univention
be open.

UCS 3.3-1 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 3.3-1

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

<feedback@univention.de>

Inhaltsverzeichnis

1. Univention Corporate Server (UCS) 3.3-1 4
2. Empfohlene Update-Reihenfolge für Umgebungen mit mehr als einem UCS-Server 5
3. Vorbereitung des Updates 6
4. Nachbereitung des Updates 7
5. Hinweise zum Einsatz einzelner Pakete 8
    5.1. Erfassung von Nutzungsstatistiken 8
    5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit 8
    5.3. Empfohlene Browser für den Zugriff auf Univention Management Console 8
6. Changelog 9
    6.1. General 9
    6.2. Basic system services 10
        6.2.1. Linux kernel and firmware packages 10
        6.2.2. Important package upgrades 10
        6.2.3. Boot Loader 10
    6.3. Domain services 10
        6.3.1. OpenLDAP 10
            6.3.1.1. Listener/Notifier domain replication 10
    6.4. Univention Management Console 10
        6.4.1. Univention Management Console web interface 10
        6.4.2. Univention Management Console server 10
        6.4.3. Computers module 11
    6.5. System services 11
        6.5.1. Mail services 11
    6.6. Services for Windows 11
        6.6.1. Univention Active Directory Connector 11
    6.7. Other changes 11

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

Mit Univention Corporate Server 3.3-1 steht das erste Point-Release für Univention Corporate Server (UCS) 3.3 zur Verfügung. Vorhandene UCS-Systeme können über das von Univention bereitgestellte Online-Repository aktualisiert werden. Alternativ können Updates über eine Update-DVD eingespielt werden. UCS 3.3-1 beinhaltet alle für UCS 3.3-0 veröffentlichten Errata-Updates. Der Maintenance-Zyklus für UCS 3 endet am 31. Dezember 2016. Weitere Informationen sind im Univention Forum zu finden.

Kapitel 2. Empfohlene Update-Reihenfolge für Umgebungen mit mehr als einem UCS-Server

In Umgebungen mit mehr als einem UCS-System muss die Update-Reihenfolge der UCS-Systeme beachtet werden:

Auf dem Domänencontroller Master wird die maßgebliche (authoritative) Version des LDAP-Verzeichnisdienstes vorgehalten, die an alle übrigen LDAP-Server der UCS-Domäne repliziert wird. Da bei Release-Updates Veränderungen an den LDAP-Schemata auftreten können, muss der Domänencontroller Master bei einem Release-Update immer als erstes System aktualisiert werden.

Kapitel 3. Vorbereitung des Updates

Es sollte geprüft werden, ob ausreichend Festplattenplatz verfügbar ist. Eine Standard-Installation benötigt min. 6 GB Speicherplatz. Das Update benötigt je nach Umfang der vorhanden Installation mindestens 1 GB weiteren Speicherplatz zum Herunterladen und Installieren der Pakete.

Für das Update sollte eine Anmeldung auf der lokalen Konsole des Systems mit dem Benutzer `root` durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über Univention Management Console durchgeführt werden.

Eine Remote-Aktualisierung über SSH wird nicht empfohlen, da dies beispielsweise bei Unterbrechung der Netzverbindung zum Abbruch des Update-Vorgangs und zu einer Beeinträchtigung des Systems führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können beispielsweise die Tools `screen` oder `at` eingesetzt werden, die auf allen Systemrollen installiert sind.

Kapitel 4. Nachbereitung des Updates

Mit UCS 3.3 werden PostgreSQL 9.1 Pakete ausgeliefert. Für PostgreSQL 8.4 wird es UCS 3.3 keine Security Updates geben. Nach dem Update auf UCS 3.3 sollte die Migration von PostgreSQL 8.4 auf PostgreSQL 9.1 erfolgen. In SDB 1292 ist das Vorgehen beschrieben.

Nach dem Update müssen die neuen oder aktualisierten Join-Skripte ausgeführt werden. Dies kann auf zwei Wegen erfolgen: Entweder über das UMC-Modul **Domänenbeitritt** oder durch Aufruf des Befehls `univention-run-join-scripts` als Benutzer `root`.

Anschließend muss das UCS-System neu gestartet werden.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken

Feedback

Bei Verwendung der UCS Core Edition (die in der Regel für Evaluationen von UCS herangezogen wird) werden anonyme Nutzungsstatistiken zur Verwendung von Univention Management Console erzeugt. Die aufgerufenen Module werden dabei von einer Instanz des Web-Traffic-Analyse-Tools Piwik protokolliert. Dies ermöglicht es Univention die Entwicklung von Univention Management Console besser auf das Kundeninteresse zuzuschneiden und Usability-Verbesserungen vorzunehmen.

Diese Protokollierung erfolgt nur bei Verwendung der UCS Core Edition. Der Lizenzstatus kann überprüft werden durch den Eintrag **Lizenz -> Lizenzinformation** des Benutzermenüs in der rechten, oberen Ecke von Univention Management Console. Steht hier unter **Lizenztyp** der Eintrag **UCS Core Edition** wird eine solche Edition verwendet. Bei Einsatz einer regulären UCS-Lizenz erfolgt keine Teilnahme an der Nutzungsstatistik.

Die Protokollierung kann unabhängig von der verwendeten Lizenz durch Setzen der Univention Configuration Registry-Variable `umc/web/piwik` auf `false` deaktiviert werden.

5.2. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit

Feedback

WebKit, Konqueror und QtWebKit werden in UCS im maintained-Zweig des Repositorys mitgeliefert, aber nicht durch Sicherheits-Updates unterstützt. WebKit wird vor allem für die Darstellung von HTML-Hilfeseiten u.ä. verwendet. Als Web-Browser sollte Firefox eingesetzt werden.

5.3. Empfohlene Browser für den Zugriff auf Univention Management Console

Feedback

Univention Management Console verwendet für die Darstellung der Web-Oberfläche zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden empfohlen:

- Chrome ab Version 14
- Firefox ab Version 10
- Internet Explorer ab Version 9
- Safari (auf dem iPad 2)

Auf älteren Browsern können Darstellungs- oder Performanceprobleme auftreten.

Kapitel 6. Changelog

Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit 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).