

Einbinden von Unix/Linux-Systemen

Thema:	Einbindung zusätzlicher Unix/Linux-Systeme in eine UCS-Domäne.
Datum:	9. Dezember 2010
Seitenzahl:	8
Versionsnummer:	7397
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Servergrundkonfiguration	3
3	Benutzerdatenbank	3
4	Kerberos	4
5	Samba	5
6	Lokale LDAP-Replik	7
7	Terminalserver	7

1 Einführung

Es besteht die Möglichkeit andere Unix- und Linux-Distributionen, im folgenden Fremdsysteme genannt, in den Vertrauenskontext der UCS-Domäne zu integrieren. Für die Nutzung dieses Vertrauenskontext sollte für das Fremdsystem ein Memberserver-Account unterhalb des Containers `cn=memberserver,cn=computers` angelegt werden. Dabei sind mindestens der Name, die IP-Adresse, ein Passwort und die DNS-Einstellungen anzugeben.

2 Servergrundkonfiguration

Die Grundkonfiguration der Fremdsysteme ist grundlegend verschieden. Es sollten aber mindestens die folgenden Punkte konfiguriert werden:

- Netzwerkkonfiguration
Hier sollte als Nameserver ein UCS-Domaincontroller-System verwendet werden.
- NTP-Client
Als NTP-Server sollte ein UCS-Domaincontroller-System verwendet werden.

Je nach Anforderung können weitere Einstellungen konfiguriert werden, wie z. B. das Einbinden der Heimatverzeichnisse oder die Druckerkonfiguration. Die nötigen Konfigurationsschritte können der distributionsspezifischen Dokumentation entnommen werden.

3 Benutzerdatenbank

Unter Linux-Systemen erfolgt die Auflösung von Benutzer und Gruppen über NSS (Name Service Switch). Da die Benutzer- und Gruppeninformationen in der UCS-Domäne im LDAP gespeichert werden, sollte das Modul **nss_ldap** verwendet werden. Je nach Distribution ist die Konfiguration unterschiedlich.

Generell müssen die folgenden Einstellungen vorgenommen werden:

- LDA-Base-DN
Der LDAP-Base-DN kann auf dem DC Master mit dem Befehl

```
univention-config-registry get ldap/base
```

abgefragt werden.
- LDAP-Server
Hier sollten die FQDNs der UCS-LDAP-Server angegeben werden, die für die LDAP-Suche verwendet werden sollen.
- LDAP TLS/SSL
Damit die TLS-Verschlüsselung funktioniert, sollte das Root-CA-Zertifikat vom DC Master kopiert werden:

```
scp <ucs-master>:/etc/univention/ssl/udsCA/CAcert.pem /etc/ssl/
```

Anschließend sollte in der jeweiligen LDAP-Konfigurationsdatei, z.B. `/etc/openldap/ldap.conf`, das Zertifikat bekannt gegeben werden:

```
TLS_CACERT /etc/ssl/CAcert.pem
```

Die Benutzer und Gruppen können jetzt mit den Befehlen

```
getent passwd  
getent group
```

abgefragt werden.

4 Kerberos

UCS verwendet die Kerberos-Implementierung Heimdal. Es sollte daher auf den Fremdsystemen auch die Heimdal- und nicht die MIT-Implementierung verwendet werden, ansonsten kann es zu Problemen bei der Passwortänderung kommen, da diese nicht standardisiert ist.

Wenn beim Anlegen des Fremdsystems als Memberserver ein Rechner-Passwort angegeben wird, erzeugt der Listener/Notifier-Mechanismus auf dem UCS DC Master eine keytab-Datei, die den Namen des Fremdsystems trägt. Diese keytab-Datei muss auf dem Fremdsystem gespeichert werden:

```
scp <ucs-master>:/var/lib/univention-heimdal/$(hostname) /etc/krb5.keytab
```

Die eigentliche Kerberos-Konfiguration wird in der Datei `/etc/krb5.conf` vorgenommen:

```
[libdefaults]
    default_realm = <REALM>
    clockskew = 300
    v4_instance_resolve = false
    v4_name_convert = {
        host = {
            rcmd = host
            ftp = ftp
        }
        plain = {
            something = something-else
        }
    }
    # Set this to false to disable MIT krb5 compatibility
    # in GSSAPI get_mic/verify_mic, and become compatible
    # with older Heimdal releases instead.
    gss_mit_compat = true

[realms]
    <REALM> = {
        kdc = <UCS Server>
    }
```

```
OTHER.REALM = {
    v4_instance_convert = {
        kerberos = kerberos
        computer = computer.some.other.domain
    }
}
[domain_realm]
.my.domain = <REALM>
```

Dabei sind die Werte **<REALM>** und **<UCS Server>** zu ersetzen. Der Wert für **<REALM>** kann auf dem DC Master mit dem Befehl

```
univention-config-registry get kerberos/realm
```

abgefragt werden. Als **<UCS Server>** ist jeder DC Master, DC Backup oder DC Slave aus der UCS-Domäne geeignet.

Für die Anmeldung gegen Kerberos sind die PAM-Konfigurationen anzupassen, hierfür muss das Paket **pam-krb5** installiert werden. Als Kerberos-Einstellung eignet sich die folgende Zeile:

```
auth sufficient pam_krb5.so forwardable ccache=/tmp/krb5_%u
```

Die Passwörter können mit dem Befehl `kpasswd` geändert werden, alternativ ist eine Passwort-Änderung über PAM mit dem Modul **pam-heimdal** möglich.

5 Samba

Die UCS-Samba-Domäne verwendet Samba 3, welches auch auf dem Fremdsystem installiert sein sollte.

Das Samba auf dem Fremdsystem ist als Memberserver zu konfigurieren.

Beispielkonfiguration `smb.conf`:

```
[global]
    debug level = 0
    syslog = 0
    max log size = 1000000
    server string = %h Fremdsystem
    netbios name = <HOSTNAME>
    ldap suffix = <LDAP/BASE>
    ldap admin dn = <SERVER/DN>
    ldap ssl = on
    ; idmap/winbind
    idmap backend = ldap:ldap://<UCS Server>
    ldap idmap suffix = cn=idmap,cn=univention
    idmap uid = 55000-64000
    idmap gid = 55000-64000
    winbind trusted domains only = yes
    winbind enum users = yes
```

```
winbind enum groups = yes
winbind separator = +
template shell = /bin/bash
template homedir = /home/%D-%U
; password sync
pam password change = no
obey pam restrictions = yes
encrypt passwords = yes
; printing
load printers = yes
printing = cups
printcap name = cups
printer admin = @"Printer-Admins", root, Administrator
; domain
security = domain
domain logons = no
domain master = no
prefered master = no
local master = no
os level = 65
wins support = no
wins server = no
workgroup = <DOMAIN>
oplocks = yes
kernel oplocks = yes
large readwrite = yes
deadtime = 15
read raw = yes
write raw = yes
max xmit = 65535
getwd cache = yes
store dos attributes = yes
preserve case = yes
short preserve case = yes
time server = yes
guest account = nobody
map to guest = Bad User
admin users = administrator
invalid users = daemon bin sys sync games man lp mail news uucp
proxy majordom postgres www-data backup mysql operator list irc gnats
alias qmaild qmails qmailr qmailq qmail1 qmailp telnetd identd ftp rwhod
gdm fetchmail faxmaster
```

Die Werte für **<Domainname>**, **<Hostname>**, **<UCS Server>**, **<Ldap Base>** und **<Server DN>** sind anzupassen. Der Wert für <Domainname> kann auf dem DC Master mit dem Befehl

```
univention-config-registry get windows/domain
```

abgefragt werden. Als <UCS Server> ist jeder DC Master, DC Backup oder DC Slave aus der UCS-Domäne geeignet. Als <Server DN> sollte der DN des Fremdsystems angegeben werden.

Das Fremdsystem benötigt schreibenden Zugriff auf das LDAP, da es gegebenenfalls IDMAP-Einträge in das LDAP-Verzeichnis schreiben muss. Mit einem Memberserver-Account wird dies

in den Standard-ACLs berücksichtigt. Das Passwort des Fremdsystems, welches beim Anlegen des Memberserver-Accounts mit Univention Directory Manager vergeben wurde, muss jetzt in der internen Samba-Datenbank bekannt gegeben werden.

```
smbpasswd -w <password>
```

Anschließend muss der Samba-Server in die Samba-Domäne joinen:

```
net join MEMBER -U root
```

Nach erfolgreicher Eingabe des root-Passwortes des DC Master ist der Fremdsystem-Samba-Server Mitglied in der Samba-Domäne des UCS-Systems.

Anschließend sollte der Samba-Dienst auf dem Fremdsystem neu gestartet werden:

```
/etc/init.d/samba restart
```

6 Lokale LDAP-Replik

Es besteht die Möglichkeit, dass das Fremdsystem eine lokale LDAP-Replik bezieht, z.B. damit über NSS die Benutzerdaten direkt aus dem lokalen LDAP-Verzeichnis gelesen werden. Hierzu wird nicht der Listener/Notifier-Mechanismus verwendet, sondern das in OpenLDAP integrierte Replikationsverfahren **syncrepl**. Hinweise zur Konfiguration finden sich unter <http://www.openldap.org/doc/admin24/replication.html>. Die Einrichtung ist außerdem in der Univention Supportdatenbank unter <http://sdb.univention.de/1120> beschrieben.

Bis UCS 2.2 unterstützte der OpenLDAP-Dienst auch das Replikationsverfahren **slurpd**. Dieses wurde aus OpenLDAP 2.4 entfernt und steht ab UCS 2.3 nicht mehr zur Verfügung.

7 Terminalserver

Das Fremdsystem kann als Terminalserver für Thin Clients verwendet werden. Dieser muss den Kerberos-RSH-Dienst anbieten. Bei den meisten Linux-Distributionen ist das Kerberos-RSH-Programm in dem entsprechenden Heimdal-Paket enthalten.

Der RSH-Dienst wird bei den meisten Distributionen über `inetd` bzw. `xinetd` gestartet. Wie der Dienst im einzelnen eingebunden werden kann, sollte dem Handbuch der eingebundenen Distribution entnommen werden. In den meisten Fällen geschieht dies automatisch.

Auf den UCS-Servern, die das Thin-Client-root-Verzeichnis anbieten, kann dann eine zusätzliche Session-Datei angelegt werden, die im GDM-Sitzungs-Auswahl-Dialog angezeigt wird. In dem Session-Skript wird eine krsh-Verbindung zu dem Fremdsystem aufgebaut. Die Datei muss im Verzeichnis `/var/lib/univention-client-root/etc/gdm/Sessions` gespeichert werden.

Beispiel:

```
#!/bin/sh

DISPLAY=:0.0
LONGKEY=$(xauth nextract - "$HOSTNAME"/unix"$DISPLAY")
KEY=${LONGKEY/* /};

krsh <Fremdsystem> "/usr/X11R6/bin/xauth add \"${HOSTNAME}\" \"${DISPLAY}\" .
\"$KEY\" && DISPLAY=$HOSTNAME:0 /opt/kde3/bin/startkde"
```

<Fremdsystem> muss durch den FQDN des Fremdsystems ersetzt und das zu startende Programm kann beliebig gewählt werden.