UCS 4.2-1 Release Notes

**Release notes for the installation and update
of Univention Corporate Server (UCS) 4.2-1**

Table of Contents

Chapter 1. Release Highlights

With Univention Corporate Server 4.2-1, the first point release of Univention Corporate Server (UCS) 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:

◦ Forwarding of e-mails can now be stored per mail user in the management system.

◦ Changing the password via UMC has been improved. This allows users from a Microsoft Active Directory domain to change their expired password. In addition, more information is shown if the password change fails.

◦ The IPv6 configuration of several services have been improved, for example the Nagios or proxy server configuration and the management system.

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

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

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

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 *4.2-0*:

6.1. General

Feedback🗩

- All security updates issued for UCS 4.2-0 are included:

  - *samba* (CVE-2017-7494) (Bug 44612).

  - *openssl* (CVE-2016-7055 CVE-2016-8610 CVE-2017-3731 CVE-2017-3732) (Bug 44751).

  - *python-cryptography* (CVE-2016-9243) (Bug 44741).

6.2. Univention Installer

Feedback🗩

- The configuration file of *univention-net-installer* has been upgraded to use the Apache 2.4 syntax (Bug 44213).

6.3. Domain services

Feedback🗩

6.3.1. OpenLDAP

Feedback🗩

6.3.1.1. LDAP schema changes

Feedback🗩

- The LDAP scheme has been expanded by additional LDAP attributes to add support for forwarding user emails to external addresses (Bug 42249).

- The possibility to change the font color on the portal page has been added (Bug 44697).

6.3.1.2. Listener/Notifier domain replication

Feedback🗩

- The BDB cache is now migrated to MDB in case it didn't happen during update (Bug 44466).

6.4. Univention Management Console

Feedback🗩

6.4.1. Univention Management Console web interface

Feedback🗩

- Values inside of grids are now sorted locale aware (Bug 44361).

- Allow UMC feedback dialog for non traceback errors (Bug 44527).

- The link to send feedback to Univention has been fixed (Bug 44381).

- The way a grid is sorted is now better configurable for module developers (Bug 44652).

- Progress bars are now escaping HTML content more strict (Bug 44498).

6.4.2. Univention Portal

Feedback🗩

- The possibility to change the font color on the portal page has been added (Bug 44697).

6.4.3. Univention Management Console server

- The reason why changing the password failed is shown again (Bug 41786).

- An error during login via SAML has been fixed (Bug 44217).

- A redirection loop during SAML login is prevented (Bug 44450).

- The PAM configuration has been adjusted to make password changes possible again if the password was expired (Bug 43859).

- The error handling on module initialization has been improved (Bug 44428).

- If the URL to access UMC contained a port a XSRF attack was wrong detected causing UMC to be unusable. This has been fixed (Bug 44564).

- The link to send feedback to Univention has been fixed (Bug 44381).

- A crash of the UMC server during handling of errors has been fixed (Bug 44365).

- A notification about the Administrator account is shown when trying to login as root (Bug 40986).

- After a failed attempt to change an expired user password via the login dialog the form fields weren't reset resulting in further authentication attempts being impossible (Bug 44720).

6.4.4. Univention App Center

- The App Center now uses a different directory for special temporary files for Docker Apps to avoid problems with the System V init *tmp* cleanup (Bug 44501).

- During the remove of Docker Apps, the App is stopped via the init script (Bug 44286).

- Error handling has been improved (Bug 44493).

- Some Docker Apps did not register their user management extensions properly. This has been fixed (Bug 44550).

- Handle errors for package manager lock during docker installation in UMC (Bug 41303)

- Handle *BadStatusLine* line error (Bug 34543).

- Admin credentials are now passed to a preinst script during App installation / upgrade (Bug 44654).

- Progress bars are now escaping HTML content more strict (Bug 44498).

- Start containers with the hosts proxy settings by default (Bug 44561).

- A script can now be run after configuring an App (Bug 44750).

- Under certain circumstances, it was possible that the CLI selected the wrong App version. This issue has been fixed (Bug 44724).

- *AdditionalPackages* defined by the App are no longer removed when uninstalling an app (Bug 44778).

- The cron job for the updater check has been deactivated in ***univention-docker-container-mode*** (Bug 44630).

- A template for Docker proxy settings has been added (Bug 44536).

www.univention.de

6.4.5. Univention Directory Manager UMC modules and command line interface

- The unmaintained and deprecated internal test suite has been removed (Bug 27286).

- Fix handling of "Change password on next login" for new user accounts (Bug 42148).

- Support for forwarding user emails to external addresses has been added (Bug 42249).

- The error handling regarding LDAP size limits has been improved (Bug 42533).

- Creating computers with IPv6 addresses is possible again (Bug 44152).

- Fix typo in users module when reading the minimal password length (Bug 44472).

- The default value of extended attributes which don't define any default has been changed from an empty string to None (Bug 41053).

- A regression in UCS 4.2 has been fixed which caused that DHCP pools which have values unknown by UDM in its *dhcpPermitList* could not be opened or modified anymore (Bug 44611).

- The font color on the portal page can be configured now (Bug 44697).

- Default values (especially from extended attributes) are now pre filled when modifying objects (Bug 41053).

6.4.6. Modules for system settings / setup wizard

- The AWS Apache start site link has been corrected (Bug 42133).

- The package *univention-self-service-master* is now also downloaded while preparing an appliance (Bug 44284).

- The package *univention-samba* is now also downloaded while preparing an appliance (Bug 44522).

- A cleanup script used in Univention App Appliances has been adapted for UCS 4.2 (Bug 44575).

- IP address changes are now also applied to portal entries (Bug 43671).

- When selecting fast demo mode in an App Appliance, all IP addresses in LDAP are reconfigured to the correct address (Bug 43140).

- The overview of changed network settings doesn't show HTML code anymore (Bug 41204).

- The decision between joining systems into UCS or Active Directory domains was confusing and has been improved (Bug 44035).

- A crash is prevented when trying to join into an Active Directory domain and the Active Directory server is not reachable (Bug 44394).

- A crash is prevented in appliance scenarios if no domain name was entered (Bug 43273).

6.4.7. Mail

- The UMC module System services showed the Cyrus IMAP service always as stopped. It does now show the correct service state. This issue has been fixed (Bug 44594).

6.5. Software deployment

- The file containing the APT repository during a UCS release update is no longer deleted on failures to allow fixing failed updates more easily (Bug 44346).

- A check to deny update on UCS member servers with the package slapd has been added to the updater preup script (Bug 44650)

6.6. Univention base libraries

- Make DNS lookup more robust for Kerberos `kinit` in *admember.check_ad_account* (Bug 38285).

- Handle *NoAnswer* exception of `dns.resolver` when looking for *_domaincontroller_master._tcp* SRV record during Active Directory member setup (Bug 38788).

- Properly stop Samba before running the Active Directory member setup (Bug 44144).

- The re-connecting methods for add and modify of python LDAP are used to better handle *SERVER_DOWN* conditions (Bug 44316).

6.7. System services

6.7.1. Univention self service

- The `memcache` service for the self service module did not start, because it was misconfigured. This issue has been fixed (Bug 44477).

6.7.2. Mail services

- The Fetchmail password attributes now disallows substring searches and are not searchable in UMC anymore (Bug 41336).

- The Fetchmail ACLs now respect overridden default group names (Bug 33648).

- After an upgrade from UCS 4.1 to UCS 4.2 the Cyrus daemons did not start automatically anymore. When installing this update the service will be enabled automatically in systemd (Bug 44377).

- The paths to Cyrus executables have been adjusted for Debian Jessie (Bug 44424, Bug 44566).

- The path to the tool to automatically purge old entries from the Cyrus "duplicate delivery database" has been fixed. As the path was wrong in the past, the tool never ran. When starting it (the first time), it may take minutes or hours (depending on the database size). Via the new Univention Configuration variables `mail/cyrus/duplicate-supression/expiry/start` and `mail/cyrus/duplicate-supression/expiry/event` this cleanup job can be configured to be run when starting Cyrus or regularly at 4:01 each night (Bug 22852).

- The package dependencies allow now to install Dovecot Pro instead of Dovecot from the UCS repositories (Bug 44559).

- Support for forwarding user emails to external addresses has been added. During the update, the Univention Configuration variables `mail/postfix/virtual/alias/maps` and `mail/postfix/virtual/mailbox/maps` are updated automatically, because some postfix virtual lookup tables have been modified. Please note, that the forwarding of emails on systems with OX App Suite will only come into effect if at least version 7.8.3-ucs2 of OX App Suite is installed (Bug 42249).

- The default of the UCR variable `mail/postfix/tls/client/level` when unset has been changed to "may". On existing UCS installations this has already been set explicitly (Bug 44589).

◦ When a relay host with authentication is used (*mail/relayauth=yes*), the Postfix option *smtp_tls_security_level* will automatically be set to "encrypt", unless `mail/postfix/tls/client/level` is set to "none" (Bug 44589).

◦ Entries in the SMTP client TLS policy table can now be configured for each domain or mail exchanger individually through the UCR variables `mail/postfix/tls/client/policy/.*` (Bug 44811).

6.7.3. Printing services

◦ Samba is now reloaded after printer has been created (Bug 44153).

6.7.4. Nagios

◦ IPv6 support for allowed hosts has been added (Bug 44454).

6.7.5. Kerberos

◦ User accounts from Active Directory are now able to change their expired password via UMC (Bug 43859).

6.7.6. Proxy services

◦ When switching to UCS 4.2 the program name of squid's Kerberos authentication handler has changed. The authentication helper of ***univention-squid*** has been changed accordingly (Bug 44287).

◦ Allow IPv6 addresses in UCR variable `squid/allowfrom` (Bug 29576).

6.7.7. Apache

◦ Exceptions for the `apache2/force_https` configuration can now be configured via UCR. When `apache2/force_https` is enabled, by default "localhost" will be excluded (Bug 44628)

6.7.8. Radius

◦ Allow *TTLS* to be disabled via UCR `freeradius/conf/auth-type/ttls` (Bug 42728)

◦ Allow the ports the server listens on to be configured via UCR `freeradius/conf/port` and `freeradius/conf/accountingport` (Bug 42729).

◦ Allow the maximum number of requests which the server keeps track of to be configured via UCR `freeradius/conf/max_requests` (Bug 42730).

6.8. Virtualization

6.8.1. Univention Virtual Machine Manager (UVMM)

◦ The unused PAM access file has been removed (Bug 33702).

6.9. Services for Windows

6.9.1. Samba

◦ The UCR variable `samba/idmap/range` has been added to configure the *uid* and *gid* range for the default (*) `idmap` backend. This can be used to avoid overlaps between that default range and the domain specific setting, which is configurable via `samba/idmap/$windows_domain/range` (Bug 44549).

- The UCR variables `samba/client/min/protocol`, `samba/min/protocol` and `samba/client/max/protocol` have been added. Please be aware that raising `samba/min/protocol` e.g. to SMB2 also requires raising `samba/client/max/protocol` to that value or higher (Bug 44591).

- Improve handling of *tombstoned* DNS objects during *DDNS* update (Bug 39806).

- Keep *DNS_TYPE_TOMBSTONE* value marker and *dnsTombstoned* attribute in sync (Bug 39806).

- Allow *DDNS* update if the account name of authenticated machine matches the name of the target record (Bug 41190).

- Don't fail join if *CNF* objects are in *serverReferenceBL* (Bug 43280)

- Don't consider unreachable UCS@school Slave DCs for joining (Bug 43478)

- Support uppercase *CN* attribute in `sysvol-cleanup.py` (Bug 43620)

- Adjust `check_essential_samba4_dns_records.sh` to change of behavior of the `host` command in UCS 4.2 (Bug 44535)

- The UCR variables `samba/client/min/protocol`, `samba/min/protocol` and `samba/client/max/protocol` have been added. Please be aware that raising `samba/min/protocol` e.g. to SMB2 also requires raising `samba/client/max/protocol` to that value or higher (Bug 44643).

- Make `sysvol-sync.sh` robust against varying *stderr* output from `rsync` (Bug 44694).

- Update Samba package and restart BIND9 on upgrade to make BIND9 load the updated dlz_bind9 module version, which contains improvements in the handling of *DDNS* updates (Bug 39806, Bug 41190).

6.9.2. Univention AD Takeover

Feedback 💬

- Avoid traceback in case AD Takeover is run in AD member mode (Bug 38983).

6.9.3. Univention S4 Connector

Feedback 💬

- Fix fetching the SID in *sync_from_ucs ALREADY_EXISTS* handling (Bug 43368)

- Fix handling special case of *Printer-Admins* (Bug 44276)

- Fix the handling of UTF-8 encoded DNs (Bug 44276)

- Don't append a trailing dot to DNS alias values if there is no dot (Bug 31311).

- Allow removal of specific sub-objects objects in *sync_from_ucs* (Bug 33882).

- Don't consider unreachable UCS@school Slave DCs when looking for hosts (Bug 43478). running a S4-Connector

- Fix handling of *Printer-Admins* (Bug 44517).

6.10. Other changes

Feedback 💬

- The KDM init script now waits for the stop of the plymouth bootsplash before starting and presenting the KDE login window (Bug 44452).

www.univention.de

- A symbolic link has been added to enable *debootstrap* for UCS 4.2 (Bug 44593).

- All *postgresql-9.4* packages are now available in UCS 4.2 (Bug 44507).

- Missing French translations have been updated (Bug 44133).

- Removed the App re-registration during the upgrade to UCS 4.2-1. This was only necessary for upgrades to UCS 4.2-0 (Bug 44812).