univention
be open.

UCS 4.0-4 Release Notes

Release Notes für die Inbetriebnahme und Aktualisierung von Univention Corporate Server (UCS) 4.0-4

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

<feedback@univention.de>

univention
be open.

Inhaltsverzeichnis

1. Release-Highlights 4
2. Hinweise zum Update 5
    2.1. Empfohlene Update-Reihenfolge 5
    2.2. UCS-Installations-DVDs nur noch als 64-Bit-Variante 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 11
        6.2.1. Boot Loader 11
    6.3. Domain services 11
        6.3.1. OpenLDAP 11
            6.3.1.1. Listener/Notifier domain replication 11
    6.4. Univention Management Console 11
        6.4.1. Univention Management Console web interface 11
        6.4.2. Univention App Center 11
        6.4.3. Univention Directory Manager UMC modules and command line interface 11
        6.4.4. Basic settings / Appliance mode 12
        6.4.5. Other modules 12
    6.5. Software deployment 12
        6.5.1. Software deployment command line tools 12
    6.6. Univention base libraries 13
    6.7. System services 13
        6.7.1. Mail services 13
        6.7.2. Spam/virus detection and countermeasures 13
        6.7.3. SSL 13
        6.7.4. Apache 13
        6.7.5. PAM / Local group cache 14
        6.7.6. RADIUS 14
    6.8. Virtualization 14
        6.8.1. Univention Virtual Machine Manager (UVMM) 14
    6.9. Container Technologies 14
    6.10. Services for Windows 14
        6.10.1. Samba 14
        6.10.2. Univention AD Takeover 15
        6.10.3. Univention S4 Connector 15
    6.11. Other changes 15

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 4.0-4 steht das vierte Point-Release für Univention Corporate Server (UCS) 4.0 zur Verfügung. Es umfasst diverse Detailverbesserungen und Fehlerkorrekturen vor allem in den Bereichen Active Directory Kompatibilität und dem UCS-Managementsystem. Sämtliche für UCS 4.0-3 veröffentlichten Sicherheitsupdates sind in diesem Update enthalten.

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-DVSs werden ab UCS 4 nur noch für 64-Bit-Archtitekturen 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`.

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-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 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 **License type UCS Core 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.

5.2. 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 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 Änderungen seit UCS 4.0-3:

6.1. General

- All security updates issued for UCS 4.0-3 are included:
  - ***eglibc*** (CVE-2015-1472 CVE-2015-1473 CVE-2012-3406 CVE-2014-4043 CVE-2014-9402 CVE-2013-7424) (Bug 37643).
  - ***icu*** (CVE-2013-1569 CVE-2013-2383 CVE-2013-2384 CVE-2013-2419 CVE-2014-6585 CVE-2014-6591 CVE-2014-7923 CVE-2014-7926 CVE-2014-7940 CVE-2014-9654 CVE-2015-4760 CVE-2014-8146 CVE-2014-8147) (Bug 37629).
  - ***policykit-1*** (CVE-2015-4625 CVE-2015-3255 CVE-2015-3218) (Bug 38909).
  - ***file*** (CVE-2014-9653 CVE-2014-9652) (Bug 37747).
  - ***nss*** (CVE-2015-2721 CVE-2015-2730 CVE-2014-1569) (Bug 37045).
  - ***openssl*** (CVE-2014-8176 CVE-2015-1788 CVE-2015-1789 CVE-2015-1790 CVE-2015-1791 CVE-2015-1792 CVE-2015-4000) (Bug 38691).
  - ***dpkg*** (CVE-2015-0840) (Bug 38243).
  - ***libgcrypt11*** (CVE-2014-3591 CVE-2015-0837) (Bug 37922).
  - ***libssh2*** (CVE-2015-1782) (Bug 38013).
  - ***subversion*** (CVE-2015-0248 CVE-2015-0251 CVE-2015-3187) (Bug 38323).
  - ***cups-filters*** (CVE-2015-3258 CVE-2015-3279) (Bug 38790).
  - ***libreoffice*** (CVE-2014-9093 CVE-2015-1774) (Bug 37073).
  - ***requests*** (CVE-2014-1829 CVE-2014-1830) (Bug 37069).
  - ***ruby1.9.1*** (CVE-2014-4975 CVE-2014-8080 CVE-2014-8090 CVE-2015-1855) (Bug 36993).
  - ***squid3*** (CVE-2015-5400) (Bug 37038).
  - ***tidy*** (CVE-2015-5522 CVE-2015-5523) (Bug 39172).
  - ***vlc*** (CVE-2013-6933 CVE-2014-9626 CVE-2014-9627 CVE-2014-9628 CVE-2014-9629 CVE-2014-9630) (Bug 36952).
  - ***zendframework*** (CVE-2014-2681 CVE-2014-2682 CVE-2014-2683 CVE-2014-2684 CVE-2014-2685 CVE-2014-4914 CVE-2014-8088 CVE-2014-8089 CVE-2015-3154 CVE-2015-5161) (Bug 37002).
  - ***cups*** (CVE-2014-9679 CVE-2015-1158 CVE-2015-1159) (Bug 37815).
  - ***e2fsprogs*** (CVE-2015-0247 CVE-2015-1572) (Bug 37744).
  - ***gnutls26*** (CVE-2015-0294 CVE-2015-0282) (Bug 38067).

- ***libgd2*** (CVE-2014-2497 CVE-2014-9709) (Bug 37089).
- ***libtasn1-3*** (CVE-2015-2806) (Bug 38246).
- ***openldap*** (CVE-2015-6908) (Bug 39340).
- ***tiff*** (CVE-2014-8127 CVE-2014-8128 CVE-2014-8129 CVE-2014-9330 CVE-2014-9655 CVE-2015-1547) (Bug 37434).
- ***firefox-de*** (CVE-2015-2708 CVE-2015-0797 CVE-2015-2710 CVE-2015-2713 CVE-2015-2716 CVE-2015-2721 CVE-2015-4000 CVE-2015-2743 CVE-2015-2734 CVE-2015-2735 CVE-2015-2736 CVE-2015-2737 CVE-2015-2738 CVE-2015-2739 CVE-2015-2740 CVE-2015-2722 CVE-2015-2733 CVE-2015-2730 CVE-2015-2728 CVE-2015-2724 CVE-2015-2725 CVE-2015-2726 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 CVE-2015-4497 CVE-2015-4498) (Bug 38523).
- ***firefox-en*** (CVE-2015-2708 CVE-2015-0797 CVE-2015-2710 CVE-2015-2713 CVE-2015-2716 CVE-2015-2721 CVE-2015-4000 CVE-2015-2743 CVE-2015-2734 CVE-2015-2735 CVE-2015-2736 CVE-2015-2737 CVE-2015-2738 CVE-2015-2739 CVE-2015-2740 CVE-2015-2722 CVE-2015-2733 CVE-2015-2730 CVE-2015-2728 CVE-2015-2724 CVE-2015-2725 CVE-2015-2726 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 CVE-2015-4497 CVE-2015-4498) (Bug 38523).
- ***iceweasel*** (CVE-2015-2708 CVE-2015-0797 CVE-2015-2710 CVE-2015-2713 CVE-2015-2716 CVE-2015-2721 CVE-2015-4000 CVE-2015-2743 CVE-2015-2734 CVE-2015-2735 CVE-2015-2736 CVE-2015-2737 CVE-2015-2738 CVE-2015-2739 CVE-2015-2740 CVE-2015-2722 CVE-2015-2733 CVE-2015-2730 CVE-2015-2728 CVE-2015-2724 CVE-2015-2725 CVE-2015-2726 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 CVE-2015-4497 CVE-2015-4498) (Bug 38541).
- ***php5*** (CVE-2014-8116 CVE-2014-9652 CVE-2015-0232 CVE-2015-0273 CVE-2015-1352 CVE-2015-2301 CVE-2015-2305 CVE-2015-2331 CVE-2015-2348 CVE-2015-2783 CVE-2015-2787 CVE-2015-3329 CVE-2015-3330 CVE-2015-3411 CVE-2015-3412 CVE-2015-4021 CVE-2015-4022 CVE-2015-4024 CVE-2015-4025 CVE-2015-4026 CVE-2015-4147 CVE-2015-4148 CVE-2015-4598 CVE-2015-4599 CVE-2015-4600 CVE-2015-4601 CVE-2015-4602 CVE-2015-4603 CVE-2015-4604 CVE-2015-4605 CVE-2015-4643 CVE-2015-4644 CVE-2015-5589 CVE-2015-5590 CVE-2015-6834 CVE-2015-6835 CVE-2015-6836 CVE-2015-6837 CVE-2015-6838) (Bug 36997).
- ***postgresql-9.1*** (CVE-2015-3165 CVE-2015-3166 CVE-2015-3167) (Bug 38608).
- ***firefox-de*** (CVE-2015-4517 CVE-2015-4521 CVE-2015-4522 CVE-2015-7174 CVE-2015-7175 CVE-2015-7176 CVE-2015-7177 CVE-2015-7180 CVE-2015-4520 CVE-2015-4519 CVE-2015-4509 CVE-2015-4506 CVE-2015-4500 CVE-2015-4511) (Bug 39387).
- ***firefox-en*** (CVE-2015-4517 CVE-2015-4521 CVE-2015-4522 CVE-2015-7174 CVE-2015-7175 CVE-2015-7176 CVE-2015-7177 CVE-2015-7180 CVE-2015-4520 CVE-2015-4519 CVE-2015-4509 CVE-2015-4506 CVE-2015-4500 CVE-2015-4511) (Bug 39387).
- ***openssh*** (CVE-2015-5352 CVE-2015-5600) (Bug 39436).
- ***qemu-kvm*** (CVE-2015-5165 CVE-2015-5745 CVE-2015-5278 CVE-2015-5279 CVE-2015-6815 CVE-2015-6855) (Bug 39546).

6.2. Basic system services

Feedback

6.2.1. Boot Loader

Feedback

- A Secure Boot-signed version of GRUB has been added (Bug 39027).

6.3. Domain services

Feedback

6.3.1. OpenLDAP

Feedback

- When using the MDB backend, the LDAP search erroneously returned the base object in some cases. This has been fixed (Bug 36343).
- The confirmation prompt in non-interactive script `univention-backup2master` has been removed (Bug 38774).

6.3.1.1. Listener/Notifier domain replication

Feedback

- Any running Univention Directory Listener and Univention Directory Notifier are now forcefully terminated before the domain is joined (Bug 38756).
- LDAP and Univention Directory Notifier connections now use the TCP keep-alive mechanism and timeouts consistently to detect stuck connections (Bug 34763).
- A filter mechanism was added to the Univention Directory Listener to prevent certain objects from being stored to the local cache (Bug 38823).

6.4. Univention Management Console

Feedback

6.4.1. Univention Management Console web interface

Feedback

- Some widgets are now filtering out values which are already selected and don't present them in a dialogue anymore (Bug 37799).
- UMC modules with long descriptions might overlap the borders of the box in the Gallery. Now the text is cut at some point (Bug 39319).
- It is now easier to find information for creating custom attributes (Bug 39234).
- If a restart of the UMC components is required, the dialogue to ask for a page reload doesn't pop up (Bug 39578).

6.4.2. Univention App Center

Feedback

- Support for UCR variable templates in App Center readme files has been added (Bug 38233).
- The current App descriptions have been integrated into the App Center package (Bug 39316).

6.4.3. Univention Directory Manager UMC modules and command line interface

Feedback

- The mapping of syntax classes to UMC widgets is now extendible via the UCR variable group `directory/manager/web/widget/.*/` (Bug 39041).

- In some cases LDAP operations against a broken LDAP connection were done which led to LDAP connection invalid error messages. In that case the operation is executed again with a new LDAP connection (Bug 38346).
- The notification for successfully creating a user or computer now appears inside the wizard dialogue (Bug 38834).
- Opening a user object is now faster (Bug 38190).
- It is now easier to find information for creating custom attributes (Bug 39234).
- In previous versions the user's display name has only been set automatically during user creation. When the first name or last name has been changed later on, the display name of the user has not been updated. Starting from this update, the display name is updated automatically upon change of first or last name if the display name contains still the default value that has been automatically created. If the display name has been altered manually and does not match the default value, no automatic update is performed (Bug 38385).
- A user's display name will only be set automatically if first or last name were changed (Bug 39292).
- In some cases the automatic update of the attribute *displayName* caused tracebacks in the S4 Connector. The UDM module users/user has been updated to fix this traceback (Bug 39409).
- It is not possible any longer to create a user with a user ID (*uidNumber*) which already exists as group ID (*gidNumber*) (and vice versa) (Bug 38796).
- DNS TXT records are now shown via the UMC DNS module (Bug 25356).
- This update corrects problems with multi-edit operations as well as create and edit operations for UCS systems that have joined an existing AD domain (Bug 39779).

6.4.4. Basic settings / Appliance mode

Feedback

- A timing issue in the ***univenton-system-activation*** package that could occur when uploading a license has been fixed (Bug 39159).
- The e-mail validation is now done by the system activation wizard page (Bug 39153).
- A link has been added to skip the first system activation wizard page so the user has the opportunity to upload an existing license directly (Bug 39154).
- The App Center notification has been fixed in the system activation wizard (Bug 39395).
- The welcome screen initscript will now detect running instances and it will not be started when the installer is running (Bug 39137).

6.4.5. Other modules

Feedback

- An error has been fixed which could occur during querying the process list (Bug 39302).
- A new diagnostic plugin has been added to check SSH connections to other UCS servers (Bug 38137).

6.5. Software deployment

Feedback

6.5.1. Software deployment command line tools

Feedback

- The update scripts have been adjusted to UCS 4.0-4 (Bug 39711).

- The command line tool `univention-upgrade` is now able to perform App updates (Bug 30417).

6.6. Univention base libraries

Feedback

- Joining an UCS system into a subdomain of an Active Directory forest failed with a Python traceback because of an unexpected reply to an LDAP search request. This issue has been fixed (Bug 37626).

6.7. System services

Feedback

6.7.1. Mail services

Feedback

- The long waiting for the DH parameter generation on the first install has been removed in the Dovecot package (Bug 38990).
- DH parameters are not created at installation time any more. Pre-calculated DH parameters for 512 and 2048 bit are provided. A one time generation of DH parameters is scheduled for the next day (Bug 37459).
- The default of the UCR variable `mail/postfix/cron/recreate/dh/parameter` is changed to not recreate the DH parameters every night. The *cronjob* of existing installations is not changed (Bug 37459).
- The activation of `mail/postfix/policy/listfilter` led to the mail server rejecting all emails. This has been fixed (Bug 39093).
- A configuration error prevented Postfix from sending emails if Dovecot was also installed. Postfix' SMTP client now always uses the Cyrus SASL implementation (Bug 39151).
- A configuration error in the Dovecot PAM stack has been fixed that led to higher than usual time to authenticate against Postfix SMTP. In some cases Postfix' authentication timeout has been reached and resulted in authentication failure (Bug 39267).
- The Dovecot server did not close its standard error file descriptor (Bug 39148).
- The Dovecot logrotate configuration has been fixed (Bug 39130).
- Dovecot now works internally with lowercase email addresses (Bug 39346).

6.7.2. Spam/virus detection and countermeasures

Feedback

- AMaViS is now configured to use the default log template. Statistic tools like logwatch work better with it (Bug 38915).
- The UCR variable `mail/antivir/amavis/debug/level` can be used to set AMaViS' log level (Bug 38915).

6.7.3. SSL

Feedback

- Deleted SSL certificates are also deleted on DC backup servers (Bug 33870).

6.7.4. Apache

Feedback

- HTTP Strict-Transport-Security (HSTS) can be enabled and configured through the UCR variables `apache2/hsts`, `apache2/hsts/max-age`, and `apache2/hsts/includeSubDomains`. See their description for more details (Bug 37637).

6.7.5. PAM / Local group cache

Feedback

- The PAM script `lock-user` (automatic user lockouts) now sets the HOME environment variable before calling UDM to avoid problems with invalid HOME directories (Bug 39369).

6.7.6. RADIUS

Feedback

- Key expansion for DES encryption has been fixed (Bug 38785).
- File system permission of the DH file on UCS slave servers was fixed (Bug 38786).
- Raise fault tolerance by trying all available LDAP servers (Bug 39039).

6.8. Virtualization

Feedback

6.8.1. Univention Virtual Machine Manager (UVMM)

Feedback

- The VirtIO drivers for Windows have been updated to version 0.1.105 to fix a problem with broken driver signatures in Microsoft Windows 2012 server (Bug 38655).

6.9. Container Technologies

Feedback

- Package upgrade will not fail anymore if docker daemon was not running (Bug 38549).
- The docker server automatically starts when booting (Bug 38549).

6.10. Services for Windows

Feedback

6.10.1. Samba

Feedback

- The Samba dlz_bind9 module didn't properly handle zone reloads. The next request after a zone reload triggered a segmentation fault. After that bind9 was automatically restarted via runit, so the crash went unnoticed in most cases. Now the zone reload has been fixed (Bug 39139).
- Microsoft Windows 2008 R2 Foundation raised an error pop-up after join. This issue has been fixed previously but the fix was not part of the last Samba package version (Bug 39254).
- NetApp filer NAS devices joined to a Samba/AD DC failed to lookup SIDs due to an issue in negotiating strong encryption for server authentication. This issue has been fixed previously but the fix was not part of the last Samba package version (Bug 39263).
- Samba is now built with the embedded Heimdal code to avoid memory management issues with the external Heimdal libraries (Bug 39244).
- The unattended Microsoft Windows `sysprep` join failed against Samba 4. This issue has been fixed (Bug 39079).
- Under certain circumstances the Samba dlz_bind9 module crashed. This issue has been fixed (Bug 39362).
- Error handling and logging has been improved in the SYSVOL sync script (Bug 38868).
- A `testparm` error message about the UCS default for `winbind separator` has been relaxed to only issue a warning message (Bug 36581).

- The ACL check in the SYSVOL sync script has been fixed (Bug 39511).

6.10.2. Univention AD Takeover

Feedback

- The DNS zones `DC=DomainDnsZones` and `DC=ForestDnsZones` are synchronized now (Bug 34184).

6.10.3. Univention S4 Connector

Feedback

- The DNS zones `DC=DomainDNSZones` and `DC=ForestDNSZones` are synchronized now, this is relevant in AD Takeover scenarios. For updated domains, this is not activated (Bug 34184).
- The synchronization of SOA record changes back to UDM has been fixed (Bug 39040).
- The package ***univention-ldb-modules*** has been rebuilt to match the new Samba version (Bug 39275).
- The S4 Connector start failed if more than 1000 search results were returned by Samba 4 (Bug 39673).

6.11. Other changes

Feedback

- Incorrect quotation marks have been removed from `/etc/lsb-release` (Bug 37725).
- The list of supported message digest, encryption and key exchange algorithms allowed by the SSH daemon can now be configured through the new UCR variables `sshd/MACs`, `sshd/Ciphers`, and `sshd/KexAlgorithms` (Bug 38609).
- The insecure SSH protocols *rsa1* and *dsa* have been disabled. They can be re-enabled through the new UCR variables `sshd/Protocol` and `sshd/HostKey` (Bug 38709).
- The handling of UCR variable `sshd/banner` has been fixed (Bug 39166).
- The program `univention-openssh-recreate-host-keys` now re-creates all host key files supported by SSH (Bug 38710).
- The number of bits used when re-creating new host keys can be overwritten through the UCR variables like `sshd/HostKey/rsa` (Bug 38711).
- The package ***lockfile-progs*** has been moved to maintained, as ***univention-base-files*** depends on it (Bug 39357).
- The programs `ntpd` and `ntpdate` won't collide with each other, when started in short succession (e.g. while booting) (Bug 39299).