Beratung und Support
Technische Plattform
Support-Netz-Portal

paedML® – stabil und zuverlässig vernetzen

Installationsanleitung

Installation der VM Nextcloud für paedML® Windows 5.x und Sophos

Stand 18.07.2023

paedML® Windows

Version: 5.x

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

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
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: 2023

Inhaltsverzeichnis

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 (Homeverzeichnisse der Benutzer und Tauschordner für Projekte) von außer-halb 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.

Das vorliegende Handbuch wurde für die Bereitstellung der Nextcloud-VM unter der paedML® Windows 5.0 angepasst. Sie gilt nicht für paedML® Windows 4.2 bzw. 4.3!

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. Optionales Einrichten der schuleigenen externen Domäne
4. Import der VM-Vorlage
5. Initialisierung der Nextcloud

Wir empfehlen Ihnen dringend, sich mit der Ausnahme des optionalen Einrichtens einer externen Domäne an die oben genannte Reihenfolge zu halten.

Bei Missachtung müssen Sie in der Regel den Arbeitsschritt zur Initialisierung der Nextcloud wiederholen.

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 Download der VM-Vorlage

Um Ihnen die Bereitstellung einer Nextcloud-VM zu erleichtern, stellen wir einen Download-Link bereit. Dort können Sie unsere VM-Vorlage auf der Basis eines Univention Corporate Server 5 herunterladen. Falls Sie die Datei noch nicht heruntergeladen haben, laden Sie sie hier herunter.

Für den Download müssen Sie sich zunächst mit Ihrer MLI-Nummer und dem zugehörigen Kennwort authentifizieren.

Die Download-Datei liegt im ZIP-Format vor und muss zuerst entpackt werden, bevor sie wie im Kapitel 2 Import der Nextcloud-VM beschrieben bereitgestellt wird.

1.5 Systemvoraussetzungen

Für die Inbetriebnahme der Nextcloud-VM gelten folgende Systemvoraussetzungen:

- **Ein dedizierter virtueller Switch für das Netzwerk DMZ (192.168.201.0/24)**
  Die Nextcloud-VM wird in einem eigenen Netzwerksegment betrieben.
- **paedML® Windows 5.x**
  Die Systemvoraussetzungen für die paedML® Windows 5.x finden Sie in unserer How-To-Anleitung zur Servervirtualisierung
- **Sophos SG UTM**
  Für Sophos SG UTM setzen wir voraus, dass sie gemäß unserer Installationsanleitung installiert und konfiguriert wurde. Falls Sie eine eigene Konfiguration verwenden, müssen Sie die erforderlichen Firewall-Regeln selbst hinzufügen und bearbeiten.
  Die Installationsanleitung für Sophos SG UTM und die ABF-Datei (Konfigurationsvorlage) finden Sie in unserem Download-Bereich: https://www.lmz-bw.de/netzwerkloesung/produkte-paedml/paedml-windows/downloads/#updates.
- **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 Univention-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.

Wenn Sie Sophos SG UTM als Firewall einsetzen und beabsichtigen, Ihre Nextcloud aus dem Internet erreichbar zu machen, dann brauchen Sie zusätzlich einen vollqualifizierten Domänennamen (FQDN) wie zum Beispiel intranet.meine-schule.de. Im Kapitel 4 Einrichten einer externen Domäne finden Sie weitere Details dazu.

Eine Kombination aus Nextcloud-VM, paedML® Windows 3.1.x und Sophos SG UTM wird nicht unterstützt. Das bedeutet: Wir können Ihnen keine technische Unterstützung anbieten.

Sie erhalten ebenfalls keine technische Unterstützung, wenn Sie weder OctoGate noch Sophos SG UTM als Firewall einsetzen.

1.6 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**

1.7 Lizenzierung (ab 500 Benutzer)

Bitte beachten Sie, dass Sie ab 500 Benutzern einen Lizenzcode benötigen, der in der Nextcloud eingetragen werden muss. Den Lizenzcode erhalten Sie von der paedML Windows Hotline.

1.8 LMZ-Nextcloud-Helferskripte_paedML5x-V3.zip herunterladen

Laden Sie zunächst die Datei **LMZ-Nextcloud-Helferskripte_paedML5x-V3.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_paedML5x-V3.zip` und setzen Sie ein Häkchen bei Zulassen.

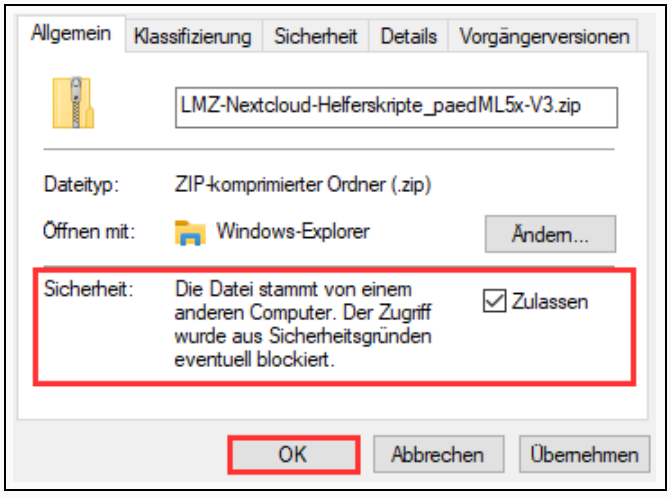


Abb. 1: LMZ-Nextcloud-Helferskripte_paedML50.zip -> Ausführung zulassen

Entpacken Sie die Datei nach `D:\Installation\paedML\Erweiterungen`.

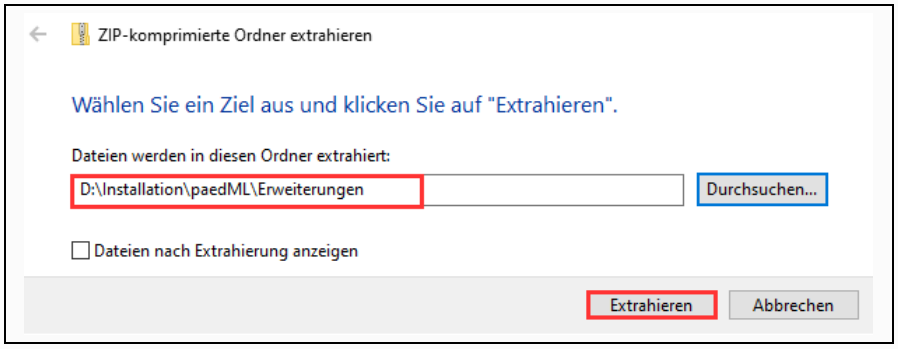


Abb. 2: LMZ-Nextcloud-Helferskripte_paedML50.zip -> Ausführung zulassen

Die so entpackten Dateien befinden sich im Ordner `D:\Installation\paedML\Erweiterungen\Nextcloud-V3` und kommen in den Kapiteln 5 LDAPS-Zertifikat und 6 Initialisierung der Nextcloud zum Einsatz.

1.9 Webbrowser

Uns ist aufgefallen, dass manche Inhalte der sog. Univention Management Console (UMC) in Microsoft Edge auf der Basis der Chromium-Engine fehlerhaft dargestellt werden können. **Aus dem Grund empfehlen wir Ihnen die Abschlussarbeiten von einem PC aus durchzuführen, auf dem alternative Webbrowser wie zum Beispiel Google Chrome oder Mozilla Firefox installiert ist.**

Beachten Sie auch, dass zur Durchführung der Wartungsarbeiten in UMC Cookies zugelassen sein müssen.

1.10 Portfreigabe

Wenn Ihre Sophos SG UTM hinter einem weiteren Router oder einem weiteren Firewall-Produkt betrieben wird, müssen Sie dafür sorgen, **dass die beiden Ports 80 und 443 auf die externe IP-Adresse Ihrer Sophos SG UTM weitergeleitet werden**.

Findet diese Weiterleitung nicht statt, können Sie weder Ihre Nextcloud aus dem Internet erreichen noch können Sie im Bedarfsfall ein kostenfreies Let's Encrypt-Zertifikat erhalten.

1.11 Tipp: How-To-Anleitung für mobile Endgeräte am Beispiel von iPads

Für die Benutzer, die die Nextcloud gerne auf einem mobilen Endgerät wie z.B. Tablet nutzen, stellen wir in unserem Download-Bereich eine How-To-Anleitung für iPads bereit.

2 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 Version 7.0 oder höher (empfohlene Version für paedML® Windows 5.0)

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

2.1 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.

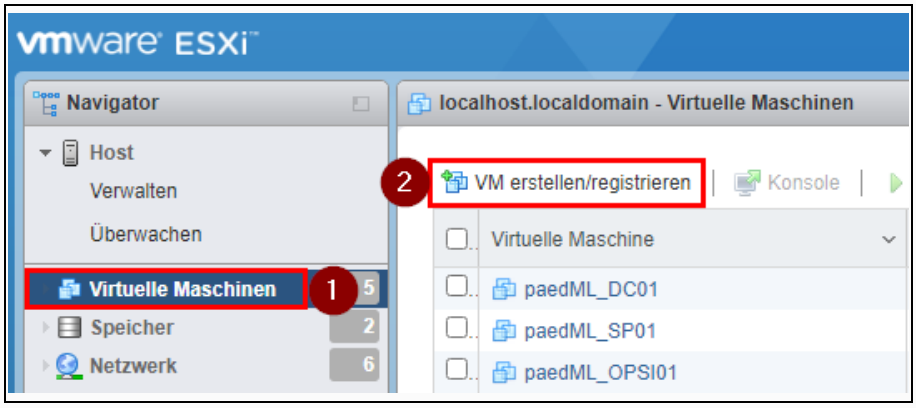


Abb. 3: Virtuelle Maschine erstellen

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

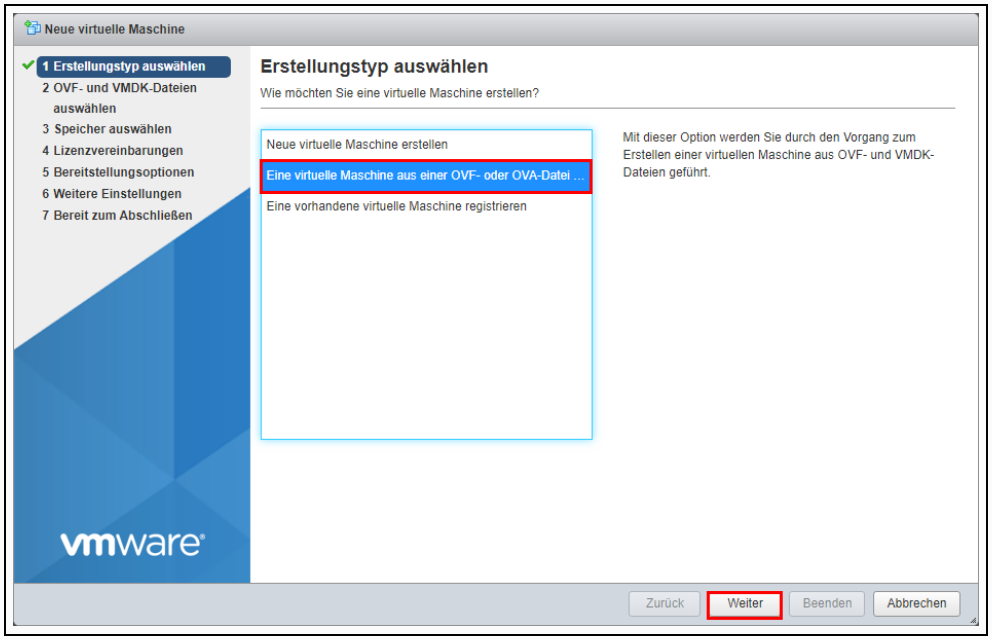


Abb. 4: VM aus einer OVF- oder OVA-Datei auswählen

4. Geben Sie Ihrer Nextcloud-VM einen Namen, z.B. `{Kürzel Ihrer Schule}_Nextcloud`.

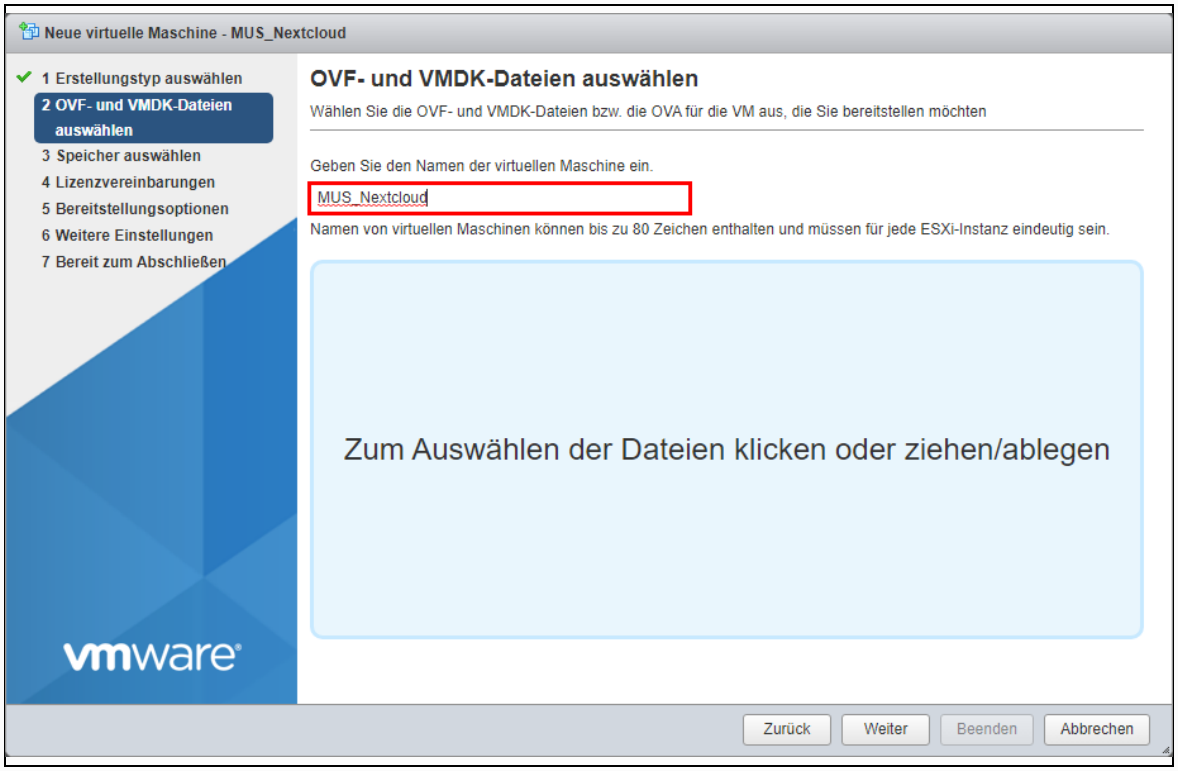


Abb. 5: VM aus einer OVF- oder OVA-Datei auswählen

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

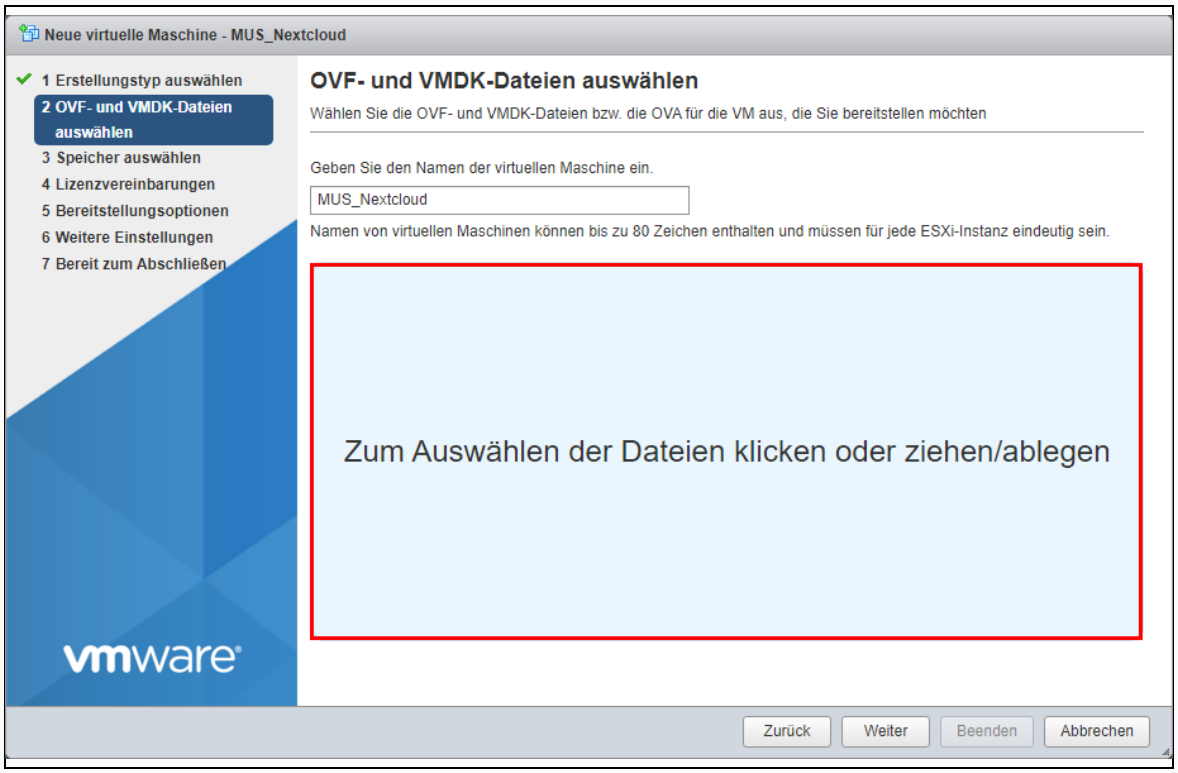


Abb. 6: VM aus einer OVF- oder OVA-Datei auswählen

6. Navigieren Sie im Datei-Explorer in den Ordner, in dem sich die VM-Vorlage befindet. **Wählen Sie die Datei Nextcloud_v3.ova aus und klicken Sie auf** Öffnen.

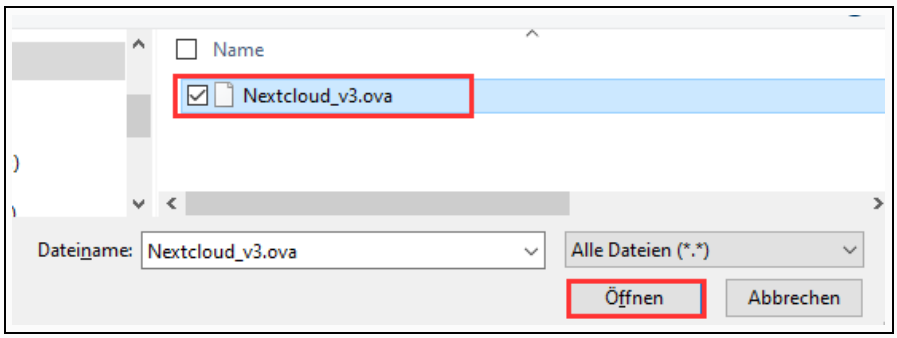


Abb. 7: Benötigte Dateien markieren und öffnen

7. Klicken Sie auf Weiter.

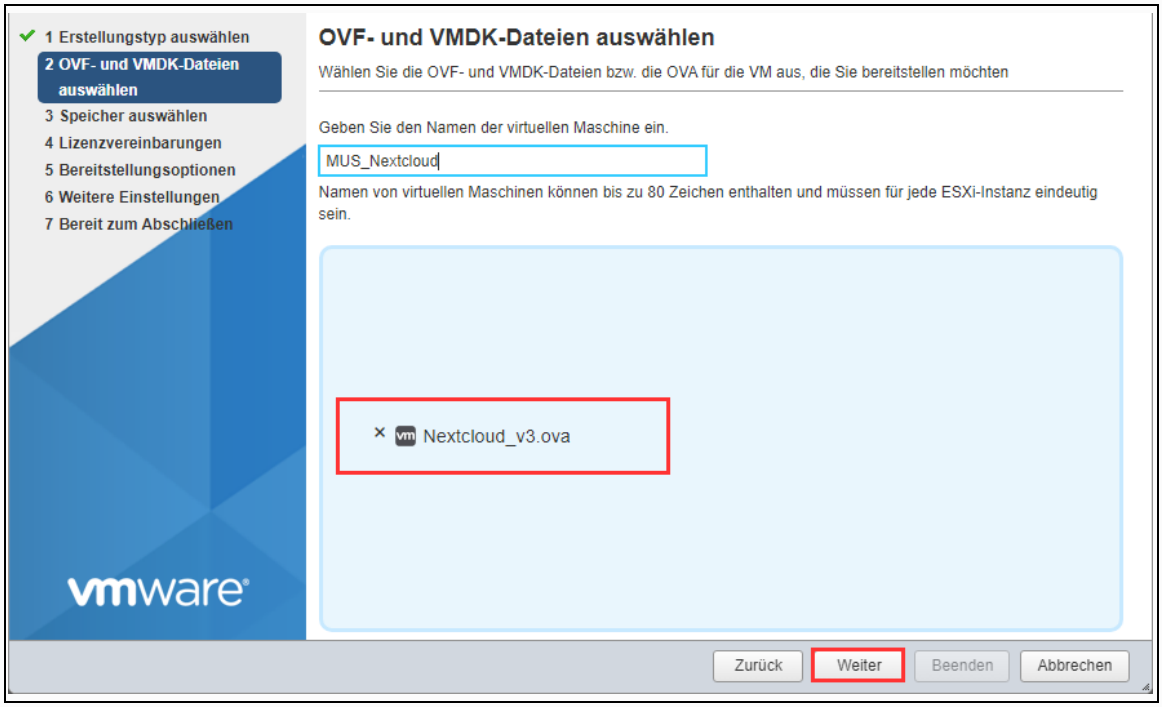


Abb. 8: OVA-Datei auswählen

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

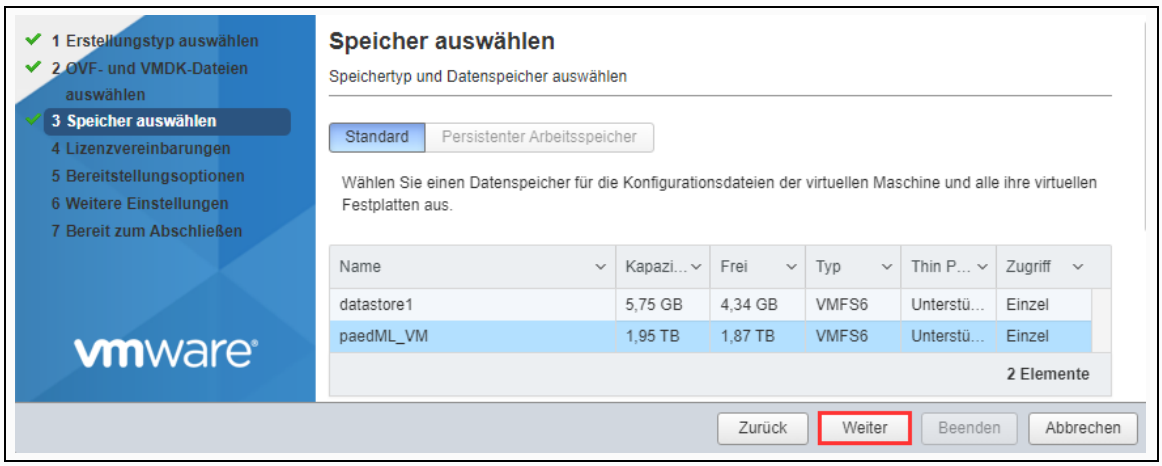


Abb. 9: Speicher auswählen

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.

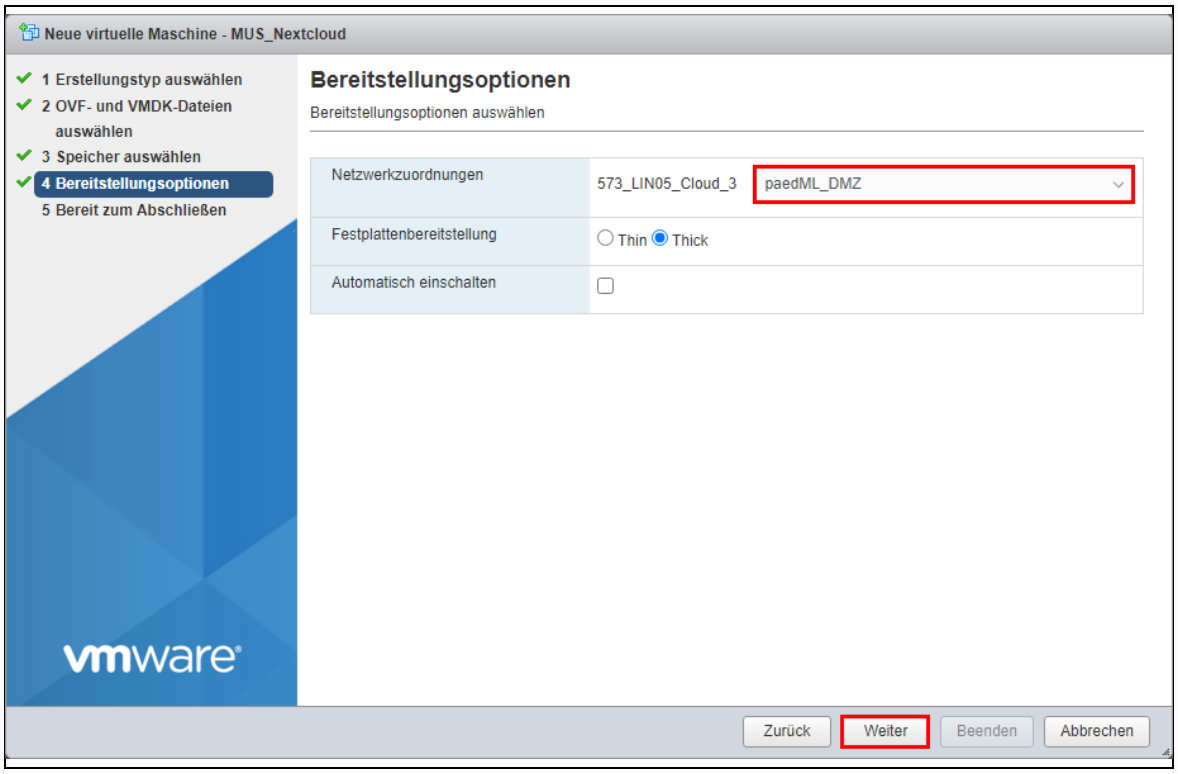


Abb. 10: Bereitstellungsoptionen festlegen

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

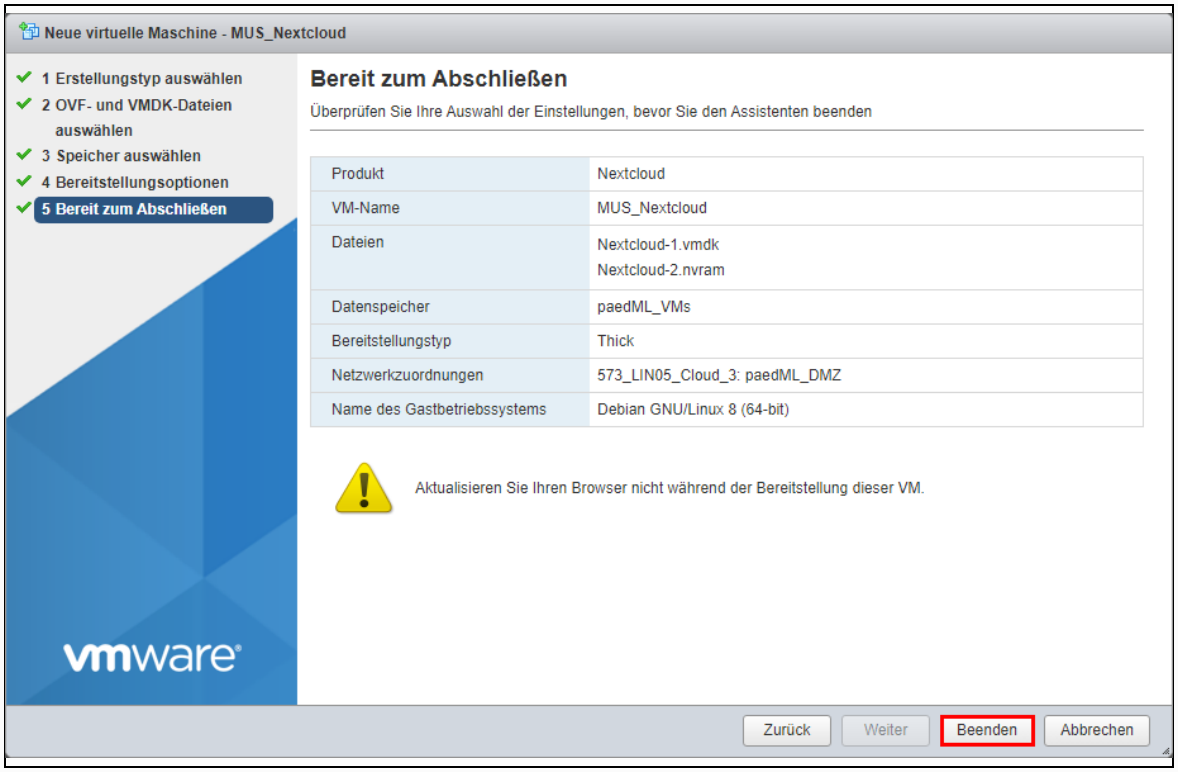


Abb. 11: Bereit zum Abschließen

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

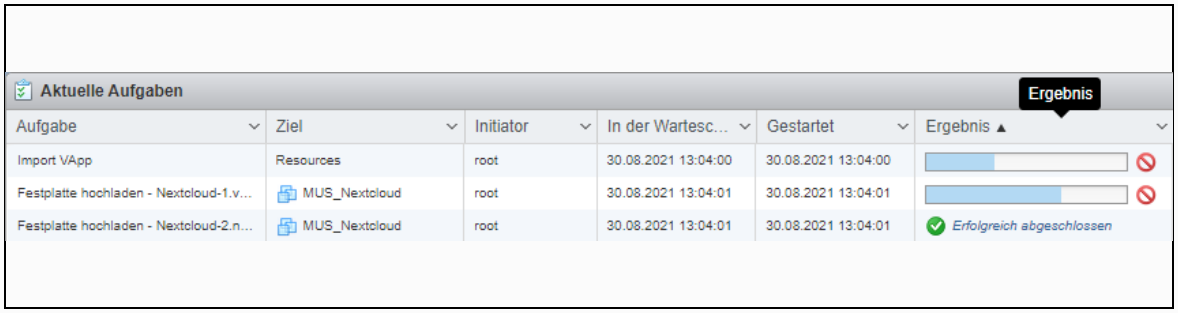


Abb. 12: Bearbeitung der aktuellen Aufgaben durch das System

2.2 [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.

2.3 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.

2.4 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.

3 Firewall anpassen

Wenn Sie Sophos SG UTM nach unserer Anleitung installiert haben, haben Sie sehr wahrscheinlich einen vSwitch mit dem Namen **paedML_DMZ** eingerichtet, jedoch im deaktivierten Zustand belassen.
In diesem Kapitel beschreiben wir, wie Sie den Netzwerkadapter für das Netz paedML_DMZ aktivieren und Anpassungen an den Firewall-Regeln vornehmen.

3.1 Netzwerkadapter bearbeiten

Wenn beim Bearbeiten Ihrer Sophos SG UTM eine technische Störung auftreten sollte, dann finden Sie im Anhang B.1 Troubleshooting: Sophos SG UTM ab Seite 58 Tipps zur Behebung einer Störung im Zusammenhang mit Sophos SG UTM.

1. Öffnen Sie als Benutzer **Administrator** oder als Benutzer **root** den Webclient Ihres ESXi-Hosts.
2. Wählen Sie die virtuelle Maschine paedML_Sophos aus. Klicken Sie auf Aktionen und anschließend auf Einstellungen bearbeiten.

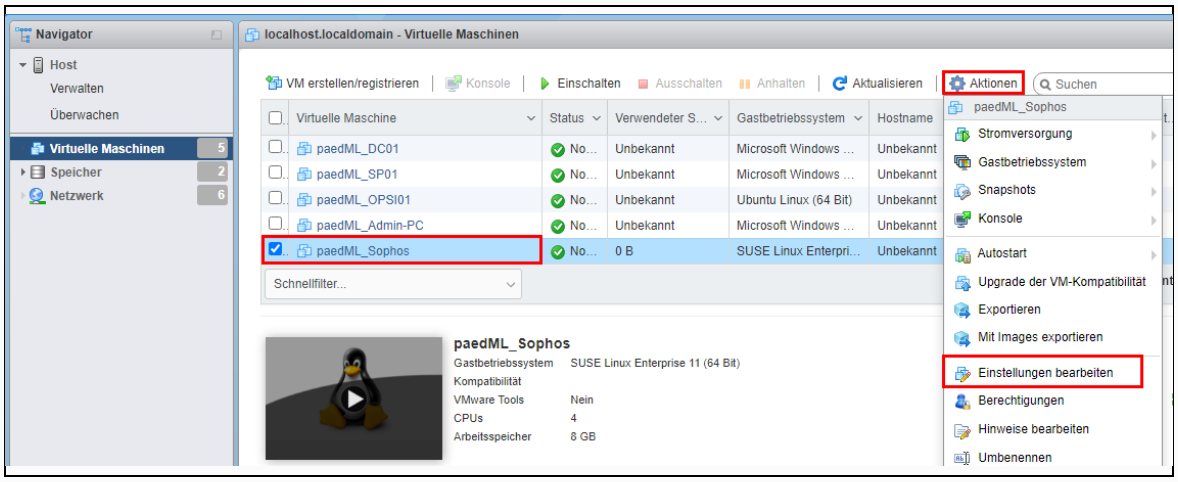


Abb. 13: vSphere Webclient -> VM-Einstellungen bearbeiten

3. Stellen Sie den Netzwerkadapter 4 auf den vSwitch paedML_DMZ um. Setzen Sie ein Häkchen bei Verbinden und schließen Sie den Vorgang mit Speichern ab.

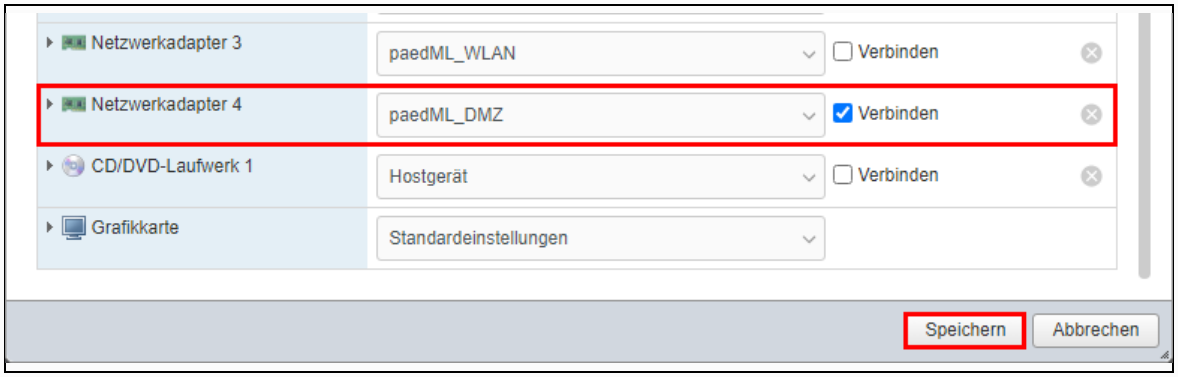


Abb. 14: Netzwerkadapter 4 anpassen und für den Boot-Vorgang aktivieren

4. Starten Sie Ihre Sophos SG UTM, falls Sie sie vor dem Bearbeiten heruntergefahren haben.

5. Öffnen Sie in einem Browser den **WebAdmin** (https://10.1.1.3:4444 bzw. https://{Hostname der UTM}:4444) Ihrer Sophos SG UTM und melden Sie sich als Benutzer **admin** an.
6. Klicken Sie auf das Menü Schnittstellen & Routing.

Abb. 15: Sophos WebAdmin -> Schnittstellen & Routing

7. Klicken Sie auf den Link Schnittstellen und anschließend auf den Button Bearbeiten bei **paedML_DMZ**.

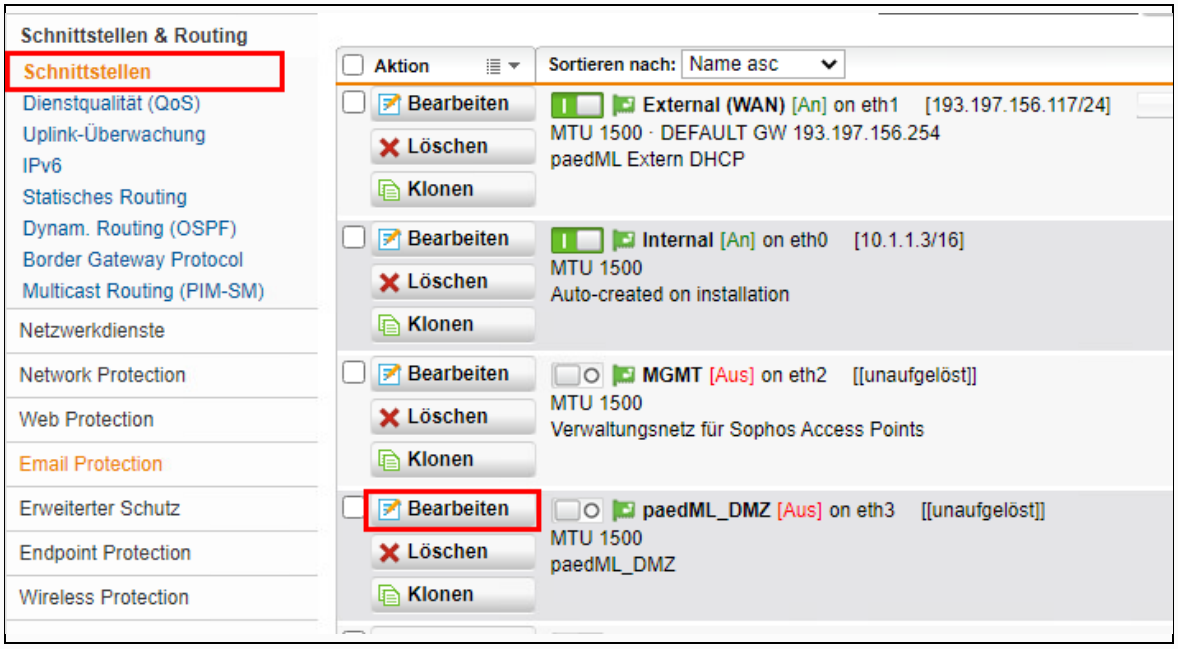


Abb. 16: WebAdmin -> Schnittstellen -> paedML_DMZ bearbeiten

8. Geben Sie als IPv4-Adresse `192.168.201.254` ein.
   Stellen Sie IPv4-Netzmaske auf /24 (255.255.255.0) um. Klicken Sie auf Speichern, um den Vorgang abzuschließen.

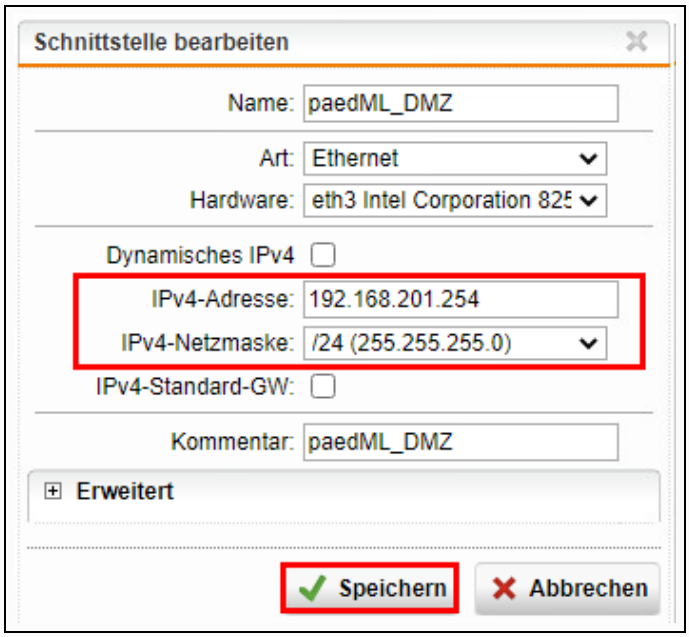


Abb. 17:IP-Konfiguration von paedML_DMZ festlegen und speichern

9. Klicken Sie auf den Schiebeschalter bei **paedML_DMZ**, um die Netzwerkschnittstelle mit der oben eingegebenen IP-Adresse zu aktivieren.

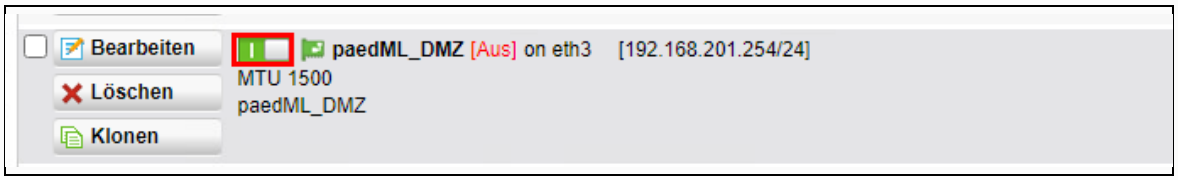


Abb. 18: WebAdmin -> paedML_DMZ aktivieren

10. Klicken Sie auf das Icon Aktualisieren, um die Änderung anzeigen zu lassen.

Verwenden Sie niemals die Aktualisierungsfunktion des Browsers! Die Aktion führt dazu, dass Sie sofort aus WebAdmin abgemeldet werden. Änderungen, die noch nicht vollständig abgeschlossen sind, können dabei verlorengehen!

Abb. 19: WebAdmin -> Konfiguration aktualisieren und neu laden

11. Kontrollieren Sie den Status der Netzwerkschnittstelle: Der Status muss sich von [Aus] (siehe Abbildung aus dem Schritt 9) auf [An] geändert haben.

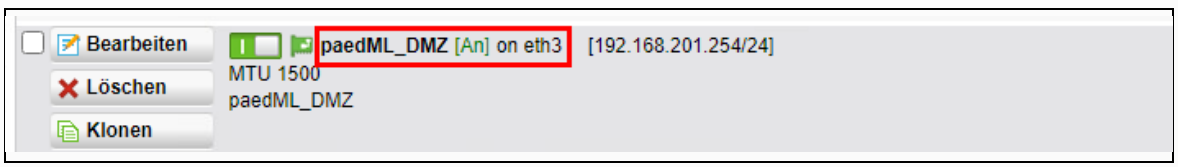


Abb. 20:Status von paedML_DMZ nach dem Refresh des WebAdmin

12. Klicken Sie auf das Menü Support und anschließend auf den Link Tools.

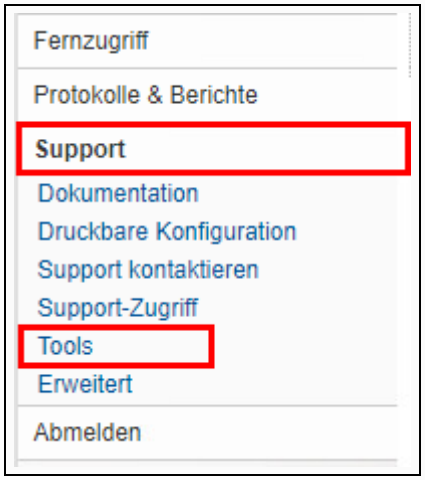


Abb. 21: WebAdmin -> Support-Tools

13. Öffnen Sie die Registerkarte Ping-Prüfung und geben Sie die IP-Adresse der Netzwerkschnittstelle paedML_DMZ `192.168.201.254` in das Eingabefeld `Hostname/IP-Adresse` ein. Klicken Sie auf Übernehmen, um die Ping-Prüfung zu starten.

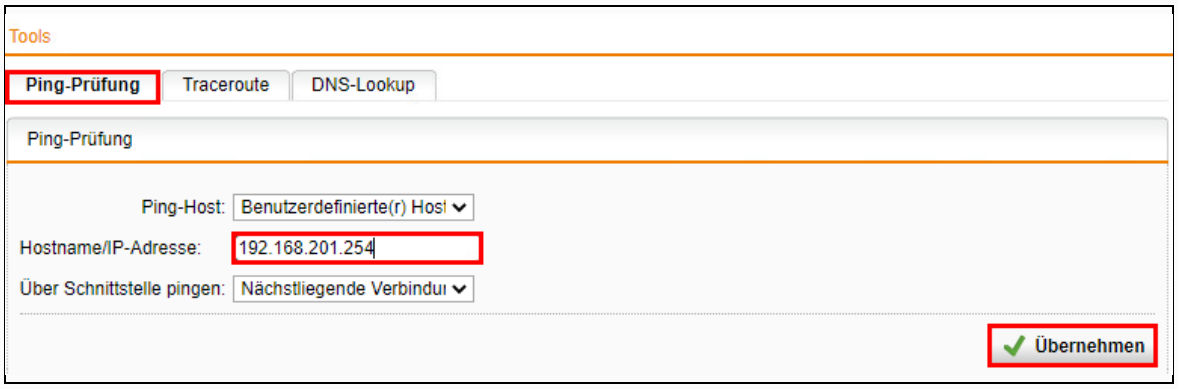


Abb. 22: Ping-Prüfung gegen DMZ-Schnittstelle / 192.168.201.254

14. Prüfen Sie das Ergebnis. Wenn die vorangegangenen Schritte erfolgreich bearbeitet wurden, dann erhalten Sie eine ähnliche Rückmeldung wie nachfolgend dargestellt.

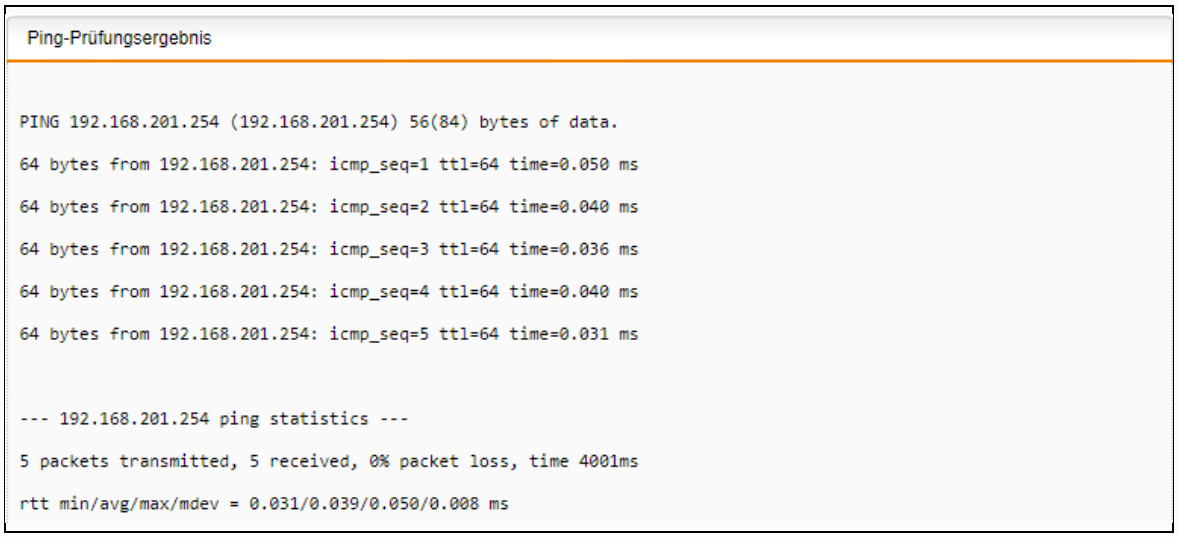


Abb. 23: Ping-Prüfung -> Status

15. Wiederholen Sie die Ping-Prüfung gegen die IP-Adresse `192.168.201.7` der Nextcloud-VM.

Abb. 24: Ping-Prüfung gegen Nextcloud-VM / 192.168.201.7

16. Kontrollieren Sie das Ergebnis.

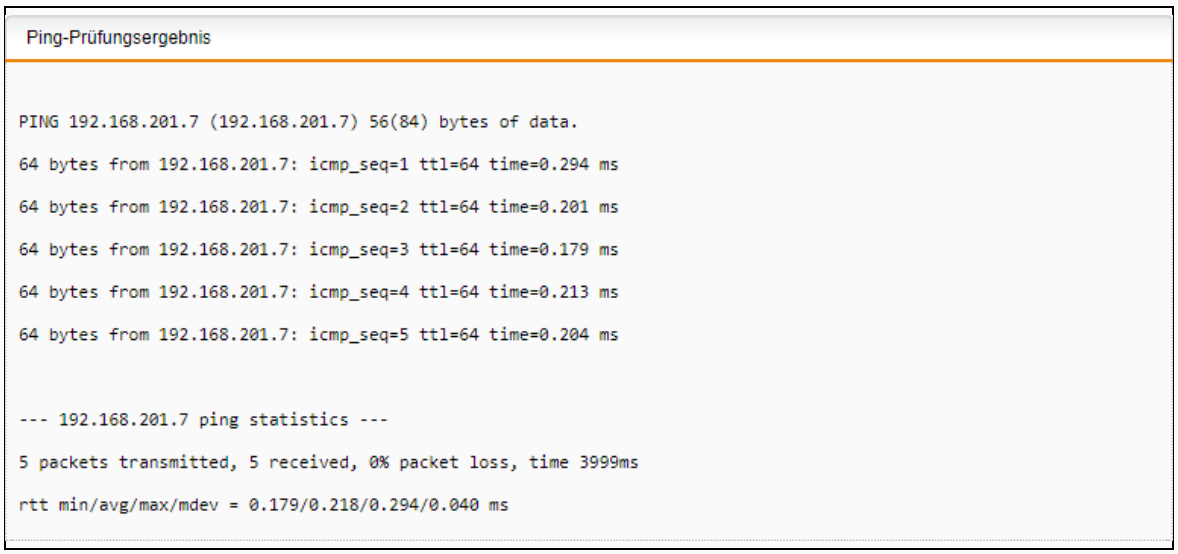


Abb. 25: Ping-Prüfung gegen Nextcloud-VM / 192.168.201.7

3.2 Firewall-Regeln aktivieren

1. Öffnen Sie als Benutzer **admin** WebAdmin.
2. Klicken Sie auf das Menü Network Protection.

Abb. 26: WebAdmin -> Network Protection

3. Öffnen Sie die Seite Firewall und setzen Sie den Ansichtsfilter auf Firewallgruppen | Nextcloud, um nur diejenigen Firewall-Regeln auflisten zu lassen, welche die Nextcloud betreffen.

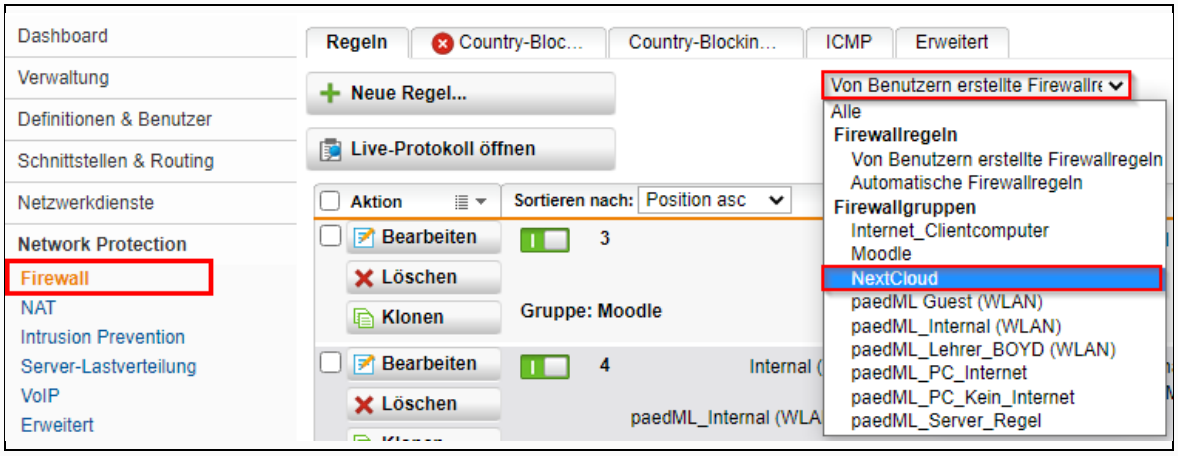


Abb. 27: Firewall-Regeln nach Nextcloud filtern

4. Durch den Ansichtsfilter sollten insgesamt sechs vordefinierte Firewall-Regeln zu sehen sein. Aktivieren Sie diese, indem Sie den jeweiligen Schiebeschalter von deaktiviert auf aktiviert (Grün) umlegen.

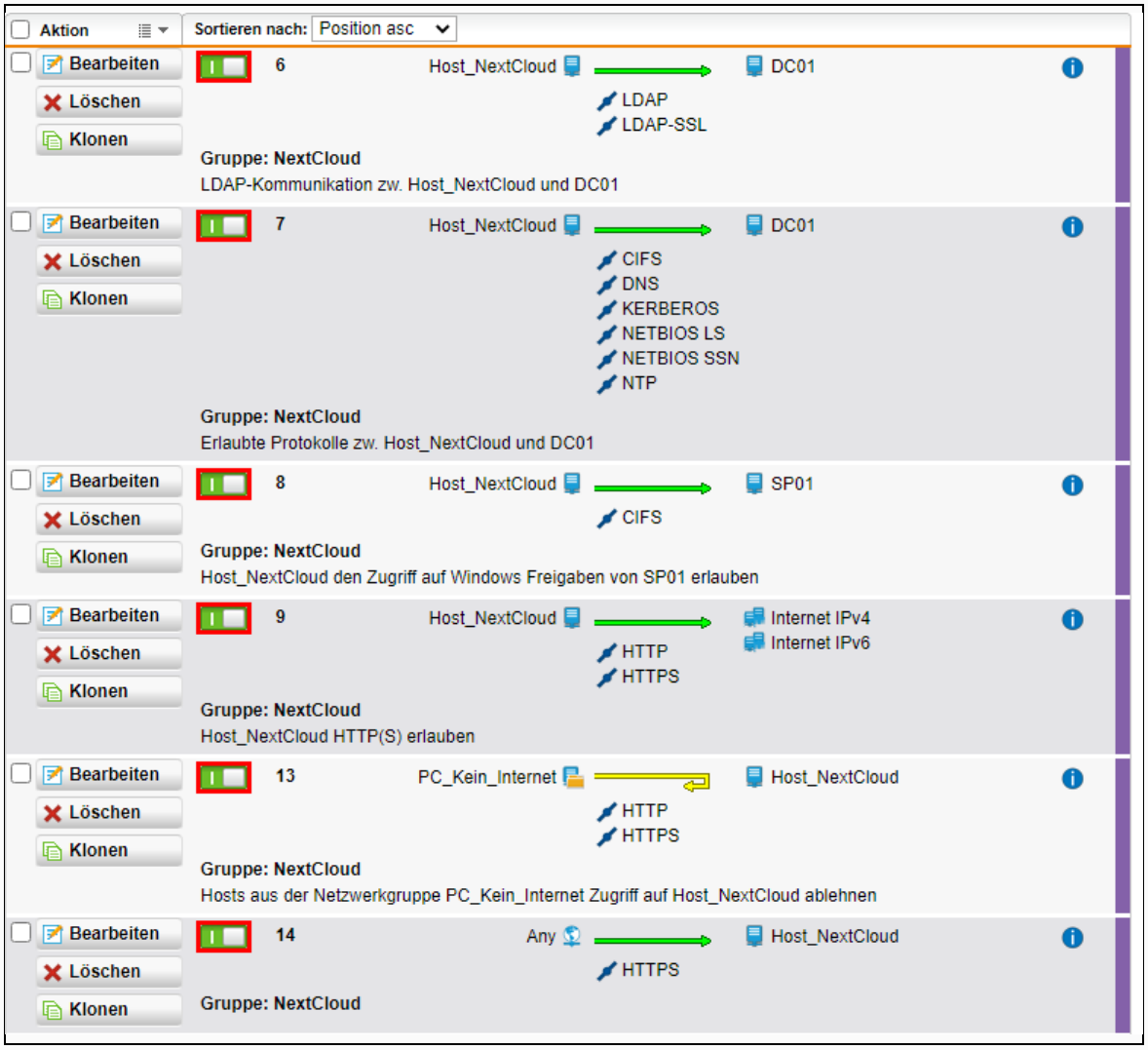


Abb. 28: Standardregeln für Nextcloud aus der LMZ-Vorlage

3.3 Firewall-Regel für SSH

Das PowerShell-Skript `LMZ-Nextcloud.ps1` aus dem Kapitel 6.1 Anpassungen in AD und DNS ab Seite 36 kopiert auf Ihren Wunsch das Zertifikat derjenigen Zertifizierungsstelle, die Ihrem DC01 das Hostzertifikat für LDAPS ausgestellt hat, in die Nextcloud-VM.

Das geht allerdings nur dann, wenn es eine Firewall-Regel gibt, die es SP01 gestattet, per SSH mit der Nextcloud-VM zu kommunizieren.

1. Öffnen Sie Sophos WebAdmin und navigieren Sie zur Konfigurationsseite Network Protection | Firewall, falls Sie WebAdmin zuvor geschlossen haben.
2. Klicken Sie auf Neue Regel.
3. Fügen Sie die neue Regel mit den folgenden Werten mit Speichern hinzu.

- **Gruppe : Nextcloud**
- **Quellen : SP01**
- **Dienste : SSH**
- **Ziele : Host_Nextcloud**
- **Aktion : Zulassen**

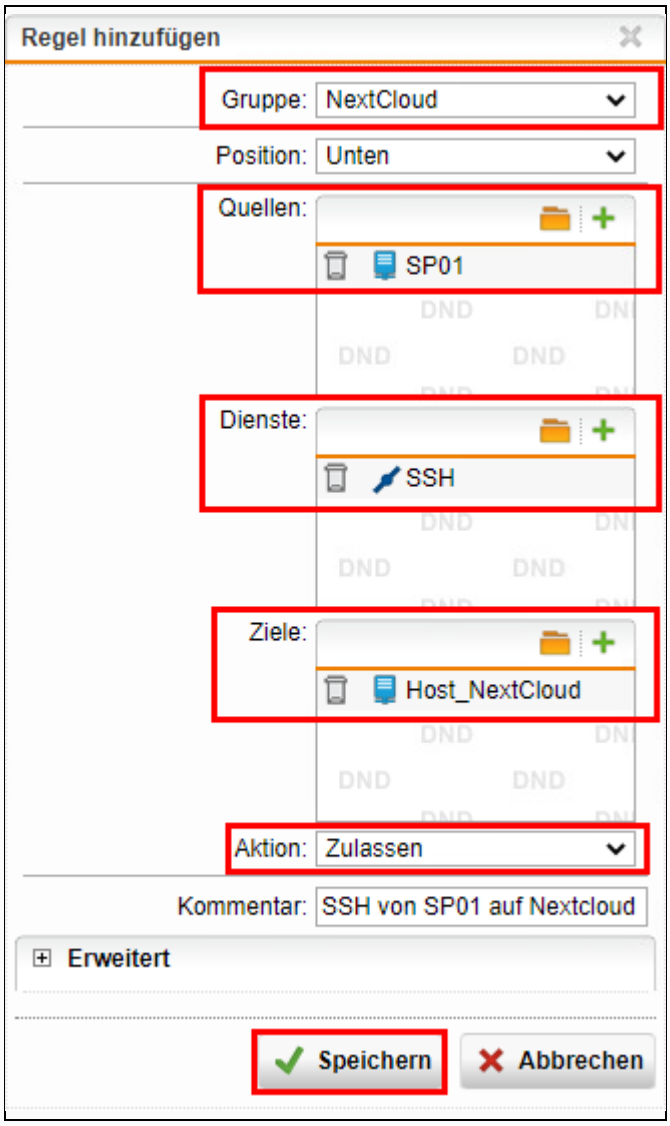


Abb. 29: Neue Firewall-Regel für SSH SP01 → Host_Nextcloud

4. Aktivieren Sie die neu hinzugefügte Regel.

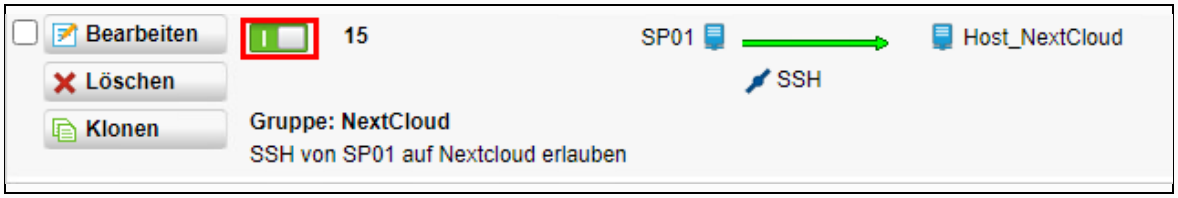


Abb. 30: Firewall-Regel für SSH SP01 → Host_Nextcloud aktivieren

Deaktivieren Sie diese Regel, wenn Sie sie nach der erfolgreichen Initialisierung der Nextcloud-VM nicht mehr brauchen.

3.4 Maskierungsregel für Nextcloud aktivieren

Damit die Nextcloud-VM eine Verbindung ins Internet aufbauen kann, muss für sie eine entsprechende Maskierungsregel festgelegt und aktiviert werden. Unsere Konfigurationsvorlage für Ihre Sophos SG UTM enthält bereits eine solche Regel, die Sie nun aktivieren müssen.

1. Öffnen Sie die Konfigurationsseite NAT.

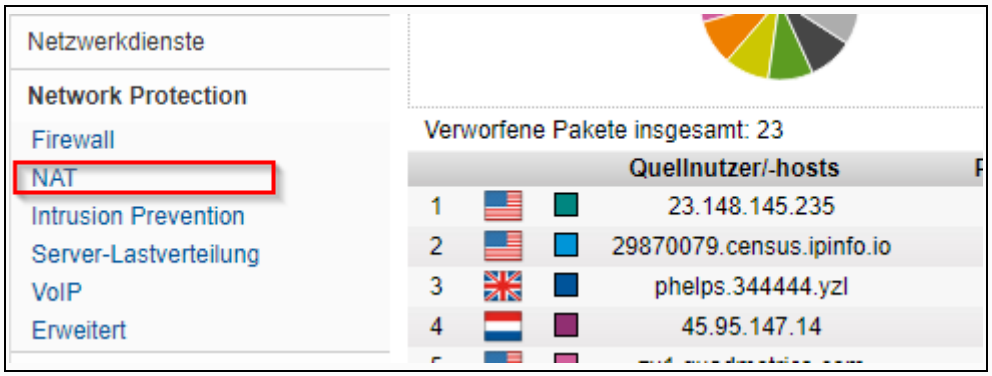


Abb. 31: WebAdmin -> Konfigurationsseite NAT

2. Klicken Sie auf die Registerkarte Maskierung.

Abb. 32: Maskierungsregeln

3. Aktivieren Sie die Maskierungsregel **Host_Nextcloud → External (WAN)**.

Abb. 33: Maskierungsregel Host_Nextcloud → External (WAN) aktivieren

3.5 NAT-Regeln bearbeiten (Optional)

Wenn Sie vorhaben, Ihre Nextcloud über eine öffentlich verfügbare Adresse aus dem Internet zugänglich zu machen, dann gibt es zwei Möglichkeiten:

- Port-Umleitung
- Reverse-Proxy

In diesem Kapitel beschreiben wir den Lösungsansatz auf Basis der Port-Umleitung. Im Anhang finden Sie eine Beispielkonfiguration für einen Reverse-Proxy.

Für den Einsatz eines Reverse-Proxys muss das Modul Webserver Protection zusätzlich kostenpflichtig lizenziert werden. Das Modul ist aus dem Grund weder in unserer Konfigurationsvorlage noch in unseren Handbüchern berücksichtigt. Sie erhalten demnach keinen technischen Support durch unsere Hotline.

Wenn Ihnen das Modul Webserver Protection zu Verfügung steht und Sie Nextcloud über einen Reverse-Proxy bereitstellen wollen, wenden Sie sich an Ihren Dienstleister.

Unsere im Anhang beschriebene Beispielkonfiguration dient Ihnen bzw. Ihrem Dienstleister lediglich als Orientierungshilfe.

1. Öffnen Sie in WebAdmin die Seite NAT unter dem Menü Network Protection.

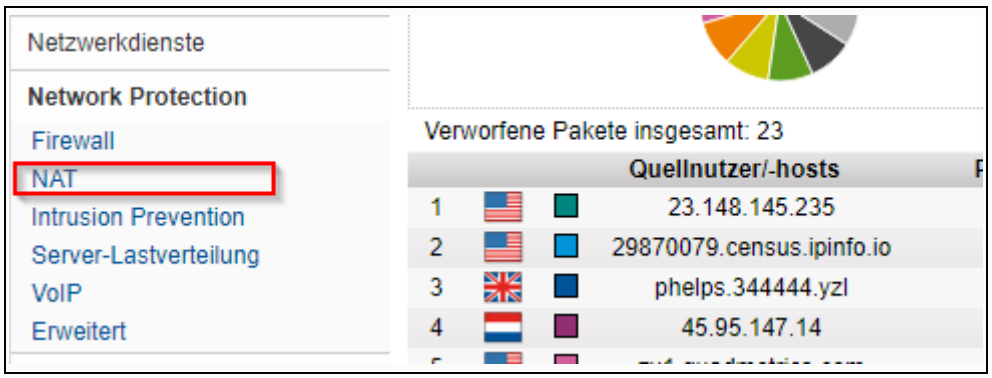


Abb. 34: WebAdmin -> Network Protection NAT

2. Klicken Sie auf die Registerkarte NAT und anschließend auf den Button Neue NAT-Regel....

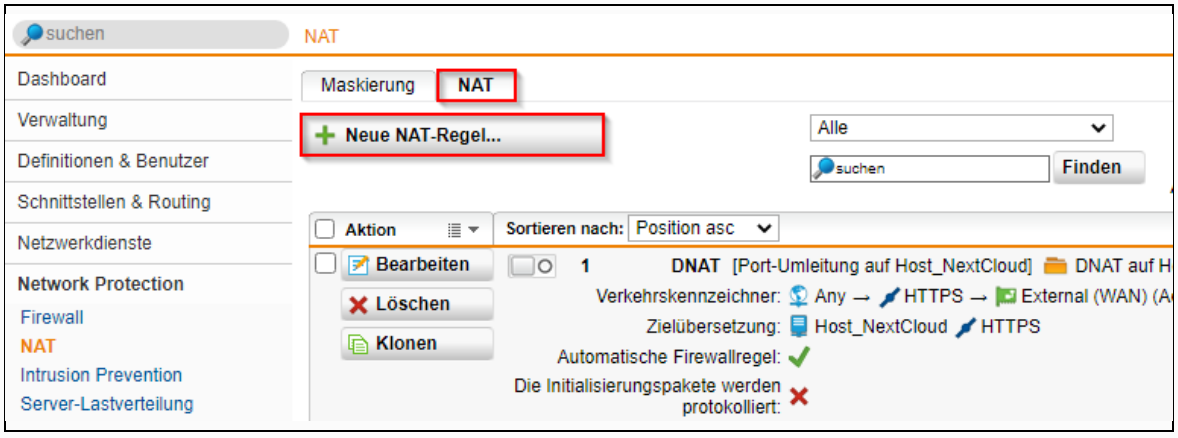


Abb. 35: WebAdmin -> Neue NAT-Regel hinzufügen

Die nachfolgende DNAT-Regel für das HTTP-Protokoll ist für das Einbinden eines Let's Encrypt-Zertifikats erforderlich.

3. Übernehmen Sie die folgenden Werte für die neue NAT-Regel:

- **(1) Gruppe : DNAT auf Host_Nextcloud**
- **(2) Regeltyp : DNAT (Ziel)**
- **(3) Datenverkehrsquelle : Any**
- **(4) Datenverkehrsdienst : HTTP**
- **(5) Datenverkehrsziel : External (WAN) (Address)**
- **(6) Ziel ändern in : Host_Nextcloud**
- **(7) Dienst ändern in : HTTP**
- **(8) Automatische Firewallregel: aktiviert**
- **(9) Kommentar: HTTP-Umleitung auf Host_Nextcloud**

Fügen Sie die neue NAT-Regel mit Speichern hinzu.

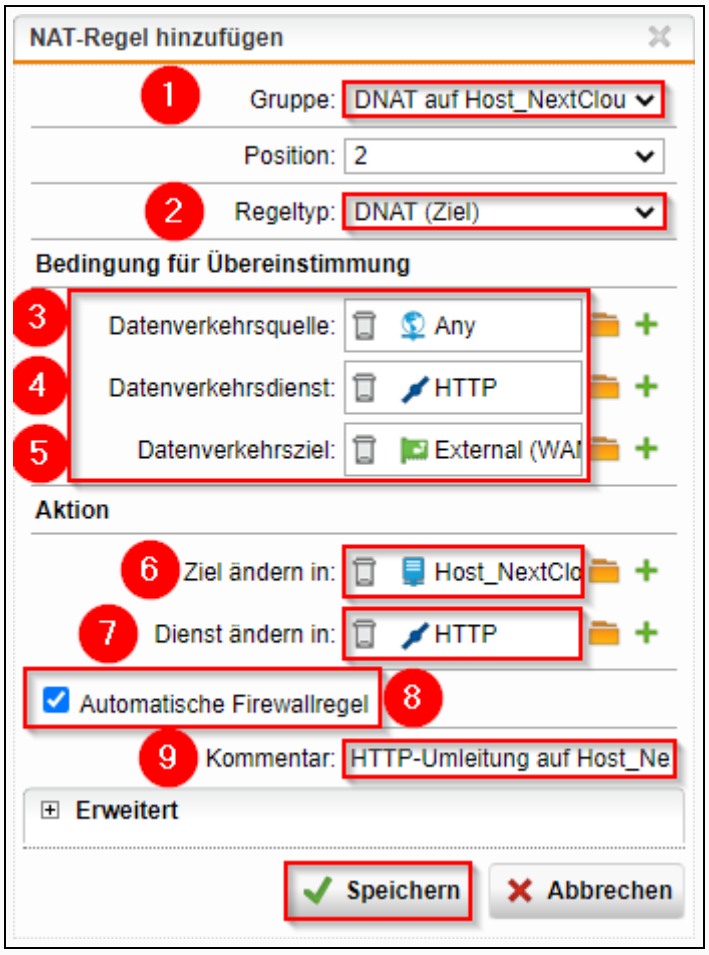


Abb. 36: DNAT auf Host_Nextcloud für HTTP

4. Aktivieren Sie nun die beiden abgebildeten DNAT-Regeln.

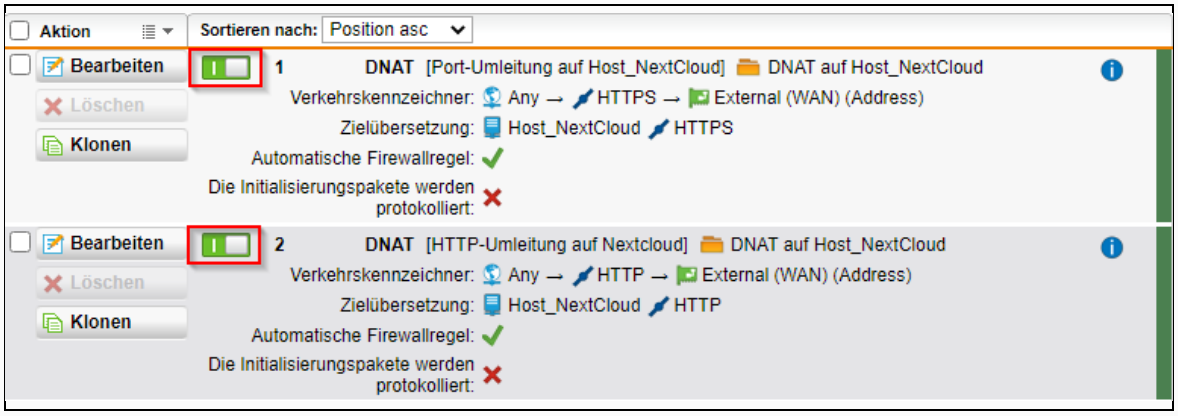


Abb. 37: Portgruppe hinzufügen > Eigenschaften definieren

Die DNAT-Regel für die Umleitung des HTTPS-Dienstes ist bereits in unserer Konfigurations-vorlage für Sophos SG UTM enthalten und muss deswegen nicht nachträglich hinzugefügt werden.

3.6 Nextcloud für den Netzwerkdienst NTP zulassen

Es ist wichtig, dass die Uhrzeit der Nextcloud mit der Ihrer Domäne synchron gehalten wird, um etwaige Anmeldstörungen zu vermeiden.

1. Öffnen Sie Sophos WebAdmin und klicken Sie auf das Menü Netzwerkdienste und anschließend auf den Link NTP.

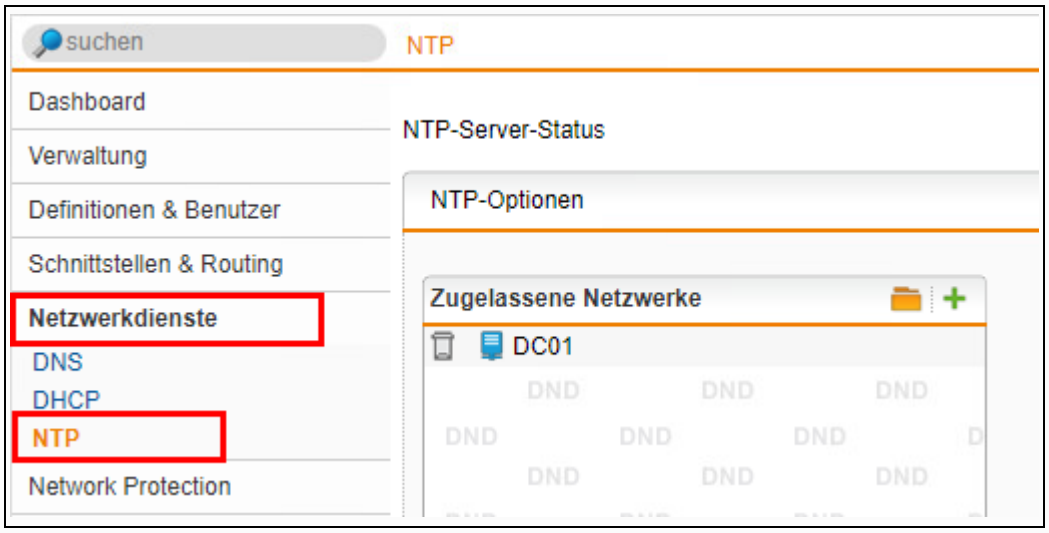


Abb. 38: WebAdmin -> Netzwerkdienst NTP

2. Fügen Sie **Host_Nextcloud** in **Zugelassene Netzwerke** hinzu und speichern Sie die Änderung mit Übernehmen.

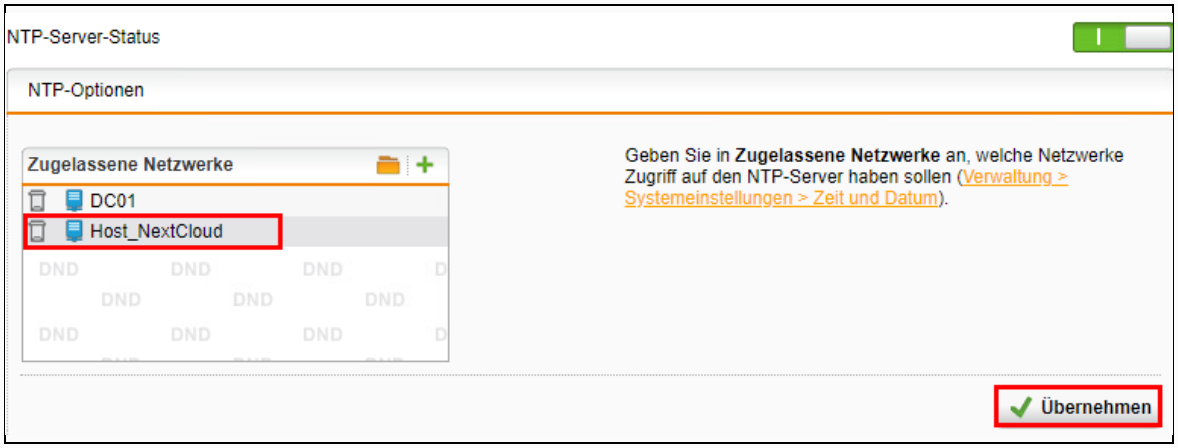


Abb. 39: NTP für Host_Nextcloud erlauben

4 Einrichten einer externen Domäne

Um die Nextcloud von außerhalb des Schulnetzes nutzen zu können, muss sie aus dem Internet erreichbar sein. Eine statische IP-Adresse von Ihrem Internetanbieter ist dafür der verlässlichste Weg.

Es besteht auch die Möglichkeit den Server durch eine Dynamische DNS (DynDNS) Adresse erreichbar zu machen. Es besteht jedoch das Risiko, dass die Adresse der Nextcloud nach einem IP-Wechsel zeitweise nicht erreichbar sein kann. Das Einrichten eines DynDNS Anbieters ist kein Gegenstand dieser Anleitung.

Im Folgenden wird beispielhaft davon ausgegangen, dass die Homepage ihrer Schule unter www.meine-schule.de erreichbar ist und die Nextcloud-VM unter der Adresse intranet.meine-schule.de erreichbar sein soll. Die Benutzer greifen dann über https://intranet.meine-schule.de/nextcloud auf die Nextcloud zu.

Zunächst sollten Sie die IP-Adresse bzw. DynDNS-Adresse Ihrer Schule in Erfahrung bringen.

Bei Unklarheiten wenden Sie sich an Ihren Schulträger bzw. Dienstleister.

Insbesondere hängt die zu verwendende IP-Adresse von der Netzstruktur ab.

Bei Ihrem Webseiten-Anbieter müssen Sie nun die Subdomäne (in unserem Beispiel wäre das intranet.meine-schule.de) beantragen bzw. selbst konfigurieren. Es sind auch andere Subdomänen denkbar.

Anschließend wird ein DNS-Eintrag gesetzt, der Aufrufe von intranet.meine-schule.de an die IP-Adresse der Schule weiterleitet.

Wie der Eintrag gesetzt wird, hängt davon ab, durch wen Ihre Schulwebseite angelegt wurde.

Bei „BelWü“ reicht eine E-Mail an hostmaster@belwue.de mit der Bitte um Setzen des Eintrages:

```
intranet.meine-schule.de IN ANAME 11.22.33.44
```

Wobei 11.22.33.44 durch ihre statische IP-Adresse oder ihr DynDNS Eintrag ersetzt werden muss.

Für weitere Anbieter wenden Sie sich bitte an deren Support oder die dort hinterlegte Dokumentation. Der Name des Eintrages kann hier variieren.

5 LDAPS-Zertifikat

Die Nextcloud wird so eingerichtet, dass sich Ihre Benutzer mit ihrem eigenen Benutzernamen und Kennwort aus der schulischen paedML anmelden können. Dafür müssen Sie im Folgenden das CA-Zertifikat des Hostzertifikats für den Host (Server) dc01.musterschule.schule.paedml exportieren.

Die LDAP-Kommunikation findet zwar nur zwischen dem Server DC01 und der Nextcloud 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 Kennwort des Benutzerkontos ldapnextcloud

1. Melden Sie sich als Domänen-Admin am Server **DC01** an.
2. Öffnen Sie die Konsole Active Directory-Benutzer und -Computer.

Abb. 40: Active Directory-Benutzer und -Computer

3. Das Benutzerkonto **ldapnextcloud** finden Sie in der **OU _ServiceAccounts**. Markieren Sie es und klicken Sie mit der rechten Maustaste auf das Benutzerkonto ldapnextcloud. Wählen Sie aus dem Kontextmenü die Option Kennwort zurücksetzen aus.

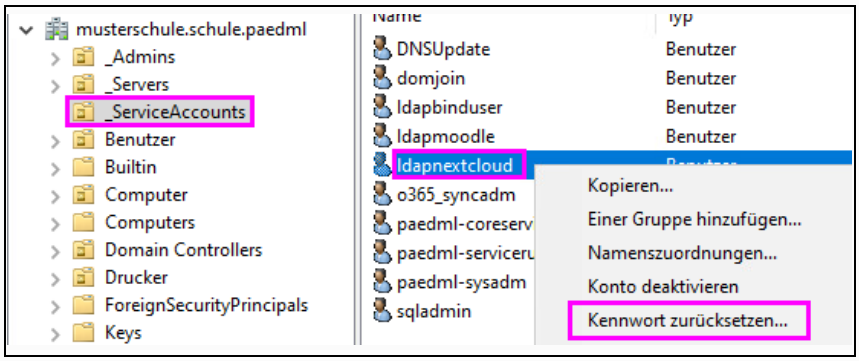


Abb. 41: ldapnextcloud

4. Geben Sie ein neues Kennwort ein und wiederholen Sie es zur Bestätigung.

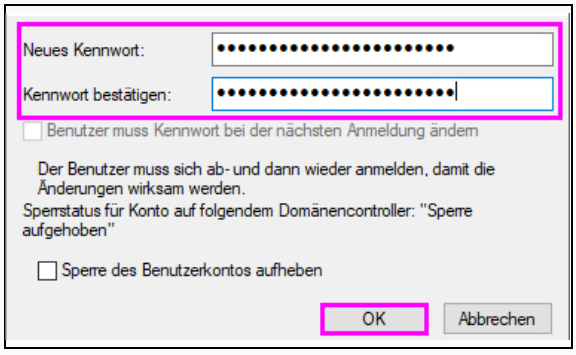


Abb. 42: ldapnextcloud -> Kennwort zurücksetzen

5.2 CA-Zertifikat exportieren

1. Melden Sie sich am Server **SP01** als Domänen-Admin an.
2. Drücken Sie auf die Tastenkombination Windows + R, um das Dialogfenster zur Ausführung eines Programms zu öffnen. Tippen Sie `mmc.exe` ein und drücken Sie auf die ENTER-Taste.

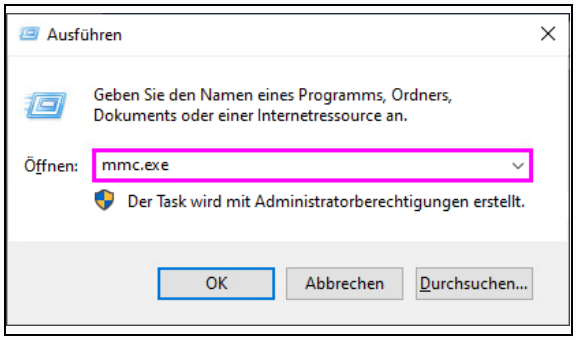


Abb. 43: MMC.exe

3. Drücken Sie auf die Tastenkombination Strg + M, um das Dialogfenster **Snap-Ins hinzufügen bzw. entfernen** zu öffnen. Scrollen Sie die Tabelle Verfügbare Snap-Ins herunter. Wählen Sie das Snap-In Zertifikate aus und klicken Sie auf den Button Hinzufügen.

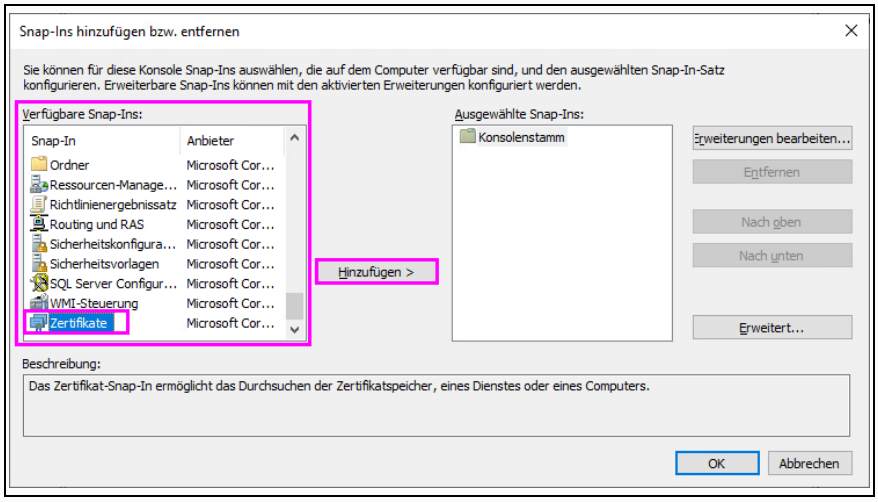


Abb. 44: Dialog Snap-Ins hinzufügen bzw. entfernen

4. Wählen Sie die Option Computerkonto aus und klicken Sie auf Weiter.

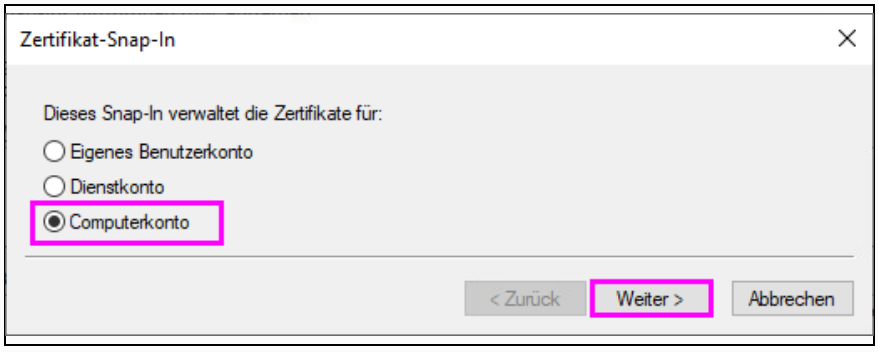


Abb. 45: Snap-In für Computerkonto laden

5. Lassen Sie die Auswahl bei der Option Lokalen Computer (Computer, auf dem diese Konsole ausgeführt werden soll) und klicken Sie auf den Button Fertig stellen.

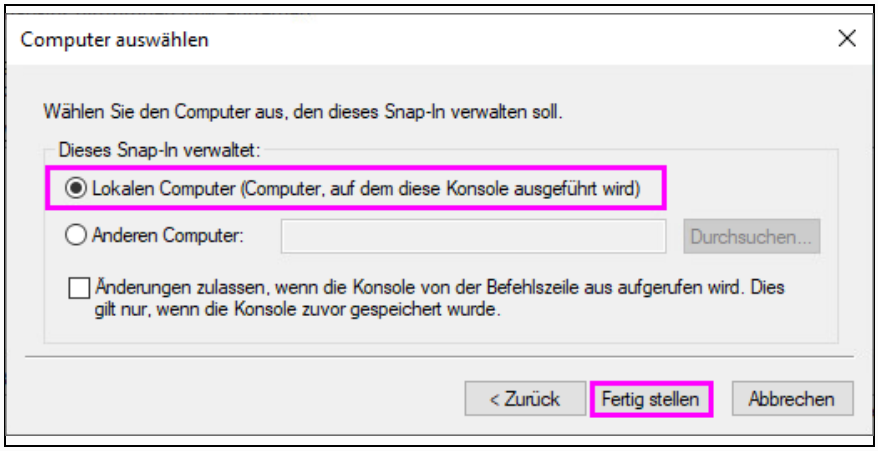


Abb. 46: Computer auswählen für das Snap-In

6. Klicken Sie auf OK, um das Dialogfenster Snap-Ins hinzufügen bzw. entfernen zu schließen.
7. Erweitern Sie den Ordner Vertrauenswürdige Stammzertifizierungsstellen. Markieren Sie im Unterordner Zertifikate das Zertifikat, das für **paedML Windows Root CA** ausgestellt wurde.

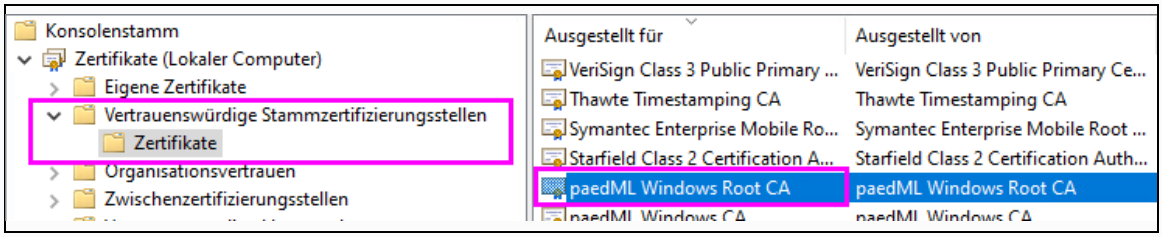


Abb. 47: Vertrauenswürdige Stammzertifizierungsstelle

8. Klicken Sie auf das markierte Zertifikat mit der rechten Maustaste und wählen Sie aus Alle Aufgaben die Option Exportieren aus.

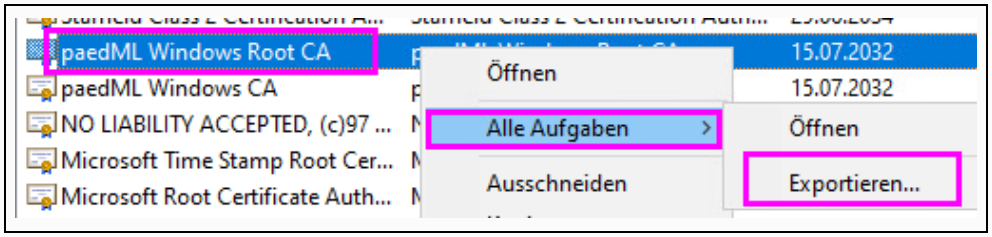


Abb. 48: Zertifikat exportieren

9. Überspringen Sie das Willkommens-Fenster mit Weiter.
10. Wählen Sie das Format **Base-64-codiert X.509 (.CER)** aus und klicken Sie auf Weiter.

Die Auswahl des Formats Base-64-codiert X.509 (.CER) ist zwingend!

Wenn Sie diesen Hinweis ignorieren, führt es unweigerlich zu einem Fehler während der Initialisierung der Nextcloud und Sie können sich vorerst nicht in der Nextcloud anmelden, bis das Zertifikat im korrekten Format ausgetauscht worden ist.

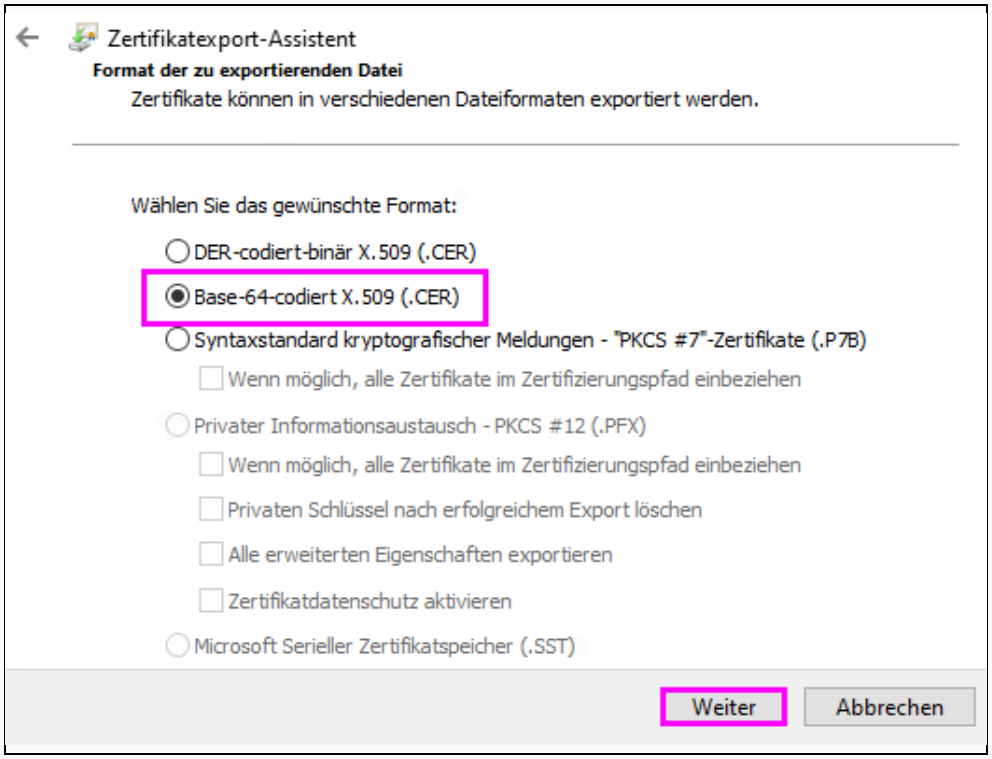


Abb. 49: Zertifikat im Format Base-64-codiert exportieren

11. Speichern Sie die Datei unter einem leicht zu merkenden Namen. Denn Sie müssen sie im Kapitel 6.1 Anpassungen in AD und DNS öffnen, um sie auf die Nextcloud übertragen zu können. Klicken Sie auf Weiter.

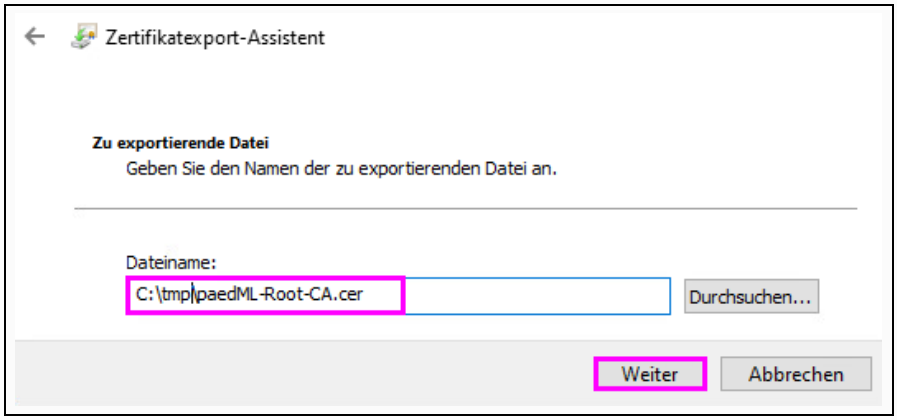


Abb. 50: Zertifikat unter einem leicht zu merkenden Namen speichern

12. Beenden Sie den Zertifikatexport-Assistenten mit Fertig stellen.

6 Initialisierung der Nextcloud

6.1 Anpassungen in AD und DNS

Das Skript LMZ-Nextcloud.ps1 fügt unter anderem zwei neue Gruppenrichtlinienobjekte in AD hinzu. Details dazu finden Sie im Anhang A Nützliche Ergänzungen ab Seite 51.

1. Öffnen Sie auf dem Server SP01 den Datei-Explorer und navigieren Sie nach `D:\Installation\paedML\Erweiterungen\Nextcloud-V3`.
2. Führen Sie das PowerShell-Skript `LMZ-Nextcloud.ps1` mit PowerShell aus.
3. 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!)**.

Abb. 51: Kennwort für Benutzer root (Nextcloud)

4. Wiederholen Sie die Kennworteingabe.

Abb. 52: Kennwort wiederholen für Benutzer root (Nextcloud)

5. Es wird nun ein Dialogfenster zur Dateiauswahl geöffnet. Wählen Sie das zu kopierende Zertifikat aus dem Kapitel 5.2 CA-Zertifikat exportieren aus und klicken Sie auf Öffnen.

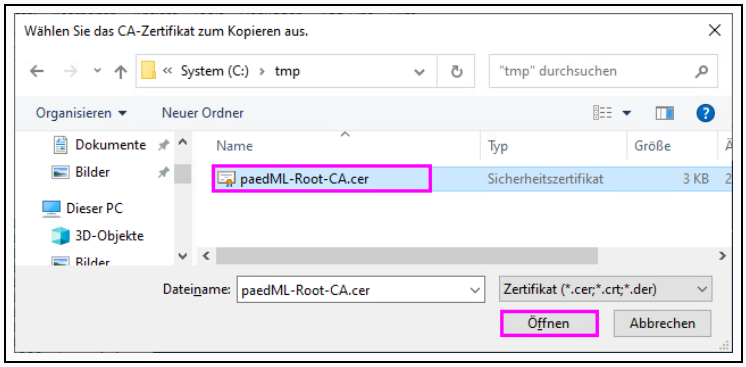


Abb. 53: Zertifikat auswählen

6. Bestätigen Sie die Dateiauswahl mit Ja.

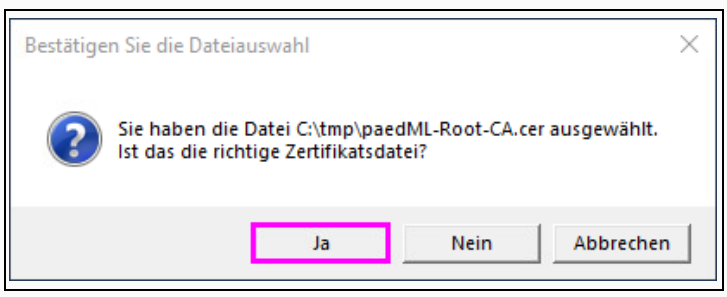


Abb. 54: Dateiauswahl bestätigen

7. Drücken Sie auf die ENTER-Taste, um das Skript zu beenden.

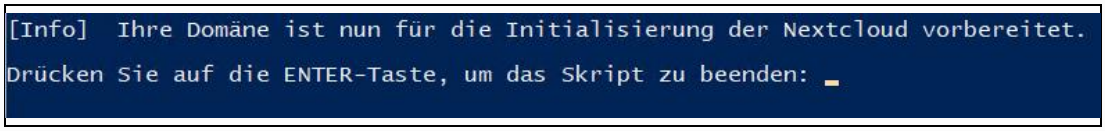


Abb. 55: Skript LMZ-Nextcloud.ps1 beenden

6.2 Nextcloud-VM initialisieren

Falls Sie eine eigene Domäne für die Nextcloud besitzen und die im Kapitel 3.5 NAT-Regeln bearbeiten (Optional) beschriebenen Weiterleitungsregeln hinzugefügt haben, müssen Sie an zwei Stellen abweichende Eingaben tätigen.

Diese Stellen werden im Text kennzeichnen wir mithilfe einer Info-Box wie diese.

Zur Initialisierung der Nextcloud-VM müssen Sie u.a. das Kennwort für das Benutzerkonto **nc_admin** festlegen. Aufgrund der Art und Weise wie dieses Kennwort **während der Initialisierungsphase** gesetzt wird, kann es vorkommen, dass ein Sonderzeichen nicht akzeptiert wird. Falls Ihr Kennwort Sonderzeichen enthält, dann verwenden Sie für die Dauer der Initialisierung ein Kennwort ohne Sonderzeichen. Sie können Ihr Kennwort später im Kapitel 7.7 Ändern des Kennworts für das Benutzerkonto nc_admin über die Benutzeroberfläche der Nextcloud ändern.

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 oder den in Windows Server 2022 eingebauten SSH-Client. Nachfolgend beschreiben wir die Initialisierung auf der Server-Konsole.

Wenn Sie das nachfolgend beschriebene Initialisierungsskript in PuTTY oder in dem SSH-Client des Windows Server 2022 ausführen, dann müssen Sie es in einer gesonderten Screen-Sitzung ausführen.

1. Melden Sie sich als Benutzer root auf der Server-Konsole der Nextcloud an. Sofern es nicht bereits geändert wurde, lautet das Kennwort „**NextCloud**“. Achten Sie bei der Eingabe des Kennworts auf die Groß- und Kleinschreibung.
2. Führen Sie zuerst den folgenden Befehl aus.

```
ucr set lmz/paedml-version='windows'
```

Abb. 56: paedml-version setzen

Wenn Sie eine eigene Domäne für die Nextcloud nutzen, ersetzen Sie den nachfolgenden Befehl durch

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

3. Führen Sie den folgenden Befehl aus, wenn Sie **keine eigene Domäne** für die Nextcloud nutzen.

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

Wenn Sie **eine eigene Domäne für die Nextcloud** besitzen, führen Sie den folgenden Befehl aus:

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

4. 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*). Notieren Sie sich das Kennwort z. B. in einem Kennwortsafe.

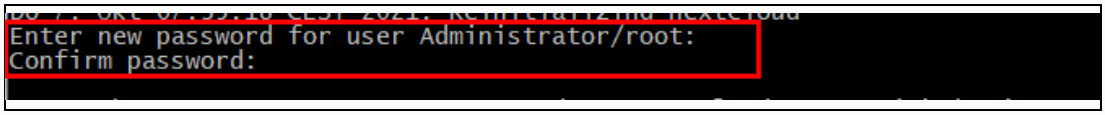


Abb. 57: lmz-initial-setup -> Kennwort für Administrator/root

Verwechseln Sie den Benutzer Administrator der Nextcloud-VM nicht mit dem Administrator Ihrer Domäne!

Hierbei handelt es sich um das Admin-Konto, das dazu genutzt wird, um Univention UCS zu verwalten und zu warten. 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 im Kapitel 5.1 Kennwort des Benutzerkontos ldapnextcloud vergeben.

Nach der Eingabe des Kennworts für das Benutzerkonto ldapnextcloud 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 ldapnextcloud eingeben. Das kann dazu führen, dass Ihre Nextcloud aus dem Internet so lange nicht erreichbar ist, bis dieser Fehler korrigiert wurde. (vgl. FAQ B.5.3 Wie kann ich externe Domäne korrigieren und Let's Encrypt Zertifikat installieren?**)**

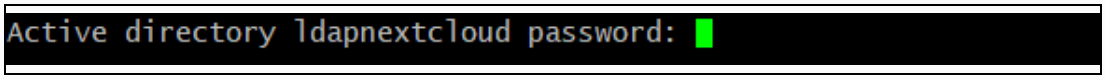


Abb. 58: lmz-initial-setup -> Kennwort für ldapnextcloud

Wenn Sie eine eigene Domäne für die Nextcloud nutzen, ersetzen Sie im nachfolgenden Schritt den Vorgabewert `nextcloud.paedml.lokal` durch Ihre eigene Domäne, zum Beispiel: `mycloud.meine-schule.de`

6. Löschen Sie den Eintrag `nextcloud.paedml.lokal` und 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`.

Abb. 59: lmz-initial-setup -> FQDN der OctoGate

7. Legen Sie ein hinreichend sicheres Kennwort (**mindestens 10 Zeichen lang**) für das Benutzerkonto **nc_admin** fest. 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.

Abb. 60: lmz-initial-setup -> Kennwort für nc_admin

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

Abb. 61: lmz-initial-setup -> Kennwort für nc_admin wiederholen

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

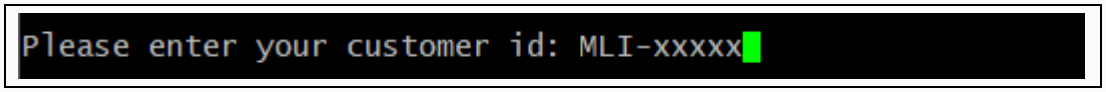


Abb. 62: lmz-initial-setup -> Eingabe MLI-Nummer

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

Abb. 63: lmz-initial-setup -> Eingabe MLI-Nummer

11. **Warten Sie, bis das Skript durchgelaufen ist. Das dauert einige Minuten (5 bis 10 Minuten).**
    Am Ende der Initialisierung werden Sie aufgefordert, den Server neu zu starten. Drücken Sie auf die ENTER-Taste, um den Neustart anzustoßen.
12. Warten Sie, 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 Initialisierung der Nextcloud abschließen

1. Melden Sie sich als Benutzer **root** in der Nextcloud an. Verwenden Sie dabei das im vorangegangenen Kapitel festgelegte Kennwort für den Benutzer **root**.
2. Führen Sie den folgenden Befehl aus, um die Initialisierung Ihrer Nextcloud fertigzustellen:

```
sh lmz-nextcloud-windows-finalize
```

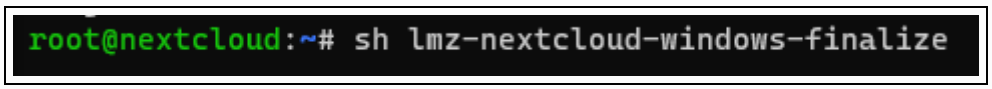


Abb. 64: lmz-nextcloud-windows-finalize

6.4 UCS-Zertifikat importieren

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

1. Melden Sie sich als Domänen-Admin am Server **SP01** an.
2. Öffnen Sie im Datei-Explorer den Ordner `D:\Installation\paedML\Erweiterungen\Nextcloud-V3`.
3. Führen Sie das PowerShell-Skript `LMZ-CopyUCSCert.ps1` aus.
4. Öffnen Sie im Datei-Explorer den Ordner `\\musterschule.schule.paedml\NETLOGON\paedML\Nextcloud\CACert`. Kontrollieren Sie, ob sich die Datei `ucs-root-ca.crt` darin befindet.

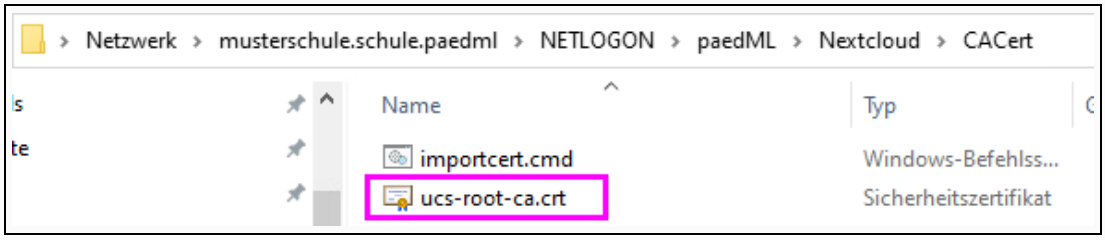


Abb. 65: CA-Zertifikat ucs-root-ca.crt

Während der Vorbereitung wurde unter anderem das GPO *paedML_Computer_alle_Nextcloud_CACert_v1.0* importiert und mit der OU Computer verknüpft. Dieses GPO sorgt dafür, dass alle Domänengeräte mit der Ausnahme von DC01 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 NETLOGON-Verzeichnis kopiert werden.

7 Abschlussarbeiten

Für die nachfolgenden Abschlussarbeiten nutzen Sie wie im Kapitel 1.9 Webbrowser beschrieben am besten Google Chrome oder Mozilla Firefox, wobei Cookies zugelassen sein müssen.

Denn: Sollte es während der Aktualisierung einer App zu einer Warnmeldung kommen, die Sie bestätigen müssen, dann ist es in Microsoft Edge (Stand 01.08.2022, Version 103.0.1264.77) aufgrund eines Darstellungsfehlers nicht möglich, die Warnmeldung zu bestätigen, um die Aktualisierung fortzusetzen.

7.1 App Center App Let's Encrypt auf Aktualisierung prüfen

1. Öffnen Sie im Browser die Univention Management Console (UMC), indem Sie die URL https://nextcloud.paedml.lokal öffnen.
2. Klicken Sie auf das Menü-Icon ☰ und anschließend auf das Menü Anmelden.

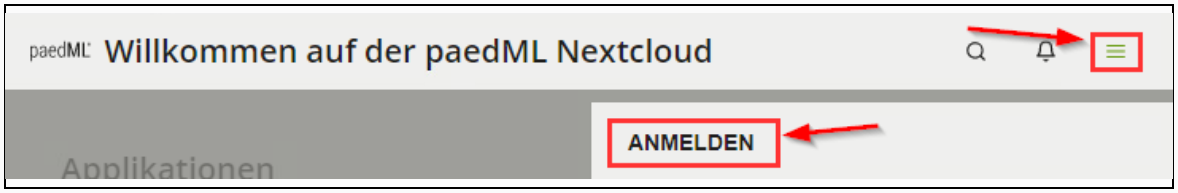


Abb. 66: Anmelden in UMC

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!**

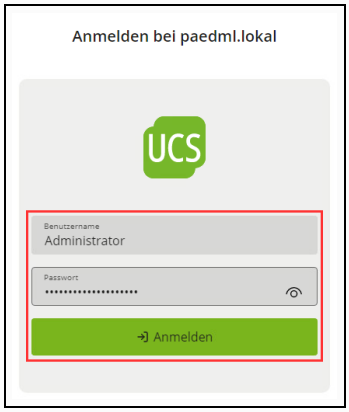


Abb. 67: Anmelden bei paedml.lokal

4. Klicken Sie auf die Kachel App Center unter der Rubrik **Favoriten**.

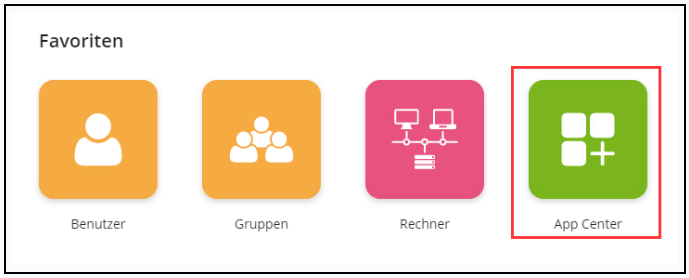


Abb. 68: Favoriten -> App Center

5. Bestätigen Sie den Hinweis, indem Sie auf den Button FORTFAHREN klicken. Öffnen Sie die Seite Software.

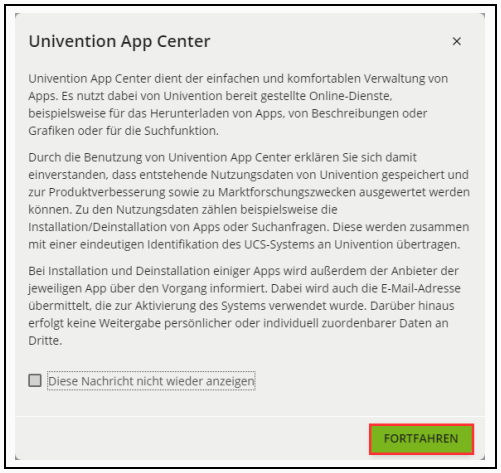


Abb. App Center Nutzungshinweis

6. Klicken Sie auf die Kachel Let's Encrypt.

Abb. 69: App Center -> Installierte Apps

7. Schließen Sie auf den Button INSTALLATION VERWALTEN.

Abb. 70: Let's Encrypt Installation verwalten

Falls es eine aktuelle Version der App Let's Encrypt gibt, erscheint der Button AKTUALISIEREN zur Auswahl. Klicken Sie auf den Button, um die App zu aktualisieren.

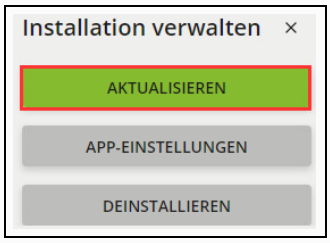


Abb. 71: Let's Encrypt aktualisieren

Falls bereits die aktuelle Version der Let's Encrypt App installiert wurde, fehlt der Button AKTUALISIEREN. Schließen Sie das Dialogfenster, indem Sie auf das X-Icon klicken.

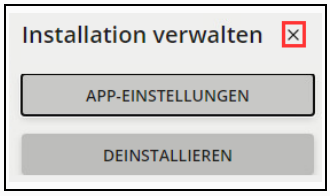


Abb. 72: Let's Encrypt keine Aktualisierung notwendig

7.2 Nextcloud aktualisieren

Prüfen Sie analog zu Kapitel 7.1 App Center App Let's Encrypt auf Aktualisierung prüfen nach, ob für die App Nextcloud eine Aktualisierung verfügbar ist und installieren Sie die Aktualisierung gegebenenfalls.

7.3 App ONLYOFFICE aktualisieren

Prüfen Sie analog zu Kapitel 7.1 App Center App Let's Encrypt auf Aktualisierung prüfen nach, ob für die App ONLYOFFICE eine Aktualisierung verfügbar ist und installieren Sie die Aktualisierung gegebenenfalls.

7.4 Quota für alle Benutzer kontrollieren

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. Melden Sie sich als Benutzer **root** in der Nextcloud-VM an.
2. Führen Sie den folgenden Befehl **in einer Zeile** aus:

```
nccmd ldap:show-config s01
```

Abb. 73: LDAP-Konfiguration auflisten

Suchen Sie in der Konfigurationstabelle nach der Option **ldapQuotaDefault**. Der Wert dieser Option sollte **0** sein.

Abb. 74: LDAP Default Quota

Steht darin ein anderer Wert als 0, führen Sie den folgende Befehl aus, um ihn zu korrigieren.

```
nccmd ldap:set-config s01 ldapQuotaDefault "0"
```

3. Führen Sie den folgenden Befehl aus.

```
nccmd config:app:set files default_quota --value="0 B"
```

Abb. 75: LDAP Default Quota

Falls Sie für den Benutzer nc_admin eine abweichende Quota-Regel definieren wollen, finden Sie im Anhang B.4 Quota-Einschränkung für Benutzer nc_admin aufheben eine Beschreibung dazu.

7.5 Tauschlaufwerk für Projekte für Schülerinnen und Schüler freigeben

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

Abb. 76: Nextcloud -> Einstellungen

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

Abb. 77: Nextcloud -> Einstellungen -> Externe Speicher

5. Hier finden Sie den Tauschordner für Projekte `T-Tausch-Projekte`. Standardmäßig ist der Ordner mit der Sicherheitsgruppe G_Lehrer verknüpft. Wenn Sie ihn Ihren Schülern ebenfalls verfügbar machen wollen, dann fügen Sie die Sicherheitsgruppen Ihrer Schüler hinzu, zum Beispiel *G_Schueler_RS*. Klicken Sie anschließend auf das Häkchen ☑, um die Änderung zu speichern.

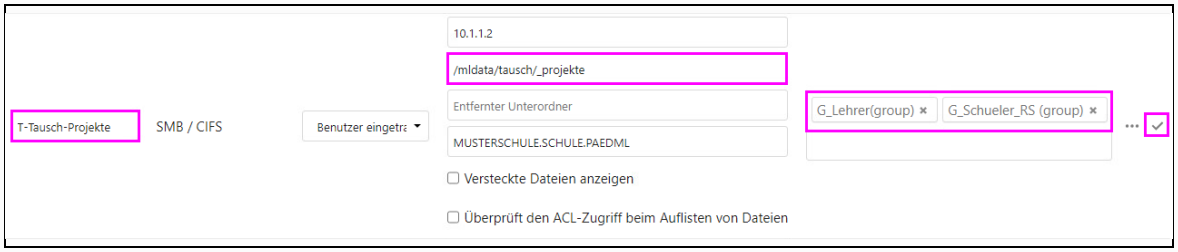


Abb. 78: Tauschverzeichnis für Schüler freigeben

Wenn mehrere Schularten in Ihrer paedML® Windows abgebildet sind, fügen Sie die Sicherheitsgruppen der jeweiligen Schularten hinzu. Sie können sich auch überlegen, für jede Schulart einen eigenen Tauschordner in Nextcloud bereitzustellen, z.B. T-Tausch-Projekte_RS, T-Tausch-Projekte_GYM usw.

7.6 Desktop-Verknüpfung für die Nextcloud anpassen

Wie zu Beginn des Kapitels 6.1 Anpassungen in AD und DNS beschrieben, fügt das Skript `LMZ-Nextcloud.ps1` fügt unter anderem zwei neue Gruppenrichtlinienobjekte im AD hinzu. Eines davon, *paedML_Benutzer_alle_Nextcloud_DesktopLink_v1.0* nämlich, erstellt auf dem Desktop der Benutzer eine Verknüpfung zur Nextcloud Ihrer Schule.

Die URL, die in der Desktopverknüpfung enthalten ist, lautet standardmäßig: https://nextcloud.paedml.lokal. Sie kann demnach nur aus dem Schulnetz benutzt werden, um die Nextcloud zu öffnen. Wenn Sie mobile Endgeräte – etwa schuleigene Notebooks – einsetzen, ist es deshalb sinnvoll, die Desktop-Verknüpfung durch die eigene, aus dem Internet erreichbare URL zu ersetzen. Wie das geht, finden Sie im Anhang A.4 Desktopverknüpfung mit dem externen FQDN anlegen.

7.7 Ändern des Kennworts für das Benutzerkonto nc_admin

Zu Beginn des Kapitels 6.2 Nextcloud-VM initialisieren haben wir Sie darauf hingewiesen, dass für den Initialisierungsvorgang einige Sonder- sowie das Leerzeichen im Kennwort für das Benutzerkonto **nc_admin** vermieden werden sollten.

Falls Sie aus dem Grund vorläufig ein simples Kennwort für das Benutzerkonto **nc_admin** festgelegt haben, sollten Sie es jetzt ändern.

1. Öffnen Sie in einem Browser die Nextcloud (https://nextcloud.paedml.lokal).
2. Melden Sie sich als Benutzer **nc_admin** an.
3. Klicken Sie auf das ADMIN-Icon im oberen rechten Bereich des Browserfensters.

Abb. 79: Benutzer nc_admin

4. Klicken Sie auf das Menü Einstellungen.

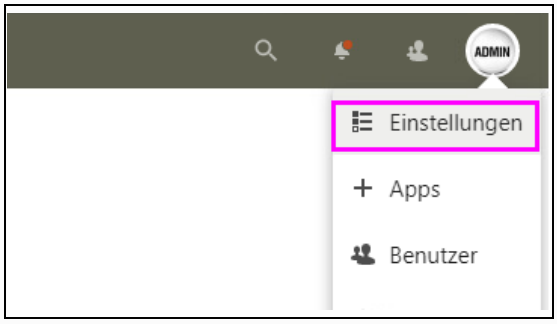


Abb. 80: Benutzer nc_admin > Einstellungen

5. Klicken Sie auf den Link Sicherheit im Navigationsbereich **Persönlich**.

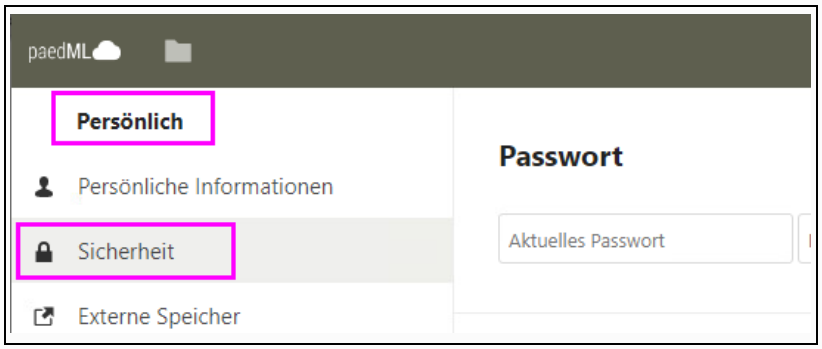


Abb. 81: Benutzer nc_admin > Einstellungen > Sicherheit

6. Geben Sie im ersten **Eingabefeld (1)** `das aktuelle Kennwort` ein. Tippen Sie im **Eingabefeld (2)** `Ihr neues Kennwort` ein. **Das neue Kennwort sollte dabei aus mindestens 8 Zeichen bestehen**. Nextcloud gibt ihnen durch eine Signalfarbe und einen Hinweistext an, ob Ihr Kennwort hinreichend stark ist.
   Klicken Sie auf Passwort ändern **(3)**, um den Vorgang abzuschließen.

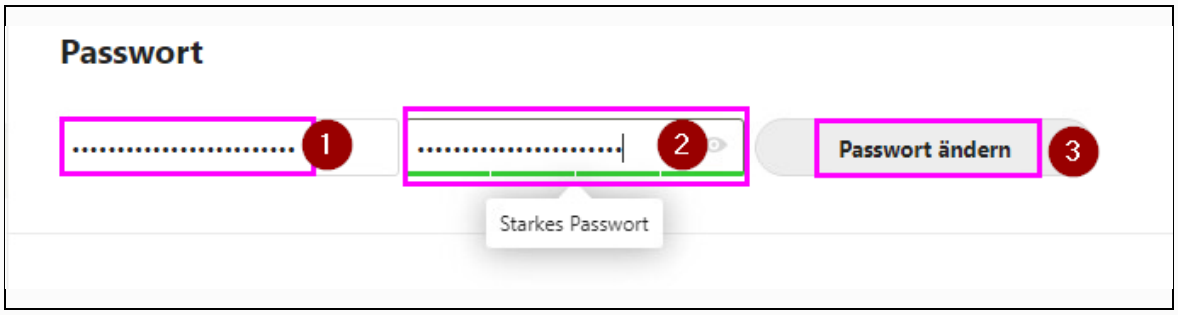


Abb. 82: Benutzer nc_admin > Einstellungen > Sicherheit > Passwort ändern

7.8 Ändern des Kennworts für die Benutzerkonten Administrator und root

Das Skript `lmz-initial-setup` nimmt sowohl für das Benutzerkonto **root** als auch für das Benutzerkonto **Administrator** dasselbe Kennwort auf.

Aus Sicherheitsgründen und im Sinne einer klaren Rollentrennung ist es jedoch sinnvoll, für beide Konten je ein eigenes Kennwort festzulegen.

7.8.1 Benutzer Administrator

1. Öffnen Sie in Ihrem Browser folgende URL: https://nextcloud.paedml.lokal.
2. Klicken Sie auf das Menü-Icon ☰ und anschließend auf das Menü Anmelden.

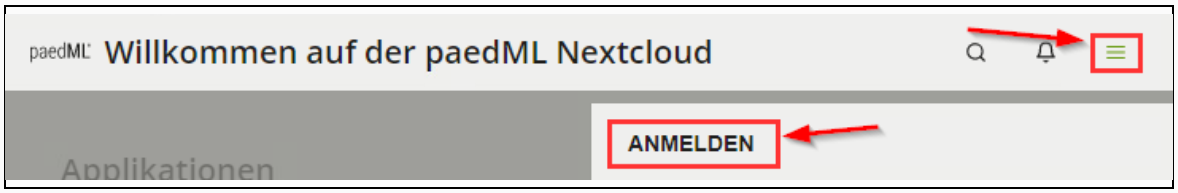


Abb. 83: Anmelden in UMC

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!**

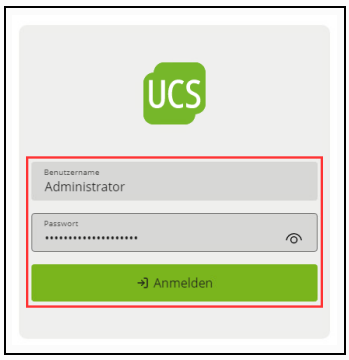


Abb. 84: Anmelden bei paedml.lokal

4. Aktivieren Sie das Kontextmenü, indem auf das Menü-Icon ☰ klicken (1). Klicken Sie auf den Link Benutzereinstellungen (2).

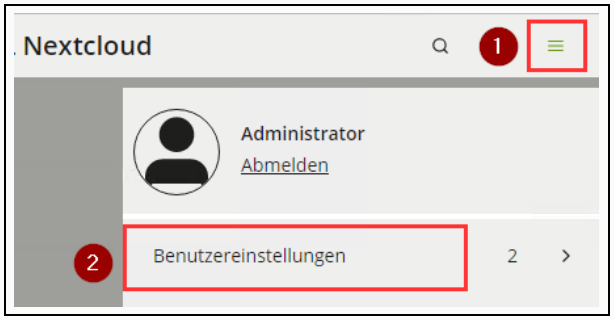


Abb. 85: Benutzereinstellungen

5. Klicken Sie auf die Schaltfläche Ihr Passwort ändern.

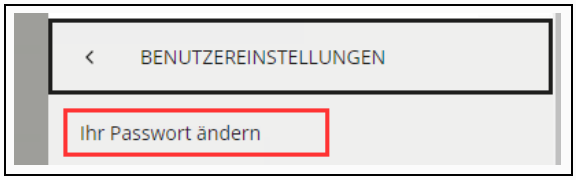


Abb. 86: Ihr Passwort ändern

6. Tippen Sie zunächst ihr aktuelles Kennwort, danach zweimal ihr neues Kennwort ein. Übernehmen Sie die Kennwortänderung, indem Sie auf den Button PASSWORT ÄNDERN klicken.

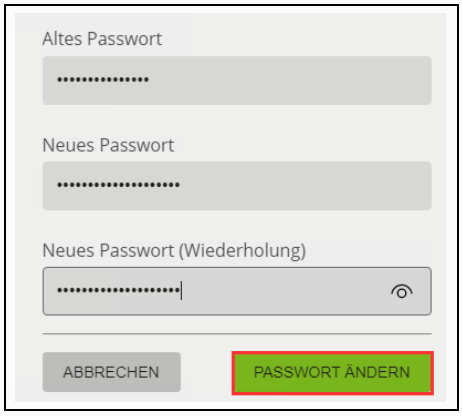


Abb. 87: UMC (Univention Management Console) > Menü > Benutzereinstellungen -> Passwort ändern

7. Melden Sie sich von der UMC ab und wiederholen Sie die Anmeldung mit Ihrem neuen Kennwort.

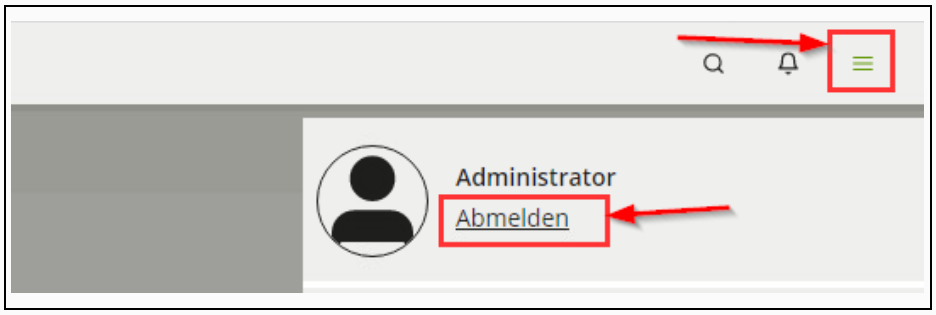


Abb. 88: UMC (Univention Management Console) > Passwort ändern

7.8.2 Benutzer root

Nachfolgend beschreiben wir, wie Sie an der Text-Console des Univention UCS Corporate Server das Kennwort des Benutzerkontos root ändern können.

Sie brauchen dafür die Web-Konsole oder vSphere Remote Console.

1. Melden Sie sich an der Text-Console der Nextcloud-VM als Benutzer **root** an.
2. Führen Sie folgenden Befehl aus:

```
passwd
```

3. Geben Sie ein neues `Passwort` ein und wiederholen Sie es.

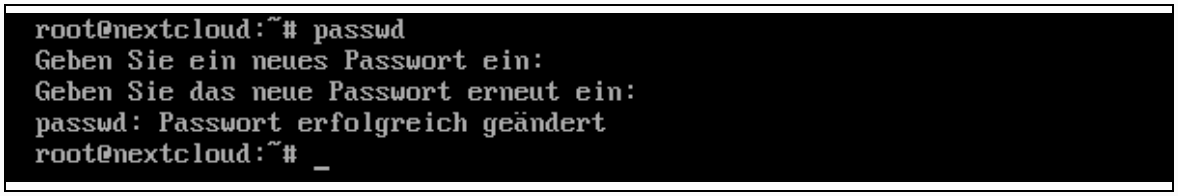


Abb. 89: Kennwort für root ändern

7.9 Snapshot bereinigen, falls vorhanden

Falls Sie vor der Initialisierung der Nextcloud wie im Kapitel 2.3 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 können.

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.

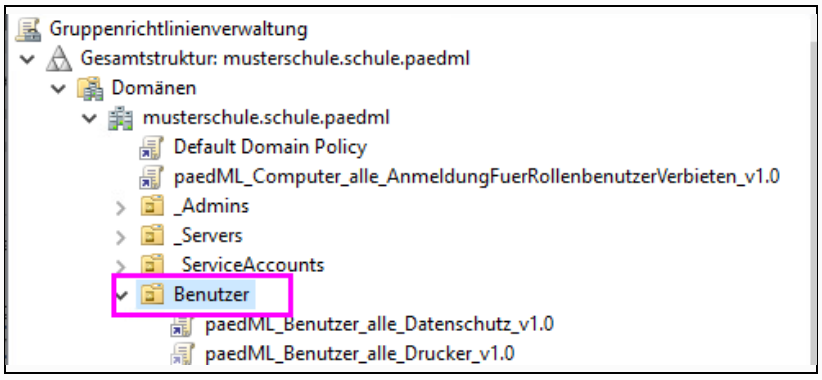


Abb. 90: Gruppenrichtlinienverwaltung -> OU Benutzer

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.

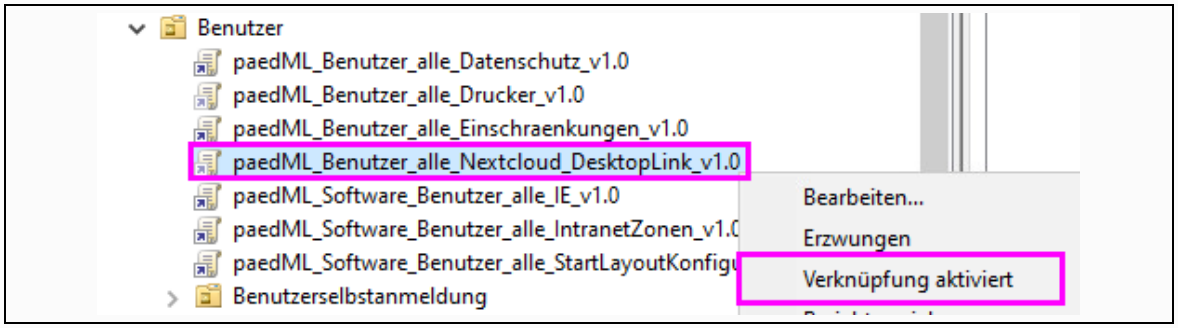


Abb. 91: Verknüpfung für paedML_Benutzer_alle_Nextcloud_DesktopLink_v1.0 deaktivieren

A.3 Externer Domänenname für Host_Nextcloud

Wenn Sie eine externe Domäne für Ihre Nextcloud eingerichtet haben, dann hilft Ihnen die hier beschriebene Ergänzung, um eine bessere Antwortzeit zu erzielen, wenn der Zugriff auf Ihre Nextcloud aus dem Schulnetz über die externe Domäne erfolgt, zum Beispiel https://cloud.meine-schule.de/nextcloud.

Löst man aus dem Schulnetz heraus den FQDN Ihrer Nextcloud, dann erhalten Sie als IP-Adresse die IP-Adresse, die im DNS-Server Ihres Providers hinterlegt wurde. (In der Regel dürfte sie die externe IP-Adresse Ihrer Firewall bzw. Ihres Routers sein)

Abb. 92: Externen FQDN der Nextcloud aufgelöst im Schulnetz

Viel besser wäre es jedoch, wenn der Name aus dem Schulnetz heraus mit der im Schulnetz bekannten IP-Adresse der Nextcloud, nämlich 192.168.201.7, aufgelöst wird.

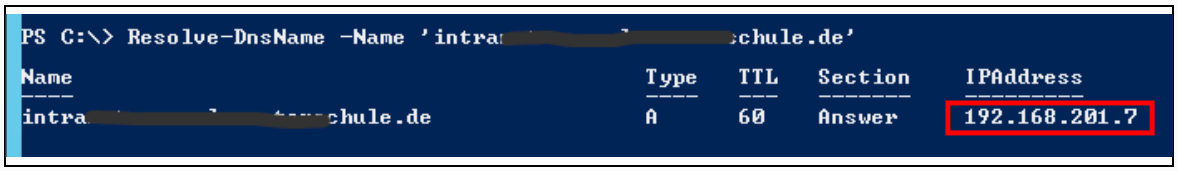


Abb. 93: Bevorzugte Auflösung des externen FQDN der Nextcloud im Schulnetz

1. Öffnen Sie im Browser WebAdmin und melden Sie sich als Benutzer **admin** an.
2. Klicken Sie auf das Menü Definitionen & Benutzer und anschließend auf den Link Netzwerkdefinitionen.

Abb. 94: WebAdmin -> Definitionen & Benutzer -> Netzwerkdefinitionen

3. Tippen Sie im Suchfeld `host_nextcloud` ein und klicken Sie auf Finden (1). Öffnen Sie die Eigenschaften der Netzwerkdefinition **Host_Nextcloud** mit Bearbeiten (2).

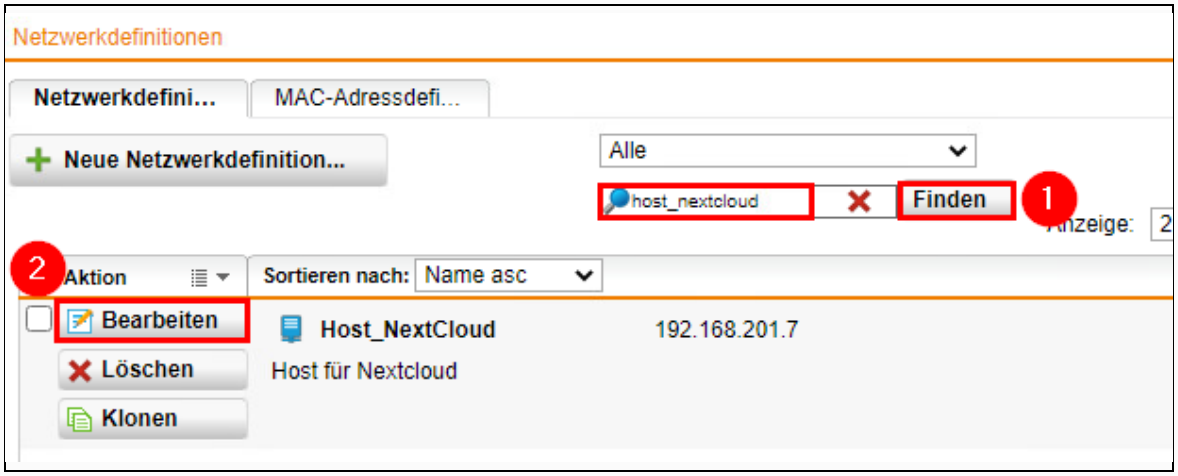


Abb. 95: Host_Nextcloud bearbeiten

4. Tragen Sie in das Eingabefeld **Hostname** den `externen Domänennamen Ihrer Nextcloud` ein und klicken Sie auf Speichern.

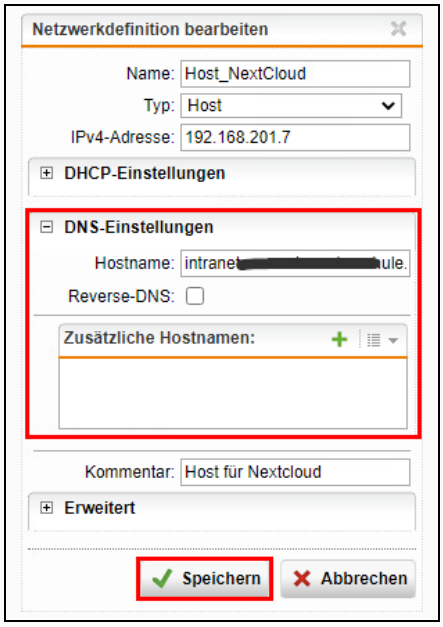


Abb. 96: DNS-Einstellungen -> Hostname eintragen

5. Laden Sie die aktuelle Seite neu.

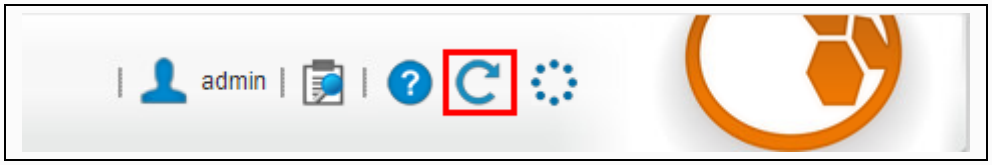


Abb. 97: Seite neu laden

6. Melden Sie sich auf dem Server **DC01** als Domänen-Admin an.
7. Öffnen Sie die Konsole **DNS-Manager**.

8. Klicken Sie mit der rechten Maustaste auf das Serverobjekt DC01 und wählen Sie Eigenschaften aus dem Kontextmenü aus.

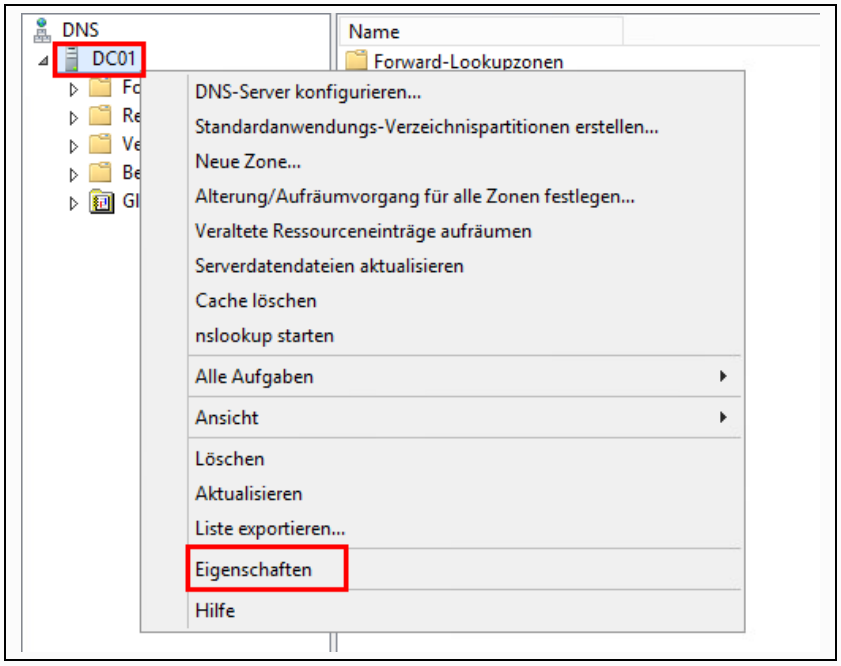


Abb. 98: DNS-Manager -> DC01 -> Eigenschaften

9. Öffnen Sie die Registerkarte Weiterleitungen. Falls die IP-Adresse Ihrer Sophos darin nicht aufgelistet wird, dann fügen Sie sie hinzu und setzen Sie sie in der Reihenfolge an die erste Stelle.

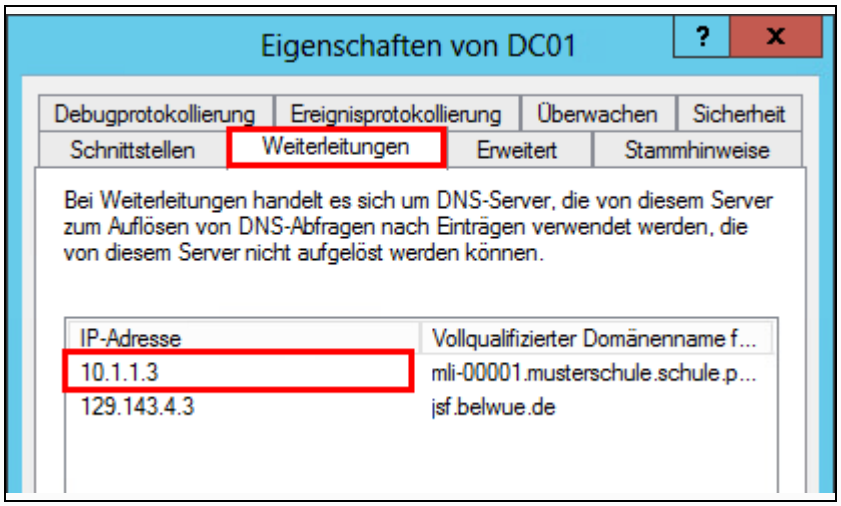


Abb. 99: DNS-Manager -> DC01 -> Weiterleitungen

10. Speichern Sie die Änderung mit OK.

Haben Sie Geduld. Es kann sein, dass es eine Weile dauert, bis eine erneute Namensauflösung die gewünschte IP-Adresse zurückgibt.

A.4 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 stattdessen die URL mit dem externen Domänennamen Ihrer Nextcloud als Desktopverknüpfung bereitstellen wollen, bearbeiten Sie das GPO wie folgt.

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

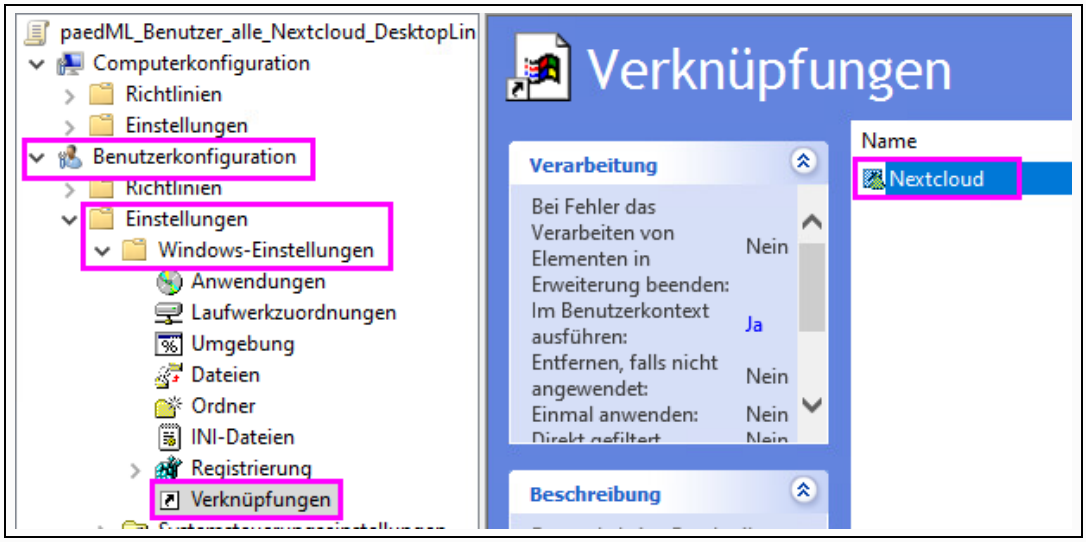


Abb. 100: Benutzerkonfiguration -> Einstellungen -> Windows-Einstellungen -> Verknüpfungen

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

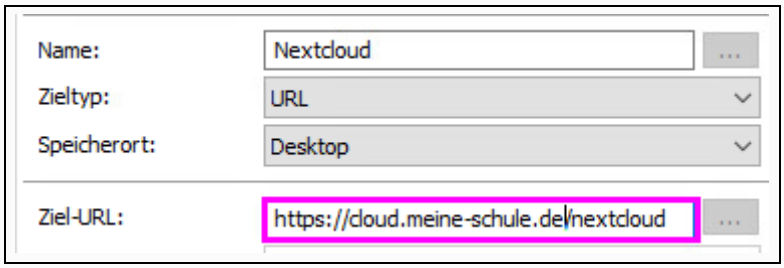


Abb. 101: Ziel-URL auf externen FQDN ändern

A.5 Lizenzcode eingeben

Wie im Kapitel 1.7 Lizenzierung (ab 500 Benutzer) vermerkt benötigen Sie einen Lizenzcode, ab 500 Benutzer. Kunden der paedML Windows erhalten einen kostenfreien Lizenzcode nach einer Anfrage an die paedML Windows-Hotline. Nachfolgend finden Sie eine Anleitung, wie Sie den Lizenzcode eingeben können.

1. Öffnen Sie in einem Browser die Nextcloud (https://nextcloud.paedml.lokal).
2. Melden Sie sich als Benutzer **nc_admin** an.
3. Klicken Sie auf das ADMIN-Icon im oberen rechten Bereich des Browserfensters.

Abb. 102: Benutzer nc_admin

4. Klicken Sie auf das Menü Apps.

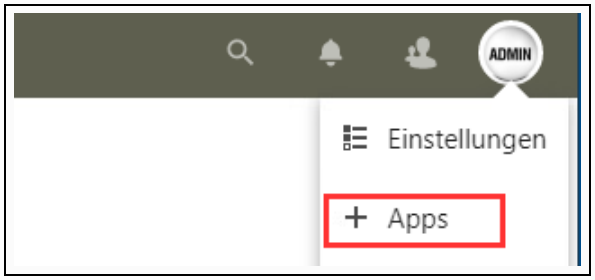


Abb. 103: Nextcloud Apps

5. Aktivieren Sie das Eingabefeld für die Suche und tippen Sie `support` ein.

Abb. 104: Apps suchen

6. Klicken Sie bei der App **Support** auf den Button Aktvieren.

Abb. 105: Support App aktivieren

7. Die Aktivierung der Support App muss durch den Administrator **nc_admin** bestätigt werden, indem Sie Ihr Kennwort eintippen und auf den Button Bestätigen klicken.

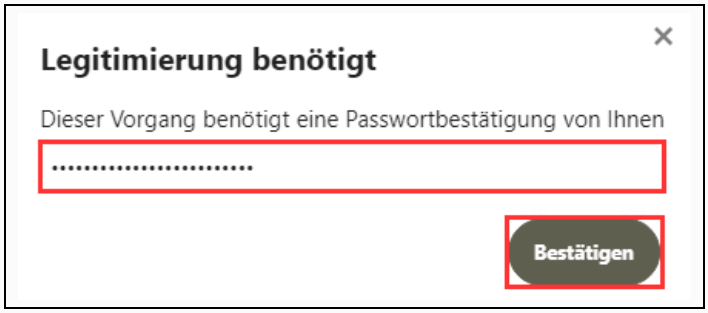


Abb. 106: Aktivierung der Support App bestätigen

8. Öffnen Sie anschließend die Seite Einstellungen.

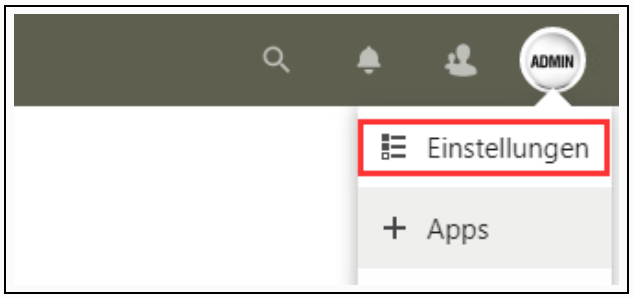


Abb. 107: Menü Einstellungen

9. Klicken Sie auf den Link Support unter der Rubrik Verwaltung.

Abb. 108: Einstellungen -> Verwaltung -> Support

10. Tippen Sie Ihren Lizenzcode ein und klicken Sie auf den Button Abonnements-Schlüssel eingeben.

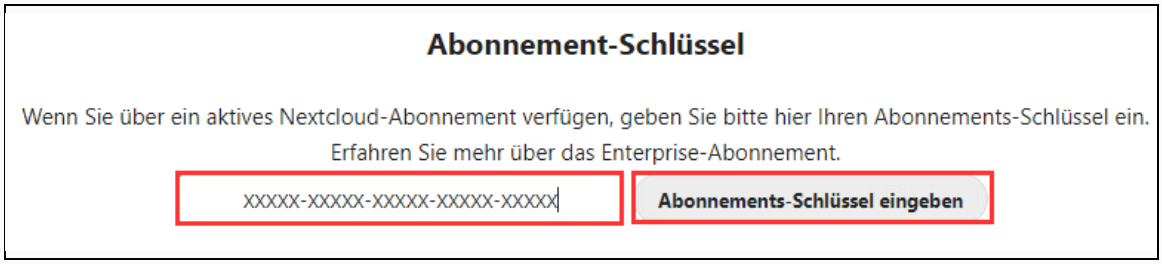


Abb. 109: Abonnement-Schlüssel

Anhang B FAQ

B.1 Troubleshooting: Sophos SG UTM

B.1.1 Wie kann ich prüfen, ob der Netzwerkadapter 4 meiner Nextcloud-VM tatsächlich als eth3 eingebunden wird?

Über die Eigenschaften des **Netzwerkadapter 4** können Sie die MAC-Adresse des Netzwerkadapters einsehen.

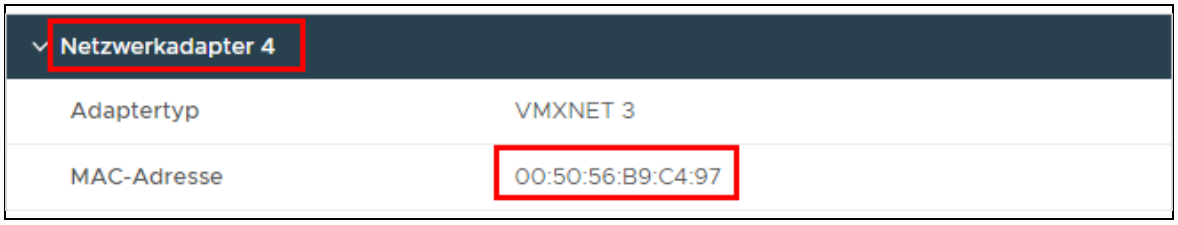


Abb. 110: MAC-Adresse des Netzwerkadapter 4

Öffnen Sie in WebAdmin die Seite **Schnittstellen → Hardware** und vergleichen Sie die MAC-Adresse der Hardware **eth3** mit der MAC-Adresse des Netzwerkadapters 4.

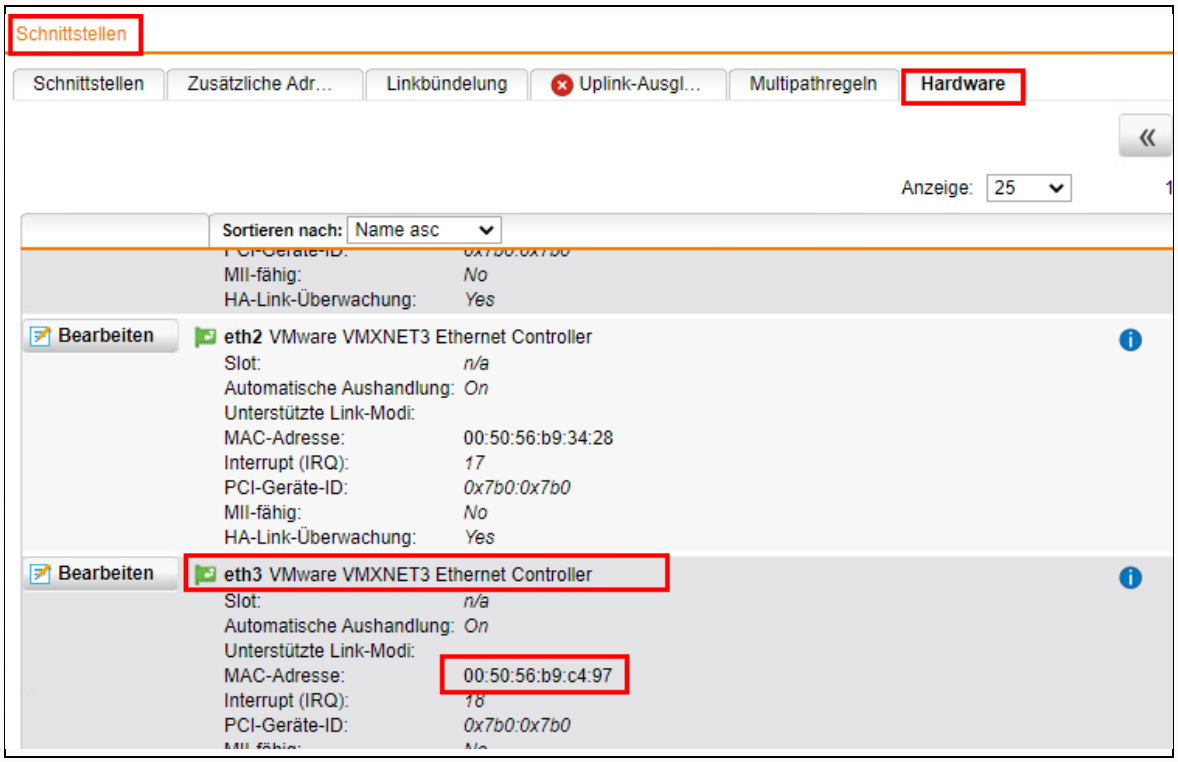


Abb. 111: MAC-Adresse der Netzwerkhardware eth3

Falls sich die beiden MAC-Adressen voneinander unterscheiden, dann müssen Sie die Schnittstellenzuordnung entsprechend anpassen. Suchen Sie auf der Seite Hardware nach derjenigen Hardware , welche die gesuchte MAC-Adresse besitzt. Notieren Sie den Hardwarenamen, z.B. eth4.

Wechseln Sie zur Registerkarte Schnittstellen und bearbeiten Sie die Schnittstelle **paedML_DMZ**. Ändern Sie die Hardware von eth3 auf die zuvor identifizierte Hardware und übernehmen Sie die Änderung mit Speichern.

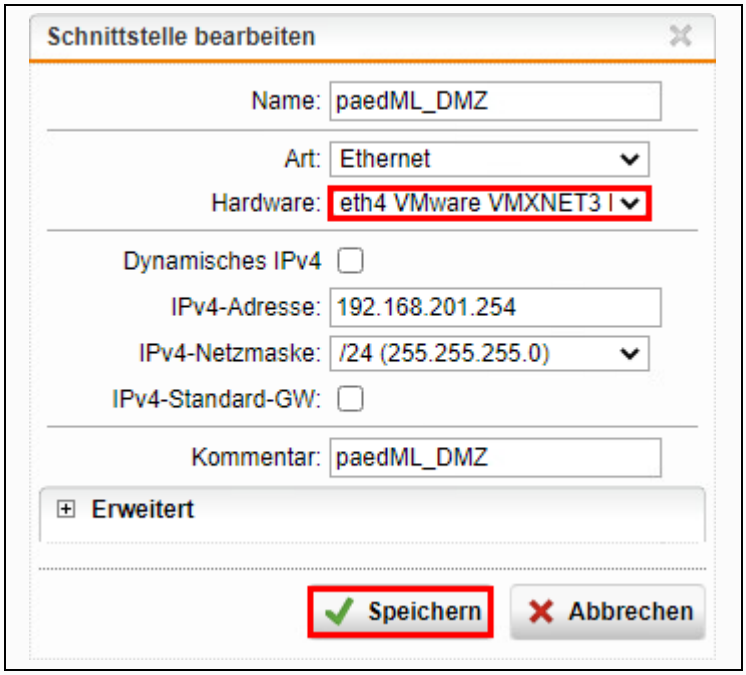


Abb. 112: Hardwareänderung der Schnittstelle paedML_DMZ

B.2 Reverse-Proxy für Nextcloud einrichten

Wie im Kapitel 3.5 NAT-Regeln bearbeiten (Optional) genannt, stellen wir an dieser Stelle lediglich eine Beispielkonfiguration vor.

Sie kann funktionieren, muss aber nicht. Das gilt insbesondere dann, wenn der Zugriff auf Nextcloud von Apps erfolgt beziehungsweise welche Nextcloud-Apps Sie zusätzlich installiert und aktiviert haben. Eine technische Unterstützung erhalten Sie deshalb für dieses Beispiel nicht.

Um die Nextcloud per Reverse-Proxy aus dem Internet erreichen zu können, müssen Sie die beiden DNAT-Regeln aus dem Kapitel 3.5 NAT-Regeln bearbeiten (Optional) deaktivieren.

Sie brauchen zunächst ein Zertifikat, bevor Sie den Reverse-Proxy für Nextcloud einrichten. Für dieses Beispiel importieren wir ein Let's Encrypt Zertifikat.

Öffnen Sie in WebAdmin die Seite Webserver Protection → Zertifikatverwaltung.

Abb. 113: WebAdmin -> Webserver Protection -> Zertifikatverwaltung

Klicken Sie auf die Registerkarte Erweitert.

Abb. 114: WAF -> Zertifikatverwaltung -> Erweitert

Aktivieren Sie die Option **Let's Encrypt Zertifikat zulassen** und speichern Sie sie mit Übernehmen.

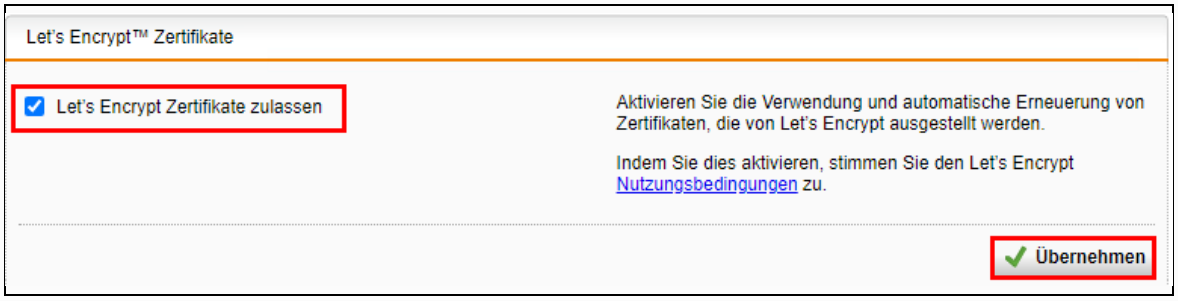


Abb. 115: Let's Encrypt Zertifikate zulassen

Wechseln Sie auf die Registerkarte Zertifikate und klicken Sie auf den Button Neues Zertifikat.

Abb. 116: WAF -> Zertifikatverwaltung -> Zertifikate

Geben Sie dem neuen Zertifikat einen aussagekräftigen Namen und übernehmen Sie die Werte aus der nachfolgenden Abbildung. Als Domäne müssen Sie Ihre eigene externe Domäne hinzufügen. Schließen Sie den Vorgang mit Speichern ab.

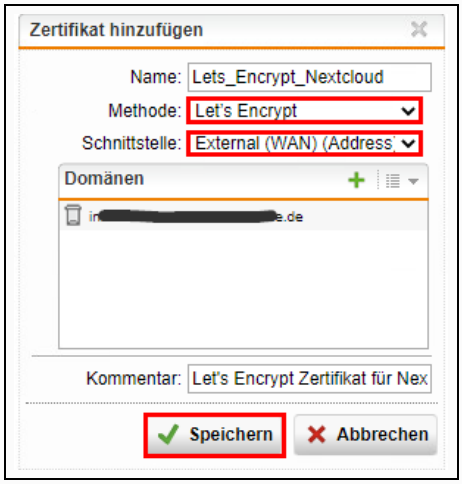


Abb. 117: Zertifikat hinzufügen

Nach dem Speichern wird das neue Zertifikat in der Tabelle aufgelistet. Es dauert eine Weile, bis das Zertifikat erfolgreich generiert und importiert wurde.

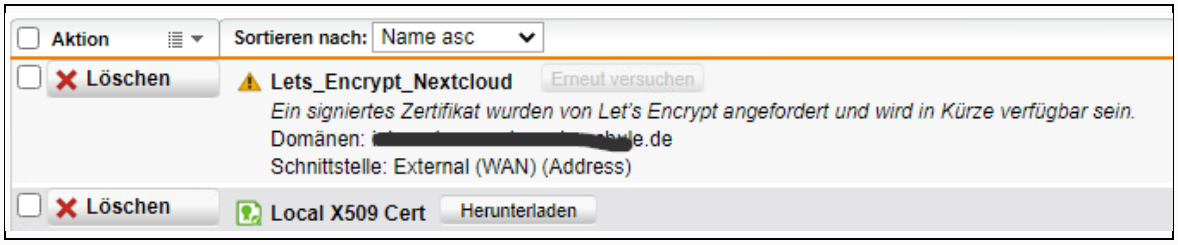


Abb. 118: Let's Encrypt Zertifikat

War der Vorgang insgesamt erfolgreich, ändert sich der Status des Zertifikats wie folgt:

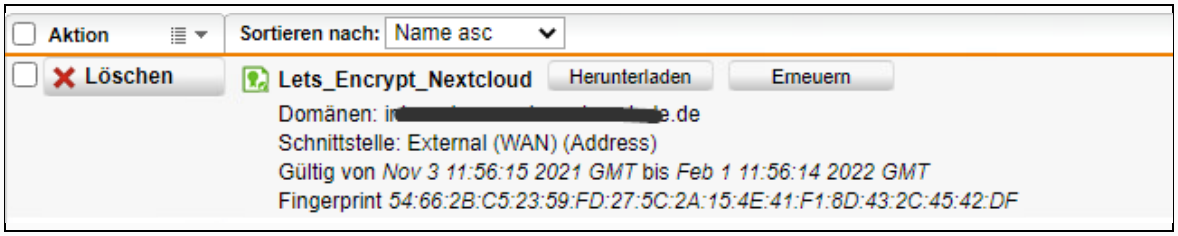


Abb. 119: Let's Encrypt Zertifikaterfolgreich importiert

Tipp: Falls der Vorgang nicht erfolgreich abgeschlossen werden kann, schauen Sie am besten in der Log-Datei Let's Encrypt nach. Darin finden Sie Hinweise, weswegen die Aktion fehlgeschlagen ist.

Das Protokoll finden Sie auf der Seite Protokolle & Berichte → Protokollansicht.

Als Nächstes müssen Sie **einen echten und einen virtuellen Webserver** mit dem Ziel **Host_NextCloud** einrichten.

Öffnen Sie in WebAdmin die Seite Webserver Protection → Web Application Firewall.

Abb. 120: WebAdmin -> Webserver Protection -> Web Application Firewall (WAF)

Klicken Sie auf die Registerkarte Echte Webserver und anschließend auf den Button Neuer echter Webserver.

Abb. 121: WAF -> Echte Webserver

Fügen Sie einen neuen echten Webserver wie folgt hinzu.

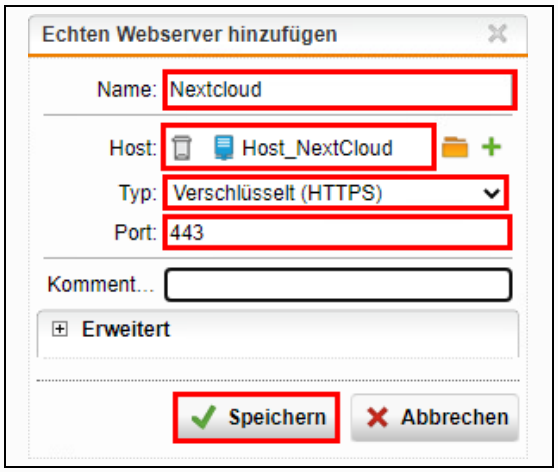


Abb. 122: WAF -> Echten Webserver hinzufügen

Fügen Sie nun auf der Registerkarte Virtuelle Webserver einen neuen virtuellen Webserver hinzu.

Abb. 123: WAF -> Virtuelle Webserver

Der neue virtuelle Webserver sollte wie folgt konfiguriert sein.

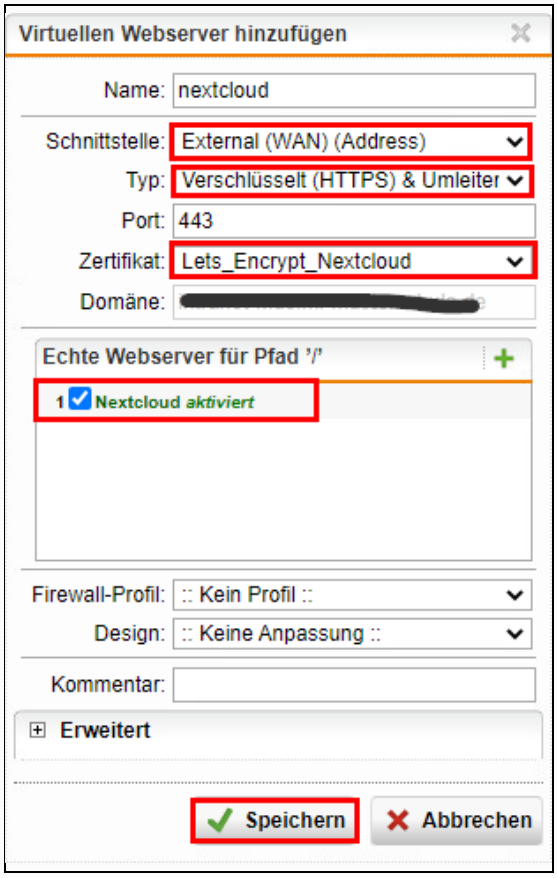


Abb. 124: Virtuellen Webserver hinzufügen

Zu diesem Zeitpunkt stehen nur bekannte Standard Firewall-Profile zur Auswahl zur Verfügung. Da sie bedingt für die Nextcloud geeignet sind, wird ein passendes Firewall-Profil in den nachfolgenden Schritten erstellt.

Vorher fügen Sie jedoch eine sog. **Site-Path-Route** hinzu. Klicken Sie dazu auf die Registerkarte Site-Path-Routing. Sie sehen darin bereits eine Site-Path-Route für den virtuellen Webserver Nextcloud. Klicken Sie auf Bearbeiten.

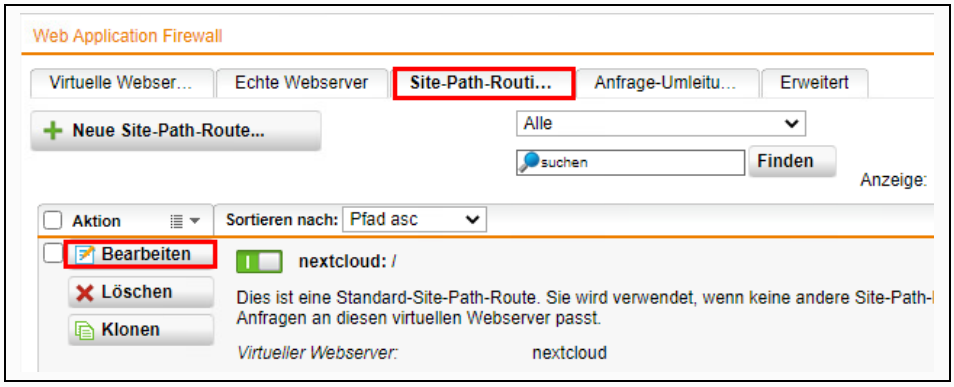


Abb. 125: Site-Path-Route Nextcloud

Ändern Sie den Pfad von `/` auf `/nextcloud` um und übernehmen Sie die Änderung mit Speichern.

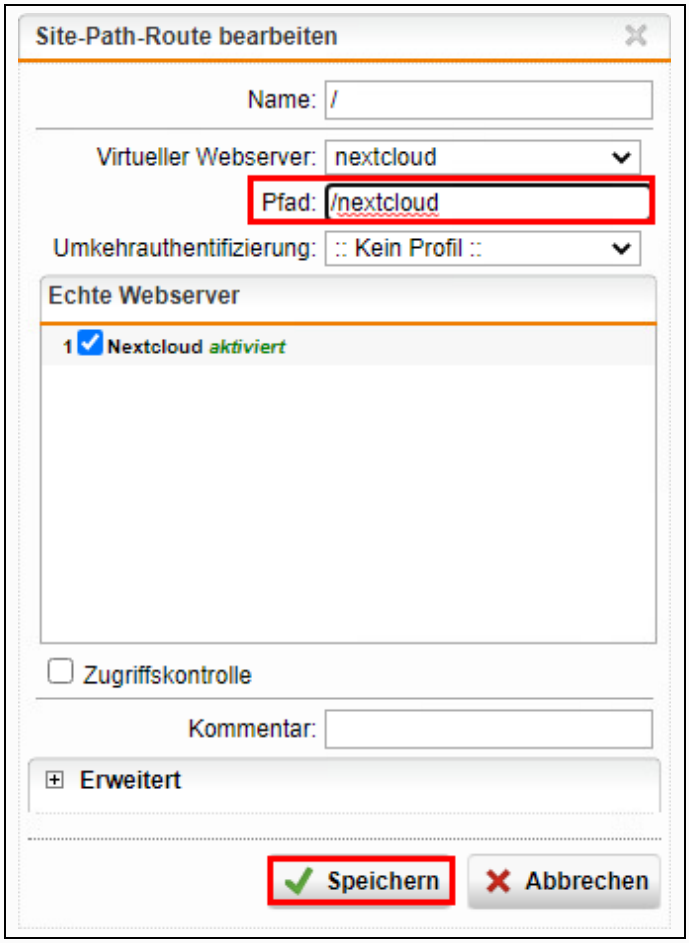


Abb. 126: Site-Path-Route bearbeiten

Wechseln Sie nun auf die Seite Firewall-Profile.

Abb. 127: Webserver Protection -> Firewall-Profile

Klicken Sie auf den Button Neues Firewall-Profil.

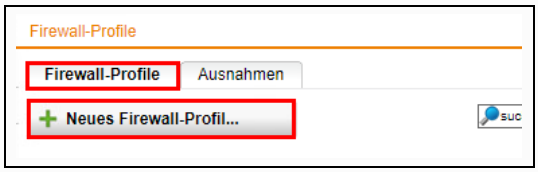


Abb. 128: Neues Firewall-Profil

In der Nachfolgenden Abbildung finden Sie eine Beispielkonfiguration, die Ihnen als Vorlage dient. Ob und welche Optionen Sie aktivieren wollen, hängt maßgeblich von Ihrem eigenen Bedürfnis ab. Das gilt insbesondere die Scan-Funktion der über die Nextcloud transportierten Dateien (Down- und Upload).

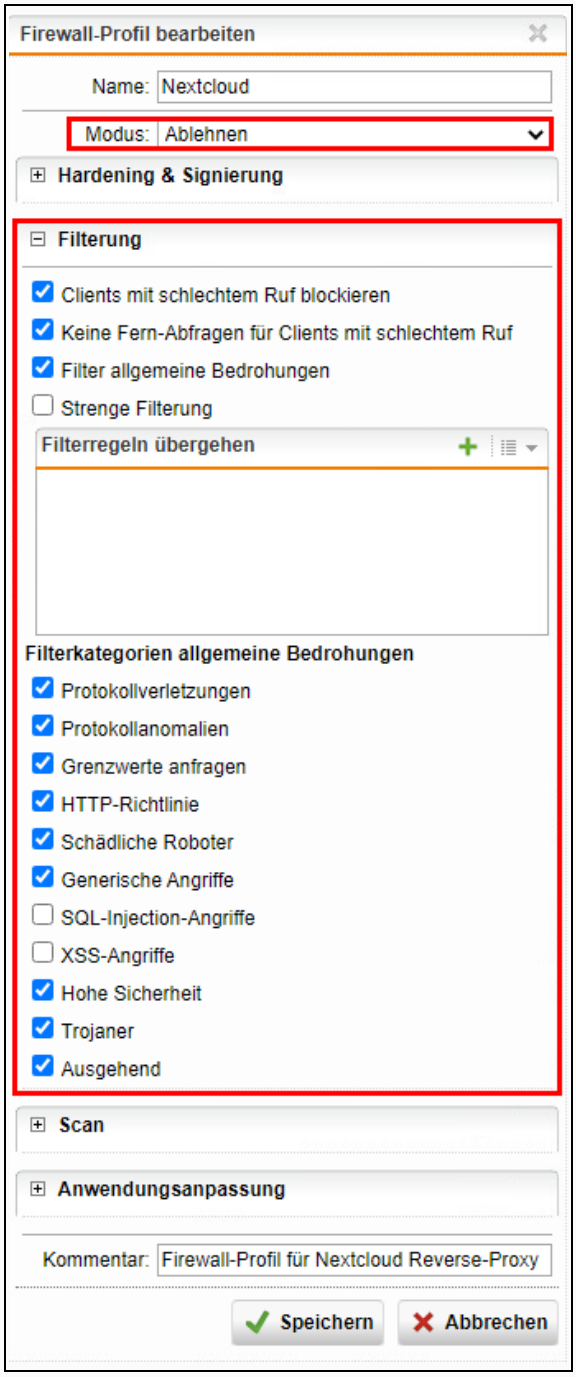


Abb. 129: Ein Beispiel für ein neues Firewall-Profil

Das Feld **Filterregeln übergehen** ist in diesem Beispiel bewusst (noch) nicht befüllt worden. **Denn Sie müssen diese Ausnahmeregeln durch Analyse der Firewall-Berichte selbst herausfinden.**

Speichern Sie das neue Firewall-Profil. Kehren Sie auf die Seite Virtuelle Webserver zurück und bearbeiten Sie den virtuellen Webserver für die Nextcloud.

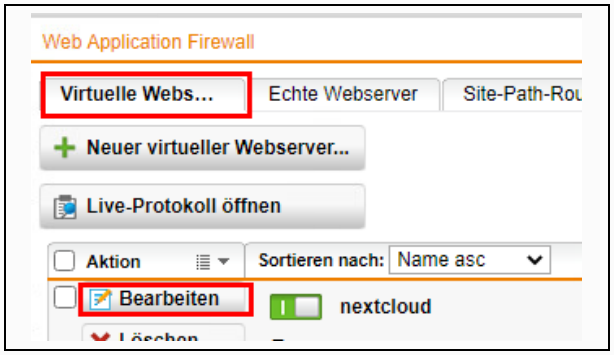


Abb. 130: Virtuellen Webserver Nextcloud bearbeiten

Wählen Sie als Firewall-Profil das oben hinzugefügte neue Profil aus und klicken Sie auf Speichern.

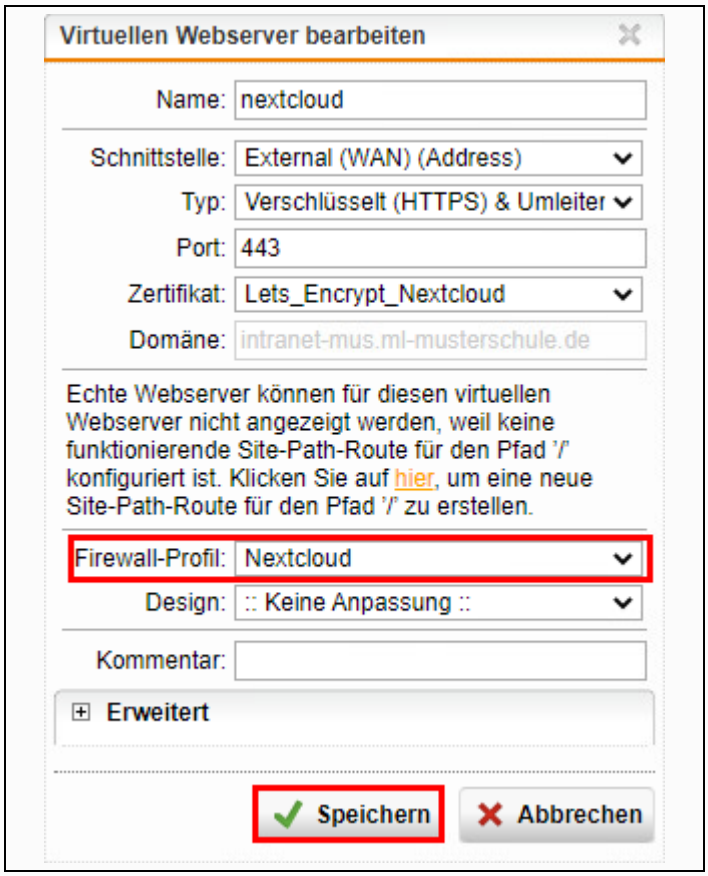


Abb. 131: Firewall-Profil auswählen

Lassen Sie sich von dem Hinweis *„Echte Webserver können … hier nicht angezeigt werden…“* nicht irritieren, da wir für dieses Beispiel bewusst die Site-Path-Route eingeschränkt haben.

Denn: Wenn der Pfad „/“ aktiv ist, dann gelangen Sie aus dem Internet auf die Seite Univention Management Console (UMC) Ihrer Nextcloud-VM. Da UMC mit Reverse-Proxy jedoch nicht funktioniert, ist es besser, die UMC durch die Einschränkung der Site-Path-Route auszublenden, um Ihre Benutzer nicht zu verunsichern.

Öffnen Sie Nextcloud über Ihre externe Domäne, z.B. https://cloud.meine-schule.de/nextcloud, aus unterschiedlichen Apps – Browser, iOS-App, Android-App usw. Melden Sie sich an und kontrollieren Sie, ob sie funktioniert.

Falls Sie WebAdmin bereits geschlossen haben, öffnen Sie ihn wieder und navigieren Sie auf die Seite Protokolle & Berichte → Webserver Protection.

Abb. 132: Protokolle & Berichte -> Webserver Protection

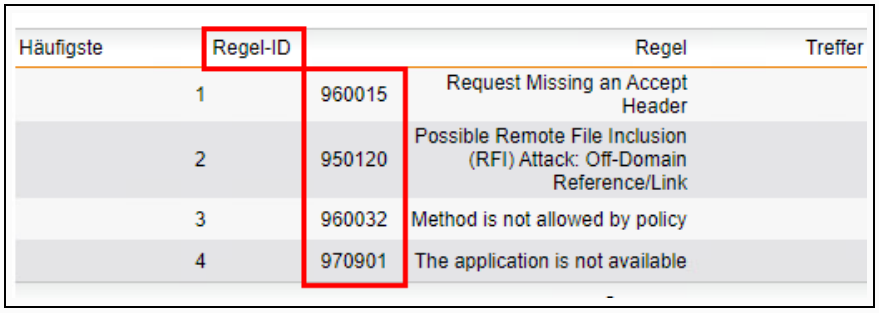
Wechseln Sie auf die Registerkarte Details.

Abb. 133: Protokolle & Berichte -> Webserver Protection

Ändern Sie die Filtereinstellung wie in der nachfolgenden Abbildung dargestellt und klicken Sie auf Aktualisieren.

Abb. 134: Protokolle & Berichte -> Webserver Protection gefiltert nach häufigsten Regeln

Sie erhalten nun eine Zusammenfassung der Regeln, die durch Firewall-Profil behandelt wurden. Notieren Sie die Regel-IDs.



Häufigste	Regel-ID	Regel	Treffer
1	960015	Request Missing an Accept Header	
2	950120	Possible Remote File Inclusion (RFI) Attack: Off-Domain Reference/Link	
3	960032	Method is not allowed by policy	
4	970901	The application is not available	

Abb. 135: Zusammenfassung der von Firewall-Profil behandelten Regeln

Fügen Sie diese Regel-IDs in Ihr für Nextcloud aktives Firewall-Profil hinzu und speichern Sie die Änderung.

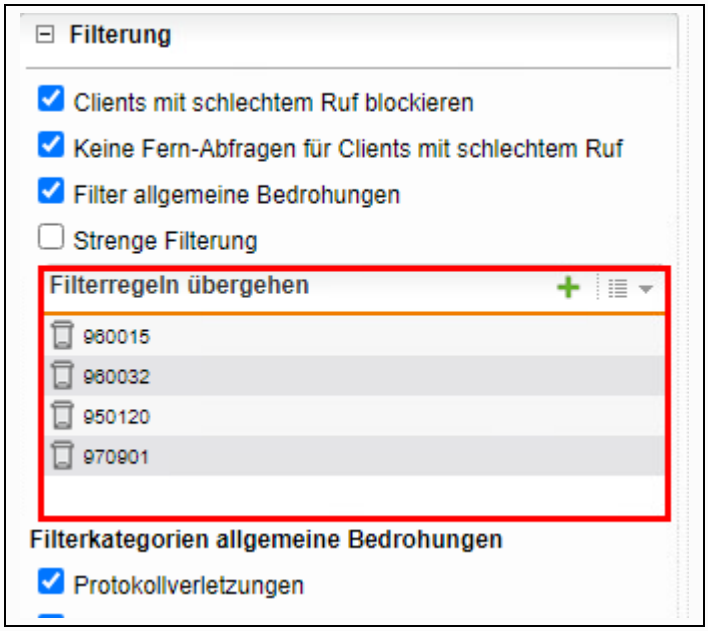


Abb. 136: Zusammenfassung der von Firewall-Profil behandelten Regeln

Mit diesem Beispiel haben wir Ihnen gezeigt, wie Sie einen Reverse-Proxy für die Nextcloud selbst einrichten können.

Sollten Sie auf Störungen stoßen, lesen Sie zuerst in dem Firewall-Bericht nach, ob zusätzliche Regeln aufgelistet werden, die in der Liste **Firewallregeln übergehen** noch fehlen. Falls ja, nehmen Sie sie in die Liste auf.

Außerdem gibt es weitere Protokolle und Berichte, die Sie zur Störungsbehebung heranziehen können. Welche es sind erfahren Sie zum Beispiel in der eingebauten Hilfe der Sophos SG UTM.

B.3 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:

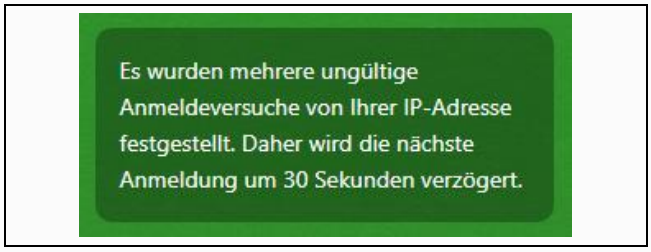


Abb. 137: Nextcloud Bruteforce Protection

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 den folgenden Befehl in einer Zeile aus:

```
nccmd security:bruteforce: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 wäre eine gute Alternative.

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.

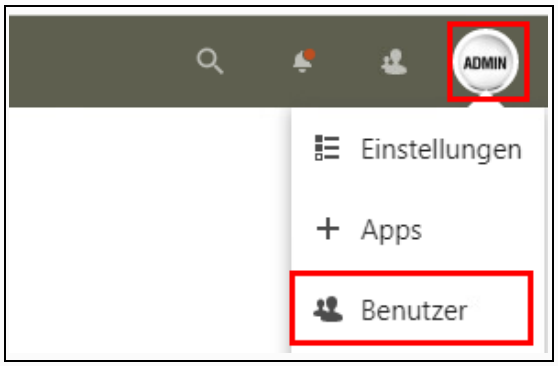


Abb. 138: Benutzer nc_admin > Benutzer

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

Abb. 139: 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.

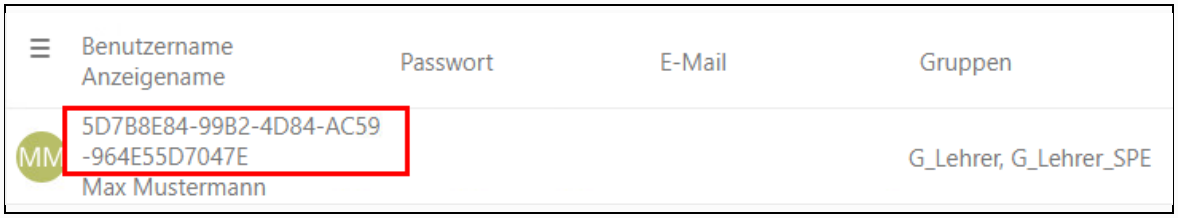


Abb. 140: Zusammenfassung der von Firewall-Profil behandelten Regeln

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

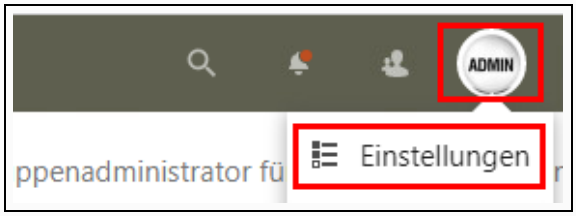


Abb. 141: Benutzer nc_admin > Einstellungen

Klicken Sie auf Protokollierung.

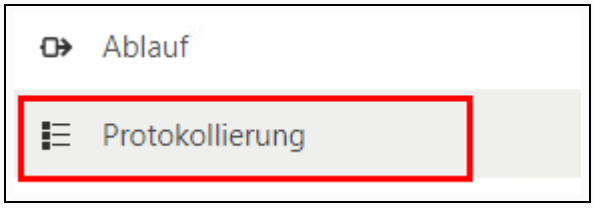


Abb. 142: Verwaltung -> Protokollierung

Klicken Sie auf das Menü-Icon ○○○.

Abb. 143: Verwaltung -> Protokollierung

Laden Sie die Log-Datei über Download logs herunter.

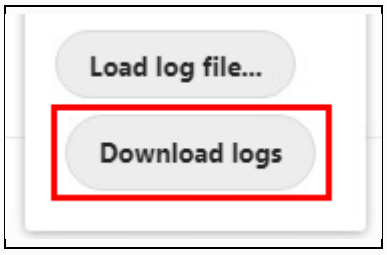


Abb. 144: Verwaltung -> Protokollierung -> Download logs

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.

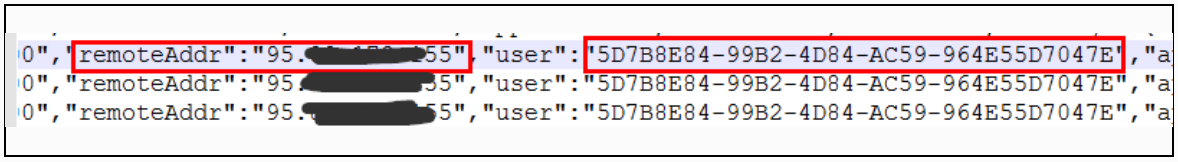


Abb. 145: Zusammenfassung der von Firewall-Profil behandelten Regeln

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

```
nccmd security:bruteforce:reset "{IP-Adresse}"
```

B.4 Quota-Einschränkung für Benutzer nc_admin aufheben

Die Quota-Einschränkung aus dem Kapitel 7.4 Quota für alle Benutzer 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.

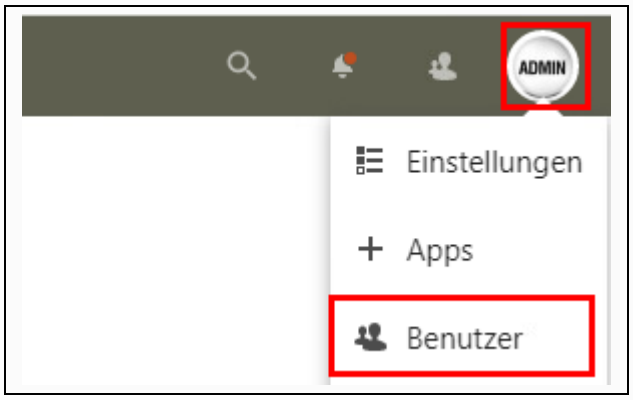


Abb. 146: Benutzer nc_admin > Benutzer

Klicken Sie auf den Link Administratoren.

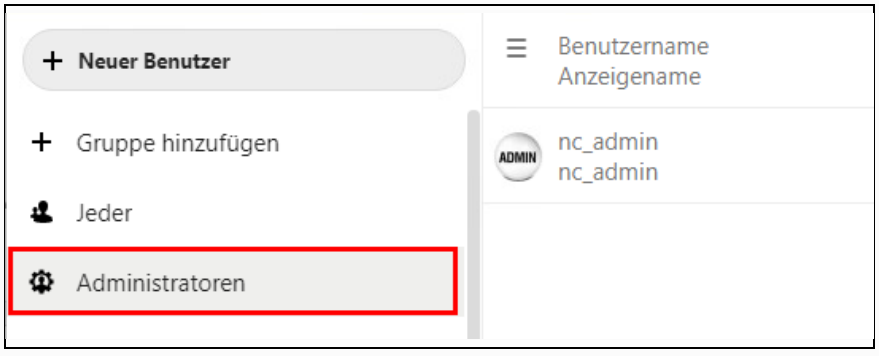


Abb. 147: Benutzerverwaltung -> Administratoren

Diese Seite enthält Spalten, die auf den ersten Blick nicht zu sehen sind, wenn Ihre Monitorauflösung geringer als 1280 Punkte in der Breite beträgt. 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.

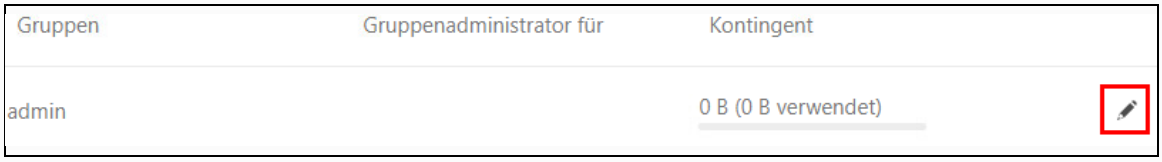


Abb. 148: Benutzerverwaltung -> Administratoren -> Bearbeiten

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. 149: Benutzerverwaltung -> Administratoren -> Kontingent festlegen

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

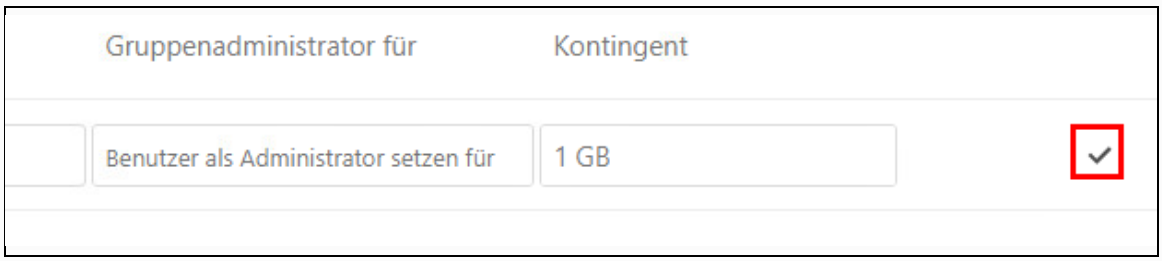


Abb. 150: Benutzerverwaltung -> Administratoren -> Bearbeiten

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 meldet das Diagnose-Modul des UCS eine kritische Warnmeldung. Auf der Univention Management Console (UMC) sehen Sie in diesem Fall die folgende Diagnose:

Abb. 151: Zertifikate (Lokaler Computer) -> Eigene Zertifikate -> Vertrauenswürdige Stammzertifizierungsstelle

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

B.5.2 Warum muss eine Port-Umleitung auf HTTP eingerichtet werden?

Eine Port-Umleitung für das Protokoll HTTP ist dann notwendig, wenn Sie Ihre Nextcloud mit einem von Let's Encrypt ausgestellten Zertifikat einrichten wollen. Das Skript von UCS verwendet dabei die sog. „HTTP-01 Challenge"-Methode, um die Domänenkonfiguration erfolgreich zu prüfen. Diese Prüfung kann bei dieser Methode nur auf dem Port 80 gelingen. (Siehe auch https://letsencrypt.org/docs/challenge-types/)

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
```

Abb. 152: /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 er den meisten Windows-Benutzern eher vertraut erscheinen dürfte.

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

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

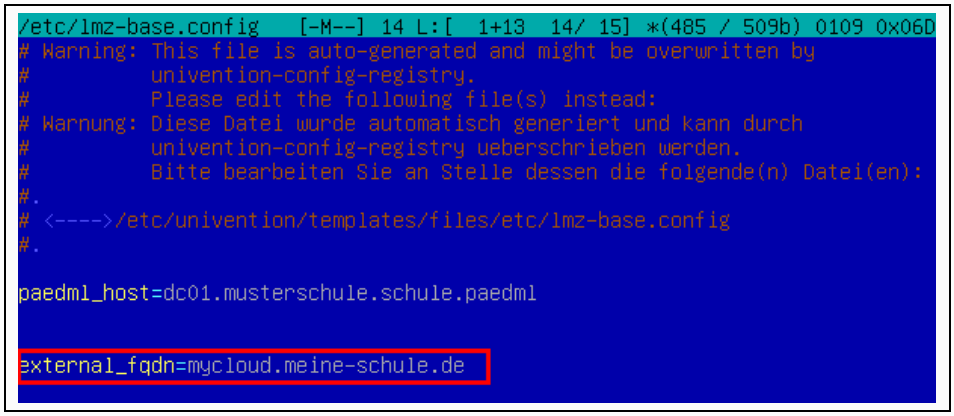


Abb. 153: Korrektur von external_fqdn

Beenden Sie `mcedit` mit F10-Taste.

Führen Sie anschließend den nachfolgenden Befehl auf der Konsole in einer Zeile aus:

```
nccmd config:system:get trusted_domains
```

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

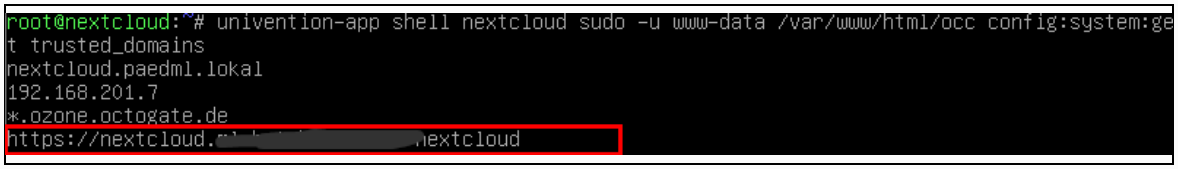


Abb. 154: Fehlerhafter Wert in trusted_domains gefunden

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

```
nccmd config: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):

```
nccmd config:system:set trusted_domains 3 -value="mycloud.meine-schule.de"
```

Kontrollieren Sie das Ergebnis mit dem Befehl:

```
nccmd config: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 Meine externe Domäne wurde geändert. Was muss ich tun?

Führen Sie alle Schritte, die im Anhang B.5.3 beschrieben werden, durch.

Anhang C Übersicht der Firewall-Regeln am Beispiel von Sophos SG UTM

Hier finden Sie eine Übersicht aller Firewall-Regeln, die für einen störungsfreien Betrieb der Nextcloud sorgen.

- **Host_NextCloud → DC01 – LDAP(S)**

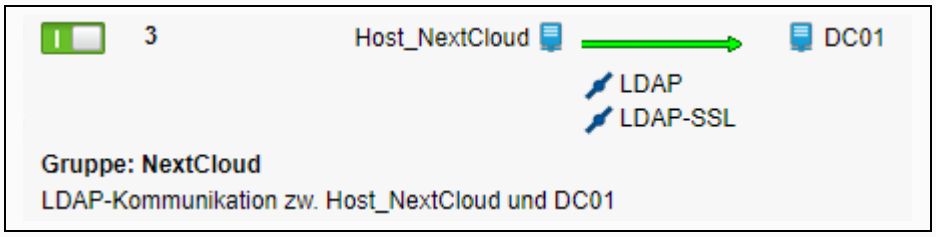


Abb. 155: Gruppe: NextCloud, LDAP zwischen Host_NextCloud und DC01

LDAP(S) wird von einem Nextcloud-Host zwingend benötigt, um Benutzer in AD finden und authentifizieren zu können. **Es handelt sich demnach um eine verbindliche Firewall-Regel, die aktiviert sein muss, sobald ein Nextcloud-Host im Netzwerk DMZ in Betrieb genommen wird**.

- **Host_NextCloud → DC01 – weitere Protokolle**

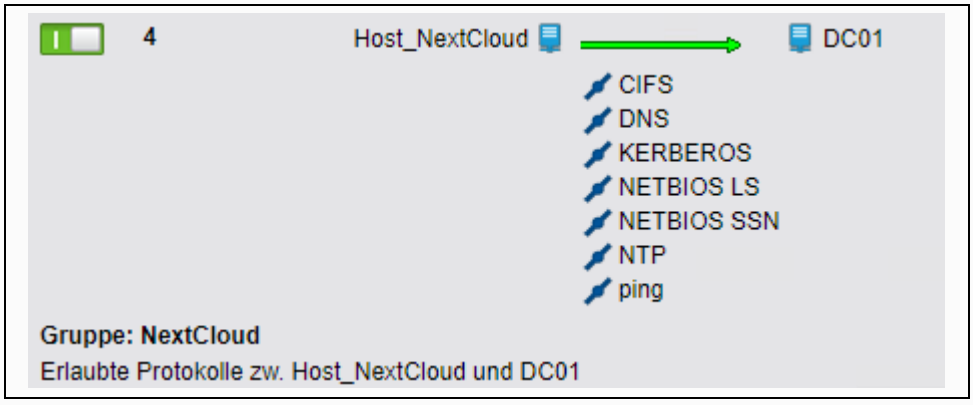


Abb. 156: Gruppe: NextCloud, weitere Protokolle zwischen Host_NextCloud und DC01

Diese Regel beinhaltet weitere erlaubte Protokolle, über Host_NextCloud mit DC01 kommunizieren darf. Es muss zusätzlich wie im Kapitel 3.2 Firewall-Regeln aktivieren ab Seite 23 beschrieben der Dienst PING hinzugefügt werden.

- **Host_NextCloud → SP01**

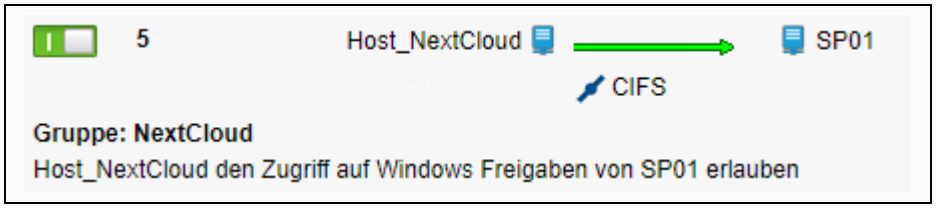


Abb. 157: Gruppe: NextCloud, CIFS (Windows Freigabe) zwischen Host_NextCloud und Sp01

Das Design der Nextcloud für paedML® sieht vor, dass er selbst keinen Datenspeicher hostet, sondern die Windows-Freigaben auf dem Server SP01 durchleitet.

Diese Regel für das CIFS-Protokoll ist demnach eine verbindliche Regel, die bei Inbetriebnahme des Nextcloud-Hosts zwingend aktiviert sein muss.

- **Host_NextCloud → Internet IPv4 / IPv6**

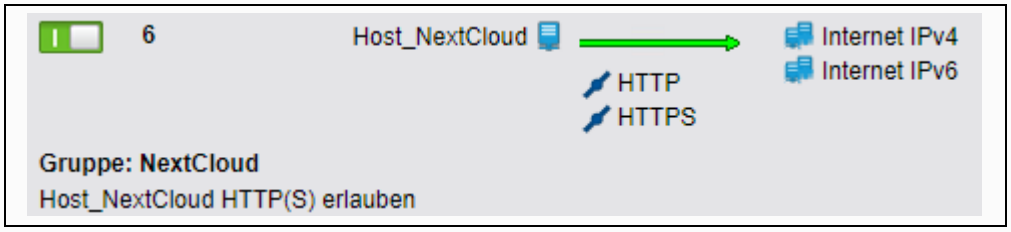


Abb. 158: Gruppe: NextCloud, HTTP ins Internet

Diese Regel sorgt dafür, dass der Nextcloud-Host aus einem Update-Server im Internet Pakete herunterladen und installieren kann.

- **PC_Kein_Internet → Host_Nextcloud (Reject/Zurückweisen)**

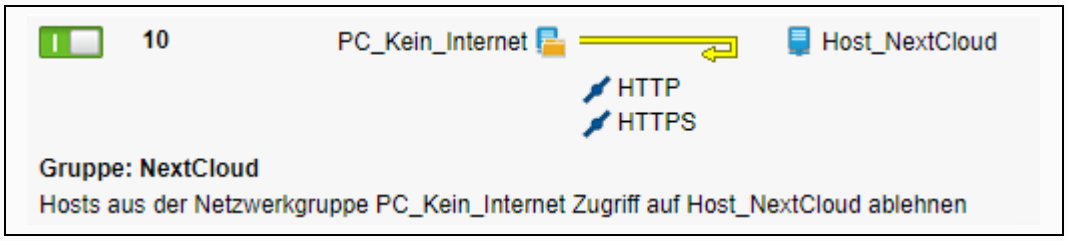


Abb. 159: Gruppe: NextCloud, Kein Zugriff von PC_Kein_Internet auf Host_NextCloud

Es muss gewährleistet werden, dass KA-Teilnehmern der Zugriff auf Nextcloud-Host verweigert wird, um einen Betrugsversuch unterbinden zu können. Das wird normalerweise durch den in der Nextcloud hinterlegten Anmeldefilter kontrolliert und durch den Einsatz des Webproxy (Web Protection) zusätzlich abgesichert.

Falls eine Webproxy-basierte Lösung nicht realisiert werden kann, dann dient diese Regel in Kombination mit der IP-basierten Internetsperre als „Notlösung“.

- **Any → Host_NextCloud**

Abb. 160: Gruppe: NextCloud, Erlaube einen Verbindungsaufbau aus dem Internet zu Host_NextCloud über HTTPS

Erlaubt den Zugriff auf die Nextcloud aus beliebigem Netz.

- **Maskierung (Masquerading)**

Abb. 161: Maskierungs-Regel für die Nextcloud-VM aus der LMZ-Konfigurationsvorlage

Für das Netzwerk paedML_DMZ gibt es keine Maskierung. Sie ist nur auf Host_NextCloud begrenzt.

- **Portweiterleitung für HTTP**

Abb. 162: Port-Umleitung von External (WAN) (Address) auf Host_NextCloud

Für die Anmeldung in Ihrer Nextcloud aus dem Internet ist diese Regel nicht erforderlich. Sie sollte dann aktiviert sein, wenn ein Let's Encrypt Zertifikat importiert bzw. erneuert werden muss.

- **Portweiterleitung für HTTPS**

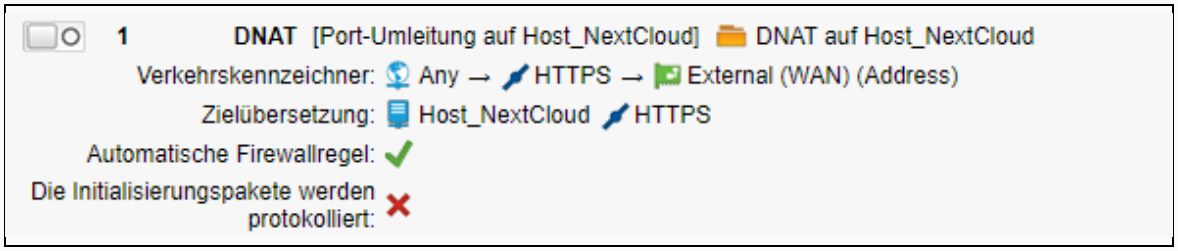


Abb. 163: Port-Umleitung von External (WAN) (Address) auf Host_NextCloud

Diese Regel muss aktiviert sein, damit eine Anmeldung in Ihrer Nextcloud aus dem Internet möglich ist.

Anhang D Known-Issues

D.1 OnlyOffice kann nur im Schulnetz benutzt werden.

Falls Sie die Nextcloud-App OnlyOffice aktiviert haben, den Zugriff auf die Nextcloud aus dem Internet jedoch über einen Reverse-Proxy kontrollieren, dann funktioniert OnlyOffice im Browser bzw. in einer App derzeit nicht.

Stellen Sie die Zugriffmethode auf die Nextcloud aus dem Internet von Reverse-Proxy auf DNAT um. Dann funktioniert OnlyOffice ebenfalls, wenn man sich aus dem Internet angemeldet hat.

D.2 Systemdiagnose gibt eine Warnmeldung für Dateiberechtigungen aus

UMC Systemdiagnose gibt folgende Warnung aus:

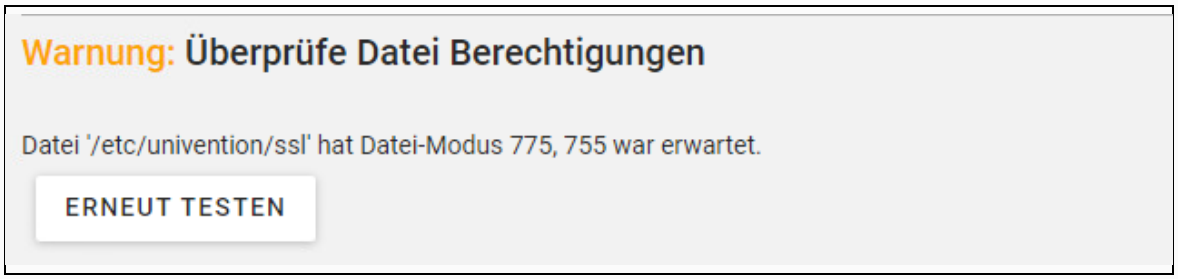


Abb. 164: UMC Systemdiagnose -> Datei Berechtigung überprüfen

Führen Sie auf der Konsole der Nextcloud-VM folgenden Befehl aus:

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

D.3 UCS Systemdiagnose meldet einen kritischen Fehler bzgl. SAML-Zertifikate

Die Systemdiagnose in der UMC meldet folgenden kritischen Fehler.

Abb. 165: UMC Systemdiagnose -> Überprüfung der SAML-Zertifikate fehlgeschlagen

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

Anhang E Standardeinstellung für das Teilen der der Dateien

Durch das Ausführen des Skripts `lmz-nextcloud-windows-finalize` wird eine neue Nextcloud-App namens *paedML Standardeinstellung für das Teilen* installiert und aktiviert.

Abb. 166: Nextcloud-App paedML Standardeinstellungen für das Teilen

Diese App setzt die Standardberechtigungen für das Teilen der Dateien und Ordner so, wie wir sie für den Einsatz der Nextcloud an Schulen für nützlich und sinnvoll halten. So werden das Erstellen, das Ändern, das Löschen und das Weiterteilen einer geteilten Datei oder eines geteilten Ordners standardmäßig verboten.

Die Standardeinstellungen der Nextcloud-App File sharing erlaubt das Erstellen, das Ändern, das Löschen und das Weiterleiten von geteilten Inhalten, sobald Sie die App File sharing aktivieren. Das kann zu ungewollten Fehlbedienungen führen, etwa das unabsichtliche Löschen der Inhalte eines geteilten Ordners oder das versehentliche Weiterleiten einer Datei an fremde Personen.

Aus dem Grund deaktivieren wir mithilfe unserer neuen App die genannten vier Funktionen beim Teilen von Dateien und Ordnern.

Wenn Sie stattdessen Ihre individuellen Einstellungen verwenden wollen, dann führen Sie auf der Nextcloud-VM als Benutzer root den folgenden Befehl aus und bearbeiten die Standardberechtigungen für das Teilen in der Benutzeroberfläche der Nextcloud als Benutzer nc_admin:

```
ucr set nextcloud/apps/antishare='disabled'
```

9 Änderungsdokumentation

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
Stand 10.08.2022 Version 1.1.0	Angepasst für die Bereitstellung der Nextcloud unter paedML® Windows 5.0
Stand 18.07.2023 Version 1.1.1	Angepasst für die Bereitstellung der Nextcloud auf der Basis von Univention UCS 5.0 und Nextcloud 24.0.7

Landesmedienzentrum Baden-Württemberg (LMZ)
Support Netz
Rotenbergstraße 111

70190 Stuttgart

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG

paedML

LMZ LANDESMEDIENZENTRUM BADEN-WÜRTTEMBERG