univention
be open.

UCS 4.3 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 4.3-5

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

<feedback@univention.de>

univention
be open.

Table of Contents

1. Release Highlights 4
2. Notes about the update 5
    2.1. Recommended update order for environments with more than one UCS server 5
    2.2. UCS installation DVD only available for 64 bit 5
3. Preparation of update 6
4. Postprocessing of the update 7
5. Notes on selected packages 8
    5.1. Collection of usage statistics 8
    5.2. Scope of security support for WebKit, Konqueror and QtWebKit 8
    5.3. Recommended browsers for the access to Univention Management Console 8
6. Changelog 9
    6.1. General 9
    6.2. Basic system services 12
        6.2.1. Boot Loader 12
    6.3. Domain services 12
        6.3.1. DNS server 12
    6.4. Univention Management Console 13
        6.4.1. Domain join module 13
    6.5. System services 13
        6.5.1. PAM / Local group cache 13
    6.6. Virtualization 13
        6.6.1. UCS Virtual Machine Manager (UVMM) 13
    6.7. Services for Windows 13
        6.7.1. Samba 13
        6.7.2. Univention S4 Connector 13

Chapter 1. Release Highlights

With Univention Corporate Server 4.3-5, the fifth point release of Univention Corporate Server (UCS) 4.3 is now available. It provides several feature improvements and extensions, new properties as well as various improvements and bugfixes. Here is an overview of the most important changes:

- Samba was updated to version 4.10.
- With 4.3-5 the update to Debian point release 9.11 is completed.
- Various security updates have been integrated into UCS 4.3-5, e.g. Samba, the Linux kernel and Dovecot. A complete list of security and package updates is available in Chapter 6.

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 10 GB of disk space. The update requires approximately 4 GB additional disk space to download and install the packages, depending on the size of the existing installation.

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. 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*. The modules opened get logged to 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 running older browsers may experience display or performance issues.

Chapter 6. Changelog

Listed are the changes since UCS 4.3-4:

6.1. General

- All security updates issued for UCS 4.3-4 are included:
  - ***apache2*** (CVE-2019-9517 CVE-2019-10081 CVE-2019-10082 CVE-2019-10092 CVE-2019-10098) (Bug 50062)
  - ***atftp*** (CVE-2019-11365 CVE-2019-11366) (Bug 49457)
  - ***bind9*** (CVE-2018-5743 CVE-2018-5745 CVE-2019-6465) (Bug 49454)
  - ***clamav*** (CVE-2019-1787 CVE-2019-1788 CVE-2019-1789 CVE-2019-12625 CVE-2019-12900) (Bug 49360 Bug 50137)
  - ***cups*** (CVE-2019-8675 CVE-2019-8696) (Bug 50153)
  - ***cups-filters*** (Bug 49722)
  - ***cyrus-imapd*** (CVE-2019-11356) (Bug 49630)
  - ***dbus*** (Bug 49661)
  - ***dovecot*** (CVE-2019-11500) (Bug 50090)
  - ***e2fsprogs*** (CVE-2019-5094) (Bug 50299)
  - ***exim4*** (CVE-2019-10149 CVE-2019-13917 CVE-2019-15846) (Bug 49602 Bug 49928 Bug 50155)
  - ***expat*** (CVE-2018-20843 CVE-2019-15903) (Bug 49762 Bug 50241)
  - ***faad2*** (CVE-2018-19502 CVE-2018-19503 CVE-2018-19504 CVE-2018-20194 CVE-2018-20195 CVE-2018-20197 CVE-2018-20198 CVE-2018-20357 CVE-2018-20358 CVE-2018-20359 CVE-2018-20361 CVE-2018-20362 CVE-2019-15296) (Bug 50195)
  - ***ffmpeg*** (Bug 49547)
  - ***firefox-esr*** (CVE-2018-18511 CVE-2019-5798 CVE-2019-7317 CVE-2019-9797 CVE-2019-9800 CVE-2019-9811 CVE-2019-9812 CVE-2019-9816 CVE-2019-9817 CVE-2019-9819 CVE-2019-9820 CVE-2019-11691 CVE-2019-11692 CVE-2019-11693 CVE-2019-11698 CVE-2019-11707 CVE-2019-11708 CVE-2019-11709 CVE-2019-11711 CVE-2019-11712 CVE-2019-11713 CVE-2019-11715 CVE-2019-11717 CVE-2019-11719 CVE-2019-11729 CVE-2019-11730 CVE-2019-11740 CVE-2019-11742 CVE-2019-11743 CVE-2019-11744 CVE-2019-11746 CVE-2019-11752) (Bug 49546 Bug 49685 Bug 49798 Bug 49895 Bug 50122)
  - ***firmware-nonfree*** (CVE-2018-5383) (Bug 49370)
  - ***ghostscript*** (Bug 49327 Bug 49456 Bug 50002 Bug 50154)
  - ***glib2.0*** (CVE-2018-16429 CVE-2019-12450 CVE-2019-13012) (Bug 50164)
  - ***gst-plugins-base1.0*** (CVE-2019-9928) (Bug 49402)

- ***heimdal*** (CVE-2018-16860 CVE-2019-12098) (Bug 49601)
- ***ibus*** (CVE-2019-14822) (Bug 50227)
- ***imagemagick*** (CVE-2019-9956 CVE-2019-10650) (Bug 49366)
- ***intel-microcode*** (CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2019-11091) (Bug 49484 Bug 49719)
- ***jquery*** (CVE-2019-11358) (Bug 49369)
- ***kauth*** (CVE-2019-7443) (Bug 49367)
- ***kconfig*** (CVE-2019-14744) (Bug 49993)
- ***libcaca*** (CVE-2018-20544 CVE-2018-20545 CVE-2018-20546 CVE-2018-20547 CVE-2018-20548 CVE-2018-20549) (Bug 50152)
- ***libebml*** (CVE-2019-13615) (Bug 50158)
- ***libgd2*** (CVE-2019-11038) (Bug 50159)
- ***libpng1.6*** (CVE-2019-7317) (Bug 49363)
- ***libreoffice*** (CVE-2019-9848 CVE-2019-9849 CVE-2019-9850 CVE-2019-9851 CVE-2019-9852 CVE-2019-9854) (Bug 49894 Bug 50019 Bug 50150)
- ***libssh2*** (CVE-2019-3855 CVE-2019-3856 CVE-2019-3857 CVE-2019-3858 CVE-2019-3859 CVE-2019-3860 CVE-2019-3861 CVE-2019-3862 CVE-2019-3863) (Bug 49294)
- ***libvirt*** (Bug 48536 Bug 49548 Bug 49717)
- ***libxslt*** (CVE-2019-11068 CVE-2019-13117 CVE-2019-13118) (Bug 50157)
- ***linux*** (CVE-2015-8553 CVE-2018-5953 CVE-2018-5995 CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2018-14625 CVE-2018-16884 CVE-2018-19824 CVE-2018-19985 CVE-2018-20169 CVE-2018-20509 CVE-2018-20510 CVE-2018-20836 CVE-2018-20856 CVE-2018-1000026 CVE-2019-0136 CVE-2019-1125 CVE-2019-3459 CVE-2019-3460 CVE-2019-3701 CVE-2019-3819 CVE-2019-3846 CVE-2019-3882 CVE-2019-3900 CVE-2019-5489 CVE-2019-6974 CVE-2019-7221 CVE-2019-7222 CVE-2019-8980 CVE-2019-9213 CVE-2019-9500 CVE-2019-9503 CVE-2019-9506 CVE-2019-10124 CVE-2019-10126 CVE-2019-10142 CVE-2019-10207 CVE-2019-10638 CVE-2019-10639 CVE-2019-11091 CVE-2019-11477 CVE-2019-11478 CVE-2019-11479 CVE-2019-11486 CVE-2019-11487 CVE-2019-11599 CVE-2019-11815 CVE-2019-11833 CVE-2019-11884 CVE-2019-13272 CVE-2019-13631 CVE-2019-13648 CVE-2019-14283 CVE-2019-14284 CVE-2019-14821 CVE-2019-14835 CVE-2019-15117 CVE-2019-15118 CVE-2019-15211 CVE-2019-15212 CVE-2019-15215 CVE-2019-15216 CVE-2019-15218 CVE-2019-15219 CVE-2019-15220 CVE-2019-15221 CVE-2019-15292 CVE-2019-15538 CVE-2019-15666 CVE-2019-15807 CVE-2019-15902 CVE-2019-15924 CVE-2019-15926) (Bug 49364 Bug 49477 Bug 49677 Bug 49892 Bug 50004 Bug 50160 Bug 50264)
- ***mariadb-10.1*** (CVE-2019-2529 CVE-2019-2537 CVE-2019-2614 CVE-2019-2627 CVE-2019-2737 CVE-2019-2739 CVE-2019-2740 CVE-2019-2805) (Bug 49362 Bug 50156)
- ***nghttp2*** (CVE-2019-9511 CVE-2019-9513) (Bug 50095)

- ***openjdk-8*** (CVE-2019-2602 CVE-2019-2684 CVE-2019-2698 CVE-2019-2745 CVE-2019-2762 CVE-2019-2769 CVE-2019-2786 CVE-2019-2816 CVE-2019-2842) (Bug 49585 Bug 49897)
- ***openssl*** (CVE-2019-1543) (Bug 49794)
- ***openssl1.0*** (CVE-2018-0732 CVE-2018-0734 CVE-2018-0737 CVE-2018-5407 CVE-2019-1559) (Bug 49796)
- ***patch*** (CVE-2018-1000156 CVE-2019-13636 CVE-2019-13638) (Bug 49936)
- ***php7.0*** (CVE-2019-11034 CVE-2019-11035 CVE-2019-11036 CVE-2019-11038 CVE-2019-11039 CVE-2019-11040 CVE-2019-11041 CVE-2019-11042) (Bug 50237)
- ***postgresql-9.6*** (CVE-2019-10130 CVE-2019-10208) (Bug 49458 Bug 49994)
- ***proftpd-dfsg*** (CVE-2015-3306 CVE-2019-12815) (Bug 49969)
- ***python-django*** (CVE-2019-6975 CVE-2019-12308 CVE-2019-12781 CVE-2019-14232 CVE-2019-14233 CVE-2019-14234 CVE-2019-14235) (Bug 49896 Bug 50001)
- ***qemu*** (Bug 49584 Bug 49713 Bug 50063)
- ***rdesktop*** (CVE-TMP49773) (Bug 49773)
- ***rsync*** (CVE-2016-9841 CVE-2016-9842 CVE-2016-9843) (Bug 49361)
- ***ruby2.3*** (CVE-2019-8320 CVE-2019-8321 CVE-2019-8322 CVE-2019-8323 CVE-2019-8324 CVE-2019-8325) (Bug 49328)
- ***samba*** (CVE-2018-16860 CVE-2019-10197 CVE-2019-12435 CVE-2019-12436) (Bug 49433 Bug 49627 Bug 50055)
- ***sdl-image1.2*** (CVE-2018-3977 CVE-2019-5051 CVE-2019-5052 CVE-2019-5057 CVE-2019-5058 CVE-2019-7635 CVE-2019-12216 CVE-2019-12217 CVE-2019-12218 CVE-2019-12219 CVE-2019-12220 CVE-2019-12221 CVE-2019-12222) (Bug 50163)
- ***sox*** (CVE-2017-11332 CVE-2017-11358 CVE-2017-11359 CVE-2017-15370 CVE-2017-15371 CVE-2017-15372 CVE-2017-15642 CVE-2017-18189 CVE-2019-8354 CVE-2019-8355 CVE-2019-8356 CVE-2019-8357 CVE-2019-1010004) (Bug 50162)
- ***subversion*** (Bug 49949)
- ***talloc*** (Bug 49479)
- ***univention-kernel-image*** (CVE-2018-5953 CVE-2018-14625 CVE-2018-16884 CVE-2018-19824 CVE-2018-19985 CVE-2018-20169 CVE-2018-20509 CVE-2018-20510 CVE-2018-1000026 CVE-2019-0136 CVE-2019-3459 CVE-2019-3460 CVE-2019-3701 CVE-2019-3819 CVE-2019-6974 CVE-2019-7221 CVE-2019-7222 CVE-2019-8980 CVE-2019-9213 CVE-2019-9506 CVE-2019-10124 CVE-2019-10142 CVE-2019-11487 CVE-2019-15211 CVE-2019-15212 CVE-2019-15215 CVE-2019-15216 CVE-2019-15218 CVE-2019-15219 CVE-2019-15220 CVE-2019-15221 CVE-2019-15292 CVE-2019-15538 CVE-2019-15666 CVE-2019-15807 CVE-2019-15924 CVE-2019-15926) (Bug 49364 Bug 50160)
- ***univention-kernel-image-signed*** (CVE-2015-8553 CVE-2018-5953 CVE-2018-5995 CVE-2018-12126 CVE-2018-12127 CVE-2018-12130 CVE-2018-14625 CVE-2018-16884 CVE-2018-19824 CVE-2018-19985 CVE-2018-20169 CVE-2018-20509 CVE-2018-20510 CVE-2018-20836

CVE-2018-20856 CVE-2018-1000026 CVE-2019-0136 CVE-2019-1125 CVE-2019-3459 CVE-2019-3460 CVE-2019-3701 CVE-2019-3819 CVE-2019-3846 CVE-2019-3882 CVE-2019-3900 CVE-2019-5489 CVE-2019-6974 CVE-2019-7221 CVE-2019-7222 CVE-2019-8980 CVE-2019-9213 CVE-2019-9500 CVE-2019-9503 CVE-2019-9506 CVE-2019-10124 CVE-2019-10126 CVE-2019-10142 CVE-2019-10207 CVE-2019-10638 CVE-2019-10639 CVE-2019-11091 CVE-2019-11477 CVE-2019-11478 CVE-2019-11479 CVE-2019-11486 CVE-2019-11487 CVE-2019-11599 CVE-2019-11815 CVE-2019-11833 CVE-2019-11884 CVE-2019-13272 CVE-2019-13631 CVE-2019-13648 CVE-2019-14283 CVE-2019-14284 CVE-2019-14821 CVE-2019-14835 CVE-2019-15117 CVE-2019-15118 CVE-2019-15211 CVE-2019-15212 CVE-2019-15215 CVE-2019-15216 CVE-2019-15218 CVE-2019-15219 CVE-2019-15220 CVE-2019-15221 CVE-2019-15292 CVE-2019-15538 CVE-2019-15666 CVE-2019-15807 CVE-2019-15902 CVE-2019-15924 CVE-2019-15926) (Bug 49364 Bug 49477 Bug 49677 Bug 49892 Bug 50004 Bug 50160 Bug 50264)

- ***unzip*** (CVE-2018-1000035 CVE-2019-13232) (Bug 49365 Bug 50151)
- ***vim*** (CVE-2019-12735) (Bug 49693)
- ***vlc*** (Bug 49660 Bug 50041)
- ***wpa*** (CVE-2019-9495 CVE-2019-9497 CVE-2019-9498 CVE-2019-9499 CVE-2019-11555) (Bug 49285 Bug 49553)
- ***zeromq3*** (CVE-2019-13132) (Bug 49893)
- ***zziplib*** (CVE-2018-6381 CVE-2018-6484 CVE-2018-6540 CVE-2018-6541 CVE-2018-6869 CVE-2018-7725 CVE-2018-7726 CVE-2018-16548) (Bug 49368)

- The following updated packages from Debian 9.11 are included (Bug 50313): ***base-files***, ***basez***, ***bio-maj-watcher***, ***bird***, ***bogl***, ***chaosreader***, ***c-icap-modules***, ***corekeeper***, ***dansguardian***, ***dar***, ***debian-archive-keyring***, ***debian-installer-netboot-images***, ***debian-installer***, ***dosbox***, ***fence-agents***, ***fig2dev***, ***fribidi***, ***fusiondirectory***, ***geant321***, ***gettext***, ***gocode***, ***groonga***, ***gsoap***, ***gthumb***, ***havp***, ***icu***, ***jackson-databind***, ***koji***, ***lemonldap-ng***, ***libapreq2***, ***libclamunrar***, ***libconvert-units-perl***, ***libdatetime-timezone-perl***, ***libevent-rpc-perl***, ***libgovirt***, ***librecad***, ***libsdl2-image***, ***libthrift-java***, ***libtk-img***, ***libu2f-host***, ***linux-latest***, ***liquidsoap***, ***llvm-toolchain-7***, ***minissdpd***, ***miniupnpd***, ***mitmproxy***, ***monkeysphere***, ***nasm-mozilla***, ***ncbi-tools6***, ***neovim***, ***nginx***, ***node-growl***, ***node-ws***, ***opendmarc***, ***openssh***, ***open-vm-tools***, ***passwordsafe***, ***pound***, ***prelink***, ***python-clamav***, ***redis***, ***reportbug***, ***resiprocate***, ***ruby-mini-magick***, ***sash***, ***signing-party***, ***slurm-llnl***, ***t-digest***, ***tenshi***, ***thunderbird***, ***tzdata***, ***usbutils***, ***xymon***, ***yubico-piv-tool***, ***z3***, ***zfs-auto-snapshot***, ***zsh***
- The following packages have been moved to the maintained repository of UCS: ***exempi*** (Bug 49479), ***libiptcdata*** (Bug 49479), ***numad*** (Bug 49548), ***tracker*** (Bug 49479)

6.2. Basic system services

Feedback

6.2.1. Boot Loader

Feedback

- Re-add accidentally dropped patch to ignore files ending on `.debian` (Bug 49440).

6.3. Domain services

Feedback

6.3.1. DNS server

Feedback

- Fix dependency header of legacy SysV init script to work in environments installed with UCS-4.2 or older and without Samba4 (Bug 49440).

6.4. Univention Management Console

Feedback

6.4.1. Domain join module

Feedback

- Package rebuilt for new ***ldb*** library version 1.5.4 required by Samba 4.10 (Bug 49479).

6.5. System services

Feedback

6.5.1. PAM / Local group cache

Feedback

- Disable PAM module `systemd` by default. It can be re-enabled by setting the Univention Configuration Registry variable `pam/session/systemd` to `true` (Bug 49910).

6.6. Virtualization

Feedback

6.6.1. UCS Virtual Machine Manager (UVMM)

Feedback

- Re-connect VMs to bridges on network restart (Bug 49604).
- Use interleaved memory policy on NUMA architectures by default (Bug 49548).

6.7. Services for Windows

Feedback

6.7.1. Samba

Feedback

- Call `samba_dnsupdate` with `--use-samba-tool` instead of `--local` if Univention Configuration Registry variable `samba4/join/dnsupdate` is active (for UCS@school with Samba 4.10) (Bug 49482).
- Run `samba-tool dbcheck --reindex` on update to Samba 4.10 (Bug 49479).
- Re-add *auth methods* option removed from upstream Samba sources (Bug 47314).
- Update to Samba 4.10.3. The dependent packages ***tevent***, ***tdb***, ***ldb*** were updated to new versions as well (Bug 49479).

6.7.2. Univention S4 Connector

Feedback

- Use new LDAP control `DSDB_CONTROL_REPLICATED_UPDATE_OID` when changing *objectSid*'s in UCS@school (Bug 49481).
- The connector now properly handles the AD password change (Bug 49480).