

UCS 4.0-5 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 4.0-5**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2016 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. Hinweise zum Update	5
2.1. Empfohlene Update-Reihenfolge	5
2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante	5
3. Vorbereitung des Updates	6
4. Nachbereitung des Updates	7
5. Hinweise zum Einsatz einzelner Pakete	8
5.1. Erfassung von Nutzungsstatistiken	8
5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit	8
5.3. Empfohlene Browser für den Zugriff auf Univention Management Console	8
6. Changelog	9
6.1. General	9
6.2. Basic system services	10
6.2.1. Linux kernel and firmware packages	10
6.2.2. Boot Loader	10
6.3. Domain services	10
6.3.1. OpenLDAP	10
6.3.1.1. Listener/Notifier domain replication	10
6.3.1.2. DNS server	10
6.4. Univention Management Console	10
6.4.1. Univention Management Console web interface	10
6.4.2. Mail	11
6.5. System services	11
6.5.1. Mail services	11
6.5.2. Proxy services	11
6.6. Virtualization	11
6.6.1. Univention Virtual Machine Manager (UVMM)	11
6.7. Services for Windows	11
6.7.1. Samba	11
6.7.2. Univention S4 Connector	12
6.8. Other changes	12


Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.0-5 steht das fünfte Point-Release für Univention Corporate Server (UCS) 4.0 zur Verfügung. Es umfasst diverse Detailverbesserungen und Fehlerkorrekturen vor allem in den Bereichen Active Directory Kompatibilität und UCS-Managementsystem. Die für UCS 4.0-4 veröffentlichten Sicherheitsupdates sind in diesem Update enthalten.

Kapitel 2. Hinweise zum Update

Während der Aktualisierung kann es zu Ausfällen von Diensten innerhalb der Domäne kommen. Aus diesem Grund sollte das Update innerhalb eines Wartungsfensters erfolgen. Grundsätzlich wird empfohlen das Update zunächst in einer Testumgebung einzuspielen und zu testen. Die Testumgebung sollte dabei identisch zur Produktivumgebung sein. Je nach Systemgeschwindigkeit, Netzwerkanbindung und installierter Software kann das Update zwischen 20 Minuten und mehreren Stunden dauern.


2.1. Empfohlene Update-Reihenfolge

Feedback 

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.

2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante

Feedback 

UCS-Installations-DVDs werden ab UCS 4 nur noch für 64-Bit-Architekturen bereitgestellt. Vorhandene 32-Bit UCS 3 Systeme können weiterhin über das Online Repository oder über Update DVDs auf UCS 4 aktualisiert werden. Die 32-Bit-Architektur wird für die gesamte UCS 4 Maintenance noch unterstützt.

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 ungefähr 2 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.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken

Feedback 

Bei Verwendung der UCS Core Edition-Version von UCS (die in der Regel für Evaluationen von UCS herangezogen wird) werden anonyme Nutzungsstatistiken zur Verwendung von 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 UCS Core Edition. Der Lizenzstatus kann überprüft werden durch den Eintrag **Lizenz** -> **Lizenzinformation** des Benutzermenüs in der rechten, oberen Ecke von Univention Management Console. Steht hier unter **License type UCS Core 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. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit

Feedback 

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.

5.3. Empfohlene Browser für den Zugriff auf Univention Management Console

Feedback 

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 33
- Firefox ab Version 24
- Internet Explorer ab Version 9
- Safari und Safari Mobile ab Version 7

Auf älteren Browsern können Darstellungs- oder Performanceprobleme auftreten.

Kapitel 6. Changelog

Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit UCS 4.0-4:


6.1. General

Feedback 

- All security updates issued for UCS 4.0-4 are included:
 - **firefox** (CVE-2015-7181 CVE-2015-7182 CVE-2015-7183 CVE-2015-7197 CVE-2015-7198 CVE-2015-7199 CVE-2015-7200 CVE-2015-7196 CVE-2015-7194 CVE-2015-7193 CVE-2015-7189 CVE-2015-7188 CVE-2015-4513) (Bug 39785)..
 - **ntp** (CVE-2014-9750 CVE-2014-9751 CVE-2015-3405 CVE-2015-5146 CVE-2015-5194 CVE-2015-5195 CVE-2015-5219 CVE-2015-5300 CVE-2015-7691 CVE-2015-7692 CVE-2015-7701 CVE-2015-7702 CVE-2015-7703 CVE-2015-7704 CVE-2015-7850 CVE-2015-7851 CVE-2015-7852 CVE-2015-7855 CVE-2015-7871) (Bug 39628).
 - **rpcbind** (CVE-2015-7236) (Bug 39548).
 - **ldb** (CVE-2015-3223 CVE-2015-5330) (Bug 40222).
 - **samba** (CVE-2015-2535 CVE-2015-3223 CVE-2015-5252 CVE-2015-5296 CVE-2015-5299 CVE-2015-5330) (Bug 39217 Bug 39276 Bug 40222).
 - **mysql-5.5** (CVE-2015-4792 CVE-2015-4802 CVE-2015-4815 CVE-2015-4816 CVE-2015-4819 CVE-2015-4826 CVE-2015-4830 CVE-2015-4836 CVE-2015-4858 CVE-2015-4861 CVE-2015-4870 CVE-2015-4879 CVE-2015-4913) (Bug 40184).
 - **openjdk-7** (CVE-2015-4734 CVE-2015-4803 CVE-2015-4805 CVE-2015-4806 CVE-2015-4835 CVE-2015-4840 CVE-2015-4842 CVE-2015-4843 CVE-2015-4844 CVE-2015-4860 CVE-2015-4868 CVE-2015-4871 CVE-2015-4872 CVE-2015-4881 CVE-2015-4882 CVE-2015-4883 CVE-2015-4893 CVE-2015-4903 CVE-2015-4911) (Bug 40042).
 - **openssh** (CVE-2016-0777 CVE-2016-0778) (Bug 40439).
 - **linux** (CVE-2013-4312 CVE-2013-7446 CVE-2015-0272 CVE-2015-1333 CVE-2015-1420 CVE-2015-2925 CVE-2015-3212 CVE-2015-3290 CVE-2015-3291 CVE-2015-4167 CVE-2015-4692 CVE-2015-4700 CVE-2015-5156 CVE-2015-5157 CVE-2015-5257 CVE-2015-5283 CVE-2015-5307 CVE-2015-5364 CVE-2015-5366 CVE-2015-5697 CVE-2015-5706 CVE-2015-5707 CVE-2015-6252 CVE-2015-6937 CVE-2015-7513 CVE-2015-7550 CVE-2015-7566 CVE-2015-7613 CVE-2015-7799 CVE-2015-7833 CVE-2015-7872 CVE-2015-7990 CVE-2015-8104 CVE-2015-8374 CVE-2015-8543 CVE-2015-8550 CVE-2015-8551 CVE-2015-8552 CVE-2015-8569 CVE-2015-8575 CVE-2015-8709 CVE-2015-8767 CVE-2016-0723 CVE-2016-0728) (Bug 38764).
 - **firefox** (CVE-2015-7214 CVE-2015-7222 CVE-2015-7213 CVE-2015-7205 CVE-2015-7212 CVE-2015-7210 CVE-2015-7201 CVE-2015-7575 CVE-2016-1935 CVE-2016-1930) (Bug 40273).
 - **gnutls26** (CVE-2015-7575 CVE-2015-8313) (Bug 40411).
 - **libxml2** (CVE-2015-1819 CVE-2015-7941 CVE-2015-7942 CVE-2015-8035 CVE-2015-5312 CVE-2015-7497 CVE-2015-7498 CVE-2015-7499 CVE-2015-7500 CVE-2015-8241 CVE-2015-8317) (Bug 38907).

- **eglibc** (CVE-2014-8121 CVE-2015-1781 CVE-2015-7547 CVE-2015-8776 CVE-2015-8777 CVE-2015-8778 CVE-2015-8779) (Bug 38407).
- **samba** (CVE-2015-7560) (Bug 40679 Bug 40850).
- **sudo** (CVE-2015-5602) (Bug 40365).
- **openssl** (CVE-2015-3194 CVE-2015-3195 CVE-2015-3196 CVE-2015-7575 CVE-2016-0705 CVE-2016-0798 CVE-2016-0797 CVE-2016-0799 CVE-2016-0702) (Bug 40188).
- **apache2** (CVE-2015-3183) (Bug 39066).

6.2. Basic system services


Feedback 

6.2.1. Linux kernel and firmware packages

Feedback 


- The Linux kernel has been updated to *3.16.7-ckt20*. It provides many bugfixes and fixes several vulnerabilities (Bug 38764).

6.2.2. Boot Loader


Feedback 

- Two new Univention Configuration Registry variable `grub/default` and `grub/savedefault` are added, which allow the selection of the next kernel to boot (Bug 40509).

6.3. Domain services

Feedback 

6.3.1. OpenLDAP

Feedback 

- The group access for the LDAPI socket interface has been removed (Bug 39812).

6.3.1.1. Listener/Notifier domain replication

Feedback 

- The flushing of the listener cache has been disabled during module initialization (Bug 39958).
- Some replicated objects were not deleted, when the LDAP server closed its side of the LDAP connection. This issue has been fixed (Bug 40066).
- The timeout for the initial LDAP search during domain join has been increased to two hours, as joining in a large domain can take much longer than the default five minutes. The time can be changed through the Univention Configuration Registry variable `listener/timeout/scans` (Bug 40230).

6.3.1.2. DNS server

Feedback 

- The Univention Configuration variables `dns/nameserver/registration/forward_zone` and `dns/nameserver/registration/reverse_zone` have been added that allow to disable the automatic registration as additional nameserver (Bug 39384).

6.4. Univention Management Console


Feedback 

6.4.1. Univention Management Console web interface

Feedback 


- The expiration date has been increased by 5 years. This results in a traceback during the login on the 29th of February. This issue has been fixed (Bug 40791).

6.4.2. Mail


Feedback 

- Domain names for mail domains are now lowercased (Bug 40108).

6.5. System services


Feedback 

6.5.1. Mail services

Feedback 


- A bug in the mailing list filter policy server allowed senders with an empty email address to send to restricted mailing lists. This issue has been fixed (Bug 40352).
- An error in the dovecot listener could lead to the unintended deletion of a shared folder if the corresponding LDAP objects was changed. This issue has been fixed (Bug 40018).
- The UMC permissions *write* and *all* for shared folders did not contain the IMAP permission for expunge. A removal of mails or moving mails was not possible. This problem has been fixed and the permission will be updated automatically if the join script of *univention-mail-dovecot* is called (Bug 40037).
- A problem regarding IMAP ACLs at shared folders with primary mail address has been fixed. ACLs that have been removed via Univention Management Console or CLI have not been removed on the IMAP server (Bug 40195).
- A file for the process of handling user renames has been moved to a secure location (Bug 40583, Bug 40584).

6.5.2. Proxy services


Feedback 

- This update adds the possibility to define the number of squid's rewrite helper processes via the new Univention Configuration Registry variable `squid/rewrite/children` (Bug 40094).
- A new configuration option `dbtemp` has been added that specifies a directory for temporary backing files of squidGuard's in-memory databases (Bug 40593).

6.6. Virtualization


Feedback 

6.6.1. Univention Virtual Machine Manager (UVMM)


Feedback 

- Some unused helper code has been removed to fix an import error of the Python libvirt module from the UVMM Univention Directory Listener module handling the dynamic addition and removal of virtualization hosts (Bug 40255).

6.7. Services for Windows

Feedback 


6.7.1. Samba

Feedback 

- The ACL check in the SYSVOL sync script is now limited to the Policies directory (Bug 40267).
- There are two new Univention Configuration Registry variables `samba4/sysvol/sync/from_upstream` and `samba4/sysvol/sync/from_downstream` which can be used to deactivate copying files from other domain controllers (Bug 40314).
- The SYSVOL sync script now checks if any changes need to be synchronized at all and it uses file locking to coordinate concurrent read and write processes (Bug 40346).


- On UCS@school Samba AD DC Slaves the **univention-samba4** joinscript could take a long time to wait in vain for an object to get synchronized to the DC Master (Bug 40387).

6.7.2. Univention S4 Connector

Feedback 

- The synchronization failed if a removed user was recreated at a different position. This issue has been fixed (Bug 40234).
- The new package **univention-nagios-s4-connector** provides a Nagios plugin to check the state of the Univention S4 Connector (Bug 40345).
- *msPrint-ConnectionPolicy* objects are now synced if the Univention Configuration Registry variable `connector/s4/mapping/msprintconnectionpolicy` is set to true. The Univention S4 Connector has to be restarted after changing this variable). This is required for UCS@school and will be set there accordingly (Bug 40299, Bug 40466).
- Univention S4 Connector was still running during re-joins. This issue has been fixed (Bug 40389).
- Wildcard DNS records didn't get synchronized any more. This issue has been fixed (Bug 40381).

6.8. Other changes

Feedback 

- The package **lksctp-tools** has been added as a new dependency of OpenJDK-7 (Bug 40042).