univention
be open.

UCS 3.3-1 Release Notes

Release notes for the installation and update of Univention Corporate Server (UCS) 3.3-1

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

<feedback@univention.de>

univention
be open.

Table of Contents

Chapter 1. Univention Corporate Server (UCS) 3.3-1

The first point release for Univention Corporate Server (UCS) 3.3 is now available in the form of Univention Corporate Server 3.3-1. 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 3.3-1 includes all the errata updates published for UCS 3.3-0. The maintenance cycle for the UCS 3 major version ends on 31 December 2016. Further information can be found in the Univention Forum.

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

PostgreSQL 9.1 is delivered with UCS 3.3. Security Updates for PostgreSQL 8.4 won't be provided with UCS 3.3. The migration from PostgreSQL 8.4 to PostgreSQL 9.1 should be done after the migration to UCS 3.3. See SDB 1292 for more details.

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.

Chapter 5. Further notes on selected packages

5.1. Collection of usage statistics

Feedback

Anonymous usage statistics on the use of Univention Management Console are collected when using the *UCS Core Edition* (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 *UCS Core Edition* license is used. The license status can be verified via the menu entry **License -> License information** of the user menu in the upper right corner of Univention Management Console. If **UCS Core 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. 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.

5.3. 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.

Chapter 6. Changelog

Listed are the changes since UCS 3.3-0:

6.1. General

- All security updates issued for UCS 3.3-0 are included:
  - ***graphicsmagick*** (CVE-2016-5118) (Bug 41442).
  - ***imagemagick*** (CVE-2016-5118) (Bug 41440).
  - ***libssh*** (CVE-2014-0017, CVE-2016-0739), (Bug 41498).
  - ***grub2*** (CVE-2015-8370) (Bug 41364).
  - ***mysql-5.5*** (CVE-2016-0505, CVE-2016-0546, CVE-2016-0596, CVE-2016-0597, CVE-2016-0598, CVE-2016-0600, CVE-2016-0606, CVE-2016-0608, CVE-2016-0609, CVE-2016-0616, CVE-2016-0640, CVE-2016-0641, CVE-2016-0642, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-2047, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-6662) (Bug 41851).
  - ***bind9*** (CVE-2015-5722, CVE-2015-8000, CVE-2015-8704, CVE-2016-1285, CVE-2016-1286, CVE-2016-2776) (Bug 41498).
  - ***linux*** (CVE-2015-7515, CVE-2016-0821, CVE-2016-1237, CVE-2016-1583, CVE-2016-2117, CVE-2016-2143, CVE-2016-2184, CVE-2016-2185, CVE-2016-2186, CVE-2016-2187, CVE-2016-3070, CVE-2016-3134, CVE-2016-3136, CVE-2016-3137, CVE-2016-3138, CVE-2016-3140, CVE-2016-3156, CVE-2016-3157, CVE-2016-3672, CVE-2016-3951, CVE-2016-3955, CVE-2016-3961, CVE-2016-4470, CVE-2016-4482, CVE-2016-4485, CVE-2016-4486, CVE-2016-4565, CVE-2016-4569, CVE-2016-4578, CVE-2016-4580, CVE-2016-4581, CVE-2016-4805, CVE-2016-4913, CVE-2016-4997, CVE-2016-4998, CVE-2016-5243, CVE-2016-5244, CVE-2014-9904, CVE-2016-5728, CVE-2016-5828, CVE-2016-5829, CVE-2016-6130, CVE-2016-6136, CVE-2016-6480, CVE-2016-6828, CVE-2016-5696, CVE-2015-8956, CVE-2016-5195, CVE-2016-7042, CVE-2016-7425) (Bug 41693,Bug 42099).
  - ***php5*** (CVE-2015-7803, CVE-2015-7804, CVE-2015-8865, CVE-2015-8866, CVE-2015-8878, CVE-2015-8879, CVE-2016-4070, CVE-2016-4071, CVE-2016-4072, CVE-2016-4073, CVE-2016-4343, CVE-2016-4537, CVE-2016-4539, CVE-2016-4541, CVE-2016-4544, CVE-2016-5093, CVE-2016-5095, CVE-2016-5096, CVE-2016-4473, CVE-2016-4538, CVE-2016-5114, CVE-2016-5399, CVE-2016-5768, CVE-2016-5769, CVE-2016-5770, CVE-2016-5771, CVE-2016-5772, CVE-2016-5773, CVE-2016-6288, CVE-2016-6289, CVE-2016-6290, CVE-2016-6291, CVE-2016-6292, CVE-2016-6294, CVE-2016-6295, CVE-2016-6296, CVE-2016-6297) (Bug 41479).
  - ***openssl*** (CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306) (Bug 42487).
  - ***python-imaging*** (CVE-2014-3589, CVE-2016-0775, CVE-2016-2533, CVE-2016-9189, CVE-2016-9190) (Bug 42900).

- ***samba*** (CVE-2016-2119, CVE-2016-2123, CVE-2016-2125, CVE-2016-2126) (Bug 43145).

6.2. Basic system services

Feedback

6.2.1. Linux kernel and firmware packages

Feedback

- The Linux kernel has been updated to 3.16.38 (Bug 41693,Bug 42099).
- The mount-point option *no_mbcache* has been added for ext4 file systems to make it possible to disable the Filesystem Meta Information Block Cache (*mbcache*). The *mbcache* is used to manage shared Extended Attributes (EAs), which are also used to store Access Control Lists (ACLs) for files and directories. For some work-loads which use EAs with many different values the cache has performance issues and can dead-lock the system in certain cases. Samba is one example which uses EAs to store the DOS attributes and NT-ACLs. The *cache* can now be disabled by adding the option *no_mbcache* in `/etc/fstab` and rebooting the system (Bug 42984).

6.2.2. Important package upgrades

Feedback

- The updater scripts have been adapted to UCS 3.3-1 (Bug 43166).

6.2.3. Boot Loader

Feedback

- On UCS systems booting via BIOS, GRUB would not be correctly updated, if debconf *grub-pc/install_devices* is empty. Additionally an error would happen if *grub-pc/install_devices* contains a wrong device. If it contains a wrong device the GRUB installation happens but fails, leading to an inconsistent installation between `/boot/grub` and the GRUB directly on the disk. This makes the system unbootable. This update checks all devices in *grub-pc/install_devices*, removing invalid devices. A guess is made for the correct boot device which will be added to *grub-pc/install_devices* if *grub-pc/install_devices* is currently empty or there were invalid devices. If any changes were made, grub-install is run on all devices in *grub-pc/install_devices*. See also SDB 1356 (Bug 41497).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

6.3.1.1. Listener/Notifier domain replication

Feedback

- A bug in handling the Notifier ID has been fixed: If the Listener was restarted multiple times, the last processed transaction ID could be lost. This led to all transactions being skipped which happened in between (Bug 41657).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- UMC is now also usable in Chrome 51 (Bug 41395).

6.4.2. Univention Management Console server

Feedback

- Some ldap search requests have been optimized in the handler modules (Bug 41518).
- Error messages regarding attribute locking have been improved (Bug 42385).

- Wildcard and automatic substring searches are now configurable via Univention Configuration Registry (Bug 42387).

6.4.3. Computers module

Feedback

- The attribute *sambaPwdLastSet* is now set for computer objects while changing the password (Bug 41516).

6.5. System services

Feedback

6.5.1. Mail services

Feedback

- *SSLv2* has been disabled by default in Cyrus IMAP. The new Univention Configuration Registry variable `mail/cyrus/ssl/cipher_list` allows to change the supported cypher list. It will however ignore *SSLv2*, as it has been disabled in the program code (Bug 41378).

6.6. Services for Windows

Feedback

6.6.1. Univention Active Directory Connector

Feedback

- The synchronization of the password hashes was implemented by using a service which was installed on the Microsoft Active Directory server. The Univention AD Connector now uses different interfaces of the Active Directory for reading and writing the password hashes. That means, the UCS AD Connector service which is installed on the Microsoft Active Directory server can be stopped after installing this update (Bug 41632).

6.7. Other changes

Feedback

- The following packages have been added to the maintained section of the software repository (Bug 42666): ***php5-imagick***, ***php5-geoip***, ***php5-memcache***, ***libssh2-php***
- The package ***device-tree-compiler*** has been moved to maintained due to QEMU being rebuilt due to the update to Xen 4.1 (Bug 41492).
- The package ***qemu*** has been rebuilt due to the update to Xen 4.1 (Bug 41492).
- The packages ***libdatetime-timezone-perl*** and ***tzdata*** have been updated to include new timezone data. The most notable change is a new leap second 2016-12-31 23:59:60 UTC as per IERS Bulletin C 52 (Bug 42878).