univention
be open.

Univention Corporate Server

Handbuch für Benutzer und Administratoren

www.univention.de

Version 4.4-9
Stand: 12. April 2022

Univention GmbH
Mary-Somerville-Straße 1
28359 Bremen
Deutschland
feedback@univention.de

univention
be open.

Inhaltsverzeichnis

Kapitel 1. Einführung

1.1. Was ist Univention Corporate Server?

Feedback

Univention Corporate Server (UCS) ist ein Linux-basiertes Serverbetriebssystem für den Betrieb und die Verwaltung von IT-Infrastruktur in Unternehmen und Behörden. UCS setzt ein durchgängiges Gesamtkonzept mit einheitlicher, zentraler Administration um und kann den Betrieb aller Komponenten in einem zusammenhängenden Sicherheits- und Vertrauenskontext, der so genannten UCS-Domäne, gewährleisten. Gleichzeitig unterstützt UCS viele offene Standards und besitzt umfangreiche Schnittstellen zu Infrastrukturkomponenten und Managementwerkzeugen anderer Hersteller, so dass es sich leicht in vorhandene Umgebungen integrieren lässt.

UCS besteht aus zuverlässiger, in Organisationen unterschiedlicher Größe erprobter Open Source Software. Diese Software wird durch das UCS-Managementsystem zu einem einheitlichen Gesamtsystem integriert. Damit ist das System nicht nur in einfachen, sondern auch in anspruchsvollen, verteilten oder virtualisierten Umgebungen einfach einsetz- und administrierbar.

Dies sind die zentralen Funktionen von UCS:

- Flexibles und umfangreiches Identity- und Infrastrukturmanagementsystem zur zentralen Administration von Servern, Computerarbeitsplätzen, Benutzern und deren Berechtigungen sowie verschiedener Serveranwendungen und Webdienste
- Dienste zur Integration des Managementsystems in vorhandene Microsoft Active Directory Domänen oder auch für die Bereitstellung dieser Dienste als Alternative zu Microsoft-basierten Serversystemen
- App Center zur einfachen Installation und Verwaltung von Erweiterungen und Anwendungen
- Umfassende Funktionen für den Betrieb virtualisierter Rechnersysteme (beispielsweise mit Windows- oder Linux-Betriebssystem) in der Cloud oder direkt auf vorhandenen UCS-Systemen
- Netzwerk- und Intranetdienste zur Verwaltung von DHCP und DNS
- Datei- und Druckdienste
- Rechnerverwaltung und Monitoring
- Maildienste

Diese Funktionen werden von unterschiedlichen Softwarepaketen in Univention Corporate Server bereit gestellt und im Verlauf dieses Handbuchs ausführlich behandelt. Im Wesentlichen lassen sich die in UCS enthaltenen Softwarepakete den folgenden drei Hauptbestandteilen zuordnen:

1. Basissystem

2. UCS-Managementsystem mit Univention Management Console

3. Das App Center, über das sich zahlreiche weitere Komponenten und Anwendungen anderer Hersteller installieren lassen

Das *Basissystem* umfasst das Betriebssystem der auf der Debian GNU/Linux basierenden und von Univention gepflegten UCS-Linux-Distribution. Es beinhaltet weitgehend die selbe Software-Auswahl wie Debian GNU/Linux sowie zusätzliche Werkzeuge zur Installation, zur Aktualisierung und zur Konfiguration von Clients und Servern.

Das *UCS-Managementsystem* realisiert einen Single-Point-of-Administration, über den die Konten aller Domänenmitglieder (Benutzer, Gruppen und Rechner) und Dienste wie DNS und DHCP in einem Verzeichnisdienst verwaltet werden. Kernkomponenten des Managementsystems sind die Dienste OpenLDAP (Verzeichnisdienst), Samba (Bereitstellung von Domänen-, Datei- und Druckdiensten für Microsoft Windows), Kerberos (Authentifizierung und Single-Sign-On), DNS (Namensauflösung im Netzwerk) und SSL/TLS (sichere Datenübertragung zwischen Systemen). Es lässt sich sowohl über eine Webanwendung (Univention Management Console) als auch an der Kommandozeile und in eigenen Skripten verwenden. Das UCS-Managementsystem ist über APIs (*Application Programming Interfaces*) erweiterbar und besitzt eine flexible Client-Server-Architektur, durch die Änderungen auf die davon betroffenen Systeme übertragen und dort aktiviert werden.

Zusätzliche Komponenten von Univention und anderen Herstellern lassen sich bequem über das *App Center* installieren und erweitern das System um zahlreiche Funktionen wie Groupware, Dokumentenmanagement oder Services für Microsoft Windows, so dass sie ebenfalls von einem UCS-System ausgeführt und über das UCS-Managementsystem verwaltet werden können.

1.2. Überblick über UCS

Feedback

Linux ist ein Betriebssystem, bei dessen Entwicklung stets Wert auf Stabilität, Sicherheit und die Kompatibilität zu anderen Betriebssystemen gelegt wurde. Dadurch ist es prädestiniert für den Einsatz als stabiles, sicheres und jederzeit verfügbares Serverbetriebssystem.

UCS ist ein auf dieser Basis aufbauendes Serverbetriebssystem, das besonders für den einfachen und sicheren Betrieb sowie die Verwaltung von Anwendungen und Infrastrukturdiensten in Unternehmen und Behörden optimiert wurde. Zur effizienten und sicheren Verwaltung brauchen solche Anwendungen die mit dem UCS-Managementsystem realisierte enge Integration mit der Benutzer- und Rechteverwaltung.

UCS kann als die Basis für die IT-Infrastruktur von Unternehmen und Behörden eingesetzt werden und dafür die zentrale Steuerung übernehmen. So leistet es einen wichtigen Beitrag für den sicheren, effizienten und wirtschaftlichen IT-Betrieb. Unternehmenskritische Anwendungen sind in ein einheitliches Konzept integriert, aufeinander abgestimmt und für den professionellen Einsatz vorkonfiguriert. Alternativ lässt es sich auch als Bestandteil vorhandener Microsoft-Domänen betreiben.

1.2.1. Inbetriebnahme

Feedback

Der Einsatz von UCS beginnt entweder mit einer klassischen Betriebssysteminstallation auf einem physikalischen Server oder als virtuelle Instanz. Weiterführende Informationen finden sich in Kapitel 2.

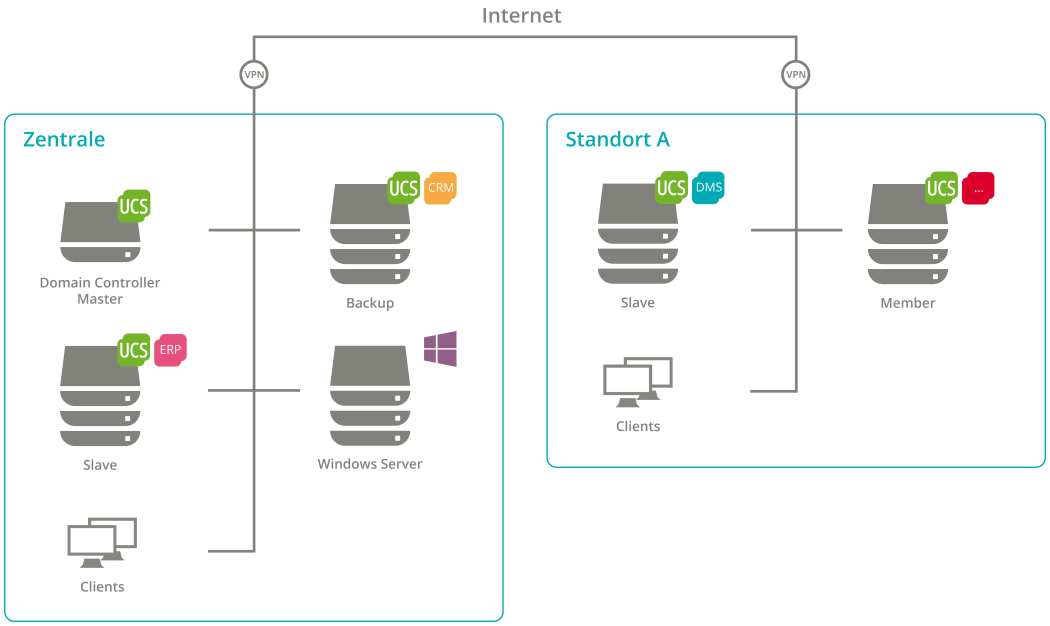
1.2.2. Domänenkonzept

Feedback

In einer mit UCS verwalteten IT-Infrastruktur können sich alle Server, Clients und Benutzer in einem einheitlichen Sicherheits- und Vertrauenskontext, der UCS-Domäne, befinden. Jedem UCS-System wird dazu bei

seiner Installation eine so genannte Systemrolle zugewiesen. Mögliche Systemrollen sind Domänencontroller, Memberserver und Client.

Abbildung 1.1. UCS-Domänenkonzept



Abhängig von der Systemrolle werden neben dem Betriebssystem grundlegende Dienste wie Kerberos, OpenLDAP, Samba, Module für den Domänenreplikationsmechanismus oder eine Root-CA (Zertifizierungsstelle) auf dem Rechner installiert und automatisch für die gewählte Systemrolle konfiguriert. Eine manuelle Einrichtung jedes einzelnen Dienstes oder Anwendung ist deswegen normalerweise nicht notwendig. Durch den modularen Aufbau und umfangreiche Konfigurationsschnittstellen lassen sich dennoch auf individuelle Bedürfnisse zugeschnittene Lösungen umsetzen.

Durch die Integration von Samba, das den Domänendienst für mit Microsoft Windows betriebene Clients und Server bereit stellt, ist Univention Corporate Server kompatibel zu Microsoft Active Directory (AD), so dass sich das System gegenüber Windows-basierten Systemen wie ein Active Directory Server verhält. Deswegen können beispielsweise Gruppenrichtlinien für Microsoft Windows-Systeme auf die gewohnte Art und Weise verwaltet werden.

Zusätzlich kann UCS auch als Teil einer vorhanden Microsoft Active Directory Domäne betrieben werden. Benutzer und Gruppen aus der Active Directory Domäne können dadurch auf Applikationen des Univention App Centers zugreifen.

Ubuntu- oder Mac OS X-Clients können ebenfalls in eine UCS-Umgebung integriert werden (siehe Abschnitt 8.1.1).

1.2.3. Erweiterbarkeit durch das Univention App Center

Das Univention App Center bietet weitere UCS-Komponenten und Erweiterungen sowie eine umfangreiche Auswahl von Softwarelösungen für Business IT-Bereiche wie Groupware, Datenaustausch, CRM oder Backup. Die Anwendungen lassen sich mit wenigen Klicks in bestehende Umgebungen installieren und sind in der Regel einsatzbereit vorkonfiguriert. Sie werden in vielen Fällen direkt in das UCS-Managementsystem integriert und stehen anschließend in der Univention Management Console zur Verfügung. Damit ist eine zentrale Verwaltung von Daten auf Domänenebene gegeben und eine separate Verwaltung, z.B. von Nutzerdaten für unterschiedliche Dienste an unterschiedlichen Orten, entfällt.

1.2.4. LDAP-Verzeichnisdienst

Feedback

Mit dem UCS-Managementsystem können alle Bestandteile der UCS-Domäne über Rechner-, Betriebssystem- und Standortgrenzen hinweg zentral verwaltet werden. Es steht somit ein echter Single-Point-of-Administration für die Domäne zur Verfügung. Ein tragendes Element des UCS-Managementsystems ist ein LDAP-Verzeichnis, in dem die domänenweit benötigten, verwaltungsrelevanten Daten vorgehalten werden. Dort wird neben Benutzerkonten und ähnlichem auch die Datenbasis von Diensten wie DHCP gespeichert. Die zentrale Datenhaltung im LDAP-Verzeichnis erspart nicht nur die wiederholte Eingabe derselben Daten, sondern verringert auch die Wahrscheinlichkeit von Fehlern und Inkonsistenzen.

Ein LDAP-Verzeichnis besitzt eine baumartige Struktur, deren Wurzel die so genannte Basis der UCS-Domäne bildet. Die UCS-Domäne realisiert den gemeinsamen Sicherheits- und Vertrauenskontext für ihre Mitglieder. Bei Benutzern begründet ein Konto im LDAP-Verzeichnis die Mitgliedschaft in der UCS-Domäne. Rechner erhalten bei Beitritt in die Domäne ein Rechnerkonto. Auch Microsoft Windows-Systeme können in die Domäne aufgenommen werden, so dass sich Benutzer dort mit ihrem Domänenpasswort anmelden können.

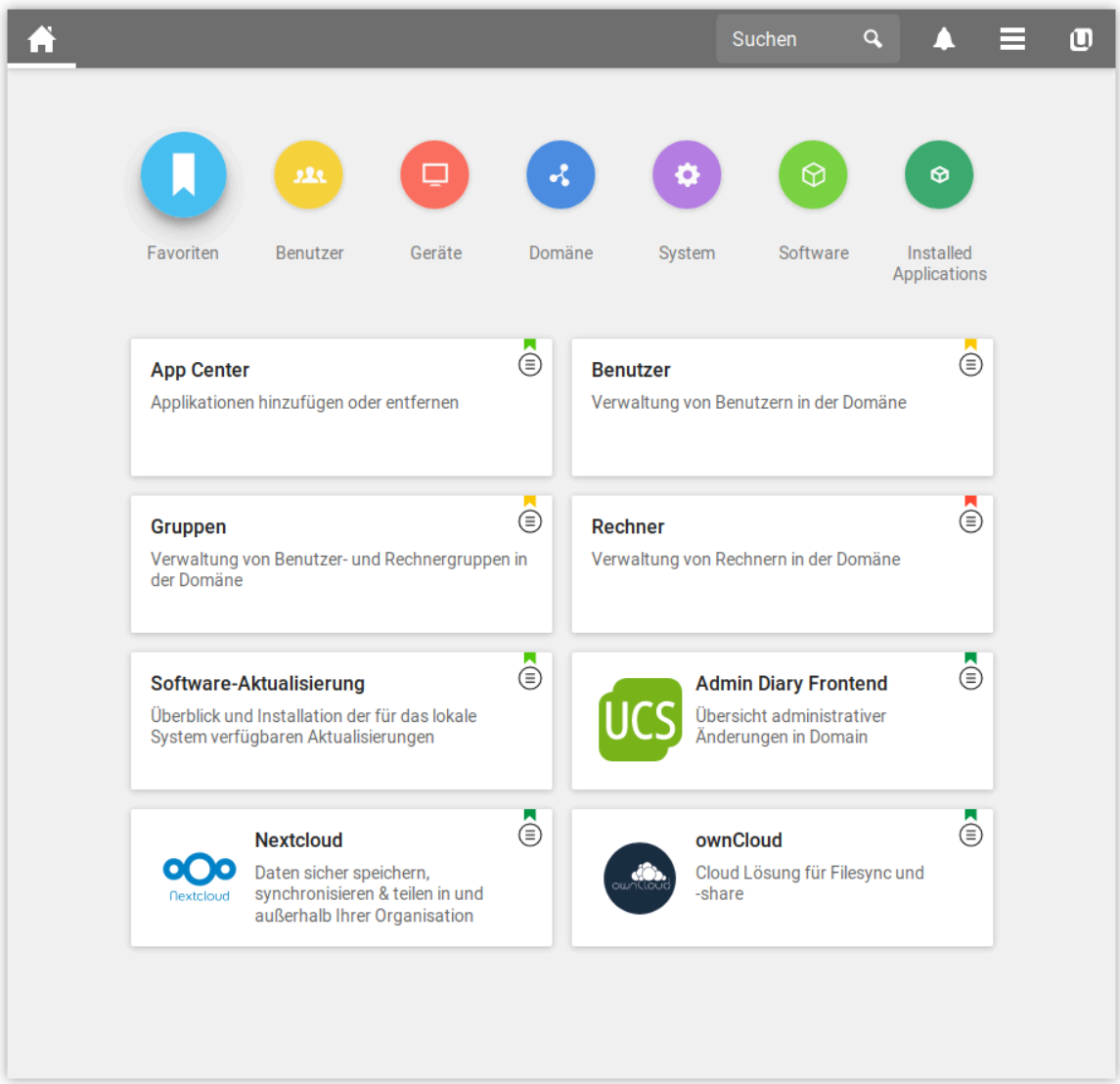
UCS setzt als Verzeichnisdienstserver OpenLDAP ein. Das Verzeichnis wird vom Domänencontroller Master bereitgestellt und auf alle anderen Domänencontroller (DCs) in der Domäne repliziert. Weil ein DC Backup im Notfall den DC Master ersetzen können soll, wird auf diesen immer das komplette LDAP-Verzeichnis repliziert. Die Replikation auf DC Slaves kann dagegen mithilfe von ACLs (Access Control Lists) auf beliebige Bereiche des LDAP-Verzeichnisses beschränkt werden, um eine selektive Replikation zu ermöglichen. Dies kann z.B. dann gewünscht sein, wenn Daten aus Sicherheitsgründen auf möglichst wenigen Servern gespeichert werden sollen. Zur sicheren Kommunikation der Systeme innerhalb der Domäne ist in UCS eine Root-CA (Zertifizierungsstelle) integriert.

Weiterführende Informationen finden sich in Abschnitt 3.4.

1.2.5. Domänenadministration

Feedback

Abbildung 1.2. Univention Management Console



Der Zugang zum LDAP-Verzeichnis erfolgt über die webbasierte Benutzerschnittstelle Univention Management Console (UMC). Daneben ermöglicht Univention Directory Manager auch die Umsetzung aller domänenweiten administrativen Aufgaben über eine Kommandozeilen-Schnittstelle. Dies eignet sich besonders für die Integration in Skripte oder automatisierte administrative Schritte.

Mit Univention Management Console können Daten des LDAP-Verzeichnisses angezeigt, bearbeitet, gelöscht sowie über eine Suche nach unterschiedlichen Kriterien gefiltert werden. Die Web-Oberfläche stellt Assistenten bereit u.a. zur Verwaltung von Benutzern, Gruppen, Netzwerken, Rechnern, Verzeichnisfreigaben und Druckern zur Verfügung. Die Rechnerverwaltung umfasst auch umfangreiche Funktionen zur Verteilung und Aktualisierung von Software. Über den integrierten LDAP-Verzeichnis-Browser können weitergehende Einstellungen vorgenommen sowie kundenspezifische Objektklassen und Attribute hinzugefügt werden.

Weiterführende Informationen finden sich in Kapitel 4.

1.2.6. Rechneradministration

Feedback

Univention Management Console ermöglicht nicht nur den Zugriff auf das LDAP-Verzeichnis, sondern auch die webbasierte Konfiguration und Administration einzelner Rechner. Dazu gehören die Anpassung von Konfigurationsdaten, die Installation von Software sowie die Überwachung und Steuerung von Diensten und dem Betriebssystem an sich. Mit dem UCS-Managementsystem ist die Domänenverwaltung sowie die Rechner-, bzw. Serverkonfiguration von jedem beliebigen Ort aus über eine komfortable, graphische Web-Oberfläche möglich.

1.2.7. Richtlinienkonzept

Feedback

Die baumartige Struktur von LDAP-Verzeichnissen ist ähnlich der eines Dateisystems. Sie stellt sicher, dass Objekte (wie z.B. Benutzer, Rechner etc.) sich in einem Container befinden, der wieder in anderen Containern enthalten sein kann. Der Wurzelcontainer wird auch als LDAP-Basis-Objekt bezeichnet.

Richtlinien beschreiben bestimmte administrative Einstellungen, die auf mehr als ein Objekt angewendet werden können. Sie erleichtern die Administration, weil sie an Container gebunden werden können und dann für alle in dem betreffenden Container befindlichen Objekte, sowie die in Unterordnern befindlichen Objekte gelten.

Beispielsweise können Benutzer nach Abteilungszugehörigkeit in unterschiedliche Container oder Organisationseinheiten (die eine besondere Form von Containern darstellen) organisiert werden. Einstellungen wie Bildschirmhintergrund oder aufrufbare Programme können dann mit Hilfe von Richtlinien an diese Organisationseinheiten gebunden werden und gelten dann für alle unterhalb der betreffenden Organisationseinheit befindlichen Benutzer.

Weiterführende Informationen finden sich in Abschnitt 4.6.

1.2.8. Listener/Notifier-Replikation

Feedback

Ein wichtiger technischer Bestandteil des UCS-Managementsystems stellt der so genannte "Listener/Notifier-Mechanismus" dar. Mit ihm lösen das Anlegen, Verändern oder Löschen von Einträgen im LDAP-Verzeichnis definierte Aktionen auf betroffenen Rechnern aus. So führt zum Beispiel das Anlegen einer Verzeichnisfreigabe mit Univention Management Console dazu, das die Freigabe zunächst in das LDAP-Verzeichnis eingetragen wird. Der Listener/Notifier-Mechanismus stellt dann sicher, dass die Konfigurationsdateien auf dem gewählten Server entsprechend erweitert werden und das Verzeichnis im Dateisystem des gewählten Servers erstellt wird, falls es noch nicht existiert.

Der Listener/Notifier-Mechanismus kann leicht um Module für weitere – auch kundenspezifische – Vorgänge ergänzt werden und wird zum Beispiel von zahlreichen Technologiepartnern für die Integration ihrer Produkte in den LDAP-Verzeichnisdienst und das UCS-Managementsystem verwendet.

Weiterführende Informationen finden sich in Abschnitt 3.5.

1.2.9. Virtualisierungs- und Cloudmanagement

Feedback

Mit dem UMC-Modul UCS Virtual Machine Manager (UVMM) verfügt UCS über ein umfangreiches und mächtiges Werkzeug zur Verwaltung hybrider Cloud-Umgebungen. In der UCS-Domäne registrierte Virtualisierungsserver und darauf betriebene virtuelle Maschinen können zentral überwacht und administriert werden. Zusätzlich bietet UVMM die Möglichkeit virtuelle Maschinen in OpenStack- oder EC2-Umgebungen zu administrieren.

Weiterführende Informationen finden sich in Kapitel 16.

1.3. Weitere Dokumentationen

Feedback

Dieses Handbuch behandelt nur einen kleinen Ausschnitt der Möglichkeiten von UCS. UCS und auf UCS aufbauende Lösungen bieten unter anderem:

- Umfangreiche Unterstützung für komplexe Serverumgebungen und Replikationsszenarien
- Weitergehende Einsatzmöglichkeiten für Microsoft Windows-Umgebungen
- Zentrales Netzmanagement mit DNS und DHCP
- System- und Netzüberwachung mit Nagios
- Druckserver-Funktionalität
- Thin-Client-Support
- Proxy-Server
- Virtualisierung
- Integriertes Backup

Unter [ucs-dokumentationen] und im Univention Wiki unter https://wiki.univention.de/ sind weitere Dokumentationen zu UCS veröffentlicht, die weiterführende Themen behandeln.

1.4. Verwendete Symbole und Konventionen

Feedback

Im Handbuch werden folgende Symbole verwendet:

Achtung

Warnungen werden hervorgehoben.

Anmerkung

Hinweise werden ebenfalls hervorgehoben.

Diese Felder beschreiben den Funktionsumfang eines UMC-Moduls:

Tabelle 1.1. Reiter Nagios-Dienst

Attribut	**Beschreibung**
Name	Ein eindeutiger Name für den Nagios-Dienst.
Beschreibung	Eine beliebige Beschreibung des Dienstes.

Menüeinträge, Schaltflächenbeschriftungen und ähnliches sind **fett** gesetzt. **[Schaltflächenbeschriftungen]** sind zusätzlich durch eckige Klammern gekennzeichnet.

Eigennamen sind *hervorgehoben*.

Computernamen, *LDAP-DNs*, `Programmnamen`, `Dateinamen und -pfade`, `Internetadressen` und *Optionen* werden ebenfalls optisch hervorgehoben.

```
Abschnitte aus Konfigurationsdateien, Bildschirmausgaben usw. sind grau
```

```
hinterlegt.
```

Ein Backslash (\) am Ende einer Zeile weist darauf hin, dass der folgende Zeilenumbruch nicht die Bedeutung eines End-of-Line hat. Das kommt z.B. bei Befehlen vor, die nicht in einer Zeile des Handbuches dargestellt werden können, an der Kommandozeile aber entweder ohne den Backslash in einem Stück oder mit dem Backslash und einem anschließenden Enter eingegeben werden müssen.

Der Weg zu einer Funktion wird ähnlich wie ein Dateipfad dargestellt. **Benutzer -> Hinzufügen** bedeutet beispielsweise, dass im Hauptmenü auf **Benutzer** und im erscheinenden Untermenü auf **Hinzufügen** zu klicken ist.

Kapitel 2. Installation

2.1. Einführung

Feedback

Die folgende Dokumentation beschreibt die Installation von Univention Corporate Server (UCS). Als Installationsmedium wird eine DVD bereitgestellt. Die Installation erfolgt interaktiv und fragt alle notwendigen System-Einstellungen in einer graphischen Oberfläche ab.

Die Installations-DVD wird für die Rechnerarchitektur *amd64* (64 Bit) bereitgestellt. Die DVD bringt neben einer Unterstützung für die weit verbreiteten BIOS-Systeme auch eine Unterstützung für den Unified Extensible Firmware Interface-Standard (UEFI) mit. Die UEFI-Unterstützung auf der DVD ist auch in der Lage, auf Systemen mit aktiviertem SecureBoot zu starten und UCS dort zu installieren.

Neben einer Installation auf Hardware oder in einer Virtualisierungslösung kann UCS auch über ein AMI-Image in der Amazon EC2-Cloud installiert werden. Hinweise dazu finden sich in Abschnitt 2.14.

Die Eingabemasken des Installers können mit der Maus oder über die Tastatur bedient werden:

- Mit der **Tabulator**-Taste kann der Fokus auf das nächste Feld bewegt werden.
- Auf das vorherige Feld wird mit der Tastenkombination **Shift**+**Tabulator** gesprungen.
- Mit der **Eingabe**-Taste werden Werte im Eingabefeld übergeben und Schaltflächen betätigt.
- Innerhalb einer Liste oder Tabelle kann mit den *Pfeiltasten* zwischen den Einträgen gewechselt werden.

Anmerkung

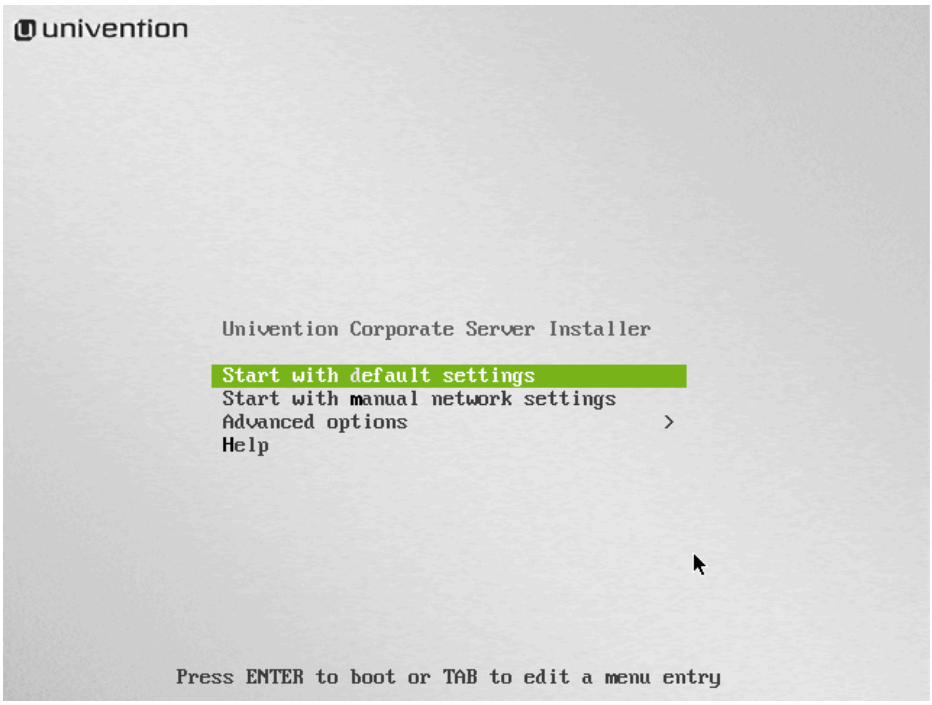
Über die Schaltfläche **Abbrechen** kann der aktuelle Konfigurationsschritt abgebrochen werden. Im anschließend angezeigten Menü kann dann ein vorhergehender Konfigurationsschritt erneut ausgewählt werden. Nachfolgende Konfigurationsschritte sind unter Umständen nicht direkt auswählbar, wenn die vorhergehenden Schritte noch nicht vollständig durchlaufen wurden.

2.2. Auswahl des Installationsmodus

Feedback

Nach dem Starten des Systems vom Installationsmedium erscheint der folgende Bootprompt:

Abbildung 2.1. Bootprompt der Installation



Hier kann zwischen verschiedenen Installationsverfahren gewählt werden.

- **Start with default settings** startet die interaktive, graphische Installation von UCS. Bei der Installation fragt das System nach einigen Parametern wie Netzwerkeinstellungen, Festplattenpartitionierung, Domäneneinstellungen und Komponentenauswahl für das zu installierende UCS-System und führt anschließend die Installation und Konfiguration durch.

- **Start with manual network settings** führt eine Standardinstallation durch, bei der das Netzwerk nicht automatisch per DHCP konfiguriert wird. Dies ist auf Systemen sinnvoll, wo das Netzwerk manuell eingerichtet werden muss.

- Das Untermenü **Advanced options** bietet die Auswahl fortgeschrittener Optionen für den Installationsprozess:

  - **Install in text mode** führt eine interaktive Standardinstallation im Textmodus durch. Dies ist auf Systemen sinnvoll, die Probleme mit der graphischen Variante des Installers zeigen.

  - **Boot from first hard drive** startet nicht die UCS-Installation, sondern das auf der ersten Festplatte installierte Betriebssystem.

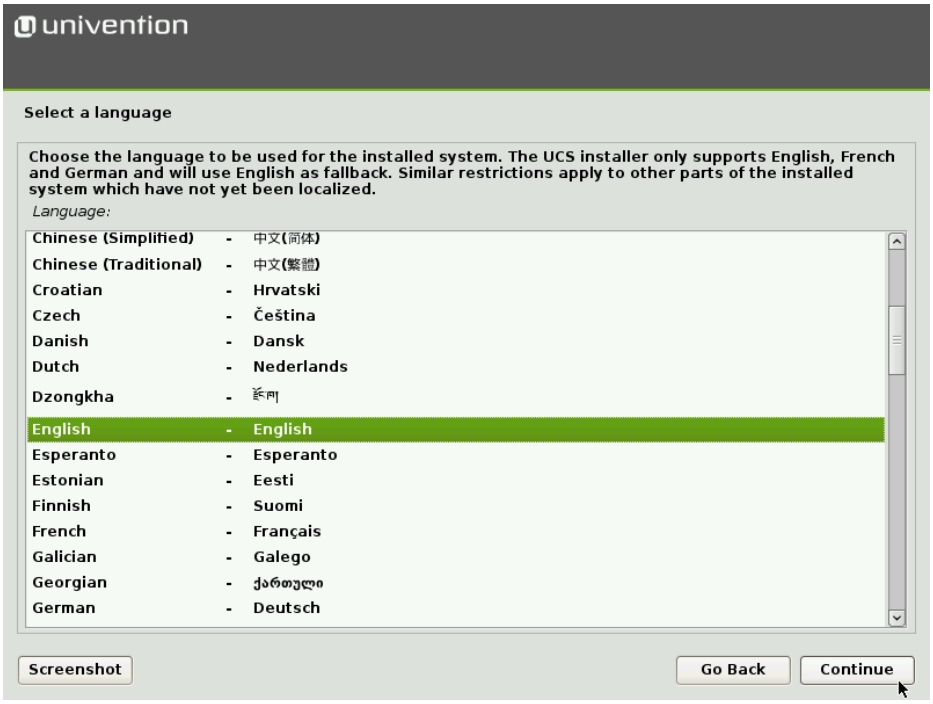
Nach der Auswahl einer der Installationsoptionen wird der Kernel vom Installationsmedium geladen. Die eigentliche Installation gliedert sich in einzelne Module, die bei Bedarf vom Installationsmedium nachgeladen werden. In einem Modul werden inhaltlich zusammenhängende Einstellungen getroffen, es gibt beispielsweise Module für die Netzkonfiguration oder die Auswahl der zu installierenden Software.

2.3. Auswahl der Installationssprache

Feedback

Im ersten Schritt wird die Systemsprache ausgewählt, die verwendet werden soll. Die Auswahl beeinflusst die Verwendung von sprachspezifischen Schriftzeichen und ermöglicht die Darstellung von Programmausgaben in den ausgewählten Sprachen im installierten UCS-System.

Abbildung 2.2. Auswahl der Installationssprache



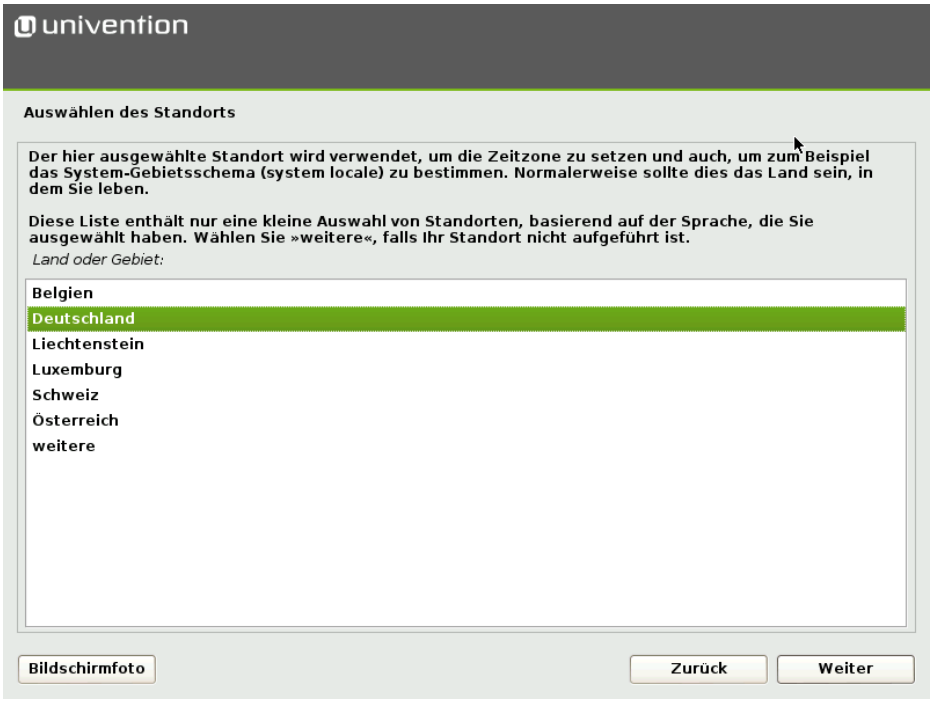
Sofern der Univention Installer die ausgewählte Sprache unterstützt, wird diese als Installationssprache verwendet, andernfalls wird Englisch verwendet. Derzeit sind Deutsch und Englisch vom Univention Installer unterstützt.

2.4. Auswahl des Standorts

Feedback

Nach der Auswahl der Systemsprache wird basierend auf der zuvor ausgewählten Sprache eine kleine Liste mit Standorten angezeigt. Wählen Sie aus der Liste einen passenden Standort aus. Der ausgewählte Standort wird verwendet, um z.B. die Zeitzone zu setzen oder den korrekten Sprachdialekt zu ermitteln. Falls kein angezeigter Standort passend sein sollte, kann über den Menüeintrag **weitere** eine umfangreichere Liste angezeigt werden.

Abbildung 2.3. Auswahl des Standorts

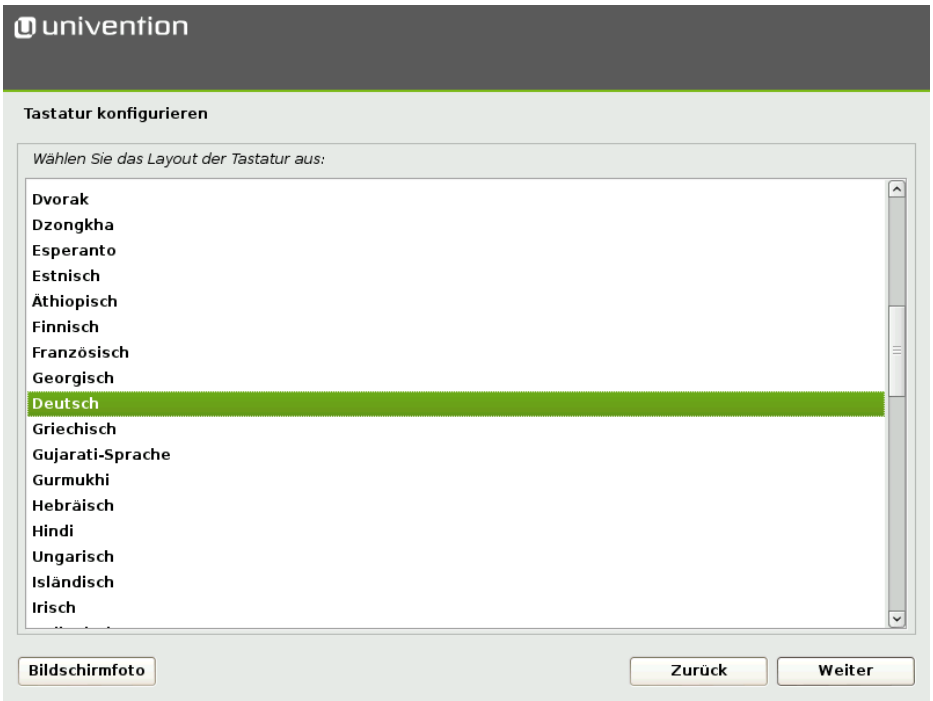


2.5. Auswahl der Tastaturbelegung

Feedback

Unabhängig von der Systemsprache kann ein Tastaturlayout ausgewählt werden. Die hier ausgewählte Sprache sollte zur verwendeten Tastatur passen, das es sonst zu Bedienproblemen kommen kann.

Abbildung 2.4. Auswahl der Tastaturbelegung

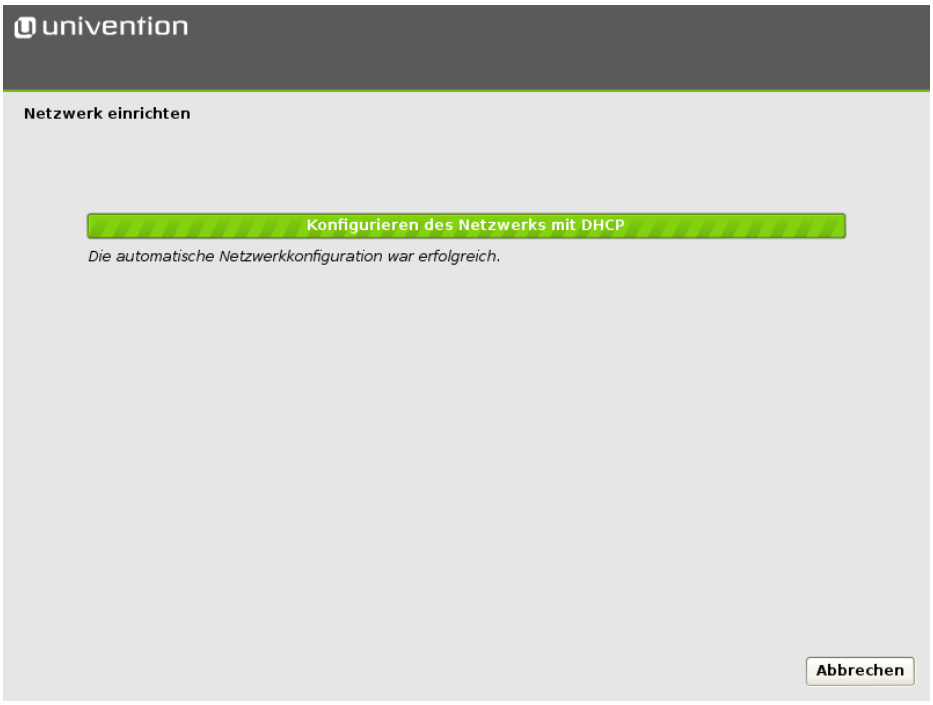


2.6. Netzwerkkonfiguration

Feedback

Initial versucht der Univention Installer eine automatische Konfiguration der Netzwerkschnittstellen vorzunehmen. Dies kann durch die Auswahl des Menüeintrags **Start with manual network settings** im Menü des Bootloaders deaktiviert werden. Dabei wird zunächst versucht, eine IPv6-Adresse über die Stateless Address Autoconfiguration (SLAAC) zu ermitteln. Sollte dies nicht erfolgreich sein, versucht der Univention Installer eine IPv4-Adresse über das Dynamic Host Configuration Protocol (DHCP) zu erfragen. Ist dies erfolgreich, wird die manuelle Netzwerkkonfiguration von Univention Installer übersprungen.

Abbildung 2.5. Automatische Netzwerkkonfiguration

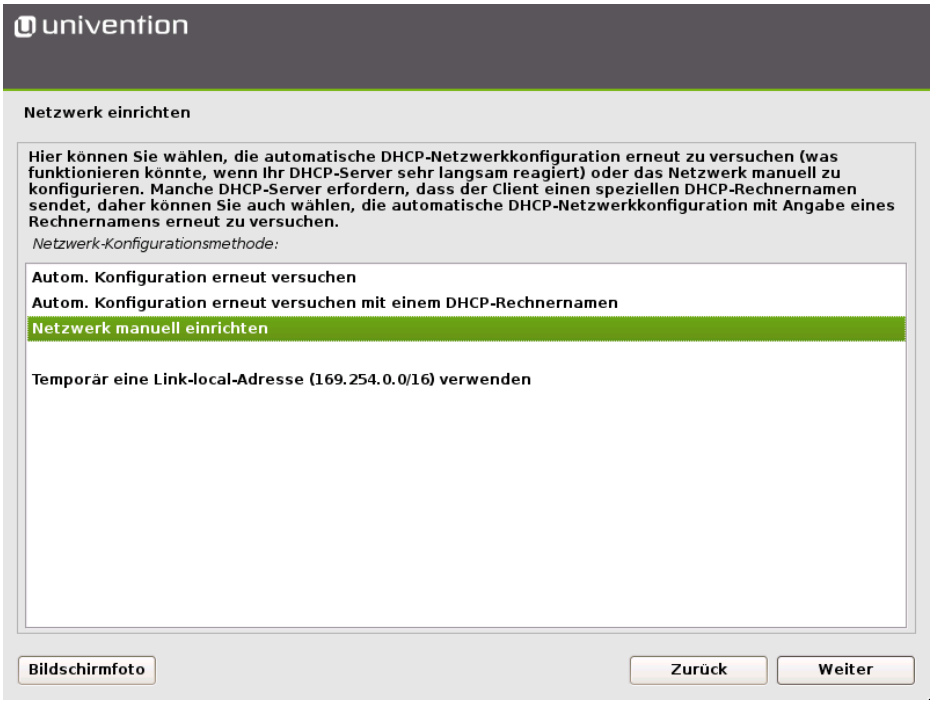


Sollte kein DHCP-Server im lokalen Netz vorhanden sein oder es soll eine statische Konfiguration der Netzwerkschnittstelle stattfinden, kann die Schaltfläche **Abbrechen** ausgewählt werden. Der Univention Installer bietet dann an, die automatische Konfiguration zu wiederholen oder die Schnittstelle manuell zu konfigurieren.

Anmerkung

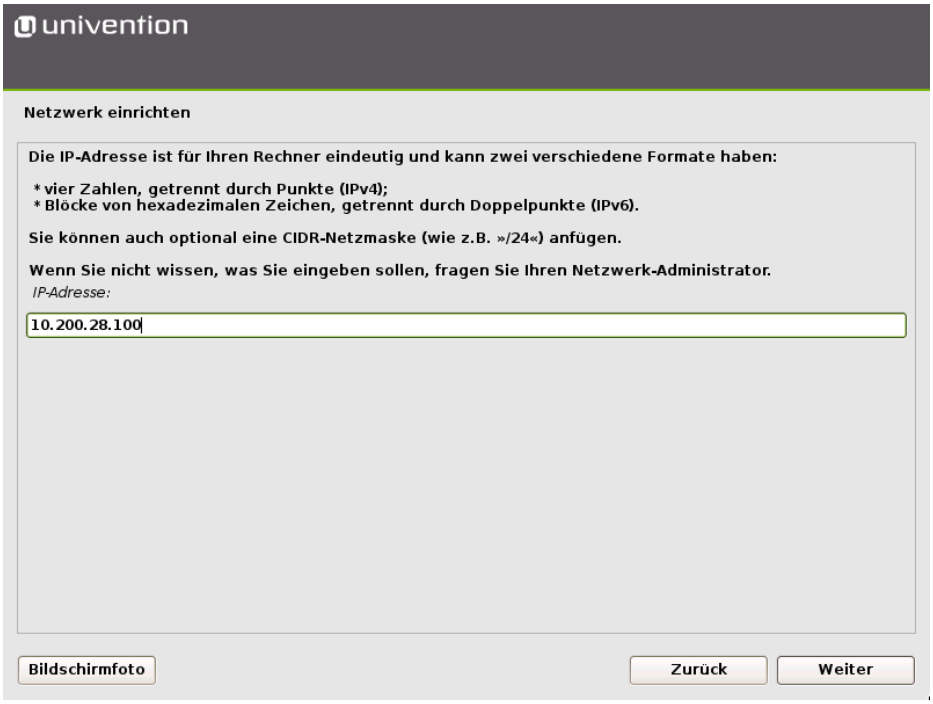
Für die Installation von Univention Corporate Server ist mindestens eine Netzwerkschnittstelle erforderlich. Wird keine unterstützte Netzwerkkarte erkannt, bietet Univention Installer eine Liste der unterstützten Treiber zur Auswahl an.

Abbildung 2.6. Auswahl der manuellen Netzwerkkonfiguration



Bei der manuellen Konfiguration kann für das System wahlweise eine statische IPv4- oder eine IPv6-Adresse angegeben werden. IPv4-Adressen haben 32 Bit Länge und werden in der Regel in vier Blöcken in Dezimalschreibweise dargestellt (z.B. `192.0.2.10`), während IPv6-Adressen vier Mal so lang sind und typischerweise hexadezimal dargestellt werden (z.B. `2001:0DB8:FE29:DE27:0000:0000:0000:000A`). Neben der Angabe einer statischen IP-Adresse werden auch Werte für Netzmaske, Gateway und DNS-Server abgefragt.

Abbildung 2.7. Angabe einer IP-Adresse



Bei der manuellen Angabe eines DNS-Server sind die folgenden Punkte zu beachten. Sie sind abhängig von späteren Verwendungszweck des UCS-Systems.

- Bei der Installation des ersten UCS-Systems einer neuen UCS-Domäne sollte die IP-Adresse des lokalen Routers (sofern dieser den DNS-Dienst bereitstellt) oder der DNS-Server des Internet-Providers angegeben werden.

- Bei der Installation jedes weiteren UCS-Systems muss als DNS-Server die IP-Adresse eines UCS-Domänencontroller-Systems angegeben werden. Dies ist notwendig, damit die automatische Erkennung des Domänencontroller Masters funktioniert. Im Zweifelsfall sollte hier die IP-Adresse des UCS-Domänencontroller Master-Systems angegeben werden.

- Soll das UCS-System während der Installation einer Windows-Active Directory-Domäne beitreten, muss als DNS-Server die IP-Adresse eines Active Directory-Domänencontroller-Systems angegeben werden. Dies ist notwendig, damit die automatische Erkennung des Windows-Active Directory-Domänencontroller funktioniert.

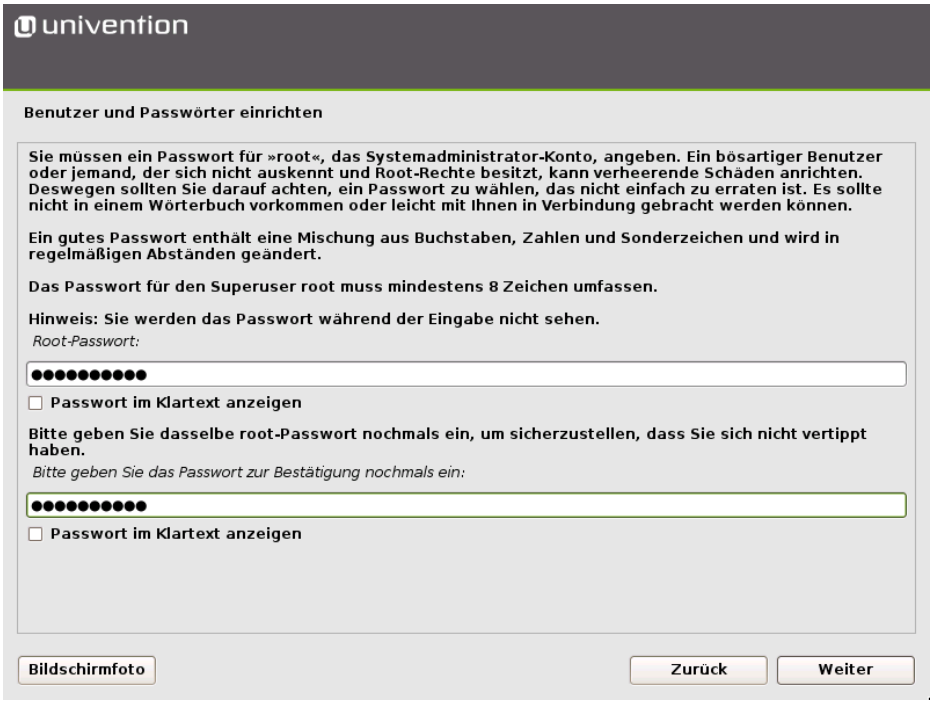
2.7. Einrichtung des root-Passworts

Feedback

Für die Anmeldung am installierten System ist die Angabe eines Passworts für den Benutzer `root` notwendig. Wird ein Domänencontroller Master installiert, wird dieses Passwort auch für den Benutzer `Administrator` eingetragen. Im späteren Betrieb können die Passworte der Benutzer `root` und `Administrator` unabhängig voneinander verwaltet werden. Das Passwort muss im zweiten Feld erneut eingetragen werden.

Das Passwort muss aus Sicherheitsgründen mindestens acht Zeichen umfassen.

Abbildung 2.8. root-Passwort einrichten



2.8. Partitionierung der Festplatten

Feedback

Der Univention Installer unterstützt die Partitionierung von Festplatten und die Erstellung von unterschiedlichen Dateisystemen (u.a. `ext4` und `XFS`). Darüber hinaus können auch Mechanismen wie der Logical Volume Manager (LVM), RAID oder mit LUKS verschlüsselte Partitionen eingerichtet werden.

Ab UCS 4.0 wählt der Univention Installer automatisch einen passenden Partitionstyp (MBR oder GPT) in Abhängigkeit von der Größe der gewählten Festplatte aus. Auf Systemen mit *Unified Extensible Firmware Interface (UEFI)* wird automatisch die GUID Partition Table (GPT) verwendet.

Zur einfacheren Installation bietet der Univention Installer geführte Installationen an. Bei der geführten Installation werden Standardschemata bzgl. Partitionierung und Formatierung auf die ausgewählte Festplatte angewendet. Darüber hinaus kann auch eine manuelle Partitionierung vorgenommen werden.

Es stehen drei Schemata für eine geführte Partitionierung zur Auswahl:

- **Geführt - vollständige Festplatte verwenden**: in diesem Schema wird für jedes Dateisystem eine eigene Partition angelegt. Abstraktionsschichten wie LVM werden nicht verwendet. Im nachfolgenden Schritt wird bestimmt, welche Dateisysteme/Partitionen erstellt werden sollen. Die Größe der Partitionen ist in diesem Schema auf die Größe der jeweiligen Festplatte beschränkt.

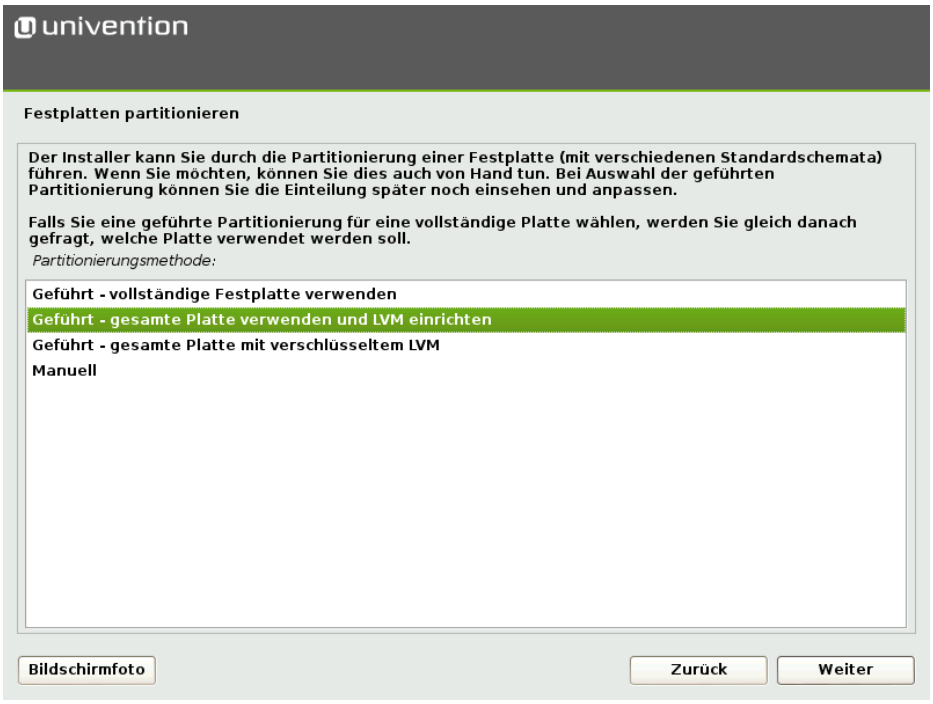
- **Geführt - gesamte Platte verwenden und LVM einrichten**: mit der Auswahl des zweiten Schemas wird auf der ausgewählten Festplatte zunächst eine LVM Volume Group eingerichtet. Anschließend wird für jedes Dateisystem ein eigenes Logical Volume innerhalb der Volume Group angelegt. Die Größe der Logical Volumes ist bei diesem Schema durch die Größe der Volume Group beschränkt, die später auch durch weitere Festplatten vergrößert werden kann. Im Zweifelsfall wählen Sie dieses Partitionierungsschema.

- **Geführt - gesamte Platte mit verschlüsseltem LVM**: diese Variante entspricht der vorherigen Variante, allerdings wird zusätzlich die LVM Volume Group verschlüsselt. Dies macht die Angabe des Passwort für die verschlüsselte Volume Group bei jedem Start von UCS notwendig.

Achtung

Bei allen drei Varianten gehen die Daten auf der ausgewählten Festplatte während der Partitionierung verloren!

Abbildung 2.9. Auswahl des Partitionierungsschemas



Im Anschluss muss aus der Liste der erkannten Festplatte eine ausgewählt werden, auf die die Partitionierungsvariante angewendet werden soll.

Für jede Partitionierungsvariante gibt es drei Untervarianten, die sich in der Anzahl der erstellten Dateisysteme unterscheiden:

- **Alle Dateien auf eine Partition**: Bei dieser Variante wird nur eine Partition bzw. ein Logical Volume erstellt, auf dem das `/`-Dateisystem angelegt wird.
- **Separate /home-Partition**: Neben einem Dateisystem für `/` wird ein weiteres Dateisystem für `/home/` angelegt.
- **Separate /home-, /usr-, /var- und /tmp-Partition**: Neben einem Dateisystem für `/` wird für `/home/`, `/usr/`, `/var/` und `/tmp/` jeweils ein eigenes Dateisystem angelegt.

Vor jeder aktiven Änderung auf der Festplatte wird diese noch einmal in einem zusätzlichen Dialog angezeigt und mit explizit bestätigt werden.

Abbildung 2.10. Bestätigung von Änderungen auf der Festplatte

Nach Abschluss der Partitionierung wird automatisch das UCS-Grundsystem sowie weitere Software installiert. Dies kann je nach Geschwindigkeit der verwendeten Hardware einige Zeit beanspruchen. Nachfolgend wird das System durch die Installation des GRUB-Bootloaders bootfähig gemacht.

2.9. Domäneneinstellungen

Feedback

Die abschließende Konfiguration des UCS-Systems beginnt mit der Auswahl eines Domänenmodus. Es stehen vier Modi zur Verfügung, die Einfluss auf die nächsten Konfigurationsschritte haben:

- Im ersten Modus, **Erstellen einer neuen UCS-Domäne**, wird das erste System einer neuen UCS-Domäne konfiguriert: ein UCS-System mit der Systemrolle *Domänencontroller Master*. In den folgenden Konfigurationsschritten werden die notwendigen Informationen zur Einrichtung eines neuen Verzeichnisdienstes, Authentifikationsdienstes sowie DNS-Servers abgefragt. Eine UCS-Domäne kann aus einem einzelnen oder mehreren UCS-Systemen bestehen. Zusätzliche UCS-Systeme können über den Modus **Einer bestehenden UCS-Domäne beitreten** nachträglich aufgenommen werden.

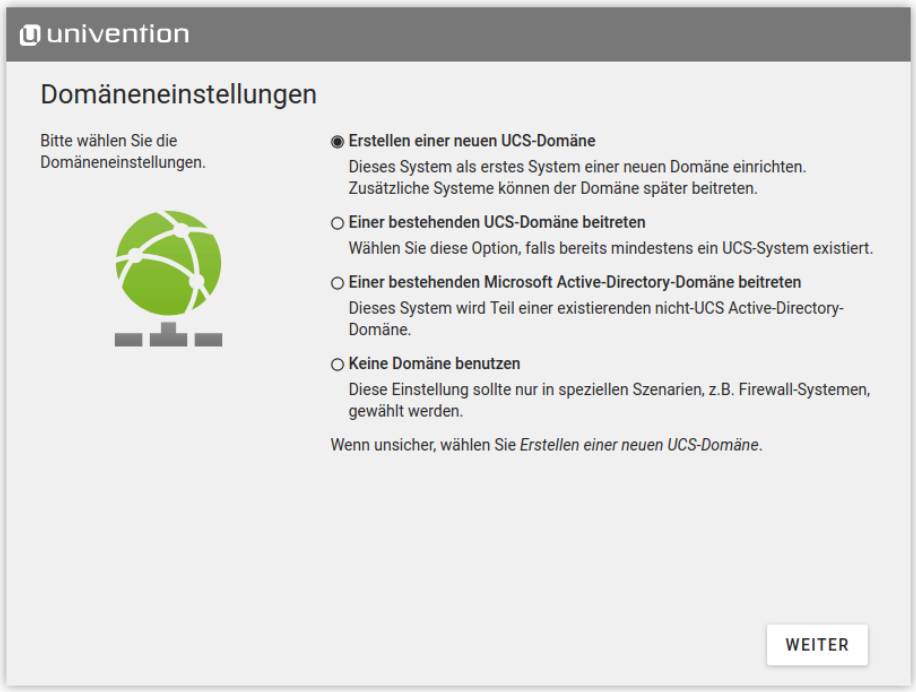
- **Einer bestehenden Active-Directory-Domäne beitreten**: Dieser Modus, in dem UCS als Mitglied einer Active Directory-Domäne betrieben wird, eignet sich, um eine Active Directory-Domäne um Applikationen zu erweitern, die auf der UCS-Plattform zur Verfügung stehen. Auf der UCS-Plattform installierte Apps sind dann für Benutzer der Active Directory-Domäne nutzbar. Nach der Auswahl dieses Modus werden alle relevanten Informationen für den Beitritt zur Active Directory-Domäne abgefragt und das UCS-System entsprechend konfiguriert.

- Mit der Auswahl des Modus **Einer bestehenden UCS-Domäne beitreten** kann das zu konfigurierende UCS-System einer bereits existierenden UCS-Domäne beitreten. Die UCS-Systemrolle, die es in der Domäne einnehmen soll, wird in einem nachgelagerten Schritt abgefragt.

- Wird der Modus **Keine Domäne benutzen** ausgewählt, stehen auf dem UCS-System keinerlei webbasierte Verwaltungsfunktionen und keinerlei Domänenfunktionalität zur Verfügung. Das UCS-System kann auch

nicht nachträglich Teil einer bestehenden UCS- oder Active Directory-Domäne werden bzw. nachträglich eine neue UCS-Domäne gründen. Weiterhin steht in diesem Modus das Univention App Center nicht zur Verfügung. Dieser Modus wird daher nur selten und in speziellen Szenarien (z.B. als Firewall-System) verwendet.

Abbildung 2.11. Domäneneinstellungen



2.9.1. Modus "Erstellen einer neuen UCS-Domäne"

Feedback

Nach der Auswahl des Modus **Erstellen einer neuen UCS-Domäne** wird in den folgenden zwei Schritten ein *Organisationsname*, eine *E-Mail-Adresse*, ein *vollständiger Rechnername* sowie eine *LDAP-Basis* abgefragt.

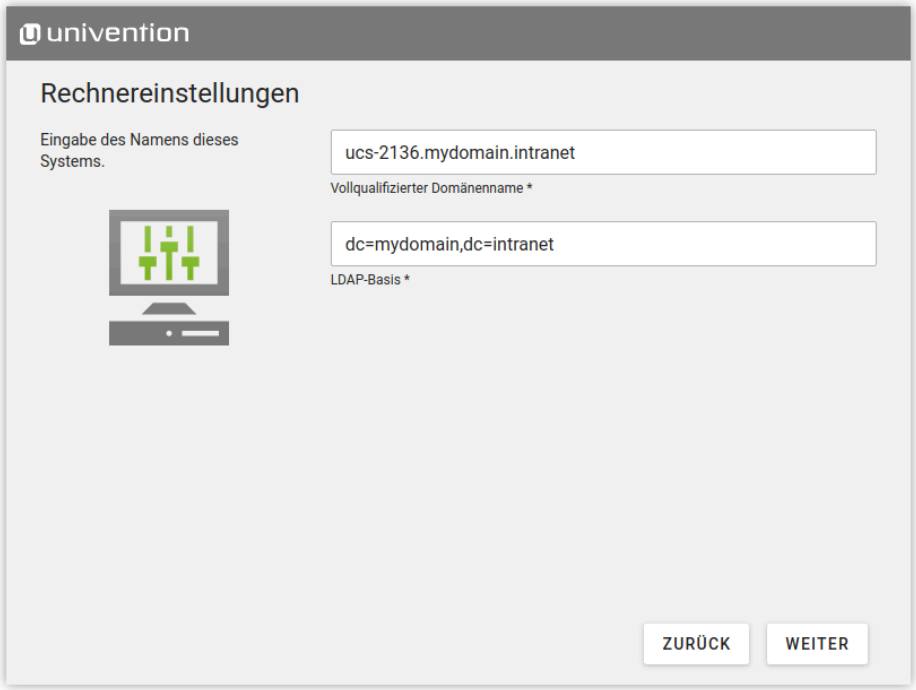
Die Angabe eines Organisationsnamens ist optional und wird im zweiten Schritt für die automatische Generierung eines Domänennamens sowie der LDAP-Basis verwendet.

Wird eine gültige E-Mail-Adresse angegeben, wird diese verwendet, um eine personalisierte Lizenz zu aktivieren, die für die Verwendung des Univention App Centers notwendig ist. Die Lizenz wird automatisch generiert und umgehend an die angegeben E-Mail-Adresse zugeschickt. Die Lizenz kann dann über den Lizenzdialog von Univention Management Console eingespielt werden.

Aus dem hier eingetragenen vollständigen Rechnernamen (ein Rechnername inkl. Domänenname) wird automatisch der Name des zu konfigurierenden UCS-Systems sowie der Name der DNS-Domäne ermittelt. Aus dem im vorigen Schritt angegebenen Organisationsnamen wird automatisch ein Vorschlag generiert. Es wird empfohlen, keine öffentlich verfügbare DNS-Domäne zu verwenden, da dies zu Problemen in der Namensauflösung führen kann.

Für die Initialisierung des Verzeichnisdienstes wird die Angabe einer LDAP-Basis benötigt. Auch hier wird ein Vorschlag automatisch aus dem vollständigen Rechnernamen abgeleitet. In der Regel kann dieser Wert unverändert übernommen werden.

Abbildung 2.12. Angabe des Rechnernamens und der LDAP-Basis



2.9.2. Modus "Einer bestehenden Active-Directory-Domäne beitreten"

Feedback

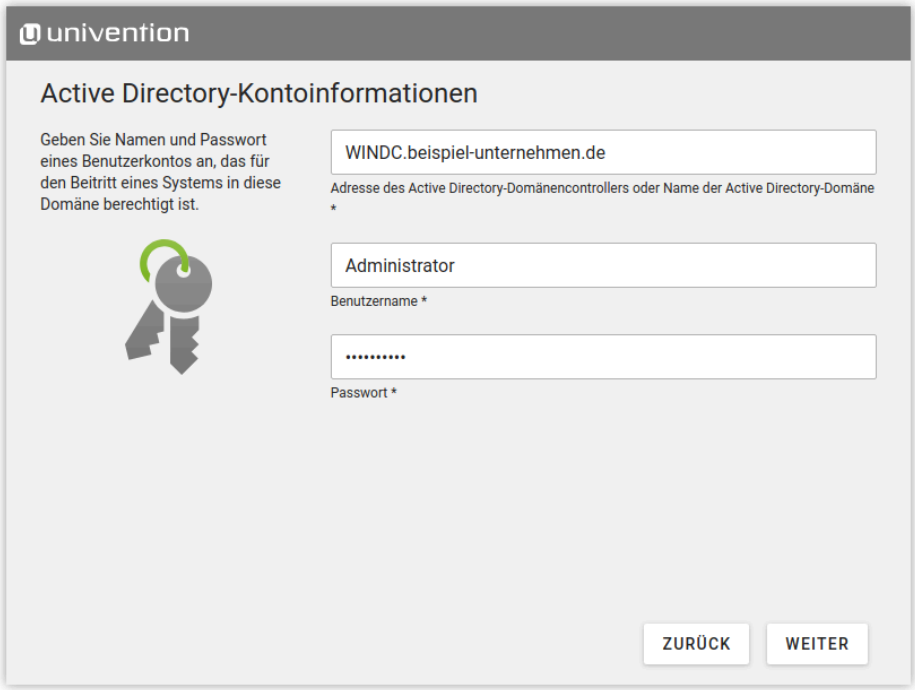
Wurde während der Netzwerkkonfiguration der DNS-Server einer Active-Directory-Domäne angegeben, wird im Schritt **Active Directory-Kontoinformationen** automatisch der Name des Active Directory-Domänencontrollers vorgeschlagen. Falls dieser Vorschlag nicht stimmen sollte, kann hier der Name eines anderen Active Directory-Domänencontrollers bzw. einer anderen Active Directory-Domäne angegeben werden.

Für den Beitritt in die Active Directory-Domäne ist die Angabe eines Active Directory-Kontos sowie des zugehörigen Passworts notwendig. Das Benutzerkonto muss die Berechtigung besitzen, neue Systeme in die Active Directory-Domäne aufzunehmen.

Zusätzlich muss ein Rechnername für das zu konfigurierende UCS-System angegeben werden. Dabei kann der vorgeschlagene Rechnername übernommen oder ein eigener Rechnername eingetragen werden. Der Domänenname des Rechners wird automatisch aus dem Domänen-DNS-Server abgeleitet. In einigen Szenarien (z.B. ein öffentlicher Mailserver) kann es notwendig sein, einen bestimmten vollständigen Rechnernamen zu verwenden. Das UCS-System wird mit dem hier angegebenen Rechnernamen der Active Directory-Domäne beitreten. Der eingerichtete Domänenname kann nach Abschluss der Konfiguration *nicht* mehr verändert werden.

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Das erste UCS-System, das einer Active Directory-Domäne beitritt, wird automatisch mit der Systemrolle Domänencontroller Master konfiguriert. Wird dieser Modus während der Installation eines weiteren UCS-Systems ausgewählt, wird der Dialog zur Auswahl einer Systemrolle angezeigt. Die einzelnen Systemrollen werden im folgenden Abschnitt genauer beschrieben.

Abbildung 2.13. Informationen zum Active Directory-Domänenbeitritt



2.9.3. Modus "Einer bestehenden UCS-Domäne beitreten"

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Das erste System einer UCS-Domäne wird immer mit der Systemrolle Domänencontroller Master installiert. Zusätzliche UCS-Systeme können der Domäne später beitreten und mit einer der folgenden Systemrollen konfiguriert werden:

- **Domänencontroller Backup**

  Der Domänencontroller Backup dient als Fallback-System des DC Master. Sollte dieser ausfallen, kann ein DC Backup die Rolle des DC Master dauerhaft übernehmen. Auf Servern mit der Rolle Domänencontroller Backup werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

- **Domänencontroller Slave**

  Auf Servern mit der Rolle Domänencontroller Slave werden die Domänendaten als Nur-Lese-Kopie gespeichert. Im Gegensatz zum Domänencontroller Backup werden jedoch nicht alle SSL-Sicherheitszertifikate gespeichert. Da die Zugriffe der auf einem Domänencontroller Slave laufenden Dienste gegen den lokalen LDAP-Verzeichnisdienst erfolgen, bieten sich DC Slave-System für Standortserver und für die Verteilung lastintensiver Dienste an.

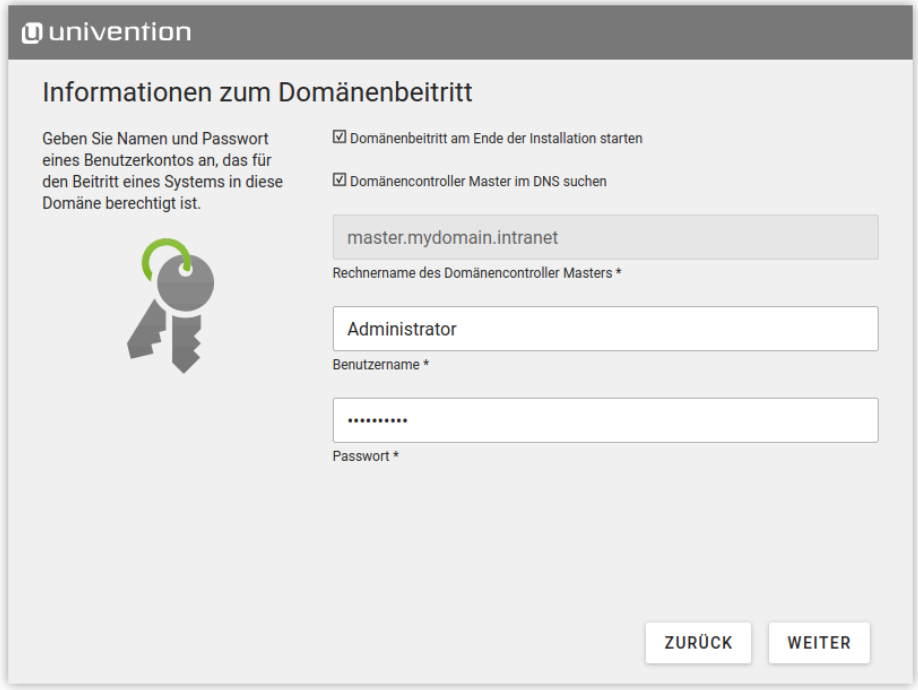
- **Memberserver**

  Memberserver sind Server-Systeme ohne lokalen LDAP-Verzeichnisdienst. Der Zugriff auf Domänendaten erfolgt hierbei über andere Server der Domäne. Sie eignen sich daher für Dienste, die keine lokale Datenbank für z.B. die Authentifizierung benötigen, beispielsweise Druck- und Dateiserver.

Nach der Auswahl der UCS-Systemrolle werden einige Informationen zum Domänenbeitritt abgefragt. Soll der Domänenbeitritt nicht automatisch während der Installation stattfinden, kann die Option **Domänenbeitritt am Ende der Installation starten** deaktiviert werden. Wurde während der Netzwerkkonfiguration der richtige DNS-Server ausgewählt, kann Univention Installer den Namen des Domänencontroller Master-Sys-

tems automatisch bestimmen. Falls doch in eine andere UCS-Domäne gejoined werden soll, kann die Option **Domänencontroller Master im DNS suchen** deaktiviert und der vollständige Rechnername des gewünschten Domänencontroller Master im Eingabefeld darunter eingetragen werden. Die für den Domänenbeitritt notwendigen Zugangsinformationen müssen in die beiden Eingabefelder **Administrator-Kontoinformationen** und **Administrator-Passwort**

Abbildung 2.14. Informationen zum Domänenbeitritt



Im nächsten Schritt muss zusätzlich ein Rechnername für das zu konfigurierende UCS-System angegeben werden. Dabei kann der vorgeschlagene Rechnername übernommen oder ein eigener Rechnername eingetragen werden. Der Domänenname des Rechners wird automatisch aus dem Domänen-DNS-Server abgeleitet. In einigen Szenarien (z.B. ein öffentlicher Mailserver) kann es notwendig sein, einen bestimmten vollständigen Rechnernamen zu verwenden. Der eingerichtete Domänenname kann nach Abschluss der Konfiguration *nicht* mehr verändert werden.

2.9.4. Modus "Keine Domäne benutzen"

Feedback

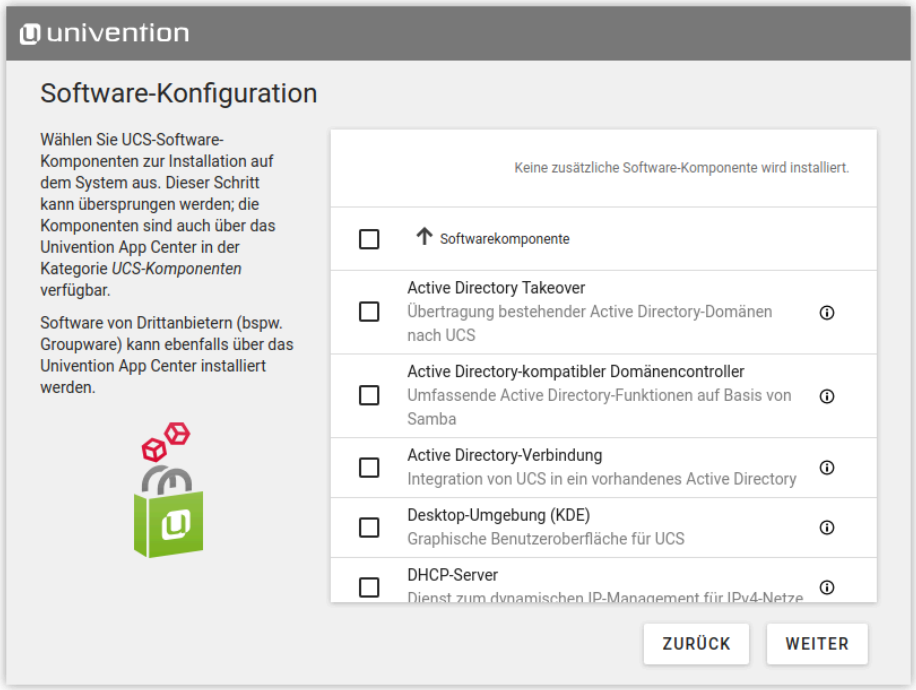
Die Konfiguration des Modus **Keine Domäne benutzen** erfordert die Angabe eines Rechnernamens für das zu konfigurierende UCS-System. Dabei kann der vorgeschlagene Rechnername übernommen oder ein eigener Rechnername eingetragen werden. Der Domänenname des Rechners wird automatisch aus dem Domänen-DNS-Server abgeleitet.

2.10. Auswahl von UCS-Software-Komponenten

Feedback

Der Schritt **Software-Konfiguration** bietet die Möglichkeit bereits während der Installation zusätzliche UCS-Komponenten zu installieren. Diese stehen auch nach der Installation über das Univention App Center in der Kategorie **UCS-Komponenten** zur Verfügung und können dort nachträglich installiert und deinstalliert werden.

Abbildung 2.15. Auswahl von UCS-Software-Komponenten



2.11. Bestätigen der Einstellungen

Feedback

In diesem Dialog werden die wichtigsten vorgenommenen Einstellungen angezeigt. Sind alle Einstellungen korrekt, kann über die Schaltfläche **System konfigurieren** die Konfiguration des UCS-Systems veranlasst werden, siehe Abbildung 2.16.

Mit der Option **System nach der Installation aktualisieren** werden verfügbare Errata-Updates automatisch installiert. Zusätzlich werden auf einem Domänencontroller Master alle verfügbaren Patch-Level-Updates und Errata-Updates installiert. Auf allen übrigen Systemrollen werden alle Patch-Level-Updates bis zum Installationsstand des Domänencontroller Master eingerichtet. (Um den Installationsstand zu prüfen, muss ein Login auf dem Domänencontroller Master erfolgen. Dazu werden die in den Join-Optionen angegebenen Anmeldedaten verwendet).

Abbildung 2.16. Installationsüberblick

Während der Konfiguration zeigt ein Fortschrittsbalken den Verlauf der Installation an.

Das Installationsprotokoll des Univention Installers wird in den folgenden Dateien abgelegt:

- `/var/log/installer/syslog`
- `/var/log/univention/management-console-module-setup.log`

Der Abschluss der Konfiguration muss über die Schaltfläche **Fertigstellen** bestätigt werden. Das UCS-System wird anschließend auf den ersten Bootvorgang vorbereitet und neugestartet.

Das System startet nun von Festplatte. Nach dem Bootvorgang können sich die Benutzer `root` und `Administrator` beim Web-Frontend Univention Management Console anmelden (siehe Kapitel 4), welche unter der während der Installation gesetzten IP-Adresse bzw. unter dem Rechnernamen erreichbar ist.

Wenn der Rechner als erstes System der UCS-Domäne (Domänencontroller Master) installiert wurde, kann nun die Lizenz eingespielt werden (siehe Abschnitt 4.4.2).

2.12. Fehlersuche bei Installationsproblemen

Feedback

Hinweise zu eventuellen Installationsproblemen finden sich in der Univention Support Datenbank unter http://sdb.univention.de im Unterpunkt *Installation*.

2.13. Installation im Textmodus

Feedback

Auf Systemen, die Probleme mit der graphischen Variante des Installers zeigen, kann der Installer auch im Textmodus gestartet werden. Im DVD-Bootmenu **Advanced options** muss dafür der Eintrag **Install in text mode** ausgewählt werden.

Während der Installation im Textmodus werden die gleichen Informationen wie im graphischen Installer angezeigt bzw. abgefragt. Jedoch wird nach der Partitionierung der Festplatten das System auf den ersten Neustart vorbereitet und schließlich neu gestartet.

Nach Abschluss des Neustarts kann die Konfiguration im Webbrowser fortgesetzt werden. Dafür muss im Browser die URL `https://SERVER-IP-ADRESSE` oder `http://SERVER-IP-ADRESSE` aufgerufen werden (HTTPS wird empfohlen). Nach dem Aufruf der Seite ist die Anmeldung mit dem Benutzer `root` erforderlich.

Die Konfiguration im Browser erfragt den Standort sowie die Netzwerkeinstellungen und fährt dann (wie in der graphischen Installation) mit dem Punkt *Domäneneinstellungen* fort.

2.14. Installation in der Amazon EC2-Cloud

Feedback

Univention stellt für UCS ein Amazon Machine Image (AMI) für die Amazon EC2 Cloud bereit. Aus diesem generischen Image für alle UCS-Systemrollen wird eine eigene Instanz abgeleitet, die über Univention Management Console konfiguriert wird (Domänenname, Softwareauswahl etc.).

Die Einrichtung einer UCS-Instanz auf Basis von Amazon EC2 ist im Univention Wiki dokumentiert [ec2-quickstart].

2.15. Installation in VMware

Feedback

Wird UCS als Gast in VMware installiert muss als **Gastbetriebssystem** die Option **Linux -> Anderes Linux-System** ausgewählt werden (UCS basiert zwar auf Debian, die Vorlagen für Debian können aber nicht verwendet werden).

Der in UCS verwendete Linux-Kernel bringt alle nötigen Unterstützungstreiber für den Betrieb in VMware direkt mit (`vmw_balloon`, `vmw_pvsci`, `vmw_vmci`, `vmwgfx` und `vmxnet3`).

Die Open-Source-Variante der VMware Tools (Open VM Tools) wird mit UCS ausgeliefert. Die Tools können über das Paket ***open-vm-tools*** installiert werden (sie sind nicht zwingend notwendig, erlauben aber z.B. die Synchronisation der Zeit auf dem Gastsystem mit dem Virtualisierungsserver).

2.16. Installation als Docker Image

Feedback

Univention stellt UCS als Docker Images im Docker Hub bereit https://hub.docker.com/r/univention/. In der Beschreibung der jeweiligen Docker Images ist erklärt, wie diese in Betrieb genommen werden können.

Die Docker Images werden bei einer Standardinstallation in einem Netzwerk betrieben, welches von außerhalb des Servers nicht direkt erreicht werden kann. Sofern mehrere Docker Images eingesetzt werden und diese auf unterschiedlichen Docker Servern betrieben werden, sollte entsprechend ein *Software Defined Network* oder eine VPN Lösung eingesetzt werden.

2.17. Installation in Citrix XenServer

Feedback

Die Einrichtung einer UCS-Instanz in Citrix XenServer ist im Univention Wiki dokumentiert [xenserver-installation].

univention
be open.

Kapitel 3. Domänendienste / LDAP-Verzeichnisdienst

3.1. Einführung

Feedback

Univention Corporate Server bietet ein plattformübergreifendes Domänenkonzept mit einem gemeinsamen Vertrauenskontext zwischen Linux- und Windows-Systemen. Innerhalb dieser Domäne ist ein Benutzer mit seinem im UCS-Managementsystem hinterlegten Benutzernamen und Passwort auf allen Systemen bekannt, und kann für ihn freigeschaltete Dienste nutzen. Das Konto wird über das Managementsystem sowohl für die Windows-Anmeldung als auch für Linux/POSIX-Systeme und Kerberos synchron gehalten. Die Verwaltung von Benutzerkonten ist in Kapitel 6 beschrieben.

Alle UCS- und Windowssysteme innerhalb einer UCS-Domäne verfügen über ein Domänenkonto, sobald sie der UCS-Domäne beigetreten sind. Der Domänenbeitritt wird in Abschnitt 3.2 beschrieben.

Jedes Rechnersystem, das Mitglied einer UCS-Domäne ist, besitzt eine Systemrolle. Aus dieser Systemrolle ergeben sich verschiedene Berechtigungen und Einschränkungen, die in Abschnitt 3.3 beschrieben sind.

Auf dem Domänencontroller Master wird die Certificate Authority (CA) der UCS-Domäne betrieben. Dort wird für jedes der Domäne beigetretene System ein SSL-Zertifikat generiert. Weitere Informationen finden sich in Abschnitt 3.6.

Alle domänenweiten Einstellungen werden in einem Verzeichnisdienst auf Basis von OpenLDAP vorgehalten. In Abschnitt 3.4 wird beschrieben wie der Speicherumfang durch LDAP-Schema-Erweiterungen ergänzt werden kann, wie eine revisionssichere LDAP-Protokollierung eingerichtet werden kann und wie Zugriffsberechtigungen auf das LDAP-Verzeichnis definiert werden können.

Die Replikation der Verzeichnisdaten innerhalb einer UCS-Domäne erfolgt über den Listener/Notifier-Mechanismus. Weitere Informationen finden sich in Abschnitt 3.5.

Kerberos ist ein Authentikationsverfahren um in verteilten Netzen über potentiell unsichere Verbindungen eine sichere Identifikation zu erlauben. Jede UCS-Domäne betreibt einen eigenen Kerberosvertrauenskontext (Realm). Weitere Informationen finden sich in Abschnitt 3.7

3.2. Domänenbeitritt

Feedback

Ein UCS, Ubuntu- oder Windows-System muss nach der Installation der Domäne beitreten. Im Folgenden werden die verschiedenen Möglichkeiten hierzu vorgestellt.

Neben UCS, Ubuntu und Mac OS X können auch weitere Unix-Systeme in die Domäne integriert werden; dies ist in [ext-doc-domain] beschrieben.

3.2.1. Domänenbeitritt von UCS-Systemen

Feedback

Es gibt drei Möglichkeiten ein UCS-System einer bestehenden Domäne beitreten zu lassen; direkt am Ende der Installation im Univention Installer (siehe Abschnitt 2.9.3) oder nachträglich durch den Befehl `univention-join` bzw. mit Univention Management Console.

Der Domänencontroller Master sollte immer auf dem aktuellsten Release-Stand der Domäne installiert sein, da beim Join eines Systems in aktuellerer Version gegen einen älteren DC Master Probleme auftreten können.

Beim Beitritt eines Rechners wird für diesen ein Rechnerkonto angelegt, die SSL-Zertifikate synchronisiert und ggf. eine LDAP-Replikation angestoßen. Außerdem werden am Ende des Join-Vorgangs *Join-Skripte* ausgeführt. Diese registrieren anhand der auf dem System installierten Software-Pakete z.B. weitere Objekte im Verzeichnisdienst (siehe Abschnitt 3.2.1.3).

Der Domänenbeitritt wird auf Client-Seite in der Logdatei `/var/log/univention/join.log` aufgezeichnet, die zur Fehleranalyse herangezogen werden kann. Auf dem Domänencontroller Master ausgeführte Aktionen werden in der Logdatei `/home/Join-Account/.univention-server-join.log` abgelegt.

Der Join-Vorgang kann jederzeit wiederholt werden. Nach bestimmten administrativen Schritten (etwa nach Änderungen wichtiger Systemeigenschaften auf dem Domänencontroller Master) kann ein erneuter Beitritt der Systeme sogar zwingend erforderlich sein.

3.2.1.1. Nachträglicher Domänenbeitritt mit `univention-join`

Feedback

`univention-join` fragt eine Reihe essentieller Parameter direkt ab, ist aber auch durch mehrere Parameter konfigurierbar:

- Der Domänencontroller Master wird im Regelfall durch eine DNS-Abfrage ermittelt. Wenn das nicht möglich sein sollte (z.B. weil ein Standortserver mit einer abweichenden DNS-Domäne beitreten soll), lässt sich der Rechnername des DC Master auch durch den Parameter `-dcname` *`HOSTNAME`* direkt angegeben werden. Der Rechnername muss dabei als vollqualifizierter Name angeben werden, also beispielsweise `master.firma.de`.

- Als Join-Account wird ein Benutzerkonto bezeichnet, das berechtigt ist, Systeme der UCS-Domäne hinzuzufügen. Standardmäßig ist dies der Benutzer `Administrator` oder ein Mitglied der beiden Gruppen `Domain Admins` und `DC Backup Hosts`. Der Join-Account kann durch den Parameter `-dcaccount` *`ACCOUNTNAME`* übergeben werden.

- Das Passwort kann durch den Parameter `-dcpwd` *`DATEI`* übergeben werden. Das Passwort wird dabei aus der angegebenen Datei ausgelesen.

- Mit dem Parameter `-verbose` werden zusätzliche Debugausgaben in die Logdateien geschrieben, die die Analyse im Fehlerfall vereinfachen.

3.2.1.2. Domänenbeitritt mit Univention Management Console

Feedback

Der Domänenbeitritt kann auch webbasiert über das UMC-Modul **Domänenbeitritt** erfolgen. Da auf einem noch nicht der Domäne beigetretenen System der Administrator-Benutzer noch nicht vorhanden ist, muss die Anmeldung an Univention Management Console als Benutzer `root` erfolgen.

Wie bei der Durchführung über die Kommandozeile sind für Domänenbeitritt Benutzername und Passwort eines Benutzers notwendig, der berechtigt ist, Rechner der Domäne hinzuzufügen. Ebenfalls wird der Domänencontroller Master über eine DNS-Abfrage automatisch ermittelt, kann aber auch explizit im angezeigten Dialogfeld eingetragen werden.

Mit der Option **Erneut beitreten** kann der Domänenbeitritt jederzeit erneut durchgeführt werden.

3.2.1.3. Join-Skripte / Unjoin-Skripte

Feedback

Join-Skripte werden während des Domänenbeitritts aufgerufen. Beispiele für von Join-Skripten vorgenommene Änderungen sind die Registrierung eines Druckservers in der Domäne oder die Anpassung von DNS-

Einträgen. Die Skripte sind Bestandteil der einzelnen Softwarepakete. Analog dazu gibt es *Unjoin-Skripte*, die nach der Deinstallation einer Softwarekomponente diese Änderungen wieder rückgängig machen.

Join-Skripte werden im Verzeichnis `/usr/lib/univention-install/` und Unjoin-Skripte in `/usr/lib/univention-uninstall/` gespeichert. Jedes Join/Unjoin-Skript verfügt über eine Version. Ein Beispiel: Ein Paket ist bereits installiert und das Join-Skript schon aufgerufen. In der neuen Version des Pakets sind nun zusätzliche Änderungen nötig und die Versionsnummer des Join-Skripts wird erhöht.

Mit dem Befehl `univention-check-join-status` kann geprüft werden, ob Join- oder Unjoin-Skripte aufgerufen werden müssen (entweder weil sie noch nie oder in einer älteren Version aufgerufen wurde).

3.2.1.3.1. Nachträgliches Ausführen von Join-/Unjoin-Skripten

Feedback

Gibt es auf einem System Join- oder Unjoin-Skripte, die noch nicht ausgeführt wurden oder die nur für eine ältere Version ausgeführt wurden, wird bei der Anmeldung an Univention Management Console eine Warnmeldung ausgegeben.

Nicht ausgeführte Join-Skripte können über das UMC-Modul **Domänenbeitritt** aufgerufen werden, in dem der Menüpunkt **Alle Skripte ausführen** aufgerufen wird.

Mit dem Befehl `univention-run-join-scripts` lassen sich alle auf einem System installierten Join-/Unjoin-Skripte ausführen. Ob sie bereits gestartet wurden, prüfen die Skripte selbständig.

Der Name des Join/Unjoin-Skripts und die Skriptausgabe werden auch in `/var/log/univention/join.log` festgehalten.

Wird `univention-run-join-scripts` auf einer anderen Systemrolle als Domänencontroller Master ausgeführt, so wird der Benutzer nach einem Benutzernamen und einem Passwort gefragt. Auf dem Domänencontroller Master kann dies durch die Option `--ask-pass` erreicht werden.

3.2.2. Windows-Domänenbeitritt

Feedback

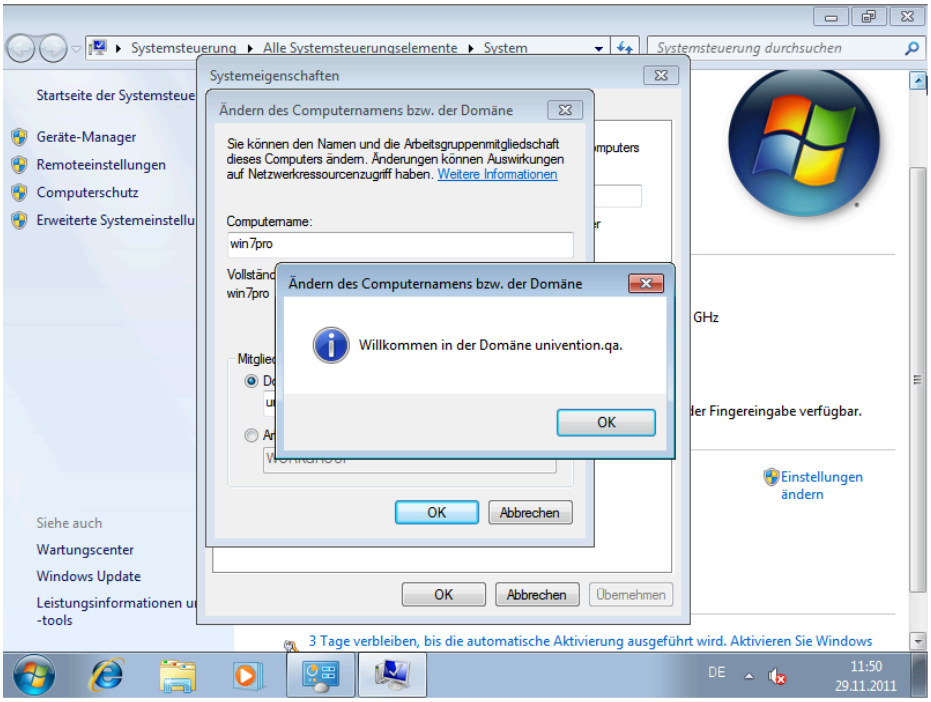
Der Domänenbeitritt von Microsoft Windows-Systemen zu einer durch Samba bereitgestellten UCS-Domäne wird nachfolgend für Windows 7/8/10 und Windows 2012 beispielhaft beschrieben. Bei anderen Windows-Versionen funktioniert der Beitritt ähnlich. Neben den Client-Versionen können auch Windows Server-Systeme der Domäne beitreten. Windows-Server treten der Domäne als Memberserver bei, ein Beitritt eines Windows-Systems als Domänencontroller wird nicht unterstützt. Weitere Hinweise finden sich in Abschnitt 9.1.

Nur domänenfähige Windows-Versionen können der UCS-Domäne beitreten, d.h. ein Domänenbeitritt mit den Home-Versionen von Windows ist nicht möglich.

Beim Domänenbeitritt wird automatisch ein Rechnerkonto für den Windows-Client erstellt (siehe Abschnitt 8.1). Angaben zu MAC- und IP-Adresse, Netzwerk, DHCP oder DNS können vor oder nach dem Domänenbeitritt in Univention Management Console ergänzt werden.

Der Domänenbeitritt wird in der Regel mit dem lokalen Administrator-Konto des Windows-Systems durchgeführt.

Abbildung 3.1. Domänenbeitritt eines Windows 7-Systems



Der Domänenbeitritt dauert einige Zeit und sollte nicht vorzeitig abgebrochen werden. Nach einem erfolgreichen Beitritt erscheint ein kleines Fenster mit der Nachricht **Willkommen in der Domäne *`Domänenname`***, die mit **[OK]** bestätigt werden muss. Abschließend muss der Rechner neu gestartet werden, um die Änderungen in Kraft zu setzen.

Domänennamen sollten auf 13 Zeichen beschränkt werden, da diese auf Seite der Windows-Clients ansonsten verkürzt dargestellt werden, was zu Anmeldefehlern führen kann.

Bei einem Domänenbeitritt gegen einen Domänencontroller auf Basis von Samba 4 muss die DNS-Konfiguration des Clients so eingerichtet sein, dass DNS-Einträge aus der DNS-Zone der UCS-Domäne aufgelöst werden können. Außerdem muss die Zeit auf dem Client-System mit der Zeit auf dem Domänencontroller synchronisiert sein.

3.2.2.1. Windows 10

Feedback

Der Domänenbeitritt ist nur mit der Pro und Enterprise-Edition von Windows 10 möglich.

Die Systemsteuerung kann über das Suchfeld **Web und Windows durchsuchen**, welches in der Startleiste zu finden ist gesucht und geöffnet werden. Unter **System und Sicherheit -> System** muss auf **Einstellungen ändern -> Ändern** geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld **Domäne** markiert und der Name der Domäne in das Eingabefeld eingetragen werden. Es sollte dabei der vollständige Domänenname verwendet werden, bspw. **mydomain.intranet**. Nach einem Klick auf die Schaltfläche **[OK]** muss in das Eingabefeld **Benutzername** der Benutzername eines Domänen Administrator, standardmäßig ist dies `Administrator` und in das Eingabefeld **Kennwort** das Passwort des Domänen Administrator eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf **[OK]** gestartet werden.

3.2.2.2. Windows 8

Feedback

Der Domänenbeitritt ist nur mit der Pro und Enterprise-Edition von Windows 8 möglich.

Die Systemsteuerung kann erreicht werden, indem der Mauszeiger in die rechte untere Bildschirmecke bewegt wird. Anschließend kann unter **Suchen** -> **Apps** nach der *Systemsteuerung* gesucht werden. Unter **System und Sicherheit** -> **System** muss auf **Einstellungen ändern** -> **Netzwerk ID** geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld **Domäne** markiert und der Name der Samba-Domäne in das Eingabefeld eingetragen werden. Nach einem Klick auf die Schaltfläche **[OK]** muss in das Eingabefeld **Name** der Name `Administrator` und in das Eingabefeld **Kennwort** das Passwort von `uid=Administrator,cn=users,`*`Basis-DN`* eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf **[OK]** gestartet werden.

3.2.2.3. Windows 7

Feedback

Der Domänenbeitritt ist nur mit der Professional, Enterprise oder Ultimate-Edition von Windows 7 möglich.

Über **Start** -> **Systemsteuerung** -> **System und Sicherheit** -> **Computernamen anzeigen** kann der Basiskonfigurationsdialog erreicht werden. Unter **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** muss **Einstellungen ändern** gewählt werden und auf **Ändern** geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld **Domäne** markiert und der Name der Samba-Domäne in das Eingabefeld eingetragen werden. Nach einem Klick auf die Schaltfläche **[OK]** muss in das Eingabefeld **Name** der Name `Administrator` und in das Eingabefeld **Kennwort** das Passwort von `uid=Administrator,cn=users,`*`Basis-DN`* eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf **[OK]** gestartet werden.

3.2.2.4. Windows Server 2012

Feedback

Die Systemsteuerung kann erreicht werden, indem der Mauszeiger in die rechte untere Bildschirmecke bewegt wird. Anschließend kann unter **Suchen** -> **Apps** nach der *Systemsteuerung* gesucht werden. Unter **System und Sicherheit** -> **System** muss auf **Einstellungen ändern** -> **Netzwerk ID** geklickt werden.

Für den Domänenbeitritt muss das Optionsfeld **Domäne** markiert und der Name der Samba-Domäne in das Eingabefeld eingetragen werden. Nach einem Klick auf die Schaltfläche **[OK]** muss in das Eingabefeld **Name** der Name `Administrator` und in das Eingabefeld **Kennwort** das Passwort von `uid=Administrator,cn=users,`*`Basis-DN`* eingetragen werden. Abschließend kann der Domänenbeitritt mit einem Klick auf **[OK]** gestartet werden.

3.2.3. Ubuntu-Domänenbeitritt

Feedback

Univention stellt den *Univention Domain Join Assistant* für die Integration von Ubuntu-Clients in eine UCS-Domäne bereit. Die Dokumentation und Installationshinweise sind auf Github[1] zu finden.

3.2.4. Mac OS X-Domänenbeitritt

Feedback

UCS unterstützt den Domänenbeitritt von Mac OS X-Clients in eine UCS-Umgebung mit Samba 4. Diese Anleitung bezieht sich auf Mac OS X 10.8.2.

Der Domänenbeitritt kann über das Systemeinstellungsmenü oder den Kommandozeilenbefehl `dsconfigad` erfolgen.

Nach erfolgtem Domänenbeitritt besteht die Möglichkeit CIFS-Freigaben zu definieren, die bei der Anmeldung eines Benutzers unterhalb von `/Volumes` automatisch eingehängt werden. Um dies zu erreichen, muss die folgende Zeile in die Datei `/etc/auto_master` eingefügt werden:

```
/Volumes    auto_custom
```

[1] https://github.com/univention/univention-domain-join

Außerdem muss die Datei `/etc/auto_custom` angelegt werden und die einzubindenden Freigaben dort in der folgenden Form aufgeführt werden:

```
subfolder name -fstype=smbfs    ://fqdn/sharename
```

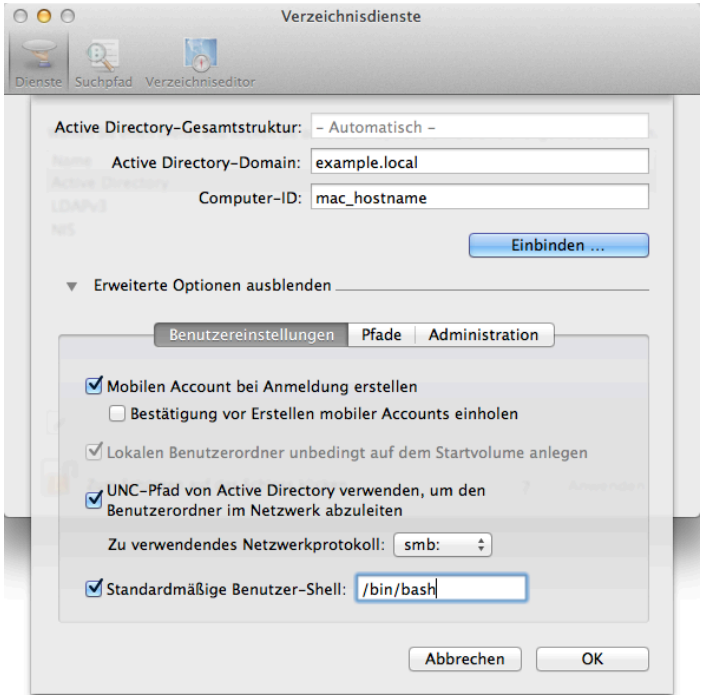
Die eingebundenen Freigaben werden nicht in der Seitenleiste des Finders angezeigt.

3.2.4.1. Domänenbeitritt über das Systemeinstellungen-Menü

Feedback

In den Systemeinstellungen kann über **Benutzer** das Menü **Anmeldeoptionen** ausgewählt werden. Die Anmeldung erfolgt durch einen Klick auf das Schloss in der linken unteren Ecke, dort muss das lokale Administrator-Konto und dessen Passwort angegeben und **Netzwerk-Account-Server: Verbinden** angeklickt werden.

Abbildung 3.2. Domänenbeitritt eines Mac OS X-Systems



In den erweiterten Einstellungen sollte die Option **Mobilen Account bei Anmeldung erstellen** aktiviert werden. Sie bietet den Vorteil, das auch ohne Verbindung zur Domäne eine Anmeldung mit der Domänenbenutzerkennung erfolgen kann

Der Domänenname muss nun im Feld **Active Directory Domain** und der Rechnername des Mac OS X-Clients in das Feld **Computer-ID** eingetragen werden. Der Domänenbeitritt erfolgt nach einem Klick auf **OK**. Für den Domänenbeitritt muss ein Konto aus der Gruppen `Domain Admins` verwendet werden, z.B. `Administrator`.

3.2.4.2. Domänenbeitritt auf den Kommandozeile

Feedback

Der Domänenbeitritt kann auch auf der Kommandozeile mit dem Befehl `dsconfigad` erfolgen:

```
dsconfigad -amac hostname-domainfqdn-ou "CN=Computers,ldap_base" \
  -uDomain Administrator-mobile enable
```

Weitere Optionen werden mit `dsconfigad -help` angezeigt.

3.3. UCS-Systemrollen

In einer UCS-Domäne können Systeme in unterschiedlichen *Systemrollen* installiert werden. Im Folgenden werden die verschiedenen Systemrollen kurz charakterisiert:

3.3.1. Domänencontroller Master

Ein System mit der Rolle Domänencontroller Master (kurz DC Master) ist der primäre Domänencontroller einer UCS-Domäne und wird immer als erstes System installiert. Auf dem DC Master werden die Domänendaten (wie z.B. Benutzer, Gruppen, Drucker) und die SSL-Sicherheitszertifikate gespeichert. Kopien dieser Daten werden automatisch auf Server mit der Rolle Domänencontroller Backup übertragen.

3.3.2. Domänencontroller Backup

Auf Servern mit der Rolle Domänencontroller Backup (kurz DC Backup) werden alle Domänendaten und SSL-Sicherheitszertifikate als Nur-Lese-Kopie gespeichert.

Der Domänencontroller Backup dient als Fallback-System des Domänencontroller Master. Sollte dieser ausfallen, kann ein Domänencontroller Backup die Rolle des Domänencontroller Master dauerhaft übernehmen (siehe Abschnitt 3.11).

3.3.3. Domänencontroller Slave

Auf Servern mit der Rolle Domänencontroller Slave (kurz DC Slave) werden die Domänendaten als Nur-Lese-Kopie gespeichert. Im Gegensatz zum Domänencontroller Backup werden jedoch nicht alle SSL-Sicherheitszertifikate gespeichert. Da die Zugriffe der auf einem Domänencontroller Slave laufenden Dienste gegen den lokalen LDAP-Datenbestand erfolgen, bieten sich DC Slave-System für Standortserver und für die Verteilung lastintensiver Dienste an.

Ein DC Slave-System kann nicht zum DC Master hochgestuft werden.

3.3.4. Memberserver

Memberserver sind Server-Systeme ohne lokalen LDAP-Server. Der Zugriff auf Domänendaten erfolgt hierbei über andere Server der Domäne.

3.3.5. Basissystem

Ein Basissystem ist ein eigenständiges System, das aber nicht Mitglied der Domäne ist. Es ist mit keinem LDAP-Server verbunden. Der UCS Update-Mechanismus und Univention Configuration Registry als Möglichkeit der Konfiguration sind Bestandteil, aber die grafische Oberfläche Univention Management Console zur Administration ist es nicht.

Ein Basissystem bietet sich somit für Dienste an, die außerhalb des Vertrauenskontextes der Domäne betrieben werden, etwa als Web-Server oder Firewall.

3.3.6. Ubuntu

Ubuntu-Clients können mit einer eigenen Systemrolle verwaltet werden, siehe Abschnitt 8.1.1.

3.3.7. Linux

Diese Systemrolle wird für die Integration von anderen Linux-Systemen als UCS und Ubuntu verwendet, z.B. für Debian- oder CentOS-Systeme. Die Integration wird in [ext-doc-domain] beschrieben.

3.3.8. Univention Corporate Client

Feedback

Ein Univention Corporate Client ist ein Desktop- oder Thin Client-System auf Basis von Univention Corporate Client.

3.3.9. Mac OS X

Feedback

Mac OS X-Systeme können einer UCS-Domäne mit Samba 4 beitreten. Weitere Hinweise finden sich in Abschnitt 3.2.4.

3.3.10. Domain Trust Account

Feedback

Ein Domain Trust Account wird für Vertrauensstellungen zwischen Windows und UCS Domänen eingerichtet.

3.3.11. IP-Managed-Client

Feedback

Ein IP-Managed-Client ermöglicht die Integration von Nicht-UCS-Systemen in das IP-Management (DNS/DHCP), z.B. für Netzwerkdrucker oder Router.

3.3.12. Windows Domänencontroller

Feedback

Windows-Domänencontroller in einer Samba 4-Umgebung werden mit dieser Systemrolle betrieben.

3.3.13. Windows Workstation/Server

Feedback

Windows-Clients und Windows-Memberserver werden mit dieser Systemrolle verwaltet.

3.4. LDAP-Verzeichnisdienst

Feedback

Univention Corporate Server speichert domänenweit vorgehaltene Daten in einem LDAP-Verzeichnisdienst auf Basis von OpenLDAP. Dieses Kapitel beschreibt die weitergehende Konfiguration und Anpassung von OpenLDAP.

In einer UCS-Domäne werden oft mehrere LDAP-Server betrieben. Die Konfiguration des/der verwendeten Server(s) wird in Abschnitt 8.4.5 beschrieben.

3.4.1. LDAP-Schemata

Feedback

In Schema-Definitionen wird festgelegt, welche Objektklassen existieren und welche Attribute darin enthalten sind - mit anderen Worten, welche Daten in einem Verzeichnisdienst gespeichert werden können. Schema-Definitionen liegen als Text-Dateien vor und werden über die Konfigurationsdatei des OpenLDAP-Servers eingebunden.

UCS verwendet nach Möglichkeit Standard-Schemata, so dass eine Interoperabilität mit anderen LDAP-Applikationen in der Regel gegeben ist. Für Univention-spezifische Attribute - etwa für den Richtlinien-Mechanismus - werden Schema-Erweiterungen mitgeliefert.

3.4.1.1. LDAP-Schema-Erweiterungen

Feedback

Um den Aufwand für kleine Erweiterungen im LDAP möglichst gering zu halten, bringt UCS ein eigenes LDAP-Schema für Kundenerweiterungen mit. Die LDAP-Objektklasse `univentionFreeAttributes` kann ohne Einschränkungen für erweiterte Attribute verwendet werden. Sie bringt 20 frei zu verwendende

Attribute (*univentionFreeAttribute1* bis *univentionFreeAttribute20*) mit und kann in Verbindung mit jedem beliebigen LDAP-Objekt (z.B. einem Benutzerobjekt) verwendet werden.

Wenn LDAP-Schema-Erweiterungen als Teil von Softwarepaketen ausgeliefert werden sollen, besteht auch die Möglichkeit diese zu paketieren und durch ein Univention Directory Listener-Modul an alle Domänencontroller Backup-Server der Domäne zu verteilen. Weitere Hinweise finden sich in [packaging-schema-extensions].

3.4.1.2. LDAP-Schema-Replikation

Feedback

Über den Listener/Notifier-Mechanismus (siehe Abschnitt 3.5) wird auch die Replikation der LDAP-Schemata automatisiert. Dies entbindet den Administrator von der Notwendigkeit, Schema-Änderungen auf allen OpenLDAP-Servern der Domäne manuell nachzupflegen. Mit der Ausführung der Schema-Replikation vor der Replikation von LDAP-Objekten wird sichergestellt, dass diese nicht aufgrund fehlender Objektklassen oder Attribute scheitert.

Auf dem Domänencontroller Master wird beim Start des OpenLDAP-Servers über alle Verzeichnisse mit Schema-Definitionen eine Prüfsumme erzeugt. Diese Prüfsumme wird mit der letzten in der Datei `/var/lib/univention-ldap/schema/md5` gespeicherten Prüfsumme verglichen.

Die eigentliche Replikation der Schema-Definitionen wird vom Univention Directory Listener initiiert. Vor jeder Abfrage einer neuen Transaktion-ID durch den Univention Directory Notifier wird dessen aktuelle Schema-ID abgefragt. Ist diese höher als die Schema-ID auf der Listener-Seite, wird über eine LDAP-Suche vom LDAP-Server des Notifier-Systems dessen aktuell verwendetes Subschema bezogen.

Das ausgelesene Subschema wird auf dem Listener-System im LDIF-Format in die Datei `/var/lib/univention-ldap/schema.conf` eingebunden und der lokale OpenLDAP-Server neu gestartet. Ist die Schema-Replikation mit diesem Schritt abgeschlossen, wird die Replikation der LDAP-Objekte fortgeführt.

3.4.2. Revisionssichere LDAP-Protokollierung

Feedback

Das Paket ***univention-directory-logger*** ermöglicht die Protokollierung von Änderungen im LDAP-Verzeichnisdienst. Da jeder Datensatz den Hash-Wert des vorhergehenden Datensatzes enthält, können Manipulationen an der Logdatei - etwa entfernte Einträge - aufgedeckt werden.

Einzelne Teilbereiche des Verzeichnisdienstes können von der Protokollierung ausgenommen werden. Diese Zweige können durch die Univention Configuration Registry-Variablen `ldap/logging/exclude1`, `ldap/logging/exclude2` etc. konfiguriert werden. Standardmässig ist der Container exkludiert, in dem die temporären Objekte gespeichert werden (`cn=temporary,cn=univention`). Die Protokollierung der LDAP-Änderungen erfolgt durch ein Univention Directory Listener-Modul, nach Univention Configuration Registry-Änderungen muss der Univention Directory Listener-Dienst neu gestartet werden.

Die Protokollierung erfolgt in die Datei `/var/log/univention/directory-logger.log` im folgenden Format:

```
START
Old Hash: Hashsumme des vorhergehenden Datensatzes
DN: DN des LDAP-Objekts
ID: Listener/Notifer-Transaktions-ID
Modifier: DN des ändernden Kontos
Timestamp: Zeitstempel im Format dd.mm.yyyy hh:mm:ss
Action: add, modify oder delete

Old Values:
 Liste der alten Attribute, ist leer wenn ein Objekt hinzugefügt wird
New Values:
```

```
 Liste der neuen Attribute, ist leer wenn ein Objekt gelöscht wird
END
```

Für jeden protokollierten Datensatz wird eine Hashsumme berechnet und zusätzlich in die Sektion *daemon.info* des Syslog-Dienstes protokolliert.

Ab UCS 4.4-0 erratum 536[1] wird in der Datei `/var/log/univention/directory-logger.log` vor jede Zeile als Präfix die jeweilige Transaktions-ID des Eintrags hinzugefügt:

```
ID 342: START
ID 342: Old Hash: 70069d51a7e2e168d7c7defd19349985
ID 342: DN: uid=Administrator,cn=users,dc=example,dc=com
ID 342: ID: 342
ID 342: Modifier: cn=admin,dc=example,dc=com
ID 342: Timestamp: 15.04.2020 09:20:40
ID 342: Action: modify
ID 342:
ID 342: Old values:
ID 342: description: Dhis is a description test
ID 342: entryCSN: 20200415091936.317108Z#000000#000#000000
ID 342: modifyTimestamp: 20200415091936Z
ID 342:
ID 342: New values:
ID 342: description: This is a description test
ID 342: entryCSN: 20200415092040.430976Z#000000#000#000000
ID 342: modifyTimestamp: 20200415092040Z
ID 342: END
```

Wurde ***univention-directory-logger*** vor dieser UCS-Version installiert, wird per Default das alte Verhalten (kein Präfix) beibehalten. Durch das Setzen der Univention Configuration Registry-Variable `ldap/logging/id-prefix=yes` kann das neue Verhalten aktiviert werden. Dieses Präfix erleichtert eine Korrelation der zusammenhängenden Zeilen bei einer Weiterverarbeitung des Protokolls in Analyse- und Monitoring-Software.

3.4.3. Timeout für inaktive LDAP-Verbindungen

Feedback

Mit der Univention Configuration Registry-Variable `ldap/idletimeout` kann ein Zeitraum in Sekunden konfiguriert werden, nach dessen Ablauf eine LDAP-Verbindung serverseitig geschlossen wird. Wenn der Wert auf 0 gesetzt wird, wird kein Ablaufzeitraum angewendet. Der Ablaufzeitraum beträgt standardmäßig sechs Minuten.

3.4.4. LDAP-Kommandozeilen-Tools

Feedback

Neben dem UMC-Webinterface gibt es auch eine Reihe von Programmen, mit denen auf der Kommandozeile auf das LDAP-Verzeichnis zugegriffen werden kann.

Das Tool `univention-ldapsearch` vereinfacht die authentifizierte Suche im LDAP-Verzeichnis. Als Argument muss ein Suchfilter übergeben werden, im folgenden Beispiel wird der Administrator anhand der User-ID gesucht:

```
univention-ldapsearch uid=Administrator
```

Der Befehl `slapcat` ermöglicht die Speicherung der aktuellen LDAP-Daten in einer Textdatei im LDIF-Format, z.B.:

[1] https://errata.software-univention.de/#/?erratum=4.4x536

```
slapcat > ldapdaten.txt
```

3.4.5. Zugriffskontrolle auf das LDAP-Verzeichnis

Feedback

Der Zugriff auf die Informationen im LDAP-Verzeichnis wird serverseitig durch Access Control Lists (ACLs) geregelt. Die ACLs werden in der zentralen Konfigurationsdatei `/etc/ldap/slapd.conf` definiert und über Univention Configuration Registry verwaltet. Die `slapd.conf` wird dabei durch ein Multifile-Template verwaltet; weitere ACL-Elemente können unterhalb von `/etc/univention/templates/files/etc/ldap/slapd.conf.d/` zwischen den Dateien `60univention-ldap-server_acl-master` und `70univention-ldap-server_acl-master-end` eingefügt werden oder die bestehenden Templates erweitert werden.

Wenn LDAP-ACL-Erweiterungen als Teil von Softwarepaketen ausgeliefert werden sollen, besteht auch die Möglichkeit diese zu paketieren und durch ein Univention Directory Listener-Modul an alle LDAP-Server der Domäne zu verteilen. Weitere Hinweise finden sich in [packaging-acl-extensions].

Die Grundeinstellung des LDAP-Servers bei Neuinstallationen mit UCS erlaubt keinen anonymen Zugriff auf das LDAP-Verzeichnis. Dieses Verhalten kann mit der Univention Configuration Registry-Variable `ldap/acl/read/anonymous` konfiguriert werden. Einzelne IP-Adressen können über die Univention Configuration Registry-Variable `ldap/acl/read/ips` für den anonymen Lesezugriff freigeschaltet werden.

Nach erfolgreicher Authentifizierung am LDAP-Server können alle Attribute eines Benutzerkontos von diesem Benutzer ausgelesen werden.

Ein zusätzlicher, interner Account, der Root-DN, besitzt darüber hinaus auch schreibenden Vollzugriff.

Unter UCS gibt es außerdem einige standardmäßig installierte ACLs, die den Zugriff auf sensitive Daten unterbinden (z.B. auf das Benutzerpasswort) und für den Betrieb notwendige Regeln setzen (etwa nötige Zugriffe auf Rechnerkonten für Anmeldungen). Der lesende und schreibende Zugriff auf diese sensitiven Daten ist nur für die Mitglieder der Gruppe `Domain Admins` vorgesehen. Dabei werden auch enthaltene Gruppen unterstützt. Mit der Univention Configuration Registry-Variable `ldap/acl/nestedgroups` kann diese Gruppen-in-Gruppen-Funktionalität für die LDAP-ACLs deaktiviert werden, wodurch eine Geschwindigkeitssteigerung bei den Verzeichnisdienstanfragen zu erwarten ist.

3.4.5.1. Delegation des Zurücksetzens von Benutzerpasswörtern

Feedback

Um einer Teilgruppe von Administratoren mit eingeschränkten Rechten, z.B. einem Helpdesk, das Zurücksetzen von Benutzerpasswörtern zu ermöglichen, kann das Paket ***univention-admingrp-user-passwordreset*** installiert werden. Es legt über ein Joinskript die Benutzergruppe `User Password Admins` an, sofern diese noch nicht existiert.

Mitglieder dieser Gruppe erhalten über zusätzliche LDAP-ACLs die Berechtigung, Passwörter von anderen Benutzern zurückzusetzen. Diese LDAP-ACLs werden bei der Paketinstallation automatisch aktiviert. Um eine andere ggf. schon existierende Gruppe statt der Gruppe `User Password Admins` zu verwenden, kann der DN der zu verwendenden Gruppe in die Univention Configuration Registry-Variable `ldap/acl/user/passwordreset/accesslist/groups/dn` eingetragen werden. Nach der Änderung ist ein Neustart des LDAP-Servers erforderlich.

Das Zurücksetzen der Passwörter kann über Univention Management Console erfolgen. In der Standardeinstellung bietet Univention Management Console nur dem Benutzer `Administrator` den Benutzer-Assistenten an, über den neue Passwörter gesetzt werden können. Während der Installation wird automatisch eine neue Richtlinie `default-user-password-admins` erstellt, die den Mitgliedern der Gruppe `User Password Admins` zugewiesen ist bzw. mit einem entsprechenden Container im LDAP-Verzeichnis verknüpft werden kann. Weitere Hinweise zur Konfiguration von UMC-Richtlinien finden sich in Kapitel Abschnitt 4.9.

Die Richtlinie ermöglicht dabei die Suche nach Benutzern sowie die Ansicht aller Attribute eines Benutzerobjektes. Wird versucht, neben dem Passwort weitere Attribute zu modifizieren, für die keine ausreichenden Zugriffsrechte auf das LDAP-Verzeichnis existieren, wird der Schreibzugriff vom Univention Directory Manager mit der Meldung *Zugriff verweigert* abgelehnt.

Achtung

Das Paket ist auf dem Domaincontroller Master- sowie den Domaincontroller Backup-Systemen zu installieren. Während der Installation wird der LDAP-Server neu gestartet und ist kurzzeitig nicht erreichbar.

Das Zurücksetzen der Passwörter durch die Passwort-Gruppe kann für sensible Benutzer oder Gruppen (z.B. Domänen-Administratoren) verhindert werden. Mit den Univention Configuration Registry-Variablen `ldap/acl/user/passwordreset/protected/uid` und `ldap/acl/user/passwordreset/protected/gid` können Benutzer und Gruppen konfiguriert werden. Mehrere Werte müssen durch Kommas getrennt werden. Nach Änderungen an den Variable ist es erforderlich, den LDAP-Server über den Befehl `/etc/init.d/slapd restart` neu zu starten. In der Standardeinstellung werden die Mitglieder der Gruppe `Domain Admins` vor Passwortänderungen geschützt.

Sollte für die Änderung des Passworts der Zugriff auf zusätzliche LDAP-Attribute notwendig sein, können die Attributnamen in der Univention Configuration Registry-Variable `ldap/acl/user/passwordreset/attributes` ergänzt werden. Nach der Änderung ist zur Übernahme ein Neustart des LDAP-Verzeichnisdienstes notwendig. Für eine UCS-Standard-Installation ist diese Variable bereits passend gesetzt.

3.4.6. Name Service Switch / LDAP-NSS-Modul

Feedback

Die in Univention Corporate Server verwendete GNU C-Standardbibliothek (***glibc***) bietet eine modulare Schnittstelle zur Auflösung von Namen von Benutzern, Gruppen und Rechnern, den *Name Service Switch*.

Das LDAP-NSS-Modul wird auf UCS-Systemen standardmäßig für den Zugriff auf die Domänen-Daten (z.B. Benutzer) verwendet. Das Modul greift dabei auf den in der Univention Configuration Registry-Variable `ldap/server/name` (und ggf. zusätzlich der `ldap/server/addition`) festgelegten LDAP-Server zu.

Das Verhalten bei nicht erreichbarem LDAP-Server kann durch die Univention Configuration Registry-Variable `nssldap/bindpolicy` festgelegt werden. Standardmäßig wird bei nicht erreichbarem Server eine erneute Verbindung aufgebaut. Wird die Variable auf `soft` gesetzt, wird kein erneuter Verbindungsaufbau durchgeführt. Dies kann den Boot eines Systems mit nicht erreichbarem LDAP-Server - z.B. in einer abgeschottenen Testumgebung - deutlich beschleunigen.

3.4.7. Syncrepl zur Anbindung von Nicht-UCS OpenLDAP-Servern

Feedback

Für die Anbindung von nicht auf UCS-Systemen installierten OpenLDAP-Servern an das UCS-Managementsystem kann parallel zum Notifier-Dienst der Syncrepl-Replikations-Dienst aktiviert werden. Dieser ist Bestandteil von OpenLDAP, registriert Veränderungen im lokalen Verzeichnisdienst und überträgt diese auf weitere OpenLDAP-Server.

3.4.8. Konfiguration des Verzeichnis-Dienstes bei Verwendung von Samba 4

Feedback

Standardmäßig ist der OpenLDAP-Server so konfiguriert, dass er zusätzlich zu den Standard-Ports 389 und 636 auch auf den Ports 7389 und 7636 Anfragen entgegennimmt.

Wird Samba 4 eingesetzt, belegt der Samba-Domänencontroller-Dienst die Ports 389 und 636. In diesem Fall wird OpenLDAP automatisch umkonfiguriert, so dass nur noch die Ports 7389 und 7636 eingesetzt werden.

Dies ist insbesondere bei der Konfiguration von syncrepl zu beachten (siehe Abschnitt 3.4.7). `univention-ldapsearch` verwendet automatisch den Standard-Port.

3.4.9. Tägliche Sicherung der LDAP-Daten

Feedback

Auf dem Domänencontroller Master und allen Domänencontroller Backup-Systemen wird der Inhalt des LDAP-Verzeichnisses durch einen Cron-Job täglich gesichert. Falls Samba 4 eingesetzt wird, wird auch dessen Daten-Verzeichnis gesichert.

Die LDAP-Daten werden im LDIF-Format im Verzeichnis `/var/univention-backup/` im Namensschema `ldap-backup_DATUM.ldif.gz` gespeichert. Sie sind nur für den Benutzer `root` lesbar. Die Samba 4 Backup-Dateien werden im Verzeichnis `/var/univention-backup/samba/` gesichert.

Mit der Univention Configuration Registry-Variable `backup/clean/max_age` kann definiert werden, wie lange alte Backup-Dateien aufgehoben werden (z.B. `backup/clean/max_age=365`, alle Dateien älter als 365 Tage werden automatisch gelöscht). Diese Variable wird bei Neuinstallationen ab UCS 4.4-7 automatisch auf 365 gesetzt. Falls die Variable nicht gesetzt ist, werden keine Backup-Dateien gelöscht.

3.5. Listener/Notifier-Domänenreplikation

Feedback

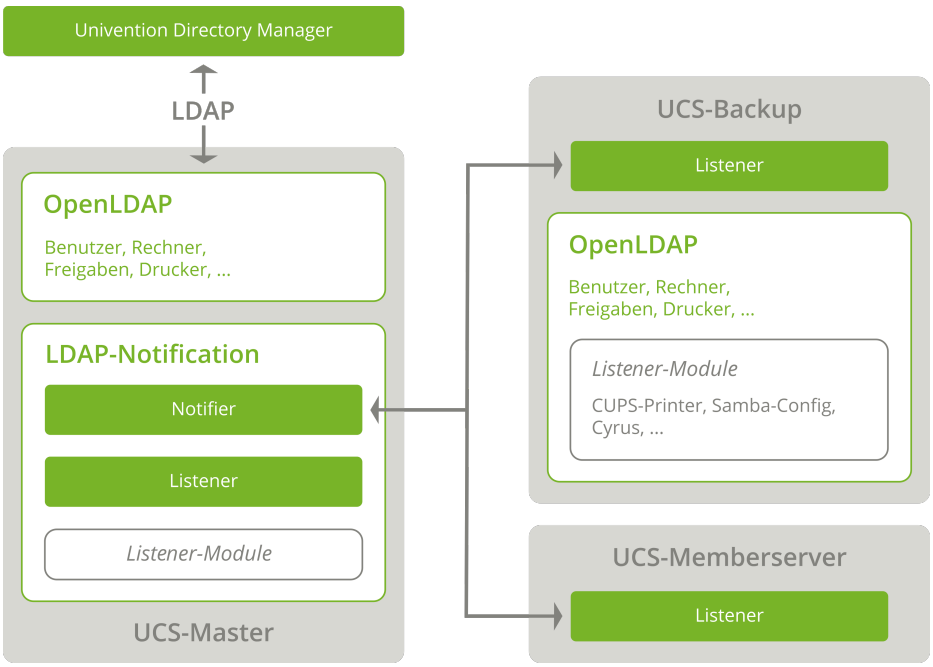
3.5.1. Ablauf der Listener/Notifier-Replikation

Feedback

Die Replikation der Verzeichnisdaten innerhalb einer UCS-Domäne erfolgt über den Listener/Notifier-Mechanismus:

- Der *Univention Directory Listener*-Dienst läuft auf jedem UCS-System.
- Auf dem Domänencontroller Master (und eventuell vorhandenen Domänencontroller Backup-Systemen) überwacht der *Univention Directory Notifier*-Dienst Änderungen im LDAP-Verzeichnis und stellt die aufgezeichneten Änderungen transaktionsbasiert den Univention Directory Listener-Diensten auf den weiteren UCS-Systemen zur Verfügung.

Abbildung 3.3. Listener/Notifier-Mechanismus



Die aktiven Univention Directory Listener-Instanzen der Domäne verbinden sich zu einem Univention Directory Notifier-Dienst. Wird auf dem Domänencontroller Master eine LDAP-Änderung durchgeführt (alle anderen LDAP-Server der Domäne sind nur lesend), wird diese durch den Univention Directory Notifier registriert und an die Listener-Instanzen gemeldet.

Jede Univention Directory Listener-Instanz verwendet eine Reihe von Univention Directory Listener-Modulen. Diese Module werden von den installierten Applikationen mitgeliefert, das Druckserver-Paket bringt z.B Listener-Module mit, die die CUPS-Konfiguration erzeugen.

Durch Univention Directory Listener-Module können Änderungen an der Domäne auch an Dienste übermittelt werden, die selbst nicht LDAP-fähig sind. Ein Beispiel ist der Druckserver CUPS: Die Druckerdefinitionen werden nicht aus dem LDAP ausgelesen, sondern aus der Datei `/etc/cups/printers.conf`. Wird nun in der UMC-Druckerverwaltung ein Drucker angelegt, wird dieser im LDAP registriert. Diese Änderung wird dann vom Univention Directory Listener-Modul *cups-printers* erkannt und basierend auf den Daten im LDAP ein Eintrag in `/etc/cups/printers.conf` hinzugefügt, modifiziert oder gelöscht.

Weitergehende Informationen zum Aufbau von Univention Directory Listener-Modulen und zur Entwicklung eigener Module finden sich in [developer-reference].

Die LDAP-Replikation erfolgt ebenfalls durch ein Listener-Modul. Ist der LDAP-Server zu dem repliziert werden soll nicht erreichbar, werden die LDAP-Änderungen in der Datei `/var/lib/univention-directory-replication/failed.ldif` zwischengespeichert. Der Inhalt dieser Datei wird beim späteren Start des LDAP-Servers automatisch in das LDAP übertragen.

Der Listener/Notifier-Mechanismus arbeitet transaktionsbasiert. Für jede Änderung im LDAP-Verzeichnis des Domänencontroller Master wird eine Transaktions-ID erhöht. Eine Univention Directory Listener-Instanz, die mehrere Transaktionen verpasst hat - weil zum Beispiel der Rechner ausgeschaltet war - fragt bei erneuter Verfügbarkeit der Verbindung automatisch alle fehlenden Transaktionen ab, bis seine lokale Transaktions-ID der des Domänencontroller Master entspricht.

3.5.2. Analyse von Listener/Notifier-Problemen

Feedback

3.5.2.1. Logdateien/Debug-Level der Replikation

Feedback

Alle Statusmeldungen des Univention Directory Listener und der aufgerufenen Listener-Module werden in die Datei `/var/log/univention/listener.log` protokolliert. Der Detailgrad der Logmeldungen kann über die Univention Configuration Registry-Variable `listener/debug/level` konfiguriert werden. Mögliche Werte reichen von 0 (nur Fehlermeldungen) bis 4 (alle Statusmeldungen). Nachdem der Debuglevel geändert wurde, muss der Univention Directory Listener neu gestartet werden.

Statusmeldungen des Univention Directory Notifier-Dienstes werden in die Datei `/var/log/univention/notifier.log` protokolliert. Der Debuglevel kann mit der Variable `notifier/debug/level` konfiguriert werden (ebenfalls von 0-4). Nachdem der Debuglevel geändert wurde, muss der Univention Directory Notifier neu gestartet werden.

3.5.2.2. Erkennung von Replikationsproblemen

Feedback

Im Regelbetrieb der Domänenreplikation (keine hohe Last auf den Systemen, keine Störungen im Netzwerk) ist die Verzögerung zwischen der Änderung in Univention Management Console bis zur Replikation auf z.B. eines Domänencontroller Slave kaum merkbar. Eine möglicherweise unvollständige Replikation kann durch einen Vergleich der Transaktions-IDs von Listener- und Notifier-Dienst identifiziert werden.

Auf dem Domänencontroller Master werden die vom Notifier-Dienst registrierten Transaktionen in aufsteigender Reihenfolge in die Datei `/var/lib/univention-ldap/notify/transaction` geschrieben. Ein Beispiel:

```
root@dcmaster:~# tail -1 /var/lib/univention-ldap/notify/transaction
```

```
836 cn=dcslave3,cn=dc,cn=computers,dc=firma,dc=de m
```

Auf dem Listener-System wird die zuletzt vom Listener empfangene Transaktion in der Datei `/var/lib/univention-directory-listener/notifier_id` gespeichert:

```
root@dcslave1:~# cat /var/lib/univention-directory-listener/notifier_id
836
```

Diese Prüfung kann auch automatisiert durch den Nagios-Dienst `UNIVENTION_REPLICATION` durchgeführt werden (siehe Abschnitt 15.3.2.1).

3.5.2.3. Neuinitialiisierung von Listener-Modulen

Feedback

Falls es zu Problemen bei der Abarbeitung eines Listener-Moduls gekommen ist, besteht die Möglichkeit, das Modul neu zu initialisieren. Dabei werden alle LDAP-Objekte mit denen das Listener-Modul arbeitet erneut übergeben.

Dem Befehl zum erneuten Initialisieren muss der Name des Listener-Moduls übergeben werden. Die installierten Listener-Module sind im Verzeichnis `/var/lib/univention-directory-listener/handlers/` zu finden.

Mit dem folgenden Befehl kann beispielsweise das Druckermodul neu initialisiert werden:

```
univention-directory-listener-ctrl resync cups-printers
```

3.6. SSL-Zertifikatsverwaltung

Feedback

Unter UCS werden sensitive Daten immer verschlüsselt über das Netzwerk übertragen, zum Beispiel durch die Verwendung von SSH für den Login auf Systeme oder durch Verwendung von Protokollen auf Basis von SSL/TLS. (*Transport Layer Security (TLS)* ist der aktuelle Protokollname, der Name des Vorgängerprotokolls *Secure Socket Layer (SSL)* ist jedoch weiterhin gebräuchlicher und wird auch in dieser Dokumentation verwendet).

SSL/TLS kommt beispielsweise bei der Listener/Notifier-Domänenreplikation oder beim HTTPS-Zugriff auf Univention Management Console zum Einsatz.

Für eine verschlüsselte Kommunikation zwischen zwei Rechnern müssen beide Kommunikationspartner die Authentizität des verwendeten Schlüssels prüfen können. Dafür besitzt jeder Rechner ein so genanntes *Rechnerzertifikat*, das von einer Zertifizierungsstelle (Certification Authority, CA) herausgegeben und signiert wird.

UCS bringt seine eigene CA mit, die bei der Installation des Domänencontroller Master automatisch eingerichtet wird und von der jedes UCS-System im Rahmen des Domänenbeitritts automatisch ein Zertifikat für sich selbst und das öffentliche Zertifikat der CA bezieht. Diese CA tritt als Root-CA auf, signiert ihr eigenes Zertifikat, und kann Zertifikate für andere Zertifizierungsstellen signieren.

Die Eigenschaften der CA werden bei der Installation basierend auf Systemeinstellungen wie der Locale automatisch festgelegt. Diese Einstellungen können auf dem Domänencontroller Master im UMC-Modul **Zertifikats-Einstellungen** nachträglich angepasst werden.

Achtung

Besteht die UCS-Domäne aus mehr als einem System müssen durch die Änderung des Root-Zertifikats auch alle anderen Rechner-Zertifikate neu ausgestellt werden! Das dafür nötige Vorgehen ist in SDB 1183[1] dokumentiert.

[1] http://sdb.univention.de/1183

Die UCS-CA befindet sich immer auf dem Domänencontroller Master. Auf jedem Domänencontroller Backup wird eine Kopie der CA vorgehalten, die über einen Cronjob standardmäßig alle 20 Minuten mit der CA auf dem Domänencontroller Master synchronisiert wird.

Achtung

Die CA wird nur vom Domänencontroller Master zum Domänencontroller Backup synchronisiert und nicht umgekehrt. Es sollte also ausschließlich die CA auf dem Domänencontroller Master verwendet werden.

Wird ein Domänencontroller Backup zum Domänencontroller Master hochgestuft (siehe Abschnitt 3.11), so kann die CA auf dem dann neuen Domänencontroller Master direkt verwendet werden.

Das UCS-Root-Zertifikat hat - ebenso wie die damit erstellten Rechnerzertifikate - einen bestimmten Gültigkeitszeitraum.

Achtung

Ist dieser Zeitraum abgelaufen, funktionieren Dienste, die ihre Kommunikation mit SSL verschlüsseln (z.B. LDAP oder die Domänenreplikation) nicht mehr. Es ist deshalb notwendig, die Gültigkeit der Zertifikate regelmäßig zu überprüfen und rechtzeitig das Root-Zertifikat zu erneuern. Für die Überwachung des Gültigkeitszeitraums wird ein Nagios-Plugin bereitgestellt. Außerdem erfolgt bei der Anmeldung an Univention Management Console eine Warnmeldung, wenn das Root-Zertifikat bald abläuft (der Warnzeitraum kann mit der Univention Configuration Registry-Variable `ssl/validity/warning` festgelegt werden und beträgt standardmäßig 30 Tage).

Die Erneuerung des Root-Zertifikats und der übrigen Rechnerzertifikate ist in SDB 1183[1] dokumentiert.

Auf UCS-Systemen überprüft ein Cronjob täglich die Gültigkeit des lokalen Rechnerzertifikats und des Root-Zertifikats und schreibt das Ablaufdatum in die Univention Configuration Registry-Variablen `ssl/validity/host` (Rechnerzertifikat) und `ssl/validity/root` (Root-Zertifikat). Die dort angegebenen Werte spiegeln die Anzahl der Tage seit dem 1.1.1970 wieder.

In Univention Management Console wird das effektive Ablaufdatum des Rechner- und Root-Zertifikats angezeigt über über das rechte, obere Benutzermenü und den Menüpunkt **Lizenz -> Lizenzinformation**.

3.7. Kerberos

Feedback

Kerberos ist ein Authentikationsverfahren um in verteilten Netzen über potentiell unsichere Verbindungen eine sichere Identifikation zu erlauben. Alle Clients verwenden dabei eine gemeinsame Vertrauensbasis, das *Key Distribution Centre* (KDC). Ein Client authentifiziert sich bei diesem KDC und erhält ein Authentizierungs-Token, das sogenannte Ticket, das zur Authentizierung innerhalb einer Kerberos-Umgebung (der sogenannten Kerberos Realm) verwendet werden kann. Der Name der Kerberos Realm wird im Rahmen der Installation des Domänencontroller Master konfiguriert und in der Univention Configuration Registry-Variable `kerberos/realm` gespeichert. Der Name der Kerberos-Realm kann nachträglich nicht angepasst werden.

Tickets sind standardmäßig acht Stunden gültig; für eine Kerberos-Domäne ist deshalb eine synchrone Systemzeit zwischen den Systemen der Kerberos Realm essentiell.

In Univention Corporate Server wird die Kerberos-Implementierung Heimdal verwendet. Auf UCS-Domänencontroller-Systemen ohne Samba 4 wird ein eigenständiger Heimdal-Dienst gestartet, während auf Samba 4-DCs Kerberos durch eine in Samba integrierte Heimdal-Version bereitgestellt wird. Verwendet man eine

[1] http://sdb.univention.de/1183

gemischte Umgebung aus UCS-Domänencontrollern mit Samba 4 und UCS-Domänencontrollern ohne Samba 4, so basieren beide Kerberos-Umgebungen auf identischen Daten (diese werden zwischen Samba 4 und OpenLDAP durch den Univention S4 Connector synchronisiert (siehe Abschnitt 9.2.2.4)).

Standardmäßig wird der KDC über einen DNS-Servicerecord ausgewählt. Der von einem System verwendete KDC kann durch die Univention Configuration Registry-Variable `kerberos/kdc` umkonfiguriert werden. Wird Samba 4 auf einem System der Domäne installiert, wird der Servicerecord umkonfiguriert, so dass nur noch die KDCs auf Samba 4-Basis angeboten werden. In einer gemischten Umgebung ist es empfehlenswert nur noch die Samba 4-KDCs zu verwenden.

Auf dem Domänencontroller Master läuft der Kerberos-Adminserver, auf dem administrative Einstellungen der Domäne vorgenommen werden können. Die meisten Einstellungen werden in Univention Corporate Server aus dem LDAP-Verzeichnis bezogen, so dass die wichtigste verbleibende Funktion das Ändern von Passwörtern darstellt. Diese können durch das Tool `kpasswd` geändert werden und werden dann auch im LDAP verändert. Der Kerberos Adminserver kann auf einem System durch die Univention Configuration Registry-Variable `kerberos/adminserver` konfiguriert werden.

3.8. Passwort-Hashes im Verzeichnisdienst

Feedback

Passwort-Hashes von Benutzern werden u.a. im Attribut *userPassword* im Verzeichnisdienst gespeichert. Für die Generierung der Passwort-Hashes wird auf die `crypt` Bibliotheksfunktion zurückgegriffen. Die eigentliche Hash-Funktion kann über die Univention Configuration Registry-Variable `password/hashing/method` definiert werden, standardmäßig wird `SHA-512` verwendet.

Alternativ dazu bietet Univention Corporate Server ab UCS 4.4-7 erratum 887[1] die Möglichkeit `bcrypt` als Hash-Funktion für Benutzerkonten zu verwenden. Dafür muss zunächst auf allen LDAP-Servern die Univention Configuration Registry-Variable `ldap/pw-bcrypt=true` gesetzt werden um das nötige Modul für OpenLDAP zu aktivieren. Andernfalls ist eine Anmeldung am LDAP-Server mit einem `bcrypt` Hash nicht möglich. Damit beim Ändern von Passwörtern nun `bcrypt` Hashes generiert werden, muss ebenfalls auf allen Servern die Univention Configuration Registry-Variable `password/hashing/bcrypt=true` gesetzt werden.

Zusätzlich können der *bcrypt Cost Factor* und die `bcrypt` Variante über die Univention Configuration Registry-Variablen `password/hashing/bcrypt/cost_factor` (`12`) und `password/hashing/bcrypt/prefix` (`2b`) angepasst werden.

Achtung

`bcrypt` ist auf maximal 72 Zeichen begrenzt. Für die Generierung der Hashes werden also nur die ersten 72 Zeichen des Kennwort verwendet.

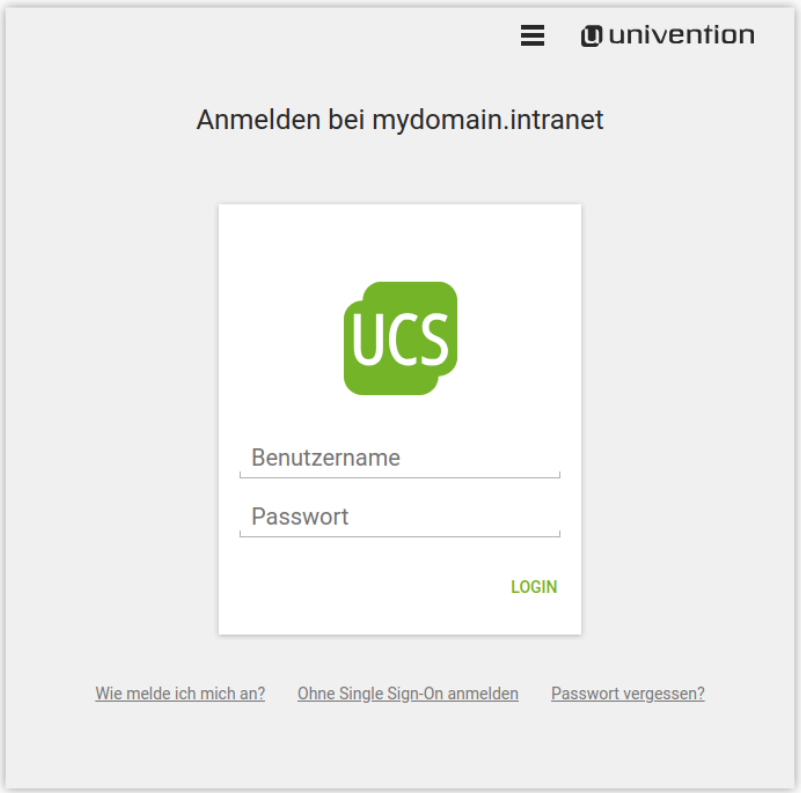
3.9. SAML Identity Provider

Feedback

SAML (Security Assertion Markup Language) ist ein XML-basierter Standard zum Austausch von Authentifizierungsinformationen, der *Single Sign-On* über Domänengrenzen hinweg erlaubt. UCS stellt auf dem Domänencontroller Master und den Domänencontroller Backup einen ausfallsicheren SAML Identity Provider bereit. Über ein kryptografisches Zertifikat wird der SAML Identity Provider bei einem externen Dienst fest registriert und vertraut diesem. Der Benutzer authentifiziert sich dann einmalig gegenüber UCS und kann den Dienst ohne erneute Authentifizierung nutzen.

[1] https://errata.software-univention.de/#/?erratum=4.4x887

Abbildung 3.4. Die *Single Sign-On*-Anmeldeseite



Der SAML 2.0 kompatible UCS Identity Provider wird durch die Integration von ***simplesamlphp*** bereitgestellt.

Der UCS Identity Provider ist eng in die UCS Domäne eingebunden. Daher müssen Rechner, von denen der UCS Identity Provider genutzt werden soll, DNS-Namen in der UCS-Domäne auflösen können. Die DNS-Server der Domäne sollten auf allen Clients eingetragen sein, um den zentralen DNS-Namen, im Normalfall `ucs-sso.`*`domainname`*, auflösen zu können.

Der UCS Identity Provider wird auf dem Domänencontroller Master und Domänencontroller Backup mit der Installation automatisch eingerichtet. Um die Ausfallsicherheit innerhalb der Domäne zu erhöhen, können weitere Systeme der Rolle Domänencontroller Backup verfügbar gemacht werden. Für den ausfallsicheren Zugriff auf den UCS Identity Provider wird standardmäßig der DNS-Eintrag `ucs-sso.`*`domainname`* registriert. Das für diesen Eintrag vorgesehene TLS Zertifikat wird auf allen beteiligten Systemen der Domäne vorgehalten. Es wird empfohlen, das Wurzelzertifikat der UCS Domäne auf allen Rechnern, die *Single Sign-On* nutzen, zu installieren.

Es besteht die Möglichkeit, die SAML-Authentifizierung mit der Kerberos Anmeldung zu verknüpfen. Das bedeutet, dass sich Nutzer mit einem gültigen Kerberos Ticket, bspw. nach einer Anmeldung an Windows oder Linux, ohne eine erneute manuelle Authentifizierung am Identity Provider anmelden können.

Um die Kerberos Authentifizierung am Identity Provider zuzulassen, muss die Univention Configuration Registry-Variable `saml/idp/authsource` von `univention-ldap` auf `univention-negotiate` gesetzt werden. Die Webbrowser müssen entsprechend so konfiguriert werden, so dass das Kerberos Ticket an den SAML Identity Provider übertragen wird. Im folgenden beispielhaft für Firefox und den Internet Explorer / Microsoft Edge:

Mozilla Firefox

In der erweiterten Firefox Konfiguration, diese ist erreichbar über die Eingabe von **about:config** in der Firefox Adresszeile, muss bei der Option **network.negotiate-auth.trusted-uris** die Adresse des Identity Providers eingetragen werden, also in der Standardeinstellung `ucs-sso.`*`domainname`*.

Microsoft Internet Explorer,
Microsoft Edge

In der Systemsteuerung müssen die **Internetoptionen** geöffnet werden und dort wird unter **Sicherheit**, **Lokales Intranet**, **Sites**, **Erweitert** die Adresse des Identity Providers hinzugefügt, also in der Standardeinstellung `ucs-sso.`*`domainname`*.

Die Kerberos Authentifizierung kann auf bestimmte IP Subnetze beschränkt werden, indem die Univention Configuration Registry-Variable `saml/idp/negotiate/filter-subnets` beispielsweise auf `127.0.0.0/16,192.168.0.0/16` gesetzt wird. Dies ist besonders nützlich, um zu verhindern, dass für Clients, die nicht zur UCS-Domäne gehören, ein Dialog für den Login angezeigt wird.

3.9.1. Anmelden per *Single Sign-On*

Feedback

Der *Single Sign-On* ist der Standard-Login für Univention Management Console, sofern `ucs-sso.`*`domainname`* erreicht werden kann. Zum Login werden die Anmeldedaten des Domänenkontos verwendet. Für den Login direkt am UCS-System (also ohne *Single Sign-On*) gelangt man über den Link **Ohne Single Sign-On anmelden**.

Über die Datei `/usr/share/univention-management-console-login/css/custom.css` kann das Design des Anmeldedialogs angepasst werden. Diese Datei wird niemals automatisch überschrieben.

Andere Webdienste leiten ebenfalls auf die Anmeldeseite des UCS Identity Providers weiter, wenn ein *Single Sign-On* durchgeführt wird. Nach erfolgreicher Authentifizierung wird der Benutzer wieder auf die Seite des Webdienstes gesendet werden. Diese Dienste müssen wie in Abschnitt 3.9.2 beschrieben registriert werden.

Der *Single Sign-On* an einem Dienst kann auch vom UCS Identity Provider initiiert werden. Dies erspart den Umweg, zunächst den externen Dienst selbst aufzurufen und sich von dort zur Authentifizierung weiterleiten zu lassen. Dazu muss der Identity Provider mit einem Link der Form `https://ucs-sso.`*`domainname`*`/simplesamlphp/saml2/idp/SSOService.php?spentityid=`*`[Service provider identifier]`* aufgerufen werden.

3.9.2. Hinzufügen eines neuen externen Service Providers

Feedback

Die am UCS Identity Provider registrierten Service Provider können über das UMC Domänen Modul **SAML identity provider** verwaltet werden. Benutzer müssen freigeschaltet werden, bevor sie sich am UCS Identity Provider für einen Dienst authentifizieren können. Service Provider können auch für Gruppen aktiviert werden, sodass sich alle Benutzer in dieser Gruppe für diesen Dienst authentifizieren können. Auf dem *Tab* **Konto** eines Benutzers, oder dem *Tab* **Allgemein** einer Gruppe, muss dazu unter **SAML Einstellungen** der Service Provider Eintrag hinzugefügt werden.

Um den UCS Identity Provider bei einem SAML Service Provider zu registrieren, wird der öffentliche Teil des *SAML-Zertifikats* auf dem Service Provider benötigt. Dieses kann über einen Download-Link im UMC Modul heruntergeladen werden. Andere Service Provider benötigen die *XML-Metadaten* des Identity Providers in Form eines Datei-*Uploads*. In der Standardkonfiguration kann die XML-Datei unter der URL `https://ucs-sso.`*`domainname`*`/simplesamlphp/saml2/idp/metadata.php` heruntergeladen werden.

Die folgenden Attribute können beim anlegen eines neuen Service Provider-Eintrags konfiguriert werden.

Tabelle 3.1. Allgemeine Felder bei der Anbindung eines Service Providers

Attribut	Beschreibung
Service Provider aktivieren	Ist diese Option gesetzt, wird die Konfiguration des Service Providers aktiviert und steht für die Anmeldung bereit.
Bezeichner des Service Providers	Definiert den internen Namen des Service Providers. Dieser wird später an Benutzerobjekt angezeigt und ausgewählt, um Benutzer für die Verbindung freizuschalten. Der Bezeichner kann später nicht mehr geändert werden.
Antwort an diese Service Provider URL nach dem Login	Nach dem erfolgreichen Login an UCS wird der Browser des Benutzers zurück zum Service Provider geleitet. Die Weiterleitung erfolgt an die hier angegebene URL.
Single *logout* URL des Service Providers	Service Provider können einen URL Endpunkt anbieten, mit dem die Session am Service Provider beendet werden kann. Loggt sich der Benutzer am UCS Identity Provider aus, wird über die hier übergebene URL ein *Logout* am Service Provider durchgeführt.
Format des `NameID` Attributs	Der Wert `NameIDFormat`, den der Service Provider erhält. Die Dokumentation des Service Providers sollte erwartete Formate erwähnen. Beispiel: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` oder `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.
Name des Attributs, das als `NameID` verwendet wird	Hier kann das LDAP Attribut eingetragen werden, das für eine eindeutige Identifizierung des Benutzers am Service Provider verwendet wird, beispielsweise `uid`.
Name der Organisation des Service Providers	Der hier eingetragene Wert wird auf der UCS *Single Sign-On*-Login-Seite angezeigt. Dem Benutzer wird so dargestellt, für welchen Dienst er sich authentifiziert.
Beschreibung dieses Service Providers	Der hier eingetragene Wert wird auf der UCS *Single Sign-On*-Login-Seite angezeigt. Hier kann eine längere Beschreibung über den Dienst angegeben werden, der auf der Login Seite in einem eigenen Absatz angezeigt wird.

Tabelle 3.2. Erweiterte Felder bei der Anbindung eines Service Providers

Attribut	Beschreibung
URL zur Datenschutzrichtlinie des Service Providers	Wird hier eine URL eingetragen, wird dem Benutzer ein Link zu dieser Seite auf der UCS Identity Provider-Login-Seite angezeigt.
Erlaube die Übertragung von LDAP Attributen an den Service Provider	Standardmäßig überträgt der UCS Identity Provider nur das auf dem Reiter **Allgemein** angegebene `NameID` Attribut an den Service Provider. Benötigt der Service Provider weitere LDAP-Benutzerattribute, kann diese Checkbox aktiviert werden. Die zu übertragenen Attribute werden dann unter **Liste der zu übermittelnden LDAP Attribute** eingetragen.
Der Wert des `Formatfeldes` für Attribute	Sollen die übertragenen Attribute mit einem besonderen `Formatwert` übertragen werden, kann dieser hier eingetragen werden. Beispiel: `urn:oasis:names:tc:SAML:2.0:nameid-format:transient` oder `urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified`.
Liste der zu übermittelnden LDAP-Attribute	Hier kann jedes zu übertragende LDAP-Attribut eingetragen werden. Zu jedem dieser Attribute können ebenfalls ein oder mehrere Service

Attribut	Beschreibung
	Attribut-Namen im nebenstehenden Feld definiert werden. Diese dienen zur Übersetzung des LDAP Attribut-Namen für den Service-Provider. Mehrere Einträge müssen durch Kommata getrennt werden. Damit der UCS Identity Provider die angegebenen Attribute verarbeiten kann, müssen sie zusätzlich am LDAP Objekt `id=default-saml-idp,cn=univention,`*`base DN`* eingetragen werden. Dort eingetragene LDAP Attribute können vom Identity Provider ausgelesen und übertragen werden.

3.9.3. Erweiterte Konfiguration

Feedback

In manchen Umgebungen kann es erforderlich sein, dass der UCS Identity Provider mehrere logische Identity Provider Instanzen bereitstellt. Die logische Trennung wird erreicht, indem der Identity Provider unterschiedliche URIs als Endpunkt anbietet. Der standardmäßig eingerichtete Endpunkt ist `https://ucs-sso.`*`domainname`*`/simplesamlphp/saml2/idp/metadata.php`. Weitere Einträge können durch das Setzen von Univention Configuration Registry-Variablen in der Form `saml/idp/entityID/supplement/`*`identifier`*`=true` erzeugt werden. Diese müssen auf allen Servern, die den UCS Identity Provider zur Verfügung stellen, gesetzt werden. Typischerweise sind dies der DC Master und alle DC Backup Server. Anschließend muss der `apache2` Dienst neu geladen werden. Um beispielsweise einen weiteren Eintrag unter der URI `https://ucs-sso.`*`domainname`*`/simplesamlphp/`*`secondIDP`*`/saml2/idp/metadata.php` einzurichten, muss die Univention Configuration Registry-Variable `saml/idp/entityID/supplement/secondIDP=true` gesetzt werden.

3.10. OpenID Connect Provider

Feedback

UCS bietet die Möglichkeit, einen OpenID Connect Provider zu installieren, mit dessen Hilfe externe Web-Dienste die Benutzeranmeldung über das OpenID Connect (OIDC) Protokoll an das UCS Identity Management delegieren können. Die OpenID Connect Provider App kann über das App Center installiert werden. Der Dienst wird von der Software Kopano Konnect bereitgestellt.

Die App kann grundsätzlich auf allen Systemrollen installiert werden. Bei einer Installation auf einem UCS System der Rolle Domänencontroller Master oder Domänencontroller Backup wird der OpenID Connect Provider unter dem DNS Eintrag für den *Single Sign-On* verfügbar gemacht, im Normalfall ist dies `ucs-sso.`*`domain.name`*. Wird die App auf einer anderen Systemrolle installiert, kann der Provider statt dessen direkt über den Hostnamen erreicht werden. Es sollte sichergestellt werden, dass die App auf allen Servern installiert ist, die unter dem `ucs-sso` DNS CNAME erreichbar sind. Die Synchronisation von Session Informationen zwischen mehreren Instanzen des OIDC Providers ist nicht vorkonfiguriert. Wenn Login Probleme bei Apps in dieser Konfiguration auftreten, empfehlen wir den OIDC Provider nur auf einem System zu betreiben, und den `ucs-sso` DNS CNAME auf dieses System zu beschränken, oder den Univention Support zu kontaktieren.

Um externe Web-Dienste per OpenID Connect an UCS anzubinden, muss für diesen Dienst ein bestimmtes Objekt des Typs `oidc/rpservice` im UCS Verzeichnisdienst vorhanden sein. Dies kann in der Univention Management Console im LDAP Browser im Container `cn=oidc` angelegt werden, der sich unterhalb des Containers `cn=univention` befindet. Hier kann über den Punkt Hinzufügen und die Auswahl **OpenID Connect Relying Party Service** ein neuer Dienst registriert werden.

Das gleiche ist auch über die Kommandozeile möglich:

```
udm oidc/rpservice create --set name=<UCS_interner_Bezeichner> \
  --position="cn=oidc,cn=univention,$(ucr get ldap/base)" \
  --set clientid=<ClientID> \
```

```
  --set clientsecret=<Ein_langes_Passwort> \
  --set trusted=yes \
  --set applicationtype=web \
  --set redirectURI=<URL_aus_Dokumentation_des_Dienstes>
```

Die Parameter des Aufrufs sind:

`name`

der beim Login im Webinterface angezeigte Dienstname.

`clientid`,
`secret`

müssen hier und beim angebundenen Dienst identisch sein (*shared secret*).

`trusted`

sollte standardmäßig auf `yes` gesetzt werden. Andernfalls wird dem Benutzer eine Bitte um Bestätigung zur Übertragung seiner Benutzerattribute an den Dienst angezeigt.

`applicationtype`

sollte für Internetdienste auf den Wert `web` gesetzt werden.

`redirectURI`

URL des Login-Endpunkts, die in der Dokumentation des jeweiligen angebundenen Dienstes zu finden ist. Ist ein Dienst über mehrere URLs erreichbar oder soll er auch per IP Adresse aufrufbar sein, müssen alle möglichen Adressen zum Attribut `redirectURI` hinzugefügt werden. Das Feld kann daher mehrfach definiert werden, wobei jeder einzelne Wert eine gültige URL enthalten muss.

Der angebundene Web-Dienst braucht für seine Konfiguration noch Informationen über die OpenID Connect Endpunkte der Provider-App. Diese sind bei installierter Provider-App unter der URL `https://ucs-sso.`*`domain.name`*`/.well-known/openid-configuration` einsehbar. Wurde die Provider-App auf einem anderen System als Domänencontroller Master oder Domänencontroller Backup installiert, ist wie oben beschrieben statt `ucs-sso.domain.name` der FQDN des jeweiligen Servers zu verwenden.

Bei der Verwendung von OpenID Connect ist auf korrekte, auflösbare DNS Namen und verifizierbare Zertifikate zu achten. Zu beachten ist dies insbesondere bei Client-Rechnern von Endbenutzern, die sowohl auf die per DNS auflösbaren Hostnamen des Web-Dienst als auch auf den OpenID Connect Provider zugreifen müssen. Außerdem müssen die extern angebundenen Web-Dienste eine Verbindung zum OpenID Connect Provider herstellen können, um darüber die Benutzerattribute abrufen zu können.

Im speziellen Fall, wo der DNS Namen des OIDC-Providers geändert werden soll, muss zunächst der entsprechende Wert in den App Einstellungen der OpenID Connect Provider App angepasst werden. Da es diverse Szenarien für die Erreichbarkeit des Providers nach der Änderung des DNS Namens gibt, kann keine automatische Änderung der Webserverkonfiguration vorgenommen werden. Es muss so zum Beispiel je nach konfiguriertem DNS Namen noch die Apache Konfiguration unter UCS angepasst werden. Die Konfigurationsdatei `/etc/apache2/conf-available/openid-connect-provider.conf` muss unter dem gesetzten DNS Namen in einem Virtual Host verfügbar gemacht werden.

Mit Version 2 der OIDC-Provider App funktioniert die Authentifizierung an OpenID Connect über den SAML Identity Provider der UCS Domäne. Ist der SAML Identity Provider von der Standardkonfiguration abweichend nicht unter `https://ucs-sso.`*`domain.name`* erreichbar, muss in den App Einstellungen die

URL korrekt eingetragen werden, unter der die SAML IdP Metadaten für die UCS Domäne abgerufen werden können. Bei inkorrekter Konfiguration dieser URL startet der OpenID Connect Provider nicht.

Mit der Authentifizierung per SAML ist die Autorisierung für die Nutzung des OpenID Connect Providers und damit zu allen per OIDC angebundenen Apps über SAML Berechtigungen steuerbar. Standardmäßig wird bei der Installation der App die Gruppe `Domänenbenutzer` für den Zugriff freigeschaltet. Wenn diese Berechtigung entfernt werden soll, muss zusätzlich in den App Einstellungen die entsprechende Option aktiviert werden, damit die Berechtigung nicht automatisch erneut hinzugefügt wird.

Der OpenID Connect Provider protokolliert Aktionen über den Docker Daemon. Die Ausgaben können beispielsweise über das Kommando `univention-app logs openid-connect-provider` eingesehen werden.

3.11. Umwandlung eines Domänencontroller Backup zum neuen Domänencontroller Master

Feedback

Eine UCS Domäne hat immer genau einen Domänencontroller Master, kann aber beliebig viele Domänencontroller Backup beinhalten. Ein Domänencontroller Backup speichert alle Domänendaten und alle SSL-Sicherheitszertifikate als Kopie, im Gegensatz zum Domänencontroller Master können jedoch keine schreibenden Änderungen vorgenommen werden.

Jeder Domänencontroller Backup kann zu einem Domänencontroller Master umgewandelt werden. Hierfür gibt es zwei typische Anwendungsfälle:

- Im Notfall nach einem Hardwareausfall des Domänencontroller Master
- Zum geplanten Ersetzen des Domänencontroller Master durch neue Hardware oder Wechsel der Architektur von i386 auf amd64

Achtung

Die Umwandlung eines Domänencontroller Backup in einen Domänencontroller Master ist ein tiefgreifender Konfigurationsschritt und sollte gründlich vorbereitet werden! Die Umwandlung kann nicht rückgängig gemacht werden.

Der zu ersetzende Domänencontroller Master muss vor Beginn der Umwandlung abgeschaltet werden und darf weder während der Umwandlung noch im Anschluss daran wieder in Betrieb genommen werden!

Im Vorfeld muss die installierte Software sowie die aktuelle Konfiguration zwischen Domänencontroller Master und Domänencontroller Backup abgeglichen werden. Wenn der Domänencontroller Master wegen eines Ausfalls nicht mehr verfügbar ist, muss eine Sicherung herangezogen werden. Im Nachgang an die Umwandlung müssen alle evtl. verbliebenen Referenzen auf den alten Domänencontroller Master entfernt bzw. korrigiert werden.

Die Umwandlung umfasst primär die Umstellung der für die Authentifizierung relevanten Dienste wie LDAP, DNS, Kerberos und Samba. Der Abgleich der installierten Software muss manuell erfolgen (über die UMC-Module **App Center** und **Paket-Verwaltung**). Wenn also z.B. auf dem vorherigen DC Master die Mailkomponente installiert war, ist diese nach der Umwandlung nicht automatisch auf dem neuen DC Master verfügbar. Um den Umfang der Nachbereitung möglichst gering zu halten, sollte im Vorfeld Abschnitt 3.12 beachtet werden.

Wurden auf dem Domänencontroller Master zusätzliche LDAP-Schema-Pakete installiert, so müssen diese vor der Umwandlung auch auf dem Domänencontroller Backup installiert werden. Die Paketliste des alten

Domänencontroller Master sollte vor der Umstellung gesichert werden, um einen Abgleich der installierten Pakete zu erlauben. Die Paketliste kann mit dem folgenden Befehl erstellt werden:

```
dpkg --get-selections \* > dpkg.selection
```

Die so auf dem Domänencontroller Master erstellte Datei sollte mit einer ebenso erstellten Datei des Domänencontroller Backup verglichen und benötigte Pakete auf dem Domänencontroller Backup nachinstalliert werden. Insbesondere alle Pakete, die ein LDAP-Schema installieren sind zwingend erforderlich. Eine Auflistung dieser LDAP-Schema-Pakete lässt sich wie folgt erstellen:

```
ls -1 /etc/ldap/schema/*.schema /usr/share/univention-ldap/schema/
*.schema | xargs dpkg -S
```

Um einfach alle installierten Pakete des Domänencontroller Master auch auf dem Domänencontroller Backup zu installieren, kann die zuvor auf dem Domänencontroller Master erstellte Datei `dpkg.selection` mit folgenden Befehlen verwendet werden:

```
dpkg --set-selections < dpkg.selection
apt-get dselect-upgrade
```

Darüber hinaus sollte der Univention Configuration Registry-Datenbestand gesichert werden, um Konfigurationsanpassungen auch auf dem neuen Domänencontroller Master abgleichen zu können. Folgende Dateien des Domänencontroller Master sind dazu mit denen auf dem Domänencontroller Backup zu vergleichen:

```
/etc/univention/base.conf
/etc/univention/base-forced.conf
```

Eine nächtliche Sicherung dieser Dateien findet sich auch in `/var/univention-backup/ucr-backup_%Y%m%d.tgz`

Die Umwandlung eines Domänencontroller Backup zum neuen Domänencontroller Master erfolgt dann durch Aufruf des Befehls `/usr/lib/univention-ldap/univention-backup2master` auf dem Domänencontroller Backup. Das System muss anschließend neu gestartet werden. Die Umstellung wird in der Logdatei `/var/log/univention/backup2master.log` protokolliert.

Folgende Schritte führt der Befehl `univention-backup2master` der Reihe nach aus:

- Prüfung der Umgebung: Bei dem System muss es sich um einen Domänencontroller Backup handeln, der der Domäne bereits beigetreten ist. Zudem wird sichergestellt, dass der Domänencontroller Master über DNS auflösbar sowie dass eine Verbindung zum Repository-Server möglich ist. Außerdem darf der Domänencontroller Master nicht mehr im Netzwerk erreichbar sein.

- Nun werden die wichtigsten Dienste OpenLDAP, Samba, Kerberos sowie Univention Directory Notifier und Listener gestoppt, elementare Univention Configuration Registry-Variable wie `ldap/master` und `server/role` umgestellt, das UCS Root-Zertifikat vom Webserver des Domänencontroller Backup abrufbar gemacht und die oben genannten Dienste wieder gestartet.

- Der DNS SRV Eintrag `kerberos-adm` wird vom alten auf den neuen Domänencontroller Master geändert

- Sofern vorhanden, wird der Univention S4 Connector (siehe Abschnitt 9.2.2.4) vom Rechnerobjekt des alten Domänencontroller Master entfernt und auf dem neuen Domänencontroller Master zur erneuten Konfiguration vorgemerkt.

- Im OpenLDAP wird die Serverrolle des neuen Domänencontroller Master auf `domaincontroller_master` geändert. Ebenfalls wird der DNS SRV Eintrag `_domaincontroller_master._tcp` korrigiert.

- Sofern vorhanden werden die Einträge des alten Domänencontroller Master aus der lokalen Samba-Datenbank des neuen Domänencontroller Master entfernt. Zudem werden die FSMO-Rollen auf den neuen Domänencontroller Master übertragen.
- Anschließend wird das Rechnerobjekt des alten Domänencontroller Master im OpenLDAP gelöscht.
- Nun wird das LDAP nach Referenzen auf den alten Domänencontroller Master durchsucht. Alle gefundenen Referenzen werden angezeigt und es wird eine Korrektur vorgeschlagen, welche einzeln geprüft und bestätigt werden muss, bspw. weitere DNS-Einträge.
- Zum Abschluss wird das Paket ***univention-server-backup*** durch ***univention-server-master*** ersetzt.

Im Anschluss sollte sowohl Univention Configuration Registry auf allen UCS-Systemen der Domäne als auch das LDAP auf dem jetzt neuen Domänencontroller Master hinsichtlich Verweisen auf den Namen und die IP-Adresse des alten Domänencontroller Master überprüft und diese ggf. angepasst werden.

3.12. Fehlertolerante Domain Einrichtung

Feedback

Einige Dienste in einer Domäne sind zentral für das Funktionieren von deren Mitgliedern. Redundanz ist ein Mittel um diesen potenziellen Bruchstellen (*single points of failure*) zu entfernen. Ein Artikel in der Univention Support Datenbank erklärt das Vorgehen um die Dienste LDAP, Kerberos, DNS, DHCP und Active Directory-kompatible Domain Controller abzusichern: SDB 1349[1].

3.13. Protokollierung von Aktivitäten in der Domäne

Feedback

Über die *Admin Diary*-App besteht die Möglichkeit, wichtige Ereignisse in der Domäne zu protokollieren. Dazu gehören unter anderem:

- Das Anlegen, Verschieben, Verändern oder Löschen von Benutzern und anderen Objekten über Univention Directory Manager
- Installation, Update und Deinstallation von Apps
- Server-Passwort-Änderungen
- Start, Ende und eventuelle Fehlschläge vom Domänenbeitritt
- Start und Ende von UCS Updates

[1] http://sdb.univention.de/1349

Abbildung 3.5. Ansicht der Ereignisse im *Admin Diary*

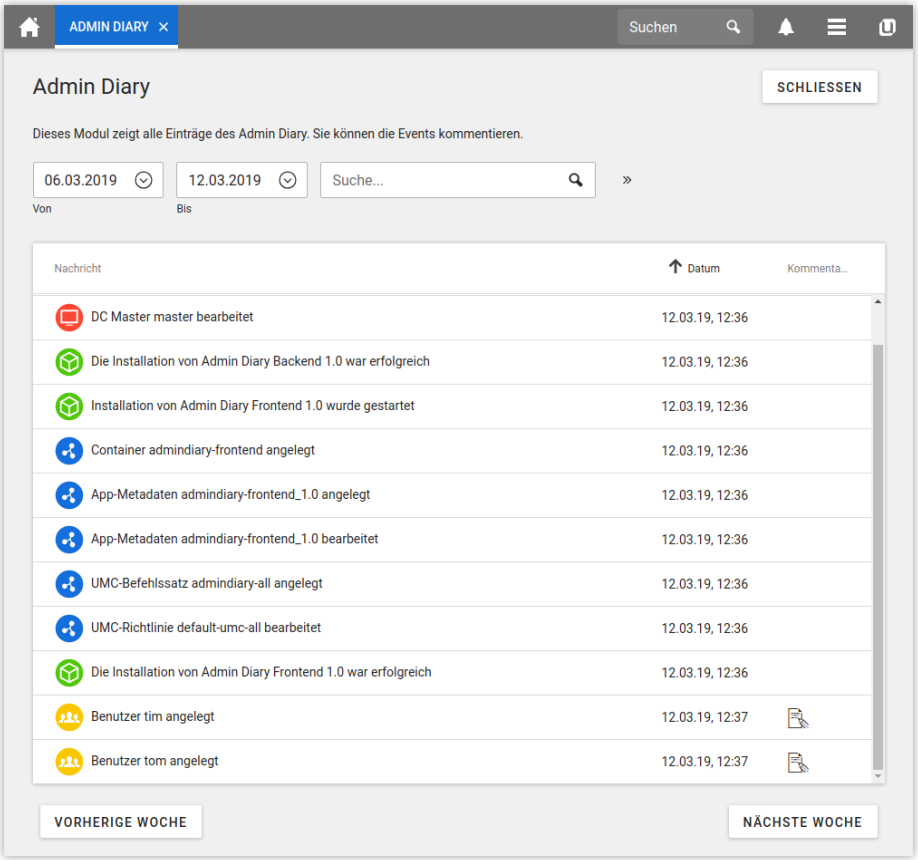
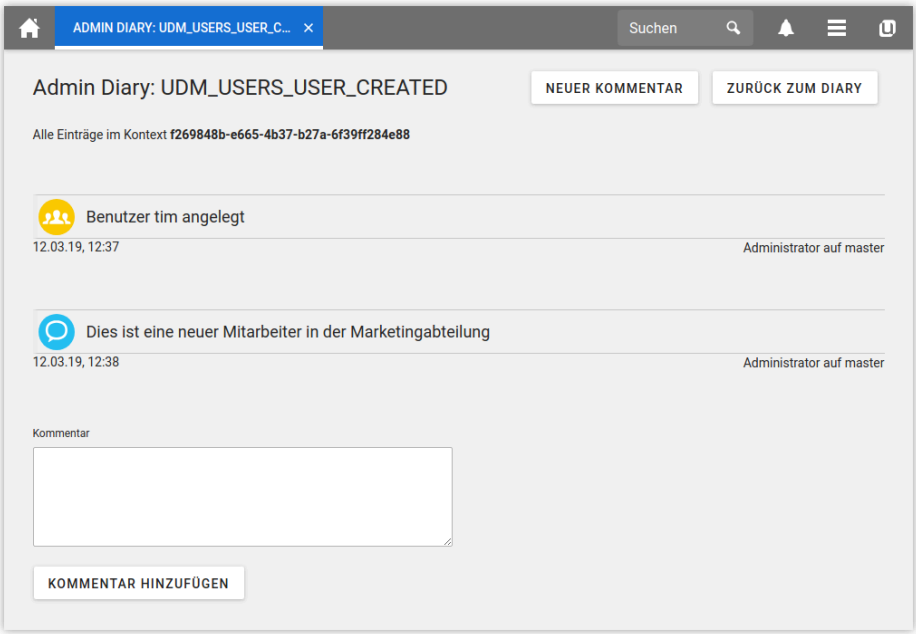


Abbildung 3.5 zeigt, wie die Ereignisse in der Univention Management Console dargestellt werden. Die angezeigten Einträge werden standardmäßig wochenweise gruppiert und können über das Suchfeld weiter eingegrenzt werden. Durch das Auswählen eines Eintrags gelangt man zu einer Detailansicht, wie sie in Abbildung 3.6 zu sehen ist. Dieser kann man weitere Details zum Wo und Wann entnehmen. Zudem besteht die Möglichkeit, das Ereignis zu kommentieren.

Abbildung 3.6. Detailansicht im *Admin Diary*



Die App besteht aus zwei Komponenten:

Admin Diary Backend

Das Backend muss auf einem System in der Domäne installiert sein, bevor das Frontend installiert werden kann. Es beinhaltet eine Anpassung für ***rsyslog*** und schreibt in eine zentrale Datenbank, standardmäßig PostgreSQL. Falls MariaDB oder MySQL vorher auf dem Zielsystem installiert ist, dann wird es statt PostgreSQL verwendet.

Admin Diary Frontend

Auch das Frontend muss mindestens einmal installiert sein, kann aber öfter installiert werden. Das Frontend beinhaltet das Univention Management Console Modul, um die Einträge anzuzeigen und zu kommentieren. Wenn es nicht auf dem selben System installiert werden soll, auf dem das Backend läuft, dann muss der Zugriff auf die zentrale Datenbank manuell eingerichtet werden. Die dazu notwendigen Schritte sind in einem separaten Artikel[2] beschrieben.

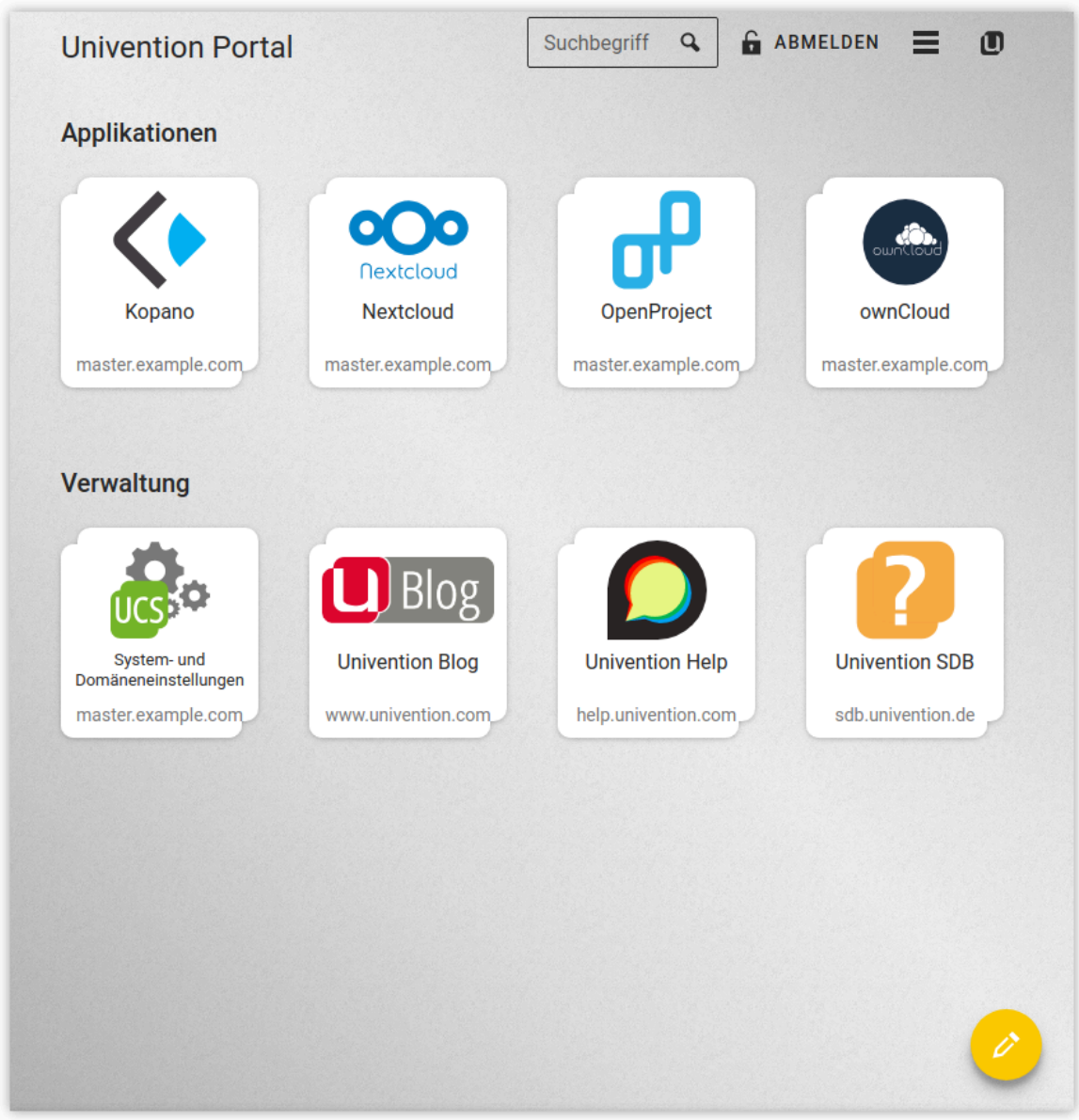
[2] https://help.univention.com/t/admin-diary-how-to-seperate-frontend-and-backend/11331

univention
be open.

Kapitel 4. UCS Web-Oberfläche

4.1. Einführung

Abbildung 4.1. UCS Portalseite



Die UCS Web-Oberfläche ist das zentrale Werkzeug zur Verwaltung der UCS-Domäne sowie für den Zugriff auf installierte Applikationen derselben.

Die UCS Web-Oberfläche untergliedert sich in mehrere Unterseiten, die alle eine ähnlich gestaltete Kopfzeile besitzen. Über die Symbole oben rechts kann eine Suche auf der aktuellen Seite durchgeführt (Lupe), sich angemeldet/abgemeldet (Schloss) oder das Benutzermenü (drei Balken) geöffnet werden. Die Anmeldung an der Oberfläche geschieht über eine zentrale Seite für alle Unterseiten von UCS sowie Drittherstellern, sofern diese einen webbasierten *Single Sign-on* unterstützen (Abschnitt 4.2).

Zentraler Ausgangspunkt für Benutzer sowie Administratoren für alle weiteren Operationen ist die UCS-Portalseite (siehe Abbildung 4.1). Die Portalseite ist standardmäßig auf dem Domänencontroller Master verfügbar und erlaubt einen Überblick über alle in der UCS-Domäne installierten Apps und weiteren Dienste. Alle

anderen Systemrollen zeigen standardmäßig zum einen die jeweils lokal auf dem System verfügbaren Apps und zum anderen einen Verweis zurück auf die Portalseite des Domänencontroller Master an. Alle Aspekte der Portalseite können umfangreich an die eigenen Bedürfnisse angepasst werden (Abschnitt 4.3).

Für Umgebungen mit mehr als einem Server ist auf der Portalseite ein Verweis auf eine Serverübersichtseite zu sehen. Diese Unterseite gibt einen Überblick über alle in der Domäne verfügbaren UCS-Systeme. Sie erlaubt die schnelle Navigation hin zu anderen Systemen, um dort bspw. über Univention Management Console Anpassungen an lokalen Einstellungen vorzunehmen.

Univention Management Console (UMC) ist das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne, dessen generelle Funktionsweise in Abschnitt 4.4 beschrieben wird. Für die Administration der unterschiedlichen Aspekte einer Domäne werden verschiedene Module bereit gestellt. Diese sind je nach Systemrolle verfügbar und werden bei Installation weiterer Software-Komponenten durch neue UMC-Module ergänzt.

Die anschließenden Abschnitte vertiefen die Benutzung einzelner Aspekte der Domänenverwaltung. Abschnitt 4.5 gibt einen Überblick über den LDAP-Verzeichnis-Browser. Die Anwendung von administrativen Einstellungen über Richtlinien wird in Abschnitt 4.6 besprochen. Wie genau der Funktionsumfangs der Domänenverwaltung erweitert werden kann ist in Abschnitt 4.7 beschrieben. Abschnitt 4.8 vertieft, wie Container und Organisationseinheiten (OU) zur Strukturierung des LDAP-Verzeichnisses genutzt werden können. Abschnitt 4.9 erläutert das Delegieren von Administrationsrechten an weitere Benutzergruppen.

Abschließend wird die Kommandozeilenschnittstelle der Domänenverwaltung dargestellt (Abschnitt 4.10) und das Auswerten von Domänendaten über die UCS-Reporting-Funktionalität erläutert (Abschnitt 4.12).

4.1.1. Zugriff

Feedback

Auf jedem UCS-System kann die UCS Web-Oberfläche über die URL `https://servername/` aufgerufen werden. Alternativ ist der Zugriff auch über die IP-Adresse des Servers möglich. Unter besonderen Umständen kann es nötig sein, über eine ungesicherte Verbindung auf die Dienste zuzugreifen (z.B. wenn für das System noch keine SSL-Zertifikate erstellt worden sind). In diesem Fall muss in der URL `http` statt `https` verwendet werden. Passwörter werden in diesem Fall im Klartext über das Netzwerk gesendet!

4.1.2. Browserunterstützung

Feedback

Die UCS Web-Oberfläche verwendet für die Darstellung zahlreiche JavaScript- und CSS-Funktionen. Cookies müssen im Browser zugelassen sein. Die folgenden Browser werden unterstützt:

- Chrome ab Version 71
- Firefox ab Version 60
- Microsoft Edge ab Version 18
- Safari und Safari Mobile ab Version 12

Auf älteren Browsern können Darstellungsprobleme auftreten.

Die UCS Web-Oberfläche ist in Deutsch und Englisch verfügbar (und Französisch wenn dieses bei der Installation von DVD als Sprache ausgewählt wurde); die Darstellungssprache kann über den Punkt **Sprache ändern** im Benutzermenü der rechten, oberen Ecke geändert werden.

4.1.3. Feedback zu UCS

Feedback

Durch die Auswahl des Menüeintrages **Hilfe -> Feedback** in dem oberen, rechten Benutzermenü kann über ein Webformular Feedback zu UCS gegeben werden.

4.1.4. Erfassung von Nutzungsstatistiken

Feedback

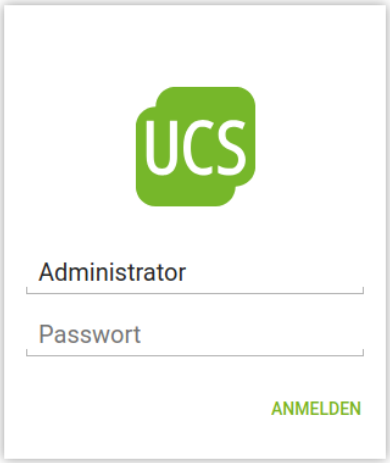
Bei Verwendung der *Core Edition* von UCS werden anonyme Nutzungsstatistiken zur Verwendung der UCS Web-Oberfläche erzeugt. Weitere Informationen finden sich in SDB 1318.

4.2. Anmeldung

Feedback

UCS stellt eine zentral Anmeldeseite zur Verfügung. Die Anmeldung an der UCS Web-Oberfläche geschieht zentral mit den Anmeldedaten des jeweiligen Domänenkontos. Auf der Portalseite kann der Anmeldevorgang entweder über das Benutzermenü und dann **Anmelden** (letzter Eintrag) oder über einen Klick auf das Schlosssymbol in der Kopfzeile oben rechts angestoßen werden. Setzt eine Seite (wie bspw. Univention Management Console) eine Anmeldung voraus, so wird automatisch auf die zentrale Anmeldeseite weitergeleitet. Zum Abmelden kann analog entweder auf das (geöffnete) Schlosssymbol in der Kopfzeile geklickt oder der Eintrag **Abmelden** im Benutzermenü (letzter Eintrag) ausgewählt werden.

Abbildung 4.2. UCS Anmeldeseite



Standardmäßig wird ein *Single Sign-On* (SSO) mittels SAML (siehe auch Abschnitt 3.9) durchgeführt, sofern `ucs-sso.`*`domainname`* erreicht werden kann. Nach erfolgter Anmeldung ist eine Sitzung gültig für alle UCS-Systeme der Domäne sowie Apps von Drittherstellern, wenn diese einen webbasierten SSO unterstützen. Kann `ucs-sso.`*`domainname`* nicht erreicht werden, geschieht die Anmeldung an dem lokalen UCS-System. Die Sitzung ist dann nur gültig für die UCS Webseiten auf dem selben System. Es ist möglich die Anmeldung am lokalen System über den Link **Ohne Single Sign-On anmelden** zu erzwingen.

In der Anmeldemaske werden **Benutzername** und **Passwort** des gewünschten Domänenkontos angegeben:

- Bei der Anmeldung mit dem `Administrator`-Konto auf Domänencontroller Master oder Domänencontroller Backup werden UMC-Module zur Verwaltung und Konfiguration des lokalen Systems sowie UMC-Module zur Verwaltung der Daten des LDAP-Verzeichnisses bereitgestellt. Das initiale Passwort dieses Kontos wurde im Einrichtungsassistent bei der Installation angegeben und stimmt mit dem initialen Passwort des lokalen `root`-Kontos überein. `Administrator` ist auch das Konto, mit dem die erste Anmeldung an einem neu installierten Domänencontroller Master-System durchgeführt werden sollte.

- In einigen Fällen kann es notwendig sein, eine Anmeldung mit dem lokalen `root`-Konto des Systems durchzuführen (siehe Abschnitt 8.4.1). Dieses Konto ermöglicht lediglich den Zugriff auf UMC-Module zur Verwaltung und Konfiguration des lokalen Systems.

http://sdb.univention.de/1318

- Bei der Anmeldung mit einem anderen Benutzerkonto werden die für diesen Benutzer freigeschalteten UMC-Module angezeigt. Weitere Informationen zur Freigabe von Modulen findet sich in Abschnitt 4.9.

Die Dauer einer Browser-Sitzung beträgt 8 Stunden bei Anmeldung über SSO, danach ist eine erneute Anmeldung erforderlich. Bei Anmeldung am lokalen UCS-System wird die Browser-Sitzung nach 8 Stunden Inaktivität automatisch geschlossen.

Es besteht die Möglichkeit durch die Installation von Drittanbietern Software, bspw. privacyIDEA, die Univention Management Console Anmeldung um eine Zwei-Faktor-Authentifizierung (2FA) zu ergänzen. Diese Erweiterungen können aus dem Univention App Center installiert werden.

4.3. UCS Portalseite

Feedback

Die Portalseiten dienen der zentralen Darstellung aller verfügbaren Dienste in einer UCS-Domäne. Da sich die Anforderung von kleinen bis hin zu großen Umgebungen in Organisationen, Behörden oder auch im Schulbetrieb stark voneinander unterscheiden, bringt UCS ein sehr flexibles und individuell anpassbares Konzept für Portalseiten mit.

Wie in Abbildung 4.3 dargestellt, können Portaleinträge (also Verweise auf Applikationen/Apps/Dienste; UDM-Objekttyp `settings/portal_entry`) keinem, einem oder mehreren Portalen zugeordnet sein. Ein Portal selbst (UDM-Objekttyp `settings/portal`) stellt alle Einträge dar, die mit ihm verknüpft sind. Ein Portal kann keinem, einem oder mehreren Rechnerobjekten zugewiesen sein (dies geschieht direkt am Rechnerobjekt selber).

Standardmäßig ist UCS so voreingestellt, dass es zwei Portale gibt. Das Portal *domain* ist mit den Domänencontroller Master und Backup Systemen der Domäne verknüpft. Neben allen installierten Applikationen in der Domäne werden hier auch Verweise zu Univention Management Console sowie zur Serverübersicht angezeigt. Das Portal *local* ist allen anderen Rechnerrollen in der Domäne zugewiesen. Hier wird neben den lokal installierten Apps ein Verweis auf die lokal verfügbare Univention Management Console Instanz sowie ein Verweis zurück auf den Domänencontroller Master der Domäne dargestellt.

Eigene Portale und Portaleinträge können entweder über das UMC-Modul **Portaleinstellungen** oder direkt auf der Portalseite angelegt und verwaltet werden.

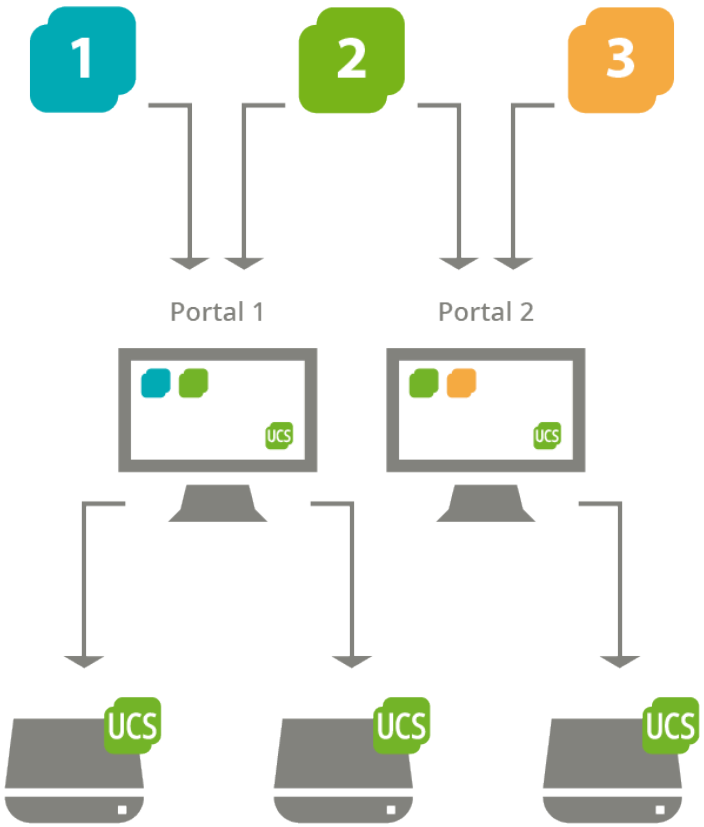
Mitglieder der Gruppe `Domain Admins` können nach der Anmeldung am Portal auf dem DC Master oder DC Backup nach einem Klick auf das gelbe Bearbeitungs-Icon neue Einträge auf dem Portal erstellen, vorhandene Einträge modifizieren, sowie die Reihenfolge oder das Design modifizieren. Es ist darüber hinaus möglich, diese Rechte auf ausgewählte Gruppen oder Benutzer zu übertragen. Hierzu gibt es eine Anleitung unter Abschnitt 4.3.1

Weiterführende Einstellungen, wie das Hinzufügen neuer Portale oder die Einstellung, welche Gruppenmitglieder welche Portaleinträge sehen dürfen, können über das UMC-Modul Portaleinstellungen durchgeführt werden.

Standardmäßig werden alle Portaleinträge für jeden angezeigt. Im UMC-Modul **Portaleinstellungen** kann pro Portal auf dem Reiter **Anonyme Besucher verwalten** konfiguriert werden, ob anonyme Besucher sich erst anmelden müssen bevor sie Einträge sehen können. Es ist auch möglich bestimmte Einträge für bestimmte Gruppen zu limitieren. Dies erfordert das LDAP-Attribut *memberOf*. Eine Auswertung von verschachtelten Gruppenmitgliedsschaften (also Gruppen in Gruppen) findet nicht statt.

Weiterführende Design Anpassungen können in der Datei `/usr/share/univention-portal/custom.css` vorgenommen werden. Dieses Datei wird während eines Updates nicht überschrieben.

Abbildung 4.3. Schema des Portal-Konzepts in UCS: Portale können frei definiert und UCS-Systemen als Startseite zugewiesen werden; ein Verweis kann auf mehreren Portalen angezeigt werden.



4.3.1. Rechte für Portaleinstellungen vergeben

Feedback

Im Folgenden wird beschrieben, wie das UMC-Modul **Portaleinstellungen** für ausgewählte Gruppen oder Benutzer zugänglich gemacht werden kann. Dies wird anhand eines Beispiels erläutert. Für das Beispiel wird davon ausgegangen, dass eine Gruppe **Portal Admins** erstellt wurde und Mitglieder dieser Gruppe Zugang zu den Portaleinstellungen haben sollen.

Auf einem **Domaincontroller-Master-System** ist zunächst eine ACL-Datei zu erstellen (für das Beispiel wurde das Verzeichnis **/opt/** verwendet):

```
/opt/62my-portal-acl.acl
```

Diese Datei hat folgenden Inhalt aufzuweisen, um die nötigen ACL-Änderungen zu ermöglichen:

```
access to dn="cn=portal,cn=univention,@%@ldap/base@%@" attrs=children
  by group/univentionGroup/uniqueMember="cn=Portal Admins,cn=groups,@
%@ldap/base@%@" write
  by * +0 break

access to dn.children="cn=portal,cn=univention,@%@ldap/base@%@"
 attrs=entry,@univentionObject,@univentionPortalEntry,
@univentionPortal,@univentionPortalCategory,children
  by group/univentionGroup/uniqueMember="cn=Portal Admins,cn=groups,@
%@ldap/base@%@" write
```

```
  by * +0 break
```

Danach ist folgender Befehl auszuführen, um ein LDAP-Objekt für die LDAP-ACLs zu erzeugen:

```
udm settings/ldapacl create \
 --position "cn=ldapacl,cn=univention,$(ucr get ldap/base)" \
 --set name=62my-portal-acl \
 --set filename=62my-portal-acl \
 --set data="$(bzip2 -c /opt/62my-portal-acl.acl | base64)" \
 --set package="62my-portal-acl" \
 --set packageversion=1
```

Wenn die ACL wieder gelöscht werden soll, kann folgender Befehl verwendet werden:

```
udm settings/ldapacl remove \
 --dn "cn=62my-portal-acl,cn=ldapacl,cn=univention,$(ucr get ldap/base)"
```

Über die UMC kann nun eine passende UMC-Richtlinie angelegt werden. Die folgenden **UMC-Operationen** müssen dafür innerhalb der Richtlinie erlaubt werden: **udm-portal**, **udm-syntax**, **udm-validate** und **udm-license**. Wie man eine Richtlinie anlegt, ist unter Abschnitt 4.6.1 beschrieben. Nun muss die neu erstellte Richtlinie nur noch dem gewünschten Objekt, in diesem Fall der Gruppe **Portal Admins**, zugewiesen werden. Dies kann ebenfalls direkt innerhalb der UMC erfolgen. Für dieses Beispiel navigiert man dafür in das Gruppenmodul und editiert dort die gewünschte Gruppe. In den Gruppeneinstellungen können unter **Richtlinien** für das Gruppenobjekt vorhandene Richtlinien ausgewählt werden. Genauere Informationen über Richtlinienzuweisung sind unter Abschnitt 4.6.2 beschrieben.

4.4. Univention Management Console

Feedback

4.4.1. Einführung

Feedback

Univention Management Console (UMC) ist das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne. Der Aufruf erfolgt von der Portalseite aus (Abschnitt 4.3) über den Link **System- und Domäneneinstellungen**, bzw. über den Link **Systemeinstellungen**. Je nach Systemrolle stehen unterschiedliche UMC-Module für die Administration von UCS zur Verfügung und werden bei Installation weiterer Software-Komponenten durch neue Module ergänzt.

UMC-Module zur Verwaltung aller im LDAP-Verzeichnis vorgehaltenen Daten (wie z.B. Benutzer, Gruppen oder Rechnerkonten) werden lediglich auf Domänencontroller Master und Domänencontroller Backup bereitgestellt. Änderungen, die in diesen Modulen vorgenommen werden, gelten für die gesamte Domäne.

UMC-Module zur Konfiguration und Administration des lokalen Systems werden auf allen Systemrollen bereitgestellt. Über diese Module können bspw. zusätzliche Applikationen installiert, Aktualisierungen eingespielt, die lokale Konfiguration über Univention Configuration Registry angepasst oder Dienste gestartet/gestoppt werden.

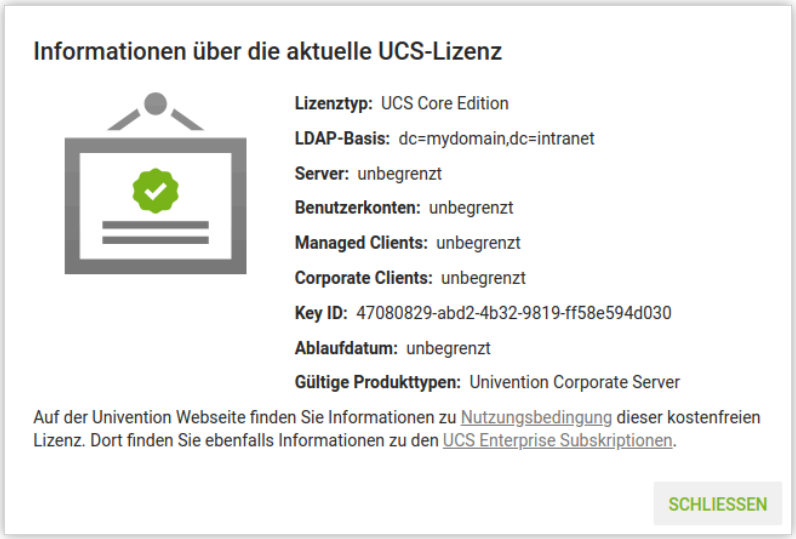
Bei der ersten Anmeldung wird ein Einführungsassistent angezeigt, der u.a. auf die Erfassung von Nutzungsstatistiken hinweist (siehe Abschnitt 4.1.4) und die Aktivierung der Lizenz anbietet (siehe Abschnitt 4.4.2).

4.4.2. Aktivierung der UCS-Lizenz / Lizenz-Übersicht

Feedback

Der momentane Lizenzierungszustand kann auf dem Domänencontroller Master einer Domäne über das Benutzermenü in der oberen, rechten Bildschirmzeile eingesehen werden. Unterhalb des Menüpunktes **Lizenz** kann der Punkt **Lizenzinformation** ausgewählt werden, um einen entsprechenden Informationsdialog zu öffnen.

Abbildung 4.4. Anzeige der UCS-Lizenz



Der Menüpunkt **Neue Lizenz importieren** öffnet einen Dialog, über den ein neuer UCS-Lizenzschlüssel aktiviert werden kann (ansonsten greift die standardmäßig installierte Core-Edition-Lizenz). Über die Schaltfläche **Importieren aus Datei...** kann eine Lizenz-Datei ausgewählt und importiert werden. Alternativ kann der Lizenz-Schlüssel auch in das darunter liegende Eingabefeld kopiert und dann über der Schaltfläche **Importieren aus Textfeld** eingespielt werden.

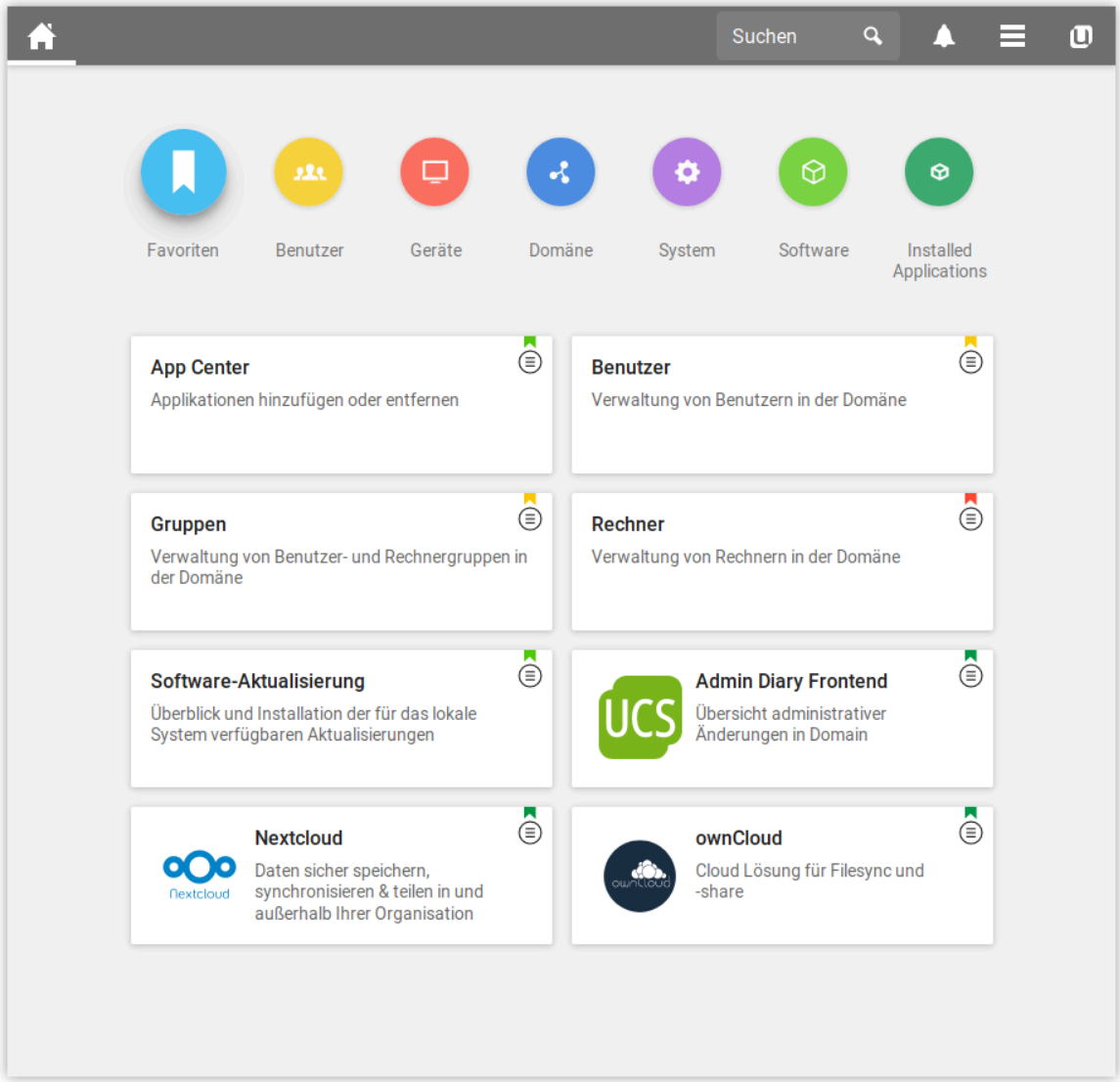
Die Installation der meisten Anwendungen aus dem Univention App Center erfordert einen individuell ausgestellten Lizenzschlüssel mit eindeutiger Schlüsselidentifikation. UCS-Core-Edition-Lizenzen können durch Klick auf die Schaltfläche **Aktivierung von UCS** aktualisiert werden. Der aktuelle Lizenzschlüssel wird dabei an Univention geschickt und der aktualisierte Schlüssel nach einigen Minuten an eine angegebene E-Mail-Adresse versendet. Der neue Schlüssel kann dann direkt eingespielt werden. Der Lizenzumfang bleibt durch die Konvertierung unverändert.

Ist die Anzahl der lizenzierten Benutzer- oder Rechner-Objekte überschritten, können keine weiteren Objekte in Univention Management Console angelegt oder bestehende editiert werden, solange keine erweiterte Lizenz eingespielt wird oder nicht mehr benötigte Benutzer oder Rechner entfernt werden. Auf der UMC-Startseite wird bei überschrittener Lizenz ein entsprechender Hinweis angezeigt.

4.4.3. Bedienung der Module zur Verwaltung von LDAP-Verzeichnisdaten

Alle UMC-Module zur Verwaltung von LDAP-Objekten wie bspw. Benutzer-, Gruppen- und Rechnerkonten oder Einstellungen für Drucker, Freigaben, Mail, Nagios und Richtlinien werden strukturell identisch bedient. Die folgenden Beispiele werden anhand der Benutzerverwaltung dargestellt, gelten aber analog für alle Module. Die Bedienung der DNS- und DHCP-Module weicht etwas ab, weitere Hinweise finden sich in Abschnitt 11.2.2 und Abschnitt 11.3.2.

Abbildung 4.5. Modulübersicht in Univention Management Console



Die inhaltlichen Eigenschaften/Konfigurationsmöglichkeiten der Module ist in folgenden Kapiteln beschrieben:

- Benutzer - Kapitel 6
- Gruppen - Kapitel 7
- Rechner - Kapitel 8
- Netzwerke - Abschnitt 11.1
- DNS - Abschnitt 11.2
- DHCP - Abschnitt 11.3
- Freigaben - Kapitel 12
- Drucker - Kapitel 13

- E-Mail - Kapitel 14
- Nagios - Abschnitt 15.3

Die Verwendung von Richtlinien (Abschnitt 4.6) und des direkten Durchsuchens des LDAP-Verzeichnisbaums (Abschnitt 4.5) wird separat beschrieben.

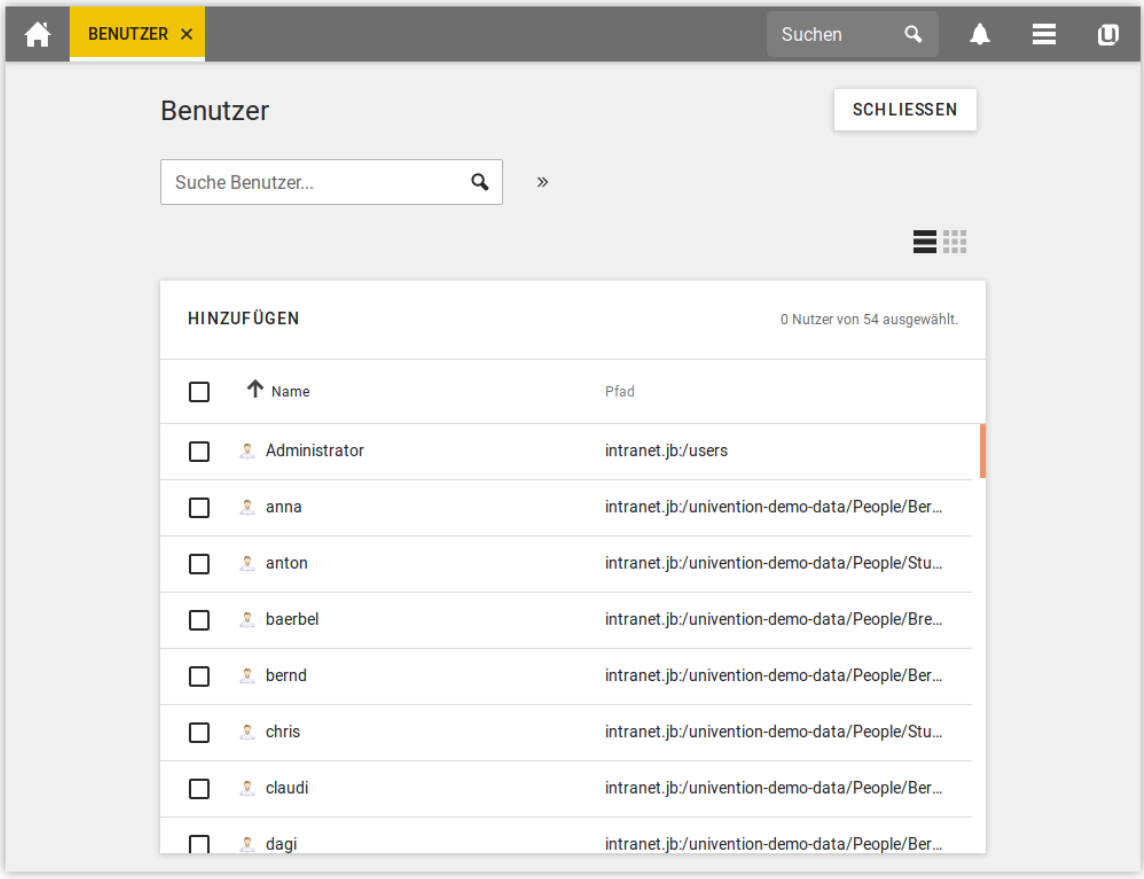
4.4.3.1. Suche nach Objekten

In der Modul-Übersicht werden alle von diesem Modul verwalteten Objekte aufgeführt. Mit **Suche** erfolgt eine Suche über eine Auswahl wichtiger Attribute (z.B. für Benutzerobjekte nach Vor- und Nachname, primärer E-Mail-Adresse, Beschreibung, Mitarbeiternummer und Benutzername). Es kann auch mit Wildcards gesucht werden, z.B. *m**.

Durch Klick auf **Erweiterte Optionen** werden weitere Suchoptionen angezeigt:

- Mit dem Auswahlfeld **Suche in** kann bestimmt werden, ob bei der Suche nach LDAP-Objekten das komplette LDAP-Verzeichnis oder nur einzelne LDAP-Container/OUs durchsucht werden. Weitere Informationen zur Strukturierung des LDAP-Verzeichnisdienstes finden sich in Abschnitt 4.8.
- Über das Auswahlfeld **Eigenschaft** kann gezielt nach einem bestimmten Attribut gesucht werden.
- Die meisten Module verwalten mehrere verschiedene Arten von LDAP-Objekten; die Rechnerverwaltung z.B. verwaltet verschiedene Objekte für die einzelnen Systemrollen. Die Suche kann auf eine Art von LDAP-Objekt beschränkt werden.
- Einige nur intern verwendete Benutzer und Gruppen (z.B. für den Domänenbeitritt) werden standardmäßig ausgeblendet. Wird die Option **Versteckte Objekte anzeigen** aktiviert, werden diese Objekte ebenfalls angezeigt.

Abbildung 4.6. Suche nach Benutzern



4.4.3.2. Anlegen von Objekten

Feedback

In der Zeile über der Tabelle mit den Objekten findet sich eine Aktionsleiste, über die mit **Hinzufügen** ein neues Objekt angelegt werden kann.

Für einige UMC-Module (Benutzer, Rechner) existieren vereinfachte Assistenten, in denen nur die wichtigsten Einstellungen abfragt werden. Durch einen Klick auf **Erweitert** werden alle Attribute angezeigt.

4.4.3.3. Bearbeiten von Objekten

Feedback

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von **Bearbeiten** kann ein Objekt bearbeitet werden. Die einzelnen Attribute sind in den entsprechenden Dokumentations-Kapiteln beschrieben. Ein Klick auf das Diskettensymbol in der farbigen Modulleiste übernimmt alle vorgenommenen Anpassungen in das LDAP-Verzeichnis. Das X-Symbol bricht die Bearbeitung ab und kehrt zur vorherigen Suchansicht zurück.

Vor jedem Eintrag in der Ergebnisliste ist ein Auswahlfeld, mit dem einzelne Objekte ausgewählt werden können. In der unteren Bildzeile wird der Auswahlstatus zusätzlich dargestellt, z.B. **2 Benutzer von 102 sind ausgewählt**. Ist mehr als ein Objekt selektiert, wird nach einem Klick auf den stilisierten Stift in der Auswahlstatusleiste der Mehrfachbearbeitungs-Modus aktiviert. Hierbei werden dieselben Attribute angezeigt wie bei der Bearbeitung eines einzelnen Objekts, Änderungen werden aber nur für die Objekte übernommen, bei denen der **Überschreiben**-Haken aktiviert wird. Es können nur Objekte gleichen Typs bearbeitet werden.

4.4.3.4. Löschen von Objekten

Feedback

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von **Löschen** wird das Objekt nach Bestätigung einer Rückfrage gelöscht. Einige Objekte verwenden interne Referenzen - z.B. kann zu Rechner-Objekten ein DNS-

oder DHCP-Objekt assoziiert werden. Diese können durch Auswahl der Option **Zugehörige Objekte löschen** ebenfalls entfernt werden.

Analog zur Auswahl mehrerer Objekte bei der Bearbeitung von Objekten können auch mehrere Objekte auf einmal entfernt werden.

4.4.3.5. Verschieben von Objekten

Feedback

Durch Rechtsklick auf ein LDAP-Objekt und Auswahl von **Verschieben nach...** kann eine LDAP-Position ausgewählt werden, an die das Objekt verschoben werden soll.

Analog zur Auswahl mehrerer Objekte bei der Bearbeitung von Objekten können auch mehrere Objekte auf einmal verschoben werden.

4.4.4. Favoriten

Feedback

Häufig benutzte UMC-Module werden in der Kategorie **Favoriten** angezeigt. Über einen Klick mit der rechten Maustaste auf ein UMC-Modul wird ein Kontextmenü angezeigt. Mit **Zu Favoriten hinzufügen**, bzw. **Aus Favoriten entfernen** kann ein UMC-Modul als Favorit markiert oder wieder entfernt werden.

4.4.5. Anzeige von Systembenachrichtigungen

Feedback

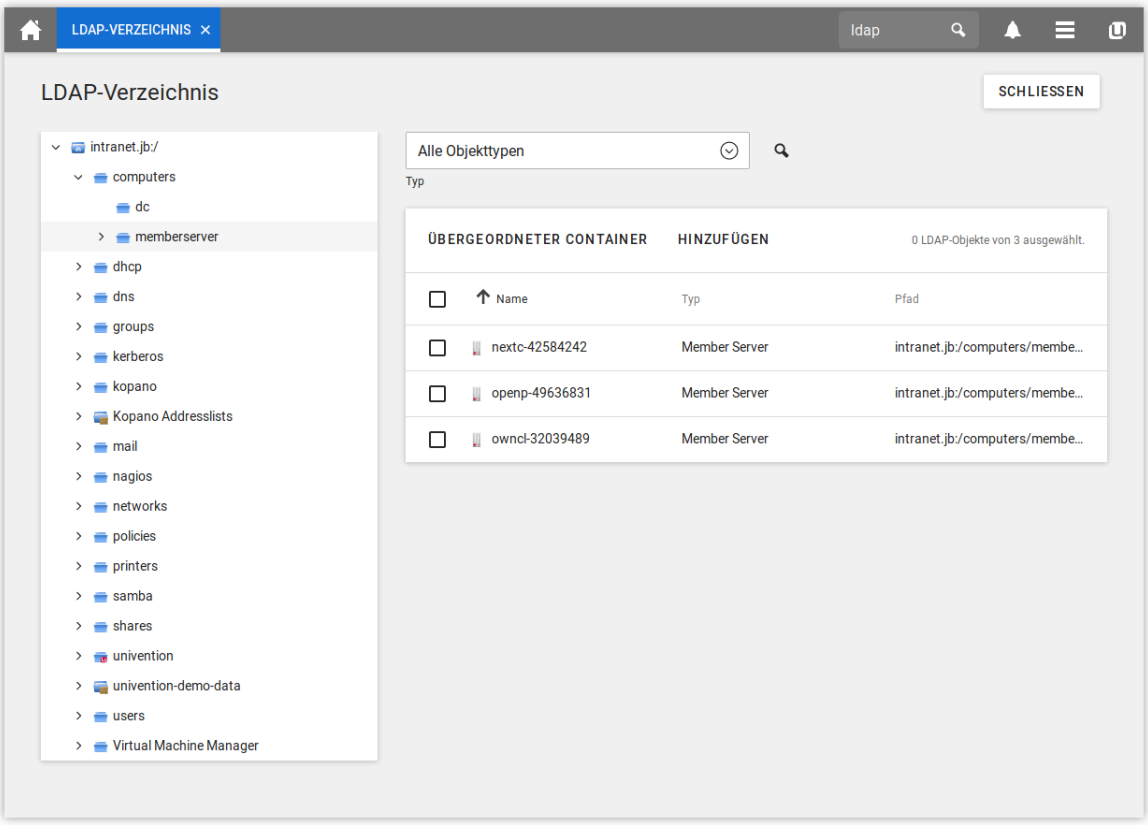
UMC-Module können den Benutzer durch Systembenachrichtigungen auf potentielle Fehler - z.B. nicht ausgeführte Join-Skripte - oder nötige Aktionen wie verfügbare Aktualisierungen hinweisen. Die Benachrichtigungen werden an der rechten Seite eingeblendet und können durch einen Mausklick ausgeblendet werden.

4.5. LDAP-Verzeichnis-Browser

Feedback

Über das UMC-Modul **LDAP-Verzeichnis** kann durch das LDAP-Verzeichnis navigiert werden. Dabei können auch Objekte im LDAP-Verzeichnis erzeugt, modifiziert oder gelöscht werden.

Abbildung 4.7. Navigation im LDAP-Verzeichnis

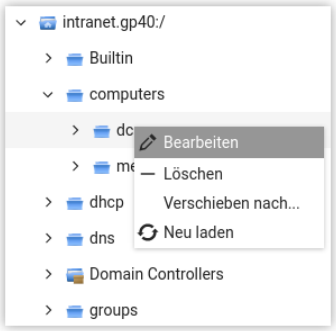


In der linken Bildschirmhälfte ist das LDAP-Verzeichnis in einer Baumstruktur dargestellt, deren Unterelemente durch die Symbole mit dem Plus- und Minuszeichen ein- und ausgeblendet werden können.

Durch Klick auf ein Element der Baumstruktur wird an diese LDAP-Position gewechselt und in der Übersichtsliste auf der linken Bildschirmhälfte, die an dieser LDAP-Position befindlichen Objekte angezeigt. Über die Auswahlliste **LDAP-Objekttyp** kann die Anzeige auf ausgewählte Attribute eingeschränkt werden.

Mit der Option **Hinzufügen** können hier auch neue Objekte eingefügt werden. Analog zu den in Abschnitt 4.4 beschriebenen Bedienelementen können hier auch bestehende Objekte editiert, gelöscht oder verschoben werden.

Abbildung 4.8. Bearbeiten von LDAP-Container-Einstellungen



Durch Rechtsklick auf ein Element der Baumstruktur können über **Bearbeiten** die Eigenschaften des Containers oder der LDAP-Basis bearbeitet werden.

4.6. Richtlinien

Feedback

Richtlinien beschreiben administrative Einstellungen, die sinnvoll auf mehr als ein Objekt angewendet werden können. Sie erleichtern die Administration, in dem sie an Container gebunden werden und dann für alle in dem betreffenden Container befindlichen Objekte, sowie die in Unterordnern befindlichen Objekte gelten. Die Einstellungen werden nach dem Prinzip der Vererbung angewendet. Auf ein Objekt wird immer der Wert angewandt, der dem Objekt am nächsten liegt.

Soll z.B. für alle Benutzer eines Standorts das gleiche Passwortablaufintervall definiert werden, kann für diese Benutzer ein eigener Container angelegt werden. Nachdem die Benutzer-Objekte in den Container verschoben wurden, kann eine Passwort-Richtlinie mit dem Container verknüpft werden. Diese Richtlinie gilt für alle enthaltenen Benutzer-Objekte.

Eine Ausnahme bilden Werte, die in einer Richtlinie als **festgelegte Attribute** gesetzt wurden. Diese können von nachgeordneten Richtlinien nicht überschrieben werden.

Mit dem Kommandozeilenprogramm `univention-policy-result` kann detailliert angezeigt werden, welche Richtlinie auf ein Verzeichnisdienst-Objekt greift.

Jede Richtlinie gilt für einen bestimmten UMC-Domänen-Objekt-Typ, also z.B. für Benutzer oder DHCP-Subnetze.

Eine Richtlinie muss zuerst angelegt werden, bevor sie einem Container oder einem LDAP-Objekt zugewiesen werden kann.

4.6.1. Anlegen einer Richtlinie

Feedback

Richtlinien können über das **Richtlinien**-Modul der Univention Management Console verwaltet werden. Die Bedienung erfolgt analog zu den in Abschnitt 4.4 beschriebenen Funktionen.

Die Attribute und Eigenschaften der Richtlinien sind in den entsprechenden Kapiteln beschrieben, also die DHCP-Richtlinien beispielsweise im Netzwerk-Kapitel.

Die Namen von Richtlinien dürfen keine Umlaute enthalten.

Unter **Referenzierende Objekte** findet sich eine Aufstellung aller Container oder LDAP-Objekte, mit denen diese Richtlinie aktuell verknüpft ist.

In den erweiterten Einstellungen einer Richtlinie können einige allgemeine Richtlinien-Optionen gesetzt werden, die in der Regel nur für Sonderfälle nötig sind:

- **Benötigte Objektklassen**: Hier können LDAP-Objektklassen angegeben werden, die ein Objekt besitzen muss, damit die Richtlinie auf dieses Objekt greift. Wenn etwa eine Benutzerrichtlinie nur für Windows-Umgebungen relevant ist, könnte hier die Objektklasse `sambaSamAccount` erzwungen werden.
- **Ausgeschlossene Objektklassen**: Analog zur Konfiguration der benötigten Objektklassen können hier Objektklassen aufgeführt werden, die ausgeschlossen werden sollen.
- **Festgelegte Attribute**: Hier können Attribute ausgewählt werden, deren Werte von nachgeordneten Richtlinien nicht verändert werden dürfen.
- **Leere Attribute**: Hier können Attribute ausgewählt werden, die in der Richtlinie leergesetzt, also ohne Wert gespeichert werden sollen. Dadurch können Werte, die ein Objekt von einer übergeordneten Richtlinie ererbt hat, entfernt werden. In nachgeordneten Richtlinien können den Attributen wieder Werte zugewiesen werden.

4.6.2. Zuweisung von Richtlinien

Feedback

Richtlinien werden auf zwei unterschiedlichen Arten Objekten zugewiesen:

- Eine Richtlinie kann der LDAP-Basis oder einem Container/OU zugewiesen werden. Dazu muss im LDAP-Verzeichnis-Browser (siehe Abschnitt 4.5) in den Eigenschaften des LDAP-Objekts der Reiter **Richtlinien** geöffnet werden.

- In den einzelnen UMC Modulen der LDAP-Verzeichnisobjekte - sofern es für den Typ Richtlinien gibt (z.B. für Benutzer) - wird ein Reiter **Richtlinien** angezeigt. Eine abweichende Richtlinie für einen Benutzer kann an dieser Stelle festgelegt werden.

Der **Richtlinien**-Konfigurationsdialog ist funktional identisch; allerdings werden bei der Zuweisung von Richtlinien an einem LDAP-Container alle Richtlinien-Typen angeboten, während bei der Zuweisung an einem LDAP-Objekt nur die für diesen Objekt-Type gültigen Richtlinien angeboten werden.

Unter **Richtlinien-Konfiguration** kann dem LDAP-Objekt oder dem Container eine Richtlinie zugewiesen werden. Die aus dieser Richtlinie resultierenden Werte werden direkt angezeigt. Die Einstellung **Ererbt** bedeutet, dass die Einstellungen wieder aus einer übergeordneten Richtlinie - sofern vorhanden - übernommen werden.

Wenn ein Objekt mit einer Richtlinie verbunden ist oder Richtlinien-Einstellungen erbt, die auf das Objekt nicht angewandt werden können, bleiben die Einstellungen ohne Auswirkung für das Objekt. Dadurch ist es z.B. möglich, eine Richtlinie mit der Wurzel des LDAP-Verzeichnisses zu verbinden, die dann für alle Objekte der Domäne, die diese Richtlinie anwenden können, gültig ist. Objekte, die diese Richtlinie nicht anwenden können, werden nicht beeinflusst.

4.6.3. Bearbeiten einer Richtlinie

Feedback

Richtlinien können im UMC-Modul **Richtlinien** bearbeitet und gelöscht werden. Die Bedienung ist in Abschnitt 4.4 beschrieben.

Achtung

Beim Bearbeiten einer Richtlinie werden die Einstellungen für alle Objekte, die mit dieser Richtlinie verbunden sind, verändert! Diese Werte aus der geänderten Richtlinie gelten also nicht nur für Objekte, die in der Zukunft hinzugefügt werden, sondern auch für diejenigen, die bereits im System eingetragen und mit der Richtlinie verbunden sind.

Im Richtlinien-Reiter der einzelnen LDAP-Objekte findet sich außerdem die Schaltfläche **Bearbeiten**, mit der die aktuell für dieses Objekt gültige Richtlinie bearbeitet werden kann.

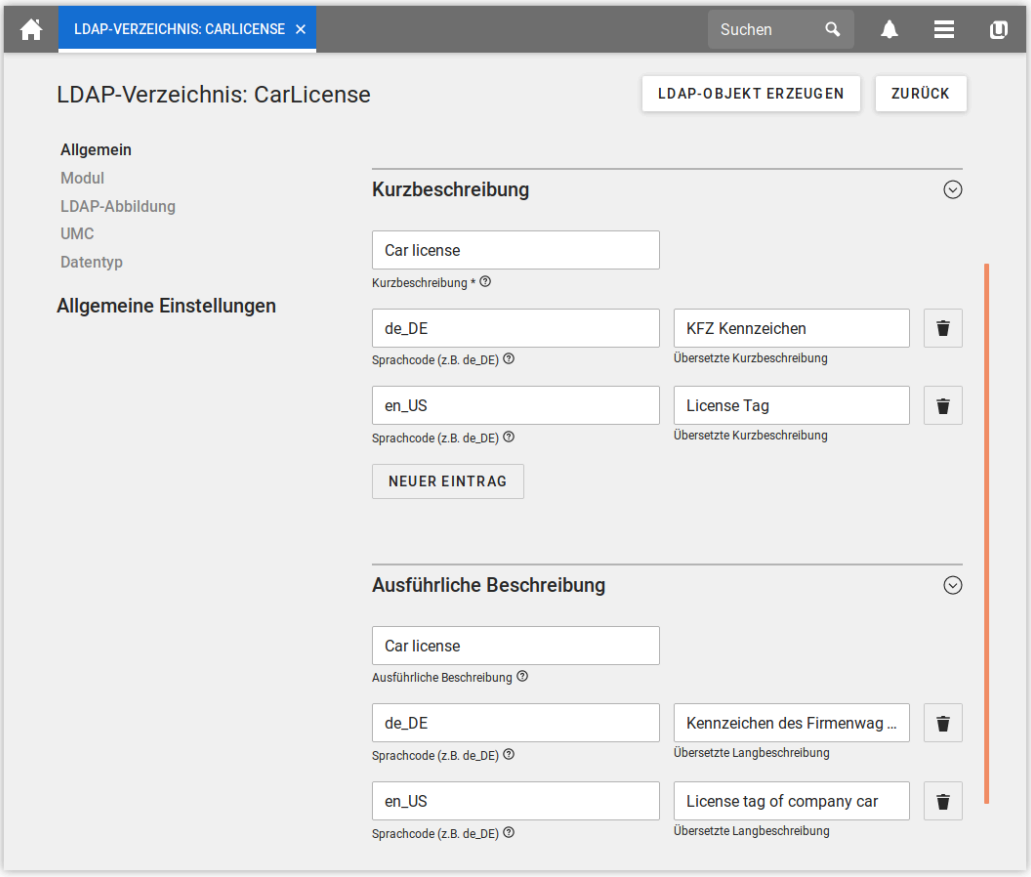
4.7. Erweiterung der UMC mit erweiterten Attributen

Feedback

Die Domänenverwaltung von Univention Management Console ermöglicht die umfassende Verwaltung der Daten einer Domäne. *Erweiterte Attribute* bieten eine Möglichkeit, neue Attribute in die Domänenverwaltung zu integrieren, die durch den UCS-Standardumfang nicht abgedeckt sind. Erweiterte Attribute werden auch von Drittanbietern für die Integration von Lösungen in UCS eingesetzt.

Erweiterte Attribute werden über das Modul **LDAP-Verzeichnis** verwaltet. Sie befinden sich im Container `univention` und dessen Untercontainer `custom attributes`. Hier können bestehende Attribute bearbeitet werden oder mit **Hinzufügen** ein Objekt vom Typ **Einstellungen: Erweitertes Attribut** angelegt werden.

Abbildung 4.9. Erweitertes Attribut zur Verwaltung von KFZ-Kennzeichen



Erweiterte Attribute können internationalisiert werden. In diesem Fall sollten Namen und Beschreibungen in Englisch verfasst werden, da dies der Standardsprache des Univention Management Console entspricht.

Tabelle 4.1. Karteikarte 'Allgemein'

Attribut	Beschreibung
Eindeutiger Name	Der Name des LDAP-Objektes, als welches das erweiterte Attribut gespeichert wird. Innerhalb eines Containers muss der Name eindeutig sein.
UDM-CLI Name	Der angegebene Attributname ist bei der Verwendung der Kommandozeilenschnittstelle Univention Directory Manager zu verwenden. Beim Anlegen des erweiterten Attributs wird hier automatisch *Eindeutiger Name* von der Karteikarte *Allgemein* übernommen und kann nachträglich modifiziert werden.
Kurzbeschreibung	Wird als Überschrift des Eingabefelds in Univention Management Console, bzw. als Attribut-Beschreibung in der Kommandozeilenschnittstelle verwendet.
Übersetzungen der Kurzbeschreibung	Damit der Titel von erweiterten Attributen auch mit anderen Spracheinstellungen in der jeweiligen Landessprache ausgegeben wird, können übersetzte Kurzbeschreibungen für mehrere Sprachen hinterlegt werden. Dazu kann in diesem Eingabefeld einem Sprachcode (z.B. `de_DE` oder `fr_FR`) die entsprechend übersetzte Kurzbeschreibung zugeordnet werden.

Attribut	Beschreibung
Ausführliche Beschreibung	Diese erweiterte Beschreibung wird für die Eingabefelder in Univention Management Console als Tooltip angezeigt.
Übersetzungen der ausführlichen Beschreibung	Zusätzliche Hinweise, die im Tooltip für ein erweitertes Attribut angezeigt werden, können ebenfalls für mehrere Sprachen hinterlegt werden. Dazu kann in diesem Eingabefeld einem Sprachcode (z.B. `de_DE` oder `fr_FR`) die entsprechend übersetzte Langbeschreibung zugeordnet werden.

Tabelle 4.2. Karteikarte 'Modul'

Attribut	Beschreibung
Zu erweiternde Module	Das Univention Directory Manager-Modul, welches durch das erweiterte Attribut ergänzt werden soll. Ein erweitertes Attribut kann auch für mehrere Module gelten.
Benötigte Optionen/Objektklassen	Einige erweiterte Attribute können nur sinnvoll verwendet werden, wenn auf der Karteikarte *(Optionen)* bestimmte Objektklassen aktiviert sind. In diesem Eingabefeld können optional eine oder mehrere Optionen hinterlegt werden, die am betreffenden Objekt aktiviert sein müssen, damit dieses erweiterte Attribut angezeigt bzw. editierbar ist.
Hook-Klasse	Die Funktionen der hier angegebenen Hook-Klasse werden während des Anlegens, Modifizierens und Löschens von Objekten mit dem erweitertem Attribut aufgerufen. Weiterführende Dokumentation findet sich in der Entwickler-Dokumentation [developer-reference]

Tabelle 4.3. Karteikarte 'LDAP-Abbildung'

Attribut	Beschreibung
LDAP-Objektklasse	Die Objektklasse, zu welcher das unter *LDAP-Abbildung* eingetragene Attribut gehört. Für erweiterte Attribute stehen mit der Objektklasse `univention-FreeAttributes` vordefinierte LDAP-Schema-Erweiterungen zur Verfügung. Weitere Hinweise finden sich in Abschnitt 3.4.1.1. Jedes LDAP-Objekt, das um ein Attribut erweitert werden soll, wird automatisch um die hier angegebene LDAP-Objektklasse erweitert, wenn vom Benutzer ein Wert für das erweiterte Attribut angegeben wurde.
LDAP-Attribut	Der Name des LDAP-Attributs, in dem die Werte am LDAP-Objekt gespeichert werden sollen. Das LDAP-Attribut muss in der angegebenen Objektklasse enthalten sein.
Objektklasse löschen, wenn das Attribut entfernt wird	Wird für ein erweitertes Attribut in Univention Management Console der Wert gelöscht, wird das Attribut vom LDAP-Objekt entfernt. Werden an diesem LDAP-Objekt keine weiteren Attribute der angegebenen *Objektklasse* verwendet, wird auch die Objektklasse vom LDAP-Objekt entfernt, sofern diese Option aktiviert ist.

Tabelle 4.4. Karteikarte 'UMC'

Attribut	Beschreibung
Dieses erweiterte Attribut nicht in der UMC anzeigen	Wenn ein Attribut anstatt durch den Administrator nur intern verwaltet werden soll, - z.B. indirekt durch Skripte - kann diese Option aktiviert werden. Das Attribut kann dann nur über das Kommandozeilen-Interface Univention Directory Manager gesetzt werden und wird in Univention Management Console nicht angezeigt.
Von der UMC-Suche ausschließen	Soll im Suchdialog eines Assistenten nicht nach einem erweiterten Attribut gesucht werden können, kann diese Option aktiviert werden, um das erweiterte Attribut aus der Liste der möglichen Sucheigenschaften zu entfernen. Dies ist nur in Sonderfällen nötig.
Ordnungsnummer	Sollen mehrere erweiterte Attribute auf einer Karteikarte verwaltet werden, kann anhand dieser Positionsnummer die Reihenfolge der Attribute beeinflusst werden. Sie werden in aufsteigender Reihenfolge bestimmt durch diese Positionsnummer jeweils am das Ende der betreffenden Gruppe und Karteikarte angehängt. Fortlaufend vergebene Positionsnummern führen dazu, dass die Attribute jeweils abwechselnd links und rechts zweispaltig angeordnet werden. Ansonsten beginnt die Platzierung in der linken Spalte. Weisen erweiterte Attribute die gleiche Positionsnummer auf, ist deren Reihenfolge zufällig.
Existierendes Eingabefeld überschreiben	In einigen Fällen ist es sinnvoll, vorgegebene Eingabefelder mit erweiterten Attributen zu überschreiben. Wird hier der interne UDM-Name eines Attributs konfiguriert, wird dessen Eingabefeld von diesem erweiterten Attribut überschrieben. Der UDM-Attributname kann mit dem Befehl `univention-directory-manager` ermittelt werden (siehe Abschnitt 4.10). Es ist zu beachten, dass diese Option bei Pflichtfeldern zu Problemen führen kann.
Beide Spalten umfassen	Alle Eingabefelder werden standardmäßig in zwei Spalten gruppiert. Diese Option kann für überlange Eingabefelder verwendet werden, die sich über die komplette Breite beider Spalten erstrecken sollen.
Name der Karteikarte	Der Name der Karteikarte in Univention Management Console, auf der das erweiterte Attribut angezeigt werden soll. Hier können auch neue Karteikarten hinzugefügt werden. Wird kein Karteikartenname angegeben, wird *Benutzerdefiniert* verwendet.
Übersetzung des Karteikartennamens	Um den Namen der Karteikarte zu übersetzen, können in diesem Eingabefeld übersetzte Karteikartennamen zum entsprechenden Sprachcode (z.B. `de_DE` oder `fr_FR`) hinterlegt werden.
Existierende Karteikarte überschreiben	Ist diese Option aktiviert, wird die betreffende Karteikarte überschrieben, bevor erweiterte Attribute darauf platziert werden. Mit Hilfe dieser Option können alle vorhandenen Eingabefelder auf einer vorgegebenen Karteikarte ausgeblendet werden. Es ist zu beachten, dass diese Option bei Pflichtfeldern zu Problemen führen kann. Verwendet die zu überschreibende Karteikarte Übersetzungen muss die überschreibende Karteikarte ebenfalls identische Übersetzungen mitbringen.

Attribut	Beschreibung
Karteikarte mit erweiterten Einstellungen	Einstellungsmöglichkeiten, die selten verwendet werden, können auf Karteikarten in den erweiterten Einstellungen platziert werden.
Gruppenname	Gruppen ermöglichen die Strukturierung einer Karteikarte. Eine Gruppe wird durch einen grauen Querbalken abgetrennt und kann ein- und ausgeklappt werden. Wird bei einem erweiterten Attribute kein Gruppenname angegeben, wird das erweiterte Attribut oberhalb der ersten Gruppe platziert.
Übersetzung des Gruppennamens	Um den Namen der Gruppe zu übersetzen, können in diesem Eingabefeld übersetzte Gruppennamen zum entsprechenden Sprachcode (z.B. `de_DE` oder `fr_FR`) hinterlegt werden.
Gruppen-Ordnungsnummer	Sollen mehrere Gruppen auf einer Karteikarte verwaltet werden, kann anhand dieser Positionsnummer die Darstellungsreihenfolge beeinflusst werden. Sie werden in aufsteigender Reihenfolge ihrer Positionsnummern dargestellt.

Tabelle 4.5. Karteikarte 'Datentyp'

Attribut	Beschreibung
Syntax-Klasse	Bei der Eingabe von Werten nimmt Univention Management Console eine Syntaxprüfung vor. Neben Standard-Syntaxdefinitionen für Zeichenketten (`string`), Zahlen (`integer`) gibt es drei Möglichkeiten einen binären Zustand auszudrücken: Die Syntax `TrueFalse` wird auf LDAP-Ebene durch die Zeichenketten `true` und `false` abgebildet, die Syntax `TrueFalseUpper` verwendet dagegen die Werte `TRUE` und `FALSE`. Die Syntax `boolean` dagegen speichert keinen Wert bzw. die Zeichenkette `1`. Standardmäßig wird die Syntax `string` verwendet. Eine Übersicht über die weiteren verfügbaren Syntax-Definitionen und eine Anleitung zur Integration eigener Syntaxen sind in [developer-reference] zu finden.
Vorgabewert	Ist hier ein Vorgabewert definiert, werden Objekte beim Anlegen mit diesem Wert initialisiert. Der Wert kann während des Anlegens noch manuell bearbeitet werden. Bereits bestehende Objekte werden nicht verändert.
Mehrfachwert	Diese Option legt fest, ob ein einzelner Wert oder mehrere Werte in der Eingabemaske eingetragen werden können. Die Einstellung muss zur Schema-Definition passen, in der für das verwendete LDAP-Attributes festgelegt ist, ob nur eine oder mehrere Instanzen des Attributs an einem LDAP-Objekt verwendet werden dürfen.
Wert wird benötigt	Ist diese Option aktiv, muss ein gültiger Wert für das erweiterte Attribut eingetragen sein, um das betreffende Objekt anzulegen oder zu speichern.
Nachträglich modifizierbar	Diese Option legt fest, ob der im erweiterten Attribut gespeicherte Wert nur während des Anlegens eines Objektes oder auch nachträglich modifiziert werden kann.
Wert wird nur intern verwaltet	Ist diese Option aktiviert, kann das Attribut nicht manuell gesetzt werden, weder beim Anlegen des Objekts, noch nachträglich. Dies ist sinn-

Attribut	Beschreibung
	voll für automatisch generierte interne Zustände, die über Hook-Funktionen oder intern in einem Modul gepflegt werden.

4.8. Strukturierung der Domäne durch angepasste LDAP-Strukturen

Feedback

Container und Organisationseinheiten (OU) dienen der Strukturierung der Daten im LDAP-Verzeichnis. Technisch unterscheiden sich beide Typen nicht, sondern eher in der Anwendung:

- Organisationseinheiten repräsentieren in der Regel real existierende Einheiten wie z.B. eine Abteilung einer Firma oder einer Behörde
- Container werden meistens für fiktive Einheiten wie z.B. alle Computer eines Unternehmens verwendet

Container und Organisationseinheiten werden im Modul **LDAP-Verzeichnis** von Univention Management Console verwaltet und werden mit **Hinzufügen** und den Objekt-Typen **Container: Container** und **Container: Organisationseinheit** angelegt.

Container und OUs dürfen prinzipiell an jeder beliebigen Position im LDAP eingefügt werden, OUs können aber nicht unterhalb von Containern angelegt werden.

Tabelle 4.6. Karteikarte 'Allgemein'

Attribut	Beschreibung
Name	Ein beliebiger Name für den Container / die Organisationseinheit.
Beschreibung	Eine beliebige Beschreibung für den Container / die Organisationseinheit.

Tabelle 4.7. Karteikarte 'Erweiterte Einstellungen'

Attribut	Beschreibung
Zu Standard-*`Objekttyp`*-Container hinzufügen	Ist diese Option aktiviert, wird der Container/die Organisationseinheit als Standard-Container für einen bestimmten Objekttyp angesehen. Wird der aktuelle Container etwa als Standard-Benutzercontainer deklariert, wird in den Masken zum Suchen und Anlegen von Benutzern dieser Container ebenfalls angezeigt.

Tabelle 4.8. Karteikarte 'Richtlinien'

Attribut	Beschreibung
	Diese Karteikarte wird in Abschnitt 4.6.2 beschrieben.

4.9. Delegierte Administration in der UMC

Feedback

In der Grundeinstellung können nur die Mitglieder der Gruppe `Domain Admins` alle UMC-Module aufrufen. Über Richtlinien kann für Gruppen oder einzelne Benutzer der Zugriff auf UMC-Module konfiguriert werden. Dies kann beispielsweise verwendet werden, um einem Helpdesk-Team die Berechtigung zu erteilen Drucker zu verwalten ohne ihnen Vollzugriff auf die Administration der Domäne zu erteilen.

Die Zuweisung von UMC-Modulen erfolgt über eine **UMC**-Richtlinie (siehe auch Abschnitt 4.6), die Benutzer- und Gruppenobjekten zugewiesen werden kann. Die Auswertung erfolgt dabei additiv, d.h. man kann

allgemeine Zugriffsrechte durch ACLs auf Gruppenmitgliedschaften erteilen und durch ACLs auf Benutzer ergänzen.

Zusätzlich zu der Zuweisung von UMC-Richtlinien, müssen für UMC-Module, die Daten des LDAP-Verzeichnisses verwalten, ebenfalls LDAP-Zugriffsrechte berücksichtigt werden. Alle im LDAP vorgenommenen Änderungen gelten für die gesamte UCS-Domäne. Daher haben in der Grundeinstellung nur Mitglieder der Gruppe `Domain Admins` sowie einige intern genutzte Konten Vollzugriff auf das UCS-LDAP. Wird ein Modul über eine UMC-Richtlinie freigegeben, muss für den Benutzer/die Gruppe zusätzlich der Zugriff in den LDAP-ACLs freigegeben werden. Weitere Hinweis zu LDAP-ACLs finden sich in Kapitel Abschnitt 3.4.5.

Tabelle 4.9. Richtlinie 'UMC'

Attribut	Beschreibung
Liste der erlaubten Operationen	Alle hier definierten UMC-Module werden dem Benutzer oder der Gruppen angezeigt, auf die diese ACL angewendet wird. Die Namen von Domänen-Modulen beginnen mit 'UDM'.

Achtung

Für den Zugriff auf UMC-Module werden nur Richtlinien ausgewertet, die Gruppen oder aber direkt Benutzer- sowie Rechnerkonten zugewiesen sind. Eine Auswertung von verschachtelten Gruppenmitgliedsschaften (also Gruppen in Gruppen) findet nicht statt.

4.10. Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)

Feedback

Der Univention Directory Manager ist die Kommandozeilenschnittstelle der Domänenverwaltungsfunktionalität von Univention Management Console. Er ergänzt die webbasierte Schnittstelle von Univention Management Console und dient als mächtiges Werkzeug für die Automatisierung administrativer Vorgängen in Skripten und zur Integration in andere Programme.

Univention Directory Manager wird als Benutzer `root` auf dem Domänencontroller Master mit dem Befehl `univention-directory-manager` (Kurzform `udm`) aufgerufen

Univention Management Console und Univention Directory Manager verwenden dieselben Domänen-Verwaltungsmodule, d.h. alle Funktionen der Webschnittstelle stehen auch im Kommandozeilen-Interface zur Verfügung.

4.10.1. Aufrufparameter der Kommandozeilenschnittstelle

Feedback

Eine komplette Liste der verfügbaren Module wird angezeigt, wenn `udm` mit dem Parameter `modules` aufgerufen wird:

```
# univention-directory-manager modules
Available Modules are:
  computers/managedclient
  computers/computer
  computers/domaincontroller_backup
  computers/domaincontroller_master
  computers/domaincontroller_slave
 [...]
```

Für jedes Modul existieren bis zu fünf Operationen:

- `list` führt alle existierenden Objekte dieses Typs auf

- `create` legt ein neues Objekt an
- `modify` zum Bearbeiten existierender Objekte
- `remove` löscht ein Objekt
- `move` zum Verschieben an eine andere Position im LDAP-Verzeichnis

Die mögliche Optionen eines UDM-Moduls und den darauf anwendbaren Operationen können durch Angabe des Operationsnamens ausgegeben werden, z.B.

```
univention-directory-manager users/user move
[...]
create options:
  --binddn                          bind DN
  --bindpwd                         bind password
[...]
modify options:
  --binddn                          bind DN
  --bindpwd                         bind password
  --dn                              Edit object with DN
[...]
remove options:
  --binddn                          bind DN
  --bindpwd                         bind password
  --dn                              Remove object with DN
  --arg                             Remove object with ARG
[...]
list options:
  --filter                          Lookup filter
[...]
move options:
  --binddn                          bind DN
  --bindpwd                         bind password
[...]
```

Nähere Informationen, Operationen und Optionen zu jedem Modul gibt der folgende Befehl aus:

```
univention-directory-manager Kategorie/Modulname
```

Dabei werden auch die Attribute des Moduls angezeigt. Bei der Operation `create` werden mit `(*)` die Attribute markiert, die beim Anlegen eines neuen Objektes zwingend angegeben werden müssen.

Einigen Attributen können mehrere Werte zugewiesen werden (z.B. Mailadressen an Benutzerobjekten). Diese Multivalue-Felder sind mit `[]` hinter dem Attributnamen markiert. Einige Attribute können nur gesetzt werden, wenn für das Objekt bestimmte Optionen gesetzt werden. Dies ist bei den einzelnen Attributen durch Angabe des Optionsnamens aufgeführt:

```
users/user variables:
  General:
    username (*)                            Username
[...]
  Contact:
    e-mail (person,[])                      E-Mail Address
```

Hier bezeichnet `username (*)`, dass dieses Attribut beim Anlegen von Benutzerobjekten immer gesetzt werden muss. Wird für das Benutzerkonto die Option `person` gesetzt (dies ist standardmäßig der Fall), können eine oder mehrere E-Mail-Adressen zu den Kontaktinformationen hinzugefügt werden.

Eine Reihe von Standard-Parametern sind für jedes Modul definiert:

- Der Parameter `--dn` wird verwendet, um bei Modifikationen bzw. beim Entfernen die LDAP-Position des Objektes anzugeben. Dabei muss die komplette DN angegeben werden, z.B:

```
univention-directory-manager users/user remove \
    --dn "uid=ldapadmin,cn=users,dc=firma,dc=de"
```

- Um anzugeben, an welcher LDAP-Position ein Objekt angelegt werden soll, wird der `--position`-Parameter verwendet. Ohne den `--position`-Parameter wird das Objekt unterhalb der LDAP-Basis angelegt! Bei der Operation `move` wird mit diesem Parameter angegeben, an welche Stelle ein Objekt verschoben werden soll, z.B:

```
univention-directory-manager computers/managedclient move \
    --dn "cn=desk01,cn=management,cn=computers,dc=firma,dc=de" \
    --position "cn=finance,cn=computers,dc=firma,dc=de"
```

- Der Parameter `--set` gibt an, dass dem darauf folgenden Attribut der angegebene Wert zugewiesen wird. Der Parameter muss je Attribut-Wert-Paar verwendet werden, z.B:

```
univention-directory-manager users/user create \
    --position "cn=users,dc=firma,dc=de" \
    --set username="mmuster" \
    --set firstname="Max" \
    --set lastname="Muster" \
    --set password="12345678"
```

- `--option` definiert die LDAP-Objektklassen eines Objekts. Wird bei einem Benutzerobjekt beispielsweise nur `pki` als Option übergeben, so kann für diesen Benutzer keine *mailPrimaryAddress* angegeben werden, da dieses Attribut Teil der Option `mail` ist:

- `--superordinate` wird zur Angabe von abhängigen, übergeordneten Modulen verwendet. Ein DHCP-Objekt beispielsweise benötigt ein DHCP-Service-Objekt, unter dem es angelegt werden kann. Dieses wird mit der Option `--superordinate` übergeben.

- Mit dem Parameter `--policy-reference` lässt sich Objekten Richtlinien zuweisen (und analog mit `--policy-dereference` entfernen). Wird eine Richtlinie an ein Objekt geknüpft, so werden die Einstellungen aus der Richtlinie für das Objekt angewendet, z.B:

```
univention-directory-manager*Kategorie/ModulnameOperation*\
    --policy-reference="cn=vertrieb,cn=pwhistory,"\
"cn=users,cn=policies,dc=firma,dc=de"
```

- Der Parameter `--ignore_exists` überspringt bereits vorhandene Objekte. Sollte ein Objekt nicht angelegt werden können, da es bereits existiert, wird trotzdem der Fehlercode 0 (kein Fehler) zurückgegeben.

- Mit `--append` und `--remove` wird einem Multivalue-Feld ein Wert hinzugefügt/entfernt, z.B:

```
univention-directory-manager groups/group modify \
    --dn "cn=Mitarbeiter,cn=groups,dc=firma,dc=de" \
    --append users="uid=kmeier,cn=users,dc=firma,dc=de" \
    --remove users="uid=jmueller,cn=users,dc=firma,dc=de"
```

4.10.2. Beispielaufrufe für die Kommandozeilenschnittstelle

Die folgenden Beispielaufrufe des Kommandozeilen-Frontend von Univention Directory Manager können als Vorlagen für eigene Skripte verwendet werden:

4.10.2.1. Benutzer

Feedback

Anlegen eines Benutzers im Standard-Benutzer-Container:

```
univention-directory-manager users/user create \
    --position "cn=users,dc=example,dc=com" \
    --set username="user01" \
    --set firstname="Random" \
    --set lastname="User" \
    --set organisation="Example company LLC" \
    --set mailPrimaryAddress="mail@example.com" \
    --set password="secretpassword"
```

Nachträgliches Hinzufügen der postalischen Adresse zum gerade angelegten Benutzer:

```
univention-directory-manager users/user modify \
    --dn "uid=user01,cn=users,dc=example,dc=com" \
    --set street="Exemplary Road 42" \
    --set postcode="28239" \
    --set city="Bremen"
```

Mit diesem Befehl werden alle Benutzer angezeigt, deren Benutzername mit *user* beginnt:

```
univention-directory-manager users/user list \
    --filter uid=user*
```

Die Suche nach Objekten mit `--filter` kann auch auf eine Position im LDAP-Verzeichnis eingeschränkt werden, in diesem Fall auf alle Benutzer im Container `cn=bremen,cn=users,dc=example,dc=com`:

```
univention-directory-manager users/user list \
    --filter uid="user*" \
    --position "cn=bremen,cn=users,dc=example,dc=com"
```

Dieser Aufruf entfernt einen Benutzer `user04`:

```
univention-directory-manager users/user remove \
    --dn "uid=user04,cn=users,dc=example,dc=com"
```

Eine Firma hat zwei Standorte mit eigens dafür angelegten Containern. Mit dem folgenden Befehl wird ein Benutzer aus dem Container für den Standort "Hamburg" in den Container für den Standort "Bremen" verschoben:

```
univention-directory-manager users/user move \
    --dn "uid=user03,cn=hamburg,cn=users,dc=example,dc=com" \
    --position "cn=bremen,cn=users,dc=example,dc=com"
```

4.10.2.2. Gruppen

Feedback

Anlegen einer Gruppe `Example Users` und Hinzufügen des Benutzers `user01` in diese Gruppe:

```
univention-directory-manager groups/group create \
    --position "cn=groups,dc=example,dc=com" \
    --set name="Example Users" \
    --set users="uid=user01,cn=users,dc=example,dc=com"
```

Nachträgliches Hinzufügen des Benutzers `user02` zur gerade angelegten Gruppe:

```
univention-directory-manager groups/group modify \
    --dn "cn=Example Users,cn=groups,dc=example,dc=com" \
```

```
    --append users="uid=user02,cn=users,dc=example,dc=com"
```

Achtung

Ein `--set` des Attributs users überschreibt im Gegensatz zu `--append` die Liste der Gruppenmitglieder.

Nachträgliches Entfernen des Benutzers `user01` aus der Gruppe:

```
univention-directory-manager groups/group modify \
    --dn "cn=Example Users,cn=groups,dc=example,dc=com" \
    --remove users="uid=user01,cn=users,dc=example,dc=com"
```

4.10.2.3. Container / Richtlinien

Feedback

Dieser Aufruf legt unterhalb des Standard-Containers `cn=computers` einen Container `cn=Bremen` für die Rechnerobjekte am Firmenstandort Bremen an. Durch die zusätzliche Option *computerPath* wird dieser Container auch direkt als Standardcontainer für Rechnerobjekte registriert (siehe Abschnitt 4.8):

```
univention-directory-manager container/cn create \
    --position "cn=computers,dc=example,dc=com" \
    --set name="bremen" \
    --set computerPath=1
```

Dieser Befehl legt eine Speicherplatzbegrenzungs-Richtlinie mit dem Namen *Default quota* mit Soft- und Hard-Limit an:

```
univention-directory-manager policies/share_userquota create \
    --position "cn=policies,dc=example,dc=com" \
    --set name="Default quota" \
    --set softLimitSpace=5GB \
    --set hardLimitSpace=10GB
```

Diese Richtlinie wird nun an den Benutzer-Container `cn=users` gebunden:

```
univention-directory-manager container/cn modify \
    --dn "cn=users,dc=example,dc=com" \
    --policy-reference "cn=Default quota,cn=policies,dc=example,dc=com"
```

Anlegen einer Univention Configuration Registry-Richtlinie, mit der die Vorhaltezeit der Logdateien auf ein Jahr eingestellt wird. Als Trennzeichen zwischen Name und Wert der Variable wird ein Leerzeichen verwendet:

```
univention-directory-manager policies/registry create \
    --position "cn=config-registry,cn=policies,dc=example,dc=com" \
    --set name="default UCR settings" \
    --set registry="logrotate/rotate/count 52"
```

Mit diesem Befehl wird an die angelegte Richtlinie ein weiterer Wert angehängt:

```
univention-directory-manager policies/registry modify \
    --dn "cn=default UCR settings,cn=config-registry,"\
"cn=policies,dc=example,dc=com" \
    --append registry='"logrotate/compress" "no"'
```

4.10.2.4. Rechner

Feedback

In folgendem Beispiel wird ein Windows-Client angelegt. Tritt dieser Client später der Samba-Domäne bei (siehe Abschnitt 3.2.2), wird dieses Rechnerkonto dann automatisch verwendet:

```
univention-directory-manager computers/windows create \
    --position "cn=computers,dc=example,dc=com" \
    --set name=WinClient01 \
    --set mac=aa:bb:cc:aa:bb:cc \
    --set ip=192.0.2.10
```

4.10.2.5. Freigaben

Feedback

Der folgende Befehl legt eine Freigabe *Documentation* auf dem Server `fileserver.example.com` an. Sofern `/var/shares/documentation/` auf dem Server noch nicht existiert, wird es durch diesen Aufruf auch gleich angelegt.

```
univention-directory-manager shares/share create \
    --position "cn=shares,dc=example,dc=com" \
    --set name="Documentation" \
    --set host="fileserver.example.com" \
    --set path="/var/shares/documentation"
```

4.10.2.6. Drucker

Feedback

Anlegen einer Druckerfreigabe `LaserPrinter01` auf dem Druckserver `printserver.example.com`. Die Eigenschaften des Druckers sind in der PPD-Datei spezifiziert, deren Name relativ zum Verzeichnis `/usr/share/ppd/` angegeben wird. Der angebundene Drucker ist netzwerkfähig und wird über das IPP-Protokoll angebunden.

```
univention-directory-manager shares/printer create \
    --position "cn=printers,dc=example,dc=com" \
    --set name="LaserPrinter01"  \
    --set spoolHost="printserver.example.com" \
    --set uri="ipp:// 192.0.2.100" \
    --set model="foomatic-rip/HP-Color_LaserJet_9500-Postscript.ppd" \
    --set location="Head office" \
    --set producer="producer: "\
"cn=HP,cn=cups,cn=univention,dc=example,dc=com"
```

> **Anmerkung**
>
> Im Parameter *`uri`* muss ein Leerzeichen zwischen dem Druckprotokoll und dem URL-Zielpfad verwendet werden. Eine Aufstellung der Druckprotokolle findet sich in Abschnitt 13.4

Drucker können zur einfacheren Verwaltung in einer Druckergruppe zusammengefasst werden. Weitere Informationen zu Druckergruppen finden sich in Abschnitt 13.5.

```
univention-directory-manager shares/printergroup create \
    --set name=LaserPrinters \
    --set spoolHost="printserver.example.com" \
    --append groupMember=LaserPrinter01 \
    --append groupMember=LaserPrinter02
```

4.10.2.7. DNS/DHCP

Feedback

Um eine IP-Vergabe über DHCP zu konfigurieren, muss ein DHCP-Rechner-Eintrag für die MAC-Adresse registriert werden. Weitere Informationen zu DHCP finden sich in Abschnitt 11.3.

```
univention-directory-manager dhcp/host create \
    --superordinate "cn=example.com,cn=dhcp,dc=example,dc=com" \
```

```
    --set host="Client222" \
    --set fixedaddress="192.0.2.110" \
    --set hwaddress="ethernet 00:11:22:33:44:55"
```

Soll ein Rechnername über DNS auflösbar sein, kann mit den folgenden Befehlen eine Vorwärts- (host record) und Reverse-Auflösung (PTR record) konfiguriert werden:

```
univention-directory-manager dns/host_record create \
    --superordinate "zoneName=example.com,cn=dns,dc=example,dc=com" \
    --set name="Client222" \
    --set a="192.0.2.110"

univention-directory-manager dns/ptr_record create \
    --superordinate "zoneName=0.168.192.in-addr.arpa,cn=dns,"\
"dc=example,dc=com" \
    --set address="110" \
    --set ptr_record="Client222.example.com."
```

Weitere Informationen zu DNS finden sich in Abschnitt 11.2.

4.10.2.8. Erweiterte Attribute

Feedback

Mit erweiterten Attributen lässt sich der Funktionsumfang von Univention Management Console flexibel erweitern, siehe Abschnitt 4.7. Im folgenden Beispiel wird ein neues Attribut eingefügt, an dem pro Benutzer das KFZ-Kennzeichen des Dienstwagens gespeichert wird. Die Werte werden in einer extra für diesen Zweck vorgesehenen Objektklasse `univentionFreeAttributes` verwaltet:

```
univention-directory-manager settings/extended_attribute create \
    --position "cn=custom attributes,cn=univention,dc=example,dc=com" \
    --set name="CarLicense" \
    --set module="users/user" \
    --set ldapMapping="univentionFreeAttribute1" \
    --set objectClass="univentionFreeAttributes" \
    --set longDescription="License plate number of the company car" \
    --set tabName="Company car" \
    --set multivalue=0 \
    --set syntax="string" \
    --set shortDescription="Car license"
```

4.11. HTTP Schnittstelle (API) der Domänenverwaltung

Feedback

UCS stellt eine HTTP API für UDM zur Verfügung, mit der UDM Objekte über HTTP-Anfragen überprüft, geändert, erstellt und gelöscht werden können.

Weitere Informationen zur API finden Sie unter [developer-reference].

4.12. Auswertung von Daten aus dem LDAP-Verzeichnis mit Univention Directory Reports

Feedback

Univention Directory Reports bietet die Möglichkeit vordefinierte Reports zu beliebigen im Verzeichnisdienst verwalteten Objekten zu erstellen.

Die Struktur der Reports wird dabei durch Vorlagen definiert. Die dafür entwickelte Beschreibungssprache ermöglicht die Verwendung von Platzhaltern, die durch die Werte aus dem LDAP-Verzeichnis ersetzt werden.

Es können dabei beliebig viele Reportvorlagen vorgegeben werden. So können beispielsweise für Benutzer wahlweise sehr detaillierte Reports oder nur einfache Adresslisten erstellt werden.

Die Erstellung von Reports ist direkt in die Weboberfläche der Univention Management Console integriert. Alternativ kann das Kommandozeilenprogramm `univention-directory-reports` verwendet werden.

Im Auslieferungszustand werden sechs Reportvorlagen von Univention Directory Reports bereitgestellt, die für Benutzer, Gruppen und Rechner verwendet werden können. Drei Vorlagen erzeugen PDF-Dokumente und drei Vorlagen CSV-Dateien, die als Import-Quelle für andere Programme verwendet werden können. Weitere Vorlagen können erstellt und registriert werden.

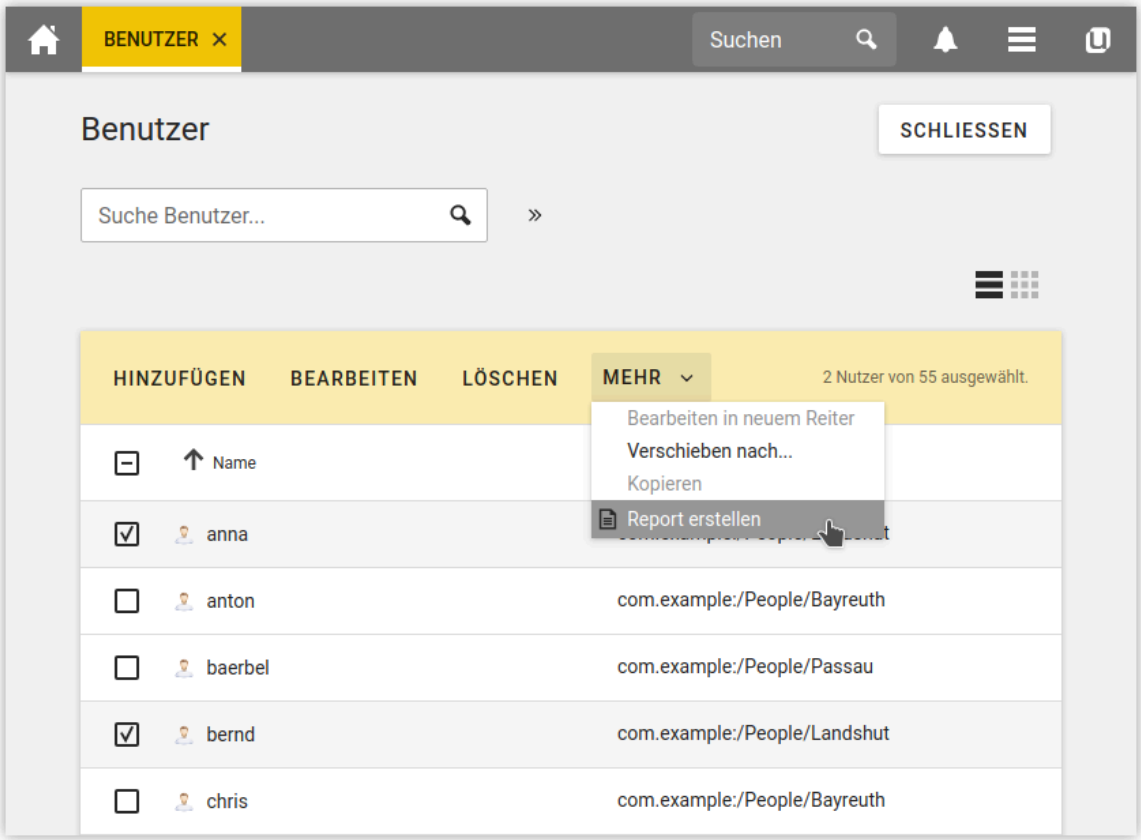
Reports können über ein Kommandozeilenprogramm oder über das Web-Interface von Univention Management Console erstellt werden.

4.12.1. Erstellen von Reports in Univention Management Console

Feedback

Um einen Report zu erstellen, muss in die UMC-Module für Benutzer, Gruppen oder Rechner gewechselt werden. Anschließend müssen alle vom Report erfassten Objekte ausgewählt werden (durch einen Klick auf den Button links von **Name** können alle Objekte selektiert werden). Ein Klick auf **Mehr -> Report erstellen** ermöglicht die Auswahl zwischen dem **Standard-Report** im PDF-Format und dem **CSV-Report** im CSV-Format.

Abbildung 4.10. Erstellen eines Reports



Die über Univention Directory Manager erzeugten Reports werden für 12 Stunden aufbewahrt und danach durch einen Cron-Job entfernt. Die Einstellungen, wann dieser Cron-Job laufen soll und wie lange diese

Reports aufbewahrt werden sollen, kann über zwei Univention Configuration Registry-Variablen definiert werden:

- `directory/reports/cleanup/cron` definiert den Zeitpunkt zu dem der Cron-Job ausgeführt werden soll.
- `directory/reports/cleanup/age` bestimmt das maximale Alter eines Report-Dokumentes in Sekunden bevor es gelöscht wird.

4.12.2. Erstellen von Reports auf der Kommandozeile

Reports können auch über die Kommandozeile mit dem Programm `univention-directory-reports` erstellt werden. Informationen zur Verwendung des Programm können über die Option `--help` abgefragt werden.

Mit dem folgenden Befehl können beispielsweise die verfügbaren Reportvorlagen für Benutzer aufgelistet werden:

```
univention-directory-reports -m users/user -l
```

4.12.3. Anpassung/Erweiterung von Univention Directory Reports

Schon vorhandene Reports können direkt mit den Voreinstellungen erstellt werden. Einige Voreinstellungen können mittels Univention Configuration Registry angepasst werden. Beispielsweise ist es möglich, das Logo, dass in der Kopfzeile jeder Seite eines PDF-Reports angezeigt wird, zu ersetzen. Dafür kann der Wert der Univention Configuration Registry-Variable `directory/reports/logo` den Namen einer Bilddatei enthalten. Dabei können gängigen Bildformate wie JPEG, PNG oder GIF verwendet werden. Das Bild wird automatisch auf eine feste Breite von 5.0 cm angepasst.

Neben dem Logo kann auch der Inhalt der Reports angepasst werden, indem neue Reportvorlagen definiert werden.

Kapitel 5. Softwareverteilung

5.1. Einführung

Feedback

Die in UCS integrierte Softwareverteilung bietet umfangreiche Möglichkeiten für den Rollout und die Aktualisierung von UCS-Installationen. Sicherheits- und Versionsupdates können über Univention Management Console, über ein Kommandozeilen-Tool und richtliniengesteuert installiert werden. Dies wird in Abschnitt 5.4 beschrieben. Die UCS-Softwareverteilung unterstützt nicht die Aktualisierung von Microsoft Windows-Systemen. Hierfür ist eine zusätzliche Windows-Softwareverteilung nötig.

Für größere Installationen besteht die Möglichkeit, einen lokalen Repository-Server einzurichten, von dem aus alle weiteren Aktualisierungen durchgeführt werden (siehe Abschnitt 5.5). Dieser Repository-Server bezieht seine Pakete entweder vom Univention-Online-Repository oder in Umgebungen ohne Internetzugriff auch durch Offline-Updates in Form von ISO-Images.

Die UCS-Softwareverteilung basiert auf den unterliegenden Debian-Paketmanagement-Tools, wird aber durch UCS-spezifische Werkzeuge ergänzt. Die verschiedenen Werkzeuge zur Installation von Software werden in Abschnitt 5.6 vorgestellt. Die Installation von Versions- und Sicherheitsupdates kann über Richtlinien automatisiert werden, siehe Abschnitt 5.7

Mit dem Software-Monitor steht ein Werkzeug zur Verfügung, mit dem alle Paketinstallationsstände zentral in einer Datenbank erfasst werden, siehe Abschnitt 5.8.

Die Erstinstallation von UCS-Systemen ist nicht Bestandteil dieses Kapitels, sie wird stattdessen in Kapitel 2 beschrieben.

5.2. Unterscheidung der Update-Varianten / Aufbau der UCS-Versionen

Feedback

Vier Arten von UCS-Updates werden unterschieden:

- *Major Releases* erscheinen ca. alle drei bis vier Jahre. Major Releases können sich von vorhergehenden Major Releases signifikant hinsichtlich ihres Leistungsumfangs, ihrer Funktionsweise und der darin enthaltenen Software unterscheiden.

- Während der Maintenance-Dauer eines Major Releases erscheinen *Minor Releases* in einem Rhythmus von ca. 10-12 Monaten. Diese Updates beinhalten die Behebung neu bekannt gewordener Fehler, sowie die Ergänzung des Produkts um zusätzliche Funktionen. Dabei erhalten Minor Releases so weit wie möglich die Kompatibilität zu vorhergehenden Versionen hinsichtlich Funktionsweise, Schnittstellen und Bedienung. Sollte eine Änderung des Verhaltens sinnvoll oder unvermeidbar sein, so wird bei der Veröffentlichung der neuen Version in den Release Notes darauf hingewiesen.

- Univention veröffentlicht fortlaufend *Errata-Updates*. Errata-Updates enthalten Korrekturen für Sicherheitslücken und Bugfixes/kleinere Erweiterungen, die zeitnah für Kundensysteme zur Verfügung gestellt werden sollen. Eine Aufstellung aller Errata-Updates findet sich unter https://errata.software-univention.de/.

- *Patchlevel Releases* fassen ca. alle drei Monate die bis dahin veröffentlichten Errata-Updates zusammen.

Jede ausgelieferte UCS-Version besitzt eine eindeutige Versionsbezeichnung; sie besteht aus einer Zahl (der Majorversion), einem Punkt, einer zweiten Zahl (der Minorversion) einem Bindestrich und einer dritten Zahl (der Patchlevelversion). Mit der Version UCS 4.2-1 wird also das erste Patchlevel-Update für das zweite Minor Update für das Major-Release UCS 4 bezeichnet.

Vor jedem Release-Update wird das *Pre-update-Skript* `preup.sh` aufgerufen. Dieses prüft z.B. ob Probleme bestehen und bricht das Update dann kontrolliert ab. Nach dem Update wird das *Post-Update-Skript* `posttup.sh` aufgerufen, das ggf. weitere Aufräumarbeiten durchführt.

Errata-Updates beziehen sich immer auf bestimmte Minor-Releases, also beispielsweise für UCS 4.4. Errata-Updates können in der Regel für alle Patchlevelversionen eines Minor Releases installiert werden.

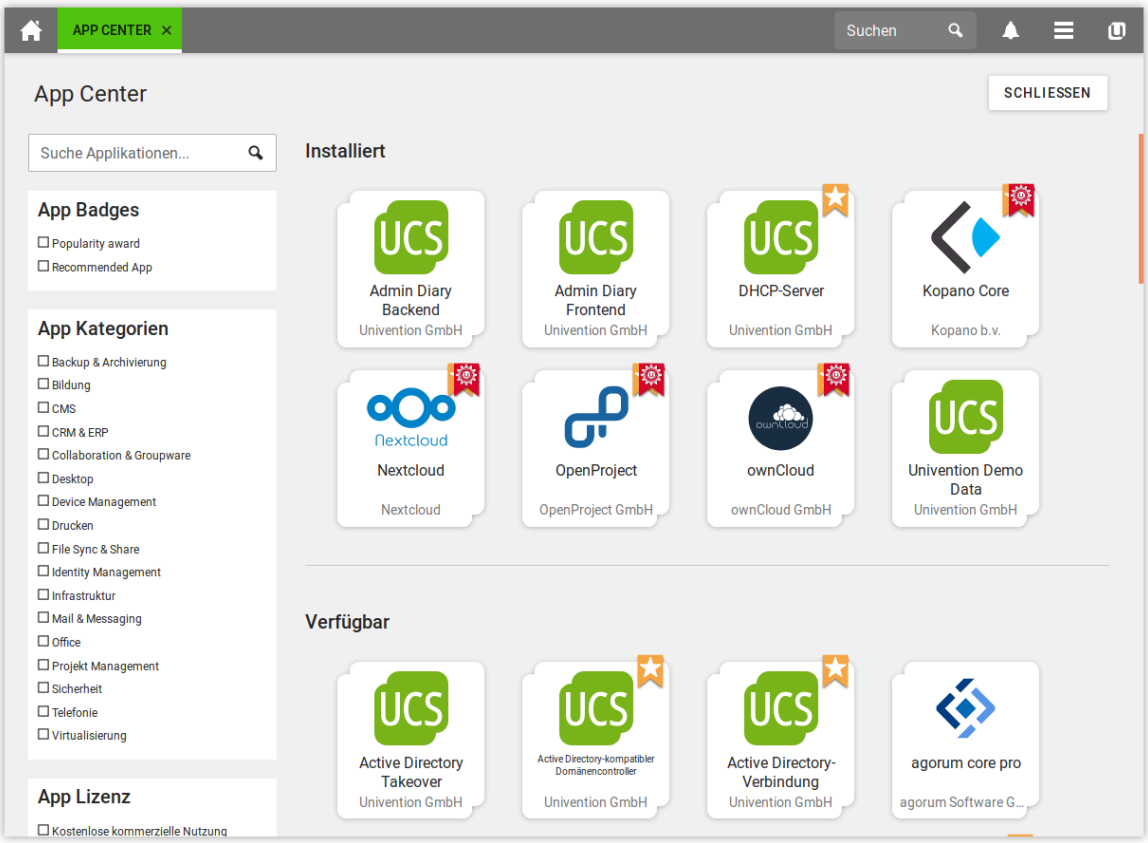
Wenn neue Release- oder Errata-Updates verfügbar sind, wird bei der Anmeldung an Univention Management Console ein entsprechender Hinweis ausgegeben. Die Verfügbarkeit neuer Updates wird außerdem per E-Mail angekündigt, entsprechende Newsletter - getrennt nach Release- und Errata-Updates - können auf der Univention-Webseite abonniert werden. Zu jedem Release-Update wird ein Release-Notes-Dokument veröffentlicht, in dem die aktualisierten Pakete, Hinweise zu Fehlerkorrekturen und neuen Funktionen aufgeführt sind.

5.3. Univention App Center

Feedback

Das Univention App Center erlaubt die einfache Einbindung von Softwarekomponenten in eine UCS-Domäne. Die Applikationen werden sowohl von Drittanbietern wie auch von Univention selbst (z.B. UCS@school) bereitgestellt. Die Maintenance und der Support für die Applikationen erfolgt durch den jeweiligen Hersteller.

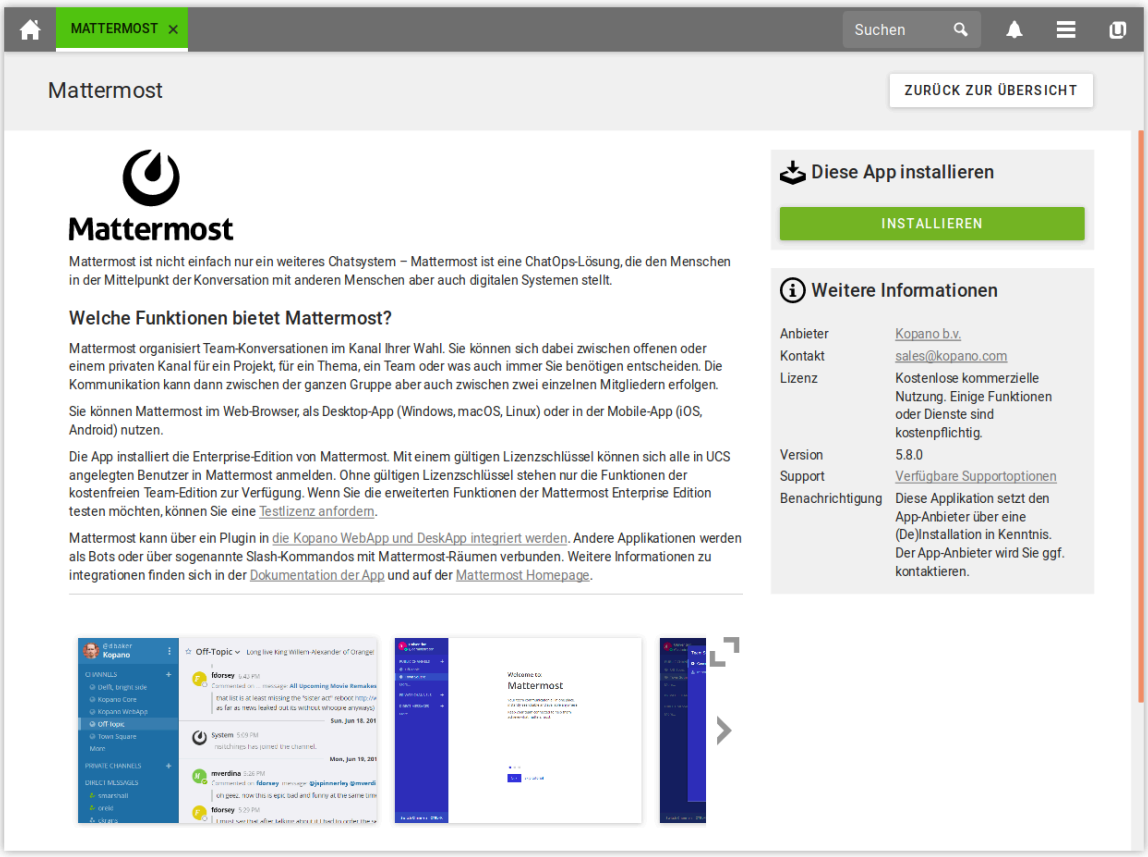
Abbildung 5.1. Überblick der verfügbaren Applikationen im App Center



Das Univention App Center kann über das UMC-Modul *App Center* aufgerufen werden. Es zeigt standardmäßig alle installierten sowie verfügbare Softwarekomponenten an. Mit **Suche Applikationen...** kann die Liste der angezeigten Applikationen auf Suchbegriffe eingeschränkt werden. Außerdem können die Applikationen anhand der **Kategorien** gefiltert werden. Weitere Filterkriterien sind die **App Badges** und die **App Lizenz**. So ist auch eine Kombination der Filter möglich. So kann die Ansicht beispielsweise auf Applikationen aus den Kategorien **`Bildung`** oder **`Office`** eingeschränkt werden. Um hieraus dann die *Recommended Apps* anzuzeigen, genügt die Aktivierung des entsprechenden Filters.

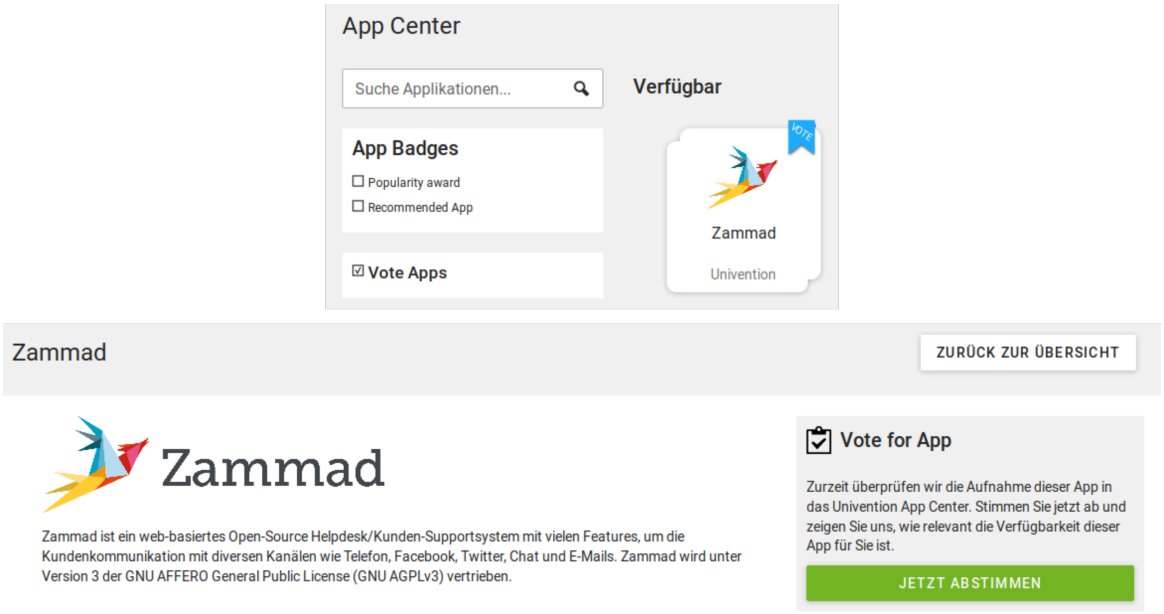
Klickt man auf eine der angezeigten Applikationen, werden weitergehende Details zu der Komponente angezeigt (u.a. Beschreibung, Hersteller, Ansprechpartner und Screenshots oder Videos). Im Feld **Benachrichtigung** wird angezeigt, ob der Hersteller der Softwarekomponente bei der Installation/Deinstallation benachrichtigt wird. Ein grobe Einordnung der Lizenzierung kann unter **Lizenz** entnommen werden. Detaillierte Informationen zur Lizenzierung können bei einigen Applikationen direkt über einen **Kaufen** Button bezogen werden. Für alle anderen Applikationen wird die Kontaktaufnahme mit dem Hersteller der Applikation über die unter **Kontakt** angezeigte E-Mail-Adresse empfohlen.

Abbildung 5.2. Details einer Applikation im App Center



Mit *Vote Apps* gibt es eine spezielle Form von Apps im App Center, die nichts auf dem UCS System installieren. Hierbei handelt es sich um Apps, für die im App Center abgestimmt werden kann. Die Abstimmungen helfen Univention und dem potentiellen App Anbieter dabei, das Interesse für diese App festzustellen. *Vote Apps* werden in der Regel nur für einen begrenzten Abstimmungszeitraum angezeigt. Dass *Vote Apps* verfügbar sind, kann an der angezeigten Filteroption **Vote Apps** in der App Center Übersicht erkannt werden.

Abbildung 5.3. Beispiel *Vote Apps* in App Center Übersicht und Detailansicht



Einige Applikationen sind möglicherweise inkompatibel mit anderen Softwarepaketen aus UCS. So setzen beispielsweise die meisten Groupwarepakete voraus, dass der UCS-Mailstack deinstalliert ist. Jede Applikation prüft, ob inkompatible Versionen installiert sind und gibt einen Hinweis, welche **Konflikte** bestehen und wie sie beseitigt werden können. Die Installation dieser Pakete wird dann zurückgehalten, bis die Konflikte beseitigt sind.

Einige Komponenten integrieren Pakete, die auf dem Domänencontroller Master installiert werden müssen (in der Regel LDAP-Schema-Erweiterungen oder Erweiterungen für das UCS-Managementsystem). Diese Pakete werden automatisch auf dem Domänencontroller Master installiert. Ist dieser nicht erreichbar, wird die Installation abgebrochen. Außerdem werden die Pakete auf allen erreichbaren Domänencontroller Backup-Systemen eingerichtet. Sofern mehrere UCS Systeme in der Domäne vorhanden sind, kann ausgewählt werden, auf welchem der Systeme die Applikation installiert werden soll.

Einige Applikationen nutzen die Container-Technologie Docker. Dadurch wird die Applikation (und ihre unmittelbare Umgebung) vom Rest gekapselt und die Sicherheit sowie die Kompatibilität von Applikationen untereinander erhöht.

Technisch wird die App als Docker Container gestartet und als Memberserver in die UCS Domäne gejoint. Für den Memberserver wird im LDAP ein zugehöriges Rechner-Objekt angelegt.

Der Container ist per Netzwerk nur von dem Rechner aus zu erreichen, auf dem die App installiert ist. Die App kann aber bestimmte Ports öffnen, die dann vom eigentlichen Rechner in den Container weitergeleitet werden. Die Firewall von UCS wird entsprechend automatisch konfiguriert, damit der Zugriff auf die Ports möglich ist.

Wird eine Kommandozeile in der Umgebung der App benötigt, muss zunächst in den Container gewechselt werden. Dazu kann folgender Befehl ausgeführt werden (hier am Beispiel der fiktiven App demo-docker-app):

```
univention-app shell demo-docker-app
```

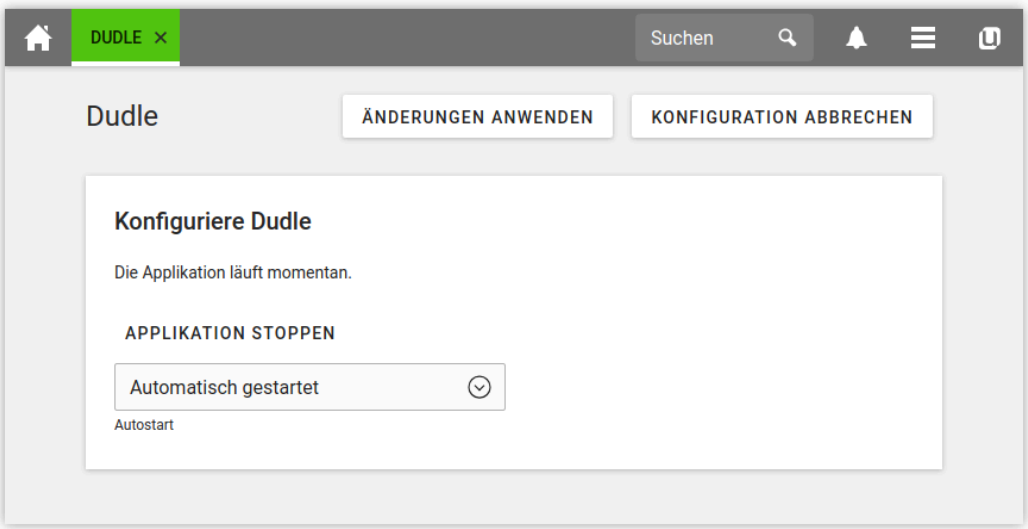
Docker Apps lassen sich über das UMC-Modul weiter konfigurieren. Die App kann gestartet und gestoppt, sowie die **Autostart**-Option gesetzt werden:

- Automatisch gestartet sorgt dafür, dass die App automatisch beim Hochfahren des Servers gestartet wird.

- Manuell gestartet verhindert den automatischen Start der App, sie kann aber über das UMC-Modul gestartet werden.
- Start wird verhindert unterbindet grundsätzlich den Start der App; sie kann dann auch nicht über das UMC-Modul gestartet werden.

Darüber hinaus können Apps ggf. über weitere Parameter angepasst werden. Das Menü dafür ist über den Button App-Einstellungen einer installierten App zu erreichen.

Abbildung 5.4. Einstellungen einer Applikation im App Center



Nach der Installation einer Applikation werden beim Klick auf das Icon einer Applikation eine oder mehrere neue Optionen angezeigt: **Deinstallieren** entfernt eine Applikation. **Öffnen** verweist auf eine Webseite oder ein UMC-Modul, mit dem die installierte Applikation weitergehend konfiguriert oder verwendet werden kann. Installiert man beispielsweise die Horde-Applikation, führt dieser Link auf den Login-Dialog. Bei Applikationen ohne Webinterface oder UMC-Modul wird die Option nicht angezeigt.

Aktualisierungen für Applikationen erfolgen unabhängig von den Release-Zyklen für Univention Corporate Server. Ist eine neue Version einer Applikation verfügbar, wird der Menüpunkt **Aktualisieren** angezeigt, der die Installation der neuen Version startet. Wenn Aktualisierungen verfügbar sind, wird außerdem im UMC-Modul **Software-Aktualisierung** Univention Management Console ein entsprechender Hinweis ausgegeben.

Eine Übersicht über die installierten Applikationen in der Domäne kann auf der UMC-Startseite unter **Installierte Applikationen** abgerufen werden. Installationen und das Entfernen von Paketen werden in der Logdatei `/var/log/univention/management-console-module-appcenter.log` protokolliert.

5.4. Aktualisierung von UCS-Systemen

Feedback

UCS-Systeme können auf zwei Wegen aktualisiert werden; entweder pro einzelnem System (über Univention Management Console oder auf der Kommandozeile) oder für größere Gruppen von UCS-Systemen automatisiert über eine UMC-Rechner-Richtlinie.

5.4.1. Update-Strategie in Umgebungen mit mehr als einem UCS-System

Feedback

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

Auf dem Domänencontroller Master wird die 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 (siehe Abschnitt 3.4.1) muss der Domänencontroller Master bei einem Release-Update immer als erstes System aktualisiert werden.

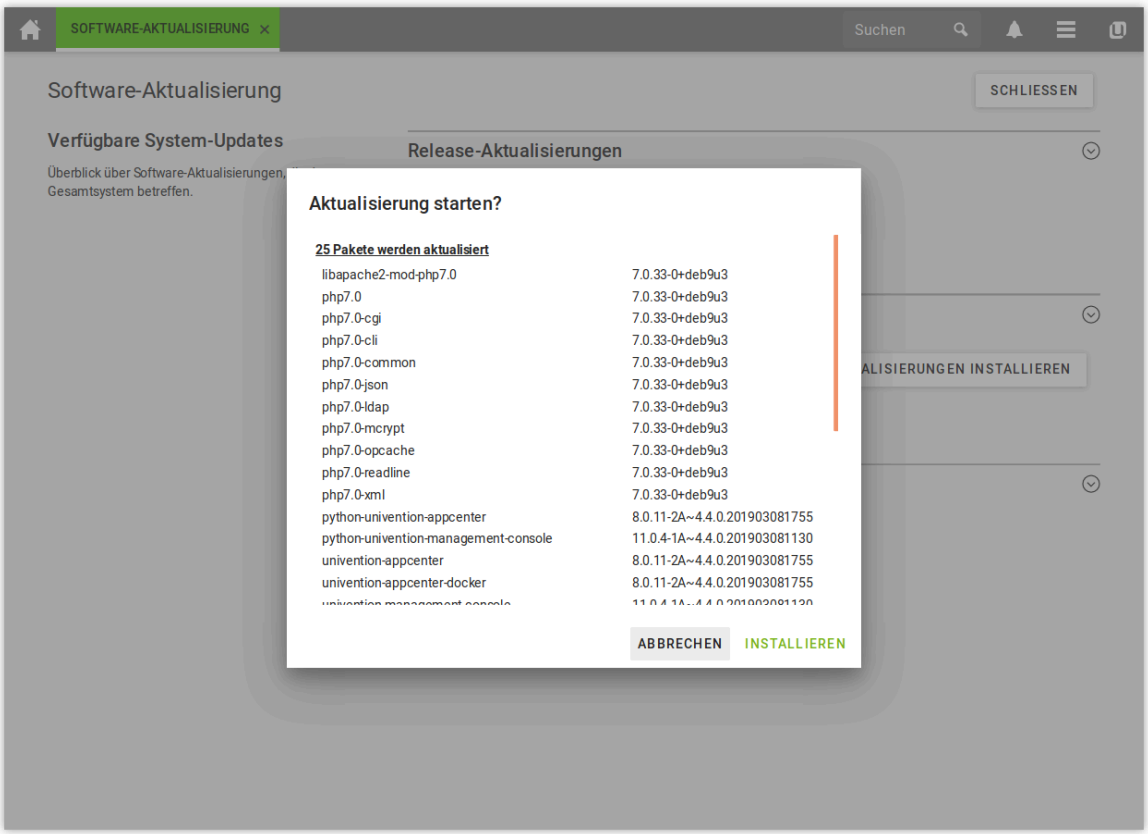
Generell ist es empfehlenswert, alle UCS-Systeme möglichst in einem Wartungsfenster zu aktualisieren. Wo dies nicht möglich ist, sollten die nicht-aktualisierten UCS-Systeme gegenüber dem Domänencontroller Master nur eine Release-Version älter sein.

5.4.2. Aktualisierung eines einzelnen Systems in Univention Management Console

Mit dem UMC-Modul **Software-Aktualisierung** können Versions- und Errata-Updates installiert werden.

In Abbildung 5.5 ist die Übersichtsseite des Moduls dargestellt. Im oberen Teil des Dialogs wird unter **Release-Aktualisierungen** der aktuelle Installationsstand angezeigt.

Abbildung 5.5. Aktualisierung eines UCS-Systems über UMC



Sollte eine neuere UCS-Version vorhanden sein, wird eine Auswahlliste präsentiert. Durch einen Klick auf **Release-Aktualisierungen installieren** werden nach Bestätigung alle Updates bis zur jeweiligen Version eingespielt. Zuvor wird ein Hinweis auf mögliche Einschränkungen der Serverdienste während des Updates angezeigt. Eventuelle Zwischenversionen werden automatisch mitinstalliert.

Durch einen Klick auf **Errata-Aktualisierungen installieren** werden alle für das aktuelle Release und die eingebundenen Komponenten verfügbaren Errata-Updates eingerichtet.

Mit **Paket-Aktualisierungen prüfen** wird eine Aktualisierung der momentan eingetragenen Paketquellen aktiviert. Dies kann etwa verwendet werden, wenn für eine Komponente eine aktualisierte Version bereitgestellt wurde.

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.4.3. Aktualisierung eines einzelnen Systems auf der Kommandozeile

Die folgenden Schritte müssen mit `root`-Rechten durchgeführt werden.

Ein einzelnes UCS-System kann auf der Kommandozeile mit dem Befehl `univention-upgrade` aktualisiert werden. Es wird geprüft, ob neue Release oder Applikations-Updates vorliegen, die dann nach Bestätigung einer Nachfrage installiert werden. Außerdem werden Paket-Aktualisierungen durchgeführt (z.B. im Rahmen eines Errata-Updates).

In der Grundeinstellung werden die zu aktualisierenden Pakete über das Netz aus einem Repository geladen. Wird ein lokales Repository eingesetzt (siehe Abschnitt 5.5.4), können Release-Updates alternativ auch über Update-DVD-Images installiert werden, die entweder als ISO-Datei oder von einem Laufwerk eingelesen werden. Dazu muss `univention-upgrade` mit den Parametern `--iso=`*`ISOIMAGEDATEI`* oder `--cdrom=`*`LAUFWERK`* aufgerufen werden.

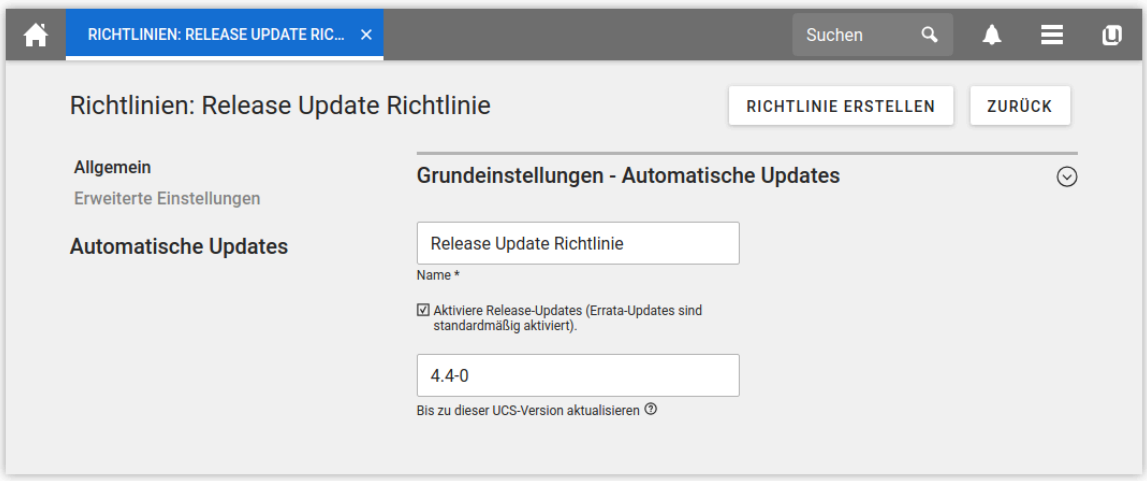
Von einer Remote-Aktualisierung über SSH wird abgeraten, da dies zum Abbruch des Update-Vorgangs führen kann. Sollte dennoch eine Aktualisierung über eine Netzverbindung durchgeführt werden, ist sicherzustellen, dass das Update bei Unterbrechung der Netzverbindung trotzdem weiterläuft. Hierfür können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

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.4.4. Aktualisierung von Systemen über eine Rechner-Richtlinie

Mit einer **Automatische Updates**-Richtlinien in den UMC-Modulen zur Rechner- und Domänenverwaltung lässt sich ein Update für mehrere Rechner konfigurieren (siehe auch Abschnitt 4.6).

Abbildung 5.6. Aktualisierung eines UCS-Systems über eine Update-Richtlinie



Nur wenn das Auswahlfeld **Aktiviere Release-Updates** aktiviert ist, wird eine Release-Aktualisierung durchgeführt.

Das Eingabefeld **Bis zu dieser UCS-Version aktualisieren** enthält die Versionsnummer, bis zu der das System aktualisiert werden soll, z.B. *4.4-0*. Wird keine Angabe gemacht, aktualisiert sich das System bis zur höchsten verfügbaren Versionsnummer.

Der Zeitpunkt, zu dem die Aktualisierung durchgeführt wird, wird über eine **Paketpflege**-Richtlinie konfiguriert (siehe Abschnitt 5.7).

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben.

5.4.5. Nachbereitung von Release-Updates

Feedback

Nach erfolgreicher Durchführung eines Release-Updates sollte geprüft werden, ob neue oder aktualisierte Join-Skripte ausgeführt werden müssen. Zur Überprüfung und zum Starten der Join-Skripte kann entweder das UMC-Modul *Domänenbeitritt* verwendet werden oder das Kommandozeilenprogramm `univention-run-join-scripts` (siehe Abschnitt 3.2.1).

5.4.6. Fehlersuche bei Updateproblemen

Feedback

Die während der Aktualisierung erzeugten Meldungen werden in die Datei `/var/log/univention/updater.log` geschrieben, die zur weiteren Fehleranalyse herangezogen werden kann.

Der Stand der Univention Configuration Registry-Variablen vor der Release-Aktualisierung wird in dem Verzeichnis `/var/univention-backup/update-to-ZIELRELEASEVERSION/` gesichert. Damit kann geprüft werden, ob und welche Variablen im Rahmen des Updates verändert wurden.

5.5. Konfiguration des Repository-Servers für Updates und Paketinstallationen

Feedback

Paketinstallationen und Updates können entweder vom Univention-Update-Server oder von einem lokal gepflegten Repository durchgeführt werden. Ein lokales Repository ist sinnvoll, wenn viele UCS-Systeme zu aktualisieren sind, da Updates in diesem Fall nur einmalig heruntergeladen werden müssen. Da Repositorys auch offline aktualisiert werden können, ermöglicht ein lokales Repository auch die Aktualisierung von UCS-Umgebungen ohne Internetanbindung.

Anhand der registrierten Einstellungen werden APT-Paketquellen für Release- und Errata-Updates sowie Addon-Komponenten im Verzeichnis `/etc/apt/sources.list.d/` automatisch generiert. Sollten auf einem System weitere Repositorys benötigt werden, können diese in die Datei `/etc/apt/sources.list` eingetragen werden.

Bei einer Neuinstallation wird in der Grundeinstellung das Univention-Repository `updates.software-univention.de` verwendet.

Das Univention-Repository und andere Repository-Komponenten unterscheiden zwischen zwei Bestandteilen:

- Der von der Maintenance abgedeckte Standard-Paketumfang von UCS befindet sich im *maintained*-Bereich. Standardmäßig ist nur der Zugriff auf diese Pakete aktiviert. Sicherheits-Updates werden zeitnah nur für Pakete aus *maintained* bereitgestellt.
- Unter *unmaintained* finden sich die weiteren Pakete, z.B. andere Mailserver als Postfix. Diese Pakete sind nicht durch Sicherheits-Updates oder anderweitige Maintenance abgedeckt. *unmaintained* ist standardmäßig nicht eingebunden

Ein lokales Repository kann - gerade bei Einbindung des unmaintained-Zweiges - viel Plattenplatz in Anspruch nehmen.

5.5.1. Konfiguration über Univention Management Console

Feedback

Im UMC-Modul **Repository-Einstellungen** kann der **Repository-Server** und die Verwendung der Maintained- und Unmaintained-Sektionen festgelegt werden.

5.5.2. Konfiguration über Univention Configuration Registry

Feedback

Der zu verwendende Repository-Server wird in die Univention Configuration Registry-Variable `repository/online/server` eingetragen und ist bei einer Neuinstallation auf `updates.software-univention.de` voreingestellt.

Das unmaintained-Repository kann durch Setzen der Univention Configuration Registry-Variable `repository/online/unmaintained` auf `yes` integriert werden.

5.5.3. Richtlinienbasierte Konfiguration des Repository-Servers

Feedback

Der zu verwendende Repository-Server kann auch über die Richtlinie **Repository-Server** in der UMC-Rechnerverwaltung festgelegt werden. In dem Auswahlfeld werden UCS-Server-Systeme angezeigt, für die ein DNS-Eintrag hinterlegt ist (siehe auch Abschnitt 4.6).

5.5.4. Einrichtung und Aktualisierung eines lokalen Repositorys

Feedback

Paketinstallationen und Updates können entweder vom Univention-Update-Server oder von einem lokal gepflegten Repository durchgeführt werden. Ein lokales Repository ist sinnvoll wenn viele UCS-Systeme zu aktualisieren sind, da Updates in diesem Fall nur einmalig heruntergeladen werden müssen. Da Repositorys auch offline aktualisiert werden können, ermöglicht ein lokales Repository auch die Aktualisierung von UCS-Umgebungen ohne Internetanbindung.

Es besteht auch die Möglichkeit lokale Repositorys zu synchronisieren, so dass beispielsweise in der Firmenzentrale ein Haupt-Repository gepflegt wird, das dann in lokale Repositorys der einzelnen Standorte synchronisiert wird. Um ein Repository einzurichten, muss der Befehl `univention-repository-create` als Benutzer `root` aufgerufen werden. Der initiale Paketbestand wird von einer Installations-DVD eingelesen, mit dem Parameter `--iso` kann hier auch ein ISO-Image übergeben werden. UCS ist nur als 64 Bit-DVD verfügbar. Das Repository wird von `univention-repository-create` mit der Architektur des angegebenen Installationsmediums erzeugt. Wird eine Umgebung betrieben, in der sowohl 32-, als auch 64 Bit-Pakete bereitgestellt werden sollen, sind die folgenden Befehle auf dem Repository-Server nötig:

```
ucr set repository/online/architectures="i386 amd64"
univention-repository-update net
```

Der Zugriff auf das Univention Online-Repository wird durch Verwendung von Secure APT über Signaturen kryptografisch gesichert. Für lokale Repositorys besteht diese Möglichkeit aktuell noch nicht, so dass beim Erstellen eines Repositorys ein Hinweis ausgegeben wird, wie Secure APT mit der Univention Configuration Registry-Variable `update/secure_apt` deaktiviert werden kann. Diese Einstellung muss auf allen UCS-Systemen gesetzt werden, die auf das Repository zugreifen.

Mit dem Tool `univention-repository-update` werden die Pakete im Repository aktualisiert. Es unterstützt zwei Modi:

- `univention-repository-update cdrom` Dabei wird das Repository über eine Update-DVD oder ein ISO-Image aktualisiert.

- `univention-repository-update net` Bei dieser Variante wird das Repository mit einem angegebenen anderen Repository-Server synchronisiert. Dieser ist in der Univention Configuration Registry-Variable `repository/mirror/server` definiert (typischerweise `updates.software-univention.de`).

Eine Übersicht über die möglichen Optionen kann mit folgendem Befehl aufgerufen werden:

```
univention-repository-update -h
```

Das Repository wird im Verzeichnis `/var/lib/univention-repository/mirror/` vorgehalten.

Durch die Univention Configuration Registry-Variable `local/repository` kann das lokale Repository aktiviert/deaktiviert werden.

5.6. Installation weiterer Software

Feedback

Die Erstauswahl der Softwarekomponenten eines UCS-Systems erfolgt im Rahmen der Installation. Die Auswahl der Softwarekomponenten erfolgt dabei funktionsbezogen, indem etwa die Komponente *Proxy-Server* ausgewählt wird, die dann über ein Meta-Paket die eigentlichen Software-Pakete nachzieht. Der Administrator muss dazu die eigentlichen Paketnamen nicht kennen. Für weitergehende Aufgaben können aber auch einzelne Pakete gezielt installiert und entfernt werden. Bei der Installation eines Pakets werden unter Umständen Pakete mitinstalliert, die für die Funktion des angegebenen Pakets erforderlich sind, die sogenannten Paketabhängigkeiten. Alle Softwarekomponenten werden aus einem Repository geladen (siehe Abschnitt 5.5).

Fremdsoftware, die nicht im Debian-Paketformat vorliegt, sollte in die Verzeichnisse `/opt/` oder `/usr/local/` installiert werden. UCS-Pakete nutzen diese Verzeichnisse nicht, so dass eine saubere Trennung von UCS- und Fremdsoftware gewährleistet ist.

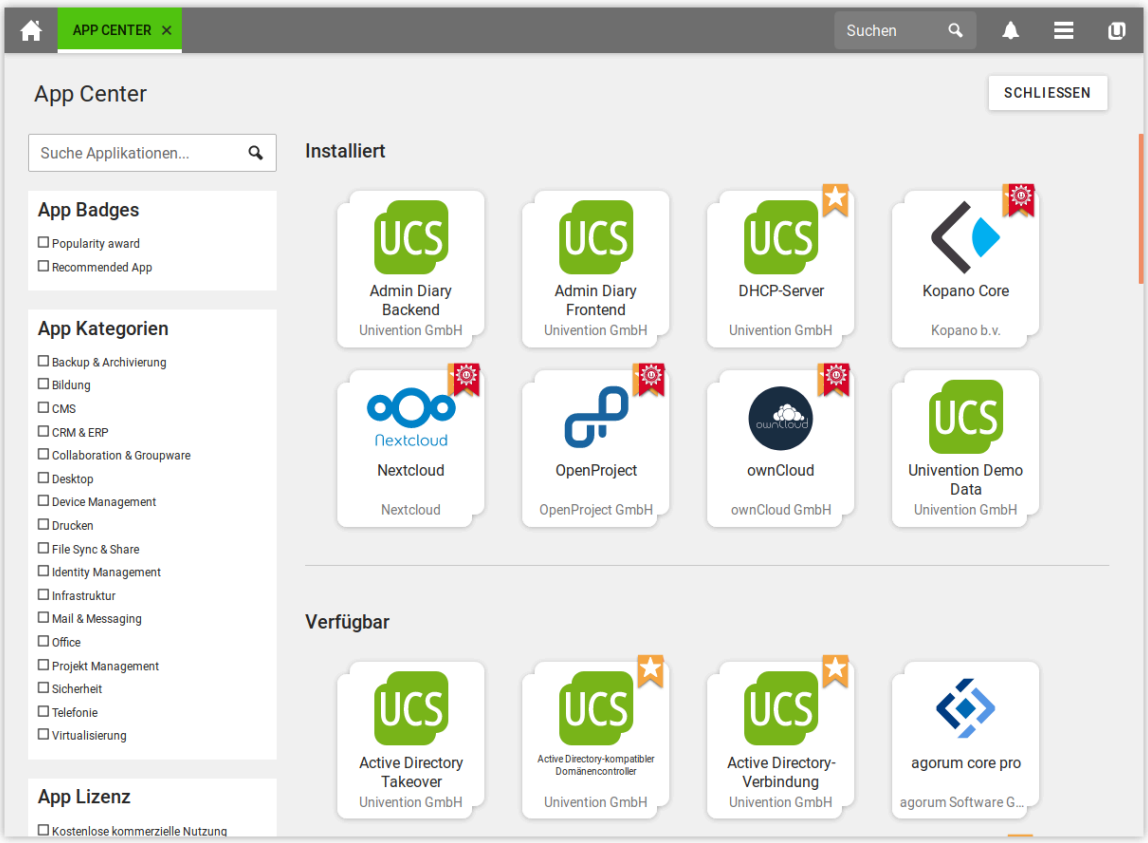
Um auf einem bereits installierten System nachträglich weitere Pakete zu installieren, stehen mehrere Möglichkeiten zur Verfügung:

5.6.1. Installation/Deinstallation von UCS-Komponenten im Univention App Center

Feedback

Alle Softwarekomponenten, die im Univention Installer angeboten werden, können auch über das Univention App Center nachträglich installiert und entfernt werden. Dazu muss die Paket-Kategorie **UCS-Komponenten** ausgewählt werden. Weitere Hinweise zum Univention App Center finden sich in Abschnitt 5.3.

Abbildung 5.7. Auswahl von UCS-Komponenten im App Center

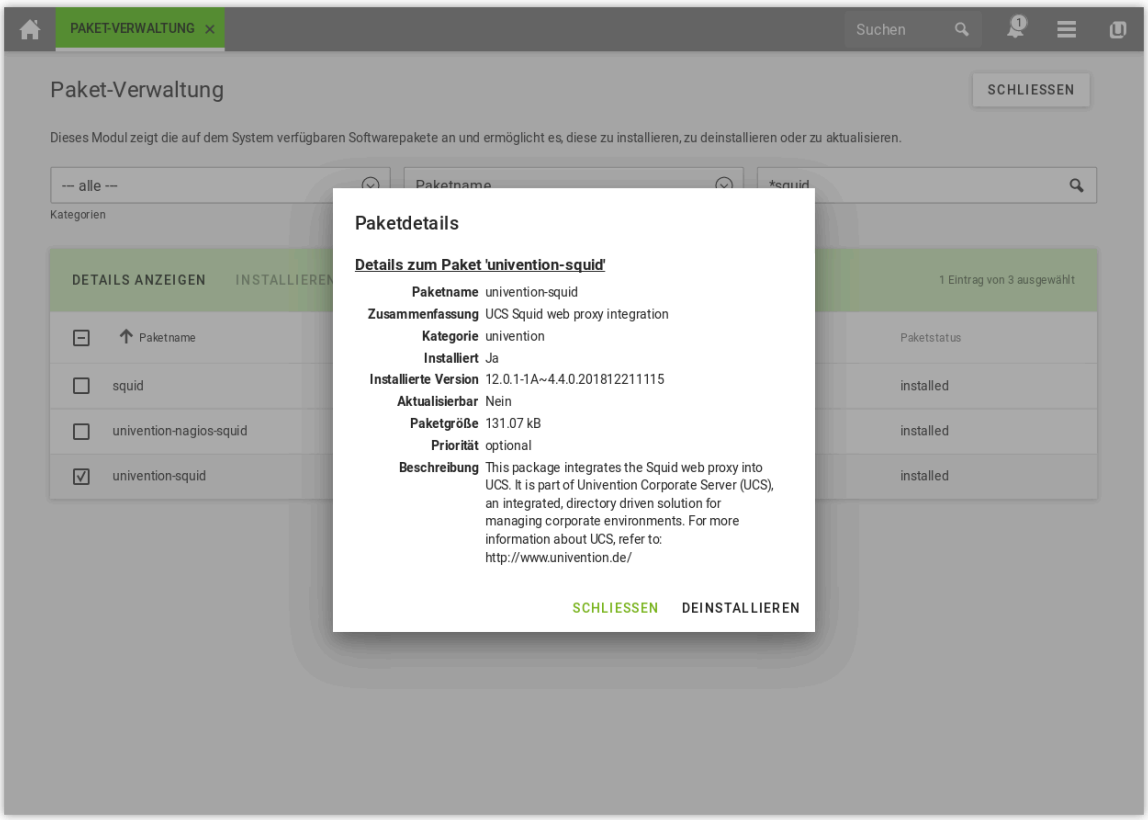


5.6.2. Installation/Deinstallation von einzelnen Paketen in Univention Management Console

Feedback

Mit dem Univention Management Console-Modul **Paket Verwaltung** können einzelne Softwarepakete installiert und deinstalliert werden.

Abbildung 5.8. Installation des Pakets *univention-squid* in Univention Management Console



Auf der Startseite wird eine Suchmaske angezeigt in der die Paketkategorie und ein Suchfilter (Name oder Beschreibung) zur Auswahl stehen. Die Ergebnisliste besteht aus einer Tabelle mit den folgenden Spalten:

- Paketname
- Paketbeschreibung
- Paketstatus

Durch einen Klick auf eine Zeile in der Ergebnisliste wird eine detaillierte Informationsseite zu dem Softwarepaket angezeigt, u.a. eine ausführliche Beschreibung und die Versionsnummer.

Zusätzlich werden ein oder mehrere Buttons angezeigt: **Installieren** wird angezeigt, falls das Softwarepaket noch nicht installiert ist, **Deinstallieren**, falls das Paket installiert ist und **Aktualisieren** falls das Softwarepaket bereits installiert, aber nicht aktuell ist. Durch **Schließen** kann zu der vorherigen Suchabfrage zurückgekehrt werden.

5.6.3. Installation/Deinstallation von einzelnen Paketen auf der Kommandozeile

Die folgenden Schritte müssen mit `root`-Rechten durchgeführt werden.

Die Installation einzelner Pakete erfolgt mit dem Kommando

```
univention-install PAKETNAME
```

Pakete können mit dem folgenden Befehl entfernt werden:

```
univention-remove PAKETNAME
```

Wenn der Name eines Pakets nicht bekannt ist, kann mit dem Kommando `apt-cache search` nach Paketen gesucht werden. Als Aufrufparameter können Teile des Namens oder Wörter, die in der Beschreibung eines Paketes vorkommen angegeben werden, z.B.

```
apt-cache search fax
```

5.6.4. Hook Skripte für Administratoren

Feedback

Benutzerdefinierte Skripte können nach jeder Installation, Aktualisierung oder Deinstallation von Apps ausgeführt werden. Solche Skripte erlauben die Automatisierung wiederkehrender administrativer Aufgaben.

Um von dieser Eigenschaft Gebrauch zu machen können Skripte in einem der folgenden Verzeichnisse abgelegt werden. Wenn ein solches Verzeichnis noch nicht existiert, kann es manuell angelegt werden.

```
/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-install.d/
/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-upgrade.d/
/var/lib/univention-appcenter/apps/{appid}/local/hooks/post-remove.d/
```

Wobei *`{appid}`* der Name einer App ist, für welche die Skripte ausgeführt werden sollen.

Dateinamen dürfen nur aus Kleinbuchstaben und Zahlen bestehen (`^[a-z0-9]+$`). Außerdem müssen die Dateien als ausführbar markiert sein (`chmod +x [Dateiname]`) denn sie werden intern von `run-parts` aufgerufen. Daher kann mit `run-parts --test [Verzeichnis]` getestet werden, ob und welche Dateien ausgeführt werden würden. Weitere Informationen können der Handbuchseite entnommen werden mit `man run-parts`.

Die `/var/log/univention/appcenter.log` enthält mögliche Fehler bei der Ausführung der Skripte und weitere Hinweise.

5.6.5. Richtlinienbasierte Installation/Deinstallation von einzelnen Paketen über Paketlisten

Feedback

Mit Paketlisten kann richtlinienbasiert Software installiert und entfernt werden. Dadurch lassen sich auch große Stückzahlen an Rechnersystemen zentral mit neuer Software versehen.

Jede Systemrolle verfügt über eine eigenen Paket-Richtlinien-Typ.

Paketrichtlinien werden im UMC-Modul *Richtlinien* mit dem Objekttyp **Richtlinie: Pakete + Systemrolle** verwaltet.

Tabelle 5.1. Karteikarte '[Pakete ...]'

Attribut	Beschreibung
Name	Ein eindeutiger Name für diese Paketliste, z.B. *Standort-Server*.
[...] Pakete Installationsliste	Eine Liste zu installierender Pakete.
[...] Pakete Deinstallationsliste	Eine Liste zu entfernender Pakete.

Die in einer Paketliste definierten Softwarepakete werden zu dem in der **Paketpflege**-Richtlinie definierten Zeitpunkt (zur Konfiguration siehe Abschnitt 5.7) installiert, bzw. deinstalliert.

Die in den Pakete-Richtlinien zuordbaren Softwarepakete werden ebenfalls im LDAP registriert.

5.7. Festlegung eines Aktualisierungs-Zeitpunkts mit der Paketpflege-Richtlinie

Feedback

Mit einer **Paketpflege**-Richtlinie (siehe auch Abschnitt 4.6) in den UMC-Modulen zur Rechner und Domänenverwaltung kann ein Zeitpunkt vorgegeben werden, an dem die folgenden Schritte durchgeführt werden:

- Prüfung auf verfügbare und zu installierende Release-Updates (siehe Abschnitt 5.4.4) und ggf. Installation
- Installation/Deinstallation von Paketlisten (siehe Abschnitt 5.6.5)
- Installation verfügbarer Errata-Updates

Alternativ können die Aktualisierungen auch beim Systemstart oder beim Herunterfahren des Systems erfolgen.

Tabelle 5.2. Karteikarte '[Paketpflege]'

Attribut	Beschreibung
Paketpflege durchführen nach Hochfahren des Systems	Falls diese Option aktiviert ist, werden die Aktualisierungsschritte während des Startvorgangs des Rechners durchgeführt.
Paketpflege durchführen vor Herunterfahren des Systems	Falls diese Option aktiviert ist, werden die Aktualisierungsschritte beim Herunterfahren des Rechners durchgeführt.
Cron Einstellung benutzen	Wird dieses Feld aktiviert, kann über die Felder *Monat*, *Wochentag*, *Tag*, *Stunde* und *Minute* ein genauer Zeitpunkt angegeben werden, an dem die Aktualisierungsschritte durchgeführt werden sollen.
Nach Paketpflege neu starten	Diese Option ermöglicht es, nach Release-Aktualisierungen optional einen automatischen Neustart des Systems durchzuführen, entweder direkt oder nach dem angegebenen Zeitintervall in Stunden.

5.8. Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor

Feedback

Der Software-Monitor ist eine Datenbank, in der Informationen über die auf UCS-Systemen installierten Softwarepakete aufgezeichnet werden. Durch diese Datenbank kann sich ein Administrator einen Überblick verschaffen, welche Release- und Paketversionen auf den Systemen der Domäne installiert sind und diese Informationen bei der schrittweisen Aktualisierung einer UCS-Domäne nutzen und Installations-Probleme erkennen.

Der Software-Monitor kann mit der Applikation *Software-Installationsmonitor* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-pkgdb*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

UCS-Systeme aktualisieren ihre Einträge bei der Installation, Entfernung und Aktualisierung von Software automatisch. Das System, auf dem der Software-Monitor betrieben wird, wird dabei durch den DNS-Service-Record `_pkgdb._tcp` lokalisiert.

Die webbasierte Abfrageschnittstelle des Software-Monitors integriert sich in die Univention Management Console und kann über das Modul **Software-Monitor** erreicht werden. Folgende Funktionen stehen zur Verfügung:

- *Systeme* erlaubt die Suche nach den installierten Versionsständen von UCS-Systemen. Es kann nach Systemnamen, UCS-Versionen und Systemrollen gesucht werden.

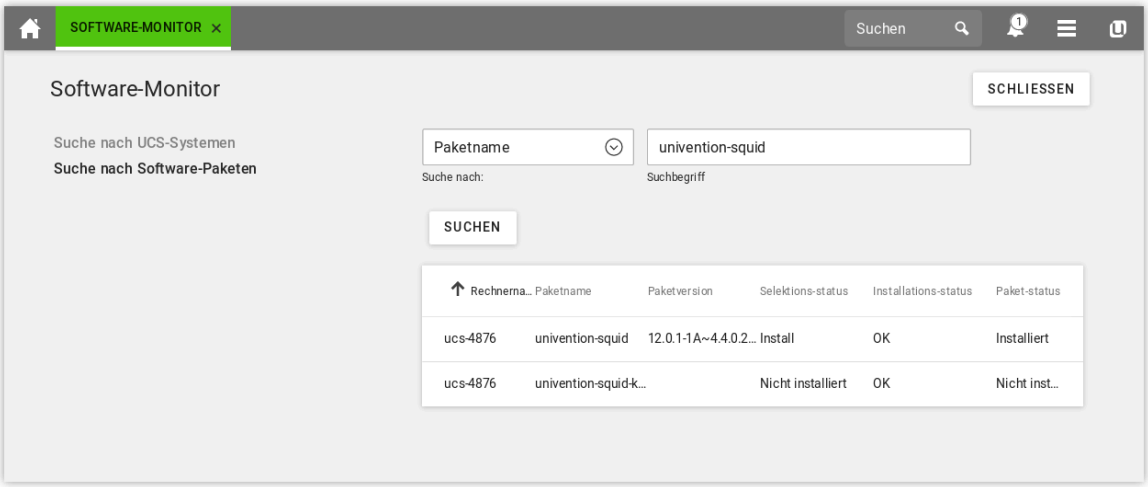
- *Pakete* ermöglicht die Suche in den von der Paketstatusdatenbank erfassten Installationsdaten. Neben der Suche nach *Paketnamen* gibt es auch die folgenden Suchmöglichkeiten zu den Installationszuständen von Paketen:

  - Der *Selektionsstatus* beeinflusst das Verhalten bei der Aktualisierung eines Pakets. Durch `Install` wird ein Paket zur Installation ausgewählt. Ist ein Paket auf `Hold` konfiguriert, so wird es von weiterer Aktualisierung ausgenommen. Es existieren zwei Möglichkeiten ein Paket zu deinstallieren: Ein mit `DeInstall` entferntes Paket hält lokal erzeugte Konfigurations-Daten weiterhin vor, während ein mit `Purge` entferntes Paket komplett gelöscht wird.

  - Der *Installationsstatus* beschreibt den Status eines installierten Pakets im Hinblick auf kommende Aktualisierungen. Der Normalfall ist `Ok`, was dazu führt, dass ein Paket bei Vorhandensein einer aktuelleren Version aktualisiert würde. Ist ein Paket auf `Hold` konfiguriert, so wird es von der Aktualisierung ausgenommen.

  - Der *Paketstatus* beschreibt den Zustand eines eingerichteten Pakets. Der Normalfall ist `Installed` für installierte und `ConfigFiles` für entfernte Pakete, alle übrigen Zustände entstehen, wenn die Installation des Pakets in verschiedenen Phasen abgebrochen wurde.

Abbildung 5.9. Suche nach Paketen im Software-Monitor



Wenn verhindert werden soll, dass UCS-Systeme Installations-Vorgänge im Software-Monitor aufzeichnen (etwa weil keine Netzwerkverbindung zur Datenbank besteht), kann dies durch Setzen der Univention Configuration Registry-Variable `pkgdb/scan` auf `no` abgeschaltet werden. Wenn die Aufzeichnungen danach wieder aktiviert werden, muss das Kommando `univention-pkgdb-scan` ausgeführt werden, damit die in der Zwischenzeit installierten Paketversionen in die Datenbank übernommen werden.

Mit dem folgenden Befehl kann der Programmbestand eines Systems wieder aus der Datenbank entfernt werden:

```
univention-pkgdb-scan --remove-system RECHNERNAME
```

Kapitel 6. Benutzerverwaltung

UCS integriert ein zentrales Identity-Management. Alle Benutzerinformationen werden in UCS zentral über Univention Management Console verwaltet und im LDAP-Verzeichnisdienst gespeichert.

Alle in die Domäne integrierten Dienste greifen dabei auf die zentralen Konto-Informationen zu, d.h. für die Benutzeranmeldung an einem Windows-Client wird die gleiche Benutzerkennung und das gleiche Passwort verwendet wie etwa bei der Anmeldung am IMAP-Server.

Die domänenweite Verwaltung von Benutzerdaten verringert den administrativen Aufwand, da Änderungen nicht auf verschiedenen Einzelsystemen nachkonfiguriert werden müssen. Darüber hinaus vermeidet dies Folgefehler, die sich durch Inkonsistenzen zwischen den einzelnen Datenbeständen ergeben können.

In UCS gibt es drei unterschiedliche Arten von Benutzern:

1. *Vollwertige Benutzerkonten*: Normale, vollwertige Benutzerkonten haben sämtliche verfügbaren Eigenschaften. Diese Benutzer können sich an UCS- oder Windows-Systemen anmelden und je nach Konfiguration auch an den installierten Apps. Die Benutzer können über das UMC-Modul **Benutzer** (siehe Abschnitt 6.1) administriert werden.

2. *Adressbucheinträge*: Adressbucheinträge können für die Pflege von internen oder externen Kontaktinformationen verwendet werden. Diese Kontakte können sich nicht an UCS- oder Windows-Systemen anmelden. Adressbucheinträge können über das UMC-Modul **Kontakte** verwaltet werden.

3. *Einfaches Authentisierungskonto*: Mit einem einfachen Authentisierungskonto wird ein Benutzer-Objekt angelegt, welches ausschließlich einen Benutzernamen und ein Passwort hat. Mit diesem Konto ist ausschließlich eine Authentisierung gegen den LDAP-Verzeichnisdienst möglich, aber keine Anmeldung an UCS- oder Windows-Systemen. Einfache Authentisierungskonten können über das UMC-Modul **LDAP-Verzeichnis** (siehe Abschnitt 4.5) erstellt werden.

6.1. Verwaltung von Benutzern mit Univention Management Console

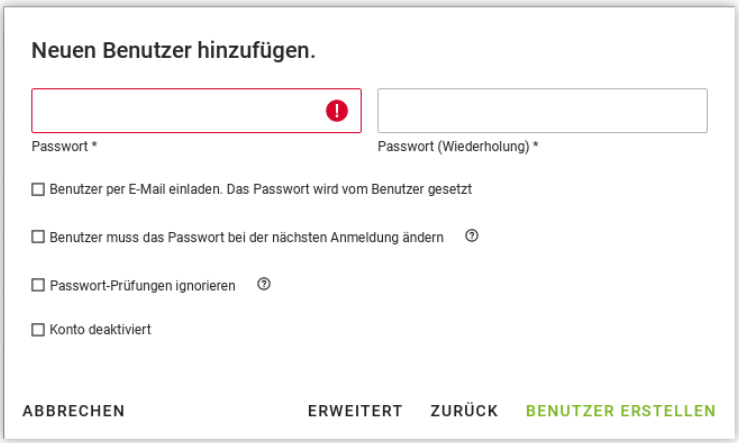
Feedback

Benutzer werden im UMC-Modul *Benutzer* verwaltet (siehe auch Abschnitt 4.4).

Abbildung 6.1. Anlegen eines Benutzers in UMC

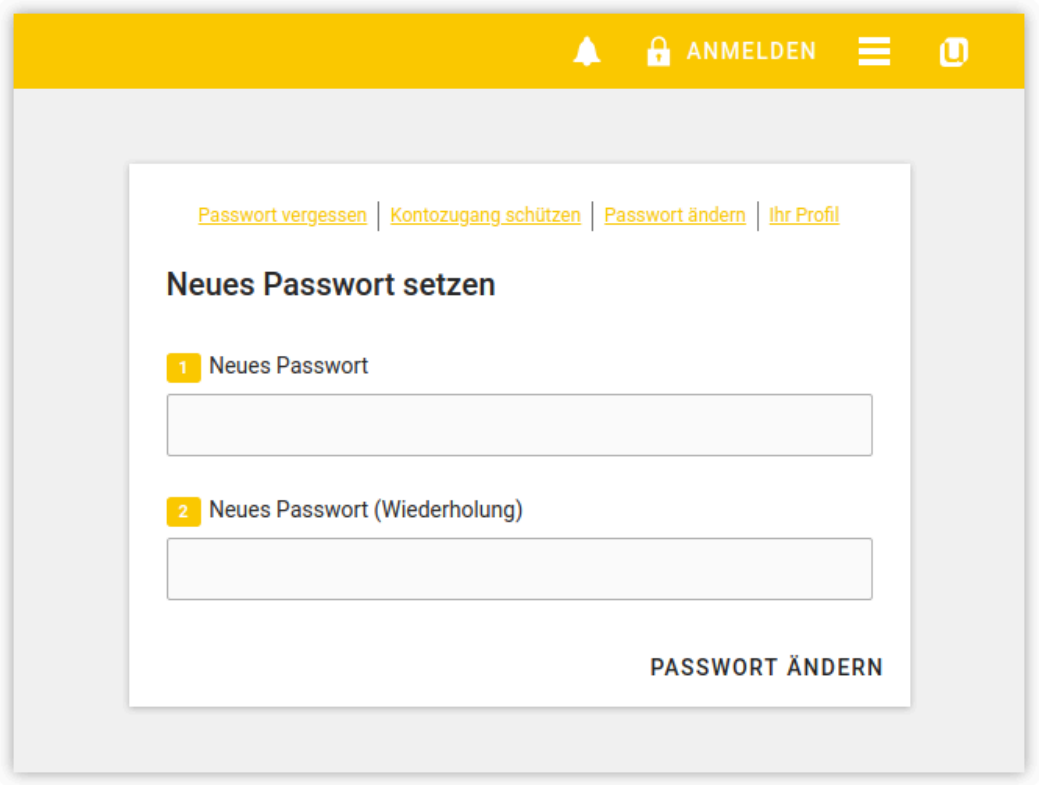
Über **Weiter** in Abbildung 6.1 gelangt man auf die zweite Seite Abbildung 6.2, auf der dann das initiale Passwort gesetzt werden kann.

Abbildung 6.2. Passwortvergabe für einen neuen Benutzer



Alternativ besteht bei installierter *Self Service-App* die Möglichkeit, das Setzen des Passworts dem Benutzer selbst zu überlassen. Dafür ist dann eine externe E-Mail-Adresse anzugeben, die als Kontakt-E-Mail-Adresse registriert wird. An diese erhält dann der Benutzer eine E-Mail mit einer Web-Adresse und einem *Token*, mit dem er sein Passwort setzen und seinen Zugang freischalten kann. Siehe dazu auch Abschnitt 6.5.2.

Abbildung 6.3. Initiales Benutzerpasswort



In der Grundeinstellung wird zum Anlegen eines Benutzers ein vereinfachter Assistent angezeigt, der nur die wichtigsten Einstellungen abfragt. Durch einen Klick auf **Erweitert** in Abbildung 6.1 werden alle Attribute angezeigt. Der vereinfachte Assistent kann deaktiviert werden, indem die Univention Configuration Registry-Variable `directory/manager/web/modules/users/user/wizard/disabled` auf `true` gesetzt wird.

Abbildung 6.4. Erweiterte Benutzeransicht

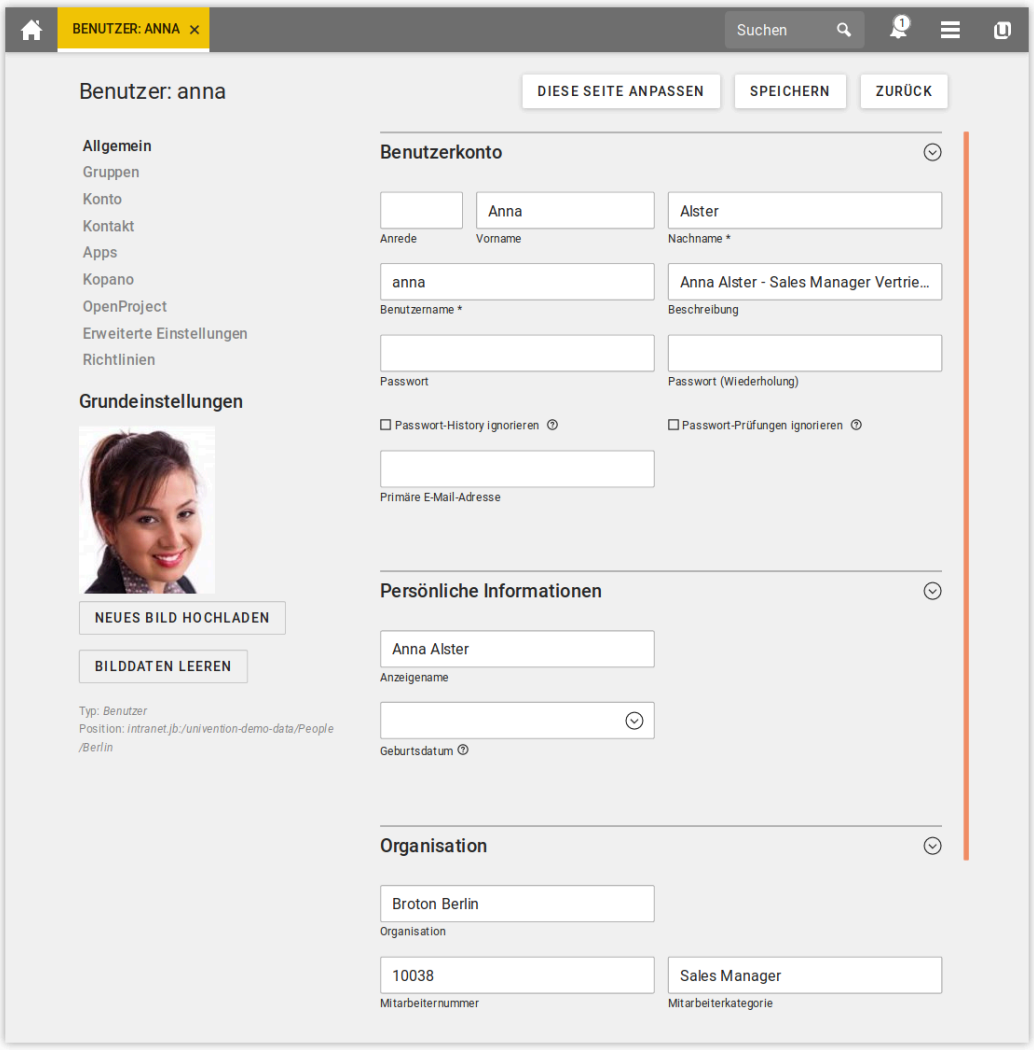


Tabelle 6.1. Karteikarte 'Allgemein'

Attribut	Beschreibung
Benutzername	Mit diesem Namen meldet sich der Benutzer am System an. Der Name muss mit einem Buchstaben beginnen und darf anschließend Buchstaben von a bis z, die Ziffern 0 bis 9, Punkte, Bindestriche oder Unterstriche enthalten. Benutzernamen dürfen keine Leerzeichen enthalten. Um die Kompatibilität mit Nicht-UCS-Systemen zu gewährleisten, wird das Anlegen von Benutzern, die sich lediglich in der Groß- und Kleinschreibung unterscheiden, verhindert. Wenn beispielsweise der Benutzername `meier` bereits existiert, wird der Benutzername `Meier` nicht mehr zugelassen. In der Grundeinstellung kann kein Benutzer mit dem Namen einer existierenden Gruppe angelegt werden. Wird die Univention Configuration Registry-Variable `directory/manager/user_group/uniqueness` auf `false` gesetzt, wird diese Prüfung aufgehoben.

Attribut	Beschreibung
Beschreibung	Hier kann eine beliebige Beschreibung für den Benutzer eingetragen werden.
Passwort	Hier wird das Passwort des Benutzers eingegeben.
Passwort (Wiederholung)	Um Tippfehler auszuschließen wird das Passwort des Benutzers erneut eingegeben.
Passwort-History ignorieren	Durch die Aktivierung dieses Auswahlkästchens wird die Passwort-History für diesen Benutzer und für diese Passwortänderung außer Kraft gesetzt. Dadurch kann dem Benutzer mit dieser Änderung ein bereits verwendetes Passwort zugewiesen werden. Weitere Hinweise zur Passwortverwaltung finden sich in Abschnitt 6.3.
Passwort-Prüfungen ignorieren	Wird diese Option aktiviert, wird die Prüfung der Passwortlänge und -qualität für diesen Benutzer und für diese Passwortänderung außer Kraft gesetzt. Dadurch kann dem Benutzer mit dieser Änderung z.B. ein kürzeres Passwort zugewiesen werden, als in der Mindestlänge vorgegeben ist. Weitere Hinweise zur Passwortverwaltung finden sich in Abschnitt 6.3.
Primäre E-Mail-Adresse	Hier wird die E-Mail-Adresse des Benutzers eingetragen, siehe Abschnitt 14.3.2.
Anrede	Die Anrede des Benutzers kann hier eingegeben werden.
Vorname	Hier wird der Vorname des Benutzers eingetragen.
Nachname	Hier wird der Nachname des Benutzers angegeben.
Anzeigename	Der Anzeigename wird automatisch aus Vor- und Nachname gebildet. In der Regel muss er nicht angepasst werden. Der Anzeigename wird u.a. in der Synchronisation mit Active Directory und Samba 4 verwendet.
Organisation	Die Organisation/das Unternehmen, dem der Benutzer angehört, wird in diesem Feld eingetragen.
Geburtsdatum	In diesem Feld kann das Geburtsdatum des Benutzers gespeichert werden.
Bild des Benutzers (JPEG-Format)	Über diese Maske kann ein Bild des Benutzers im JPEG-Format im LDAP hinterlegt werden. Standardmäßig ist die Dateigröße auf 512 Kilobyte limitiert.
Mitarbeiternummer	Die Mitarbeiter- oder Personalnummer kann in dieses Feld eingetragen werden.
Mitarbeiterkategorie	Hier kann die Kategorie des Mitarbeiters festgelegt werden.
Vorgesetzter	Der Vorgesetzte des Benutzers kann hier ausgewählt werden.

Tabelle 6.2. Karteikarte 'Gruppen'

Attribut	Beschreibung
Primäre Gruppe	In dieser Auswahlliste kann die primäre Gruppe für den Benutzer festgelegt werden. Zur Auswahl stehen alle in der Domäne eingetragenen Gruppen. Standardmäßig ist die Gruppe `Domain Users` als Vorgabe eingestellt.
Gruppen	Hier können weitere Gruppenzugehörigkeiten des Benutzers neben der primären Gruppe eingestellt werden.

Tabelle 6.3. Karteikarte 'Konto'

Attribut	Beschreibung
Konto ist deaktiviert	Mir dem Auswahlkästchen **Konto ist deaktiviert** kann das Benutzerkonto deaktiviert werden. Wenn es aktiviert ist, kann sich der Benutzer nicht am System anmelden. Das betrifft alle Methoden für die Authentifikation. Ein typischer Anwendungsfall ist ein Benutzer, der das Unternehmen verlassen hat. Eine Kontodeaktivierung kann in einer heterogenen Umgebung ggf. auch durch externe Tools ausgelöst werden.
Konto-Ablaufdatum	In diesem Eingabefeld wird ein Datum vorgegeben, an dem das Konto automatisch gesperrt wird. Dies ist sinnvoll für zeitlich befristete Benutzerkonten, z.B. für Praktikanten. Wenn das Datum entfernt oder ein anderes, zukünftiges Datum eingetragen wird, kann sich der Benutzer wieder anmelden.
Passwort bei der nächsten Anmeldung ändern	Wenn dieses Auswahlkästchen aktiviert ist, muss der Benutzer bei der nächsten Anmeldung an der Domäne sein Passwort ändern.
Passwort-Ablaufdatum	Wenn das Passwort zu einem bestimmten Datum abläuft, wird dieses Datum in diesem Eingabefeld angezeigt. Das Eingabefeld ist nicht direkt änderbar, siehe Abschnitt 6.3. Ist ein Passwort-Ablaufintervall definiert, wird das Passwort-Ablaufdatum bei Kennwortänderungen automatisch angepasst. Wird kein **Passwort-Ablaufdatum** gesetzt, werden evtl. bestehende frühere Ablaufdaten entfernt.
Aussperrung zurücksetzen	Wenn das Benutzerkonto aus Sicherheitsgründen automatisch gesperrt worden ist, meist weil ein Benutzer sein Passwort zu oft fehlerhaft eingegeben hat, kann dieses Auswahlkästchen dazu verwendet werden, um das Konto manuell schon vor Ablauf der Sperrzeit zu entsperren. Eine temporäre Aussperrung kann auftreten, wenn ein Administrator eine entsprechende domänenweite Einstellung definiert wurde. Es gibt drei unterschiedliche Mechanismen, die eine Aussperrung auslösen können, falls die entsprechend konfiguriert wurden: ◦ Fehlgeschlagene Authentifikation per PAM an einem UCS-Server (siehe Abschnitt 6.6). Fehlgeschlagene Authentifikation per LDAP (falls das Overlay-Modul `ppolicy` aktiviert und konfiguriert wurde). Fehlgeschlagene Authentifikation per Samba/AD (falls die Samba domain *passwordsettings* konfiguriert wurden).
Aussperrung endet	Wenn das Benutzerkonto aus Sicherheitsgründen automatisch gesperrt worden ist, meist weil ein Benutzer sein Passwort zu oft fehlerhaft eingegeben hat, zeigt dieses Feld den Zeitpunkt an, ab dem das Konto regulär automatisch entsperrt wird.
Aktiverungsdatum	Wenn ein Benutzerkonto erst an einem bestimmten, zukünftigen Datum aktiviert werden soll Dann kann man hier das Datum einstellen. Ein Cron-Job prüft periodisch, ob Benutzerkonten aktiviert werden müssen. Per Voreinstellung geschieht das alle 15 Minuten. Wird hier ein Datum eingestellt, das in der Zukunft liegt, dann wird beim Speichern automatisch auch das Konto als deaktiviert markiert.

Attribut	Beschreibung
Laufwerk für das Windows-Heimatverzeichnis	Wenn das Windows-Heimatverzeichnis bei diesem Benutzer auf einem anderen Windows-Laufwerk erscheinen soll, als in der Samba-Konfiguration vorgegeben, so kann hier ein Laufwerksbuchstabe eingetragen werden, z.B. `M:`.
Windows-Heimatverzeichnis	Hier wird der Pfad zu dem Verzeichnis angegeben, das als Windows-Heimatverzeichnis für den Benutzer dienen soll, z.B. `\\ucs-file-server\meier`.
Anmeldeskript	Hier wird das benutzerspezifische Anmeldeskript relativ zur Netlogon-Freigabe eingetragen, z.B. `user.bat`.
Profilverzeichnis	Das Profilverzeichnis für den Benutzer kann hier angegeben werden, e.g. `\\ucs-file-server\user\profile`.
Relative ID	Die relative ID (RID) ist der lokale Teil der SID-Domänenkennung. Wenn ein Benutzer eine bestimmte RID erhalten soll, so kann diese hier eingetragen werden. Wenn keine RID eingetragen wird, so wird automatisch die nächste freie RID verwendet. Die RID kann nachträglich nicht geändert werden, es sind ganze Zahlen ab 1000 zulässig. RIDs unter 1000 sind Standard-Gruppen und anderen speziellen Objekten vorbehalten.
Samba-Privilegien	Mit dieser Auswahlmaske können einem Benutzer ausgewählte Windows-Systemrechte zugewiesen werden, etwa die Berechtigung ein System in die Domäne zu joinen.
Erlaubte Zeiten für Windows-Anmeldungen	In diesem Eingabefeld werden Zeitspannen festgelegt, zu denen sich dieser Benutzer an Windows-Rechnern anmelden kann. Wird keine Einstellung in diesem Feld vorgenommen, so kann sich der Benutzer zu jeder Tageszeit anmelden.
Anmeldung nur an diesen Microsoft Windows-Rechnern zulassen	Diese Einstellung gibt an, an welchen Rechnern sich der Benutzer anmelden darf. Werden keine Einstellungen vorgenommen, ist der Benutzer berechtigt, sich an jedem Rechner anzumelden.
UNIX-Heimatverzeichnis	Der Verzeichnispfad zum Heimatverzeichnis des Benutzers.
Login-Shell	In diesem Feld wird die Login-Shell des Benutzers eingetragen. Dieses Programm wird bei der textbasierten Anmeldung des Benutzers gestartet. Standardmäßig wird hier `/bin/bash` eingetragen.
Benutzer-ID	Wenn der Benutzer eine bestimmte Benutzer-ID erhalten soll, so kann die Benutzer-ID in dieses Feld eingetragen werden. Wird kein Wert vorgegeben, wird automatisch eine freie Benutzer-ID zugewiesen. Die Benutzer-ID kann nur beim Hinzufügen des Benutzers angegeben werden, beim späteren Bearbeiten des Benutzers kann die Benutzer-ID nicht geändert werden und wird ausgegraut dargestellt.
Gruppen-ID der primären Gruppe	Hier wird die Gruppen-ID der primären Gruppe des Benutzers angezeigt. Die primäre Gruppe kann im Reiter **Allgemein** geändert werden.
Heimatverzeichnisfreigabe	Wird hier eine Freigabe ausgewählt, wird das Heimatverzeichnis auf dem angegebenen Server gespeichert. Erfolgt keine Auswahl, werden die Benutzerdaten auf dem jeweiligen Anmeldesystem gespeichert.
Pfad der Heimatverzeichnisfreigabe	Hier wird der Pfad zum Heimatverzeichnis relativ zur **Heimatverzeichnisfreigabe** angegeben. Beim Neuanlegen eines Benutzers ist der Benutzername als Vorgabewert bereits eingetragen.

Tabelle 6.4. Karteikarte 'Kontakt'

Attribut	Beschreibung
E-Mail-Adresse(n)	Hier können weitere E-Mail-Adressen hinterlegt werden. Diese werden nicht vom Mailserver ausgewertet. Die Werte werden im LDAP-Attribut *mail* gespeichert. Die meisten Adressbuch-Applikationen suchen im LDAP nach diesem Attribut.
Telefonnummer(n)	Dieses Feld beinhaltet die geschäftlichen Telefonnummern des Benutzers.
Abteilungsnummer	Hier kann die Abteilungsnummer des Mitarbeiters angegeben werden.
Raumnummer	Die Raumnummer des Benutzers.
Straße	Die Straße und die Hausnummer der Geschäftsadresse des Benutzers kann hier eingetragen werden.
Postleitzahl	Dieses Feld beinhaltet die Postleitzahl der Geschäftsadresse des Benutzers.
Stadt	Dieses Feld beinhaltet die Stadt der Geschäftsadresse des Benutzers.
Telefonnummer(n) Mobil	Hier werden die privaten Mobilfunknummern des Benutzers eingetragen.
Telefonnummer(n) Festnetz	Die privaten Festnetznummern können hier angegeben werden.
Rufnummer(n) Pager	Pager-Rufnummern werden in diesem Feld angegeben.
Private Adresse	Eine oder mehrere private Postadressen des Benutzers können in diesem Feld angegeben werden.

Tabelle 6.5. Karteikarte 'Mail'

Diese Karteikarte wird in den erweiterten Einstellungen angezeigt. Die Einstellungen sind in Abschnitt 14.3.2 beschrieben.

Tabelle 6.6. Karteikarte '(Optionen)'

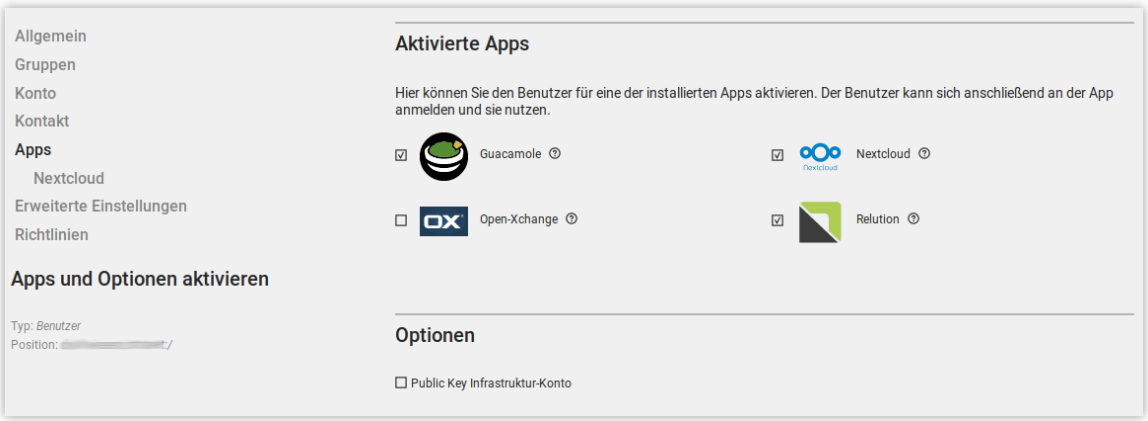
Attribut	Beschreibung
Public Key Infrastruktur-Konto	Wenn dieses Auswahlkästchen nicht markiert ist, erhält der Benutzer die Objektklasse `pkiUser` nicht.

6.2. Benutzeraktivierung für Apps

Feedback

Viele Apps aus dem App Center sind mit dem zentralen Identity Management in UCS verknüpft. Dadurch können Systemadministratoren die Benutzer für Apps aktivieren. In manchen Fällen können noch weitere App spezifische Einstellungen für den Benutzer vorgenommen werden. Das ist abhängig von der App und wie diese das Identity Management nutzt.

Abbildung 6.5. Benutzeraktivierung für installierte Apps



Sobald eine App in der UCS-Umgebung installiert ist, die die Benutzeraktivierung verwendet, erscheint sie mit Logo im Reiter **Apps** des Benutzers im UMC Modul *Benutzer*. Mit einem Haken in der Checkbox wird der Benutzer für die App aktiviert. Wenn noch weitere Einstellungen für die Berechtigung gemacht werden können, erscheint ein zusätzlicher Reiter mit dem Namen der App, um diese Parameter zu setzen. Die App Aktivierung und die Parameter werden am Benutzerobjekt im LDAP-Verzeichnisdienst von UCS gespeichert.

Um einem Benutzer die Berechtigung zur Nutzung einer App wieder zu entziehen, genügt es, den Haken aus Checkbox zu entfernen.

Wenn die App deinstalliert wird, wird die Checkbox der Benutzeraktivierung für die App vom Reiter **Apps** des Benutzers im UMC Modul entfernt.

6.3. Management der Benutzerpasswörter

Feedback

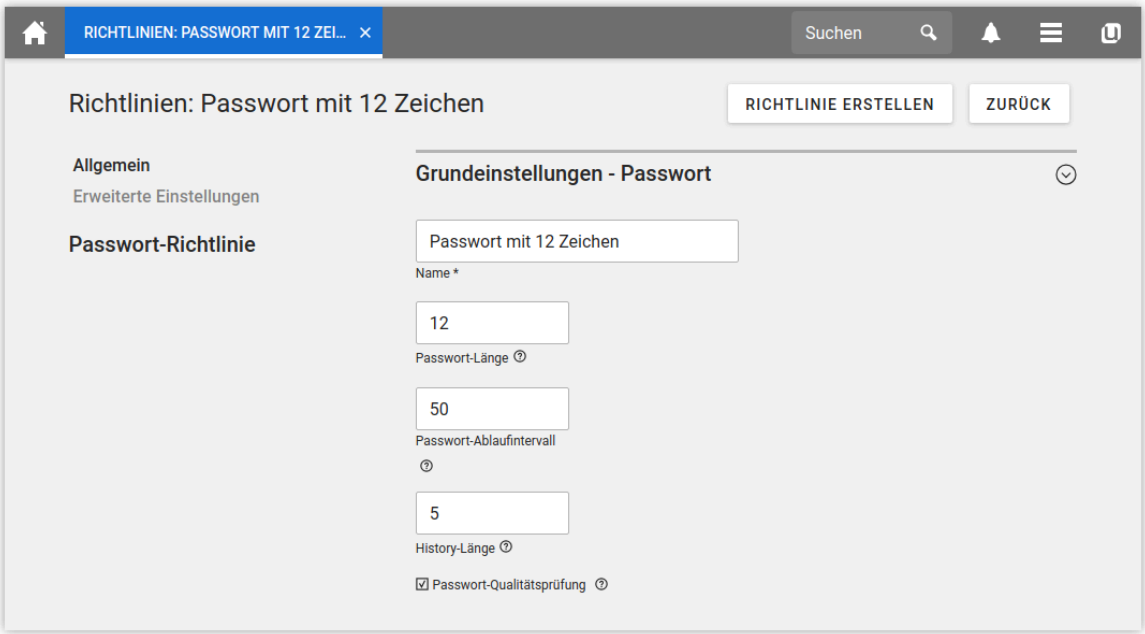
Schwer zu erratende Passwörter und regelmäßige Passwortwechsel sind ein wichtiger Baustein der Systemsicherheit einer UCS-Domäne. Folgende Eigenschaften lassen sich für Benutzer über eine *Passwort*-Richtlinie konfigurieren. Wird Samba eingesetzt, greifen für Anmeldungen an Windows-Clients die Einstellungen des Samba-Domänenobjekts (siehe Abschnitt 6.4). Die Einstellungen des Samba-Domänenobjekts und der Richtlinie sollten identisch gesetzt werden, sonst greifen für Anmeldungen an Windows- und UCS-Systemen unterschiedliche Passwortanforderungen.

Für jeden im Managementsystem gespeicherten Benutzer wird das Passwort in verschiedenen Attributen gespeichert:

- Das Attribut *krb5Key* speichert das Kerberos-Passwort
- Das Attribut *userPassword* speichert das Unix-Passwort (das in anderen Linux-Distributionen in `/etc/shadow` gespeichert wird
- Das Attribut *sambaNTPassword* enthält den von Samba verwendeten NT-Passwort-Hash

Passwortänderungen werden immer über Kerberos initiiert, entweder über die UCS-PAM-Konfiguration oder über Samba.

Abbildung 6.6. Konfiguration einer Passwort-Richtlinie



- Die *Passwort-Historie* speichert die letzten Passwortänderungen in Form von Hashes. Diese Passwörter können dann vom Benutzer bei einer Änderung nicht als neues Kennwort verwendet werden. Mit einer Passwort-Historie von z.B. fünf müssten fünf neue Passwörter verwendet werden, bis ein Kennwort erneut verwendet werden kann. Wenn keine Speicherung der Passwort-Historie erfolgen soll, muss der Wert auf 0 gesetzt werden.

  Die Passwörter werden nicht rückwirkend gespeichert. Wenn beispielsweise ursprünglich zehn Passwörter gespeichert wurden und der Wert auf drei herabgesetzt wird, werden die älteren sieben Passwörter bei der nächsten Passwort-Änderung aus der Historie entfernt. Wird danach die Historien-Länge wieder erhöht, müssen erst wieder Passwörter 'angesammelt' werden.

- Die *Passwort-Länge* ist die Anzahl an Zeichen, die ein Nutzer-Passwort mindestens enthalten muss. Wird nichts eintragen, beträgt die Mindestlänge acht Zeichen. Der Vorgabewert von acht Zeichen für die Passwort-Länge ist fest vorgegeben. Er gilt deswegen immer, wenn keine Richtlinie gesetzt ist und das Auswahlkästchen **Passwort-Länge ignorieren** nicht markiert ist, also auch, wenn die Passwort-Richtlinie *default-settings* gelöscht wurde. Wenn keine Prüfung der Passwortlänge erfolgen soll, muss der Wert auf 0 gesetzt werden. Pro Server kann über die Univention Configuration Registry-Variable `password/quality/length/min` ein Defaultwert konfiguriert werden, der auf Benutzerkonten angewendet wird, denen keine *UDM* Passwort-Richtlinie zugewiesen ist. Die Beschreibung der Univention Configuration Registry-Variable enthält weitere Details.

- Ein *Passwort-Ablaufintervall* forciert regelmäßige Passwortänderungen. Bei der Anmeldung an Univention Management Console, Kerberos, Windows-Clients und an UCS-Systemen wird nach Ablauf des Intervalls in Tagen ein Passwortwechsel erzwungen. Die verbleibende Gültigkeit des Kennworts wird in der Benutzerverwaltung unter **Passwort-Ablaufdatum** im Reiter **Konto** angezeigt. Wird das Eingabefeld leer belassen, wird kein Passwort-Ablaufintervall angewendet.

- Ist die Option *Passwort-Qualitätsprüfung* aktiviert, werden für Passwortänderungen in Samba, Univention Management Console und Kerberos zusätzliche Prüfungen vorgenommen, die auch eine Wörterbuchprüfung beinhalten.

  Die Konfiguration erfolgt über Univention Configuration Registry und sollte auf allen Anmeldeservern erfolgen. Folgende Prüfungen können erzwungen werden:

- Die Mindestanzahl von Zahlen in dem neuen Passwort (`password/quality/credit/digits`).
- Die Mindestanzahl von Grossbuchstaben in dem neuen Passwort (`password/quality/credit/upper`).
- Die Mindestanzahl von Kleinbuchstaben in dem neuen Passwort (`password/quality/credit/lower`).
- Die Mindestanzahl von Zeichen in dem neuen Passwort, die keine Buchstaben oder Ziffern sind (`password/quality/credit/other`).
- Einzelne Zeichen/Ziffern können ausgeschlossen werden (`password/quality/forbidden/chars`).
- Einzelne Zeichen/Ziffern können erzwungen werden (`password/quality/required/chars`).
- Standard-Microsoft-Passwortkomplexitätskriterien können angewendet werden (`password/quality/mspolicy`). Dies kann entweder zusätzlich zu den `python-cracklib` Checks geschehen (Wert `yes`) oder statt dessen (`sufficient`). Die Beschreibung der Univention Configuration Registry-Variable enthält weitere Details.

6.4. Passwort-Einstellungen für Windows-Clients bei Verwendung von Samba

Mit dem Samba-Domänenobjekt können die Passwortanforderungen bei der Anmeldung an Windows-Clients in einer Samba-Domäne festgelegt werden.

Das Samba-Domänenobjekt wird über das UMC-Modul *LDAP-Verzeichnis* verwaltet. Es befindet sich im Container `samba` unterhalb der LDAP-Basis und trägt den NetBIOS-Namen der Domäne.

Die Einstellungen des Samba-Domänenobjekts und der Richtlinie (siehe Abschnitt 6.3) sollten identisch gesetzt werden, sonst greifen für Anmeldungen für Anmeldungen an Windows- und UCS-Systemen unterschiedliche Passwortanforderungen.

Tabelle 6.7. Reiter 'Allgemein'

Attribut	Beschreibung
Passwort-Länge	Die Anzahl an Zeichen, die ein Nutzer-Passwort mindestens enthalten muss.
Passwort-History	Die letzten Passwortänderungen werden in Form von Hashes gespeichert. Diese Passwörter können dann vom Benutzer bei einer Änderung nicht als neues Kennwort verwendet werden. Mit einer Passwort-History von z.B. fünf müssten fünf neue Passwörter verwendet werden, bis ein Kennwort erneut verwendet werden kann.
Minimales Passwortalter	Der hier festgelegte Zeitraum muss min. seit der letzten Passwortänderungen vergangen sein, bis ein Benutzer sein Passwort das nächste Mal setzen kann.
Maximales Passwortalter	Nach Ablauf des hier hinterlegten Zeitraums muss das Passwort vom Benutzer bei der nächsten Anmeldung geändert werden. Bleibt der Wert leer, ist das Passwort unbegrenzt gültig.

6.5. Benutzer Selbstverwaltung

Feedback

6.5.1. Passwortwechsel über Univention Management Console

Feedback

In Univention Management Console kann jeder Benutzer sein Passwort über das Modul **Passwort ändern** neu setzen. Dieses wird auch bei Auswahl des Eintrages **Einstellungen -> Passwort ändern** im oberen, rechten Benutzermenü aufgerufen. Damit das Passwort geändert werden kann, muss zunächst das aktuelle angegeben werden. Die Änderung wird dann direkt über den PAM-Stack (siehe Abschnitt 8.4.4) durchgeführt und ist danach zentral für alle Dienste verfügbar.

6.5.2. Passwort-Verwaltung über *Self Service-App*

Feedback

Durch die Installation der *UCS-Komponenten* **Self Service Backend** auf dem UCS Master und **Self Service** in der Domäne über das **App Center** werden Benutzer dazu befähigt, ihr Passwort ohne die Interaktion mit einem Administrator zu verwalten.

Die *Self Service-App* registriert einen Web-Dienst in dem Portal, auf den über eine eigene Webseite zugegriffen werden kann: **Passwort ändern**. Sie erlaubt es Benutzern, unter Angabe ihres alten Passwortes ein neues Passwort zu setzen, oder aber ihr vergessenes Passwort zurückzusetzen. Für das Zurücksetzen des Passworts wird ein *Token* an eine vorher dafür registrierte Kontakt-E-Mail-Adresse gesendet, das dann auf der Webseite vom Benutzer einzugeben ist.

Die Funktionalität kann auf bestimmte Benutzer(gruppen) eingeschränkt werden; das geschieht über die vier Univention Configuration Registry-Variablen `umc/self-service/passwordreset/{blacklist,whitelist}/{users,groups}`. Dabei gilt, dass, falls ein Benutzer auf einer Blacklist und auf einer Whitelist steht, die Blacklist Vorrang hat. Für die Variablen gilt, dass Gruppen in Gruppen unterstützt werden. Der Default erlaubt die Nutzung für alle Domänenbenutzer außer den Administratoren.

Mit den folgenden Univention Configuration Registry-Variablen können einzelne Funktionen der Passwort-Verwaltung aktiviert bzw. deaktiviert werden.

`umc/self-service/passwordreset/frontend/enabled`

Aktiviert bzw. deaktiviert die "Passwort vergessen"-Seite des *Self Service* auf einzelnen Systemen.

`umc/self-service/passwordreset/backend/enabled`

Aktiviert bzw. deaktiviert die Backend-Funktionalität der "Passwort vergessen"-Seite. Diese Univention Configuration Registry muss auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry-Variable `self-service/backend-server` definiert ist, da Anfragen bezüglich dieser Variablen an das *Self Service Backend* weitergeleitet werden.

`umc/self-service/protect-account/frontend/enabled`

Aktiviert bzw. deaktiviert die "Kontozugang schützen"-Seite des *Self Service* auf einzelnen Systemen.

`umc/self-service/protect-account/backend/enabled`

Aktiviert bzw. deaktiviert die Backend-Funktionalität der "Kontozugang schützen"-Seite. Diese Univention Configuration Registry muss auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry-Variable `self-service/backend-server` definiert ist, da Anfragen bezüglich dieser Variablen an das *Self Service Backend* weitergeleitet werden.

`umc/self-service/passwordchange/frontend/enabled`

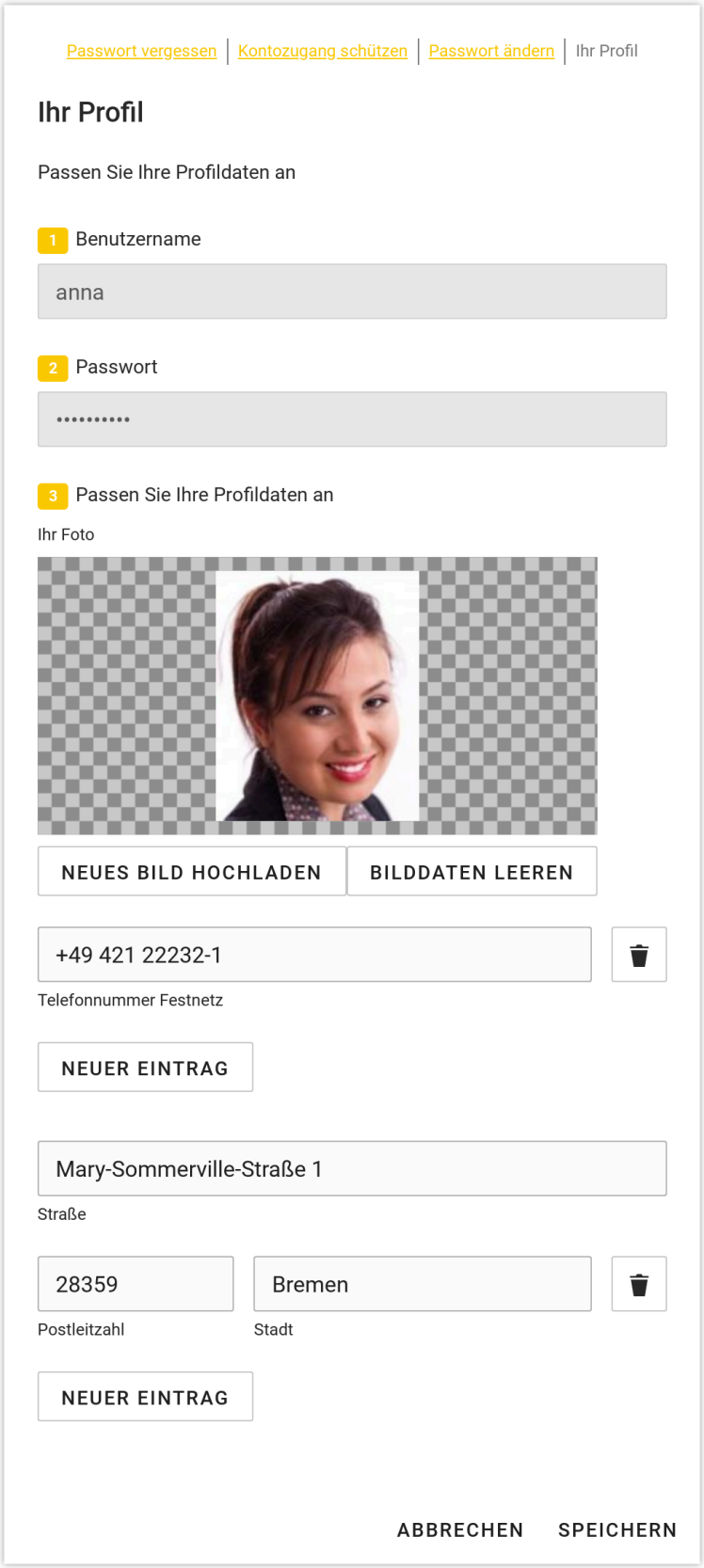
Aktiviert bzw. deaktiviert die "Passwort ändern"-Seite des *Self Service* auf einzelnen Systemen.

Das Design der *Self Service-App* kann durch die Datei `/usr/share/univention-self-service/www/css/custom.css` angepasst werden. Diese Datei wird während eines Updates nicht überschrieben.

6.5.3. Benutzerprofilselbstverwaltung

Am Benutzerkonto im LDAP-Verzeichnisdienst können weitere personenbezogene Daten gespeichert werden. Dies beinhaltet u.a. ein Bild, private Adressen und weitere Kontaktinformationen. Standardmäßig können diese nur von Administratoren aktualisiert werden. Alternativ können aber auch ausgewählte Felder für den Benutzer selber freigeschaltet werden. Der kann diese Daten über die *Self Service-App* selber pflegen.

Abbildung 6.7. Profilverwaltung



Dafür müssen folgende Univention Configuration Registry-Variablen konfiguriert werden:[1]

`self-service/ldap_attributes`

Über diese Variable werden die *LDAP* Attribute konfiguriert, die ein Benutzer selber an seinem Benutzerkonto modifizieren kann. Die Namen der Attribute sind durch Komma zu trennen. Diese Variable ist auf dem Domänencontroller Master (und Domänencontroller Backups) zu setzen.

`self-service/udm_attributes`

Über diese Variable werden die *UDM* Attribute konfiguriert, die ein Benutzer modifizieren kann. Die Namen der Attribute sind durch Komma zu trennen. Diese Variable ist auf allen beteiligten Server-Systemen zu setzen, auf denen die *Self Service-App* installiert ist (ebenso auf dem Domänencontroller Master).

`umc/self-service/profiledata/enabled`

Diese Variable muss auf allen beteiligten Server-Systemen auf `true` gesetzt werden, um den Mechanismus zu aktivieren.

`umc/self-service/allow-authenticated-use`

Diese Variable definiert, ob beim Öffnen und Modifizieren des eigenen Benutzerprofils die Angabe von Benutzername und Passwort notwendig ist, wenn man bereits am Univention Portal angemeldet ist. Ab UCS 4.4-7 wird diese Univention Configuration Registry-Variable bei Erstinstallationen des *Self Service* automatisch auf `true` gesetzt, was die Verwendung einer vorhandenen Portalsitzung aktiviert. Die Felder **Benutzername** und **Passwort** werden dann automatisch ausgefüllt bzw. nicht mehr angezeigt. Systeme, die auf UCS 4.4-7 aktualisiert werden, behalten die alte Verhaltensweise bei, indem automatisch der Wert auf `false` gesetzt wird. Es ist zu beachten, dass diese Variable auf allen beteiligen Systemen inkl. Domänencontroller Master auf den gleichen Wert gesetzt sein muss.

Die Funktionalität kann auf bestimmte Benutzer(gruppen) eingeschränkt werden; das geschieht über die vier Univention Configuration Registry-Variablen `umc/self-service/profiledata/{blacklist,whitelist}/{users,groups}`. Dabei gilt, dass, falls ein Benutzer auf einer Blacklist und auf einer Whitelist steht, die Blacklist Vorrang hat. Für die Variablen gilt, dass Gruppen in Gruppen unterstützt werden. Der Default erlaubt die Nutzung für alle Domänenbenutzer außer den Administratoren.

6.5.4. Selbstregistrierung

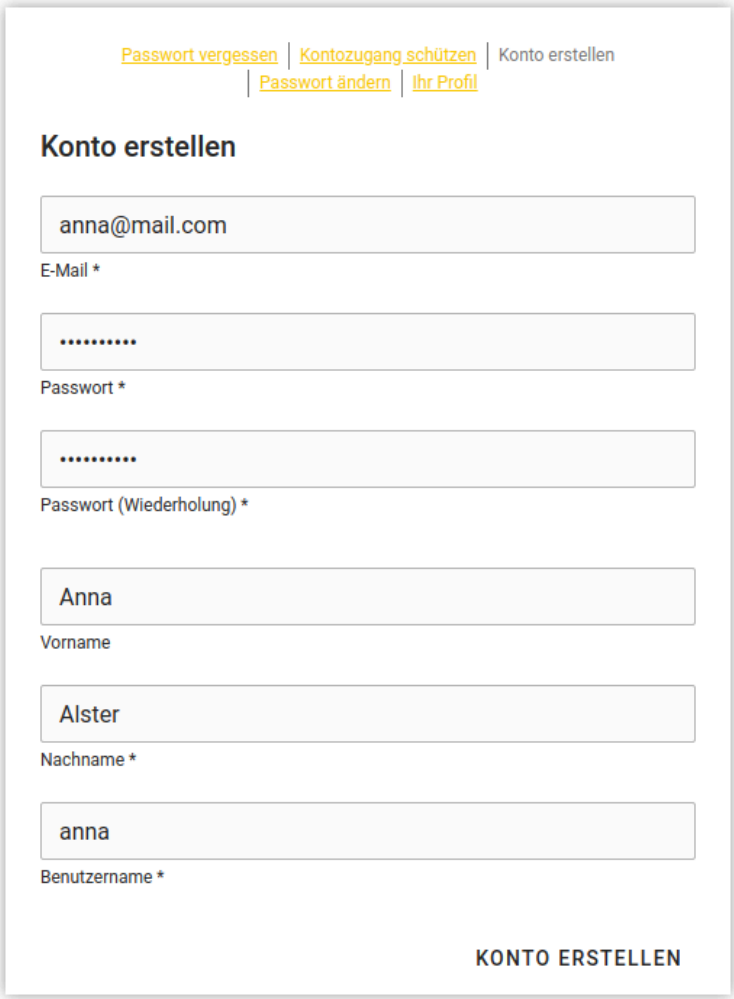
Feedback

Der *Self Service* ermöglicht es Benutzern, sich selbst zu registrieren, wodurch ein Benutzerkonto erstellt wird, das per E-Mail verifiziert werden muss. Bei Benutzerkonten, die über den *Self Service* erstellt werden, wird das *RegisteredThroughSelfService* Attribut des Benutzers auf TRUE und das *PasswordRecoveryEmailVerified* Attribut auf FALSE gesetzt. Nachdem der Benutzer sein Konto über die *Verifizierungs-E-Mail* verifiziert hat wird das *PasswordRecoveryEmailVerified* Attribut auf TRUE gesetzt.

[1] Beide *attributes* Variablen müssen zueinander passen. Die Namen der Attribute und deren Zuordnung kann man über folgenden Aufruf erhalten:
```
python -c 'from univention.admin.handlers.users.user import mapping;print("\n".join(map("{0[0]:>30s} {0[1][0]:<30s}".format, sorted(mapping._map.items()))))'
```

6.5.4.1. Kontoerstellung

Abbildung 6.8. Selbstregistrierung



Die "Konto erstellen" Seite kann mit der Univention Configuration Registry-Variable `umc/self-service/account-registration/frontend/enabled` auf einzelnen Systemen aktiviert bzw. deaktiviert werden.

Aspekte der "Konto erstellen" Seite und der Kontoerstellung selbst können mit den folgenden Univention Configuration Registry-Variablen konfiguriert werden. Diese Variablen müssen auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry-Variable `self-service/backend-server` definiert ist, da Anfragen bezüglich dieser Variablen an das *Self Service Backend* weitergeleitet werden.

`umc/self-service/account-registration/backend/enabled`

Mit dieser Variable kann die Selbstregistrierung deaktiviert/aktiviert werden.

`umc/self-service/account-registration/usertemplate`

Mit dieser Variable kann eine Benutzervorlage (Abschnitt 6.7) angegeben werden, die für die Erstellung von selbst registrierten Konten verwendet wird.

`umc/self-service/account-registration/usercontainer`

Mit dieser Variable kann ein Container angegeben werden, unter dem die selbst registrierten Benutzer angelegt werden.

`umc/self-service/account-registration/udm_attributes`

Diese Variable konfiguriert, welche *UDM-Attribute* eines Benutzerkontos auf der Seite "Konto erstellen" des *Self Service* angezeigt werden. Die Namen der *UDM-Attribute* müssen als kommasepariert Liste angegeben werden.

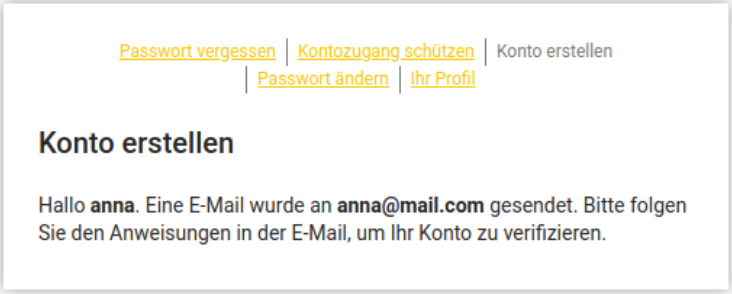
`umc/self-service/account-registration/udm_attributes/required`

Diese Variable konfiguriert, welche der über die Univention Configuration Registry-Variable `umc/self-service/account-registration/udm_attributes` definierten *UDM-Attribute* vom Benutzer angegeben werden müssen. Die Namen der *UDM-Attribute* müssen als kommasepariert Liste angegeben werden.

6.5.4.2. *Verifizierungs-E-Mail*

Nachdem ein Benutzer auf **Konto erstellen** geklickt hat, sieht er eine Nachricht, dass eine E-Mail für die Kontoverifizierung versendet wurde.

Abbildung 6.9. Senden der *Verifizierungs-E-Mail*



Aspekte der *Verifizierungs-E-Mail* und des *Verifizierungs-Tokens* können über die folgenden Univention Configuration Registry-Variablen konfiguriert werden. Diese Variablen müssen auf dem *Self Service Backend* gesetzt werden, der über die Univention Configuration Registry-Variable `self-service/backend-server` definiert ist, da Anfragen bezüglich dieser Variablen an den *Self Service Backend* weitergeleitet werden.

`umc/self-service/account-verification/email/webserver_address`

Definiert den *Host-Teil*, der in der *Verifizierungs-Link-URL* verwendet werden soll. Standardmäßig wird der FQDN des über die Univention Configuration Registry-Variable `self-service/backend-server` definierten *Self Service Backend* verwendet, da diese Univention Configuration Registry-Variable dort ausgewertet wird.

`umc/self-service/account-verification/email/sender_address`

Definiert die *Absenderadresse* der *Verifizierungs-E-Mail*. Die Voreinstellung ist `Account Verification Service <noreply@FQDN>`.

`umc/self-service/account-verification/email/server`

Servername oder IP-Adresse des zu verwendenden Mail-Servers.

`umc/self-service/account-verification/email/text_file`

Ein Pfad zu einer Textdatei, deren Inhalt für den Körper der *Verifizierungs-E-Mail* verwendet wird. Der Text kann die folgenden Zeichenfolgen enthalten, die entsprechend ersetzt werden: *{link}*, *{token}*, *{tokenlink}* und *{username}*. Als Standard wird die Datei `/usr/lib/python2.7/dist-packages/univention/management/console/modules/passwordreset/sending/verification_email_body.txt` verwendet.

`umc/self-service/account-verification/email/token_length`

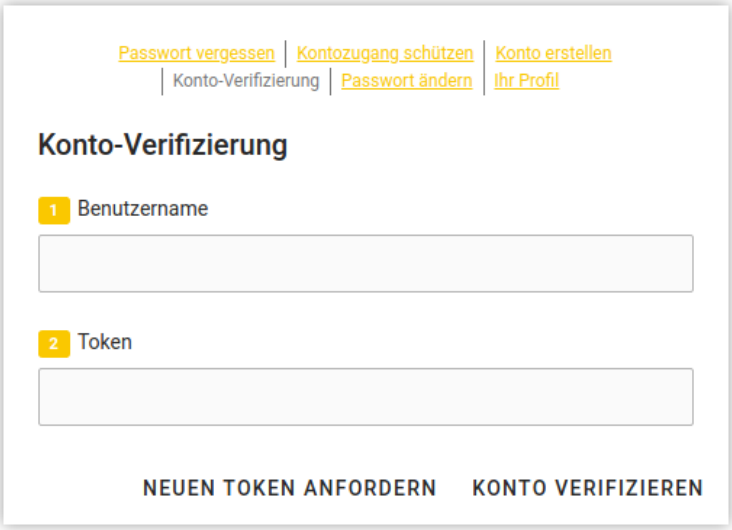
Definiert die Anzahl der Zeichen, die für den *Verifizierungs-Token* verwendet wird. Als Standard werden 64 Zeichen verwendet.

6.5.4.3. Kontoverifizierung

Feedback

Wenn der Benutzer dem *Verifizierungs-Link* aus der E-Mail folgt, gelangt er auf die Seite "Kontoverifizierung" des *Self Service*.

Abbildung 6.10. Kontoverifizierung

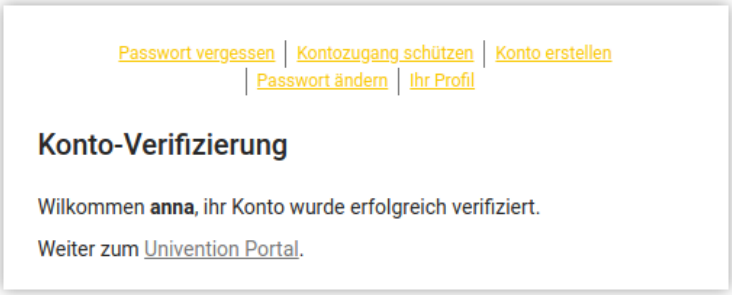


Die "Kontoverifizierung" Seite kann mit der Univention Configuration Registry-Variable `umc/self-service/account-verification/frontend/enabled` auf einzelnen Systemen aktiviert bzw. deaktiviert werden.

Die Kontoverifizierung und die Anforderung neuer *Verifizierungs-Token* kann mit der Univention Configuration Registry-Variable `umc/self-service/account-verification/backend/enabled` deaktiviert/aktiviert werden. Diese Variablen muss auf dem *Self Service Backend* gesetzt werden, das über die Univention Configuration Registry-Variable `self-service/backend-server` definiert ist.

Nach erfolgreicher Kontoverifizierung wird eine Nachricht angezeigt, was der Benutzer als nächstes tun kann. Diese Nachricht kann mit der Univention Configuration Registry-Variable `umc/self-service/account-verification/next-steps` konfiguriert werden. Eine lokalisierte Nachricht kann konfiguriert werden, indem eine Locale an die Variable angehängt wird. Z.B. `umc/self-service/account-verification/next-steps/de`.

Abbildung 6.11. Kontoverifizierung



Der SSO Login kann konfiguriert werden den Login für unverifizierte, selbst registrierte Konten zu verbieten. Dies wird über die Univention Configuration Registry-Variable `saml/idp/selfservice/check_email_verification` konfiguriert. Diese Einstellung muss auf dem Domänencontroller Master und allen Domänencontroller Backups vorgenommen werden. Für Konten, die durch einen Administrator angelegt wurden hat diese Einstellung keine Auswirkung.

Die Nachricht, welche auf der SSO Login Seite für unverifizierte, selbst registrierte Konten angezeigt wird, kann mit den Univention Configuration Registry-Variablen `saml/idp/selfservice/account-verification/error-title` und `saml/idp/selfservice/account-verification/error-descr` konfiguriert werden. Eine lokalisierte Nachricht kann konfiguriert werden, indem eine Locale an die Variable angehängt wird. Z.B. `saml/idp/selfservice/account-verification/error-title/de`.

6.5.5. *Selbst-Deregistrierung*

Der *Self Service* ermöglicht es Benutzern, die Löschung ihres eigenen Kontos zu beantragen. Diese Funktion kann mit der Univention Configuration Registry-Variable `umc/self-service/account-deregistration/enabled` aktiviert werden, wodurch der Button "Meinen Account löschen" auf der Seite "Ihr Profil" des *Self Service* angezeigt wird (Abschnitt 6.7).

Wenn ein Benutzer beantragt hat, sein Konto zu löschen, wird es nicht direkt gelöscht sondern deaktiviert. Zusätzlich wird das *DeregistredThroughSelfService* Attribut des Benutzers auf `TRUE` gesetzt und das *DeregistrationTimestamp* Attribut des Benutzers wird in der *GeneralizedTime*-LDAP-Syntax[2] auf die aktuelle Zeit gesetzt. Wenn der Benutzer eine *PasswordRecoveryEmail* angegeben hat, wird er eine E-Mail-Benachrichtigung erhalten, die mit den folgenden Univention Configuration Registry-Variablen konfiguriert werden kann.

`umc/self-service/account-deregistration/email/sender_address`

Definiert die E-Mail-Adresse des Absenders für Benachrichtigung. Die Voreinstellung ist `Password Reset Service <noreply@FQDN>`.

`umc/self-service/account-deregistration/email/server`

Servername oder IP-Adresse des zu verwendenden Mail-Servers.

`umc/self-service/account-deregistration/email/text_file`

Ein Pfad zu einer Textdatei, deren Inhalt für den Körper der E-Mail verwendet wird. Der Text kann die folgenden Zeichenfolgen enthalten, die entsprechend ersetzt werden: *`{username}`*. Als Standard wird die Datei `/usr/lib/python2.7/dist-packages/univention/management/conso-`

[2] https://ldapwiki.com/wiki/GeneralizedTime

`le/modules/passwordreset/sending/deregistration_notification_e-mail_body.txt` verwendet.

Der *Self Service* stellt unter `/usr/share/univention-self-service/delete_deregistered_accounts.py` ein Skript zur Verfügung, das zum Löschen aller users/user Objekte verwendet werden kann, bei denen *DeregistredThroughSelfService* auf `TRUE` gesetzt ist und deren *DeregistrationTimestamp* älter ist als eine angegebene Zeit. Der folgende Befehl würde Benutzer löschen, deren *DeregistrationTimestamp* älter als 5 Tage und 2 Stunden ist.

```
/usr/share/univention-self-service/delete_deregistered_accounts.py \
 --timedelta-days 5 --timedelta-hours 2
```

Für alle möglichen Argumente zum Skript siehe:

```
/usr/share/univention-self-service/delete_deregistered_accounts.py \
 --help
```

Das Skript kann regelmäßig ausgeführt werden, indem ein Cron-Job über Univention Configuration Registry erstellt wird.

```
ucr set cron/delete_deregistered_accounts/command=\
/usr/share/univention-self-service/delete_deregistered_accounts.py\
' --timedelta-days 30' \
 cron/delete_deregistered_accounts/time='00 06 * * *'  # daily at 06:00
```

Weitere Informationen über die Einstellung von Cron-Jobs über Univention Configuration Registry können in Abschnitt 8.4.8.3 gefunden werden.

Die Funktionalität kann auf bestimmte Benutzer(gruppen) eingeschränkt werden; das geschieht über die vier Univention Configuration Registry-Variablen `umc/self-service/account-deregistration/{blacklist,whitelist}/{users,groups}`. Dabei gilt, dass, falls ein Benutzer auf einer Blacklist und auf einer Whitelist steht, die Blacklist Vorrang hat. Für die Variablen gilt, dass Gruppen in Gruppen unterstützt werden. Der Default erlaubt die Nutzung für alle Domänenbenutzer außer den Administratoren.

6.6. Automatisches Sperren von Benutzern nach fehlgeschlagenen Anmeldungen

Feedback

Standardmäßig kann ein Benutzer sein Passwort beliebig oft falsch eingeben. Um Brute Force-Angriffe auf Passwörter zu erschweren, kann eine automatische Sperre von einem Benutzerkonto nach einer konfigurierbaren Anzahl von fehlerhaften Anmeldungen aktiviert werden.

UCS vereinheitlicht verschiedene Methoden zur Authentifizierung und Autorisierung von Benutzern. Abhängig von den installierten Softwarekomponenten kann es verschiedene Mechanismen geben, wie fehlgeschlagene Anmeldeversuche konfiguriert und gezählt werden.

Im folgenden werden die drei unterschiedlichen Methoden beschrieben.

6.6.1. Samba Active Directory Dienste

Feedback

In Samba Active Directory Umgebungen werden diverse Dienste von Samba bereitgestellt, wie bspw. Kerberos. Um Benutzer nach fehlgeschlagenen Anmeldungen zu sperren, kann das Tool `samba-tool` verwendet werden.

- `samba-tool domain passwordsettings show` zeigt die aktuell eingestellten Werte.
- `samba-tool domain passwordsettings set --account-lockout-threshold=5` legt fest, wie oft ein Benutzer versuchen kann, sich mit einem falschen Passwort anzumelden, bevor das Konto gesperrt wird.
- `samba-tool domain passwordsettings set --account-lockout-duration=3` legt die Anzahl der Minuten fest, die ein Konto gesperrt wird, nachdem zu viele falsche Passwörter eingegeben wurden.
- `samba-tool domain passwordsettings set --reset-account-lockout-after=5` legt die Anzahl der Minuten fest, nach der der Zähler zurückgesetzt wird. Wenn ein Konto automatisch nach der konfigurierten Aussperrungsdauer entsperrt wird, dann wird der Zähler nicht direkt mit zurückgesetzt, um das Konto noch eine gewisse Zeit unter strikter Beobachtung zu halten. In dem Zeitfenster nach dem Ende der Aussperrung und vor der endgültigen Rücksetzung des Zählers führt ein einziger erneuter Login-Versuch mit einem falschen Passwort direkt wieder zu einer Sperrung des Kontos.

Die manuelle Entsperrung eines Benutzers erfolgt in der Benutzerverwaltung auf dem Reiter **Konto** über die Aktivierung der Checkbox **Aussperrung zurücksetzen**.

6.6.2. PAM-Stack

Feedback

Das automatische Sperren von Benutzern nach fehlgeschlagenen Anmeldungen im PAM-Stack kann durch Setzen der Univention Configuration Registry-Variable `auth/faillog` auf `yes` aktiviert werden. Die Obergrenze an fehlerhaften Passworteingaben, bei der eine Kontosperre aktiviert wird, wird in der Univention Configuration Registry-Variable `auth/faillog/limit` konfiguriert. Unterhalb des Limits wird nach einer korrekten Passworteingabe der Zähler jedesmal wieder zurückgesetzt.

Die Sperre im PAM-Stack ist standardmäßig nur auf ein lokales System begrenzt. Wenn ein Benutzer also auf einem System zu oft sein Passwort falsch eingegeben hat, kann er sich auf einem anderen System weiterhin anmelden. Durch Setzen der Univention Configuration Registry-Variable `auth/faillog/lock_global` kann die Sperre auch global erfolgen und wird im LDAP registriert. Die globale Sperrung kann nur auf Domänencontroller Master/Backup-Systemen eingesetzt werden, da andere Systemrollen nicht über die nötigen Berechtigungen im LDAP-Verzeichnis verfügen. Auf allen Servern der genannten Systemrollen wird die Aussperrung aber automatisch auch lokal umgesetzt bzw. über das verwendete Listener-Modul auch wieder zurückgenommen, abhängig vom aktuellen Aussperrungs-Zustands des Kontos im LDAP-Verzeichnis.

Standardmäßig ist die Sperre über den PAM-Stack unbegrenzt gültig, sie kann aber auch nach Ablauf eines Intervalls automatisch wieder aufgehoben werden. Hierzu ist in der Univention Configuration Registry-Variable `auth/faillog/unlock_time` ein Zeitraum in Sekunden anzugeben. Wird der Wert auf 0 gesetzt, wird die Sperre direkt wiederaufgehoben.

Der `root`-Benutzer ist standardmäßig von der Passwort-Sperre ausgenommen, kann aber durch Setzen der Univention Configuration Registry-Variable `auth/faillog/root` auf `yes` ebenfalls aufgenommen werden.

Werden Konten nur lokal gesperrt, kann der Administrator ein Benutzerkonto durch Eingabe des Befehls `faillog -r -u USERNAME` entsperren. Erfolgt die Sperrung global im LDAP, kann der Benutzer in Univention Management Console im Reiter **Konto** in den Benutzer-Optionen **Aussperrung zurücksetzen** zurückgesetzt werden.

6.6.3. OpenLDAP

Feedback

Bei Domänencontrollern kann die automatische Kontosperre für den Fall eines wiederholten LDAP-Authentifizierungsfehlers aktiviert werden. Voraussetzung ist, dass das MDB LDAP-Backend verwendet wird. Dies

ist seit UCS 4 das Standard Backend, vorherige Systeme müssen auf das MDB LDAP-Backend migriert werden, siehe [ucs-performance-guide].

Die Aktivierung der automatischen Kontosperrung muss pro Domänencontroller aktiviert werden. Dazu müssen die Univention Configuration Registry-Variablen `ldap/ppolicy` und `ldap/ppolicy/enabled` auf `yes` gesetzt werden und der OpenLDAP Server muss neu gestartet werden:

```
ucr set ldap/ppolicy=yes ldap/ppolicy/enabled=yes
/etc/init.d/slapd restart
```

Die Standardrichtlinie ist so ausgelegt, dass fünf wiederholte LDAP-Authentifizierungsfehler innerhalb eines Überwachungsintervalls von fünf Minuten dazu führen, dass das authentifizierende Konto in UMC gesperrt wird. Ein gesperrtes Konto kann nur von einem Domain-Administrator über Univention Management Console freigeschaltet werden.

Die Anzahl der wiederholten LDAP-Authentifizierungsfehler kann in dem Konfigurationsobjekt mit der `objectClass` `pwdPolicy` angepasst werden:

```
univention-ldapsearch objectclass=pwdPolicy
```

Das Attribut `pwdMaxFailure` bestimmt die Anzahl der LDAP-Authentifizierungsfehler vor der Sperrung. Das Attribut `pwdMaxFailureCountInterval` bestimmt das Zeitintervall in Sekunden, das berücksichtigt wird. LDAP-Authentifizierungsfehler außerhalb dieses Intervalls werden bei der Zählung vernachlässigt.

Um den Account erst nach 10 Versuchen zu sperren kann der folgende Befehl verwendet werden:

```
ldapmodify -x -D cn=admin,$(ucr get ldap/base) -y /etc/ldap.secret
 <<__EOT__
dn: cn=default,cn=ppolicy,cn=univention,$(ucr get ldap/base)
changetype: modify
replace: pwdMaxFailure
pwdMaxFailure: 10
__EOT__
```

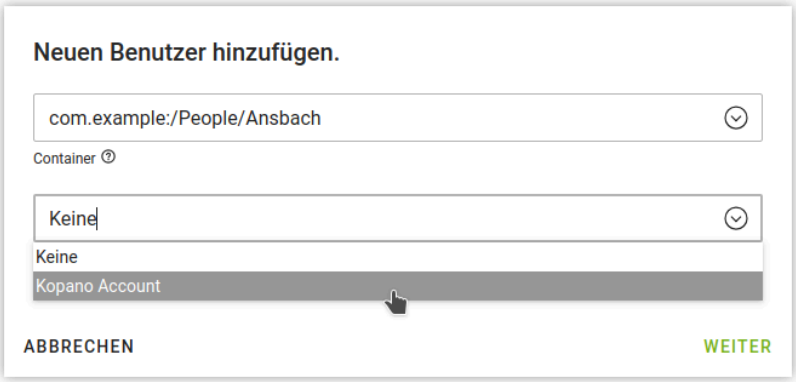
Die manuelle Entsperrung eines Benutzers erfolgt in der Benutzerverwaltung auf dem Reiter **Konto** über die Aktivierung der Checkbox **Aussperrung zurücksetzen**.

6.7. Benutzervorlagen

Feedback

Mit einer Benutzervorlage können beim Anlegen eines Benutzers Einstellungen vorgegeben werden. Ist mindestens eine Benutzervorlage definiert, kann sie beim Anlegen eines Benutzer ausgewählt werden.

Abbildung 6.12. Auswahl einer Benutzervorlage



Benutzervorlagen werden im UMC-Modul **LDAP-Verzeichnis** verwaltet. Dort muss in den Container `univention` und dort in den Untercontainer `templates` gewechselt werden. Hier kann über **Hinzufügen** mit dem Objekt-Typ **Einstellungen: Benutzervorlage** eine neue Benutzervorlage angelegt werden.

In einer Benutzervorlage kann entweder ein fester Wert vorgegeben werden (z.B. für die Anschrift) oder ein Attribut der Benutzerverwaltung referenziert werden. Attribute werden dabei in spitzen Klammern referenziert.

Eine Liste möglicher Attribute kann mit dem Befehl:

```
univention-directory-manager users/user
```

im Abschnitt *users/user variables* der Ausgabe ermittelt werden.

Wird beim Hinzufügen eines Benutzers eine Benutzervorlage verwendet, überschreibt diese alle in der Vorlage vorkommenden Felder mit dem in der Vorlage gesetzten Wert. Dabei gilt ein leeres Feld ebenfalls als auf "" gesetzt.

Es können auch nur Teilwerte von Attributen übernommen werden und Werte in Groß-/Kleinschreibung konvertiert werden:

So kann beispielsweise das UNIX-Heimatverzeichnis unter `/home/<title>.<lastname>` angelegt werden oder die primäre E-Mail-Adresse mit **`<firstname>.<lastname>@firma.com`** vordefiniert werden. Ersetzungen sind grundsätzlich für beliebige Werte möglich, eine syntaktische oder semantische Überprüfung erfolgt jedoch nicht. Wird beispielsweise beim Anlegen des Benutzers kein Vorname angegeben, würde die obige E-Mail-Adresse mit einem Punkt beginnen und wäre somit nach dem E-Mail-Standard ungültig. Ähnliche Fehlerquellen können auch im Umgang mit Dateipfaden etc. auftreten. Nicht auflösbare Attribute (etwa durch Tippfehler in der Vorlage) werden gelöscht.

Wird nicht der komplette Attributwert, sondern nur ein einzelnes Zeichen des Attributs benötigt, kann in der Benutzervorlage nach dem Attributnamen der Index des benötigten Zeichens in eckigen Klammern angegeben werden. Die Zählung der Zeichen des Attributs beginnt bei 0, so dass z.B. der Index 1 dem zweiten Zeichen des Attributwertes entspricht. Mit **`<firstname>[0].<lastname>@firma.com`** wird beispielsweise eine E-Mail-Adresse aus dem ersten Buchstaben des Vornamens sowie dem Nachnamen gebildet.

Eine Teilzeichenkette des Attributwerts kann über die Angabe eines Bereichs in eckigen Klammern erreicht werden. Dabei ist der Index des ersten benötigten Zeichens sowie der Index des letzten benötigten Zeichens plus 1 anzugeben. Die Angabe **`<firstname>[2:5]`** gibt z.B. das dritte bis fünfte Zeichen des Vornamens zurück.

Das Anhängen von `:lower` oder `:upper` an den Attributnamen führt dazu, dass der Attributwert in Klein- oder Großschreibung umgewandelt wird, z.B. **`<firstname:lower>`**. Wird ein Modifikator wie `:lower` an das Ende des Feldes angehängt, wird der komplette Wert umgewandelt, z.B. **`<lastname>@company.com<:lower>`**.

Durch die Option `:umlauts` werden Sonderzeichen wie è, ä oder ß in entsprechende ASCII-Zeichen umgewandelt.

Durch die Option `:alphanum` werden alle nicht alphanumerischen Zeichen, wie ` oder # entfernt. In der UCR Variable `directory/manager/templates/alphanum/whitelist` können Zeichen definiert werden, die von dieser Option ignoriert werden. Zu beachten ist, dass wenn diese Option auf das ganze Feld angewendet wird, auch manuell gesetzte Zeichen entfernt werden. Zum Beispiel das @-Zeichen in der E-Mail-Adresse. Daher sollte man diese Option nur auf einzelne Attribute anwenden oder die Whitelist anpassen.

Die Optionen `:strip` bzw. `:trim` entfernen alle Leerzeichen am Anfang und Ende der Zeichenkette.

Optionen können auch kombiniert werden, z.B: `:umlauts,upper`.

6.8. Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos

Feedback

Achtung

Bevor Sie diese Funktion verwenden, lesen Sie bitte diesen Support-Artikel über die Aktivierung des `lastbind` `Overlay-Moduls`[3].

Das optionale `lastbind` Overlay-Modul[4] für OpenLDAP ermöglicht die Aufzeichnung des Zeitstempels der letzten erfolgreichen LDAP-Anmeldung im *authTimestamp* Attribut und kann z.B. zur Erkennung nicht genutzter Konten verwendet werden.

Das `lastbind` Overlay-Modul kann aktiviert werden, indem die Univention Configuration Registry-Variable `ldap/overlay/lastbind` auf `yes` gesetzt und der OpenLDAP-Server neu gestartet wird. Wenn das Modul auf einem UCS-Server aktiviert ist, wird der Zeitstempel einer erfolgreichen LDAP-Anmeldung eines Kontos, in das *authTimestamp* Attribut jenes Kontos geschrieben. Die Univention Configuration Registry-Variable `ldap/overlay/lastbind/precision` kann verwendet werden, um die Zeit in Sekunden zu konfigurieren, die vergehen muss, bevor das *authTimestamp* Attribut aktualisiert wird. Dies verhindert eine große Anzahl von Schreiboperationen, die die Leistung beeinträchtigen können.

Das *authTimestamp* Attribut kann nur auf dem LDAP-Server abgefragt werden, auf dem das `lastbind` Overlay-Modul aktiviert ist. Es wird nicht auf andere LDAP-Server repliziert. Aus diesem Grund kann das Skript `/usr/share/univention-ldap/univention_lastbind.py` ausgeführt werden, um den jüngsten *authTimestamp* Wert von allen erreichbaren LDAP-Servern in der UCS-Domäne zu sammeln und in das erweiterte UDM Attribut *lastbind* eines Benutzers zu speichern. Das Skript kann aufgerufen werden, um das erweiterte Attribut *lastbind* eines oder aller Benutzer zu aktualisieren. Das erweiterte Attribut *lastbind* wird auf das LDAP-Attribut *univentionAuthTimestamp* abgebildet.

Eine Möglichkeit, das erweiterte Attribute *lastbind* aktuell zu halten, ist durch das Anlagen eines Cron-Jobs via UCR:

```
ucr set cron/update_lastbind_attribute/command='/usr/share/univention-
ldap/univention_lastbind.py --allusers' \
       cron/update_lastbind_attribute/time='00 06 * * *'  # Täglich um
 06:00 Uhr
```

Weitere Informationen über die Einstellung von Cron-Jobs über UCR können in Abschnitt 8.4.8.3 gefunden werden.

[3] https://help.univention.com/t/14404
[4] http://manpages.ubuntu.com/manpages/xenial/man5/slapo-lastbind.5.html

Kapitel 7. Gruppenverwaltung

Berechtigungen werden in UCS überwiegend auf Basis von *Gruppen* unterschieden. Gruppen werden im LDAP gespeichert und sind somit auf allen Systemen identisch. Gruppen können nicht nur Benutzerkonten enthalten, sondern optional auch Rechnerkonten aufnehmen.

Auf jedem System gibt es darüberhinaus auch noch lokale Benutzergruppen, die vor allem für den Zugriff auf Hardware verwendet werden. Diese werden nicht durch das UCS-Managementsystem verwaltet, sondern in der Datei `/etc/group` gespeichert.

Die Zuordnung von Benutzern zu Gruppen erfolgt auf zwei Wegen:

- In der Benutzerverwaltung kann einem Benutzer eine Auswahl von Gruppen zugewiesen werden (siehe Abschnitt 6.1)
- In der Gruppenverwaltung kann einer Gruppe eine Auswahl von Benutzern zugeordnet werden (siehe Abschnitt 7.1)

7.1. Verwaltung von Gruppen in Univention Management Console

Feedback

Gruppen werden im UMC-Modul *Gruppen* verwaltet (siehe auch Abschnitt 4.4).

Abbildung 7.1. Anlegen einer Gruppe in UMC

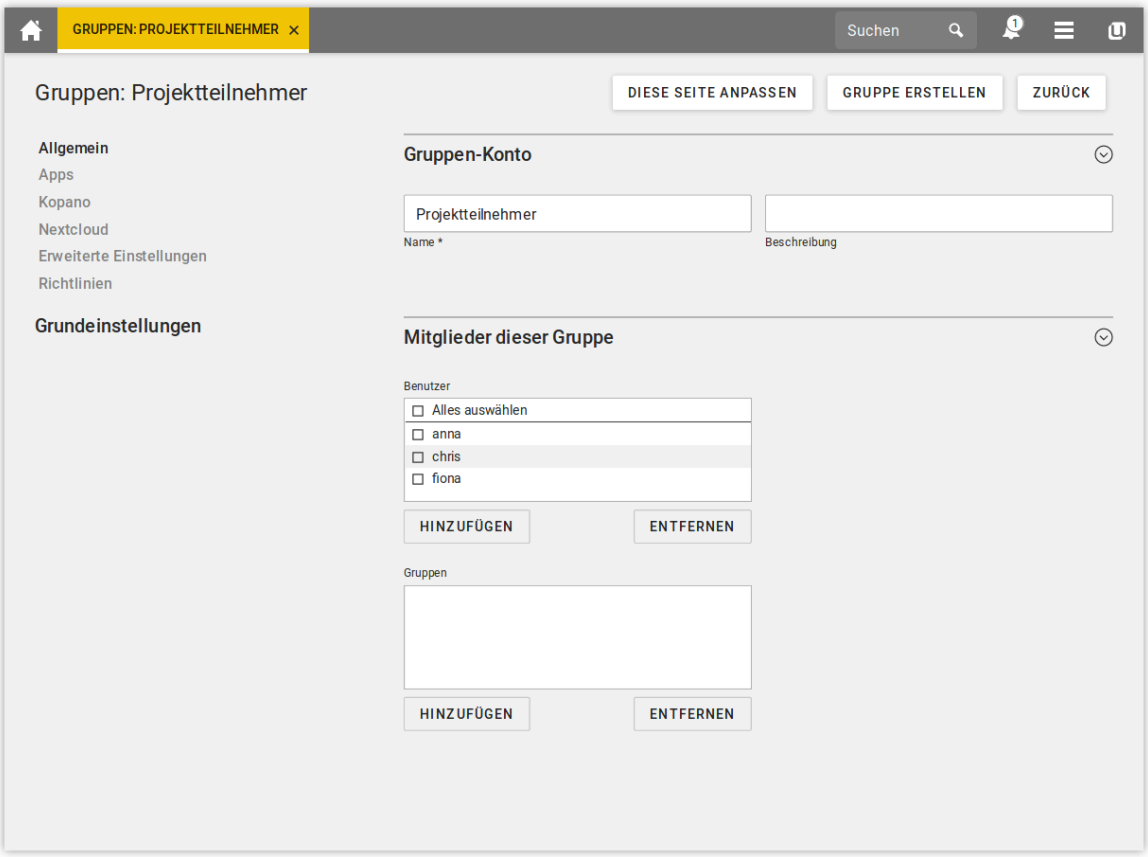


Tabelle 7.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name (*)	Der Name der Gruppe muss mit einem Buchstaben oder einer Ziffer beginnen und auch enden. Die übrigen Zeichen des Gruppennamens dürfen aus Buchstaben, Ziffern, Leerzeichen, Bindestrichen oder Punkten bestehen. In der Grundeinstellung kann keine Gruppe mit dem Namen eines existierenden Benutzers angelegt werden. Wird die Univention Configuration Registry-Variable `directory/manager/user_group/uniqueness` auf `false` gesetzt, wird diese Prüfung aufgehoben.
Beschreibung	Hier kann eine beliebige Beschreibung für die Gruppe eingetragen werden.
Benutzer	In diesem Eingabefeld können Benutzer als Mitglieder in diese Gruppe aufgenommen werden.
Gruppen	In diesem Eingabefeld können Gruppen als Mitglieder in diese Gruppe aufgenommen werden (Gruppen in Gruppen).

Tabelle 7.2. Reiter 'Erweiterte Einstellungen'

Attribut	Beschreibung
Mail	Diese Optionen definieren eine Mailgruppe und sind in Abschnitt 14.3.4 dokumentiert.
Enthaltene Rechner	In diesem Feld können Rechner als Mitglieder in diese Gruppe aufgenommen werden.
Mitglied von	Hier kann diese Gruppe einer oder mehreren anderen Gruppen als Mitglied hinzugefügt werden (Gruppen in Gruppen).
Gruppen ID	Wenn der Gruppe eine bestimmte Gruppen-ID zugewiesen werden soll, kann die Gruppen-ID in diesem Eingabefeld eingetragen werden. Ansonsten wird der Gruppe automatisch die nächste freie Gruppen-ID zugeordnet. Sie kann nachträglich nicht geändert werden und wird beim Bearbeiten der Gruppe ausgegraut angezeigt. Als Gruppen-ID können ganze Zahlen zwischen 1000 und 59999 sowie zwischen 65536 und 1000000 frei vergeben werden.
Windows -> Relative ID	Die Relative ID (RID) ist der lokale Teil der Security ID (SID) und wird in Windows- bzw. Samba-Domänen verwendet. Wenn der Gruppe eine bestimmte RID zugewiesen werden soll, kann sie in diesem Eingabefeld eingetragen werden. Ansonsten wird automatisch eine RID zugewiesen. Die RID kann nachträglich nicht geändert werden und wird beim Bearbeiten der Gruppe ausgegraut angezeigt. Die RIDs bis 1000 sind Standard-Gruppen und anderen speziellen Objekten vorbehalten. Bei Verwendung von Samba 4 wird die die RID durch Samba generiert und kann nicht vorgegeben werden.
Windows -> Gruppentyp	Dieser Gruppentyp wird ausgewertet, wenn der Benutzer sich an einer Domäne auf Basis von Samba/AD anmeldet. Man unterscheidet zwischen drei Windows-Gruppentypen: ◦ *Globale Gruppe:* Diese Gruppen sind domänenweit bekannt. In Univention Management Console sind neu erstellte Gruppen standardmäßig von diesem Typ. ◦ *Lokale Gruppe:* Lokale Gruppen sind nur auf Windows-Servern von Bedeutung. Wird auf einem Windows-Server eine lokale Gruppe erstellt, ist sie nur dem Server bekannt und ist nicht domänenweit verfügbar. UCS hingegen unterscheidet nicht zwischen lokalen und globalen Gruppen. Von einer AD-Domäne übernommene lokale Gruppen werden in UCS wie globale Gruppen verwaltet. ◦ *Bekannte Gruppe:* Unter diesem Gruppentyp werden von Samba- bzw. Windows-Servern vorkonfigurierte Gruppen zusammengefasst, die in der Regel über besondere Berechtigungen verfügen, z.B. `Power Users`.
Windows -> AD Gruppentyp	Dieser Gruppentyp wird nur ausgewertet, wenn der Benutzer sich an einer Domäne auf Basis von Samba 4 anmeldet (das Active Directory-Domänendienste bereitstellt). Diese Gruppen sind in Abschnitt 7.4 beschrieben.

Attribut	Beschreibung
Windows -> Samba-Privilegien	Mit dieser Eingabemaske wird einer Gruppe Windows-Systemrechte zugewiesen, z.B. die Berechtigung einen Windows-Client in die Domäne zu joinen. Diese Funktionalität ist in Abschnitt 6.1 dokumentiert.

Tabelle 7.3. Reiter 'Optionen'

Diese Karteikarte steht nur beim Hinzufügen von Gruppen zur Verfügung, nicht aber beim Bearbeiten von Gruppen. Sie ermöglicht es, bestimmte LDAP-Objektklassen für die Gruppe abzuwählen. Die Eingabefelder für Attribute dieser Klassen können dann nicht ausgefüllt werden.	
Attribut	**Beschreibung**
Samba-Gruppe	Dieses Auswahlkästchen gibt an, ob die Gruppe die Objektklasse `sambaGroupMapping` erhält.
POSIX-Gruppe	Dieses Auswahlkästchen gibt an, ob die Gruppe die Objektklasse `posixGroup` erhält.

7.2. Verschachtelung von Gruppen

Feedback

UCS unterstützt die Verschachtelung von Gruppen (auch bekannt als "Gruppen in Gruppen"). Dies vereinfacht die Verwaltung der Gruppen: Werden in einer Domäne beispielsweise zwei Standorte verwaltet, können zwei Gruppen `Techniker Standort A` und `Techniker Standort B` gebildet werden, denen jeweils die Benutzerkonten der Standort-Techniker zugewiesen werden. Um eine standortübergreifende Techniker-Gruppe zu bilden, reicht es dann aus, die Gruppen `Techniker Standort A` und `Techniker Standort B` als Mitglieder dieser Gruppe zu definieren.

Zyklische Abhängigkeiten von Gruppen in Gruppen werden erkannt und abgewiesen. Diese Prüfung kann durch die Univention Configuration Registry-Variable `directory/manager/web/modules/groups/group/checks/circular_dependency` deaktiviert werden. Auch bei direkten Gruppenänderungen ohne das UCS-Managementsystem müssen zyklische Mitgliedschaften vermieden werden.

Die Auflösung der verschachtelten Gruppenmitgliedschaften erfolgt während der Expandierung des Gruppencaches (siehe Abschnitt 7.3) und ist somit für Applikationen transparent.

7.3. Lokaler Gruppencache

Feedback

Aus dem LDAP aufgelöste Benutzer- und Rechnerinformationen werden durch den Name Server Cache Daemon zwischengespeichert, siehe Abschnitt 8.4.9.

Die Zwischenspeicherung der Gruppen erfolgt seit UCS 3.1 aus Performance- und Stabilitätsgründen nicht mehr über den NSCD, sondern durch das NSS-Modul ***libnss-extrausers***. Die Gruppeninformationen werden automatisch durch das Skript `/usr/lib/univention-pam/ldap-group-to-file.py` in die Datei `/var/lib/extrausers/group` exportiert und dort von dem NSS-Modul ausgelesen.

Der Export erfolgt in der Grundeinstellung alle 15 Minuten durch einen Cron-Job und wird zusätzlich gestartet wenn der Univention Directory Listener 15 Sekunden inaktiv gewesen ist. Der Intervall für die Cron-Aktualisierung wird über die Univention Configuration Registry-Variable `nss/group/cachefile/invalidate_interval` in Cron-Syntax (siehe Abschnitt 8.4.8.2) festgelegt Das Listener-Modul kann über die Univention Configuration Registry-Variable `nss/group/invalidate_cache_on_changes` aktiviert/deaktiviert werden (`true`/`false`).

Während des Generierens der Gruppencache-Datei kann das Skript prüfen, ob die Gruppenmitglieder weiterhin im LDAP-Verzeichnis vorhanden sind. Wird für die Verwaltung der Verzeichnisdaten nicht ausschließ-

lich Univention Management Console eingesetzt, kann diese zusätzliche Prüfung durch Setzen der Univention Configuration Registry-Variable `nss/group/cachefile/check_member` auf `true` aktiviert werden.

7.4. Synchronisation von Active Directory-Gruppen bei Verwendung von Samba 4

Wird Samba 4 eingesetzt, werden die Gruppenmitgliedschaften zwischen dem Samba 4-Verzeichnisdienst und dem OpenLDAP-Verzeichnisdienst durch den Univention S4-Connector synchronisiert, d.h. jede Gruppe auf UCS-Seite ist einer Gruppe im Active Directory assoziiert. Allgemeine Hinweise zum Univention S4 Connector finden sich in Abschnitt 9.2.2.4.

Einzige Ausnahme sind die *Pseudo-Gruppen* (manchmal auch als Systemgruppen bezeichnet). Diese werden nur intern von Active Directory/Samba 4 verwaltet, z.B. enthält die Gruppe `Authenticated Users` eine Liste aller aktuell an einem System angemeldeten Benutzer. Pseudo-Gruppen sind im UCS-Verzeichnisdienst vorhanden; sie werden aber nicht durch den Univention S4 Connector synchronisiert und müssen normalerweise nicht bearbeitet werden. Dies betrifft die folgenden Gruppen:

- `Anonymous Logon`, `Authenticated Users`, `Batch`, `Creator Group`
- `Creator Owner`, `Dialup`, `Digest Authentication`
- `Enterprise Domain Controllers`, `Everyone`, `IUSR`, `Interactive`
- `Local Service`, `NTLM Authentication`, `Network Service`, `Network`
- `Nobody`, `Null Authority`, `Other Organization`, `Owner Rights`
- `Proxy`, `Remote Interactive Logon`, `Restricted`, `SChannel Authentication`
- `Self`, `Service`, `System`, `Terminal Server User`, `This Organization`
- `World Authority`

Man unterscheidet in Samba 4/Active Directory zwischen den folgenden vier AD-Gruppentypen. Diese Gruppentypen können auf zwei Arten von Gruppen angewendet werden; *Sicherheitsgruppen* konfigurieren Berechtigungen (entsprechend den UCS-Gruppen), während *Verteilungsgruppen* für Mailverteiler genutzt werden:

- *Lokale Gruppen* existieren immer nur lokal auf einem Rechner. Eine lokale Gruppe, die in Samba 4 angelegt wurde, wird durch den Univention S4 Connector synchronisiert und erscheint daher auch in der UMC. Es besteht aber keine Notwendigkeit lokale Gruppen in der UMC anzulegen.
- *Globale Gruppen* sind der Standardtyp für neu angelegte Gruppen in der UMC. Eine globale Gruppe gilt für eine Domäne, es können aber keine Konten anderer Domänen aufgenommen werden. Besteht eine Vertrauensstellung zu einer Domäne, werden die Gruppen dort angezeigt und es können Berechtigungen zugewiesen werden. Die aktuelle Version von UCS unterstützt allerdings weder mehrfache Domänen/Forests, noch von UCS ausgehende Vertrauensstellungen.
- *Domänenlokale Gruppen* können auch Mitglieder anderer Domänen aufnehmen (sofern zu diesen eine Vertrauenstellung besteht oder sie Teil eines Forests ist). Domänenlokale Gruppen werden aber nur in der eigenen Domäne angezeigt. Die aktuelle Version von UCS unterstützt allerdings weder mehrfache Domänen/Forests, noch von UCS ausgehende Vertrauensstellungen.
- *Universelle Gruppen* können Mitglieder aus allen Domänen aufnehmen und diese Mitglieder werden auch in allen Domänen eines Forests angezeigt. Diese Gruppen werden in einem separaten Segment des Verzeichnisdienstes gespeichert, dem sogenannten Global Catalog. Domänen-Forests werden aktuell von Samba 4 nicht unterstützt.

7.5. Overlay-Modul zur Anzeige der Gruppeninformationen an Benutzerobjekten

Im UCS-Verzeichnisdienst werden Gruppenmitgliedschaften nur an den Gruppenobjekten und nicht am jeweiligen Benutzerobjekt gespeichert. Einige Applikationen erwarten jedoch die Gruppenmitgliedschaften an den Benutzerobjekten (z.B. im Attribut *memberOf*). Durch ein optionales Overlay-Modul im LDAP-Server können diese Attribute automatisch anhand der Gruppeninformationen angezeigt werden. Die zusätzlichen Attribute werden nicht in das LDAP geschrieben, sondern bei einer Anfrage durch das Overlay-Modul ermittelt und angezeigt.

Achtung

Bevor Sie diese Funktion verwenden, lesen Sie bitte SDB 1278 über die Aktivierung des `memberOf Overlay-Moduls`.

Dazu muss auf allen LDAP-Servern das Paket ***univention-ldap-overlay-memberof*** installiert werden. Anschließend muss `/usr/share/univention-ldap-overlay-memberof/univention-update-memberof` auf allen Servern aufgerufen werden.

In der Grundeinstellung wird das Benutzerattribut *memberOf* dargestellt. Mit der Univention Configuration Registry-Variable `ldap/overlay/memberof/memberof` kann auch ein anderes Attribut konfiguriert werden.

http://sdb.univention.de/1278

univention
be open.

Kapitel 8. Rechnerverwaltung

8.1. Verwaltung der Rechnerkonten in Univention Management Console

Feedback

Alle UCS-, Linux- und Windowssysteme innerhalb einer UCS-Domäne verfügen über ein Rechner-Domänenkonto, mit dem sich die Systeme untereinander authentifizieren und mit dem sie auf das LDAP-Verzeichnis zugreifen.

Das Rechnerkonto wird in der Regel automatisch beim Join des Systems zur UCS-Domäne angelegt (siehe Abschnitt 3.2), das Rechnerkonto kann jedoch auch vor dem Domänenbeitritt angelegt werden.

Das Passwort für das Rechnerkonto wird beim Domänenbeitritt automatisch erzeugt und in der Datei `/etc/machine.secret` gespeichert. Das Passwort umfasst in der Grundeinstellung 20 Zeichen (konfigurierbar über die Univention Configuration Registry-Variable `machine/password/length`). Das Passwort wird in festen Intervallen automatisch neu generiert (in der Grundeinstellung 21 Tage, konfigurierbar über die Univention Configuration Registry-Variable `server/password/interval`). Die Passwortrotation kann über die Variable `server/password/change` auch deaktiviert werden.

Für jede Systemrolle existiert ein eigenständiger Rechnerobjekttyp. Weitergehende Hinweise zu den einzelnen Systemrollen finden sich in Abschnitt 3.3.

Rechnerkonten werden im Modul **Rechner** von Univention Management Console verwaltet.

In der Grundeinstellung wird zum Anlegen eines Rechners ein vereinfachter Assistent angezeigt, der nur die wichtigsten Einstellungen abfragt. Durch einen Klick auf **Erweitert** werden alle Attribute angezeigt. Ist dem ausgewählten Netzwerk-Objekt (siehe Abschnitt 11.1) eine DNS-Forward-Zone und/oder eine DNS-Reverse-Zone zugeordnet (siehe Abschnitt 11.2), wird für den Rechner automatisch ein Host-Record und/oder Pointer-Record angelegt. Ist für das Netzwerk-Objekt ein DHCP-Service konfiguriert und wird eine MAC-Adresse konfiguriert, wird ein DHCP-Rechner-Eintrag angelegt (siehe Abschnitt 11.3)

Der vereinfachte Assistent kann für alle Systemrollen deaktiviert werden, indem die Univention Configuration Registry-Variable `directory/manager/web/modules/computers/computer/wizard/disabled` auf `true` gesetzt wird.

Abbildung 8.1. Anlegen eines Rechners in UMC

Abbildung 8.2. Erweiterte Rechneransicht

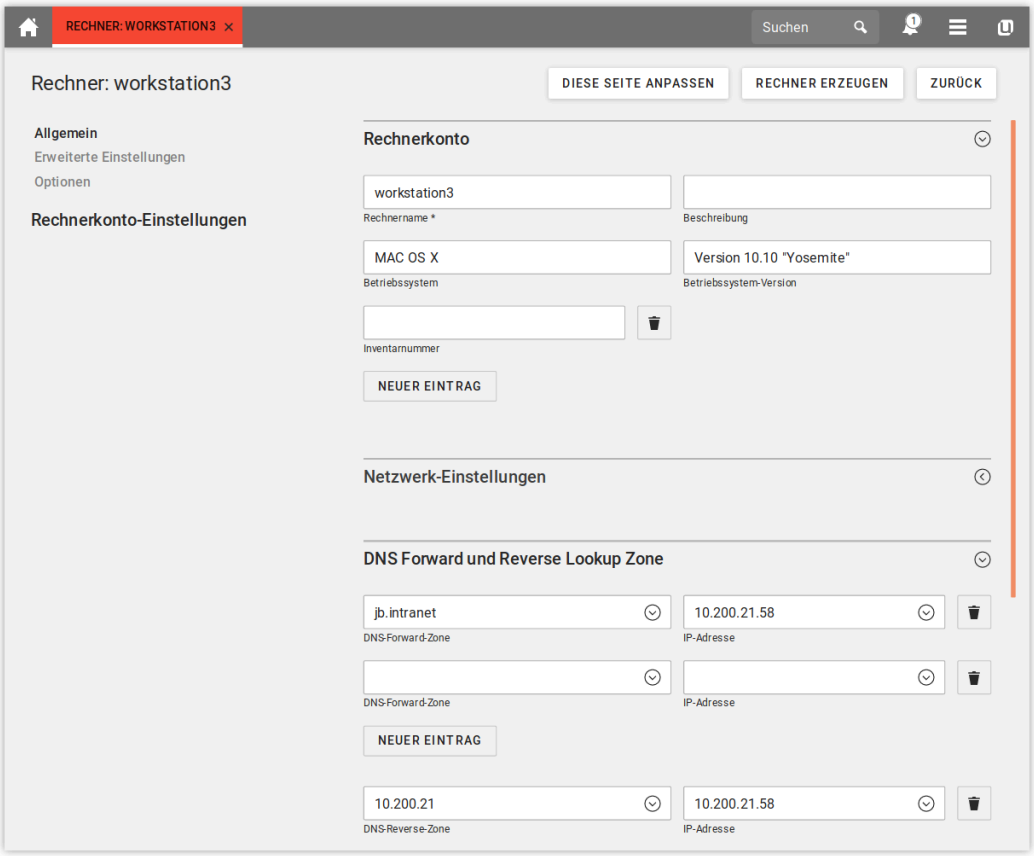


Tabelle 8.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name	In dieses Eingabefeld muss der Rechnername eingetragen werden. Um die Kompatibilität mit verschiedenen Betriebssystemen und Diensten zu gewährleisten, sollten Rechnernamen ausschließlich die Buchstaben *a* bis *z* in Kleinschreibung, Zahlen, Bindestriche und Unterstriche enthalten. Umlaute und Sonderzeichen sind nicht erlaubt. Der Punkt wird als Trennzeichen zwischen den einzelnen Bestandteilen eines voll qualifizierten Domänennamens interpretiert und darf deswegen nicht innerhalb des Rechnernamens verwendet werden. Rechnernamen sollten mit einem Buchstaben beginnen. Microsoft Windows akzeptiert nur Rechnernamen mit maximal 13 Zeichen, so dass man sich bei Rechnernamen grundsätzlich auf 13 Zeichen beschränken sollte, sofern nicht ausgeschlossen ist, dass Microsoft Windows zum Einsatz kommen wird. Der Rechnername kann nach dem Anlegen nur bei den Systemrollen *Windows Workstation/Server*, *Mac OS X Client* und *IP-Managed-Client* verändert werden.
Beschreibung	Für den Rechner kann in diesem Eingabefeld eine beliebige Beschreibung hinterlegt werden.

Attribut	Beschreibung
Inventarnummer	Hier können Inventarnummern für Rechner hinterlegt werden.
Netzwerk	Der Rechner kann einem bereits angelegten Netzwerk-Objekt zugeordnet werden. Hinweise zur IP-Konfiguration finden sich in Abschnitt 11.1.
MAC-Adresse	An dieser Stelle kann die MAC-Adresse des Rechners eingetragen werden, z.B. `2e:44:56:3f:12:32`. Soll der Rechner einen DHCP-Eintrag erhalten, ist die Angabe der MAC-Adresse zwingend erforderlich.
IP-Adresse	Hier können feste IP-Adressen für den Rechner eingegeben werden. Wenn auf der Karteikarte **Allgemein** ein Netzwerk ausgewählt wurde, wird die IP-Adresse, die dem Rechner aus dem Netzwerk automatisch zugewiesen wurde, hier angezeigt. Weitere Hinweise zur IP-Konfiguration finden sich in Abschnitt 11.1. Eine hier (also im LDAP-Verzeichnis) eingetragene IP-Adresse kann dem Rechner nur über DHCP zugewiesen werden. Sollte kein DHCP-Server verwendet werden, so muss die IP-Adresse auch lokal auf dem Rechner konfiguriert werden, siehe Abschnitt 8.2.4. Werden die eingetragenen IP-Adressen eines Rechners ohne Wechsel der DNS-Zonen geändert, werden diese im Rechner-Objekt und - soweit vorhanden - auch automatisch in den DNS-Einträgen in der Forward und Reverse Lookup Zone geändert. Falls die IP-Adresse des Rechners noch an anderen Stellen eingetragen wurde, müssen diese Einträge manuell geändert werden! Wurde beispielsweise in einer DHCP-Boot-Richtlinie nicht der Name des Boot-Servers, sondern seine IP-Adresse dort eingetragen, muss diese IP-Adresse manuell durch das Bearbeiten der Richtlinie angepasst werden.
Forward-Zone für DNS-Eintrag	Die DNS-Forward-Zone, in die der Rechner eingetragen wird. Die Zone dient der Auflösung des Rechnernamens in die zugewiesene IP-Adresse. Hinweise zur IP-Konfiguration finden sich in Abschnitt 11.1.
Reverse-Zone für DNS-Eintrag	Die DNS-Reverse-Zone, in die der Rechner eingetragen wird. Mit der Zone wird die IP-Adresse des Rechners in einen Rechnernamen aufgelöst. Hinweise zur IP-Konfiguration finden sich in Abschnitt 11.1.
Service für DHCP-Eintrag	Wenn ein Rechner seine IP-Adresse über DHCP beziehen soll, muss hier ein DHCP-Service zugeordnet werden. Hinweise zur IP-Konfiguration finden sich in Abschnitt 11.1. Bei der Zuweisung muss darauf geachtet werden, dass die DHCP-Server des DHCP-Service-Objekts für das physikalische Netzwerk zuständig sind. Wurde auf der Karteikarte **Allgemein** ein Netzwerk ausgewählt, wird automatisch ein für das Netzwerk passender Eintrag hinzugefügt, der nachträglich manuell angepasst werden kann.

Tabelle 8.2. Reiter 'Konto' (erweiterte Einstellungen)

Attribut	Beschreibung
Passwort	Das Passwort des Rechnerkontos wird in der Regel automatisch erstellt und rotiert. Für Sonderfälle wie die Einbindung externer Systeme kann es in diesem Feld auch explizit konfiguriert werden.

Attribut	Beschreibung
	Dasselbe Passwort muss dann auch lokal auf dem Rechner in die Datei `/etc/machine.secret` eingetragen werden.
Primäre Gruppe	In diesem Auswahlfeld kann die primäre Gruppe des Rechners selektiert werden. Das ist nur notwendig, wenn von den automatisch eingestellten Vorgabewerten abgewichen werden soll. Der Vorgabewert für einen DC Master oder DC Backup lautet `DC Backup Hosts`, für einen DC Slave `DC Slave Hosts` und für Memberserver `Computers`.

Tabelle 8.3. Reiter 'Unix-Konto' (erweiterte Einstellungen)

Attribut	Beschreibung
UNIX-Heimatverzeichnis (*)	In diesem Eingabefeld kann ein abweichendes Heimatverzeichnis für das Rechner-Konto eingetragen werden. Der automatisch eingestellte Vorgabewert für das Heimatverzeichnis lautet `/dev/null`.
Login-Shell	Falls eine vom Vorgabewert abweichende Login-Shell für das Rechner-Konto verwendet werden soll, kann die Login-Shell in diesem Eingabefeld manuell angepasst werden. Der automatisch eingestellte Vorgabewert sieht `/bin/sh` als Login-Shell vor.

Tabelle 8.4. Reiter 'Dienste' (erweiterte Einstellungen)

Attribut	Beschreibung
Dienst	Mit einem Dienst-Objekt können Applikationen oder Dienste feststellen, ob auf einem Rechner oder generell in der Domäne ein Dienst verfügbar ist.

Anmerkung

Die Karteikarte 'Dienste' wird nur auf UCS-Serversystemrollen angezeigt.

Tabelle 8.5. Reiter '(Re)installation' (erweiterte Einstellungen)

Diese Karteikarte wird für den Univention Net Installer verwendet, siehe [ext-doc-inst].

Tabelle 8.6. Reiter 'DNS-Alias' (erweiterte Einstellungen)

Attribut	Beschreibung
Zone für DNS-Alias	Wenn für den Rechner im Feld **Forward Lookup Zone für DNS-Eintrag** ein Zoneneintrag zur Vorwärtsauflösung eingerichtet wurde, können hier zusätzlich Alias-Einträge konfiguriert werden, über die der Rechner erreichbar ist.

Tabelle 8.7. Reiter 'Gruppen' (erweiterte Einstellungen)

In diesem Reiter kann der Rechner in verschiedene Gruppen aufgenommen werden.

Tabelle 8.8. Reiter 'Nagios-Dienste' (erweiterte Einstellungen)

In diesem Reiter wird festgelegt, welche Nagios-Prüfungen für diesen Rechner durchgeführt werden, siehe Abschnitt 15.3.3.3.

Tabelle 8.9. Reiter 'Nagios-Benachrichtigung' (erweiterte Einstellungen)

In diesem Reiter wird festgelegt, welche Benutzer bei fehlschlagenden Nagios-Prüfungen benachrichtigt werden, siehe Abschnitt 15.3.3.3.

Tabelle 8.10. Reiter 'UVMM' (erweiterte Einstellungen)

In diesem Reiter wird festgelegt, welche Virtualisierungs-Server durch UVMM verwaltbar sind (siehe Kapitel 16).

Tabelle 8.11. Reiter '(Optionen)'

Attribut	Beschreibung
Die Karteikarte ermöglicht es, einzelne LDAP-Objektklassen für den Rechner zu konfigurieren. Die Eingabefelder für Attribute abgewählter Objektklassen werden dann nicht angezeigt. Nicht alle Objektklassen können nachträglich verändert werden.	
Kerberos Prinzipal	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklassen `krb5Principal` und `krb5KDCEntry` nicht.
POSIX Konto	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklasse `posixAccount` nicht.
Samba-Konto	Ist dieses Auswahlkästchen nicht markiert, erhält der Rechner die Objektklasse `sambaSamAccount` nicht.
Nagios-Unterstützung	Nur wenn diese Option aktiviert ist, können Nagios-Prüfungen für dieses Rechnerkonto konfiguriert werden.

8.1.1. Integration von Ubuntu-Clients

Feedback

Ubuntu-Clients können mit einer eigenen Rechnerrolle in Univention Management Console verwaltet werden. Die Netzwerkeigenschaften für DNS/DHCP können dabei ebenfalls mit Univention Management Console verwaltet werden.

Die Anwendung von Richtlinien wird nicht unterstützt.

Auf den Ubuntu-Systemen müssen einige Konfigurationsanpassungen vorgenommen werden, die in der erweiterten Dokumentation beschrieben sind [ext-doc-domain].

8.2. Konfiguration von Hardware und Treibern

Feedback

8.2.1. Verfügbare Kernel-Varianten

Feedback

Der Standard-Kernel in UCS 4.4 basiert auf dem Linux-Kernel 4.9. Prinzipiell sind drei verschiedene Arten von Kernel-Paketen zu unterscheiden:

- Ein *Kernel-Image-Paket* stellt einen lauffähigen Kernel bereit, der installiert und gestartet werden kann.
- Ein *Kernel-Source-Paket* stellt den Quellcode für einen Kernel bereit. Aus diesem kann beispielsweise ein angepasster Kernel erstellt werden, indem Funktionen aktiviert oder deaktiviert werden können.
- Ein *Kernel-Header-Paket* stellt Schnittstellen-Informationen bereit, die von externen Paketen benötigt werden, wenn diese auf Kernel-Funktionen zugreifen müssen. Sie werden typischerweise zum Übersetzen externer Kernel-Treiber benötigt.

Im Regelfall ist für den Betrieb eines UCS-Systems nur die Installation eines Kernel-Image-Paketes notwendig.

Der Standard-Kernel in UCS für i386-basierte Systeme ist der sogenannte *bigmem-Kernel* für Prozessoren mit PAE-Unterstützung, der 64 GB RAM unterstützt. Für ältere i386-basierte Systeme wird ein zweiter Kernel ohne PAE-Unterstützung bereitgestellt, der maximal 4 GB Arbeitsspeicher unterstützt. Der Standard-Kernel für amd64-Systeme besitzt keine solchen Einschränkungen.

Mehrere Kernel-Varianten können parallel installiert sein. Dies stellt sicher, dass im Fehlerfall immer auf eine ältere Variante zurückgegriffen werden kann. Um ein System trotzdem immer auf dem jeweils aktuellen Stand halten zu können, werden sogenannte Meta-Pakete bereitgestellt, die immer auf die aktuell für UCS empfohlene Kernel-Version verweisen und diese im Update-Fall jeweils nachinstallieren.

Die folgenden Meta-Pakete stehen unter i386 / 32 Bit zur Verfügung:

- ***univention-kernel-image*** - Standard-Kernel (max. 64 GB RAM)
- ***univention-kernel-image-486*** - Kernel für Systeme ohne PAE-Support (max. 4 GB RAM)

Die folgenden Meta-Pakete stehen unter amd64 / 64 Bit zur Verfügung:

- ***univention-kernel-image*** - Standard-Kernel

8.2.2. Treiber-Management / Kernel-Module

Der Boot-Prozess erfolgt zweistufig unter Verwendung einer Initial RAM Disk (kurz initrd). Diese besteht aus einem Archiv mit weiteren Treibern und Programmen. Der Boot-Manager GRUB (siehe Abschnitt 8.2.3) lädt den Kernel und die initrd in den Arbeitsspeicher, wo das initrd-Archiv entpackt und als temporäres Root-Dateisystem gemountet wird. Aus diesem wird dann das tatsächliche Root-Dateisystem eingebunden, woraufhin abschließend das temporäre Archiv wieder entfernt und der Systemstart eingeleitet wird.

Die zu verwendenden Treiber werden beim Systemstart automatisch erkannt und durch den Device Manager udev geladen. Dabei werden außerdem die notwendigen System-Verknüpfungen unter `/dev/` angelegt. Wenn Treiber nicht erkannt werden (was vorkommen kann, wenn keine entsprechenden Hardware-IDs registriert sind oder Hardware verwendet wird, die nicht automatisch erkannt werden kann, etwa ISA-Steckkarten), so können zu ladende Kernel-Module durch die Univention Configuration Registry-Variable `kernel/modules` hinzugefügt werden. Soll mehr als ein Kernel-Modul geladen werden, so müssen diese durch ein Semikolon voneinander getrennt werden. Mit der Univention Configuration Registry-Variable `kernel/blacklist` kann eine Liste von einem oder mehreren Kernel-Modulen konfiguriert werden, für die das automatische Laden verhindert wird. Mehrere Einträge müssen ebenfalls durch ein Semikolon getrennt werden.

Im Gegensatz zu anderen Betriebssystemen liefert der Linux-Kernel (von wenigen Ausnahmen abgesehen) alle Treiber für Komponenten aus einer Hand. Im Regelfall ist es deshalb nicht notwendig Treiber aus externen Quellen nachzuinstallieren.

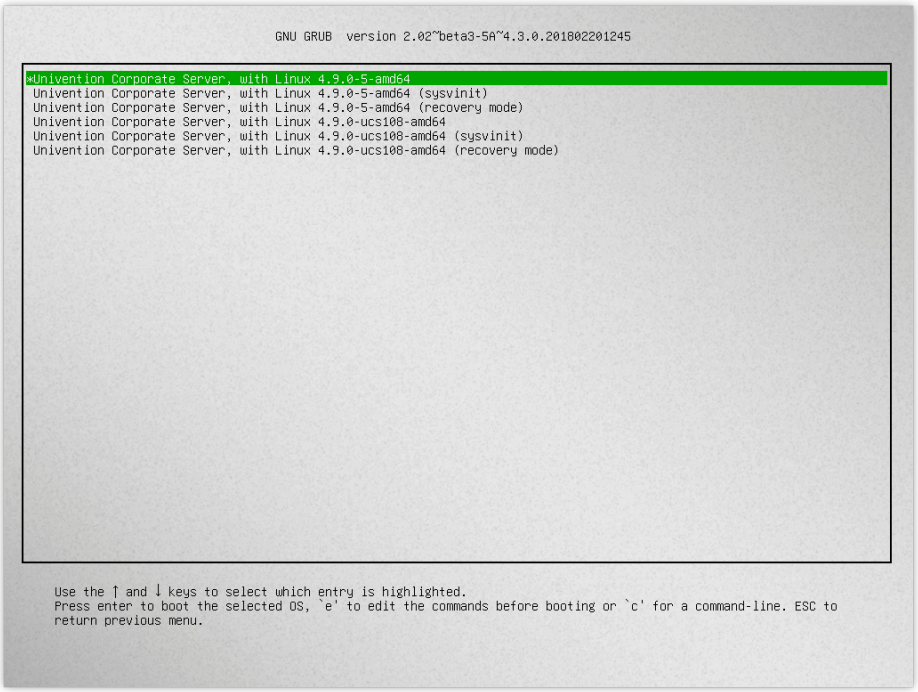
Wenn doch externe Treiber oder Kernelmodule benötigt werden, können diese über *Dynamic Kernel Module Support* (DKMS) eingebunden werden. Es stellt eine standardisierte Schnittstelle für Kernelquellen bereit und erlaubt es, Module automatisch für jeden installierten Kernel zu übersetzen. Dazu müssen neben dem Paket ***dkms*** auch die Kernel-Header-Pakete ***univention-kernel-headers*** für die gewünschten Kernel installiert werden. Zu beachten ist, dass nicht alle externen Kernelmodule mit allen Kernel kompatibel sind.

8.2.3. GRUB Boot-Manager

Als Boot-Manager wird in Univention Corporate Server GNU GRUB 2 verwendet. GRUB stellt ein Auswahlmenü bereit, aus dem eine zu bootende Linux-Kernel-Variante oder ein weiteres Betriebssystem ausgewählt

werden kann. GRUB kann auch direkt auf Dateisysteme zugreifen, so dass im Fehlerfall etwa ein abweichender Kernel geladen werden kann.

Abbildung 8.3. GRUB-Auswahlmenü



GRUB wird in einem zweistufigen Verfahren geladen: in den Master Boot Record der Festplatte wird der Stage 1-Loader geschrieben, der auf die Daten der Stage 2 verweist, welche den Großteil des übrigen Boot-Vorgangs übernimmt.

Die Auswahl der zu startenden Kernel im Boot-Menü wird in der Datei `/boot/grub/grub.cfg` abgelegt. Diese Datei wird automatisch generiert, es stehen alle installierten Kernel-Pakete zur Auswahl. Durch Auswahl der Option **Memory test** kann das Speicher-Testprogramm `Memtest86+` gestartet werden, das Konsistenzprüfungen auf dem Arbeitsspeicher durchführt.

Standardmäßig wird fünf Sekunden auf die Auswahl des zu bootenden Kernels gewartet. Durch die Univention Configuration Registry-Variable `grub/timeout` kann ein abweichender Wert in Sekunden konfiguriert werden.

In der Grundeinstellung wird in einen *800x600* Pixel großen Bildschirm unter 16 Bit Farbtiefe gewechselt. Durch die Univention Configuration Registry-Variable `grub/gfxmode` kann ein anderer Modus ausgewählt werden. Es werden nur Auflösungen unterstützt, die über VESA BIOS Extentions gesetzte werden können. Eine Liste der verfügbaren Modi findet sich unter https://en.wikipedia.org/wiki/VESA_BIOS_Extensions. Die Eingabe erfolgt im Format ***`HORIZONTALxVERTIKAL@FARBTIEFEBIT`***, also z.B. `1024x768@16`.

Kernel-Optionen für die gestarteten Linux-Kernel können mit der Univention Configuration Registry-Variable `grub/append` übergeben werden. Mit der `grub/xenhopt` können Optionen an den Xen-Hypervisor übergeben werden.

Die grafische Darstellung während des Bootvorgangs - der sogenannte Splash-Screen - kann durch Setzen der Univention Configuration Registry-Variable `grub/bootsplash` auf `nosplash` deaktiviert werden.

In älteren Xen-Umgebungen wird zum Booten paravirtualisierter Systeme noch eine Version von PyGrub verwendet, die auf die ältere GRUB 1-Konfigurationsdatei `/boot/grub/menu.lst` angewiesen ist. Diese

wird automatisch erzeugt, sofern sie noch nicht existiert. Dieses Verhalten kann durch Setzen der Univention Configuration Registry-Variable `grub/generate-menu-lst` auf `no` deaktiviert werden.

8.2.4. Netz-Konfiguration

Feedback

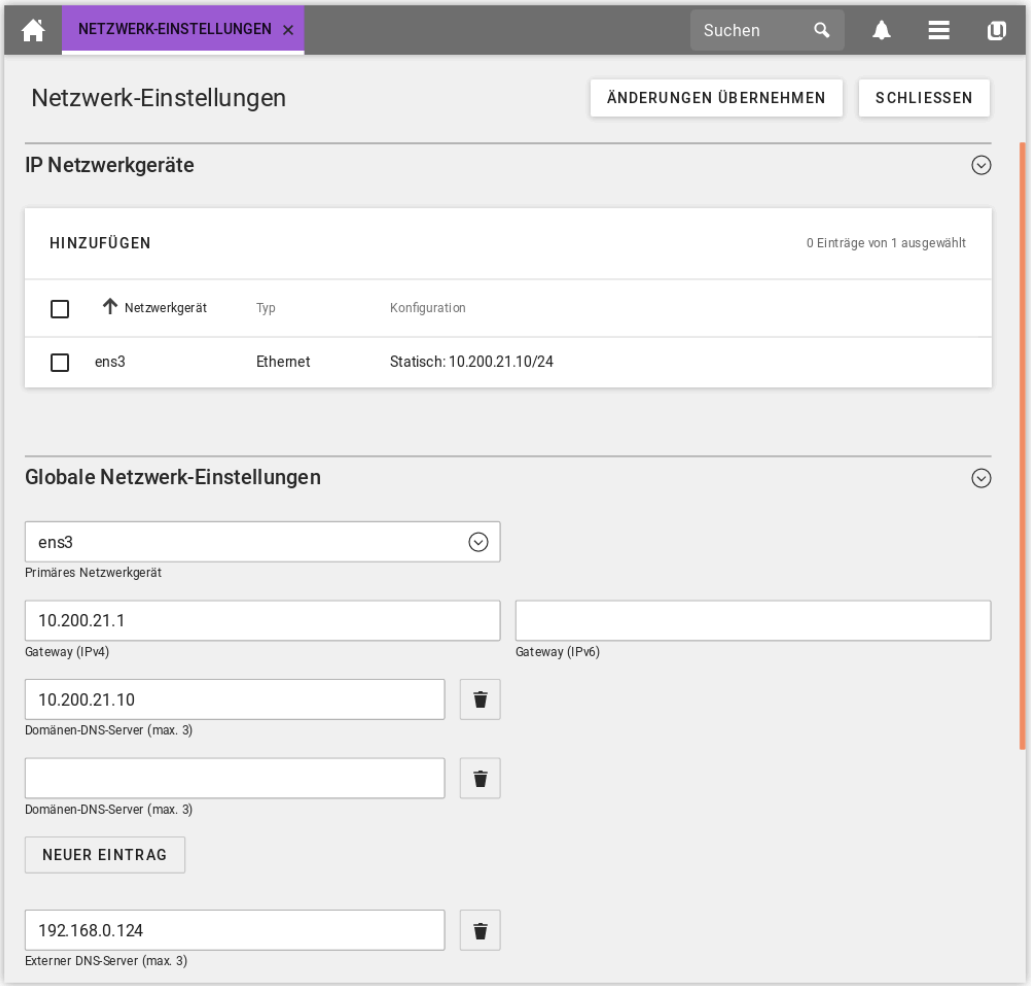
8.2.4.1. Netzwerk-Interfaces

Feedback

Die Konfiguration von Netzwerk-Interfaces kann in Univention Management Console über das Modul **Netzwerk-Einstellungen** angepasst werden.

Die Konfiguration wird in Univention Configuration Registry-Variablen gespeichert, die auch direkt gesetzt werden können. Die Variablen sind in den einzelnen Abschnitten zusätzlich in Klammern aufgeführt.

Abbildung 8.4. Konfiguration der Netzwerkeinstellungen



Unter **IPv4-Netzwerkgeräte** und **IPv6-Netzwerkgeräte** werden alle im System verfügbaren Netzwerkkarten aufgeführt (es werden nur Netzwerkinterfaces im Schema `ethX` dargestellt).

Netzwerkschnittstellen können für IPv4 und/oder IPv6 konfiguriert werden. IPv4-Adressen haben 32 Bit Länge und werden in der Regel in vier Blöcken in Dezimalschreibweise dargestellt (z.B. `192.0.2.10`), während IPv6-Adressen vier Mal so lang sind und typischerweise hexadezimal dargestellt werden (z.B. `2001:0DB8:FE29:DE27:0000:0000:0000:0000`).

8.2.4.1.1. Konfiguration von IPv4-Adressen

Feedback

Wenn die Option **Dynamisch (DHCP)** nicht gewählt wurde, muss die IP-Adresse eingegeben werden, die an die Netzwerkkarte gebunden werden soll. Zusätzlich zur **IPv4-Adresse** muss die **Netzmaske** angegeben werden. Mit **DHCP-Anfrage** kann eine Adresse von einem DHCP-Server abgefragt werden. Sofern die Option **Dynamisch (DHCP)** nicht aktiviert wird, werden die aus der DHCP-Anfrage erhaltenen Werte dann statisch konfiguriert.

Auch Server-Systeme können per DHCP konfiguriert werden. Dies ist z.B. bei einigen Cloud-Anbietern notwendig. Schlägt die Vergabe einer IP-Adresse für einen Server fehl, wird ersatzweise eine zufällige Link-Local-Adresse (`169.254.x.y`) konfiguriert.

Die über DHCP erhaltene Adresse wird für UCS-Serversysteme auch in das LDAP-Verzeichnis geschrieben.

> **Anmerkung**
>
> Nicht alle Dienste (z.B. DNS-Server) sind für eine Verwendung auf einem DHCP-basierten Server geeignet.

(UCR-Variablen: `interfaces/ethX/address`, `interfaces/ethX/netmask`, `interfaces/ethX/type`)

Neben den physischen Interfaces können auch zusätzliche virtuelle Interfaces in der Form `interfaces/ethX_Y/Eigenschaft` definiert werden.

8.2.4.1.2. Konfiguration von IPv6-Adressen

Feedback

Die IPv6-Adresse kann auf zwei Arten konfiguriert werden: Bei der **Automatischen Konfiguration (SLAAC)** kommt Stateless Address Autoconfiguration (SLAAC) zum Einsatz. Dabei wird die IP-Adresse von den Routern des lokalen Netzsegmentes zugewiesen. Alternativ kann die Adresse auch durch Angabe von **IPv6-Adresse** und **IPv6-Präfix** statisch konfiguriert werden. Im Gegensatz zu DHCP wird bei SLAAC keine Zuweisung von weitergehenden Daten wie dem zu verwendenden DNS-Server durchgeführt. Hierfür gibt es mit DHCPv6 ein Zusatzprotokoll, das bei der dynamischen Zuweisung aber nicht zum Einsatz kommt. Eine Netzwerkkarte kann verschiedene IPv6-Adressen bedienen. Der **Bezeichner** ist ein eindeutiger Name für einzelne Adressen. Die Haupt-Adresse verwendet immer den Bezeichner *default*, für alle anderen Adressen können funktionale Bezeichner vergeben werden z.B. *Interface-Mailserver*.

(UCR-Variablen: `interfaces/ethX/ipv6/address`, `interfaces/ethX/ipv6/prefix`, `interfaces/eth0/ipv6/acceptRA` aktiviert SLAAC).

Unter **Globale Netzwerk-Einstellungen** können weitere netzwerkbezogene Einstellungen vorgenommen werden.

Unter **Gateway (IPv4)** und **Gateway (IPv6)** können die für die IP-Adresse im Subnetz eingesetzten Standard-Gateways für IPv4 und IPv6 eingegeben werden. Für IPv6 ist die Angabe eines Gateways nicht erforderlich, wird jedoch empfohlen. Ein hier konfiguriertes IPv6-Gateway hat Vorrang vor Router Advertisements, die ansonsten die Route ändern könnten.

(UCR-Variablen: `gateway`, `ipv6/gateway`)

8.2.4.1.3. Konfiguration der Nameserver

Feedback

Zwei Typen von DNS-Servern werden unterschieden:

- Ein **externer DNS-Server** wird für die Auflösung von Rechnernamen und Adressen außerhalb der UCS-Domäne verwendet, z.B. `univention.de`. Dies ist typischerweise ein Nameserver, der vom Internet Provider betrieben wird.

- Ein **Domänen-DNS-Server** ist ein lokaler Nameserver der UCS-Domäne. Dort werden in der Regel die Rechnernamen und IP-Adressen der UCS-Domäne verwaltet. Wird eine Adresse im lokalen Datenbestand nicht aufgefunden, wird automatisch ein externer DNS-Server angefragt. Die DNS-Daten werden im LDAP-Verzeichnisdienst gespeichert, d.h. alle Domänen-DNS-Server liefern identische Daten aus.

Bei der Installation eines Domänencontroller Master wird nur ein **externer DNS-Server** abgefragt, da im Rahmen der Installation immer ein Domänen-DNS-Server eingerichtet wird. Dieser kann dann von den anderen Systemen der Domäne verwendet wird. Über die Schaltfläche **[Mehr]** können weitere Nameserver aufgenommen werden.

Auf den Systemrollen Domänencontroller Master, Domänencontroller Backup und Domänencontroller Slave läuft ein lokaler DNS-Server. Hier kann durch Angabe von **Domänen-DNS-Server** konfiguriert werden, welcher Server primär für die Namensauflösung verwendet wird.

(UCR-Variablen: `nameserver1` bis `nameserver3`, `dns/forwarder1` bis `dns/forwarder3`,

8.2.4.1.4. Konfiguration von Bridges/Bonding/VLANs

Feedback

UCS unterstützt komplexe Netzwerk-Konfigurationen mit Bridges, Bonding und VLAN-Netzen:

- *Bridges* werden oft von Virtualisierungslösungen verwendet, um virtualisierte Netzwerkkarten einer virtuellen Maschine mit der physischen Netzwerkkarte des Virtualisierungsservers zu verbinden.
- *Bonding* erhöht die Ausfallsicherheit, in dem mehrere physikalische Netzwerkkarten für den Zugriff auf ein Netzwerk gebündelt werden.
- *VLANs* können verwendet werden um den Netzwerkverkehr in einem physikalischen Netzwerk logisch auf ein oder mehrere virtuelle Unternetze aufzuteilen.

8.2.4.1.4.1. Voraussetzungen bei Verwendung von UCS Virtual Machine Manager

Feedback

Bei der Installation der Applikation *KVM Virtualisierungsserver* wird die Netzwerkkonfiguration verändert: Es wird eine Bridge mit dem Namen `br0` angelegt, in die die Netzwerkkarte mit dem Namen `eth0` eingehängt wird. Zusätzliche Netzwerkkarten werden nicht adaptiert.

Bei einem Update von UCS 3.2 verhindert die Konfiguration die Verwendung der fortgeschrittenen Netzwerkkonfiguration. Sie kann durch das Setzen der folgenden UCR-Variablen deaktiviert werden:

```
# für KVM:
ucr set uvmm/kvm/bridge/autostart=no
# Danach die UMC-Basiseinstellungen reaktivieren:
ucr unset umc/modules/setup/network/disabled/by
```

Danach muss der Server neu gestartet werden. Bei existierenden virtuellen Maschinen müssen danach die Namen der Netzwerkinterfaces angepasst werden, was in Abschnitt 16.5.4 beschrieben ist. Weiterhin wird empfohlen, die UVMM-Profile für neue virtuelle Maschinen anzupassen, was in Abschnitt 16.6.1 beschrieben ist.

8.2.4.1.4.2. Bridging

Feedback

Der häufigste Anwendungsfall für *Bridging* ist die gemeinsame Nutzung einer physischen Netzwerkkarte durch eine oder mehrere virtuelle Maschinen. Anstatt eine Netzwerkkarte für jede virtuelle Maschine und den Virtualisierungsserver selbst zu verwenden, werden alle System durch einen gemeinsamen Uplink angebunden. Eine Bridge kann mit einem in Software realisierten Switch verglichen werden, über den einzelne Hosts miteinander verbunden werden. Die verwendete Hardware-Netzwerkkarte wird als *Bridge Port* bezeichnet.

Um eine Bridge zu konfigurieren muss unter **Hinzufügen** als **Netzwerkgerätetyp** *Bridge* ausgewählt werden. Der **Name des neuen Bridge-Netzwerkgerätes** kann beliebig gewählt werden. Anschließend muss auf **Weiter** geklickt werden.

Unter **Bridge ports** kann die physische Netzwerkkarte ausgewählt werden, die den Uplink darstellt. Im typischen Anwendungsfall der Anbindung virtueller Maschinen über nur eine Netzwerkkarte kann keine Schleife auftreten. Wird die Bridge zur Verbindung zweier Netzwerkkarten verwendet, wird das Spanning Tree Protocol (STP) zur Vermeidung von Netzwerkschleifen eingesetzt[1]. Die Einstellung **Forwarding delay** konfiguriert die Wartezeit in Sekunden, während der bei Aufbau einer Verbindung durch STP Informationen über die Netzwerktopologie gesammelt werden. Wird die Bridge zur Anbindung virtueller Maschinen über eine physische Netzwerkkarte verwendet, sollte STP dann deaktiviert werden, in dem der Wert auf 0 gesetzt wird. Ansonsten kann es zu Problemen bei der Verwendung von DHCP führen, da die während der Wartezeit versendeten Pakete nicht weitergeleitet werden.

Über das Eingabefeld **Weitere Geräteoptionen** können beliebige weitere Bridge-Parameter konfiguriert werden. Dies ist nur in Ausnahmefällen nötig, eine Übersicht der möglichen Einstellungen findet sich in der Manpage bridge-utils-interfaces(5).

Nach einem Klick auf **Weiter** kann der Bridge optional eine IP-Adresse zugewiesen werden. Diese kann dann auch als Netzwerkinterface auf dem Virtualisierungshost verwendet werden. Die Einstellungsmöglichkeiten sind dieselben wie in Abschnitt 8.2.4.1.1 und Abschnitt 8.2.4.1.2 beschrieben.

8.2.4.1.4.3. Bonding

Mit *Bonding* können zwei (oder mehr) physische Netzwerkkarten zur Erhöhung des Durchsatzes oder zur Verbesserung der Redundanz in Failoverszenarien gebündelt werden.

Um ein Bonding zu konfigurieren muss unter **Hinzufügen** als **Netzwerkgerätetyp** *Kanalbündelung (Bonding)* ausgewählt werden. Der **Name des neuen Bonding-Netzwerkgerätes** kann beliebig gewählt werden. Anschließend muss auf **Weiter** geklickt werden.

Unter **Bond slaves** werden die Netzwerkkarten ausgewählt, die Teil des Bonding-Interfaces sind. Für das Failover-Szenarien (s.u.) können über **Bond primary** die Netzwerkkarten ausgewählt werden, die bevorzugt verwendet werden sollen.

Der **Modus** konfiguriert die Verteilung der Netzwerkkarten innerhalb des Bondings:

- **balance-rr (0)** verteilt die Pakete der Reihe nach gleichmässig auf die verfügbaren Netzwerkschnittstellen innerhalb des Bondings. Dies erhöht den Durchsatz und verbessert die Ausfallsicherheit. Zur Verwendung dieser Variante müssen die verwendeten Netzwerk-Switches *Link Aggregation* unterstützen.

- Bei Verwendung von **active-backup (1)** ist nur jeweils eine Netzwerkkarte des Bonding-Interfaces aktiv (in der Grundeinstellung die Netzwerkschnittstelle aus **Bond primary**). Fällt die primäre Netzwerkkarte aus, wird dies durch den Linux-Kernel erkannt und auf eine der weiteren Karten des Bondings umgeschaltet. Diese Variante erhöht die Ausfallsicherheit. Sie kann mit jedem Netzwerk-Switch verwendet werden.

Darüber hinaus existieren noch weitere Bonding-Methoden. Diese sind in der Regel nur für Sonderfälle relevant und sind unter [bonding] beschrieben.

Zur Erkennung ausgefallener Netzwerkverbindungen wird das Media Independent Interface (MII) der Netzwerkkarten verwendet. Die Einstellung **MII link monitoring frequency** legt das Prüfintervall in Millisekunden fest.

Unter **Weitere Bonding-Optionen** können beliebige weitere Bonding-Parameter konfiguriert werden. Dies ist nur in Ausnahmefällen nötig, eine Übersicht der möglichen Einstellungen findet sich unter [bonding].

Nach einem Klick auf **Weiter** kann dem Bonding-Interface eine IP-Adresse zugewiesen werden. Sollte eine der bestehenden Netzwerkkarten, die Bestandteil des Bonding-Interfaces sind schon eine IP-Adresse zuge-

[1] Der Linux-Kernel implementiert lediglich STP, nicht die Varianten Rapid STP oder Multiple STP.

wiesen haben, so wird diese Konfiguration entfernt. Die Einstellungsmöglichkeiten sind dieselben wie in Abschnitt 8.2.4.1.1 und Abschnitt 8.2.4.1.2 beschrieben.

8.2.4.1.4.4. VLANs

VLANs können verwendet werden um den Netzwerkverkehr in einem physischen Netzwerk logisch auf ein oder mehrere virtuelle Unternetze aufzuteilen. Jedes dieser virtuellen Netze ist eine eigenständige Broadcast-Domäne. So kann etwa in einem Firmennetzwerk das Netz für die Mitarbeiter von einem Gastnetz für Besucher unterschieden werden, obwohl die selbe physikalische Verkabelung genutzt wird. Die Zuordnung der einzelnen Endgeräte zu den VLANs erfolgt durch Konfiguration auf den verwendeten Switches. Die Netzwerk-Switches müssen 802.1q VLANs unterstützen.

Es werden zwei Typen von Verbindungen zwischen Netzwerkkarten unterschieden:

- Eine Verbindung transportiert nur Pakete eines spezifischen VLANs. In diesem Fall werden die Datenpakete *ungetagged* übertragen.

  Dies ist typischerweise der Fall, wenn nur ein einzelnes Endgerät über diese Netzwerkverbindung angebunden wird.

- Eine Verbindung transportiert Pakete aus mehreren VLANs. Dies wird auch als *trunk link* bezeichnet. In diesem Fall ist jedes Paket über eine VLAN-ID einem VLAN zugeordnet. Bei der Weiterleitung zwischen „trunk links“ und spezifischen VLANs übernimmt der Netzwerk-Switch die Aufgabe, anhand der VLAN-IDs die Pakete zu filtern und die VLAN-IDs hinzuzufügen und zu entfernen.

  Diese Verbindungsart wird vornehmlich zwischen Switches bzw. Servern eingesetzt.

  Einige Switches erlauben es auch Pakete mit und ohne VLAN-Tag über eine gemeinsame Verbindung zu schicken, darauf wird hier aber nicht weiter eingegangen.

Mit der Konfiguration eines VLANs in Univention Management Console kann für einen Rechner konfiguriert werden, an welchen VLANs er teilnehmen möchte. Ein Beispiel wäre ein interner Firmen-Webserver, der sowohl für die Mitarbeiter, als auch für die Benutzer des Gastnetzes verfügbar sein soll.

Um ein VLAN zu konfigurieren muss unter **Hinzufügen** als **Netzwerkgerätetyp** *Virtuelles LAN* ausgewählt werden. Die Netzwerkschnittstelle, für die das VLAN konfiguriert wird, wird mit **Übergeordnetes Netzwerkgerät** angegeben. Die **VLAN ID** ist der eindeutige Bezeichner für das VLAN. Gültige Werte sind 1 bis 4095. Anschließend muss auf **Weiter** geklickt werden.

Nach einem Klick auf **Weiter** kann dem VLAN-Interface eine IP-Adresse zugewiesen werden. Die Einstellungsmöglichkeiten sind dieselben wie in Abschnitt 8.2.4.1.1 und Abschnitt 8.2.4.1.2 beschrieben. Bei der Vergabe einer IP-Adresse muss darauf geachtet werden, dass die Adresse zum zugeordneten VLAN-Adressbereich passt.

8.2.4.2. Konfiguration des Proxyzugriffs

Die meisten Kommandozeilen-Tools, die Zugriffe auf Webserver durchführen (z.B. `wget`, `elinks` oder `curl`), prüfen, ob die Umgebungsvariable `http_proxy` gesetzt ist. Ist dies der Fall, wird automatisch der in dieser Variable eingestellte Proxy-Server verwendet.

Über die Univention Configuration Registry-Variable `proxy/http` kann das Setzen dieser Umgebungsvariable `http_proxy` durch einen Eintrag in `/etc/profile` aktiviert werden. Dabei muss die Proxy-URL angegeben werden, also z.B. `http://192.0.2.100`.

Der Proxy-URL kann optional auch die Angabe eines Ports folgen, welcher durch einen Doppelpunkt abzutrennen ist, z.B. `http://192.0.2.100:3128`. Erfordert der Proxy eine Authentifizierung des zugrei-

fenden Benutzers, so können die Benutzerinformationen in der Form `http://username:password@192.0.2.100` übergeben werden.

Die Umgebungsvariable wird nicht für aktuell geöffnete Sitzungen übernommen. Damit die Änderung aktiv wird, muss eine Neuanmeldung erfolgen.

Die UCS-Programme zur Paketverwaltung unterstützen ebenfalls den Betrieb über einen Proxy und lesen die Univention Configuration Registry-Variable direkt aus.

Einzelne Domänen können von der Verwendung des Proxys ausgenommen werden, in dem sie kommasepariert in die Univention Configuration Registry-Variable `proxy/no_proxy` aufgenommen werden. Unterdomänen werden dabei berücksichtigt; eine Ausnahme für `software-univention.de` wirkt sich also auch auf `updates.software-univention.de` aus.

8.2.5. Konfiguration der Bildschirmeinstellungen

Die Konfiguration der Grafikauflösungen und Monitor-Parameter erfolgt in der Grundeinstellung über eine automatische Erkennung der Grafikkarte und des Monitors. Dabei wird automatisch der beste für die Grafikkarte verfügbare Treiber ausgewählt und die Monitorauflösung auf den höchsten vom Monitor unterstützten Wert gesetzt.

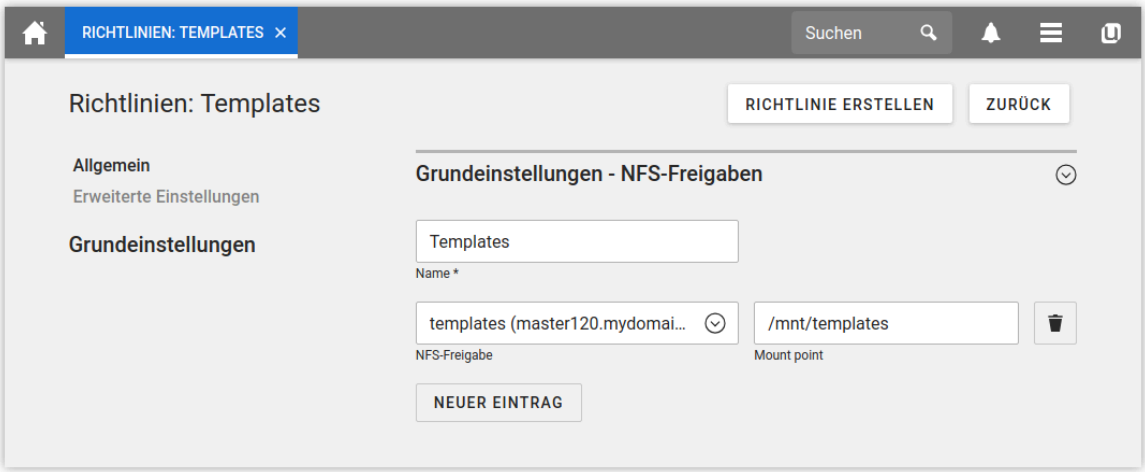
Die Einstellungen können auch über eine Univention Configuration Registry-Richtlinie gesetzt werden. Die manuelle Konfiguration ist auch nötig, wenn ein Dual-Monitor-Betrieb verwendet werden soll. Im folgenden eine Auswahl der wichtigen Einstellungen und die dazugehörigen UCR-Variablen in Klammern:

- **Grafikkarten-Treiber** wählt den zuständigen Xorg-Treiber aus (`xorg/device/driver`).
- Unter **Auflösung des primären Monitors** ist die Bildschirmauflösung des Hauptmonitors einzutragen. Die Angabe von Breite und Höhe in Pixeln ist durch ein "x" zu trennen, z.B. `1024x768` (`xorg/resolution`).
- **Auflösung des sekundären Monitors** definiert die Bildschirmauflösung eines eventuellen zweiten Monitors. Dieser bildet zusammen mit dem primären Monitor eine gemeinsame Bildschirmfläche (`xorg/resolution/secondary`).
- Das Auswahlfeld **Position des sekundären Monitors** gibt die relative Position des sekundären Monitors gegenüber dem primären Monitor an (`xorg/display/relative-position`).
- Die **Farbtiefe** ist in Bit pro Pixel anzugeben. Zulässige Werte sind 1, 2, 4, 8, 16 und 24. (24 Bit ist True Color-Farbtiefe) (`xorg/screen/DefaultDepth`).

8.2.6. Einbinden von NFS-Freigaben

Mit der Richtlinie **NFS-Freigaben** der Rechnerverwaltung in Univention Management Console können NFS-Freigaben konfiguriert werden, die auf dem System gemountet werden. Zur Auswahl steht eine **NFS-Freigabe**, die unter dem in **Mount point** angegebenen Dateipfad eingehängt wird.

Abbildung 8.5. Einbinden einer NFS-Freigabe



8.2.7. Erfassung von unterstützter Hardware

Feedback

Univention erfasst Informationen über Hardware, die mit UCS kompatibel und bei Kunden im Einsatz ist. Die hierbei verarbeiteten Informationen werden über das UMC-Modul **Systeminformationen** erfasst.

Alle Daten werden dabei anonymisiert an Univention weitergeleitet und erst nach Benutzereinwilligung übermittelt.

Im Start-Dialog finden sich die Eingabefelder **Hersteller** und **Modell**, die mit aus den DMI-Informationen der Hardware ermittelten Werten vorausgefüllt sind. Die Felder können auch angepasst und ein zusätzlicher **Kommentar** angegeben werden.

Wenn die Übermittlung der Systeminformationen im Rahmen einer Support-Anfrage erfolgt, sollte die Option **Dies bezieht sich auf einen Supportfall** aktiviert werden. Im folgenden Feld kann dann eine Ticketnummer angegeben werden, die die Zuordnung vereinfacht und eine schnellere Bearbeitung ermöglicht.

Nach einem Klick auf **Weiter** wird eine Übersicht der ermittelten Systeminformationen ausgegeben. Außerdem wird ein komprimiertes Tar-Archiv erstellt, das eine Liste mit den im System verwendeten Hardware-Komponenten enthält und über **Archiv mit den Systeminformationen** heruntergeladen werden kann.

Nach einem erneuten Klick auf **Weiter** kann der Übermittlungsweg der Daten an Univention ausgewählt werden. **Hochladen** überträgt die Daten per HTTPS, **Mail senden** führt zu einem Dialog, der die für den Versand nötigen Schritte aufführt.

8.3. Verwaltung der lokalen Systemkonfiguration mit Univention Configuration Registry

Feedback

8.3.1. Einführung

Feedback

Univention Configuration Registry ist das zentrale Werkzeug zur Verwaltung der lokalen Systemkonfiguration eines UCS-basierten Systems. Ein direktes Editieren der Konfigurationsdateien ist dabei in der Regel nicht nötig.

Einstellungen werden in einem Registrierungsmechanismus in einem einheitlichen Format festgelegt, den sogenannten *Univention Configuration Registry-Variablen*. Diese Variablen werden verwendet, um aus Kon-

figurationsdatei-Vorlagen (den sogenannten *Univention Configuration Registry-Templates*) die effektiv von den Diensten/Programmen verwendeten Konfigurationsdateien zu generieren.

Dieses Verfahren bietet eine Reihe von Vorteilen:

- In der Regel müssen keine Konfigurationsdateien manuell editiert werden. Dies vermeidet Fehler durch ungültige Syntax von Konfigurationseinstellungen o.ä.
- Es existiert ein einheitliches Interface zum Editieren der Einstellungen und die unterschiedlichen Syntaxformate der Konfigurationsdateien werden vor dem Administrator verborgen.
- Die Einstellungen werden von der eigentlichen Konfigurationsdatei entkoppelt, d.h. wenn eine Software in einer neuen Version ein anderes Konfigurationsformat verwendet, wird einfach ein neues Template im neuen Format ausgeliefert anstatt eine aufwendige und fehlerträchtige Konvertierung der bestehenden Konfigurationsdatei vorzunehmen.
- Die in einer durch Univention Configuration Registry verwalteten Konfigurationsdatei verwendeten Variablen werden intern zugeordnet. Das stellt sicher, dass beim Ändern einer UCR-Variable alle Konfigurationsdateien, auf die sich die veränderte Variable bezieht, neu erstellt werden.

Univention Configuration Registry-Variablen können auf der Kommandozeile über den Befehl `univention-config-registry` (Kurzform: `ucr`) oder über das UMC-Modul **Univention Config Registry** konfiguriert werden.

Da die meisten Pakete ihre Konfiguration über Univention Configuration Registry durchführen und bei der Installation entsprechende Grundeinstellungen eingerichtet werden, sind nach der Installation eines UCS-Systems bereits einige Hundert Univention Configuration Registry-Variablen gesetzt.

UCR-Variablen können auch effizient in Shell-Skripten verwendet werden, um auf Systemeinstellungen wie den Rechnernamen zuzugreifen.

Die Benennung der Variablen folgt einer baumartigen Struktur, wobei ein Schrägstrich als Trennzeichen von Namensbestandteilen verwendet wird. Beispielsweise handelt es sich bei allen mit `ldap` beginnenden Univention Configuration Registry-Variablen um Einstellungen, die den lokalen Verzeichnisdienst betreffen.

Zu den meisten Variablen ist eine Beschreibung hinterlegt, die die Verwendung und Funktion erläutert.

Wenn eine Konfigurationsdatei durch ein UCR-Template verwaltet wird und die gewünschte Einstellung nicht bereits durch eine vorhandene Variable abgedeckt ist, muss statt der Konfigurationsdatei das UCR-Template erweitert werden. Würde die Konfigurationsdatei direkt angepasst, würde bei der nächsten Neugenerierung der Datei - z.B. beim Setzen einer registrierten UCR-Variable - die lokale Anpassung wieder überschrieben. Die Anpassung von UCR-Templates ist in Abschnitt 8.3.5 beschrieben.

Ein Teil der über Univention Configuration Registry konfigurierten Einstellungen sind systemspezifisch (z.B. der Rechnername), viele Eigenschaften können jedoch auch auf mehrere Rechner angewendet werden. Mithilfe der *Univention Configuration Registry-Richtlinie* in den UMC-Modulen zur Domänenverwaltung können Variablen zusammengefasst und auf mehr als einen Rechner angewendet werden.

Die Auswertung der Univention Configuration Registry-Variablen auf einem UCS-System erfolgt vierstufig:

- Als Erstes werden lokale Univention Configuration Registry-Variablen ausgewertet.
- Die lokalen Variablen werden von Richtlinien-Variablen überstimmt, die aus dem Verzeichnisdienst bezogen werden.
- Die Option `--schedule` dient zum Setzen lokaler Variablen, die nur für einen gewissen Zeitraum gelten sollen. Diese Ebene der Univention Configuration Registry ist reserviert für lokale Einstellungen, die durch zeitgesteuerte Mechanismen in Univention Corporate Server automatisiert vorgenommen werden.

- Durch Verwendung der Option `--force` beim Setzen einer lokalen Variable werden aus den Verzeichnisdienst übernommene Einstellung ebenso wie Variablen der Schedule-Ebene überstimmt und statt dessen der angegebene Wert für das lokale System festgelegt. Beispiel:

```
univention-config-registry set --force mail/messagesizelimit=1000000
```

Wird eine Variable gesetzt, die durch eine übergeordnete Richtlinie überschrieben wird, erscheint eine Warnmeldung.

Die Verwendung der Univention Configuration Registry-Richtlinie ist in Abschnitt 8.3.4 dokumentiert.

8.3.2. Verwendung des Web-Interface in Univention Management Console

Feedback

Über das Modul **Univention Configuration Registry** von Univention Management Console können die Variablen eines Systems angezeigt und verändert werden, außerdem besteht die Möglichkeit über **Hinzufügen** neue Variablen zu setzen.

Auf der Startseite wird eine Suchmaske angezeigt. Alle Variablen sind anhand einer **Kategorie** klassifiziert, etwa alle LDAP-bezogenen Einstellungen.

In der Suchmaske kann als Filter das **Suchattribut** angegeben werden, das sich auf den Variablennamen, den Wert oder die Beschreibung beziehen kann.

Nach erfolgter Suche werden die gefundenen Variablen in einer Tabelle angezeigt, dabei wird der Variablenname und der Wert angezeigt. Bewegt man den Mauszeiger auf den Variablennamen, wird eine weiterführende Beschreibung der Variable angezeigt.

Mit einem Klick auf das Icon mit dem stilisierten Stift wird die Einstellung einer Variable bearbeitet. Das Icon mit dem stilisierten Minuszeichen erlaubt das Löschen einer Variable.

8.3.3. Verwendung des Kommandozeilenfrontends

Feedback

Das Kommandozeileninterface von Univention Configuration Registry wird über den Befehl `univention-config-registry` aufgerufen. Alternativ kann auch die Kurzform `ucr` verwendet werden.

8.3.3.1. Abfrage einer UCR-Variable

Feedback

Eine einzelne Univention Configuration Registry-Variable kann mit dem Aufrufparameter `get` ausgelesen werden:

```
univention-config-registry get ldap/server/ip
```

Mit dem Aufrufparameter `dump` können auch alle aktuell gesetzten Variablen ausgegeben werden:

```
univention-config-registry dump
```

8.3.3.2. Setzen von UCR-Variablen

Feedback

Mit dem Aufrufparameter `set` kann eine Variable gesetzt werden. Der Name der Variable kann frei gewählt werden, darf aber ausschließlich aus Buchstaben, Punkten, Zahlen, Binde- und Schrägstrichen bestehen.

```
univention-config-registry set VARIABLENNAME=WERT
```

Ist die Variable schon vorhanden, wird der Inhalt aktualisiert. Ansonsten wird ein neuer Eintrag angelegt.

Beim Setzen einer Univention Configuration Registry-Variable erfolgt keine Syntaxprüfung. Die Änderung einer Variable bewirkt, dass alle Konfigurationsdateien, für die diese Variable registriert ist, unmittelbar neu geschrieben werden. Die betroffenen Dateien werden auf der Kommandozeile ausgegeben.

Dabei ist zu beachten, dass beim Setzen einer UCR-Variable zwar die Konfiguration eines Dienstes aktualisiert wird, der entsprechende Dienst aber nicht automatisch neu gestartet wird! Der Neustart muss manuell erfolgen.

Gleichzeitige Änderungen mehrerer Variablen in einer Befehlszeile sind möglich. Wenn sich diese auf ein- und dieselbe Konfigurationsdatei beziehen, wird diese nur einmal neu geschrieben:

```
univention-config-registry set \
    dns/forwarder1=192.0.2.2 \
    sshd/xforwarding="no" \
    sshd/port=2222
```

Auch ein bedingtes Setzen ist möglich. Soll z.B. ein Wert nur dann in einer Univention Configuration Registry-Variable gespeichert werden, wenn die Variable noch nicht vorhanden ist, kann dies durch ein Fragezeichen statt des Gleichheitszeichens beim Zuweisen des Wertes erreicht werden:

```
univention-config-registry set dns/forwarder1?192.0.2.2
```

8.3.3.3. Suche nach Variablen und gesetzten Werten

Feedback

Mit dem Parameter `search` kann nach einer Variable gesucht werden. Dieser Befehl sucht nach Variablennamen, welche die Zeichenkette *nscd* enthalten und gibt diese mit den aktuellen Belegungen aus:

```
univention-config-registry search nscd
```

Es kann alternativ auch nach gesetzten Variablen-Werten gesucht werden. Dieser Aufruf sucht nach allen Variablen, die auf `master.example.com` gesetzt sind:

```
univention-config-registry search --value master.example.com
```

Bei der Suche können auch Suchmuster in Form von regulären Ausdrücken verwendet werden. Das vollständige Format ist unter https://docs.python.org/2/library/re.html dokumentiert.

8.3.3.4. Löschen von UCR-Variablen

Feedback

Mit dem Aufrufparameter `unset` kann eine Variable entfernt werden. Das folgende Beispiel löscht die Variable `dns/forwarder2`. Auch hier können mehrere zu löschende Variablen übergeben werden:

```
univention-config-registry unset dns/forwarder2
```

8.3.3.5. Neuerzeugung von Konfigurationsdateien aus ihrem Template

Feedback

Mit dem Aufrufparameter `commit` wird eine Konfigurationsdatei aus ihrem Template neu erzeugt. Der Name der Konfigurationsdatei ist als Parameter anzugeben, z.B.:

```
univention-config-registry commit /etc/samba/smb.conf
```

Da UCR-Templates beim Editieren von UCR-Variablen in der Regel automatisch neu erzeugt werden, wird dies vor allem für Tests verwendet.

Wird beim Aufruf von `ucr commit` kein Dateiname angegeben, werden sämtliche durch Univention Configuration Registry verwalteten Dateien neu aus den Vorlagen erzeugt. In der Regel sollte es allerdings nicht notwendig sein, alle Konfigurationsdateien neu zu erzeugen.

8.3.3.6. Übernahme von Variablen in Shell-Skripte

Feedback

Über den Aufrufparameter `shell` werden Univention Configuration Registry-Variablen und ihre aktuellen Belegungen in einem Format ausgegeben, das in Shell-Skripten verwendet werden kann:

```
univention-config-registry shell ldap/server/name
```

Dabei werden verschiedene Konvertierungen vorgenommen: Schrägstriche in Variablennamen werden durch Unterstriche ersetzt und in den Werten enthaltene Zeichen, die in Shell-Skripten eine besondere Bedeutung haben, werden durch Anführungszeichen geschützt.

Damit Univention Configuration Registry-Variablen als Umgebungsvariablen in einem Shell-Skript eingelesen werden, muss die Ausgabe von Univention Configuration Registry durch den Befehl `eval` ausgeführt werden:

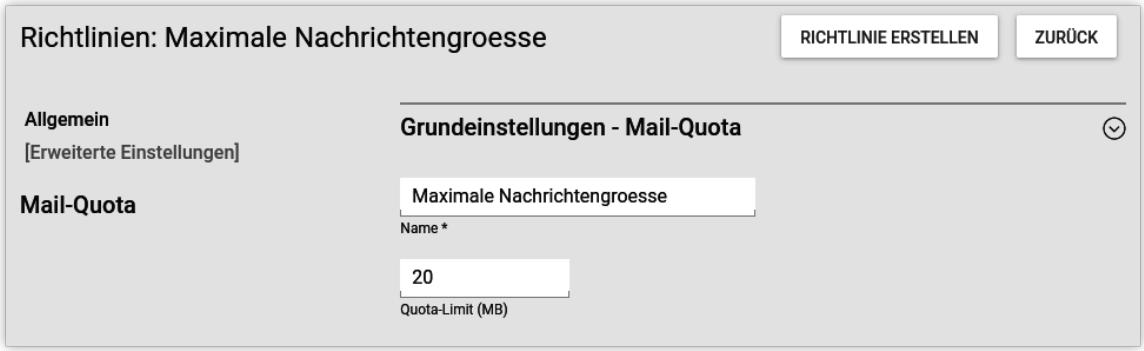
```
# eval "$(univention-config-registry shell ldap/server/name)"
# echo "$ldap_server_name"
master.firma.de
```

8.3.4. Richtlinienbasierte Konfiguration von UCR-Variablen

Feedback

Ein Teil der über Univention Configuration Registry konfigurierten Einstellungen sind systemspezifisch (z.B. der Rechnername), viele Eigenschaften können jedoch auch auf mehrere Rechner angewendet werden. Mithilfe der im **Richtlinien**-Modul von Univention Management Console verwalteten **Univention Configuration Registry**-Richtlinie können Variablen zusammengefasst und auf mehr als einen Rechner angewendet werden.

Abbildung 8.6. Konfiguration der maximalen Mailgröße über eine Richtlinie



Zuerst muss für die anzulegende Richtlinie ein **Name** gesetzt werden, unter dem die Variablen später einzelnen Rechner-Objekten zugewiesen werden können.

Außerdem muss mindestens eine **Variable** konfiguriert und ein **Wert** zugewiesen werden.

Diese Richtlinie kann dann einem Rechner-Objekt oder einem Container/OU zugewiesen werden (siehe Abschnitt 4.6.2). Es ist zu beachten, dass die Auswertung der konfigurierten Werte gegenüber den übrigen Richtlinien abweicht: Die Werte werden nicht direkt auf die Rechner übertragen, sondern durch Univention Directory Policy auf den zugewiesenen Rechner geschrieben. Das dabei verwendete Zeitintervall wird durch die Univention Configuration Registry-Variable `ldap/policy/cron` konfiguriert und erfolgt standardmäßig stündlich.

8.3.5. Anpassung von UCR-Templates

Feedback

Ein Univention Configuration Registry-Template ist im im einfachsten Fall eine Kopie der ursprünglichen Konfigurationsdatei, in der die Stellen, an denen der Wert einer Variable verwendet werden soll, eine Referenz auf den Variablennamen enthalten.

Für komplexere Szenarien kann auch Inline-Python-Code integriert werden, der dann auch komplexere Konstrukte wie etwa bedingte Abfragen erlaubt.

Anmerkung

Univention Configuration Registry-Templates sind in den entsprechenden UCS-Software-Paketen als Konfigurationsdateien enthalten. Bei der Aktualisierung von Paketen wird überprüft, ob Änderungen an Konfigurationsdateien vorgenommen wurden. Wenn Konfigurationsdateien nicht mehr im Auslieferungszustand vorliegen, werden diese nicht überschrieben. Stattdessen wird eine neue Version im selben Verzeichnis mit der Endung `.debian.dpkg-new` abgelegt. Sollen Änderungen an Univention Configuration Registry-Templates vorgenommen werden, werden diese Templates bei der Aktualisierung ebenfalls nicht überschrieben und im selben Verzeichnis mit der Endung `.dpkg-new` oder `.dpkg-dist` abgelegt. Entsprechenden Hinweise werden in die Log-Datei `/var/log/univention/updater.log` geschrieben. Dies tritt nur auf, wenn UCR-Templates lokal angepasst werden.

Die UCR-Templates werden im Verzeichnis `/etc/univention/templates/files/` abgelegt. Der Pfad zu den Vorlagen entspricht dem absoluten Pfad zu der Konfigurationsdatei mit vorangestelltem Pfad zum Vorlagenverzeichnis. So findet sich zum Beispiel die Vorlage für die Konfigurationsdatei `/etc/issue` unter `/etc/univention/templates/files/etc/issue`.

Damit Konfigurationsdateien von Univention Configuration Registry korrekt verarbeitet werden können, müssen sie im UNIX-Format vorliegen. Werden Konfigurationsdateien z.B. unter DOS oder Windows bearbeitet, werden Steuerzeichen zur Kennzeichnung des Zeilenumbruchs eingefügt, die die Verwendung der Datei durch Univention Configuration Registry stören.

8.3.5.1. Referenzierung von UCR-Variablen in Templates

Feedback

Im einfachsten Fall kann eine UCR-Variable im Template direkt referenziert werden. Als Platzhalter dient der Variablenname, der von der Zeichenkette `@%@` eingefasst wird. Als Beispiel die Option für die Aktivierung von X11-Forwarding in der Konfigurationsdatei `/etc/ssh/sshd_config` des OpenSSH-Servers:

```
X11Forwarding @%@sshd/xforwarding@%@
```

Neu eingefügte Referenzen auf UCR-Variablen werden automatisch von Templates ausgewertet, eine zusätzliche Registrierung ist nur bei der Verwendung von Inline-Python-Code nötig (siehe Abschnitt 8.3.5.2).

8.3.5.2. Integration von Inline-Python-Code in Templates

Feedback

In UCR-Templates kann beliebiger Python-Code eingebettet werden, in dem ein von der Zeichenkette `@!@` eingefasster Codeblock eingefügt wird. Mit solchen Blöcken können z.B. bedingte Abfragen umgesetzt werden, so dass beim Ändern eines Parameters über eine Variable weitere abhängige Einstellungen automatisch in die Konfigurationsdatei aufgenommen werden. Folgende Code-Sequenz konfiguriert beispielsweise Netzwerk-Einstellungen anhand der Univention Configuration Registry-Einstellungen:

```
@!@
if configRegistry.get('apache2/ssl/certificate'):
    print 'SSLCertificateFile %s' % \
        configRegistry['apache2/ssl/certificate']
@!@
```

Alle mit der print-Funktion ausgegebenen Daten werden dabei in die generierte Konfigurationsdatei geschrieben. Die in Univention Configuration Registry gespeicherten Daten können über das `ConfigRegistry`-Objekt abgefragt werden, z.B.:

```
@!@
if configRegistry.get('version/version') and \
        configRegistry.get('version/patchlevel'):
    print 'UCS %(version/version)s-%(version/patchlevel)s' % \
        configRegistry
@!@
```

Im Gegensatz zu direkt referenzierten UCR-Variablen (siehe Abschnitt 8.3.5.1) müssen Variablen, auf die in Inline-Python-Code zugegriffen wird, explizit registriert werden.

Die in Konfigurationsdateien verwendeten Univention Configuration Registry-Variablen werden unterhalb des Verzeichnisses `/etc/univention/templates/info/` in *info*-Dateien registriert, die in der Regel nach dem Paketnamen mit der Dateiendung `.info` benannt werden. Wird neuer Python-Code in die Vorlagen eingefügt oder bestehender Code so verändert, dass er zusätzliche oder andere Variablen nutzt, so muss einer der bestehenden `.info`-Dateien modifiziert oder eine neue hinzugefügt werden.

Nach der Änderung von `.info`-Dateien muss der Befehl `ucr update` aufgerufen werden.

8.4. Basis-Systemdienste

Feedback

Dieser Abschnitt beschreibt grundlegende System-Dienste einer UCS-Installation, wie etwa die Konfiguration der Authentifizierungs-Schnittstelle PAM, des System-Loggings und des NSCD.

8.4.1. Administrativer Zugriff mit dem Root-Konto

Feedback

Für den administrativen Vollzugriff existiert auf jedem UCS-System das `root`-Konto. Das Passwort wird beim Installieren des Systems festgelegt. Der root-Benutzer wird nicht im LDAP-Verzeichnis gespeichert, sondern in den lokalen Benutzerkonten.

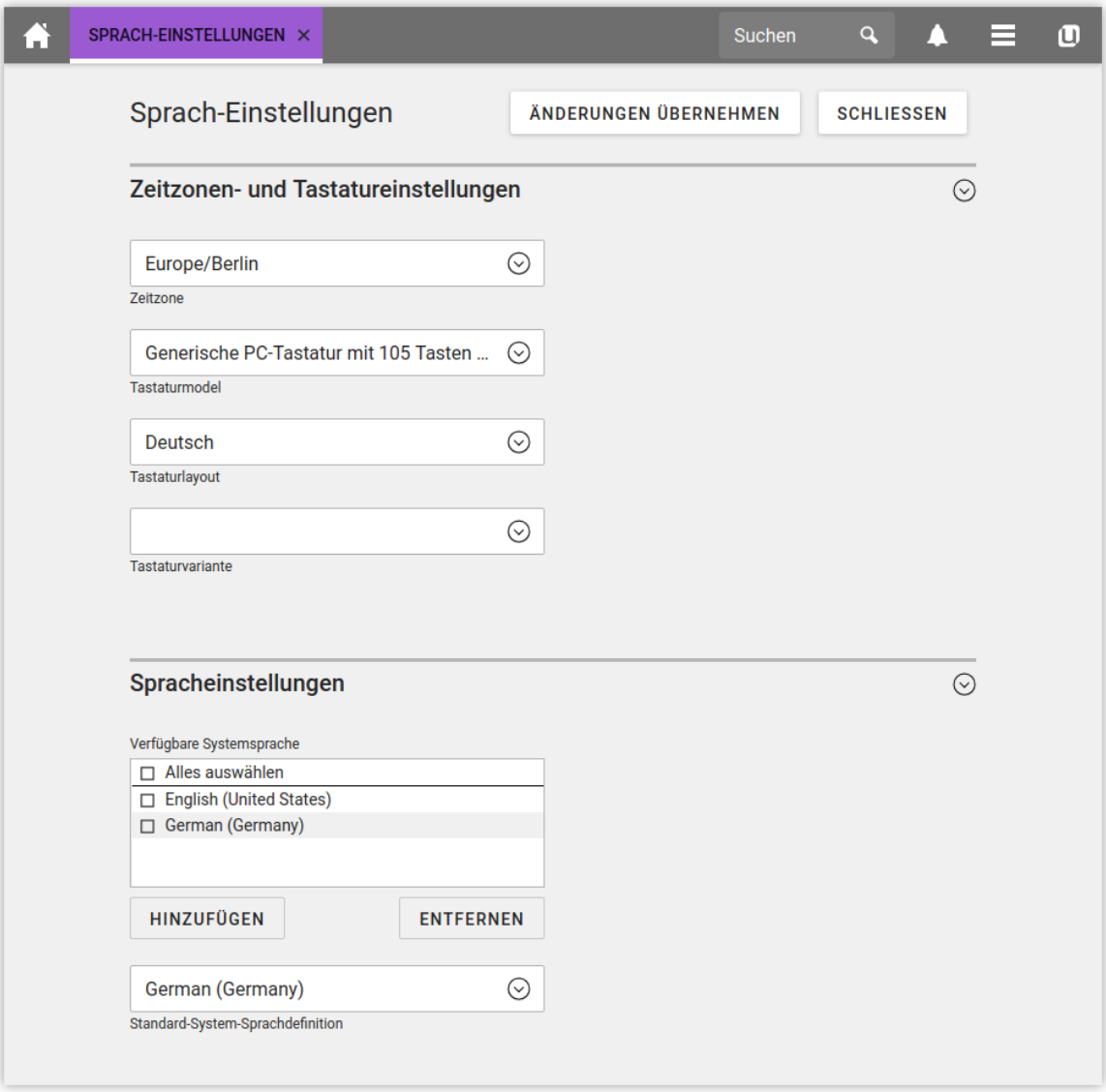
Das Passwort für den lokalen root-Nutzer kann über die Kommandozeile mit den Befehl `passwd` geändert werden. Es ist zu beachten, dass hierbei keine Prüfungen hinsichtlich der Passwortlänge/-Stärke und bereits verwendeter Passwörter durchgeführt wird.

8.4.2. Konfiguration der Sprach- und Tastatur-Einstellungen

Feedback

Unter Linux werden Lokalisierungseigenschaften für Software in *Locales* definiert. Konfiguriert werden u.a. Einstellungen wie Datums- sowie zu nutzende Währungsformate, verwendete Zeichensätze und die Sprachauswahl für internationalisierte Programme. Die installierten Locales können in Univention Management Console unter **Sprach-Einstellungen -> Verfügbare Systemsprachen** geändert werden. Unter **Standard-System-Sprachdefinition** wird die Standard-Locale festgelegt.

Abbildung 8.7. Konfiguration der Spracheinstellungen



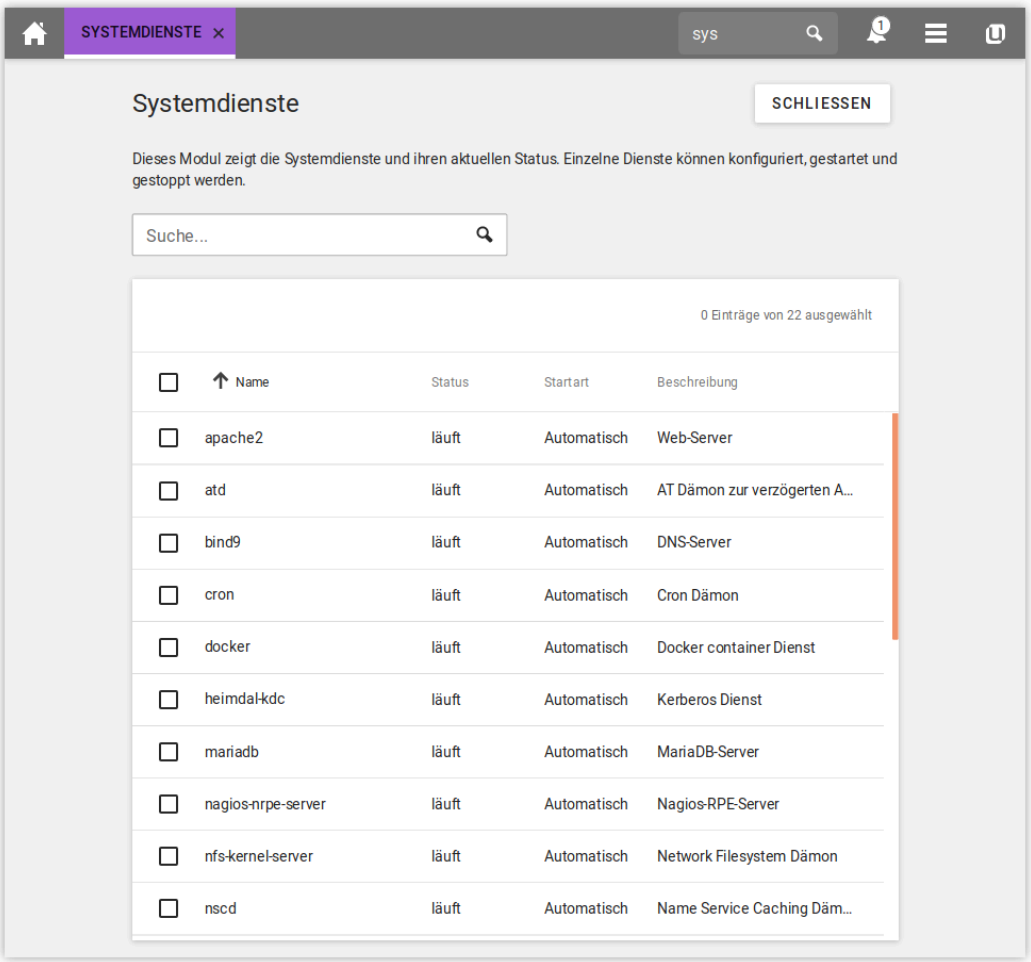
Das **Tastaturlayout** im Menüpunkt **Zeitzonen- und Tastatureinstellungen** greift bei lokalen Anmeldungen an dem Rechner.

8.4.3. Starten/Stoppen von Systemdiensten / Konfiguration des automatischen Starts

Feedback

Mit dem UMC-Modul **Systemdienste** kann der aktuelle Status eines Systemdienstes geprüft und dieser ggf. gestartet oder gestoppt werden.

Abbildung 8.8. Übersicht der Systemdienste



In der Liste aller auf dem System installierten Dienste ist unter **Status** der aktuelle Laufzeitstatus und eine **Beschreibung** aufgeführt. Unter **mehr** kann der Dienst gestartet, gestoppt oder neu gestartet werden.

In der Grundeinstellung wird jeder Dienst automatisch beim Systemstart gestartet. In einigen Fällen kann es sinnvoll sein, den Dienst nicht direkt zu starten, sondern z.B. erst nach Konfiguration weiterer Einstellungen. Mit der Aktion **Manuell starten** wird der Dienst nicht beim Systemstart automatisch gestartet, kann aber nachträglich gestartet werden. Mit der Aktion **Niemals starten** wird auch der nachträgliche Start unterbunden.

8.4.4. Authentifizierung / PAM

Feedback

Authentifizierungs-Dienste werden in Univention Corporate Server durch *Pluggable Authentication Modules* (PAM) realisiert. Dabei werden unterschiedliche Anmeldeverfahren auf eine gemeinsame Schnittstelle abgebildet, so dass eine neue Anmeldemethode keine Anpassungen an bestehenden Applikationen benötigt.

8.4.4.1. Anmeldebeschränkungen für ausgewählte Benutzer

Feedback

In der Grundeinstellung können sich nur der `root`-Benutzer und Mitglieder der Gruppe `Domain Admins` remote über SSH und lokal auf einem `tty` anmelden.

Diese Einschränkung kann mit der Univention Configuration Registry-Variable `auth/DIENST/restrict` konfiguriert werden. Der Zugriff auf diesen Dienst kann durch Setzen der Variablen `auth/`

`DIENST/user/BENUTZERNAME` und `auth/DIENST/group/GRUPPENNAME` auf `yes` freigegeben werden.

Anmeldebeschränkungen werden unterstützt für SSH (`sshd`), FTP (`ftp`), die Anmeldung am Login-Manager KDM (`kdm`), Anmeldung an einem `tty` (`login`), `rlogin` (`rlogin`), PPP (`ppp`) und andere Dienste (`other`). Ein Beispiel für SSH:

```
auth/sshd/group/Administrators: yes
auth/sshd/group/Computers: yes
auth/sshd/group/DC Backup Hosts: yes
auth/sshd/group/DC Slave Hosts: yes
auth/sshd/group/Domain Admins: yes
auth/sshd/restrict: yes
```

8.4.5. Konfiguration des verwendeten LDAP-Servers

Feedback

In einer UCS-Domäne können mehrere LDAP-Server betrieben werden. Der primär verwendete wird mit der Univention Configuration Registry-Variable `ldap/server/name` festgelegt, weitere Server können über die Univention Configuration Registry-Variable `ldap/server/addition` angegeben werden.

Alternativ können die LDAP-Server auch über die Richtlinie **LDAP-Server** in der UMC-Rechnerverwaltung festgelegt werden. Die Reihenfolge der Server bestimmt die Reihenfolge der Anfragen des Rechners an die Server, falls ein LDAP-Server nicht erreichbar sein sollte.

In der Grundeinstellung ist nach Installation/Domänenbeitritt nur `ldap/server/name` gesetzt. Ist mehr als ein LDAP-Server vorhanden, ist es empfehlenswert zur Verbesserung der Ausfallsicherung min. zwei LDAP-Server über die **LDAP-Server**-Richtlinie zuzuweisen. Bei einer auf mehrere Standorte verteilten Umgebung sollte darauf geachtet werden möglichst LDAP-Server aus dem lokalen Netz vorzugeben.

8.4.6. Konfiguration des verwendeten Druckservers

Feedback

Der zu verwendende Druckserver kann mit der Univention Configuration Registry-Variable `cups/server` festgelegt werden.

Alternativ kann der Server auch über die Richtlinie **Druckserver** in der UMC-Rechnerverwaltung festgelegt werden.

8.4.7. Protokollierung/Abfrage von Systemmeldungen und -zuständen

Feedback

8.4.7.1. Logdateien

Feedback

Alle UCS-spezifischen Logdateien (z.B. für die Listener/Notifier-Replikation) werden im Verzeichnis `/var/log/univention/` abgelegt. Serverdienste protokollieren in ihre jeweilige Standard-Logdateien; Apache beispielsweise in die Datei `/var/log/apache2/error.log`.

Die Logdateien werden durch logrotate verwaltet. Es sorgt dafür, dass Logdateien in einem Intervall (konfigurierbar in Wochen über die Univention Configuration Registry-Variable `log/rotate/weeks`, standardmäßig 12) fortlaufend benannt werden und ältere Logdateien anschließend gelöscht werden. Die aktuelle Logdatei für den Univention Directory Listener findet sich beispielsweise in der Datei `listener.log`, die der Vorwoche in `listener.log.1` usw.

Alternativ können Logdateien auch erst beim Erreichen einer bestimmten Größe rotiert werden. Soll beispielsweise erst ab einer Größe von 50 MB rotiert werden, kann dazu die Univention Configuration Registry-Variable `logrotate/rotates` auf `size 50M` gesetzt werden.

Über die Univention Configuration Registry-Variable `logrotate/compress` kann konfiguriert werden, ob die älteren Logdateien zusätzlich mit `gzip` komprimiert werden sollen.

8.4.7.2. Protokollierung des Systemzustands

Feedback

Mit `univention-system-stats` kann der aktuelle Systemzustand in die Datei `/var/log/univention/system-stats.log` protokolliert werden. Protokolliert werden dabei folgende Werte:

- Der freie Speicherplatz auf den Systempartitionen (`df -lhT`)
- Die aktuelle Prozessliste (`ps auxf`)
- Zwei `top`-Aufstellungen der aktuellen Prozesse und Auslastung (`top -b -n2`)
- Den aktuell freien Arbeitsspeicher (`free`)
- Die Zeit, die seit dem Start des Systems vergangen ist (`uptime`)
- Temperatur-, Lüfter- und Spannungskennzahlen aus lm-sensors (`sensors`)
- Eine Aufstellung der aktuellen Samba-Verbindungen (`smbstatus`)

Die Laufzeiten in denen der Systemzustand protokolliert werden soll, können durch die Univention Configuration Registry-Variable `system/stats/cron` in Cron-Syntax definiert werden, z.B. `0,30 * * * *` für eine Protokollierung jeweils zu jeder vollen und halben Stunde. Die Protokollierung wird durch Setzen der Univention Configuration Registry-Variable `system/stats` auf `yes` aktiviert und ist bei Neuinstallationen ab UCS 3.0 die Grundeinstellung.

8.4.7.3. Anzeige von Systemstatistiken in Univention Management Console

Feedback

Das UMC-Modul **Statistiken** zeigt die Auslastung des Systems an. Dabei wird jeweils eine Grafik für die unterschiedlichen Zeiträume angezeigt:

- Die letzten 24 Stunden
- Die vergangene Woche
- Der vergangene Monat
- Das vergangene Jahr

Folgende Systeminformationen werden protokolliert:

- Die Auslastung des Hauptspeichers in Prozent
- Die Prozessor-Auslastung des Systems
- Die Anzahl der jeweils aktiven Terminalserver-Sitzungen
- Die Auslastung der Auslagerungsdatei (Swap)

8.4.7.4. Prozessübersicht in Univention Management Console

Feedback

Das UMC-Modul **Prozessübersicht** zeigt eine Tabelle der aktuellen Prozesse auf dem System an. Die Prozesse können nach den folgenden Eigenschaften sortiert werden, in dem auf den entsprechenden Tabellenkopf geklickt wird:

- Die CPU-Nutzung in Prozent

- Der Benutzername, unter dem der Prozess läuft
- Speicherverbrauch in Prozent
- Die Prozess-ID

Unter dem Menüpunkt **mehr** können Prozesse beendet werden. Hierbei werden zwei Arten der Terminierung unterschieden:

- Die Aktion **Beenden** schickt dem Prozess eine Benachrichtigung vom Typ `SIGTERM`, dies ist der Regelfall bei der kontrollierten Beendigung von Programmen.
- In Einzelfällen kann es vorkommen, dass sich ein Programm - z.B. nach einem Absturz - nicht mehr über dieses Verfahren beenden lässt. In diesem Fall kann mit der Aktion **Beenden erzwingen** das Signal `SIGKILL` geschickt werden um den Prozess forciert zu beenden.

Das Beenden über `SIGTERM` ist in der Regel vorzuziehen, da viele Programme dann einen kontrollierten Programmabbruch einleiten und z.B. ein Speichern von Dateien o.ä. durchführen.

8.4.7.5. System-Fehlerdiagnose in Univention Management Console

Feedback

Um ein UCS-System auf verschiedene bekannte Probleme hin zu analysieren bietet das UMC-Modul **System-Fehlerdiagnose** eine entsprechende Benutzerschnittstelle.

Das Modul wertet eine Reihe ihm bekannter Problemszenarien aus und bietet Lösungsvorschläge an, wenn es in der Lage ist gefundene Probleme automatisch zu beheben. Diese Funktion wird durch zusätzliche Schaltflächen dargestellt. Darüber hinaus werden Links zu weiterführenden Artikeln und zu entsprechenden UMC-Modulen angezeigt.

8.4.8. Ausführen von wiederkehrenden Aktionen mit Cron

Feedback

Regelmäßig wiederkehrende Aktionen (wie z.B. das Verarbeiten von Logdateien) können mit dem Cron-Dienst zu einem definierten Zeitpunkt gestartet werden. Eine solche Aktion bezeichnet man auch als Cron-Job.

8.4.8.1. Stündliches/tägliches/wöchentliches/monatliches Ausführen von Skripten

Feedback

Auf jedem UCS-System sind vier Verzeichnisse vordefiniert, `/etc/cron.hourly/`, `/etc/cron.daily/`, `/etc/cron.weekly/` und `/etc/cron.monthly/`. Shell-Skripte, die in diesen Verzeichnissen abgelegt werden und als ausführbar markiert sind, werden automatisch stündlich, täglich, wöchentlich oder monatlich ausgeführt.

8.4.8.2. Definition eigener Cron-Jobs in `/etc/cron.d/`

Feedback

Ein Cron-Job wird in einer Zeile definiert, die aus insgesamt sieben Spalten aufgebaut ist:

- Minute (0-59)
- Stunde (0-23)
- Tag (1-31)
- Monat (1-12)
- Wochentag (0-7) (0 und 7 stehen dabei für den Sonntag)
- Name des ausführenden Benutzers (z.B. root)
- Der auszuführende Befehl

Die Zeitangaben können dabei in verschiedenen Formaten vorgenommen werden. Es kann entweder eine konkrete Minute/Stunde/etc. vorgegeben werden oder mit einem * eine Aktion zu jeder Minute/Stunde/etc. ausgeführt werden. Es können auch Intervalle definiert werden, */2 führt als Minutenangabe beispielsweise dazu, dass eine Aktion jede zweite Minute ausgeführt wird.

Einige Beispiele:

```
30 * * * * root /usr/sbin/jitter 600 /usr/share/univention-samba/slave-
sync
*/5 * * * * www-data /usr/bin/php -q /usr/share/horde/reminders.php
```

8.4.8.3. Definition eigener Cron-Jobs in Univention Configuration Registry

Feedback

Cron-Jobs können auch in Univention Configuration Registry definiert werden. Das ist besonders nützlich, wenn sie über eine Univention Directory Manager-Richtlinie gesetzt und somit auf mehr als einen Rechner angewendet werden.

Jeder Cron-Job setzt sich dabei aus min. zwei Univention Configuration Registry-Variablen zusammen. *JOB-NAME* ist dabei ein allgemeiner Bezeichner.

- `cron/JOBNAME/command` legt den auszuführenden Befehl fest (Angabe erforderlich)
- `cron/JOBNAME/time` setzt die Ausführungszeit fest (siehe Abschnitt 8.4.8.2) (Angabe erforderlich)
- Standardmäßig wird der Cron-Job als Benutzer `root` ausgeführt. Mit `cron/JOBNAME/user` kann ein abweichender Benutzer angegeben werden.
- Wird unter `cron/JOBNAME/mailto` eine Email-Adresse hinterlegt, wird die Ausgabe des Cron-Jobs per Email dorthin gesendet.
- Mit `cron/JOBNAME/description` kann eine Beschreibung hinterlegt werden.

8.4.9. Name Service Cache Daemon

Feedback

Um häufige Anfragen unveränderter Daten zu beschleunigen, werden Namensauflösungen durch den *Name Service Cache Daemon* (NSCD) zwischengespeichert. Werden diese erneut angefragt, muss so nicht eine vollständige neue LDAP-Anfrage durchgeführt werden, sondern die Daten können direkt aus dem Cache bezogen werden.

Die Zwischenspeicherung der Gruppen erfolgt seit UCS 3.1 aus Performance- und Stabilitätsgründen nicht mehr über den NSCD, sondern durch einen lokalen Gruppencache, siehe Abschnitt 7.3.

Die zentrale Konfigurations-Datei des NSCD (`/etc/nscd.conf`) wird durch Univention Configuration Registry verwaltet.

Der Zugriff auf den Cache erfolgt über eine Hash-Tabelle. Die Größe dieser Hash-Tabelle kann über Univention Configuration Registry konfiguriert werden und sollte größer sein als die Anzahl der gleichzeitig verwendeten Benutzer/Rechner. Aus technischen Gründen sollte als Größe der Tabelle eine Primzahl verwendet werden. Die folgende Tabelle führt die Standardwerte der Variablen auf:

Tabelle 8.12. Standardgrößen der NSCD Hash-Tabellen

Variable	Standardgröße der Hash-Tabelle
`nscd/hosts/size`	6007
`nscd/passwd/size`	6007

Bei sehr großen Caches kann es nötig sein, die Größe der Cache-Datenbank im Arbeitsspeicher zu erhöhen. Dies kann mit den Univention Configuration Registry-Variablen `nscd/hosts/maxdbsize` und `nscd/passwd/maxdbsize` konfiguriert werden.

Standardmäßig startet NSCD fünf Threads. In Umgebungen, in denen viele Zugriffe erfolgen, kann es erforderlich sein, die Anzahl durch die Univention Configuration Registry-Variable `nscd/threads` zu erhöhen.

In der Grundeinstellung wird ein aufgelöster Gruppen- oder Rechnername eine Stunde im Cache vorgehalten und ein Benutzername zehn Minuten. Durch die Univention Configuration Registry-Variablen `nscd/hosts/positive_time_to_live` und `nscd/passwd/positive_time_to_live` können diese Zeiträume erweitert oder verringert werden (die Angabe erfolgt in Sekunden).

Gelegentlich kann es nötig sein, den Cache des NSCD manuell zu invalidieren. Die kann individuell pro Cache-Tabelle durch folgende Befehle geschehen:

```
nscd -i passwd
nscd -i hosts
```

Der Detailgrad der Logmeldungen kann mit der Univention Configuration Registry-Variable `nscd/debug/level` konfiguriert werden.

8.4.10. RDP Anmeldung mit XRDP

Feedback

XRDP ist ein auf Univention Corporate Server laufender Dienst, der es Benutzern erlaubt, eine X Sitzung über das Remote Desktop Protocol (RDP)[2] aufzubauen. Das Protokoll wird von Microsoft Windows und vielen anderen Betriebssystemen nativ unterstützt und benötigt damit keine Installation von zusätzlicher Software auf Client PCs.

8.4.10.1. Installation

Feedback

XRDP ist über das App Center (siehe Abschnitt 5.3) verfügbar und kann über das entsprechende Univention Management Console Modul App Center installiert werden, auch auf mehreren Systemen. Nach der Installation läuft ein XRDP Server[3].

8.4.10.2. Konfiguration

Feedback

8.4.10.2.1. Erlaubte Benutzer

Feedback

Standardmäßig dürfen sich alle Benutzer der UNIX Gruppe `Domain Admins` über RDP verbinden. Der Name der Gruppe kann über die Univention Configuration Registry-Variable `xrdp/access/admins` geändert werden.

8.4.10.2.2. Maximale Anzahl gleichzeitiger Sitzungen

Feedback

Die maximale Anzahl gleichzeitiger RDP Sitzungen ist standardmäßig auf `10` beschränkt und kann mit der Univention Configuration Registry-Variable `xrdp/sessions/max` geändert werden.

8.4.10.2.3. Anpassung Anmeldefenster

Feedback

Der Titel und die Bilder im Anmeldefenster können über die Univention Configuration Registry-Variable `xrdp/title` und `xrdp/imagedir` angepasst werden. Das Verzeichnis muss vier Bilddateien im Windows Bitmap Format enthalten. Die ersten beiden werden als rechteckiges Logo an der linken Seite des Eingabefeldes verwendet und die anderen beiden Dateien werden für das Banner genutzt, dass unter dem Eingabefenster angezeigt wird.

[2] https://de.wikipedia.org/wiki/Remote_Desktop_Protocol
[3] http://www.xrdp.org/

`ad24b.bmp`

24 bit farbiges Logo, 140 x 140

`ad256.bmp`

256 farbiges Logo, 140 x 140

`xrdp24b.bmp`

24 bit farbiges Banner, 256 x 192

`xrdp256.bmp`

256 farbiges Banner, 256 x 192

8.4.10.3. Client Software

Feedback

- Microsoft Windows verfügt über einen eingebauten RDP Client. Er zeigt eine Zertifikatswarnung, solange das UCS Zertifikat nicht importiert worden ist.
- UCS und viele andere Linux Distributionen beinhalten rdesktop[4] und FreeRDP[5].
- Für Apple iOS gibt es iResktop[6].
- Für Android gibt es mehrere Apps[7].

8.4.10.4. Bekannte Probleme: Falsches Keyboard Layout

Feedback

Bei der Anmeldung an KDE mit XRDP, wird die Tastatur standardmäßig mit dem US Layout konfiguriert. Um das zu ändern, muss das Startmenü geöffnet und zum **Computer Reiter** gewechselt werden, weiter über die **Systemeinstellungen** zu **Region & Sprachen**. Dort muss das **Tastatur Layout** geöffnet und **Aktiviere Tastaturlayouts** aktiviert werden. Das gewünschte Layout kann anschließend von der Liste der verfügbaren Layouts links ausgewählt werden. Ein Klick auf den rechten Pfeil fügt das Layout hinzu. Die Hoch/Runter Pfeiltasten verändern die Reihenfolge in der rechten Liste der **Aktiven Layouts**. Änderungen anwenden und Applikation schließen. Hintergrundinformationen zu dem Problem finden sich in der Projekt Dokumentation[8].

8.4.10.5. Alternativen

Feedback

VNC

Virtual Network Connect bietet ein einfacheres Protokoll, das zum Beispiel für KVM verwendet wird.

SSH

Bietet standardmäßig nur eine Textkonsole, aber kann für das native Tunneln von X Sitzungen verwendet werden.

8.4.11. SSH-Zugriff auf Systeme

Feedback

Bei der Installation eines UCS-Systems wird in der Vorauswahl ein SSH-Server mitinstalliert. Über SSH können verschlüsselte Verbindungen zu Rechnern durchgeführt werden, wobei auch die Identität eines Rechners

[4] http://www.rdesktop.org/
[5] http://www.freerdp.com/
[6] http://www.irdesktop.com/
[7] https://play.google.com/store/search?q=rdp+client%26c=apps
[8] https://github.com/FreeRDP/FreeRDP/wiki/Keyboard

über eine Prüfsumme sichergestellt werden kann. Wesentliche Aspekte der Konfiguration des SSH-Servers lassen sich über Univention Configuration Registry anpassen:

Standardmäßig ist der Login des privilegierten `root`-Benutzers per SSH erlaubt (etwa um ein neu installiertes System an einem entfernten Standort zu konfigurieren, auf dem noch keine weiteren Benutzer angelegt wurden).

- Wird die Univention Configuration Registry-Variable `sshd/permitroot` auf `without-password` gesetzt, so wird für den `root`-Benutzer keine interaktive Passwort-Abfrage mehr durchgeführt, sondern beispielsweise nur eine Public-Key-basierte Anmeldung, was Brute-Force-Attacken auf Passwörter vermeidet.

- Soll für den `root`-Benutzer überhaupt keine SSH-Anmeldung mehr möglich sein, kann dies durch Setzen der Univention Configuration Registry-Variable `auth/sshd/user/root` auf `no` deaktiviert werden.

Mit der Univention Configuration Registry-Variable `sshd/xforwarding` kann konfiguriert werden, ob eine X11-Ausgabe über SSH weitergeleitet werden soll. Dies ist u.a. nötig, um einem Benutzer die Möglichkeit zu geben durch einen Login mit `ssh -X ZIELRECHNER` ein Programm mit grafischer Ausgabe auf einem entfernten Rechner zu starten. Die möglichen Einstellungen sind `yes` und `no`.

Der Standard-Port für SSH-Verbindungen ist Port 22 über TCP. Wenn ein abweichender Port verwendet werden soll, kann dies über die Univention Configuration Registry-Variable `sshd/port` konfiguriert werden.

8.4.12. Konfiguration der Zeitzone / Zeitsynchronisation

Die Zeitzone, in der ein System angesiedelt ist, kann in Univention Management Console unter **Sprach-Einstellungen -> Zeitzone** geändert werden.

Asynchrone Systemzeiten zwischen den einzelnen Rechnern einer Domäne können die Quelle vielfältiger Fehler bedeuten: Sie verringern beispielsweise die Verlässlichkeit von Log-Dateien, stören den Kerberos-Betrieb und können die korrekte Auswertung von Passwortablaufintervallen stören.

In einer Domäne dient standardmäßig der Domänencontroller Master als Zeitserver. Über die Univention Configuration Registry-Variablen `timeserver`, `timeserver2` und `timeserver3` können externe NTP-Server als Zeitquelle eingebunden werden.

Eine manuelle Zeitsynchronisation kann durch den Befehl `ntpdate` gestartet werden.

Windows-Clients, die in eine Samba 4-Domäne gejoint wurden, akzeptieren nur signierte NTP-Zeitanfragen. Wird die Univention Configuration Registry-Variable `ntp/signed` auf `yes` gesetzt, werden die NTP-Pakete durch Samba 4 signiert.

Kapitel 9. Services für Windows

9.1. Einführung

UCS kann Active Directory (AD) Dienste anbieten, Mitglied einer Active Directory-Domäne sein oder Objekte zwischen Active Directory-Domänen und einer UCS-Domäne synchronisieren.

Aus Sicht von Windows-Systemen kann UCS die Aufgaben von Windows-Serversystemen übernehmen:

- Domänencontrollerfunktionalität / Authentifizierungsdienste
- Dateidienste
- Druckdienste

Alle diese Dienste werden in UCS durch die Software Samba bereitgestellt.

UCS unterstützt zusätzlich die weitgehend automatische Migration einer bestehenden Microsoft Active Directory Domäne zu UCS. Dabei werden alle Benutzer, Gruppen, Rechnerobjekte und Gruppenrichtlinien übernommen ohne das die Windows-Clients erneut der Domäne beitreten müssen. Dies ist in Abschnitt 9.4 beschrieben.

Microsoft Active Directory-Domänencontroller können aktuell nicht einer UCS-Samba-Domäne beitreten. Diese Funktionalität ist zu einem späteren Zeitpunkt geplant.

Samba kann zum jetzigen Zeitpunkt noch nicht einem Active Directory Forest beitreten.

Eingehende Vertrauensstellungen mit anderen Active Directory Domänen sind konfigurierbar. In dieser Konstellation vertraut die externe Active Directory Domäne den Authentifizierungsentscheidungen der UCS-Domäne (Windows vertraut UCS), so dass sich Benutzer auch an Systemen und Active Directory basierten Diensten in der Windows-Domäne anmelden können (siehe Abschnitt 9.5). Ausgehende Vertrauensstellungen mit Active Directory Domänen (UCS vertraut Windows) sind aktuell nicht unterstützt.

Anmerkung

Die Nutzung von UCS als Windows NT-kompatiblen Domänencontroller ist seit UCS 4.3 nicht mehr unterstützt.

9.2. Betrieb einer Samba-Domäne auf Basis von Active Directory

Feedback

9.2.1. Installation

Feedback

Samba als AD-Domänencontroller kann auf allen UCS-Domänencontrollern mit der Applikation *Active Directory-kompatibler Domänencontroller* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-samba4*** installiert werden. Auf den Systemrollen Domänencontroller Master und Domänencontroller Backup muss zusätzlich ***univention-s4-connector*** installiert werden (anschließend muss der Befehl `univention-run-join-scripts` aufgerufen werden). Weitere Informationen finden sich in Abschnitt 5.6.

Ein Samba-Memberserver kann auf UCS-Memberservern mit der Applikation *Windows-kompatibler Fileserver* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepakete ***univention-samba*** installiert werden (anschließend muss der Befehl `univention-run-join-scripts` aufgerufen werden). Weitere Informationen finden sich in Abschnitt 5.6.

Samba unterstützt auch den Betrieb als *read-only domain controller*. Die Einrichtung ist in [ext-doc-win] dokumentiert.

9.2.2. Dienste einer Samba-Domäne

Feedback

9.2.2.1. Authentifizierungsdienst

Feedback

Benutzeranmeldungen können nur auf Microsoft Windows-Systemen erfolgen, die der Samba-Domäne beigetreten sind. Der Domänenbeitritt ist in Abschnitt 3.2.2 dokumentiert.

Benutzer, die sich an einem Windows-System anmelden erhalten bei der Anmeldung ein Kerberos-Ticket, mit dem die weitere Authentifizierung durchgeführt wird. Mit diesem Ticket wird dann auf die Ressourcen der Domäne zugegriffen.

Häufige Fehlerquellen bei fehlschlagenden Anmeldungen sind:

- Für eine funktionierende Kerberos-Authentifizierung ist eine Synchronisation der Systemzeiten zwischen Windows-Client und Domänencontroller zwingend erforderlich. In der Grundeinstellung wird beim Systemstart die Systemzeit über NTP aktualisiert. Dies kann mit dem Befehl `w32tm /resync` auch manuell erfolgen.

- Während der Anmeldung müssen DNS-Service-Records aufgelöst werden. Der Windows-Client sollte daher als DNS-Nameserver die IP-Adresse des Domänencontrollers verwenden.

9.2.2.2. Dateidienste / File-Server

Feedback

Ein Dateiserver stellt zentral benötigte Dateien über das Netz bereit und ermöglicht es unter anderem Benutzerdaten auf einem zentralen Server zu bündeln.

Die in UCS integrierten Dateidienste unterstützen eine Bereitstellung von Freigaben auf Basis von `CIFS`/`SMB` (siehe Kapitel 12). Sofern das unterliegende Dateisystem Access Control Lists (ACLs) unterstützt (verwendbar bei `ext3`, `ext4` und `XFS`) sind ACLs auch von Windows-Clients verwendbar.

Dateidienste können auch mit Samba Active Directory-Domänencontrollern bereitgestellt werden. Generell wird in Samba-Umgebungen - analog zu den Microsoft-Empfehlungen für Active Directory - empfohlen Domänencontroller- und Datei/Druckdienste zu trennen, d.h. Domänencontroller für die Anmeldung und Memberserver für Datei-/Druckdienste zu verwenden. Dies stellt sicher, dass hohe Last auf einem Fileserver nicht zu Störungen im Anmeldedienst führen. Für kleine Umgebungen, in denen keine Möglichkeit für den Betrieb zweier Server gegeben ist, können Datei- und Druckdienste auch mit auf einem Domänencontroller betrieben werden.

Samba unterstützt das `CIFS`-Protokoll und den Nachfolger `SMB2`. Verwendet man einen Client, der `SMB2` unterstützt (ab `Windows Vista`, also auch `Windows 7/8`), verbessert sich die Performance und die Skalierbarkeit.

Das Protokoll kann über die Univention Configuration Registry-Variable `samba/max/protocol` konfiguriert werden. Sie muss auf allen Samba-Servern gesetzt und anschließend der/die Samba-Server neu gestartet werden.

- `NT1` konfiguriert `CIFS` (unterstützt von allen Windows-Versionen)

- `SMB2` konfiguriert `SMB2` (unterstützt ab `Windows Vista`/`Windows 7`)

- `SMB3` konfiguriert `SMB3` (unterstützt ab `Windows 8`)

9.2.2.3. Druckdienste / Print-Server

Feedback

Samba bietet die Möglichkeit, unter Linux eingerichtete Drucker als Netzwerkdrucker für Windows-Clients freizugeben. Die Verwaltung der Druckerfreigaben und die Integration der Druckertreiber ist in Kapitel 13 beschrieben.

Druckdienste können auch mit Samba AD-Domänencontrollern bereitgestellt werden. Hierbei sind die in Abschnitt 9.2.2.2 beschriebenen Einschränkungen zu beachten.

9.2.2.4. Univention S4 Connector

Feedback

Samba stellt einen separaten LDAP-Verzeichnisdienst bereit. Die Synchronisation zwischen dem UCS-LDAP und dem Samba-LDAP erfolgt durch einen internen Systemdienst, den Univention S4 Connector. Der Connector ist standardmäßig auf dem Domänencontroller Master aktiviert und benötigt normalerweise keine weitere Konfiguration.

Hinweise zum Status der Synchronisation finden sich in der Logdatei `/var/log/univention/connector-s4.log`. Weitere Informationen zur Fehleranalyse von eventuellen Connectorproblemen finden sich in SDB 1235.

Mit dem Befehl `univention-s4search` kann im Samba-Verzeichnisdienst gesucht werden. Wird es als Benutzer `root` aufgerufen, werden automatisch die nötigen Credentials des Maschinenkontos verwendet:

```
root@master:~# univention-s4search sAMAccountName=Administrator
# record 1
dn: CN=Administrator,CN=Users,DC=example,DC=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Administrator
instanceType: 4
(..)
```

9.2.2.5. DRS-Replikation der Verzeichnisdaten

Feedback

Samba-AD-Domänen verwenden das Directory Replication System (DRS) zur Replikation der Verzeichnisdaten. DRS erlaubt Multimasterreplikation, d.h. die schreibenden Änderungen mehrerer Domänencontroller werden auf Protokollebene synchronisiert. Die Verwendung von Snapshots in Virtualisierungslösungen sollte daher beim Einsatz von Samba 4 vermieden und Samba 4 auf einem Server betrieben werden, der durchgehend eingeschaltet bleibt.

Mit jedem weiteren Samba-AD-Domänencontroller steigt die Komplexität der Multimasterreplikation. Es sollte daher geprüft werden, ob weitere Samba-AD-Domänencontroller nötig sind oder für neue Server nicht ein Memberserver die bessere Wahl ist.

Hinweise zur Analyse von DRS-Replikationsproblemen finden sich in SDB 1235.

9.2.2.6. Synchronisation der SYSVOL-Freigabe

Feedback

Die SYSVOL-Freigabe ist eine Freigabe, die in Active Directory/Samba Gruppenrichtlinien und Anmeldeskripte bereitstellt. Sie wird zwischen allen Domänencontrollern synchronisiert und im Verzeichnis `/var/lib/samba/sysvol/` gespeichert.

In Microsoft Active Directory wird die SYSVOL-Freigabe durch den File Replication Service (eingeführt mit Windows 2000), bzw. durch das Distributed File System (ab `Windows 2008 R2`) synchronisiert. Diese Replikationsmethoden sind in Samba noch nicht vollständig implementiert. Die Synchronisation zwischen den Samba-Domänencontrollern erfolgt in UCS durch einen Cron-Job (standardmäßig alle fünf Minuten, konfigurierbar durch die Univention Configuration Registry-Variable `samba4/sysvol/sync/cron`.

9.2.3. Konfiguration und Management von Windows-Desktops

Feedback

9.2.3.1. Gruppenrichtlinien

Feedback

9.2.3.1.1. Einführung

Feedback

Gruppenrichtlinien sind eine Active Directory-Funktion, die die zentrale Konfiguration von Vorgaben für Rechner und Benutzer erlaubt. Gruppenrichtlinien werden auch von Samba-AD-Domänen unterstützt. Die Richtlinien greifen nur auf Windows-Clients; Linux- oder Mac OS-Systeme werten die Richtlinien nicht aus.

http://sdb.univention.de/1235
http://sdb.univention.de/1235

Gruppenrichtlinien werden ausgehend von der englischen Bezeichnung *Group policy objects* auch oft als GPOs bezeichnet. Genauer gesagt kann ein Gruppenrichtlinienobjekt eine Reihe von Richtlinien beinhalten. Trotz ihres Namens lassen sich Gruppenrichtlinienobjekte nicht direkt bestimmten Benutzergruppen zuweisen, sondern sie werden vielmehr mit bestimmten AD-Verwaltungseinheiten (Domänen, Sites oder Organisationseinheiten) im Samba-Verzeichnisdienst (Samba DS/AD) verknüpft und beziehen sich dadurch auf untergeordnete Objekte. Eine gruppen- oder benutzerspezifische Auswertung ist nur indirekt über die *Sicherheitseinstellungen* eines Gruppenrichtlinienobjekts möglich, in denen sich das Recht *Gruppenrichtlinie übernehmen* gezielt auf bestimmte Gruppen, Benutzer oder Computer einschränken lässt.

Grundsätzlich sind die *Gruppenrichtlinien* (*Group Policies* (GPO)) von den sehr ähnlich benannten *Gruppenrichtlinieneinstellungen* (*Group Policy Preferences* (GPP)) zu unterscheiden:

- Die über *Gruppenrichtlinien* (GPOs) getroffenen Vorgaben sind bindend, während sich über *Gruppenrichtlinieneinstellungen* (GPPs) nur Präferenzen in die Registry von Windows-Clients eintragen lassen, die aber unter Umständen am Client überschrieben werden können.

- Die über *Gruppenrichtlinien* (GPOs) getroffenen Vorgaben werden zudem dynamisch auf die Zielobjekte angewendet, wo hingegen die über *Gruppenrichtlinieneinstellungen* (GPPs) getroffenen Einstellungen statisch in die Registry von Windows-Clients eintragen werden (man spricht hier auch von Tattooing).

Aus diesen Gründen sind *Gruppenrichtlinien* (GPOs) in den meisten Fällen den *Gruppenrichtlinieneinstellungen* (GPPs) vorzuziehen. Dieses Kapitel bezieht sich im weiteren ausschließlich auf *Gruppenrichtlinien* (GPOs).

Gruppenrichtlinien werden im Gegensatz zu den UCS-Richtlinien (siehe Abschnitt 4.6) nicht in Univention Management Console, sondern mit einem separaten Editor konfiguriert, mit der *Gruppenrichtlinienverwaltung*, die Teil der *Remote Server Administration Tools* (RSAT) ist. Die Einrichtung ist in Abschnitt 9.2.3.1.2 dokumentiert.

Es existieren zwei Arten von Richtlinien:

- *Benutzerrichtlinien* konfigurieren die Einstellungen eines Benutzers, z.B. die Vorkonfiguration des Desktops. Auch Anwendungen können über Gruppenrichtlinien konfiguriert werden (z.B. die Startseite des Microsoft Internet Explorers oder Einstellungen in LibreOffice).

- *Computer-Richtlinien* definieren die Einstellungen von Windows-Clients.

Computerrichtlinien werden erstmals beim Systemstart ausgewertet, Benutzerrichtlinien bei der Anmeldung. Die Richtlinien werden auch für angemeldete Benutzer/laufende Systeme fortlaufend ausgewertet und aktualisiert (in der Grundeinstellung alle 90-120 Minuten, der Zeitraum wird zur Vermeidung von Lastspitzen nach dem Zufallsprinzip variiert).

Die Auswertung der Gruppenrichtlinien kann durch Aufruf des Befehls `gpupdate /force` auch gezielt gestartet werden.

Einige Richtlinien - z.B. zur Installation von Software oder für Anmeldeskripte - werden nur bei der Anmeldung (Benutzerrichtlinien) oder beim Systemstart (Rechnerrichtlinien) ausgewertet.

Die meisten Gruppenrichtlinien setzen nur einen Wert in der Windows-Registry, der dann von Windows oder einer Applikation ausgewertet wird. Da Standardbenutzer keine Einstellungen in dem entsprechenden Teil der Windows Registry editieren können, können so auch eingeschränkte Benutzer-Desktops konfiguriert werden, in denen z.B. Benutzer den Windows Task Manager nicht aufrufen dürfen.

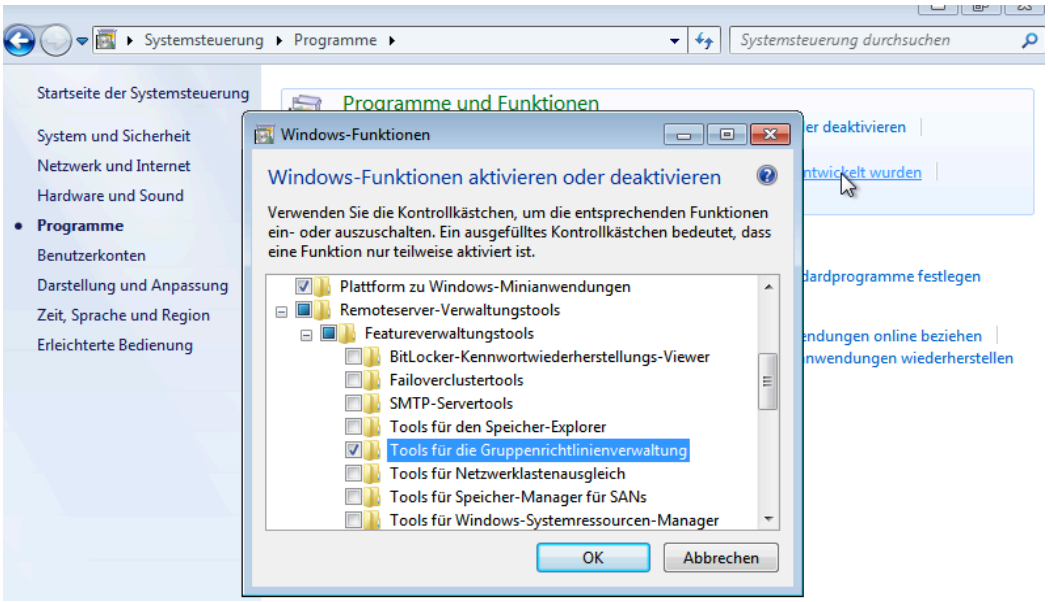
Die Gruppenrichtlinien werden in der SYSVOL-Freigabe gespeichert, siehe Abschnitt 9.2.2.6. Verknüpft mit Benutzer- und Rechnerkonten werden sie im Samba-Verzeichnisdienst.

9.2.3.1.2. Installation der Gruppenrichtlinienverwaltung

Feedback

Die Gruppenrichtlinienverwaltung kann als Teil der *Remote Server Administration Tools* auf Windows Clients installiert werden. Sie können für Windows 7 unter [1], für Windows 8 unter *Remote Server Administration Tools (RSAT) for Windows 8* [2] oder für Windows 10 unter *Remote Server Administration Tools (RSAT) for Windows 10* [3] bezogen werden.

Abbildung 9.1. Aktivierung der Gruppenrichtlinienverwaltung



Nach der Installation muss die Gruppenrichtlinienverwaltung in der Windows-Systemsteuerung noch aktiviert werden, in dem unter **Start -> Systemsteuerung -> Programme -> Windows-Funktionen aktivieren und deaktivieren -> Remoteserver-Verwaltungstools -> Featureverwaltungs-Tools** die Option **Tools für die Gruppenrichtlinienverwaltung** aktiviert wird.

Nach der Aktivierung kann die Gruppenrichtlinienverwaltung unter **Start -> Verwaltung -> Gruppenrichtlinienverwaltung** aufgerufen werden.

9.2.3.1.3. Konfiguration von Richtlinien mit der Gruppenrichtlinienverwaltung

Feedback

Gruppenrichtlinien können nur von Benutzern konfiguriert werden, die Mitglied der Gruppe `Domain Admins` sind (z.B. der `Administrator`). Bei der Anmeldung muss beachtet werden, dass keine Anmeldung mit dem lokalen Administrator-Konto erfolgt, sondern mit dem Administrator-Konto der Domäne. Die Gruppenrichtlinienverwaltung kann auf einem beliebigen System der Domäne aufgerufen werden.

Wenn mehr als ein Samba-Domänencontroller eingesetzt wird, muss die Replikation der GPO-Daten berücksichtigt werden, siehe Abschnitt 9.2.3.1.4.

Es gibt zwei prinzipielle Möglichkeiten GPOs zu erstellen:

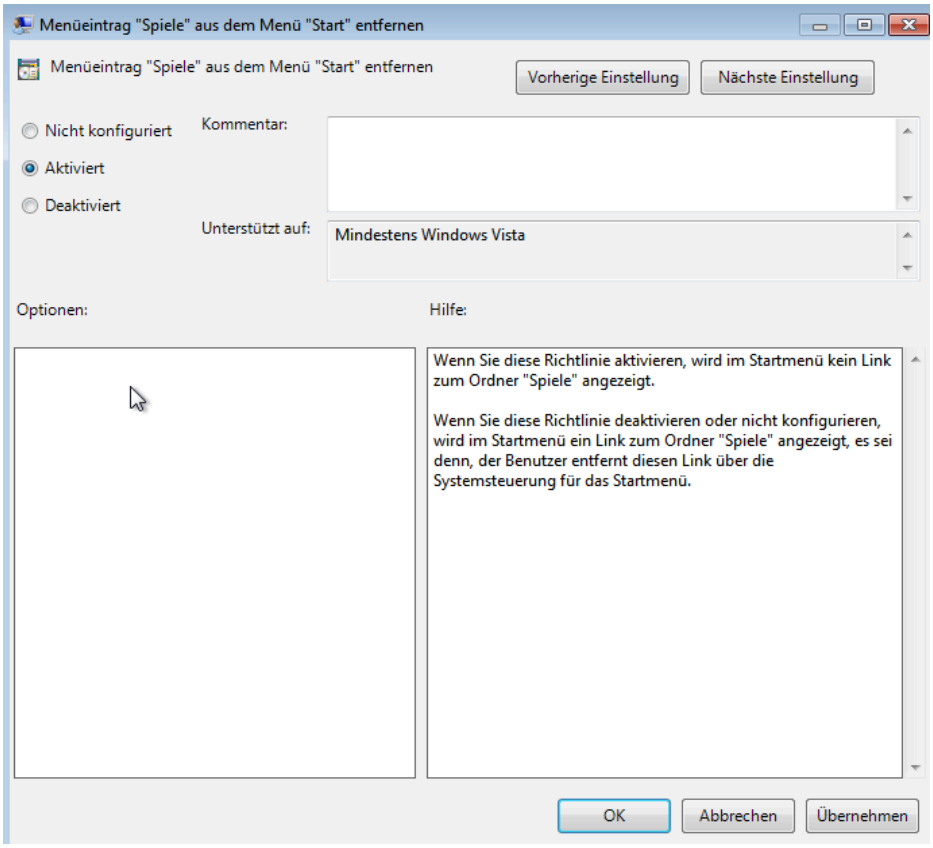
- Sie können im **Gruppenrichtlinienobjekte**-Order angelegt und dann mit verschiedenen Positionen im LDAP verknüpft werden. Dies ist sinnvoll, wenn eine Richtlinie mit mehreren Positionen im LDAP verknüpft werden soll.

[1] http://www.microsoft.com/en-us/download/details.aspx?id=7887
[2] http://www.microsoft.com/de-de/download/details.aspx?id=28972
[3] https://www.microsoft.com/en-us/download/details.aspx?id=45520

- Die GPO kann ad hoc an einer LDAP-Position erstellt und dabei direkt verknüpft werden. Für kleine und mittlere Domänen ist das der einfachere Weg. Auch ad hoc erstellte Domänen werden im **Gruppenrichtlinienobjekte**-Ordner angezeigt.

Eine Richtlinie kann drei Zustände annehmen; sie kann aktiviert, deaktiviert oder nicht gesetzt sein. Die Auswirkung bezieht sich immer auf die Formulierung der Richtlinie. Wenn diese beispielsweise **Deaktiviere Feature xy** heißt, muss die Richtlinie aktiviert werden um das Feature abzuschalten. Einige Richtlinien haben zusätzliche Optionen, z.B. könnte die Richtlinie **Aktiviere Mail-Quota** eine zusätzliche Option mitbringen um die Speichermenge zu verwalten.

Abbildung 9.2. Bearbeiten einer Richtlinie



Zwei Standard-Richtlinienobjekte sind vordefiniert:

- Das *Default Domain Policy* Objekt kann verwendet werden, um globale Richtlinien für alle Benutzer und Rechner der gesamten Domäne zu konfigurieren.

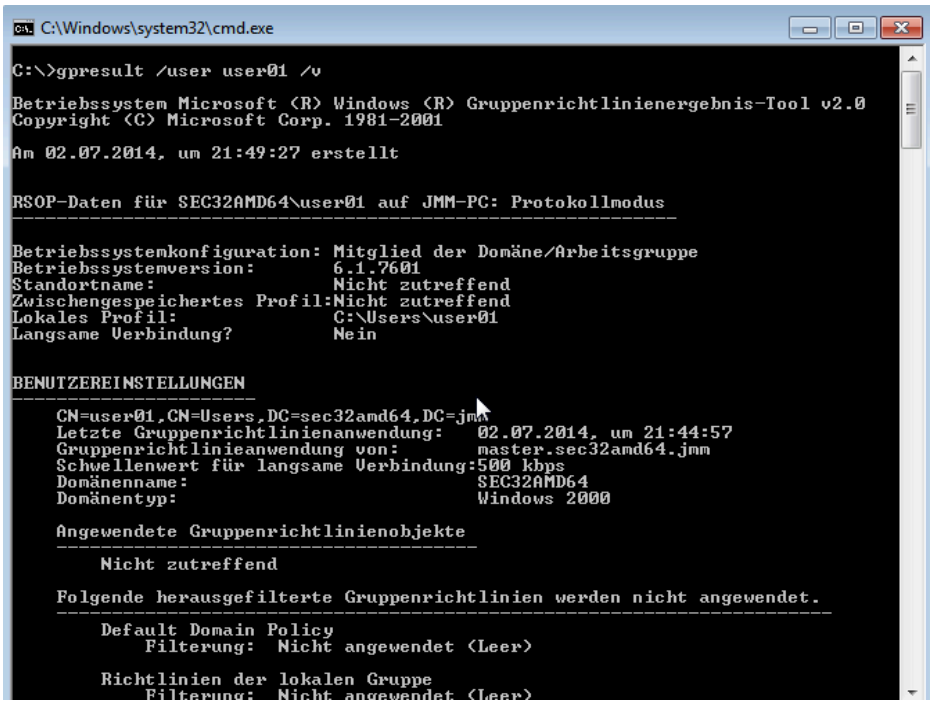
- Das *Default Domain Controllers Policy* Objekt hat in einer Samba-Domäne keine Verwendung (in einer Microsoft AD-Domäne würden die Richtlinien für Microsoft-Domänencontroller über dieses Objekt erfolgen). Die Konfiguration der Samba-Domänencontroller erfolgt in UCS weitgehend über Univention Configuration Registry.

AD-Domänen können in Sites strukturiert werden. Dies kann z.B. verwendet werden um Standorte in einer Domäne zu gruppieren. Im Hauptmenü der Gruppenrichtlinienverwaltung werden alle Sites aufgeführt. Dort findet sich auch eine Liste von Domänen. Die aktuellen Samba-Versionen unterstützen keine Forest-Domänen, so dass hier immer nur eine Domäne angezeigt wird.

Eine Domäne kann in verschiedene Organisations-Einheiten (OUs) strukturiert werden. Dies kann z.B. verwendet werden, um die Mitarbeiter der Buchhaltung und die Benutzer der Verwaltung in unterschiedlichen LDAP-Positionen zu speichern.

Gruppenrichtlinien können sich gegenseitig überlagern. Es gilt das Prinzip der Vererbung, d.h. höherliegende Richtlinien überschreiben die untergeordneten. Die effektiven Richtlinien für einen Benutzer können sowohl mit dem Modellierungsassistenten der Gruppenrichtlinienverwaltung als auch an der Windows-Kommandozeile mit dem Befehl `gpresult /user BENUTZERNAME /v` auf dem Windows-Client angezeigt werden:

Abbildung 9.3. Auswertung der GPO für den Benutzer `user01`



Die Richtlinien werden in folgender Reihenfolge ausgewertet:

- Richtlinien der *Default Domain Policy* gelten als Grundeinstellung für alle Benutzer und Rechner der gesamten Domäne.
- Mit einer OU verknüpfte Richtlinien überschreiben Richtlinien aus der Default Domain Policy. Sind OUs weiter verschachtelt, greifen im Konfliktfall die jeweils "untersten" Richtlinien, d.h. die, die näher am Zielobjekt verknüpft sind. Es gilt folgende Auswertungsreihenfolge:
  - Zuweisung einer Richtlinie zu einer Active Directory-Site
  - Vorgaben der Default Domain Policy
  - Zuweisung einer Richtlinie zu einer Organisationseinheit / OU (jede unterliegende OU überstimmt wiederum Richtlinien aus übergeordneten OUs)

Ein Beispiel: Eine Firma verbietet allgemein den Zugriff auf den Windows Task Manager. Dazu wird im *Default Domain Policy*-Objekt die Richtlinie **Zugriff auf Task Manager unterbinden** aktiviert. Für einige technisch versierte Benutzer soll der Task Manager dennoch verfügbar sein. Diese Benutzer sind in der OU *Technik* abgelegt. Nun wird ein zusätzliches Gruppenrichtlinienobjekt angelegt, in dem Richtlinie **Zugriff**

auf Task Manager unterbinden auf *deaktiviert* gesetzt wird. Dieses neue GPO wird mit der OU *Technik* verbunden.

9.2.3.1.4. Konfiguration von Gruppenrichtlinien in Umgebungen mit mehr als einem Samba-Domänencontroller

Feedback

Eine Gruppenrichtlinie besteht technisch aus zwei Teilen: Zum einen gibt es ein Verzeichnis im Dateisystem der Domänencontroller, das die eigentlichen Richtlinien-Dateien enthält, die auf dem Windows-System umgesetzt werden sollen (gespeichert in der SYSVOL-Freigabe (siehe Abschnitt 9.2.2.6)). Zum anderen gibt es ein gleichnamiges Objekt im LDAP-Baum des Samba-Verzeichnisdienstes (Samba DS/AD), das üblicherweise unter einem LDAP-Container namens *Group Policy Objects* abgelegt ist.

Während die LDAP-Replikation zwischen Domänencontrollern innerhalb weniger Sekunden umgesetzt ist, werden die Dateien in der SYSVOL-Freigabe in der Grundeinstellung nur alle fünf Minuten repliziert. Es ist zu beachten, dass die Anwendung von neu konfigurierten Gruppenrichtlinien in diesem Zeitraum fehlschlagen kann, falls ein Client zufällig einen Domänencontroller konsultiert, der noch nicht die aktuellen Dateien zu sich repliziert hat.

9.2.3.1.5. Administrative Vorlagen (ADMX/ADM)

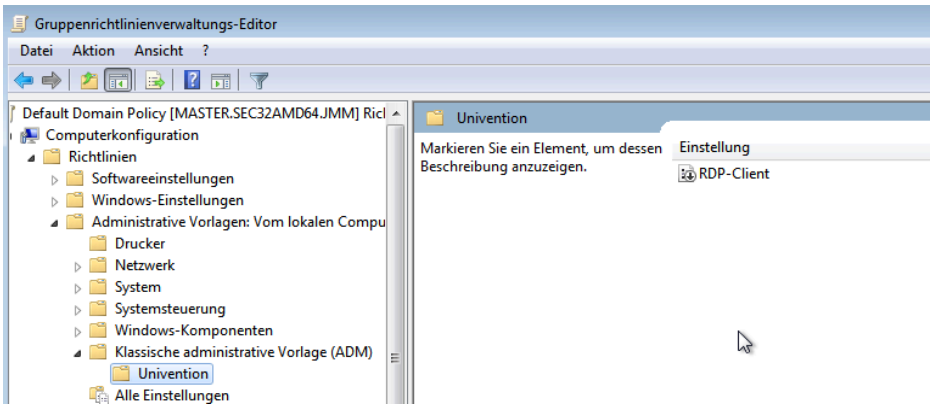
Feedback

Die in der Gruppenrichtlinienverwaltung angezeigten Richtlinien können durch sogenannte *Administrative Vorlagen* erweitert werden. In einer solchen Vorlage wird definiert unter welchem Namen die Richtlinie in der Gruppenrichtlinienverwaltung erscheinen soll und welcher Wert dadurch in der Windows-Registry gesetzt wird. Administrative Vorlagen werden in sogenannten *ADMX-Dateien* (früher *ADM-Dateien*) gespeichert [admx-reference]. ADMX-Dateien bieten unter anderem den Vorteil, dass sie zentral über mehrere Domänencontroller bereitgestellt werden können, damit die Gruppenrichtlinienverwaltung an allen Windows-Clients die gleichen Konfigurationsmöglichkeiten zeigt [admx-central].

Das folgende Beispiel für eine ADM-Datei definiert eine Rechner-Richtlinie, in der ein Registry-Key des (fiktiven) Univention RDP-Client konfiguriert wird. ADM-Dateien können über Third-Party-Werkzeuge in das neuere ADMX-Format umgewandelt werden. Weiterführende Informationen zum Format von ADM-Dateien sind unter [microsoft-adm-templates] und [adm-templates-howto] zu finden. Die administrativen Vorlagen müssen die Dateiendung `.adm` verwenden:

```
CLASS MACHINE
CATEGORY "Univention"
POLICY "RDP-Client"
KEYNAME "Univention\RDP\StorageRedirect"
EXPLAIN "Ist diese Option aktiviert, wird Soundausgabe im RDP-Client
 aktiviert"
VALUENAME "Sound-Weiterleitung"
VALUEON "Aktiviert"
VALUEOFF "Deaktiviert"
END POLICY
END CATEGORY
```

Abbildung 9.4. Die eingebundene administrative Vorlage



Die ADM-Datei kann anschließend in das ADMX-Format umgewandelt oder aber direkt über die Gruppenrichtlinienverwaltung importiert werden. Dazu wird im Kontextmenü der **Administrativen Vorlagen** die Option **Vorlagen hinzufügen -> entfernen** aufgerufen. Mit **Hinzufügen** kann dann eine ADM-Datei importiert werden. Die administrativen Vorlagen werden ebenfalls in der SYSVOL-Freigabe gespeichert und repliziert, wodurch die Gruppenrichtlinienverwaltung von den Windows-Clients aus auf sie zugreifen kann.

9.2.3.1.6. Anwendung von Richtlinien auf Basis von Rechnereigenschaften (WMI-Filter)

Feedback

Richtlinien können auch auf Basis von Systemeigenschaften konfiguriert werden. Diese Eigenschaften werden über die Windows Management Instrumentation-Schnittstelle (WMI) bereitgestellt. Der darauf aufbauende Mechanismus wird als *WMI-Filterung* bezeichnet. Damit ist es beispielsweise möglich eine Richtlinie nur auf PCs mit einer 64 Bit-Prozessor-Architektur oder mit min. 8 GB RAM anzuwenden. Ändert sich eine Eigenschaft eines Systems (z.B. weil mehr Speicher eingebaut wurde), wird der jeweilige Filter automatisch vom Client neu ausgewertet.

Die WMI-Filter werden in der Domänenstruktur im Container **WMI-Filter** angezeigt. Mit **Neu** kann ein weiterer Filter definiert werden. Unter **Abfragen** werden die Filterregeln definiert. Die Regeln werden in einer SQL-ähnlichen Syntax definiert. Regel-Beispiele finden sich in [microsoft-wmi-filter] und [add-wmi-filters].

9.2.3.2. Anmeldeskripte / NETLOGON-Freigabe

Feedback

Die NETLOGON-Freigabe dient der Bereitstellung von Anmeldeskripten in Windows-Domänen. Die Anmeldeskripte werden nach der erfolgreichen Anmeldung eines Benutzers ausgeführt und ermöglichen die Anpassung der Arbeitsumgebung des Benutzers. Die Skripte müssen in einem für Windows ausführbaren Format gespeichert werden, wie z.B. `bat`.

Die Anmeldeskripte werden unter `/var/lib/samba/sysvol/`*`Domänenname`*`/scripts/` abgelegt und werden unter dem Freigabennamen *NETLOGON* bereitgestellt. Die NETLOGON-Freigabe wird im Rahmen der SYSVOL-Replikation repliziert. Der Dateiname des Skripts muss relativ zu diesem Verzeichnis angegeben werden.

Das Anmeldeskript kann pro Benutzer zugewiesen werden, siehe Abschnitt 6.1.

9.2.3.3. Konfiguration des Servers, auf dem das Heimatverzeichnis abgelegt wird

Feedback

Das Heimatverzeichnis wird benutzerbezogen in Univention Management Console definiert siehe Abschnitt 6.1. Dies erfolgt mit der Einstellung **Windows-Heimatverzeichnis**, z.B. `\\ucs-file-server\meier`.

Für das Zuweisen des Heimatverzeichnis-Servers an mehrere Benutzer auf einmal kann der Mehrfachbearbeitungsmodus von Univention Management Console verwendet werden, siehe Abschnitt 4.4.3.3.

9.2.3.4. Servergespeicherte Profile

Feedback

Samba unterstützt servergespeicherte Profile, d.h. Einstellungen der Benutzer werden auf einem Server gespeichert. In diesem Verzeichnis werden auch die Dateien gespeichert, die der Benutzer im Ordner *Eigene Dateien* speichert. Sie werden zwischenzeitlich lokal auf dem Windows-Rechner vorgehalten und erst bei der Abmeldung auf den Samba-Server synchronisiert.

Wird der Profilpfad in Univention Management Console geändert, wird ein neues Profilverzeichnis angelegt. Die Daten aus dem alten Profilverzeichnis bleiben dabei erhalten und können manuell in das neue Profilverzeichnis kopiert beziehungsweise verschoben werden. Abschließend kann das alte Profilverzeichnis gelöscht werden.

In Samba-Domänen mit Active Directory-Support werden in der Voreinstellung keine serverseitigen Profile verwendet.

Das Profilverzeichnis kann über eine Gruppenrichtlinie konfiguriert werden, die unter **Computerkonfiguration -> Richtlinien -> Administrative Vorlagen -> System -> Benutzerprofile -> Pfad des servergespeicherten Profils für alle Benutzer festlegen** zu finden ist.

Anmerkung

Der Administrator-Benutzer greift standardmäßig mit root-Berechtigungen auf Freigaben zu. Wenn dadurch das Profilverzeichnis mit root als Benutzer angelegt wird, sollte es manuell mit dem Befehl `chown` an den Administrator vergeben werden.

9.3. Active Directory-Verbindung

Feedback

9.3.1. Einführung

Feedback

Univention Corporate Server kann auf zwei unterschiedliche Arten mit einer bestehenden Active Directory-Domäne (AD-Domäne) zusammen betrieben werden. Beide Varianten lassen sich durch die Applikation *Active Directory-Verbindung* aus dem Univention App Center einrichten (siehe Abschnitt 5.6). Diese steht auf einem Domänencontroller Master und Domänencontroller Backup zur Verfügung.

Die beiden Varianten sind:

- UCS als Teil (Domänen-Mitglied) einer AD-Domäne (siehe Abschnitt 9.3.2)
- Synchronisation von Kontendaten zwischen einer AD-Domäne und einer UCS-Domäne (siehe Abschnitt 9.3.3)

In beiden Modi wird unter UCS der Active Directory-Verbindungsdienst verwendet (kurz UCS AD-Connector), der Verzeichnisdienstobjekte zwischen einem Windows 2012/2016/2019-Server mit Active Directory (AD) und dem OpenLDAP-Verzeichnis aus Univention Corporate Server synchronisieren kann.

Im ersten Fall, der Konfiguration eines UCS-Serversystems als Mitglied einer AD-Domäne, dient das AD als führender Verzeichnisdienst und das jeweilige UCS-System tritt dem Vertrauenskontext der AD-Domäne bei. Durch die Domänenmitgliedschaft hat das UCS-System limitierten Zugriff auf Kontodaten der Active Directory-Domäne. Die Einrichtung dieses Betriebsmodus ist im Detail in Abschnitt 9.3.2 beschrieben.

Der zweite Modus, der sich über die App *Active Directory-Verbindung* konfigurieren lässt, dient dazu, die UCS Domäne parallel zu einer bestehenden AD-Domäne zu betreiben. In diesem Modus ist jedem Domänen-Benutzer sowohl in der UCS- als auch in der AD-Domäne ein gleichnamiges Benutzerkonto zugeordnet. Durch die Namensidentität und die Synchronisation der verschlüsselten Passwortdaten ermöglicht dieser

Modus einen transparenten Zugriff zwischen beiden Domänen. Die Authentifikation eines Benutzers in der UCS-Domäne geschieht in diesem Modus direkt innerhalb der UCS-Domäne und ist damit nicht direkt abhängig von der AD-Domäne. Die Einrichtung diese Betriebsmodus ist im Detail in Abschnitt 9.3.3 beschrieben.

9.3.2. UCS als Mitglied einer Active Directory-Domäne

Bei der Konfiguration eines UCS-Serversystems als Mitglied einer AD-Domäne (*AD member*-Modus) dient das AD als führender Verzeichnisdienst und das jeweilige UCS-System tritt dem Vertrauenskontext der AD-Domäne bei. Das UCS-System ist nicht in der Lage selbst als Active Directory Domänencontroller zu arbeiten. Durch die Domänenmitgliedschaft hat das UCS-System limitierten Zugriff auf Kontodaten der Active Directory-Domäne, die es über den UCS AD-Connector aus dem AD ausliest und lokal in den eigenen OpenLDAP-basierten Verzeichnisdienst schreibt. In dieser Konfiguration schreibt der UCS AD-Connector keine Änderungen in das AD.

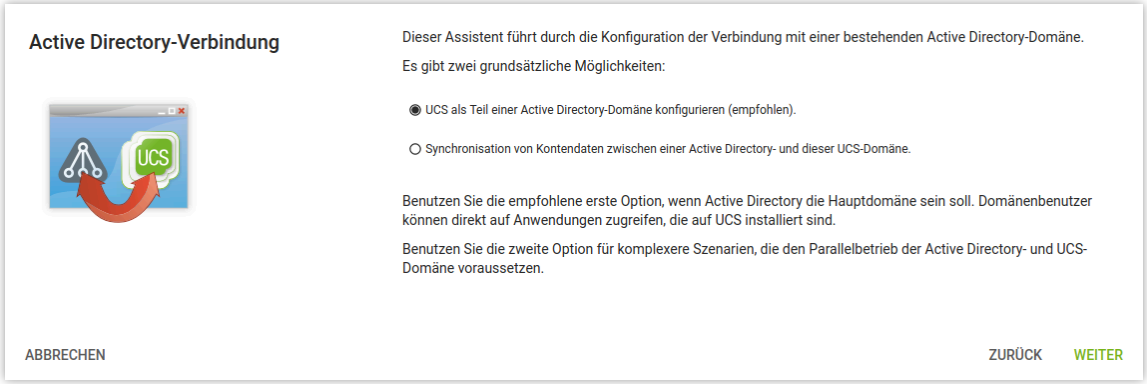
Der *AD member*-Modus eignet sich, um eine AD-Domäne durch Applikationen zu erweitern, die auf der UCS-Plattform zur Verfügung stehen. Auf der UCS-Plattform installierte Apps sind dann für Benutzer der AD-Domäne nutzbar. Die Authentifikation erfolgt dabei weiter gegen native Microsoft AD-Domänencontroller.

Der Einrichtungsassistent kann direkt bei der UCS Installation durch die Auswahl *Einer bestehenden Active-Directory-Domäne beitreten* gestartet werden. Nachträglich kann der Einrichtungsassistent mit der Applikation *Active Directory-Verbindung* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-ad-connector*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

Anmerkung

- Der *AD member*-Modus kann nur auf einem Domänencontroller Master konfiguriert werden.
- Der Name der DNS-Domäne des UCS-Systems muss mit dem der AD-Domäne übereinstimmen. Die Hostnamen selbst müssen natürlich unterschiedlich sein.
- Alle AD- und UCS-Server in einer Connector-Umgebung sollten dieselbe Zeitzone verwenden.

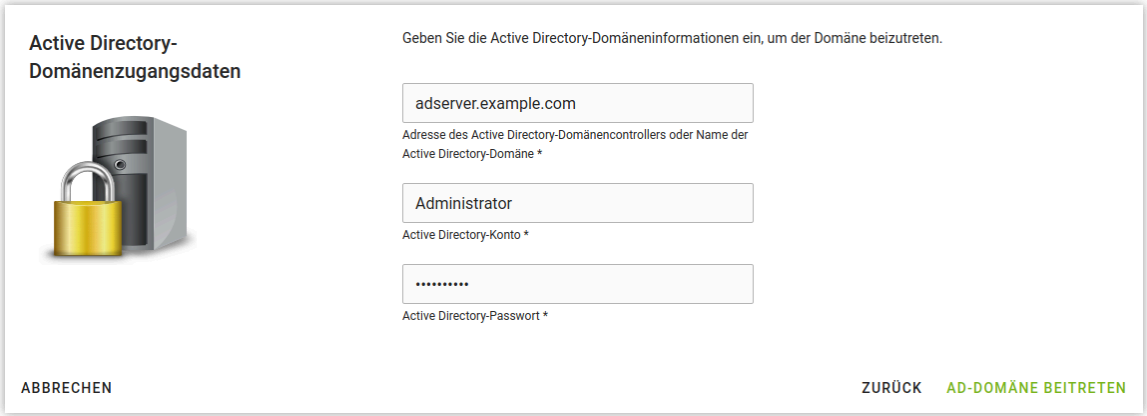
Abbildung 9.5. Konfiguration des Betriebsmodus als Teil einer AD-Domäne



Im ersten Dialog der Einrichtungsassistenten ist der Punkt *UCS als Teil einer AD-Domäne konfigurieren* vorausgewählt und kann mit **[Weiter]** bestätigt werden.

Im nächsten Dialog wird die Adresse eines AD-Domänencontrollers sowie der Name des Standard-Administrator-Kontos der AD-Domäne und dessen Passwort abgefragt. Hier sollte das Standard-AD-Administratorkonto verwendet werden. Der angegebene AD-Domänencontroller muss auch DNS-Dienste für die Domäne bereitstellen. Durch Betätigen der Schaltfläche **[AD-Domäne beitreten]** wird der Domänenbeitritt gestartet.

Abbildung 9.6. Domänenbeitritt zu einer AD-Domäne



Falls die Systemzeit des UCS-Systems mehr als 5 Minuten gegenüber der Systemzeit des AD-Domänencontrollers vorgeht, ist eine manuelle Angleichung der Systemzeiten notwendig. Dies ist notwendig, da die AD-Kerberos-Infrastruktur zur Authentifizierung verwendet wird. Systemzeiten sollten dabei nicht zurückgestellt werden, um Inkonsistenzen zu vermeiden.

Der Domänenbeitritt läuft automatisch ab. Der abschließende Dialog sollte mit **[Fertigstellen]** bestätigt werden. Danach sollte mit einem Klick auf **[Neustart]** der UMC-Server neu gestartet werden.

Anmerkung

Nach Einrichtung des *AD member*-Modus findet die Authentifikation gegen den AD-Domänencontroller statt. *Daher gilt für den Administrator jetzt das Passwort aus der AD-Domäne.* Falls einer AD-Domäne mit nicht-englischsprachiger Sprachkonvention beigetreten wurde, dann wird das `Administrator`-Konto aus UCS während des Domänenbeitritts automatisch in die Schreibweise des AD umbenannt. Gleiches gilt für alle Benutzer- und Gruppenobjekte mit *Well Known SID* (z.B. `Domain Admins`).

Warnung

Falls zuvor neben dem Domänencontroller Master weitere UCS-Systeme schon Teil der UCS-Domäne waren, dann müssen diese der Domäne neu beitreten. Dabei erkennen sie, dass der Domänencontroller Master sich im *AD member*-Modus befindet und treten ebenfalls der Authentifikationsstruktur der AD-Domäne bei und können dann z.B. zusätzlich Samba-Dateifreigaben bereitstellen.

Anmerkung

Da in diesem Modus die AD-Kerberos-Infrastruktur zur Authentifizierung von Benutzern verwendet wird, ist es essenziell, dass die Systemzeiten von UCS und AD-Domänencontroller synchron sind (mit einer Toleranz von 5 Minuten). Zu diesem Zweck ist unter UCS der AD-Domänencontroller als NTP-Zeitserver konfiguriert. Im Falle von Authentifikationsproblemen sollte immer als erstes die Systemzeit überprüft werden.

Nach dieser Einrichtung kann das UMC-Modul *Active Directory-Verbindung* zur weiteren Administration verwendet werden, z.B. um zu prüfen, ob der Dienst läuft und ihn ggf. neu zu starten (siehe Abschnitt 9.3.3.3).

Um eine verschlüsselte Verbindung zwischen Active Directory und Domänencontroller Master nicht nur für die Authentifikation, sondern auch für den Datenaustausch an sich zu verwenden, kann auf dem AD-Domänencontroller das Root-Zertifikat der Zertifizierungsstelle exportiert und über das UMC-Modul hochgeladen werden. Weitere Informationen dazu liefert Abschnitt 9.3.3.2.

Per Voreinstellung überträgt die so eingerichtete Active Directory-Verbindung keine Passwortdaten aus AD in den UCS-Verzeichnisdienst. Einige Apps aus dem App Center benötigen verschlüsselte Passwortdaten. Sofern eine App diese benötigt, wird ein entsprechender Hinweis im App Center angezeigt.

Im *AD member*-Modus liest der UCS AD-Connector Objektdaten per Voreinstellung mit den Berechtigungen des Maschinenkontos des Domänencontroller Masters aus dem AD. Für das Auslesen von verschlüsselten Passwortdaten sind dessen Berechtigungen nicht ausreichend. Daher muss in diesem Fall zusätzlich manuell die LDAP-DN eines privilegierten Replikationsbenutzers in die Univention Configuration Registry-Variable `connector/ad/ldap/binddn` eingetragen werden. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Kennwort muss auf dem Domänencontroller Master in eine Datei gespeichert werden und ihr Dateiname muss in die Univention Configuration Registry-Variable `connector/ad/ldap/bindpw` eingetragen werden. Falls zu einem späteren Zeitpunkt das Zugriffspasswort geändert wurde, muss das neue Passwort in diese Datei eingetragen werden. Die Zugriffsrechte für die Datei sollten so eingeschränkt werden, dass nur der Besitzer `root` Zugriff hat.

Die folgenden Kommandos zeigen die Schritte beispielhaft:

```
ucr set connector/ad/ldap/binddn=Administrator
ucr set connector/ad/ldap/bindpw=/etc/univention/connector/password
touch /etc/univention/connector/password
chmod 600 /etc/univention/connector/password
echo -n "Administrator password" > /etc/univention/connector/password
ucr set connector/ad/mapping/user/password/kinit=false
```

Falls gewünscht, kann zu einem späteren Zeitpunkt der AD-Domänencontroller auch durch den Domänencontroller Master abgelöst werden. Dies ist über die Applikation *Active Directory Takeover* möglich (siehe Abschnitt 9.4).

9.3.3. Einrichtung des UCS AD-Connectors

Feedback

Als Alternative zur Mitgliedschaft in einer AD-Domäne, die im vorherigen Abschnitt beschrieben ist, kann der UCS Active Directory-Connector dazu verwendet werden, Benutzer- und Gruppenobjekte zwischen einer UCS-Domäne und einer AD-Domäne zu synchronisieren. Diese Betriebsart erlaubt über die unidirektionale Synchronisation hinaus auch die bidirektionale Synchronisation. In dieser Betriebsart bestehen beide Domänen parallel und ihre Authentifikationssysteme funktionieren unabhängig. In diesem Betriebsmodus werden per Voreinstellung auch verschlüsselten Passwortdaten synchronisiert.

In der Standardeinstellung werden Container, Organisationseinheiten, Benutzer, Gruppen und Rechner synchronisiert.

Hinweise zu den in der Grundeinstellung konfigurierten Attributen und zu beachtende Besonderheiten finden sich in Abschnitt 9.3.5.

Durch die in beiden Domänen gleichen Benutzereinstellungen können Benutzer transparent auf Dienste beider Umgebungen zugreifen. Nachdem eine Domänenanmeldung an einer UCS-Domäne durchgeführt wurde, ist anschließend eine Verbindung zu einer Dateifreigabe oder einem Exchange-Server mit Active Directory ohne erneute Passwortabfrage möglich. Auf den Ressourcen der anderen Domäne finden Benutzer und Administratoren gleichnamige Benutzer und Gruppen vor und können so mit den gewohnten Rechtestrukturen arbeiten.

Nach dem erstmaligen Start des Connectors wird die Initialisierung vorgenommen. Dabei werden alle Einträge aus dem UCS gelesen und entsprechend dem eingestellten Mapping in AD-Objekte umgewandelt und auf AD-Seite hinzugefügt, bzw., falls bereits vorhanden, modifiziert. Anschließend werden alle Objekte aus dem AD gelesen und in UCS-Objekte umgewandelt und entsprechend auf UCS-Seite hinzugefügt bzw. modifiziert. Solange noch Änderungen vorliegen, werden die Verzeichnisdienst-Server weiter abgefragt. Der UCS AD-Connector kann auch in einem unidirektionalen Modus betrieben werden.

Nach dem initialen Sync werden weitere Änderungen in einem festen Intervall abfragt. Dieser Wert ist auf fünf Sekunden eingestellt und kann manuell per Univention Configuration Registry-Variable `connector/ad/poll/sleep` angepasst werden.

Sollte ein Objekt nicht synchronisiert werden können, so wird dieses Objekt zunächst zurückgestellt ("rejected"). Nach einer konfigurierbaren Anzahl von Durchläufen - das Intervall kann im per Univention Configuration Registry-Variable `connector/ad/retryrejected` angepasst werden - wird erneut versucht diese Änderungen wieder einzuspielen. Der Standardwert beträgt zehn Durchläufe. Außerdem wird bei einem Neustart des UCS AD-Connectors ebenfalls versucht, die zuvor zurückgewiesenen Änderungen erneut zu synchronisieren.

9.3.3.1. Grundkonfiguration des UCS AD-Connectors

Der UCS AD-Connector wird über den Assistenten **Active Directory-Verbindung** der Univention Management Console konfiguriert.

Der Einrichtungsassistent kann mit der Applikation *Active Directory-Verbindung* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-ad-connector*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

Anmerkung

Alle AD- und UCS-Server in einer Connector-Umgebung müssen dieselbe Zeitzone verwenden.

Warnung

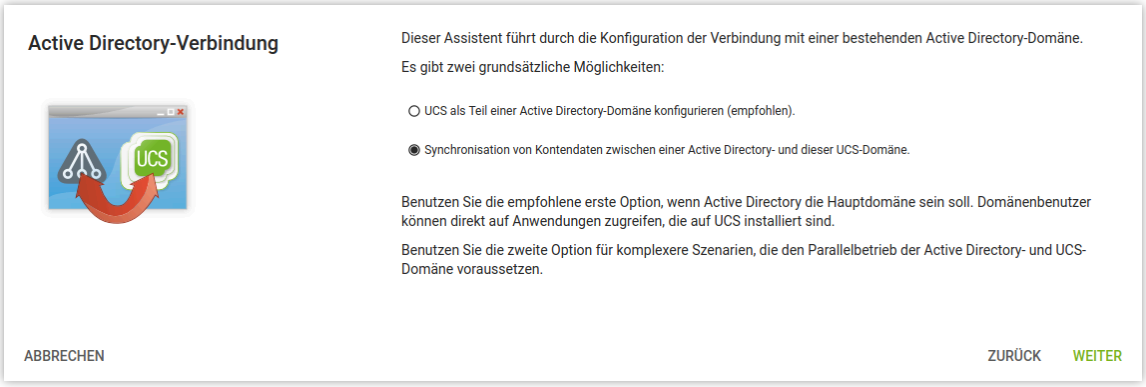
Trotz intensiver Tests kann aufgrund der Vielfalt der Konfigurations- und Betriebsvarianten einer AD-Domäne nicht ausgeschlossen werden, dass die Ergebnisse des Synchronisationsvorgangs den Betrieb einer produktiven Domäne beeinträchtigen. Der UCS AD-Connector sollte daher vorab in einer getrennten Umgebung auf die jeweiligen Anforderungen geprüft werden.

Es ist zu empfehlen, die folgenden Schritte mit einem Webbrowser vom AD-Domänencontroller aus durchzuführen, da Dateien auf den AD-Domänencontroller herunter geladen und in Univention Management Console hochgeladen werden müssen.

Internet Explorer 6 - der auf Windows 2003-Systemen vorinstalliert ist - wird durch Univention Management Console nicht unterstützt. Hier sollte zuerst eine Aktualisierung des Browsers durchgeführt oder ein alternativer Browser installiert werden.

Im ersten Dialog der Einrichtungsassistenten muss der Punkt *Synchronisation von Kontendaten zwischen einer AD und dieser UCS-Domäne* ausgewählt und mit **[Weiter]** bestätigt werden.

Abbildung 9.7. Konfiguration des UCS AD-Connectors in UMC



Im nächsten Dialog wird die Adresse eines AD-Domänencontrollers abgefragt. Hier kann die IP-Adresse oder ein voll qualifizierter DNS-Name eingegeben werden. Wenn der Rechnername des AD-Systems für das UCS-System nicht auflösbar sein sollte, kann entweder unter UCS der AD DNS-Server als DNS-Forwarder konfiguriert werden oder es kann in der DNS-Verwaltung von Univention Management Console ein DNS-Host-Record für das AD-System angelegt werden (siehe Abschnitt 11.2.2.3).

Alternativ kann auch über Univention Configuration Registry ein statischer Eintrag in `/etc/hosts` aufgenommen werden, z.B. mit

```
ucr set hosts/static/192.0.2.100=w2k8-32.ad.example.com
```

Im Feld **Active Directory-Konto** wird der Benutzer konfiguriert, der für den Zugriff auf das AD verwendet wird. Die Einstellung wird in der Univention Configuration Registry-Variable `connector/ad/ldap/binddn` gespeichert. Der Replikationsbenutzer muss im AD Mitglied der Gruppe `Domänen-Admins` sein.

Das verwendete Kennwort für den Zugriff muss im Feld **Active Directory-Passwort** eingetragen werden. Es wird auf dem UCS-System lokal in einer Datei gespeichert, die nur für den Benutzer `root` lesbar ist.

Abschnitt 9.3.3.5 beschreibt die Schritte, die notwendig sind, falls diese Zugangsdaten zu einem späteren Zeitpunkt angepasst werden müssen.

Nach Klick auf **[Weiter]** prüft der Einrichtungsassistent die Verbindung zum AD-Domänencontroller. Falls keine SSL/TLS-verschlüsselte Verbindung aufgebaut werden kann wird eine Warnung ausgegeben in der zur Installation einer Zertifizierungsstelle auf dem AD-Domänencontroller geraten wird. Es wird empfohlen diesem Rat zu folgen. Nach diesem Schritt kann die Einrichtung durch erneuten Klick auf **[Weiter]** fortgesetzt werden. Falls weiterhin keine SSL/TLS-verschlüsselte Verbindung aufgebaut werden kann, wird in einem Sicherheitshinweis nachgefragt, ob die Synchronisation ohne SSL-Verschlüsselung eingerichtet werden soll. Falls dies gewünscht ist, kann die Einrichtung durch Klick auf **[Fortfahren ohne Verschlüsselung]** fortgesetzt werden. In diesem Fall findet die Synchronisation der Verzeichnisdaten unverschlüsselt statt.

Falls der AD-Domänencontroller SSL/TLS-verschlüsselte Verbindungen unterstützt, bietet der Einrichtungsassistent im nächsten Schritt das **Hochladen des AD-Root-Zertifikats** an. Dieses Zertifikat muss vorher aus der AD-Zertifizierungsstelle exportiert werden (siehe Abschnitt 9.3.3.2). Falls dieser Schritt hingegen übersprungen wird, kann das Zertifikat auch zu einem späteren Zeitpunkt über das UMC-Modul hochgeladen und die SSL/TLS-Verschlüsselung aktiviert werden (bis dahin werden dann aber alle Verzeichnisdaten unverschlüsselt synchronisiert).

Der Connector kann in verschiedenen Modi betrieben werden, die im nächsten Dialog **Konfiguration der Active Directory-Domänensynchronisation** ausgewählt werden können. Neben einer bidirektionalen Synchronisation kann auch unidirektional von AD nach UCS oder unidirektional von UCS in das AD repliziert werden. Nach Auswahl des Modus muss auf **[Weiter]** geklickt werden.

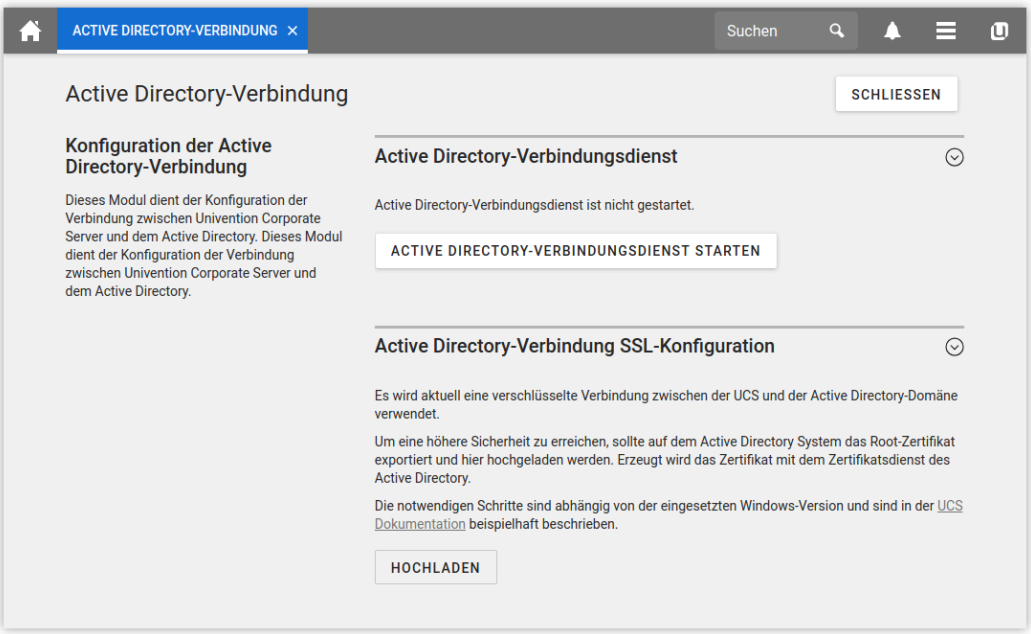
Nach einem Klick auf **[Weiter]** wird die Konfiguration übernommen und der UCS AD-Connector wird gestartet. Der abschließende Dialog muss dann durch Klick auf **[Fertigstellen]** geschlossen werden.

Nach dieser Einrichtung kann das UMC-Modul *Active Directory-Verbindung* zur weiteren Administration des UCS Active Directory Connectors verwendet werden, z.B. um zu prüfen, ob der Dienst läuft und ihn ggf. neu zu starten (siehe Abschnitt 9.3.3.3).

Anmerkung

Der Connector kann auch mehrere AD-Domänen mit einer UCS-Domäne synchronisieren; dies ist in [ext-doc-win] dokumentiert.

Abbildung 9.8. Administrationsdialog für die Active Directory-Verbindung



9.3.3.2. Import des SSL-Zertifikats des Active Directory

Feedback

Auf dem Active Directory-System muss nun ein SSL-Zertifikat erzeugt und das Root-Zertifikat exportiert werden, damit eine verschlüsselte Kommunikation stattfinden kann. Erzeugt wird das Zertifikat mit dem Zertifikatsdienst des Active Directory. Die nötigen Schritte sind abhängig von der eingesetzten Windows-Version und werden hier beispielhaft für drei Varianten dargestellt.

Die verschlüsselte Verbindung zwischen UCS-System und Active Directory kann auch deaktiviert werden, indem die Univention Configuration Registry-Variable `connector/ad/ldap/ssl` auf `no` gesetzt wird. Diese Einstellung betrifft nicht die Synchronisation der verschlüsselten Passwortdaten.

9.3.3.2.1. Export unter Windows 2003

Feedback

Falls der Zertifikatsdienst nicht installiert ist, so kann dieser nachinstalliert werden: **Start -> Einstellungen -> Systemsteuerung -> Software -> Windows Komponenten, Zertifikatsdienst auswählen -> Weiter Stammzertifizierungsstelle des Unternehmens wählen -> Weiter, Domänen Namen angeben -> Weiter -> Weiter**. Anschließend sollte der Server neu gestartet werden.

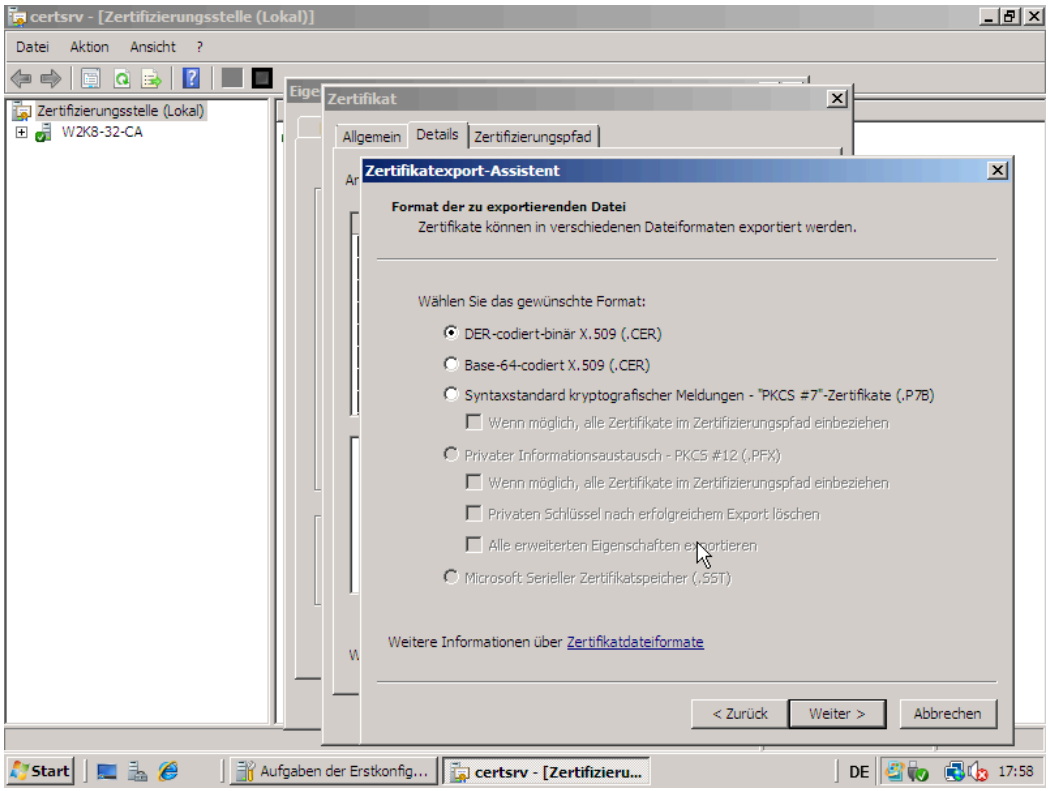
Dieses Zertifikat muss exportiert und auf das UCS System kopiert werden: **Zertifizierungsstelle -> AD-Domäne -> Eigenschaften -> Zertifikat anzeigen -> Details -> In Datei kopieren -> DER-codiert-binaer X.509**.

9.3.3.2.2. Export unter Windows 2008

Feedback

Falls der Zertifikatsdienst nicht installiert ist, so muss dieser nachinstalliert werden:

Abbildung 9.9. Export des Root-Zertifikats unter Windows 2008



Start -> Systemsteuerung -> Programme und Funktionen -> Windows-Funktionen aktivieren oder deaktivieren -> Rollen -> Rollen hinzufügen -> Weiter -> Haken bei Active Directory-Zertifikatsdienste aktivieren -> Weiter -> Weiter -> Zertifizierungsstelle aktivieren -> Unternehmen auswählen -> Stammzertifierungsstelle auswählen -> Neuen privaten Schlüssel erstellen -> Weiter -> Die vorgeschlagenen Kryptoeinstellungen mit Weiter akzeptieren -> Den vorgeschlagenen Namen der Zertifizierungsstelle akzeptieren -> Eine beliebige Gültigkeitsdauer auswählen -> Weiter -> Standardpfad für die Zertifikatsdatenbank akzeptieren . Im abschließenden Dialog erscheint eine Warnmeldung, dass Name und Domäneneinstellung nach Installation der Zertifizierungsstelle nicht mehr geändert werden können. Dies muss mit **Installieren** bestätigt werden.

Anschließend muss der AD-Server neu gestartet werden.

Dieses Zertifikat muss nun exportiert und auf das UCS System kopiert werden: **Start -> Programme -> Verwaltung -> Zertifizierungsstelle**. Dort wird eine Rechnerliste angezeigt und unter jedem System die Elemente **Gesperrte Zertifikate**, **Ausgestellte Zertifikate**, **Ausstehende Anforderungen**, **Fehlgeschlagene Anforderungen** und **Zertifikatsvorlagen** angezeigt. Hier muss ein Rechtsklick auf den Rechnernamen erfolgen - nicht auf eines der Elemente darunter - und **Eigenschaften** ausgewählt werden. Das Root-Zertifikat heisst in der Regel **Zertifikat Nr. 0**. Dann **Zertifikat anzeigen -> Details -> In Datei kopieren -> DER-codiert-binär X.509 (.CER) -> Auswahl eines beliebigen Dateinamens und Speicherpfad -> Fertig stellen**.

9.3.3.2.3. Export unter Windows Server 2012

Feedback

Falls der Zertifikatsdienst nicht installiert ist, so muss dieser nachinstalliert werden:

Der Server-Manager muss geöffnet werden. Dort im Menü **Verwalten -> Rollen und Features hinzufügen** die Rolle **Active Directory-Zertifikatsdienste** auswählen. Bei der Auswahl der Rollendienste reicht es aus, nur die **Zertifizierungsstelle** auszuwählen. Anschließend wird im Server-Manager in der oberen Leiste ein gelbes Warndreieck angezeigt. Hier muss die Option **Active Directory-Zertifikatsdienste auf dem Zielser-**

ver konfigurieren ausgewählt werden. Als zu konfigurierender Rollendienst wird **Zertifizierungsstelle** ausgewählt. Der Installationstyp ist **Unternehmenszertifizierungsstelle -> Stammzertifizierungsstelle**. Nun muss auf **Neuen privaten Schlüssel erstellen** geklickt und die vorgeschlagenen Kryptoeinstellungen und der vorgeschlagene Name der Zertifizierungsstelle bestätigt werden. Die Gültigkeitsdauer kann beliebig gewählt werden. Als Datenbankort können die Standardpfade verwendet werden.

Anschließend muss der AD-Server neu gestartet werden.

Dieses Zertifikat muss nun exportiert und auf das UCS-System kopiert werden: **Server-Manager -> AD-Zertifikatsdienste**. Dann ein Rechts-Klick auf den Server und Auswahl von **Zertifizierungsstelle**. Dort wird eine Rechnerliste angezeigt und unter jedem System die Elemente **Gesperrte Zertifikate**, **Ausgestellte Zertifikate**, **Ausstehende Anforderungen**, **Fehlgeschlagene Anforderungen** und **Zertifikatsvorlagen** angezeigt. Hier muss ein Rechtsklick auf den Rechnernamen erfolgen - nicht auf eines der Elemente darunter - und **Eigenschaften** ausgewählt werden. Das Root-Zertifikat heisst in der Regel *Zertifikat Nr. 0*. Dann **Zertifikat anzeigen -> Details -> In Datei kopieren -> DER-codiert-binär X.509 (.CER) -> Auswahl eines beliebigen Dateinamens und Speicherpfad -> Fertig stellen**.

9.3.3.2.4. Kopieren des AD-Zertifikats auf das UCS-System

Feedback

Nun muss das SSL-AD-Zertifikat über den Univention Management Console-Assistenten in das UCS-System importiert werden.

Dies erfolgt durch einen Klick auf **[Hochladen]** im Untermenü **Active Directory-Verbindung SSL-Konfiguration**.

Hierbei öffnet sich ein Fenster, in dem eine Datei ausgewählt wird. Das hochgeladene Zertifikat wird dadurch für den UCS AD-Connector verfügbar gemacht.

9.3.3.3. Start/Stopp des Active Directory Connectors

Feedback

Abschließend kann der Connector über **[Active Directory-Verbindungsdienst starten]** gestartet werden und bei Bedarf über **[Active Directory-Verbindungsdienst stoppen]** angehalten werden. Alternativ kann ein Starten/Stoppen auch über Kommandozeile durch die Befehle `/etc/init.d/univention-ad-connector start` und `/etc/init.d/univention-ad-connector stop` erfolgen.

9.3.3.4. Funktionstest der Grundeinstellungen

Feedback

Die korrekte Grundkonfiguration des Connectors lässt sich prüfen, indem vom UCS-System aus im Active Directory gesucht wird. Hier kann z.B. mit `univention-adsearch cn=Administrator` nach dem Administrator-Konto im Active Directory gesucht werden.

Da `univention-adsearch` auf die in Univention Configuration Registry-Variable gespeicherte Konfiguration zugreift, kann auf diesem Weg die Erreichbarkeit/Konfiguration des Active Directory-Zugriffs geprüft werden.

9.3.3.5. Änderung des AD-Zugriffspassworts

Feedback

Die vom UCS AD-Connector benötigten Zugangsdaten zum Active Directory werden über die Univention Configuration Registry-Variable `connector/ad/ldap/binddn` und `connector/ad/ldap/bindpw` konfiguriert. Falls das Passwort sich geändert hat oder ein anderes Benutzerkonto verwendet werden soll, können diese Variablen manuell angepasst werden. Über die Univention Configuration Registry-Variable `connector/ad/ldap/binddn` wird die LDAP-DN eines privilegierten Replikationsbenutzers konfiguriert. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Kennwort muss lokal auf dem UCS-System in eine Datei gespeichert werden, deren Dateiname in der Univention Configuration Registry-Variable `connector/ad/ldap/bindpw` eingetragen sein muss. Die Zugriffsrechte für die

Datei sollten so eingeschränkt werden, dass nur der Besitzer `root` Zugriff hat. Die folgenden Kommandos zeigen dies beispielhaft:

```
eval "$(ucr shell)"
echo "Updating ${connector_ad_ldap_bindpw?}"
echo "for AD sync user ${connector_ad_ldap_binddn?}"
touch "${connector_ad_ldap_bindpw?}"
chmod 600 "${connector_ad_ldap_bindpw?}"
echo -n "Current AD Syncuser password" > "${connector_ad_ldap_bindpw?}"
```

9.3.4. Werkzeuge / Fehlersuche

Feedback

Mit dem UCS AD-Connector werden einige Tools und Logdateien bereitgestellt:

9.3.4.1. `univention-adsearch`

Feedback

Dieses Tool ermöglicht die einfache LDAP-Suche im Active Directory. In AD gelöschte Objekte werden immer mit angezeigt (diese werden in AD weiterhin in einem LDAP-Unterbaum vorgehalten). Als erste Option erwartet das Skript einen LDAP-Filter, die zweite Option kann eine Liste der anzuzeigenden LDAP-Attribute sein, z.B.:

```
univention-adsearch cn=administrator cn givenName
```

9.3.4.2. `univention-connector-list-rejected`

Feedback

Dieses Tool führt die DNs nicht synchronisierter Objekte auf. Zusätzlich wird, sofern zwischengespeichert, die korrespondierende DN im jeweils anderen LDAP-Verzeichnis angegeben. Abschließend gibt *lastUSN* die ID der letzten von AD synchronisierten Änderung an.

9.3.4.3. Logdateien

Feedback

Zur Fehlersuche bei Synchronisationsproblemen finden sich entsprechende Meldungen in folgenden Dateien auf dem UCS-System:

```
/var/log/univention/connector.log
/var/log/univention/connector-status.log
```

9.3.5. Details zur vorkonfigurierten Synchronisation

Feedback

In der Grundeinstellung werden einige Container durch Filter von der Synchronisation ausgeschlossen. Diese finden sich in der Konfigurationsdatei `/etc/univention/connector/ad/mapping` unter der Einstellung *global_ignore_subtree*. Sollen einzelne Benutzer von der Synchronisation ausgeschlossen werden, können deren Benutzername der Univention Configuration Registry-Variable `connector/ad/mapping/user/ignorelist` hinzugefügt werden. Für mehr Flexibilität kann auch ein Filter in der Univention Configuration Registry-Variable `connector/ad/mapping/user/ignorefilter` angegeben werden. Dieser Filter unterstützt jedoch nicht die volle LDAP-Filter Syntax. Er ist immer abhängig von Groß- und Kleinschreibung und der Platzhalter "*" kann nur alleinstehend angegeben werden.

9.3.5.1. Container und Organisationseinheiten

Feedback

Container und Organisationseinheiten werden zusammen mit ihrer Beschreibung synchronisiert. Die Container `cn=mail` und `cn=kerberos` werden auf beiden Seiten ignoriert. Bei Containern sind einige Besonderheiten auf AD-Seite zu beachten. Active Directory bietet im **Manager für Benutzer und Gruppen** keine Möglichkeit, Container anzulegen. AD zeigt diese im erweiterten Modus aber an (**Ansicht -> Erweiterte Funktionen**).

9.3.5.1.1. Besonderheiten

Feedback

- Unter AD gelöschte Container oder Organisationseinheiten werden unter UCS rekursiv gelöscht, das bedeutet, dass evtl. nicht synchronisierte Unterobjekte, die in AD nicht zu sehen sind, ebenfalls entfernt werden.

9.3.5.2. Gruppen

Feedback

Gruppen werden anhand des Gruppennamens synchronisiert, dabei findet eine Berücksichtigung der primären Gruppe eines Benutzers statt (die unter AD nur am Benutzer im LDAP hinterlegt wird).

Gruppenmitglieder, die im anderen System z.B. aufgrund von Ignore-Filtern kein Gegenstück haben, werden ignoriert (bleiben also Mitglied der Gruppe).

Zusätzlich wird die Beschreibung der Gruppe synchronisiert.

9.3.5.2.1. Besonderheiten

Feedback

- Unter AD wird der *Prä-Windows 2000 Name* (LDAP-Attribut *samAccountName*) verwendet, daher kann eine Gruppe im Active Directory mit anderem Namen erscheinen als unter UCS.

- Der Connector ignoriert Gruppen, die im Univention Directory Manager unter **Samba Gruppentyp** als *Bekannte Gruppe* konfiguriert wurden. Eine Synchronisation von SID oder RID findet nicht statt.

- Gruppen, die im Univention Directory Manager unter **Samba Gruppentyp** als *Lokale Gruppe* konfiguriert wurden, werden vom Connector als *globale Gruppen* in das Active Directory synchronisiert.

- Neu angelegte oder verschobene Gruppen werden immer im gleichen Untercontainer auf der Gegenseite angelegt. Existieren während der Initialisierung gleichnamige Gruppen in unterschiedlichen Containern, werden die Mitglieder synchronisiert, nicht jedoch die Position im LDAP. Wird eine solche Gruppe auf einer Seite verschoben ist der Zielcontainer auf der anderen Seite identisch, so dass sich die DNs der Gruppen ab diesem Zeitpunkt nicht mehr unterscheiden.

- Bestimmte Gruppennamen werden anhand einer Mapping-Tabelle umgesetzt, so dass z.B. die UCS-Gruppe `Domain Users` mit der AD-Gruppe `Domänen-Benutzer`. synchronisiert wird. Dieses Mapping kann in englischsprachigen AD-Domänen dazu führen, das die deutschsprachigen Gruppen angelegt werden und sollte in diesem Fall deaktiviert werden. Dazu kann die Univention Configuration Registry-Variable `connector/ad/mapping/group/language` verwendet werden.

  Die vollständige Tabelle ist:

UCS-Gruppe	***AD-Gruppe***
`Domain Users`	`Domänen-Benutzer`
`Domain Admins`	`Domänen-Admins`
`Windows Hosts`	`Domänencomputer`

- Die Repräsentation von Gruppen in Gruppen unterscheidet sich zwischen AD und UCS. Sind unter UCS Gruppen Mitglieder von Gruppen, so können diese Objekte nicht immer auf AD-Seite synchronisiert werden und erscheinen in der Liste der zurückgewiesenen Objekte. Verschachtelte Gruppen sollten daher aufgrund der in Active Directory vorliegenden Einschränkungen immer nur dort zugewiesen werden.

- Wird im Univention Directory Manager eine globale Gruppe `A` als Mitglied einer anderen globalen Gruppe `B` aufgenommen, so erscheint diese Mitgliedschaft aufgrund von AD-internen Beschränkungen unter `Windows 2000/2003` nicht im Active Directory. Wird Gruppe `A` anschließend umbenannt, geht die Gruppenmitgliedschaft in Gruppe `B` verloren. Ab `Windows 2008` besteht diese Einschränkung nicht mehr, dort können im Active Directory auch globale Gruppen verschachtelt werden.

9.3.5.3. Benutzer

Feedback

Benutzer werden wie Gruppen anhand des Benutzernamens bzw. anhand des AD-Prä-Windows 2000 Namens synchronisiert. Direkt übermittelt werden die Attribute *Vorname*, *Nachname*, *primäre Gruppe* (sofern auf der anderen Seite vorhanden), *Organisation*, *Beschreibung*, *Straße*, *Stadt*, *PLZ*, *Profilpfad*, *Anmeldeskriptpfad*, *Deaktiviert* und *Kontoablaufdatum*. Indirekt werden zusätzlich *Passwort*, *Passwortablaufdatum* und *Ändern des Passwortes beim nächsten Login* synchronisiert. Vorbereitet, aber auf Grund unterschiedlicher Syntax in der Mapping-Konfiguration auskommentiert, sind *Primäre Mail-Adresse* und *Telefonnummer*.

Ausgenommen werden die Benutzer `root` und `Administrator`.

9.3.5.3.1. Besonderheiten

Feedback

- Benutzer werden ebenfalls anhand des Namens identifiziert, so dass für Benutzer, die vor der ersten Synchronisation auf beiden Seiten angelegt wurden, hinsichtlich der Position im LDAP das gleiche Verhalten gilt wie bei Gruppen.
- Es kann vorkommen, dass ein unter AD anzulegender Benutzer, dessen Passwort zurückgewiesen wurde, nach sofortigem erneuten Anlegen aus AD gelöscht wird. Grund dafür ist, das AD diesen Benutzer zunächst anlegt und nach dem Abweisen des Passwortes sofort wieder löscht. Werden diese Operationen nach UCS übertragen, werden sie auch wieder zurück nach AD übermittelt. Wurde der Benutzer auf AD-Seite schon vor der Rückübertragung der Operation erneut eingetragen, so wird er nach der Rückübertragung gelöscht. Das Auftreten dieses Verhaltens ist abhängig von dem eingestellten Polling-Intervall des Connectors.
- AD und UCS legen neue Benutzer per Voreinstellung in eine bestimmte primäre Gruppe (meist `Domain Users` bzw. `Domänen Benutzer`). Während der ersten Synchronisation von UCS nach AD werden die Benutzer daher immer in dieser Gruppe Mitglied.

9.4. Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover

Feedback

9.4.1. Einführung

Feedback

UCS unterstützt die Übernahme von Benutzern, Gruppen, Rechnerobjekten und Gruppenrichtlinienobjekten (GPOs) aus einer bestehenden Active Directory (AD)-Domäne. Die Windows-Clients müssen dabei nicht erneut der Domäne beitreten. Diese Übernahme ist ein interaktiver Prozess, der aus drei Phasen besteht:

- Kopieren aller Objekte aus Active Directory nach UCS
- Kopieren der Gruppenrichtliniendateien aus Active Directory nach UCS
- Abschalten des AD-Servers und Zuweisung der FSMO-Rollen auf den UCS-Domänencontroller

Die folgenden Voraussetzungen müssen für die Übernahme erfüllt sein:

- Der UCS-Domänencontroller (Domänencontroller Master) muss mit einem eindeutigen Rechnernamen installiert werden, der nicht in der AD-Domäne vorhanden ist.
- Der UCS-Domänencontroller muss mit demselben DNS-Domänennamen, NetBIOS-Domänennamen und Kerberos-Domänennamen installiert werden wie die AD-Domäne. Es wird empfohlen auch die selbe LDAP-Basis-DN zu verwenden.
- Der UCS-Domänencontroller muss eine IPv4-Adresse im selben Subnetz wie der zu übernehmende Active Directory-Domänencontroller verwenden.

Achtung

Sofern das System bereits Mitglied in einer Active Directory Domäne ist (Abschnitt 9.3.2), wird durch die Installation der *Active Directory Takeover* Applikation diese Mitgliedschaft entfernt. Deshalb sollte die Installation der *Takeover* Applikation erst kurz vor der eigentlichen Übernahme der Active Directory Domäne erfolgen.

Für die Migration muss die Applikation *Active Directory Takeover* aus dem Univention App Center installiert werden. Sie muss auf dem System installiert werden, auf dem der Univention S4 Connector läuft (siehe Abschnitt 9.2.2.4, normalerweise der Domänencontroller Master).

9.4.2. Vorbereitung

Feedback

Es wird empfohlen die folgenden Schritte durchzuführen, bevor die Übernahme initiiert wird:

- Ein Backup des/der AD-Server(s) sollte durchgeführt werden.
- Sind Benutzeranmeldungen auf dem AD-Server erlaubt (durch Domänenanmeldungen oder Terminalserversitzungen) wird empfohlen diese zu deaktiviert und alle Dienste zu stoppen die Daten verarbeiten (z.B. Mailserver). Dies stellt sicher das durch den Rollback auf ein Backup oder einen Snapshot keine Daten verloren gehen.
- Es wird empfohlen auf dem AD-Server dasselbe `Administrator`-Passwort zu verwenden wie in der UCS-Domäne. Werden verschiedene Passwörter verwendet, wird anhand der Zeitstempel verglichen welches Passwort aktueller ist und dieses verwendet.
- In der Grundeinstellung ist das lokale `Administrator` Konto auf dem AD-Server deaktiviert. Es sollte in der lokalen Benutzerverwaltung aktiviert werden.

Die Aktivierung des `Administrator`-Kontos wird empfohlen weil dieses Konto über die nötigen Berechtigungen verfügt um die Gruppenrichtlinien-Dateien in der SYSVOL-Freigabe zu kopieren. Der Benutzer kann entweder im AD-Verwaltungs-Tool für Benutzer und Gruppen oder mit den folgenden Kommandos auf der Kommandozeile aktiviert werden:

```
net user administrator /active:yes
net user administrator PASSWORT
```

9.4.3. Domänenmigration

Feedback

Die Übernahme muss auf dem UCS-Domänencontroller gestartet werden, auf dem der Univention S4 Connector läuft (normalerweise der Domänencontroller Master). Während der Übernahme sollte Samba nur auf diesem UCS-System laufen. Gibt es weitere Samba-Domänencontroller müssen diese angehalten werden. Dies ist wichtig um replikationsbedingte Dateninkonsistenzen zu vermeiden.

Andere Samba-Systeme können gestoppt werden, indem auf jedem UCS-Domänencontroller als Benutzer `root` folgender Befehl ausgeführt wird:

```
/etc/init.d/samba4 stop
```

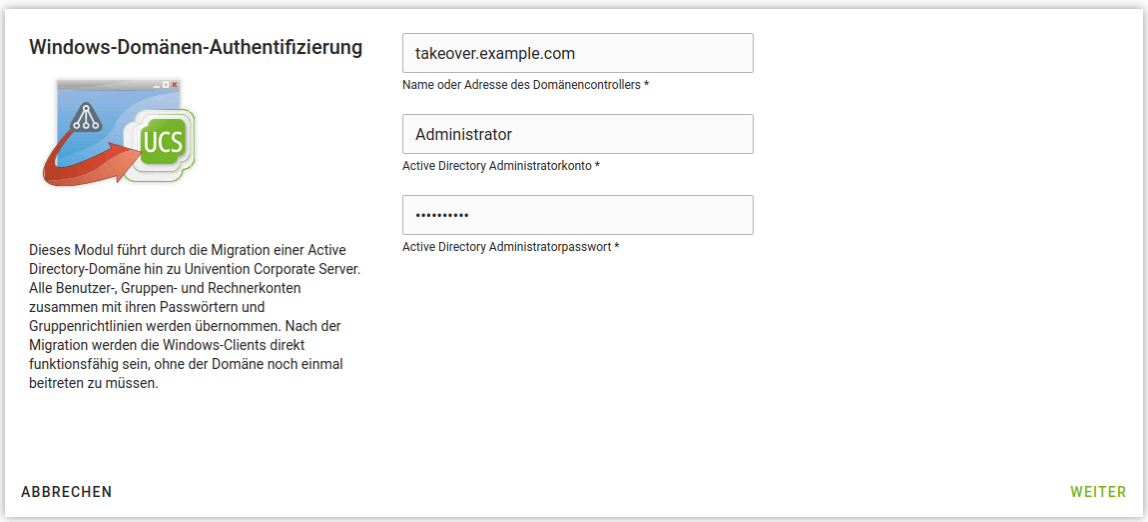
Nachdem sichergestellt wurde, dass keine anderen Samba-Domänencontroller laufen, kann die Übernahme beginnen. Wurde die UCS-Domäne mit einer UCS-Version vor 3.2 installiert muss zuerst die folgende Univention Configuration Registry-Variable gesetzt werden:

```
ucr set connector/s4/mapping/group/grouptype=false
```

Die Übernahme erfolgt mit dem Univention Management Console-Modul **Active Directory Takeover**. Unter **Name oder Adresse des Domänencontrollers** muss die IP-Adresse des AD-Systems angegeben werden.

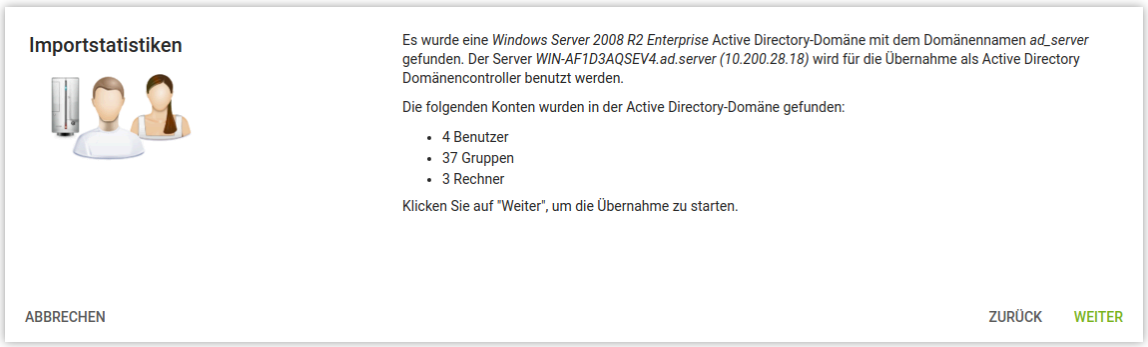
Unter **Active Directory Administratorkonto** muss ein Konto der AD-Domäne angegeben werden, das Mitglied der AD-Gruppe `Domain Admins` ist (z.B. der `Administrator`) und unter **Active Directory Administratorpasswort** das dazugehörige Passwort.

Abbildung 9.10. Erste Phase der Domänenmigration



Das Modul prüft, ob der AD-Domänencontroller erreicht werden kann und zeigt die zu migrierenden Domänendaten an:

Abbildung 9.11. Übersicht über die zu migrierenden Daten



Nach einem Klick auf **Weiter** werden die folgenden Schritte automatisch durchgeführt. Zusätzliche Informationen werden nach `/var/log/univention/ad-takeover.log` sowie nach `/var/log/univention/management-console-module-adtakeover.log` protokolliert.

- Anpassung der Systemzeit des UCS-Systems auf die Systemzeit der Active Directory-Domäne (wenn diese um mehr als drei Minuten nachgeht)
- Beitritt des UCS-Domänencontrollers in die Active Directory-Domäne
- Start von Samba und dem Univention S4 Connector zur Replikation der AD-Objekte in das UCS-OpenLDAP-Verzeichnis
- Wenn ein Benutzerkonto oder eine Gruppe mit einer "*Well Known*" RID nach UCS OpenLDAP synchronisiert wird, setzt ein Listener-Modul auf jedem UCS-System lokal eine Univention Configuration Registry Variable, die dem englischen Namen den nicht-englischen Namen zuordnet. Diese Variablen werden

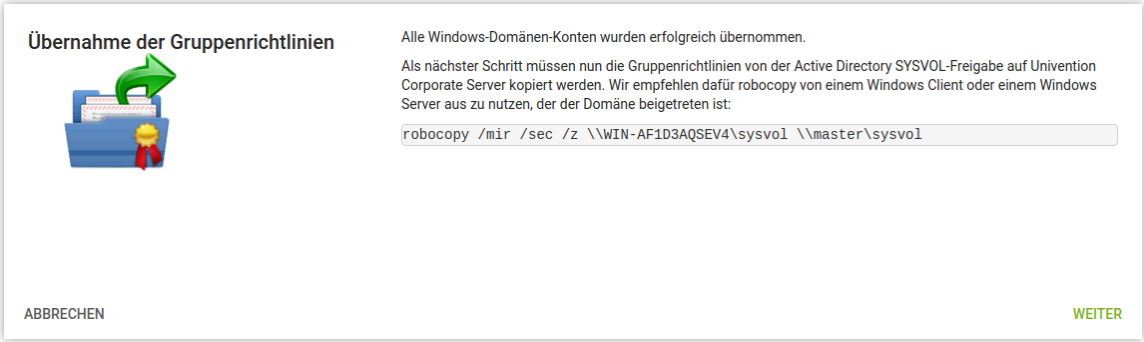
verwendet, um die in den UCS-Konfigurationsdateien verwendeten englischen Begriffe in die im Active Directory verwendeten Namen zu übersetzen. Wenn zum Beispiel `Domain Admins` einen anderen Namen im AD hat, dann wird die Univention Configuration Registry Variable `groups/default/domainadmins` auf den spezifischen Namen gesetzt (analog für Benutzer, z.B. `users/default/administrator`).

Nun enthält der UCS-Domänencontroller alle Benutzer, Gruppen und Rechner aus der Active Directory-Domäne. Im nächsten Schritt wird die SYSVOL-Freigabe kopiert, in der u.a. die Gruppenrichtlinien gespeichert werden.

Nun muss eine Anmeldung als `Administrator` am Active Directory-Domänencontroller erfolgen und dort die Dateien mit den Gruppenrichtlinien aus der SYSVOL-Freigabe des AD-Servers auf den UCS-Server kopiert werden.

Das aufzurufende Kommando wird im UMC-Modul angezeigt. Wenn es erfolgreich aufgerufen wurde, muss mit **Weiter** bestätigt werden.

Abbildung 9.12. Kopieren der Sysvol-Freigabe

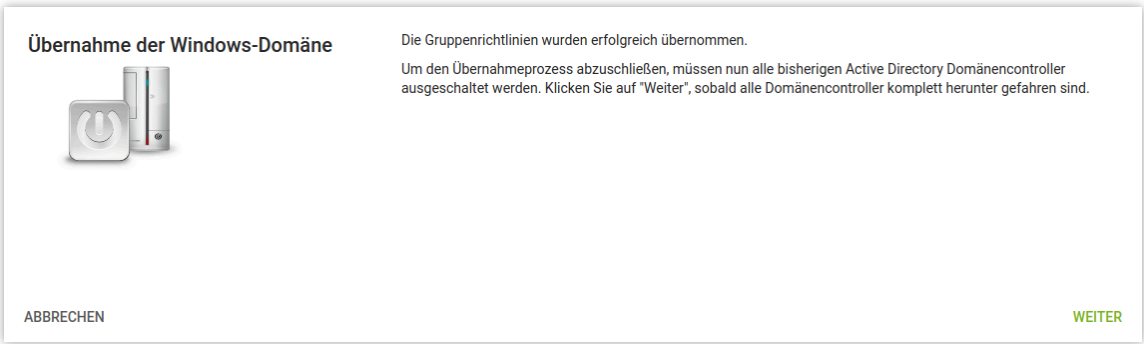


Wenn `robocopy` nicht vorhanden ist, kann es mit den Windows Server 2003 Resource Kit Tools nachinstalliert werden. Ab Windows 2008 ist es vorinstalliert.

Hinweis: Die `robocopy`-Option *`/mir`* spiegelt das Quellverzeichnis mit dem Zielverzeichnis. Es muss beachtet werden das bei einem erneuten Aufruf des Tools Dateien, die im Quellverzeichnis gelöscht wurden auch im Zielverzeichnis gelöscht werden.

Nach erfolgreichem Abschluss dieser Schritte sollten der/die AD-Domänencontroller heruntergefahren werden. Anschließend muss im UMC-Modul auf **Weiter** geklickt werden.

Abbildung 9.13. Herunterfahren des/der AD-Systeme



Die folgenden Schritte werden nun automatisch durchgeführt:

- Übertragung der FSMO-Rollen auf den UCS-Domänencontroller. Diese kennzeichnen verschiedene Aufgaben, die ein Server in einer AD-Domäne übernehmen kann.
- Einrichten des Rechnernamens des AD-Servers als DNS-Alias (siehe Abschnitt 11.2.2.2) für den UCS-Server
- Konfiguration der IP-Adresse des AD-Servers als zusätzliche virtuelle IP-Adresse des UCS-Servers
- Verschiedene Anpassungen, z.B. Entfernen des alten AD-Domänencontroller-Eintrags aus der Samba SAM-Datenbank.
- Abschließender Neustart von Samba und DNS-Server

9.4.4. Abschluss der Übernahme

Feedback

Abschließend müssen noch die folgenden Schritte durchgeführt werden:

- Der Domänenfunktionslevel der migrierten AD-Domäne muss mit dem folgenden Kommando geprüft werden:

```
samba-tool domain level show
```

Wenn das Kommando die Meldung *ATTENTION: You run SAMBA 4 on a forest function level lower than Windows 2000 (Native)* anzeigt müssen die folgenden Befehle aufgerufen werden:

```
samba-tool domain level raise --forest-level=2003 --domain-level=2003
samba-tool dbcheck --fix --yes
```

- Gab es in der migrierten AD-Domäne mehr als einen Domänencontroller, müssen die Rechnerkonten der weiteren Domänencontroller in der Rechnerverwaltung der UMC gelöscht werden. Außerdem müssen sie aus der Samba SAM-Datenbank gelöscht werden. Dies kann erfolgen, indem von einem migrierten Windows-Client eine Anmeldung als Mitglied der Gruppe `Domain Admins` erfolgt und das AD-Verwaltungstool für Benutzer und Computer aufgerufen wird.
- Gibt es weitere Samba-Domänencontroller, müssen diese neu der Domäne beitreten.
- Alle Windows-Clients müssen neu gestartet werden.

9.4.5. Tests

Feedback

Es wird empfohlen nach der Übernahme gründliche Tests mit Windows-Clients durchzuführen, z.B.:

- Anmeldung auf einem migrierten Client mit einem migrierten Benutzer
- Anmeldung auf einem migrierten Client als Administrator
- Test der Gruppenrichtlinien
- Domänenbeitritt eines neuen Windows-Clients
- Anlegen eines neuen Benutzers und Anmeldung an einem Windows-Client

9.5. Vertrauensstellungen

Feedback

Vertrauensstellungen zwischen Domänen ermöglichen es den Benutzern einer Domäne, sich an Rechnern einer anderen Domäne anzumelden.

Vertrauensstellungen können unidirektional oder bidirektional eingerichtet werden. Technisch entspricht eine bidirektionale Vertrauensstellung zwei unidirektional konfigurierten Vertrauensstellungen in beide Richtungen.

Die Terminologie von Vertrauensstellungen hängt von der Perspektive der vertrauenden oder der vertrauten Domäne ab: Aus Sicht der vertrauenden Domäne ist die Vertrauensstellung *ausgehend* und aus Sicht der vertrauten Domäne *eingehend*.

Ausgehende Vertrauensstellungen (UCS vertraut Windows) werden in Samba/AD-Domänen nicht unterstützt. Entsprechend werden auch keine bidirektionalen Vertrauensstellungen unterstützt.

Während der Einrichtung und Nutzung von Vertrauensstellungen müssen sich die Domänencontroller der beiden Domänen über das Netzwerk erreichen und gegenseitig per DNS identifizieren können. Zumindest die voll qualifizierten DNS Namen der Domänencontroller der jeweils anderen Domäne müssen auflösbar sein, damit die Kommunikation zwischen den Domänen funktioniert. In beiden Domänen richtet man zu diesem Zweck eine bedingtes DNS Weiterleitung ein.

Für das folgende Beispiel sei angenommen, dass der UCS Samba/AD DC Master `master.ucsdom.example` die IP-Adresse `192.0.2.10` hat und dass der Active Directory Domänencontroller `dc1.addom.example` der entfernten Domäne die IP-Adresse `192.0.2.20` hat.

Auf der UCS-Seite lässt sich die bedingte Weiterleitung von DNS-Anfragen mit folgenden Schritten als `root` einrichten:

```
cat >> /etc/bind/local.conf.samba4 <<%EOR

zone "addom.example" {
type forward;
forwarders { 192.0.2.20; };
};
%EOR
service bind9 restart
```

Der Erfolg kann mit überprüft werden mit `host dc1.addom.example`.

Zusätzlich kann es sinnvoll sein, für den Domänencontroller der entfernten Active Directory Domäne einen statischen Eintrag in der Datei `/etc/hosts` anzulegen:

```
ucr set hosts/static/192.0.2.20=dc1.addom.example
```

Auf dem Windows AD DC kann über die DNS-Server Konsole eine sogenannte Bedingte Weiterleitung (*Conditional Forwarding*) für die UCS-Domäne eingerichtet werden.

Nach dieser Vorarbeit kann die Vertrauensstellung direkt von der Kommandozeile des UCS Samba/AD DCs eingerichtet werden.

Vertrauensstellungen können nur auf Domänencontrollern eingerichtet werden, gelten dann aber für die gesamte Domäne.

In Samba/AD Domänen ist diese Konstellation sehr einfach an der Kommandozeile über das Werkzeug `samba-tool` einzurichten:

```
samba-tool domain trust create addom.example \
          -k no -UADDOM\\Administrator%ADAdminPassword \
          --type=external --direction=incoming
```

Mit folgenden Kommandos kann die Vertrauensstellung überprüft werden:

```
samba-tool domain trust list
wbinfo --ping-dc –domain=addom.example
wbinfo --check-secret –domain=addom.example
```

Nach der Einrichtung sollte sich ein Benutzer an Systemen der Windows Active Directory Domäne anmelden können. Als Login-Name muss dabei entweder das Format `UCSDOM\username` oder der Kerberos Prinzipal in der Notation `username@ucsdom.example` angegeben werden.

Kapitel 10. Identity Management Anbindung an Cloud-Dienste

10.1. Einführung

Feedback

UCS bietet ein integriertes Identity Management System. Über Univention Management Console können u.a. Benutzer oder Gruppen sehr einfach administriert werden. Abhängig von den installierten Diensten stehen diese Identitäten über unterschiedliche Schnittstellen bereit, bspw. via LDAP.

Mit Hilfe von bereitgestellten Erweiterungen, sogenannten Apps, kann das Managementsystem so erweitert werden, dass Benutzer oder Gruppen auch direkt in Cloud-Dienste repliziert werden. Im App Center sind u.a. Erweiterung für Microsoft 365 oder G Suite vorhanden.

Dank Single Sign-on (SSO) können sich die Benutzer mit ihrem gewohnten Passwort anmelden und anschließend sofort online in der Cloud arbeiten. Dabei bleibt das Passwort im Unternehmensnetzwerk und wird nicht zum Cloud Dienst übertragen.

In den folgenden Kapiteln ist die Einrichtung des Microsoft 365 und des Google Apps for Work Connector beschrieben.

10.2. Microsoft 365 Connector

Feedback

Der Microsoft 365 Connector ermöglicht die Synchronisation der Benutzer, Gruppen und Teams zu einer Azure Active Directory Domäne, welche von Microsoft 365 verwendet wird. Dabei lässt sich steuern, welche der in UCS angelegten Benutzer Microsoft 365 verwenden dürfen. Die so ausgewählten Benutzer werden entsprechend von UCS in die Azure Active Directory Domäne provisioniert. Es kann dabei konfiguriert werden, welche Attribute synchronisiert werden und Attribute können dabei anonymisiert werden.

Die Single Sign-on Anmeldung an Microsoft 365 erfolgt über die in UCS integrierte SAML-Implementierung, d.h. die Authentifizierung erfolgt dabei gegen den UCS-Server und es werden keine Passwort-Hashes zu Microsofts Azure Cloud übertragen. Die Authentifikation des Benutzers erfolgt ausschließlich über den Webbrowser des Clients. Dieser sollte aber die DNS-Namen der UCS-Domäne auflösen können, das ist insbesondere für Mobilgeräte wichtig zu beachten.

10.2.1. Einrichtung

Feedback

Für den Einsatz des Microsoft 365 Connectors wird ein Microsoft 365 Administrator Konto, ein entsprechendes Konto im Azure Active Directory, sowie eine von Microsoft verifizierte Domäne[1] benötigt. Die ersten

[1] https://azure.microsoft.com/de-de/documentation/articles/active-directory-add-domain/

beiden werden zu Testzwecken kostenlos von Microsoft bereitgestellt. Für das Konfigurieren des SSO wird jedoch eine eigene Internet-Domäne benötigt, in der TXT-Records erstellt werden können.

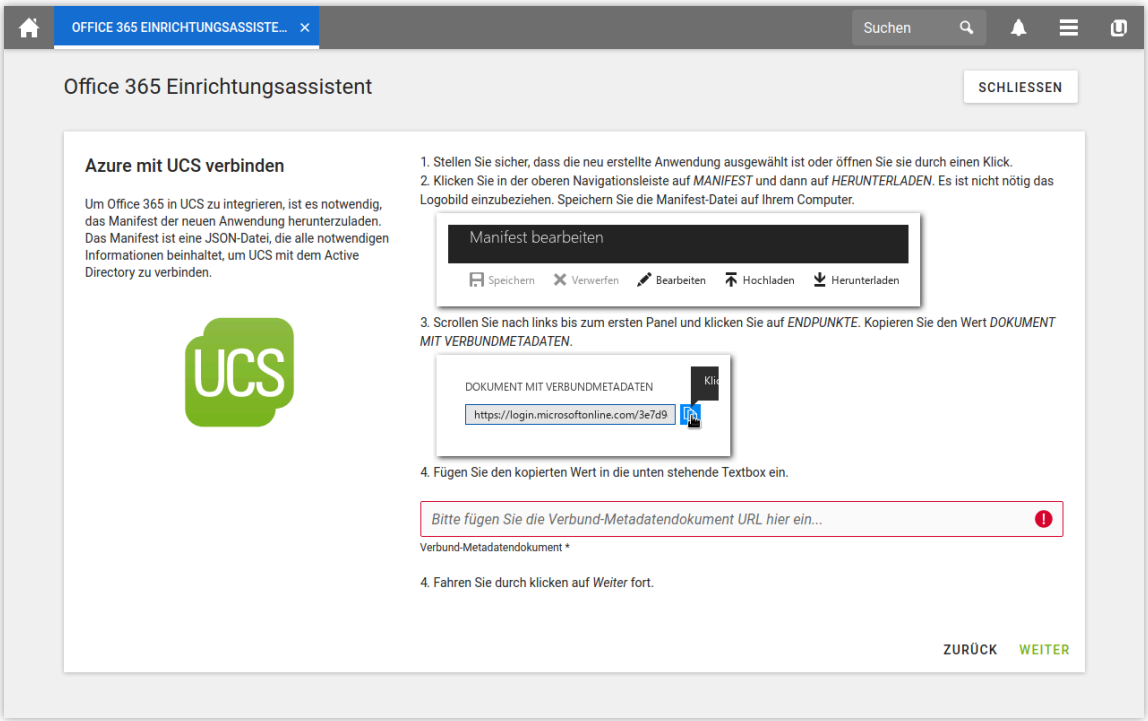
Falls noch keine Microsoft 365 Subskription vorhanden ist, so kann diese via https://www.office.com/ im Bereich **kostenlos testen für Unternehmen** konfiguriert werden. Mit einem privaten Microsoft Konto ist eine Verbindung nicht möglich.

Anschließend sollte eine Anmeldung mit einem **Microsoft 365 Administratorkonto** im **Microsoft 365 Admin Center** erfolgen. In der linken Navigationsleiste ganz unten ist **Azure AD** auszuwählen, welches in einem neuen Fenster das **Azure Management Portal** öffnet.

Unter dem Menüpunkt **Domänen** kann nun die eigene Domäne hinzugefügt und verifiziert werden. Dafür ist es notwendig, einen TXT-Record im DNS der eigenen Domäne zu erzeugen. Dieser Vorgang kann einige Minuten in Anspruch nehmen. Anschließend sollte der **Status** der konfigurierten Domäne als **überprüft** angezeigt werden.

Nun kann die Microsoft 365 App aus dem App Center auf dem UCS System installiert werden. Die Installation dauert nur wenige Minuten. Anschließend steht ein Einrichtungsassistent (Wizard) für die Einrichtung zur Verfügung. Mit Abschluss des Einrichtungsassistenten ist die Installation abgeschlossen und der Connector ist einsatzbereit.

Abbildung 10.1. Microsoft 365 Einrichtungsassistent



10.2.2. Konfiguration

Feedback

Nach der Einrichtung über den Einrichtungsassistenten kann über das Benutzermodul an jedem Benutzerobjekt auf dem Reiter **Microsoft 365** konfiguriert werden, dass dieser Benutzer ins Microsoft 365 provisioniert wird. Der Verbrauch und die Zuweisung von Lizenzen ist im **Microsoft 365 Admin Center** zu erkennen.

10.2.2.1. Benutzer

Feedback

Wird eine Änderung am Benutzer durchgeführt, so werden die Änderungen auch in die Azure Active Directory Domäne repliziert. Es erfolgt keine Synchronisation aus dem Azure Active Directory in das UCS System.

Das bedeutet Änderungen, die im Azure Active Directory oder Office Portal vorgenommen, können durch Änderungen an den gleichen Attributen in UCS unter Umständen wieder überschrieben werden.

Aufgrund von Sicherheitsrichtlinien des Azure Active Directory können Benutzer oder Gruppen im Azure AD während der Synchronisation nicht gelöscht werden. Sie werden lediglich deaktiviert und umbenannt. Die Lizenzen werden im Azure Active Directory entzogen, so dass diese für andere Benutzer zur Verfügung stehen. Benutzer und Gruppen, deren Namen mit **ZZZ_deleted** anfangen, können im **Microsoft 365 Admin Center** gelöscht werden.

Es ist notwendig in Microsoft 365 ein Land für den Benutzer zu konfigurieren. Der Connector nutzt dafür die Angabe des Landes aus den Kontaktdaten des Benutzers oder, wenn nicht gesetzt, die Einstellung des Servers. Mit Hilfe der Univention Configuration Registry-Variable `office365/attributes/usageLocation` kann ein 2-Zeichen-Kürzel, bspw. DE vorgegeben werden.

Über die Univention Configuration Registry-Variable `office365/attributes/sync` wird konfiguriert, welche LDAP Attribute (z. B. Vorname, Nachname, etc.) eines Benutzerkontos synchronisiert werden. Es handelt sich um eine kommaseparierte Liste von LDAP Attributen. Somit ist eine Anpassung an die eigenen Bedürfnisse einfach möglich.

Mit der Univention Configuration Registry-Variable `office365/attributes/anonymize` können kommasepariert LDAP Attribute angegeben werden, die zwar im Azure Active Directory angelegt, jedoch mit Zufallswerten gefüllt werden. Die Univention Configuration Registry-Variablen `office365/attributes/static/.*` erlauben das Füllen von Attributen auf Microsoft Seite mit einem vordefinierten Wert.

Mit der Univention Configuration Registry-Variable `office365/attributes/never` können kommasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese in `office365/attributes/sync` oder `office365/attributes/anonymize` auftauchen.

Die Univention Configuration Registry-Variablen `office365/attributes/mapping/.*` definieren eine Abbildung der UCS LDAP Attribute zu Azure Attributen. Diese Variablen müssen normalerweise nicht verändert werden. Die Synchronisation der Gruppen der Microsoft 365 Benutzer kann mit der Univention Configuration Registry-Variable `office365/groups/sync` aktiviert werden.

Änderungen an Univention Configuration Registry-Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

10.2.2.2. Teams

Feedback

Für die Nutzung von Teams muss die Synchronisation von Gruppen per Univention Configuration Registry-Variable `office365/groups/sync=yes` aktiviert werden, anschließend muss der Dienst Univention Directory Listener neugestartet werden. Sollen UCS-Gruppen als Teams in Microsoft 365 angelegt werden, so müssen die Gruppen auf dem Reiter **Microsoft 365** über die Checkbox **Microsoft 365 Team** als Team konfiguriert werden. Des Weiteren ist es notwendig, auf demselben Reiter einen Besitzer des Teams zu definieren. Weitere Einstellungen am Team können von den Team-Besitzern direkt im Teams Interface vorgenommen werden. Nach der Aktivierung einer Gruppe als Team werden die Gruppenmitglieder dem neuen Team hinzugefügt. Die Provisionierung eines neuen Teams in Microsoft 365 kann einige Minuten in Anspruch nehmen.

Es muss sichergestellt sein, dass die Benutzer eines Teams in Azure eine Lizenz erhalten, in der die Nutzung von Teams enthalten ist.

10.2.3. Synchronisation von Benutzern in mehrere Azure *Active Directories*

Feedback

Der Microsoft 365 Connector kann Benutzer in mehrere Azure *Active Directories* synchronisieren. Sind mehrere Verbindungen verfügbar, können an jedem Benutzerkonto individuell die Azure AD Instanzen zugewie-

sen werden, in denen ein Account erstellt werden soll. Ein Benutzer bekommt in jedem der seinem UCS Konto zugewiesenen Azure AD ein separates Konto mit eindeutigem Benutzernamen (*Userprincipalname*, UPN).

Jede zusätzlich eingerichtete Azure AD Verbindung erhält einen vom Administrator festzulegenden Verbindungsalias als eindeutigen Namen. Für die Verwaltung der Aliase kann das Programm `/usr/share/univention-office365/scripts/manage_adconnections` verwendet werden. Ein neuer Alias kann über das Kommando `/usr/share/univention-office365/scripts/manage_adconnections create <Aliasname>` erstellt werden. Dies konfiguriert unter anderem die Univention Configuration Registry-Variable `office365/adconnection/wizard` auf den neu erstellten Alias um. Der Wert dieser Univention Configuration Registry-Variable bestimmt, welche Azure Verbindung durch den Microsoft 365 Einrichtungswizard konfiguriert wird.

Nach dem Anlegen muss die Verbindung wie gewohnt über den Microsoft 365 Einrichtungswizard eingerichtet werden, damit Benutzer synchronisiert werden können.

Um Single-Sign-On mit mehreren Azure AD Verbindungen zu ermöglichen, muss für jede weitere Verbindung ein neuer logischer SAML Identity Provider erstellt werden. Dies ist in Abschnitt 3.9.3 beschrieben. -er Identity Provider sollte dabei denselben Namen wie der Verbindungsalias erhalten. Wurde ein anderer Name gewählt, muss das PowerShell Skript zur Einrichtung der Single-Sign-On Verbindung manuell angepasst werden. Auf allen für das Single-Sign-On der Domäne zuständigen Domaincontrollern muss also beispielsweise die Univention Configuration Registry-Variable in der Form `saml/idp/entityID/supplement/Aliasname=true` gesetzt werden.

Ein UCS Benutzer kann in einer Browser-Sitzung nur zu einem Azure AD gleichzeitig verbunden sein. Um die Verbindung zu wechseln, ist ein Abmelden an Microsoft 365 notwendig.

Zur weiteren Konfiguration gibt es die Univention Configuration Registry-Variable `office365/defaultalias`. Diese legt fest, in welches Azure AD ein Benutzer- oder Gruppenkonto synchronisiert wird, falls am Benutzerkonto keines explizit ausgewählt wurde. Soll das Konto in ein anderes Azure AD synchronisiert werden, muss bei der Aktivierung für Microsoft 365 das entsprechende Azure AD Verbindungsalias als Ziel ausgewählt werden.

10.2.4. Fehlersuche

Feedback

Meldungen während der Einrichtung werden in der folgenden Logdatei `/var/log/univention/management-console-module-office365.log` protokolliert.

Bei Synchronisationsproblemen sollte die Logdatei des Univention Directory Listener geprüft werden: `/var/log/univention/listener.log`. Einige Aktionen des Connectors verwenden Operationen der Azure Cloud mit langer Laufzeit, insbesondere bei der Verwendung von Teams. Diese Operationen werden in der Logdatei `/var/log/univention/listener_modules/ms-office-async.log` protokolliert. Mit Hilfe der Univention Configuration Registry-Variable `office365/debug/werror` können mehr Debugausgaben aktiviert werden.

10.3. Google Apps for Work Connector

Feedback

Der Google Apps for Work Connector ermöglicht die Synchronisation der Benutzer und Gruppen zu einer G Suite Domäne. Dabei lässt sich steuern, welche der in UCS angelegten Benutzer G Suite verwenden dürfen. Die so ausgewählten Benutzer werden entsprechend von UCS in die G Suite Domäne provisioniert. Es kann dabei konfiguriert werden, welche Attribute synchronisiert werden und Attribute können dabei anonymisiert werden.

Die Single Sign-on Anmeldung an G Suite erfolgt über die in UCS integrierte SAML-Implementierung, d.h. die Authentifizierung erfolgt dabei gegen den UCS-Server und es werden keine Passwort-Hashes zur G Suite Domäne übertragen. Die Authentifikation des Benutzers erfolgt ausschließlich über den Webbrowser des Clients. Dieser sollte aber die DNS-Namen der UCS-Domäne auflösen können, das ist insbesondere für Mobilgeräte wichtig zu beachten.

10.3.1. Einrichtung

Feedback

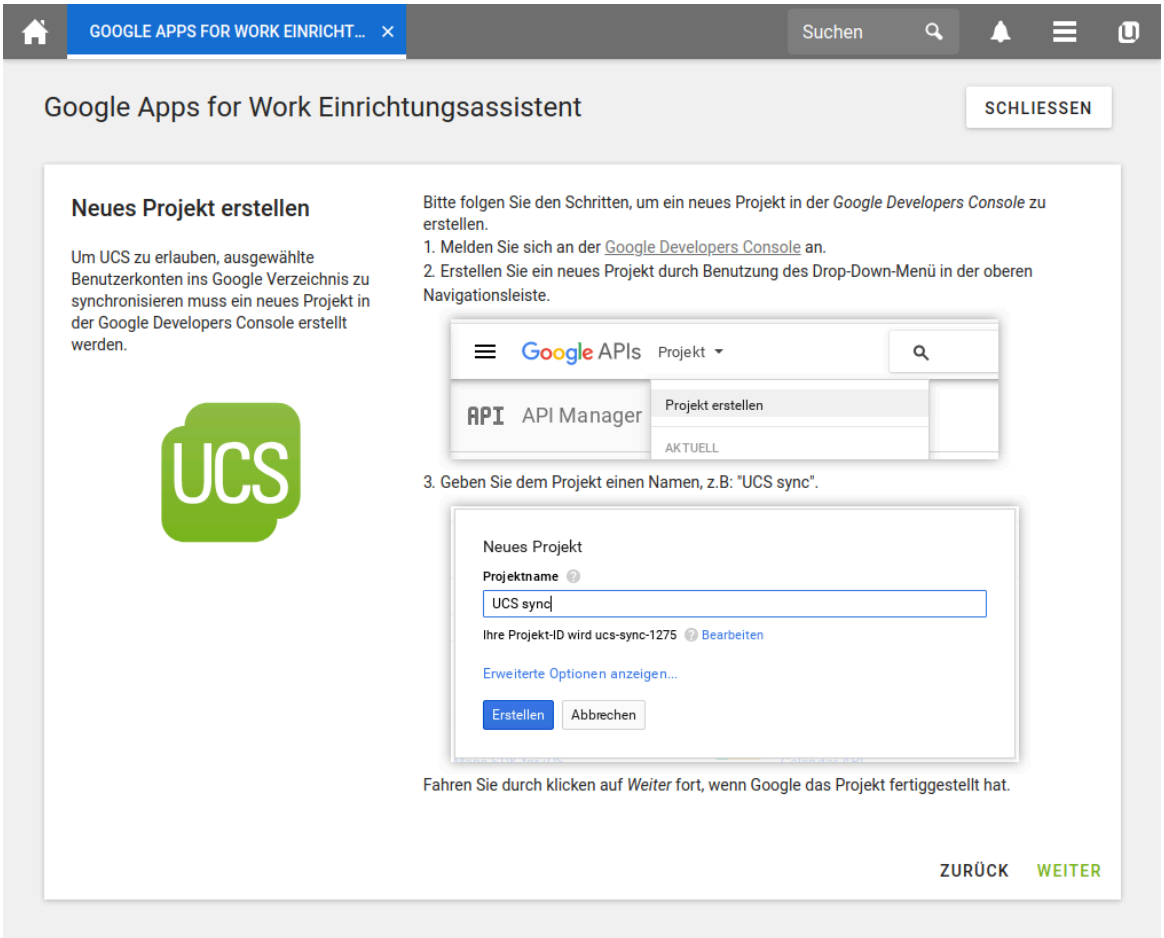
Für den Einsatz des Google Apps for Work Connectors wird ein G Suite Administrator Konto, ein entsprechendes Konto in der G Suite Domäne, sowie eine von Google verifizierte Domäne[2] benötigt. Die ersten beiden werden zu Testzwecken kostenlos von Google bereitgestellt. Für das Konfigurieren des SSO wird jedoch eine eigene Internet-Domäne benötigt, in der TXT-Records erstellt werden können.

Falls noch keine G Suite Subskription vorhanden ist, so kann diese via https://gsuite.google.com/setup-hub/ mit dem Link **Jetzt kostenlos testen** konfiguriert werden. Mit einem privaten Gmail Konto ist eine Verbindung nicht möglich.

Anschließend sollte eine Anmeldung mit einem **G Suite Administratorkonto** in der Admin-Konsole[3] erfolgen. Nun sollte die Verifikation der Domäne erfolgen. Dafür ist es notwendig, einen TXT-Record im DNS der eigenen Domäne zu erzeugen. Dieser Vorgang kann einige Minuten in Anspruch nehmen.

Nun kann der Google Apps for Work Connector aus dem App Center auf dem UCS System installiert werden. Die Installation dauert nur wenige Minuten. Anschließend steht ein Einrichtungsassistent (Wizard) für die Einrichtung zur Verfügung. Mit Abschluss des Einrichtungsassistenten ist die Installation abgeschlossen und der Connector ist einsatzbereit.

Abbildung 10.2. Google Apps for Work Einrichtungsassistent



[2] https://support.google.com/a/topic/9196?hl=de
[3] https://admin.google.com/

10.3.2. Konfiguration

Feedback

Nach der Einrichtung über den Einrichtungsassistenten kann über das Benutzermodul an jedem Benutzerobjekt auf dem Reiter **Google Apps** konfiguriert werden, dass dieser Benutzer zu G Suite provisioniert wird.

Wird eine Änderung am Benutzer durchgeführt, so werden die Änderungen auch in die G Suite Domäne repliziert. Es erfolgt keine Synchronisation aus der G Suite Domäne in das UCS-System. Das bedeutet Änderungen, die in der G Suite Domäne vorgenommen wurden, können durch Änderungen an den gleichen Attributen in UCS unter Umständen wieder überschrieben werden.

Wird bei einem Benutzer die Google Apps Eigenschaft entfernt, so wird der Benutzer entsprechend in der G Suite Domäne gelöscht.

Über die Univention Configuration Registry-Variable `google-apps/attributes/mapping/.*` wird konfiguriert, welche LDAP Attribute (z. B. Vorname, Nachname, etc.) eines Benutzerkontos synchronisiert werden. Die Univention Configuration Registry-Variable und ihre Werte spiegeln die verschachtelte Datenstruktur der G Suite Benutzerkonten wider. Die Namen, die in den Werten dem Prozentzeichen folgen, sind die Attribute im UCS LDAP. Werden alle Univention Configuration Registry-Variablen `google-apps/attributes/mapping/.*` entfernt, so werden keine Daten außer der primären E-Mail-Adresse synchronisiert.

Mit der Univention Configuration Registry-Variable `google-apps/attributes/anonymize` können kommasepariert LDAP Attribute angegeben werden, die zwar in der G Suite Domäne angelegt, jedoch mit Zufallswerten gefüllt werden.

Mit der Univention Configuration Registry-Variable `google-apps/attributes/never` können kommasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese per `google-apps/attributes/mapping` oder `google-apps/attributes/anonymize` konfiguriert sind.

Die Synchronisation der Gruppen der Google Apps for Work Benutzer kann mit der Univention Configuration Registry-Variable `google-apps/groups/sync` aktiviert werden.

Änderungen an Univention Configuration Registry-Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

10.3.3. Fehlersuche

Feedback

Meldungen während der Einrichtung werden in der folgenden Logdatei `/var/log/univention/management-console-module-googleapps.log` protokolliert.

Bei Synchronisationsproblemen sollte die Logdatei des Univention Directory Listener geprüft werden: `/var/log/univention/listener.log`. Mit Hilfe der Univention Configuration Registry-Variable `google-apps/debug/werror` können mehr Debugausgaben aktiviert werden.

univention
be open.

Kapitel 11. IP- und Netzverwaltung

Dieses Kapitel beschreibt wie IP-Adressen für die in einer UCS-Domäne verwalteten Rechnersysteme zentral über Univention Management Console verwaltet und per DHCP zugewiesen werden können.

Netzwerk-Objekte (Abschnitt 11.1) fassen verfügbare IP-Adressbereiche eines Netzes zusammen. Die DNS-Auflösung sowie die Vergabe von IP-Adressen über DHCP sind in UCS integriert und werden genauer in Abschnitt 11.2 sowie Abschnitt 11.3 erläutert.

Ein- und ausgehende Netzwerkverbindungen können über die in UCS integrierte *Univention Firewall* auf Basis von `iptable` begrenzt werden (Abschnitt 11.4).

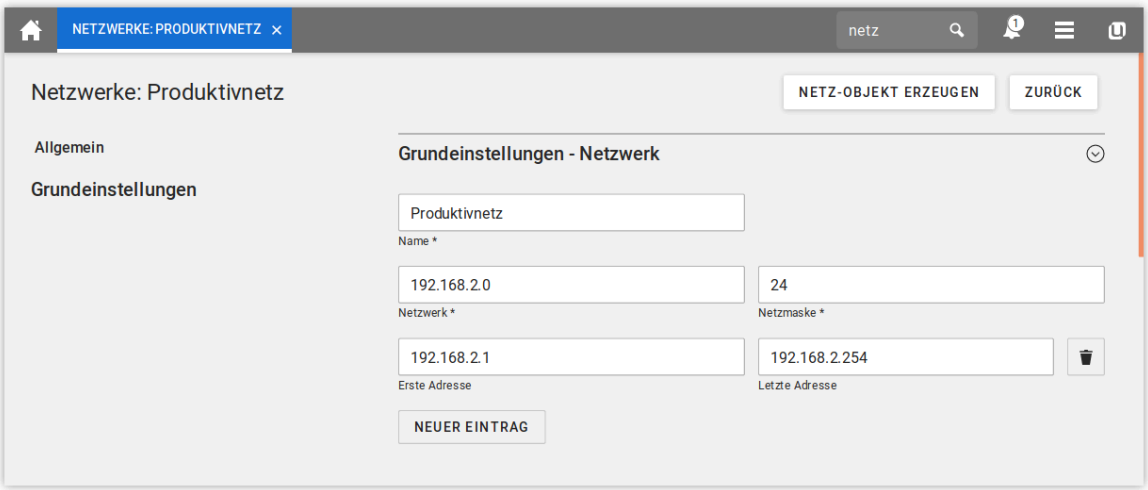
Die Integration des Proxy-Servers Squid ermöglicht das Zwischenspeichern von Web-Inhalten und die Umsetzung inhaltlicher Richtlinien für den Web-Zugriff (Abschnitt 11.5).

11.1. Netzwerk-Objekte

Feedback

Mit *Netzwerk-Objekten* lassen sich Eigenschaften eines Netzes zentral erfassen, z.B. die verfügbaren IP-Adressen und die DNS- und DHCP-Zonen, in denen die Systeme angesiedelt sind.

Abbildung 11.1. Erstellen eines Netzwerk-Objekts



So kann beispielsweise ein Netzwerk-Objekt *Produktivnetz* definiert werden, das sich über die IP-Adressen von `192.0.2.0` bis `192.0.2.254` erstreckt. Wird nun ein Windows-Rechnerobjekt angelegt, muss nun nur das Netzwerk-Objekt ausgewählt werden. Es wird dann intern geprüft, welche der IP-Adressen des Netzes bereits vergeben sind und die nächste freie ausgewählt. Wird ein Rechnerobjekt entfernt, wird die Adresse automatisch wieder neu vergeben. Dies erspart dem Administrator eine manuelle Verwaltung verfügbarer Adressen.

Für Netzwerk-Objekte können sowohl IPv4-, als auch IPv6-Adressen verwendet werden.

Netzwerk-Objekte werden im UMC-Modul *Netzwerke* verwaltet (siehe auch Abschnitt 4.4).

Tabelle 11.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name	In diesem Eingabefeld ist der Name des Netzwerks einzutragen. Unter diesem Namen erscheint das Netzwerk auch in der Rechnerverwaltung.
Netzwerk	In diesem Eingabefeld muss die Netzwerk-Adresse in Oktettschreibweise eingetragen werden, z.B. `192.0.2.0`
Netzmaske	Die Netzmaske kann in diesem Eingabefeld wahlweise als Bitzahl (Netzpräfix) oder in Oktettschreibweise eingetragen werden. Wenn die

Attribut	Beschreibung
	Netzmaske in Oktettschreibweise eingegeben wird, wird sie automatisch in den entsprechenden Netzpräfix umgewandelt und später auch ausgegeben.
IP-Adressbereich	In diesem Feld können ein oder mehrere IP-Adressbereiche angelegt werden. Wenn später ein Gerät diesem Netzwerk zugeordnet werden soll, wird dem Gerät automatisch die nächste freie IP-Adresse aus den hier eingetragenen IP-Adressbereichen zugewiesen. Wenn an dieser Stelle kein IP-Adressbereich eingerichtet wird, verwendet das System automatisch den Bereich, der sich aus dem Netzwerk und der Netzmaske ergibt. Im Untermenü **DNS-Einstellungen** können Forward Lookup Zone und Reverse Lookup Zone ausgewählt werden. Wird später ein Gerät diesem Netzwerk zugeordnet, wird für das Gerät automatisch ein Host Record in der Forward Lookup Zone beziehungsweise ein Pointer Record in der Reverse Lookup Zone angelegt. Die Zonen werden ebenfalls in Univention Management Console verwaltet, siehe Abschnitt 11.2.2.1. Wird hier keine Zone ausgewählt, werden bei der Zuweisung zu einem Rechnerobjekt keine DNS-Records angelegt. Die DNS-Einträge können aber weiterhin manuell gesetzt werden.
Forward Lookup Zone für DNS-Einträge	Hier ist die Forward Lookup Zone anzugeben, in die Geräte aus diesem Netzwerk eingetragen werden sollen. Über diese Zone wird die Auflösung des Rechnernamens zu einer IP-Adresse durchgeführt.
Reverse Lookup Zone für DNS-Einträge	Hier ist die Reverse Lookup Zone anzugeben, in die Geräte aus diesem Netzwerk eingetragen werden sollen. Über diese Zone wird die Rückwärtsauflösung der IP-Adresse zu einem Rechnernamen durchgeführt. Im Untermenü **DHCP-Einstellungen** kann dem Netzwerk ein DHCP-Service zugeteilt werden. Wird später ein Gerät diesem Netzwerk zugeordnet, wird für das Gerät automatisch ein DHCP-Rechner-Eintrag mit der festen IP-Adresse unterhalb des gewählten DHCP-Services angelegt. Die DHCP-Service-Einstellungen werden ebenfalls in Univention Management Console verwaltet, siehe Abschnitt 11.3.2. Wird hier keine DHCP-Service ausgewählt, wird bei der Zuweisung zu einem Rechnerobjekt kein DHCP-Rechner-Eintrag angelegt. Ein solcher Eintrag kann aber weiterhin manuell zugewiesen werden.

11.2. Verwaltung von DNS-Daten mit BIND

Feedback

UCS integriert BIND für die Namensauflösung über das Domain Name System (DNS). Die meisten DNS-Funktionen werden für die DNS-Auflösung in der lokalen Domäne verwendet, die UCS-BIND-Integration kann aber prinzipiell auch für einen öffentlichen Nameserver eingesetzt werden.

Auf allen Domänencontroller-Systemrollen ist BIND immer verfügbar, eine Installation auf anderen Systemrollen wird nicht unterstützt.

Die Konfiguration der von einem UCS-System zu verwendenden Nameserver ist in Abschnitt 8.2.4 dokumentiert.

Folgende DNS-Daten werden unterschieden:

- Eine *Forward Lookup Zone* enthält Informationen, die zum Auflösen von DNS-Namen in IP-Adressen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen authoritativen, primären Nameserver, dessen Informationen für eine Zone maßgeblich sind. Untergeordnete Server synchronisieren sich mit dem authoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA-Record*.

- Der *MX-Record* einer Forward Lookup Zone ist eine für das E-Mail-Routing notwendige DNS-Information. Er verweist auf den Rechner, der für eine Domäne Mails entgegennimmt.

- *TXT-Records* enthalten menschenlesbaren Text und können beschreibende Informationen zu einer Forward Lookup Zone enthalten.

- Ein *CNAME-Record* (desweiteren auch als *Alias-Record* bezeichnet) verweist auf einen vorhandenen, kanonischen DNS-Namen. So kann beispielsweise der kanonische Rechnername des Mailservers einen Alias-Eintrag *mailserver* erhalten, der dann in die Mail-Clients eingetragen wird. Zu einem kanonischen Namen können beliebig viele CNAME-Records definiert werden.

- Ein *A-Record* (unter IPv6 *AAAA-Record*) weist einem DNS-Namen eine IP-Adresse zu. A-Records werden in UCS auch als *Host-Records* bezeichnet.

- Mit einem *SRV-Record* (in UCS als *Service Record* bezeichnet) kann im DNS Informationen über verfügbare Systemdienste hinterlegt werden. In UCS werden Service Records u.a. verwendet, um LDAP-Server oder den Domänencontroller Master domänenweit bekannt zu machen.

- Eine *Reverse Lookup Zone* enthält Informationen, die zur Auflösung von IP-Adressen in DNS-Namen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen authoritativen, primären Nameserver, dessen Informationen für eine Zone massgeblich sind. Untergeordnete Server synchronisieren sich mit dem authoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA Record*.

- Ein *PTR-Record (Pointer Record)* erlaubt die Auflösung einer IP-Adresse in einen Rechnernamen. Er stellt damit in einer Reverse Lookup Zone in etwa das Äquivalent zu einem Host Record in einer Forward Lookup Zone dar.

11.2.1. Konfiguration des BIND-Dienstes

Feedback

11.2.1.1. Konfiguration der Debug-Ausgaben von BIND

Feedback

Der Detailgrad der Debugausgaben von BIND kann über die Univention Configuration Registry-Variablen `dns/debug/level` und `dns/dlz/debug/level` (für das Samba-Backend, siehe Abschnitt 11.2.1.2) konfiguriert werden. Die möglichen Werte reichen von 0 (keine Debug-Ausgaben) bis 11. Eine komplette Aufstellung der Detailgrade findet sich unter [bind-loglevel].

11.2.1.2. Konfiguration des Daten-Backends des Nameservers

Feedback

In einer typischen BIND-Installation auf einem Nicht-UCS-System wird die Konfiguration durch das Bearbeiten von Zonen-Dateien durchgeführt. In UCS wird BIND komplett über Univention Management Console konfiguriert, das seine Daten im LDAP-Verzeichnis speichert.

BIND kann zwei verschiedene Backends für seine Konfigurationsdateien verwenden:

- Das *LDAP-Backend* greift auf die Daten im OpenLDAP-Verzeichnis zu. Dieses Backend ist der Standard. Der DNS-Dienst ist in diesem Fall zweigeteilt: Der *BIND-Proxy* ist der primäre Nameserver und bedient den DNS-Standard-Port 53. Ein zweiter Server im Hintergrund arbeitet auf Port 7777. Werden Daten der internen DNS-Zonen im LDAP bearbeitet, wird die Zonendatei auf dem zweiten Server basierend auf den LDAP-Informationen aktualisiert und durch einen Zonentransfer an den BIND-Proxy übertragen.

- Samba 4 stellt eine Active Directory-Domäne bereit. Active Directory ist eng mit DNS verknüpft, u.a. für DNS-Updates von Windows-Clients oder für die Lokalisierung des Netlogon-Shares. Wird Samba 4 eingesetzt, wird der betreffende Domänencontroller auf die Verwendung des *Samba-Backend*s umgestellt. Die DNS-Datenbank wird dabei in der Samba-internen LDB-Datenbank vorgehalten, die direkt von Samba aktualisiert wird. BIND greift dann über die DLZ-Schnittstelle auf die Samba-DNS-Daten zu.

Bei Verwendung des Samba-Backends wird für jede DNS-Anfrage eine Suche im LDAP durchgeführt. Bei Verwendung des OpenLDAP-Backends wird nur bei Änderungen der DNS-Daten im Verzeichnisdienst gesucht. Die Verwendung des LDAP-Backends kann daher zu einer Reduzierung der Systemlast auf Samba 4-Systemen führen.

Das Backend wird über die Univention Configuration Registry-Variable `dns/backend` konfiguriert. Die DNS-Verwaltung ändert sich durch das verwendete Backend nicht und erfolgt in beiden Fällen über Univention Management Console.

11.2.1.3. Konfiguration von Zonentransfers

Feedback

In der Grundeinstellung erlaubt der UCS-Nameserver Zonentransfers der DNS-Daten. Ist der UCS-Server aus dem Internet erreichbar, kann dadurch eine Liste aller Rechnernamen und IP-Adressen abgefragt werden. Der Zonentransfer kann bei Verwendung des OpenLDAP-Backends durch Setzen der Univention Configuration Registry-Variable `dns/allow/transfer` auf `none` deaktiviert werden.

11.2.2. Konfiguration der DNS-Daten in Univention Management Console

Feedback

DNS-Daten werden standardmäßig im Container `cn=dns,`*`Basis-DN`* abgelegt. Forward- und Reverse-Lookup-Zonen werden direkt in dem Container abgelegt. In den jeweiligen Zonen können zusätzliche DNS-Objekte wie z.B. Pointer-Records angelegt werden.

In Eingabefeldern für Rechner sollte immer der relative oder vollqualifizierte Domänenname und nicht die IP-Adresse des Rechners verwendet werden. Um zu verhindern, dass der Domänenname erneut angehängt wird, sollte ein FQDN immer mit einem Punkt abgeschlossen werden.

In der linken Spalte des UMC-Moduls **DNS** befindet sich eine Liste aller Forward- und Reverse-Lookup-Zonen. Um ein Objekt einer Zone hinzuzufügen - etwa einen Alias-Record zu einer Forward-Zone - muss die entsprechende Zone ausgewählt werden. Durch **Hinzufügen** wird das Objekt dann in dieser Zone angelegt. Um eine neue Forward- oder Reverse-Zone anzulegen, muss zuerst **Alle DNS-Zonen** selektiert werden, der Klick auf **Hinzufügen** legt dann eine neue Zone an. Wird ein Objekt unterhalb einer Zone angelegt, wird die Zone in den UMC-Dialogen als *übergeordnetes Objekt* bezeichnet.

11.2.2.1. Forward Lookup Zonen

Feedback

Forward Lookup Zonen enthalten Informationen, die zum Auflösen von DNS-Namen in IP-Adressen verwendet werden. Sie werden im UMC-Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um eine weitere Forward Lookup Zone anzulegen, muss **Alle DNS-Zonen** selektiert werden und **Hinzufügen -> DNS: Forward Lookup Zone** ausgewählt werden.

Abbildung 11.2. Konfiguration einer Forward Lookup Zone in UMC

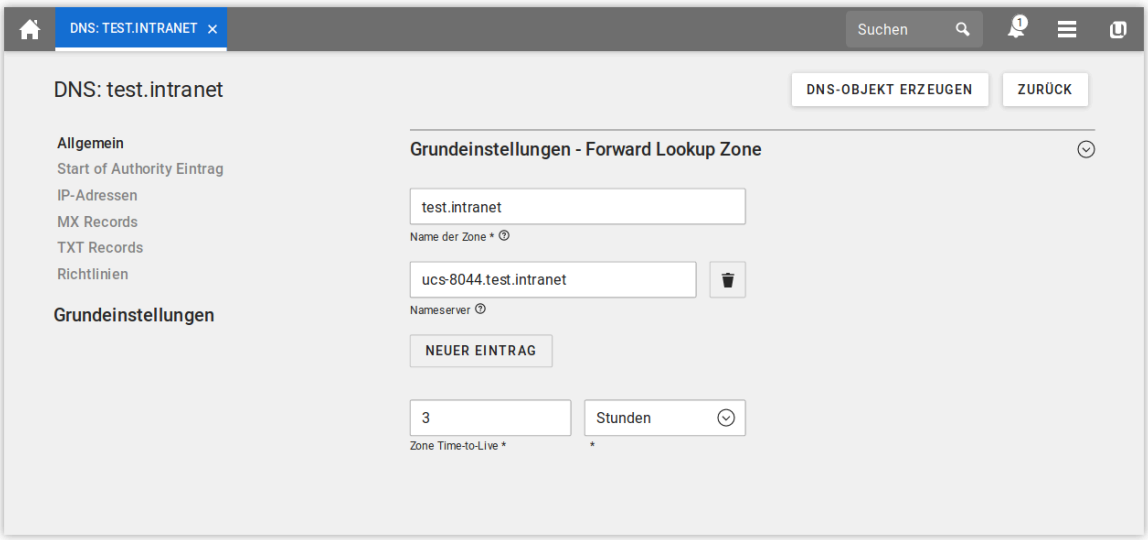


Tabelle 11.2. Reiter 'Allgemein'

Attribut	Beschreibung
Name der Zone	Der komplette Name der DNS-Domäne, für die die Zone zuständig sein soll. In Zonennamen darf der Domänenname nicht mit einem Punkt abgeschlossen werden!
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen. Der Wert wird in Sekunden gespeichert.
Nameserver	Der FQDN mit abschließendem Punkt oder der relative Domänenname der zuständigen Nameserver. Der erste Eintrag in der Liste ist der primäre Nameserver der Zone.

Tabelle 11.3. Reiter 'Start of Authority Eintrag'

Attribut	Beschreibung
Verantwortliche Person	Die E-Mail-Adresse der für die Verwaltung der Zone verantwortlichen Person.
Seriennummer	Anhand der Seriennummer erkennen andere DNS-Server, ob sich Zonendaten geändert haben. Der Slave-Nameserver vergleicht die Seriennummer seiner Kopie mit der auf dem Master-Nameserver. Ist die Seriennummer auf dem Slave niedriger als auf dem Master, so kopiert der Slave die geänderten Daten. Es gibt zwei häufig verwendete Muster für die Seriennummer: ◦ Beginn mit 1 unter Inkrementierung der Seriennummer bei jeder Änderung ◦ Unter Einbeziehung des Datums kann die Zahl im Format ***JJJJMMTTNN*** eingegeben werden, wobei *J* für Jahr, *M* für Monat, *T* für Tag und *N* für die Nummer der Änderung an diesem Tag steht.

Attribut	Beschreibung
	Wird die Seriennummer nicht von Hand geändert, wird sie automatisch bei jeder Änderung inkrementiert.
Aktualisierungsintervall	Die Zeitspanne in Sekunden, nach der der Slave-Nameserver überprüft, ob seine Kopie der Zonendaten noch aktuell ist.
Intervall für erneute Versuche	Die Zeitspanne in Sekunden, nach der der Slave-Nameserver nach einer fehlgeschlagenen Aktualisierungs-Anfrage erneut versucht, die Aktualität seiner Zonendaten-Kopie zu überprüfen. Üblicherweise wird diese Zeitspanne kürzer gewählt als das Aktualisierungsintervall, darf aber auch gleich lang sein.
Ablaufintervall	Die Zeitspanne in Sekunden, nach der die Zonendaten-Kopie auf dem Slave ungültig wird, wenn ihre Aktualität nicht überprüft werden konnte. Bei einem Ablaufintervall von einer Woche bedeutet dies beispielsweise, dass die Zonendaten-Kopie ungültig wird, wenn eine Woche lang alle Aktualisierungs-Anfragen fehlgeschlagen sind. In dem Fall wird davon ausgegangen, dass die Daten nach der Ablaufzeit zu veraltet sind, um weiter verwendet zu werden. Der Slave-Nameserver kann dann keine Namensauflösungs-Anfragen für diese Zone mehr beantworten.
Negative Time-to-Live	Die Negative Time-to-Live gibt in Sekunden an, wie lange andere Server *No-such-Domain*-Antworten (NXDOMAIN) im Cache behalten dürfen. Der Wert darf nicht mehr als 3 Stunden betragen, der Standard sind 3 Stunden.

Tabelle 11.4. Reiter 'IP-Adressen'

Attribut	Beschreibung
IP-Adressen der Zone	Mit diesem Eingabefeld können eine oder mehrere IP-Adressen angegeben werden, die zurückgegeben werden, wenn der Name der Zone aufgelöst wird. Die hier hinterlegten Adressen werden von Microsoft Windows-Clients in AD-kompatiblen Domänen abgefragt.

Tabelle 11.5. Reiter 'MX Records'

Attribut	Beschreibung
Mail-Server	Hier wird der für diese Domäne zuständige Mail-Server als vollqualifizierter Domänenname mit abschließendem Punkt eingetragen. Es dürfen nur kanonische Namen und keine Alias-Namen verwendet werden.
Priorität	Ein Zahlenwert zwischen 0 und 65535. Stehen mehrere Mail-Server für den MX-Record zur Verfügung, wird zuerst versucht, den Server mit dem niedrigsten Prioritätswert in Anspruch zu nehmen.

Tabelle 11.6. Reiter 'TXT Records'

Attribut	Beschreibung
TXT Record	Ein beschreibender Text zu dieser Zone. Text Records dürfen keine Umlaute oder sonstige Sonderzeichen enthalten.

11.2.2.2. CNAME-Record (Alias-Records)

Feedback

CNAME-Records / Alias-Records werden im UMC-Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit **Hinzufügen -> DNS: Alias Record** kann dann ein neuer Record angelegt werden.

Tabelle 11.7. Reiter 'Allgemein'

Attribut	Beschreibung
Alias	Der Aliasname als FQDN mit abschließendem Punkt oder als relativer Domänenname, der auf den kanonischen Namen verweisen soll.
Kanonischer Name	Der kanonische Name des Rechners, auf den der Alias verweisen soll, angegeben als FQDN mit abschließendem Punkt oder als relativer Domänenname.

11.2.2.3. A/AAAA-Records (Host Records)

Feedback

Host-Records werden im UMC-Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit **Hinzufügen -> DNS: Host Record** kann dann ein neuer Record angelegt werden.

Beim Hinzufügen oder Bearbeiten eines Rechner-Objekts kann ein Host Record automatisch erstellt oder geändert werden.

Tabelle 11.8. Reiter 'Allgemein'

Attribut	Beschreibung
Rechnername	Der FQDN mit abschließendem Punkt oder der relativen Domänenname des Rechners.
IP-Adresse	Die IPv4 und/oder IPv6-Adressen, auf die der Host Record verweisen soll.
Zone Time-to-Live	Die Time-to-Live gibt in Sekunden an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

11.2.2.4. Service Records

Feedback

Service Records werden im Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Forward Lookup Zone ausgewählt werden. Mit **Hinzufügen -> DNS: Service Record** kann dann ein neuer Record angelegt werden.

Abbildung 11.3. Konfiguration eines Service Records

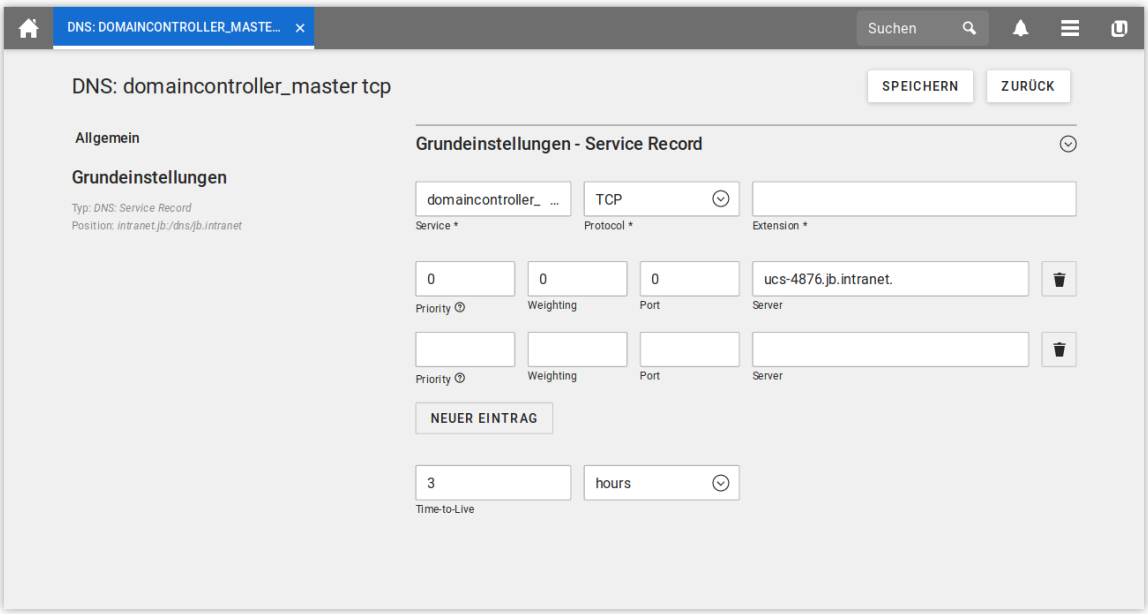


Tabelle 11.9. Reiter 'Allgemein'

Attribut	Beschreibung
Dienst	Der Name, unter dem der Dienst erreichbar sein soll.
Protokoll	Der Protokoll, über das der Record erreichbar ist (`TCP`, `UDP`, `MSDCS` oder `SITES`).
Erweiterung	Über dieses Eingabefeld können weitere Parameter übergeben werden.
Priorität	Eine ganze Zahl zwischen 0 und 65535. Stellen mehrere Server denselben Dienst zur Verfügung, wendet sich der Client zuerst an den Server mit dem niedrigeren Prioritätswert.
Gewichtung	Eine ganze Zahl zwischen 0 und 65535. Die Gewichtung dient der Lastverteilung zwischen Servern mit gleicher Priorität. Wenn mehrere Server denselben Dienst zur Verfügung stellen und denselben Prioritätswert haben, wird die Last im Verhältnis der Gewichtungen auf die Server verteilt. Beispiel: `Server1` hat eine Priorität von 1 und eine Gewichtung von 1, während `Server2` ebenfalls eine Priorität von 1, aber eine Gewichtung von 3 hat. In diesem Fall wird `Server2` dreimal so oft verwendet wie `Server1`. Die Belastung wird abhängig vom Dienst beispielsweise als Anzahl der Anfragen oder Verbindungen gemessen.
Port	Der Port, über den der Dienst auf dem Server zu erreichen ist (gültige Werte liegen zwischen 1 und 65535).
Server	Der Name des Servers, auf dem der Dienst bereitgestellt wird, als FQDN mit abschließendem Punkt oder als relativer Domänenname. Für jeden Dienst können über die Auswahlbox auch mehrere Server eingetragen werden.

Attribut	Beschreibung
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

11.2.2.5. Reverse Lookup Zonen

Eine Reverse Lookup Zone dient zur Umwandlung von IP-Adressen in Rechnernamen. Sie werden im UMC-Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um eine weitere Reverse Lookup Zone anzulegen, muss **Alle DNS-Zonen** selektiert werden und **Hinzufügen -> DNS: Reverse Lookup Zone** ausgewählt werden.

Tabelle 11.10. Reiter 'Allgemein'

Attribut	Beschreibung
Subnetz	Die IP-Adresse des Netzwerkes, für das die Reverse Lookup Zone gültig sein soll. Wenn beispielsweise das betreffende Netz aus den IP-Adressen `192.0.2.0` bis `192.0.2.255` besteht, wäre `192.0.2` einzutragen.
Zone Time-to-Live	Die Time-to-Live gibt an, wie lange diese Daten von anderen DNS-Servern im Cache gespeichert werden dürfen.

Tabelle 11.11. Reiter 'Start of Authority Eintrag'

Attribut	Beschreibung
Verantwortliche Person	Die E-Mail-Adresse der für die Verwaltung der Zone verantwortlichen Person (mit abschließendem Punkt).
Nameserver	Der FQDN mit abschließendem Punkt oder der relative Domänenname der zuständigen Nameserver. Der erste Eintrag in der Liste ist der primäre Nameserver der Zone.
Seriennummer	Siehe die Dokumentation zu Forward Lookup Zonen in Abschnitt 11.2.2.1.
Aktualisierungsintervall	Siehe die Dokumentation zu Forward Lookup Zonen in Abschnitt 11.2.2.1.
Intervall für erneute Versuche	Siehe die Dokumentation zu Forward Lookup Zonen in Abschnitt 11.2.2.1.
Ablaufintervall	Siehe die Dokumentation zu Forward Lookup Zonen in Abschnitt 11.2.2.1.
Minimum Time-to-Live	Siehe die Dokumentation zu Forward Lookup Zonen in Abschnitt 11.2.2.1.

11.2.2.6. Pointer Records

Pointer-Records werden im UMC-Modul *DNS* verwaltet (siehe auch Abschnitt 4.4). Um einen weiteren Record anzulegen, muss in der linken Spalte eine Reverse Lookup Zone ausgewählt werden. Mit **Hinzufügen -> DNS: Pointer Record** kann dann ein neuer Record angelegt werden.

Tabelle 11.12. Reiter 'Allgemein'

Attribut	Beschreibung
Adresse	Die letzten Oktett der IP-Adresse des Rechners (abhängig vom Netz-Präfix, siehe unten).
Pointer	Der FQDN des Rechners mit abschließendem Punkt.

Attribut	Beschreibung
	Ein Beispiel: In einem Netzwerk mit 24 Bit langem Netz-Präfix (Netzmaske `255.255.255.0`) soll für den Rechner `client001` mit der IP-Adresse `192.0.2.101` ein Pointer angelegt werden. In das Feld **Adresse** ist dann **`101`** und in **Pointer** **`client001.firma.com.`** einzutragen. Bei einem Netzwerk mit 16 Bit langem Netz-Präfix (Netzmaske `255.255.0.0`) müssten für diesen Rechner die letzten zwei Oktette in umgekehrter Reihenfolge (hier **`101.1`**) eingetragen werden. In das Feld **Pointer** wäre auch hier **`client001.firma.com.`** einzutragen.

11.3. IP-Vergabe über DHCP

Feedback

11.3.1. Einführung

Feedback

Das *Dynamic Host Configuration Protocol* (DHCP) weist Rechnern eine IP-Adresse, die Subnetz-Maske und gegebenenfalls weitere Einstellungen wie Gateway oder NetBIOS-Server zu. Die IP-Adresse kann fest oder dynamisch vergeben werden.

Die Verwendung von DHCP ermöglicht eine zentrale Vergabe und Kontrolle von IP-Adressen über das LDAP-Verzeichnis ohne manuelle Einträge an den einzelnen Rechnersystemen vorzunehmen.

Die DHCP-Integration in UCS unterstützt nur IPv4.

In einem *DHCP-Service* werden DHCP-Server mit einer gemeinsamen LDAP-Konfiguration zusammengefasst. Globale Konfigurationsparameter werden am DHCP-Service angegeben, spezifische Parameter in den Objekten darunter.

Ein DHCP-Server kann mit der Applikation *DHCP-Server* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-dhcp*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

Jeder DHCP-Server verteilt IP-Adressen über DHCP. In der Grundeinstellungen werden nur statische IP-Adressen an im UCS-LDAP registrierte Rechnerobjekte vergeben.

Werden ausschließlich feste IP-Adressen vergeben, können beliebig viele DHCP-Server in einem DHCP-Service verwendet werden. Alle DHCP-Server greifen auf identische Daten aus dem LDAP zurück und bieten den DHCP-Clients die Daten mehrfach an. DHCP-Clients akzeptieren dann die erste Antwort und verwerfen die übrigen.

Werden auch dynamisch IP-Adressen verteilt, muss der DHCP-Failover-Mechanismus eingesetzt werden. Dabei können maximal zwei DHCP-Server pro Subnetz verwendet werden.

Mit einem *DHCP-Rechner*-Eintrag wird ein Rechner dem DHCP-Service bekannt gemacht. Für Rechner, die per DHCP eine feste IP-Adresse beziehen sollen, ist ein DHCP-Rechner-Objekt zwingend erforderlich. DHCP-Rechner-Objekte müssen in der Regel nicht manuell erstellt werden, weil diese automatisch angelegt werden, wenn einem Rechnerobjekt mit fester IP-Adresse ein DHCP-Service zugewiesen wird.

Für jedes Subnetz wird ein *DHCP-Subnetz*-Eintrag benötigt, unabhängig davon, ob dynamische IP-Adressen aus diesen Subnetzen vergeben werden sollen.

Über die Einrichtung von *DHCP-Pools* innerhalb von Subnetzen können den verschiedenen IP-Adressbereichen unterschiedliche Konfigurationsparameter zugeordnet werden. Auf diese Weise können unbekannte Rechner in einem IP-Adressbereich zugelassen und von einem anderen IP-Adressbereich ausgeschlossen werden. DHCP-Pools können nur unterhalb von DHCP-Subnetz-Objekten angelegt werden.

Falls mehrere IP-Subnetze gemeinsam dasselbe physikalische Ethernet-Netzwerk verwenden, sollten diese als *DHCP Shared Subnet* unterhalb eines **DHCP Shared Network** eingetragen werden. **DHCP Shared Subnet**-Objekte können nur unterhalb von **DHCP Shared Network**-Objekten angelegt werden.

Werte, die auf einer Ebene der DHCP-Konfiguration angegeben werden, gelten immer für diese und alle darunterliegenden Ebenen, sofern dort keine anderen Angaben gemacht werden. Ähnlich wie bei Richtlinien gilt immer der Wert, der dem Objekt am nächsten ist.

11.3.2. Aufbau der DHCP-Konfiguration durch DHCP-LDAP-Objekte

In der linken Spalte des UMC-Moduls **DHCP** befindet sich eine Liste aller DHCP-Services. Um einem DHCP-Service ein Objekt hinzuzufügen - etwa ein weiteres Subnetz - muss der entsprechende Service ausgewählt werden. Durch **Hinzufügen** wird das Objekt dann in diesem Service angelegt. Um einen neuen DHCP-Service anzulegen, muss zuerst **Alle DHCP-Dienste** selektiert werden, der Klick auf **Hinzufügen** legt dann einen neue Service an. Wird ein Objekt unterhalb eines Services angelegt, wird der Service in den UMC-Dialogen als *übergeordnetes Objekt* bezeichnet.

11.3.2.1. Verwaltung von DHCP-Services

DHCP-Services werden im UMC-Modul *DHCP* verwaltet (siehe auch Abschnitt 4.4). Um einen neuen DHCP-Service anzulegen muss zuerst **Alle DHCP-Dienste** in der linken Spalte des UMC-Moduls selektiert werden. Ein Klick auf **Hinzufügen** legt dann einen neue Service an.

Ein DHCP-Server kann nur einen DHCP-Service bedienen; wenn ein weiterer DHCP-Service verwendet werden soll, muss dafür ein separater DHCP-Server eingerichtet werden (siehe Abschnitt 11.3.2.2).

Am DHCP-Service-Objekt werden häufig folgende Parameter festgelegt, die dann für alle Rechner gültig sind, die von diesem DHCP-Service bedient werden (es sei denn, es werden auf tieferen Ebenen andere Angaben gemacht):

- **Domänenname** und **DNS-Server** unter **Richtlinie: DHCP DNS**
- **NetBIOS-Nameserver** unter **Richtlinie: DHCP NetBIOS**

Eine Beschreibung dieser und der anderen DHCP-Richtlinien findet sich unter Abschnitt 11.3.3.

Tabelle 11.13. Reiter 'Allgemein'

Attribut	Beschreibung
Service-Name	In dieses Eingabefeld muss ein beliebiger, aber eindeutiger Name für den DHCP-Service eingetragen werden, z.B. `firma.com`.

11.3.2.2. Verwaltung von DHCP-Server-Einträgen

Jeder Server, der den DHCP-Dienst anbieten soll, benötigt zwingend einen *DHCP-Server*-Eintrag im LDAP-Verzeichnis. Der Eintrag muss in der Regel nicht von Hand angelegt werden, sondern wird durch das Join-Skript des ***univention-dhcp***-Pakets angelegt. Um dennoch manuell einen weiteren Record anzulegen, muss im UMC-Modul *DHCP* in der linken Spalte ein DHCP-Service ausgewählt werden. Mit **Hinzufügen -> DHCP Server** kann dann ein neuer Server registriert werden.

Tabelle 11.14. Reiter 'Allgemein'

Attribut	Beschreibung
Server-Name	In diesem Eingabefeld ist der Rechnername, der den DHCP-Dienst anbieten soll, einzutragen, z.B. `ucs-master`.

Attribut	Beschreibung
	Ein Server kann immer nur einen einzigen DHCP-Dienst anbieten und kann deshalb nicht gleichzeitig in mehreren DHCP-Services eingetragen sein.

11.3.2.3. Verwaltung von DHCP-Subnetzen

DHCP-Subnetze werden im UMC-Modul *DHCP* verwaltet (siehe auch Abschnitt 4.4). Um ein weiteres Subnetz anzulegen, muss in der linken Spalte ein DHCP-Service ausgewählt werden. Mit **Hinzufügen -> DHCP: Subnetz** kann dann ein neues Subnetz angelegt werden.

Ein DHCP-Subnetz-Eintrag ist für jedes Subnetz, aus dem dynamische oder feste IP-Adressen vergeben werden sollen, zwingend erforderlich. Das Eintragen von IP-Adressbereichen ist nur notwendig, wenn IP-Adressen dynamisch vergeben werden sollen.

Falls *DHCP:Shared Subnet*-Objekte verwendet werden sollen, sollten die entsprechenden Subnetze unterhalb des dafür angelegten *DHCP:Shared Network*-Containers angelegt werden (siehe Abschnitt 11.3.2.6).

Tabelle 11.15. Reiter 'Allgemein'

Attribut	Beschreibung
Subnetz-Adresse	In diesem Eingabefeld ist die IP-Adresse des Subnetzes in Oktettschreibweise einzutragen, z.B. `192.0.2.0`.
Netzmaske	Die Netzmaske kann in diesem Eingabefeld wahlweise als Dezimalzahl des Netzpräfix oder in Oktettschreibweise eingetragen werden. Wenn die Netzmaske in Oktettschreibweise eingegeben wird, wird sie automatisch in den entsprechenden Netzpräfix umgewandelt und später auch ausgegeben.
Dynamische Adresszuweisung	Hier können ein einzelner oder mehrere IP-Adressbereiche eingerichtet werden, die für die dynamische Vergabe zur Verfügung stehen. Der Bereich erstreckt sich von **Erste Adresse** bis **Letzte Adresse** in Oktettschreibweise. **Achtung** Dynamische IP-Adressbereiche für ein Subnetz sind immer entweder ausschließlich im Subnetz-Eintrag oder ausschließlich in einem oder mehreren gesonderten Pool-Einträgen anzugeben. Die IP-Adressbereich-Eintragstypen innerhalb eines Subnetzes dürfen nicht gemischt werden! Wenn in einem Subnetz verschiedene IP-Adressbereiche mit unterschiedlichen Konfigurationen eingesetzt werden sollen, müssen dafür Pool-Einträge angelegt werden.

Auf dieser Ebene wird häufig über dir Karteikarte **Richtlinie: DHCP Routing** das Gateway für alle Rechner in diesem Subnetz festgelegt (es sei denn, es werden an DHCP-Pools andere Angaben gemacht).

11.3.2.4. Verwaltung von DHCP-Pools

DHCP-Pools können nur über das UMC-Modul *LDAP-Verzeichnis* verwaltet werden. Dazu muss in ein DHCP-Subnetz-Objekt navigiert werden - ein DHCP-Pool-Objekt muss immer unterhalb eines DHCP-Subnetz-Objektes angelegt werden - und dort mit **Hinzufügen** ein **DHCP: Pool**-Objekt eingefügt werden.

Wenn in einem Subnetz DHCP-Pools angelegt werden, sollten keine IP-Adressbereiche im Subnetz-Eintrag definiert werden. Diese sind ausschließlich in den Pool-Einträgen anzulegen.

Tabelle 11.16. Reiter 'Allgemein'

Attribut	Beschreibung
Name	In dieses Eingabefeld muss ein beliebiger, aber eindeutiger Name für den DHCP-Pool eingetragen werden, z.B. `testnetz.firma.com`.
Dynamischer Bereich	Hier können die IP-Adressen in Oktettschreibweise angegeben werden, die dynamisch vergeben werden.

Tabelle 11.17. Reiter 'Fortgeschritten'

Attribut	Beschreibung
Failover Peer	Der Name einer Failover-Konfiguration, die von Hand in der Datei `/etc/dhcp/local.conf` konfiguriert werden werden. Hinweise zur Einrichtung finden sich in [dhcp-failover].
Erlaube bekannte Clients	Ein Computer wird durch seine MAC-Adresse identifiziert. Ist dieses Feld auf **erlauben** gesetzt oder nicht gesetzt, ist ein Computer mit einem DHCP-Rechner-Eintrag (siehe Abschnitt 11.3.2.5) berechtigt eine IP-Adresse aus diesem Pool zu beziehen. Ist es auf **verbieten** gesetzt, erhalten diese Computer keine IP-Adresse aus dem Pool.
Erlaube unbekannte Clients	Ein Computer wird durch seine MAC-Adresse identifiziert. Ist dieses Feld auf **erlauben** gesetzt oder nicht gesetzt, ist ein Computer ohne DHCP-Rechner-Eintrag (siehe Abschnitt 11.3.2.5) berechtigt eine IP-Adresse aus diesem Pool zu beziehen. Ist es auf **verbieten** gesetzt, erhalten diese Computer keine IP-Adresse aus dem Pool.
Dynamische BOOTP-Clients erlauben	*BOOTP* ist das Vorgängerprotokoll von DHCP. Es kennt keinen Mechanismus zum Aktualisieren eines Leases und weist Adressen zeitlich unbeschränkt zu, was den Pool erschöpfen kann. Ist diese Option auf **erlauben** gesetzt können Clients auch über BOOTP eine Adresse aus diesem Pool zu beziehen.
Alle Clients	Wird diese Option auf **verbieten** gesetzt, wird der Pool global deaktiviert. Diese Option ist nur in Ausnahmefällen sinnvoll.

11.3.2.5. Registrierung von Rechnern mit DHCP-Rechner-Objekten

Mit einem *DHCP:Rechner*-Eintrag wird der betreffende Rechner im DHCP-Service registriert. Rechner können in Abhängigkeit von ihrem Registrierungs-Status behandelt werden. Bekannte Rechner können feste oder dynamische IP-Adressen vom DHCP-Service beziehen; unbekannte Rechner erhalten nur dynamische IP-Adressen.

Üblicherweise werden beim Hinzufügen eines Rechners über die Rechnerverwaltung automatisch DHCP-Rechner-Einträge erstellt. Unterhalb des DHCP-Service-Objekts gibt es die Möglichkeit, manuell DHCP-Rechner-Einträge hinzuzufügen oder bestehende Einträge, egal ob manuell oder automatisch erzeugt, zu bearbeiten.

DHCP-Rechner-Objekte werden im UMC-Modul *DHCP* verwaltet (siehe auch Abschnitt 4.4). Um einen Rechner manuell im DHCP zu registrieren, muss in der linken Spalte des Moduls ein DHCP-Service ausgewählt werden. Mit **Hinzufügen** -> **DHCP: Rechner** kann dann ein Rechner registriert werden.

Tabelle 11.18. Reiter 'Allgemein'

Attribut	Beschreibung
Rechnername	In diesem Eingabefeld ist ein Name für den Rechner einzugeben (der in der Regel auch einen Eintrag in der Rechnerverwaltung besitzt). Es emp-

Attribut	Beschreibung
	fiehlt sich, in beiden Einträgen denselben Namen und dieselbe MAC-Adresse für den Rechner zu verwenden, um die Zuordnung zu erleichtern.
Netzwerktyp	In dieser Auswahlliste ist der Typ des verwendeten Netzwerks auszuwählen. Hier ist nahezu immer **Ethernet** auszuwählen.
Adresse	In diesem Eingabefeld ist die MAC-Adresse der Netzwerkkarte einzutragen, z.B. `2e:44:56:3f:12:32` oder `2e-44-56-3f-12-32`.
Feste IP-Adressen	Hier können dem Rechner eine oder mehrere feste IP-Adressen zugewiesen werden. Neben einer IP-Adresse kann auch ein vollqualifizierter Domänenname angegeben werden, der vom DHCP-Server in eine oder mehrere IP-Adressen aufgelöst wird.

11.3.2.6. Verwaltung von DHCP Shared Networks / DHCP Shared Subnets

Feedback

DHCP:Shared Network-Objekte nehmen Subnetze auf, die ein physikalisches Netzwerk gemeinsam nutzen.

DHCP-Shared-Network-Objekte werden im UMC-Modul *DHCP* verwaltet (siehe auch Abschnitt 4.4). Um ein Shared Network anzulegen, muss in der linken Spalte des Moduls ein DHCP-Service ausgewählt werden. Mit **Hinzufügen -> DHCP: Shared Network** kann dann ein Netzwerk registriert werden.

> **Achtung**
>
> Ein Shared-Network muss mindestens einen Shared-Subnet-Eintrag enthalten. Anderenfalls beendet sich der DHCP-Dienst und kann nicht gestartet werden, bis die Konfiguration korrigiert ist.

Tabelle 11.19. Reiter 'Allgemein'

Attribut	Beschreibung
Shared Network Name	In dieses Eingabefeld ist ein Name für das Shared Network einzutragen.

Als *DHCP:Shared Subnet* werden Subnetze deklariert, die gemeinsam dasselbe physikalische Netzwerk verwenden. Alle Subnetze, die dasselbe Netzwerk verwenden, müssen unterhalb desselben Shared Network-Containers angelegt werden. Für jedes Subnetz ist ein eigenes *DHCP:Shared Subnet*-Objekt anzulegen.

DHCP-Shared-Subnet-Objekte können nur über das UMC-Modul *LDAP-Verzeichnis* verwaltet werden. Dazu muss in ein DHCP-Shared Network-Objekt navigiert werden - ein DHCP-Shared Subnet-Objekt muss immer unterhalb eines DHCP-Shared Network-Objektes angelegt werden - und dort mit **Hinzufügen** ein **DHCP: Shared Subnet**-Objekt eingefügt werden.

11.3.3. Konfiguration von Clients durch DHCP-Richtlinien

Feedback

> **Anmerkung**
>
> Viele Einstellungen für DHCP werden über Richtlinien konfiguriert. Diese finden auch Anwendung auf DHCP-Rechner-Objekte, wenn eine Richtlinie mit der LDAP-Basis oder einem der anderen dazwischenliegenden Container verknüpft ist. Da die Einstellungen an DHCP-Rechner-Objekte die höchste Priorität haben, werden andere Einstellungen an Subnetz- oder Service-Objekten ignoriert.
>
> DHCP-Richtlinien sollten von daher direkt mit den DHCP-Netzwerk-Objekten (bspw. den DHCP-Subnetzen) verknüpft werden. [1]

[1] Alternativ kann in den erweiterten Einstellungen der Richtlinien unter **Objekt** bei **Ausgeschlossene Objektklassen** die LDAP-Klasse `univentionDhcpHost` hinzugefügt werden. Solche Richtlinien finden dann nicht länger auf die DHCP-Rechner-Objekt Anwendung, wodurch dann die Einstellungen aus DHCP-Subnetz und -Service benutzt werden.

Tipp

Bei Verwendung der Kommandozeile `udm dhcp/host list` (siehe auch Abschnitt 4.10.2.7) kann die Option `--policies 0` verwendet werden, um die effektiven Einstellungen anzeigen zu lassen.

11.3.3.1. Vorgabe des Gateways

Feedback

Das Default-Gateway kann per DHCP über eine Richtlinie vom Typ *DHCP Routing* festgelegt werden, die im UMC-Modul **Richtlinien** verwaltet wird (siehe auch Abschnitt 4.6).

Tabelle 11.20. Reiter 'Allgemein'

Attribut	Beschreibung
Router	Hier sind die Namen oder IP-Adressen der Router einzutragen. Dabei ist darauf zu achten, dass der DHCP-Server diese Namen in IP-Adressen auflösen kann. Die Router werden vom Client in der Reihenfolge angesprochen, in der sie in der Auswahlliste erscheinen.

11.3.3.2. Vorgabe der DNS-Server

Feedback

Die von einem Client zu verwendenden Nameserver können per DHCP über eine Richtlinie vom Typ *DHCP DNS* festgelegt werden, die im UMC-Modul **Richtlinien** verwaltet wird (siehe auch Abschnitt 4.6).

Tabelle 11.21. Reiter 'Allgemein'

Attribut	Beschreibung
Domänenname	Der Name der Domäne, den der Client automatisch an Rechnernamen anhängt, die er zur Auflösung an den DNS-Server schickt und die keine vollqualifierten Domänennamen sind. Üblicherweise wird hier der Name der Domäne verwendet, der der Client angehört.
DNS-Server	Hier können IP-Adressen oder vollqualifizierte Domänennamen (FQDNs) von DNS-Servern hinzugefügt werden. Bei der Verwendung von FQDNs ist darauf zu achten, dass der DHCP-Server die Namen in IP-Adressen auflösen kann. Die DNS-Server werden von den Clients entsprechend der hier angegebenen Reihenfolge kontaktiert.

11.3.3.3. Vorgabe des WINS-Server

Feedback

Der zu verwendende WINS-Server kann per DHCP über eine Richtlinie vom Typ *DHCP NetBIOS* festgelegt werden, die im UMC-Modul **Richtlinien** verwaltet wird (siehe auch Abschnitt 4.6).

Tabelle 11.22. Reiter 'NetBIOS'

Attribut	Beschreibung
NetBIOS-Nameserver	Hier sind die Namen oder IP-Adressen der NetBIOS-Nameserver (auch bekannt als WINS-Server) einzutragen. Dabei ist darauf zu achten, dass der DHCP-Server diese Namen in IP-Adressen auflösen kann. Die angegebenen Server werden vom Client in der Reihenfolge angesprochen, in der sie in der Auswahlliste erscheinen.

Attribut	Beschreibung
NetBIOS Scope	Der NetBIOS over TCP/IP-Scope für den Client nach der Spezifikation in RFC 1001[1] und RFC 1002[1]. Bei der Angabe des NetBIOS Scopes ist die Groß- und Kleinschreibung zu beachten.
NetBIOS Node Type	Dieses Auswahlfeld legt den Node Type eines Clients fest. Mögliche Werte sind: ◦ **1 B-node** (Broadcast: kein WINS) ◦ **2 P-node** (Peer: ausschließlich WINS) ◦ **4 M-node** (Mixed: erst Broadcast, dann WINS) ◦ **8 H-node** (Hybrid: erst WINS, dann Broadcast)

11.3.3.4. Konfiguration der DHCP-Vergabedauer (Lease)

Die Gültigkeit einer vergebenen IP-Adresse - ein sogenanntes DHCP-Lease - kann über eine Richtlinie vom Typ *DHCP Lease-Zeit* festgelegt werden, die im UMC-Modul **Richtlinien** verwaltet wird (siehe auch Abschnitt 4.6).

Tabelle 11.23. Reiter 'Lease-Zeit'

Attribut	Beschreibung
Standard Lease-Zeit	Wenn der Client keine bestimmte Lease-Zeit anfragt, so wird die Standard-Lease-Zeit zugewiesen. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.
Maximale Lease-Zeit	Die maximale Lease-Zeit gibt die längste Zeitspanne an, die für einen Lease vergeben werden kann. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.
Minimale Lease-Zeit	Die minimale Lease-Zeit gibt die kürzeste Zeitspanne an, die ein Lease gültig sein soll. Bleibt das Eingabefeld leer, wird der Vorgabewert des DHCP-Servers verwendet.

11.3.3.5. Konfiguration von Bootserver/PXE-Einstellungen

Mit einer *DHCP Boot*-Richtlinie werden Rechnern Konfigurationsparameter für das Booten über über BOOTP/PXE zugewiesen. Sie wird im UMC-Modul **Richtlinien** verwaltet (siehe auch Abschnitt 4.6).

Tabelle 11.24. Reiter 'Boot'

Attribut	Beschreibung
Boot-Server	In diesem Eingabefeld ist die IP-Adresse oder der FQDN des PXE-Boot-Servers einzutragen, von dem der Client die Boot-Datei laden soll. Wird in diesem Eingabefeld kein Wert eingetragen, bootet der Client von dem DHCP-Server, von dem er seine IP-Adresse bezieht.
Boot-Dateiname	Hier ist der Pfad zur Boot-Datei einzutragen. Der Pfad muss relativ zum Basisverzeichnis des TFTP-Dienstes (`/var/lib/univention-client-boot/`) angegeben werden.

[1] http://tools.ietf.org/html/rfc1001
[1] http://tools.ietf.org/html/rfc1002

11.3.3.6. Weitere DHCP-Richtlinien

Feedback

Einige weitere DHCP-Richtlinien stehen zur Verfügung, sind aber nur für Sonderfälle nötig.

- *DNS Aktualisierung* erlaubt die Konfiguration von dynamischen DNS-Aktualisierungen. Diese können bislang noch nicht gegen einen LDAP-basierten DNS-Dienst durchgeführt werden, wie er von UCS bereitgestellt wird.
- *DHCP Erlauben/Verbieten* erlaubt die Konfiguration verschiedener Optionen, die kontrollieren was für DHCP-Clients erlaubt ist. Diese sind nur in Ausnahmefällen nötig.
- *DHCP Verschiedenes* erlaubt die Konfiguration verschiedener Optionen, die nur in Ausnahmefällen nötig sind.

11.4. Paketfilter mit Univention Firewall

Feedback

Die Univention Firewall integriert einen Paketfilter auf Basis von ***iptables*** in Univention Corporate Server.

Dies ermöglicht die gezielte Filterung unerwünschter Dienste, die Absicherung von Rechnern während Installationsarbeiten, und stellt die Basis für komplexere Szenarien wie Firewalls oder Application Level Gateways bereit. Univention Firewall ist in der standardmäßig auf allen Univention Corporate Server-Installationen enthalten.

In der Grundeinstellung werden eingehende Pakete für alle Ports blockiert/abgelehnt. Jedes UCS-Paket bringt Regeln mit, die die von dem Paket benötigten Ports wieder freigeben.

Die Konfiguration erfolgt im Wesentlichen über Univention Configuration Registry-Variablen. Die Definition von solchen Paketfilter-Regeln ist in [developer-reference] dokumentiert.

Darüber hinaus werden die im Verzeichnis `/etc/security/packetfilter.d/` liegenden Konfigurationsskripte in alphabetischer Reihenfolge ausgeführt. Standardmäßig sind alle Skripte mit zwei führenden Ziffern benannt, so dass eine einfache Festlegung der Reihenfolge möglich ist. Die Skripte müssen als ausführbar markiert sein.

Nach Änderungen der Paketfilter-Einstellungen muss der Dienst ***univention-firewall*** neu gestartet werden.

Die Univention Firewall kann durch Setzen der Univention Configuration Registry-Variable `security/packetfilter/disabled` auf `true` deaktiviert werden.

11.5. Web-Proxy für Caching und Policy Management/Virenscan

Feedback

Die Proxy-Integration ermöglicht die Verwendung eines Web-Caches zur Verbesserung der Performance und Kontrolle des Datenverkehrs. Sie basiert auf dem bewährten Proxy-Server Squid und unterstützt die Protokolle HTTP, FTP und HTTPS.

Ein Proxy-Server nimmt Anfragen nach Internetinhalten entgegen und prüft, ob diese Inhalte bereits in einem lokalen Cache vorhanden sind. Ist dies der Fall, werden die angefragten Daten aus dem lokalen Cache bereitgestellt. Sind die Daten noch nicht vorhanden, werden die Inhalte vom jeweiligen Webserver abgerufen und in den lokalen Cache eingefügt. Hierdurch können die Antwortzeiten für die Anwender sowie das Transfervolumen über den Internetzugang verringert werden.

Als zusätzliche Komponente kann die Software DansGuardian installiert werden. Damit ist es möglich, dass Internetinhalte vor der Auslieferung an den Anwender überprüft und gefiltert werden, um so Dateien auf Viren zu scannen oder den Zugriff auf unerwünschte Inhalte zu unterbinden.

Einige weiterführende Funktionen der Proxy-Dienste - wie etwa die Kaskadierung von Proxy-Servern - werden in [ext-doc-net] beschrieben.

11.5.1. Installation

Feedback

Squid kann mit der Applikation *Proxyserver / Webcache (Squid)* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-squid*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

Der Dienst wird mit für den Betrieb ausreichenden Standardeinstellungen konfiguriert, sodass eine sofortige Verwendung möglich ist. Der Port, auf dem der Dienst erreichbar ist, kann nach eigenen Wünschen konfiguriert werden (siehe Abschnitt 11.5.5.1), voreinstellt ist Port 3128.

Werden Änderungen an der Konfiguration vorgenommen, muss Squid neu gestartet werden. Dies kann entweder über Univention Management Console oder auf der Kommandozeile erfolgen:

```
/etc/init.d/squid restart
```

Neben den in diesem Dokument beschriebenen Konfigurationsmöglichkeiten über Univention Configuration Registry können in der `/etc/squid/local.conf` auch beliebige weitere Squid-Optionen gesetzt werden.

DansGuardian kann über das Paket ***univention-dansguardian*** installiert werden, siehe Abschnitt 11.5.7.

In der erweiterten Netzwerk-Dokumentation sind weitergehende Proxy-Funktionen (Kaskadierung von Proxys, transparente Proxys und die Integration eines Virenscanners in den Proxy) [ext-doc-net].

11.5.2. Caching von Webseiten/FTP

Feedback

Squid ist ein *Caching proxy*, d.h. zuvor schon einmal angefragte Inhalten können aus einem Cache zur Verfügung gestellt werden ohne erneut vom jeweiligen Webserver geladen zu werden. Die reduziert das Datenaufkommen über die Internetanbindung und kann zu einer schnelleren Beantwortung von HTTP-Anfragen führen.

In manchen Umgebungen ist diese Caching-Funktionalität allerdings nicht notwendig bzw. muss bei kaskadierten Proxys nicht bei allen aktiviert sein. Für diese Szenarien kann die Caching-Funktion des Squid mit der Univention Configuration Registry-Variable `squid/cache` deaktiviert werden, indem diese auf den Wert `no` gesetzt wird. Anschließend muss Squid neu gestartet werden.

11.5.3. Protokollierung von Zugriffen

Feedback

Sämtliche Zugriffe, die über den Proxy-Server vorgenommen werden, werden in der Logdatei `/var/log/squid/access.log` erfasst. Anhand dieser Logdatei ist es möglich, nachzuvollziehen auf welche Webseiten zugegriffen wurde.

Bei Verwendung von DansGuardian werden sämtliche Zugriffe in der Datei `/var/log/dansguardian/access.log` protokolliert.

11.5.4. Einschränkung des Zugriffs auf erlaubte Netzwerke

Feedback

Standardmäßig darf nur aus lokalen Netzwerken auf den Proxy-Server zugegriffen werden. Ist z.B. an dem Rechner, auf dem Squid installiert wurde, ein Netzwerkinterface mit der Adresse `192.0.2.10` und der Netzmaske `255.255.255.0` vorhanden, dürfen nur Rechner aus dem Netzwerk `192.0.2.0/24` auf den Proxy-Server zugreifen. Weitere Netzwerke können über die Univention Configuration Registry-Variable `squid/allowfrom` angegeben werden. Dabei muss die CIDR-Notation verwendet werden, mehrere Netzwerke sind durch Leerzeichen zu trennen.

```
univention-config-registry set squid/allowfrom="192.0.2.0/24
 192.0.2.0/24"
```

Nach einem Neustart von Squid ist jetzt der Zugriff aus den Netzwerken `192.0.2.0/24` und `192.0.2.0/24` erlaubt. Durch Angabe von `all` kann der Zugriff auch aus allen Netzen erlaubt werden.

Wenn Squid zusammen mit DansGuardian eingesetzt wird, d.h. die Viren- oder Webinhaltsfilterung aktiviert wird, kann Squid den Zugriff nicht prüfen, da die Verbindungen über DansGuardian erfolgen. In diesem Fall kann der Zugriff über DansGuardian eingeschränkt werden.

11.5.5. Konfiguration der verwendeten Ports

Feedback

11.5.5.1. Zugriffs-Port

Feedback

Standardmäßig ist der Web-Proxy über den Port 3128 erreichbar. Ist ein anderer Port gewünscht, kann dieser über die Univention Configuration Registry-Variable `squid/httpport` konfiguriert werden. Bei Verwendung von Univention Firewall muss zusätzlich die Paketfilterkonfiguration angepasst werden.

Beim Einsatz des Inhalts- und Virenscanners (siehe Abschnitt 11.5.7) ist dieser an Stelle von Squid unter dem konfigurierten Port erreichbar. Squid belegt dann den nächsthöheren Port. Dies sollte beachtet werden, wenn es weitere Anwendungen gibt, die auf diesem Port Dienste anbieten sollen.

11.5.5.2. Erlaubte Ports

Feedback

In der Standardkonfiguration leitet Squid nur Anfragen von Clients weiter, die an die Netzwerkports 80 (HTTP), 443 (HTTPS) oder 21 (FTP) gerichtet werden. Die Liste der erlaubten Ports kann über die Univention Configuration Registry-Variable `squid/webports` geändert werden, mehrere Angaben sind dabei durch Leerzeichen zu trennen:

```
univention-config-registry set squid/webports="80 443"
```

Durch diese Einstellung wird nur noch der Zugriff auf die Ports 80 und 443 (HTTP und HTTPS) erlaubt.

11.5.6. Benutzer-Authentifizierung am Proxy

Feedback

Oftmals ist es notwendig, dass nur bestimmte Benutzer Zugriff auf Webseiten erhalten sollen. Squid ermöglicht die benutzerbezogene Zugriffsregelung über Gruppenmitgliedschaften. Um eine Überprüfung der Gruppenmitgliedschaft zu ermöglichen, ist es hierbei erforderlich, dass eine Anmeldung des Benutzers am Proxy-Server durchgeführt wird.

> **Achtung**
>
> Um zur verhindern, dass nicht autorisierte Benutzer trotzdem Webseiten abrufen können, sind weitere Maßnahmen erforderlich, damit diese Benutzer nicht am Proxy-Server vorbei auf das Internet zugreifen können. Dies kann z.B. erreicht werden, in dem in der Firewall alle HTTP-Anfragen mit Ausnahme des Proxys unterbunden werden.

Proxy-Authentifizierung und die damit erst mögliche Überprüfung der Gruppenzugehörigkeiten muss zuerst aktiviert werden. Dafür werden drei verschiedene Mechanismen angeboten:

- Die Authentifizierung erfolgt direkt gegen den LDAP-Server. Dazu muss die Univention Configuration Registry-Variable `squid/basicauth` auf `yes` gesetzt werden und Squid neu gestartet werden.
- Die Authentifizierung wird über die NTLM-Schnittstelle durchgeführt. Benutzer, die an einem Windows-Client angemeldet sind, müssen dann beim Zugriff auf den Proxy keine weitere Authentifizie-

rung durchführen. Um NTLM-Authentifizierung zu aktivieren muss die Univention Configuration Registry-Variable `squid/ntlmauth` auf `yes` gesetzt werden und Squid neu gestartet werden.

- Die Authentifizierung erfolgt über Kerberos. Benutzer, die an einem Windows-Client angemeldet sind, der Mitglied einer Samba 4-Domäne ist, authentifizieren sich am Proxy mit dem Ticket, das sie im Rahmen der Domänenanmeldung erhalten haben. Um Kerberos-Authentifizierung zu aktivieren muss das Paket ***univention-squid-kerberos*** auf jedem Proxyserver installiert werden. Anschließend muss die Univention Configuration Registry-Variable `squid/krb5auth` auf `yes` gesetzt werden und Squid neu gestartet werden.

Bei Verwendung von NTLM-Authentifizierung wird standardmäßig für jede HTTP-Anfrage eine NTLM-Authentifizierung durchgeführt. Wird beispielsweise die Webseite `https://www.univention.de/` aufgerufen, werden neben der eigentlichen HTML-Seite auch weitere Unterseiten und Bilder nachgeladen. Die NTLM-Authentifizierung kann domänenbezogenen zwischengespeichert werden: Wird die Univention Configuration Registry-Variable `squid/ntlmauth/keepalive` auf `yes` gesetzt, wird für nachgelagerte HTTP-Anfragen derselben Domäne keine weitere NTLM-Authentifizierung durchgeführt. Bei Problemen mit lokalen Benutzerkonten kann es helfen diese Variable auf `no` zu setzen.

In der Grundeinstellung können alle Benutzer auf den Proxy zugreifen. Mit der Univention Configuration Registry-Variable `squid/auth/allowed_groups` kann der Zugriff auf eine oder mehrere Gruppen beschränkt werden. Bei Angabe mehrerer Gruppen sind diese durch ein Semikolon zu trennen.

11.5.7. Filterung/Prüfung von Webinhalten mit DansGuardian

Feedback

DansGuardian nimmt Webseiten-Anforderungen aus dem Netzwerk entgegen und prüft, ob diese Zugriffe erlaubt sind. Falls ja, wird die Anfrage an den Proxy-Server Squid weitergeleitet. DansGuardian erlaubt beispielsweise die Sperrung einzelner Dateiarten und -endungen oder des Zugriffs auf Webseiten oder Domains.

Abbildung 11.4. Sperrung einer Web-Seite durch DansGuardian

Angeforderte Dateien können außerdem auf Viren überprüft werden. Dabei kommt in der Standardeinstellung der freie Virenscanner ClamAV zum Einsatz. Die Integration weiterer Virenscanner ist möglich. Dies ist in der erweiterten Netzwerk-Dokumentation beschrieben [ext-doc-net].

Achtung

Der direkte Zugriff auf den Proxy-Server Squid ist hierbei auf Zugriffe vom lokalen Rechner ('localhost') eingeschränkt. Anwender, die auf dem System arbeiten, auf dem Squid und DansGuardian installiert sind, haben so die Möglichkeit, die Filterfunktionen zu umgehen, indem Sie direkt auf Squid zugreifen. Der Web-Proxy und DansGuardian sollten deshalb nur auf dedizierten Systemen installiert werden, auf denen Anwender sich nicht anmelden können.

Nach der Installation von ***univention-dansguardian*** sind der Virenscanner und der Filter für Webinhalte aktiviert.

Das Filtern von Web-Inhalten und der Virenscanner können getrennt voneinander konfiguriert werden. Um den Inhaltsfilter zu deaktivieren, muss die Univention Configuration Registry-Variable `squid/contentscan` auf `no` gesetzt und Squid neu gestartet werden. Um den Virenscanner abzuschalten, ist Univention Configuration Registry-Variable `squid/virusscan` auf `no` zu setzen. Ist keine der beiden Variablen auf `yes` gesetzt, wird DansGuardian nicht verwendet. Nach Änderungen an den Variablen muss Squid und - sofern installiert - DansGuardian neu gestartet werden.

11.5.8. Definition von Inhaltsfiltern für DansGuardian

Webinhalte können anhand von Dateiendungen, MIME-Typen, Webseiten sowie einzelnen URLs gefiltert werden. Es ist dabei möglich, einzelne Rechner oder Nutzer aus der Filterung auszunehmen.

Die Filterfunktion kann über die folgenden Univention Configuration Registry-Variablen konfiguriert werden. Sollen dabei mehrere Werte angegeben werden, sind diese jeweils durch Leerzeichen zu trennen. Die Filterung wird bei DansGuardian auf Basis von Gruppenzugehörigkeiten durchgeführt, d.h. es können pro Gruppe verschiedene Regeln definiert und dadurch verschiedene Berechtigungen beim Zugriff auf das Web realisiert werden. Welche Gruppen von DansGuardian betrachtet werden, wird in der Univention Configuration Registry-Variable `dansguardian/groups` definiert.

Dabei ist zu beachten, dass die erste Gruppe in der Liste eine besondere Rolle spielt. Alle Benutzer, die keiner der angegebenen Gruppen zugeordnet werden können, werden dieser zugeordnet, d.h. die definierten Filteregeln gelten. In der Regel wird dieser Gruppe somit die geringste Berechtigung zugeordnet.

Gruppenänderungen werden erst nach einem Neustart von DansGuardian wirksam, entweder durch das UMC-Modul **Systemdienste** oder auf der Kommandozeile durch den Befehl:

```
/etc/init.d/dansguardian restart
```

Für Änderungen von Filterregeln reicht es aus die Konfigurationsdateien mit dem folgenden Kommando neu einzulesen:

```
dansguardian -g
```

Die Variablen zur Definition der Filterregeln enthalten den Gruppennamen, welcher in der folgenden Liste durch *`group`* ersetzt wird.

Tabelle 11.25. UCR-Variablen für Filterregeln'

UCR-Variable	Beschreibung
`dansguardian/groups/`*`group`*`/banned/extensions`	Dateien mit den angegebenen Dateiendungen dürfen nicht heruntergeladen werden. Der Trennpunkt muss dabei mit angegeben werden. Ist diese Variable leer, werden Standardwerte verwendet. Um alle Dateiendungen zu erlauben, muss die Variable auf ' ' gesetzt werden (Zeichenkette mit einem Leerzeichen). Beispiel: **`'.doc .xls .exe'`**.

UCR-Variable	Beschreibung
`dansguardian/groups/`*`group`*`/banned/mimetypes`	Dateien mit dem angegebenen MIME-Type dürfen nicht heruntergeladen werden. Der MIME-Type wird dabei vom ausliefernden Webserver (bzw. einer darauf laufenden Anwendung) festgelegt. Normalerweise sollten die zu den oben erläuterten Dateiendungen passenden MIME-Type angegeben werden. Ist diese Variable leer, werden Standardwerte verwendet. Um alle MIME-Types zu erlauben, muss die Variable auf ' ' gesetzt werden (Zeichenkette mit einem Leerzeichen). Beispiel: *audio/mpeg application/zip*
`dansguardian/groups/`*`group`*`/banned/sites`	Hiermit können komplette Webseiten gesperrt werden. Beispiel: `illegal-example-website.com`
`dansguardian/groups/`*`group`*`/banned/urls`	Im Gegensatz zum vorherigen Parameter können hiermit einzelne URLs von Webseiten gesperrt werden.
`dansguardian/`*`group`*`/exception/urls`	Der Zugriff auf die hier angegebenen URLs wird nicht durch DansGuardian geprüft.
`dansguardian/`*`group`*`/exception/sites`	Der Zugriff auf die hier angegebenen Webseiten wird nicht durch DansGuardian geprüft.
`dansguardian/bannedipaddresses`	Diese Variable ermöglicht es, einzelne Rechner anhand der IP-Adresse komplett vom Zugriff auf den Proxy-Server auszuschließen.
`dansguardian/exceptionipaddresses`	Hiermit können für einzelne Rechner sämtliche Filterfunktionen deaktiviert werden, sodass von diesem Rechner alle Dateien über den Proxy-Server heruntergeladen werden dürfen. Dies kann nützlich sein, wenn z.B. von einem Administrations-Rechner Dateien für weitere Benutzer heruntergeladen werden sollen.

Achtung

Die Definition einer Ausnahmeregel bei Inhaltsfiltern mit `dansguardian/`*`group`*`/exception/*` führt dazu, dass diese auch von einem Virenscan ausgenommen werden.

11.6. RADIUS

Feedback

Die ***RADIUS*** App erhöht die Sicherheit für mit UCS verwaltete IT-Infrastrukturen durch Zugangskontrollen zu WiFi Netzwerken für Benutzer, Gruppen und Endgeräte über das RADIUS-Protokoll[2]. Die Konfiguration erfolgt über Blacklisten und Whitelisten direkt am Benutzer-, Gruppen- oder Endgeräte-Objekt im UCS Managementsystem. Registrierte Benutzer werden mit ihrem üblichen Domänenpasswort authentisiert, so dass unter anderem *Bring-Your-Own-Device-Konzepte* ermöglicht werden.

11.6.1. Installation

Feedback

RADIUS steht über das App Center (siehe Abschnitt 5.3) zur Verfügung und kann über das entsprechende Univention Management Console-Modul **App Center** installiert werden. Die App kann auf mehreren Systemen installiert werden. Nach der Installation startet die App einen FreeRADIUS[3]-Server. *Authenticators* (z.B. *Access Points*) können den Server via RADIUS kontaktieren und Netzwerkzugangsanfragen prüfen.

[2] https://de.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service
[3] http://freeradius.org/

11.6.2. Konfiguration

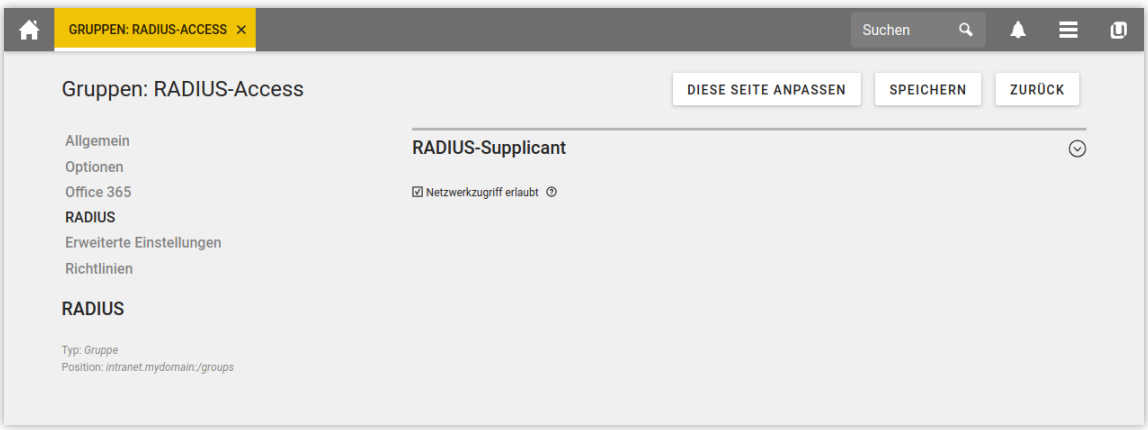
Feedback

11.6.2.1. Erlaubte Benutzer

Feedback

Standardmäßig hat kein Benutzer Zugang zum Netzwerk. Indem die Checkbox für **Netzwerkzugriff erlaubt** im **RADIUS** Reiter aktiviert wird, erhält der Benutzer Zugriff auf das Netzwerk. Die Checkbox kann auch für Gruppen gesetzt werden, so dass alle Benutzer in der Gruppe Zugang erlangen.

Abbildung 11.5. Beispiel für eine Gruppe, die ihren Benutzern Zugang gewährt



11.6.2.2. MAC-Adressfilter

Feedback

Standardmäßig ist allen Geräten der Zugang zum Netzwerk erlaubt, vorausgesetzt der verwendete Benutzer hat Zugriff. Der Netzwerkzugriff kann auch auf spezifische Geräte begrenzt werden. Das kann durch Setzen der Univention Configuration Registry-Variable `radius/mac/whitelisting` auf `true` erreicht werden. Sobald aktiviert, wird das Geräteobjekt beim Zugriff des Geräts auf das Netzwerk über das LDAP-Attribut *macAddress* abgerufen und dem entsprechenden Geräteobjekt muss der Zugang zum Netzwerk auch erlaubt sein (entweder direkt oder über eine der Gruppen).

11.6.2.3. *Access Points* verwalten

Feedback

Alle *Access Points* (Netzwerkzugangspunkte) müssen dem RADIUS-Server bekannt sein. Ein *Access Point* lässt sich entweder pro RADIUS-Server über die Datei `/etc/freeradius/3.0/clients.conf` konfigurieren oder domänenweit per Univention Management Console. Für jeden *Access Point* sollte ein zufälliges, gemeinsames Geheimnis erzeugt werden (Zum Beispiel über den Befehl `makepasswd`.). Der Name kann frei gewählt werden.

Beispiel für einen Eintrag in der `clients.conf` Datei:

```
client AP01 {
    secret = a9RPAeVG
    ipaddr = 192.0.2.101
}
```

Um *Access Points* per Univention Management Console zu verwalten, muss für den *Access Point* ein Rechnerobjekt existieren. Dieses Rechnerobjekt benötigt die Option *RADIUS-Authenticator* (Abbildung 11.6). Für einen *Access Point* bietet sich ein *IP-Managed-Client* als Rechnerobjekt an. Im **RADIUS**-Reiter des Objekts lassen sich nach dem Hinzufügen der Option die Eigenschaften des *Access Points* festlegen (Abbildung 11.7). Es müssen mindestens die IP-Adresse am Rechnerobjekt und ein gemeinsamer, geheimer Schlüssel gesetzt sein. Die Eigenschaften *NAS-Type* und Virtueller Server müssen in der Regel nicht verändert werden.

Access Points, welche per Univention Management Console konfiguriert sind, sind anschließend allen RADIUS-Servern in der Domäne bekannt. Dabei werden die *Access Points* über den Univention Directory Listener in die Datei `/etc/freeradius/3.0/clients.univention.conf` geschrieben und der RADIUS-Server neu gestartet. Um Änderungen zusammenzufassen, geschieht dies verzögert (etwa 15 Sekunden). Neue *Access Points* haben erst nach diesem Neustart Zugriff auf den RADIUS-Server.

Abbildung 11.6. Setzen der RADIUS-Option

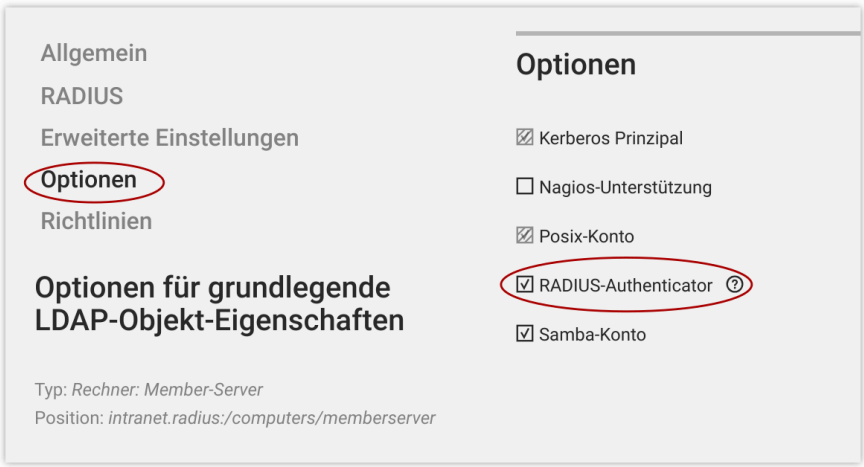
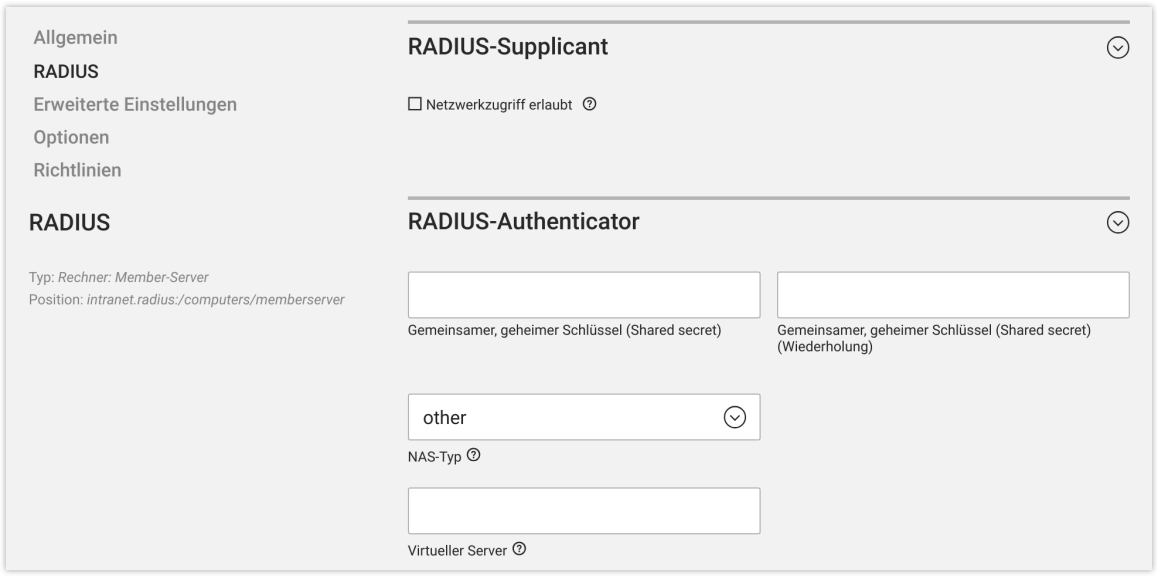


Abbildung 11.7. RADIUS an einem Computerobjekt einstellen



11.6.2.4. *Access Points* und Clients einstellen

Feedback

Die *Access Points* müssen so konfiguriert sein, dass sie 802.1x ("WPA Enterprise") Authentisierung verwenden. Außerdem sollte die "RADIUS Server" Adresse auf die Adresse des Servers gesetzt sein, auf dem die ***RADIUS***-App installiert ist. Das Passwort muss auf den Wert des gemeinsamen Schlüssels aus der Univention Management Console, bzw. des `secret` aus dem Eintrag in der `clients.conf`, gesetzt sein.

WiFi Clients müssen so konfiguriert sein, dass sie *WPA* mit *PEAP* und *MSCHAPv2* für die Authentisierung verwenden.

11.6.3. Fehlersuche

Die ***RADIUS***-App verfügt über eine Logdatei unter `/var/log/univention/radius_ntlm_auth.log`. Die Ausführlichkeit der Logmeldungen lässt sich über die Univention Configuration Registry-Variable `freeradius/auth/helper/ntlm/debug` steuern. Der ***FreeRADIUS-Server*** loggt nach `/var/log/freeradius/radius.log`.

Das Werkzeug ***univention-radius-check-access*** kann zur Untersuchung der aktuellen Zugangsregeln für einen bestimmten Benutzer und/oder eine MAC-Adresse verwendet werden. Es kann als Benutzer root auf dem Server ausgeführt werden, wo das Paket ***univention-radius*** installiert ist.

```
root@master211:~# univention-radius-check-access --username=stefan
DENY 'uid=stefan,cn=users,dc=ucs,dc=local'
'uid=stefan,cn=users,dc=ucs,dc=local'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=local'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=local'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=local'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=local'
Thus access is DENIED.
```

```
root@master211:~# univention-radius-check-access --username=janek
DENY 'uid=janek,cn=users,dc=ucs,dc=local'
'uid=janek,cn=users,dc=ucs,dc=local'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=local'
-> ALLOW 'cn=Network Access,cn=groups,dc=ucs,dc=local'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=local'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=local'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=local'
-> 'cn=Network Access,cn=groups,dc=ucs,dc=local'
Thus access is ALLOWED.
root@master211:~#
```

Das Werkzeug gibt eine detaillierte Erläuterung und setzt den Rückgabewert abhängig vom Ergebnis der Zugangsprüfung (0 für *Zugang gestattet*, 1 für *Zugang verweigert*).

Kapitel 12. Freigaben-Verwaltung

UCS unterstützt die zentrale Verwaltung von Verzeichnisfreigaben. Eine in Univention Management Console registrierte Freigabe wird im Rahmen der UCS-Domänenreplikation auf beliebigen Serversystemen der UCS-Domäne angelegt.

Die Bereitstellung für die zugreifenden Clients kann über CIFS (unterstützt von Windows/Linux-Clients) und/oder NFS (vorrangig unterstützt von Linux/Unix) erfolgen. Die in der Univention Management Console verwalteten NFS-Freigaben können von Clients sowohl über NFSv3, als auch über NFSv4 eingebunden werden.

Wird eine Verzeichnisfreigabe gelöscht, bleiben die in dem Verzeichnis freigegebenen Daten auf einem Server erhalten.

Um auf einer Freigabe Access Control Lists einzusetzen, muss das unterliegende Linux-Dateisystem POSIX-ACLs unterstützen. In UCS unterstützen die Dateisysteme `ext3`, `ext4` und `XFS` POSIX-ACLs. Die Samba-Konfiguration erlaubt außerdem die Speicherung von DOS-Datei-Attributen in erweiterten Attributen des Unix-Dateisystems. Um erweiterte Attribute zu nutzen, muss die Partition mit der Mount-Option `user_xattr` eingebunden werden.

12.1. Zugriffsrechte auf Daten in Freigaben

Feedback

Die Verwaltung von Zugriffsrechten auf Dateien erfolgt in UCS anhand von Benutzern und Gruppen. Alle Fileserver der UCS-Domäne greifen über das LDAP-Verzeichnis auf identische Benutzer- und Gruppendaten zu.

Pro Datei werden drei Zugriffsrechte unterschieden: Lesen, Schreiben und Ausführen. Pro Verzeichnis gelten ebenfalls drei Zugriffsrechte: Ebenso Lesen und Schreiben, das Ausführ-Recht bezieht sich hier auf die Berechtigung in ein Verzeichnis zu wechseln.

Jede Datei/Verzeichnis wird von einem Benutzer und einer Gruppe besessen. Die drei oben genannten Rechte können jeweils auf den Besitzer, die Besitzer-Gruppe und alle anderen angewendet werden.

Ist die *setuid*-Option für eine ausführbare Datei gesetzt, kann diese von Benutzern mit den Rechten des Besitzers oder der Besitzergruppe ausgeführt werden.

Wird die Option *setgid* für ein Verzeichnis gesetzt, erben dort angelegte Dateien die Besitzergruppe des Verzeichnisses. Werden weitere Verzeichnisse angelegt, erben diese ebenfalls die Option.

Ist die Option *sticky bit* für ein Verzeichnis aktiviert, können Dateien in dem Verzeichnis nur von dem Besitzer der Datei oder durch den root-Benutzer gelöscht werden.

Mit Access Control Lists sind noch mächtigere Berechtigungsmodelle möglich. Die Konfiguration von ACLs ist in SDB 1042 beschrieben.

Im Unix-Berechtigungsmodell - und somit unter UCS - reicht das Schreibrecht auf eine Datei nicht aus, um die Berechtigungen einer Datei zu verändern. Dies bleibt den Besitzern/der Besitzergruppe einer Datei vorbe-

http://sdb.univention.de/1042

halten. Unter Microsoft Windows hingegen verfügen alle Benutzer mit Schreibrechten auch die über Berechtigung, die Berechtigungen anzupassen. Dieses Verhalten kann für CIFS-Freigaben angepasst werden (siehe Abschnitt 12.2).

Beim Anlegen einer Verzeichnisfreigabe werden nur initiale Besitzer und Zugriffsrechte vergeben. Existiert das Verzeichnis bereits, werden die Berechtigungen des vorhandenen Verzeichnisses angepasst.

Berechtigungsänderungen an einem freigegebenen Verzeichnis, die direkt im Dateisystem vorgenommen wurden, werden nicht an das LDAP-Verzeichnis weitergeleitet. Wird die Berechtigungen/Besitzer in Univention Management Console bearbeitet, werden die Änderungen im Dateisystem überschrieben. Einstellungen der Freigabewurzel sollten deshalb nur mit Univention Management Console gesetzt und bearbeitet werden. Die weitere Anpassung der Zugriffsrechte der unterliegenden Verzeichnisses erfolgt dann von den zugreifenden Clients, z.B. über den Windows-Explorer, oder direkt über Kommandozeilenbefehle auf dem Fileserver.

Die Freigabe *homes* nimmt unter Samba eine Sonderstellung ein. Sie dient der Freigabe der Heimatverzeichnisse der Benutzer. Für jeden Benutzer wird diese Freigabe automatisch in das eigene Heimatverzeichnis umgewandelt. Deswegen ignoriert Samba die der Freigabe zugewiesenen Rechte und verwendet die Rechte des jeweiligen Heimatverzeichnisses.

12.2. Verwaltung von Freigaben in UMC

Feedback

Verzeichnisfreigaben werden im UMC-Modul *Freigaben* verwaltet (siehe auch Abschnitt 4.4).

Beim Hinzufügen/Bearbeiten/Entfernen einer Freigabe wird diese in die Datei `/etc/exports`, bzw. in die Samba-Konfigurationsdatei eingetragen/modifiziert oder entfernt.

Abbildung 12.1. Anlegen einer Freigabe in UMC

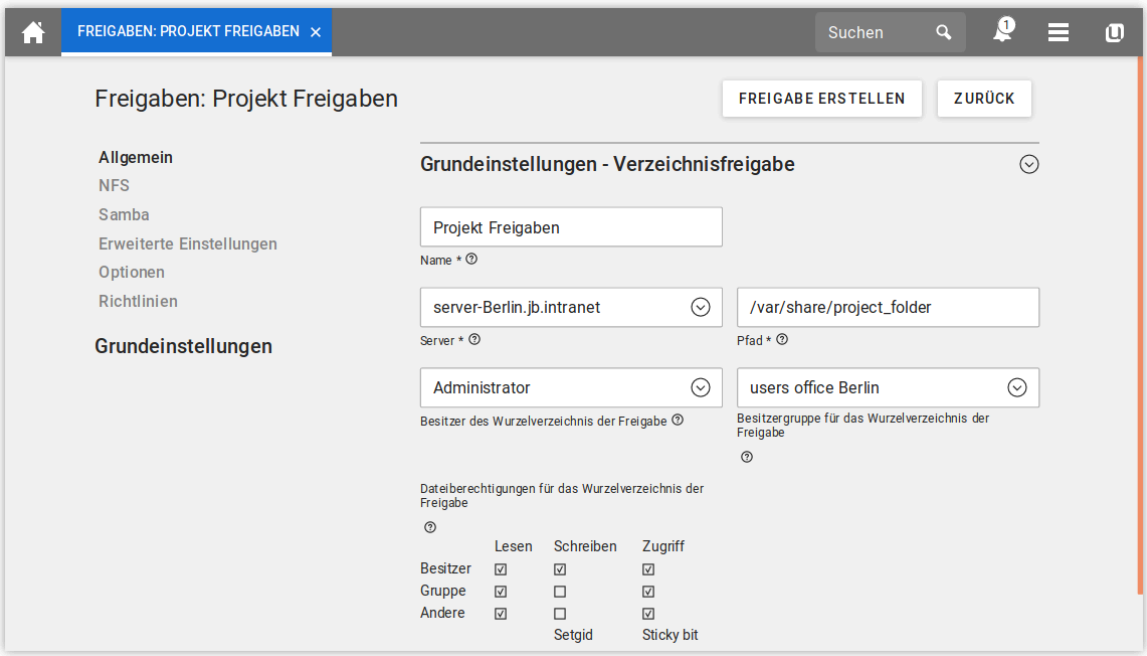


Tabelle 12.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name	Hier ist der Name der Freigabe einzutragen. Der Name darf nur aus Buchstaben, Ziffern, Punkten oder Leerzeichen bestehen und muss mit mit einem Buchstaben oder einer Ziffer beginnen und enden.

Attribut	Beschreibung
Server	Der Server, auf dem die Freigabe liegt. Zur Wahl stehen alle im LDAP-Verzeichnis für die Domäne eingetragenen Rechner vom Typ Domänencontroller Master/Backup/Slave und Memberserver, die in einer DNS Forward Lookup Zone im LDAP-Verzeichnis eingetragen sind.
Pfad	Der absolute Pfad des freizugebenden Verzeichnisses ohne Anführungszeichen (auch wenn der Pfad z.B. Leerzeichen enthält). Wenn das Verzeichnis noch nicht existiert, wird es automatisch auf dem ausgewählten Server angelegt. Ist die Univention Configuration Registry-Variable `listener/shares/rename` auf `yes` gesetzt, wird bei der Änderung des Pfads der Inhalt eines bestehenden Verzeichnisses verschoben. Auf und unterhalb von `/proc`, `/tmp`, `/root`, `/dev` und `/sys` können keine Freigaben angelegt oder dorthin verschoben werden.
Besitzer des Wurzelverzeichnis der Freigabe	Der Benutzer, der das Wurzelverzeichnis der Freigabe gehören soll, siehe Abschnitt 12.1.
Besitzergruppe für das Wurzelverzeichnis der Freigabe	Die Gruppe, der das Wurzelverzeichnis der Freigabe gehören soll, siehe Abschnitt 12.1.
Dateiberechtigungen für das Wurzelverzeichnis der Freigabe	Die Lese-, Schreib- und Zugriffsrechte für das Wurzelverzeichnis der Freigabe, siehe Abschnitt 12.1.

Tabelle 12.2. Reiter 'NFS'

Attribut	Beschreibung
NFS-Schreibzugriff	Erlaubt schreibenden NFS-Zugriff auf diese Freigabe, ansonsten kann die Freigabe nur lesend verwendet werden.
Subtree-Überprüfung	Wird nur ein Unterverzeichnis eines Dateisystems exportiert, muss der NFS-Server bei jedem Zugriff überprüfen, ob die zugegriffene Datei auf dem exportierten Dateisystem und in dem exportierten Pfad liegt. Für diese Prüfung werden Pfad-Informationen an den Client übergeben. Die Aktivierung dieser Funktion kann zu Problemen führen, wenn eine auf dem Client geöffnete Datei umbenannt wird.
User-ID für Root-Benutzer ändern (Root-Squashing)	Die Identifikation von Nutzern im NFS-Standardverfahren erfolgt über User-IDs. Um zu verhindern, dass ein lokaler Root-Nutzer auf fremden Freigaben ebenfalls mit Root-Rechten arbeitet, kann der Root-Zugriff umgelenkt werden. Ist diese Option aktiviert, erfolgen Root-Zugriffe als Benutzer nobody. Die standardmäßig leere lokale Gruppe `staff` verfügt über Privilegien, die `root`-Rechten recht nahe kommen, wird aber vom Umlenkungs-Mechanismus nicht berücksichtigt. Dies sollte bei der Aufnahme von Nutzern in diese Gruppe berücksichtigt werden!
NFS-Synchronisation	Der Synchronisations-Modus für die Freigabe. Mit der Einstellung `sync` werden Daten direkt auf das unterliegende Speichermedium geschrieben. Die gegenteilige Einstellung - `async` - kann die Performance verbessern, birgt aber auch das Risiko von Datenverlusten wenn der Server ohne kontrolliertes Herunterfahren abgeschaltet wird.
Zugriff nur für diese Rechner, IP-Adressen oder Netze erlauben	Standardmäßig wird allen Rechnern der Zugriff auf eine Freigabe erlaubt. In die Auswahlliste können Rechnernamen und IP-Adres-

Attribut	Beschreibung
	sen aufgenommen werden, auf die dann der Zugriff auf die Freigabe beschränkt wird. Hier ließe sich etwa der Zugriff auf eine Freigabe mit Maildaten auf den Mailserver der Domäne einschränken.

Tabelle 12.3. Reiter 'Samba'

Attribut	Beschreibung
Samba-Name	Der NetBIOS-Name der Freigabe. Unter diesem Namen wird die Freigabe auf auf Windows-Rechnern in der Netzwerkumgebung angezeigt.. Univention Management Console übernimmt beim Hinzufügen einer Verzeichnisfreigabe als Vorgabe den Namen, der auf der Karteikarte **Allgemein** im Feld **Name** eingetragen ist.
Samba-Schreibzugriff	Erlaubt den Schreibzugriff auf diese Freigabe.
Freigabe wird in der Windows-Netzwerkumgebung angezeigt	Konfiguriert, ob diese Freigabe auf Windows-Rechnern in der Netzwerkumgebung angezeigt werden soll.
Anonymen Nur-Lese-Zugriff mit Gastbenutzer erlauben	Erlaubt den Zugriff auf diese Freigabe ohne Passwortabfrage. Alle Zugriffe werden dabei über einen gemeinsamen Gast-Nutzer `nobody` durchgeführt.
MSDFS-Wurzel	Diese Option ist in Abschnitt 12.3 dokumentiert.
Benutzer mit Schreibrechten dürfen die Berechtigungen verändern	Wird diese Option aktiviert, erhalten alle Benutzer mit Schreibrechten auf eine Datei auch die Möglichkeiten Berechtigungen, ACL-Einträge und Dateibesitzrechte zu ändern, siehe Abschnitt 12.1.
Verstecke nicht lesbare Dateien und Verzeichnisse	Wenn diese Option aktiviert ist, werden Dateien, die anhand der Dateirechte für einen Benutzer nicht lesbar sind, für diesen nicht angezeigt.
VFS-Objekte	Virtual File System (VFS)-Module werden in Samba verwendet, um Aktionen vor dem Zugriff auf das Dateisystem einer Freigabe auszuführen, z.B. ein Virenscanner, der jede infizierte Datei, auf die in der Freigabe zugegriffen wird, in einem Quarantänebereich ablegt oder eine serverseitige Implementierung einer Papierkorb-Löschung von Dateien.

Tabelle 12.4. Reiter 'Samba-Rechte' (erweiterte Einstellungen)

Attribut	Beschreibung
Erzwungener Benutzer	Der Benutzername, mit dessen Namen, Rechten und primärer Gruppe alle Dateioperationen zugreifender Benutzer ausgeführt werden sollen. Der Benutzername wird erst verwendet, nachdem der Benutzer mit seinem tatsächlichen Benutzernamen und gültigem Passwort eine Verbindung zur Samba-Freigabe aufgebaut hat. Ein gemeinsamer Benutzername ist nützlich, um Dateien gemeinsam zu benutzen, kann bei falscher Anwendung aber Sicherheitsprobleme verursachen.
Erzwungene Gruppe	Eine Gruppe, die alle Benutzer, die sich mit dieser Freigabe verbinden, als primäre Gruppe verwenden sollen. Dadurch gelten die Rechte dieser Gruppe als Gruppenrechte für alle diese Benutzer. Eine hier eingetragene Gruppe hat Vorrang über eine Gruppe, die über das Eingabefeld **Erzwungener** zur primären Gruppe eines Benutzers geworden ist. Wird dem Gruppennamen ein Plus-Zeichen vorangestellt, wird die Gruppe nur solchen Benutzern als primäre Gruppe zugeschrieben, die

Attribut	Beschreibung
	bereits Mitglied dieser Gruppe sind. Alle anderen Benutzer behalten ihre gewöhnliche primäre Gruppe
Gültige Benutzer oder Gruppen	Namen von Benutzern oder Gruppen, die auf diese Samba-Freigabe zugreifen dürfen. Alle anderen Benutzern wird der Zugriff verweigert. Wenn das Feld leer ist, dürfen alle Benutzer - ggf. mit ihrem Passwort - auf die Freigabe zugreifen. Diese Option ist nützlich, um Zugriffe auf eine Freigabe über die Dateiberechtigungen hinaus auf Ebene des Fileservers abzusichern. Die Einträge sind durch Leerzeichen zu trennen. Durch die Zeichen @, + und & in Verbindung mit einem Gruppennamen kann den Mitgliedern der angegebenen Gruppe die Berechtigung zum Zugriff auf die Samba-Freigabe erteilt werden: ◦ Ein Name, der mit @ beginnt, wird zunächst als NIS-Netgroup interpretiert. Wenn keine NIS-Netgroup mit diesem Namen gefunden wird, wird der Name als UNIX-Gruppe angesehen. ◦ Ein Name, der mit + beginnt, wird ausschließlich als UNIX-Gruppe aufgefasst, ein Name, der mit & beginnt, ausschließlich als NIS-Netgroup. ◦ Ein Name, der mit +& beginnt, wird zunächst als UNIX-Gruppe interpretiert. Wenn keine UNIX-Gruppe mit diesem Namen gefunden wird, wird der Name als NIS-Netgroup betrachtet. Die Zeichen &+ als Namensanfang entsprechen @.
Nicht erlaubte Benutzer oder Gruppen	Die hier aufgeführten Benutzer oder Gruppen dürfen auf diese Samba-Freigabe nicht zugreifen. Die Syntax ist identisch zu den gültigen Benutzern. Wenn ein Benutzer oder eine Gruppe in der Liste der gültigen Benutzer und der nicht erlaubten Benutzer enthalten ist, so wird der Zugriff verweigert.
Schreibberechtigung auf diese Benutzer/Gruppen beschränken	Nur die aufgeführten Benutzer oder Gruppen erhalten Schreibrecht auf die diese Freigabe.
Zugelassene Rechner/Netze	Namen von Rechnern, die auf diese Samba-Freigabe zugreifen dürfen. Allen anderen Rechnern wird der Zugriff verweigert. Neben Rechnernamen können auch IP- oder Netzwerkadressen angegeben werden, bspw. `192.0.2.0/255.255.255.0`.
Nicht zugelassene Rechner/Netze	Das Gegenteil von den zugelassenen Rechnern. Sollte ein Rechner in beiden Listen auftauchen, so wird dem Rechner der Zugriff auf die Samba-Freigabe gestattet.
NT ACL-Support	Ist diese Option aktiviert, versucht Samba, POSIX-ACLs unter Windows anzuzeigen und Änderungen an den ACLs, die unter Windows vorgenommen werden, in die POSIX-ACLs zu übernehmen. Wenn die Option nicht gesetzt ist, werden vorhandene POSIX-ACLs beachtet, aber nicht unter Windows angezeigt und können von dort nicht verändert werden.
Ererbte ACLs	Bei Aktivierung dieser Option erbt jede in dieser Freigabe neu erzeugte Datei die ACL (Access Control List) des Verzeichnisses, in dem sie angelegt wird.

Attribut	Beschreibung
Neue Dateien und Verzeichnisse erhalten den Besitzer des übergeordneten Verzeichnisses	Bei Aktivierung dieser Option wird jede neu erzeugte Datei dem Besitzer des übergeordneten Verzeichnis zugeordnet und nicht dem Benutzer, der die Datei erstellt hat.
Neue Dateien und Verzeichnisse erhalten die Zugriffsrechte des übergeordneten Verzeichnisses	Bei Aktivierung dieser Option werden für jede Datei oder jedes Verzeichnis, die in einer Freigabe neu erzeugt werden, automatisch die UNIX-Rechte des übergeordneten Verzeichnisses übernommen.

Wenn von einem Windows-Rechner aus eine neue Datei auf einem Samba-Server angelegt wird, werden die Rechte der Datei in mehreren Schritten gesetzt.

1. Zunächst werden die DOS-Rechte in Unix-Rechte übersetzt.

2. Anschließend werden die Rechte durch den **Datei-Modus** gefiltert. Nur die Unix-Rechte, die im Datei-Modus markiert sind, bleiben erhalten. Rechte, die hier nicht gesetzt sind, werden entfernt. Die Rechte müssen also als Unix-Rechte und im Datei-Modus gesetzt sein, um erhalten zu bleiben.

3. Im nächsten Schritt werden die Rechte um die unter **Erzwinge Datei-Modus** gesetzten Rechte ergänzt. Als Ergebnis hat die Datei alle Rechte, die nach Schritt 2 oder unter **Erzwinge Datei-Modus** gesetzt sind. Rechte, die unter **Erzwinge Datei-Modus** markiert sind, werden also auf jeden Fall gesetzt.

Entsprechend erhält ein neu angelegtes Verzeichnis zunächst die Rechte, die sowohl als Unix-Rechte als auch im **Verzeichnis-Modus** gesetzt sind. Danach werden die Rechte ergänzt, die unter **Erzwinge Verzeichnis-Modus** markiert sind.

In ähnlicher Weise werden die Sicherheits-Einstellungen auf bestehende Dateien und Verzeichnisse angewandt, deren Rechte unter Windows bearbeitet werden:

Ausschließlich Rechte, die im **Sicherheits-Modus** bzw. **Sicherheits-Verzeichnis-Modus** markiert sind, können von Windows aus verändert werden. Anschließend werden die Rechte, die unter **Erzwinge Sicherheits-Modus** bzw. **Erzwinge Sicherheits-Verzeichnis-Modus** markiert sind, auf jeden Fall gesetzt.

Die Parameter **Datei-Modus** und **Erzwinge Datei-Modus** bzw. **Verzeichnis-Modus** und **Erzwinge Verzeichnis-Modus** finden also beim Anlegen einer Datei bzw. eines Verzeichnisses Anwendung, die Parameter **Sicherheits-Modus** und **Erzwinge Sicherheits-Modus** bzw. **Sicherheits-Verzeichnis-Modus** und **Erzwinge Sicherheits-Verzeichnis-Modus** beim Ändern der Rechte.

Anmerkung

Es ist zu beachten, dass sich die Sicherheitseinstellungen nur auf den Zugriff über Samba beziehen.

Der Benutzer auf Windows-Seite erhält keinen Hinweis, dass die Datei- bzw. Verzeichnisrechte gegebenenfalls entsprechend den Samba-Einstellungen auf dieser Karteikarte verändert werden.

Tabelle 12.5. Reiter 'Erweiterte Samba-Rechte' (erweiterte Einstellungen)

Attribut	Beschreibung
Datei-Modus	Die Rechte, die Samba beim Anlegen einer Datei übernehmen soll, sofern sie unter Windows gesetzt sind.
Verzeichnis-Modus	Die Rechte, die Samba beim Anlegen eines Verzeichnisses übernehmen soll, sofern sie unter Windows gesetzt sind.
Erzwinge Datei-Modus	Die Rechte, die Samba beim Anlegen einer Datei auf jeden Fall setzen soll, also unabhängig davon, ob sie unter Windows gesetzt wurden oder nicht.

Attribut	Beschreibung
Erzwinge Verzeichnis-Modus	Die Rechte, die Samba beim Anlegen eines Verzeichnisses auf jeden Fall setzen soll, also unabhängig davon, ob sie unter Windows gesetzt wurden oder nicht.
Sicherheitsmodus	Die Dateirechte, an denen Samba Änderungen von Windows-Seite aus zulassen soll.
Verzeichnis-Sicherheitsmodus	Die Verzeichnisrechte, an denen Samba Änderungen von Windows-Seite aus zulassen soll.
Erzwinge Sicherheitsmodus	Die Rechte, die Samba auf jeden Fall setzen soll (unabhängig davon, ob die Rechte unter Windows gesetzt wurden oder nicht), wenn die Rechte einer Datei von Windows-Seite aus geändert werden.
Erzwinge Verzeichnis-Sicherheitsmodus	Die Rechte, die Samba auf jeden Fall setzen soll, wenn die Rechte eines Verzeichnisses von Windows-Seite aus geändert werden (unabhängig davon, ob die Rechte unter Windows gesetzt wurden oder nicht).

Tabelle 12.6. Reiter 'Samba-Optionen' (erweiterte Einstellungen)

Attribut	Beschreibung
Locking	Unter Locking versteht man das Sperren konkurrierender Zugriffe auf eine Datei. Bei Aktivierung dieses Auswahlkästchens sperrt Samba auf Client-Anfrage den Zugriff auf Dateien. Das Deaktivieren von Locking kann nützlich sein, um die Performance zu erhöhen, sollte jedoch auf Freigaben mit Schreibzugriff grundsätzlich nicht gesetzt werden, weil Dateien bei konkurrierenden Schreibzugriffen ohne Locking korrumpiert werden können.
Blocking Locks	Clients können einen Lock-Request mit einem Zeitlimit für einen Bereich einer geöffneten Datei senden. Kann Samba einem Lock-Request nicht entsprechen und ist diese Option aktiviert, so versucht Samba bis zum Ablauf des Zeitlimits periodisch den angefragten Dateibereich zu sperren. Ist die Option deaktiviert, wird kein weiterer Versuch unternommen.
Strict Locking	Ist diese Option aktiviert, prüft Samba bei jedem Lese- und Schreibzugriff, ob die Datei gesperrt ist und verweigert ggf. den Zugriff. Auf einigen Systemen kann dies lange dauern. Ist die Option deaktiviert, prüft Samba nur auf Client-Anfrage, ob eine Datei gesperrt ist. Gut konfigurierte Clients bitten in allen wichtigen Fällen um eine Prüfung, so dass diese Option im Regelfall nicht notwendig ist.
Oplocks	Wird diese Option aktiviert, verwendet Samba so genannte *opportunistic locks*. Dies kann die Zugriffsgeschwindigkeit auf Dateien deutlich erhöhen. Allerdings erlaubt die Option Clients Dateien in großem Umfang lokal zwischenzuspeichern. Deswegen kann es in unzuverlässigen Netzwerken nötig sein, auf Oplocks zu verzichten.
Level 2 Oplocks	Bei Aktivierung dieser Option unterstützt Samba eine erweiterte Form der Oplocks, sogenannte *opportunistic read-only locks* oder auch Level-2-Oplocks. Windows-Clients, die ein Read-write-Oplock auf eine Datei halten, können dieses Oplock dann zu einem Read-only-Oplock herunterstufen anstatt das Oplock ganz aufgeben zu müssen, sobald

Attribut	Beschreibung
	ein zweiter Client die Datei öffnet. Alle Clients, die Level-2-Oplocks unterstützen, speichern dann nur Lesezugriffe auf die Datei zwischen. Wenn einer der Clients in die Datei schreibt, werden alle anderen Clients benachrichtigt, ihre Oplocks aufzugeben und ihre Zwischenspeicher zu löschen. Es wird empfohlen, diese Option zu aktivieren, um den Zugriff auf Dateien, die normalerweise nicht geschrieben werden (z.B. Programme/ausführbare Dateien) zu beschleunigen. **Anmerkung** Wenn Kernel-Oplocks unterstützt werden, werden Level-2-Oplocks nicht bewilligt, selbst wenn die Option aktiviert ist. Die Option ist nur wirksam, wenn das Auswahlkästchen **Oplocks** ebenfalls markiert ist.
Fake Oplocks	Bei Aktivierung dieser Optionen bewilligt Samba alle Oplock-Anfragen unabhängig von der Anzahl auf eine Datei zugreifender Clients. Dies verbessert die Performance deutlich und ist sinnvoll bei Freigaben, auf die nur lesend zugegriffen werden kann (z.B. CD-ROMs) oder bei denen sichergestellt ist, dass niemals mehrere Clients gleichzeitig auf sie zugreifen können. Wenn nicht ausgeschlossen werden kann, dass mehrere Clients lesend und schreibend auf eine Datei zugreifen, sollte die Option nicht aktiviert werden, weil es sonst zu Datenverlusten kommen kann.
Blockgröße	Die Blockgröße in Byte, in der freier Festplattenplatz an Clients gemeldet werden soll. Standardmäßig beträgt sie 1024 Byte.
Richtlinie für das Caching beim Client	Konfiguriert, auf welche Weise Clients Dateien aus dieser Freigabe offline zwischenspeichern sollen. Zur Wahl stehen *manuell*, *Dokumente*, *Programme* und *deaktiviert*.
Verstecke Dateien	Dateien und Verzeichnisse, die unter Windows nicht sichtbar sein sollen. Die Dateien bzw. Verzeichnisse erhalten das Datei-Attribut *hidden*. Datei- bzw. Verzeichnisnamen müssen unter Beachtung von Groß- und Kleinschreibung angegeben werden. Die einzelnen Einträge sind durch Schrägstriche zu trennen. Da der Schrägstrich nicht als Verzeichnistrenner eingegeben werden kann, dürfen nur Namen, aber keine Pfade eingetragen werden. Alle Dateien bzw. Verzeichnisse mit diesen Namen innerhalb der Freigabe werden dann versteckt. Die Namen dürfen Leerzeichen und die Platzhalter * und ? enthalten. */.*/test/* z.B. versteckt alle Dateien und Verzeichnisse, die mit einem Punkt beginnen oder test heißen. **Anmerkung** Einträge in diesem Feld beeinflussen die Geschwindigkeit von Samba, da vor Anzeige von Freigabeinhalten alle Dateien und Verzeichnisse auf Übereinstimmung mit den gesetzten Filtern geprüft werden müssen.

Attribut	Beschreibung
Postexec-Skript	Ein Skript oder ein Befehl, der auf dem Server ausgeführt werden soll, wenn die Verbindung zu dieser Freigabe beendet wird.
Preexec-Skript	Ein Skript oder ein Befehl, der auf dem Server bei jeder Verbindungsaufnahme zu dieser Freigabe ausgeführt werden soll.

Tabelle 12.7. Reiter 'Samba-Erweiterte-Einstellungen' (erweiterte Einstellungen)

Attribut	Beschreibung
Erweiterte Einstellungen für Freigaben	Neben den standardmäßig konfigurierbaren Eigenschaften einer Samba-Freigabe ermöglicht diese Einstellung beliebige weitere Samba-Einstellungen an einer Freigabe zu setzen. Eine Liste der verfügbaren Optionen kann mit dem Befehl `man smb.conf` abgerufen werden. Unter **Schlüssel** ist der Name der Option anzugeben und unter **Value** der zu setzende Wert. Doppelt angegebene Konfigurationsoptionen werden nicht überprüft. **Achtung** Das Setzen erweiterter Samba-Einstellungen ist nur in Sonderfällen nötig. Die Optionen sollten vor dem Setzen gründlich geprüft werden, da sie unter Umständen sicherheitsrelevante Auswirkungen haben können.

Tabelle 12.8. Reiter 'Erweiterte NFS-Einstellungen' (erweiterte Einstellungen)

Attribut	Beschreibung
Erweiterte NFS-Einstellungen für Freigaben	Neben den im Reiter **NFS** konfigurierbaren Eigenschaften einer NFS-Freigabe ermöglicht diese Einstellung beliebige weitere NFS-Einstellungen an einer Freigabe zu setzen. Eine Liste der verfügbaren Optionen kann mit dem Befehl `man 5 exports` abgerufen werden. Doppelt angegebene Konfigurationsoptionen werden nicht überprüft. **Achtung** Das Setzen erweiterter NFS-Einstellungen ist nur in Sonderfällen nötig. Die Optionen sollten vor dem Setzen gründlich geprüft werden, da sie unter Umständen sicherheitsrelevante Auswirkungen haben können.

Tabelle 12.9. Reiter 'Optionen'

Attribut	Beschreibung
Für Samba-Clients exportieren	Diese Option legt fest, ob die Freigabe für Samba-Clients exportiert werden soll.
Für NFS-Clients exportieren	Diese Option legt fest, ob die Freigabe für NFS-Clients exportiert werden soll.

12.3. Unterstützung von MSDFS

Feedback

Das Microsoft Distributed File System (MSDFS) ist ein verteiltes Dateisystem, das es ermöglicht, Freigaben über mehrere Server und Pfade auf eine virtuelle Ordner-Hierarchie abzubilden. Dadurch kann die Last auf verschiedene Server verteilt werden.

Das Setzen der **MSDFS-Wurzel** Option an einer Freigabe (siehe Abschnitt 12.2) gibt an, dass es sich bei dem freigegebenen Ordner um eine Freigabe handelt, die für MSDFS genutzt werden kann. Nur innerhalb einer solchen MSDFS-Wurzel werden Verweise auf andere Freigaben angezeigt, andernfalls werden diese ausgeblendet.

Um die Funktionen eines verteilten Dateisystem nutzen zu können, muss auf dem Fileserver die Univention Configuration Registry-Variable `samba/enable-msdfs` auf `yes` gesetzt werden. Anschließend muss der Samba-Dienst neu gestartet werden.

Um einen Verweis mit dem Namen `zufb` von Server `sa` in der Freigabe `fa` auf die Freigabe `fb` des Servers `sb` anzulegen muss im Ordner `fa` folgender Befehl ausgeführt werden.

```
ln -s msdfs:sb\\fb zufb
```

Dieser Verweis wird in jedem MSDFS fähigem Client (z.B. `Windows 2000` und `Windows XP`) als regulärer Ordner angezeigt.

Achtung

Auf Wurzel-Verzeichnisse sollten nur eingeschränkte Benutzergruppen Schreibzugriff haben. Andernfalls könnten Benutzer Verweise auf andere Freigaben umlenken und so Dateien abfangen oder manipulieren. Weiterhin müssen Pfade zu den Freigaben und die Verweise komplett klein geschrieben werden. Sollten Änderungen an den Verweisen vorgenommen werden, müssen beteiligte Clients neu gestartet werden. Weitere Informationen dazu befinden sich in der Samba Dokumentation [samba3-howto-chapter-20] im Kapitel 'Hosting a Microsoft Distributed File System Tree'.

12.4. Konfiguration von Dateisystem-Quota

Feedback

UCS erlaubt die Limitierung des Speicherplatzes, den ein Benutzer auf einer Partition verwenden kann. Diese Schwellwerte können entweder als eine Menge von Speicherplatz (z.B. 500 MB pro Benutzer) oder als maximale Anzahl von Dateien ohne feste Größenbeschränkung angegeben werden.

Unterschieden werden dabei zwei Arten von Schwellwerten:

- Das *Hard-Limit* ist die maximale Speichermenge, die ein Benutzer in Anspruch kann. Wird sie erreicht, können keine weiteren Dateien angelegt werden.

- Wird das *Soft-Limit* erreicht - das kleiner sein muss als das Hard-Limit - und liegt der Speicherplatzverbrauch weiterhin unter dem Hard-Limit, wird dem Benutzer eine Übergangsfrist von sieben Tagen eingeräumt um unbenutzte Daten zu löschen. Nach Ablauf der sieben Tage können keine weiteren Dateien mehr angelegt oder verändert werden. Benutzern, die über CIFS auf ein Dateisystem mit erschöpfter Quota zugreifen, wird eine Warnung angezeigt (als Schwellwert wird dabei das Soft-Limit angesetzt).

Ein konfigurierter Quota-Wert von *0* wird als unbegrenzte Quota ausgewertet.

Quotas können entweder über das UMC-Modul **Dateisystem Quota** oder über eine Richtlinie für Freigaben definiert werden, siehe Abschnitt 12.4.2.

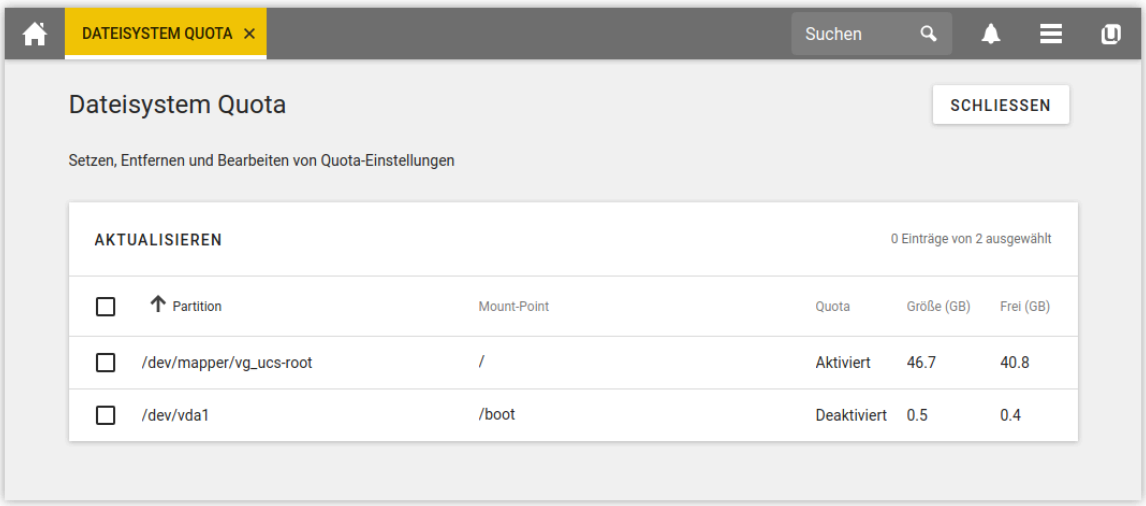
Dateisystem-Quota können nur auf Partitionen mit den Dateisystemen `ext2`, `ext3`, `ext4` und `xfs` angelegt werden. Bevor Dateisystem-Quota konfiguriert werden, muss der Quota-Support pro Partition aktiviert werden, siehe Abschnitt 12.4.1.

12.4.1. Aktivierung von Dateisystem-Quota

Feedback

Im UMC-Modul **Dateisystem Quota** werden alle Partitionen aufgeführt, auf denen Quota eingerichtet werden können. Es werden nur Partitionen angezeigt, die aktuell unter einem Mount Point eingebunden sind.

Abbildung 12.2. Aktivierung von Quota



Der aktuelle Quota-Status (Aktiviert/Deaktiviert) wird angezeigt und kann mit **Aktivieren** und **Deaktivieren** verändert werden.

Nachdem auf einer xfs Root-Partition Quota aktiviert wurde, muss das System neu gestartet werden

12.4.2. Konfiguration von Dateisystem-Quota

Feedback

Quotas können entweder über das UMC-Modul **Dateisystem Quota** oder über eine Richtlinie für Freigaben definiert werden, siehe Abschnitt 4.6. Die Konfiguration über die Richtlinie erlaubt die Festlegung eines Standard-Werts für alle Benutzer, während das UMC-Modul eher für die flexible Konfiguration von Benutzer-Quota für einzelne Benutzer geeignet ist.

Die benutzerspezifischen Quota können im UMC-Modul **Dateisystem Quota** editiert werden. Für alle aktivierten Partitionen kann mit dem Bleistift-Symbol die erlaubten Speichermengen festgelegt werden. Alle Einstellungen werden benutzerspezifisch festgelegt. Mit **Hinzufügen** können die Schwellwerte für Soft- und Hard-Limits für einen Benutzer festgelegt werden.

Die Quota-Einstellungen können auch über eine Freigaben-Richtlinie von Typ **Benutzer-Quota** festgelegt werden. Die Einstellungen gelten für alle Benutzer einer Freigabe; es ist nicht möglich an einer Richtlinie für verschiedene Benutzer unterschiedliche Quota-Limitierungen festzulegen.

Über eine Freigabe-Richtlinie gesetzte Quotaeinstellungen werden standardmäßig nur einmal ausgewertet und auf das Dateisystem angewendet. Sollte sich die Einstellung ändern, wird dies nicht automatisch bei der nächsten Anmeldung des Benutzers angewendet. Um geänderte Quota-Werte zu übernehmen, kann an der Freigabe-Richtlinie der Punkt *Einstellungen bei jedem Login anwenden* aktiviert werden.

Quota-Richtlinien können nur auf Partitionen angewendet werden, für die die Quota-Unterstützung im UMC-Modul aktiviert wurde, siehe Abschnitt 12.4.1.

Anmerkung

Dateisystem-Quotas können immer nur auf vollständige Partitionen angewendet werden. Auch wenn die Richtlinien für Freigaben definiert werden, werden sie auf vollständige Partitionen angewendet. Wenn also beispielsweise auf einem Server drei Freigaben bereitgestellt werden, die alle auf der separaten `/var/`-Partition abgelegt werden und werden drei verschiedene Richtlinien konfiguriert und angewendet, so gilt die restriktivste Einstellung für die komplette Partition. Wenn unterschiedliche Quota verwendet werden sollen, wird empfohlen die Daten auf individuelle Partitionen zu verteilen.

12.4.3. Auswertung von Quota bei der Anmeldung

Feedback

Die im UCS-Managementsystem definierten Einstellungen werden bei der Anmeldung an UCS-Systemen durch das im PAM-Stack aufgerufene Tool `univention-user-quota` ausgewertet und aktiviert.

Wenn keine Quota eingesetzt werden soll, kann die Auswertung durch Setzen der Univention Configuration Registry-Variable `quota/userdefault` auf `no` deaktiviert werden.

Wird die Univention Configuration Registry-Variable `quota/logfile` auf einen beliebigen Dateinamen gesetzt, wird die Aktivierung der Quotas in die angegebene Datei protokolliert.

12.4.4. Abfrage des Quota-Status durch Administratoren oder Benutzer

Feedback

Die für ein System definierten Quota-Begrenzungen können als Benutzer mit dem Befehl `repquota -va` aufgelistet werden, z.B.:

```
*** Report für user Quotas auf Gerät /dev/vdb1
Blockgnadenfrist: 7days; Inodegnadenfrist: 7days
                        Block Limits                Dateilimits
Benutzer        belegt  weich   hart  Gnade   belegt weich hart  Gnade
---------------------------------------------------------------------
root      --       20       0       0              2     0     0
Administrator --       0       0  102400              0     0     0
user01    --  234472 2048000 4096000              2     0     0
user02    --       0 2048000 4096000              0     0     0

Statistik:
Gesamtblockzahl: 8
Datenblöcke: 1
Enträge: 4
Durchschnittlich verwendet: 4,000000
```

Angemeldete Benutzer können mit dem Befehl `quota -v` die für sie geltenden Quota-Grenzen und die aktuelle Auslastung abfragen.

Weitergehende Informationen zu den Befehlen finden sich in den Manpages der Befehle.

Kapitel 13. Druckdienste

13.1. Einführung

Univention Corporate Server beinhaltet ein Drucksystem, mit dem sich auch komplexe Umgebungen realisieren lassen. Drucker und Druckergruppen werden dabei in Univention Management Console verwaltet.

Die Druckdienste basieren auf *CUPS (Common Unix Printing System)*. Druckaufträge werden von CUPS in Warteschlangen verwaltet und in die Druckformate der angeschlossenen Drucker umgewandelt. Die Druckerwarteschlangen werden ebenfalls in Univention Management Console verwaltet, siehe Abschnitt 13.6.

Alle in CUPS eingerichteten Drucker können von UCS-Systemen direkt verwendet werden und werden bei Verwendung von Samba automatisch auch für Windows-Rechner bereitgestellt.

Die technischen Fähigkeiten eines Druckers werden in sogenannten PPD-Dateien spezifiziert. In diesen Dateien ist beispielsweise festgehalten, ob ein Drucker farbig drucken kann, ob ein beidseitiger Druck möglich ist, welche Papierschächte vorhanden sind, welche Auflösungen unterstützt und welche Druckerbefehlssprachen unterstützt werden (z.B. PCL oder PostScript).

Druckaufträge werden von CUPS mit Hilfe von Filtern in ein Format umgewandelt, das der jeweilige Drucker interpretieren kann, also z.B. in PostScript für einen PostScript-fähigen Drucker.

UCS bringt eine Vielzahl von Filtern und PPD-Dateien direkt mit, so dass die meisten Drucker ohne zusätzlich zu installierende Treiber angesprochen werden können. Die Einrichtung weiterer PPD-Dateien ist in Abschnitt 13.9 beschrieben.

Ein Drucker kann entweder direkt an den Druckserver angeschlossen sein (z.B. über die USB-Schnittstelle oder einen Parallelport) oder über Remote-Protokolle mit einem Druckserver kommunizieren (z.B. TCP/IP-fähige Drucker, die über IPP oder LPD angebunden werden).

Netzwerkdrucker mit eigener IP-Adresse sollten als IP-Managed-Client in der UMC-Rechnerverwaltung registriert werden (siehe Abschnitt 3.3).

CUPS bietet die Möglichkeit Druckergruppen zu definieren. Die darin enthaltenen Drucker werden abwechselnd zur Bearbeitung von Druckaufträgen herangezogen, was eine automatische Lastverteilung zwischen räumlich benachbarten Druckern ermöglicht.

Mit dem Druck-Quota-System, das über das Paket ***univention-printquota*** installiert wird, kann eine Erweiterung zur Ermittlung angefallener Druckkosten und zur Limitierung zu druckender Seiten installiert werden. Die Einrichtung und Konfiguration ist in der erweiterten Dokumentation beschrieben [ext-print-doc].

Es können auch Druckerfreigaben von Windows-Systemen in den CUPS-Druckserver integriert werden, dies ist in Abschnitt 13.4 dokumentiert.

13.2. Installation eines Druckservers

Feedback

Ein Druckserver kann mit der Applikation *Druckserver (CUPS)* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-printserver*** installiert und `univention-run-join-scripts` aufgerufen werden. Weitere Informationen finden sich in Abschnitt 5.6.

13.3. Einstellung lokaler Konfigurationseigenschaften eines Druckservers

Feedback

Die Konfiguration von CUPS als Druckserver erfolgt über Einstellungen aus dem LDAP-Verzeichnisdienst und Univention Configuration Registry. Wird die Univention Configuration Registry-Variable `cups/include/local` auf `true` gesetzt, wird zusätzlich die Datei `/etc/cups/cupsd.local.conf` eingebunden, in der beliebige weitere Optionen hinterlegt werden können. Änderungen an dieser Datei benötigen `ucr commit /etc/cups/cupsd.conf` um aktiv zu werden.

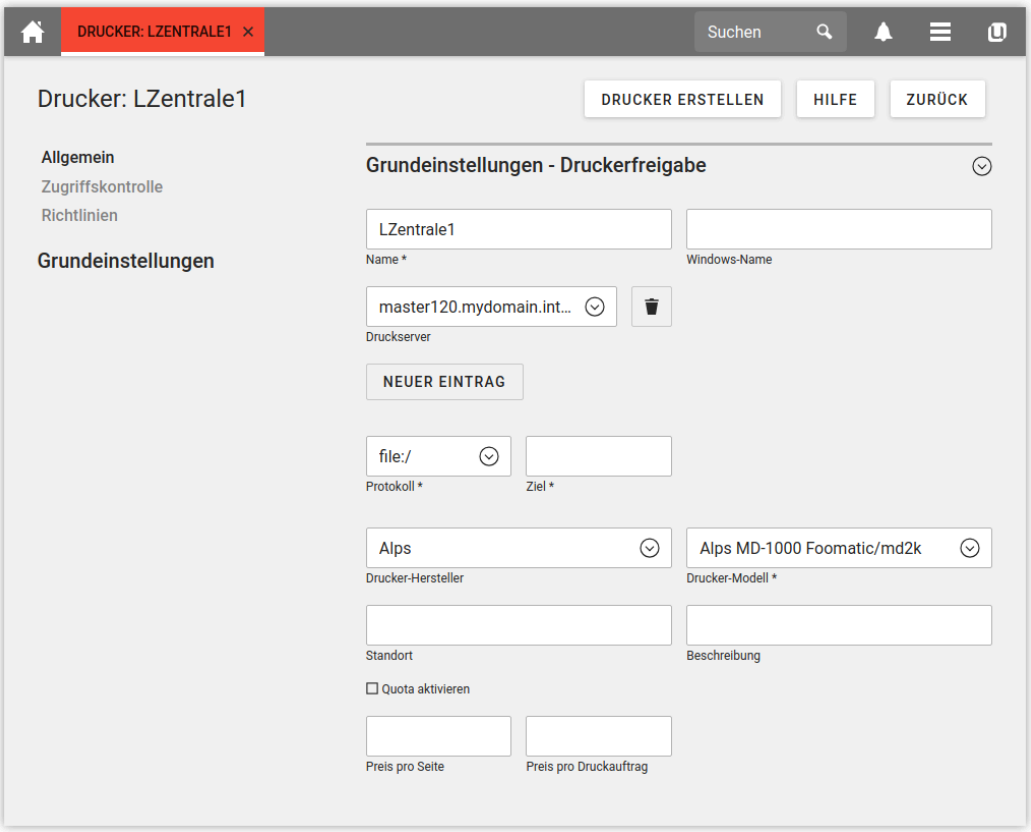
Tritt bei der Verarbeitung einer Drucker-Queue ein Fehler auf (z.B. weil der angebundene Drucker ausgeschaltet ist), wird in der Grundeinstellung die weitere Bearbeitung der Warteschlange gestoppt. Diese muss dann durch den Administrator wieder aktiviert werden (siehe Abschnitt 13.6). Wird die Univention Configuration Registry-Variable `cups/errorpolicy` auf *retry-job* gesetzt, versucht CUPS alle dreißig Sekunden automatisch erfolglose Druckaufträge erneut durchzuführen.

13.4. Konfiguration von Druckerfreigaben

Feedback

Druckerfreigaben werden im UMC-Modul *Drucker* mit dem Objekttyp **Druckerfreigabe: Drucker** verwaltet (siehe auch Abschnitt 4.4).

Abbildung 13.1. Anlegen einer Druckerfreigabe



Beim Hinzufügen, Entfernen oder Bearbeiten einer Druckerfreigabe wird der Drucker automatisch auch in CUPS konfiguriert. CUPS verfügt über keine LDAP-Schnittstelle für die Druckerkonfiguration, stattdessen wird über ein Listener-Modul die CUPS-Druckerkonfiguration (`printers.conf`) generiert. Wenn Samba eingesetzt wird, werden die Druckerfreigaben automatisch auch für Windows-Clients bereitgestellt.

Tabelle 13.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name (*)	Dieses Eingabefeld enthält den Namen der Druckerfreigabe, der von CUPS verwendet wird. Unter diesem Namen erscheint der Drucker unter Linux und Windows. Der Name darf alphanumerische Zeichen (also die Buchstaben a bis z in Groß- und Kleinschreibung und die Ziffern 0 bis 9) sowie Binde- und Unterstriche enthalten. Andere Zeichen (einschließlich Leerzeichen) sind nicht erlaubt.
Druckserver (*)	Ein Druckserver verwaltet die Druckerqueue für den freizugebenden Drucker und wandelt - falls notwendig - die Druckdaten in das passende Druckerformat um. Ist der Drucker nicht bereit, speichert der Druckserver die anstehenden Druckaufträge zwischen und sendet sie später zum Drucker. Werden mehrere Druckserver angegeben, wird der Druckauftrag vom Client zum ersten Druckserver gesendet, der erreichbar ist. Nur Domänencontroller und Memberserver, auf denen das Paket ***univention-printserver*** installiert wurde, werden in der Liste angezeigt.
Protokoll und Ziel (*)	Diese beiden Eingabefelder legen fest, wie der Druckserver auf den Drucker zugreift:

Attribut	**Beschreibung**
	Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die Konfiguration lokal an den Server angeschlossener Drucker: ◦ `parallel://devicedatei` Beispiel: `parallel://dev/lp0` ◦ `socket://server:port` Beispiel: `socket://printer_03:9100` ◦ `usb://devicedatei` Beispiel: `usb://dev/usb/lp0` Die folgende Liste beschreibt die Syntax der einzelnen Protokolle für die Konfiguration von Netzwerk-Druckern: ◦ `http://server[:port]/pfad` Beispiel: `http://192.0.2.10:631/printers/remote` ◦ `ipp://server/printers/queue` Beispiel: `ipp://printer_01/printers/kopierer` ◦ `lpd://server/queue` Beispiel: `lpd://192.0.2.30/bwdraft` Das Protokoll `cups-pdf` wird zur Anbindung eines Pseudo-Druckers verwendet, der aus allen Druckaufträgen ein PDF-Dokument erzeugt. Die Einrichtung ist in Abschnitt 13.7 dokumentiert. Das Protokoll `file://` erwartet als Ziel einen Dateinamen. Der Druckauftrag wird dann nicht auf einen Drucker geschrieben, sondern in diese Datei, was für Testzwecke nützlich sein kann. Die Datei wird mit jedem Druckauftrag neu geschrieben. Mit dem Protokoll `smb://` kann eine Windows-Druckerfreigabe eingebunden werden. Um beispielsweise die Druckerfreigabe *laser01* des Windows-Systems *win01* über Univention Management Console einzubinden, muss als Ziel *win01/laser01* angegeben werden. Dabei sollten Hersteller und Modell-Typ entsprechend des verwendeten Geräts gewählt werden. Der Druckserver nutzt dabei die verwendeten Druckermodell-Einstellungen um die Druckaufträge ggf. umzuwandeln und sendet diese anschließend an die URI `smb://win01/laser01`. Hierbei werden keine Windows-Treiber verwendet. Unabhängig von diesen Einstellungen kann die Druckerfreigabe auch weiterhin von anderen Windows-Systemen mit den entsprechenden Druckertreibern eingebunden werden.
Drucker-Hersteller	Nach der Auswahl des Herstellers des Druckers wird die Auswahlliste *Drucker-Modell* automatisch aktualisiert.

Attribut	Beschreibung
Drucker-Modell (*)	Diese Auswahlliste zeigt alle verfügbaren Drucker-PPD-Dateien für den ausgewählten *Drucker-Hersteller* an. Wenn das gesuchte Drucker-Modell nicht vorhanden ist, kann ein ähnliches Modell ausgewählt werden und mit einem Drucktest die korrekte Funktion überprüft werden. In Abschnitt 13.9 wird erläutert, wie die Liste der Drucker-Modelle erweitert werden kann.
Samba-Name	Für einen Drucker kann ein zusätzlicher Name vergeben werden, unter dem er von Windows aus erreichbar sein soll. Im Gegensatz zum CUPS-Namen (siehe **Name**) darf der Samba-Name Leerzeichen und Umlaute enthalten. Der Drucker steht für Windows dann sowohl unter dem CUPS-Namen als auch unter dem Samba-Namen zur Verfügung. Die Verwendung des Samba-Namens zusätzlich zum CUPS-Namen ist z.B. dann sinnvoll, wenn der Drucker nach einer Migration unter Windows mit einem Namen verwendet wurde, der Leerzeichen oder Umlaute enthielt. Der Drucker kann dann weiterhin unter diesem Namen erreicht werden und die Windows-Rechner müssen nicht umkonfiguriert werden.
Quota aktivieren	Wurden Quota für den Drucker aktiviert, greifen die Quota-Einstellungen der Richtlinie **[Druck-Quota]**. Hierfür muss das Druck-Quota-System installiert sein, siehe [ext-printdoc].
Preis pro Druckauftrag	Dem Benutzer wird für jeden Druckauftrag der in diesem Eingabefeld angegebene Wert berechnet. Die anfallenden Kosten werden im Konto des Benutzers aufsummiert und dienen zur genauen Abrechnung von Druckkosten. Wird kein Wert angegeben, findet keine Druckkostenberechnung statt. Hierfür muss das Druck-Quota-System installiert sein.
Standort	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit einem beliebigen Text gefüllt werden.
Beschreibung	Diese Angabe wird von einigen Anwendungen bei der Druckerauswahl angezeigt. Sie kann mit beliebigem Text gefüllt werden.

Tabelle 13.2. Reiter 'Zugriffskontrolle'

Attribut	Beschreibung
Zugriffslisten	Über diese Auswahl lassen sich Zugriffsrechte für den Drucker festlegen. Der Zugriff kann auf bestimmte Gruppen oder Benutzer beschränkt werden oder er kann generell freigegeben und spezifisch für bestimmte Gruppen oder Benutzer gesperrt werden. Standardmäßig ist der Zugriff für alle Gruppen und Benutzer zugelassen. Diese Rechte werden auch für die entsprechende Samba-Druckerfreigabe übernommen, so dass beim Drucken über Samba die gleichen Zugriffsrechte gelten, wie beim Drucken direkt über CUPS. Die Zugriffskontrolle ist z.B. sinnvoll für die Verwaltung von Druckern an mehreren Standorten, so dass den Benutzern an Standort A nicht die Druckerfreigaben von Standort B angezeigt werden.

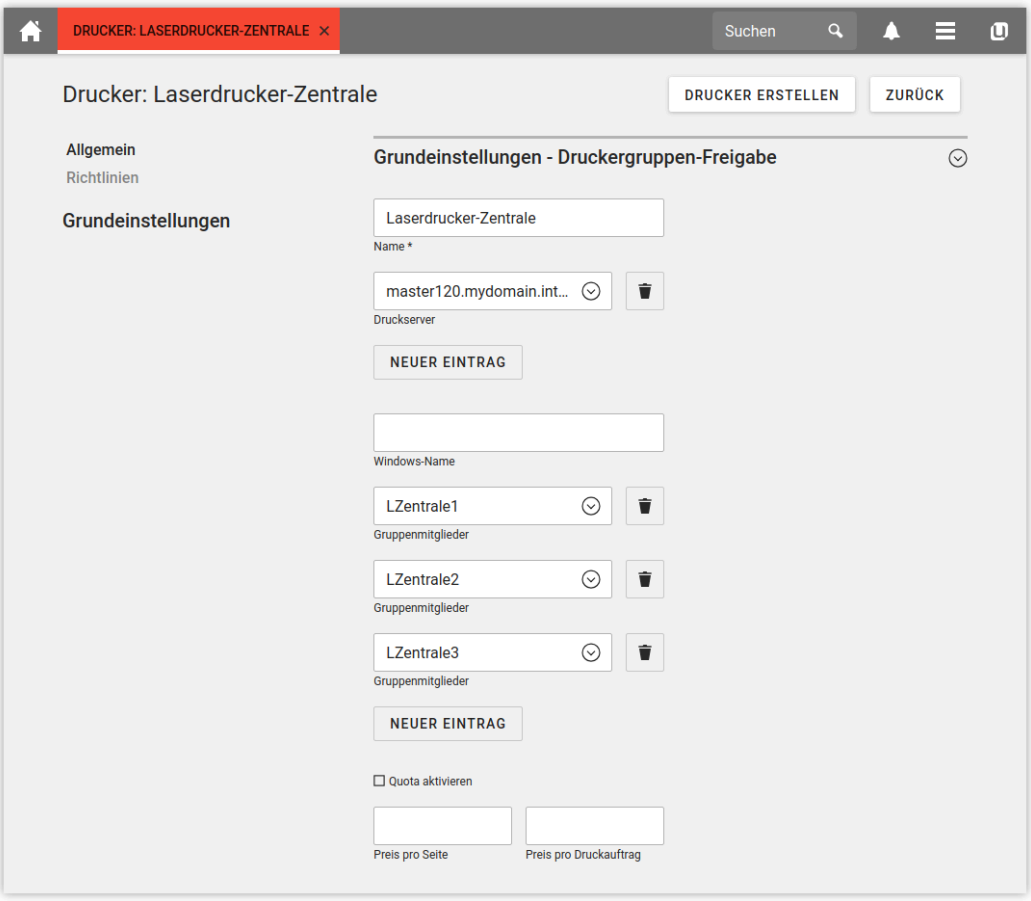
Attribut	Beschreibung
Zugelassene/abgewiesene Benutzer	Diese Auswahl führt einzelne Benutzer auf, für die der Zugriff reguliert werden soll.
Zugelassene/abgewiesene Gruppen	Diese Auswahl führt Gruppen auf, für die der Zugriff reguliert werden soll.

13.5. Konfiguration von Druckergruppen

Feedback

CUPS bietet die Möglichkeit Drucker in Klassen zusammenzufassen. In UCS sind diese als Druckergruppen implementiert. Druckergruppen erscheinen für Clients wie normale Drucker. Eine Druckergruppe erhöht die Verfügbarkeit des Druckdienstes. Wird auf eine Druckergruppe gedruckt, wird der Auftrag an den ersten verfügbaren Drucker der Druckergruppe geschickt. Die Auswahl der Drucker erfolgt nach dem Round-Robin-Prinzip, so dass eine gleichmäßige Auslastung angestrebt wird.

Abbildung 13.2. Konfiguration einer Druckergruppe



Eine Druckergruppe muss mindestens einen Drucker als Mitglied haben. Es können nur Drucker des gleichen Druckservers als Mitglieder der Gruppe gesetzt werden.

Achtung

Die Fähigkeit, Druckerfreigaben von verschiedenen Druckservern in einer Druckergruppe zusammenzufassen, ermöglicht es auch, Druckergruppen als Mitglieder einer Druckergruppe zu setzen.

Eine Druckergruppe könnte sich dadurch selbst als Gruppenmitglied enthalten. Dies ist unbedingt zu vermeiden.

Druckergruppen werden im UMC-Modul *Drucker* mit dem Objekttyp **Druckerfreigabe: Druckergruppe** verwaltet (siehe auch Abschnitt 4.4).

Tabelle 13.3. Karteikarte 'Allgemein'

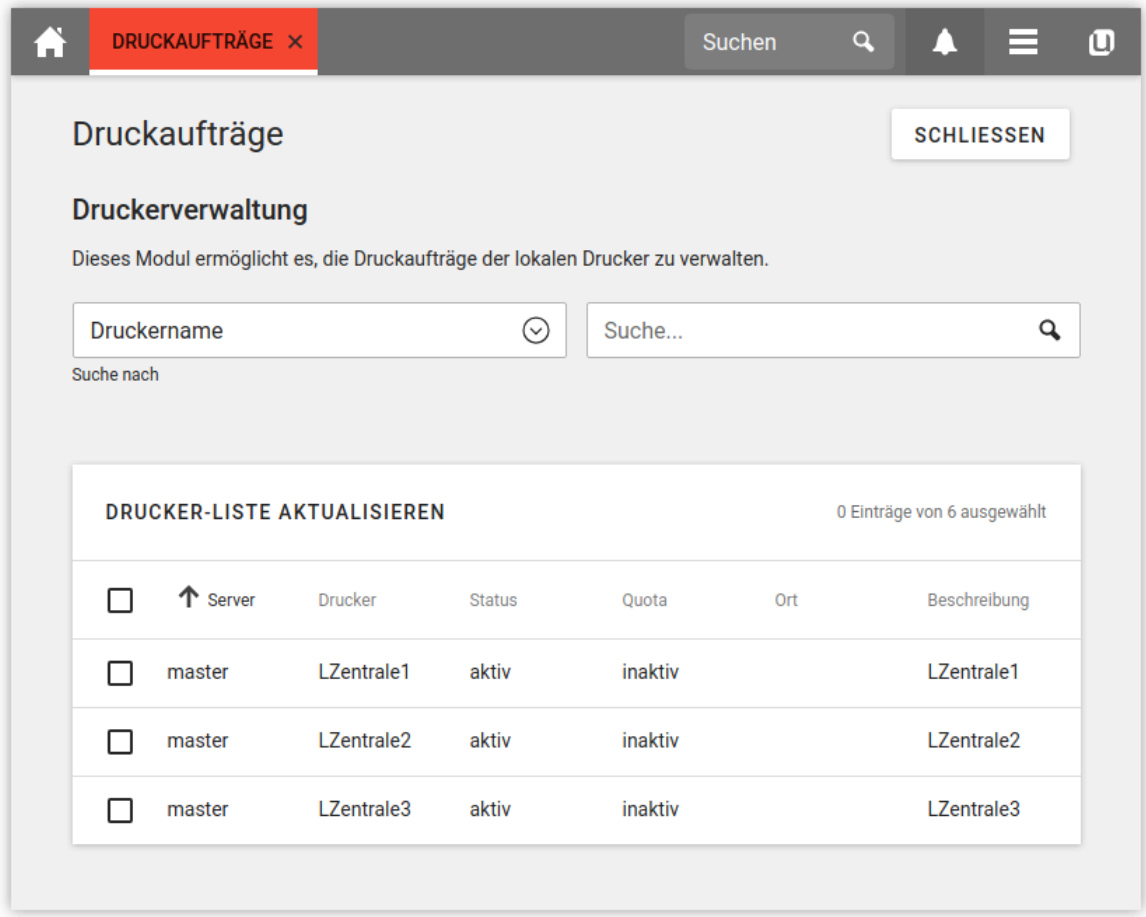
Attribut	**Beschreibung**
Name (*)	Dieses Eingabefeld enthält den Namen der Druckergruppenfreigabe, der von CUPS verwendet wird. Unter diesem Namen erscheint die Druckergruppe unter Linux und Windows. Der Name darf alphanumerische Zeichen (also die Buchstaben a bis z in Groß- und Kleinschreibung und die Ziffern 0 bis 9) sowie Binde- und Unterstriche enthalten. Andere Zeichen (einschließlich Leerzeichen) sind nicht erlaubt.
Druckserver (*)	Drucker, die hier angegebenen Servern zugeordnet sind, können in der darunter angeordneten Auswahl in die Liste der **Gruppenmitglieder** aufgenommen werden.
Samba-Name	Für eine Druckergruppe kann ein zusätzlicher Name vergeben werden, unter dem sie von Windows aus erreichbar sein soll. Im Gegensatz zum CUPS-Namen (siehe *Name*) darf der Samba-Name Leerzeichen und Umlaute enthalten. Der Drucker steht für Windows dann sowohl unter dem CUPS-Namen als auch unter dem Samba-Namen zur Verfügung. Die Verwendung des Samba-Namens zusätzlich zum CUPS-Namen ist z.B. dann sinnvoll, wenn die Druckergruppe schon früher unter Windows mit einem Namen verwendet wurde, der Leerzeichen oder Umlaute enthielt. Die Druckergruppe kann dann weiterhin unter diesem Namen erreicht werden und die Windows-Rechner müssen nicht umkonfiguriert werden.
Gruppenmitglieder	Durch diese Liste werden Drucker der Druckergruppe zugeordnet.
Quota aktivieren	Wurden Quota für die Druckergruppe aktiviert, gelten die Quota-Einstellungen der Richtlinie **[Druck-Quota]**. Hierfür muss das Druck-Quota-System installiert sein, siehe [ext-printdoc].
Preis pro Seite	Dem Benutzer wird für jede gedruckte Seite der in diesem Eingabefeld angegebene Wert berechnet. Die anfallenden Kosten werden im Konto des Benutzers aufsummiert und dienen zur genauen Abrechnung von Druckkosten. Wird kein Wert angegeben, findet keine Druckkostenberechnung statt. Hierfür muss das Druck-Quota-System installiert sein.
Preis pro Druckauftrag	Dem Benutzer wird für jeden Druckauftrag der in diesem Eingabefeld angegebene Wert berechnet. Die anfallenden Kosten werden im Konto des Benutzers aufsummiert und dienen zur genauen Abrechnung von Druckkosten. Wird kein Wert angegeben, findet keine Druckkostenberechnung statt. Hierfür muss das Druck-Quota-System installiert sein.

13.6. Verwaltung von Druckaufträgen und Druckerwarteschlangen

Feedback

Das UMC-Modul **Drucker Administration** erlaubt auf Druckservern den Status der angeschlossenen Drucker zu prüfen, angehaltene Drucker neu zu starten oder Druckaufträge aus den Warteschlagen zu entfernen.

Abbildung 13.3. Drucker-Administration



Auf der Startseite des Moduls befindet sich eine Suchmaske, mit der die vorhandenen Drucker ausgewählt werden können. In der Ergebnisliste wird zu dem jeweiligen Drucker der Server, der Name, der Status, die Druck-Quota-Eigenschaften, der Standort und die Beschreibung angezeigt. Durch Markieren der Drucker und Ausführen einer der beiden Aktionen **deaktivieren** bzw. **aktivieren**, kann der Status mehrerer Drucker gleichzeitig geändert werden.

Die Konfiguration der Druck-Quota-Einstellungen ist in der erweiterten Dokumentation beschrieben [ext-print-doc].

Durch den Klick auf einen Druckernamen können Details zu dem ausgewählten Drucker angezeigt werden. Zu den angezeigten Informationen gehört auch eine Liste der aktuell existierenden Druckaufträge, die noch in der Warteschlange des Druckers sind. Durch Markieren der Druckaufträge und Auswahl der Aktion **[Löschen]** können Druckaufträge aus der Warteschlange entfernt werden.

13.7. Generierung von PDF-Dokumenten aus Druckaufträgen

Feedback

Durch die Installation des Pakets ***univention-printserver-pdf*** wird ein Druckserver um den speziellen Druckertyp **cups-pdf** erweitert, der eingehende Druckaufträge in das PDF-Format umwandelt und für den jeweiligen Benutzer lesbar in ein Verzeichnis auf dem Druckserver ausgibt. Nach der Installation des Pakets sollte `univention-run-join-scripts` aufgerufen werden.

Beim Anlegen eines PDF-Druckers in Univention Management Console (siehe Abschnitt 13.4) muss als Protokoll **cups-pdf:/** ausgewählt werden, das Ziel-Feld bleibt leer.

Als **Drucker-Hersteller** muss *PDF* und als **Drucker-Modell Generic CUPS-PDF Printer** ausgewählt werden.

Das Zielverzeichnis für die generierten PDF-Dokumente wird über die Univention Configuration Registry-Variable `cups/cups-pdf/directory` festgelegt. Standardmäßig wird es auf `/var/spool/cups-pdf/%U` gesetzt, so dass cups-pdf für jeden Benutzer ein eigenes Verzeichnis verwendet.

Anonym eingegangene Druckaufträge werden in das durch die Univention Configuration Registry-Variable `cups/cups-pdf/anonymous` vorgegebene Verzeichnis ausgegeben (Standardeinstellung: `/var/spool/cups-pdf/`).

In der Grundeinstellung werden die generierten PDF-Dokumente unbegrenzt aufbewahrt. Wird die Univention Configuration Registry-Variable `cups/cups-pdf/cleanup/enabled` auf `true` gesetzt werden alte PDF-Druckaufträge über einen Cron-Job gelöscht. Die Aufbewahrungszeit in Tagen kann mit der Univention Configuration Registry-Variable `cups/cups-pdf/cleanup/keep` konfiguriert werden.

13.8. Einbinden von Druckerfreigaben auf Windows-Clients

Feedback

Die in Univention Management Console eingerichteten Druckerfreigaben können auf Windows-Systemen als Netzwerkdrucker hinzugefügt werden. Dies erfolgt über die Systemsteuerung unter **Drucker -> Netzwerkdrucker hinzufügen**. Die Druckertreiber müssen beim ersten Zugriff eingerichtet werden. Wurden die Treiber serverseitig hinterlegt (siehe unten), erfolgt die Zuweisung des Treibers automatisch.

Druckerfreigaben werden in der Regel mit den mitgelieferten Windows-Druckertreibern betrieben. Der Netzwerkdrucker kann auf Windows-Seite alternativ mit einem Standard-PostScript-Druckertreiber eingerichtet werden. Wenn auf einen Farbdrucker zugegriffen werden soll, sollte auf Windows-Seite ein Treiber für einen PostScript-fähigen Farbdrucker verwendet werden, z.B. *HP Color LaserJet 8550*.

Achtung

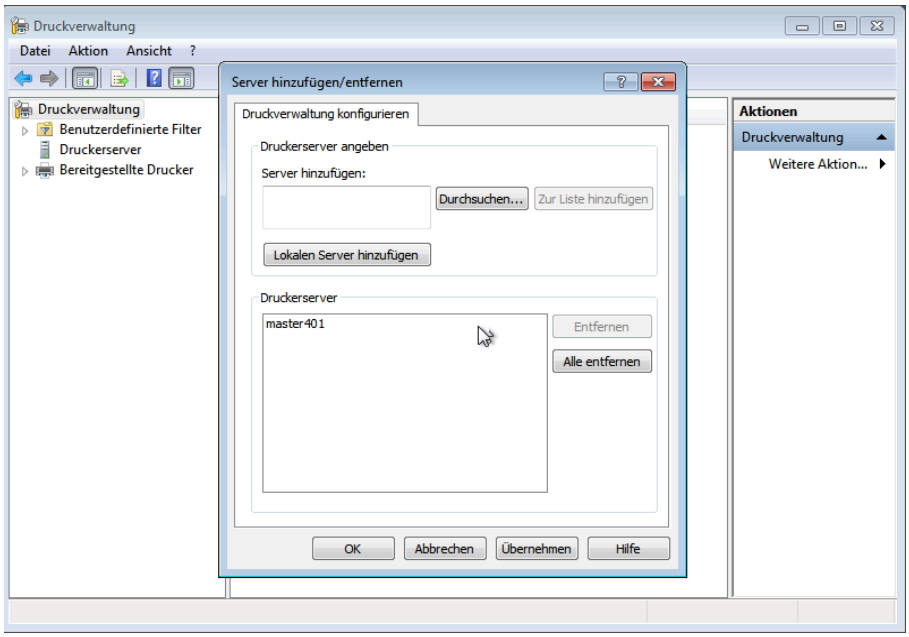
Der Zugriff auf einen Drucker ist für einen regulären Benutzer nur möglich, wenn dieser über lokale Rechte zur Treiberinstallation verfügt oder ein entsprechender Druckertreiber auf dem Druckserver hinterlegt wurde. Ist dies nicht der Fall kann es zu einer Windows Fehlermeldung kommen, die besagt, dass die Berechtigungen nicht ausreichen, um eine Verbindung mit dem Drucker herzustellen.

Windows unterstützt ein Verfahren zur serverseitigen Bereitstellung von Druckertreibern auf dem Druckserver (*Point 'n' Print*). Die folgende Anleitung beschreibt die Bereitstellung der Druckertreiber unter Windows 7 bzw. Windows 8 für eine in der UMC konfigurierte Druckerfreigabe. Zuerst müssen die Druckertreiber auf dem Druckserver hinterlegt werden, danach werden die Drucker mit einem Druckertreiber verknüpft. Die Benutzerführung unter Windows bietet zahlreiche Stolperfallen, es ist wichtig den einzelnen Schritten exakt zu folgen!

1. Zuerst müssen die Druckertreiber von der Webseite des Herstellers heruntergeladen werden. Wird eine Umgebung verwendet, in der die 64 Bit-Versionen von Windows eingesetzt werden, müssen die Treiber unbedingt in beiden Versionen bezogen werden (32 und 64 Bit). Benötigt werden die `INF`-Dateien.

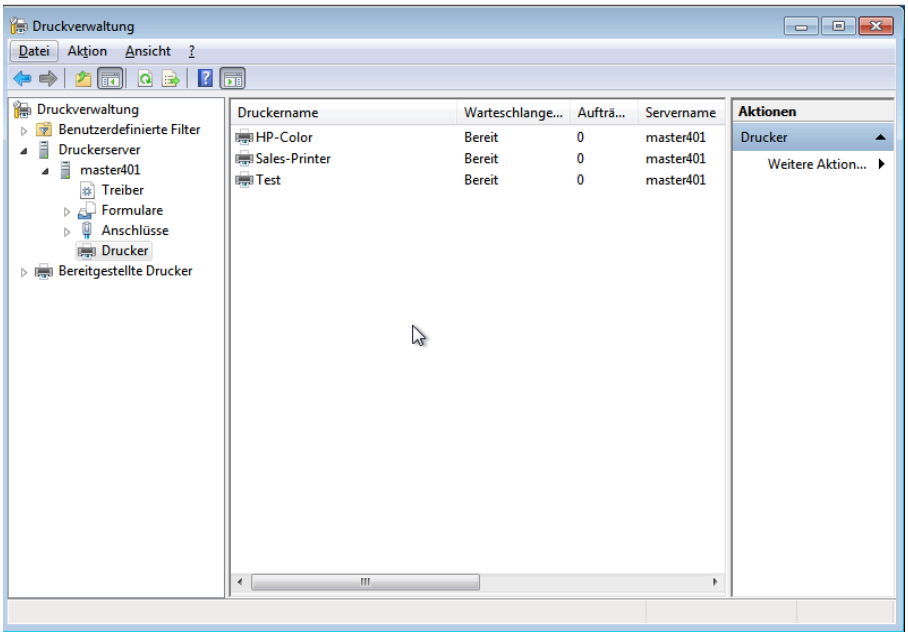
2. Nun muss das Programm **printmanagement.msc** (Druckerverwaltung) gestartet werden. Im Menüpunkt **Aktion** kann mit einem Klick auf **Server hinzufügen/entfernen** ein weiterer Server hinzugefügt werden. In dem Eingabefeld **Server hinzufügen** muss der Name des Druckerservers eingetragen werden.

Abbildung 13.4. Druckerserver hinzufügen



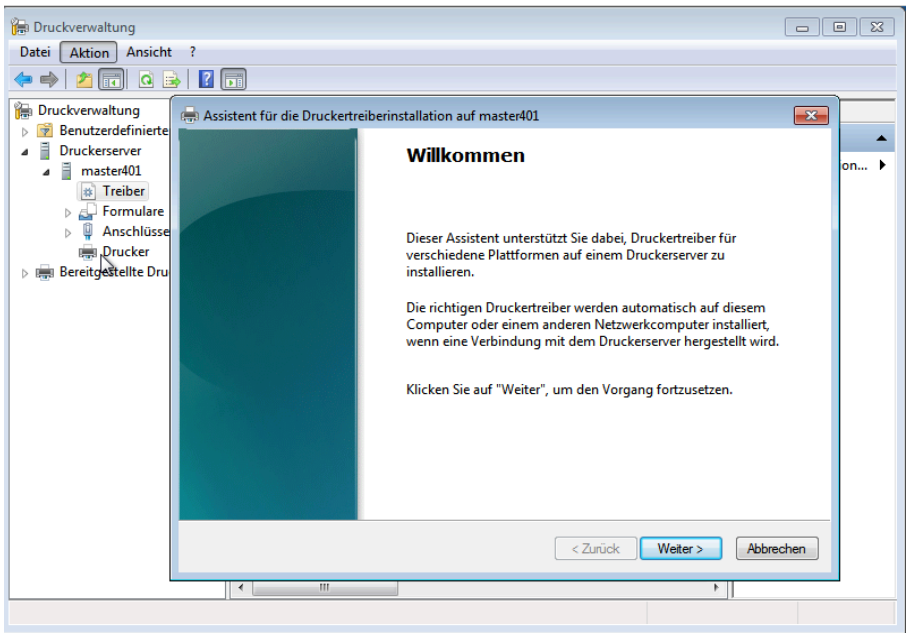
3. In der Druckerverwaltung sollte der neu hinzugefügte Druckserver nun aufgelistet werden. Durch einen Klick auf **Drucker** werden die aktuell auf dem Druckerserver eingerichteten Druckerfreigaben angezeigt.

Abbildung 13.5. Druckerliste



4. Mit einem Klick auf den Eintrag **Treiber** werden die hinterlegten Druckertreiber aufgelistet. Im Menüpunkt **Aktion** kann mit einem Klick auf **Treiber hinzufügen** der Dialog für die Treiberinstallation gestartet werden. Wir empfehlen die Druckertreiber direkt vom Hersteller herunterzuladen und diese während der Treiberinstallation auszuwählen. Wird eine Umgebung verwendet, in der die 64 Bit-Versionen von Windows eingesetzt werden, sollte zunächst geprüft werden, ob auf dem UCS Samba System die Univention Configuration Registry-Variable `samba/spoolss/architecture` auf `Windows x64` gesetzt ist. Falls das nicht der Fall ist, müssen die Treiber unbedingt für 32 und 64 Bit hochgeladen werden, andernfalls kann auf die 32 Bit Treiber verzichtet werden, wenn ausschliesslich 64 Bit Windows Systeme in der Domäne zum Einsatz kommen. Die Treiber können für verschiedene Windows-Architekturen entweder in getrennten Schritten nacheinander oder direkt in einem Vorgang hochgeladen werden. Falls beide Treiberarchitekturen gleichzeitig zum Hochladen ausgewählt werden, dann muss im anschließenden Dateiauswahldialog als erstes der 64 Bit Treiber gewählt werden. Nachdem Windows diese Dateien zum Server hochgeladen hat, fragt es dann erneut nach dem Ort für die 32 Bit Treiber. Danach werden auch diese zum Server hochgeladen.

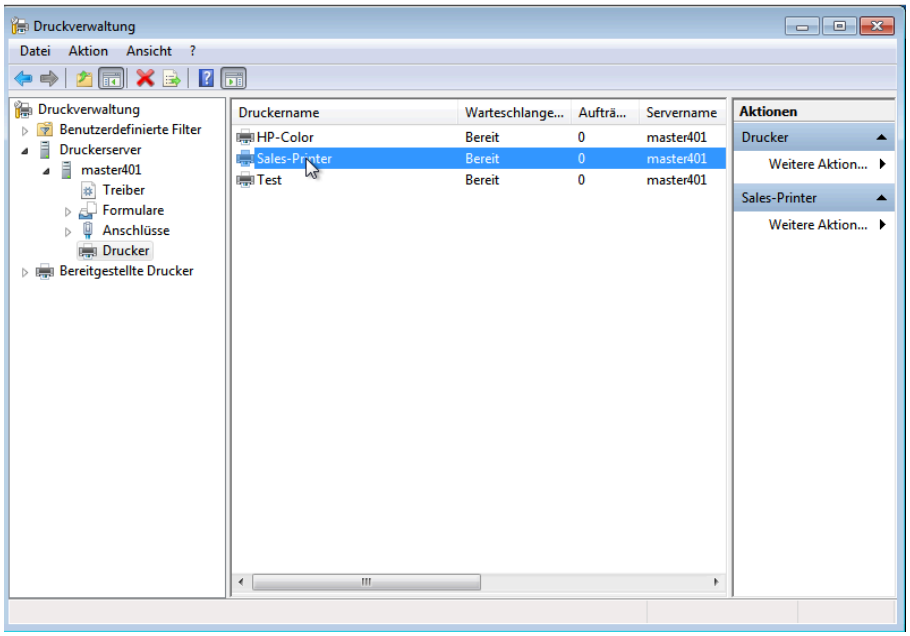
Abbildung 13.6. Treiberinstallation



5. Nach diesen Schritten sind die Treiber auf dem UCS Druckserver im Verzeichnis `/var/lib/samba/drivers/` gespeichert.

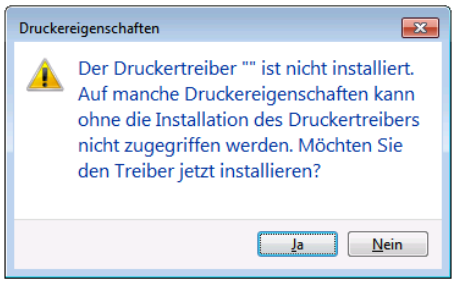
6. Nun muss die Druckerfreigabe noch mit dem hochgeladenen Druckertreiber verknüpft werden. Dazu wird im Programm **printmanagement.msc** die Liste der vom Druckserver bereitgestellten Drucker aufgerufen. Dort werden durch einen Doppelklick auf den **Drucker** die Eigenschaften aufgelistet.

Abbildung 13.7. Drucker auswählen



7. Ist noch kein Druckertreiber hinterlegt, wird eine Meldung angezeigt, dass noch kein Druckertreiber installiert ist. Die Frage, ob der Treiber installiert werden soll, muss hier mit **Nein** bestätigt werden.

Abbildung 13.8. Fehlermeldung beim ersten Zugriff



8. Nun muss im Reiter **Erweitert** unter **Treiber** der hochgeladene Treiber aus dem Dropdown-Menü ausgewählt werden. Anschließend muss auf **Übernehmen** geklickt werden (Wichtig: Nicht auf **OK**!).

9. Falls der betreffende Druckertreiber das erste mal einem Drucker zugewiesen wird, dann wird ein Dialog angezeigt, in dem gefragt wird, ob dem Drucker vertraut wird. Dies muss mit **Treiber installieren** bestätigt werden. Nun werden die serverseitig hinterlegten Druckertreiber auf den Client heruntergeladen. Falls der betreffende Druckertreiber schon zuvor einmal auf diese Weise vom Druckerserver auf das betreffende Windows System heruntergeladen worden ist, dann meldet Windows an dieser Stelle eine Fehlermeldung `0x0000007a`. Diese kann ignoriert werden.

10. Wichtig: Nun sollte nicht direkt auf **OK** geklickt werden, sondern es muss noch einmal auf den Reiter **Allgemein** gewechselt werden. Auf dem Reiter muss weiterhin der alte Name der Druckerfreigabe angezeigt werden. In UCS Releases vor UCS 4.0-1 kann es vorkommen, dass das Windows System hier den Namen der Druckerfreigabe in den Namen des Druckertreibers geändert hat. Wenn man dies so übernehmen würde, dann wäre der Drucker nicht mehr mit der Freigabe assoziiert! Wenn dieser Fall eingetreten ist, muss der Name des Druckers auf dem Reiter **Allgemein** (das erste Eingabefeld, neben dem stilisierten Druckersymbol) wieder auf den Namen der Druckerfreigabe geändert werden. Hier ist das in der Druckerverwaltung der UMC konfigurierte Feld **Samba-Name** zu verwenden (oder falls dies leer gelassen wurde, dann der Wert aus **Name**). Wenn der Name auf diese Weise zurückgesetzt werden musste, dann fragt Windows beim abschließenden Klick auf **OK** nach, ob man sich sicher ist, dass man den Namen ändern möchte. Dies ist zu bestätigen.

11. Um dem Windows Druckertreiber nun die Möglichkeit zu geben, korrekte Standard-Einstellungen für den Drucker zu speichern, sollte nun auf den Reiter **Geräteeinstellungen** gewechselt werden. Der Name dieses Reiters ist herstellerspezifisch und kann auch mit **Einstellungen** oder einfach **Konfiguration** bezeichnet sein. Ein abschließender Klick auf **OK** schließt den Dialog. Danach kann direkt eine Testseite gedruckt werden. Sollte Windows hier eine Fehlermeldung `0x00000006` ausgeben, muss in den Druckereinstellungen erneut geprüft werden, ob sich ein herstellerspezifischer Reiter namens **Geräteeinstellungen** (oder ähnlich) findet. Dieser sollte geöffnet und dann einfach mit **OK** bestätigt werden. Dies schließt den Dialog und speichert Druckertreibereinstellungen (*PrinterDriverData*) in der Samba Registry.

12. Es ist sinnvoll zu diesem Zeitpunkt auch direkt die Papiergröße und ähnliche Einstellungen vorzunehmen, damit diese an der Druckerfreigabe gespeichert werden. Andere Windows Systeme, die später auf die Druckerfreigabe zugreifen finden dann automatisch die korrekten Einstellungen. Diese Einstellungen lassen sich in den meisten Fällen dadurch öffnen, indem in den Druckereigenschaften auf dem Reiter **Erweitert** auf die Schaltfläche **Standardwerte...** geklickt wird. Der sich öffnende Dialog ist ebenfalls herstellerabhängig. Typischerweise findet sich die Einstellung für Papiergröße und Orientierung auf einem Reiter **Seite Einrichten** oder auch **Papier/Qualität**. Nach Bestätigung des Dialogs durch Klick auf **OK** speichert der Druckertreiber diese Einstellungen (als `Default DevMode`) für den Drucker in der Samba Registry.

13.9. Integration weiterer PPD-Dateien

Feedback

Die technischen Fähigkeiten eines Druckers werden in sogenannten PPD-Dateien spezifiziert. In diesen Dateien ist beispielsweise festgehalten, ob ein Drucker farbig drucken kann, ob ein beidseitiger Druck möglich ist, welche Papierschächte vorhanden sind, welche Auflösungen unterstützt und welche Druckerbefehlssprachen unterstützt werden (z.B. PCL oder PostScript).

Neben den bereits im Standardumfang enthaltenen PPD-Dateien können weitere über Univention Management Console hinzugefügt werden. Die PPD wird in der Regel vom Hersteller des Druckers bereitgestellt und muss auf den Druckservern in das Verzeichnis `/usr/share/ppd/` kopiert werden.

Die Druckertreiberlisten werden im UMC-Modul **LDAP-Verzeichnis** verwaltet. Dort muss in den Container `univention` und dort in den Untercontainer `cups` gewechselt werden. Für die meisten Druckerhersteller existieren bereits Druckertreiberlisten. Diese können ergänzt werden oder eine neue hinzugefügt werden.

Tabelle 13.4. Karteikarte 'Allgemein'

Attribut	Beschreibung
Name (*)	Der Name der Druckertreiberliste. Unter diesem Namen erscheint die Liste in der Auswahlliste **Drucker-Hersteller** auf der Karteikarte **Allgemein** der Druckerfreigaben (siehe Abschnitt 13.4).
Treiber	Der Pfad zur PPD-Datei, relativ zu dem Verzeichnis `/usr/share/ppd/`. Soll beispielweise die Datei `/usr/share/ppd/laserjet.ppd` verwendet werden, so ist hier `laserjet.ppd` einzutragen. Es können auch `gzip`-komprimierte Dateien (Dateiendung `.gz`) angegeben werden.
Beschreibung	Eine Beschreibung des Druckertreibers, unter der er in der Auswahlliste **Drucker-Modell** auf der Karteikarte **Allgemein** der Druckerfreigaben erscheint.

Kapitel 14. Maildienste

14.1. Einführung

Feedback

Univention Corporate Server stellt Maildienste bereit, auf die Benutzer sowohl über Standard-Mail-Clients wie Thunderbird, als auch über das Webmail-Interface Horde zugreifen können.

Für den Mailempfang und -versand wird Postfix verwendet. In der Grundinstallation wird auf jedem UCS-System eine für die lokale Mailzustellung ausgelegte Konfiguration eingerichtet. Postfix nimmt in dieser Konfiguration E-Mails nur vom lokalen System entgegen, und auch die Zustellung erfolgt nur für lokale Systembenutzer.

Durch die Installation der Mailserver-Komponente wird ein vollständiger Mailtransport über SMTP umgesetzt (siehe Abschnitt 14.2). Postfix wird bei der Installation der Komponente umkonfiguriert, so dass bei eingehenden E-Mails eine Gültigkeitsüberprüfung in Form einer Suche im LDAP-Verzeichnis durchgeführt wird. Das bedeutet, dass E-Mails nur für im LDAP-Verzeichnis eingetragene oder über einen Alias definierte E-Mail-Adressen akzeptiert werden.

Mit der Mailserver-Komponente wird ebenfalls der IMAP-Dienst Dovecot auf dem System installiert. Dieser stellt E-Mailkonten für die Benutzer der Domäne bereit und bietet entsprechende Schnittstellen für den

Zugriff durch E-Mail-Clients an. Dovecot ist für den Abruf von E-Mails über IMAP und POP3 vorkonfiguriert. Der Zugriff über POP3 kann durch Setzen der Univention Configuration Registry-Variable `mail/dovecot/pop` auf `no` deaktiviert werden. Das gleiche gilt für IMAP und die Univention Configuration Registry-Variable `mail/dovecot/imap`. Auch die weitere Konfiguration der Mailserver erfolgt über Univention Configuration Registry (siehe Abschnitt 14.8).

Anmerkung

Seit Univention Corporate Server Version 4.0-2 wird standardmäßig Dovecot als IMAP- und POP3-Server verwendet. Die Integration von Cyrus ist seit Univention Corporate Server Version 4.3-0 nicht mehr verfügbar.

Die Verwaltung der Benutzerdaten des Mailservers (z.B. E-Mail-Adressen oder Verteiler) erfolgt über Univention Management Console und ist in Abschnitt 14.3 dokumentiert. Benutzerdaten werden in LDAP gespeichert. Die Authentifizierung wird anhand der primären E-Mail-Adresse eines Benutzers durchgeführt, d.h. sie muss als Benutzername in Mail-Clients eingetragen werden. Sobald einem Benutzer im LDAP-Verzeichnis eine primäre E-Mail-Adresse zugeordnet wird, legt ein Listener-Modul ein IMAP-Postfach auf dem Mail Home Server an. Durch die Angabe eines Mail Home Servers können E-Mail-Konten der Benutzer auch auf mehrere Mailserver verteilt werden (siehe Abschnitt 14.8.10).

Optional können durch Postfix empfangene E-Mails vor der weiteren Verarbeitung durch Dovecot auf Spam-Inhalte und Viren hin untersucht werden. Spam-Mails werden über die Klassifizierungssoftware SpamAssassin erkannt (Abschnitt 14.4), für die Erkennung von Viren und anderer Malware wird ClamAV eingesetzt (Abschnitt 14.5).

In der Voreinstellung werden E-Mails an fremde Domänen direkt dem zuständigen SMTP-Server der Domäne zugestellt. Die Ermittlung erfolgt dabei durch die Auflösung des MX-Records im DNS. Der Mailversand kann auch von einem Relay-Host z.B. beim Internet-Provider übernommen werden (siehe Abschnitt 14.8.1).

Für den webbasierten Zugriff auf E-Mails steht das Horde-Framework zur Verfügung (siehe Abschnitt 14.10). Das UCS-Mailsystem bietet keine Groupware-Funktionalität wie gemeinsam genutzte Kalender oder Termineinladungen. Es existieren aber auf UCS basierende Groupwaresysteme, die sich in das UCS-Managementsystem integrieren, bspw. Kolab, Zarafa oder Open-Xchange. Weiterführende Informationen finden sich im Univention App Center (siehe Abschnitt 5.3).

14.2. Installation

Feedback

Ein Mailserver kann mit der Applikation *Mailserver* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-mail-server*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6. Mailserver können auf allen Server-Systemrollen installiert werden. Die Verwendung eines Domänencontrollers wird wg. häufiger LDAP-Zugriffe empfohlen.

Die Laufzeitdaten des Dovecot-Servers werden im Verzeichnis `/var/spool/dovecot/` abgelegt. Falls dieses Verzeichnis auf einem NFS-Laufwerk liegen sollte, lesen Sie bitte Abschnitt 14.8.11.

Das Webmail-Interface Horde kann über das Univention App Center installiert werden (siehe Abschnitt 5.3).

14.3. Verwaltung der Mailserver-Daten

Feedback

14.3.1. Verwaltung von Mail-Domänen

Feedback

Eine Mail-Domäne ist ein gemeinsamer Namensraum für E-Mail-Adressen, Mailinglisten und IMAP-Gruppen-Ordner. Postfix unterscheidet bei der Zustellung von E-Mails zwischen lokalen und externen Domänen. Nur für E-Mail-Adressen lokaler Domänen wird die Mailzustellung vorgenommen. Der Name einer Mail-Domäne darf nur aus Kleinbuchstaben, den Ziffern 0-9, Punkten und Bindestrichen bestehen.

Mit UCS lassen sich mehrere Mail-Domänen verwalten. Die verwalteten Mail-Domänen müssen dabei nicht der DNS-Domäne des Servers entsprechen, sondern sind frei wählbar. Die auf einem Mailserver registrierten Mail-Domänen werden automatisch in der Univention Configuration Registry-Variable `mail/hosteddomains` gespeichert.

Damit auch externe Absender E-Mails an die Mitglieder der Domäne versenden können, müssen in der Konfiguration der autoritativen DNS-Nameserver MX-Records angelegt werden, die den UCS-Server als Mailserver für die Domäne ausweisen. Diese DNS-Anpassungen werden üblicherweise von Internet-Providern vorgenommen.

Mail-Domänen werden im UMC-Modul *E-Mail* mit dem Objekttyp **Mail-Domäne** verwaltet.

14.3.2. Zuordnung von E-Mail-Adressen zu Benutzern

Einem Benutzer können drei verschiedene Arten von E-Mail-Adressen zugeordnet werden:

- Die *primäre E-Mail-Adresse* wird zur Authentifizierung an Postfix und Dovecot verwendet. Primäre E-Mail-Adressen müssen eindeutig sein. Pro Benutzer kann nur eine primäre E-Mail-Adresse konfiguriert werden. Sie definiert auch das IMAP-Postfach des Benutzers. Wenn dem Benutzer ein Mail Home Server zugeordnet ist (siehe Abschnitt 14.8.10), wird das IMAP-Postfach automatisch durch ein Univention Directory Listener-Modul erstellt. Der Domänenanteil der E-Mail-Adresse muss in Univention Management Console registriert sein (siehe Abschnitt 14.3.1).

- E-Mails an *alternative E-Mail-Adressen* werden ebenfalls in das Postfach des Benutzers zugestellt. Es können beliebig viele Adressen angegeben werden. Die alternativen E-Mail-Adressen müssen nicht eindeutig sein; besitzen zwei Benutzer die gleiche Adresse, erhalten beide Benutzer alle E-Mails, die an diese Adresse gesandt werden. Der Domänenanteil der E-Mail-Adresse muss in Univention Management Console registriert sein (siehe Abschnitt 14.3.1). Um E-Mails an alternative E-Mail-Adressen zu erhalten, muss ein Benutzer eine primäre E-Mail-Adresse besitzen.

- Wenn *Weiterleitungs-E-Mail-Adressen* für einen Benutzer konfiguriert sind, werden E-Mails, die er über die primäre oder über alternative E-Mail-Adressen empfängt, an diese weiter geleitet. Optional kann eine Kopie der eingehenden Nachrichten in das Postfach des Benutzers zugestellt werden. Es können beliebig viele Adressen angegeben werden. Weiterleitungs-E-Mail-Adressen müssen weder eindeutig, noch muss ihr Domänenanteil in Univention Management Console registriert sein.

Anmerkung

E-Mail-Adressen können die Zeichen a-z, die Ziffern 0-9, Punkte, Bindestriche und Unterstriche enthalten. Als weitere Vorgabe müssen die E-Mail-Adressen mit einem Buchstaben beginnen und ein @-Zeichen enthalten. Um E-Mail-Adressen vergeben zu können, muss vorher mindestens eine Mail-Domäne registriert werden (siehe Abschnitt 14.3.1).

E-Mail-Adressen werden im UMC-Modul *Benutzer* verwaltet. Die **primäre E-Mail-Adresse** wird im Reiter **Allgemein** im Untermenü **Benutzer-Konto** eingetragen. **Alternative E-Mail-Adressen** können unter **Erweiterte Einstellungen -> Mail** eingetragen werden.

Anmerkung

Sobald das Benutzerkonto konfiguriert ist, kann eine Anmeldung am UCS-Mail-Stack (`IMAP`/`POP3`/`SMTP`) erfolgen. Wurde das Benutzerkonto deaktiviert (oder das Passwort geändert), ist eine Anmeldung am Mail-Stack für eine Dauer von 5min weiterhin möglich. Der Grund hierfür ist der Authentifizierungscache des Mail-Stacks. Um den Cache zu invalidieren, führen Sie

```
doveadm auth cache flush
```

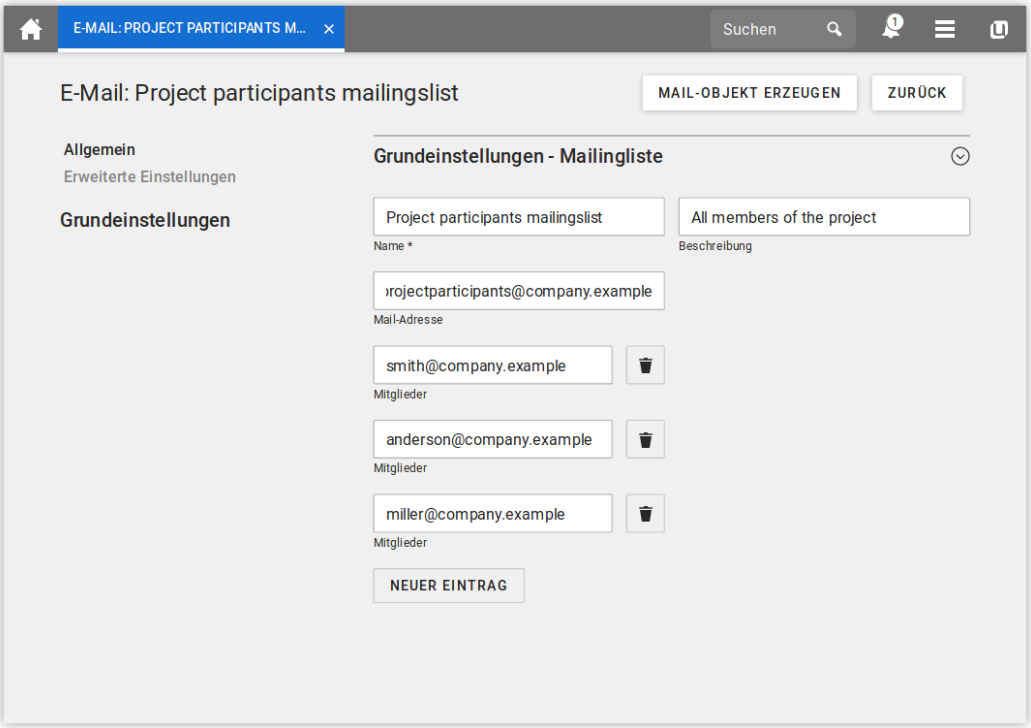
auf dem Mailserver aus. Die Ablaufzeit des Caches kann auf dem Mailserver mit der Univention Configuration Registry-Variable `mail/dovecot/auth/cache_ttl` sowie `mail/dovecot/auth/cache_negative_ttl` konfiguriert werden.

14.3.3. Verwaltung von Mailinglisten

Feedback

Mailinglisten werden zum Austausch von E-Mails in geschlossenen Gruppen verwendet. Jede Mailingliste verfügt über eine eigene E-Mail-Adresse. Wird an diese Adresse eine E-Mail gesendet, empfangen sie alle Mitglieder der Mailingliste.

Abbildung 14.1. Einrichtung einer Mailingliste



Mail-Domänen werden im UMC-Modul *E-Mail* mit dem Objekttyp **Mailingliste** verwaltet. Unter **Name** ist ein frei wählbarer Name der Mailingliste anzugeben, die Angabe einer **Beschreibung** ist optional. Als **Mail-Adresse** ist die E-Mail-Adresse der Mailingliste einzugeben. Der Domänenteil der Adresse muss dabei einer der verwalteten Mail-Domänen entsprechen. Unter **Mitglieder** können beliebig viele Adressen aufgenommen werden, im Gegensatz zu Mailgruppen (siehe Abschnitt 14.3.4) können hier auch externe E-Mail-Adressen aufgenommen werden. Nach dem Anlegen einer Mailingliste ist diese umgehend verfügbar.

In der Grundeinstellung kann jeder an die Mailingliste schreiben. Um Missbrauch zu verhindern, besteht die Möglichkeit den Senderkreis einzuschränken. Dazu muss die Univention Configuration Registry-Variable `mail/postfix/policy/listfilter` auf dem Mailserver auf `yes` gesetzt und Postfix neu gestartet werden. Unter **Erweiterte Einstellungen** können dann **Benutzer, die berechtigt sind, E-Mails an diese Liste zu versenden** und **Gruppen, die berechtigt sind, E-Mails an diese Liste zu versenden** festgelegt werden. Ist hier ein Feld gesetzt, ist das Senden nur den berechtigten Nutzern/Gruppen erlaubt.

14.3.4. Verwaltung von Mailgruppen

Feedback

Es besteht die Möglichkeit eine Mailgruppe zu bilden: Dabei wird einer Benutzer-Gruppe eine E-Mail-Adresse zugewiesen. E-Mails an diese Adresse werden dann allen Gruppenmitgliedern an ihre primäre E-Mail-Adresse zugestellt.

Mailgruppen werden im UMC-Modul *Gruppen* verwaltet (siehe auch Kapitel 7).

Die E-Mail-Adresse der Mailgruppe wird im Eingabefeld **Mail-Adresse** unter **Erweiterte Einstellungen** festgelegt. Der Domänenteil der Adresse muss einer der verwalteten Mail-Domänen entsprechen.

In der Grundeinstellung kann jeder an die Mailgruppe schreiben. Um Missbrauch zu verhindern, besteht die Möglichkeit den Senderkreis einzuschränken. Dazu muss die Univention Configuration Registry-Variable `mail/postfix/policy/listfilter` auf dem Mailserver auf `yes` gesetzt und Postfix neu gestartet werden.

Unter **Erweiterte Einstellungen** können **Benutzer, die berechtigt sind, E-Mails an diese Gruppe zu versenden** und **Gruppen, die berechtigt sind, E-Mails an diese Gruppe zu versenden** festgelegt werden. Ist hier ein Feld gesetzt, ist das Senden nur den berechtigten Nutzern/Gruppen erlaubt.

14.3.5. Verwaltung von globalen IMAP-Ordnern

Ein gemeinsamer Zugriff auf E-Mails ist in vielen Arbeitsgruppen die Grundlage der Zusammenarbeit. Mit UCS können Benutzer sehr einfach Ordner in Ihren eigenen Postfächern anlegen und Berechtigungen vergeben, so dass es weiteren Benutzern gestattet ist, E-Mails in diesen Ordnern zu lesen oder weitere E-Mails in diesen Ordnern abzulegen.

Alternativ können eigene IMAP-Ordner für Benutzer oder Benutzergruppen freigegeben werden. Ein solcher Ordner wird als globaler IMAP-Ordner bezeichnet. Globale IMAP-Ordner werden im UMC-Modul *Mail* mit dem Objekttyp **Mail-Ordner (IMAP)** verwaltet.

Globale IMAP-Ordner können nicht umbenannt werden. Die Univention Configuration Registry-Variable `mail/dovecot/mailbox/rename` kommt daher nicht zur Anwendung. Nur wenn `mail/dovecot/mailbox/delete` auf `yes` gesetzt ist (Standard ist `no`), wird ein globaler IMAP-Ordner beim Löschen im UMC-Modul *Mail* auch tatsächlich von der Festplatte gelöscht.

Abbildung 14.2. Einrichtung eines globalen IMAP-Ordners

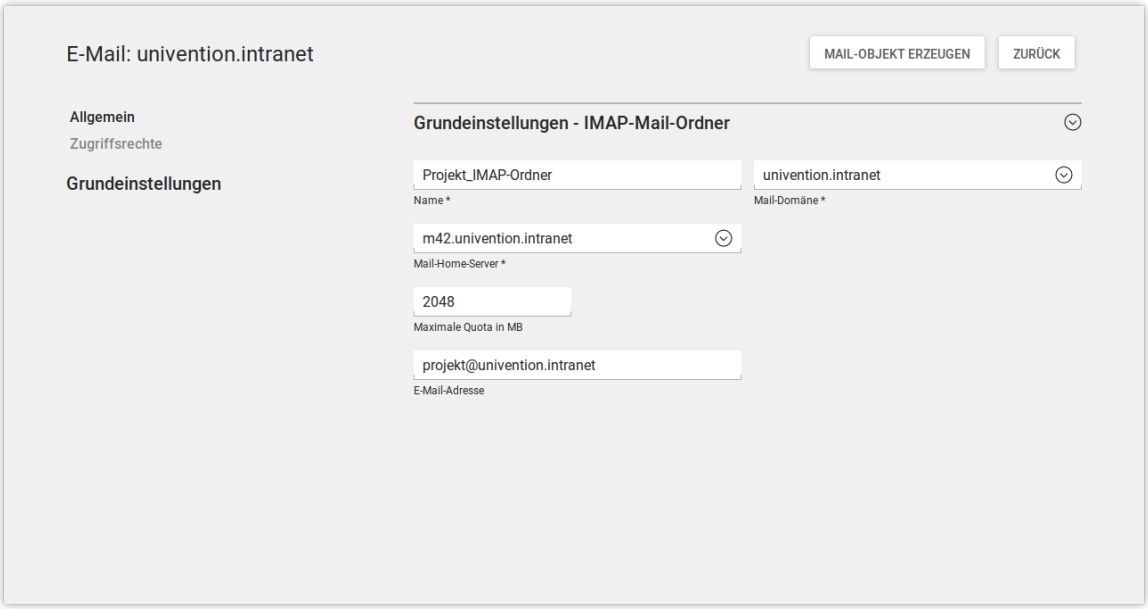


Tabelle 14.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name (*)	Der Name, unter dem der IMAP-Ordner im E-Mail-Client verfügbar ist. Der Name unterscheidet sich je nach dem, ob eine E-Mail-Adresse konfiguriert wird (siehe Zeile "Mail-Adresse" unten) oder nicht. Wird keine Mail-Adresse konfiguriert, erscheint der IMAP-Ordner im Client als `name@domain/INBOX`. Wird eine Mail-Adresse verwendet, wird der Name die Form `shared/name@domain` haben.
Mail-Domäne (*)	Jeder globale IMAP-Ordner ist einer Mail-Domäne zugeordnet. Die Verwaltung der Domänen ist in Abschnitt 14.3.1 dokumentiert.
Mail Home Server (*)	Ein IMAP-Ordner ist einem Mail Home Server zugeordnet. Weitere Hinweise finden sich in Abschnitt 14.8.10.
Maximale Quota in MB	Mit dieser Einstellung kann die maximale Gesamtgröße aller E-Mails in diesem Ordner festgelegt werden.
Mail-Adresse	Hier kann eine E-Mail-Adresse angegeben werden, durch die E-Mails direkt an den IMAP-Ordner gesendet werden können. Ist hier keine Adresse gesetzt, so kann nur aus E-Mail-Clients heraus in den Ordner geschrieben werden. Der Domänenanteil der E-Mail-Adresse muss in Univention Management Console registriert sein (siehe Abschnitt 14.3.1).

Tabelle 14.2. Reiter 'Zugriffsrechte'

Attribut	Beschreibung
Name (*)	Hier können Zugriffsberechtigungen auf Basis von Benutzern oder Gruppen vergeben werden. Benutzer werden mit Ihrem Benutzernamen eingetragen, als Gruppen werden die in Univention Management Console angelegten Gruppen verwendet. Die Zugriffsrechte haben folgende Auswirkungen für einzelne Benutzer oder Mitglieder der angegebenen Gruppe: Keine Es ist kein Zugriff möglich. Der Ordner wird nicht in der Ordnerliste angezeigt. lesen Es darf nur lesend auf bestehende Einträge zugegriffen werden. anhängen Bestehende Einträge dürfen nicht verändert werden, nur neue Einträge erzeugt werden. schreiben Neue Einträge in diesem Ordner anlegen, bestehende verändern oder bestehende löschen ist erlaubt.

Attribut	Beschreibung
	senden Eine E-Mail an diesen Ordner als Empfänger senden ist zugelassen. Dies wird nicht von jedem Client unterstützt. alles Umfasst alle Berechtigungen von 'schreiben' und erlaubt zusätzlich das Ändern von Zugriffsrechten.

14.3.6. Mail-Quota

Die Größe der Benutzerpostfächer kann über Mail-Quotas eingeschränkt werden, bei deren Erreichen vom Mailserver keine weiteren E-Mails für das Postfach angenommen werden, bis der Benutzer alte Mails aus seinem Konto entfernt hat.

Die Grenze wird in Megabytes im Feld **Mail-Quota** festgelegt, die unter **Erweiterte Einstellungen** -> **Mail** verwaltet wird. Der Standardwert ist `0` und bedeutet, dass keine Beschränkung aktiv ist. Für das Zuweisen einer Quota an mehrere Benutzer auf einmal, kann der Mehrfachbearbeitungsmodus von Univention Management Console verwendet werden, siehe Abschnitt 4.4.3.3.

Der Benutzer kann ab einer bestimmten erreichten Postfachgröße gewarnt werden und erhält dann eine Mail mit dem Hinweis, dass seine Speicherressourcen nahezu ausgelastet sind. Der Administrator kann den Schwellwert in Prozent, den Betreff der Nachricht und ihren Inhalt angeben:

- In der Univention Configuration Registry-Variable `mail/dovecot/quota/warning/text/PROZENT=TEXT` kann der Schwellwert konfiguriert werden, ab dem eine Warnmeldung ausgegeben werden soll. `PROZENT` muss als Zahl zwischen 0 und 100 ohne Prozentzeichen angegeben werden, TEXT wird der Inhalt der E-Mail.

  Wenn `TEXT` die Zeichenkette `$PERCENT` enthält, wird diese in der E-Mail mit dem überschrittenen Wert ersetzt.

  Der Wert der Univention Configuration Registry-Variable `mail/dovecot/quota/warning/subject` wird als Betreff der E-Mails verwendet.

- Bei der Installation des Mail-Server-Paketes werden Betreff und zwei Warn-Nachrichten automatisch konfiguriert:

  - `mail/dovecot/quota/warning/subject` wird gesetzt auf `Quota-Warning`
  - `mail/dovecot/quota/warning/text/80` wird gesetzt auf `Your mailbox has filled up to over $PERCENT%.`
  - `mail/dovecot/quota/warning/text/95` wird gesetzt auf `Attention: Your mailbox has already filled up to over $PERCENT%. Please delete some messages or contact the administrator.`

14.4. Spamerkennung und -filterung

Unerwünschte und nicht angeforderte E-Mails werden als Spam bezeichnet. Zur automatisierten Erkennung solcher E-Mails integriert UCS die Software SpamAssassin und Postgrey. SpamAssassin versucht anhand von Heuristiken über Herkunft, Form und Inhalt einer E-Mail zu erkennen, ob sie erwünscht ist oder nicht. Postgrey ist ein Policy Server für Postfix der "Greylisting" implementiert. Greylisting ist eine Spam-Erkennungsmethode die E-Mail beim ersten Zustellversuch eines externen Servers ablehnt. Mailserver von Spam-

versendern unternehmen häufig keinen zweiten Zustellversuch, während legitime Server dies tun. Die Integration erfolgt über die Pakete ***univention-spamassassin*** und ***univention-postgrey***, die bei der Einrichtung des Mailserver-Pakets automatisch eingerichtet werden.

SpamAssassin arbeitet mit einem Punktesystem, das mit steigender Punktzahl eine höhere Wahrscheinlichkeit für Spam ausdrückt. Punkte werden nach verschiedenen Kriterien vergeben, die beispielsweise auf Schlagworte innerhalb der E-Mail oder fehlerhafte Codierungen ansprechen. In der Grundeinstellung werden nur Mails bis zu einer Größe von 300 Kilobyte geprüft. Dies kann mit der Univention Configuration Registry-Variable `mail/antispam/bodysizelimit` konfiguriert werden. E-Mails, die als Spam klassifiziert wurden - also eine bestimmte Anzahl Punkte überschreiten - werden bei der Auslieferung durch Dovecot nicht im Posteingang des Empfängers, sondern im darunter liegenden Ordner *Spam* abgelegt. Der Name des Ordners kann mit der Univention Configuration Registry-Variable `mail/dovecot/folder/spam` konfiguriert werden. Die Filterung erfolgt durch ein Sieve-Skript, das beim Anlegen des IMAP-Postfachs eines Benutzers automatisch generiert wird.

Der in die Sieve-Skripte eingetragene Schwellwert, ab der E-Mails als Spam deklariert werden, ist mit der Univention Configuration Registry-Variable `mail/antispam/requiredhits` konfigurierbar. Die Voreinstellung (`5`) muss in der Regel nicht angepasst werden. Je nach Erfahrung im eigenen Umfeld kann dieser Wert aber auch niedriger angesetzt werden. Es muss dann jedoch mit mehr E-Mails gerechnet werden, die fälschlich als Spam erkannt wurden. Die Änderung des Schwellwerts wirkt sich nicht auf bestehende Benutzer aus, diese können den Wert aber im Horde-Webclient selbst anpassen (siehe Abschnitt 14.10.4).

Zusätzlich gibt es die Möglichkeit, E-Mails mit einem Bayes-Klassifikator bewerten zu lassen. Dieser vergleicht eine eingehende E-Mail mit statistischen Daten, die er aus bereits verarbeiteten E-Mails gewonnen hat und kann so seine Bewertung an die Mailgewohnheiten anpassen. Die Bayes-Klassifizierung wird vom Benutzer selbst gesteuert, in dem nicht vom System aber vom Benutzer als Spam erkannte E-Mails in den Unterordner *Spam* verschoben und eine Auswahl legitimer Mails in den Unterordner *Ham* (`mail/dovecot/folder/ham`) kopiert werden. Diese Ordner werden täglich ausgewertet und noch nicht erfasste oder bisher falsch klassifizierte Daten in einer gemeinsamen Datenbank erfasst. Diese Auswertung ist in der Grundeinstellung aktiviert und kann mit der Univention Configuration Registry-Variable `mail/antispam/learndaily` konfiguriert werden.

Die Spam-Filterung kann durch Setzen der Univention Configuration Registry-Variable `mail/antivir/spam` auf `no` deaktiviert werden. Bei Änderungen an Univention Configuration Registry-Variablen, die die Spamerkennung betreffen, muss der AMaViS-Dienst und Postfix neu gestartet werden.

14.5. Viren- und Malwareerkennung

Feedback

Die UCS-Maildienste integrieren eine Viren- und Malwareerkennung über das Paket ***univention-antivir-mail***, das bei der Einrichtung des Mailserver-Pakets automatisch eingerichtet wird. Der Virenscan kann mit der Univention Configuration Registry-Variable `mail/antivir` deaktiviert werden.

Alle ein- und ausgehenden E-Mails werden auf Viren geprüft. Wird ein Virus erkannt, wird die E-Mail unter Quarantäne gestellt, d.h. auf dem Server unerreichbar für den Benutzer abgelegt. Der ursprüngliche Empfänger erhält eine Benachrichtigung per E-Mail über diese Maßnahme. Bei Bedarf kann der Administrator die E-Mail aus dem Verzeichnis `/var/lib/amavis/virusmails/` wiederherstellen oder löschen. Eine automatische Löschung erfolgt nicht.

Die Software AMaViSd-new dient als Schnittstelle zwischen dem Mailserver und verschiedenen Virenscannern. Der freie Virenscanner ClamAV ist im Paket enthalten und nach der Installation sofort einsatzbereit. Die für die Virenerkennung nötigen Signaturen werden automatisch und kostenfrei durch den Freshclam-Dienst bezogen und aktualisiert.

Alternativ oder zusätzlich können andere Virenscanner in AMaViS eingebunden werden. Nach Änderungen an der AMaViS- oder ClamAV-Konfiguration müssen Postfix und AMaViS neu gestartet werden.

14.6. Identifikation von Spam Quellen mit *DNS basierten Blackhole List* (DNSBL)

Feedback

Eine weitere Möglichkeit gegen Spam vorzugehen ist die Verwendung von *DNS-based Blackhole List* (DNSBL) bzw. *Real-time Blackhole List* (RBL). DNSBL sind Listen von IP Adressen, von denen der Betreiber denkt, dass sie (potentiell) Quellen von Spam sind. Die Listen werden per DNS abgefragt. Ist dem DNS-Server die IP des sendenden E-Mail-Servers bekannt, so wird die Nachricht abgelehnt. Der Check einer IP-Adresse ist schnell und vergleichsweise ressourcenschonend. Er findet *vor* dem Annehmen der Nachricht statt. Erst nach dem Empfang findet die aufwändige Inhaltsüberprüfung mit SpamAssassin und Anti-Virus statt. Postfix hat eine eingebaute Unterstützung für DNSBL (http://www.postfix.org/postconf.5.html#reject_rbl_client).

Im Internet existieren DNSBL von verschiedenen Projekten und Firmen. Bitte informieren Sie sich auf deren Webseiten über Konditionen und Preise.

Um DNSBL mit Postfix zu verwenden muss die Univention Configuration Registry-Variable `mail/postfix/smtpd/restrictions/recipient/SEQUENZ=REGEL` gesetzt werden. Mit ihr können Empfangsbeschränkungen über die Postfix-Option *smtpd_recipient_restrictions* konfiguriert werden (siehe http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions). Die Sequenznummer dient der alphanumerisch Sortierung mehrerer Regeln, über die die Reihenfolge beeinflusst werden kann.

Tipp

Existierende *smtpd_recipient_restrictions* Regeln können wie folgt aufgelistet werden:

```
ucr search --brief mail/postfix/smtpd/restrictions/recipient
```

In einer unveränderten Univention Corporate Server Postfix Installation sollten die DNSBL am Ende der *smtpd_recipient_restrictions* Regeln angehängt werden. Zum Beispiel so:

```
ucr set mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client
 ix.dnsbl.manitu.net"
```

14.7. Integration von Fetchmail zum Abrufen von Mail von externen Postfächern

Feedback

Im Regelfall nimmt der UCS-Maildienst Mails für die Benutzer des UCS-Domäne direkt über SMTP entgegen. UCS bietet zusätzlich eine optionale Integration der Software Fetchmail zum Abrufen von Emails von externen POP3 oder IMAP-Postfächern.

Fetchmail kann über das Univention App Center installiert werden; dort muss die Applikation **Fetchmail** ausgewählt werden und auf **Installieren** geklickt werden.

Nach Abschluss der Installation finden sich in der Benutzerverwaltung im Reiter **Erweiterte Einstellungen -> Mailabruf von externen Servern** zusätzliche Eingabefelder, mit denen der Mailabruf von einem externen Server konfiguriert werden kann. Die Mails werden dabei in die Postfächer der jeweiligen Benutzer eingeliefert (die primäre E-Mail-Adresse muss dafür konfiguriert sein).

Der Abruf erfolgt alle zwanzig Minuten sobald mindestens ein Postfach für den Abruf konfiguriert wurde. Nach der initialen Konfiguration eines Benutzers muss Fetchmail im UMC-Modul **Systemdienste** gestartet werden. Dort kann der Start des Dienstes auch deaktiviert werden (alternativ durch Setzen der Univention Configuration Registry-Variable `fetchmail/autostart` auf `false`).

Tabelle 14.3. Reiter 'Mailabruf von externen Servern'

Attribut	Beschreibung
Benutzername	Der Benutzername, der für den Abruf der Mail an den Mailserver übergeben werden soll.
Passwort	Das Passwort, das für den Mailabruf verwendet werden soll.
Protokoll	Der Abruf kann über die Protokolle IMAP oder POP3 erfolgen.
Externer Mailserver	Der Name des Mailservers, von dem die Mails abgerufen werden sollen.
Verbindung verschlüsseln (SSL/TLS)	Ist diese Option aktiviert, erfolgt der Mailabruf verschlüsselt (sofern dies vom Mailserver unterstützt wird).
Mails auf dem Server nicht löschen	In der Grundeinstellungen werden die abgerufenen Mails nach dem Transfer auf dem Server gelöscht. Ist diese Option aktiviert, kann dies unterbunden werden.

14.8. Konfiguration des Mailservers

Feedback

14.8.1. Konfiguration eines Relay-Hosts für den Mailversand

Feedback

In der Grundeinstellung baut Postfix beim Versenden einer E-Mail an eine nicht-lokale Adresse eine direkte SMTP-Verbindung an den für diese Domain zuständigen Mailserver auf. Dieser Server wird durch eine Abfrage des MX-Records im DNS ermittelt.

Alternativ kann auch ein Mail-Relay-Server zu Einsatz kommen, also ein Server der die Mails entgegen nimmt und den weiteren Versand abwickelt. Ein solcher Mail-Relay-Server kann beispielsweise von einer übergeordneten Konzernzentrale oder vom Internet-Provider bereitgestellt werden. Ein Relay-Server muss als vollqualifizierter Domänenname (FQDN) in die Univention Configuration Registry-Variable `mail/relayhost` eingetragen werden.

Ist für den Versand die Authentifizierung gegenüber dem Relay-Host notwendig, muss die Univention Configuration Registry-Variable `mail/relayauth` auf `yes` gesetzt und die Datei `/etc/postfix/smtp_auth` bearbeitet werden. In dieser Datei muss der Relay-Host, der Benutzername und das Passwort in einer Zeile hinterlegt werden:

```
FQDN-RelayhostBenutzername:Passwort
```

Anschließend muss für diese Datei

```
postmap /etc/postfix/smtp_auth
```

aufgerufen werden, damit die Änderungen durch Postfix übernommen werden.

Anmerkung

Um eine verschlüsselte Verbindung bei der Verwendung eines Relay-Hosts sicherzustellen, muss die Postfix-Option `smtp_tls_security_level=encrypt` gesetzt sein. Univention Corporate Server setzt diese Option automatisch, wenn `mail/relayhost` gesetzt und `mail/relayauth` auf `yes` gesetzt ist und `mail/postfix/tls/client/level` nicht auf `none` stehen.

14.8.2. Konfiguration der maximalen E-Mailgröße

Feedback

Mit der Univention Configuration Registry-Variable `mail/messagesizelimit` kann die maximale Größe in Byte für ein- und ausgehende E-Mails festgelegt werden. Die voreingestellte Maximalgröße beträgt 10240000 Byte. Nach Änderung der Einstellung muss Postfix neu gestartet werden. Wird `0` als Wert konfi-

guriert, so wird die Begrenzung aufgehoben. Es ist zu beachten, dass Emailanhänge durch die Base64-Kodierung um ca. ein Drittel vergrössert werden.

Wird Horde (siehe Abschnitt 14.10) eingesetzt, müssen außerdem die Univention Configuration Registry-Variablen `php/limit/filesize` und `php/limit/postsize` angepasst werden. Als Wert muss in beide Variablen die maximale Größe in Megabyte eingetragen werden. Anschließend muss der Apache-Webserver neu gestartet werden.

14.8.3. Konfiguration einer Blindkopie zur Anbindung von E-Mail-Archivierungslösungen

Wird die Univention Configuration Registry-Variable `mail/archivefolder` auf eine E-Mail-Adresse gesetzt, sendet Postfix eine Blindkopie aller ein- und ausgehenden E-Mails an diese Adresse. So kann eine Archivierung aller E-Mails erreicht werden. Die E-Mail-Adresse muss bereits existieren. Sie kann entweder eine in Univention Corporate Server registrierte E-Mail-Adresse eines Benutzers sein, oder von einem externen Dienst bereitgestellt werden. Standardmäßig ist die Variable nicht gesetzt.

Anschließend muss Postfix neu gestartet werden.

14.8.4. Konfiguration von Softbounces

Bei einer Reihe von Fehlersituationen (z.B. bei nicht vorhandenen Benutzern) kann es zu einem Bounce der betroffenen Mail kommen, d.h. die Mail wird an den Absender zurückgesendet. Mit dem Setzen der Univention Configuration Registry-Variable `mail/postfix/softbounce` auf `yes` werden Mails nie mit einem Bounce zurückgesendet, sondern immer weiterhin in der Queue vorgehalten. Diese Einstellung ist insbesondere für Konfigurationsarbeiten am Mailserver sehr nützlich.

14.8.5. Konfiguration der SMTP Ports

Auf einem Univention Corporate Server-Mailserver ist Postfix so konfiguriert, dass es auf Verbindungen an drei Ports wartet:

- Port 25 (`SMTP`) sollte nur von anderen Mailservern verwendet werden. Standardmäßig ist die Authentifikation an diesem Port deaktiviert. Wenn das Einliefern von E-Mails an Port 25 erlaubt werden soll, kann die Univention Configuration Registry-Variable `mail/postfix/mastercf/options/smtp/smtpd_sasl_auth_enable=yes` gesetzt werden.
- Port 465 (`SMTPS`) erlaubt die Authentifikation gegenüber dem Mailserver und das Einliefern von E-Mails über eine mit SSL verschlüsselte Verbindung. `SMTPS` wurde zugunsten von Port 587 als veraltet erklärt, wird jedoch für Altsysteme aktiviert gelassen.
- Port 587 (`Submission`) erlaubt die Authentifikation gegenüber dem Mailserver und das Einliefern von E-Mails über eine TLS-verschlüsselte Verbindung. Die Verwendung von STARTTLS wird erzwungen.

Der `Submission`-Port sollte von E-Mail-Clients bevorzugt verwendet werden. Die Verwendung der Ports 25 und 465 zur Einlieferung von E-Mails ist überholt.

14.8.6. Konfiguration zusätzlicher Prüfungen durch postscreen

Bei der Verwendung eines Mailservers, der direkt vom Internet aus erreichbar ist, besteht immer die Gefahr, dass Versender von Spam oder defekte Mailserver kontinuierlich versuchen, auf dem UCS-System ungewollte Mails (z.B. Spam) abzuliefern.

Um die Last des Mailservers für solche Fälle zu reduzieren, bringt Postfix einen eigenen Dienst mit dem Namen postscreen mit, der Postfix vorgeschaltet wird und die eingehenden SMTP-Verbindungen annimmt.

Mit diesen Verbindungen werden zunächst einige leichtgewichtige Tests durchgeführt. Ist das Ergebnis positiv, wird die Verbindung an Postfix durchgereicht. Im negativen Fall wird die SMTP-Verbindung beendet und somit die eingehende Mail abgelehnt, bevor sie im Verantwortungsbereich des UCS Mailservers angekommen ist.

In der Standardeinstellung ist postscreen nicht aktiv. Durch das Setzen der Univention Configuration Registry-Variable `mail/postfix/postscreen/enabled` auf den Wert `yes` kann postscreen aktiviert werden.

Über diverse UCR-Variablen mit dem Präfix `mail/postfix/postscreen/` können weitere Einstellungen vorgenommen werden. Eine Liste der UCR-Variablen nebst Beschreibungen können z.B. auf der Kommandozeile über den Befehl `ucr search --verbose mail/postfix/postscreen/` abgerufen werden.

Anmerkung

Nach jeder Änderung einer UCR-Variable für postscreen sollte die Konfiguration von Postfix und postscreen neu geladen werden, was über den Befehl `service postfix reload` ausgelöst werden kann.

14.8.7. Eigene Anpassung der Postfix Konfiguration

Die Konfiguration von Postfix, welche sich in der Datei `/etc/postfix/main.cf` befindet, wird über Univention Configuration Registry-Variablen definiert. Eine Erweiterung der Konfiguration, die über die vorhandenen Univention Configuration Registry-Variablen hinaus geht, ist ebenso möglich.

Existiert die Datei `/etc/postfix/main.cf.local`, so wird ihr Inhalt an die Datei `main.cf` angehängt. Damit Änderungen an `main.cf.local` nach `main.cf` übernommen werden, muss der folgende Befehl ausgeführt werden:

```
ucr commit /etc/postfix/main.cf
```

Zum Übernehmen der Änderungen durch den Postfix Dienst muss dieser neu geladen werden:

```
service postfix reload
```

Wird in der Datei `main.cf.local` eine Postfix Variable gesetzt, die zuvor auch in `main.cf` gesetzt wurde, so schreibt Postfix eine Warnung in die Logdatei `/var/log/mail.log`.

Anmerkung

Wenn das Verhalten des E-Mail-Servers nicht der Erwartung entspricht, sollten zuerst die Einstellungen, die durch `main.cf.local` aktiviert wurden, rückgängig gemacht werden. Dazu muss die Datei umbenannt oder ihr Inhalt auskommentiert werden. Im Anschluss müssen die beiden oben genannten Kommandos ausgeführt werden. Die Konfiguration entspricht dann wieder der Standardkonfiguration von UCS.

14.8.8. Konfiguration des Alias Expansion Limits

Werden E-Mails an einer Gruppe gesendet, die wiederum andere Gruppen enthält, kann es passieren, dass diese E-Mails nicht akzeptiert werden. Das liegt daran, dass Postfix durch eine Virtual Alias Expansion versucht, die Anzahl der ursprünglichen Empfänger entsprechend zu erweitern. Diese Anzahl wird standardmäßig auf 1000 Nutzer begrenzt und kann daher zu gering sein.

Um den Wert auf beispielsweise 5000 Nutzer zu erhöhen, muss die folgende Zeile in `/etc/postfix/main.cf.local` hinzugefügt bzw. angepasst werden:

```
virtual_alias_expansion_limit = 5000
```

Danach muss Postfix neugestartet werden:

```
service postfix restart
```

14.8.9. Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten

Das Postfach eines Benutzers ist mit der primären E-Mail-Adresse verknüpft und nicht mit dem Benutzernamen. Mit der Univention Configuration Registry-Variable `mail/dovecot/mailbox/rename` kann das Verhalten bei der Änderung der primären E-Mail-Adresse konfiguriert werden.

- Ist die Variable auf `yes` gesetzt, wird das IMAP-Postfach des Benutzers umbenannt. Dies ist seit UCS 3.0 die Standardeinstellung.
- Bei der Einstellung `no`, sind nach dem Ändern der primären E-Mail-Adresse eines Benutzers seine bisherigen E-Mails nicht mehr erreichbar! Wird einem anderen Benutzer eine ehemals vergebene primäre E-Mail-Adresse zugewiesen, bekommt dieser Zugriff auf die alte IMAP-Struktur dieses Postfachs.

Mit der Univention Configuration Registry-Variable `mail/dovecot/mailbox/delete` kann konfiguriert werden, ob IMAP-Postfächer automatisch gelöscht werden sollen. Der Wert `yes` aktiviert die Löschung des betroffenen IMAP-Postfachs bei folgenden Aktionen:

- dem Löschen des Benutzerkontos
- dem Entfernen der primären Mailadresse von einem Benutzerkonto
- dem Ändern des Mail Home Servers auf ein anderes System

In der Grundeinstellung (`no`) bleiben die Postfächer bei diesen Aktionen erhalten und müssen ggf. manuell gelöscht werden.

Aus der Kombination der beiden Variablen ergeben sich folgende vier Fälle, wenn E-Mail-Adressen geändert werden:

Tabelle 14.4. Umbenennung von E-Mail-Adressen

`mail/dovecot/mailbox/…`	**Bedeutung**
`rename=yes` und `delete=no` (Standard)	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
`rename=yes` und `delete=yes`	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
`rename=no` und `delete=no`	Eine neue, leere Mailbox wird erzeugt. Die alte bleibt unter dem alten Namen auf der Festplatte erhalten und ist damit vorerst für Benutzer nicht zu erreichen.
`rename=no` und `delete=yes`	Eine neue, leere Mailbox wird erzeugt. Die alte Mailbox wird inkl. aller enthaltenen Mails von der Festplatte gelöscht.

14.8.10. Verteilung einer Installation auf mehrere Mailserver

Das UCS-Mailsystem bietet die Möglichkeit die Benutzer auf mehrere Mailserver zu verteilen. Dazu wird jedem Benutzer ein sogenannter Mail Home Server zugewiesen, auf dem die Maildaten des Benutzers abge-

legt werden. Beim Zustellen einer E-Mail wird der zuständige Home Server automatisch aus dem LDAP-Verzeichnis ermittelt.

Es ist zu beachten, dass globale IMAP-Ordner (siehe Abschnitt 14.3.5) einem Mail Home Server zugeordnet sind.

Beim ändern des Mail Home Servers eines Benutzers werden dessen E-Mails *nicht* automatisch auf den neuen Server verschoben.

14.8.11. Mailserver-Speicher auf NFS

Dovecot unterstützt das Speichern von E-Mails und Index-Dateien auf Cluster-Dateisystemen und NFS. Einige Einstellungen sind jedoch nötig, um Datenverluste in bestimmten Situationen zu vermeiden.

Die folgenden Einstellungen gehen davon aus, dass auf Mailboxen nicht gleichzeitig von mehreren Servern aus zugegriffen wird. Das ist der Fall, wenn jedem Benutzer ein Mail Home Server zugeordnet ist.

- `mail/dovecot/process/mmap_disable = yes`
- `mail/dovecot/process/dotlock_use_excl = yes`
- `mail/dovecot/process/mail_fsync = always`

Um eine bessere Performance zu erreichen, können Index-Dateien statt zusammen mit den Nachrichten im NFS auch auf der lokalen Festplatte gespeichert werden. Sie sind dann unter `/var/lib/dovecot/index/` zu finden. Setzen Sie dafür die Univention Configuration Registry-Variable `mail/dovecot/location/separate_index = yes`.

Mit diesen Einstellungen sollte normalerweise alles problemlos funktionieren. Die im Einsatz befindlichen Server- und Client-Systeme sind jedoch so vielfältig, dass hier noch ein paar Hinweise folgen, wie bei Schwierigkeiten weiter vorgegangen werden kann:

- Wenn NFSv2 im Einsatz ist (nicht der Fall, wenn der NFS-Server ein Univention Corporate Server ist), setzen Sie bitte `mail/dovecot/process/dotlock_use_excl = no`.
- Falls kein lockd eingesetzt wird (nicht der Fall auf Univention Corporate Server-Systemen) oder falls trotz des Einsatzes von lockd Locking-Fehler auftreten, setzen Sie `mail/dovecot/process/lock_method = dotlock`. Dies verringert die Performance, aber behebt die meisten Locking-bezogenen Probleme.
- Dovecot kann mit `mail/dovecot/process/mail_nfs_storage = yes` angewiesen werden, wenn nötig, den NFS Cache zu leeren. Dies funktioniert jedoch nicht immer, daher kann es zu sporadischen Fehlern kommen. Das gleiche gilt für das Leeren des NFS-Cache nach dem Schreiben von Index-Dateien: `mail/dovecot/process/mail_nfs_index = yes`.
- In der Documentation des Dovecot Servers sind weitere Hinweise zu finden: [dovecot-wiki-clusterfs] [dovecot-wiki-nfs]

14.8.12. Beschränkung der Verbindungsanzahl

In der Standardeinstellung in UCS wird Dovecot für jeweils maximal 400 gleichzeitige Verbindungen per IMAP und POP3 ausgeliefert. Diese reichen sicher aus, um 100 gleichzeitig eingeloggte IMAP-Benutzer zu bedienen, unter Umständen deutlich mehr. Wie viele IMAP-Verbindungen Benutzer gleichzeitig geöffnet haben, hängt von den eingesetzten Clients ab. Webmail öffnet nur einzelne, kurzlebige Verbindungen. Desktop E-Mail-Programme halten über lange Zeit mehrere Verbindungen offen. Mobile Clients halten über

lange Zeit wenige Verbindungen offen, aber beenden diese oft nicht von sich aus, so dass sie unnötig lang Ressourcen belegen. Die Beschränkungen dienen primär dazu, einem Denial-of-service-Angriff durch sehr viele geöffnete Prozesse und Netzwerkverbindungen zu widerstehen.

Um die in diesem Augenblick offenen Verbindungen zu sehen, kann folgender Befehl ausgeführt werden:

```
doveadm who
```

Um die Gesamtanzahl auszugeben:

```
doveadm who -1 | wc -l
```

Um die Beschränkungen zu verändern, können die Univention Configuration Registry-Variablen `mail/dovecot/limits/*` angepasst werden. Der Vorgang ist auf Grund des komplexen Zusammenspiels dieser Variablen nur halb automatisch. Die Bedeutung aller Variablen kann in der Dovecot Dokumentation nachgelesen werden: [dovecot-wiki-services].

Da bei Dovecot verschiedene Prozesse für Login und Zugriff auf die E-Mail-Dateien zuständig sind, können diese getrennt konfiguriert werden. Zusätzlich wird getrennt konfiguriert wie viele Verbindungen zu einem Dienst erlaubt sind und wie viele Prozesse für einen Dienst gestartet werden. Durch das Setzen von `mail/dovecot/limits/default_client_limit = 3000` würde die Beschränkung für die Anzahl an Verbindungen zu den POP3- und IMAP-Diensten verändert, nicht jedoch für die erlaubte Anzahl an Prozessen. In der Univention Corporate Server Standardeinstellung läuft Dovecot im *High-security mode*: Jede Verbindung wird von einem separaten Login-Prozess betreut. Da standardmäßig nur 400 Prozesse erlaubt sind, können auch nicht mehr Verbindungen geöffnet werden.

Um 3000 Verbindungen von Benutzern zu ihren E-Mails zu erlauben, muss daher eine weitere Univention Configuration Registry-Variable gesetzt werden:

```
ucr set mail/dovecot/limits/default_client_limit=3000
ucr set mail/dovecot/limits/default_process_limit=3000
doveadm reload
```

Ein Blick in `/var/log/dovecot.info` offenbart nun eine Warnung:

```
config: Warning: service auth { client_limit=2000 } is lower than
 required under max. load (15000)
config: Warning: service anvil { client_limit=1603 } is lower than
 required under max. load (12003)
```

Die Dienste `auth` (Zuständig für Login und SSL-Verbindungen) sowie `anvil` (Zuständig für Statistiken) haben noch das Standardlimit. Es werden zwar je 3000 POP3- und IMAP-Verbindungen und -Prozesse erlaubt, aber die Anzahl der Prozesse für Login und SSL ist nun zu niedrig um sie alle zu bedienen. Dies wird dazu führen, dass Logins fehlschlagen.

Die hohen Werte kommen dadurch zustande, dass mit `default_client_limit` und `default_process_limit` nicht nur die Beschränkungen von IMAP und POP3 erhöht werden, sondern auch einiger weiterer Dienste wie `lmtp` und `managesieve-login`. Diese Dienste können nun mehr zu überwachende Prozesse starten und theoretisch mehr Authentifizierungen durchführen, wodurch sich die maximale Anzahl gleichzeitiger Verbindungen zu den Diensten `auth` und `anvil` erhöht.

Die Werte für die Dienste müssen nun der Fehlermeldung entsprechend angepasst werden:

```
ucr set mail/dovecot/limits/auth/client_limit=15000
ucr set mail/dovecot/limits/anvil/client_limit=12003
doveadm reload
```

Ein Blick in `/var/log/dovecot.info` offenbart nun noch eine letzte Warnung:

```
master: Warning: fd limit (ulimit -n) is lower than required under max.
 load (2000 < 15000),…
 because of service auth { client_limit }
```

Das vom Linux-Kernel kontrolliere `ulimit` (die erlaubte Anzahl gleichzeitig geöffneter Dateien/Verbindungen pro Prozess) wird nur bei einem Neustart des Dovecot-Dienstes verändert, daher:

```
invoke-rc.d dovecot restart
```

Nun erscheint keine Fehlermeldung mehr, und IMAP- und POP3-Server akzeptieren nun beide je 3000 Verbindungen.

Univention Corporate Server konfiguriert Dovecot so, dass es standardmäßig im *High-security mode* läuft. In Installationen mit 10.000en Benutzern kann Dovecot im *High-performance mode* betrieben werden. Der Performance-Leitfaden beschreibt, wie dieser konfiguriert werden kann: [ucs-performance-guide].

14.9. Konfiguration von Mail-Clients für den Mailserver

Feedback

Um einen Mail-Client mit dem UCS-Mailserver zu verwenden wird die Verwendung von IMAP empfohlen. Durch STARTTLS wird bei Verwendung von SMTP (für den Mailversand) und IMAP (für den Mailabruf/-synchronisation) nach einer initialen Aushandlungsphase auf eine TLS-gesicherte Verbindung umgeschaltet. Als Authentifizierungsmethode sollte *Passwort (plain text)* in Verbindung mit *STARTTLS* verwendet werden. Die Benennung der Methode unterscheidet sich je nach Mail-Client. Der folgende Screenshot zeigt exemplarisch die Einrichtung von Mozilla Thunderbird:

Abbildung 14.3. Einrichtung von Mozilla Thunderbird

14.10. Webmail und Verwaltung von E-Mail-Filtern mit Horde

Feedback

UCS integriert mehrere Applikationen des Horde-Frameworks für den Webzugriff auf E-Mails und zur webbasierten Verwaltung von serverseitigen E-Mail-Filterregeln auf Basis von Sieve. Horde kann über das Univention App Center installiert werden (siehe Abschnitt 5.3).

14.10.1. Anmeldung und Übersicht

Feedback

Die Horde-Anmeldemaske ist auf der Übersichtswebseite (siehe Abschnitt 4.2) unter **Horde Webclient** verlinkt und kann auch direkt unter `http://SERVERNAME/horde/` erreicht werden.

Abbildung 14.4. Anmeldung an Horde

Als **Benutzername** kann entweder der UCS-Benutzername oder die primäre E-Mail-Adresse eingegeben werden. Das Webmail-Interface kann in verschiedenen Darstellungsvarianten verwendet werden. Die gewünschte Variante kann unter **Modus** ausgewählt werden. Für Standard-Workstations wird die Verwendung des dynamischen Interfaces empfohlen. Die weitere Dokumentation orientiert sich an dieser Variante. Die Auswahl der **Sprache** hat bei vielen Browsern keine Auswirkung, da die bevorzugte Spracheinstellung des Browsers Vorrang hat.

In der oberen Bildleiste finden sich mehrere Menüpunkte (z.B. **Webmail** oder **Adressbuch**), mit denen zwischen den einzelnen Modulen gewechselt werden kann.

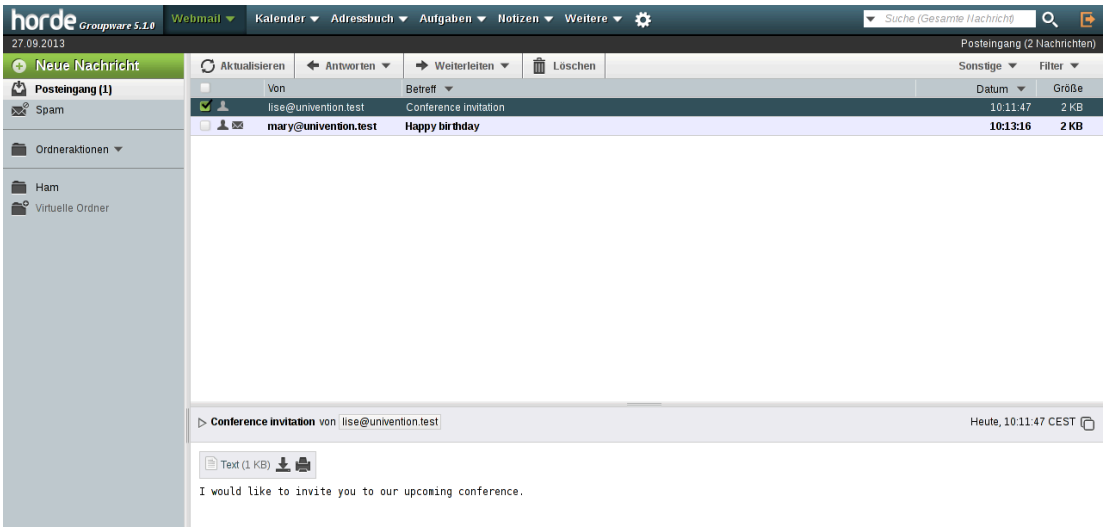
Durch Klick auf das Zahnrad-Symbol kann Horde vom Benutzer personalisiert werden.

14.10.2. Webbasierter Mailzugriff

Feedback

Horde bietet alle Standardfunktionen eines E-Mail-Clients, wie das Versenden, Weiterleiten oder Löschen von E-Mails. E-Mails können in Ordner einsortiert werden und werden standardmäßig im **Posteingang** abgelegt. Beim ersten Versenden einer E-Mail wird automatisch ein *Gesendet*-Ordner erstellt.

Abbildung 14.5. Webmail (Posteingang)



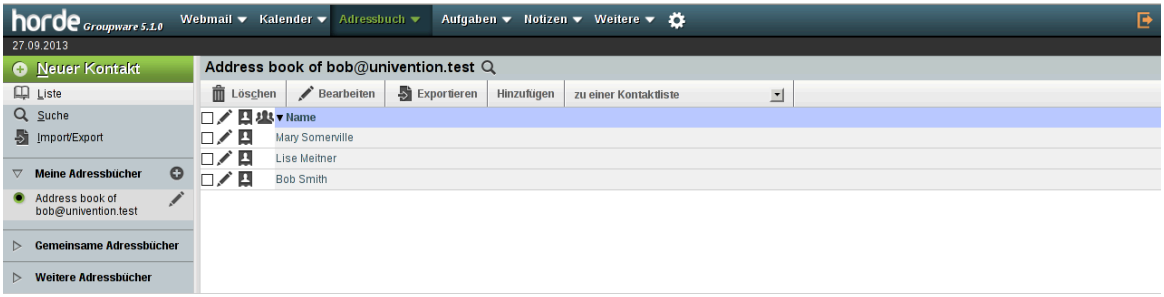
Horde unterscheidet zwei Arten von Löschungen: Eine mit **Löschen** entfernte E-Mail wird zuerst in den Ordner *Papierkorb* verschoben. Sie kann von dort wieder in andere Ordner verschoben werden, solange der Papierkorb nicht mit **Leeren** geleert wird.

14.10.3. Adressbuch

Feedback

In diesem Modul werden E-Mail-Adressen und weitere Kontaktdaten verwaltet. Die hier erfassten Informationen werden in einer Horde-eigenen SQL-Datenbank gespeichert.

Abbildung 14.6. Adressbuch für Webmail



Mit der einfachen oder erweiterten Suche gefundene Kontaktdaten lassen sich in eigene Adressbücher kopieren und dort bearbeiten. Neue Kontakte können über den Menü-Punkt **Neuer Kontakt** eingetragen werden. Über **Meine Adressbücher** können auch zusätzliche persönliche Adressbücher erstellt werden.

Über den Menü-Punkt **Liste** lässt sich der Inhalt von Adressbüchern anzeigen. Die Listen lassen sich durch Klick auf einen gewünschten Spaltenkopf (Name, Vorname, etc.) alphabetisch sortieren. Ein Klick auf das Lupen-Symbol in der Kopfzeile des jeweiligen Adressbuches (direkt neben dem Adressbuchnamen) öffnet ein Suchfeld, durch das man einfach innerhalb des angezeigten Adressbuchs suchen kann. Aus einer Liste können einzelne Adressen zur anschließenden Verwendung durch ein Kreuz in der ersten Spalte markiert werden, z.B. um sie als Datei in einem bestimmten Dateiformat zu exportieren oder in ein anderes Adressbuch zu kopieren.

14.10.4. E-Mail-Filter

Feedback

Dovecot unterstützt serverseitige Filterskripte, die in einer eigenen Skriptsprache namens Sieve geschrieben werden. Das Filter-Modul erlaubt die Generierung dieser Filterskripte. Sie gelten allgemein, greifen also auch für Benutzer, die über einen Standard-Mail-Client auf ihre Postfächer zugreifen.

Abbildung 14.7. Filterverwaltung in Horde

Die Regeln lassen sich unter **Webmail** -> **Filter** bearbeiten und ergänzen. Die Filter werden in der durchnummerierten Reihenfolge auf eingehende E-Mails angewandt. Ihre Position lässt sich sowohl über die Pfeile rechts als auch durch direkte Eingabe einer Nummer in der Spalte `Verschieben` anpassen. Einzelne Filterregeln können in der Spalte `Aktiviert` an- und abgeschaltet werden.

Unter **Spam** kann benutzerbezogen angepasst werden, welcher Spam-Schwellwert gelten soll. Der angegebene **Spam-Level** ist der SpamAssassin-Schwellwert. Eine E-Mail, die diesen Wert erreicht, wird in den angegebenen Ordner verschoben.

Unter **Abwesenheit** lässt sich ein Zeitraum festlegen, in dem auf eingehende E-Mails automatisch vom Mailserver mit einer Antwort-E-Mail reagiert wird. Text und Betreff der E-Mail ist frei wählbar.

Über **Neue Regel** können eigene Regeln erstellt werden, bspw. zur automatischen Sortierung von eingehenden E-Mails in themenbezogene Mailordner.

Ein Klick auf **Skript** zeigt den Quelltext des generierten Sieve-Skripts an.

Kapitel 15. Infrastruktur-Monitoring

15.1. Einführung

Feedback

UCS bietet zwei unterschiedliche Lösungen für das Monitoring der Infrastruktur. Einerseits das UCS Dashboard mit dessen Hilfe Administratoren sehr schnell den Zustand der Domänen und einzelner Server abzulesen. Anderseits gibt es mit Nagios die Möglichkeit, fortlaufend im Hintergrund Rechner und Dienste zu überprüfen und proaktiv eine Benachrichtigung auszulösen, sollte eine Warnstufe erreicht werden.

In den folgenden Kapiteln werden die beiden unterschiedlichen Lösungen beschrieben.

15.2. UCS Dashboard

Feedback

15.2.1. Einführung und Aufbau

Feedback

Das UCS Dashboard ermöglicht es Administratoren, den Zustand der Domäne und einzelner Server schnell und übersichtlich auf sogenannten Dashboards abzulesen. Die Dashboards sind über einen Web-Browser erreichbar, greifen im Hintergrund auf eine Datenbank zu und liefern kontinuierlich aktualisierte Reports über bestimmte Aspekte der Domäne oder der Server.

Voraussetzung für die Nutzung der *UCS Dashboard* App ist eine gültige Subskription. Mehr Informationen dazu sind auf der Webseite https://www.univention.de/produkte/preise/ zu finden.

15.2.2. Installation

Feedback

Das UCS Dashboard besteht aus drei Teilen:

- Die UCS Dashboard App für die Visualisierung von Daten aus der zentralen Datenbank. Diese Komponente basiert auf der Softwarekomponente Grafana.
- Die UCS Dashboard Database App, eine Zeitserien-Datenbank für die Speicherung der Metriken. Diese Datenbank wird durch die Software Prometheus bereitgestellt.

- Die UCS Dashboard Client App für die Bereitstellung der Metriken von Serversystemen. Dieser baut auf dem Prometheus Node-Exporter auf.

Die App *UCS Dashboard* kann aus dem Univention App Center auf einem Server in der Domäne installiert werden. Derzeit ist die Installation nur auf den Systemrollen Domaincontroller Master, Backup oder Slave erlaubt. Die Apps *UCS Dashboard Database* und *UCS Dashboard Client* werden automatisch auf dem System mitinstalliert.

Die App *UCS Dashboard Client* sollte auf jedem UCS-System installiert werden. Nur dadurch werden die Daten des Systems auf dem Dashboard dargestellt.

15.2.3. Nutzung

Feedback

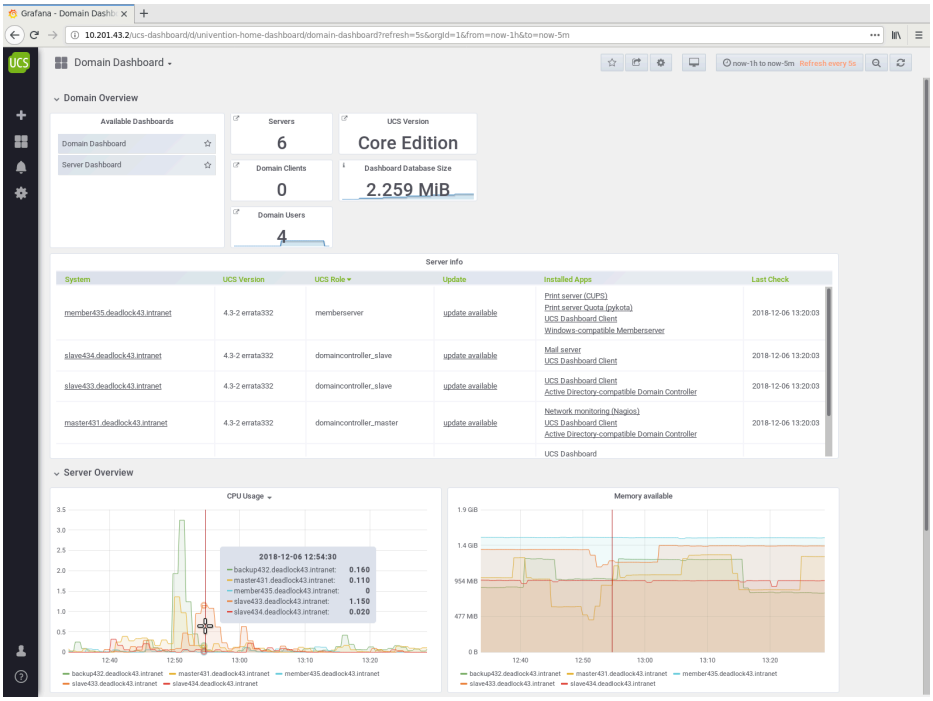
Nach der Installation ist das UCS Dashboard im Portal verlinkt. Alternativ kann es direkt über `https://SERVERNAME-OR-IP/ucs-dashboard/` erreicht werden.

Der Zugriff wird in der Standardeinstellung ausschließlich Benutzern der Gruppe `Domain Admins` (z.B. der Benutzer Administrator) gewährt.

15.2.3.1. Domain Dashboard

Feedback

Abbildung 15.1. Domain Dashboard



Nach der Anmeldung wird standardmäßig das Domain Dashboard geöffnet. Auf diesem Dashboard werden allgemeine Informationen über die Domäne angezeigt, bspw. wie viele Server und wie viele Benutzer in der Umgebung existieren.

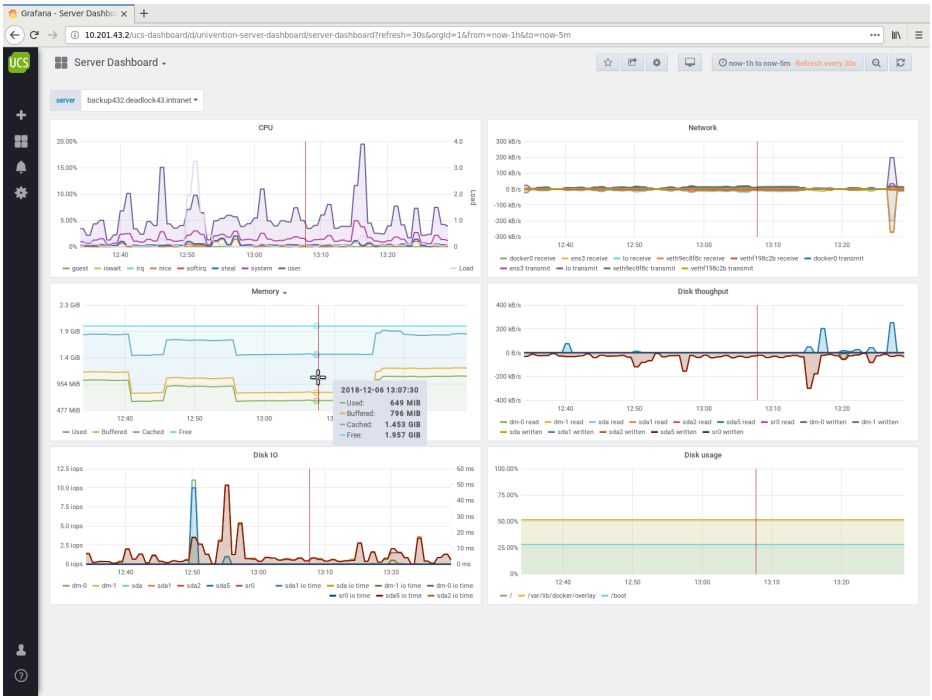
Weiter sind auf dem Dashboard, in einer tabellarischen Übersicht, die UCS-Systeme aufgelistet inkl. weiterer Informationen, wie bspw. die Server Rolle, die installierten Apps oder ob ein Update verfügbar ist.

Zusätzlich wird die CPU-Auslastung, Arbeitsspeicherauslastung, der freie Festplattenspeicher und der Status der LDAP-Replikation angezeigt. Dabei werden in den Grafiken jeweils alle Serversysteme angezeigt.

15.2.3.2. Server Dashboard

Feedback

Abbildung 15.2. Server Dashboard



Standardmäßig wird zusätzlich das Server Dashboard eingerichtet. Auf diesem Dashboard sind detaillierte Informationen zu einzelnen Serversystemen aufgelistet, wie bspw. die CPU- oder Speicherauslastung oder der Netzwerkdurchsatz.

Die Server können im Dropdown **server** ausgewählt werden. Anschließend werden die Grafiken entsprechend aktualisiert.

15.2.3.3. Eigene Dashboards

Feedback

Die beiden mitgelieferten Dashboards *Domain Dashboard* und *Server Dashboard* können nicht verändert werden, da diese von Univention durch Aktualisierungen ergänzt und verändert werden können.

Stattdessen können eigene Dashboards erstellt werden. Auf diesen Dashboards können dann entweder bereits vorhandene Elemente hinzugefügt werden oder auch neue Elemente erstellt werden. Dazu muss lediglich auf das Plus Zeichen am linken Rand geklickt werden. Anschließend existiert ein neues Dashboard, welches mit Elementen befüllt werden kann.

15.3. Nagios

Feedback

15.3.1. Einführung und Aufbau

Feedback

Mit Hilfe der Software Nagios ist es möglich, komplexe IT-Strukturen aus Netzen, Rechnern und Diensten fortlaufend automatisch auf korrekte Funktion zu überprüfen.

Für das Monitoring bringt Nagios eine umfassende Sammlung an Überwachungsmodulen mit. Diese können neben der Abfrage von Systemkennzahlen (z.B. CPU- und Speicherauslastung, freie Festplattenkapazität) auch die Erreichbarkeit und Funktion unterschiedlicher Dienste (z.B. SSH, SMTP, HTTP) testen. Für die Funktionstests werden in der Regel einfache Programmschritte wie das Ausliefern einer Testmail oder das Auflösen eines DNS-Eintrags durchgeführt. Neben den in Nagios enthaltenen Standardmodulen werden auch

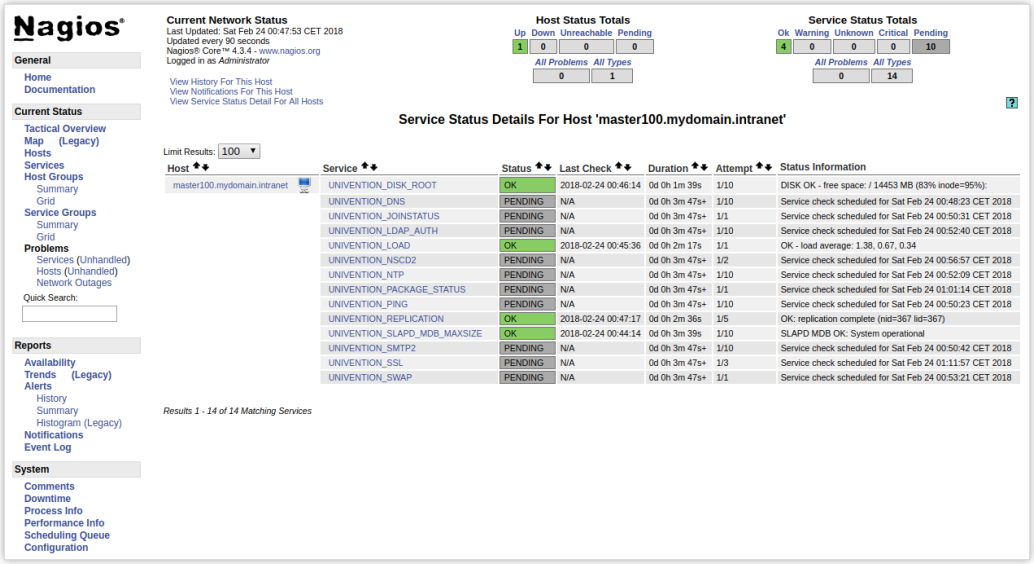
UCS-spezifische Überwachungsmodule mitgeliefert, mit denen etwa die Listener/Notifier-Replikation überwacht werden kann.

Nagios unterscheidet drei grundlegende Betriebszustände für einen Dienst:

- *OK* ist der Regelbetrieb
- *CRITICAL* beschreibt einen aufgetretenen Fehler, z.B. ein Webserver, der nicht erreichbar ist
- *WARNING* deutet auf einen möglicherweise bald auftretenden Fehlerzustand hin und ist somit eine Vorstufe zu *CRITICAL*. Beispiel: Der Test für ausreichend freien Speicherplatz auf der Root-Partition löst erst ab 90 Prozent Füllstand einen Fehler aus, aber bereits ab 75 Prozent eine Warnung.

Beim Wechsel eines Betriebszustands kann eine vorher festgelegte Kontaktperson über die mögliche Fehlfunktion informiert werden. Neben der reaktiven Benachrichtigung im Fehlerfall kann der aktuelle Status auch jederzeit laufend in einer webbasierten Oberfläche abgefragt werden, in der die Status-Informationen übersichtlich dargestellt werden.

Abbildung 15.3. Nagios Status-Webinterface



Nagios besteht aus drei Hauptkomponenten:

- Die Kernkomponente einer Nagios-Installation ist der *Nagios-Server*, der für die Erhebung und Speicherung der Überwachungsdaten zuständig ist.
- Die eigentliche Ermittlung der Statusinformationen wird von den *Nagios-Plugins* getätigt, die in regelmäßigen Abständen vom Nagios-Server aufgerufen werden. Die erhobenen Informationen werden im Nagios-Server gespeichert.
- Einige Statusinformationen können nicht über das Netz abgefragt werden kann (z.B. die Abfrage des freien Speicherplatzes auf einer Festplattenpartition). In diesem Fall kommt der NRPED-Dienst (Nagios Remote Plugin Executor Daemon) zum Einsatz, welcher nach einer Anfrage des Nagios-Servers auf dem entfernten Rechner Nagios-Plugins ausführt und die erhobenen Informationen anschließend zurückleitet. Der NRPED wird durch die Komponente *Nagios-Client* bereitgestellt, die auf allen UCS-Systemrollen vorinstalliert wird.

Die Nagios-Konfiguration erfolgt in Univention Management Console, die Nagios-Konfigurationsdateien werden automatisch aus den im LDAP-Verzeichnis gespeicherten Informationen generiert.

15.3.2. Installation

Feedback

Ein Nagios-Server kann mit der Applikation *Netzwerküberwachung (Nagios)* aus dem Univention App Center installiert werden. Alternativ kann das Softwarepaket ***univention-nagios-server*** installiert werden (anschließend muss `univention-run-join-scripts` aufgerufen werden). Weitere Informationen finden sich in Abschnitt 5.6. Der Nagios-Server kann auf beliebigen Systemrollen installiert werden, wobei die Verwendung eines Domänencontroller-Systems empfohlen wird. Der Nagios-Client ist auf allen Systemrollen standardmäßig installiert.

Sofern der Nagios-Server auf einem anderen System als dem Domänencontroller Master installiert wird, so muss auf allen Systemen, auf denen der Nagios-Client installiert ist, die Univention Configuration Registry-Variable `nagios/client/allowedhosts` mit dem FQDN des Nagios-Servers gesetzt werden. Am einfachsten kann dies über eine Univention Configuration Registry Richtlinie umgesetzt werden, weitere Informationen sind im Kapitel Abschnitt 8.3.4 zu finden.

Neben den Standard-Plugins, die mit der Installation des Pakets ***univention-nagios-client*** mitgebracht werden, können zusätzliche Plugins über folgende Pakete nachinstalliert werden:

- ***univention-nagios-raid*** Überwachung des Software-RAID-Status
- ***univention-nagios-smart*** Prüfung des S.M.A.R.T.-Status von Festplatten
- ***univention-nagios-opsi*** Prüfung der Softwareverteilung opsi
- ***univention-nagios-ad-connector*** Prüfung des AD Connectors

Einige der Pakete werden bei der Installation der entsprechenden Dienste automatisch mit eingerichtet. Wird beispielsweise der UCS AD Connector eingerichtet, bringt dieser das Überwachungs-Plugin ***univention-nagios-ad-connector*** mit.

15.3.2.1. Vorkonfigurierte Nagios-Prüfungen

Feedback

Während der Installation werden automatisch grundlegende Nagios-Prüfungen für die UCS-Systeme der Domäne eingerichtet. Die Einbindung weiterer Dienste wird in Abschnitt 15.3.3.1 dokumentiert.

Nagios-Dienst	**Funktion**
`UNIVENTION_PING`	Testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando `ping`. In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50ms bzw. 100ms überschreitet oder Paketverluste von 20% bzw. 40% auftreten.
`UNIVENTION_DISK_ROOT`	Überwacht den Füllstand der `/`-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% bzw. 10% wird der Fehlerzustand gesetzt.
`UNIVENTION_DNS`	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit der öffentlichen DNS-Server durch die Abfrage des Rechnernamens `www.univention.de`. Ist für die UCS-Domäne kein DNS-Forwarder definiert, schlägt diese Abfrage fehl. In diesem Fall kann `www.univention.de` z.B. gegen den FQDN des Domaincontroller Master ersetzt werden, um die Funktion des Namensauflösung zu testen.
`UNIVENTION_LOAD`	Überwacht die Systemlast.
`UNIVENTION_LDAP`	Überwacht den auf Domänencontrollern laufenden LDAP-Server.
`UNIVENTION_NTP`	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 bzw. 120 Sekunden auf, wird der Fehlerzustand erreicht.

Nagios-Dienst	Funktion
UNIVENTION_SMTP	Testet den Mailserver.
UNIVENTION_SSL	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Domänencontroller Master- und Domänencontroller Backup-Systeme geeignet.
UNIVENTION_SWAP	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% bzw. 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer `failed.ldif`-Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD	Testet die Verfügbarkeit des Name Server Cache Dienstes. Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess ein WARNING-Event.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den NetBIOS-Dienst zuständig ist. Läuft kein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_JOINSTATUS	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein CRITICAL-Event ausgelöst, sind nichtaufgerufene Joinskripte vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Domänencontroller Master/Backup). Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft kein `cupsd`-Prozess oder ist die Weboberfläche auf Port 631 ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_DANSGUARDIAN	Überwacht den Webfilter DansGuardian. Läuft kein DansGuardian-Prozess oder ist der DansGuardian-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
UNIVENTION_LIBVIRTD_KVM	Prüft den Status eines KVM-Virtualisierungs-Servers über eine Anfrage an `virsh` und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_LIBVIRTD_XEN	Prüft den Status eines Xen-Virtualisierungs-Servers über eine Abfrage an `virsh` und gibt den Status CRITICAL zurück, wenn die Rückmeldung mehr als zehn Sekunden dauert.
UNIVENTION_UVMMD	Prüft den Status des UCS Virtual Machine Managers über eine Anfrage der verfügbaren Nodes. Können sie nicht aufgelöst werden, wird der Status CRITICAL zurückgegeben.

Für die oben genannten Dienste wurden Standardparameter festgelegt, die auf die Ansprüche der meisten UCS-Installationen zugeschnitten sind. Sollten diese Standardparameter nicht geeignet sein, können sie nachträglich angepasst werden. Dies ist in Abschnitt 15.3.3.1 dokumentiert.

Die folgenden Nagios-Dienste sind erst nach der Installation zusätzlicher Pakete auf dem jeweiligen Nagios-Client verfügbar (siehe Abschnitt 15.3.2):

Nagios-Dienst	**Funktion**
`UNIVENTION_OPSI`	Überwacht den opsi-Daemon. Läuft kein opsi-Prozess oder die opsi-Weboberfläche ist nicht erreichbar, wird der Status CRITICAL zurückgegeben.
`UNIVENTION_SMART_SDA`	Prüft den S.M.A.R.T.-Status der Festplatte `/dev/sda`. Für die Festplatten `sdb`, `sdc` und `sdd` existieren entsprechende Nagios-Dienste.
`UNIVENTION_RAID`	Prüft den Status des Software-RAIDs über `/proc/mdadm` und gibt den Status CRITICAL zurück, sofern eine Festplatte des RAID-Verbunds ausgefallen ist, bzw. den Status WARNING zurück, wenn der Recovery-Vorgang läuft.
`UNIVENTION_ADCONNECTOR`	Prüft den Status des Active Directory Connectors. Läuft kein Connector-Prozess, wird der Status CRITICAL zurückgegeben. Existiert mehr mehr als ein Prozess pro Connector-Instanz gibt es eine WARNING. Treten Rejects auf, gibt es eine WARNING. Kann der AD-Server nicht erreicht werden, tritt ein CRITICAL-Zustand ein. Das Plugin kann auch in Multi-Connector-Instanzen verwendet werden. Dabei muss der Name der Instanz als Parameter übergeben werden.

15.3.3. Konfiguration der Nagios-Überwachung

Feedback

Folgende Einstellungen können in Univention Management Console vorgenommen werden:

- Alle Nagios-Prüfungen, die einem Rechner zugewiesen werden sollen, müssen zuvor registriert werden. Dies erfolgt über *Nagios-Dienst*-Objekte (siehe Abschnitt 15.3.3.1).
- Die Zuweisung, welche Prüfungen an einem Rechner durchgeführt werden sollen und welche Kontaktperson im Fehlerfall benachrichtigt werden soll, erfolgt an den jeweiligen Rechnerobjekten.
- Nagiosprüfungen können zeitlich beschränkt werden, z.B. indem die Prüfung der Druckserver nur werktags von 8h bis 20h durchgeführt wird. Dies erfolgt über *Nagios-Zeitraum*-Objekte, siehe Abschnitt 15.3.3.2.

In der Grundeinstellung werden bereits zahlreiche Prüfungen für jeden Rechner festgelegt, d.h. eine Nagios-Grundkonfiguration wird eingerichtet, ohne dass weitere Anpassungen nötig sind.

15.3.3.1. Konfiguration eines Nagios-Dienstes

Feedback

Ein Nagios-Dienst definiert die Überwachung eines Dienstes. Einem solchen Objekt kann eine beliebige Anzahl an Rechnern zugeordnet werden, so dass durch die einmalige Angabe von zu verwendenden Nagios-Plugins sowie Überprüfungs- und Benachrichtigungsparametern eine Dienstüberprüfung auf den angegebenen Rechnern eingerichtet werden kann.

Nagios-Dienste werden im UMC-Modul *Nagios* mit dem Objekttyp **Nagios-Dienst** verwaltet (siehe auch Abschnitt 4.4). Nagios verfügt über keine LDAP-Schnittstelle für die Monitoring-Konfiguration, stattdessen

werden die Konfigurationsdateien beim Hinzufügen/Entfernen/Bearbeiten eines Nagios-Dienstes durch ein Listener-Modul generiert.

Abbildung 15.4. Konfiguration eines Nagios-Dienstes

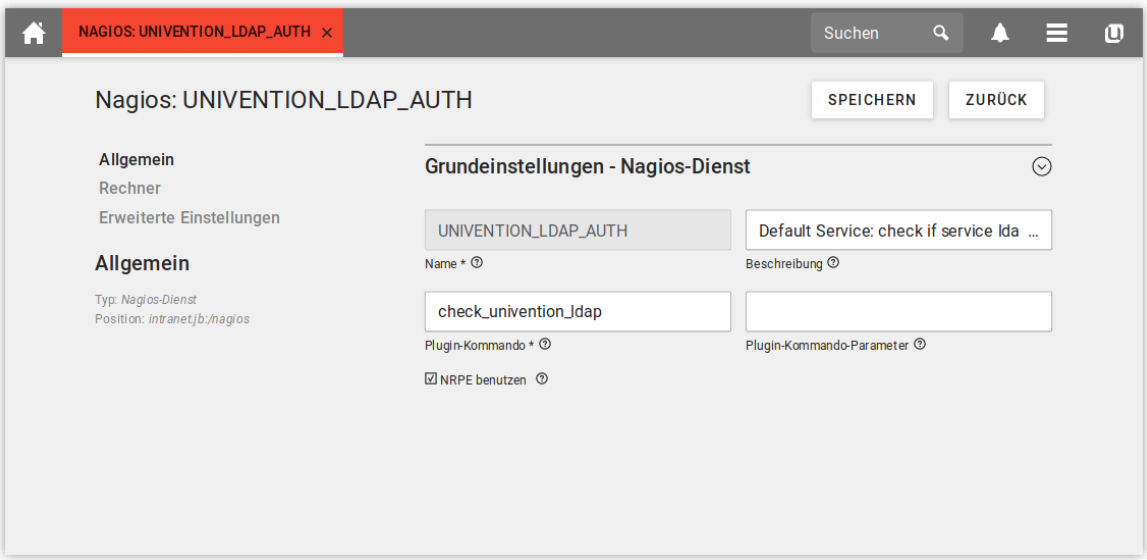


Tabelle 15.1. Reiter 'Allgemein'

Attribut	Beschreibung
Name	Ein eindeutiger Name für den Nagios-Dienst.
Beschreibung	Eine beliebige Beschreibung des Dienstes.
Plugin-Kommando	Das aufzurufende Plugin-Kommando. Jedes Plugin-Kommando legt einen vordefinierten Plugin-Aufruf fest. Diese werden in den Konfigurationsdateien im Verzeichnis `/etc/nagios-plugins/config/` festgelegt, z.B. `check_disk`.
Plugin-Kommando-Parameter	Da nicht alle Parameter der Nagios-Plugins in den Plugin-Kommandos vordefiniert werden können, ist oft die Angabe zusätzlicher Parameter notwendig. Die hier angegeben Parameter werden durch Ausrufungszeichen ("!") getrennt. (z.B. **`20%!10%!/home`**).
NRPE benutzen	Kann der Test eines Dienstes nicht remote ausgeführt werden (z.B. Prüfung des verfügbaren Plattenplatzes auf der Root-Partition), kann über den Nagios Remote Plugin Executor Daemon (NRPED) das Plugin auf einem entfernten UCS-System aufgerufen werden. Dazu muss dort das Paket ***univention-nagios-client*** installiert sein.

Tabelle 15.2. Reiter 'Intervalle' (erweiterte Einstellungen)

Attribut	Beschreibung
Prüfintervall	Das Prüfintervall definiert den zeitlichen Abstand in Minuten zwischen zwei Überprüfungen des Dienstes.
Prüfintervall im Fehlerfall	Sollte die letzte Überprüfung des Dienstes nicht den Zustand *OK* zurückgeliefert haben, verwendet Nagios ein anderes Zeitintervall für die weiteren Überprüfungen. Im Fehlerfall kann so die Überprüfungsfrequenz

Attribut	Beschreibung
	erhöht werden. Wurde der Zustand *OK* wieder erreicht, verwendet Nagios wieder das reguläre Prüfintervall. Der Wert ist in Minuten anzugeben.
Maximale Anzahl der Überprüfungen	Liefert eine Überprüfung einen Nicht-*OK*-Zustand zurück, wird die hier angegebene Anzahl an Überprüfungen abgewartet, bevor die zuständigen Kontaktpersonen benachrichtigt werden. Erreicht der Dienst vor dem Erreichen des hier angegebenen Limits wieder den Zustand *OK*, wird der interne Zähler zurückgesetzt und es findet keine Benachrichtigung statt. **Anmerkung** Die zeitliche Verzögerung einer Benachrichtigung richtet sich sowohl nach der *maximalen Anzahl an Überprüfungen* als auch dem *Prüfintervall im Fehlerfall*. Bei einem *Prüfintervall im Fehlerfall* von zwei Minuten und einer *maximalen Anzahl an Überprüfungen* von 10 findet die erste Benachrichtigung nach 20 Minuten statt.
Prüfzeitraum	Um die Überprüfung eines Dienstes zeitlich einzuschränken, kann ein Prüfzeitraum angegeben werden. Außerhalb dieses Zeitraums finden keine Überprüfungen und somit auch keine Benachrichtigungen statt. Dies kann bei Geräten oder Diensten sinnvoll sein, die z.B. über Nacht deaktiviert werden.

Tabelle 15.3. Reiter 'Benachrichtigungen' (erweiterte Einstellungen)

Attribut	Beschreibung
Benachrichtigungsintervall	Ist der Fehlerfall für einen Dienst eingetreten, werden die Kontaktpersonen in dem hier angegebenen Intervall wiederholt benachrichtigt. Ein Wert von 0 deaktiviert die wiederholte Benachrichtigung. Der Wert ist in Minuten anzugeben. Würde beispielsweise ein Intervall von 240 festgelegt, würde alle vier Stunden eine Benachrichtigung verschickt.
Benachrichtigungszeitraum	Benachrichtigungen an die Kontaktpersonen werden nur in dem hier angegebenen Zeitraum versendet. Wechselt ein Dienst außerhalb des hier angegebenen Zeitraums in einen Nicht-*OK*-Zustand, wird die erste Benachrichtigung erst mit Erreichen des angegebenen Zeitraums versendet, sofern der Nicht-*OK*-Zustand bis dahin erhalten bleibt. **Anmerkung** Benachrichtigungen für Störungen, die außerhalb des angegebenen Zeitraums beginnen und enden, werden nicht nachgeholt.
Benachrichtigen, wenn Zustand WARNING erreicht wird	Konfiguriert, ob bei dem Wechsel des Dienst-Zustands auf *WARNING* (siehe Abschnitt 15.3.1) eine Benachrichtigung verschickt wird.
Benachrichtigen, wenn Zustand CRITICAL erreicht wird	Konfiguriert, ob bei dem Wechsel des Dienst-Zustands auf *CRITICAL* (siehe Abschnitt 15.3.1) eine Benachrichtigung verschickt wird.
Benachrichtigen, wenn Zustand UNREACHABLE erreicht wird	Wenn ein Rechner-Objekt einem anderen Objekt untergeordnet ist (siehe Abschnitt 15.3.3.3), kann bei dem Ausfall eines überordneten Systems der Status nicht mehr abgefragt werden. Mit dieser Option kann konfiguriert werden, ob dann eine Benachrichtigung ausgelöst wird.

Attribut	Beschreibung
Benachrichtigen, wenn Zustand RECOVERED erreicht wird	Konfiguriert, ob bei Korrektur eines Fehler-/Warn-/Nichterreichbarkeitszustands auf den Normalzustand eine Benachrichtigung verschickt wird. Benachrichtigungen werden beim Erreichen des Zustandes "RECOVERED" nur versendet, wenn zuvor auch eine Benachrichtigung für das ursprüngliche Problem ("WARNING"/"CRITICAL"/"UNREACHABLE") versendet wurde.

Tabelle 15.4. Reiter 'Rechner'

Attribut	Beschreibung
Zugeordnete Rechner	Die Dienst-Überprüfung wird für bzw. auf den hier zugeordneten Rechnern durchgeführt.

15.3.3.2. Konfiguration eines Überwachungszeitraums

Nagios-Zeitraum-Objekte werden von Nagios-Diensten verwendet, um Zeiträume festzulegen, in denen Dienstüberprüfungen stattfinden oder Kontaktpersonen benachrichtigt werden sollen. Die Angabe der Zeiträume wird für jeden einzelnen Wochentag getrennt durchgeführt.

Nagios-Dienste werden im UMC-Modul *Nagios* mit dem Objekttyp **Nagios-Zeitraum** verwaltet (siehe auch Abschnitt 4.4).

Nagios verfügt über keine LDAP-Schnittstelle für die Monitoring-Konfiguration, stattdessen werden die Konfigurationsdateien beim Hinzufügen/Entfernen/Bearbeiten eines Nagios-Zeitraums durch ein Listener-Modul generiert.

Bei der Installation werden drei Standard-Zeiträume eingerichtet. Die automatisch angelegten Zeitrahmen können manuell verändert oder gelöscht werden. Sie werden jedoch teilweise von den ebenfalls automatisch angelegten Nagios-Dienst verwendet. Es ist zu beachten, dass das Löschen eines Nagios-Zeitraums nur dann möglich ist, wenn es nicht mehr von Nagios-Diensten verwendet wird:

Nagios:Zeitraum	Funktion
24x7	Dieses Objekt definiert einen Zeitraum, der Montags um 0:00 Uhr beginnt und ohne zwischenzeitliche Unterbrechungen am Sonntag um 24:00 Uhr endet.
WorkHours	Definiert die Zeitrahmen von 8 Uhr bis 16 Uhr jeweils von Montag bis Freitag.
NonWorkHours	Das Gegenstück zum Nagios-Zeitraum *WorkHours*. Deckt die Zeitrahmen von 0 Uhr bis 8 Uhr sowie 16 Uhr bis 24 Uhr jeweils Montag bis Freitag sowie am Samstag und Sonntag jeweils von 0 Uhr bis 24 Uhr ab.

Tabelle 15.5. Reiter 'Allgemein'

Attribut	Beschreibung
Name	Ein eindeutiger Name für den Nagios-Zeitraum.
Beschreibung	Ein beliebiger Beschreibungstext.
Montag - Sonntag	Dieses Feld enthält eine Liste von Zeiträumen. Soll für einen Wochentag kein Zeitraum definiert werden, muss das entsprechende Wochentagsfeld leer bleiben. Die Angabe eines Zeitraums erfordert immer zweistellige Stunden- und Minutenangaben, die durch einen Doppelpunkt getrennt werden. Start- und Endzeitpunkt werden durch einen Bindestrich getrennt. Sollen für einen Wochentag mehrere Zeiträume definiert

Attribut	Beschreibung
	werden, können diese durch ein Komma getrennt in das Textfeld eingetragen werden. Ein ganzer Tag wird durch den Zeitraum *00:00-24:00* repräsentiert, z.B. *08:00-12:00,12:45-17:00*.

15.3.3.3. Zuordnung von Nagios-Prüfungen zu Rechnern

Alle in Univention Management Console verwaltbaren Rechnerobjekte lassen sich mit Nagios überwachen. Nagios-Dienste können nur dann an ein Rechner-Objekt gebunden werden, wenn für diesen eine IP-Adresse sowie ein entsprechender Eintrag für die DNS-Forward-Zone angegeben wurde. Zur Aktivierung der Nagios-Unterstützung muss am betreffenden Rechnerobjekt die Option **Nagios** eingeschaltet werden. Nach der Aktivierung sind zwei zusätzliche Eingabefeldgruppen unter dem Reiter **Erweiterte Einstellungen** verfügbar, die u.a. eine komfortable Zuordnung der Nagios-Dienste ermöglichen.

Abbildung 15.5. Zuweisung von Nagios-Prüfungen zu einem Rechner

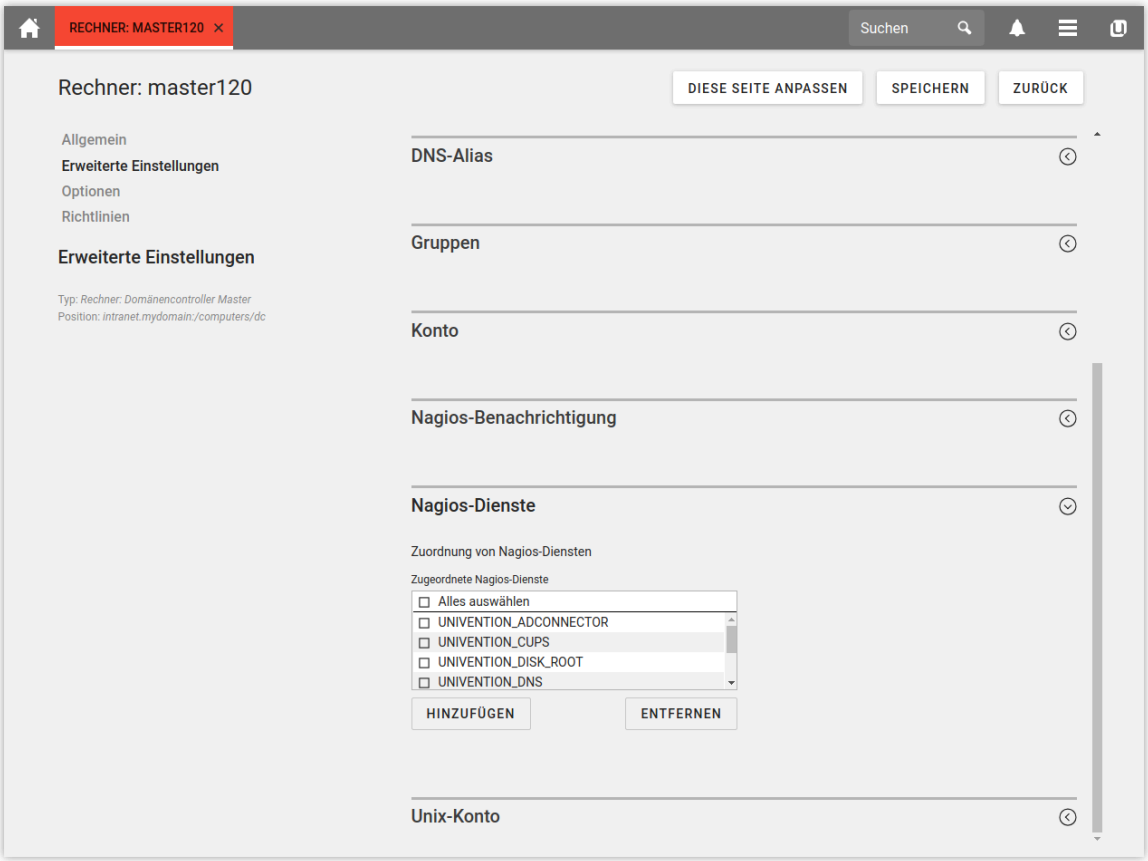


Tabelle 15.6. Karteikarte 'Nagios-Dienste' (erweiterte Einstellungen)

Attribut	Beschreibung
Zugeordnete Nagios-Dienste	Es werden hier alle Nagios-Dienste aufgelistet, die für den aktuellen Rechner geprüft werden sollen. Parallel dazu ist weiterhin die Zuordnung von Rechnern am Nagios-Dienst-Objekt möglich.

Tabelle 15.7. Karteikarte 'Nagios-Benachrichtigung' (erweiterte Einstellungen)

Attribut	Beschreibung
Email-Adressen für Nagios-Benachrichtigungen	Diese Liste enthält die Email-Adressen von Kontaktpersonen, die beim Feststellen einer Störung per Email benachrichtigt werden sollen. Werden hier keine Email-Adressen angegeben, wird der lokale `root`-Benutzer benachrichtigt.
Übergeordnete Rechner	Durch die Angabe von übergeordneten Rechnern können Abhängigkeiten zwischen Rechnern definiert werden. Nagios testet fortlaufend, ob die einzelnen Rechner erreichbar sind. Sollte ein übergeordneter Rechner nicht erreichbar sein, werden keine Benachrichtigungen für Dienststörungen des untergeordneten Rechners versendet. Die angegebenen Abhängigkeiten verwendet Nagios darüber hinaus in der Benutzeroberfläche zur graphischen Darstellung. **Anmerkung** Es dürfen keine Schleifen bei der Angabe der übergeordneten Rechner entstehen. Der Nagios-Server würde in diesem Fall die neue Konfiguration nicht übernehmen bzw. sich nicht starten lassen.

15.3.3.4. Einbindung von manuell erstellten Konfigurationsdateien

Feedback

Sollen zu den durch das Listener-Module erstellten Nagios-Server-Konfigurationsdateien Erweiterungen hinzugefügt werden, können die manuell erstellten Konfigurationsdateien im Verzeichnis `/etc/nagios/conf.local.d/` abgelegt werden. Die hinzugefügten Konfigurationsdateien werden erst nach einem Neustart des Nagios-Servers beachtet.

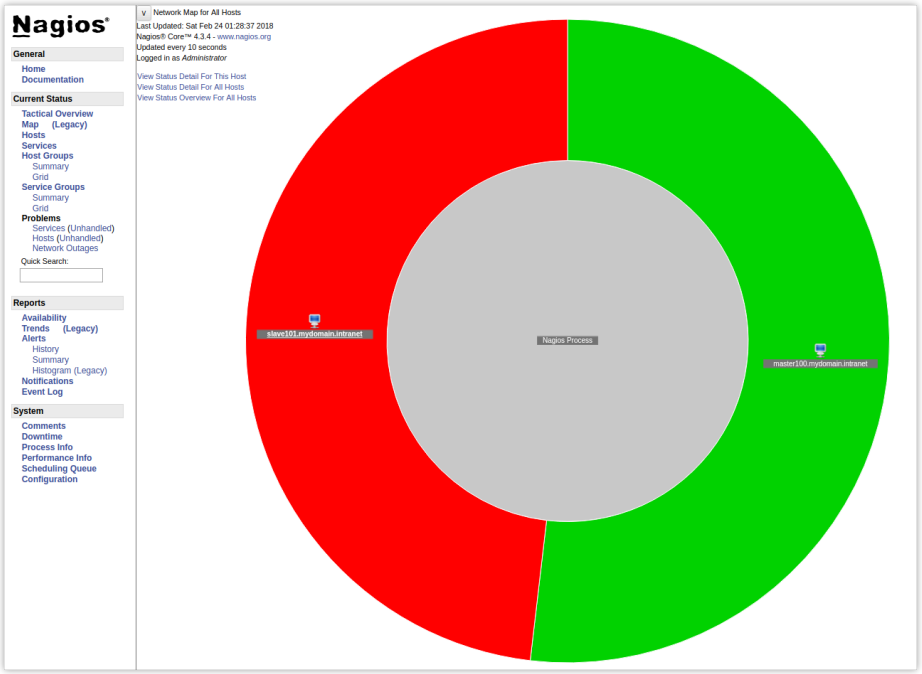
Erweiterungen der NRPE-Konfiguration können im Verzeichnis `/etc/nagios/nrpe.local.d/` abgelegt werden. Änderungen treten erst nach einem Neustart des Nagios NRPE-Daemons in Kraft.

15.3.4. Abfrage des Systemstatus über das Nagios-Webinterface

Feedback

Die Nagios-Oberfläche ist auf der Übersichtswebseite (siehe Abschnitt 4.2) unter **Nagios** verlinkt und kann auch direkt unter `https://`*`SERVERNAME-ODER-IP`*`/nagios/` erreicht werden.

Abbildung 15.6. Nagios-Statusübersicht



Der Zugriff wird in der Standardeinstellung ausschließlich Benutzern der Gruppe `Domain Admins` (z.B. der Benutzer Administrator) gewährt. Es besteht auch die Möglichkeit den Kreis der Anmeldeberechtigten zu erweitern.

15.3.5. Integration eigener Plugins

Feedback

Die in UCS mitgelieferten und vorkonfigurierten Nagios-Plugins können durch selbst geschriebene oder externe Plugins ergänzt werden. Unter https://exchange.nagios.org/ findet sich eine Vielzahl verfügbarer Module.

Dieser Abschnitt beschreibt am Beispiel des Plugins `check_e2fs_next_fsck` die Einbindung eines externen Plugins. Das Plugin prüft, ob ein Filesystem-Check ansteht und liefert eine Warnung wenn dieser sieben oder weniger Tage bevorsteht und einen Fehlerzustand, wenn beim nächsten Reboot ein Filesystem-Check stattfindet.

Je nachdem ob das Plugin über NRPE aufgerufen wird oder nicht, unterscheidet sich die Installation:

- Wird das Plugin über NRPE aufgerufen, muss es auf allen Nagios-Servern und auf allen zu prüfenden Systemen in das Verzeichnis `/usr/lib/nagios/plugins` kopiert werden.
- Benötigt das Plugin keinen lokalen Zugriff, muss es nur auf den Nagios-Server(n) in das Verzeichnis `/usr/lib/nagios/plugins` kopiert werden.

Das Plugin muss als ausführbare Datei markiert sein (`chmod a+x PLUGIN`).

Einige Plugins sind ausschließlich in Perl, Python oder Shell geschrieben und benötigen keine externen Bibliotheken oder Programme. Diese Interpreter sind auf allen UCS-Systemen immer installiert. Wenn das Plugin hingegen externe Programme oder Bibliotheken verwendet, muss sichergestellt werden, das diese auf allen zu prüfenden Systemen (NRPE-Plugin) oder auf den Nagios-Servern (Fern-Prüfung) installiert sind.

Das Nagios-Plugin muss nun registriert werden. Dies erfolgt durch ein Makro im Verzeichnis `/etc/nagios-plugins/config/`. Hierbei kann z.B. eine Datei wie `local.cfg` verwendet werden, in der dann alle

lokal registrierten Plugins eingetragen werden. Das folgende Beispiel registriert das Plugin `check_e2fs_next_fsck`:

```
define command{
   command_name   check_fsck
   command_line   /usr/lib/nagios/plugins/check_e2fs_next_fsck
 }
```

Viele Plugins verwenden auch Parameter, um die Schwellwerte für Warnungen und Fehler zu konfigurieren. Diese werden dann in der *command_line*-Zeile festgelegt. Analog zu dem Plugin selbst muss die Makro-Datei bei Verwendung von NRPE auf alle zu überwachenden Systeme kopiert werden. Die Plugins, Makros und eventuellen Abhängigkeiten können auch in ein Debian-Paket paketiert werden. Weitere Hinweise dazu finden sich in [developer-reference].

Nun muss der Nagios-Dienst neu gestartet werden:

```
/etc/init.d/nagios restart
```

Abschließend muss das neue Plugin noch in Univention Management Console als **Nagios-Dienst** registriert werden, siehe Abschnitt 15.3.3.1. Als **Plugin-Kommando** muss der unter *command_name* in der Makro-Datei registriert Name angegeben werden, in diesem Beispiel `check_fsck` und die Option **NRPE benutzen** aktiviert werden. Der neu registrierte Dienst kann nun einzelnen Systemen zugewiesen werden, siehe Abschnitt 15.3.3.3.

Kapitel 16. Virtualisierung

16.1. Einführung

Feedback

UCS Virtual Machine Manager (UVMM) ist ein Werkzeug für die Verwaltung hybrider Cloud-Umgebungen. Es können in der UCS-Domäne registrierte KVM-Virtualisierungsserver und darauf betriebene virtuelle Maschinen zentral überwacht und administriert werden. Zusätzlich können virtuelle Maschinen in OpenStack- oder EC2-Umgebungen administriert werden. Die Administration erfolgt über das Univention Management Console-Modul *Virtuelle Maschinen*.

In den virtualisierten Systemen kann im Prinzip jedes beliebige Betriebssystem verwendet werden.

16.2. Installation

Feedback

UCS Virtual Machine Manager kann mit der Applikation *UCS Virtual Machine Manager* aus dem Univention App Center installiert werden. Die Applikation kann auch direkt bei der Installation eines neuen UCS Servers ausgewählt werden. Alternativ kann das Softwarepaket ***univention-virtual-machine-manager-daemon*** installiert werden. Weitere Informationen finden sich in Abschnitt 5.6.

Die Verwaltung von OpenStack Cloud-Instanzen ist direkt nach der Installation der Applikation mit dem Univention Management Console Modul *Virtuelle Maschinen (UVMM)* möglich. Für die Verwaltung von virtu-

ellen Maschinen in der Amazon EC2 Cloud muss die Applikation *Amazon EC2 Cloud-Verbindung* installiert werden.

Um vor Ort einen KVM Virtualisierungsserver für die Verwaltung durch UCS Virtual Machine Manager hinzuzufügen, muss die Applikation *KVM Virtualisierungsserver* aus dem Univention App Center auf einem Server der Domäne installiert werden. Die Applikation kann auch direkt bei der Installation eines neuen UCS Servers ausgewählt werden. Alternativ kann das Softwarepaket ***univention-virtual-machine-manager-node-kvm*** installiert werden.

Zum Betrieb von KVM wird zwingend CPU-Virtualisierungunterstützung benötigt. Diese wird von nahezu allen aktuellen x86 CPUs bereitgestellt. Zu Details kann die Webseite des KVM Projekts konsultiert werden: http://www.linux-kvm.org/.

Zusätzlich sollte bei der Installation eines Virtualisierungsservers die Architektur beachtet werden. Nur auf UCS-Systemen, die mit der amd64-Architektur installiert sind, können auch 64-Bit-Systeme virtualisiert werden. Für den Einsatz als Virtualisierungsserver wird die Verwendung eines 64-Bit-Systems (amd64) empfohlen.

16.3. Anlegen von Verbindungen zu Cloud Computing Instanzen

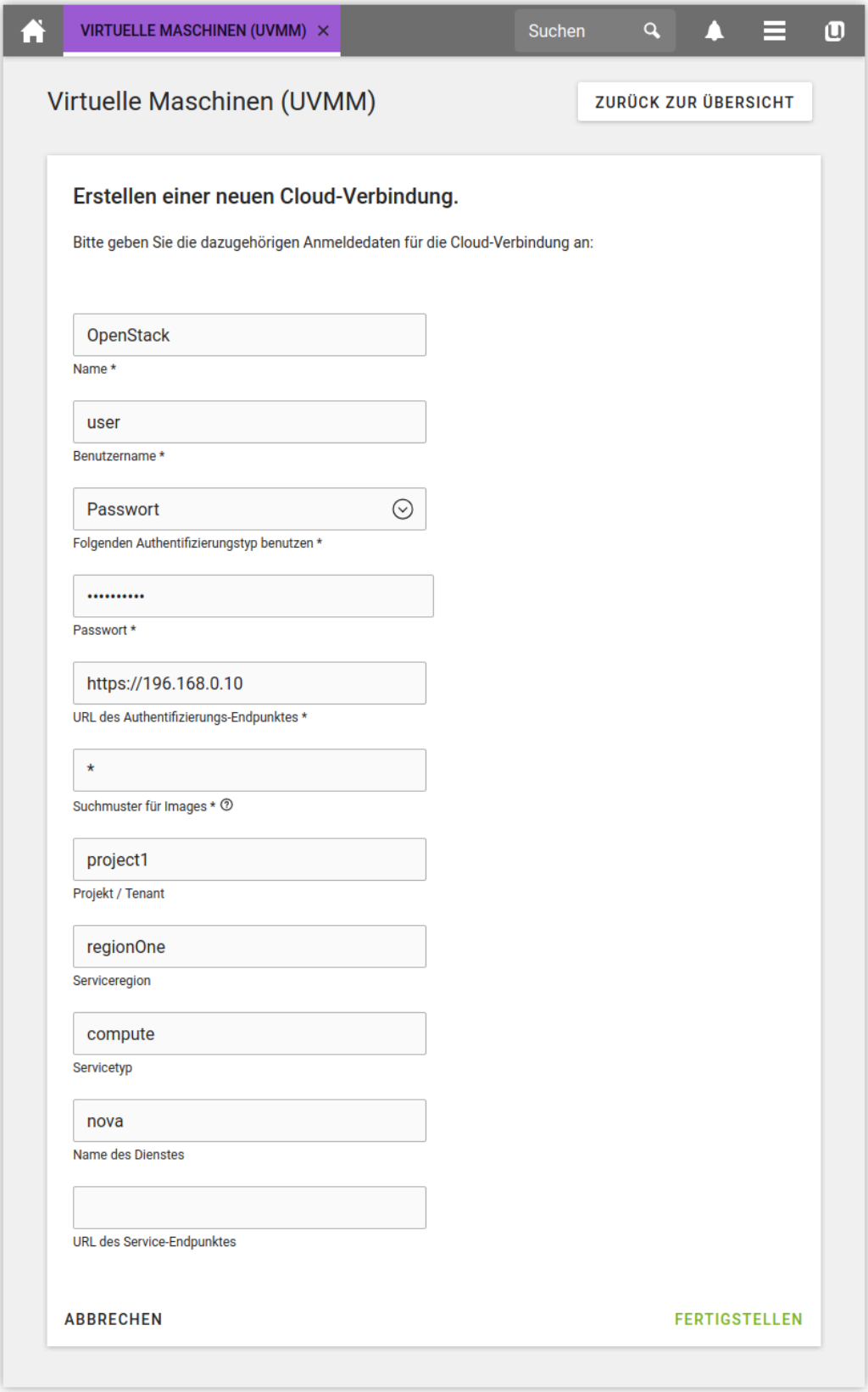
UCS Virtual Machine Manager unterstützt Verbindungen zu OpenStack. Durch die Installation der Applikation *Amazon EC2 Cloud-Verbindung* ist auch das Verwalten von virtuellen Maschinen in der Amazon EC2 Cloud möglich.

Um eine neue Verbindung anzulegen, muss das Univention Management Console Modul *Virtuelle Maschinen (UVMM)* geöffnet werden. Durch einen Klick auf **Erstellen** öffnet sich ein Assistent, in dem der Punkt **Erstellen einer neuen Cloud-Verbindung** gewählt werden muss. Im nun verfügbaren Dropdown Feld kann die Art der Verbindung gewählt werden, mit einem Klick auf **Weiter** startet der Einrichtungsassistent. Sind die Einstellungen getätigt, wird mit einem Klick auf **Fertigstellen** die Verbindung hergestellt. Falls ein Fehler auftritt, wird dieser angezeigt und die Verbindungseinstellungen können korrigiert werden. Wenn die Verbindung erfolgreich hergestellt wurde, wird eine Warteanimation angezeigt, während alle verbindungsspezifischen Informationen der Cloud Verbindung geladen werden. Dies umfasst zum Beispiel die vorhandenen Instanzen und verfügbare Images, um neue Instanzen anlegen zu können.

16.3.1. Anlegen einer OpenStack Verbindung

Feedback

Abbildung 16.1. Anlegen einer Verbindung zu einer OpenStack Instanz



Um eine Verbindung zu einer OpenStack Instanz herzustellen, sind im Einrichtungsassistenten folgende Einstellungen vorzunehmen:

Tabelle 16.1. Felder bei der Einrichtung einer OpenStack Verbindung

Attribut	Beschreibung
Name	Definiert den Namen der Verbindung. Dieser wird später in der Baumansicht des Univention Management Console Moduls angezeigt.
Benutzername	Der Benutzername, der zur Authentifizierung an OpenStack benutzt werden soll.
Folgenden Authentifizierungstyp nutzen	Es kann zwischen zwei Werten gewählt werden. Der zugehörige Wert wird im darunterliegenden Feld eingegeben. Passwort Das zum Benutzernamen gehörige Passwort. API-Schlüssel Der API-Schlüssel, der dem Benutzer Zugriff verschafft.

URL des Authentifizierungs-Endpunktes	Hier ist die URL einzutragen, unter der der Authentifizierungs-Endpunkt der OpenStack Instanz erreichbar ist. Soll eine verschlüsselte Verbindung aufgebaut werden, ist die URL in der Form `https://[...]` anzugeben. Da für die verschlüsselte Verbindung das öffentliche Zertifikat der OpenStack Instanz verwendet wird, muss dieses dem UCS-System, auf dem die Applikation *UCS Virtual Machine Manager* installiert ist, verfügbar gemacht werden. Dazu muss das öffentliche Zertifikat in PEM Kodierung auf dem UCS-Server in das Verzeichnis `/usr/local/share/ca-certificates/` kopiert werden und mit der Endung `.crt` versehen sein. Die folgenden Kommandos konvertieren ein Zertifikat in die korrekte Kodierung und machen das Zertifikat bekannt:
	
	`openssl x509 -in [pfad/zum/openstack-zertifikat] \`
	`-outform pem -out /usr/local/share/ca-certificates/openstack.crt`
	
	`update-ca-certificates`
	
	Das öffentliche Zertifikat des OpenStack Authentifizierungs-Endpunktes ist der Konfiguration der OpenStack Instanz zu entnehmen. Der entsprechende Wert zum Pfad des Zertifikats ist in der `keystone.conf` unter *ca_certs* zu finden.

Suchmuster für Images	Wenn eine neue virtuelle Maschine erstellt werden soll, werden als Quell-Images nur solche Images angezeigt werden, die dem hier konfigurierten Suchmuster entsprechen. Durch den Standardwert "*" (Sternchen) werden alle verfügbaren Images angezeigt.
Projekt / Tenant	Der Projekt- oder Tenantname, der dem Benutzer innerhalb der OpenStack Umgebung zugewiesen ist.
Serviceregion	Der Name der Region, in der der Benutzer arbeiten soll. Der OpenStack Standardwert ist **`regionOne`**.

Attribut	Beschreibung
Servicetyp	Der Typ des Dienstes, unter dem die Cloud Compute Funktionalität zur Verfügung steht. Der Standardwert ist **`compute`**.
Name des Dienstes	Der Name des Dienstes, unter dem die Cloud Compute Funktionalität zur Verfügung steht. Der Standardwert ist **`nova`**.
URL des Service-Endpunktes	Optionaler Wert: Normalerweise wird die URL des Service-Endpunktes automatisch ermittelt, wenn sich der Benutzer an OpenStack anmeldet. Sollte die automatische Ermittlung nicht möglich sein, kann hier die entsprechende URL angegeben werden.

16.3.2. Anlegen einer EC2 Verbindung

Feedback

Um eine Verbindung zu Amazon EC2 herzustellen, sind im Einrichtungsassistenten folgende Einstellungen vorzunehmen:

Tabelle 16.2. Felder bei der Einrichtung einer Amazon EC2 Verbindung

Attribut	Beschreibung
Name	Definiert den Namen der Verbindung. Dieser wird später in der Baumansicht des Univention Management Console Moduls angezeigt.
EC2 Region	Hier wird ausgewählt, zu welcher EC2 Region die Verbindung aufgebaut werden soll. Virtuelle Maschinen sind immer genau einer Region zugeordnet und in anderen Regionen nicht sichtbar. Auch die Auswahl der verfügbaren Images kann sich zwischen den Regionen unterscheiden. Univention UCS Images sind in allen unterstützten Regionen verfügbar.
Access Key ID	Die Zugriffs-ID, die dem Amazon EC2 Konto zugeordnet ist, vergleichbar mit einem Benutzernamen.
Geheimer Zugriffsschlüssel (Secret Access Key)	Der geheime Schlüssel zum Zugriff über das Amazon EC2 Konto, vergleichbar mit einem Passwort.
Suchmuster für AMIs	Imagedateien als Quelle für neue Instanzen werden als AMI bezeichnet. Der hier angegebene Suchfilter beschränkt die Anzeige von auswählbaren AMIs beim anlegen einer neuen virtuellen Instanz. Durch den Wert "*" (Sternchen) werden alle verfügbaren Images angezeigt.

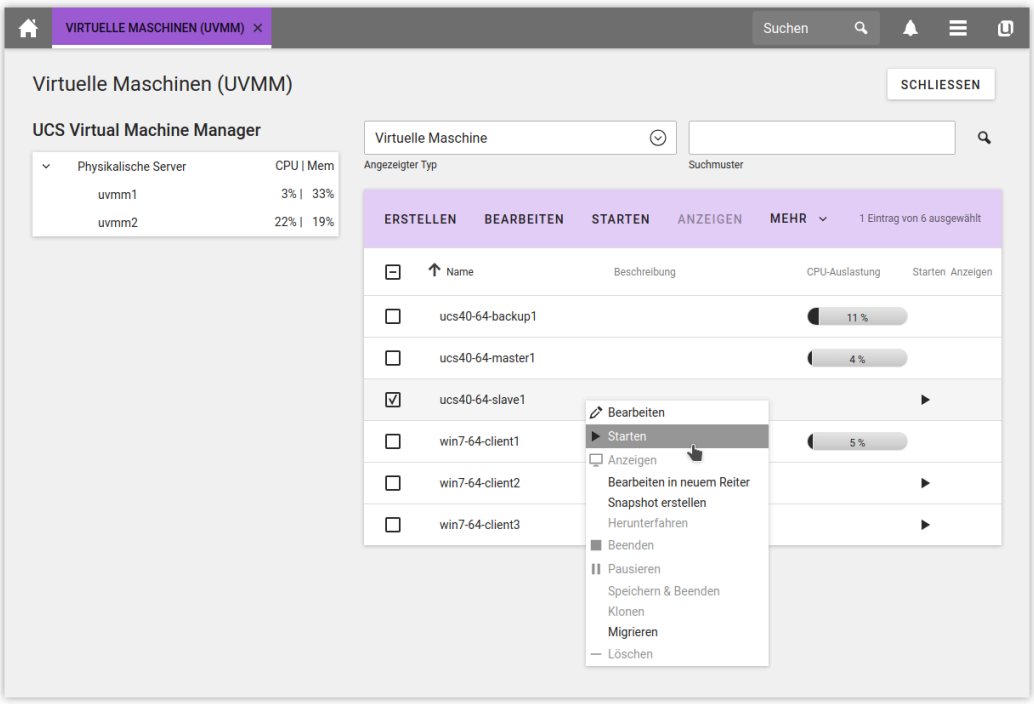
16.4. Verwaltung virtueller Maschinen mit Univention Management Console

Feedback

Die Verwaltung virtueller Maschinen im UCS Virtual Machine Manager erfolgt über das UMC-Modul *Virtuelle Maschinen (UVMM)*. Es bietet die Möglichkeit virtuelle Maschinen anzulegen, zu bearbeiten, zu löschen und den Status zu ändern. Diese Funktionen sind prinzipiell unabhängig von der eingesetzten Virtualisierungstechnik (vor Ort oder cloudbasiert), können sich aber im Detail unterscheiden. Was dabei zu beachten ist, wird in den folgenden Abschnitten zu den Beschreibungen der Funktionen erläutert.

16.4.1. Operationen (Starten/Stoppen/Pausieren/Löschen/Migrieren/Klonen von virtuellen Maschinen)

Abbildung 16.2. Übersicht über die virtuellen Maschinen



Im Hauptdialog des UMC-Moduls wird auf der linken Seite eine Liste angezeigt, die einen Überblick über die vorhandenen Virtualisierungsserver und die konfigurierten Verbindungen zu Cloud Computing Systemen anzeigt. In der rechten Bildschirmhälfte werden alle virtuellen Maschinen aufgeführt. Klickt man auf den Namen eines Virtualisierungs-Servers oder einer Cloud Computing Verbindung, werden nur noch die zugehörigen virtuellen Maschinen dargestellt. Über die Suchmaske kann auch nach einzelnen virtuellen Maschinen gesucht werden.

In der Übersichtsliste der virtuellen Maschinen kann anhand des Rechner-Icons erkannt werden, in welchem Status sich diese befindet, d.h. ob sie läuft (Rechnersymbol mit grünem Pfeil), gespeichert(Suspend) (Rechnersymbol mit gelben Längsstrichen) oder angehalten (Rechner ohne Zusatzsymbol) ist. Virtuelle Maschinen in Cloud Computing Umgebungen können zusätzlich als gelöscht (Rechner mit rotem Kreuz) oder als ausstehend (Rechner mit Sanduhr) dargestellt werden.

Mit dem Icon, das einen Pfeil nach rechts darstellt, kann eine virtuelle Maschine gestartet werden.

Auf laufende Maschinen auf KVM-Virtualisierungsservern kann - sofern konfiguriert - über das VNC-Protokoll zugegriffen werden. Das Icon mit der stilisierten Leinwand öffnet eine Verbindung über noVNC, einen HTML5-basierten VNC-Client. Für den Zugriff können auch beliebige andere VNC-Clients verwendet werden; der VNC-Zugriffsport wird in einem Tooltip über dem Rechnernamen angezeigt.

Mit dem Auswahlfeld **mehr** können weitere Aktionen durchgeführt werden. Folgende Operationen stehen auf laufenden Maschinen zur Verfügung, die auf vor Ort laufenden KVM-Virtualisierungsservern betrieben werden:

Beenden

: schaltet die Maschine aus. Dabei ist zu beachten, dass dabei das Betriebssystem der virtuellen Maschine vorher nicht runtergefahren wird, d.h. es mit dem Ausschalten eines Rechners zu vergleichen.

Pausieren

weist der Maschine keine weitere CPU-Zeit zu. Dadurch wird weiterhin der Arbeitsspeicher auf dem physikalischen Rechner belegt, die Maschine an sich aber angehalten.

Speichern und beenden

sichert den Inhalt des Arbeitsspeichers der Maschine auf Festplattenspeicher und weist der Maschine keine weitere CPU-Zeit zu, d.h. gegenüber **Pausieren** wird außerdem noch der Arbeitsspeicher freigegeben.

Migrieren

verschiebt die virtuelle Maschinen auf einen anderen Virtualisierungsserver. Weitere Hinweise finden sich in Abschnitt 16.5.7.

Folgende Operationen stehen auf gespeicherten oder ausgeschalteten Maschinen zur Verfügung:

Löschen

Nicht mehr benötigte virtuelle Maschinen können mitsamt ihrer Festplatten und ISO-Images gelöscht werden. Die zu löschenden Image-Dateien können dabei in einer Liste ausgewählt werden. Es ist zu beachten, dass ISO-Images und möglicherweise auch Festplatten-Images ggf. noch von anderen Maschinen verwendet werden.

Migrieren

verschiebt die virtuelle Maschinen auf einen anderen Virtualisierungs-Server. Weitere Hinweise finden sich in Abschnitt 16.5.7

Klonen

erzeugt eine Kopie der aktuellen VM. Die Kopie wird dabei mit einem frei wählbaren, neuen Namen versehen. Die MAC-Adressen von Netzwerk-Interfaces werden übernommen, können alternativ aber auch zufällig neu generiert werden. Eingebundene CD- und DVD-Laufwerke der Quell-VM werden standardmäßig in den Klon übernommen, während Festplatten kopiert werden, sofern der Speicherbereich das Kopieren unterstützt. Sicherungspunkte werden nicht übernommen!

Folgende Operationen stehen für virtuelle Maschinen zur Verfügung, die in cloudbasierten Umgebungen betrieben werden:

Neu starten (hard)

Startet die virtuelle Maschine neu, als wäre der Reset-Knopf betätigt worden. Hierbei kann es zu Datenverlust kommen.

Neu starten (soft)

Sendet ein ACPI-Reset Event an die virtuelle Maschine. Wenn das Betriebssystem der virtuellen Maschine dies korrekt interpretiert, wird ein geordneter Neustart durchgeführt.

Herunterfahren (soft)

Sendet ein ACPI-Shutdown Event an die virtuelle Maschine Wenn das Betriebssystem der virtuellen Maschine dies korrekt interpretiert, wird es geordnet heruntergefahren und ausgeschaltet.

Pausieren

Weist der Maschine keine weitere CPU-Zeit zu. Dadurch wird weiterhin der Arbeitsspeicher auf dem physikalischen Rechner belegt, die Maschine an sich aber angehalten.

Speichern und beenden

Sichert den Inhalt des Arbeitsspeichers der Maschine auf Festplattenspeicher und weist der Maschine keine weitere CPU-Zeit zu, d.h. gegenüber **Pausieren** wird außerdem noch der Arbeitsspeicher freigegeben.

Löschen

Schaltet die virtuelle Maschine aus und löscht alle dazugehörigen Daten unwiderruflich.

16.4.2. Erstellen einer virtuellen Maschine über eine Cloud Verbindung

Feedback

Virtuelle Maschinen in cloudbasierten Virtualisierungsumgebungen können in UVMM durch Klick auf **Erstellen** mit einem Assistenten in wenigen Schritten erstellt werden.

In der Eingabemaske **Erstellen einer virtuellen Maschine oder einer Cloud-Verbindung** kann ausgewählt werden, auf über welche Cloud Verbindung die virtuelle Maschine angelegt werden soll. Nach der Auswahl einer Verbindung und einem Klick auf **Weiter**, gelangt man zum Assistenten zum anlegen einer neuen virtuellen Maschine. Nach dem Festlegen der Parameter wird die neue virtuelle Maschine nach einem Klick auf **Fertigstellen** angelegt.

Tabelle 16.3. Erstellen einer virtuellen Maschine über eine Cloud Verbindung

Attribut	**Beschreibung**
Name	Definiert den Namen der virtuellen Maschine.
Auswahl des Quell-Images / Quell-AMIs	Der initiale Zustand einer virtuellen Maschine beim anlegen wird über ein Quell-Image (OpenStack) oder Quell-AMI (EC2) festgelegt. Ein solches Image enthält meist ein vorbereitetes Betriebssystem, dass vom Nutzer nach dem Start individualisiert werden kann. Es können beliebig viele virtuelle Maschinen aus einem Quell-Image erstellt werden.
Wahl der Instanzgröße	Einer virtuellen Maschine wird beim anlegen eine Instanzgröße zugeordnet. Diese setzt sich zusammen aus verfügbarem Arbeitsspeicher und der Größe des verfügbaren Festplattenspeichers. Beim Anlegen einer virtuellen Maschine in einer OpenStack Umgebung wird über die Größe auch die Anzahl der CPU-Kerne bestimmt.
Auswahl eines Schlüsselpaares	Um den sicheren Zugriff auf die virtuelle Maschine per ssh zu ermöglichen, wird der Maschine beim ersten Start ein ssh-Schlüssel zur Konfiguration des rootaccounts hinzugefügt. Mit diesem Schlüssel ist der ssh Zugriff auf die Maschine ohne Passwort möglich. Dazu muss der Zugriff auf den privaten Schlüsselteil des Schlüsselpaares bestehen. Der Zugriff auf die Instanz kann z.b. mit folgendem Aufruf erfolgen, wenn die Instanz läuft: `ssh -i [pfad/zum/privaten/schluessel] root@[ip-adresse-der-instanz]`
Konfigurieren einer Sicherheitsgruppe	Diese Einstellung konfiguriert, welche Sicherheitsgruppe für die neue virtuelle Maschine gesetzt wird. Eine Sicherheitsgruppe bestimmt, welche TCP-Ports für den externen Zugriff auf eine virtuelle Maschine freigegeben werden.

16.4.3. Bearbeiten einer virtuellen Maschine über eine Cloud Verbindung

Feedback

Durch Auswahl einer virtuellen Maschine und einem Klick auf **Bearbeiten** können auf einer separaten Seite die konfigurierten Einstellungen der virtuellen Maschine eingesehen werden. Insbesondere die IP-Adresse, über die die virtuelle Maschine erreichbar ist, ist hier einsehbar.

16.4.4. Erstellen einer virtuellen Maschine mit KVM

Feedback

Virtuelle Maschinen auf vor Ort betriebenen KVM Virtualisierungsservern können in UVMM durch einen Klick auf **Erstellen** mit einem Assistenten in wenigen Schritten erstellt werden.

In der Eingabemaske **Erstellen einer virtuellen Maschine oder einer Cloud-Verbindung** kann ausgewählt werden, auf welchem Virtualisierungs-Server die virtuelle Maschine angelegt werden soll. Wird hier ein KVM Virtualisierungsserver ausgewählt und **Weiter** gewählt, gelangt man zur Auswahl des Maschinenprofils. Mit der Auswahl des **Profil**s werden einige grundlegende Einstellungen für die virtuelle Maschine vorgegeben werden (siehe Abschnitt 16.6).

Die virtuelle Maschine wird nun mit einem **Namen** und einer optionalen **Beschreibung** versehen. Anschließend wird der **Arbeitsspeicher** und die **Anzahl der CPUs** zugewiesen. Die Option **Direktzugriff aktivieren** legt fest, ob auf die Maschine über das VNC-Protokoll zugegriffen werden kann. Dies ist im Regelfall erforderlich für die initiale Betriebssysteminstallation.

Nun werden die Laufwerke der virtuellen Maschine konfiguriert. Die Verwaltung von Laufwerken ist in Abschnitt 16.5.1 dokumentiert.

Ein Klick auf **Fertigstellen** schließt das Anlegen der virtuellen Maschine ab.

16.4.5. Bearbeiten der Einstellungen einer virtuellen Maschine

Feedback

In der Übersichtsliste der virtuellen Maschinen kann durch Klick auf das Icon mit dem stilisierten Stift eine virtuelle Maschine bearbeitet werden.

Abbildung 16.3. Bearbeiten der Laufwerkseinstellung eines DVD-Laufwerks

Die meisten Einstellungen einer virtuellen Maschine können nur verändert werden, wenn sie ausgeschaltet ist.

Tabelle 16.4. Reiter 'Allgemein'

Attribut	Beschreibung
Name	Definiert den Namen der virtuellen Maschine. Dieser muss nicht mit dem Namen des Rechners im LDAP-Verzeichnis übereinstimmen.
Betriebssystem	Das in der virtuellen Maschine installierte Betriebssystem. Hier kann ein beliebiger Text eingetragen werden.
Kontakt	Definiert den Ansprechpartner für die virtuelle Maschine. Wird hier eine E-Mail-Adresse angegeben, so kann über die dann erscheinende Verknüpfung ein externes E-Mail-Programm aufgerufen werden.
Beschreibung	Hier kann eine beliebige Beschreibung hinterlegt werden, z.B. zur Funktion der virtuellen Maschine (*Mailserver*) oder zu deren Zustand. Die Beschreibung wird in der Übersicht der virtuellen Maschinen als Mouseover angezeigt.

Der Reiter **Geräte** erlaubt die Konfiguration der Laufwerke und Netzwerkschnittstellen. Eine Einführung zu den unterstützen Geräten, Speicherformaten und Speicherbereichen findet sich Abschnitt 16.5.1, zu den unterstützen Netzwerkkarten-Einstellungen in Abschnitt 16.5.4.

Unter **Laufwerke** sind alle existierenden Laufwerke aufgeführt, die dabei verwendeten Image-Dateien, deren Größe und die zugeordneten Speicherbereiche. Mit dem Klick auf das stilisierte Minus-Zeichen kann das Laufwerk ausgehängt werden (die Image-Datei kann optional mitgelöscht werden).

Mit **Bearbeiten** können Einstellungen nachträglich angepasst werden. Mit **Paravirtualisiertes Laufwerk** lässt sich festlegen, ob der Zugriff auf das Laufwerk paravirtualisiert erfolgen soll. Diese Einstellung sollte für eine virtuelle Maschine mit bereits installiertem Betriebssystem nach Möglichkeit nicht mehr verändert werden, da dann ggf. Partitionen nicht mehr angesprochen werden können.

Werden zu einer existierenden Maschine weitere Laufwerke oder Netzwerkkarten hinzugefügt, wird die Verwendung von Paravirtualisierung anhand des referenzierten Profils oder aus den Eigenschaften der virtuellen Maschine über Heuristiken ermittelt.

Mit **Laufwerk hinzufügen** kann ein weiteres Laufwerk hinzugefügt werden.

Unter **Netzwerkschnittstellen** findet sich eine Liste aller Netzwerkkarten, die durch Anklicken der beiden Schaltflächen bearbeitet bzw. gelöscht werden können. Außerdem können über **Hinzufügen einer Netzwerkschnittstelle** neue Netzwerkkarten hinzugefügt werden.

Im Reiter **Sicherungspunkte** findet sich eine Liste aller bestehenden Sicherungspunkte. Eine Einführung zu Sicherungspunkten findet sich in Abschnitt 16.5.6. Mit **Wiederherstellen** kann auf einen alten Stand zurückgekehrt werden.

Achtung

Durch das Zurücksetzen auf einen alten Stand geht der aktuelle Stand verloren. Es spricht aber nichts dagegen, den aktuellen Stand zuvor in einem weiteren Sicherungspunkt zu sichern.

Mit einem Klick auf das stilisierte Minus-Zeichen kann ein Sicherungspunkt entfernt werden. Der aktuelle Stand der Maschine bleibt davon unberührt.

Mit **Neuen Sicherungspunkt erstellen** kann ein Sicherungspunkt unter einem frei wählbaren Namen erstellt werden, z.B. *DC Master vor Update auf UCS 4.0-1*. Zusätzlich wird der Zeitpunkt abgespeichert, zu dem der Sicherungspunkt erstellt wird.

Im Reiter **Zielrechner für Migration** können die Hostsysteme konfiguriert werden, auf die die virtuelle Maschine migriert werden kann. Weitere Hinweise zur Migration finden sich in Abschnitt 16.5.7.

Tabelle 16.5. Reiter 'Erweitert'

Attribut	**Beschreibung**
Architektur	Legt die Architektur der emulierten Hardware fest. Dabei ist zu beachten, dass nur auf Virtualisierungsservern der Architektur amd64 virtuelle 64-Bit-Maschinen angelegt werden können. Diese Option wird auf i386-Systemen nicht angezeigt.
Anzahl der CPUs	Definiert wie viele CPU-Sockel der virtuellen Maschine zugeteilt werden. Die Anzahl der NUMA-Knoten, Cores und CPU-Threads ist derzeit nicht konfigurierbar.
CPU Modell	Das Modell der CPU für die virtuelle Maschine. Die Liste der nutzbaren Modelle hängt vom konkreten Hostsystem ab. Eine vollständige Liste der verfügbaren Modelle erhält man auf der Kommandozeile über `virsh domcapabilities`. Weitere Informationen - insbesondere zur Live-Migration - siehe Abschnitt 16.5.7.2.
Speicher	Die Größe des zugewiesenen Arbeitsspeichers.
RTC Referenz	Bei vollvirtualisierten Systemen wird pro virtueller Maschine eine Rechneruhr emuliert (paravirtualisierte Systeme greifen direkt auf die Uhr des Virtualisierungsservers zurück). Diese Option speichert die Zeitzone der emulierten Uhr; sie kann entweder die **Koordinierte Weltzeit (UTC)** oder die **lokalen Zeitzone** verwenden. Für Linux-Systeme wird die Verwendung von UTC empfohlen, für Microsoft Windows-Systeme die Verwendung der lokalen Zeitzone.
Bootreihenfolge	Legt bei vollvirtualisierten Maschinen die Reihenfolge fest, in der das emulierte BIOS der virtuellen Maschine die Laufwerke nach bootbaren Medien durchsucht. Bei paravirtualisierten Maschinen kann lediglich eine Festplatte ausgewählt werden, aus der der Kernel benutzt werden soll.
Hyper-V Enlightenment	Erlaubt es Gastsystemen wie `Microsoft Windows` effizienter als virtuelle Maschine zu laufen.
VM immer mit Host starten	Definiert, ob die virtuelle Maschine jedesmal automatisch gestartet werden soll, wenn das Hostsystem selber startet.
Direktzugriff (VNC)	Definiert, ob der VNC-Zugriff zur virtuellen Maschine aktiviert werden soll. Ist die Option aktiv, kann über das UMC-Modul durch einen HTML5-basierten VNC-Client - oder einen beliebigen anderen Client - direkt auf die virtuelle Maschine zugegriffen werden. Die VNC-URL wird in einem Tooltip angezeigt.
Global verfügbar	Erlaubt den VNC-Direktzugriff auch von anderen Systemen als dem Virtualisierungsserver.
VNC Passwort	Setzt ein Passwort für die VNC-Verbindung.
Tastaturlayout	Legt das Layout für die Tastatur in der VNC-Sitzung fest.

16.5. KVM-bezogene Merkmale von UVMM

Feedback

16.5.1. Image-Dateien virtueller Maschinen

Feedback

Werden virtuelle Festplatten zu einer Maschine hinzugefügt, werden im Regelfall für die Datenhaltung *Image-Dateien* verwendet. Eine Image-Datei kann entweder neu erzeugt werden oder eine bereits vorhandene Image-Datei einer virtuellen Maschine zugewiesen werden. Alternativ kann einer virtuellen Maschine auch ein natives Block-Device (Festplattenpartition, Logical-Volume, iSCSI-Volume) zugewiesen werden. Die direkte Verwendung von Block-Devices bietet Performance-Vorteile und ist weniger anfällig gegen Rechnerabstürze.

Auf KVM-Systemen können Image-Dateien in zwei Formaten verwaltet werden: Standardmäßig werden sie im **Erweiterten Format (qcow2)** angelegt. Dieses unterstützt Copy-on-write, was bedeutet, dass eine Änderung nicht das Original überschreibt, sondern die neue Version stattdessen an einer anderen Position abgelegt wird. Die interne Referenzierung wird dann so aktualisiert, dass wahlweise sowohl die Originalversion als auch die neue Version zugreifbar sind. Nur bei Verwendung von Festplatten-Images im **Erweiterten Format** können Sicherungspunkte erstellt werden. Alternativ kann auch im **Einfachen Format (raw)** auf ein Festplatten-Image zugegriffen werden.

Zur Beschleunigung von Zugriffen auf Speichermedien verwenden Betriebssysteme einen sogenannten *Page Cache*. Wenn auf Daten zugegriffen wird, die vorher schon von einer Festplatte gelesen wurden und diese im Cache noch vorhanden sind, entfällt ein vergleichsweise langsamer Zugriff auf das Speichermedium und die Anfrage wird aus dem Page Cache bedient.

Schreibzugriffe werden in der Regel auch nicht unmittelbar auf die Festplatte geschrieben, sondern oft gebündelt und dadurch effizienter geschrieben. Dies birgt allerdings die Gefahr eines Datenverlustes, wenn z.B. ein System abstürzt oder die Stromversorgung unterbrochen wird: Die Daten, die bis dahin nur im Schreibcache vorgehalten wurden und noch nicht auf das Speichermedium synchronisiert wurden, sind dann verloren. Bei modernen Betriebssystemen wird in der Regel dafür gesorgt, dass anstehende Schreibänderungen nach maximal einigen Sekunden auf die Festplatte geschrieben werden.

Um zu vermeiden, das Daten sowohl im Page Cache des Wirtsystems als auch des Gastssystems doppelt vorgehalten werden, können mit der Option **Caching** verschiedene Cache-Strategien konfiguriert werden, die die Verwendung des Page Caches des Wirtsystems beeinflussen:

- Die Grundeinstellung seit UCS-3.1 ist **none**: Dabei greift KVM direkt auf die Festplatte zu und umgeht den Page Cache auf dem Virtualisierungsserver. Lesezugriffe werden jedesmal direkt von der Festplatte beantwortet und Schreibzugriffe direkt an die Festplatte durchgereicht.

- Mit der Strategie **write-through** wird der Page Cache auf dem Virtualisierungsserver benutzt, jedoch wird jeder Schreibzugriff auch direkt an das Speichermedium durchgereicht. Auf Virtualisierungsservern mit viel freiem Hauptspeicher können Lesezugriffe gegenüber **none** effizienter sein. I.d.R. wirkt sich das doppelte Caching aber eher negativ auf die Gesamtperformance aus [1].

- Wird die Strategie **write-back** verwendet, wird der Page Cache des Hosts sowohl für Lese- als auch für Schreibzugriffe genutzt. Schreibzugriffe werden zunächst nur im Page Cache durchgeführt, bevor dieser dann irgendwann später erst auf die Festplatte geschrieben wird. Ein Crash des Hostsystems kann dadurch zu Datenverlusten führen.

- Mit der Strategie **unsafe** werden Synchronisationsanforderungen ignoriert, die vom Gastsystem gesendet werden, um explizit das Schreiben ausstehender Daten auf das Speichermedium zu erzwingen. Dies erhöht gegenüber **write-back** abermals die Performance, führt aber bei einem Crash des Hostsystems zu Daten-

[1] Es empfiehlt sich eher, den freien Speicher den VMs direkt zur Verfügung zu stellen, so dass diese diesen zusätzlichen Speicher selbst effizienter nutzen können, u.a. auch zum Cachen.

verlust. Diese Variante ist nur für Testsysteme oder vergleichbare Installationen sinnvoll, in denen ein Datenverlust durch einen Absturz des Hostsystem verschmerzbar ist.

- Die Strategie **directsync** entspricht **none**, nur dass hier nach jedem Schreibzugriff nochmals explizit eine Synchronisation erzwungen wird.

- Die Option **Hypervisor-Standard** ist abhängig von der UCS-Version und der KVM-Version, mit der ein Gastsystem installiert wurde: Ursprünglich war der Standardwert bis UCS 3.0 implizit **write-through**, aber mit UCS 3.1 wurde KVM so modifiziert, dass für alte VMs jetzt statt dessen **none** verwendet wird. Bei mit UCS 3.1 neu angelegten VMs entspricht der Standardwert wieder implizit **write-through**, allerdings werden neue VMs explizit mit **none** angelegt.

Wenn eine Live-Migration virtueller Maschinen zwischen verschiedenen Virtualisierungsservern erfolgen soll, muss der Speicherbereich auf einem System abgelegt werden, auf das alle Virtualisierungsserver zugreifen können (z.B. eine NFS-Freigabe oder ein iSCSI-Target). Dies wird in Abschnitt 16.5.2.1 beschrieben.

Festplatten-Images werden mit der angegebenen Größe als Sparse-Datei angelegt, d.h. diese Dateien wachsen erst bei der Verwendung bis zur maximal angegebenen Größe und benötigen initial nur geringen Speicherplatz. Da hierbei die Gefahr besteht, dass dadurch im laufenden Betrieb der Speicherplatz erschöpft ist, sollte eine Nagios-Überwachung integriert werden, siehe Abschnitt 15.3.

Festplatten-Images sollten nach Möglichkeit paravirtualisiert angesprochen werden. Bei UCS-Systemen, die virtualisiert unter KVM installiert werden, wird durch die Auswahl des UCS-Profils automatisch ein paravirtualisierter Zugriff aktiviert. Die Konfiguration von Microsoft Windows-Systemen ist in Abschnitt 16.5.5 dokumentiert.

16.5.2. Speicherbereiche

Feedback

Image-Dateien werden in sogenannten Speicherbereichen abgelegt. Diese können entweder lokal auf dem Virtualisierungsserver oder auf einer Freigabe abgelegt werden. Die Anbindung eines Speicherbereichs über iSCSI ist in [ext-doc-uvmm] beschrieben.

16.5.2.1. Zugriff auf den Standard-Speicherbereich über eine Freigabe

Feedback

Jeder Virtualisierungsserver stellt in der Voreinstellung einen Speicherbereich mit dem Namen *default* zur Verfügung. Dieser liegt auf den Virtualisierungsservern unterhalb des Verzeichnisses `/var/lib/libvirt/images/`.

Um einen einfachen Zugriff auf den Speicherbereich zu ermöglichen, kann eine Freigabe für das Verzeichnis `/var/lib/libvirt/images/` eingerichtet werden. Dazu muss im UMC-Modul **Freigaben** eine Freigabe mit den folgenden Optionen angelegt werden. Auf die Freigabe kann dann anschließend einfach von Windows-Clients über eine CIFS-Netzwerkfreigabe (oder auch über einen NFS-Mount) zugegriffen werden.

- Allgemein/Grundeinstellungen
  - Name: **`UVMM-Pool`**
  - Server: Der Rechnername des UVMM-Servers
  - Pfad: **`/var/lib/libvirt/images`**
  - Verzeichnis-Besitzer, Verzeichnis-Gruppe und Verzeichnismodus können beibehalten werden
- Erweiterte Einstellungen/Samba-Rechte
  - Gültige Benutzer oder Gruppen: **`Administrator`**

Die Image-Dateien einer virtuellen Festplatten enthalten sämtliche Nutzdaten des virtualisierten Systems! Die Option **Gültige Benutzer oder Gruppen** stellt sicher, dass unabhängig von den Dateisystemberechtigungen nur der Administrator-Benutzer auf die Freigabe zugreifen kann.

16.5.2.2. Hinzufügen eines Speicherbereichs

Feedback

Ein weiterer Speicherbereich kann nicht über Univention Management Console angelegt werden. Stattdessen muss eine Anmeldung als Benutzer `root` auf einen Virtualisierungs-Server erfolgen. Die folgenden Schritte sind dafür nötig:

- Das Verzeichnis, in dem die Daten des Speicherbereichs abgelegt werden sollen, muss angelegt werden, in diesem Beispiel `/mnt/storage/`.
- Mit dem folgenden Befehl wird der neue Speicherbereich *Testpool* erstellt:

```
virsh pool-define-as Testpool dir - - - - "/mnt/storage"
```

- Die von UVMM verwendete Bibliothek libvirt unterscheidet zwischen aktiven und inaktiven Speicherbereichen. Um den Speicherbereich direkt verwenden zu können, muss er aktiviert werden:

```
virsh pool-start Testpool
```

  Der folgende Befehl stellt sicher, dass der Pool automatisch beim nächsten Systemstart aktiviert wird:

```
virsh pool-autostart Testpool
```

16.5.2.3. Verschieben des default-Speicherbereichs

Feedback

Um den unterliegenden Dateipfad eines Speicherbereichs nachträglich zu ändern, muss eine Anmeldung als Benutzer `root` auf dem Virtualisierungs-Server erfolgen. Die folgenden Schritte sind dafür nötig:

- Die Univention Configuration Registry-Variable `uvmm/pool/default/path` muss auf das neue Verzeichnis geändert werden.
- Die folgenden Befehle entfernen den alten Speicherbereich; durch einen Neustart des UVMM wird der Speicherbereich unter dem neuen Pfad angelegt:

```
virsh pool-destroy default
virsh pool-undefine default
invoke-rc.d univention-virtual-machine-manager-daemon restart
invoke-rc.d univention-virtual-machine-manager-node-common restart
```

16.5.3. CD/DVD/Disketten-Laufwerke in virtuellen Maschinen

Feedback

CD-/DVD-ROM-/Disketten-Laufwerke können auf zwei Arten eingebunden werden:

- Aus einem Speicherbereich kann ein ISO-Image zugewiesen werden. Wurde kein zusätzlicher Speicherbereich angelegt, werden die ISO-Dateien im Speicherbereich *default* aus dem Verzeichnis `/var/lib/libvirt/images/` ausgelesen.
- Alternativ kann auch ein physisches Laufwerk des Virtualisierungsservers mit der virtuellen Maschine verbunden werden.

Ein Diskettenlaufwerk kann einer virtuellen Maschine ebenfalls über ein Image (im `VFD`-Format) oder durch Durchreichung eines physischen Laufwerks bereitgestellt werden.

Werden Laufwerke für eine neu zu installierende Maschine definiert, muss sichergestellt werden, dass von dem CD-ROM-Laufwerk gebootet wird. Das UVMM-Profil (siehe Abschnitt 16.6) gibt die Bootreihenfolge

für vollvirtualisierte Maschinen bereits vor. Bei paravirtualisierten Maschinen wird es durch die Reihenfolge bei der Definition der Laufwerke festgelegt und kann auch nachträglich in den Einstellungen angepasst werden.

16.5.4. Netzwerk-Karten virtueller Maschinen

Feedback

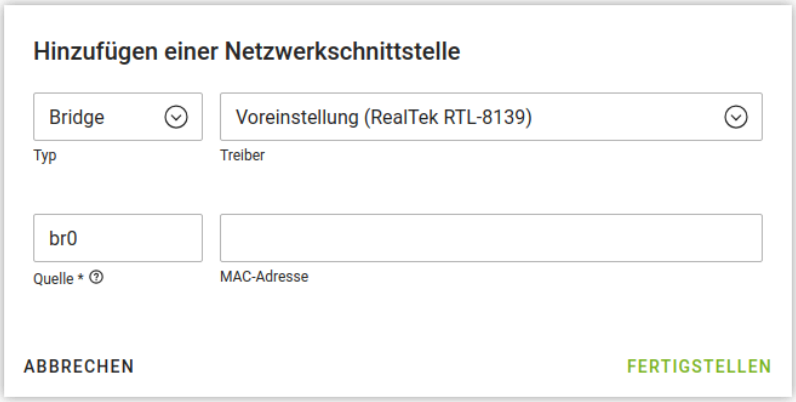
Beim Anlegen einer virtuellen Maschine wird dieser automatisch eine Netzwerkkarte mit zufällig erstellter MAC-Adresse zugewiesen. Diese kann ggf. nachträglich verändert werden.

Zwei Typen von Netzwerkverbindung sind möglich:

- In der Grundeinstellung wird mit einer *Bridge* auf dem Virtualisierungsserver direkt auf das Netz zugegriffen. Die virtuelle Maschine verwendet dabei ihre eigene IP-Adresse und ist damit auch von anderen Rechnern aus erreichbar.

- Netzwerkkarten vom Typ *Network Address Translation (NAT)* werden in einem privaten Netz auf dem Virtualisierungsserver definiert. Dabei muss der virtuellen Maschine eine IP-Adresse aus dem Netz `192.0.2.0/24` gegeben werden. Über NAT wird dieser virtuellen Maschine der Zugang zum externen Netz erteilt, so dass der Zugriff über die IP-Adresse des Virtualisierungsservers erfolgt. Die virtuelle Maschine ist damit nicht von anderen Rechnern erreichbar, kann aber selber beliebige ausgehende Verbindungen aufbauen.

Abbildung 16.4. Hinzufügen einer virtuellen Netzwerkkarte



Die UVMM-Server sind für NAT und Bridging vorkonfiguriert. Allerdings gibt es Einschränkungen für Netzwerkkarten vom Typ Bridge, welche in Abschnitt 8.2.4.1.4.1 beschrieben sind. Für jede virtuelle Maschine kann das zu verwendende Netzwerk über die Option **Quelle** ausgewählt werden.

Netzwerkkarten vom Typ NAT sind nur durch die im Netz `192.0.2.0/24` verfügbaren IP-Adressen begrenzt.

Über die Option **Treiber** kann ausgewählt werden, welche Art von Netzwerkkarte bereitgestellt wird. Die **Realtek RTL-8139** wird von nahezu jedem Betriebssystem unterstützt, die **Intel Pro-1000** bietet erweiterte Fähigkeiten und ein **Paravirtualisiertes Gerät** die beste Performance.

16.5.5. Paravirtualisierung (virtIO)-Treiber für Microsoft Windows-Systeme

Feedback

KVM unterstützt Paravirtualisierung über die virtIO Schnittstelle. Durch die Verwendung von Paravirtualisierung können die virtualisierten Systeme einen direkten Zugriff auf die Ressourcen des Virtualisierungs-

servers erhalten. Dies verbessert die Performance erheblich. Die Verwendung von Paravirtualisierung wird empfohlen.

Aktuelle Linux-Systeme unterstützen standardmäßig Paravirtualisierung. Mit der Installation der KVM-Pakete werden passende Images bereitgestellt, die dann in der Laufwerksverwaltung in eine virtuelle Maschine eingebunden werden können. Die Images werden in den mit der Univention Configuration Registry-Variable `uvmm/pool/default/path` festgelegten Speicherbereich integriert: Auf KVM-Virtualisierungsservern wird ein ISO-Image mit dem Namen *KVM Windows drivers* bereitgestellt, dass die virtIO-Virtualisierungstreiber für Microsoft Windows enthält.

16.5.5.1. Installation der virtIO-Treiber für KVM-Instanzen

Feedback

Bei Windows-Systemen, die unter KVM installiert werden muss *vor* Beginn der Windows-Installation Paravirtualisierung für die verwendeten Festplatten aktiviert werden.

Die virtIO-Schnittstelle erlaubt einer virtuellen Maschine den effizienten Zugriff auf Netzwerk- und Speicher-Ressourcen des KVM-Hypervisors. Die folgenden Schritte beschreiben die Einrichtung der virtIO-Treiber unter Windows 7.

- Ein CDROM/DVD-Laufwerk muss eingerichtet und das Image **KVM Windows drivers** zugewiesen werden.
- Für die Festplatten-Laufwerke muss im **Geräte**-Dialog des UCS Virtual Machine Manager die Option **Paravirtualisiertes Laufwerk** aktiviert werden.
- Für die Netzwerkkarte(n) muss der **Treiber** auf **Paravirtualisiert (virtio)** konfiguriert werden.
- Die initialen Schritte der Windows-Installation sind unverändert. Im Partitionierungs-Dialog erscheint die Warnung, dass nicht auf Massenspeicher zugegriffen werden kann; dies stellt keinen Fehler dar. Im selben Menü können die virtIO-Treiber mit **Treiber laden** eingerichtet werden. Unter Windows 7 (und ebenso Windows 2003/2008) muss **Red Hat virtIO SCSI Controller** und **Red Hat virtIO Ethernet Adapter** ausgewählt werden. Nach der Treiber-Installation ist die Festplatte im Windows-Installationsdialog sichtbar und die Installation kann fortgesetzt werden.
- Nach Abschluss der Installation werden die Geräte `Red Hat virtIO SCSI Disk Device` und `Red Hat virtIO Ethernet Adapter` im Windows-Gerätemanager angezeigt.

16.5.6. Sicherungspunkte

Feedback

UVMM bietet die Möglichkeit, den Inhalt von Arbeits- und Festplattenspeicher einer virtuellen Maschine in Sicherungspunkten zu speichern. Zu diesen kann später wieder zurückgewechselt werden, was gerade bei Software-Updates ein nützliches "Sicherungsnetz" darstellt.

Sicherungspunkte können nur mit Instanzen verwendet werden, deren Festplatten-Images ausschließlich das qcow2-Format verwenden. Alle Sicherungspunkte werden dabei im Copy-on-write-Verfahren (siehe Abschnitt 16.4.4) direkt in den Festplatten-Image-Dateien gespeichert.

16.5.7. Migration virtueller Maschinen

Feedback

UVMM bietet die Möglichkeit eine virtuelle Maschine von einem auf einen anderen physikalischen Server zu migrieren. Dies funktioniert sowohl mit ausgeschalteten, wie auch mit laufenden Maschinen (Live-Migration). Die Option wird nur angeboten, wenn sich min. zwei Virtualisierungsserver in der Domäne befinden. Die Migration von Instanzen zwischen Cloud Computing Umgebungen oder vor Ort Virtualisierungsservern ist nicht möglich.

Abbildung 16.5. Migrieren einer virtuellen Maschine

Bei der Migration ist zu beachten, dass die Image-Dateien der eingebundenen Festplatten und CD-ROM-Laufwerk von beiden Virtualisierungsservern zugreifbar sein müssen. Dies kann beispielsweise dadurch realisiert werden, dass die Images auf einem zentralen Storage abgelegt werden. Hinweise zur Einrichtung einer solchen Umgebung finden sich unter Abschnitt 16.5.2.

16.5.7.1. Migration virtueller Maschinen ausgefallener Virtualisierungsserver

Die Konfigurationen der virtuellen Maschinen aller Virtualisierungsserver werden zentral durch UCS Virtual Machine Manager erfasst. Ist ein Server ausgefallen (die Ausfallerkennung erfolgt periodisch alle fünfzehn Sekunden), wird der Server und die darauf betriebenen virtuellen Maschinen mit einem roten Symbol als unerreichbar markiert, eine Warnmeldung angezeigt und als einzige Operation das **Migrieren** der virtuellen Maschine angeboten.

Nach der Migration wird die virtuelle Maschine in UVMM auf dem ausgefallenen Virtualisierungsservers lediglich ausgeblendet und bleibt dort weiterhin definiert.

Achtung

Es ist unbedingt sicherzustellen, dass die virtuelle Maschine auf dem Ursprungs- und dem Ausweichserver nicht parallel gestartet sind, da ansonsten beide gleichzeitig in die selben Image-Dateien schreiben, was zu Datenverlusten führt. Falls virtuelle Maschinen nach dem Start automatisch gestartet werden, sollte durch Trennen der Netzwerkverbindung oder Einschränkung des Zugriffs auf den Speicherbereich ein gemeinsamer Zugriff unbedingt verhindert werden.

Falls der ausgefallene Rechner wieder aktiviert wird, - z.B. weil die Stromversorgung nur temporär unterbrochen war - sind die virtuellen Maschinen weiterhin lokal auf dem System definiert und werden erneut an UVMM gemeldet, d.h. die Maschine wird dann doppelt angezeigt.

Deshalb sollte anschließend eine der beiden Maschinen entfernt werden. Die verwendeten Image-Dateien der Laufwerke sollten dabei *nicht* mitgelöscht werden.

16.5.7.2. Migration von virtuellen Maschinen zwischen Servern mit unterschiedlichen CPUs

Virtuelle Maschinen können zwischen Servern mit kompatiblen CPUs migriert werden. Neuere CPUs sind normalerweise abwärtskompatibel mit vorherigen Generationen der CPU und fügen nur neuere Funktionen hinzu. Die Umkehrung dagegen ist nicht wahr: Falls das Gast-Betriebssystem sich entschieden hat, eine neuere Funktion zu nutzen, und diese nach der Migration nicht mehr zur Verfügung steht, wird die virtuelle Maschine abstürzen.

Standardmäßig ist kein bestimmtes CPU-Modell explizit konfiguriert: Der virtuellen Machine werden vielmehr direkt die CPU-Funktionen des jeweiligen Virtualisierungsserver durchgereicht. Der Vorteil ist, dass

die Performance höher ist, der Nachteil ist, dass es dadurch zu Abstürzen bei der Live-Migration kommen kann. Um die Migration zwischen inkompatiblen CPUs zu verhindern kann UVMM das CPU-Modell der Server beachten. Diese Funktionalität muss pro virtueller Maschine konfiguriert werden und wird erst nach einem Neustart der virtuellen Machine wirksam. Ein Reboot des laufenden Gastbetriebssystems reicht nicht; die virtuelle Maschine muss ggf. aus und erneut gestartet werden.

Auf dem Reiter **Erweitert** der VM kann das CPU Modell explizit konfiguriert werden.

Über die Univention Configuration Registry-Variable `uvmm/vm/cpu/host-model` kann das Anpassen der virtuellen Maschinen automatisiert werden. Die folgenden Werte sind erlaubt:

`missing`

UVMM aktiviert die Überprüfung für alle virtuellen Maschinen, für die nicht bereits das CPU-Model explizit konfiguriert ist.

`always`

UVMM aktiviert die Überprüfung für alle virtuellen Maschinen, unabhängig davon, ob bereits ein CPU-Model explizit konfiguriert ist oder nicht. Die Überschreibt jede andere vorhandene Konfiguration eines CPU-Models.

`remove`

UVMM entfernt jede Konfiguration eines CPU-Models.

- nicht gesetzt -

UVMM konfiguriert kein virtuelle Maschinen um. Dies ist der Standard.

Achtung

Falls mehrere UVMM Dienste benutzt werden, so sollte die Univention Configuration Registry-Variable `uvmm/vm/cpu/host-model` auf allen UCS-Systemen identisch gesetzt werden.

16.6. Profile

Feedback

Profile werden benutzt, um die anfänglichen Einstellungen für neue virtuelle Maschinen festzulegen. Unter anderem beinhalten diese folgende Einstellungen:

- Präfix für den Namen neuer virtueller Maschinen
- Anzahl der virtuellen CPUs
- CPU Modell
- Standard-RAM-Größe
- Standardgröße für neue Festplatten-Images
- Standard-Boot-Reihenfolge für vollvirtualisierte virtuelle Maschinen
- Benutzung der paravirtualisierten Gerätetreiber
- Standardeinstellung für den Direktzugriff per VNC
- Name der Netzwerk-Bridge-Schnittstelle

Die UVMM-Profile werden aus dem LDAP-Verzeichnis gelesen und können dort auch angepasst werden. Zu finden sind die Profile im UMC-Modul **LDAP-Verzeichnis** im Container `cn=Profiles,cn=Virtual Machine Manager`. Dort können auch weitere Profile hinzugefügt werden.

16.6.1. Ändern des Standardnetzwerkes

Der Name der Bridge für das Standardnetzwerk ist in den UVMM-Profilen gespeichert. Wenn das Standardnetzwerk `br0` geändert wird, müssen diese angepasst werden. Der folgende Befehl aktualisiert alle Profile auf die Bridge *$NEU*, die momentan als Netzwerkschnittstelle *$ALT* benutzen:

```
udm uvmm/profile list --filter interface="$ALT" |
 sed -ne 's/^DN: //p' |
 xargs -r -d '\n' -n 1 udm uvmm/profile modify --set interface="$NEU" --
dn
```

Kapitel 17. Datensicherung mit Bacula

17.1. Einführung

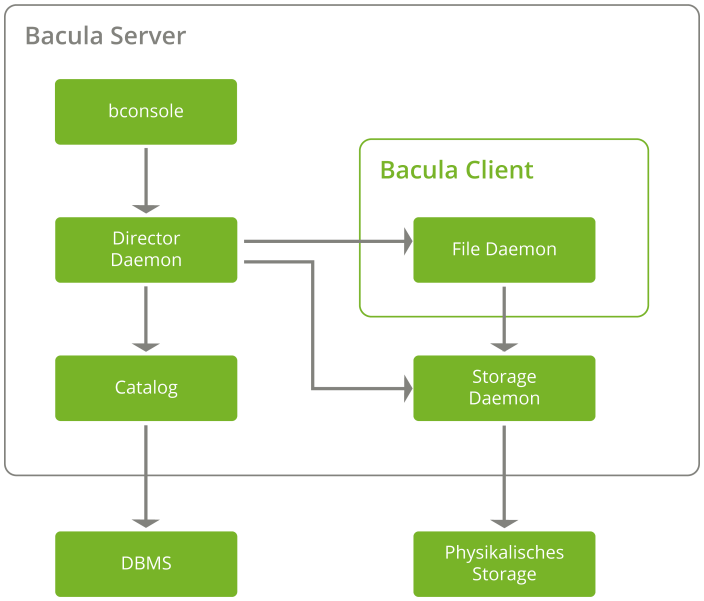
Bacula ist ein netzwerkfähiges Datensicherungsprogramm mit einer Client/Server-Architektur. Es erlaubt die Datensicherung und -wiederherstellung in heterogenen Umgebungen. Dieses Kapitel bezieht sich auf das Paket ***univention-bacula***, welches als Komponente von UCS ausgeliefert wird. Im Univention App Center können weitere Backup-Softwarelösungen ausgewählt und installiert werden, u.a. auch Bacula Enterprise.

Bacula besteht aus einer Reihe von einzelnen Diensten und Programmen, die die verschiedenen Aspekte der Datensicherung kontrollieren:

- Der *Director Daemon* ist die zentrale Steuereinheit, in dem die meisten Einstellungen zum Backup und Restore gespeichert sind. Im Director werden die übrigen Bacula-Dienste konfiguriert.
- Der *Storage Daemon* kontrolliert den Zugriff auf die Backupmedien (z.B. eine Tape Library oder Festplatten) und nimmt die Anweisungen des *Directors* entgegen, von welchen Systemen gesichert oder zurückgesichert werden soll.
- Der *File Daemon* ist auf den Clients installiert und nimmt die Anweisungen des *Directors* entgegen, welche Dateien über welchen *Storage Daemon* gesichert oder zurückgesichert werden sollen.
- Der *Catalog* speichert alle Sicherungen in einer Datenbank und ermöglicht das Rücksichern einzelner Dateien oder Verzeichnisse.
- Die *Bacula Console* ist das zentrale Benutzerinterface für den *Director Daemon*. Von dort können *Backup/Restore Jobs* gestartet werden. Auch administrative Aufgaben - wie das Einbinden von Backupmedien - oder die Abfrage von Statusinformationen werden darüber realisiert.
- Das *Bacula Administration Tool* ist eine grafische Version der *Bacula Console*.

Die Backup-Einstellungen (zu sichernde Daten, Backup-Modus- und -zeiten) werden also im *Director Daemon* konfiguriert und das Backup automatisch oder über die *Bacula Console* gestartet. Der *File Daemon* gibt dann die zu sichernden Daten an den *Storage Daemon* weiter, der für die Speicherung der Daten auf physikalischen Medien sorgt. Zusätzlich werden Meta-Information zu den Backups über den *Catalog* in einer Datenbank gesichert.

Abbildung 17.1. Bacula Schema



17.2. Umfang der Datensicherung auf einem UCS-System

Feedback

Wenn ausreichend Sicherungskapazität zur Verfügung steht, ist es empfehlenswert ein System vollständig zu sichern. Allerdings müssen nicht alle Daten auf einem UCS-System gesichert werden. Die mit UCS mitgelieferten Programmpakete beispielsweise stehen nach einer Neuinstallation ohnehin wieder zur Verfügung.

Die folgenden Informationen geben nur einen Überblick über ein typisches System. Je nach installierter Software können sich Abweichungen ergeben. Dies muss im Einzelfall geprüft werden und sollte mit einem testweisen Restore getestet werden!

Die Verzeichnisse `/dev/`, `/proc/` und `/sys/` enthalten nur Dateien, die vom Kernel automatisch generiert werden, sie brauchen nicht gesichert werden.

Diese Daten sollten in der Regel immer gesichert werden: Die Verzeichnisse `/home/` und `/root/` enthalten Benutzerdaten, in `/etc/` wird die Konfiguration des UCS-Systems gespeichert und das Verzeichnis `/var/` enthält Laufzeitdaten wie etwa die Mails eines Mailservers.

Die Verzeichnisse `/bin/`, `/boot`, `/lib/`, `/usr/` und `/sbin/` enthalten im Normalfall nur Programme/Daten, die durch die UCS-Installation mitgeliefert werden.

17.3. Installation

Feedback

In dieser Dokumentation wird davon ausgegangen, dass sich der *Director Daemon*, *Storage Daemon* und *Catalog* auf einem System, dem Bacula-Server, befinden. Diese Komponenten werden durch Installation des Pakets ***univention-bacula*** eingerichtet.

Der *File Daemon* muss auf allen System, auf denen Daten gesichert werden sollen, mit dem Paket ***bacula-client*** installiert werden.

Die Datenspeicherung des Catalogs erfolgt in einer PostgreSQL-Datenbank, die während der Installation angelegt und eingerichtet wird. Die Zugriffsinformationen dieser Datenbank (Datenbankname, Name/

Passwort des Datenbankbenutzers) stehen anschließend in der Datei `/etc/dbconfig-common/bacula-director-pgsql.conf` in den Feldern `dbc_dbpass` und `dbc_dbuser`.

17.4. Konfiguration der Backupkomponenten

Feedback

Die Konfiguration der Bacula-Dienste erfolgt über verschiedene Konfigurationsdateien. Im folgenden werden wichtige Optionen vorgestellt, weiterführende Konfigurations-Optionen werden in der Bacula-Dokumentation beschrieben.

17.4.1. Directory Daemon

Feedback

Der Directory Daemon wird über den Abschnitt *Director* der Konfigurationsdatei `/etc/bacula/bacula-dir.conf` verwaltet.

Die Standardwerte können beibehalten werden, lediglich die Option `DirAddress` sollte von `127.0.0.1`, also `localhost`, auf die IP-Adresse des Bacula-Servers geändert werden. Außerdem sollte das `Password`-Feld gesetzt werden:

```
Director {
  Name = sec-dir
  DIRport = 9101
  QueryFile = "/etc/bacula/scripts/query.sql"
  WorkingDirectory = "/var/lib/bacula"
  PidDirectory = "/var/run/bacula"
  Maximum Concurrent Jobs = 1
  Password = "master-dir-password"
  Messages = Daemon
  DirAddress = 192.0.2.125
}
```

17.4.2. Storage

Feedback

Der Storage Daemon wird über den Abschnitt *Storage* der Konfigurationsdatei `/etc/bacula/bacula-sd.conf` verwaltet.

Hier können die Vorgabewerte weitgehend beibehalten werden; nur die Option `SDAddress` sollte auf die IP-Adresse des Storage Daemons angepasst werden.

```
Storage {
  Name = sec-sd
  SDPort = 9103
  WorkingDirectory = "/var/lib/bacula"
  Pid Directory = "/var/run/bacula"
  Maximum Concurrent Jobs = 20
  SDAddress = 192.0.2.125
}
```

Im Abschnitt *Director* wird auf den Bacula-Server verwiesen und ein Passwort gesetzt, das dieser beim Zugriff verwenden muss:

```
Director {
  Name = sec-dir
  Password = "master-storage-password"
}
```

17.4.3. File Daemon

Feedback

Der File Daemon wird über die Konfigurationsdatei `/etc/bacula/bacula-fd.conf` verwaltet und muss auf allen Systemen eingerichtet werden, die gesichert werden sollen.

Im Abschnitt *Director* muss die Option `Name` auf den Namen des *Directors* gesetzt werden (siehe Abschnitt 17.4.1). Pro System muss ein Client-Passwort festgelegt werden. Außerdem muss hier die Option `FDAddress` im Abschnitt *FileDaemon* auf die IP-Adresse des Rechners gesetzt werden.

```
Director {
  Name = sec-dir
  Password = "client-password"
}
```

```
FileDaemon {
  Name = sec-fd
  FDport = 9102
  WorkingDirectory = /var/lib/bacula
  Pid Directory = /var/run/bacula
  Maximum Concurrent Jobs = 20
  FDAddress = 192.0.2.125
}
```

Jeder zu sichernde Rechner muss außerdem im Director mit dem oben festgelegten Passwort registriert in der Datei `/etc/bacula/bacula-dir.conf` registriert werden:

```
Client {
  Name = client-host
  Address = 192.0.2.125
  FDPort = 9102
  Catalog = MyCatalog
  Password = "client-password"
  File Retention = 30 days
  Job Retention = 6 months
  AutoPrune = yes
}
```

17.4.4. Bacula Console

Feedback

Die Bacula Console wird die Konfigurationsdatei `/etc/bacula/bconsole.conf` verwaltet.

Hier muss im Abschnitt *Director* die Adresse des Rechners, auf dem der Director Daemon läuft und dessen Passwort (siehe Abschnitt 17.4.1) angegeben werden:

```
Name = localhost-dir
  DIRport = 9101
  address = 192.0.2.125
  Password = "master-dir-password"
```

17.4.5. Firewall-Anpassungen

Feedback

In der Grundeinstellung von Univention Firewall werden eingehende Pakete für alle Ports blockiert/abgelehnt.

Die für Bacula verwendeten Ports müssen entsprechend freigegeben werden. Auf allen Systemen muss der Zugriff auf den Filedaemon freigegeben werden. Dies erfolgt durch Setzen der Univention Configurati-

on Registry-Variable `security/packetfilter/package/bacula/tcp/9102/all` auf `ACCEPT` und einen anschließenden Neustart von Univention Firewall.

Auf dem Bacula-Server muss zusätzlich Port 9103 nach dem gleichen Schema freigegeben werden.

In einem verteilten Setup müssen ggf. noch die Ports 9101/TCP (Verbindungen von der Console zum Directory) und 9103/TCP (Verbindungen von Directory und File Daemon zum Storage Daemon freigegeben werden.

17.5. Konfiguration des Backups (Intervall, Daten etc.)

Feedback

In Bacula werden *Ressourcen* definiert, die in einem *Job* zusammengefasst eine bestimmte Aktion, wie das Backup der Daten X vom Rechner Y auf das Medium Z, repräsentieren. Es gibt u.a. folgende Ressourcen:

- Der Zugriff auf physikalische Backupmedien wird in einem *Device* definiert, z.B. der Gerätetyp und wie es angeschlossen wurde.
- Die verschiedenen Backupmedien (z.B. Bänder oder Festplatten) werden als *Volume* bezeichnet. Volumes können manuell, aber auch direkt vom Director erzeugt werden. Bacula versieht die Volumes dabei mit Software-Labeln zur Identifizierung.
- Bacula verwaltet die Volumes in *Pools*. Dort sind beliebig viele Volumes zusammengeschlossen und deren Eigenschaften definiert. Backups erfolgen ausschließlich auf Pools. Bacula verwaltet dabei die Auslastung der Volumes und überwacht, wann Volumes wieder überschrieben werden dürfen.
- In einem *Schedule* wird definiert, wann eine Aktion ausgeführt wird. Hier können zusätzlich weitere Optionen für eine Aktion gesetzt oder überschrieben werden.
- Ein *FileSet* definiert, welche Dateien oder Verzeichnisse gesichert werden sollen, ob diese komprimiert werden und welche Metainformationen (z.B. ACLs) gesichert werden.
- Jeder Rechner, von dem Daten gesichert werden sollen, wird in Bacula als *Client* behandelt. *Client*-Jobs definieren, um welchen Rechner es sich handelt und wie auf den *File Daemon* des Clients zugegriffen werden kann (z.B. Passwort).

Ein *Job* führt alle die oben genannten Informationen zusammen. Jobs sind entweder vom Typ Restore oder Backup. Außerdem wird hier das Sicherungsverfahren der Backup-Läufe (inkrementelle, volle oder differentielle Sicherung) definiert.

Mit *Messages* wird definiert, wie mit Bacula-Statusnachrichten umgegangen werden soll. Meldungen können u.a. in Log-Dateien geschrieben, auf der Konsole angezeigt oder per Email verschickt werden.

In [bacula-config-example] findet sich eine Beispiel-Konfiguration, die als Vorlage für Backups verwendet werden kann und die oben genannten Ressourcen weitergehend beschreibt.

17.6. Administration über die Bacula Console

Feedback

Mit der *Bacula Console* können Informationen über den Status von Bacula ausgelesen, Backup-Jobs gestartet oder Daten zurückgesichert werden. Gestartet wird sie mit dem Befehl `bconsole`.

Das Kommando `status` zeigt Status-Informationen an. Es wird z.B. eine Liste der anstehenden, laufenden und beendeten Jobs des Directors ausgegeben.

Backup-Jobs können automatisch - z.B. an jedem Wochentag - gestartet werden. Backups und Rücksicherungen können aber auch interaktiv über die Bacula Console gestartet werden:

- Mit dem Kommando `run` kann ein Job gestartet werden. Es wird daraufhin ein Liste der verfügbaren Jobs angezeigt, aus denen der gewünschte Job ausgewählt werden muss. Mit dem Kommando `mod` können

Optionen wie der Sicherungstyp für den Job gesetzt bzw. geändert werden. Nach Bestätigung durch **yes** wird der Job gestartet.

- Mit dem Kommando `restore` können Daten zurückgesichert werden. Nun kann mit `3 (Enter list of comma separated JobIds to select)` ein Backup-Job ausgewählt werden, von dem Daten zurückgesichert werden sollen. Dann erscheint ein Dateibrowser, in dem mit den Standardkommandos `cd` und `ls` navigiert werden kann. Hier können mittels `mark FILE` bzw. `mark -r DIR` Dateien bzw. Verzeichnisse für die Rücksicherung markiert werden. Sind alle gewünschten Daten markiert, wird der Dateibrowser mit `done` beendet. Nach der Angabe des Clients und der Bestätigung einiger Optionen für den Restore-Job (z.B. wohin die Daten kopiert werden sollen) kann der Restore-Job mit **yes** gestartet werden. Nach Abschluss befinden sich die ausgewählten Daten im konfigurierten Rücksicherungsverzeichnis. Falls für ein Backup oder Restore ein Tape benötigt wird, das sich nicht im Laufwerk befindet, fordert Bacula dieses Tape explizit an.

Weitere Informationen über die Bacula Console können der Bacula-Dokumentation bzw. dem Kommando `help` entnommen werden.

17.7. Sicherung der Catalog-Datenbank

Feedback

Die Metadaten der Sicherung werden im Catalog gespeichert. Standardmäßig wird der Catalog in einer PostgreSQL-Datenbank gespeichert, die ebenfalls gesichert werden sollte. Dies erfolgt über einen Backup-Job, der einen SQL-Dump der Datenbank sichert.

```
# Backup the catalog database (after the nightly save)
Job {
  Name = "BackupCatalog"
  JobDefs = "DefaultJob"
  Level = Full
  FileSet="Catalog"
  Schedule = "WeeklyCycleAfterBackup"
  # This creates an ASCII copy of the catalog
  # Arguments to make_catalog_backup.pl are:
  #  make_catalog_backup.pl catalog-name
  RunBeforeJob = "/etc/bacula/scripts/make_catalog_backup.pl MyCatalog"
  # This deletes the copy of the catalog
  RunAfterJob = "/etc/bacula/scripts/delete_catalog_backup"
  Write Bootstrap = "/var/lib/bacula/%n.bsr"
  Priority = 11
}

...

# This schedule does the catalog. It starts after the WeeklyCycle
Schedule {
  Name = "WeeklyCycleAfterBackup"
  Run = Full sun-sat at 23:10
}

...

# This is the backup of the catalog
FileSet {
  Name = "Catalog"
  Include {
    Options {
```

```
      signature = MD5
    }
    File = "/var/lib/bacula/bacula.sql"
  }
}
```

Über die Anweisungen `RunBeforeJob` und `RunAfterJob` werden vor bzw. nach der eigentlichen Sicherung Skripte ausgeführt. Im Falle des Catalogs wird mit `make_catalog_backup` vor der Sicherung ein SQL-Dump der Catalog-Datenbank erzeugt und unter `/var/lib/bacula/bacula.sql` gespeichert. Nach erfolgter Sicherung wird diese Datei wieder entfernt.

Zusätzlich wird für das Backup des Catalogs mit `Write Bootstrap` eine Bootstrap-Datei erzeugt. In dieser Datei wird protokolliert, wie die Daten wiederhergestellt werden können, d.h. auf welchem Volume sie gespeichert sind und wo auf dem Volume sie sich befinden. Normalerweise übernimmt dies der Catalog selbst, für den Fall der Rücksicherung der Catalog-Datenbank wird jedoch die Bootstrap-Datei benötigt. Sie sollte unabhängig von Bacula zusätzlich gesichert werden.

Der Backup-Job des Catalogs, mit dazugehörigem *FileSet* und *Schedule*, ist als Vorlage bereits in der Konfiguration des *Director Daemon* enthalten und muss lediglich angepasst werden.

17.8. Weiterführende Informationen

Weitere Informationen zur Bacula-Einrichtung sind unter anderem auf den folgenden Webseiten zu finden:

- http://www.bacula.org/
- http://wiki.bacula.org/doku.php
- http://www.bacula.org/5.2.x-manuals/en/main/main.pdf
- https://de.wikipedia.org/wiki/Bacula
- http://old.bacula.org/de/dev-manual/Kurzanleitung.html

Literaturverzeichnis

[ucs-dokumentationen] Univention GmbH. 2019. *UCS Dokumentation Übersicht*. https://docs.software-univention.de/.

[admx-reference] Microsoft. 2014. *Referenzhandbuch für die Gruppenrichtlinien-ADMX-Syntax*. https://technet.microsoft.com/en-us/library/1db6fd85-d682-4d7d-9223-6b8dfafddc1c.

[admx-central] Mark Morowczynski. 2011. *How to Implement the Central Store for Group Policy Admin Templates, Completely (Hint: Remove Those .ADM files!)*. https://blogs.technet.microsoft.com/askpfeplat/2011/12/12/how-to-implement-the-central-store-for-group-policy-admin-templates-completely-hint-remove-those-adm-files/.

[microsoft-wmi-filter] Microsoft. 2005. *WMI filtering using GPMC*. https://www.microsoft.com/en-US/download/details.aspx?id=53314.

[add-wmi-filters] Mark Heitbrink. 2013. *Filtern von Gruppenrichtlinien anhand von Benutzergruppen, WMI und Zielgruppenadressierung*. http://www.gruppenrichtlinien.de/artikel/filtern-von-gruppenrichtlinien-anhand-von-benutzergruppen-wmi-und-zielgruppenadressierung/.

[adm-templates-howto] Florian Frommherz. 2007. *How to create custom ADM templates*. http://www.frickelsoft.net/blog/downloads/howto_admTemplates.pdf.

[microsoft-adm-templates] Microsoft. 2014. *Writing Custom ADM Files for System Policy Editor*. https://support.microsoft.com/en-us/kb/225087.

[bonding] Thomas Davis et al.. 2011. *Linux Ethernet Bonding Driver HOWTO*. https://www.kernel.org/doc/Documentation/networking/bonding.txt.

[dhcp-failover] ISC. 2013. *A Basic Guide to Configuring DHCP Failover*. https://kb.isc.org/article/AA-00502/31.

[developer-reference] Univention GmbH. 2022. *Univention Developer Reference*. https://docs.software-univention.de/developer-reference-5.0.html.

[bind-loglevel] O'Reilly. 1998. *Reading Bind Debugging Output*. http://www.diablotin.com/librairie/networking/dns-bind/ch12_01.htm.

[samba3-howto-chapter-20] Jelmer R. Vernooij and John H. Terpstra and Gerald (Jerry) Carter. 2010. *The Official Samba 3.2.x HOWTO and Reference Guide*. http://www.samba.org/samba/docs/Samba3-HOWTO.pdf#chapter.20.

[packaging-acl-extensions] Univention GmbH. 2022. *Packaging LDAP ACL Extensions*. https://docs.software-univention.de/developer-reference-5.0.html#settings:ldapacl.

[packaging-schema-extensions] Univention GmbH. 2022. *Packaging LDAP Schema Extensions*. https://docs.software-univention.de/developer-reference-5.0.html#settings:ldapschema.

[ucs-performance-guide] Univention GmbH. 2022. *UCS performance guide*. https://docs.software-univention.de/performance-guide-5.0.html.

[ext-doc-inst] Univention GmbH. 2022. *Extended installation documentation*. https://docs.software-univention.de/ext-installation/5.0/en/.

[ext-doc-uvmm] Univention GmbH. 2019. *Extended virtualization documentation*. https://docs.software-univention.de/uvmm-4.4.html.

[ext-doc-win] Univention GmbH. 2022. *Extended Windows integration documentation*. https://docs.software-univention.de/ext-windows/5.0/en/.

[ext-print-doc] Univention GmbH. 2022. *Extended print services documentation*. https://docs.software-univention.de/printers-4.4.html.

[ext-doc-domain] Univention GmbH. 2022. *Extended domain services documentation*. https://docs.software-univention.de/ext-domain/5.0/en/.

[ext-doc-net] Univention GmbH. 2022. *Extended IP and network management documentation*. https://docs.software-univention.de/ext-networks/5.0/en/.

[ec2-quickstart] Univention GmbH. 2016. *Univention Wiki - Amazon EC2 Quickstart*. http://wiki.univention.de/index.php?title=Amazon_EC2_Quickstart.

[xenserver-installation] Univention GmbH. 2016. *Univention Wiki - Citrix XenServer*. http://wiki.univention.de/index.php?title=Citrix_Xen_Server.

[bacula-config-example] Univention GmbH. 2013. *Bacula Beispielkonfiguration*. http://wiki.univention.de/index.php?title=Bacula_configuration_example.

[dovecot-wiki-clusterfs] Timo Sirainen. 2013. *Dovecot Wiki: Mail storage on shared disks*. http://wiki2.dovecot.org/MailLocation/SharedDisk.

[dovecot-wiki-nfs] Timo Sirainen. 2016. *Dovecot Wiki: NFS*. http://wiki2.dovecot.org/NFS.

[dovecot-wiki-services] Timo Sirainen. 2016. *Dovecot Wiki: Service configuration*. http://wiki2.dovecot.org/Services.