

UCS 4.0-1 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 4.0-1**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2015 Univention GmbH

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

<feedback@univention.de>

Jede aufgeführte Marke und jedes Warenzeichen steht im Eigentum ihrer jeweiligen eingetragenen Rechtsinhaber. Linux ist ein eingetragenes Warenzeichen von Linus Torvalds.

The mentioned brand names and registered trademarks are owned by the respective legal owners in each case. Linux is a registered trademark of Linus Torvalds.

Inhaltsverzeichnis

1. Release-Highlights	5
2. Hinweise zum Update	6
2.1. Empfohlene Update-Reihenfolge	6
2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante	6
3. Vorbereitung des Updates	7
4. Nachbereitung des Updates	8
5. Hinweise zum Einsatz einzelner Pakete	9
5.1. Netzwerkinstallation von UCS	9
5.2. Erfassung von Nutzungsstatistiken	9
5.3. Umfang des Sicherheits-Supports von WebKit, Konqueror und QtWebKit	9
5.4. Empfohlene Browser für den Zugriff auf Univention Management Console	9
6. Changelog	10
6.1. General	10
6.2. Basic system services	11
6.2.1. Linux kernel and firmware packages	11
6.2.2. Other system services	11
6.3. Domain services	12
6.3.1. LDAP schema changes	12
6.3.2. Listener/Notifier domain replication	12
6.3.3. DNS server	12
6.4. Univention Management Console	12
6.4.1. Univention Management Console web interface	12
6.4.2. Univention Management Console server	13
6.4.3. Univention App Center	14
6.4.4. Basic settings / Appliance mode	14
6.4.5. Users module	15
6.4.6. Univention Directory Reports	15
6.4.7. Computers module	15
6.4.8. DNS module	15
6.4.9. License module	16
6.4.10. System diagnostic module	16
6.4.11. Online update module	16
6.4.12. Policies	16
6.4.13. Printers module	16
6.4.14. Other modules	16
6.4.15. Univention Directory Manager command line interface and related tools	17
6.5. Software deployment	17
6.5.1. Software monitor	17
6.5.2. Software deployment command line tools	17
6.6. Univention base libraries	17
6.7. System services	17
6.7.1. Spam/virus detection and countermeasures	17
6.7.2. Printing services	18
6.7.3. SSL	18
6.7.4. Univention System Info	18
6.7.5. Apache	18
6.7.6. Other services	18
6.8. Virtualization	18
6.8.1. Univention Virtual Machine Manager (UVMM)	18
6.9. Services for Windows	19
6.9.1. Samba	19
6.9.2. Univention AD Takeover	19

6.9.3. Univention S4 Connector	19
6.9.4. Univention Active Directory Connection	19
6.10. Other changes	20

Kapitel 1. Release-Highlights


Mit Univention Corporate Server 4.0-1 steht das erste Point-Release für Univention Corporate Server (UCS) 4.0 zur Verfügung. Es umfasst diverse Detailverbesserungen und Fehlerkorrekturen. Die wichtigsten Änderungen im Überblick:

- Das Debian Wheezy 7.8 Point-Update wurde integriert.
- Die Lizenz der *Free for personal use edition*-Edition wurde auf 50 Benutzer und 50 Clients erweitert.
- Verbesserungen im Appliance-Modus ermöglichen eine einfachere Inbetriebnahme von UCS-Systemen
- Der Beitritt zu einer Active Directory-Domäne wurde vereinfacht.
- Zahlreiche Fehlerkorrekturen und Verbesserungen in Samba, u.a. in der Druckeranbindung und bei der Verwendung von Microsoft SharePoint
- Zahlreiche Verbesserungen in Design und Usability der Univention Management Console

Kapitel 2. Hinweise zum Update

Während der Aktualisierung kann es zu Ausfällen von Diensten innerhalb der Domäne kommen. Aus diesem Grund sollte das Update innerhalb eines Wartungsfensters erfolgen. Grundsätzlich wird empfohlen das Update zunächst in einer Testumgebung einzuspielen und zu testen. Die Testumgebung sollte dabei identisch zur Produktivumgebung sein. Je nach Systemgeschwindigkeit, Netzwerkanbindung und installierter Software kann das Update zwischen 20 Minuten und mehreren Stunden dauern.


2.1. Empfohlene Update-Reihenfolge

Feedback 

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.

2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante

Feedback 

UCS-Installations-DVDs werden ab UCS 4 nur noch für 64-Bit-Architekturen bereitgestellt. Vorhandene 32-Bit UCS 3 Systeme können weiterhin über das Online Repository oder über Update DVDs auf UCS 4 aktualisiert werden. Die 32-Bit-Architektur wird für die gesamte UCS 4 Maintenance noch unterstützt.

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 ungefähr 2 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


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`.

Die Konfiguration des UCS-Nameservers BIND ist anfällig für Open-Resolver-Angriffe, die für Distributed Denial of Service (DDoS)-Angriffe auf andere Systeme im Internet verwendet werden können. Die Standard-Konfiguration wird daher verändert, so dass rekursive Anfragen nur von IP-Adressen privater Adressbereiche, link-lokaler Adressen, localhost und lokalen Netzen durchgeführt werden können. Wenn die Nameserver auch von anderen Systemen angefragt werden können sollen, müssen diese über die Univention Configuration Registry-Variable `dns/allow/query/cache` freigegeben werden. Diese Änderung wird nur bei Neuinstallationen durchgeführt. Weitere Hinweise zur Umstellung bestehender Systemen finden sich unter SDB 1298.

Anschließend muss das UCS-System neu gestartet werden.


Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Netzwerkinstallation von UCS

Feedback 

Die Profil-basierte Netzwerkinstallation von UCS steht mit UCS 4.0-1 noch nicht zur Verfügung. Die Unterstützung wird zu einem späteren Zeitpunkt nachgeliefert. Der Status kann in unserem Issue-Tracker nachvollzogen werden: Bug 35537.

5.2. Erfassung von Nutzungsstatistiken


Feedback 

Bei Verwendung der *Free for personal use*-Version von UCS (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 *Free-for-Personal-Use-Lizenz*. Der Lizenzstatus kann überprüft werden durch den Eintrag **Lizenz** -> **Lizenzinformation** des Benutzermenüs in der rechten, oberen Ecke von Univention Management Console. Steht hier unter **LDAP-Basis Free for personal use edition** wird eine solche Version 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.

5.3. 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.

5.4. 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 33
- Firefox ab Version 24
- Internet Explorer ab Version 9
- Safari und Safari Mobile ab Version 7

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 Änderung seit UCS 4.0-0:


6.1. General

Feedback 


- All security updates issued for UCS 4.0-0 are included:
 - **bind9** (CVE-2014-8500) (Bug 37248)
 - **bsd-mailx** (CVE-2014-7844) (Bug 37370)
 - **eglibc** (CVE-2015-0235, CVE-2012-6656, CVE-2014-6040, CVE-2014-7817) (Bug 37047)
 - **firefox-de, firefox-en** (CVE-2014-1587, CVE-2014-1589, CVE-2014-1590, CVE-2014-1592, CVE-2014-1593, CVE-2014-1594, CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296) (Bug 37141, Bug 37536)
 - **libevent** (CVE-2014-6272) (Bug 37452)
 - **libksba** (CVE-2014-9087) (Bug 37035)
 - **libtasn1-3** (CVE-2014-3467, CVE-2014-3468, CVE-2014-3469) (Bug 37054)
 - **linux** (CVE-2014-3610, CVE-2014-3611, CVE-2014-3646, CVE-2014-3647, CVE-2014-3673, CVE-2014-3687, CVE-2014-3688, CVE-2014-3690, CVE-2014-7825, CVE-2014-7826, CVE-2014-7841, CVE-2014-7842, CVE-2014-7970, CVE-2014-7975, CVE-2014-8086, CVE-2014-8884, CVE-2014-9090, CVE-2014-9322, (Bug 36969)
 - **lua50** (CVE-2014-5461) (Bug 36332)
 - **ntp** (CVE-2014-9293, CVE-2014-9294, CVE-2014-9295, CVE-2014-9296, CVE-2014-9297, CVE-2014-9298) (Bug 37408, Bug 37693)
 - **openjdk-7** (CVE-2014-6457, CVE-2014-6502, CVE-2014-6504, CVE-2014-6506, CVE-2014-6511, CVE-2014-6512, CVE-2014-6517, CVE-2014-6519, CVE-2014-6531, CVE-2014-6558, CVE-2014-6601, CVE-2015-0395, CVE-2015-0412, CVE-2015-0408, CVE-2015-0383, CVE-2015-0407, CVE-2015-0410, CVE-2014-6587, CVE-2014-3566, CVE-2014-6593, CVE-2014-6585, CVE-2014-6591) (Bug 37577, Bug 36985)
 - **openvpn**: CVE-2014-8104 (Bug 37139)
 - **openssl** (CVE-2014-3570, CVE-2014-3571, CVE-2014-3572, CVE-2014-8275, CVE-2015-0204, CVE-2015-0205, CVE-2015-0206) (Bug 37494)
 - **qemu-kvm** (CVE-2014-8106) (Bug 37212)
 - **samba** (CVE-2014-8143) (Bug 37496)
 - **unzip** (CVE-2014-8139, CVE-2014-8140, CVE-2014-8141) (Bug 37412)
 - **xorg-server** (CVE-2014-8091, CVE-2014-8092, CVE-2014-8093, CVE-2014-8094, CVE-2014-8095, CVE-2014-8096, CVE-2014-8097, CVE-2014-8098, CVE-2014-8099, CVE-2014-8100, CVE-2014-8101, CVE-2014-8102) (Bug 37274)

- The Debian Wheezy update 7.8 has been integrated. It fixes several security issues in addition to the errata security issues already issued:
 - *curl* (CVE-2014-3707, CVE-2014-8150) (Bug 36967)
 - *apache2* (CVE-2013-5704) (Bug 36984)
 - *tcpdump* (CVE-2014-8769, CVE-2014-8767, CVE-2014-9140) (Bug 37042)
 - *wpa* (CVE-2014-3686) (Bug 37051)
 - *wget* (CVE-2014-4877) (Bug 37052)
 - *ppp* (CVE-2014-3158) (Bug 37066)
 - *flac* (CVE-2014-8962, CVE-2014-9028) (Bug 37096)
 - *jasper* (CVE-2014-8137, CVE-2014-8138, CVE-2014-8157, CVE-2014-8158, CVE-2014-9029) (Bug 37210)
 - *heirloom-mailx* (CVE-2014-7844, CVE-2004-2771) (Bug 37373)
 - *wireshark* (CVE-2014-8710, CVE-2014-8711, CVE-2014-8712, CVE-2014-8713, CVE-2014-8714, CVE-2015-0562, CVE-2015-0564) (Bug 36995)
 - *subversion* (CVE-2014-0032, CVE-2014-3580) (Bug 37043)
 - *dbus* (CVE-2014-7824) (Bug 37048)
 - *libcrypt11* (CVE-2014-5270) (Bug 37057)
 - *mutt* (CVE-2014-9116) (Bug 37074)
 - *libyaml-libyaml-perl* (CVE-2014-9130) (Bug 37113)
 - *pyyaml* (CVE-2014-9130) (Bug 37115)
 - *libyaml* (CVE-2014-9130) (Bug 37117)
 - *graphviz* (CVE-2014-9157) (Bug 37293)
 - *mime-support* (CVE-2014-7209) (Bug 37429)
 - *file* (CVE-2014-3710, CVE-2014-8116, CVE-2014-8117, CVE-2014-9620) (Bug 37053)

6.2. Basic system services


Feedback 

6.2.1. Linux kernel and firmware packages

Feedback 


- The Linux kernel has been updated to 3.16.7-ckt2. It provides many bugfixes and fixes several vulnerabilities (Bug 36969).

6.2.2. Other system services


Feedback 

- The file system check now ignores clock skew problems, which previously required manual user interaction (Bug 36233).

6.3. Domain services


Feedback 

6.3.1. LDAP schema changes

Feedback 


- The object class `msGPOContainer` has been extended to support the new attribute `msNTSecurityDescriptor` (Bug 36979).
- The `univentionUserTemplate` object class has been adapted to include all attributes from the `person`, `organizationalPerson` and `inetOrgPerson` standard LDAP schemas (Bug 35775).

6.3.2. Listener/Notifier domain replication

Feedback 


- Fix the shutdown of Univention Directory Listener if a `failed.ldif` file exists (Bug 37291).

6.3.3. DNS server


Feedback 

- The configuration of the UCS DNS name server BIND9 was prone to open resolver attacks, which are used to launch Distributed Denial of Service (DDoS) attacks against other hosts of the internet. To prevent such abuse the default configuration will be changed to allow 'recursive queries' only from IP addresses of the private address ranges, link-local address ranges, localhost and local networks. If the name servers need to be queried from any other hosts outside those network, they must be configured using the Univention Configuration Registry variable `dns/allow/query/cache`. This change gets only applied for newly installed domain controllers. See SDB 1298 for additional details (Bug 37553).

6.4. Univention Management Console

Feedback 


6.4.1. Univention Management Console web interface

Feedback 

- The UMC requires JavaScript. If it is disabled in the web browser, a warning message is displayed. The styling of the notification has been improved (Bug 36338). Also, display a warning if an Internet Explorer version earlier than version 9 is used (it mis-renders SVG graphics) (Bug 36914)
- Added an arrow to the UMC grids that indicates which column is used for sorting (Bug 36357).
- Several buttons are now properly aligned to corresponding input fields (Bug 36291).
- The **Favorites** category button now fades in and out, depending on whether favorite modules are chosen or not (Bug 36787).
- A exception was logged in the JavaScript console if the grid was resized and if notifications were hidden. This has been removed (Bug 36645).
- Fixed a bug which prevented that UMC components could write into their logfiles (Bug 37317).
- The icon on the policy reference button is now shown (Bug 36291).
- The `LocationMatch` directive of Apache is now only configured for the UMC (Bug 37518).
- Don't let Firefox ask for resending POST form data when logging out of UMC (Bug 36445).
- Fix an endless login animation if the login fails due to a stopped UMC server (Bug 36636).
- Fix the error message which is shown if no network connection is possible on client side (Bug 36680).
- Fix the visibility of error messages when a login dialogue is opened (Bug 36400).

- The notification while changing objects which are part of an Active Directory domain has been placed in a more visible area (Bug 36732).
- The error message if the connection to the LDAP server fails has been extended (Bug 35719).
- The `get_exception_method()` has been removed. Error information are now provided by the UDM base exception itself (Bug 35273, Bug 30088). Exceptions are not re-raised anymore as this hides important error information in traceback feedback reports (Bug 32979).
- It is now prevented that a search with a given attribute name can raise a bad search filter exception (Bug 28383).
- An error message is now shown when trying to operate on non-existing objects (Bug 34246).
- Searching for an invalid object type will not raise an exception anymore. Opening a non-existent object (e.g. object was moved / deleted) now shows an error message instead of raising an exception (Bug 35350).
- Error handling has been improved in case a UDM module could not be identified (Bug 34680).
- Inform about automatically set default values when opening a object (Bug 36700).
- Error handling of UDM modules has been improved by adding default methods which contain information about the current edited object type (Bug 34985).
- Unnecessary scrollbars have been removed from the UCS installer software selection (Bug 37730).


6.4.2. Univention Management Console server

Feedback 

- Fix an error regarding the error handling of closed UMC module process sockets (Bug 37036).
- The JavaScript method `umc.tools.umcpProgressSubCommand` did not send the UMCP flavour along with a request and could therefore fail due to insufficient permissions (Bug 36875).
- Fix error if the UMC server and the UMC module try to close the module process at the same time (Bug 35231).
- Fix a server crash caused by corrupted translation files (Bug 36658).
- The UMCP command `udm/layout` failed if a DN was given which could not be identified as a UDM object (Bug 29231).
- Allows UMC modules to set the response status when the module initialization fails. This is required to show the login dialogue after a password change (Bug 34353).
- The query of the LDAP DN of the user logging into the UMC has been fixed. Previously users without a POSIX account were not found (Bug 37178).
- Fixed the handling of crashed UMC module processes (Bug 37367).
- Add the UMCP flavour to error information when a traceback occurs (Bug 37169).
- Connections to the LDAP server weren't closed after the session timeout. This caused a UMC server crash due to max open file limits (Bug 37453).
- Mask passwords when logging changed properties at debug level 4 (Bug 36591).
- Enhance the look of various error messages (Bug 36291).


- Fixed error handling when renaming the currently logged in user (Bug 35280).
- Additional exceptions during the creation of UDM objects are now handled (Bug 20044).
- Ask for closing the detail page if changes to the object have been done (Bug 30088).

6.4.3. Univention App Center

Feedback 

- If the details of a package are opened which is not longer available (e.g. the repository has been removed), an error occurred. This has been fixed (Bug 37403).
- The translation file for installed apps modules may have been corrupted during a release update. This has been fixed (Bug 37571).
- Extended one command to allow searching for multiple components at once (needed for updater module) (Bug 37364).
- The checkbox **Use unmaintained repositories** is now placed above the **Apply changes** button (Bug 36457).
- After trying to install a software component in the repository settings module a white page occurred which prevented installation (Bug 36868).


6.4.4. Basic settings / Appliance mode

Feedback 

- The Firefox address bar is now always hidden (Bug 35583).
- If the DNS lookup of the master domain controller fails during a UCS domain join, a warning message is now displayed (Bug 34238).
- When joining into an Active Directory domain, log messages from the Active Directory join were not logged (Bug 37049).
- The default keyboard layout for German has been corrected (Bug 36936).
- The branding of the appliance wizard can now be customised via the Univention Configuration Registry variables `umc/web/appliance/name` and `umc/web/appliance/logo` (Bug 37488).
- The wizard failed if the system had more than four physical network devices. This has been fixed (Bug 37001, Bug 36884).
- The wizard now shows information about how to reach the system and UMC after the configuration process (Bug 36938).
- In text mode or after aborting the configuration, a message is shown to the user how the UMC can be accessed after reboot (Bug 36968).
- The DNS error message when selecting a system role is now prompted as an alert dialogue (Bug 36940).
- The DNS domain check when selecting a system role has been adjusted to correctly determine an UCS domain (Bug 36440).
- If the UCS system has not been configured yet, a corresponding message is shown during login at console/via SSH asking the user to use the UMC to complete configuration. (Bug 36971).
- Some text field descriptions have been adapted (Bug 36723).


- Only system setup scripts belonging to the current module are now executed when changing settings via the modules for changing certificate, language and network settings (Bug 36939).
- A DHCP lease may be now requested in the UCS setup wizard via unmarking and remarking the DHCP checkbox on the network page (Bug 36665).
- The syntax check for the LDAP base has been adjusted to be more specific (Bug 36334).
- The search for system locales has been adjusted such that wildcards are implicitly used (Bug 29922).
- The configuration of keyboard model and keyboard variant has been corrected (Bug 37105).
- It is now possible to prevent domain joining. The profile variable *start/join* was previously not evaluated (Bug 36701).
- Reset join credentials if they are incorrect (Bug 36876).
- The DHCP query in the **Network settings** dialogue has been fixed (Bug 35851).
- The package removal in appliance mode has been corrected (Bug 36874).
- Fix the configuration of primary devices and *bond-miimon* in bonding network devices (Bug 36340, Bug 36342).
- The gateway input field is not required anymore. This allows to set up systems without connection to the internet (Bug 36586).
- Fix base system deployment if no domainname is specified (Bug 36873).

6.4.5. Users module

Feedback 


- Users without the POSIX option are now able to change their password in the Univention Management Console (Bug 31828).
- Fixed setting of the user expiry date if a user account is disabled (Bug 36330).
- Fixed the removal of the account expiry date of a user (Bug 25279).
- A PNG file can now be specified as user photo. It will be internally converted into JPEG (Bug 36273).
- The user properties *CtxBrokenSession*, *CtxReconnectSession* and *CtxRASDialin* now have default values. They prevented changes via UMC when not having sufficient LDAP permission to change these attributes (Bug 29884, Bug 37592).

6.4.6. Univention Directory Reports

Feedback 


- Fixed a problem which prevented the creation of reports in some circumstances (Bug 36234).

6.4.7. Computers module

Feedback 


- Automatic IP assignment for a network will now show an error message if there is no more IP available to use instead of a traceback (Bug 33527).

6.4.8. DNS module

Feedback 


- Setting the attribute DNS time to an empty value does not trigger an error anymore (Bug 33256).

6.4.9. License module

Feedback 


- Internal "hidden" users are now ignored in the license check (Bug 37654).
- The *Free for personal use edition* license has been extended to 50 users and 50 clients. Existing license keys need to be updated, please see SDB 1295 for details (Bug 37448).

6.4.10. System diagnostic module

Feedback 


- Added a plugin which checks the package status (Bug 35861).
- Fixed the timeout value for pinging the gateway. It blocked the diagnosis if the gateway was not reachable (Bug 37032).

6.4.11. Online update module

Feedback 


- List all App Center apps (or other components) blocking a release update (Bug 37364). The message shown has been improved (Bug 37363).
- The dialogue showing the list of packages to be updated/installed is now limited in its maximum height (Bug 36291).
- Adapted the link to the new errata overview page (Bug 33539).
- Open the **Software update** module upon UMC startup during release updates and show a information dialogue about the current update process (Bug 37357).
- The hints and warning messages before or during the execution of a UCS update have been clarified (Bug 37360).
- In some situations the software upgrade didn't show any update progress. This has been fixed (Bug 37564).

6.4.12. Policies

Feedback 


- The **Release** policy has been renamed into **Automatic updates** and its property descriptions have been improved (Bug 33190).
- It is now possible to change the password of a user after setting an empty password length in the referenced password policy (Bug 8429).

6.4.13. Printers module

Feedback 


- The Samba share option `force_printername` was activated implicitly during modifications of existing print shares. Now it only gets activated on new print shares and if the UCR variable `samba/force_printername` is not set to `no` or `false` (Bug 37123).

6.4.14. Other modules

Feedback 


- Close the progress bar for server shutdown if no permission exists to shutdown the server (Bug 36992).
- After changing the own password a login dialogue is shown if a LDAP connection needs to be re-established (Bug 34353).
- Remove references to the network object when deleting it (Bug 35099).

6.4.15. Univention Directory Manager command line interface and related tools

Feedback 


- Added support for the following operators in a UDM filter: <, <=, >=, >. (Bug 36970).

6.5. Software deployment

Feedback 


- When executing a maintenance or release policy, a requested reboot is now only performed once all updates have been performed (Bug 37231).
- Detect broken HTTP proxies like DansGuardian, which block downloading the Packages files and updater scripts while still signalling success (Bug 37345).
- Old Samba TDB files are now handled in the pre-update script (Bug 37534).
- The update scripts have been adjusted to UCS 4.0-1 (Bug 37661).
- The Scalix schema check have been removed from the pre-update script (Bug 37145).

6.5.1. Software monitor

Feedback 


- It is now possible again to search for UCS systems (Bug 35700).
- Translations of some error messages have been fixed (Bug 35700).
- The connection to the PostgreSQL server is re-established in case of an error (Bug 35700).

6.5.2. Software deployment command line tools

Feedback 


- When using `univention-upgrade` all components blocking an update are now displayed (Bug 37349).
- The available Univention App Center apps can now be queried on the command line by running `univention-add-app` with the parameter `--list` (Bug 37153).

6.6. Univention base libraries


Feedback 

- A new script `univention-install-joinscript` has been added. It can be used when developing packages for UCS that ship with a join script (Bug 32525).
- Fix a segmentation fault in `univention-debug` when reopening the logfile (Bug 37317).

6.7. System services


Feedback 

6.7.1. Spam/virus detection and countermeasures

Feedback 


- An obsolete cron job (`/etc/cron.daily/amavisd-new`) has been removed (Bug 36928).
- The new Univention Configuration Registry variable `variable mail/antispam/headertag` can be used to define a string to prepend to subject header field for SPAM messages. If the variable is unset (default), the subject is not modified (Bug 36664).
- The AMaViS service was always listed as stopped in the **System services** module of the Univention Management Console. This has been fixed (Bug 36998).

6.7.2. Printing services

Feedback 


- The permissions for the `pykotadmin.conf` Univention Configuration Registry template have been fixed (Bug 36859).

6.7.3. SSL

Feedback 


- Prior to the generation of the CA, the system time is updated. A timeout of 15 seconds has been added to the use of `rdate` to query the current time from a NTP time server, as this sometimes stalls endlessly (Bug 36934, Bug 36935, Bug 36937).

6.7.4. Univention System Info

Feedback 


- Fix error during parsing of `univention-system-info` output (Bug 36923).
- Fix the domain where archive uploads are sent to (Bug 31192).
- Improve error handling (Bug 33092).
- Fix uploading of archive for specific `dmidecode` versions (Bug 37384).

6.7.5. Apache

Feedback 

- This update disables the insecure SSL protocol v3. It is possible to override this by setting the Univention Configuration Registry variable `apache2/ssl/v3` to `true` before or after the update (Bug 36232).

6.7.6. Other services

Feedback 

- The startup mode of the MySQL database can now be configured via the Univention Configuration Registry variable `mysql/autostart` (Bug 13811).
- The new Univention Configuration Registry variable `mail/saslauthd/cache/timeout` (default 1800) has been added to define the `saslauthd` expiration time of the authentication cache (in seconds) (Bug 36949).

6.8. Virtualization

Feedback 


6.8.1. Univention Virtual Machine Manager (UVMM)

Feedback 


- If no connection to the UVMM daemon is possible, an error message is now displayed instead of a traceback (Bug 33963).
- Fix loading the kernel module `bridge` during initial installation (Bug 37215).
- The timeout for the `libvirtd` liveness check has been raised to 30 seconds (if the Univention Configuration Registry variable `libvirt/check/timeout` hadn't been modified locally (Bug 36605).
- Add a time stamp to the output of the `libvirt-check.sh` script output (Bug 35069).
- Temporary files for noVNC token files are now created on the same partition to fix a problem with cross-device renaming (Bug 36988). Also, fix the noVNC links for VMs running on localhost (Bug 36105).
- Display a HTTPS link for the first public and private IP of cloud instances (Bug 36905).

- Add tooltips displaying the security group and key pair in the instance wizard (Bug 36906).
- Fix header button of the cloud connection wizard to close only wizard and not the full module (Bug 36585).
- Add a progress bar while waiting for modifications of the state of a virtual instance (Bug 36380).
- Update the information of running cloud instances more often after adding, changing the state or deleting an instance (Bug 37301).
- Handle failure to stop UVMMd during update more gracefully (Bug 36927).
- Add a time stamp to the UVMMd check script output (Bug 37040) and log the complete output (Bug 34352).
- Ignore errors reading UVMM profiles (Bug 34542).

6.9. Services for Windows


Feedback 

6.9.1. Samba

Feedback 


- The SharePoint document search showed no results due to failing group membership check This has been fixed (Bug 37233).
- Quick successions of restarting Samba through init script restart could leave behind a single unresponsive samba process. This has been fixed (Bug 37343).
- The default for the Samba print server architecture was 32 bits. Now on newly installed systems the print server architecture is determined by the host architecture. Additionally the `smb.conf` parameter `spoolss:architecture` can be adjusted manually by setting the new Univention Configuration Registry variable `samba/spoolss/architecture` (see `man smb.conf`). On updated systems this UCR variable is maintained to keep the old default (Bug 34068, Bug 37476).
- A potential issue during the in-place migration from Samba 3 to Samba 4 has been fixed (Bug 36395).

6.9.2. Univention AD Takeover

Feedback 


- Several spelling mistakes have been fixed (Bug 35199).

6.9.3. Univention S4 Connector

Feedback 

- LDAP base DN's with uppercase letters caused synchronization rejects. This has been fixed (Bug 33110).
- GPO Security Descriptors can now be synchronized between OpenLDAP and the Samba directory service. By default this is not activated, an upcoming errata update for UCS@school 4.0 will make use of this feature (Bug 36980).
- Ignore `cn=Subschema` and warn if Univention Directory Listener didn't pass a `entryUUID` (Bug 36981).

6.9.4. Univention Active Directory Connection


Feedback 

- Check that the join account is member of the `Domain Admins` group in Active Directory (Bug 35562, Bug 37168).
- Don't fail if dynamic DNS update are disabled in the Active Directory domain (Bug 35870).
- Handle renames of the Administrator account in Active Directory (Bug 36776) and in UCS (Bug 36778).

Other changes

- Support direct unconditional clock synchronization with the Active Directory server (Bug 37481, Bug 36406).
- LDAP base DN's with uppercase letters caused synchronization rejects. This has been fixed (Bug 37450).

6.10. Other changes

Feedback 

- The following packages have been added to the maintained package repository (Bug 36467, Bug 36735, Bug 36609, Bug 37669, Bug 37288, Bug 36583):
 - *altermime*
 - *asterisk-config*
 - *asterisk-core-sounds-en-gsm*
 - *asterisk-modules*
 - *asterisk-moh-opsound-gsm*
 - *asterisk-voicemail*
 - *asterisk*
 - *autopoint*
 - *dahdi-linux*
 - *dahdi*
 - *docutils-doc*
 - *freetds-common*
 - *fxload*
 - *libalgorithm-diff-perl*
 - *libalgorithm-diff-xs-perl*
 - *libalgorithm-merge-perl*
 - *libapache2-mod-python*
 - *libapache2-svn*
 - *libart-2.0-2*
 - *libboost-thread1.49.0*
 - *libcorosync4*
 - *libfile-fcntllock-perl*
 - *libid3tag0*
 - *libjansson4*
 - *libmail-sendmail-perl*
 - *libopenais3*
 - *libopenr2-3*
 - *libpri1.4*
 - *libsox-fmt-mp3*
 - *libss7-1*
 - *openjdk-7-jdk*
 - *php-mdb2-driver-mysql*
 - *php-net-ldap2*
 - *php-net-url2*
 - *php5-sqlite*
 - *python-clearsilver*
 - *python-genshi*
 - *python-jinja2*
 - *python-renderpm*
 - *python-reportlab-accel*
 - *python-utidylib*
 - *ripole*
 - *smarty3*
 - *sox*
 - *trac*

- *vpb-driver-source*
 - *asterisk-modules*
 - *libcoroipcc4*
 - *libfile-fcntllock-perl*
 - *libgmime-2.6-0*
 - *libiksemel3*
 - *libmail-sendmail-perl*
 - *libopencore-amrnb0*
 - *libopencore-amrwb0*
 - *libpri1.4*
 - *libresample1*
 - *libsasl3*
 - *libsasvt3*
 - *libsox2*
 - *libsox-fmt-alsa*
 - *libsox-fmt-base*
 - *libsox-fmt-mp3*
 - *libsybdb5*
 - *libtonezone2.0*
 - *libvpb0*
 - *python-feedparser*
 - *python-libxslt1*
 - *python-mock*
 - *python-openid*
 - *python-passlib*
 - *python-psycogp2*
 - *python-pybabel*
 - *python-pychart*
 - *python-pydot*
 - *python-pypdf*
 - *python-unittest2*
 - *python-vatnumber*
 - *python-vobject*
 - *python-werkzeug*
 - *antiword*
 - *python-babel*
- This update silences the PHP cron job, which is cleaning up old PHP session files. Due to a mis-configuration from previous upgrades it was sending emails containing error messages every 30 minutes. This has been fixed (Bug 36621).
 - Timestamps were added to store the start and end times of individual join scripts in `join.log` (Bug 36290).
 - A traceback in `ucslint` module 0001 has been fixed. This traceback could appear if there were problems while reading the join scripts of the source package (Bug 37688).