univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-2

Release 5.0-2

Nov 04, 2022

CONTENTS

CHAPTER

ONE

GENERAL

- Various unused Python 2 modules has been removed from the Debian packages (Bug #54706).
- The server password change mechanism has been adjusted to first validate that the new machine password successfully replicated in OpenLDAP before finally changing the password locally in Samba/AD. Quickly reverting password changes in AD easily breaks DRS replication, so prevent this situation from happening (Bug #53205).
- All security updates issued for UCS 5.0-1 are included:
  - **apache2** (CVE-2021-44224, CVE-2021-44790) (Bug #54298)
  - **bind9** (CVE-2021-25220) (Bug #54573)
  - **cifs-utils** (CVE-2022-27239, CVE-2022-29869) (Bug #54818)
  - **clamav** (CVE-2022-20698) (Bug #54599)
  - **cups** (CVE-2020-10001, CVE-2022-26691) (Bug #54598, Bug #54808)
  - **cyrus-sasl2** (CVE-2022-24407) (Bug #54490)
  - **dpkg** (Bug #54810)
  - **expat** (CVE-2021-45960, CVE-2021-46143, CVE-2022-22822, CVE-2022-22823, CVE-2022-22824, CVE-2022-22825, CVE-2022-22826, CVE-2022-22827, CVE-2022-23852, CVE-2022-23990, CVE-2022-25235, CVE-2022-25236, CVE-2022-25313, CVE-2022-25314, CVE-2022-25315) (Bug #54448, Bug #54480)
  - **firefox-esr** (CVE-2021-4140, CVE-2021-38503, CVE-2021-38504, CVE-2021-38506, CVE-2021-38507, CVE-2021-38508, CVE-2021-38509, CVE-2021-43534, CVE-2021-43535, CVE-2021-43536, CVE-2021-43537, CVE-2021-43538, CVE-2021-43539, CVE-2021-43541, CVE-2021-43542, CVE-2021-43543, CVE-2021-43545, CVE-2021-43546, CVE-2022-1097, CVE-2022-1196, CVE-2022-1529, CVE-2022-1802, CVE-2022-22737, CVE-2022-22738, CVE-2022-22739, CVE-2022-22740, CVE-2022-22741, CVE-2022-22742, CVE-2022-22743, CVE-2022-22745, CVE-2022-22747, CVE-2022-22748, CVE-2022-22751, CVE-2022-22754, CVE-2022-22756, CVE-2022-22759, CVE-2022-22760, CVE-2022-22761, CVE-2022-22763, CVE-2022-22764, CVE-2022-24713, CVE-2022-26381, CVE-2022-26383, CVE-2022-26384, CVE-2022-26386, CVE-2022-26387, CVE-2022-26485, CVE-2022-26486, CVE-2022-28281, CVE-2022-28282, CVE-2022-28285, CVE-2022-28286, CVE-2022-28289, CVE-2022-29909, CVE-2022-29911, CVE-2022-29912, CVE-2022-29914, CVE-2022-29916, CVE-2022-29917, CVE-2022-31736, CVE-2022-31737, CVE-2022-31738, CVE-2022-31740, CVE-2022-31741, CVE-2022-31742, CVE-2022-31747) (Bug #54345, Bug #54442, Bug #54512, Bug #54543, Bug #54654, Bug #54730, Bug #54787, Bug #54819)
  - **flac** (CVE-2020-0499) (Bug #54608)
  - **ghostscript** (Bug #54314)
  - **gmp** (CVE-2021-43618) (Bug #54602)
  - **gzip** (CVE-2022-1271) (Bug #54672)
  - **intel-microcode** (CVE-2021-0127, CVE-2021-0145, CVE-2021-33120) (Bug #54605)

- **jbig2dec** (CVE-2020-12268) (Bug #54610)
- **libpcap** (CVE-2019-15165) (Bug #54601)
- **libxml2** (CVE-2022-23308, CVE-2022-29824) (Bug #54609, Bug #54788)
- **linux**, **linux-latest**, **linux-signed-amd64**, (CVE-2020-29374, CVE-2020-36322, CVE-2021-3640, CVE-2021-3744, CVE-2021-3752, CVE-2021-3760, CVE-2021-3764, CVE-2021-3772, CVE-2021-4002, CVE-2021-4083, CVE-2021-4135, CVE-2021-4149, CVE-2021-4155, CVE-2021-4202, CVE-2021-4203, CVE-2021-20317, CVE-2021-20321, CVE-2021-20322, CVE-2021-22600, CVE-2021-28711, CVE-2021-28712, CVE-2021-28713, CVE-2021-28714, CVE-2021-28715, CVE-2021-28950, CVE-2021-38300, CVE-2021-39685, CVE-2021-39686, CVE-2021-39698, CVE-2021-39713, CVE-2021-41864, CVE-2021-42739, CVE-2021-43389, CVE-2021-43975, CVE-2021-43976, CVE-2021-44733, CVE-2021-45095, CVE-2021-45469, CVE-2021-45480, CVE-2022-0001, CVE-2022-0002, CVE-2022-0322, CVE-2022-0330, CVE-2022-0435, CVE-2022-0487, CVE-2022-0492, CVE-2022-0617, CVE-2022-0644, CVE-2022-22942, CVE-2022-23036, CVE-2022-23037, CVE-2022-23038, CVE-2022-23039, CVE-2022-23040, CVE-2022-23041, CVE-2022-23042, CVE-2022-23960, CVE-2022-24448, CVE-2022-24958, CVE-2022-24959, CVE-2022-25258, CVE-2022-25375, CVE-2022-26966) (Bug #54541, Bug #54607)
- **lxml** (CVE-2021-43818) (Bug #54346)
- **mariadb-10.3** (CVE-2021-35604, CVE-2021-46659, CVE-2021-46661, CVE-2021-46662, CVE-2021-46663, CVE-2021-46664, CVE-2021-46665, CVE-2021-46667, CVE-2021-46668, CVE-2022-24048, CVE-2022-24050, CVE-2022-24051, CVE-2022-24052) (Bug #54604)
- **nbd** (CVE-2022-26495, CVE-2022-26496) (Bug #54542)
- **nss** (CVE-2022-22747) (Bug #54375)
- **ntfs-3g** (CVE-2021-46790, CVE-2022-30783, CVE-2022-30784, CVE-2022-30785, CVE-2022-30786, CVE-2022-30787, CVE-2022-30788, CVE-2022-30789) (Bug #54857)
- **openldap** (CVE-2022-29155) (Bug #54627, Bug #54783)
- **openssl** (CVE-2021-4160, CVE-2022-0778, CVE-2022-1292, CVE-2022-2068) (Bug #54557, Bug #54764, Bug #54901)
- **pillow** (CVE-2022-22815, CVE-2022-22816, CVE-2022-22817) (Bug #54366)
- **policykit-1** (CVE-2021-4034) (Bug #54374)
- **postgresql-11** (CVE-2022-1552) (Bug #54751)
- **rsyslog** (CVE-2019-17041, CVE-2019-17042, CVE-2022-24903) (Bug #54600, Bug #54809)
- **samba** (CVE-2021-43566, CVE-2021-44142, CVE-2022-0336) (Bug #53629, Bug #54015, Bug #54200, Bug #54278, Bug #54369)
- **squid** (CVE-2021-28116, CVE-2021-46784) (Bug #54907)
- **tiff** (CVE-2022-0561, CVE-2022-0562, CVE-2022-0865, CVE-2022-0891, CVE-2022-0907, CVE-2022-0908, CVE-2022-0909, CVE-2022-0924, CVE-2022-22844) (Bug #54595)
- **vim** (CVE-2019-20807, CVE-2021-3770, CVE-2021-3778, CVE-2021-3796) (Bug #54606)
- **xorg-server** (CVE-2021-4008, CVE-2021-4009, CVE-2021-4010, CVE-2021-4011) (Bug #54270)
- **xterm** (CVE-2022-24130) (Bug #54603)
- **xz-utils** (CVE-2022-1271) (Bug #54671)
- **zlib** (CVE-2018-25032) (Bug #54631)

- The following updated packages from Debian 10.12 are included (Bug #54866): **aide**, **apache-log4j1.2**, **apache-log4j2**, **atftp**, **base-files**, **beads**, **btrbk**, **cargo-mozilla**, **chrony**, **cimg**,

condor, **debian-edu-config**, **debian-installer-netboot-images**, **debian-installer**, **detox**, **djvulibre**, **ecdsautils**, **evolution-data-server**, **exo**, **faad2**, **ffmpeg**, **firejail**, **gerbv**, **glibc**, **graphicsmagick**, **h2database**, **htmldoc**, **http-parser**, **icu**, **ipython**, **jtharness**, **jtreg**, **lemonldap-ng**, **leptonlib**, **libdatetime-timezone-perl**, **libencode-perl**, **libetpan**, **libextractor**, **libjackson-json-java**, **libmodbus**, **libphp-adodb**, **librecad**, **libsdl1.2**, **lighttpd**, **llvm-toolchain-11**, **lrzip**, **lxcfs**, **mailman**, **mediawiki**, **modsecurity-apache**, **needrestart**, **node-getobject**, **openjdk-11**, **openscad**, **opensc**, **php-illuminate-database**, **phpliteadmin**, **plib**, **privoxy**, **prosody**, **publicsuffix**, **python-bottle**, **python-virtualenv**, **raptor2**, **redis**, **ros-ros-comm**, **roundcube**, **ruby2.5**, **ruby-httpclient**, **rust-cbindgen**, **rustc-mozilla**, **smarty3**, **snapd**, **sogo**, **sphinxsearch**, **spip**, **strongswan**, **subversion**, **thunderbird**, **trafficserver**, **tryton-proteus**, **tryton-server**, **tzdata**, **uriparser**, **usbview**, **varnish**, **vlc**, **waitress**, **wavpack**, **webkit2gtk**, **weechat**, **wireshark**, **wordpress**, **zsh**, **zziplib**,

- The following packages have been moved to the maintained repository of UCS: **python-jose** (Bug #54666), **python-keycloak** (Bug #54689), **univention-support-info**, (Bug #53358)

CHAPTER

TWO

UNIVENTION INSTALLER

- Remove left-over static host configuration for `127.0.1.1` (Bug #49042).

CHAPTER

THREE

BASIC SYSTEM SERVICES

3.1 Univention Configuration Registry

- Adapted the code due to a Linux kernel API change in *v5.7-rc1~128*, where `open(O_EXCL)` now returns `EEXIST`, instead of `EISDIR` (Bug #54476).
- The remaining scripts have all been migrated to Python 3 (Bug #54208).
- The Python-API of Univention Configuration Registry has been extended to offer a method `get_int()`, that can be used to avoid receiving a string, when an integer is required. If the value of the requested Univention Configuration Registry Variable is not a number, the default value is returned verbatim instead (Bug #20933).

3.1.1 Changes to templates and modules

- The Univention Configuration Registry template for the file `/etc/hosts`, now always produces the same output given the same configuration (Bug #54558).
- Clarified the description of the Univention Configuration Registry Variable `logrotate/rotate/count` (Bug #54691).

CHAPTER

FOUR

DOMAIN SERVICES

4.1 OpenLDAP

- The `ppolicy` overlay module uses embedded Python. This has been migrated to Python 3 (Bug #54582).
- The behavior of the `translog` overlay was modified to skip grandchildren of the `cn=temporary, cn=univention`, container. This new behavior can be controlled by the Univention Configuration Registry Variable `ldap/translog-ignore-temporary`. This reduces the number of replication transactions during creation of users and groups significantly. As a result it increases the replication performance and reduces the rate at which the `cn=translog` LMDB backend database gets filled. This variable is applicable only to the Primary Directory Node. The package **`univention-ldap-server`** activates this variable by default (Bug #48626).

4.1.1 Listener/Notifier domain replication

- An error when deactivating a listener module through UCR has been fixed (Bug #54696).
- `univention-translog import --min` *`TID`* had no effect (Bug #54794).
- Several memory issues have been fixed (Bug #49868).
- The Notifier sometimes failed to process all transaction in bulk and aborted. This lead to the Notifier making no progress and filling the log file with the same error messages again and again. Transactions are now processes incrementally (Bug #49868).
- If the number of transactions was lower than 1000, only a partial number of transactions has been imported during the join of a backup (Bug #54203).

4.2 DNS server

- The Univention Configuration Registry Variable `dns/timeout-start` is now also considered in the `systemd` unit `univention-bind-ldap`. This can be used in cases where a large number of DNS zones slows down the start of the DNS server bind. This only affects systems which have `dns/backend` set to `ldap`. i.e. systems that are not configured as Samba/AD DC. After changing the variable, running **`systemctl daemon-reload`** once is required (Bug #54108).

4.3 Univention Directory Listener

- The unused method `get_configuration()` has been removed from the `ListenerModuleConfiguration` class in the `univention.listener.handler_configuration` module (Bug #54501).

CHAPTER

FIVE

UNIVENTION MANAGEMENT CONSOLE

5.1 Univention Management Console web interface

- A new widget suggesting mail domains while typing has been introduced (Bug #54467).
- The logic for mapping UDM syntax classes to UMC front end widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug #38762).
- The domain component in an LDAP path is not shown in wrong reversed order anymore (Bug #53678).
- In case of a long-lasting login, certain UMC modules do not work properly. If this happens, a message will be displayed to the user containing a link to KB 6413 (Bug #54032).
- A new method has been added to generate and set a service specific password for a user (Bug #54438).
- The UDM REST API now supports UDM object types containing - in their name (Bug #54063).
- The `entryUUID` and `dn` of newly created objects are now included in the response (Bug #54347).
- The UDM REST API now supports multiprocessing via the Univention Configuration Registry Variable `directory/manager/rest/processes`. Further details can be found in the performance guide (Bug #50050).

5.2 Univention Portal

- The Portal server now fetches user information from the UMC server asynchronously (Bug #53853).
- Fixed various accessibility issues (Bug #54556).
- Fixed various CSS issues (Bug #54556).
- Added new tooltips. They comply with accessibility requirements (Bug #54556).
- Improved the translation widget when editing portal entries (Bug #54556).
- Fixed drag and drop behavior when using the keyboard, added screen reader support (Bug #54556).
- The portal now integrates the self service functionality: Reset passwords, change profile, verify accounts, etc is now possible from within the portal (Bug #54556).
- The French translation of UDM portal attributes has been updated (Bug #54029).
- Some requests have been excluded from `apache2/force_https`, so that the portal tiles in the UMC are shown even if https is forced (Bug #53296).
- The Portal server now provides a navigation endpoint (Bug #54618).
- Keywords can now be added to portal entries. They are not visible, but searchable (Bug #54295).
- Entries can now be opened in new tabs with a specific internal name (“target”) (Bug #54633).

5.3 Univention Management Console server

- The function `DNSanitizer()` has been added to the Python module variable `__all__` to prevent warnings for developers (Bug #52445).
- The cookie attribute `SameSite` can now be set for UMC cookies via the Univention Configuration Registry Variable `umc/http/cookie/samesite` (Bug #54484).
- **`univention-management-console-dev`** now depends on both **`imagemagick`** and **`inkscape`** (Bug #54043).

5.4 Univention App Center

- The reason why servers are excluded from the app-installation drop-down menu is displayed again (Bug #54460).
- Change order and prioritize App specific settings over App Center settings when populating the environment file. This is required for some upcoming Apps to be installed (Bug #54612).
- Allow for the `tmpfs`, that are created for a docker app to be defined in the apps ini file (Bug #54562).
- A race condition was fixed, that caused apps to lose their installation status (Bug #54452).
- Validate the form when choosing the installation host (Bug #53523).
- Make the check regarding network conflicts with docker more robust (Bug #54082).

5.5 Univention Directory Manager UMC modules and command line interface

- The mapping of syntax class to UMC widgets via the Univention Configuration Registry Variable `directory/manager/web/widget/.*` has been removed. This can now be achieved via syntax classes directly (Bug #54840).
- An error introduced in UCS 5.0 erratum 335 has been repaired which caused that e.g. the selection list of printer model in the printer shares module could not be fetched (Bug #54849).
- The error handling of the syntax class `jpegPhoto` was broken since UCS 5.0-0 and has been repaired (Bug #54769).
- Clarified error message for invalid host name or FQDN (Bug #54663).
- The available mail domains are now suggested when entering values for the attribute `mailPrimaryAddress` of objects `users/user` (Bug #54467).
- Syntax classes can now depend on another UDM property and restrict their choices based on that (Bug #53843).
- The logic for mapping UDM syntax classes to UMC front end widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug #38762).
- A crash while accessing an user with multiple user certificates has been repaired (Bug #54617).
- Changing the case of the name or email attributes will no longer be prevented by the locking mechanism (Bug #52760).
- Some redundant log messages logging password hashes were removed (Bug #54348).
- The performance of the license check has been improved to reduce the initial login time (Bug #52292).
- Backend functionality for service specific passwords has been added. It cannot be used via CLI (Bug #54438).
- When removing a policy the policy is removed from the referencing objects (Bug #16966).

- Searching with patterns containing umlauts is possible again (Bug #53975).
- It is now possible to search for the user expiry date of `users/user` objects (Bug #54150).
- Two resource sharing conflicts on Python dictionaries have been fixed, that could lead to tracebacks when modules are reloaded in a multi-threaded context (Bug #53581).
- Moving of `users/ldap` objects is possible again. This was broken due to the Python 3 migration in UCS 5.0 (Bug #54085).
- When user templates were members of groups an error was raised which prevented opening or modifying that group. Templates as group members are now ignored in UDM module `groups/group`, (Bug #54402).
- When setting an user as a member of a group in UDM, that had the same UID but a different DN of another member, the related attribute `memberUid` of the group got dropped. This happened in the cool Solution user-group-sync during move operations (Bug #54297).
- The French translation of UDM extended attributes has been updated (Bug #54029).
- The `entryUUID` of an LDAP object is now exposed by the UDM API (Bug #54883).

5.6 Modules for system settings / setup wizard

- The package **univention-system-setup** has been migrated to Python 3 (Bug #51318).

5.7 Domain join module

- When executing join scripts via UMC module `Domain Join` the progress bar will now display the name of the currently running script instead of the last script that was finished (Bug #33255).
- The joinscript of **univention-samba4** did pass the credentials in clear text to other tools like **ldb-search** as command line arguments. To reduce the attack surface it now uses a file instead (Bug #53100).
- Joining a backup node into a single server UCS@school environment failed because the LDB module `univention_samaccountname_ldap_check`, attempted to create an object of type `computers/windows` for it which always failed because the account name was already taken by the `computers/domaincontroller_backup` object (Bug #54768).
- Several memory and open file descriptor leaks have been fixed. An error restarting Samba during package installation has been fixed. The build system for the package has been cleaned up (Bug #48823).

5.8 Univention Directory Reports

- The script **univention-directory-reports** now offers two new options: The option `--output-dir` allows specification of the output directory and `--output-name` allows to specify the file name of the report (Bug #54153).

5.9 System diagnostic module

- A new diagnostic plugin has been added to detect cases where the group membership attributes `uniqueMember` and `memberUid` are no longer consistent (Bug #48652).
- `52_mail_acl_sync` will no longer fail if multiple IMAP mail folders exist (Bug #54675).
- A new diagnostic plugin has been added to detect cases where an LDAP schema is missing that is actually still referenced by some objects (Bug #53455).
- The script **`univention-run-diagnostic-check`** now displays links in the description of failed tests (Bug #50756).
- Disk usage checks will now handle log level evaluations of Univention Configuration Registry Variable `ldap/debug/level` correctly (Bug #49354).
- A diagnostic warning for the Samba replication status will now be formatted properly (Bug #53341).
- Mounted ISO images are no longer included in the disk usage diagnostic plugin (Bug #49353).
- The Python 3 compatibility when handling exceptions in certain diagnostic plugins has been corrected (Bug #53306).
- A diagnostic module has been added to check the Univention Configuration Registry Variable `notifier/protocol/version`, (Bug #54264).
- **`univention-run-diagnostic-checks`** now offers to run a group of tests and also to exclude some of the tests (Bug #53969).
- The script **`univention-run-diagnostic-check`** is now executed with machine account credentials by default (Bug #54515).
- The detection of **`slapschema`** error message has been improved in **`62_check_slapschema`**, (Bug #54681).

5.10 File system quota module

- Setting quotas for accounts with a fully numeric username has been fixed (Bug #54638).

5.11 Other modules

- Syntax classes can now depend on another UDM property and restrict their choices based on that (Bug #53843).
- The logic for mapping UDM syntax classes to UMC front end widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug #38762).
- A UMC operation set enabling the creation of UDM Reports was added (Bug #54109).
- Byte values are now correctly decoded for the labels of choices delivered by the syntax class `LDAP_Search`, (Bug #54190).
- The domain component in a LDAP path is not shown in wrong reversed order anymore (Bug #53678).
- The Univention Configuration Registry Variable `directory/manager/web/modules/users/user/wizard/property/ invite/default` will now work properly and can be used to activate the *invite user via e-mail* option in the user wizard by default (Bug #54316).

CHAPTER

SIX

UNIVENTION BASE LIBRARIES

- Detecting UMC specific files did not work for packages having files, which have blanks in their filenames. This lead to error messages during package upgrades and inconsistent cache behavior (Bug #54047).
- `UCSVersion` not includes the erroneous input parameter is included in the error message for debugging (Bug #49061).
- Added the new function `generate_password()` that can generate random passwords. The new function `password_config()` can be used to get parameters for that from UCR (Bug #54555).
- Changing a user password is now possible again when the referenced password history policy did not define values for password length or history length (Bug #51354).
- For **`Python-ldap-3.3.0`** (and higher) some TLS settings are no longer immediately materialized. To ensure correct behavior of TLS encrypted LDAP connections, the option `OPT_X_TLS_NEWCTX` will be necessary for future UCS versions (Bug #54408).

CHAPTER

SEVEN

SOFTWARE DEPLOYMENT

- **univention-upgrade --updateto** is parsed earlier and exits on wrong parameter (Bug #49061).
- **apt-get --force-yes** option is deprecated and has been replaced with `--allow-unauthenticated`, `--allow-downgrades` `--allow-remove-essential`, `--allow-change-held-packages` (Bug #48891).
- App updates invoked by **univention-upgrade** will now work correctly (Bug #53666).

CHAPTER

EIGHT

SYSTEM SERVICES

8.1 PostgreSQL

- During the upgrade to UCS 5.0-1 PostgreSQL 11 might have been disabled by setting the Univention Configuration Registry Variable `postgres11/autostart=no` by accident (Bug #54255).

8.2 Docker

- The script **`migrate_container_MountPoints_to_v2_config`** is deprecated since UCS 4.3 and has been removed (Bug #52539).
- The package **`univention-docker-container-mode`** is deprecated since UCS 4.3 and has been replaced by an empty transitional package (Bug #52539).

8.3 SAML

- The cookie attributes `Secure` and `SameSite` can now be set for the session and language cookies of SAML Identity Providers via Univention Configuration Registry Variable `saml/idp/session-cookie/secure`, `saml/idp/session-cookie/samesite`, `saml/idp/language-cookie/secure` and `saml/idp/language-cookie/samesite`, (Bug #54483).
- The link to the self service has been changed to point to the new portal based self service (Bug #54556).
- An internal ID has been fixed, which caused the German translation not being shown when new passwords did not match (Bug #54268).
- The French translation of UDM extended attributes has been updated (Bug #54029).

8.4 Univention self service

- The logic for mapping UDM syntax classes to UMC front end widgets and to get the dynamic choices for a UDM syntax have been moved into the UDM syntax classes (Bug #38762).
- The Self Service now adds its dedicated portal to make use of the new features in Univention Portal. For more, see Univention Help 19671 (Bug #54556).
- A new backend function has been added that can set service specific passwords for a user (Bug #54434).
- The e-mail template for password reset tokens now support additional placeholders for the properties `title`, `initials`, `displayName`, `firstname`, `lastname`, `mailPrimaryAddress`, `employeeNumber` and `organisation` (Bug #48960).
- The package has been migrated to Python 3. Custom plugins for sending the password recovery tokens also need to be migrated to Python 3 (Bug #51327, Bug #54466).

- The French translation of UDM extended attributes and portal attributes has been updated (Bug #54029).

8.5 Mail services

- The French translation of UDM extended attributes has been updated (Bug #54029).
- A bug where antivirus signatures could not get updated properly on fresh installations has been fixed (Bug #54070).

8.6 Dovecot

- The French translation of UDM extended attributes has been updated (Bug #54029).

8.7 Postfix

- Error handling in the script `/usr/share/univention-mail-postfix/listfilter.py`, has been repaired (Bug #54560).

8.8 Monitoring / Nagios

- A new monitoring system has been implemented based on **`Prometheus`**, **`Prometheus Alertmanager`** and **`Grafana`**. During the upgrade all current Nagios services are migrated to Monitoring alerts (Bug #54748, Bug #54749, Bug #54750).
- The configuration of NRPE plugin definitions was broken due to the migration to Python 3 and has been repaired (Bug #53681).
- The Nagios plugins in **`univention-nagios-client`**, have been converted to Python 3 (Bug #52258).

8.9 Apache

- Apache can now be configured to only support TLS v1.3 connections by setting the Univention Configuration Registry Variable `ucr set apache2/ssl/tlsv13=true`, (Bug #54306).

8.10 RADIUS

- The RADIUS server can now assign VLAN IDs to user connections if their group has set the attribute `vlanId`. The Univention Configuration Registry Variable `freeradius/vlan-id` has been added to set a VLAN ID even if the user is no member of any such group (Bug #25916).
- A new Univention Configuration Registry Variable `radius/use-service-specific-passwords.` has been added: If enabled, the authentication is done against a RADIUS specific password, not the domain password of the user (Bug #54409).
- An error while adding the French translation to an extended attribute during the package update has been fixed (Bug #54461).
- The French translation of UDM extended attributes has been updated (Bug #54029).
- Updating an old RADIUS installation will now correctly update the description for the extended attributes `networkAccessGroups` and `NetworkAccessComputers`, (Bug #54341).

8.11 Proxy services

- The package **univention-squid** has been migrated to Python 3 (Bug #53357).

8.12 Kerberos

- The Kerberos ticket lifetime was made configurable via Univention Configuration Registry Variable `kerberos/defaults/ticket-lifetime`, (Bug #52987).

8.13 SSL

- Some web browsers refused wildcard certificates generated by **univention-certificates** because the information was only stored in `common name` but required in `subject alternative names`, too (Bug #53288).

8.14 DHCP server

- Add UCR packages to profile for network installation (Bug #54259).

CHAPTER

NINE

SERVICES FOR WINDOWS

9.1 Samba

- Samba has been updated to version 4.16.2 (Bug #54682).
- In some cases, in UCS@school the `log.smbd`, filled with a message because a Windows 10 client attempted to access user files, which is denied by the NTACLs. While the origin of that behavior is still unknown, no negative side effects are known. To avoid overflowing the log file, we adjusted the log message to only start appearing at the debug level 2. Default log level is 1 (Bug #52979).
- **samba-tool** now supports passing credentials using the option `--authentication-file` and the machine password using the option `--machinepass-file` (Bug #53101).
- The share configuration of `vfs objects`, `write list`, `hosts allow` and `hosts deny` was broken because of too excessive escaping of quotes and has been repaired (Bug #49842).
- The share setting `map acl inherit = yes` has been broken since UCS 5.0-0 and is not working properly again (Bug #54688).
- The access to home shares via NTLM authentication on UCSMEMBER has been fixed (Bug #54200).
- The joinscript of **univention-samba4** did pass the credentials in clear text to other tools like **ldbsearch** as command line arguments. To reduce the attack surface it now uses a file instead (Bug #53100).
- During a server password change the Samba process was not restarted in some cases. The script to restart Samba was fixed to ensure the service is restarted successfully (Bug #54356).
- The Kerberos ticket lifetime was made configurable via Univention Configuration Registry Variable `kerberos/defaults/ticket-lifetime`, (Bug #52987).

9.2 Univention AD Takeover

- **samba-tool** now supports passing machine password using the option `--machinepass-file` (Bug #53101).
- **samba-tool** now supports passing credentials using the options `-A | --authentication-file` (Bug #53101).
- Performing an Active Directory takeover will work when the original AD contains Group Policy Objects that use non ASCII encoding (Bug #54196).
- Invalid (empty) UCR network interface configuration lead to network failure during AD Takeover (Bug #54359).
- On systems updated from UCS 4.4 the AD-Takeover could abort with a traceback because the **systemctl** command was not found under the path specified in the Python code (Bug #54238).

9.3 Univention S4 Connector

- The user expiry was off by one day between UCS and Samba. This discrepancy has been removed (Bug #53012).

9.4 Univention Active Directory Connection

- For **`Python-ldap-3.3.0`** (and higher) some TLS settings are no longer immediately materialized. To ensure correct behavior of TLS encrypted LDAP connections, the option `OPT_X_TLS_NEWCTX` will be necessary for future UCS versions (Bug #54408).

CHAPTER

TEN

OTHER CHANGES

- Improve message consistency between the man page and the `--help` messages (Bug #54588).
- Fix spelling mistake of **`rsync`** in `doc/univention-ssh.8`, (Bug #54588).
- Update the **`univention-scp --help`** and **`univention-rsync`** message to specify that the `--no-split` option must be set before the password file parameter (Bug #54588).
- Added support for RFC6265bis *SameSite* cookie attribute (Bug #54483).
- Fixed Python 2 compatibility of UCR template `slapd.conf.d/65admingrp-user-passwordreset`, introduced by UCS 5.0 erratum 308 (Bug #54790).
- The start of OpenLDAP could fail if the ACL lines got too long. This could happen if the Univention Configuration Registry Variable `ldap/acl/user/passwordreset/.*` have a lot of values (Bug #54744).
- The group membership cache now returns an empty list instead of None when requesting non-existing keys. This fixes a traceback in the Microsoft 365 connector listener, when not every `ADConnectionAlias` has at least one user (Bug #54572).
- The French translation of UDM extended attributes has been updated (Bug #54029).
- A new attribute `univentionRadiusPassword` has been added to the user class (Bug #54395).
- The French translation of UDM extended attributes has been updated (Bug #54029).
- A new Univention Configuration Registry Variable `ldap/translog-ignore-temporary` has been created to control if UDM temporary objects should be considered for replication by the OpenLDAP `translog`, overlay which feeds the Listener/Notifier. This reduces the number of replication transactions during creation of users and groups significantly. As a result it increases the replication performance and reduces the rate at which the `cn=translog` LMDB backend database gets filled. This variable is applicable only to the Primary Directory Node. By default is will be set to `yes`, during package installation and update (Bug #48626).
- A new LDAP attribute has been introduced with UCS 5.0 erratum 100. As re-indexing is time consuming the decision was made to delay the indexing until 5.0-2 and not to do it via an errata update. Therefore, a manual fix for customers is available and the required steps are documented at Univention Help 19248 (Bug #54092).
- The French translation package has been given a comprehensive update to align it to the current source code. All missing translation strings have been added and all outdated ones updated along with some general improvements of existing translation strings (Bug #54029).
- Bugs in the localization template files were updated to fix the creation and update process of language packages (Bug #54029).

INDEX

C

D

E

F

K

L

N

P

R

S

U