

UCS Performance Guide

Thema:	Univention Corporate Server Optimierungen	
Datum:	7. August 2009	
Seitenzahl:	13	
Versionsnummer:	3650	
Autoren:	Univention GmbH	feedback@univention.de

Inhaltsverzeichnis

1	Einführung	3
2	Basiskonfiguration	3
2.1	Auswahl laufender Dienste	3
2.2	NSCD	5
3	OpenLDAP	6
3.1	Indizes	6
3.2	Konfiguration der LDAP-Datenbank	8
3.3	OpenLDAP-ACLs	10
4	Lastverteilung	10
4.1	LDAP-Replikation	11
4.2	Authentifikation	12
4.3	Terminaldienste	12
5	Mailsysteme	12
5.1	Dateisystem	13
5.2	Logdateien	13
5.3	Dienste verteilen	13

1 Einführung

Mit der Installation von Univention Corporate Server (UCS) werden die ausgewählten Serveranwendungen betriebsbereit konfiguriert. Dennoch kann es in komplexen Umgebungen oder bei besonderen Anforderungen sinnvoll sein, Konfigurationsanpassungen gemäss der spezifischen Anforderungen vorzunehmen.

Mit Updates der UCS-Distribution können zusätzliche Dienste und Anwendungen Einzug halten, die mit der ursprünglichen Konfiguration nicht optimal bedient sind. Ebenso werden durch die Einführung neuer Techniken zusätzliche Optimierungsmöglichkeiten geschaffen, deren Einführung nicht während des Updates möglich bzw. sinnvoll sind.

In den folgenden Absätzen werden Anpassungsmöglichkeiten und aktualisierungsbezogene Optimierungen von UCS aufgezeigt, die es ermöglichen, das System auf die speziellen Bedürfnisse anzupassen.

2 Basiskonfiguration

Wesentliche Aspekte der Grundkonfiguration werden bei der Installation entschieden. Zur Partitionierung, der Auswahl der Dateisysteme und der benötigten Dienste finden sich Informationen im UCS-Handbuch.

2.1 Auswahl laufender Dienste

Mit der Umstellung oder Erweiterung von Servern können zuvor auf einem System benötigte oder angebotene Dienste überflüssig werden. Da diese in der Regel unnötige Ressourcen binden, kann eine Deaktivierung sinnvoll sein. Diese kann vorübergehend durch Beenden des Dienstes, langfristig durch Deaktivierung der zugehörigen Startskripte oder endgültig durch Deinstallation des Softwarepaketes erfolgen.

Bei allen Schritten sind mögliche Folgen zu bedenken, ein unbedacht gestoppter oder entfernter Dienst kann weitreichende Konsequenzen haben. Angefangen bei der Beeinträchtigung der Benutzer über Nichterreichbarkeit einzelner Server bis hin zu Datenverlusten durch die Deinstallation. Alle Maßnahmen sollten daher zunächst unter Testbedingungen und nach einem erfolgreichen Backup ausgeführt werden.

2.1.1 Identifizieren nicht benötigter Dienste

Die wesentlichen angebotenen Serverdienste finden sich in Univention Management Console unter dem Punkt **System-Dienste**. Während jeweils einzeln zu klären ist, ob der Dienst in der vorliegenden Umgebung benötigt wird, sollten für die Verfügbarkeit des Systems einige Basisdienste nicht beendet oder deaktiviert werden:

- **OpenLDAP**

Der LDAP-Server dient der Authentifizierung von Benutzern und der Speicherung aller über den Univention Directory Manager vorgenommenen Konfigurationseinstellungen. Eine Deaktivierung macht alle Dienste, für die eine Authentifikation notwendig ist, für Domänenbenutzer unerreichbar.

- **Apache**

Der Webserver stellt UCS-spezifische Dienste zur Verfügung. Neben der Konfiguration über Univention Directory Manager oder Univention Management Console wird er auch für anonymen Informationsaustausch zwischen Thin Client und Terminalserver über HTTP-Anfragen oder für das Software-Repository benötigt.

- **OpenSSH**

Der SSH-Server stellt für die Administration die grundlegende Zugriffsmöglichkeit auf den Server dar, die auch bei Problemen mit anderen Diensten erreichbar bleiben sollte. Der SSH-Zugriff wird von Univention-Tools (auf Grundlage von `univention-ssh`) auch für die Informationsaustausch zwischen Servern verwendet, z.B. beim Join-Vorgang.

- **NSCD**

Der Name Service Caching Daemon ist keine zwingende Anforderung für den Betrieb anderer Dienste. Besonders in großen Umgebungen entlastet er jedoch andere Dienste (LDAP, DNS) bei häufigen Anfragen. Die Deaktivierung kann zu signifikanten Performanceeinbußen führen.

- **BIND**

Der Domain Name Service BIND dient z.B. über Service-Records UCS-Diensten zur Konfiguration. Eine Deinstallation sollte nur durchgeführt werden, wenn sichergestellt ist, dass kein System diese Instanz verwendet.

Die weiteren in Univention Management Console aufgeführten Dienste können ohne Beeinträchtigung der direkten Erreichbarkeit des Systems deaktiviert werden.

Weitere aktivierte Dienste können über Systemwerkzeuge identifiziert werden. Dazu können laufende Prozesse über `top` oder `ps` abgefragt werden, über das Netzwerk erreichbare Dienste werden von `nmap` gefunden. Die zum offenen Port gehörenden Prozesse identifiziert `netstat` oder `lsof`.

2.1.2 Deaktivierung

In Univention Management Console können Dienste beendet oder der automatische Start deaktiviert werden. Dabei werden weder Anwendungen deinstalliert noch gehen Daten verloren. Univention Management Console greift dabei auf die im Verzeichnis `/etc/init.d` liegenden Init-Skripte zurück.

Das Beenden eines Dienstes kann auch über den Befehl `/etc/init.d/<Dienst> stop` erfolgen. Soll der Start des Dienstes mit dem nächsten Reboot nicht mehr erfolgen müssen die zugehörigen symbolischen Links in den Verzeichnissen `/etc/rc<level>.d` entfernt

werden. Das kann über das Tool `update-rc.d` erfolgen. Für Samba wäre dazu folgender Befehl notwendig:

```
update-rc.d samba remove -f
```

Für die Reaktivierung ist die Option **remove** durch **defaults** zu ersetzen. Ohne weitere Angabe werden die Dienste immer im Runlevel 2 unter Sequence Code 20 gestartet. Für Samba würde daher u.a. ein Link unter `/etc/rc2.d/S20samba` erstellt. Für einige Dienste ist jedoch die Angabe eines anderen Runlevels oder Sequence Code notwendig, um die Abhängigkeiten zwischen den Diensten nicht zu verletzen. Der OpenLDAP-Server muss beispielsweise in Runlevel 2 vor Samba gestartet werden und bekommt daher Sequence Code 19:

```
update-rc.d slapd 19 2
```

Die korrekten Angaben sollten vor einer manuellen Deaktivierung dokumentiert werden, da sie nur durch eine Neuinstallation des Pakets wiederhergestellt werden können. Ausgenommen sind Dienste, die über Univention Management Console (de-)aktiviert werden.

2.1.3 Deinstallation

Die komplette Deinstallation von Diensten gibt zusätzlich zur Deaktivierung auch in Anspruch genommenen Festplattenplatz frei. Dabei muss jedoch beachtet werden, dass dienstspezifische Informationen gelöscht werden können, die bei einer erneuten Installation manuell wiederhergestellt werden müssen (z.B. Datenbankinhalte).

Jedes Paket kann durch Univention Management Console oder die Paketlisten-Richtlinie in Univention Directory Manager deinstalliert werden. Manuell wird das Paket durch

```
apt-get remove <Paket>
```

entfernt. Bei allen Varianten ist zu beachten, dass vom zu deinstallierenden Paket abhängige Pakete ebenfalls deinstalliert werden. Eine Übersicht vorab bietet Univention Management Console, manuell kann die Deinstallation durch

```
apt-get remove <Paket> -s -u
```

simuliert werden.

2.2 NSCD

Der Name Service Caching Daemon bietet allen Diensten, die Zugriff auf Benutzer, Gruppen oder DNS-Daten benötigen, einen performanten Cache. Dabei werden Anfragen beispielsweise bei der Authentifikation zwischengespeicherter Benutzer und Gruppen lokal abgearbeitet, ohne Sie an den LDAP-Server zu richten.

Die Größe des von NSCD vorgehaltenen Cache ist voreingestellt auf Umgebungen mit bis zu einigen Tausend Benutzern und einigen hundert Gruppen. In größeren Umgebungen

oder bei zahlreichen Gruppen kann eine Erweiterung sinnvoll sein, die über Univention Configuration Registry-Variablen vorgenommen wird:

Variable	Voreinstellung
nscd/passwd/size	3001
nscd/group/size	211
nscd/hosts/size	3001

Der Passwd-Cache umfasst dabei alle Accounts. In UCS-Umgebungen trifft das auch auf Rechneraccounts zu. Der Hosts-Cache bezieht sich auf DNS-Anfragen.

Die gesetzten Werte sollte für eine optimale Performance des Cache Primzahlen sein. Die optimale Größe ist abhängig vom Einsatzgebiet des Systems. Sie sollte mindestens die maximale Anzahl der gleichzeitigen Zugriffe umfassen. Wird das System beispielsweise als Samba-Server eingesetzt, sollte der Passwd-Cache die Anzahl aller Rechner und Benutzer, die simultan auf den Server zugreifen werden, enthalten können.

3 OpenLDAP

Als Kernelement bei Betrieb und Verwaltung eines UCS-Systems spielt die Performance des LDAP-Servers eine zentrale Rolle für die Gesamtperformance des Systems. Optimierungsmöglichkeiten gibt es dabei auf Seite von Server und Client. Die hier aufgeführten Möglichkeiten beschreiben nur die Serverkonfiguration.

3.1 Indizes

OpenLDAP führt vergleichbar mit anderen Datenbanksystemen Indizes über häufig angefragte Attribute. Im Gegensatz zu anderen Attributen wird bei indizierten eine Suchanfrage nicht über den vollständigen, unsortierten Datenbankinhalt ausgeführt, sondern über einen optimierten Teilbereich.

Ein Index bedeutet immer Redundanz, da die Daten des indizierten Attributs zusätzlich zum Gesamtbestand im Index gespeichert werden. Der Aufbau und die Aktualisierung des Index benötigen zusätzliche Operationen bei Schreibzugriffen auf das LDAP-Verzeichnis, so dass mit jedem zusätzlichen Index Veränderungen am LDAP-Verzeichnis potentiell langsamer werden.

Die Gesamtperformance profitiert im Regelfall mehr von zusätzlichen Indizes, als dass sie unter langsameren Schreibzugriffen leidet. Mit Einführung eines Index über Gruppenmitgliedschaften lassen sich in sehr großen Umgebungen (einige zehntausend Benutzer) die Anfragezeiten nach Gruppen eines Users von einigen Minuten auf Zeiten im Sekundenbereich optimieren, während Schreibzugriffe kaum messbar verzögert werden.

Mit den UCS-Versionen wurden die voreingestellten Indizes häufig erweitert. Dabei ist es jedoch nicht möglich, ohne manuellen Eingriff zusätzliche Attribute zu indizieren.

Die LDAP-Indizes können aus dem Post-Installations-Skript des Pakets **univention-ldap-server** bezogen werden. Dazu muss aus der Datei `/var/lib/dpkg/info/univention-ldap-server.postinst` der Aufruf von `univention-config-registry` für `ldap/index/eq`, `ldap/index/pres` und `ldap/index/sub` kopiert werden. Dabei muss das Fragezeichen durch ein Gleichheitszeichen ersetzt werden, z.B.

```
univention-config-registry set ldap/index/sub="uid,cn,sn,givenName,mail,\
description,displayName,mailPrimaryAddress,mailAlternativeAddress,\
default,zoneName,sambaSID"
```

Nach jeder Veränderung an der Konfiguration muss der LDAP-Server angehalten und das Tool `slapindex` gestartet werden. Ein einfacher Neustart des LDAP-Servers aktualisiert den Index nicht und führt dazu, dass neu zu indizierende Attribute bei Anfragen leer erscheinen, da Sie nur noch im Index gesucht werden.

Bei der Indizierung von großen Verzeichnissen muss damit gerechnet werden, dass `slapindex` Laufzeiten im Stundenbereich erreichen kann.

Auf älteren UCS-Installationen sollte die Konfiguration der Indizes auf aktuelle Bedürfnisse kontrolliert werden. Veränderungen sind dabei über Univention Configuration Registry-Variablen möglich:

Variable	Voreinstellung (UCS 2.0-0)
ldap/index/eq	objectClass, uidNumber, gidNumber, memberUid, ou, uid, cn, sn, givenName, mail, description, displayName, sambaSID, sambaPrimaryGroupSID, sambaDomainName, uniqueMember, macAddress, dhcpHWAddress, krb5PrincipalName, aRecord, relativeDomainName, pTRRecord, zoneName, mailPrimaryAddress, mailAlternativeAddress, univentionServerRole, univentionService, kolabHomeServer, automountInformation, sambaAcctFlags, univentionPolicyReference
ldap/index/pres	objectClass, uidNumber, gidNumber, memberUid, ou, uid, cn, sn, givenName, mail, description, displayName, uniqueMember, macAddress, dhcpHWAddress, krb5PrincipalName, aRecord, mailPrimaryAddress, mailAlternativeAddress, kolabHomeServer, univentionPolicyReference
ldap/index/sub	uid, cn, sn, givenName, mail, description, displayName, mailPrimaryAddress, mailAlternativeAddress, default, zoneName, sambaSID
ldap/index/approx	uid, mail, alias, cn, sn, givenName

Die Variablen unterscheiden die zur Verfügung stehenden Index-Varianten **approx**, **eq**, **pres** und **sub**. Details zur Bedeutung der Indizes bietet der LDAP-Administrator Guide von OpenLDAP.

Das Attribut **uid** findet sich beispielsweise in allen vier Indizes wieder, **sambaSID** nur in

eq. Ob und in welchen Indizes ein Attribut aufgenommen werden kann, ist abhängig vom LDAP-Schema.

3.2 Konfiguration der LDAP-Datenbank

Die Daten des Verzeichnis-Dienstes werden vom LDAP-Server in einer Datenbank im Berkeley-Datenbank-Format (BDB) gespeichert. Jeder Datensatz ist dabei über einen Schlüssel erreichbar. BDB ist eine Datenbank-Bibliothek und bietet keine externen Zugriffsmöglichkeiten wie etwa eine SQL-Abfrageschnittstelle.

Die Konfiguration von BDB findet wesentlich über die Datei `/var/lib/univention-ldap/ldap/DB_CONFIG` statt. Diese wird unter UCS durch ein `univention-config-registry`-Template geschrieben. Ohne weitere Angaben ist der Inhalt:

```
set_cachesize 0 90000000 1
set_lg_bsize 262144
set_lg_max 1048576
```

Die Werte zu **`set_cachesize`** bestimmen die Größe des Cache, indem sie die verfügbare Menge in GB und Byte sowie die Anzahl der zu verwenden Blöcke im Arbeitsspeicher definieren. Voreingestellt ist eine Größe von ca. 90MB. Diese Größenordnung wird, sofern genügend Daten vorhanden sind, zusätzlich vom `slapd`-Prozess im Arbeitsspeicher benötigt. Der Cache sollte als Richtlinie immer groß genug sein, um alle Indizes aufnehmen zu können.

Mit **`set_lg_bsize`** und **`set_lg_max`** werden maximale Größe (in Byte) und Alter (in Sekunden) der BDB-Transaktionslogs definiert. Diese Dateien liegen ebenfalls im Datenverzeichnis und speichern angefragte Modifikation vor Ihrer Ausführung. Im Falle eines Abbruchs der Transaktion oder unsauberen Beendens des LDAP-Servers können anhand der letzten Logdateien die letzten Transaktionen kontrolliert und so ein konsistenter Datenbankzustand wiederhergestellt werden.

Für die meisten Änderungen an `DB_CONFIG` wird ein Aufruf des Tools `db_recover` benötigt, mit dem die neue Konfiguration für die Datenbank übernommen wird. Dieses Tool führt ebenfalls die Wiederherstellung der Datenbankkonsistenz anhand der Logdateien durch. Um einen störungsfreien Start von OpenLDAP zu gewährleisten, wird in einer BDB-Konfiguration `db_recover` vor jedem Start des LDAP-Servers über dessen Init-Skript ausgeführt. Nach dem Ändern von BDB-spezifischen Univention Configuration Registry-Variablen reicht es also, den LDAP-Server neu zu starten.

Zur Kontrolle von BDB steht das Tool `db4.2_stat` zur Verfügung. Bei laufendem LDAP-Server können u.a. aktuelle Informationen zur maximalen Cachegröße, Cachennutzung und Datensatz-Locking abgefragt werden. Der Aufruf des Tools sollte im Datenbankverzeichnis erfolgen.

Die angegebene Konfiguration ergibt sich, wenn keine BDB-bezogenen Univention Configuration Registry-Variablen gesetzt sind. Zur Manipulation der eingeführten Werte können folgende Univention Configuration Registry-Variablen gesetzt werden:

```
ldap/database/bdb/set_cachesize = "0 90000000 1"  
ldap/database/bdb/set_lg_bsize = "262144"  
ldap/database/bdb/set_lg_max = "1048576"
```

Um die zahlreichen zusätzlichen Optionen zugänglich zu machen, kann eine komma-separierte Liste der gewünschten Optionen in der Variable **ldap/database/bdb/db_config_options = "<option1>,<option2>"** angegeben werden. Die Wertzuweisung erfolgt dann durch Einführen der Variablen **ldap/database/bdb/<option1>** und **ldap/database/bdb/<option2>**.

In größeren Umgebungen können folgende Veränderungen sinnvoll sein:

- **Vergrößern des Cache**

Ein größerer Cache kann die LDAP-Zugriffe vom Dateisystem entkoppeln und besonders bei häufig angefragten Objekten zu Verbesserungen führen. Der Cache muss immer kleiner als der für OpenLDAP zur Verfügung stehende Arbeitsspeicher sein. Auswertungen zum verwendeten Cache bietet ein Aufruf von `db4.2_stat -m`.

- **Erhöhen der maximalen Anzahl von Locks**

BDB erlaubt per Voreinstellung maximal 1000 Locks für konkurrierende Zugriffe (locks), Benutzer (lockers) oder Objekte (objects). Auf den zentralen Systemen können durch gleichzeitigen Zugriff vieler anfragender Server oder große administrative Veränderungen Zugriffe verweigert werden, die vom Client im Regelfall als "critical extension unavailable" oder "implementation specific error" registriert werden. Eine Auswertung der tatsächlich verwendeten Locks gibt `db4.2_stat -c`.

Die Locks lassen sich durch die DB_Config-Optionen **set_lk_max_lockers**, **set_lk_max_locks** und **set_lk_max_objects** bestimmen. Eine Erhöhung auf 2000 Locks aller Parameter erfolgt mit univention-config-registry:

```
univention-config-registry set \  
  ldap/database/bdb/db_config_options="set_lk_max_lockers ,\  
  set_lk_max_locks , set_lk_max_objects "  
univention-config-registry set ldap/database/bdb/set_lk_max_lockers=2000  
univention-config-registry set ldap/database/bdb/set_lk_max_locks=2000  
univention-config-registry set ldap/database/bdb/set_lk_max_objects=2000
```

Dabei ist zu beachten, dass gegebenenfalls vorhandene Optionen in der Univention Configuration Registry-Variable **ldap/database/bdb/db_config_options** ergänzt werden.

- **Verteilen der Daten auf verschiedene Speichermedien**

Um auf Systemen mit großem LDAP-Verzeichnis die Gesamtperformance zu steigern, können BDB-Datenbank und BDB-Transaktionslog auf unterschiedlichen Speichermedien abgelegt werden.

Die Konfiguration erfolgt vergleichbar der Locking-Einstellungen über univention-config-registry.

Die Transaktionslogs von BDB können sehr groß werden. Über einen in BDB enthaltenen Mechanismus können nicht mehr benötigte Transaktions-Logs automatisch entfernt werden, dieser Mechanismus wird ebenfalls über Univention Configuration

Registry-Variablen aktiviert. Es müssen folgende Einstellungen vorgenommen werden:

```
ldap/database/bdb/db_config_options: set_flags
ldap/database/bdb/set_flags: DB_LOG_AUTOREMOVE
```

Informationen zu den weiteren Tools und Optionen zu BDB finden sich in der Online-Dokumentation der BerkeleyDB unter <http://www.sleepycat.com>.

3.3 OpenLDAP-ACLs

Der Zugriff auf die Informationen im LDAP-Verzeichnis wird serverseitig durch Access Control Lists (ACLs) geregelt. Die ACLs werden in der zentralen Konfigurations-Datei `/etc/ldap/slapd.conf` definiert und über Univention Configuration Registry verwaltet. Die `slapd.conf` wird dabei durch ein Multifile-Template verwaltet; weitere ACL-Elemente können unterhalb von `/etc/univention/templates/files/etc/ldap/slapd.conf.d/` zwischen den Dateien `60univention-ldap-server_acl-master` und `70univention-ldap-server_acl-master-end` eingefügt werden oder die bestehenden Templates erweitert werden.

Unter UCS gibt es darüberhinaus einige standardmässig installierte ACLs, die den Zugriff auf sensitive Daten unterbinden (z.B. auf das Benutzerpasswort) und für den Betrieb notwendige Regeln setzen (etwa nötige Zugriffe auf Rechnerkonten für Anmeldungen). Der lesende und schreibende Zugriff auf diese sensitiven Daten ist nur für die Mitglieder der Gruppe "Domain Admins" vorgesehen. Dabei werden auch enthaltene Gruppen unterstützt. Mit der Univention Configuration Registry-Variable `ldap/ac1/nestedgroups` kann diese Gruppen-in-Gruppen-Funktionalität für die LDAP-ACLs deaktiviert werden, wodurch eine Geschwindigkeitssteigerung bei den Verzeichnisdienst-Anfragen zu erwarten ist.

4 Lastverteilung

UCS-Systeme in der Standardkonfiguration für viele Dienste den den Domänencontroller Master als Anlaufpunkt. Mit steigender Anzahl von Clients ist die Verteilung der Abfragen auf andere Server notwendig.

Einige der auf einem Domänencontroller Master bei der Installation angebotenen Dienste sollten in komplexen Umgebungen daher auf anderen System installiert werden:

- Fileservices
- Druckservices
- Terminaldienste
- Mail

- HTTP-Proxy
- Paket-Repository
- Softwaredatenbank

Zentrale Dienste finden zwangsläufig ihren Anlaufpunkt am Domänencontroller Master, dazu einige Hinweise:

4.1 LDAP-Replikation

Die Replikation von Veränderungen am LDAP durch administrative Eingriffe oder Passwortänderungen hat immer ihren Ursprung auf dem Domänencontroller Master. Alle anderen UCS-Systeme (außer Thin Client und Basissystem) erfahren diese über den Univention Directory Notifier-Mechanismus und fragen die geänderten Datensätze ab. Für diese Anfrage kommen zunächst nur Systeme mit einer vollständigen Replik in Frage, die in einer UCS-Umgebung neben dem Domänencontroller Master nur auf dem Domänencontroller Backup zu finden ist.

Die Auswahl des anzufragenden Systems nimmt der Client beim Start des Listener-Dienstes oder Abbruch einer bestehenden Verbindung zufällig zwischen Domänencontroller Master und den zur Verfügung stehenden Domänencontroller Backups vor. Nur Domänencontroller Backups verbinden immer zum Domänencontroller Master. Zur Entlastung ist es also möglich, ein weiteres Domänencontroller Backup-System aufzusetzen. Sobald der Server im LDAP eingetragen ist, nehmen die Clients ihn in die Liste der abzufragenden Server auf.

Durch Setzen der Univention Configuration Registry-Variable **listener/ignoremaster** auf **yes** können Anfragen an den Domänencontroller Master deaktiviert werden. Vom lokalen Listener-Dienst werden Verbindungen dann nur noch zu Domänencontroller Backups aufgebaut.

Die zufällige Auswahl eines Servers kann durch Setzen der Univention Configuration Registry-Variablen **notifier/server** umgangen werden. Der hier eingetragene Hostname bzw. die eingetragene IP wird anschließend immer vom Listener verwendet. Diese Variable sollte daher nicht auf einem Domänencontroller Master- oder Domänencontroller Backup-System gesetzt werden.

Durch die Angabe des zu verwendenden Notifiers ist es jedoch möglich, die Replikation auch über Domänencontroller Slave-Server durchzuführen. Es ist bei verteilten Netzen beispielsweise sinnvoll, die UCS-Systeme (insbesondere Managed Clients und Mobile Clients) eines Standorts an einen lokalen Server zu binden. Ist dieser ein Domänencontroller Slave, kann dort ein Notifier über

```
apt-get install univention-directory-notifier
```

nachträglich installiert werden.

Bei allen Änderungen müssen die betroffenen Dienste neu gestartet werden.

4.2 Authentifikation

Die Authentifikation der meisten Dienste unter UCS erfolgt gegen einen LDAP-Server. Systeme ohne eigenen LDAP-Server (Memberserver, Managed-/Mobile-Clients) fragen dabei per Voreinstellung den Domänencontroller Master an. Ausnahme sind Thin-Clients, die bevorzugt den Terminalserver oder LDAP-Server in ihrem Subnetz verwenden.

Die Konfiguration des zu verwendenden Servers erfolgt durch die Univention Configuration Registry-Variablen *ldap/server/name* und *ldap/server/ip*, die auch durch eine LDAP-Server-Richtlinie gesetzt werden können. Es sollten also z.B. alle Clients und Memberserver eines Standorts oder einer Abteilung auf einen lokalen Domänencontroller Slave oder Domänencontroller Backup konfiguriert werden.

Hochfrequentierte Server (insbesondere Mailserver) sollten immer als Domänencontroller Slave installiert werden, so dass LDAP-Anfragen lokal abgearbeitet werden können.

4.3 Terminaldienste

UCS-Terminaldienste implementieren die Möglichkeit einer automatischen Lastverteilung auf mehrere Terminalserver. Die Konfiguration erfolgt durch Angabe mehrerer Server an der entsprechenden Thin-Client-Richtlinie.

Bei der Anmeldung des Benutzers fordert der Thin-Client von jedem der eingetragenen Server die aktuelle Auslastung an. Der Benutzer wird dann mit dem derzeit am geringsten belasteten Server verbunden. Dabei ist weniger die Zahl der dort angemeldeten Benutzer sondern mehr die Art der laufenden Prozesse entscheidend. Zusätzlich werden so Verbindungsversuche zu ausgefallenen Servern unterbunden.

Für Windows-Terminaldienste ist dieses Vorgehen nicht implementiert, da die Abfrage der aktuellen Auslastung von remote nicht möglich ist. Die Lastverteilung kann hier administrativ erfolgen, indem jeweils eine Gruppe von Thin-Clients einem Terminalserver zugeordnet wird. Alternativ kann ein DNS-Eintrag gewählt werden, dem mehrere IP-Adressen verschiedener Terminalserver zugeordnet werden. In beiden Fällen ist jedoch kein lastbezogener Ausgleich oder ein Schutz vor ausgefallenen Servern möglich.

5 Mailsysteme

Die Verarbeitung einer Mail auf einem vollständig konfigurierten UCS-System inklusive Spam- und Virenfilter erfordert eine große Anzahl von Datei- und LDAP-Operationen. Neben den bereits aufgeführten Optimierungen von LDAP-Indizes können weitere Maßnahmen vorgenommen werden.

5.1 Dateisystem

Das Mailsystem, bestehend aus Cyrus, Postfix, Spamassassin und Amavis, legt an verschiedenen Stellen im Dateisystem Daten ab, auf die unterschiedlich oft zugegriffen werden muss. Neben Optimierungen durch RAID-Systeme besteht die Möglichkeit, diese auf unterschiedlichen Medien abzulegen.

- `/var/log`
Während der Verarbeitung ein- und ausgehender Mails werden Logmeldungen erzeugt, die in diesem Verzeichnis abgelegt werden.
- `/var/spool/cyrus/mail`
Hier werden eingehende und in IMAP-Foldern abgelegte Mails von Cyrus gespeichert. In den Unterverzeichnissen a,...,z findet eine Zuordnung nach Benutzernamen statt, so dass es auf großen Servern möglich ist, die Datenhaltung weiter aufzuteilen.
- `/var/spool/postfix`
Postfix speichert die ein- und ausgehenden Mails in diesem Verzeichnis zwischen.

5.2 Logdateien

Cyrus legt je User eine Logdatei unter `/var/lib/cyrus/log` ab, in der benutzerbezogen jeder IMAP-Zugriff protokolliert wird. Diese Dateien erreichen schnell einige MB je User. Sie können, wenn keine Generierung von Logdateien gewünscht ist, gelöscht werden.

Soll das benutzerbezogene Logging wieder aktiviert werden genügt es, die entsprechende Datei über `touch` anzulegen und über `chown` dem User **cyrus** zuzuordnen. Cyrus erzeugt diese Dateien nur für neue Benutzer.

5.3 Dienste verteilen

Reichen die Kapazitäten eines Servers nicht zur Bearbeitung aller Mails, kann die Verteilung der Dienste auf mehrere Server sinnvoll sein. Dazu können verschiedene Ansätze gewählt werden. Die naheliegendste Umsetzung ist die Aufteilung der Mailempfänger auf unterschiedliche, z.B. standortbezogene Subdomains. Ein Server kann eine oder mehrere Subdomains übernehmen, die Registrierung erfolgt durch das Setzen der entsprechenden MX-Records über Univention Directory Manager im DNS. Zur detaillierten Konfiguration finden sich weitere Informationen im UCS-Handbuch.

Denkbar ist ebenfalls eine Aufteilung der Dienste auf verschiedene Server. So kann die Hauptlast für den Versand der Mails auf eigenständige Server für Postfix, Spamassassin und Amavis aufgeteilt werden. Der IMAP-Server Cyrus bietet weitere Möglichkeiten, über IMAP-Cluster den Mailzugriff auf verschiedene Server zu verteilen. Hier besteht derzeit kein vorgegebenes bzw. UCS-spezifisches Verfahren, so dass zur Konfiguration auf die Dokumentation der jeweiligen Dienste zurückgegriffen werden sollte.