univention
be open.

UCS 4.3 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.3-5

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

<feedback@univention.de>

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.3-5 steht das fünfte Point-Release für Univention Corporate Server (UCS) 4.3 zur Verfügung. Es umfasst Funktionserweiterungen und Verbesserungen, neue Eigenschaften sowie diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Samba wurde auf Version 4.10 aktualisiert.
- Mit 4.3-5 wird die Aktualisierung auf den Stand des Debian Release 9.11 abgeschlossen.
- Diverse Security Updates wurden in UCS 4.3-5 integriert, bspw. für Samba, den Linux Kernel und Dovecot. Eine vollständige Liste von Security- und Paketupdates ist in Kapitel 6 zu finden.

Kapitel 2. Hinweise zum Update

Während der Aktualisierung kann es zu temporären Ausfällen von Diensten innerhalb der Domäne kommen. Aus diesem Grund sollte das Update innerhalb eines Wartungsfensters erfolgen. Grundsätzlich wird empfohlen, das Update zunächst in einer Testumgebung einzuspielen und zu testen. Die Testumgebung sollte dabei identisch zur Produktivumgebung sein. Je nach Systemgeschwindigkeit, Netzwerkanbindung und installierter Software kann das Update zwischen 20 Minuten und mehreren Stunden dauern.

2.1. Empfohlene Update-Reihenfolge

Feedback

In Umgebungen mit mehr als einem UCS-System muss die Update-Reihenfolge der UCS-Systeme beachtet werden:

Auf dem Domänencontroller Master wird die maßgebliche (authoritative) Version des LDAP-Verzeichnisdienstes vorgehalten, die an alle übrigen LDAP-Server der UCS-Domäne repliziert wird. Da bei Release-Updates Veränderungen an den LDAP-Schemata auftreten können, muss der Domänencontroller Master bei einem Release-Update immer als erstes System aktualisiert werden.

2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante

Feedback

UCS-Installations-DVDs werden ab UCS 4 nur noch für 64-Bit-Architekturen bereitgestellt. Vorhandene 32-Bit UCS 3 Systeme können weiterhin über das Online Repository oder über Update DVDs auf UCS 4 aktualisiert werden. Die 32-Bit-Architektur wird für die gesamte UCS 4 Maintenance noch unterstützt.

Kapitel 3. Vorbereitung des Updates

Es sollte geprüft werden, ob ausreichend Festplattenplatz verfügbar ist. Eine Standard-Installation benötigt min. 10 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation ungefähr 4 GB zusätzlichen Speicherplatz zum Herunterladen und Installieren der Pakete.

Für das Update sollte eine Anmeldung auf der lokalen Konsole des Systems mit dem Benutzer `root` durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über Univention Management Console durchgeführt werden.

Eine Remote-Aktualisierung über SSH wird nicht empfohlen, da dies beispielsweise bei Unterbrechung der Netzverbindung zum Abbruch des Update-Vorgangs und zu einer Beeinträchtigung des Systems führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können beispielsweise die Tools `screen` oder `at` eingesetzt werden, die auf allen UCS Systemrollen installiert sind.

Kapitel 4. Nachbereitung des Updates

Nach dem Update müssen die neuen oder aktualisierten Join-Skripte ausgeführt werden. Dies kann auf zwei Wegen erfolgen: Entweder über das UMC-Modul **Domänenbeitritt** oder durch Aufruf des Befehls `univention-run-join-scripts` als Benutzer `root`.

Anschließend muss das UCS-System neu gestartet werden.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken

Feedback

Bei Verwendung der UCS Core Edition werden anonyme Nutzungsstatistiken zur Verwendung von Univention Management Console erzeugt. Die aufgerufenen Module werden dabei von einer Instanz des Web-Traffic-Analyse-Tools Piwik protokolliert. Dies ermöglicht es Univention die Entwicklung von Univention Management Console besser auf das Kundeninteresse zuzuschneiden und Usability-Verbesserungen vorzunehmen.

Diese Protokollierung erfolgt nur bei Verwendung der UCS Core Edition. Der Lizenzstatus kann überprüft werden durch den Eintrag **Lizenz - > Lizenzinformation** des Benutzermenüs in der rechten, oberen Ecke von Univention Management Console. Steht hier unter **Lizenztyp** der Eintrag **UCS Core Edition** wird eine solche Edition verwendet. Bei Einsatz einer regulären UCS-Lizenz erfolgt keine Teilnahme an der Nutzungsstatistik.

Die Protokollierung kann unabhängig von der verwendeten Lizenz durch Setzen der Univention Configuration Registry-Variable `umc/web/piwik` auf `false` deaktiviert werden.

5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit

Feedback

WebKit, Konqueror und QtWebKit werden in UCS im maintained-Zweig des Repositorys mitgeliefert, aber nicht durch Sicherheits-Updates unterstützt. WebKit wird vor allem für die Darstellung von HTML-Hilfeseiten u.ä. verwendet. Als Web-Browser sollte Firefox eingesetzt werden.

5.3. Empfohlene Browser für den Zugriff auf Univention Management Console

Feedback

Univention Management Console verwendet für die Darstellung der Web-Oberfläche zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden empfohlen:

- Chrome ab Version 37
- Firefox ab Version 38
- Internet Explorer ab Version 11
- Safari und Safari Mobile ab Version 9

Mit älteren Browsern können Darstellungs- oder Performanceprobleme auftreten.

Kapitel 6. Changelog

Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit 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***, ***biomaj-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).