univention
be open.

Changelog for Univention Corporate Server (UCS) 5.0-4

Release 5.0-4

Aug 17, 2023

CONTENTS

CHAPTER

ONE

GENERAL

- All security updates issued for UCS 5.0-3 are included:
  - **apache2** (CVE-2006-20001, CVE-2021-33193, CVE-2022-36760, CVE-2022-37436, CVE-2023-25690, CVE-2023-27522) (Bug #55778, Bug #56013)
  - **apr-util** (CVE-2022-25147) (Bug #55738)
  - **avahi** (CVE-2023-1981) (Bug #56034)
  - **clamav** (CVE-2023-20032, CVE-2023-20052) (Bug #55734)
  - **cpio** (CVE-2019-14866, CVE-2021-38185) (Bug #56115)
  - **cups-filters** (CVE-2023-24805) (Bug #56082)
  - **cups** (CVE-2023-32324) (Bug #56116)
  - **curl** (CVE-2023-23916, CVE-2023-27533, CVE-2023-27535, CVE-2023-27536, CVE-2023-27538) (Bug #55760, Bug #56011)
  - **emacs** (CVE-2022-48337, CVE-2022-48339, CVE-2023-28617) (Bug #56063)
  - **firefox-esr** (CVE-2023-0767, CVE-2023-1945, CVE-2023-25728, CVE-2023-25729, CVE-2023-25730, CVE-2023-25732, CVE-2023-25735, CVE-2023-25737, CVE-2023-25739, CVE-2023-25742, CVE-2023-25744, CVE-2023-25746, CVE-2023-25751, CVE-2023-25752, CVE-2023-28162, CVE-2023-28164, CVE-2023-28176, CVE-2023-29533, CVE-2023-29535, CVE-2023-29536, CVE-2023-29539, CVE-2023-29541, CVE-2023-29548, CVE-2023-29550, CVE-2023-32205, CVE-2023-32206, CVE-2023-32207, CVE-2023-32211, CVE-2023-32212, CVE-2023-32213, CVE-2023-32215, CVE-2023-34414, CVE-2023-34416,) (Bug #55720, Bug #55895, Bug #55974, Bug #56062, Bug #56142)
  - **firmware-nonfree** (CVE-2020-12362, CVE-2020-12363, CVE-2020-12364, CVE-2020-24586, CVE-2020-24587, CVE-2020-24588, CVE-2021-23168, CVE-2021-23223, CVE-2021-37409, CVE-2021-44545, CVE-2022-21181) (Bug #55935)
  - **freeradius** (CVE-2022-41859, CVE-2022-41860, CVE-2022-41861) (Bug #55758)
  - **ghostscript** (CVE-2023-28879) (Bug #55948)
  - **gnutls28** (CVE-2023-0361) (Bug #55723)
  - **heimdal** (CVE-2022-3437, CVE-2022-45142) (Bug #55674)
  - **imagemagick** (CVE-2020-19667, CVE-2020-25665, CVE-2020-25666, CVE-2020-25674, CVE-2020-25675, CVE-2020-25676, CVE-2020-27560, CVE-2020-27750, CVE-2020-27751, CVE-2020-27754, CVE-2020-27756, CVE-2020-27757, CVE-2020-27758, CVE-2020-27759, CVE-2020-27760, CVE-2020-27761, CVE-2020-27762, CVE-2020-27763, CVE-2020-27764, CVE-2020-27765, CVE-2020-27766, CVE-2020-27767, CVE-2020-27768, CVE-2020-27769, CVE-2020-27770, CVE-2020-27771, CVE-2020-27772, CVE-2020-27773, CVE-2020-27774, CVE-2020-27775, CVE-2020-27776, CVE-2020-29599, CVE-2021-20176, CVE-2021-20224, CVE-2021-20241, CVE-2021-20243, CVE-2021-20244, CVE-2021-20245, CVE-2021-20246, CVE-2021-20309, CVE-2021-20312, CVE-2021-20313, CVE-2021-3574, CVE-2021-3596,

CVE-2021-39212, CVE-2022-28463, CVE-2022-32545, CVE-2022-32546, CVE-2022-32547, CVE-2022-44267, CVE-2022-44268) (Bug #55869, Bug #55896, Bug #56081)

- **intel-microcode** (CVE-2022-21216, CVE-2022-21233, CVE-2022-33196, CVE-2022-33972, CVE-2022-38090) (Bug #55933)
- **ldb** (CVE-2023-0614) (Bug #55892)
- **libde265** (CVE-2023-24751, CVE-2023-24752, CVE-2023-24754, CVE-2023-24755, CVE-2023-24756, CVE-2023-24757, CVE-2023-24758, CVE-2023-25221) (Bug #55780)
- **libwebp** (CVE-2023-1999) (Bug #56118)
- **libxml2** (CVE-2023-28484, CVE-2023-29469) (Bug #56033)
- **linux-latest** (CVE-2022-2873, CVE-2022-3424, CVE-2022-3545, CVE-2022-36280, CVE-2022-3707, CVE-2022-41218, CVE-2022-45934, CVE-2022-4744, CVE-2022-47929, CVE-2023-0045, CVE-2023-0266, CVE-2023-0394, CVE-2023-0458, CVE-2023-0459, CVE-2023-0461, CVE-2023-1073, CVE-2023-1074, CVE-2023-1078, CVE-2023-1079, CVE-2023-1118, CVE-2023-1281, CVE-2023-1513, CVE-2023-1670, CVE-2023-1829, CVE-2023-1855, CVE-2023-1859, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2162, CVE-2023-2194, CVE-2023-23454, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2023-28328, CVE-2023-30456, CVE-2023-30772) (Bug #56032)
- **linux-signed-amd64** (CVE-2022-2873, CVE-2022-3424, CVE-2022-3545, CVE-2022-36280, CVE-2022-3707, CVE-2022-41218, CVE-2022-45934, CVE-2022-4744, CVE-2022-47929, CVE-2023-0045, CVE-2023-0266, CVE-2023-0394, CVE-2023-0458, CVE-2023-0459, CVE-2023-0461, CVE-2023-1073, CVE-2023-1074, CVE-2023-1078, CVE-2023-1079, CVE-2023-1118, CVE-2023-1281, CVE-2023-1513, CVE-2023-1670, CVE-2023-1829, CVE-2023-1855, CVE-2023-1859, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2162, CVE-2023-2194, CVE-2023-23454, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2023-28328, CVE-2023-30456, CVE-2023-30772) (Bug #56032)
- **linux** (CVE-2022-2873, CVE-2022-3424, CVE-2022-3545, CVE-2022-36280, CVE-2022-3707, CVE-2022-41218, CVE-2022-45934, CVE-2022-4744, CVE-2022-47929, CVE-2023-0045, CVE-2023-0266, CVE-2023-0394, CVE-2023-0458, CVE-2023-0459, CVE-2023-0461, CVE-2023-1073, CVE-2023-1074, CVE-2023-1078, CVE-2023-1079, CVE-2023-1118, CVE-2023-1281, CVE-2023-1513, CVE-2023-1670, CVE-2023-1829, CVE-2023-1855, CVE-2023-1859, CVE-2023-1989, CVE-2023-1990, CVE-2023-1998, CVE-2023-2162, CVE-2023-2194, CVE-2023-23454, CVE-2023-23455, CVE-2023-23559, CVE-2023-26545, CVE-2023-28328, CVE-2023-30456, CVE-2023-30772) (Bug #56032)
- **mariadb-10.3** (CVE-2022-47015) (Bug #56117)
- **nss** (CVE-2020-12400, CVE-2020-12401, CVE-2020-12403, CVE-2020-6829, CVE-2023-0767) (Bug #55735)
- **openssl** (CVE-2022-2097, CVE-2022-4304, CVE-2022-4450, CVE-2023-0215, CVE-2023-0286, CVE-2023-0464, CVE-2023-0465, CVE-2023-0466, CVE-2023-2650) (Bug #55737, Bug #56141)
- **pcre2** (CVE-2019-20454, CVE-2022-1586, CVE-2022-1587) (Bug #55897)
- **php7.3** (CVE-2022-31631, CVE-2023-0567, CVE-2023-0568, CVE-2023-0662) (Bug #55759)
- **postgresql-11** (CVE-2022-41862, CVE-2023-2454, CVE-2023-2455) (Bug #55676, Bug #56061)
- **python2.7** (CVE-2015-20107, CVE-2019-20907, CVE-2020-26116, CVE-2020-8492, CVE-2021-3177, CVE-2021-3733, CVE-2021-3737, CVE-2021-4189, CVE-2022-45061) (Bug #56101)
- **python-cryptography** (CVE-2023-23931) (Bug #55739)
- **python-ipaddress** (CVE-2020-14422) (Bug #56079)

  - **qemu** (CVE-2020-14394, CVE-2020-17380, CVE-2020-29130, CVE-2021-3409, CVE-2021-3592, CVE-2021-3593, CVE-2021-3594, CVE-2021-3595, CVE-2022-0216, CVE-2022-1050) (Bug #55881)
  - **requests** (CVE-2023-32681) (Bug #56155),
  - **samba** (CVE-2023-0614, CVE-2023-0922) (Bug #55892)
  - **systemd** (CVE-2023-26604) (Bug #55928)
  - **tiff** (CVE-2023-0795, CVE-2023-0796, CVE-2023-0797, CVE-2023-0798, CVE-2023-0799, CVE-2023-0800, CVE-2023-0801, CVE-2023-0802, CVE-2023-0803, CVE-2023-0804) (Bug #55736)
  - **unbound** (CVE-2020-28935, CVE-2022-30698, CVE-2022-30699, CVE-2022-3204) (Bug #55932)
  - **vim** (CVE-2022-4141, CVE-2023-0054, CVE-2023-1175, CVE-2023-2610) (Bug #56143)
  - **xorg-server** (CVE-2023-0494, CVE-2023-1393) (Bug #55675, Bug #55934)

- The following updated packages from Debian 10.13 are included: **389-ds-base**, **acme-tool**, **amanda**, **aptly**, **asterisk**, **binwalk**, **c-ares**, **connman**, **distro-info-data**, **dnscrypt-proxy**, **duktape**, **epiphany-browser**, **etcd**, **ffmpeg**, **fscrypt**, **g10k**, **git**, **gitlab-shell**, **gitlab-workhorse**, **gobuster**, **gokey**, **golang-1.11**, **golang-github-opencontainers-selinux**, **golang-go.crypto**, **golang-web-socket**, **gopass**, **graphite-web**, **grunt**, **haproxy**, **hub**, **hugo**, **jackson-databind**, **joblib**, **jruby**, **json-smart**, **kamailio**, **keepalived**, **kopanocore**, **liba-pache2-mod-auth-mellon**, **libapache2-mod-auth-openidc**, **libdatetime-time-zone-perl**, **libgit2**, **libmicrohttpd**, **libraw**, **libreoffice**, **libsdl2**, **libssh**, **linux-5.10**, **linux-signed-5.10-amd64**, **lldpd**, **maradns**, **mono**, **mpv**, **nbconvert**, **netatalk**, **node-css-what**, **nodejs**, **node-nth-check**, **node-url-parse**, **notary**, **nvidia-graphics-drivers-legacy-390xx**, **obfs4proxy**, **openimageio**, **openjdk-11**, **openvswitch**, **packer**, **protobuf**, **pypdf2**, **python-django**, **python-werkzeug**, **rain-loop**, **rclone**, **redis**, **restic**, **ruby2.5**, **ruby-rack**, **ruby-sidekiq**, **shim-signed**, **snapd**, **sniproxy**, **snort**, **sofia-sip**, **sox**, **spip**, **sqlite**, **sqlparse**, **sssd**, **svgpp**, **syncthing**, **syslog-ng**, **sysstat**, **texlive-bin**, **thunderbird**, **tomcat9**, **trafficserver**, **tzdata**, **udisks2**, **webkit2gtk**, **wireless-regdb**, **wireshark**, **xapian-core**, **xfig**, **xrdp**, **zabbix**

1.1 Univention Configuration Registry

- Future compatibility with Python 3.11 has been added (Bug #55632).

1.1.1 Changes to templates and modules

- A wrong Python format string in the **rsyslog** configuration has been fixed, which is used by the following Univention Configuration Registry Variables (Bug #56042): `syslog/input/udp`, `syslog/input/tcp`, and `syslog/input/relp`.
- Allow NFS shares to be mounted on exporting host itself to prevent data-loss on shared access (Bug #50193).
- The deprecated command **univention-keyboardmapping** has been removed (Bug #50193).

1.1.2 Listener/Notifier domain replication

- Future compatibility with Python 3.11 has been added (Bug #55632).
- The fix for Bug #54986 introduced an issue with the handling of *start- stop-daemon* that could result in an error message during **`systemctl restart univention-directory-notifier`** (Bug #55957).
- Implement **`univention-translog reindex`** to re-built the transaction index file in case it gets corrupted. Univention Directory Notifier (UDN) already has code to maintain the index, but after certain error cases the index may become corrupt and has to be re-built. The code in UDN isn't optimized to re-index many transactions in batch and shows performance issues for large transaction files (Bug #54797).
- All new Object Identifiers (OIDs) for internally defined object classes (OCs) and attribute types (ATs) from OpenLDAP 2.5 have been added to the exclude list of Univention Directory Listener module `replication.py`. Also all OIDs of OCs and ATs provided internally by OpenLDAP modules have been added. The list of excluded OIDs is no longer maintained in `replication.py` itself, but is now stored in the file `/usr/share/univention-ldap/oid_skip` (Bug #55927).

1.2 Univention Management Console web interface

- Future compatibility with Python 3.11 has been added (Bug #55632).
- It is now possible to access UDM modules with numbers in their name through the UDM REST API (Bug #55551).
- The debug level is now correctly passed to child processes if it's set through UCR (Bug #56051).
- Updated the copyright file. We don't ship icons from `iconmonstr.com` since UCS 5.0 (Bug #55862).
- Form input fields that load values now show a standby animation (Bug #56053).
- Text within disabled text boxes in the light theme is now displayed with better contrast when viewed in the Safari browser (Bug #55939).

1.3 Univention Portal

- The Portal is now able to display announcements, which are realized through a new UDM module **portals/announcement** (Bug #55175).
- The old UDM modules for the UCS 4.4 Portal have been renamed to better distinguish between them in the web user interface (Bug #55409).
- The documentation wasn't specific enough about what command to run, after the Univention Configuration Registry Variable `portal/default-dn` changed. Running **`univention-portal update`** after changing the Univention Configuration Registry Variable is enough (Bug #55871).
- The *Choose a tab* dialog box now displays tabs with their background color (Bug #55919).
- Updating the portal information now uses a local UDM connection, thus removing potential load on the Primary Node in large environments (Bug #56113).
- Future compatibility with Python 3.11 has been added (Bug #55632).
- The self-service notifications no longer show mixed language (English and German) when users modify their profile or change their password (Bug #55664).

1.4 Univention Management Console server

- The Univention Management Console server and web server have been merged into a single executable. The implementation now uses **Tornado** instead of the UCS specific Python Notifier implementation (Bug #43633).
- Restarts of the Univention Management Console in Debian maintainer scripts and join scripts are now done using `deb-systemd-invoke` to respect policy layer (Bug #54586).
- Disable the SOAP binding for single sign-out in the identity provider metadata to make sure UCS doesn't use SOAP for the UMC SAML logout (Bug #56069).
- The join script now uses Python 3 instead of Python 2 to update SAML metadata. Future compatibility with Python 3.11 has been added (Bug #55632).
- The error message shown during password reset or change now appends the text from the Univention Configuration Registry Variable `umc/login/password-complexity-message/.*` when password complexity criteria don't match (Bug #55529).
- The usage of multiple languages in various messages, such as notifications, has been eliminated (Bug #55664).
- For UCS 5.0-3 the UMC services where converted to **systemd**. These services are essential to continue running even when updates are installed from UMC. Due to an oversight the first UCS 5.0 erratum 583 triggered a latent bug, which causes the service to stop during the upgrade, which kills any web session and cancels the update process running in the background. This update adds a mitigation to prevent the service from stopping during the update (Bug #55753).
- A missing Python 2.7 dependency has been added so that UMC modules using Python 2.7 work again (Bug #55752).
- Building the downstream package *Univention System Setup* failed because of some missing package dependencies in *Univention Management Console*. They have been added with UCS 5.0-3 and changed by UCS 5.0 erratum 595, but were added to the wrong binary packages (Bug #55776).
- A crash of the UMC server and UMC web server is now prevented (Bug #55959).
- The Univention Configuration Registry template for the Apache configuration in UMC multiprocessing mode has been repaired (Bug #55726).
- The UMC join script won't overwrite the Univention Configuration Registry Variable `umc/saml/idp-server` during execution (Bug #55951).
- The script **univention-management-console-client** now accesses UMC through the HTTP interface instead of the deprecated UMCP (Bug #55913).
- Some missing German translations have been added (Bug #56010).

1.5 Univention App Center

- The message and the button label in the UMC App Center presented when a pinned App should be removed or upgraded was made more consistent (Bug #55679).
- Some installation code now runs with Python 3 instead of Python 2. Future compatibility with Python 3.11 has been added (Bug #55632).
- The App Center listener now removes files from its queue that contain `entryUUIDs` whose corresponding UDM objects can't be found. These files can't be processed by the listener and would otherwise remain in the queue forever and cause infinite error logging (Bug #56072).
- The command **univention-app shell** now supports the option `--service_name` to specify the docker compose service name where the command is executed in (Bug #56038).
- Error messages during app installations are now being translated (Bug #55664).

- The App Center now supports adding custom settings to an app with a file `/var/lib/univention-appcenter/apps/$APP_ID/custom.settings`. This file has the same format as the standard App Center settings file (Bug #55765).

1.6 Univention Directory Manager and command line interface

- The usability of the shares module has been overhauled (Bug #44997, Bug #40599, Bug #7843, Bug #31388, Bug #42805, Bug #44997, Bug #50701, Bug #53785, Bug #19868, Bug #21349).
- The *Simple UDM API* now has a parameter to initialize a machine connection against the local **slapd** (Bug #56113).
- Newly set passwords are now always added to the password history even if the check for password history is disabled (Bug #56020).
- Future compatibility with Python 3.11 has been added (Bug #55632).
- The syntax for `IComputer_FQDN` was using a wrong regular expression, which did accept some invalid values and was also susceptible to a regular expression denial of service vulnerability (Bug #33684).
- Problems during concurrently reloading of UDM modules have been resolved (Bug #54597).
- Policies are now correctly written back in the *Simple UDM API* (Bug #56146).

1.7 Modules for system settings / setup wizard

- Future compatibility with Python 3.11 has been added (Bug #55632).

1.8 Domain join module

- Future compatibility with Python 3.11 has been added (Bug #55632).
- The binary package **univention-management-console-module-join** has been split from the source package **univention-join** into a separate one to prevent a circular build dependency (Bug #55870).
- The package is now using the latest **ldb** version (Bug #55892).

1.9 System diagnostic module

- Two messages in the SAML certificate diagnostic check contained a typographical error (typo) in the German translation. The messages show up when the diagnostic check complains about SAML certificates. The typo has been fixed (Bug #55874).
- Future compatibility with Python 3.11 has been added (Bug #55632).

1.10 File system quota module

- Translations for the search bar in the UMC module *Filesystem quotas* have been added (Bug #55664).

1.11 Other modules

- Future compatibility with Python 3.11 has been added (Bug #55632).

CHAPTER

TWO

UNIVENTION BASE LIBRARIES

- Future compatibility with Python 3.11 has been added (Bug #55632).
- A regression in UCS 5.0 erratum 683 during package installation in Univention System Setup has been corrected (Bug #56111).

CHAPTER

THREE

SOFTWARE DEPLOYMENT

- Fix the link to the release notes of future UCS releases (Bug #55667).
- Fixed a regression where the UCS updater did ignore the URL path of components when creating the list of repositories in the file `/etc/apt/sources.list.d/20_ucs-online-component.list` (Bug #55636).
- A pre update check is now executed with Python 3 instead of Python 2 (Bug #55632).

3.1 Docker

- Containers using glibc version 2.34 or above require the system calls `clone3` and `faccessat2`. These system calls have been added to the default docker **`seccomp`** rules that are used by single container apps in the App Center. (Bug #55360).

3.2 SAML

- **`SimpleSAMLPHP`** is configured as a service provider in Keycloak, meaning it acts as a proxy and uses Keycloak as a backend. This is part of the migration from **`SimpleSAMLPHP`** to Keycloak in UCS (Bug #56074).
- New commands have been added to **`univention-keycloak`** to create attribute mappers from the LDAP object to the internal Keycloak object (`user- attribute-ldap-mapper`) and to create *user attribute* mappers and *name identifier* mappers for SAML clients (`saml-client-user-attribute-mapper`, `saml-client- nameid-mapper`, Bug #56096).
- The package **`univention-keycloak`** now supports the `keycloak/server/sso/path` app setting from the Keycloak app (Bug #56022).
- The command **`upgrade-config`** has been added to **`univention-keycloak`**. This is used during upgrades of the Keycloak app to update the domain wide Keycloak configuration (Bug #55866).
- Sub-commands for registering LDAP mapper, password update and self service extensions have been added to **`univention-keycloak`** (Bug #55663).

3.3 Univention self service

- A regression introduced in UCS 5.0-3 has been fixed, which caused that accessing available password reset methods wasn't possible anymore (Bug #55684).
- The error message shown during password reset or when creating a new account now appends the text from the Univention Configuration Registry Variable `umc/login/password-complexity- message/.*` when password complexity criteria didn't match (Bug #55529).

- Self-service user attributes specified in Univention Configuration Registry Variable `self-service/udm_attributes` can be configured as read-only through the Univention Configuration Registry Variable `self-service/udm_attributes/read-only` (Bug #55733).

3.4 Mail services

- The migration of Fetchmail extended attributes has been moved to the join script `univenition-fetchmail` to fix errors in environments where **univention-fetchmail** is installed on a non-primary node. The old extended attributes have also been restored to fix errors in environments where **univention-fetchmail** is running on a server that hasn't yet been upgraded (Bug #55882).
- New checks have been added to the script **migrate-fetchmail.py** to avoid errors during execution when a Fetchmail configuration is incomplete (Bug #55893).
- Fixed error in UDM caused by the syntax of Fetchmail extended attributes. The bug occurred when hooks of other extended attributes of the user module initialize a UDM module (e.g `settings/extended_attribuets`, Bug #55910).
- Fix error in join script `univention-fetchmail-schema` execution caused by a script. On member nodes now the correct credentials are used to connect to LDAP. The join script also verifies if the file `/etc/fetchmailrc` exists (Bug #55766).
- The hooks, syntax files and scripts are now installed on the package **univention-fetchmail-schema** to avoid errors in installations where **univention-fetchmail** is installed on Managed Nodes or Replica Directory Nodes (Bug #55681).
- The listener module `fetchmail` now correctly loads the file `/etc/fetchmailrc` when there are entries from UIDs with a single character or with other valid characters like "" (Bug #55682).

3.5 Printing services

- Updates no longer overwrite existing print-server configuration values with the defaults (Bug #55860).
- Future compatibility with Python 3.11 has been added (Bug #55632).
- **cups** has been updated, so that printing multiple copies now works (Bug #55886).

3.6 RADIUS

- It's now possible to login with the mail primary address in addition to the username (Bug #55757).
- The maximum TLS version has been changed to 1.2 to prevent issues with Microsoft Windows 10 and 11 clients. The maximum TLS version can be specified in the Univention Configuration Registry Variable `freeradius/conf/tls-max-version` (Bug #55247).

3.7 Proxy services

- Future compatibility with Python 3.11 has been added (Bug #55632).

3.8 Samba

- **samba** has been updated to version 4.18.3 (Bug #55907).
- The AD password change has been moved to another package to avoid problems on systems that don't have **univention-samba** installed (Bug #54390).
- The logrotate configuration for **samba-dcerpcd** and **:program:samba-bgqd** has been fixed (Bug #55597).
- The final restart of Samba at the end of a package update has been adjusted to the new daemon signature in the process list (Bug #55677).
- Under special conditions, the listener module `samba4-idmap.py` wrote invalid values in the attributes `xidNumber` of the file `idmap.ldb`. During package update they will be fixed (Bug #55686).
- When uploading printer drivers, PE files with a higher version now replace older files, regardless of the case of the filename (Bug #52051).
- The Samba init scripts `samba-ad-dc` and `samba` now also stop the services **samba-dcerpcd** and **samba-bgqd** (Bug #55727).
- In scenarios where a UCS AD domain runs next to a native Microsoft AD domain with an AD-Connector that mirrors users and password hashes between both, the option `auth methods` is usually adjusted on the UCS AD DCs to make access to SMB shares hosted on UCS member servers possible for Microsoft AD users without needing to type in their password again. Since UCS 5.0 this broke Samba logon on the UCS AD DCs themselves. The Samba patch has been adjusted to only consider the method `sam_ignoredomain` from the list of values specified through the Univention Configuration Registry Variable `samba/global/options/"auth methods"` or directly in the Samba `local.conf` as configuration parameter `auth methods`. If Samba finds this particular method in the Samba configuration, then it now only appends it to the standard list of authentication methods, rather than replacing the standard list completely. This approach should be more robust with respect to Samba release updates (Bug #55727).
- Running the init script `samba-ad-dc` with the operation `restart` left Samba in a state that didn't recognize non-local domains. It has been made more robust by taking care that **nmbd** is started again before the main **samba** daemon (Bug #55727, Bug #55678).
- In domains with larger numbers of users the command **wbinfo -u** didn't return any results (Bug #55962).
- By default allow the KDC to issue services tickets using AES encryption. Prior to UCS 5.0-4, by default Samba only issued service tickets that use the `RC4` cipher (also known as `arcfour`) as ticket encryption type. This default applies unless a service principal explicitly has `msDS-SupportedEncryptionTypes` set in the SAM database, which is the case for domain controllers, which explicitly also support AES as ticket encryption type for service tickets, for example for SMB or DCERPC. With UCS 5.0-4, the Samba configuration now additionally supports AES ticket encryption types for service tickets by default. This is controlled by a new Univention Configuration Registry Variable `samba/kdc_default_domain_supported_enctypes` (Bug #56077).

3.9 Univention S4 Connector

- Handling of rejects due to invalid pickle files has been repaired (Bug #55774).
- The script **resync_object_from_ucs.py** has an option `--first` which allows a particular DN or filtered list of DNs to be replicated with priority. This update fixes the sort order to actually put the DNs to the first position in the synchronization queue (Bug #55880).
- If the system was upgraded from UCS 4.4 and had rejected objects the internal SQLite database was corrupted. The database will be repaired (Bug #54586).
- The check for a running S4-Connector is now checking for Python 3 only processes (Bug #55632).
- A translation for the MS group policy attribute has been added (Bug #55664).

3.10 Univention Active Directory Connection

- If the system was upgraded from UCS 4.4 and had rejected objects the internal SQLite database was corrupted. The database will be repaired (Bug #54587).
- A server password change script for AD member mode has been moved from **univention-ad-connector** to **univention-role-server-common** to cover different use cases (Bug #55940).
- Handling of rejects due to invalid pickle files has been repaired (Bug #55774).
- The check for a running AD-Connector is now checking for Python 3 only processes (Bug #55632).
- A new server password change script has been added for AD member mode (Bug #54390).

CHAPTER

FOUR

OTHER CHANGES

- `Content-Security-Policy` is removed from UCS realm init configuration, since it is handled by Apache configuration (Bug #55866).
- This extension allows a group of people to reset the passwords of other users. Privileged users can be exempted, for example *Domain Admins*. The set of these users is stored in Univention Configuration Registry Variable `ldap/acl/user/passwordreset/internal/groupmemberlist/`, but the ordering was not stable and could change on each invocation of **`ldap-group-to-file.py`**. This lead to a restart of **`slapd`**, which interrupted access to LDAP on a regular basis. This has been fixed by sorting the users and restarting **`slapd`** only when the set of users changes (Bug #56099).
- The scripts of **`univention-l10n`** to manage translation are now executed with Python 3 instead of Python 2 (Bug #55632).
- Future compatibility with Python 3.11 has been added (Bug #55632).

INDEX

B

C

E

F

K

L

P

S

U