

UCS 3.2-2 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 3.2-2**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2014 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. Release-Highlights	#	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 / 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 die Univention Management Console	#	8#
5.5. Einschränkungen im Samba 4-Betrieb	#	9#
5.6. Installation in VirtualBox	#	9#
5.7. Installation in Citrix XenServer	#	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. Univention Installer	#	11#
6.3. Basic system services	#	11#
6.3.1. Univention Configuration Registry	#	11#
6.4. Domain services	#	11#
6.4.1. OpenLDAP	#	11#
6.4.1.1. Listener/Notifier domain replication	#	11#
6.5. Univention Management Console	#	11#
6.5.1. Univention Management Console web interface	#	11#
6.5.2. Univention Management Console server	#	12#
6.5.3. Univention App Center	#	12#
6.5.4. Users module	#	12#
6.5.5. Users module	#	12#
6.5.6. License module	#	12#
6.5.7. Other modules	#	12#
6.5.8. Univention Directory Manager command line interface and related tools	#	13#
6.5.9. Development of modules for Univention Management Console	#	13#
6.6. Univention Library	#	13#
6.7. System services	#	13#
6.7.1. Mail services	#	13#
6.7.2. Nagios	#	13#
6.7.3. Proxy services	#	14#
6.8. Virtualisation	#	14#
6.8.1. Univention Virtual Machine Manager	#	14#
6.9. Services for Windows	#	14#
6.9.1. Samba AD domain support	#	14#
6.9.2. Univention AD Takeover	#	15#
6.9.3. Univention S4 Connector	#	15#
6.10. Other changes	#	15#
Literaturverzeichnis	#	16#

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 3.2-2 steht das zweite Point-Release für Univention Corporate Server (UCS) zur Verfügung. Es beinhaltet alle für UCS 3.2-1 veröffentlichten Errata-Updates:

- Der Domänenbeitritt von Windows-Clients mit fehlerhafter Systemzeit wurde vereinfacht; ein vorheriges Synchronisieren der Systemzeit ist nun nicht mehr nötig. Außerdem werden Passwortsperrern nach erfolglosen Anmeldungen nun auch in Samba-AD-Domänen unterstützt.
- Univention AD Takeover - die UCS-Lösung zur automatischen Migration einer Active Directory-Domäne zu UCS - kann nun auch über ein Univention Management Console-Modul durchgeführt werden.
- Das Univention App Center wurde weiter ausgebaut, z.B. werden können nun auch Applikationen bereitgestellt werden, die nicht für alle Prozessor-Architekturen verfügbar sind.
- Die Konfiguration des Zugriff auf WLAN-Netze über das RADIUS-Protokoll kann über die neue Radius-App nun in der Univention Management Console konfiguriert werden.
- Das Debian-Point Update 6.0.9 wurde integriert. Es bringt zahlreiche Bugfixes mit sich.

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 Console mit dem Benutzer *root* durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über die Univention Management Console durchgeführt werden.

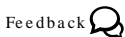
Eine Remote-Aktualisierung über SSH wird nicht empfohlen, da dies beispielsweise bei Unterbrechung der Netzverbindung zum Abbruch des Update-Vorgangs und zu einer Beeinträchtigung des Systems führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, 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 sollte das UCS-System neu gestartet werden.

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



Preup- und Postup-Skripte sind Skripte, die vor und nach Release-Updates aufgerufen werden (z.B. zur Nachbereitung des Updates, etwa die Deinstallation obsoleter Pakete). Ab UCS 3.2 werden diese Skripte kryptographisch signiert, um eine unerlaubte Modifikation zu verhindern. Beim Update und Spiegeln des Repositories 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 Signaturdateien 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; 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 der 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 wird keine Nutzungsstatistik gesammelt.

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 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 sie 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 die 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 Active-Directory-Funktionen noch nicht vollständig zur Verfügung:

- Microsoft Windows Domänencontroller dürfen aktuell nicht in eine Samba 4-Domäne beitreten.
- 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 aktuell keine Forest-Domänen.
- Samba 4 unterstützt aktuell 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.

Als Workaround muß vor dem Neustart der UCS-VM entweder die Installations-DVD aus den Laufwerkeinstellungen der VirtualBox-VM entfernt werden oder beim Start der virtuellen Instanz **F12** gedrückt werden 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 Änderung seit UCS 3.2-1:

6.1. General

Feedback 


- All security updates issued for UCS 3.2-1 are included.
- The Debian point update 6.0.9 has been integrated. It provides many bugfixes and also addresses some security issues (Bug 33272, Bug 33283, Bug 33287, Bug 33500, Bug 33776, Bug 33868, Bug 34136).

6.2. Univention Installer


Feedback 

- If a base system was selected as the system role, a warning is now displayed explaining the consequences (Bug 34329).
- The warning about the missing BIOS boot partition is now displayed again after modifying the partition table (Bug 34334).

6.3. Basic system services


Feedback 

6.3.1. Univention Configuration Registry


Feedback 

- In some cases the file ownership was not preserved correctly when a file is committed (Bug 34241).
- The program `univention-check-templates` now also checks UCR template files for modifications by using the MD5 hash sum managed by `dpkg` (Bug 24010).

6.4. Domain services


Feedback 

6.4.1. OpenLDAP

Feedback 


- If the LDAP server is not available the tool `univention-ldapsearch` now tries to reconnect to the LDAP server. The count can be configured via the Univention Configuration Registry-Variable `ldap/client/retry/count`, which is set to 10 by default (Bug 34292, Bug 34293).
- LDAP schema extensions are now included sorted by their file name to guarantee stable ordering (Bug 34406).
- The OpenLDAP init script has been revised (Bug 34440).

6.4.1.1. Listener/Notifier domain replication


Feedback 

- The shutdown message has been adjusted (Bug 32605).
- Moved objects are now tracked by their unique `entryUUID`. This fixes an issue, when objects in LDAP are modified and moved in short order, or while the listener is not running. (Bug 34355).

6.5. Univention Management Console

Feedback 


6.5.1. Univention Management Console web interface

Feedback 

- Display glitches with some progress bars have been fixed (Bug 34181).


- The detection of Internet Explorer 11 has been fixed (Bug 33990).

6.5.2. Univention Management Console server

Feedback 


- Added a method to the Univention Management Console web server to retrieve the client's IP address (Bug 34288).
- The UMC web server uses Apache as a proxy server. The timeout for proxy requests can now be configured with the Univention Configuration Registry-Variable `umc/http/session/timeout` (Bug 34005).

6.5.3. Univention App Center

Feedback 


- Renamed the button for buying an app from **Shop** to **Buy** (Bug 34183).
- Whitelisting and blacklisting of apps is now done based on the applications' ID (Bug 34145).
- Renamed the App ID for Tine 2.0 from `tine20org` to `tine20` to reflect that this is the commercial version (Bug 33728).
- Components in the App Center's tab **Repository Settings** may have default packages which can be installed. Before this is done, the App Center now updates the package list (Bug 34278).
- Applications may now specify supported architectures. If an application only supports 64 bit, a 32 bit operating system will refuse to install it (Bug 34320).
- The tool `univention-register-apps` exits after two minutes if it gets stuck (Bug 34834).

6.5.4. Users module

Feedback 


- LDAP objects with the attribute `univentionObjectFlag:functional` are now ignored (Bug 34395).

6.5.5. Users module

Feedback 


- A traceback has been fixed which could occur when creating computer objects with a given DHCP or DNS zone, but without an IP address. The traceback could also occur when removing DHCP/DNS zones along with all IP addresses. (Bug 33843).

6.5.6. License module

Feedback 


- In the license dialog, the LDAP base DN is also shown when using the free-for-personal-use license (Bug 34117).
- LDAP objects with the attribute `univentionObjectFlag:functional` are now ignored (Bug 34395).

6.5.7. Other modules

Feedback 


- The **Change password** module showed an endless loading animation after successfully applying changes. Now the form is reloading properly (Bug 34367).
- The labels for widgets regarding the type of LDAP objects have been changed as the old ones could not reflect the grammatical case (Bug 34038).

6.5.8. Univention Directory Manager command line interface and related tools

Feedback 


- UDM no longer creates temporary objects in `cn=univention` when moving containers, because `cn=univention` is ignored by the S4 connector and the S4 connector does not recognize the move (Bug 34266).

6.5.9. Development of modules for Univention Management Console

Feedback 


- Python UDM extensions are now installed with `update-python-support` (Bug 34421).
- The default value of a UDM property is now configurable via Univention Configuration Registry (e.g. by setting `directory/manager/web/modules/users/user/properties/mailHomeServer/default`) (Bug 23765).

6.6. Univention Library


Feedback 

- `ldap_extension.py` now moves files using the Python function `shutil.move` instead of `os.rename`. This allows moving files across partitions (Bug 34104).
- `ldap_extension.py` did not handle the activation of a new LDAP extension correctly and restarted the LDAP server too often (Bug 34800).
- This update fixes *shell-univention-lib* to call Univention Configuration Registry with an absolute path to work regardless of the current `PATH` setting, especially for cases where `/usr/sbin/` is not in `PATH` (Bug 29241).

6.7. System services


Feedback 

6.7.1. Mail services

Feedback 


- The Postfix policy service `listfilter` (which is used to restrict e-mail delivery to groups and lists) is now executed as the user `listfilter` instead of the user `cyrus`. This allows the deployment of this feature in environments without the component *univention-mail-cyrus* (Bug 26910).
- The new Univention Configuration Registry-Variables `mail/postfix/ldatable/starttls`, `mail/postfix/ldatable/tlsrequirecert` and `mail/postfix/ldatable/tlscacertfile` have been introduced to define whether and how Postfix should use TLS for LDAP lookups (Bug 34198).
- The listener module handling shared IMAP folders configured in the Univention Management Console now honours the Univention Configuration Registry-Variable `mail/cyrus/mailbox/delete` when deleting IMAP folders (Bug 34165).

6.7.2. Nagios

Feedback 


- The Univention Configuration Registry templates for the configuration and init files of the Nagios Remote Plugin Executor (NRPE) have been configured to use the PID file `/var/run/nagios/nrpe.pid` (Bug 34063).
- A buffer overflow in the `setuid` wrapper has been fixed (Bug 34041).

6.7.3. Proxy services


Feedback 

- `cache_dir null /tmp` is no longer set if caching is disabled. This fixes the operation of Squid without caching (Bug 33332).
- The Univention Configuration Registry-Variable `squid/redirect` can now be used to configure the `url_rewrite_program` configuration directive of Squid. If the variable is set to `squidguard`, then `/usr/bin/squidGuard -c /etc/squid/squidGuard.conf` is used for `url_rewrite_program` (Bug 32429).
- The join script of **univention-squid-kerberos** now checks if the service principal account already exists (Bug 33779, Bug 34575). In addition the saltPrincipal has been added to the Samba 4 keytab entry for the proxy service principal (Bug 32292).
- The Univention Configuration Registry-Variable `squid/forwardedfor` has been added to configure Squid's `forwarded_for` configuration directive (Bug 34025).

6.8. Virtualisation


Feedback 

6.8.1. Univention Virtual Machine Manager


Feedback 

- The HTML5 VNC plugin now prevents browsers from caching `vnc_auto.html`. This avoids certificate problems with HTTPS connections using Internet Explorer (Bug 33968).
- The init script now uses `force-stop` and `force-restart` to handle blocked UVMMd processes (Bug 34321).
- A broken link to an Support Database article has been replaced by a link to the manual (Bug 34425).
- `libvirt-check.sh` has been added to virtualization nodes. It periodically tests if `libvirtd` responds and restarts `libvirtd` if necessary (Bug 33966).
- The logging of `libvirtd` can now be controlled using the Univention Configuration Registry-Variables `libvirt/log/level`, `libvirt/log/filters` and `libvirt/log/outputs` (Bug 34170).

6.9. Services for Windows

Feedback 


6.9.1. Samba AD domain support

Feedback 

- Domain account lockout for Windows clients joined into a Samba AD domain are now possible (Bug 34443, Bug 34305, Bug 32974).
- Support for correcting skewed clocks during domain was added. This allows joining Windows clients without requiring a time synchronisation first (Bug 34439).
- `samba-tool dbcheck` now also lists/handles name conflict objects and objects without object class (Bug 33616).
- The domain services database module was affected by a segmentation fault when handling objects without object class (Bug 33977).
- Versions in the package dependencies have been updated (Bug 33972).
- Randomise domain controllers in DFS referral replies, e.g. for the SYSVOL share (Bug 34370).
- Several possible deadlock situations in the DRS replication have been fixed (Bug 34545).


- MS DFS support is now enabled on Samba AD domain controllers by default. With this new setting Windows clients ask for DFS redirects for the SYSVOL share, which may improve efficient network usage in branch site configurations (Bug 34326).
- `univention-samba4-backup` has been added to backup the samba provision directory. This tool is periodically executed by cron (configurable via the Univention Configuration Registry-Variable `samba4/backup/cron`) (Bug 34113).

6.9.2. Univention AD Takeover

Feedback 


- The AD takeover can now be performed through a Univention Management Console module (Bug 34019, Bug 34139).

6.9.3. Univention S4 Connector

Feedback 

- The S4 connector Python modules are now only built for Python 2.6 (Bug 31320).
- The user `pcpatch` is no longer ignored by default (Bug 34394).
- The start of multiple S4 connector instances is now prevented (Bug 34410).
- When creating a user in UCS a stronger password is used which fulfills the password complexity settings (Bug 34478).
- The Univention Configuration Registry-Variable `connector/s4/listener/disabled` has been added. If it is set to `true` the listener does not write any changes. This is helpful on a Domänencontroller Backup. The variable is not set by default during this upgrade (Bug 33858).
- During the group membership synchronization from Samba 4 to OpenLDAP an object mapping problem has been fixed (Bug 34197).

6.10. Other changes

Feedback 

- The package `univention-radius` has been added (Bug 29465).
- The `/etc/issue` welcome message mentions where to find the management system. After installing this update the message will only be shown on domain controllers and member servers (Bug 34330).
- The dependency list of the package `univention-directory-manager-modules` has been updated. Prior to this change, `slapd` was left installed on a Memberserver when using the appliance mode which could lead to problems when this system was querying LDAP (Bug 34201).
- The UDM CLI program `univention-directory-manager` now tries to start the internal UDM CLI server again if the first start was aborted (Bug 34784).

Literaturverzeichnis

[ucs-handbuch] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. <http://docs.univention.de/manual-3.2.html>.