

# UCS Performance Guide

Thema:	Univention Corporate Server Optimierungen	
Datum:	17. Mai 2010	
Seitenzahl:	<a href="#">13</a>	
Versionsnummer:	5493	
Autoren:	Univention GmbH	<a href="mailto:feedback@univention.de">feedback@univention.de</a>

## Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b>	<b>3</b>
<b>2</b>	<b>Entfernen nicht benötigter Dienste</b>	<b>3</b>
2.1	Identifizieren nicht benötigter Dienste . . . . .	3
2.2	Deaktivierung der Systemdienste . . . . .	4
2.3	Deinstallation der Systemdienste . . . . .	4
<b>3</b>	<b>Name Server Cache Daemon (NSCD)</b>	<b>4</b>
<b>4</b>	<b>OpenLDAP</b>	<b>5</b>
4.1	Indizes . . . . .	5
4.2	Konfiguration des Datenbank-Backends . . . . .	8
4.3	OpenLDAP-ACLs . . . . .	10
<b>5</b>	<b>Lastverteilung</b>	<b>10</b>
5.1	LDAP-Replikation . . . . .	10
5.2	Authentifikation . . . . .	11
5.3	Terminaldienste . . . . .	12
<b>6</b>	<b>Mailsysteme</b>	<b>12</b>
6.1	Dateisystem . . . . .	12
6.2	Logdateien . . . . .	13
6.3	Dienste verteilen . . . . .	13
<b>7</b>	<b>Squid</b>	<b>13</b>

## 1 Einführung

Bei der Installation von Univention Corporate Server werden die ausgewählten Serveranwendungen betriebsbereit vorkonfiguriert. 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 spezielle Bedürfnisse anzupassen.

## 2 Entfernen nicht benötigter 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. Dies 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 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 ein Dienst in der vorliegenden Umgebung benötigt wird, sollten für die Verfügbarkeit des Systems einige Basisdienste nicht beendet oder deaktiviert werden:

- **LDAP Server (slapd):** 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 für das Software-Repository benötigt.

- **OpenSSH:** Der SSH-Server stellt für die Remote-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 den 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 Nameserver Bind stellt DNS-Service-Records bereit, die ggf. von anderen Systemen in der UCS-Domäne verwendet werden.

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 die offenen Ports gehörenden Prozesse können mit den Befehlen `netstat` oder `lsof` identifiziert werden.

## 2.2 Deaktivierung der Systemdienste

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. Weitere Informationen finden sich im UCS-Handbuch im Abschnitt über die Univention Management Console.

## 2.3 Deinstallation der Systemdienste

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).

Weitere Informationen zur Deinstallation von Softwarepaketen finden sich im UCS-Handbuch im Kapitel über die Software-Verteilung.

# 3 Name Server Cache Daemon (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. In größeren Umgebungen kann eine Erweiterung sinnvoll sein. Weitere Hinweise finden sich im Basis-Systemdienste-Kapitel des UCS-Handbuchs.

## 4 OpenLDAP

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

Weitere Hinweise finden sich in der OpenLDAP-Dokumentation unter <http://www.openldap.org/doc/admin24/tuning.html>.

### 4.1 Indizes

OpenLDAP führt vergleichbar mit anderen Datenbanksystemen Indizes über häufig angefragte Attribute. Bei indizierten Attributen wird 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 Gesamtpformance profitiert jedoch 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 neuen UCS-Releases werden die voreingestellten Indizes häufig erweitert. Ab UCS 2.3-2 können die Indizes automatisch aktualisiert werden: Ist die Univention Configuration Registry-Variable `ldap/index/autorebuild` auf **yes** oder **true** gesetzt, so werden die auf dem System konfigurierten LDAP-Indizes automatisch ergänzt und das Kommando `slapindex` zum Neuaufbau der Indizes verwendet.

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 2.3-2)
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, homeDirectory, univentionUDMPropertyVersion, univentionUDMPropertyModule, univentionUDMPropertyShortDescription, univentionUDMPropertyLongDescription, univentionUDMPropertySyntax, univentionUDMPropertyMultivalue, univentionUDMPropertyDefault, univentionUDMPropertyLdapMapping, univentionUDMPropertyObjectClass, univentionUDMPropertyDeleteObjectClass, univentionUDMPropertyValueMayChange, univentionUDMPropertyLayoutTabName, univentionUDMPropertyLayoutOverwriteTab, univentionUDMPropertyLayoutOverwritePosition, univentionUDMPropertyLayoutPosition, univentionUDMPropertyCLIName, univentionUDMPropertyTranslationShortDescription, univentionUDMPropertyTranslationLongDescription, univentionUDMPropertyTranslationTabName, univentionUDMPropertyOptions, univentionUDMPropertyLayoutTabAdvanced, univentionUDMPropertyValueRequired, univentionUDMPropertyHook, univentionUDMPropertyDoNotSearch, univentionLicenseModule, cNAMERecord, univentionNagios-Hostname, univentionLicenseObject, sambaSIDList, sambaGroupType

ldap/index/pres	objectClass, uidNumber, gidNumber, memberUid, ou, uid, cn, sn, givenName, mail, description, displayName, uniqueMember, macAddress, dhcpHWaddress, krb5PrincipalName, aRecord, mailPrimaryAddress, mailAlternativeAddress, kolabHomeServer, univentionPolicyReference, homeDirectory, automountInformation, univentionUDMPropertyVersion, univentionUDMPropertyModule, univentionUDMPropertyShortDescription, univentionUDMPropertyLongDescription, univentionUDMPropertySyntax, univentionUDMPropertyMultivalue, univentionUDMPropertyDefault, univentionUDMPropertyLdapMapping, univentionUDMPropertyObjectClass, univentionUDMPropertyDeleteObjectClass, univentionUDMPropertyValueMayChange, univentionUDMPropertyLayoutTabName, univentionUDMPropertyLayoutOverwriteTab, univentionUDMPropertyLayoutOverwritePosition, univentionUDMPropertyLayoutPosition, univentionUDMPropertyCLIName, univentionUDMPropertyTranslationShortDescription, univentionUDMPropertyTranslationLongDescription, univentionUDMPropertyTranslationTabName, univentionUDMPropertyOptions, univentionUDMPropertyLayoutTabAdvanced, univentionUDMPropertyValueRequired, univentionUDMPropertyHook, univentionUDMPropertyDoNotSearch
ldap/index/sub	uid, cn, sn, givenName, mail, description, displayName, mailPrimaryAddress, mailAlternativeAddress, default, zoneName, sambaSID, automountInformation
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.

Bei Bedarf kann bei der Suche nach der Ursache für Performance-Probleme der Debug-Level des LDAP-Servers erhöht werden, damit für die Dauer der Analyse bei jedem Suchvorgang Hinweise in die Datei `/var/log/syslog` geschrieben werden, falls ein gesuchtes Attribut noch nicht indiziert ist. Die Meldungen entsprechen je nach Index-Typ einem der folgenden Beispiele:

```
slapd[3459] <= bdb_approx_candidates: (lastname) not indexed
slapd[3459] <= bdb_equality_candidates: (cNAMERecord) not indexed
slapd[3459] <= bdb_presence_candidates: (testAttribute) not indexed
slapd[3459] <= bdb_substring_candidates: (zoneName) not indexed
```

Da nur bei tatsächlichen Suchoperationen entsprechende Meldungen ausgegeben werden, ist es hier sinnvoll, direkt die realistischen, praxisrelevanten Systemoperationen auszulösen, deren Performance optimiert werden soll, und dabei die Log-Ausgaben zu beobachten. Um diese Meldungen zu aktivieren, kann die Univention Configuration Registry-Variable `ldap/debug/level` z.B. auf den Wert **stats** gesetzt und danach der LDAP-Serverprozess per `invoke-rc.d slapd restart` neu gestartet werden. Da die detaillierte Protokollierung sowohl die Performance des LDAP-Servers beeinträchtigt, als auch Plattenplatz für die Log-Dateien verbraucht, sollte abgewogen werden, zu welchem Zeitpunkt eine solche Analyse durchgeführt werden kann. Nach Abschluss sollte der Debug-Level wieder auf 0 zurückgesetzt und der LDAP-Server neu gestartet werden.

## 4.2 Konfiguration des Datenbank-Backends

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 über Univention Configuration Registry-Variablen statt, die die Datei `/var/lib/univention-ldap/ldap/DB_CONFIG` schreiben.

Die Univention Configuration Registry-Variable `ldap/database/bdb/set_cachesize` bestimmt die Größe des Cache, indem sie die verfügbare Menge in GB und Byte sowie die Anzahl der zu verwenden Blöcke im Arbeitsspeicher definiert. 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.

Die Univention Configuration Registry-Variable `ldap/database/bdb/set_lg_bsize` kontrolliert die maximale Größe des BDB-Transaktionslogs in Byte. Diese Dateien liegen ebenfalls im Datenverzeichnis und speichern angefragte Modifikation vor Ihrer Ausführung. Im Falle eines Abbruchs der Transaktion oder eines 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 `db4.7_stat` zur Verfügung. Bei laufendem LDAP-Server können u.a. aktuelle Informationen zur maximalen Cachegröße, Cachenutzung und Datensatz-Locking abgefragt werden. Der Aufruf des Tools sollte im Datenbank-Verzeichnis erfolgen.

Um zusätzliche Optionen zu setzen, kann eine kommaseparierte Liste der ge-

wünschten 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 `db4.7_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 `db4.7_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 kann in Univention Configuration Registry konfiguriert werden:

```
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-Variablen `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 Configuration 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. Dazu 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>.

### 4.3 OpenLDAP-ACLs

Der Zugriff auf die Informationen im LDAP-Verzeichnis wird serverseitig durch Access Control Lists (ACLs) geregelt. Allgemeine Hinweise zur Konfiguration von ACLs in UCS finden sich im Verzeichnisdienst-Kapitel des UCS-Handbuchs.

Unter UCS gibt es 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 sensitive 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.

## 5 Lastverteilung

UCS-Systeme verwenden in der Standardkonfiguration für viele Dienste 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 Systemen installiert werden:

- Fileservices
- Druckservices
- Terminaldienste
- Mail
- HTTP-Proxy
- Paket-Repository
- Softwaredatenbank

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

### 5.1 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-Variable `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 das Paket ***univention-directory-notifier*** nachträglich installiert werden. Dazu ist auf den Memberservern und den Clients durch die Univention Configuration Registry-Variable `notifier/server` der Domänencontroller Slave als Verzeichnisquelle einzutragen.

Bei allen Änderungen müssen die betroffenen Dienste neu gestartet werden.

## 5.2 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. 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.

## 5.3 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.

## 6 Mailsysteme

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

### 6.1 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/domain`  
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.

## 6.2 Logdateien

Cyrus kann je User eine Logdatei unter `/var/lib/cyrus/log` ablegen, 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.

## 6.3 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. **Cyrus Murder für UCS** ist als Zusatz-Komponente verfügbar.

## 7 Squid

Wird der Squid-Proxy-Dienst mit NTLM-Authentifizierung verwendet, erfolgt die Authentifizierung über den Winbind-Dienst. Die Kommunikation mit Winbind erfolgt über eine Art Queue, standardmässig werden bis zu fünf laufende NTLM-Anfragen parallel verarbeitet. Antwortet der Winbind-Dienst langsam oder erfolgen viele parallele Proxy-Anfragen, kann es passieren, dass die Obergrenze der Queue erreicht wird und der Benutzer von Squid einen Authentifizierungsfehler erhält. Ab UCS 2.3-2 kann die Queue-Größe durch die Univention Configuration Registry-Variable `squid/ntlmauth/children` konfiguriert werden.