univention
be open.

UCS 3.2-6 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 3.2-6

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

<feedback@univention.de>

Table of Contents

Chapter 1. Univention Corporate Server (UCS) 3.2-6

The sixth point release for Univention Corporate Server (UCS) is now available in the form of Univention Corporate Server 3.2-6. 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 3.2-6 ISO images available for new installations. UCS 3.2-6 includes all the errata updates published for UCS 3.2-5. An overview of the most important changes:

- The release contains several security updates which have been released in the previous weeks and months as errata updates for UCS 3.2-5. Among others, it contains updated packages for the ***Linux kernel***, ***OpenSSL***, ***glibc***, ***sudo***.
- Various tools using the PAM stack now support the configuration of multiple LDAP servers. Such a configuration can be used to improve the reliability of authentication services.
- The login performance in large environments has been improved: Time consuming queries for quota settings have been separated from the login process.
- Provided that UCS receives a network configuration via `DHCP`, additional parameters like routing information are now also evaluated.

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 system's local console as user `root`, and the update should be initiated there. Alternatively, the update can be conducted using Univention Management Console.

Remote updating via SSH is not recommended as this may result in the update procedure being cancelled, e.g., if the network connection is interrupted. In consequence, this can affect the system severely. 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, e.g., using the tools `screen` and `at`. These tools are installed on all system roles by default.

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 user `root`.

Subsequently the UCS system needs to be restarted.

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

Feedback

Pre-up and post-up 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 3.2-5 3.2-6; 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 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 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 right 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.

Independent of the license 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 and 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 web browser.

5.4. Recommended browsers for the access to 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 and vice versa.
- 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 support forest domains.
- Samba 4 does not 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 3.2-5:

6.1. General

Feedback

All security updates issued for UCS 3.2-5 are included:

- ***cairo*** (CVE-2013-7439) (Bug 38251)
- ***eglibc*** (CVE-2012-3405 CVE-2012-3406 CVE-2012-3480 CVE-2012-4412 CVE-2012-4424 CVE-2013-0242 CVE-2013-1914 CVE-2013-4237 CVE-2013-4332 CVE-2013-4357 CVE-2013-4458 CVE-2013-4788 CVE-2013-7423 CVE-2013-7424 CVE-2014-4043) (Bug 37644)
- ***firefox-de*** (CVE-2015-0801 CVE-2015-0807 CVE-2015-0813 CVE-2015-0815 CVE-2015-0816 CVE-2015-0817 CVE-2015-0818 CVE-2015-0822 CVE-2015-0827 CVE-2015-0831 CVE-2015-0835 CVE-2015-0836) (Bug 37882 Bug 38180)
- ***firefox-en*** (CVE-2015-0801 CVE-2015-0807 CVE-2015-0813 CVE-2015-0815 CVE-2015-0816 CVE-2015-0817 CVE-2015-0818 CVE-2015-0822 CVE-2015-0827 CVE-2015-0831 CVE-2015-0835 CVE-2015-0836) (Bug 37882 Bug 38180)
- ***FreeType*** (CVE-2014-9656 CVE-2014-9657 CVE-2014-9658 CVE-2014-9660 CVE-2014-9661 CVE-2014-9663 CVE-2014-9664 CVE-2014-9666 CVE-2014-9667 CVE-2014-9669 CVE-2014-9670 CVE-2014-9671 CVE-2014-9672 CVE-2014-9673 CVE-2014-9675) (Bug 37756)
- ***krb5*** (CVE-2014-4341 CVE-2014-4342 CVE-2014-4343 CVE-2014-4344 CVE-2014-5352 CVE-2014-4345 CVE-2014-9421 CVE-2014-9422 CVE-2014-9423) (Bug 37680)
- ***libSDL1.2*** (CVE-2013-7439) (Bug 38251)
- ***libX11*** (CVE-2013-7439) (Bug 38251)
- ***libXext*** (CVE-2013-7439) (Bug 38251)
- ***libXfixes*** (CVE-2013-7439) (Bug 38251)
- ***libXi*** (CVE-2013-7439) (Bug 38251)
- ***libXrandr*** (CVE-2013-7439) (Bug 38250)
- ***libXrender*** (CVE-2013-7439) (Bug 38251)
- ***libXv*** (CVE-2013-7439) (Bug 38251)
- ***Linux*** (CVE-2013-7421 CVE-2014-3645 CVE-2014-3646 CVE-2014-3690 CVE-2014-8133 CVE-2014-8134 CVE-2014-9419 CVE-2014-9420 CVE-2014-9529 CVE-2014-9584 CVE-2014-9585 CVE-2014-9644 CVE-2014-9683 CVE-2015-1421 CVE-2015-1593) (Bug 37353)
- ***ntp*** (CVE-2014-9297 CVE-2014-9298) (Bug 37703)
- ***OpenJDK-6*** (CVE-2014-3566 CVE-2014-6585 CVE-2014-6587 CVE-2014-6591 CVE-2014-6593 CVE-2014-6601 CVE-2015-0383 CVE-2015-0395 CVE-2015-0407 CVE-2015-0408 CVE-2015-0410 CVE-2015-0412) (Bug 37576)
- ***OpenSSL*** (CVE-2015-0209 CVE-2015-0286 CVE-2015-0287 CVE-2015-0288 CVE-2015-0289 CVE-2015-0292) (Bug 37959)

- ***Open-VM-tools*** (CVE-2013-7439) (Bug 38251)
- ***PostgreSQL-8.4*** (CVE-2015-0241 CVE-2015-0243 CVE-2015-0244 CVE-2014-8161) (Bug 37703)
- ***sudo*** (CVE-2014-0106 CVE-2014-9680) (Bug 37853)
- ***TeXLive-bin*** (CVE-2013-7439) (Bug 38251)
- ***TightVNC*** (CVE-2013-7439) (Bug 38251)
- ***xen-4.1*** (CVE-2015-2044 CVE-2015-2045 CVE-2015-2151 CVE-2015-3456) (Bug 37956 Bug 38173)
- ***xserver-xorg-video-vmware*** (CVE-2013-7439) (Bug 38251)

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- The Linux kernel has been updated to 3.10.71. This provides many bugfixes (Bug 37353).

6.2.2. Quota

Feedback

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed in the script `univention-user-quota` (Bug 38078).
- An error message about an unbound variable has been removed from the script `univention-group-quota` (Bug 38079).
- The quota settings are now written to a cache directory by a listener module. The PAM script which sets the quota settings to the share uses this cache directory. This improves the login performance (Bug 36989).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- If a password has been changed via Samba 4, the account expiry setting was not always considered. This has been fixed (Bug 31429).
- The file `msgpo.schema` adjusted in UCS 3.2-5 erratum 276 would get replaced by a not-adjusted version during an update to UCS 4.0. This erratum avoids this by implementing a `dpkg` diversion for that file, which will get removed again in an erratum for UCS 4.0-2 (Bug 38488).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- The navigation arrow is now shown again when multiple tabs are opened (Bug 37618).

6.4.2. Online update module

Feedback

- A default time-out of 10 minutes was added to the updater, after which stalled HTTP connections are aborted (Bug 37901).

6.5. Software deployment

6.5.1. Software deployment command line tools

- The update scripts have been adjusted to UCS 3.2-6 (Bug 38516).

6.6. Univention Library

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed (Bug 38078).

6.7. System services

6.7.1. Mail services

- Additional arguments for `smtpd` processes may now be added via Univention Configuration Registry variables. The given arguments are automatically added to the configuration file `/etc/postfix/master.cf`. The following UCR variable prefixes are currently supported:
  - `mail/postfix/mastercf/options/smtp/...`
  - `mail/postfix/mastercf/options/smtps/...`

  (Bug 38062)
- The first changes to the `main.cf` framework have been done for defining a custom restriction rule set via Univention Configuration Registry variables for Postfix' `smtps` port (465). There is currently no change in Postfix behaviour (Bug 31738).

6.8. Services for Windows

6.8.1. Samba

- If the first configured LDAP server was not reachable, timeouts could occur during the share access on a member server. This has been fixed (Bug 13784).

6.8.2. Univention S4 Connector

- The password expiry attributes are now set in OpenLDAP if the password has been changed in Active Directory/Samba 4 (Bug 38494).

6.9. Other changes

- If the first configured LDAP server was not reachable, timeouts could occur during the login. This has been fixed in ***univention-home-mounter*** (Bug 38078).
- An error in a network script terminated the DHCP script responsible for updating the network configuration too early, which lead to RFC 3442 classless routes not being applied (Bug 37689).

Bibliography

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