

## UCS 4.4 Release Notes



**Release notes for the installation and update  
of Univention Corporate Server (UCS) 4.4-1**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2019 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.

## Table of Contents

1. Release Highlights .....	4
2. Notes about the update .....	5
2.1. Recommended update order for environments with more than one UCS server .....	5
2.2. UCS installation DVD only available for 64 bit .....	5
3. Preparation of update .....	6
4. Postprocessing of the update .....	7
5. Notes on selected packages .....	8
5.1. Univention Directory Notifier .....	8
5.2. Collection of usage statistics .....	8
5.3. Scope of security support for WebKit, Konqueror and QtWebKit .....	8
5.4. Recommended browsers for the access to Univention Management Console .....	8
6. Changelog .....	9
6.1. General .....	9
6.2. Basic system services .....	12
6.2.1. Boot Loader .....	12
6.3. Domain services .....	12
6.3.1. OpenLDAP .....	12
6.3.1.1. Listener/Notifier domain replication .....	12
6.4. Univention Management Console .....	13
6.4.1. Univention Management Console web interface .....	13
6.4.2. Univention Portal .....	13
6.4.3. Univention Management Console server .....	13
6.4.4. Univention App Center .....	14
6.4.5. Univention Admin Diary .....	15
6.4.6. Univention Directory Manager UMC modules and command line interface .....	15
6.4.7. Modules for system settings / setup wizard .....	16
6.4.8. Domain join module .....	16
6.4.9. Users module .....	16
6.4.10. System diagnostic module .....	17
6.4.11. Filesystem quota module .....	17
6.5. Univention base libraries .....	17
6.6. System services .....	17
6.6.1. DHCP .....	17
6.6.2. DNS .....	17
6.6.3. Mail .....	17
6.6.4. PAM .....	18
6.6.5. SAML .....	18
6.6.6. Univention self service .....	18
6.6.7. Printing services .....	18
6.6.8. Nagios .....	18
6.6.9. Kerberos .....	19
6.6.10. NFS .....	19
6.7. Virtualization .....	19
6.7.1. UCS Virtual Machine Manager (UVMM) .....	19
6.8. Services for Windows .....	19
6.8.1. Samba .....	19
6.8.2. Univention S4 Connector .....	20
6.8.3. Univention Active Directory Connection .....	20
6.9. Other changes .....	20

# Chapter 1. Release Highlights


With Univention Corporate Server 4.4-1, the first point release of Univention Corporate Server (UCS) 4.4 is now available. It provides several feature improvements and extensions, new properties as well as various improvements and bugfixes. Here is an overview of the most important changes:

- By configuring *stylesheets*, the look and feel of the login and self-service websites can be customized.
- There are significant performance improvements of the Directory Manager in environments with extensive LDAP structures.
- A new feature in the App Center gives hints for additional apps, based on the apps already installed in the environment.
- A beta version of the new UDM Rest API has been released.
- The source code of some UCS packages has been adapted for future migration to Python 3.
- Various security updates have been integrated into UCS 4.4-1, e.g. Samba, the Linux kernel and Dovecot. A complete list of security and package updates is available in Chapter 6.

## Chapter 2. Notes about the update

During the update some services in the domain may not be available temporarily, that is why the update should occur in a maintenance window. It is recommended to test the update in a separate test environment prior to the actual update. The test environment should be identical to the production environment. Depending on the system performance, network connection and the installed software the update will take between 20 minutes and several hours.


### 2.1. Recommended update order for environments with more than one UCS server

Feedback 

In environments with more than one UCS system, the update order of the UCS systems must be borne in mind:

The authoritative version of the LDAP directory service is maintained on the master domain controller and replicated to all the remaining LDAP servers of the UCS domain. As changes to the LDAP schema can occur during release updates, the master domain controller must always be the first system to be updated during a release update.

### 2.2. UCS installation DVD only available for 64 bit

Feedback 

Starting with UCS 4.0, installation DVD are only provided for the x86 64 bit architecture (amd64). Existing 32 bit UCS 3 systems can still be updated to UCS 4.0 through the online repository or by using update DVD. The 32 bit architecture will be supported over the entire UCS 4 maintenance period.

## Chapter 3. Preparation of update

It must be checked whether sufficient disk space is available. A standard installation requires a minimum of 10 GB of disk space. The update requires approximately 4 GB additional disk space to download and install the packages, depending on the size of the existing installation.

For the update, a login should be performed on the system's local console as user `root`, and the update should be initiated there. Alternatively, the update can be conducted using Univention Management Console.

Remote updating via SSH is not recommended as this may result in the update procedure being canceled, e.g., if the network connection is interrupted. In consequence, this can affect the system severely. If updating should occur over a network connection nevertheless, it must be verified that the update continues in case of disconnection from the network. This can be achieved, e.g., using the tools `screen` and `at`. These tools are installed on all UCS system roles by default.

Univention provides a script that checks for problems which would prevent the successful update of the system. Prior to the update, this script can be downloaded and executed on the UCS system.

```
# download
curl -Oos http://updates.software-univention.de/download/univention-
update-checks/pre-update-checks-4.4{, .gpg}

# run script
gpgv --keyring /usr/share/keyrings/univention-archive-key-ucs-4x.gpg \
    pre-update-checks-4.4.gpg pre-update-checks-4.4 && bash pre-
update-checks-4.4

...

Starting pre-update checks ...

Checking app_appliance ... OK
Checking block_update_of_NT_DC ... OK
Checking cyrus_integration ... OK
Checking disk_space ... OK
Checking hold_packages ... OK
Checking ldap_connection ... OK
Checking ldap_schema ... OK
...
```


## Chapter 4. Postprocessing of the update

Following the update, new or updated join scripts need to be executed. This can be done in two ways: Either using the UMC module **Domain join** or by running the command `univention-run-join-scripts` as user `root`.

Subsequently the UCS system needs to be restarted.


# Chapter 5. Notes on selected packages

## 5.1. Univention Directory Notifier

Feedback 

Due to a design flaw in the Univention Directory Notifier network protocol version 2 any user can retrieve information about changes to the LDAP directory. A new protocol version 3 was implemented with UCS 4.3-3 erratum 427. For backward compatibility with old UCS systems the Univention Directory Notifier still provided version 2 by default. For new installations starting with UCS-4.4 only version 3 is enabled by default. Protocol version 2 can be re-enabled by changing the Univention Configuration Registry variable `notifier/protocol/version` to 2 and restarting the Univention Directory Notifier.

## 5.2. Collection of usage statistics


Feedback 

Anonymous usage statistics on the use of Univention Management Console are collected when using the *UCS Core Edition*. The modules opened get logged to an instance of the web traffic analysis tool Piwik. This makes it possible for Univention to tailor the development of Univention Management Console better to customer needs and carry out usability improvements.

This logging is only performed when the *UCS Core Edition* license is used. The license status can be verified via the menu entry **License** - > **License information** of the user menu in the upper right corner of Univention Management Console. If **UCS Core Edition** is listed under **License type**, this version is in use. When a regular UCS license is used, no usage statistics are collected.


Independent of the license used, the statistics generation can be deactivated by setting the Univention Configuration Registry variable `umc/web/piwik` to *false*.

## 5.3. Scope of security support for WebKit, Konqueror and QtWebKit

Feedback 

WebKit, Konqueror and QtWebKit are shipped in the maintained branch of the UCS repository, but not covered by security support. WebKit is primarily used for displaying HTML help pages etc. Firefox should be used as web browser.

## 5.4. Recommended browsers for the access to Univention Management Console

Feedback 

Univention Management Console uses numerous JavaScript and CSS functions to display the web interface. Cookies need to be permitted in the browser. The following browsers are recommended:

- Chrome as of version 71
- Firefox as of version 60
- Safari and Safari Mobile as of version 12
- Microsoft Edge as of version 18

As of this release Internet Explorer is not supported by Univention Management Console anymore.


Users running older browsers may experience display or performance issues.



# Chapter 6. Changelog

Listed are the changes since UCS 4.4-0:

## 6.1. General


Feedback 

- All security updates issued since UCS 4.4-0 are included:
  - *firefox-esr* (CVE-CVE-2018-18506, CVE-CVE-2019-9788, CVE-CVE-2019-9790, CVE-CVE-2019-9791, CVE-CVE-2019-9792, CVE-CVE-2019-9793, CVE-CVE-2019-9795, CVE-CVE-2019-9796, CVE-CVE-2019-9810, CVE-CVE-2019-9813) (Bug 49078)
  - *liblivemedia* (CVE-CVE-2019-6256, CVE-CVE-2019-7314, CVE-CVE-2019-9215) (Bug 49022)
  - *ntfs-3g* (CVE-CVE-2019-9755) (Bug 49080)
  - *openjdk-8* (CVE-CVE-2019-2422) (Bug 49079)
  - *dovecot* (CVE-CVE-2019-7524) (Bug 49206)
  - *apache2* (CVE-CVE-2018-17189, CVE-CVE-2018-17199, CVE-CVE-2019-0196, CVE-CVE-2019-0211, CVE-CVE-2019-0217, CVE-CVE-2019-0220) (Bug 49237)
  - *systemd* (CVE-CVE-2018-1049, CVE-CVE-2018-15686, CVE-CVE-2019-3842) (Bug 49262)
  - *wget* (CVE-CVE-2019-5953) (Bug 49242)
  - *libssh2* (CVE-CVE-2019-3855, CVE-CVE-2019-3856, CVE-CVE-2019-3857, CVE-CVE-2019-3858, CVE-CVE-2019-3859, CVE-CVE-2019-3860, CVE-CVE-2019-3861, CVE-CVE-2019-3862, CVE-CVE-2019-3863) (Bug 49292)
  - *ghostscript* (CVE-CVE-2019-3835, CVE-CVE-2019-3838) (Bug 49331)
  - *ruby2.3* (CVE-CVE-2019-8320, CVE-CVE-2019-8321, CVE-CVE-2019-8322, CVE-CVE-2019-8323, CVE-CVE-2019-8324, CVE-CVE-2019-8325) (Bug 49332)
  - *wpa* (CVE-CVE-2019-9495, CVE-CVE-2019-9497, CVE-CVE-2019-9498, CVE-CVE-2019-9499) (Bug 49334)
  - *clamav* (CVE-CVE-2019-1787, CVE-CVE-2019-1788, CVE-CVE-2019-1789) (Bug 49385)
  - *firmware-nonfree* (CVE-CVE-2018-5383) (Bug 49379)
  - *gst-plugins-base1.0* (CVE-CVE-2019-9928) (Bug 49401)
  - *jquery* (CVE-CVE-2019-11358) (Bug 49372)
  - *kauth* (CVE-CVE-2019-7443) (Bug 49375)
  - *libpng1.6* (CVE-CVE-2019-7317) (Bug 49376)
  - *linux* (CVE-CVE-2018-5953, CVE-CVE-2018-14625, CVE-CVE-2018-16884, CVE-CVE-2018-19824, CVE-CVE-2018-19985, CVE-CVE-2018-20169, CVE-CVE-2018-1000026, CVE-CVE-2019-3459, CVE-CVE-2019-3460, CVE-CVE-2019-3701, CVE-CVE-2019-3819, CVE-CVE-2019-6974, CVE-CVE-2019-7221, CVE-CVE-2019-7222, CVE-CVE-2019-8980, CVE-CVE-2019-9213, CVE-CVE-2019-10124) (Bug 49377)


- **mariadb-10.1** (CVE-CVE-2019-2529, CVE-CVE-2019-2537) (Bug 49373)
- **rsync** (CVE-CVE-2016-9841, CVE-CVE-2016-9842, CVE-CVE-2016-9843) (Bug 49371)
- **univention-kernel-image-signed** (CVE-CVE-2018-5953, CVE-CVE-2018-14625, CVE-CVE-2018-16884, CVE-CVE-2018-19824, CVE-CVE-2018-19985, CVE-CVE-2018-20169, CVE-CVE-2018-1000026, CVE-CVE-2019-3459, CVE-CVE-2019-3460, CVE-CVE-2019-3701, CVE-CVE-2019-3819, CVE-CVE-2019-6974, CVE-CVE-2019-7221, CVE-CVE-2019-7222, CVE-CVE-2019-8980, CVE-CVE-2019-9213, CVE-CVE-2019-10124) (Bug 49377)
- **univention-kernel-image** (CVE-CVE-2018-5953, CVE-CVE-2018-14625, CVE-CVE-2018-16884, CVE-CVE-2018-19824, CVE-CVE-2018-19985, CVE-CVE-2018-20169, CVE-CVE-2018-1000026, CVE-CVE-2019-3459, CVE-CVE-2019-3460, CVE-CVE-2019-3701, CVE-CVE-2019-3819, CVE-CVE-2019-6974, CVE-CVE-2019-7221, CVE-CVE-2019-7222, CVE-CVE-2019-8980, CVE-CVE-2019-9213, CVE-CVE-2019-10124) (Bug 49377)
- **unzip** (CVE-CVE-2018-1000035) (Bug 49374)
- **zziplib** (CVE-CVE-2018-6381, CVE-CVE-2018-6484, CVE-CVE-2018-6540, CVE-CVE-2018-6541, CVE-CVE-2018-6869, CVE-CVE-2018-7725, CVE-CVE-2018-7726, CVE-CVE-2018-16548) (Bug 49378)
- **samba** (CVE-CVE-2018-16860) (Bug 49432)
- **atftp** (CVE-CVE-2019-11365, CVE-CVE-2019-11366) (Bug 49452)
- **bind9** (CVE-CVE-2018-5743, CVE-CVE-2018-5745, CVE-CVE-2019-6465) (Bug 49450)
- **ghostscript** (CVE-CVE-2019-3839) (Bug 49451)
- **linux** (CVE-CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091) (Bug 49476)
- **postgresql-9.6** (CVE-CVE-2019-10130) (Bug 49453)
- **univention-kernel-image-signed** (CVE-CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091) (Bug 49476)
- **intel-microcode** (CVE-CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091) (Bug 49483)
- **ffmpeg** (CVE-CVE-2018-15822, CVE-CVE-2018-1999011, CVE-CVE-2019-9718, CVE-CVE-2019-11338) (Bug 49545)
- **firefox-esr** (CVE-CVE-2018-18511, CVE-CVE-2019-5798, CVE-CVE-2019-7317, CVE-CVE-2019-9797, CVE-CVE-2019-9800, CVE-CVE-2019-9816, CVE-CVE-2019-9817, CVE-CVE-2019-9819, CVE-CVE-2019-9820, CVE-CVE-2019-11691, CVE-CVE-2019-11692, CVE-CVE-2019-11693, CVE-CVE-2019-11698) (Bug 49544)
- **wpa** (CVE-CVE-2019-11555) (Bug 49552)
- **openjdk-8** (CVE-CVE-2019-2602, CVE-CVE-2019-2684, CVE-CVE-2019-2698) (Bug 49583)
- **gemu** (CVE-CVE-2018-11806, CVE-CVE-2018-12617, CVE-CVE-2018-16872, CVE-CVE-2018-17958, CVE-CVE-2018-18849, CVE-CVE-2018-18954, CVE-CVE-2018-19364, CVE-CVE-2018-19489, CVE-CVE-2019-3812, CVE-CVE-2019-6778, CVE-CVE-2019-9824, CVE-

- CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091, CVE-CVE-2019-12155) (Bug 49582)
- *cyrus-imapd* (CVE-CVE-2019-11356) (Bug 49631)
  - *exim4* (CVE-CVE-2019-10149) (Bug 49603)
  - *heimdal* (CVE-CVE-2018-16860, CVE-CVE-2019-12098) (Bug 49599)
  - *dbus* (CVE-CVE-2019-12749) (Bug 49659)
  - *linux* (CVE-CVE-2019-3846, CVE-CVE-2019-5489, CVE-CVE-2019-9500, CVE-CVE-2019-9503, CVE-CVE-2019-10126, CVE-CVE-2019-11477, CVE-CVE-2019-11478, CVE-CVE-2019-11479, CVE-CVE-2019-11486, CVE-CVE-2019-11599, CVE-CVE-2019-11815, CVE-CVE-2019-11833, CVE-CVE-2019-11884) (Bug 49676)
  - *samba* (CVE-CVE-2019-12435, CVE-CVE-2019-12436) (Bug 49626)
  - *univention-kernel-image-signed* (CVE-CVE-2019-3846, CVE-CVE-2019-5489, CVE-CVE-2019-9500, CVE-CVE-2019-9503, CVE-CVE-2019-10126, CVE-CVE-2019-11477, CVE-CVE-2019-11478, CVE-CVE-2019-11479, CVE-CVE-2019-11486, CVE-CVE-2019-11599, CVE-CVE-2019-11815, CVE-CVE-2019-11833, CVE-CVE-2019-11884) (Bug 49676)
  - *vim* (CVE-CVE-2019-12735) (Bug 49691)
  - *vlc* (CVE-CVE-2019-5439) (Bug 49658)
  - *firefox-esr* (CVE-CVE-2019-11707) (Bug 49684)
  - *intel-microcode* (CVE-CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091) (Bug 49718)
  - *libvirt* (CVE-CVE-2019-10161, CVE-CVE-2019-10167) (Bug 49710)
  - *expat* (CVE-CVE-2018-20843) (Bug 49761)
  - *gemu* (CVE-CVE-2018-12126, CVE-CVE-2018-12127, CVE-CVE-2018-12130, CVE-CVE-2019-11091) (Bug 49714)
  - *rdesktop* (CVE-CVE-TMP49772) (Bug 49772)
  - *firefox-esr* (CVE-CVE-2019-11708) (Bug 49797)
  - *openssl1.0* (CVE-CVE-2019-1559) (Bug 49795)
  - *openssl* (CVE-CVE-2019-1543) (Bug 49793)
  - *samba* (CVE-CVE-2019-3870, CVE-2019-3880) (Bug 49034, Bug 49025)
  - *univention-directory-notifier* (Bug 48466)
  - The following packages have been moved to the maintained repository of UCS: *numad* (Bug 47574), *python-setproctitle* (Bug 49176), *configparser* (Bug 49588)

## 6.2. Basic system services


Feedback 

### 6.2.1. Boot Loader


Feedback 

- Fix usage of Univention Configuration Registry Python module in *univention-bootsplash*. (Bug 49129)

## 6.3. Domain services


Feedback 

### 6.3.1. OpenLDAP

Feedback 

- OpenLDAP restricts the number of returned entries when searching. This can be configured using the Univention Configuration Registry variable `ldap/sizelimit`, which defaults to 400k. This is not enough for `univention-translog prune`. Remove the limit for searches connecting via `ldapi:///`. (Bug 49505)
- Use `slaptest` for LDAP schema checking in the `ldap_extension` module. (Bug 49596)
- Increase the length of the LDAP root password (`/etc/ldap/rootpw.conf`) used for LDAP replication to improve security against brute force attacks. (Bug 48606)
- By default `univention-ldapsearch` appends the argument `-o ldif-wrap=no` now. (Bug 48683)

#### 6.3.1.1. Listener/Notifier domain replication


Feedback 

- The `resync_objects.py` helper script now respects the configured local LDAP port. (Bug 49228)
- Check available file system space before writing transactions. (Bug 28233)
- Fix regression from UCS 4.3-3 erratum 426 in `cn=translog` setup, which reset the LDAP indexes. (Bug 48971)
- Since UCS 4.3-3 erratum 427 the Univention Directory Notifier (UDN) writes transactions both to the file `/var/lib/univention-ldap/notify/transaction` and the `cn=translog` database in OpenLDAP. A failed write to the later can make UDN abort, in which case UDN is restarted automatically and writes the pending transactions to said file again. This leads to inconsistency. The order has been swapped to prevent this issue from happening again. The transaction file might require manual corrections if UDN fails to start up properly. (Bug 49198)
- Deprecated and unused code has been removed. (Bug 49277)
- Add `univention-translog check --fix` command to check (and fix) inconsistency between the files `/var/lib/univention-ldap/notify/transaction`, `/var/lib/univention-ldap/notify/transaction.index`, `/var/lib/univention-ldap/listener/listener`, and `/var/lib/univention-ldap/last_id`. (Bug 49201)
- Implement command `univention-translog prune` to prune old transactions from the `transaction` file and database. This can be used to save space.


### Warning

This procedure is dangerous and should ONLY be executed if ALL Univention Directory Listener (UDL) in the domain have processed all previous transactions. Otherwise the *UDLs* will no longer be able to process transactions and affected systems must be re-joined! Systems, which have not been running for some time or are restored from backup, must also be re-joined if their last processed transaction is no longer part contained in the purged `translog`. (Bug 48729)

## 6.4. Univention Management Console


Feedback 

### 6.4.1. Univention Management Console web interface

Feedback 


- Change dependency of package *univention-dojo-dev* from *openjdk-7* to *default-jre-headless* as the former is deprecated and no longer maintained. (Bug 49508)
- The legacy path `/umcp/` to access UMC backend has been removed. (Bug 49639)
- The design of the UMC login page can now be adjusted via `/usr/share/univention-management-console-login/css/custom.css`. (Bug 49436)
- UMC does not respond with an error anymore if no English locale is configured. (Bug 47602)
- The UMC for UCS Core Editions shows a notification that informs about the UCS Ambassador Program. (Bug 49731)
- Error messages during login or password changing are translated again. (Bug 49029)
- The SAML identity provider is not configured in UMC anymore if it is disabled via the Univention Configuration Registry variable `umc/web/sso/enabled`. (Bug 48224)
- The label and icon of some widgets are now configurable. (Bug 49730)
- Notifications can now be shown non-truncated. (Bug 49731)
- A cross site scripting vulnerability in *umc.widgets.Editor* has been fixed. This affected portal entries. (Bug 48812)
- Preparations for better browser cache-control have been implemented. (Bug 48995)
- It is possible to define standby animations for form dependencies now. (Bug 46919)
- Password input fields can now have a button to show the password in clear text. (Bug 49099)
- Grids can now automatically encode HTML entities (Bug 48972)

### 6.4.2. Univention Portal

Feedback 

- Portal entries which are limited to users are now shown when the user is logged in via email address. (Bug 49619)
- Whether portal entries are opened in the same tab or a new tab is now configurable. (Bug 45318)
- Debug statements were added to the portal server listener. (Bug 49113)
- The file permissions for the cache directory of the Portal is now stricter. This prevents warnings in the System diagnostic UMC module. (Bug 48814)
- Obsolete code has been removed. (Bug 48943)
- The robustness of the `univention-portal-server` has been increased. (Bug 49526)
- The `univention-portal-server` is reloaded after a server password rotation. (Bug 49746)


### 6.4.3. Univention Management Console server

Feedback 

- The error message for a failed password change has been improved. (Bug 48897)

- The UCS identity provider configuration is always fetched when executing the `joinscript 92univention-management-console-web-server.inst` (Bug 48198)
- Obsolete code has been removed. (Bug 48943)
- The UMC now uses `json` instead of `simplejson`. (Bug 47377)
- Corrupt translation files cannot cause UMC to crash anymore. (Bug 49775)
- LDAP connection problems could result in an error loop, with the following error `ldapError: Insufficient access`. This has been fixed by ensuring a new connection is used after LDAP connection problems. (Bug 46089)
- A crash of UMC in rare situations has been corrected. (Bug 48157)
- The `pam_cracklib` behavior prior to UCS 4.3 erratum 450 has been restored. Therefore password changes do not require strong passwords anymore if no password policy is defined in the domain. (Bug 49239)


## 6.4.4. Univention App Center

 Feedback 

- Log rotation for container logs has been enabled in the docker daemon, and can be configured via the Univention Configuration Registry variables `docker/daemon/default/opts/log-driver` (default `json-file`) and `docker/daemon/default/map/log-opt` (default `max-file=4,max-size=10m`). (Bug 47416)
- Added a new listener to save a mapping for App Attributes that the UDM UMC module may read (Bug 48895)
- Extended Attributes are only searched for in the correct LDAP container (Bug 48982)
- A crash when registering attributes is prevented during the activation of new schema extensions. (Bug 45513)
- Docker image verification was removed from the App Center code. Instead, we rely on the functions of Docker itself. (Bug 48670)
- The App Center waits for a `dpkg` lock before attempting to install database software packages. If starting the database service fails anyway, we now send more verbose information. (Bug 48669)
- The package `univention-appcenter` is now built with `dh_python2`. (Bug 49145)
- A visual flickering in the App Center overview has been removed. (Bug 49089)
- Create app password file on host before starting container. (Bug 49491)
- The App Center now shows app suggestions based on already installed apps. (Bug 49510)
- Handling of the docker-compose Univention Configuration Registry template file has been fixed. (Bug 49517)
- Abort installation if `machine.secret` could not be copied into container. (Bug 49543)
- Improve error handling during container start. (Bug 48881)
- More debug messages during `SetupFailed`. (Bug 49625)
- Do not revert (remove, reinstall old) after failed App update. (Bug 49645)
- The docker App upgrade message has been changed. (Bug 49742)


- Suggestions based on currently installed Apps are now dynamically loaded from the App Center server. (Bug 49770)

### 6.4.5. Univention Admin Diary

Feedback 

- The Admin Diary now displays dates correctly in Safari (Bug 49579)
- HTML entities in the Diary overview are now properly encoded (Bug 48972)
- Improve robustness and traceback logging. (Bug 49056)
- Fix traceback in `admin diary . client . write _ event ( )` in *univention-updater* occurring in Docker containers during docker build. (Bug 49056)

### 6.4.6. Univention Directory Manager UMC modules and command line interface


Feedback 

- A new package has been added which contains a prototype of a HTTP service for the Univention Directory Manager. (Bug 49667)
- Creating reports of objects which reference not existing objects is possible again. This was the case for secretary of user objects and networks of computer objects. (Bug 47922)
- Rely on the App Center listener to create the App Attributes mapping rather than doing it in the UMC module (Bug 48895)
- Preparations for better browser cache-control have been implemented. (Bug 48995)
- Requesting a Univention license activation during the initial system configuration has been repaired. (Bug 49384)
- The `computers / * UDM` handlers now share a common base class. Code redundancy has therefore been reduced. (Bug 41659)
- Searching for IP addresses of DNS host records is now possible. The Zone Time-to-Live and Mail Exchange properties of DNS objects aren't shown in the search field list anymore in UMC. (Bug 40668)
- A crash of UDM is prevented which was caused by an extended attribute that overwrites a not existing layout group. (Bug 48551)
- The object class `univentionPolicyReference` is now removed from objects when the last policy is dereferenced. (Bug 46466)
- The search filter `dnsAlias` in the computer modules has been repaired. (Bug 31494)
- Referenced portal entries and categories are now correctly updated when renaming or moving portal settings. (Bug 49526)
- Stop caching machine connection in new UDM API for long running services. (Bug 49746)
- It is now possible to specify LDAP server controls in some UDM handlers `lookup ( )` method. (Bug 49638)
- Clean code by shortening *univention.debug* usage. (Bug 49422)
- Explicit initialization of the default values of Univention Directory Manager properties has been removed from the code of all UDM modules. (Bug 49235)

### Modules for system settings / setup wizard


- The `users/user` UDM module now uses the LDAP filter `univentionObjectType=users/user` when searching for objects to increase performance. (Bug 48390)
- When opening container objects, a lookup is performed to check whether this container is the default container for certain UDM objects. This lookup is now cached which makes opening many objects at once considerably faster. (Bug 49408)
- After renaming an object the internal DN (`self.dn`) is updated correctly. The old DN can now be obtained via `self.old_dn`. This fixes the concurrent renaming and update of group membership for e.g. computer objects. (Bug 41694)
- Several German translations have been updated. (Bug 49359)
- Univention Directory Manager handlers now share a common base class. Code redundancy has therefore been reduced. (Bug 35687)
- Default containers for domain controller computer objects can now be configured. (Bug 46919)
- It is now possible again to modify the LDAP base, for example reference policies. This was broken since UCS 4.3-0. (Bug 46919)
- `udm users/user create` without `--set username` does not cause an exception anymore. (Bug 48441)
- Various LDAP filters are now escaped. (Bug 42791)
- The use of obsolete `univention.admin.config` has been removed. (Bug 27804)

## 6.4.7. Modules for system settings / setup wizard

 Feedback 


- A message is shown to warn about the inability to install **Samba4** or UCS@school if a host name with more than 13 characters is chosen. (Bug 43326)
- Fixed a special case for the initial domain join, the DC master hostname may now differ from the value read from the DNS server. (Bug 48134)
- The unused dependency to `python-simplejson` has been removed. (Bug 35687)
- Requesting a Univention license activation during the initial system configuration has been repaired. (Bug 49384)
- For UCS@school: The setup process now includes a new confirmation prompt in UCS@school environments to make sure that the server should be set up with the correct UCS@school role (educational, administrative or central). (Bug 49271)

## 6.4.8. Domain join module

 Feedback 

- If a `failed.ldif` file exists at the start of a join, it will be removed. (Bug 47603)
- Fixed joining host into an UCS domain when using bonded network interfaces. (Bug 49298)
- The path to `/usr/sbin/univention-admin-diary-entry-create` is now explicit in `univention-join` (Bug 48972)


## 6.4.9. Users module

 Feedback 

- Prevent high CPU usage in the `Users` module. (Bug 47985)




## 6.4.10. System diagnostic module

Feedback 


- Updated `sysvolcheck` check (Bug 46643)
- Remove the `sysvolcheck` as it reports irritating false positives for GPOs created via GPMC. (Bug 49335)

## 6.4.11. Filesystem quota module

Feedback 


- Previously, when quota policies were set on multiple shares that are located on the same mountpoint, a quota policy that had a value of zero (meaning no quota is enforced) would overwrite smaller quota policies. This behavior has been changed to always choose the smallest value. (Bug 48000)

## 6.5. Univention base libraries


Feedback 

- Split low-level C implementation from Python binding to simplify transition to using `dh_python2` and adding Python 3 support. (Bug 49130)
- Unify pure-python version `debug2.py` again with C-version `debug.py`. (Bug 46100)
- Deprecate `function` class in favor of `trace` decorator. (Bug 43422)
- Preparations for better browser cache-control have been implemented. (Bug 48995)
- The `python3-univention` package dependencies have been adjusted. (Bug 49136)
- The package dependency loop for `python-univention-debug` has been broken by introducing a new binary package `python-univention-namespace`. (Bug 49506)
- It is now possible to specify LDAP server controls in the `univention.ldap.access.search()` methods. (Bug 49638)
- The package `univention-python` now uses `dh_python2` instead of `python-support`. Therefore Python modules are installed into `/usr/lib/python2.7/dist-packages/univention/`. (Bug 49140)

## 6.6. System services


Feedback 

### 6.6.1. DHCP

Feedback 


- The setting for `unknownClients` from the UMC policy `DHCP Scope` is no longer applied to a DHCP pool statement. This is not allowed by the syntax of the DHCP daemon. (Bug 20222)

### 6.6.2. DNS

Feedback 

- Fix dependency header of legacy SysV init script to work in environments installed with UCS-4.2 or older and without Samba4. (Bug 49441)
- The robustness of the listener for DNS zones has been improved. Certain LDAP DNS objects could cause path injection vulnerabilities causing arbitrary file reading and modifications as well as crashes of the bind service. (Bug 41005)


### 6.6.3. Mail

Feedback 

- LDAP ACL ordering on DC slaves allowed regular users access to private information. Reordering of ACLs fixes this issue. (Bug 48608)


- Prevent creation of empty mailboxes in `/var/spool/dovecot/private/` by unsuccessful login attempts of users without a primary mail address. (Bug 49038)
- Add SNI Support to *univention-mail-dovecot*. Additional FQDNs and certificates can be configured with Univention Configuration Registry variable `mail/dovecot/ssl/sni/$fqdn/certificate=$path_to_certificate` and `mail/dovecot/ssl/sni/$fqdn/key=$path_to_certificate_key` (Bug 48485)

### 6.6.4. PAM

Feedback 


- An open SSH connection will now properly get closed when shutting down a system. (Bug 47233)

### 6.6.5. SAML

Feedback 


- The session duration of the identity provider is now configurable with the new Univention Configuration Registry variable `saml/idp/session-duration`. With this update, the default value for a SAML session is raised from 8 to 12 hours. (Bug 49503)
- The design of the UMC single sign-on page can now be adjusted via `/usr/share/univention-management-console-login/css/custom.css`. (Bug 49436)

### 6.6.6. Univention self service

Feedback 


- Fixed links to the Self Service-App not working when the Univention Configuration Registry variable `umc/self-service/profiledata/enabled` is set to `false`. (Bug 45041)
- The Self Service-App can now be styled via the `/var/www/univention/self-service/css/custom.css` CSS file. (Bug 49343)
- Fix German translation. (Bug 49380)

### 6.6.7. Printing services

Feedback 


- It is now possible to use space characters in samba printer names. (Bug 48947)
- A security vulnerability in the listener has been fixed which caused overwriting or removal of arbitrary files. (Bug 49296)
- The package description has been fixed. (Bug 28681)
- Fix regression caused by UCS 4.4-1 erratum 94 in *ghostscript* (Bug 49721)
- The cups configuration in `/etc/cups/cupsd.local.conf` is applied again. Since UCS 4.3 erratum 149 the cups `Include` directive has been removed. Changes in the `/etc/cups/cupsd.local.conf` configuration require a `ucr commit /etc/cups/cupsd.conf` now. (Bug 48437)
- The listener now handles DN syntax correctly. (Bug 43430)

### 6.6.8. Nagios

Feedback 


- A Nagios check for the `cn=translog` database has been added. (Bug 48422)
- A Nagios check for the `univention-directory-listener` database has been added. To apply it on a slave domain controller, backup domain controller or member server execute: `univention-run-join-scripts --force --run-scripts 30univention-nagios-client.inst` (Bug 48617)

## 6.6.9. Kerberos

Feedback 


- The build system for the package *univention-python-heimdal* has been changed to *dh\_python2*. (Bug 49139)

## 6.6.10. NFS


Feedback 

- A newline injection vulnerability has been fixed which allowed to add further entries to `/etc/exports`. (Bug 44054)

## 6.7. Virtualization


Feedback 

### 6.7.1. UCS Virtual Machine Manager (UVMM)


Feedback 

- Re-connect VMs to bridges on network restart. (Bug 47701)
- Use interleaved memory policy on NUMA architectures by default. (Bug 49574)
- Fix Python traceback while handling `select()` exception. (Bug 49403)
- Preparations for better browser cache-control have been implemented. (Bug 48995)
- Re-compile libvirt with NUMA support enabled. (Bug 49574)
- Since UCS 4.3 erratum 269 UVMM can be configured to check the CPU model before performing a live migration. Due to a bug in *libvirt* the use of `host-model` does not survive the creation of snapshots or suspend to disk and gets rewritten to the concrete CPU model of the host system. This has been fixed. Old snapshots created and domains suspended before this erratum might fail to start, in which case the CPU configuration must be manually removed from the XML description using `virsh snapshot-edit` or `virsh save-image-edit` respectively. (Bug 49425)

## 6.8. Services for Windows

Feedback 


### 6.8.1. Samba

Feedback 

- Improve `samba-tool ntacl sysvolcheck` to reduce reporting false positives. This can be run by using new option `--mask-msad-differences`. Without the new option the reporting is unchanged. This is another step in the ongoing quest of improving the quality this tool for NTACL inheritance. (Bug 46643)
- The folder `windows-profiles` in the home share is now hidden. (Bug 48541)
- Several vulnerabilities in the listener for shares have been fixed: The name of shares are validated. The blacklist for share paths is now evaluated correctly. Configuration values are now correctly quoted to prevent injecting multiple further share entries. (Bug 44054)
- Re-add `auth methods` option removed from upstream Samba sources (Bug 49426)
- If samba fails to set the new password in a server password change, the changes will be reverted. (Bug 48541)
- UCS will now use password generation from samba for administrator accounts (Bug 49193)
- Set correct permissions for lock file on upstream server during `sysvol` synchronization. (Bug 48917)


- Fix permissions of template files `dns_update_list` and `spn_update_list`. (Bug 49025)
- Update to Samba 4.10.1 (Bug 49034)
- Internal improvement: fixed quoting of shell variables. (Bug 48989)
- When `univention-samba4-backup` fails, cron will automatically send system-mails to root. (Bug 49399)

## 6.8.2. Univention S4 Connector

Feedback 


- A trivial Univention Configuration Registry syntax error has been fixed in the `joinscript` (Bug 35237)
- Remove `lockingdb` and `s4cache` during re-join (Bug 40773)
- When the S4-Connector starts, it logged the group cache initialization at level INFO. In debugging situations that can lead to a lot of output in `connector-s4.log` which is hard to scroll. The log volume of the group cache init has been lowered to log level ALL. (Bug 48364)
- The scripts `remove_ucs_rejected.py` and `remove_s4_rejected.py` now escapes SQL syntax. (Bug 49445)
- Avoid rejects when DNS records have an uppercase DC attribute. (Bug 49643)
- Fix traceback password `sync_to_ucs` for machine accounts. (Bug 49649)
- The package now uses `dh_python2` instead of `python-support`. Therefore Python modules are installed into `/usr/lib/python2.7/dist-packages/univention/s4connector/`. (Bug 49176)
- The detection of a running `univention-s4-connector` has been enhanced. (Bug 49176)
- Duplicated code for the detection of `superordinates` has been removed. (Bug 45068)
- Dead code for obsolete custom attributes from UCS 2 has been removed. (Bug 41554)
- Excluding sub-trees from synchronization by S4-Connector is now possible by configuring Univention Configuration Registry variables matching the pattern `connector/s4/mapping/ignore subtree/`. (Bug 47008)
- The use of obsolete `univention.admin.config` has been removed. (Bug 27804)

## 6.8.3. Univention Active Directory Connection

Feedback 

- Dead code for obsolete custom attributes from UCS 2 has been removed from `univention-ad-connector`. (Bug 41553)
- References to the obsolete password service in `univention-ad-connector` have been removed. (Bug 49111)

## 6.9. Other changes

Feedback 

- The package `univention-errata-level` has been updated to reset the Univention Configuration Registry variable `version/erratalevel` to 0 (Bug 48654).
- If samba fails to set the new password in a server password change, the changes will be reverted. (Bug 49193)
- The function `getRootDnConnection()` has been fixed. (Bug 49024)

- The LDAP ACLs for read access to `cn=monitor` can now be extended via Univention Configuration Registry variables. (Bug 49387)
- Fix escaping of LDAP DN, filters and shell arguments (Bug 46323)
- The creation of a default LDAP server policy is now configurable via the Univention Configuration Registry variable `ldap/create-ldap-server-policy`. (Bug 49386)
- Log `stderr` if LDAP schema validation fails. (Bug 49500)
- A `symlink` and code execution vulnerability has been fixed in `univention.lib.listenerSharePath`. (Bug 44054)
- Python 3 compatibility for `univention.lib.admember` has been enhanced. (Bug 49176)
- A path traversal vulnerability in the `ldap_extension.py` listener utilities has been fixed. (Bug 41780)
- The detection of running services has been enhanced. (Bug 49176)
- The script `univention-policy-update-config-registry` now has a new option to specify the LDAP server from which to get the policies. (Bug 35208)
- Multiple `rsyslog` remote servers can now be specified in the Univention Configuration Registry variable `syslog/remote`. (Bug 48508)
- Univention Configuration Registry templates which generate binary data have been fixed. This was broken since UCS 4.4-1 erratum 167 and could cause crashes of Univention Management Console due to corruptly generated translation files. (Bug 49775)
- Make the `systemd` service timeout for `mysqld` configurable via the Univention Configuration Registry variable `mariadb/startup/timeout`. (Bug 46901)
- The escaping of LDAP filters and distinguished names has been corrected. (Bug 40055)
- Reconnect to DRS service in case the DRS replication for the password synchronization fails. (Bug 45127)
- Default containers for `computers/domaincontroller_master` objects can now be configured. During the upgrade every default container for computer objects are set as default container for `computers/domaincontroller_master` except `cn=computers` and `cn=memberservers,cn=computer`. (Bug 46919)
- Re-add accidentally dropped patch to `insserv` to ignore files ending on `.debian`. (Bug 49441)
- `ucs-lint`: Also ignore temporary directory used by `dh_python2`. (Bug 42480)
- `ucs-lint`: Fixed applying `debian/ucslint.overrides` when used with paths. (Bug 49520)