

Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Installationsanleitung

Installation der VM Nextcloud für paedML® Windows und OctoGate

Stand 24.11.2021 / V 1.0.0

paedML® Windows

Version: 4.x

Impressum

Herausgeber

Landesmedienzentrum Baden-Württemberg (LMZ)
Support-Netz
Rotenbergstraße 111
70190 Stuttgart

Autoren

der Zentralen Expertengruppe Netze (ZEN),
Support-Netz, LMZ

Martin Ewest
Markus Finkenbein
Ulrich Hollritt
Soo-Dong Kim
Antonius Schnetter

Endredaktion

Redaktion Support Netz

Bildnachweis Symbole Titelseite

CC By 3.0 US von Gregor Cresnar, The Noun Project

Weitere Informationen

www.support-netz.de
www.lmz-bw.de

Änderungen und Irrtümer vorbehalten.

Veröffentlicht: 2021

Die Nutzung dieses Handbuches ist ausschließlich für eigene Zwecke zulässig. Die Nutzung sowie die Weitergabe dieses Handbuches zu kommerziellen Zwecken wie z.B. Schulungen ist nur nach ausdrücklicher Einwilligung durch das LMZ erlaubt.

© Landesmedienzentrum Baden-Württemberg

Inhaltsverzeichnis

1	Einführung	7
1.1	Zweck des Handbuchs	7
1.2	Zielgruppe	7
1.3	Typografische Konventionen	7
1.4	Systemvoraussetzungen.....	8
1.5	Hinweise zum technischen Support.....	9
1.6	LMZ-Nextcloud-Helferskript.zip herunterladen	9
1.7	Weiterführende Dokumentationen	10
2	DMZ einrichten	11
2.1	Einen virtuellen Switch (vSwitch) Hinzufügen	11
2.1.1	Standard-Switch ohne Uplink.....	12
2.1.2	Standard-Switch mit Uplink.....	13
2.2	Portgruppe hinzufügen	13
3	Import der Nextcloud-VM	15
3.1	Nextcloud-VM importieren.....	15
3.2	[Optional] Einstellungen der Nextcloud-VM bearbeiten	19
3.3	Snapshot erstellen	19
3.4	Nextcloud-VM hochfahren	20
4	OctoGate anpassen	21
4.1	Firmware kontrollieren und ggf. aktualisieren	21
4.2	OctoGate an DMZ-Netz anschließen.....	21
4.3	Kontrolle der Firewall-Regeln	26
5	LDAPS-Zertifikat	28
5.1	LDAPS-Zertifikat ermitteln.....	28
5.2	LDAPS einrichten	35
5.3	Kontrolle.....	36
6	Initialisierung der Nextcloud	39
6.1	Anpassungen in AD und DNS.....	39
6.1.1	Keine LDAPS-Konfiguration	40
6.1.2	LDAPS mit dem PowerShell-Skript New-paedMLCAOnDC.ps1 eingerichtet	40
6.1.3	LDAPS mit eigenem Hostzertifikat	41
6.1.4	LDAPS mit OctoGate-Zertifikat	43
6.2	Nextcloud-VM initialisieren.....	44

6.3	UCS-Zertifikat importieren.....	46
7	Abschlussarbeiten	47
7.1	Quota für alle Benutzer setzen.....	47
7.2	Tauschlaufwerke für Schülerinnen und Schüler freigeben.....	47
7.3	App Center App Let's Encrypt aktualisieren.....	48
7.4	Zertifikatdateien bereinigen.....	52
7.5	Snapshot bereinigen, falls vorhanden.....	52
8	Backup	53
Anhang A Nützliche Ergänzungen.....		54
A.1	Verknüpfung auf Client-Desktops.....	54
A.2	Desktop-Verknüpfung deaktivieren	54
A.3	Desktopverknüpfung mit dem externen FQDN anlegen.....	55
Anhang B FAQ.....		57
B.1	Welche Angaben muss ich zwingend nennen, damit meine Supportanfrage an support@octogate.de zügig bearbeitet werden kann?	57
B.2	Trouble-Shooting: Octogate.....	58
B.2.1	Wie bzw. wo finde ich die Firmware-Version meiner OctoGate Firewall?.....	58
B.2.2	Meine OctoGate Firewall läuft mit einer älteren Firmware-Version. An wen muss ich mich wenden, um sie auf die Version 3.0.51 oder höher aktualisieren zu können?.....	58
B.2.3	Abweichende IP-Adresse von eth1	58
B.3	LDAP/LDAPS.....	59
B.3.1	Obwohl LDAPS eingerichtet ist, findet das Skript Get-LDAPSCertificate.ps1 keine LDAPS-Konfiguration	59
B.3.2	Mein LDAPS-Zertifikat konnte nicht auf die Nextcloud-VM kopiert werden. Wo muss ich sie manuell kopieren?	61
B.4	Eigene externe Domäne verwenden.....	61
B.5	Nextcloud-Provisioning.....	65
B.5.1	Warum muss ein PING-Check gegen die IP-Adresse meiner Firewall gemacht werden?...65	
B.5.2	Was kann ich tun, damit meine OctoGate-Firewall eine Ping-Anfrage aus der Nextcloud-VM akzeptiert?	66
B.5.3	Wie kann ich externe Domäne korrigieren und Let's Encrypt Zertifikat installieren?.....	66
B.5.4	Gibt es einen <i>Shortcut</i> für den OCC-Befehl?	67
B.6	Nextcloud.....	68
B.6.1	Anmeldung in Nextcloud wird verzögert bzw. ist oft nicht möglich.	68
B.6.2	Quota-Einschränkung für Benutzer nc_admin aufheben	70
B.6.3	Wie kann ich prüfen, ob die Nextcloud-VM die Uhrzeit von OctoGate bezieht?.....	72
Anhang C LDAPS einrichten mit OctoGate-Zertifikat.....		74

Anhang D	Known-Issues	83
D.1	OnlyOffice kann nur im Schulnetz benutzt werden.....	83
D.2	Systemdiagnose gibt eine Warnmeldung für Dateiberechtigungen aus.....	83
D.3	Benutzer können sich nicht anmelden, nachdem Imz-initial-skript ein weiteres Mal ausgeführt wurde.....	83
D.4	UCS Systemdiagnose meldet einen kritischen Fehler bzgl. SAML-Zertifikate	84
9	Änderungsdokumentation	85

Vorwort

Zielgruppe	Schwierigkeitsgrad
Händler, Dienstleister, Administratoren	Für fortgeschrittene Anwender

Das [Landesmedienzentrum Baden-Württemberg](#) stellt ab sofort allen Schulen, die paedML® Windows erworben haben und als pädagogische Musterlösung einsetzen, die Nextcloud als eine Erweiterung zur paedML® Windows bereit. Sie wird als eine vorkonfigurierte VM-Vorlage zum Download angeboten, die Sie als eine virtuelle Maschine (kurz VM) auf Ihrem bestehenden vSphere ESXi-Host installieren können.

Die Erweiterung durch Nextcloud in der paedML® Windows ermöglicht einen komfortablen Zugriff auf die in der Schule bekannten Verzeichnisse (Laufwerke H:\, T:\ und für Lehrer zusätzlich S:\) von außerhalb des pädagogischen Netzwerks. So können z. B. Dateien, die später im Unterricht gebraucht werden, bereits von zu Hause aus in das eigene Home-Verzeichnis oder in den Tauschordner auf dem Schulserver hinterlegt werden.

Mit Geräten, die nicht oder nicht vollständig in die paedML® Windows integriert sind, kann somit leichter auf die Laufwerke der paedML zugegriffen werden. Daten können heruntergeladen, verarbeitet und hochgeladen werden. Damit ist eine Be- und Verarbeitung von Daten mit schuleigenen und privaten Geräten in und außerhalb der Schule möglich.

Da diese Nextcloud im eigenen pädagogischen Netz der Schule bzw. des Schulträgers betrieben wird, hat die Schule die alleinige Kontrolle über die in der Nextcloud gespeicherten Daten.

Benutzername und Kennwort sind in der Nextcloud identisch mit denen in der pädagogischen Umgebung der Schule. Es werden keine separaten Benutzerkonten für die Anmeldung und Nutzung des Nextcloud angelegt.

Wie bei jeder Cloudlösung kann eine langsame Internetverbindung das Arbeiten mit Nextcloud massiv beeinträchtigen. Das gilt bei einem Zugriff von zu Hause für die private Internetverbindung, vor allem aber für die Internetverbindung des Schulservers.



Aufgrund der besseren Lesbarkeit wird in diesem Handbuch meist nur die männliche Form (generisches Maskulinum) verwendet. Die weibliche Form ist selbstverständlich immer mit eingeschlossen.

1 Einführung

1.1 Zweck des Handbuchs

Die Nextcloud der [paedML® Windows](#) ist eine vom [Landesmedienzentrum Baden-Württemberg](#) (kurz LMZ) vorkonfigurierte Nextcloud. Diese kann mit geringem Aufwand für die Administratoren installiert und betrieben werden. Es sind nur diejenigen Nextcloud-Apps aktiviert, die wir für den Einsatz in Kombination mit einer paedML® für sinnvoll halten.

Im vorliegenden Handbuch beschreiben wir, wie Sie unsere VM-Vorlage bereitstellen und konfigurieren. Das umfasst:

1. Anpassung der Firewall
2. LDAP-SSL (LDAPS) einrichten
3. Import der VM-Vorlage
4. Initialisierung der Nextcloud

1.2 Zielgruppe

Das vorliegende Handbuch ist geeignet für:

- Dienstleister
- Erfahrene Administratoren

Kenntnisse über die Funktionsweise und die Administration mit [VMware vSphere](#) setzen wir voraus. Darüber hinaus sind Kenntnisse über Linux sehr hilfreich, da unsere VM-Vorlage auf der Linux-Distribution [Univention Corporate Server](#) (kurz UCS) basiert, die auch die Basis unseres Schwesterprodukts [paedML® Linux](#) bildet.

1.3 Typografische Konventionen

Zur besseren Lesbarkeit werden in unseren Handbüchern bestimmte Elemente typografisch vom Rest des Textes abgehoben.

- *Hervorhebungen* und *Eigennamen* in diesem Dokument sind kursiv gekennzeichnet.
- **Hervorhebungen** sind fett ausgezeichnet.
- **Ausgaben** oder **Abfragen von Programmen**, sowie **Zitate** sind fett und kursiv gekennzeichnet.
- Ausführbare Dateien und vom Benutzer auszuführende Tastatureingaben an Konsolen (wie Login-Daten, Befehle sowie Programm-Code) werden durch die Darstellung in `Courier New` vom Rest des Textes abgesetzt.
- Dateinamen und Laufwerkspfade werden ebenfalls durch die Darstellung in `Courier New` vom Rest des Textes abgesetzt.
- Schaltflächen und Tastenbeschriftungen werden durch Rahmen hervorgehoben.
- [Internet-Links](#) und [Querverweise](#) in diesem Dokument sind blau formatiert. Durch Anklicken können Sie an das dort hinterlegte Ziel springen.

- Rahmen in Abbildungen:
Magenta/Rot: Hervorheben der im Anleitungstext benannten Stellen
GRÜN: Hinweis auf verwendete Filter in der Schulkonsole ODER weitere Hervorhebung in einer Abbildung

Hinweise und Tipps werden durch besondere Symbole gekennzeichnet und grafisch vom Text abgehoben:



Durch Hinweisfelder werden Sie auf bestimmte Gegebenheiten hingewiesen, deren Missachtung Probleme verursachen können. Die Nutzung eines Programms kann dadurch beeinträchtigt werden.



Dieses Feld kennzeichnet Inhalte, die nicht von der Hotline unterstützt werden.

Es handelt sich um Funktionen und Programme, die nicht Bestandteil der Entwicklung der paedML® Windows sind. Diese Programme sind in der Regel zu komplex und zu umfangreich, um in Ihrer Tiefe durch die Hotline unterstützt werden zu können.

Andererseits bewirken Änderungen in den beschriebenen Funktionen Abweichungen von Standardeinstellungen der paedML® Windows.



Das Tipp-Feld gibt Hinweise, die nicht zwingend notwendig, aber hilfreich sind.

1.4 Systemvoraussetzungen

Für die Inbetriebnahme der Nextcloud-VM gelten folgende Systemvoraussetzungen:

- **vSphere ESXi 6.5 oder höher**
 Unsere VM-Vorlage ist kompatibel zur VM-Version 13. Die VM-Version 13 wird ab VMware vSphere ESXi 6.5 oder höher unterstützt.
- **Ein dedizierter virtueller Switch für das Netzwerk DMZ (192.168.201.0/24)**
 Die Nextcloud-VM wird in einem eigenen Netzwerksegment betrieben. Weitere Details dazu entnehmen Sie aus dem [Kapitel 2 DMZ einrichten](#).
- **paedML® Windows 3.1.1 oder paedML® Windows 4.x**
- **OctoGate 3.0.51 oder höher**
 Die Firmware-Version 3.0.51 unseres Kooperationspartners, [OctoGate IT Security Systems GmbH](#), enthält alle für den Betrieb der Nextcloud-VM notwendigen Firewall-Regeln. Sie müssen jedoch die Konfigurationsanpassungen aus den beiden [Kapiteln 2 DMZ einrichten](#) und [4 OctoGate anpassen](#) vornehmen und vor allem die Netzwerkschnittstelle DMZ Ihrer OctoGate-Firewall durch den technischen Support der Firma OctoGate IT Security Systems GmbH aktivieren lassen.
- **Serverzertifikat für LDAPS**
 Wir empfehlen dringend, für die Benutzerauthentifizierung auf LDAPS (verschlüsselte Übertragung der Benutzerdaten) umzustellen. Dafür wird ein Serverzertifikat benötigt. Weitere Details finden Sie im [Kapitel 5 LDAPS-Zertifikat](#).

- **MLI-Nummer und das zur MLI-Nummer zugehörige Kennwort**
Während der Initialisierung der Nextcloud-VM müssen Sie Ihre MLI-Nummer und das zugehörige Kennwort hinterlegen. Diese Informationen sind zwingend erforderlich, damit Ihre Nextcloud-VM Updates aus dem Univenton-Repository beziehen und installieren kann.



Die Nextcloud-VM hat die statische IP-Adresse 192.168.201.7/24. Diese darf nicht geändert werden.

Aus dem Grund muss die Adresse des Netzwerks DMZ 192.168.201.0/24 festgelegt sein.

1.5 Hinweise zum technischen Support

Trotz sorgfältiger Testreihen können wir Störungen während der Installation der Nextcloud nicht gänzlich ausschließen. Wir bieten Ihnen daher:

- Hilfestellung zum Inhalt des Handbuchs
- Unterstützung beim Umsetzen der im Handbuch beschriebenen Arbeitsschritte
- Unterstützung zur Behebung von Störungen, die während der Bereitstellung der VM-Vorlage auftreten, zum Beispiel durch defekte Download-Dateien
- Unterstützung zur Behebung von Störungen, die durch Missverständnisse bezüglich der Firewall-Konfiguration entstehen
- Unterstützung der LDAPS-Konfiguration
- Unterstützung zur Behebung von Störungen, die während der Initialisierung der Nextcloud auftreten

Wir weisen Sie an einigen Stellen im Handbuch daraufhin, dass für ein bestimmtes Feature beziehungsweise für eine Konfigurationsänderung kein technischer Support möglich ist.

Im Allgemeinen gilt: Für Störungen, die durch Ihre individuellen Änderungen oder durch das Missachten der von uns genannten Voraussetzungen auftreten, können wir **keinen technischen Support bieten!**



Dazu gehören zum Beispiel:

- **Konvertieren der VM-Vorlage für eine ESXi-Version, die älter ist als die in diesem Kapitel genannte Minimalversion**
- **Konvertieren und Bereitstellen unserer VM-Vorlage auf einem alternativen Hypervisor**
- **Ändern der IP-Adresse der Nextcloud-VM**
- **Störungen, die durch die Installation einer Nextcloud-App aus nicht geprüfter Quelle verursacht werden**
- **Störungen, die durch eine von uns nicht unterstützte Firewall auftreten**

1.6 LMZ-Nextcloud-Helferskript.zip herunterladen

Laden Sie zunächst die Datei **LMZ-Nextcloud-Helferskripte.zip** aus unserem Download-Portal herunter.



Falls Sie die Datei direkt auf dem Server SP01 herunterladen, sollten Sie die Datei zur Ausführung zulassen. Sonst wird die Ausführung des PowerShell-Skripts zunächst unterbunden und Sie werden aufgefordert, der Ausführung des aus dem Internet heruntergeladenen Skripts ausdrücklich zuzustimmen.

Öffnen Sie die Eigenschaften der Datei `LMZ-Nextcloud-Helferskript.zip` und setzen Sie ein Häkchen bei Zulassen.

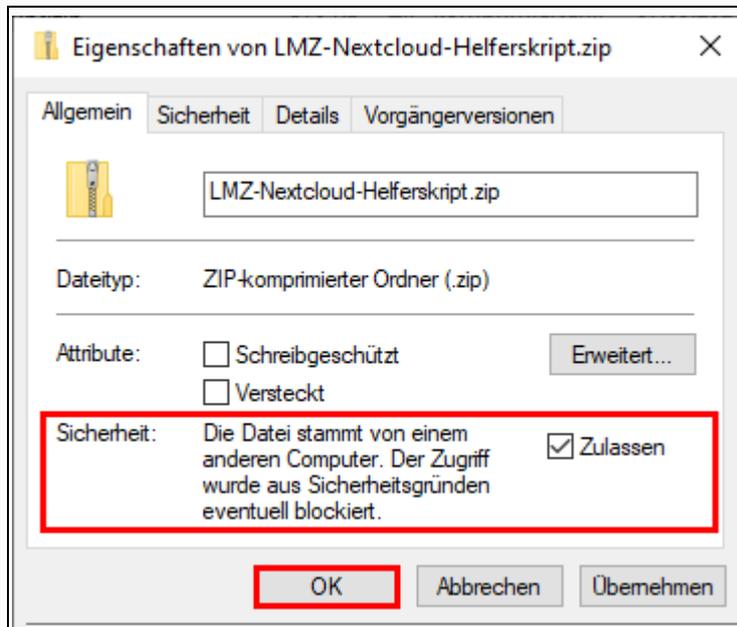


Abb. 1: Portgruppe hinzufügen > Eigenschaften definieren

Entpacken Sie die Datei und kopieren Sie anschließend die ausführbare Datei `LMZ-Nextcloud.exe` nach SP01 und entpacken Sie das Archiv mit einem Doppelklick auf `LMZ-Nextcloud.exe`.

Die so entpackten Dateien befinden sich im Ordner `D:\Installation\paedML\Erweiterungen\Nextcloud` und kommen in den [Kapiteln 5 LDAPS-Zertifikat](#) und [6 Initialisierung der Nextcloud](#) zum Einsatz.

1.7 Weiterführende Dokumentationen

- Handbuch für Administratoren – Nextcloud in der paedML® Windows
- Benutzerhandbuch – Nextcloud in der paedML® Windows
- Hersteller-Doku zu Nextcloud

2 DMZ einrichten

2.1 Einen virtuellen Switch (vSwitch) Hinzufügen



Es wird nur das Hinzufügen eines virtuellen Standard-Switches beschrieben. Falls Sie sich für das Einrichten eines Distributed Switches interessieren, wenden Sie sich an Ihren Dienstleister oder lesen Sie in der Herstellerdokumentation nach.

Wenn Sie bereits einen vSwitch für DMZ eingerichtet haben, dann können Sie dieses Kapitel überspringen.

Es gibt zwei Möglichkeiten einen virtuellen Standard-Switch hinzuzufügen:

- **Der Switch wird mit einer Netzwerkschnittstelle gekoppelt.**

In diesem Fall weisen Sie dem virtuellen Switch eine physische Netzwerkschnittstelle zu. Dadurch können Sie weitere Geräte – physische wie auch virtuelle – an diesem Switch anschließen. Wenn Sie beispielsweise beabsichtigen, weitere Hosts – eigener Webserver, NAS usw. – ebenfalls in Ihrem DMZ zu betreiben, sollten Sie sich für diese Möglichkeit entscheiden.

- **Der Switch besitzt keine Netzwerkschnittstelle.**

Wenn die Nextcloud-VM der einzige Dienst ist, den Sie in Ihrem DMZ bereitstellen wollen, dann muss der virtuelle Switch über keine physische Netzwerkschnittstelle verfügen. Bei Bedarf lässt sich diese später noch hinzufügen.

1. Öffnen Sie den **Webclient Ihres ESXi-Hosts** in einem Browser und melden Sie sich als **Administrator** bzw. als Benutzer **root** an.
2. Klicken Sie auf den Link **Netzwerk**.



Abb. 2: vSphere Webclient > Netzwerk

3. Klicken Sie auf die Registerkarte **Virtuelle Switches** und anschließend auf den Button **Virtuellen Standard-Switch hinzufügen**.

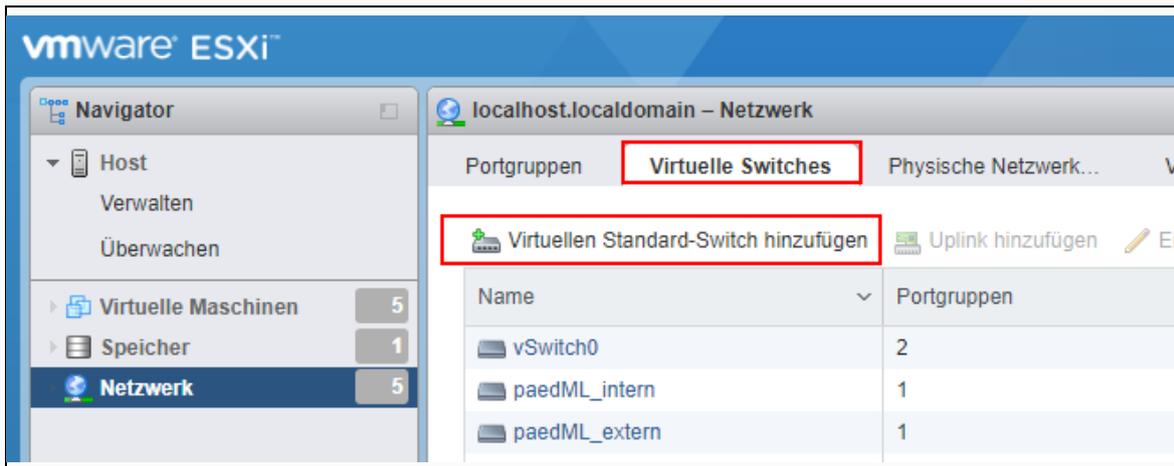


Abb. 3: vSphere Webclient > Netzwerk > Virtuelle Switches > Standard-Switch hinzufügen

2.1.1 Standard-Switch ohne Uplink

Entfernen Sie das Auswahlfeld Uplink, falls es wie in der folgenden Abbildung dargestellt zu sehen ist. Klicken Sie dazu auf das -Symbol.



Abb. 4: Virtueller Standard-Switch ohne Uplink

Geben Sie dem virtuellen Switch einen aussagekräftigen Namen, zum Beispiel *paedML_DMZ*. Klicken Sie auf **Hinzufügen**, um den Vorgang abzuschließen.



Abb. 5: Virtueller Standard-Switch ohne Uplink

2.1.2 Standard-Switch mit Uplink

Geben Sie dem virtuellen Switch einen aussagekräftigen Namen, zum Beispiel *paedML_DMZ*. Wählen Sie außerdem für **Uplink 1** diejenige Netzwerkschnittstelle aus, die Sie für ihn vorgesehen haben. Klicken Sie auf **Hinzufügen**, um den Vorgang abzuschließen.



Das Auswahlfeld Uplink 1 erscheint nur dann, wenn Ihr ESXi-Host über mindestens eine freierverfügbare Netzwerkschnittstelle verfügt.

Um einen virtuellen Standard-Switch mit Uplink – d.h. einer Netzwerkschnittstelle – hinzufügen zu können, müssen Sie demnach vorher für eine frei verfügbare Netzwerkschnittstelle gesorgt haben.

Virtuellen Standard-Switch hinzufügen - paedML_DMZ

Uplink hinzufügen

vSwitch-Name	paedML_DMZ
MTU	1500
Uplink 1	vmnic5 - Betriebsbereit, 1000 mbps
Verbindungserkennung	Klicken Sie zum Erweitern
Sicherheit	Klicken Sie zum Erweitern

Hinzufügen Abbrechen

Abb. 6: Virtueller Standard-Switch mit Uplink

2.2 Portgruppe hinzufügen

Der im [Kapitel 2.1 Einen virtuellen Switch \(vSwitch\) Hinzufügen](#) hinzugefügte Switch muss mit einer Portgruppe verknüpft werden, damit Sie die Nextcloud-VM mit diesem Switch verbinden können.

1. Wechseln Sie zur Registerkarte **Portgruppen** und klicken Sie auf den Button **Portgruppe hinzufügen**.

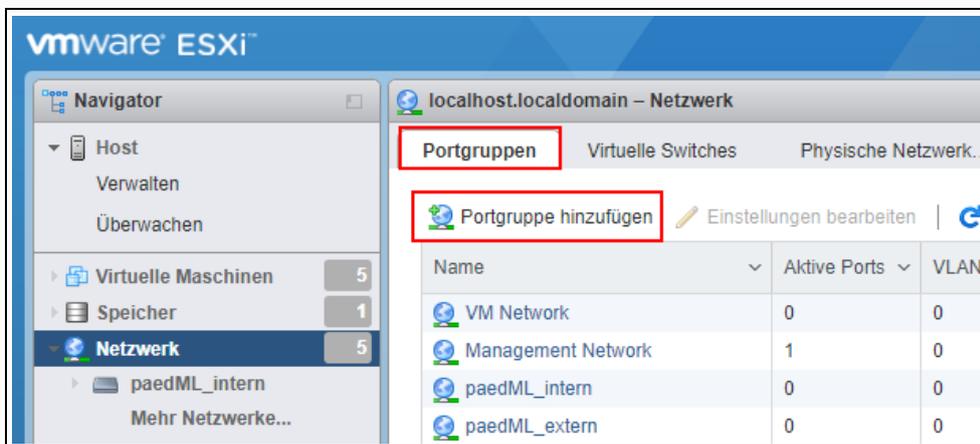
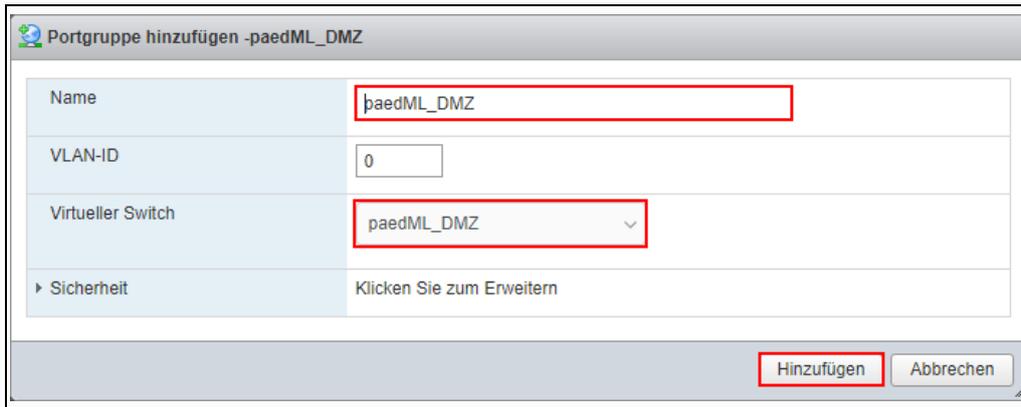


Abb. 7: vSphere Webclient > Netzwerk > Portgruppe hinzufügen

2. Geben Sie der Portgruppe eine aussagekräftige Bezeichnung und weisen Sie ihr den im [Kapitel 2.1](#) hinzugefügten Switch zu.



Portgruppe hinzufügen -paedML_DMZ	
Name	paedML_DMZ
VLAN-ID	0
Virtueller Switch	paedML_DMZ
▶ Sicherheit	Klicken Sie zum Erweitern

Hinzufügen Abbrechen

Abb. 8: Portgruppe hinzufügen > Eigenschaften definieren

3. Klicken Sie auf **Hinzufügen**, um den Vorgang abzuschließen.

3 Import der Nextcloud-VM



Die nachfolgenden Schritte beschreiben den Import der Nextcloud-VM aus der OVF-Vorlage und das Bearbeiten der VM-Einstellungen unter Verwendung des Webclient des vSphere ESXi Hypervisors ab Version 6.5.

Die Darstellung sowie die Bedienung der Oberfläche unterscheidet sich deshalb von einem vCenter Webclient. Inhaltliche Unterschiede sollte es jedoch nicht geben.

3.1 Nextcloud-VM importieren

1. Öffnen Sie den Webclient Ihres ESXI-Hosts und melden Sie sich als Benutzer Administrator oder als Benutzer root an.
2. Klicken Sie auf den Link **Virtuelle Maschinen** und anschließend auf **VM erstellen/registrieren**.

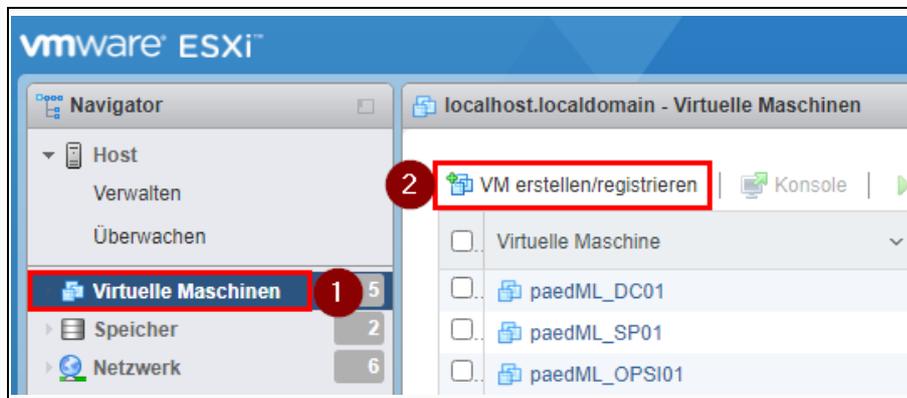


Abb. 9: Virtuelle Maschine erstellen

3. Wählen Sie die Aktion **Eine virtuelle Maschine aus einer OVF- oder OVA-Datei...** aus und klicken Sie auf **Weiter**.

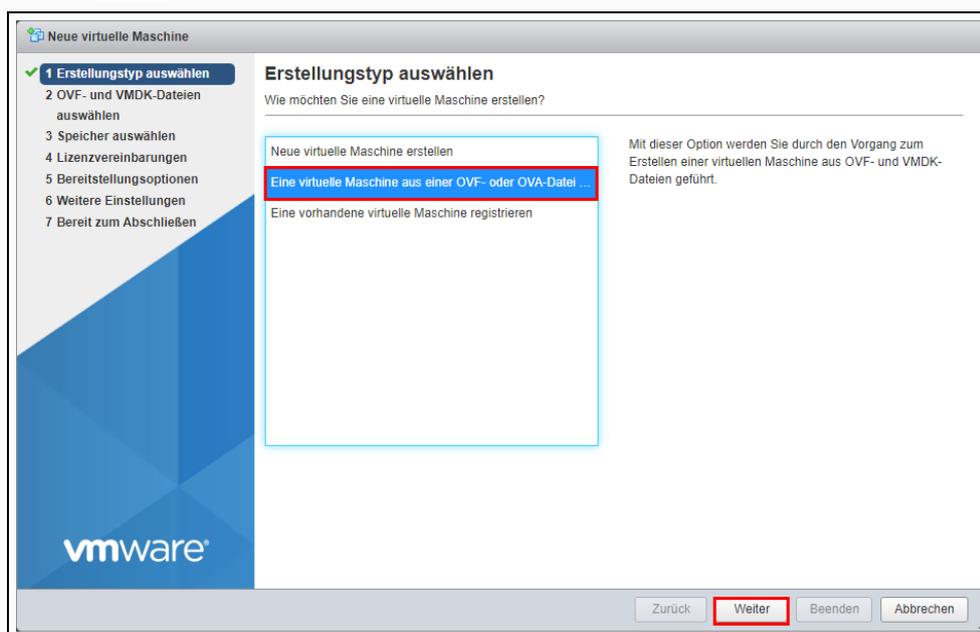


Abb. 10: VM aus einer OVF- oder OVA-Datei auswählen

4. Geben Sie Ihrer Nextcloud-VM einen Namen, zum Beispiel {Kürzel Ihrer Schule}_Nextcloud.

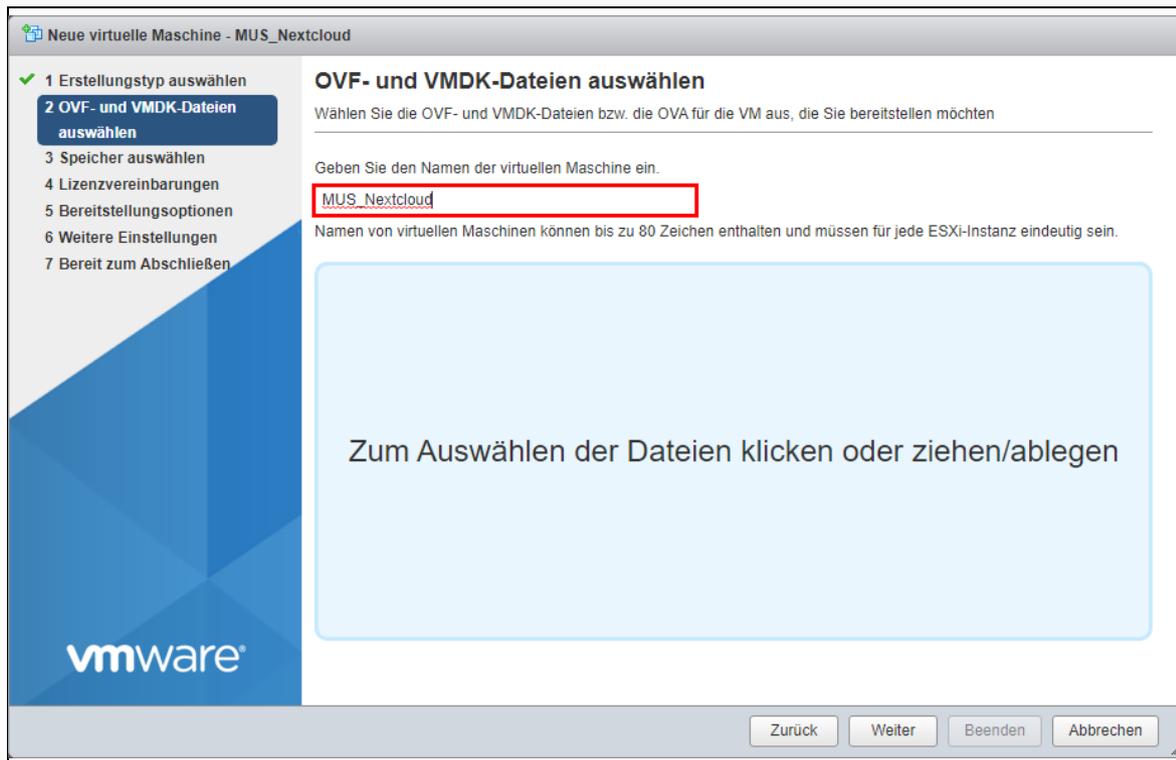


Abb. 11: VM aus einer OVF- oder OVA-Datei auswählen

5. Klicken Sie auf die Schaltfläche **Zum Auswählen der Dateien klicken oder ziehen/ablegen**.

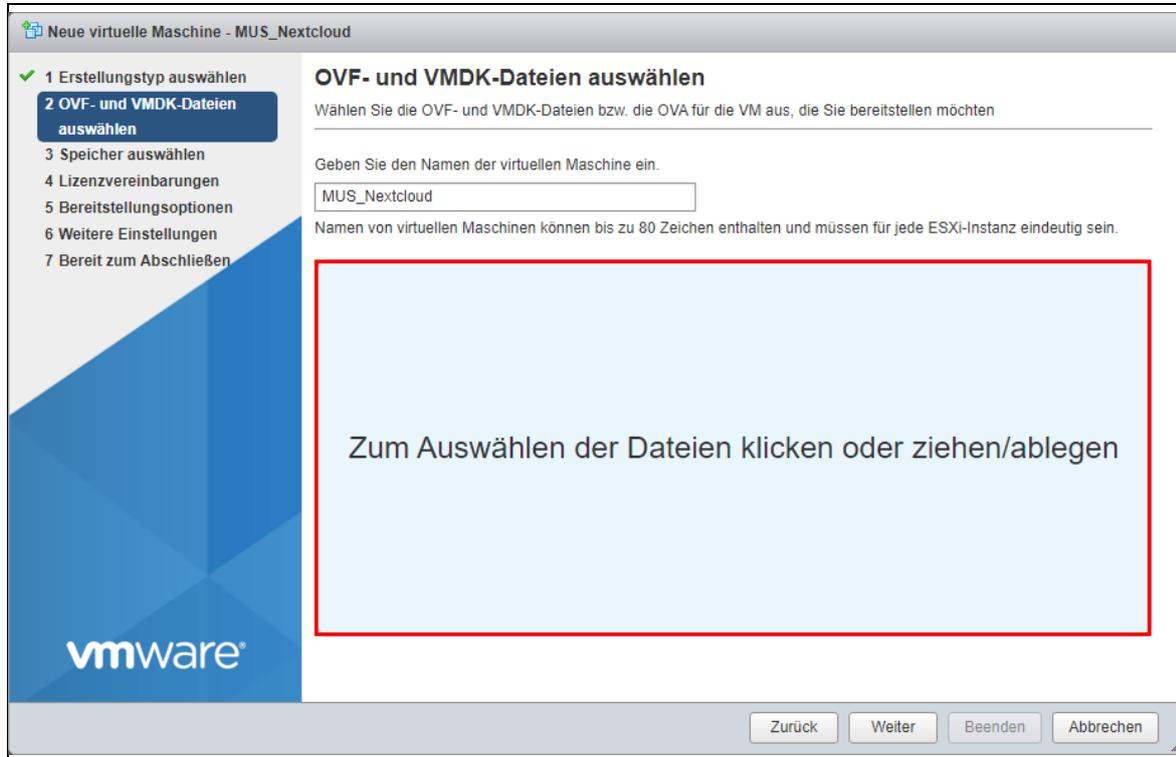


Abb. 12: VM aus einer OVF- oder OVA-Datei auswählen

6. Navigieren Sie im Datei-Explorer in den Ordner, in dem sich die entpackten Dateien der VM-Vorlage befinden. **Wählen Sie alle Dateien aus und klicken Sie auf Öffnen.**

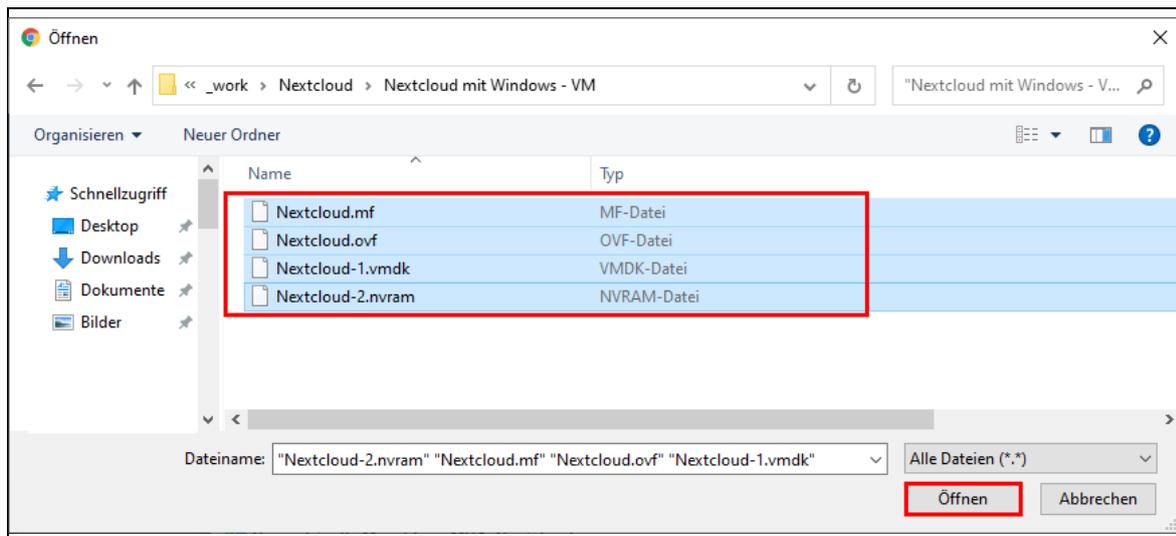


Abb. 13: Benötigte Dateien markieren und öffnen

7. Kontrollieren Sie, ob **alle** Dateien **außer Nextcloud.mf** aufgelistet werden und klicken Sie auf Weiter.

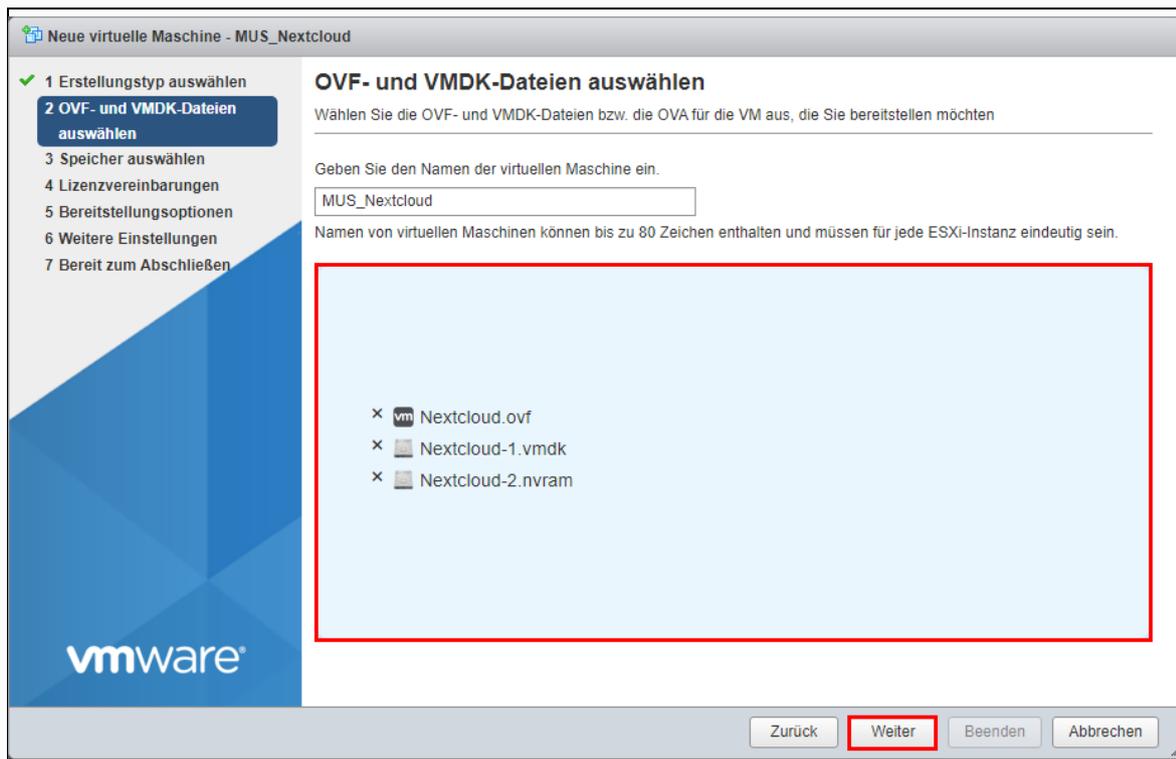


Abb. 14: Name der VM festlegen

8. Wählen Sie den Datastore aus, in den Sie die Nextcloud kopieren wollen, und klicken Sie auf **Weiter**.

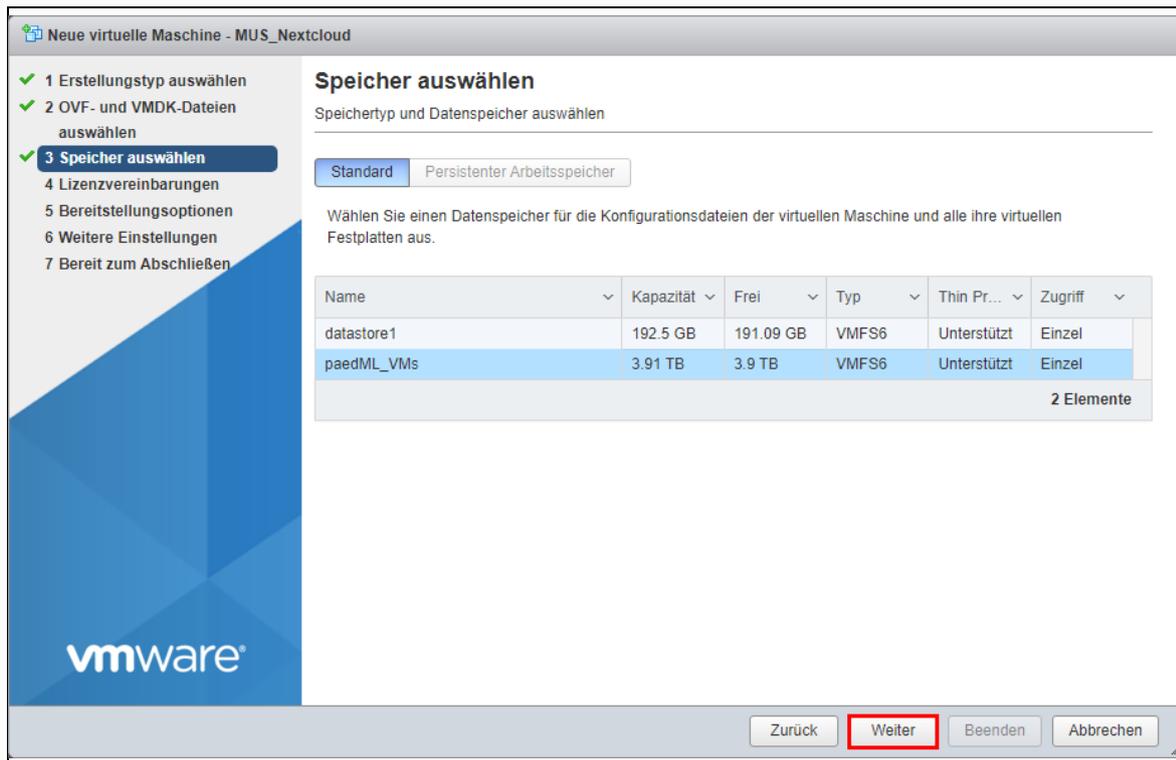


Abb. 15: Speicher auswählen

9. Ordnen Sie der VM das Netzwerk für DMZ zu. Wenn Sie unserem Namensvorschlag gefolgt sind, dann lautet der Name des Netzwerks *paedML_DMZ*. Setzen Sie Festplattenbereitstellung auf **Thick** und entfernen Sie das Häkchen bei **Automatisch einschalten**. Klicken Sie danach auf **Weiter**.

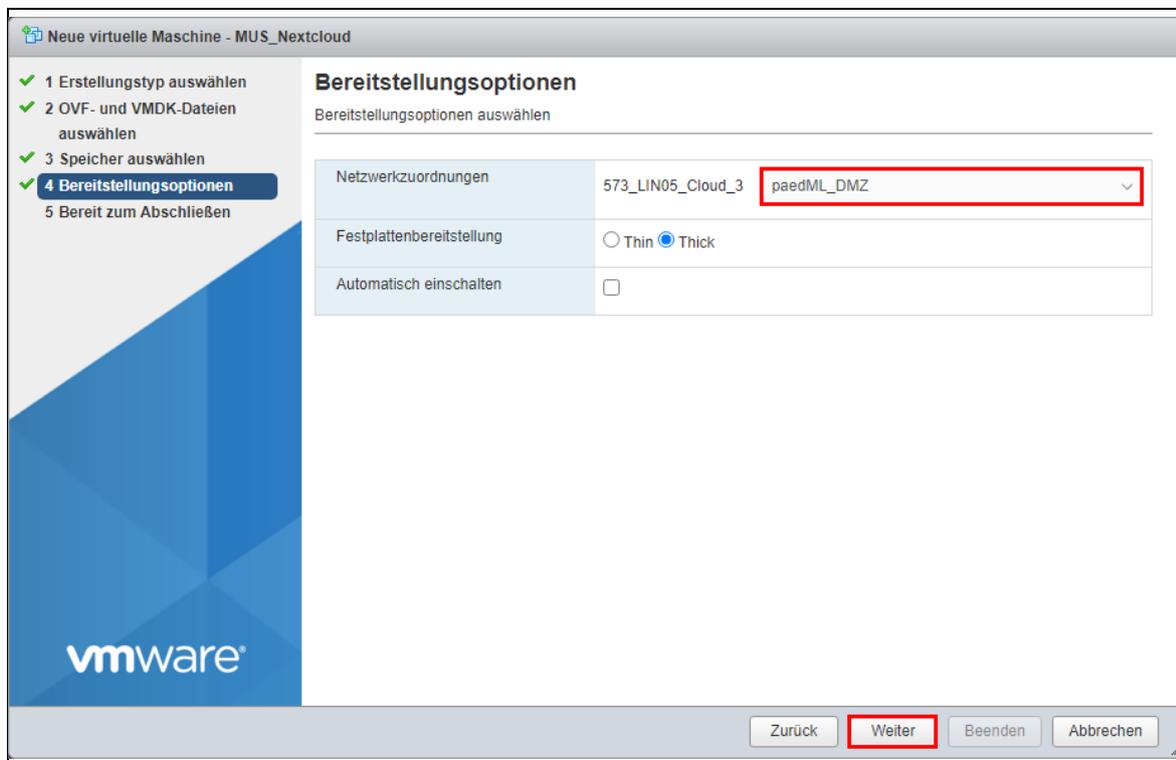


Abb. 16: Bereitstellungsoptionen festlegen

10. Kontrollieren Sie nochmals die von Ihnen gewählten Einstellungen und starten Sie den Import der VM aus der OVF-Vorlage mit **Beenden**.

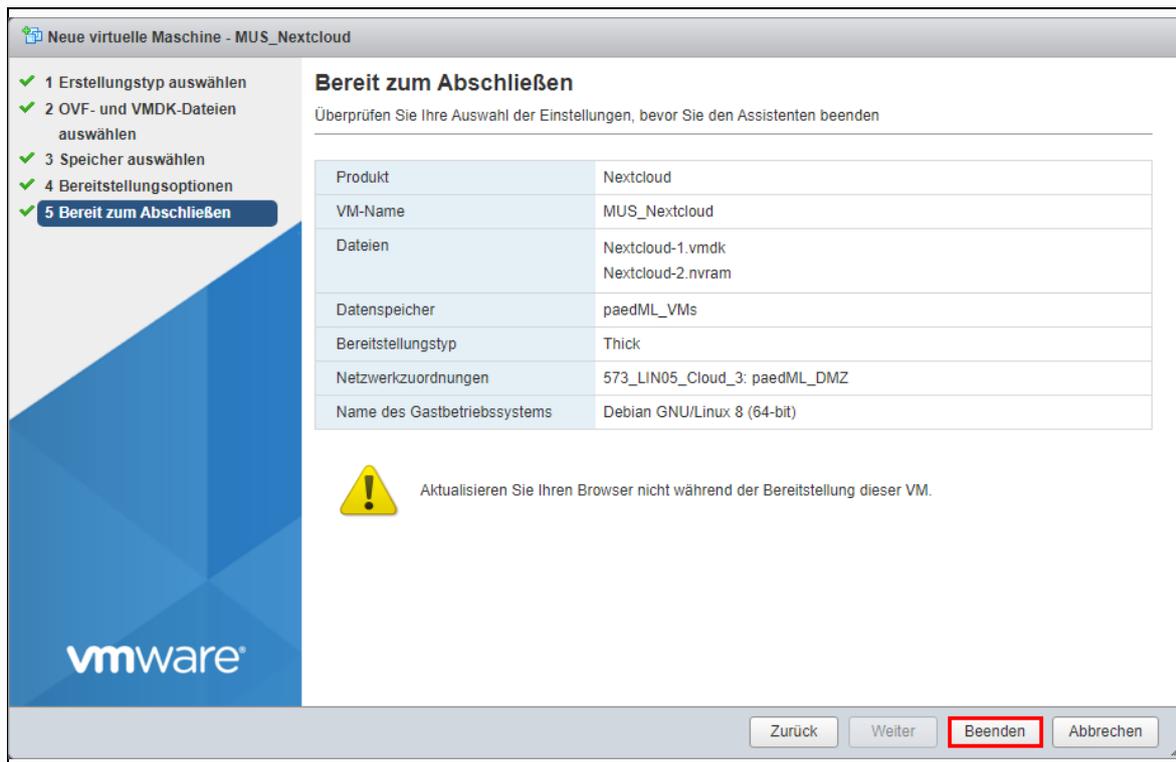


Abb. 17: Bereit zum Abschließen

Nach dem Beenden des Assistenten beginnt der eigentliche Importvorgang. Sie können den Bearbeitungsfortschritt im Bereich Aktuelle Aufgaben verfolgen.

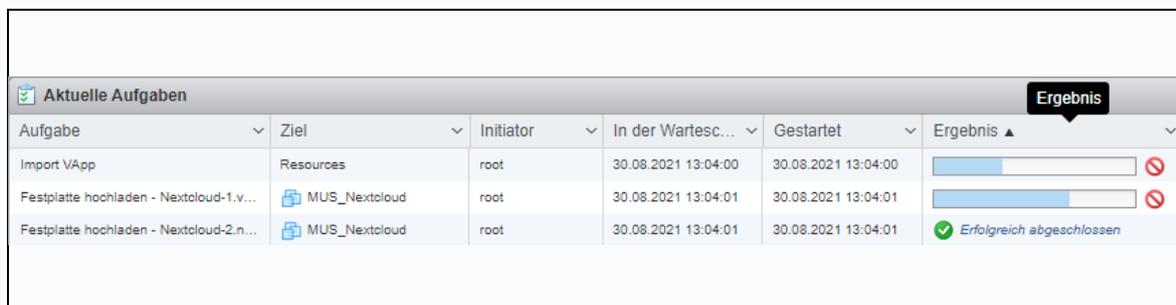


Abb. 18: Bearbeitung der aktuellen Aufgaben durch das System

3.2 [Optional] Einstellungen der Nextcloud-VM bearbeiten

Die Nextcloud-VM beansprucht standardmäßig zwei vCPU und 8 GB RAM. Falls Ihnen diese Einstellungen für Ihre Schule ungeeignet erscheinen, bearbeiten Sie die VM, um die Anzahl der CPUs sowie die Menge der Arbeitsspeicher Ihrem Bedarf entsprechend anzupassen.

3.3 Snapshot erstellen

Erstellen Sie ein Snapshot der Nextcloud-VM, am besten im ausgeschalteten Zustand. So können Sie den Grundzustand zügig wiederherstellen, falls es während der Initialisierung der Nextcloud-VM zu einer Fehlkonfiguration oder gar zu einem schwerwiegenden Fehler kommt.



Snapshots können signifikanten Einfluss auf die Leistungsfähigkeit Ihrer virtuellen Maschinen ausüben. Es ist deshalb ratsam, nach der erfolgreichen Initialisierung der Nextcloud-VM, diese herunterzufahren und alle zur Installationszeit angelegten Snapshots der Nextcloud-VM zu löschen.

Weitere Details und Empfehlungen finden Sie u.a. hier: <https://blogs.vmware.com/performance/2021/06/performance-best-practices-for-vmware-snapshots.html>.

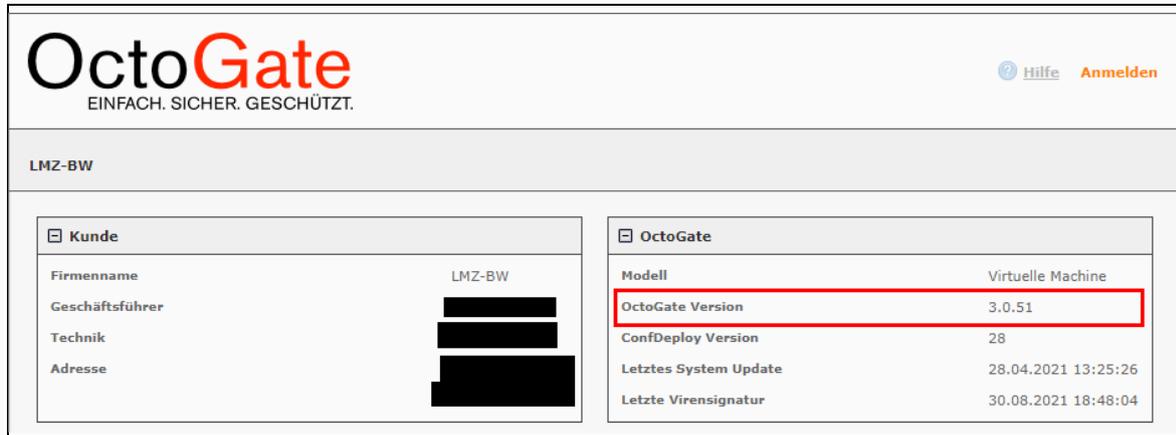
3.4 Nextcloud-VM hochfahren

Fahren Sie die Nextcloud-VM hoch. In den nachfolgenden Kapiteln finden Kontrollschritte statt, die nur dann ausgeführt werden können, wenn die VM eingeschaltet ist.

4 OctoGate anpassen

4.1 Firmware kontrollieren und ggf. aktualisieren

1. Öffnen Sie in einem Browser die WebGUI Ihrer OctoGate.
2. Überprüfen Sie die Versionsnummer OctoGate Version.



The screenshot shows the OctoGate web interface. At the top left is the OctoGate logo with the tagline 'EINFACH. SICHER. GESCHÜTZT.'. At the top right are links for 'Hilfe' and 'Anmelden'. Below the header, the user 'LMZ-BW' is logged in. The main content area is divided into two panels. The left panel, titled 'Kunde', shows customer information: Firmenname (LMZ-BW), Geschäftsführer, Technik, and Adresse. The right panel, titled 'OctoGate', shows system details: Modell (Virtuelle Maschine), OctoGate Version (3.0.51, highlighted with a red box), ConfDeploy Version (28), Letztes System Update (28.04.2021 13:25:26), and Letzte Virensignatur (30.08.2021 18:48:04).

Abb. 19: Version der OctoGate prüfen

Sollte die Versionsnummer der Firmware niedriger sein als 3.0.51, wenden Sie sich an den technischen Support der Fa. OctoGate, um Ihre OctoGate auf die Version 3.0.51 oder höher aktualisieren zu lassen.

4.2 OctoGate an DMZ-Netz anschließen

Ihre OctoGate muss mit dem im [Kapitel 2 DMZ einrichten](#) hinzugefügten virtuellen Switch (kurz vSwitch) für DMZ verbunden werden. Standardmäßig sehen wir dafür den **Netzwerkadapter 2 (eth1)** vor.



Falls Sie den Netzwerkadapter 2 (eth1) bereits für ein eigenes Netz nutzen und Ihre OctoGate deshalb mit einem anderen frei verfügbaren vSwitch verbinden müssen, dann bedarf es einer individuell angepassten Firewall-Konfiguration.

Wenden Sie sich dazu an den Support des Herstellers.

1. Fahren Sie OctoGate herunter.
2. Öffnen Sie als Benutzer Administrator bzw. root den Webclient Ihres ESXi-Hosts.
3. Setzen Sie ein Häkchen bei der virtuellen Maschine **paedML_OctoGate**.
4. Klicken Sie auf **Aktionen** und anschließend auf **Einstellungen bearbeiten**.

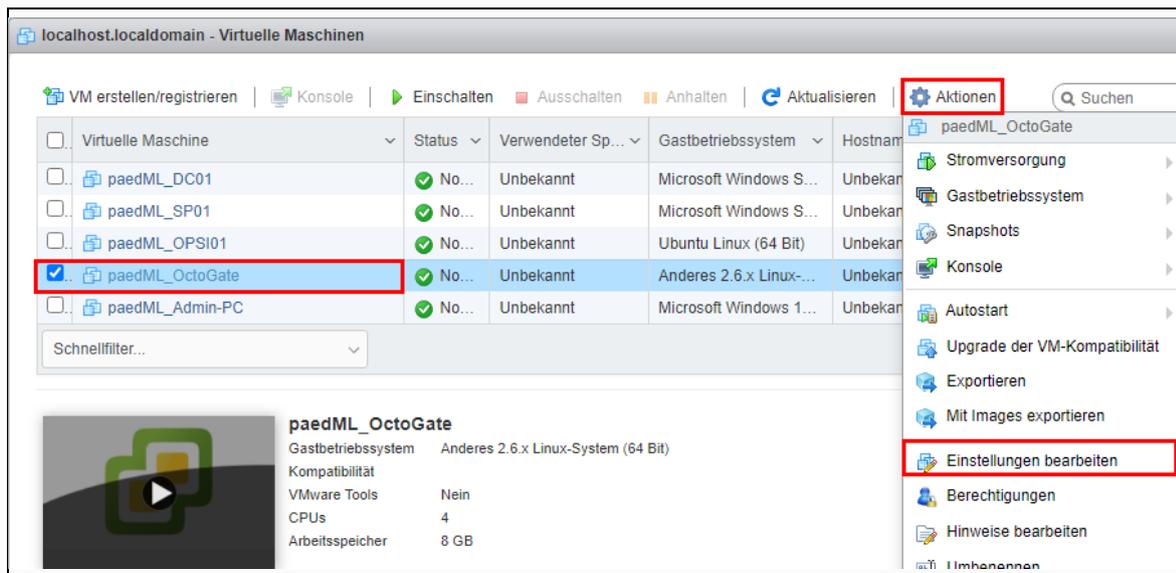


Abb. 20: OctoGate-Einstellungen im ESXi-Host bearbeiten

5. Stellen Sie den **Netzwerkadapter 2** auf den im Kapitel 2.1 **Einen virtuellen Switch (vSwitch) Hinzufügen** hinzugefügten vSwitch – zum Beispiel *paedML_DMZ* – um. Setzen Sie ein Häkchen bei **Verbinden** und schließen Sie den Vorgang mit **Speichern** ab.

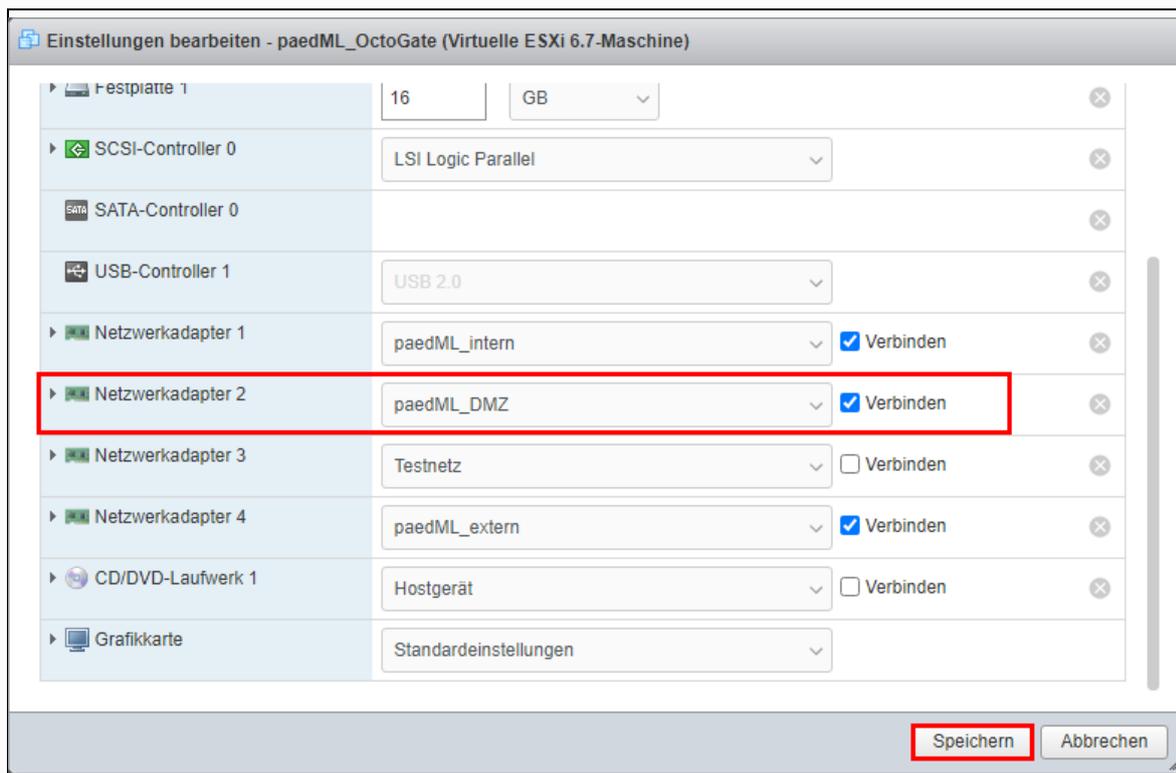


Abb. 21: OctoGate mit der DMZ verbinden

6. Schalten Sie OctoGate wieder ein und öffnen Sie im Browser die WebGUI der OctoGate.
7. Klicken Sie auf **Anmelden** und melden Sie sich als Benutzer **admin** an.

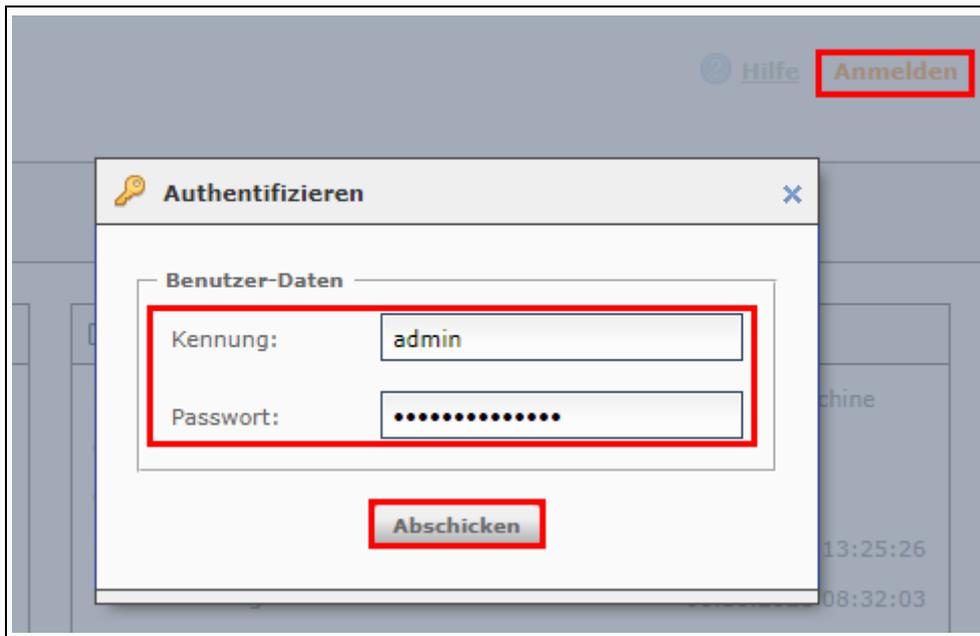


Abb. 22: Anmeldemaske für OctoGate WebGUI

8. Klappen Sie **Netzwerk** (1) auf. Klicken Sie anschließend auf den Link **IP-Adressen** (2).

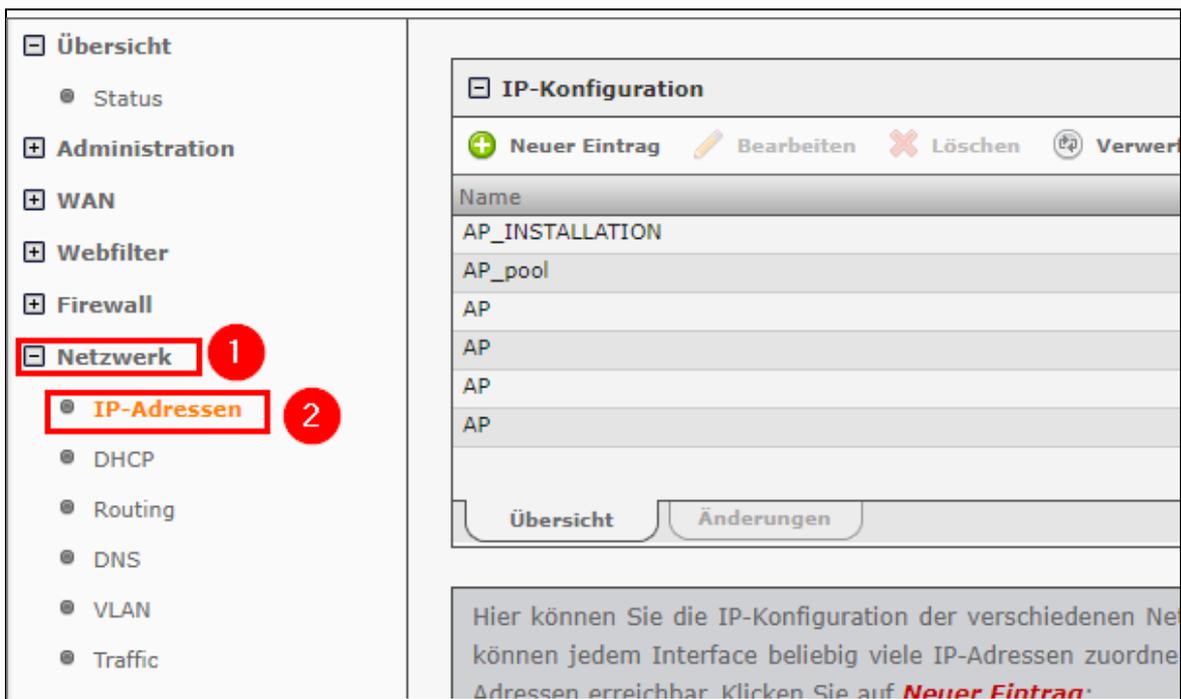


Abb. 23: IP-Konfiguration in der OctoGate

9. Kontrollieren Sie ob im Inhaltsbereich eine IP-Konfiguration gibt, die mit dem IP-Bereich der neuen paedML_DMZ in Konflikt steht. Also eine IP 192.168.201.x (Stimmt das bei einem 24er Netz?) Falls eine IP-Adresse 192.168.201.x vorhanden ist, kontaktieren Sie den Support der Fa. OctoGate, um eine Konfigurationsanpassung bezüglich der DMZ-Schnittstelle für Nextcloud durchführen zu lassen.

Name	IP-Adresse	Interface	Subnetz
AP_INSTALLATION	192.168.1.3	WLAN	24
AP_pool	192.168.7.2	VLAN_INT...	24
AP	192.168.32.1	VLAN_AP2...	20
AP	192.168.48.1	VLAN_AP2...	20
AP	192.168.64.1	VLAN_AP2...	20
AP	192.168.80.1	VLAN_AP2...	20

Abb. 24: Übersicht der IP-Konfiguration

10. Wenn kein störender Eintrag vorhanden ist, klicken Sie auf **Neuer Eintrag**.

11. Tragen Sie folgende Werte ein und speichern Sie sie mit **OK**:

Name : **Nextcloud**
IP-Adresse : **192.168.201.254**
Interface : **DMZ**
Subnetz : **24**
Subnetzmaske : **Bit**

IP-Konfiguration
Neuer Eintrag

Name :

IP-Adresse :

Interface :

Subnetz :

Bit Dezimal

Abb. 25: Neue IP-Konfiguration

12. Klicken Sie im Menübereich der WebGUI-Oberfläche auf **Speichern**.



Abb. 26: Änderungen speichern

13. Klicken Sie auf **Übernehmen**, um das Speichern der neuen IP-Konfiguration zu bestätigen.



Abb. 27: Neue IP-Konfiguration übernehmen

14. Kehren Sie zurück zum WebClient des ESXi-Hosts und melden Sie sich ggf. wieder an.

15. Öffnen Sie die Konsolenansicht der OctoGate.

16. Drücken Sie auf die Tastenkombination **ALT+F5**, um auf Login-Prompt zu gelangen.

17. Sie sehen das folgende Login-Prompt. Drücken Sie nun auf die Tastenkombination **ALT+F2**.

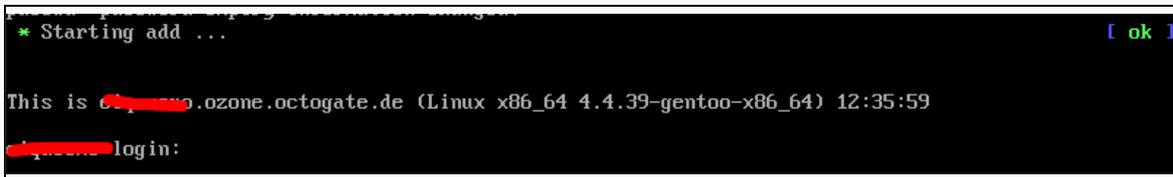


Abb. 28: OctoGate Login-Prompt

18. Navigieren Sie mit den Pfeil-Tasten auf die Zeile **Shell : Viewer-User** und drücken Sie auf **ENTER**.

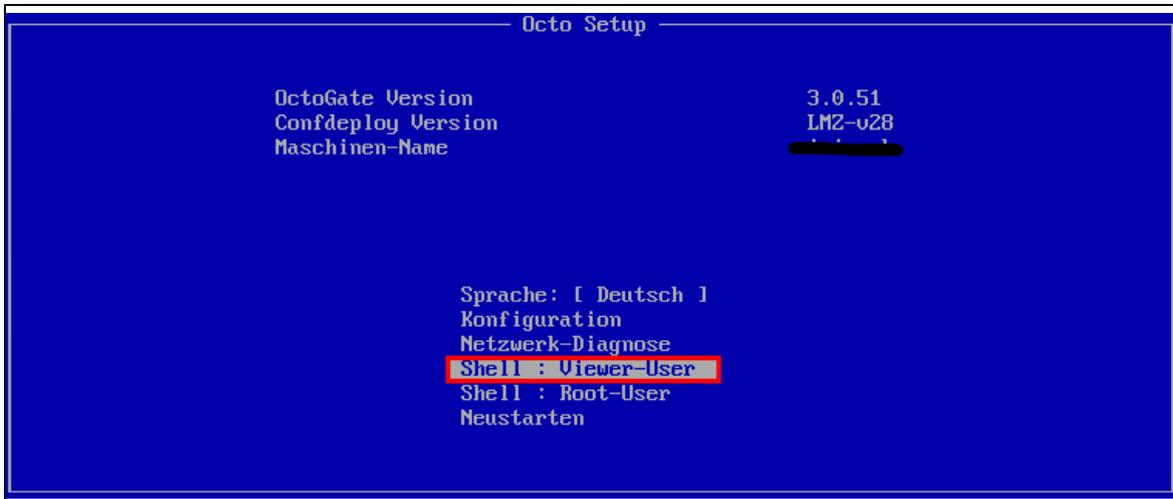


Abb. 29: Octo Setup -> Shell: Viewer-User

19. Führen Sie den Befehl `ping -c 4 192.168.201.254` aus.

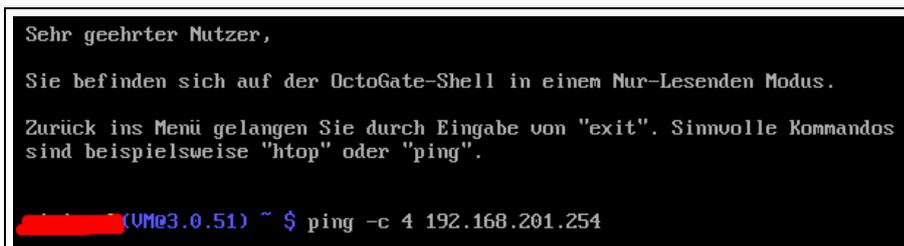


Abb. 30: Den Netzwerkadapter 2 anpingen

Der Befehl sendet genau viermal eine PING-Anfrage an die Netzwerkadresse 192.168.201.254. Das ist die IP-Adresse des zuvor angepassten Netzwerkadapters 2.

Wenn der Netzwerkadapter korrekt angepasst und erfolgreich eingebunden wurde, dann erhalten Sie eine Erfolgsmeldung ähnlich wie nachfolgend dargestellt:

```
(VM@3.0.51) ~ $ ping -c 4 192.168.201.254
PING 192.168.201.254 (192.168.201.254) 56(84) bytes of data.
64 bytes from 192.168.201.254: icmp_seq=1 ttl=64 time=0.050 ms
64 bytes from 192.168.201.254: icmp_seq=2 ttl=64 time=0.049 ms
64 bytes from 192.168.201.254: icmp_seq=3 ttl=64 time=0.038 ms
64 bytes from 192.168.201.254: icmp_seq=4 ttl=64 time=0.050 ms

--- 192.168.201.254 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.038/0.046/0.050/0.009 ms
(VM@3.0.51) ~ $
```

Abb. 31: Rückmeldung des Ping-Befehls

War der Test erfolgreich, dann führen Sie nacheinander folgende Befehle aus:

```
ping -c 4 192.168.201.7
ping -c 4 10.1.1.1
ping -c 4 10.1.1.2
```



Der Befehl `ping -c 4 192.168.201.7` funktioniert nur dann, wenn die Nextcloud-VM eingeschaltet ist.

Sollten die oben genannten PING-Befehle Fehlermeldungen zurückgeben, dann finden Sie im [Anhang B.2 Trouble-Shooting: Octogate, ab Seite 58](#) Tipps zur Behebung einer Störung im Zusammenhang mit OctoGate.

4.3 Kontrolle der Firewall-Regeln

1. Wechseln Sie zur VM Nextcloud im WebClient des ESXi-Hosts.
2. Melden Sie sich als Benutzer `root` mit dem Kennwort `NextCloud` an. Achten Sie bei der Eingabe des Kennworts unbedingt auf die Groß- und Kleinschreibung.

```
Univention DC Master 4.4-8:
The UCS management system is available at https://nextcloud.paedml1.lokal1/ (192.168.201.7)
You can log into the Univention Management Console - the principal tool to manage
users, groups, etc. - using the "Administrator" account and the password selected
for the root user on the master domain controller.

nextcloud login: root
Password:
```

Abb. 32: Erste Anmeldung am Host Nextcloud

3. Führen Sie die folgenden Befehle nacheinander aus und kontrollieren Sie das Ergebnis.

```
ping -c 4 10.1.1.3  
ping -c 4 192.168.201.254  
ping -c 4 10.1.1.1
```



Das Ausführen der oben genannten Befehle sendet je vier PING-Anfragen an die genannten IP-Adressen.

Falls eine der IP-Adressen und insbesondere die IP-Adresse 10.1.1.3 keine Antwort zurücksendet, nehmen Sie Kontakt mit der Hotline der Firma [OctoGate IT Security Systems GmbH](#).

Im [Anhang B.1](#) finden Sie weitere Informationen darüber, welche Angaben Sie in einer E-Mail nennen müssen.

Sie können mit den Anpassungen in AD und DNS sowie mit der Initialisierung der Nextcloud erst dann fortfahren, wenn diese Störung behoben wurde.

5 LDAPS-Zertifikat

Ihre Benutzer melden sich in Nextcloud mit ihrem Account der schulischen paedML, das heißt mit ihrem Benutzernamen und dem eigenen Kennwort aus dem pädagogischen Netz, an.



Technisch betrachtet erfolgt die Benutzerauthentifizierung jedoch nicht direkt in Nextcloud. Stattdessen leitet Nextcloud das Tupel bestehend aus dem Benutzernamen und dessen Kennwort über das Netzwerkprotokoll LDAP (Lightweight Directory Access Protocol) an DC01 weiter. Das bedeutet: In Wirklichkeit werden Ihre Benutzer gegen den Active Directory Service von Ihrem DC01 authentifiziert (Kennwortprüfung) und autorisiert (Rollenprüfung: Lehrer, Schüler usw.).



Die LDAP-Kommunikation findet zwar nur zwischen DC01 und Nextcloud, also auf Ihrem physikalischen Server, statt. Sie sollten dennoch die Kommunikation zwischen DC01 und Nextcloud über das Netzwerkprotokoll LDAPS absichern, um den Transport des Benutzerkontos mit dem zugehörigen Kennwort im Klartext über das Netzwerk zu vermeiden.

5.1 LDAPS-Zertifikat ermitteln

Um die Übertragung der Benutzerdaten zwischen dem AD und der Nextcloud absichern zu können, muss das Zertifikat der Zertifizierungsstelle (CA-Zertifikat) später auf die Nextcloud übertragen werden (siehe [Kapitel 6.1 Anpassungen in AD und DNS](#)). Dabei handelt es sich um dasjenige Zertifikat, mit dem das Hostzertifikat für DC01 generiert und signiert wurde.

Wir stellen ein PowerShell-Skript zur Verfügung, um Ihnen das Auffinden des CA-Zertifikats zu erleichtern.

1. Öffnen Sie auf dem Server SP01 den Datei-Explorer und navigieren Sie nach `D:\Installation\paedML\Erweiterungen\Nextcloud`.
2. Führen Sie das PowerShell-Skript `Get-LDAPSCertificate.ps1` aus.

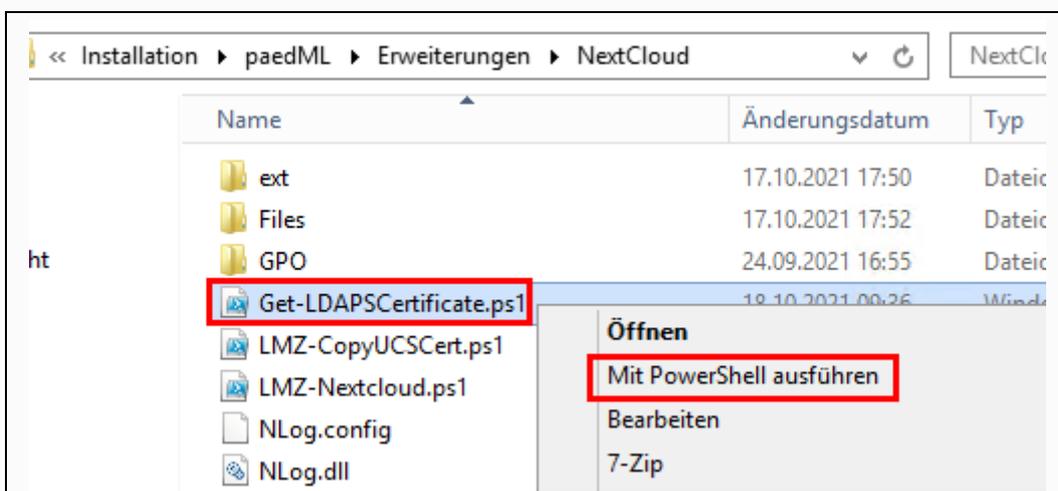


Abb. 33: `Get-LDAPSCertificate.ps1` ausführen

Das Skript untersucht, ob auf dem Server DC01 LDAPS bereits eingerichtet wurde. Es gibt demnach zwei mögliche Rückmeldungen:

- Eine LDAPS-Konfiguration wurde nicht gefunden.
- Es werden Informationen über die für LDAPS importierten Zertifikate angezeigt.

Wenn LDAPS auf DC01 nicht eingerichtet wurde, fahren Sie mit dem nächsten [Kapitel 5.2 LDAPS einrichten](#) fort. Wurde ein LDAPS-Zertifikat gefunden, dann müssen Sie noch folgende Schritte bearbeiten, bevor Sie mit dem [Kapitel 6.1 Anpassungen in AD und DNS](#) fortfahren.

Scrollen Sie das Ausgabefenster nach unten bzw. nach oben, bis die Zeile
-----END CERTIFICATE-----

zu sehen ist. Suchen Sie darunter nach der Zeile, die mit `issuer=` beginnt.

Notieren Sie den Namen **CN = {Name der Zertifizierungsstelle}**.

```
Administrator: Windows PowerShell
00q15VUxH4ozqcn/jmrvLgmuLhc9tD8QrUkY3XZsS90i4gC89 jZ0qRepf F4TqD
002KQNeyp1c./ntSQ6Wa7i1A+9U9muXQ12tERN/LE3TN7k6Lo8ZgaERHm5xgQBwFR0
i2MM9aGyrD9Wdt0q1fKS5pVehMo.jtHow23ZZI+Hd/H16HhkaBeDheNxeVNov9 i1
Y1EpawmsERpn1uadJ/do6TpWiC4vAgMBAAGjY jBgMCoGA1UdEQQjMCGCH2RjMDEu
bXUzdGUyc2NoAWxLLnNjaHUzZS5vYWUkbWwwEwYDURO1BAwwCgYI KwYBBQUHAwEw
HQYDURO0BBYEFauEge4zXaen6K/15907DNpuxcNjMA0GCSqGSI b3DQEBQwUAA4Gw
AG6/vEZH+m1Bt9eaeU+g7VrizmrBei/3GZWHegNqaIA9YDHUymk1J/UKKvUtPgUy
MhIHdn141MhxSFAZKsy9N+5p2UzCjg2n113YFBwg6WJUes19Y9r3UAupJGemyu2S
Ylhx9Li4QZ2e9RlycEeac6XvlnZgXhugmZQvhd3yeED
-----END CERTIFICATE-----
Server certificate
subject=C = DE, ST = Baden-Wuerttemberg, L = Stuttgart, O = LMZ-BW, OU = LDAPS, CN = dc01.musterschule.schule.paedml, emailaddress = support@octogate.de
issuer=C = DE, ST = NRW, L = Paderborn, O = OctoGate IT Security Systems GmbH, CN = OctoGate, emailaddress = support@octogate.de
No client certificate CA names sent
Client Certificate Types: RSA sign, DSA sign, ECDSA sign
Requested Signature Algorithms: RSA+SHA512:ECDSA+SHA512:RSA+SHA256:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA384
Shared Requested Signature Algorithms: RSA+SHA512:ECDSA+SHA512:RSA+SHA256:RSA+SHA384:ECDSA+SHA256:ECDSA+SHA384
Peer signing digest: SHA256
Peer signature type: RSA
Server Temp Key: ECDH, prime256v1, 256 bits
SSL handshake has read 2009 bytes and written 491 bytes
Verification error: unable to verify the first certificate
New, TLSv1.2, Cipher is ECDHE-RSA-AES256-SHA384
Server public key is 4096 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
Protocol : TLSv1.2
Cipher : ECDHE-RSA-AES256-SHA384
Session-ID: 19490000DDFB5CB7F7F54251B6C66975550C9F0F6D973FEC091248D532E23E02
Session-ID-ctx:
Master-Key: A949BE485D6835692FC1A4E1354CAB56C9F456188C5B9982FF52D5EFC0804872C87AE1ABDD2C4625396CFD8E71D27FB
PSK identity: None
PSK identity hint: None
SRP username: None
Start Time: 1634542805
Timeout : 7200 (sec)
Verify return code: 21 (unable to verify the first certificate)
Extended master secret: yes
Drücken Sie auf eine beliebige Taste, um das Skript zu beenden:
```

Abb. 34: Issuer ermitteln



Wenn das gesuchte Zertifikat, wie in der obigen Abbildung dargestellt, von OctoGate stammt, ignorieren Sie die nachfolgenden Schritte und fahren Sie mit dem [Kapitel 5.3 Kontrolle](#) fort.



Die nachfolgenden Schritte sind dann notwendig, wenn Sie LDAPS mit Ihren eigenen Zertifikaten eingerichtet haben. In diesem müssen Sie das CA-Zertifikat in eine Datei exportieren, um es später im [Kapitel 6.1 Anpassungen in AD und DNS](#) auf die Nextcloud kopieren zu können.

3. Tippen Sie auf die Windows-Taste und tippen Sie `mmc.exe`, um MMC zu öffnen.



Abb. 35: mmc.exe ausführen

4. Klicken Sie auf Datei und wählen Sie anschließend Snap-In hinzufügen/entfernen... aus.

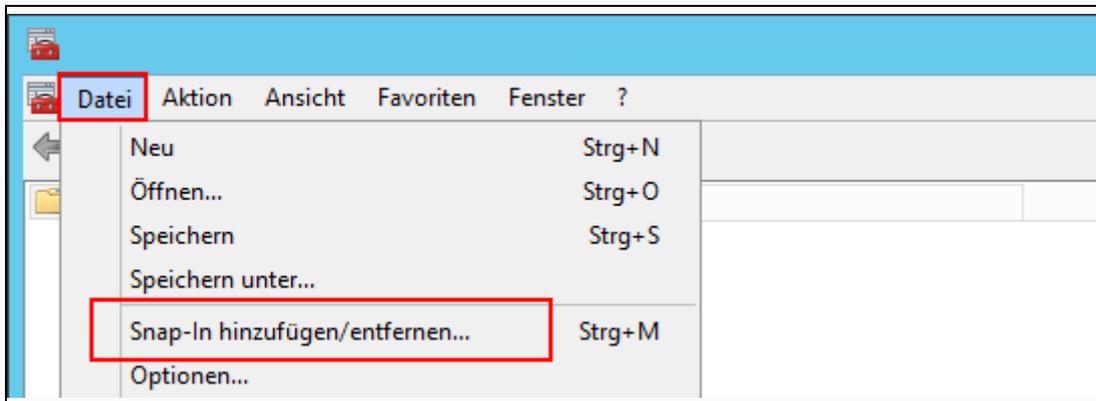


Abb. 36: MMC > Snap-In hinzufügen

5. Als Snap-In wählen Sie Zertifikate aus und klicken auf Hinzufügen.

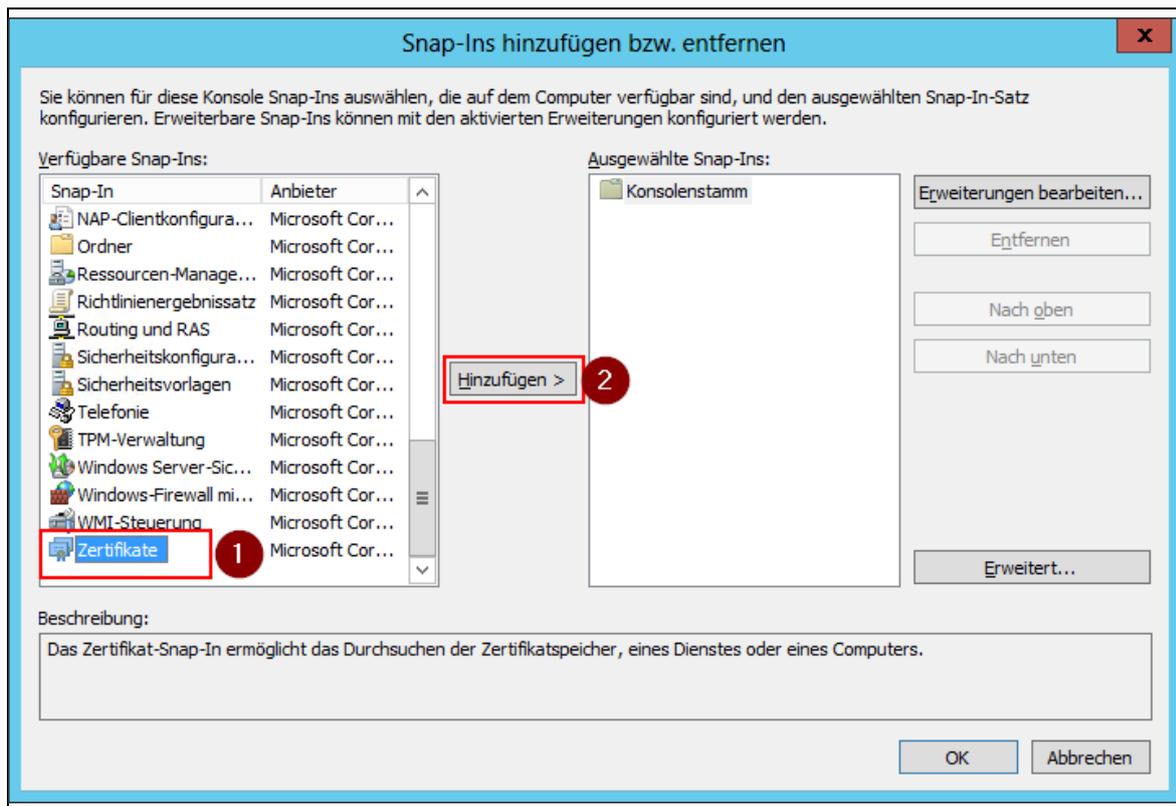


Abb. 37: MMC > Snap-In hinzufügen > Zertifikate

6. Wählen Sie **Computerkonto** aus und klicken Sie auf **Weiter**.

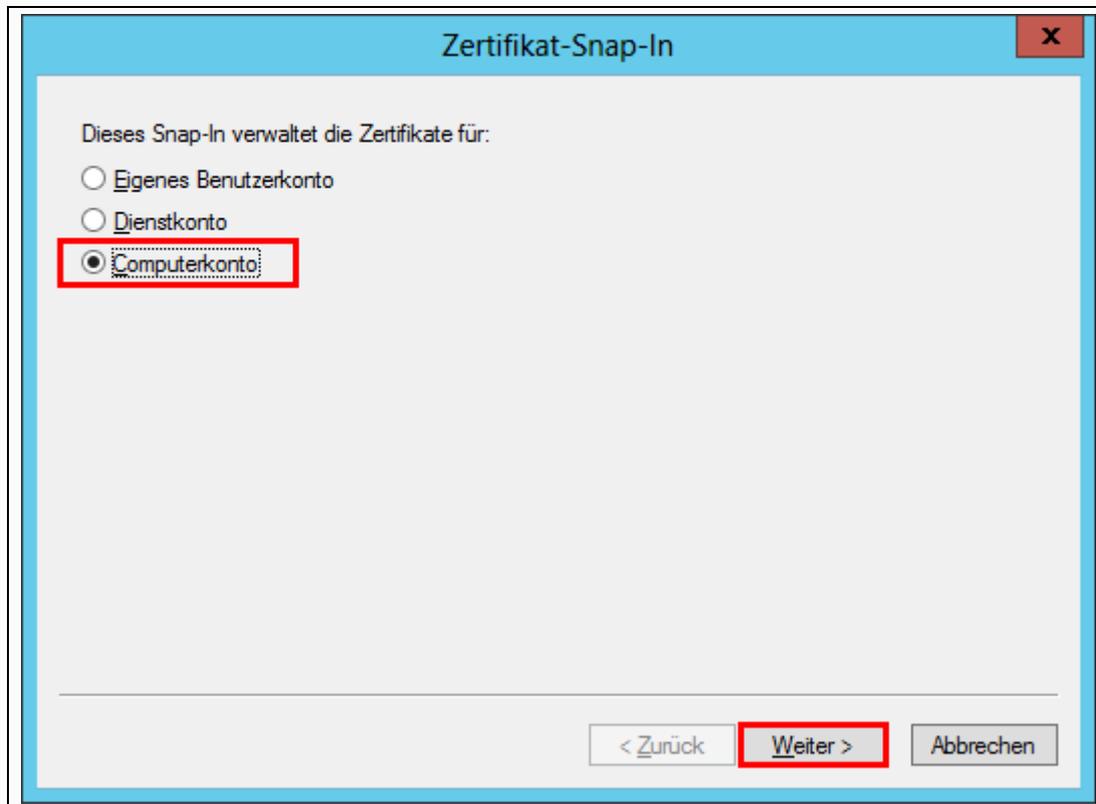


Abb. 38: MMC > Snap-In hinzufügen > Zertifikate -> Computerkonto

7. Wählen Sie die Option **Anderen Computer** aus und geben Sie als Computernamen DC01 ein. Klicken Sie anschließend auf **Fertig stellen**.

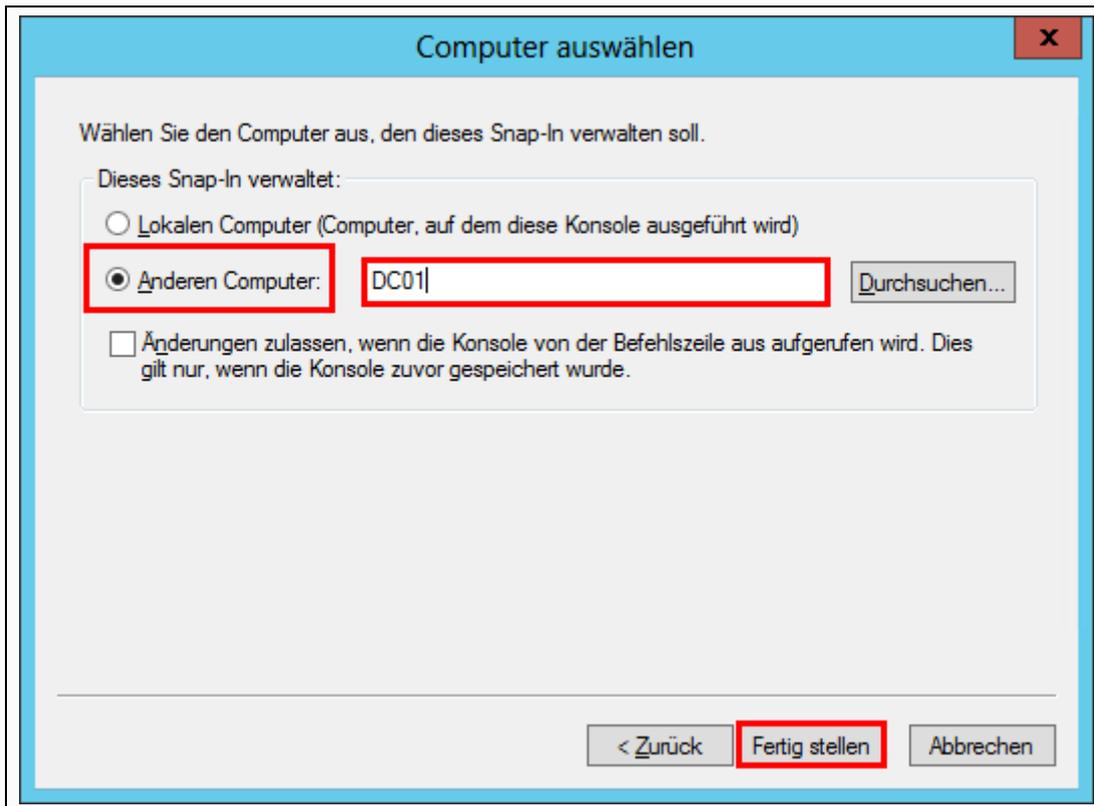


Abb. 39: MMC > Snap-In hinzufügen > Fertig stellen

8. Schließen Sie das Dialogfenster **Snap-Ins hinzufügen bzw. entfernen** mit **OK**.
9. Navigieren Sie zu `\\DC01\Vertrauenswürdige Stammzertifizierungsstellen` → `Zertifikate`.

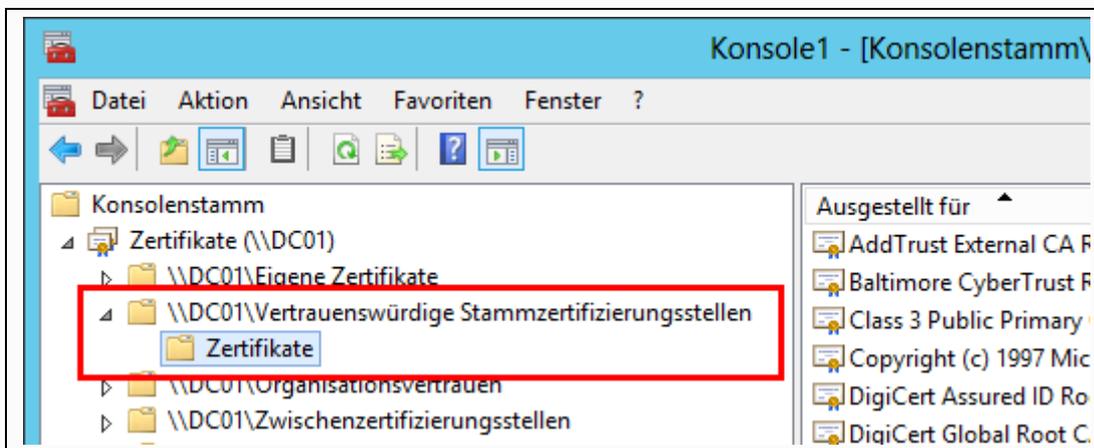


Abb. 40: Zertifikatspeicher \\DC01\Vertrauenswürdige Stammzertifizierungsstellen

10. Suchen Sie nach dem Zertifikat, das in der Spalte **Ausgestellt von** den Namen der Zertifizierungsstelle trägt, den Sie im **Schritt 2** weiter oben ermittelt haben.

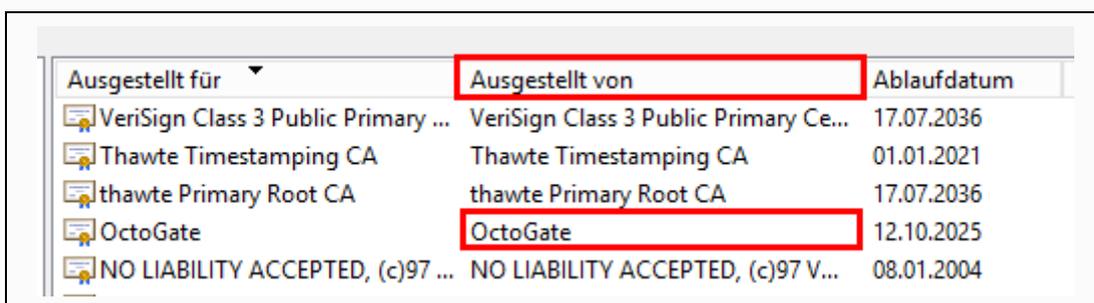


Abb. 41: Zertifikatspeicher

11. Markieren Sie das Zertifikat mit der rechten Maustaste und wählen Sie **Alle Aufgaben** → **Exportieren** aus.

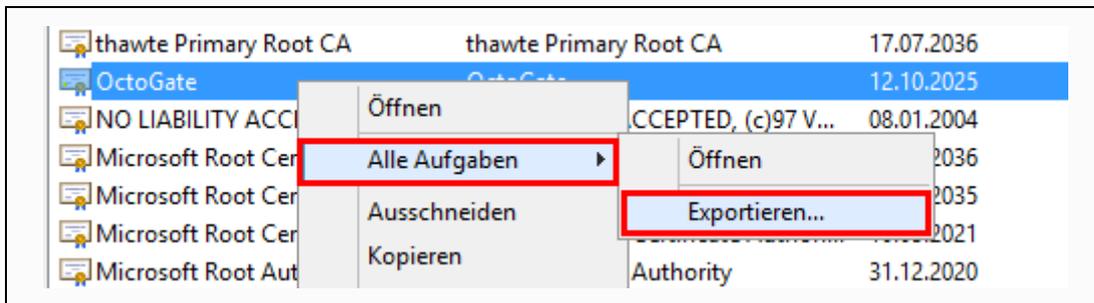


Abb. 42: Zertifikatspeicher -> Zertifikat exportieren

12. Klicken Sie auf **Weiter**.

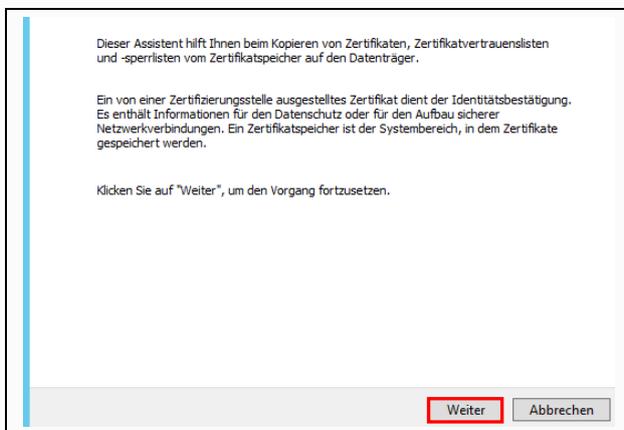


Abb. 43: Zertifikatspeicher -> Zertifikat exportieren

13. Wählen Sie als Exportformat **Base-64-codiert X.509 (.CER)** aus und klicken Sie auf **Weiter**.

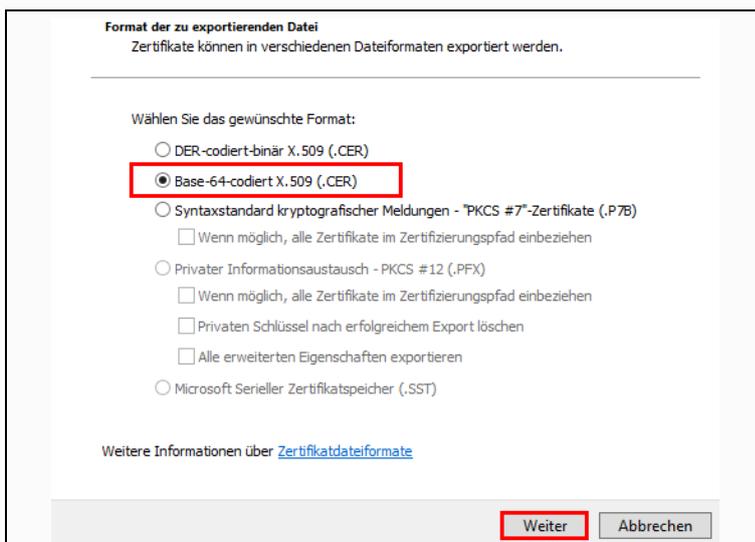


Abb. 44: Zertifikatspeicher -> Zertifikat exportieren -> Format auswählen

14. Geben Sie der Datei einen Namen samt Ordnerpfad, z.B. C:\tmp\Meine-CA.cer, ein und klicken Sie auf **Weiter**.

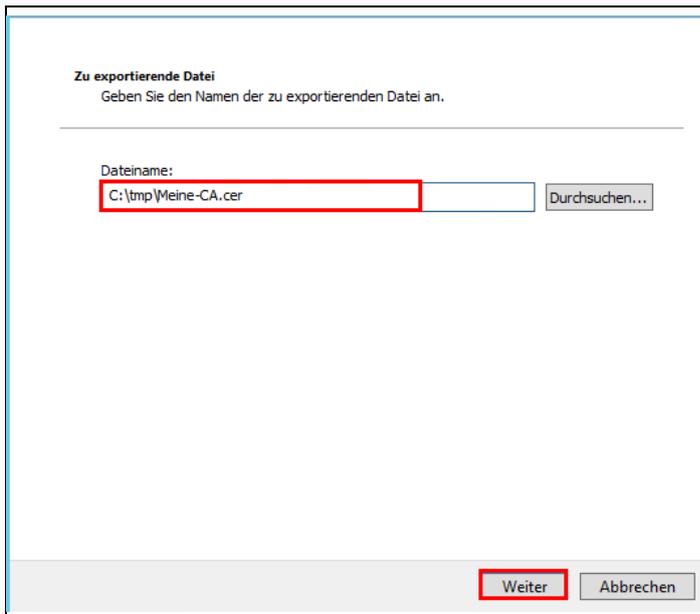


Abb. 45: Zertifikatspeicher -> Zertifikat exportieren -> Dateiname eingeben



Notieren Sie sich den Speicherpfad. Das Zertifikat müssen Sie im [Kapitel 6.1 Anpassungen in AD und DNS](#) angeben, damit es auf Ihre Nextcloud übertragen werden kann.

15. Kontrollieren Sie die Zusammenfassung und klicken Sie auf **Fertig stellen**.

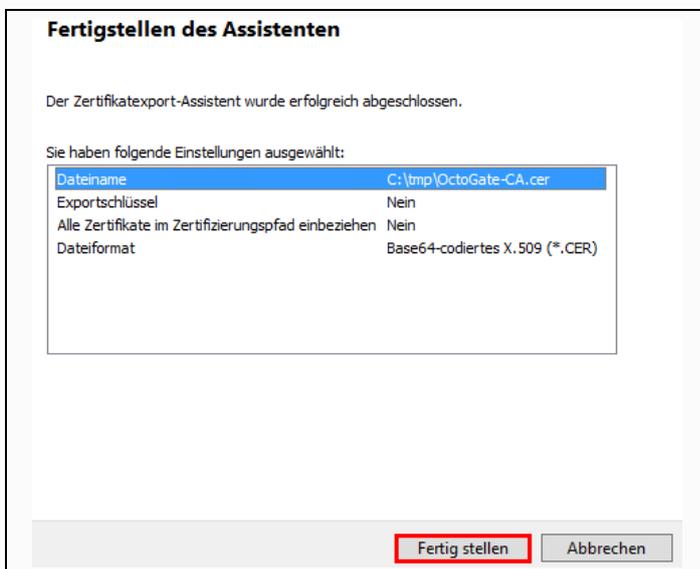


Abb. 46: Zertifikatspeicher -> Zertifikat exportieren -> Dateiname eingeben

16. Schließen Sie den Zertifikatexport-Assistenten mit **OK**.

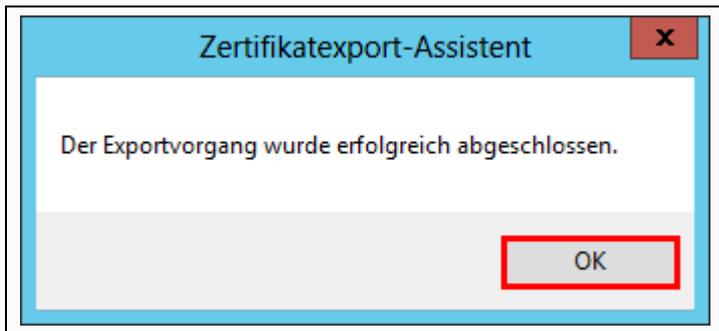


Abb. 47: Zertifikatexport-Assistent beenden

17. Schließen Sie MMC und das PowerShell-Fenster, sofern sie noch geöffnet sind.

5.2 LDAPS einrichten



Sie können dieses Kapitel überspringen, wenn die Kontrolle nach LDAPS aus dem vorangegangenen Kapitel erfolgreich war.

Wenn auf Ihrem Server DC01 noch kein LDAPS eingerichtet wurde, dann öffnen Sie im Datei-Explorer den Ordner `D:\Installation\paedML\Erweiterungen\Nextcloud`.

Führen Sie das PowerShell-Skript `New-paedMLCAOnDC.ps1` aus.



Abb. 48: `New-paedMLCAOnDC.ps1`

Das Skript erzeugt mit dem Open-Source Tool [OpenSSL](#) alle für LDAPS notwendigen Zertifikate und importiert sie automatisch in den passenden Zertifikatsspeicher. Wir verwenden dabei eine speziell für den Einsatz unter dem Windows-Betriebssystem kompilierte [Version](#), die von den Entwicklern des Open-Source Tools [curl](#) zum Download bereitgestellt wird.

Die mithilfe des OpenSSL generierten Zertifikate sind:

- **DC01.musterschule.schule.paedml**
Das ist das **Host-Zertifikat für den Server DC01**. Mit diesem Zertifikat verschlüsselt der Server DC01 die übertragenen Benutzerdaten. Die Gültigkeitsdauer des Host-Zertifikats beträgt fünf Jahre.
- **CA.crt**
Das ist das **Zertifikat der Zertifizierungsstelle mit dem CN paedML Windows Root CA**. Durch das Skript wird es sowohl auf DC01 als auch auf SP01 in der Zertifikatspeicher Vertrauenswürdige Stammzertifizierungsstellen importiert. Die Gültigkeitsdauer des CA-Zertifikats beträgt zehn Jahre.



Sie finden auf dem Server DC01 alle Konfigurations- und Zertifikatsdateien, die während der Ausführung des PowerShell-Skripts generiert wurden, und zwar im Ordner: D:\pa-edML\certs.

Wenn Sie vorhaben, mit OpenSSL weitere Zertifikate selbst zu erzeugen, dann empfehlen wir Ihnen diesen Ordner zu archivieren – am besten als mit einem Kennwort gesichertes ZIP-Archiv – und das Archiv an einem hinreichend sicheren Ort (zum Beispiel NAS mit einem gesicherten Zugang) zu bewahren. Löschen Sie am besten den Ordner, nachdem Sie das Archiv auf einen externen Datenträger gesichert haben.



Ein Export der CA-Zertifikats wie im [Kapitel 5.1 LDAPS-Zertifikat ermitteln](#) beschrieben ist nicht erforderlich. Das CA-Zertifikat wird für die Initialisierung der Nextcloud automatisch kopiert.

5.3 Kontrolle

1. Öffnen Sie in einem Browser die **WebGUI** Ihrer **OctoGate**.
2. Melden Sie sich als Benutzer **admin** an.
3. Klicken Sie auf **Downloads** und laden Sie die ZIP-Datei **OctoGate CA Importer** herunter.

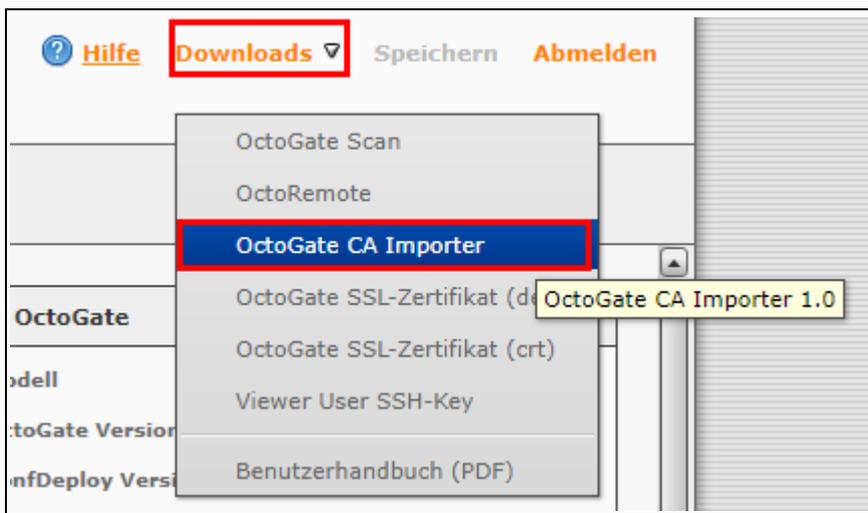


Abb. 49: OctoGate CA Importer

4. Entpacken Sie die ZIP-Datei `OctoimportCA.zip` und führen Sie durch Doppelklick die Datei `OctoimportCA.exe` aus.
5. Sie erhalten eine Erfolgsmeldung.
6. Wechseln Sie auf DC01 und melden Sie sich ggf. als Administrator an.
7. Drücken Sie auf die Tastenkombination **Windows**-Taste und **R**. Tippen Sie `ldp.exe` ein und drücken Sie auf **ENTER**.

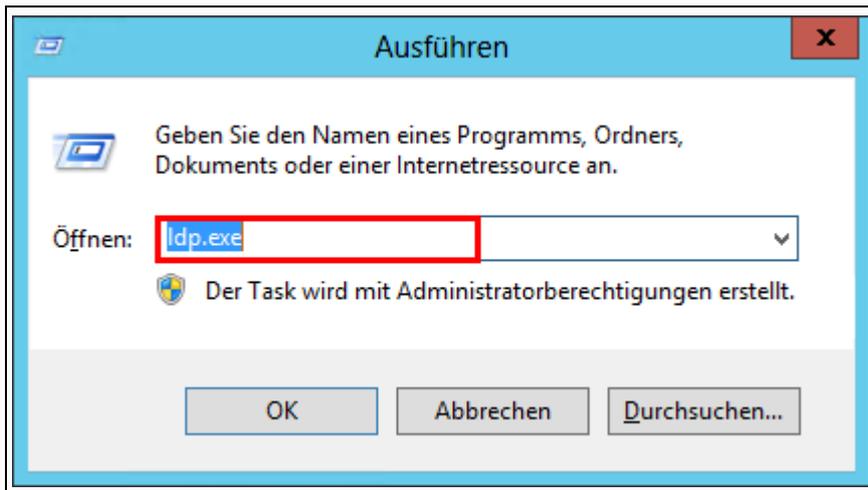


Abb. 50: LDP öffnen

8. Klicken Sie auf das Menü **Verbindung** und auf **Verbinden...**.



Abb. 51: LDP -> Verbindung

9. Geben Sie folgende Werte ein und klicken Sie auf **OK**:

Server : dc01.musterschule.schule.paedml

Port : 636

SSL : Aktiviert

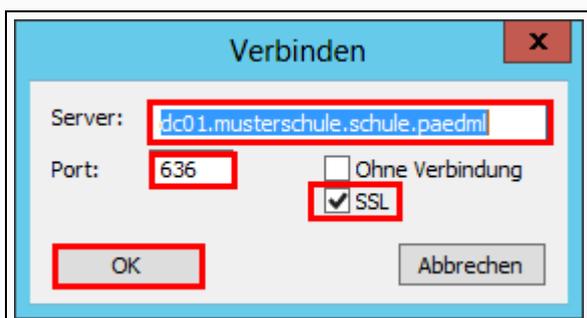


Abb. 52: LDP -> Verbindungsoptionen

10. Drücken Sie im Programm die Tastenkombination **Strg+B**.

11. Setzen Sie den Bindungstyp auf **Bindung als aktuell angemeldeter Benutzer** und klicken Sie auf **OK**.

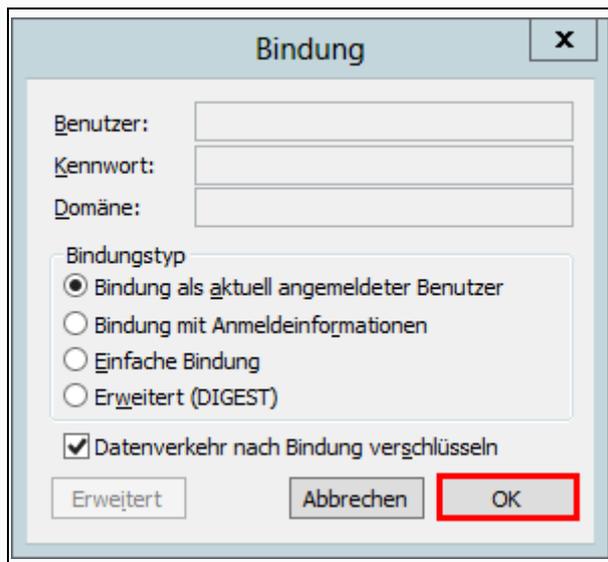


Abb. 53: LDP -> Verbindung

Wenn der Import bzw. die Erstellung des Serverzertifikats aus dem vorangegangenen Kapitel erfolgreich war, erscheint neben der RootDSE-Info der erfolgreiche Anmeldestatus.

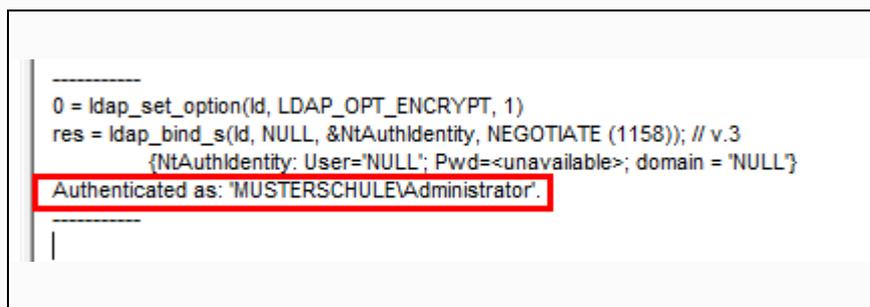


Abb. 54: LDP -> Verbindung erfolgreich hergestellt

Schließen Sie das Fenster Idaps.

6 Initialisierung der Nextcloud



Wenn Ihre OctoGate Firewall hinter einem weiteren Router oder einem weiteren Firewall-Produkt betrieben wird, müssen Sie dafür sorgen, dass der für LDAP Authentifizierung vorgesehene Port auf dem Router bzw. auf der vorgeschalteten Firewall ebenfalls geöffnet und an Octogate/Sophos weitergeleitet werden.

6.1 Anpassungen in AD und DNS

Bevor die Initialisierungsskripte auf der Nextcloud-VM ausgeführt werden, müssen Sie zunächst einen sogenannten Binduser für LDAP-Kommunikation einrichten. Außerdem sollten Sie das Serverzertifikat für LDAPS in den Ordner `/usr/local/share/ca-certificates` auf der Nextcloud-VM kopieren. Darüber hinaus müssen zusätzliche Einträge in DNS hinterlegt werden, damit Ihre Nextcloud mit einem Klartextnamen statt der IP-Adresse 192.168.201.7 aufgerufen werden kann.



Das Skript `LMZ-Nextcloud.ps1` fügt unter anderem zwei neue Gruppenrichtlinienobjekte im AD hinzu. Details dazu finden Sie im [Anhang A Nützliche Ergänzungen](#).

1. Öffnen Sie auf dem Server SP01 den Datei-Explorer und navigieren Sie nach `D:\Installation\paedML\Erweiterungen\Nextcloud`.
2. Führen Sie das PowerShell-Skript `LMZ-Nextcloud.ps1` mit PowerShell aus.
3. Legen Sie das Kennwort des LDAP-Bindusers **ldapnextcloud** fest.
4. Notieren Sie sich das Kennwort z. B. in Ihrem Kennwortsafe.

```
Info: Bitte prüfen, ob der Binduser 'ldapnextcloud' vorhanden ist.
[Info] Der LDAP-Binduser "ldapnextcloud" existiert nicht. Das Benutzerkonto wird angelegt...
Geben Sie das Kennwort des LDAP-Bindusers ein: *****_
```

Abb. 55: Kennwort LDAP-Binduser `ldapnextcloud`

5. Wiederholen Sie das Kennwort.

```
Geben Sie das Kennwort des LDAP-Bindusers ein: *****
Wiederholen Sie das Kennwort des LDAP-Bindusers: *****
```

Abb. 56: Kennwortwiederholen für den LDAP-Binduser `ldapnextcloud`



Bevor Sie die nachfolgende Kontrollabfrage bejahen, sollten Sie kurz innehalten und prüfen, ob LDAPS tatsächlich konfiguriert wurde.

Bejahen Sie sie, obwohl Sie [Kapitel 5 LDAPS-Zertifikat](#) nicht bearbeitet und damit LDAPS nicht konfiguriert haben, sorgen Sie selbst dafür, dass sich kein Benutzer in Nextcloud anmelden kann, bis die LDAP-Konfiguration manuell korrigiert wurde.

Als Nächstes müssen Sie entscheiden, ob Sie LDAPS für die Nextcloud konfigurieren wollen, um die Übertragung der Benutzeranmeldedaten – d.h. Benutzername und Kennwort – abzusichern. Dafür gibt es grundsätzlich folgende vier Fallunterscheidungen:

- LDAPS wird nicht konfiguriert. → [Kapitel 6.1.1](#)
- LDAPS war nicht konfiguriert und wurde mit Hilfe des PowerShell-Skripts `New-paedMLCAOnDC.ps1` eingerichtet → [Kapitel 6.1.2](#)
- LDAPS wird mit Ihrem eigenen Hostzertifikat eingerichtet. → [Kapitel 6.1.3](#)
- LDAPS wird mit dem Zertifikat der OctoGate eingerichtet. → [Kapitel 6.1.4](#)

Für ein besseres Verständnis gliedern wir diese vier Fallunterscheidungen jeweils in einem in sich abgeschlossenen Unterkapitel.

6.1.1 Keine LDAPS-Konfiguration

6. Verneinen Sie die Frage „**Möchten Sie LDAPS konfigurieren?**“, indem Sie auf die Taste **N** drücken.



Abb. 57: Soll LDAPS für Nextcloud konfiguriert werden?

7. Die nächste Frage wird ebenfalls verneint.

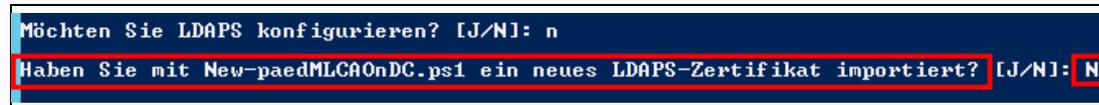


Abb. 58: Wurden LDAPS-Zertifikate mit `New-paedMLCAOnDC.ps1` generiert?

8. Drücken Sie auf eine beliebige Taste, um das Skript zu beenden.

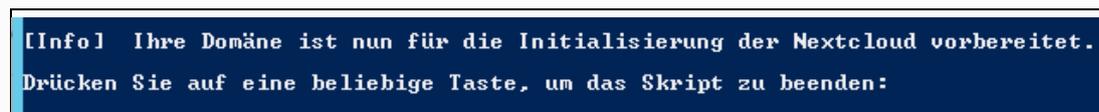


Abb. 59: Skript `LMZ-Nextcloud.ps1` beenden

6.1.2 LDAPS mit dem PowerShell-Skript `New-paedMLCAOnDC.ps1` eingerichtet

6. Drücken Sie auf die Taste **J**, falls Sie wie im [Kapitel 5.2 LDAPS einrichten](#) beschrieben mithilfe des PowerShell-Skripts `New-paedMLCAOnDC.ps1` neue LDAPS-Zertifikate generiert und importiert haben.



Abb. 60: Soll LDAPS für Nextcloud konfiguriert werden?

7. Beantworten Sie die darauffolgende Frage ebenfalls mit **Ja**, indem Sie auf die Taste **J** drücken.

```
Möchten Sie LDAPS konfigurieren? [J/N]: j
Haben Sie mit New-paedMLCAOnDC.ps1 ein neues LDAPS-Zertifikat importiert? [J/N]: j
```

Abb. 61: Wurden LDAPS-Zertifikate mit New-paedMLCAOnDC.ps1 generiert?

- Geben Sie das Kennwort des Benutzers **root** der **Nextcloud-VM** ein. Wenn Ihre Nextcloud zum ersten Mal initialisiert wird, dann lautet das Kennwort „NextCloud“ (ohne Anführungszeichen!).

```
Geben Sie das Kennwort des Benutzers root <Nextcloud> ein: *****
wiederholen sie das kennwort des benutzers root <nextcloud>: _
```

Abb. 62: Kennwort für Benutzer root (Nextcloud)

- Wiederholen Sie die Kennworteingabe.

```
Geben Sie das Kennwort des Benutzers root <Nextcloud> ein: *****
Wiederholen Sie das Kennwort des Benutzers root <Nextcloud>: *****
```

Abb. 63: Kennwort wiederholen für Benutzer root (Nextcloud)

- Drücken Sie auf eine beliebige Taste, um das Skript zu beenden.

```
[Info] Ihre Domäne ist nun für die Initialisierung der Nextcloud vorbereitet.
Drücken Sie auf eine beliebige Taste, um das Skript zu beenden:
```

Abb. 64: Skript LMZ-Nextcloud.ps1 beenden

6.1.3 LDAPS mit eigenem Hostzertifikat



Hier nehmen wir an, dass Sie LDAPS auf Ihrem DC01 mit Ihrem eigenen Hostzertifikat – zum Beispiel mithilfe von Active Directory-Zertifikatdienste oder OpenSSL selbst generiert – eingerichtet haben.

- Drücken Sie auf die Taste **J**.

```
Geben Sie das Kennwort des LDAP-Bindusers ein: *****
Wiederholen Sie das Kennwort des LDAP-Bindusers: *****
Möchten Sie LDAPS konfigurieren? [J/N]: j
```

Abb. 65: Soll LDAPS für Nextcloud konfiguriert werden?

- Beantworten Sie die darauffolgende Frage mit **Nein**, indem Sie auf die Taste **N** drücken.

```
Möchten Sie LDAPS konfigurieren? [J/N]: j
Haben Sie mit New-paedMLCAOnDC.ps1 ein neues LDAPS-Zertifikat importiert? [J/N]: n
```

Abb. 66: Wurden LDAPS-Zertifikate mit New-paedMLCAOnDC.ps1 generiert?

- Drücken Sie ein weiteres Mal auf die Taste **N**, um die Frage nach einem OctoGate Hostzertifikat mit Nein zu beantworten.

```
Haben Sie mit New-paedMLCAOnDC.ps1 ein neues LDAPS-Zertifikat importiert? [J/N]: n
Murde LDAPS mit einem Hostzertifikat von OctoGate eingerichtet? [J/N]: N
```

Abb. 67: OctoGate Hostzertifikat?

9. Geben Sie das Kennwort des Benutzers **root** der **Nextcloud-VM** ein. Wenn Ihre Nextcloud zum ersten Mal initialisiert wird, dann lautet das Kennwort „**NextCloud**“ (ohne Anführungszeichen!).

```
Geben Sie das Kennwort des Benutzers root (Nextcloud) ein: *****
wiederholen Sie das kennwort des benutzers root (Nextcloud): _
```

Abb. 68: Kennwort für Benutzer root (Nextcloud)

10. Wiederholen Sie die Kennworteingabe.

```
Geben Sie das Kennwort des Benutzers root (Nextcloud) ein: *****
Wiederholen Sie das Kennwort des Benutzers root (Nextcloud): *****
```

Abb. 69: Kennwort wiederholen für Benutzer root (Nextcloud)

11. Es wird nun ein Dialogfenster zur Dateiauswahl geöffnet. Wählen Sie das zu kopierende Zertifikat aus und klicken Sie auf Öffnen.

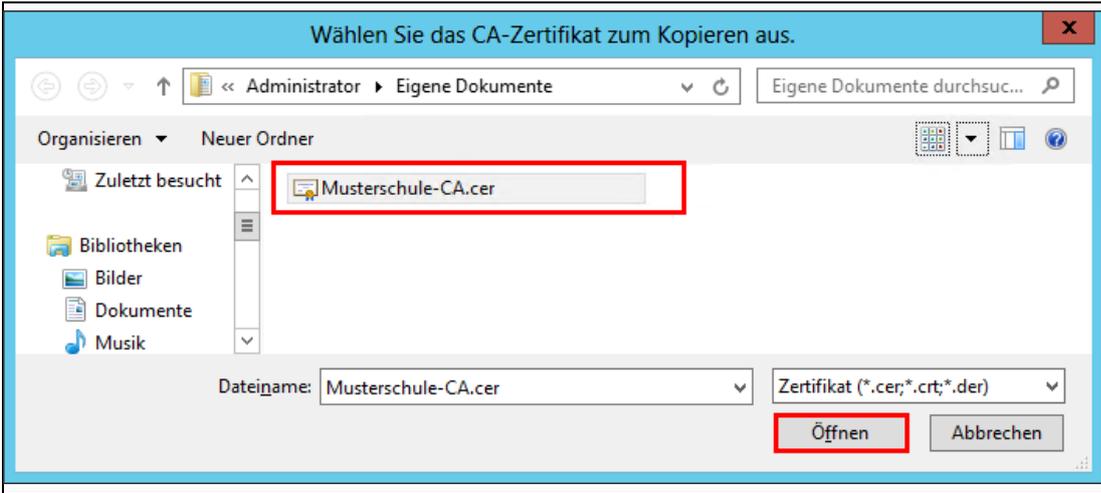


Abb. 70: Zertifikat auswählen

12. Bestätigen Sie die Dateiauswahl mit Ja. Klicken Sie auf Nein, um die Dateiauswahl zu wiederholen.

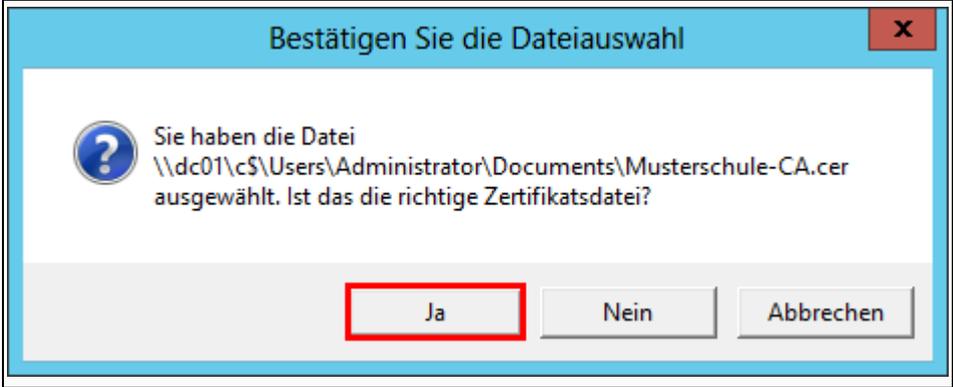


Abb. 71: Dateiauswahl bestätigen

13. Drücken Sie auf eine beliebige Taste, um das Skript zu beenden.

```
[Info] Ihre Domäne ist nun für die Initialisierung der Nextcloud vorbereitet.  
Drücken Sie auf eine beliebige Taste, um das Skript zu beenden:
```

Abb. 72: Skript LMZ-Nextcloud.ps1 beenden

6.1.4 LDAPS mit OctoGate-Zertifikat

6. Drücken Sie auf die Taste **J**.

```
Geben Sie das Kennwort des LDAP-Bindusers ein: *****  
Wiederholen Sie das Kennwort des LDAP-Bindusers: *****  
Möchten Sie LDAPS konfigurieren? [J/N]: j
```

Abb. 73: Soll LDAPS für Nextcloud konfiguriert werden?

7. Beantworten Sie die darauffolgende Frage mit **Nein**, indem Sie auf die Taste **N** drücken.

```
Möchten Sie LDAPS konfigurieren? [J/N]: j  
Haben Sie mit New-paedMLCAOnDC.ps1 ein neues LDAPS-Zertifikat importiert? [J/N]: n
```

Abb. 74: Wurden LDAPS-Zertifikate mit New-paedMLCAOnDC.ps1 generiert?

8. Drücken Sie auf die Taste **J**, um die Frage nach dem Hostzertifikat von OctoGate mit Ja zu beantworten.

```
Haben Sie mit New-paedMLCAOnDC.ps1 ein neues LDAPS-Zertifikat importiert? [J/N]: n  
Wurde LDAPS mit einem Hostzertifikat von OctoGate eingerichtet? [J/N]: J
```

Abb. 75: OctoGate Hostzertifikat?

9. Geben Sie das Kennwort des Benutzers **root** der **Nextcloud-VM** ein. Wenn Ihre Nextcloud zum ersten Mal initialisiert wird, dann lautet das Kennwort „**NextCloud**“ (ohne Anführungszeichen!).

```
Geben Sie das Kennwort des Benutzers root (Nextcloud) ein: *****  
Wiederholen Sie das Kennwort des Benutzers root (Nextcloud): _
```

Abb. 76: Kennwort für Benutzer root (Nextcloud)

10. Wiederholen Sie die Kennworteingabe.

```
Geben Sie das Kennwort des Benutzers root (Nextcloud) ein: *****  
Wiederholen Sie das Kennwort des Benutzers root (Nextcloud): *****
```

Abb. 77: Kennwort wiederholen für Benutzer root (Nextcloud)

11. Drücken Sie auf eine beliebige Taste, um das Skript zu beenden.

```
[Info] Ihre Domäne ist nun für die Initialisierung der Nextcloud vorbereitet.  
Drücken Sie auf eine beliebige Taste, um das Skript zu beenden:
```

Abb. 78: Skript LMZ-Nextcloud.ps1 beenden

6.2 Nextcloud-VM initialisieren

Nachdem Sie soeben die notwendigen Ergänzungen im AD vorgenommen haben, geht es weiter mit der Initialisierung der Nextcloud-VM.

Die Initialisierung kann dabei entweder direkt auf der Server-Konsole der VM über den ESXi-Host erfolgen oder über einen SSH-Client wie PuTTY. Nachfolgend beschreiben wir die Initialisierung auf der Server-Konsole.



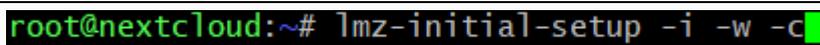
Um eine bessere Darstellung der Inhalte zu erreichen, wurden die Screenshots aus einer PuTTY-Sitzung entnommen. Inhaltliche Unterschiede ergeben sich dadurch nicht.



Wenn Sie das nachfolgend beschriebene Initialisierungsskript in PuTTY ausführen, dann muss es in einer gesonderten Screen-Sitzung ausgeführt werden.

1. Melden Sie sich als Benutzer `root` auf der Server-Konsole der Nextcloud an. Das Kennwort lautet „`NextCloud`“. Achten Sie bei der Eingabe des Kennworts auf die Groß- und Kleinschreibung.
2. Führen Sie folgenden Befehl aus.

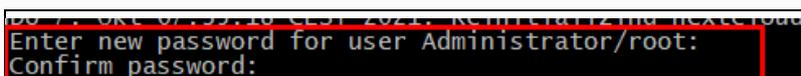
```
lmz-initial-setup -i -w -c
```



```
root@nextcloud:~# lmz-initial-setup -i -w -c
```

Abb. 79: `lmz-initial-setup` ausführen

3. Legen Sie ein hinreichend sicheres Kennwort (mindestens 8 Zeichen) für die beiden Benutzerkonten **Administrator** und **root** fest. Wiederholen Sie das Kennwort zur Kontrolle (*Confirm password*).
4. Notieren Sie sich das Kennwort z. B. in einem Kennwortsafe.



```
Enter new password for user Administrator/root:  
Confirm password:
```

Abb. 80: `lmz-initial-setup` -> Kennwort für Administrator/root



Verwechseln Sie den Benutzer Administrator nicht mit dem Administrator Ihrer Domäne!

Hierbei handelt es sich um das Admin-Konto, das dazu genutzt wird, um UCS zu konfigurieren. Aus diesem Grund empfehlen wir, ein separates Kennwort festzulegen. Das heißt konkret: Das Kennwort des UCS-Administrators sollte sich vom Kennwort des Domänen-Admins unterscheiden.

5. Geben Sie das Kennwort des Benutzerkontos **ldapnextcloud** ein. Das Kennwort haben Sie zuvor vergeben. Es handelt sich um den LDAP-Binduser und sein Kennwort) (vgl. [Kapitel 6.1 Anpassungen in AD und DNS](#)).

Nach der Eingabe des Kennworts für das Benutzerkonto Idapnextcloud erscheint sofort eine weitere Eingabeaufforderung zur Eingabe Ihrer externen Domäne für Ihre Nextcloud.



Da im Gegensatz zu der Kennworteingabe für den Benutzer root und Administrator keine Kennwortüberprüfung durch wiederholte Eingabe erfolgt, besteht hier die Gefahr, dass Sie statt der externen Domäne das Kennwort des Benutzerkontos Idapnextcloud eingeben. Das führt dazu, dass Ihre Nextcloud aus dem Internet so lange nicht erreichbar ist, bis dieser Fehler korrigiert wurde.

```
Active directory Idapnextcloud password: █
```

Abb. 81: Imz-initial-setup -> Kennwort für Idapnextcloud

6. Geben Sie den **vollständigen Namen (FQDN) Ihrer externen Domäne** ein. Beim Einsatz der OctoGate als Firewall, ist es der **FQDN Ihrer OctoGate**, zum Beispiel `abcdefgh.ozone.octogate.de`.

```
Active directory Idapnextcloud password:
External web address for this server: █.ozone.octogate.de
```

Abb. 82: Imz-initial-setup -> FQDN der OctoGate

7. Legen Sie ein hinreichend sicheres Kennwort für das Benutzerkonto **nc_admin** fest.
8. Notieren Sie das Kennwort z. B. in einem Kennwortsafe.



Das Benutzerkonto `nc_admin` gehört dem Administrator der Nextcloud. Das heißt: Alle Änderungen für Nextcloud werden mithilfe dieses Benutzerkontos vorgenommen.

```
Type a secure password!
Enter new password for user nc_admin: █
```

Abb. 83: Imz-initial-setup -> Kennwort für nc_admin

9. Wiederholen Sie das Kennwort für das Benutzerkonto **nc_admin**.

```
Type a secure password!
Enter new password for user nc_admin:
Confirm password: █
```

Abb. 84: Imz-initial-setup -> Kennwort für nc_admin wiederholen

10. Geben Sie Ihre **MLI-Nummer** ein.

```
Please enter your customer id: MLI-xxxxx █
```

Abb. 85: Imz-initial-setup -> Eingabe MLI-Nummer

11. Geben Sie das Kennwort für Ihre MLI-Nummer ein.

```
Please enter your customer id: MLI-█
Enter password for user MLI-█: █
```

Abb. 86: Imz-initial-setup -> Eingabe MLI-Nummer

- Warten Sie, bis das Skript durchgelaufen ist. Das dauert einige Minuten.
Am Ende der Initialisierung werden Sie aufgefordert, den Server neu zu starten. Drücken Sie auf die **ENTER**-Taste, um den Neustart anzustoßen.
- Warten Sie kurz bis Nextcloud gestartet ist, bevor Sie weiterarbeiten.



Sollte es während der Initialisierung zu Fehlern kommen, kopieren Sie die Log-Datei `paedml-initial-setup.log` aus dem Ordner `/var/log` und fügen Sie sie dem Anhang Ihrer E-Mail an windows-hotline@lmz-bw.de bei.

Die Log-Datei können Sie mit einem geeigneten Tool – zum Beispiel WinSCP – auf Ihren Computer übertragen.

6.3 UCS-Zertifikat importieren

Nach der Initialisierung der Nextcloud ist es notwendig, das CA-Zertifikat des UCS auf alle Geräte in Ihrem Schulnetz zu kopieren, um Anmeldestörung aufgrund eines nicht validierten Serverzertifikats vermeiden zu können.

- Melden Sie sich als Domänen-Admin am Server **SP01** an.
- Öffnen Sie im Datei-Explorer den Ordner `D:\Installation\paedML\Erweiterungen\Nextcloud`.
- Führen Sie das PowerShell-Skript `LMZ-CopyUCSCert.ps1` aus.
- Öffnen Sie im Datei-Explorer den Ordner `\\DC01\netlogon\paedML_3.0\Nextcloud\CACert`. Kontrollieren Sie, ob sich die Datei `ucs-root-ca.crt` darin befindet.



Abb. 87: CA-Zertifikat `ucs-root-ca.crt`

Während der Vorbereitung wurde unter anderem das GPO `paedML_Computer_alle_Nextcloud_CA-Cert_v1.0` importiert und mit der OU Computer verknüpft. Dieses GPO sorgt dafür, dass alle Domänengeräte mit der Ausnahme von DC01 und SP01 das CA-Zertifikat des UCS (das ist der Host, der die Nextcloud als Dienst bereitstellt) beim nächsten Neustart installieren. Damit das funktioniert muss die Zertifikatsdatei wie oben beschrieben von UCS in das NETLOGN-Verzeichnis kopiert werden.

7 Abschlussarbeiten

7.1 Quota für alle Benutzer setzen



Aufgrund eines fehlenden Befehls in einem der Initialisierungsskripte wird keine Quota-Beschränkung für den Speicherplatz gesetzt.

Es ist wichtig, dass Sie den in diesem Kapitel beschriebenen Befehl unbedingt ausführen, bevor Sie Ihre Nextcloud allen Benutzern zur Nutzung freigeben!

Wenn Sie keine Quota-Beschränkung definieren, dann laufen Sie die Gefahr, dass es auf der Festplatte Ihrer Nextcloud-VM bald keine freie Speicherkapazität mehr zur Verfügung steht. Im schlimmsten Fall kann das dazu führen, dass die Nextcloud nicht mehr genutzt werden kann.

1. Öffnen Sie den **Webclient Ihres ESXi-Hosts** in einem Browser und melden Sie sich als **Administrator** bzw. als Benutzer **root** an.
2. Öffnen Sie die Konsolenansicht der Nextcloud-VM (Webkonsole oder Remote-Konsole).
3. Melden Sie sich als Benutzer **root** in der Nextcloud-VM an.
4. Führen Sie folgenden Befehl aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:app:set files default_quota --value="0 B"
```

```
root@nextcloud:~# univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:app:set files default_quota --value="0 B"
```

Abb. 88: Quota-Beschränkung setzen

Der Befehl sorgt dafür, dass die Benutzer keine Dateien direkt in den Datastore der Nextcloud speichern können. Dadurch sorgen Sie dafür, dass Ihre Benutzer ihre Dateien stets in ihrem Home- bzw. in einem Tauschverzeichnis auf dem Server SP01 speichern.

7.2 Tauschlaufwerke für Schülerinnen und Schüler freigeben



Aufgrund einer fehlenden Angabe in einer Konfigurationsdatei stehen den Schülerinnen und Schülern – im Gegensatz zu den Lehrkräften – kein Tauschverzeichnis zur Verfügung, wenn sie sich in Nextcloud angemeldet haben.

In diesem Kapitel beschreiben wir, wie Sie Schülerinnen und Schülern ihre Tauschverzeichnisse bereitstellen.

1. Kehren Sie zurück auf SP01.
2. Öffnen Sie in Ihrem Browser die URL <https://nextcloud.paedml.lokal/nextcloud>.
3. Melden Sie sich als Benutzer **nc_admin** an.
4. Klicken Sie auf das Admin-Icon und anschließend auf Einstellungen.

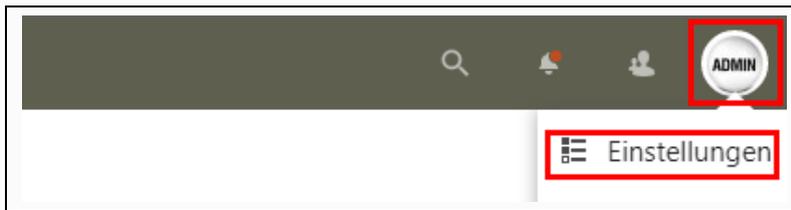


Abb. 89: Nextcloud -> Einstellungen

5. Klicken Sie im Menü-Bereich Verwaltung auf den Link **Externe Speicher**.

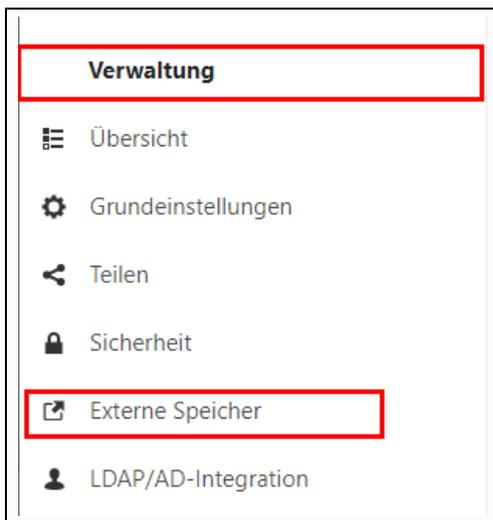


Abb. 90: Nextcloud -> Einstellungen -> Externe Speicher

6. Fügen Sie für den (schon vorhandenen) externen Speicher **T-Tausch** (1) die Sicherheitsgruppen Ihrer Schüler hinzu (2), zum Beispiel `G_Schueler_RS`. Klicken Sie anschließend auf das Häkchen , um die Änderung zu speichern.

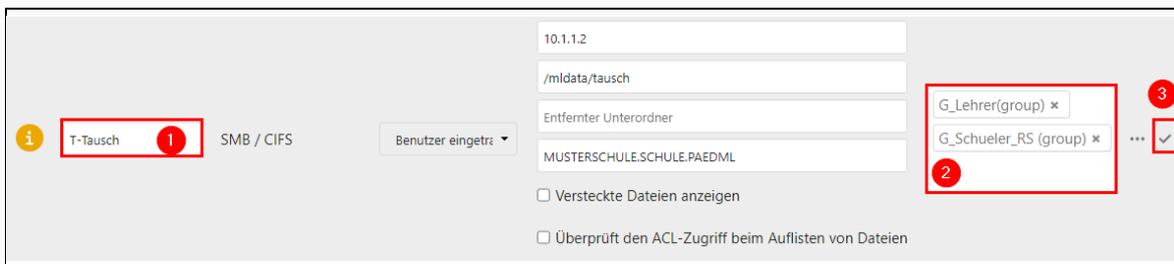


Abb. 91: Tauschverzeichnis für Schüler freigeben



Wenn mehrere Schularten in Ihrer paedML® Windows abgebildet sind, fügen Sie die Sicherheitsgruppen der jeweiligen Schularten hinzu. Verwenden aus Datenschutzgründen nicht die übergreifende Sicherheitsgruppe `G_Schueler`.

7.3 App Center App Let's Encrypt aktualisieren



Zum Zeitpunkt der Fertigstellung dieser Anleitung hat Univention eine Aktualisierung der App Let's Encrypt veröffentlicht. Da sie in der Version 1.2.2-20 einen Bug behebt, der beim Erneuern eines Let's Encrypt Zertifikats auftreten kann, empfehlen wir Ihnen, die App zu aktualisieren.

1. Öffnen Sie im Browser die Univenton Management Console (UMC), indem Sie die URL <https://nextcloud.paedml.lokal> öffnen.
2. Klicken Sie auf die Schaltfläche **ANMELDEN**.

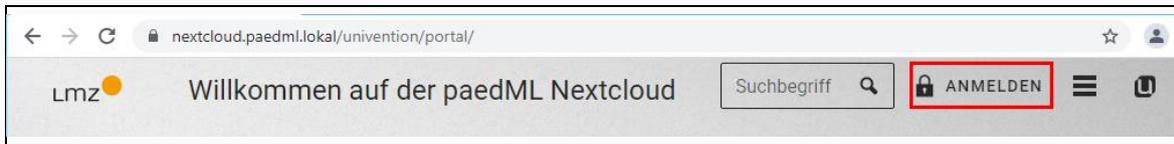


Abb. 92: Anmelden in UMC

3. Melden Sie sich als Benutzer **Administrator**. Das Kennwort haben Sie während der Initialisierung der Nextcloud-VM festgelegt. **Achten Sie unbedingt auf die Schreibweise: Der Benutzername Administrator muss mit dem Großbuchstaben A beginnen!**

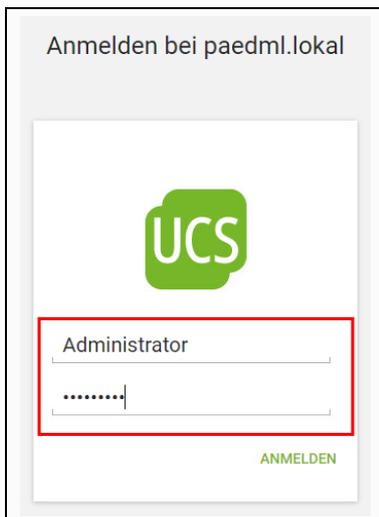


Abb. 93: Anmelden bei paedml.lokal

4. Klicken Sie auf die Kachel **System- und Domäneneinstellungen** unter der Rubrik **Verwaltung**.



Abb. 94: System- und Domäneneinstellungen

5. Öffnen Sie die Seite **Software**.

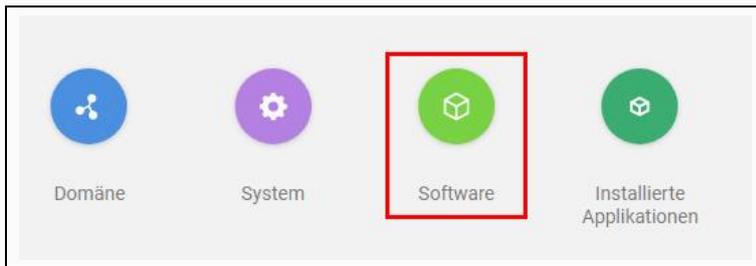


Abb. 95: System- und Domäneneinstellungen -> Software

6. Klicken Sie auf **App Center**.

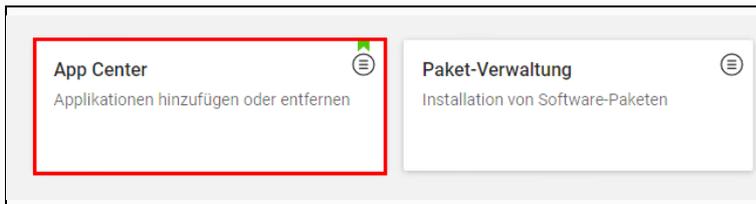


Abb. 96: System- und Domäneneinstellungen -> Software -> App Center

7. Schließen Sie den Info-Dialog zur App Center mit einem Klick auf **FORTFAHREN**.

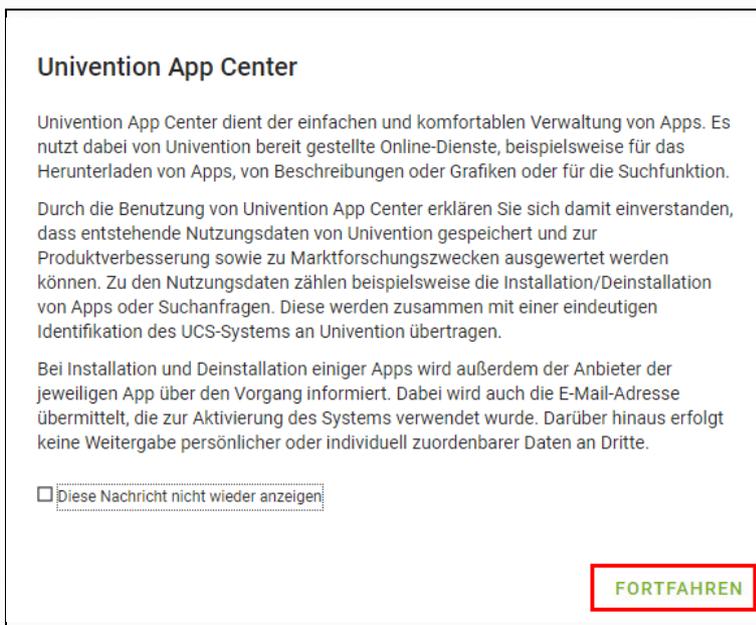


Abb. 97: Hinweis zu Univention App Center

8. Klicken Sie auf die Kachel **Let's Encrypt** bei **Installiert**.

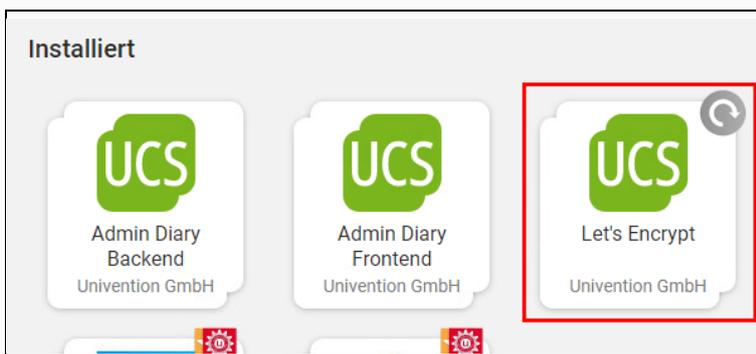


Abb. 98: App Center -> Let's Encrypt

9. Kontrollieren Sie zunächst, ob die **Version 1.2.2-20 oder höher als verfügbares Update** erscheint.

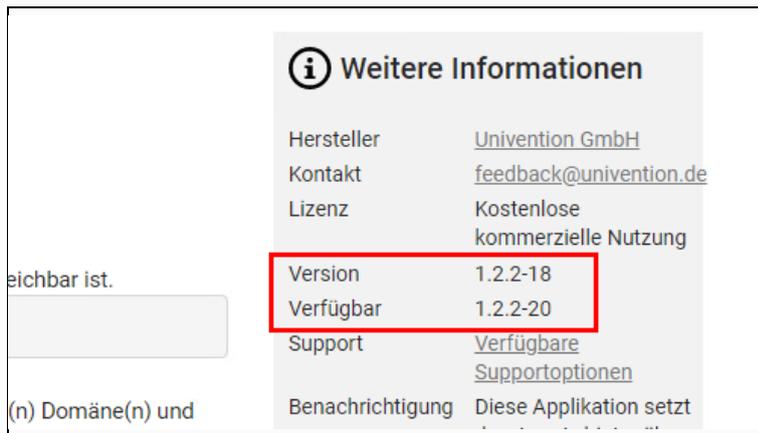


Abb. 99: Let's Encrypt -> Update verfügbar

10. Falls die Version 1.2.2-20 oder eine höhere Version verfügbar ist, scrollen Sie das Browserfenster so lange herunter, bis die Schaltfläche **AKTUALISIEREN** bei **Installation lokal verwalten** zu sehen ist. Starten Sie die Aktualisierung mit **AKTUALISIEREN**.

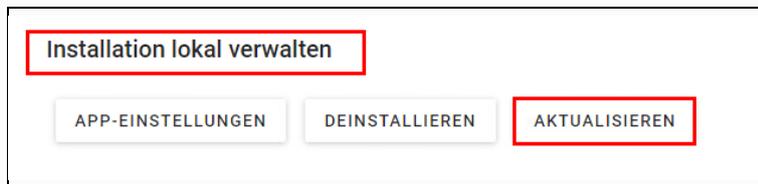


Abb. 100: Let's Encrypt -> Aktualisieren

11. Sie erhalten nun ChangeLog-Information zur neuen Version. Klicken Sie erneut auf **AKTUALISIEREN**.

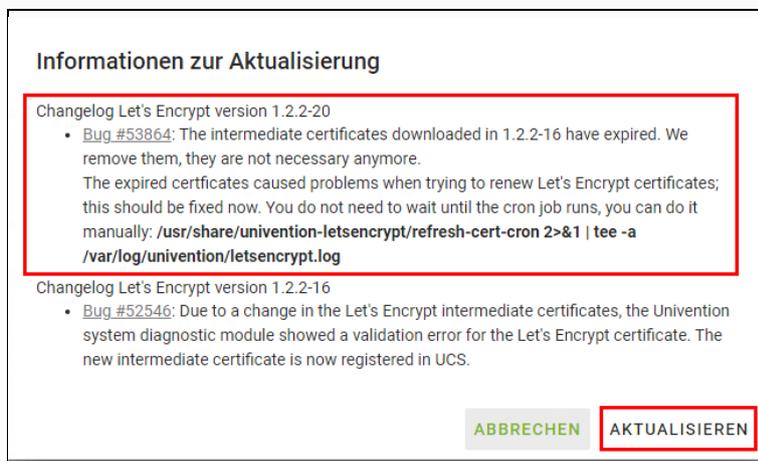


Abb. 101: Let's Encrypt -> ChangeLog

12. Falls das nachfolgende Dialogfenster erscheint, klicken Sie auf **TROTZDEM AKTUALISIEREN**.



Abb. 102: Let's Encrypt -> Aktualisierung bestätigen

Kontrollieren Sie die Versionsnummer nach erfolgreicher Aktualisierung der App.



Abb. 103: Let's Encrypt -> Aktualisierung abgeschlossen

7.4 Zertifikatdateien bereinigen

Falls Sie LDAPS-Zertifikate wie im [Kapitel 5.2 LDAPS einrichten](#) beschrieben als Vorbereitung für die Initialisierung der Nextcloud generiert haben, können Sie nun entscheiden, ob Sie die dabei generierten Dateien behalten oder entfernen möchten.

Sie finden diese sowohl auf dem Server DC01 als auch auf dem Server SP01 im Ordner `D:\pa-edML_certs`.



Behalten Sie diese Dateien nur dann, wenn Sie vorhaben, weitere Zertifikate für Ihre Zwecke selbst generieren wollen. Das gilt insbesondere für die beiden Dateien `ca.crt` und `ca.key` auf Dem Server DC01. Denn der Diebstahl dieser beiden Dateien kann dazu führen, dass ein Unberechtigter mit deren Hilfe beliebige Serverzertifikate für Ihre Server erzeugen und missbrauchen kann.

7.5 Snapshot bereinigen, falls vorhanden

Falls Sie vor der Initialisierung der Nextcloud wie im [Kapitel 3.3 Snapshot erstellen](#) vorgeschlagen ein Snapshot Ihrer Nextcloud-VM erstellt haben, sollten Sie Ihre VM nun herunterfahren und das Snapshot entfernen.

8 Backup

Integrieren Sie Ihre Nextcloud-VM in Ihre Backuplösung. Wir empfehlen spätestens mit der Einführung der Nextcloud als private Cloud ein tägliches Backup, um Dateninkonsistenzen bei einem Ausfall einer der VMs oder des Hosts zu minimieren.



Die Dateien Ihrer Nextcloud-Benutzer liegen auf dem Server der paedML® Windows, genauer: In den persönlichen Home- und den Tauschverzeichnissen der Benutzer.

Das heißt: Ein Backup der Nextcloud-VM dient primär dazu, dass sowohl die Benutzer- als auch die Konfigurationsdatenbank der Nextcloud gesichert und im Bedarfsfall zügig wiederhergestellt werden kann.

Anhang A Nützliche Ergänzungen

A.1 Verknüpfung auf Client-Desktops

Durch das Ausführen des Skripts LMZ-Nextcloud.ps1 aus dem [Kapitel 6.1 Anpassungen in AD und DNS](#) werden zwei neue Gruppenrichtlinienobjekte (GPO) in AD hinzugefügt:

- **paedML_Computer_alle_Nextcloud_CACert_v1.0 (verknüpft mit der OU Computer)**
Das GPO sorgt dafür, dass das für den Aufruf der Nextcloud aus dem Schulnetz erforderliche Stammzertifikat ucs-root-ca.crt auf alle Clientcomputer in Ihrem Netz ausgerollt wird. Ohne dieses Zertifikat erscheint beim Öffnen der Nextcloud ein Warnhinweis darüber, dass der Benutzer im Begriff sei, eine nicht vertrauenswürdige Website zu öffnen.
- **paedML_Benutzer_alle_Nextcloud_DesktopLink_v1.0 (verknüpft mit der OU Benutzer)**
Das GPO sorgt dafür, dass auf dem Desktop eines Benutzers eine Verknüpfung zu Ihrer Nextcloud hinzugefügt wird. Das heißt: Nach der Anmeldung auf einem Clientcomputer im Schulnetz finden Ihre Benutzer eine Desktop-Verknüpfung namens Nextcloud. Das ermöglicht das Öffnen der Nextcloud ohne die Eingabe der URL in Ihrem Schulnetz.

A.2 Desktop-Verknüpfung deaktivieren

Falls Sie die durch das Skript LMZ-Nextcloud.ps1 automatisch hinzugefügte Desktop-Verknüpfung nicht für sinnvoll halten, deaktivieren Sie das GPO wie folgt:

1. Öffnen Sie als Domänen-Admin die Gruppenrichtlinienverwaltungs-Konsole auf dem Server DC01.
2. Navigieren Sie zur OU Benutzer.

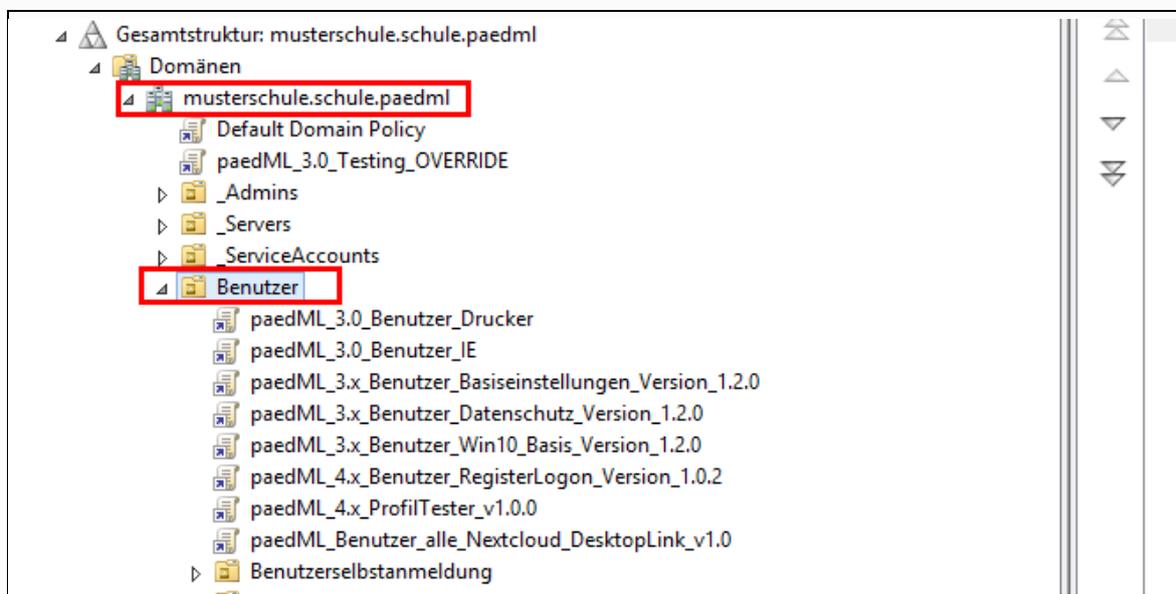


Abb. 104: Gruppenrichtlinienverwaltung -> OU Benutzer

3. Klicken Sie mit der rechten Maustaste auf das GPO paedML_Benutzer_alle_Nextcloud_Desktop-Link_v1.0 und entfernen Sie das Häkchen bei Verknüpfung aktiviert.

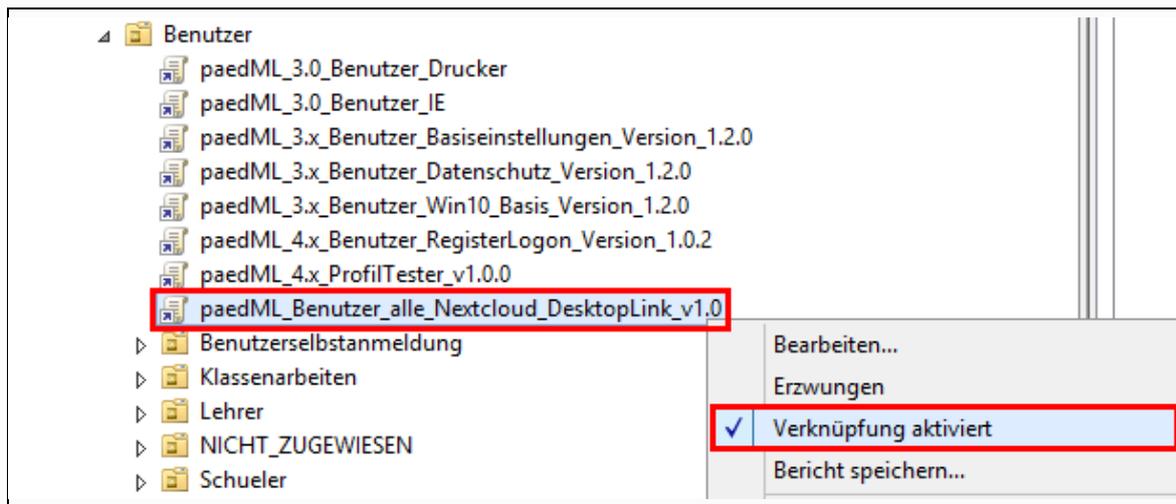


Abb. 105: Verknüpfung für paedML_Benutzer_alle_Nextcloud_DesktopLink_v1.0 deaktivieren

A.3 Desktopverknüpfung mit dem externen FQDN anlegen

Das mitgelieferte GPO **paedML_Benutzer_alle_Nextcloud_DesktopLink_v1.0** fügt auf dem Desktop der Benutzer eine URL-Verknüpfung auf die Nextcloud mit der URL <https://nextcloud.paedml.lokal> hinzu. Wenn Sie die URL stattdessen mit dem externen Domännennamen Ihrer Nextcloud als Desktopverknüpfung bereitstellen wollen, bearbeiten Sie das GPO.

Die gesuchte Einstellung finden Sie unter **Benutzerkonfiguration → Einstellungen → Windows-Einstellungen → Verknüpfungen**.



Abb. 106: Benutzerkonfiguration -> Einstellungen -> Windows-Einstellungen -> Verknüpfungen

Öffnen Sie das Objekt **Nextcloud** und ändern Sie das Ziel auf die URL Ihrer externen Domäne, z.B. <https://cloud.meine-schule.de/nextcloud>.

Name:	<input type="text" value="Nextcloud"/>	...
Zieltyp:	<input type="text" value="URL"/>	▼
Speicherort:	<input type="text" value="Desktop"/>	▼
Ziel-URL:	<input type="text" value="https://cloud.meine-schule.de/nextcloud"/>	...
Argumente:	<input type="text"/>	

Abb. 107: Ziel-URL auf externen FQDN ändern

Anhang BFAQ

B.1 Welche Angaben muss ich zwingend nennen, damit meine Supportanfrage an support@octogate.de zügig bearbeitet werden kann?

Für einen erfolgreichen Betrieb der Nextcloud für paedML® Windows in Kombination mit OctoGate-Firewall ist es notwendig, die Netzwerkschnittstelle DMZ durch den technischen Support unseres Kooperationspartners, OctoGate IT Security Systems GmbH, aktivieren zu lassen.

Damit Ihre Anfrage per E-Mail zügig bearbeitet werden kann, bedarf es einiger Informationen. Das sind:

- **Hostname Ihrer OctoGate-Firewall**
Der Hostname bestehend aus acht Buchstaben dient dazu, um Ihre Firewall und Ihren Kundenstatus zu identifizieren.
- **Muss die Firmware Ihrer Firewall aktualisiert werden?**
Wie in diesem Handbuch beschrieben, muss die Firmware in der Version 3.0.51 oder höher installiert sein. Erfüllt Ihre Firewall diese Voraussetzung nicht, dann müssen Sie zusätzlich angeben, dass ein Upgrade der Firmware erforderlich ist.
- **Aktivierung der Netzwerkschnittstelle DMZ mit der Standard-IP-Adresse 192.168.201.254/24**
Wenn die Schnittstelle DMZ bis jetzt nicht gebraucht wurde und deshalb mit der vorgegebenen IP-Adresse 192.168.201.254/24 konfiguriert werden kann, teilen Sie dem technischen Support explizit mit, dass die Netzwerkschnittstelle DMZ mit der Standard-IP-Adresse aktiviert werden soll.
- **Aktivierung der Netzwerkschnittstelle DMZ mit einer anderen IP-Adresse**
Falls die Netzwerkschnittstelle DMZ bereits anderweitig benutzt wird, dann müssen Sie dem technischen Support zwingend mitteilen, dass eine Konfiguration mit alternativer Adresse erforderlich ist. Das Support-Team der Fa. OctoGate IT Security Systems GmbH hilft Ihnen, einen passenden Lösungsansatz zu finden.
- **Darf der technische Support meine Firewall bei Bedarf automatisch neustarten?**
Es kann unter Umständen nicht ausgeschlossen werden, dass ein Neustart Ihrer Firewall nach der Anpassung und Aktivierung der Netzwerkschnittstelle DMZ erforderlich ist. Teilen Sie daher explizit mit, ob Sie einen automatischen Neustart pauschal gestatten wollen.

Textbausteine für eine Störungsmeldung:

- **PING an 10.1.1.3 und/oder 192.168.201.254 scheitert**

Sehr geehrte Damen und Herren,

ich habe meinen OctoGate-Host gemäß der Anleitung angepasst, um Nextcloud-VM des Landesmedienzentrums BW für paedML Windows integrieren zu können.

Obwohl meine Firmware auf die Version 3.0.51 aktualisiert und die DMZ-Schnittstelle korrekt angepasst wurde, ist es nicht möglich, von meinem Nextcloud-Host (192.168.201.7) aus die IP-Adressen 10.1.1.3 und 192.168.201.254 anzupingen. Bitte sorgen Sie dafür, dass die beiden IP-Adressen per PING erreichbar werden.

Der Name meines OctoGate-Hosts lautet: abcdefgh

Vielen Dank und freundliche Grüße

Monika Mustermann

▪ Firmware muss aktualisiert werden

Sehr geehrte Damen und Herren,

für die Bereitstellung und die Inbetriebnahme der Nextcloud-VM des LMZ BW muss mein OctoGate-Host auf die Version 3.0.51 aktualisiert werden. Aktualisieren Sie bitte meinen OctoGate-Host zum nächstmöglichen Zeitpunkt. Falls ein Neustart des OctoGate-Hosts erforderlich ist, bitte ich Sie um eine Angabe darüber, wann die Aktualisierung stattfinden wird.

Der Name meines OctoGate-Hosts lautet: abcdefgh

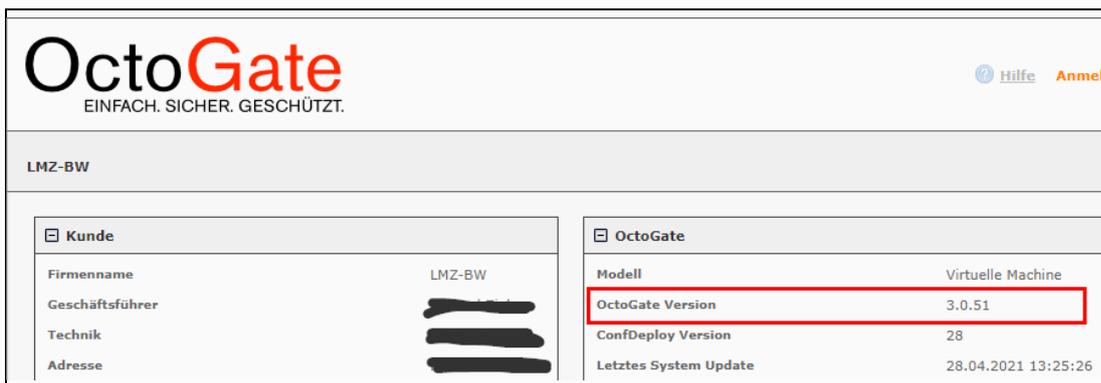
Vielen Dank und freundliche Grüße

Monika Mustermann

B.2 Trouble-Shooting: Octogate

B.2.1 Wie bzw. wo finde ich die Firmware-Version meiner OctoGate Firewall?

Die Firmware-Version finden Sie zum Beispiel auf der WebGUI-Oberfläche Ihrer OctoGate.



LMZ-BW	
Kunde	
Firmenname	LMZ-BW
Geschäftsführer	██████████
Technik	██████████
Adresse	██████████
OctoGate	
Modell	Virtuelle Maschine
OctoGate Version	3.0.51
ConfDeploy Version	28
Letztes System Update	28.04.2021 13:25:26

Abb. 108: Version der OctoGate

B.2.2 Meine OctoGate Firewall läuft mit einer älteren Firmware-Version. An wen muss ich mich wenden, um sie auf die Version 3.0.51 oder höher aktualisieren zu können?

Wenden Sie sich direkt an den Support der Fa. OctoGate. Welche Angaben Sie dafür machen müssen finden Sie in [B.1 Welche Angaben muss ich zwingend nennen, damit meine Supportanfrage an support@octogate.de zügig bearbeitet werden kann? Auf Seite 57.](#)

B.2.3 Abweichende IP-Adresse von eth1

Wenn Sie die Schnittstelle eth1 bereits nutzen, um ein eigenes Netz abzubilden, dann sollten Sie wie im [Kapitel 2 DMZ einrichten ab Seite 11](#) beschrieben einen zusätzlichen vSwitch hinzufügen und die IP-Adressen gemäß unserer Vorgabe definieren.

Für die Anpassung der notwendigen Firewall-Regeln wenden Sie sich direkt an den Support der Fa. OctoGate. Welche Angaben Sie dafür angeben müssen finden Sie in [B.1 Welche Angaben muss ich zwingend](#)

nennen, damit meine Supportanfrage an support@octogate.de zügig bearbeitet werden kann? auf Seite 57.

B.3 LDAP/LDAPS

B.3.1 Obwohl LDAPS eingerichtet ist, findet das Skript Get-LDAPSCertificate.ps1 keine LDAPS-Konfiguration

Für eine erfolgreiche Überprüfung einer korrekten LDAPS-Konfiguration muss das Serverzertifikat validiert werden können. Gelingt dies nicht, nehmen wir an, dass LDAPS nicht eingerichtet ist. Prüfen Sie folgendes:

Fallbeispiel 1: Hostzertifikat für LDAPS wurde für das Dienstkonto Active Directory-Domänendienste importiert.

1. Melden Sie sich am Server DC01 als Domänen-Admin an.
2. Öffnen Sie **MMC** und fügen Sie das Snap-In **Zertifikate** für den Dienst **Active Directory-Domänendienste** hinzu. Wie das geht, finden Sie z.B. im [Anhang C LDAPS einrichten mit OctoGate-Zertifikat](#).
3. Erweitern Sie die Struktur **Zertifikate – Dienst (Active Directory-Domänendienste)** und prüfen Sie nach, ob im Speicher **NTDS\Eigene Zertifikate** ein Zertifikat zu finden ist.

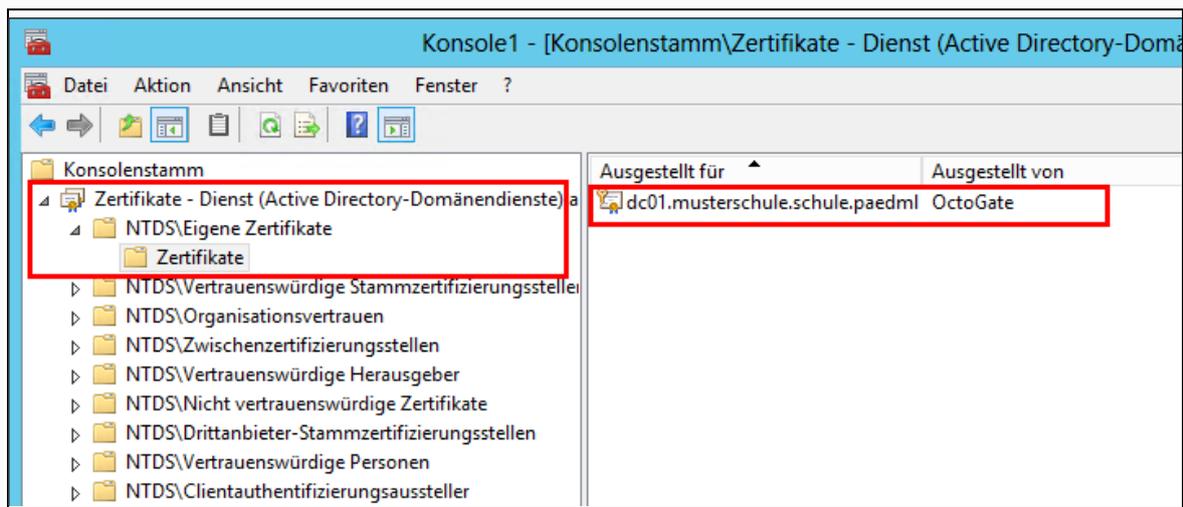


Abb. 109: Zertifikate – Dienst (Active Directory-Domänendienste) -> NTDS\Eigene Zertifikate

Falls Sie darin ein Hostzertifikat – üblicherweise mit dem vollständigen Domännennamen des DC01 dc01.musterschule.schule.paedml – vorfinden, notieren Sie den Namen des Ausstellers. Im obigen Beispiel ist der Aussteller OctoGate.

4. Erweitern Sie die Struktur NTDS\Vertrauenswürdige Stammzertifizierungsstelle und prüfen Sie nach, ob Sie darin das Zertifikat des Ausstellers finden.

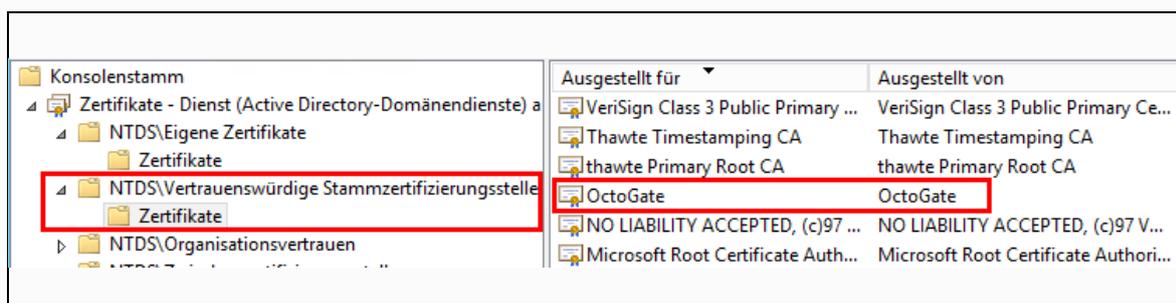


Abb. 110: Zertifikate – Dienst (Active Directory-Domänendienste) -> NTDS\Vertrauenswürdige Stammzertifizierungsstelle

Finden Sie in diesem Zertifikatspeicher kein Zertifikat des im Schritt 3 festgestellten Ausstellers, müssen Sie das fehlende Zertifikat des Ausstellers importieren. Wenn Sie anschließend das Skript `Get-LDAPSCertificate.ps1` erneut ausführen, sollte ein positives Ergebnis erfolgen. (Vgl. [Kapitel 5.1 LDAPS-Zertifikat ermitteln](#))

Fallbeispiel 2: Hostzertifikat für LDAPS wurde für das Computerkonto importiert.

1. Melden Sie sich am Server DC01 als Domänen-Admin an.
2. Öffnen Sie **MMC** und fügen Sie das Snap-In **Zertifikate** für das Computerkonto lokaler Computer. Wie das geht, finden Sie z.B. im [Kapitel 5.1 LDAPS-Zertifikat ermitteln ab Seite 28](#).
3. Erweitern Sie die Struktur **Zertifikate (Lokaler Computer)** und prüfen Sie nach, ob im Speicher **Eigene Zertifikate** ein Zertifikat zu finden ist.

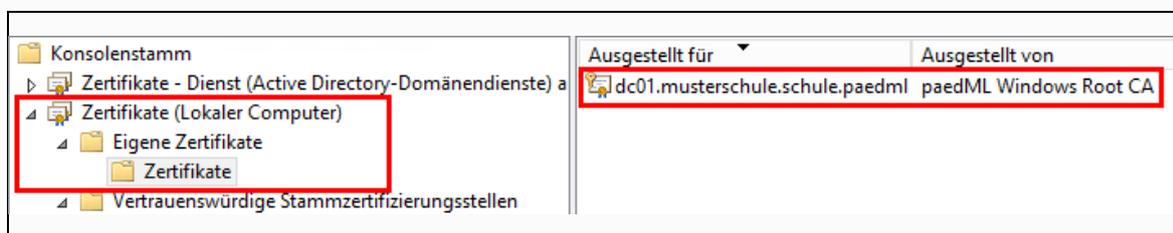


Abb. 111: Zertifikate (Lokaler Computer) -> Eigene Zertifikate

Falls Sie darin ein Hostzertifikat – üblicherweise mit dem vollständigen Domännennamen des DC01 `dc01.musterschule.schule.paedml` – vorfinden, notieren Sie den Namen des Ausstellers. Im obigen Beispiel heißt der Aussteller `paedML Windows Root CA`.

4. Erweitern Sie die Struktur Vertrauenswürdige Stammzertifizierungsstelle und prüfen Sie nach, ob Sie darin das Zertifikat des Ausstellers finden.

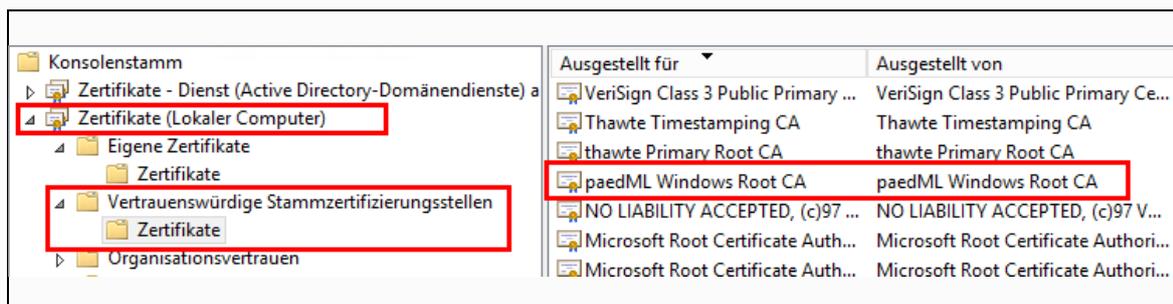


Abb. 112: Zertifikate (Lokaler Computer) -> Eigene Zertifikate -> Vertrauenswürdige Stammzertifizierungsstelle

Finden Sie in diesem Zertifikatspeicher kein Zertifikat des im Schritt 3 festgestellten Ausstellers, müssen Sie das fehlende Zertifikat des Ausstellers importieren. Wenn Sie anschließend das Skript `Get-LDAPSCertificate.ps1` erneut ausführen, sollte ein positives Ergebnis erfolgen. (Vgl. [Kapitel 5.1 LDAPS-Zertifikat ermitteln](#))

B.3.2 Mein LDAPS-Zertifikat konnte nicht auf die Nextcloud-VM kopiert werden. Wo muss ich sie manuell kopieren?

Falls es während des Kopiervorgangs – z.B. durch Firewall oder Virenschanner – zu einem Kopierfehler kommt, können Sie ihre Zertifikatsdatei mit einem Tool wie z.B. WinSCP auf Ihre Nextcloud-VM kopieren.

Die Datei **muss** in den Ordner `/usr/local/share/ca-certificates` auf der Nextcloud-VM kopiert und **unter dem Namen `paedMLWinCACert.crt` gespeichert werden.**

Wenn auf Ihrem Server ein SSH-Client wie z.B. PuTTY installiert ist, dann können Sie Ihre Zertifikatsdatei in PowerShell oder CMD mit folgendem Befehl – Achtung alles in einer einzigen Zeile – kopieren:

```
pscp.exe -q -l root -pw "NextCloud" C:\tmp\Meine-CA.crt  
192.168.201.7:/usr/local/share/ca-certificates/paedMLWinCACert.crt
```

Das Speichern der Zertifikatsdatei unter dem Namen `paedMLWinCACert.crt` sorgt dafür, dass das Initialisierungsskript `lmz-initial-setup` (siehe [Kapitel 6.2 Nextcloud-VM initialisieren](#)) sie erkennt und Ihre Nextcloud automatisch für LDAPS-Verbindung konfiguriert.

B.4 Eigene externe Domäne verwenden

Für den Fall, dass Sie eine eigens für die Nextcloud reservierte externe Domäne nutzen müssen, brauchen Sie insgesamt 4 Konfigurationsanpassungen:

- Portweiterleitungen für HTTP (wird für Let's Encrypt Zertifikat benötigt) und HTTPS.
- Aufnahme der externen Domäne als Trusted Domain in Nextcloud
- Konfigurationsdatei `/etc/lmz-base.config` bearbeiten
- DNS-Eintrag auf DC01

Diese 4 Schritte beschreiben wir im Folgenden an einem Beispiel. Für das Beispiel nutzen wir eine externe Domäne namens `mycloud.meine-schule.de`.

Portweiterleitungen

1. Öffnen Sie im Browser die OctoGate WebGUI und melden Sie sich als Benutzer **admin** an.
2. Klicken Sie auf `Firewall` und anschließend `Portweiterleitungen`.



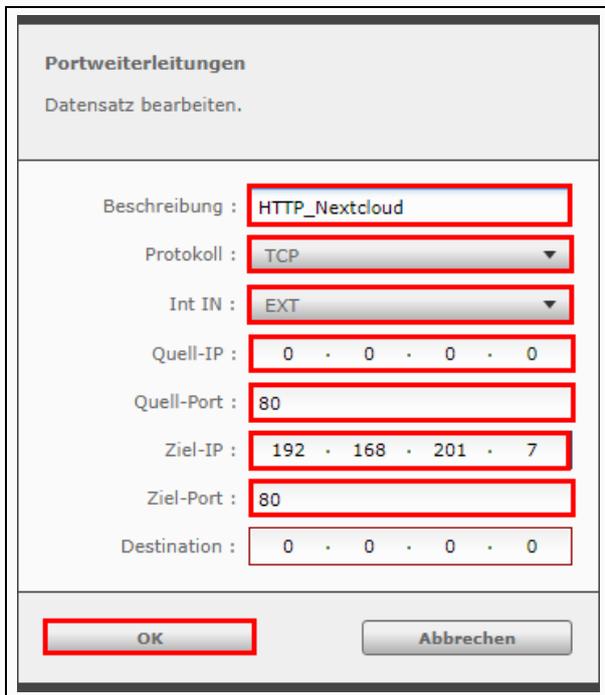
Abb. 113: Firewall -> Portweiterleitungen

3. Klicken Sie auf Neuer Eintrag.



Abb. 114: Portweiterleitungen für 80 und 443

4. Konfigurieren Sie eine Weiterleitungsregel für das **Protokoll HTTP (Port 80)**, indem Sie als **Quell-Port und Ziel-Port 80** eintragen. Übernehmen Sie die Konfiguration mit **OK**.



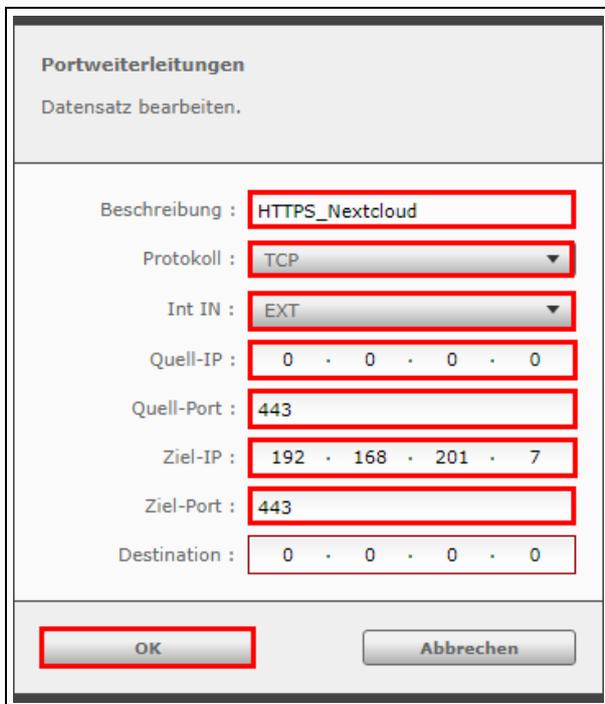
The screenshot shows the 'Portweiterleitungen' dialog box with the following configuration:

- Beschreibung: HTTP_Nextcloud
- Protokoll: TCP
- Int IN: EXT
- Quell-IP: 0 . 0 . 0 . 0
- Quell-Port: 80
- Ziel-IP: 192 . 168 . 201 . 7
- Ziel-Port: 80
- Destination: 0 . 0 . 0 . 0

Buttons: OK, Abbrechen

Abb. 115: Portweiterleitungen für HTTP, Port 80

5. Konfigurieren Sie eine Weiterleitungsregel für das **Protokoll HTTPS (Port 443)**, indem Sie als **Quell-Port und Ziel-Port 443** eintragen. Übernehmen Sie die Konfiguration mit **OK**.



The screenshot shows the 'Portweiterleitungen' dialog box with the following configuration:

- Beschreibung: HTTPS_Nextcloud
- Protokoll: TCP
- Int IN: EXT
- Quell-IP: 0 . 0 . 0 . 0
- Quell-Port: 443
- Ziel-IP: 192 . 168 . 201 . 7
- Ziel-Port: 443
- Destination: 0 . 0 . 0 . 0

Buttons: OK, Abbrechen

Abb. 116: Portweiterleitungen für HTTPS, Port 443

6. Klicken Sie auf **Speichern**, um die beiden, neuen Regeln dauerhaft zu übernehmen.



Abb. 117: Änderungen speichern

7. Beantworten Sie die anschließende Kontrollabfrage mit **Übernehmen**.



Abb. 118: Änderungen übernehmen

Externe Domäne als Trusted Domain für Nextcloud hinzufügen

Melden Sie sich als Benutzer root in der Nextcloud-VM an und führen Sie folgenden Befehl aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:system:get trusted_domains
```

Zählen Sie die ausgegebenen Zeilen. Standardmäßig finden Sie immer die nachfolgenden drei Zeilen:

```
nextcloud.paedml.lokal
192.168.201.7
*.ozone.octogate.de
```

Fügen Sie Ihre eigene Domäne wie folgt hinzu. Sie müssen dabei eine Index-Nummer angeben. Da die Zählung der Index-Nummer stets von 0 beginnt, ist die Zahl genauso groß wie die Anzahl der Zeilen, die der oben genannte Befehl ausgibt. In diesem Beispiel lautet die Index-Nummer demnach: 3.

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:system:set trusted_domains 3 --value="mycloud.meine-schule.de"
```

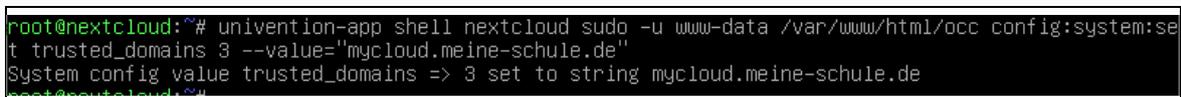


Abb. 119: OCC set trusted_domains

Kontrollieren Sie das Ergebnis mit:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:system:get trusted_domains
```

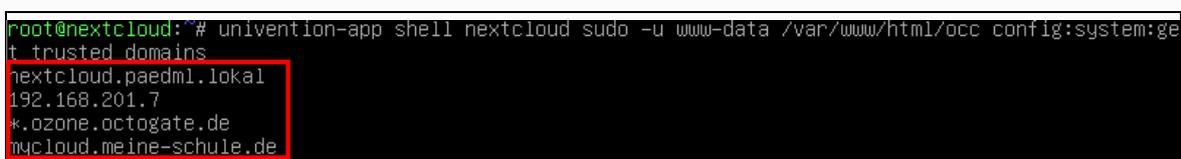


Abb. 120: OCC get trusted_domains

/etc/lmz-base.config bearbeiten

Öffnen Sie die Datei `/etc/lmz-base.config` mit dem Editor **mcedit**.

```
mcedit /etc/lmz-base.config
```

```
root@nextcloud:~# mcedit_/etc/lmz-base.config
```

Abb. 121: `/etc/lmz-base.config` in einem Editor öffnen.



Die Wahl des Editors ist selbstverständlich Ihnen überlassen. Wir haben uns für dieses Beispiel für **mcedit** entschieden, da seine Oberfläche und Bedienung den meisten Windows-Benutzern eher vertraut erscheinen dürfte.

Auf UCS finden Sie u.a. die Editoren *nano*, *pico*, *vi(m)* und sogar *emacs*.

Korrigieren Sie Ihre externe Domäne und speichern Sie die Datei mit der **F2**-Taste.

```
/etc/lmz-base.config [-M--] 14 L:[ 1+13 14/ 15] *(485 / 509b) 0109 0x06D
# Warning: This file is auto-generated and might be overwritten by
# univention-config-registry.
# Please edit the following file(s) instead:
# Warnung: Diese Datei wurde automatisch generiert und kann durch
# univention-config-registry ueberschrieben werden.
# Bitte bearbeiten Sie an Stelle dessen die folgende(n) Datei(en):
#
# <---->/etc/univention/templates/files/etc/lmz-base.config
#
paedml_host=dc01.musterschule.schule.paedml
external_fqdn=mycloud.meine-schule.de
```

Abb. 122: Korrektur von `external_fqdn`

Beenden Sie **mcedit** mit **F10**-Taste.

Führen Sie nun den nachfolgenden Befehl aus:

```
lmz-initial-setup -t
```

DNS auf DC01 anpassen

Melden Sie sich auf dem Server DC01 als Domänen-Admin an.

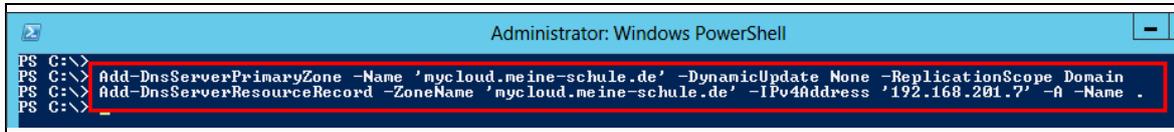
Öffnen Sie PowerShell und führen die folgenden zwei Befehle nacheinander aus. Den Platzhalter {meine Domäne} ersetzen Sie dabei durch Ihre eigene Domäne.



Der Punkt am Ende der zweiten Befehlszeile – nach dem Parameter `-Name` – ist kein Tippfehler!

```
Add-DnsServerPrimaryZone -Name '{meine Domäne}' -DynamicUpdate None -ReplicationScope Domain
```

```
Add-DnsServerResourceRecord -ZoneName '{meine Domäne}' -IPv4Address '192.168.201.7' -A -Name .
```



```
Administrator: Windows PowerShell
PS C:\> Add-DnsServerPrimaryZone -Name 'mycloud.meine-schule.de' -DynamicUpdate None -ReplicationScope Domain
PS C:\> Add-DnsServerResourceRecord -ZoneName 'mycloud.meine-schule.de' -IPv4Address '192.168.201.7' -A -Name .
PS C:\>
```

Abb. 123: DNS-Zone und -ResourceRecord hinzufügen

Kontrollieren Sie das Ergebnis mit `nslookup {meine Domäne}`:



```
PS C:\> nslookup.exe mycloud.meine-schule.de
Server: dc01.musterschule.schule.paedml
Address: 10.1.1.1

Name: mycloud.meine-schule.de
Address: 192.168.201.7
```

Abb. 124: Kontrolle mit nslookup

B.5 Nextcloud-Provisioning

B.5.1 Warum muss ein PING-Check gegen die IP-Adresse meiner Firewall gemacht werden?

Der Univention Corporate Server (UCS) der Nextcloud-VM prüft die Verfügbarkeit der Internetverbindung u.a. durch einen PING-Check an die IP-Adresse des Gateways. Ist Ihre Firewall aus Sicherheitsgründen so konfiguriert, dass sie nicht Ping-sichtbar ist, dann liefert das Diagnose-Modul des UCS eine kritische Warnmeldung. Auf der Univention Management Console (UMC) sehen Sie in diesem Fall folgende Diagnose:



Kritisch: Gateway ist nicht erreichbar

Das gateway '192.168.201.254' konnte nicht erreicht werden. Bitte durch Benutzung des [Modul "Netzwerk-Einstellungen"](#) sicherstellen, dass Gateway- und zusammengehörige Netzwerkeinstellungen korrekt konfiguriert sind.
Wenn diese Einstellungen richtig sind liegt das Problem im Gateway selbst:
Stellen Sie sicher, dass die Hardware des Gateway-Geräts korrekt funktioniert.

PING 192.168.201.254 (192.168.201.254) 56(84) bytes of data.

-- 192.168.201.254 ping statistics --
4 packets transmitted, 0 received, 100% packet loss, time 3058ms

ERNEUT TESTEN

Abb. 125: Zertifikate (Lokaler Computer) -> Eigene Zertifikate -> Vertrauenswürdige Stammzertifizierungsstelle

Aus diesem Grund führt das Initialisierungsskript `Imz-initial-setup` einen PING-Check aus und bricht ab, wenn es keine Antwort auf seine Ping-Anfrage erhält.

B.5.2 Was kann ich tun, damit meine OctoGate-Firewall eine Ping-Anfrage aus der Nextcloud-VM akzeptiert?

Die notwendige Anpassung muss auf der Kommandozeile der OctoGate erfolgen. Nehmen Sie wie im [B.1 Welche Angaben muss ich zwingend nennen, damit meine Supportanfrage an support@octogate.de zügig bearbeitet werden kann?](#) beschriebenen Kontakt zu OctoGate-Support auf.

B.5.3 Wie kann ich externe Domäne korrigieren und Let's Encrypt Zertifikat installieren?

Sie müssen sich entweder per SSH oder direkt auf der Serverkonsole der Nextcloud-VM als Benutzer `root` anmelden.

Öffnen Sie die Datei `/etc/lmz-base.config` mit dem Editor `mcedit`.

```
mcedit /etc/lmz-base.config
```

```
root@nextcloud:~# mcedit_/etc/lmz-base.config
```

Abb. 126: `/etc/lmz-base.config` in einem Editor öffnen.



Die Wahl des Editors ist selbstverständlich Ihnen überlassen. Wir haben uns für dieses Beispiel deswegen für `mcedit` entschieden, da seine Oberfläche und Bedienung den meisten Windows-Benutzern eher vertraut erscheinen dürfte.

Auf UCS finden Sie u.a. die Editoren `nano`, `pico`, `vi(m)` und sogar `emacs`.

Korrigieren Sie Ihre externe Domäne und speichern Sie die Datei mit der `F2`-Taste.

```
/etc/lmz-base.config [-M--] 14 L:[ 1+13 14/ 15] *(485 / 509b) 0109 0x06D
# Warning: This file is auto-generated and might be overwritten by
# univention-config-registry.
# Please edit the following file(s) instead:
# Warnung: Diese Datei wurde automatisch generiert und kann durch
# univention-config-registry ueberschrieben werden.
# Bitte bearbeiten Sie an Stelle dessen die folgende(n) Datei(en):
# <---->/etc/univention/templates/files/etc/lmz-base.config
#
paedml_host=dc01.musterschule.schule.paedml
external_fqdn=mycloud.meine-schule.de
```

Abb. 127: Korrektur von `external_fqdn`

Beenden Sie `mcedit` mit `F10`-Taste.

Führen Sie anschließend den nachfolgenden Befehl auf der Konsole aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:system:get trusted_domains
```

Prüfen Sie die Ausgabe nach einem Tippfehler o.ä. bzgl. Ihrer externen Domäne.

```
root@nextcloud:~# univention-app shell nextcloud sudo -u www-data /var/www/html/occ config:system:ge
t trusted_domains
nextcloud.paedml.lokal
192.168.201.7
*.ozone.octogate.de
https://nextcloud.m...nextcloud
```

Abb. 128: Fehlerhafter Wert in trusted_domains gefunden

Falls Sie einen fehlerhaften Wert wie in der obigen Abbildung dargestellt gefunden haben, korrigieren Sie ihn mit:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ con-
fig:system:delete trusted_domains 3
```

Mit dem Befehl löschen Sie zunächst den fehlerhaften Eintrag. Die Ziffer 3 aus dem Beispiel bedeutet, dass Sie die vierte Zeile aus der Konsolenausgabe – die Zählung beginnt nämlich bei 0 – löschen möchten.

Anschließend müssen Sie noch mit dem nachfolgenden Befehl den korrekten Wert für die gelöschte Zeile eintragen (den Platzhalter mycloud.meine-schule.de müssen Sie durch Ihre eigene Domäne ersetzen):

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ con-
fig:system:set trusted_domains 3 -value="mycloud.meine-schule.de"
```

Kontrollieren Sie das Ergebnis mit dem Befehl:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ con-
fig:system:get trusted_domains
```

Wenn die Korrektur erfolgreich war, dann aktualisieren Sie das Let's Encrypt Zertifikat mit:

```
lmz-initial-setup -t
```

B.5.4 Gibt es einen *Shortcut* für den OCC-Befehl?

Nein. Sie können aber einen Alias definieren. Führen Sie dazu den folgenden Befehl auf der Serverkonsole aus:

```
echo "alias nccmd='univention-app shell Nextcloud sudo -u www-data
/var/www/html/occ'" >> ~/.bashrc
```

Wenn Sie sich ab- und wieder anmelden, können Sie den OCC-Befehl fortan mit dem Alias `nccmd` ausführen.

Um den Alias sofort, d.h. ohne Neuanmeldung, zu aktivieren führen Sie den nachfolgenden Befehl aus:

```
source ~/.bashrc
```

B.6 Nextcloud

B.6.1 Anmeldung in Nextcloud wird verzögert bzw. ist oft nicht möglich.

Nextcloud hat eine Sicherheitsfunktion, die eine Anmeldung bis zu 30 Sekunden absichtlich verzögert. Das passiert in der Regel dann, wenn ein Benutzer mehrere fehlgeschlagene Anmeldeversuche unternommen hat. Dann erhält der Benutzer auf der Anmeldeseite der Nextcloud zum Beispiel folgenden Hinweis:

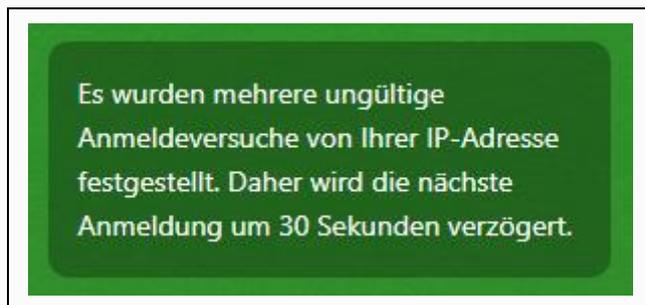


Abb. 129: Nextcloud Brute-force Protection

Um dem betroffenen Benutzer helfen zu können, müssen Sie die IP-Adresse seines Gerätes freigeben.

Melden Sie sich als Benutzer `root` an der Nextcloud-VM an.

Sofern der betroffene Benutzer oder Sie die IP-Adresse des Gerätes kennen, führen Sie folgenden Befehl aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ security:brute-force:reset "{IP-Adresse}"
```

Der Platzhalter `{IP-Adresse}` steht für die tatsächliche IP-Adresse des Gerätes.

Wenn die *Blockade* im Schulnetz stattfindet, dann ist es relativ einfach, die IP-Adresse des betroffenen Gerätes zu finden, z.B. mit dem Commando `ipconfig`. Fanden die fehlerhaften Anmeldeversuche jedoch außerhalb des Schulnetzes – z.B. von Zuhause aus – statt, dann müssen Sie sehr wahrscheinlich die öffentliche IP-Adresse des Internet-Routers von Ihrem Benutzer in Erfahrung bringen und diese freigeben. Sollte Ihr Benutzer nicht in der Lage sein, Ihnen diese IP-Adresse mitzuteilen, können Sie die Information aus der Log-Datei der Nextcloud versuchen, zu ermitteln.



Für die Untersuchung der Log-Datei ist ein Editor sehr hilfreich, der Dateien mit Zeilenende-Sequenz LF – grob übersetzt Dateien aus Linux/Unix – darstellen kann. NotePad++ oder Visual Studio Code wären eine gute Wahl.

Beispiel: Benutzer Max Mustermann (Benutzername `max.mustermann`) hat von Zuhause aus mehrmals vergeblich versucht, sich in der Nextcloud der Schule anzumelden. Nun erhält er den oben gezeigten Hinweis und kann sich nicht anmelden. Er bittet Sie um Hilfe.

Melden Sie sich in der Nextcloud als Benutzer `nc_admin` an. Öffnen Sie Benutzerverwaltung über das `Admin`-Icon.

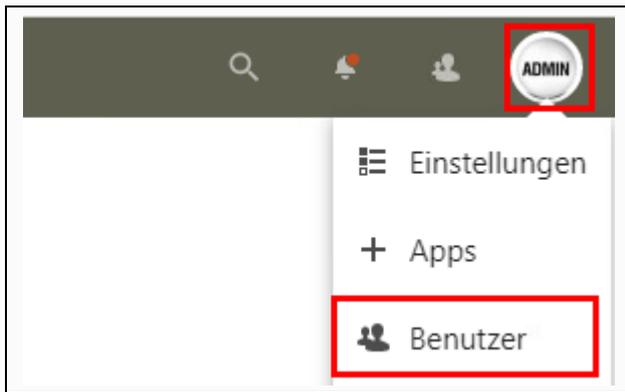


Abb. 130: Benutzer nc_admin > Benutzer

Klicken Sie auf das Suchsymbol (1) und tippen Sie den Benutzernamen ein.

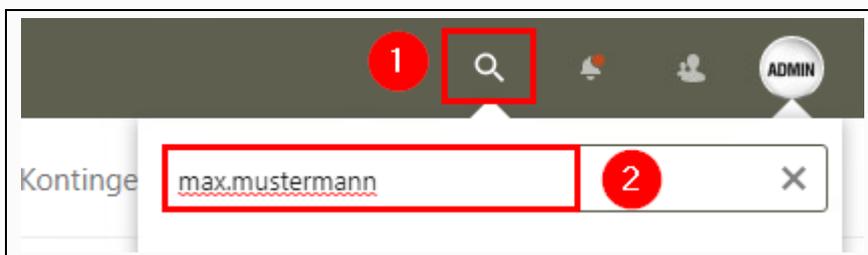


Abb. 131: Nach Benutzernamen suchen

Kopieren Sie die 36-stellige ID des Benutzers. Falls es mehrere Benutzer mit demselben Vor- und Nachnamen gibt, hilft Ihnen die Gruppenzugehörigkeit, den gesuchten Benutzer zu identifizieren.

Benutzername Anzeigenname	Passwort	E-Mail	Gruppen
 5D7B8E84-99B2-4D84-AC59-964E55D7047E Max Mustermann			G_Lehrer, G_Lehrer_SPE

Abb. 132: Zusammenfassung der von Firewall-Profil behandelten Regeln

Öffnen Sie nun die Seite Einstellungen über das Admin-Icon.

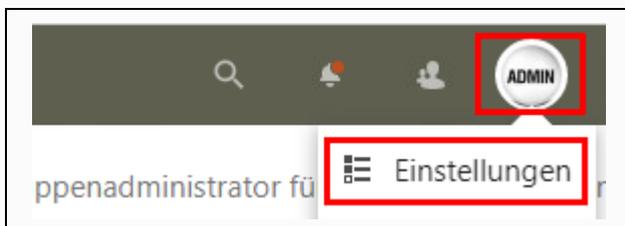


Abb. 133: Benutzer nc_admin > Einstellungen

Klicken Sie auf **Protokollierung**.



Abb. 134: Verwaltung -> Protokollierung

Klicken Sie auf das Menü-Icon **...**.



Abb. 135: Verwaltung -> Protokollierung

Laden Sie die Log-Datei über **Download logs** herunter.

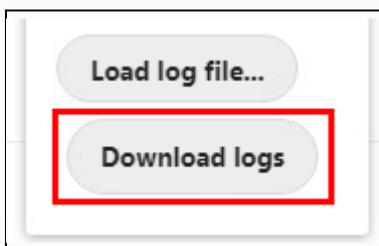


Abb. 136: Verwaltung -> Protokollierung -> Download logs

Öffnen Sie die heruntergeladene Log-Datei `nextcloud.log` in einem Editor, z.B. NotePad++.

Suchen Sie darin nach der oben kopierten Benutzer-ID. Sie sehen dann die gesuchte IP-Adresse des Benutzers.

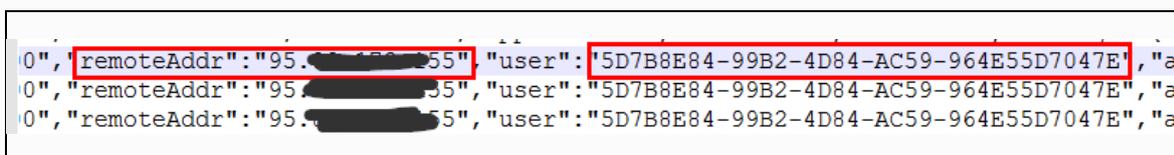


Abb. 137: Zusammenfassung der von Firewall-Profil behandelten Regeln

Melden Sie sich als Benutzer `root` an der Nextcloud-VM an, entweder über die (Remote-)Console oder über SSH und führen Sie folgenden Befehl aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ security:bruteforce:reset "{IP-Adresse}"
```

B.6.2 Quota-Einschränkung für Benutzer `nc_admin` aufheben

Die Quota-Einschränkung aus dem [Kapitel Fehler! Verweisquelle konnte nicht gefunden werden. Fehler! Verweisquelle konnte nicht gefunden werden.](#) betrifft auch den Benutzer `nc_admin`. Wenn Sie die Quota-Einschränkung 0 Bytes für den Benutzer `nc_admin` aufheben wollen, gehen Sie wie folgt vor:

Melden Sie sich in der Nextcloud als Benutzer **nc_admin** an. Öffnen Sie Benutzerverwaltung über das **Admin**-Icon.

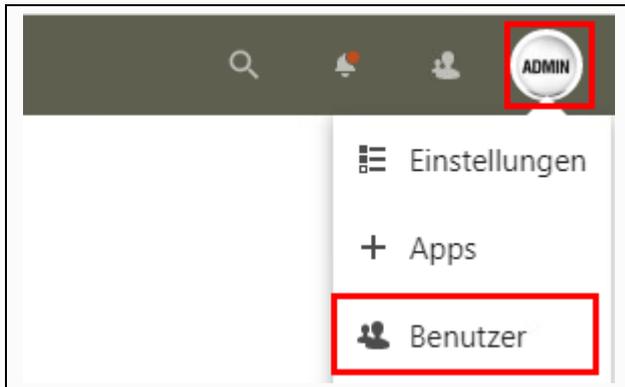


Abb. 138: Benutzer nc_admin > Benutzer

Klicken Sie auf den Link **Administratoren**.

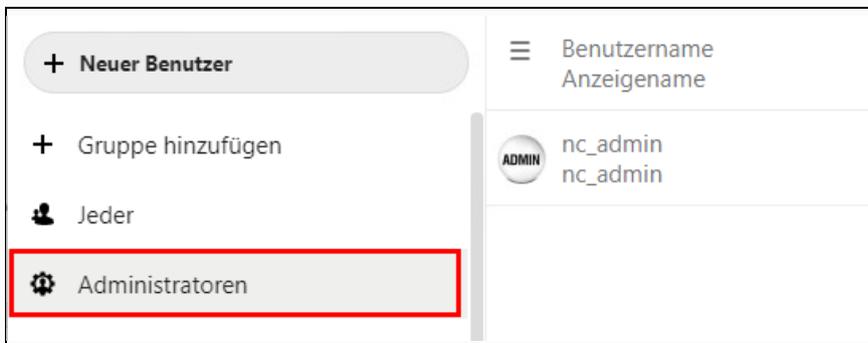


Abb. 139: Benutzerverwaltung -> Administratoren



Diese Seite enthält Spalten, die auf den ersten Blick nicht zu sehen sind, wenn Ihre Monitorauflösung geringer als 1280 Punkte in der Breite bietet. Um sie bearbeiten zu können müssen Sie die Seite nach rechts scrollen. Das geht entweder mit der Pfeil-Taste oder durch das Verschieben des horizontalen Scroll-Balkens im Browserfenster.

Klicken Sie auf das **Stift**-Icon, um Kontingent (Quota) bearbeiten zu können.

Gruppen	Gruppenadministrator für	Kontingent
admin		0 B (0 B verwendet) 

Abb. 140: Benutzerverwaltung -> Administratoren -> Bearbeiten

Sie können entweder einen der Standardwerte aus der Abbildung auswählen und übernehmen oder einen eigenen Wert festlegen, indem Sie Ihren gewünschten Wert in das Eingabefeld Kontingent eintragen. **Von der Auswahl Unbegrenzt raten wir allerdings ab.**

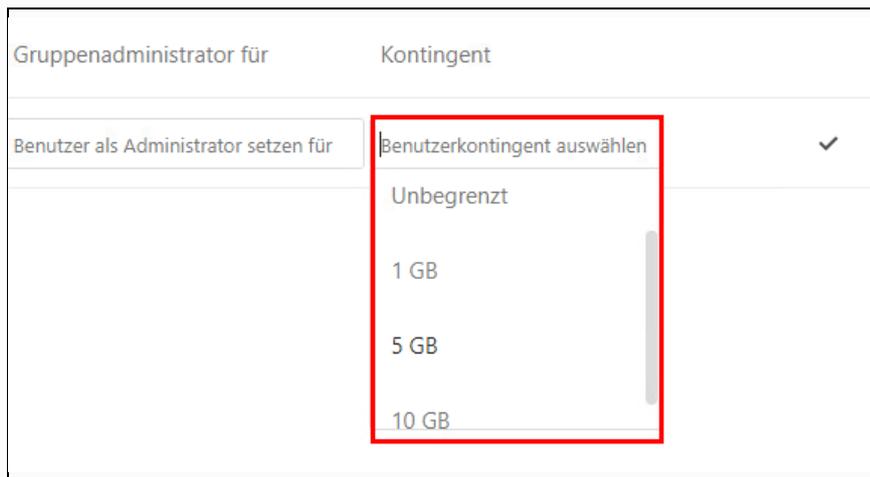


Abb. 141: Benutzerverwaltung -> Administratoren -> Kontingent festlegen

Kontrollieren Sie den Wert und speichern Sie die Änderung, indem Sie auf das -Symbol klicken.

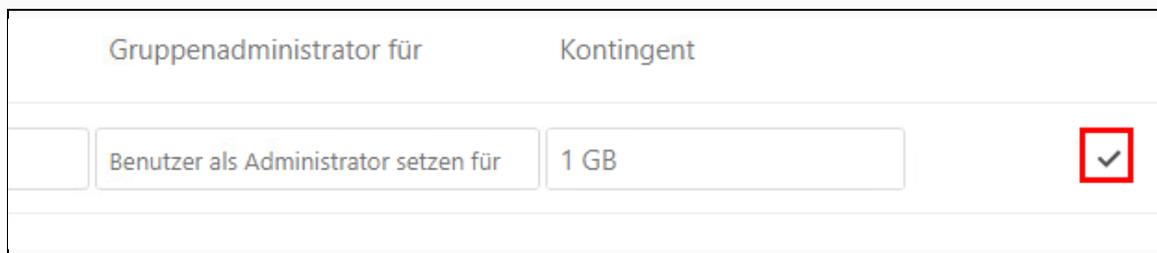


Abb. 142: Benutzerverwaltung -> Administratoren -> Bearbeiten

B.6.3 Wie kann ich prüfen, ob die Nextcloud-VM die Uhrzeit von OctoGate bezieht?

Melden Sie sich als Benutzer **root** auf der Nextcloud-VM an.

Führen Sie folgenden Befehl aus:

```
timedatectl status
```

Kontrollieren Sie die Ausgabe. Bei Erfolg sollten Sie eine ähnliche Rückmeldung erhalten wie nachfolgend dargestellt.

```
root@nextcloud:~# timedatectl status
   Local time: Do 2021-10-14 21:52:50 CET
   Universal time: Do 2021-10-14 20:52:50 UTC
     RTC time: Do 2021-10-14 20:52:51
   Time zone: Europe/Berlin (CET, +0100)
 Network time on: yes
NTP synchronized: yes
 RTC in local TZ: no
```

Abb. 143: Ping-Einstellungen des Gateways

Falls keine Synchronisation erfolgt, führen Sie folgenden Befehl aus:

```
ucr get timeserver
```

Der Rückgabewert muss 10.1.1.3 sein.

Anhang CLDAPS einrichten mit OctoGate-Zertifikat

Sie brauchen wie im [Kapitel 1.4 Systemvoraussetzungen auf Seite 8](#) beschreiben ein Serverzertifikat.

1. Melden Sie sich auf dem Server **DC01** als **Domänenadministrator** an.
2. Drücken Sie auf die **Windows**-Taste und tippen Sie `mmc.exe`, um MMC zu öffnen.



Abb. 144: mmc.exe

3. Klicken Sie auf **Datei** und wählen Sie anschließend **Snap-In hinzufügen/entfernen...** aus.

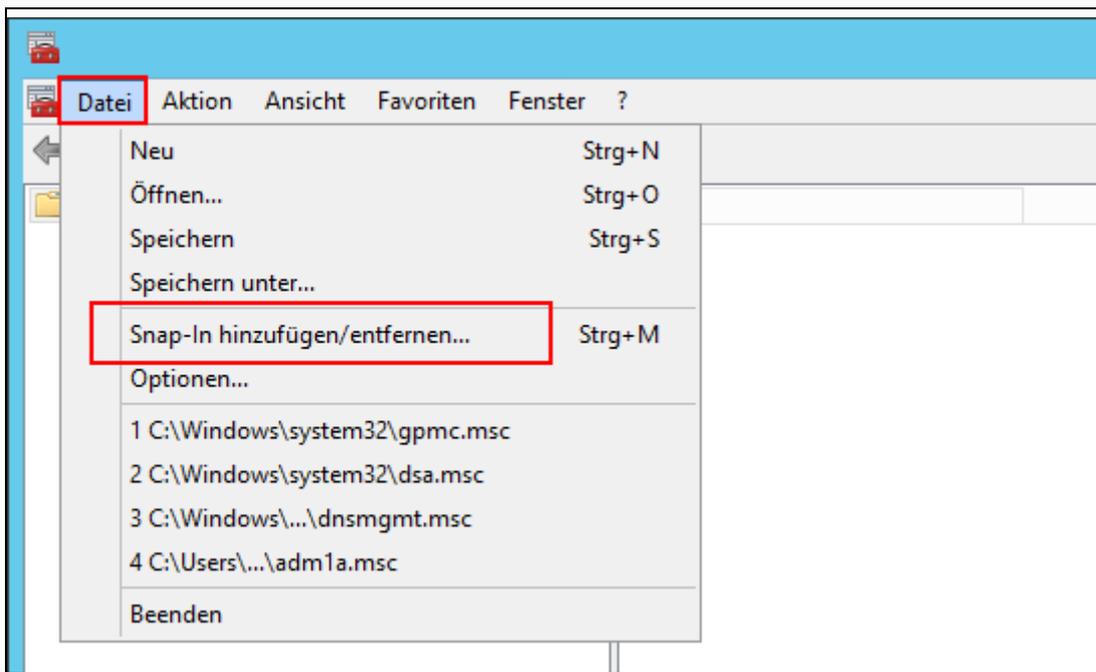


Abb. 145: MMC > Snap-In hinzufügen

4. Als Snap-In wählen Sie **Zertifikate** aus und klicken auf **Hinzufügen**.

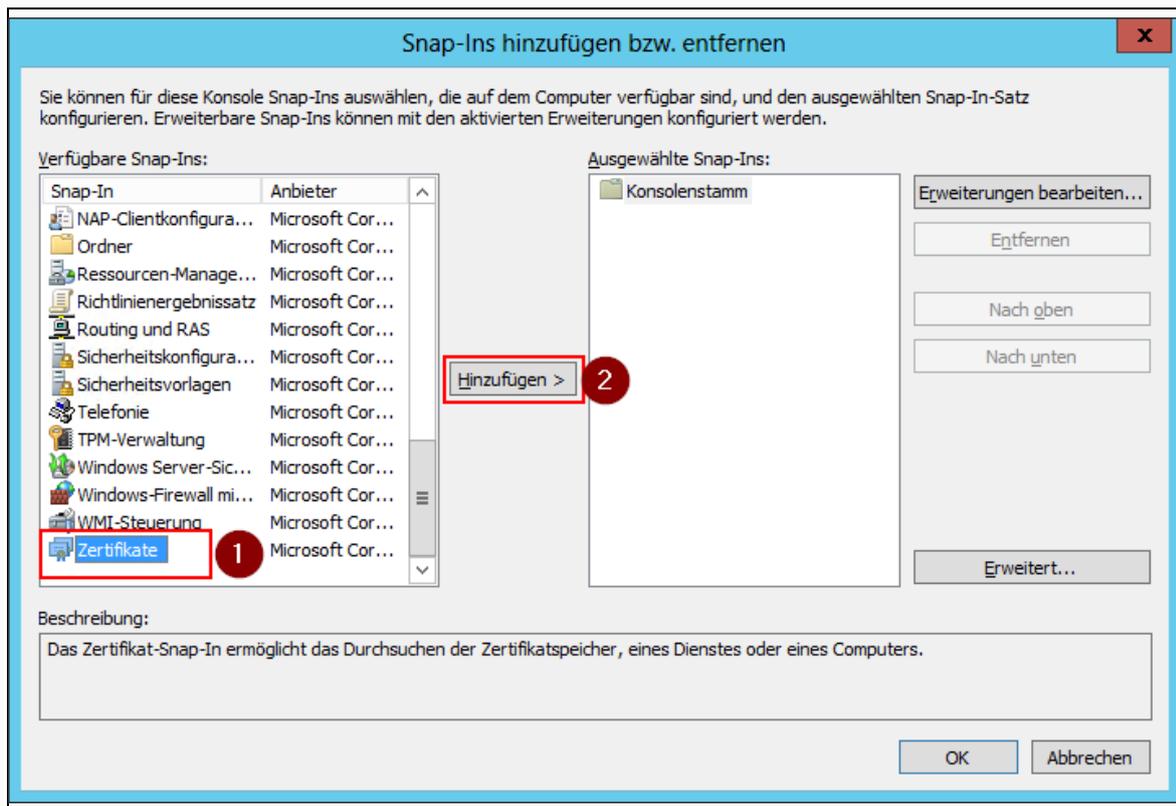


Abb. 146: MMC > Snap-In hinzufügen > Zertifikate

5. Wählen Sie als Ziel **Dienstkonto** aus und klicken Sie auf Weiter.

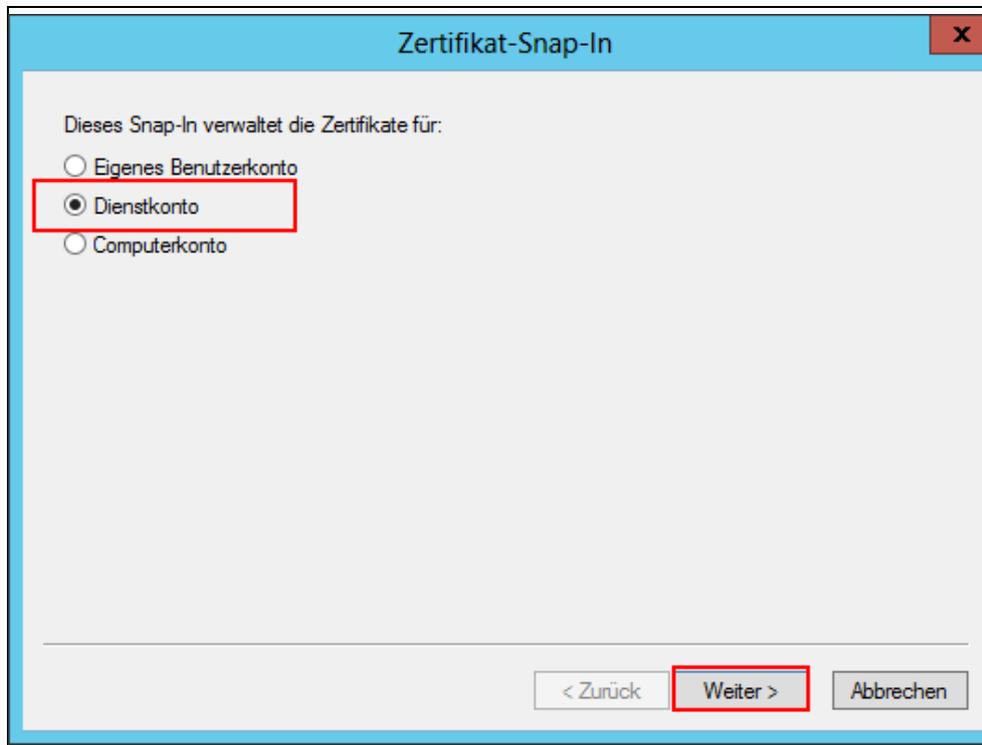


Abb. 147: MMC > Snap-In hinzufügen > Zertifikate > Auswahl Dienstkonto

6. Als Computer wählen Sie **Lokalen Computer** aus. **Weiter**.

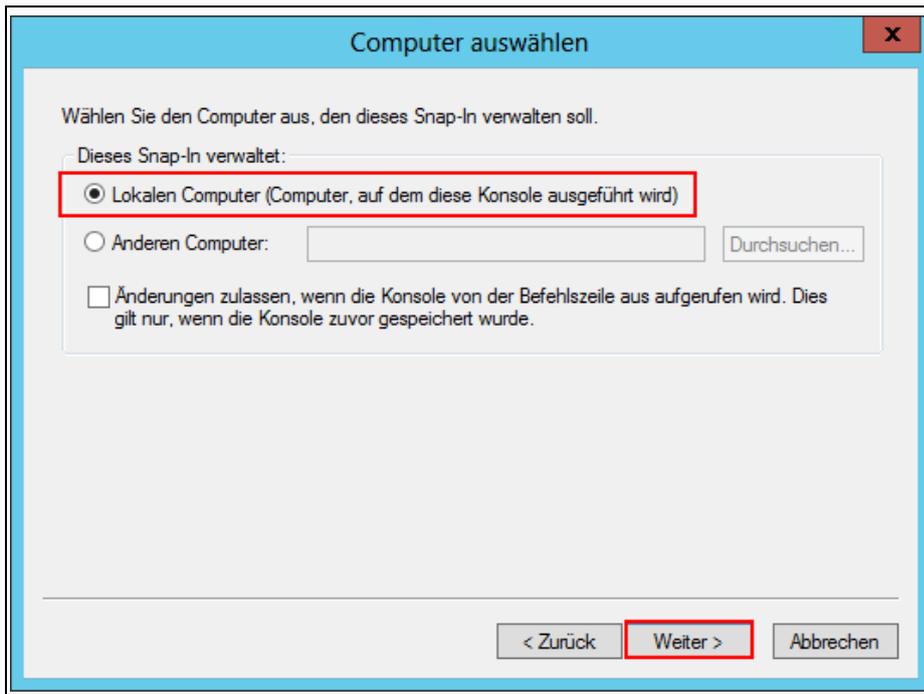


Abb. 148: MMC > Snap-In hinzufügen > Zertifikate > Auswahl Dienstkonto > Auswahl Computer

- Wählen Sie als Dienstkonto **Active Directory-Domänendienste** aus und schließen Sie den Vorgang mit **Fertig stellen** ab.

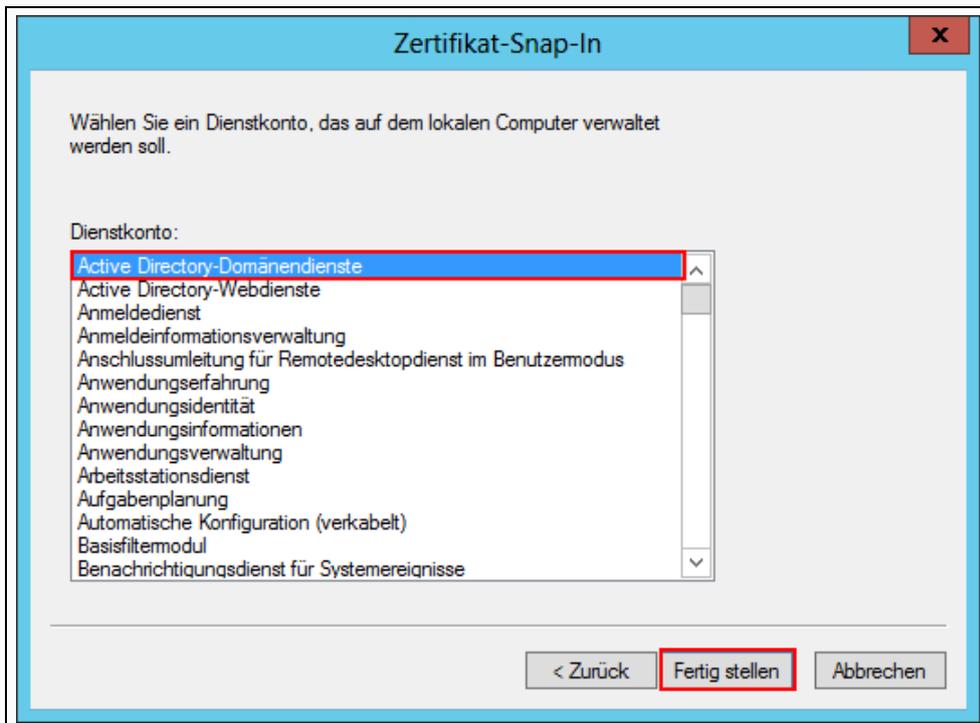


Abb. 149: MMC > Snap-In hinzufügen > Zertifikate > Auswahl Dienstkonto > Active Directory-Domänendienste

- Klicken Sie auf **OK**.

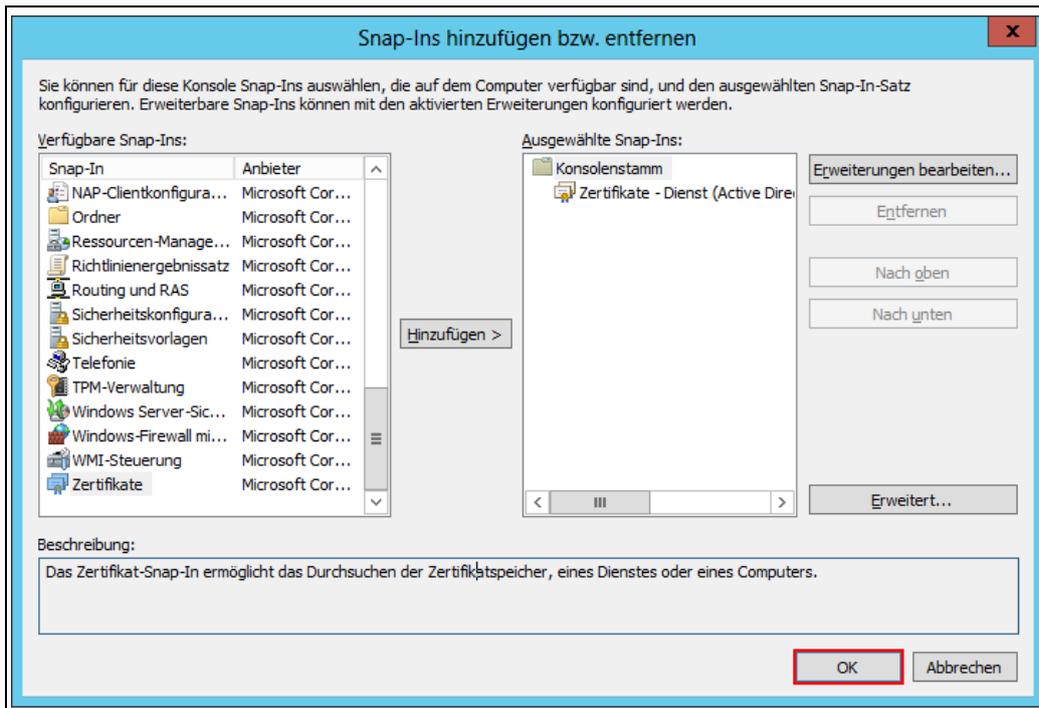


Abb. 150: MMC > Snap-In hinzufügen

9. Klicken Sie mit der rechten Maustaste auf den Ordner `NTDS\Eigene Zertifikate`. Wählen Sie aus dem Kontextmenü `Alle Aufgaben > Importieren` aus.

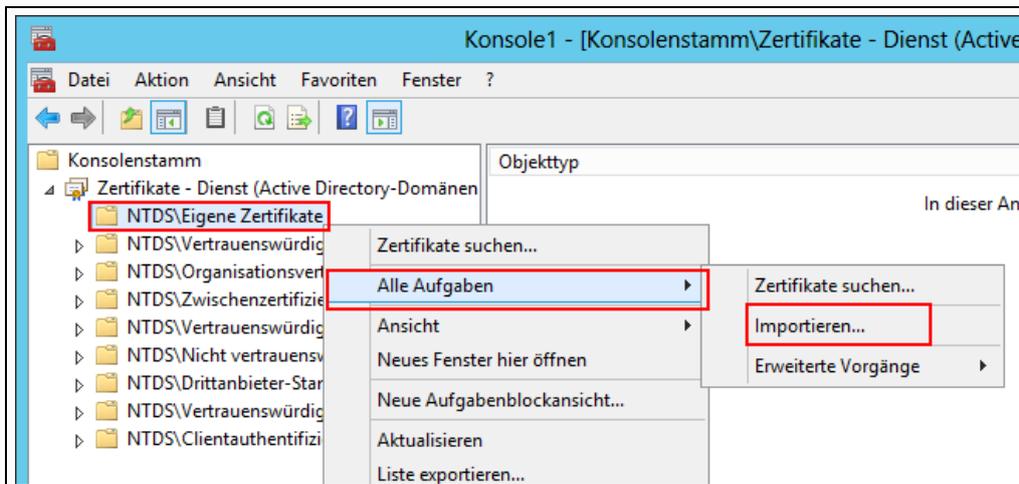


Abb. 151: MMC > Zertifikate > Zertifikat importieren

10. Weiter

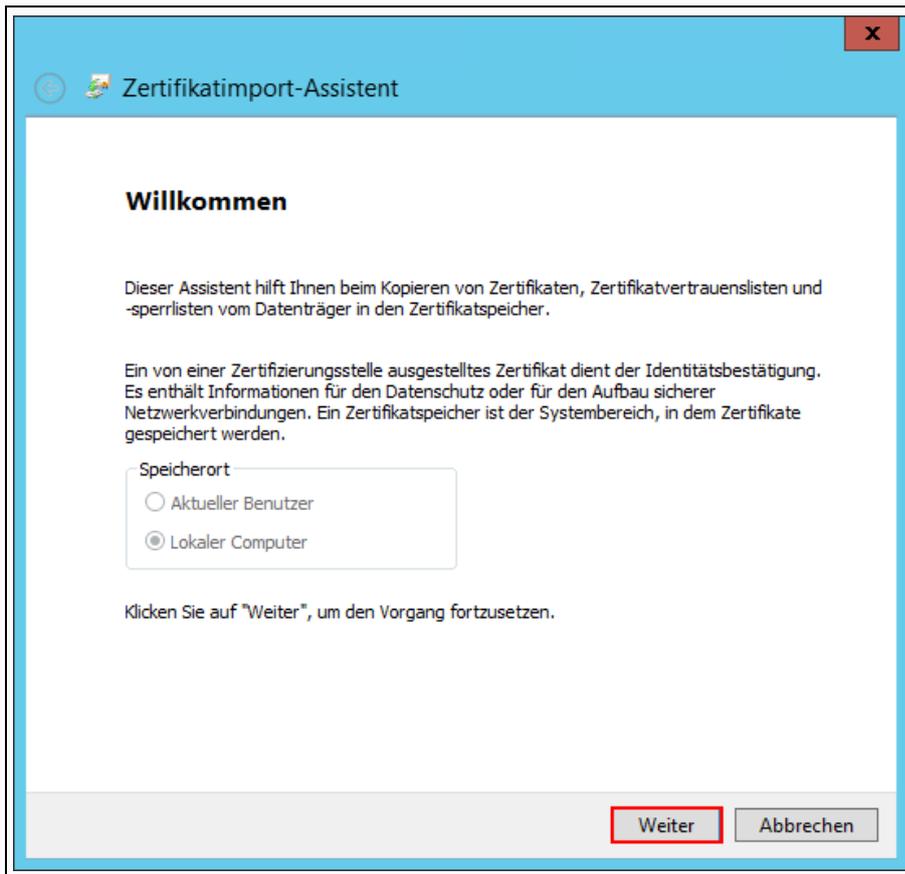


Abb. 152: Zertifikatimport-Assistent > Auswahl Lokaler Computer

11. Klicken Sie auf Durchsuchen.

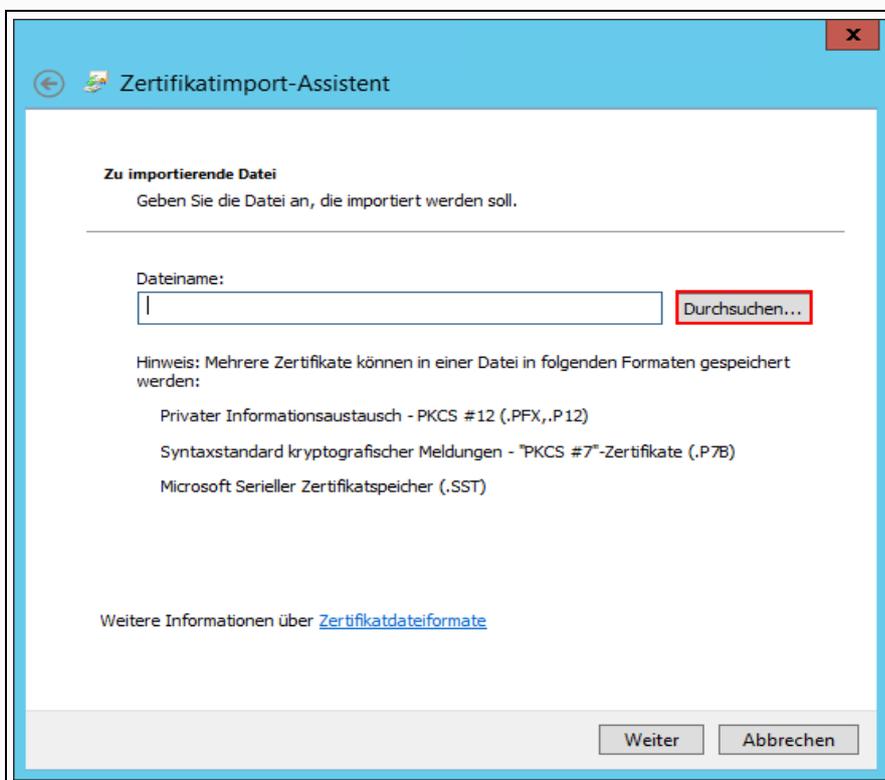


Abb. 153: Zertifikatimport-Assistent > Dateiauswahl

12. Navigieren Sie zu dem Ordner, in dem Sie die Zertifikatsdatei gespeichert haben. Stellen Sie den Dateiauswahlfilter auf **Privater Informationsaustausch** um (1) und wählen Sie die Datei **musterschule_ldaps.pfx** (2) aus.

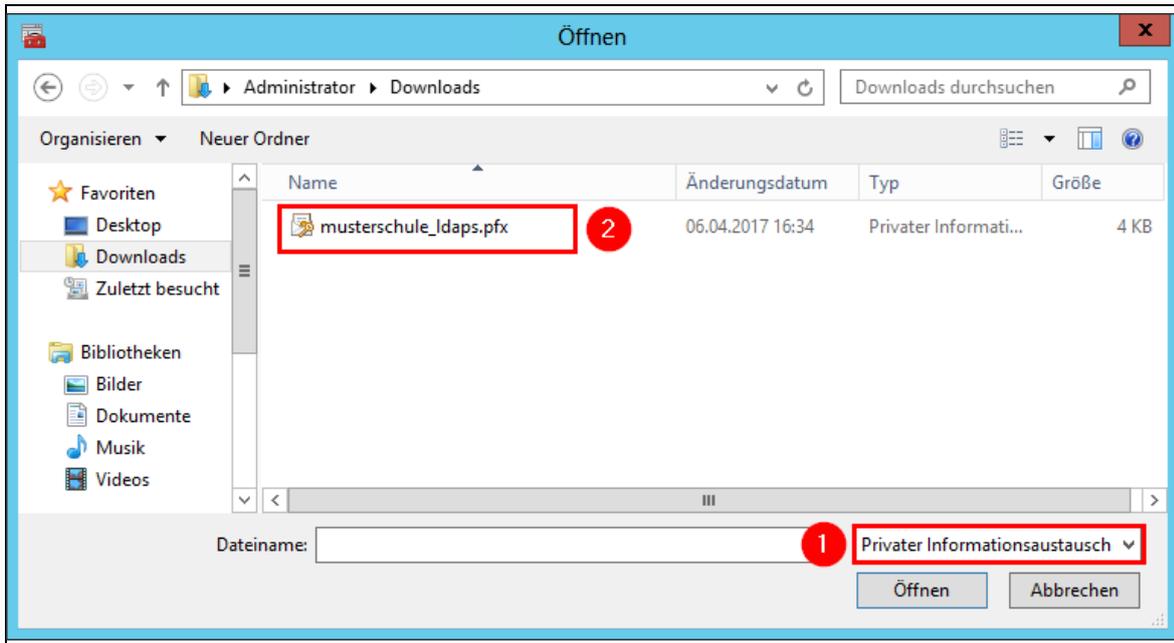


Abb. 154: Zertifikatsimport-Assistent > Auswahl der Zertifikatsdatei

13. Bestätigen Sie die Dateiauswahl mit **Weiter**.
14. Geben Sie das Kennwort für das Serverzertifikat ein und setzen Sie ein Häkchen bei **Alle erweiterten Eigenschaften mit einbeziehen**. Klicken Sie anschließend auf **Weiter**.

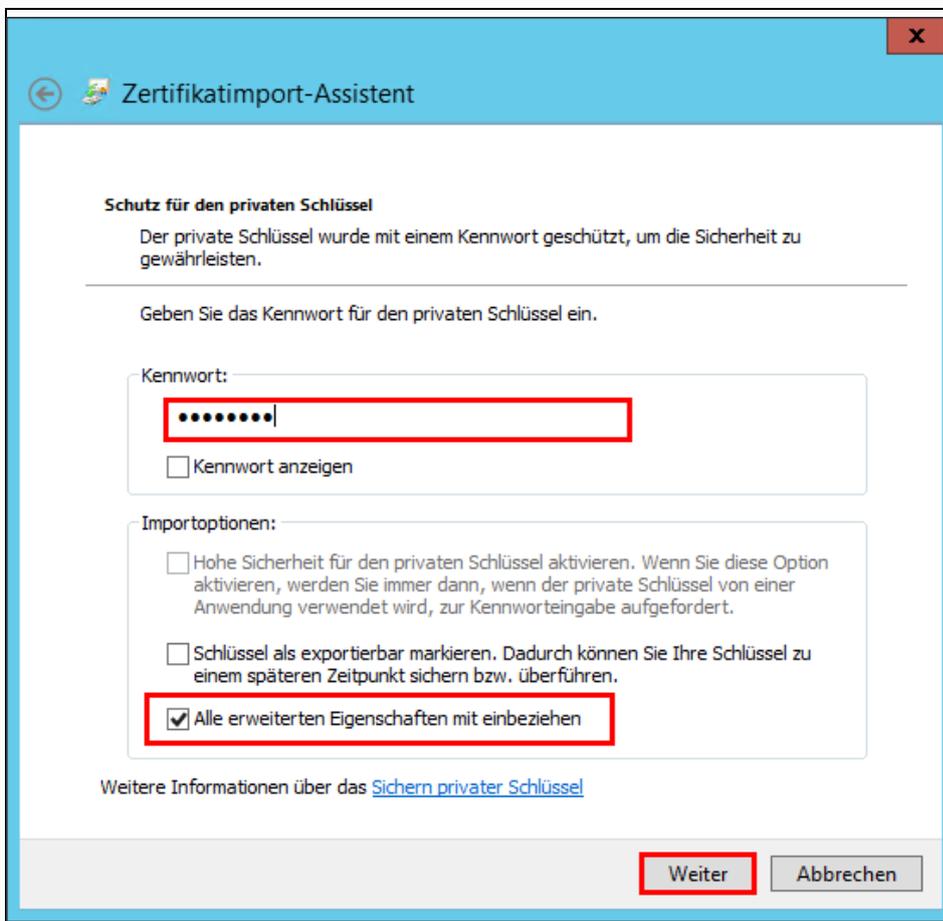


Abb. 155: Zertifikatsimport-Assistent > Importoptionen

15. Kontrollieren Sie den Zertifikatsspeicher. **Dieser muss NTDS\Eigene Zertifikate lauten.** Klicken Sie anschließend auf **Weiter**.

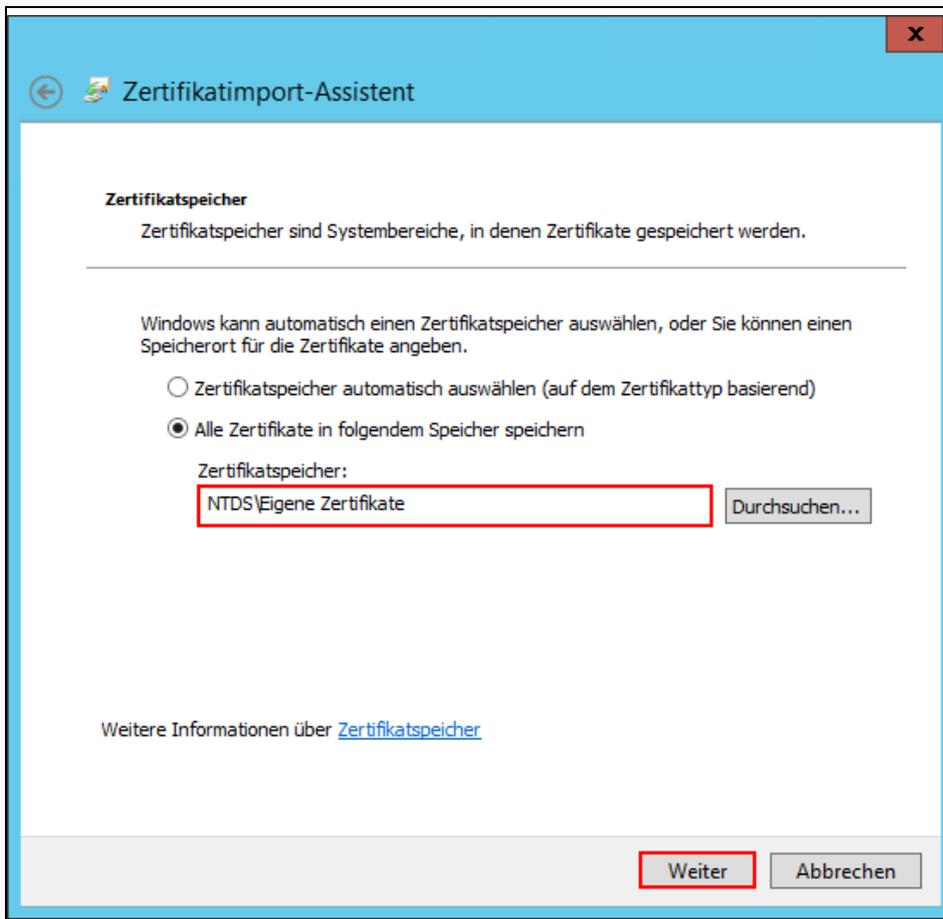


Abb. 156: Zertifikatsimport-Assistent > Zertifikatsspeicher

16. **Fertig stellen**

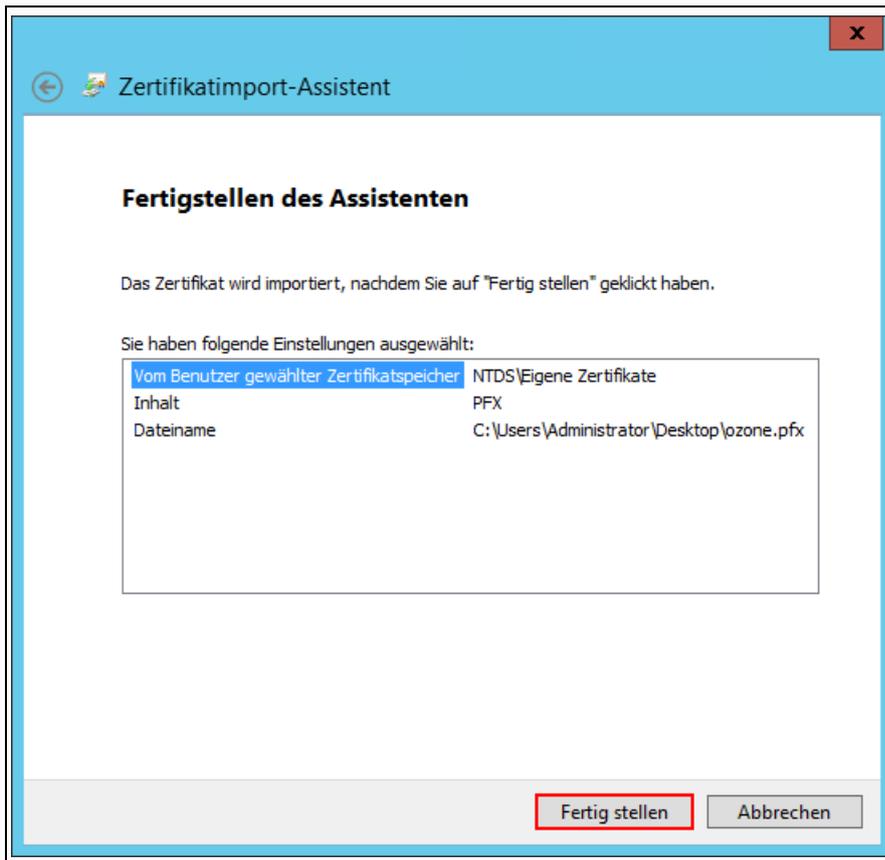


Abb. 157: Zertifikatimport-Assistent > Fertig stellen

17. Bei Erfolg erscheint folgende Rückmeldung. Falls stattdessen eine Fehlermeldung erscheint, prüfen Sie nach, ob die korrekte Zertifikatsdatei ausgewählt wurde, und wiederholen Sie den gesamten Vorgang.

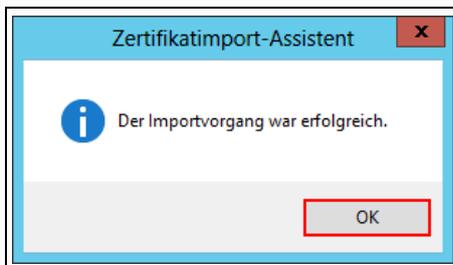


Abb. 158: MMC > Snap-In hinzufügen > Zertifikate > Auswahl Dienstkonto > Active Directory-Domänendienste

18. MMC schließen.
19. Öffnen Sie in einem Browser die **WebGUI** Ihrer **OctoGate**.
20. Melden Sie sich als Benutzer **admin** an.
21. Klicken Sie auf Downloads und laden Sie die ZIP-Datei **OctoGate CA Importer** herunter.

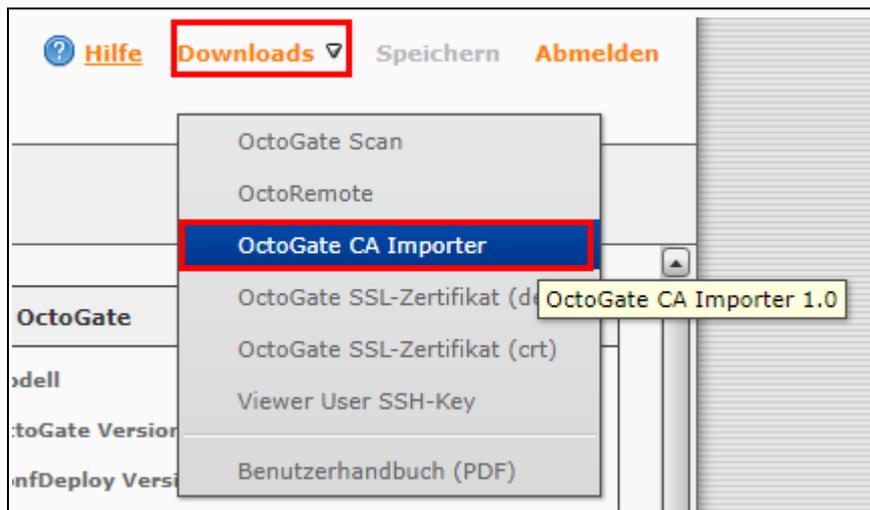


Abb. 159: OctoGate CA Importer

22. Entpacken Sie die ZIP-Datei `OctoimportCA.zip` und führen Sie die Datei `OctoimportCA.exe` aus.

Anhang DKnown-Issues

D.1 OnlyOffice kann nur im Schulnetz benutzt werden.

Der Zugriff auf Ihre Nextcloud aus dem Internet erfolgt in Kombination mit OctoGate standardmäßig über einen Reverse-Proxy. Um OnlyOffice hinter einem Reverse-Proxy nutzen können, bedarf es jedoch weiterer Konfigurationsanpassung, die in der derzeitigen Standardkonfiguration der Nextcloud fehlt. Aus diesem Grund funktioniert OnlyOffice nur im Schulnetz.

D.2 Systemdiagnose gibt eine Warnmeldung für Dateiberechtigungen aus

UMC Systemdiagnose gibt folgende Warnung aus:



Abb. 160: UMC Systemdiagnose -> Datei Berechtigung überprüfen

Lösung/Workaround: Es handelt sich hierbei um einen Fehlalarm. Ignorieren Sie diese Warnmeldung.

D.3 Benutzer können sich nicht anmelden, nachdem lmz-initial-skript ein weiteres Mal ausgeführt wurde.

Das Skript lmz-initial-setup weist in der aktuellen Version einen Fehler auf, so dass ein fehlerhafter Hostname eingetragen wird, wenn Sie das Skript ein weiteres Mal ausführen. Aus dem Grund ist dann keine Benutzeranmeldung möglich.

Um den Fehler zu beheben, gehen Sie wie folgt vor:

Melden Sie sich als Benutzer **root** in der Nextcloud-VM an und führen Sie den nachfolgenden Befehl – alles in einer Zeile – aus:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ ldap:show-config | grep ldapHost
```

Falls die Ausgabe wie in der nachfolgenden Abbildung dargestellt wird, dann ist das die Störungsursache.

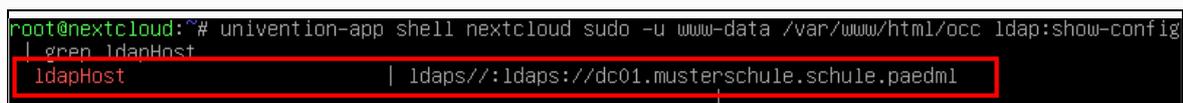


Abb. 161: Fehlerhafter Wert für ldapHost

Korrigieren Sie den Wert mit:

```
univention-app shell nextcloud sudo -u www-data /var/www/html/occ ldap:set-  
config s01 ldapHost "ldaps://dc01.musterschule.schule.paedml"
```

D.4 UCS Systemdiagnose meldet einen kritischen Fehler bzgl. SAML-Zertifikate

Die Systemdiagnose in der UMC meldet folgenden kritischen Fehler.

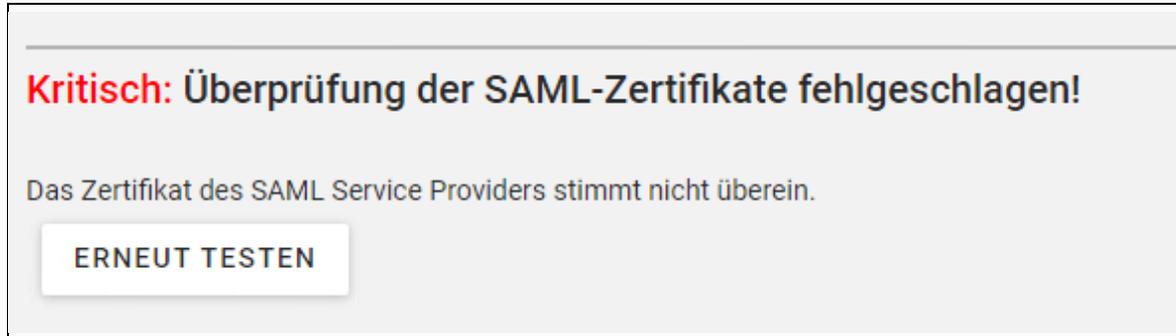


Abb. 162: UMC Systemdiagnose -> Überprüfung der SAML-Zertifikate fehlgeschlagen

Diese vermeintlich kritische Fehlermeldung können Sie ignorieren, da unsere Nextcloud-VM mit keiner UCS-Domäne verbunden ist.

9 Änderungsdocumentation

Trotz sorgfältiger Überprüfung können in der vorliegenden Update-Anleitung zur paedML® Windows 4.1 Fehler auftreten. Wir bemühen uns, Anregungen und Hinweise aus dem Kundenkreis, die einem besseren Verständnis der Anleitung dienen, fortlaufend zu berücksichtigen. Auf dieser Seite finden Sie eine kurze Zusammenfassung aller für die konkrete Arbeit relevanten Korrekturen und inhaltlichen Überarbeitungen.

Version	Geänderte oder ergänzte Kapitel
Stand 18.11.2021 Version 1.0.0	Initialversion

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111
70190 Stuttgart

© Landesmedienzentrum Baden-Württemberg, 2020

