univention
be open.

UCS 4.1-2 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 4.1-2

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 4.1-2, the second 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 4.1-2, among others for Samba, Apache, OpenSSL and the GNU C Library (glibc).
- The update to Samba 4.3.7 includes various security updates. In addition, several issues have been fixed, for example, failed login attempts are now counted correctly.
- The Active Directory Connector now uses Active Directory standard interfaces for synchronizing the password hashes. Thus, the Windows password synchronization service is no longer needed.
- The presentation of the apps in the Univention App Center has been improved, among others the App license terms are now displayed.

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 4.1-1:

6.1. General

Feedback

- All security updates issued for UCS 4.1-1 are included:
  - ***eglibc*** (CVE-2014-8121 CVE-2015-1781 CVE-2015-7547 CVE-2015-8776 CVE-2015-8777 CVE-2015-8778 CVE-2015-8779) (Bug 40022).
  - ***samba*** (CVE-2015-7560) (Bug 40680).
  - ***sudo*** (CVE-2015-5602) (Bug 40364).
  - ***apache2*** (CVE-2015-3183) (Bug 40929).
  - ***isc-dhcp*** (CVE-2015-8605) (Bug 40545).
  - ***openssl*** (CVE-2015-1794 CVE-2015-3193 CVE-2015-3194 CVE-2015-3195 CVE-2016-0701 CVE-2016-0702 CVE-2016-0705 CVE-2016-0797 CVE-2016-0798 CVE-2016-0799 CVE-2016-0800) (Bug 40187).
  - ***samba*** (CVE-2015-5370 CVE-2016-2110 CVE-2016-2111 CVE-2016-2112 CVE-2016-2113 CVE-2016-2114 CVE-2016-2115 CVE-2016-2118) (Bug 40988).

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- The mount-point option *no_mbcache* has been added for ext4 file systems to disable the *Filesystem Meta Information Block Cache (mbcache)*. The cache is used to manage shared Extended Attributes (*EAs*), which are also used to store Access Control Lists (ACLs) for files and directories. For some work-loads which use *EAs* with many different values the cache has performance issues and can dead-lock the system in certain cases. Samba is one example which uses *EAs* to store the DOS attributes and NT ACLs. The cache can be disabled by re-mounting the file system using `mount -o remount,no_mbcache "$fs"` or by adding the option *no_mbcache* in `/etc/fstab` and rebooting the system (Bug 41054).
- The meta packages for the *non-PAE i486* kernel image and header files have been removed (Bug 40912).

6.2.2. Univention Configuration Registry

Feedback

- Service information files in `/etc/univention/service.info/services` are now only considered if they carry the filename suffix `.cfg`. The behavior is now similar to the treatment of UCR info files. (Bug 40383).

6.2.3. Boot Loader

Feedback

- On UCS systems booting via BIOS, an error would happen if debconf *grub-pc/install_devices* contains a wrong device. If it contains a wrong device the GRUB installation happens but fails, leading to an inconsistent installation between /boot/grub and the GRUB directly on the disk. This makes the system not bootable. This update checks all devices in *grub-pc/install_devices*, removing invalid devices. Additionally a guess is made for the correct boot device which will be added to *grub-pc/install_devices* if *grub-pc/install_devices*

is currently empty or there were invalid devices. If any changes were made, grub-install is run on all devices in *grub-pc/install_devices*. See also SDB 1356 and SDB 1357. (Bug 40654, Bug 40660).

- Localization of the GRUB boot menu has been disabled. The title string gets translated to the preferred language of the user triggering menu generation process. This breaks selecting a boot kernel through the Univention Configuration Registry variable `grub/default`, as it doesn't work on systems using a different language (Bug 41046).
- Remove extra argument to `grub-mkdevicemap` as it is not needed (Bug 40586).
- The menu titles are now quoted to allow strings containing blanks (Bug 25157).
- Disable saving the selection by default as it is not supported on all file systems (Bug 40557).
- Add support to configure serial console support through the Univention Configuration Registry variables `grub/terminal` and `grub/serialcommand`. Thanks to *Lutz Willek* for the patch (Bug 40596).

6.3. Univention Management Console

Feedback

6.3.1. Univention Management Console web interface

Feedback

- If error messages contained a "%" they weren't displayed in UMC. This issue has been fixed (Bug 40749).
- The expiration date has been increased by 5 years. This results in a traceback during the login on the 29th of February. This issue has been fixed (Bug 40790).
- It's now possible to use multiple languages in one session when using HTTP basic authentication (via command line) (Bug 40806).
- The *umc.store* API allows to contain Arrays in query requests now (Bug 38639).
- An error in the comparison function *umc.tools.cmpObjects* which could cause that e.g. sorting the grid header wasn't possible anymore has been fixed (Bug 35407).
- The location where UMC redirects after logout is now configurable via the Univention Configuration Registry variable `umc/logout/location` (Bug 40613).
- The UMC login page does not warn about an insecure connection when logging in from the same machine the UMC runs on (Bug 40638).
- Error dialogs concerning Piwik are now suppressed (Bug 30822).
- Ensure that the first non-empty UMC category is shown at startup (Bug 40923).
- Add a hook interface for other packages for extending the behavior of UMC (Bug 40118).
- The user menu in the UMC is now more touch-friendly for small screens and the use on mobile devices (Bug 38622).
- The context menu for links is now working as expected (Bug 40939).
- Wizards are now scrolling to the top when switching the page (Bug 40939).
- Minor bugfixes for the widget *LinkList* to accept static values (Bug 41081).
- The context menu for link tiles in the UMC overview is now correctly displayed (Bug 41087).

- Module tiles in the UMC overview are now correctly flagged favorites (Bug 41161).

6.3.2. Univention Management Console server

Feedback

- A UMC server crash is prevented which might happen during session timeout (Bug 40627).
- The property *translationId* for UMC XML files was previously only evaluated for UMC module flavors. With this update, *translationId* is also correctly evaluated for module and link entries (Bug 40930).
- The UMC server process now runs with 64512 maximum number of opened files. The robustness of the UMC server has been enhanced (Bug 39909).

6.3.3. Univention App Center

Feedback

- Docker Apps now do not have their repository removed in the container (Bug 40315).
- Upgrading Apps now does not lead to an error just after the installation of packages (Bug 40674).
- Upgrading Apps now does not lead to an error when upgrading their master packages (Bug 40713).
- The application information like vendor, description were HTML encoded twice at some places (Bug 35324).
- If no package changes are detected an application could not be upgraded (Bug 40005).
- The error handling of the apps module has been improved (Bug 40797).
- The application metadata are ensured to be updated before installing or upgrading an application. This prevents errors when installing applications on remote hosts (Bug 40804).
- Apps may define ports they want to occupy exclusively. Docker Apps checked before installation whether an already installed App excepts exclusive access to one of these ports. This check has been extended to Non-Docker Apps (Bug 40508).
- Apps now show general information about the terms under which the software may be used. If the App ships a license file, it may be read before and after installation (Bug 40428).
- Internal adaptations have been added to allow for extending App Center functionalities (Bug 40827).
- `univention-register-apps` now uses the new App Center API and has been deprecated (Bug 40754).
- An error during loading the App Center cache has been fixed which prevented using the App Center when the cache file was corrupted (Bug 40875).
- Malformed files for meta information could cause the App Center to show a traceback. This has been fixed, those files are ignored now (Bug 40874).
- Upon upgrading the App Center software package, the App cache could get outdated. This caused an error in the App Center in some cases (Bug 40882).
- Improved the image gallery in the details page of an app. The handling of YouTube videos has been improved and enlarging thumbnails is smoother (Bug 39794).
- A help text still mentioned the Free-for-personal-Use Edition. This has been replaced with the UCS Core Edition (Bug 38530).

- The overview of software changes has been enhanced (Bug 39896).
- A margin has been added to the footer buttons of the installation error page (Bug 39907).
- Join scripts and unjoin scripts are now correctly removed while installing and uninstalling an App (Bug 40879).
- Minor code changes make other projects easier that rely on the App Center (Bug 40943).
- `univention-app` shell now correctly exits with the exit code of the called command (Bug 40550).
- `univention-app` installed unsigned packages. This issue has been fixed (Bug 40861).
- The Package Management module can be opened via hash again (Bug 40991).
- Details of software packages can be shown again (Bug 40992).
- The installation status of Docker Apps was determined incorrectly by certain functions of the App Center. This has been fixed (Bug 41009).
- Join scripts of Docker Apps are run via `univention-run-join-scripts` instead of being called directly (Bug 40984).
- The certificate of the App Center server is now always validated in HTTPS connections (Bug 30620).
- When extracting new App meta data, the permissions are set explicitly for these files instead of relying on the archive (Bug 41029).
- Some images were not shown in Internet Explorer. This issue has been resolved (Bug 39927).
- The parameter for creating a Docker Container can now be adjusted by the App (Bug 41062).
- Additional App files of installed Apps are now also updated (Bug 39368).

6.3.4. Univention Directory Manager UMC modules and command line interface

Feedback

- Some LDAP search requests have been optimized in the handler modules (Bug 40651).
- In situations where the IP address of a created computer contained two equal blocks (e.g. 10.10.20.0/24) invalid pointer records were created. This issue has been fixed (Bug 39030).
- The layout of DNS service and text records have been adjusted to be more readable (Bug 40775).
- It is now prevented to create extended attributes for users with required fields without specifying a default value. Those extended attributes caused problems during upgrading to UCS 4.1 or installing various apps (Bug 40824).
- The search filter for *name* in the *dns/dns* module now also finds zones and pointer records (Bug 23804).
- The search filter for *dhcpPermitList* in the *dhcp/pool* lookup function has been fixed (Bug 39343).
- The search filter for *fqdn* has been adapted so it can be used to search for multiple computers (Bug 34327).
- Some columns which show more information in the grid of UMC have been added to the DNS handler modules (Bug 38639).
- The error message for malformed paths in shares has been improved (Bug 41040).

- Multiple modules allowed to select special Docker host objects when it came to choosing a computer object. This option has been removed as it makes no sense (Bug 41041).
- importing the python modules of *univention.admin* doesn't depend on the order or previous imports anymore (Bug 33359).
- The correct referencing objects are now shown in a policy. Previously caching caused wrong objects to be shown (Bug 33344).
- A link that redirects to the subscription prices for UCS on the Univention website has been added to the license dialog of UCS core editions (Bug 41174).
- Searching for a specific object type underneath of *cn=univention* in the LDAP directory did not yield results and has been repaired (Bug 32843).
- Searching for properties which require an exact match did not work because the LDAP filter was prepended with *. The search for e.g. the *gidNumber* of a group is now possible again (Bug 37904).
- Searching for properties using the *LDAPSearch* syntax class caused a traceback. This issue has been fixed (Bug 38635).
- The *users/self* module can now be activated again via setting the Univention Configuration Registry variable `umc/module/udm/users/self/disabled` to `false` (Bug 39016).

6.3.5. Modules for system settings / setup wizard

Feedback

- Access restrictions on non DC master App Appliances have been corrected in the system activation package (Bug 39700).
- App Appliances now ensure that the UCS domain they join has an activated license (Bug 39700).
- The virtual keyboard to enter special characters now supports touch devices (Bug 40572).
- The initial setup used a script to update the App Center files that failed under certain circumstances. Now a script is called that works in unjoined environments (Bug 40897).
- The detection of a docker environment caused the PXE installation to fail. This issue has been fixed (Bug 41143).
- The list of supported browser versions which is displayed on the console upon login to a UCS system (message of the day) has been updated (Bug 40580).

6.3.6. DNS module

Feedback

- The PTR record entries are now sorted numerical in the overview of a reverse zone (Bug 40747).
- The DNS module now displays more information in the grid columns and forward zones are now shown before reverse zones in the tree view (Bug 38639).

6.3.7. Printers module

Feedback

- Performance of the UMC print quota overview has been improved (Bug 33792).

6.3.8. Other modules

Feedback

- Hosts which are docker containers are now excluded from the check in the diagnostic module if the SSH connection to these hosts is possible (Bug 40563).

6.4. Software deployment

Feedback

- The `preup.sh` and `postup.sh` scripts have been updated to match UCS-4.1-2 (Bug 41157).
- Linux 4.1 kernel package are now also considered for removal an upgrades (Bug 40748).
- The change from HTTP to HTTPS breaks the old updater from UCS-4.0-4, which is still running after the update to 4.1-0. As such all updates stop there. Running the same command again continues installing updates, as then the new updater is used. This update fixes this problem by re-executing the updater after each update to guarantee, that the latest version is always used (Bug 40338).
- The `dists/**/Packages*` files created for local repositories did contain multiple entries for the same package. This breaks the Debian installer and other tools like `debootstrap`, which use a simpler implementation than APT. A filter has been added to filter out old versions and duplicate entries (Bug 40932).
- Software package versions from the current release are preferred over packages from previous releases even when they are newer (Bug 41083).
- The version patchlevel is now set to the correct value in the package ***univention-updater*** (Bug 41165).
- The detection of the local repository prefix has been fixed (Bug 41166).

6.5. System services

Feedback

6.5.1. SAML

Feedback

- The joinscript uses cURL instead of wget to configure SAML service provider setting to prevent conflicts with old SHA-1 or MD5 SSL certificates (Bug 40658).
- A unjoin-script has been added which removes the SAML configuration for UMC (Bug 40738).
- The creation of the internal SAML LDAP user ignores extended attributes now (Bug 40741).
- The extended attribute for the SAML service provider can now be used in user templates (Bug 40895).

6.5.2. Univention self service

Feedback

- The robustness and performance have been increased by not forking a UMC module process on each HTTP request (Bug 40799).

6.5.3. Kerberos

Feedback

- The Univention Configuration Registry variable description for `kerberos/autostart` did not clearly explain that this variable needs to remain set to *no* on Samba4/AD DCs (Bug 40383).

6.5.4. Apache

Feedback

- Some links in the footer of the UCS overview site have been changed (Bug 41175).

6.5.5. PAM / Local group cache

Feedback

- The time limit of ldap searches in ***libnss-ldap*** is now configurable via the Univention Configuration Registry variable `nssldap/timelimit` and defaults to 30 seconds. This prevents hanging UMC server processes when changing network and IP settings in certain circumstances (Bug 40968).

6.6. Services for Windows

Feedback

6.6.1. Samba

Feedback

- In case an account locking password policy has been defined for the domain, e.g. via `samba-tool domain passwordsettings`, the *badPwdCount* increased in steps of two for each failed login attempt at a Windows client (Bug 40328).
- The patch for CVE-2015-5252 caused a regression for the special share path `/`. This issue has been fixed (Bug 40847).
- This update sets the new `smb.conf` option *ldap server require strong auth* to *allow_sasl_over_tls*. Additionally it configures *tls verify peer* to *ca_and_name*. The raised security requirements of Samba server components may require configuration adjustments for older clients. Univention Corporate Client (UCC) 1.0 running a Linux kernel version prior to 3.8 for example require an adjustment of the *mount.cifs options*. In that case the value for mount option *sec* needs to be adjusted to *ntlmsspi*, e.g. by setting `ucr set ucc/mount/cifshome/options="serverino,sec=ntlmsspi"`. UCC 2.x clients (i.e. Linux kernel above 3.8) don't require this adjustment (Bug 40988).
- This update makes additional `smb.conf` options configurable via Univention Configuration Registry: `samba/ntlm/auth`, `samba/server/signing` `samba/tls/verify/peer` `samba/tls/priority` `samba/tls/dh/params/file` and `samba/ldap/server/require/strong/auth` (Bug 41034).

6.6.2. Univention AD Takeover

Feedback

- The Active Directory takeover fails if the Active Directory NetBIOS domain name is unusual. This issue has been fixed (Bug 39070).

6.6.3. Univention Active Directory Connection

Feedback

- Support for synchronization of the OpenLDAP attribute *mailAlternativeAddress* with the AD attribute *proxyAddresses* has been added. This can be switched on for users and groups individually by the new pair of Univention Configuration Registry variables `connector/ad/mapping/user/alternativemail` and `connector/ad/mapping/group/alternativemail` (Bug 40357).
- The synchronization of the password hashes was implemented by using a service which was installed on the Microsoft Active Directory server. The Univention AD Connector now uses different interfaces of the Active Directory for reading and writing the password hashes. That means, the UCS AD Connector service which is installed on the Microsoft Active Directory server can be stopped after installing this update (Bug 40745).
- If a user was moved on UCS side, the group cache wasn't always updated and an error occurred. This issue has been fixed (Bug 41028).
- The AD Connector is now restarted after rotating the AD Connector log files (Bug 32265).

6.7. Other changes

Feedback

- Various issues have been fixed in ***ucslint*** which checks a source package for errors (Bug 40386, Bug 40639, Bug 40647).
- Plymouth now uses the framebuffer renderer as default (Bug 40715).