

UCS 3.2-3 Release Notes



**Release Notes für die Inbetriebnahme und Aktualisierung
von Univention Corporate Server (UCS) 3.2-3**

Alle Rechte vorbehalten. / All rights reserved.

(c) 2002-2014 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. Empfohlene Update-Reihenfolge für Umgebungen mit mehr als einem UCS-Server	6
3. Vorbereitung des Updates	7
4. Nachbereitung des Updates	8
4.1. Betrieb eines lokalen Repository-Servers / Preup- und Postup-Skripte	8
5. Hinweise zum Einsatz einzelner Pakete	9
5.1. Erfassung von Nutzungsstatistiken bei Verwendung der Free-For-Personal-Use-Version.....	9
5.2. UEFI-Installations-DVD	9
5.3. Umfang des Sicherheits-Supports von Webkit, Konqueror und QtWebKit	9
5.4. Empfohlene Browser für den Zugriff auf die Univention Management Console	9
5.5. Einschränkungen im Samba 4-Betrieb	10
5.6. Installation in VirtualBox	10
5.7. Installation in Citrix XenServer	10
5.8. Migration einer Samba 3-Umgebung auf Samba 4	10
5.9. Xen	11
6. Changelog	12
6.1. General	12
6.2. Univention Installer	12
6.3. Univention Updater	12
6.4. Basic system services	12
6.4.1. NFS	12
6.4.2. procps	12
6.4.3. rsync	12
6.4.4. Web	12
6.4.5. Quota	12
6.5. Domain services	13
6.5.1. Univention Directory Manager	13
6.5.2. OpenLDAP	13
6.5.2.1. LDAP ACL changes	13
6.5.2.2. LDAP schema changes	13
6.5.2.3. Listener/Notifier domain replication	13
6.5.3. Join	14
6.6. Univention Management Console	14
6.6.1. Univention Management Console web interface	14
6.6.2. Univention Management Console server	15
6.6.3. Univention App Center	15
6.6.4. Basic settings / Appliance mode	16
6.6.5. Computers module	16
6.6.6. Other modules	16
6.6.7. Univention Directory Manager command line interface and related tools	16
6.7. Univention Library	16
6.8. System services	17
6.8.1. Spam/virus detection and countermeasures	17
6.8.2. Nagios	17
6.8.3. Proxy services	17
6.8.4. PAM / Local group cache	17
6.8.5. Other services	17
6.9. Virtualisation	17
6.9.1. Xen	17
6.10. Services for Windows	18
6.10.1. Samba NT domain support	18
6.10.2. Samba AD domain support	18

6.10.3. Univention AD Takeover	18
6.10.4. Univention S4 Connector	19
6.10.5. Univention Active Directory Connector	19
6.11. Other changes	19
Literaturverzeichnis	21

Kapitel 1. Release-Highlights

Mit Univention Corporate Server 3.2-3 steht das dritte Point-Release für Univention Corporate Server (UCS) zur Verfügung. Es beinhaltet alle für UCS 3.2-2 veröffentlichten Errata-Updates:

- Das neue Modul *Active Directory-Verbindung* führt die durch UCS verwaltete Domäne und ein bestehendes Active Directory zusammen. UCS steht dann als Plattform für den integrierten Betrieb von Apps in einer Active Directory-Domäne zur Verfügung.
- Der UCS-Einrichtungsassistent wurde komplett überarbeitet und führt den Nutzer nun deutlich komfortabler durch die Domänenkonfiguration von UCS, indem z.B. Konfigurationseinstellungen automatisch ermittelt und entsprechende Vorschläge gemacht werden.
- PHP 5.4.4 wurde nach UCS 3.2 zurück portiert. Es kann aus einem separaten Repository installiert werden und wird darüber auch mit Sicherheitsupdates versorgt.
- Die OpenLDAP-Replikation wurde deutlich verbessert, indem Änderungen im Verzeichnisdienst nun mit einer eindeutigen ID verfolgt werden. Das erhöht die Replikationsgeschwindigkeit und verringert Replikationsfehler.
- Das Linux-Kernel-Paket wurde auf Version 3.10.11 aktualisiert. Dies verbessert neben vielen Bugfixes auch den Hardware-Support.
- Die Active Directory-Kompatibilität wurde weiter verbessert, indem nun das Microsoft Data Protection Application Program Interface (DPAPI) unterstützt wird.

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.

Generell ist es empfehlenswert, alle UCS-Systeme möglichst in einem Wartungsfenster zu aktualisieren.

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 Console mit dem Benutzer *root* durchgeführt und das Update dort gestartet werden. Alternativ kann das Update über die 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 folgenden Befehls als Benutzer *root*:

```
univention-run-join-scripts
```

Anschließend sollte das UCS-System neu gestartet werden.

4.1. Betrieb eines lokalen Repository-Servers / Preup- und Postup-Skripte

Feedback 

Preup- und Postup-Skripte sind Skripte, die vor und nach Release-Updates aufgerufen werden (z.B. zur Nachbereitung des Updates, etwa die Deinstallation obsoleter Pakete). Ab UCS 3.2 werden diese Skripte kryptographisch signiert, um eine unerlaubte Modifikation zu verhindern. Beim Update und Spiegeln des Repositories werden diese Signaturen überprüft. Sind diese ungültig oder fehlen, so wird die Aktion abgebrochen.

Wird ein Repository-Server mit UCS 3.1-x betrieben, muß dieser auf UCS 3.2 aktualisiert werden, bevor weitere Systeme auf UCS 3.2-1 oder neuer aktualisiert werden können.

Wenn ein Update des Repository-Servers nicht möglich ist, müssen die Signaturdateien manuell heruntergeladen werden:

```
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; 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
```

Alternativ kann die Prüfung der Signaturen auch deaktiviert werden, was ein Sicherheitsrisiko darstellen kann. Für den Repository-Server kann dazu die Univention Configuration Registry-Variable `repository/mirror/verify` auf *false* gesetzt werden. Für das Update muß auf allen Systemen die Univention Configuration Registry-Variable `repository/online/verify` auf *false* gesetzt werden.

Kapitel 5. Hinweise zum Einsatz einzelner Pakete

5.1. Erfassung von Nutzungsstatistiken bei Verwendung der Free-For-Personal-Use-Version

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 der 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 der 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 durch einen Klick auf das Zahnrad-Symbol in der rechten, oberen Ecke der Univention Management Console und die Auswahl von **Lizenzinformationen** geprüft werden. Steht hier unter **Lizenztyp** *Free for personal use edition* wird eine solche Version verwendet. Bei Einsatz einer regulären UCS-Lizenz wird keine Nutzungsstatistik gesammelt.

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

5.2. UEFI-Installations-DVD

Für die Architektur *amd64* steht neben der Standard-Installations-DVD auch ein Medium mit Unterstützung für den Unified Extensible Firmware Interface-Standard (UEFI) bereit.

Auf Systemen, die nur einen UEFI-Start unterstützen, muss die UEFI-Installations-DVD anstelle der Standard-DVD verwendet werden.

5.3. Umfang des Sicherheits-Supports von Webkit, Konqueror und QtWebKit

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 die Univention Management Console


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.

5.5. Einschränkungen im Samba 4-Betrieb


Feedback 

In Samba 4 stehen einige Active-Directory-Funktionen noch nicht vollständig zur Verfügung:

- Microsoft Windows Domänencontroller dürfen aktuell nicht in eine Samba 4-Domäne beitreten.
- Eine selektive Replikation ist mit Samba 4 nicht möglich, da diese durch Active Directory prinzipiell nicht unterstützt wird (in UCS@school basiert die selektive Replikation auf der Listener/Notifier-Replikation).
- Samba 4 unterstützt aktuell keine Forest-Domänen.
- Samba 4 unterstützt aktuell keine Vertrauensstellungen.

Weitere Hinweise finden sich in Kapitel 8 des [ucs-handbuch].


5.6. Installation in VirtualBox

Feedback 

Bei der Installation von UCS in der Virtualisierungslösung VirtualBox vor Version 4.2 kann folgender VirtualBox-Bug auftreten: Wenn von der Installations-DVD gebootet wird, bietet GRUB die Option **Boot from first harddisk partition** an. Wählt man diese Option aus, friert VirtualBox ein.

Als Workaround muß vor dem Neustart der UCS-VM entweder die Installations-DVD aus den Laufwerkeinstellungen der VirtualBox-VM entfernt werden oder beim Start der virtuellen Instanz **F12** gedrückt werden und die Festplatte als Bootpartition ausgewählt werden. UCS startet danach dann problemlos.

5.7. Installation in Citrix XenServer


Feedback 

Bei der Installation von UCS in der Virtualisierungslösung Citrix XenServer 6.0 - 6.2 wird mit der standardmäßig emulierten Cirrus-Grafikkarte das GRUB-Menü des Univention Installers nicht angezeigt. Der Univention Installer kann durch Drücken der **ENTER**-Taste direkt gestartet werden; alternativ startet die Installation automatisch nach sechzig Sekunden. Der dann gestartete Univention Installer wird normal dargestellt.

Um GRUB korrekt darzustellen, kann die von XenServer emulierte Grafikkarte umkonfiguriert werden. Dazu muss eine Anmeldung als Benutzer *root* auf dem XenServer-System folgen. Mit dem Befehl `xe vm-list` muss zuerst die UUID der virtuellen Maschine ermittelt werden. Mit dem folgenden Befehl wird dann die emulierte Grafikkarte auf VGA umkonfiguriert:

```
xe vm-param-set uuid=UUIDVM platform:vga=std
```

5.8. Migration einer Samba 3-Umgebung auf Samba 4

Feedback 

Es existieren zwei grundlegende Verfahren zur Migration von Samba 3 auf Samba 4:

- Aufbau einer parallelen Samba 4-Domäne. Beide Domänen verwenden unterschiedliche NetBIOS-Namen und SIDs. Die Clients treten dann schrittweise der Samba 4-Domäne bei.
- Migration aller Systeme innerhalb eines Wartungsfensters.

Beide Verfahren sind im Univention Wiki ausführlich dokumentiert: http://wiki.univention.de/index.php?title=Migration_from_Samba_3_to_Samba_4.


5.9. Xen

Wenn der Xen Hypervisor benutzt wird und das Speicherlimit über die Univention Configuration Registry-Variable `grub/xenhopt` begrenzt wurde, sollte der Wert aktualisiert und um die `,max:-`Angabe erweitert werden. Weitere Details finden sich unter http://wiki.univention.de/index.php?title=UVMM_Quickstart-3.1#Konfiguration_der_Dom0.

Kapitel 6. Changelog


Die Changelogs mit den detaillierten Änderungsinformationen werden nur in Englisch gepflegt. Aufgeführt sind die Änderungen seit UCS 3.2-2:

6.1. General

Feedback 


- All security updates issued for UCS 3.2-2 are included.

6.2. Univention Installer

Feedback 


- The component *Active Directory Connector* has been renamed to *Active Directory Connection* in the software selection of the installer (Bug 35414).

6.3. Univention Updater

Feedback 

- The local UCR variable *uuid/license* is now removed if the key ID is missing in the UCS license (Bug 34809).
- `univention-add-app` no longer registers a link on the UCS startsite and removes the component again if called with `--master` (just like the App Center module) (Bug 35022).
- The component installation status is now transferred via the apt user agent (Bug 33807).

6.4. Basic system services


Feedback 

6.4.1. NFS

Feedback 


- This update fixes a bug in the NFS utils package for users with many groups (Bug 34597).

6.4.2. procps

Feedback 


- This update fixes a bug in the procps package for users with many groups (Bug 34596).

6.4.3. rsync

Feedback 


- This update adds a new option `--dirs-update` to rsync (Bug 34430).
- The parameter `--dirs-update` was introduced with erratum 121. When using this parameter it could happen that the permissions were not transferred as expected. This error has been fixed. (Bug 35105).

6.4.4. Web

Feedback 

- The URL of the Univention App Center landing page has changed. Therefore, the corresponding links in the UCS overview page have been adapted (Bug 34864).
- Links to local web interfaces of installed Apps were placed on top of the UCS overview page if no priority was specified via UCR. They will now be positioned at the end (Bug 33750).


6.4.5. Quota

Feedback 


- The quota for the root (/) partition can now be configured via the filesystem quota UMC module (Bug 31277).

- Update for univention-user-quota. Evaluate the share policy flag "*reapplyeverylogin*" and (re-)apply quota settings on every user login if set (Bug 33174).
- Correct behaviour while searching for the most restrictive user quota settings on a mountpoint (Bug 33174).

6.5. Domain services


Feedback 

6.5.1. Univention Directory Manager

Feedback 


- Removing all Nagios services from a computer object no longer yields an error (Bug 33120, Bug 34037).
- Same for Nagios hosts (Bug 34037).
- Adding a DNS reverse zone to a computer object while removing an IP address no longer yields an error as well (Bug 34250).
- Documentation for a UCR variable added that makes the name of an object in the frontend grid configurable (Bug 34200).
- Removed the input field Organisation from the group *Personal information* and added it to the group *Organisation* (Bug 28630).
- Added new option to share-userquota policy: Reapply quota on every login (Bug 33174).
- Add possibility to mark UDM properties as readonly when UCS is part of an Active Directory domain (Bug 34092).
- The script "proof_uniqueMembers" will no more crash on empty uniqueMember attributes (Bug 33030).

6.5.2. OpenLDAP

Feedback 


- This update adds *entryUUID* to the list of indexed LDAP attributes, which is used by the Univention Directory Listener to track moved objects (Bug 34815).
- The OpenLDAP schema for NIS (nis.schema) has been altered: The schema definition of the attribute *shadowExpire* contains now a ORDERING statement (Bug 35329).
- A new OpenLDAP overlay module has been added: *pwd_scheme_kinit*. It allows to set the userPassword attribute to *{KINIT}* which redirects the authentication to a kerberos server (Bug 35092).
- Support for the overlay module *pwd_scheme_kinit* has been added (Bug 35093).
- The UCR variable *ldap/sasl/secprops/maxssf* has been added to configure the *sasl_secprops_maxssf* value in */etc/ldap/ldap.conf* (Bug 35513).

6.5.2.1. LDAP ACL changes

Feedback 


- A regression in the LDAP ACLs has been fixed. The ACLs for the "dc" and "memberserver" containers now again allow subfolders (in *cn=dc* resp. *cn=memberserver*) (Bug 34554).

6.5.2.2. LDAP schema changes

Feedback 

- New share-userquota binary attribute: Reapply quota on every login (Bug 33174).


6.5.2.3. Listener/Notifier domain replication

Feedback 

- The case of distinguished names (DN) sometime differs between different clients and is now ignored (Bug 34835).


- A rename of an LDAP object can lead to a single-values attribute becoming multi-valued, which breaks multiple modules, especially the synchronization to Samba. The listener now implements `delold=1` and removes all old RDNs to just keep the new RDN (Bug 34802).
- When an object is renamed or moved via a container, which is later deleted, the listener fails to follow the rename. This has been fixed by creating a fake temporary container (Bug 34833).
- In case of an error the replication listener handler is now restarted with the old object from the directory listener (Bug 34759).
- This update fixes a replication problem, when an object is removed and re-created at the same location. This happened when a failing listener module prevents the removal of the object from the listener cache, which is used to track objects being moved (Bug 35261).

6.5.3. Join


 Feedback 

- `univention-join` now checks for the AD member mode during the join. If the domain is in the AD member mode, `univention-join` configures the local system as part of the AD domain. (Bug 35470 Bug 35446).

6.6. Univention Management Console

 Feedback 


6.6.1. Univention Management Console web interface

 Feedback 

- The UMC grid can now allow the execution of an action even though some of the selected items are not executable with regard to the action (Bug 34965).
- A function has been added to reload the modules of the overview tab on the fly (Bug 34243).
- A default link to UMC has been added on the UCS overview page for unjoined systems (Bug 34317).
- When installing a new system which is neither a master domain controller master nor a backup domain controller backup, the UMC entry in the UCS overview page will no longer consider the UMC a domain administration tool, as the domain modules are only available on master and backup systems (Bug 33615).
- A timeout problem in the UMC web server has been fixed (Bug 35052).
- When a user cancels the dialogue which asks for a UMC server restart, the modules on the UMC overview page are now reloaded (Bug 34243).
- CSS rules have been adapted to apply the UMC theme to `dijit/form/Select` (Bug 34484).
- The `async` attribute is now used in the script tag that loads `dojo.js` (Bug 34484).
- UMC tabs and header are not shown in the appliance mode (Bug 34484).
- In the appliance mode, only the specified JavaScript module is loaded upon startup instead of all accessible JavaScript modules (Bug 34484).
- Dynamic reloading of translations is now supported (Bug 34484).
- A widget for radio buttons has been added (Bug 34484).
- A method `defer()` has been added to `umc/tools` (Bug 34484).
- The validation of forms has been fixed, such that invalid fields are marked with a red exclamation mark when calling `umc/widgets/Form:validate()` (Bug 34484).


- Vertical scrolling issues with *umc/widgets/Grid* in Firefox have been fixed (Bug 34484).
- The configuration property *labelConf* has been added to be able to configure LabelPanels directly (Bug 34484).
- Allow dynamic changing of *inlineLabel* in *umc/widgets/TextBox* (Bug 34484).
- The convenience method *isPageVisible()* has been added to *umc/widgets/Wizard* (Bug 34484).

6.6.2. Univention Management Console server

Feedback 


- The internal cache of UMC modules in the UMC Server is now invalidated before they are requested (Bug 34243).
- It is now possible for UMC modules to provide a user friendly error message when initialization failed (Bug 34723).
- Changes of system clock (e.g. due to NTP updates) will not make UMC processes die by timeout anymore (Bug 34105).
- The UMC server parses operation set strings more carefully now to avoid server crashes (Bug 25196).
- The error handling of requests have been improved (Bug 34244).

6.6.3. Univention App Center

Feedback 


- Improved performance: Applications are opened immediately when clicking on them from the app gallery (Bug 31915).
- Improved performance: When new apps are added or existing apps' meta information changes, new files need to be downloaded from the server. If many files have changed, instead of downloading them all one after another, a compiled archive is downloaded and the files are extracted. This also fixes issues with many concurrent connections opened on the App Center server (Bug 32935).
- A dedicated component for the Radius application is removed (if Radius is installed). It was added by mistake as *univention-radius* is part of the main repository (Bug 34867).
- The UCR variable *repository/app_center/installed* is now set and kept up-to-date. It reflects the state of the installation status of all apps (Bug 35177).
- The details of an application do not show the note whether this application sends information to the vendor or not if it is a UCS component (Bug 35176).
- Fixed LDAP errors when registering applications: ID and Version of an application are now escaped (Bug 35136).
- The UCR variable *repository/app_center/installed* is initially set during installation/update of this package (Bug 35271).
- When the system is part of a Windows Active Directory domain, certain applications are not shown (Bug 35454).
- When the system is part of a Windows Active Directory domain, certain applications warn before installation that a password service needs to be running on the Windows Domain Controller (Bug 35453).
- Linked the UCR variable *repository/app_center/installed* to the creation of certain UMC module definition files. This fixes issues with modules not showing up in *Installed Apps* after the initial setup of the server (Bug 35565).

6.6.4. Basic settings / Appliance mode

Feedback 


- The setup wizard for UCS appliance has been entirely re-structured and rewritten, obsolete code paths have been cleaned up. Some of the new features include:
 - A live search for world-wide cities to preconfigure locale settings.
 - Wizard language can be changed on the fly without a page load.
 - Some fields (host + domain name, gateway address etc.) are pre-filled with suggested values to ease the configuration.
 - The UCS license activation can now be carried within the wizard.
 - UCS components from the App Center can be installed in the wizard. (Bug 34484)
- Running setup scripts will not terminate when the UMC module process does, and also keep the UMC module process from timing out (Bug 34105).
- Added welcome page with instructions to set a root password before accessing the setup wizard for EC2 setups (Bug 34388).

6.6.5. Computers module

Feedback 


- A traceback has been fixed which could occur when creating computer objects with a given DHCP or DNS zone, but without an IP address. The traceback could also occur when removing DHCP/DNS zones along with all IP addresses (Bug 33843).

6.6.6. Other modules

Feedback 


- When the initialization of the UMC module *univention-pkgdb*, or any command execution, fails because the PostgreSQL is not running, a user friendly error message will be shown instead of debug information in a feedback dialog (Bug 34723).

6.6.7. Univention Directory Manager command line interface and related tools

Feedback 

- The property that is used in the first column of the grid ("Name") is now configurable via UCR (Bug 34200).
- Some UDM attributes are shown as readonly if the domain is part of an Active Directory Domain (Bug 34092).
- Display a warning in Active Directory Mode before creating objects which are not synchronized back to AD (Bug 34093).
- Display a human readable error message when the connection to the LDAP server failed (Bug 34244).


6.7. Univention Library

Feedback 


- Several functions for configuring the AD member mode have been added to univention-lib (Bug 34091, Bug 35470, Bug 35467, Bug 35520, Bug 35551, Bug 35566).
- When an object is renamed in LDAP, the old relative distinguished name (RDN) values are kept by default. This leads to situations, where an attribute declared as single-valued may become multi-valued, which

breaks the replication to Samba 4 and confuses several other listener modules. This erratum changes the low-level Univention LDAP code to remove the old RDN values as well, as all other code paths already do so (Bug 34971).

6.8. System services


Feedback 

6.8.1. Spam/virus detection and countermeasures

Feedback 


- ClamAV has been updated to version 0.98.1 (Bug 33995).

6.8.2. Nagios

Feedback 


- Change `UNIVENTION_NTP` Nagios check to compare NTP server time by using the plugin `check_ntp_time`. The previous check also queried NTP server configuration options, which are not relevant for this check and, since UCS 3.2 errata 20, are not allowed to be queried from external sources (Bug 34570).

6.8.3. Proxy services

Feedback 


- The UCR variable `squid/forwardedfor` has been added to configure Squid's `forwarded_for` configuration directive (Bug 34025).

6.8.4. PAM / Local group cache

Feedback 


- Kerberos authentication is now limited to non-local accounts with `UID >= 1000`. The limit can be configured through the new Univention Configuration Registry variable `pam/krb5/minimum_uid` (Bug 34315).
- The mapping of user and group names in the UCR templates was not updated in all cases. This has been fixed (Bug 34742).
- The listener module `well-known-sid-name-mapping` now recognizes SID changes (Bug 35501).

6.8.5. Other services


Feedback 

- This update provides the older version 3.72 of `syslinux`, a boot loader for Linux. It is used by the UCS network installer. Due to some BIOS incompatibilities the newer `syslinux` from UCS-3 fails to boot some notebooks like the DELL E6510 either locally or via PXE. The older version can be installed as a replacement version if such problems occur. For this the packages `"syslinux3"` and `"syslinux3-common"` must be installed instead of `"syslinux"` and `"syslinux-common"` by using the command-line tool `"univention-install"` as the user `"root"` or as an Administrator through the UMC web interface by using the App-center module (Bug 33531).
- AD member mode has been added to `univention-heimdal` (Bug 35470).

6.9. Virtualisation


Feedback 

6.9.1. Xen


Feedback 

- This update rate-limits a log message printed by the QEMU device model to prevent the log-file from growing by 50 MiB/s after a virtual machine has been migrated (Bug 35488).
- A kernel OOPS on the Xen host while rebooting a Xen VM has been fixed. The error is caused by the Xen `netback` subsystem (Bug 35178).

6.10. Services for Windows


 Feedback 

6.10.1. Samba NT domain support

 Feedback 


- In Samba 3.6 and older the execution right in the ACL was not checked, so a client could execute a file even if it did not have execute rights on the file. In Samba 4.0, this has been fixed. To re-establishing the old behaviour the new UCR variable *samba/acl/allow/execute/always* has been added (default: True) (Bug 33785).
- Missing initialization of the UCR variable *samba/role* has been added to the postinst script of *univention-samba* (Bug 35584).

6.10.2. Samba AD domain support

 Feedback 


- Modifications of access rights of GPOs could get reset by the sysvol replication. This affected directories in the sysvol share (Bug 33751).
- Clean up */var/lib/samba/private* before new provision (relevant for UCS@school Slave PDCs) (Bug 32246).
- Preserve */var/lib/samba/**, only clear private subdir before re-join (Bug 35000).
- Preserve *rIDNextRID* during re-join and provision (Bug 34754).
- This update fixes an issue which caused a problem for the Windows DPAPI. To users it appeared as if stored credentials for Windows applications would not be remembered any longer by the applications after they changed the logon password for their account. Domains affected by this need to manually remove the object "CN=BCKUPKEY_PREFERRED Secret" from the Samba directory service after the update to make Samba internally generate a new ticket for the Backupkey protocol (Bug 35287).
- In Samba 3.6 and older the execution right in the ACL was not checked, so a client could execute a file even if it did not have execute rights on the file. In Samba 4.0, this has been fixed. To re-establishing the old behaviour the new UCR variable *samba/acl/allow/execute/always* has been added (default: True) (Bug 35137).
- The *univention-samba4* join script now always cleans up the samba private directory before the join and if the samba4 join fails, the join is aborted (Bug 34422).
- A typo in *univention-samba4-backup* has been fixed (Bug 35084).
- The UCR variable *samba4/backup/cron/options* has been added to configure options for the *univention-samba4-backup* script started by cron (Bug 35085).
- AD member mode has been added to *univention-samba* (Bug 35095, Bug 35470, Bug 35467).
- The *joinscript* of *univention-samba4* was adjusted to abort if the domain is in AD member mode (Bug 35252).

6.10.3. Univention AD Takeover

 Feedback 

- The UMC module for AD Takeover has been adjusted to fix a case where the path to one of the two default GPOs did not match the actual folder copied from the Windows AD server (Bug 34776).
- The UMC module for AD Takeover has been adjusted to support UCS domains in AD member mode (Bug 35346).

6.10.4. Univention S4 Connector

Feedback 


- The *entryUUID* of deleted objects in OpenLDAP is now saved to a local cache. This will prevent a recreation of deleted objects (Bug 32263).
- The synchronization has been changed to a diff based algorithm (Bug 33621).
- In some cases a removed group membership was not synchronized from OpenLDAP to Samba 4 in write mode (Bug 35238).
- Restart bind9 instead of samba4 if the *ldap/master* can't be resolved (Bug 34865).
- Two tools for removing rejected objects have been added:

```
/usr/share/univention-s4-connector/remove_ucs_rejected.py
```

```
/usr/share/univention-s4-connector/remove_s4_rejected.py  
(Bug 32194).
```


- Add a new parameter "acl xattr update mtime" for use in `smb.conf` share sections. This will be used for the `sysvol` share to make `rsync` recognize permission changes on directories (Bug 34431).
- An error in the internal conversation of the attribute *userParameters* has been fixed. This error could lead to a blocked samba process (Bug 34777).
- DNS updates of records with existing IPv6 addresses have been fixed (Bug 34868).
- Issues with the NetApp join have been fixed (Bug 34886).
- The `joinscript` of package *univention-s4-connector* was adjusted to abort if the domain is in AD member mode (Bug 35500).
- The command line script `univention-ad-takeover` has been removed since the UMC module is more recent (Bug 35514).

6.10.5. Univention Active Directory Connector

Feedback 

- Support for the `ad/member` mode has been added (Bug 35091).
- In some cases a removed group membership was not synchronized from OpenLDAP to Active Directory in write mode (Bug 35234).
- The AD certificate chain is no longer checked if there is no root certificate configured (Bug 35253).
- Kerberos support has been added to the UCS AD connector (Bug 35349).
- A script has been added for renaming groups and users with Well Known SIDs to the corresponding name in the AD domain. This script is for internal use by the setup wizard for the UCS in AD member mode (Bug 35507).
- A script has been added to grant read permission to the `CN=Deleted Objects` container in Active Directory. This is only required for the AD Member mode (Bug 35566).

6.11. Other changes

Feedback 

- The following packages have been moved to the maintained repository

Other changes

- *texlive-generic-extra* (Bug 33611)
- *python-dateutil*, *python-tz*, *libboost-thread1.42.0*, *libssp-uuid16*, *libxerces-c3.1*, *php-auth*, *augeas-lenses*, *libaugeas0*, *python-augeas*, *python-cheetah*, *libmail-spf-perl*, *manpages-dev*, *re2c*, *zend-framework* (Bug 34260)
- *rsyslog-relp* (Bug 34872)
- *php5-sqlite* (Bug 35030)
- *libapache2-mod-perl2*, *libapache2-reload-perl*, *libyaml-libyaml-perl*, *libdevel-symdump-perl*, *libbsd-resource-perl* (Bug 35160)
- *mt-st* (Bug 35388)
- This update provides the new archive signing key for UCS 4.0. UCS 4.0 is not released yet, but we already distribute the key in advance to ensure the availability of the archive key when updating from UCS 3.2-3 to UCS 4.0 at a later point (Bug 35213).

Literaturverzeichnis

[ucs-handbuch] Univention GmbH. 2013. *Univention Corporate Server - Manual for users and administrators*. <http://docs.univention.de/manual-3.2.html>.