univention
be open.

UCS 4.4 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.4-8

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2020 Univention GmbH

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

<feedback@univention.de>

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

univention
be open.

Inhaltsverzeichnis

1. Release-Highlights 4
2. Hinweise zum Update 5
    2.1. Empfohlene Update-Reihenfolge 5
    2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante 5
3. Vorbereitung des Updates 6
4. Nachbereitung des Updates 7
5. Hinweise zum Einsatz einzelner Pakete 8
    5.1. Erfassung von Nutzungsstatistiken 8
    5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit 8
    5.3. Empfohlene Browser für den Zugriff auf Univention Management Console 8
6. Changelog 9
    6.1. General 9
    6.2. Basic system services 12
        6.2.1. Univention Configuration Registry 12
            6.2.1.1. Changes to templates and modules 12
        6.2.2. Boot Loader 12
    6.3. Domain services 12
        6.3.1. OpenLDAP 12
            6.3.1.1. Listener/Notifier domain replication 12
    6.4. Univention Management Console 12
        6.4.1. Univention Management Console web interface 12
        6.4.2. Univention Portal 13
        6.4.3. Univention Management Console server 13
        6.4.4. Univention App Center 13
        6.4.5. Univention Directory Manager UMC modules and command line interface 14
        6.4.6. Other modules 14
    6.5. Software deployment 14
    6.6. System services 14
        6.6.1. Docker 14
        6.6.2. SAML 15
        6.6.3. Univention self service 15
        6.6.4. Postfix 15
        6.6.5. Spam/virus detection and countermeasures 15
        6.6.6. Printing services 15
        6.6.7. Nagios 15
        6.6.8. Apache 15
        6.6.9. Proxy services 15
        6.6.10. Kerberos 15
        6.6.11. Other services 16
    6.7. Virtualization 16
        6.7.1. UCS Virtual Machine Manager (UVMM) 16
    6.8. Services for Windows 16
        6.8.1. Univention S4 Connector 16
        6.8.2. Univention Active Directory Connection 16
    6.9. Other changes 16

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.4-8 steht das achte Point-Release für Univention Corporate Server (UCS) 4.4 zur Verfügung. Es umfasst Funktionserweiterungen und Verbesserungen, neue Eigenschaften sowie diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Die Performance des UMC Webservers in großen Umgebungen mit vielen Anfragen wurde verbessert, indem der Webserver mit mehreren Prozessen gestartet werden kann, um mehrere CPU Kerne zu nutzen. Hierfür wurde der UMC Webserver von *single-* auf *multiprocessing* umgestellt. Die Anzahl der Prozesse ist konfigurierbar.

- Diverse Verbesserungen wurden in Vorbereitung auf UCS 5.0 vorgenommen. Unter anderem wird das UCS Upgrade blockiert, wenn installierte Apps unter UCS 5.0 noch nicht verfügbar sind.

- Der S4 Connector synchronisiert nun auch das Attribut `gidNumber` für Gruppenobjekte.

- Diverse Security Updates wurden in UCS 4.4-8 integriert, bspw. für PostgreSQL, Samba, den Linux Kernel und MariaDB.

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.

Univention bietet ein Skript an, mit dem Probleme, die das Update des UCS Systems verhindern würden, schon vor dem Update erkannt werden können. Dieses Skript kann vor dem Update manuell auf das System geladen und ausgeführt werden:

```
# download
curl -OOs https://updates.software-univention.de/download/univention-
update-checks/pre-update-checks-4.4{,.gpg}

# run script
gpgv --keyring /usr/share/keyrings/univention-archive-key-ucs-4x.gpg
 pre-update-checks-4.4.gpg \
        pre-update-checks-4.4 && bash pre-update-checks-4.4

...

Starting pre-update checks ...

Checking app_appliance ...                          OK
Checking block_update_of_NT_DC ...                  OK
Checking cyrus_integration ...                      OK
Checking disk_space ...                             OK
Checking hold_packages ...                          OK
Checking ldap_connection ...                        OK
Checking ldap_schema ...                            OK
...
```

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 71
- Firefox ab Version 60
- Safari und Safari Mobile ab Version 12
- Microsoft Edge ab Version 18

Der Internet Explorer wird ab diesem Release nicht mehr von Univention Management Console unterstützt.

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 *4.4-7*:

6.1. General

Feedback

- All security updates issued for UCS 4.4-7 are included:
  - ***apt*** (CVE-2020-27350) (Bug 52486)
  - ***bind9*** (CVE-2020-8625) (Bug 52819)
  - ***busybox*** (CVE-2011-5325 CVE-2015-9261 CVE-2016-2147 CVE-2016-2148 CVE-2017-15873 CVE-2017-16544 CVE-2018-1000517 CVE-2021-28831) (Bug 52804 Bug 53037)
  - ***cairo*** (CVE-2020-35492) (Bug 52548)
  - ***cloud-init*** (CVE-2021-3429) (Bug 52969)
  - ***curl*** (CVE-2020-8284 CVE-2020-8285 CVE-2020-8286) (Bug 52529)
  - ***dnsmasq*** (Bug 53001)
  - ***dovecot*** (CVE-2020-24386 CVE-2020-25275) (Bug 52550)
  - ***ffmpeg*** (Bug 52730)
  - ***firefox-esr*** (CVE-2020-16042 CVE-2020-16044 CVE-2020-26971 CVE-2020-26973 CVE-2020-26974 CVE-2020-26976 CVE-2020-26978 CVE-2020-35111 CVE-2020-35113 CVE-2021-23953 CVE-2021-23954 CVE-2021-23960 CVE-2021-23964 CVE-2021-23968 CVE-2021-23969 CVE-2021-23973 CVE-2021-23978 CVE-2021-23981 CVE-2021-23982 CVE-2021-23984 CVE-2021-23987) (Bug 52528 Bug 52571 Bug 52752 Bug 52858 Bug 52998)
  - ***flac*** (CVE-2017-6888 CVE-2020-0499) (Bug 52543)
  - ***gdisk*** (CVE-2020-0256 CVE-2021-0308) (Bug 52793)
  - ***gst-plugins-bad1.0*** (CVE-2021-3185) (Bug 52685)
  - ***imagemagick*** (CVE-2017-14528 CVE-2020-19667 CVE-2020-25665 CVE-2020-25666 CVE-2020-25674 CVE-2020-25675 CVE-2020-25676 CVE-2020-27560 CVE-2020-27750 CVE-2020-27754 CVE-2020-27757 CVE-2020-27758 CVE-2020-27759 CVE-2020-27760 CVE-2020-27761 CVE-2020-27762 CVE-2020-27763 CVE-2020-27764 CVE-2020-27765 CVE-2020-27766 CVE-2020-27767 CVE-2020-27768 CVE-2020-27769 CVE-2020-27770 CVE-2020-27771 CVE-2020-27772 CVE-2020-27773 CVE-2020-27774 CVE-2020-27775 CVE-2020-29599 CVE-2021-20176 CVE-2021-20241 CVE-2021-20244 CVE-2021-20246) (Bug 52664 Bug 52999)
  - ***intel-microcode*** (CVE-2020-8695 CVE-2020-8696 CVE-2020-8698) (Bug 52754)
  - ***jquery*** (CVE-2020-11022 CVE-2020-11023) (Bug 53000)
  - ***ldb*** (CVE-2020-27840 CVE-2021-20277) (Bug 52916)
  - ***libbsd*** (CVE-2019-20367) (Bug 52822)

- ***libcaca*** (CVE-2021-3410) (Bug 52908)
- ***libebml*** (CVE-2021-3405) (Bug 53121)
- ***libsdl2*** (CVE-2019-7575 CVE-2019-7577 CVE-2019-7578 CVE-2019-7635 CVE-2019-7636 CVE-2019-7638 CVE-2019-13616 CVE-2020-14409 CVE-2020-14410) (Bug 52728)
- ***libupnp*** (CVE-2020-13848) (Bug 52907)
- ***linux*** (CVE-2019-19318 CVE-2019-19813 CVE-2019-19816 CVE-2020-0427 CVE-2020-8694 CVE-2020-14351 CVE-2020-25645 CVE-2020-25656 CVE-2020-25668 CVE-2020-25669 CVE-2020-25704 CVE-2020-25705 CVE-2020-27673 CVE-2020-27675 CVE-2020-27815 CVE-2020-27825 CVE-2020-28374 CVE-2020-28974 CVE-2020-29568 CVE-2020-29569 CVE-2020-29660 CVE-2020-29661 CVE-2020-36158 CVE-2021-3178 CVE-2021-3347 CVE-2021-26930 CVE-2021-26931 CVE-2021-26932 CVE-2021-27363 CVE-2021-27364 CVE-2021-27365 CVE-2021-28038) (Bug 52549 Bug 52905)
- ***lxml*** (CVE-2018-19787 CVE-2020-27783 CVE-2021-28957) (Bug 52451 Bug 52531 Bug 52997)
- ***mariadb-10.1*** (CVE-2020-14765 CVE-2020-14812 CVE-2021-27928) (Bug 52729 Bug 52996)
- ***openexr*** (CVE-2020-16588 CVE-2020-16589) (Bug 52487)
- ***openjdk-8*** (CVE-2020-14779 CVE-2020-14781 CVE-2020-14782 CVE-2020-14792 CVE-2020-14796 CVE-2020-14797 CVE-2020-14798 CVE-2020-14803) (Bug 52533)
- ***openjpeg2*** (CVE-2020-27814 CVE-2020-27823 CVE-2020-27824 CVE-2020-27841 CVE-2020-27844 CVE-2020-27845) (Bug 52794)
- ***openldap*** (CVE-2020-25692 CVE-2020-25709 CVE-2020-25710 CVE-2020-36221 CVE-2020-36222 CVE-2020-36223 CVE-2020-36224 CVE-2020-36225 CVE-2020-36226 CVE-2020-36227 CVE-2020-36228 CVE-2020-36229 CVE-2020-36230 CVE-2021-27212) (Bug 52163 Bug 52406 Bug 52747)
- ***openssl*** (CVE-2020-1971 CVE-2021-23840 CVE-2021-23841) (Bug 52527 Bug 52826)
- ***openssl1.0*** (CVE-2020-1971 CVE-2021-23840 CVE-2021-23841) (Bug 52526 Bug 52823)
- ***p11-kit*** (CVE-2020-29361 CVE-2020-29362) (Bug 52542)
- ***php-pear*** (CVE-2020-36193) (Bug 53056)
- ***postgresql-9.6*** (CVE-2020-25694 CVE-2020-25695 CVE-2020-25696) (Bug 52461)
- ***pygments*** (CVE-2021-20270 CVE-2021-27291) (Bug 52906 Bug 52967)
- ***python-apt*** (CVE-2020-27351) (Bug 52490 Bug 52544)
- ***python-django*** (CVE-2021-3281 CVE-2021-23336 CVE-2021-28658) (Bug 52753 Bug 52824 Bug 53057)
- ***python-pysaml2*** (CVE-2017-1000433 CVE-2021-21239) (Bug 52857)
- ***python2.7*** (CVE-2019-16935 CVE-2021-23336) (Bug 53122)
- ***python3.5*** (CVE-2021-3177 CVE-2021-3426 CVE-2021-23336) (Bug 53040)

- ***qemu*** (Bug 52450 Bug 52820 Bug 53054)
- ***samba*** (CVE-2020-27840 CVE-2021-20277) (Bug 52916)
- ***screen*** (CVE-2021-26937) (Bug 52825)
- ***shadow*** (CVE-2017-12424 CVE-2017-20002) (Bug 52968)
- ***smarty3*** (CVE-2018-13982 CVE-2018-16831 CVE-2021-26119 CVE-2021-26120) (Bug 53041, Bug 53119)
- ***spamassassin*** (CVE-2020-1946) (Bug 53039)
- ***sqlite3*** (CVE-2019-20218) (Bug 52488)
- ***squid3*** (CVE-2020-15049 CVE-2020-15810 CVE-2020-15811 CVE-2020-24606 CVE-2020-25097) (Bug 52182 Bug 52966)
- ***sudo*** (CVE-2021-3156) (Bug 52704)
- ***underscore*** (CVE-2021-23358) (Bug 53038)
- ***univention-kernel-image*** (CVE-2019-19318 CVE-2019-19813 CVE-2019-19816 CVE-2020-27815 CVE-2020-27825 CVE-2020-28374 CVE-2020-29568 CVE-2020-29569 CVE-2020-29660 CVE-2020-29661 CVE-2020-36158 CVE-2021-3178 CVE-2021-3347 CVE-2021-26930 CVE-2021-26931 CVE-2021-26932 CVE-2021-27363 CVE-2021-27364 CVE-2021-27365 CVE-2021-28038) (Bug 52905)
- ***univention-kernel-image-signed*** (CVE-2019-19318 CVE-2019-19813 CVE-2019-19816 CVE-2020-0427 CVE-2020-8694 CVE-2020-14351 CVE-2020-25645 CVE-2020-25656 CVE-2020-25668 CVE-2020-25669 CVE-2020-25704 CVE-2020-25705 CVE-2020-27673 CVE-2020-27675 CVE-2020-27815 CVE-2020-27825 CVE-2020-28374 CVE-2020-28974 CVE-2020-29568 CVE-2020-29569 CVE-2020-29660 CVE-2020-29661 CVE-2020-36158 CVE-2021-3178 CVE-2021-3347 CVE-2021-26930 CVE-2021-26931 CVE-2021-26932 CVE-2021-27363 CVE-2021-27364 CVE-2021-27365 CVE-2021-28038) (Bug 52549 Bug 52905)
- ***wavpack*** (CVE-2018-19840 CVE-2018-19841 CVE-2019-11498 CVE-2019-1010315 CVE-2019-1010317 CVE-2019-1010319 CVE-2020-35738) (Bug 52663)
- ***wireshark*** (CVE-2019-12295 CVE-2019-13619 CVE-2019-16319 CVE-2019-19553 CVE-2020-7045 CVE-2020-9428 CVE-2020-9430 CVE-2020-9431 CVE-2020-11647 CVE-2020-13164 CVE-2020-15466 CVE-2020-25862 CVE-2020-25863 CVE-2020-26418 CVE-2020-26421 CVE-2020-26575 CVE-2020-28030) (Bug 52755)
- ***wpa*** (CVE-2021-0326 CVE-2021-27803) (Bug 52821 Bug 52903)
- ***xerces-c*** (CVE-2018-1311) (Bug 52530)
- ***xorg-server*** (CVE-2020-14360 CVE-2020-25712 CVE-2021-3472) (Bug 53118)
- ***xterm*** (CVE-2021-27135) (Bug 52796)
- ***zeromq3*** (CVE-2021-20234 CVE-2021-20235) (Bug 52904)

- The following updated packages from Debian 9.13 are included (Bug 53084): ***ca-certificates***, ***libdate-time-timezone-perl***, ***linux-latest***, ***tzdata***, ***activemq***, ***adminer***, ***ansible***, ***awstats***, ***brotli***, ***connman***, ***coturn***,

crmsh, ***csync2***, ***debian-security-support***, ***drupal7***, ***firejail***, ***golang-1.7***, ***golang-1.8***, ***golang-golang-x-net-dev***, ***golang-websocket***, ***gssproxy***, ***highlight.js***, ***influxdb***, ***jupyter-notebook***, ***leptonlib***, ***libhibernate3-java***, ***libmediainfo***, ***libpano13***, ***libxstream-java***, ***libzstd***, ***linux-4.19***, ***linux-latest-4.19***, ***mediawiki***, ***minidlna***, ***mqtt-client***, ***mumble***, ***mupdf***, ***musl***, ***mutt***, ***netty***, ***node-ini***, ***open-build-service***, ***openvswitch***, ***pacemaker***, ***pdfresurrect***, ***php-horde-text-filter***, ***php-nette***, ***postsrsd***, ***privoxy***, ***python-bleach***, ***python-bottle***, ***python-certbot***, ***redis***, ***roundcube***, ***ruby-mechanize***, ***ruby-redcarpet***, ***salt***, ***shibboleth-sp2***, ***slirp***, ***snapd***, ***spice-vda-gent***, ***spip***, ***sympa***, ***tcpflow***, ***thunderbird***, ***tomcat8***, ***unbound1.9***, ***unrar-free***, ***velocity***, ***velocity-tools***, ***vips***, ***x11vnc***, ***xcftools***, ***zsh***

- The following packages have been moved to the maintained repository of UCS: ***moreutils*** (Bug 52743), ***python-bcrypt*** (Bug 52693), ***python-monotonic*** (Bug 52273)

6.2. Basic system services

Feedback

6.2.1. Univention Configuration Registry

Feedback

6.2.1.1. Changes to templates and modules

Feedback

- Fix a Python 3 compatibility error in the Univention Configuration Registry template for `/etc/hosts` (Bug 52919).

6.2.2. Boot Loader

Feedback

- The generated `/boot/grub/grub.cfg` is compatible with the upgrade to UCS 5 (Bug 53117).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- Support for the password scheme *bcrypt* has been added. The Univention Configuration Registry variable `ldap/pw-bcrypt` has been added to activate the module ***bcrypt*** in OpenLDAP (Bug 52693).
- From now on SHA-512 hashes are used for the LDAP service accounts `admin` and `backup` (Bug 52696).

6.3.1.1. Listener/Notifier domain replication

Feedback

- The notifier sometimes did not recognize a transaction until the next one occurred. Two causes for this behavior have been fixed (Bug 51804).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- A cross site scripting vulnerability in the Univention Management Console menu has been fixed (Bug 52665).
- Package version bump to ensure package update will be done in all scenarios (Bug 52371).
- The OpenAPI schema has been adjusted to be compliant: The *example* property of parameters has been removed as it conflicts with *examples* (Bug 52862).
- The OpenAPI schema of the UDM REST API now contains `201` as additional possible status code for modify operations. It is returned in case an object was moved (Bug 52725).

- The OpenAPI schema of the UDM REST API now returns `200` as status code for the retrieval of object creation templates (Bug 52723).

6.4.2. Univention Portal

Feedback

- Fetching of user information is now done against the Apache HTTP interface instead of directly against the UMC web server (Bug 52293).

6.4.3. Univention Management Console server

Feedback

- Fix translation of a ***pwdQuality*** related error message which led to German/English mix in Univention Management Console (Bug 52198).
- The Univention Configuration Registry variable `pam/krb5/ticket_after_pwchange` has been added to restore the default behavior of the PAM module `krb5`. See https://help.univention.com/t/17403 for more information (Bug 52188).
- A `KeyError` is prevented when a session timer has already been removed (Bug 52535).
- The evaluation of disallow option pattern in the ACL definitions has been repaired (Bug 25197).
- A crash of the Univention Management Console server has been fixed (Bug 52699).
- A cross site scripting vulnerability has been fixed (Bug 52665).
- The Python Notifier implementation is used (among others) by the Univention Management Console server to handle the communication between the main server process and the UMC module processes. If any UMC module process fails to start within a few seconds the module process is forcefully terminated by the server process. Under high load a fallback implementation is invoked to terminate all child processes, which sometimes is too eager and kills unrelated processes using `` `python2.7``. This included UCS services like UCS Virtual Machine Manager, UMC server, UMC web server, UMC REST API, UCS Portal server and Univention S4 connector. The broken fallback mechanism has been disabled and removed (Bug 52518).
- The fix addresses a memory leak in ***univention-management-console-server*** which was introduced in erratum UCS 4.4-8 erratum 848. In addition, a log message was moved from the *process* to the *info* log level (Bug 52508).
- UMC now shows a banner to the upcoming Univention Summit 2021 once (Bug 52499).
- The removal of sessions has been optimized (Bug 52273).
- The UMC web server is now multiprocessing capable (Bug 52293).
- Data stored for outstanding SAML queries are now removed when a SAML response is received (Bug 52444).
- SAML identities are now cached in a BDB database instead of in memory (Bug 52442).
- Expired sessions are now removed from the SAML cache (Bug 52443).
- The UMC server is now multiprocessing capable (Bug 52371).

6.4.4. Univention App Center

Feedback

- Fix traceback when using Univention App Center once App ini file with install permissions is present in cache (Bug 52852).
- The app parameter *DockerScriptInit* can now be configured via Univention Configuration Registry (Bug 52839).

- The LDAP ACL UCR templates now have valid Python 3 syntax for compatibility with the UCS 5.0 update (Bug 52815).
- The new subcommand `update-check` has been added to `univention-app` to check whether an UCS update with the currently installed Apps is possible (Bug 52771).
- To reduce the risk of problems during the upgrade of apps an unnecessary second call of `docker.pull` has been removed (Bug 52456).

6.4.5. Univention Directory Manager UMC modules and command line interface

Feedback

- Changing the user password via UMC if *bcrypt* is activated is now possible (Bug 52832).
- Support for *bcrypt* user password hashes has been added to the UDM. *bcrypt* can be activated with the Univention Configuration Registry variable `password/hashing/bcrypt` (default: `false`). The *bcrypt* cost factor and variant can be configured with the Univention Configuration Registry variables `password/hashing/bcrypt/cost_factor` (default: `12`) and `password/hashing/bcrypt/prefix` (default: `2b`) (Bug 52693).
- The argument `--remove-option` of the UDM CLI command `create` has been repaired (Bug 52576).

6.4.6. Other modules

Feedback

- The Python Notifier implementation is used (among others) by the Univention Management Console server to handle the communication between the main server process and the UMC module processes. If any UMC module process fails to start within a few seconds the module process is forcefully terminated by the server process. Under high load a fallback implementation is invoked to terminate all child processes, which sometimes is too eager and kills unrelated processes using `` `python2.7 ``. This included UCS services like UCS Virtual Machine Manager, UMC server, UMC web server, UMC REST API, UCS Portal server and Univention S4 connector. The broken fallback mechanism has been disabled and removed (Bug 52518).
- The timer is now using a monotonic clock so that system time adjustments do not affect the timer execution (Bug 52273).
- A cross site scripting vulnerability has been fixed in ***univention-management-console-module-password-change*** (Bug 52665).

6.5. Software deployment

Feedback

- The ***univention-updater*** UCR templates now have valid Python 3 syntax for compatibility with the UCS 5.0 update (Bug 52813).
- The ***univention-updater*** now checks if the locally installed apps are available for the next UCS version (Bug 52771).
- The ***univention-updater*** now supports updating to UCS 5, once it is released (Bug 51865).

6.6. System services

Feedback

6.6.1. Docker

Feedback

- The new Univention Configuration Registry variable `docker/daemon/default/opts/registry-mirrors` can be used to define custom registry mirrors for the docker daemon. It is also possible

now to configure arbitrary JSON encoded data, which gets mixed into the Docker daemon configuration file `/etc/docker/daemon.json` via the Univention Configuration Registry variable `docker/daemon/default/json` (Bug 52344).

- Add system call `statx` to docker *seccomp* profile (Bug 52478).

6.6.2. SAML

Feedback

- This is a new upstream version of ***stunnel4*** (Bug 52196).
- A watchdog service `univention-stunnel4-watchdog` has been added, which restarts the `stunnel4` service, if it does not respond any more, but is marked as active. This can be activated by setting the Univention Configuration Registry variable `ucs/server/sso/stunnel4/watchdog/active=true` and restarting the service `univention-stunnel4-watchdog` (Bug 52196).
- Package version bump to ensure package update will be done in all scenarios (Bug 52371).
- The memory consumption of ***python-pysaml2*** has been optimized (Bug 52466, Bug 52467).

6.6.3. Univention self service

Feedback

- *ucsversionstart* and *ucsversionend* is now set during registering of the LDAP ACL extension. This is required for the upgrade to UCS 5 (Bug 52955).

6.6.4. Postfix

Feedback

- The default Postfix version compatibility level was raised from 2 to 3 (Bug 46895).

6.6.5. Spam/virus detection and countermeasures

Feedback

- A unjoin script has been added (Bug 52962).

6.6.6. Printing services

Feedback

- The UCR templates are now compatible with Python 3 for the UCS 5.0 upgrade (Bug 52814).

6.6.7. Nagios

Feedback

- A unjoin script for ***univention-nagios-dansguardian*** has been added (Bug 52962).
- Univention Configuration Registry variables are now unset on package removal (Bug 52980).

6.6.8. Apache

Feedback

- Package version bump to ensure package update will be done in all scenarios (Bug 52371).

6.6.9. Proxy services

Feedback

- The UCR templates are now compatible with Python 3 for the UCS 5.0 upgrade (Bug 52814).

6.6.10. Kerberos

Feedback

- The behavior of the PAM module `krb5` has been changed. From now on the module no longer tries to obtain a new ticket after a password change (as this is error prone due to timing issues in the password syn-

chronization). The old behavior can be restored by setting the Univention Configuration Registry variable `pam/krb5/ticket_after_pwchange=true` (sets the `ticket_after_pwchange` flag in the PAM configuration). See https://help.univention.com/t/17403 for more information (Bug 52188).

- Version number has been increased to restart the `heimdal-kdc`. This is necessary to allow for the *mspwd-policy* feature to work correctly (Bug 52198).
- More specific error messages are passed through from ***heimdal*** to Univention Management Console in case of a failed ***pwdQuality*** check (Bug 52198).

6.6.11. Other services

Feedback

- Univention Configuration Registry variables are now unset on package removal (Bug 52981).

6.7. Virtualization

Feedback

6.7.1. UCS Virtual Machine Manager (UVMM)

Feedback

- Restore schema file system path to `/usr/share/univention-ldap/schema/` to prevent a possible error when updating the package simultaneously on multiple systems (Bug 52867).
- Register files from package ***univention-virtual-machine-manager-schema*** in LDAP in preparation for UCS 5 (Bug 51955).

6.8. Services for Windows

Feedback

6.8.1. Univention S4 Connector

Feedback

- The attribute *gidNumber* on users will be synchronized from UCS to Samba4, but not from Samba4 to UCS (Bug 50278).
- The attribute *gidNumber* on groups is now synced from UCS to Samba4. The attribute is only set if an UCS object is modified. Multiple objects can be resynchronized with the tool `/usr/share/univention-s4-connector/resync_object_from_ucs.py --filter`, which accepts an LDAP filter (Bug 50766).

6.8.2. Univention Active Directory Connection

Feedback

- If a modification is done in AD and the user does not yet exist in UCS, the connector should set all values on the UCS object, if they have changed or not. Not doing that, led to rejects due to missing mandatory values (Bug 52261).
- The connector creates a temporary password before synchronizing the users actual password. This temporary password did not conform to MS standard password complexity. This led to rejects, due to the password being too simple (Bug 52439).

6.9. Other changes

Feedback

- The Univention Configuration Registry variable `pam/krb5/ticket_after_pwchange` has been added to restore the default behavior of the PAM module ***krb5***. See https://help.univention.com/t/17403 for more information (Bug 52188).