univention
be open.

UCS 4.2-5 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 4.2-5

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 4.2-5, the fifth Point-Release for Univention Corporate Server (UCS) 4.2 is now available. It includes various detail improvements and bug fixes, especially in the areas of Active Directory Compatibility and UCS Management System. The security updates released for UCS 4.2-4 are included in this update.

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 *4.2-4*:

6.1. General

- All security updates issued for UCS 4.2-4 are included:
  - ***base-files*** (Bug 47572)
  - ***bind9*** (CVE-2018-5740) (Bug 47750)
  - ***busybox*** (CVE-2011-5325 CVE-2014-9645 CVE-2015-9261 CVE-2016-2147 CVE-2016-2148 CVE-2017-15873 CVE-2017-16544 CVE-2018-1000517) (Bug 47519)
  - ***clamav*** (CVE-2018-0202 CVE-2018-0360 CVE-2018-0361 CVE-2018-1000085) (Bug 47474 Bug 47614)
  - ***cups*** (CVE-2017-18248 CVE-2018-4180 CVE-2018-4181 CVE-2018-6553) (Bug 47570)
  - ***curl*** (CVE-2018-14618 CVE-2018-1000301) (Bug 47554 Bug 47772)
  - ***dnsmasq*** (Bug 47529)
  - ***evolution-data-server*** (CVE-2016-10727) (Bug 47542)
  - ***exiv2*** (CVE-2018-10958 CVE-2018-10998 CVE-2018-10999 CVE-2018-11531 CVE-2018-12264 CVE-2018-12265) (Bug 47530)
  - ***faad2*** (CVE-2017-9218 CVE-2017-9219 CVE-2017-9220 CVE-2017-9221 CVE-2017-9222 CVE-2017-9223 CVE-2017-9253 CVE-2017-9254 CVE-2017-9255 CVE-2017-9256 CVE-2017-9257) (Bug 47574)
  - ***file*** (CVE-2018-10360) (Bug 47553)
  - ***firefox-esr*** (CVE-2018-5150 CVE-2018-5154 CVE-2018-5155 CVE-2018-5156 CVE-2018-5157 CVE-2018-5158 CVE-2018-5159 CVE-2018-5168 CVE-2018-5178 CVE-2018-5183 CVE-2018-5188 CVE-2018-6126 CVE-2018-12359 CVE-2018-12360 CVE-2018-12362 CVE-2018-12363 CVE-2018-12364 CVE-2018-12365 CVE-2018-12366 CVE-2018-12368) (Bug 47536)
  - ***fuse*** (CVE-2018-10906) (Bug 47605)
  - ***gdm3*** (CVE-2018-14424) (Bug 47761)
  - ***ghostscript*** (CVE-2016-10317 CVE-2018-10194) (Bug 47526)
  - ***git*** (CVE-2015-1196 CVE-2018-11233 CVE-2018-11235) (Bug 47547)
  - ***gnupg*** (CVE-2018-12020) (Bug 47563)
  - ***gnupg2*** (CVE-2018-12020) (Bug 47548)
  - ***imagemagick*** (CVE-2017-10995 CVE-2017-11533 CVE-2017-11535 CVE-2017-11639 CVE-2017-13143 CVE-2017-17504 CVE-2017-17879 CVE-2018-5248 CVE-2018-11251 CVE-2018-12599 CVE-2018-12600) (Bug 47537)

- ***intel-microcode*** (CVE-2018-3615 CVE-2018-3620 CVE-2018-3639 CVE-2018-3640 CVE-2018-3646) (Bug 47543 Bug 47670)
- ***lame*** (CVE-2017-9869 CVE-2017-9870 CVE-2017-9871 CVE-2017-9872 CVE-2017-15018 CVE-2017-15045 CVE-2017-15046) (Bug 47555)
- ***lcms2*** (CVE-2018-16435) (Bug 47773)
- ***libarchive-zip-perl*** (CVE-2018-10860) (Bug 47535)
- ***libdatetime-timezone-perl*** (Bug 47556)
- ***libgcrypt20*** (CVE-2018-0495) (Bug 47562)
- ***libidn*** (CVE-2017-14062) (Bug 47525)
- ***libipc-run-perl*** (Bug 47573)
- ***libmspack*** (CVE-2017-6419 CVE-2017-11423 CVE-2018-14679 CVE-2018-14680 CVE-2018-14681 CVE-2018-14682) (Bug 47575)
- ***libsoup2.4*** (CVE-2018-12910) (Bug 47520)
- ***libtirpc*** (CVE-2018-14622) (Bug 47752)
- ***libvncserver*** (CVE-2018-7225) (Bug 47546)
- ***libx11*** (CVE-2018-14598 CVE-2018-14599 CVE-2018-14600) (Bug 47753)
- ***libxcursor*** (CVE-2015-9262) (Bug 47615)
- ***linux*** (CVE-2017-17975 CVE-2017-18216 CVE-2017-18218 CVE-2017-18222 CVE-2017-18224 CVE-2017-18255 CVE-2017-18257 CVE-2018-1066 CVE-2018-1087 CVE-2018-1092 CVE-2018-1093 CVE-2018-1108 CVE-2018-1118 CVE-2018-1120 CVE-2018-1130 CVE-2018-3620 CVE-2018-3639 CVE-2018-3646 CVE-2018-5390 CVE-2018-6412 CVE-2018-7757 CVE-2018-8087 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897 CVE-2018-9363 CVE-2018-10021 CVE-2018-10087 CVE-2018-10876 CVE-2018-10877 CVE-2018-10878 CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10940 CVE-2018-12233 CVE-2018-13405 CVE-2018-13406 CVE-2018-14734 CVE-2018-15572 CVE-2018-15594 CVE-2018-1000199) (Bug 47063)
- ***memcached*** (CVE-2016-8705 CVE-2017-9951 CVE-2018-1000115 CVE-2018-1000127) (Bug 47533)
- ***mutt*** (CVE-2018-14349 CVE-2018-14350 CVE-2018-14351 CVE-2018-14352 CVE-2018-14353 CVE-2018-14354 CVE-2018-14355 CVE-2018-14356 CVE-2018-14357 CVE-2018-14358 CVE-2018-14359 CVE-2018-14360 CVE-2018-14361 CVE-2018-14362 CVE-2018-14363) (Bug 47521)
- ***ncurses*** (CVE-2017-16879) (Bug 47559)
- ***opencv*** (CVE-2016-1516 CVE-2017-12597 CVE-2017-12598 CVE-2017-12599 CVE-2017-12601 CVE-2017-12603 CVE-2017-12604 CVE-2017-12605 CVE-2017-12606 CVE-2017-12862 CVE-2017-12863 CVE-2017-12864 CVE-2017-14136 CVE-2017-17760 CVE-2017-1000450 CVE-2018-5268 CVE-2018-5269) (Bug 47524)

- ***openjdk-7*** (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 CVE-2018-2790 CVE-2018-2794 CVE-2018-2795 CVE-2018-2796 CVE-2018-2797 CVE-2018-2798 CVE-2018-2799 CVE-2018-2800 CVE-2018-2814 CVE-2018-2815) (Bug 47470)

- ***openssh*** (CVE-2015-6563 CVE-2015-6564 CVE-2016-1908 CVE-2016-3115 CVE-2016-6515 CVE-2016-10009 CVE-2016-10011 CVE-2016-10012 CVE-2016-10708 CVE-2017-15906 CVE-2018-15473) (Bug 47628 Bug 47778)

- ***patch*** (CVE-2018-1000156) (Bug 47528)

- ***perl*** (CVE-2018-12015) (Bug 47550)

- ***php5*** (CVE-2018-5712 CVE-2018-7584 CVE-2018-10545 CVE-2018-10546 CVE-2018-10547 CVE-2018-10548 CVE-2018-10549 CVE-2018-14851 CVE-2018-14883) (Bug 47558 Bug 47754)

- ***policykit-1*** (CVE-2018-1116) (Bug 47532)

- ***postgresql-9.4*** (CVE-2018-1053 CVE-2018-1058 CVE-2018-10915) (Bug 47527)

- ***procps*** (CVE-2018-1122 CVE-2018-1123 CVE-2018-1124 CVE-2018-1125 CVE-2018-1126) (Bug 47564)

- ***rar*** (Bug 47552)

- ***reportbug*** (Bug 47560)

- ***ruby2.1*** (CVE-2015-9096 CVE-2016-2337 CVE-2016-2339 CVE-2016-7798 CVE-2017-0898 CVE-2017-0899 CVE-2017-0900 CVE-2017-0901 CVE-2017-0902 CVE-2017-0903 CVE-2017-10784 CVE-2017-14033 CVE-2017-14064 CVE-2017-17405 CVE-2017-17742 CVE-2017-17790 CVE-2018-6914 CVE-2018-8777 CVE-2018-8778 CVE-2018-8779 CVE-2018-8780 CVE-2018-1000073 CVE-2018-1000074 CVE-2018-1000075 CVE-2018-1000076 CVE-2018-1000077 CVE-2018-1000078 CVE-2018-1000079) (Bug 47557 Bug 47684)

- ***samba*** (CVE-2018-10858 CVE-2018-10919) (Bug 47429)

- ***soundtouch*** (CVE-2017-9258 CVE-2017-9259 CVE-2017-9260) (Bug 47539)

- ***spice*** (CVE-2018-10873) (Bug 47755)

- ***subversion*** (Bug 47523)

- ***taglib*** (CVE-2018-11439) (Bug 47561)

- ***talloc*** (Bug 47429)

- ***tiff*** (CVE-2017-11613 CVE-2017-13726 CVE-2017-18013 CVE-2018-5784 CVE-2018-7456 CVE-2018-8905 CVE-2018-10963) (Bug 47545)

- ***tzdata*** (Bug 47556)

- ***univention-kernel-image*** (CVE-2017-17975 CVE-2017-18216 CVE-2017-18218 CVE-2017-18222 CVE-2017-18224 CVE-2017-18255 CVE-2017-18257 CVE-2018-1066 CVE-2018-1087 CVE-2018-1092 CVE-2018-1093 CVE-2018-1108 CVE-2018-1118 CVE-2018-1120 CVE-2018-1130 CVE-2018-3620 CVE-2018-3639 CVE-2018-3646 CVE-2018-5390 CVE-2018-6412 CVE-2018-7757

CVE-2018-8087 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897 CVE-2018-9363 CVE-2018-10021 CVE-2018-10087 CVE-2018-10876 CVE-2018-10877 CVE-2018-10878 CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10940 CVE-2018-12233 CVE-2018-13405 CVE-2018-13406 CVE-2018-14734 CVE-2018-15572 CVE-2018-15594 CVE-2018-1000199) (Bug 47063)

- ***univention-kernel-image-signed*** (CVE-2017-17975 CVE-2017-18216 CVE-2017-18218 CVE-2017-18222 CVE-2017-18224 CVE-2017-18255 CVE-2017-18257 CVE-2018-1066 CVE-2018-1087 CVE-2018-1092 CVE-2018-1093 CVE-2018-1108 CVE-2018-1118 CVE-2018-1120 CVE-2018-1130 CVE-2018-3620 CVE-2018-3639 CVE-2018-3646 CVE-2018-5390 CVE-2018-6412 CVE-2018-7757 CVE-2018-8087 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897 CVE-2018-9363 CVE-2018-10021 CVE-2018-10087 CVE-2018-10876 CVE-2018-10877 CVE-2018-10878 CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10940 CVE-2018-12233 CVE-2018-13405 CVE-2018-13406 CVE-2018-14734 CVE-2018-15572 CVE-2018-15594 CVE-2018-1000199) (Bug 47063)
- ***wireshark*** (CVE-2018-7334 CVE-2018-7335 CVE-2018-7419 CVE-2018-9261 CVE-2018-11358 CVE-2018-11362 CVE-2018-14339 CVE-2018-14340 CVE-2018-14341 CVE-2018-14342 CVE-2018-14343 CVE-2018-14368 CVE-2018-14369) (Bug 47534)
- ***wpa*** (CVE-2018-14526) (Bug 47571)
- ***xdg-utils*** (CVE-2017-18266) (Bug 47540)
- ***xerces-c*** (CVE-2017-12627) (Bug 47541)
- ***xml-security-c*** (Bug 47522)
- ***zendframework*** (CVE-2016-4861) (Bug 47531)

- The following updated packages from Debian Jessie 8.11 are included (Bug 47793): ***389-ds-base***, ***adminer***, ***ant***, ***batik***, ***blender***, ***blktrace***, ***bouncycastle***, ***bwm-ng***, ***cgit***, ***cinnamon***, ***confuse***, ***debian-installer-netboot-images***, ***debian-security-support***, ***dh-make-perl***, ***discount***, ***dns-root-data***, ***dojo***, ***dokuwiki***, ***dropbear***, ***git-annex***, ***gosa***, ***gpac***, ***graphicsmagick***, ***kamailio***, ***lava-server***, ***libcgroup***, ***libextractor***, ***libgit2***, ***linux-4.9***, ***linux-latest-4.9***, ***mactelnet***, ***mailman***, ***mariadb-10.0***, ***mercurial***, ***mgetty***, ***mosquitto***, ***network-manager-vpnc***, ***nvidia-graphics-drivers***, ***nvidia-graphics-drivers-legacy-304xx***, ***openjpeg2***, ***otrs2***, ***php-horde-crypt***, ***php-horde-image***, ***phpmyadmin***, ***plexus-archiver***, ***prosody***, ***psensor***, ***python-mimeparse***, ***python-xmltodict***, ***redis***, ***resiprocate***, ***ruby-passenger***, ***ruby-sprockets***, ***ruby-zip***, ***sam2p***, ***slurm-llnl***, ***spice-gtk***, ***spip***, ***squirrelmail***, ***sssd***, ***strongswan***, ***sympa***, ***thunderbird***, ***tomcat-native***, ***tomcat7***, ***tomcat8***, ***twitter-bootstrap3***, ***user-mode-linux***, ***vim-syntastic***, ***virtualbox-guest-additions-iso***, ***wordpress***, ***xen***, ***znc***, ***zookeeper***, ***zsh***, ***zutils***

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- New version to follow Debian changes (Bug 47544).

6.2.2. Univention Configuration Registry

Feedback

6.2.2.1. Changes to templates and modules

Feedback

- Univention Configuration Registry `autostart` variables are now correctly evaluated across all scopes (Bug 47260).

6.3. Univention Management Console

Feedback

6.3.1. Univention Management Console server

Feedback

- Fix memory leak caused by Python notifier traceback handling (Bug 47569).
- In certain situations after reloading the browser window the error message “There are no modules available for the currently authenticated user” was incorrectly displayed (Bug 46998).
- A problem with the SAML authentication which could lead to the Univention Management Console web interface becoming unresponsive has been fixed (Bug 47109).

6.3.2. Univention App Center

Feedback

- Fix memory leak caused by Python notifier traceback handling (Bug 47569).
- The command `univention-app` took every App from every UCS version into (Bug 47207).

6.3.3. Modules for system settings / setup wizard

Feedback

- Fix memory leak caused by Python notifier traceback handling (Bug 47569).

6.3.4. Domain join module

Feedback

- Fix memory leak caused by Python notifier traceback handling (Bug 47569).

6.3.5. Software update module

Feedback

- The updater message for UCS releases that receive extended maintenance was clarified (Bug 45672).

6.3.6. Other modules

Feedback

- Fix a memory leak preventing the Python garbage collector from freeing UCS Virtual Machine Manager connection instances (Bug 47569).

6.4. System services

Feedback

6.4.1. Cyrus

Feedback

- The PAM stack has been fixed to allow the login via username (Bug 42759).

6.4.2. Dovecot

Feedback

- The PAM stack has been fixed to allow the login via username (Bug 42759).

6.4.3. Postfix

Feedback

- The PAM stack has been fixed to allow the login via username (Bug 42759).

6.4.4. Apache

Feedback

- Added headers *X-Forwarded-Proto* and *X-Forwarded-SSL* so that certain Apps work correctly behind a proxy (Bug 47071).

6.5. Virtualization

Feedback

6.5.1. Univention Virtual Machine Manager (UVMM)

Feedback

- The hosts in the dialog Migrate domain are now sorted (Bug 47342).
- Make CPU-Usage column visibility configurable. The visibility is controlled by the Univention Configuration Registry variable `uvmm/umc/showcpuusage` (Bug 47137).
- Update to VirtIO driver for Windows to version 0.1.141-1 (Bug 47112).

6.6. Services for Windows

Feedback

6.6.1. Samba

Feedback

- After a server password change restart all of samba, not just the AD/DC component (Bug 47637).
- Adjust default for Univention Configuration Registry variable `samba/ntlm/auth` (`ntlm auth`) to `ntlmv2-only` (Bug 47100).
- Update package ***tevent*** to version 0.9.34 as required by Samba 4.6.15 (Bug 47429).
- When joining a new Samba/AD DC, Samba replicates all LDAP partitions independently. Depending on timing the replication of the linked attribute *serverReference* could fail, if `CN=Configuration` gets replicated before the main domain partition. As a result DRS replication could fail (Bug 47749).
- Fix regression: `samba-tool ntacl sysvolcheck` traceback due to `/var/lib/samba/netlogon` (Bug 47710).

6.6.2. Univention S4 Connector

Feedback

- The Univention Directory Listener module now restarts the connector if extended attributes are modified (Bug 47048).
- When objects are deleted or moved remove their DN from both group member mapping caches. This affected UCS@school (Bug 46971).

6.6.3. Univention Active Directory Connection

Feedback

- The Univention Directory Listener module now restarts the connector if extended attributes are modified (Bug 47050).

6.7. Other changes

Feedback

- If more than one hard disk drive is detected during UCS installation, the target disk for the grub installer can be selected Bug 47822.