

UCS 3.2-6 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 3.2-6**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2015 Univention GmbH

Mary-Somerville-Straße 1, 28359 Bremen, Deutschland/Germany

<feedback@univention.de>

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

Inhaltsverzeichnis

1. Univention Corporate Server (UCS) 3.2-6	4
2. Empfohlene Update-Reihenfolge für Umgebungen mit mehr als einem UCS-Server	5
3. Vorbereitung des Updates	6
4. Nachbereitung des Updates	7
4.1. Betrieb eines lokalen Repository-Servers / Preup- und Postup-Skripte	7
5. Hinweise zum Einsatz einzelner Pakete	8
5.1. Erfassung von Nutzungsstatistiken bei Verwendung der Free-For-Personal-Use-Version.....	8
5.2. UEFI-Installations-DVD	8
5.3. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit	8
5.4. Empfohlene Browser für den Zugriff auf Univention Management Console	8
5.5. Einschränkungen im Samba 4-Betrieb	9
5.6. Installation in <i>VirtualBox</i>	9
5.7. Installation in <i>Citrix XenServer</i>	9
5.8. Migration einer Samba 3-Umgebung auf Samba 4	9
5.9. Xen	10
6. Changelog	11
6.1. General	11
6.2. Basic system services	12
6.2.1. Linux kernel and firmware packages	12
6.2.2. Quota	12
6.3. Domain services	12
6.3.1. OpenLDAP	12
6.4. Univention Management Console	12
6.4.1. Univention Management Console web interface	12
6.4.2. Online update module	12
6.5. Software deployment	13
6.5.1. Software deployment command line tools	13
6.6. Univention Library	13
6.7. System services	13
6.7.1. Mail services	13
6.8. Services for Windows	13
6.8.1. Samba	13
6.8.2. Univention S4 Connector	13
6.9. Other changes	13
Literaturverzeichnis	14

Kapitel 1. Univention Corporate Server (UCS) 3.2-6

Mit Univention Corporate Server 3.2-6 steht das sechste Point-Release für Univention Corporate Server (UCS) zur Verfügung. Vorhandene UCS-Systeme können über das von Univention bereitgestellte Online-Repository aktualisiert werden. Alternativ können Updates über eine Update-DVD eingespielt werden. Für Neuinstallationen stehen UCS 3.2-6 ISO-Images zur Verfügung. UCS 3.2-6 beinhaltet alle für UCS 3.2-5 veröffentlichten Errata-Updates. Die wichtigsten Änderungen im Überblick:

- Das Release enthält diverse Sicherheitsupdates, die in den letzten Wochen und Monaten für UCS 3.2-5 als Errata Updates veröffentlicht wurden. U.a. enthalten sind aktualisierte Pakete für den **Linux Kernel**, **OpenSSL**, **glibc**, **sudo**.
- Diverse Tools aus dem PAM Stack unterstützen nun die Konfiguration von mehreren LDAP Servern. Eine solche Konfiguration kann genutzt werden, um die generelle Ausfallsicherheit zu erhöhen.
- In großen Umgebungen wurde die Login Performance verbessert: Aufwendige Quota Abfragen wurden dazu aus dem Login Prozess ausgelagert.
- Sofern UCS die Netzwerkeinstellungen via DHCP bezieht, werden nun weitere Parameter ausgewertet, wie bspw. Routing-Informationen.

Kapitel 2. Empfohlene Update-Reihenfolge für Umgebungen mit mehr als einem UCS-Server

In Umgebungen mit mehr als einem UCS-System muss die Update-Reihenfolge der UCS-Systeme beachtet werden:

Auf dem Domänencontroller Master wird die maßgebliche (authoritative) Version des LDAP-Verzeichnisdienstes vorgehalten, die an alle übrigen LDAP-Server der UCS-Domäne repliziert wird. Da bei Release-Updates Veränderungen an den LDAP-Schemata auftreten können, muss der Domänencontroller Master bei einem Release-Update immer als erstes System aktualisiert werden.

Generell ist es empfehlenswert, alle UCS-Systeme möglichst in einem Wartungsfenster zu aktualisieren.

Kapitel 3. Vorbereitung des Updates

Es sollte geprüft werden, ob ausreichend Festplattenplatz verfügbar ist. Eine Standard-Installation benötigt min. 6 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation mindestens 1 GB weiteren Speicherplatz zum Herunterladen und Installieren der Pakete.

Für das Update sollte eine Anmeldung auf der lokalen Konsole des Systems mit dem Benutzer `root` durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über Univention Management Console durchgeführt werden.


Eine Remote-Aktualisierung über SSH wird nicht empfohlen, da dies beispielsweise bei Unterbrechung der Netzverbindung zum Abbruch des Update-Vorgangs und zu einer Beeinträchtigung des Systems führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können beispielsweise die Tools `screen` oder `at` eingesetzt werden, die auf allen Systemrollen installiert sind.

Kapitel 4. Nachbereitung des Updates

Nach dem Update müssen die neuen oder aktualisierten Join-Skripte ausgeführt werden. Dies kann auf zwei Wegen erfolgen: Entweder über das UMC-Modul **Domänenbeitritt** oder durch Aufruf des Befehls `univention-run-join-scripts` als Benutzer `root`.

Anschließend muss das UCS-System neu gestartet werden.

4.1. Betrieb eines lokalen Repository-Servers / Preup- und Postup-Skripte

Feedback 

Preup- und Postup-Skripte sind Skripte, die vor und nach Release-Updates aufgerufen werden (z.B. zur Nachbereitung des Updates, etwa die Deinstallation nicht mehr benötigter Pakete). Ab UCS 3.2 werden diese Skripte kryptographisch signiert, um eine unerlaubte Modifikation zu verhindern. Beim Update und Spiegeln der Repository-Inhalte werden diese Signaturen überprüft. Sind diese ungültig oder fehlen, so wird die Aktion abgebrochen.

Wird ein Repository-Server mit UCS 3.1-x betrieben, muss dieser auf UCS 3.2 aktualisiert werden, bevor weitere Systeme auf UCS 3.2-1 oder neuer aktualisiert werden können.

Wenn ein Update des Repository-Servers nicht möglich ist, müssen die Dateien mit den Signaturen manuell heruntergeladen werden:

```
LOCAL_DIR="/var/lib/univention-repository/mirror"
SERVER="http://updates.software-univention.de"
for release in 3.2-0 3.2-1 3.2-2 3.2-3 3.2-4 3.2-5 3.2-6; do
  for script in preup postup; do
    file="3.2/maintained/$release/all/$script.sh.gpg"
    wget -O "$LOCAL_DIR/$file" "$SERVER/$file"
  done
done
```

Alternativ kann die Prüfung der Signaturen auch deaktiviert werden, was ein Sicherheitsrisiko darstellen kann. Für den Repository-Server kann dazu die Univention Configuration Registry-Variable `repository/mirror/verify` auf `false` gesetzt werden. Für das Update muss auf allen Systemen die Univention Configuration Registry-Variable `repository/online/verify` auf `false` gesetzt werden.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken bei Verwendung der Free-For-Personal-Use-Version

Bei Verwendung der Free for personal use-Version von UCS (die in der Regel für Evaluationen von UCS herangezogen wird) werden anonyme Nutzungsstatistiken zur Verwendung der Univention Management Console erzeugt. Die aufgerufenen Module werden dabei von einer Instanz des Web-Traffic-Analyse-Tools Piwik protokolliert. Dies ermöglicht es Univention die Entwicklung von Univention Management Console besser auf das Kundeninteresse zuzuschneiden und Usability-Verbesserungen vorzunehmen.

Diese Protokollierung erfolgt nur bei Verwendung der Free-for-Personal-Use-Lizenz. Der Lizenzstatus kann durch einen Klick auf das Zahnrad-Symbol in der rechten, oberen Ecke der Univention Management Console und die Auswahl von **Lizenzinformationen** geprüft werden. Steht hier unter **Lizenztyp Free for personal use edition** wird eine solche Version verwendet. Bei Einsatz einer regulären UCS-Lizenz erfolgt keine Teilnahme an der Nutzungsstatistik.

Die Protokollierung kann unabhängig von der verwendeten Lizenz durch Setzen der Univention Configuration Registry-Variable `umc/web/piwik` auf `false` deaktiviert werden.

5.2. UEFI-Installations-DVD

Für die Architektur *amd64* steht neben der Standard-Installations-DVD auch ein Medium mit Unterstützung für den Unified Extensible Firmware Interface-Standard (UEFI) bereit.

Auf Systemen, die nur einen UEFI-Start unterstützen, muss die UEFI-Installations-DVD anstelle der Standard-DVD verwendet werden.

5.3. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit

WebKit, Konqueror und QtWebKit werden in UCS im maintained-Zweig des Repositorys mitgeliefert, aber nicht durch Sicherheits-Updates unterstützt. WebKit wird vor allem für die Darstellung von HTML-Hilfeseiten u.ä. verwendet. Als Web-Browser sollte Firefox eingesetzt werden.

5.4. Empfohlene Browser für den Zugriff auf Univention Management Console


Univention Management Console verwendet für die Darstellung der Web-Oberfläche zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden empfohlen:

- Chrome ab Version 14
- Firefox ab Version 10
- Internet Explorer ab Version 9

- Safari (auf dem iPad 2)

Auf älteren Browsern können Darstellungs- oder Performanceprobleme auftreten.

5.5. Einschränkungen im Samba 4-Betrieb


Feedback 

In Samba 4 stehen einige Funktionen des *Active-Directory* nicht vollständig zur Verfügung:

- Microsoft Windows Domänencontroller dürfen nicht einer Samba 4-Domäne beitreten und umgekehrt.
- Eine selektive Replikation ist mit Samba 4 nicht möglich, da diese durch Active Directory prinzipiell nicht unterstützt wird (in UCS@school basiert die selektive Replikation auf der Listener/Notifier-Replikation).
- Samba 4 unterstützt keine Forest-Domänen.
- Samba 4 unterstützt keine Vertrauensstellungen.

Weitere Hinweise finden sich in Kapitel 8 des [ucs-handbuch].


5.6. Installation in *VirtualBox*

Feedback 

Bei der Installation von UCS in der Virtualisierungslösung *VirtualBox* vor Version 4.2 kann folgender *VirtualBox*-Bug auftreten: Wenn von der Installations-DVD gebootet wird, bietet GRUB die Option **Boot from first harddisk partition** an. Wählt man diese Option aus, friert *VirtualBox* ein.

Zur Abhilfe muss vor dem Neustart der virtuellen Maschine entweder die Installations-DVD aus den Laufwerkseinstellungen der *VirtualBox*-VM entfernt werden oder beim Start der virtuellen Instanz **F12** gedrückt und die Festplatte als Bootpartition ausgewählt werden. UCS startet danach dann problemlos.

5.7. Installation in *Citrix XenServer*


Feedback 

Bei der Installation von UCS in der Virtualisierungslösung *Citrix XenServer 6.0 - 6.2* wird mit der standardmässig emulierten *Cirrus*-Grafikkarte das GRUB-Menü des Univention Installers nicht angezeigt. Der Univention Installer kann durch Drücken der **ENTER**-Taste direkt gestartet werden; alternativ startet die Installation automatisch nach sechzig Sekunden. Der dann gestartete Univention Installer wird normal dargestellt.

Um GRUB korrekt darzustellen, kann die von *XenServer* emulierte Grafikkarte umkonfiguriert werden. Dazu muss eine Anmeldung als Benutzer `root` auf dem *XenServer*-System folgen. Mit dem Befehl `xe vm-list` muss zuerst die UUID der virtuellen Maschine ermittelt werden. Mit dem folgenden Befehl wird dann die emulierte Grafikkarte auf VGA umkonfiguriert:

```
xe vm-param-set uuid=UUIDVM platform:vga=std
```

5.8. Migration einer Samba 3-Umgebung auf Samba 4

Feedback 

Es existieren zwei grundlegende Verfahren zur Migration von Samba 3 auf Samba 4:

- Aufbau einer parallelen Samba 4-Domäne. Beide Domänen verwenden unterschiedliche NetBIOS-Namen und SIDs. Die Clients treten dann schrittweise der Samba 4-Domäne bei.
- Migration aller Systeme innerhalb eines Wartungsfensters.

Beide Verfahren sind im Univention Wiki ausführlich dokumentiert: http://wiki.univention.de/index.php?title=Migration_from_Samba_3_to_Samba_4.


5.9. Xen

Wenn der Xen Hypervisor benutzt wird und das Speicherlimit über die Univention Configuration Registry-Variable `grub/xenhopt` begrenzt wurde, sollte der Wert aktualisiert und um die `,max:-`Angabe erweitert werden. Weitere Details finden sich unter http://wiki.univention.de/index.php?title=UVMM_Quickstart-3.1#Konfiguration_der_Dom0.

Kapitel 6. Changelog

Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit UCS 3.2-5:

6.1. General

Feedback 

All security updates issued for UCS 3.2-5 are included:


- **cairo** (CVE-2013-7439) (Bug 38251)
- **eglibc** (CVE-2012-3405 CVE-2012-3406 CVE-2012-3480 CVE-2012-4412 CVE-2012-4424 CVE-2013-0242 CVE-2013-1914 CVE-2013-4237 CVE-2013-4332 CVE-2013-4357 CVE-2013-4458 CVE-2013-4788 CVE-2013-7423 CVE-2013-7424 CVE-2014-4043) (Bug 37644)
- **firefox-de** (CVE-2015-0801 CVE-2015-0807 CVE-2015-0813 CVE-2015-0815 CVE-2015-0816 CVE-2015-0817 CVE-2015-0818 CVE-2015-0822 CVE-2015-0827 CVE-2015-0831 CVE-2015-0835 CVE-2015-0836) (Bug 37882 Bug 38180)
- **firefox-en** (CVE-2015-0801 CVE-2015-0807 CVE-2015-0813 CVE-2015-0815 CVE-2015-0816 CVE-2015-0817 CVE-2015-0818 CVE-2015-0822 CVE-2015-0827 CVE-2015-0831 CVE-2015-0835 CVE-2015-0836) (Bug 37882 Bug 38180)
- **FreeType** (CVE-2014-9656 CVE-2014-9657 CVE-2014-9658 CVE-2014-9660 CVE-2014-9661 CVE-2014-9663 CVE-2014-9664 CVE-2014-9666 CVE-2014-9667 CVE-2014-9669 CVE-2014-9670 CVE-2014-9671 CVE-2014-9672 CVE-2014-9673 CVE-2014-9675) (Bug 37756)
- **krb5** (CVE-2014-4341 CVE-2014-4342 CVE-2014-4343 CVE-2014-4344 CVE-2014-5352 CVE-2014-4345 CVE-2014-9421 CVE-2014-9422 CVE-2014-9423) (Bug 37680)
- **libSDL1.2** (CVE-2013-7439) (Bug 38251)
- **libX11** (CVE-2013-7439) (Bug 38251)
- **libXext** (CVE-2013-7439) (Bug 38251)
- **libXfixes** (CVE-2013-7439) (Bug 38251)
- **libXi** (CVE-2013-7439) (Bug 38251)
- **libXrandr** (CVE-2013-7439) (Bug 38250)
- **libXrender** (CVE-2013-7439) (Bug 38251)
- **libXv** (CVE-2013-7439) (Bug 38251)
- **Linux** (CVE-2013-7421 CVE-2014-3645 CVE-2014-3646 CVE-2014-3690 CVE-2014-8133 CVE-2014-8134 CVE-2014-9419 CVE-2014-9420 CVE-2014-9529 CVE-2014-9584 CVE-2014-9585 CVE-2014-9644 CVE-2014-9683 CVE-2015-1421 CVE-2015-1593) (Bug 37353)
- **ntp** (CVE-2014-9297 CVE-2014-9298) (Bug 37703)
- **OpenJDK-6** (CVE-2014-3566 CVE-2014-6585 CVE-2014-6587 CVE-2014-6591 CVE-2014-6593 CVE-2014-6601 CVE-2015-0383 CVE-2015-0395 CVE-2015-0407 CVE-2015-0408 CVE-2015-0410 CVE-2015-0412) (Bug 37576)

- **OpenSSL** (CVE-2015-0209 CVE-2015-0286 CVE-2015-0287 CVE-2015-0288 CVE-2015-0289 CVE-2015-0292) (Bug 37959)
- **Open-VM-tools** (CVE-2013-7439) (Bug 38251)
- **PostgreSQL-8.4** (CVE-2015-0241 CVE-2015-0243 CVE-2015-0244 CVE-2014-8161) (Bug 37703)
- **sudo** (CVE-2014-0106 CVE-2014-9680) (Bug 37853)
- **TeXLive-bin** (CVE-2013-7439) (Bug 38251)
- **TightVNC** (CVE-2013-7439) (Bug 38251)
- **xen-4.1** (CVE-2015-2044 CVE-2015-2045 CVE-2015-2151 CVE-2015-3456) (Bug 37956 Bug 38173)
- **xserver-xorg-video-vmware** (CVE-2013-7439) (Bug 38251)

6.2. Basic system services


Feedback 

6.2.1. Linux kernel and firmware packages

Feedback 


- The Linux kernel has been updated to 3.10.71. This provides many bugfixes (Bug 37353).

6.2.2. Quota


Feedback 

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed in the script `univention-user-quota` (Bug 38078).
- An error message about an unbound variable has been removed from the script `univention-group-quota` (Bug 38079).
- The quota settings are now written to a cache directory by a listener module. The PAM script which sets the quota settings to the share uses this cache directory. This improves the login performance (Bug 36989).

6.3. Domain services

Feedback 

6.3.1. OpenLDAP


Feedback 

- If a password has been changed via Samba 4, the account expiry setting was not always considered. This has been fixed (Bug 31429).
- The file `msgpo.schema` adjusted in UCS 3.2-5 erratum 276 would get replaced by a not-adjusted version during an update to UCS 4.0. This erratum avoids this by implementing a `dpkg` diversion for that file, which will get removed again in an erratum for UCS 4.0-2 (Bug 38488).

6.4. Univention Management Console


Feedback 

6.4.1. Univention Management Console web interface

Feedback 


- The navigation arrow is now shown again when multiple tabs are opened (Bug 37618).

6.4.2. Online update module


Feedback 

- A default time-out of 10 minutes was added to the updater, after which stalled HTTP connections are aborted (Bug 37901).

6.5. Software deployment


Feedback 

6.5.1. Software deployment command line tools

Feedback 


- The update scripts have been adjusted to UCS 3.2-6 (Bug 38516).

6.6. Univention Library


Feedback 

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed (Bug 38078).

6.7. System services


Feedback 

6.7.1. Mail services


Feedback 

- Additional arguments for `smtpd` processes may now be added via Univention Configuration Registry variables. The given arguments are automatically added to the configuration file `/etc/postfix/master.cf`. The following UCR variable prefixes are currently supported:
 - `mail/postfix/mastercf/options/smtp/...`
 - `mail/postfix/mastercf/options/smtps/...`
(Bug 38062)
- The first changes to the `main.cf` framework have been done for defining a custom restriction rule set via Univention Configuration Registry variables for Postfix' `smtps` port (465). There is currently no change in Postfix behaviour (Bug 31738).

6.8. Services for Windows

Feedback 

6.8.1. Samba

Feedback 


- If the first configured LDAP server was not reachable, timeouts could occur during the share access on a member server. This has been fixed (Bug 13784).

6.8.2. Univention S4 Connector

Feedback 

- The password expiry attributes are now set in OpenLDAP if the password has been changed in Active Directory/Samba 4 (Bug 38494).

6.9. Other changes

Feedback 

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed in *univention-home-mounter* (Bug 38078).
- An error in a network script terminated the DHCP script responsible for updating the network configuration too early, which lead to RFC 3442 classless routes not being applied (Bug 37689).

Literaturverzeichnis

[ucs-handbuch] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. <http://docs.univention.de/manual-3.2.html>.