univention
be open.

UCS 3.2-4 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 3.2-4

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

feedback@univention.de

univention
be open.

Table of Contents

Chapter 1. Univention Corporate Server (UCS) 3.2-4

The fourth point release for Univention Corporate Server (UCS) is now available in the form of Univention Corporate Server 3.2-4. The online repository provided by Univention can be used to update existing UCS systems or, alternatively, updates can be installed from an update DVD. There are also UCS 3.2-4 ISO images available for new installations. UCS 3.2-4 includes all the errata updates published for UCS 3.2-3.

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 3.2-3 3.2-4; 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.

Regardless 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-manual].

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.

5.9. Xen

Feedback

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 3.2-3:

6.1. General

Feedback

All security updates issued for UCS 3.2-3 are included:

- Package ***apt*** CVE-2014-0487 CVE-2014-0488 CVE-2014-0489 CVE-2014-6273 (Bug 35948, Bug 35986, Bug 36277).
- Package ***bash***: CVE-2014-6271 CVE-2014-7169 CVE-2014-7186 CVE-2014-7187 (Bug 35992, Bug 36008).
- Package ***curl***: CVE-2014-3613 (Bug 35874).
- Package ***firefox-de***: CVE-2014-1547 CVE-2014-1555 CVE-2014-1556 CVE-2014-1557 CVE-2014-1544 CVE-2014-1562 CVE-2014-1567 CVE-2014-1568 CVE-2014-1574 CVE-2014-1576 CVE-2014-1577 CVE-2014-1578 CVE-2014-1581 CVE-2014-1585 CVE-2014-1586 CVE-2014-1583 (Bug 35807, Bug 35993, Bug 36175).
- Package ***firefox-en***: CVE-2014-1547 CVE-2014-1555 CVE-2014-1556 CVE-2014-1557 CVE-2014-1544 CVE-2014-1562 CVE-2014-1567 CVE-2014-1568 CVE-2014-1574 CVE-2014-1576 CVE-2014-1577 CVE-2014-1578 CVE-2014-1581 CVE-2014-1585 CVE-2014-1586 CVE-2014-1583 (Bug 35807, Bug 35993, Bug 36175).
- Package ***lua50***: CVE-2014-5461 (Bug 35770).
- Package ***lua5.1***: CVE-2014-5461 (Bug 35771).
- Package ***poppler***: CVE-2010-5110 (Bug 33265).
- Package ***procmail***: CVE-2014-3618 (Bug 35817).
- Package ***squid3***: CVE-2014-3609 (Bug 35732).
- Package ***xen-4.1***: CVE-2013-4368 CVE-2014-1950 CVE-2014-2599 CVE-2014-3124 CVE-2014-4021 CVE-2014-7154 CVE-2014-7155 CVE-2014-7156 CVE-2014-7188 (Bug 34115).

6.2. Univention Updater

Feedback

- The HTTP HEAD query of the updater now also transfers the component installation status (Bug 35645).
- The tool *univention-repository-create* has been updated and is now able to handle UCS-4 DVDs (Bug 36269).
- The updater package is now limited to Python 2.6 (Bug 34781).
- The postup.sh script was adapted to the univention-check-templates return codes (Bug 34972).

6.3. Basic system services

Feedback

6.3.1. Linux kernel and firmware packages

Feedback

- An overflow in the KVM time handling code prevented the start of a VM. This has been fixed (Bug 35808).

- In some situations the Xen netback driver caused an OOPS and prevented any VM from accessing the network. This has been fixed (Bug 35826).

6.3.2. Univention Configuration Registry

Feedback

- Skip writing of internal cache during configHandlers.load() if the process has no write permission (Bug 35368).
- univention-check-templates has been fixed to correctly handle conffiles with spaces (Bug 35202).

6.4. Domain services

Feedback

6.4.1. Univention Directory Manager

Feedback

- The modification of the alternative mail address is now allowed in AD member mode (Bug 35672).
- The syntax for group names has been adapted. The default group names of a French Active Directory are allowed now (Bug 35521).
- A traceback has been fixed if more than one colon is set in the automountInformation attribute (Bug 34541).
- The setting of the Kerberos principal name for computer/macos objects have been fixed (Bug 35526).
- A backslash in the `home share path` value of a user no longer results in a traceback (Bug 35953).

6.4.2. OpenLDAP

Feedback

6.4.2.1. Listener/Notifier domain replication

Feedback

- The notifier join script now waits for the first initialization of the listener on a DC master. This avoids a race condition during the DC master installation (Bug 35723).
- A replication issue has been fixed which could occur when joining a UCS DC into a domain which had the memberof LDAP overlay active at some point and later deactivated it (Bug 35480).
- Locking and signal handling of the univention-directory-listener has been improved (Bug 34013).
- Schema replication needs to filter out new operational (i.e. builtin) LDAP attributes which will be activated in UCS 4.0 (Bug 36113).
- Object replication needs to filter out operational ppolicy LDAP attributes which may be found on a UCS 4.0 master (Bug 36353).

6.4.3. Join

Feedback

- univention-join no longer overwrites the join.log on DC slave (Bug 34909).

6.5. Univention Management Console

Feedback

6.5.1. Univention Management Console web interface

Feedback

- If an email address is given during the system setup, the startup wizard won't ask for an activation address. This prevents a possible double registration (Bug 35711).

6.5.2. Univention Management Console server

Feedback

- Some displaying issues in UMC related to the new AD member mode have been fixed (Bug 35610).
- The handling of connections between the UMC parts has been improved. Faulty connections will be closed and if the connection between UMC server and UMC module dies, the UMC module shuts down immediately (Bug 32818).
- The broken timer handling in the qt backend of python-notifier has been fixed. This problem could lead e.g. to never stopping UMC modules (Bug 36472).

6.5.3. Basic settings / Appliance mode

Feedback

- After deactivating DHCP in the appliance wizard and switching to manual network configuration, the network interface remained in DHCP mode and ignored the static network configuration. This issue has been fixed (Bug 35601).
- Fixed suggestion of FQDN build from value entered in the organization field in appliance mode (Bug 34090).
- Moved setup of apache startsite on EC2 to an earlier stage in the boot process (Bug 35587).
- Do not show Firefox data submission policy popup during system setup (Bug 35721).
- The Windows NETBIOS domain name can now be up to 15 characters long (Bug 35605).
- Problems with reloading values and displaying messages after saving changes have been corrected (Bug 35599).
- The UMC now warns the user if DHCP is selected but a link-local IP address is used. This can occur if DHCP is preconfigured but no DHCP lease could be obtained (Bug 35815).

6.5.4. Users module

Feedback

- In AD member mode users and clients synchronized from Active Directory are now ignored in the license count (Bug 35647).
- Failures on report creation can not block UMC usage anymore (Bug 34333).
- Long base DNs in license files are now handled correctly (Bug 35580).
- A possible double registration is now prevented by a new ucr variable (Bug 35711).

6.6. Software deployment

Feedback

6.6.1. Software monitor

Feedback

- A traceback in the pkgdb listener has been fixed (Bug 35367).

6.7. Univention Library

Feedback

- The AD member setup does now ignore the spelling of the domain name (Bug 35757).
- The python module atjobs is now EINTR-safe, i.e., for interrupted function call signals (Bug 31319).

- This update fixes a problem with reading progress report lines from 'dpkg' while installing Apps, which lead to the installation getting stuck (Bug 35729).

6.8. System services

Feedback

6.8.1. Mail services

Feedback

- The listener module hosteddomains.py has been moved from univention-mail-server to univention-mail-postfix (Bug 35232).
- Several UCR variables have been added to univention-mail-postfix to allow better configuration of postfix's perfect forward secrecy. (for detailed description please see -> ucr search variable_name).
  - mail/postfix/smtpd/tls/dh1024/param/file
  - mail/postfix/smtpd/tls/dh512/param/file
  - mail/postfix/smtpd/tls/loglevel
  - mail/postfix/smtp/tls/loglevel
  - mail/postfix/cron/recreate/dh/parameter

  During installation of this update univention-mail-postfix creates a set of DH parameter files for EDH ciphers to use instead of the built-in parameters. Also, a cronjob /etc/cron.d/univention-mail-postfix has been added to weekly recreate the DH parameter files (creating/recreating these parameter files can take a while, depending on the quality of the systems random source) (Bug 35923).

6.8.2. Printing services

Feedback

- Assigning a Windows printer driver to a Samba print share renamed the share to the name of the printer driver which may be confusing and could trigger a Windows error message (code 0x0000007a). Test page printing would fail in this case. Now the UCS management tools create Samba printer shares with the option `force printername` which is provided by Samba as a workaround for this issue. The option get's set while creating new or modifying existing printer shares. The new default can be reverted by settings the UCR variable samba/force_printername to no or false. The following command can be run once on each UCS print server to set the option for all print shares hosted locally: `univention-directory-listener-ctrl resync cups-printers` (Bug 33505).

6.8.3. Nagios

Feedback

- This update corrects problems in the apache configuration due to a dead symlink during the package installation process. In specific setups this could have led to installation errors (Bug 35078).

6.8.4. SSL

Feedback

- The default hash function has been changed to sha256. This is configurable via the UCR variable ssl/default/hashfunction (Bug 35836).
- The default key size has been changed to 2048 bits. This is configurable via the UCR variable ssl/default/bits (Bug 30545).

6.8.5. Proxy services

Feedback

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

- The update for squid3 to fix CVE-2014-3609 erroneously removed SSL support. This update restores the SSL functionality (Bug 35980).

6.8.6. PAM / Local group cache

Feedback

- The UCR default for the security limit max open files has been fixed (now 32768) (Bug 35362).

6.8.7. Other services

Feedback

- This update disables the insecure protocols SSL 2.0 and SSL 3.0 for the Apache Webserver. It is possible to override this by setting the UCR variable apache2/ssl/v2 and/or apache2/ssl/v3 to "true" before or after the update (Bug 36173).
- This update fixes RADIUS access for clients in Samba AD domains (Bug 35516).

6.9. Virtualisation

Feedback

6.9.1. Xen

Feedback

- The code signing certificate for the GPLPV drivers expired and has been replaced with a new certificate valid until 10.10.2017. The new driver version is 0.11.0.373 (Bug 35849).

6.10. Services for Windows

Feedback

6.10.1. Samba

Feedback

- All winbind processes are stopped correctly during samba4 join in 96univention-samba4.inst (Bug 35600).
- The backup script univention-samba4-backup now ignores the tar file changed as we read its warning (Bug 35392).
- When installing broken printdrivers, samba returned a wrong error code (access denied). This has been fixed (Bug 32771).
- A bug has been fixed which could prevent a takeover of Windows 2012 servers with enabled recycle bin (Bug 35443).
- The main samba (not smbd) processes have been restricted to 1024 open files. Now they use the value configured in the UCR variable samba/max_open_files (Bug 34514).
- A smbd crash on filenames with non-ascii characters has been fixed (Bug 36162).

6.10.2. Univention AD Takeover

Feedback

- When running AD takeover out of AD member mode it's necessary to flush samba caches to steer clear of IDMAP issues (Bug 35564).
- If the spelling case of the domain name differs between AD and UCS the GPO check failed. This get's fixed now by renaming the domain specific directory in the sysvol share (Bug 35769).

6.10.3. Univention S4 Connector

Feedback

- A traceback due to an undefined variable in the password synchronization module has been fixed (Bug 33263).

- The SID synchronization from OpenLDAP to Samba 4 has been fixed. This is used in UCS@school environments (Bug 35626).
- A locking table has been added to the S4 connector which is used to avoid the synchronisation of incomplete objects (Bug 35391).
- A synchronization error for the telephone number has been fixed (Bug 31172).
- The inital group membership sync has been fixed if the group exists on both sides and the group members are different (Bug 33319).
- Objects which are deleted in Samba 4 are now recursively removed in OpenLDAP (Bug 27290).
- The sync_mode is now being checked in the post modify membership update functions (Bug 35251).
- The S4 connector doesn't no longer delete the OpenLDAP domain controller object if the deleted Samba 4 object was a Windows computer (Bug 35563).

6.10.4. Univention Active Directory Connector

- A couple of messages have been improved in the UMC wizard (Bug 35602).
- The determination of the Active Directory language has been fixed. This is needed for the group name mapping (Bug 35572).
- The password synchronization can now be disabled by setting the UCR variable 'connector/ad/mapping/user/password/disabled' to 'true' (Bug 35895).
- A connection traceback has been fixed in the AD member mode wizard (Bug 35701).

Bibliography

[ucs-manual] Univention GmbH. 2014. *Univention Corporate Server - Manual for users and administrators*. http://docs.univention.de/manual-3.2.html.