



Univention Corporate Server - Handbuch für Benutzer und Administratoren

Release 5.2

07.06.2026

Die Quellen dieses Dokuments sind unter der [GNU Affero General Public License v3.0 only](#) lizenziert.

1	Einführung	1
1.1	Was ist Univention Corporate Server?	1
1.2	Was ist Univention Nubus?	1
1.3	Überblick über UCS	1
1.4	Weitere Dokumentationen	2
1.5	Verwendete Symbole und Konventionen	3
2	Installation	5
2.1	Auswahl des Installationsmodus	5
2.2	Auswahl der Installationsprache	5
2.3	Auswahl des Standorts	5
2.4	Auswahl der Tastaturbelegung	5
2.5	Netzwerkkonfiguration	6
2.6	Einrichtung des root-Passworts	6
2.7	Partitionierung der Festplatten	6
2.8	Domäneneinstellungen	6
2.9	Bestätigen der Einstellungen	6
2.10	Fehlersuche bei Installationsproblemen	7
2.11	Installation im Textmodus	7
2.12	Installation in der Amazon EC2-Cloud	7
2.13	Installation in VMware	7
3	Domänendienste / LDAP-Verzeichnisdienst	9
3.1	Domänenbeitritt	9
3.2	UCS-Systemrollen	11
3.3	LDAP-Verzeichnisdienst	12
3.4	Listener/Notifier-Domänenreplikation	14
3.5	Provisioning Service	14
3.6	SSL-Zertifikatsverwaltung	19
3.7	Kerberos	19
3.8	Passwort-Hashes im Verzeichnisdienst	19
3.9	Single Sign-On	19
3.10	Umwandlung eines Backup Directory Node zum neuen Primary Directory Node	19
3.11	Fehlertolerante Domain Einrichtung	19
3.12	Protokollierung von Aktivitäten in der Domäne	20
4	UCS Web-Oberfläche	21
4.1	Einführung	22
4.2	Anmelden	23
4.3	UCS Portalseite	24
4.4	Zustimmung zur Verwendung von Cookies	24

4.5	Univention Management Console-Module	25
4.6	LDAP-Verzeichnis-Browser	26
4.7	Richtlinien	27
4.8	Erweiterung von UMC-Modulen mit erweiterten Attributen	27
4.9	Strukturierung der Domäne durch angepasste LDAP-Strukturen	28
4.10	Delegierte Administration für UMC-Module	28
4.11	Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)	28
4.12	HTTP Schnittstelle (API) der Domänenverwaltung	29
4.13	Auswertung von Daten aus dem LDAP-Verzeichnis mit Univention Directory Reports	29
4.14	Let's Encrypt	30
5	Softwareverteilung	31
5.1	Unterscheidung der Update-Varianten / Aufbau der UCS-Versionen	31
5.2	Univention App Center	31
5.3	Aktualisierung von UCS-Systemen	32
5.4	Konfiguration des Repository-Servers für Updates und Paketinstallationen	32
5.5	Installation weiterer Software	33
5.6	Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie	34
5.7	Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor	34
6	Benutzerverwaltung	35
6.1	Verwaltung von Benutzern über Univention Management Console Modul	36
6.2	Benutzeraktivierung für Apps	37
6.3	Verwaltung der Benutzerpasswörter	37
6.4	Passwort-Einstellungen für Windows-Clients bei Verwendung von Samba	38
6.5	Benutzer Selbstverwaltung	38
6.6	Automatisches Sperren von Benutzern nach fehlgeschlagenen Anmeldungen	39
6.7	Benutzervorlagen	39
6.8	Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos	39
6.9	Wiederverwendung von Benutzereigenschaften verhindern	39
6.10	Papierkorb	40
7	Gruppenverwaltung	45
7.1	Zuordnung von Benutzergruppen	45
7.2	Empfehlung für Definition von Gruppennamen	45
7.3	Verwaltung von Gruppen über Univention Management Console Modul	45
7.4	Verschachtelte Gruppen mit Gruppen in Gruppen	46
7.5	Lokaler Gruppencache	46
7.6	Synchronisation von Active Directory-Gruppen bei Verwendung von Samba/AD	46
7.7	Overlay-Modul zur Anzeige der Gruppeninformationen an Benutzerobjekten	46
8	Rechnerverwaltung	47
8.1	Verwaltung der Rechnerkonten über Univention Management Console Modul	47
8.2	Konfiguration von Hardware und Treibern	48
8.3	Verwaltung der lokalen Systemkonfiguration mit Univention Configuration Registry	50
8.4	Basis-Systemdienste	52
9	Services für Windows	55
9.1	Betrieb einer Samba-Domäne auf Basis von Active Directory	55
9.2	Active Directory-Verbindung	64
9.3	Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover	80
9.4	Vertrauensstellungen	84
10	Identity Management Anbindung an Cloud-Dienste	87
10.1	Microsoft 365 Connector	87
10.2	Google Apps for Work Connector	92
11	IP- und Netzverwaltung	95
11.1	Netzwerk-Objekte	95

11.2	Verwaltung von DNS-Daten mit BIND	95
11.3	IP-Vergabe über DHCP	98
11.4	Paketfilter mit Univention Firewall	100
11.5	Web-Proxy für Caching und Policy Management/Virensan	101
11.6	RADIUS	103
12	Verwaltung von Freigaben	113
12.1	Zugriffsrechte auf Daten in Freigaben	113
12.2	Verwaltung von Freigaben über Univention Management Console Modul	114
12.3	Unterstützung von MSDFS	115
12.4	Konfiguration von Dateisystem-Quota	116
13	Druckdienste	119
13.1	Installation eines Druckservers	120
13.2	Einstellung lokaler Konfigurationseigenschaften eines Druckservers	120
13.3	Konfiguration von Druckerfreigaben	120
13.4	Konfiguration von Druckergruppen	120
13.5	Verwaltung von Druckaufträgen und Druckerwarteschlangen	120
13.6	Generierung von PDF-Dokumenten aus Druckaufträgen	121
13.7	Einbinden von Druckerfreigaben auf Windows-Clients	122
13.8	Integration weiterer PPD-Dateien	126
14	Maildienste	127
14.1	Installation	128
14.2	Verwaltung der Mailserver-Daten	128
14.3	Spamerkennung und -filterung	129
14.4	Viren- und Malwareerkennung	130
14.5	Identifikation von Spam Quellen mit DNS basierten Blackhole Listen	130
14.6	Integration von Fetchmail zum Abrufen von Mail von externen Postfächern	131
14.7	Konfiguration des Mailservers	132
14.8	Konfiguration von Mail-Clients für den Mailserver	138
14.9	OX Connector	139
15	Infrastruktur-Monitoring	141
15.1	UCS Dashboard	141
15.2	Monitoring	142
15.3	Nagios	150
16	Anhang	153
16.1	Univention Configuration Registry Variablen	153
16.2	Literaturverzeichnis	170
16.3	Stichwortverzeichnis	170
	Literaturverzeichnis	171
	Stichwortverzeichnis	173

Wichtig

Univention migriert derzeit Teile dieses Handbuchs zu *Univention Corporate Server - Operation Manual* [1]. Für jeden verschobenen Abschnitt finden Sie einen Link auf seine neue Position in diesem Dokument. Sollten Sie den gesuchten Inhalt hier nicht finden, konsultieren Sie *Univention Corporate Server - Operation Manual* [1] direkt.

Der Inhalt dieses Abschnitts ist umgezogen nach [Einleitung](#)¹ in *Univention Corporate Server - Operation Manual* [1].

1.1 Was ist Univention Corporate Server?

Der Inhalt dieses Abschnitts ist umgezogen nach [Was ist UCS?](#)² in *Univention Corporate Server - Operation Manual* [1].

1.2 Was ist Univention Nubus?

Der Inhalt dieses Abschnitts ist umgezogen nach [Nubus und UCS verstehen](#)³ in *Univention Corporate Server - Operation Manual* [1].

1.3 Überblick über UCS

Der Inhalt dieses Abschnitts ist umgezogen nach [Schlüsselkonzepte](#)⁴ in *Univention Corporate Server - Operation Manual* [1].

1.3.1 Inbetriebnahme

Der Inhalt dieses Abschnitts ist umgezogen nach [Schlüsselkonzepte](#)⁵ in *Univention Corporate Server - Operation Manual* [1].

¹ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro>

² <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-understanding-nubus-for-ucs-whats-ucs>

³ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-understanding-nubus-for-ucs>

⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-key-concepts>

⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-key-concepts>

1.3.2 Domänenkonzept

Der Inhalt dieses Abschnitts ist umgezogen nach [Domänenkonzept](#)⁶ in *Univention Corporate Server - Operation Manual* [1].

1.3.3 Erweiterbarkeit durch das Univention App Center

Der Inhalt dieses Abschnitts ist umgezogen nach [Univention App Center](#)⁷ in *Univention Corporate Server - Operation Manual* [1].

1.3.4 LDAP-Verzeichnisdienst

Der Inhalt dieses Abschnitts ist umgezogen nach [LDAP-Verzeichnisdienst](#)⁸ in *Univention Corporate Server - Operation Manual* [1].

1.3.5 Domänenadministration

Der Inhalt dieses Abschnitts ist umgezogen nach [Management UI](#)⁹ in *Univention Corporate Server - Operation Manual* [1].

1.3.6 Rechneradministration

Der Inhalt dieses Abschnitts ist umgezogen nach [Schlüsselkonzepte](#)¹⁰ in *Univention Corporate Server - Operation Manual* [1].

1.3.7 Richtlinienkonzept

Der Inhalt dieses Abschnitts ist umgezogen nach [Richtlinienkonzept](#)¹¹ in *Univention Corporate Server - Operation Manual* [1].

1.3.8 Listener/Notifier-Replikation

Der Inhalt dieses Abschnitts ist umgezogen nach [Listener/Notifier-Replikation](#)¹² in *Univention Corporate Server - Operation Manual* [1].

1.4 Weitere Dokumentationen

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
- Druckserver-Funktionalität
- Proxy-Server

Unter *UCS documentation overview* [2] sind weitere Dokumentationen zu UCS veröffentlicht, die weiterführende Themen behandeln.

⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-domain-concept>

⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-app-center>

⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-ldap-directory-service>

⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-management-ui>

¹⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-key-concepts>

¹¹ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-policy-concept>

¹² <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro-listener-notifier-replication>

1.5 Verwendete Symbole und Konventionen

Im Handbuch werden folgende Symbole verwendet:

Vorsicht

Warnungen werden hervorgehoben.

Bemerkung

Hinweise werden ebenfalls hervorgehoben.

Diese Felder beschreiben den Funktionsumfang eines UMC-Moduls:

Tab. 1.1: Reiter DHCP-Dienst

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

Menüeinträge, Schaltflächenbeschriftungen und ähnliches sind *in dieser Schriftform* gesetzt.

Eigennamen sind *hervorgehoben*.

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

Befehle und Tastatureingaben werden optisch hervorgehoben.

Abschnitte aus Konfigurationsdateien, Bildschirmausgaben usw. werden als Codeblock formatiert.

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.

Der Inhalt dieses Abschnitts wurde nach [System Deployment](#)¹³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.1 Auswahl des Installationsmodus

Der Inhalt dieses Abschnitts wurde nach [Installationsmodus auswählen](#)¹⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.2 Auswahl der Installationssprache

Der Inhalt dieses Abschnitts wurde nach [Sprache auswählen](#)¹⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.3 Auswahl des Standorts

Der Inhalt dieses Abschnitts wurde nach [Standort auswählen](#)¹⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.4 Auswahl der Tastaturbelegung

Der Inhalt dieses Abschnitts wurde nach [Tastaturbelegung auswählen](#)¹⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

¹³ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/index.html#deployment>

¹⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-install-mode>

¹⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-language>

¹⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-location>

¹⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-keyboard-layout>

2.5 Netzwerkkonfiguration

Der Inhalt dieses Abschnitts wurde nach [Netzwerkkonfiguration einrichten](#)¹⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.6 Einrichtung des root-Passworts

Der Inhalt dieses Abschnitts wurde nach [Root-Passwort festlegen](#)¹⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.7 Partitionierung der Festplatten

Der Inhalt dieses Abschnitts wurde nach [Festplatte partitionieren](#)²⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.8 Domäneneinstellungen

Der Inhalt dieses Abschnitts wurde nach [Einrichtung der Domäne](#)²¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.8.1 Namenskonvention für Rechnernamen

Der Inhalt dieses Abschnitts wurde nach [Namenskonvention für Rechnernamen](#)²² in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.8.2 Modus *Erstellen einer neuen UCS-Domäne*

Der Inhalt dieses Abschnitts wurde nach [Modus: Neue UCS-Domäne erstellen](#)²³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.8.3 Modus *Einer bestehenden Active-Directory-Domäne beitreten*

Der Inhalt dieses Abschnitts wurde nach [Modus: Einer bestehenden Active Directory Domäne beitreten](#)²⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.8.4 Modus *Einer bestehenden UCS-Domäne beitreten*

Der Inhalt dieses Abschnitts wurde nach [Modus: Einer bestehenden UCS-Domäne beitreten](#)²⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.9 Bestätigen der Einstellungen

Der Inhalt dieses Abschnitts wurde nach [Installationseinstellungen bestätigen](#)²⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

¹⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-network-setup>

¹⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-password>

²⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/initial-system-configuration.html#deployment-initial-system-configuration-partitioning>

²¹ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-domain-setup>

²² <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-domain-setup-naming>

²³ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-domain-setup-new-domain>

²⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-domain-setup-ad-member>

²⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-domain-setup-join-ucs>

²⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/domain-setup.html#deployment-installation-physical-confirm-settings>

2.10 Fehlersuche bei Installationsproblemen

Der Inhalt dieses Abschnitts wurde nach Fehlerbehebung bei Installationsproblemen²⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.11 Installation im Textmodus

Der Inhalt dieses Abschnitts wurde nach Installation im Textmodus²⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.12 Installation in der Amazon EC2-Cloud

Der Inhalt dieses Abschnitts wurde nach Cloud Installation²⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

2.13 Installation in VMware

Der Inhalt dieses Abschnitts wurde nach VMware-spezifische Überlegungen³⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

²⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/trouble.html#deployment-installation-troubleshooting>

²⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/install.html#deployment-installation-text-mode>

²⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/install.html#deployment-installation-cloud>

³⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/deployment/install.html#deployment-installation-vmware>

Domänendienste / LDAP-Verzeichnisdienst

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 *Benutzerverwaltung* (Seite 35) beschrieben.

Alle UCS- und Windowssysteme innerhalb einer UCS-Domäne verfügen über ein Domänenkonto, sobald sie der UCS-Domäne beigetreten sind. Der Domänenbeitritt wird in *Domänenbeitritt* (Seite 9) beschrieben.

Auf dem Primary Directory Node 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 *SSL-Zertifikatsverwaltung* (Seite 19).

Jedes Rechnersystem, das Mitglied einer UCS-Domäne ist, besitzt eine Systemrolle. Aus dieser Systemrolle ergeben sich verschiedene Berechtigungen und Einschränkungen, die in *UCS-Systemrollen* (Seite 11) beschrieben sind.

Alle domänenweiten Einstellungen werden in einem Verzeichnisdienst auf Basis von OpenLDAP vorgehalten. In *LDAP-Verzeichnisdienst* (Seite 12) 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 *Listener/Notifier-Domänenreplikation* (Seite 14).

UCS bietet zusätzlich einen Provisionierungsdienst auf der Ebene von UDM-Objekten an, der eine API für Apps bereitstellt, um Informationen zu abonnieren über Änderungen der IAM-Daten in der Domäne. Weitere Informationen finden Sie unter *Provisioning Service* (Seite 14).

Kerberos ist ein Authentifikationsverfahren 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 *Kerberos* (Seite 19).

3.1 Domänenbeitritt

Der Inhalt dieses Abschnitts wurde nach *Domänenbeitritt*³¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

³¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join>

3.1.1 Domänenbeitritt von UCS-Systemen

Der Inhalt dieses Abschnitts wurde nach [Wie UCS-Systeme Domänen beitreten](#)³² in *Univention Corporate Server - Operation Manual* [1] verschoben.

Nachträglicher Domänenbeitritt mit *univention-join*

Der Inhalt dieses Abschnitts wurde nach [Nachfolgende Domänenbeitritte mit univention-join](#)³³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Domänenbeitritt über Univention Management Console Modul

Der Inhalt dieses Abschnitts wurde nach [Einer Domäne über das Verwaltungsmodul beitreten](#)³⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Join-Skripte / Unjoin-Skripte

Der Inhalt dieses Abschnitts wurde nach [Join-Skripte und Unjoin-Skripte](#)³⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Nachträgliches Ausführen von Join-/Unjoin-Skripten

Der Inhalt dieses Abschnitts wurde nach [Join-Skripte und Unjoin-Skripte](#)³⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.1.2 Windows-Domänenbeitritt

Der Inhalt dieses Abschnitts wurde nach [Windows Domänenbeitritte](#)³⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Unterstützte Windows Versionen

Der Inhalt dieses Abschnitts wurde nach [Unterstützte Windows-Versionen](#)³⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Windows 11

Der Inhalt dieses Abschnitts wurde nach [Windows 11](#)³⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Windows 10

Der Inhalt dieses Abschnitts wurde nach [Windows 10](#)⁴⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Windows Server 2012 / 2016 / 2019 / 2022

Der Inhalt dieses Abschnitts wurde nach [Windows Server 2012 / 2016 / 2019 / 2022 / 2025](#)⁴¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

³² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-ucs>

³³ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-univention-join>

³⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-ucs-umc>

³⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-ucs-joinscripts>

³⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-ucs-joinscripts>

³⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-windows>

³⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-windows-versions>

³⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-windows-11>

⁴⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-windows-10>

⁴¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-windows-server>

3.1.3 Ubuntu-Domänenbeitritt

Der Inhalt dieses Abschnitts wurde nach [Ubuntu Domänenbeitritte](#)⁴² in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.1.4 macOS-Domänenbeitritt

Der Inhalt dieses Abschnitts wurde nach [macOS-Domänenbeitritte](#)⁴³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Domänenbeitritt über das Systemeinstellungen-Menü

Der Inhalt dieses Abschnitts wurde nach [macOS-Domänenbeitritte](#)⁴⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Domänenbeitritt auf den Kommandozeile

Der Inhalt dieses Abschnitts wurde nach [Domänenbeitritt in der Befehlszeile](#)⁴⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2 UCS-Systemrollen

Der Inhalt dieses Abschnitts wurde nach [Systemrollen verstehen](#)⁴⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.1 Primary Directory Node

Der Inhalt dieses Abschnitts wurde nach [Primary Directory Node](#)⁴⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.2 Backup Directory Node

Der Inhalt dieses Abschnitts wurde nach [Backup Directory Node](#)⁴⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.3 Replica Directory Node

Der Inhalt dieses Abschnitts wurde nach [Replica Directory Node](#)⁴⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.4 Managed Node

Der Inhalt dieses Abschnitts wurde nach [Managed Node](#)⁵⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

⁴² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-ubuntu>

⁴³ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-macos>

⁴⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-macos>

⁴⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/domain-join.html#domain-infrastructure-join-macos-cli>

⁴⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles>

⁴⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-primary-directory-node>

⁴⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-backup-directory-node>

⁴⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-replica-directory-node>

⁵⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-managed-node>

3.2.5 Ubuntu

Der Inhalt dieses Abschnitts wurde nach [Ubuntu](#)⁵¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.6 Linux

Der Inhalt dieses Abschnitts wurde nach [Linux](#)⁵² in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.7 macOS

Der Inhalt dieses Abschnitts wurde nach [macOS](#)⁵³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.8 Domain Trust Account

Der Inhalt dieses Abschnitts wurde nach [Domain Trust Account](#)⁵⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.9 IP-Client

Der Inhalt dieses Abschnitts wurde nach [IP-Client](#)⁵⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.10 Windows Domänencontroller

Der Inhalt dieses Abschnitts wurde nach [Windows Domain Controller](#)⁵⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.2.11 Windows Workstation/Server

Der Inhalt dieses Abschnitts wurde nach [Windows Workstation und Windows Server](#)⁵⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3 LDAP-Verzeichnisdienst

Der Inhalt dieses Abschnitts wurde nach [LDAP-Verzeichnisdienst](#)⁵⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.1 LDAP-Schemata

Der Inhalt dieses Abschnitts wurde nach [LDAP-Schemata](#)⁵⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

LDAP-Schema-Erweiterungen

Der Inhalt dieses Abschnitts wurde nach [LDAP Schema-Erweiterungen](#)⁶⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

⁵¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-ubuntu>

⁵² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-linux>

⁵³ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-macos>

⁵⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-domain-trust-account>

⁵⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-ip-managed-client>

⁵⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-windows-domain-controller>

⁵⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/system-roles.html#domain-infrastructure-system-roles-windows-workstation-server>

⁵⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory>

⁵⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-schema>

⁶⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-schema-extension>

LDAP-Schema-Replikation

Der Inhalt dieses Abschnitts wurde nach LDAP Schema-Replikation⁶¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.2 Revisions sichere LDAP-Protokollierung

Der Inhalt dieses Abschnitts wurde nach Protokollierung von LDAP-Änderungen zur Erkennung von Manipulationen⁶² in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.3 Timeout für inaktive LDAP-Verbindungen

Der Inhalt dieses Abschnitts wurde nach Zeitüberschreitung für inaktive LDAP-Verbindungen⁶³

3.3.4 LDAP-Kommandozeilen-Tools

Der Inhalt dieses Abschnitts wurde nach LDAP-Befehlszeilenwerkzeuge⁶⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.5 Zugriffskontrolle auf das LDAP-Verzeichnis

Der Inhalt dieses Abschnitts wurde nach Konfiguration der LDAP-Zugriffskontrolle⁶⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Delegation des Zurücksetzens von Benutzerpasswörtern

Der Inhalt dieses Abschnitts wurde nach Delegation des Rechts zum Zurücksetzen von Benutzerpasswörtern⁶⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.6 Name Service Switch / LDAP-NSS-Modul

Der Inhalt dieses Abschnitts wurde nach Name Service Switch und LDAP-NSS-Modul⁶⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.7 Konfiguration des Verzeichnis-Dienstes bei Verwendung von Samba/AD

Der Inhalt dieses Abschnitts wurde nach Konfiguration des Verzeichnisdienstes bei Verwendung von Samba/AD⁶⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.3.8 Tägliche Sicherung der LDAP-Daten

Der Inhalt dieses Abschnitts wurde nach Tägliches Backup von LDAP-Daten⁶⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

⁶¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-schema-replication>

⁶² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-logger>

⁶³ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-timeout-inactive-con>

⁶⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-cli-tools>

⁶⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-acls>

⁶⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-delegate-password-r>

⁶⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-nss>

⁶⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-samba-4>

⁶⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ldap-directory.html#domain-infrastructure-ldap-directory-backup>

3.4 Listener/Notifier-Domänenreplikation

3.4.1 Ablauf der Listener/Notifier-Replikation

Der Inhalt dieses Abschnitts wurde nach Domänenreplikation mit Listener und Notifier⁷⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.4.2 Analyse von Listener/Notifier-Problemen

Der Inhalt dieses Abschnitts wurde nach Fehlerbehebung bei Listener und Notifier⁷¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Logdateien/Debug-Level der Replikation

Der Inhalt dieses Abschnitts wurde nach Log-Dateien lesen und Debug-Level festlegen⁷² in *Univention Corporate Server - Operation Manual* [1] verschoben.

Erkennung von Replikationsproblemen

Der Inhalt dieses Abschnitts wurde nach Probleme bei der Replikation identifizieren⁷³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Neuinitialisierung von Listener-Modulen

Der Inhalt dieses Abschnitts wurde nach Listener-Module neu initialisieren⁷⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.5 Provisioning Service

Der *Provisioning Service* ist ein Ereignis- und Messaging-Dienst, der interessierte Dienste über Ereignisse im LDAP-Verzeichnisdienst benachrichtigen kann. Wenn sich Daten im LDAP-Verzeichnis auf dem Primary Directory Node ändern, erhält der *Provisioning Service* eine Benachrichtigung über die Änderung und informiert alle abonnierten Dienste über die Änderung. Im Gegensatz zum Univention Directory Listener liefert er die UDM-Darstellung der geänderten Objekte anstelle der LDAP-Darstellung.

Diese Seite beschreibt die Installation und Konfiguration des *Provisioning Service* in UCS. Weitere Informationen zur Funktionsweise des *Provisioning Service* finden Sie unter *Provisioning Service*⁷⁵ in *Nubus for Kubernetes - Architecture Manual 1.x* [3].

Bemerkung

Es gibt keine in UCS integrierten Dienste, die den *Provisioning Service* nutzen. Sie können Dienste erstellen, die den *Provisioning Service* verwenden, wie dokumentiert unter *Provisioning API*⁷⁶ in *Nubus - Customization and Modification Manual 1.x* [4].

Bemerkung

Der *Provisioning Service* ist Teil von Univention Nubus in der *Identity Store and Directory Service* Komponente. Weitere Informationen über Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 1)

⁷⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/listener-notifier.html#listener-notifier>

⁷¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/listener-notifier.html#listener-notifier-troubleshooting>

⁷² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/listener-notifier.html#listener-notifier-troubleshooting-logfiles>

⁷³ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/listener-notifier.html#listener-notifier-troubleshooting-replication>

⁷⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/listener-notifier.html#listener-notifier-troubleshooting-init-modules>

⁷⁵ <https://docs.software-univention.de/nubus-kubernetes-architecture/latest/en/components/provisioning-service.html#component-provisioning-service>

⁷⁶ <https://docs.software-univention.de/nubus-customization/latest/en/api/provisioning.html#customization-api-provisioning>

3.5.1 Installation

Das Univention App Center stellt den *Provisioning Service* als App bereit. UCS installiert ihn nicht standardmäßig. Sie können ihn auf dem Primary Directory Node und auf jedem Backup Directory Node installieren. Es ist nicht möglich, den *Provisioning Service* auf anderen Server-Systemrollen zu installieren. Der *Provisioning Service* besteht aus den folgenden Apps:

provisioning-service

Die App **provisioning-service** ist eine Container-App, die die Hauptfunktionen des *Provisioning Service* bereitstellt.

provisioning-service-backend

Die App **provisioning-service-backend** ist eine paketbasierte App, die Integrationspakete unter UCS installiert. Das App Center installiert sie automatisch als Abhängigkeit von **provisioning-service**. Die Pakete enthalten ein Listener-Modul und eine Hostkonfiguration für die TLS-Verschlüsselung zwischen mehreren Installationen.

Um den *Provisioning Service* zu installieren, wählen Sie eine der folgenden Installationsmethoden. Das App Center wendet mehrere Einstellungen auf den *Provisioning Service* an. Weitere Informationen finden Sie unter *Provisioning Service Einstellungen* (Seite 16).

App Center

Sie können die App **provisioning-service** wie jede andere App über das Univention App Center installieren. Allgemeine Informationen zum Univention App Center und dessen Verwendung für die Softwareinstallation finden Sie unter *Univention App Center* (Seite 31).

Kommandozeile

Um die App über die Kommandozeile zu installieren, verwenden Sie den Befehl in [Quellcode 3.1](#).

Quellcode 3.1: Installation des *Provisioning Service* über die Kommandozeile

```
$ univention-app install provisioning-service
```

3.5.2 Ablauf der Provisionierung

Der *Provisioning Service* liefert einen Stream von Ereignissen über Datenänderungen im LDAP-Verzeichnisdienst. Er verwendet die folgenden Komponenten:

Provisioning Listener

Ein Univention Directory Listener-Listener-Modul, das auf alle LDAP-Operationen reagiert und diese Änderungen an den *Provisioning Service* weiterleitet. Das Univention Directory Listener-Modul `nubus-provisioning.py` benachrichtigt den *Provisioning Service*. Es läuft nur auf Primary Directory Node.

Provisioning UDM Transformer

Der *Provisioning UDM Transformer* wandelt auf LDAP-Ebene eingehende Änderungsereignisse durch Aufruf der *UDM-HTTP-REST-API* um in Provisioning-Ereignisse auf UDM-Ebene. Er läuft nur auf Primary Directory Node.

Provisioning Prefill Service

Der *Provisioning Prefill Service* überträgt alle UDM-Objekte des abonnierten Typs an die abonnierte Verbraucher-App. Er läuft nur auf dem Primary Directory Node.

Provisioning Dispatcher

Der *Provisioning Dispatcher* leitet Ereignisse über alle UDM-Objekte an die Provisionierungs-Queues der abonnierten Apps weiter. Er läuft auf Primary Directory Node and Backup Directory Node.

Provisioning API

Die *Provisioning-API* läuft auf Primary Directory Node und Backup Directory Node und ist die API, die Anwendungen zum Abonnieren von Ereignissen verwenden.

NATS

NATS realisiert das eigentliche Event-Streaming.

Auf dem Backup Directory Node verbindet sich der *Provisioning Dispatcher* mit dem **NATS**-Dienst, der auf dem Primary Directory Node läuft. Er überträgt Daten über eine TLS-verschlüsselte Verbindung.

Siehe auch

Provisioning Service⁷⁷

in *Nubus for Kubernetes - Architecture Manual 1.x* [3] für Informationen über die Architektur des *Provisioning Service*

Provisioning API⁷⁸

in *Nubus - Customization and Modification Manual 1.x* [4] für Informationen darüber, wie der *Provisioning Service* verwendet und ein Abonnement für einen *Provisioning Consumer*“ erstellt wird.

3.5.3 Endpunkte und Ports

Der *Provisioning Service* stellt Endpunkte und Ports bereit, wie in [Tab. 3.1](#) beschrieben.

Sie können auf die *Provisioning-API* lokal über `http://localhost:7777`“ oder remote über `https://<Primary FQDN>/univention/provisioning/` zugreifen.

Tab. 3.1: Endpunkte und Ports

Port	Zweck
4230	Der stunnel -Port. Sie können ihn über die UCR-Variable <code>nats/stunnel/accept/port</code> (Seite 18) anpassen.
4222	NATS-Client-Verbindungen.“
7777	Provisioning API.
8222	NATS Monitoring Endpunkt.“

Wichtig

Der *Provisioning Dispatcher* benötigt Zugriff auf die *UDM HTTP REST API* auf Port 443 auf Primary Directory Node und Backup Directory Node.

3.5.4 Provisioning Service Logdateien

Wenn Sie Probleme mit dem *Provisioning Service* haben, können Sie die folgenden Logdateien konsultieren:

- Die Container des *Provisioning Service* schreiben ihre Meldungen nach `/var/log/syslog`.
- Das Listener-Modul `nubus-provisioning.py`, das den *Provisioning Service* mit Informationen versorgt, schreibt Meldungen nach `/var/log/univention/listener_modules/nubus-provisioning.log`.
- Der Dienst **stunnel**, der die TLS-Verschlüsselung zwischen Primary Directory Node und Backup Directory Node sicherstellt, schreibt Meldungen in die Datei `/var/log/stunnel4/stunnel.log`.

3.5.5 Provisioning Service Einstellungen

Die folgenden Referenzen zeigen die verfügbaren Einstellungen innerhalb der *Provisioning Service*-App. Univention empfiehlt, die Standardwerte beizubehalten.

⁷⁷ <https://docs.software-univention.de/nubus-kubernetes-architecture/latest/en/components/provisioning-service.html#component-provisioning-service>

⁷⁸ <https://docs.software-univention.de/nubus-customization/latest/en/api/provisioning.html#customization-api-provisioning>

Um die Einstellungen nach der Installation der App zu ändern, melden Sie sich beim UCS-Verwaltungssystem mit einem Benutzerkonto aus der Gruppe `Domain Admins` an und gehen Sie zu: *App Center* ▶ *Provisioning Service* ▶ *Installationen verwalten* ▶ *Instanz per Checkbox auswählen* ▶ ... *Mehr* ▶ *App-Einstellungen*. Auf der Seite *Konfigurieren Provisioning Service* können Sie die Einstellungen ändern und diese auf die App anwenden, indem Sie auf *Änderungen anwenden* klicken.

Das App Center *reinitialisiert* dann die Docker-Container für die *Provisioning Service*-App oder startet sie neu. *Reinitialisieren* bedeutet, dass das App Center die laufenden Container, aus denen die App besteht, verwirft und einen neuen Satz von Containern erstellt, basierend auf den gerade geänderten Einstellungen.

Für einige Einstellungsänderungen müssen Sie den `univention-directory-listener` neu starten. Führen Sie den Befehl in [Quellcode 3.2](#) aus.

Quellcode 3.2: *Directory Listener* neu starten

```
$ systemctl restart univention-directory-listener
```

App-Settings

Die *Provisioning Service* app bietet die folgenden App-Settings.

`provisioning-service/udm-rest-api-host`

Vollqualifizierter Domänenname (FQDN) des UDM-REST-API-Hosts.

Notwendig	Voreinstellung	Gesetzt
Ja	Wert von <code>ldap/master</code> (Seite 159)	Installation und App-Konfiguration

`provisioning-service/primary`

Vollqualifizierter Domänenname (FQDN) des Primary Directory Node.

Notwendig	Voreinstellung	Gesetzt
Ja	Wert von <code>ldap/master</code> (Seite 159)	Installation und App-Konfiguration

`nats/max_retry_count`

Anzahl der Wiederholungen, die der *Provisioning Listener* (Seite 15) versucht, jede Transaktion mit dem Provisionierungs-NATS-Dienst zu synchronisieren. Nachdem Sie diese Einstellung geändert haben, müssen Sie den `univention-directory-listener` neu starten, siehe [Quellcode 3.2](#).

Notwendig	Voreinstellung	Gesetzt
Ja	3	Installation und App-Konfiguration

`nats/retry_delay`

Die Anzahl der Sekunden, die zwischen jedem Versuch zur Synchronisierung einer Transaktion mit dem Provisionierungs-NATS-Dienst gewartet werden soll. Nachdem Sie diese Einstellung geändert haben, müssen Sie den `univention-directory-listener` neu starten, siehe [Quellcode 3.2](#).

Notwendig	Voreinstellung	Gesetzt
Ja	1	Installation und App-Konfiguration

`nats/max_reconnect_attempts`

Die maximale Anzahl von Versuchen, die Verbindung zum NATS-Dienst wiederherzustellen. Nachdem Sie diese Einstellung geändert haben, müssen Sie den `univention-directory-listener` neu starten, siehe [Quellcode 3.2](#).

Notwendig	Voreinstellung	Gesetzt
Ja	3	Installation und App-Konfiguration

UCR-Variablen

Zusätzlich berücksichtigt der *Provisioning Service* die folgenden UCR-Variablen, die nicht in den App-Einstellungen erscheinen. Univention empfiehlt, die Standardwerte beizubehalten.

nats/stunnel/accept/port

Empfangs-Portnummer des **stunnel**, der die **NATS**-Verbindung zwischen Primary Directory Node und Backup Directory Node sichert.

Notwendig	Voreinstellung	Gesetzt
Ja	4230	Installation und App-Konfiguration.

nats/stunnel/connect/port

Verbindungsport des **stunnel**, der die Verbindung sichert zwischen einem *Provisioning Dispatcher* auf Backup Directory Node und **NATS** auf Primary Directory Node. Muss mit dem *nats/stunnel/accept/port* (Seite 18) des Primary Directory Node übereinstimmen.

Notwendig	Voreinstellung	Gesetzt
Ja	4230	Installation und App-Konfiguration.

nats/stunnel/cert

Zertifikat für die **stunnel NATS**-Verbindung zwischen einem *Provisioning Dispatcher* auf einem Backup Directory Node und **NATS** auf Primary Directory Node.

Notwendig	Voreinstellung	Gesetzt
Ja	/etc/univention/ssl/@%ldap/ master@%/cert.pem	Installation und App-Konfiguration.

nats/stunnel/key

Zertifikatsschlüssel, der für die Verbindung zwischen *Provisioning Dispatcher* auf einem Backup Directory Node und **NATS** auf Primary Directory Node verwendet wird.

Notwendig	Voreinstellung	Gesetzt
Ja	/etc/univention/ssl/@%ldap/ master@%/private.key	Installation und App-Konfiguration.

nats/stunnel/cacert

Das CA-Zertifikat, das für die Verbindung zwischen *Provisioning Dispatcher* auf einem Backup Directory Node und **NATS** auf Primary Directory Node verwendet wird.

Notwendig	Voreinstellung	Gesetzt
Ja	/etc/univention/ssl/ucsCA/ CAcert.pem	Installation und App-Konfiguration.

3.6 SSL-Zertifikatsverwaltung

Der Inhalt dieses Abschnitts wurde nach [Zertifikatsverwaltung](#)⁷⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.7 Kerberos

Der Inhalt dieses Abschnitts wurde nach [Kerberos](#)⁸⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.7.1 KDC Auswahl

Der Inhalt dieses Abschnitts wurde nach [KDC Auswahl](#)⁸¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.7.2 Kerberos Adminserver

Der Inhalt dieses Abschnitts wurde nach [Kerberos-Administrations-Server](#)⁸² in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.8 Passwort-Hashes im Verzeichnisdienst

Der Inhalt dieses Abschnitts wurde nach [Passwort-Hashes](#)⁸³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.9 Single Sign-On

UCS bietet *Single Sign-On*-Funktionalität mit einem mit SAML 2.0 und OpenID Connect kompatiblen, auf **Keycloak** aufsetzenden Identity Provider. UCS installiert diesen Identity Provider standardmäßig nicht. Falls Sie einen Identity Provider benötigen, müssen Sie die App *Keycloak* über das Univention App Center installieren. Informationen, wie man eine App installiert, finden Sie unter *Installation/Deinstallation von UCS-Komponenten im Univention App Center* (Seite 33).

Eine umfangreiche Dokumentation, die die Konfiguration der **Keycloak** App, das Anlegen von Clients und mehr beschreibt, finden Sie unter [Introduction](#)⁸⁴ im *Univention Keycloak app documentation* [5].

3.10 Umwandlung eines Backup Directory Node zum neuen Primary Directory Node

Der Inhalt dieses Abschnitts wurde nach [Redundanz und Failover für den Primary Directory Node](#)⁸⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

3.11 Fehlertolerante Domain Einrichtung

Der Inhalt dieses Abschnitts wurde nach [Einrichtung einer fehlertoleranten Domäne](#)⁸⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

⁷⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/tls.html#domain-infrastructure-tls>

⁸⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/kerberos.html#domain-infrastructure-kerberos>

⁸¹ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/kerberos.html#domain-infrastructure-kerberos-kdc>

⁸² <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/kerberos.html#domain-infrastructure-kerberos-administration-server>

⁸³ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/password-hashes.html#password-management-hashes>

⁸⁴ <https://docs.software-univention.de/keycloak-app/latest/index.html#doc-entry>

⁸⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ha.html#deployment-primary-dn-resilience>

⁸⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/ha.html#deployment-primary-dn-resilience-fault-tolerant-setup>

3.12 Protokollierung von Aktivitäten in der Domäne

Der Inhalt dieses Abschnitts wurde nach [Protokollierung von Aktivitäten in der Domäne](#)⁸⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

⁸⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/domain-infrastructure/activity-logging.html#domain-activity-logging>

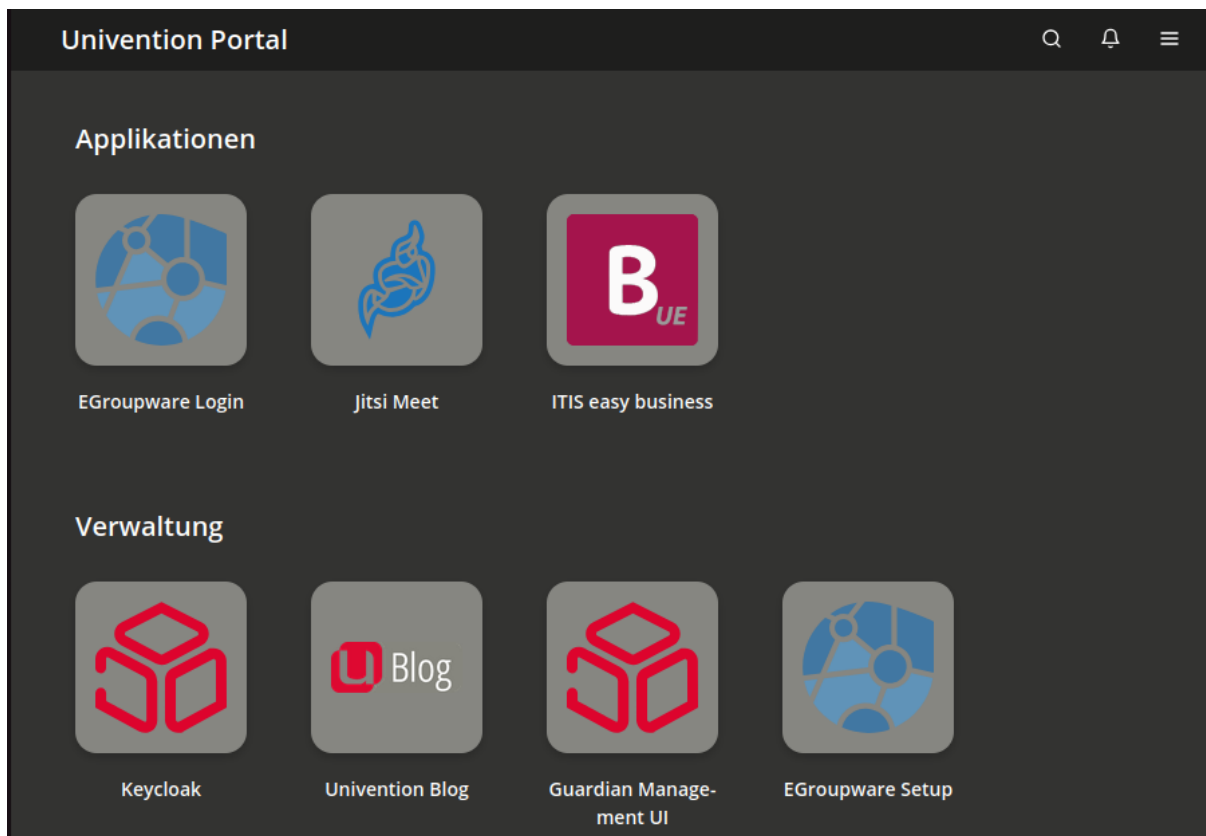


Abb. 4.1: UCS Portalseite

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) oder das Benutzermenü (drei Balken) geöffnet werden (dort kann man sich auch anmelden). 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 (*Anmelden* (Seite 23)).

Zentraler Ausgangspunkt für Benutzer sowie Administratoren für alle weiteren Operationen ist die UCS-Portalseite (siehe *UCS Portalseite* (Seite 21)). Die Portalseite ist standardmäßig auf allen Systemrollen verfügbar und erlaubt einen Überblick über alle in der UCS-Domäne installierten Apps und weiteren Dienste. Alle Aspekte der Portalseite können umfangreich an die eigenen Bedürfnisse angepasst werden (*UCS Portalseite* (Seite 24)).

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 z.B. durch UMC-Module Anpassungen an lokalen Einstellungen vorzunehmen.

Univention Management Console (UMC) Module sind das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne, dessen generelle Funktionsweise in *Univention Management Console-Module* (Seite 25) beschrieben wird. Für die Administration der unterschiedlichen Aspekte einer Domäne werden je nach Systemrolle verschiedene Module bereit gestellt. Zusätzlich installierte Software-Komponenten können ihre eigenen UMC-Module mitbringen.

Die anschließenden Abschnitte vertiefen die Benutzung einzelner Aspekte der Domänenverwaltung. *LDAP-Verzeichnis-Browser* (Seite 26) gibt einen Überblick über den LDAP-Verzeichnis-Browser. Die Anwendung von administrativen Einstellungen über Richtlinien wird in *Richtlinien* (Seite 27) besprochen. Wie genau der Funktionsumfang der Domänenverwaltung erweitert werden kann, ist in *Erweiterung von UMC-Modulen mit erweiterten Attributen* (Seite 27) beschrieben. *Strukturierung der Domäne durch angepasste LDAP-Strukturen* (Seite 28) vertieft, wie Container und Organisationseinheiten (OU) zur Strukturierung des LDAP-Verzeichnisses genutzt werden können. *Delegierte Administration für UMC-Module* (Seite 28) erläutert das Delegieren von Administrationsrechten an weitere Benutzergruppen.

Abschließend wird die Kommandozeilenschnittstelle der Domänenverwaltung dargestellt (*Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)* (Seite 28)) und das Auswerten von Domänenendaten über die UCS-Reporting-Funktionalität erläutert (*Auswertung von Daten aus dem LDAP-Verzeichnis mit Univention Directory Reports* (Seite 29)).

Bemerkung

Das UCS Web-Oberfläche ist Teil von Univention Nubus in der *Management UI* Komponente. Weitere Informationen zu Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 1).

4.1 Einführung

4.1.1 Zugriff

Der Inhalt dieses Abschnitts ist umgezogen nach *Anmeldung*⁸⁸ in *Nubus Handbuch 1.x* [6].

4.1.2 Browserunterstützung

Der Inhalt dieses Abschnitts ist umgezogen nach *Browser-Kompatibilität*⁸⁹ in *Nubus Handbuch 1.x* [6].

4.1.3 Zwischen dunklem und hellem Theme für UCS Web-Oberflächen umschalten

Der Inhalt dieses Abschnitts ist umgezogen nach *Zwischen hellem und dunklem Design wechseln*⁹⁰ in *Univention Corporate Server - Operation Manual* [1].

⁸⁸ <https://docs.software-univention.de/nubus-manual/latest/de/auth.html#nubus-authentication-sign-in>

⁸⁹ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-browser-compatibility>

⁹⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/theme.html#management-interface-theming-light-dark>

4.1.4 Erstellen eines eigenen Themes/Anpassen des Designs von UCS Web-Oberflächen

Der Inhalt dieses Abschnitts ist umgezogen nach [Ein benutzerdefiniertes Design erstellen](#)⁹¹ in *Univention Corporate Server - Operation Manual* [1].

4.1.5 Feedback zu UCS

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

4.1.6 Erfassung von Nutzungsstatistiken

Bei Verwendung der *Core Edition* von UCS (wird generell zur Evaluierung von UCS verwendet) werden anonyme Nutzungsstatistiken zur Verwendung der UCS Web-Oberfläche erzeugt. Weitere Informationen finden sich in [KB 6701 - Data collection in Univention Corporate Server](#)⁹².

4.2 Anmelden

Der Inhalt dieses Abschnitts ist umgezogen nach [Anmeldung](#)⁹³ in *Nubus Handbuch 1.x* [6] und [Wählen Sie das richtige Benutzerkonto](#)⁹⁴ in *Univention Corporate Server - Operation Manual* [1].

4.2.1 Portal Tabs bei Abmeldung aktualisieren

Der Inhalt dieses Abschnitts ist umgezogen nach [Browser-Reiter bei Abmeldung aktualisieren](#)⁹⁵ in *Univention Corporate Server - Operation Manual* [1].

4.2.2 Wählen Sie das richtige Benutzerkonto

Der Inhalt dieses Abschnitts ist umgezogen nach [Wählen Sie das richtige Benutzerkonto](#)⁹⁶ in *Univention Corporate Server - Operation Manual* [1].

4.2.3 Single Sign-On

Der Inhalt dieses Abschnitts ist umgezogen nach [Single Sign-On](#)⁹⁷ in *Univention Corporate Server - Operation Manual* [1].

SAML für Single Sign-On

Der Inhalt dieses Abschnitts ist umgezogen nach [SAML-Konfiguration für Single Sign-On](#)⁹⁸ in *Univention Corporate Server - Operation Manual* [1].

OpenID Connect für Single Sign-On

Der Inhalt dieses Abschnitts ist umgezogen nach [OpenID Connect für Single Sign-On](#)⁹⁹ in *Univention Corporate Server - Operation Manual* [1].

⁹¹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/theme.html#management-interface-theming-custom>

⁹² <https://help.univention.com/t/6701>

⁹³ <https://docs.software-univention.de/nubus-manual/latest/de/auth.html#nubus-authentication-sign-in>

⁹⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sign-in-choose-account>

⁹⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#nubus-authentication-sign-out-refresh-tabs>

⁹⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sign-in-choose-account>

⁹⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso>

⁹⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-saml>

⁹⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc>

Aktivierung

Der Inhalt dieses Abschnitts ist umgezogen nach [OpenID Connect für Single Sign-On aktivieren](#)¹⁰⁰ in *Univention Corporate Server - Operation Manual* [1].

AnmeldeLinks erstellen

Der Inhalt dieses Abschnitts ist umgezogen nach [AnmeldeLinks erstellen](#)¹⁰¹ in *Univention Corporate Server - Operation Manual* [1].

Verifizierung und Logdateien

Der Inhalt dieses Abschnitts ist umgezogen nach [Überprüfung und Protokolldateien](#)¹⁰² in *Univention Corporate Server - Operation Manual* [1].

Deaktivieren

Der Inhalt dieses Abschnitts ist umgezogen nach [OpenID Connect für Single Sign-On deaktivieren](#)¹⁰³ in *Univention Corporate Server - Operation Manual* [1].

Identity Provider mit nicht standardmäßigem FQDN

Der Inhalt dieses Abschnitts ist umgezogen nach [Identitätsanbieter mit nicht standardmäßigem FQDN](#)¹⁰⁴ in *Univention Corporate Server - Operation Manual* [1].

Univention Portal und UMC mit nicht standardmäßigem FQDN

Der Inhalt dieses Abschnitts ist umgezogen nach [Nicht standardmäßiger FQDN für das Univention Portal und die Management UI](#)¹⁰⁵ in *Univention Corporate Server - Operation Manual* [1].

Back-Channel Abmeldung

Der Inhalt dieses Abschnitts ist umgezogen nach [Back-Channel Abmeldung](#)¹⁰⁶ in *Univention Corporate Server - Operation Manual* [1].

4.3 UCS Portalseite

Der Inhalt dieses Abschnitts ist umgezogen nach [Univention Portal](#)¹⁰⁷ in *Nubus Handbuch 1.x* [6].

4.3.1 Rechte für Portaleinstellungen vergeben

Der Inhalt dieses Abschnitts ist umgezogen nach [Berechtigungen für Portaleinstellungen](#)¹⁰⁸ in *Nubus Handbuch 1.x* [6].

4.4 Zustimmung zur Verwendung von Cookies

Der Inhalt dieses Abschnitts ist umgezogen nach [Einwilligung zur Verwendung von Cookies](#)¹⁰⁹ in *Univention Corporate Server - Operation Manual* [1].

¹⁰⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-activate>

¹⁰¹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-sign-in-links>

¹⁰² <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-verification>

¹⁰³ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-deactivate>

¹⁰⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-non-standard-fqdn>

¹⁰⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-non-standard-fqdn-portal>

¹⁰⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/auth.html#management-interface-auth-sso-oidc-back-channel-sign-out>

¹⁰⁷ <https://docs.software-univention.de/nubus-manual/latest/de/portal.html#nubus-portal>

¹⁰⁸ <https://docs.software-univention.de/nubus-manual/latest/de/portal.html#nubus-portal-settings-permissions>

¹⁰⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/cookie-consent.html#management-interface-cookie-consent>

4.5 Univention Management Console-Module

Univention Management Console-Module (UMC-Module) sind das zentrale Werkzeug zur webbasierten Administration der UCS-Domäne. Sie werden auf der Portalseite (*UCS Portalseite* (Seite 24)) für angemeldete Administratoren angezeigt. Je nach Systemrolle sind unterschiedliche UMC-Module verfügbar. Zusätzlich installierte Software-Komponenten können ihre eigenen neuen UMC-Module mitbringen.

UMC-Module zur Verwaltung aller im LDAP-Verzeichnis vorgehaltenen Daten (wie z.B. Benutzer, Gruppen oder Rechnerkonten) werden lediglich auf einem Primary Directory Node und Backup Directory Node 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 z.B. zusätzliche Applikationen installiert, Aktualisierungen eingespielt, die lokale Konfiguration über Univention Configuration Registry angepasst oder Dienste gestartet/gestoppt werden.

4.5.1 Aktivierung der UCS-Lizenz / Lizenz-Übersicht

Der Inhalt dieses Abschnitts ist umgezogen nach *UCS-Lizenz aktivieren*¹¹⁰ in *Univention Corporate Server - Operation Manual* [1].

4.5.2 Bedienung der Module zur Verwaltung von LDAP-Verzeichnisdaten

Alle UMC-Module zur Verwaltung von LDAP-Objekten wie z.B. Benutzer-, Gruppen- und Rechnerkonten oder Einstellungen für Drucker, Freigaben, Mail 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 *Konfiguration der DNS-Daten über Univention Management Console Modul* (Seite 97) und *Aufbau der DHCP-Konfiguration durch DHCP-LDAP-Objekte* (Seite 99).

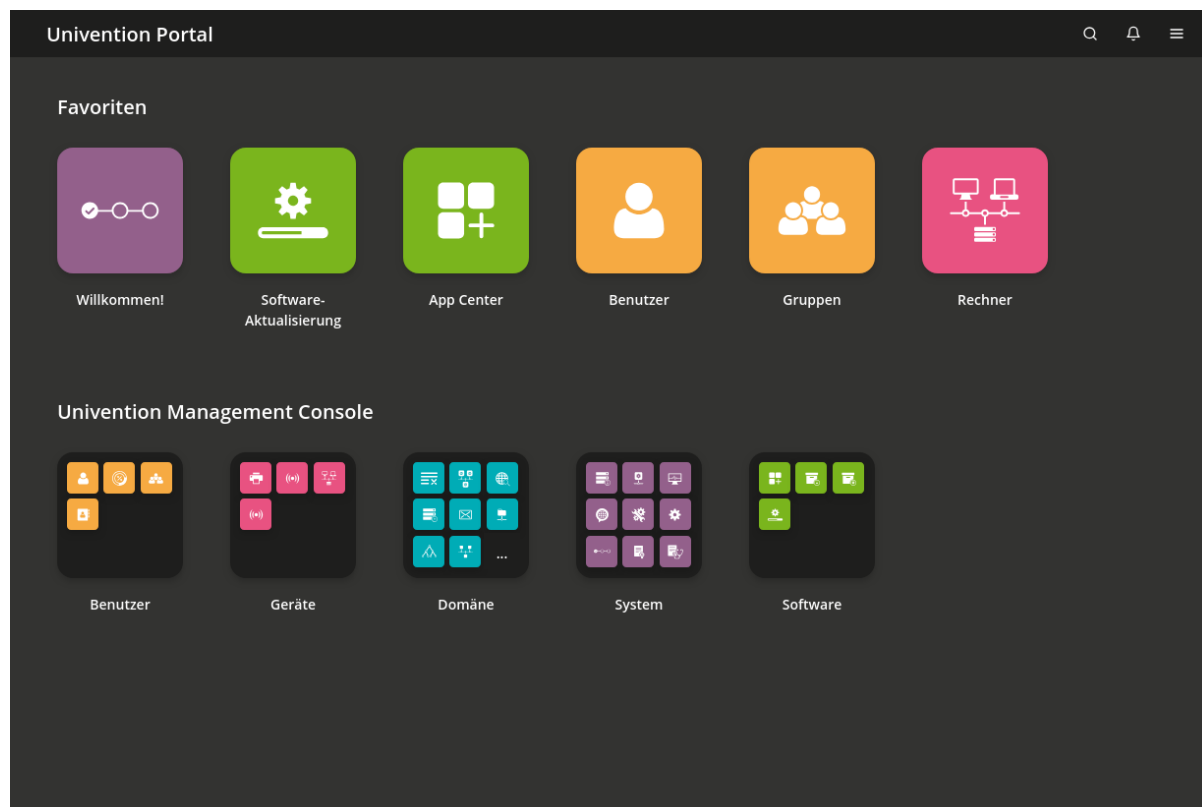


Abb. 4.2: Modulübersicht

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

¹¹⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/license.html#management-interface-license>

- Benutzer - *Benutzerverwaltung* (Seite 35)
- Gruppen - *Gruppenverwaltung* (Seite 45)
- Rechner - *Rechnerverwaltung* (Seite 47)
- Netzwerke - *IP- und Netzverwaltung* (Seite 95)
- DNS - *Verwaltung von DNS-Daten mit BIND* (Seite 95)
- DHCP - *IP-Vergabe über DHCP* (Seite 98)
- Freigaben - *Verwaltung von Freigaben* (Seite 113)
- Drucker - *Druckdienste* (Seite 119)
- E-Mail - *Maildienste* (Seite 127)
- Nagios - *Nagios* (Seite 150)

Die Verwendung von Richtlinien (*Richtlinien* (Seite 27)) und das direkte Durchsuchen des LDAP-Verzeichnisbaums (*LDAP-Verzeichnis-Browser* (Seite 26)) werden separat beschrieben.

Suche nach Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [Nach Objekten suchen](#)¹¹¹ in *Nubus Handbuch 1.x* [6].

Anlegen von Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [Objekte erstellen](#)¹¹² in *Nubus Handbuch 1.x* [6].

Bearbeiten von Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [Objekte bearbeiten](#)¹¹³ in *Nubus Handbuch 1.x* [6].

Löschen von Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [Objekte löschen](#)¹¹⁴ in *Nubus Handbuch 1.x* [6].

Verschieben von Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [Objekte verschieben](#)¹¹⁵ in *Nubus Handbuch 1.x* [6].

4.5.3 Anzeige von Systembenachrichtigungen

Der Inhalt dieses Abschnitts ist umgezogen nach [System-Benachrichtigungen anzeigen](#)¹¹⁶ in *Nubus Handbuch 1.x* [6].

4.6 LDAP-Verzeichnis-Browser

Der Inhalt dieses Abschnitts ist umgezogen nach [LDAP Verzeichnis Modul](#)¹¹⁷ in *Nubus Handbuch 1.x* [6].

¹¹¹ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-management-modules-operations-search>

¹¹² <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-management-modules-operations-create>

¹¹³ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-management-modules-operations-edit>

¹¹⁴ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-management-modules-operations-delete>

¹¹⁵ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-management-modules-operations-move>

¹¹⁶ <https://docs.software-univention.de/nubus-manual/latest/de/ui.html#nubus-ui-notifications>

¹¹⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/ldap.html#nubus-domain-ldap>

4.7 Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Anmeldung](#)¹¹⁸ in *Nubus Handbuch 1.x* [6].

4.7.1 Anlegen einer Richtlinie

Der Inhalt dieses Abschnitts ist umgezogen nach [Eine Richtlinie erstellen](#)¹¹⁹ in *Nubus Handbuch 1.x* [6].

4.7.2 Zuweisung von Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Richtlinien zuweisen](#)¹²⁰ in *Nubus Handbuch 1.x* [6].

4.7.3 Bearbeiten einer Richtlinie

Der Inhalt dieses Abschnitts ist umgezogen nach [Richtlinien bearbeiten](#)¹²¹ in *Nubus Handbuch 1.x* [6].

4.8 Erweiterung von UMC-Modulen mit erweiterten Attributen

Der Inhalt dieses Abschnitts ist umgezogen nach [Verwaltungsmodule erweitern](#)¹²² in *Nubus Handbuch 1.x* [6].

4.8.1 Erweiterte Attribute - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Allgemein - erweiterte Attribute](#)¹²³ in *Nubus Handbuch 1.x* [6].

4.8.2 Erweiterte Attribute - Reiter Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Modul - erweiterte Attribute](#)¹²⁴ in *Nubus Handbuch 1.x* [6].

4.8.3 Erweiterte Attribute - Reiter LDAP-Abbildung

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter LDAP-Zuordnung - erweiterte Attribute](#)¹²⁵ in *Nubus Handbuch 1.x* [6].

4.8.4 Erweiterte Attribute - Reiter UMC

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter UMC - erweiterte Attribute](#)¹²⁶ in *Nubus Handbuch 1.x* [6].

4.8.5 Erweiterte Attribute - Reiter Datentyp

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Datentyp - erweiterte Attribute](#)¹²⁷ in *Nubus Handbuch 1.x* [6].

¹¹⁸ <https://docs.software-univention.de/nubus-manual/latest/de/auth.html#nubus-authentication-sign-in>

¹¹⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/policies.html#nubus-domain-policies-create>

¹²⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/policies.html#nubus-domain-policies-assign>

¹²¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/policies.html#nubus-domain-policies-edit>

¹²² <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes>

¹²³ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes-tab-general>

¹²⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes-tab-module>

¹²⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes-tab-ldap-mapping>

¹²⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes-tab-umc>

¹²⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/extend.html#nubus-domain-extended-attributes-tab-data-type>

4.9 Strukturierung der Domäne durch angepasste LDAP-Strukturen

Der Inhalt dieses Abschnitts ist umgezogen nach [Benutzerdefinierte LDAP-Strukturen](#)¹²⁸ in *Nubus Handbuch 1.x* [6].

4.9.1 Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Allgemein - LDAP Verzeichnis](#)¹²⁹ in *Nubus Handbuch 1.x* [6].

4.9.2 Reiter Erweiterte Einstellungen

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Erweiterte Einstellungen - LDAP Verzeichnis](#)¹³⁰ in *Nubus Handbuch 1.x* [6].

4.9.3 Reiter Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Richtlinien - LDAP Verzeichnis](#)¹³¹ in *Nubus Handbuch 1.x* [6].

4.10 Delegierte Administration für UMC-Module

Der Inhalt dieses Abschnitts ist umgezogen nach [Delegierte Administration für Verwaltungsmodule](#)¹³² in *Univention Corporate Server - Operation Manual* [1].

4.11 Kommandozeilenschnittstelle der Domänenverwaltung (Univention Directory Manager)

Der Inhalt dieses Abschnitts ist umgezogen nach [Befehlszeilenschnittstelle für die Domänenverwaltung](#)¹³³ in *Univention Corporate Server - Operation Manual* [1].

4.11.1 Aufrufparameter der Kommandozeilenschnittstelle

Der Inhalt dieses Abschnitts ist umgezogen nach [Parameter der Befehlszeilenschnittstelle](#)¹³⁴ in *Univention Corporate Server - Operation Manual* [1].

4.11.2 Beispielaufrufe für die Kommandozeilenschnittstelle

Der Inhalt dieses Abschnitts ist umgezogen nach [Beispiele für die Befehlszeilenschnittstelle](#)¹³⁵ in *Univention Corporate Server - Operation Manual* [1].

¹²⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/ldap.html#nubus-domain-ldap-user-defined-structure>

¹²⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/ldap.html#nubus-domain-ldap-user-defined-structure-tab-general>

¹³⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/ldap.html#nubus-domain-ldap-user-defined-structure-tab-advanced>

¹³¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/ldap.html#nubus-domain-ldap-user-defined-structure-tab-policies>

¹³² <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/delegated-administration.html#management-interface-delegated-administration>

management-interface-delegated-administration

¹³³ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command>

¹³⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-parameters>

¹³⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples>

Benutzer

Der Inhalt dieses Abschnitts ist umgezogen nach [Benutzer](#)¹³⁶ in *Univention Corporate Server - Operation Manual* [1].

Gruppen

Der Inhalt dieses Abschnitts ist umgezogen nach [Gruppen](#)¹³⁷ in *Univention Corporate Server - Operation Manual* [1].

Container / Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Container](#)¹³⁸ und [Richtlinien](#)¹³⁹ in *Univention Corporate Server - Operation Manual* [1].

Rechner

Der Inhalt dieses Abschnitts ist umgezogen nach [Computer](#)¹⁴⁰ in *Univention Corporate Server - Operation Manual* [1].

Freigaben

Der Inhalt dieses Abschnitts ist umgezogen nach [Freigaben](#)¹⁴¹ in *Univention Corporate Server - Operation Manual* [1].

Drucker

Der Inhalt dieses Abschnitts ist umgezogen nach [Drucker](#)¹⁴² in *Univention Corporate Server - Operation Manual* [1].

DNS/DHCP

Der Inhalt dieses Abschnitts ist umgezogen nach [DNS](#) und [DHCP](#)¹⁴³ in *Univention Corporate Server - Operation Manual* [1].

Erweiterte Attribute

Der Inhalt dieses Abschnitts ist umgezogen nach [Erweiterte Attribute](#)¹⁴⁴ in *Univention Corporate Server - Operation Manual* [1].

4.12 HTTP Schnittstelle (API) der Domänenverwaltung

Der Inhalt dieses Abschnitts ist umgezogen nach [HTTP Schnittstelle für Domänenverwaltung](#)¹⁴⁵ in *Univention Corporate Server - Operation Manual* [1].

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

Der Inhalt dieses Abschnitts ist umgezogen nach [Verzeichnisberichte](#)¹⁴⁶ in *Univention Corporate Server - Operation Manual* [1].

¹³⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-users>

¹³⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-groups>

¹³⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-contain>

¹³⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-policies>

¹⁴⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-comput>

¹⁴¹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-shares>

¹⁴² <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-printers>

¹⁴³ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-dns-dh>

¹⁴⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/udm-command.html#management-interface-udm-command-examples-extends>

¹⁴⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/http-api.html#iam-http-api>

¹⁴⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/directory-reports.html#management-interface-directory-reports>

4.13.1 Erstellen von Reports in Univention Management Console-Modulen

Der Inhalt dieses Abschnitts ist umgezogen nach Erstellen Sie Berichte über Verwaltungsmodule¹⁴⁷ in *Univention Corporate Server - Operation Manual* [1].

4.13.2 Erstellen von Reports auf der Kommandozeile

Der Inhalt dieses Abschnitts ist umgezogen nach Erstellen Sie Berichte über die Befehlszeile¹⁴⁸ in *Univention Corporate Server - Operation Manual* [1].

4.13.3 Anpassung/Erweiterung von Univention Directory Reports

Der Inhalt dieses Abschnitts ist umgezogen nach Passen Sie Berichte an¹⁴⁹ in *Univention Corporate Server - Operation Manual* [1].

4.14 Let's Encrypt

Der Inhalt dieses Abschnitts ist umgezogen nach Let's Encrypt¹⁵⁰ in *Univention Corporate Server - Operation Manual* [1].

¹⁴⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/directory-reports.html#management-interface-directory-reports-create-umc>

¹⁴⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/directory-reports.html#management-interface-directory-reports-create-cli>

¹⁴⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/directory-reports.html#management-interface-directory-reports-customize>

¹⁵⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/lets-encrypt.html#lifecycle-lets-encrypt>

Die in UCS integrierte Softwareverteilung bietet umfangreiche Möglichkeiten für den Rollout und die Aktualisierung von UCS-Installationen. Sicherheits- und Versionsupdates können über das UMC-Modul *Software-Aktualisierung*, über ein Kommandozeilen-Tool und richtliniengesteuert installiert werden. Dies wird in *Aktualisierung von UCS-Systemen* (Seite 32) 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 *Konfiguration des Repository-Servers für Updates und Paketinstallationen* (Seite 32)).

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 *Installation weiterer Software* (Seite 33) vorgestellt. Die Installation von Versions- und Sicherheitsupdates kann über Richtlinien automatisiert werden, siehe *Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie* (Seite 34).

Mit dem Software-Monitor steht ein Werkzeug zur Verfügung, mit dem alle Paketinstallationsstände zentral in einer Datenbank erfasst werden, siehe *Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor* (Seite 34).

Die Erstinstallation von UCS-Systemen ist nicht Bestandteil dieses Kapitels, sie wird stattdessen in *Installation* (Seite 5) beschrieben.

5.1 Unterscheidung der Update-Varianten / Aufbau der UCS-Versionen

Der Inhalt dieses Abschnitts ist umgezogen nach *Nubus für UCS Versionierung*¹⁵¹ in *Univention Corporate Server - Operation Manual* [1].

5.2 Univention App Center

Der Inhalt dieses Abschnitts ist umgezogen nach *Univention App Center*¹⁵² in *Univention Corporate Server - Operation Manual* [1].

¹⁵¹ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/versioning.html#lifecycle-versioning>

¹⁵² <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/app-center.html#lifecycle-app-center>

5.3 Aktualisierung von UCS-Systemen

Der Inhalt dieses Abschnitts ist umgezogen nach [Update Strategien](#)¹⁵³ in *Univention Corporate Server - Operation Manual* [1].

5.3.1 Update-Strategie in Umgebungen mit mehr als einem UCS-System

Der Inhalt dieses Abschnitts ist umgezogen nach [Planen Sie Updates in Multiserver Umgebungen](#)¹⁵⁴ in *Univention Corporate Server - Operation Manual* [1].

5.3.2 Aktualisierung eines einzelnen Systems im Univention Management Console Modul Software-Aktualisierung

Der Inhalt dieses Abschnitts ist umgezogen nach [Update über das Verwaltungsmodul](#)¹⁵⁵ in *Univention Corporate Server - Operation Manual* [1].

5.3.3 Aktualisierung eines einzelnen Systems auf der Kommandozeile

Der Inhalt dieses Abschnitts ist umgezogen nach [Update über die Befehlszeile](#)¹⁵⁶ in *Univention Corporate Server - Operation Manual* [1].

5.3.4 Aktualisierung von Systemen über eine Rechner-Richtlinie

Der Inhalt dieses Abschnitts ist umgezogen nach [Update über eine Richtlinie](#)¹⁵⁷ in *Univention Corporate Server - Operation Manual* [1].

5.3.5 Fehlersuche bei Updateproblemen

Der Inhalt dieses Abschnitts ist umgezogen nach [Fehlerbehebung bei Update-Problemen](#)¹⁵⁸ in *Univention Corporate Server - Operation Manual* [1].

5.4 Konfiguration des Repository-Servers für Updates und Paketinstallationen

Der Inhalt dieses Abschnitts ist umgezogen nach [Lokale Repository-Server](#)¹⁵⁹ in *Univention Corporate Server - Operation Manual* [1].

5.4.1 Konfiguration über Univention Management Console Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Konfiguration über das Verwaltungsmodul](#)¹⁶⁰ in *Univention Corporate Server - Operation Manual* [1].

5.4.2 Konfiguration über Univention Configuration Registry

Der Inhalt dieses Abschnitts ist umgezogen nach [Konfiguration über die Univention Configuration Registry](#)¹⁶¹ in *Univention Corporate Server - Operation Manual* [1].

¹⁵³ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies>

¹⁵⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies-multiple-systems-environments>

¹⁵⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies-methods-management-module>

¹⁵⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies-methods-command-line>

¹⁵⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies-methods-policy>

¹⁵⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/update-strategies.html#lifecycle-update-strategies-troubleshooting>

¹⁵⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/local-repository-servers.html#lifecycle-local-repository-servers>

¹⁶⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/local-repository-servers.html#lifecycle-local-repository-management-module>

¹⁶¹ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/local-repository-servers.html#lifecycle-local-repository-ucr>

5.4.3 Richtlinienbasierte Konfiguration des Repository-Servers

Der Inhalt dieses Abschnitts ist umgezogen nach [Richtlinienbasierte Konfiguration des Repository-Servers](#)¹⁶² in *Univention Corporate Server - Operation Manual* [1].

5.4.4 Einrichtung und Aktualisierung eines lokalen Repositories

Der Inhalt dieses Abschnitts ist umgezogen nach [Erstellen und Aktualisieren eines lokalen Repositories](#)¹⁶³ in *Univention Corporate Server - Operation Manual* [1].

5.5 Installation weiterer Software

Der Inhalt dieses Abschnitts ist umgezogen nach [Paket-Installation und -Verwaltung](#)¹⁶⁴ in *Univention Corporate Server - Operation Manual* [1].

5.5.1 Installation/Deinstallation von UCS-Komponenten im Univention App Center

Der Inhalt dieses Abschnitts ist umgezogen nach [Installation mittels Univention App Center](#)¹⁶⁵ in *Univention Corporate Server - Operation Manual* [1].

5.5.2 Installation/Entfernung einzelner Pakete über Univention Management Console-Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Installation mittels Management UI](#)¹⁶⁶ in *Univention Corporate Server - Operation Manual* [1].

5.5.3 Installation/Deinstallation von einzelnen Paketen auf der Kommandozeile

Der Inhalt dieses Abschnitts ist umgezogen nach [Installation über die Befehlszeile](#)¹⁶⁷ in *Univention Corporate Server - Operation Manual* [1].

5.5.4 Hook Skripte für Administratoren

Der Inhalt dieses Abschnitts ist umgezogen nach [Automatisieren Sie Aufgaben rund um Aktionen von Apps mit Hook-Skripten](#)¹⁶⁸ in *Univention Corporate Server - Operation Manual* [1].

5.5.5 Richtlinienbasierte Installation/Deinstallation von einzelnen Paketen über Paketlisten

Der Inhalt dieses Abschnitts ist umgezogen nach [Zentralisierte Paket-Verwaltung mit Richtlinien](#)¹⁶⁹ in *Univention Corporate Server - Operation Manual* [1].

¹⁶² <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/local-repository-servers.html#lifecycle-local-repository-policy>

¹⁶³ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/local-repository-servers.html#lifecycle-local-repository-create>

¹⁶⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management>

¹⁶⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management-appcenter>

¹⁶⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management-umc>

¹⁶⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management-commandline>

¹⁶⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management-hooks>

¹⁶⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-installation-management.html#lifecycle-package-installation-management-policy>

5.6 Festlegung eines Aktualisierungszeitpunkts mit der Paketpflege-Richtlinie

Der Inhalt dieses Abschnitts ist umgezogen nach [Richtlinie zur Paketpflege](#)¹⁷⁰ in *Univention Corporate Server - Operation Manual* [1].

5.7 Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor

Der Inhalt dieses Abschnitts ist umgezogen nach [Software-Monitor](#)¹⁷¹ in *Univention Corporate Server - Operation Manual* [1].

¹⁷⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/package-maintenance-policy.html#lifecycle-package-maintenance-policy>

¹⁷¹ <https://docs.software-univention.de/ucs-operation/5.2/de/lifecycle/software-monitor.html#lifecycle-software-monitor>

Benutzerverwaltung

UCS integriert ein zentrales Identity-Management. Alle Benutzerinformationen werden in UCS zentral über das UMC-Modul *Benutzer* verwaltet und im LDAP-Verzeichnisdienst gespeichert.

Bemerkung

Die Benutzerverwaltung ist Teil von Univention Nubus in der *Directory Manager* Komponente. Weitere Informationen zu Nubus finden Sie unter *Was ist Univention Nubus?* (Seite 1)

Alle in die Domäne integrierten Dienste greifen dabei auf die zentralen Kontoinformationen 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.

Arten von Benutzerkonten

In UCS gibt es drei unterschiedliche Arten von Benutzerkonten:

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 *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 36)) 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 *LDAP-Verzeichnis-Browser* (Seite 26)) erstellt werden.

Empfehlung zur Definition von Benutzernamen

Ein sehr wichtiges und erforderliches Attribut für Benutzerkonten ist der Benutzername. Um Konflikte mit den verschiedenen Werkzeugen zu vermeiden, die Benutzerkonten in UCS verarbeiten, folgen Sie diesen Empfehlungen für die Definition von Benutzernamen:

- Verwenden Sie Buchstaben (a-z und A-Z), Ziffern (0-9), Punkte (.), Bindestriche (-) und Unterstriche (_) aus dem ASCII-Zeichensatz in Benutzernamen. Unicode-Zeichen und Umlaute werden ebenfalls unterstützt.
- Der Benutzername muss mit einem Buchstaben, einer Ziffer oder einem Unterstrich beginnen und mit einem Buchstaben, einer Ziffer oder einem Bindestrich enden.
- Verwenden Sie keine Leerzeichen in Benutzernamen.
- Verwenden Sie nicht @, \$ oder einer der folgenden Zeichen " / \ [] : ; | = , + * ? < > ' in Benutzernamen. Diese Zeichen führen zu Fehlern bei der Kerberos-, Active Directory- und Samba-Synchronisation.

Empfohlene Länge von Benutzernamen:

- Um eine breite Kompatibilität mit Windows-Clients und Altsystemen zu gewährleisten, halten Sie Benutzernamen zwischen 4 und 20 Zeichen. Obwohl UCS Benutzernamen mit einem einzelnen Zeichen erlaubt, unterstützen viele externe Systeme diese nicht.
- Benutzernamen mit mehr als 20 Zeichen verursachen Probleme in zwei Situationen:
 - Windows-Clients können sich nicht anmelden, da die Microsoft-Spezifikation den SAM account name auf 20 Zeichen begrenzt.
 - Die Synchronisation mit einer externen Active Directory-Domäne schlägt fehl, da AD das 20-Zeichen-Limit mit einem kritischen Fehler erzwingt.
 - Die *Management UI* zeigt eine Warnung an, wenn ein Benutzername 20 Zeichen überschreitet.

Die traditionelle Empfehlung folgt diesem regulären Ausdruck: `^[a-z][a-z0-9-]{2,18}[a-z0-9]$`. Dieses Muster ist restriktiver als die tatsächliche Validierung im System, die auch Punkte, Unterstriche und Großbuchstaben erlaubt.

Behandeln Sie die zuvor aufgeführten Anforderungen als Richtlinien für breite Kompatibilität, nicht als strikte Durchsetzungsregeln. Beachten Sie mögliche Nebenwirkungen bei der Definition von Benutzernamen außerhalb dieser Richtlinien, besonders bei der Integration mit Altsystemen oder Windows-Clients.

6.1 Verwaltung von Benutzern über Univention Management Console Modul

Dieser Abschnitt beschreibt die Benutzerverwaltung über das UMC-Modul *Benutzer*.

6.1.1 Assistent zur Benutzererstellung

Der Inhalt dieses Abschnitts wurde nach *Assistent zum Erstellen von Benutzern*¹⁷² in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.1.2 Modul Benutzerverwaltung - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach *Reiter Allgemein - Benutzerverwaltung*¹⁷³ in *Nubus Handbuch 1.x* [6].

¹⁷² <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-create-wizard.html#iam-user-create-wizard>

¹⁷³ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/user.html#nubus-user-management-users-tab-general>

6.1.3 Modul Benutzerverwaltung - Reiter Gruppen

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Gruppen - Benutzerverwaltung¹⁷⁴ in *Nubus Handbuch 1.x* [6].

6.1.4 Modul Benutzerverwaltung - Reiter Konto

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Konto - Benutzerverwaltung¹⁷⁵ in *Nubus Handbuch 1.x* [6].

6.1.5 Modul Benutzerverwaltung - Reiter Kontakt

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Kontakt - Benutzerverwaltung¹⁷⁶ in *Nubus Handbuch 1.x* [6].

6.1.6 Modul Benutzerverwaltung - Reiter Mail

Diese Karteikarte wird in den erweiterten Einstellungen angezeigt.

Die Einstellungen sind in *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 128) beschrieben.

6.1.7 Modul Benutzerverwaltung - Reiter Optionen

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Optionen - Benutzerverwaltung¹⁷⁷ in *Nubus Handbuch 1.x* [6].

6.2 Benutzeraktivierung für Apps

Der Inhalt dieses Abschnitts wurde nach Benutzeraktivierung für Apps¹⁷⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.3 Verwaltung der Benutzerpasswörter

Der Inhalt dieses Abschnitts wurde nach Benutzerkennwort-Verwaltung¹⁷⁹ in *Nubus Handbuch 1.x* [6] verschoben.

6.3.1 Arten von Passwortrichtlinien

Der Inhalt dieses Abschnitts wurde nach Passwort-Richtlinientypen¹⁸⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.3.2 Passwortrichtlinieneinstellungen in UMC

Der Inhalt dieses Abschnitts wurde nach Passwort-Richtlinien-Einstellungen¹⁸¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

¹⁷⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/user.html#nubus-user-management-users-tab-groups>

¹⁷⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/user.html#nubus-user-management-users-tab-account>

¹⁷⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/user.html#nubus-user-management-users-tab-contact>

¹⁷⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/user.html#nubus-user-management-users-tab-options>

¹⁷⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-activation-apps.html#iam-user-activation-apps>

¹⁷⁹ <https://docs.software-univention.de/nubus-manual/latest/de/users/password-management.html#nubus-user-password-management>

¹⁸⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/policies.html#password-management-policies-types>

¹⁸¹ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/policies.html#password-management-policies-settings>

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

Der Inhalt dieses Abschnitts wurde nach [Samba-Domänen Passwort-Richtlinie](#)¹⁸² in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.5 Benutzer Selbstverwaltung

Informationen zum Festlegen einer Benutzer-Passwortrichtlinie finden Sie unter *Verwaltung der Benutzerpasswörter* (Seite 37).

6.5.1 Passwortwechsel über UCS Portal

Der Inhalt dieses Abschnitts wurde nach [Benutzerpasswort ändern](#)¹⁸³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.5.2 Passwort-Verwaltung über Self Service App

Der Inhalt dieses Abschnitts wurde nach [Installation und Aktivierung](#)¹⁸⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.5.3 Profilverwaltung

Der Inhalt dieses Abschnitts wurde nach [Kontaktinformationen](#)¹⁸⁵ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.5.4 Selbstregistrierung

Der Inhalt dieses Abschnitts wurde nach [Benutzer-Registrierung](#)¹⁸⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Kontoerstellung

Der Inhalt dieses Abschnitts wurde nach [Registrierungsformular](#)¹⁸⁷ in *Univention Corporate Server - Operation Manual* [1] verschoben.

Verifizierungsmail

Der Inhalt dieses Abschnitts wurde nach [E-Mail-Verifizierung](#)¹⁸⁸ in *Univention Corporate Server - Operation Manual* [1] verschoben.

¹⁸² <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/samba-policies.html#password-management-windows-client>

¹⁸³ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/policies.html#password-management-policies-change>

¹⁸⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-installation>

¹⁸⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-contact-information>

¹⁸⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-registration>

¹⁸⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-registration-registration-form>

¹⁸⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-registration-email-verification>

Kontoverifizierung

Der Inhalt dieses Abschnitts wurde nach [Konto-Aktivierung](#)¹⁸⁹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.5.5 Selbst-Deregistrierung

Der Inhalt dieses Abschnitts wurde nach [Benutzer-Abmeldung](#)¹⁹⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.6 Automatisches Sperren von Benutzern nach fehlgeschlagenen Anmeldungen

Der Inhalt dieses Abschnitts wurde nach [Benutzerkonto-Sperrung nach fehlgeschlagenen Anmeldeversuchen](#)¹⁹¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.6.1 Samba Active Directory Dienste

Der Inhalt dieses Abschnitts wurde nach [Kontosperrung für Samba und Active Directory konfigurieren](#)¹⁹² in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.6.2 PAM-Stack

Der Inhalt dieses Abschnitts wurde nach [Kontosperrung für den PAM-Stack konfigurieren](#)¹⁹³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.6.3 OpenLDAP

Der Inhalt dieses Abschnitts wurde nach [Kontosperrung für den PAM-Stack konfigurieren](#)¹⁹⁴ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.7 Benutzervorlagen

Der Inhalt dieses Abschnitts wurde nach [Benutzerkonto-Vorlagen](#)¹⁹⁵ in *Nubus Handbuch 1.x* [6] verschoben.

6.8 Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos

Der Inhalt dieses Abschnitts wurde nach [Zeitpunkt der letzten Anmeldung erfassen, um inaktive Konten zu erkennen](#)¹⁹⁶ in *Univention Corporate Server - Operation Manual* [1] verschoben.

6.9 Wiederverwendung von Benutzereigenschaften verhindern

Der Inhalt dieses Abschnitts wurde nach [Blocklisten Modul](#)¹⁹⁷ in *Nubus Handbuch 1.x* [6] verschoben.

¹⁸⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-registration-account-activation>

¹⁹⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/password-management/user-self-service.html#end-user-self-service-deregistration>

¹⁹¹ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-lockout.html#iam-user-lockout>

¹⁹² <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-lockout.html#iam-user-lockout-samba>

¹⁹³ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-lockout.html#iam-user-lockout-pam>

¹⁹⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/user-lockout.html#iam-user-lockout-pam>

¹⁹⁵ <https://docs.software-univention.de/nubus-manual/latest/de/users/templates.html#nubus-user-templates>

¹⁹⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/last-bind.html#iam-last-bind>

¹⁹⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/blocklists.html#nubus-domain-blocklists>

6.9.1 Aktivieren von Blocklisten

Der Inhalt dieses Abschnitts wurde nach [Blocklisten aktivieren](#)¹⁹⁸ in *Nubus Handbuch 1.x* [6] verschoben.

6.9.2 Konfigurieren von Blocklisten

Der Inhalt dieses Abschnitts wurde nach [Blocklisten konfigurieren](#)¹⁹⁹ in *Nubus Handbuch 1.x* [6] verschoben.

6.9.3 Einträge in der Blockliste verwalten

Der Inhalt dieses Abschnitts wurde nach [Einträge in der Blockliste verwalten](#)²⁰⁰ in *Nubus Handbuch 1.x* [6] verschoben.

6.9.4 Abgelaufene Blocklisteneinträge

Der Inhalt dieses Abschnitts wurde nach [Abgelaufene Blocklisteneinträge](#)²⁰¹ in *Nubus Handbuch 1.x* [6] verschoben.

6.9.5 LDAP ACLs für Blocklisten

Standardmäßig kann jeder UCS Knoten in der Domäne und jedes Mitglied der Gruppe `Domain Admins` Blocklisteneinträge schreiben. Und jeder kann lesen. Sie können die Berechtigungen für den Primary Directory Node und den Backup Directory Nodes mit den folgenden Univention Configuration Registry Variablen konfigurieren:

- `ldap/database/internal/acl/blocklists/groups/read` (Seite 158)
- `ldap/database/internal/acl/blocklists/groups/write` (Seite 158)

Wenn Sie zum Beispiel einem Benutzer das Recht geben wollen, Einträge in der Blockliste zu löschen, der nicht Mitglied der Gruppe `Domain Admins` ist, müssen Sie eine Gruppe mit diesem Benutzer als Mitglied erstellen und den LDAP DN dieser Gruppe zu `ldap/database/internal/acl/blocklists/groups/write` (Seite 158) hinzufügen.

6.10 Papierkorb

Added in version 5.2-3-erratum-298: Seit [UCS 5.2 erratum 298](#)²⁰² unterstützt UCS eine *Papierkorb*-Funktion für Benutzer- und Gruppenobjekte in UDM.

Der *Papierkorb* ist eine Funktion in UDM, mit der gelöschte Verzeichnisobjekte vorübergehend gespeichert werden können. Der *Papierkorb* ermöglicht es Administratoren, die versehentlich UDM Objekte entfernt haben, diese Objekte in ihrem ursprünglichen Zustand wieder herzustellen.

Wenn der *Papierkorb* über eine Richtlinie aktiviert ist, verschiebt UDM gelöschte Objekte in einen speziellen *Papierkorb*-Container, bevor sie aus dem LDAP-Verzeichnis entfernt werden. UDM bewahrt die ursprünglichen Objektdaten zusammen mit Metadaten über die Löschung auf. Sie können alle vorhandenen Einträge im *Papierkorb* in UMC, UDM und der UDM HTTP REST API anzeigen und diese Objekte in ihren ursprünglichen Zustand vor dem Löschen wiederherstellen. UDM löscht Einträge im *Papierkorb* nach einer konfigurierbaren Aufbewahrungszeit automatisch.

Dieser Abschnitt beschreibt, wie Sie den *Papierkorb* aktivieren, eine Richtlinie dafür definieren und ihn verwalten. Außerdem finden Sie Informationen zum automatischen Löschen von Einträgen, zur Konfiguration und zur Protokollierung.

¹⁹⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/blocklists.html#nubus-domain-blocklists-activate>

¹⁹⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/blocklists.html#nubus-domain-blocklists-configure>

²⁰⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/blocklists.html#nubus-domain-blocklists-manage>

²⁰¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/blocklists.html#nubus-domain-blocklists-expired-entries>

²⁰² <https://errata.software-univention.de/#/?erratum=5.2x298>

6.10.1 Einschränkungen

Die Implementierung des *Papierkorbs* unterliegt den folgenden technischen Einschränkungen:

- Der *Papierkorb* unterstützt nur die UDM Typen `users/user` und `groups/group`.
- Der *Papierkorb* ist nur für Nubus for UCS verfügbar.

6.10.2 Papierkorb aktivieren

Um den *Papierkorb* zu aktivieren, setzen Sie auf dem Primary Directory Node und allen Backup Directory Nodes die Univention Configuration Registry Variable `listener/module/recyclebin/deactivate` (Seite 42) auf `false`.

Starten Sie anschließend den *Directory Listener* auf dem Primary Directory Node mit dem Befehl in [Quellcode 6.1](#) neu.

Quellcode 6.1: *Directory Listener* neu starten

```
$ systemctl restart univention-directory-listener
```

6.10.3 Richtlinie für den Papierkorb

Administratoren können den *Papierkorb* mit einer oder mehreren *Papierkorb*-Richtlinien konfigurieren, siehe [Richtlinien](#) (Seite 27).

Nachdem Sie eine *Papierkorb*-Richtlinie erstellt und mit einem Containerobjekt im LDAP-Verzeichnis verknüpft haben, gilt die *Papierkorb*-Konfiguration für alle Objekte innerhalb des Containers. Bevor ein Objekt entfernt wird, überprüft UDM, ob eine solche Richtlinie gilt, und verschiebt das Objekt in den *Papierkorb*.

Die *Papierkorb*-Richtlinie hat die folgenden Konfigurationseigenschaften:

Papierkorb aktiviert

Legt fest, ob der *Papierkorb* für Objekte aktiv ist. Auch wenn ein Container über eine verknüpfte *Papierkorb*-Richtlinie verfügt, können Sie diese hiermit deaktivieren.

UDM Module für Papierkorb

Legt eine Liste von UDM Modultypen fest, für die die *Papierkorb*-Richtlinie gilt, z. B. `users/user` oder `groups/group`.

Ignorierte Objektklassen

Definiert eine Liste von LDAP-Objektklassen, die Ausnahmen für den *Papierkorb* darstellen. Wenn ein Administrator ein Objekt löscht und das Objekt einer dieser Objektklassen besitzt, verschiebt UDM das Objekt nicht in den *Papierkorb*-Container.

Aufbewahrungszeit in Tagen

Legt die Aufbewahrungsdauer in Tagen fest, für die UDM Objekte im *Papierkorb* aufbewahrt, bevor sie endgültig gelöscht werden. Sie müssen sicherstellen, dass der Wert der Aufbewahrungszeit zwischen den Werten der Univention Configuration Registry Variablen `ldap/database/internal/overlay/dds/min-ttl` (Seite 42) und `ldap/database/internal/overlay/dds/max-ttl` (Seite 42) liegt. Beide Variablen legen Sie auf dem Primary Directory Node fest.

6.10.4 Objekte im Papierkorb verwalten

Administratoren können Einträge im *Papierkorb* mit dem UMC-Modul *Papierkorb* oder mit dem Befehlszeilentool `udm` und dem UDM Modul `recyclebin/removedobject` verwalten.

Ihnen stehen folgende Aktionen zur Verfügung:

- Alle vorhandenen Einträge im *Papierkorb* anzeigen, *list*.
- Objekte dauerhaft löschen, *delete*.
- Objekte wiederherstellen, *restore*.

Durch das Wiederherstellen von Objekten aus dem *Papierkorb* werden diese im Status, den sie vor dem Löschen hatten, zur LDAP-Datenbank hinzugefügt. Dazu gehören beispielsweise Passwörter und Gruppenmitgliedschaften für Benutzerobjekte.

6.10.5 Automatisches Löschen von Einträgen im Papierkorb

UDM erstellt Einträge im *Papierkorb*, wenn ein Administrator ein UDM Objekt entfernt, auf das eine *Papierkorb*-Richtlinie zutrifft.

Die Richtlinie definiert auch eine Aufbewahrungsfrist, siehe *Aufbewahrungszeit in Tagen* (Seite 41). Der Eintrag im *Papierkorb* übernimmt diese Aufbewahrungsfrist aus seiner Richtlinie als Eigenschaft `time-to-live`. UDM löscht automatisch Einträge im *Papierkorb*, die ihre Aufbewahrungsfrist erreicht haben. Gelöschte Einträge können nicht wiederhergestellt werden.

In Nubus übernimmt die *Dynamic Directory Services* Funktion des OpenLDAP-Servers die automatische Bereinigung.

6.10.6 Konfiguration über UCR

Die folgende Referenz zeigt die verfügbaren Einstellungen für den *Papierkorb*. Sie müssen diese Einstellungen auf dem Primary Directory Node ändern.

`listener/module/recyclebin/deactivate`

Steuert, ob der *Papierkorb* aktiv ist. Der Standardwert ist `true`.

Um den *Papierkorb* zu aktivieren, siehe *Papierkorb aktivieren* (Seite 41).

`ldap/database/internal/overlay/dds/min-ttl`

Legt die Mindestlebensdauer (TTL) in Sekunden für Einträge im *Papierkorb* fest. Der Standardwert beträgt 86400 Sekunden, also ein Tag.

Nachdem Sie den Wert geändert haben, müssen Sie den LDAP-Server neu starten, siehe [Quellcode 6.2](#).

`ldap/database/internal/overlay/dds/max-ttl`

Legt die maximale Lebensdauer (TTL) in Sekunden für Einträge im *Papierkorb* fest. Der Standardwert beträgt 31536000 Sekunden, also 365 Tage.

Nachdem Sie den Wert geändert haben, müssen Sie den LDAP-Server neu starten, siehe [Quellcode 6.2](#).

Wichtig

Um den LDAP-Dienst neu zu starten, führen Sie die folgenden Schritte aus:

1. Stellen Sie sicher, dass die UCS-Domäne die folgenden Bedingungen erfüllt:
 - Es findet kein Massenimport von Benutzerdaten statt, beispielsweise über `UCS@school`, oder es erfolgt keine Initialisierung des *AD Connector* oder des *S4 Connector*.
 - Kein UCS-System tritt der Domäne bei.
 - Es werden keine Systemupdates oder Aktualisierungen von Apps durchgeführt.
 - Listener und Connectoren sind inaktiv.
2. Starten Sie den LDAP-Server auf dem Primary Directory Node mit dem Befehl in [Quellcode 6.2](#) neu.

Quellcode 6.2: LDAP-Server neu starten

```
$ systemctl restart slapd
```

6.10.7 Protokollinformationen

Die folgenden Dateien enthalten Informationen zur Erstellung von Einträgen im *Papierkorb* und zum Wiederherstellungsprozess.

`/var/log/univention/listener.log` auf dem Primary Directory Node

Enthält Protokollinformationen zur Erstellung von Einträgen im *Papierkorb*.

`/var/log/univention/management-console-module-udm.log`

Enthält Protokollinformationen zur Wiederherstellung von Objekten mit UMC.

`/var/log/univention/directory-manager-rest.log`

Enthält Protokollinformationen zur Wiederherstellung von Objekten mit der *UDM HTTP REST API*.

Der Inhalt dieses Abschnitts wurde nach [Gruppenverwaltung](#)²⁰³ in *Nubus Handbuch 1.x* [6] verschoben.

7.1 Zuordnung von Benutzergruppen

Der Inhalt dieses Abschnitts wurde nach [Benutzer zu Gruppen zuweisen](#)²⁰⁴ in *Nubus Handbuch 1.x* [6] verschoben.

7.2 Empfehlung für Definition von Gruppennamen

Der Inhalt dieses Abschnitts wurde nach [Empfehlung für die Definition von Gruppennamen](#)²⁰⁵ in *Nubus Handbuch 1.x* [6] verschoben.

7.3 Verwaltung von Gruppen über Univention Management Console Modul

Der Inhalt dieses Abschnitts wurde nach [Gruppen Verwaltungsmodul](#)²⁰⁶ in *Nubus Handbuch 1.x* [6] verschoben.

7.3.1 Gruppenmanagement Modul - Reiter Allgemein

Der Inhalt dieses Abschnitts wurde nach [Reiter Allgemein - Gruppenverwaltung](#)²⁰⁷ in *Nubus Handbuch 1.x* [6] verschoben.

7.3.2 Gruppenmanagement Modul - Reiter Erweiterte Einstellungen

Der Inhalt dieses Abschnitts wurde nach [Reiter Erweiterte Einstellungen - Gruppenverwaltung](#)²⁰⁸ in *Nubus Handbuch 1.x* [6] verschoben.

²⁰³ <https://docs.software-univention.de/nubus-manual/latest/de/groups.html#nubus-groups>

²⁰⁴ <https://docs.software-univention.de/nubus-manual/latest/de/groups.html#nubus-groups-assignement>

²⁰⁵ <https://docs.software-univention.de/nubus-manual/latest/de/groups.html#nubus-groups-recommendation-group-name>

²⁰⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/groups.html#nubus-groups-management>

²⁰⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/groups.html#nubus-groups-management-tab-general>

²⁰⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/groups.html#nubus-groups-management-tab-advanced>

7.3.3 Gruppenmanagement Modul - Reiter Optionseinstellungen

Der Inhalt dieses Abschnitts wurde nach Reiter Optionen - Gruppenverwaltung²⁰⁹ in *Nubus Handbuch 1.x* [6] verschoben.

7.4 Verschachtelte Gruppen mit Gruppen in Gruppen

Der Inhalt dieses Abschnitts wurde nach Verschachtelte Gruppen²¹⁰ in *Univention Corporate Server - Operation Manual* [1] verschoben.

7.5 Lokaler Gruppencache

Der Inhalt dieses Abschnitts wurde nach Caching von Gruppen²¹¹ in *Univention Corporate Server - Operation Manual* [1] verschoben.

7.6 Synchronisation von Active Directory-Gruppen bei Verwendung von Samba/AD

Der Inhalt dieses Abschnitts wurde nach Synchronisation von Gruppen mit Active Directory²¹² in *Univention Corporate Server - Operation Manual* [1] verschoben.

7.7 Overlay-Modul zur Anzeige der Gruppeninformationen an Benutzerobjekten

Der Inhalt dieses Abschnitts wurde nach Overlay-Modul für Gruppen²¹³ in *Univention Corporate Server - Operation Manual* [1] verschoben.

²⁰⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/users/groups.html#nubus-groups-management-tab-options>

²¹⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/group-management.html#ucs-operation-groups-management-nested>

²¹¹ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/group-management.html#ucs-operation-groups-management-cache>

²¹² <https://docs.software-univention.de/ucs-operation/5.2/de/iam/group-management.html#ucs-operation-groups-management-ad-group-sync>

²¹³ <https://docs.software-univention.de/ucs-operation/5.2/de/iam/group-management.html#ucs-operation-groups-management-overlay>

8.1 Verwaltung der Rechnerkonten über Univention Management Console Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Rechner Modul](#)²¹⁴ in *Nubus Handbuch 1.x* [6].

8.1.1 Modul Rechnerverwaltung - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Allgemein - Rechner Verwaltung](#)²¹⁵ in *Nubus Handbuch 1.x* [6].

8.1.2 Modul Rechnerverwaltung - Reiter Konto

Der Inhalt dieses Abschnitts ist umgezogen nach [Abschnitt Konto](#)²¹⁶ in *Nubus Handbuch 1.x* [6].

8.1.3 Modul Rechnerverwaltung - Reiter Unix-Konto

Der Inhalt dieses Abschnitts ist umgezogen nach [Abschnitt Konto](#)²¹⁷ in *Nubus Handbuch 1.x* [6].

8.1.4 Modul Rechnerverwaltung - Reiter Dienste

Der Inhalt dieses Abschnitts ist umgezogen nach [Abschnitt Dienste](#)²¹⁸ in *Nubus Handbuch 1.x* [6].

8.1.5 Modul Rechnerverwaltung - Reiter (Re)installation

Der Inhalt dieses Abschnitts ist umgezogen nach [Abschnitt \(Re\)installation](#)²¹⁹ in *Nubus Handbuch 1.x* [6].

²¹⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management>

²¹⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-general-tab>

²¹⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-account>

²¹⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-account>

²¹⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-services>

²¹⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-deployment>

8.1.6 Modul Rechnerverwaltung - Reiter DNS-Alias

Der Inhalt dieses Abschnitts ist umgezogen nach Abschnitt DNS Alias²²⁰ in *Nubus Handbuch 1.x* [6].

8.1.7 Modul Rechnerverwaltung - Reiter Dienste

Der Inhalt dieses Abschnitts ist umgezogen nach Abschnitt Alarme²²¹ in *Nubus Handbuch 1.x* [6].

8.1.8 Modul Rechnerverwaltung - Reiter Gruppen

Der Inhalt dieses Abschnitts ist umgezogen nach Abschnitt Gruppen²²² in *Nubus Handbuch 1.x* [6].

8.1.9 Modul Rechnerverwaltung - Reiter Optionen

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Optionen - Rechner Verwaltung²²³ in *Nubus Handbuch 1.x* [6].

8.1.10 Integration von Ubuntu-Clients

Der Inhalt dieses Abschnitts ist umgezogen nach Rechner Modul²²⁴ in *Nubus Handbuch 1.x* [6].

8.2 Konfiguration von Hardware und Treibern

8.2.1 Verfügbare Kernel-Varianten

Der Inhalt dieses Abschnitts ist umgezogen nach Kernel-Pakete²²⁵ in *Univention Corporate Server - Operation Manual* [1].

8.2.2 Treiber-Management / Kernel-Module

Der Inhalt dieses Abschnitts ist umgezogen in folgende Abschnitte in *Univention Corporate Server - Operation Manual* [1] umgezogen:

- Boot-Prozess und Laden von Treibern²²⁶
- Automatische Treibererkennung²²⁷
- Standard- und externe Treiber²²⁸
- Externe Treiber und DKMS²²⁹

8.2.3 GRUB Boot-Manager

Der Inhalt dieses Abschnitts ist umgezogen nach Boot-Manager²³⁰ in *Univention Corporate Server - Operation Manual* [1].

²²⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-dns-alias>

²²¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-alerts>

²²² <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-section-groups>

²²³ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management-table-options>

²²⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/computers.html#nubus-computer-management>

²²⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/kernel.html#system-administration-kernel-packages>

²²⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/kernel.html#system-administration-kernel-modules-loading>

²²⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/kernel.html#system-administration-kernel-modules-detection>

²²⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/kernel.html#system-administration-kernel-modules-standard>

²²⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/kernel.html#system-administration-kernel-modules-external>

²³⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/boot-manager.html#system-administration-boot-manager>

8.2.4 Netzwerk Konfiguration

Der Inhalt dieses Abschnitts ist umgezogen nach [Netzwerk Konfiguration](#)²³¹ in *Univention Corporate Server - Operation Manual* [1].

Konfiguration von IPv4-Adressen

Der Inhalt dieses Abschnitts ist umgezogen nach [IPv4-Adressen konfigurieren](#)²³² in *Univention Corporate Server - Operation Manual* [1].

Konfiguration von IPv6-Adressen

Der Inhalt dieses Abschnitts ist umgezogen nach [IPv6-Adressen konfigurieren](#)²³³ in *Univention Corporate Server - Operation Manual* [1].

Konfiguration der Nameserver

Der Inhalt dieses Abschnitts ist umgezogen nach [DNS-Server definieren](#)²³⁴ in *Univention Corporate Server - Operation Manual* [1].

Bridges, Bonding, VLANs

Der Inhalt dieses Abschnitts ist umgezogen nach [Erweiterte Netzwerk Konfigurationen](#)²³⁵ in *Univention Corporate Server - Operation Manual* [1].

Konfiguration von Bridging

Der Inhalt dieses Abschnitts ist umgezogen nach [Bridging konfigurieren](#)²³⁶ in *Univention Corporate Server - Operation Manual* [1].

Konfiguration von Bonding

Der Inhalt dieses Abschnitts ist umgezogen nach [Bonding konfigurieren](#)²³⁷ in *Univention Corporate Server - Operation Manual* [1].

Konfiguration VLAN

Der Inhalt dieses Abschnitts ist umgezogen nach [VLAN konfigurieren](#)²³⁸ in *Univention Corporate Server - Operation Manual* [1].

8.2.5 Konfiguration des Proxyzugriffs

Der Inhalt dieses Abschnitts ist umgezogen nach [Proxy-Einstellungen mit UCR Variablen konfigurieren](#)²³⁹ in *Univention Corporate Server - Operation Manual* [1].

²³¹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/index.html#system-administration-network>

²³² <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/basic.html#system-administration-network-ipv4>

²³³ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/basic.html#system-administration-network-ipv6>

²³⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/basic.html#system-administration-network-name-servers>

²³⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/advanced.html#system-administration-network-advanced>

system-administration-network-advanced

²³⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/advanced.html#system-administration-network-bridge>

system-administration-network-bridge

²³⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/advanced.html#system-administration-network-bonding>

system-administration-network-bonding

²³⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/network/advanced.html#system-administration-network-vlan>

system-administration-network-vlan

²³⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/proxy.html#system-administration-proxy>

8.2.6 Einbinden von NFS-Freigaben

Mit der Richtlinie *NFS-Freigaben* in den UMC-Modulen für die Rechnerverwaltung 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.

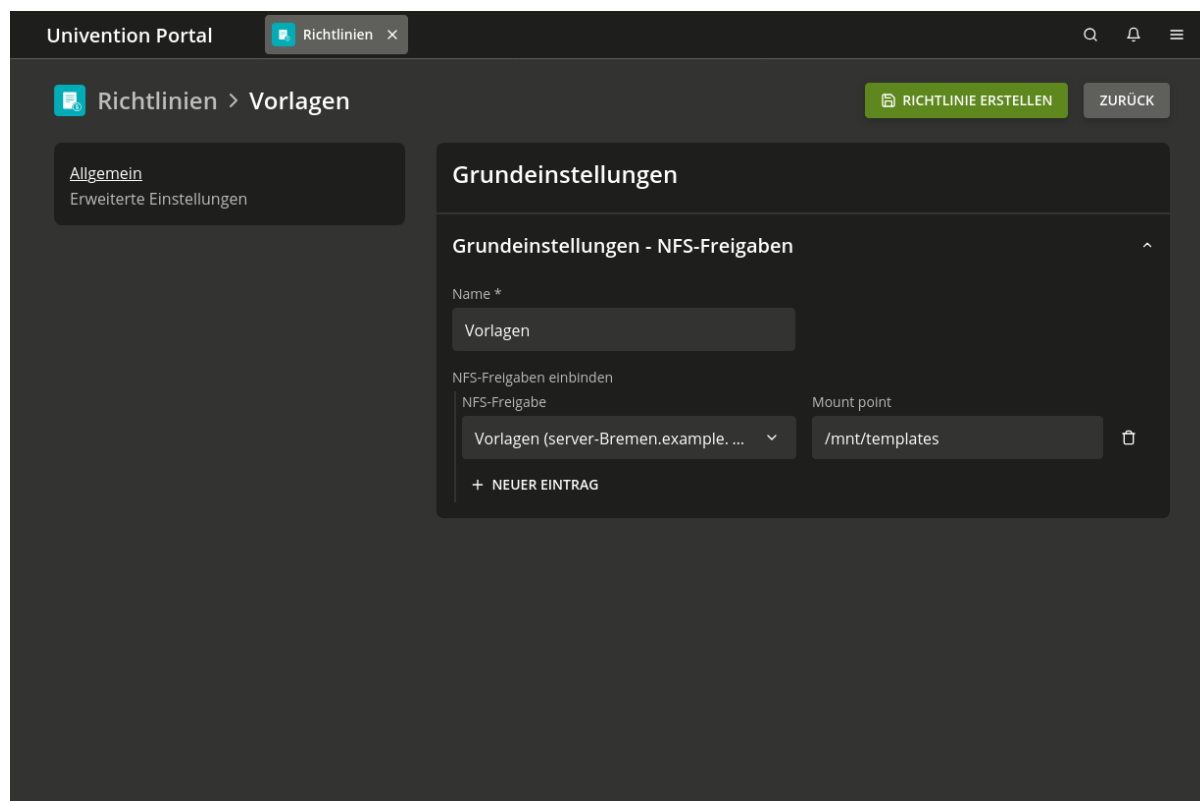


Abb. 8.1: Einbinden einer NFS-Freigabe

8.2.7 Erfassung von unterstützter Hardware

Der Inhalt dieses Abschnitts ist umgezogen nach [Hardwareinformationen](#)²⁴⁰ in *Univention Corporate Server - Operation Manual* [1].

8.3 Verwaltung der lokalen Systemkonfiguration mit Univention Configuration Registry

Der Inhalt dieses Abschnitts ist umgezogen nach [Das lokale System mit der Univention Configuration Registry konfigurieren](#)²⁴¹ in *Univention Corporate Server - Operation Manual* [1].

8.3.1 Verwendung des Univention Management Console Moduls

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Variablen in der Management UI verwalten](#)²⁴² in *Univention Corporate Server - Operation Manual* [1].

²⁴⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/management-interface/hardware-information.html#management-interface-hardware-information>

²⁴¹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr>

²⁴² <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-umc>

8.3.2 Verwendung des Kommandozeilenfrontends

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Variablen auf der Befehlszeile verwalten](#)²⁴³ in *Univention Corporate Server - Operation Manual* [1].

Abfrage einer UCR-Variable

Der Inhalt dieses Abschnitts ist umgezogen nach [Eine UCR-Variable abfragen](#)²⁴⁴ in *Univention Corporate Server - Operation Manual* [1].

Setzen von UCR-Variablen

Der Inhalt dieses Abschnitts ist umgezogen nach [Eine UCR-Variable setzen](#)²⁴⁵ in *Univention Corporate Server - Operation Manual* [1].

Suche nach Variablen und gesetzten Werten

Der Inhalt dieses Abschnitts ist umgezogen nach [Nach Variablen suchen](#)²⁴⁶ in *Univention Corporate Server - Operation Manual* [1].

Löschen von UCR-Variablen

Der Inhalt dieses Abschnitts ist umgezogen nach [Eine UCR-Variable löschen](#)²⁴⁷ in *Univention Corporate Server - Operation Manual* [1].

Neuerzeugung von Konfigurationsdateien aus ihrem Template

Der Inhalt dieses Abschnitts ist umgezogen nach [Eine Konfigurationsdatei aus der Vorlage neu generieren](#)²⁴⁸ in *Univention Corporate Server - Operation Manual* [1].

Übernahme von Variablen in Shell-Skripten

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Variablen in Shell-Skripten verwenden](#)²⁴⁹ in *Univention Corporate Server - Operation Manual* [1].

8.3.3 Richtlinienbasierte Konfiguration von UCR-Variablen

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Variablen mit Richtlinien konfigurieren](#)²⁵⁰ in *Univention Corporate Server - Operation Manual* [1].

8.3.4 Anpassung von UCR-Templates

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Vorlagen anpassen](#)²⁵¹ in *Univention Corporate Server - Operation Manual* [1].

Referenzierung von UCR-Variablen in Templates

Der Inhalt dieses Abschnitts ist umgezogen nach [UCR-Variablen in Vorlagen referenzieren](#)²⁵² in *Univention Corporate Server - Operation Manual* [1].

²⁴³ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line>

²⁴⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-query>

²⁴⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-set>

²⁴⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-search>

²⁴⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-delete>

²⁴⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-regenerate>

²⁴⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-command-line-source>

²⁵⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-policy>

²⁵¹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-templates>

²⁵² <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-templates-reference>

Integration von Inline-Python-Code in Templates

Der Inhalt dieses Abschnitts ist umgezogen nach [Eingebetteten Python-Code in Vorlagen integrieren](#)²⁵³ in *Univention Corporate Server - Operation Manual* [1].

8.4 Basis-Systemdienste

Der Inhalt dieses Abschnitts ist umgezogen nach [Systemadministration](#)²⁵⁴ in *Univention Corporate Server - Operation Manual* [1].

8.4.1 Administrativer Zugriff mit dem Root-Konto

Der Inhalt dieses Abschnitts ist umgezogen nach [Administrativer Zugriff mit dem Root-Konto](#)²⁵⁵ in *Univention Corporate Server - Operation Manual* [1].

8.4.2 Konfiguration der Sprach- und Tastatureinstellungen

Der Inhalt dieses Abschnitts ist umgezogen nach [Sprach-, Locale- und Tastatureinstellungen](#)²⁵⁶ in *Univention Corporate Server - Operation Manual* [1].

8.4.3 Starten/Stoppen von Systemdiensten / Konfiguration des automatischen Starts

Der Inhalt dieses Abschnitts ist umgezogen nach [Systemdienste verwalten](#)²⁵⁷ in *Univention Corporate Server - Operation Manual* [1].

8.4.4 Authentifizierung / PAM

Der Inhalt dieses Abschnitts ist umgezogen nach [Authentifizierung mit PAM](#)²⁵⁸ in *Univention Corporate Server - Operation Manual* [1].

Anmeldebeschränkungen für ausgewählte Benutzer

Der Inhalt dieses Abschnitts ist umgezogen nach [Authentifizierung mit PAM](#)²⁵⁹ in *Univention Corporate Server - Operation Manual* [1].

8.4.5 Konfiguration des verwendeten LDAP-Servers

Der Inhalt dieses Abschnitts ist umgezogen nach [Den LDAP-Server konfigurieren](#)²⁶⁰ in *Univention Corporate Server - Operation Manual* [1].

8.4.6 Konfiguration des verwendeten Druckerservers

Der Inhalt dieses Abschnitts ist umgezogen nach [Den Druckserver konfigurieren](#)²⁶¹ in *Univention Corporate Server - Operation Manual* [1].

²⁵³ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/ucr.html#system-administration-ucr-templates-python>

²⁵⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/index.html#system-administration>

²⁵⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/access-and-authentication.html#system-administration-root-account>

system-administration-root-account

²⁵⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/regional-settings.html#system-administration-language-locale-keyboard-setting>

²⁵⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/system-services.html#system-administration-service-management>

²⁵⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/access-and-authentication.html#system-administration-pam>

system-administration-pam

²⁵⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/access-and-authentication.html#system-administration-pam>

system-administration-pam

²⁶⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/system-services.html#system-administration-ldap-server>

²⁶¹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/system-services.html#system-administration-print-server>

8.4.7 Protokollierung/Abfrage von Systemmeldungen und -zuständen

Der Inhalt dieses Abschnitts ist umgezogen nach [Log-Dateien und Log-Rotation](#)²⁶² in *Univention Corporate Server - Operation Manual* [1].

Logdateien

Der Inhalt dieses Abschnitts ist umgezogen nach [Log-Dateien und Log-Rotation](#)²⁶³ in *Univention Corporate Server - Operation Manual* [1].

Protokollierung des Systemzustands

Der Inhalt dieses Abschnitts ist umgezogen nach [Diagnose über die Befehlszeile](#)²⁶⁴ in *Univention Corporate Server - Operation Manual* [1].

Prozessübersicht über Univention Management Console Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Diagnose in der Management UI](#)²⁶⁵ in *Univention Corporate Server - Operation Manual* [1].

Systemdiagnose über Univention Management Console Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [Systemdiagnose in der Management UI ausführen](#)²⁶⁶ in *Univention Corporate Server - Operation Manual* [1].

8.4.8 Ausführen von wiederkehrenden Aktionen mit Cron

Der Inhalt dieses Abschnitts ist umgezogen nach [Einleitung](#)²⁶⁷ in *Univention Corporate Server - Operation Manual* [1].

Stündliches/tägliches/wöchentliches/monatliches Ausführen von Skripten

Der Inhalt dieses Abschnitts ist umgezogen nach [Wiederkehrende Aktionen mit Cron ausführen](#)²⁶⁸ in *Univention Corporate Server - Operation Manual* [1].

Definition eigener Cron-Jobs in `/etc/cron.d/`

Der Inhalt dieses Abschnitts ist umgezogen nach [Lokale Cron-Jobs in `/etc/cron.d/` definieren](#)²⁶⁹ in *Univention Corporate Server - Operation Manual* [1].

Definition eigener Cron-Jobs in Univention Configuration Registry

Der Inhalt dieses Abschnitts ist umgezogen nach [Cron-Jobs in der Univention Configuration Registry definieren](#)²⁷⁰ in *Univention Corporate Server - Operation Manual* [1].

8.4.9 Name Service Cache Daemon

Der Inhalt dieses Abschnitts ist umgezogen nach [Name Service Cache Daemon](#)²⁷¹ in *Univention Corporate Server - Operation Manual* [1].

²⁶² <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/logging.html#system-administration-logging>

²⁶³ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/logging.html#system-administration-logging>

²⁶⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/diagnostics.html#system-administration-diagnostics-cli>

²⁶⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/diagnostics.html#system-administration-diagnostics-umc>

²⁶⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/diagnostics.html#system-administration-diagnostics-management-module>

²⁶⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/index.html#intro>

²⁶⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/cron.html#system-administration-cron>

²⁶⁹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/cron.html#system-administration-cron-local>

²⁷⁰ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/cron.html#system-administration-cron-ucr>

²⁷¹ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/system-services.html#system-administration-nscd>

8.4.10 SSH-Zugriff auf Systeme

Der Inhalt dieses Abschnitts ist umgezogen nach [SSH-Anmeldung an Systemen](#)²⁷² in *Univention Corporate Server - Operation Manual* [1].

8.4.11 Konfiguration der Zeitzone / Zeitsynchronisation

Der Inhalt dieses Abschnitts ist umgezogen nach [Zeitzone und Zeitsynchronisation](#)²⁷³ in *Univention Corporate Server - Operation Manual* [1].

²⁷² <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/access-and-authentication.html#system-administration-ssh-login>

²⁷³ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/regional-settings.html#system-administration-time-zone-synchronization>

Services für Windows

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 dass die Windows-Clients erneut der Domäne beitreten müssen. Dies ist in *Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover* (Seite 80) 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 *Vertrauensstellungen* (Seite 84)). Ausgehende Vertrauensstellungen mit Active Directory Domänen (UCS vertraut Windows) sind aktuell nicht unterstützt.

9.1 Betrieb einer Samba-Domäne auf Basis von Active Directory

9.1.1 Installation

Samba als AD-Domänencontroller kann auf allen UCS Directory Nodes 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 Primary Directory Node und Backup Directory Node muss zusätzlich **univention-s4-connector** installiert werden. Anschließend muss der Befehl **univention-run-join-scripts** aufgerufen werden. Weitere Informationen finden sich in *Installation weiterer Software* (Seite 33).

Ein Datei- und Druckserver kann auf UCS Managed Nodes mit der Applikation **Windows-kompatibler File-server** 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 *Installation weiterer Software* (Seite 33).

Samba unterstützt auch den Betrieb als *read-only domain controller*. Die Einrichtung ist in *Extended Windows integration documentation* [7] dokumentiert.

9.1.2 Dienste einer Samba-Domäne

Authentifizierungsdienst

Benutzeranmeldungen können nur auf Microsoft Windows-Systemen erfolgen, die der Samba-Domäne beigetreten sind. Der Domänenbeitritt ist in *Windows-Domänenbeitritt* (Seite 10) 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.

Dateidienste

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 *Verwaltung von Freigaben* (Seite 113)). Sofern das unterliegende Dateisystem Access Control Lists (ACLs) unterstützt (verwendbar bei `ext4` und `XFS`) sind ACLs auch von Windows-Clients verwendbar.

Dateidienste können auch von Samba Active Directory-Domänencontrollern, d.h. auf UCS Directory Nodes bereitgestellt werden. Generell wird in Samba-Umgebungen - analog zu den Microsoft-Empfehlungen für Active Directory - empfohlen Domänencontroller- und Datei/Druckdienste zu trennen, d.h. UCS Directory Nodes für die Anmeldung und Managed Nodes 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` (Seite 167) 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**)

Druckdienste

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 *Druckdienste* (Seite 119) beschrieben.

Druckdienste können auch mit Samba AD-Domänencontrollern bereitgestellt werden. Hierbei sind die in *Dateidienste* (Seite 56) beschriebenen Einschränkungen zu beachten.

Univention S4 Connector

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 Primary Directory Node 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 [KB 32 - Samba 4 Troubleshooting](#)²⁷⁴.

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@primary:~# 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
(..)
```

DRS-Replikation der Verzeichnisdaten

Samba/AD-Domänen verwenden das Directory Replication System (DRS) zur Replikation der Verzeichnisdaten. DRS erlaubt Multimasterreplikation, d.h. die schreibenden Änderungen mehrerer Samba/AD-Domänencontroller werden auf Protokollebene synchronisiert. Die Verwendung von Snapshots in Virtualisierungslösungen sollte daher beim Einsatz von Samba/AD vermieden und Samba/AD 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 auf Basis von UCS Directory Nodes nötig sind oder für neue Server nicht ein UCS Managed Node die bessere Wahl ist.

Hinweise zur Analyse von DRS-Replikationsproblemen finden sich in [KB 32 - Samba 4 Troubleshooting](#)²⁷⁵.

Synchronisation der SYSVOL-Freigabe

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) oder durch das Distributed File System (ab Windows 2008 R2) synchronisiert. Diese Replikationsmethoden sind in Samba noch nicht vollständig implementiert. Die Synchronisation zwischen den Samba/AD-Domänencontrollern erfolgt in UCS durch einen Cron-Job (standardmäßig alle fünf Minuten, konfigurierbar durch die Univention Configuration Registry Variable `samba4/sysvol/sync/cron` (Seite 167)).

9.1.3 Konfiguration und Management von Windows-Desktops

Gruppenrichtlinien

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.

²⁷⁴ <https://help.univention.com/t/32>

²⁷⁵ <https://help.univention.com/t/32>

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 AD/DS) 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 *Richtlinien* (Seite 27)) nicht über UMC-Module, sondern mit einem separaten Editor konfiguriert, mit der *Gruppenrichtlinienverwaltung*, die Teil der *Remote Server Administration Tools* (RSAT) ist. Die Einrichtung ist in *Installation der Gruppenrichtlinienverwaltung* (Seite 58) dokumentiert.

Es existieren zwei Arten von Richtlinien:

Benutzerrichtlinien

Benutzerrichtlinien konfigurieren die Einstellungen eines Benutzers, z.B. die Vorkonfiguration des Desktops. Auch Anwendungen können über Gruppenrichtlinien konfiguriert werden (z.B. die Startseite des Browsers oder Einstellungen in LibreOffice).

Computer-Richtlinien

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 *Synchronisation der SYSVOL-Freigabe* (Seite 57). Sie werden mit Benutzer- und Rechnerkonten im Samba-Verzeichnisdienst verknüpft.

Installation der Gruppenrichtlinienverwaltung

Die *Gruppenrichtlinienverwaltung* kann als Teil der *Remote Server Administration Tools* auf Windows Clients installiert werden. Sie können für Windows 10 unter *Remote Server Administration Tools (RSAT) for Windows 10*²⁷⁶ bezogen werden.

²⁷⁶ <https://www.microsoft.com/en-us/download/details.aspx?id=45520>

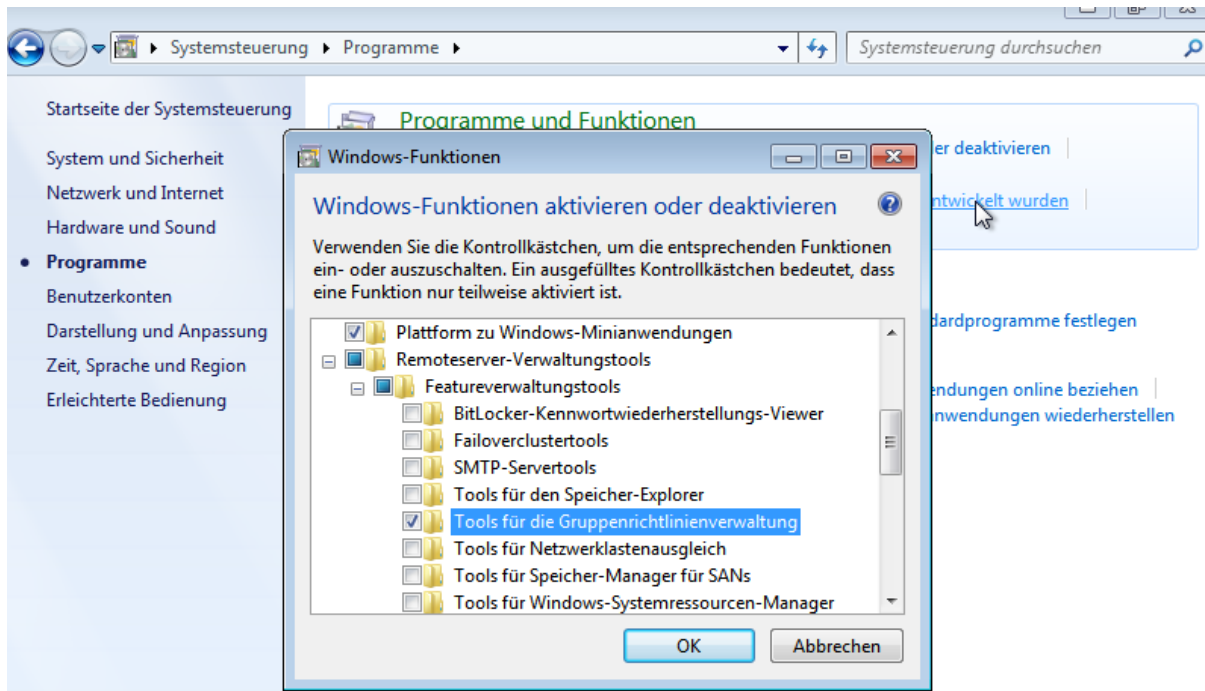


Abb. 9.1: Aktivierung der Gruppenrichtlinienverwaltung

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* ▶ *Featureverwaltungstools* die Option *Tools für die Gruppenrichtlinienverwaltung* aktiviert wird.

Nach der Aktivierung kann die Gruppenrichtlinienverwaltung unter *Start* ▶ *Verwaltung* ▶ *Gruppenrichtlinienverwaltung* aufgerufen werden.

Konfiguration von Richtlinien mit der Gruppenrichtlinienverwaltung

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 *Konfiguration von Gruppenrichtlinien in Umgebungen mit mehr als einem Samba-Domänencontroller* (Seite 62).

Es gibt zwei prinzipielle Möglichkeiten GPOs zu erstellen:

- Sie können im *Gruppenrichtlinienobjekte*-Ordner angelegt und dann mit verschiedenen Positionen im LDAP verknüpft werden. Dies ist sinnvoll, wenn eine Richtlinie mit mehreren Positionen im LDAP verknüpft werden soll.
- 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.

Zwei Standard-Richtlinienobjekte sind vordefiniert:

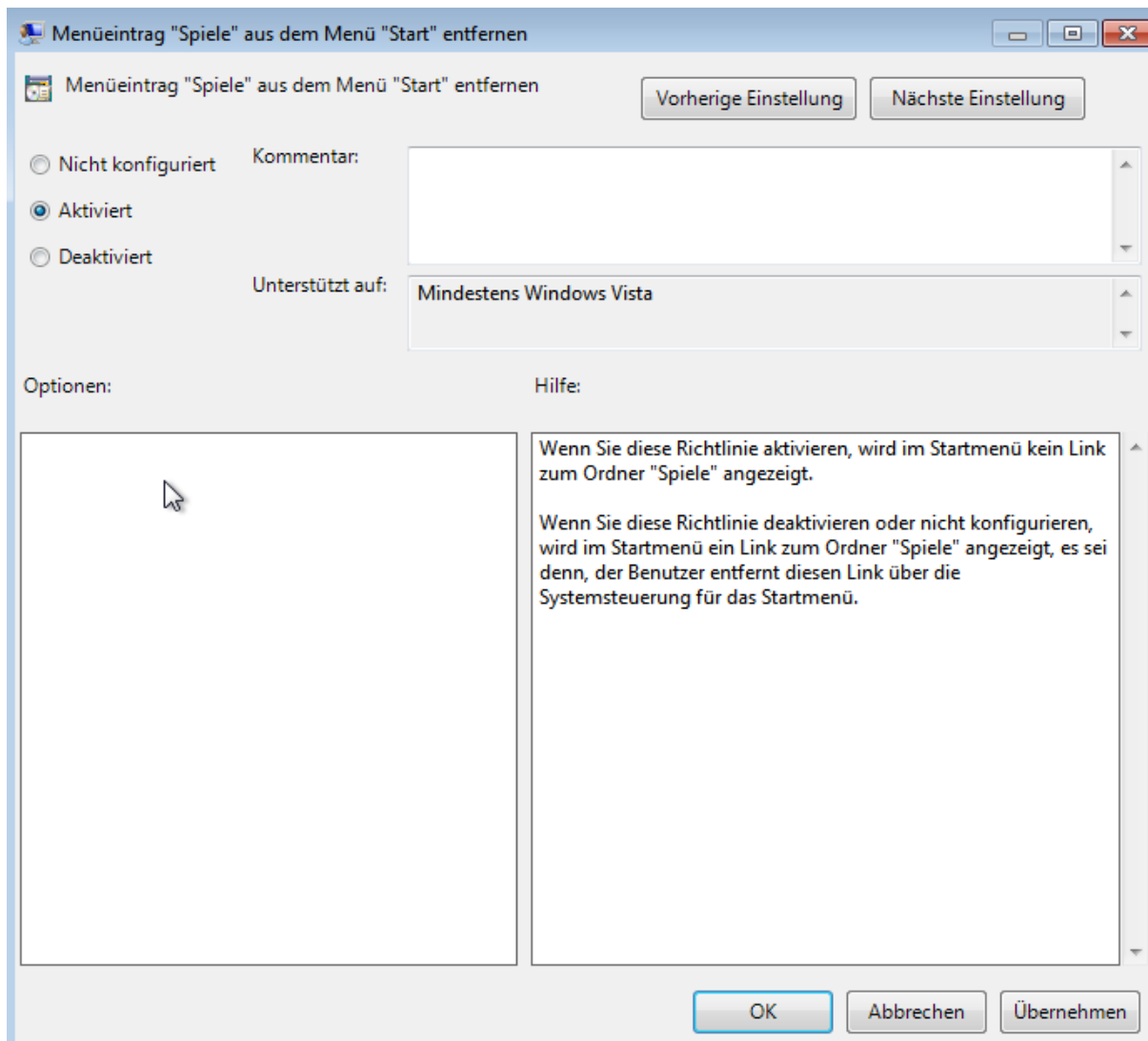


Abb. 9.2: Bearbeiten einer Richtlinie

Default Domain Policy

Das *Default Domain Policy* Objekt kann verwendet werden, um globale Richtlinien für alle Benutzer und Rechner der gesamten Domäne zu konfigurieren.

Default Domain Controllers Policy

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 Organisationseinheiten (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.

```

C:\Windows\system32\cmd.exe

C:\>gpresult /user user01 /v

Betriebssystem Microsoft (R) Windows (R) Gruppenrichtlinienergebnis-Tool v2.0
Copyright (C) Microsoft Corp. 1981-2001

Am 02.07.2014, um 21:49:27 erstellt

RSOP-Daten für SEC32AMD64\user01 auf JMM-PC: Protokollmodus
-----

Betriebssystemkonfiguration: Mitglied der Domäne/Arbeitsgruppe
Betriebssystemversion:      6.1.7601
Standortname:              Nicht zutreffend
Zwischengespeichertes Profil: Nicht zutreffend
Lokales Profil:            C:\Users\user01
Langsame Verbindung?      Nein

BENUTZEREINSTELLUNGEN
-----

CN=user01,CN=Users,DC=sec32amd64,DC=jmm
Letzte Gruppenrichtlinienanwendung: 02.07.2014, um 21:44:57
Gruppenrichtlinienanwendung von:    master.sec32amd64.jmm
Schwellenwert für langsame Verbindung: 500 kbps
Domänenname:                      SEC32AMD64
Domänentyp:                        Windows 2000

Angewendete Gruppenrichtlinienobjekte
-----
Nicht zutreffend

Folgende herausgefilterte Gruppenrichtlinien werden nicht angewendet.
-----

Default Domain Policy
  Filterung: Nicht angewendet (Leer)

Richtlinien der lokalen Gruppe
  Filterung: Nicht angewendet (Leer)

```

Abb. 9.3: Auswertung der GPO für den Benutzer `user01`

Die Richtlinien werden in folgender Reihenfolge ausgewertet:

1. Richtlinien der *Default Domain Policy* gelten als Grundeinstellung für alle Benutzer und Rechner der gesamten Domäne.
2. Mit einer OU verknüpfte Richtlinien überschreiben Richtlinien aus der Default Domain Policy. Sind OUs wei-

ter 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 einem Active Directory Standort
- 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.

Konfiguration von Gruppenrichtlinien in Umgebungen mit mehr als einem Samba-Domänencontroller

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 *Synchronisation der SYSVOL-Freigabe* (Seite 57))). Zum anderen gibt es ein gleichnamiges Objekt im LDAP-Baum des Samba-Verzeichnisdienstes (Samba AD/DS), 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.

Administrative Vorlagen (ADMX/ADM)

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, siehe *Group Policy ADMX Syntax Reference Guide* [8].

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, siehe *How to Implement the Central Store for Group Policy Admin Templates, Completely (Hint: Remove Those .ADM files!)* [9].

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 Drittwerkzeuge in das neuere ADMX-Format umgewandelt werden. Die administrativen Vorlagen müssen die Dateieindung `.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
```

Die ADM-Datei kann anschließend in das ADMX-Format umgewandelt oder aber direkt über die Gruppenrichtlinienverwaltung importiert werden. Dazu wird im Kontextmenü *Administrativen Vorlagen* ▶ *Vorlagen hinzufügen* ▶ *entfernen* aufgerufen. Mit *Hinzufügen* kann dann eine ADM-Datei importiert werden. Die administrativen Vorlagen

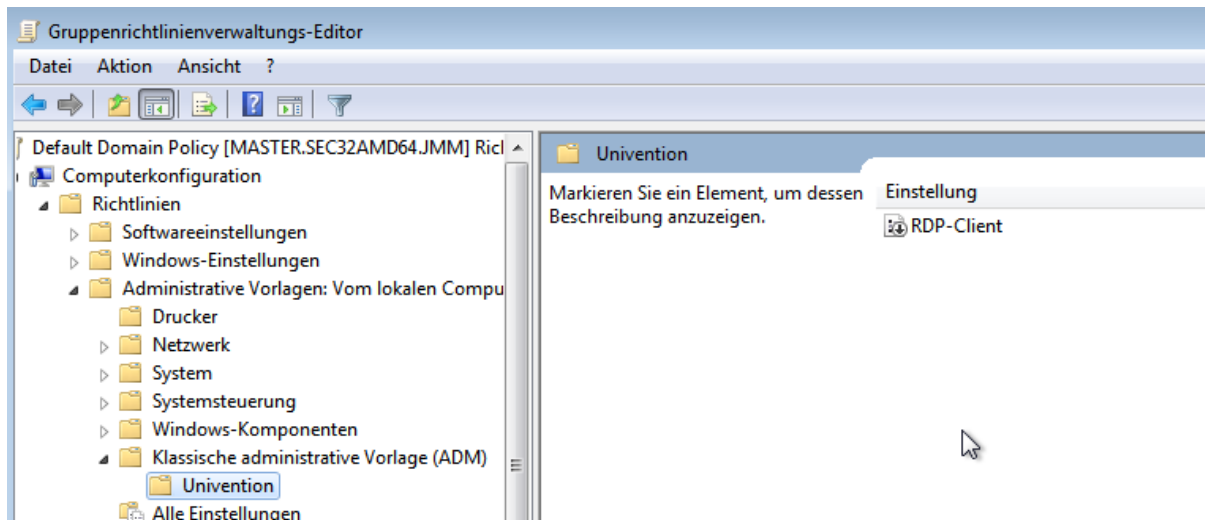


Abb. 9.4: Die eingebundene administrative Vorlage

werden ebenfalls in der SYSVOL-Freigabe gespeichert und repliziert, wodurch die Gruppenrichtlinienverwaltung von den Windows-Clients aus auf sie zugreifen kann.

Anwendung von Richtlinien auf Basis von Rechnereigenschaften (WMI-Filter)

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 mindestens 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 [10] und Heitbrink [11].

Anmeldeskripte / NETLOGON-Freigabe

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/Domänennamen/scripts/` abgelegt und unter dem Freigabennamen *NETLOGON* bereitgestellt. Der Dateiname des Skripts muss relativ zu diesem Verzeichnis angegeben werden.

Die NETLOGON-Freigabe wird im Rahmen der SYSVOL-Replikation repliziert.

Das Anmeldeskript kann pro Benutzer zugewiesen werden, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 36).

Konfiguration des Servers, auf dem das Heimatverzeichnis abgelegt wird

Das Heimatverzeichnis wird benutzerbezogen im UMC-Modul *Benutzer* definiert, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 36). Dies erfolgt mit der Einstellung *Windows-Heimatverzeichnis*, z.B. `\ucs-file-servermeier`.

Für das Zuweisen des Heimatverzeichnis-Servers an mehrere Benutzer auf einmal kann der Mehrfachbearbeitungsmodus von UMC-Modulen verwendet werden, siehe *Bearbeiten von Objekten* (Seite 26).

Servergespeicherte Profile

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.

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. Wenn hier z.B. der UNC-Pfad `%LOGONSERVER%\%USERNAME%\windows-profiles\default` eingetragen wird, dann werden die Verzeichnisse `windows-profiles\default.v?` im Heimatverzeichnis des Benutzers auf dem jeweils gewählten Logonserver verwendet.

Alternativ kann das Profilverzeichnis individuell für einzelne Benutzerkonten definiert werden. Das ist im UMC-Modul *Benutzer* unter dem Reiter *Konto* des Benutzerkontos über das Feld *Profilverzeichnis* möglich. Der entsprechende UDM-Attributname heißt `profilepath`. Mit OpenLDAP als Backend wird dies im LDAP-Attribut `sambaProfilePath` gespeichert.

Wird der Profilpfad 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.

Bemerkung

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.

9.2 Active Directory-Verbindung

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 *Installation weiterer Software* (Seite 33)). Diese steht auf einem Primary Directory Node und Backup Directory Node zur Verfügung.

Die beiden Varianten sind:

- UCS als Teil (Domänen-Mitglied) einer AD-Domäne (siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 65))
- Synchronisation von Kontendaten zwischen einer AD-Domäne und einer UCS-Domäne (siehe *Einrichtung des UCS AD-Connectors* (Seite 68)).

In beiden Modi wird unter UCS der Dienst **Active Directory-Verbindung** verwendet (kurz UCS AD-Connector), der Verzeichnisdienstobjekte zwischen einem Microsoft Windows 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 *UCS als Mitglied einer Active Directory-Domäne* (Seite 65) 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 dieses Betriebsmodus ist im Detail in *Einrichtung des UCS AD-Connectors* (Seite 68) beschrieben.

9.2.1 Unterstützte Windows-Versionen in Active Directory-Verbindung

Active Directory-Verbindung unterstützt Microsoft Windows Server in den Versionen 2012, 2016, 2019, 2022 und 2025.

Warnung

Active Directory-Verbindung verwendet den RPC-Aufruf `SamrSetInformationUser2` gegen Active Directory Domänencontroller um NT/RC4-Passwort-Hashes *nach* Active Directory zu synchronisieren, ohne Klartext-Passwörter zu speichern.

Microsoft entschied, keinen vergleichbaren RPC-Aufruf zu implementieren oder zu dokumentieren, um stärkere Kerberos-Passwort-Hashes *nach* Active Directory zu synchronisieren.

Um die Ausgabe von Kerberostickets für diese Benutzerkonten zu ermöglichen, setzt **Active Directory-Verbindung** das entsprechende Bit `RC4-HMAC` in `msDS-SupportedEncryptionTypes` für Konten, wenn es geänderte Passwort-Hashes nach Active Directory synchronisiert. Das Microsoft Update [KB5082063](#) veränderte die `DefaultDomainSupportedEncTypes`, um `RC4-HMAC`-Hashes standardmäßig zu deaktivieren. Daher ist es notwendig, dieses Bit zu setzen, um den Active Directory KDC für diese Benutzerkonten Kerberostickets ausgeben zu lassen. Wenn ein Passwortwechsel von Active Directory ausgeht und **Active Directory-Verbindung** den Passwortwechsel zurück nach Nubus synchronisiert, dann entfernt **Active Directory-Verbindung** das Bit wieder.

Siehe auch

[How to manage Kerberos KDC usage of RC4 for service account ticket issuance changes related to CVE-2026-20833²⁷⁷](#)

9.2.2 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 *Installation weiterer Software* (Seite 33).

Bemerkung

- Der *AD member*-Modus kann nur auf einem Primary Directory Node konfiguriert werden.
- Der Name der DNS-Domäne des UCS-Systems muss mit dem der AD-Domäne übereinstimmen. Die Hostnamen selbst müssen natürlich unterschiedlich sein.

²⁷⁷ <https://support.microsoft.com/en-gb/topic/how-to-manage-kerberos-kdc-usage-of-rc4-for-service-account-ticket-issuance-changes-related-to-cve-2026-20833>

- Alle AD- und UCS-Server in einer Connector-Umgebung sollten dieselbe Zeitzone verwenden.

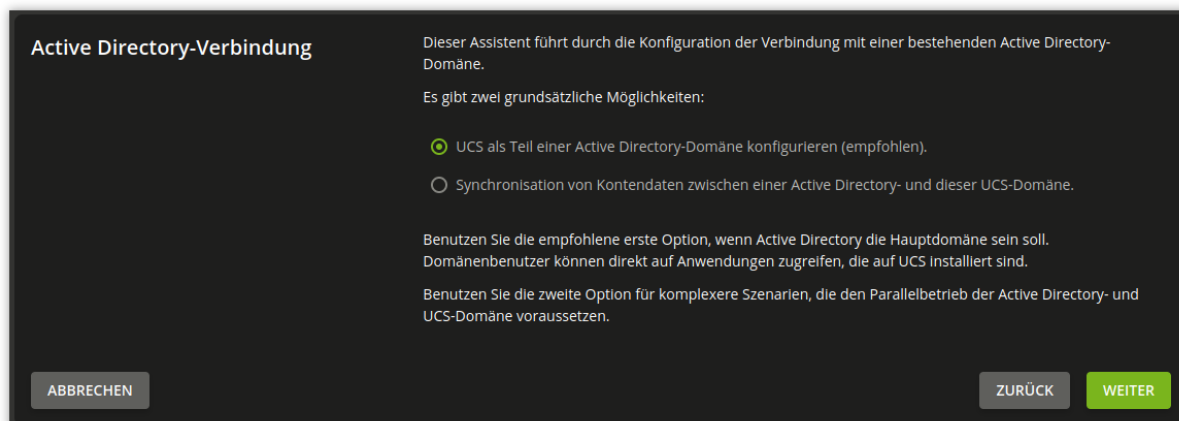


Abb. 9.5: Konfiguration des Betriebsmodus als Teil einer AD-Domäne

Im ersten Dialog des 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 Administrator-Konto 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.

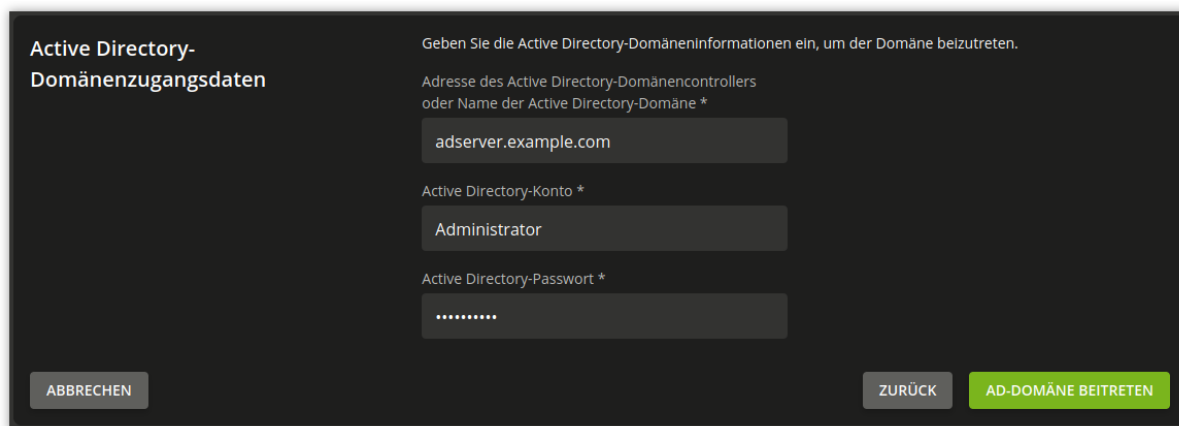


Abb. 9.6: Domänenbeitritt zu einer AD-Domäne

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.

Bemerkung

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 Primary Directory Node weitere UCS-Systeme schon Teil der UCS-Domäne waren, dann müssen diese der Domäne neu beitreten. Dabei erkennen sie, dass der Primary Directory Node sich im *AD member*-Modus befindet und treten ebenfalls der Authentifikationsstruktur der AD-Domäne bei und können dann z.B. zusätzlich Samba-Dateifreigaben bereitstellen.

Bemerkung

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 gegebenenfalls neu zu starten (siehe *Start/Stop des Active Directory Connectors* (Seite 72)).

Um eine verschlüsselte Verbindung zwischen Active Directory und Primary Directory Node 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 *Import des SSL-Zertifikats des Active Directory* (Seite 70).

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 Primary Directory Nodes 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` (Seite 154) eingetragen werden. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Passwort muss auf dem Primary Directory Node in eine Datei gespeichert werden und ihr Dateiname muss in die Univention Configuration Registry Variable `connector/ad/ldap/bindpw` (Seite 154) 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 Primary Directory Node abgelöst werden. Dies ist über die Applikation *Active Directory Takeover* möglich (siehe *Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover* (Seite 80)).

9.2.3 Einrichtung des UCS AD-Connectors

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. Dieser Betriebsmodus setzt die Synchronisation verschlüsselter Passwortdaten voraus.

In der Standardeinstellung werden Container, Organisationseinheiten, Benutzer, Gruppen und Rechner synchronisiert.

Der UCS AD Connector kann nur auf einem Primary Directory Node oder einem Backup Directory Node installiert werden.

Hinweise zu den in der Grundeinstellung konfigurierten Attributen und zu beachtende Besonderheiten finden sich in [Details zur vorkonfigurierten Synchronisation](#) (Seite 79).

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, und, falls bereits vorhanden, modifiziert. Anschließend werden alle Objekte aus dem AD gelesen und in UCS-Objekte umgewandelt und entsprechend auf UCS-Seite hinzugefügt oder 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 abgefragt. Dieser Wert ist auf fünf Sekunden eingestellt und kann manuell per Univention Configuration Registry-Variable `connector/ad/poll/sleep` (Seite 154) 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` (Seite 154) 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.

Grundkonfiguration des UCS AD-Connectors

Der UCS AD-Connector wird über einen Assistenten im UMC-Modul *Active Directory-Verbindung* konfiguriert.

Das Modul 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 [Installation weiterer Software](#) (Seite 33).

Bemerkung

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 im Assistenten hochgeladen werden müssen.

Im ersten Dialog der Einrichtungsassistenten muss der Punkt *Synchronisation von Kontendaten zwischen einer AD und dieser UCS-Domäne* ausgewählt und mit *Weiter* bestätigt werden.

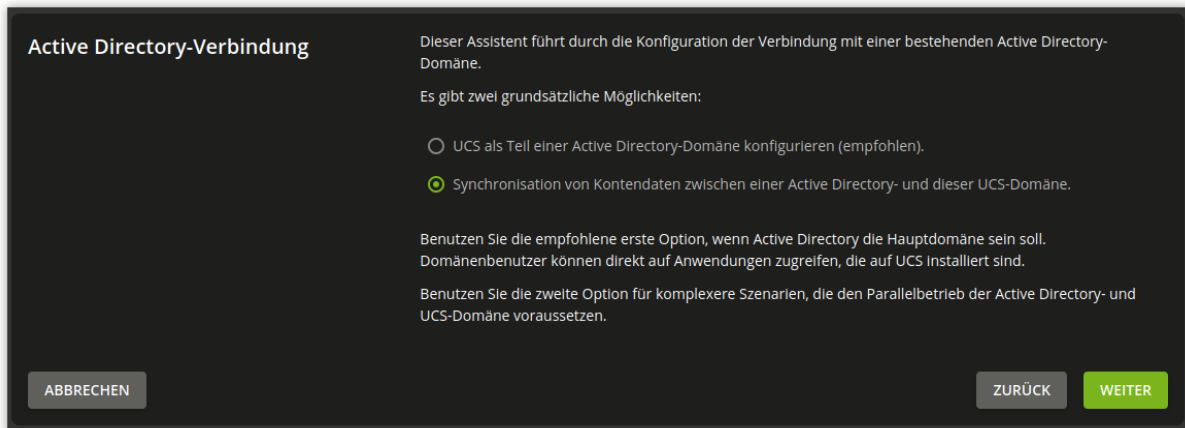


Abb. 9.7: Konfiguration des UCS AD-Connectors über UMC-Modul

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 im UMC-Modul *DNS* ein DNS-Host-Record für das AD-System angelegt werden (siehe [A/AAAA-Records \(Host Records\)](#) (Seite 98)).

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` (Seite 154) gespeichert. Der Replikationsbenutzer muss im AD Mitglied der Gruppe `Domänen-Admins` sein.

Das verwendete Passwort 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.

[Änderung des AD-Zugriffspassworts](#) (Seite 72) 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.

UCS 5.0 erfordert TLS 1.2, welches für Windows Server Releases vor 2012R2 manuell auf dem Windows Server aktiviert werden muss. UCS 5.0 unterstützt die Hash-Funktion SHA-1 nicht mehr. Falls für die Erstellung des AD Root-Zertifikat oder des Zertifikat des Windows Servers dieses Verfahren verwendet wurde, dann sollten diese ersetzt werden.

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 [Import des SSL-Zertifikats des Active Directory](#) (Seite 70)). 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 gegebenenfalls neu zu starten (siehe *Start/Stop des Active Directory Connectors* (Seite 72)).

Bemerkung

Der Connector kann auch mehrere AD-Domänen mit einer UCS-Domäne synchronisieren; dies ist in *Extended Windows integration documentation* [7] dokumentiert.

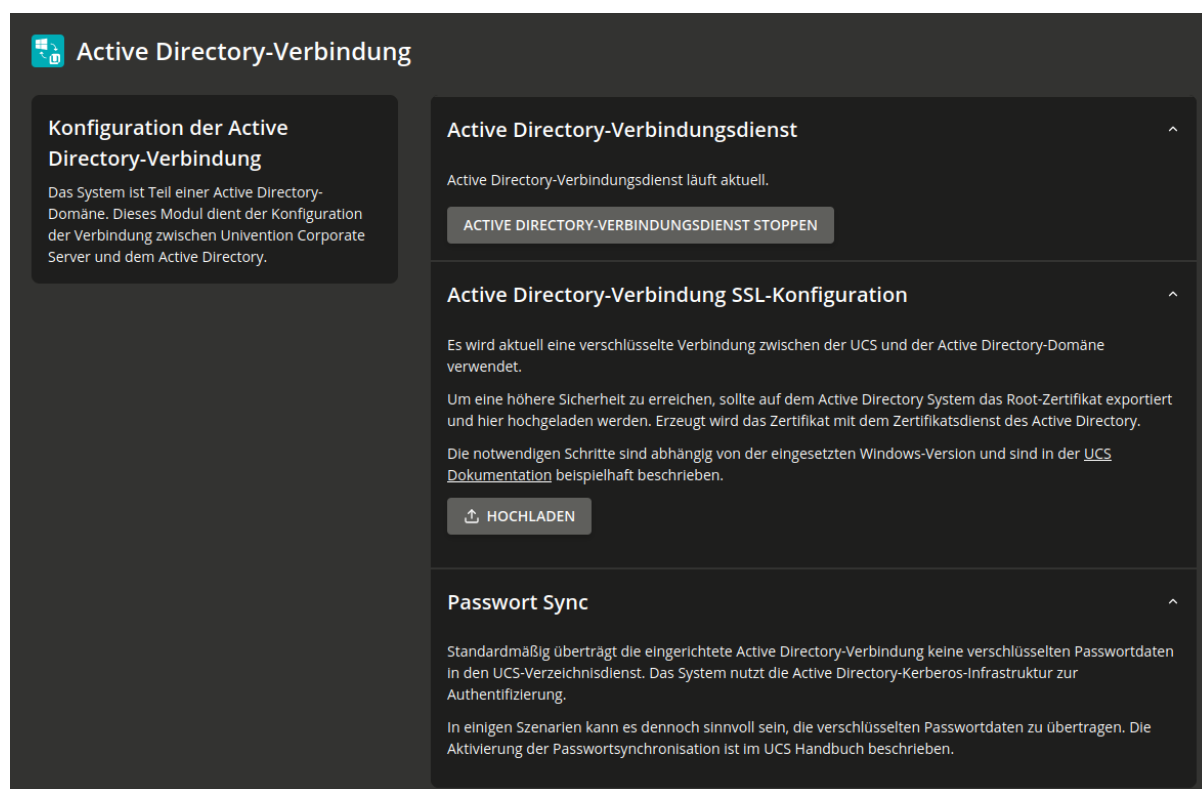


Abb. 9.8: Administrationsdialog für die Active Directory-Verbindung

Import des SSL-Zertifikats des Active Directory

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` (Seite 154) auf `no` gesetzt wird. Diese Einstellung betrifft nicht die Synchronisation der verschlüsselten Passwortdaten.

Export unter Microsoft Windows Server

Falls der Zertifizierungsdienst noch nicht installiert ist, installieren Sie ihn in Ihre Domäne mit den folgenden Schritten, bevor sie fortfahren:

1. Öffnen Sie den *Server Manager*.
2. Wählen Sie unter *Verwalten* ▶ *Rollen und Features hinzufügen* die Rolle *Active Directory-Zertifikatsdienste* aus.
3. Wählen Sie in der Liste der Dienste die *Zertifizierungsstelle* aus. Die obere Leiste des *Server Managers* zeigt ein gelbes Warndreieck an.
4. Wählen Sie die Option *Active Directory-Zertifikatsdienste konfigurieren* auf dem Server und konfigurieren Sie die *Zertifizierungsstelle* als ausgewählten Rollendienst.
5. Wählen Sie *Unternehmenszertifizierungsstelle* ▶ *Stammzertifizierungsstelle* als Installationstyp.
6. Klicken Sie *Neuen privaten Schlüssel erstellen*, bestätigen Sie die vorgeschlagenen Verschlüsselungseinstellungen und den Namen der *Zertifizierungsstelle*.
7. Wählen Sie einen beliebigen Zeitraum für die Gültigkeit und verwenden Sie die Standardpfade für den Speicherort der Datenbank.
8. Starten Sie abschließend Ihren Windows Active Directory Server neu, damit die Änderungen wirksam werden.

Siehe auch

Installieren der Zertifizierungsstelle²⁷⁸

für eine detaillierte Beschreibung der Installation der *Zertifizierungsstelle* in *Installieren der Zertifizierungsstelle* [12].

Um das Zertifikat der *Zertifizierungsstelle* zu exportieren, gehen Sie wie folgt vor:

1. Öffnen Sie den *Server Manager*.
2. Wählen Sie die Rolle *AD-Zertifikatsdienste*.
3. Klicken Sie mit der rechten Maustaste auf den Namen des Windows-Servers und wählen Sie *Zertifizierungsstelle*. Das Fenster mit der *Zertifizierungsstelle* öffnet sich. Ein Baum von Rechnern erscheint unter *Zertifizierungsstelle* auf der linken Seite.

Unter jedem aufgelisteten Rechner befinden sich die Elemente *Gesperrte Zertifikate*, *Ausgestellte Zertifikate*, *Ausstehende Anforderungen*, *Fehlgeschlagene Anforderungen* und *Zertifikatsvorlagen*.
4. Klicken Sie in der Serverliste mit der rechten Maustaste auf den Windows-Server, der Ihre *Zertifizierungsstelle* bedient, und wählen Sie *Eigenschaften*. Verwechseln Sie ihn nicht mit einem der anderen Elemente.
5. Im Fenster *Eigenschaften* wählen Sie *Generell* ▶ *Stammzertifikat* ▶ *Zertifikat Nr. 0* und klicken auf *Zertifikat anzeigen*.

Wichtig

Es ist wichtig, das Zertifikat zu kopieren, das normalerweise den Namen *Zertifikat Nr. 0* trägt, da die App **AD Connection** genau dieses Zertifikat für eine sichere Verbindung benötigt.

6. Wählen Sie im sich öffnenden Fenster *Zertifikat* die Registerkarte *Details* und klicken Sie auf *In Datei kopieren*

²⁷⁸ <https://learn.microsoft.com/de-de/windows-server/networking/core-network-guide/cnbg/server-certs/install-the-certification-authority>

Kopieren des AD-Zertifikats auf das UCS-System

Nun muss das SSL-AD-Zertifikat über das UMC-Modul 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.

Start/Stop des Active Directory Connectors

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.

Funktionstest der Grundeinstellungen

Die korrekte Grundkonfiguration des Connectors lässt sich prüfen, indem vom UCS-System aus im Active Directory gesucht wird. Mit folgendem Befehl kann z.B. nach dem Administrator-Konto im Active Directory gesucht werden:

```
$ univention-adsearch cn=Administrator
```

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.

Änderung des AD-Zugriffspassworts

Die vom UCS AD-Connector benötigten Zugangsdaten zum Active Directory werden über die Univention Configuration Registry Variable `connector/ad/ldap/binddn` (Seite 154) und `connector/ad/ldap/bindpw` (Seite 154) 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` (Seite 154) wird die LDAP-DN eines privilegierten Replikationsbenutzers konfiguriert. Dieser muss im AD Mitglied der Gruppe `Domänen-Admins` sein. Das entsprechende Passwort muss lokal auf dem UCS-System in eine Datei gespeichert werden, deren Dateiname in der Univention Configuration Registry Variable `connector/ad/ldap/bindpw` (Seite 154) 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?}"
```

9.2.4 Werkzeuge / Fehlersuche

Die **Active Directory Connection** stellt die folgenden Werkzeuge und Protokolldateien für die Diagnose zur Verfügung:

`univention-adsearch`

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.:

Beispiel:

```
$ univention-adsearch cn=admin administrator cn givenName
```

univention-adconnector-list-rejected

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.

Dieses Skript könnte eine Fehlermeldung oder eine unvollständige Ausgabe anzeigen, wenn der AD Connector in Betrieb ist.

remove_ad_rejected.py

Sie können dieses Skript verwenden, um ein AD-Objekt aus der Liste der abgelehnten AD-Objekte zu entfernen, das sich in der internen Datenbankdatei `/etc/univention/connector/internal.sqlite` befindet.

Beispiel:

```
$ /usr/share/univention-ad-connector/remove_ad_rejected.py \  
-c connector <AD object DN>
```

remove_ucs_rejected.py

Mit diesem Skript können Sie ein UCS Verzeichnisobjekt aus der Liste der abgelehnten UCS-Objekte entfernen, das sich in der internen Datenbankdatei `/etc/univention/connector/internal.sqlite` befindet.

Beispiel:

```
$ /usr/share/univention-ad-connector/remove_ucs_rejected.py \  
-c connector <UCS object DN>
```

resync_object_from_ad.py

Sie können dieses Skript verwenden, um Verzeichnisobjekte von AD zu UCS erneut zu synchronisieren. Verwenden Sie es, um ein einzelnes oder mehrere Verzeichnisobjekte zu synchronisieren.

Beispiel:

```
# to re-synchronize a single object  
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \  
-c connector <object DN>  
  
# to re-synchronize all objects matching a specific filter  
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \  
-c connector \  
--filter "(objectClass=posixAccount)"  
  
# to re-synchronize all objects matching a specific base  
$ /usr/share/univention-ad-connector/resync_object_from_ad.py \  
-c connector \  
--filter "(objectClass=posixAccount)" \  
--base "dc=example,dc=com"
```

resync_object_from_ucs.py

Sie können dieses Skript verwenden, um Verzeichnisobjekte von UCS nach AD erneut zu synchronisieren. Verwenden Sie es, um ein einzelnes oder mehrere Verzeichnisobjekte zu synchronisieren.

Beispiele:

```
# to re-synchronize a single object  
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \  
-c connector <object DN>  
  
# to re-synchronize all objects matching a specific filter  
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \  
-c connector <object DN>
```

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```

-c connector \
--filter "<LDAP filter>" \

# to re-synchronize all objects matching a specific base
$ /usr/share/univention-ad-connector/resync_object_from_ucs.py \
-c connector \
--filter "<LDAP filter>" \
--base "<base dn>" \

```

prepare-new-instance

Sie können dieses Skript verwenden, um AD-Verbindungsinstanzen zu erstellen. Das Skript kopiert die erforderlichen Dateien und setzt bestimmte UCR-Variablen.

Alternativ können Sie dieses Skript auch verwenden, um eine AD-Verbindungsinstanz zu löschen. Das Skript löscht dann intern die Dateien für die Instanz und setzt die UCR-Variablen zurück.

well-known-sid-object-rename

Sie können dieses Skript verwenden, um Benutzer und Gruppen mit bekannten SIDs in UDM umzubenennen. Die **AD Connection** verwendet es, um Benutzer und Gruppen mit bekannten SIDs umzubenennen.

make-deleted-objects-readable-for-this-machine

Sie können dieses Skript verwenden, um Zugriff zum Auflisten und Lesen auf `CN=Deleted Objects` in Active Directory zu gewähren.

Logdateien

Zur Fehlersuche bei Synchronisationsproblemen finden sich entsprechende Meldungen in folgenden Dateien auf dem UCS-System:

- `/var/log/univention/connector-ad.log`
- `/var/log/univention/connector-ad-status.log`

9.2.5 Selektive Synchronisation

Sie können die **Active Directory Connection** so konfigurieren, dass nur eine bestimmte Auswahl von Quellobjekten synchronisiert wird. Sie können die Quellobjekte nach Kriterien auswählen, die in den folgenden Abschnitten ausführlich beschrieben werden:

- Auswahl von Objekten nach Standort im LDAP-Teilbaum
- Auswahl von Objekten durch Übereinstimmung mit einem LDAP-Filter
- Auswahl aller Elemente außer nach Standort im LDAP-Teilbaum
- Auswahl aller Elemente außer durch Übereinstimmung mit einem LDAP-Filter

Nur bestimmte LDAP-Teilbäume zulassen

Um den Connector so zu konfigurieren, dass er nur bestimmte Teilbäume der LDAP-Struktur synchronisiert, können Sie die folgenden UCR-Variablen verwenden:

connector/ad/mapping/allowsubtree/.*/ucs

Für die Synchronisation von UCS LDAP-Verzeichnis zu Active Directory

Verwenden Sie diese Univention Configuration Registry Variable, um einen DN aus Ihrem UCS LDAP-Verzeichnis für die Synchronisation mit dem angeschlossenen Active Directory zu definieren. Die *AD-Verbindung* berücksichtigt dann nur UCS LDAP-Objekte für die Synchronisation, die sich in Teilbäumen befinden, die durch eine dieser UCR-Variablen spezifiziert sind. Die LDAP-Basis muss in den DNs enthalten sein und der Vergleich der DNs ist unabhängig von der Groß- und Kleinschreibung.

Siehe die Erklärung des Platzhalters `. *` weiter unten.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/allowsubtree/school1/ucs="ou=school1,dc=ucs,
↪domain"
$ ucr set connector/ad/mapping/allowsubtree/school2/ucs="ou=school2,dc=ucs,
↪domain"
```

connector/ad/mapping/allowsubtree/.*/ad

Für die Synchronisation von Active Directory zum UCS Verzeichnisdienst

Verwenden Sie diese Univention Configuration Registry Variable, um einen DN aus Ihrem Active Directory für die Synchronisation mit Ihrem UCS LDAP-Verzeichnis zu definieren. Die *AD-Verbindung* berücksichtigt dann nur Active Directory Objekte für die Synchronisation, die sich in Teilbäumen befinden, die durch eine dieser UCR-Variablen festgelegt sind. Die LDAP-Basis muss in den DNs enthalten sein, und beim Vergleich der DNs wird nicht zwischen Groß- und Kleinschreibung unterschieden.

Siehe die Erklärung des Platzhalters `.*` weiter unten.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/allowsubtree/school1/ad="ou=school1,dc=ad,domain
↪"
$ ucr set connector/ad/mapping/allowsubtree/school2/ad="ou=school2,dc=ad,domain
↪"
```

Platzhalter `.*`

Der Teil `.*` der Variable ist ein Platzhalter, den Sie als individuelle Bezeichnung für jede Variable verwenden können. Wenn Sie diesen Ansatz verfolgen, können Sie eine Reihe von UCR-Variablen der beschriebenen Typen erstellen. Jede Variable enthält nur einen DN.

Für jeden LDAP-Teilbaum, den Sie für die Synchronisierung zulassen möchten, müssen Sie eine separate Univention Configuration Registry Variable konfigurieren.

connector/ad/mapping/allow-subtree-ancestors

Um auch die Vorfahren der Wurzel eines LDAP-Teilbaums, der in `connector/ad/mapping/allowsubtree/.*/[ad|ucs]` definiert wurde, zu synchronisieren, aktivieren Sie diese Variable:

```
$ ucr set connector/ad/mapping/allow-subtree-ancestors=yes
```

Bei komplexen Strukturen kann dies die Konfiguration der selektiven Synchronisierung erleichtern. Diese Variable wird für alle Teilbäume angewendet, die in `connector/ad/mapping/allowsubtree/.*/[ad|ucs]` aufgeführt sind.

Nachdem Sie die UCR-Variablen definiert oder geändert haben, müssen Sie die **Active Directory Verbindung** neu starten.

Tipp

Die **Active Directory Verbindung** bestimmt die Position des Zielobjekts durch dynamische und statische Faktoren wie die Mapping Attribute `dn_mapping_function` und `position_mapping`, sofern sie im Mapping für einzelne Objekttypen konfiguriert sind. Die Position des entsprechenden Zielobjekts kann also außerhalb der Teilbäume liegen, die den Univention Configuration Registry Variablen entsprechen.

Warnung

Wenn Sie die Konfiguration `.../allowsubtree/.*/[ad|ucs]` verwenden und ein Quellobjekt aus einem betrachteten Teilbaum an eine Position verschieben, die außerhalb des kombinierten Geltungsbereichs aller Ihrer `.../allowsubtree/.*/[ad|ucs]` Definitionen liegt, dann entfernt die **Active Directory Verbindung** das Objekt aus dem Zielverzeichnis.

Nur Objekte zulassen, die einem LDAP-Filter entsprechen

Sie können für jede Art von Objekt einen LDAP-Filter konfigurieren. **Active Directory Verbindung** synchronisiert nur LDAP-Objekte, die diesem Filter entsprechen. Alle anderen LDAP-Objekte werden ignoriert.

Für die bidirektionale Synchronisierung muss der Filter sowohl mit dem UCS Objekt als auch mit dem AD-Objekt übereinstimmen. Wird ein Objekt, das mit dem Filter übereinstimmt, gelöscht, löscht der Connector auch das entsprechende Objekt auf der anderen Seite.

`connector/ad/mapping/{type}/allowfilter`

Der Connector synchronisiert nur die Objekte mit dem Objekttyp `{type}`, die diesem LDAP-Filter entsprechen. `{type}` kann einer der folgenden Werte sein:

- `user`
- `group`
- `container`
- `ou`
- `windowscomputer`

Zum Beispiel:

```
$ ucr set connector/ad/mapping/user/allowfilter="(description=sync) "
```

Nach dem Ändern dieser Einstellungen müssen Sie die **Active Directory Verbindung** neu starten.

Bemerkung

Dieser Filter unterstützt jedoch nicht die vollständige LDAP-Filtersyntax. Es wird immer zwischen Groß- und Kleinschreibung unterschieden. Sie können nur den Platzhalter `*` als Einzelwert ohne andere Zeichen verwenden.

Wichtig

Wenn ein Objekt, das mit dem Filter übereinstimmt, so geändert wird, dass der Filter nicht mehr passt, **synchronisiert** der Connector keine Änderung. Das bedeutet, dass der Connector weiterhin Änderungen von der anderen Seite auf das Objekt anwendet.

Wenn Sie die Synchronisierung für ein Objekt ausschalten wollen, müssen Sie die Änderung auf beiden Seiten, UCS und Active Directory, vornehmen.

Ignorieren von Objekten aus bestimmten LDAP-Teilbäumen

Um den Connector so zu konfigurieren, dass er Objekte aus bestimmten LDAP-Teilbäumen ignoriert, können Sie die folgende Univention Configuration Registry Variable verwenden:

`connector/ad/mapping/ignoresubtree/.*`

Die Variable definiert die Stellen im Verzeichnisdienst, die der Connector von der Synchronisation ausschließt. Die Werte können Positionen in Active Directory und im UCS LDAP-Verzeichnis enthalten. Standardmäßig ist die Variable nicht gesetzt.

Zum Beispiel:

```
$ ucr set connector/ad/mapping/ignoresubtree/ignore1="cn=alumni,dc=ucs,domain"  
$ ucr set connector/ad/mapping/ignoresubtree/ignore2="cn=alumni,dc=ad,domain"
```

Nach der Änderung dieser Einstellung müssen Sie die **Active Directory Verbindung** neu starten.

Objekte durch LDAP-Filter ignorieren

Um Objekte von der Synchronisierung auszuschließen, können Sie ihre Namen zu den folgenden Univention Configuration Registry Variable hinzufügen:

`connector/ad/mapping/{type}/ignorelist`

Der Connector synchronisiert **keine** Objekte, die diese Variable als Werte definiert. Trennen Sie mehrere Werte durch Kommas. Für die möglichen Werte für `{type}`, siehe Tab. 9.1. Die Tabelle zeigt auch, welche LDAP-Attribute Sie je nach Objekttyp im Filter berücksichtigen müssen.

Tab. 9.1: Zuordnung, welcher `{type}` welches LDAP-Attribut benötigt

<code>{type}</code>	Wert aus LDAP-Attribut
user	uid
group	cn
container	cn
ou	ou
windowscomputer	cn

Der Typ `user` berücksichtigt zum Beispiel das LDAP-Attribut `uid`:

```
$ ucr set connector/ad/mapping/user/ignorelist="Administrator,krbtgt,root,
↳pcpatch,mmustermann"
```

Wichtig

Einige der `ignorelist`-Einstellungen haben Voreinstellungen, die für die Funktionalität des Connector wichtig sind. Achten Sie darauf, dass Sie diese Einstellungen nicht überschreiben. Sie können den aktuellen Wert einer Univention Configuration Registry Variable mit dem folgenden Befehl überprüfen:

```
$ ucr get connector/ad/mapping/user/ignorelist
```

Für mehr Flexibilität können Sie auch einen LDAP-Filter setzen, um Objekte zu ignorieren. Verwenden Sie die folgende Univention Configuration Registry Variable:

`connector/ad/mapping/{type}/ignorefilter`

Der Connector synchronisiert **keine** Objekte, die diesem LDAP-Filter entsprechen. `{type}` kann einen der folgenden Werte haben:

- user
- group
- container
- ou
- windowscomputer

Zum Beispiel:

```
$ ucr set connector/ad/mapping/user/ignorefilter="(description=no sync)"
```

Bemerkung

Dieser Filter unterstützt jedoch nicht die vollständige LDAP-Filtersyntax. Es wird immer zwischen Groß- und Kleinschreibung unterschieden. Sie können nur den Platzhalter `*` als Einzelwert ohne andere Zeichen verwenden.

Nach dem Ändern dieser Einstellungen müssen Sie die **Active Directory Verbindung** neu starten.

Vorrang der Regeln

In diesem Abschnitt wird die Verarbeitungsreihenfolge für die bisher dokumentierten Einstellungen zur selektiven Synchronisation beschrieben.

Die **Active Directory Verbindung** verarbeitet die Regeln für Erlauben und Ignorieren in einer definierten Reihenfolge. Abhängig vom Ergebnis der Auswertung verhält sich der Connector wie folgt:

- Wenn eine Regel dazu führt, dass der Connector ein Objekt ignoriert, stoppt der Connector die Verarbeitung der Regel und synchronisiert kein Objekt.
- Wenn eine Regel dazu führt, dass der Connector ein Objekt verarbeitet, wertet der Connector die nächste Regel aus. Wenn die Regel die letzte Regel war und es keine nächste Regel gibt, synchronisiert der Connector das Objekt.

Der Connector wertet die Regeln für jedes Objekt in der folgenden Reihenfolge aus:

1. Teilbaum zulassen:

UCR Variablen

`connector/ad/mapping/allowsubtree/.*/ucs` (Seite 74), `connector/ad/mapping/allowsubtree/.*/ad` (Seite 75) und `connector/ad/mapping/allow-subtree-ancestors` (Seite 75)

Keine Übereinstimmung

Keine Synchronisation. Abarbeitung der Regeln beenden.

Übereinstimmung

Fortsetzen.

2. Filter zulassen:

UCR Variable

`connector/ad/mapping/{type}/allowfilter` (Seite 76)

Keine Übereinstimmung

Keine Synchronisation. Abarbeitung der Regeln beenden.

Übereinstimmung

Fortsetzen.

3. Unterbaum ignorieren:

UCR Variable

`connector/ad/mapping/ignoresubtree/.*` (Seite 76)

Keine Übereinstimmung

Fortsetzen.

Übereinstimmung

Keine Synchronisation. Abarbeitung der Regeln beenden.

4. Filter ignorieren:

UCR Variablen

`connector/ad/mapping/{type}/ignorelist` (Seite 77) und `connector/ad/mapping/{type}/ignorefilter` (Seite 77)

Keine Übereinstimmung

Fortsetzen.

Übereinstimmung

Keine Synchronisation. Abarbeitung der Regeln beenden.

5. Ende der Regeln.

6. Objekt synchronisieren.

9.2.6 Details zur vorkonfigurierten Synchronisation

Standardmäßig schließt die **Active Directory Verbindung** einige LDAP-Teilbäume von der Synchronisation aus. Sie finden die Liste der ignorierten Teilbäume in der Datei `/var/log/univention/connector-ad-mapping.log` unter der Einstellung `ignore_subtree` für jeden Objekttyp.

Container und Organisationseinheiten

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*).

Berücksichtigen Sie die folgenden Besonderheiten:

- Unter AD gelöschte Container oder Organisationseinheiten werden unter UCS rekursiv gelöscht, das bedeutet, dass nicht synchronisierte Unterobjekte, die in AD nicht zu sehen sind, ebenfalls entfernt werden.

Gruppen

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.

Besonderheiten

Berücksichtigen Sie die folgenden Besonderheiten:

- 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, dass die deutschsprachigen Gruppen angelegt werden und sollte in diesem Fall deaktiviert werden. Dazu kann die Univention Configuration Registry Variable `connector/ad/mapping/group/language` (Seite 154) 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.

Benutzerdefinierte Mappings

Für benutzerdefinierte Mappings, siehe [Active Directory Connection custom mappings](#)²⁷⁹ in *Univention Developer Reference* [13].

Benutzer

Benutzer werden wie Gruppen anhand des Benutzernamens und anhand des AD-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`.

Berücksichtigen Sie die folgenden Besonderheiten:

- 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 Abfrageintervall des Connectors.
- AD und UCS legen neue Benutzer per Voreinstellung in eine bestimmte primäre Gruppe (meist `Domain Users` und `Domänen Benutzer`). Während der ersten Synchronisation von UCS nach AD werden die Benutzer daher immer in dieser Gruppe Mitglied.

9.3 Migration einer Active Directory-Domäne zu UCS mit Univention AD Takeover

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:

1. Kopieren aller Objekte aus Active Directory nach UCS
2. Kopieren der Gruppenrichtliniendateien aus Active Directory nach UCS
3. Abschalten des AD-Servers und Zuweisung der FSMO-Rollen auf den UCS Directory Node

Die folgenden Voraussetzungen müssen für die Übernahme erfüllt sein:

- Der UCS Directory Node (Primary Directory Node) muss mit einem eindeutigen Rechnernamen installiert werden, der nicht in der AD-Domäne vorhanden ist.

²⁷⁹ <https://docs.software-univention.de/developer-reference/5.2/en/misc.html#ad-connection-custom-mappings>

- Der UCS Directory Node muss mit demselben DNS-Domännennamen, NetBIOS-Domännennamen und Kerberos-Domännennamen installiert werden wie die AD-Domäne. Es wird empfohlen auch die selbe LDAP-Basis-DN zu verwenden.
- Der UCS Directory Node muss eine IPv4-Adresse im selben Subnetz wie der zu übernehmende Active Directory-Domänencontroller verwenden.

Vorsicht

Sofern das System bereits Mitglied in einer Active Directory Domäne ist, 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 *Univention S4 Connector* (Seite 57), normalerweise der Primary Directory Node).

9.3.1 Vorbereitung

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 Terminalserver-sitzungen), wird empfohlen, diese zu deaktivieren 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 PASSWORD
```

9.3.2 Domänenmigration

Die Übernahme muss auf dem UCS Directory Node gestartet werden, auf dem der Univention S4 Connector läuft (normalerweise der Primary Directory Node). Während der Übernahme sollte Samba nur auf diesem UCS-System laufen. Gibt es weitere UCS Samba/AD Nodes, muss Samba auf diesen angehalten werden. Dies ist wichtig um replikationsbedingte Dateninkonsistenzen zu vermeiden.

Andere UCS Samba/AD-Systeme können gestoppt werden, indem auf jedem UCS Directory Node als Benutzer `root` folgender Befehl ausgeführt wird

```
$ /etc/init.d/samba4 stop
```

Nachdem sichergestellt wurde, dass keine anderen Samba/AD-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/groupstype=false
```

Die Übernahme erfolgt mit dem UMC-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.

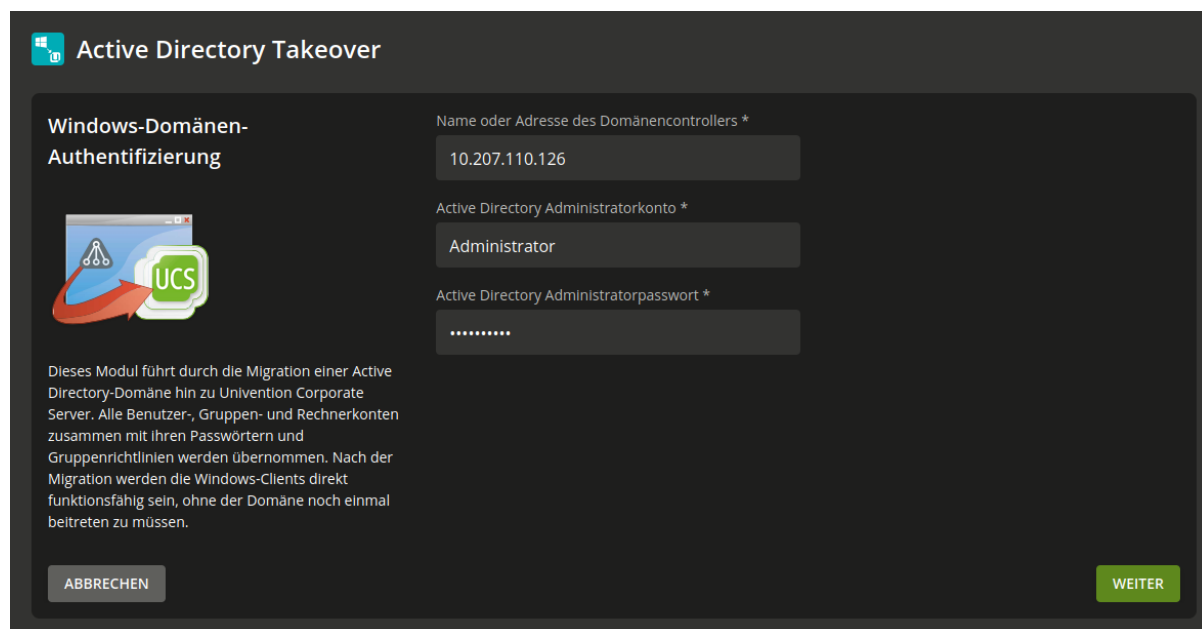


Abb. 9.9: Erste Phase der Domänenmigration

Das Modul prüft, ob der AD-Domänencontroller erreicht werden kann und zeigt die zu migrierenden Domänenanaten an.

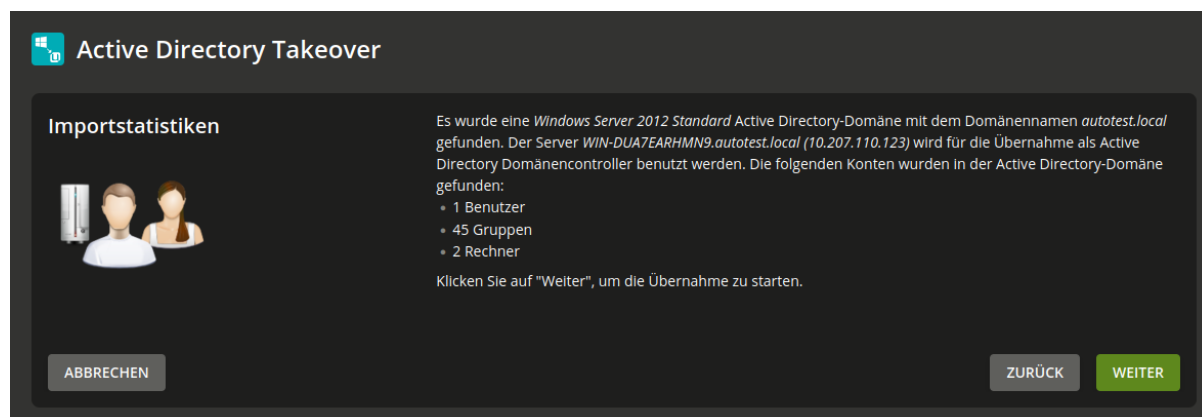


Abb. 9.10: Übersicht über die zu migrierenden Daten

Nach einem Klick auf *Weiter* werden die folgenden Schritte automatisch durchgeführt:

1. Anpassung der Systemzeit des UCS-Systems auf die Systemzeit der Active Directory-Domäne (wenn diese um mehr als drei Minuten nachgeht).
2. Beitritt des UCS Directory Nodes in die Active Directory-Domäne.
3. Start von Samba und dem Univention S4 Connector zur Replikation der AD-Objekte in das UCS-OpenLDAP-Verzeichnis.
4. 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` (Seite 157) auf den spezifischen Namen gesetzt (analog für Benutzer, z.B. `users/default/administrator` (Seite 169)).

Zusätzliche Informationen werden nach `/var/log/univention/ad-takeover.log` sowie nach `/var/log/univention/management-console-module-adtakeover.log` protokolliert.

Nun enthält der UCS Directory Node 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.

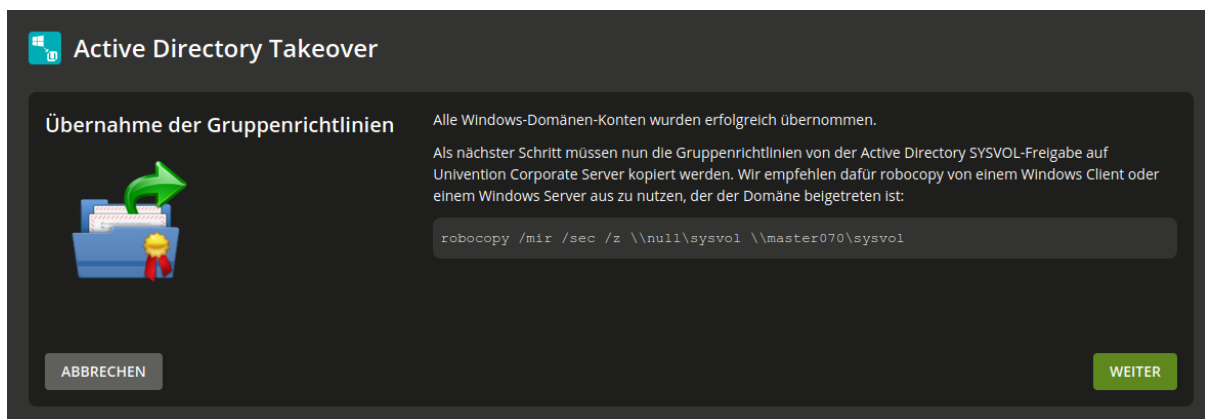


Abb. 9.11: Kopieren der SYSVOL-Freigabe

Wenn `robocopy` nicht vorhanden ist, kann es mit den Windows Server 2003 Resource Kit Tools nachinstalliert werden. Ab Windows 2008 ist es vorinstalliert.

Bemerkung

Hinweis: Die `robocopy`-Option `/mir` spiegelt das Quellverzeichnis mit dem Zielverzeichnis. Es muss beachtet werden, dass 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.

Die folgenden Schritte werden nun automatisch durchgeführt:

1. Übertragung der FSMO-Rollen auf den UCS Directory Node. Diese kennzeichnen verschiedene Aufgaben, die ein Server in einer AD-Domäne übernehmen kann.
2. Einrichten des Rechnernamens des AD-Servers als DNS-Alias (siehe *CNAME-Record (Alias-Records)* (Seite 98)) für den UCS-Server.
3. Konfiguration der IP-Adresse des AD-Servers als zusätzliche virtuelle IP-Adresse des UCS-Servers.
4. Verschiedene Anpassungen, z.B. Entfernen des alten AD-Domänencontroller-Eintrags aus der Samba SAM-Datenbank.
5. Abschließender Neustart von Samba und DNS-Server.

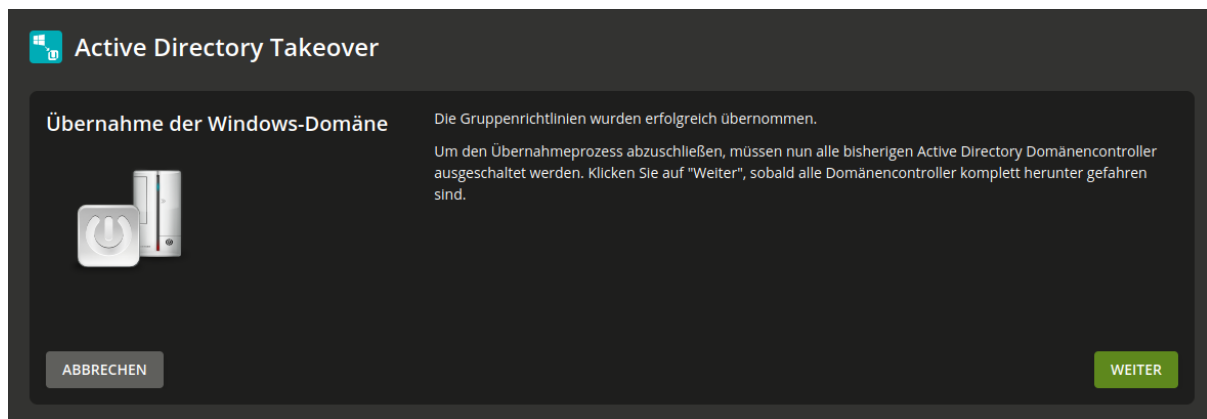


Abb. 9.12: Herunterfahren des/der AD-Systeme

9.3.3 Abschluss der Übernahme

Abschließend müssen noch die folgenden Schritte durchgeführt werden:

1. 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
```

2. Gab es in der migrierten AD-Domäne mehr als einen Domänencontroller, müssen die Rechnerkonten der weiteren Domänencontroller im UMC-Modul *Rechnerverwaltung* gelöscht werden. Außerdem müssen sie aus der Samba SAM-Datenbank gelöscht werden. Dies kann erreicht werden, 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.
3. Gibt es weitere Samba-Domänencontroller, müssen diese neu der Domäne beitreten.
4. Alle Windows-Clients müssen neu gestartet werden.

9.3.4 Tests

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.

9.4 Vertrauensstellungen

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 bedingte DNS Weiterleitung ein.

Für das folgende Beispiel sei angenommen, dass der UCS Samba/AD DC Primary Directory Node `primary.ucsdm.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 <<__EOT__
zone "addom.example" {
    type forward;
    forwarders { 192.0.2.20; };
};
__EOT__
$ systemctl restart named
```

Der Erfolg kann mit folgendem Befehl überprüft werden:

```
$ 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.

Vertrauensstellungen können nur auf Domänencontrollern eingerichtet werden, gelten dann aber für die gesamte Domäne.

Nach dieser Vorarbeit kann die Vertrauensstellung direkt von der Kommandozeile des UCS Samba/AD DCs eingerichtet werden. 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@ucsdm.example` angegeben werden.

Identity Management Anbindung an Cloud-Dienste

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, z.B. 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.

10.1 Microsoft 365 Connector

Der **Microsoft 365 Connector** ermöglicht die Synchronisation von Benutzern, Gruppen und Teams mit einer Azure Directory Domain. Über den Connector können Administratoren steuern, welche Benutzerkonten in UCS den Service Microsoft 365 nutzen können. Der Connector stellt die ausgewählten Benutzerkonten in der Azure Active Directory Domäne bereit. Administratoren können konfigurieren, welche Attribute von Benutzerkonten der Connector synchronisiert und welche Attribute der Connector während der Synchronisation anonymisiert.

Der Connector richtet Single Sign-On über den offenen Standard SAML ein. In dieser Konstellation ist UCS der Identity Provider und Microsoft 365 der Service Provider. Nutzer können über Single Sign-On in ihrem Webbrowser auf Microsoft 365 zugreifen, indem sie sich bei UCS anmelden.

Das Authentifizierungsverfahren überträgt keine Passwort-Hashes an Microsoft Azure Cloud. Die Benutzer authentifizieren sich ausschließlich über ihren Webbrowser. Der Webbrowser muss in der Lage sein, die DNS-Einträge der UCS-Domäne aufzulösen, was insbesondere bei mobilen Geräten zu beachten ist.

Wichtig

Das Single Sign-On Setup zwischen UCS und Microsoft 365 nutzt den offenen Standard Security Assertion Markup Language (SAML). Der Webbrowser des Benutzers ist das zentrale Element für die Authentifizierungskommunikation. Daher unterstützen UCS und der **Microsoft 365 Connector** Single Sign-On zu Microsoft 365 nur über den Webbrowser des Benutzers.

10.1.1 Einrichtung

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**²⁸⁰ benötigt. Die ersten 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.

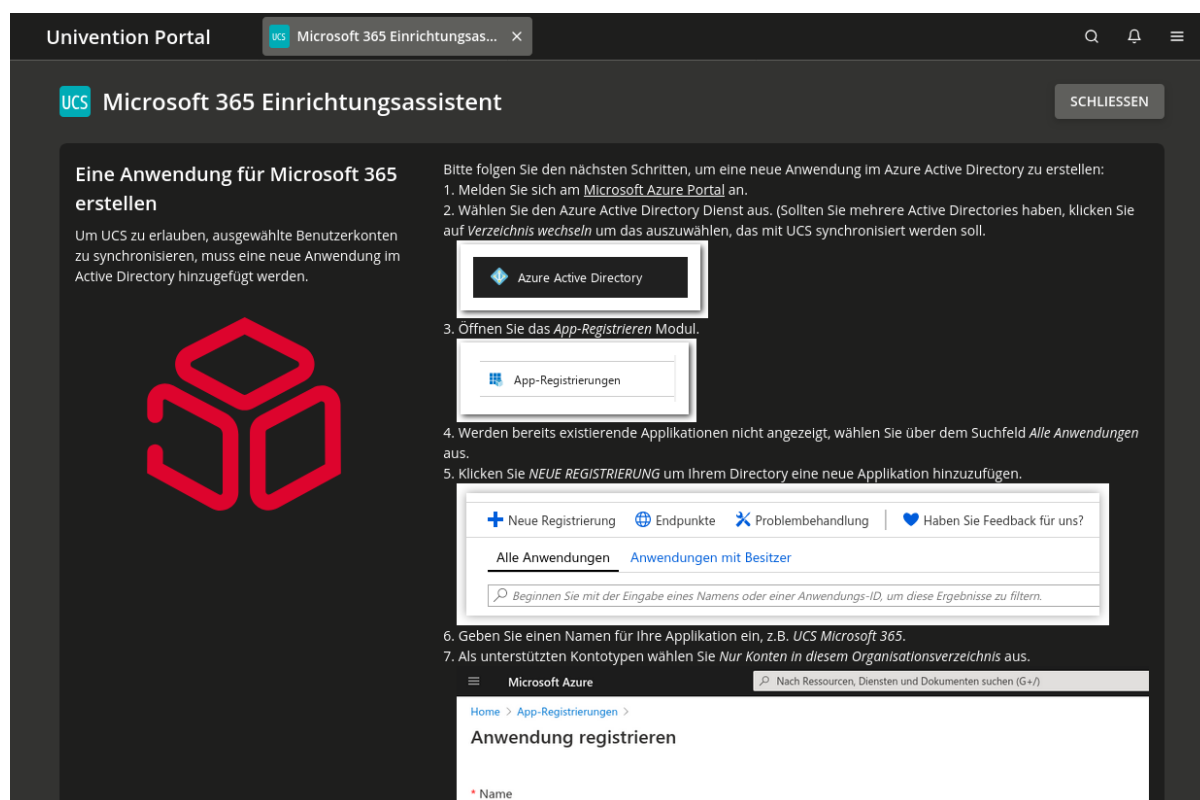


Abb. 10.1: Microsoft 365 Einrichtungsassistent

10.1.2 Konfiguration

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.

²⁸⁰ <https://learn.microsoft.com/de-de/entra/fundamentals/add-custom-domain>

Benutzer

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 werden, 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` (Seite 164) kann ein 2-Zeichen-Kürzel, z.B. DE vorgegeben werden.

Über die Univention Configuration Registry Variable `office365/attributes/sync` (Seite 164) wird konfiguriert, welche LDAP Attribute (z.B. Vorname, Nachname) 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` (Seite 164) 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/.*` (Seite 164) erlauben das Füllen von Attributen auf Microsoft Seite mit einem vordefinierten Wert.

Mit der Univention Configuration Registry Variable `office365/attributes/never` (Seite 164) können kommasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese in `office365/attributes/sync` (Seite 164) oder `office365/attributes/anonymize` (Seite 164) auftauchen.

Die Univention Configuration Registry Variablen `office365/attributes/mapping/.*` (Seite 164) 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` (Seite 165) aktiviert werden.

Änderungen an Univention Configuration Registry Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

Gruppen

Der **Microsoft 365 Connector** kann Gruppen mit Microsoft Azure Active Directory synchronisieren. Der Connector synchronisiert eine Gruppe, wenn sie mindestens einen Benutzer enthält, der für *Microsoft 365* aktiviert ist. Standardmäßig erstellt der Connector die Gruppe als *Sicherheitsgruppe* in *Microsoft 365*.

Sie können die Synchronisation aktivieren, indem Sie die Univention Configuration Registry Variable `office365/groups/sync` (Seite 165) auf `yes` setzen.

Added in version 5.0-7-erratum-1060: Mit [UCS 5.0 erratum 1060²⁸¹](#) können Sie den Gruppentyp auf `Microsoft365 Group` in der UMC auf der Registerkarte *Microsoft 365* ändern.

Wenn das UCS-System, auf dem der Connector installiert ist, nicht mindestens diese Versionsstand hat, können Sie den Gruppentyp nicht ändern.

Wenn Sie den Gruppentyp ändern, löscht der Connector die bestehende Gruppe in *Microsoft 365*, und erstellt eine Gruppe mit dem von Ihnen definierten Gruppentyp. *Microsoft 365* erlaubt es nicht, die Gruppentyp-Eigenschaft einer bestehenden Gruppe zu ändern. Der Connector fügt die Gruppenmitglieder zur Gruppe hinzu, und, wenn die Gruppe ein *Microsoft 365 Team* ist, erstellt der Connector auch das Team.

²⁸¹ <https://errata.software-univention.de/#/?erratum=5.0x1060>

Vorsicht

Das Ändern des Gruppentyps kann sich auf die Berechtigungen und Einstellungen der Gruppe in *Microsoft 365* auswirken. Ändern Sie Gruppentypen mit Vorsicht.

Sie können den Standard-Gruppentyp einer Microsoft 365-Gruppe ändern. Die folgenden Gruppentypen sind verfügbar:

- Security
- Microsoft 365 Group

Um den Gruppentyp zu ändern, müssen Sie den Standardwert des erweiterten Attributs `UniventionMicrosoft365GroupType` auf einen der verfügbaren Gruppentypen ändern:

```
$ udm settings/extended_attribute modify \
  --dn "cn=UniventionMicrosoft365GroupType,cn=custom attributes,cn=univention,
  ↪$(ucr get ldap/base)" \
  --set default="Microsoft 365 Group"
```

Added in version 6.3: Beginnend mit Version 6.3 können Sie die Sichtbarkeit von `Microsoft365` Gruppen in der UMC auf der Registerkarte *Microsoft 365* ändern. Die neue Voreinstellung ist `Private`.

Wenn der *Microsoft 365 Connector* auf dem UCS-System nicht mindestens Version 6.3 hat, können Sie die Gruppensichtbarkeit nicht ändern.

Sie können den Standard-Gruppentyp einer Microsoft 365-Gruppe ändern. Die folgenden Gruppentypen sind verfügbar:

Private

Voreinstellung bei Nubus

Public

Voreinstellung bei Azure

None

Azure legt die Standardeinstellung fest.

Weitere Informationen zur Bedeutung dieser Optionen finden Sie unter [Sichtbarkeitsoptionen für Gruppen in Microsoft Graph REST API v1.0](#)²⁸².

Um die Standard-Gruppensichtbarkeit zu ändern, müssen Sie den Standardwert des erweiterten Attributs `UniventionMicrosoft365GroupVisibility` auf eine der verfügbaren Optionen ändern. Führen Sie den Befehl in [Quellcode 10.1](#) aus, um den Standardwert zu ändern.

Quellcode 10.1: Ändern der Voreinstellung des erweiterten Attributs `UniventionMicrosoft365GroupVisibility`

```
$ udm settings/extended_attribute modify \
  --dn "cn=UniventionMicrosoft365GroupVisibility,cn=custom attributes,
  ↪cn=univention,$(ucr get ldap/base)" \
  --set default="" # oder --remove default
```

Teams

Für die Nutzung von Teams muss die Synchronisation von Gruppen per `Univention Configuration Registry Variable` `office365/groups/sync` (Seite 165) mit dem Wert `yes` aktiviert werden, anschließend muss der Dienst `Univention Directory Listener` neu gestartet 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

²⁸² <https://learn.microsoft.com/de-de/graph/api/resources/group?view=graph-rest-1.0#group-visibility-options>

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. Das Einrichten 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.

10.1.3 Synchronisation von Benutzern in mehrere Azure Active Directories

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 zugewiesen 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` (Seite 164) 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. Der Wizard übernimmt diese Aufgabe automatisch.

Der 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.

IdP initiierte Logins können über die Kacheln im Univention Portal angestoßen werden, die die App während der Konfiguration der ersten Verbindung erstellt. Alle folgenden Verbindungen brauchen dann aber eigene Kacheln; die App erzeugt keine weiteren. Stattdessen existiert das Skript `/usr/share/univention-office365/scripts/generate-portal-tile-for-ad-connection`, das entsprechende Kacheln erstellen kann. Das Skript braucht als erstes Argument den Namen der Azure AD Verbindung, weitere Argumente können genutzt werden, um die Sichtbarkeit der Kachel einzuschränken: Bei sehr vielen Verbindungen (und damit auch sehr vielen Kacheln) kann das Portal leicht überladen wirken. Im Portal können Kacheln auf bestimmte Gruppen beschränkt werden; diese Gruppen kann man dem Skript übergeben. Die Kachel wird einem Benutzer in diesem Fall nur dann angezeigt, wenn er Mitglied mindestens einer der Gruppen ist. Bitte beachten Sie, dass das bedeutet, dass die Kachel dann nur gesehen werden kann, wenn sich der Benutzer bereits eingeloggt hat.

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` (Seite 164). 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.

10.1.4 Fehlersuche

Meldungen während der Einrichtung werden in der 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` (Seite 164) können mehr Debugausgaben aktiviert werden.

10.2 Google Apps for Work Connector

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.

10.2.1 Einrichtung

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](#)²⁸³ 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 [Google Workspace für Ihre Organisation einrichten](#)²⁸⁴ 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](#)²⁸⁵ 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.

10.2.2 Konfiguration

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 Variablen `google-apps/attributes/mapping/.*` (Seite 157) wird konfiguriert, welche LDAP Attribute (z.B. Vorname, Nachname) 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/.*` (Seite 157) entfernt, so werden keine Daten außer der primären E-Mail-Adresse synchronisiert.

Mit der Univention Configuration Registry Variable `google-apps/attributes/anonymize` (Seite 157) können kommaspariert LDAP Attribute angegeben werden, die zwar in der G Suite Domäne angelegt, jedoch mit Zufalls-werten gefüllt werden.

²⁸³ <https://support.google.com/a/topic/9196?hl=de>

²⁸⁴ <https://knowledge.workspace.google.com/admin/getting-started/set-up-google-workspace-for-your-organization?hl=de>

²⁸⁵ <https://admin.google.com/>

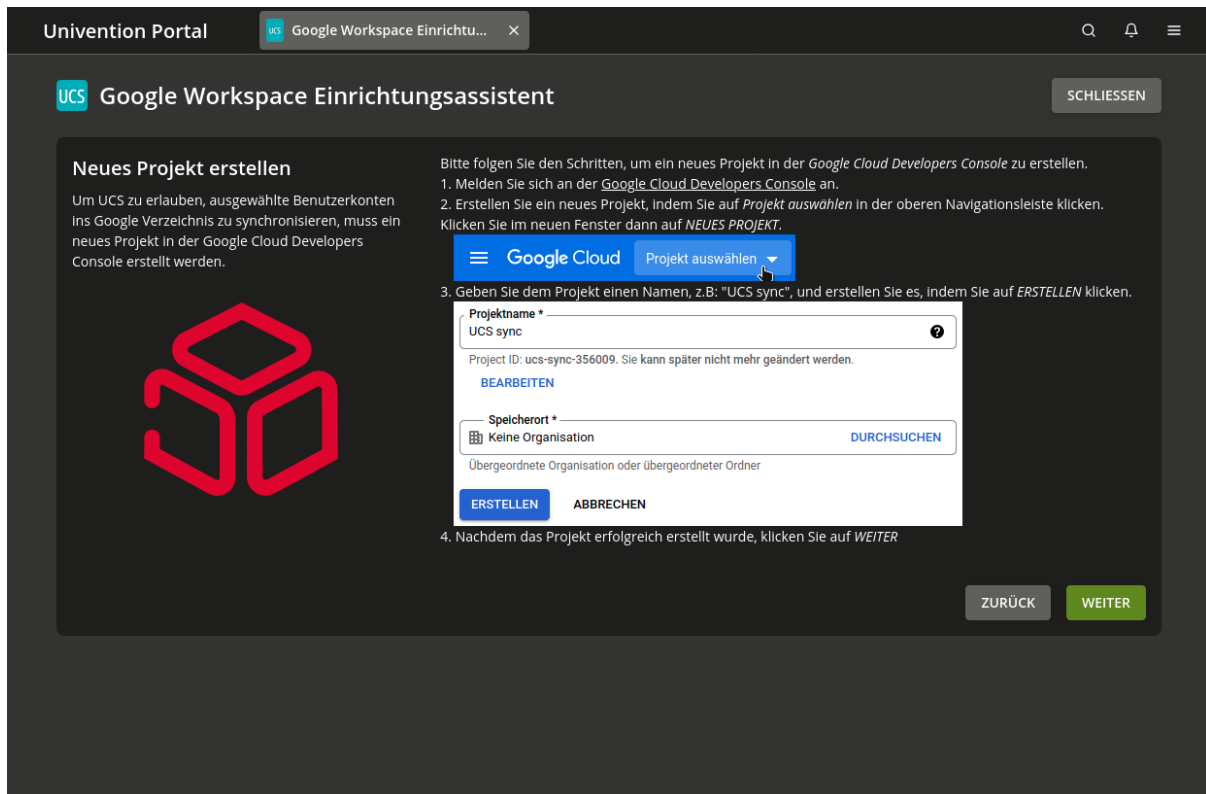


Abb. 10.2: Google Apps for Work Einrichtungsassistent

Mit der Univention Configuration Registry Variable `google-apps/attributes/never` (Seite 157) können komasepariert LDAP Attribute angegeben werden, die nicht synchronisiert werden sollen, selbst wenn diese per `google-apps/attributes/mapping/.*` (Seite 157) oder `google-apps/attributes/anonymize` (Seite 157) konfiguriert sind.

Die Synchronisation der Gruppen der Google Apps for Work Benutzer kann mit der Univention Configuration Registry Variable `google-apps/groups/sync` (Seite 157) aktiviert werden.

Änderungen an Univention Configuration Registry Variablen werden erst nach dem Neustart des Univention Directory Listener umgesetzt.

10.2.3 Fehlersuche

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` (Seite 157) können mehr Debugausgaben aktiviert werden.

IP- und Netzverwaltung

Dieses Kapitel beschreibt wie IP-Adressen für die in einer UCS-Domäne verwalteten Rechnersysteme zentral über UMC-Module verwaltet und per DHCP zugewiesen werden können.

Netzwerk-Objekte (Seite 95) 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 *Verwaltung von DNS-Daten mit BIND* (Seite 95) sowie *IP-Vergabe über DHCP* (Seite 98) erläutert.

Ein- und ausgehende Netzwerkverbindungen können über die in UCS integrierte *Univention Firewall* auf Basis von `iptables` begrenzt werden (*Paketfilter mit Univention Firewall* (Seite 100)).

Die Integration des Proxy-Servers Squid ermöglicht das Zwischenspeichern von Web-Inhalten und die Umsetzung inhaltlicher Richtlinien für den Web-Zugriff (*Web-Proxy für Caching und Policy Management/Virensan* (Seite 101)).

11.1 Netzwerk-Objekte

Der Inhalt dieses Abschnitts ist umgezogen nach *Netzwerke Modul*²⁸⁶ in *Nubus Handbuch 1.x* [6].

11.2 Verwaltung von DNS-Daten mit BIND

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 UCS Directory Node 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 *Netzwerk Konfiguration* (Seite 49) dokumentiert.

Folgende DNS-Daten werden unterschieden:

Forward Lookup Zone

Eine *Forward Lookup Zone* enthält Informationen, die zum Auflösen von DNS-Namen in IP-Adressen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen autoritativen, primären Nameserver, dessen Informationen für eine Zone maßgeblich sind. Untergeordnete Server synchronisieren sich mit dem autoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA-Record*.

²⁸⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/network.html#nubus-domain-network-management>

MX-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 E-Mails entgegennimmt.

TXT-Records

TXT-Records enthalten menschenlesbaren Text und können beschreibende Informationen zu einer Forward Lookup Zone enthalten.

CNAME-Record

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.

A-Record

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.

SRV-Record

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 Primary Directory Node domänenweit bekannt zu machen.

Reverse Lookup Zone

Eine *Reverse Lookup Zone* enthält Informationen, die zur Auflösung von IP-Adressen in DNS-Namen herangezogen werden. Jede DNS-Zone verfügt über mindestens einen autoritativen, primären Nameserver, dessen Informationen für eine Zone maßgeblich sind. Untergeordnete Server synchronisieren sich mit dem autoritativen Server über Zonentransfers. Der Eintrag, der eine solche Zone auszeichnet, ist der *SOA Record*.

PTR-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

Konfiguration der Debug-Ausgaben von BIND

Der Detailgrad der Debugausgaben von BIND kann über die Univention Configuration Registry-Variablen *dns/debug/level* (Seite 156) und *dns/dlz/debug/level* (Seite 156) (für das Samba-Backend, siehe *Konfiguration des Daten-Backends des Nameservers* (Seite 96)) konfiguriert werden. Die möglichen Werte reichen von 0 (keine Debug-Ausgaben) bis 11. Eine komplette Aufstellung der Detailgrade findet sich unter Liu and Albitz [14].

Konfiguration des Daten-Backends des Nameservers

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 UMC-Module konfiguriert, das seine Daten im LDAP-Verzeichnis speichert.

BIND kann zwei verschiedene Backends für seine Konfigurationsdateien verwenden:

LDAP-Backend

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-Backend

Samba/AD 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 der Netlogon-Freigabe. Wird Samba/AD eingesetzt, wird der betreffende UCS Directory Node auf die Verwendung des *Samba-Backends* 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/AD-Systemen führen.

Das Backend wird über die Univention Configuration Registry Variable `dns/backend` (Seite 155) konfiguriert. Die DNS-Verwaltung ändert sich durch das verwendete Backend nicht und erfolgt in beiden Fällen über UMC-Module.

Konfiguration von Zonentransfers

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` (Seite 155) auf `none` deaktiviert werden.

11.2.2 Konfiguration der DNS-Daten über Univention Management Console Modul

Der Inhalt dieses Abschnitts ist umgezogen nach [DNS Modul](#)²⁸⁷ in *Nubus Handbuch 1.x* [6].

Forward Lookup Zone

Der Inhalt dieses Abschnitts ist umgezogen nach [Forward Lookup Zone](#)²⁸⁸ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Forward Lookup - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Allgemein - DNS Forward Lookup Zone](#)²⁸⁹ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Forward Lookup - Reiter Start of Authority

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Start of Authority - DNS Forward Lookup Zone](#)²⁹⁰ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Forward Lookup - Reiter IP Adressen

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter IP Adressen - DNS Forward Lookup Zone](#)²⁹¹ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Forward Lookup - Reiter MX Records

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter MX Einträge - DNS Forward Lookup Zone](#)²⁹² in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Forward Lookup - Reiter TXT Records

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter TXT Einträge - DNS Forward Lookup Zone](#)²⁹³ in *Nubus Handbuch 1.x* [6].

²⁸⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns>

²⁸⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone>

²⁸⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone-general-tab>

²⁹⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone-soa-tab>

²⁹¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone-ip-addresses-tab>

²⁹² <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone-mx-records-tab>

²⁹³ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-forwardzone-txt-records-tab>

CNAME-Record (Alias-Records)

Der Inhalt dieses Abschnitts ist umgezogen nach CNAME Alias-Einträge²⁹⁴ in *Nubus Handbuch 1.x* [6].

A/AAAA-Records (Host Records)

Der Inhalt dieses Abschnitts ist umgezogen nach A/AAAA Host Einträge²⁹⁵ in *Nubus Handbuch 1.x* [6].

Service Records

Der Inhalt dieses Abschnitts ist umgezogen nach Service-Einträge²⁹⁶ in *Nubus Handbuch 1.x* [6].

Reverse Lookup Zone

Der Inhalt dieses Abschnitts ist umgezogen nach Reverse Lookup Zone²⁹⁷ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Reverse Lookup - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Allgemein - DNS Reverse Lookup Zone²⁹⁸ in *Nubus Handbuch 1.x* [6].

DNS UMC Modul Reverse Lookup - Reiter Start of Authority

Der Inhalt dieses Abschnitts ist umgezogen nach Reiter Start of Authority - DNS Reverse Lookup Zone²⁹⁹ in *Nubus Handbuch 1.x* [6].

Pointer Records

Der Inhalt dieses Abschnitts ist umgezogen nach Pointer Eintrag³⁰⁰ in *Nubus Handbuch 1.x* [6].

11.3 IP-Vergabe über DHCP

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 *Installation weiterer Software* (Seite 33).

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.

²⁹⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-records-alias>

²⁹⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-records-host>

²⁹⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-records-service>

²⁹⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-reversezone>

²⁹⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-reversezone-general-tab>

²⁹⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-reversezone-soa-tab>

³⁰⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dns.html#nubus-domain-dns-records-pointer>

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.

11.3.1 Aufbau der DHCP-Konfiguration durch DHCP-LDAP-Objekte

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Modul](#)³⁰¹ in *Nubus Handbuch 1.x* [6].

Verwaltung von DHCP-Services

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Dienste](#)³⁰² in *Nubus Handbuch 1.x* [6].

Verwaltung von DHCP-Server-Einträgen

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Server](#)³⁰³ in *Nubus Handbuch 1.x* [6].

Verwaltung von DHCP-Subnetzen

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Subnetze](#)³⁰⁴ in *Nubus Handbuch 1.x* [6].

Verwaltung von DHCP-Pools

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Pools](#)³⁰⁵ in *Nubus Handbuch 1.x* [6].

Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Allgemein - DHCP Pool](#)³⁰⁶ in *Nubus Handbuch 1.x* [6].

Reiter Erweiterte Einstellungen

Der Inhalt dieses Abschnitts ist umgezogen nach [Reiter Erweiterte Einstellungen - DHCP Pool](#)³⁰⁷ in *Nubus Handbuch 1.x* [6].

³⁰¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp>

³⁰² <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-services>

³⁰³ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-servers>

³⁰⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-subnets>

³⁰⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-pools>

³⁰⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-pools-tab-general>

³⁰⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-pools-tab-advanced>

Registrierung von Rechnern mit DHCP-Rechner-Objekten

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Host](#)³⁰⁸ in *Nubus Handbuch 1.x* [6].

Verwaltung von DHCP Shared Networks / DHCP Shared Subnets

Der Inhalt dieses Abschnitts ist umgezogen nach [DHCP Shared Network](#)³⁰⁹ in *Nubus Handbuch 1.x* [6].

11.3.2 Konfiguration von Clients durch DHCP-Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Konfiguration von Clients durch DHCP Richtlinien](#)³¹⁰ in *Nubus Handbuch 1.x* [6].

Vorgabe des Gateways

Der Inhalt dieses Abschnitts ist umgezogen nach [Einstellung des Gateways](#)³¹¹ in *Nubus Handbuch 1.x* [6].

Vorgabe der DNS-Server

Der Inhalt dieses Abschnitts ist umgezogen nach [Einstellen der DNS-Server](#)³¹² in *Nubus Handbuch 1.x* [6].

Vorgabe des WINS-Server

Der Inhalt dieses Abschnitts ist umgezogen nach [Einstellen der NetBIOS Server](#)³¹³ in *Nubus Handbuch 1.x* [6].

Konfiguration der DHCP-Vergabedauer (Lease)

Der Inhalt dieses Abschnitts ist umgezogen nach [Konfiguration der DHCP-Lease Zeit](#)³¹⁴ in *Nubus Handbuch 1.x* [6].

Konfiguration von Bootserver/PXE-Einstellungen

Der Inhalt dieses Abschnitts ist umgezogen nach [Konfiguration der Boot Server](#)³¹⁵ in *Nubus Handbuch 1.x* [6].

Weitere DHCP-Richtlinien

Der Inhalt dieses Abschnitts ist umgezogen nach [Weitere DHCP-Richtlinien](#)³¹⁶ in *Nubus Handbuch 1.x* [6].

11.4 Paketfilter mit Univention Firewall

Die Univention Firewall integriert einen Paketfilter auf Basis von `iptables` in Univention Corporate Server.

Sie ermöglicht die gezielte Filterung unerwünschter Dienste und die Absicherung von Rechnern während Installationsarbeiten. Darüber hinaus stellt sie die Basis für komplexere Szenarien wie Firewall-Regeln oder Application Level Gateways bereit. Univention Firewall ist standardmäßig in allen Univention Corporate Server-Installationen enthalten.

Standardmäßig blockiert UCS alle eingehenden Ports. Jedes UCS-Paket stellt Regeln bereit, die die vom Paket benötigten Ports wieder freigeben. Firewall-Regeln werden hauptsächlich über Univention Configuration Registry-Variablen konfiguriert. Informationen zur Definition von Paketfilter-Regeln finden Sie unter [Network packet filter](#)³¹⁷ in *Univention Developer Reference* [13].

³⁰⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-hosts>

³⁰⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-shared-network>

³¹⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies>

³¹¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-gateway>

³¹² <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-dns-servers>

³¹³ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-netbios>

³¹⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-dhcp-leases>

³¹⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-dhcp-boot>

³¹⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/dhcp.html#nubus-domain-dhcp-policies-further>

³¹⁷ <https://docs.software-univention.de/developer-reference/5.2/en/misc.html#misc-nacl>

Darüber hinaus enthält das Verzeichnis `/etc/security/packetfilter.d/` Skripte mit Firewall-Regeln. Die Namen aller Skripte beginnen mit zwei Ziffern, was eine nummerierte Reihenfolge ermöglicht. Die Skripte müssen als ausführbar markiert sein, damit UCS sie ausführen kann.

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` (Seite 167) auf `true` deaktiviert werden.

Siehe auch

netfilter/iptables Projekt-Homepage - Dokumentation zum netfilter/iptables Projekt³¹⁸
für einen Überblick über die verfügbare Dokumentation zu `iptables`.

Iptables Tutorial³¹⁹
ein Tutorial zu `iptables` von Oscar Andreasson.

iptables(8) Manpage³²⁰
für Informationen zur Konfiguration von Firewall-Regeln mit `iptables`.

Packet Filtering HOWTO³²¹
für ein Howto zur Paketfilterung mit `iptables`.

11.5 Web-Proxy für Caching und Policy Management/Virenschan

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.

Einige weiterführende Funktionen der Proxy-Dienste - wie etwa die Kaskadierung von Proxy-Servern - werden in *Extended IP and network management documentation* [15] beschrieben.

11.5.1 Installation

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 *Installation weiterer Software* (Seite 33).

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 *Zugriffsport* (Seite 102)), voreingestellt ist Port 3128.

Werden Änderungen an der Konfiguration vorgenommen, muss Squid neu gestartet werden. Dies kann entweder über das UMC-Modul *Systemdienste* oder auf der Kommandozeile erfolgen:

```
$ systemctl restart squid
```

Neben den in diesem Dokument beschriebenen Konfigurationsmöglichkeiten über Univention Configuration Registry können in der Datei `/etc/squid/local.conf` auch beliebige weitere Squid-Optionen gesetzt werden.

³¹⁸ <https://www.iptables.org/documentation/>

³¹⁹ <https://www.frozentux.net/iptables-tutorial/iptables-tutorial.html>

³²⁰ <https://manpages.debian.org/bookworm/iptables/iptables.8.en.html>

³²¹ <https://www.iptables.org/documentation/HOWTO/packet-filtering-HOWTO.html>

11.5.2 Caching von Webseiten

Squid ist ein *Caching proxy*, d.h. zuvor schon einmal angefragte Inhalte können aus einem Cache zur Verfügung gestellt werden ohne erneut vom jeweiligen Webserver geladen zu werden. Dies 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 oder 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` (Seite 168) deaktiviert werden, indem diese auf den Wert `no` gesetzt wird. Anschließend muss Squid neu gestartet werden.

11.5.3 Protokollierung von Zugriffen

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.

11.5.4 Einschränkung des Zugriffs auf erlaubte Netzwerke

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` (Seite 167) angegeben werden. Dabei muss die CIDR-Notation verwendet werden, mehrere Netzwerke sind durch Leerzeichen zu trennen.

Beispiel:

```
$ univention-config-registry set squid/allowfrom="192.0.2.0/24 192.0.3.0/24"
```

Nach einem Neustart von Squid ist jetzt der Zugriff aus den Netzwerken `192.0.2.0/24` und `192.0.3.0/24` erlaubt. Durch Angabe von `all` kann der Zugriff auch aus allen Netzen erlaubt werden.

11.5.5 Konfiguration der verwendeten Ports

Zugriffsport

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` (Seite 168) konfiguriert werden. Bei Verwendung von Univention Firewall muss zusätzlich die Paketfilterkonfiguration angepasst werden.

Erlaubte Ports

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` (Seite 168) geändert werden, mehrere Angaben sind dabei durch Leerzeichen zu trennen.

Beispiel:

```
$ 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

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.

Vorsicht

Um zu 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, indem 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:

LDAP Server Authentifizierung

Die Authentifizierung erfolgt direkt gegen den LDAP-Server. Dazu müssen die Univention Configuration Registry Variable `squid/basicauth` (Seite 167) auf `yes` gesetzt und Squid neu gestartet werden.

NTLM Authentifizierung

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 Authentifizierung durchführen. Um NTLM-Authentifizierung zu aktivieren, müssen die Univention Configuration Registry Variable `squid/ntlmauth` (Seite 168) auf `yes` gesetzt und Squid neu gestartet werden.

Kerberos Authentifizierung

Die Authentifizierung erfolgt über Kerberos. Benutzer, die an einem Windows-Client angemeldet sind, der Mitglied einer Samba/AD-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 müssen die Univention Configuration Registry Variable `squid/krb5auth` (Seite 168) auf `yes` gesetzt 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` (Seite 168) 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` (Seite 167) kann der Zugriff auf eine oder mehrere Gruppen beschränkt werden. Bei Angabe mehrerer Gruppen sind diese durch ein Semikolon zu trennen.

11.6 RADIUS

Die **RADIUS** App erhöht die Sicherheit für mit UCS verwaltete IT-Infrastrukturen durch Zugangskontrollen zu WLAN-Netzwerken für Benutzer, Gruppen und Endgeräte über das **RADIUS-Protokoll**³²². Die Konfiguration erfolgt über Blacklisten und Whitelisten direkt am Benutzer-, Gruppen- oder Endgeräte-Objekt im UCS Managementsystem. Registrierte Benutzer werden mit ihrem üblichen Domänenpasswort oder alternativ mit einem eigens erzeugten RADIUS-Passwort authentisiert, so dass unter anderem *Bring-Your-Own-Device-Konzepte* ermöglicht werden.

11.6.1 Installation

RADIUS steht über das App Center (siehe *Univention App Center* (Seite 31)) zur Verfügung und kann über das entsprechende UMC-Modul *App Center* installiert werden. Die App kann auf mehreren Systemen installiert werden. Nach der Installation startet die App einen **FreeRADIUS**³²³ Server. *Authenticators* (z.B. *Access Points*) können den Server via RADIUS kontaktieren und Netzwerkzugangsanfragen prüfen.

Die RADIUS App kann auch auf UCS@school Systemen installiert werden. In diesem Fall kann der Zugang an Benutzer oder Gruppen unabhängig von der Internetregel oder Computerraumeinstellungen vergeben werden.

³²² https://de.wikipedia.org/wiki/Remote_Authentication_Dial-In_User_Service

³²³ <https://www.freeradius.org/>

11.6.2 Konfiguration

Erlaubte Benutzer

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.

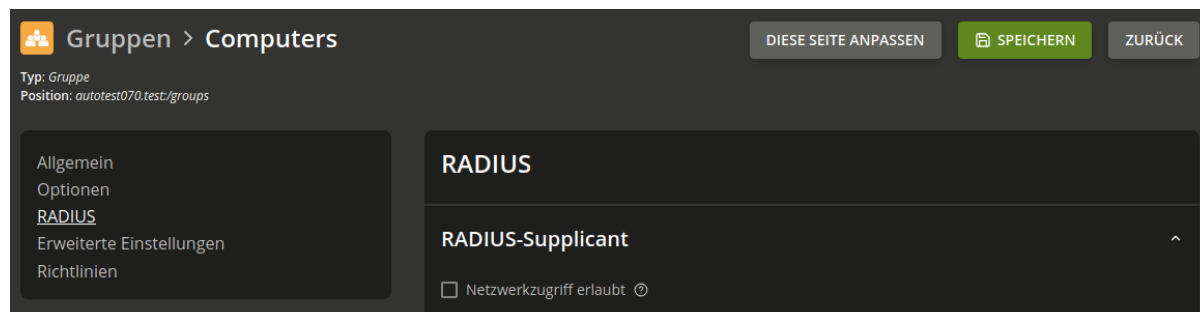


Abb. 11.1: Beispiel für eine Gruppe, die ihren Benutzern Zugang gewährt

Dienst-spezifisches Passwort

Standardmäßig authentifizieren sich die Benutzer mit ihrem Passwort für die Domäne. RADIUS verwendet ein de-ziertes Passwort, wenn ein Administrator den Parameter Univention Configuration Registry Variable *radius/use-service-specific-password* (Seite 166) auf *true* setzt. Benutzer können ein spezielles Passwort für die Verwendung von WLAN über die *Self Service App* (Seite 38) anfordern. UCS und die *Self Service App* generieren ein Zufallspasswort für jede Passwortanfrage. Bei Bedarf können die Benutzer jederzeit ein Zufallspasswort erzeugen, wodurch auch das bestehende Passwort ungültig wird.

Um die dienst-spezifische Passwortseite in der *Self Service App* zu aktivieren, muss der Administrator die Univention Configuration Registry Variable *umc/self-service/service-specific-passwords/backend/enabled* auf dem UCS-System, auf dem die *Self Service Backend App* installiert ist, auf den Wert *true* setzen.

UCS ermöglicht die Konfiguration der Passwortqualität für die automatisch generierten und dienst-spezifischen Passwörter durch die folgenden Univention Configuration Registry Variablen. Eine Beschreibung finden Sie in den Verweisen auf die jeweiligen generischen Passwortqualitätseinstellungen.

Tab. 11.1: RADIUS Passwortqualitätsparameter

RADIUS Passwortqualitätsparameter	Allgemeiner Qualitätsparameter für Passwörter
<code>password/radius/quality/credit/digits</code>	<code>password/quality/credit/digits</code> (Seite 165)
<code>password/radius/quality/credit/lower</code>	<code>password/quality/credit/lower</code> (Seite 165)
<code>password/radius/quality/credit/other</code>	<code>password/quality/credit/other</code> (Seite 165)
<code>password/radius/quality/credit/upper</code>	<code>password/quality/credit/upper</code> (Seite 165)
<code>password/radius/quality/forbidden/chars</code>	<code>password/quality/forbidden/chars</code> (Seite 165)
<code>password/radius/quality/length/min</code>	<code>password/quality/length/min</code> (Seite 165)

Wichtig

Die Einstellungen in den `password/quality/**` Univention Configuration Registry Variablen haben keinen Einfluss auf das dienst-spezifische Passwort.

WLAN-Passwort ×

Um sich am WLAN anzumelden, benötigen Sie ein gesondertes Passwort. Das Passwort wird vom System erzeugt und ist gültig, bis es wieder überschrieben wird. Sie können das Passwort einmalig beim Anlegen ansehen. Ein neues Passwort kann jederzeit erzeugt werden, womit das alte ungültig wird.

Benutzername*

Passwort*

Ihr neues Passwort lautet:

Bitte hinterlegen Sie es jetzt auf Ihrem Gerät.
Das Passwort wird nicht noch einmal angezeigt.

WLAN-PASSWORT ERZEUGEN

Abb. 11.2: Seite im Self Service, um ein RADIUS-spezifisches Passwort zu bekommen

Um die Passwortqualität zu konfigurieren, wählen Sie von den folgenden Reitern das Szenario aus, das Ihrer Umgebung entspricht, in der Sie die **RADIUS** App installiert haben.

Führen Sie die folgenden Schritte aus, um die Passwortqualität zu konfigurieren.

Voraussetzung

Sie haben die **RADIUS** App auf dem Primary Directory Node installiert.

1. Die verfügbaren Qualitätsparameter für Passwörter finden Sie entweder in [Tab. 11.1](#) oder in Ihrem System.

Öffnen Sie **auf dem Primary Directory Node** die Befehlszeile und sehen Sie die verfügbaren Qualitätsparameter für Passwörter nach:

```
$ ucr search password/radius/quality
```

2. Wählen Sie den Parameter, den Sie ändern möchten, und stellen Sie die entsprechende Univention Configuration Registry Variable ein, z. B. die minimale Passwortlänge.

```
$ ucr set password/radius/quality/length/min=32
```

Führen Sie die folgenden Schritte aus, um die Passwortqualität zu konfigurieren.

Voraussetzung

Sie haben die Anwendung **RADIUS** auf einem **anderen** UCS System installiert, als den Primary Directory Node.

1. Die verfügbaren Qualitätsparameter für Passwörter finden Sie entweder in [Tab. 11.1](#) oder in Ihrem System.

Auf dem UCS-System, auf dem die **RADIUS** App installiert ist, öffnen Sie die Befehlszeile und sehen Sie die verfügbaren Qualitätsparameter für Passwörter nach:

```
$ ucr search password/radius/quality
```

2. Wählen Sie den Parameter, den Sie ändern möchten, und setzen Sie die entsprechende Univention Configuration Registry Variable, z. B. die minimale Passwortlänge. Öffnen Sie auf dem Primary Directory Node die Befehlszeile und führen Sie den folgenden Befehl aus:

```
$ ucr set password/radius/quality/length/min=32
```

3. Unabhängig vom Szenario müssen Sie schließlich die *UDM HTTP REST API* auf dem Primary Directory Node neu starten. Öffnen Sie die Befehlszeile und führen Sie den folgenden Befehl aus.

```
$ systemctl restart univention-directory-manager-rest.service
```

MAC-Adressfilter

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* (Seite 166) 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).

MAC Authentication Bypass für Computerobjekte

MAC Authentication Bypass (MAB) ist ein proprietärer Fallback-Modus zu 802.1X für Geräte, die keine 802.1X-Authentifizierung unterstützen, wie Netzwerkdrucker oder drahtlose Telefone. MAB ist eine Option, die es solchen Geräten ermöglicht, sich mit ihrer MAC-Adresse als Benutzernamen beim Netzwerk zu authentifizieren.

Dieser Abschnitt beschreibt, wie Sie die MAC-Adresse eines Geräts zur Authentifizierung verwenden und ihm über MAB ein VLAN der entsprechenden Netzwerkinfrastruktur zuweisen. Um MAC Authentication Bypass zu aktivieren, setzen Sie die Univention Configuration Registry Variable *freeradius/conf/allow-mac-address-authentication* (Seite 156) auf `true`.

Wichtig

Geräte, die sich mit MAB authentifizieren, ignorieren die Netzwerkzugangseinstellungen:

- Univention Configuration Registry Variable `radius/mac/whitelisting` (Seite 166)
- Die Checkbox *Netzwerkzugriff zulassen* beim Computerobjekt und in der Gruppeneinstellung

Warnung

Angreifer können MAC-Adressen ausspionieren. Betrachten Sie jeden Anschluss als gefährdet, an dem Ihr Switch die Verwendung von MAB zulässt. Vergewissern Sie sich, dass Sie geeignete Maßnahmen ergriffen haben, um Ihr Netzwerk weiterhin sicher zu halten.

Um einem Computer die VLAN-ID zuzuweisen, müssen Sie ihn zur Gruppe des Computerobjekts hinzufügen, dass die entsprechende VLAN ID hat. Gehen Sie im UCS-Managementsystem wie folgt vor:

1. Öffnen Sie *Geräte* ▶ *Computer*.
2. Klicken Sie das Computerobjekt, das Sie bearbeiten möchten.
3. Gehen Sie zu *Erweiterte Einstellungen* ▶ *Gruppen*.
4. Um eine Gruppe mit VLAN-IDs hinzuzufügen, klicken Sie auf *ADD*, wählen Sie `Virtual LAN ID` aus der Dropdown-Liste *Objekteigenschaft* und aktivieren Sie die entsprechende Gruppe, um sie hinzuzufügen.
5. Um zu speichern, klicken Sie auf *HINZUFÜGEN* im *Objekte hinzufügen* Dialog und *SAVE* in *Erweiterte Einstellungen*.

Um die VLAN-ID einer Benutzergruppe zuzuweisen, müssen Sie sie zu den Benutzergruppeneinstellungen hinzufügen. Führen Sie im UCS-Managementsystem die folgenden Schritte aus:

1. Öffnen Sie *Benutzer* ▶ *Gruppen*.
2. Klicken Sie die Benutzergruppe zum Bearbeiten oder erstellen Sie eine neue Benutzergruppe.
3. Gehen Sie zu *RADIUS*.
4. Geben Sie die VLAN ID als Zahl in das Feld *Virtual LAN ID*.
5. Zum Speichern, klicken Sie *SPEICHERN*.

Wenn einem Computerobjekt mehrere Gruppen mit VLAN-IDs zugeordnet sind, wählt UCS die VLAN-ID mit der niedrigsten Nummer aus und weist sie zu. Um eine Standard VLAN-ID zu konfigurieren, setzen Sie diese als Wert in die Univention Configuration Registry Variable `freeradius/vlan-id` (Seite 156).

Nachdem Sie die Konfiguration abgeschlossen haben, gibt der Radius-Server die zugewiesene VLAN-ID an Anfragen mit der angegebenen MAC-Adresse zurück.

UCS speichert die MAC-Adresse im LDAP-Verzeichnis als Zeichenkette in Kleinbuchstaben mit dem Doppelpunkt (:) als Trennzeichen, zum Beispiel `00:00:5e:00:53:00`.

Added in version 5.0-6-erratum-1011: Mit UCS 5.0 erratum 1011³²⁴ kann der Radius-Server mit verschiedenen Formaten der MAC Adresse für Benutzernamen umgehen, wenn MAB verwendet wird.

Geräte, die MAB verwenden, benutzen ihre MAC-Adresse als Benutzernamen und sie können unterschiedliche Formate dafür verwenden. Der Radius-Server unterstützt verschiedene Formate, die Groß- und Kleinschreibung unterscheiden. In der folgenden Liste sind die getesteten Formate aufgeführt:

- `XX:XX:XX:XX:XX:XX`
- `XX-XX-XX-XX-XX-XX`
- `XX.XX.XX.XX.XX.XX`

³²⁴ <https://errata.software-univention.de/#/?erratum=5.0x1011>

- XXXX.XXXX.XXXX
- XXXXXXXXXXXXX

Bemerkung

Für nicht-standardisierte Formate können Sie einen regulären Ausdruck in der Univention Configuration Registry Variable `freeradius/conf/mac-addr-regexp` (Seite 156) konfigurieren, der mit Ihrem benutzerdefinierten MAC-Adressformat zusammen passt.

Je nach regulärem Ausdruck kann es vorkommen, dass die zuvor aufgeführten Formate nicht mehr funktionieren.

Wichtig

Alle Geräte, die MAB verwenden, müssen dasselbe Passwort haben, da *dienstspezifische Passwörter* (Seite 104) nicht funktionieren, und der Switch muss das Passwort kennen. Sie können nur ein Gerätepasswort im Switch konfigurieren. Sie können Ihr eigenes Passwort für die Geräte mit MAB erstellen, zum Beispiel `mab request format attribute 2 password1`.

Wenn die Netzwerkinfrastruktur ein anderes Format vorsieht, können Sie das Format häufig neu konfigurieren. Für Cisco-Switches können Sie zum Beispiel `mab request format attribute 1 groupize 2 separator : lowercase` verwenden, wie in [Configurable MAB Username and Password](#)³²⁵ beschrieben.

Access Points verwalten

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 über das UMC-Modul *Rechner*. 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 eines Access Points in der `clients.conf` Datei:

```
client AP01 {
    secret = a9RPAeVG
    ipaddr = 192.0.2.101
}
```

Um *Access Points* über das UMC-Modul *Rechner* zu verwalten muss ein Rechnerobjekt erstellt oder ausgewählt werden und die Option *RADIUS-Authenticator* (*Setzen der RADIUS-Option* (Seite 109)) aktiviert werden. Für einen *Access Point* bietet sich ein *IP-Client* als Rechnerobjekt an. Im *RADIUS*-Reiter des Objekts lassen sich nach dem Hinzufügen der Option die Eigenschaften des *Access Points* festlegen (*RADIUS-Authenticator Optionen* (Seite 109)). 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 über UMC-Modul *Rechner* 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.

Konfiguration von Access Point und Client

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 `secret` aus dem Eintrag in der `clients.conf` für den Access Point gesetzt sein.

³²⁵ https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_aaa/configuration/15-e/sec_usr_aaa-15-e-book/sec_usr-config-mab-username-pwd.html

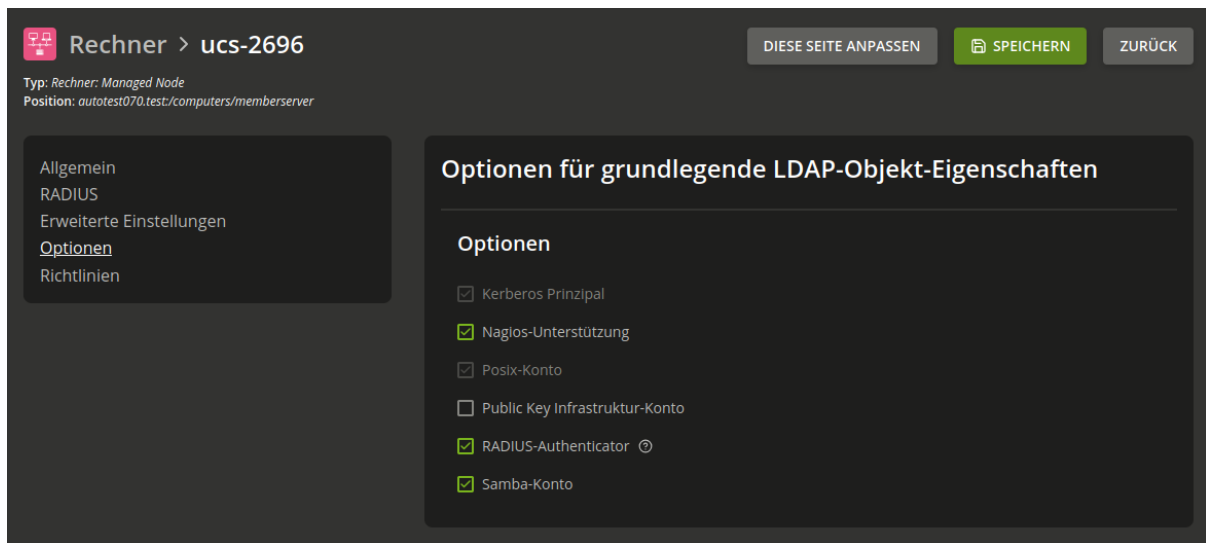


Abb. 11.3: Setzen der RADIUS-Option

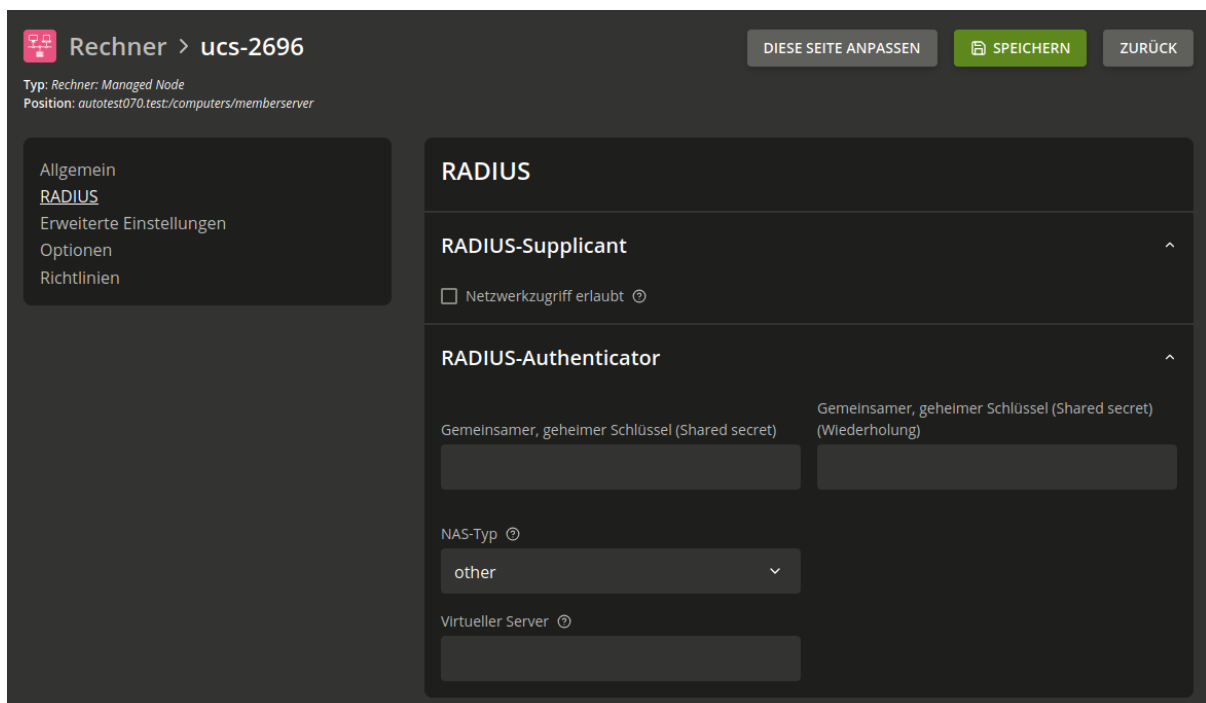


Abb. 11.4: RADIUS-Authenticator Optionen

WLAN Clients müssen so konfiguriert sein, dass sie *WPA* mit *PEAP* und *MSCHAPv2* für die Authentisierung verwenden.

VLAN IDs

Virtual Local Area Networks (VLANs) können verwendet werden, um den Datenverkehr der Benutzer auf der Netzwerkebene zu trennen. UCS kann so konfiguriert werden, dass es eine VLAN-ID in der Radius-Antwort des Radius-Authentifizierungsprozesses gemäß **RFC 3580 / IEEE 802.1X**³²⁶ zurück gibt. Weitere Informationen finden Sie in *Konfiguration VLAN* (Seite 49).

Die VLAN-ID für einen Benutzer kann konfiguriert werden, indem der Benutzer einer Gruppe mit einer VLAN-ID zugewiesen wird.

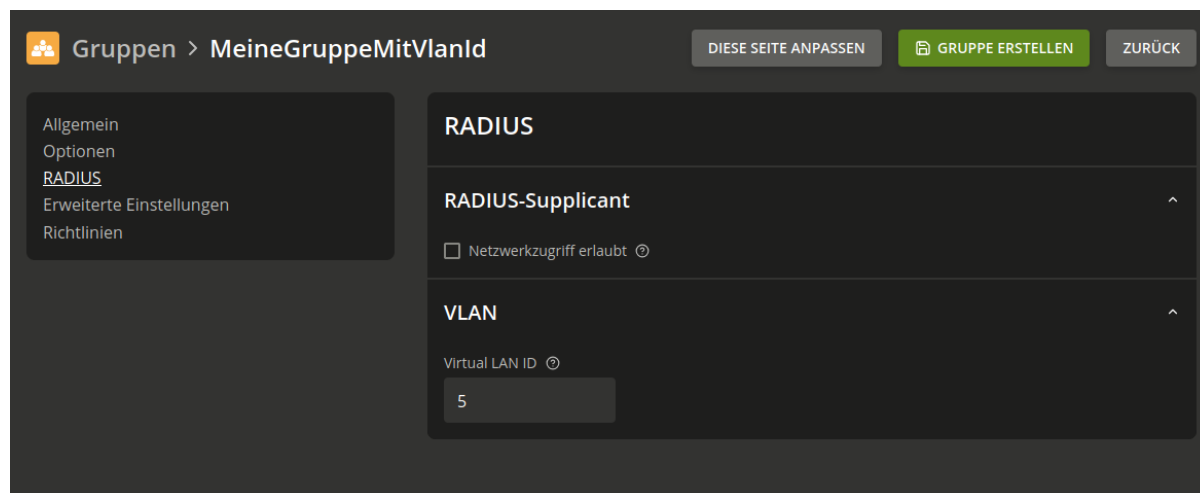


Abb. 11.5: Zuweisung VLAN ID zu einer Benutzergruppe

Eine Standard VLAN-ID kann in der Univention Configuration Registry Variable `freeradius/vlan-id` (Seite 156) konfiguriert werden. Diese Standard VLAN-ID wird zurückgegeben, wenn der Benutzer nicht Mitglied einer Gruppe mit einer VLAN-ID ist. Die Radius Antwort wird keine VLAN-ID enthalten, wenn der Benutzer nicht Mitglied einer Gruppe mit VLAN-ID ist und keine Standard VLAN-ID definiert ist.

TLS 1.3 deaktivieren

Radius verwendet Transport Layer Security (TLS) zur Verschlüsselung des Webverkehrs. Die aktuellen Versionen aller wichtigen Betriebssysteme unterstützen TLS 1.3. Bei einigen Betriebssystemen, wie Microsoft Windows 10, gibt es Probleme mit der verwendeten Radius-Implementierung. Detaillierte Informationen finden Sie unter [Bug #55247](#)³²⁷.

Wenn Sie diese noch verwenden, müssen Sie TLS v1.3 möglicherweise deaktivieren. Um TLS auf Version 1.2 zu beschränken, ändern Sie die Univention Configuration Registry Variable `freeradius/conf/tls-max-version` auf den Wert `1.2`.

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` (Seite 156) 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:

³²⁶ <https://datatracker.ietf.org/doc/html/rfc3580.html>

³²⁷ https://forge.univention.org/bugzilla/show_bug.cgi?id=55247

```
root@primary211:~# univention-radius-check-access --username=stefan --station-id_
↳none
DENY 'uid=stefan,cn=users,dc=ucs,dc=example'
'uid=stefan,cn=users,dc=ucs,dc=example'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=example'
Thus access is DENIED.
```

```
root@primary211:~# univention-radius-check-access --username=janeK --station-id_
↳none
DENY 'uid=janeK,cn=users,dc=ucs,dc=example'
'uid=janeK,cn=users,dc=ucs,dc=example'
-> DENY 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> ALLOW 'cn=Network Access,cn=groups,dc=ucs,dc=example'
-> 'cn=Domain Users,cn=groups,dc=ucs,dc=example'
-> -> DENY 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> -> 'cn=Users,cn=Builtin,dc=ucs,dc=example'
-> 'cn=Network Access,cn=groups,dc=ucs,dc=example'
Thus access is ALLOWED.
root@primary211:~#
```

Das Werkzeug gibt eine detaillierte Erläuterung und setzt den Rückgabewert abhängig vom Ergebnis der Zugangsprüfung (0 für *Zugang gestattet*, 1 für *Zugang verweigert*).

Verwaltung von Freigaben

UCS unterstützt die zentrale Verwaltung von Verzeichnisfreigaben. Eine im UMC-Modul *Freigaben* 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 im UMC-Modul 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 `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

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
- Ausführen

Pro Verzeichnis gelten ebenfalls drei Zugriffsrechte: Lesen, Schreiben und das Recht zu Ausführen von Programm, dass sich hier auf die Berechtigung bezieht, 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.

setuid

Ist die *setuid*-Option für eine ausführbare Datei gesetzt, kann diese von Benutzern mit den Rechten des Besitzers oder der Besitzergruppe ausgeführt werden.

setgid

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.

sticky bit

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 1042³²⁸ 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 vorbehalten. Unter Microsoft Windows hingegen verfügen alle Benutzer mit Schreibrechten auch über die Berechtigung, die Berechtigungen anzupassen. Dieses Verhalten kann für CIFS-Freigaben angepasst werden (siehe *Verwaltung von Freigaben über Univention Management Console Modul* (Seite 114)).

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. Werden Berechtigungen oder Besitzer im UMC-Modul *Freigaben* bearbeitet, werden die Änderungen im Dateisystem überschrieben. Einstellungen der Freigabewurzel sollten deshalb nur mit dem UMC-Modul 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 zugewiesenen Rechte der Freigabe und verwendet die Rechte des jeweiligen Heimatverzeichnisses.

12.2 Verwaltung von Freigaben über Univention Management Console Modul

Der Inhalt dieses Abschnitts wurde nach *Freigaben Modul*³²⁹ in *Nubus Handbuch 1.x* [6] verschoben.

12.2.1 Freigaben UMC Modul - Reiter Allgemein

Der Inhalt dieses Abschnitts wurde nach *Reiter Allgemein - Freigabenverwaltung*³³⁰ in *Nubus Handbuch 1.x* [6] verschoben.

12.2.2 Freigaben UMC Modul - Reiter NFS

Freigaben UMC Modul - NFS Gruppe

Der Inhalt dieses Abschnitts wurde nach *Reiter NFS - Freigabenverwaltung*³³¹ in *Nubus Handbuch 1.x* [6] verschoben.

Freigaben UMC Modul - Gruppe Erweiterte NFS-Einstellungen

Der Inhalt dieses Abschnitts wurde nach *Reiter NFS - Freigabenverwaltung*³³² in *Nubus Handbuch 1.x* [6] verschoben.

12.2.3 Freigaben UMC Modul - Reiter Samba

Der Inhalt dieses Abschnitts wurde nach *Reiter Samba - Freigabenverwaltung*³³³ in *Nubus Handbuch 1.x* [6] verschoben.

³²⁸ <https://help.univention.com/c/knowledge-base/supported/48>

³²⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares>

³³⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-general-tab>

³³¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-nfs-tab>

³³² <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-nfs-tab>

³³³ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab>

Freigaben UMC Modul - Gruppe Samba

Der Inhalt dieses Abschnitts wurde nach [Abschnitt Samba - Freigabenverwaltung](#)³³⁴ in *Nubus Handbuch 1.x* [6] verschoben.

Freigaben UMC Modul - Gruppe Samba-Rechte

Der Inhalt dieses Abschnitts wurde nach [Abschnitt Samba-Rechte - Freigabenverwaltung](#)³³⁵ in *Nubus Handbuch 1.x* [6] verschoben.

Freigaben UMC Modul - Gruppe erweiterte Samba-Rechte

Der Inhalt dieses Abschnitts wurde nach [Abschnitt Erweiterte Samba-Rechte - Freigabenverwaltung](#)³³⁶ in *Nubus Handbuch 1.x* [6] verschoben.

Freigaben UMC Modul - Gruppe Samba-Optionen

Der Inhalt dieses Abschnitts wurde nach [Abschnitt Samba Optionen - Freigabenverwaltung](#)³³⁷ in *Nubus Handbuch 1.x* [6] verschoben.

Freigaben UMC Modul - Gruppe Samba-Erweiterte-Einstellungen

Der Inhalt dieses Abschnitts wurde nach [Abschnitt Erweiterte Samba-Einstellungen - Freigabenverwaltung](#)³³⁸ in *Nubus Handbuch 1.x* [6] verschoben.

12.2.4 Freigaben UMC Modul - Reiter Optionen

Der Inhalt dieses Abschnitts wurde nach [Reiter Optionen - Freigabenverwaltung](#)³³⁹ in *Nubus Handbuch 1.x* [6] verschoben.

12.3 Unterstützung von MSDFS

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 *Verwaltung von Freigaben über Univention Management Console Modul* (Seite 114)) 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 Dateisystems nutzen zu können, muss auf dem Fileserver die Univention Configuration Registry Variable `samba/enable-msdfs` (Seite 166) 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.

³³⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab-samba>

³³⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab-samba-permissions>

³³⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab-samba-extended-permissions>

³³⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab-samba-options>

³³⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-samba-tab-samba-custom-settings>

³³⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/shares.html#nubus-domain-shares-options-tab>

Vorsicht

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 Jelmer R. Vernooij and Carter [16].

12.4 Konfiguration von Dateisystem-Quota

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:

Hard-Limit

Das *Hard-Limit* ist die maximale Speichermenge, die ein Benutzer in Anspruch kann. Wird sie erreicht, können keine weiteren Dateien angelegt werden.

Soft-Limit

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 *Konfiguration von Dateisystem-Quota* (Seite 117).

Dateisystem-Quota können nur auf Partitionen mit den Dateisystemen `ext4` und `xfs` angelegt werden. Bevor Dateisystem-Quota konfiguriert werden, muss der Quota-Support pro Partition aktiviert werden, siehe *Aktivierung von Dateisystem-Quota* (Seite 116).

12.4.1 Aktivierung von Dateisystem-Quota

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-Punkt eingebunden sind.

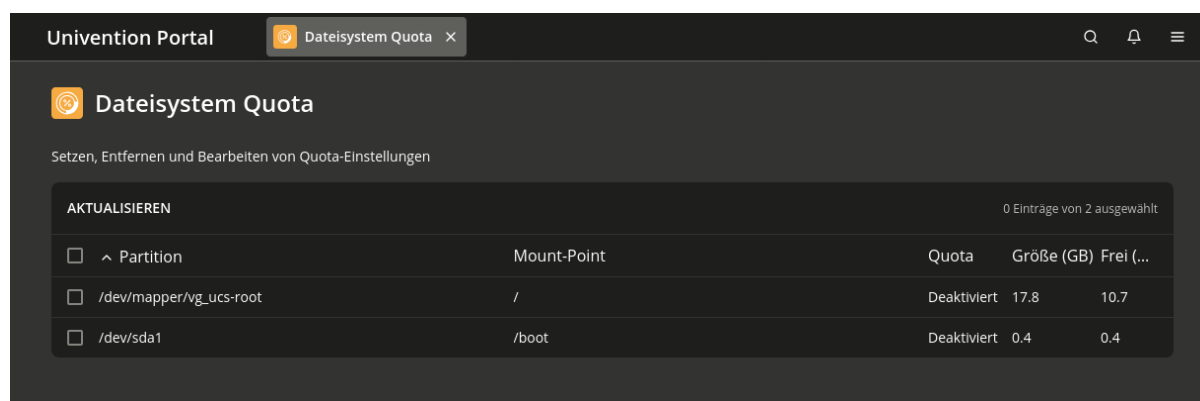


Abb. 12.1: Das UMC Modul *Dateisystem Quota*

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

Quotas können entweder über das UMC-Modul *Dateisystem Quota* oder über eine Richtlinie für Freigaben definiert werden, siehe *Richtlinien* (Seite 27). 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 können 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 *Aktivierung von Dateisystem-Quota* (Seite 116).

Bemerkung

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

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` (Seite 166) auf `no` deaktiviert werden.

Wird die Univention Configuration Registry Variable `quota/logfile` (Seite 166) 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

Ein Benutzer kann die für ein System definierten Quota-Begrenzungen mit dem Befehl `repquota -vCa` einsehen, z.B.:

```
*** Report for user quotas on device /dev/vdb1
Block grace time: 7days; Inode grace time: 7days

```

User	used	Block limits			File limits			
		soft	hard	grace	used	soft	hard	grace
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	

(Fortsetzung auf der nächsten Seite)

(Fortsetzung der vorherigen Seite)

```
Statistics:  
Total blocks: 8  
Data blocks: 1  
Entries: 4  
Used average: 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.

Univention Corporate Server beinhaltet ein Drucksystem, mit dem sich auch komplexe Umgebungen realisieren lassen. Drucker und Druckergruppen werden dabei im UMC-Modul *Drucker* 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 im UMC-Modul *Druckaufträge* verwaltet, siehe *Verwaltung von Druckaufträgen und Druckerwarteschlangen* (Seite 120).

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 *Integration weiterer PPD-Dateien* (Seite 126) 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-Client im UMC-Modul *Rechner* registriert werden (siehe *UCS-Systemrollen* (Seite 11)).

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.

Es können auch Druckerfreigaben von Windows-Systemen in den CUPS-Druckserver integriert werden, dies ist in *Konfiguration von Druckerfreigaben* (Seite 120) dokumentiert.

13.1 Installation eines Druckservers

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 *Installation weiterer Software* (Seite 33).

13.2 Einstellung lokaler Konfigurationseigenschaften eines Druckers

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` (Seite 155) 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-Warteschlange 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 *Verwaltung von Druckaufträgen und Druckerwarteschlangen* (Seite 120)). Wird die Univention Configuration Registry Variable `cups/errorpolicy` (Seite 154) auf `retry-job` gesetzt, versucht CUPS alle dreißig Sekunden automatisch erfolglose Druckaufträge erneut durchzuführen.

13.3 Konfiguration von Druckerfreigaben

Der Inhalt dieses Abschnitts wurde nach *Drucker-Modul*³⁴⁰ in *Nubus Handbuch 1.x* [6] verschoben.

13.3.1 Drucker UMC Modul - Reiter Allgemein

Der Inhalt dieses Abschnitts wurde nach *Reiter Allgemein - Drucker-Modul*³⁴¹ in *Nubus Handbuch 1.x* [6] verschoben.

13.3.2 Drucker UMC Modul - Reiter Zugriffskontrolle

Der Inhalt dieses Abschnitts wurde nach *Reiter Zugriffskontrolle - Drucker-Modul*³⁴² in *Nubus Handbuch 1.x* [6] verschoben.

13.4 Konfiguration von Druckergruppen

Der Inhalt dieses Abschnitts wurde nach *Druckergruppen*³⁴³ in *Nubus Handbuch 1.x* [6] verschoben.

13.5 Verwaltung von Druckaufträgen und Druckerwarteschlangen

Das UMC-Modul *Druckaufträge* erlaubt auf Druckservern den Status der angeschlossenen Drucker zu prüfen, angehaltene Drucker neu zu starten oder Druckaufträge aus den Warteschlangen zu entfernen.

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, der Standort und die Beschreibung angezeigt. Durch Markieren der Drucker und Ausführen einer der beiden Aktionen *deaktivieren* oder *aktivieren*, kann der Status mehrerer Drucker gleichzeitig geändert werden.

³⁴⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/printers.html#nubus-devices-printers>

³⁴¹ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/printers.html#nubus-devices-printers-tab-general>

³⁴² <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/printers.html#nubus-devices-printers-tab-access-control>

³⁴³ <https://docs.software-univention.de/nubus-manual/latest/de/management/devices/printers.html#nubus-devices-printers-groups>

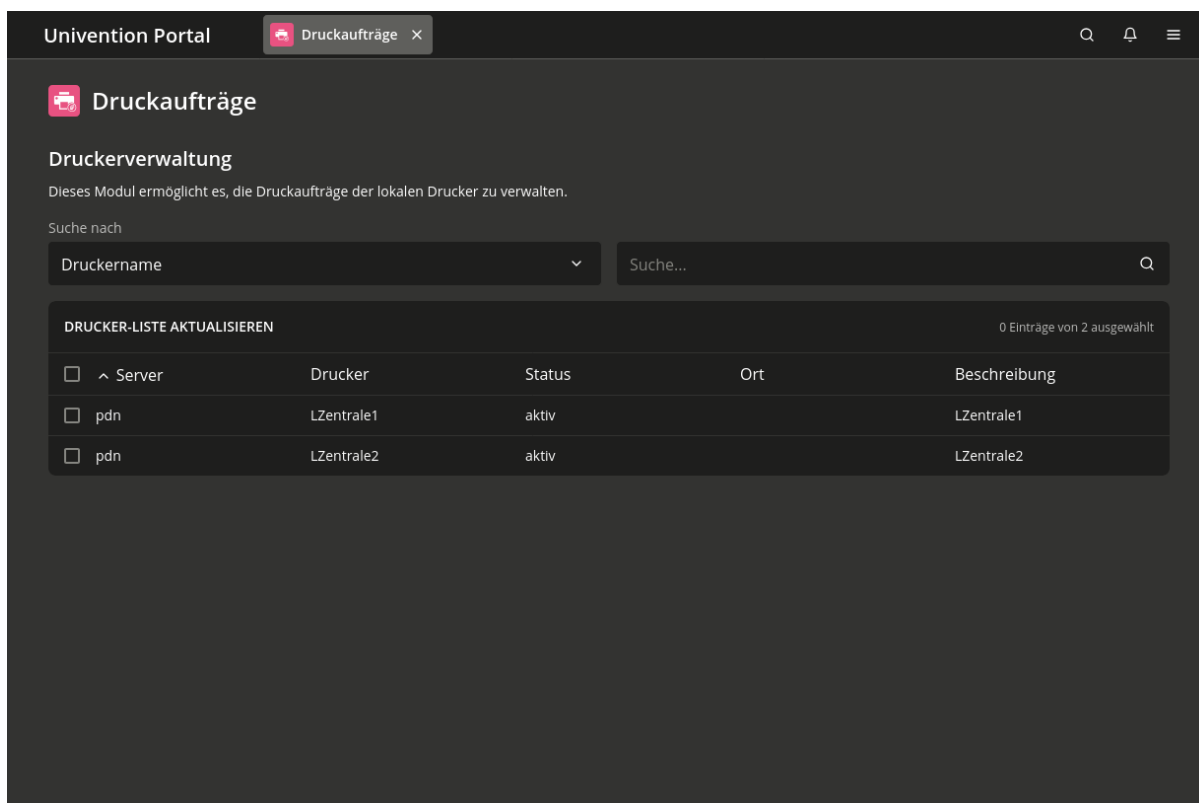


Abb. 13.1: Drucker-Administration

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.

13.6 Generierung von PDF-Dokumenten aus Druckaufträgen

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 im UMC-Modul *Drucker* (siehe *Konfiguration von Druckerfreigaben* (Seite 120)) 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` (Seite 154) 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` (Seite 154) 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` (Seite 154) 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` (Seite 154) konfiguriert werden.

13.7 Einbinden von Druckerfreigaben auf Windows-Clients

Die im UMC-Modul *Drucker* 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*.

Vorsicht

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 für eine im UMC-Modul *Drucker* 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.
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.
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` (Seite 167) 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.

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.
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.

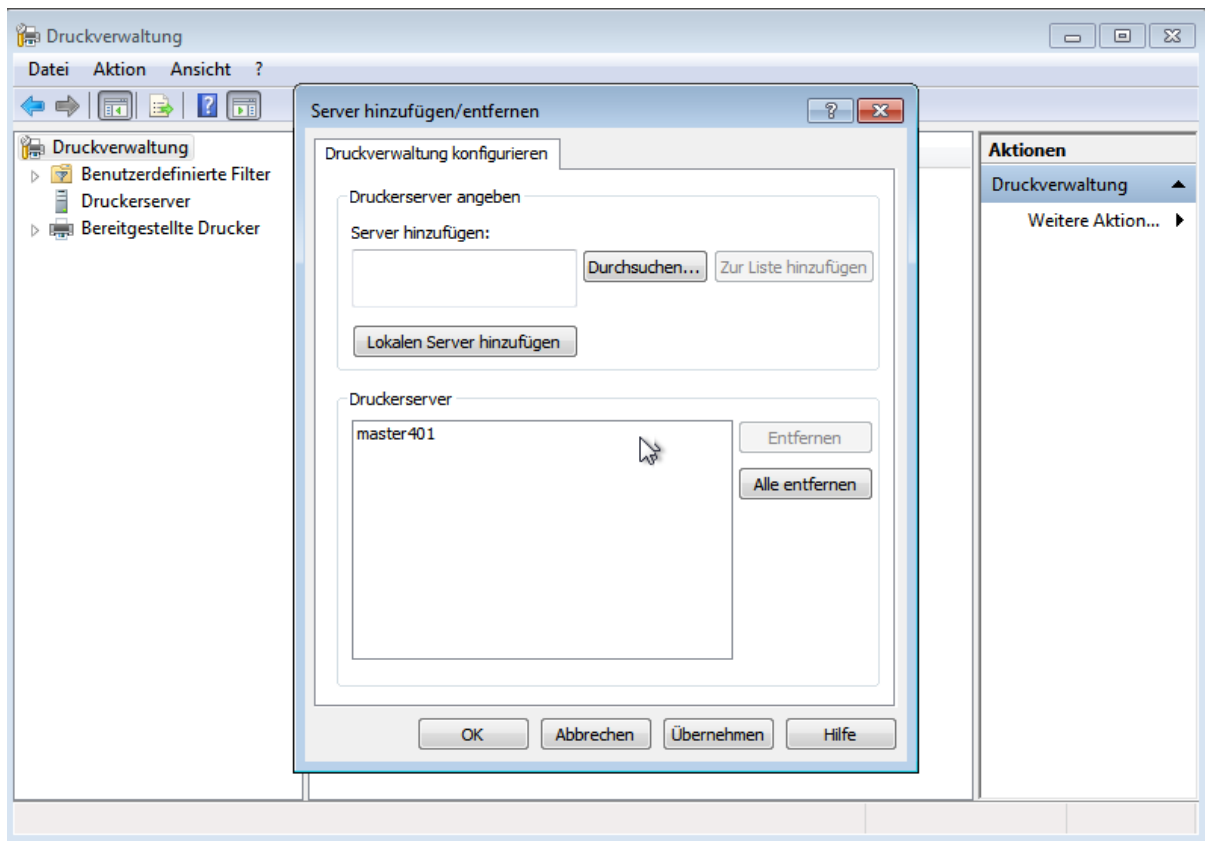


Abb. 13.2: Druckerserver hinzufügen

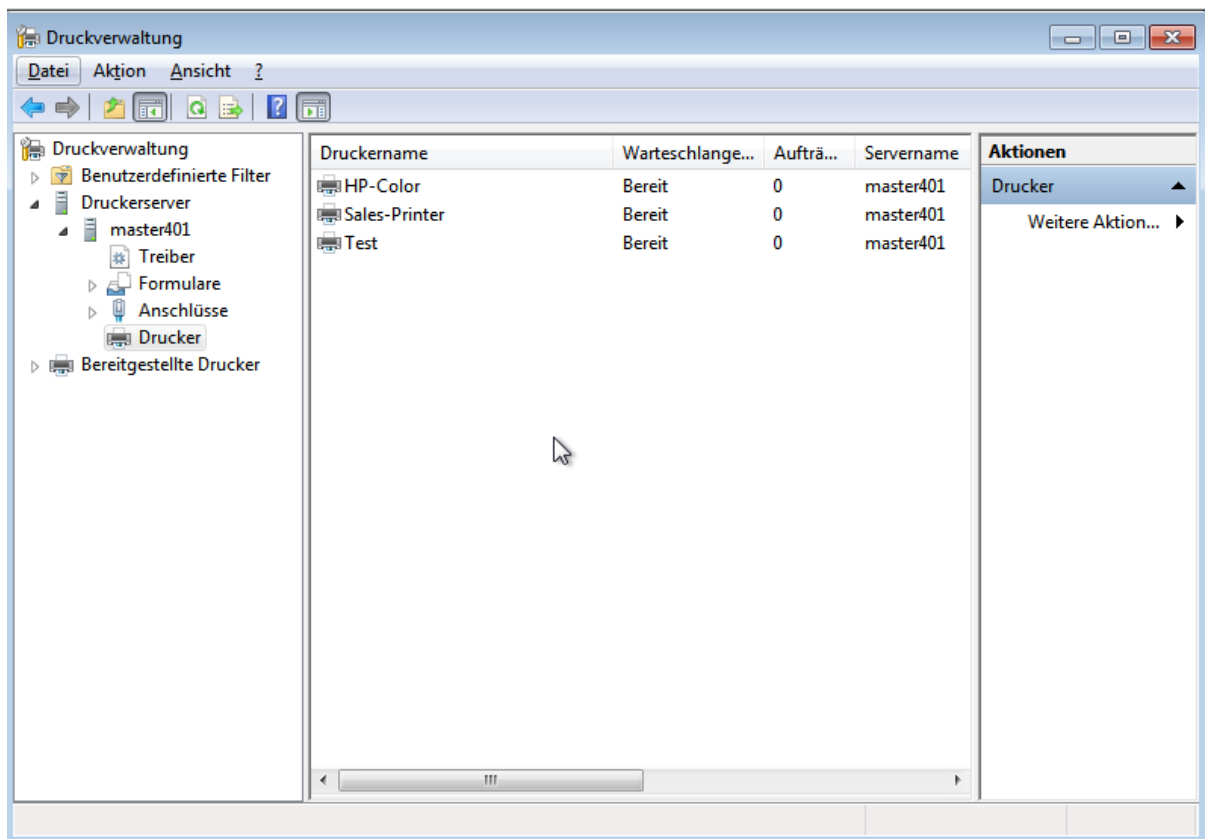


Abb. 13.3: Druckerliste

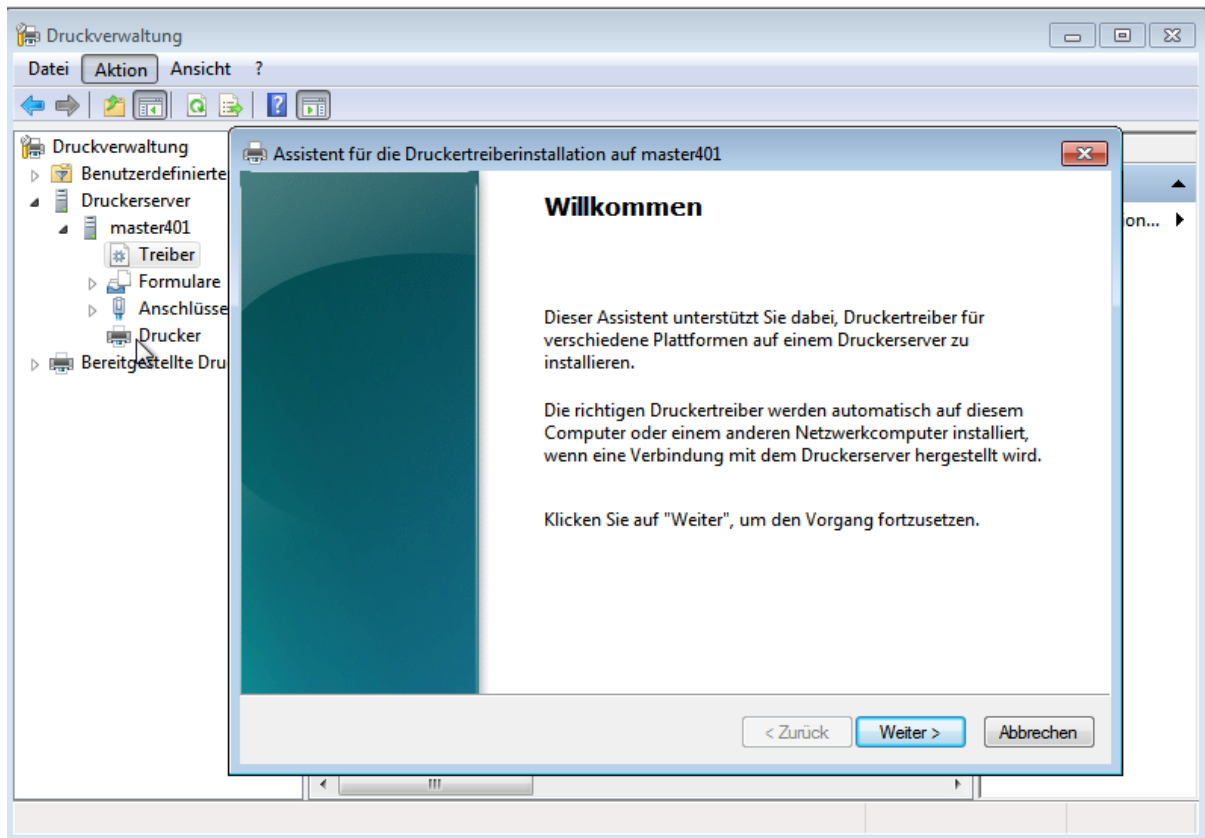


Abb. 13.4: Treiberinstallation

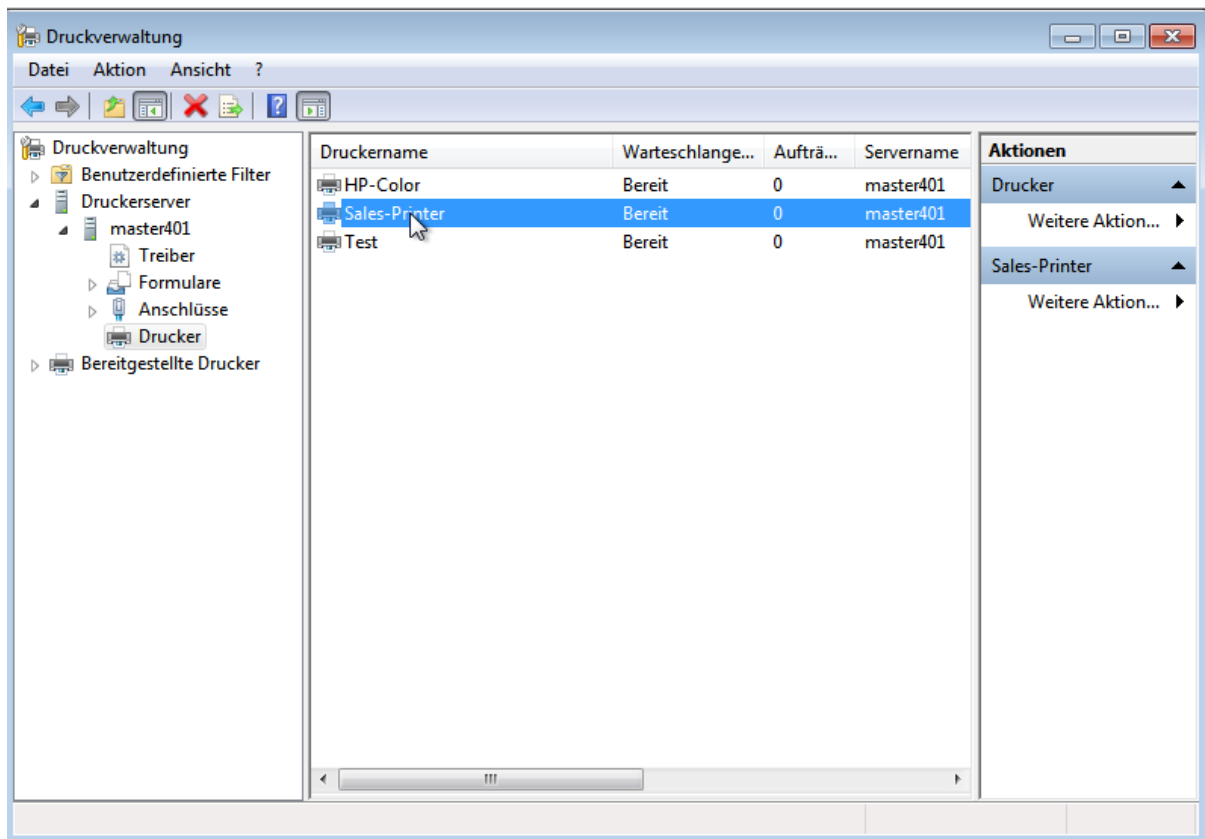


Abb. 13.5: Drucker auswählen

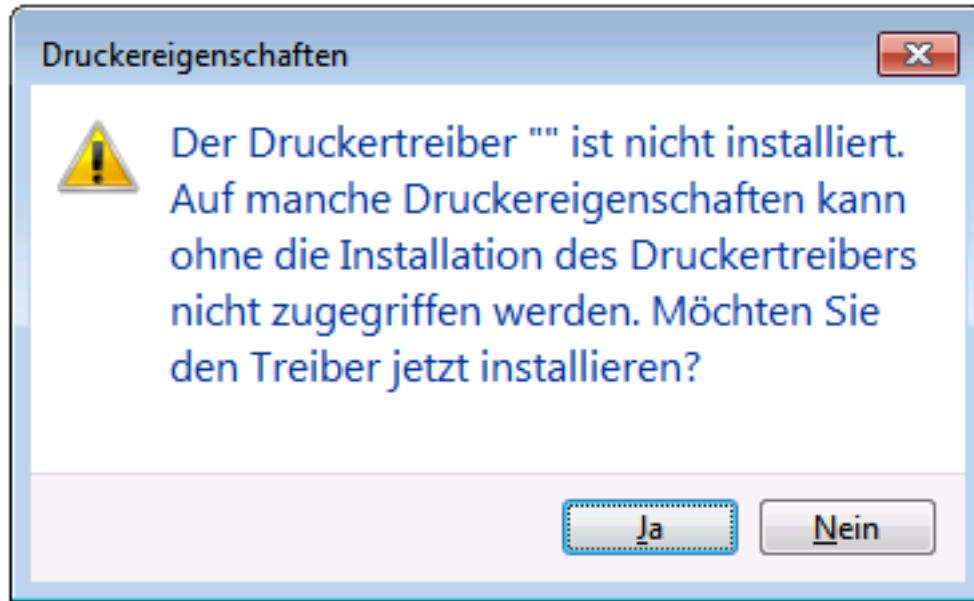


Abb. 13.6: Fehlermeldung beim ersten Zugriff

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 im UMC-Modul *Drucker* konfigurierte Feld *Windows-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. Typi-

scherweise 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.

13.8 Integration weiterer PPD-Dateien

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 UMC-Module 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.

Tab. 13.1: Reiter *Allgemein*

Attribut	Beschreibung
Name (*)	Der Name der Druckertreiberliste. Unter diesem Namen erscheint die Liste in der Auswahlliste <i>Drucker-Hersteller</i> auf der Karteikarte <i>Allgemein</i> der Druckerfreigaben (siehe <i>Konfiguration von Druckerfreigaben</i> (Seite 120)).
Treiber	Der Pfad zur PPD-Datei, relativ zu dem Verzeichnis <code>/usr/share/ppd/</code> . Soll beispielsweise die Datei <code>/usr/share/ppd/laserjet.ppd</code> verwendet werden, so ist hier <code>laserjet.ppd</code> einzutragen. Es können auch gzip -komprimierte Dateien (Dateiendung <code>.gz</code>) angegeben werden.
Beschreibung	Eine Beschreibung des Druckertreibers, unter der er in der Auswahlliste <i>Drucker-Modell</i> auf der Reiter <i>Allgemein</i> der Druckerfreigaben erscheint.

Univention Corporate Server (UCS) stellt Maildienste bereit, auf die Benutzer über Standard-Mail-Clients wie Thunderbird 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 *Installation* (Seite 128)). 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/pop3` (Seite 161) auf `no` deaktiviert werden. Das gleiche gilt für IMAP und die Univention Configuration Registry Variable `mail/dovecot/imap` (Seite 161). Auch die weitere Konfiguration der Mailserver erfolgt über Univention Configuration Registry (siehe *Konfiguration des Mailservers* (Seite 132)).

Die Verwaltung der Benutzerdaten des Mailservers (z.B. E-Mail-Adressen oder Verteiler) erfolgt über UMC-Module und ist in *Verwaltung der Mailserver-Daten* (Seite 128) 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 *Verteilung einer Installation auf mehrere Mailserver* (Seite 136)).

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 (*Spamerkennung und -filterung* (Seite 129)), für die Erkennung von Viren und anderer Malware wird **ClamAV** eingesetzt (*Viren- und Malwareerkennung* (Seite 130)).

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 *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 132)).

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, z.B. Kopano oder Open-Xchange. Weiterführende Informationen finden sich im Univention App Center (siehe *Univention App Center* (Seite 31)).

14.1 Installation

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 *Installation weiterer Software* (Seite 33). Mailserver können auf allen Server-Systemrollen installiert werden. Die Verwendung eines UCS Directory Nodes wird wegen 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 *Mailserver-Speicher auf NFS* (Seite 136).

14.2 Verwaltung der Mailserver-Daten

14.2.1 Verwaltung von Mail-Domänen

Der Inhalt dieses Abschnitts ist umgezogen nach *Verwaltung von Mail-Domänen*³⁴⁴ in *Nubus Handbuch 1.x* [6].

14.2.2 Zuordnung von E-Mail-Adressen zu Benutzern

Der Inhalt dieses Abschnitts ist umgezogen nach *Zuweisung von E-Mailadressen an Benutzer*³⁴⁵ in *Nubus Handbuch 1.x* [6].

14.2.3 Verwaltung von Mailinglisten

Der Inhalt dieses Abschnitts ist umgezogen nach *Verwaltung von Mailinglisten*³⁴⁶ in *Nubus Handbuch 1.x* [6].

14.2.4 Verwaltung von Mailgruppen

Der Inhalt dieses Abschnitts ist umgezogen nach *Verwaltung von Mailgruppen*³⁴⁷ in *Nubus Handbuch 1.x* [6].

14.2.5 Verwaltung von globalen IMAP-Ordern

Der Inhalt dieses Abschnitts ist umgezogen nach *Verwaltung von IMAP-Mail-Ordern*³⁴⁸ in *Nubus Handbuch 1.x* [6].

Globaler IMAP-Ordner - Reiter Allgemein

Der Inhalt dieses Abschnitts ist umgezogen nach *Reiter Allgemein - IMAP-Mail-Ordners*³⁴⁹ in *Nubus Handbuch 1.x* [6].

Globale IMAP-Ordner - Reiter Zugriffsrechte

Der Inhalt dieses Abschnitts ist umgezogen nach *Reiter Zugriffsrechte - IMAP-Mail-Ordner*³⁵⁰ in *Nubus Handbuch 1.x* [6].

³⁴⁴ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-management>

³⁴⁵ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-users>

³⁴⁶ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-mailinglists>

³⁴⁷ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-groups>

³⁴⁸ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-shared-folders>

³⁴⁹ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-shared-folders-general-tab>

³⁵⁰ <https://docs.software-univention.de/nubus-manual/latest/de/management/domain/mail.html#nubus-domain-mail-shared-folders-access-rights-tab>

14.2.6 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 UMC-Modulen verwendet werden, siehe *Bearbeiten von Objekten* (Seite 26).

Der Benutzer kann ab einer bestimmten erreichten Postfachgröße gewarnt werden und erhält dann eine Mail mit dem Hinweis, dass seine Speicherressourcen nahezu ausgeschöpft 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` (Seite 162) kann der Schwellwert konfiguriert werden, ab dem eine Warnmeldung ausgegeben werden soll, zum Beispiel: `mail/dovecot/quota/warning/text/PROZENT=TEXT`

PROZENT muss als Zahl zwischen 0 und 100 ohne Prozentzeichen angegeben werden.

TEXT ist 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` (Seite 162) 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` (Seite 162) 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.`

14.3 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 Spamversendern 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/bodysize-limit` (Seite 160) 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` (Seite 161) 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` (Seite 160) 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.

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` (Seite 161)) 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` (Seite 160) konfiguriert werden.

Die Spam-Filterung kann durch Setzen der Univention Configuration Registry Variable `mail/antivir/spam` (Seite 161) auf `no` deaktiviert werden. Bei Änderungen an Univention Configuration Registry-Variablen, die die Spamerkennung betreffen, muss der AMaViS-Dienst und Postfix neu gestartet werden.

14.4 Viren- und Malwareerkennung

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 Virens캔 kann mit der Univention Configuration Registry Variable `mail/antivir` (Seite 160) 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 Virensıcannern. Der freie Virensıcanner 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 Virensıcanner in AMaViS eingebunden werden. Nach Änderungen an der AMaViS- oder ClamAV-Konfiguration müssen Postfix und AMaViS neu gestartet werden.

14.5 Identifikation von Spam Quellen mit DNS basierten Blackhole Listen

Eine weitere Möglichkeit gegen Spam vorzugehen ist die Verwendung von *DNS-based Blackhole List* (DNSBL) oder *Real-time Blackhole Lists* (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 DNSBLs](#)³⁵¹.

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` (Seite 162) mit einem Schlüssel-Wert-Paar `SEQUENCE=RULE` gesetzt werden: `mail/postfix/smtpd/restrictions/recipient/SEQUENCE=RULE`.

Mit ihr können Empfangsbeschränkungen über die Postfix-Option `smtpd_recipient_restrictions` konfiguriert werden (siehe [Postfix Einstellung `smtpd_recipient_restrictions`](#)³⁵²). Die Sequenznummer dient der alphanumerisch Sortierung mehrerer Regeln, über die die Reihenfolge beeinflusst werden kann.

³⁵¹ http://www.postfix.org/postconf.5.html#reject_rbl_client

³⁵² http://www.postfix.org/postconf.5.html#smtpd_recipient_restrictions

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:

```
$ ucr set mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client ix.dnsbl.
↪manitu.net"
```

14.6 Integration von Fetchmail zum Abrufen von Mail von externen Postfächern

Im Regelfall nimmt der UCS-Maildienst Mails für die Benutzer der 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 der Installation stellen die Reiter *Erweiterte Einstellungen* ▶ *Mailabruf von externen Servern (Single)* und *Erweiterte Einstellungen* ▶ *Mailabruf von externen Servern (Multi)* zusätzliche Eingabefelder bereit. Verwenden Sie diese, um den Abruf von Mails von externen Servern zu konfigurieren.

Fetchmail liefert Mails zu den Posteingängen der jeweiligen Benutzer. Der Account des Benutzers muss dafür über eine primäre E-Mail-Adresse verfügen. Vor der Verwendung von *Multidrop-Konfigurationen* lesen Sie bitte **THE USE AND ABUSE OF MULTIDROP MAILBOXES**³⁵³.

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` (Seite 156) auf `false`).

Tab. 14.1: Reiter *Mailabruf von externen Servern (Single)*

Attribut	Beschreibung
Benutzername	Der Benutzername für die Verbindung zum Mailserver.
Passwort	Das Passwort für die Verbindung zum Mailserver.
Protokoll	Das Protokoll, welches Fetchmail zum Abrufen von Mails verwendet. Wählen Sie entweder <code>IMAP</code> oder <code>POP3</code> .
Externer Mailserver	Der Name des Mailservers, den Fetchmail verwendet, um Mails abzurufen.
SSL verwenden	Diese Option aktiviert einen verschlüsselten Abruf von Mails. Dies muss ebenfalls vom Mailserver unterstützt werden.
Mails auf dem externen Server nicht löschen	In der Grundeinstellung löscht Fetchmail die abgerufenen Mails nach deren Übertragung vom externen Server. Um die Mails auf dem externen Server zu behalten, diese Option aktivieren.

³⁵³ <https://www.fetchmail.info/fetchmail-man.html#the-use-and-abuse-of-multidrop-mailboxes>

Tab. 14.2: Reiter *Mailabruf von externen Servern (Multi)*

Attribut	Beschreibung
Benutzername	Der Benutzername für die Verbindung zum Mailserver.
Passwort	Das Passwort für die Verbindung zum Mailserver.
Protokoll	Das Protokoll, welches Fetchmail zum Abrufen von Mails verwendet. Wählen Sie entweder IMAP oder POP3.
Externer Mailserver	Der Name des Mailservers, den Fetchmail verwendet, um Mails abzurufen.
Lokale Domännennamen	Eine durch Leerzeichen getrennte Liste lokaler Domännennamen. Feld leer lassen, um alle lokalen Domänen zu verwenden.
Virtuelle <i>Qmail</i> Präfix	Fetchmail entfernt den angegebenen Präfix von der Mailadresse aus dem Header, welche mit der Option <i>Envelope-Header</i> angegeben ist. Wenn dieser Wert beispielsweise <code>example-prefix-</code> ist und Fetchmail eine Mail abrufen, in deren Header <code>example-prefix-info@remotedomain.com</code> vorkommt, leitet Fetchmail die Mail an <code>info@localdomain.com</code> weiter.
<i>Envelope-Header</i>	Ändert den Wert des Headers, in welchem Fetchmail eine Kopie der <i>Envelope-Adresse</i> erwartet. Fetchmail verwendet diesen zur Umleitung von E-Mails.
SSL verwenden	Diese Option aktiviert einen verschlüsselten Abruf von Mails. Dies muss ebenfalls vom Mailserver unterstützt werden.
Mails auf dem externen Server nicht löschen	In der Grundeinstellung löscht Fetchmail die abgerufenen Mails nach deren Übertragung vom externen Server. Um die Mails auf dem externen Server zu behalten, diese Option aktivieren.

14.7 Konfiguration des Mailservers

Dieser Abschnitt beschreibt die Konfiguration des Mailservers **Postfix** in UCS.

14.7.1 Konfiguration eines Relay-Hosts für den Mailversand

Standardmäßig stellt **Postfix** eine direkte SMTP-Verbindung zu dem für die Domain zuständigen Mailserver her, wenn es eine E-Mail an eine nicht lokale Adresse sendet.

Alternativ dazu kann **Postfix** einen Mail-Relay Server verwenden. Dabei handelt es sich um einen Server, der E-Mails empfängt und deren Transport übernimmt. Administratoren können diese Art von Mail-Relay Servern verwenden, z. B. solche, die von der Firmenzentrale oder dem Internet-Provider bereitgestellt werden.

Um einen Relayhost einzurichten, geben Sie ihn als vollqualifizierten Domännennamen (FQDN) in der Univention Configuration Registry Variable `mail/relayhost` (Seite 163) an.

Beispiele

- `ucr set mail/relayhost="mx01.example.com"`

Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port 25.

- `ucr set mail/relayhost="mx01.example.com:587"`

Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port 587.

Postfix ermittelt die tatsächliche Zieladresse des Relay Mailservers durch Abfrage des MX/SRV Eintrags im DNS. Um die MX Abfrage zu deaktivieren, verwenden Sie das Format `[FQDN-Relay-Host]`, wie in den folgenden Beispielen zu sehen:

- `ucr set mail/relayhost="[mx01.example.com]"`

Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port 25.

- `ucr set mail/relayhost="[mx01.example.com]:587"`

Der Mailserver liefert ausgehende Mail an den Mailserver `mx01.example.com` auf Port 587.

Wenn für das Senden eine Authentifizierung auf dem Relayhost erforderlich ist, setzen Sie die Univention Configuration Registry Variable `mail/relayauth` (Seite 163) auf `yes` und bearbeiten Sie die Datei `/etc/postfix/smtplib_auth`. Geben Sie in dieser Datei den FQDN des Relayhost, den Benutzernamen und das Passwort in einer Zeile in folgendem Format ein: `FQDN Relayhost Benutzername:Passwort`. Der Teil für `FQDN Relayhost` muss genau wie der Wert von `mail/relayhost` (Seite 163) aussehen.

Beispiele

- `mx01.example.com:587 outgoing-username@example.com:verySecretPassword`
- `[mx01.example.com]:587 outgoing-username@example.com:verySecretPassword` mit ausgeschalteter MX Abfrage

Um die Änderungen in **Postfix** zu übernehmen, führen Sie die folgenden Befehle aus:

1. Aktualisieren Sie die Authentifizierungszuordnung:

```
$ postmap /etc/postfix/smtplib_auth
```

2. Wenn Sie `mail/relayauth` (Seite 163) geändert haben, müssen Sie die Datei für die TLS-Richtlinien aktualisieren:

```
$ postmap /etc/postfix/tls_policy
```

3. Wenn Sie `mail/relayhost` (Seite 163) geändert haben, müssen Sie dem Mailserver sagen, dass er die Konfiguration neu laden soll:

```
$ service postfix reload
```

Bemerkung

Um eine verschlüsselte Verbindung bei Verwendung eines Relay-Hosts zu gewährleisten, müssen Sie die **Postfix**-Konfigurationsoption `smtplib_tls_security_level` auf `encrypt` setzen.

Univention Corporate Server setzt diese Option automatisch, wenn die Univention Configuration Registry Variablen `mail/relayhost` (Seite 163) und `mail/relayauth` (Seite 163) den Wert `yes` haben und wenn `mail/postfix/tls/client/level` (Seite 163) nicht den Wert `none` hat.

Siehe auch

postconf(5)³⁵⁴ - Manual Seite für `postconf` - Postfix Konfigurationsparameter
für eine Referenz der Konfigurationswerte `relayhost`³⁵⁵, und `smtplib_sasl_password_maps`³⁵⁶.

14.7.2 Konfiguration der maximalen E-Mailgröße

Mit der Univention Configuration Registry Variable `mail/messagesizelimit` (Seite 162) 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 konfiguriert, so wird die Begrenzung aufgehoben. Es ist zu beachten, dass Emailanhänge durch die `base64`-Kodierung um ca. ein Drittel vergrößert werden.

³⁵⁴ <https://manpages.debian.org/bookworm/postfix/postconf.5.en.html>

³⁵⁵ [https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#relayhost_\(default:_empty\)](https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#relayhost_(default:_empty))

³⁵⁶ [https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#smtplib_sasl_password_maps_\(default:_empty\)](https://manpages.debian.org/bookworm/postfix/postconf.5.en.html#smtplib_sasl_password_maps_(default:_empty))

14.7.3 Konfiguration einer Blindkopie zur Anbindung von E-Mail-Archivierungslösungen

Wird die Univention Configuration Registry Variable `mail/archivefolder` (Seite 161) 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.

14.7.4 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` (Seite 163) 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.

14.7.5 Konfiguration der SMTP Ports

Auf einem Univention Corporate Server Mailserver ist Postfix so konfiguriert, dass es auf Verbindungen an drei Ports lauscht:

Port 25 - SMTP

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` (Seite 162) auf `yes` gesetzt werden.

Port 465 - SMTPS

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

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.

14.7.6 Konfiguration zusätzlicher Prüfungen

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` (Seite 162) auf den Wert `yes` kann `postscreen` aktiviert werden.

Über diverse UCR-Variablen mit dem Präfix `mail/postfix/postscreen/` (Seite 162) können weitere Einstellungen vorgenommen werden. Eine Liste der UCR-Variablen nebst Beschreibungen können z.B. auf der Kommandozeile über folgenden Befehl abgerufen werden:

```
$ ucr search --verbose mail/postfix/postscreen/
```

Bemerkung

Nach jeder Änderung einer UCR-Variable für `postscreen` sollte die Konfiguration von Postfix und `postscreen` neu geladen werden, was über den Befehl `systemctl reload postfix` ausgelöst werden kann.

14.7.7 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:

```
$ systemctl reload postfix
```

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`.

Bemerkung

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.

14.7.8 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 oder angepasst werden:

```
virtual_alias_expansion_limit = 5000
```

Danach muss Postfix neugestartet werden:

```
$ systemctl restart postfix
```

14.7.9 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` (Seite 161) 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` (Seite 161) 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, wenn eine der obigen Aktionen durchgeführt wird.

Aus der Kombination der beiden Variablen ergeben sich folgende vier Fälle, wenn E-Mail-Adressen geändert werden:

Tab. 14.3: Umbenennung von E-Mail-Adressen

mail/dovecot/mailbox/...	Bedeutung
<code>rename=yes</code> und <code>delete=no</code> (Standard)	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
<code>rename=yes</code> und <code>delete=yes</code>	Die bestehende Mailbox wird umbenannt. E-Mails bleiben erhalten und sind unter dem neuen Namen erreichbar.
<code>rename=no</code> und <code>delete=no</code>	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.
<code>rename=no</code> und <code>delete=yes</code>	Eine neue, leere Mailbox wird erzeugt. Die alte Mailbox wird inklusive aller enthaltenen Mails von der Festplatte gelöscht.

14.7.10 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 abgelegt 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 *Verwaltung von globalen IMAP-Ordnern* (Seite 128)) 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.

14.7.11 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` (Seite 162)=`yes`
- `mail/dovecot/process/dotlock_use_excl` (Seite 162)=`yes`
- `mail/dovecot/process/mail_fsyc` (Seite 162)=`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` (Seite 161)=`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` (Seite 162)=`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` (Seite 161)=`dotlock`. Dies verringert die Performance, aber behebt die meisten Locking-bezogenen Probleme.
- Dovecot kann mit `mail/dovecot/process/mail_nfs_storage` (Seite 162)=`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` (Seite 162)=`yes`.

Siehe auch

Mail Location Settings³⁵⁷ in der Dovecot Dokumentation

für weitere Informationen über Mailbox Orte.

Shared mailboxes³⁵⁸ in der Dovecot Dokumentation

für weitere Informationen über das Teilen von Mailboxen.

NFS³⁵⁹ in der Dovecot Dokumentation

für weitere Informationen über die Verwendung von Dovecot mit NFS.

14.7.12 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` (Seite 161)/`*` angepasst werden. Der Vorgang ist auf Grund des komplexen Zusammenspiels dieser Variablen nur halb automatisch. Die Bedeutung aller Variablen kann in [Dovecot Dokumentation: Service configuration](#)³⁶⁰ nachgelesen werden.

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.

³⁵⁷ https://doc.dovecot.org/2.3/configuration_manual/mail_location/

³⁵⁸ https://doc.dovecot.org/2.3/configuration_manual/shared_mailboxes/

³⁵⁹ https://doc.dovecot.org/2.3/configuration_manual/nfs/

³⁶⁰ https://doc.dovecot.org/2.3/configuration_manual/service_configuration/

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 kontrollierte `ulimit` (die erlaubte Anzahl gleichzeitig geöffneter Dateien/Verbindungen pro Prozess) wird nur bei einem Neustart des Dovecot-Dienstes verändert, daher:

```
$ systemctl restart dovecot
```

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 zehntausenden Benutzern kann Dovecot im *High-performance mode* betrieben werden. Der Performance-Leitfaden beschreibt, wie dieser konfiguriert werden kann, siehe *UCS performance guide* [17].

14.8 Konfiguration von Mail-Clients für den Mailserver

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.

Konto einrichten

Ihr Name: Ihr Name, wie er anderen Personen gezeigt wird

E-Mail-Adresse:

Passwort:

Passwort speichern

Folgende Einstellungen wurden durch Testen des genannten Servers gefunden

	Server-Adresse	Port	SSL	Authentifizierung
Posteingang-Server: <input type="text" value="IMAP"/>	<input type="text" value="10.200.3.18"/>	<input type="text" value="143"/>	<input type="text" value="STARTTLS"/>	<input type="text" value="Passwort, normal"/>
Postausgang-Server: <input type="text" value="SMTP"/>	<input type="text" value="10.200.3.18"/>	<input type="text" value="587"/>	<input type="text" value="STARTTLS"/>	<input type="text" value="Passwort, normal"/>

Benutzername: Posteingang-Server: Postausgang-Server:

Abb. 14.1: Einrichtung von Mozilla Thunderbird

14.9 OX Connector

OX Connector ist eine App im Univention App Center. Sie synchronisiert ausgewählte Benutzer und Gruppen zu **OX App Suite** und entfernten Installation wie zum Beispiel ein **OX App Suite** bei einem Hosting Anbieter. Seit **OX Connector** Version 2.1.2 und **OX App Suite** Version 7.10.6-ucs4, integriert der **OX Connector** mit **OX App Suite** aus dem Univention App Center, um Nutzer- und Gruppenkonten zu **OX App Suite** zu synchronisieren.

Warnung

OX App Suite Versionen älter als 7.10.6-ucs4 beinhalten ihre eigene Synchronisation. **OX Connector** synchronisiert sich nicht mit diesen Versionen und darf daher nicht mit der separaten App **OX App Suite** aus dem App Center verwendet werden.

Siehe auch

OX Connector App Dokumentation

Weitere Informationen über den **OX Connector** finden Sie in [Integration of OX Connector and OX App Suite app](#)³⁶¹ in der entsprechenden Dokumentation unter *Univention OX Connector app documentation* [18], verfügbar nur in Englisch.

³⁶¹ <https://docs.software-univention.de/ox-connector-app/latest/limitations.html#limit-ox-app-suite-app>

UCS bietet zwei unterschiedliche Lösungen für das Monitoring der Infrastruktur.

Das UCS Dashboard hilft einerseits den Administratoren, schnell den Zustand von Domänen und einzelnen Servern zu erfassen. Zum anderen ist es unter UCS 4.4 mit Nagios möglich, Rechner und Dienste im Hintergrund zu überprüfen und proaktiv eine Benachrichtigung auszulösen, wenn eine Warnstufe erreicht wird. Ab UCS 5.0-2 können Prometheus und Prometheus Alertmanager zur Überwachung eingesetzt. Mit UCS 5.0 wurde die Unterstützung für die Nagios Serverkomponente eingestellt.

15.1 UCS Dashboard

Der Inhalt dieses Abschnitts ist umgezogen nach [UCS Dashboard](#)³⁶² in *Univention Corporate Server - Operation Manual* [1].

15.1.1 Installation

Der Inhalt dieses Abschnitts ist umgezogen nach [Installation](#)³⁶³ in *Univention Corporate Server - Operation Manual* [1].

15.1.2 Nutzung

Der Inhalt dieses Abschnitts ist umgezogen nach [Zugriff auf das UCS Dashboard](#)³⁶⁴ in *Univention Corporate Server - Operation Manual* [1].

Domain Dashboard

Der Inhalt dieses Abschnitts ist umgezogen nach [Domain Dashboard](#)³⁶⁵ in *Univention Corporate Server - Operation Manual* [1].

³⁶² <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard>

³⁶³ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-installation>

³⁶⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-access>

³⁶⁵ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-domain>

Server Dashboard

Der Inhalt dieses Abschnitts ist umgezogen nach [Server Dashboard](#)³⁶⁶ in *Univention Corporate Server - Operation Manual* [1].

Alert Dashboard

Der Inhalt dieses Abschnitts ist umgezogen nach [Alert Dashboard](#)³⁶⁷ in *Univention Corporate Server - Operation Manual* [1].

Eigene Dashboards

Der Inhalt dieses Abschnitts ist umgezogen nach [Benutzerdefinierte Dashboards](#)³⁶⁸ in *Univention Corporate Server - Operation Manual* [1].

15.2 Monitoring

Added in version 5.0-2: UCS 5.0-2 unterstützt die Überwachung von Alarmen durch *Prometheus*-Metriken.

Mit *Prometheus*, *Prometheus Node Exporter*, und *Prometheus Alertmanager* können Administratoren die korrekte Funktion von komplexen IT-Strukturen aus Netzwerken, Rechnern und Diensten kontinuierlich und automatisch überprüfen.

Der Prometheus Node Exporter exportiert eine umfassende Sammlung von Metriken in die Prometheus Datenbank. Neben der Abfrage von Systemindikatoren wie CPU, Speichernutzung und freien Speicherplatz, testen sie die Verfügbarkeit und den Betrieb von verschiedenen Diensten wie SSH, SMTP und HTTP. Betriebstests führen im Allgemeinen Programmschritte wie die Zustellung einer Test-E-Mail oder die Auflösung eines DNS-Eintrags durch. Der Prometheus Node Exporter bietet UCS spezifische Alarme zusätzlich zu den bereits enthaltenen Startmetriken, zum Beispiel einen Alarm für die Listener/Notifier-Replikation.

Wenn sich der Betriebszustand ändert, informiert die Überwachung einen vorher festgelegten Ansprechpartner über die mögliche Störung. Zusätzlich zur reaktiven Benachrichtigung im Fehlerfall können Administratoren den aktuellen Status jederzeit kontinuierlich in der Web-Oberfläche *Grafana UCS Dashboard*, das die Statusinformationen kompakt anzeigt, überprüfen.

Siehe UCS Dashboard *Installation* (Seite 141) für eine Übersicht über alle beteiligten Komponenten.

Administratoren definieren die Alarmkonfiguration in Univention Management Console. Ein Listener Modul generiert automatisch die Konfigurationsdateien aus den Informationen im LDAP-Verzeichnis.

15.2.1 Installation

Zur Installation der UCS Dashboard Komponenten siehe *Installation* (Seite 141).

Zusätzlich zu den Komponenten des UCS Dashboards müssen Sie die App *Prometheus Alertmanager* und den *univention-monitoring-client* installieren.

Für jedes UCS-System, das der Administrator auf dem Dashboard anzeigen möchte, muss er die App *UCS Dashboard Client* installieren. Das Paket `univention-monitoring-client` hängt von *UCS Dashboard Client* ab und wird standardmäßig auf jedem UCS-System installiert, um die Alarmfunktionalität bereitzustellen.

Prometheus Alertmanager

Die *Prometheus Alertmanager* App versendet Benachrichtigungen über ausgelöste Alarme, zum Beispiel per E-Mail. Der Alertmanager benötigt einige Einstellungen, um korrekt zu funktionieren.

Die Einstellungen umfassen die Empfänger der E-Mail-Benachrichtigungen. Außerdem benötigen die App-Einstellungen einen Wert für einen SMTP-Server, um E-Mail-Benachrichtigungen zu senden. Der Alertmanager unterstützt die SMTP-Authentifizierungsmethoden `PLAIN`, `LOGIN` und `CRAM-MD5` sowie die Kommunikation via TLS. Keine Authentifizierung wird verwendet, wenn Sie alle Felder der App-Einstellungen bezüglich Authentifizierung leer lassen.

³⁶⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-server>

³⁶⁷ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-alert>

³⁶⁸ <https://docs.software-univention.de/ucs-operation/5.2/de/monitoring/dashboard.html#infrastructure-monitoring-ucs-dashboard-custom>

App Center ÄNDERUNGEN ANWENDEN KONFIGURATION ABBRECHEN

Konfiguriere Prometheus Alertmanager

Die App läuft momentan.

APP STOPPEN

Autostart
Automatisch gestartet

Administration

Komma separierte Liste von E-Mail Adressen, die Notifikationen zu Alarmen des Monitoring Systems bekommen sollen.

Benachrichtigung senden, wenn ein Alarm behoben ist.

SMTP-Host und Port, der für den Versand der E-Mail-Benachrichtigungen verwendet werden soll (z.B. localhost:25).

Globale E-Mail-Absenderadresse. Wird verwendet, wenn Empfänger-von nicht gesetzt ist.

TLS bei der Kommunikation mit dem SMTP-Host verwenden.

Benutzername für die SMTP-Authentifizierungsmethoden CRAM-MD5, LOGIN und PLAIN. Keine Authentifizierung, wenn leer gelassen.

Passwort für die SMTP-Authentifizierungsmethoden LOGIN und PLAIN. Passwort für die SMTP-Authentifizierungsmethoden LOGIN und PLAIN. (Wiederholung)

Identität für die SMTP-Authentifizierungsmethoden

`univention-monitoring-client`

Das Paket `univention-monitoring-client` stellt Standard Alarm Plugins zur Überprüfung des Systemzustands bereit.

Administratoren können mit den folgenden Paketen Plugins installieren, die über die Standard-Plugins hinausgehen, die mit dem `univention-monitoring-client` Paket bereitgestellt werden.

- `univention-monitoring-raid`: Überwachung des Software-RAID-Status
- `univention-monitoring-smart`: Prüfung des S.M.A.R.T.-Status von Festplatten
- `univention-monitoring-opsi`: Prüfung der Software OPSI
- `univention-monitoring-cups`: Prüfung des Druckerdienstes CUPS
- `univention-monitoring-squid`: Prüfung des Squid proxy Servers
- `univention-monitoring-samba`: Prüfung des Samba 4 Dienstes
- `univention-monitoring-s4-connector`: Prüfung des S4-Connector
- `univention-monitoring-ad-connector`: Prüfung des AD Connectors

Einige Dienste richten ihr jeweiliges Paket zur Überwachung bereits bei der Installation ein. Wenn Administratoren zum Beispiel den `UCS AD Connector` einrichten, enthält es automatisch das Plugin für die Überwachung.

15.2.2 Vorkonfigurierte Überwachungstests

Die Installation richtet automatisch grundlegende Überwachungstests für UCS Systeme ein. Alle Alarme haben die Bezeichnung (*Label*) *severity* mit dem Wert `critical` oder `warning`.

Tab. 15.1: Vorkonfigurierte Alarme

Alarm	Beschreibung
UNIVENTION_DISK_ROOT und UNIVENTION_DISK_ROOT_WARNING	Überwacht den Füllstand der /-Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% oder 10% wird der Fehlerzustand gesetzt.
UNIVENTION_DNS	Testet die Funktion des lokalen DNS-Servers und die Erreichbarkeit des öffentlichen DNS-Servers durch Abfrage des Rechnernamens <code>www.univention.de</code> . Wenn kein DNS-Forwarder für die UCS-Domäne definiert ist, schlägt diese Anfrage fehl. In diesem Fall kann <code>www.univention.de</code> durch den FQDN des Primary Directory Node ersetzt werden, zum Beispiel in der <code>monitoring/dns/lookup-domain</code> um die Funktion der Namensauflösung zu testen.
UNIVENTION_LDAP_AUTH	Überwacht den auf Directory Nodes laufenden LDAP-Server.
UNIVENTION_LOAD und UNIVENTION_LOAD_WARNING	Überwacht die Systemlast.
UNIVENTION_NTP und UNIVENTION_NTP_WARNING	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 oder 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTD	Testet, ob der SMTP-Server erreichbar ist. Der Alarm wird ausgelöst, wenn er nicht erreichbar ist.
UNIVENTION_SSL und UNIVENTION_SSL_WARNING	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Primary Directory Node und Backup Directory Nodes geeignet.
UNIVENTION_SWAP und UNIVENTION_SWAP_WARNING	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% oder 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION und UNIVENTION_REPLICATION_WARNING	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer <code>failed.ldif</code> -Datei sowie den Stillstand der Replikation und warnt vor zu großen Differenzen der Transaktions-IDs.
UNIVENTION_NSCD und UNIVENTION_NSCD2	Testet die Verfügbarkeit des Name Server Cache Dienstes (NSCD). Läuft kein NSCD-Prozess wird ein <i>critical</i> Alarm ausgelöst, läuft mehr als ein Prozess, wird ein <i>warning</i> Alarm ausgelöst.
UNIVENTION_WINBIND	Testet die Verfügbarkeit des Winbind-Dienstes. Läuft kein Prozess, wird ein <i>critical</i> Alarm ausgelöst.
UNIVENTION_SMBD	Testet die Verfügbarkeit des Samba-Dienstes. Läuft kein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_NMBD	Testet die Verfügbarkeit des NMBD-Dienstes, der in Samba für den NetBIOS-Dienst zuständig ist. Läuft kein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_JOINSTATUS und UNIVENTION_JOINSTATUS_WARNING	Prüft den Join-Status eines Systems. Ist ein System noch nicht Mitglied der Domäne, wird ein <i>critical</i> Alarm ausgelöst, sind nicht-aufgerufene Join-Skripte vorhanden, wird ein <i>warning</i> Alarm ausgelöst.
UNIVENTION_KPASSWDD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Primary/Backup Directory Node). Läuft weniger oder mehr als ein Prozess, wird ein Alarm ausgelöst.
UNIVENTION_PACKAGE_STATUS	Überwacht den Status der installierten Debian-Pakete. Wenn ein Paket den Status <i>half-installed</i> hat, wird ein Alarm ausgelöst.
UNIVENTION_SLAPD_MDB_MAXSIZE und UNIVENTION_SLAPD_MDB_MAXSIZE_WARNING	Überwacht den Anteil der freien Speicherseiten des <i>mdb</i> Backends von SLAPD für mehrere Verzeichnisse.
UNIVENTION_LISTENER_MDB_MAXSIZE und UNIVENTION_LISTENER_MDB_MAXSIZE_WARNING	Überwacht den Anteil der freien Speicherseiten des <i>mdb</i> Backends von SLAPD für mehrere Verzeichnisse.

Die folgenden Alarme sind nur verfügbar, sobald zusätzliche Pakete installiert wurden (siehe *Monitoring installation* (Seite 142))

Tab. 15.2: Zusätzliche Alarme

Alarm	Beschreibung
UNIVENTION_OPSI	Überwacht den OPSI-Daemon. Läuft kein OPSI-Prozess oder die OPSI-Weboberfläche ist nicht erreichbar, wird ein Alarm zurückgegeben.
UNIVENTION_SMART_SDA	Prüft den S.M.A.R.T.-Status der Festplatte <code>/dev/sda</code> . Für die Festplatten <code>sdb</code> , <code>sdc</code> und <code>sdd</code> existieren entsprechende Alarme.
UNIVENTION_RAID und UNIVENTION_RAID_WARNING	Prüft den Status des Software-RAIDs über <code>/proc/mdadm</code> und löst einen <i>critical</i> Alarm aus, sofern eine Festplatte des RAID-Verbunds ausgefallen ist, oder einen <i>warning</i> Alarm, wenn der Recovery-Vorgang läuft.
UNIVENTION_ADCONNECTOR und UNIVENTION_ADCONNECTOR_WARNING	Prüft den Status des Active Directory Connectors: <ul style="list-style-type: none"> • Läuft kein Connector-Prozess, wird ein Alarm zurückgegeben. • Existiert mehr als ein Prozess pro Connector-Instanz, wird ein <i>warning</i> Alarm ausgelöst. • Treten Rejects auf, wird ein <i>warning</i> Alarm ausgelöst. • Kann der AD-Server nicht erreicht werden, wird ein Alarm zurückgegeben. <p>Das Plugin kann auch in Multi-Connector-Instanzen verwendet werden.</p>
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft der <code>cupsd</code> -Prozess nicht oder ist die Weboberfläche nicht erreichbar, wird ein <i>critical</i> Alarm ausgelöst.
UNIVENTION_SQUID	Überwacht den Proxy Squid. Läuft kein Squid-Prozess oder der Squid-Proxy ist nicht erreichbar, wird ein Alarm zurückgegeben.
UNIVENTION_RAID und UNIVENTION_RAID_WARNING	Überwacht den Status der vorhandenen RAID Geräte. Der <i>warning</i> Alarm wird im Falle folgender RAID Status ausgelöst: <ul style="list-style-type: none"> • Rebuilding • Reconstruct • Replaced Drive • Expanding • Warning • Verify <p>Der <i>critical</i> Alarm wird für folgende RAID Status ausgelöst:</p> <ul style="list-style-type: none"> • Degraded • Dead • Failed • Error • Missing
UNIVENTION_S4CONNECTOR und UNIVENTION_S4CONNECTOR_WARNING	Überwacht den Status des Samba 4 Servers. Ein <i>warning</i> Alarm wird ausgelöst, wenn der Samba 4 erreichbar ist, aber keine Ablehnungen (<i>rejects</i>) vorhanden sind. Ein <i>critical</i> Alarm wird ausgelöst, wenn der Server nicht erreichbar ist.
UNIVENTION_SAMBA_REPLICATION	Überwacht den Status der Samba-Replikation. Der Alarm wird ausgelöst, wenn ein Fehler der Replikation vorliegt.

15.2.3 Konfiguration

Univention Management Console bietet die folgenden Einstellungen:

- Administratoren müssen den Alarm konfigurieren (siehe *Monitoring installation* (Seite 142)) und festlegen, auf welchen Computern der Domäne ein Alarm aktiv sein soll (siehe *Zuweisung von Alarmen an Computer* (Seite 148)).
- Um die Kontaktperson zu konfigurieren, die der *Alertmanager* im Falle von Fehlern und Alarmen benachrichtigt, muss die entsprechende Einstellung in der **Prometheus Alertmanager** App gesetzt werden (siehe *Monitoring installation* (Seite 142)).

- Administratoren können Alarme für eine bestimmte Zeit stumm schalten. Siehe die [Prometheus Alertmanager Dokumentation](#)³⁶⁹. Benutzen Sie das *Prometheus Alertmanager* Webinterface für diese Einstellungen.

Die Grundeinstellungen definieren bereits eine Vielzahl von Tests für jeden Computer, z.B. eine Grundkonfiguration der Alarme, ohne dass weitere Anpassungen vorgenommen werden müssen.

Konfiguration der Alarme

Ein Alert definiert die Überwachung eines Dienstes oder eines Zustandes, zum Beispiel freier Festplattenspeicher. Administratoren können eine beliebige Anzahl von Computern einem solchen Alert-Objekt zuordnen.

Administratoren verwalten Alarme im UMC-Modul *Monitoring* mit dem Objekttyp *Alert*, siehe *Modul Rechnerverwaltung - Reiter Dienste* (Seite 48). Prometheus hat keine LDAP-Schnittstelle für die Überwachungskonfiguration. Stattdessen generiert ein Listener-Modul die Konfigurationsdateien, wenn Administratoren Alarme hinzufügen, bearbeiten oder entfernen.

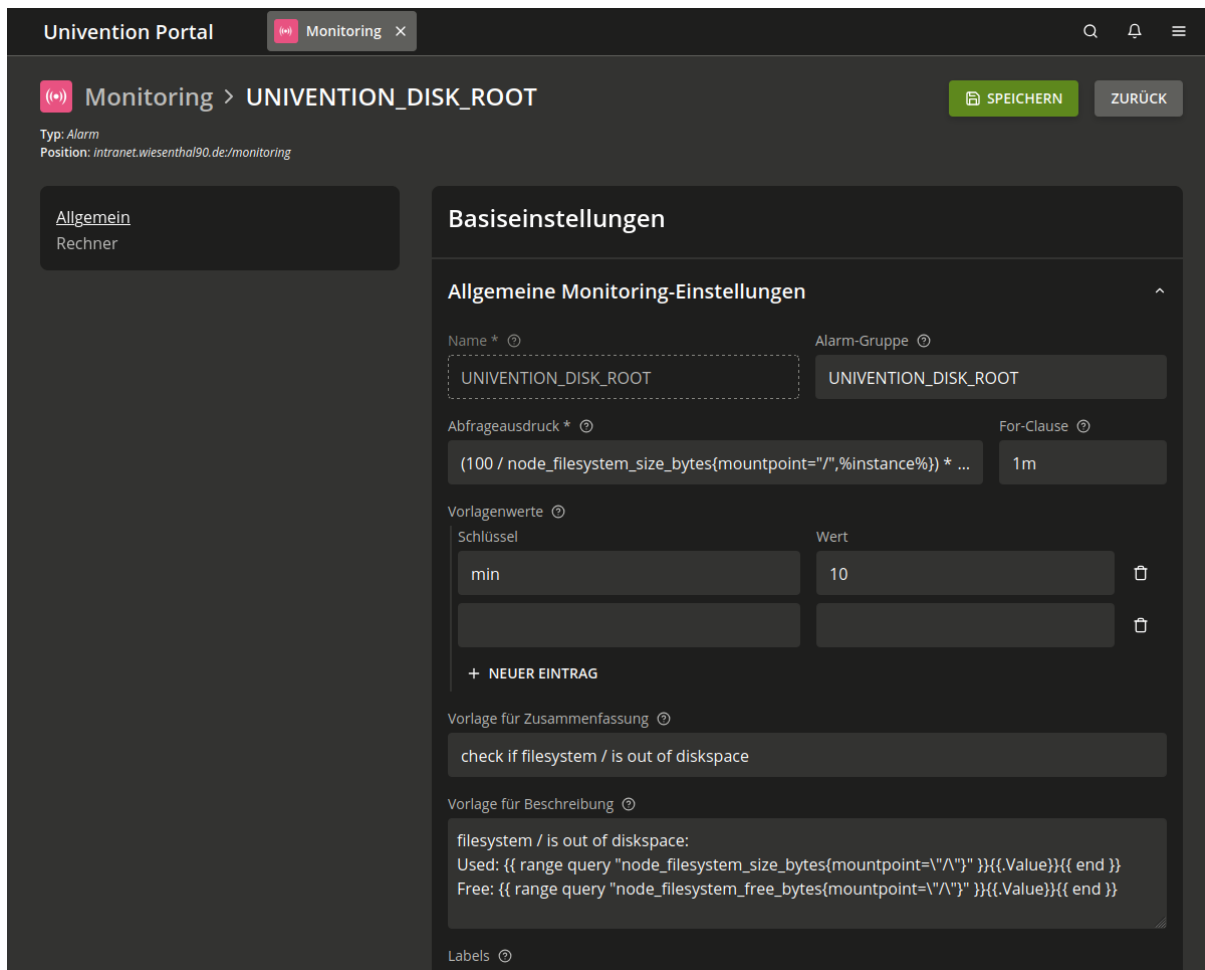


Abb. 15.1: Konfiguration eines Alarms

³⁶⁹ <https://prometheus.io/docs/alerting/latest/alertmanager/#silences>

Tab. 15.3: Reiter *Allgemein*

Attribut	Beschreibung
Name	Eine eindeutige Bezeichnung für den Alarm.
Alarm-Gruppe	Legt die Gruppe fest, die den Alarm enthält. Mehrere Alarme können derselben Gruppe angehören.
Abfrageausdruck	Prometheus Abfrage, die den Alarm auslöst. Der Alarm wird ausgelöst, wenn die angegebene Abfrage einen nicht leeren Vektor zurück gibt. Für Details zur Syntax, siehe die Prometheus documentation ³⁷⁰ .
For-Clause	Definiert die Zeit, in der das Ergebnis des Abfrageausdrucks nicht leer sein muss, bis der Alarm ausgelöst wird.
Vorlage für Zusammenfassung	Der Titel des Alarms, der im Dashboard und in den E-Mail-Benachrichtigungen für Alarme angezeigt wird.
Vorlage für Beschreibung	Die Beschreibung des Alarms, die im Dashboard und in den E-Mail-Benachrichtigungen für Alarme angezeigt wird.
Labels	Prometheus fügt den Alarmen Bezeichnungen (<i>Labels</i>) hinzu. Bezeichnungen helfen bei der Abfrage von Alarmen. Zum Beispiel: <i>severity</i> mit dem Wert <i>critical</i> oder <i>warning</i> .
Vorlagenwerte	Abfrageausdrücke, Beschreibungen und Zusammenfassungen können variable Werte verwenden. Zum Beispiel: Referenziere <i>max</i> durch <i>%max%</i> .

Tab. 15.4: Reiter *Rechner*

Attribut	Beschreibung
Zugeordnete Rechner	<i>Prometheus</i> führt die Abfrage auf den hier referenzierten Rechnern aus. Das Listener Modul führt die Tests für den Alert aus. Es ersetzt den Begriff <i>%instance%</i> im Abfrageausdruck durch einen regulären Ausdruck, der mit den zugewiesenen Rechnern übereinstimmt.

Zuweisung von Alarmen an Computer

Prometheus kann alle Computer überwachen, die mit Univention Management Console verwaltet werden.

Navigieren Sie in Univention Management Console zu *Computers* und wählen Sie den Computer aus, auf dem Sie Alarme aktivieren möchten. Wählen und fügen Sie die gewünschten Alarme im Reiter *Erweiterte Einstellungen* unter *Warnmeldungen* aus und speichern Sie Ihre Änderungen.

Tab. 15.5: Reiter *Erweiterte Einstellungen*

Attribut	Beschreibung
zugewiesene Warnmeldungen	Listet alle zugewiesenen Alarme für den aktuellen Computer auf. Fügen Sie hier Alarme hinzu oder entfernen Sie sie.

Neue Alarme erstellen

In diesem Abschnitt wird beschrieben, wie Sie ein benutzerdefiniertes Skript hinzufügen, um neue Metriken zu sammeln und Alarme zu erstellen.

Als Administrator können Sie die vorkonfigurierten Alarme, die mit UCS geliefert werden, durch zusätzliche Alarme ergänzen. Ein Alarmprüfung Skript exportiert Metriken über den Rechner, auf dem es läuft, an *Prometheus*. Eine *PromQL*-Abfrage auf Metriken definiert einen Alarm in *Prometheus*. Für weitere Informationen darüber, wie man eigene benutzerdefinierte Checks schreibt, siehe [Querying basis](#)³⁷¹.

Kopieren Sie das benutzerdefinierte Alarmprüfung Skript in das Verzeichnis `/usr/share/univention-monitoring-client/scripts/` auf dem UCS-System, das die benutzerdefinierten Metriken

³⁷⁰ <https://prometheus.io/docs/prometheus/latest/querying/basics/>

³⁷¹ <https://prometheus.io/docs/prometheus/latest/querying/basics/>

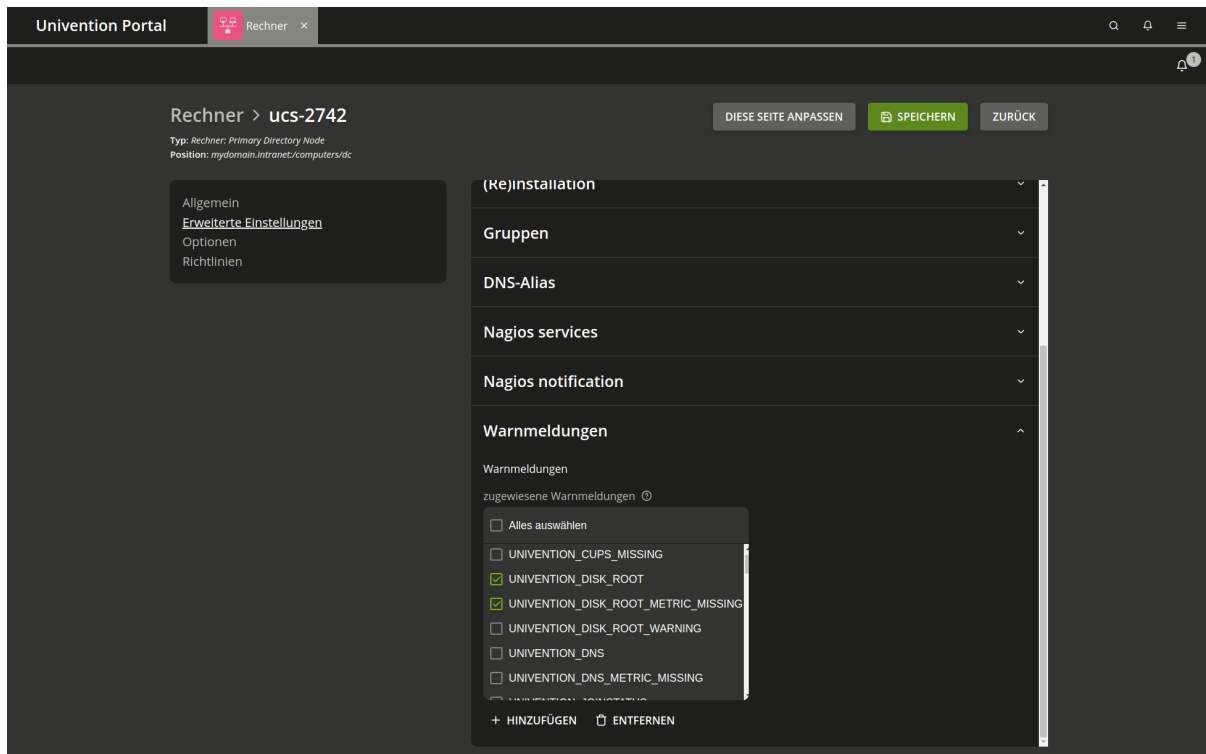


Abb. 15.2: Zuweisung eines Alarms an einen Computer

exportieren soll. Ändern Sie den Dateimodus auf *ausführbar* mit **chmod a+x PLUGIN**.

Alle von UCS gelieferten Alert Checks verwenden Python. Benutzerdefinierte Prüfungen können Perl, Python oder Shell verwenden und benötigen keine externen Bibliotheken oder Programme. Alle UCS-Systeme stellen immer die benötigten Interpreter zur Verfügung.

Verwendet die benutzerdefinierte Alarmprüfung dagegen externe Programme oder Bibliotheken, müssen Sie diese auf allen UCS-Systemen installieren, die die benutzerdefinierte Prüfung verwenden sollen.

Das Skript für die Alarmprüfung exportiert eine oder mehrere Metriken, indem es sie in eine Textdatei schreibt. Es muss gültige *Prometheus* Metriken in eine `.prom` Datei im `/var/lib/prometheus/node-exporter/` Verzeichnis schreiben. *Prometheus* importiert diese Datei.

Sie müssen den benutzerdefinierten Alarm in Univention Management Console konfigurieren, siehe *Konfiguration der Alarme* (Seite 147). Sie müssen einen Prometheus Ausdruck für die Metrik des Skripts in das Feld *Query expression* eingeben. Um den benutzerdefinierten Alarm zu UCS-Systemen zuzuordnen, siehe *Zuweisung von Alarmen an Computer* (Seite 148).

Siehe auch

Prometheus Namenskonventionen

[Metric and label naming](#)³⁷²

Text-basiertes Format einer `.prom`-Datei

[Exposition formats](#)³⁷³

³⁷² <https://prometheus.io/docs/practices/naming/>

³⁷³ https://prometheus.io/docs/instrumenting/exposition_formats/

15.3 Nagios

Mit UCS 5.0 wurde die Unterstützung für die Nagios Serverkomponente eingestellt. Die Systeme können jedoch weiterhin über NRPE überwacht werden.

15.3.1 Installation

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

Einige der Pakete werden bei der Installation der entsprechenden Dienste automatisch mit eingerichtet. Wird beispielsweise der UCS AD Connector eingerichtet, bringt dieser das Überwachungsplugin `univention-nagios-ad-connector` mit.

15.3.2 Vorkonfigurierte Nagios-Prüfungen

Während der Installation werden automatisch grundlegende Nagios-Prüfungen für die UCS-Systeme der Domäne eingerichtet.

Tab. 15.6: Vorkonfigurierte Nagios-Prüfungen

Nagios-Dienst	Beschreibung
UNIVENTION_PING	Testet die Erreichbarkeit des überwachten UCS-Systems mit dem Kommando <code>ping</code> . In der Standardeinstellung wird der Fehlerzustand erreicht, wenn die Antwortzeit 50 ms oder 100 ms überschreitet oder Paketverluste von 20% oder 40% auftreten.
UNIVENTION_DISK_ROOT	Überwacht den Füllstand der <code>/</code> -Partition. Unterschreitet der verbleibende freie Platz in der Standardeinstellung 25% oder 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 <code>www.univention.de</code> . Ist für die UCS-Domäne kein DNS-Forwarder definiert, schlägt diese Abfrage fehl. In diesem Fall kann <code>www.univention.de</code> z.B. gegen den FQDN des Primary Directory Node ersetzt werden, um die Funktion der Namensauflösung zu testen.
UNIVENTION_LDAP	Überwacht den auf Directory Nodes laufenden LDAP-Server.
UNIVENTION_LOAD	Überwacht die Systemlast.
UNIVENTION_NTP	Fragt auf dem überwachten UCS-System die Uhrzeit beim NTP-Dienst ab. Tritt eine Abweichung von mehr als 60 oder 120 Sekunden auf, wird der Fehlerzustand erreicht.
UNIVENTION_SMTP	Testet den Mailserver.
UNIVENTION_SSL	Testet die verbleibende Gültigkeitsdauer der UCS-SSL-Zertifikate. Dieses Plugin ist nur für Primary Directory Node und Backup Directory Nodes geeignet.
UNIVENTION_SWAP	Überwacht die Auslastung der Swap-Partition. Unterschreitet der verbleibende freie Platz den Schwellwert (in der Standardeinstellung 40% oder 20%), wird der Fehlerzustand gesetzt.
UNIVENTION_REPLICATION	Überwacht den Status der LDAP-Replikation, erkennt das Vorhandensein einer <code>failed.ldif</code> -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 (NSCD). Läuft kein NSCD-Prozess wird ein CRITICAL-Event ausgelöst, läuft mehr als ein Prozess, wird ein WARNING-Event ausgelöst.
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 nicht-aufgerufene Join-Skripte vorhanden, wird ein WARNING-Event zurückgeliefert.
UNIVENTION_KPASSWDD	Prüft die Verfügbarkeit des Kerberos-Passwort-Dienstes (nur verfügbar auf Primary/Backup Directory Node). Läuft weniger oder mehr als ein Prozess, wird ein CRITICAL-Event ausgelöst.
UNIVENTION_CUPS	Überwacht den CUPS-Druckdienst. Läuft <code>cupsd</code> -Prozess oder ist die Weboberfläche auf Port 631 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.

Die folgenden Nagios-Dienste sind nur auf dem jeweiligen Nagios Client verfügbar, sobald zusätzliche Pakete installiert wurden (siehe *Installation* (Seite 150)):

Tab. 15.7: Zusätzliche Nagios Checks

Nagios-Dienst	Beschreibung
UNIVENTION_OPST	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 <code>/dev/sda</code> . Für die Festplatten <code>sdb</code> , <code>sdc</code> und <code>sdd</code> existieren entsprechende Nagios-Dienste.
UNIVENTION_RAID	Prüft den Status des Software-RAIDs über <code>/proc/mdadm</code> und gibt einen CRITICAL Alarm zurück, sofern eine Festplatte des RAID-Verbunds ausgefallen ist, oder einen WARNING Alarm zurück, wenn der Recovery-Vorgang läuft.
UNIVENTION_ADCONNECTOR	<p>Prüft den Status des Active Directory Connectors:</p> <ul style="list-style-type: none"> • Läuft kein Connector-Prozess, wird der Status CRITICAL zurückgegeben. • Existiert 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. <p>Das Plugin kann auch in Multi-Connector-Instanzen verwendet werden. Dabei muss der Name der Instanz als Parameter übergeben werden.</p>

16.1 Univention Configuration Registry Variablen

Dieser Anhang listet Univention Configuration Registry Variablen auf, die im Handbuch erwähnt werden.

appcenter/update/skip-zsync

Wenn diese Variable auf `true` gesetzt wird, wird **zsync** beim App Center Update übersprungen und die Metadaten werden direkt per HTTPS heruntergeladen. Dies ist nützlich in Umgebungen mit restriktiven Proxies, die nur HTTPS erlauben oder keine HTTP-Range-Requests unterstützen.

appcenter/update/zsync-timeout

Legt ein Timeout in Sekunden für **zsync**-Operationen fest. Wenn **zsync** innerhalb dieser Zeit nicht abgeschlossen wird, schlägt der Vorgang fehl und es wird auf den direkten Download zurückgegriffen. Dies verhindert lange Wartezeiten in problematischen Proxy-Umgebungen. Standardwert ist 10 Sekunden. Kann auf 0 gesetzt werden, um das Timeout zu deaktivieren. Empfohlener Bereich: 5-300 Sekunden.

auth/faillog

Konfiguriert das automatische Sperren von Benutzern nach fehlgeschlagenen Anmeldungen im PAM Stack. Zum Aktivieren, setze den Wert auf `yes`. Für mehr Informationen, siehe *PAM-Stack* (Seite 39).

auth/faillog/limit

Konfiguriert die Obergrenze an fehlerhaften Anmeldeversuchen für eine Benutzerkontosperrung. Für mehr Informationen, siehe *PAM-Stack* (Seite 39).

auth/faillog/lock_global

Konfiguriert auf Primary Directory Node und Backup Directory Node eine globale Sperre nach fehlerhaften Anmeldeversuchen im LDAP-Verzeichnis. Für mehr Informationen, siehe *PAM-Stack* (Seite 39).

auth/faillog/root

Um das Benutzerkonto `root` der Sperrung des PAM-Stack-Kontos zu unterwerfen, setzen Sie den Wert auf `yes`. Die Voreinstellung ist `no`. Für weitere Informationen, siehe *PAM-Stack* (Seite 39).

auth/faillog/unlock_time

Legen Sie ein Zeitintervall fest, in dem eine Kontosperrung aufgehoben wird. Der Wert wird in Sekunden angegeben. Der Wert 0 setzt die Sperre sofort zurück. Für weitere Informationen, siehe *PAM-Stack* (Seite 39).

auth/sshd/user/root

Um die SSH-Anmeldung für den Benutzer `root` komplett zu verbieten, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 54).

backup/clean/max_age

Legt fest, wie lange ein UCS-System alte Sicherungsdateien der LDAP-Daten aufbewahrt. Erlaubte Werte sind ganzzahlige Zahlen und definieren Tage. Das System löscht keine Sicherungsdateien, wenn die Variable nicht gesetzt ist. Siehe *Tägliche Sicherung der LDAP-Daten* (Seite 13).

connector/ad/ldap/binddn

Konfiguriert den LDAP-DN eines privilegierten Replikationsbenutzers. Für weitere Informationen, siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 65) und *Änderung des AD-Zugriffspassworts* (Seite 72).

connector/ad/ldap/bindpw

Legt das Passwort eines privilegierten Replikationsbenutzers fest. Für weitere Informationen, siehe *UCS als Mitglied einer Active Directory-Domäne* (Seite 65) und *Änderung des AD-Zugriffspassworts* (Seite 72).

connector/ad/ldap/ssl

Um die verschlüsselte Kommunikation zwischen dem UCS System und Active Directory zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Import des SSL-Zertifikats des Active Directory* (Seite 70).

connector/ad/mapping/group/language

Konfiguriert die Zuordnung für die Umwandlung von Gruppennamen in anglophonen AD Domänen. Für weitere Informationen, siehe *Gruppen* (Seite 79).

connector/ad/poll/sleep

Konfiguriert das Intervall für die Abfrage nach Änderungen in der AD-Domäne. Die Voreinstellung ist 5 Sekunden. Für weitere Informationen, siehe *Einrichtung des UCS AD-Connectors* (Seite 68).

connector/ad/retryrejected

Konfiguriert die Anzahl der Zyklen, die der UCS AD Connector versucht, ein Objekt aus der AD-Domäne zu synchronisieren, wenn es nicht synchronisiert werden kann. Der Standardwert ist 10 Zyklen. Für weitere Informationen, siehe *Einrichtung des UCS AD-Connectors* (Seite 68).

connector/debug/level

Debug-Level für die Debug-Ausgaben in `/var/log/univention/connector-s4.log`. Mögliche Werte sind 0-4.

connector/debug/udm/level

Debug-Level für alle Operation von UDM, protokolliert in `/var/log/univention/connector-s4.log`. Mögliche Werte sind 0-5.

cups/cups-pdf/anonymous

Legt das Zielverzeichnis für den *Generic CUPS-PDF Printer* für anonyme Druckaufträge fest. Standardmäßig ist dies der Wert `/var/spool/cups-pdf/`. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 121).

cups/cups-pdf/cleanup/enabled

Um veraltete Druckaufträge des *Generic CUPS-PDF Printer* zu bereinigen, setzen Sie den Wert auf `true`. Für die Speicherzeit, siehe *cups/cups-pdf/cleanup/keep* (Seite 154). Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 121).

cups/cups-pdf/cleanup/keep

Legt die Speicherzeit in Tagen für PDF-Dateien aus dem *Generic CUPS-PDF Printer* fest. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 121).

cups/cups-pdf/directory

Legt das Zielverzeichnis für den *Generic CUPS-PDF Printer* fest. Standardmäßig ist dies der Wert `/var/spool/cups-pdf/%U` und verwendet für jeden Benutzer ein anderes Verzeichnis. Für weitere Informationen, siehe *Generierung von PDF-Dokumenten aus Druckaufträgen* (Seite 121).

cups/errorpolicy

Um fehlgeschlagene Druckaufträge automatisch alle 30 Sekunden zu wiederholen, setzen Sie den Wert auf `retry-job`. Für weitere Informationen, siehe *Einstellung lokaler Konfigurationseigenschaften eines Druckservers* (Seite 120).

cups/include/local

Um die Konfiguration aus `/etc/cups/cupsd.local.conf` einzubeziehen, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Einstellung lokaler Konfigurationseigenschaften eines Druckservers* (Seite 120).

cups/server

Definiert den Druckserver, der von einem UCS-System verwendet werden soll. Für weitere Informationen, siehe *Konfiguration des verwendeten Druckservers* (Seite 52).

directory/manager/blocklist/cleanup/cron

Diese Variable bestimmt, wie oft UDM nach abgelaufenen Blocklisteneinträge sucht und diese entfernt. Der Wert folgt der *cron Syntax*³⁷⁴ für die Zeitdefinition. Der Standardwert ist auf täglich um 8:00 Uhr morgens gesetzt. Weitere Informationen finden Sie unter *Abgelaufene Blocklisteneinträge* (Seite 40).

directory/manager/blocklist/enabled

Aktiviert die Verwaltung von Blocklisteneinträgen in UDM. Der Standardwert ist `false`. Für Informationen über die Aktivierung, siehe *Aktivieren von Blocklisten* (Seite 40).

directory/manager/cmd/debug/level

Diese Variable konfiguriert den Detailgrad der Protokollierung in `/var/log/univention/directory-manager-cmd.log`. Mögliche Werte: 0-5 (0: nur Fehlermeldungen bis 5: alle Debugausgaben).

directory/manager/rest/debug/level

Der Detailgrad der Logmeldungen in `/var/log/univention/directory-manager-rest.log`. Mögliche Werte: 0-5/99 (0: nur Fehlermeldungen bis 5: alle Debugausgaben, mit 99 werden auch sensible Daten wie Klartext-Passwörter protokolliert).

directory/manager/templates/alphanum/whitelist

Definieren Sie eine Erlaubnisliste von Zeichen, die nicht durch die Option `:alphanum` für die Wertedefinition in Benutzervorlagen entfernt werden. Für weitere Informationen, siehe *Benutzervorlagen* (Seite 39).

directory/manager/user_group/uniqueness

Steuert, ob UCS Benutzer mit demselben Benutzernamen wie bestehende Gruppen verhindert. Um die Prüfung auf Eindeutigkeit zu deaktivieren, setzen Sie den Wert auf `false`. Für weitere Informationen, siehe *Modul Benutzerverwaltung - Reiter Allgemein* (Seite 36).

directory/manager/web/modules/computers/computer/wizard/disabled

Um den vereinfachten Assistenten für die Computerverwaltung zu deaktivieren, setzen Sie diese Variable auf `true`. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 47).

directory/manager/web/modules/groups/group/checks/circular_dependency

Steuert die Prüfung auf zirkuläre Abhängigkeiten bei verschachtelten Gruppen. Um sie zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Verschachtelte Gruppen mit Gruppen in Gruppen* (Seite 46).

directory/manager/web/modules/users/user/wizard/disabled

Deaktiviert den vereinfachten Assistenten zum Anlegen von Benutzern, wenn der Wert auf `true` gesetzt ist. In der Standardeinstellung ist der Assistent aktiviert. Für weitere Informationen, siehe *Verwaltung von Benutzern über Univention Management Console Modul* (Seite 36).

directory/reports/logo

Definiert den Pfad und den Namen einer Bilddatei zur Verwendung als Logo in einer Univention Directory Report PDF-Datei. Für weitere Informationen, siehe *Anpassung/Erweiterung von Univention Directory Reports* (Seite 30).

dns/allow/transfer

Um den DNS-Zonentransfer bei Verwendung des OpenLDAP-Backends zu deaktivieren, setzen Sie den Wert auf `none`. Für weitere Informationen, siehe *Konfiguration von Zonentransfers* (Seite 97).

³⁷⁴ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/cron.html#cron-syntax>

dns/backend

Konfiguriert das DNS-Backend. Für weitere Informationen, siehe *Konfiguration des Daten-Backends des Nameservers* (Seite 96).

dns/debug/level

Konfiguriert den Debug-Level für BIND. Für weitere Informationen, siehe *Konfiguration der Debug-Ausgaben von BIND* (Seite 96).

dns/dlz/debug/level

Konfiguriert den Debug-Level für das Samba DNS Backend. Für weitere Informationen, siehe *Konfiguration der Debug-Ausgaben von BIND* (Seite 96).

dns/forwarder1

Definiert den ersten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

dns/forwarder2

Definiert den zweiten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

dns/forwarder3

Definiert den dritten *externen DNS-Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

fetchmail/autostart

Steuert den automatischen Start von Fetchmail. Um Fetchmail zu deaktivieren, setzen Sie den Wert auf `false`. Für weitere Informationen, siehe *Integration von Fetchmail zum Abrufen von Mail von externen Postfächern* (Seite 131).

freeradius/auth/helper/ntlm/debug

Konfiguriert den Debug-Level oder die Ausführlichkeit für die Protokollierung von FreeRADIUS-Meldungen. Für weitere Informationen, siehe *Fehlersuche* (Seite 110).

freeradius/conf/allow-mac-address-authentication

Konfiguriert, ob Radius die MAC-Adresse als Benutzernamen und Passwort für die 802.1X-Authentifizierung zulässt. Der Standardwert ist `false`. Für weitere Informationen, siehe *MAC Authentication Bypass für Computerobjekte* (Seite 106).

freeradius/conf/mac-addr-regexp

Konfiguriert den regulären Ausdruck für die MAC-Adresse für den Radius Server. Der reguläre Ausdruck muss sechs Gruppen enthalten, wobei jede Gruppe ein Byte der MAC-Adresse darstellt.

Der Standardwert ist der reguläre Ausdruck: `([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})[^0-9a-f]?([0-9a-f]{2})`

Added in version 5.0-6-erratum-...: Mit [UCS 5.0 erratum 1011³⁷⁵](#) kann der Radius-Server mit verschiedenen Formaten der MAC-Adressen für den Benutzernamen bei Verwendung von MAB umgehen.

Für weitere Informationen und Effekte, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 132).

freeradius/conf/tls-max-version

Konfiguriert die maximale TLS Version, die der Server zu verwenden versucht. Einige Betriebssysteme unterstützen möglicherweise nicht die neueste Version, siehe *TLS 1.3 deaktivieren* (Seite 110).

freeradius/vlan-id

Konfiguriert den Ersatzwert für die VLAN-ID für Benutzer, die nicht Mitglied einer Gruppe mit einer VLAN-ID sind. Für weitere Informationen, siehe *VLAN IDs* (Seite 110).

³⁷⁵ <https://errata.software-univention.de/#/?erratum=5.0x1011>

gateway

Konfiguriert das IPv4-Netzwerk-Gateway. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 49).

google-apps/attributes/anonymize

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das Google Apps for Work Connector synchronisiert, aber mit zufälligen Daten füllt. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Für weitere Informationen, siehe *Konfiguration* (Seite 92).

google-apps/attributes/mapping/. *

Definiert eine Zuordnung von UCS LDAP-Attributen eines Benutzerkontos für die Synchronisation zu Google Apps Attributen. Die Standardeinstellungen reichen in der Regel für die meisten Umgebungsanforderungen aus. Für weitere Informationen, siehe *Konfiguration* (Seite 92).

google-apps/attributes/never

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Google Apps for Work Connector nie synchronisiert, auch wenn sie in *google-apps/attributes/mapping/. ** (Seite 157) oder *google-apps/attributes/anonymize* (Seite 157) erwähnt werden. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Konfiguration* (Seite 92).

google-apps/debug/werror

Konfigurieren Sie zusätzliche Debugausgaben für Google Apps for Work. Für weitere Informationen, siehe *Fehlersuche* (Seite 93).

google-apps/groups/sync

Ermöglicht die Synchronisation von Gruppen der Google Apps for Work Benutzergruppen mit dem Wert *yes*. Für weitere Informationen, siehe *Konfiguration* (Seite 92).

groups/default/domainadmins

Konfiguriert den Standardgruppennamen für die Domänenadministratorgruppe. Der Wert kann während einer AD-Übernahme geändert werden. Für weitere Informationen, siehe *Domänenmigration* (Seite 81).

grub/append

Definiert Linux-Kernel-Boot-Optionen, die der GRUB-Bootloader an den Linux-Kernel zum Systemstart weitergibt. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 48).

grub/bootsplash

Um den Splash-Screen beim Systemstart zu deaktivieren, setzen Sie den Wert auf *nosplash*. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 48).

grub/gfxmode

Legt die Bildschirmgröße und Farbtiefe für das GRUB-Bootmenü fest. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 48).

grub/timeout

Legt die Wartezeit in Sekunden im GRUB-Bootmenü fest. Während dieser Wartezeit können alternative Bootmenüeinträge ausgewählt werden. Der Standardwert ist 5 Sekunden. Für weitere Informationen, siehe *GRUB Boot-Manager* (Seite 48).

grub/xenhopt

Legt Optionen fest, die an den Xen-Hypervisor übergeben werden. Weitere Informationen finden Sie unter *GRUB Boot-Manager* (Seite 48).

interfaces/ethX/address

Legt die Netzwerk-IPv4-Adresse für die Schnittstelle *ethX* fest. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 49).

interfaces/ethX/netmask

Definiert die Netzwerkmaske für die Schnittstelle *ethX*. Ersetzen Sie *X* durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 49).

interfaces/ethX/type

Legt den Netzwerkschnittstellentyp für die Schnittstelle `ethX` fest. Ersetzen Sie `X` durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 49).

interfaces/ethX_Y/setting

Definiert eine zusätzliche virtuelle Schnittstelle. Ersetzen Sie `X` und `Y` durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv4-Adressen* (Seite 49).

interfaces/ethX/ipv6/address

Legt die Netzwerk-IPv6-Adresse für die Schnittstelle `ethX` fest. Ersetzen Sie `X` durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 49).

interfaces/ethX/ipv6/prefix

Legt das Netzwerk-IPv6-Präfix für die Schnittstelle `ethX` fest. Ersetzen Sie `X` durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 49).

interfaces/ethX/ipv6/acceptRA

Aktiviert die zustandslose Adressautokonfiguration (SLAAC) für die Schnittstelle `ethX`. Ersetzen Sie `X` durch den tatsächlichen Wert für die Schnittstelle. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 49).

ipv6/gateway

Konfiguriert das IPv4-Netzwerk-Gateway. Für weitere Informationen, siehe *Konfiguration von IPv6-Adressen* (Seite 49).

kerberos/adminserver

Definiert das System, das den Kerberos-Adminserver bereitstellt. Siehe *Kerberos Adminserver* (Seite 19).

kerberos/kdc

Enthält den Verweis auf den KDC. Normalerweise wählt ein UCS-System den zu verwendende KDC aus einem DNS-Diensteintrag aus. Mit dieser Variable können Administratoren einen alternativen KDC konfigurieren.

kerberos/realm

Enthält den Namen des Kerberos-Realms. Siehe *Kerberos* (Seite 19).

kernel/blacklist

Definiert zusätzliche Linux-Kernelmodule, die während des Systemstarts geladen werden müssen. Einzelne Elemente müssen durch ein Semikolon (;) getrennt werden. Für weitere Informationen, siehe *Treiber-Management / Kernel-Module* (Seite 48).

kernel/modules

Definiert Linux-Kernel-Module, die beim Systemstart nicht geladen werden dürfen. Einzelne Einträge müssen mit einem Semikolon (;) getrennt werden. Für weitere Informationen, siehe *Treiber-Management / Kernel-Module* (Seite 48).

ldap/authz-regex/federated-accounts

Legt fest, ob der `authz-regex` hinzugefügt werden soll, um bei `federated accounts` SASL-Benutzernamen LDAP-DNs zuzuordnen. Achtung: Bei Aktivierung funktioniert die Anmeldung mit einem normalen Benutzer mit einer UUID als Benutzername nicht mehr.

ldap/authz-regex/users

Legt fest, ob der `authz-regex` hinzugefügt werden soll, um SASL-Benutzernamen LDAP-DNs zuzuordnen.

ldap/database/internal/acl/blocklists/groups/read

Liste der DNs von Gruppen, die Lesezugriff auf alle Objekte unter dem Container `cn=blocklists` in der internen Datenbank haben. Für weitere Informationen, siehe *LDAP ACLs für Blocklisten* (Seite 40).

ldap/database/internal/acl/blocklists/groups/write

Liste der DNs von Gruppen, die Schreibzugriff auf alle Objekte unter dem Container `cn=blocklists` in der internen Datenbank haben. Für weitere Informationen, siehe *LDAP ACLs für Blocklisten* (Seite 40).

ldap/acl/read/anonymous

Steuert, ob der LDAP-Server anonymen Zugriff auf das LDAP-Verzeichnis zulässt. In der Standardkonfiguration lässt der LDAP-Server keinen anonymen Zugriff auf das LDAP-Verzeichnis zu.

ldap/acl/read/ips

Eine Liste von IP-Adressen, für die der LDAP-Server anonymen Zugriff erlaubt. Siehe *Zugriffskontrolle auf das LDAP-Verzeichnis* (Seite 13).

ldap/acl/nestedgroups

Steuert, ob verschachtelte Gruppen erlaubt sind. Standardmäßig sind verschachtelte Gruppen aktiviert. Siehe *Zugriffskontrolle auf das LDAP-Verzeichnis* (Seite 13).

ldap/acl/user/passwordreset/accesslist/groups/dn

Verwenden Sie eine andere Gruppe als die Standardgruppe `User Password Admins`, um Benutzerpasswörter zurückzusetzen. Der Wert ist ein Distinguished Name (DN) für eine Benutzergruppe. Siehe *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 13).

ldap/acl/user/passwordreset/attributes

Wenn Benutzer, die die Passwörter anderer Benutzer ändern dürfen, Zugriff auf zusätzliche LDAP-Attribute benötigen, die für die Passwortänderung erforderlich sind, konfigurieren Sie diese in dieser Variablen. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 13).

ldap/acl/user/passwordreset/protected/uid

Konfiguriert Benutzer mit ihrer Benutzerkennung, um sie vom Zurücksetzen von Benutzerpasswörtern durch Administratoren, die Benutzerpasswörter ändern dürfen, auszuschließen. Trennen Sie mehrere Werte mit einem Komma. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 13).

ldap/acl/user/passwordreset/protected/gid

Konfiguriert Gruppen mit ihrer Gruppenkennung, um sie vom Zurücksetzen von Benutzerpasswörtern durch Administratoren, die Benutzerpasswörter ändern dürfen, auszuschließen. Trennen Sie mehrere Werte mit einem Komma. Weitere Informationen finden Sie unter *Delegation des Zurücksetzens von Benutzerpasswörtern* (Seite 13).

ldap/idletimeout

Konfiguriert eine Zeitspanne in Sekunden, nach der die LDAP-Verbindung auf der Serverseite unterbrochen wird. Siehe *Timeout für inaktive LDAP-Verbindungen* (Seite 13).

ldap/logging/exclude1

Einzelne Bereiche des Verzeichnisdienstes von der Protokollierung ausschließen. Siehe *Revisionssichere LDAP-Protokollierung* (Seite 13).

ldap/logging/excludeN

Siehe *ldap/logging/exclude1* (Seite 159).

ldap/logging/id-prefix

Fügt die Transaktions-ID eines Eintrags in das Verzeichnisprotokoll ein. Mögliche Werte sind der Standardwert `yes` und `no`. Siehe *Revisionssichere LDAP-Protokollierung* (Seite 13).

ldap/master

Enthält den FQDN des Primary Directory Node in der Domäne.

ldap/overlay/lastbind

Um das `lastbind`-Overlay-Modul für den LDAP-Server zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos* (Seite 39).

ldap/overlay/lastbind/precision

Legt die Zeit in Sekunden fest, die vergehen muss, bevor der `authTimestamp` durch das `lastbind`-Overlay wieder aktualisiert wird. Für weitere Informationen, siehe *Overlay-Modul zur Aufzeichnung der letzten erfolgreichen LDAP-Anmeldung eines Kontos* (Seite 39).

ldap/policy/cron

Zeitintervall für das Schreiben profilbasierter UCR-Variablen in ein UCS-System. Der Standardwert ist eine Stunde. Für weitere Informationen, siehe *Richtlinienbasierte Konfiguration von UCR-Variablen* (Seite 51).

ldap/ppolicy/enabled

Um die automatische Kontosperrung zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *OpenLDAP* (Seite 39).

ldap/pw-bcrypt

Aktiviert `bcrypt` als Passworthash-Methode, wenn auf `true` gesetzt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 19).

ldap/server/addition

Zusätzlicher LDAP-Server, den ein UCS-System nach Informationen im Verzeichnisdienst abfragen kann.

ldap/server/name

Der LDAP-Server, den das System nach Informationen im Verzeichnisdienst abfragt.

listener/debug/level

Legt die Detailebene für Protokollmeldungen des Listeners in `/var/log/univention/listener.log` fest. Die möglichen Werte reichen von 0 (nur Fehlermeldungen) bis 4 (alle Statusmeldungen). Nach einer Änderung des Debug-Levels muss der Univention Directory Listener neu gestartet werden.

listener/shares/rename

Inhalte bestehender Freigabeverzeichnisse werden verschoben, wenn der Pfad zu einer Freigabe geändert wird und der Wert auf `yes` gesetzt wird. Für weitere Informationen, siehe *Freigaben UMC Modul - Reiter Allgemein* (Seite 114).

local/repository

Aktiviert und deaktiviert das lokale Repository. Für weitere Informationen, siehe *Einrichtung und Aktualisierung eines lokalen Repositories* (Seite 33).

logrotate/compress

Steuert, ob rotierte Protokolldateien mit `gzip` komprimiert werden. Für weitere Informationen, siehe *Logdateien* (Seite 53).

log/rotate/weeks

Konfiguriert das Rotationsintervall der Protokolldateien auf einem UCS-System in Wochen. Der Standardwert ist 12 Wochen. Für weitere Informationen, siehe *Logdateien* (Seite 53).

logrotate/rotates

Konfiguriert die Rotation der Protokolldateien entsprechend der Dateigröße, zum Beispiel `size 50M`. Für weitere Informationen, siehe *Logdateien* (Seite 53).

machine/password/length

Definieren Sie die Länge des Computer-Passworts, auch *machine secret* genannt. Der Standardwert ist 20. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 47).

mail/antispam/bodysizelimit

Legt die Größe der E-Mails fest, die von SpamAssassin auf Spam untersucht werden. Der Standardwert ist 300 Kilobytes. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 129).

mail/antispam/learndaily

Konfiguriert die Auswertung von Ham E-Mails im Ham-Ordner für die tägliche Auswertung. Die Auswertung ist standardmäßig aktiviert. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 129).

mail/antispam/requiredhits

Legt den Schwellenwert in Punkten fest, ab dem eine E-Mail als Spam eingestuft wird. Der Standardwert ist 5. Für weitere Informationen, siehe *Spamerkennung und -filterung* (Seite 129).

mail/antivir

Um die Viren- und Schadsoftware-Erkennung für ein- und ausgehende E-Mails zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Viren- und Malwareerkennung* (Seite 130).

mail/antivir/spam

Legt fest, ob der Spam-Filter aktiv ist. Um die Spam-Filterung zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Viren- und Malwareerkennung* (Seite 130).

mail/archivefolder

Konfiguriert Postfix so, dass alle ein- und ausgehenden E-Mails zu Archivierungszwecken als Blindkopie an diese E-Mail-Adresse gesendet werden. Die Variable ist standardmäßig nicht gesetzt. Für weitere Informationen, siehe *Konfiguration einer Blindkopie zur Anbindung von E-Mail-Archivierungslösungen* (Seite 134).

mail/dovecot/auth/cache_ttl

Konfiguriert die Ablaufzeit des Authentifizierungscaches in Dovecot für den E-Mail-Dienst. Weitere Informationen finden Sie unter *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 128).

mail/dovecot/auth/cache_negative_ttl

Konfiguriert die Ablaufzeit des Authentifizierungscaches in Dovecot für den E-Mail-Dienst. Weitere Informationen finden Sie unter *Zuordnung von E-Mail-Adressen zu Benutzern* (Seite 128).

mail/dovecot/folder/ham

Legt den Namen des Ordners für E-Mails fest, die SpamAssassin als *ham* betrachtet. Der Standardwert ist `Ham`. Für weitere Informationen, siehe *Spamererkennung und -filterung* (Seite 129).

mail/dovecot/folder/Spam

Legt den Namen des Ordners fest, in den SpamAssassin als Spam eingestufte E-Mails verschiebt. Der Standardwert ist `Spam`. Für weitere Informationen, siehe *Spamererkennung und -filterung* (Seite 129).

mail/dovecot/imap

Steuert den IMAP-Protokolldienst im Dovecot IMAP-Dienst. Um den Zugriff auf E-Mails über IMAP zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Maildienste* (Seite 127).

mail/dovecot/limits

Konfiguriert verschiedene Verbindungsgrenzen für den Dovecot-Dienst. Für weitere Informationen, siehe *Beschränkung der Verbindungsanzahl* (Seite 137).

mail/dovecot/location/separate_index

Konfiguriert den Dovecot-Dienst so, dass er einen vom Speicherort der E-Mail-Nachrichten getrennten Index verwendet. Um den separaten Index zu aktivieren, setzen Sie den Wert auf `yes`. Dovecot schreibt den Index in `/var/lib/dovecot/index/`. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/mailbox/rename

Legt fest, wie die Dovecot-Dienste auf Änderungen der primären E-Mail-Adresse reagieren. Der Standardwert ist `yes` und ändert den Namen des IMAP-Postfachs des Benutzers. Für weitere Informationen über die Werte, siehe *Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten* (Seite 135).

Gemeinsame Ordner werden nicht umbenannt. Weitere Informationen finden Sie unter *Verwaltung von globalen IMAP-Ordern* (Seite 128).

mail/dovecot/mailbox/delete

Konfiguriert die Löschung eines IMAP-Postfachs. Der Standardwert ist `no` und behält die Mailbox. Für weitere Informationen, siehe *Handhabung der Postfächer bei Änderung der E-Mail-Adresse und Löschung von Benutzerkonten* (Seite 135).

Der Wert wirkt sich auch auf freigegebene IMAP-Ordner aus. Für weitere Informationen, siehe *Verwaltung von globalen IMAP-Ordern* (Seite 128).

mail/dovecot/pop3

Steuert den POP3-Protokolldienst im Dovecot IMAP-Dienst. Um den Zugriff auf E-Mails über POP3 zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Maildienste* (Seite 127).

mail/dovecot/process/lock_method

Steuert die Sperrmethode für *lockd*. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/process/mail_nfs_index

Konfiguriert den Dovecot-Dienst so, dass er nach dem Schreiben von Indexdateien die NFS-Zwischenspeicher leert, wenn er auf *yes* gesetzt ist. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/process/mail_nfs_storage

Konfiguriert den Dovecot-Dienst so, dass er die NFS-Caches leert, wenn er auf *yes* gesetzt ist. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/process/mmap_disable

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/process/dotlock_use_excl

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/process/mail_fsync

Erlaubt die Speicherung von E-Mails auf NFS. Für weitere Informationen, siehe *Mailserver-Speicher auf NFS* (Seite 136).

mail/dovecot/quota/warning/subject

Legt den Betreff für die E-Mail an den Benutzer fest, der die konfigurierte Quotengrenze überschreitet. Für weitere Informationen, siehe *Mail-Quota* (Seite 129).

mail/dovecot/quota/warning/text

Konfiguriert den E-Mail-Textkörper für die E-Mail an den Benutzer, der die konfigurierte Quotengrenze überschreitet. Prozentuale Werte können unterschiedliche Texte haben. Um z.B. einen Text für 50 % des Kontingents zu konfigurieren, setzen Sie `mail/dovecot/quota/warning/text/50=Ihr Text`.

Für weitere Informationen, siehe *Mail-Quota* (Seite 129).

mail/hosteddomains

Konfiguriert die von UCS verwalteten Mail-Domänen. Für weitere Informationen, siehe *Verwaltung von Mail-Domänen* (Seite 128).

mail/messagesizelimit

Legt die maximale Größe einer E-Mail in Bytes für eingehende und ausgehende E-Mails fest. Die Standard-einstellung ist 10240000 Bytes. Für weitere Informationen, siehe *Konfiguration der maximalen E-Mailgröße* (Seite 133).

mail/postfix/mastercf/options/smtp/smtpd_sasl_auth_enable

Um die Authentifizierung für die Übermittlung von E-Mails an Port 25 zu aktivieren, setzen Sie den Wert auf *yes*. Für weitere Informationen, siehe *Konfiguration der SMTP Ports* (Seite 134).

mail/postfix/policy/listfilter

Um den Personenkreis einzuschränken, der E-Mails an Mailinglisten senden darf, setzen Sie den Wert auf *yes* und starten Sie den Postfix-Dienst neu. Für weitere Informationen, siehe *Verwaltung von Mailinglisten* (Seite 128) und *Verwaltung von Mailgruppen* (Seite 128).

mail/postfix/postscreen/

Ein Präfix von Variablen zur Konfiguration von **postscreen**. Für weitere Informationen, siehe *Konfiguration zusätzlicher Prüfungen* (Seite 134).

mail/postfix/postscreen/enabled

Um den Postscreen für die Überprüfung der Berechtigung eingehender E-Mails zu aktivieren, setzen Sie den Wert auf *yes*. Für weitere Informationen, siehe *Konfiguration zusätzlicher Prüfungen* (Seite 134).

mail/postfix/smtpd/restrictions/recipient

Konfiguriert die DNS-basierte Blackhole-Liste (DNSBL) für Postfix im Format `mail/postfix/smtpd/restrictions/recipient/SEQUENCE=REGEL`.

Zum Beispiel:

```
mail/postfix/smtpd/restrictions/recipient/80="reject_rbl_client
ix.dnsbl.manitu.net".
```

Für weitere Informationen, siehe *Identifikation von Spam Quellen mit DNS basierten Blackhole Listen* (Seite 130).

mail/postfix/softbounce

Um E-Mails nach einem Mail-Bounce nicht zurückzusenden, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration von Softbounces* (Seite 134).

mail/postfix/tls/client/level

Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 132).

mail/relayauth

Wenn eine Authentifizierung für das Mail-Relay erforderlich ist, setzen Sie den Wert auf `yes` und fügen Sie die Anmeldeinformationen in `/etc/postfix/smtp_auth` ein. Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 132).

mail/relayhost

Konfiguriert den voll qualifizierten Domänennamen (FQDN) eines Mail-Relay-Servers. Für weitere Informationen, siehe *Konfiguration eines Relay-Hosts für den Mailversand* (Seite 132).

nameserver1

Definiert den ersten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

nameserver2

Definiert den zweiten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

nameserver3

Definiert den dritten *Domain DNS Server*. Weitere Informationen finden Sie unter *Konfiguration der Nameserver* (Seite 49).

notifier/debug/level

Legt die Detailebene für die Protokollmeldungen des Notifiers in `/var/log/univention/notifier.log` fest. Die möglichen Werte reichen von 0 (nur Fehlermeldungen) bis 4 (alle Statusmeldungen). Nach einer Änderung des Debug-Levels muss der Univention Directory Notifier neu gestartet werden.

nscd/debug/level

Legt die Detailebene für Protokollmeldungen des NSCD fest. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 53).

nscd/hosts/maxdbsize

Konfiguriert die Größe der Hash-Tabelle des NSCD für Hosts. Der Standardwert ist 6007. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 53).

nscd/hosts/positive_time_to_live

Legt die Zeit fest, die ein aufgelöster Hostname im Cache von NSCD gehalten wird. Die Voreinstellung ist eine Stunde in Sekunden (3600). Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 53).

nscd/threads

Konfiguriert die Anzahl der Threads, die NSCD verwendet. Der Standardwert ist 5. Für weitere Informationen, siehe *Name Service Cache Daemon* (Seite 53).

nss/group/cachefile/check_member

Wenn mit `true` aktiviert, prüft das Cronjob Skript zum Exportieren des lokalen Gruppen-Caches auch, ob die Gruppenmitglieder noch im LDAP-Verzeichnis vorhanden sind. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 46).

nss/group/cachefile/invalidate_interval

Legt das Intervall fest, das bestimmt, wann der lokale Gruppen-Cache als ungültig gilt und ein neuer Export durchgeführt wird. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 46).

nss/group/cachefile/invalidate_on_changes

Aktiviert oder deaktiviert den Listener, um den lokalen Gruppencache ungültig zu machen. Um den Listener zu aktivieren, setzen Sie den Wert auf `true`. Andernfalls setzen Sie den Wert auf `false`. Für weitere Informationen, siehe *Lokaler Gruppencache* (Seite 46).

nssldap/bindpolicy

Steuert die Maßnahmen, die das UCS-System ergreift, wenn der LDAP-Server nicht erreichbar ist. Siehe *Name Service Switch / LDAP-NSS-Modul* (Seite 13).

ntp/signed

Der NTP-Server antwortet mit Anfragen, die von Samba/AD signiert sind, wenn der Wert auf `yes` gesetzt ist. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 54).

office365/adconnection/wizard

Definiert den Azure AD-Verbindungsalias, der bei der nächsten Ausführung des Microsoft 365-Konfigurationsassistenten verwendet wird. Für weitere Informationen, siehe *Synchronisation von Benutzern in mehrere Azure Active Directories* (Seite 91).

office365/attributes/anonymize

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365 Connector synchronisiert, aber mit zufälligen Daten füllt. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 89).

office365/attributes/mapping/.*

Definiert eine Zuordnung von LDAP-Attributen eines Benutzerkontos für die Synchronisierung mit Azure Attributen. Die Standardeinstellungen reichen in der Regel für die meisten Umgebungsanforderungen aus. Für weitere Informationen, siehe *Benutzer* (Seite 89).

office365/attributes/never

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365-Connector nie synchronisiert, auch wenn es in *office365/attributes/sync* (Seite 164) oder *office365/attributes/anonymize* (Seite 164) erwähnt wird. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 89).

office365/attributes/static/.*

Konfiguriert LDAP-Attribute für die Synchronisierung mit vordefinierten Werten. Weitere Informationen finden Sie unter *Benutzer* (Seite 89).

office365/attributes/sync

Konfiguriert die LDAP-Attribute eines Benutzerkontos, das der Microsoft 365 Connector synchronisiert. Der Wert ist eine kommagetrennte Liste von LDAP-Attributen. Weitere Informationen finden Sie unter *Benutzer* (Seite 89).

office365/attributes/usageLocation

Legt das Standardland für den Benutzer in Microsoft 365 fest. Die Werte sind 2-Zeichen-Abkürzungen für Länder. Weitere Informationen finden Sie unter *Benutzer* (Seite 89).

office365/debug/werror

Konfigurieren Sie zusätzliche Fehlerbehebungen für den Microsoft 365 Connector. Für weitere Informationen, siehe *Fehlersuche* (Seite 91).

office365/defaultalias

Konfiguriert den Standardverbindungsalias für Microsoft 365-aktivierte Benutzer und Gruppen. Weitere Informationen finden Sie unter *Synchronisation von Benutzern in mehrere Azure Active Directories* (Seite 91).

office365/groups/sync

Aktiviert die Synchronisierung von Gruppen der Microsoft 365-Benutzer. Um Teams zu verwenden, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Teams* (Seite 90).

password/hashing/bcrypt

Aktiviert `bcrypt` als Passworthash-Methode, wenn auf `true` gesetzt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 19).

password/hashing/bcrypt/cost_factor

Definiert den `bcrypt` Kostenfaktor und ist standardmäßig auf 12 eingestellt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 19).

password/hashing/bcrypt/prefix

Definiert das Präfix `bcrypt` und ist standardmäßig auf 2b eingestellt. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 19).

password/hashing/method

Legt die Hash-Methode für die Passwort-Hashes fest. Die Voreinstellung ist `SHA-512`. Siehe *Passwort-Hashes im Verzeichnisdienst* (Seite 19).

password/quality/credit/digits

Legt die Mindestanzahl von Zeichen für ein neues Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/credit/lower

Legt die Mindestanzahl von benötigten Kleinbuchstaben im neuen Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/credit/other

Legt die Mindestanzahl der nötigen Zeichen im neuen Passwort fest, die weder Buchstaben noch Ziffern sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/credit/upper

Legt die Mindestanzahl von benötigten Großbuchstaben im neuen Passwort fest. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/forbidden/chars

Definiert die Zeichen und Ziffern, die für Passwörter nicht erlaubt sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/length/min

Legt die Mindestlänge für ein Passwort pro UCS-System für Benutzer fest, die nicht einer UDM-Passwortrichtlinie unterliegen. Der Wert `yes` wendet die Prüfungen der `python-cracklib` an. Der Wert `sufficient` beinhaltet keine `python-cracklib`-Prüfungen. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/mspolicy

Definiert die standardmäßigen Microsoft-Kennwortkomplexitätskriterien.

Die Werte `yes`, `1` oder `true` aktivieren die Standard Microsoft Passwortkomplexitätskriterien zusätzlich zu den anderen Kriterien, die mit `python-cracklib` überprüft werden.

Der Wert `sufficient` wendet nur die Standard Microsoft Passwortkomplexitätskriterien ohne `python-cracklib` an.

Der Standardwert ist nicht gesetzt und entspricht dem Wert `false`.

Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

password/quality/required/chars

Definiert einzelne Zeichen, die für Passwörter notwendig sind. Für weitere Informationen, siehe *Verwaltung der Benutzerpasswörter* (Seite 37).

pkgdb/scan

Steuert, ob ein UCS-System Installationsprozesse im Softwaremonitor speichert. Um dies zu deaktivieren, setzen Sie den Wert `no`. Für weitere Informationen, siehe *Zentrale Überwachung von Softwareinstallationsständen mit dem Software-Monitor* (Seite 34).

portal/auth-mode

Legt den Authentifizierungsmodus für das UCS-Portal fest. Setzen Sie ihn auf `saml`, wenn Sie SAML für die Single Sign-On Anmeldung aktivieren wollen. Für weitere Informationen, siehe *Anmelden* (Seite 23).

portal/default-dn

Legt den LDAP-DN des Portalobjekts fest, das die Daten für das Portal enthält. Führen Sie nach der Änderung des Variablenwerts den Befehl `univention-portal update` aus. Weitere Informationen finden Sie unter *UCS Portalseite* (Seite 24).

proxy/http

Legt den HTTP-Proxyserver auf dem UCS-Hostsystem fest. Für weitere Informationen, siehe *Konfiguration des Proxyzugriffs* (Seite 49).

proxy/https

Legt den HTTPS-Proxyserver auf dem UCS-Hostsystem fest. Für weitere Informationen, siehe *Konfiguration des Proxyzugriffs* (Seite 49).

proxy/no_proxy

Legt eine Liste von Domänen fest, die nicht über einen HTTP-Proxy verwendet werden. Die Einträge werden durch Kommas getrennt. Weitere Informationen finden Sie unter *Konfiguration des Proxyzugriffs* (Seite 49).

quota/logfile

Um die Aktivierung von Quotas in einer Datei zu protokollieren, geben Sie die Datei in dieser Variablen an. Für weitere Informationen, siehe *Auswertung von Quota bei der Anmeldung* (Seite 117).

quota/userdefault

Um die Auswertung der Benutzerquoten während der Anmeldung zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Auswertung von Quota bei der Anmeldung* (Seite 117).

radius/mac/whitelisting

Um nur bestimmten Netzwerkgeräten den Zugang zu einem Netzwerk über RADIUS zu erlauben, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *MAC-Adressfilter* (Seite 106).

radius/use-service-specific-password

Um ein spezielles Benutzerpasswort für RADIUS anstelle des Domänenpassworts zu verwenden, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Dienst-spezifisches Passwort* (Seite 104).

repository/mirror/server

Legt einen anderen Repository-Server als Quelle für den lokalen Spiegel fest. Standardwert: `updates.software-univention.de`. Für weitere Informationen, siehe *Einrichtung und Aktualisierung eines lokalen Repositories* (Seite 33).

repository/online/component/.*/unmaintained

DEPRECATED! Legt fest, wie mit nicht gewarteten Paketen aus zusätzlichen Repositories verfahren werden soll. Um dies zu aktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Konfiguration des Repository-Servers für Updates und Paketinstallationen* (Seite 32).

repository/online/server

Der Repository-Server, der verwendet wird, um nach Updates zu suchen und Pakete herunterzuladen. Standardwert: `updates.software-univention.de`. Für weitere Informationen, siehe *Konfiguration über Univention Configuration Registry* (Seite 32).

samba/enable-msdfs

Um das Microsoft Distributed File System (MSDFS) zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Samba neu. Für weitere Informationen, siehe *Unterstützung von MSDFS* (Seite 115).

samba/max/protocol

Konfiguriert das Dateidienstprotokoll, das Samba auf dem UCS verwendet. Die erlaubten Werte sind `NT1`, `SMB2` und `SMB3`. Für weitere Informationen, siehe *Dateidienste* (Seite 56).

samba/spoolss/architecture

Definiert die Systemarchitektur für den Druckspooler in Samba. Setzen Sie die Werte auf `Windows x64`, wenn Ihre Umgebung eine 64-Bit-Version von Microsoft Windows enthält. Für weitere Informationen, siehe *Einbinden von Druckerfreigaben auf Windows-Clients* (Seite 122).

samba4/sysvol/sync/cron

Legt das Zeitintervall für die Synchronisierung zwischen Samba/AD-Domänencontrollern für die SYSVOL-Freigabe fest. Der Standardwert ist fünf Minuten. Für weitere Informationen, siehe *Synchronisation der SYSVOL-Freigabe* (Seite 57).

saml/idp/entityID/supplement/[identifizier]

Aktiviert zusätzliche lokale Identitätsanbieter für SAML auf einem UCS-System, das als UCS-Identitätsanbieter dient. Zum Aktivieren setzen Sie den Wert auf `true`.

saml/idp/selfservice/check_email_verification

Steuert, ob die Single Sign-On Anmeldungen von nicht verifizierten und selbst registrierten Benutzerkonten verweigert wird. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 39).

security/packetfilter/disabled

Um Univention Firewall zu deaktivieren, setzen Sie den Wert auf `true`. Für weitere Informationen, siehe *Paketfilter mit Univention Firewall* (Seite 100).

self-service/backend-server

Definiert das UCS-System, auf dem das Backend der Anwendung **Self Service** installiert ist. Weitere Informationen finden Sie unter *Passwort-Verwaltung über Self Service App* (Seite 38).

server/password/change

Aktiviert oder deaktiviert die Passwortrotation auf einem UCS-System. Standardmäßig ist die Passwortrotation aktiviert. Für weitere Informationen, siehe *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 47).

server/password/interval

Legt das Intervall in Tagen fest, in dem das Passwort des Computerkontos neu generiert wird. Der Standardwert ist auf 21 Tage eingestellt. Weitere Informationen finden Sie unter *Verwaltung der Rechnerkonten über Univention Management Console Modul* (Seite 47).

server/role

Enthält den Namen der Serverrolle des UCS-Systems. Für weitere Informationen, siehe *UCS-Systemrollen* (Seite 11).

squid/auth/allowed_groups

Um den Zugriff auf den Squid-Webproxy zu beschränken, definieren Sie eine Liste von Gruppennamen, die durch Semikolon (;) getrennt sind. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 102).

squid/allowfrom

Konfiguriert zusätzliche Netzwerke, um den Zugriff auf den Squid-Webproxy zu ermöglichen. Trennen Sie die Einträge mit Leerzeichen und verwenden Sie die CIDR-Notation, zum Beispiel `192.0.2.0/24`. Weitere Informationen finden Sie unter *Einschränkung des Zugriffs auf erlaubte Netzwerke* (Seite 102).

squid/basicauth

Um die direkte Authentifizierung für den Squid-Webproxy gegenüber dem LDAP-Server zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 102).

squid/cache

Um die Caching-Funktion des Squid-Webproxies zu deaktivieren, setzen Sie den Wert auf `no`. Für weitere Informationen, siehe *Caching von Webseiten* (Seite 102).

squid/httpport

Konfiguriert den Port für Squid Web Proxy, an dem der Daemon auf eingehende Verbindungen wartet. Der Standardwert ist `3128`. Für weitere Informationen, siehe *Zugriffsport* (Seite 102).

squid/krb5auth

Um die Authentifizierung über Kerberos für den Squid-Webproxy zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 102).

squid/ntlmauth

Um die Authentifizierung für den Squid-Webproxy über die NTLM-Schnittstelle zu aktivieren, setzen Sie den Wert auf `yes` und starten Sie Squid neu. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 102).

squid/ntlmauth/keepalive

Um weitere NTLM-Authentifizierung für nachfolgende HTML-Anfragen an dieselbe Website zu deaktivieren, setzen Sie den Wert auf `yes`. Für weitere Informationen, siehe *Benutzer-Authentifizierung am Proxy* (Seite 102).

squid/webports

Konfiguriert die Liste der zulässigen Ports für den Squid-Webproxy. Trennen Sie die Einträge durch Leerzeichen. Für weitere Informationen, siehe *Erlaubte Ports* (Seite 102).

sshd/permitroot

Konfiguriert, wie der SSH-Daemon die Anmeldung für den Benutzer `root` erlaubt. Der Wert `without-password` fragt nicht interaktiv nach dem Passwort. Die Anmeldung erfordert den öffentlichen SSH-Schlüssel. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 54).

sshd/port

Konfigurieren Sie den Port, den der SSH-Daemon benutzt, um auf Verbindungen zu warten. Der Standardwert ist `22`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 54).

sshd/xforwarding

Legt fest, ob der SSH-Daemon X11-Weiterleitung erlaubt. Gültige Werte sind `yes` und `no`. Für weitere Informationen, siehe *SSH-Zugriff auf Systeme* (Seite 54).

ssl/validity/host

Zeichnet das Ablaufdatum des Zertifikats des lokalen Computers auf jedem UCS-System auf. Der Wert gibt die Anzahl der Tage seit dem *1. Januar 1970* an.

ssl/validity/root

Zeichnet das Ablaufdatum des Stammzertifikats auf jedem UCS-System auf. Der Wert gibt die Anzahl der Tage seit dem *1. Januar 1970* an.

ssl/validity/warning

Legt den Warnzeitraum für die Ablaufprüfung des SSL/TLS-Root-Zertifikats fest. Der Standardwert ist `30` Tage. Siehe *SSL-Zertifikatsverwaltung* (Seite 19).

system/stats

Aktiviert oder deaktiviert die Protokollierung des Systemstatus. Der Standardwert ist `yes`. Für weitere Informationen, siehe *Protokollierung des Systemzustands* (Seite 53).

system/stats/cron

Legt die Laufzeiten fest, wann `univention-system-stats` ausgeführt wird. Der Wert folgt der `cron-Syntax`³⁷⁶. Für weitere Informationen, siehe *Protokollierung des Systemzustands* (Seite 53).

³⁷⁶ <https://docs.software-univention.de/ucs-operation/5.2/de/system-administration/cron.html#cron-syntax>

timeserver

Konfiguriert den ersten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 54).

timeserver2

Konfiguriert den zweiten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 54).

timeserver3

Konfiguriert den dritten externen NTP-Zeitserver. Für weitere Informationen, siehe *Konfiguration der Zeitzone / Zeitsynchronisation* (Seite 54).

ucs/web/theme

Wählen Sie das Thema für UCS Web-Oberfläche. Der Wert entspricht einer CSS-Datei unter `/usr/share/univention-web/themes/` mit demselben Namen ohne Erweiterung für den Dateinamen.

umc/server/debug/level

Diese Variable konfiguriert den Detailgrad der Logmeldungen in `/var/log/univention/management-console-server.log`. Mögliche Werte: 0-5/99 (0: nur Fehlermeldungen bis 5: alle Debugausgaben, mit 99 werden auch sensible Daten wie Klartext-Passwörter protokolliert).

umc/module/debug/level

Der Detailgrad der Logmeldungen in `/var/log/univention/management-console-module-*`. Mögliche Werte: 0-5/99 (0: nur Fehlermeldungen bis 5: alle Debugausgaben, mit 99 werden auch sensible Daten wie Klartext-Passwörter protokolliert).

umc/self-service/account-deregistration/enabled

Um die **Self Service**-Deregistrierung zu aktivieren, setzen Sie die Variable auf `True`. Weitere Informationen finden Sie unter *Selbst-Deregistrierung* (Seite 39).

umc/self-service/account-verification/backend/enabled

Aktiviert oder deaktiviert die Kontoverifizierung und die Anforderung neuer Verifizierungstokens für den **Self Service**. Weitere Informationen finden Sie unter *Kontoverifizierung* (Seite 39).

users/default/administrator

Legt den Standardbenutzernamen für den Domänenadministrator fest. Der Wert kann während einer AD-Übernahme geändert werden. Für weitere Informationen, siehe *Domänenmigration* (Seite 81).

umc/http/session/timeout

Konfiguriert die Zeitspanne in Sekunden für die Browser-Sitzung, nach der das UCS-Managementsystem eine erneute Anmeldung verlangt. Der Standardwert ist 28800 Sekunden für 8 Stunden.

umc/web/oidc/enabled

Wenn mit `true` aktiviert, versucht UMC zuerst eine Single Sign-On Anmeldung über OpenID Connect, bevor es die normale Anmeldung verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 23).

umc/oidc/issuer

Konfiguriert den OIDC Identity Provider für die UMC OIDC Authentifizierung. Falls die Variable nicht gesetzt ist, wird der Wert `https://ucs-sso-ng.ucs.test/realms/ucs` verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 23).

umc/oidc/rp/server

Definiert den FQDN der *Relying Party* für UMC. Falls die Variable nicht gesetzt ist, wird der FQDN des UCS System verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 23).

umc/web/sso/enabled

Wenn mit `true` aktiviert, versucht UMC zuerst eine Single Sign-On Anmeldung über SAML, bevor es die normale Anmeldung verwendet. Weitere Informationen finden Sie unter *Anmelden* (Seite 23).

update/debug/level

Debug-Level für die Debug-Ausgaben in `/var/log/univention-updater.log`. Mögliche Werte sind 0-5.

16.2 Literaturverzeichnis

16.3 Stichwortverzeichnis

Das genindex bietet direkt Links zu den Inhaltsthemen. Sie enthält die Begriffe aus der Wortliste in Fettschrift.

Literaturverzeichnis

- [1] *Univention Corporate Server - Operation Manual*. Univention GmbH, 2025-2026. URL: <https://docs.software-univention.de/ucs-operation/5.2/de/>.
- [2] *UCS documentation overview*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/>.
- [3] *Nubus for Kubernetes - Architecture Manual 1.x*. Univention GmbH, 2024-2026. URL: <https://docs.software-univention.de/nubus-kubernetes-architecture/latest/en/>.
- [4] *Nubus - Customization and Modification Manual 1.x*. Univention GmbH, 2024-2026. URL: <https://docs.software-univention.de/nubus-customization/latest/en/>.
- [5] *Univention Keycloak app documentation*. Univention GmbH, 2023. URL: <https://docs.software-univention.de/keycloak-app/latest/>.
- [6] *Nubus Handbuch 1.x*. Univention GmbH, 2024-2026. URL: <https://docs.software-univention.de/nubus-manual/1.x/de/>.
- [7] *Extended Windows integration documentation*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/ext-windows/5.2/en/index.html>.
- [8] *Group Policy ADMX Syntax Reference Guide*. Microsoft, July 2021. URL: [https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753471\(v=ws.10\)?redirectedfrom=MSDN](https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc753471(v=ws.10)?redirectedfrom=MSDN).
- [9] *How to Implement the Central Store for Group Policy Admin Templates, Completely (Hint: Remove Those .ADM files!)*. Microsoft, September 2018. URL: <https://techcommunity.microsoft.com/blog/coreinfrastructureandsecurityblog/how-to-implement-the-central-store-for-group-policy-admin-templates-completely-h/255448>.
- [10] Microsoft, editor. *Windows Server 2003/2003 R2*, chapter WMI filtering using GPMC, pages 18372f. Microsoft, January 2005. URL: <https://www.microsoft.com/en-US/download/details.aspx?id=53314>.
- [11] Mark Heitbrink. *Filtern von Gruppenrichtlinien anhand von Benutzergruppen, WMI und Zielgruppenadressierung*. January 2013. URL: <https://www.gruppenrichtlinien.de/artikel/filtern-von-gruppenrichtlinien-anhand-von-benutzergruppen-wmi-und-zielgruppenadressierung/>.
- [12] *Installieren der Zertifizierungsstelle*. Microsoft, März 2023. URL: <https://learn.microsoft.com/de-de/windows-server/networking/core-network-guide/cncg/server-certs/install-the-certification-authority>.
- [13] *Univention Developer Reference*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/developer-reference/5.2/en/index.html>.
- [14] Cricket Liu and Paul Albitz. *DNS and BIND*, chapter 12 Reading BIND Debugging Output, pages 502. O'Reilly, 3rd edition, September 1998. URL: https://www.diablotin.com/librairie/networking/dnsbind/ch12_01.htm.

- [15] *Extended IP and network management documentation*. Univention GmbH. URL: <https://docs.software-univention.de/ext-networks/5.2/en/index.html>.
- [16] Jelmer R. Vernooij, John H. Terpsta and Gerald (Jerry) Carter. *The Official Samba 3.2.x HOWTO and Reference Guide*, chapter 20 - Hosting a Microsoft Distributed File System Tree, pages 381–384. Samba Project, May 2009. URL: <https://www.samba.org/samba/docs/old/Samba3-HOWTO/msdfs.html>.
- [17] *UCS performance guide*. Univention GmbH, 2021. URL: <https://docs.software-univention.de/ext-performance/5.2/en/index.html>.
- [18] *Univention OX Connector app documentation*. Univention GmbH, 2023. URL: <https://docs.software-univention.de/ox-connector-app/latest/>.

B

bonding
 network, 49
bridge
 network, 49
Bugzilla
 Bug #55247, 110

C

connector/ad/ldap/binddn, 67, 69, 72
connector/ad/ldap/bindpw, 67, 72
connector/ad/ldap/ssl, 70
connector/ad/mapping/allowsubtree/.*/[ad|ucs], 75
connector/ad/mapping/allowsubtree/.*/ad, 78
connector/ad/mapping/allowsubtree/.*/ucs, 78
connector/ad/map-ping/allow-subtree-ancestors, 78
connector/ad/mapping/group/language, 79
connector/ad/mapping/ignoresubtree/.*, 78
connector/ad/mapping/{type}/allowfilter, 78
connector/ad/mapping/{type}/ignorefilter, 78
connector/ad/mapping/{type}/ignorelist, 78
connector/ad/poll/sleep, 68
connector/ad/retryrejected, 68
cups/cups-pdf/anonymous, 121
cups/cups-pdf/cleanup/enabled, 121
cups/cups-pdf/cleanup/keep, 121, 154
cups/cups-pdf/directory, 121
cups/errorpolicy, 120
cups/include/local, 120

D

dns/allow/transfer, 97
dns/backend, 97
dns/debug/level, 96
dns/dlz/debug/level, 96

E

Errata updates
 UCS 5.0 erratum 1011, 107, 156
 UCS 5.0 erratum 1060, 89
 UCS 5.2 erratum 298, 40

F

fetchmail/autostart, 131
freeradius/auth/helper/ntlm/debug, 110
freeradius/conf/allow-mac-address-authentication, 106
freeradius/conf/mac-addr-regexp, 108
freeradius/conf/tls-max-version, 110
freeradius/vlan-id, 107, 110

G

google-apps/attributes/anonymize, 92, 93, 157
google-apps/attributes/mapping/.*, 92, 93, 157
google-apps/attributes/never, 93
google-apps/debug/werror, 93
google-apps/groups/sync, 93
groups/default/domainadmins, 83

H

hostname, 6
 allowed characters, 6
 Create new UCS domain, 6
 Join existing Active Directory domain, 6
 Join existing UCS domain, 6
 length, 6
 naming convention, 6

K

Knowledge Base
 KB 32, 57
 KB 6701, 23

L

ldap/database/internal/acl/block-lists/groups/read, 40

ldap/database/internal/acl/block-
lists/groups/write, 40
ldap/database/internal/over-
lay/dds/max-ttl, 41
ldap/database/internal/over-
lay/dds/min-ttl, 41
ldap/logging/exclude1, 159
ldap/master, 17
listener/module/recyclebin/deactivate, 41

M

mail/antispam/bodysizelimit, 129
mail/antispam/learneddaily, 130
mail/antispam/requiredhits, 129
mail/antivir, 130
mail/antivir/spam, 130
mail/archivefolder, 134
mail/dovecot/folder/ham, 130
mail/dovecot/folder/Spam, 129
mail/dovecot/imap, 127
mail/dovecot/limits, 137
mail/dovecot/limits/default_client_limit,
137
mail/dovecot/location/separate_index, 136
mail/dovecot/mailbox/delete, 136
mail/dovecot/mailbox/rename, 135
mail/dovecot/pop3, 127
mail/dovecot/process/dotlock_use_excl, 136
mail/dovecot/process/lock_method, 137
mail/dovecot/process/mail_fsyc, 136
mail/dovecot/process/mail_nfs_index, 137
mail/dovecot/process/mail_nfs_storage, 137
mail/dovecot/process/mmap_disable, 136
mail/dovecot/quota/warning/subject, 129
mail/dovecot/quota/warning/text, 129
mail/dovecot/quota/warning/text/80, 129
mail/dovecot/quota/warning/text/95, 129
mail/messagesizelimit, 133
mail/postfix/mastercf/opti-
ons/smtp/smtpd_sasl_auth_enable,
134
mail/postfix/postscreen/, 134
mail/postfix/postscreen/enabled, 134
mail/postfix/smtpd/restrictions/recipient,
130
mail/postfix/softbounce, 134
mail/postfix/tls/client/level, 133
mail/relayauth, 133
mail/relayhost, 132, 133
monitoring/dns/lookup-domain, 145

N

nats/stunnel/accept/port, 16, 18
network
802.1q, 49
bonding, 49
bridge, 49
etherchannel, 49

link aggregation, 49
switch, 49
teaming, 49
trunking, 49
vlan, 49

O

office365/adconnection/wizard, 91
office365/attributes/anonymize, 89, 164
office365/attributes/mapping/.*, 89
office365/attributes/never, 89
office365/attributes/static/.*, 89
office365/attributes/sync, 89, 164
office365/attributes/usageLocation, 89
office365/debug/werror, 92
office365/defaultalias, 91
office365/groups/sync, 89, 90

P

password/quality/credit/digits, 104
password/quality/credit/lower, 104
password/quality/credit/other, 104
password/quality/credit/upper, 104
password/quality/forbidden/chars, 104
password/quality/length/min, 104

Q

quota/logfile, 117
quota/userdefault, 117

R

radius/mac/whitelisting, 106, 107
radius/use-service-specific-password, 104
RFC
RFC 3580, 110

S

samba/enable-msdfs, 115
samba/max/protocol, 56
samba/spoolss/architecture, 122
samba4/sysvol/sync/cron, 57
security/packetfilter/disabled, 101
squid/allowfrom, 102
squid/auth/allowed_groups, 103
squid/basicauth, 103
squid/cache, 102
squid/httpport, 102
squid/krb5auth, 103
squid/ntlmauth, 103
squid/ntlmauth/keepalive, 103
squid/webports, 102

U

umc/self-service/service-specific-passwords/backend/en-
104
Umgebungsvariable
appcenter/update/skip-zsync, 153

- appcenter/update/zsync-timeout, 153
- auth/faillog, 153
- auth/faillog/limit, 153
- auth/faillog/lock_global, 153
- auth/faillog/root, 153
- auth/faillog/unlock_time, 153
- auth/sshd/user/root, 153
- backup/clean/max_age, 153
- connector/ad/ldap/binddn, 67, 69, 72, 154
- connector/ad/ldap/bindpw, 67, 72, 154
- connector/ad/ldap/ssl, 70, 154
- connector/ad/mapping/allowsubtree/.*/[ad|ucs], 75
- connector/ad/mapping/allowsubtree/.*/ad, 75, 78
- connector/ad/mapping/allowsubtree/.*/ucs, 74, 78
- connector/ad/mapping/allow-subtree-ancestors, 75, 78
- connector/ad/mapping/group/language, 79, 154
- connector/ad/mapping/ignoresubtree/.*, 76, 78
- connector/ad/mapping/{type}/allowfilter, 76, 78
- connector/ad/mapping/{type}/ignorefilter, 77, 78
- connector/ad/mapping/{type}/ignorelist, 77, 78
- connector/ad/poll/sleep, 68, 154
- connector/ad/retryrejected, 68, 154
- connector/debug/level, 154
- connector/debug/udm/level, 154
- cups/cups-pdf/anonymous, 121, 154
- cups/cups-pdf/cleanup/enabled, 121, 154
- cups/cups-pdf/cleanup/keep, 121, 154
- cups/cups-pdf/directory, 121, 154
- cups/errorpolicy, 120, 154
- cups/include/local, 120, 155
- cups/server, 155
- directory/manager/blocklist/cleanup/cron, 155
- directory/manager/blocklist/enabled, 155
- directory/manager/cmd/debug/level, 155
- directory/manager/rest/debug/level, 155
- directory/manager/templates/alpha-num/whitelist, 155
- directory/manager/user_group/uniqueness, 155
- directory/manager/web/modules/computers/computer/wizard/disabled, 155
- directory/manager/web/modules/groups/group/checks/circular_dependency, 155
- directory/manager/web/modules/users/user/wizard/disabled, 155
- directory/reports/logo, 155
- dns/allow/transfer, 97, 155
- dns/backend, 97, 155
- dns/debug/level, 96, 156
- dns/dlz/debug/level, 96, 156
- dns/forwarder1, 156
- dns/forwarder2, 156
- dns/forwarder3, 156
- fetchmail/autostart, 131, 156
- freeradius/auth/helper/ntlm/debug, 110, 156
- freeradius/conf/allow-mac-address-authentication, 106, 156
- freeradius/conf/mac-addr-regexp, 108, 156
- freeradius/conf/tls-max-version, 110
- freeradius/conf/tls-max-version, 156
- freeradius/vlan-id, 107, 110, 156
- gateway, 156
- google-apps/attributes/anonymize, 92, 93, 157
- google-apps/attributes/mapping/.*, 92, 93, 157
- google-apps/attributes/never, 93, 157
- google-apps/debug/werror, 93, 157
- google-apps/groups/sync, 93, 157
- groups/default/domainadmins, 83, 157
- grub/append, 157
- grub/bootsplash, 157
- grub/gfxmode, 157
- grub/timeout, 157
- grub/xenhopt, 157
- interfaces/ethX/address, 157
- interfaces/ethX/ipv6/acceptRA, 158
- interfaces/ethX/ipv6/address, 158
- interfaces/ethX/ipv6/prefix, 158
- interfaces/ethX/netmask, 157
- interfaces/ethX/type, 157
- interfaces/ethX_Y/setting, 158
- ipv6/gateway, 158
- kerberos/adminserver, 158
- kerberos/kdc, 158
- kerberos/realm, 158
- kernel/blacklist, 158
- kernel/modules, 158
- ldap/acl/nestedgroups, 159
- ldap/acl/read/anonymous, 158
- ldap/acl/read/ips, 159
- ldap/acl/user/passwordreset/accesslist/groups/dn, 159
- ldap/acl/user/passwordreset/attributes, 159
- ldap/acl/user/passwordreset/protected/gid, 159

- ldap/acl/user/passwordreset/protected/uid, 159
- ldap/authz-regexp/federated-accounts, 158
- ldap/authz-regexp/users, 158
- ldap/database/internal/acl/blocklists/groups/read, 40, 158
- ldap/database/internal/acl/blocklists/groups/write, 40, 158
- ldap/database/internal/overlay/dds/max-ttl, 41, 42
- ldap/database/internal/overlay/dds/min-ttl, 41, 42
- ldap/idletimeout, 159
- ldap/logging/exclude1, 159
- ldap/logging/excludeN, 159
- ldap/logging/id-prefix, 159
- ldap/master, 17, 159
- ldap/overlay/lastbind, 159
- ldap/overlay/lastbind/precision, 159
- ldap/policy/cron, 159
- ldap/ppolicy/enabled, 160
- ldap/pw-bcrypt, 160
- ldap/server/addition, 160
- ldap/server/name, 160
- listener/debug/level, 160
- listener/module/recyclebin/deactivate, 41, 42
- listener/shares/rename, 160
- local/repository, 160
- log/rotate/weeks, 160
- logrotate/compress, 160
- logrotate/rotates, 160
- machine/password/length, 160
- mail/antispam/bodysizelimit, 129, 160
- mail/antispam/learndaily, 130, 160
- mail/antispam/requiredhits, 129, 160
- mail/antivir, 130, 160
- mail/antivir/spam, 130, 161
- mail/archivefolder, 134, 161
- mail/dovecot/auth/cache_negative_ttl, 161
- mail/dovecot/auth/cache_ttl, 161
- mail/dovecot/folder/ham, 130, 161
- mail/dovecot/folder/Spam, 129, 161
- mail/dovecot/imap, 127, 161
- mail/dovecot/limits, 137, 161
- mail/dovecot/limits/default_client_limit, 137
- mail/dovecot/location/separate_index, 136, 161
- mail/dovecot/mailbox/delete, 136, 161
- mail/dovecot/mailbox/rename, 135, 161
- mail/dovecot/pop3, 127, 161
- mail/dovecot/process/dotlock_use_excl, 136, 162
- mail/dovecot/process/lock_method, 137, 161
- mail/dovecot/process/mail_fsyc, 136, 162
- mail/dovecot/process/mail_nfs_index, 137, 162
- mail/dovecot/process/mail_nfs_storage, 137, 162
- mail/dovecot/process/mmap_disable, 136, 162
- mail/dovecot/quota/warning/subject, 129, 162
- mail/dovecot/quota/warning/text, 129, 162
- mail/dovecot/quota/warning/text/80, 129
- mail/dovecot/quota/warning/text/95, 129
- mail/hosteddomains, 162
- mail/messagesizelimit, 133, 162
- mail/postfix/mastercf/options/smtp/smtpd_sasl_auth_enable, 134, 162
- mail/postfix/policy/listfilter, 162
- mail/postfix/postscreen/, 134, 162
- mail/postfix/postscreen/enabled, 134, 162
- mail/postfix/smtpd/restrictions/recipient, 130, 162
- mail/postfix/softbounce, 134, 163
- mail/postfix/tls/client/level, 133, 163
- mail/relayauth, 133, 163
- mail/relayhost, 132, 133, 163
- monitoring/dns/lookup-domain, 145
- nameserver1, 163
- nameserver2, 163
- nameserver3, 163
- nats/max_reconnect_attempts, 17
- nats/max_retry_count, 17
- nats/retry_delay, 17
- nats/stunnel/accept/port, 16, 18
- nats/stunnel/cacert, 18
- nats/stunnel/cert, 18
- nats/stunnel/connect/port, 18
- nats/stunnel/key, 18
- notifier/debug/level, 163
- nscd/debug/level, 163
- nscd/hosts/maxdbsize, 163
- nscd/hosts/positive_time_to_live, 163
- nscd/threads, 163
- nss/group/cachefile/check_member, 163
- nss/group/cachefile/invalidate_inter-val, 164
- nss/group/cachefile/invalidate_on_changes, 164
- nssldap/bindpolicy, 164
- ntp/signed, 164
- office365/adconnection/wizard, 91, 164
- office365/attributes/anonymize, 89, 164
- office365/attributes/mapping/*.*, 89, 164

office365/attributes/never, 89, 164
office365/attributes/static/.*, 89, 164
office365/attributes/sync, 89, 164
office365/attributes/usageLocation, 89, 164
office365/debug/werror, 92, 164
office365/defaultalias, 91, 164
office365/groups/sync, 89, 90, 165
password/hashing/bcrypt, 165
password/hashing/bcrypt/cost_factor, 165
password/hashing/bcrypt/prefix, 165
password/hashing/method, 165
password/quality/credit/digits, 104, 165
password/quality/credit/lower, 104, 165
password/quality/credit/other, 104, 165
password/quality/credit/upper, 104, 165
password/quality/forbidden/chars, 104, 165
password/quality/length/min, 104, 165
password/quality/mspolicy, 165
password/quality/required/chars, 165
pkgdb/scan, 166
portal/auth-mode, 166
portal/default-dn, 166
provisioning-service/primary, 17
provisioning-service/udm-rest-api-host, 17
proxy/http, 166
proxy/https, 166
proxy/no_proxy, 166
quota/logfile, 117, 166
quota/userdefault, 117, 166
radius/mac/whitelisting, 106, 107, 166
radius/use-service-specific-password, 104, 166
repository/mirror/server, 166
repository/online/component/./unmaintained, 166
repository/online/server, 166
samba/enable-msdfs, 115, 166
samba/max/protocol, 56, 167
samba/spoolss/architecture, 122, 167
samba4/sysvol/sync/cron, 57, 167
saml/idp/entityID/supplement/[identifier], 167
saml/idp/selfservice/check_email_verification, 167
security/packetfilter/disabled, 101, 167
self-service/backend-server, 167
server/password/change, 167
server/password/interval, 167
server/role, 167
squid/allowfrom, 102, 167
squid/auth/allowed_groups, 103, 167
squid/basicauth, 103, 167
squid/cache, 102, 168
squid/httpport, 102, 168

squid/krb5auth, 103, 168
squid/ntlmauth, 103, 168
squid/ntlmauth/keepalive, 103, 168
squid/webports, 102, 168
sshd/permitroot, 168
sshd/port, 168
sshd/xforwarding, 168
ssl/validity/host, 168
ssl/validity/root, 168
ssl/validity/warning, 168
system/stats, 168
system/stats/cron, 168
timeserver, 168
timeserver2, 169
timeserver3, 169
ucs/web/theme, 169
umc/http/session/timeout, 169
umc/module/debug/level, 169
umc/oidc/issuer, 169
umc/oidc/rp/server, 169
umc/self- ser-
 vice/service-specific-passwords/backend/enabled, 104
umc/self-service/account-deregistration/enabled, 169
umc/self-service/account-verification/backend/enabled, 169
umc/server/debug/level, 169
umc/web/oidc/enabled, 169
umc/web/sso/enabled, 169
update/debug/level, 169
users/default/administrator, 83, 169
users/default/administrator, 83

V

vlan
 network, 49