univention
be open.

# Changelog for Univention Corporate Server (UCS) 5.0-7

***Release 5.0-7***

**Mar 15, 2024**

# CONTENTS

CHAPTER

# ONE

# GENERAL

- The dependency of **univention-fix-ucr-dns** on **py3dns** has been replaced by **dnspython** to support EDNS (Extended Domain Name System), which is required for virtual machines on AWS- EC2 and OpenStack. This also fixes an issue with "Amazon Provided DNS", which only supports "recursive queries": as such they were not identified as forwarding DNS services and did not get moved from Univention Configuration Registry Variables `nameserver[123]` to `dns/forwarder[123]`. This resulted in UCS domain specific queries being sent wrongly to the "Amazon Provided DNS", which then were not able to answer them and returned a failure instead, leading to all kind of application errors (Bug #56911).
- All security updates issued for UCS 5.0-6 are included:
  - **bind9** (CVE-2023-3341) (Bug #57029)
  - **bluez** (CVE-2023-45866) (Bug #56921)
  - **curl** (CVE-2023-28322, CVE-2023-46218) (Bug #56941)
  - **exim4** (CVE-2023-51766) (Bug #56968)
  - **firefox-esr** (CVE-2023-6856, CVE-2023-6857, CVE-2023-6858, CVE-2023-6859, CVE-2023-6860, CVE-2023-6861, CVE-2023-6862, CVE-2023-6863, CVE-2023-6864, CVE-2023-6865, CVE-2023-6867, CVE-2024-0741, CVE-2024-0742, CVE-2024-0746, CVE-2024-0747, CVE-2024-0749, CVE-2024-0750, CVE-2024-0751, CVE-2024-0753, CVE-2024-0755, CVE-2024-1546, CVE-2024-1547, CVE-2024-1548, CVE-2024-1549, CVE-2024-1550, CVE-2024-1551, CVE-2024-1552, CVE-2024-1553) (Bug #56939, Bug #57008, Bug #57085)
  - **gnutls28** (CVE-2024-0553) (Bug #57086)
  - **imagemagick** (CVE-2023-1289, CVE-2023-34151, CVE-2023-39978, CVE-2023-5341) (Bug #57080)
  - **intel-microcode** (CVE-2023-23583) (Bug #56920)
  - **jinja2** (CVE-2024-22195) (Bug #57007)
  - **libde265** (CVE-2023-49465, CVE-2023-49467, CVE-2023-49468) (Bug #56948)
  - **linux** (CVE-2021-44879, CVE-2023-0590, CVE-2023-1077, CVE-2023-1206, CVE-2023-1989, CVE-2023-25775, CVE-2023-3212, CVE-2023-3390, CVE-2023-34319, CVE-2023-34324, CVE-2023-35001, CVE-2023-3609, CVE-2023-3611, CVE-2023-3772, CVE-2023-3776, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-40283, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4244, CVE-2023-42753, CVE-2023-42754, CVE-2023-42755, CVE-2023-45863, CVE-2023-45871, CVE-2023-4622, CVE-2023-4623, CVE-2023-4921, CVE-2023-51780, CVE-2023-51781, CVE-2023-51782, CVE-2023-5717, CVE-2023-6606, CVE-2023-6931, CVE-2023-6932) (Bug #56972)
  - **linux-latest** (CVE-2021-44879, CVE-2023-0590, CVE-2023-1077, CVE-2023-1206, CVE-2023-1989, CVE-2023-25775, CVE-2023-3212, CVE-2023-3390, CVE-2023-34319, CVE-2023-34324, CVE-2023-35001, CVE-2023-3609, CVE-2023-3611, CVE-2023-3772, CVE-2023-3776, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-40283, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4244, CVE-2023-42753, CVE-2023-42754, CVE-2023-42755, CVE-2023-45863, CVE-2023-45871,

CVE-2023-4622, CVE-2023-4623, CVE-2023-4921, CVE-2023-51780, CVE-2023-51781, CVE-2023-51782, CVE-2023-5717, CVE-2023-6606, CVE-2023-6931, CVE-2023-6932) (Bug #56972)

- **linux-signed-amd64** (CVE-2021-44879, CVE-2023-0590, CVE-2023-1077, CVE-2023-1206, CVE-2023-1989, CVE-2023-25775, CVE-2023-3212, CVE-2023-3390, CVE-2023-34319, CVE-2023-34324, CVE-2023-35001, CVE-2023-3609, CVE-2023-3611, CVE-2023-3772, CVE-2023-3776, CVE-2023-39189, CVE-2023-39192, CVE-2023-39193, CVE-2023-39194, CVE-2023-40283, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208, CVE-2023-4244, CVE-2023-42753, CVE-2023-42754, CVE-2023-42755, CVE-2023-45863, CVE-2023-45871, CVE-2023-4622, CVE-2023-4623, CVE-2023-4921, CVE-2023-51780, CVE-2023-51781, CVE-2023-51782, CVE-2023-5717, CVE-2023-6606, CVE-2023-6931, CVE-2023-6932) (Bug #56972)
- **mariadb-10.3** (CVE-2023-22084) (Bug #57005)
- **openjdk-11** (CVE-2024-20918, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20952) (Bug #57010)
- **openssh** (CVE-2021-41617, CVE-2023-48795, CVE-2023-51385) (Bug #56940)
- **pillow** (CVE-2023-50447) (Bug #57032)
- **postfix** (CVE-2023-51764) (Bug #57030)
- **squid** (CVE-2023-46728, CVE-2023-46846, CVE-2023-46847, CVE-2023-49285, CVE-2023-49286, CVE-2023-50269) (Bug #56964, Bug #57009)
- **sudo** (CVE-2023-28486, CVE-2023-28487, CVE-2023-7090) (Bug #57031)
- **unbound** (CVE-2023-50387, CVE-2023-50868) (Bug #57081)
- **univention-mail-postfix** (CVE-2023-51764) (Bug #56957)
- **wpa** (CVE-2023-52160) (Bug #57108)
- **xorg-server** (CVE-2023-6377, CVE-2023-6478, CVE-2023-6816, CVE-2024-0229, CVE-2024-21885, CVE-2024-21886) (Bug #56923, Bug #57006)

- The following updated packages from Debian 10.13 are included:

  **ansible asterisk cjson debian-security-support engrampa fontforge gsoap haproxy iwd keystone kodi libapache2-mod-auth-openidc libgit2 libjwt libreoffice libspreadsheet-parseexcel-perl libspreadsheet-parsexlsx-perl libuv1 man-db openvswitch osslsigncode php-guzzlehttp-psr7 php-phpseclib phpseclib python-asyncssh python-django rabbitmq-server rear ruby-httparty spip subunit tinyxml wireshark wordpress xerces-c yard**

- The following packages have been moved to the maintained repository of UCS:

  **orcania** (Bug #49006), **rhonabwy** (Bug #49006), **ulfius** (Bug #49006), **yder** (Bug #49006)

CHAPTER

TWO

# BASIC SYSTEM SERVICES

## 2.1 Univention Configuration Registry

- Fix traceback when `Interfaces()` is used with `ReadOnlyConfigRegistry()` (Bug #56911).

CHAPTER

THREE

# DOMAIN SERVICES

## 3.1 OpenLDAP

- During normal replication objects with `objectClass=lock` are not replicated. But during initial join they were. By adjusting the filter in the listener module this is now avoided, speeding up initial replication (Bug #56954).

### 3.1.1 Listener/Notifier domain replication

- During normal replication objects with `objectClass=lock` are not replicated. But during initial join they were. By adjusting the filter in the listener module this is now avoided, speeding up initial replication (Bug #56954).
- In case the communication to the notifier fails, e.g. due to a restart of the Univention Directory Notifier service on the Primary Directory Node, the listener did not retry but exit and relies on **`systemd`** to get restarted. This strategy does not work during the initialization phase while joining, when the listener is not yet run as **`systemd`** service. A retry mechanism has been introduced for this case, which is similar to what we already did for the connection to the LDAP server. There is a new Univention Configuration Registry Variable `listener/notifier/retries` with default 30. There is an exponential back-off algorithm to delay the retries and log messages are generated showing what is going on (Bug #57024).

## 3.2 DNS server

- DNS zones are now detected by having a `SOA` record instead of having a relative name `@`. This is allowed as DNS labels might consist of any 8-bit octets including an escaped `\@`. Deleting such entries resulted into the complete zone being dropped from **`BIND9`** (Bug #50385).
- The listener module writing the **`BIND9`** configuration files now ignores DNS zone files with invalid file names (Bug #57013).

CHAPTER

FOUR

# UNIVENTION MANAGEMENT CONSOLE

## 4.1 Univention Management Console web interface

- For enhanced automated testing the UDM HTTP REST API now handles requests with mime type `application/json-patch+json` (Bug #55555).
- The UDM HTTP REST API now supports authentication via the `Bearer` authentication scheme (Bug #49006).
- UDM HTTP REST API now supports a different LDAP base for each Univention Directory Manager module. This is a requirement for the blocklist feature (Bug #57039).
- After log rotating log files of the UDM HTTP REST API, the service is reloaded so that it logs into the new files (Bug #54338).
- All Univention Directory Manager log lines are now prefixed with the request ID. This can be disabled via the Univention Configuration Registry Variable `directory/manager/rest/debug/prefix-with-request-id` (Bug #56970).
- For containerized environments, the UDM HTTP REST API OpenAPI Schema user interface is now exposed via the UDM HTTP REST API server as well (Bug #57058).
- The replacement of the fallback Univention Management Console logger has been adjusted to use **`univention.logging`** (Bug #55324).

## 4.2 Univention Portal

- The HTML title and icon of the Portal is now configurable via the Univention Configuration Registry Variables `umc/web/title` and `umc/web/favicon` (Bug #56917).
- The labels of the self-service password forgotten form were always displayed in English when they were accessed directly via URL without navigating through the portal (Bug #56853).

## 4.3 Univention Management Console server

- The custom `univention.debug` wrapper of Univention Management Console has been replaced by the new logging interface `univention.logging` (Bug #55324).
- The Univention Configuration Registry Variable `ldap/server/sasl/mech_list` has been added to allow restricting the list of SASL (Simple Authentication and Security Layer) mechanisms that the local LDAP server offers. By default GSS-SPNEGO and NTLM get disabled with the update, because they don't work properly with **`slapd`** in UCS (Bug #56868).

- Due to frequent corruption of the on-disk SAML (Secure Authentication Markup Language) identity cache the default in multiprocessing mode has been changed to the in-memory cache. The Univention Configuration Registry Variable `umc/saml/in-memory-identity-cache` has therefore been removed (Bug #54880).
- The valid URI schemes for the SAML attribute consuming service and single logout endpoints are now configurable via the Univention Configuration Registry Variable `umc/saml/schemes` (Bug #57060).
- The Univention Management Console has been prepared to support login via OpenID Connect, which is currently unsupported and therefore disabled by default (Bug #49006).
- The HTML title and icon of Univention Management Console is now configurable via the Univention Configuration Registry Variables `umc/web/title` and `umc/web/favicon` (Bug #56917).
- An icon that is shown in the UCS license import dialog in Univention Management Console had to be replaced with a new one that has an OSI compliant license (Bug #56717).

## 4.4 Univention App Center

- The replacement of the fallback Univention Management Console logger has been adjusted to use `univention.logging` (Bug #55324).

## 4.5 Univention Directory Manager and command line interface

- The Univention Configuration Registry Policy Univention Directory Manager module now has an attribute indicating that it supports being assigned to an object multiple times (Bug #57046).
- A file descriptor leak in the Univention Directory Manager CLI server has been fixed (Bug #57089).
- Fix reaping terminated child processes (Bug #7735).
- Fix a potential infinite loop in handling Samba logon hour syntax (Bug #28496).
- Adjusted DNS object handling to fix compatibility with the UDM HTTP REST API (Bug #55555).
- The cron job for deleting expired block list entries now runs only if block lists are activated (Bug #57102).
- Fix escaping of DNS labels and names (Bug #50385).
- Allow using domain `home.arpa` from **RFC 8375** (Bug #55612).
- The StartTLS operation mode is now configurable via the Univention Configuration Registry Variable `directory/manager/starttls`. This is required in a Kubernetes environment (Bug #57098).
- The log messages of Univention Directory Manager are now logged via the Python `logging` interface, which is configured to still log to the `univention.debug` log stream. This is a prerequisite for prefixing log lines with the request ID in the UDM HTTP REST API (Bug #56970).
- The `uldap` library now supports the SASL binding mechanism `OAUTHBEARER` (Bug #49006).
- On UCS 5.2 systems purely numeric user and group names are no longer allowed by default. The Univention Configuration Registry Variables `directory/manager/user/enable-legacy-username-format` and `directory/manager/group/enable-legacy-cn-format` have been added to optionally allow such names if needed. System upgrades detect whether fully numeric names are already in use, in which case they are automatically allowed (Bug #56232).
- The new logging interface `univention.logging` is used to initialize `univention.debug` (Bug #55324).
- A missing dependency to **`python-univention-debug`** has been added, which preserves Python 2.7 compatibility (Bug #57064).

## 4.6 Modules for system settings / setup wizard

- The Univention Directory Manager CLI daemon is now restarted after setting the LDAP base during system setup (Bug #57039).
- A incompatibility with newer versions of **dnspython** has been fixed (Bug #56911).

## 4.7 System diagnostic module

- The diagnostic plugin for checking SAML (SSO (Single Sign-on)) certificates now also supports the Keycloak identity provider (Bug #55976).
- The diagnostic module **31_file_permissions** has been extended to include sensitive files for OIDC (OpenID Connect) configuration (Bug #49006).
- A check has been added to verify that the LDAP server's configuration file has the file system permissions 0640 (Bug #57038).

## 4.8 Other modules

- A Univention Management Console module for blocklist lists and entries has been added (Bug #57043).
- Existing Univention Configuration Registry policies attached to a container are no longer deleted when multiple ones previously existed and a new one is added (Bug #57046).
- The error handling when super-ordinate objects don't exist has been repaired (Bug #55555).

CHAPTER

FIVE

# UNIVENTION BASE LIBRARIES

- A new Python module `univention.logging` has been introduced which provides a Python `logging` handler for `univention.debug`. It allows software components to use the `logging` interface of Python while logging into a `univention.debug` stream (Bug #55324).
- Log messages are no longer erroneously logged by the wrong logger when `univention.debug2` is used but `univention.logging` isn't imported (Bug #57026).
- The detection of the correct log level has been repaired in case `univention.debug` was not initialized via `univention.logging` (Bug #57101).
- The StartTLS operation mode is now configurable via the Univention Configuration Registry Variable `directory/manager/starttls`. This is required in a Kubernetes environment (Bug #57098).
- An unused dependency on **`py3dns`** has been removed (Bug #56911).
- The `uldap` library now supports the SASL binding mechanism `OAUTHBEARER` (Bug #49006).
- The log messages of `uldap` are now logged via the Python `logging` interface, which is configured to still log to the `univention.debug` log stream. This is a prerequisite for prefixing log lines with the request ID in the UDM HTTP REST API (Bug #56970).
- The new LDAP database `cn=internal` has been added to store blocklist entries (Bug #57038).
- The LDAP server has been extended with the `OAUTHBEARER` SASL mechanism, which is disabled by default (Bug #49006).
- A memory leak in the UDM HTTP REST API has been fixed, which was caused by not discarding unused weak references in the `univention.lib.i18n.Translation` (Bug #56420).

CHAPTER

SIX

# SOFTWARE DEPLOYMENT

- On UCS 5.2 systems purely numeric user and group names are no longer allowed by default. The Univention Configuration Registry Variables `directory/manager/user/enable-legacy-username-format` and `directory/manager/group/enable-legacy-cn-format` have been added to optionally allow such names if needed. System upgrades detect whether fully numeric names are already in use, in which case they are automatically allowed (Bug #56232).
- **`univention-system-stats`** collects system information periodically. One of the commands it uses is **`top`**. The parameter `c` has been added to show the complete process command line in the output of **`top`** (Bug #50567).

## 6.1 Software monitor

- The dependency on **`py3dns`** has been replaced by **`dnspython`** to support EDNS, which is required for virtual machines on AWS-EC2 and OpenStack (Bug #56911).
- The StartTLS operation mode is now configurable via the Univention Configuration Registry Variable `directory/manager/starttls`. This is required in a Kubernetes environment (Bug #57098).

CHAPTER

SEVEN

# SYSTEM SERVICES

## 7.1 SAML

- The **univention-keycloak** scripts has been extended to support more parameters for the **init** command (Bug #57001).
- The standard configuration for Keycloak has been changed to allow machine accounts to login (Bug #57100).
- The package **univention-keycloak** ships the command line script **univention- keycloak-migration-status** which is used before the update to UCS 5.2 to check whether the migration to Keycloak is complete. The requirement to install the Keycloak app before the update has been dropped. The update to UCS 5.2 will be possible without the installation of the Keycloak app (Bug #56888).
- Commands to manage proxy realms (supplemental logical IDP (Identity Provider)'s in Keycloak that authenticate users on the default IDP) have been added to **univention-keycloak** (Bug #56884).
- The **univention-keycloak** scripts has been extended to support more parameters for the `oidc/rp` creation (Bug #49006).

## 7.2 Univention self service

- The connection settings for the **memcached** and **PostgreSQL** databases are now configurable via Univention Configuration Registry Variables. This is a requirement to run the self service in a containerized environment (Bug #57061).

## 7.3 Mail services

- Avoid duplicate entries in `/etc/fetchmailrc` when running a listener re-synchronization (Bug #56521).
- Fixed migration script LDAP filter to only process user objects (Bug #57090).
- The Fetchmail listener now writes atomically to `/etc/fetchmailrc` (Bug #56587).

## 7.4 Dovecot

- The type of the Univention Configuration Registry Variable `mail/dovecot/logging/auth_verbose_passwords` has been changed to `str`, so that the validation in Univention Configuration Registry strict type setting mode passes (Bug #56520).

## 7.5 RADIUS

- The Univention Configuration Registry Variable `freeradius/conf/allow-mac-address-authentication` has been added to to allow authentication via MAC address and VLAN-assignment for computer objects. By default, this feature is disabled (Bug #56060).

## 7.6 Other services

- The directory `/var/log/univention/listener_modules/` and `/var/log/apt/history.log` are now also fetched in a Univention Support Information archive (Bug #56962).

CHAPTER

EIGHT

# SERVICES FOR WINDOWS

## 8.1 Samba

- When joining a system to a UCS domain with a large number of objects in the LDAP directory, the script **`create_spn_account.sh`** restarted the S4-Connector too often while waiting for the service principal name to appear in the Samba/AD SAM directory, possibly causing additional delay. (Bug #57027).
- When stopping the Samba processes, a process could remain e.g. bound to port 135, causing problems for Samba restarts. The script stopping the processes has been made more robust (Bug #56914).

## 8.2 Univention S4 Connector

- During normal replication objects with `objectClass=lock` are not replicated. But during initial join they were. By adjusting the filter in the listener module this is now avoided, speeding up initial replication (Bug #56954).
- Initial join could take a long time in cases where customers have a lot of DNS records in Samba/AD. The joinscript now prioritizes objects (DNS zones etc) that are essential for operation of Samba/AD. This improves usability during initial joins and rejoins (Bug #56956).
- Group member DNs with containing special characters that require escaping can be notated in different ways. When comparing them, this has not been taken into consideration, leading to rejects and tracebacks in the log file. (Bug #57072).
- The StartTLS operation mode is now configurable via the Univention Configuration Registry Variable `directory/manager/starttls`. This is required in a Kubernetes environment (Bug #57098).

## 8.3 Univention Active Directory Connection

- During normal replication objects with `objectClass=lock` are not replicated. But during initial join they were. By adjusting the filter in the listener module this is now avoided, speeding up initial replication (Bug #56954).
- Group member DNs with containing special characters that require escaping can be notated in different ways. When comparing them, this has not been taken into consideration, leading to rejects and tracebacks in the log file. (Bug #57072).
- The StartTLS operation mode is now configurable via the Univention Configuration Registry Variable `directory/manager/starttls`. This is required in a Kubernetes environment (Bug #57098).

CHAPTER

NINE

# OTHER CHANGES

- A PAM and a SASL module for `OAUTHBEARER` (**RFC 7628**) has been introduced (Bug #49006).

# INDEX

## B



## C

## D



## E

## F



## L



## M



## N



## R



## U