univention
be open.

UCS 4.1-3 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 4.1-3

Mary-Somerville-Straße 1, 28359 Bremen, Deutschland/Germany

<feedback@univention.de>

univention
be open.

Table of Contents

Chapter 1. Release Highlights

With Univention Corporate Server 4.1-3, the third point release of Univention Corporate Server (UCS) 4.1 is now available. It provides various improvements and bugfixes. An overview of the most important changes:

- Several important security updates have been integrated in UCS 4.1-3, among others for libvirt, OpenSSL, QEMU and Samba. Furthermore, security updates in the standard LDAP ACLs and the UMC servers have been integrated.
- The App Center has been further developed in many places and more options have been implemented for migrating Apps to Docker Apps.
- The replication of directory service objects has been stabilized for several corder cases.
- The domain join of additional Samba based domain controllers is now possible with more than 100.000 directory service objects.
- The App Appliances have been expanded, so it is now possible for App providers to define their own branding, and to activate a fast demo mode. This allows a quick test of a pre-configured appliance.

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 2 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 4.1-2:

6.1. General

Feedback

- All security updates issued for UCS 4.1-2 are included:
  - ***openssl*** (CVE-2016-2105 CVE-2016-2106 CVE-2016-2107 CVE-2016-2108 CVE-2016-2109) (Bug 41197).
  - ***libvirt*** (CVE-2015-5313) (Bug 40317).
  - ***qemu-kvm*** (CVE-2015-7295 CVE-2015-7504 CVE-2015-7504 CVE-2015-7512 CVE-2015-8345 CVE-2015-8504 CVE-2015-8558 CVE-2015-8743 CVE-2016-1568 CVE-2016-1714 CVE-2016-1922 CVE-2016-3710 CVE-2016-3712) (Bug 40634).
  - ***qemu*** (CVE-2015-7295 CVE-2015-7504 CVE-2015-7504 CVE-2015-7512 CVE-2015-8345 CVE-2015-8504 CVE-2015-8558 CVE-2015-8743 CVE-2016-1568 CVE-2016-1714 CVE-2016-1922 CVE-2016-3710 CVE-2016-3712) (Bug 40634).
  - ***imagemagick*** (CVE-2016-3714 CVE-2016-3715 CVE-2016-3716 CVE-2016-3717 CVE-2016-3718) (Bug 41331).
  - ***libgd2*** (CVE-2015-8874 CVE-2016-3074) (Bug 41209).
  - ***openjdk-7*** (CVE-2015-7575 CVE-2015-8126 CVE-2015-8472 CVE-2016-0402 CVE-2016-0448 CVE-2016-0466 CVE-2016-0483 CVE-2016-0494 CVE-2016-0636 CVE-2016-0686 CVE-2016-0687 CVE-2016-0695 CVE-2016-3425 CVE-2016-3427) (Bug 40483).
  - ***graphicsmagick*** (CVE-2016-5118) (Bug 41441).
  - ***imagemagick*** (CVE-2016-5118) (Bug 41439).
  - ***samba*** (CVE-2016-2119) (Bug 41729).

6.2. Basic system services

Feedback

6.2.1. Univention Configuration Registry

Feedback

- Setting an UCR variable with the conditional "?" operator didn't set the variable if it already existed in another scope. This is changed to only check the scope the variable is set in (Bug 40728).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- Starting the LDAP daemon on *i686* systems with a MDB backend and a MDB `maxsize` of at least 2147483648 could potentially fail. The init script now triple checks the start (Bug 33993).

6.3.1.1. LDAP ACL changes

Feedback

- Access to the UVMM object classes is now more restrictive (Bug 41723).

- Regular users are prevented from changing their object class (Bug 41179).
- Users can now only create objects with *univentionAdminUserSettings* object class underneath of *cn=admin-settings* (Bug 41180).
- Various restrictions for Memberserver and Domaincontrollers have been added to the LDAP ACL (Bug 41715).

6.3.1.2. Listener/Notifier domain replication

Feedback

- IPv6 support was added to `get_notifier_id.py` (Bug 39509).
- The help messages for `univention-directory-listener-ctrl` have been improved. Also two new subcommand `modules` and `status` have been added (Bug 3490).
- Some string and integer comparison bugs have been fixed (Bug 38696).
- The Listener did not drop root privileges in all error cases. This issue has been fixed (Bug 34324).
- Some old and no longer needed code has been removed to reduce the memory footprint (Bug 30227).
- Some debug messages have been cleaned up (Bug 34738).
- Some data structures are no longer allocated dynamically but put onto the stack to make the Listener more robust against memory allocation problems (Bug 34507).
- A bug in handling the notifier ID has been fixed: If the Listener was restarted multiple times, the last processed transaction ID could be lost. This led to all transactions being skipped which happened in between (Bug 41261).
- The locking has been improved to prevent multiple instances of the Listener running at the same time (Bug 22383).
- The transaction log is now only written on systems where the Notifier is installed as well to prevent the hard disk from filling up (Bug 40600).
- The code for *flat-mode* replication has been removed (Bug 30489).
- The check for a full file system was inverted and has been fixed (Bug 28232).
- LDAP objects having a multi-valued RDN attributes are now handled correctly during a rename and move (Bug 33594).
- A traceback in failed LDIF mode has been fixed (Bug 41347).
- The replication module now logs more information in case of an object class violation (Bug 31757).
- The replication module no longer runs as the user root. The directory `/var/lib/univention-directory-replication/` is now owned by the user listener. The `failed.ldif` files are now owned by the user listener and the LDAP connections are now made by the user listener (Bug 34324).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- UMC is now also usable in Chrome 51 (Bug 41224).
- Show a warning message if browser cookies are disabled and ask the user to enable them (Bug 28665).

- Make it possible to collect usage data from the system setup to make future improvements to the user experience even better (Bug 40551).

6.4.2. Univention Management Console server

Feedback

- The Sanitizer base class now accepts a parameter `allow_none` to allow `None` values (Bug 41424).
- A new *DNSanitizer* has been added, to validate LDAP distinguished names (Bug 41423).
- A UMC server crash is now prevented in specific circumstances after login (Bug 41070).
- A UMC server crash is now prevented for requests with malicious request data (Bug 41370).
- The UMC client does not evaluate python code in its arguments anymore (Bug 41736).

6.4.3. Univention App Center

Feedback

- When upgrading a regular App to a Docker App, the Apache proxy settings were not written correctly. This has been fixed (Bug 41178).
- The German and English description about the sale of licenses and support in the Univention App Center has been aligned (Bug 40757).
- Docker Apps did not register their web interface correctly in the UCS overview site. This has been fixed (Bug 40842).
- When Docker Apps were updated, a new version of the shipped join script was not recognized. This has been fixed, the join script is now correctly installed and executed (Bug 41452).
- The button on the App page which read *Open module* or *Open Website* has been relabeled to just *Open* (Bug 41227).
- One could not uninstall Apps that other Apps required to be installed somewhere in the domain, even if this App was installed several times. This has been fixed (Bug 41217).
- Minor code changes make other projects easier that rely on the App Center (Bug 41360, Bug 41770).
- Uninstalling an App failed when the App was not properly registered before (Bug 41542).
- Tests run before upgrading an App used the installed version, not the to-be-installed version (Bug 41532).
- A function to detect a docker bridge network conflict has been added (Bug 41596).
- The use of UDM handler objects has been optimized (Bug 41658).
- Access to the object class *univentionApp* is now more restrictive (Bug 41724).
- The App Center now displays a warning if a conflict between the systems network settings and the docker bridge network has been detected (Bug 40515).
- When searching for Apps, the Vendor (and Maintainer) of the App is considered (Bug 41702).
- Apps may now require a specific version to be already installed, before an upgrade is possible (Bug 33537).
- When opening an App in the Gallery that is not yet installed, a notification is sent to Univention (Bug 41690).
- When (un)installing an App, a notification is always sent to Univention. If the App does not say otherwise, this notification is anonymized (Bug 41691).

- When a non Docker version of an App was installed, the upgrade to a Docker version is prohibited unless the App says it is safe to upgrade (Bug 41804).
- The App Center sometimes installed the last-to-latest App version (Bug 41841).
- Executing missing join scripts in a Docker Container is now supported (Bug 39551).

6.4.4. Univention Directory Manager UMC modules and command line interface

Feedback

- Extended options are now also evaluated for user objects (Bug 41017).
- The UDM command line tool now supports the use of `--remove` on single value attributes. Before `--set attribute=` had to be used (Bug 41172).
- Some old code which handled custom attributes has been removed (Bug 41266).
- The object class of extended options is now always added or removed to the object without the need to change an attribute (Bug 25240).
- The extended attribute option to remove the object class if it is no longer needed has been re-enabled (Bug 41207).
- The attribute *sambaPwdLastSet* is now set for computer objects while changing the password (Bug 41367).
- Syntax classes based on UDM_Attribute with single value attributes has been fixed to correctly detect the possible field values (Bug 41290).
- Extended options are now always evaluated when instantiating a UDM object (Bug 41580).
- Special characters (such as +) are now correctly escaped when composing a DN for a newly created object (Bug 40041).
- Some LDAP filters are now properly escaped (Bug 40129).
- A man in the middle attack and a local root code execution vulnerability in the UDM CLI client has been fixed (Bug 40422).

6.4.5. Modules for system settings / setup wizard

Feedback

- This update publishes some minor adjustments in the source code (Bug 40913).
- The package ***phantomjs*** has been added. It is necessary for the new App appliances (Bug 40934).
- Apps may now provide design information for branding UCS appliances (Bug 40826).
- Apps may now provide more detailed information on the first steps to take after their initial installation/setup (Bug 38957).
- App appliances may be configured to offer a fast setup mode with a pre-configured UCS domain (Bug 41622).
- A new option for setting up a UCS system has been added which allows a fast instantiation for demo purposes. Some more aspects of the setup process have been improved w.r.t. reliability and speed (Bug 40046).
- Some more corrections have been applied for the fast UCS instantiation (Bug 41283, Bug 41932).

- A UCR variable for enabling/disabling the fast instantiation has been added (Bug 41622).
- Problems with a hanging setup process when finishing have been corrected (Bug 40985).
- The timeout for internal LDAP queries during changes of network configurations has been adjusted for the UCS setup process (Bug 40968).
- The rendering of the welcome screen after booting a UCS system has been improved and OverlayFS log messages have been removed (Bug 41026).
- Problems with a disabled repository after setup have been corrected (Bug 40710).
- An error dialog has been corrected which eventually showed up during the setup process stating that no module would be available (Bug 40751).
- A typo in the header for the initial setup of UCS on an Amazon EC2 instance has been corrected (Bug 40673).
- Enable collection of usage data during the system setup to allow future improvements to the user experience (Bug 40551).
- Regenerate the system UUID during the fast setup demo mode to ensure a unique system (Bug 41140).
- Errors that occur during the system setup of UCS can now be sent as feedback to Univention by the user (Bug 40782).
- Redirection problems for app appliances at the end of the setup wizard have been corrected (Bug 41793).
- The AD connector is now automatically installed if UCS is joining an AD domain (Bug 37333).

6.5. Software deployment

Feedback

- The command `univention-add-app` has been adapted to reflect changes in the App Center package (Bug 33537).
- Clarified a confusing message when UCS release updates are blocked because of missing Apps or components (Bug 40458).
- The Updater was adapted for UCS 4.1-3 (Bug 41895).

6.6. Univention base libraries

Feedback

- The method *get_schema()* has been added to the class *univention.uldap.access* which returns LDAP schema information (Bug 41207).
- A faulty policy type detection has been fixed that could lead to wrong results of `univention_policy_result`. This misbehavior affected the DHCP service and other services using `univention_policy_result` (Bug 41641).
- The python ldap utilities are now used for splitting a DN's in *univention.ulap* (Bug 40129).
- Handling of DN's has been improved (Bug 40041).
- No modrdn operations are performed anymore if the DN didn't changed when modifying a object with uppercase letters in the attribute name of its RDN. This was a regression caused by UCS 4.1-2 errata 207 (Bug 41785).

6.7. System services

Feedback

6.7.1. SAML

Feedback

- The SAML package is now handled in the translation process (Bug 41222).

6.7.2. SSL

Feedback

- `univention-certificate check` now also checks the expiry date of the certificate (Bug 31369).
- `univention-certificate new` now also accepts the `-days` parameter (Bug 39257).
- `univention-certificate` now checks the UCS server role, as its full functionality is only available on the 'DC Master' (Bug 24094).
- Changing the Univention Configuration Registry variable `ssl/default/hashfunction` and `ssl/default/bits` now takes immediate effect (Bug 40498).
- During the initial CA creation *2.debian.pool.ntp.org* is used in addition, which also contains IPv6 capable time servers (Bug 25285).
- The certificate revocation list in now updated periodically. The intervals are configured through the Univention Configuration Registry variable `ssl/crl/interval` and `ssl/crl/validity` (Bug 35748).
- The SSL extension example has been fixed to work with with non-bash-shells (Bug 39045).
- Locking has been added to prevent parallel execution when managing certificates (Bug 35027).
- Server certificates are no longer revoked and re-created when the LDAP host entry is only moved (Bug 41230).
- The new Univention Configuration Registry variable `ssl/ca/cipher` can be used to chose the encryption mechanism for the private key of the root CA. The new default is *aes256* (Bug 37621).
- The new Univention Configuration Registry variable `ssl/host/objectclass` can be used to configure the LDAP object classes for which SSL certificates are automatically created (Bug 38903).
- Some shell variable quoting problems have been fixed in the shell library for SSL handling (Bug 41917).

6.7.3. Proxy services

Feedback

- The timeout for the SPN account samba search in the join script has been increased (and is now configurable via the Univention Configuration Registry variable `squid/kerberos/join/timeout`) (Bug 41443).

6.7.4. PAM / Local group cache

Feedback

- The Name-Service-Switch (NSS) module *extrausers* is used to get user group information from LDAP. The implementation of `getgrouplist()` was not thread-safe, which caused (for example `libvirtd`) to crash on restart. Proper locking has been added (Bug 39775).

6.8. Virtualization

Feedback

6.8.1. Univention Virtual Machine Manager (UVMM)

Feedback

- Allow creating snapshots of VMs with more than 4 GiB RAM which is supported with QEMU since version 1.1 (Bug 35581).

- A default password for all VNC sessions can be configured through the new Univention Configuration Registry variable `uvmm/kvm/vnc/password` (Bug 41340).

6.9. Container Technologies

Feedback

- The docker daemon options are now configurable via the Univention Configuration Registry variable `docker/daemon/default/opts/$PARAM=$VALUE` (Bug 40515).
- The start of the docker daemon is aborted if a docker bridge network conflict has been detected (Bug 40515).
- Use the docker *bip* setting for docker specific iptables rules (Bug 40515).
- Workaround cron hard-link issue on OverlayFS (Bug 39677).
- Executing missing join scripts in a Docker Container is now supported (Bug 39551).

6.10. Services for Windows

Feedback

6.10.1. Samba

Feedback

- This update fixes regressions from Errata update 411 (Bug #40988) (Bug 41193).
- The default RPC timeout has been increased from 60 to 480 seconds. Thus, a join with more than 100.000 objects will work (Bug 41021).
- Reliability of `samba_dnsupdate` has been improved on UCS@school DC Slaves by using localhost for DNS related Kerberos operations. This fixes an intermittent error in the `98univention-samba4slavepdc-dns.inst` joinscript (Bug 34908).
- The restart command of the samba init wrapper script has been adjusted to avoid restarting `samba-ad-dc` after NMBD (Bug 41551).
- The *GetGroupsForUser* SAMR RPC call has been adjusted to make use of the *memberOf* attribute (Bug 41644).
- Two additional regression patches from the *badlock* update have been merged (Bug 41729).

6.10.2. Univention S4 Connector

Feedback

- The mapping for *msPrintConnectionPolicy* has been fixed (Bug 41309)..
- A restart of the Samba LDAP server during the initialization phase of the connector could lead to an endless loop in the the initialization. This issue has been fixed (Bug 41288).
- Add support for overriding IPv4 and IPv6 addresses of specific DNS host records. Feature added for upcoming UCS@school release (Bug 41482).
- Allow recreation of object deleted in Samba/AD if visible in OpenLDAP (Bug 41756).
- Allow recreation of account deleted in Samba/AD if *objectSid* matches (Bug 41864).
- When an object gets moved out of visibility for an UCS@school Samba/AD PDC Slave attributes passed to the S4-Connector were mixed up. This caused the next object modified to be marked internally as deleted by the S4-Connector, while it is perfectly healthy in fact. While this update fixes the issue, manual steps are be required to unmark the objects and restore normal sync (Bug 41884).

6.10.3. Univention Active Directory Connection

Feedback

- A traceback due to empty *proxyAddresses* in AD during the synchronization has been fixed (Bug 41246).
- Close the SAMR user connection during password sync to Active Directory (Bug 41247).

6.11. Other changes

Feedback

- `ucslint` no longer warns about files processed by some `debhelper` scripts supporting the `--name` argument (Bug 41603).
- `ucslint` now also accepts `"${@}"` for padding join credentials (Bug 34253).
- `ucslint` warns when `univention-ldapsearch -x` is used (Bug 38853).
- The boot splash has been extended to allow adjustments of its design (Bug 41821, Bug 39465).
- The package ***univention-mysql*** has been added. It allows to configure arbitrary MySQL settings through UCR variables named `mysql/config/$group/$option` (Bug 39471, Bug 40216).
- When installing a translation generated by this package, UCR variables concerning the locale are now set correctly (Bug 40917).
- JavaScript files are now handled correctly on package generation (Bug 40936).
- The translation process is simplified by requiring less steps (Bug 41223).