univention
be open.

UCS 4.4 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.4-0

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

<feedback@univention.de>

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.4-0 steht das vierte Minor Release für Univention Corporate Server (UCS) 4 zur Verfügung. Es umfasst Funktionserweiterungen und Verbesserungen, neue Eigenschaften sowie diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Mit dem Release steht die neue App *Admin Diary* bereit, mit der administrative Ereignisse von allen UCS Instanzen einer Domäne zentral eingesehen und ausgewertet werden können. Änderungen an Benutzern, Gruppen oder anderen Objekten im Verzeichnisdienst sind darüber genauso nachverfolgbar wie Updates von Servern oder (De-)Installationen von Apps.

  Das *Admin Diary* wird als zwei Komponenten ausgeliefert: Ein Backend für die Datenhaltung in einer SQL Datenbank und ein Frontend für die Integration in die UMC. Die Erfassung der Ereignisse ist Teil von UCS 4.4 und wird mit Installation des Backends automatisch aktiviert.

- Die Self-Service App wurde in zwei Bereichen erweitert:

  - Endanwender können das Webinterface des Self-Service nun nicht nur für Passwortänderungen nutzen, sondern auch für das Editieren der eigenen Kontaktinformationen.

  - Administratoren wird jetzt die Möglichkeit geboten, den Self-Service zum Einladen neuer Nutzer per Mail zu verwenden. In diesem Verfahren wird neuen Anwendern ein Token des Self-Service übermittelt, mit dem sie das vorbereitete Konto in der UCS Domäne um Passwort und Kontaktinformationen erweitern können.

- Das Portal wurde um die Möglichkeit erweitert, Anwender direkt auf die Anmeldeseite zu verweisen und bei einem leeren Portal Hinweistexte anzuzeigen. Die Darstellungen wurden optimiert und sind jetzt per CSS anpassbar. Weiter verfügt das Portal jetzt über ein verbessertes Berechtigungsmanagement, mit dem mehr Zugriffsschutz auf Serverseite möglich ist, was die Grundlage für zukünftige Funktionen bildet.

- Die RADIUS App wurde vereinheitlicht durch das Zusammenführen der Implementierungen von UCS@school und der UCS App. Im Rahmen der Implementierung wurde der Austausch von *Shared Secrets* z.B. mit WLAN Access Points vereinfacht: Die Access Point Konfiguration kann nun über das UMC Modul für Rechnerobjekte vorgenommen werden.

- Samba wurde auf Version 4.10 RC2 aktualisiert, wodurch zahlreiche Verbesserungen einfließen.

  So werden mit dieser Version Vertrauensstellungen (*Trusts*) zwischen UCS und Microsoft Active Directory Domänen konfigurierbar. Damit ist es beispielsweise möglich, das in UCS administrierte Nutzer Zugriff auf in Microsoft Domänen betriebenen Services erhalten.

  Weiter unterstützt Samba jetzt *Fine Grained Password Policies*, mit denen es möglich ist unterschiedliche und detaillierte Passwort-Richtlinien innerhalb der Microsoft Active Directory bzw. Kerberos Domäne zu definieren.

- Die Benutzerführung in der Univention Management Console wurden in vielen Punkten verbessert. Dazu gehören eine klarere Darstellung von Eingabeelementen, eine bessere Handhabung von langen Ergebnislisten und eine effizientere Darstellung auf kleinen Displays.

- Die von installierten Apps mitgebrachten Einstellungen an Benutzerobjekten können jetzt an einer übersichtlichen Stelle am Benutzer editiert werden. Damit wird sowohl die Administration von UCS als auch die Integration durch App Provider vereinfacht.

- Für App Anbieter sind die *Install Permissions* eine neue Funktion im App Center: Damit kann pro Version angeben werden, ob die App für die Installation ein Vertragsverhältnis zwischen Nutzer und Anbieter

erfordert. Damit unterstützt das App Center besser entsprechende Geschäftsmodelle der App Anbieter und Nutzer können besser erkennen, welche Versionen einer App verfügbar sind.

- UCS 4.4-0 basiert auf dem im Februar veröffentlichten Debian Release 9.8. 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.

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 http://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. Univention Directory Notifier

Feedback

Durch einen Entwurfsfehler im Univention Directory Notifier Netzwerkprotokoll Version 2 kann jeder Benutzer an Informationen über Änderungen am LDAP-Verzeichnisdienst kommen. Ein neues Protokoll Version 3 wurde mit UCS-4.3-3 Erratum 427 implementiert. Für die Kompatibilität mit alten UCS Systemen bot Univention Directory Notifier standardmäßig weiterhin Version 2 an. Beginnend mit UCS-4.4 bieten neue Installationen standardmäßig nur noch Version 3 an. Protokoll 2 kann reaktiviert werden, indem die Univention Configuration Registry-Variable `notifier/protocol/version` auf `2` geändert und Univention Directory Notifier neu gestartet wird.

5.2. 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.

5.3. 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.

5.4. 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 *4.3-3*:

6.1. General

- All security updates issued since UCS 4.3-3 are included:
  - ***apt*** (CVE-2019-3462) (Bug 48513)
  - ***cups*** (CVE-2017-18248, CVE-2018-4700) (Bug 48772)
  - ***curl*** (CVE-2018-16890, CVE-2019-3822, CVE-2019-3823) (Bug 48786)
  - ***dovecot*** (CVE-2019-3814) (Bug 48774)
  - ***firefox-esr*** (CVE-2018-12405, CVE-2018-17466, CVE-2018-18356, CVE-2018-18492, CVE-2018-18493, CVE-2018-18494, CVE-2018-18498, CVE-2018-18500, CVE-2018-18501, CVE-2018-18505, CVE-2019-5785) (Bug 48319, Bug 48589, Bug 48779)
  - ***freerdp*** (CVE-2018-8786, CVE-2018-8787, CVE-2018-8788, CVE-2018-8789) (Bug 48775)
  - ***ghostscript*** (Bug 48415, Bug 48537)
  - ***glibc*** (CVE-2017-15670, CVE-2017-15671, CVE-2017-15804, CVE-2017-16997, CVE-2017-18269, CVE-2017-1000408, CVE-2017-1000409, CVE-2018-11236, CVE-2018-11237) (Bug 48778)
  - ***intel-microcode*** (CVE-2018-3639, CVE-2018-3640) (Bug 48781)
  - ***libapache2-mod-perl2*** (CVE-2011-2767) (Bug 48785)
  - ***libarchive*** (CVE-2016-10209, CVE-2016-10349, CVE-2016-10350, CVE-2017-14166, CVE-2017-14501, CVE-2017-14502, CVE-2017-14503, CVE-2018-1000877, CVE-2018-1000878, CVE-2018-1000880) (Bug 48408)
  - ***libemail-address-perl*** (CVE-2015-7686, CVE-2018-12558) (Bug 48777)
  - ***libgd2*** (CVE-2019-6977, CVE-2019-6978) (Bug 48614)
  - ***libphp-phpmailer*** (CVE-2018-19296) (Bug 48306)
  - ***libreoffice*** (CVE-2018-16858) (Bug 48592)
  - ***libvirt*** (Bug 47617)
  - ***libvirt-python*** (Bug 47617)
  - ***libvncserver*** (CVE-2018-6307, CVE-2018-15126, CVE-2018-15127, CVE-2018-20019, CVE-2018-20020, CVE-2018-20021, CVE-2018-20022, CVE-2018-20023, CVE-2018-20024) (Bug 48591)
  - ***linux***, ***univention-kernel-image-signed*** (CVE-2017-18249, CVE-2018-1128, CVE-2018-1129, CVE-2018-5848, CVE-2018-12896, CVE-2018-13053, CVE-2018-13096, CVE-2018-13097, CVE-2018-13100, CVE-2018-14610, CVE-2018-14611, CVE-2018-14612, CVE-2018-14613,

CVE-2018-14614, CVE-2018-14616, CVE-2018-16862, CVE-2018-17972, CVE-2018-18281, CVE-2018-18690, CVE-2018-18710, CVE-2018-19407) (Bug 48782)

- ***openssh*** (CVE-2018-20685, CVE-2019-6109, CVE-2019-6111) (Bug 48780)
- ***openssl1.0*** (CVE-2018-0732, CVE-2018-0734, CVE-2018-0737, CVE-2018-5407) (Bug 48388)
- ***php-pear*** (CVE-2018-1000888) (Bug 48590)
- ***php7.0*** (CVE-2018-14851, CVE-2018-14883, CVE-2018-17082, CVE-2018-19518, CVE-2018-19935, CVE-2019-9020, CVE-2019-9021, CVE-2019-9022, CVE-2019-9023, CVE-2019-9024) (Bug 48309)
- ***policykit-1*** (CVE-2018-19788) (Bug 48307)
- ***python-django*** (CVE-2019-3498) (Bug 48464)
- ***qemu*** (Bug 47617)
- ***qtbase-opensource-src*** (CVE-2018-15518, CVE-2018-19870, CVE-2018-19873) (Bug 48593)
- ***rdesktop*** (CVE-2018-8791, CVE-2018-8792, CVE-2018-8793, CVE-2018-8794, CVE-2018-8795, CVE-2018-8796, CVE-2018-8797, CVE-2018-8798, CVE-2018-8799, CVE-2018-8800, CVE-2018-20174, CVE-2018-20175, CVE-2018-20176, CVE-2018-20177, CVE-2018-20178, CVE-2018-20179, CVE-2018-20180, CVE-2018-20181, CVE-2018-20182) (Bug 48776)
- ***sox*** (CVE-2014-8145) (Bug 48783)
- ***spice*** (CVE-2019-3813) (Bug 48594)
- ***systemd*** (CVE-2018-16864, CVE-2018-16865, CVE-2018-16866, CVE-2019-3815, CVE-2019-6454) (Bug 48463, Bug 48499, Bug 48759)
- ***uriparser*** (CVE-2018-19198, CVE-2018-19199, CVE-2018-19200) (Bug 48784)
- ***vlc*** (Bug 48462)
- ***wayland*** (CVE-2017-16612) (Bug 48773)
- ***wireshark*** (CVE-2018-12086, CVE-2018-18225, CVE-2018-18226, CVE-2018-18227, CVE-2018-19622, CVE-2018-19623, CVE-2018-19624, CVE-2018-19625, CVE-2018-19626, CVE-2018-19627, CVE-2018-19628) (Bug 48409)
- ***zeromq3*** (CVE-2019-6250) (Bug 48500)

- The following updated packages from Debian 9.8 are included (Bug 48332): ***ansible***, ***arc***, ***astroml-addons***, ***base-files***, ***c3p0***, ***ca-certificates-java***, ***chkrootkit***, ***chromium***, ***compactheader***, ***coturn***, ***courier***, ***debian-edu-config***, ***debian-installer-netboot-images***, ***debian-installer***, ***debian-security-support***, ***dnspython***, ***drupal7***, ***egg***, ***erlang***, ***espeakup***, ***flatpak***, ***ganeti-os-noop***, ***glx-alternatives***, ***gnulib***, ***gnupg2***, ***golang-1.7***, ***golang-1.8***, ***graphite-api***, ***grokmirror***, ***ibus***, ***icinga2***, ***ikiwiki***, ***isort***, ***jdupes***, ***kmodpy***, ***libapache-mod-jk***, ***libb2***, ***libdatetime-timezone-perl***, ***libemail-address-list-perl***, ***libextractor***, ***libgpod***, ***libssh***, ***libu2f-host***, ***linux-igd***, ***lttng-modules***, ***mistral***, ***monkeysign***, ***mosquitto***, ***mpqc***, ***netatalk***, ***nvidia-graphics-drivers***, ***nvidia-modprobe***, ***nvidia-persistenced***, ***nvidia-settings***, ***nvidia-xconfig***, ***openni2***, ***openvpn***, ***parsedatetime***, ***pdns***, ***pdns-recursor***, ***photocollage***, ***postfix***, ***postgresql-9.6***, ***postgrey***, ***pylint-django***, ***python-acme***, ***python-arpy***, ***python-certbot-apache***, ***python-certbot-nginx***, ***python-certbot***, ***python-hypothesis***, ***python-josepy***, ***pyzo***, ***r-cran-readxl***, ***rssh***, ***rtkit***, ***ruby-loofah***, ***ruby-rack***, ***ruby-sanitize***, ***sl-modem***, ***sogo-connector***, ***ssh-agent-filter***, ***supercollider***, ***sympa***, ***thunderbird***, ***tmpreaper***, ***twitter-bootstrap3***, ***tzdata***, ***uglifyjs***, ***vm***, ***vulture***, ***wicd***, ***wordpress***, ***wvstreams***, ***xapian-core***, ***xen***, ***xkeycaps***, ***yosys***, ***z3***

- The following packages have been moved to the maintained repository of UCS: ***fail2ban*** (Bug 47566), ***libmaxminddb*** (Bug 48409)
- All `debian/changelog` files have been updated to the machine-readable DEP-5 format. The copyright of all packages has been extended to 2019 (Bug 28499):

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- Always set UCR variable `update/reboot/required` when a new kernel is installed (Bug 48349).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

6.3.1.1. Listener/Notifier domain replication

Feedback

- Implement new Univention Directory Notifier Protocol Version 3, which does not transmit Distinguished Names over an unencrypted and unauthenticated channel (Bug 48427).
- The new script `univention-replicate-many` can be used to re-replicate multiple objects at once (Bug 41262).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- The recommended browser versions have been updated (Bug 47829).
- The Univention logo has been updated (Bug 48700).
- The feature of modern browsers to automatically fill out HTML form fields has been improved (Bug 46198).
- The design of the web interface has been improved (Bug 48471, Bug 48723).

6.4.2. Univention Portal

Feedback

- The portal now has its own service. ***univention-portal-server*** filters entries that shall only be seen by users of certain groups in the backend, instead of serving all and the frontend hides them. Permissions on nested groups are now evaluated correctly (Bug 48358, Bug 48595).
- The portal can now be customized via a custom CSS file (Bug 48506).
- The user guidance in the portal has been improved. It is now possible to define whether users have to be logged in to visit the portal. Furthermore a custom message can be configured to show to users that are not logged in and would be presented with an empty portal otherwise (Bug 48546).
- The portal now depends on ***netcat-openbsd*** to ensure that it's join script is IPv6 compatible (Bug 46556).

6.4.3. Univention Management Console server

Feedback

- The errors from ***pam_cracklib*** are evaluated again when changing the password via Univention Management Console (Bug 48684).

6.4.4. Univention App Center

Feedback

- The UMC module obtained a graphical overhaul and new filters (Bug 48449, Bug 48483, Bug 48846).
- It is now possible to show a preview of certain Apps that are not (yet) installable. These Apps can be voted for to get more insights whether users would want this App in the App Center (Bug 48472).
- The App Center is now able to handle Apps with install permissions. This describes App versions that can only be installed when the App has been bought from the Univention App Center store (Bug 48624, Bug 48544, Bug 48127, Bug 48753).

6.4.5. Univention Admin Diary

Feedback

- There are two new UCS apps, the ***Admin Diary Frontend*** and the ***Admin Diary Backend*** (Bug 48675, Bug 48341, Bug 48717, Bug 48342, Bug 48343, Bug 48476).

6.4.6. Univention Directory Manager UMC modules and command line interface

Feedback

- A singular and plural object name have been added for every module (Bug 48738).

6.4.7. Modules for system settings / setup wizard

Feedback

- Make the software components for UCS available during installation when it is run in French (Bug 44162).

6.4.8. Domain join module

Feedback

- Having multiple (virtual) network interfaces with the same MAC address caused the domain join to fail (Bug 48475).
- Copy `cn=translog` database for transaction log to backup domain controller while joining (Bug 48427).

6.4.9. Users module

Feedback

- A new tab **Apps** has been added to users, which allows to enable and disable apps (Bug 48621, Bug 48839).
- The wizard for creating new users now allows to use an e-mail invitation for that user instead of setting an initial password (Requires the App ***Self Service***) (Bug 48660).

6.4.10. System diagnostic module

Feedback

- Use new Univention Directory Notifier Protocol Version 3 for check (Bug 48427).
- Fixed error in Check well known SIDs system diagnostic test (Bug 48477).
- Added command line tool `univention-run-diagnostic-checks` which can be used to execute the diagnostic checks (Bug 47650).
- A typo has been fixed in the error output of the Kerberos DDNS update check (Bug 48385).
- The proxy server test has been fixed (Bug 48385).

6.4.11. Filesystem quota module

Feedback

- Quotas on `XFS` file systems are shown again on the Univention Management Console (Bug 48315).

6.4.12. Other modules

Feedback

- A crash in the UCS management system module is prevented if widget definitions are configured via Univention Configuration Registry variables (Bug 48494).

6.5. Univention base libraries

Feedback

- Support activation of the `cn=monitor` backend for statistical information. To activate this, set Univention Configuration Registry variable `ldap/monitor` to `true` and restart the LDAP server service (`slapd`) (Bug 41213).
- Add `cn=translog` database for transaction log (Bug 48427).
- During the update, a resynchronization of the listener module `ldap_extension` is performed on backup domain controller and slave domain controller systems to correct possible inconsistencies in LDAP ACLs (Bug 48530).
- Enabled `cn=config` backend, accessible via `ldapi:///` only (Bug 43515).
- Add ***univention-lib*** implementation of `die()` function to `ldap.sh` (Bug 47424).
- Due to a logic error it could happen that not all LDAP ACL registered in LDAP were active on newly installed master domain controller systems. This could lead to information disclosure or replication errors. The error is now fixed and when updating the ***univention-ldap-server*** package, missing LDAP ACLs are automatically activated (Bug 48530).
- Do not send cron mails for a successful `ldap-backup` cron job (Bug 48014).
- The syntax class `mailinglist_name` was integrated into `syntax.py` (Bug 48383).

6.6. Software deployment

Feedback

- The repository tools `univention-repository-addpackage`, `univention-repository-delpackage` and `univention-repository-merge` are deprecated and are removed with UCS-4.4 (Bug 29505).
- The packages index files under `dists/` are now also mirrored. This is required for the PXE network installer (Bug 46600).
- Added the Univention Configuration Registry variable `update/debug/level` for changing the debug level of the UCS updater (Bug 47913).
- The error message complaining about the missing `postmirror.sh` file is no longer displayed (Bug 27761).
- When mirroring distributions the default architecture was not detected correctly and URLs were scheduled for download multiple times (Bug 48424).
- The updater scripts `preup.sh` and `postup.sh` have been adapted to the needs of UCS 4.4 (Bug 48808).
- The updater has been fixed to work with a local repository only initialized by `univention-repository-create` from DVD (Bug 48910).
- `univention-repository-create` now checks if ***univention-debmirror*** is installed before installing it (Bug 48151).

6.7. System services

Feedback

6.7.1. SAML

Feedback

- The ***univention-saml*** Apache *VirtualHost* configuration can now be extended by placing `.conf` files in the directory `/etc/apache2/sso-vhost.conf.d/` (Bug 48348).

6.7.2. Univention self service

Feedback

- If the self service is installed, a daemon on the master domain controller now sends an invitation email to users that were created with respective settings in the UMC (Bug 48446).
- It is now possible to define attributes a self service user can modify with the Univention Configuration Registry variables `self-service/ldap_attributes` and `self-service/udm_attributes` (Bug 48447, Bug 48710)

6.7.3. Printing services

Feedback

- Allow switching to `None`, `smb` (raw) printer model (Bug 47843).
- Ensure `/usr/share/cups/model` is a link to `/usr/share/ppd/` (Bug 47435).

6.7.4. Nagios

Feedback

- Fixed a local root exploit in the SUID wrapper for the Nagios check `univention_ldap` (Bug 48616).
- Fixed an uncaught type error in the ***nagios-server*** listener (Bug 43426).

6.7.5. RADIUS

Feedback

- Network access servers for example wireless access points can now be configured with Univention Directory Manager. Any existing `clients.conf` is not converted and can still be used to configure clients manually (Bug 25935). Switch to Python `passlib` for DES encryption (Bug 48460). Move `clients.conf.example` into the right folder (Bug 46561). Improved logging for ***univention-radius-ntlm-auth*** which is used by FreeRADIUS to authenticate users. Log entries are written to `radius_ntlm_auth.log`. The log level can be adjusted with the Univention Configuration Registry variable `freeradius/auth/helper/ntlm/debug`. Internal changes to enable the UCS@school RADIUS implementation to build upon the ***univention-radius*** package (Bug 46018).

6.8. Virtualization

Feedback

6.8.1. UCS Virtual Machine Manager (UVMM)

Feedback

- Normalize CPU utilization of host and update error and migration status atomically (Bug 48340).
- Show CPU usage in tree of virtualization hosts (Bug 35196).
- Fix tooltips preventing button clicks (Bug 45498).
- Add Hyper-V Enlightment for Windows VMs (Bug 48024).
- The target hosts for live migration can now be configured even when the virtual machine is running (Bug 48199).

- Fix parsing memory and disk capacity (Bug 36661).
- Fix file permissions of backup directory (Bug 47741).
- Add support for post-copy migration (Bug 47617).
- Small layout adjustments for the updated UMC design (Bug 48859, Bug 46198, Bug 48471)
- Add RAM overcommitment protection through Univention Configuration Registry variable `uvmm/overcommit/reserved` (Bug 48901).

6.9. Services for Windows

Feedback

6.9.1. Samba

Feedback

- The `samba-tool ntacl sysvolcheck` didn't map owner LA to DA properly while checking, leading to irritating, unnecessary error messages (Bug 44282).
- The package ***samba*** has be updated to version `4.10.0~rc2` (Bug 48084).
- Accounts for service principals are now created with UDM (Bug 47955).
- Activation of UCS@school specific LDB modules has been moved from `97libunivention-ldb-modules.inst` to `96univention-samba4.inst` to simplify package structure (Bug 47955).

6.9.2. Univention S4 Connector

Feedback

- Moving objects in UCS with a LDAP base different in UCS and Samba has been fixed (Bug 48362).
- Password synchronization has been adjusted to Samba 4.10 (Bug 48142).

6.10. Other changes

Feedback

- The package ***univention-errata-level*** has been updated to reset the Univention Configuration Registry variable `version/erratalevel` to `0` (Bug 48654).
- For security reasons all join scripts now use a password file (Bug 46969).
- Hooks have been added to the join process (Bug 47940, Bug 48801).
- The join status file is now reset a second time right after the join hooks of type `join/pre-joinscripts` have been called. This prevents join problems on backup domain controller system in case the join hook installed additional software (Bug 48751).