

UCS 2.4 Release Notes

Thema:	Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 2.4
Datum:	31. August 2010
Seitenzahl:	11
Versionsnummer:	6415
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1	Überblick über wichtige Änderungen in UCS 2.4	3
1.1	Virtualisierung	3
1.2	Linux-Kernel	4
1.3	Samba	4
1.4	UCS-Managementsystem	4
1.5	Aktivierung des Management-Designs aus UCS 2.2	5
1.6	Univention Active Directory Connector	5
1.7	Kolab2 Webclient Horde	6
1.8	Quellcode	6
2	Vorbereitung und Durchführung des Release-Updates	7
2.1	Verwendung von 3rd-Party-Software	7
2.2	Vorbereitung des Release-Updates	7
2.3	Durchführung des Release-Updates	8
2.4	Nachbereitung und Prüfung des Updates	9
3	Empfohlene Anpassungen nach Durchführung des Updates	10
4	Paket-Abkündigungen (End Of Life)	10
4.1	Support für Cyrus 2.1	10
4.2	Unidump	10
4.3	LILO	10
4.4	PostgreSQL 7.4	11
4.5	Benutzerdefinierte Attribute	11
4.6	KDE 3	11

Mit UCS 2.4 bringt Univention das vierte Minor-Update für UCS 2 heraus. Um Probleme bei der Durchführung des Updates zu vermeiden und vom vollen Nutzen der neuen Funktionen zu profitieren, wird dringend empfohlen, die Hinweise in diesen Release Notes zu beachten.

Neben den einleitenden Informationen zur neuen Version muss besonders das Kapitel 1 beachtet werden.

Weitere Informationen zu UCS 2.4 finden sich auf den folgenden Seiten:

- Univention Webseite
http://www.univention.de/ucs_highlights_2x.html
- UCS-Dokumentation
<http://www.univention.de/dokumentation.html>
- Univention Supportdatenbank
<http://sdb.univention.de>
- Univention Wiki
<http://wiki.univention.de>
- Univention Forum
<http://forum.univention.de>

Alle UCS-Kunden mit laufendem Maintenancevertrag können von der vorhergehenden Version auf UCS 2.4 aktualisieren. Dazu gehören auch Nutzer der Free For Personal Use-Edition.

Univention sichert Maintenance-Updates von mindestens fünf Jahren für UCS 2 zu. Nach dem Erscheinen von UCS 3 wird UCS 2 unabhängig davon außerdem mindestens ein weiteres Jahr mit Maintenance-Updates unterstützt.

1 Überblick über wichtige Änderungen in UCS 2.4

Eine detaillierte Aufstellung aller Änderungen findet sich im Changelog zu UCS 2.4:

http://www.univention.de/fileadmin/produkte/pdf_dokumente/changelog-2.4.pdf

1.1 Virtualisierung

Mit **Univention Virtual Machine Manager** (UVMM) steht mit dem Release von UCS 2.4 ein neues grafisches Administrationswerkzeug zur Verfügung, mit dem UCS-Virtualisierungsserver überwacht und die virtuellen Maschinen auf diesen Systemen verwaltet werden können. Als Managementoberfläche dient ein Univention Management Console-Modul, welches auf einem System innerhalb der UCS-Domäne ausgeführt werden kann.

Als Virtualisierungstechnologien werden Xen und KVM unterstützt und über die Abstraktionsbibliothek libvirt angesprochen.

Xen steht in UCS 2.4 in der Version 3.4.3 zur Verfügung und kann sowohl mit Kernel 2.6.32, als auch mit Kernel 2.6.18 verwendet werden. Empfohlen ist der Einsatz auf Kernel 2.6.32.

Für KVM (Kernel-based Virtual Machine) in UCS 2.4 muss zwingend Kernel 2.6.32 eingesetzt werden.

1.2 Linux-Kernel

Der Linux-Kernel wurde auf Version 2.6.32 aktualisiert und ersetzt die bisherigen Kernel-Versionen 2.6.26 und 2.6.30. Wurde mit UCS 2.3 eine der beiden genannten Kernel-Versionen eingesetzt, so wird bei der Aktualisierung auf UCS 2.4 automatisch der Kernel in der Version 2.6.32 installiert und als Standard beim nächsten Systemstart verwendet. Die bisherigen Kernel-Versionen bleiben installiert und können im Notfall wieder gestartet werden.

Kernel 2.6.32 spricht IDE-PATA-Geräte mit anderen Gerätenamen als ältere Kernel an. Daher werden bei einem Update auf UCS 2.4 mit Kernel 2.6.32 Gerätenamen (/dev/sd* und /dev/hd*) in allen notwendigen Konfigurationsdateien auf die UUID-Notation umgeschrieben. Weitere Informationen dazu können unter folgender Adresse gefunden werden:

<http://sdb.univention.de/1140>

Bei Neuinstallationen wird als Voreinstellung die Kernel-Variante mit Unterstützung für 64 GB Hauptspeicher aktiviert ("bigmem"). Auf älteren Prozessoren (z.B. 486/Pentium) steht die dafür nötige PAE-Erweiterung nicht zur Verfügung. Auf diesen Systemen muss in der Kernel-Auswahl des UCS Installers stattdessen der Standard 686-Kernel ausgewählt werden.

Neben Kernel 2.6.32 steht auch weiterhin Kernel 2.6.18 zur Verfügung.

Der Kernel-Support für das verteilte Blockdevice DRBD ist im 2.6.32-Kernel integriert. Die Userspace-Tools für DRBD funktionieren nur mit dem DRBD-Kernel-Support aus 2.6.32. Soll DRBD mit dem 2.6.18-Kernel verwendet werden, müssen die Userspace-Tools manuell eingerichtet werden.

1.3 Samba

Die Standard-Samba-Version wurde auf Version 3.5.4 aktualisiert. Als Alternative zu Samba 3.5.4 kann weiterhin Samba 3.3 aus UCS 2.3 verwendet werden. Das genaue Vorgehen dazu ist in der Univention Supportdatenbank beschrieben:

<http://sdb.univention.de/1141>

1.4 UCS-Managementsystem

Das Online-Update-Modul wurde überarbeitet und in der Benutzerführung optimiert. Somit können spätere Aktualisierungen auf die nächsten UCS-Versionen noch einfacher durchgeführt werden. Auch das Einbinden von weiteren UCS-Komponenten wird dadurch deutlich einfacher.

Die Anmeldung an Univention Directory Manager und Univention Management Console kann nun in einem Single Sign On durchgeführt werden. Auch weitere Applikationen können in dieses

Single Sign On Verfahren integriert werden. Ausführliche Informationen dazu sind im Univention Wiki zu finden.

http://wiki.univention.de/index.php?title=Single-Sign-On_in_UDM_und_UMC

Passwortqualitätsprüfungen (Wörterbuchprüfungen, Sonderzeichen usw.) können nun zentral im Univention Directory Manager verwaltet werden und gelten für alle Passwort-Varianten (Kerberos, Samba, Posix), unabhängig über welches Verfahren das Passwort geändert wird. Die Aktivierung kann dabei richtlinienbasiert durchgeführt werden.

Optional können Benutzerkonten nun automatisch gesperrt werden, wenn ein Benutzer sein Passwort zu oft fehlerhaft eingegeben hat.

In der Benutzerverwaltung wurden die Checkboxen für **Deaktiviert** und **Gesperrt** in Auswahllisten umgewandelt. Hier besteht nun eine umfangreichere Auswahl der einzelnen Zustände. Zu beachten ist, dass eine gegenseitige Verbindung der einzelnen Zustände besteht: Wenn beispielsweise das Konto für LDAP/POSIX deaktiviert wird, so ist eine Windows Anmeldung nicht möglich, da hierfür ein gültiger LDAP/POSIX-Account benötigt wird.

Aus Sicherheitsgründen sollte ein nicht mehr zugelassener Benutzer immer sowohl deaktiviert, als auch gesperrt werden. Wird ein Benutzer nur deaktiviert aber nicht gesperrt, so sind weiterhin LDAP-Verbindungen mit der Benutzerkennung möglich. Weitere Hinweise sind im UCS 2.4-Handbuch im Kapitel Univention Directory Manager zu finden:

<http://www.univention.de/dokumentation.html>

Das Setzen von Dateisystemquota für Gruppen kann nun einfach über das Tool **univention-group-quota** durchgeführt werden. Dies führt vor allem in Umgebungen mit mehreren tausend Benutzern zu erheblichen Performancesteigerungen.

Die in das Managementsystem integrierten Nagios-Plugins wurden erweitert und erlauben nun beispielsweise auch die Überwachung von CUPS, Squid, Dansguardian, Software RAID, OPSI und des SMART-Status von Festplatten.

1.5 Aktivierung des Management-Designs aus UCS 2.2

In UCS 2.3 wurde ein neues Design für das Management-System eingeführt. Dieses ist das empfohlene Design und wird per Voreinstellung auch in UCS 2.4 verwendet. Das Design aus UCS 2.2 kann aber weiterhin verwendet werden. Das genaue Vorgehen dazu ist in der Univention Supportdatenbank beschrieben:

<http://sdb.univention.de/1143>

1.6 Univention Active Directory Connector

Der Univention Active Directory Connector unterstützt nun vollständig die 64-Bit-Varianten von Windows Server, beispielsweise Windows 2008 R2.

Mit der AD Connector-Version aus UCS 2.4 kann derzeit keine SSL-gesicherte LDAP-Verbindung zum Active Directory eines Windows 2000 Server aufgebaut werden. Windows

2003 und spätere Versionen sind nicht betroffen. Um den Univention AD Connector mit Windows 2000 einsetzen zu können, muss deshalb die Univention Configuration Registry-Variable `connector/ad/ldap/ssl` auf **no** gesetzt werden. Die Kommunikation mit dem Passwortdienst und somit die Synchronisation von Passworthashes ist davon nicht betroffen, dies erfolgt weiter per SSL.

Zusätzlich muss unter Microsoft Windows 2000 der Passwort-Dienst manuell registriert werden. Dazu müssen die folgenden Befehle in einer Kommandozeile eingegeben werden:

```
c:\winnt\UCS-AD-Connector\ucs-ad-connector.exe -install
net start "UCS AD Connector"
sc config "UCS AD Connector" start= auto
```

1.7 Kolab2 Webclient Horde

Der Kolab2 Webclient Horde wurde auf Version 1.2.5 aktualisiert. Mit dieser Version steht das Univention-Farbschema nicht mehr zur Verfügung. Standardmäßig wird bei neuen Benutzern das Farbschema **Silver Surfer** konfiguriert. Es wird empfohlen alle Benutzer auf dieses Farbschema umzustellen.

Ein per SyncML angeschlossener Client verdoppelt neu hinzugefügte Kontakte, die nicht über den Kolab2 Webclient Horde angelegt wurden, nachdem der SyncML Client mehrfach synchronisiert hat. Univention wird dafür in Kürze einen Hotfix bereitstellen. Weitere Informationen dazu sind im Univention Bugzilla zu finden:

https://forge.univention.org/bugzilla/show_bug.cgi?id=19757

1.8 Quellcode

Der Quellcode zu den von Univention entwickelten UCS-Paketen wird jetzt unter der Lizenz GNU AGPL V3 (bisher: GNU GPL V2) veröffentlicht. Neben der Möglichkeit zum Download der Quellcodepakete stehen aktuelle Quellcodeversionen nun auch im öffentlichen SVN zur Verfügung. Weitere Informationen:

<http://wiki.univention.de/index.php?title=Source-Download>

1.8.1 Wichtige Programmaktualisierungen

- OpenLDAP 2.4.23
- OpenOffice.org 3.2
- Firefox 3.6
- Adobe Reader 9.3
- Dojo 1.4.3

2 Vorbereitung und Durchführung des Release-Updates

Die Hinweise zu Paketen und Neuerungen in den folgenden Abschnitten müssen auf Auswirkungen in der Zielumgebung für das Update geprüft werden. Es wird dringend empfohlen, das Update in einer Testumgebung zu testen.

Falls Ihnen von Univention angepasste Paketversionen bereitgestellt wurden, so muss geprüft werden, ob die angepassten Pakete durch die Aktualisierung auf UCS 2.4-0 überschrieben werden – vorzugsweise in einer Testumgebung. Sollten Sie hier Probleme feststellen oder die ursprünglichen Anpassungen für die aktuellen UCS-2.4-Paketversionen benötigen, so wenden Sie sich bitte an Univention.

Für Scalix für UCS, UCS TCS 3.0, UCD 3.0 und UCS@school werden Updates zur Verwendung dieser UCS-Erweiterungen mit UCS 2.4 erst nach dem Release von UCS 2.4 bereitgestellt werden. Falls eine dieser Erweiterungen verwendet wird, muss mit der Aktualisierung der UCS-Installation noch gewartet werden.

2.1 Verwendung von 3rd-Party-Software

Bei der Verwendung von 3rd-Party-Software ist **vor** dem Update mit dem Hersteller/Vertriebspartner der 3rd-Party-Software zu klären, ob diese mit der neuen Version von Univention Corporate Server weiterhin uneingeschränkt einsetzbar ist.

Updates für Produkte Dritter, die zusammen mit UCS ausgeführt werden können oder UCS als Basis verwenden, werden nicht durch Univention veröffentlicht, sondern durch die jeweiligen Hersteller oder Vertriebspartner.

2.2 Vorbereitung des Release-Updates

Vor dem Update muss ein vollständiges Backup des zu aktualisierenden Systems durchgeführt werden. Es ist sicherzustellen, dass das System aus dem Backup wieder vollständig hergestellt werden kann.

Vor der Aktualisierung muss geprüft werden, ob keine Probleme mit dem aktuellen System bestehen, die zu Fehlern während des Updates führen können. Dazu sind u. a. die folgenden Schritte durchzuführen:

- Es muss sichergestellt werden, dass keine nicht von Univention oder einem anderen Hersteller für UCS herausgegebenen Pakete installiert sind, beispielsweise lokal installierte Debian-Pakete. Diese können die Auflösung der Paketabhängigkeiten während der Installation stören.
- Die Aktualisierung von UCS auf die Version 2.4 darf nur auf UCS 2.3-2 Systemen durchgeführt werden. Dabei dürfen keine unvollständig installierten Pakete vorhanden sein. Dies kann etwa mit dem Software-Monitor aus der Univention Management Console geprüft werden.

- Es sollte ausreichend freier Festplattenplatz vorhanden sein. Mit weniger als 5GB freiem Festplattenplatz darf das Update nur dann durchgeführt werden, wenn die Funktionsfähigkeit des Updates zuvor auf einem Testsystem mit gleicher Softwareauswahl nachgewiesen wurde.
- Wenn ein System aktualisiert wird, auf dem virtualisierte Xen-Instanzen betrieben werden, müssen die Xen-Instanzen vor dem Update beendet werden.

2.3 Durchführung des Release-Updates

Ein wesentlicher Aspekt bei der Entwicklung und Pflege von UCS ist die durchgehende Update-Fähigkeit: Eine UCS-Installation kann ohne größere Eingriffe auf die jeweils folgende Version aktualisiert werden. Dazu veröffentlicht Univention die Pakete in einem Online Repository. Zusätzlich stehen parallel zu den Installations-DVDs für ein neues UCS-Release Update-DVDs in Form von ISO-Images zur Verfügung.

Bei einem UCS-Release-Update können aktualisierte Pakete zuerst in ein innerhalb der eigenen Infrastruktur betriebenes Repository eingespielt werden, um danach die UCS-Systeme der Domäne aus diesem Repository zu aktualisieren.

Beim Einspielen eines Release-Updates in einer UCS-Umgebung muss das System mit der Rolle **Domaincontroller Master** als erstes System aktualisiert und neu gestartet werden, anschließend sollten die vorhandenen Domänencontroller Backup-Systeme aktualisiert werden. Nach dem Einspielen eines Release-Updates muss das entsprechende System neu gestartet werden.

Es wird empfohlen, Release-Updates über die lokale Console oder entsprechende Tools, beispielsweise `at` oder `screen`, einzuspielen, da insbesondere beim Aktualisieren über eine SSH-Sitzung oder an einem Thin Client die Verbindung zwischen den Rechnern abrechen kann.

UCS-Release-Updates werden auf dem UCS-System mit dem Kommando `univention-updater` oder über das **Online Updates**-Modul in Univention Management Console installiert. Das Kommando `univention-updater` unterstützt dabei die folgenden Varianten:

- Über den Befehl `univention-updater cdrom` kann ein System von einer eingelegten Update-DVD aktualisiert werden. Standardmäßig wird über das Kommando `mount /cdrom` die DVD eingehängt. Mit dem Parameter `--iso` kann direkt die ISO-Abbilddatei der Update-DVD angegeben werden. Falls ein lokales Repository vorhanden ist, so wird dies zunächst aktualisiert und anschließend wird das lokale Repository für die Aktualisierung verwendet.
- Um ein System von einem bereits aktualisierten Repository, beispielsweise dem Online Repository (apt.univention.de), auf ein neues Release zu aktualisieren, wird `univention-updater net` verwendet. Auch in diesem Fall wird ein vorhandenes lokales Repository zuerst aktualisiert. Die anschließende System-Aktualisierung verwendet dann das lokale Repository.
- Falls ein UCS-Release-Update bereits in das lokale Repository des Systems eingespielt worden ist, kann `univention-updater local` aufgerufen werden. Dann wird für die Aktualisierung direkt das lokale Repository verwendet.

In jedem Fall kann über den Parameter `--update-to` angegeben werden, bis zu welcher Version ein System aktualisiert werden soll. Höhere Versionsnummern werden somit nicht installiert.

Am Ende des Updates sollte die folgende Ausgabe erscheinen:

```
System is up to date (UCS 2.4-0)
```

Erscheint diese Meldung nicht, so sollte die Datei `/var/log/univention/updater.log` auf Fehlermeldungen untersucht werden. Weiterhin sind die Hinweise in Kapitel 2.4 zu beachten. Zusätzliche Informationen können in der Univention Support-Datenbank <http://sdb.univention.de> und im Univention Forum <http://forum.univention.de> gefunden werden.

2.4 Nachbereitung und Prüfung des Updates

Nach dem Update müssen die Systeme neu gestartet werden. Wenn der Domänencontroller Master aktualisiert wurde, sollten Managed und Mobile Clients sowie Memberserver ebenfalls neu gestartet werden.

Nach dem Update sollte auf jedem System überprüft werden, ob alle Join-Skripte ausgeführt wurden. Dies kann entweder über die Univention Management Console oder über das Kommandozeilen-Tool `univention-run-join-scripts` durchgeführt werden.

Um sicherzustellen, dass für das Update genug Platz in dem Verzeichnis `/boot` ist, werden vorab die Sicherungskopien der `initrd`-Dateien, in das Verzeichnis `/var/backups/univention-initrd.bak/` verschoben. Sollten diese nicht mehr benötigt werden, kann das Verzeichnis nach dem Update gelöscht werden.

Zusätzlich empfiehlt es sich zu prüfen, ob alle installierten Kernel-Versionen auf dem System noch benötigt werden und gegebenenfalls ältere Versionen zu deinstallieren. Die Deinstallation kann über das folgende Kommando durchgeführt werden:

```
apt-get remove linux-image-<Version des Kernels>
```

Das System muss nach dem Update mit der Versionsnummer "2.4-0-0" am Bootprompt starten. Ob alle Softwarepakete aktualisiert wurden, kann über den zentralen Softwaremonitor oder die lokale Univention Management Console geprüft werden. Der vollständige Verlauf des Updates ist in der Datei `/var/log/univention/updater.log` protokolliert.

Über das Kommando `apt-get update; apt-get dist-upgrade` kann geprüft werden, ob Pakete nicht aktualisiert, sondern zurückgehalten wurden. Das sollte besonders beim Einsatz von Nicht-Standardpaketen geprüft werden. Dies löst die Meldung **The following packages have been kept back:** aus.

3 Empfohlene Anpassungen nach Durchführung des Updates

MD5 ist eine kryptografische Einwegfunktion, die in UCS-Versionen bis 2.2 für die Generierung der Rechner-SSL-Zertifikate verwendet wurde. Verschiedene kryptografische Analysefortschritte der letzten Jahre haben gezeigt, dass MD5 gegenüber dem Hash-Algorithmus SHA-1 Schwächen aufweist. Seit UCS 2.3 setzt `univention-ssl` bei der Generierung von Zertifikaten deshalb standardmässig SHA-1 ein. Ältere Zertifikate sollten ggf. neu generiert werden. Der Hash-Algorithmus eines Zertifikates kann folgendermassen ermittelt werden:

```
univention-certificate list
univention-certificate dump -name ZERTIFIKATSNAME \
    | grep "Signature Algorithm"
```

Wenn in der Ausgabe ***sha1WithRSAEncryption*** erscheint, wird SHA-1 eingesetzt, wird dort ***md5WithRSAEncryption*** angezeigt, kommt MD5 zum Einsatz.

Die Aktualisierung der SSL-Zertifikate ist in der Univention Support Datenbank beschrieben: <http://sdb.univention.de/1000>

4 Paket-Abkündigungen (End Of Life)

4.1 Support für Cyrus 2.1

UCS 2.x verwendet Cyrus 2.2. Alte Installationen, die noch im inkompatiblen 2.1-Format betrieben werden, müssen innerhalb der UCS 2.x-Serie migriert werden, da die Unterstützung für dieses Format in UCS 3.0 entfernt werden wird. Die Cyrus-Migration ist in einem technischen Dokument (***Cyrus-Migration***) beschrieben, das von der Univention-Webseite bezogen werden kann:

http://www.univention.de/doku_admin.html

4.2 Unidump

Unidump wird in UCS 3.0 nicht mehr enthalten sein. Univention empfiehlt den Wechsel auf Bacula, das über das Paket ***univention-bacula*** installiert werden kann.

4.3 LILO

Der Bootloader LILO wird in UCS 3.0 nicht mehr enthalten sein. Das Update von LILO auf GRUB wird unter <http://sdb.univention.de/1072> genauer beschrieben.

4.4 PostgreSQL 7.4

PostgreSQL 7.x wird in UCS 3.0 nicht mehr unterstützt werden. Die Migration auf PostgreSQL 8.3 wird empfohlen.

4.5 Benutzerdefinierte Attribute

In UCS 2.2 wurde die Möglichkeit eingeführt, Erweiterungen des Univention Directory Managers durch erweiterte Attribute vorzunehmen. Der Funktionsumfang dieser Attribute ist deutlich umfangreicher als die schon länger in UCS verfügbaren benutzerdefinierten Attribute. In UCS 3.0 werden die benutzerdefinierten Attribute nicht mehr unterstützt.

4.6 KDE 3

KDE 3 wird mit UCS 3.0 nicht mehr unterstützt. Mit Univention Corporate Desktop 3 steht bereits ein aktualisierter Linux-Desktop auf Basis von KDE 4 für UCS bereit.