univention
be open.

# Szenarien zum Einsatz von UCS@school - Organisation und Aufbau zentral verwalteter IT-Infrastrukturen für Schulen

***Release 5.0***

**05.09.2022**

# Inhalt

UCS@school bietet die ideale Lösung, um eine zentral verwaltete IT-Infrastruktur mit einem einheitlichen Identity-Management aufzubauen. Weitere IT-Dienste können integriert und anschließend zentral über das UCS Management verwaltet und schulübergreifend für den Zugriff über unterschiedlichste Geräte zur Verfügung gestellt werden. Damit werden Schulträger und Ministerien in die Lage versetzt, aktuelle Anforderungen aus Medienentwicklungsplänen und von Schulen effizient und sicher zu erfüllen.

Mit diesem Dokument möchten wir Ihnen eine Anleitung an die Hand geben, um typische Szenarien für den Einsatz von UCS@school effizient aufzubauen. Wir greifen dabei auf langjährige Erfahrungen zurück, die Univention in diversen Projekten mit Schulträgern beim erfolgreichen Einsatz von UCS@school gewonnen hat.

Mit diesem Dokument möchten wir Ihnen einen kurzen Überblick über vier typische IT-Szenarien für Bundesländer, Schulträger und Schulen geben:

- Bildungsclouds
- Zentrales schulisches WLAN
- Zentral verwaltete schulische IT-Infrastruktur
- Schulische IT-Infrastruktur ohne dezentrale Schulserver

Außerdem finden Sie einige Tipps, welche Punkte nach unserer Erfahrung Schlüsselfaktoren für eine erfolgreiche Projektabwicklung, Rollout und Betrieb einer Infrastruktur in Schulen darstellen. Und wir haben eine Checkliste mit wichtigen Fragen zusammengestellt, mit denen Sie sich vor dem Projektbeginn beschäftigen sollten.

Für den Einstieg in das Dokument sind *Szenarien* (Seite 3) und *Checklisten: Organisatorisch und technisch* (Seite 9) vorgesehen. Die Kapitel geben einen Überblick zu den üblichen Einsatzszenarien und bieten Checklisten mit Fragen, deren Beantwortung die Einführung von UCS@school erleichtert. Die Checklisten verweisen darüber hinaus auf die weiterführenden technischen Themen in diesem Dokument, die erprobte Lösungen aus der Praxis aufzeigen.

Die Kapitel *Checklisten: Organisatorisch und technisch* (Seite 9) geben einen Überblick zu üblichen Einsatzszenarien von UCS@school (Bildungscloud, Zentrales schulisches WLAN, zentrales Management, schulische IT-Infrastruktur ohne Schulserver) und bieten Checklisten mit Fragen, anhand derer Sie einfach überprüfen können, ob Sie bereits die notwendigen Voraussetzungen für die Einführung von UCS@school erfüllen oder ob Sie in bestimmten Bereichen noch Bedingungen erfüllen müssen. Die Checklisten verweisen darüber hinaus auch auf weiterführende technische Themen, die in diesem Dokument vorgestellt werden und die erprobte Lösungen aus der Praxis aufzeigen.

KAPITEL 1

# Szenarien

In diesem Kapitel beschreiben wir Ihnen Szenarien, in denen UCS@school häufig eingesetzt wird. In diesem Dokument sind diese Szenarien in ihrem Umfang klar voneinander abgegrenzt. In der Praxis ist diese strikte Trennung nur selten der Fall und es treten in der Regel gemischte Formen auf. Die Umsetzung eines bestimmten in diesem Papier beschriebenen Szenarios schließt somit nicht aus, dass Sie im Laufe der Zeit weitere Szenarien auf Basis der bestehenden Umgebung umsetzen können.

## 1.1 Servicestufen: UCS@school

Univention bietet für die Szenarien 1 bis 4 unterschiedliche Servicestufen für die Unterstützung in Projekten an. Kunden entscheiden beim Kauf von UCS@school, welche Servicestufe für Sie in der aktuellen Situation am passendsten ist. Ein Wechsel auf eine andere Servicestufe ist jederzeit möglich. Voraussetzung in allen Servicestufen ist das Vorhandensein eines User Helpdesks, der die Supportanfragen aus den Schulen entgegen nimmt und die weitere Bearbeitung einleitet.

Welche Servicestufen gibt es?

A. **Software und Support**: Univention liefert Software und Support, der Kunde kümmert sich selbst um Betrieb, Updates und Backup.

B. **Betrieb im Rechenzentrum des Kunden**: Univention liefert Software und Support und übernimmt Betrieb, Updates und Backup im Rechenzentrum des Kunden.

C. **UCS@school as a Service**: Univention liefert Software und Support und übernimmt Betrieb, Updates und Backup im eigenen Rechenzentrum. Kunden können sofort starten, ohne Investitionen in Hardware oder Software tätigen zu müssen.

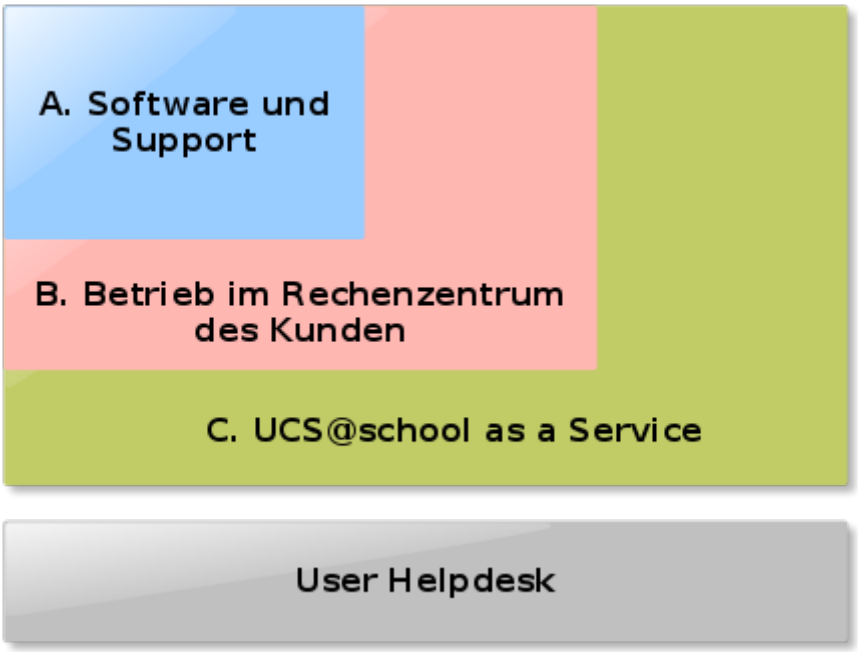


Abb. 1.1: Servicestufen: UCS@school

## 1.2 Szenario 1: Bildungscloud

Dieses Szenario ermöglicht es Schulträgern und Ministerien, eine effiziente Bildungscloud für ihre Schulen aufzubauen. Die Instanzen von Univention Corporate Server werden zentral in einem Rechenzentrum betrieben und stellen das Identity- und Access-Management zur Verfügung. An dieses werden unterschiedliche IT-Angebote angebunden, die von den Schulen benötigt werden. Zum Beispiel E-Mail und Groupware-Lösungen oder Lernmanagement-Systeme.

Lehrkräfte und Schüler*innen können alle angeschlossenen Angebote mit einem einzigen persönlichen Benutzerkonto und Passwort nutzen. Die Angebote können dabei sowohl vor Ort in den Schulen als auch von unterwegs oder von zu Hause genutzte werden.

Merkmale:

- Unabhängigkeit von der jeweiligen IT-Ausstattung der Schulen
- Bereitstellung orts- und zeitunabhängiger IT-Angebote für Lehrkräfte und Schüler*innen
- Effizienter Betrieb durch zentrale Administration
- Integration beliebiger IT-Angebote oder vorkonfigurierter Angebote aus dem Univention App Center
- Senkung des Aufkommens im Helpdesk durch Self-Service für vergessene Passwörter

## 1.3 Szenario 2: Zentrales schulisches WLAN

Dieses Szenario ermöglicht es Schulträgern, den Zugang zum WLAN in ihren Schulen zentral zu steuern und den Zugang nur bekannten Lehrkräften und Schüler*innen zu gewähren. Dazu wird Univention Corporate Server zentral in einem Rechenzentrum betrieben und dient als Identity- und Access-Management.

Die Schulen sind mit diesem Rechenzentrum beispielsweise mittels eines VPN-Zugangs verbunden. In den Schulen werden WLAN Access Points installiert, die RADIUS unterstützen (WPA2-Enterprise / IEEE 802.1X).

Ergänzend können auch wie in Szenario 1 weitere IT-Angebote an die zentralen Systeme angebunden werden.

Merkmale:

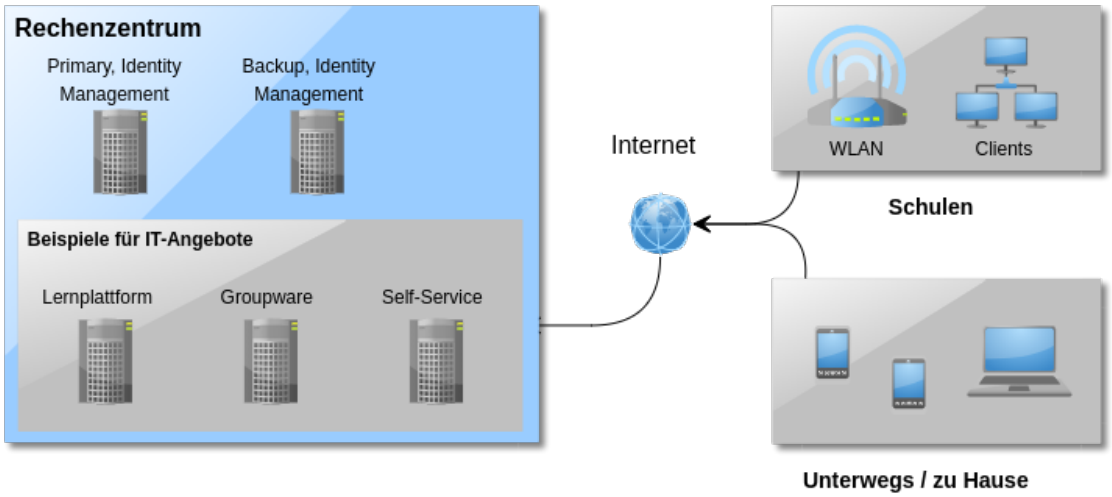


Abb. 1.2: Zentrales Identity-Management mit integrierten IT-Angeboten

- Unabhängigkeit von Schulserver-Lösungen in den Schulen
- Geringe zusätzliche Anforderungen an die Bandbreite der Schule
- Absicherung des WLAN-Zugangs durch Verwendung persönlicher Zugangsdaten für Lehrkräfte und Schüler
- Effizienter Betrieb durch zentrale Administration
- Integration beliebiger IT-Angebote oder vorkonfigurierter Angebote aus dem Univention App Center

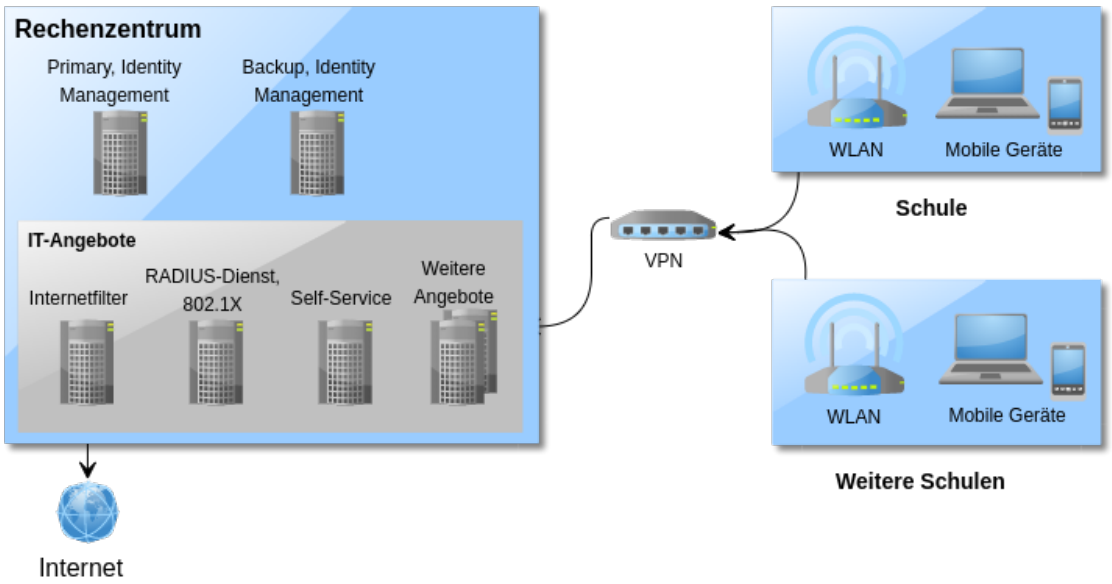


Abb. 1.3: Zentrales Identity-Management, WLAN und weitere IT-Angebote für Schulen

## 1.4 Szenario 3: Zentral verwaltete schulische IT-Infrastruktur

Dieses Szenario ermöglicht es Schulträgern, die gesamte IT-Infrastruktur ihrer Schulen zentral zu verwalten und pädagogische Funktionen dezentral in den Schulen bereitzustellen. Dazu ergänzt es die in *Szenario 2* (Seite 4) beschriebene WLAN Lösung um an den Schulen betriebene Schulserver. Diese stellen vor Ort die benötigten Infrastruktur-Dienste wie DHCP, DNS, Active Directory kompatible Domäne, Dateifreigaben, Proxy, aber auch pädagogische Funktionen wie Computerraumsteuerung, Klassenarbeitsmodus, Passwörter zurücksetzen und Softwareverteilung bereit.

Merkmale:

- Vollständige Bereitstellung der IT-Infrastruktur in den Schulen
- Unabhängigkeit der Schule gegenüber Ausfällen des Internetzugangs/VPNs
- Effizienter Betrieb durch zentrale Administration
- Integration beliebiger IT-Angebote oder vorkonfigurierter Angebote aus dem Univention App Center

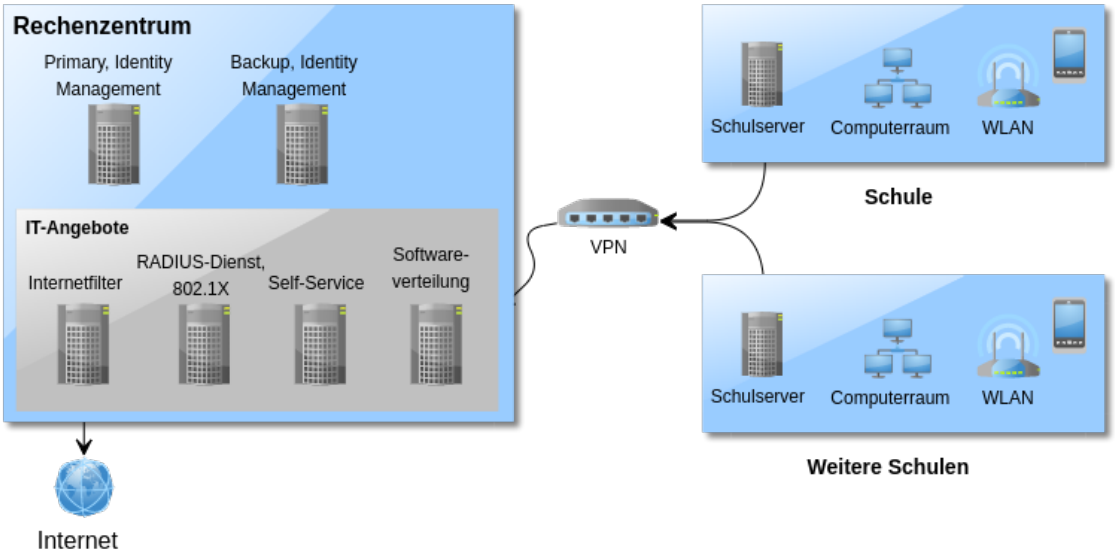


Abb. 1.4: Zentral verwaltete schulische IT-Infrastruktur mit Schulservern an den Schulen

## 1.5 Szenario 4: Schulische IT-Infrastruktur ohne dezentrale Schulserver

Dieses Szenario ermöglicht es Schulträgern, die gesamte IT-Infrastruktur ihrer Schulen zentral zu verwalten, wie in *Szenario 3* (Seite 6) beschrieben, mit der Ergänzung, dass die Schulserver nicht in den Schulen, sondern im Rechenzentrum betrieben werden.

Voraussetzung ist eine sehr gute und zuverlässige Anbindung der Schulen an dieses Rechenzentrum. Durch die Verlagerung der Schulserver ins Rechenzentrum können die Hardware-Ressourcen effizienter verwendet werden und gleichzeitig reduzieren sich die Kosten für die Wartung.

Merkmale:

- Vollständige Bereitstellung der IT-Infrastruktur in den Schulen
- Abhängigkeit der Schule gegenüber Ausfällen des Internetzugangs/VPNs
- Effizienter Betrieb durch zentrale Administration und bessere Ressourcennutzung

- Effiziente Wartung durch einfacheren Zugang zu den Systemen
- Integration beliebiger IT-Angebote oder vorkonfigurierter Angebote aus dem Univention App Center

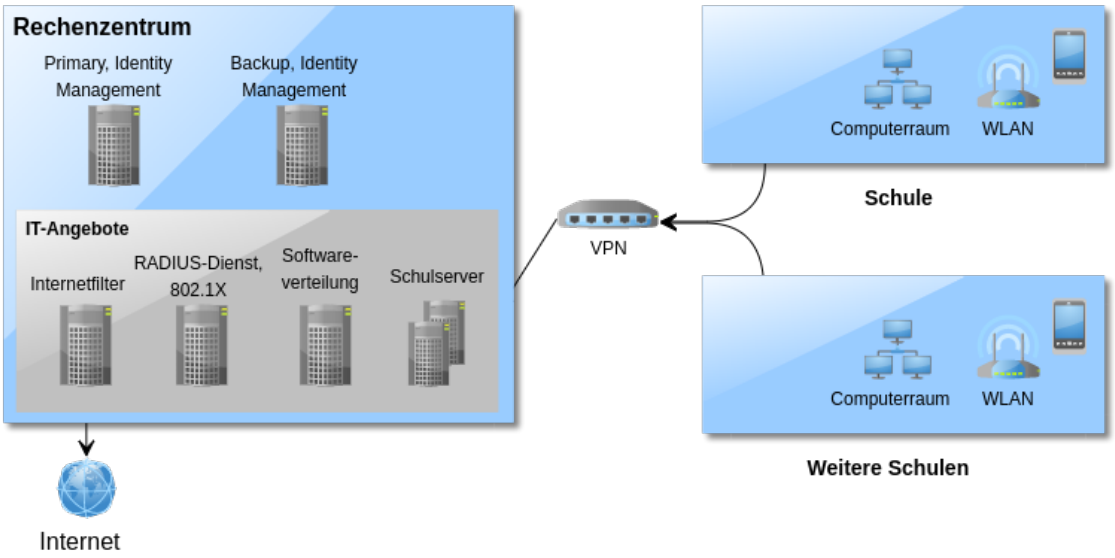


Abb. 1.5: Zentral verwaltete schulische IT-Infrastruktur ohne dezentrale Schulserver

KAPITEL 2

# Checklisten: Organisatorisch und technisch

Im Folgenden haben wir einige Fragen zusammengestellt, über die Sie sich direkt am Anfang der Projektplanung Gedanken machen sollten.

## 2.1 Organisation

- Welches Szenario soll umgesetzt werden? Siehe *Szenarien* (Seite 3).
- Wer ist Betreiber der Gesamtinfrastruktur?
- Verfügt der Betreiber über das erforderliche Wissen? Siehe *Initialer Workshop* (Seite 13).
- Wie werden Schulen über die Einführung der neuen IT-Infrastruktur informiert? Siehe *Informationsveranstaltung für die Schulen* (Seite 13).
- Wer baut in den Schulen Server, Rechner und Drucker auf und tauscht diese im Fehlerfall aus?
- In welcher Reihenfolge erfolgt der Rollout an den Schulen (nicht in allen Szenarien notwendig)? Siehe *Planung des Rollout* (Seite 13).
- In welchem zeitlichen Rahmen soll der Rollout der Pilot-Installation und später der Gesamtinfrastruktur erfolgen?
- Welche administrativen Aufgaben sollen durch die Schulen übernommen werden, zum Beispiel Passwörter zurücksetzen?
- Wie werden Schulen mit den neuen Lösungen w.z.B. UCS@school vertraut gemacht? Siehe *Schulung der Lehrkräfte* (Seite 14).
- Wie und bei wem melden Schulen Probleme? Siehe *Support-Kanäle* (Seite 22).
- Wie wird die Qualität des erbrachten IT-Angebots gemessen? Welches sind die entscheidenden Parameter, um dies zu messen?
- Wie wird sichergestellt, dass die zukünftigen Anforderungen der Schulen erfasst und von der Gesamtinfrastruktur erfüllt werden?
- Wer ist verantwortlich für die Pflege von Informationen in der Schulverwaltungssoftware und wie können diese Daten importiert werden?

## 2.2 Zentral bereitgestellte IT-Angebote

- Wo werden die zentralen Server betrieben? Siehe *Zentrale Server* (Seite 23).
- Nach welchen Konzepten wird die Gesamtinfrastruktur betrieben, insbesondere Netzkonzept, sowie Namenskonzepte für Benutzer und Rechner? Siehe *Konzeptionelle Voraussetzungen* (Seite 15).
- Wie wird die Aufrechterhaltung des Betriebs sichergestellt, zum Beispiel Monitoring, Datensicherung und Notfallpläne? Siehe *Installation eines zentralen Managed Node für Monitoring* (Seite 31) und *Datensicherung und Wiederherstellung* (Seite 21).
- Wer führt die initiale Installation und Einrichtung durch?
  - Installation der UCS Systeme mit der App **`UCS@school`**, siehe *Installation* (Seite 29).
  - Welche Basiskonfigurationen sollen vorgenommen werden? Siehe *Basiskonfiguration* (Seite 33).
  - Wie erfolgt der Import von Benutzer-, Rechner- und Netzdaten? Siehe *Datenimport* (Seite 37).
- Welche VPN-Lösung wird eingesetzt (nicht in allen Szenarien notwendig)? Siehe *Verbindung zur Zentrale* (Seite 27).
- Welche über die Basis IT-Infrastruktur hinausgehenden Angebote und Einstellungen sollen angeboten werden? Wie werden die über das Internet zugänglichen zentralen Angebote vor unerwünschtem Zugriff geschützt?
- Soll die Schulen zukünftig über einen zentralen Proxy auf das Internet zugreifen?
- Wie erfolgt der Zugriff auf zentral bereitgestellte Webdienste (Portal, Self-Service …) aus dem Internet?
  - Stellt der Rechenzentrumsbetreiber *Load Balancer* und *Reverse Proxy* als Dienst bereit?
  - Welche externen Domänennamen sollen für den Zugriff auf die Webdienste verwendet werden?
  - Ist sichergestellt, dass zu den Domänennamen passende SSL/TLS Zertifikate vorhanden sind und diese regelmäßig erneuert werden?

## 2.3 Dezentral an den Schulen bereitgestellte IT-Angebote

- Wer ist lokaler Ansprechpartner für die IT-Infrastruktur in der Schule?
- Setzt die Schule bereits eine Schulserver-Lösung ein? Welche Funktionen sind der Schule wichtig?
- Wie schnell und stabil ist der Internetzugang der Schule? Siehe *Internetzugang* (Seite 26).
- Wer betreibt den Internetzugang und ist für die Entstörung zuständig?
- Welche aktiven und passiven Netzkomponenten sind im Einsatz, zum Beispiel DSL-Router/Switches/Access Points, und wer kennt die Zugangsdaten?
- Welches IP-Netz wird aktuell in der Schule verwendet? Welche Komponenten müssen angepasst werden, um das Netzkonzept (siehe *Zentral bereitgestellte IT-Angebote* (Seite 10)) umzusetzen?
- Ist in der Schule strukturierte Verkabelung in allen Computerräumen vorhanden? Siehe *Strukturierte Verkabelung* (Seite 25). Wie sind die Patchfelder und Netzdosen belegt?
- Welche Bauarbeiten und Beschaffungen müssen vorgenommen werden, um die Betriebsbereitschaft für die Schule herzustellen?
- Kann mit dem verfügbaren Internetzugang ein VPN betrieben werden (nicht in allen Szenarien notwendig)? Siehe *Verbindung zur Zentrale* (Seite 27).

## 2.4 WLAN und BYOD

- Kann mit dem verfügbaren Internetzugang ein VPN betrieben werden?
- Sind professionelle Access Points vorhanden, die VLANs, mehrere SSIDs sowie RADIUS bzw. IEEE 802.1X unterstützen?
- Wie können die Access Points zentral konfiguriert werden? Ist eine Management Software oder ein WLAN-Controller vorhanden?
- Wo wird der RADIUS-Service betrieben?
- Wie greifen die mobilen Geräte auf das Internet zu, zum Beispiel direkt oder über einen transparenten Proxy?
- Wie hoch sind die notwendigen Investitionen, um die Betriebsbereitschaft für das WLAN herzustellen?
- Welche IT-Angebote, zentral und dezentral, sollen von den Geräten im WLAN verwendet werden können?

KAPITEL 3

# Vorbereitende Maßnahmen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien

In vergangenen Projekten haben sich folgende Schritte bewährt.

## 3.1 Initialer Workshop

Ziel des Workshops ist es die existierenden Konzepte auf die konkrete Umsetzung abzubilden. Dabei hat es sich bewährt, auf Erfahrungen und Vorgehensweisen aufzubauen, die unter anderem auch in diesem Dokument erfasst sind. Im Rahmen des Workshops sollten direkt die zentralen Systeme und eine Demo-Schule installiert werden, die in der folgenden Zeit als Referenz und Test- bzw. Demo-Umgebung verwendet werden kann.

## 3.2 Informationsveranstaltung für die Schulen

Ziel der Informationsveranstaltung ist es, die Lehrkräfte in den Schulen mit in den Prozess der Einführung der neuen IT-Infrastruktur zu involvieren. Eine bereits installierte Demo-Schule kann dazu dienen, das System initial zu präsentieren. Es hat sich in vielen Projekten gezeigt, dass solche Informationsveranstaltungen auch nach dem Rollout regelmäßig stattfinden sollten, um neue Anforderungen und Feedback aufzunehmen.

## 3.3 Planung des Rollout

Ziel ist es, den Rollout der IT-Infrastruktur mit erfolgreichen Meilensteinen zu beginnen. Dafür gilt es, die am besten geeigneten Schulen zu identifizieren und diese als erste auszustatten. In vielen Projekten haben wir die Erfahrung gemacht, dass Schulen, die die folgenden Kriterien erfüllen, besonders gut für den Start geeignet sind:

- Überschaubare, gut ausgebaute IT-Infrastruktur
- Konkreter Bedarf nach einer Lösung
- Geringer Migrationsaufwand von bestehenden Lösungen

- Wenige Sonderfälle
- Motivierte Schulleitung und IT-Verantwortliche an der Schule

Sind diese Schulen erfolgreich ausgestattet worden, so können sie als Referenz für anderen Schulen dienen. Schrittweise können nun komplexere Umgebungen ausgerollt werden.

## 3.4 Schulung der Lehrkräfte

Die Lehrkräfte sollten im Umgang mit den Rechnern, den pädagogischen Funktionen und den weiteren Webdiensten der in der Schule genutzten Anwendungen geschult werden. Auch dazu sollten wiederkehrende Termine angeboten werden.

KAPITEL 4

# Konzeptionelle Voraussetzungen

Die folgenden Empfehlungen bauen auf Erfahrungen auf, die sich in diversen Projekten bewährt haben. Nicht alle sind zwingend umzusetzen und Abweichungen sind jederzeit möglich.

## 4.1 Netzkonzept

**Gültigkeit**

Für die Szenarien *2* (Seite 4), *3* (Seite 6) und *4* (Seite 6).

In UCS@school wird für jede Schule mindestens ein Subnetz benötigt, sobald an den Schulen Endgeräte eingesetzt werden sollen. Abhängig vom Szenario kann eine einzelne Schule auch mehr als ein Subnetz erhalten.

Für den Aufbau einer Umgebung mit mehreren Schulen empfehlen wir die Verwendung des privaten Netzes `10.0.0.0/8`. Dieses wird für die Schulen in viele Subnetze unterteilt. Für jede Schule wird ein `/16`-Netz reserviert, das Platz für 65.536 IP-Adressen bietet und nach Bedarf in weitere Subnetze unterteilt wird.

Tab. 4.1: Zuteilung der Subnetze zu Schulen

| Subnetz (CIDR) | Schule |
|---|---|
| `10.0.0.0/16` | Zentrale Systeme |
| `10.1.0.0/16` | 1. Schule |
| `10.2.0.0/16` | 2. Schule |
| `10.3.0.0/16` | 3. Schule |
| `10.4.0.0/16` | 4. Schule |
| `10.....0/16` | *Weitere Schulen* |

Voraussetzung für die Verwendung von Subnetzen ist, dass aus dem Netz, in dem die zentralen Systeme stehen, alle anderen Subnetze erreicht werden können. Dies kann beispielsweise über ein Site-to-Site VPN oder eine Standleitung

realisiert werden. Eine Verbindung zwischen Schulen ist nicht notwendig und wird häufig auch nicht gewünscht.

**Bemerkung:** Bei mehr als 255 Schulen kann das vorgeschlagene Netzkonzept nicht verwendet werden.

### 4.1.1 Beispiele für Subnetzkonzepte

Im Folgenden werden zwei Beispiele für die Schulnetze gezeigt. Das erste für ein Schulnetz für kleinere Schulen mit wenigen Endgeräten, zum Beispiel Grundschulen, das zweite für sehr große Schulen mit vielen Endgeräten und mehreren Subnetzen, zum Beispiel Berufsschulen. Vorweg erfolgt die Definition des Subnetzes für die zentralen Systeme.

Um die Subnetze in UCS@school bekannt zu machen, müssen diese importiert werden. In *Netze* (Seite 40) ist beschrieben wie der Import vorzunehmen ist, welche Informationen anzugeben sind und welche Hilfsmittel dafür zur Verfügung stehen.

Tab. 4.2: Zentrales Subnetz

| Subnetz (CIDR) | DHCP-Adressbereich | Anzahl IP-Adressen | Verwendung |
|---|---|---|---|
| `10.0.0.0/24` | – | 254 | Subnetz für zentrale Systeme |

Alle zentralen Instanzen von UCS@school werden in diesem Netz installiert. Auf eine Adressvergabe via DHCP wird verzichtet, alle Systeme erhalten eine statisch zugewiesene IP-Adresse. Weitere Subnetze, wie zum Beispiel eine Demilitarisierte Zone (DMZ), können bei Bedarf ergänzt werden.

### 4.1.2 Beispiel Subnetz Grundschule

Tab. 4.3: Netze für Beispiel-Grundschule

| Subnetz (CIDR) | DHCP-Adressbereich | Anzahl IP-Adressen | Verwendung |
|---|---|---|---|
| `10.1.0.0/24` | `10.1.0.1–10.1.0.254` | 254 | Kleines Netz für eine Grundschule |

In diesem Beispiel werden eventuell vorhandene Server und Endgeräte im selben Netz betrieben. Dieses Modell richtet sich an kleine Schulen mit wenigen Endgeräten. Bei Bedarf können weitere Subnetze ergänzt werden, da das für die Schule reservierte `/16`-Netz nur zu einem kleinen Teil ausgeschöpft wurde.

### 4.1.3 Beispiel Subnetz Berufsschule

Tab. 4.4: Netze für Beispiel-Berufsschule

| Subnetz (CIDR) | DHCP-Adressbereich | Anzahl IP-Adressen | Verwendung |
|---|---|---|---|
| 10.42.1.0/24 | – | 254 | Netz für Server und Netzgeräte, statische IP-Adressen |
| 10.42.2.0/24 | 10.42.2.10 – 10.42.2.250 | 254 | Netz für Schulverwaltung, erweiterbar auf /23 (510 IP-Adressen) |
| 10.42.4.0/24 | 10.42.4.10 – 10.42.4.250 | 254 | Netz für edukativen Bereich 1, erweiterbar auf /23 (510 IP-Adressen) |
| 10.42.6.0/24 | 10.42.6.10 – 10.42.6.250 | 254 | Netz für edukativen Bereich 2, erweiterbar auf /23 (510 IP-Adressen) |
| 10.42.8.0/24 | 10.42.8.10 – 10.42.8.250 | 254 | Netz für edukativen Bereich 3, erweiterbar auf /23 (510 IP-Adressen) |
| 10.42.10.0/24 | 10.42.10.10 – 10.42.10.250 | 254 | Netz für edukativen Bereich 4, erweiterbar auf /23 (510 IP-Adressen) |
| 10.42.128.0/20 | 10.42.128.100 – 10.42.143.250 | 4094 | Gäste WLAN / BYOD, erweiterbar auf /128 (16.382 IP-Adressen) |
| 10.42.192.0/20 | 10.42.192.100 – 10.42.207.250 | 4094 | Schuleigenes WLAN mit RADIUS-Authentifizierung, erweiterbar auf /18 (16.382 IP-Adressen) |

In diesem Beispiel werden einzelne Subnetze für WLAN, Server, Verwaltung und edukativen Bereich betrieben. Dieses Modell richtet sich an große Schulen mit vielen Endgeräten. Die Subnetze sind so gewählt, dass sie sich bei Bedarf noch erweitern lassen. Die Unterteilung des edukativen Bereichs in einzelne Subnetze kann beispielsweise pro Gebäude, pro Etage oder sogar pro Computerraum erfolgen. Netzdrucker können in die Subnetze aufgenommen werden, in denen sich auch die zugehörigen Endgeräte befinden oder es wird ein eigenes Druckernetz hinzugefügt.

## 4.2 Konzept zur Benennung von Objekten

In einer UCS@school-Domäne für ein oder mehrere Schulen gibt es viele Objekte, die eindeutige Namen benötigen. So brauchen zum Beispiel Benutzerkonten eindeutige Benutzernamen und E-Mail-Adressen. Schulklassen brauchen eindeutige Bezeichnungen, um sie von gleichnamigen Klassen in anderen Schulen zu unterscheiden. Rechnerobjekte benötigen Rechnernamen und Schulen benötigen eine Kurzbezeichnung für die Organisationseinheit im Verzeichnisdienst, in dem die zugehörigen Objekte gespeichert werden. Ein Konzept zur Benennung von Objekten verfolgt die Ziele, Eindeutigkeit herzustellen und gleichzeitig die Bedeutung und Zuordnung des jeweiligen Objekts offensichtlich zu machen. Im Folgenden zeigen wir Konzepte für unterschiedliche Objekttypen auf, die sich in der Praxis bewährt haben.

### 4.2.1 Name der Domäne

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Der Name der Domäne definiert mehrere zugehörige Namen:

- LDAP-Basis des Verzeichnisdienstes
- DNS-Domäne
- Kerberos-Realm
- Samba/Active Directory-Domäne

Die Wahl dieses Namens hat umfangreiche Auswirkungen auf die gesamte UCS@school-Installation und sollte entsprechend mit Bedacht gewählt werden, insbesondere weil eine nachträgliche Änderung nicht möglich ist.

In bisherigen Projekten hat es sich als sinnvoll erwiesen, einen bislang nicht verwendeten Domänennamen sowohl für den Zugriff aus dem Internet als auch für die Benennung der internen UCS-Domäne zu verwenden.

Wird beispielsweise `example.org` als Domänenname ausgewählt, muss auch Univention Corporate Server mit diesem Domänennamen installiert werden. Zudem muss sichergestellt sein, dass die öffentliche Internet-Domain `example.org` vom Betreiber bei einem Domain-Name-Registrar registriert wurde und dass weitere öffentliche Subdomains angelegt werden können.

---

**Bemerkung:** Mit dem hier empfohlenen Vorgehen wird ein sog. *Split-DNS-Szenario* eingerichtet. Die von Univention Corporate Server für interne Funktionen bereitgestellten DNS-Dienste lösen Hostnamen auf internen IP-Adressen auf, während öffentliche DNS-Server die selben Hostnamen auf die öffentlichen IP-Adressen auflösen müssen.

---

- Beispiel für die Hauptdomain (auch interne UCS-Domäne): `example.org`
- Beispiel für das Portal (Zugriff von außen): `portal.example.org`
- Beispiel für eine Anwendung wie beispielsweise Webmail (Zugriff von außen): `mail.example.org`

Bei der Wahl des Domänennamens sind einige Punkte zu beachten:

- Es ist wichtig, dass die DNS-Domäne vom Betreiber verwaltet wird. Es muss sichergestellt werden, dass der gewählte Domänenname für UCS@school im öffentlichen Internet noch nicht verwendet wird.
- Für den nicht empfohlenen Fall, dass die Verwendung einer öffentlichen DNS-Domäne nicht möglich ist und stattdessen ein selbst ausgewählter, interner DNS-Name verwendet wird, so sind folgende Regeln zu beachten:
  - Offizielle DNS-Domänen sollten nicht verwendet werden, wenn sie nicht unter eigener Kontrolle stehen, z.B. `deutschland.de`.
  - Inoffiziell verwendete Top-Level-Domänen sollten nicht verwendet werden, zum Beispiel `.corp` oder `.lan`. Bei ihnen besteht die Gefahr, dass es zu späteren Namenskollisionen kommt.
  - `.local` sollte nicht als Top-Level-Domäne gewählt werden. Die Endung ist offiziell für mDNS (Multicast DNS) vorgesehen und führt bei einer Verwendung zu Problemen mit macOS, Windows und Linux-Betriebssystemen.
- Im internen Netz werden dem Domänennamen für UCS@school die Namen der Rechner und Server vorangestellt, um für diese Systeme einen voll qualifizierten DNS-Namen (FQDN) zu bilden. Zum Beispiel ist der Rechner `ucsrz01` somit intern unter dem FQDN `ucsrz01.example.org` zu erreichen.
- In UCS@school werden mindestens im Falle der Schulserver auch Samba Active Directory Domaincontroller betrieben. Aus Gründen der Abwärtskompatibilität wird dabei auch immer ein NetBIOS- bzw. *Legacy-Domänenname* erstellt. Im Falle von `example.org` als DNS-Domänenname würde automatisch `EXAMPLE` als NetBIOS-Domänenname gesetzt sein.

  Der NetBIOS-Domänenname ist auf 15 Zeichen begrenzt. Dies kann zu Situationen führen, in denen der NetBIOS-Domänenname ungünstig abgeschnitten wird. Wählt man beispielsweise `schulen-musterstadt.de` als DNS-Domänenname, würde der automatisch abgeleitete NetBIOS-Domänenname `SCHULEN-MUSTERS` lauten. Dieser Name ist beispielsweise beim Anmeldebildschirm an Windows-Clients der Domäne zu sehen. Möchte man nun lieber `MUSTERSTADT` als Anzeigename dort sehen, so ist auf dem UCS@school-Server bereits während der Installation der gewünschte `NetBIOS-Domänenname` zu setzen (siehe auch KB 6390 - How to define the NetBIOS name during installation[1]).

[1] https://help.univention.com/t/6390

### 4.2.2 Zentrale Server

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Zentrale Server:

- Schema: `[System][Standort][Laufnummer]`
- Beispiel: System UCS, Standort Rechenzentrum, erstes System: `ucsrz01`
- Weitere Beispiele:
  - Primary Directory Node: `ucsrz01`
  - Backup Directory Node: `ucsrz02`, `ucsrz03`
  - Replica Directory Node: `ucsrz04`
  - Managed Node: `ucsrz05`

Der Name darf eine Länge von 13 Zeichen nicht überschreiten und sollte nicht mit einer Ziffer beginnen.

### 4.2.3 Rechner und Schulserver

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Rechner:

- Schema: `[Betriebssystem]-[Kurzbezeichnung Schule]-[Laufnummer]`
- Beispiele: `win-042-001`, `win-042-002`, `mac-042-001`

Netzgeräte, wie Router, Switches, USV, Drucker:

- Schema: `[Gerätetyp]-[Kurzbezeichnung Schule]-[Laufnummer]`
- Beispiele: `rou-042-001`, `swi-042-003`, `usv-042-001`, `dru-042-012`

Schulserver:

- Schema: `[Rollenbezeichnung]-[Kurzbezeichnung Schule]-[Laufnummer]`
- Beispiele:
  - Edukativer Schulserver: `sedu-042-01`
  - Schulserver Schulverwaltung: `sadm-042-01`

Der Name darf eine Länge von 13 Zeichen nicht überschreiten und sollte nicht mit einer Ziffer beginnen.

### 4.2.4 Benutzernamen und Klassenbezeichnungen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Benutzerkonten und Klassen hängen in UCS@school sehr eng zusammen. So werden beim Import von Benutzerkonten ebenfalls die Klassen angegeben, zu denen die jeweiligen Konten gehören. Das heißt sowohl beim Import von Klassen, also auch beim Import von Benutzerkonten müssen die gleichen Bezeichnungen für Klassen verwendet werden und es ist deshalb hilfreich, ein einheitliches Schema zu spezifizieren.

Bei Benutzerkonten ergibt sich darüber hinaus die Herausforderung, dass sich die Benutzernamen ändern können, zum Beispiel aufgrund von Heirat, Scheidung, im Rahmen einer Namens- oder Personenstandänderung oder zur Behebung von Tippfehlern. In der Praxis hat sich nicht bewährt, unveränderliche Daten wie Personal- oder Schülernummern als Benutzernamen zu verwenden, da diese unpersönlich und schwer zu merken sind.

Die Änderung von Benutzernamen stellt also eine Herausforderung im Betrieb dar, weil die an UCS@school angeschlossenen Subsysteme ggf. den Benutzernamen als identifizierendes Merkmal (also zur Zuordnung von Daten zu Benutzerkonten) verwenden.

Beispiele für Subsysteme sind E-Maildienste, Dateifreigaben und -tauschsysteme oder Lernplattformen. Ändert sich der Benutzername, müssen in den Subsystemen ggf. aufwendig Daten dem neuen Benutzernamen zugeordnet werden. Dieses Problem kann umgangen werden, wenn frühzeitig, vor der Einführung eines neuen Subsystems darauf geachtet wird, dass die Zuordnung von Daten zu Benutzerkonten über ein unveränderliches Merkmal geschieht, zum Beispiel die Personalnummer. Gleichzeitig muss sichergestellt werden, dass die Anmeldung am Subsystem jedoch über den einfach zu merkenden Benutzernamen erfolgt.

Schüler*innen:

- Schema: `[Vorname][1. Buchstabe Nachname][Laufnummer]`
- Beispiel: Mary Selig → `marys`
- Beispiel Namenskonflikt: Mary Sander → `marys2`

Lehrkräfte und Mitarbeiter*innen:

- Schema: `[1. Buchstabe Vorname][Nachname][Laufnummer]`
- Beispiel: Mareike Müller → `mmueller`
- Beispiel Namenskonflikt: Martina Müller → `mmueller2`

Für Benutzerkonten kann das gewünschte Schema im Importmechanismus hinterlegt werden, siehe *UCS@school - Handbuch zur CLI-Import-Schnittstelle* [1].

Klassennamen müssen mit der Kurzbezeichnung der Schule (hier im Beispiel `042` und `011`) als Präfix beginnen:

- Schema: `[Kurzbezeichnung Schule]-[Klasse]`
- Beispiele: `042-1a`, `042-5a`, `011-5a`, `011-5b`

### 4.2.5 Allgemeine Konventionen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Folgende Konventionen haben sich in allen Szenarien bewährt:

- Alle Objektnamen sollten durchgängig Kleinbuchstaben verwenden.
- Sofern nicht anders angegeben, sollte die Länge von Objektnamen 15 Zeichen nicht überschreiten. Dies ist wichtig für Benutzernamen, insbesondere von Schüler*innen.

## 4.3 Monitoring

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Die rechtzeitige Erkennung von Fehlern und möglichen Anzeichen ist ein elementarer Bestandteil des professionellen IT-Betriebs. Univention Corporate Server hat deshalb die Monitoring-Software *Nagios* fest integriert und für viele relevante Parameter vorkonfiguriert. *Nagios* selbst dient zum Monitoring des aktuellen Zustands.

Das Monitoring erfolgt für UCS@school immer aus der Zentrale heraus. Entsprechend ist ein Server-System für den Betrieb des Monitoring-Dienstes vorzusehen, siehe *Installation eines zentralen Managed Node für Monitoring* (Seite 31).

*Nagios* selbst ist nicht darauf ausgelegt, Informationen darüber zu liefern, in welche Richtung sich eine Umgebung entwickelt, da keine Langzeitinformationen gespeichert werden.

Ein Beispiel ist die Entwicklung der Belegung des Festplattenplatzes. Solche Informationen sind für den Betrieb einer umfangreichen IT-Infrastruktur erforderlich. Um diese Informationen zu erfassen, kann zum Beispiel die App **`UCS Dashboard`** verwendet werden, deren UCS Dashboard[2] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] dokumentiert ist.

## 4.4 Datensicherung und Wiederherstellung

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Eine zentral mit UCS@school verwaltete Umgebung stellt üblicherweise Dienste für tausende Personen zur Verfügung. Mit der zunehmenden Anforderung nach orts- und zeitunabhängiger Verfügbarkeit muss sichergestellt werden, dass nicht nur die Dienste, sondern auch die Daten den Anforderungen entsprechend zur Verfügung gestellt werden. Dreierlei Daten sind dabei zu unterscheiden:

- Konfigurationen und Einstellungen, die Administratoren vorgenommen haben
- Steuerinformationen, zum Beispiel die Daten im Identitätsmanagement
- Von Personen erzeugte Daten, zum Beispiel E-Mails

Die Sicherung der Daten muss gewährleistet sein, um im Fehlerfall die Funktionsfähigkeit wiederherzustellen. Als Minimalumfang muss eine dateibasierte Sicherung, zum Beispiel mit Hilfe des Befehls **`rsync`** erfolgen. Folgende Daten sollten in der Sicherung berücksichtigt werden:

Zentrale Server:

- `/var/univention-backup`: Nächtliche Sicherung der Univention Configuration Registry-, OpenLDAP- und Samba-Datenbank, sowie der Inhalte der SYSVOL-Freigabe.
- `/etc/univention/ssl` auf dem Primary Directory Node und den Backup Directory Node-Servern: Beinhaltet das Root-Zertifikat der internen Zertifizierungsstelle und alle Rechner-Zertifikate.
- `/etc/*.secret` auf allen Systemen.

Schulserver, sofern vorhanden:

- `/var/univention-backup`: Nächtliche Sicherung der Univention Configuration Registry. Die Sicherung der OpenLDAP- und Samba-Datenbanken braucht nicht gesichert werden, da diese beim erneuten Domänenbeitritt des Schulservers vom Primary Directory Node oder Backup Directory Node repliziert werden.

[2] https://docs.software-univention.de/manual/5.0/de/monitoring/dashboard.html#dashboard-general

- `/home`: Beinhaltet die Benutzerprofile und die Heimatlaufwerke der Benutzer, sowie die Freigaben der Klassen und Arbeitsgruppen.

Folgende Punkte haben sich als allgemein bewährtes Vorgehen herauskristallisiert:

- Die Datensicherung sollte auf ein vom Univention Corporate Server-System physikalisch getrenntes Gerät erfolgen, zum Beispiel ein *Network Attached Storage (NAS)*.
- Die Datensicherung sollte überwacht werden, zum Beispiel durch ein Plugin im Monitoring-Dienst, das bei Misserfolg warnt.
- Die Wiederherstellung sollte in regelmäßigen Abständen getestet werden.

## 4.5 Support-Kanäle

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Für den erfolgreichen Betrieb von UCS@school ist es erforderlich, dass ein Helpdesk aufgebaut wird, der Fragen aus den Schulen direkt annehmen kann. Abhängig von der gewünschten *Servicestufe* (Seite 3) kann es darüber hinaus notwendig sein, ein Team von technischen Mitarbeiter*innen zu schulen, die den Betrieb der Umgebung durchführen.

Neben passenden Werkzeugen zur Kommunikation und Fernwartung, zum Beispiel ein Ticket-System, müssen auch die Support- und Eskalationswege definiert und abgestimmt werden. Im Folgenden ein Beispiel für Eskalationswege:

- IT-Verantwortliche an den Schulen kontaktieren den Helpdesk über das Helpdesk-Modul in UCS@school oder direkt per E-Mail an das Ticketsystem. In dringenden Fällen steht eine Hotline zur Verfügung, die telefonisch erreicht werden kann.
- Der Helpdesk übernimmt den First- und Second-Level-Support, ggf. in Zusammenarbeit mit einem lokalen Dienstleister.
- In weitergehenden Fällen unterstützt Univention mit Third-Level-Support.

KAPITEL 5

# Netzinfrastruktur- und Hardware-Voraussetzungen

Im Folgenden werden die Netzinfrastruktur- und Hardware-Voraussetzungen für den Einsatz von UCS@school beschrieben. Die beschriebenen Voraussetzungen sind Richtwerte, die wir ermittelt haben. Im Einzelfall ist jedoch genau zu prüfen, ob die Voraussetzungen mit den gestellten Anforderungen übereinstimmen.

Allgemein hat sich für den Betrieb von Univention Corporate Server bewährt, eine Virtualisierungslösung einzusetzen. Die Dimensionierung der Virtualisierungsserver muss sich dabei an den Anforderungen der virtualisierten Systeme richten und dabei noch genügend Möglichkeiten zur nachträglichen Erweiterung bereithalten. Eine Zuweisung von mehr als den vorhandenen Ressourcen (Überprovisionierung) wird abgeraten. Für den Speicherplatz sollten mindestens SAS-Festplatten mit 10.000 Umdrehungen pro Minute zum Einsatz kommen, idealerweise aber SSD-Festplatten (mindestens für die I/O-intensiven Dienste wie OpenLDAP und Samba unter `/var/lib/`.)

Die genannten Werte sind die Minimalanforderungen für die oben beschriebenen Szenarien. Abhängig von der Größe der Umgebung und Anzahl der aktiven Geräte und Personen können die Anforderungen höher liegen. Die tatsächliche Auslastung der einzelnen Systeme sollte fortlaufend durch das *Monitoring* (Seite 21) überwacht werden, um Engpässe zu vermeiden. Im Folgenden werden die Server, ihre Funktionen und die jeweiligen Anforderungen beschrieben.

## 5.1 Zentrale Server

### 5.1.1 Identity Management

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Systeme vom Typ Primary Directory Node und Backup Directory Node stellen das Identitätsmanagement mit der zugrunde liegenden LDAP-Datenbank zur Verfügung.

Minimale Systemvoraussetzungen:

- 4 CPU-Kerne
- 8 GB RAM
- 100 GB Speicherplatz

Die primären Lastszenarien des Primary Directory Node sind:

- Viele lesende Zugriffe auf die LDAP-Datenbank, da neben der Administration alle weiteren Systeme regelmäßig Information abfragen.
- Schreibende Zugriffe auf die LDAP-Datenbank, sobald Änderungen vorgenommen werden. Insbesondere beim initialen Import und beim Schuljahreswechsel wird die LDAP-Datenbank stark belastet.

Die I/O-Performance der Festplatten dieser Server ist besonders wichtig, zusammen mit ausreichend Arbeitsspeicher, der insbesondere beim initialen Import und beim Schuljahreswechsel notwendig ist.

Backup Directory Node dienen der Lastverteilung und Ausfallsicherheit. Es sollte immer mindestens ein Backup Directory Node in der Domäne vorhanden sein. Darüber hinaus können bei Bedarf weitere Backup Directory Node-Systeme hinzugefügt werden.

Sollte der Primary Directory Node durch einen irreparablen Schaden ausfallen, kann ein Backup Directory Node-System zum Primary Directory Node hochgestuft werden. Dieser Vorgang ist nicht umkehrbar, daher sollte die Position der Backup Directory Node-Systeme innerhalb der Netzinfrastruktur entsprechend gewählt werden, damit jedes einzelne System im Extremfall alle Aufgaben des Primary Directory Node übernehmen kann.

### 5.1.2 RADIUS

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Minimale Systemvoraussetzungen:

- 2 CPU-Kerne
- 4 GB RAM
- 50 GB Speicherplatz

### 5.1.3 Monitoring

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Minimale Systemvoraussetzungen:

- 2 CPU-Kerne
- 4 GB RAM
- 50 GB Speicherplatz

### 5.1.4 IT-Angebote, wie Groupware und Lernplattformen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Für weitere IT-Angebote können keine Minimalanforderungen genannt werden, da diese sowohl von der Anzahl der parallelen Benutzer als auch von der Anwendung selbst abhängig sind. Eine Abstimmung mit dem jeweiligen Hersteller ist in aller Regel notwendig.

## 5.2 Dezentrale Systeme

### 5.2.1 Schulserver

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Auch hier spielt vor allem die Anzahl gleichzeitig aktiver Benutzerkonten und Endgeräte eine Rolle.

Minimale Systemvoraussetzungen für *kleine Schulen (z.B. Grundschulen)* (25 Computer, 25 Tablets, 150 Benutzerkonten):

- 2 CPU-Kerne
- 4 GB RAM
- 100 GB Speicherplatz für das System selbst
- bis zu 100 GB Speicherplatz für Benutzerdaten

Minimale Systemvoraussetzungen für *mittelgroße Schulen* (100 Computer, 100 Tablets, 600 Benutzerkonten):

- 4 CPU-Kerne
- 16 GB RAM
- 100 GB Speicherplatz für das System selbst
- ab 400 GB Speicherplatz für Benutzerdaten

Minimale Systemvoraussetzungen für *große Schule (z.B. Berufsschulen)* (300 Computer, 200 Tablets, 1500 Benutzerkonten):

- 8 CPU-Kerne
- 32 GB RAM
- 100 GB Speicherplatz für das System selbst
- ab 1.000 GB Speicherplatz für Benutzerdaten

## 5.3 Netzinfrastruktur

### 5.3.1 Strukturierte Verkabelung

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Die Schulen sollten über eine strukturierte Verkabelung im Schulgebäude verfügen. Dies schließt ein, das möglichst nur Switches und Netzkomponenten mit Management-Funktion verwendet werden. Damit werden Probleme vermieden, die durch fehlerhafte Verkabelung entstehen und es wird möglich, die Qualität der erbrachten Leistung bis auf Ebene des Netzes zu messen. Darüber hinaus können Sicherheitsmechanismen implementiert werden, die bei zunehmender Verwendung der IT-Infrastruktur immer wichtiger werden.

### 5.3.2 WLAN-Infrastruktur

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Für die Einführung von WLAN in Schulen gehen wir hier davon aus, dass die gesamte Schule mit WLAN ausgestattet werden soll und alle Schüler*innen mit mindestens einem mobilen Endgerät im WLAN aktiv sein werden, auch wenn dies nicht sofort realisiert werden kann.

Um dieses Ziel zu erreichen, ist eine *Strukturierte Verkabelung* (Seite 25) Grundvoraussetzung. Darüber hinaus werden professionelle Access Points benötigt, die mehr als 40 parallel eingebuchte mobile Geräte unterstützen, ohne dass der Access Point z.B. aufgrund von Speichermangel abstürzt. Mit professionellen Access Points lassen sich darüber hinaus auch weitere Sicherheits- und Administrationsmechanismen, wie VLAN, realisieren.

### 5.3.3 Internetzugang

**Gültigkeit**

Für Szenario *2* (Seite 4) und *3* (Seite 6).

Die Schulen sollten über zuverlässige Internetzugänge verfügen, die maximal 1x pro Nacht getrennt werden. Die Geschwindigkeit des Zugangs sollte mindestens 16 MBit/s betragen. Ausschlaggebend für die notwendige Geschwindigkeit ist die Anzahl der gleichzeitig aktiven Endgeräte. Als Richtwert kann von einem Bedarf von mindestens 0,3 MBit/s pro aktivem Gerät ausgegangen werden. Dies ist insbesondere bei der Einführung von WLAN und Bring Your Own Device (BYOD) zu beachten, da Lehrkräfte und Schüler*innen ggf. über mehr als ein Gerät pro Person verfügen werden.

### 5.3.4 Internetzugang: Schulserver im Rechenzentrum

**Gültigkeit**

Für Szenario *4* (Seite 6).

Die folgende Schätzung der Bandbreite gilt ausschließlich für *Szenario 4: Schulische IT-Infrastruktur ohne dezentrale Schulserver* (Seite 6), in dem alle Schulserver aus den Schulen in ein zentrales Rechenzentrum überführt werden. In den Schulen verbleiben nur die Endgeräte, die zur Nutzung der IT notwendig sind.

Die Anforderungen der anderen Szenarien sind in *Internetzugang* (Seite 26) beschrieben.

Die nötigen Bandbreiten im lokalen Schulnetz können je nach Anwendungsfall stark schwanken. Die folgende Tabelle gibt einen groben Überblick über Richtwerte nach Schultyp. Die benötigte Bandbreite liegt zwischen 2-5 MBit/s für schuleigene Geräte. Dabei ist zu beachten, dass z.B. zum Schulstundenbeginn oder zum Pausenbeginn mit Lastspitzen zu rechnen ist.

Tab. 5.1: Minimalanforderungen für die Anbindung nach Schultyp

| Schultyp | Typische Anzahl Clients | Typische Netznutzung | Mindestens nötige Bandbreite |
|---|---|---|---|
| Grundschulen | ~20 Clients | Geringe Netznutzung (~2 MBit/s) | 40 MBit/s |
| Weiterführende Schulen | ~90 Clients | Mittlere Netznutzung (~3 MBit/s) | 270 MBit/s |
| Berufsschulen | ~300 Clients | Hohe Netznutzung (>5 MBit/s) | 1,5 GBit/s |

### 5.3.5 Verbindung zur Zentrale

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Die Schulen müssen an die zentralen Systeme angebunden werden, damit eine Steuerung der Netze, Endgeräte und ggf. Server von zentraler Stelle möglich wird. Um die Verbindung aufzubauen, können VPN-Technologien, Standleitungen oder private Netze verwendet werden.

Die Bandbreite der verfügbaren Anbindung beeinflusst entscheidend die möglichen Szenarien. *Szenario 4* (Seite 6) ist zum Beispiel nur bei einer sehr guten Anbindung im Bereich von 1 GBit/s oder mehr sinnvoll möglich. Bei VPN über handelsübliche DSL-Leitungen empfiehlt sich stattdessen die Umsetzung von *Szenario 3* (Seite 6).

KAPITEL 6

# Installation

Die Installation von UCS@school ist grundlegend in Installation[3] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] und in Installation[4] in *UCS@school - Handbuch für Administratoren* [3] beschrieben. In diesem Abschnitt geben wir zusätzliche Hinweise zur Installation, insbesondere im Hinblick auf die Umsetzung der definierten Konzepte.

- Zur Installation wird das aktuellste UCS Installationsmedium[5] empfohlen.
- Der Pfad `/var/log` sollte auf eine eigene Partition gelegt werden, damit bei erhöhten Aufkommen an Log-Informationen nicht die Systempartition voll läuft und in der Folge die Funktionsfähigkeit des Gesamtsystems zusammenbricht.
- Ist die Verfügbarkeit von performanten Festplatten (zum Beispiel SSDs) begrenzt und reicht nicht für das gesamte System aus, so sollte zumindest `/var/lib` als eigene Partition auf performanten Festplatten angelegt werden.
- Je nach System und verwendeten Diensten (beispielsweise für Schulserver mit lokalen Benutzerdaten) sollte die Auslagerung auf einem eigenen Dateisystem auch für den Pfad `/home` erfolgen.

## 6.1 Installation des Primary Directory Node

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

- Die IP-Adresskonfiguration erfolgt entsprechend dem Netzkonzept.
- Als Externer DNS-Server bzw. DNS-Forwarder ist die IP-Adresse des DNS-Servers des Internetproviders oder des Rechenzentrum-Betreibers einzutragen.
- Die folgende Option ist auszuwählen, um den Primary Directory Node zu installieren: *Erstellen einer neuen |UCSUCS|-Domäne*.
- Nach der Eingabe des Domänennamen wird automatisch eine LDAP-Basis vorgeschlagen. Diese sollte entsprechend des Namenskonzeptes angepasst werden.

[3] https://docs.software-univention.de/manual/5.0/de/installation.html#installation-chapter
[4] https://docs.software-univention.de/ucsschool-manual/5.0/de/installation/index.html#install
[5] https://www.univention.de/download/download-ucs/

- Das installierte System ist abschließend bis zum letzten verfügbaren Errata-Update zu aktualisieren.
- Nach Abschluss der Installation ist über das Univention App Center die App **UCS@school** zu installieren.
- Im Anschluss an die Installation der App **UCS@school** ist in der Univention Management Console in der Kategorie *Schuladministration* der *UCS@school Einrichtungsassistent* zu starten und die Option *Multi-Server Umgebung* zu wählen und der Assistent bis zum Ende auszuführen.
- Für Szenario *3* (Seite 6) und *4* (Seite 6):

  Um Gruppenrichtlinien für alle Schulen über eine zentrale Stelle verwalten zu können, muss zudem über das Univention App Center die App **Active Directory kompatibler Domänen-Controller** installiert werden.

  Soll der NetBIOS-Domänenname nicht automatisch erzeugt werden, ist dieser vor der Installation explizit zu konfigurieren (siehe auch *Name der Domäne* (Seite 17)).

  Sollen in der UCS@school-Domäne mehr als 50.000 Benutzer verwaltet werden, setzen Sie sich bitte vorab mit Univention in Verbindung, um Möglichkeiten zur Performanceoptimierung zu besprechen.
- Abschließend ist zu prüfen, ob alle Join-Skripte erfolgreich ausgeführt wurden. Dies kann in der Univention Management Console in der Kategorie *Domäne* mit dem Modul *Domänenbeitritt* geprüft werden.

## 6.2 Installation eines Backup Directory Node

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Zur Lastverteilung bei der LDAP-Replikation können neben dem ersten, unbedingt notwendigen Backup Directory Node Server zusätzlich noch weitere Backup Directory Node Systeme aufgesetzt werden.

- Es ist sicherzustellen, dass zuvor auf dem Primary Directory Node alle verfügbaren Updates installiert wurden.
- Die IP-Adresskonfiguration erfolgt entsprechend des Netzkonzepts.
- Als DNS-Server ist die IP-Adresse des Primary Directory Node einzutragen. Der DNS-Forwarder wird beim Domänenbeitritt automatisch vom Primary Directory Node übernommen und braucht somit nicht eingetragen zu werden.
- Die folgende Option ist auszuwählen, um den Backup Directory Node als Mitglied der Domäne zu installieren: *Einer bestehenden UCS-Domäne beitreten*. Anschließend ist die Rolle *Backup Directory Node* auszuwählen.
- Das installierte System ist abschließend bis zum letzten verfügbaren Errata-Update zu aktualisieren. Anschließend ist der Domänenbeitritt zu starten.
- Während des Domänenbeitritts wird die App **UCS@school** automatisch installiert. Dies ist über das Univention App Center zu prüfen.
- Alle benötigten Pakete werden während des Domänenbeitritts installiert.
- Im Anschluss an die Installation der App **UCS@school** ist in der Univention Management Console in der Kategorie *Schuladministration* zu prüfen, dass der *UCS@school Einrichtungsassistent* erfolgreich abgeschlossen wurde.
- Abschließend ist zu prüfen, ob alle Join-Skripte erfolgreich ausgeführt wurden. Dies kann in der Univention Management Console in der Kategorie *Domäne* mit dem Modul *Domänenbeitritt* geprüft werden.

Weitere Hinweise zur Installation eines Schulservers und zum UCS@school Einrichtungsassistent finden sich auch in Installation eines Schulservers[6] in *UCS@school - Handbuch für Administratoren* [3].

[6] https://docs.software-univention.de/ucsschool-manual/5.0/de/installation/multi.html#school-installation-replica-directory-node

## 6.3 Installation eines zentralen Replica Directory Node für RADIUS, Groupware, Collaboration, Lernplattformen usw.

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Nach Möglichkeit sollte für jeden Dienst ein separater Server mit der Rolle *Replica Directory Node* verwendet werden.

- Es ist sicherzustellen, dass zuvor auf dem Primary Directory Node alle verfügbaren Updates installiert wurden.
- Die IP-Adresskonfiguration erfolgt entsprechend des Netzkonzepts.
- Als DNS-Server sind die IP-Adressen des Primary Directory Node und des Backup Directory Node einzutragen. Der DNS-Forwarder wird beim Domänenbeitritt automatisch vom Primary Directory Node übernommen und braucht somit nicht eingetragen zu werden.
- Die folgende Option ist auszuwählen, um den Replica Directory Node als Mitglied der Domäne zu installieren: *Einer bestehenden UCS-Domäne beitreten*. Anschließend ist die Rolle *Replica Directory Node* auszuwählen und zu bestätigen, dass es sich um einen zentralen Replica Directory Node handelt und explizit nicht um einen Schulserver.
- Das installierte System ist abschließend bis zum letzten verfügbaren Errata-Update zu aktualisieren. Falls noch nicht erfolgt, ist der Domänenbeitritt zu starten.
- Nach Abschluss der Installation ist über das Univention App Center die gewünschte App, zum Beispiel **`RADIUS`**, zu installieren.
- Die App **`UCS@school`** soll hier **nicht** installiert werden.
- Abschließend ist zu prüfen, ob alle Join-Skripte erfolgreich ausgeführt wurden. Dies kann in der Univention Management Console in der Kategorie *Domäne* mit dem Modul *Domänenbeitritt* geprüft werden.

## 6.4 Installation eines zentralen Managed Node für Monitoring

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

- Es ist sicherzustellen, dass zuvor auf dem Primary Directory Node alle verfügbaren Updates installiert wurden.
- Die IP-Adresskonfiguration erfolgt entsprechend des Netzkonzepts.
- Als DNS-Server sind die IP-Adressen des Primary Directory Node und des Backup Directory Node einzutragen. Der DNS-Forwarder wird beim Domänenbeitritt automatisch vom Primary Directory Node übernommen und braucht somit nicht eingetragen zu werden.
- Die folgende Option ist auszuwählen, um den Replica Directory Node als Mitglied der Domäne zu installieren: *Einer bestehenden UCS-Domäne beitreten*. Anschließend ist die Rolle *Managed Node* auszuwählen.
- Es ist sicherzustellen, dass der Primary Directory Node alle verfügbaren Updates installiert hat.
- Das installierte System ist abschließend bis zum letzten verfügbaren Errata-Update zu aktualisieren. Anschließend ist der Domänenbeitritt zu starten.
- Nach Abschluss der Installation ist über das Univention App Center die App **`Nagios`**, zu installieren.
- Es ist empfohlen, das Monitoring des aktuellen Zustands der Umgebung um die Speicherung von Langzeitinformationen zu ergänzen. Weitere Informationen sind in *Monitoring* (Seite 21) zu finden.
- Die App **`UCS@school`** darf **nicht** installiert werden.

- Abschließend ist zu prüfen, ob alle Join-Skripte erfolgreich ausgeführt wurden. Dies kann in der Univention Management Console in der Kategorie *Domäne* mit dem Modul *Domänenbeitritt* geprüft werden.
- Damit **Nagios** lauffähig ist, muss sichergestellt sein, dass die globale Univention Configuration Registry-Richtlinie `ucsschool-ucr-settings` auf alle anderen Systeme wirkt.

  Dies kann überprüft werden, indem der Wert der Univention Configuration Registry-Variable *nagios/client/allowedhosts* (Seite 34) auf den anderen Servern abgerufen wird.

  Sollten trotzdem keine Statusinformationen über einen Server angezeigt werden, so müssen ggf. die Dienste **univention-directory-listener** und **nagios-nrpe-server** neu gestartet werden.

## 6.5 Installation eines Replica Directory Node als Schulserver

**Gültigkeit**

Für *Szenario 3* (Seite 6)

Vor der Installation des Schulservers muss die zugehörige Schule mitsamt dem Namen für den Schulserver auf dem Primary Directory Node angelegt werden. Es ist zudem empfehlenswert auch die der Schule zugehörigen Netzwerke vorab zu importieren. Bitte fahren Sie zunächst mit dem *Datenimport* (Seite 37) fort, importieren mindestens Schulen und Netzwerke und kommen dann zu diesem Abschnitt für die Installation des Schulservers zurück.

- Es ist sicherzustellen, dass zuvor auf dem Primary Directory Node alle verfügbaren Updates installiert wurden.
- Es ist sicherzustellen, dass zuvor die Schule mitsamt dem Namen für den Schulserver sowie die Netzwerke auf dem Primary Directory Node entsprechend der Beschreibung in *Schulen* (Seite 37) angelegt bzw. importiert wurden.
- Bei der Partitionierung sollte darauf geachtet werden, dass der Pfad `/home` auf einem eigenen Dateisystem abgelegt wird, damit aufgrund von übermäßig vielen Benutzerdaten die Systempartition nicht voll läuft.
- Die IP-Adresskonfiguration erfolgt entsprechend des Netzkonzepts.
- Als DNS-Server sind die IP-Adressen des Primary Directory Node und des Backup Directory Node einzutragen. Der DNS-Forwarder wird beim Domänenbeitritt automatisch vom Primary Directory Node übernommen und braucht somit nicht eingetragen zu werden.
- Die folgende Option ist auszuwählen, um den Replica Directory Node als Mitglied der Domäne zu installieren: *Einer bestehenden UCS-Domäne beitreten*. Anschließend ist die Rolle *Replica Directory Node* auszuwählen.
- Es ist darauf zu achten, dass der bei der Installation angegebene Rechnername mit dem Namen des Schulservers übereinstimmt, der beim Anlegen der Schule angegeben wurde. Dies muss der Fall sein, damit der Server im weiteren Verlauf als edukativer Schulserver eingerichtet werden kann und explizit nicht als zentraler Replica Directory Node.
- Das installierte System automatisch bis zum letzten verfügbaren Errata-Update aktualisieren, den Domänenbeitritt starten und dabei die App **UCS@school** installieren.
- Alle benötigten Pakete werden während des Domänenbeitritts installiert und für die zu replizierende Schule konfiguriert.
- Abschließend ist zu prüfen, ob alle Join-Skripte erfolgreich ausgeführt wurden. Dies kann in der Univention Management Console in der Kategorie *Domäne* mit dem Modul *Domänenbeitritt* geprüft werden.
- Soll der Schulserver auch als DHCP-Server fungieren (empfohlen), muss noch die App **DHCP-Server** über das Univention App Center installiert werden.

Weitere Hinweise zur Installation eines Schulservers und zum UCS@school Einrichtungsassistent finden sich auch in Installation eines Schulservers[7] in *UCS@school - Handbuch für Administratoren* [3].

[7] https://docs.software-univention.de/ucsschool-manual/5.0/de/installation/multi.html#school-installation-replica-directory-node

KAPITEL 7

# Basiskonfiguration

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Folgende Konfigurationen müssen **vor** dem Anlegen der ersten Schulen umgesetzt werden.

## 7.1 Zustellung von Systemmails

Univention Corporate Server verschickt regelmäßig E-Mails, um aktuelle Ereignisse aus dem Monitoring und Ergebnisse von Routineaufgaben zu kommunizieren. Diese E-Mails sind für den Betrieb von großer Wichtigkeit und müssen unbedingt beachtet werden. Damit diese E-Mail zugestellt werden können, ist der E-Mailversand wie folgt zu konfigurieren.

Um eine einfache und homogene Konfiguration der Univention Configuration Registry-Variablen zu erreichen, sollten Univention Configuration Registry-Richtlinien verwendet werden.

1. E-Mailalias für `root` auf ein System stellen/umleiten: Wenn zum Beispiel alle E-Mails an den Benutzer `root` an den Primary Directory Node umgeleitet werden sollen, ist die Univention Configuration Registry-Variable *`mail/alias/root`* (Seite 35) auf den Wert `root@ucsrz01.example.org` zu stellen. `example.org` muss durch den tatsächlichen Domänennamen ersetzt werden.

2. Anschließend ist auf dem Zielsystem, in diesem Beispiel auf dem Primary Directory Node, die Zieladresse für alle E-Mails an `root` zu hinterlegen. Die E-Mailadresse wird ebenfalls über Univention Configuration Registry-Variable *`mail/alias/root`* (Seite 35) festgelegt, zum Beispiel `admins@example.org`.

3. Damit das Zielsystem die E-Mail annehmen kann, ist auf dem Zielsystem die App **`Mailserver`** zu installieren. Außerdem ist der Zugang zu einem entfernten Mailserver zu konfigurieren, über den die E-Mails zugestellt werden können. Die Konfiguration eines Relay-Hosts für den Mailversand[8] ist in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2] beschrieben.

4. Mit dieser Konfiguration werden alle E-Mails, die auf einem beliebigen Server an den Benutzer `root` geschickt werden, an die konfigurierte E-Mailadresse weitergeleitet.

   Es ist sinnvoll zu prüfen, ob es weitere lokale Konten von Systembenutzern gibt, die E-Mails erhalten. Diese sollte alle auf den Benutzer `root` umgeleitet werden. Insbesondere sind die Univention Configuration

[8] https://docs.software-univention.de/manual/5.0/de/mail/configuration-server.html#mail-serverconfig-relay

Registry-Variablen `mail/alias/postmaster` und `mail/alias/webmaster` auf den Wert `root` zu setzen.

## 7.2 Globale Univention Configuration Registry-Richtlinie

Die globale Univention Configuration Registry-Richtlinie wird in der Univention Management Console über die Kategorie *Domäne* und das Modul *Richtlinien* bearbeitet. Die Richtlinie hat den Namen **ucsschool-ucr-settings** und ist vom Typ Univention Configuration Registry. Um folgende Einträge sollte die Richtlinie erweitert werden:

**directory/manager/web/module/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen der Univention Directory Manager-Module. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `0`

**ucsschool/wizards/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen der UCS@school-Module. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `false`

**ucsschool/assign-teachers/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen des UCS@school-Moduls zum Zuweisen von Lehrkräften. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `false`

**ucsschool/assign-classes/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen des UCS@school-Moduls zum Zuweisen von Klassen. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `false`

**ucsschool/workgroups/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen des UCS@school-Moduls zum Bearbeiten von Arbeitsgruppen. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `false`

**ucsschool/passwordreset/autosearch**
Deaktiviert die automatische Suche nach allen Objekten beim Öffnen des UCS@school-Moduls zum Zurücksetzen von Passwörtern. Dies beschleunigt das Arbeiten mit vielen LDAP-Objekten.

Wert: `false`

**ucsschool/passwordreset/autosearch_on_change**
Deaktiviert die automatische Suche nach allen Objekten im UCS@school-Modul zum Zurücksetzen von Passwörtern nachdem der Suchfilter geändert wurde. Dies vereinheitlicht das Verhalten der UCS@school-Module, kann bei Bedarf aber auch auf dem Standardwert belassen bzw. nicht angepasst werden.

Wert: `false`

**samba4/sysvol/sync/from_downstream**
Konfiguriert die SYSVOL-Replikation unidirektional vom Primary Directory Node zu den UCS@school Schulservern. Dies beugt Problemen mit der Replikation vor.

Wert: `false`

**samba4/sysvol/sync/from_upstream/delete**
Konfiguriert die SYSVOL-Replikation unidirektional vom Primary Directory Node zu den UCS@school Schulservern. Dies beugt Problemen mit der Replikation vor.

Wert: `true`

**nagios/client/allowedhosts**
Erlaubt den Zugriff des Monitoring-Servers, **Nagios**, auf den *NRPE-Dienst* der übrigen Systeme.

Wert: `[IP-Adresse des Monitoring Servers, zum Beispiel 10.0.0.20]`

**ucsschool/helpdesk/recipient**
Definiert die E-Mailadresse, an die Nachrichten vom UCS@school Helpdesk-Modul geschickt werden. Die Zustellung sollte unbedingt getestet werden! Siehe auch *Zustellung von Systemmails* (Seite 33).

Wert: `[E-Mailadresse des Helpdesks, zum Beispiel admins@example.org]`

**mail/alias/root**
Definiert die E-Mailadresse für Systemmails (Cron / Monitoring). Die Zustellung sollte unbedingt getestet werden! Siehe auch *Zustellung von Systemmails* (Seite 33).

Wert: `[E-Mailadresse des Betreibers, zum Beispiel admins@example.org]`

**ucsschool/import/generate/policy/dhcp/dns/set_per_ou**
Verhindert das automatische Anlegen bestimmter DHCP-DNS-Richtlinien für den Edukativ-Bereich der Schulen. Bei der Verwendung des Verwaltungsnetzes ist dies hinderlich. Die notwendigen DHCP-Richtlinien werden später durch den Netzimport korrekt angelegt

Wert: `false`

## 7.3 Zentrale Univention Configuration Registry-Richtlinie

Eine Univention Configuration Registry-Richtlinie für die zentralen Server wird benötigt, um sicherzustellen, dass die Konfigurationen der Server gleichartig sind. Dazu ist in der Univention Management Console über die Kategorie *Domäne* und das Modul *Richtlinien* zu öffnen und die zentrale Richtlinie anzulegen.

Dazu wird eine neue Richtlinie vom Typ Univention Configuration Registry im Container `policies/config-registry` erstellt. Die Richtlinie soll `ucr_central` heißen und folgende Einträge enthalten:

Tab. 7.1: UCR-Variablen zur Zeitserver-Konfiguration

| UCR-Variable | Wert | Beschreibung |
|---|---|---|
| `timeserver`[9] | `[FQDN oder IP-Adresse des ersten externen Zeitservers]` | Zeitserver von dem die gesamte Domäne ihre Uhrzeit bezieht. Beispiele: `ptbtime1.ptb.de` oder `0.europe.pool.ntp.org`. |
| `timeserver2`[10] | `[FQDN oder IP-Adresse des zweiten externen Zeitservers]` | Zeitserver von dem die gesamte Domäne ihre Uhrzeit bezieht. Beispiele: `ptbtime1.ptb.de` oder `0.europe.pool.ntp.org`. |
| `timeserver3`[11] | `[FQDN oder IP-Adresse des dritten externen Zeitservers]` | Zeitserver von dem die gesamte Domäne ihre Uhrzeit bezieht. Beispiele: `ptbtime1.ptb.de` oder `0.europe.pool.ntp.org`. |

**Bemerkung:** Die UCS@school Schulserver setzen automatisch den Primary Directory Node und die Backup Directory Node-Server als Zeitserver. Damit wird automatisch eine Kaskadierung erreicht.

Abschließend ist die Richtlinie mit den zentralen Servern zu verknüpfen. In der Univention Management Console ist dazu in der Kategorie *Domäne* das Modul *LDAP-Verzeichnis* auszuwählen und der Container `computers` zu öffnen. Nun ist mit der rechten Maustaste der Container anzuklicken und die Option *Bearbeiten* zu selektieren.

[9] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-timeserver
[10] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-timeserver2
[11] https://docs.software-univention.de/manual/5.0/de/appendix/variables.html#envvar-timeserver3

Auf Reiter Richtlinien ist nun der Punkt *Richtlinie: Univention Configuration Registry* zu öffnen und als dem Dropdown *Richtlinien-Konfiguration* die eben erstellte Richtlinie `ucr_central` auszuwählen.

Die Richtlinie wird nun auf alle Systeme unterhalb des Containers `computer` vererbt.

KAPITEL 8

# Datenimport

Nach Abschluss der Installation der zentralen Systeme sind die Daten in das LDAP-Verzeichnis zu importieren, die für die Einrichtung und den Betrieb von Schulen benötigt werden. Dies sind Informationen über die Schulen, die IP-Netze, Benutzerkonten und weitere Objekte.

Der Datenimport sollte erfolgen, bevor Schulserver und Rechner ausgerollt werden. Weiterhin sollten die unterschiedlichen Daten in der Reihenfolge importiert werden, wie sie in diesem Kapitel vorgegeben ist. Darüber hinaus sollten die Daten, die in CSV-Dateien gespeichert werden, für die spätere Analyse und Überarbeitung gesichert abgelegt werden.

## 8.1 Schulen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Im ersten Schritt werden die Schulen importiert. Durch den Datenimport wird im LDAP-Verzeichnis die Container-Struktur erstellt, die für die späteren Importe benötigt wird. Um alle Schulen in einem Schritt zu importieren, ist eine CSV-Datei zu erstellen.

Das Vorgehen zum Import ist wie folgt:

- `Vorlage für den Import` öffnen und Tabelle *Schulen* ausfüllen.
  - Die Spalten für *Schulkürzel*, *Schulname* und *Server Pädagogik* sind Pflichtfelder.
  - Die Spalte *Server Verwaltung* ist optional.
  - Die Spalte *Server Fileshare* bleibt im Normalfall leer. Sie kann in ganz bestimmten Fällen ausgefüllt werden.
- Export der Tabelle ins CSV-Format mit Komma als Trennzeichen für Felder.
- Die CSV-Datei `schulen.csv` ist auf dem Primary Directory Node in folgendem Verzeichnis abzulegen: `/usr/local/ucsschool/import_data/`. Das Verzeichnis muss ggf. zuerst angelegt werden: `mkdir -p /usr/local/ucsschool/import_data`

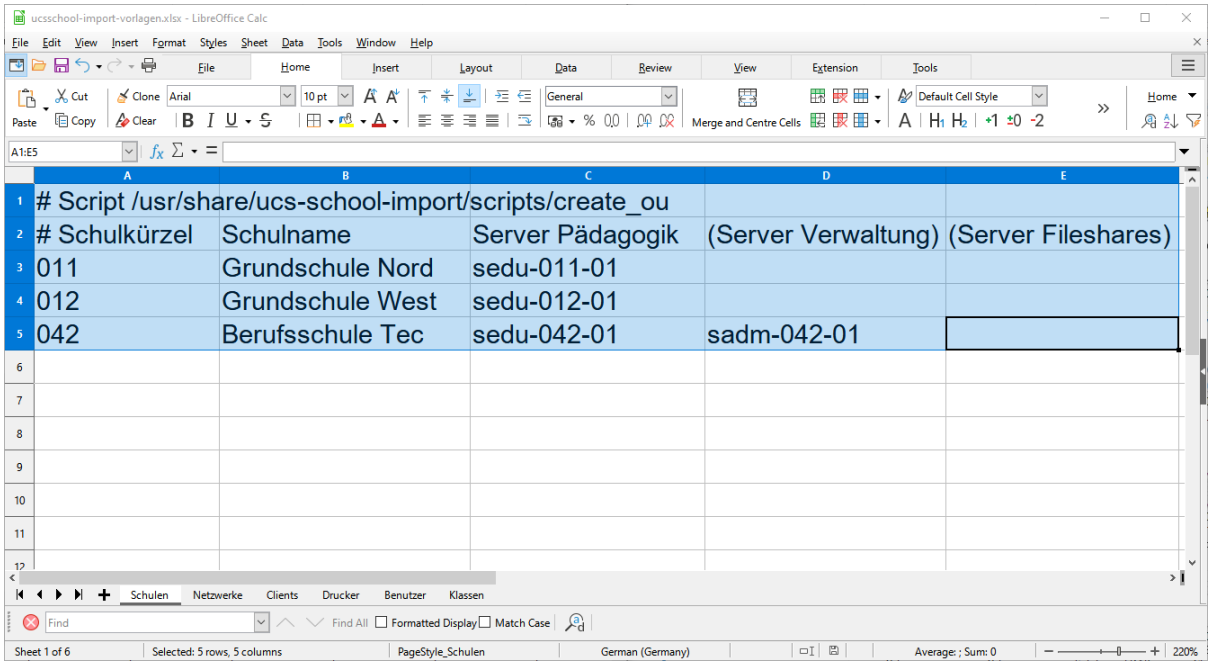


Abb. 8.1: Schulen

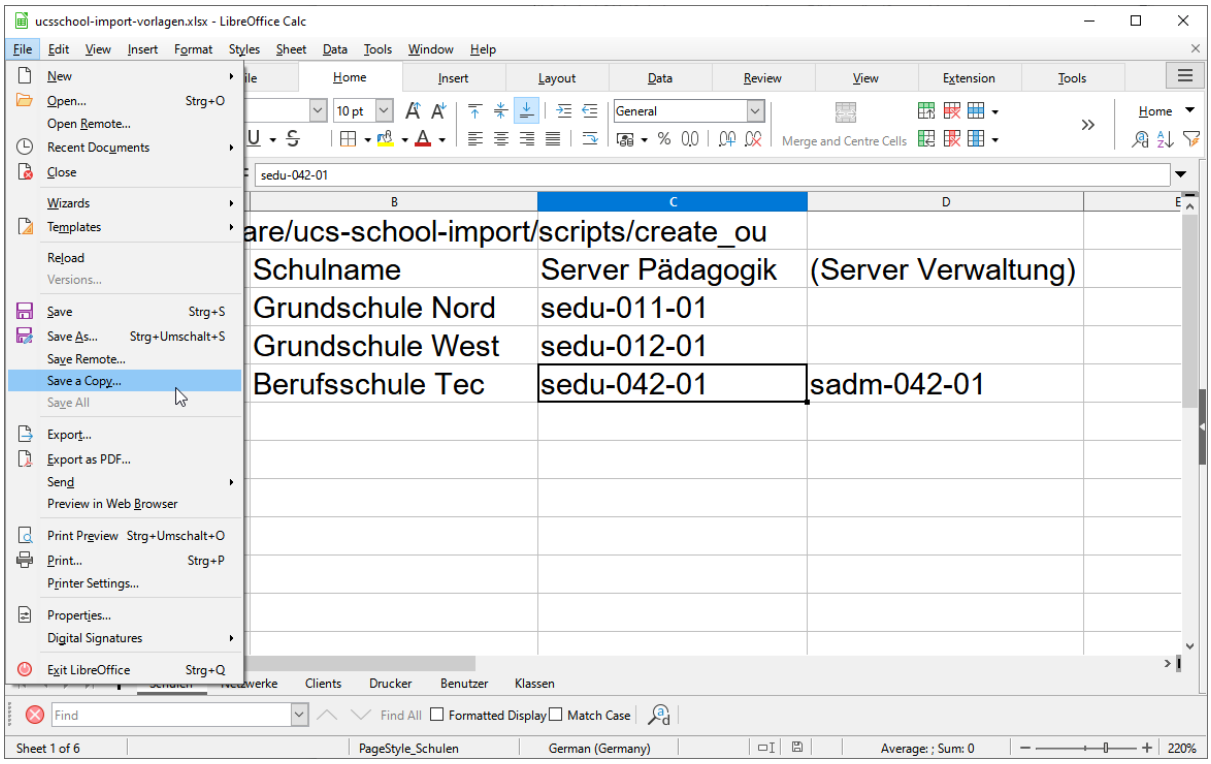


Abb. 8.2: Kopie speichern als CSV-Datei

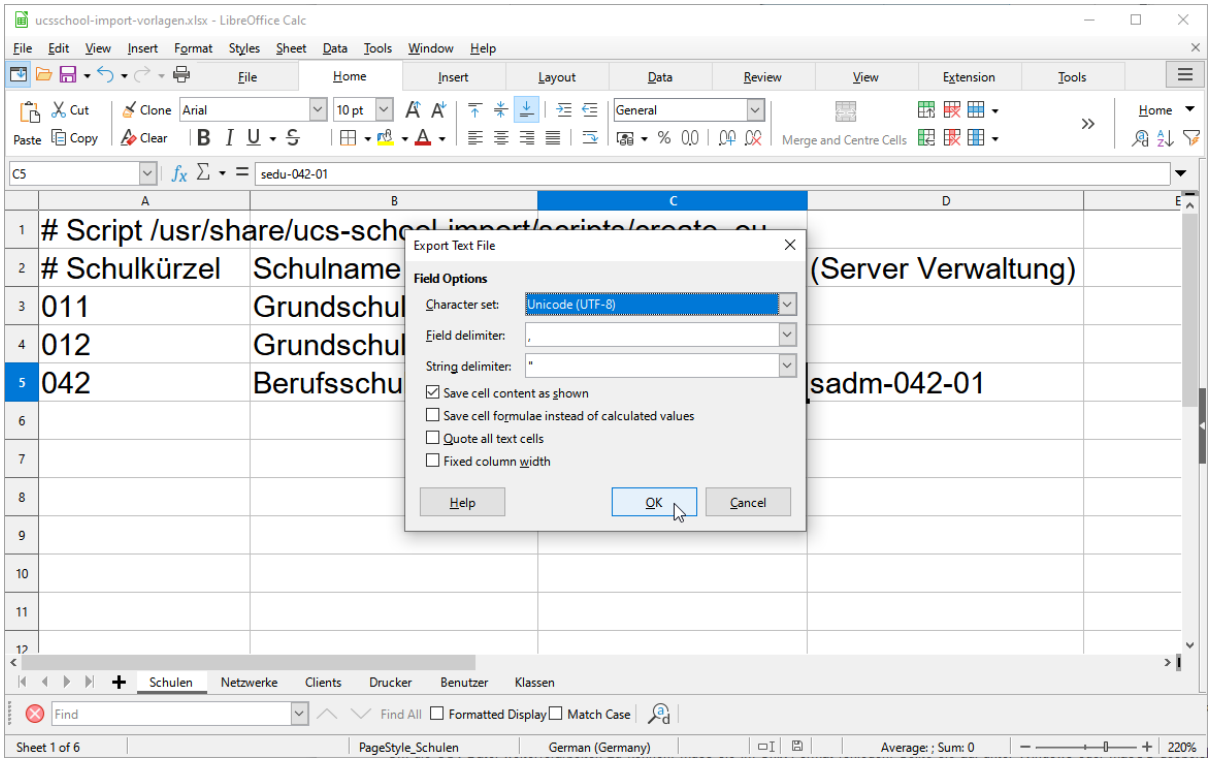


Abb. 8.3: Export Parameter

- Um die CSV-Datei weiterverarbeiten zu können, muss sie im Unix-Format vorliegen. Sollte sie auf unter Windows oder macOS gespeichert worden sein, so muss sie konvertiert werden. Dazu ist auf dem Primary Directory Node der folgende Befehl auf die Datei anzuwenden:

```
$ dos2unix schulen.csv
```

  Vorweg muss das Paket **dos2unix** installiert werden, siehe Konfiguration des Repository-Servers für Updates und Paketinstallationen[12] in *Univention Corporate Server - Handbuch für Benutzer und Administratoren* [2]. Nach der Aktivierung des Repositories ist der folgende Befehl zu Installation des Pakets auszuführen:

```
$ univention-install dos2unix
```

  Alternativ kann die Datei auf dem Primary Directory Node mit dem Texteditor **Vim** geöffnet und dieser zum konvertieren verwendet werden:

```
$ vim schulen.csv
  # In der Vim Befehlszeile:
  :set ff=unix
  :wq
```

- Die CSV-Datei aus der Vorlage enthält noch zwei Kopfzeilen, die mit dem Zeichen # beginnen, diese müssen vor der weiteren Verarbeitung entfernt werden:

```
$ sed -i '1,2d' /usr/local/ucsschool/import_data/schulen.csv
```

- Der Import kann abschließend mit folgendem Befehl ausgeführt werden:

```
$ /usr/share/ucs-school-import/scripts/create_ou \
  --infile=/usr/local/ucsschool/import_data/schulen.csv
```

[12] https://docs.software-univention.de/manual/5.0/de/software/repository-server.html#software-config-repo

## 8.2 Netze

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Der Import der Netze ist notwendig, um Rechner und Server in den Schulen einrichten zu können. Beim Import werden unter anderem passende Richtlinien für DHCP, DNS und Routing erstellt.

Die Netze sind entsprechend der *Netzkonzept* (Seite 15) in eine CSV-Datei einzutragen. In Skriptbasierter Import von Netzwerken[13] in *UCS@school - Handbuch für Administratoren* [3] ist das Datenformat für den Import beschrieben.

In der Datei `ucsschool-import-vorlagen.xlsx` ist eine Vorlage in der Tabelle *Netze* vorhanden, die verwendet werden kann. Es ist zu beachten, dass der Feldtrennzeichen in diesem Fall *Tabulator* sein muss.

Das weitere Vorgehen ist wie folgt:

- Die CSV-Datei `networks.csv` ist auf dem Primary Directory Node in folgendem Verzeichnis abzulegen: `/usr/local/ucsschool/import_data/`.
- Die CSV-Datei aus der Vorlage enthält noch zwei Kopfzeilen, die mit dem Zeichen # beginnen, diese müssen vor der weiteren Verarbeitung entfernt werden:

```
$ sed -i '1,2d' /usr/local/ucsschool/import_data/networks.csv
```

- Der Import kann abschließend mit folgendem Befehl ausgeführt werden:

```
$ /usr/share/ucs-school-import/scripts/import_networks \
    /usr/local/ucsschool/import_data/networks.csv
```

## 8.3 Rechner

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Der Import von Rechnern ist insbesondere notwendig, um die Rechner in den Schulen mit der richtigen MAC-Adresse in UCS@school zu hinterlegen, so dass diese über DHCP konfiguriert und in den UCS@school UMC-Modulen verwendet werden können. Weitere Dienste, wie Softwareverteilungslösungen verwenden diese Informationen ebenfalls weiter.

Das Datenformat der CSV-Datei ist in Import von Rechnerkonten für Windows-PCs[14] in *UCS@school - Handbuch für Administratoren* [3] beschrieben.

Es sollte eine CSV-Datei je Schule erstellt werden, die alle Rechner der jeweiligen Schule entsprechend des Netz- und Namenskonzeptes enthält.

In der Datei `ucsschool-import-vorlagen.xlsx` ist eine Vorlage in der Tabelle *Rechner* vorhanden, die verwendet werden kann. Es ist zu beachten, dass der Feldtrennzeichen in diesem Fall *Tabulator* sein muss.

Das weitere Vorgehen ist wie folgt:

- Die CSV-Datei `computers_SCHULE.csv` ist auf dem Primary Directory Node in folgendem Verzeichnis abzulegen: `/usr/local/ucsschool/import_data/`
- Die CSV-Datei aus der Vorlage enthält noch zwei Kopfzeilen, die mit dem Zeichen # beginnen, diese müssen vor der weiteren Verarbeitung entfernt werden:

[13] https://docs.software-univention.de/ucsschool-manual/5.0/de/manage-school-imports.html#school-schoolcreate-network-import
[14] https://docs.software-univention.de/ucsschool-manual/5.0/de/manage-school-imports.html#school-schoolcreate-computers

```
$ sed -i '1,2d' /usr/local/ucsschool/import_data/computers_SCHULE.csv
```

- Der Import kann abschließend mit folgendem Befehl ausgeführt werden:

```
$ /usr/share/ucs-school-import/scripts/import_computer \
    /usr/local/ucsschool/import_data/computers_SCHULE.csv
```

## 8.4 Drucker

**Gültigkeit**

Für Szenario *3* (Seite 6) und *4* (Seite 6).

Der Import der Drucker ist notwendig, damit für diese automatisch eine entsprechende DNS- und DHCP-Konfiguration vorgenommen wird und die Drucker sofort in der Schule im Netz verfügbar sind.

Das Datenformat der CSV-Datei ist in Konfiguration von Druckern an der Schule[15] in *UCS@school - Handbuch für Administratoren* [3] beschrieben.

In der Datei `ucsschool-import-vorlagen.xlsx` ist eine Vorlage in der Tabelle *Drucker* vorhanden, die verwendet werden kann. Es ist zu beachten, dass der Feldtrennzeichen in diesem Fall *Tabulator* sein muss.

Das weitere Vorgehen ist wie folgt:

- Die CSV-Datei `printers.csv` ist auf dem Primary Directory Node in folgendem Verzeichnis abzulegen: `/usr/local/ucsschool/import_data/`
- Die CSV-Datei aus der Vorlage enthält noch zwei Kopfzeilen, die mit dem Zeichen `#` beginnen, diese müssen vor der weiteren Verarbeitung entfernt werden:

```
$ sed -i '1,2d' /usr/local/ucsschool/import_data/printers.csv
```

- Der Import kann abschließend mit folgendem Befehl ausgeführt werden:

```
$ /usr/share/ucs-school-import/scripts/import_printer \
    /usr/local/ucsschool/import_data/printers.csv
```

## 8.5 Benutzer / Klassen

**Gültigkeit**

Für *alle* (Seite 3) Szenarien.

Für UCS@school gibt es momentan mehrere Möglichkeiten Nutzer und Klassen in das System zu importieren.

Die Konfiguration des kommandozeilenbasierten Benutzerimports ist in *UCS@school - Handbuch zur CLI-Import-Schnittstelle* [1] dokumentiert.

Die Einrichtung und Verwendung des zugehörigen Univention Management Console Moduls ist in Installation, Konfiguration und Dateiformat[16] in *UCS@school - Handbuch für den grafischen Benutzer-Import* [4] nachzulesen.

[15] https://docs.software-univention.de/ucsschool-manual/5.0/de/manage-school-imports.html#school-setup-cli-printers
[16] https://docs.software-univention.de/ucsschool-umc-user-import/5.0/de/install.html#install-conf-format

# Literaturverzeichnis


[1] *UCS@school - Handbuch zur CLI-Import-Schnittstelle*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-import/5.0/de/index.html.

[2] *Univention Corporate Server - Handbuch für Benutzer und Administratoren*. Univention GmbH, 2021. URL: https://docs.software-univention.de/manual/5.0/de/.

[3] *UCS@school - Handbuch für Administratoren*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-manual/5.0/de/index.html.

[4] *UCS@school - Handbuch für den grafischen Benutzer-Import*. Univention GmbH, 2021. URL: https://docs.software-univention.de/ucsschool-umc-user-import/5.0/de/index.html.

# Stichwortverzeichnis