univention
be open.

UCS 4.1-5 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.1-5

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

<feedback@univention.de>

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.1-5 steht das fünfte Point-Release für Univention Corporate Server (UCS) 4.1 zur Verfügung. Es umfasst diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Samba wurde mit wichtigen Sicherheitsupdates aktualisiert.
- Der Linux Kernel wurde auf den letzten stabilen 4.1er *Longterm*-Kernel aktualisiert. Dieser beinhaltet diverse Sicherheitsaktualisierungen, Verbesserungen in der Stabilität, sowie neuere und aktualisierte Treiber für eine verbesserte Hardware-Unterstützung.
- Die Startzeit des App Center UMC Moduls wurde verbessert. Diese Optimierung wird durch das differenzielle Herunterladen von aktualisierten Daten vom App Center Server mit Hilfe von ***zsync*** erreicht.

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. 6 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation ungefähr 2 GB weiteren 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 (die in der Regel für Evaluationen von UCS herangezogen wird) 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

Auf 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 4.1-4:

6.1. General

Feedback

- All security updates issued for UCS 4.1-4 are included:
  - ***mysql-5.5*** (CVE-2016-5483 CVE-2017-3302 CVE-2017-3305 CVE-2017-3308 CVE-2017-3309 CVE-2017-3329 CVE-2017-3453 CVE-2017-3456 CVE-2017-3461 CVE-2017-3462 CVE-2017-3463 CVE-2017-3464 CVE-2017-3600) (Bug 44516).
  - ***univention-kernel-image-signed*** (CVE-2017-6951 CVE-2017-7187 CVE-2017-7261 CVE-2017-7294 CVE-2017-7472 CVE-2017-7618 CVE-2017-7645 CVE-2016-10229 CVE-2016-2188 CVE-2016-8405 CVE-2016-9191 CVE-2016-9604 CVE-2017-5549 CVE-2017-5669 CVE-2017-7273 CVE-2017-8924 CVE-2017-8925) (Bug 44706).
  - ***dpkg*** (CVE-2015-0860) (Bug 43147 Bug 43173).
  - ***php5*** (CVE-2016-2554 CVE-2016-3141 CVE-2016-3142 CVE-2016-4342 CVE-2016-5385 CVE-2016-7124 CVE-2016-7128 CVE-2016-7129 CVE-2016-7130 CVE-2016-7131 CVE-2016-7132 CVE-2016-7411 CVE-2016-7412 CVE-2016-7413 CVE-2016-7414 CVE-2016-7416 CVE-2016-7417 CVE-2016-7418 CVE-2016-7478 CVE-2016-9934 CVE-2016-9935 CVE-2016-10158 CVE-2016-10159 CVE-2016-10160 CVE-2016-10161 CVE-2017-7272) (Bug 42987).
  - ***nss*** (CVE-2016-9074 CVE-2017-5461 CVE-2017-5462 CVE-2017-7502) (Bug 42858).
  - ***ghostscript*** (CVE-2013-5653 CVE-2015-3228 CVE-2016-7976 CVE-2016-7977 CVE-2016-7978 CVE-2016-7979 CVE-2016-8602 CVE-2016-10219 CVE-2016-10220 CVE-2017-5951 CVE-2017-8291) (Bug 39423).
  - ***libxml2*** (CVE-2016-4658 CVE-2016-5131) (Bug 42892).
  - ***wget*** (CVE-2016-4971 CVE-2017-6508) (Bug 41662).
  - ***samba*** (CVE-2017-11103) (Bug 44983).
  - ***openjdk-7*** (CVE-2016-3458 CVE-2016-3500 CVE-2016-3508 CVE-2016-3550 CVE-2016-3606 CVE-2016-5542 CVE-2016-5554 CVE-2016-5573 CVE-2016-5582 CVE-2016-5597 CVE-2017-3272 CVE-2017-3289 CVE-2017-3241 CVE-2017-3260 CVE-2016-5546 CVE-2017-3253 CVE-2016-5548 CVE-2016-5549 CVE-2017-3252 CVE-2016-5552 CVE-2016-5547 CVE-2017-3261 CVE-2017-3231 CVE-2016-2183) (Bug 41871).
  - ***vim*** (CVE-2016-1248 CVE-2017-5953 CVE-2017-6349 CVE-2017-6350 CVE-2017-11109) (Bug 43111).
  - ***libxslt*** (CVE-2016-4738 CVE-2017-5029) (Bug 42890).
  - ***libupnp*** (CVE-2016-8863) (Bug 43219).
  - ***unzip*** (CVE-2014-9636 CVE-2014-9913 CVE-2015-7696 CVE-2015-7697 CVE-2016-9844) (Bug 37657).
  - ***heimdal*** (CVE-2017-11103) (Bug 44985).

- ***dnsmasq*** (CVE-2015-3294 CVE-2017-14491 CVE-2017-14492 CVE-2017-14494) (Bug 38379).
- ***samba*** (CVE-2016-2123 CVE-2016-2125 CVE-2016-2126) (Bug 43132 Bug 43144 Bug 43176).
- ***univention-kernel-image*** (CVE-2016-7042 CVE-2015-1350 CVE-2015-8709 CVE-2015-8956 CVE-2016-6213 CVE-2016-7039 CVE-2016-7097 CVE-2016-7425 CVE-2016-8399 CVE-2016-8632 CVE-2016-8655 CVE-2016-8633 CVE-2016-9178 CVE-2016-9588 CVE-2016-10088 CVE-2016-10147 CVE-2017-2583 CVE-2017-2584 CVE-2017-5551) (Bug 42754).
- ***postgresql-9.1*** (CVE-2017-7486 CVE-2017-7546 CVE-2017-7547) (Bug 45236).
- ***univention-kernel-image*** (CVE-2017-6951 CVE-2017-7187 CVE-2017-7261 CVE-2017-7294 CVE-2017-7472 CVE-2017-7618 CVE-2017-7645 CVE-2016-10229 CVE-2016-2188 CVE-2016-8405 CVE-2016-9191 CVE-2016-9604 CVE-2017-5549 CVE-2017-5669 CVE-2017-7273 CVE-2017-8924 CVE-2017-8925) (Bug 44706).
- ***samba*** (CVE-2017-2619) (Bug 43678).
- ***mysql-5.5*** (CVE-2016-5584 CVE-2016-7440) (Bug 42875).
- ***qemu-kvm*** (CVE-2016-3710 CVE-2016-3712 CVE-2016-2857 CVE-2016-4439 CVE-2016-6351 CVE-2015-5239 CVE-2016-4020 CVE-2016-5403 CVE-2016-7116 CVE-2016-7161 CVE-2016-7170 CVE-2016-7908 CVE-2016-8576 CVE-2016-8577 CVE-2016-8578 CVE-2016-8669 CVE-2016-7909 CVE-2016-8909 CVE-2016-8910 CVE-2016-9101 CVE-2016-9102 CVE-2016-9103 CVE-2016-9104 CVE-2016-9105 CVE-2016-9106) (Bug 40920).
- ***imagemagick*** (CVE-2016-10144 CVE-2016-10145 CVE-2016-10146 CVE-2016-8677 CVE-2017-5506 CVE-2017-5507 CVE-2017-5508 CVE-2017-5510 CVE-2017-5511 CVE-2017-6498 CVE-2017-6500 CVE-2017-7606 CVE-2017-7619 CVE-2014-9841 CVE-2015-8900 CVE-2015-8901 CVE-2015-8902 CVE-2015-8903 CVE-2017-7941 CVE-2017-7943 CVE-2017-8343 CVE-2017-8344 CVE-2017-8345 CVE-2017-8346 CVE-2017-8347 CVE-2017-8348 CVE-2017-8349 CVE-2017-8350 CVE-2017-8351 CVE-2017-8352 CVE-2017-8353 CVE-2017-8354 CVE-2017-8355 CVE-2017-8356 CVE-2017-8357 CVE-2017-8765 CVE-2017-8830 CVE-2017-9098 CVE-2017-9141 CVE-2017-9142 CVE-2017-9143 CVE-2017-9144 CVE-2017-9261 CVE-2017-9262 CVE-2017-9405 CVE-2017-9407 CVE-2017-9409 CVE-2017-9439 CVE-2017-9500 CVE-2017-9501 CVE-2017-10995 CVE-2017-11166 CVE-2017-11352 CVE-2017-11360 CVE-2017-11446 CVE-2017-11448 CVE-2017-11449 CVE-2017-11450 CVE-2017-11478 CVE-2017-11505 CVE-2017-11523 CVE-2017-11524 CVE-2017-11525 CVE-2017-11526 CVE-2017-11527 CVE-2017-11528 CVE-2017-11529 CVE-2017-11530 CVE-2017-11531 CVE-2017-11532 CVE-2017-11533 CVE-2017-11534 CVE-2017-11535 CVE-2017-11537 CVE-2017-11539 CVE-2017-11639 CVE-2017-11640 CVE-2017-11644 CVE-2017-11724 CVE-2017-11751 CVE-2017-11752 CVE-2017-12140 CVE-2017-12418 CVE-2017-12427 CVE-2017-12428 CVE-2017-12429 CVE-2017-12430 CVE-2017-12431 CVE-2017-12432 CVE-2017-12433 CVE-2017-12435 CVE-2017-12563 CVE-2017-12564 CVE-2017-12565 CVE-2017-12566 CVE-2017-12587 CVE-2017-12640 CVE-2017-12641 CVE-2017-12642 CVE-2017-12643 CVE-2017-12654 CVE-2017-12664 CVE-2017-12665 CVE-2017-12668 CVE-2017-12670 CVE-2017-12674 CVE-2017-12675 CVE-2017-12676 CVE-2017-12877 CVE-2017-12983 CVE-2017-13133 CVE-2017-13134 CVE-2017-13139 CVE-2017-13142 CVE-2017-13143 CVE-2017-13144 CVE-2017-13146 CVE-2017-13658 CVE-2017-10928 CVE-2017-11141 CVE-2017-11170 CVE-2017-11188 CVE-2017-12691 CVE-2017-12692 CVE-2017-12693 CVE-2017-12875 CVE-2017-13758 CVE-2017-13768 CVE-2017-13769 CVE-2017-14060 CVE-2017-14172 CVE-2017-14173 CVE-2017-14174 CVE-2017-14175 CVE-2017-14224 CVE-2017-14249 CVE-2017-14341 CVE-2017-14400 CVE-2017-14505 CVE-2017-14607 CVE-2017-14682 CVE-2017-14739 CVE-2017-14741 CVE-2017-14989 CVE-2017-15016 CVE-2017-15017

CVE-2017-15277 CVE-2017-15281 CVE-2014-8354 CVE-2014-8355 CVE-2014-8562 CVE-2014-8716 CVE-2016-10062) (Bug 43448).

- ***freetype*** (CVE-2014-9674 CVE-2014-9745 CVE-2014-9746 CVE-2014-9747 CVE-2016-10244 CVE-2016-10328) (Bug 40548).
- ***python-imaging*** (CVE-2016-0775 CVE-2016-2533 CVE-2016-9189 CVE-2016-9190) (Bug 37067).
- ***bash*** (CVE-2016-7543) (Bug 42874).
- ***expat*** (CVE-2012-6702 CVE-2015-1283 CVE-2016-0718 CVE-2016-5300) (Bug 39421).
- ***qemu*** (CVE-2016-9911 CVE-2016-9921 CVE-2016-9922 CVE-2017-2620 CVE-2017-2615 CVE-2017-5973 CVE-2017-5898) (Bug 43359).
- ***qemu*** (CVE-2016-3710 CVE-2016-3712 CVE-2016-2857 CVE-2016-4439 CVE-2016-6351 CVE-2015-5239 CVE-2016-4020 CVE-2016-5403 CVE-2016-7116 CVE-2016-7161 CVE-2016-7170 CVE-2016-7908 CVE-2016-8576 CVE-2016-8577 CVE-2016-8578 CVE-2016-8669 CVE-2016-7909 CVE-2016-8909 CVE-2016-8910 CVE-2016-9101 CVE-2016-9102 CVE-2016-9103 CVE-2016-9104 CVE-2016-9105 CVE-2016-9106) (Bug 40920).
- ***nspr*** (CVE-2016-1951) (Bug 41565).
- ***libevent*** (CVE-2016-10195 CVE-2016-10196 CVE-2016-10197) (Bug 43552).
- ***postgresql-9.1*** (CVE-2015-5288 CVE-2016-0766 CVE-2016-0773 CVE-2016-5423 CVE-2016-5424) (Bug 40717).
- ***asterisk*** (CVE-2011-3389 CVE-2015-3008 CVE-2016-2232 CVE-2016-2316 CVE-2016-7551 CVE-2016-9938 CVE-2017-14099 CVE-2017-14100 CVE-2017-14603) (Bug 40975).
- ***openldap*** (CVE-2017-9287) (Bug 44732).
- ***mysql-5.5*** (CVE-2017-3635 CVE-2017-3636 CVE-2017-3641 CVE-2017-3648 CVE-2017-3651 CVE-2017-3652 CVE-2017-3653) (Bug 45106).
- ***linux*** (CVE-2017-6951 CVE-2017-7187 CVE-2017-7261 CVE-2017-7294 CVE-2017-7472 CVE-2017-7618 CVE-2017-7645 CVE-2016-10229 CVE-2016-2188 CVE-2016-8405 CVE-2016-9191 CVE-2016-9604 CVE-2017-5549 CVE-2017-5669 CVE-2017-7273 CVE-2017-8924 CVE-2017-8925) (Bug 44706).
- ***tiff3*** (CVE-2015-7554 CVE-2016-5318 CVE-2015-8781 CVE-2015-8782 CVE-2015-8783 CVE-2015-8784 CVE-2016-9533 CVE-2016-9534 CVE-2016-9535) (Bug 42897).
- ***icu*** (CVE-2015-2632 CVE-2015-4844 CVE-2016-0494 CVE-2016-6293 CVE-2014-9911 CVE-2016-7415) (Bug 41952).
- ***samba*** (CVE-2017-12150 CVE-2017-12151 CVE-2017-12163) (Bug 45389).
- ***php5*** (CVE-2015-7803 CVE-2015-7804 CVE-2015-8865 CVE-2015-8866 CVE-2015-8878 CVE-2015-8879 CVE-2016-4070 CVE-2016-4071 CVE-2016-4072 CVE-2016-4073 CVE-2016-4343 CVE-2016-4537 CVE-2016-4539 CVE-2016-4541 CVE-2016-4544 CVE-2016-5093 CVE-2016-5095 CVE-2016-5096 CVE-2016-4473 CVE-2016-4538 CVE-2016-5114 CVE-2016-5399 CVE-2016-5768 CVE-2016-5769 CVE-2016-5770 CVE-2016-5771 CVE-2016-5772 CVE-2016-5773 CVE-2016-6288 CVE-2016-6289 CVE-2016-6290 CVE-2016-6291 CVE-2016-6292 CVE-2016-6294 CVE-2016-6295 CVE-2016-6296 CVE-2016-6297) (Bug 40918).

- ***samba*** (CVE-2017-7494) (Bug 44613).
- ***squid3*** (CVE-2016-2571 CVE-2016-4051 CVE-2016-4052 CVE-2016-4053 CVE-2016-4054 CVE-2016-4554 CVE-2016-4555 CVE-2016-4556) (Bug 40834).
- ***openssl*** (CVE-2016-7055 CVE-2016-8610 CVE-2017-3731 CVE-2017-3732) (Bug 42925).
- ***linux*** (CVE-2016-7042 CVE-2015-1350 CVE-2015-8709 CVE-2015-8956 CVE-2016-6213 CVE-2016-7039 CVE-2016-7097 CVE-2016-7425 CVE-2016-8399 CVE-2016-8632 CVE-2016-8655 CVE-2016-8633 CVE-2016-9178 CVE-2016-9588 CVE-2016-10088 CVE-2016-10147 CVE-2017-2583 CVE-2017-2584 CVE-2017-5551) (Bug 42754).
- ***tar*** (CVE-2016-6321) (Bug 42893).
- ***memcached*** (CVE-2016-8704 CVE-2016-8705 CVE-2016-8706) (Bug 42836).
- ***bind9*** (CVE-2016-9131 CVE-2016-9147 CVE-2016-9444) (Bug 43362 Bug 28748).
- ***qemu-kvm*** (CVE-2016-9911 CVE-2016-9921 CVE-2016-9922 CVE-2017-2620 CVE-2017-2615 CVE-2017-5973 CVE-2017-5898) (Bug 43360).
- ***ntp*** (CVE-2016-1547 CVE-2016-1548 CVE-2016-1550 CVE-2016-2516 CVE-2016-2518) (Bug 40770).
- ***bind9*** (CVE-2016-2848 CVE-2016-8864) (Bug 42747).
- ***imagemagick*** (CVE-2016-4563 CVE-2014-9805 CVE-2014-9806 CVE-2014-9807 CVE-2014-9808 CVE-2014-9809 CVE-2014-9810 CVE-2014-9811 CVE-2014-9812 CVE-2014-9813 CVE-2014-9814 CVE-2014-9815 CVE-2014-9816 CVE-2014-9817 CVE-2014-9818 CVE-2014-9819 CVE-2014-9821 CVE-2014-9822 CVE-2014-9823 CVE-2014-9824 CVE-2014-9826 CVE-2014-9828 CVE-2014-9829 CVE-2014-9830 CVE-2014-9831 CVE-2014-9832 CVE-2014-9833 CVE-2014-9834 CVE-2014-9835 CVE-2014-9836 CVE-2014-9837 CVE-2014-9838 CVE-2014-9839 CVE-2014-9840 CVE-2014-9843 CVE-2014-9844 CVE-2014-9845 CVE-2014-9846 CVE-2014-9847 CVE-2014-9848 CVE-2014-9849 CVE-2014-9851 CVE-2014-9853 CVE-2014-9854 CVE-2014-9907 CVE-2015-8957 CVE-2015-8958 CVE-2015-8959 CVE-2016-4562 CVE-2016-4564 CVE-2016-5010 CVE-2016-5687 CVE-2016-5688 CVE-2016-5689 CVE-2016-5690 CVE-2016-5691 CVE-2016-5841 CVE-2016-5842 CVE-2016-6491 CVE-2016-6823 CVE-2016-7101 CVE-2016-7514 CVE-2016-7515 CVE-2016-7516 CVE-2016-7517 CVE-2016-7518 CVE-2016-7519 CVE-2016-7520 CVE-2016-7521 CVE-2016-7522 CVE-2016-7523 CVE-2016-7524 CVE-2016-7526 CVE-2016-7527 CVE-2016-7528 CVE-2016-7529 CVE-2016-7530 CVE-2016-7531 CVE-2016-7532 CVE-2016-7533 CVE-2016-7534 CVE-2016-7535 CVE-2016-7536 CVE-2016-7537 CVE-2016-7538 CVE-2016-7539 CVE-2016-8707 CVE-2016-8862 CVE-2016-8866 CVE-2016-9556 CVE-2016-7799) (Bug 41663).
- ***python-pysaml2*** (CVE-2016-10127) (Bug 43393).
- ***nagios3*** (CVE-2014-1878 CVE-2016-9565 CVE-2016-9566) (Bug 37088).
- ***openssl*** (CVE-2016-2182) (Bug 42961).
- ***mysql-5.5*** (CVE-2017-3238 CVE-2017-3243 CVE-2017-3244 CVE-2017-3258 CVE-2017-3265 CVE-2017-3291 CVE-2017-3312 CVE-2017-3313 CVE-2017-3317 CVE-2017-3318) (Bug 43380).
- ***univention-kernel-image-signed*** (CVE-2016-7042 CVE-2015-1350 CVE-2015-8709 CVE-2015-8956 CVE-2016-6213 CVE-2016-7039 CVE-2016-7097 CVE-2016-7425 CVE-2016-8399 CVE-2016-8632 CVE-2016-8655 CVE-2016-8633 CVE-2016-9178 CVE-2016-9588 CVE-2016-10088 CVE-2016-10147 CVE-2017-2583 CVE-2017-2584 CVE-2017-5551) (Bug 42754).

- ***libav*** (CVE-2014-7933 CVE-2014-8541 CVE-2014-8543 CVE-2014-8544 CVE-2014-8545 CVE-2014-8546 CVE-2014-8547 CVE-2014-8548 CVE-2014-9603 CVE-2014-9604 CVE-2014-9676 CVE-2015-1872 CVE-2015-5479 CVE-2015-8365 CVE-2016-1897 CVE-2016-1898 CVE-2016-2326 CVE-2016-3062 CVE-2016-7393 CVE-2016-7424 CVE-2016-9819 CVE-2016-9820 CVE-2016-9821 CVE-2016-9822 CVE-2017-7208 CVE-2017-7862 CVE-2017-9992) (Bug 37024).

6.2. Basic system services

Feedback

6.2.1. Univention Configuration Registry

Feedback

- The functionality to manage services has been changed to ignore processes running in a Docker container (Bug 40659).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- OpenLDAP has been re-built to make it Multi-Arch-aware (Bug 41558).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- Some help dialogs in the UMC where not displayed correctly. This has been fixed (Bug 43084).
- The maximum request size can now be configured via the Univention Configuration Registry variable `umc/http/max_request_body_size` (Bug 42357).
- The login dialog after a session timeout is now centered on the view-port and not at the top of the page. Making the login immediately possible without the need to scroll to the top (Bug 40492).
- The UMC overview page shows a banner that links to the Univention Summit website (Bug 42979).
- Erroneous pop-ups when clicking a non UMC module link on the overview page are no longer generated (Bug 42980).

6.4.2. Univention App Center

Feedback

- The App Center now uses a different directory for special temporary files for Docker Apps to avoid problems with the ***sysvinit***'s `tmp` cleanup (Bug 44387).
- Notifications about App updates of Docker Apps were not sent. This has been corrected (Bug 44148).
- When an App sets it HTTP port to 0, disable the HTTP link for the App Center link and for the `ucs-overview` link (Bug 43657).
- A bug in detecting apps on domain hosts has been fixed (Bug 41801).
- Docker Apps now support UDP ports to be opened (Bug 43108).
- In case the App Center runs in container mode, join scripts etc. are not copied to the system (Bug 42934).
- The backend now correctly determines whether an App is a UCS component (Bug 43363).

- Container passwords aren't changed anymore during container upgrades (Bug 45290).
- A script can now be run after configuring an App (Bug 43838).
- *AdditionalPackages* defined by the App are no longer removed when uninstalling an app (Bug 44772).
- The documentation has been extended (Bug 42761).
- Added the command `univention-app dev-set` to support development tools (Bug 43040).
- For developers, reverting a local App Center does remove the App Center directories completely (Bug 43074).
- When upgrading from a Non-Docker version to a Docker version, the old version was removed even the installation process of the new version was not successful (Bug 42969).
- The ini attribute *License* is now passed to the frontend (Bug 42798).
- Hiding dockerized versions of installed Apps did not work when upgrading from UCS 4.0 (Bug 43075).
- Adjust code so that other projects may extend the App Center lib (Bug 42834).
- Start App container with the hosts proxy settings by default (Bug 44785).
- If the download of App meta data via ***zsync*** fails, the archive is downloaded via an HTTPS request (Bug 45291).
- Fixed the utility function for creating LDAP objects not honoring existing objects (Bug 42928).
- When trying to upgrade to a Docker version of a formerly Non-Docker App, a link to a migration guide is shown if available (Bug 43038).
- Admin credentials are now passed to a `preinst` script during App installation / upgrade (Bug 44655).
- App Logos are linked to the UMC front-end immediately after the initial System setup (Bug 45748).

6.4.3. Univention Directory Manager UMC modules and command line interface

Feedback

- The Python API for UDM modules finds the superordinate object automatically if it is not given (Bug 43423).
- An error was fixed that prevented syntax classes which were set via Univention Configuration Registry to be used with a `ComboBox` widget (Bug 43094).
- If a user template defined a default value for *mailHomeServer*, the value has not been set. This has been fixed (Bug 42903).
- UDM objects with the object flags synced and docker can now be deleted (Bug 44954).
- Add missing dependency ***python-univention-license*** to fix error when using the `univention.admin.license` Python module (Bug 43298).
- Removing objects which don't have sub-elements is now possible even if the LDAP admin size limit is reached (Bug 43236).
- Objects underneath containers of superordinate entries like DHCP services are shown again in the tree view (Bug 43048).

- Fixed a regression in UCS 4.1-3 Erratum 319 which caused failures in the Asterisk4UCS App module (Bug 43423).

6.4.4. Modules for system settings / setup wizard

Feedback

- DNS settings are updated correctly when using app appliances (Bug 42944).
- The screen-saver is now deactivated while configuring the system (Bug 42944).
- Install ***univention-welcome-screen*** earlier in the setup process (Bug 42915).

6.4.5. Univention Directory Reports

Feedback

- The Univention Directory Reports created via the UMC are now access protected (Bug 45680).

6.4.6. License module

Feedback

- A fallback to the machine account has been added to `univention_license_ldap_init()` (Bug 35157).

6.4.7. Software update module

Feedback

- The updater message for UCS releases that receive extended maintenance was clarified (Bug 45671).

6.4.8. Policies

Feedback

- LDAP connections are now always TLS encrypted (Bug 43031).

6.5. Software deployment

Feedback

- The Updater has been adapted for UCS 4.1-5 (Bug 45648).
- The user-agent string has been extended with statistics (Bug 43107).

6.6. System services

Feedback

6.6.1. Mail services

Feedback

- The package dependencies allow now to install Dovecot Pro instead of Dovecot from the Debian repositories (Bug 44567).
- LDAP queries are now escaped correctly, when checking access for a restricted mailing list (Bug 41055).

6.6.2. SSL

Feedback

- The local system SSL certificates are correctly regenerated during system join (Bug 44322).
- The command `sign` has been added to `univention-certificate` to allow creating certificates for external Certificate Signing Requests (Bug 22085).
- The local system SSL certificates are correctly regenerated when refreshing certificates (Bug 44322).

6.6.3. Proxy services

Feedback

- The Squid proxy server now uses STARTTLS to encrypt all LDAP connections (Bug #43675) (Bug 43675).

- Univention Configuration Registry variables `squid/cache/format`, `squid/cache/directory`, `squid/cache/size`, `squid/cache/l1_size`, `squid/cache/l2_size` to configure the cache settings have been added (Bug 37381).

6.6.4. Apache

Feedback

- Exceptions for the `apache2/force_https` configuration can now be configured via Univention Configuration Registry. When `apache2/force_https` is enabled, by default `localhost` will be excluded (Bug 43603).

6.7. Virtualization

Feedback

6.7.1. Univention Virtual Machine Manager (UVMM)

Feedback

- In some cases during live migration the KVM clock is not monotone, which leads to the virtual machine being stuck until the clock has caught up again. This has been fixed (Bug 45117).

6.8. Container Technologies

Feedback

- Allow release update in container mode even if the UCS master's version is lower (Bug 42923).
- Install package updates when updating the app in container mode (Bug 43177).
- Restoring Univention Configuration Registry in container mode after an image exchange has been fixed (Bug 43324).

6.9. Services for Windows

Feedback

6.9.1. Samba

Feedback

- The Univention Configuration Registry variables `samba/client/min/protocol`, `samba/min/protocol` and `samba/client/max/protocol` have been added. Please be aware that raising `samba/min/protocol` e.g. to SMB2 also requires raising `samba/client/max/protocol` to that value or higher (Bug 44646).
- Samba 4.5 creates an DNS object `_msdcs` below the position `CN=MicrosoftDNS,CN=System`. If `CN=System` is still used by BIND9, the DRS replication will be stopped. This can only happen if Samba 4 was installed before UCS 4.0-4 and a Samba 4 system is installed or rejoined. This update removes the created DNS object and prevented its recreation (Bug 43288).

6.9.2. Univention S4 Connector

Feedback

- A race condition between writing and reading cached data has been fixed (Bug 43235).
- The mapping for LDAP attributes of DNS objects is now case insensitive (Bug 43259).
- The synchronization of DNS zones now also works in special setups, where `samba4/ldap/base` differs from `ldap/base` (Bug 42393).
- When adjusting a GPO security filter via Group Policy Management Console repeatedly in a short time, the S4-Connector could revert changes, depending on timing. Now the S4-Connector checks if a change has happened in Samba/AD since the last sync and avoids overwriting the attribute *nTSecurityDescriptor* in that case (Bug 41571).

- The init-script has been fixed to check for an already running instance of the S4 connector. The PID file is removed on shutdown. The `status` action has been added, too (Bug 40659).
- An issue with renaming windows clients has been fixed (Bug 43321).
- 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 44291).
- Fix handling of `Printer-Admins` and searching for conflicting deleted objects by *objectsid* (Bug 44289).
- Added new Univention Configuration Registry variables `connector/s4/mapping/{gpo,wmifilter,msprintconnectionpolicy}/syncmode` (Bug 43629).
- UCS@school specific settings have been moved into the join script (Bug 45329).
- Sync client initiated renaming of Windows machine accounts from Samba/AD to OpenLDAP (Bug 37388).
- DNs of Windows clients joined from the client itself where not in sync with the corresponding OpenLDAP DNs (Bug 40435).

6.9.3. Univention Active Directory Connection

Feedback

- The AD-Connector can now handle *sync_mode* configuration on a per attribute granularity (Bug 42618).
- The LDAP modification list can now be logged in case of a trace-back if the changes are synchronized from UCS to Active Directory (Bug 29988).
- The *samAccountName* synchronization for Windows clients has been set to write only because a changed *samAccountName* attribute in Active Directory is handled via the *CN* synchronization (Bug 43229).
- The lookup for the LDAP base DN of the Active Directory server has been fixed (Bug 40816).
- The mapping for the MS-Exchange related attribute *proxyAddresses* has been revised to synchronize the OpenLDAP attribute *mailPrimaryAddress* with the default value configured in *proxyAddresses* (Bug 43216). In detail:

  1. When reading from Active Directory, the value with `SMTP:` prefix is now written to the OpenLDAP attribute *mailPrimaryAddress*. Before this update *mailPrimaryAddress* used to be synchronized with the value of the Active Directory *mail* attribute instead. The Active Directory *mail* attribute has informative character.
  2. In the other direction, i.e. writing from OpenLDAP to Active Directory, the value of *mailPrimaryAddress* continues to be written to the *mail* attribute and now additionally gets written into the *proxyAddresses* as default value, i.e. prefixed with `SMTP:`.
  3. `smtp:` prefixed values in *proxyAddresses* continue to be synchronized with OpenLDAP *mailAlternativeAddress*

- A race condition between writing and reading cached data has been fixed (Bug 42507).

6.10. Other changes

Feedback

- Add missing `INIT INFO` headers in various packages to help the update to UCS 4.2 (Bug 45109,).
- New leap second 2016-12-31 23:59:60 UTC as per IERS Bulletin C 52 in ***tzdata*** (Bug 42877).

- The root SSL certificate used for the UCS domain is now registered as a trusted root certificate for all applications using `/etc/ssl/certs/` (Bug 39179).
- Joining a UCS system into a domain now works for hostnames, where the corresponding host LDAP entry was created using a different casing (Bug 39068).
- Redirect warning messages to `join.log` in `univention-join` (Bug 43381).
- The ***syslog*** configuration has been extended to allow logging to remote hosts. Several protocols are supported:
  UDP fast, but messages can get lost or get dropped in congested networks.
  TCP more reliable, but can block the sending syslog daemon.
  RELP reliable, but non standard; can also block the syslog daemon.

  Sending must be enabled explicitly. For this the new Univention Configuration Registry variables `syslog/remote`, `syslog/remote/fallback` and `syslog/remote/selector` have been added. Receiving must also be enabled explicitly. For this the new Univention Configuration Registry variables `syslog/input/udp`, `syslog/input/tdp` and `syslog/input/relp` have been added. Please note, that log messages are sent unencrypted and in clear text! It is recommended to use this only in protected networks, as passwords and other sensitive data might leak otherwise (Bug 15728).
- The configuration for ***logrotate*** has been extended to allow a file-by-file configuration through the Univention Configuration Registry variables `logrotate/$facility/...`. All remaining files are handled by `logroate/syslog-other/...` (Bug 41816).
- Several new Univention Configuration Registry variables `syslog/...` have been added to enable/disable logging of events of certain facilities to the corresponding targets:

  `syslog/auth` `/var/log/auth.log`

  `syslog/cron` `/var/log/cron.log`

  `syslog/kern` `/var/log/kern.log`

  `syslog/daemon` `/var/log/daemon.log`

  `syslog/user` `/var/log/user.log`

  `syslog/lpr` `/var/log/lpr.log`

  `syslog/mail` `/var/log/mail.*`

  `syslog/news` `/var/log/news.*`

  `syslog/syslog` `/var/log/syslog` (catch-all for all messages)

  `syslog/debug` `/var/log/debug` (only debug messages)

  `syslog/messages` `/var/log/messages` (all except debug and errors)

  `syslog/xconsole` `/dev/xconsole` (used by graphical console)

  The new Univention Configuration Registry variable `syslog/syslog/avoid_duplicate_messages` can be used to remove messages logged to other targets from `/var/log/syslog`. By default messages get logged multiple times. Further more the selector for certain files can now be customized through the following new Univention Configuration Registry variables: (Bug 41815).
  `syslog/syslog/selector` `[*.*]`

```
syslog/debug/selector     [*.=debug;auth,authpriv,news,mail.none]
syslog/messages/selector  [*.=info-
                          warn;auth;authpriv;cron;daemon;mail;news.none]
syslog/xconsole/selector  [daemon,mail.*;news.err;*.debug-warn]
```