UCS 3.2-2 Release Notes

**Release notes for the installation and update
of Univention Corporate Server (UCS) 3.2-2**

Table of Contents

Chapter 1. Release highlights

With Univention Corporate Server 3.2-2, the second point release for Univention Corporate Server (UCS) is now available. It includes all errata updates issued for UCS 3.2-1.

- Domain joining of Windows clients with incorrect system times has been simplified; it is now no longer necessary to synchronise the system time in advance. In addition, password lockouts following unsuccessful login attempts are now also supported in Samba AD domains.

- Univention AD Takeover - the UCS solution for the automatic migration of an Active Directory domain to UCS - can now also be performed via a Univention Management Console module.

- The Univention App Center has been expanded further, for example: it is now also possible to provide applications which are not available for all processor architectures.

- The configuration of the access to WLAN networks via the RADIUS protocol can now be configured in the Univention Management Console thanks to the new Radius app.

- The Debian point update 6.0.9 has been integrated. It includes a wide range of bug fixes.

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

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; 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

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.

Indendepent 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

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

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

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

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

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

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

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.

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 for details.

Chapter 6. Changelog

Listed are the changes since UCS 3.2-1:

6.1. General

Feedback

- All security updates issued for UCS 3.2-1 are included.

- The Debian point update 6.0.9 has been integrated. It provides many bugfixes and also addresses some security issues (Bug 33272, Bug 33283, Bug 33287, Bug 33500, Bug 33776, Bug 33868, Bug 34136).

6.2. Univention Installer

Feedback

- If a base system was selected as the system role, a warning is now displayed explaining the consequences (Bug 34329).

- The warning about the missing BIOS boot partition is now displayed again after modifying the partition table (Bug 34334).

6.3. Basic system services

Feedback

6.3.1. Univention Configuration Registry

Feedback

- In some cases the file ownership was not preserved correctly when a file is committed (Bug 34241).

- The program `univention-check-templates` now also checks UCR template files for modifications by using the MD5 hash sum managed by `dpkg` (Bug 24010).

6.4. Domain services

Feedback

6.4.1. OpenLDAP

Feedback

- If the LDAP server is not available the tool `univention-ldapsearch` now tries to reconnect to the LDAP server. The count can be configured via the Univention Configuration Registry variable `ldap/client/retry/count`, which is set to 10 by default (Bug 34292, Bug 34293).

- LDAP schema extensions are now included sorted by their file name to guarantee stable ordering (Bug 34406).

- The OpenLDAP init script has been revised (Bug 34440).

6.4.1.1. Listener/Notifier domain replication

Feedback

- The shutdown message has been adjusted (Bug 32605).

- Moved objects are now tracked by their unique `entryUUID`. This fixes an issue, when objects in LDAP are modified and moved in short order, or while the listener is not running. (Bug 34355).

6.5. Univention Management Console

Feedback

6.5.1. Univention Management Console web interface

Feedback

- Display glitches with some progress bars have been fixed (Bug 34181).

- The detection of Internet Explorer 11 has been fixed (Bug 33990).

6.5.2. Univention Management Console server

- Added a method to the Univention Management Console web server to retrieve the client's IP address (Bug 34288).

- The UMC web server uses Apache as a proxy server. The timeout for proxy requests can now be configured with the Univention Configuration Registry variable `umc/http/session/timeout` (Bug 34005).

6.5.3. Univention App Center

- Renamed the button for buying an app from **Shop** to **Buy** (Bug 34183).

- Whitelisting and blacklisting of apps is now done based on the applications' ID (Bug 34145).

- Renamed the App ID for Tine 2.0 from tine20org to tine20 to reflect that this is the commercial version (Bug 33728).

- Components in the App Center's tab **Repository Settings** may have default packages which can be installed. Before this is done, the App Center now updates the package list (Bug 34278).

- Applications may now specify supported architectures. If an application only supports 64 bit, a 32 bit operating system will refuse to install it (Bug 34320).

- The tool `univention-register-apps` exits after two minutes if it gets stuck (Bug 34834).

6.5.4. Users module

- LDAP objects with the attribute `univentionObjectFlag:functional` are now ignored (Bug 34395).

6.5.5. Users module

- 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).

6.5.6. License module

- In the license dialog, the LDAP base DN is also shown when using the free-for-personal-use license (Bug 34117).

- LDAP objects with the attribute univentionObjectFlag:functional are now ignored (Bug 34395).

6.5.7. Other modules

- The **Change password** module showed an endless loading animation after successfully applying changes. Now the form is reloading properly (Bug 34367).

- The labels for widgets regarding the type of LDAP objects have been changed as the old ones could not reflect the grammatical case (Bug 34038).

www.univention.de

6.5.8. Univention Directory Manager command line interface and related tools

- UDM no longer creates temporary objects in `cn=univention` when moving containers, because `cn=univention` is ignored by the S4 connector and the S4 connector does not recognize the move (Bug 34266).

6.5.9. Development of modules for Univention Management Console

- Python UDM extensions are now installed with `update-python-support` (Bug 34421).

- The default value of a UDM property is now configurable via Univention Configuration Registry (e.g. by setting `directory/manager/web/modules/users/user/properties/mail-HomeServer/default`) (Bug 23765).

6.6. Univention Library

- `ldap_extension.py` now moves files using the Python function `shutil.move` instead of `os.rename`. This allows moving files across partitions (Bug 34104).

- `ldap_extension.py` did not handle the activation of a new LDAP extension correctly and restarted the LDAP server too often (Bug 34800).

- This update fixes *shell-univention-lib* to call Univention Configuration Registry with an absolute path to work regardless of the current `PATH` setting, especially for cases where `/usr/sbin/` is not in `PATH` (Bug 29241).

6.7. System services

6.7.1. Mail services

- The Postfix policy service listfilter (which is used to restrict e-mail delivery to groups and lists) is now executed as the user *listfilter* instead of the user *cyrus*. This allows the deployment of this feature in environments without the component **univention-mail-cyrus** (Bug 26910).

- The new Univention Configuration Registry variables `mail/postfix/ldaptable/starttls`, `mail/postfix/ldaptable/tlsrequirecert` and `mail/postfix/ldaptable/tlscacertfile` have been introduced to define whether and how Postfix should use TLS for LDAP lookups (Bug 34198).

- The listener module handling shared IMAP folders configured in the Univention Management Console now honours the Univention Configuration Registry variable `mail/cyrus/mailbox/delete` when deleting IMAP folders (Bug 34165).

6.7.2. Nagios

- The Univention Configuration Registry templates for the configuration and init files of the Nagios Remote Plugin Executor (NRPE) have been configured to use the PID file `/var/run/nagios/nrpe.pid` (Bug 34063).

- A buffer overflow in the setuid wrapper has been fixed (Bug 34041).

6.7.3. Proxy services

Feedback

- *cache_dir null /tmp* is no longer set if caching is disabled. This fixes the operation of Squid without caching (Bug 33332).

- The Univention Configuration Registry variable `squid/redirect` can now be used to configure the *url_rewrite_program* configuration directive of Squid. If the variable is set to *squidguard*, then */usr/bin/squidGuard -c /etc/squid/squidGuard.conf* is used for *url_rewrite_program* (Bug 32429).

- The join script of **univention-squid-kerberos** now checks if the service principal account already exists (Bug 33779, Bug 34575). In addition the saltPrincipal has been added to the Samba 4 keytab entry for the proxy service principal (Bug 32292).

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

6.8. Virtualisation

Feedback

6.8.1. Univention Virtual Machine Manager

Feedback

- The HTML5 VNC plugin now prevents browsers from caching `vnc_auto.html`. This avoids certificate problems with HTTPS connections using Internet Explorer (Bug 33968).

- The init script now uses *force-stop* and *force-restart* to handle blocked UVMMd processes (Bug 34321).

- A broken link to an Support Database article has been replaced by a link to the manual (Bug 34425).

- `libvirt-check.sh` has been added to virtualization nodes. It periodically tests if libvirtd responds and restarts libvirtd if necessary (Bug 33966).

- The logging of libvirtd can now be controlled using the Univention Configuration Registry variables `libvirt/log/level`, `libvirt/log/filters` and `libvirt/log/outputs` (Bug 34170).

6.9. Services for Windows

Feedback

6.9.1. Samba AD domain support

Feedback

- Domain account lockout for Windows clients joined into a Samba AD domain are now possible (Bug 34443, Bug 34305, Bug 32974).

- Support for correcting skewed clocks during domain was added. This allows joining Windows clients without requiring a time synchronisation first (Bug 34439).

- `samba-tool dbcheck` now also lists/handles name conflict objects and objects without object class (Bug 33616).

- The domain services database module was affected by a segmentation fault when handling objects without object class (Bug 33977).

- Versions in the package dependencies have been updated (Bug 33972).

- Randomise domain controllers in DFS referral replies, e.g. for the SYSVOL share (Bug 34370).

- Several possible deadlock situations in the DRS replication have been fixed (Bug 34545).

www.univention.de

- MS DFS support is now enabled on Samba AD domain controllers by default. With this new setting Windows clients ask for DFS redirects for the SYSVOL share, which may improve efficient network usage in branch site configurations (Bug 34326).

- `univention-samba4-backup` has been added to backup the samba provision directory. This tool is periodically executed by cron (configurable via the Univention Configuration Registry variable `samba4/backup/cron`) (Bug 34113).

6.9.2. Univention AD Takeover

Feedback 🗩

- The AD takeover can now be performed through a Univention Management Console module (Bug 34019, Bug 34139).

6.9.3. Univention S4 Connector

Feedback 🗩

- The S4 connector Python modules are now only built for Python 2.6 (Bug 31320).

- The user `pcpatch` is no longer ignored by default (Bug 34394).

- The start of multiple S4 connector instances is now prevented (Bug 34410).

- When creating a user in UCS a stronger password is used which fulfills the password complexity settings (Bug 34478).

- The Univention Configuration Registry variable `connector/s4/listener/disabled` has been added. If it is set to *true* the listener does not write any changes. This is helpful on a backup domain controller. The variable is not set by default during this upgrade (Bug 33858).

- During the group membership synchronization from Samba 4 to OpenLDAP an object mapping problem has been fixed (Bug 34197).

6.10. Other changes

Feedback 🗩

- The package *univention-radius* has been added (Bug 29465).

- The `/etc/issue` welcome message mentions where to find the management system. After installing this update the message will only be shown on domain controllers and member servers (Bug 34330).

- The dependency list of the package *univention-directory-manager-modules* has been updated. Prior to this change, *slapd* was left installed on a member server when using the appliance mode which could lead to problems when this system was querying LDAP (Bug 34201).

- The UDM CLI program `univention-directory-manager` now tries to start the internal UDM CLI server again if the first start was aborted (Bug 34784).

Bibliography

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