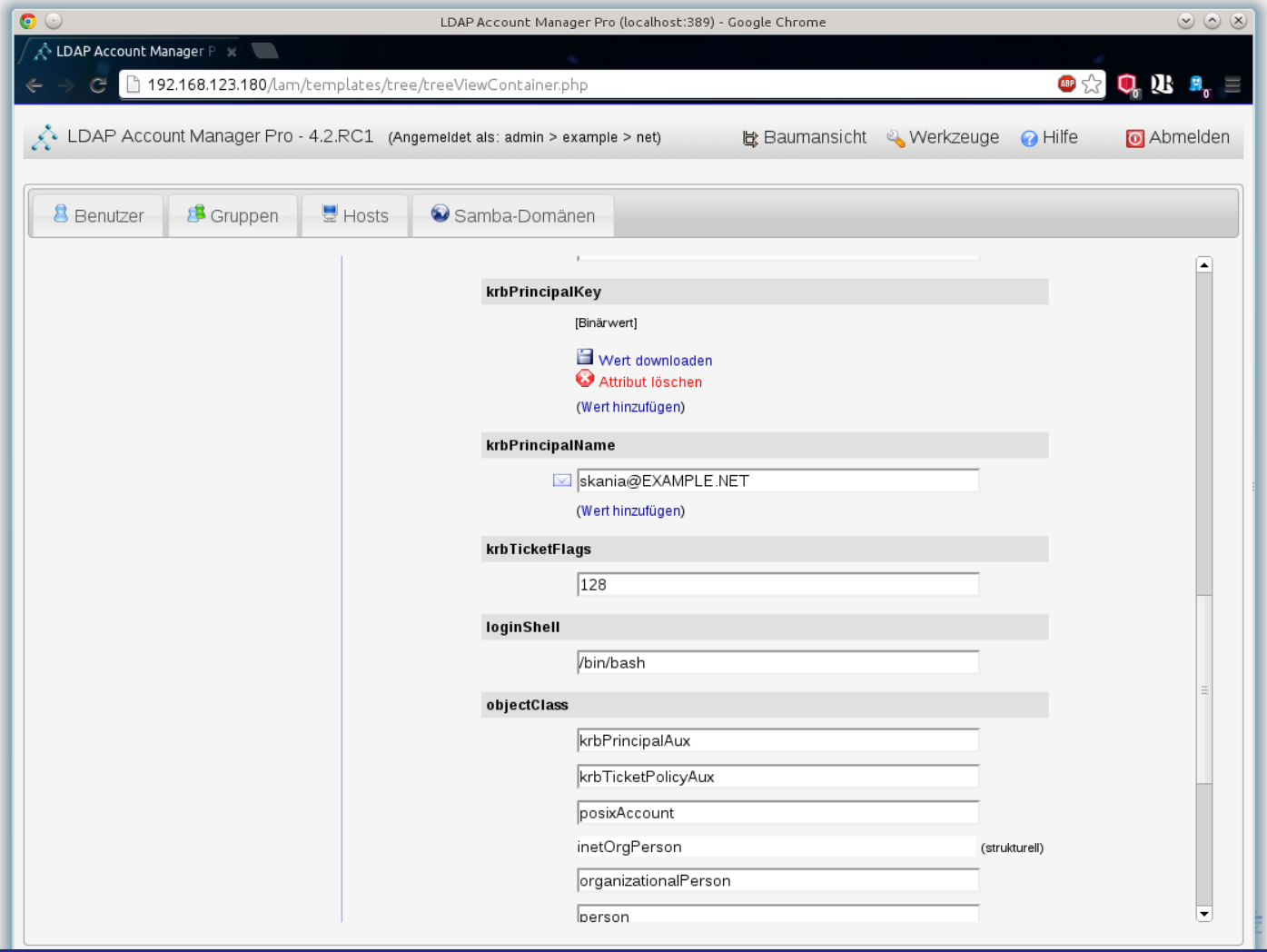
- Kerberos-Eigenschaften hinzufügen
- ```
  kadmin:  add_principal -x dn="uid=ktom,ou=users,dc=example,dc=net" \
           -pw geheim ktom

  WARNING: no policy specified for ktom@EXAMPLE.NET; defaulting to no policy
  Principal "ktom@EXAMPLE.NET" created.
  ```
  ```

Jetzt kann der Neue auch Kerberos

- Da ist er!
- ```
  root@ldapserver:~# ldapsearch -x "(uid=ktom)" -LLL
  dn: uid=KTom,ou=users,dc=example,dc=net
  objectClass: posixAccount
  objectClass: inetOrgPerson
  objectClass: organizationalPerson
  objectClass: person
  objectClass: krbPrincipalAux
  objectClass: krbTicketPolicyAux
  homeDirectory: /home/KTom
  loginShell: /bin/bash
  uid: KTom
  cn: Kater Tom
  uidNumber: 10000
  gidNumber: 10000
  sn: Tom
  givenName: Kater
  krbLoginFailedCount: 0
  krbPrincipalName: ktom@EXAMPLE.NET
  krbPrincipalKey:: ... bUR9UDSDvnBp9Z09LFYoa1vwx3fqLiwY=
  krbLastPwdChange: 20130527124220Z
  krbLastSuccessfulAuth: 20130527124512Z
  krbExtraData:: AAKsVKNRcm9vdC9hZG1pbkBFWEFNUExFLk5FVAA=
  krbExtraData:: AAgBAA==
  ```
  ```

So sieht es grafisch aus



Ein praktisches Beispiel bitte!

- Kerberos-Authentifizierung mit ssh

Und was ist jetzt mit den Tickets bei ssh?

- Datei /etc/ssh/sshd_config auf dem Server
- ```
  # GSSAPI options
  GSSAPIAuthentication yes
  GSSAPICleanupCredentials yes
  GSSAPIKeyExchange yes
  ```
- Datei /etc/krb5.conf auf dem Client
- ```
  [appdefaults]
          forward = true
          forwardable = true
  ```

Und was ist jetzt mit den Tickets bei ssh?

- Datei /etc/ssh/sshd_config auf dem Server
- ```
  # GSSAPI options
  GSSAPIAuthentication yes
  GSSAPICleanupCredentials yes
  GSSAPIKeyExchange yes
  ```
- Datei /etc/krb5.conf auf dem Client
- ```
  [appdefaults]
          forward = true
          forwardable = true
  ```

Und was ist jetzt mit den Tickets bei ssh?

- Datei /etc/ssh/sshd_config auf dem Server
- ```
  # GSSAPI options
  GSSAPIAuthentication yes
  GSSAPICleanupCredentials yes
  GSSAPIKeyExchange yes
  ```
- Datei /etc/krb5.conf auf dem Client
- ```
  [appdefaults]
          forward = true
          forwardable = true
  ```

Und was ist jetzt mit den Tickets bei ssh?

- Datei /etc/ssh/sshd_config auf dem Server
- ```
  # GSSAPI options
  GSSAPIAuthentication yes
  GSSAPICleanupCredentials yes
  GSSAPIKeyExchange yes
  ```
- Datei /etc/krb5.conf auf dem Client
- ```
  [appdefaults]
          forward = true
          forwardable = true
  ```

Was muss der Benutzer jetzt machen?

- Anpassen der Datei /.ssh/config
- ```
  Host ldapserver.example.net
        GSSAPIDelegateCredentials yes
        GSSAPIRenewalForcesRekey yes
        GSSAPIKeyExchange yes
  ```
- Hosts können auch zentral über die /etc/ssh/ssh_config verwaltet werden
  ```

Was muss der Benutzer jetzt machen?

- Anpassen der Datei /.ssh/config
- ```
  Host ldapserver.example.net
          GSSAPIDelegateCredentials yes
          GSSAPIRenewalForcesRekey yes
          GSSAPIKeyExchange yes
  ```
- Hosts können auch zentral über die /etc/ssh/ssh_config verwaltet werden
  ```

Was muss der Benutzer jetzt machen?

- Anpassen der Datei /.ssh/config
- ```
  Host ldapserver.example.net
          GSSAPIDelegateCredentials yes
          GSSAPIRenewalForcesRekey yes
          GSSAPIKeyExchange yes
  ```
- Hosts können auch zentral über die /etc/ssh/ssh_config verwaltet werden
  ```

Und wie sieht das in der Praxis aus?

- Der LAM zur Benutzerverwaltung
- ssh Ticketverwaltung