univention
be open.

UCS 4.3 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.3-2

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

<feedback@univention.de>

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.3-2 steht das zweite 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:

- Während der Aktualisierung auf neue UCS Release- oder Patchlevelversionen wird die Univention Management Console in einen Wartungsmodus versetzt. Während der Wartungsmodus aktiv ist, wird der Fortschritt des Updates auf einer einfachen Webseite dargestellt.

- Samba wurde auf Version 4.7.8 aktualisiert. Aus Sicherheitsgründen ist jetzt die Authentifizierung mit *NTLMv1* nicht mehr erlaubt. Sofern noch sehr alte Systeme oder Anwendungen im Einsatz sind, die unbedingt *NTLMv1* benötigen, so kann dies per Univention Configuration Registry wieder aktiviert werden.

- Der Installationswizard wurde erweitert, so dass vor dem Start der Installation mögliche Probleme beim Domänenbeitritt und der Internetanbindung identifiziert werden und Lösungsmöglichkeiten aufgezeigt werden können.

- Eine manuell erstellte oder angepasste SAML Konfiguration für einen Dienst kann nun direkt im LDAP abgelegt werden. Diese Konfiguration wird dann auf alle am Single Sign On beteiligten Identity Provider in der Domäne repliziert.

- Der AD Connector wurde um Werkzeuge erweitert, einzelne Objekte oder ganze Teilbäume erneut zu synchronisieren und Rejects gezielt zu entfernen.

- Diverse Security Updates wurden in UCS 4.3-2 integriert, bspw. für den Linux Kernel, *Samba* und *Apache2*. Eine vollständige Liste 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 *4.3-1*:

6.1. General

- All security updates issued for UCS 4.3-1 are included:
  - ***amd64-microcode*** (CVE-2017-5715) (Bug 47616)
  - ***apache2*** (CVE-2018-1302) (Bug 47510)
  - ***base-files*** (Bug 47512)
  - ***clamav*** (CVE-2018-0360 CVE-2018-0361) (Bug 47404)
  - ***cups*** (CVE-2017-15400 CVE-2018-4180 CVE-2018-4181 CVE-2018-4182 CVE-2018-4183 CVE-2018-6553) (Bug 47354)
  - ***curl*** (CVE-2018-1000301) (Bug 47283)
  - ***devscripts*** (Bug 47488)
  - ***discover*** (Bug 47484)
  - ***dpkg*** (Bug 47503)
  - ***exiv2*** (CVE-2018-10958 CVE-2018-10998 CVE-2018-10999 CVE-2018-11531 CVE-2018-12264 CVE-2018-12265) (Bug 47301)
  - ***faad2*** (CVE-2017-9218 CVE-2017-9219 CVE-2017-9220 CVE-2017-9221 CVE-2017-9222 CVE-2017-9223 CVE-2017-9253 CVE-2017-9254 CVE-2017-9255 CVE-2017-9256 CVE-2017-9257) (Bug 47505)
  - ***ffmpeg*** (Bug 47504)
  - ***file*** (CVE-2018-10360) (Bug 47507)
  - ***firefox-esr*** (CVE-2018-5156 CVE-2018-5188 CVE-2018-6126 CVE-2018-12359 CVE-2018-12360 CVE-2018-12362 CVE-2018-12363 CVE-2018-12364 CVE-2018-12365 CVE-2018-12366 CVE-2018-12368) (Bug 47285)
  - ***fuse*** (CVE-2018-10906) (Bug 47498)
  - ***gdm3*** (CVE-2018-14424) (Bug 47588)
  - ***ghostscript*** (CVE-2016-10317 CVE-2018-10194) (Bug 47481)
  - ***git*** (CVE-2018-11233 CVE-2018-11235) (Bug 47287)
  - ***gnupg1*** (CVE-2018-12020) (Bug 47291)
  - ***gnupg2*** (CVE-2018-12020) (Bug 47290)
  - ***imagemagick*** (CVE-2018-5248 CVE-2018-11251 CVE-2018-12599 CVE-2018-12600) (Bug 47486)

- ***intel-microcode*** (CVE-2018-3615 CVE-2018-3620 CVE-2018-3639 CVE-2018-3640 CVE-2018-3646) (Bug 47606 Bug 47669)
- ***libdatetime-timezone-perl*** (Bug 47477)
- ***libgcrypt20*** (CVE-2018-0495) (Bug 47288)
- ***libipc-run-perl*** (Bug 47501)
- ***libmicrodns*** (Bug 47294)
- ***libmspack*** (CVE-2017-6419 CVE-2017-11423 CVE-2018-14679 CVE-2018-14680 CVE-2018-14681 CVE-2018-14682) (Bug 47513)
- ***libnfs*** (Bug 47294)
- ***libsoup2.4*** (CVE-2018-12910) (Bug 47475)
- ***libvncserver*** (CVE-2018-7225) (Bug 47293)
- ***linux*** (CVE-2017-5753 CVE-2017-17975 CVE-2017-18222 CVE-2017-18255 CVE-2018-1066 CVE-2018-1087 CVE-2018-1092 CVE-2018-1093 CVE-2018-1108 CVE-2018-1118 CVE-2018-1120 CVE-2018-1130 CVE-2018-3620 CVE-2018-3639 CVE-2018-3646 CVE-2018-5391 CVE-2018-5814 CVE-2018-6412 CVE-2018-7757 CVE-2018-8087 CVE-2018-8781 CVE-2018-8822 CVE-2018-8897 CVE-2018-10021 CVE-2018-10087 CVE-2018-10124 CVE-2018-10853 CVE-2018-10876 CVE-2018-10877 CVE-2018-10878 CVE-2018-10879 CVE-2018-10880 CVE-2018-10881 CVE-2018-10882 CVE-2018-10883 CVE-2018-10940 CVE-2018-11506 CVE-2018-12233 CVE-2018-13405 CVE-2018-1000199 CVE-2018-1000204) (Bug 47490)
- ***memcached*** (CVE-2016-8705 CVE-2017-9951 CVE-2018-1000115 CVE-2018-1000127) (Bug 47295)
- ***openjdk-8*** (CVE-2018-2952) (Bug 47577)
- ***openssh*** (CVE-2018-15473) (Bug 47629)
- ***patch*** (CVE-2018-1000156) (Bug 47485)
- ***perl*** (CVE-2018-12015) (Bug 47292)
- ***phonon-backend-vlc*** (Bug 47294)
- ***php7.0*** (CVE-2018-5712 CVE-2018-7584 CVE-2018-10545 CVE-2018-10546 CVE-2018-10547 CVE-2018-10548 CVE-2018-10549 CVE-2018-14884) (Bug 47491)
- ***postgresql-9.6*** (CVE-2018-1058 CVE-2018-1115 CVE-2018-10915 CVE-2018-10925) (Bug 47482)
- ***procps*** (CVE-2018-1122 CVE-2018-1123 CVE-2018-1124 CVE-2018-1125 CVE-2018-1126) (Bug 47296)
- ***python-django*** (CVE-2017-12794 CVE-2018-14574) (Bug 47502)
- ***qemu*** (CVE-2017-5715 CVE-2017-15038 CVE-2017-15119 CVE-2017-15124 CVE-2017-15268 CVE-2017-15289 CVE-2017-16845 CVE-2017-17381 CVE-2017-18043 CVE-2018-5683 CVE-2018-7550) (Bug 47303)
- ***reportbug*** (Bug 47506)

- ***rootskel-gtk*** (Bug 47090)
- ***ruby2.3*** (CVE-2017-17405 CVE-2017-17742 CVE-2017-17790 CVE-2018-6914 CVE-2018-8777 CVE-2018-8778 CVE-2018-8779 CVE-2018-8780 CVE-2018-1000073 CVE-2018-1000074 CVE-2018-1000075 CVE-2018-1000076 CVE-2018-1000077 CVE-2018-1000078 CVE-2018-1000079) (Bug 47500)
- ***samba*** (CVE-2018-1139 CVE-2018-10858 CVE-2018-10918 CVE-2018-10919) (Bug 47428)
- ***shared-mime-info*** (Bug 47483)
- ***subversion*** (Bug 47478)
- ***systemd*** (CVE-2017-15908) (Bug 47509)
- ***tzdata*** (Bug 47477)
- ***vlc*** (Bug 47294 Bug 47479)
- ***wireshark*** (CVE-2018-7320 CVE-2018-7334 CVE-2018-7335 CVE-2018-7419 CVE-2018-9261 CVE-2018-9264 CVE-2018-9273 CVE-2018-11358 CVE-2018-11360 CVE-2018-11362) (Bug 47284)
- ***xapian-core*** (CVE-2018-0499) (Bug 47489)
- ***xdg-utils*** (CVE-2017-18266) (Bug 47289)
- ***xerces-c*** (CVE-2017-12627) (Bug 47487)
- ***xml-security-c*** (Bug 47476)

- The following updated packages from Debian Stretch 9.5 are included (Bug 47659): ***2ping***, ***abiword***, ***adminer***, ***ant***, ***auto-complete-el***, ***awffull***, ***ax25-tools***, ***blender***, ***blktrace***, ***bouncycastle***, ***camo***, ***cffi***, ***cgit***, ***check-postgres***, ***chromium-browser***, ***clustershell***, ***debian-installer***, ***debian-installer-netboot-images***, ***debian-security-support***, ***dehydrated***, ***disc-cover***, ***django-xmlrpc***, ***dosbox***, ***dpdk***, ***dput-ng***, ***elastix***, ***email2trac***, ***faker***, ***fastkml***, ***ganeti***, ***git-annex***, ***glx-alternatives***, ***gosa***, ***gridengine***, ***insserv***, ***jdresolve***, ***jetty9***, ***kamailio***, ***keystone***, ***lava-server***, ***libb64***, ***libdate-holidays-de-perl***, ***libextractor***, ***liblouis***, ***libosmium***, ***llvm-toolchain-4.0***, ***local-apt-repository***, ***loook***, ***mailman***, ***miniupnpd***, ***mutt***, ***network-manager-vpnc***, ***nss-pam-ldapd***, ***nvidia-graphics-drivers***, ***obfsproxy***, ***openstack-debian-images***, ***php-horde-image***, ***piglit***, ***plexus-archiver***, ***psad***, ***pysurfer***, ***python-cluster***, ***python-pyorick***, ***python-scruffy***, ***r-cran-mi***, ***redis***, ***ruby-rack-protection***, ***ruby-sprockets***, ***rustc***, ***salt***, ***showq***, ***slurm-llnl***, ***source-highlight***, ***spip***, ***starplot***, ***strongswan***, ***sus***, ***symfony***, ***tclreadline***, ***thefuck***, ***thunderbird***, ***tinyproxy***, ***tlslite-ng***, ***tolua***, ***tomcat8***, ***unison***, ***variety***, ***vim-syntastic***, ***wordpress***, ***xen***, ***xrdp***, ***znc***

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- Update to Linux kernel 4.9.110-8 (Bug 47490).
- New micro code update for AMD CPUs (Bug 47616).
- New micro code update for Intel CPUs (Bug 47606, Bug 47669).

6.2.2. Univention Configuration Registry

Feedback

- Relax `dpkg` trigger execution to `noawait` when Univention Configuration Registry templates are installed or updated (Bug 47356).

6.2.2.1. Changes to templates and modules

Feedback

- The Univention Configuration Registry template for `/etc/rsyslog.conf` has been fixed. Modules configured by the Univention Configuration Registry variables `syslog/input/*` are now activated correctly (Bug 47035).
- Univention Configuration Registry `autostart` variables are now correctly evaluated across all scopes (Bug 46300).
- Some configuration values of `/etc/ssh/sshd_config` were not mapped to Univention Configuration Registry variables (Bug 39704).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- Fix regression in erratum 155: the OpenLDAP server fails to start during system setup when updates are already installed during installation (Bug 47452).
- Some debug message levels in LDAP overlays have been adjusted to more sensible values (Bug 47196).

6.3.1.1. LDAP schema changes

Feedback

- A LDAP schema of OX AppSuite is re-registered due to problems in the handling of the Univention App Center's *DefaultMasterPackages* (Bug 47581).

6.3.1.2. Listener/Notifier domain replication

Feedback

- Reconnect to LDAP server in case of an error (Bug 41514).

6.3.2. DNS server

Feedback

- The `BIND9` service is now a native `systemd` service and does not use `runsv` anymore (Bug 43689).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- The language sensitive sorting used in the grid via the `Intl.Collator` object is now used for other widgets as well (Bug 47195).
- Fixed a bug where the calendar widget would not display the date (Bug 47201).
- Some errors were not displayed correctly in the Inform vendor dialogs (Bug 47133).
- An error in the conversion of SVG to PNG images has been resolved (Bug 47188).

6.4.2. Univention Management Console server

Feedback

- Fix memory leak caused by Python notifier traceback handling (Bug 47114).

- During a release update, Apache will serve the maintenance page instead of UMC (Bug 37223).
- Enable bad password lockout policy in UMC (Bug 46978).
- A problem with the SAML authentification which could lead to the UMC web interface becoming unresponsive has been fixed (Bug 46870).

6.4.3. Univention App Center

Feedback

- The command `univention-app logs` has been introduced for Docker Apps (Bug 46433).
- The `univention-appcenter-listener-converter` has been fixed (Bug 47644).
- Fix memory leak caused by Python notifier traceback handling (Bug 47114).
- Docker Apps no longer have a default for the attribute that controls which command is used to start the container. If not given, the command specified during the build of the image will now be used (Bug 42970).
- The user `root` is used inside containers to run scripts (Bug 47340).
- Timezone setup during docker app installations has been fixed (Bug 47373).
- For processing asynchronous notifications the new service ***univention-appcenter-listener-converter*** has been added (Bug 47315).
- A new Univention Directory Listener module has been added to notify Apps when relevant objects change in LDAP (Bug 47265).
- Fix finding the wrong version in the App Cache. This issue could result in Apps being unregistered (Bug 47383).
- Fixed a bug that made the installation of certain Apps impossible when invoked from a remote server (Bug 47158).
- Certain Apps could not be upgraded when installed on a non-Master system (Bug 47253).
- Improved cache performance of the App Center (Bug 46821).
- The command `univention-app` took every App from every UCS version into consideration. Now non-Docker Apps are excluded when the UCS version of the App and the one of the system do not match (Bug 47187).

6.4.4. Univention Directory Manager UMC modules and command line interface

Feedback

- The property *Account is deactivated* of an user object was wrongly considered to be empty and resulted in a notification in the UMC (Bug 47199).
- Ignore case during change of attribute *mailPrimaryAddress* on user objects (Bug 47415).
- Add support for DNS `NS` records (Bug 32626).

6.4.5. Modules for system settings / setup wizard

Feedback

- Warn about already existing hostname when joining the system to the domain (Bug 46045).

- Raise the required memory for UCS to 1 GB (Bug 45206).
- Fix memory leak caused by Python notifier traceback handling (Bug 47114).
- Warn about unreachable repository servers when configuring the system (Bug 47105).
- Detect potential problems with the domain join when configuring the system (Bug 42022).
- Improve error messages of join failures (Bug 42366).
- Clarification what kind of updates are installed on the last page of the Univention System Setup (Bug 45931).

6.4.6. Software update module

Feedback

- During a release update Univention Management Console will no longer be accessible. Instead a minimalistic web page informs about the progress of the update. UMC will be available again as soon as the update finished (Bug 37223).

6.4.7. Domain join module

Feedback

- Exit samba slave PDC join scripts early if the system is not a UCS@school slave (Bug 47234).
- Fix memory leak caused by Python notifier traceback handling (Bug 47114).
- Add option to the `univention-join` tool for checking problems without altering the system (Bug 42022).
- Improve error messages of join failures (Bug 42366).
- `univention-server-join` now checks and reports conflicts in name, role, MAC and IP address to provide better error feedback (Bug 42124).

6.4.8. System diagnostic module

Feedback

- Only show `samba-tool dbcheck` errors as critical (Bug 46197).

6.4.9. Other modules

Feedback

- Fix UMC crashing on system time change (Bug 44222).

6.5. Univention base libraries

Feedback

- The new Univention Configuration Registry variable `ldap/attributeoptions` has been added to configure the `slapd.conf` `attributeoptions` parameter. The default for `attributeoptions` has changed from `entry-` to `entry-,lang-` (Bug 47246).
- Some debug message levels in LDAP overlays have been adjusted to more sensible values (Bug 47196).
- Protect code of `getMailFromMailOrUid` from execution on module load (Bug 47206).

6.6. Software deployment

Feedback

- Show a warning and allow examination of the `updater.log` file in UMC if the last release update failed (Bug 47592).

- The progress of a release update is written to a status file so that the package ***univention-maintenance-mode*** may read it to update the progress accordingly (Bug 37223).
- Code for the deprecated UCS-2.x and UCS-3.x repository layout has been removed (Bug 36719).
- Network errors while trying to contact the update server do not result in a traceback anymore. Instead, a readable error message is shown (Bug 41536).

6.7. System services

Feedback

6.7.1. PostgreSQL

Feedback

- Use `deb-systemd-invoke stop "postgresql@$ver-*"` to prevent upgrading/removing server packages from stopping other major version clusters when running `systemd`. (Use `deb-systemd-invoke` instead of `invoke-rc.d`; Jessie's `invoke-rc.d` does not support service patterns.) (Bug 47511).

6.7.2. Docker

Feedback

- During the initial setup by Univention System Setup the package gets always installed inside the `chroot` environment. `systemd` is not yet used there, but the legacy SysV init scripts. Its stop action reports an error as the daemon is not running. This aborts the removal of the package, which is done when setting up a Base system (Bug 47194).

6.7.3. SAML

Feedback

- Raw service provider configurations can now be added to Univention Directory Manager `saml/serviceprovider` objects. The configuration will be replicated to all domain IdP servers. In addition, the configuration option of ***simplesamlphp*** LDAP *get_attributes* is now done in LDAP. The current value set to the Univention Configuration Registry variables is migrated to the updated configuration (Bug 47309).
- When operating Apache without a separate *VirtualHost* entry for single sign-on, a *rewrite* rule in the scope of other configuration rules limited execution of further rewrite rules. This fix restricts the rewrite rule to the single sign-on directory (Bug 47241).

6.7.4. Dovecot

Feedback

- The PAM stack has been fixed to allow the login via username (Bug 47642).

6.7.5. Postfix

Feedback

- The PAM stack has been fixed to allow the login via username (Bug 47642).

6.7.6. Nagios

Feedback

- A Nagios warning for CUPS due to usage of `HTTP/1.0` has been fixed (Bug 46698).

6.7.7. Proxy services

Feedback

- Setting the Univention Configuration Registry variable `squid/krb5auth/keepalive` to `off` did not have any effect (Bug 47425).

6.7.8. SSL

Feedback

- Update Mozilla certificate authority bundle to version 2.22 (Bug 47480).

6.8. Virtualization

Feedback

6.8.1. UCS Virtual Machine Manager (UVMM)

Feedback

- Make CPU-Usage column visibility configurable. The visibility is controlled by the Univention Configuration Registry variable `uvmm/umc/showcpuusage` (Bug 47268).
- Snapshots can now be created from the context menu of the grid overview (Bug 41772).
- The hosts in the dialog Migrate domain are now sorted (Bug 47182).
- Update to VirtIO driver for Windows to version 0.1.141-1 (Bug 47321).
- Fix a memory leak preventing the Python garbage collector from freeing connection instances (Bug 47114).

6.9. Services for Windows

Feedback

6.9.1. Samba

Feedback

- Update package ***tevent*** to version 0.9.36 as required by Samba 4.7.8 (Bug 47428).
- Adjust default for Univention Configuration Registry variable `samba/ntlm/auth` (`ntlm auth`) to `ntlmv2-only` (Bug 46782).
- Share options in ***univention-samba-local-config*** have been fixed (Bug 46975).
- Some scripts have been restored, that were deleted by a previous cleanup (Bug 47095).
- After a server password change restart all services of Samba, not just the AD/DC component (Bug 47638).
- Two new Univention Configuration Registry variables have been added to give more granular control over the behavior of the SYSVOL synchronization:

  `samba4/sysvol/sync/from_upstream/delete` — control whether a downstream DC should delete local changes during the synchronization from the upstream DC (only useful in UCS@school with unidirectional synchronization from upstream DC).

  `samba4/sysvol/sync/fix_gpt_ini` — control whether old, redundant `gpt.ini` files should be deleted after the synchronization to the local SYSVOL directory (Bug 47576).

- Improved error message for UCS@school slave join (Bug 47388).
- Continue `samba-tool dbcheck --fix` even if a modification failed (Bug 45982).

6.9.2. Univention S4 Connector

Feedback

- When objects are renamed in UCS update their DN in the group member mapping caches (Bug 47636).
- Sync *pwdLastSet* changes also in case the hashes didn't actually change (Bug 47391).

- Add support for DNS `NS` records (Bug 32626).

6.9.3. Univention Active Directory Connection

Feedback

- The connector's AD binary attributes list has been updated (Bug 47025).
- A regression of Bug 45779 affecting the AD connection wizard has been fixed (Bug 47430).
- Four new tools have been added: `resync_object_from_ad.py`, `resync_object_from_ucs.py`, `remove_ad_rejected.py`, `remove_ucs_rejected.py` (Bug 47232).
- The listener module now restarts the connector if extended attributes are modified (Bug 47049).