

## UCS 3.2-3 Release Notes



**Release notes for the installation and update  
of Univention Corporate Server (UCS) 3.2-3**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2014 Univention GmbH

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

[feedback@univention.de](mailto:feedback@univention.de)

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

## Table of Contents

1. Release highlights .....	5
2. Recommended update order for environments with more than one UCS server .....	6
3. Preparation of update .....	7
4. Postprocessing of the update .....	8
4.1. Operating a local repository server / pre-up/ post-up scripts .....	8
5. Further notes on selected packages .....	9
5.1. Collection of usage statistics when using the free-for-personal-use version .....	9
5.2. UEFI installation DVD .....	9
5.3. Scope of security support for Webkit, Konqueror und QtWebKit .....	9
5.4. Recommended browsers for the access to the Univention Management Console .....	9
5.5. Restrictions in Samba 4 operation .....	10
5.6. Installation in VirtualBox .....	10
5.7. Installation in Citrix XenServer .....	10
5.8. Migration of a Samba 3 environment to Samba 4 .....	10
5.9. Xen .....	11
6. Changelog .....	12
6.1. General .....	12
6.2. Univention Installer .....	12
6.3. Univention Updater .....	12
6.4. Basic system services .....	12
6.4.1. NFS .....	12
6.4.2. procps .....	12
6.4.3. rsync .....	12
6.4.4. Web .....	12
6.4.5. Quota .....	12
6.5. Domain services .....	13
6.5.1. Univention Directory Manager .....	13
6.5.2. OpenLDAP .....	13
6.5.2.1. LDAP ACL changes .....	13
6.5.2.2. LDAP schema changes .....	13
6.5.2.3. Listener/Notifier domain replication .....	13
6.5.3. Join .....	14
6.6. Univention Management Console .....	14
6.6.1. Univention Management Console web interface .....	14
6.6.2. Univention Management Console server .....	15
6.6.3. Univention App Center .....	15
6.6.4. Basic settings / Appliance mode .....	16
6.6.5. Computers module .....	16
6.6.6. Other modules .....	16
6.6.7. Univention Directory Manager command line interface and related tools .....	16
6.7. Univention Library .....	16
6.8. System services .....	17
6.8.1. Spam/virus detection and countermeasures .....	17
6.8.2. Nagios .....	17
6.8.3. Proxy services .....	17
6.8.4. PAM / Local group cache .....	17
6.8.5. Other services .....	17
6.9. Virtualisation .....	17
6.9.1. Xen .....	17
6.10. Services for Windows .....	18
6.10.1. Samba NT domain support .....	18
6.10.2. Samba AD domain support .....	18

6.10.3. Univention AD Takeover .....	18
6.10.4. Univention S4 Connector .....	19
6.10.5. Univention Active Directory Connector .....	19
6.11. Other changes .....	19
Bibliography .....	21

# Chapter 1. Release highlights

With Univention Corporate Server 3.2-3, the third point release for Univention Corporate Server (UCS) is now available. It includes all errata updates issued for UCS 3.2-2.

- The new module *Active Directory Connection* merges the domain administrated by UCS and an existing Active Directory. UCS is then available as a platform for the integrated operation of apps in an Active Directory domain.
- The UCS setup wizard has been completely overhauled and now guides users particularly comfortably through the domain configuration of UCS and detects, for example, configuration settings automatically and suggests useful defaults.
- PHP 5.4.4 has been back-ported to UCS 3.2. It can be installed from a separate repository and will receive security updates.
- The OpenLDAP replication has been improved significantly by tracking changes in the directory service with unique IDs. The replication performance has been improved and replication errors have been reduced.
- The Linux Kernel package has been updated to version 3.10.11. Besides many bug fixes, this improves the hardware support.
- The Active Directory compatibility has been improved. UCS now supports the Microsoft Data Protection Application Program Interface (DPAPI).

## Chapter 2. Recommended update order for environments with more than one UCS server

In environments with more than one UCS system, the update order of the UCS systems must be borne in mind:

The authoritative version of the LDAP directory service is maintained on the master domain controller and replicated on all the remaining LDAP servers of the UCS domain. As changes to the LDAP schemes can occur during release updates, the master domain controller must always be the first system to be updated during a release update.

It is generally advisable to update all UCS systems in one maintenance window whenever possible.

## Chapter 3. Preparation of update

It must be checked whether sufficient disk space is available. A standard installation requires a minimum of 6 GB of disk space. Depending on the scope of the existing installation, the update will require at least another 1 GB of disk space for the downloading and installation of the packages.

For the update, a login should be performed on the console with the *root* user and then the update started there. Alternatively, the update can be initiated using the Univention Management Console.

Remote updating via SSH is not recommended as this may result in the update procedure being cancelled if the network connection is interrupted, for example, and this can affect the system. If updating should occur over a network connection nevertheless, it must be verified that the update continues despite disconnection from the network. This can be done, for example, using the tools `screen` and `at`, which are installed on all system roles.

## Chapter 4. Postprocessing of the update

Following the update, new or updated join scripts need to be executed. This can be done in two ways: Either using the UMC module **Domain join** or by running the command `univention-run-join-scripts` as the user `root`.

Subsequently the UCS system should be restarted.

### 4.1. Operating a local repository server / pre-up/ post-up scripts Feedback

Pre-up and postup scripts are scripts which are run before and after release updates (e.g., for post-processing the update, for example by uninstalling obsolete packages). As of UCS 3.2, these scripts are cryptographically signed to prevent unauthorized modification. During the update and when mirroring the repository these signatures are checked. If they're invalid or missing, the action is aborted.

If a repository server is operated with UCS 3.1-x, it should be updated to UCS 3.2 before additional systems can be updated to UCS 3.2-1 or newer.

If it is not possible to update the repository server, the signature files must be downloaded manually:

```
LOCAL_DIR="/var/lib//univention-repository/mirror"
SERVER="http://updates.software-univention.de"
for release in 3.2-0 3.2-1 3.2-2 3.2-3; do
  for script in preup postup; do
    file="3.2/maintained/$release/all/$script.sh.gpg"
    wget -O "$LOCAL_DIR/$file" "$SERVER/$file"
  done
done
```

Alternatively, it is also possible to disable the signature checks, which can be a security risk. For the repository server this can be done by setting the Univention Configuration Registry variable `repository/mirror/verify` to `false`. For the update the Univention Configuration Registry variable `repository/online/verify` must be set to `false` on all systems.

## Chapter 5. Further notes on selected packages

### 5.1. Collection of usage statistics when using the free-for-personal-use version

Feedback 

Anonymous usage statistics on the use of the Univention Management Console are collected when using the *free for personal use* version of UCS (which is generally used for evaluating UCS). The modules opened are logged in an instance of the web traffic analysis tool Piwik. This makes it possible for Univention to tailor the development of the Univention Management Console better to customer needs and carry out usability improvements.

This logging is only performed when the free-for-personal-use license is used. The license status can be verified by clicking on the cog symbol in the top righthand corner of the Univention Management Console and selecting **License information**. If *Free for personal use edition* is listed under **License type**, this version is in use. When a regular UCS license is used, no usage statistics are collected.

Indendependent of the licence used, the statistics generation can be deactivated by setting the Univention Configuration Registry variable `umc/web/piwik` to *false*.

### 5.2. UEFI installation DVD

Feedback 

In addition to the standard installation DVD there is also a medium with support for the Unified Extensible Firmware Interface standard (UEFI) available for the amd64 architecture.

It must be used instead of the standard DVD on systems which only support a UEFI boot.

### 5.3. Scope of security support for Webkit, Konqueror und QtWebKit

Feedback 

Webkit, Konqueror and QtWebKit are shipped in the maintained branch of the UCS repository, but not covered with security support. Webkit is primarily used for displaying HTML help pages etc. Firefox should be used as the web browser.

### 5.4. Recommeded browsers for the access to the Univention Management Console

Feedback 

Univention Management Console uses numerous JavaScript and CSS functions to display the web interface. Cookies need to be permitted in the browser. The following browsers are recommended:

- Chrome as of version 14
- Firefox as of version 10
- Internet Explorer as of version 9
- Safari (on the iPad 2)

Users with older browsers may experience display or performance problems.

## 5.5. Restrictions in Samba 4 operation

Feedback 

Some Active Directory functions are currently not available in Samba 4:

- Microsoft Windows domain controllers must not be joined in a Samba 4 domain currently.
- Selective replication is not possible with Samba 4 as this is not supported by Active Directory in principle (in UCS@school selective replication is implemented through the listener/notifier replication mechanism).
- Samba 4 does not currently support forest domains.
- Samba 4 does not currently support trust relationships.

Further information can be found in Chapter 8 of the [ucs-handbuch].

## 5.6. Installation in VirtualBox

Feedback 

During the installation of UCS in the virtualization solution VirtualBox, a VirtualBox bug may appear which has been corrected in version 4.2: if UCS has been successfully installed and the DVD is still in the disk drive, the installation DVD offers the option **Boot from first harddisk partition**. If you select this option, VirtualBox freezes.

For Linux distributions which still use Virtualbox 4.0 or 4.1, either the installation DVD should be removed from the drive settings of the VirtualBox VM or **F12** pressed when starting the virtual instance and the hard drive selected as a boot partition as a workaround before starting the UCS VM. UCS will then start successfully.

## 5.7. Installation in Citrix XenServer

Feedback 

When UCS is installed in the virtualization solution Citrix XenServer 6.0 - 6.2, the GRUB menu of the Univention installer is not shown with the Cirrus graphics card emulated as standard. The Univention Installer can be started directly by pressing the **ENTER** key; alternatively, the installation starts automatically after sixty seconds. The Univention Installer which then starts is displayed as normal.

To display GRUB correctly, the graphics card emulated by XenServer can be reconfigured. This is done by logging on to the XenServer system as the *root* user. Firstly, the `xe vm-list` command is used to determine the UUID of the virtual machine. The following command is then used to reconfigure the emulated graphics card to VGA:

```
xe vm-param-set uuid=UUIDVM platform:vga=std
```

## 5.8. Migration of a Samba 3 environment to Samba 4

Feedback 

There are two basic procedures for migrating Samba 3 to Samba 4:

- Setup of a parallel Samba 4 domain. Both domains use different NetBIOS names and SIDs. The clients then join the Samba 4 step by step.
- Migration of all systems within one maintenance window.

Both procedures are documented in detail in the Univention Wiki: [http://wiki.univention.de/index.php?title=Migration\\_from\\_Samba\\_3\\_to\\_Samba\\_4](http://wiki.univention.de/index.php?title=Migration_from_Samba_3_to_Samba_4).

## 5.9. Xen

If the Xen hypervisor is used and the memory limit for the Dom0 has been configured using the Univention Configuration Registry-Variable `grub/xenhopt`, the value should be updated to include the `,max:` part as well. See the [http://wiki.univention.de/index.php?title=UVMM\\_Quickstart-3.1/en#Configuring\\_the\\_Dom0](http://wiki.univention.de/index.php?title=UVMM_Quickstart-3.1/en#Configuring_the_Dom0) for details.

# Chapter 6. Changelog

Listed are the changes since UCS 3.2-2:

## 6.1. General

Feedback 

- All security updates issued for UCS 3.2-2 are included.

## 6.2. Univention Installer

Feedback 

- The component *Active Directory Connector* has been renamed to *Active Directory Connection* in the software selection of the installer (Bug 35414).

## 6.3. Univention Updater

Feedback 

- The local UCR variable *uuid/license* is now removed if the key ID is missing in the UCS license (Bug 34809).
- `univention-add-app` no longer registers a link on the UCS startsite and removes the component again if called with `--master` (just like the App Center module) (Bug 35022).
- The component installation status is now transferred via the apt user agent (Bug 33807).

## 6.4. Basic system services

Feedback 

### 6.4.1. NFS

Feedback 

- This update fixes a bug in the NFS utils package for users with many groups (Bug 34597).

### 6.4.2. procps

Feedback 

- This update fixes a bug in the procps package for users with many groups (Bug 34596).

### 6.4.3. rsync

Feedback 

- This update adds a new option `--dirs-update` to rsync (Bug 34430).
- The parameter `--dirs-update` was introduced with erratum 121. When using this parameter it could happen that the permissions were not transferred as expected. This error has been fixed. (Bug 35105).

### 6.4.4. Web

Feedback 

- The URL of the Univention App Center landing page has changed. Therefore, the corresponding links in the UCS overview page have been adapted (Bug 34864).
- Links to local web interfaces of installed Apps were placed on top of the UCS overview page if no priority was specified via UCR. They will now be positioned at the end (Bug 33750).

### 6.4.5. Quota

Feedback 

- The quota for the root (/) partition can now be configured via the filesystem quota UMC module (Bug 31277).

- Update for univention-user-quota. Evaluate the share policy flag "*reapplyeverylogin*" and (re-)apply quota settings on every user login if set (Bug 33174).
- Correct behaviour while searching for the most restrictive user quota settings on a mountpoint (Bug 33174).

## 6.5. Domain services

Feedback 

### 6.5.1. Univention Directory Manager

Feedback 

- Removing all Nagios services from a computer object no longer yields an error (Bug 33120, Bug 34037).
- Same for Nagios hosts (Bug 34037).
- Adding a DNS reverse zone to a computer object while removing an IP address no longer yields an error as well (Bug 34250).
- Documentation for a UCR variable added that makes the name of an object in the frontend grid configurable (Bug 34200).
- Removed the input field Organisation from the group *Personal information* and added it to the group *Organisation* (Bug 28630).
- Added new option to share-userquota policy: Reapply quota on every login (Bug 33174).
- Add possibility to mark UDM properties as readonly when UCS is part of an Active Directory domain (Bug 34092).
- The script "proof\_uniqueMembers" will no more crash on empty uniqueMember attributes (Bug 33030).

### 6.5.2. OpenLDAP

Feedback 

- This update adds *entryUUID* to the list of indexed LDAP attributes, which is used by the Univention Directory Listener to track moved objects (Bug 34815).
- The OpenLDAP schema for NIS (*nis.schema*) has been altered: The schema definition of the attribute *shadowExpire* contains now a ORDERING statement (Bug 35329).
- A new OpenLDAP overlay module has been added: *pwd\_scheme\_kinit*. It allows to set the userPassword attribute to *{KINIT}* which redirects the authentication to a kerberos server (Bug 35092).
- Support for the overlay module *pwd\_scheme\_kinit* has been added (Bug 35093).
- The UCR variable *ldap/sasl/secprops/maxssf* has been added to configure the *sasl\_secprops\_maxssf* value in */etc/ldap/ldap.conf* (Bug 35513).

#### 6.5.2.1. LDAP ACL changes

Feedback 

- A regression in the LDAP ACLs has been fixed. The ACLs for the "dc" and "memberserver" containers now again allow subfolders (in *cn=dc* resp. *cn=memberserver*) (Bug 34554).

#### 6.5.2.2. LDAP schema changes

Feedback 

- New share-userquota binary attribute: Reapply quota on every login (Bug 33174).

#### 6.5.2.3. Listener/Notifier domain replication

Feedback 

- The case of distinguished names (DN) sometime differs between different clients and is now ignored (Bug 34835).

- A rename of an LDAP object can lead to a single-values attribute becoming multi-valued, which breaks multiple modules, especially the synchronization to Samba. The listener now implements `delold=1` and removes all old RDNs to just keep the new RDN (Bug 34802).
- When an object is renamed or moved via a container, which is later deleted, the listener fails to follow the rename. This has been fixed by creating a fake temporary container (Bug 34833).
- In case of an error the replication listener handler is now restarted with the old object from the directory listener (Bug 34759).
- This update fixes a replication problem, when an object is removed and re-created at the same location. This happened when a failing listener module prevents the removal of the object from the listener cache, which is used to track objects being moved (Bug 35261).

### 6.5.3. Join

 Feedback 

- `univention-join` now checks for the AD member mode during the join. If the domain is in the AD member mode, `univention-join` configures the local system as part of the AD domain. (Bug 35470 Bug 35446).

## 6.6. Univention Management Console

 Feedback 

### 6.6.1. Univention Management Console web interface

 Feedback 

- The UMC grid can now allow the execution of an action even though some of the selected items are not executable with regard to the action (Bug 34965).
- A function has been added to reload the modules of the overview tab on the fly (Bug 34243).
- A default link to UMC has been added on the UCS overview page for unjoined systems (Bug 34317).
- When installing a new system which is neither a master domain controller master nor a backup domain controller backup, the UMC entry in the UCS overview page will no longer consider the UMC a domain administration tool, as the domain modules are only available on master and backup systems (Bug 33615).
- A timeout problem in the UMC web server has been fixed (Bug 35052).
- When a user cancels the dialogue which asks for a UMC server restart, the modules on the UMC overview page are now reloaded (Bug 34243).
- CSS rules have been adapted to apply the UMC theme to `dijit/form/Select` (Bug 34484).
- The `async` attribute is now used in the script tag that loads `dojo.js` (Bug 34484).
- UMC tabs and header are not shown in the appliance mode (Bug 34484).
- In the appliance mode, only the specified JavaScript module is loaded upon startup instead of all accessible JavaScript modules (Bug 34484).
- Dynamic reloading of translations is now supported (Bug 34484).
- A widget for radio buttons has been added (Bug 34484).
- A method `defer()` has been added to `umc/tools` (Bug 34484).
- The validation of forms has been fixed, such that invalid fields are marked with a red exclamation mark when calling `umc/widgets/Form:validate()` (Bug 34484).

- Vertical scrolling issues with *umc/widgets/Grid* in Firefox have been fixed (Bug 34484).
- The configuration property *labelConf* has been added to be able to configure LabelPanels directly (Bug 34484).
- Allow dynamic changing of *inlineLabel* in *umc/widgets/TextBox* (Bug 34484).
- The convenience method *isPageVisible()* has been added to *umc/widgets/Wizard* (Bug 34484).

## 6.6.2. Univention Management Console server

Feedback 

- The internal cache of UMC modules in the UMC Server is now invalidated before they are requested (Bug 34243).
- It is now possible for UMC modules to provide a user friendly error message when initialization failed (Bug 34723).
- Changes of system clock (e.g. due to NTP updates) will not make UMC processes die by timeout anymore (Bug 34105).
- The UMC server parses operation set strings more carefully now to avoid server crashes (Bug 25196).
- The error handling of requests have been improved (Bug 34244).

## 6.6.3. Univention App Center

Feedback 

- Improved performance: Applications are opened immediately when clicking on them from the app gallery (Bug 31915).
- Improved performance: When new apps are added or existing apps' meta information changes, new files need to be downloaded from the server. If many files have changed, instead of downloading them all one after another, a compiled archive is downloaded and the files are extracted. This also fixes issues with many concurrent connections opened on the App Center server (Bug 32935).
- A dedicated component for the Radius application is removed (if Radius is installed). It was added by mistake as *univention-radius* is part of the main repository (Bug 34867).
- The UCR variable *repository/app\_center/installed* is now set and kept up-to-date. It reflects the state of the installation status of all apps (Bug 35177).
- The details of an application do not show the note whether this application sends information to the vendor or not if it is a UCS component (Bug 35176).
- Fixed LDAP errors when registering applications: ID and Version of an application are now escaped (Bug 35136).
- The UCR variable *repository/app\_center/installed* is initially set during installation/update of this package (Bug 35271).
- When the system is part of a Windows Active Directory domain, certain applications are not shown (Bug 35454).
- When the system is part of a Windows Active Directory domain, certain applications warn before installation that a password service needs to be running on the Windows Domain Controller (Bug 35453).
- Linked the UCR variable *repository/app\_center/installed* to the creation of certain UMC module definition files. This fixes issues with modules not showing up in *Installed Apps* after the initial setup of the server (Bug 35565).

## 6.6.4. Basic settings / Appliance mode

Feedback 

- The setup wizard for UCS appliance has been entirely re-structured and rewritten, obsolete code paths have been cleaned up. Some of the new features include:
  - A live search for world-wide cities to preconfigure locale settings.
  - Wizard language can be changed on the fly without a page load.
  - Some fields (host + domain name, gateway address etc.) are pre-filled with suggested values to ease the configuration.
  - The UCS license activation can now be carried within the wizard.
  - UCS components from the App Center can be installed in the wizard. (Bug 34484)
- Running setup scripts will not terminate when the UMC module process does, and also keep the UMC module process from timing out (Bug 34105).
- Added welcome page with instructions to set a root password before accessing the setup wizard for EC2 setups (Bug 34388).

## 6.6.5. Computers module

Feedback 

- A traceback has been fixed which could occur when creating computer objects with a given DHCP or DNS zone, but without an IP address. The traceback could also occur when removing DHCP/DNS zones along with all IP addresses (Bug 33843).

## 6.6.6. Other modules

Feedback 

- When the initialization of the UMC module *univention-pkgdb*, or any command execution, fails because the PostgreSQL is not running, a user friendly error message will be shown instead of debug information in a feedback dialog (Bug 34723).

## 6.6.7. Univention Directory Manager command line interface and related tools

Feedback 

- The property that is used in the first column of the grid ("Name") is now configurable via UCR (Bug 34200).
- Some UDM attributes are shown as readonly if the domain is part of an Active Directory Domain (Bug 34092).
- Display a warning in Active Directory Mode before creating objects which are not synchronized back to AD (Bug 34093).
- Display a human readable error message when the connection to the LDAP server failed (Bug 34244).

## 6.7. Univention Library

Feedback 

- Several functions for configuring the AD member mode have been added to univention-lib (Bug 34091, Bug 35470, Bug 35467, Bug 35520, Bug 35551, Bug 35566).
- When an object is renamed in LDAP, the old relative distinguished name (RDN) values are kept by default. This leads to situations, where an attribute declared as single-valued may become multi-valued, which

breaks the replication to Samba 4 and confuses several other listener modules. This erratum changes the low-level Univention LDAP code to remove the old RDN values as well, as all other code paths already do so (Bug 34971).

## 6.8. System services

Feedback 

### 6.8.1. Spam/virus detection and countermeasures

Feedback 

- ClamAV has been updated to version 0.98.1 (Bug 33995).

### 6.8.2. Nagios

Feedback 

- Change `UNIVENTION_NTP` Nagios check to compare NTP server time by using the plugin `check_ntp_time`. The previous check also queried NTP server configuration options, which are not relevant for this check and, since UCS 3.2 errata 20, are not allowed to be queried from external sources (Bug 34570).

### 6.8.3. Proxy services

Feedback 

- The UCR variable `squid/forwardedfor` has been added to configure Squid's `forwarded_for` configuration directive (Bug 34025).

### 6.8.4. PAM / Local group cache

Feedback 

- Kerberos authentication is now limited to non-local accounts with `UID >= 1000`. The limit can be configured through the new Univention Configuration Registry variable `pam/krb5/minimum_uid` (Bug 34315).
- The mapping of user and group names in the UCR templates was not updated in all cases. This has been fixed (Bug 34742).
- The listener module `well-known-sid-name-mapping` now recognizes SID changes (Bug 35501).

### 6.8.5. Other services

Feedback 

- This update provides the older version 3.72 of `syslinux`, a boot loader for Linux. It is used by the UCS network installer. Due to some BIOS incompatibilities the newer `syslinux` from UCS-3 fails to boot some notebooks like the DELL E6510 either locally or via PXE. The older version can be installed as a replacement version if such problems occur. For this the packages `"syslinux3"` and `"syslinux3-common"` must be installed instead of `"syslinux"` and `"syslinux-common"` by using the command-line tool `"univention-install"` as the user `"root"` or as an Administrator through the UMC web interface by using the App-center module (Bug 33531).
- AD member mode has been added to `univention-heimdal` (Bug 35470).

## 6.9. Virtualisation

Feedback 

### 6.9.1. Xen

Feedback 

- This update rate-limits a log message printed by the QEMU device model to prevent the log-file from growing by 50 MiB/s after a virtual machine has been migrated (Bug 35488).
- A kernel OOPS on the Xen host while rebooting a Xen VM has been fixed. The error is caused by the Xen `netback` subsystem (Bug 35178).

## 6.10. Services for Windows

Feedback 

### 6.10.1. Samba NT domain support

Feedback 

- In Samba 3.6 and older the execution right in the ACL was not checked, so a client could execute a file even if it did not have execute rights on the file. In Samba 4.0, this has been fixed. To re-establishing the old behaviour the new UCR variable *samba/acl/allow/execute/always* has been added (default: True) (Bug 33785).
- Missing initialization of the UCR variable *samba/role* has been added to the postinst script of univention-samba (Bug 35584).

### 6.10.2. Samba AD domain support

Feedback 

- Modifications of access rights of GPOs could get reset by the sysvol replication. This affected directories in the sysvol share (Bug 33751).
- Clean up `/var/lib/samba/private` before new provision (relevant for UCS@school Slave PDCs) (Bug 32246).
- Preserve `/var/lib/samba/*`, only clear private subdir before re-join (Bug 35000).
- Preserve *rIDNextRID* during re-join and provision (Bug 34754).
- This update fixes an issue which caused a problem for the Windows DPAPI. To users it appeared as if stored credentials for Windows applications would not be remembered any longer by the applications after they changed the logon password for their account. Domains affected by this need to manually remove the object "CN=BCKUPKEY\_PREFERRED Secret" from the Samba directory service after the update to make Samba internally generate a new ticket for the Backupkey protocol (Bug 35287).
- In Samba 3.6 and older the execution right in the ACL was not checked, so a client could execute a file even if it did not have execute rights on the file. In Samba 4.0, this has been fixed. To re-establishing the old behaviour the new UCR variable *samba/acl/allow/execute/always* has been added (default: True) (Bug 35137).
- The univention-samba4 join script now always cleans up the samba private directory before the join and if the samba4 join fails, the join is aborted (Bug 34422).
- A typo in univention-samba4-backup has been fixed (Bug 35084).
- The UCR variable *samba4/backup/cron/options* has been added to configure options for the *univention-samba4-backup* script started by cron (Bug 35085).
- AD member mode has been added to univention-samba (Bug 35095, Bug 35470, Bug 35467).
- The joinscript of univention-samba4 was adjusted to abort if the domain is in AD member mode (Bug 35252).

### 6.10.3. Univention AD Takeover

Feedback 

- The UMC module for AD Takeover has been adjusted to fix a case where the path to one of the two default GPOs did not match the actual folder copied from the Windows AD server (Bug 34776).
- The UMC module for AD Takeover has been adjusted to support UCS domains in AD member mode (Bug 35346).

## 6.10.4. Univention S4 Connector

Feedback 

- The *entryUUID* of deleted objects in OpenLDAP is now saved to a local cache. This will prevent a recreation of deleted objects (Bug 32263).
- The synchronization has been changed to a diff based algorithm (Bug 33621).
- In some cases a removed group membership was not synchronized from OpenLDAP to Samba 4 in write mode (Bug 35238).
- Restart bind9 instead of samba4 if the *ldap/master* can't be resolved (Bug 34865).
- Two tools for removing rejected objects have been added:

```
/usr/share/univention-s4-connector/remove_ucs_rejected.py
```

```
/usr/share/univention-s4-connector/remove_s4_rejected.py  
(Bug 32194).
```

- Add a new parameter "acl xattr update mtime" for use in `smb.conf` share sections. This will be used for the `sysvol` share to make `rsync` recognize permission changes on directories (Bug 34431).
- An error in the internal conversation of the attribute *userParameters* has been fixed. This error could lead to a blocked samba process (Bug 34777).
- DNS updates of records with existing IPv6 addresses have been fixed (Bug 34868).
- Issues with the NetApp join have been fixed (Bug 34886).
- The `joinscript` of package *univention-s4-connector* was adjusted to abort if the domain is in AD member mode (Bug 35500).
- The command line script `univention-ad-takeover` has been removed since the UMC module is more recent (Bug 35514).

## 6.10.5. Univention Active Directory Connector

Feedback 

- Support for the `ad/member` mode has been added (Bug 35091).
- In some cases a removed group membership was not synchronized from OpenLDAP to Active Directory in write mode (Bug 35234).
- The AD certificate chain is no longer checked if there is no root certificate configured (Bug 35253).
- Kerberos support has been added to the UCS AD connector (Bug 35349).
- A script has been added for renaming groups and users with Well Known SIDs to the corresponding name in the AD domain. This script is for internal use by the setup wizard for the UCS in AD member mode (Bug 35507).
- A script has been added to grant read permission to the `CN=Deleted Objects` container in Active Directory. This is only required for the AD Member mode (Bug 35566).

## 6.11. Other changes

Feedback 

- The following packages have been moved to the maintained repository

*Other changes*

- *texlive-generic-extra* (Bug 33611)
- *python-dateutil, python-tz, libboost-thread1.42.0, libosp-uuid16, libxerces-c3.1, php-auth, augeas-lenses, libaugeas0, python-augeas, python-cheetah, libmail-spf-perl, manpages-dev, re2c, zendframework* (Bug 34260)
- *rsyslog-relp* (Bug 34872)
- *php5-sqlite* (Bug 35030)
- *libapache2-mod-perl2, libapache2-reload-perl, libyaml-libyaml-perl, libdevel-symlinks-perl, libsd-resource-perl* (Bug 35160)
- *mt-st* (Bug 35388)
- This update provides the new archive signing key for UCS 4.0. UCS 4.0 is not released yet, but we already distribute the key in advance to ensure the availability of the archive key when updating from UCS 3.2-3 to UCS 4.0 at a later point (Bug 35213).

# Bibliography

[ucs-handbuch] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. <http://docs.univention.de/manual-3.2.html>.