

Leseprobe

Ein Heimserver, der nicht nur läuft, sondern erklärbar bleibt

Auszüge aus Band 1, Band 2 und Band 3

Norbert Nissen-Henschke

heimserverprojekt.de

Worum es in diesem Projekt geht

Die meisten Anleitungen für ein NAS beginnen mit einem Gerät und arbeiten sich durch dessen Funktionen. Das ist nachvollziehbar, führt aber schnell zu einer Sammlung einzelner Lösungen, die für sich funktionieren und zusammen schwer zu warten sind.

Dieses Projekt geht den umgekehrten Weg. Es beginnt beim Gesamtsystem: beim Netzwerk, bei den Wegen, die Daten nehmen, und bei der Frage, was eigentlich passieren soll, wenn etwas ausfällt. Erst danach wird installiert.

Die Grundlage ist keine Theorie, sondern eine real aufgebaute Umgebung mit zwei Synology-Systemen, die über mehrere Jahre gewachsen ist – einschließlich der Irrwege, die dabei entstanden sind. Genau diese Irrwege sind Teil des Buches, denn sie erklären mehr über ein System als jede fehlerfreie Anleitung.

Der Leitgedanke: Ein Heimserver wird nicht dadurch zuverlässig, dass viele Dienste laufen, sondern dadurch, dass verständlich ist, warum jeder Dienst existiert, wo er läuft, wovon er abhängt und wie sein Ergebnis geprüft wird.

Was dieses Buch anders macht

- Jede Entscheidung wird begründet. Nicht nur, welcher Schalter umgelegt wird, sondern warum genau dieser.
- Fehler sind Teil der Architektur. Reale Fehlerbilder aus dem Projekt werden vollständig aufgearbeitet: Symptom, Ursache, Diagnoseweg, Lösung, Nachweis und Übertragbarkeit.
- Nichts wird behauptet, was nicht geprüft wurde. Jeder Aufbau ist auf beiden Systemen praktisch nachvollzogen worden, bevor er ins Buch kam.
- Du wirst geduzt und mitgenommen. Das Buch richtet sich ausdrücklich auch an Einsteiger, ohne dabei technisch oberflächlich zu werden.

Jede Änderung im Projekt folgt derselben Reihenfolge. Sie wird in Band 1 eingeführt und trägt anschließend alle weiteren Bände:

Der Fünf-Schritte-Ablauf: das Prinzip hinter jeder Änderung

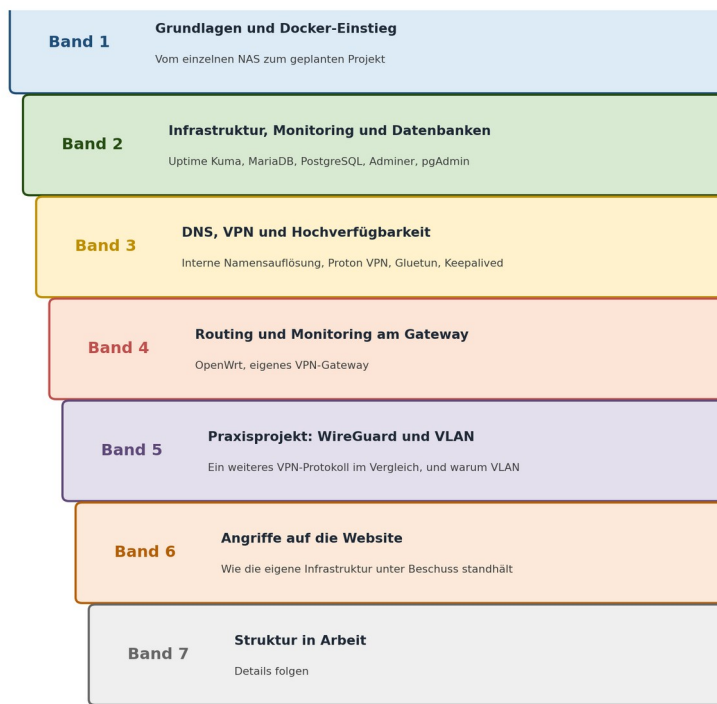


Der Fünf-Schritte-Ablauf aus Band 1, Kapitel 1

Wie die Reihe aufgebaut ist

Die Bände bauen aufeinander auf. Was in einem Band entsteht, ist im nächsten Band Voraussetzung. Dadurch wächst eine einzelne, zusammenhängende Umgebung, statt dass mehrere voneinander unabhängige Beispielaufbauten nebeneinander stehen.

Der Aufbau der Reihe



Jeder Band setzt auf dem vorherigen auf – die Umgebung wächst mit. Das Grundprinzip gilt für jedes NAS, unabhängig vom Hersteller.

Die Bände der Reihe und ihre Schwerpunkte

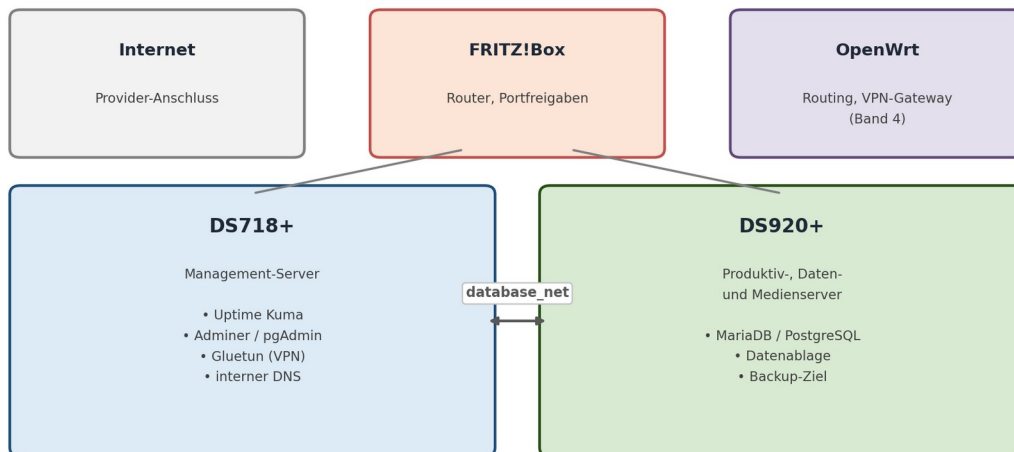
Band 1 legt das Fundament: Bestandsaufnahme einer gewachsenen Umgebung, die Entscheidung für Container, die ersten Schritte mit Docker Compose und am Ende ein Reverse Proxy als gemeinsame Eingangstür für Webdienste. Band 2 macht daraus eine beobachtbare Infrastruktur mit Monitoring und einer eigenen Datenbankebene. Band 3 kümmert sich um die Wege im Netz: interne Namensauflösung, kontrollierte VPN-Verbindungen und am Ende ein hochverfügbares VPN-Gateway mit automatischer Umschaltung zwischen beiden NAS-Systemen. Band 4 führt Routing und Monitoring auf einem eigenen OpenWrt-Gateway weiter. Die geplanten Bände 5 und 6 gehen anschließend zu einem weiteren Praxisprojekt mit WireGuard und VLAN sowie zur Frage, wie die eigene Infrastruktur gezielten Angriffen standhält.

Band 4 ist bereits in Arbeit, die Bände 5 bis 7 sind in Planung.

Das Gesamtsystem

Zwei Synology-Systeme mit bewusst getrennten Rollen bilden den Kern des Projekts. Die Rollenverteilung folgt nicht allein der Leistung der Geräte. Entscheidend ist, welche Dienste bei einem Ausfall weiterhin erreichbar sein sollen und wo die jeweiligen Daten sinnvoll aufgehoben sind.

Das Gesamtsystem im Projekt



Zwei eigenständige Synology-Systeme mit klar getrennten Rollen – kein Cluster, aber ein geplanter Verbund.

Die beiden NAS-Systeme und ihre Rollen im Projekt

Wichtig: Diese Trennung ist keine vollständige Hochverfügbarkeit. Sie ist aber ein sinnvoller erster Schritt: Kontrolle und Nutzdaten liegen nicht auf demselben Gerät.

Leseprobe 1

Band 1 · Kapitel 1 · Projektidee und Ausgangslage

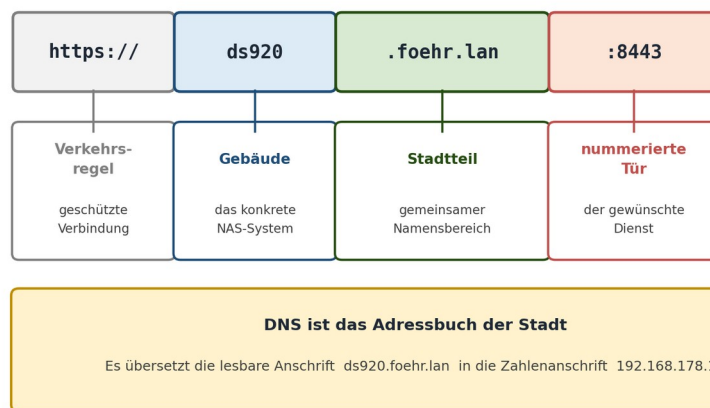
Das Heimnetz als Stadtteil – vom Namen zur richtigen Tür

Für einen Neuling wirken Namen, IP-Adressen und Ports zunächst wie drei verschiedene Sprachen. Deshalb begleitet uns durch das ganze Buch das Bild einer kleinen Stadt – es zeigt, warum ein richtiger Name allein noch nicht zur richtigen Anwendung führt.

Stell dir dein Heimnetz wie eine Stadt vor. Der Bereich foehr.lan ist unser Stadtteil. Das Gerät ds920 ist dort ein bestimmtes Gebäude. Der vollständige Name ds920.foehr.lan ist die gut lesbare Anschrift dieses Gebäudes. DNS arbeitet wie ein Adressbuch und findet dazu die Zahlenanschrift.

Am Gebäude angekommen, brauchst du noch die richtige Tür. Genau diese Aufgabe übernimmt der Port: Port 443, Port 8080 oder Port 8443 ist eine nummerierte Software-Tür zu einem bestimmten Dienst. Gemeint ist dabei keine sichtbare Netzbuchse am Gerät.

Das Heimnetz als Stadt: eine Adresse Stück für Stück gelesen



Eine richtige Anschrift mit der falschen Türnummer führt ebenso wenig ans Ziel wie die richtige Tür am falschen Gebäude.

Eine vollständige Adresse, Stück für Stück gelesen

Diese Werte stammen aus unserer Umgebung. Bei dir können Stadtteil, Anschrift und Türnummer anders heißen – das Prinzip bleibt dasselbe.

Merke: Eine richtige Anschrift mit der falschen Türnummer führt ebenso wenig ans Ziel wie die richtige Tür am falschen NAS.

Leseprobe 2

Band 1 • Kapitel 6 • Reverse Proxy

Was zwei Tage Fehlersuche wirklich gezeigt haben

Die beteiligten Komponenten ließen sich einzeln erfolgreich prüfen. Apache lieferte Inhalte. PHP arbeitete. Das interne Docker-Netzwerk löste Dienstnamen auf. Der Reverse Proxy konnte das Backend erreichen. Trotzdem erschien die Webseite von außen nicht.

Genau hier wäre es leicht gewesen, erneut Container zu löschen, Compose-Dateien zu verändern oder Zertifikate neu anzulegen. Stattdessen wurde die Anfrage als zusammenhängender Weg betrachtet: Internet, Router, internes Zielgerät, veröffentlichter Proxy-Port, Docker-Netzwerk und schließlich der Webserver.

Die Suche dauerte zwei Tage, weil der sichtbare Fehler am Ende der Kette lag, während die Ursache deutlich früher saß. Die Portfreigaben im Router verwendeten zwar die richtigen Portnummern, zeigten nach ihrer Neuerstellung jedoch auf das falsche NAS.

Prüfung	Ergebnis	Schlussfolgerung
Webserver direkt im internen Weg	Seite antwortet	Webserver und Inhalt funktionieren.
Proxy zum Backend	Interne Weiterleitung funktioniert	Docker-Netzwerk und Zielname sind nicht die Ursache.
Externer Aufruf	Keine Webseite	Der Fehler liegt vor oder am öffentlichen Eingang.
Ziel der Portfreigabe	Weiterleitung zeigt auf falsches NAS	Die Anfrage erreicht den richtigen Proxy nicht.

Die Korrektur der Zieladresse war klein. Die daraus entstandene Arbeitsweise war wesentlich größer: Nicht dort suchen, wo der Fehler sichtbar wird, sondern jeden Übergang mit einem passenden Test prüfen. Ein Test darf nicht nur Aktivität zeigen; er muss eine konkrete Vermutung bestätigen oder ausschließen.

Kapitelziel erreicht: Die Webseite ist nicht nur erreichbar. Wir können erklären, warum die Architektur so aufgebaut wurde und wie der vollständige Weg einer Anfrage geprüft wird.

Leseprobe 3

Band 2 · Kapitel 3 · MariaDB

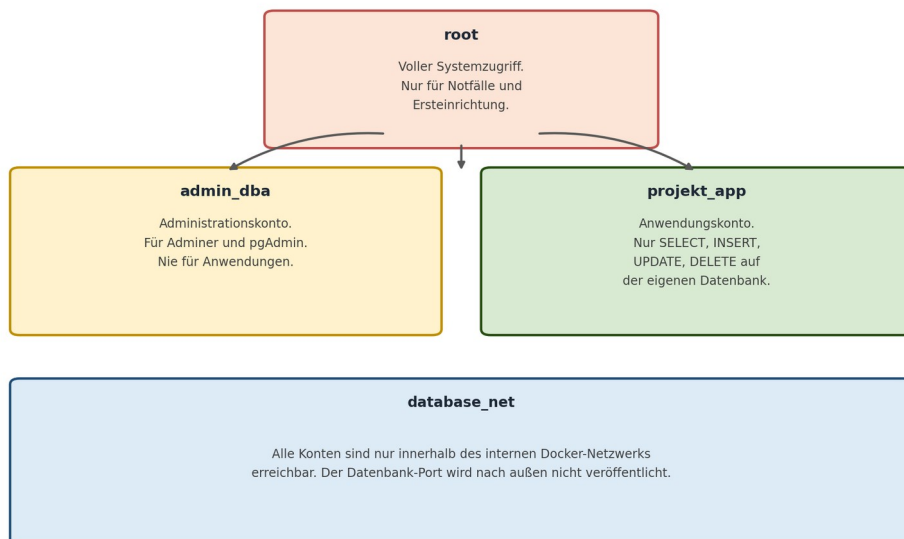
Benutzer und Rechte verstehen

Im Alltag verwendest du weder das Datenbank-Root-Konto noch den Superuser für jede Aufgabe. Stattdessen arbeitest du mit getrennten Administrations- und Anwendungskonten. So bleiben Änderungen nachvollziehbar und Rechte auf das notwendige Maß begrenzt.

MariaDB unterscheidet Konten dabei nicht nur nach Benutzername, sondern nach der Kombination aus Benutzer und zugelassenem Host. Ein Konto für den Zugriff von der lokalen Maschine ist deshalb ein anderes Konto als eines, das Verbindungen aus dem Netzwerk zulässt – auch wenn der Benutzername identisch lautet.

Konkret heißt das: Meldest du dich direkt im Container an, verbindest du dich lokal. Ein Verwaltungscontainer, der über das Netzwerk zugreift, benötigt dagegen ein eigenes Konto. Die Datenbank behandelt beide als vollständig getrennte Konten.

Benutzer- und Rechteprinzip in der Datenbank



Drei Konten mit klar abgegrenzten Aufgaben

Merke: Eine erfolgreiche Anmeldung allein genügt nicht als Nachweis. Erst wenn geprüft ist, dass ein Konto genau die vorgesehenen Rechte besitzt und keine systemweiten Änderungen ausführen kann, ist die Einrichtung abgeschlossen.

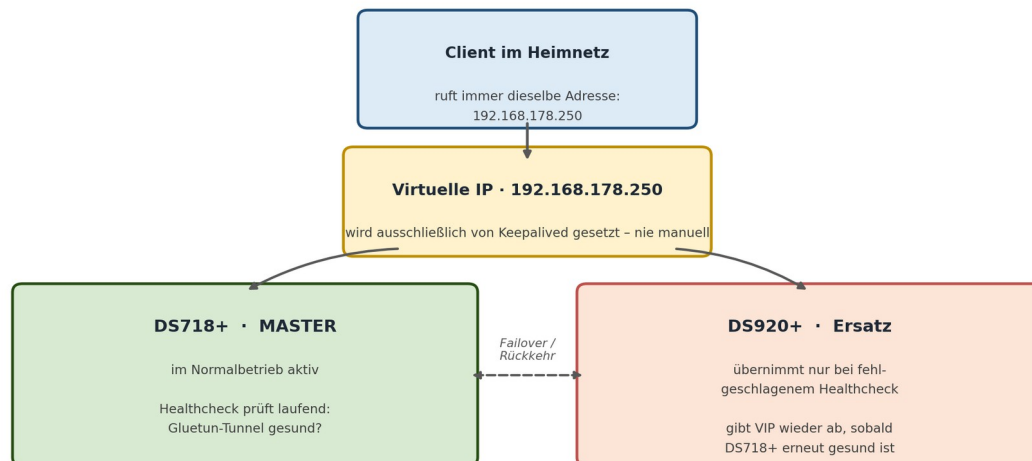
Leseprobe 4

Band 3 · Kapitel 7.1 · Latenzzeiten des VPN sind schlecht

Wenn die auffällige Zahl nicht die Ursache ist

Am Ende von Band 3 tragen beide NAS-Systeme gemeinsam ein hochverfügbares VPN-Gateway: Eine virtuelle Adresse wechselt bei Bedarf automatisch vom bevorzugten System auf das Ersatzsystem, ohne dass ein Client davon etwas merkt – solange alles funktioniert.

Hochverfügbarkeit mit Keepalived: eine Adresse, zwei Systeme



Eine virtuelle IP allein ist noch kein Beweis – erst der geprüfte Weg durch Routing, Tunnel und DNS zählt.

Die virtuelle IP, die zwischen beiden NAS wechseln kann

Genau in dieser Umgebung tauchte ein Fall auf, der zeigt, wie trügerisch ein einzelner Messwert sein kann. Der VPN-Weg wirkte spürbar langsam. Eine gemessene Latenz von rund 14 Millisekunden sah verdächtig aus – und wäre eine bequeme Erklärung gewesen.

Statt sofort den Anbieter oder den Serverstandort zu wechseln, wurde die gesamte Kette geprüft, die hinter der virtuellen Adresse steckt. Das Ergebnis überraschte: Die auffällige Zahl war gar nicht die Ursache.

Fehlerbild: Der VPN-Weg fühlte sich langsam an. Eine auffällige Latenzmessung schien das zu bestätigen.

Ursache: Der Healthserver von Gluetun war auf beiden NAS zeitweise nicht erreichbar, Keepalived stand deshalb auf FAULT, und auf einem der Systeme war eine vom anderen übernommene Schnittstellenangabe schlicht falsch.

Diagnose: Ein Analyse-Skript erfasst Tunnelstatus, Healthserver, Keepalived-Zustand, Schnittstellen, virtuelle Adresse und den öffentlichen Ausgang in einem Durchlauf – statt einzelner Konsolenbefehle, deren Zusammenhang man sich merken muss.

Lösung: Healthserver und Schnittstellenangabe wurden getrennt je NAS korrigiert. Die virtuelle Adresse blieb dabei unangetastet: Sie wird ausschließlich von Keepalived gesetzt, nie von Hand.

Übertragbarkeit: Eine auffällige Zahl ist eine Beobachtung, keine Diagnose. Latenz, Healthcheck und virtuelle Adresse sind drei unterschiedliche Ebenen – wer sie vermischt, repariert am Ende das Falsche.

Wie es weitergeht

Die Leseprobe zeigt vier kurze Ausschnitte aus drei Bänden – vom ersten Stadtplan-Bild in Kapitel 1 von Band 1 bis zur Fehlersuche in einem hochverfügbaren VPN-Gateway am Ende von Band 3. Dazwischen liegt derselbe rote Faden: erst verstehen, dann entscheiden, dann prüfen.

Was die Leseprobe nicht zeigen kann, ist die Menge. Über drei Bände hinweg entsteht eine vollständige, tatsächlich betriebene Infrastruktur: zwei NAS-Systeme, eine Datenbankplattform mit MariaDB und PostgreSQL, ein eigenes Monitoring, kontrollierte interne Namensauflösung und ein VPN-Gateway, das bei einem Ausfall automatisch umschaltet – jeder Schritt begründet, jeder Fehlerfall real und nachvollziehbar dokumentiert.

Für wen das Buch gedacht ist: Für alle, die ein NAS besitzen – ganz gleich welcher Hersteller und welche Bauart – und mehr wollen als eine Sammlung angeklickter Funktionen. Das Prinzip ist überall dasselbe, nur System und Software unterscheiden sich. Vorkenntnisse in Docker sind hilfreich, aber nicht nötig – Band 1 beginnt bei den Grundlagen.

Warum es sich lohnt, dranzubleiben

- Du baust keine Einzellösung nach, sondern eine zusammenhängende Infrastruktur, die mit jedem Band wächst.
- Jeder Fehlerfall im Buch ist real passiert – mit derselben Diagnosekette, die du bei dir zu Hause anwenden kannst.
- Skripte und vollständige Konfigurationsdateien gibt es im Downloadbereich, statt sie aus dem Buch abzutippen.
- Du entscheidest selbst, wie weit du gehst: Band 1 allein ergibt bereits einen sauberen, erklärbaren Einstieg.

Skripte und Konfigurationsdateien

Die im Buch verwendeten Skripte und vollständigen Konfigurationsdateien werden in einem eigenen Downloadbereich bereitgestellt. Damit musst du längere Konfigurationen nicht von Hand übertragen.

Hinweis: Übernimm eine Datei trotzdem nie ungeprüft. Pfade, Volumebezeichnungen, Ports, Benutzernamen und andere Umgebungswerte müssen zu deinem eigenen System passen.

Neugierig auf mehr? Diese Leseprobe ist ein Ausschnitt aus einem laufend wachsenden Projekt. Wer bei den nächsten Bänden – WireGuard und VLAN in einem weiteren Praxisprojekt, dazu ein Band zu Angriffen auf die eigene Website – dabei sein möchte, findet aktuelle Informationen auf heimserverprojekt.de.

DAS SYNOLOGY HEIMSERVER-Projekt

Norbert Nissen-Henschke · heimserverprojekt.de