

007 Nextcloud-Installation und Konfiguration

Administration Aufgabe
Anforderungsniveau: Schwer

1 Ziel der Aufgabe

Diese Aufgabe fokussiert sich auf die Installation, Konfiguration und den Betrieb von Nextcloud als zentrale Plattform für ca. 20 Mitarbeiter, die Kundendaten erfassen und austauschen. Alle nötigen Komponenten (Webserver, HTTPS, Backup, Monitoring, Benutzerverwaltung) sollen implementiert werden. Eine separate Datenbankanbindung (z. B. LDAP/AD) ist nicht Bestandteil dieser Aufgabe.

2 Aufgabenbeschreibung

Setzen Sie auf einer (virtuellen) Hetzner Cloud-Maschine eine lauffähige Nextcloud-Instanz in einer möglichst automatisierten und dokumentierten Umgebung auf. Berücksichtigen Sie dabei folgende Teilaufgaben:

1. Grundlegende Servereinrichtung

- Bieten wir Ihnen bei Bedarf Hetzner Cloud-Zugänge (Maschine mit Debian 12 oder Ubuntu 22.04 LTS). Richten Sie das Betriebssystem ein und führen Sie ein grundlegendes Update (`apt update && apt upgrade`) durch.
- Erstellen Sie einen neuen Systembenutzer `nextcloud` ohne Root-Rechte, der später Besitzrechte an den Nextcloud-Dateien erhält.
- Richten Sie Basis-Firewall-Regeln (mit `ufw` oder `iptables`) ein: Öffnen Sie nur HTTP (80) und HTTPS (443) für den öffentlichen Zugriff und SSH (22) nur für Ihr Büro-/Subnetz.

2. Webserver und PHP-Konfiguration

- Installieren Sie Apache2 (mit `mod_php`) oder Nginx (mit PHP-FPM) einschließlich aller benötigten PHP-Erweiterungen (`php7.4-fpm` oder `php8.1-fpm`):
 - `php-curl`, `php-gd`, `php-imagick`, `php-mbstring`, `php-xml`, `php-zip`, `php-intl`, `php-bz2` u. a.

- Konfigurieren Sie den Webserver für Nextcloud: Legen Sie das DocumentRoot auf `/var/www/nextcloud` an und passen Sie virtual host (Apache) oder server block (Nginx) entsprechend an.
- Setzen Sie sinnvolle PHP-Parameter (z. B. `memory_limit`, `upload_max_filesize`, `post_max_size`, `max_execution_time`) so, dass Nextcloud flüssig läuft.

3. Nextcloud-Installation

- Laden Sie Nextcloud (Version 3.14.1 oder höher) unter <https://nextcloud.com> herunter und entpacken Sie das Paket nach `/var/www/nextcloud`.
- Geben Sie dem Systembenutzer `nextcloud` Eigentümerrechte auf das Verzeichnis (`chown -R nextcloud:www-data /var/www/nextcloud`). Passen Sie Dateisystemrechte (`chmod -R 750`) an.
- Führen Sie die Nextcloud-Webinstaller-URL (z. B. <https://meine-domain.tld/nextcloud>) auf und verbinden Sie die Weboberfläche mit der zuvor erstellten Datenbank `nextcloud`.

4. HTTPS und Zertifikate

- Installieren Sie Certbot und generieren Sie ein offizielles Let's Encrypt-Zertifikat für Ihre Domain (z. B. `certbot -apache` oder `certbot -nginx`).
- Aktivieren Sie HTTP/2 und erzwingen Sie HTTPS (Redirect von Port 80 auf 443).
- Für interne Tests (staging) können Sie ein selbstsigniertes Zertifikat erstellen und in `/etc/ssl/` ablegen. Dokumentieren Sie den Ablauf.

5. Benutzer- und Rechtemanagement in Nextcloud

- Richten Sie in Nextcloud 20 Benutzerkonten ein (z. B. `user01` bis `user20`). Legen Sie drei Gruppen an (z. B. `sales`, `support`, `management`). Verteilen Sie die Benutzer entsprechend.
- Definieren Sie Ordnerstrukturen und Zugriffsrechte für Kundendaten:

6. Aktivieren Sie Ende-zu-Ende-Verschlüsselung (E2EE) oder serverseitige Verschlüsselung, um Kundendaten vor unberechtigtem Zugriff zu schützen.

7. Beschreiben Sie im Administrationshandbuch, wie Freigaben, externe Shares und Verschlüsselung in Nextcloud konfiguriert werden.

Backup- und Wiederherstellungsstrategie

- Erstellen Sie ein Bash-Skript (z. B. `backup_nextcloud.sh`), das folgende Schritte automatisiert:
 - Stoppen des Webservers (Apache2/Nginx).
 - Sichern des Verzeichnisses `/var/www/nextcloud` als `tar.gz` mit Datum im Dateinamen.
 - Sichern der Datenbank `nextcloud` (z. B. mit `mysqldump`).
 - Starten des Webservers.
 - Löschen von Backups, die älter als 14 Tage sind.
- Binden Sie dieses Skript als Cron-Job ein, der täglich um 02:00 Uhr nachts läuft.
- Führen Sie eine Wiederherstellung auf einer separaten Testinstanz (ebenefalls via Hetzner Cloud) durch und dokumentieren Sie jeden Schritt.

Monitoring und Logging

- Installieren Sie ein leichtgewichtiges Monitoring-Tool (z. B. *Prometheus* Node Exporter oder *Zabbix-Agent*). Richten Sie Basis-Metriken ein:
 - Systemauslastung (CPU, RAM, Disk-I/O).
 - Status des Webservers (Prozessprüfung und HTTP-Statuscode 200).
 - Verfügbarkeit der Nextcloud-URL (HTTP-Ping).
- Konfigurieren Sie zentralisiertes Log-Management (z. B. *rsyslog* + *Graylog*): Sammeln Sie Apache/Nginx-Logs und Systemlogs. Erstellen Sie eine einfache Suche, um Fehler (5xx-Statuscodes) zu identifizieren.
- Dokumentieren Sie, wie Alarme (z. B. E-Mail oder Slack-Benachrichtigung) bei einem Ausfall des Nextcloud-Dienstes konfiguriert werden.

Performance-Optimierung und Sicherheit (Optional)

- Aktivieren Sie Caching mittels *Redis* oder *APCu* für Nextcloud. Fügen Sie die entsprechenden Konfigurationen in `config.php` hinzu.
- Setzen Sie einen Reverse Proxy (z. B. Nginx als Proxy vor Apache2) und aktivieren Sie Gzip-Kompression.

- Prüfen Sie die Sicherheit von Nextcloud mit dem integrierten *Security Setup Warnings*-Tool und beheben Sie etwaige Mängel.
- Führen Sie regelmäßige `apt` Security-Updates durch und dokumentieren Sie die letzten Aktualisierungen.

Dokumentation und Übergabe

- Verfassen Sie ein Administrationshandbuch (Markdown oder PDF) mit allen Konfigurationsdateien (z. B. `nginx.conf`, `config.php`, `backup_nextcloud.sh`).
- Erstellen Sie eine Übersicht der Hetzner Cloud-Instanz: Instanz-ID, IP-Adresse, Betriebssystem-Version und Ablaufdatum temporärer Zugangsdaten.
- Beschreiben Sie einen einfachen Prozess, wie ein zweiter Administrator im Notfall übernehmen kann (Zugangsdaten-Management, Dokumentations-Pfad).

3 Anforderungen

- **Automatisierung:** Wo möglich Shell-Skripte, Cron-Jobs oder Ansible-Playbooks verwenden.
- **Sicherheit:** Prinzipien des Least Privilege einhalten (Nextcloud-Dateien im Besitz des `nextcloud`-Users, Firewall-Regeln, HTTPS). Sichere Verschlüsselung (TLS, E2EE) nutzen.
- **Dokumentation:** Alle Schritte in einem klar strukturierten Handbuch nachvollziehbar festhalten.
- **Testumgebung:** Wiederherstellung und Tests auf separater Hetzner-Instanz durchführen.
- **Skalierbarkeit:** Gestaltung der Konfiguration für ca. 20 gleichzeitige Benutzer; Hinweise, wie man bei steigendem Nutzeraufkommen (z. B. Reverse Proxy Cluster, Load Balancer) reagieren könnte.

Viel Erfolg bei der Umsetzung!

Stand: 31. Mai 2025