univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-10

Release 5.0-10

Mar 11, 2025

CONTENTS

CHAPTER

ONE

GENERAL

- UCS 5.0-10 includes all issued security updates issued for UCS 5.0-9:
  - **amavisd-new** (CVE-2024-28054) (Bug #57823)
  - **amd64-microcode** (CVE-2023-20569, CVE-2023-20584, CVE-2023-31315, CVE-2023-31356) (Bug #57766)
  - **apache2** (CVE-2024-38473, CVE-2024-38474, CVE-2024-38475) (Bug #57618, Bug #57752)
  - **avahi** (CVE-2023-1981, CVE-2023-38469, CVE-2023-38470, CVE-2023-38471, CVE-2023-38472, CVE-2023-38473) (Bug #57809)
  - **bind9** (CVE-2024-11187) (Bug #57982)
  - **busybox** (CVE-2021-28831, CVE-2021-42374, CVE-2021-42378, CVE-2021-42379, CVE-2021-42380, CVE-2021-42381, CVE-2021-42382, CVE-2021-42384, CVE-2021-42385, CVE-2021-42386, CVE-2022-48174, CVE-2023-42364, CVE-2023-42365) (Bug #57938)
  - **clamav** (CVE-2024-20505, CVE-2024-20506) (Bug #57798)
  - **cups** (CVE-2024-35235, CVE-2024-47175) (Bug #57647)
  - **cups-filters** (CVE-2024-47076, CVE-2024-47176) (Bug #57626)
  - **e2fsprogs** (CVE-2022-1304) (Bug #57648)
  - **exim4** (CVE-2021-38371, CVE-2022-3559, CVE-2023-42117, CVE-2023-42119) (Bug #57781)
  - **expat** (CVE-2024-45490, CVE-2024-45491, CVE-2024-45492) (Bug #57644)
  - **ffmpeg** (CVE-2020-20898, CVE-2020-22040, CVE-2020-22051, CVE-2020-22056, CVE-2021-38090, CVE-2021-38091, CVE-2021-38092, CVE-2021-38093, CVE-2021-38094, CVE-2022-48434, CVE-2023-49502, CVE-2023-50010, CVE-2023-51793, CVE-2023-51794, CVE-2023-51798, CVE-2024-31578, CVE-2024-32230, CVE-2024-35366, CVE-2024-35367, CVE-2024-35368, CVE-2024-36616, CVE-2024-36617, CVE-2024-36618) (Bug #57715, Bug #57939)
  - **firmware-nonfree** (CVE-2023-35061, CVE-2023-38417, CVE-2023-47210) (Bug #57625)
  - **ghostscript** (CVE-2024-46951, CVE-2024-46953, CVE-2024-46955, CVE-2024-46956) (Bug #57767)
  - **git** (CVE-2024-50349, CVE-2024-52006) (Bug #57937)
  - **glib2.0** (CVE-2024-52533) (Bug #57769)
  - **gtk+2.0** (CVE-2024-6655) (Bug #57668)
  - **gtk+3.0** (CVE-2024-6655) (Bug #57669)
  - **hplip** (CVE-2020-6923) (Bug #57893)
  - **intel-microcode** (CVE-2024-21853, CVE-2024-23918, CVE-2024-23984, CVE-2024-24968) (Bug #57768, Bug #57825)
  - **iproute2** (CVE-2019-20795) (Bug #57624)

- **libarchive** (CVE-2024-20696) (Bug #57750)
- **libheif** (CVE-2023-0996, CVE-2024-41311) (Bug #57699, Bug #57741)
- **libsepol** (CVE-2021-36084, CVE-2021-36085, CVE-2021-36086, CVE-2021-36087) (Bug #57696)
- **libsoup2.4** (CVE-2024-52530, CVE-2024-52531, CVE-2024-52532) (Bug #57808)
- **libxml2** (CVE-2016-9318, CVE-2017-16932, CVE-2023-39615, CVE-2023-45322, CVE-2024-25062) (Bug #57664, Bug #57722)
- **linux-5.10** (CVE-2021-3669, CVE-2022-43945, CVE-2022-48666, CVE-2022-48733, CVE-2023-31083, CVE-2023-52889, CVE-2024-25741, CVE-2024-26629, CVE-2024-27019, CVE-2024-27397, CVE-2024-31076, CVE-2024-36014, CVE-2024-36015, CVE-2024-36016, CVE-2024-36270, CVE-2024-36288, CVE-2024-36484, CVE-2024-36489, CVE-2024-36901, CVE-2024-36938, CVE-2024-36974, CVE-2024-36978, CVE-2024-37078, CVE-2024-37356, CVE-2024-38381, CVE-2024-38546, CVE-2024-38547, CVE-2024-38548, CVE-2024-38552, CVE-2024-38555, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38577, CVE-2024-38578, CVE-2024-38579, CVE-2024-38582, CVE-2024-38583, CVE-2024-38586, CVE-2024-38589, CVE-2024-38590, CVE-2024-38596, CVE-2024-38597, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38605, CVE-2024-38607, CVE-2024-38612, CVE-2024-38618, CVE-2024-38619, CVE-2024-38621, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38635, CVE-2024-38637, CVE-2024-38659, CVE-2024-38662, CVE-2024-38780, CVE-2024-39468, CVE-2024-39482, CVE-2024-39487, CVE-2024-40947, CVE-2024-41007, CVE-2024-41009, CVE-2024-41011, CVE-2024-41012, CVE-2024-41042, CVE-2024-41090, CVE-2024-41091, CVE-2024-41098, CVE-2024-42114, CVE-2024-42228, CVE-2024-42246, CVE-2024-42259, CVE-2024-42265, CVE-2024-42272, CVE-2024-42276, CVE-2024-42280, CVE-2024-42281, CVE-2024-42283, CVE-2024-42284, CVE-2024-42285, CVE-2024-42286, CVE-2024-42287, CVE-2024-42288, CVE-2024-42289, CVE-2024-42290, CVE-2024-42292, CVE-2024-42295, CVE-2024-42297, CVE-2024-42301, CVE-2024-42302, CVE-2024-42304, CVE-2024-42305, CVE-2024-42306, CVE-2024-42308, CVE-2024-42309, CVE-2024-42310, CVE-2024-42311, CVE-2024-42312, CVE-2024-42313, CVE-2024-43828, CVE-2024-43829, CVE-2024-43830, CVE-2024-43834, CVE-2024-43835, CVE-2024-43839, CVE-2024-43841, CVE-2024-43846, CVE-2024-43849, CVE-2024-43853, CVE-2024-43854, CVE-2024-43856, CVE-2024-43858, CVE-2024-43860, CVE-2024-43861, CVE-2024-43867, CVE-2024-43871, CVE-2024-43879, CVE-2024-43880, CVE-2024-43882, CVE-2024-43883, CVE-2024-43884, CVE-2024-43889, CVE-2024-43890, CVE-2024-43892, CVE-2024-43893, CVE-2024-43894, CVE-2024-43905, CVE-2024-43907, CVE-2024-43908, CVE-2024-43914, CVE-2024-44935, CVE-2024-44944, CVE-2024-44946, CVE-2024-44947, CVE-2024-44948, CVE-2024-44952, CVE-2024-44954, CVE-2024-44960, CVE-2024-44965, CVE-2024-44968, CVE-2024-44971, CVE-2024-44974, CVE-2024-44987, CVE-2024-44988, CVE-2024-44989, CVE-2024-44990, CVE-2024-44995, CVE-2024-44998, CVE-2024-44999, CVE-2024-45003, CVE-2024-45006, CVE-2024-45008, CVE-2024-45016, CVE-2024-45018, CVE-2024-45021, CVE-2024-45025, CVE-2024-45028, CVE-2024-46673, CVE-2024-46674, CVE-2024-46675, CVE-2024-46676, CVE-2024-46677, CVE-2024-46679, CVE-2024-46685, CVE-2024-46689, CVE-2024-46702, CVE-2024-46707, CVE-2024-46713, CVE-2024-46714, CVE-2024-46719, CVE-2024-46721, CVE-2024-46722, CVE-2024-46723, CVE-2024-46724, CVE-2024-46725, CVE-2024-46731, CVE-2024-46737, CVE-2024-46738, CVE-2024-46739, CVE-2024-46740, CVE-2024-46743, CVE-2024-46744, CVE-2024-46745, CVE-2024-46747, CVE-2024-46750, CVE-2024-46755, CVE-2024-46756, CVE-2024-46757, CVE-2024-46758, CVE-2024-46759, CVE-2024-46763, CVE-2024-46771, CVE-2024-46777, CVE-2024-46780, CVE-2024-46781, CVE-2024-46782, CVE-2024-46783, CVE-2024-46791, CVE-2024-46798, CVE-2024-46800, CVE-2024-46804, CVE-2024-46814, CVE-2024-46815, CVE-2024-46817, CVE-2024-46818, CVE-2024-46819, CVE-2024-46822, CVE-2024-46828, CVE-2024-46829, CVE-2024-46840, CVE-2024-46844) (Bug #57718)
- **linux-signed-5.10-amd64** (CVE-2021-3669, CVE-2022-43945, CVE-2022-48666, CVE-2022-48733, CVE-2023-31083, CVE-2023-52889, CVE-2024-25741, CVE-2024-26629, CVE-2024-27019, CVE-2024-27397, CVE-2024-31076, CVE-2024-36014, CVE-2024-36015, CVE-2024-36016, CVE-2024-36270, CVE-2024-36288, CVE-2024-36484, CVE-2024-36489,

CVE-2024-36901, CVE-2024-36938, CVE-2024-36974, CVE-2024-36978, CVE-2024-37078, CVE-2024-37356, CVE-2024-38381, CVE-2024-38546, CVE-2024-38547, CVE-2024-38548, CVE-2024-38552, CVE-2024-38555, CVE-2024-38558, CVE-2024-38559, CVE-2024-38560, CVE-2024-38565, CVE-2024-38567, CVE-2024-38577, CVE-2024-38578, CVE-2024-38579, CVE-2024-38582, CVE-2024-38583, CVE-2024-38586, CVE-2024-38589, CVE-2024-38590, CVE-2024-38596, CVE-2024-38597, CVE-2024-38598, CVE-2024-38599, CVE-2024-38601, CVE-2024-38605, CVE-2024-38607, CVE-2024-38612, CVE-2024-38618, CVE-2024-38619, CVE-2024-38621, CVE-2024-38627, CVE-2024-38633, CVE-2024-38634, CVE-2024-38635, CVE-2024-38637, CVE-2024-38659, CVE-2024-38662, CVE-2024-38780, CVE-2024-39468, CVE-2024-39482, CVE-2024-39487, CVE-2024-40947, CVE-2024-41007, CVE-2024-41009, CVE-2024-41011, CVE-2024-41012, CVE-2024-41042, CVE-2024-41090, CVE-2024-41091, CVE-2024-41098, CVE-2024-42114, CVE-2024-42228, CVE-2024-42246, CVE-2024-42259, CVE-2024-42265, CVE-2024-42272, CVE-2024-42276, CVE-2024-42280, CVE-2024-42281, CVE-2024-42283, CVE-2024-42284, CVE-2024-42285, CVE-2024-42286, CVE-2024-42287, CVE-2024-42288, CVE-2024-42289, CVE-2024-42290, CVE-2024-42292, CVE-2024-42295, CVE-2024-42297, CVE-2024-42301, CVE-2024-42302, CVE-2024-42304, CVE-2024-42305, CVE-2024-42306, CVE-2024-42308, CVE-2024-42309, CVE-2024-42310, CVE-2024-42311, CVE-2024-42312, CVE-2024-42313, CVE-2024-43828, CVE-2024-43829, CVE-2024-43830, CVE-2024-43834, CVE-2024-43835, CVE-2024-43839, CVE-2024-43841, CVE-2024-43846, CVE-2024-43849, CVE-2024-43853, CVE-2024-43854, CVE-2024-43856, CVE-2024-43858, CVE-2024-43860, CVE-2024-43861, CVE-2024-43867, CVE-2024-43871, CVE-2024-43879, CVE-2024-43880, CVE-2024-43882, CVE-2024-43883, CVE-2024-43884, CVE-2024-43889, CVE-2024-43890, CVE-2024-43892, CVE-2024-43893, CVE-2024-43894, CVE-2024-43905, CVE-2024-43907, CVE-2024-43908, CVE-2024-43914, CVE-2024-44935, CVE-2024-44944, CVE-2024-44946, CVE-2024-44947, CVE-2024-44948, CVE-2024-44952, CVE-2024-44954, CVE-2024-44960, CVE-2024-44965, CVE-2024-44968, CVE-2024-44971, CVE-2024-44974, CVE-2024-44987, CVE-2024-44988, CVE-2024-44989, CVE-2024-44990, CVE-2024-44995, CVE-2024-44998, CVE-2024-44999, CVE-2024-45003, CVE-2024-45006, CVE-2024-45008, CVE-2024-45016, CVE-2024-45018, CVE-2024-45021, CVE-2024-45025, CVE-2024-45028, CVE-2024-46673, CVE-2024-46674, CVE-2024-46675, CVE-2024-46676, CVE-2024-46677, CVE-2024-46679, CVE-2024-46685, CVE-2024-46689, CVE-2024-46702, CVE-2024-46707, CVE-2024-46713, CVE-2024-46714, CVE-2024-46719, CVE-2024-46721, CVE-2024-46722, CVE-2024-46723, CVE-2024-46724, CVE-2024-46725, CVE-2024-46731, CVE-2024-46737, CVE-2024-46738, CVE-2024-46739, CVE-2024-46740, CVE-2024-46743, CVE-2024-46744, CVE-2024-46745, CVE-2024-46747, CVE-2024-46750, CVE-2024-46755, CVE-2024-46756, CVE-2024-46757, CVE-2024-46758, CVE-2024-46759, CVE-2024-46763, CVE-2024-46771, CVE-2024-46777, CVE-2024-46780, CVE-2024-46781, CVE-2024-46782, CVE-2024-46783, CVE-2024-46791, CVE-2024-46798, CVE-2024-46800, CVE-2024-46804, CVE-2024-46814, CVE-2024-46815, CVE-2024-46817, CVE-2024-46818, CVE-2024-46819, CVE-2024-46822, CVE-2024-46828, CVE-2024-46829, CVE-2024-46840, CVE-2024-46844) (Bug #57718)

- **mariadb-10.3** (CVE-2024-21096) (Bug #57652)
- **nss** (CVE-2023-6135, CVE-2024-6602, CVE-2024-6609) (Bug #57740)
- **ntfs-3g** (CVE-2021-33285, CVE-2021-33286, CVE-2021-33287, CVE-2021-33289, CVE-2021-35266, CVE-2021-35267, CVE-2021-35268, CVE-2021-35269, CVE-2021-39251, CVE-2021-39252, CVE-2021-39253, CVE-2021-39254, CVE-2021-39255, CVE-2021-39256, CVE-2021-39257, CVE-2021-39258, CVE-2021-39259, CVE-2021-39260, CVE-2021-39261, CVE-2021-39262, CVE-2021-39263, CVE-2021-46790, CVE-2022-30783, CVE-2022-30784, CVE-2022-30785, CVE-2022-30786, CVE-2022-30787, CVE-2022-30788, CVE-2022-30789, CVE-2022-40284, CVE-2023-52890) (Bug #57646)
- **ntp** (CVE-2020-11868, CVE-2020-15025, CVE-2023-26555) (Bug #57807)
- **openjdk-11** (CVE-2024-21208, CVE-2024-21210, CVE-2024-21217, CVE-2024-21235, CVE-2025-21502) (Bug #57698, Bug #57936)
- **openssh** (CVE-2020-14145, CVE-2025-26465) (Bug #57981)
- **openssl** (CVE-2023-5678, CVE-2024-0727, CVE-2024-2511, CVE-2024-4741, CVE-2024-5535, CVE-2024-9143) (Bug #57782)

- **perl** (CVE-2020-16156, CVE-2023-31484) (Bug #57716)
- **php7.3** (CVE-2024-11233, CVE-2024-11234, CVE-2024-11236, CVE-2024-8925, CVE-2024-8927, CVE-2024-8929, CVE-2024-8932) (Bug #57683, Bug #57824)
- **postgresql-11** (CVE-2024-10976, CVE-2024-10977, CVE-2024-10978, CVE-2024-10979) (Bug #57899)
- **python-cryptography** (CVE-2020-25659) (Bug #57697)
- **python-django** (CVE-2024-53907, CVE-2024-56374) (Bug #57935)
- **python-tornado** (CVE-2023-28370, CVE-2024-52804) (Bug #57850)
- **python-urllib3** (CVE-2024-37891) (Bug #57983)
- **python3.7** (CVE-2023-27043, CVE-2024-11168, CVE-2024-6232, CVE-2024-6923, CVE-2024-7592, CVE-2024-9287) (Bug #57780)
- **rsync** (CVE-2024-12085, CVE-2024-12086, CVE-2024-12087, CVE-2024-12088, CVE-2024-12747) (Bug #57883)
- **ruby2.5** (CVE-2024-35176, CVE-2024-39908, CVE-2024-41123, CVE-2024-41946, CVE-2024-43398, CVE-2024-49761) (Bug #57898)
- **shadow** (CVE-2018-7169, CVE-2023-29383, CVE-2023-4641) (Bug #57720)
- **simplesamlphp** (CVE-2024-52596, CVE-2024-52806) (Bug #57799)
- **sqlite3** (CVE-2019-19244, CVE-2021-36690, CVE-2023-7104) (Bug #57645)
- **tiff** (CVE-2023-25433, CVE-2023-52356, CVE-2024-7006) (Bug #57892)
- **unbound** (CVE-2024-43167, CVE-2024-43168, CVE-2024-8508) (Bug #57751)
- **xorg-server** (CVE-2024-9632) (Bug #57721)

- UCS 5.0-10 includes the following updated packages from Debian ELTS:

  emacs krb5 libtasn1-6 libxml2 xorg-server ca-certificates-java distro-info-data ruby2.5 tzdata ucf activemq ark asterisk astropy c-icap-modules context cyrus-imapd dcmtk dnsmasq editorconfig-core fastnetmon frr git-lfs gst-plugins-base1.0 gstreamer1.0 havp icinga2 iperf3 lemonldap-ng libapache-mod-jk libcpan-reporter-smoker-perl libgsf libmodule-scandeps-perl libpam-tacplus libpgjava libreoffice libtar linux-6.1 linux-signed-6.1-amd64 mpg123 needrestart nodejs pg-snakeoil pypy python-clamav qt-base-opensource-src redis smarty3 sssd sympa texlive-bin tomcat9 twisted vlc waitress wireshark zeromq3

CHAPTER

TWO

BASIC SYSTEM SERVICES

2.1 Univention Configuration Registry

2.1.1 Changes to templates and modules

- The Linux kernel parameters for the garbage collection of ARP cache entries can now be set with UCR and have their default values increased (Bug #57712).

2.2 Boot Loader

- To support Secure Boot in Debian 10 (Buster) ELTS, the SecureBoot shim needs to be updated to include the `Freexian` public certificate which was used to sign the ELTS Linux kernel and other packages. This update adds that certificate to the shim alongside the Debian public CA, which allows to boot both old (signed by Debian) and new (signed by `Freexian`) packages (Bug #57718).

CHAPTER

THREE

DOMAIN SERVICES

3.1 LDAP Directory Manager

- Improve performance of `_ldap_modlist()` in `groups/group` handler to speed up modifications of very large groups (Bug #57960).
- Enforce JPEG conversion for all profile pictures not just PNG (Bug #57672).
- The **`univention-license-check`** didn't count system accounts correctly in case of an `unlimited` license. This has been fixed (Bug #57713).
- Dynamic `udm_filter` for UDM syntax classes have been fixed so that a syntax which depends on the value of another property for its `udm_filter` works again (Bug #57733).

CHAPTER

FOUR

UNIVENTION MANAGEMENT CONSOLE

4.1 Univention Portal

- Unique HTML identifiers have been added to each self-service module to simplify custom CSS usage (Bug #57731).

4.2 Univention Management Console server

- As Keycloak's OpenID Connect URIs are checked case sensitively, the default URIs set during the join script setup were rejected on servers which contained uppercase letters. All generated URIs are converted to lowercase from now on (Bug #57679).
- Improved database session management under high load to prevent errors. Sessions are now properly closed, ensuring better stability in high concurrency environments (Bug #57680).
- The OpenID Connect front-channel logout feature now works properly in environments where the OpenID Connect Provider is hosted on a different domain than the UMC (Bug #57516).
- Make connection pool settings `pool_size`, `max_overflow`, `pool_timeout`, and `pool_recycle` configurable through `univention-management-console-settings` for improved resource management (Bug #57714).
- Delete UMC session when OpenID Connect token can't be refreshed after OP session deleted (Bug #57515).
- A package dependency to the Python library **`psycopg2`** has been added (Bug #57622).
- The automatic browser reload of the `univention-portal` led to a visual logout every 5 minutes, since the initial assertion was expired then (Bug #57563).

4.3 Univention App Center

- **`univention-app update-check`** didn't report all missing apps during a UCS upgrade. Some docker apps may be missed due to working on the wrong cache. This has been fixed (Bug #57802).
- `univention-appcenter` now provides UCR templates for PostgreSQL 15 (Bug #57802).
- Files uploaded as an App Setting were saved with the wrong content if uploaded during app installation (Bug #57996).

4.4 User management

- The `Message-ID` header has been added to emails sent through the user self service to prevent rejection by certain email providers (Bug #57953).
- The UMC module is now a singleton, that means that multiple requests won't create new instances of the module, but will be handled by one single module process. This can greatly increase performance and decrease memory consumption (Bug #57609).

4.5 Univention Directory Reports

- Fixed the handling of UDM properties with complex syntax, for example `dnsEntryZoneForward`, that prevented users from using them in customized report templates (Bug #57431).

4.6 System diagnostic module

- The diagnostic check `04_saml_certificate_check` could show a traceback if UMC wasn't configured for any kind of single sign-on. This has been fixed (Bug #57746).
- The script **`univention-report-support-info`** now keeps the generated archive per default. The option `--cleanup` has been added to the script, to overrule this new behavior (Bug #57641).

4.7 LDAP directory browser

- When using OpenID Connect login the Univention Management Console Univention Directory Manager Module sometimes wouldn't load when the LDAP server was restarted (Bug #57533).

CHAPTER

FIVE

UNIVENTION BASE LIBRARIES

- OpenLDAP is now configured to use the `sortvals` option for the attributes `uniqueMember` and `memberUid`. This improves the performance when modifying user objects or group objects in environments with groups with several thousand members. The attributes for the `sortvals` option can be configured via the UCR variable Univention Configuration Registry Variable `ldap/server/sortvals` (Bug #52175).

CHAPTER

SIX

SOFTWARE DEPLOYMENT

- After a system update through the *Software Update* UMC module, the user now stays in the module to view the system status instead of being redirected to the UMC overview page (Bug #57838).
- Don't provide the option to update to a new UCS release if some Docker apps aren't yet released for that release (Bug #57802).

CHAPTER

SEVEN

SYSTEM SERVICES

7.1 SAML

- Fixed the link to the 5.2 changelog in `univention-keycloak-migration-status` (Bug #57975).
- The tool `univention-keycloak` was enabled to update an existing authentication flow so that it replaces the Kerberos authentication step with a conditional sub-flow which can enable Kerberos authentication depending on the client IP address (Bug #56474).
- The script **`univention-keycloak-migration-status`** has been adjusted to check the setting `ucs/server/sso/uri`, which will be used from UCS 5.2 onward (Bug #57806).
- Skip `91univention-saml.inst` in case the primary is on UCS 5.2. In this case **`simpleSAMLphp`** is no longer supported and the steps in `91univention-saml.inst` aren't needed (Bug #57839).

7.2 Proxy services

- You can now manually configure the squid cache settings. Any value other than `ufs` in the UCR variable `squid/cache/format` disables the cache configuration in `squid.conf`. A custom squid cache configuration can be added to `/etc/squid/local.conf` (Bug #57963).

CHAPTER

EIGHT

SERVICES FOR WINDOWS

8.1 Samba

- Since updating from Kernel 4.19 to Kernel 5.10 the behavior of the `xfs` file system seems to have changed with respect to the handling of `xattrs`. As a symptom, `rsync -aAX` as used by the script `sysvol-sync.sh` seems to remove `trusted.SGI_ACL_FILE` and `trusted.SGI_ACL_DEFAULT` when synchronizing from the SYSVOL from a system with an `ext4` partition, which doesn't have those, but only the usual `system.posix_acl_access` and `system.posix_acl_default`. The script `sysvol-sync.sh` has been adjusted to filter the synchronized `xattrs` to only consider `security.NTACL` and not touch any other `xattrs` (Bug #57529).
- The join script has been adjusted to stop **`winbindd`** first during provisioning. This should avoid unnecessary waiting time when stopping the other samba processes in the next step (Bug #57310).
- In environments where the *Active Directory Domain Controller* app has been configured to use `mdb` as backend key value store for the `sam.ldb` database, the command **`samba-tool domain backup offline`** could run into a deadlock in case parallel changes to the `sam.ldb` where made, for example through dynamic DNS updates. That command is used by the script `univention-samba4-backup`. This was caused by an interplay of three components, the script `samba-tool`, the command `mdb_copy` and the process attempting to modify the `sam.ldb`. This update avoids this issue by reverting upstream changes made for Samba bug 14676 which where introduced there in anticipation of `lmdb` version `0.9.26`, which UCS `5.0` doesn't use (Bug #57734).
- The init script `/etc/init.d/samba-ad-dc` has been adjusted to explicitly stop `winbindd` and `smbd` processes too and also check for `pids` in their respective process group. This can be necessary during package updates, in case the `winbind.postinst` and `samba.postinst` scripts start these processes separately instead of as child of the main `samba` process. This should avoid **`/etc/init.d/samba restart`**` failing with error message `NT_STATUS_ADDRESS_ALREADY_ASSOCIATED` in `log.samba` (Bug #57310).

8.2 Univention Active Directory Connection

- Rejects in the connector for objects in AD that can't be completely read are now properly deleted (Bug #57737).
- Starting with UCS 5.0-0 the *AD Connector* had an issue with rewriting mixed case AD DNs in the presence of a custom `position_mapping`. This problem has been fixed, so that mixed case DNs from AD are mapped properly to UCS LDAP DNs again, avoiding unintelligible rejects (Bug #57565).

INDEX

B

C

E

L

S

U