UCS 4.1-0 Release Notes

**Release notes for the installation and update
of Univention Corporate Server (UCS) 4.1-0**

Table of Contents

Chapter 1. Release Highlights

An overview of the most important changes:

- The Univention App Center integrates the container technology Docker. With Docker, it is possible to run Apps separately and encapsulated from each other. This increases the security of the UCS domain and reduces the dependencies of the Apps on other software libraries. The integration of Docker is transparent to the users. The App Center will automatically perform the startup and configuration of the Docker containers.

- The Univention App Center's usability has been improved further. Apps are now displayed more clearly. The App detail pages have been cleaned up and supplemented by a rating in the categories Vendor Supported, Popularity's Award and Editor's Award. The classification is based on data such as the installation base of the Apps or the maintenance behavior of the App providers. Thus, the transparency and comparability of Apps are increased.

- Single-sign-on via SAML is a product component from UCS 4.1 and works out of the box with the UCS management system. Once logged in, you can switch between web applications without an additional login.

- Users can independently change their password or reset it in case of a forgotten password via the new Self Service. In this case, a token will be sent to an e-mail address or mobile phone number that has to be defined in advance by the users. The then received token can be used to set a new password.

- The Linux kernel has been updated to the latest stable version of the 4.1 long-term kernel. This includes several security updates as well as new and updated drivers for better hardware support.

- Samba has been updated to version 4.3.1. Besides many detail improvements, Samba 4.3 provides support for SMB 3.1.1, which was introduced by Microsoft with Windows 10 and provides security improvements and more features.

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. Univention App Center

Feedback ⤶

If applications have been installed from the Univention App Center, the update can only be performed once all installed applications are available in a compatible version. Some applications are updated to newer versions during the UCS update. If an application is not yet available for UCS 4.1, a statement about the release date can be obtained from the application provider.

2.3. 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.

3.1. Removed/unsupported Components

Feedback ⊋

Some components have been removed and are not shipped any longer with UCS 4.1:

• PostgreSQL 8.4 is no longer provided in UCS 4.1. The migration of existing databases to PostgreSQL 9.1 is described in SDB 1292.

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 33
- Firefox as of version 24
- Internet Explorer as of version 9
- Safari and Safari Mobile as of version 7

Users with older browsers may experience display or performance issues.

5.4. Handling of maintained and unmaintained packages

With UCS 4.1 the handling of maintained and unmaintained packages has been changed.

- The *Installation DVD* now only contains the packages required to install a new UCS system with all the components provided by Univention. Previously the DVD contained all other maintained packages too. They have been removed from the DVD to decrease the download size.
- The full set of maintained packages is provided through the *Update DVD*. It can be used to update a local repository.

- All packages (maintained and unmaintained) are available online through https://updates.software-univention.de/.

With this change the definition of maintained also changed: maintained is now defined on the basis of the *source package*, while previously it was defined on a subset of *binary packages*. This might lead to an increased space requirement for local repositories, as maintained now consists of more packages than in previous releases.

Chapter 6. Changelog

Listed are the changes since UCS 4.0-4:

6.1. General

- All packages have been adapted to UCS 4.1 (Bug 39729).

- The codename for UCS 4.1 has been set to *Vahr* (Bug 39223).

- The package *univention-container-role-common* has been added. It is used to strip down the base of installed packages in a Docker image (Bug 38283).

- The errata level is reset during the upgrade to UCS 4.1 (Bug 39312).

6.2. Univention Installer

- The default inode density for partitions smaller than 4TB has been increased from 1 inode per 16KiB to 1 inode per 8KiB. This adjustment should avoid running out of inodes on system volumes. This only affects creation of new filesystem volumes (Bug 39432).

6.3. Basic system services

6.3.1. Linux kernel and firmware packages

- The Linux kernel has been updated to 4.1.12 (Bug 38873, Bug 38872).

6.3.2. Boot Loader

- The boot menu on the installation DVD has been improved. The DHCP request can now be skipped directly (Bug 39554).

6.3.3. Other system services

- The network registration is now skipped in the init script `univention-network-common` if UCS is running in a Docker container because the network registration for this mode is implemented in the init script `univention-docker-container-mode` (Bug 38365).

- `univention-firewall` now creates port forwarding rules for services in Docker containers (Bug 38307).

- Prevent an error when logging into a docker container without network interface (Bug 38861).

6.4. Domain services

6.4.1. OpenLDAP

- OpenLDAP has been updated to version 2.4.42 (Bug 38876).

- The directory logger and the *ldap_extension* listener module now restart the OpenLDAP server only if it was running (Bug 39683).

- The OpenLDAP server might be started multiple times during the upgrade. This is no longer a problem for the OpenLDAP package scripts (Bug 39683).

- The graceful-restart of the OpenLDAP init script has been adjusted to reduce the grace time (Bug 39719).

- The group access for the LDAPI socket interface has been removed (Bug 39811).

6.4.1.1. LDAP ACL changes

- The permissions for GSSAPI SASL authentication have been fixed (Bug 29482, Bug 39877).

- The hosts can now modify their own *operatingSystem* and *operatingSystemVersion* attributes (Bug 39915).

6.5. Univention Management Console

6.5.1. Univention Management Console web interface

- Support for logging in with the primary email address at UMC has been added (Bug 38528).

- Unmovable objects are no longer shown as movable (Bug 20439).

- All UMC cookies are now restricted to the path `/univention-management-console/`. Therefore, the entry point `/umcp/` has been moved to `/univention-management-console/` (Bug 38820).

- The session and username cookie are now suffixed with the port to allow multiple parallel UMC session on the same host (Bug 38344).

- A service entry for Univention Management Console has been added and the ***univention-management-console-web-server*** join script adds this service automatically to the LDAP host entry (Bug 39553).

- The Univention Management Console login now supports authentication via SAML (Bug 31943, Bug 39549, Bug 39552).

- The dropdown menu to switch the Univention Management Console uses the SAML single-sign-on process now. The previously used UMC single-sign-on implementation has been replaced with SAML (Bug 39227).

- The dependency of ***univention-dojo-dev*** has changed to ***OpenJDK 7*** (Bug 39572).

- The integration of the browser history into UMC has been improved and added to UDM modules (Bug 39033).

- The Univention Management Console login is now extensible to support authentication via a one time password (Bug 39611).

6.5.2. Univention Management Console server

- The exception `SystemExit` is now caught by the UMC server and not shown as a traceback to the user (Bug 39031).

- A memory leak in the UMC webserver has been fixed which could occur when a SSL communication between UMC webserver and UMC server was not possible (Bug 38402).

- The UMC PAM configuration has been extended. It is now possible to integrate additional services via PAM such as multi factor authentication modules (Bug 39612).

6.5.3. Univention App Center

- The App Center is now able to install docker based apps. These apps are installed in a small container (minimal UCS) within the host system (Bug 38887, Bug 39185, Bug 39258, Bug 39374, Bug 39331, Bug

39184, Bug 39183, Bug 39196, Bug 39496, Bug 39417, Bug 39330, Bug 39192, Bug 39467, Bug 39462, Bug 39629, Bug 39204, Bug 39189, Bug 39587, Bug 39189, Bug 39660, Bug 39434, Bug 39199, Bug 39820, Bug 39822, Bug 39716).

- The variable `UCSOverviewCategory` now accepts the value *None* in which case any UCR variable once registered will be removed (Bug 39718).

- The source package has been renamed to ***univention-appcenter*** to reflect the fact that the UMC module is a frontend for the Univention App Center (Bug 39585).

- The design of the UMC App Center module has been adjusted, and some usability aspects have been improved (Bug 38894, Bug 39653, Bug 39665, Bug 39651, Bug 39835, Bug 39668).

- App logos must be in the SVG format from UCS 4.1 on. Logos are referenced in the *INI* or META files as `Logo` and `LogoDetailPage` where the latter optional entry may define a different logo which is displayed in the app detail view (Bug 39525, Bug 39656).

- The property `Screenshot` has been replaced with the property `Thumbnails` which allows a comma separated list of pictures or *youtube* URIs (Bug 39654, Bug 39524).

- Apps can be rated. This rating is shown on the detail page of an App (Bug 38891).

- Every time an app is opened from the Gallery, the session is refreshed silently to prevent logouts (Bug 39655).

- The App Center now checks a digital signature of the index of app meta files (Bug 39591).

- The global App Center now only suggests app updates on remote hosts when that's UCS version matches the local version (Bug 39912).

- The searched keyword in the App Center resets if the category gets changed (Bug 39652).

6.5.4. Modules for system settings / setup wizard

Feedback

- It is now possible to to black list the page for selecting the system role and use a pre-configured role value instead (Bug 38315).

- The ***System Setup*** wizard now can have a configurable domain while the hostname itself is fixed. This is needed for Docker based apps (Bug 38275, Bug 38154).

- During the initial system setup, the restart of the webserver is no longer disabled. This is needed for Docker based apps (Bug 39476).

6.5.5. Computers module

Feedback

- The UDM attributes *operatingSystem* and *operatingSystemVersion* can now be set for domain controllers and member servers (Bug 39915).

6.5.6. Policies

Feedback

- When adding an object without policies referenced, no traceback occurs anymore (Bug 37667).

6.5.7. Other modules

Feedback

- Various modules are now able to handle ***python-psutil*** API changes (Bug 39322, Bug 39323).

www.univention.de

6.6. Software deployment

- The size of the UCS installation DVD has been reduced by removing all packages not strictly required for installation from the DVD. All maintained packages are still available online or through the update DVD (Bug 38913).

- The updater scripts `preup.sh` and `postup.sh` have been adapted to the needs of UCS 4.1 (Bug 39271).

- The UDM attributes *operatingSystem* and *operatingSystemVersion* of an UCS server are now set during the upgrade (Bug 39915).

- The updater now uses the protocol `HTTPS` to access the Univention Software Repository at `https://updates.software-univention.de/` by default (Bug 39306).

- The updater now uses the proxy defined in the Univention Configuration Registry variable `proxy/https` for `HTTPS` connections. If `proxy/https` is not defined, the fallback `proxy/http` is used (Bug 39922).

- The Univention Configuration Registry variable `proxy/address`, `proxy/port`, `proxy/username` and `proxy/password` are no longer used to configure the package toolkit `apt`. Please use the Univention Configuration Registry variable `proxy/http` or `proxy/https` instead (Bug 39922).

- The updater now uses the license UUID (Univention Configuration Registry variable `license/uuid`) to access the Univention Software Repository at `https://updates.software-univention.de/` by default (Bug 39305).

- The updater now skips downloading translation files and differential `Packages` files (Bug 28022).

- The updater `preup.sh` script now checks if the DC master has already been updated (Bug 37260).

- The fatal error message in `univention-upgrade` now references the logfile `/var/log/univention/updater.log` for further details (Bug 31006).

- `univention-upgrade` now uses `--enable-app-updates` by default (Bug 39082).

6.6.1. Software deployment command line tools

- The mount point for CD-ROM images in `univention-updater` and `univention-repository-update` has been fixed (Bug 36721).

6.7. Univention base libraries

- The function `is_ucr_true` has been added to the package *shell-univention-lib* (Bug 27701).

- The package *OpenSSL* has been updated to version `1.0.2d` (Bug 39500).

- The package *cURL* treated warning alerts as fatal during the TLS handshake, which prevented connecting to some `https://` servers using SNI. This has been fixed (Bug 39603).

6.8. System services

6.8.1. SAML

- The SAML identity provider app has been integrated into UCS (Bug 38881, Bug 39468).

- The package **univention-saml** is installed on DC Master and DC Backup systems automatically during the UCS 4.1 upgrade (Bug 39313).

- Single-sign-on via SAML 2.0 is now possible with Univention Management Console (Bug 39171, Bug 39178, Bug 31943).

- A download link for the public certificate of the identity provider has been added to the module (Bug 32786).

- Every SAML identity provider registers its default IP address via DNS at the host record *ucs-sso* to provide a failover configuration. The name can be changed before joining the UCS system through the Univention Configuration Registry variable `ucs/server/sso/fqdn` (Bug 39386, Bug 39574, Bug 39399).

- The SimpleSAMLphp certificate is now created in the joinscript instead of the postinst of the package (Bug 39255).

- The SimpleSAMLphp files `authsources.php` and `saml20-idp-hosted.php` have been changed to a UCR multifile template (Bug 39250).

- SimpleSAMLphp has been updated to version 1.13.2-1 (Bug 38982).

- *AssertionConsumerService* is now a multi-value field (Bug 39015).

- The ACL evaluation of SimpleSAMLphp has been fixed (Bug 38935).

- Renaming of a service provider is now prevented as the user references weren't updated when doing so (Bug 38934).

- Transmitting LDAP attributes from the identity provider is now possible and does not cause exceptions in SimpleSAMLphp anymore (Bug 38927).

- The *entityID* of the identity provider is now configurable via the Univention Configuration Registry variable `saml/idp/entityID` (Bug 33912).

- The SAML identity provider now uses a dedicated LDAP user to access the LDAP and a separate user is used to access SSO specific web-content by apache2 (Bug 38947).

- The App Center module has been adapted to work with single-sign-on (Bug 39226).

- The UMC server and LDAP server allow authentication with a SAML assertion via the packages pam-saml and cy2-saml (Bug 39315).

- **PHP** syntax is now correctly escaped and validated when writing the **simplesamlphp** service provider configuration (Bug 38933).

- The SAML join script has been moved from **univention-saml-schema** to **univention-saml** (Bug 39472).

- A required password change, expired passwords, locked and disabled accounts are detected by the SAML login and the user is informed, while login is denied (Bug 39181).

- **stunnel4** has been updated to 5.18, and now supports certificate validation for the connected memcache instances (Bug 39479).

- The default *NameID* identifier format for configured service providers is changed to *urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified* (Bug 39431).

- The SAML schema package now restarts the OpenLDAP server only if it was running (Bug 39683).

- Display problems for the Internet Explorer compatibility mode have been corrected (Bug 39850).

6.8.2. Univention self service

- The user can now change or reset her/his password by using the password self-service (Bug 39597).

6.8.3. Mail services

- Authentication (and thus submitting) has been disabled by default on port 25. Set Univention Configuration Registry variable `mail/postfix/mastercf/options/smtp/ smtpd_sasl_auth_enable=yes` to enable the old behavior (Bug 39021).

- The `Dovecot Managesieve` service is now also available via IPv6 (Bug 39702).

- A problem with postfix' start script `/etc/init.d/postfix` has been fixed that could lead to the inability to start/stop postfix in docker containers (Bug 39542).

- When installing **univention-mail-postfix** for the first time, 512 bit DH parameters for Postfix are now generated immediately and 2048 bit DH parameters are scheduled by the join script to be generated on the next day (Bug 39482).

6.8.4. Kerberos

- The dependency to **univention-home-mounter** has been removed from the Kerberos rsh daemon (Bug 39490).

6.8.5. SSL

- **univention-ssl** can now create certificates for FQDNs longer than 64 characters. The OpenSSL extension *Subject Alternative Name* is used in such a case (Bug 38859).

6.8.6. Apache

- **univention-apache** now ships expandable *VirtualHost* configuration files (Bug 38807).

6.8.7. PAM / Local group cache

- The dependency on **univention-home-mounter** has been changed to a recommendation in the **univention-pam** package (Bug 39490).

6.8.8. Other services

- **univention-postgresql** has been split into multiple packages, one for each PostgreSQL version (Bug 39595). **univention-bacula** does not create the PostgreSQL configuration files for not-installed versions anymore (Bug 39595). **univention-pkgdb** does not create the PostgreSQL configuration files for not-installed versions anymore (Bug 39595).

6.9. Virtualization

6.9.1. Univention Virtual Machine Manager (UVMM)

- UVMM profiles for Windows 10 have been added (Bug 39335).

- The description of a virtual machine is dynamically displayed as a grid column (Bug 38676).

- The user can now select the MAC address inside the interface grid. (Bug 33546).

6.9.2. Operate UCS as virtual machine

- The package *qemu* has been updated and has been re-compiled with support for Xen disabled. The package *libvirt* has also been re-compiled with support for Xen disabled (Bug 39685).

6.10. Container Technologies

- The package *docker.io* has been updated to *1.6* (Bug 39350).

- OverlayFS has been configured as the Docker storage driver (Bug 39412, Bug 39418).

- The packages *univention-docker-container-mode* and *univention-appliance-docker-container* have been added. These packages help to run UCS in a Docker container (Bug 39331, Bug 38260).

- The function ucs_registerLDAPExtension from package *shell-univention-lib* now supports the options packagename and packageversion (Bug 38205).

- When joining a UCS domain, Docker containers do not register their IP and MAC addresses in the computer object (Bug 38437).

- UCR can now modify files on a bind-mounted filesystem in a Docker container (Bug 38011).

- The Heimdal Kerberos installation does not fail anymore in a Docker container (Bug 38295).

- No keyboard or console font setup is done inside a Docker container (Bug 38763).

- A docker repository is now hosted on docker.software-univention.de (Bug 39188).

- A docker init script has been added which properly stops and restarts running containers (Bug 39474).

- Docker images running UCS in container mode now update their IP addresses in LDAP if one is already registered there. This is useful because Docker dynamically assigns IP addresses during container restarts (Bug 38334).

- Docker images running UCS in container mode now try to register the IP also with a consul and etcd service running on the Docker host (Bug 38331).

- The Docker log file is now readable only by root and the docker process (Bug 39494).

- The App Center checks the digital checksum of docker images hosted on docker.software-univention.de before downloading them. The integrity of the container maintainer scripts are verified in this manner as well (Bug 39194).

- The time zone in Docker containers is now set to the same as the host (Bug 39483).

- A base image for UCS hosted apps has been created and uploaded to docker.software-univention.de (Bug 39187).

6.11. Services for Windows

6.11.1. Samba

- Samba has been updated to version 4.3.1 (Bug 38874).

- The default domain and forest function level for new installations is now *2008 R2* (Bug 38800).

- The Univention Configuration Registry variable `samba/register/exclude/interfaces` has been added. The IP addresses of theses network interfaces are not registered automatically in DNS. By default the variable is set to `docker0` (Bug 39466).

- The Univention Configuration Registry variable `samba/max/protocol` doesn't get set any longer for new installations. Additionally, if it was set to the default "SMB2" it will get unset as well during updates. The purpose of this change is to give customers the highest protocol level considered stable by the Samba defaults. Currently this is `SMB3_11`. (Bug 32939).

- The `IPC$ share` is not explicitly configured any longer in the default configuration where `samba4/service/smb` is `s3fs`. This change avoids a lot of unnecessary warning messages from samba (Bug 29227).

- The Samba package now restarts the OpenLDAP server only if it was running (Bug 39683).

- The in place upgrade of *Samba 3/NT4* to *Samba 4/AD* has been fixed (Bug 39932, Bug 37646).

6.11.2. Univention AD Takeover

Feedback

- The FSMO roles *domaindnsmaster* and *forestdnsmaster* are now seized during the takeover (Bug 39222).

- Installation of **Univention AD Takover** now also installs **fping** (Bug 39723).

6.12. Other changes

Feedback

- Asterisk has been updated to 11.13.1. It provides many bugfixes and fixes several vulnerabilities (Bug 37738, Bug 39285)

- *univention-join* now correctly checks for the existence of `nscd`. This is needed in a minimal environment (Bug 38662).

- `nscd` terminates its children when stopping (Bug 38135).

- The packages for the default `settings/packages` Univention Directory Manager objects have been updated (Bug 32443).

- Several package dependencies in Docker related base packages have been changed (Bug 39410).

- The response handling in the `univention.lib.umc_connection.UMCConnection` library has been improved (Bug 39599).

- The *iceweasel* package has been put into unmaintained status, so it will not be considered any longer for security updates. It has not been used anyway as **firefox-en** and **firefox-de** are installed e.g. for the system setup (Bug 38281).