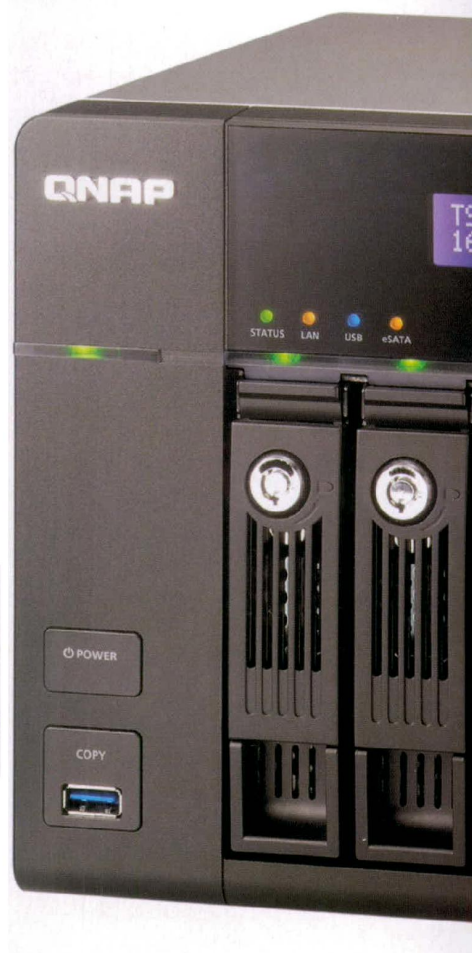


VIER NAS-APPARATEN GETEST

BACK-UP OVER HET INTERNET

TEKST: HENK VAN DE KAMER

We weten allemaal dat het maken van een back-up belangrijk is. Maar hoeveel van onze lezers doen het ook dagelijks? Wie al zijn data op een NAS heeft staan, zou die back-up gemakkelijk kunnen automatiseren over het internet naar een tweede NAS. In dit artikel zoeken we de ideale kandidaat.



Een standaardtest van een serie apparaten is saai. Voor deze test van Network Attached Storage- ofwel NAS-apparaten hebben we dan ook gekozen voor een andere aanpak. We gaan ervan uit dat een fabrikant geen apparaat op de markt zal brengen als aan de basisfunctionaliteit niet wordt voldaan. Omdat een moderne NAS gewoon een volwaardige computer is en dus veel meer kan, hebben wij een serie fabrikanten de volgende opdracht gegeven:

Een goede back-up bevindt zich off-site, bijvoorbeeld bij een familielid in een andere stad. PC-Active is daarom op zoek naar een NAS waarmee een back-up over het internet mogelijk wordt. Uiteraard stellen wij hoge eisen aan beveiliging; denk aan zaken als versleuteling en toegang op basis van ip-adres. Samenwerken met Windows, Mac OS en Linux zijn uiteraard een pre, evenals een laag stroomverbruik.

Back-up

Vaak denkt men dat een NAS meteen een backup is. Dat is pertinent niet waar! Zoals de afkorting al zegt, is het gewoon een vorm van dataopslag die dankzij het netwerk handig door alle pc's is te gebruiken. De misvatting komt door de Raid-beveiliging, want daarvoor kan één harddisk - soms zelfs twee - uitvallen terwijl uw data gewoon beschikbaar blijven en u dus kunt doorwerken. Maar een virus kan nog steeds alle data wissen en ook bij diefstal of brand bent u alles kwijt. Daarom stellen we twee eisen aan een goede back-up: *off-line* en *off-site*. De eerste betekent dat de

data niet direct beschikbaar zijn - Raid zorgt juist daarvoor - en de tweede dat een ramp bij u thuis geen gevolgen heeft voor uw data.

Een oplossing is een tweede NAS waarop u alles kopieert en die vervolgens veilig opbergen in een bankkluis. Maar het kan handiger. In plaats van een bankkluis parkeren we die NAS - mogelijk staat daar al een exemplaar te snorren - bij een vriend in een andere stad en laten we daar automatisch elke nacht een tweede kopie van onze data uploaden. En andersom; dat is natuurlijk wel zo aardig. Dat het geheel off-site is, zal iedereen duidelijk zijn. Ook aan de off-line-eis wordt voldaan, want ondanks de internetverbinding kunt u niet gemakkelijk bij uw bestanden aan de andere kant.

Rsync

Alle geteste apparaten kunnen standaard doen wat wij vragen, maar meestal alleen naar de eigen producten. De standaard onder Linux - en dat gebruiken de meeste NAS-apparaten - is rsync ofwel remote synchronisatie. Dit programma overlegt - lees: protocol - met zijn collega aan de andere kant wat er gedaan moet worden om alles weer gelijk te trekken zonder overbodige uploads. Er bestaat een rsync daemon ofwel hetzelfde protocol, maar dan permanent luisterend op poort 873. Alle geteste apparaten hebben deze en kunnen zo een back-up ontvangen. Maar vreemd genoeg is nauwelijks nagedacht over de omgekeerde situatie. Het rsync-protocol is onversleuteld. Als we aan beide kanten het rsync-commando - dus niet de daemon -



gebruiken, moet één partij inloggen op een server die commando's kan uitvoeren. Zo'n server is bijvoorbeeld SSH - Secure Shell - en daarmee krijgen we meteen een versleutelde verbinding en dat is voor een back-up eigenlijk verplicht. Tenzij de bestanden zelf al versleuteld zijn. Dat is sowieso handig; kan de tegenpartij ook niet in de verleiding komen om in uw zaken te neuzen. Dat versleutelen moet wel per bestand [1], want anders kan het slimme rsync niet gebruikt worden. We kunnen u nu al verklappen dat geen van de deelnemers ondanks onze vraag een oplossing voor dit probleem biedt. In de komende maanden gaan we uitzoeken of en hoe dit oplosbaar is.

Testopzet

Als ontvanger van onze back-up [2] is een Synology DS111 gebruikt bij de burens. Off-site, maar u wilt een grotere afstand! Omdat de eigen Synology-back-up niet aan onze eisen voldoet, is er geen sprake van oneerlijk voordeel. Via de firewall op de NAS is alleen poort 22 - SSH - bereikbaar voor ons ip-adres. Op het systeem is tot slot een gebruiker hvdkamer aangemaakt en daarmee moeten alle deelnemers het doen. Beide huishoudens zijn onlangs voorzien van glasvezel en hebben een 25 Mbit/s up- en download. Vooral die eerste is erg belangrijk in onze opdracht. Met 25 Mbit/s kunnen we 2,5 megabyte per seconde uploaden en hiermee komt u grofweg op negen gigabyte per uur uit. De complete terrabyte die we tot onze beschikking hadden, is dan nog steeds een halve dag. Dankzij rsync moeten we éénmalig een complete

back-up maken; daarna gaat het alleen om veranderingen en dat zal een stuk minder zijn. Elk van de apparaten wordt leeg verkocht en wij hebben ze voorzien van twee 1 TB-schijven van Western Digital - voor de kenners WD10EARS - die tussendoor steeds zijn gewist [3]. De schrijfsnelheid is zo'n 120 MiB/s, dus compleet volschrijven kost drie uur. Die tijd kost ook het initialiseren van Raid1: beide schijven moeten identiek worden, ook als er nog geen bestandje is geplaatst. Alle deelnemers beschikken over een gigabit aansluiting, maar aangezien de internetverbinding de beperkende factor is, voldeed de oude 100 Mbit/s-switch prima.

Deelnemers

Uiteindelijk staan er vier apparaten op onze tafel: Netgear ReadyNAS Ultra 2, Qnap TS-559 Pro II TurboNAS, Synology DS211+ en de Thecus N2200XXX. De veel duurdere Qnap heeft vijf en de rest een tweeslots voor 3,5 inch SATA-harddisks. Die aansluiting maakt hotswap - verwijderen van een harddisk tijdens bedrijf - mogelijk en dat is weer interessant voor Raid1 of hoger. Naast Raid1 kan ook worden gekozen voor het niet-veilige Raid0 of JBOD - Just a Bunch Of

Firewall

Een firewall kent twee mogelijke instellingen: 'alles mag behalve' of 'niets mag behalve'. De eerste is handig op servers waar u alleen noodzakelijke diensten draait en die wilt beveiligen. De andere komt meer voor en zouden we op onze NAS willen gebruiken om te zorgen dat alleen bepaalde adressen toegang hebben. Deze moeten dan wel een vast ip-adres hebben, of u moet dagelijks de firewall - kan automatisch - aanpassen. De firewall onder Linux heet iptables voor IPv4 en ip6tables voor IPv6. Als we ip-adres 111.222.333.444 willen toestaan naar de SSH-poort, kunnen we het volgende Bash script gebruiken:

```
#!/bin/bash
```

```
iptables -F
```

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A INPUT -p TCP -s 111.222.333.444 --dport 22 -j ACCEPT
```

```
iptables -A INPUT -j DROP
```

```
iptables -A OUTPUT -j ACCEPT
```

De -F flusht alle regels en zorgt dus voor een situatie waarin meestal alles mag. De tweede regel zorgt ervoor dat inkomend verkeer dat hoort bij toegestane uitgaande verbindingen, wordt doorgelaten. De derde regel zorgt voor de toegang en de vierde blokkeert alle andere inkomende verbindingen. De laatste regel tenslotte zorgt ervoor dat al het uitgaande verkeer is toegestaan. Uiteraard kunt u ook hier restrictiever zijn. Dit voorbeeld werkt, maar dan kunt u vanaf het lokale netwerk niet meer bij de NAS komen. Om dat op te lossen moet u de volgende regel na de tweede toevoegen:

```
iptables -A INPUT -s 192.168.x.0/24 -j ACCEPT
```

Daarmee wordt al het lokale verkeer op netwerk x toegestaan. En ja, ook dit kunt u weer verfijnen.



De Netgear in een strakke ijzeren behuizing

Drives - om zo alle ruimte beschikbaar te krijgen. Gaat dan echter een disk kapot, dan bent u ook de data op de andere schijven kwijt!

Drie apparaten hebben een Kensington-lock, maar of u daarmee diefstal gaat voorkomen? Het wordt hooguit wat lastiger. Twee apparaten kunnen met een simpel slotje - wederom niet bedoeld tegen inbraak - een ongelukkige hotswap voorkomen. Alle apparaten hebben een zogenoemde *copy button* waarmee een aangesloten usb-stick of in geval van een SD-slot een geheugenkaartje gebackupt kan worden. Tot slot hadden de meeste deelnemers twee netwerkaansluitingen waarmee *failover* - overschakelen op de andere verbinding - of samenvoegen tot een supersnelle verbinding mogelijk is.

Netgear ReadyNAS Ultra 2

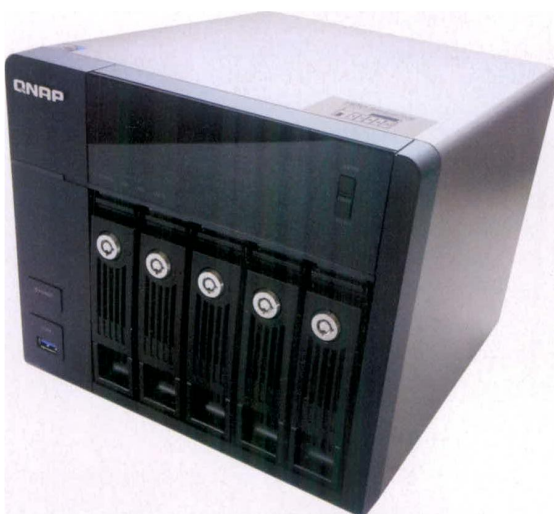
Het duurde even voordat wij doorhadden [4] hoe het apparaat geïnitieerd kon worden. Met behulp van het RAIDar-installatieprogramma - beschikbaar

voor Windows, Mac en Linux - kan Raid1 gekozen worden. Na afloop is 4,5 GiB afgesnoept voor een verouderd besturingssysteem dat waarschijnlijk uit een flashdrive komt. Het geheel kan online up-to-date worden gebracht. Het apparaat maakt trouwens meer lawaai dan ons lief is en ondanks het fraaie uiterlijk zouden wij het verbannen naar de meterkast.

De SSH-toegang is niet standaard, maar kan gemakkelijk via een add-on worden toegevoegd. Daarmee verliezen we wel de support, maar wie weet waarmee hij of zij bezig is kan dat rustig negeren. Via de commandline blijkt iptables aanwezig - echter geen firewall via de webinterface - maar door afwezige kernelmodules is het nauwelijks bruikbaar. Ook zonder firewallbescherming kan via rsync over SSH de back-up gedaan worden.

Qnap TS-559 Pro II TurboNAS

Omdat wij geen prijsklasse hadden genoemd, was het even schrikken. Met de vijf bays en het lcd-scherm ziet het er indrukwekkend uit. Als enige kan het apparaat zichzelf configureren met lege harddisks. Wij kozen echter voor de webinterface die platformafhankelijk is [5]. Er wordt 2,0 GiB gebruikt voor het installeren van een verouderde versie. Na inloggen wordt ons daar meteen op gewezen en kunnen we online updaten. Het geheel is met twee harddisks erg stil en mag wat ons betreft dus in de werkkamer blijven staan. Op de achterkant zien we een VGA-aansluiting, maar voordat u enthousiast wordt: deze is alleen voor onderhoud. Via de webinterface is SSH-toegang aan te zetten, maar alleen admin kan hiervan gebruikmaken. Weliswaar kunnen we daarmee onze back-up via rsync over SSH voor elkaar krijgen, andersom wordt lastiger, tenzij we de burens het admin-wachtwoord gaven. Qua firewall zien we geen mogelijkheden in de webinterface en via de commandline wordt duidelijk dat iptables ontbreekt en is vervangen door het ons niet bekende `ip_filter`.



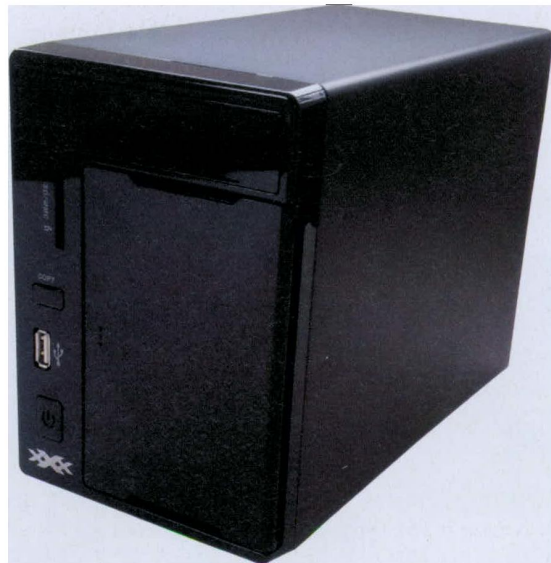
Qnap met maar liefst vijf slots voor harddisks



Qnap: rechtsonder zit de VGA-aansluiting



De fraai vormgegeven Synology



De Thecus is iets hoger vanwege de PCIe-uitbreiding

Synology DS211+

Na het plaatsen van de lege harddisks verwacht het systeem dat we via de Synology Assistant - beschikbaar voor Windows, Mac en Linux - een image van het besturingssysteem uploaden vanaf een werkmachine [6]. Dat lijkt omslachtig, maar als u tevoren de meest recente versie ophaalt is alles wel meteen up-to-date. Na afloop wordt 4,4 GiB in beslag genomen door twee Raid1-partities. De rest van de ruimte kunt u naar believen indelen. De gebruikte OpenSSH-server is gepatcht om samen te werken met het gebruikersbeheer via de webinterface. Daardoor kunt u als root inloggen met het wachtwoord van het admin-account. Helaas zorgt de patch er ook voor dat sshfs en scp - twee onderdelen die wij al snel misten - niet werken. Standaard kunnen gewone gebruikers niet op de shell inloggen, maar dat is gelukkig aan te passen [3]. Waarmee ons back-upidee via rsync en SSH-verbinding toch is uit te voeren.

Thecus N2200XXX

Deze luidruchtige NAS hoort thuis in de meterkast. Aan de achterkant zien we iets interessants; na het openen van de kast wordt duidelijk dat u een PCIe x1 *low-profile* uitbreidingskaart kunt plaatsen. Het geheel gebruikt bij de initialisatie geen DHCP en via de web-interface is dat ook niet aan te passen [7]. Wij moesten dus een Windows-machine - een Mac had ook gekund - regelen om dat aan te passen via speciale software. Een andere optie was SSH-toegang geweest, maar deze is niet beschikbaar. Waarmee ons back-upidee ook niet uitvoerbaar is. We hebben nog geprobeerd om de rsync daemon op de Synology DS111 te gebruiken, maar om onduidelijke redenen lukt ons dat niet. De test-knop geeft ook geen uitsluitsel.

Ons oordeel

De verwachting dat alle apparaten in ieder geval doen wat we van een NAS verwachten, is helemaal uitge-

Type	Synology	Netgear	Thecus	Qnap
	DS211+	ReadyNAS Ultra 2	N2200XXX	TurboNAS TS-559 Pro II
Website	http://www.synology.com	http://www.netgear.com	http://www.thecus.com	http://www.qnap.com
Straatprijs	vanaf € 310,-	vanaf € 240,-	vanaf € 300,-	vanaf € 895,-
Processor	Marvell ARMv5 (88FR131)	Intel Atom D425	Intel Atom D525	Intel Atom D525
Geheugen (MiB)	512	1024	1024	1024
LAN	1x	2x	2x	2x
eSATA	ja	nee	ja	ja (2x)
USB	3x	3x	3x	6x
Kensington-slot	ja	ja	nee	ja
SD/MMC	ja	nee	ja	nee
Bijzonderheden	-	-	slotje op tray / PCIe x1	slotje op trays / VGA
Verbruik (Watt) ³	9/22	17/28	24/39	24/36
Afmetingen (bx dx h cm)	11x23x16	10x22x14	12x24x17	21x24x18
Gewicht (kg) ¹	1,3	2,1	3,0	4,6 ²

1: exclusief harddisk en losse voeding; 2: inclusief interne voeding; 3: ruststand/peik

⊗ komen. Nu vroeg onze test bewust *meer*, om zo een duidelijke winnaar aan te wijzen. Ons back-upidee bleek helemaal niet zo eenvoudig. Sommige apparaten lijken het te kunnen, maar dan zijn er ofwel de nodige beperkingen of u moet in de buidel tasten voor een online dienst. Zo bekeken is er dus geen enkele winnaar! Met meer uitzoekwerk is vast iets te maken, maar dan wordt toegang via SSH essentieel. Thecus is daardoor de duidelijke verliezer: geen SSH-

IPv6

Bij de Netgear en de Qnap staat IPv6 standaard uit, maar deze kan via de webinterface aangezet worden. Voorzover wij kunnen nagaan, doet de Thecus niet aan IPv6. De Synology krijgt *out-of-the-box* via onze Fritz!box 7270 en SixXS-tunnel een IPv6-adres. In de firewall kunnen we een enkel IPv6-adres gebruiken, maar het subnetveld weigert de bekende notaties te accepteren en kan alleen overweg met IPv4. Via de commandline konden we via ip6tables zien dat dit deel van de firewall correct werd ingesteld, maar contact maken via SSH bleek onmogelijk totdat we de firewall weer uitschakelden [2]. Na contact met Synology is ons gevraagd om de IPv6-functionaliteit verder te debuggen. Uiteraard werken wij daar graag aan mee.

toegang, ook niet via onofficiële weg [8]. Netgear wordt derde: met de officiële add-on verliest u de support [9]. Op de tweede plaats komt Qnap: SSH staat standaard aan, maar alleen voor de admin [10]. Uiteindelijk wint dus Synology: ondanks de beperkingen kan deze het meest [11]. Het apparaat wint sowieso op punten vanwege de werkende IPv4-firewall, het lage stroomverbruik en de zeer actieve gemeenschap. Het apparaat straalt gewoon lol uit. Dat het geheel op een ARM-processor draait, mag de pret niet drukken. Voor wie iets minder avontuurlijk is, ook Synology heeft producten met een Atom-processor, maar die hebben uiteraard een hoger verbruik. ⊗

INFORMATIE

- [1] http://en.wikipedia.org/wiki/Filesystem-level_encryption
- [2] <http://www.hetlab.tk/tests/nas-test-inregelen-ontvanger>
- [3] <http://www.hetlab.tk/tests/nas-test-dom-doen>
- [4] <http://www.hetlab.tk/tests/nas-test-netgear>
- [5] <http://www.hetlab.tk/tests/nas-test-qnap>
- [6] <http://www.hetlab.tk/tests/nas-test-synology-herstellen>
- [7] <http://www.hetlab.tk/tests/nas-test-thecus>
- [8] <http://www.hetlab.tk/tests/nas-test-geen-ssh>
- [9] <http://www.hetlab.tk/tests/nas-test-ssh-op-netgear>
- [10] <http://www.hetlab.tk/tests/nas-test-ssh-volgens-qnap>
- [11] <http://www.hetlab.tk/tests/nas-test-proefbestand>

WOORDENLIJST

Tijdens het schrijven kwamen we in de verschillende menu's de nodige kreten tegen. Een kleine opfriscursus.

NFS

Network File System is ooit ontwikkeld door Sun, ver voordat wij als thuisgebruikers doorhadden dat bestanden ook via het netwerk kunnen komen. Later maakten Apple en Microsoft een soortgelijk iets, maar dit is van oudsher de manier waarop Linux het opstarten van bestanden en zelfs het compleet opstarten van het besturingssysteem mogelijk maakt.

WEBDAV

Web-based Distributed Authoring and Versioning ofwel een manier om bestanden beschikbaar te maken via een webserver. Omdat de beheerinterface sowieso deze laatste gebruikt en webverkeer bijna nergens geblokkeerd wordt, is het de manier om bestanden via het internet te kunnen delen.

SMART

Self-Monitoring, Analysis and Reporting Technology ofwel de techniek die moderne harddisks gebruiken om interne informatie als temperatuur, aantal defecte sectoren en andere problemen beschikbaar te maken. Sommige van deze waarden zijn een indicatie voor het op handen zijnde overlijden.

NOTIFICATIE

Voor SMART en problemen in de Raid-synchronisatie is het handig als het systeem deze kenbaar kan maken via een sms'je of e-mail. Voor het versturen van een sms gebruikt het systeem ofwel een speciaal e-mailadres of het aanroepen van een speciale webpagina.

JUMBO FRAMES

Traditioneel is een tcp/ip-pakketje maximaal 1500 bytes groot. Met name op gigabit-snelheden en bij grote hoeveelheden data is dit een beperkende factor. Een jumbo frame is een veel grotere hoeveelheid data in een pakketje, maar dan moet alle apparatuur dit wel ondersteunen.

UPS

Uninterruptible power supply ofwel een batterij waarmee aangesloten apparaten door kunnen werken bij stroomuitval. De data kunnen ondanks de Raid beschadigd raken als niet alle harddisks de nieuwe gegevens hebben verwerkt. Een groot deel van deze problemen wordt opgelost door moderne bestandssystemen, maar het kan nooit kwaad als een NAS zichzelf op een nette manier kan uitzetten als de stroom wegvalt.

iSCSI

Internet SCSI - het alternatief van SATA - ofwel de SCSI-opdrachten die normaliter meteen naar een harde schijf gaan, komen daar nu via het internet. We spreken over *target* ofwel ontvanger en *initiator* ofwel verzender van data. De iSCSI-ruimte kunnen we voorzien van een eigen bestandssysteem dat onafhankelijk is van wat de NAS intern gebruikt. Hier ligt waarschijnlijk de oplossing om data te versleutelen voordat deze op de NAS terechtkomen en daar dan geback-upt worden.

SNMP

Simple Network Management Protocol ofwel een systeem om allerlei apparaten via het netwerk in de gaten te kunnen houden. Hierboven gaven we al aan dat met name SMART- en Raid-toestand erg belangrijk zijn. Op een centrale computer kunnen deze en andere gegevens via SNMP verzameld worden en aldaar tot actie leiden.