univention
be open.

UCS 4.2-4 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 4.2-4

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

<feedback@univention.de>

Table of Contents

Chapter 1. Release Highlights

With Univention Corporate Server 4.2-4, the fourth point release of Univention Corporate Server (UCS) 4.2 is now available. It provides several feature improvements and extensions, new properties as well as various improvements and bugfixes. An overview of the most important changes are:

- Support for creating subfolders in shared folders was added to the Dovecot integration.
- The package ***univention-ldap-overlay-memberof*** is now automatically installed during the system configuration of backup domain controller and slave domain controller systems if the *memberOf* overlay module is enabled on the master domain controller.
- Individual changes to the Postfix configuration can now be added to the files `main.cf.local` and `master.cf.local`.
- A confirmation dialog has been added which is shown after a user changed their password at the self-service module.
- A new API for programming of Univention Directory Listener modules was added.
- Various security updates have been integrated into UCS 4.2-4, e.g. OpenLDAP, the Linux kernel, Samba, MySQL and PostgreSQL. A complete list 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 6 GB of disk space. Depending on the scope of the existing installation, the update will require about another 1 GB of disk space for download and installation all packages.

For the update, a login should be performed on the system's local console as user `root`, and the update should be initiated there. Alternatively, the update can be conducted using Univention Management Console.

Remote updating via SSH is not recommended as this may result in the update procedure being canceled, e.g., if the network connection is interrupted. In consequence, this can affect the system severely. If updating should occur over a network connection nevertheless, it must be verified that the update continues in case of disconnection from the network. This can be achieved, e.g., using the tools `screen` and `at`. These tools are installed on all UCS system roles by default.

Chapter 4. Postprocessing of the update

Following the update, new or updated join scripts need to be executed. This can be done in two ways: Either using the UMC module **Domain join** or by running the command `univention-run-join-scripts` as user `root`.

Subsequently the UCS system needs to be restarted.

Chapter 5. Further notes on selected packages

5.1. Collection of usage statistics

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 *4.2-3*:

6.1. General

Feedback

- When Univention System Setup detects that the LDAP overlay module *memberOf* is activated on the master domain controller the package ***univention-ldap-overlay-memberof*** is automatically installed (Bug 46091).
- All security updates issued for UCS 4.2-3 are included:
  - ***apache2*** CVE-2016-0736 CVE-2016-2161 CVE-2016-8743 CVE-2017-3167 CVE-2017-3169 CVE-2017-7668 CVE-2017-7679 CVE-2017-9788 CVE-2017-9798 CVE-2017-15710 CVE-2017-15715 CVE-2018-1283 CVE-2018-1301 CVE-2018-1303 CVE-2018-1312 (Bug 44400)
  - ***asterisk*** CVE-2017-17090 (Bug 46113)
  - ***augeas*** CVE-2017-7555 (Bug 45356)
  - ***beep*** CVE-2018-0492 (Bug 46767)
  - ***bind9*** CVE-2017-3145 (Bug 46238)
  - ***bluez*** CVE-2017-1000250 (Bug 45551)
  - ***c-ares*** CVE-2017-1000381 (Bug 46247)
  - ***catdoc*** CVE-2017-11110 (Bug 45150)
  - ***clamav*** CVE-2017-12374 CVE-2017-12375 CVE-2017-12376 CVE-2017-12377 CVE-2017-12378 CVE-2017-12379 CVE-2017-12380 (Bug 46180)
  - ***curl*** CVE-2017-8816 CVE-2017-8817 CVE-2017-1000100 CVE-2017-1000101 CVE-2017-1000254 CVE-2017-1000257 CVE-2018-1000007 CVE-2018-1000120 CVE-2018-1000121 CVE-2018-1000122 (Bug 45604)
  - ***db*** CVE-2017-10140 (Bug 46240)
  - ***db5.3*** CVE-2017-10140 (Bug 46241)
  - ***dovecot*** CVE-2017-14461 CVE-2017-15130 CVE-2017-15132 (Bug 46481)
  - ***emacs24*** CVE-2017-14482 (Bug 45612)
  - ***erlang*** CVE-2017-1000385 (Bug 46115)
  - ***exim4*** CVE-2017-1000369 CVE-2018-6789 (Bug 44861)
  - ***expat*** CVE-2016-9063 CVE-2017-9233 (Bug 44859)
  - ***firebird2.5*** CVE-2017-6369 (Bug 46246)
  - ***firefox-esr*** CVE-2017-7753 CVE-2017-7779 CVE-2017-7784 CVE-2017-7785 CVE-2017-7786 CVE-2017-7787 CVE-2017-7791 CVE-2017-7792 CVE-2017-7793 CVE-2017-7798 CVE-2017-7800 CVE-2017-7801 CVE-2017-7802 CVE-2017-7803 CVE-2017-7805 CVE-2017-7807 CVE-2017-7809 CVE-2017-7810 CVE-2017-7814 CVE-2017-7818 CVE-2017-7819 CVE-2017-7823 CVE-2017-7824

CVE-2017-7826 CVE-2017-7828 CVE-2017-7830 CVE-2017-7843 CVE-2018-5089 CVE-2018-5091 CVE-2018-5095 CVE-2018-5096 CVE-2018-5097 CVE-2018-5098 CVE-2018-5099 CVE-2018-5102 CVE-2018-5103 CVE-2018-5104 CVE-2018-5117 CVE-2018-5125 CVE-2018-5127 CVE-2018-5129 CVE-2018-5130 CVE-2018-5131 CVE-2018-5144 CVE-2018-5145 CVE-2018-5146 CVE-2018-5147 CVE-2018-5148 (Bug 45611 Bug 46689)

- ***freeradius*** CVE-2017-10978 CVE-2017-10979 CVE-2017-10980 CVE-2017-10981 CVE-2017-10982 CVE-2017-10983 (Bug 45232)

- ***freerdp*** CVE-2017-2834 CVE-2017-2835 CVE-2017-2836 CVE-2017-2837 CVE-2017-2838 CVE-2017-2839 (Bug 45154)

- ***freetype*** CVE-2016-10244 CVE-2017-8105 CVE-2017-8287 (Bug 44574)

- ***gcc-4.9*** CVE-2017-5715 (Bug 46029 Bug 46209)

- ***gdk-pixbuf*** CVE-2017-2862 CVE-2017-1000422 (Bug 45603)

- ***ghostscript*** CVE-2017-9611 CVE-2017-9612 CVE-2017-9726 CVE-2017-9727 CVE-2017-9739 CVE-2017-9835 CVE-2017-11714 (Bug 45616)

- ***git*** CVE-2017-14867 CVE-2017-1000117 (Bug 45235)

- ***glibc*** CVE-2017-1000366 (Bug 44860)

- ***gnupg*** CVE-2017-7526 (Bug 45362)

- ***gnutls28*** CVE-2017-5334 CVE-2017-5335 CVE-2017-5336 CVE-2017-5337 CVE-2017-7507 CVE-2017-7869 (Bug 44855)

- ***graphite2*** CVE-2017-7771 CVE-2017-7772 CVE-2017-7773 CVE-2017-7774 CVE-2017-7775 CVE-2017-7776 CVE-2017-7777 (Bug 44864)

- ***gst-plugins-bad1.0*** CVE-2016-9809 CVE-2016-9812 CVE-2016-9813 CVE-2017-5843 CVE-2017-5848 (Bug 46122)

- ***gst-plugins-base1.0*** CVE-2016-9811 CVE-2017-5837 CVE-2017-5839 CVE-2017-5842 CVE-2017-5844 (Bug 44417)

- ***gst-plugins-good1.0*** CVE-2016-10198 CVE-2016-10199 CVE-2017-5840 CVE-2017-5841 CVE-2017-5845 (Bug 46123)

- ***gstreamer1.0*** CVE-2017-5838 (Bug 46124)

- ***icu*** CVE-2017-7867 CVE-2017-7868 CVE-2017-14952 CVE-2017-15422 (Bug 44415 Bug 46768)

- ***imagemagick*** CVE-2017-9144 CVE-2017-9261 CVE-2017-9262 CVE-2017-9405 CVE-2017-9407 CVE-2017-9409 CVE-2017-9439 CVE-2017-9440 CVE-2017-9501 CVE-2017-10928 CVE-2017-11141 CVE-2017-11170 CVE-2017-11188 CVE-2017-11352 CVE-2017-11360 CVE-2017-11447 CVE-2017-11448 CVE-2017-11449 CVE-2017-11450 CVE-2017-11478 CVE-2017-11505 CVE-2017-11524 CVE-2017-11525 CVE-2017-11526 CVE-2017-11527 CVE-2017-11528 CVE-2017-11529 CVE-2017-11530 CVE-2017-11640 CVE-2017-12431 CVE-2017-12640 CVE-2017-12877 CVE-2017-12983 CVE-2017-13134 CVE-2017-13139 CVE-2017-13144 CVE-2017-13758 CVE-2017-13769 CVE-2017-14224 CVE-2017-14607 CVE-2017-14682 CVE-2017-14989 CVE-2017-15277 CVE-2017-16546 (Bug 45145)

- ***intel-microcode*** CVE-2017-5715 (Bug 46982)

- ***isc-dhcp*** CVE-2017-3144 CVE-2018-5732 CVE-2018-5733 (Bug 46548)
- ***jasper*** CVE-2016-9591 CVE-2016-10249 CVE-2016-10251 (Bug 44332)
- ***kde4libs*** CVE-2017-6410 CVE-2017-8422 (Bug 44678)
- ***kdepim*** CVE-2017-9604 (Bug 46135)
- ***krb5*** CVE-2015-2694 CVE-2016-3119 CVE-2016-3120 CVE-2017-11368 (Bug 46136)
- ***libav*** CVE-2017-16803 (Bug 46364)
- ***libcrypto++*** CVE-2015-2141 CVE-2016-3995 CVE-2016-9939 (Bug 46137)
- ***libffi*** CVE-2017-1000376 (Bug 44862)
- ***libgcrypt20*** CVE-2017-7526 CVE-2017-9526 (Bug 44857)
- ***libgd2*** CVE-2017-6362 CVE-2017-7890 (Bug 45349)
- ***libmad*** CVE-2017-8372 CVE-2017-8373 CVE-2017-8374 (Bug 46963)
- ***libmspack*** CVE-2017-6419 CVE-2017-11423 (Bug 46138)
- ***libmwaw*** CVE-2017-9433 (Bug 46139)
- ***libonig*** CVE-2017-9224 CVE-2017-9226 CVE-2017-9227 CVE-2017-9228 CVE-2017-9229 (Bug 46140)
- ***libraw*** CVE-2017-6886 CVE-2017-6887 (Bug 45350)
- ***librelp*** CVE-2018-1000140 (Bug 46769)
- ***libreoffice*** CVE-2017-12607 CVE-2017-12608 CVE-2018-6871 CVE-2018-10119 CVE-2018-10120 (Bug 45916)
- ***libsoup2.4*** CVE-2017-2885 (Bug 45230)
- ***libtirpc*** CVE-2017-8779 (Bug 44674)
- ***libvirt*** CVE-2017-2635 CVE-2017-1000256 CVE-2018-1064 CVE-2018-5748 CVE-2018-6764 (Bug 45635)
- ***libvorbis*** CVE-2018-5146 (Bug 46693)
- ***libvpx*** CVE-2017-13194 (Bug 46482)
- ***libwpd*** CVE-2017-14226 (Bug 46141)
- ***libx11*** CVE-2016-7942 CVE-2016-7943 (Bug 46142)
- ***libxcursor*** CVE-2017-16612 (Bug 46143)
- ***libxfixes*** CVE-2016-7944 (Bug 46144)
- ***libxfont*** CVE-2017-13720 CVE-2017-13722 (Bug 45621)
- ***libxi*** CVE-2016-7945 CVE-2016-7946 (Bug 46145)

- ***libxml-libxml-perl*** CVE-2017-10672 (Bug 44776 Bug 45754)

- ***libxml2*** CVE-2017-0663 CVE-2017-7375 CVE-2017-7376 CVE-2017-9047 CVE-2017-9048 CVE-2017-9049 CVE-2017-9050 CVE-2017-15412 (Bug 45355 Bug 46242)

- ***libxrandr*** CVE-2016-7947 CVE-2016-7948 (Bug 46146)

- ***libxslt*** CVE-2017-5029 (Bug 46147)

- ***libxtst*** CVE-2016-7951 CVE-2016-7952 (Bug 46148)

- ***libxv*** CVE-2016-5407 (Bug 46150)

- ***libxvmc*** CVE-2016-7953 (Bug 46149)

- ***linux*** CVE-2017-0861 CVE-2017-5715 CVE-2017-5753 CVE-2017-5754 CVE-2017-8824 CVE-2017-13166 CVE-2017-15115 CVE-2017-16536 CVE-2017-16647 CVE-2017-16649 CVE-2017-16650 CVE-2017-16911 CVE-2017-16994 CVE-2017-16995 CVE-2017-17448 CVE-2017-17449 CVE-2017-17450 CVE-2017-17558 CVE-2017-17712 CVE-2017-17741 CVE-2017-17805 CVE-2017-17806 CVE-2017-17807 CVE-2017-17862 CVE-2017-17863 CVE-2017-18193 CVE-2017-1000405 CVE-2017-1000407 CVE-2017-1000410 CVE-2018-5344 CVE-2018-7480 CVE-2018-1000028 (Bug 45981 Bug 46009 Bug 46029 Bug 46209)

- ***mysql-5.5*** CVE-2017-10268 CVE-2017-10378 CVE-2017-10379 CVE-2017-10384 CVE-2018-2562 CVE-2018-2622 CVE-2018-2640 CVE-2018-2665 CVE-2018-2668 CVE-2018-2755 CVE-2018-2761 CVE-2018-2771 CVE-2018-2773 CVE-2018-2781 CVE-2018-2813 CVE-2018-2817 CVE-2018-2818 CVE-2018-2819 (Bug 45633 Bug 46865)

- ***ncurses*** CVE-2017-10684 CVE-2017-10685 CVE-2017-11112 CVE-2017-11113 CVE-2017-13728 CVE-2017-13729 CVE-2017-13730 CVE-2017-13731 CVE-2017-13732 CVE-2017-13733 CVE-2017-13734 (Bug 46152)

- ***net-snmp*** CVE-2015-5621 CVE-2018-1000116 (Bug 46770)

- ***nss*** CVE-2017-7805 (Bug 45618)

- ***openexr*** CVE-2017-9110 CVE-2017-9112 CVE-2017-9116 (Bug 45363)

- ***openjdk-7*** CVE-2017-3509 CVE-2017-3511 CVE-2017-3526 CVE-2017-3533 CVE-2017-3539 CVE-2017-3544 CVE-2017-10053 CVE-2017-10067 CVE-2017-10074 CVE-2017-10081 CVE-2017-10087 CVE-2017-10089 CVE-2017-10090 CVE-2017-10096 CVE-2017-10101 CVE-2017-10102 CVE-2017-10107 CVE-2017-10108 CVE-2017-10109 CVE-2017-10110 CVE-2017-10115 CVE-2017-10116 CVE-2017-10118 CVE-2017-10135 CVE-2017-10176 CVE-2017-10193 CVE-2017-10198 CVE-2017-10243 CVE-2017-10274 CVE-2017-10281 CVE-2017-10285 CVE-2017-10295 CVE-2017-10345 CVE-2017-10346 CVE-2017-10347 CVE-2017-10348 CVE-2017-10349 CVE-2017-10350 CVE-2017-10355 CVE-2017-10356 CVE-2017-10357 CVE-2017-10388 CVE-2018-2579 CVE-2018-2588 CVE-2018-2599 CVE-2018-2602 CVE-2018-2603 CVE-2018-2618 CVE-2018-2629 CVE-2018-2633 CVE-2018-2634 CVE-2018-2637 CVE-2018-2641 CVE-2018-2663 CVE-2018-2677 CVE-2018-2678 (Bug 44687 Bug 46320)

- ***openssl*** CVE-2017-3735 CVE-2017-3736 CVE-2017-3737 CVE-2017-3738 (Bug 45750)

- ***openvpn*** CVE-2017-7479 CVE-2017-7508 CVE-2017-7520 CVE-2017-7521 (Bug 44969)

- ***p7zip*** CVE-2015-1038 CVE-2016-2335 CVE-2017-17969 (Bug 46245)

- ***perl*** CVE-2017-6512 CVE-2017-12837 CVE-2017-12883 CVE-2018-6913 (Bug 44776)
- ***php5*** CVE-2017-11142 CVE-2017-11143 CVE-2017-11144 CVE-2017-11145 CVE-2017-11628 CVE-2017-12933 CVE-2017-16642 (Bug 46154)
- ***pjproject*** CVE-2017-9359 CVE-2017-9372 (Bug 45234)
- ***poppler*** CVE-2017-9406 CVE-2017-9408 CVE-2017-9775 CVE-2017-9776 CVE-2017-9865 CVE-2017-14517 CVE-2017-14518 CVE-2017-14519 CVE-2017-14520 CVE-2017-14617 CVE-2017-14929 CVE-2017-14975 CVE-2017-14976 CVE-2017-14977 CVE-2017-15565 CVE-2017-1000456 (Bug 46153)
- ***postgresql-9.4*** CVE-2017-12172 CVE-2017-15098 (Bug 45752 Bug 45753)
- ***postgresql-common*** CVE-2017-8806 (Bug 45752 Bug 45753)
- ***procmail*** CVE-2017-16844 (Bug 46155)
- ***proftpd-dfsg*** CVE-2016-3125 CVE-2017-7418 (Bug 46156)
- ***pyjwt*** CVE-2017-11424 (Bug 46157)
- ***qemu*** CVE-2016-8667 CVE-2016-9603 CVE-2017-6505 CVE-2017-7377 CVE-2017-7471 CVE-2017-7493 CVE-2017-8086 CVE-2017-8112 CVE-2017-8309 CVE-2017-8379 CVE-2017-8380 CVE-2017-9310 CVE-2017-9330 CVE-2017-9373 CVE-2017-9374 CVE-2017-9375 CVE-2017-9524 CVE-2017-10664 CVE-2017-10806 CVE-2017-10911 CVE-2017-11334 CVE-2017-11434 CVE-2017-12809 CVE-2017-13672 CVE-2017-13711 CVE-2017-14167 (Bug 46217)
- ***rpcbind*** CVE-2017-8779 (Bug 44674 Bug 46158)
- ***rsync*** CVE-2017-16548 CVE-2017-17433 CVE-2017-17434 (Bug 46159)
- ***samba*** CVE-2018-1050 CVE-2018-1057 (Bug 46485)
- ***sane-backends*** CVE-2017-6318 (Bug 46244)
- ***sdl-image1.2*** CVE-2017-2887 CVE-2017-12122 CVE-2017-14440 CVE-2017-14441 CVE-2017-14442 CVE-2017-14448 CVE-2017-14450 CVE-2018-3837 CVE-2018-3838 CVE-2018-3839 (Bug 45620)
- ***sensible-utils*** CVE-2017-17512 (Bug 46160)
- ***simplesamlphp*** CVE-2017-12867 CVE-2017-12869 CVE-2017-12874 CVE-2017-18121 CVE-2017-18122 CVE-2018-6519 CVE-2018-6521 CVE-2018-7644 (Bug 46480)
- ***smarty3*** CVE-2017-1000480 (Bug 46169)
- ***spice*** CVE-2017-7506 (Bug 45143)
- ***squid3*** CVE-2018-1000024 CVE-2018-1000027 (Bug 46392)
- ***subversion*** CVE-2016-8734 CVE-2017-9800 (Bug 44776 Bug 45233)
- ***sudo*** CVE-2017-1000368 (Bug 46161)
- ***systemd*** CVE-2016-7796 (Bug 46134)

- *tcpdump* CVE-2017-11108 CVE-2017-11541 CVE-2017-11542 CVE-2017-11543 CVE-2017-12893 CVE-2017-12894 CVE-2017-12895 CVE-2017-12896 CVE-2017-12897 CVE-2017-12898 CVE-2017-12899 CVE-2017-12900 CVE-2017-12901 CVE-2017-12902 CVE-2017-12985 CVE-2017-12986 CVE-2017-12987 CVE-2017-12988 CVE-2017-12989 CVE-2017-12990 CVE-2017-12991 CVE-2017-12992 CVE-2017-12993 CVE-2017-12994 CVE-2017-12995 CVE-2017-12996 CVE-2017-12997 CVE-2017-12998 CVE-2017-12999 CVE-2017-13000 CVE-2017-13001 CVE-2017-13002 CVE-2017-13003 CVE-2017-13004 CVE-2017-13005 CVE-2017-13006 CVE-2017-13007 CVE-2017-13008 CVE-2017-13009 CVE-2017-13010 CVE-2017-13011 CVE-2017-13012 CVE-2017-13013 CVE-2017-13014 CVE-2017-13015 CVE-2017-13016 CVE-2017-13017 CVE-2017-13018 CVE-2017-13019 CVE-2017-13020 CVE-2017-13021 CVE-2017-13022 CVE-2017-13023 CVE-2017-13024 CVE-2017-13025 CVE-2017-13026 CVE-2017-13027 CVE-2017-13028 CVE-2017-13029 CVE-2017-13030 CVE-2017-13031 CVE-2017-13032 CVE-2017-13033 CVE-2017-13034 CVE-2017-13035 CVE-2017-13036 CVE-2017-13037 CVE-2017-13038 CVE-2017-13039 CVE-2017-13040 CVE-2017-13041 CVE-2017-13042 CVE-2017-13043 CVE-2017-13044 CVE-2017-13045 CVE-2017-13046 CVE-2017-13047 CVE-2017-13048 CVE-2017-13049 CVE-2017-13050 CVE-2017-13051 CVE-2017-13052 CVE-2017-13053 CVE-2017-13054 CVE-2017-13055 CVE-2017-13687 CVE-2017-13688 CVE-2017-13689 CVE-2017-13690 CVE-2017-13725 (Bug 45564)

- *tiff* CVE-2014-8127 CVE-2016-3658 CVE-2016-9535 CVE-2016-10095 CVE-2016-10266 CVE-2016-10267 CVE-2016-10269 CVE-2016-10270 CVE-2017-5225 CVE-2017-7592 CVE-2017-7593 CVE-2017-7594 CVE-2017-7595 CVE-2017-7596 CVE-2017-7597 CVE-2017-7598 CVE-2017-7599 CVE-2017-7600 CVE-2017-7601 CVE-2017-7602 CVE-2017-9147 CVE-2017-9403 CVE-2017-9404 CVE-2017-9935 CVE-2017-9936 CVE-2017-10688 CVE-2017-11335 CVE-2017-12944 CVE-2017-13726 CVE-2017-13727 CVE-2017-18013 (Bug 44571)

- *univention-kernel-image* CVE-2017-0861 CVE-2017-5715 CVE-2017-5753 CVE-2017-5754 CVE-2017-8824 CVE-2017-13166 CVE-2017-15115 CVE-2017-16536 CVE-2017-16647 CVE-2017-16649 CVE-2017-16650 CVE-2017-16911 CVE-2017-16994 CVE-2017-16995 CVE-2017-17448 CVE-2017-17449 CVE-2017-17450 CVE-2017-17558 CVE-2017-17712 CVE-2017-17741 CVE-2017-17805 CVE-2017-17806 CVE-2017-17807 CVE-2017-17862 CVE-2017-17863 CVE-2017-18193 CVE-2017-1000405 CVE-2017-1000407 CVE-2017-1000410 CVE-2018-5344 CVE-2018-7480 CVE-2018-1000028 (Bug 45981 Bug 46009 Bug 46029 Bug 46209)

- *univention-kernel-image-signed* CVE-2017-0861 CVE-2017-5715 CVE-2017-5753 CVE-2017-5754 CVE-2017-8824 CVE-2017-13166 CVE-2017-15115 CVE-2017-16536 CVE-2017-16647 CVE-2017-16649 CVE-2017-16650 CVE-2017-16911 CVE-2017-16994 CVE-2017-16995 CVE-2017-17448 CVE-2017-17449 CVE-2017-17450 CVE-2017-17558 CVE-2017-17712 CVE-2017-17741 CVE-2017-17805 CVE-2017-17806 CVE-2017-17807 CVE-2017-17862 CVE-2017-17863 CVE-2017-18193 CVE-2017-1000405 CVE-2017-1000407 CVE-2017-1000410 CVE-2018-5344 CVE-2018-7480 CVE-2018-1000028 (Bug 45981 Bug 46009 Bug 46029 Bug 46209)

- *unrar-nonfree* CVE-2012-6706 (Bug 46163)

- *varnish* CVE-2017-12425 (Bug 45157)

- *vlc* CVE-2017-8310 CVE-2017-8311 CVE-2017-8312 CVE-2017-8313 CVE-2017-9300 CVE-2017-9301 CVE-2017-10699 (Bug 44968)

- *w3m* (Bug 46243)

- *wget* CVE-2017-13089 CVE-2017-13090 CVE-2018-0494 (Bug 45638 Bug 46980)

  - ***wireshark*** CVE-2017-11408 CVE-2017-17083 CVE-2017-17084 CVE-2017-17085 CVE-2018-5334 CVE-2018-5335 CVE-2018-5336 (Bug 46164)

  - ***wpa*** CVE-2017-13077 CVE-2017-13078 CVE-2017-13079 CVE-2017-13080 CVE-2017-13081 CVE-2017-13082 CVE-2017-13086 CVE-2017-13087 CVE-2017-13088 (Bug 45628)

  - ***xorg-server*** CVE-2015-3164 CVE-2017-2624 CVE-2017-10971 CVE-2017-10972 CVE-2017-12176 CVE-2017-12177 CVE-2017-12178 CVE-2017-12179 CVE-2017-12180 CVE-2017-12181 CVE-2017-12182 CVE-2017-12183 CVE-2017-12184 CVE-2017-12185 CVE-2017-12186 CVE-2017-12187 CVE-2017-13721 CVE-2017-13723 (Bug 44973)

  - ***zziplib*** CVE-2017-5974 CVE-2017-5975 CVE-2017-5976 CVE-2017-5978 CVE-2017-5979 CVE-2017-5980 CVE-2017-5981 (Bug 44856)

- The following updated packages from Debian Jessie 8.10 are included (Bug 46967): ***activemq***, ***apf-firewall***, ***apt-cacher***, ***apt-xapian-index***, ***atril***, ***audiofile***, ***awstats***, ***bareos***, ***bashburn***, ***bchunk***, ***binutils***, ***bitlbee***, ***boinc***, ***botan1.10***, ***bouncycastle***, ***bzr***, ***cfitsio***, ***chkrootkit***, ***chromium-browser***, ***commons-daemon***, ***connman***, ***courier-filter-perl***, ***cqrlog***, ***cups***, ***cvs***, ***debconf***, ***debian-archive-keyring***, ***debian-edu-doc***, ***debian-history***, ***debian-installer-netboot-images***, ***debian-installer***, ***debian-security-support***, ***debmirror***, ***debootstrap***, ***deluge***, ***dns-root-data***, ***dput***, ***dropbear***, ***drupal7***, ***dwww***, ***elog***, ***enigmail***, ***eterm***, ***ettercap***, ***evince***, ***fontforge***, ***fop***, ***foremost***, ***foxyproxy***, ***freeplane***, ***freexl***, ***gajim***, ***galternatives***, ***gifsicle***, ***gimp***, ***git-annex***, ***gitolite3***, ***gnats***, ***gnome-media***, ***gnome-screenshot***, ***gnome-settings-daemon***, ***groovy2***, ***groovy***, ***gsoap***, ***gst-plugins-ugly1.0***, ***gtk+2.0***, ***guile-2.0***, ***gunicorn***, ***hexchat***, ***hunspell-en-us***, ***icedove***, ***icedove***, ***icoutils***, ***initramfs-tools***, ***init-select***, ***installation-guide***, ***irqbalance***, ***irssi***, ***jackrabbit***, ***jackson-databind***, ***jhead***, ***jython***, ***kamailio***, ***kedpm***, ***keyringer***, ***knot***, ***konversation***, ***kup***, ***ldap-account-manager***, ***libapache2-mod-perl2***, ***libcgi-application-plugin-anytemplate-perl***, ***libclamunrar***, ***libdata-faker-perl***, ***libdatetime-timezone-perl***, ***libdbi***, ***libdvdnav***, ***libembperl-perl***, ***libhtml-microformats-perl***, ***libhttp-proxy-perl***, ***libidn2-0***, ***libindicate***, ***libio-socket-ssl-perl***, ***liblouis***, ***libmateweather***, ***libofx***, ***libosinfo***, ***libosip2***, ***libpam4j***, ***libsdl2-image***, ***libspring-ldap-java***, ***libsys-syscall-perl***, ***libterralib***, ***libvorbisidec***, ***libwmf***, ***libwnckmm***, ***libx11-protocol-other-perl***, ***libxstream-java***, ***libytnef***, ***linux-latest***, ***logback***, ***lucene-solr***, ***lxc***, ***lxterminal***, ***mailman***, ***mariadb-10.0***, ***mercurial***, ***metar***, ***minicom***, ***mobile-broadband-provider-info***, ***modsecurity-crs***, ***mongodb***, ***mosquitto***, ***most***, ***mupdf***, ***mysql-connector-java***, ***ndisc6***, ***ndoutils***, ***netcfg***, ***newsbeuter***, ***nginx***, ***nostalgy***, ***nvidia-graphics-drivers-legacy-304xx***, ***nvidia-graphics-drivers***, ***nvidia-graphics-modules***, ***offlineimap***, ***openchange***, ***openjpeg2***, ***openmpi***, ***openocd***, ***openoffice.org-dictionaries***, ***opensaml2***, ***openssh***, ***optipng***, ***os-prober***, ***otrs2***, ***partman-ext3***, ***pdns***, ***pdns-recursor***, ***php-radius***, ***pidgin***, ***plexus-utils2***, ***plexus-utils***, ***plv8***, ***poco***, ***polarssl***, ***puppet***, ***python-colorlog***, ***python-django***, ***python-gnupg***, ***python-plumbum***, ***python-tablib***, ***quagga***, ***quassel***, ***radare2***, ***r-base***, ***readline5***, ***request-tracker4***, ***rkhunter***, ***rt-authen-externalauth***, ***ruby-omniauth***, ***ruby-ox***, ***sage-extension***, ***sam2p***, ***sendmail***, ***sharutils***, ***shibboleth-sp2***, ***shutter***, ***sieve-extension***, ***sitesummary***, ***slurm-llnl***, ***smb4k***, ***smemstat***, ***spip***, ***squirrelmail***, ***strongswan***, ***supervisor***, ***sus***, ***synergy***, ***syslinux***, ***tabix***, ***tcpdf***, ***thunderbird***, ***tnef***, ***tomcat6***, ***tomcat7***, ***tomcat8***, ***tomcat-native***, ***tor***, ***transfig***, ***transmission***, ***transmissionrpc***, ***tryton-server***, ***tzdata***, ***unbound***, ***uwsgi***, ***uzbek-wordlist***, ***webissues-server***, ***weechat***, ***wordpress***, ***wordpress-shibboleth***, ***xarchiver***, ***xen***, ***xfce4-weather-plugin***, ***xmltooling***, ***xmobar***, ***yara***, ***zabbix***, ***zookeeper***

6.2. Basic system services

Feedback

6.2.1. Univention Configuration Registry

Feedback

6.2.1.1. Changes to templates and modules

Feedback

- The *SplitMode* setting of systemd-journald can now be set with the Univention Configuration Registry variable `systemd/journald/SplitMode` (Bug 46750).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

6.3.1.1. Listener/Notifier domain replication

Feedback

- A new API for programming of Univention Directory Listener modules was added (Bug 44786).
- To prevent `systemctl` from reporting a wrong status for the `univention-directory-listener` service, the `runsv` timeout has been increased to 30 seconds (Bug 46313).
- To prevent `systemctl` from reporting a wrong status for the `univention-directory-notifier` service, the `runsv` timeout has been increased to 30 seconds (Bug 46312).
- Very large LDAP schema definitions could prevent the LDAP server on backup domain controller and slave domain controller from starting. The fix ensures that such schemas are handled correctly (Bug 46743).

6.3.2. DNS server

Feedback

- To prevent `systemctl` from reporting a wrong status for the `univention-bind` service, the `runsv` timeout has been increased to 30 seconds (Bug 46310).
- Logging in the joinscript has been improved (Bug 42110).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- The sorting performance for lists in Univention Management Console has been improved (Bug 45076).
- Displaying of Python stack traces in Univention Management Console can now be prevented by setting the Univention Configuration Registry variable `umc/http/show_tracebacks` to `false` (Bug 45395).
- A JavaScript error that prevented the execution of startup hooks causing the menu to be empty on the portal site (Bug 45836).
- The Univention Management Console overview page now shows a banner that links to the Univention Summit website (Bug 45826).
- A notification about the advantages of using the Enterprise Edition of UCS is displayed after the login on specific systems (Bug 45809).
- The selection checkbox which have no possible actions have been removed from the `pkgdb` Univention Management Console module (Bug 44173).

6.4.2. Univention Management Console server

Feedback

- The password dialog that is shown upfront some functions in Univention Management Console when using a Single Sign On (SAML) session can now be submitted by pressing **Enter** (Bug 46882).
- SAML session handling with LDAP connections is improved and should not throw server tracebacks anymore (Bug 44621).
- Messages directed to the user are not displayed as an error anymore (Bug 46319).

- Displaying of Python stack traces in Univention Management Console can now be prevented by setting the Univention Configuration Registry variable `umc/http/show_tracebacks` to `false` (Bug 45395).
- A problem when using Internet Explorer 11 has been corrected which lead to broken redirections if the SAML identity provider is not resolvable during login (Bug 45424).
- The Univention Summit Banner is now only shown on systems using the Core Editions (Bug 45940).
- The Univention Management Console overview page now shows a banner that links to the Univention Summit website (Bug 45826).

6.4.3. Univention App Center

Feedback

- File permissions for `/etc/machine.secret` in App containers have been fixed (Bug 46835).
- Calling `univention-upgrade` non-interactively may have caused an error while upgrading Apps when run on a master domain controller (Bug 46703).
- Filter UCS components is now more robust with respect to diverted caches (Bug 45796).
- Show a rating's description when hovering over it (Bug 46060).
- Improved caching lookups to reduce startup time of the module (Bug 44783).
- Show the translated text for the license type of the App (Bug 45499).
- Upgrading an App failed when required App Settings were used. This has been fixed (Bug 46222).
- Customize environment variable name `LDAP_HOSTDN` (Bug 46223).
- Limit the number of backups created when uninstalling Docker Apps (Bug 44480).
- Univention now receives more detailed error messages when App installations fail (Bug 45808).
- An upgrade path between a Docker image for UCS 4.1 and one for UCS 4.2 was added (Bug 45795).

6.4.4. Modules for system settings / setup wizard

Feedback

- The package ***univention-ldap-overlay-memberof*** is now automatically installed during the system configuration of master domain controller and slave domain controller systems if the *memberOf* overlay module is enabled on the master domain controller (Bug 44448).

6.4.5. Domain join module

Feedback

- The error return codes when joining computers have been improved (Bug 45263).
- The logging of joinscript failures has been improved (Bug 42110).

6.4.6. Users module

Feedback

- It is now prevented to set mail addresses without local part or without domain part (Bug 46021).
- Kerberos authentication failed due to expired keys when the domain wide Samba *maxPwdAge* setting was is too large. Univention Directory Manager and Univention Management Console now restrict the values that can be set for *sambaMaxPwdAge* and *sambaMinPwdAge* (Bug 41865).

6.4.7. License module

- Add information about blocking browser add-ons to system activation error message (Bug 45899).

6.4.8. System diagnostic module

- The diagnostics module now correctly detects the file permissions of the Open-Xchange apps cache directory (Bug 46363).

6.4.9. Filesystem quota module

- The quota module now supports partitions mounted with the journaled quota option (Bug 45668).

6.4.10. Other modules

- The statistic graphics in the Univention Management Console module are now access protected (Bug 45192).

6.5. Software deployment

- The statistic graphics in the Univention Management Console module are now access protected (Bug 45192).
- Links in the log view during installing software upgrades via the Univention Management Console module can now be clicked (Bug 45060).
- A JavaScript error is prevented if receiving the maintenance status information is not possible (Bug 44080).

6.5.1. Software monitor

- Loading animations are now shown in the Univention Management Console module (Bug 45623).
- The selection checkbox which have no possible actions have been removed from the Univention Management Console module ***pkgdb*** (Bug 44173).

6.6. System services

6.6.1. SAML

- Restart the `univention-saml` daemon after an upgrade to prevent timeouts (Bug 46212).
- On the single-sign on login page only the domainname instead of the servers hostname is now shown (Bug 44121).
- The access permissions for the SAML Identify Provider certificate have been corrected (Bug 44704).

6.6.2. Univention self service

- Changing a password of an expired user account is possible again and a confirmation dialog has been added which is shown after changing the password (Bug 45813).
- The creation of postgresql database and users has been moved from the post installation script into the joinscript (Bug 44393).

- Notifications about successful password changes are shown again (Bug 45457).

- Users from an Active Directory domain now can reset their password via the Self Service. To enable the feature, the Univention Configuration Registry variables `ad/reset/username` and `ad/reset/password` need to be set (Bug 44867).

6.6.3. Mail services

Feedback

- The service status of some mail related services has been fixed and is now shown correctly in Univention Management Console (Bug 43555).

6.6.4. Dovecot

Feedback

- When moving a user's mailbox to a different filesystem, set owner and group for all files on the target filesystem (Bug 46893).

- The creation of ACLs for shared folders with ACLs including users or groups with a space character has been fixed (Bug 45921).

- Support for creating subfolders in shared folders was added. Please note that during the update, ACLs specified in LDAP will be forcefully written to Dovecot's shared folders to fix possible missing access rights (Bug 41138).

6.6.5. Postfix

Feedback

- Postfix' service `postscreen` has been integrated and can be configured via the Univention Configuration Registry variables prefixed by `mail/postfix/postscreen/`. The service performs lightweight checks on incoming SMTP connections to reject e.g. spam early (Bug 45607).

- If Univention Configuration Registry variable `mail/postfix/policy/listfilter/use_sasl_username` was set to `yes`, the `listfilter` policy service rejected all mail unexpectedly. The `listfilter` policy service has been fixed and now handles Cyrus SASL authentication correctly (Bug 45422).

- The content of the files `main.cf.local` and `master.cf.local` will now be appended to `/etc/postfix/main.cf` and `/etc/postfix/master.cf` respectively. After editing the `*.local` files, `ucr commit /etc/postfix/*.cf` must be called (Bug 44922).

- The `listfilter` policy service can now write debugging information to the mail log, when the Univention Configuration Registry variable `mail/postfix/policy/listfilter/debug` is set to `yes` (Bug 44473).

- The service status is now correctly detected and shown in Univention Management Console (Bug 43555).

6.6.6. Nagios

Feedback

- A Nagios check for the LDAP database maximum size has been added. With the LDAP MDB database backend, a maximum size is configured for the database (Univention Configuration Registry variable `ldap/database/mdb/maxsize`). If the maximum size is reached, write requests are no longer possible. The new plugin checks the effective size of the database and returns a warning if 75%, or critical if 90% are in use. The plugin is activated for all domain controllers upon the installation of the Nagios packages. For updates, the plugin has to be activated manually. This can be done by executing the following commands on the Nagios server and the client. `univention-run-join-scripts --force --run-scripts 26univention-nagios-common.inst 30univention-nagios-client.inst` (Bug 45685).

6.6.7. DHCP server

Feedback

- To prevent `systemctl` from reporting a wrong status for the `univention-dhcp` service, the `runsv` timeout has been increased to 30 seconds (Bug 46311).

6.6.8. Other services

Feedback

- The `iptables` chains will not be erased anymore when `univention-firewall` is stopped, if the Univention Configuration Registry variable `security/packetfilter/disabled` is set (Bug 45541).

6.7. Virtualization

Feedback

6.7.1. Univention Virtual Machine Manager (UVMM)

Feedback

- It is now possible to limit the target hosts a VM can be migrated to. The setting can be configured in the virtual machine detail view (Bug 45846).
- This update provides an updated version of ***OpenBIOS***, which is required for the new version of QEMU only for emulating the SPARC architecture.(Bug 46217).
- This is an update for the BIOS a virtual machine in UCS Virtual Machine Manager uses. On reset the original BIOS code was not copied back completely, which could result in virtual machines getting stuck after reboots. In order for virtual machines to load the updated BIOS, the virtual machine has to be shutdown and started again. A reboot does not suffice (Bug 44084).

6.8. Services for Windows

Feedback

6.8.1. Samba

Feedback

- Added a more detailed error message for the domain join (Bug 46762).
- Ignore unsupported Kerberos encryption types (Bug 46301).
- Fixed a segmentation fault of the `rpc_server` process when replicating as a non administrator with `GUID_DRS_GET_CHANGES` (Bug 45800).

6.8.2. Univention S4 Connector

Feedback

- `connector-tracebacks.log` is not written any longer (Bug 38140).
- Ignore unsupported Kerberos encryption types (Bug 46301).
- Rejects for DNs containing non-ASCII characters could not be saved, because ***python-sqlite3*** doesn't accept UTF-8, causing rejects not to be visible but keeping the S4-Connector retrying endlessly, flooding the logs with rejects (Bug 44369).