UCS 4.2-3 Release Notes

**Release notes for the installation and update
of Univention Corporate Server (UCS) 4.2-3**

Table of Contents

Chapter 1. Release Highlights

With Univention Corporate Server 4.2-3, the third point release of Univention Corporate Server (UCS) 4.2 is now available. It provides several feature improvements and extensions, new properties as well as various improvements and bugfixes. An overview of the most important changes are:

◦ The UMC system diagnostic module has been extended with a large amount of additional tests. They the administrator to check the system health of the UCS system and the whole domain.

◦ The management system usability and configureability has been expanded. Wizards and dialogs have been redesigned regarding their useability. Additional configuration options for the single sign-on have been added, e.g. the certificate can now be configured.

◦ When joining into an active directory domain, additional checks are now executed. This enables the detection of known issues which are shown to the user along with advice how to fix them.

◦ Various security updates have been integrated into UCS 4.2-3, e.g. OpenLDAP, the Linux kernel, Samba, MySQL and PostgreSQL.

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 6 GB of disk space. Depending on the scope of the existing installation, the update will require about another 1 GB of disk space for download and installation all packages.

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.

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. Further notes on selected packages

5.1. Collection of usage statistics

Feedback ⌖

Anonymous usage statistics on the use of Univention Management Console are collected when using the *UCS Core Edition* (which is generally used for evaluating UCS). The modules opened are logged in 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*.

5.2. 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.

5.3. 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 37

◦ Firefox as of version 38

◦ Internet Explorer as of version 11

◦ Safari and Safari Mobile as of version 9

Users with older browsers may experience display or performance issues.

Chapter 6. Changelog

Listed are the changes since UCS *4.2-2*:

6.1. General

- All security updates issued for UCS 4.2-2 are included:

  - *univention-kernel-image* (CVE-2016-7097 CVE-2016-9191 CVE-2016-6213 CVE-2016-8405 CVE-2017-0786 CVE-2017-2583 CVE-2017-2584 CVE-2017-2618 CVE-2017-6951 CVE-2017-7184 CVE-2017-7346 CVE-2017-7472 CVE-2017-7482 CVE-2017-7518 CVE-2017-7533 CVE-2017-7541 CVE-2017-7542 CVE-2017-7558 CVE-2017-8831 CVE-2017-9605 CVE-2017-10663 CVE-2017-10810 CVE-2017-10911 CVE-2017-11176 CVE-2017-11473 CVE-2017-11600 CVE-2017-12153 CVE-2017-12154 CVE-2017-12192 CVE-2017-12762 CVE-2017-14156 CVE-2017-14489 CVE-2017-14991 CVE-2017-15265 CVE-2017-12188 CVE-2017-12193 CVE-2017-13080 CVE-2017-16528 CVE-2017-16532 CVE-2017-16537 CVE-2017-16645 CVE-2017-16646 CVE-2017-1000111 CVE-2017-1000112 CVE-2017-1000252 CVE-2017-1000255 CVE-2017-1000364 CVE-2017-1000365 CVE-2017-1000370 CVE-2017-1000371) (Bug 45242).

  - *dnsmasq* (CVE-2015-3294 CVE-2017-14491 CVE-2017-14492 CVE-2017-14493 CVE-2017-14494) (Bug 45617).

  - *univention-kernel-image-signed* (CVE-2016-7097 CVE-2016-9191 CVE-2016-6213 CVE-2016-8405 CVE-2017-0786 CVE-2017-2583 CVE-2017-2584 CVE-2017-2618 CVE-2017-6951 CVE-2017-7184 CVE-2017-7346 CVE-2017-7472 CVE-2017-7482 CVE-2017-7518 CVE-2017-7533 CVE-2017-7541 CVE-2017-7542 CVE-2017-7558 CVE-2017-8831 CVE-2017-9605 CVE-2017-10663 CVE-2017-10810 CVE-2017-10911 CVE-2017-11176 CVE-2017-11473 CVE-2017-11600 CVE-2017-12153 CVE-2017-12154 CVE-2017-12192 CVE-2017-12762 CVE-2017-14156 CVE-2017-14489 CVE-2017-14991 CVE-2017-15265 CVE-2017-12188 CVE-2017-12193 CVE-2017-13080 CVE-2017-16528 CVE-2017-16532 CVE-2017-16537 CVE-2017-16645 CVE-2017-16646 CVE-2017-1000111 CVE-2017-1000112 CVE-2017-1000252 CVE-2017-1000255 CVE-2017-1000364 CVE-2017-1000365 CVE-2017-1000370 CVE-2017-1000371) (Bug 45242).

  - *linux* (CVE-2016-7097 CVE-2016-9191 CVE-2016-6213 CVE-2016-8405 CVE-2017-0786 CVE-2017-2583 CVE-2017-2584 CVE-2017-2618 CVE-2017-6951 CVE-2017-7184 CVE-2017-7346 CVE-2017-7472 CVE-2017-7482 CVE-2017-7518 CVE-2017-7533 CVE-2017-7541 CVE-2017-7542 CVE-2017-7558 CVE-2017-8831 CVE-2017-9605 CVE-2017-10663 CVE-2017-10810 CVE-2017-10911 CVE-2017-11176 CVE-2017-11473 CVE-2017-11600 CVE-2017-12153 CVE-2017-12154 CVE-2017-12192 CVE-2017-12762 CVE-2017-14156 CVE-2017-14489 CVE-2017-14991 CVE-2017-15265 CVE-2017-12188 CVE-2017-12193 CVE-2017-13080 CVE-2017-16528 CVE-2017-16532 CVE-2017-16537 CVE-2017-16645 CVE-2017-16646 CVE-2017-1000111 CVE-2017-1000112 CVE-2017-1000252 CVE-2017-1000255 CVE-2017-1000364 CVE-2017-1000365 CVE-2017-1000370 CVE-2017-1000371) (Bug 45242).

  - *asterisk* (CVE-2017-14099 CVE-2017-14100 CVE-2017-14603) (Bug 45365).

  - *samba* (CVE-2017-14746 CVE-2017-15275) (Bug 45665).

  - *libav* (CVE-2015-8365 CVE-2016-9821 CVE-2016-9822 CVE-2017-7208 CVE-2017-7862 CVE-2017-9992) (Bug 44659).

  - *samba* (CVE-2017-12150 CVE-2017-12151 CVE-2017-12163) (Bug 38217 Bug 44305 Bug 45063 Bug 45388).

9

6.2. Domain services

6.2.1. OpenLDAP

- The description of the Univention Configuration Registry variable `ldap/acl/read/anonymous` has been fixed (Bug 37976).

- Cleanup old backups in *univention-ldap-backup* (Bug 38554).

6.2.1.1. LDAP ACL changes

- An LDAP ACL preventing access to objects with user ID `root` has been added (Bug 11800).

6.3. Univention Management Console

6.3.1. Univention Management Console web interface

- The styling of dialogs has been adapted to the new design (Bug 43999).

- The Univention Blog has been added to the help menu entries (Bug 45281).

- For privacy reasons the username is no longer stored in a cookie or in an HTML5 local storage, to remember the last logged in user (Bug 45461, Bug 45390).

- `build-report.txt` was removed from the Debian package *univention-web* (Bug 45391).

- The directory listing of `/var/www/univention/` has been disabled (Bug 45394).

- Adding and removing favorite modules now works properly again (Bug 44526).

- A failed login caused the login button to become invisible. This is now prevented (Bug 44989).

- The `max open files soft limit` of the UMC server has been raised (Bug 45309).

- The SAML authentication robustness has been improved. Errors during LDAP authentication now contain more information about the cause (Bug 44382).

- The text of app and module tiles is now resized dynamically e.g. when the screen size changes (Bug 45477).

- An UMC server crash which happened occasionally is prevented (Bug 45254).

- Long words in the descriptions of app and module tiles are now wrapped into a new line (Bug 45477).

- The styling of calendar and date selection widgets has been improved (Bug 45491).

- A standby animation is shown until all form values are loaded when modifying objects (Bug 45574).

- The transition for hiding and showing the Favorites category works properly again (Bug 44526).

- The selection in grids is now kept when changing the sort order or the visual presentation (Bug 45261).

- It was not possible to enable `checkboxes` which used the boolean syntax in an extended attribute with a default value of `1` because they were detected as already activated. This behavior has been corrected (Bug 45066).

- The search field in `combobox` widgets is shown again when the LDAP size limits are reached (Bug 44905).

- The `Content-Security-Policy` did not include https://piwik.univention.de if the Univention Configuration Registry `umc/web/piwik` had been set to false (Bug 45396).

- The help menu entries have been optimized (Bug 45281).

6.3.2. Univention Portal

- A portal entry to the Univention Blog has been added for Core Edition systems (Bug 45412).

- The portal site was empty when the portal name was not translated into English (`en_US`) (Bug 45688).

6.3.3. Univention Management Console server

- A crash of the UMC server is now prevented which happened while the system load is very high (Bug 45676).

- Since erratum 139 `umc/module/timeout` was not evaluated anymore which caused that the connection to module processes was closed after 30 seconds (Bug 45307).

6.3.4. Univention App Center

- App Logos are linked to the UMC front-end immediately after the initial System setup (Bug 45765).

- Improved the label in the App Center gallery: It is now more clear that Apps may be installed on other servers than the local host (Bug 41010).

- The handling of cache files is now more careful, leading to less error messages (Bug 45556).

- When connecting to the MySQL server fails during the installation of Apps with database integration, a helpful error message is shown instead of a traceback (Bug 44441).

- Fixed an issue when using the App Center on the command line without proper file descriptors (Bug 43238).

- Handle certain (SSL related) LDAP connection problems more gracefully (Bug 39325).

- Fixed the permissions of `PasswordFile` settings (Bug 45543).

- Improved handling of error messages in UMC (Bug 45569).

- Gracefully fail when the image of a Docker App cannot be downloaded (Bug 40110).

- The styling of dialogs has been adapted to the new design (Bug 43999).

- Minor styling adjustments when displaying `README` information before installation (Bug 44002).

- App installations now have finer grained error codes in case something goes wrong (Bug 43061).

- Fixed problems during the registrations of Apps (Bug 44502).

- The development tools now support App specific Test scripts (Bug 45493).

- The App Center could operate on an outdated cache. This has been fixed (Bug 44607).

- Fix problems when trying to upgrade an App that has no newer version (Bug 44384).

- The App Center now operates on Apps of the next UCS version while the upgrade to that version is running (Bug 45429).

- IPv6 addresses are now handled correctly and all available IP addresses of a system are written to the portal entry (beforehand, only the default IP addresses were used) (Bug 44117).

- Container passwords aren't changed anymore during container upgrades (Bug 43823).

- If the download of App meta data via `zsync` fails, the archive is downloaded via an HTTPS request (Bug 45227).

6.3.5. Univention Directory Manager UMC modules and command line interface

- Assign well known SIDs when creating users for well known security identifiers like `krbtgt`, `guest` or `administrator` (Bug 44333).

- The `sambaAcctFlags` attribute is now correctly set when the `locked` and `deactivated` properties are changed at once during modification of user objects (Bug 45287).

- `univention.admin.modules.update()` is now thread safe (Bug 45540).

- The misleading parameter name *module* has been renamed into *obj* in the stub methods of `simpleHook` (Bug 32375).

- Exceptions in the lookup function of policy and settings modules are now caught more granular (Bug 37171).

- The DNS module did not show any entries if an IPv6 reverse zone exists (Bug 45600).

6.3.6. Modules for system settings / setup wizard

- The styling of dialogs has been adapted to the new design (Bug 43999).

- The primary interface is set to the first configured one, avoiding not configured interfaces (Bug 40657).

- A warning is now shown when a UCS system tries to join into a domain with a lower UCS version on the UCS master (Bug 42059).

- UCS App appliances now check for a valid license before starting the join process (Bug 42910).

- The detection of the master domain controller FQDN during the initial system configuration has been fixed if the nameserver is not the DC Master (Bug 45170).

- When joining into an Active Directory domain where an UCS system is already part of an dialog to replace this system is shown if that system is not reachable (Bug 43745).

- When joining into an Active Directory domain any existing `_domaincontroller_master._tcp` SRV record will be replaced with the new one (Bug 43745).

6.3.7. Domain join module

- A test to check whether the UCS master uses the `memberOf` LDAP extension has been added to `univention-join` (Bug 42505).

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.3.8. Univention Directory Reports

- The files created by *univention-directory-reports* via the UMC module are now access protected (Bug 45644).

6.3.9. Process overview module

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.3.10. Printers module

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.3.11. Filesystem quota module

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.3.12. Univention Configuration Registry module

- The styling of dialogs has been adapted to the new design (Bug 43999).

- Cleanup old backups in `univention-config-registry-backup` (Bug 38554).

6.3.13. Other modules

- Various checks have been added to *univention-management-console-module-diagnostic* (Bug 36012, Bug 40393, Bug 44902, Bug 35858, Bug 44876, Bug 44881, Bug 35865, Bug 40465, Bug 35860, Bug 38974, Bug 40228, Bug 37628, Bug 35859, Bug 40605, Bug 45118, Bug 40227, Bug 35863, Bug 44875, Bug 44874, Bug 36748, Bug 38238).

6.4. Univention base libraries

- The installation of *univention-samba* while joining a DC Slave into an Active Directory domain is now more robust (Bug 45406).

- More debug output has been added to `admember.py` (Bug 38442).

- Ignore STDOUT in backup cleanup cron job (to avoid unnecessary cron mails) (Bug 45408).

- The referral handling in *univention-python* for modify operations has been fixed (Bug 45505).

- An `OrderedSet` implementation has been added (Bug 45249).

- Introduce Univention Configuration Registry variables `backup/clean/max_age`, `backup/clean/min_backups` and new function `clean_old_backups` (Bug 38554).

- Fixed issue in AD Member mode `check_ad_account` (Bug 44762).

- The re-connecting methods for `add` and `modify` of *python-ldap* are used to better handle SERVER_DOWN conditions. This was broken since erratum 116 (Bug 45474).

- A Python dictionary listing RIDs for well known security identifiers has been added (Bug 44333).

- The `PackageManger` now also holds the APT lock to prevent errors in the App Center (Bug 43619).

6.5. Software deployment

- App updates within `univention-upgrade` were searched within the wrong set of Apps. This has been fixed (Bug 45548).

- The error handling has been improved during querying update servers for maintenance information in *univention-updater*(Bug 44824).

6.6. System services

6.6.1. SAML

- The Apache certificates for the SAML virtual host `ucs-sso.$domainname` are now configurable via Univention Configuration Registry variables (Bug 40927).

- It is now possible to configure whether SAML errors and stack traces are displayed to the user via the Univention Configuration Registry variable `saml/idp/show-errors` (Bug 45393).

- The Apache directory listing for `/var/www/saml/` has been disabled (Bug 45394).

- The automatic redirection to the SAML single sign-on login may now be disabled by setting the Univention Configuration Registry variable `umc/web/sso/enabled` to false (Bug 45597).

6.6.2. Univention self service

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.6.3. Nagios

- A new plugin has been added that checks the Debian package status. The plugin is *not* registered by default on existing installations. If the plugin shall be used, the join script `30univention-nagios-client` has to be re-executed or the Nagios service `UNIVENTION_PACKAGE_STATUS` needs to be added in the computer's Nagios settings in the Directory Management (Bug 40370).

- Since (samba) erratum 165 the `UNIVENTION_SMBD` Nagios service failed. The service plugin has been fixed (Bug 45454).

- The `nscd` check has been fixed and should not incorrectly report the unknown program bound to nscd socket error anymore (Bug 45414).

6.6.4. Apache

- The exclusion rules defined in the Univention Configuration Registry variables `apache2/force_https/exclude/.*` are now interpreted as regular expression patterns (Bug 45449).

6.6.5. Radius

- The RADIUS helper program `univention-radius-ntlm-auth` now supports different formats for station ids, e.g. `1122.3344.5566` or `11-22-33-44-55-66`. All non-hexadecimal characters are removed automatically before checking the station id (Bug 42722).

6.7. Virtualization

6.7.1. Univention Virtual Machine Manager (UVMM)

- The styling of dialogs has been adapted to the new design (Bug 43999).

6.8. Container Technologies

- Only set nameserver Univention Configuration Registry variables from environment if not joined yet Docker Container Mode(Bug 45172).

6.9. Services for Windows

6.9.1. Samba

- The Samba parameter `name resolve order` can now be set through Univention Configuration Registry variable `samba/name/resolve/order` (Bug 37946, Bug 36089).

- New scripts `univention-samba-lockedout` and `univention-samba-unlock` to list the samba locked-out and unlock status of users have been added (Bug 35071).

- Support `<interfaces/primary>` as a keyword for the Univention Configuration Registry variable `samba/interfaces` has been added. Now, newly installed Samba 4 systems will set `samba/interfaces` to `lo` and the primary interface which is represented via `interfaces/primary`. Thus, Samba will by default only listen on those two interfaces. This can be configured afterwards via Univention Configuration Registry variables `samba/interfaces`, `samba/interfaces/bindonly` and `samba/register/exclude/interfaces` (Bug 35072).

- The Univention Configuration Registry variable `samba/logonscript` has been removed (Bug 41057).

- Improve cleanup of old backups in `univention-samba4-backup` (Bug 38554).

- Create `Windows 10` default profile (`default.V6`) in ***univention-skel*** (Bug 44895).

- The listener module for samba shares now correctly encodes filenames. Share names containing special characters caused errors (Bug 45338).

- Fixed samba drivers permission in join script and `postinst` (Bug 41849).

- Abort samba provision during join if broken symbolic links in `/var/lib/samba/sysvol/` are found (Bug 45062).

- Run `samba-tool dbcheck --cross-ncs --fix --yes` on update if there are inconsistencies. A backup of `/var/lib/samba/private/` is performed and the fix is skipped if the available disk space is too low (Bug 44635).

- Some special options for joining Samba Slaves PDCs in UCS@school were ignored. This has been fixed (Bug 44885).

- The join of (administrative) Samba Slaves PDCs in UCS@school has been fixed (Bug 45596).

- The listener module for samba shares now correctly encodes filenames. Share names containing special characters caused errors (Bug 38688).

6.9.2. Univention S4 Connector

- The S4 connector no longer overwrites the *msGPO* links in OpenLDAP while joining the UCS system (Bug 45439).

- A check for the correct RID of the `krbtgt` account (and fix if possible) has been added (Bug 44333).

- The detection of the primary group during creation of user objects with special characters in their *samAccountName* has been fixed (Bug 44374).

- UCS@school specific settings have been moved into the join script (Bug 45210).

- The S4 Connector now handles invalid pickle files (Bug 34648).

◦ An error during removing a GPO has been corrected (Bug 45088).

◦ The S4 Connector synchronizes attributes with a case sensitive compare. Previously a case insensitive compare was the default (Bug 39309).

6.9.3. Univention Active Directory Connection

◦ Adapt to code changes in ***univention-lib*** (Bug 43745).

◦ The error handling in the UMC module has been improved (Bug 41619).

◦ It is now prevented to start multiple instances of the AD Connector (Bug 41335).

◦ LDAP operations are now correctly escaped in the AD Connector (Bug 11658).

◦ It is possible to start the AD Connector service process in foreground (Bug 45037).

◦ Fixed errors in the SQLite escaping in the AD Connector (Bug 38619).

◦ `univention-adsearch` now accepts multiple attributes in the LDAP filter (Bug 45134).

◦ Some objects were identified as the wrong object type. The identification handling has been fixed (Bug 45011).

◦ The AD-Connector skips (re)recreation of UDM deleted objects (Bug 40813).

◦ Fixed a deletion problem with nested groups in the AD Connector (Bug 18680).

6.10. Other changes

◦ The styling of App Appliance dialogs have been adapted to the new design (Bug 43999).

◦ The default value of the Univention Configuration Registry variable `repository/mirror/recreate_packages` has been changed to `no`, as re-creating the `Packages` files without the corresponding `override` files breaks `debootstrap` (Bug 45185).

◦ Move cache invalidation after daemon restart for `nscd` (Bug 40371).

◦ On DC backup and slave check for pending listener transactions before changing the server password (Bug 39283).

www.univention.de