UCS 3.2-7 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 3.2-7

Table of Contents

www.univention.de

Chapter 1. Univention Corporate Server (UCS) 3.2-7

The seventh point release for Univention Corporate Server (UCS) is now available in the form of Univention Corporate Server 3.2-7. The online repository provided by Univention can be used to update existing UCS systems or, alternatively, updates can be installed from an update DVD. UCS 3.2-7 includes all the errata updates published for UCS 3.2-6. 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 3.2-6. Among others, it contains updated packages for *OpenSSL*, *glibc*, *ntp*.

- The Linux kernel has been updated to the latest stable version of the 3.10 longterm kernel, *3.10.87*. It includes several security updates and bugfixes.

- The number of concurrent AMaViS processes can now easily configured via Univention Configuration Registry. In environments with a very high volume of mail the mail delivery may be delayed if not enough AMaViS processes are started.

- The DNS server *bind9* has been updated to *9.8.4-P1*. It includes various enhancements and bugfixes.

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

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 cryptographical-ly 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 3.2-7; 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 reposi-tory server this can be done by setting the Univention Configuration Registry variable `repository/mir-ror/verify` to `false`. For the update the Univention Configuration Registry variable `reposito-ry/online/verify` must be set to `false` on all systems.

www.univention.de

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

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.

www.univention.de

Chapter 6. Changelog

Listed are the changes since UCS 3.2-6:

6.1. General

All security updates issued for UCS 3.2-6 are included:

- *qemu-kvm* (CVE-2012-6075 CVE-2014-0150 CVE-2014-2894 CVE-2013-4344 CVE-2014-0142 CVE-2014-0143 CVE-2014-0144 CVE-2014-0145 CVE-2014-0146 CVE-2014-0147 CVE-2014-0223 CVE-2014-0222 CVE-2014-3640 CVE-2014-3689 CVE-2014-7815 CVE-2014-8106 CVE-2014-3615 CVE-2015-3456 CVE-2015-4037 CVE-2015-3209) (Bug 33279)

- *clamav* (CVE-2014-9050 CVE-2013-6497 CVE-2014-9328 CVE-2015-1461 CVE-2015-1462 CVE-2015-1463 CVE-2015-2170 CVE-2015-2221 CVE-2015-2222 CVE-2015-2668 CVE-2015-2305) (Bug 36965)

- *curl* (CVE-2014-3707 CVE-2014-8150 CVE-2015-3143 CVE-2015-3148) (Bug 36468)

- *ntp* (CVE-2015-1798 CVE-2015-1799) (Bug 38245)

- *bind9* (CVE-22014-8500 CVE-22015-1349 CVE-22015-4620 CVE-22015-5477) (Bug 37247)

- *linux* (CVE-2015-2150 CVE-2014-8159 CVE-2015-0239 CVE-2014-8160 CVE-2014-7822 CVE-2015-0239 CVE-2015-1805 CVE-2014-9710 CVE-2015-3332 CVE-2015-3636 CVE-2015-5364 CVE-2015-5366 CVE-2015-2830 CVE-2015-3331 CVE-2015-3339) (Bug 38008)

- *eglibc* (CVE-2015-1781) (Bug 38115)

- *firefox-de* (CVE-2015-0797 CVE-2015-2710 CVE-2015-2713 CVE-2015-2716 CVE-2015-2721 CVE-2015-2722 CVE-2015-2724 CVE-2015-2725 CVE-2015-2726 CVE-2015-2728 CVE-2015-2730 CVE-2015-2733 CVE-2015-2734 CVE-2015-2735 CVE-2015-2736 CVE-2015-2737 CVE-2015-2738 CVE-2015-2739 CVE-2015-2740 CVE-2015-2743 CVE-2015-4000 CVE-2015-4475 CVE-2015-4478 CVE-2015-4479 CVE-2015-4480 CVE-2015-4482 CVE-2015-4484 CVE-2015-4485 CVE-2015-4486 CVE-2015-4487 CVE-2015-4488 CVE-2015-4489 CVE-2015-4491 CVE-2015-4492 CVE-2015-4493) (Bug 38524)

- *firefox-en* (CVE-2015-0797 CVE-2015-2710 CVE-2015-2713 CVE-2015-2716 CVE-2015-2721 CVE-2015-2722 CVE-2015-2724 CVE-2015-2725 CVE-2015-2726 CVE-2015-2728 CVE-2015-2730 CVE-2015-2733 CVE-2015-2734 CVE-2015-2735 CVE-2015-2736 CVE-2015-2737 CVE-2015-2738 CVE-2015-2739 CVE-2015-2740 CVE-2015-2743 CVE-2015-4000 CVE-2015-4475 CVE-2015-4478 CVE-2015-4479 CVE-2015-4480 CVE-2015-4482 CVE-2015-4484 CVE-2015-4485 CVE-2015-4486 CVE-2015-4487 CVE-2015-4488 CVE-2015-4489 CVE-2015-4491 CVE-2015-4492 CVE-2015-4493) (Bug 38524)

- *icu* (CVE-2013-0900 CVE-2013-1569 CVE-2013-2383 CVE-2013-2384 CVE-2013-2419 CVE-2013-2924 CVE-2014-6585 CVE-2014-6591 CVE-2014-7923 CVE-2014-7926 CVE-2014-7940 CVE-2014-9654 CVE-2015-4760) (Bug 33284)

- *jasper* (CVE-2014-9029 CVE-2014-8137 CVE-2014-8138 CVE-2014-8157 CVE-2014-8158) (Bug 33281)

- *nspr* (CVE-2014-1545) (Bug 35097)

- *nss* (CVE-2011-3389 CVE-2013-1741 CVE-2013-5606 CVE-2014-1491 CVE-2014-1492 CVE-2014-1544 CVE-2014-1568 CVE-2014-1569) (Bug 33281)

- *openjdk-6* (CVE-2015-0460 CVE-2015-0469 CVE-2015-0477 CVE-2015-0478 CVE-2015-0480 CVE-2015-0488) (Bug 38303)

- *openssl* (CVE-2014-8176 CVE-2015-1789 CVE-2015-1790 CVE-2015-1791 CVE-2015-1792 CVE-2015-4000) (Bug 38692)

- *php5* (CVE-2014-0237 CVE-2014-0238 CVE-2014-2270 CVE-2014-8117 CVE-2014-9652 CVE-2014-9705 CVE-2015-0232 CVE-2015-2301 CVE-2015-2331 CVE-2015-2783 CVE-2015-2787 CVE-2015-3329 CVE-2015-3330 CVE-2015-4604 CVE-2015-4605) (Bug 37093)

- *wget* (CVE-2014-4877) (Bug 36368)

6.2. Basic system services

6.2.1. Linux kernel and firmware packages

- The Linux kernel has been updated to *3.10.87*. It provides many bugfixes and fixes several vulnerabilities (Bug 38008).

6.3. Univention Management Console

6.3.1. Univention Management Console web interface

- The PID file is no longer created world-writable (Bug 25162).

6.3.2. Univention Management Console server

- The mapping of syntax classes to UMC widgets is now extendable via the UCR variable group `directory/manager/web/widget/.*/"` (Bug 38743).

6.4. Software deployment

6.4.1. Software deployment command line tools

- The update scripts have been adjusted to UCS 3.2-7 (Bug 38972).

6.5. System services

6.5.1. Spam/virus detection and countermeasures

- To configure the max. number of concurrent AMaViS processes, a new UCR variable has been introduced: `mail/antivir/max_servers`. When unset, the current default 2 is used (Bug 38937).

6.5.2. Apache

- The configuration of the SSL/TLS support in Apache has been improved.

  - Apache no longer accepts various insecure ciphers and hash algorithms (e.g. RC4, MD5 and the outdated export ciphers) by default. Note that such algorithms would not have been negotiated if the TLS client supports current crypto algorithms. A different set of ciphers can be configured using the new UCR variable `apache2/ssl/ciphersuite`.

- If the new UCR variable `apache2/ssl/honorcipherorder` is set, the server choice of ciphers is used instead of the ciphers preferred by the TLS client.

Please refer to the UCR variable descriptions for additional details (Bug 38632).

6.5.3. DNS

- The DNS server *bind9* has been updated to *9.8.4-P1*. It provides many bugfixes and fixes several vulnerabilities (Bug 37247).

6.6. Services for Windows

6.6.1. Samba

- This update adds support for the default profile directory paths of Windows 8, 8.1 and 10. For new users they will now be created automatically on first logon (Bug 38644).

6.6.2. Univention S4 Connector

- A bug concerning renaming computer objects has been fixed (Bug 31083).

6.7. Other changes

- The time zone database was updated to include information about the scheduled leap second at the end of June 2015 (Bug 38719).

Bibliography

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