

UCS 2.1-0 Changelog

Thema:	Protokollierung der Änderungen zwischen den Univention Corporate Server-Versionen 2.0-2 und 2.1-0
Datum:	12. August 2008
Seitenzahl:	12
Versionsnummer:	1956
Autoren:	Univention GmbH feedback@univention.de

Inhaltsverzeichnis

1 Hinweise zum Update	3
1.1 Vorbereitung des Updates	3
1.2 Nachbereitung des Updates	3
2 Allgemein	3
3 Sicherheitsupdates	4
4 Univention Managementsystem	5
4.1 Univention Directory Manager	6
4.2 Univention Management Console	6
5 Univention Groupware Server	7
5.1 Kolab2-Groupware-Webclient Horde	7
5.2 Maildienste	8
6 Thin Client-Infrastruktur	8
7 Univention Corporate Desktop	8
8 Services for Windows/Samba	9
9 Univention Active Directory Connector	10
10 Linux Kernel und Kernel-Module	10
11 Weitere Dienste und Pakete	11

1 Hinweise zum Update

Falls Ihnen von Univention angepasste Paketversionen bereitgestellt wurden, so sollte geprüft werden, ob durch die Aktualisierung auf UCS 2.1-0 die angepassten Pakete überschrieben werden – vorzugsweise in einer Testumgebung. Sollten Sie hier Probleme feststellen oder die gemachten Anpassungen für die aktuellen UCS-2.1-Paketversionen benötigen, so wenden Sie sich bitte an Univention.

1.1 Vorbereitung des Updates

Wird ein System mit UCS 1.3 oder 2.0 ohne Anlegen eines lokalen Repositories installiert, wurde vom Installer trotzdem ein Eintrag in die Datei `/etc/apt/sources.list` aufgenommen, der das Repository über den DNS-Alias **univention-repository** referenziert. Wenn in der Domäne kein weiteres Repository existiert, kann dies dazu führen, dass Univention Updater mit der Fehlermeldung **Failed to execute apt-get update** abbricht. In diesem Fall sollte in der Datei `/etc/apt/sources.list` die folgende Zeile auskommentiert oder entfernt werden:

```
deb http://univention-repository.domain.test/univention-cdrom/packages/ ./
```

Im überarbeiteten Univention Installer für UCS 2.0 und UCS 2.1 wird bei nicht angelegtem Repository automatisch das Univention Online Repository eingebunden.

1.2 Nachbereitung des Updates

Nach dem Update sollte auf jedem System überprüft werden, ob alle Join-Skripte ausgeführt wurden. Dies kann entweder über die Univention Management Console oder über das neue Kommandozeilen-Tool `univention-run-join-scripts` durchgeführt werden.

2 Allgemein

- Je nach gewähltem Lizenzierungsmodell kontrolliert die Lizenzüberprüfung jetzt Maschinen- oder Benutzerkonten. Dies hat zur Folge, dass die Lizenzüberprüfung restriktiver ist. Sollten die Lizenzen nicht mehr ausreichen, bspw. bei der "free for personal use"-Lizenz, so wenden Sie sich bitte an Univention (feedback@univention.de). Für den privaten Gebrauch werden auf Anfrage auch größere Lizenzen ausgegeben.
- Ein Darstellungsfehler in `univention-license-check` bei der Anzeige der Anzahl der verwendeten Benutzerlizenzen wurde behoben.
- Die Unterstützung für die Architektur `amd64` bzw. `x86_64` wurde der Distribution hinzugefügt. Dafür wurden mehrere Pakete angepasst, u.a. Firefox und die Firefox-Plugins.

- Ein Fehler, der die Ausführung von `univention-system-setup-boot` während des Bootvorgangs verhindert hat, wurde behoben.
- Ein Fehler im Paket **libnss-ldap** wurde behoben, der zu Anwendungsabstürzen bei der Verwendung des PAM-Stacks führen konnte.
- Fünf neue Systemgruppen (`scanner`, `nvrnm`, `rdma`, `kvm` und `fuse`) und ein neuer Systembenutzer (`tss`) werden nun angelegt. Dies verhindert einige Fehlermeldungen des `udev`-Dienstes während des Bootvorgangs.
- `cdrom`-Quellen in der Datei `/etc/apt/sources.list` werden ab sofort während des Aufrufs von `univention-updater` und `univention-actualise` permanent auskommentiert.
- Es wurde der Befehl `univention-repository-create` hinzugefügt, um das nachträgliche Anlegen eines lokalen Repositories zu erleichtern.
- Ein Fehler in der Repository-Verwaltung wurde behoben, der dazu führen konnte, dass Updates trotz nicht gesetzter Release-Richtlinie auf UCS-Systemen eingespielt wurden.

3 Sicherheitsupdates

- Die Blacklists für kompromittierte SSH-Schlüssel wurde nach `/usr/share/ssh` verschoben. Außerdem steht nun ein zusätzliches Paket **openssl-blacklist-extra** bereit, in dem betroffene Schlüssel in Nicht-Standard-Schlüssellängen gespeichert sind.
- OpenSSH ersetzt betroffene Host-Keys nun automatisch und der Befehl `ssh-vulnkey` prüft nun auch Einträge in der Datei `/.ssh/authorized_keys` in denen Optionen gesetzt sind.
- Das Paket **openssl-blacklist** stellt Blacklists für generische OpenSSL-Schlüssel bereit. Mit dem Befehl `openssl-vulnkey` können Schlüssel getestet werden. Die folgenden zwei Befehle können verwendet werden, um alle Schlüssel unterhalb von `/etc/univention/ssl` zu testen:

```
find /etc/univention/ssl -name '*key' | xargs -- openssl-vulnkey
find /etc/univention/ssl -name '*pem' | xargs -- openssl-vulnkey
```
- Der Benutzer "Administrator" ist jetzt standardmäßig Mitglied in der Gruppe "Domain Users".
- Das Paket **openvpn-blacklist** stellt eine Blacklist für kompromittierte OpenVPN-Schlüssel zur Verfügung. Mit dem Befehl `openvpn-vulnkey` können Schlüssel getestet werden. Außerdem wurde OpenVPN modifiziert, so dass es mit Servern, die kompromittierte Schlüssel verwenden, keine Verbindung mehr aufbaut.
- Alle Sicherheitsupdates für UCS 2.0 bis einschließlich Update 5 wurden integriert.

4 Univention Managementsystem

- Die Kommandozeilenversionen von Univention Directory Manager und Univention Configuration Registry sind jetzt neben den langen Befehlen `univention-directory-manager` und `univention-config-registry` auch unter den Kurzbefehlen `udm` und `ucr` aufrufbar.
- Im Replikationsmodul kann durch das Setzen der Univention Configuration Registry-Variable `ldap/replication/filesystem/check` eine Überprüfung des freien Festplattenspeichers vorgenommen werden. Sollte der freie Platz kleiner als `ldap/replication/filesystem/limit` (Angabe in Megabytes) sein, so wird die Replikation beendet und es wird eine E-Mail an die in `ldap/replication/filesystem/recipient` gespeicherte Adresse gesendet.
- Das Skript `univention-run-join-scripts` wurde hinzugefügt, welches das Ausführen der Join-Skripte auf der Kommandozeile ermöglicht.
- Die Methode für den Neustart des Verzeichnisdienstes während des Updates wurde so verbessert, dass ein laufender Dienst sicher beendet und neu gestartet wird.
- Freigabecontainer gejointer Rechner werden jetzt automatisch als Standard-Freigabecontainer markiert.
- Univention Configuration Registry-Richtlinien können sich jetzt auch auf Univention Configuration Registry-Variablen beziehen, die Bindestriche oder Unterstriche enthalten. Um dies zu ermöglichen, werden die Univention Configuration Registry-Richtlinien jetzt Base16-kodiert im Verzeichnisdienst gespeichert. Eine Konvertierung findet während des Updates des Pakets **`univention-config-registry`** auf einem DC-Master-System automatisch statt. Die bisherige Kodierung im Verzeichnisdienst bleibt zunächst parallel zu der neuen erhalten, um abhängigen Systemen einen reibungslosen Übergang zu ermöglichen. Dabei ist zu beachten, dass Änderungen an Univention Configuration Registry-Richtlinien nur in der neuen Kodierung geschrieben werden und daher nur von Systemen in der UCS-Domäne ausgewertet werden, auf denen das Releaseupdate auf UCS 2.1 eingespielt wurde. Mit dem Skript `univention-config-registry-policy-encoding` (in `/usr/lib/univention-directory-policy`) können dann, nach dem Releaseupdate aller Systeme in der UCS-Domäne, die alten, noch im LDAP-Verzeichnis gespeicherten Attribute mit der Option `-removeold` entfernt werden.
- Mit der Univention Configuration Registry-Variable `ldap/idletimeout` kann der Timeout für inaktive Verbindungen zum LDAP-Server konfiguriert werden. Mit der Variable `nssldap/idle/timelimit` kann der Timeout der **`libnss`**-Schnittstelle gesetzt werden. Wenn ein Wert für `ldap/idletimeout` gesetzt wird, so sollte ein kleinerer Wert für `nssldap/idle/timelimit` gewählt werden.
- Das LDAP-Attribut **`homeDirectory`** wurde dem LDAP-Index hinzugefügt.
- Die UCS-Domänencontroller haben jetzt die Berechtigung im Verzeichnisdienst Windows-Rechner anzulegen. Mit der Univention Configuration Registry-Variable `ldap/ac1/slavepdc` kann diese Berechtigung gesteuert werden. In der Standardinstellung wird der Zugriff erlaubt.

- Das Paket ***univention-directory-logger*** wurde der Distribution hinzugefügt. Mit diesem Paket können Änderungen im Univention-LDAP-Verzeichnis protokolliert werden.
- Während der Installation des Pakets ***univention-policy-result*** wird das Intervall für die Ausführung des ***policy-result***-Cronjobs wieder gesetzt.

4.1 Univention Directory Manager

- Das Einspielen einer Lizenz kann nun im Univention Directory Manager über den Menüpunkt **Über** vorgenommen werden.
- Das Skript `listpwexpiry` zum Ermitteln von Benutzern mit anstehendem Passwortwechsel wurde dem Paket ***univention-directory-manager-tools*** hinzugefügt.
- Die Handhabung von Umlauten in Benutzernamen und Benutzerpasswörtern wurde auf UTF-8 umgestellt.
- Beim Anlegen neuer Benutzerkonten werden ab sofort nur Benutzernamen zugelassen, die bis auf den ersten Buchstaben kleingeschrieben sind. Für den ersten Buchstaben wird auch weiterhin Großschreibung akzeptiert.
- Ein Tippfehler in dem Skript zum automatischen Aufräumen der Univention Directory Reports, die über das Web-Frontend erstellt worden sind, wurde korrigiert. In der Voreinstellung werden jetzt nächtlich die erstellten Reports gelöscht.
- Mit Univention Directory Reports können jetzt auch Reports im CSV-Format erstellt werden. Für Benutzer, Gruppen und Rechner sind Report-Vorlagen im Lieferumfang enthalten.
- Ein Zugriff auf den Univention Directory Manager über eine ungesicherte Verbindung führt nun zu einem Warnhinweis und erfordert eine gesonderte Bestätigung.
- Es wurde eine neue Option ***Einfaches Authentisierungskonto*** für Benutzer-Objekte hinzugefügt. Diese Benutzer können ausschließlich eine LDAP-Authentisierung durchführen.
- MX-Records und TXT-Records können ab sofort am betreffenden DNS-Forward-Zone-Objekt bearbeitet werden. Die eigenständigen MX- und TXT-Record-Objekte wurden im Univention Directory Manager entfernt.
- Es wurden zwei weitere Optionen für Samba-Freigaben aufgenommen, um Benutzern mit Schreibrechten das Verändern der Zugriffsrechte zu erlauben und um für Benutzer nicht lesbare Dateien und Verzeichnisse zu verstecken.

4.2 Univention Management Console

- Die vorhandenen Module werden in Univention Management Console auf dem Reiter **Übersicht** jetzt mehrzeilig mit maximal 10 Modulen pro Zeile angezeigt.

- Ein Fehler in der Behandlung der Univention Management Console-ACLs wurde behoben, der die Anmeldung an der Univention Management Console verhindern konnte.
- Unter bestimmten Umständen haben sich Univention Management Console-Modulprozesse nicht beendet. Dieser Fehler wurde jetzt behoben.
- Ein Zugriff auf die Univention Management Console über eine ungesicherte HTTP-Verbindung führt nun zu einem Warnhinweis und erfordert eine gesonderte Bestätigung.
- Ein neues Univention Management Console-Modul ermöglicht Administratoren den Neustart und das Herunterfahren des jeweiligen Computersystems über den Webbrowser.
- Die Übersetzung der Univention Management Console wurde überarbeitet.
- Beim Anzeigen von Fehlermeldungen in Univention Management Console wurde unter bestimmten Umständen ein Traceback angezeigt. Dieser Fehler wurde jetzt behoben.

5 Univention Groupware Server

- Beim Öffnen einer E-Mail in KDE Kontakt konnte es bei bestimmten Umständen zu einem Absturz kommen. Dieses Problem wurde behoben.
<https://intevation.de/roundup/kolab/issue2233>
- Das Bearbeiten von Aufgaben in KDE Kontakt konnte zu einem Absturz führen. Dieses Verhalten wurde behoben.
<https://intevation.de/roundup/kolab/issue2286>
- Die automatische Terminannahme bei Ressourcen-Benutzern wurde an PHP5 angepasst.
- Es ist jetzt möglich, gemeinsame IMAP-Ordner mit einer Mailadresse zu versehen. Mails an diese Adresse werden direkt in den IMAP-Ordner zugestellt.
- Ein Fehler bei der Erstellung von gemeinsamen IMAP-Ordnern wurde behoben. Im "user"-Namensraum sind jetzt auch Unterordner möglich.
- Für gemeinsame IMAP-Ordner kann jetzt im Univention Directory Manager die Verwendung als Groupware-Ordner sowie der jeweilige Typ (Mail, Kalender, Kontakte, ...) festgelegt werden.

5.1 Kolab2-Groupware-Webclient Horde

- Der Kolab2-Groupware-Webclient Horde wurde grundlegend überarbeitet und sämtliche Komponenten wurden aktualisiert.

- Der Kolab2-Groupware-Webclient Horde bietet jetzt eine SyncML-Schnittstelle an, mit der die Groupware-Benutzer die Kalender- und die Adressbuch-Einträge mit ihrem Mobiltelefon synchronisieren können. Das Mobiltelefon muss den SyncML-Standard unterstützen.
- Benutzer, die kein Groupware-Konto besitzen, können sich jetzt auch an Horde anmelden. Ihnen steht dort das Webmail-Modul zur Verfügung.
- Die Datenbankberechtigungen wurde so geändert, dass der Benutzer "horde" vollen Zugriff auf die erstellten Horde-Tabellen hat.

5.2 Maildienste

- Die Operation Verschieben wurde für E-Mail-Ordner (**mail/folders**) vorübergehend deaktiviert.
- ClamAV wurde auf Version 0.93.1 aktualisiert. Dies behebt unter anderem eine Inkompatibilität mit aktuellen Viren-Signaturen, die durch eine sehr lange Verarbeitungszeiten die Mail-Auslieferung stören konnte.
- Ein Syntaxfehler in der Konfiguration des Freshclam-Werkzeugs (Teil des Virenscauers Clamav) wurde behoben.

6 Thin Client-Infrastruktur

- Das Thin Client-System wurde grundlegend überarbeitet, u.a. werden nun USB-Devices und Scanner am Thin Client unterstützt. Weitere Hinweise sind im UCS-Handbuch zu finden.

7 Univention Corporate Desktop

- KDE wurde auf Version 3.5.9 aktualisiert.
- Der KDE-Groupwareclient Kontact wurde auf eine aktuelle Version aus dem vom Kolab Konsortium gepflegten Enterprise-Branch aktualisiert.
- OpenOffice.org wurde auf Version 2.4 aktualisiert.
- Firefox wurde auf Version 3 aktualisiert.
- Die Firefox-Startseite wird während des Updates auf http://www.univention.de/ucd-welcome-2_1-0.html gesetzt, sofern die Startseite nicht manuell angepasst wurde.
- Beim Drucken in Firefox wird nicht mehr kprinter verwendet, da die Unterstützung hierfür in Firefox 3 nicht mehr vorhanden ist.

- Das Standard-KDE-Design für UCS 2.0 wurde vom Standard-Profil in das Profil "ucs-green" ausgelagert und für UCS 2.1 steht das neue Design als "ucs-green21" zur Verfügung. Das neue Design wird beim Update automatisch als Richtlinie gesetzt, falls kein anderes Desktop-Design gesetzt ist. Soll ein Benutzer als KDE-Profil-Vorlage verwendet werden, so sollte diesem Benutzer explizit das KDE-Profil "none" zugewiesen werden.
- Falls einem Benutzer kein KDE-Profil zugewiesen ist und der Benutzer sich erstmals am System anmeldet, so wird der KDE-Einrichtungsassistent gestartet.
- Die Konfiguration des grafischen Anmeldemanager GDM wurde grundlegend überarbeitet, u.a. erfolgt beim Starten kein Signalton mehr und der X-Server wird mit der Option `-nolisten tcp` gestartet.
- Das Paket **univention-gdm** hat nun eine Abhängigkeit auf das Paket **univention-gdm-sessions**.
- Die VNC-Desktopfreigabe wird nun über den KDE-eigenen Service zur Verfügung gestellt. Aktiviert wird sie am Arbeitsplatz des Benutzers im KDE-Menupunkt **System** → **Krfb - Arbeitsfläche freigeben**. Über **Einrichten** öffnet sich das **KDE-Kontrollmodul**, wo man **Verbindungen ohne Einladung zulassen** kann. Standardmäßig ist die Option **Für eine uneingeladene Verbindung um Bestätigung bitten** aktiviert, so dass der angemeldete Benutzer bei jedem Zugriff kurz über einen KDE-Dialog um Erlaubnis gebeten wird, auch wenn kein Passwort für die Freigabe eingetragen wurde.
- Durch das Beheben eines Fehlers in der Datei `KDE.Session` werden bei Angabe mehrerer KDE-Desktopprofile diese nun auch der Reihe nach ausgewertet.
- Mit dem neuen KDE-Profil "ucs-kde-menu21" steht ein angepasstes KDE-Menü zur Verfügung. Dieses wird nach dem Update des Paketes **univention-kde** per Desktop-Richtlinie als domänenweiter Standard verwendet. Durch das Setzen der Univention Configuration Registry-Variable `kde/menu/keep` auf den Wert **true** kann dies verhindert werden.

8 Services for Windows/Samba

- Samba wurde auf Version 3.0.30 aktualisiert. Zusätzlich wurden einige Erweiterungen aus der kommenden Samba-Version zurückportiert, u.a. wird nun ein lokaler winbind-Prozess auf einem Samba-PDC unterstützt. Dies wird häufig für Single-Sign-On verwendet.
- Die Samba-Konfigurationsoptionen, bspw. die Passwortlänge oder das maximale Passworalter, werden ab sofort am Samba-Domänenobjekt verwaltet. Vor UCS 2.1 wurden die Einstellungen am Samba-Config-Objekt gespeichert und durch ein Univention Directory Listener-Modul per `pdbedit` in die lokale Samba-Datenbank übertragen. Samba bietet jetzt die Möglichkeit die Einträge direkt aus dem LDAP-Verzeichnis zu lesen, somit werden die Einstellungen, die ab sofort per `pdbedit` geschrieben werden, auch direkt im LDAP-Verzeichnis gespeichert. Eine automatische Konvertierung der Daten erfolgt nicht.

- Samba verwendet jetzt auch LDAP-Server, die in `ldap/server/addition` aufgelistet sind, als `passdb`-Backend.
- Über eine Univention Configuration Registry-Variable kann jetzt der Timeout der LDAP-Verbindung konfiguriert werden.
- Das Joinen von Windows Clients gegen einen Samba-PDC auf einem nicht DC Master wird nun erlaubt.

9 Univention Active Directory Connector

Durch einige der Änderungen/Erweiterungen wurde die Default Mapping-Definition ergänzt bzw. erweitert. Um diese Funktionen bei Updates nutzen zu können, müssen manuell angepasste Mapping-Definitionen entsprechend dem neuen Default erweitert werden.

- Das Mapping zwischen deutschen Standardgruppennamen im AD und englischen in UCS kann jetzt per Univention Configuration Registry (de-)aktiviert werden.
- Der Synchronisations-Modus (`sync`, `read`, `write`) kann jetzt global per Univention Configuration Registry konfiguriert werden.
- Die Synchronisation des Attributs ***description*** ist im Windows 2000-Modus jetzt deaktiviert, kann aber per Univention Configuration Registry aktiviert werden.
- Tracebacks zur Fehlersuche werden jetzt in einer eigenen Log-Datei `connector-tracebacks.log` ausgegeben.
- Fehler bei der Synchronisation von verschachtelten Gruppen wurden beseitigt.
- Einschränkungen bei der Zuordnung von Gruppenmitgliedschaften im initialen Sync und bei der selektiven Synchronisation wurden beseitigt. Um diese Änderung in laufenden Installationen zu nutzen, muss die mapping-Datei angepasst werden.
- Rejects in Gruppenmitgliedschaften während der Erstsynchronisation wurden beseitigt.
- Die Univention Configuration Registry-Variablen wurden für Univention Management Console dokumentiert und beschrieben.
- Der `global_ignore_subtree` wird im Mapping jetzt auch für OUs berücksichtigt.
- Das Verschieben von Objekten aus ignorierten Bereichen im AD in Bereiche zur Synchronisation führt nicht mehr zu Rejects.

10 Linux Kernel und Kernel-Module

- Neben dem Standard-Kernel auf 2.6.18-Basis kann nun auch ein Kernel auf 2.6.24-Basis installiert werden. Dieser bietet keine Unterstützung für den Betrieb als Xen-Wirtssystem (Dom0).

- Mehrere Debian-Kernel-Patches wurden in den Kernel 2.6.18 integriert; neben einigen Fehlerkorrekturen wird dadurch auch Support für neuere Hardware bereitgestellt (AMD/ATI SB700, Intel ICH9, 3ware 9650SE, Intel i965).
- Der im Thin Client-Betrieb verwendete Kernel wurde mit zahlreichen Sicherheits-Updates versehen.
- Die Kernel Module **drbd8** und **squashfs** wurden aktualisiert, so dass diese auch für den 2.6.24er Kernel gebaut werden können.
- Die FSC-Serverview-Module stehen für Kernel 2.6.18 zur Verfügung. Zusätzlich wurden für Kernel 2.6.24 die Kernel-Module angepasst und gebaut. Diese werden aber nicht offiziell von FSC unterstützt. Sobald FSC offizielle Module für Kernel 2.6.24 bereitstellt, wird Univention die Integration prüfen.

11 Weitere Dienste und Pakete

- Die Backuplösung **bacula** wurde zur Distribution hinzugefügt. In zukünftigen UCS-Versionen wird bacula unidump ersetzen.
- Auf der Startseite der auf UCS-Systemen installierten Webserver wird der Verweis auf den DC Master nur dann angezeigt, wenn die Univention Configuration Registry-Variable `ldap/master` gesetzt ist. Der Verweis erfolgt jetzt standardmäßig verschlüsselt (HTTPS).
- Das Paket **shtool** wurde für UCS gebaut.
- Beim Login wird die Standard motd-Meldung von Debian jetzt nicht mehr angezeigt.
- Das Paket **univention-passwd-store** wurde der Distribution hinzugefügt. Nachdem das Paket installiert wurde, können Benutzer die Kommandos `sso-rdesktop` oder `sso-ssh` ohne die erneute Eingabe ihres Passwortes nutzen.
- Bei einigen vom PAM-Stack ausgeführten Skripte wurde ein **exit 0** am Ende der Skripte hinzugefügt, wodurch der Login-Vorgang nicht mehr fälschlicherweise abgebrochen wird.
- Um eine Anmeldung an UCS-Systemen auch mit beendetem `nscd`-Prozess zu ermöglichen, wurde der Konfigurationseintrag **bind_policy** in der Datei `/etc/libnss-ldap.conf` entfernt. Durch das Setzen der Univention Configuration Registry-Variable `nssldap/bindpolicy` kann das alte Verhalten wiederhergestellt werden.
- Das Paket **univention-config-registry** hat ab sofort eine Abhängigkeit auf das Paket **psmisc**.
- Das Programm `univention-security-update` wurde korrigiert, um Kompatibilität mit UCS 2.1 herzustellen.
- Das `rdate`-Startskript ruft nun `ntpdate` zur Zeitsynchronisation auf, falls die Synchronisation über `rdate` nicht erfolgreich war.

- Bei der Aktualisierung des Kernels wird jetzt sichergestellt, dass die initrd-Dateien neu generiert werden, damit der neue Bootsplash verwendet wird.
- Auf einigen Systemen wurde bei der Installation die USB-Tastatur nicht erkannt. Dieses Problem wurde behoben.
- Im Kommandozeilen-Tool `univention-setquota` wurde zwei Syntaxfehler behoben.