

ct

ct

*IT-magazine
voor de
liefhebber*

7
2024

Acer Veriton N2590G
Mini-pc met Core i5-1335U

MULTI-GIGABIT NETWERKEN

- ▶ Maak je netwerk sneller
- ▶ Test van managed switches
- ▶ Technieken en interfaces

GETEST

- Laptopprocessors van AMD, Intel en Apple
- Acer Chromebook Plus 515
- 27"-monitoren met 4K en USB-C
- Shuttle DL30N mini-pc barebone met N100
- Asus Expertbook B3604CM laptop
- Deepcool AK500 Digital cpu-koeler

VIRTUALISATIE

- Kies de juiste software
- Aan de slag met Proxmox

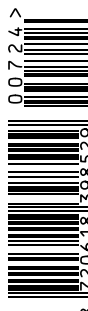
GROTE SSD-TEST

- Met PCIe 4.0 of 5.0
- Is sneller ook beter?

EN VERDER

- Windows krijgt sudo-commando
- Bouwvoorstel Core i-14000 kantoor-pc
- Emuleer een Atari ST
- Thunderbolt: zo werkt het
- Passkeys met opensource tools
- Secure Boot onder Linux

F&L



€8,99

Foscam T8EP, 4K UHD POE buiten beveiligingscamera



Spotlight



Weerbestendig ontwerp
voor buitengebruik



Mens/voertuig
detectie



Ondersteuning Amazon
Alexa en Google Home



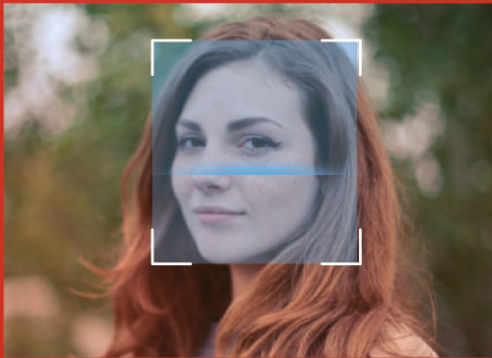
Tweeweg audio
voor communicatie



Nachtzicht



Voordelen Foscam:



Slimme detectie



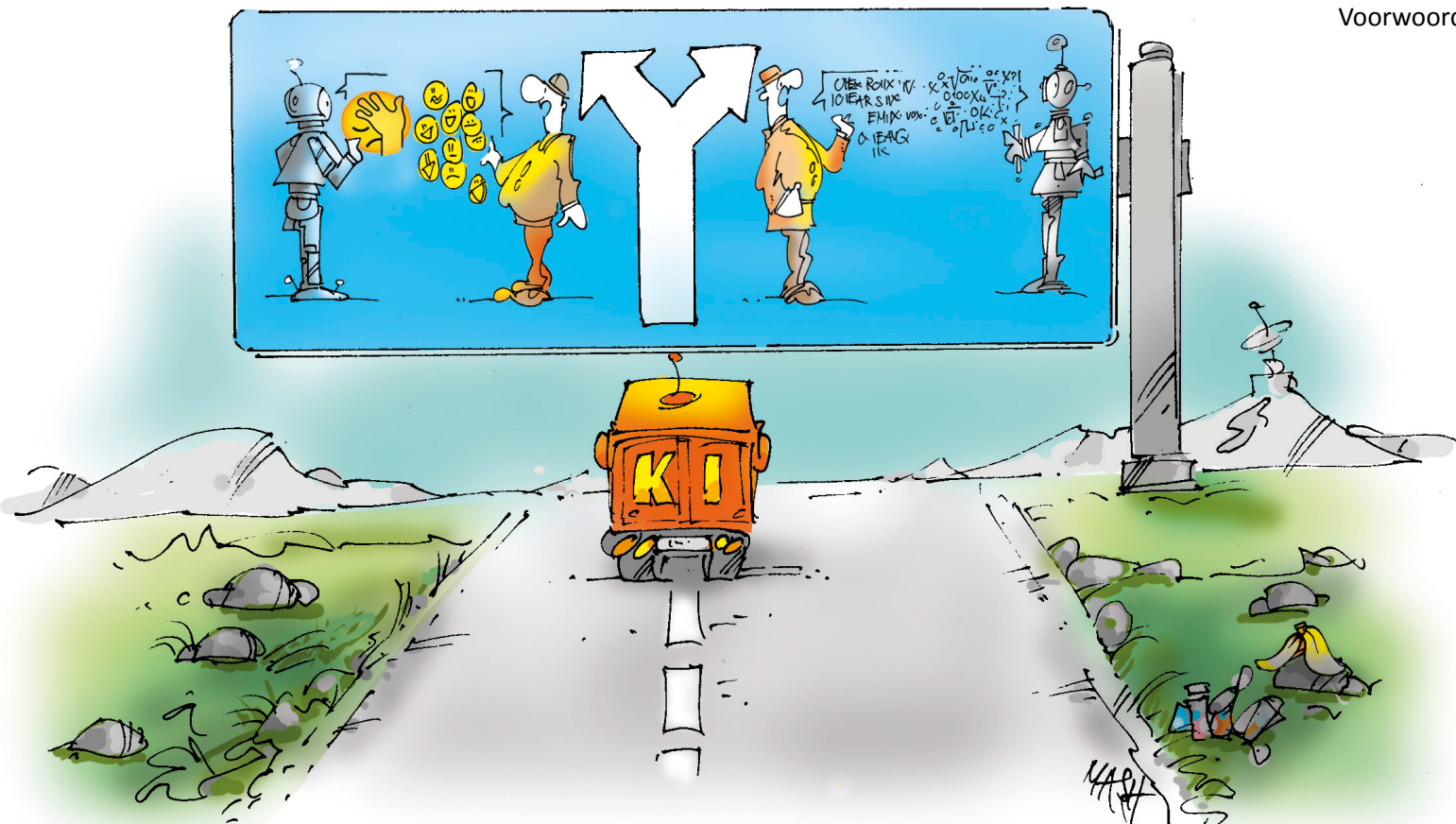
Hoge kwaliteit



Gratis Foscam app

Foscam familie





AI: genie of waanzin?

Generatieve artificiële intelligentie kan en mag mensen niet vervangen. Met die bewoordingen stellen veel bedrijven en brancheorganisaties ons in ieder geval eensgezind gerust. Om daar vervolgens meteen aan toe te voegen dat AI alleen diegenen zal vervangen die niet weten hoe ze het moeten gebruiken.

Dat is niet meer dan een schaamteloos dreigement: als je niet met je tijd meegaat, is jouw tijd gekomen. Degenen die daar van onder de indruk zijn en nu op de kar springen, daarbij denkend dat ze alle fouten en mislukkingen uit het verleden in één klap ongedaan kunnen maken met dure licenties voor tekst- en beeldgeneratoren, zouden over een paar jaar als de grote verliezers uit de bus kunnen komen.

Hoe meer machine-learning systemen zogenaamd kunnen denken en hoe meer menselijke vaardigheden ze simuleren, des te waakzamer en kritischer je moet worden. Ondanks al het enthousiasme over wat technisch mogelijk is, moet je je sterke punten behouden en zelf politieke en culturele ontwikkelingen blijven vormgeven, het wetenschappelijk denken promoten, verstandige beslissingen nemen en niet blindelings vertrouwen op technologie.

Met ChatGPT kun je redelijke teksten over allerlei onderwerpen schrijven, en dat ook in verschillende stijlen. Maar meestal leidt dat tot vrij doorsnee teksten met stereotype formuleringen – nog los van de noodzaak tot factchecking.

Je kunt met AI iedereen op een groepsfoto in de camera laten kijken en laten glimlachen. Maar dat leidt wel tot een eenheidsworst, waarbij alle diverse menselijke gezichtsuitdrukkingen gereduceerd worden tot dezelfde Mona Lisa-achtige glimlach.

Googles Med-PaLM 2 kan een groot aantal medische vragen beantwoorden, maar zijn de resultaten net zo goed als die van artsen? Zeker niet, tot nu toe werkt dat alleen voor gestandaardiseerde benchmarks.

En los daarvan zullen internationale medische platforms ons gezondheidszorgsysteem gegarandeerd niet redden, maar eerder uitknijpen als een citroen. Er zijn nu al veel huisartsen die het (te) druk hebben met het ontzenuwen van desinformatie bij hun patiënten.

Kortom, er zijn allerlei ontwikkelingen gaande waarbij AI een belangrijke rol kan en gaat spelen – maar nu nog even niet. De techbedrijven tonen met hun wanhopige zoektocht naar authentieke trainingsgegevens momenteel zelf aan hoe waardevol het menselijk origineel nog is.

Als je de grote taalmodellen voedt met door AI gegenereerde inhoud, degenereren ze na een paar keer trainen al zodanig dat ze alleen nog maar onzin uitkramen.

AI kan ons op dit moment ondersteunen bij veel alledaagse taken en dat is een goede zaak. Maar we moeten er wel voorzichtig mee zijn. Want als we teveel in een hoerastemming terecht dreigen te komen, kunnen we wel eens van een kouwe kermis terugkomen.

Veel plezier

Noud van Kruijsbergen

36

Multi-gigabit netwerken

Je NAS heeft een snelle 2,5Gbit/s-aansluiting en het moederbord van je pc ook, maar het versturen van grote bestanden gaat nog steeds met een trage 115 MB/s? Dat kan ook anders. We testen slimme switches voor multigigabit netwerken en geven uitleg over switchfuncties.

50

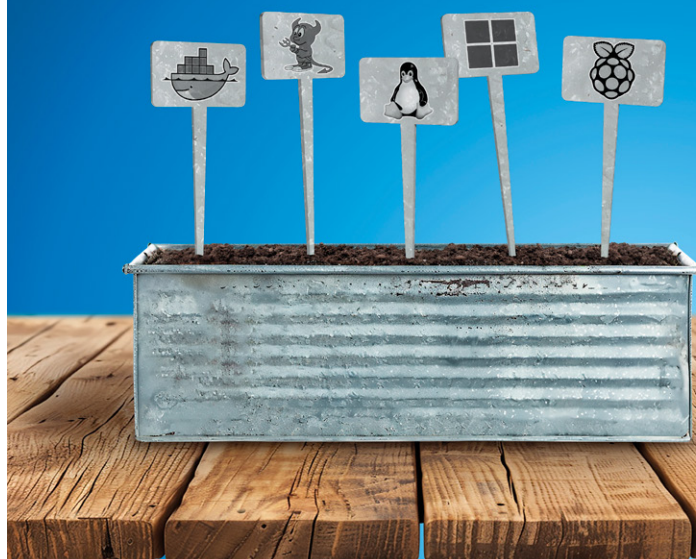
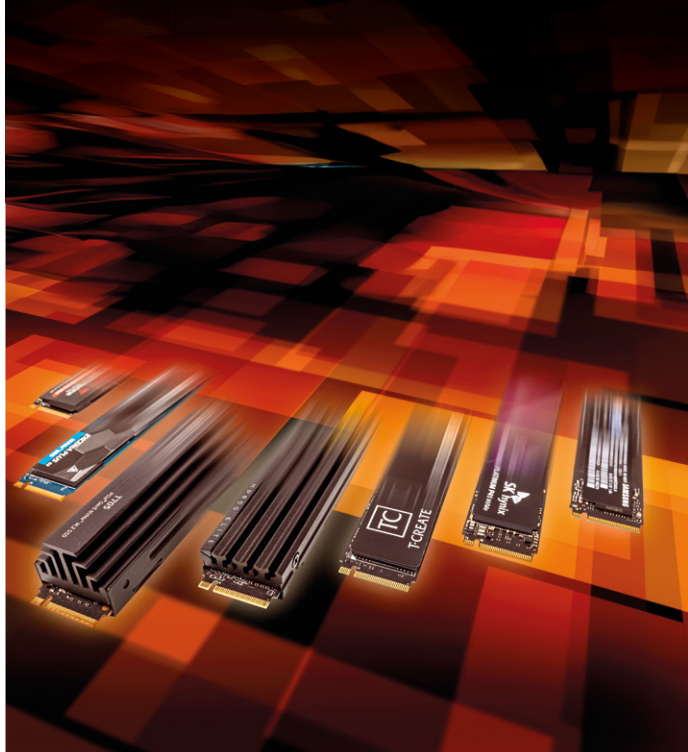
Grote ssd-test

PCIe 4.0 is tegenwoordig de standaard voor snelle ssd's. De koellichamen van de nog snellere 5.0-modellen worden steeds dikker en het geluidsniveau neemt ook toe: er is al een ssd opgedoken met twee ventilatoren.

78

Virtualisatie

VMware prijst zichzelf een beetje de markt uit door alleen nog abonnementen te verkopen of producten op te heffen. Op veel gebieden was het ook al niet meer toonaangevend. We bekijken de interessantste alternatieven: van desktopvirtualisatie met macOS-software tot de veelzijdige Proxmox-server. Veel daarvan is gratis of zelfs opensource.



Thema's

Multi-gigabit netwerken

- 36 Maak je LAN sneller
- 40 Slimme switches voor multi-gigabit netwerken
- 44 Uitleg over switchfuncties

Grote ssd-test

- 50 PCIe 4.0- en 5.0-ssd's getest

Virtualisatie

- 78 Virtualisatie: de juiste software
- 82 Introductie: Proxmox VE
- 86 Aan de slag met Proxmox VE

Nieuws

- 6 Algemeen
- 8 Hardware
- 10 Mobiel
- 12 Processors
- 14 Linux
- 32 Lifestyle
- 34 Surftips

Software

- 28 UTM: desktopvirtualisatie voor macOS
- 28 Blue Recorder 0.2.0 screenrecorder
- 30 Fedora 40 Workstation Linux-distributie
- 33 Apps
- 35 Game: No Rest for the Wicked
- 98 Windows krijgt sudo-commando
- 112 c't-rescue: tips en trucs om uit te breiden

Hardware

- 16 MeLE Quieter 4C F5Q mini-pc
- 16 Deepcool AK500 Digital cpu-koeler
- 17 Acer Veriton N2590G mini-pc
- 20 QNAP TBS-h574TX compacte NAS
- 20 Epos EXPAND Vision 1 usb-webcam
- 21 Acer Chromebook Plus 515
- 22 Palit GeForce RTX 3050 KalmX 6GB
- 22 Scythe Mugen 6 towerkoeler
- 23 Samsung Galaxy Book4 Pro 360 laptop
- 24 Asus ExpertBook B3604CM laptop
- 25 Shuttle XPC slim DL30N barebone
- 26 Dell Precision 7875 Tower workstation

- 27 Acer Connect Endureo M3 5G mobiele wifi
- 64 Laptopprocessors van AMD, Apple en Intel vergeleken
- 70 Twee 3D-printers getest
- 74 27-inch monitoren met 4K-resolutie en USB-C
- 92 Bouwvoorstel: stille en zuinige kantoor-pc
- 122 Mini-pc's via USB-C van stroom voorzien

Achtergrond

- 60 Hoe ChatGPT e.a. zuiniger kunnen gaan rekenen
- 102 DNS-record HTTPS is in gebruik genomen
- 106 Concepten en ontwikkelingen van Thunderbolt
- 108 Secure Boot en opstartproblemen onder Linux
- 140 Atari ST emuleren met FPGA-baord Tang Nano 20K

Praktijk

- 96 FAQ: NAS
- 118 De techniek-wirwar van Outlook-add-ins
- 126 Passkeys gebruiken met opensource tools
- 130 Thuisnetwerkgrenzen overwinnen met OpenWrt
- 136 Tips en trucs

Vaste rubrieken

- 3 Voorwoord
- 4 Inhoud
- 145 Colofon
- 146 Volgend nummer



- 24 Asus ExpertBook B3604CM laptop
- 27 Acer Connect Endureo M3 5G mobiele wifi
- 44 Uitleg over switchfuncties
- 86 Aan de slag met Proxmox VE
- 102 DNS-record HTTPS is in gebruik genomen
- 118 De techniek-wirwar van Outlook-add-ins
- 126 Passkeys gebruiken met opensource tools
- 130 Thuisnetwerkgrenzen overwinnen met OpenWrt

Abonnement afsluiten?

Kijk voor actuele aanbiedingen op www.ct.nl/abo

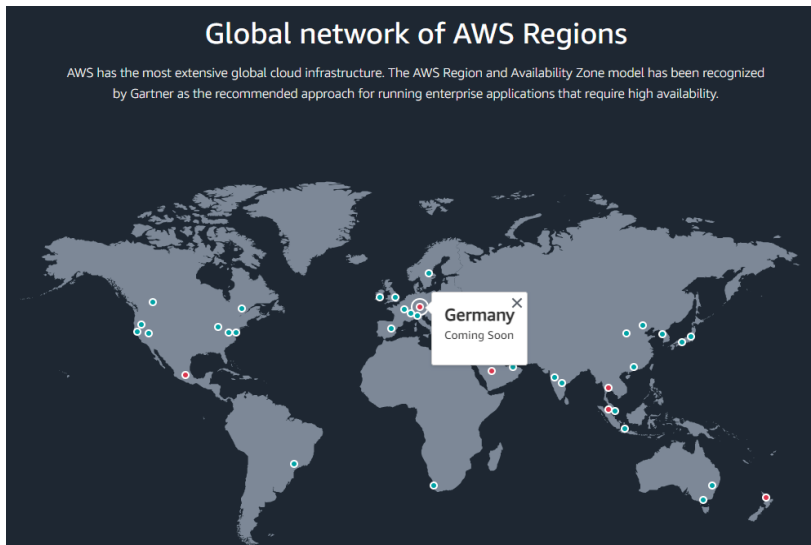
Cloudtak Amazon investeert in Europese cloud

De cloudtak van Amazon (Amazon Web Services, AWS) heeft een nieuwe CEO gekregen en kondigt de European Sovereign Cloud aan, een divisie die onafhankelijk gaat draaien. Adam Selipsky is vervan-

gen door Matt Garman. German werkt al sinds 2005 bij Amazon: hij kwam binnen als stagiair en werkte later fulltime als productmanager bij Amazon Web Services, later als manager voor marketing, support, sales en professionele diensten.

AWS gaat 7,8 miljard euro investeren in de European Sovereign Cloud, en het wordt een onafhankelijke cloud om te helpen voldoen aan alle EU-regelgeving. Het is geen geheim dat er van diverse kanten kritiek werd geuit door gebruikers die hun data niet bij Amerikaanse bedrijven mogen, willen of kunnen parkeren. De European Sovereign Cloud wordt opgezet en onderhouden door Europese werknemers, en gaat voldoen aan alle EU-eisen om alle klantdata en metadata in de EU te houden. Er komt onder andere een AWS-regio in Duitsland (Brandenburg), waar de eerste 7,8 miljard aan investering naartoe gaat. De schatting van Amazon is dat er in totaal 17,2 miljard in de European Sovereign Cloud wordt gepompt.

Amazon Web Services bestaat sinds 2006 en is actief in 102 zones in 32 geografische regio's en biedt diensten voor onder andere cloudopslag, databases, netwerken, analytics, machine learning, AI, IoT en VR en AR.



Amazon Web Services gaat flink investeren in de Europese cloud, waaronder in een nieuwe AWS-regio in Duitsland.

Facebook en Instagram: verslavend voor kinderen?

Het klinkt een beetje als een open deur, maar de Europese Commissie gaat Meta aan een onderzoek onderwerpen omdat er zorgen bestaan dat Facebook en Instagram verslavend gedrag bij kinderen kunnen veroorzaken. Sowieso is de EC bezorgd over de manier waarop Meta controles uitvoert op de leeftijd van gebruikers en de identiteit.

Meta heeft al eerder veel informatie verstrekt op navraag van de Europese Commissie, en die gegevens zijn nu de aanleiding om een zeer diepgravend onderzoek te starten. De Europese Commissie geeft wel aan

dat het starten van een onderzoek niet gelijk staat aan een beschuldiging aan het adres van Meta. Er wordt ook onderzocht of Meta voldoet aan de nieuwe DSA-wet waarbij de privacy en veiligheid voor minderjarigen moet worden gewaarborgd.

Na het afronden van het onderzoek wordt er dan besloten of er wordt ingegrepen en of dat er een straf wordt uitgedeeld. Een overtreding van de DSA-wet kan tot 6 procent van de jaaromzet aan boete opleveren, wat bij Meta kan uitkomen op een bedrag van ruim 7 miljard euro.

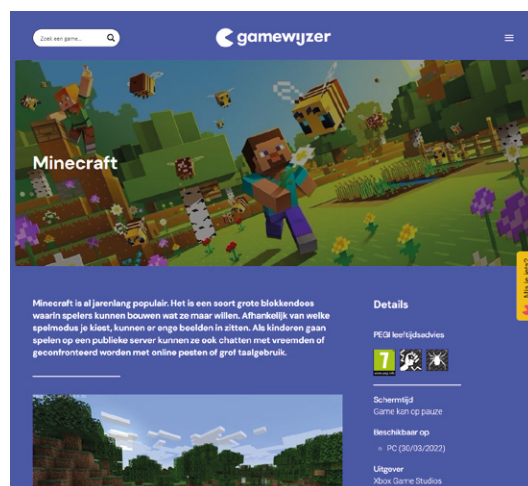
Gamewijzer gelanceerd

We kennen de Kijkwijzer voor films, series en tv-programma's, en van dezelfde makers (het Nederlands Instituut voor de Classificatie van Audiovisuele Media) is nu de Gamewijzer beschikbaar via

gamewijzer.nl. Die website biedt ouders en opvoeders informatie en tips over hoe ze moeten omgaan met games en gamende kinderen.

Er bestaat al het PEGI-systeem voor leeftijdsclassificatie voor games. Die geeft aan in hoeverre er voor kinderen ongewenste elementen in games zijn opgenomen. Kijkwijzer had een overzicht over games met wat informatie, maar dat is nu losgekoppeld. Ook bleek er veel behoefte te zijn aan een Kijkwijzer voor games. De Gamewijzer is vooral bedoeld voor voorlichting.

Per game wordt aangegeven of kinderen betaalde aankopen kunnen doen of in contact kunnen komen met anderen, wat kan leiden tot online pesten of grof taalgebruik. Alle varianten van de games worden besproken met uitleg, waaronder over hoe je afspraken kunt maken over schermtijd (is er een pauze-optie, is het mogelijk om tussentijds op te slaan) en of je ouderlijk toezicht kunt instellen. Er is ook een gamewoordenboek aanwezig waarin de diverse (in)game-termen duidelijk worden uitgelegd.





VERBIND EN WERK SAMEN MET GEMAK



De **ProLite XUB2790QSUH** is niet alleen een geweldige monitor voor communicatie, maar ook voor productiviteit en comfort.

Deze 27-inch IPS-monitor is de perfecte keuze voor thuiswerkers die behoefte hebben aan een beeldscherm van hoge kwaliteit en een naadloze verbinding. De monitor heeft een ingebouwde 1080p-webcam en microfoon die compatibel zijn met Windows Hello, zodat u zich in één oogopslag kunt aanmelden en binnen enkele seconden kunt beginnen met videoconferenties. Het heeft ook ingebouwde luidsprekers die duidelijk en helder geluid leveren voor uw gesprekken en entertainment. Deze QHD (2560x1440)-monitor is voorzien van een in hoogte verstelbare voet met draaifunctie, flikkervrije LED's en een blue light reducer die vermoeide ogen en overbelasting vermindert, zodat u elke dag comfortabel kunt werken.



Vind uw monitor op
www.iiyama.com

Sennheiser HD 620S

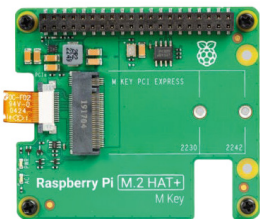
De populaire HD600-reeks van Sennheiser is uitgebreid met de HD 620S. Die koptelefoon is gericht op audiofielen en voldoet aan de vraag naar een HD 600-serie koptelefoon die je ook kan afsluiten van afleidingen. De gesloten koptelefoon heeft een typisch serie 600-design met een fijn draagcomfort en geen optische poespas. De hoofdband is versterkt met metaal, net als de oorschelpbehuizingen. De kabel van 1,8 meter met 3,5mm-jack (en meegeleverde 6,2mm-adapter) is afneembaar, waardoor je kunt kiezen voor diverse kabellengtes en kabels met inline-microfoon. Hij is op te bergen in de meegeleverde opbergtas. Binnenkort verschijnt er ook nog een gebalanceerde 4,4mm-kabel voor het gebruik in combinatie met specifieke hifi-apparatuur.

Het hart van de HD 620S wordt gevormd door de 42mm dynamische transducer, die zorgt voor zowel een authentiek geluid als een diepe uitgesproken bas, met krachtige dynamiek over het complete frequentiespectrum. Dat maakt de HD 620S niet alleen



geschikt voor audiofielen, maar ook gamers die zoveel mogelijk details willen oppikken. De Sennheiser HD 620S heeft een adviesprijs van 350 euro.

NVMe voor de Pi: M.2 HAT+-module



De verkoop van een M.2-module voor de Raspberry Pi is gestart: de M.2 HAT+-module maakt het mogelijk om een NVMe-ssd aan te sluiten op een Raspberry Pi. Er is uitvoerig getest met diverse ssd's, maar ook andere PCIe-apparaten, voordat het product beschikbaar is gemaakt. Dankzij de FFC-connector (flexible flat cable) op de Raspberry Pi 5 sluit je de pcb-module met een flatcable aan op het PCIe-slot van de Pi 5. Door de PCIe 2.0-interface met een enkele lane haal je wel maar maximaal 500 MB/s, maar dat is voor de

meeste toepassingen waarvoor een Raspberry Pi wordt ingezet meer dan voldoende.

Via de HAT+-module kun je een ssd in 2230- of 2242-formaat aansluiten. De Hat+-module levert tot 3 ampère aan het aangesloten device. Een NVMe-ssd is ook bruikbaar als bootdevice voor je Pi. Zorg dan wel dat je de laatste firmware draait. De module kan dankzij de spacers bovenop een Pi met actieve koeling worden gemonteerd. De M.2 HAT+-module is verkrijgbaar voor een prijs tussen 12 en 15 euro.

LG UltraGear 32" dual-mode oled-scherm

De LG UltraGear 32-inch 32GS95UE-B met dual-mode oled-scherm is nu eindelijk ook in de lage(re) landen beschikbaar geworden. Het matte 4K-scherm (3840 × 2160 pixels) haalt 240 Hz, maar heeft een bijzonder trucje. Het scherm is met een druk op de knop om te schakelen naar een full hd-resolutie met 480 Hz.



Daardoor kun je afhankelijk van je kijk- of gamingwensen wisselen naar de meest geschikte modus.

Het scherm biedt FreeSync Premium Pro en G-Sync (compatible) en DisplayHDR True Black 400 en is qua kleuren al gekalibreerd in de fabriek. De responstijd ligt op 0,03 ms (GtG). De standaard helderheid ligt op 275 nits met een piekhelderheid van 1300.

De monitor heeft een DisplayPort-aansluiting (versie 1.4), twee keer HDMI 2.1, een usb-hub en een 3,5-mm audiojack die je van onderaf in de behuizing prikt. Hij biedt ook twee ingebouwde speakers van elk 10 W die het panel zelf laten trillen, waardoor het geluid uit het scherm lijkt te komen. Het scherm is eenvoudig ontworpen met een vrijwel randloos design zonder overbodige toeters en bellen. De achterkant heeft een tweetal lichtstroken.

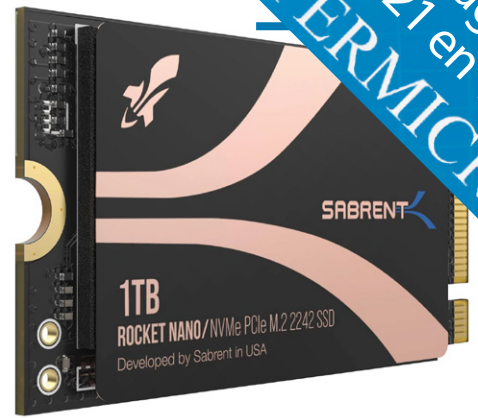
De voet is stevig en ruimtebesparend. Het scherm kan worden gekanteld, zijwaarts worden gedraaid, verticaal worden gedraaid en in hoogte worden veresteld. Een VESA-mount optie (10 bij 10 centimeter) is aanwezig.

Het scherm verbruikt maximaal 60 watt en bij gemiddeld gebruik 55 watt. In de slaapstand wordt er minder dan een halve watt uit het stopcontact getrokken. De LG UltraGear 32GS95UE-B gaat 1400 euro kosten.

Sabrent Rocket Nano 4-ssd

De Sabrent Rocket Nano 4 is een compacte PCIe 4.0 M.2 2242-ssd die gericht is op compacte apparaten (zoals een NUC) en gaming-handhelds zoals de Lenovo Legion Go. De Nano 4 heeft een DRAM-loze Phison E27T-controller, bevat 3D NAND en Sabrent meldt een snelheid tot 5 GB/s – maar geeft geen specifieke lees- en schrijfsnelheden.

Met een adapter is de compacte ssd uiteraard altijd nog te verlengen tot 2280-formaat zodat hij in vrijwel elk normaal desktopmoederbord gestopt kan worden. Er is voorlopig alleen nog maar een 1TB-versie aangekondigd, die 100 dollar gaat kosten.



Zie pag 11, 13, 121 en 147
SUPERMICR

Thunderbolt Share

Intel gaat het mogelijk maken om twee pc's via Thunderbolt direct aan elkaar te koppelen en op die manier via een software-oplossing meerdere handige opties te bieden. Intel heeft die techniek Thunderbolt Share gedoopt. Verbinden kan direct of via een dockingstation of monitor, waarbij elk apparaat Thunderbolt 4 of 5 moet ondersteunen en Windows 10 of 11 moet draaien.

Thunderbolt Share gaat een viertal opties mogelijk maken. Zo kun je de andere pc bedienen, waarbij het beeld zonder enige vorm van compressie wordt overgestuurd. Bij 1080p is 60 Hz mogelijk, daarboven hangt het af van de hardware van de gebruikte pc's.

Ook wordt het mogelijk om met een eenvoudig te gebruiken interface mappen te synchroniseren, bestanden over te hevelen via een soort dualpane-Verkenner en data over te zetten van een oude naar een nieuwe pc. Intel maakt dat mogelijk via software die in licentie beschikbaar wordt voor pc-fabrikanten of fabrikanten van Thunderbolt-accessoires. De software moet als je dit leest beschikbaar zijn. Bij aanschaf van een apparaat met Thunderbolt Share-certificering mag je de software op twee pc's installeren.

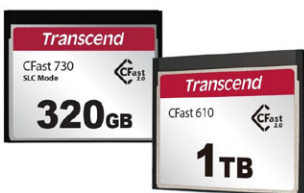
De beveiliging van de verbinding wordt geregeld via op VT-d gebaseerde databescherming. Er is al een aantal fabrikanten bezig met apparaten die de Thunderbolt Share-functies gaan bieden, waaronder Acer, Belkin, Kensington, Lenovo, MSI en Razer.



Transcend CFX730 & CFX610 CF-kaarten

De Transcend CFX730 en CFX610 CFast-kaarten zijn gericht op data-integriteit en duurzaamheid, specifiek voor gaming- en entertainment-apparatuur, medische apparaten en systemen die 24/7 draaien. Ze voldoen aan de CFast 2.0-specificatie. De capaciteit loopt van 20 GB tot 320 GB voor de CFX730 en 64 GB tot 1 TB voor de CFX610. De CFX730 heeft een SL-mode die een endurance tot 100K program/erase cycles en een stabiele schrijfperformance garandeert, voor bijvoorbeeld embedded systemen.

De CF-kaarten zijn ook beschikbaar in Wide Temperature-versies met een vergrote temperatuurrange van -40 tot 85 graden. Beide kaarten bieden een write protection-functie om data tegen per ongeluk wissen te beschermen en bad block-management om de levensduur te verlengen. De LDPC ECC-engine detecteert datafouten. Hardwarematige AES-encryptie is beschikbaar. De kaarten hebben drie jaar garantie. De prijzen waren op het moment van schrijven nog niet bekend.



SanDisk Desk Drive 4 & 8 GB

Voor grotere hoeveelheden back-upstorage komt Western Digital in het SanDisk-portfolio met de SanDisk Desk Drive. Die externe ssd is beschikbaar in twee capaciteiten: 4 en 8 TB. De Desk Drive biedt via USB-C Gen 2 snelheden tot maximaal 10Gbit/s (tot 1000 MB/s) en is compact genoeg om relatief opvallend een plekje op je bureau te krijgen met 9,9 bij 9,9 bij 4,0 centimeter. Hij weegt 268 gram. Zijn design doet wat denken aan een streamingbox, hij heeft een rubberen onderkant tegen wegglijden.

Je kunt hem veilig vastmaken met een Kensington-slotuitsparing. De ssd moet wel extern van de no-

dige energie worden voorzien: een compacte adapter wordt meegeleverd, net als een USB-C-kabel en adapter naar USB type A.

Voor het maken van back-ups wordt software van Acronis meegeleverd. De externe ssd heeft een garantietermijn van 3 jaar.

De 4TB-versie kost zo'n 425 euro, de 8TB-versie gaat voor 780 euro over de toonbank.



Goedkopere Pixel

Net als bij Apple zijn ook Googles Pixel-smartphones steeds prijziger geworden. Naast de Pixel 8 (vanaf 800 euro) en Pixel 8 Pro (vanaf 1100 euro) heeft Google onlangs een nieuwe model geïntroduceerd in de goedkopere a-serie: de Pixel 8a. De vanaf-prijs van 550 euro is alleen in relatieve zin 'goedkoper' te noemen en zit alsnog aan de bovenkant van de middenklasse. Het kan echter een aantrekkelijk alternatief zijn voor de duurdere modellen.

Alle drie de modellen hebben dezelfde Google Tensor G3-cpu, waardoor de prestaties overeenkomen. Het Pro-model presteert in sommige gevallen iets beter omdat het 12 GB RAM heeft in plaats van 8 GB. Vooral in vergelijking met de non-Pro Pixel 8 mis je echter weinig bij de Pixel 8a. Het scherm heeft dezelfde 120Hz maximale verversingsfrequentie, al is die bij de 8a adaptive van 1-120 Hz terwijl de 8 schakelt tussen 60/120 Hz. De resolutie is hetzelfde en het scherm van de 8a is met 6,1 inch slechts 0,1 inch kleiner. Dankzij het meer premium design met dunnere randen is de Pixel 8 echter een iets kleiner toestel.

Andere verschillen zijn een lagere IP-rating voor de 8a en andere camerasensors. Bij de Pixels is het echter vooral Googles software die zorgt voor prima foto's. De Pixel 8a verschilt verder alleen in details, zoals een lagere oplaadsnelheid en de beschikbare



kleuren: Aloë (groen), Baaiblaauw, Obsidiaan (zwart) en Porselein (wit).

Net als andere recente Pixels krijgt de Pixel 8a zeven jaar lang functiereleases en beveiligingsupdates, de langste ondersteuningstermijn voor Android-smartphones naast Samsung. Nieuwe softwarefuncties voor Android verschijnen vaak eerst exclusief op de Pixels.

Uiteraard mag de term AI niet ontbreken: de Pixel Camera met AI biedt allerlei trucs om je foto's en video's te bewerken en verbeteren, zoals onderwerpen in foto's weghalen of verschuiven, storende geluiden zoals wind uit video's halen en speciale nachtfoto's maken. Ook op andere plekken zoals bij het zoeken ('circle-to-search') wordt AI ingezet. De Pixel 8a is ook voor Nederland en België uitgebracht en via de betreffende online Google Store beschikbaar.

Nieuwe iPads

Voor het eerst in lange tijd (eind 2022) heeft Apple nieuwe iPads uitgebracht: de iPad Pro 2024 en de iPad Air 2024. Beide zijn voorzien van een snellere chip dan de voorganger: de Air heeft een M2-SoC en de Pro de nieuwe M4. Het Pro-model heeft bovendien een oled-display en is aanzienlijk lichter en dunner geworden (5,3 mm voor het 11-inch model, 5,1 mm voor 13-inch). Daardoor is het voordeel van draagbaarheid ten opzichte van een MacBook weer groter, ook al neem je accessoires mee zoals het nieuwe Magic Keyboard. De eveneens nieuwe Pencil Pro werkt met beide modellen.

De iPad Air 2024 is in twee formaten te koop met prijzen vanaf 719 euro voor het 11-inch-model en 969 euro voor de 13-inch-versie. De iPad Pro 2024 begint vanaf 1219 euro voor het 11-inch-model en 1569 euro voor de 13-inch.



(G)een stapje terug



Apple en Samsung hebben wereldwijd met afstand het grootste marktaandeel bij smartphones, Apple haalde in 2023 de helft van alle inkomsten binnen. Terwijl allerlei fabrikanten zoals LG, Nokia en Motorola zijn gestopt met smartphones of hun merknaam verkocht hebben aan Chinese fabrikanten, is Sony ondanks terugkerende berichten die het tegendeel beweren nog niet uit de smartphonemarkt gestapt. Er is weer een nieuw topmodel verschenen in Sony's Xperia-smartphonereeks, de Xperia 1 VI.

Sony bewandelt bij smartphones een eigen pad: zo krijg je bij Sony nog steeds een scherm zonder cameragat of-notch, maar met dunne randen om het scherm. Ook de beeldverhouding is apart: Sony heeft de extreem langgerekte 21:9 verhouding bij de Xperia 1 VI laten varen, maar 19.5:9 is wederom afwijkend. Bij de resolutie doet Sony een stapje terug en krijg je niet meer de (onnodig hoge) 4K van vorige modellen,

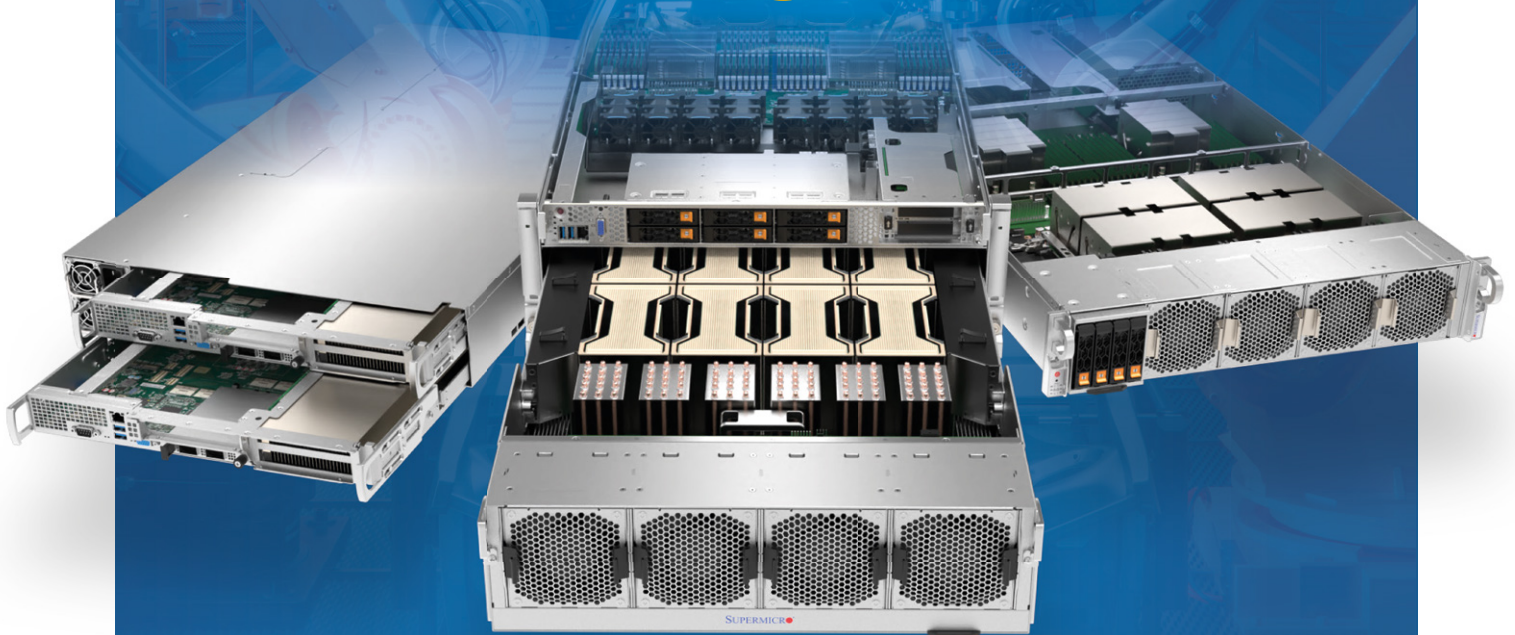
maar FHD+ met 1-120 Hz verversingsfrequentie. In de nieuwste iPhones, Galaxy's en andere top-smartphones en uiteraard in deze Xperia zitten camerasensors van Sony. Vooral de optische zoom van de telelens met 85-170 mm equivalent is bijzonder.

In tegenstelling tot bij veel fabrikanten is er relatief weinig AI aanwezig in de camera-software, die bij de Xperia is teruggebracht tot een enkele app. Het toestel heeft alle specificaties van een topmodel, zoals de nieuwste Snapdragon 8 Gen 3 en 12 GB RAM. Sony biedt nog steeds een 3,5mm-hoofdtelefoonaansluiting en veel audiotechniek zoals 360 Reality Audio en Hi-Res wireless audio.

Sony wijkt helaas ook af van de trend van steeds langere ondersteuning: doorgaans krijg je slechts 2 jaar Android-updates en 3 jaar beveiligingsupdates. Met een prijs vanaf 1400 euro zal dit toestel de smartphonemarkt dan ook moeilijk gaan veranderen.

SUPERMICRO

AI Building Blocks



Construct Your Optimized AI Solutions
from the Largest NVIDIA-Certified Systems™ Portfolio

SMBE Belgium

+32 495 533 245
www.smbe.be
sales@smbe.be

TWP Computer

+31 20 638 9057
www.twp.nl
info@twp.nl

Server Storage Solution

+32 9 261 5310
www.s3s.be
sales@s3s.be

NCS International

+31 544 47 0000
www.ncs.nl
info@ncs.nl

ServerDirect BV

+31(0) 85-3018585
www.ServerDirect.nl
sales@serverdirect.nl



Learn More at www.supermicro.com

© Supermicro and Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries.

DOLGEDRAAID

BIOS-updates voor defecte Intel-processors

Fabrikanten van moederborden reageren op instabiliteit in processors uit de Core i-13000K en Core i-14000K series met een nieuw BIOS-profiel, waardoor de processors volgens de specificaties van Intel kunnen draaien. Er is echter nog niemand die de verantwoordelijkheid op zich neemt voor Intels jarenlange veronachtzaming van de specificaties.

Christian Hirsch en Noud van Kruysbergen

An het begin van het jaar doken er meldingen op van gebruikers van wie de Core i-processors onstabiel draaiden. Vooral de overklokbare K-modellen van de 13e en 14e generatie, zoals de Core i9-14900K, zijn getroffen. Er is geen duidelijk foutpatroon, maar er verschijnen meldingen van vermeend onvoldoende grafisch geheugen bij 3D-games gebaseerd op Unreal Engine 5 of blauwe schermen bij het compileren van software. De problemen worden vaak pas na een paar weken of maanden duidelijk op systemen die de Intel-processors automatisch overklokken, waar veel eigenaren zich niet van bewust zijn. Met de specificaties op de cpudatasheets draaien de computers wel stabiel. Toch raken de processors beschadigd en daarom vervangt Intel ze na een klacht.

In een bericht aan pc- en moederbordfabrikanten vraagt Intel hen nu om alle grenswaarden van de cpu's na te leven en standaard beschermende functies te activeren. Dat zou eigenlijk vanzelfsprekend moeten zijn. In reactie daarop verspreiden de moederbordfabrikanten Asus, Gigabyte en MSI BIOS-updates die een zogeheten baseline-profiel toevoegen, waarmee de cpu's conform de specificatie draaien. Je moet dat echter zelf activeren.

Fabrikanten hebben dat probleem zelf veroorzaakt omdat de meeste moederborden de K-modellen van de Core i-processors al jaren laten werken met utopisch hoge limieten voor vermogen en stroom, die de toch al hoge Intel-aanbevelingen van 253 watt en 307 ampère ver overschrijden. Intel heeft dat jarenlang getolereerd.

We wijzen bij elke moederbordtest al jaren op die riskante standaardinstellingen. De zuinigste borden en voedingen hebben echter weinig nut als de Intel-specificaties voor Turbo Boost 2.0 en de limieten voor het Thermal Design Power (TDP) van de processors onder volledige belasting worden genegeerd. Het gevolg is dat de processors buiten de specificatie draaien, door het hogere energieverbruik kunnen ze oververhit raken en daardoor minder goed presteren. In geval van problemen bemoeilijkt dat ook de foutdiagnose. Daarnaast is het voor de meeste gebruikers onmogelijk om de juiste waarden in te stellen tussen de vele overklokinstellingen bij de BIOS-instellingen, zodat de cpu volgens de specificaties van Intel draait.

Bij processorstests zorgen we er daarom voor dat Power Limit 1 (PL1), Power Limit 2 (PL2), Turbo Window Duration (PLTau) en Maximum Current (IccMax) correct ingesteld zijn. We zijn zelfs verschillende keren bekritiseerd voor het 'kunstmatig vertragen van processors'. Het is geen verrassing dat de problemen die gepaard gaan met overklokken nu aan het licht komen.

Maar waarom houden moederbordfabrikanten zich niet gewoon aan die richtlijnen? Daar is Intel deels schuldig aan. In een interview met het Amerikaanse online



tijdschrift Anandtech in 2019 legde Guy Therien (hij is een Intel Fellow en Chief Architect, Performance Segmentation) uit dat het binnen Intels specificaties valt voor moederbordfabrikanten om de vermogenslimieten te overschrijden. Volgens hem vindt overklokken alleen plaats wanneer hogere klokmultiplicatieniveaus worden ingesteld dan de niveaus die standaard worden geleverd.

Het verhogen van de vermogens- en stroomlimieten leidt in de praktijk echter ook tot hogere klokfrequenties. Dat snelheidsvoordeel van meestal maar een paar procentpunten wordt graag geaccepteerd door de moederbordfabrikanten, maar vermoedelijk ook door Intel. Het nadeel is echter voor minder technisch onderlegde gebruikers die hoge elektriciteitsrekeningen, duurdere koeling en krachtigere voedingen betalen of zelfs worstelen met instabiliteit.

AMD laat zien hoe het beter kan. Al zijn moederborden voldoen aan de AMD-specificaties af fabriek, die niet alleen gelden voor de vermogenslimiet, maar ook voor de maximale stroom en korte stroompieken. Onze vraag aan Intel is dan ook om moederbordfabrikanten te verplichten ervoor te zorgen dat elke processor voldoet aan de publiekelijk gedocumenteerde limieten met de fabriekinstellingen van het BIOS. **ct**



www.ct.nl/softlink/2407012

Performance-invloed baseline-profiel

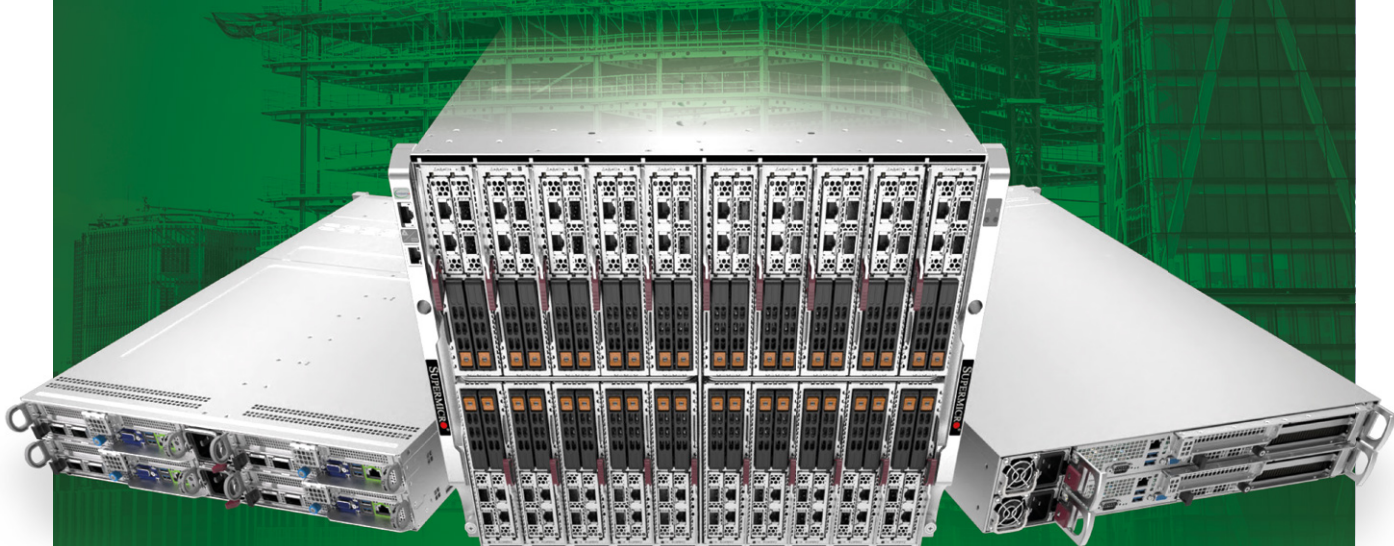
Profiel	Voorinstellingen	Cinebench 2024 [punten]	Energieverbruik [W]
		beter ►	◄ beter
BIOS defaults	PL1=253 W, PL2=4095W, PLTau=165s, Iccmax=512A	2152	405
Intel baseline	PL1=253 W, PL2=253W, PLTau=56s, Iccmax=280A	2003	319

hardware: Core i9-14900K, Asus ROG Strix Z790-E Gaming WIFI, 32 GB DDR5-5600, ssd

SUPERMICRO

HIGH PERFORMANCE

Building Blocks



Construct Your Optimized IT Solutions
from World Record Performance HPC Systems

SMBE Belgium

+32 495 533 245
www.smbe.be
sales@smbe.be

TWP Computer

+31 20 638 9057
www.twp.nl
info@twp.nl

Server Storage Solution

+32 9 261 5310
www.s3s.be
sales@s3s.be

NCS International

+31 544 47 0000
www.ncs.nl
info@ncs.nl

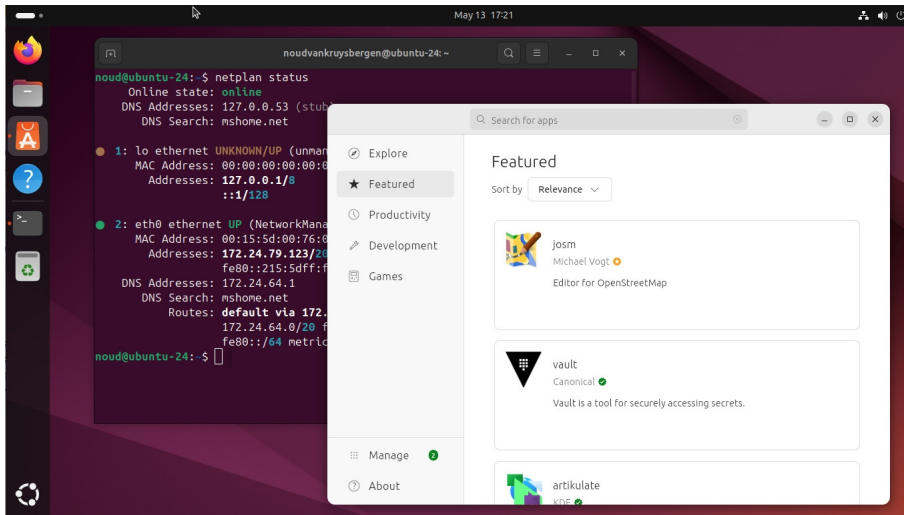
ServerDirect BV

+31(0) 85-3018585
www.ServerDirect.nl
sales@serverdirect.nl

SUPERMICR

Learn More at www.supermicro.com

© Supermicro and Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries.



CONSEQUENTE EVOLUTIE

Ubuntu Desktop 24.04 LTS

Canonical heeft veel functies van Ubuntu Server geïntegreerd in Ubuntu Desktop 24.04 LTS, iets waar desktopgebruikers ook van zullen profiteren. Als je wilt upgraden van een oudere versie moet je echter nog even wachten.

Niklas Dierking en Noud van Kruysbergen

Canonical heeft de nieuwe versie Ubuntu 24.04 LTS Noble Numbat uitgebracht, die standaard vijf jaar lang van updates zal worden voorzien. Als je een Ubuntu Pro-abonnement neemt, dat gratis is voor particulieren en maximaal vijf machines, krijg je 10 jaar lang beveiligingsupdates (Expanded Security Maintenance). Met de betaalde add-on voor Ubuntu Pro kun je de ondersteuning tot twaalf jaar verlengen.

UBUNTU LIGT OP SCHEMA

Het nieuwe installatieprogramma maakte zijn debuut al bij Ubuntu 23.10, maar heeft een paar nieuwe trucjes geleerd. Nadat je je eigen taal hebt geselecteerd, vraagt het installatieprogramma nu of je de toegankelijkheidsfuncties wilt activeren, zoals een verhoogd contrast, een schermvergroter of een schermlezer.

Het gebruikt hetzelfde back-end (Subiquity) als de serverversie. Daardoor vinden steeds meer functies uit de serverwereld hun weg naar de desktop. Een hoogtepunt is de nieuwe automatische installatie, die

beheerders en power-users zal bevallen. Dan geef je het installatieprogramma een bestand mee met de naam `autoinstall.yaml`, bijvoorbeeld vanuit een GitHub-repository of via je eigen webserver, dat dient als blauwdruk voor de Ubuntu-installatie. Het bevat de netwerkconfiguratie, de te installeren software en nog veel meer, zodat je meestal geen eigen ISO-images meer hoeft te maken als je Ubuntu op meerdere machines installeert.

Bij het instellen van de schijven biedt het installatieprogramma opnieuw het ZFS-bestandssysteem en je kunt de TPM (Trusted Platform Module) gebruiken om de harde schijf volledig te versleutelen. Beide opties zijn daarbij nog experimenteel. TPM-encryptie heeft nog steeds te lijden onder het feit dat het niet werkt met externe kernelmodules. De eigen driver voor grafische Nvidia-kaarten is daarom niet beschikbaar.

Bij de interactieve installatie is de optie 'Default selection' nu standaard. Die bevat alleen een Firefox-snap en een paar hulpprogramma's. Mozilla's Thunderbird

volgt Firefox en is ook alleen beschikbaar als snap. De webcamapplicatie Cheese vangt Snapshot. De Gnome Games-collectie is verwijderd.

De trend naar declaratieve configuratie zet zich zelfs na het installeren voort. Bij Ubuntu 24.04 laat Canonical gebruikers kennismaken met NetPlan 1.0, een abstractielaag voor netwerkconfiguratie. NetPlan haalt zijn informatie uit een YAML-bestand en vertaalt de configuratie vervolgens naar de syntaxis van het betreffende back-end, bijvoorbeeld de NetworkManager. Ubuntu 24.04 LTS heeft veel vernieuwingen op de desktop te danken aan de Gnome 46-desktopomgeving.

(SN)APP CENTER

Als je overstapt van Ubuntu 22.04 naar 24.04 maak je kennis met het nieuwe App Center (applicatiecentrum). De app-store is vooral gericht op het installeren en beheren van snap-pakketten. De ontwikkelaars hebben updates voor apparaatfirmware uitbesteed aan een aparte applicatie.

Online lees je vaak dat je klassieke Debian-pakketten niet meer kunt installeren of verwijderen met het App Center. Dat klopt niet, maar de ontwikkelaars doen wel moeite om het je niet makkelijk te maken. Als je bijvoorbeeld naar VLC zoekt, toont het App Center in eerste instantie alleen het snap-pakket. Als je echter op 'See all results' klikt, kun je de resultaten filteren op Debian-pakketten. De geïnstalleerde snaps worden weergegeven bij het menu Manage, om een Debian-pakket met het App Center te verwijderen, moet je er opnieuw naar zoeken.

CONCLUSIE

Als je een oudere Ubuntu-versie wilt upgraden naar 24.04 LTS moet je nog even wachten. Canonical zelf adviseert om te wachten tot de eerste zogeheten point-release (24.04.1), die gepland staat voor augustus.

Ubuntu 24.04 LTS is de volgende stap op weg naar Canonicals visie van een Linux-distributie die lang meegaat, waar geen expertkennis voor nodig is en die ook geschikt is voor beheerde werkstations. Door desktop en server samen te voegen en te focussen op snap, vermindert de distributeur ook de onderhoudsinspanning voor zijn eigen ontwikkelaars.

Ubuntu 24.04 LTS is al met al geen baanbrekende release met killer-features, maar dat hoeft ook niet. Als je geen problemen met snap hebt, biedt de nieuwe Ubuntu een moderne en solide basis voor de komende jaren.



acer

Acer Enduro M3

THE POWER OF THE WILD

Superieure
5G-verbinding
in 135+ landen

Geen
SIM-kaart
vereist

flexibele
internationale
SIMO-databundels

Verbind
tot wel 16
apparaten



5G mobiele WiFi-hotspot

Altijd internet
onderweg en op vakantie

Verkrijgbaar bij o.a. MediaMarkt, Coolblue, De Wit Schijndel, bol en onze Acer Online Store.

MeLE Quieter 4C F5Q

De Quieter 4C mini-pc is zo groot als een chocoladereep. Hij kan via USB-C zowel data versturen als beelden naar een monitor en kan zijn energie zowel uit de monitor putten als uit een powerbank. De mini-pc heeft echter ook een aantal mindere eigenschappen.

Christof Windeck

Bijzonder aan deze mini-pc is dat een van de twee USB-C-aansluitingen behalve data-transfer zowel DP Alt Mode biedt als USB PD in twee richtingen. Daardoor kan deze mini-pc zijn voeding uit een USB-C monitor halen of juist een (mobiele) monitor voeden en via dezelfde USB-C-kabel beeldsignalen en data doorsturen. Dat zien we vaak bij laptops, maar helaas zeer zelden bij mini-pc's. Ook aansluiten via een USB-C-dock is mogelijk.

De tweede USB-C-aansluiting is alleen voor voeding. De bijgeleverde voeding levert altijd 12V en kan daarmee andere USB-C apparaten beschadigen. Dat is vooral riskant als je apparaten hebt met een USB-C-aansluiting die alleen 5 of 9 volt verdragen. Een geel etiket aan de kabel moet hiervoor waarschuwen.

De mini-pc vereist zelf 12V en tot 2 ampère, oftewel een 24W-voeding. Dat red je in principe ook met een krachtige USB-C-powerbank.

De Quieter 4C biedt verder aansluitingen zoals 2 x HDMI 2.0b, 3 x USB-A (2 x USB 3.2, 1 x USB 2.0), RJ45 en een 3,5-mm audiojack. Er is een oude en trage Wi-Fi 5-chip ingebouwd en een eveneens trage microSD-kaartlezer.

Afgezien van de USB-C-ondersteuning lijkt de Quieter 4C op andere mini-pc's met Intels goedkope N100 cpu: hij voldoet voor

kantoorwerkzaamheden en internetten en de geïntegreerde UHD graphics speelt veel 4K-video's zonder haperen af.

Met 16 GB vastgesoldeerd RAM is er genoeg werkgeheugen. Jammer is dat MeLE Windows 11 Pro op het trage eMMC-flashgeheugen heeft geïnstalleerd en niet op de veel snellere M.2-sdd. Daardoor duurt booten bijna een halve minuut.

De passieve koeling voldoet en de mini-pc wordt niet te heet. De N100 staat vast ingesteld op een TDP van 6W, zodat de mini-pc zuiniger, maar ook langzamer is dan andere die op 10W zijn ingesteld. Toch verbruikt hij idle 7 watt, terwijl een bijvoorbeeld Asus ExpertCenter PN42 toekan met 4,5 watt. Dat is vooral jammer als je hem met een powerbank voedt.

De oorzaak daarvan kan liggen in het nauwelijks aangepaste AMI standaard-BIOS, dat zelfs nog de (niet vertrouwde!) AMI-testsleutel als platform-key bevat.

Op de fabrikantenwebsite vonden we zoals bij veel Chinese mini-pc's geen BIOS-updates. De prijs van 210 euro die we betaalden vonden we online ook nergens meer.

Voor die prijs biedt de Quieter 4C een nette 16 GB en veel aansluitmogelijkheden, vooral via USB-C. De trage eMMC-flash en wifi, schadelijke voeding en gebrekkige BIOS zijn echter flinke minpunten.

- ▲ **USB-C met DP Alt en PD**
- ▼ **schadelijke voeding**
- ▼ **gebrekkig BIOS**

cpu / RAM

Intel N100 / 16 GB LPD-DR4X-4267taal

opslag

256 GB eMMC-flash, 256 GB M.2-ssd (PCIe 3.0 x4, 2280)

wifi / LAN

Intel Wireless-AC 9560, 2x2 / Realtek RTL8111

afmetingen / gewicht

13,2 x 8,4 x 1,7 cm / 200 g

€ 210



Deepcool AK500 Digital

De Deepcool AK500 Digital koelt cpu's uit de hogere middenklasse en heeft als bijzonderheid een display op de bovenkant zitten.

Benjamin Kraft

De towerkoeler is geschikt voor alle Intel- of AMD-cpu's van de laatste tien jaar. Hij houdt zich aan de keep-out area rondom de cpu-socket en is daarmee geschikt voor channel-systemen met RAM aan beide kanten van de cpu. Het installeren is eenvoudig dankzij de goed geïllustreerde instructies.

Partytrick van de AK500 Digital is het statusscherm bovenop, dat informatie geeft over het cpu-gebruik en de temperatuur. De Deepcool Digital-app leest die uit via een interne USB 2.0-verbinding met het moederbord. Twee led-lichtstroken bovenop zijn via een driepins moederbordkabel aan te sturen via ARGB-systemen van Asus, Asrock, Gigabyte, MSI en Razer.

Bij de test maakte de Deepcool AK500 indruk, zowel thermisch als akoestisch. Hij hield bij stresstests de cpu op 80 °C en met 0,5 sone na 10 minuten bleef hij stil. Met nog meer belasting stijgt de ventilatorcurve steil en begint de ventilator te zoemen.

De Deepcool AK500 is een blikvanger en houdt cpu's effectief en stil koel, met reserves voor meer vermogen.

- ▲ **scherm op koeler**
- ▲ **stil en effectief**
- ▼ **geluid bij zeer krachtige cpu's**

cpu-sockets

AMD: AM5/AM4; Intel: LGA1700/1200/115X/2066/ 2011-v3/2011

afmetingen (b x h x d) / gewicht

12,7 x 16,0 x 11,7 cm / 1291 g

meegeleverd

thermische pasta, schroevendraaier, low noise-adapter

€ 75

Acer Veriton N2590G mini-pc

De Acer Veriton mini-pc is een klein apparaat dat bijzonder geschikt is voor kantoorwerk. Met de meegeleverde beugel bevestig je hem eenvoudig achter je scherm en houdt je hem buiten het zicht.

Daniel Dupré

Hardwarefabrikant Acer is vooral bekend om zijn laptops en beeldschermen, maar heeft ook mini-pc's in zijn assortiment. Die kleine desktop-pc's zijn populair omdat je er alleen maar een toetsenbord en scherm op hoeft aan te sluiten zonder dat je een grote computerkast onder je bureau hoeft op te bergen. Om zo klein te kunnen zijn, lenen de pc's hun hardware uit laptops. Mini-pc's bieden zo de voordelen van twee werelden – maar soms ook de nadelen.

Het eerste wat opvalt als je de pc inschakelt, is dat de interne ventilator continu hoorbaar draait – ook al is dat zeer zacht. Het maakt daarbij veel uit waar en hoe je hem neerzet. Plat op het bureau maakte hij meer geluid dan wanneer we hem op de meegeleverde voet verticaal plaatsten. Waar in sommige laptops of mini-pc's de ventilator onder systeembelasting geluid maakt alsof het systeem gaat opstijgen, ging de ventilator in de Veriton wel iets luider draaien, maar niet significant. Je wordt niet opgeschrikt door enorm geluid wanneer de pc even iets harder moet rekenen.

Acer levert een beugel mee waarmee je de Veriton achterop een VESA-compatibele monitor kunt bevestigen. Daarmee zal de pc niet alleen minder hoorbaar zijn, maar blijft hij ook uit het zicht. Met een compatibele monitor kun je de Veriton bovendien via het scherm inschakelen.

In de Veriton zit een 13e generatie Raptor Lake Core i5-1335U-processor die over twee power- en acht efficiency-kernen beschikt. De twee power-kernen hebben hyperthreading, waarmee het besturingsstelsel en applicaties in totaal twaalf cpu-threads tot hun beschikking hebben. De cpu haalt volgens Intel maximaal 4,6 GHz. De processor heeft een basisvermogen (PBP) van 15 watt, dat kan oplopen tot 55 watt tijdens het turbovenster dat 28 seconden mag duren.

De processor in de Veriton zorgt ervoor dat programma's snel opstarten. Het systeem draait zijn hand niet om voor standaard kantoortaken zoals e-mail, tekstverwerking, spreadsheets en browsen op het internet. De acht efficiency-kernen bieden voldoende prestaties voor wat incidentele beeldbewerking, maar voor veeleisende render- of videoprojecten zal een krachtigere cpu beter zijn. Voor gamen is het systeem niet geschikt, een oudere game draait hooguit met lage detailinstellingen.

tigere cpu beter zijn. Voor gamen is het systeem niet geschikt, een oudere game draait hooguit met lage detailinstellingen.

Bij het testmodel heeft Acer helaas een beetje beknibbeld op de opslag en het geheugen: er zat een bescheiden 256GB-ssd in (WD PC SN740) en maar 8 GB DDR4-3200 werkgeheugen. Het goede nieuws is wel dat er binnenin nog een vrij M.2- en RAM-slot zitten om het geheugen en de opslag naar wens uit te breiden.

Aan de voorzijde van het apparaat zitten naast de audio-combijkack twee USB-A-poorten (USB 3.2 gen 2 en USB 2.0) en een USB-C 3.2 gen 2-poort. Aan de achterzijde zitten dan nog eens twee USB 3.2 gen 1- en twee USB 2.0-poorten, een gigabit-ethernetpoort en een aansluiting voor de meegeleverde wifi-antenne. Via de aanwezige HDMI-, DisplayPort- en USB 3.2 gen 2-poorten kun je drie schermen aansluiten. Ten slotte is er nog de aansluiting voor de voeding – het is helaas niet mogelijk om de Veriton via USB-C van stroom te voorzien.

Acer levert het systeem met de nodige bloatware zoals een McAfee-proefversie, een paar patience-achtige games en web-links naar Booking.com, DropBox Express-VPN, en nog een aantal meer. Office-programma's zijn al voorgeïnstalleerd, maar je hebt wel een Microsoft-account nodig om daar mee te kunnen werken. Als je op sommige apps op de lijst met apps klikt, blijken die niet geïnstalleerd te zijn, maar opent de Microsoft Store. Het is wel mogelijk om die apps en links te verwijderen.

Acer levert met de Veriton N2590G mini-pc een prettig kleine pc voor wie op zoek is naar een klein apparaat voor kantoorwerkzaamheden. De hardware voldoet prima voor office-programma's, surfen en een klein beetje beeldbewerking. Het apparaat is onder belasting altijd beheersbaar stil, een continue maar zachte ruis blijft idle altijd hoorbaar. Jammer is wel dat Acer heeft beknibbeld op het meegeleverde werkgeheugen en met name de opslag. Gelukkig zijn beide dankzij de vrije poorten eenvoudig uit te breiden.

- ▲ compacte mini-pc
- ▲ redelijke prestaties
- ▼ (te) krappe RAM en opslag



besturingssysteem

Windows 11 Pro

processor

Intel Core i5-1335U decacore (10-core), 1,30 GHz 64-bit processor

geheugen

8 GB DDR4 SDRAM, max 32 GB (2 × Memory slots)

ssd

256 GB (PCI Express 4.0)

graphics

Intel Iris Xe Graphics gedeeld DDR4 SDRAM

netwerk

Gigabit Ethernet, Wi-Fi 6e (IEEE 802.11ax), Bluetooth 5

I/O-uitbreidingen

3 × M.2-interfaces, 2 × USB 3.2 Gen 1 Type-A-poorten, 1 × USB 3.2 Gen 2 Type-A-poort, 1 × USB 3.2 Gen 2 Type-C-poort, totaal 8 × usb-poorten

verbruik, maximaal

65 W

afmetingen (h × b × d)

30 × 178 × 178 mm

benchmarks

PCMark10: 5479 punten; Cinebench R23: 7926 (MT) 1688 (ST)

€ 849



Hou je IT-kennis breed en up-to-date

Hardware-reviews • Tech-achtergronden • Praktijk-workshops
Artificiële Intelligentie • Windows en Linux • Security • en meer

Met een c't abonnement krijg je:

- Inzicht in IT-ontwikkelingen, achtergronden en onderliggende technieken
- IT-informatie vanuit verrassende invalshoeken om je kennis te verbreden
- Praktijkartikelen en uitgebreide hard- en softwaretests door onze IT-kenners

Ontvang
10x c't magazine
van ~~€89,90~~ voor

€60,-

Abonneer je nu via www.ct.nl/abo
of bel naar +31 (0)24 2027 825



WINDOWS 11 24H2 WERKT OP OUDERE PC'S OPEENS NIET MEER www.ct.nl

IT-magazine voor de liefhebber

7 2024 **Acer Veriton N2590G** Mini-pc met Core i5-1335U

MULTI-GIGABIT NETWERKEN

- ▶ Maak je netwerk sneller
- ▶ Test van managed switches
- ▶ Technieken en interfaces

GETEST

- Laptopprocessors van AMD, Intel en Apple
- Acer TravelMate P6 14-inch laptop
- 27"-monitoren met 4K en USB-C
- Prusa MK4 en Bambu Lab P1S 3D-printers
- Asus Expertbook B3604CM laptop
- Deepcool AK500 Digital cpu-koeler

VIRTUALISATIE

- Kies de juiste software
- Aan de slag met Proxmox

GROTE SSD-TEST

- Met PCIe 4.0 of 5.0
- Is sneller ook beter?

EN VERDER

- Windows krijgt sudo-commando
- Bouwvoorstel Core i-14000 kantoor-pc
- Emuleer een Atari ST
- Thunderbolt: zo werkt het
- Passkeys met opensource tools
- Secure Boot onder Linux

7 Juli 2024

Adhockers tegen reclame • Secure Boot problemen • Apple Vision Pro VR-dit • Internetstijfheid meten • Zwart

**c't app:
digitaal lezen
& opslaan
pdf's**



QNAP TBS-h574TX

De QNAP TBS-h574TX is een compacte NAS met 5 slots voor snelle storage in M.2- of E1.S-formaat. Hij biedt zowel een 2,5- als 10Gbit/s-netwerkpoort plus twee Thunderbolt 4-poorten, snelle usb-poorten en zelfs HDMI. Dat leidt tot een veelzijdige NAS die via diverse mogelijkheden toegang tot snelle opslag biedt

Alieke van Sommeren

Bij het uitpakken komt een compacte, overwegend metalen en strak ogende behuizing tevoorschijn. De NAS is verkrijgbaar in twee versies: de TBS-h574TX-i5-16G met een Intel Core i5-cpu met 16 GB RAM, en de TBS-h574TX-i3-12G met een Intel Core i3-cpu met 12 GB geheugen. Aan de voorkant zitten onder meer een snelle 10Gbit/s USB type A-poort en Thunderbolt 4-poort direct onder handbereik. Achterop zitten onder andere een 2,5Gbit/s- en 10Gbit/s-netwerkpoort, HDMI, Thunderbolt 4 en twee usb-poorten (type A USB 2.0 en type A met 10 Gbit/s).

Aan de rechter zijkant zit een vergrendelingsknop voor het frontje, waar de 5 slots voor de flashopslag achter zitten. Elke drivehouder haal je eenvoudig met een hendeltje los. In de slots zitten al adapters voor M.2-ssd's, die je met een klein plastic schuifje vergrendelt. De NAS kan ook overweg met de (erg prijzige) E1.S-ssd's. Daarbij moet je wel met tools aan de gang. We hebben de TBS-h574TX getest met twee Kingston KC3000-ssd's van 4 TB in RAID 1.

Na het vullen van de drivebays start je de configuratie via de cloud of de Qfinder Pro-tool. Door de HDMI-poort kun je de NAS ook direct aansluiten op een scherm

cpu / RAM

Intel i3-1320PE / 12 GB

drivebays

5 × M.2 2280 of E1.S tot 15mm

aansluitingen

2 × Thunderbolt 4, USB type A 2.0, voeding,

2 × USB 3.2 type A Gen 2 (10 Gbit/s), HDMI 1.4

leds / bedieningselementen

status, USB copy, ssd 1 t/m 5 /

USB copy, reset, power

energieverbruik

46 W

afmetingen / gewicht

6,0 × 21,5 × 19,9 cm / 2,24 kg

meegeleverd

120W-adapter, netwerkkabel (10 Gbit/s),

handleiding

vanaf € 1550

en met behulp van een usb-toetsenbord (of QNAP IR-afstandsbediening) de instructies opvolgen. Dankzij de HDMI-poort kun je de NAS via HybridDesk Station gebruiken als desktop-pc om te internetten, als media-pc of om (live) camerabeelden te bekijken.

De drives in de NAS zijn beperkt tot PCIe 3.0 x2, waarmee je in theorie tot maximaal 2 GB/s haalt. Je komt er het dichtst bij in de buurt via Thunderbolt op een Mac (1750 MB/s), al zijn de snelheden wel afhankelijk van bijvoorbeeld al dan geen encryptie en deduplicatie. De 10- en, 2,5Gbit/s-poorten worden makkelijk volledig benut.

Aansluiten via Thunderbolt maakt de NAS ook erg bruikbaar voor onderweg, en de 10Gbit/s usb-poorten zorgen dat je extern geschoten materiaal snel op de NAS kunt veiligstellen. Het is erg prettig dat die twee snelle opties ook meteen aan de voorkant van de NAS beschikbaar zijn.

Tijdens het doorlopen van de instellingen en het aanmaken van de opslagpool ging de NAS al snel hoorbaar te werk. De kleine fans draaien al snel veel lawaaiiger rondjes met een wat hinderlijk bijgeluid. De twee casefans en de cpu-fan houden de NAS wel netjes op een prima temperatuur.

De NAS is compact en misstaat niet op je bureau, maar daar is hij eigenlijk net iets te lawaaiiger voor. Geheugenuitbreiding is ook geen optie, al zul je daar bij de meeste toepassingen ook geen behoefte aan hebben. Daar staat tegenover dat de NAS compact en zelfs draagbaar is. Het aantal en de snelheid van de aansluitingen is ruim en dik in orde.

▲ compact en snel (TB4, 2,5/10 Gbit/s)

▶ geheugen niet uitbreidbaar

▶ vrij luid



Epos Expand Vision 1

Nieuwe webcam-modellen kunnen zich inmiddels hooguit nog onderscheiden in kwaliteit. En dat is precies wat de Epos Expand Vision 1 doet.

Noud van Kruijsbergen

De Epos Vision 1 is klein en licht, en past daardoor makkelijk in je tas, beschermt door de meegeleverde case. De USB-C-kabel met haakse plug steekt niet ver uit.

De driver wordt automatisch geïnstalleerd en zet een zwevend menu op het scherm. Daarmee kun je tijdens gebruik onder meer zoomen naar panoramaniveau en inzoomen naar een close-up, het beeld spiegelen, en het lichtniveau en de kleurtemperatuur instellen. De webcam heeft ook een mechanisch privacy-schuifje.

De 4K-camera levert een haarscherp beeld – maar hou er rekening mee dat je die 4K alleen bij de panoramaweergave gebruikt. Bij de instellingen Standaard en Close-up lijkt je met pan&tilt-knoppen het beeld te kunnen verplaatsen, maar dan gebruik je met de digitale zoom alleen maar een deel van die 4K-resolutie.

De camera is gecertificeerd voor Microsoft Teams, Unify en Zoom. De twee omnidirectionele en noisecancellende microfoons pikken je stem goed op, ook in een wat drukker kantooromgeving.

De Epos Expand Vision 1 is zeker voor laptopgebruikers een duidelijke upgrade ten opzichte van de ingebouwde webcams en microfoons. Door zijn handzaamheid is hij bovendien makkelijk mee te nemen.

▲ scherp beeld

▲ geluid

▲ effectieve instellingen

camera / zoom

4K groothoek / 8 × digitaal

video

tot 2160p / 60 Hz

microfoon

180°, 110-10.000 Hz

meegeleverd

1,2m USB-C 3.0-kabel, hardcase

€ 209



Acer Chromebook Plus 515

Zowel qua hardware als qua software zijn moderne Chromebooks flink geëvolueerd sinds de oorspronkelijke ‘browser met een toetsenbord’. De Chromebook Plus zou een volgende stap moeten markeren.

Marco den Teuling

Er is heel wat veranderd aan Chromebooks sinds het eenvoudige begin, zowel qua software als qua hardware. Behalve de Chrome-browser met alle online toepassingen, kun je tegenwoordig op een Chromebook ook Android-apps uit Googles Play Store en Linux-toepassingen gebruiken. Voor die apps is een touchscreen echter wel praktisch en voor Linux moet de hardware krachtig genoeg zijn. En doordat daarmee de oorspronkelijke ‘online only’-laptop veel meer data lokaal moet opslaan, voldoet de beperkte opslagruimte van eerdere Chromebooks ook niet meer.

Het label Chromebook Plus van Acers Chromebook maakt duidelijk dat dit model aan bepaalde minimumeisen voldoet qua cpu, werkgeheugen en opslag. De 8GB RAM voldoen aan de eisen, en de Intel Core i5-1335U-processor met tien cores en 256 GB opslag zitten er ruim boven. Daarmee is het draaien van Linux-applicaties en installeren van een groot aantal apps geen enkel probleem.

Ook het full-hd IPS-panel (hier met touchbediening) en de 1080p-webcam zijn volgens de eisen. Die webcam is voorzien van een schuifje om hem te blinderen.

Voor een IPS-scherm is de horizontale kijkhoek vrij klein, maar het scherm reageert vlot op aanrakingen. Dat de hardware van deze Chromebook krachtig genoeg is, blijkt verder uit het feit dat het Steam-installatieprogramma standaard in de launcher aangeboden wordt. Niet dat je er meteen zware 3D-games op kunt draaien, maar de geïntegreerde Intel Iris Xe graphics voldoen in combinatie met de andere hardware in ieder geval prima voor casual of lichtere games.

Ook een wat zwaardere game zoals Civilization V draaide goed, al kostte het starten daarvan wel wat tijd. Veel Windows-versies van games draaien tegenwoordig op Linux/Chrome OS met daaronder de Proton-emulatielaag.

Qua hardware is Acers Chromebook Plus 515 verder uitgerust met twee USB-C-aansluitingen (voor grafische uitvoer, om hem op te laden en data te versturen). Prettig is dat er een aan ieder kant

cpu / geheugen
Intel Core i5-1335U (10 cores) /
8 GB LPDDR5X RAM
opslag
256 GB ssd
afmetingen / gewicht
23,8 × 36,1 × 20,0 cm / 1,4 kg
€ 660



zo'n aansluiting zit, zodat de voeding links of rechts aangesloten kan worden.

Een HDMI-poort, USB-A (USB 3.2 Gen 1) en 3,5-mm audiojack en twee naar boven gerichte speakers maken het plaatje compleet. De positie van de speakers zorgt voor een duidelijker geluid, wat bijvoorbeeld bij videoconferenties prettig is.

De hardware van Acers Chromebook Plus 515 draait Chrome OS soepel, zoals je mag verwachten. Ook tijdens het draaien van zwaardere toepassingen blijft de laptop stil. Daarbij helpt dat bij het openklappen van het deksel de onderkant van de laptop automatisch iets wordt opgetild. De cpu-temperatuur kwam tijdens tests niet boven de 60 graden uit en de laptop bleef aan de onderkant draaglijk warm, zodat je hem prima op je schoot kunt houden. De 53Wh-accu houdt het met het lichte Chrome OS makkelijk een werkdag vol, tenzij je gaat gamen of zware Linux-software draait.

Aan de doorsnee donkergrijze kunststof behuizing zie je het verschil tussen deze Chromebook Plus en een ‘gewone’ Chromebook niet. Plus betekent niet per se een Premium uiterlijk of design. Het kunststof helpt wel om het gewicht met 1,4 kg vrij laag te

houden voor een 15-inch laptop. De Acer Chromebook Plus 515 presteert bovendien zoals je van een krachtige Chromebook mag verwachten. Je krijgt daarnaast Wi-Fi 6E en toetsenbordverlichting, wat voor de prijs ook wel mag.

Op een Chromebook Plus verwacht je dat Chrome OS wat extra's biedt. Behalve een proefversie van Adobe Photoshop online krijg je een paar andere extra's, zoals de premium-versie van Adobe Express en video- en geluidsverbeteringen bij bepaalde videoconferentie-apps. Bij Google Foto's kun je de Magische gum gebruiken die ook op Googles Pixel-smartphones beschikbaar is. Je kunt met bestandssynchronisatie de grotere opslagruimte benutten om bestanden offline te benaderen.

Dat er in Chrome OS verder nog weinig meerwaarde van het Plus-label valt te ontdekken is Googles verantwoordelijkheid. Misschien komt daar verandering in als de beloofde ‘powerful AI capabilities’ daadwerkelijk beschikbaar komen.

- ▲ **prima prestaties**
- ▲ **stil en draagbaar**
- ▼ **nog weinig ‘Plus’ in Chrome OS**

Palit GeForce RTX 3050 KalmX 6GB

Nvidia lanceert de GeForce RTX 3050 met slechts 6 GB die goedkoper en kleiner is. De Palit GeForce RTX 3050 KalmX 6GB is een variant die passief gekoeld wordt, maar helaas ook trager is dan het origineel.

Christof Windeck

De 6GB-versie is inmiddels de vierde variant van de GeForce RTX 3050. Deze naamgeving maakt het al niet bepaald overzichtelijk en omdat hij aanzienlijk langzamer is dan zijn naamgenoten, is Nvidia hier bijna misleidend bezig. Een benaming als RTX 3040 zou veel passender zijn.

De Palit KalmX met passieve (en dus stille) koeling is verkrijgbaar voor 220 euro. Er zijn een aantal modellen die nog een paar tientjes minder kosten, waarmee dat de goedkoopste RTX-grafische kaarten van Nvidia zijn. De Intel Arc A300- en AMD Radeon RX 6500/6400-series zijn goedkopere DirectX 12 Ultimate raytracing-kaarten, maar die presteren ook minder.

Nvidia beperkt de GA107 grafische chip tot 2304 shadercores en 96 parallelle data-lijnen naar het 6 GB GDDR6-geheugen. De processor werkt nog steeds met de oudere Ampere-architectuur. Hierdoor biedt hij geen tussentijdse beeldberekening via DLSS AI-upscaling.

Het verbruik is geconfigureerd op maximaal 70 watt, wat de prestaties verder beperkt. Vergeleken met de RTX 3050 met 8 GB is het uiteindelijke resultaat een vermindering van 30 procent. Vergeleken met een GeForce GTX 1660 Super was de 3050 6 GB ongeveer 20 procent langzamer. Hij was slechts in staat om de GeForce GTX 1060, die bijna acht jaar oud is, met ongeveer 10 procent te verslaan, hoewel dit alleen geldt voor games met rastergraphics, aangezien de GTX 1060 geen raytracing ondersteunt.

De 3050 6GB kan niet concurreren met een Radeon RX 6600. Hij is in sommige gevallen maar half zo snel met rasterafbeeldingen, soms loopt hij echter maar 10 procent achter met raytracing. De RTX 3050 6GB presteert daarentegen vaak ongeveer

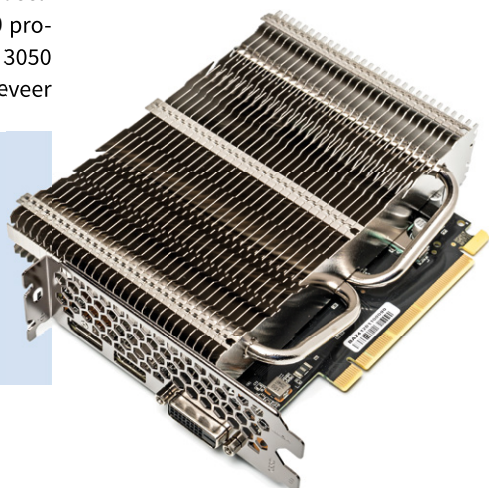
100 procent beter dan AMD's goedkope RX 6500 XT en is dus twee keer zo snel.

Je moet het advies van fabrikant Palit over de luchtstroom in de behuizing wel serieus nemen, anders raakt de kaart oververhit en gaat hij bij langdurige belasting afremmen. In idle is de Palit RTX 3050 KalmX tevreden met zes watt met een Full HD-monitor en 10 tot 12 watt met 4K-monitoren met 60 tot 144 hertz. Onder volledige belasting hebben we 75 watt gemeten in plaats van de beloofde 70 watt, met individuele pieken van een paar milliseconden die oplopen tot 90 watt. Hoewel er geen problemen optraden tijdens de test is dit meer dan het PCI Express slot moet leveren.

De KalmX beschikt over een DisplayPort 1.4a DSC, een HDMI 2.1-aansluiting en een dual-link DVI-D voor een derde scherm. Afgezien van een Spartaanse folder met een verwijzing naar de driver download, levert de fabrikant geen andere accessoires.

De RTX 3050 6GB is een instap-grafische kaart met raytracing-capaciteit voor ongeveer 190 euro. De passieve koeling van Palit kost ongeveer 30 euro extra. De naam kan onervaren klanten gemakkelijk misleiden en hen doen hopen op meer prestaties dan in werkelijkheid worden geleverd. De prestaties zijn alleen voldoende voor Full HD-gaming in gemiddelde tot hoge detailniveaus. Bij hogere resoluties of met raytracing loopt de kaart vast.

- ▲ passief gekoeld dus stil
- ▼ nog trager dan het origineel
- ▼ te lage prestaties voor raytracing



gpu / grafisch geheugen
GA107 / 6 GB GDDR6
shaders / TMUs / ROPs
2304 / 72 / 32
afmetingen (l x h x b)
16,8 x 13,6 x 4,0 cm
geluidsproductie idle / belast
<0,1 sone / <0,1 sone

€ 220



Scythe Mugen 6

De zesde generatie van de Scythe Mugen processorkoeler houdt processors effectief koel en doet dat fluisterstil.

Benjamin Kraft

Vergeleken met zijn voorganger zit de Mugen 6 verder richting achterzijde en bovenzijde op het moederbord, wat meer ruimte biedt aan dikke grafische kaarten en grote RAM-modules. Opvallend is de nieuwe ventilator met zijn grote naaf en negen sterk gebogen bladen. Naast de standaard versie is er ook de Mugen 6 Dual Fan Black Edition, waarbij zelfs het montage-materiaal matzwart is.

In de test hield de koeler een Core i5-14600K makkelijk koel. In idle is de ventilator praktisch onhoorbaar. De cpu bereikte met Prime95 ongeveer 80 °C met pieken tot 87 °C. Op 1200 rpm bleef de ventilator met 0,2 sone fluisterstil, bij circa 2000 rpm is het 1,5 sone. Met de dual fan-versie daalde de temperatuur met ongeveer 2 °C, maar de prestaties verbeterden niet verder. Een Core i7-14700K bleef daarmee ook koel, zij het met warmtepieken tot 94 °C. De dubbele ventilator haalde 0,7 sone met circa 1500 rpm, op volle snelheid 2,2 sone.

De Scythe Mugen 6 koelt beter en stiller dan zijn voorganger. De dual fan-variant is bijna van dezelfde klasse als twin-tower koelers zoals de Corsair A115 of Noctua NH-D15 – maar voor de helft van de prijs.

- ▲ koelt stil en efficiënt
- ▲ duidelijke handleiding
- ▲ niet duur

cpu-sockets
AMD: AM5/AM4, Intel: LGA1700/1200/115X/
2066/2011-v3/2011
afmetingen (b x h x d) / gewicht
13,2 x 15,4 x 10,6 cm / 1013 g
geluid bij PWM 25 / 50 / 75 / 100
<0,1 / 0,1 / 0,6 / 1,5 sone

€ 53 (dual fan: € 60)

Samsung Galaxy Book4 Pro 360

De Galaxy Book4 Pro 360 herbergt moderne techniek in een slanke behuizing met een oled-touchscreen. Bovendien kun je de 360-variant omklappen en als tablet gebruiken.

Daniel Dupré

De Galaxy Book4 Pro 360 wordt geleverd in een minimalistische platte doos waarop een foto van een nog plattere laptop prijkt. De inhoud is even minimalistisch: naast de Galaxy Book zit er een pen, kabel en poweradapter in, en een smalle envelop met een quickstart guide en garantieverwaarden.

De foto op de doos houdt je niet voor de gek: het apparaat zelf is met nog geen 13 millimeter bijzonder plat. Gezien het grote 16-inch scherm weegt het apparaat met 1,66 kg relatief weinig. De enigszins vingerafdrukgevoelige metalen behuizing van de Galaxy Book4 is stevig zonder merkbare torsie als je het apparaat aan een kant oppakt. Om het scherm zit een smalle rand die bovenin iets breder is om de 2 megapixel webcam te huisvesten.

Qua aansluitingen zijn we snel klaar: aan de rechterzijde zit een USB-A 3.2-poort, een combo-jack en een microSD-poort. Links zitten een HDMI 2.1-poort en twee USB-C Thunderbolt 4-poorten, waarvan er een bezet is als je de laptop aan de voeding aansluit. Er zit helaas geen ethernetpoort op, maar met Wi-Fi 6E ben je in principe voorzien van een lekker snelle draadloze verbinding.

Bij het openklappen valt meteen de joekel van een touchpad op. Die is met 10,5 × 15 cm zowaar hoger dan het toetsenbord. Of zo'n groot touchpad nu echt iets toevoegt is een kwestie van smaak, omdat je ook je handen er overheen moet leggen om te kunnen typen.

Het toetsenbord met backlight is prettig ingedeeld en er is een numeriek toetsenblok. De toetsen zijn zeer plat met een korte travel en vereisen wat gewenning.

Samsung heeft de Book4 Pro voorzien van een touchscreen dat achterover kan klappen, zodat je het apparaat ook als een tablet kunt gebruiken. Het fysieke toetsenbord wordt dan automatisch gedeactiveerd en je kunt Windows met je vingers of de stylus bedienen.

De Book4 heeft een oledscherm dat in het oog springt met heldere, volle kleuren. Samsung noemt het Dynamic AMOLED 2X. Het matte, 120 hertz 3K-scherm met 16:10-verhouding moet het aandeel blauw licht reduceren en heeft een 'Cinema-ervaring'-certificering gekregen van de

certificeringsinstantie SGS dankzij het ruime kleurenspectrum van 120% van DCI-P3. Het scherm heeft een maximale helderheid van 400 nits met pieken tot 500 nits bij HDR-content.

Samsung voorziet de Galaxy Book4 van een Intel Core Ultra 7 155H die over 6 P-cores en 8 E-cores beschikt. Daarnaast heeft hij ook nog twee zogenaamde Low Power Efficiency Cores, die voor een lager energieverbruik moeten zorgen. Volgens HWInfo heeft de cpu in de Book4 een TDP van 28 watt en Samsung noemt een turbopiek van 4,8 GHz. Bij de Cinebench R23-benchmark haalt de laptop een bijzonder respectabele multicore-score van 9710 punten en een singlecore-score van 1707. Met 16 GB DDR5-RAM en met 1TB kun je wat de opslagruimte betreft ook goed vooruit. De ingebouwde ssd is prima, maar niet de snelste: de SN740 NVMe-ssd van Western Digital haalt met CrystalDiskMark 8 waarden van 5226 voor het lezen en 4975 voor het schrijven.

Samsung heeft de koeling van de Book4 goed voor elkaar. Met een idle Windows 11-desktop blijft de laptop volledig stil. Wanneer hij aan de bak moet gaan de ventilator ruisen, maar doet dat kortstondig en het geluid blijft binnen de perken.

Samsung weet een zeer behoorlijk geluid te halen met de vier AKG Dolby Atmos-speakers – waar je zowaar nog ruimtelijk effect door waarneemt, mits je niet te ver van de laptop afzit.

Samsung stopt het systeem wel redelijk vol met zijn eigen software. Het bedrijf wil graag dat je Samsung-tools gebruikt en het liefst in samenwerking met een Samsung-smartphone. Dat kan leuk zijn als je er een hebt, maar voor andere gebruikers die er geen hebben zitten die applicaties alleen maar in de weg.

Wat het besturingssysteem betreft is het verrassend dat Samsung ervoor heeft



processor
Intel Core Ultra 7 155H, Intel Arc-graphics
RAM, opslag
16 GB LPDDR5 SO-DIMM, 1TB M.2-ssd
scherm
16" WQXGA+ AMOLED (2880 × 1800) mat touchscreen
draadloze verbinding
Wi-Fi 6E, 802.11 ax 2x2, bluetooth v5.3
aansluitingen
1 × HDMI 2.1, 2 × Thunderbolt 4, 1 × USB 3.2, microSD, combo-jack
afmetingen, gewicht
36 × 25 × 1,3 cm, 1,66 kg
€ 2299

gekozen om de Galaxy Book4 Pro 360 van Windows 11 Home te voorzien. Veel van de bovengenoemde aspecten van de Book4 duiden op een laptop voor professioneel gebruik – niet in de laatste plaats door het woord Pro in de productnaam. Op de productpagina raadt Samsung bedrijven ook aan om voor Windows 11 Professional te kiezen, maar biedt die optie niet aan gebruikers die de Book4 op de website bestellen.

De Galaxy Book4 Pro 360 is met 2300 euro niet goedkoop, maar je krijgt er veel voor terug: een mooi, groot oled touchscreen en behoorlijk krachtige hardware in een zeer plat apparaat. De integratiedrang met Galaxy-smartphones daargelaten is het een fijne laptop voor professioneel en/of creatief gebruik.

- ▲ **krachtige, stille prestaties**
- ▲ **veelzijdig goed scherm**
- ▼ **Galaxy-integratiedrang**

Asus ExpertBook B3604CM

De ExpertBook B3 van Asus heeft alles wat je van een laptop voor op kantoor of onderweg mag verwachten: genoeg systeemreserves voor uitgebreide kantoor toepassingen en door AI ondersteunde mogelijkheden qua beeld en geluid voor duidelijke videovergaderingen.

Noud van Kruisbergen

Wat bij de ExpertBook meteen opvalt is het matzwarte uiterlijk met het eveneens zwarte maar glimmende ASUS-logo. Daarmee is meteen duidelijk dat het om een zakelijke laptop gaat. Jammer wel dat de laptop daardoor nogal vatbaar is voor vingerafdrukken.

De aan-uitknop is de vierde knop van linksboven, wat even zoeken is, maar waardoor je hem niet snel per ongeluk aan of uit zult zetten. Het numerieke toetsenbord heeft met drie bij zes smalle knoppen een iets andere indeling, maar dat werkt al snel best prettig. De overige toetsen zijn van normaal formaat en bieden een prettige tegendruk – daar kun je makkelijk uren mee werken. De onderste toetsenrij met de Windows-knop en de spatiebalk is iets hoger, waardoor de pijltjestoetsen op één rij passen. De rechter Ctrl-toets zou moeten fungeren als Copilot-toets, maar dat heeft nog weinig nut. Vooralsnog dient hij als een soort recent-knop en geeft een overzicht van de laatst geopende applicaties.

Het touchpad is bijna zeven inch groot en is prima geschikt om nauwkeurige muisbewegingen mee te maken. Je kunt het met een functietoets uitschakelen als dat nodig is. De toetsenbordverlichting is in- en uitschakelbaar, maar is beperkt tot alleen de knoppen 1 tot met 4 – waarom dat zo is, is niet helemaal duidelijk.

Al tijdens het installeren van de obligate Windows 11 Pro-updates valt het niet reflecterende 16-inch IPS-display op met een resolutie van 1920×1200 pixels in 16:10-verhouding, wat verticaal net wat meer werkruimte biedt. De maximale opgegeven helderheid van 300 cd/m² haalden we met 274 cm/m² niet, maar dat is genoeg voor de meeste werksituaties en voor onderweg.

De Intel Core Ultra 7 155U is een van de nieuwe mobiele processoren uit de Meteor Lake-serie. Hij heeft 2 P-cores en 8+2 E-cores. Daar is 16 GB DDR5-5600 RAM aan toegevoegd – in het testmodel was dat van SK Hynix – en een 512 GB PCIe 4.0 M.2-ssd van Solidigm.

De ExpertBook B3 heeft een grafische adapter in de vorm van de geïntegreer-

processor / RAM / opslag

Intel Core Ultra 7 155U / 16 GB DDR5-5600 RAM / 512 GB PCIe 4.0 M.2-ssd

aansluitingen

RJ45, 3,5mm-audio, HDMI 2,1, 2 × USB 3.2 Gen 2 type-A, 2 × Thunderbolt 4 type-C

meegeleverd

65W-voeding

€ 295



de Intel Meteor Lake-graphics. Daarnaast heeft hij een aparte Intel-NPU (Neural Processing Unit) met de naam AI Boost.

De Cinebench R23 singlecore-score is 1668 en multicore 6468. Dat zijn geen monsterscores, maar daar is deze processor met zijn TDP van 15 watt en deze laptop ook niet op gefocust. Daarbij loopt het ruisniveau van de koeling bij singlecore op tot 49 dB, bij multicore is dat maar 41 dB. Bij normaal gebruik hoor je echter niets, want pure singlecore-toepassingen zul je in de praktijk weinig gebruiken. Zelfs bij intensieve kopieertaken komt het geluidsniveau dan niet boven de 34 dB uit en verdwijnt daarmee in de achtergrondruis.

We kregen PCMark 10 niet opgestart vanwege een parse-error, waarvan we de oorzaak niet konden achterhalen.

De snelheid van de ssd blijft met 3493 MB/s voor lezen en 1650 MB/s voor schrijven (gemeten met CrystalDiskMark) wat weg van de mogelijkheden van PCIe 4.0, maar dit is geen creators-laptop waarop met grote videobestanden gewerkt gaat worden.

De USB 2.0 HD-camera maakt 720p-opnames, wat voldoende is voor video-calls met bijvoorbeeld Teams. Door de NPU-processor kun je de achtergrond licht of zwaarder later vervagen en kun je jezelf automatisch laten framen. De microfoon heeft een AI-ruisonderdrukking die je kunt uitschakelen, met als extra handigheid

een aparte functietoets om de microfoon snel te (un) muten. Met uitzondering van de gigabit-netwerkpoot aan de linker kant zitten alle andere aansluitingen aan de rechterkant: een 3,5mm combi-audiojack, 2 × USB 3.2 Gen 2 type-A, een volwaardige HDMI 2.1-poort en 2 × Thunderbolt 4 type-C voor onder meer de 65W-voeding. Andere ExpertBook-versies hebben ook een smart-cardlezer en een nanoSIM-slot, en ook een vingerafdruksensor, infraroodcamera en zelfs touchscreen met stylus behoren tot de mogelijkheden. Het basismodel is voorzien van Wi-Fi 6E (160MHz) middels een AX211-module.

De extra geïnstalleerde software is beperkt tot de ASUS Business Manager, de ASUS ExpertWdiget voor het instellen van hotkeys en de MyASUS-app voor het registreren van je laptop. Helaas bezetten die laatste twee wel de extra functietoetsen F10 en F12.

De ExpertBook B3 is al met al een moderne laptop met alle hedendaagse mogelijkheden. Het geteste basismodel met een Ultra 7-processor biedt genoeg reserves voor allerlei zakelijke toepassingen. Alle essentiële benodigdheden voor op kantoor en onderweg zijn zonder verdere opsmuk aanwezig.

- ▲ moderne mogelijkheden
- ▲ zakelijk gebruik
- ▶ AI-processor

Shuttle DL30N

De DL30N-barebone is met wat geheugen en opslag uit te breiden tot een moderne mini-pc met DDR5 en 2,5 Gbit/s. Maar ook oudgedienden VGA en RS232 ontbreken niet, wat deze Shuttle tot een barebone met veel toepassingsmogelijkheden maakt.

Noud van Kruijsbergen

De DL30N van Shuttle is een barebone waar een Intel N100-processor in zit – de rest moet je zelf toevoegen. Waarbij die rest dan bestaat uit geheugen en opslag.

De N100 is een Alder Lake N-processor met 4 kernen, met een TDP van 6 watt en een turbo van 3,4 GHz. Dit is dus geen snelheidsmonster, maar een mini-pc die geschikt is voor kantoor- of thuiswerk-pc voor minder veeleisende werkzaamheden. Het feit dat de processor zonder ventilator gekoeld wordt bevestigt dat beeld. Dankzij de twee seriële COM-poorten is hij bovendien ook industrieel inzetbaar.

Je kunt er maximaal een DDR5-4800 SO-DIMM van 16 GB in kwijt. Om dat te installeren moet je het deksel losschroeven en naar achteren schuiven, en het bevestigingsplaatje voor een 2,5-inch ssd verwijderen. Er liggen dan meteen ook twee M.2-slots vrij. Het ene is bedoeld voor een 2242/2260/2280-ssd. Dat kan een PCIe x2/NVMe of SATA-variant zijn. Het 2230-slot is voor een wifimodule, waaronder de optionele WLN-M1 voor Wi-Fi 6 en Bluetooth 5.2. In de achterkant van de DL30N zitten al openingen voor de antennes.

Daarnaast kun je een 2,5-inch SATA-schijf of -ssd als extra of enig opslagmedium bevestigen.

De DL30N is ruimhartig voorzien van aansluitingen. Aan de achterkant zitten om te beginnen vier USB 3.2 Gen 1-poorten en twee RJ45-netwerkaansluitingen van 2,5 Gbit/s. Naast de genoemde RS232-poorten

(waarvan een ook RS422 en RS485 ondersteunt) heeft deze mini-pc nog HDMI 2.0b, DisplayPort 1.4 plus een VGA-poort, die bij moderne pc's steeds minder vaak voorkomt, maar bij industriële toepassingen waar minder grafische mogelijkheden nodig zijn nog wel populair is.

De geïntegreerde graphics van de N100-processor maken het mogelijk dat alle drie de grafische poorten tegelijkertijd gebruikt worden, zodat je zonder extra hulpmiddelen een werkplek met drie schermen kunt creëren. Met de meegeleverde brackets en schroeven kun je de DL30N bovendien op een VESA-mount achter een van de monitoren bevestigen. Aan de voorkant zitten nog eens vier USB 3.2 Gen 1-poorten en 3,5mm-jacks voor een hoofdtelefoon en microfoon.

Om Windows te installeren moet je eerst alle stuurprogramma's van de website van Shuttle downloaden. Shuttle blijft volharden in het meeleveren van een driver-dvd, maar daar heb je bij een mini-pc als deze DL30N weinig aan als je geen dvd-drive in huis hebt.

Bovendien herkent Windows 11 veel van de hardware vanuit zichzelf automatisch al, want voor de meeste onderdelen bestaan namelijk reguliere stuurprogramma's van bijvoorbeeld Intel en Realtek. Ook het installeren van een Linux-distributie is daardoor geen probleem.

De lees- en schrijfsnelheden met een Samsung 980 Pro M2-ssd zijn met respec-

tiefelijk 1777 en 1627 MB/s niet denderend, een Crucial SATA 3.3-ssd kwam met 561 en 508 MB/s aardig in de buurt van de maximale SATA6-snelheid.

De Cinebench R23-scores van 510 voor single- en 1876 voor multi-core bevestigen dat de DL30N geen prestatieve hoogvlieger is. De PCMark 10-score van 2895 illustreert dat eveneens, met een hoogste deelwaarde van Essentials van 6823. Maar zoals gezegd, daar gaat het bij deze mini-pc met zijn N100-processor ook niet om.

De meegeleverde 19V/65W-voeding heeft een voedingskabel en een netsnoer van beide 1,75 meter lang, zodat je met 3,5 meter altijd wel een geschikte plek voor deze mini-pc kunt vinden. Met alleen een Windows-bureaublad blijft het energieverbruik beperkt tot 7,1 watt. Bij een cpu-stresstest loopt dat op tot 19 watt. Ook met andere stresstests kwam het energieverbruik met onze configuratie niet boven de 25 watt uit.

Als de Shuttle op een bureau staat wordt de onderkant zo'n 46 graden warm, terwijl de bovenkant tot 38 komt. Als je hem staand gebruikt met de optionele PS02-stand wordt hij wat meer door de lucht gekoeld en zijn die waarden lager. Het feit dat hij verder geheel stil is moet ergens een beetje gecompenseerd worden.

De Shuttle DL30N blijft met aanvulling van wat geheugen en opslag ruim onder de 500 euro, wat prima is voor een mini-pc voor veel toepassingen. Met moderne (2 maal 2,5 Gbit/s netwerk, DDR5-RAM) zowel als oude (VGA, RS232) technologie en veel aansluit- en uitbreidingsmogelijkheden.

processor / RAM / opslag

Intel N100 quadcore / max 16 GB DDR5-4800 SO-DIMM / 2,5-inch SATA, M.2-2280 NVMe/SATA

aansluitingen achter

4 × USB 3.2 Gen 1, 2 × RJ45 2,5 Gbit/s, 2 × RS232, HDMI 2.0b, DisplayPort 1.4, VGA

aansluitingen voor

4 × USB 3.2 Gen 1, 3,5-mm hoofdtelefoon- en microfoonjack

afmetingen

19,0 × 16,5 × 4,3 cm

€ 295

▲ **moderne technologie**

▲ **stil**

▶ **processor niet de snelste**



Dell Precision 7875 Tower

Dell rust dit high-end workstation uit met het topmodel Ryzen Threadripper Pro 7995WX en twee stuks Nvidia RTX 6000 Ada. We hadden moeite om software te vinden die de enorme performance volledig benut.

Christian Hirsch en Marco den Teuling

Een krachtig workstation met veel cpu-cores en snelle grafische kaarten kan tijd – en daarmee geld – besparen als taken goed te paralleliseren zijn. De Precision 7875 die we konden testen had een bijna maximale configuratie waar we ook als doorgewinterde testers van onder de indruk waren: AMD's snelste desktop-cpu met 96 cores, in combinatie met 128 GB DDR5-RAM via acht geheugenkanalen. Elk van de twee RTX 6000 Ada-kaarten heeft 18.176 shader-cores en 48 GB GDDR6-RAM. Dat heeft zijn prijs: samen met twee PCIe-4.0-sdd's is de totaalprijs net geen 40.000 euro.

Het workstation oogt saai van buiten, maar binnenin onderscheidt het zich van een gewone pc. Bijna alle componenten zijn zonder gereedschap verwisselbaar. De cpu-fans zijn geplaatst in een verwijderbaar aanzuigkanaal, zodat voeding, cpu en grafische kaarten hun eigen thermische zone hebben. Bij het opstarten wordt een

pre-boot-check uitgevoerd en behalve het BIOS is er een grafische diagnose in de firmware die PCIe-poorten, kabels, fans, stations, processor en werkgeheugen op fouten controleert.

Er zijn zes slots voor PCIe-kaarten in x16- en x8-formaat, waarvan er drie met PCIe 5.0 werken. Twee daarvan worden door een RTX 6000 Ada bezet. Voor sdd's zijn er intern twee M.2-slots plus extern een actief gekoeld wisselframe voor een module waarin een M.2-sdd past. Daarnaast zijn er meerdere drive bays voor 2,5- of 3,5-inch SATA-schijven. Een daarvan is extern toegankelijk.

Daaronder zit verrassend genoeg een DVD-brander er is een sd-kaartlezer die tot 278 MB/s leest. We vonden het wel vreemd dat Dell bij een workstation kiest voor een RAID0-configuratie van de sdd's, met één ervan in het wisselframe. Dat zorgt weliswaar voor een doorvoer tot 12 GB/s, maar als bij uitval (of uitnemen) de RAID beschadigd raakt, ben je alle data en de systeempartitie kwijt.

Het workstation beschikt verder over snel Wi-Fi 6E (1,6 Gbit/s dichtbij / 600 Mbit/s op 20 meter), twee onboard LAN-poorten met 10 en 1 Gbit/s en een extra dual-port 10Gbit/s-netwerkaart.

De 96-core Threadripper Pro 7995-WX ging bij Cinebench R23 door de 100.000-puntengrens heen en kwam met R24 op 5882 punten uit. Een Lenovo Thinkstation PX met twee 60-core Xeons was ruim 29 procent langzamer met 4542 punten.

cpu (kernen) / RAM / graphics / opslag

AMD Ryzen Threadripper PRO 7995WX / 96 (192) / 128 GB (DDR5-4800 RDIMM ECC) / 2 x Nvidia RTX 6000 Ada (48 GB) / 2 x SK Hynix 1TB PC801 (PCIe 4.0 x4)

benchmarks

Cinebench 2024 ST / MT: 108 / 5882
3DMark Time Spy 9704, met 16 cores: 33510

energieverbruik

118 W (idle, DP UHD) / 538 W (cpu max.) / 1154 W (cpu en gpu max.)

€ 39.045

Het verschil met een 64-core Threadripper Pro 7980X is echter maar zeven procent doordat Cinebench niet veel meer dan 70 cores kan benutten.

Dat niet alle cores benut kunnen worden zagen we terug bij andere software, de 3D-benchmark 3DMark presteerde zelfs slechter met alle cores dan begrensd op 16 cpu-cores. Bij ondersteunde AI-toepassingen laten de twee RTX 6000 Ada-kaarten als CUDA-team de cpu in het stof bijten. In het 3D-renderprogramma Blender (Lone Monk-scene) was de 92-core Threadripper 37 procent sneller dan de 64-core Threadripper en vier procent sneller dan de twee Xeons.

Het CUDA-team had maar een zesde van de tijd van de cpu nodig (nog zonder OptiX-optimisaties). Niet alle software kan echter beide gpu's gebruiken. De Threadripper-cpu biedt geen voordeel bij toepassingen die maar een enkele core benutten en verliest met 1 core in Cinebench R24 zelfs van de veel goedkopere en hoger geklokte Ryzen 7000- en Core i-14000-desktop-cpu's.

De enorme performance en uitgebreide uitrusting vergt veel energie. Het idle energieverbruik met het bureaublad van Windows 11 Pro is al 150 watt en bij maximaal belasten van de cpu en twee gpu's loopt dat op tot meer dan 1100 watt. Het geluidsniveau stijgt daarbij ook van 0,9 sone tot meer dan 9 sone. Het is aan te raden het workstation remote te gebruiken of een goed afgesloten koptelefoon te dragen.

De Precision 7875 Tower laat zien wat technisch mogelijk is bij workstations en biedt topprestaties. Ook professionele software kan echter niet altijd de 96 cpu-cores benutten en bij sommige programma's blijft ook een van de dure RTX-6000-Ada kaarten onbenut.

De workstationconfiguratie moet wel nauwkeurig worden afgestemd op de werkzaamheden, anders geef je onnodig duizenden euro's uit.

- ▲ enorme performance
- ▲ goed ontworpen systeem
- ▼ energieverbruik en lawaai



Acer Connect Enduro M3 5G Mobile Wi-Fi

De Acer Connect is een snel en makkelijk op te zetten mobiele wifirouter die wereldwijd zelf het beste 4G/5G-netwerk selecteert. Je kunt hem dan als hotspot gebruiken of er een mobiel apparaat zoals een laptop rechtstreeks op aansluiten via usb-tethering.

Noud van Krusbergen

Ben je vaak op reis voor je werk of op vakantie en moet je regelmatig even online voor contact met je collega's of om een reisblog bij te werken, dan weet je hoe lastig het kan zijn om op sommige plekken een internetverbinding te vinden. Ieder land heeft bijvoorbeeld zijn eigen mobiele providers. Binnen Europa is dat gelukkig niet zo'n probleem omdat hier roaming mogelijk is, maar daarbuiten moet je bijvoorbeeld telkens aparte simkaarten kopen, of je moet wachten tot je bij een hotel of andere gelegenheid bent waar er een wifihotspot is. Dan kun je op die manier online. Dat heeft vaak het nadeel dat het een open hotspot is en dus niet veilig: iedereen die wil kan je netwerkverkeer meekijken. In dergelijke situaties is het ook lang niet altijd mogelijk om een stabiele VPN-verbinding te maken.

Dat zijn de situaties waarin de Acer Connect Enduro M3 5G Mobile Wi-Fi van pas komt. Het geheim zit al in de naam verscholen: het is een mobiele wifirouter die via 5G contact maakt met internet. Het grote voordeel zit hem in het feit dat de verbinding niet via één bepaalde provider verloopt, maar SIMO gebruikt. Met SIMO heb je veilig mobiel internet in meer dan 135 landen wereldwijd. SIMO werkt niet met providers, maar zoekt de beste lokale 4G- of 5G-netwerken op. Dit gebruikt een virtuele simtechnologie waar je geen fysieke simkaart voor nodig hebt.

Je kunt kiezen uit een Connect met om te beginnen 1 of 20 GB aan data. Als je het apparaat instelt kun je Engels, Chinees of Duits als taal kiezen. De tijdzone kun je het best op Auto laten staan om overal de goede tijd te hebben. De Connect toont een qr-code die je met je telefoon of tablet scant. Daarmee ga je naar de SIMO-website om je Connect aan een account te koppelen en de eerste gratis bundel te activeren.

Daarmee is het configureren eigenlijk al klaar. Op het startscherm kun je het wifipictogram aanklikken om de inloggegevens voor het 2,4 en 5 GHz-netwerk op Wi-Fi 62x2 MIMO te zien (of te scannen met de qr-code). De verbinding is standaard versleuteld met WPA3. Je kunt de standaard SSID en het wachtwoord op de Connect aanpassen.

Op de website van SIMO kun je de nog resterende GB zien, maar via het menu van de Connect kun je het dataverbruik ook zien. Als je bundel op is, kun je een dagkaart kopen voor 7 euro, wat bijvoorbeeld op een beurs of congres vaak veel goedkoper is dan het wifi van de betreffende locatie. Bij de Pay-Per-GB-optie kun je kiezen uit 1 of 10 GB voor respectievelijk 6 en 39 euro. Die bedragen zijn wat lager als je je wilt beperken tot de zogeheten Popular Destinations.

Daarnaast heb je nog de mogelijkheid tot een Global Unlimited Data, waarbij je voor 99 euro een maand lang kunt internetten. Tot 20 GB kan dat op volle snelheid, daarboven wordt het langzamer.

Er zijn ook databundels alleen voor Europa en Afrika, waaronder 69 euro voor een maand unlimited en 4 euro voor een dagkaart. Het is ook mogelijk een eigen simkaart in de Connect stoppen voor als je de databundel van SIMO niet wilt gebruiken. Dat kan in je eigen land of binnen Europa voordeliger zijn.

Met de optie USB Tethering (die staat standaard uit) kun je een laptop (Windows, Linux en Mac) met een USB-C-kabel aansluiten. Op een Windows-laptop wordt dan meteen een Ethernet-netwerk aangeemaakt. Speedtest.net herkende een Odido-netwerk en kwam tot 154 respectievelijk 27 Mbit/s voor down- en upload. Op onze iPhone 12 kwamen we met die provider op dezelfde plek tot vergelijkbare waarden.

Tijdens de usb-tethering kun je de hotspotfunctie uitzetten, dat scheelt weer in de accuduur. Als je de Connect via usb hebt aangesloten, wordt hij meteen ook weer opgeladen. De accu levert een stevige 6500 mAh, en kan daardoor ook als powerbank

gebruikt worden om bijvoorbeeld je telefoon onderweg opgeladen te houden.

De Connect kan onderweg sowieso wel tegen een stootje met zijn MIL-STD-810H-certificering. Die standaard is ontwikkeld door het Amerikaanse ministerie van Defensie en heeft betrekking op allerlei omgevingscondities zoals hoge en lage temperaturen, vocht en schokken. Daarnaast is de Connect IP-54-gecertificeerd voor bescherming tegen stof en water.

De Connect is daarom een handige reisgenoot voor wie veel (internationaal) onderweg is: nooit meer op zoek naar specifieke buitenlandse providers of surfen op onveilige hotspots, maar snel en makkelijk altijd en overal online. Houd in het achterhoofd dat de prijs van 329 euro voor de Connect al inclusief een 20GB-bundel ter waarde van 69 euro is.

- ▲ wereldwijd online
- ▲ verschillende dataplannen
- ▶ binnen Europa roaming

processor / RAM

Mediatek Octa Core A78/A55 / GB LPDDR4X/8GB eMMC

mobiel / wifi / usb

4G/5G / 802.11ax 2x2 MIMO 2,4 en 5 GHz / USB 3.0 type C

accu

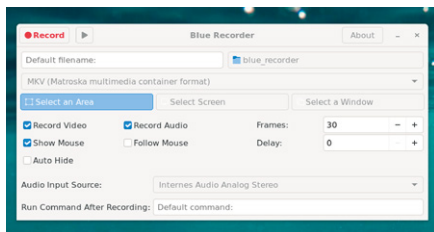
6500 mAh

afmetingen / gewicht

13,8 x 8,3 x 1,7 cm / 250 gr

€ 329





Blue Recorder 0.2.0

Blue Recorder neemt het Linux-bureaublad, afzonderlijke gebieden of een specifiek venster op – naar wens met commentaar via een microfoon.

Liane M. Dubowy

Met korte screencasts met of zonder geluid laat je snel zien hoe iets werkt. Blue Recorder maakt zulke opnames in enkele stappen: vink een paar vakjes aan en klik op Record. Alle beschikbare opties zijn duidelijk zichtbaar in het hoofdvenster.

Blue Recorder neemt een gedefinieerd gebied, een venster of het hele bureaublad op. Het beste laat je Blue Recorder automatisch bestandsnamen toewijzen met de datum en tijd. Anders moet je de naam telkens wijzigen, omdat de tool bestanden zonder waarschuwing overschrijft.

De optie 'Select a Window' suggereert dat slechts één venster wordt opgenomen, maar als er andere vensters in beeld zijn, worden die ook meegenomen. Als je een menu opent dat groter is dan het geselecteerde gebied, wordt het afgesneden.

Blue Recorder ondersteunt MP4, MKV, WebM, GIF, AVI, WMV en NUT als opnameformaten en kan ook geluid opnemen, zodat je commentaar kunt geven op een screencast.

Hoewel Blue Recorder zich iets anders gedraagt onder X en Wayland, ondersteunen veel andere schermrecorders het nieuwe displayserverprotocol helemaal niet. De tool kan niet op tegen complexe tools als OBS Studio, maar werkt veel makkelijker.

- ▲ makkelijk in gebruik
- ▲ geluid erbij opnemen
- ▶ verschil werking X/Wayland

producent

Salem Yaslem,
github.com/xlmnxp/blue-recorder/
systeemeisen

Linux met flatpak-ondersteuning

gratis

UTM

macOS kan Windows, Linux, macOS en andere besturingssystemen in virtuele machines draaien. Apple is hiervoor echter wel een gebruikersinterface vergeten. UTM regelt dat alsnog en maakt van je Macs een universele pc.

Peter Siering

In macOS versie 10 (Yosemite) werd een hypervisor toegevoegd aan het besturingsstelsel en in versie 12 (Monterey) werden API's toegevoegd om virtuele machines te starten. Apple heeft daar nog geen GUI voor uitgebracht. Ondertussen zijn er verschillende softwareprojecten opgedoken die virtualisatie bruikbaar maken. UTM is momenteel bijzonder populair. De software is gratis te downloaden of voor 10 euro te koop via de App Store: de opbrengst is bedoeld om verdere ontwikkeling te financieren.

De interface van UTM zorgt ervoor dat je Linux, Windows en macOS met een paar muisklikken werkend krijgt in een virtuele machine. Virtuele machines kun je op basis van standaardcomponenten bij elkaar klikken of je kunt images uit een galerij selecteren. Afhankelijk van de cpu-architectuur van de Mac is ARM of x86 de juiste keuze. Dankzij de Rosetta-technologie van Apple, die 64-bit x86-code tijdens runtime vertaalt naar ARM-code, draaien 64-bit Linux-distributies voor x86 ook in een virtuele machine zonder dat emulatie ze vertraagt.

Onder de motorkap van UTM zit de universele emulator QEMU. Deze biedt virtuele machines een pc-achtige omgeving en helpt ook bij het beheer van virtuele resources zoals virtuele schijven, netwerken en grafische kaarten. De ontwikkelaars konden dat bijzonder eenvoudig regelen omdat Apple para-gevirtualiseerde stuurprogramma's in de virtuele machines implementeert via de VirtIO-interfaces. Met andere woorden, ze gebruiken beproefde technologie die algemeen wordt gebruikt in de Linux- en Windows-omgeving om de prestatieverslindende emulatie van apparaten te vervangen door een directe lijn naar virtualisatie.

UTM maakt geen geheim van zijn roots: als je met de hand virtuele machines maakt, laat de software zien wat QEMU kan: het biedt dan onder andere ook emulatie van een Rasp-

berry Pi 3B. Helaas werkt dat nog niet, wellicht wel met een verandering van QEMU 7.2 naar versie 8. De UTM-ontwikkelaars zijn echter nog niet overgestapt op QEMU 8 vanwege de sterk verminderde prestaties.

Wat UTM op dit moment nog mist zijn snapshots. Het belangrijkste wat daarvoor ontbreekt is een gebruikersinterface. QEMU die als basis wordt gebruikt kan dergelijke snapshots maken, afhankelijk van het formaat dat wordt gebruikt voor de virtuele schijven. Je kunt jezelf helpen met het programma `qemu-img`, dat je met homebrew installeert. Over vindingrijke gebruikers gesproken: de bugtracker op GitHub met ongeveer 600 tickets is het bewijs van een levendig ontwikkeling en veel actieve gebruikers; je kunt er zowel nuttige antwoorden als veel issues vinden.

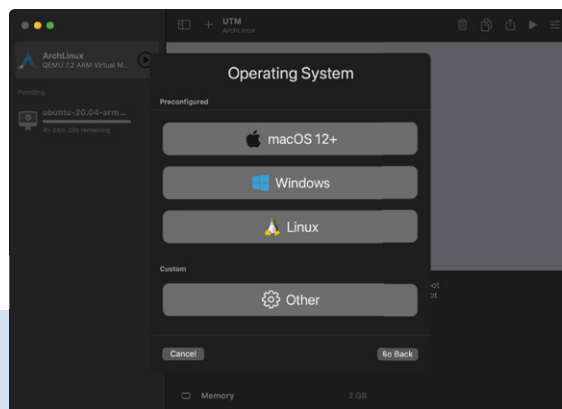
Voor de volledigheid: UTM draait ook op iOS-apparaten. Voor zover wij weten gebruikt het daar echter alleen QEMU-emulatie en executieversnelling, omdat Apple virtualisatie nog niet in het besturingssysteem heeft verankerd. In de praktijk werkte UTM zeer goed op een MacBook Air met een M3-processor en Sonoma als besturingssysteem. Volgens bugrapporten is het zinvol om een modern macOS te gebruiken omdat Apple geleidelijk aan de geïntegreerde virtualisatie uitbreidt, recentelijk met functies voor het suspenden en opnieuw opstarten van virtuele machines.

- ▲ prima interface, gratis/goedkoop
- ▲ veel virtuele machines beschikbaar
- ▶ (nog) geen UI voor snapshots

systeemeisen

macOS ab Version 12 (Monterey)

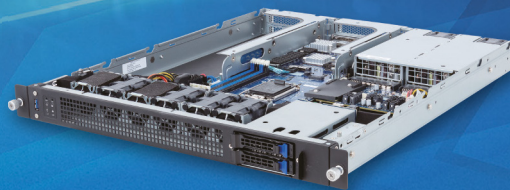
€ 10



GIGABYTE™

Setting the Standard for Excellence

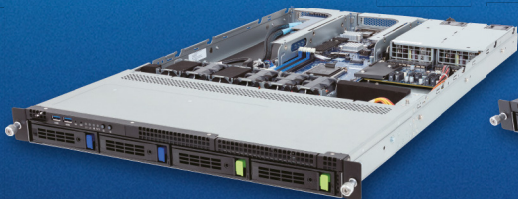
Intel® Xeon® E-2400 Solutions



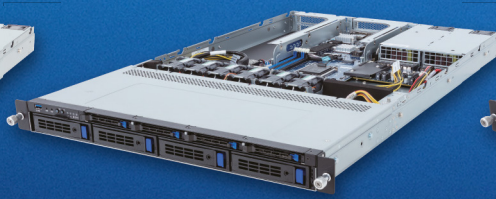
E133-X10



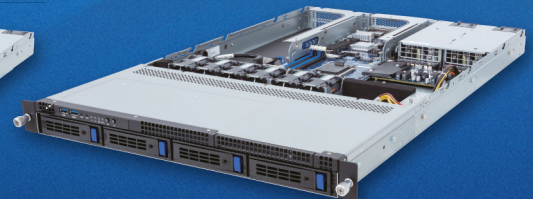
R123-X00



R133-X10



R133-X11



R133-X13



Discover Full Product Range
gigabyte.com/Enterprise

* Intel, the Intel logo, Xeon, and other Intel marks are trademarks of Intel Corporation or its subsidiaries.

Fedora 40 preview

Fedora 40 ziet er uit als een relatief weinig spectaculaire release. De grootste vernieuwingen zitten in de desktops. De KDE-versie gooit X11 eruit.

Niklas Dierking en Daniel Dupré

De Linux-distributie Fedora houdt zich meestal niet in als het aankomt op het introduceren van nieuwe technologie en nieuwe software op de desktop. Bij Fedora 40 zul je echter weinig nieuwe functies tegenkomen die niet te danken zijn aan de desktop-omgevingen Gnome 46 of KDE Plasma 6. We hebben de bètaversie bekeken.

Na het opstarten van het live systeem, wordt je begroet door het bekende Fedora installatieprogramma Anaconda. Eigenlijk wilden de ontwikkelaars Fedora 39 al van een nieuwe installer voorzien (Anaconda Web UI), maar dat lijkt vooralsnog helaas niet te gebeuren. Het werd eerst uitgesteld naar Fedora 40, toen naar versie 41, ten dele omdat de partitioneringstool op dat moment veranderingen direct doorvoert. Dat is een gedrag dat gebruikers van het oude installatieprogramma niet gewend zijn en kan leiden tot gegevensverlies.

DESKTOP BANDBREEDTE

Fedora 40 Workstation levert Gnome 46 als de desktopomgeving. Een van de meest prominente nieuwe functies is inloggen op afstand via RDP (Remote Desktop Protocol), zelfs als er op dat moment geen sessie actief is. Gebruikers configureren het inloggen op afstand in het nieuwe Systeem-paneel bij de instellingen. Bij een test werkte het op afstand inloggen op Linux-computers met

de Gnome-app 'Verbindingen', maar pas nadat we SELinux op de doelcomputer hadden uitgeschakeld. SELinux schakel je uit met het commando `sudo setenforce 0`. Hij blijft dan uitgeschakeld tot een herstart.

De Gnome-ontwikkelaars hebben ook het pad ingekort naar de globale zoekfunctie in de Nautilus-bestandsbeheerder, die nu kan worden geactiveerd via een knop in de linkerbovenhoek van het venster.

Voor het eerst ondersteunt Gnome 46 variabele framerate (Variable Refresh Rate, VRR) in Wayland-modus – mits de juiste hardware beschikbaar is. VRR synchroniseert de vernieuwingsfrequentie van de monitor met de uitvoer van de grafische kaart. De Gnome-ontwikkelaars bestempen de functie nog als experimenteel.

Fedora 40 wordt geleverd met de nieuwe KDE-versie Plasma 6. Het voorstel van de KDE SIG (Special Interest Group) van het Fedora-project om volledig op Wayland te vertrouwen en X weg te laten, leidde tot onvrede onder sommige leden van de Fedora-gemeenschap, maar won uiteindelijk. Als je X nodig hebt, kun je het installeren vanuit de Fedora-repository's.

VERBORGEN FUNCTIES

Fedora 40 bevat andere nuttige vernieuwingen die meer onder de radar verborgen blijven. De NetworkManager gebruikt nu ARP

(Address Resolution Protocol) om te controleren of een andere host in het netwerk al een gewenst IPv4 adres gebruikt, om zo adresconflicten te vermijden.

Bovendien wijst de NetworkManager nu een eigen MAC-adres toe aan elk draadloos netwerk, zoals Apple-apparaten dat al doen. Dat moet zorgen voor een betere gegevensbescherming bij het gebruik van wifi.

Bij Fedora 40 neemt de distributie afscheid van Delta-RPM's. Die werden oorspronkelijk geïntroduceerd zodat voor updates alleen het verschil met een bestaand pakket gedownload hoefde te worden. Met een snelle internetverbinding – waar tegenwoordig veel gebruikers over beschikken – duurde het vaak langer om een nieuw RPM-pakket samen te stellen uit een delta-RPM dan om simpelweg een bijgewerkte versie te downloaden.

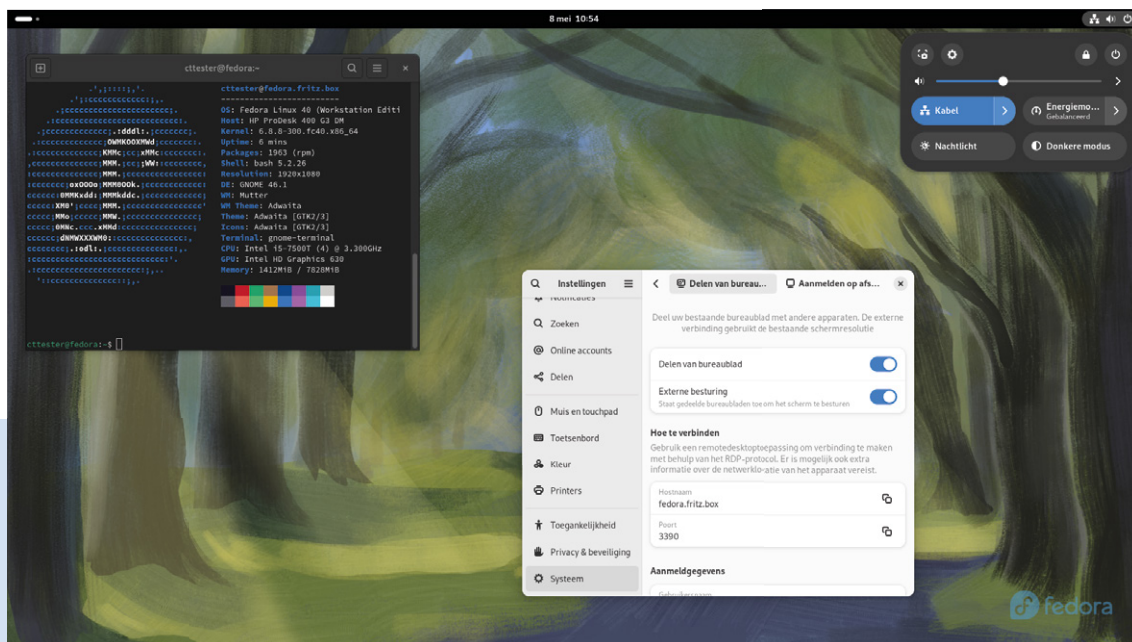
CONCLUSIE

Vergeleken met vorige Fedora-edities biedt Fedora 40 niet veel nieuws. Desalniettemin zullen Fedora-gebruikers blij zijn met nieuwere software en een vernieuwde desktop-omgeving. Fedora 40 is beschikbaar en zal tot mei 2025 van updates worden voorzien.

- ▲ **nieuwe Gnome-desktop**
- ▲ **veel ondergrondse vernieuwingen**
- ▼ **nieuwe installer weer uitgesteld**

systeemeisen
x86-64-processor
(2 GHz, dualcore),
15 GB opslag,
2 GB RAM
support
tot circa mei 2025

Gratis



MSI Commercial 14

MSI brengt een nieuw model laptop uit in zijn portfolio: de MSI Commercial 14. Zoals de naam al doet vermoeden is deze laptop gericht op de zakelijke gebruiker, met krachtige hardware en praktische voorzieningen om productief aan de slag te gaan. Maar MSI vergeet daarbij niet dat er ook nog een wereld buiten het werk is.

De MSI Commercial 14 is ontworpen voor professionals die onderweg top-prestaties nodig hebben. De specificaties zijn dan ook niet mis. Het kloppende hart van de laptop is een 13^e generatie Intel Core i7-13700H-processor. Die heeft 6 P-cores en 8 E-cores voor een totaal van 14 cores. Dankzij hyperthreading op de P-cores kunnen er 20 threads tegelijkertijd worden verwerkt, ideaal voor multitasken en veeleisende taken die veel cores benutten. Ook als je slechts een enkele taak snel wilt uitvoeren heeft de processor genoeg reserves, met een maximale turbofrequentie van 5 GHz voor een enkele performance-core.

Voor multitasken en het zonder haperingen switchen tussen verschillende taken is ook voldoende geheugen belangrijk en dat is bij de MSI Commercial 14 met 32 GB RAM ruim aanwezig. Dat is nog uit te breiden tot maximaal 64 GB. Je zult bij deze laptop ook niet snel gebrek aan opslagruimte hebben, aangezien de ingebouwde SSD een capaciteit van 1 TB heeft.

PRODUCTIEVER WERKEN

Topspecificaties zijn mooi, maar in de praktijk hangt productief werken vaak af van praktische details. Belangrijker nog dan een snelle laptop, is een laptop die je in staat stelt zo productief mogelijk te zijn – zonder hindernissen. De MSI Commercial 14 biedt verschillende zaken die daarvoor zorgen.

Zo biedt het 14-inch IPS-display met een resolutie van 1920 × 1200 pixels een goed evenwicht tussen draagbaarheid en voldoende werkoppervlak. De beeldverhouding van 16:10 is voor productief bezig zijn een stuk praktischer dan de bij laptopschermen gangbare 16:9 beeldverhouding. Je hebt meer ruimte in de hoogte voor teksten, webpagina's, tabellen enzovoort. Een tweede scherm is makkelijk aan te sluiten via de HDMI-poort of via de USB-C-connector met Thunderbolt 4. Dat laatste maakt zelfs het doorlinken van een derde scherm zonder extra kabel naar de laptop mogelijk (de 'matrix display'-functie van Thunderbolt 4).

Ook praktisch is de mogelijkheid om biometrisch in te loggen of de laptop te ontgrendelen met Windows Hello, zonder steeds je

wachtwoord te hoeven invoeren. Dat kan zowel met de in het toetsenbord ingebouwde vingerafdruks scanner als via gezichtsherkenning met de ingebouwde webcam. Die webcam is ook praktisch voor videoconferenties, die je dankzij MSI AI kunt houden met goede beeld- en geluidskwaliteit. De beeldkwaliteit bij slechte belichting wordt hierdoor verbeterd en de AI Noise Cancellation Pro zorgt dat je stem accuraat en zonder storende omgevingsgeluiden wordt doorgegeven.

Andere praktische kenmerken van de MSI Commercial 14 zijn bijvoorbeeld de MSI Center software waarmee je makkelijk schakelt tussen verschillende bedrijfsmodi van de laptop voor verschillende taken en omstandigheden en de aanwezigheid van een netwerkpoort voor een bekabelde netwerkverbinding. Veel laptops hebben zo'n poort tegenwoordig niet meer. Het kan echter erg praktisch zijn om snel met een netwerk te verbinden door eenvoudigweg een kabel in te pluggen, in plaats van wifi-gegevens te moeten invoeren.

VERANTWOORD ONDERNEMEN

Dankzij de krachtige specificaties en praktische voorzieningen kun je met de MSI Commercial 14 productief aan de slag, maar MSI heeft ook oog voor andere zaken zoals duurzaamheid. Ook in dat opzicht is het een verantwoorde aankoop, onder meer door de gebruikte materialen. Zo is voor de bouw van de laptop gebruik gemaakt van PCR plastic (Post-Consumer Recycled). Dat is gerecycled plastic dat af-

komstig is uit afgedankte producten van consumenten, instellen en bedrijven – en dat is de grootste afvalstroom ter wereld. Het gebruik van dat materiaal draagt niet alleen bij aan een duurzame laptop, maar ook aan een groenere wereld. Ook bij het verpakkingsmateriaal is gebruikgemaakt van duurzame materialen.

Een lange levensduur van de laptop draagt ook bij aan duurzaamheid en dat wordt bijvoorbeeld bereikt door de robuuste constructie. Alle MSI-laptops ondergaan enorme strenge tests, zodat ze voldoen aan de militaire norm MIL-STD-810H. Het morsbestendige ontwerp van het toetsenbord voorkomt bovendien dat per ongeluk gemorste vloeistof het moederbord en andere componenten bereikt, zodat ook dat risico beperkt wordt.

Om het plaatje compleet te maken, is de laptop ook nog voorzien van snel Wi-Fi 6E en Bluetooth 5.3 voor draadloze connectiviteit, 3 USB type A-poorten voor diverse randapparaten (USB 3.2 Gen 1) en uiteraard Windows 11 Pro. Dat alles is verpakt in een compacte behuizing van 31,4 × 23,6 × 1,9 cm die eenvoudig in een laptoptas past en met een gewicht van 1,6 kg makkelijk mee te dragen is.





PICAMKIT

▷ kck.st/4diA2BR • vanaf € 130

Arducam heeft een kant-en-klare Raspberry Pi 5-camera (met tripod-schroefdraad) gemaakt: de Pivstation 5. Er zijn drie varianten voor specifieke toepassingen en bepaalde lenzen, die bij de kits inbegrepen zijn. Voor een perfecte autofocus en zeer hoge resolutie is er de Hawkeye met 64 megapixel met dual-modus autofocus. De Darksee is voor ultra-low light-omstandigheden met een ultragevoelige sensor van Sony met STARVIS2-tech, NIR-boosted, 8 megapixel en low-noise. En als laatste is er de Klarity met wederom een Sony-sensor, 20 megapixel en extreme scherpte voor zowel een hoge resolutie als hoge gevoeligheid. Alle kits hebben een Raspberry Pi 5 met 4 GB RAM ingebouwd en verbruiken 7,5 watt. Als add-ons zijn er adapterringen voor lenzen van Nikon en Canon.



www.ct.nl/softlink/2407032



VERRIJKT GELUID

▷ kck.st/4aZUPrT • vanaf € 560

Draadloze speakers met RGB? Nou, dat kan wel extravaganter: de Haloasis A1 gebruikt holografische projectie dankzij minileds. Hij zou niet misstaan in een scène uit de sci-fi actie-RPG Cyberpunk 2077. Hij biedt niet alleen visualisaties (360 graden zichtbaar) van je muziek en het weergeven van songteksten (hallo karaoke-avond!). Als de speaker namelijk geen audio-input krijgt, kan hij alsnog zwevende content tonen als een screensaver, zoals de tijd, het weer of andere informatie. De A1 biedt daarnaast aan beide zijanten ook nog RGB-ringen voor extra sfeerverlichting. De vormgeving doet wat denken aan een rol die in een houder hangt. Hij heeft naast twee speakers een ingebouwde downfiring subwoofer. De A1 werkt naadloos samen met Spotify, YouTube Music, Apple Music, Amazon Music en Tidal en je verbindt via Bluetooth 5.0. De speaker is ook verticaal te plaatsen. Bedienen kan behalve via de app ook via een touchpanel.

DESKTOP-CNC

▷ kck.st/3TZlfdk • vanaf € 1305

Met de Carvera Air haal je een slimme en veelzijdige compacte CNC-machine in huis. Hout, plastic, aluminium, koper, was, epoxy en zelfs het maken van (dubbelzijdige) pcb's is een optie. De machine is opgebouwd met een stevig die-cast frame en een volledig af te sluiten behuizing tegen stof en vuil – naast veiliger voor jezelf ook nog geluiddempend. De Air werkt in combinatie met de bekende CAD/CAM-software als AutoCAD, Fusion 360 en meer, en de maker stopt er zijn eigen CAM-software bij. Epoxy, laseren en pcb-opties zitten in add-ons, en ook materialen zijn via add-ons te verkrijgen. De machine is 50 bij 45 bij 45 centimeter groot, het werkoppervlak 30 bij 20 bij 13 cm bij 3-assen en 9,2 bij 20 centimeter bij 4-assig-werk. Bedienen kan via usb en wifi, en de controllersoftware werkt op alle gangbare (mobiele) besturingssystemen.





OP DE RAILS

▷ Android / iOS
(gratis)

Als je het leuk vindt om met treinen (klein of groot) in de weer te zijn, is het rails leggen tussen station(s) in **Teeny Tiny Trains** een prima (en lichtelijk verslavend) tijdverdrijf. Het spel begint rustig met wat uitleg: leg de juiste stukken spoor op hun plek om de trein het station te laten bereiken. Dat kan door te tekenen of de juiste stukken te selecteren. Uiteraard wordt het steeds lastiger, met meer stations en treinen en het aanpassen van instellingen voor bepaalde spoordelen waarbij

je er uiteraard voor moet waken dat de treinen niet tegen elkaar opbotsen of ontsporen.

Soms moet je ook letten op welke trein er het eerste een station binnen mag rijden. Dat mondt uit in goed vooruit plannen en uiteraard na af en toe de nodige ontsporingen en botsingen de boel toch weer netjes op de rails krijgen. Je bent met de gratis versie wel even zoet, als je alle hoofdstukken wil vrijschakelen kost je dat eenmalig 4 euro. Leuk extraatje: via de community worden zelfgemaakte levels gedeeld, zodat je vrijwel nooit uitgespeeld raakt.

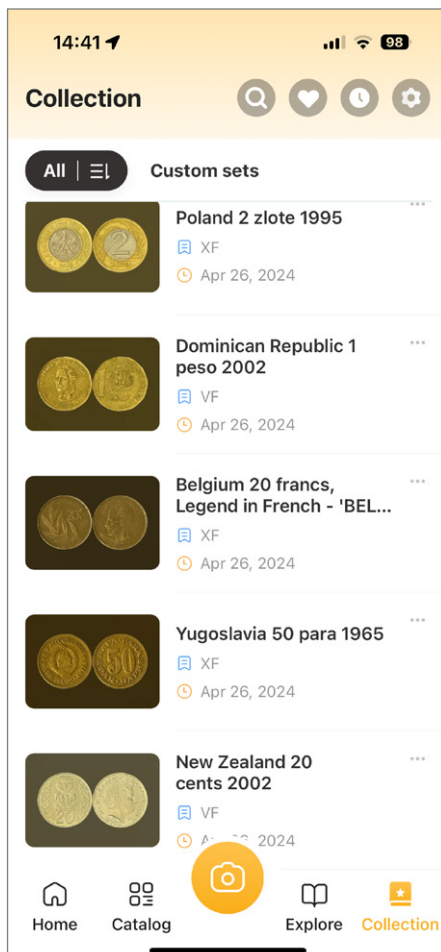


BEWUST BRUIN

▷ iOS (gratis)

Lekker dat de zon weer uitbundig schijnt, maar het blijft belangrijk om niet te enthousiast onbeschermd buiten rond te lopen. **Sunbeam: UV Index** helpt je om verantwoord in de zon te zijn. Als je je huidtype invult (volgens de Fitzpatrick-huidtypering, uitleg staat er netjes bij), en je opgesmeerde SPF-factor instelt, kan er gerichtere informatie worden getoond. Met het overzicht voor de komende uren en dagen weet je precies hoe fel de zon zijn werk gaat doen en wanneer de fles zonnebrandcrème weer opnieuw erbij gepakt moet worden.

De uitgebreidere (smeer)informatie en ook de hoeveelheid vitamine D die je theoretisch kunt binnenhalen zitten achter het Pro-abonnement van een bescheiden 9 euro per jaar. Voor vitamine D (ook niet onbelangrijk) is een dagelijks doel in te stellen: in Nederland en België is de zonkracht in het algemeen niet al te groot, dus elke hap verantwoord vitamine D binnenkrijgen is welkom. Ook op vakantie in landen dichterbij de evenaar is gerichtere anti-zonnebrandinformatie absoluut geen overbodige luxe.

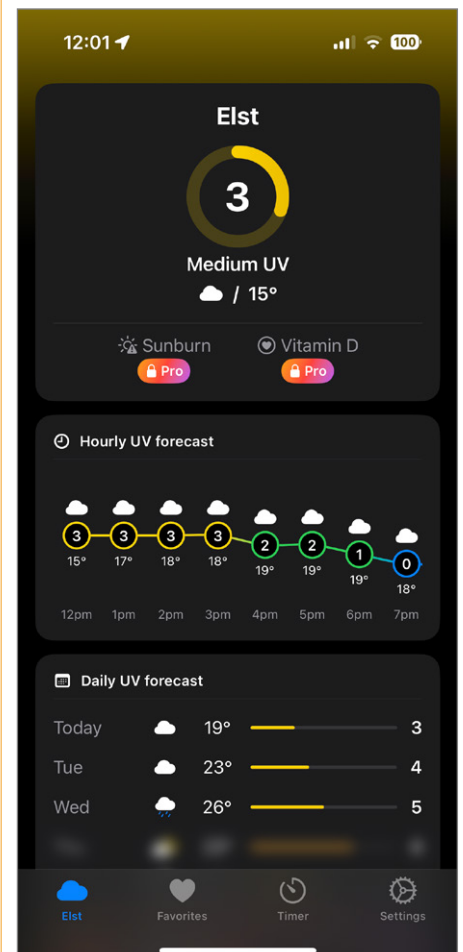


WISSELGELD

▷ Android / iOS
(gratis)

Ergens weggestopt in menige la ligt een stoffig doosje met onbekende munten: toch stiekem wel leuk om te achterhalen wat ze zijn en of ze nog wat waarde hebben. **Coin-Snap: Coin Identifier** maakt snel plaatjes van de voor- en achterkant van je munten en gaat dan aan de slag met identificeren. Hij geeft niet alleen aan wat hij denkt dat het muntje is en in welke periode het beschikbaar was, maar ook welke kwaliteit het heeft. Het herkennen ging bij onze testmunten prima, zelfs met wat slecht leesbare munten, maar de staat van de munten kun je beter zelf aangeven, dat is blijkbaar nog vrij lastig.

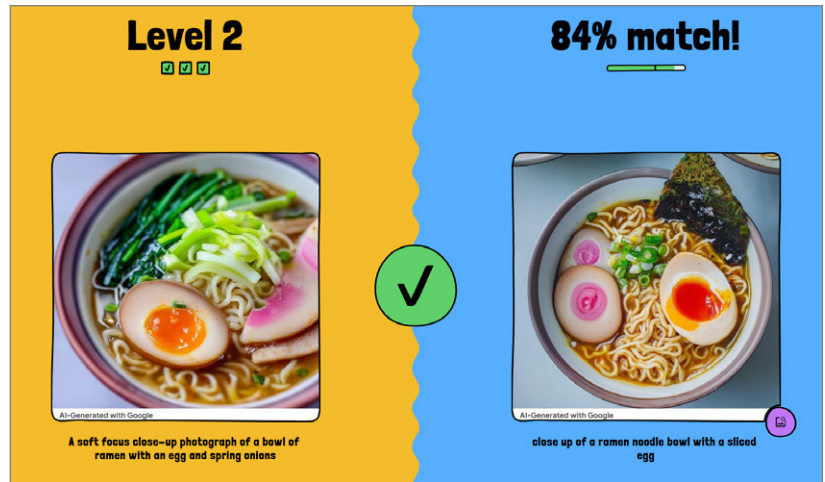
Na het herkennen voeg je de munt(en) eventueel toe aan je collectie. Als je er een meer nauwkeurige gradatie bij invoert krijg je een betere schatting van de waarde. Naast dat alles biedt de app ook toegang tot veel informatie over (munt)geld, van bijzondere munten tot boeken. Met het gratis account kun je met een kleine collectie meer dan prima vooruit, anders ontgrendel je voor 30 euro per jaar meer opties.



PROMPTIDOM

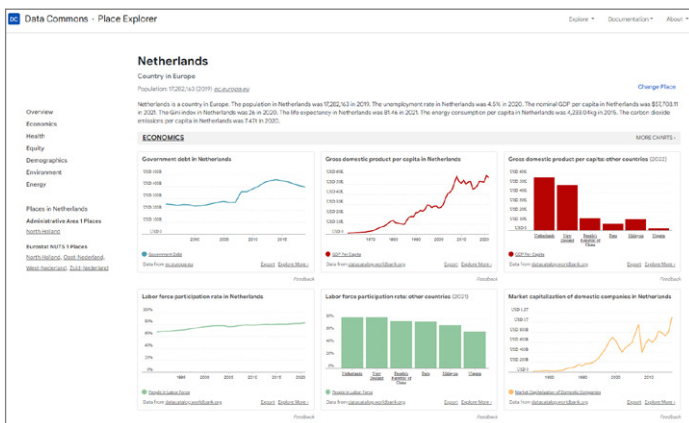
▷ experiments.withgoogle.com/say-what-you-see

Prompts gebruiken lijkt erg makkelijk, maar laten we eerlijk zijn: het kan nooit kwaad om je daar toch wat fatsoenlijker in te verdiepen. Het zit hem toch echt in de details. En dat maakt **experiments.withgoogle.com/say-what-you-see** makkelijk via een soort van gamification: de site laat je omschrijven wat je op een door Google AI gegenereerde afbeelding ziet met een prompt en schotelt je een score voor (hoeveel procent je matcht). Je eigen prompt tekent dan uiteraard ook je eigen afbeelding en zo leer je niet alleen beter omschrijven wat je wilt, maar het maakt ook kleine aanpassingen meteen zichtbaar. Tijdens het leren krijg je tips om je prompt te verbeteren. Maar let wel op: je krijgt maar drie promptpogingen per level (elk level bestaat uit drie afbeeldingen) om door te kunnen.



PUBLIEKELIJK VEEL DATA

▷ datacommons.org

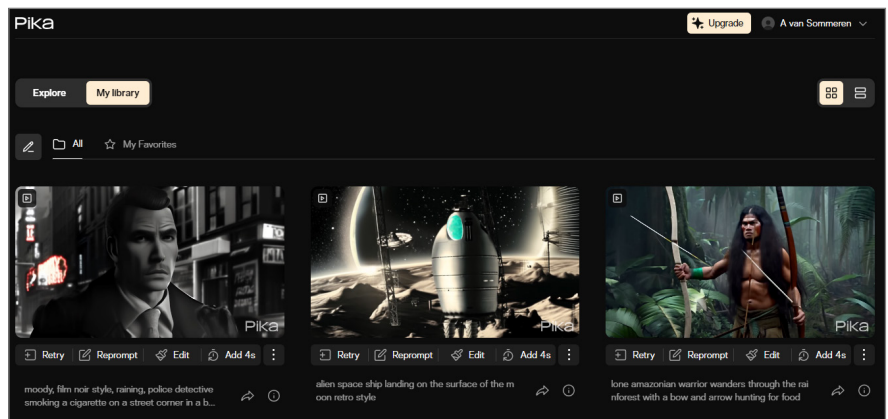


Veel data is publiekelijk toegankelijk, maar hoe struin je daar makkelijk doorheen? Via **datacommons.org** kun je op een eenvoudige zoekbalk je zoekopdracht opgeven en zo zoeken in onder meer vrij beschikbare agrarische, biomedische, demografische, economische, onderwijstechnische en gezondheidsinformatie. Google heeft er een makkelijk doorzoekbaar geheel van gemaakt voor iedereen die de openbare data (nuttig) kan gebruiken. Ben je een ontwikkelaar? Dan regel je via REST-, Python- en Google Sheet-API's toegang tot alle data voor onderwijs, academische- en journalistieke onderzoeken. De site heeft wel veel Amerikaanse data, maar er zit informatie uit 256 landen in verwerkt. Als je geen zin hebt om gericht te zoeken, kun je ook rustig door onderwerpen heen struinen, of de diverse losse tools gebruiken voor informatie over plaatsen, kaarten of statistische variabelen. Er zijn zelfs tutorials voor het analyseren van data met de API's.

VIDEOGENERATIE

▷ pika.art

Via **pika.art** kun je korte videofragmenten (en ook stilstaande beelden) in elkaar draaien. Alles begint natuurlijk met het invoeren van een mooie uitvoerige prompt, waarbij je in dit geval lip-sync kunt aanzetten en geluidseffecten of bestaand beeldmateriaal kunt toevoegen. Vooraf zijn er ook nog wat uitgebreide aanpassingen zoals het aantal fps en hoe sterk de beweging moet zijn, of de beeldverhouding of specifieke stijl aan te vinken of te tweaken. Het uiteindelijke resultaat is slechts een paar seconden lang, maar soms neemt het genereren genoeg tijd in beslag voor een snel kopje koffie. Met een betaald abonnement maak je de lengte van je video langer en is het resultaat te upscalen. Soms zijn de resultaten zelfs met vrij weinig informatie al erg goed ogend. Bekijk zeker ook de galerij via het explore-tabblad voor de nodige inspiratie.



NO REST FOR THE WICKED

▷ Moon Studios GmbH / Private Division • vanaf € 40 • Windows, PS5, Xbox series X/S

In *No rest for the wicked* ben je een Cerim, een strijder die is toegewijd aan het uitroeien van de Pestilence, een oude plaag. Die lijkt na de recente dood van de koning te zijn teruggekeerd en jij gaat op onderzoek naar het eiland Isola Sacra om die geruchten te onderzoeken.

Een lokale groep rebellen laat je schip stranden en je spoelt zonder wapens of uitrusting aan op het eiland. Zo begint dit actie-avontuur, waarin je verzeild raakt in een strijd tussen verschillende facties. Het gaat in deze game niet zozeer om het verhaal, maar meer om de actie. En hoewel je soms je weg moet zoeken, kunt koken, bouwen en meer, gaat die actie toch vooral om het vechten.

De reis aan boord van het schip dient als een soort tutorial, waarbij de basis van het bewegen en vechten kort geïntroduceerd wordt. Dat is geen kwestie van blind op knoppen drukken, maar vraagt om goede reacties en timing. Je kunt aanvallen blokkeren, weggrollen of rennen om ze te ontwijken.

Aanvallers hebben bepaalde patronen en je kunt daar met jouw bewegingen op inspelen om schade te vermijden of aanvallers zelfs tijdelijk te verlammen. Het is bepaald niet makkelijk en doet denken aan *Dark Souls*-games, hoewel de knoptoewijzingen net anders zijn. We hebben het over knoppen, want de game speelt het best met een controller en dat wordt door de ontwikkelaars ook aanbevolen.

Enmaal op het eiland kun je allerlei wapens vinden en het wapen bepaalt hoe je beweegt en hoe (snel) je aanvalt. Ook het



totale gewicht van alles wat je met je meedraagt is daarop van invloed: als je zwaarbent, ben je veel langzamer, maar kun je bijvoorbeeld wel tegenstanders een schouderduw geven.

Behalve wapens kun je ook beschermende uitrusting, ingrediënten voor bijvoorbeeld (helende) maaltijden, sleutels voor deuren of poorten en allerlei andere items vinden of kopen van andere personages.

Maar gevechten blijven het belangrijkste aspect en zijn meestal niet te vermijden. Wie houdt van een uitdaging, kan hier veel plezier uit halen – anderen zullen tevergeefs zoeken naar een optie om de moeilijkheid aan te passen.

Drankjes om je gezondheid te herstellen kun je alleen gebruiken met een pauze ertussen. Daar komt bij dat je maar beperk-

te plek hebt om spullen mee te dragen en je wapens en uitrusting slijten en steeds gerepareerd moeten worden. Er zijn ook relatief weinig punten ('whispers') waar je je voortgang kunt bewaren.

Zoals bij de meeste actie-RPG's zit er niet veel roleplaying in, maar je kunt wel als je genoeg ervaringspunten verdient je karakter aanpassen. Zo kun je je 'poise' verhogen om zelf steviger op je benen te staan of juist je levenspunten verhogen, je snelheid, hoeveel je kunt dragen en andere kenmerken verbeteren.

Enmaal in de grote (vervallen) stad op het eiland aangekomen heb je nog meer mogelijkheden. Je kunt je wapens of beschermende uitrusting verbeteren, een woning betrekken en van alles maken, ook om je woning te verfraaien.

Je komt allerlei karakters tegen die je daarbij kunnen helpen en waar je items en ingrediënten kunt kopen of verkopen. De stemacteurs bij gesproken dialogen zijn niet altijd even overtuigend, maar het geluid is verder sfeervol.

Grafisch is *No rest for the wicked* soms wat donker maar zeer fraai, met afwisselende omgevingen en mooie lichteffecten en animaties van de karakters.

Het gevoel van de wereld ontdekken is aanwezig, doordat de kaart pas wordt onthuld als je een gebied verkent. De game lijkt helaas niet erg geoptimaliseerd, met zeer traag opstarten en haperingen op minder krachtige systemen.

Maar als je pc en jijzelf het aankunnen en je echt houdt van een uitdaging, is dit een spel dat je niet met rust laat.



OPSCHALEN

Maak je LAN sneller

Je NAS heeft een snelle 2,5Gbit/s-aansluiting en het moederbord van je pc ook, maar het versturen van grote bestanden gaat nog steeds met een trage 115 MB/s? Dat kan ook anders.

Ernst Ahlers en Noud van Kruysbergen



ALLES OVER DIT ONDERWERP

- | | |
|---|-----------|
| ▶ Maak je LAN sneller | 36 |
| ▷ Slimme switches voor snelle netwerken | 40 |
| ▷ Uitleg switchfuncties | 44 |

Er zijn talloze redenen om je netwerk sneller te gaan maken. En dat kun je op zich ook zonder al teveel speciale kennis in een handomdraai doen: vervang bijvoorbeeld gewoon de oude gigabit-ethernet-switch door een modernere versie. Dat zal de maximale doorvoersnelheid sowieso al verdubbelen van 115 naar 230 MB/s. Je hoeft daar geen nieuwe kabels voor te leggen. Als je de switch niet kunt vervangen omdat die bijvoorbeeld in de router zit, dan kun je daarop altijd nog een nieuwe, snellere aansluiten.

In principe kun je kiezen tussen switches voor 2,5, 5 en 10 Gbit/s, maar een upgrade van de gebruikelijke 1 Gbit/s (1G) naar 2,5 Gbit/s (2G5) loont waarschijnlijk het meest. Sinds een paar maanden zijn er al bruikbare 2G5-switches te koop voor minder dan 100 euro [1].

Een snelle switch versnelt sowieso elk dataverkeer via je netwerk, maar de grootste tijdswinst zit hem in toegang tot grote video's, fotodatabases, back-ups en bij het verplaatsen van images van virtuele machines.

Een 2G5-switch legt ook de basis voor de volgende wifi-upgrade, aangezien Wi-Fi 6 onder gunstige omstandigheden al meer dan 1 Gbit/s naar mobiele apparaten kan versturen. Wi-Fi 6E verdubbelt dat zelfs als twee clients tegelijkertijd gegevens verzenden op verschillende frequentiebanden (5 en 6 GHz). Als dergelijk verkeer via een 1G-switch loopt, wordt de snelheid tot dat niveau teruggebracht.

Bij onze test haalde de nieuwe Wi-Fi 7-standaard, die je nu in steeds meer apparaten tegen zult gaan komen, al een gemiddelde van 2,7 Gbit/s op de 6GHz-band, en op piekmomenten zelfs al bijna 4 Gbit/s [2]. Een Wi-Fi 7-basisstation moet daarom ten minste een 2G5-verbinding hebben om ervoor te zorgen dat het kabelnetwerk het wifi niet vertraagt. Als het wifi met drie radiomodules werkt voor drie frequentiebanden, dan is 5G-ethernet aan te raden. Goede Wi-Fi 7-accesspoints hebben standaard zelfs 10G-interfaces.

Tot slot ligt de volgende versnelling van internettoegang in het verschiet: internet via de kabel en zeker via glasvezel wordt steeds sneller – 1 Gbit/s is al zo'n beetje standaard en upgrades richting de 10 Gbit/s zijn al beschikbaar. Als je zo'n upgrade wilt doorvoeren, zul je het downloaden en uploaden in je eigen netwerk niet de bottleneck willen laten zijn en moet je minstens 2G5-ethernet hebben.

Het volgende artikel beschrijft een aantal praktische aspecten van het gebruik van multigigabit-switches. We hebben een aantal apparaten die als managed switches ook aan hogere eisen voldoen op een rijtje gezet.

Bij die eisen horen het van stroom voorzien van wifistations en camera's via de netwerkkabel (Power-over-Ethernet, PoE), het kunnen instellen van netwerkzones (VLAN's) en netwerkdiagnostiek. In het artikel erna leggen we de functies van de switches in detail uit, zodat je er makkelijker een kunt kiezen.

OUDE KABELS KUNNEN BLIJVEN

Het mooie van multigigabit-ethernet is dat het werkt op je oude kabels. De bijbehorende NBase-T-standaard (IEEE 802.3bz) levert 5 Gbit/s – zelfs over CAT5e-kabels. Dat type kabel was oorspronkelijk alleen ontworpen voor 1 Gbit/s tot 100 meter. Alleen voor 10 Gbit/s (10GBase-T) heb je minimaal CAT6a nodig voor de maximale afstand.

Bij nieuwbouw of renovatie moet elke kamer dan twee netwerkaansluitingen hebben. Idealiter komen de datakabels terecht in flexibele buizen, die een elektricien kan aanleggen. Dan kun je de kabels later verwisselen zonder allerlei muren open te hoeven breken.

Als je aan de verre toekomst denkt is CAT8, dat waarschijnlijk ook 40 Gbit/s over korte afstanden aankan, de juiste keuze. Voor alle anderen volstaat het goedkopere CAT7. Om twee kabels door een flexibele beschermingslang te laten passen, moet die een binnendiameter van minstens 17,5 millimeter hebben (type EN 25).

Je kunt bij nieuwbouw bij het aanleggen van een netwerk geld besparen door de bouwers de kabels zelf in de flexibele buizen te laten trekken en die naar een centrale plek in huis te laten lopen. In [3] staat daar wat basisinformatie over.

GLASVEZEL IN PLAATS VAN KOPER

Ethernet via een koperen kabel met RJ45-stekkers zal in de nabije toekomst waarschijnlijk de standaarduitrusting blijven voor kantoor- en thuis-elektronica omdat dat een stabielere en permanent snellere verbinding biedt dan wifi.

Bij kleine bedrijven en thuis kan glasvezel een goed alternatief voor koperkabels zijn, bijvoorbeeld als er bijgebouwen moeten worden aangesloten of er verschillende verdiepingen moeten worden overbrugd. Een optische verbinding voorkomt dan problemen die veroorzaakt kunnen worden door eventuele potentiaalverschillen tussen verschillende groepen. Bovendien is het bereik groter: tot 500 meter met 10GBase-SR voor 10 Gbit/s op multimode-draden.



Je kunt pc's en laptops aansluiten op een snel netwerk via een ingebouwde netwerkkkaart of een usb-adapter. Via usb is eenvoudiger, maar dat kan momenteel niet zonder verlies bij 5G-ethernet.

Bij het upgraden van een netwerk zijn SFP+-slots op een switch geen overbodige luxe, zelfs niet als je in eerste instantie niet van plan bent met glasvezel te gaan werken. Het slot kan ook een extra koperen socket worden met een NBase-T-module als er op een gegeven moment een gebrek aan poorten is – en dat moment is er altijd eerder dan je denkt.

PC-UPGRADE

Als je een oudere computer wilt voorzien van een nieuwe netwerkkaart, zijn er al 2G5-kaarten te koop vanaf 20 euro. De Delock 81260 is een 5G-kaart die we tegenkwamen voor zo'n 50 euro. NBase-T-kaarten die zelfs tot 10 Gbit/s gaan zijn ook al te koop vanaf 70 euro.

Usb-adapters om te upgraden zijn momenteel alleen de moeite waard voor 2G5. Sommige zijn ook geschikt voor 5G-ethernet, maar die gebruiken USB 3.2 Gen 1 met 5000 Mbit/s. Er gaat dan wat snelheid verloren door de timingreserves in het usb-protocol, dus je hoeft niet meer dan 3,5 Gbit/s netwerkdoorvoer te verwachten.

Tot nu toe zijn we nog geen ethernetadapters voor USB 3.2 Gen 2x2 tegengekomen die met 20 Gbit/s aan de usb-kant tot 10 Gbit/s van het netwerk naar de pc kunnen sturen. De USB 4-hubs met een ethernetpoort die op dit moment beschikbaar zijn, bieden alleen 2G5. Als je meer wilt, moet je eens kijken naar Thunderbolt-docks – die dan wel minstens 200 euro kosten.

Wanneer we 2G5 of 5G schrijven als afkorting voor 2,5 of 5 Gbit/s ethernet, betekent dat ook de lagere snelheidsniveaus van 100 Mbit/s en 1000 Mbit/s, ook bekend als 1GE worden ondersteund. Dat komt omdat de ethernetstandaarden op elkaar voortborduren en compatibiliteit met de belangrijkste voorgangers verplicht is.

GELD EN ENERGIE

Meer snelheid kost meer: eenvoudige multigigabit-switches voor 2,5 Gbit/s met een handvol poorten zijn momenteel te koop vanaf ongeveer 70 euro, terwijl gigabit-ethernetversies maar een paar tientjes kosten. Het prijsverschil zal waarschijnlijk kleiner worden naarmate de aantallen toenemen.

De managed versies (zie het volgende artikel) kosten meer. Bij PoE-switches is het verschil kleiner omdat de basisprijs door de extra elektronica sowieso hoger is. Je betaalt ook meer gebruikskosten: een poort met een 1000Mbit/s-verbinding (gigabit-ethernet) verbruikt ongeveer 0,3 watt, maar bij 2G5 is dat al zo'n 0,8 watt. Het energieverbruik neemt ongeveer lineair toe – bij 10 Gbit/s moet je op ongeveer 2 watt per poort rekenen.

Hoe meer snelle apparaten op de switch aangesloten zijn, des te hoger het energieverbruik in ruststand. Het opgenomen vermogen neemt echter nauwelijks toe wanneer de switch gegevens aan het versturen is. Het idle-verbruik is daarom bepalend voor de elektriciteitsrekening. We hebben als basisverbruik bij eenvoudige 2G5-switches 2 tot 5 watt gemeten met een 1G-verbinding [1].

Het sneller maken van je netwerk thuis of op kantoor is dus niet gratis. Maar als je het geld ervoor overhebt, gaat het kopiëren van grote bestanden een stuk sneller en ben je voorbereid op de snellere internettoegang die binnenkort waarschijnlijk overal gaat komen.



Literatuur

- [1] Ernst Ahlers en Marco den Teuling, Snelle ethernetswitches om kleine netwerken te upgraden, c't 1-2/2024, p.100
- [2] Ernst Ahlers en Alieke van Sommeren, Vier Wi-Fi 7-basisstations met drie clients, c't 5/2024, p.60
- [3] Andrijan Möcker en Alieke van Sommeren, Goedkope snelle netwerkbekabeling voor thuis, c't 8-9/2023, p.98

Datasnelheden van netwerktechnieken en pc-interfaces

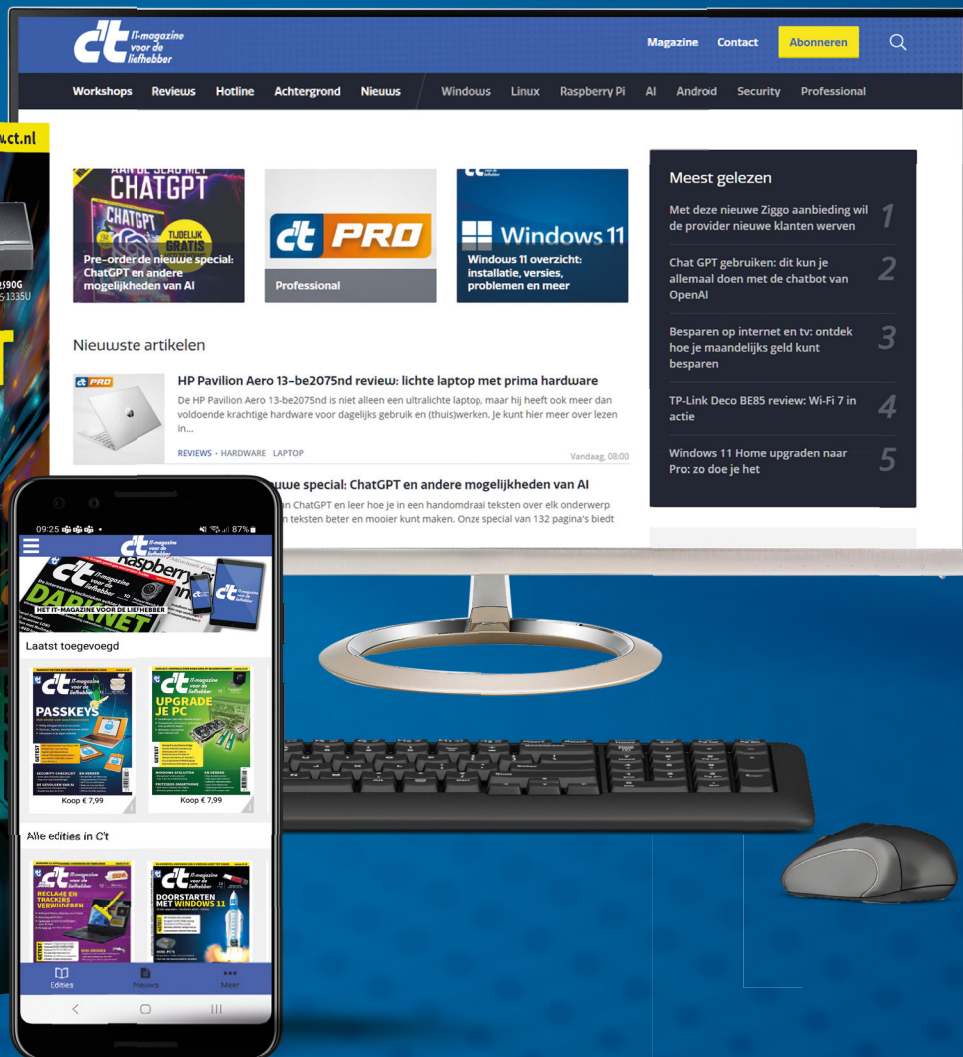
Techniek	Standaard	Bruto snelheid ¹	Netto snelheid ²	In MB/s ²
NFC	ISO/IEC 14443 / 15693	0,0004 Gbit/s	0,0004 Gbit/s	0,05 MB/s
Bluetooth	2.1/3.0/4.2/5.3 (EDR)	0,003 Gbit/s	0,0021 Gbit/s	0,26 MB/s
Fast ethernet	100Base-T	0,1 Gbit/s	0,094 Gbit/s	tot 11 MB/s
Wifi	Wi-Fi 4 (IEEE 802.11n)	0,072–0,3 Gbit/s	0,036–0,15 Gbit/s	tot 20 MB/s
USB	2.0 ³	0,48 Gbit/s	0,38 Gbit/s	tot 45 MB/s
Wifi	Wi-Fi 5 (IEEE 802.11ac)	0,433–1,73 Gbit/s	0,24–1,05 Gbit/s	tot 130 MB/s
Gigabit-ethernet	1000Base-T	1 Gbit/s	0,94 Gbit/s	tot 115 MB/s
Wifi	Wi-Fi 6 (IEEE 802.11ax)	0,6–2,4 Gbit/s	0,3–1,6 Gbit/s	tot 190 MB/s
Multigigabit-ethernet	NBase-T 2.5	2,5 Gbit/s	2,4 Gbit/s	tot 280 MB/s
USB	3.0 = 3.2 Gen 1 ³	5 Gbit/s	4,0 Gbit/s	tot 480 MB/s
Multigigabit-ethernet	NBase-T 5	5 Gbit/s	4,7 Gbit/s	tot 560 MB/s
SATA	3 (6G) ³	6 Gbit/s	4,5 Gbit/s	tot 560 MB/s
Wifi	Wi-Fi 7 (IEEE 802.11be)	0,7–11,5 Gbit/s	0,5–8,0 Gbit/s	tot 1000 MB/s
USB	3.2 Gen 2 ³	10 Gbit/s	8,0 Gbit/s	tot 1100 MB/s
10-Gigabit-ethernet	10GBase-T/SR/LR	10 Gbit/s	9,4 Gbit/s	tot 1100 MB/s
USB	3.2 Gen 2x2 ³	20 Gbit/s	17 Gbit/s	tot 2100 MB/s
25-Gigabit-ethernet	25GBase-T/xR ⁴	25 Gbit/s	24 Gbit/s ⁵	tot 2900 MB/s ⁵
40-Gigabit-ethernet	40GBase-T/xR ⁴	40 Gbit/s	38 Gbit/s ⁵	tot 4600 MB/s ⁵
100-Gigabit-ethernet	100GBase-T/xR ⁴	100 Gbit/s	94 Gbit/s ⁵	tot 11.000 MB/s ⁵

¹ Hangt voor wifi in de praktijk af van de hardware-uitrusting van de apparaten (aantal antennes) en van de gebruikte band, de bruikbare signaalbreedte en de afstand

² Voor grote bestanden met ethernet en wifi, waarbij wifi sterk beïnvloed wordt door de bezetting van de draadloze band door naburige netwerken

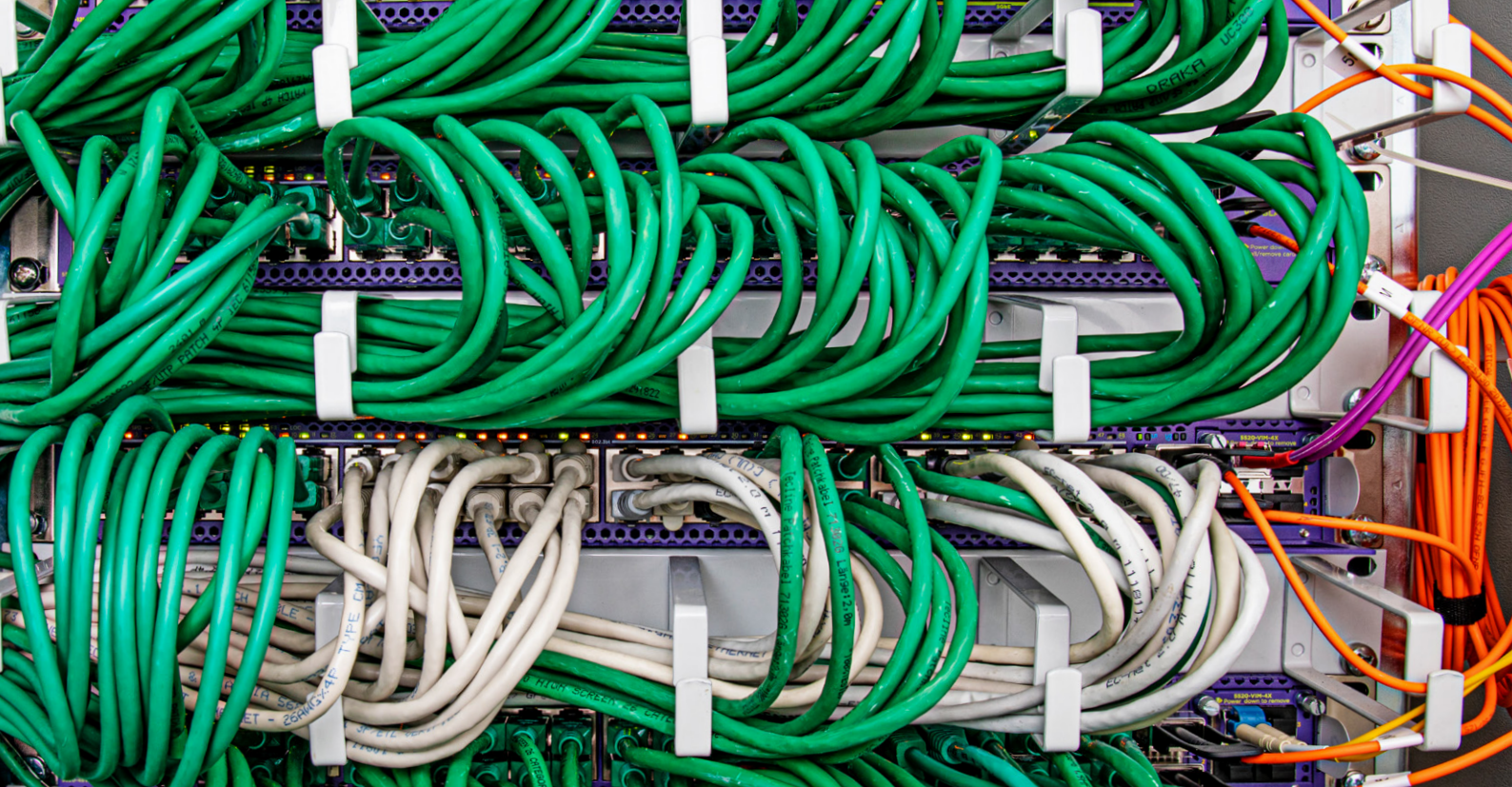
³ Netto snelheid is afhankelijk van chipsets in pc's en apparaten voor massaopslag ⁴ Verschillende mediatypen, koper alleen geëxtrapoléerd over een paar meter ⁵ Naar boven afgerond

Altijd op de hoogte zijn van het laatste nieuws, workshops en reviews?



Scan mij

Meld je aan voor onze gratis wekelijkse nieuwsbrief
Kijk op www.ct.nl/nieuwsbrief



SNELLE NETWERKVERDELERS

Slimme multigigabit-switches

Met multigigabit-ethernet maak je sneller back-ups en kopieer je images van virtuele machines sneller dan met gigabit-ethernet. Maar soms heeft een switch naast brute kracht ook wat hersens nodig. Dergelijke managed switches zijn nu ook betaalbaar met 2,5 Gbit/s.

Ernst Ahlers en Noud van Kruijsbergen

Eenvoudige switches voor 2,5 Gbit/s (2G5) zijn inmiddels te koop voor minder dan 100 euro [1]. Waarom zou je dan honderden euro's uitgeven? Het antwoord bestaat uit verschillende onderdelen: energie, verdeel en heers, en diagnostiek.

We hebben de markt voor managed multigigabit-switches gescand en de belangrijkste kenmerken van dertien typische producten samengevat in de tabel op de laatste pagina. Twijfelachtige aanbiedingen uit online bronnen hebben we daarbij weggelaten omdat het niet zeker is of die over zes maanden nog steeds beschikbaar zullen zijn en of je er ooit firmware-updates voor zult krijgen.

Als je je LAN wilt upgraden, moet je eerst de poortvereisten bepalen: tel alle apparaten die een RJ45-LAN-poort hebben bij elkaar op, met vooral ook de apparaten die al draadloos werken via wifi, maar ook een netwerkpoort hebben. Dat komt omdat elk apparaat dat je verplaatst van wifi naar LAN het draadloze spectrum ontlast, waardoor er meer capaciteit overblijft voor mobiele apparaten. Voeg 20 procent toe aan het totaal voor eventuele uitbreidingen de komende maanden of jaren. Daarmee weet je hoeveel poorten een switch minimaal moet hebben.

Kijk ook naar de ruimtelijke verdeling van de poorten. In de praktijk is het vaak eenvoudiger om groepen te vormen met twee of meer kleinere switches die via een snelle lijn met elkaar verbonden zijn.

Voor de verbinding tussen de switches wordt meestal een glasvezelkabel gebruikt. Dat is energiezuiniger bij 10 Gbit/s en overbrugt grotere afstanden. Bij de 10GBase-SR standaard binnen gebouwen is dat 300 tot 550 meter op multimode-vezels, afhankelijk van het type module.

Bij glasvezelkabels (optische vezels) zijn de connectoren lastig te bevestigen. Bij kleine kantoren en thuisnetwerken is dat echter te vermijden met kant-en-klare glasvezelpatchkabels. Die zijn verkrijgbaar als multimode-versie (OM3 of OM4) in lengtes van één tot enkele honderden meters, ook als gepantserde en dus bijzonder robuuste versie of als aardkabel. Voor lange lengtes betaal je ongeveer een euro per meter dubbeladerige glasvezelkabel. Vier-, acht- en twaalfaderige types zijn overeenkomstig duurder. Het enige lastige is om de kabels door boorgaten te leiden.

DATASNELWEG

Als je drie of meer switches met elkaar verbindt in een ring om de betrouwbaarheid te vergroten, activeer je de functie Rapid Spanning Tree (RSTP). Die herkent en onderbreekt lussen die anders tot broadcast-storms zouden leiden. Als een sectie uitvalt, reactiveert RSTP de reservelink binnen een halve seconde zodat alle switches onmiddellijk opnieuw verbonden zijn.

Als het dataverkeer op de backbone toeneemt, kun je bij apparaten met vier SFP+-slots twee verbindingen samenvoegen (link-aggregation), waardoor

de doorvoer verdubbeld wordt. Dat wordt sterk vergemakkelijkt door een moduleklasse die al enkele jaren wijdverspreid is: 10GBase-BX verzendt 10 Gbit/s via een vezel met verschillende golflengten (kleuren) voor de transmissierichtingen. Met vier van die modules kunnen de twee vezels van de bestaande lijn worden gebruikt voor twee links. Hoewel 10GBase-BX-modules iets duurder zijn dan bij 10GBase-SR, is dat veel goedkoper dan het trekken van nieuwe kabels.

SFP VERSUS SFP+

SFP- en SFP+-modules kunnen uitgewisseld worden tijdens het gebruik (hot-pluggable). De switches herkennen het moduletype aan de hand van een identifieerder die via een I2C-achtige tweedraads bus loopt. Sommige switchfabrikanten gebruiken dat om de werking van producten van derden te blokkeren.

Generieke modules van distributeurs zoals fs.com werken meestal in de meeste switches. Als je het zekere voor het onzekere wilt nemen, koop dan SFP-modules van hetzelfde merk als de switch. Veel switches tonen de module-informatie op hun configuratiepagina. Daar staat dan bijvoorbeeld de fabrikant, het serienummer, type en de bedrijfsparameters (temperatuur, zend- en ontvangsvermogen).

In SFP+-slots voor 10 Gbit/s kunnen meestal ook SFP-modules voor 1 Gbit/s gebruikt worden. Er is echter geen garantie, dat is een kwestie van experimenteren. Als het werkt, kan de switchpoort worden vastgezet op 1 Gbit/s. Een vervangende 10-Gbit/s-module zal dan niet werken, dan moet je de switch opnieuw opstarten of de configuratie handmatig aanpassen.

Omgekeerd moet een SFP+-module in een SFP-slot in principe werken. Maar dat heeft geen zin, want SFP-modules zijn altijd goedkoper dan SFP+-types. Als je een switch met een SFP-slot wilt voorzien van optische modules, gebruik dan SFP-types. Een snelle test van drie SFP+-modules in een oudere switch met een SFP-slot mislukte in ons geval.

Gebruik verder altijd dezelfde moduletypes aan beide zijden van een glasvezelverbinding aangezien er op optisch niveau meestal geen automatische onderhandeling over de verbindingssnelheid is zoals bij koperpoorten (autonegotiation). Een 10GBase-SR-module zal geen verbinding tot stand brengen met een 1000Base-SR-type.

ENERGIE EN DATA

Snelle koperverbindingen vergen meer energie dan licht, maar ze kunnen iets wat met glasvezel niet mogelijk is: energie leveren aan het aangesloten apparaat via Power-over-Ethernet. Dan heb je geen stopcontact in de buurt nodig. Om dat te doen, zet de switch tot 57 volt op de datalijnen en levert tot 2 ampère stroom, in verschillende vermogensklassen voor verschillende gebruikers.

VoIP-telefoons kunnen wel volstaan met de maximale 15 watt van de eerste IEEE standaard 802.3af, die meestal gespecificeerd wordt als PoE. Wifi-basisstations (accesspoints) en bewakingscamera's hebben meestal maximaal 30 watt nodig (IEEE 802.3at,

PoE+), 802.3bt (PoE++) levert tot 90 watt via de kabel. Dat is voldoende voor eenvoudige alles-in-één pc's, zoals betaalterminals.

Volledige belasting op alle poorten is een uitzondering. Elektronica ontwerpen voor zo'n worst-case-scenario is duur. Daarom beperken fabrikanten het totale vermogen tot een lagere waarde, vooral voor switches met veel poorten. Daar moet je rekening mee houden bij het toewijzen van de poorten.

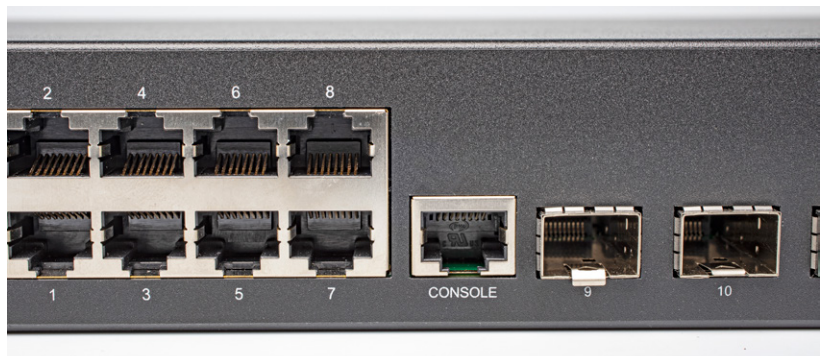
Verschillende instelbare parameters helpen daarbij: de vermogenslimiet specificeert het maximale vermogen van een poort. Die waarde is gebaseerd op de hierboven vermelde vermogensklassen. Vaak kunnen tussenliggende waarden worden geselecteerd of kan de limiet vrij worden ingevoerd.

De PoE-prioriteit wordt gebruikt om aan te geven welke apparaten nog steeds stroom moeten krijgen als het maximale totale vermogen is bereikt (prioriteit hoog) en welke apparaten mogen worden uitgeschakeld (laag). PoE-profielen maken het instellen eenvoudiger als er een groot aantal identieke apparaten op de switch is aangesloten. Dan hoeft je niet meerdere parameters aan te passen, maar kun je een zelf gedefinieerd profiel selecteren.

Bij sommige switches kun je ook een tijdsperiode opgeven waarbinnen de apparaten van stroom moeten worden voorzien. Dat kan helpen om energie te besparen: de switch schakelt gebruikers die 's nachts niet nodig zijn, zoals sommige wifi-basisstations en VoIP-telefoons, dan automatisch uit.

Een PoE-watchdog, ook bekend als PoE Auto Recovery, helpt netwerkapparaten waarvan de firmware af en toe hapert, weer op gang: de switch pingt het apparaat dan. Als dat niet reageert binnen een configureerbare periode, koppelt de watchdog de poort enkele seconden los van de voeding en start het geblokkeerde apparaat opnieuw op.

Als je slechts een paar apparaten via PoE moet voeden, ben je beter af met een handvol injectors, aangezien PoE-switches aanzienlijk duurder zijn. Een injector heeft twee ethernetaansluitingen en een voedingsingang. Hij wordt aangesloten op de switch tussen de poort en het patchpanel waar de muurkabel naar het doelapparaat uitkomt.



Pc's, printers, wifi-basisstations en andere apparaten worden aangesloten op de RJ45-poorten (links) van een switch. De SFP+-slots (rechts) bieden plaats aan optische modules of DAC-kabels. De consolepoort geeft de beheerder toegang via een seriële interface voor het geval er iets verkeerd gaat bij het configureren van VLAN's en hij wordt buitengesloten van het netwerk.

Optische modules voor SFP- en SFP+-slots hebben meestal twee LC-bussen voor de heen- en terugweg via twee glasvezelkernen (links). Bidi-modules hebben slechts één vezel nodig en zenden in beide richtingen via verschillende golflengtes. Een NBase-T-module kan gebruikt worden om achteraf een snelle extra koperpoort toe te voegen en DAC-kabels (rechts) koppelen apparaten in hetzelfde 19-inch rack.



ENERGIE AFTAPPEN

Als het te voeden apparaat PoE niet ondersteunt, kan de stroom met een PoE-splitter uit de ethernetkabel worden gehaald en via de gewone voeding naar het apparaat geleid. Aftappers zijn beschikbaar voor de verschillende vermogensklassen en met een selecteerbare uitgangsspanning. Je moet ze instellen op de ingangsspanning van de verbruiker. Let erop dat er een set adapters voor verschillende laagspannings-pluggen (DC) wordt meegeleverd.

Zeer nieuwe modellen hebben een USB-C-PD 3.0-aansluiting in plaats van een kabeluitgang, die op verzoek van de verbruiker een spanning tussen 5 en 24 volt levert. De LevelOne POS-5001 levert bijvoorbeeld tot 45 watt.

Zorg ervoor dat alle splitters ten minste geschikt zijn voor gigabit-ethernet (1000 Mbit/s). Sommige modellen geven slechts twee van de vier aderen door, waardoor de gegevenssnelheid beperkt blijft tot een slome 100 Mbit/s (0,1 Gbit/s, Fast Ethernet).

ZONES INSTELLEN

Verschillende netwerkzones maken het mogelijk om het dataverkeer van verschillende gebruikersgroepen in het LAN te scheiden [2]. De ethernet-technologie daarvoor heet VLAN (Virtual Local Area Network) – meer daarover in het volgende artikel.

Een switch moet alle 4094 mogelijke identifiers (VLAN Identifier, VID) aankunnen en niet slechts een subset (zoals 0 tot 255). Dat is inmiddels echter standaard, dus het wordt steeds belangrijker hoeveel VLAN's tegelijkertijd actief kunnen zijn. Helaas geeft niet elke fabrikant een concreet aantal op.

Voor thuishandlers of in een klein bedrijf is een handvol VLAN's voldoende. De 24 of 64 die gebruikelijk zijn in switches voor kleine LAN's zijn te weinig voor een groter bedrijf, dan kan het aantal VLAN's al snel richting de 100 gaan. In dergelijke omgevingen zijn functies zoals automatische VLAN-configuratie via GVRP of automatische toewijzing van VoIP-telefoons aan een geprioriteerd Voice-VLAN ook nuttig.

Netwerkzones met VLAN's zijn al lang niet meer alleen voor bedrijfsnetwerken. Draytek was een van de eerste routerfabrikanten die VLAN's toegankelijk maakte voor kleinschalige netwerken. Andere aanbieders zoals Synology hebben zich daarbij aangesloten [3], en ook het gratis routerbesturingssysteem OpenWrt ondersteunt VLAN's [4].

Betere switches zijn in staat om te cascaderen en kunnen vrijwel het hele bedrijfsnetwerk met zijn x-aantal netwerkzones in een bovenliggend VLAN (QinQ) verpakken. Daardoor kan het bedrijfsverkeer in een netwerk tussen meerdere locaties getransporteerd worden of kunnen verschillende bedrijven die op dezelfde locaties actief zijn een lijn delen.

Managed switches voor multigigabit-ethernet

Fabrikant	Cisco	D-Link	Draytek	EnGenius
Model	CBS350-8MP-2X	DMS-1100-10TP	PQ2200xb	ECS2512
Hardware-uitrusting				
Koperpoorten	8 × 2G5, 2 × 10G	8 × 2G5	16 × 2G5	8 × 2G5
SFP+-Slots / Shared	2 / ✓	2 / –	4 / –	4 / –
Power-over-Ethernet / max. vermogen	4 × 60 W, 4 × 30 W / 240 W	8 × 30 W / 240 W	4 × 90 W, 12 × 30 W / 400 W	– / –
Stacking-poorten	✓ (via SFP+)	–	–	–
Management-poorten	serieel (RJ45), USB	–	serieel (RJ45)	serieel (RJ45)
Ventilatorloos	–	–	–	n.b.
Switching-functies				
Beheer via CLI / browser	✓ / ✓	– / ✓	✓ / ✓	✓ / ✓
Veilige kanalen / ook via IPv6	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
RSTP / MSTP	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Link-aggregatie / LACP	✓ / ✓	✓ / ✓	✓ / ✓	✓ / –
VLAN's / gelijktijdig actief	✓ / 4094	✓ / 4094	✓ / 24	✓ / n.b.
GVRP / voice-VLAN / QinQ	✓ / ✓ / ✓	– / ✓ / –	✓ / ✓ / ✓	– / ✓ / –
QoS: 802.1p / DSCP	✓ / ✓	✓ / n.b.	✓ / ✓	✓ / ✓
IGMPv3- / MLD-snooping	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Remote Syslog / SNMP	✓ / ✓	n.b. / ✓	✓ / ✓	✓ / ✓
LLDP / CDP	✓ / ✓	✓ / –	✓ / –	– / –
802.1X-authenticator / supplicant	✓ / ✓	– / –	✓ / –	✓ / –
Poort- / remote-mirroring	✓ / ✓	✓ / –	✓ / –	– / –
Prijs (mei 2024)	€ 1430	€ 804	€ 724	€ 660
✓ aanwezig – niet aanwezig n.b. niet bekend				

MIRROR, MIRROR

Als je het dataverkeer van hosts moet opnemen en analyseren voor het oplossen van problemen in het LAN, gebruik je software zoals Wireshark. Dat wordt echter lastig als de tool niet geïnstalleerd kan worden op de host in kwestie of als de aanwezigheid ervan het gedrag zou beïnvloeden. Sommige beheerders plaatsen dan een tap tussen de switch en de host om het dataverkeer daarnaar om te leiden en in te kunnen zien.

Bij switches die in staat zijn tot port-mirroring is er geen extra hardware nodig. Die functie kan het dataverkeer dat via één of meerdere poorten loopt spiegelen naar een andere verbinding. Er kan informatie verloren gaan als de te bewaken poort of poorten moeten worden begrensd tot 1 Gbit/s.

Dat komt omdat een 1GE-poort in beide richtingen samen tot 2 Gbit/s kan transporteren, wat zonder verlies moet worden geregistreerd. Als je 2G5-ethernet volledig wilt analyseren, dan is een vrij SFP+-slot handig waarop je de recorder-pc aansluit.

De betere apparaten ondersteunen ook remote-mirroring. Ze registreren de data op de betreffende poort en sturen de gegevens via de backbone naar een andere switch, waar ze verder doorgestuurd worden.

BEHUIZING

De meeste snelle switches hebben een ventilator, en bij modellen met PoE draait die soms op hoge snelheid – en dat zelfs zonder belasting. Dergelijke apparaten moeten niet in de buurt van werkplekken worden gezet, maar worden afgezonderd in een technische ruimte. Zonder PoE draaien de ventilatoren in

het algemeen veel stiller, maar in een stil kantoor nog steeds hinderlijk.

Switches bevinden zich idealiter in een schakelkast met een 19-inch rack en afsluitbare deur. Dat is niet meteen omdat je bang moet zijn voor vandalisme of datadiefstal, maar als iemand per ongeluk blijft haken achter een backbonekabel en die uit de poort trekt, kan een hele werkgroep plotseling worden losgekoppeld van het netwerk.

Een kleine 19-inch kast in een kantoor dempt ook het geluid van de switches enigszins, waardoor het een goed compromis is als er geen aparte serverruimte ingericht kan worden.

Net als je wifirouter werkt een switch de klok rond en heeft hij energie nodig. Voor de modellen in de tabel zonder PoE moet je rekenen op een idle energieverbruik van 5 tot 15 watt – afhankelijk van het aantal bezette poorten en de onderhandelde datasnelheid. Tel daar een halve watt tot een hele watt per optische module bij op.

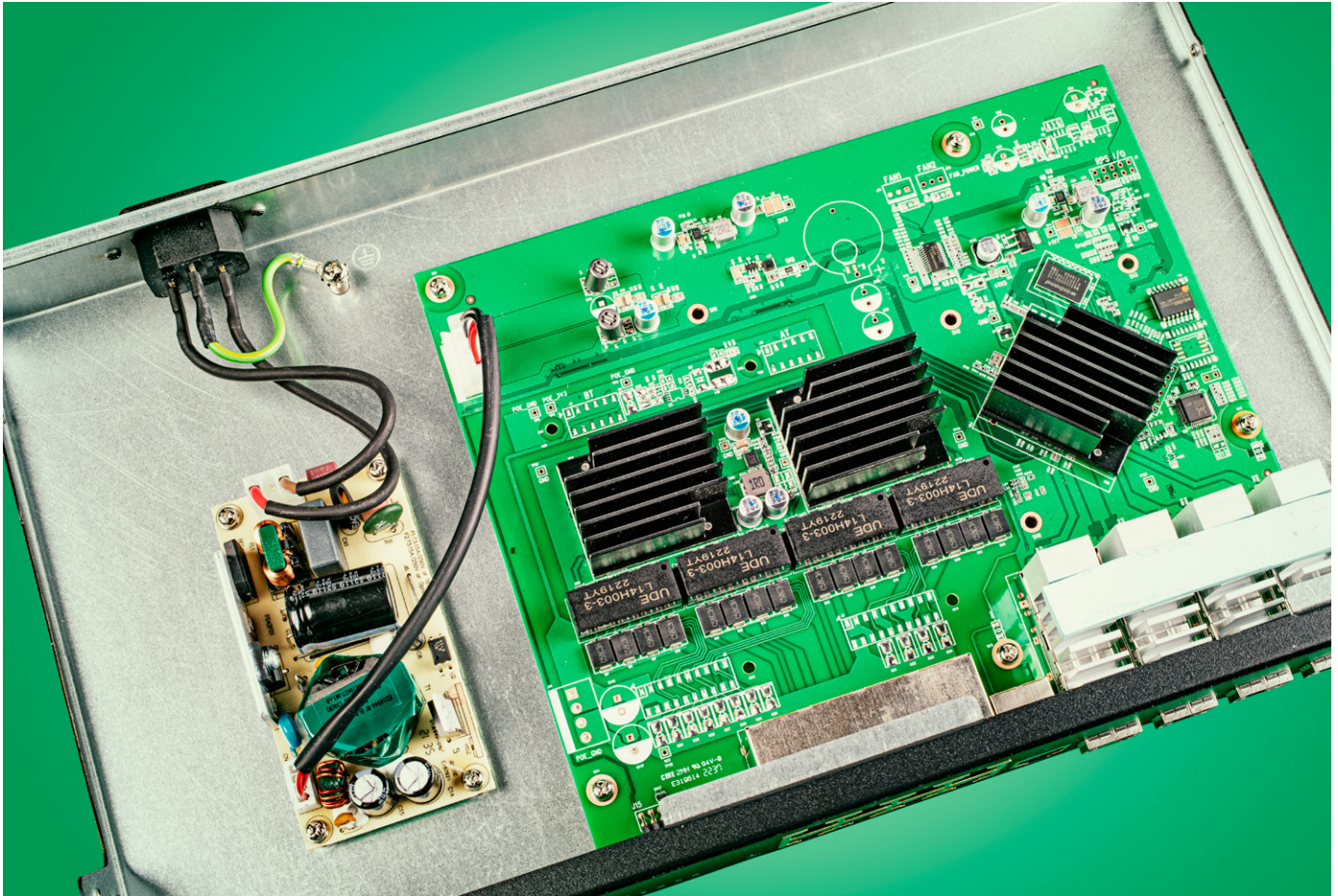
Bij PoE-switches is de basisbelasting iets hoger en sterk afhankelijk van het type en het aantal aangesloten verbruikers dat op de switch aangesloten is. Als de fabrikanten bij de specificaties al waarden opgeven, dan is dat meestal het slechtste geval (alle poorten bezet en maximaal gebruikt) en dus zeker te hoog voor jouw toepassing.



Literatuur

- [1] Ernst Ahlers en Marco den Teuling, Snelle ethernetswitches om kleine netwerken te upgraden, c't 1-2/2024, p.100
- [2] Ernst Ahlers en Jan Mulder, Veilig achter het hekwerk, c't 6/2017, p.110
- [3] Ernst Ahlers en Noud van Kruijsbergen, Synology RT6600ax, c't 7/2022, p.23
- [4] Ernst Ahlers en Noud van Kruijsbergen, OpenWrt instellen als router voor meerdere netwerkzones, c't 6/2019, p.138

Lancom Systems	Mikrotik	Netgear	QNAP	TP-Link	Trendnet	Ubiquiti	Zyxel
GS-3528XP	CRS310-8G+2S+IN	MS108EUP	QSW-M2108-2C	SG3210X-M2	TPE-3102WS	USW-Enterprise-8-PoE	XS1930-10
12 × 2G5, 12 × 1G	8 × 2G5	8 × 2G5	8 × 2G5, 2 × 10G	8 × 2G5	8 × 2G5	8 × 2G5	8 × 10G
4 / –	2 / –	– / –	2 / ✓	2 / –	2 / –	2 / –	2 / –
24 × 30 W / 370 W	– / –	4 × 60 W, 4 × 30 W / 240 W	– / –	– / –	8 × 30 W / 240 W	8 × 30 W / 120 W	– / –
–	–	–	–	–	–	–	–
serieel (RJ45)	USB	–	serieel (RJ45)	serieel (RJ45), USB	serieel (RJ45)	–	–
–	–	✓	–	✓	–	–	–
✓ / ✓	✓ / ✓	– / ✓	– / ✓	✓ / ✓	✓ / ✓	(Unifi-controller)	✓ / ✓
✓ / ✓	✓ / ✓	✓ / –	– / –	✓ / ✓	✓ / ✓	(Unifi-controller)	✓ / ✓
✓ / ✓	✓ / ✓	– / –	✓ / –	✓ / ✓	✓ / ✓	✓ / n.b.	✓ / ✓
✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
✓ / 4094	✓ / 4094	✓ / 64	✓ / n.b.	✓ / 4094	✓ / 256	✓ / n.b.	✓ / 4094
✓ / ✓ / ✓	– / – / ✓	– / ✓ / –	– / – / –	✓ / ✓ / ✓	✓ / ✓ / –	– / ✓ / –	✓ / ✓ / ✓
✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	n.b. / n.b.	✓ / ✓
✓ / ✓	✓ / ✓	✓ / –	– / –	✓ / ✓	✓ / ✓	✓ / n.b.	✓ / ✓
n.b. / ✓	✓ / ✓	– / –	– / –	✓ / ✓	✓ / ✓	(Unifi-controller)	✓ / ✓
✓ / –	✓ / –	– / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
✓ / –	✓ / ✓	– / –	– / –	✓ / –	✓ / –	✓ / –	✓ / –
✓ / –	✓ / –	✓ / –	– / –	✓ / –	✓ / –	✓ / –	✓ / –
€ 1260	€ 205	€ 320	€ 470	€ 235	€ 460	€ 495	€ 510



WAT IEDERE BEHEERDER MOET WETEN

Functies van netwerkswiches

In dit artikel leggen we de achtergronden en functies van netwerkswiches uitgebreid uit, zodat je daarna genoeg basiskennis hebt om als beheerder aan de slag te kunnen.

Benjamin Pfister en Noud van Kruysbergen



Of het nu gaat om kleine, grote of zeer grote netwerken, switches vormen altijd de basis voor de digitale processen en services die erin draaien door te bemiddelen in de communicatie tussen de verschillende netwerkapparaten. Dat geldt ook voor een thuisnetwerk, hoewel switches daar vaak een onopvallende rol in een router spelen.

Zodra een netwerk dan echter meer dan vier ethernetapparaten moet verbinden, moet je een externe switch toevoegen, die dan bijvoorbeeld je smarthome-apparaten met je router verbindt.

De eenvoudigste manier om dat te doen is met unmanaged switches. Die voorzie je van stroom, je sluit de ethernetkabels aan die naar de netwerkapparaten leiden en vervolgens kun je de netwerkcommunicatie (switching) jarenlang zorgeloos overlaten aan het automatische systeem van het apparaat.

De duurdere configureerbare switches oftewel managed switches hebben echter veel nuttige func-

ties, waarvan je eerst moet weten wat ze doen. Daarom noemen we hier de belangrijkste hardware- en softwarefuncties van managed switches.

FRAMES

Netwerken verzenden de gebruiksgegevens in frames die het bron- en bestemmingsadres (Media Access Control Address, ook bekend als het hardware-adres) in de header bevatten. Dat is de basis voor de switch-functie. Op basis van het bronadres leert de switch via welke poort hij welk apparaat in het netwerk kan bereiken als hij daar een frame heen moet sturen. De switch koppelt de adressen in een tabel aan poorten. En zoals verderop beschreven, kan hij daarbij ook rekening houden met VLAN-identifiers (tags of ID's) van virtuele netwerken om de bestemming te bepalen.

Volgens de IEEE-standaard 802.3 zijn standaard ethernetframes tussen 64 en 1518 bytes lang, afhankelijk van de gebruiksgegevens die verzonden moeten worden. Bij VLAN's is dat 68 tot 1522 bytes.

Jumboframes transporteren tot 12.000 bytes. Omdat het aandeel gebruiksgegevens per ethernetframe daardoor toeneemt ten opzichte van het aandeel overheadinformatie, neemt ook de maximale doorvoersnelheid toe – we kwamen tot een toename van 9400 naar 9900 Mbps. Jumboframes zijn echter

niet gestandaardiseerd, dus is het onzeker of communicatie in verschillende netwerken daarmee zal werken.

SWITCHING

Er zijn twee switching-varianten, Store and Forward en Cut Through. Bij Store and Forward ontvangt de switch het hele frame en controleert de checksum. Als het berekende resultaat overeenkomt met die in het frame, zoekt het naar het bestemmingsadres en de uitgaande poort en stuurt het frame daarheen door – zo niet, dan wordt het frame zonder commentaar weggegooid.

Bij Cut Through-switching begint het doorstuurproces zodra de switch het doeladres in het frame identificeert. De rest vindt plaats zoals bij Store and Forward. In het algemeen is Store and Forward langzamer door een hogere latentie omdat een frame eerst op juistheid wordt gecontroleerd voordat het doorgestuurd wordt. Cut Through is normaal gesproken sneller omdat er geen foutcontrole plaatsvindt. Het risico op foutverspreiding is echter groter dan bij Store and Forward, omdat foutieve frames ongezien doorgestuurd worden.

Afhankelijk van het type communicatie wordt een pakket naar slechts één bestemming gestuurd (unicast), naar meerdere deelnemers in een subnet (multicast) of naar alle abonnees (broadcast). Multicasts en broadcasts gaan naar alle poorten van een subnet, behalve naar waar het frame vandaan kwam. Hetzelfde gebeurt bij Unknown Unicast Floodings als de switch in zijn tabel geen MAC-adres van een bestemming kan vinden.

Multicasts zijn groepen binnen een netwerk, zoals alle deelnemers die lokale apparaatnamen omzetten naar ip-adressen via mDNS (IPv6-adres ff02::fb, IPv4-adres 224.0.0.251, elk via UDP-poort 5353). De switch koppelt IPv4-broadcasts via ethernet-broadcast aan het MAC-adres FF:FF:FF:FF:FF:FF.

IPv4-broadcasts zijn bijvoorbeeld nodig voor dynamische IP-adrestoewijzing via het Dynamic Host Configuration Protocol of voor het Address Resolution Protocol om IPv4-adressen om te zetten naar MAC-adressen. Aangezien broadcasts worden uitgegeven op alle poorten van een switch behalve de inkomende poort, vertragen ze het andere verkeer enigszins. Dat throttling-effect neemt toe bij grote netwerken waar meerdere switches automatisch een gemeenschappelijk broadcastdomein vormen.

ARCHITECTUUR

Managed ethernetswitches bestaan uit verschillende elementen. Aan de buitenkant zitten de interfaces (poorten) voor de ethernetkabels. Er zijn verschillende poorten, afhankelijk van het type switch. Ze zijn alleen ontworpen voor koperkabels of kunnen worden opgewaardeerd voor gebruik met glasvezelkabels met behulp van insteekbare optische modules.

Koperpoorten worden veel gebruikt in reguliere thuisnetwerken en bedrijfsnetwerken als Registered Jack 45, oftewel RJ45-aansluitingen. In industriële

omgevingen worden M8- en M12-aansluitingen gebruikt ter bescherming tegen stof en vocht in ruwe omgevingen.

De huidige kantoorswitches bieden via de acht-pins RJ45-aansluiting 10 Mbit/s tot 10 Gbit/s met kabellengtes tot 100 meter (per segment). Als een segment twee switches verbindt, is dat een cascade. Omdat elke switch een inkomend signaal vernieuwt voordat het wordt doorgestuurd, kunnen meerdere segmenten met elkaar worden verbonden met behulp van cascades.

Glasvezelverbindingen zijn echter praktischer: afhankelijk van het systeem kunnen ze 80 kilometer overbruggen en omdat er zich bij glasvezel geen elektrische potentialen opbouwen, kunnen problemen worden vermeden bij het verbinden van gebouwen met verschillende stroomvoorzieningen.

Tegenwoordig zijn unmanaged gigabit-switches redelijk populair en al te koop voor een paar tientjes. Afhankelijk van het netwerk communiceren ze automatisch met 10, 100 of 1000 Mbit/s.

In de herfst van 2023 daalde de prijs van switches die 2,5 Gbit/s (2G5) aankunnen voor het eerst onder de 100 euro. Ze behoren tot de nog jonge klasse van multigigabit-switches die met 2,5, 5 en 10 Gbit/s werken (afgekort tot 2G5, 5G en 10G).

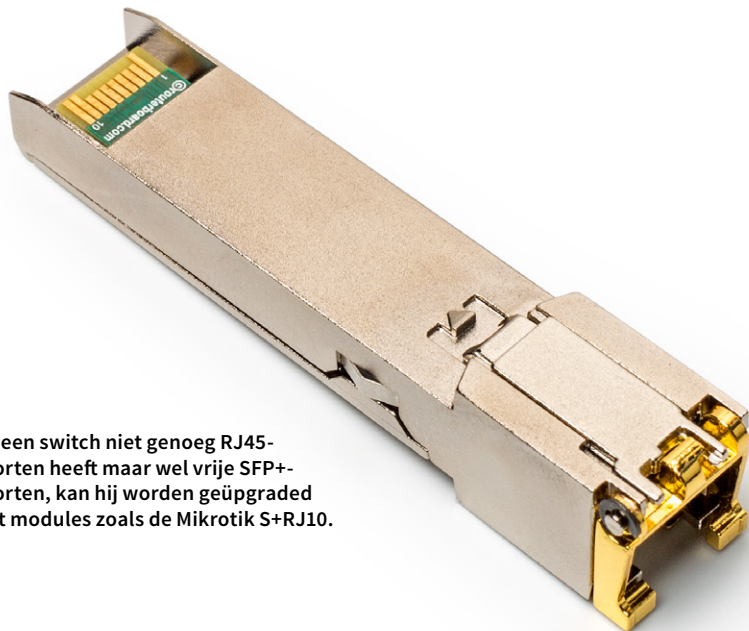
Alle drie de klassen kunnen de tussenniveaus aan met standaard CAT5e-kabels, waardoor er geen nieuwe installaties nodig zijn. Boven 5G loopt de maximale segmentlengte van dergelijke kabels terug tot ongeveer 50 meter. Dus als je bij 10 Gbit/s tot 100 meter moet overbruggen, heb je kabels van hogere kwaliteit nodig (CAT6a, CAT7).

Multigigabit-switches zijn niet alleen handig omdat je daar een snellere verbinding met daarvoor geschikte NAS-apparaten mee kunt opzetten dan via gigabit-kabels, maar ook omdat de ethernetapparaten dan op gelijke snelheid blijven met de wifi-accesspoints, die momenteel al meer dan 1 Gbit/s leveren (Wi-Fi 6 en Wi-Fi 7).

Wanneer twee ethernetapparaten contact maken, onderhandelen ze automatisch over de hoogste



Gigabit-switches waren lange tijd de norm bij kleine en middelgrote netwerken. Sinds het najaar van 2023 is de prijs van multigigabit-switches echter gedaald tot onder de 100 euro, wat betekent dat apparaten met 2,5 Gbit/s geleidelijk aan gebruikelijker worden.



Als een switch niet genoeg RJ45-poorten heeft maar wel vrije SFP+-poorten, kan hij worden geüpgraded met modules zoals de Mikrotik S+RJ10.

gemeenschappelijke gegevensnelheid en andere verbindingseigenschappen. Bij managed switches kunnen sommige poortparameters geconfigureerd worden: auto-negotiation voor het automatisch onderhanden van de snelheid, flow-control en de bedrading van aansluiting (doorlopende of gekruiste lijnen, Medium Dependent Interface: MDI of MDIX).

Leuk weetje: tot 100 Mbit/s kan de toewijzing van de communicatierichtingen ook worden geconfigureerd (half-duplex: afwisselend zenden en ontvangen of full-duplex: gelijktijdig zenden en ontvangen). Vanaf 1 Gbit/s werken de switches altijd in full-duplex-modus.

De handmatige poortinstellingen zijn over het algemeen nuttiger als de automatische instellingen onjuist zijn, bijvoorbeeld als de snelheidsonderhandeling of het automatisch herkennen van de pin-toewijzing mislukt.

MODULAIRE POORTEN

Hoe hoger de vereisten voor doorvoer en bereik, des te waarschijnlijker het is dat glasvezelkabels gebruikt worden. Dat is bijvoorbeeld het geval bij verbindingen van switch naar switch (uplink) of voor servers die gegevens snel moeten transporteren. Om redenen van flexibiliteit worden daar modulaire slots voor gebruikt.

Onder de modulaire poorten zijn Small Form-Factor Pluggables (SFP) gebruikelijk in verschillende vormen. Koperen modules met RJ45-aansluitingen worden gebruikt om standaard netwerkapparaten aan te sluiten.

Bij klassieke glasvezelverbindingen is er keuze tussen transceivers voor verschillende golflengten, zoals voor 850, 1310 of 1550 nanometer in varianten voor multimode of singlemode vezels. De bandbreedtes gaan momenteel tot 800 Gbit/s.

De varianten Enhanced Small-Form Pluggable Ports (SFP+) en SFP28 zijn ontworpen voor 10G-ethernet en 25G. Met Quad Small Form Factor Pluggables, QSFP en QSFP+, gaat er maximaal 40 gigabit door de lijn, bij QSFP28 is dat maximaal 100G via vier optische kanalen. QSFP-DD voor 800G is momenteel het maximum.

STACKPOORTEN

Sommige switchmodellen hebben fabrikantspecifieke poorten aan de achterkant. Daarmee kunnen twee of meer switches gecombineerd worden – het aantal varieert afhankelijk van het model. De Cisco Catalyst 9300X, die vaak in bedrijfsomgevingen gebruikt wordt, kan worden gecombineerd tot een groep van acht switches voor redundantiedoelinden en levert tot 1 Tbit/s.

De apparaten die op zo'n manier gekoppeld zijn in stacks gedragen zich als één logische switch. Een daarvan wordt de actieve master voor het beheer (Management Plane) en de besturingsinformatie (Control Plane). Dat betekent dat je niet in elke switch van een stack iedere parameter afzonderlijk moet aanpassen, maar dat bij de master kunt doen voor alle poorten van de hele structuur.

De andere switches zijn passief wat betreft het beheer. Je kunt als beheerder de master bepalen door daar een hoge prioriteit aan toe te kennen. Als een switch met een hogere prioriteit wordt toegevoegd, wordt die de nieuwe master zodra de vorige opnieuw opstart. Als er geen waarde ingesteld is, wordt de switch met de kortste opstarttijd de master. Als twee of meer switches even snel zijn, wordt degene waarvan de netwerkpoort die gebruikt wordt voor het koppelen de laagste numerieke waarde (MAC-adres) heeft de master. Als de master uitvalt, neemt een van de passieve leden de masterrol over.

INTERNE SWITCHARCHITECTUUR

Er zijn verschillende andere componenten die de werking en prestaties beïnvloeden. Bij switches die uitgebreid kunnen worden met een insteekkaart of -module, verbindt de backplane de systeemcomponenten als een logische bus. Dat kan passief of actief zijn. Actieve backplanes bestaan uit elektronische modules en besturingselementen, terwijl passieve backplanes alleen bestaan uit een printplaat met connectoren. De doorvoer van de backplane moet overeenkomen met de maximale bidirectionele gegevensnelheid van alle poorten (Line-Rate Forwarding of ook Non-Blocking architectuur genoemd).

De Forwarding Controller stuurt inkomende gegevenspakketten door naar hun bestemming. De controller bepaalt de route voornamelijk op basis van het MAC-adres van de bestemming. Afhankelijk van de uitrusting en configuratie kan een switch ook rekening houden met het lidmaatschap van een virtueel LAN (VLAN) en de richtlijnen van zijn pakketfilter of, in routermodus, de Layer 3-architectuur van het netwerk – in dat geval vindt hij de bestemming op basis van het ip-adres.

Controllers transporteren inkomend en uitgaand verkeer in combinatie met een scheduler en een buffer die het verkeer buffert. De buffer varieert in grootte afhankelijk van het type switch en de switch gebruikt die om pakketten tijdelijk op te slaan in een wachtrij in geval van overbelasting. Van daaruit vindt het doorsturen naar de Forwarding Controller plaats volgens de scheduler-richtlijnen, zodat bijvoorbeeld

pakketten van tijdkritische diensten voorrang krijgen boven andere pakketten (Quality of Service, QoS, zie hieronder).

Achter de Forwarding Controller bevindt zich meestal een Rewrite Engine die de inhoud van de datapakketten (frames) herschrijft, bijvoorbeeld door het bestemmings-MAC-adres van de volgende hop in te voeren als de bestemming buiten het lokale netwerk ligt. Die functies werden geïmplementeerd als onveranderlijke Application Specific Integrated Circuits (ASIC), maar steeds meer fabrikanten doen dat nu als Field Programmable Gate Arrays (FPGA), wat firmware-updates mogelijk maakt.

De cpu van een switch ontvangt alle pakketten die de hardware niet zelf verwerkt. Oftewel: de cpu implementeert alle processen en protocollen die draaien op de Control en Management Layer, zoals spanning-tree, routing, lijnbundeling volgens het Link Aggregation Control Protocol (LACP), en command-line-sessies via Secure Shell (SSH) en dergelijke.

Om de apparaten te beheren, worden ze geleverd met een managementcontroller, die meestal verbonden is met een lokale consolepoort. Oudere switches hebben daar seriële poorten voor, nieuwere doen dat met usb-poorten. De cpu gebruikt de managementcontroller om Telnet, SSH, HTTP/S en SNMP-sessies af te handelen – verkeer dat voor de cpu zelf bedoeld is. Omdat SNMP en Telnet tot versie 3 niet-versleutelde toegangsgegevens verzenden, zijn die protocolversies normaal gesproken uitgeschakeld – en dat moet zo blijven.

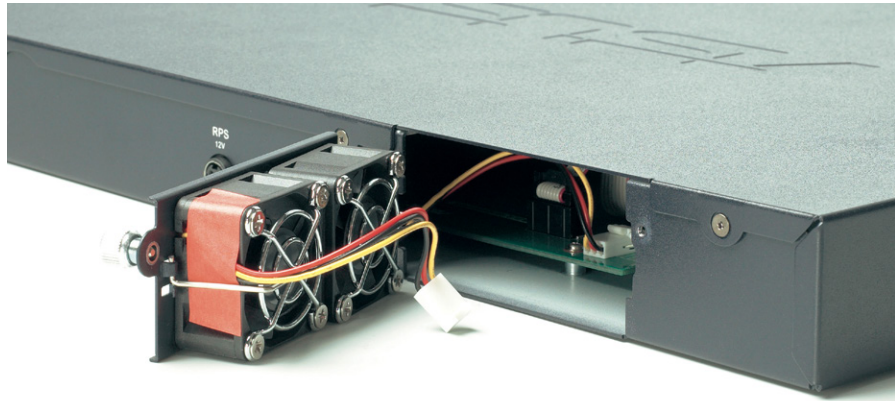
De basis van alle elektronische werking is ook bij switches de voeding. Er zijn drie verschillende soorten voedingseenheden: extern, intern vast of intern maar vervangbaar. Interne, vervangbare voedingsseenheden kunnen meestal tijdens bedrijf worden verwisseld (hot-swappable), op voorwaarde dat een tweede voedingseenheid ervoor zorgt dat er stroom beschikbaar blijft.

Het vermogen varieert afhankelijk van het type switch, het aantal poorten en extra vermogen voor het voeden van ethernetapparaten met Power-over-Ethernet (PoE). Switches vanaf zo'n 24 poorten of meer en vooral die met PoE-voeding, worden actief gekoeld door ventilatoren. Die ventilatoren kunnen ook vast geïnstalleerd of vervangbaar zijn, en sommige zijn hot-swappable.

VLAN

VLAN's (Virtual Local Area Networks) kunnen worden gebruikt om een fysiek netwerk op te delen in logische netwerken. Dat kun je gebruiken om organisatorische eenheden of beveiligingszones van elkaar te scheiden. Je kunt het ook gebruiken om lokale apparaten of bepaalde apparaatgroepen in onder te brengen. Een thuisnetwerk kun je bijvoorbeeld onderverdelen in drie VLAN's: één voor de pc's, een voor gasten en een voor alleen IoT-apparaten zoals smart-tv's.

In het eenvoudigste geval wordt een VLAN toegewezen aan een switchpoort. Poorten met een vaste VLAN-toewijzing worden access-poorten genoemd.



Bij sommige switches kunnen de ventilatoren worden vervangen zonder ze uit het rack te hoeven halen. Sommige modellen zijn zelfs voorzien van redundante, vervangbare ventilatoren, die je kunt vervangen zonder de switch uit te schakelen.

In sommige gevallen moeten frames van meerdere VLAN's via één poort verzonden worden, bijvoorbeeld tussen twee switches. Daar werden propriëtaire procedures zoals Interswitch Link (ISL) voor gebruikt, maar tegenwoordig zijn trunk-poorten overeenkomstig de IEEE 802.1Q-standaard gebruikelijk.

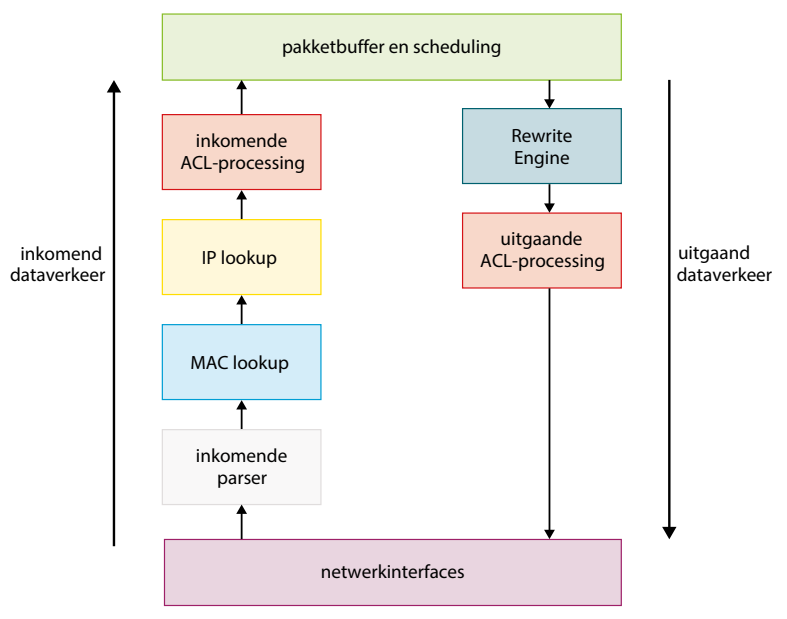
VLAN's zijn genummerd van 1 tot 4094 (VLAN-ID). Sommige goedkope managed switches kunnen slechts 64 of 256 VLAN's tegelijk aan. Systemen voor netwerktoegangsbeheer wijzen VLAN-ID's dynamisch toe op basis van eindapparaateigenschappen.

Aan een VLAN mag slechts één IPv4- en één IPv6-subnet worden toegewezen en alle hosts in een VLAN moeten ip-adressen uit die adresruimten krijgen.

Apparaten die in verschillende VLAN's zitten kunnen alleen indirect met elkaar communiceren via een

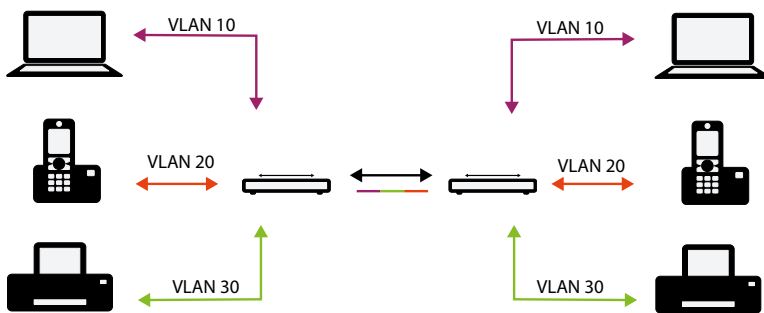
Frame doorsturen in de switch

Controllers transporteren het inkomend en uitgaand verkeer in combinatie met een scheduler en een buffer die het verkeer buffert. Daardoor kan de switch frames bij een overbelasting tijdelijk opslaan in een wachtrij.



Voorbeeld van een VLAN-indeling

Een fysiek netwerk kan worden opgedeeld in verschillende virtuele netwerken (VLAN) met behulp van VLAN-technologie. Dat kun je gebruiken om beveiligingszones te creëren tussen apparaten van verschillende betrouwbaarheid.



inter-VLAN-router of Layer 3-switch. Daar zijn routingsfuncties op basis van VLAN-interfaces (Switched Virtual Interfaces, SVI) voor nodig.

PRIORITERING

Met Quality of Service (QoS) kunnen frames met voorrang of langzamer worden doorgestuurd, afhankelijk van de servicekenmerken. Om dat te doen, classificeert een switch inkomende frames, markeert ze en sorteert ze in wachtrijen met verschillende transmissieprioriteiten alvorens ze te verzenden. Op die manier kan een switch frames van tijdkritische diensten zoals telefonie en videoconferencing hoger prioriteren en bij voorkeur verzenden om de latentie (looptijd), latentiefleuctuaties (jitter) en het frameverlies te minimaliseren en zo de kwaliteit van dergelijke diensten zo hoog mogelijk te houden.

Frames die niet tijdkritisch zijn, zoals e-mails, komen in wachtrijen met een lagere prioriteit terecht en wachten even tot de dringende frames verzonden zijn. De QoS-markeringen kunnen gebruikt worden door alle tussenstations op de weg naar de bestemming om inkomende frames op dezelfde manier te behandelen. Netwerkkapparaten zoals ip-telefoons en pc's kunnen ook frames markeren – op Layer 2 of 3.

Een markering op Layer 2 gebeurt in overeenstemming met de IEEE 802.1Q-standaard. Apparaten voeren de prioriteiten (ToS/Type of Service) bij ethernetframes in, in overeenstemming met IEEE 802.1p. Markering op ip-niveau (Layer 3) in overeenstemming met Differentiated Services Codepoint (DSCP) is nu gebruikelijk. Daar zijn zes bits in de ip-header voor gereserveerd. Om bijvoorbeeld VoIP-pakketten met voorrang te verzenden, worden ze gemarkeerd met de decimale waarde 46 (Expedited Forwarding, EF).

Sommige switches kunnen VoIP-telefoons identificeren op basis van hun MAC-adres of met behulp van het Link Layer Discovery-protocol. Ze stoppen ze dan automatisch in het voorbereide voice-VLAN en markeren hun frames met een hoog ToS-niveau. Om dat te doen, veranderen ze de 6-bit DSCP automatisch naar een 3-bit ToS met behulp van een vooraf gedefinieerde tabel.

POWER OVER ETHERNET

IP-telefoons, webcams en accesspoints zijn typische apparaten die op wat verder weg van de gebouwinfrastructuur gebruikt worden. Om op installatiekosten te besparen, is het daarom wenselijk die via een enkele kabel in het netwerk op te nemen en ook van stroom te voorzien. Jaren geleden ontwikkelden sommige bedrijven eigen methoden om dat via ethernetkabels te doen (Power-over-Ethernet, PoE).

Tegenwoordig zijn er echter PoE-technologieën die gebaseerd zijn op IEEE-specificaties. De kleine Raspberry Pi kan daardoor ook via PoE gevoed worden. Managed switches hebben daar stroomcontrolefuncties voor en kunnen PoE-apparaten daarom ook automatisch opnieuw opstarten. Zo kunnen bewakingscamera's worden uitgeschakeld wanneer bewoners het huis binnenkomen en ingeschakeld wanneer ze het huis verlaten. Hoewel sommige unmanaged switches ook PoE-hardware hebben, hebben ze geen stroomcontrolefuncties.

Een switch levert volgens IEEE 802.3af tot 15,4 watt per poort, maximaal 30 watt volgens 802.3at en 802.3bt levert zelfs tot 90 watt per poort. Omdat niet elk eindapparaat het volledige vermogen nodig heeft, zijn ze ingedeeld in vermogensklassen.

MANAGEMENT

Managed switches kunnen via verschillende interfaces beheerd worden, zoals Zero Touch Provisioning. Eenvoudige modellen zijn alleen toegankelijk via hun webinterface. Vooral beginners in het netwerkbeheer geven waarschijnlijk de voorkeur aan een browser omdat dat makkelijker is om het overzicht te houden. Webverkeer moet in het algemeen versleuteld zijn met TLS, zodat aanvallers de inloggegevens niet te makkelijk kunnen achterhalen. De betere apparaten hebben niet alleen lokale accounts voor beheerderstoegang, maar kunnen accounts ook verbinden met een centraal beheer (AD, LDAP) met behulp van de protocollen Radius of TACACS+.

Sommige fabrikanten publiceren API's (Application Programming Interfaces) voor grotere modellen. Daarmee kunnen beheerders wijzigingen of query's automatiseren, wat tijd kan besparen bij het beheer van een groot aantal switches. Beheer via API loont echter niet altijd omdat je tijd moet investeren in query-scripts. Daarom gebruiken veel beheerders liever een commandline-interface. Die heb je in ieder geval ook nodig voor de initiële configuratie, die meestal wordt uitgevoerd via een lokale console met een seriële RS-232-kabel.

Eenmaal ingesteld, verloopt het beheer meestal via versleutelde SSH-sessies. Ervaren beheerders werken daar vaak sneller mee dan wanneer ze de webinterface gebruiken en met behulp van scripts zijn automatiseringen mogelijk. Daarvoor moet je de structuur en de commando's van de switches kennen. Veel switches kunnen ook automatisch worden beheerd met eenvoudige Ansible-modules.

Om switches van meer dan één fabrikant op dezelfde manier te beheren, kun je het fabrikant-

onafhankelijke Simple Network Monitoring Protocol (SNMP) gebruiken. Hou er wel rekening mee dat SNMP het dataverkeer en ook de vertrouwelijke inloggegevens pas vanaf versie 3 versleutelt.

Gegevens kunnen via SNMP afhankelijk van automatisatie zowel gelezen als geschreven worden. De gegevens zijn onderverdeeld in elementen en hiërarchisch georganiseerd (Management Information Bases, MIB's). De switch gebruikt SNMP-traps om informatie naar een ontvanger van de trap te sturen in het geval van bepaalde gebeurtenissen, zoals een Link Down Event. Switches kunnen dergelijke statusberichten of waarschuwingen ook naar een syslog-server sturen, zodat je bijvoorbeeld beveiligingsincidenten kunt analyseren.

De laatste jaren bieden fabrikanten steeds meer beheerfuncties aan vanuit de cloud, die worden weergegeven via een webinterface. Die switches hebben daarom een internetverbinding nodig naar de cloudprovider. Bij cloud-based switches zoals die van Cisco Meraki en Juniper Mist loopt alleen het beheer via de cloud en blijven de gebruiksgegevens lokaal.

Cloud-based beheer kan dankzij de gecentraliseerde aanpak tijd en moeite besparen, bijvoorbeeld bij het beheren van een netwerk dat uit meerdere vestigingen bestaat. Het kan echter ook extra inspanning vergen omdat je er als beheerder voor moet zorgen dat persoonlijke metadata worden overgedragen, opgeslagen en behandeld in overeenstemming met de AVG. De kosten die switchfabrikanten in rekening brengen voor de clouddienst zijn ook een nadeel. En in het geval van hoge beschikbaarheidseisen moet je voorzorgsmaatregelen nemen om een switch te kunnen beheren, zelfs als de internetverbinding uitvalt, bijvoorbeeld door gebruik te maken van vervangende lijnen via mobiele communicatie of door het te kunnen delegeren aan lokale gebruikers.

OPTIMALISATIES

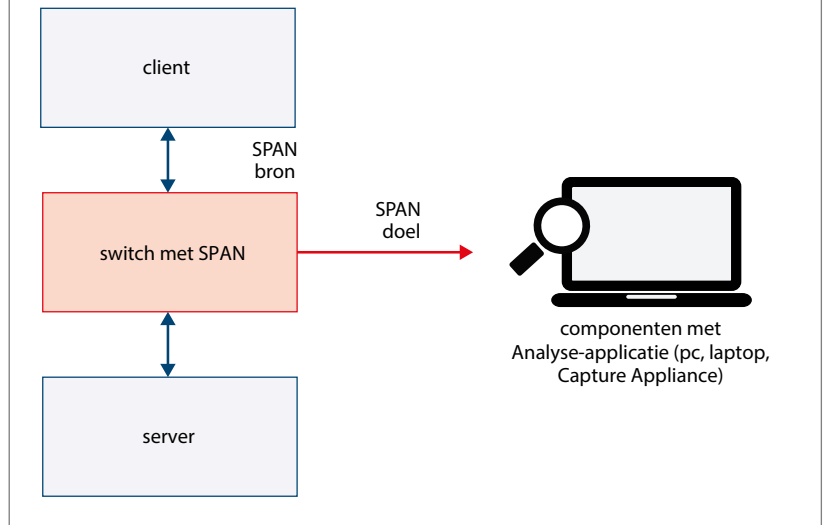
Managed switches kunnen meerdere poorten bundelen in één ethernetlijn in overeenstemming met IEEE 802.1AX-2008 en de oudere 802.3ad (Link Aggregation). Dat verhoogt de betrouwbaarheid en doorvoer van een ethernetlijn. Je kunt daar twee of meer switches mee bundelen en veel servers en NAS-apparaten ermee op een switch aansluiten.

Link Aggregation tussen switches is echter alleen zinvol als hun links niet kunnen worden geüpgraded van GE naar 10GE, en tussen een NAS en een switch als meerdere gebruikers vaak grote hoeveelheden data tegelijkertijd verplaatsen. Aangezien alle pakketten van een enkele ethernetdialog via dezelfde link verzonden moeten worden, neemt de gegevensnelheid van een enkele sessie niet toe. Een bundel van twee links kan echter meer sessies bevatten dan een enkele link.

Bundels kunnen statisch worden geconfigureerd, maar in de praktijk is het beter om het bundelen over te laten aan een Link Aggregation-protocol. In dat geval melden de externe stations voortdurend aan elkaar welke poorten geschikt zijn voor bundeling. Als

Spiegelpoort

Switches kunnen SPAN-poorten gebruiken om het dataverkeer van andere poorten door te sturen naar bijvoorbeeld een pc, die de gegevens vervolgens opneemt voor verdere analyses.



een station op afstand de bundeling niet goed activeert of een doorsturing mislukt, wordt de defecte poort uit de combinatie geschrapt, waardoor frameverlies wordt voorkomen.

Unmanaged switches kunnen geen ethernetverbindingen bundelen. Als twee van die switches toch via twee kabels met elkaar verbonden zijn, ontstaat er een loop die resulteert in een broadcast-storm die het netwerk meteen lamlegt.

Managed switches herkennen dergelijke loops met behulp van het Spanning Tree-protocol en blokkeren de redundante poorten dan (zie de link op deze pagina). Managed switches verwijderen die beperking wanneer linkbundeling actief is. Beveiligingsfuncties zoals pakketfiltering op poortniveau (poort-ACL's), poortbeveiliging op basis van MAC-adressen en toegangscontrolesystemen zijn bij managed switches ook gebruikelijk.

Voor netwerkanalyses hebben de apparaten spiegelpoorten (Switched Port Analyzer, SPAN, ook bekend als mirror-poorten). Dat kun je gebruiken om de datastroom van een bronpoort of VLAN te spiegelen naar een extra uitvoerpoort en het daar vast te leggen met bijvoorbeeld een pc die tools zoals tshark of Wireshark gebruikt om zoveel mogelijk van de uitvoerframes naar de schijf te schrijven. De opname kan vervolgens worden geanalyseerd met Wireshark.

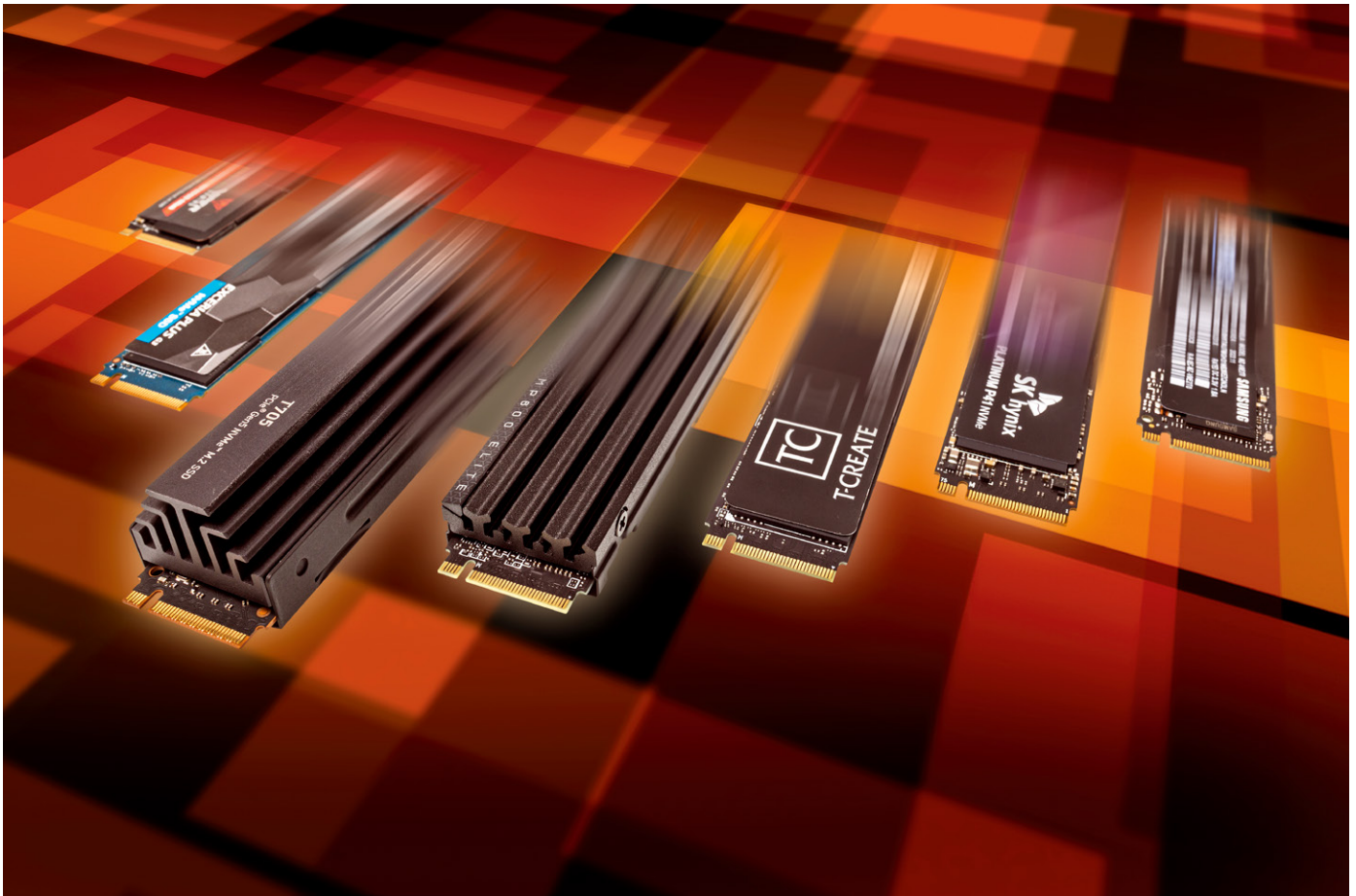
CONCLUSIE

De voordelen van managed switches ten opzichte van unmanaged switches wegen ruimschoots op tegen de nadelen. Voor beheerders van grote netwerken zijn ze onmisbaar. Bij kleine netwerken kunnen ze alleen al met hun VLAN-functie de beveiliging verbeteren. Ze kunnen namelijk worden gebruikt om het thuisnetwerk in zones te verdelen die onveilige smarthomegadgets en dergelijke weghouden van apparaten met gevoelige gegevens.



www.ct.nl/softlink/2407044





SNELLE STORAGE

PCIe 4.0- en 5.0-ssd's getest

PCIe 4.0 is tegenwoordig de standaard voor snelle ssd's. De koellichamen van de nog snellere 5.0-modellen worden steeds dikker en het geluidsniveau neemt ook toe: er is al een ssd opgedoken met twee ventilatoren.

Lutz Labs en Alieke van Sommeren

Er is de afgelopen drie maanden geen enkele nieuwe 3.0-ssd op de markt gekomen, dus de dagen van PCIe 3.0 lijken ook bij de instap-ssd's geteld te zijn. Nieuwe M.2-ssd's werken minimaal met PCIe 4.0. De meeste ssd's zijn 80 millimeter lang, maar er zijn ook twee modellen in de piepkleine 2230- en 2242-formaten in deze test.

De snellere 5.0-modellen hebben een primeur: er is al een ssd die bijna de maximaal mogelijke interfacesnelheid met meer dan 14 GB/s haalt. De hier geteste exemplaren zijn de Corsair MP600 Elite en MP600 Micro, HP FX700 en FX900 Plus, Kioxia Exceria Plus G3 SSD, Patriot VP4000 Mini, Silicon Power US75, SK Hynix Platinum P41 SSD en de Teamgroup TCreate Classic PCIe 4.0 DL SSD – allemaal met PCIe 4.0. Uit het 5.0-assortiment zijn dat de Crucial T705 PCIe Gen5 NVMe SSD, de MSI Spatium M570 Pro Frozr en de PNY CS3150. Ergens daartussenin zit de Samsung SSD 990 Evo, die werkt met vier PCIe 4.0-lanes

of twee PCIe 5.0-lanes: de snelheid is bijna hetzelfde, daarover later meer.

De VP4000 Mini SSD in 2230-formaat kwam ons bekend voor. Hij lijkt erg op de 2230-ssd's van Corsair, Seagate, Silicon Power en Teamgroup die in eerdere nummers al aan bod geweest zijn. De print op het pcb en de meetresultaten suggereren ook dat de VP4000 Mini is geproduceerd door controllerfabrikant Phison, net als de andere genoemde modellen.

Dat is niet verrassend, aangezien Phison een van de grootste ssd-fabrikanten ter wereld is, ook al zijn veel kopers van die ssd's zich niet bewust van dat feit en trekken ze zich er ook niets van aan. Dat geldt ook voor de 5.0-ssd's van MSI en PNY: de componenten en serienummers komen overeen met die van ssd's uit eerdere tests, ze zijn ook gebouwd door Phison.

De T705 van Crucial doet visueel denken aan zijn voorganger, de T700. Dat is niet verwonderlijk, want afgezien van het flashgeheugen (en de firmwareversie) zijn er geen verschillen. Het snellere NAND-flashgeheugen maakt zijn debuut in de T705, de eerste ssd die gebruik maakt van de 2400 MT/s snelheid van de Phison E26-controller. Het is fijn dat het koellichaam van de ssd niet groter is geworden, want zo past hij nog steeds in de meeste systemen.

We moesten ons testsysteem aanpassen voor een van de andere 5.0-ssd's: de MSI Spatium M570



Corsair MP600 Elite

De MP600 Elite voegt nog een model toe aan de MP600 familie van Corsair, maar wat valt er nog te verzinnen na de toevoegingen Elite, Pro, Pro LPX en Core? De Elite maakt gebruik van de DRAM-loze Phison E27T ssd-controller, die Phison net had onthuld op de CES in januari, samen met TLC-flashgeheugen van Kioxia.

Dat maakt de MP600 Elite behoorlijk snel, maar bij een test met PCMark 10 belandt hij in de onderste regionen. Dat kan mogelijk te wijten zijn aan de vrij kleine SLC-cache. Die is volgens onze metingen slechts 40 GB groot. De opdruk op het pcb suggereert dat Corsair de MP600 Elite ook door Phison laat produceren.

- ▲ moderne controller
- ▼ duur



Corsair MP600 Micro

Weer een MP600 van Corsair, dit keer met de toevoeging Micro. Corsair doelt daarmee echter niet op de kleinst mogelijke type 2230-ssd, maar op de op één na grootste met een lengte van 42 millimeter (de 2230-ssd uit de 600 serie heet Core Mini). Corsair heeft ook flashchips aan de onderkant gemonteerd, dus hij past misschien niet in een heel dunne laptop.

Corsair betaalt flink voor de exclusiviteit van het 2242-formaat, hij hoort in deze test bij de PCIe 4.0-ssd's met het hoogste aantal cent per GB. De snelheden zijn laag voor een PCIe 4.0-ssd, dankzij het redelijk snelle TLC-geheugen wordt hij pas na langere tijd trager bij het schrijven.

- ▲ compact
- ▼ duur



Crucial T705 PCIe Gen5 NVMe M.2 SSD

De Crucial T705 verschilt van zijn voorganger, de T700, eigenlijk alleen door het snellere geheugen. Het is de eerste ssd die een leesnelheid van meer dan 14 GB/s haalt en die snelheid langer vasthoudt. Het relatief kleine koellichaam is voldoende om de componenten van de ssd onder de smelttemperatuur van iets meer dan 80 °C te houden.

Er is een 4TB-versie van deze ssd aangekondigd, die meer dan 800 euro gaat kosten. De T705 is ook verkrijgbaar zonder koellichaam, de prijs ligt dan een klein tikje lager. De speciale 2TB-editie met een wit koellichaam is overpriced.

- ▲ zeer snel
- ▼ erg duur

Pro Froz is in totaal 72 millimeter hoog en paste niet meer onder de luchtkoeler van de Ryzen-cpu op ons Asrock-moederbord. We hebben meteen ook waterkoeling geïnstalleerd: de Cooler Masterliquid ML240L V2 zorgde ervoor dat de processor tijdens het testen niet oververhit raakt. Dat zou anders snel gebeuren bij het bepalen van de maximaal haalbare IOPS-prestaties, omdat de cpu dan net onder de 100 procent wordt belast.

We hebben de SanDisk Extreme M.2 niet meegenomen in deze test: volgens de fabrikant is die qua constructie vrijwel identiek aan de WD Black SN770, het verschil zit hem vooral in een ander kleur sticker. Verbatim heeft de lancering van zijn 12 GB/s Vi12000 uitgesteld, we hopen die bij de volgende test mee te nemen. We hadden graag een blik geworpen op de NN5Pro PCIe 5.0-ssd van de Japanse fabrikant Nextorage, een dochteronderneming van Phison, maar volgens de fabrikant zal die niet in de Benelux te koop zijn. De Amerikaanse fabrikant Sabrent heeft ook zijn eerste 5.0-ssd afgeleverd, waarvan de verwachting is dat meer dan 14 GB/s zal halen. Helaas is hij op dit moment alleen verkrijgbaar in de VS.

VERGELIJKINGSMATERIAAL

We hebben weer een aantal oudere, maar nog steeds interessante ssd's ter vergelijking opgenomen. Je vindt de korte kenmerken en de verwijzingen in een apart kader. De benchmarks samen met de nieuwe modellen die we hier testen hebben we ook weer op een rij gezet. Ssd's met PCIe 3.0 hebben we niet meer opgenomen, want voor hetzelfde geld kun je een veel snellere ssd krijgen met PCIe 4.0.

Over prijzen gesproken: die zijn weer gestegen. De iets oudere modellen kosten nu ruim 20 procent meer dan drie maanden geleden. De situatie is anders voor nieuwere modellen, zo kost de Micron 2400 2230 een aantal tientjes minder dan drie maanden geleden en de Lexar NM790 is qua prijs ongeveer gelijk gebleven.

Hoewel de twee PCIe 5.0-ssd's ook goedkoper zijn geworden, hebben we ze vervangen: de Crucial T700 maakte plaats voor zijn opvolger en de Seagate 540 Firecuda, met een maximum van 10 GB/s, behoort tot de eerste generatie PCIe 5.0-ssd's. Als je een PCIe 5.0-ssd wilt installeren, moet je op zijn minst gaan voor de tweede generatie met 12 GB/s. Als voorbeeld hebben we de Corsair MP700 Pro genomen, die met zijn kleine



HP SSD FX700

De HP FX700 is afkomstig van de Chinese fabrikant BiWin, die al enige tijd ssd's verkoopt onder het HP-label. We hadden de ssd in december al in huis, maar omdat de marktintroductie uitgesteld werd, mochten we daar nog niets over zeggen.

BiWin gebruikt QLC-flash van YMTC en de Maxiotek 1602A-controller – beide van Chinese makelij. De FX700 zou snel genoeg moeten zijn voor dagelijks gebruik, maar het QLC-flashgeheugen is zwakker voor langdurige taken. De ssd haalt slechts 162 MB/s bij volledig volschrijven met H2testw, de op één na laagste waarde in deze test.

- ▲ betaalbaar
- ▼ traag bij lang schrijven



HP SSD FX900 Plus

De FX900 verschilt van de FX700 alleen op het gebied van flashgeheugen, maar dat behoort tot een compleet andere klasse: het TLC-flashgeheugen van YMTC is aanzienlijk sneller. Daardoor haalt de FX900 hoge waarden voor langdurige schrijfsessies en het resultaat van PCMark 10 is ook ruim twee keer zo hoog als dat van de FX700.

De FX900 is een van de weinige 4TB-ssd's die alleen aan de bovenkant met chips is uitgerust. Daardoor past hij ook in krappe laptops. De prijs per GB is ook een van de lagere bij de PCIe 4.0-ssd's.

- ▲ betaalbaar
- ▲ snel



Kioxia Exceria Plus G3 SSD

Kioxia maakt de goedkoopste ssd in deze test, maar ook een van de traagste: de Exceria Plus G3 haalt iets meer dan 5 GB/s bij het lezen en nog geen 4 GB/s bij het schrijven. Ondanks het nominaal snelle TLC-geheugen, haalt hij slechts 400 MB/s bij het volschrijven met H2testw.

Kioxia gebruikt zijn eigen geheugen uit de BiCS6-serie met 162 lagen, maar in tegenstelling tot wat gebruikelijk is, heeft het geen eigen ssd-controller. In plaats daarvan is de Phison E21T verantwoordelijk voor het verdelen van de data.

- ▲ goedkoop
- ▼ traag

koellichaam nog in veel installatiesituaties moet passen. De ventilator blaast langs het koellichaam en is stil in vergelijking met andere ssd-ventilatoren.

De goedkoopste PCIe 4.0-ssd met 1 TB in deze test is de WD Blue SN580, maar hij is alsnog wat tientjes duurder dan eind vorig jaar. Nieuw is de Patriot VP4300, een van de snellere PCIe 4.0-modellen. Met prijzen vanaf 65 euro is het prijsniveau niet al te gek.

Bij sommige van die goedkope modellen doe je mee aan een onderdelenloterij: de fabrikanten kopen controllers en flashgeheugen zo goedkoop mogelijk in en zetten daar hun ssd's mee in elkaar. Ze garanderen minimale snelheden en endurance, maar geen componenten. We zouden bijvoorbeeld elke drie maanden een goedkope model ssd kunnen kopen en zien van welke onderdelen die gemaakt is, maar de winst in kennis zou klein zijn: het volgende kwartaal kunnen de componenten weer compleet anders zijn.

Er zijn deze keer twee vertegenwoordigers van de 2230-ssd's: de Micron 2400 is de goedkoopste, maar de SN770M van Western Digital is sneller. Die wist zich tijdens de test duidelijk te onderscheiden van andere fysiek kleinere ssd's.

ACTIEVE EN PASSIEVE KOELING

De nieuwe PCIe 5.0-ssd's onderscheiden zich duidelijk van de massa M.2-ssd's. De controllerfabrikant Phison levert een koellichaam en een ventilator in het referentieontwerp voor ssd's met zijn E26. PNY houdt zich daar zelfs twee keer aan: er zitten twee ventilatoren in het koellichaam, wat een storend geluid kan veroorzaken bij een open pc-opstelling. De vraag is of je bereid bent om die extra herrie te accepteren of dat je dat misschien alleen wilt doen als de ssd's daardoor sneller werken en langer meegaan.

De MSI Spatium M570 heeft een enorm koellichaam, maar geen ventilator. De Crucial T705 met een hoogte van slechts 20 millimeter zou daarentegen in bijna elke desktop-pc moeten passen. Zelfs onder hoge belasting kwam de T705 tijdens de test niet verder dan 80 °C, alleen daarboven verminderden zijn prestaties. In de praktijk zal dat slechts zelden voorkomen.

TWEE OF VIER LANES

Ssd's met PCIe 5.0 zijn sneller dan ssd's met PCIe 4.0. Of toch niet? Samsung heeft met de 990 Evo een



MSI Spatium M570 Pro Frozr

MSI bouwt in de hoogte: het koellichaam van de Spatium M570 Pro Frozr is 72 millimeter hoog. De rest van de ssd is min of meer bekend, het is een PCIe 5.0-ssd gemaakt door controllerfabrikant Phison en medium-speed TLC-NAND met 2000 MT/s wordt gebruikt voor het flashdeel.

Dat betekent dat de ssd ongeveer 12 GB/s lees- en schrijfsnelheden haalt en dankzij de goede warmteafvoer niet oververhit raakt tijdens langdurige tests. Desondanks haalt hij maar net iets minder dan 2000 punten bij PCMark 10, maar blijft hij maar net achter bij de T705 bij de volledige schrijftest met H2testw.

- ▲ snel
- ▼ hoge koeler, duur

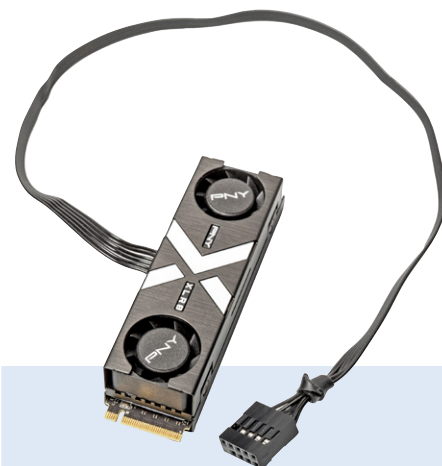


Patriot VP4000 Mini

De VP4000 Mini van Patriot is een 2230-ssd met PCIe 4.0, die in deze vorm al te koop is onder andere namen: Emtec, Teamgroup, Silicon Power en anderen hebben hem al besteld bij controllerfabrikant Phison en er hun eigen label op geplakt.

Deze ssd is behoorlijk snel bij korte acties en haalt meer dan 5 GB/s bij het lezen, maar het QLC-flashgeheugen kan het niet meer bijhouden bij het schrijven voor langere periodes. Bij de duurttest met H2testw haalt de VP4000 Mini slechts 134 MB/s – sommige harde schijven zijn sneller dan dat.

- ▲ zeer compact
- ▼ traag bij lang schrijven



PNY CS3150

RGB-verlichting in de koeler en twee ventilatoren: de CS3150 van PNY geeft licht en maakt lawaai – maar helaas te veel van het laatste. We kwamen onder volledige belasting tot 4,1 sone. De twee ventilatoren slagen er echter in om de temperatuur van de ssd onder alle belastingomstandigheden onder de 56 °C te houden.

De ventilatoren en RGB-bediening hebben een interne usb-header nodig, terwijl de verlichting en snelheidscurve kunnen worden aangepast via de PNY VelocityX-app. Zoek naar de iets oudere versie 1.2, die intuïtiever is. Zoals verwacht is de eerste PCIe 5.0-ssd met slechts 1 TB in deze test iets langzamer dan de grotere versies.

- ▲ snel
- ▼ luid, duur

hybride ssd gebouwd die dezelfde snelheid haalt in 4.0- en 5.0-slots. Het is de eerste Samsung-ssd met de nieuwe interface, maar toch langzamer dan de 990 Pro, die voorlopig waarschijnlijk de snelste Samsung-ssd zal blijven. In het 5.0-slot gebruikt de 990 Evo slechts twee van de snelle lanes en haalt daarmee bijna dezelfde snelheid als met vier 4.0-lanes.

Samsung-manager Daniel Maric gaf ons één reden in het bijzonder voor die ongebruikelijke combinatie: met slechts twee lanes verbruikt de ssd aanzienlijk minder energie dan met vier, maar ondanks herhaalde navraag kon Samsung de besparingen bij twee lanes verder niet kwantificeren.

Samsung bouwt de ssd minder voor de eindgebruikers en meer voor laptopfabrikanten. Zij profiteren niet alleen van het lagere energieverbruik, maar kunnen ook twee van de schaarse PCIe-lanes voor andere doeleinden inzetten.

FLASHGEHEUGENMARKT

De prijzen blijven stijgen omdat de fabrikanten hun productiebeperkingen nog niet opgeven. En daarvoor kunnen ze hun winsten weer verhogen. Volgens

marktonderzoeksbureau Trendforce hebben flashgeheugenfabrikanten in het laatste kwartaal van 2023 11,5 miljard dollar binnengehaald, een stijging van ongeveer 24,5 procent ten opzichte van het derde kwartaal.

Samsung blijft marktleider met een aandeel van 37 procent, gevolgd door de SK Group met SK Hynix en Solidigm, de voormalige flashdivisie van Intel, met 22 procent.

Die wordt gevolgd door productiepartners Western Digital (15 procent) en Kioxia (13 procent), evenals Micron (10 procent) en de rest, waarvan 5 procent waarschijnlijk voornamelijk afkomstig is van het Chinese bedrijf YMTC.

Het is echter de vraag of YMTC zijn marktaandeel verder zal kunnen uitbreiden aangezien het op een andere zwarte lijst is beland: het Amerikaanse leger mag geen apparaten meer kopen die chips van het Chinese bedrijf bevatten.

Als je alleen naar ssd's kijkt en het geheugen in smartphones, geheugenkaarten en industriële systemen buiten beschouwing laat, is de verdeling iets anders. Fabrikanten wisten 88 miljoen ssd's te ver-



Samsung SSD 990 Evo

De eerste PCIe 5.0-ssd van Samsung is een beetje van alles wat: in een PCIe 4.0-slot is hij net zo snel als in een PCIe 5.0-slot. Als een typische Evo-ssd is hij aanzienlijk langzamer dan de Pro-serie, maar ook goedkoper.

Het is vreemd dat hij bij de test veel sneller is dan Samsung beweert: Samsung belooft ongeveer 5 GB/s voor sequentieel lezen, wat we ook haalden met één worker en een querydiepte van 32. Met vier workers en een querydiepte van 32 is hij echter veel sneller en haalde hij 6,8 GB/s – zowel met PCIe 4.0 als 5.0. Samsung kon daar geen verklaring voor geven.

- ▲ interessante techniek
- ▼ relatief traag



Silicon Power US75

De US75 van Silicon Power is vergelijkbaar met de FX900 van HP: een MAP-1602A ssd-controller en het TLC-flashgeheugen van YMTC. De gemeten waarden verschillen echter een beetje, vooral bij het schrijven. De US75 haalt iets hogere waarden met lometer en ook bij de duurtest met H2testw.

Bij de tests met PCMark 10 blijft hij echter achter: de iets lagere waarde voor geschiktheid als systeemschijf is van minder belang, maar de bijna 30 procent lagere waarde bij PCMark 10 is absoluut negatief. BiWin kan misschien beter flashgeheugen installeren.

- ▲ snel
- ▼ hoog idle energieverbruik



SK Hynix Platinum P41 SSD

SK Hynix is in de Benelux geen bekend merk. Men kocht een paar jaar geleden de flashdivisie van Intel, maar is zelf al lange tijd fabrikant van NAND-flashgeheugen.

Sk Hynix vertrouwt in zijn P41-ssd op zijn eigen TLC-flashgeheugen met 176 lagen en een zelf ontwikkelde ssd-controller. Dat betekent dat de P41 aan de top van de PCIe 4.0-limiet zit. Bij de duurtest met H2testw presteert hij zelfs beter dan de nominaal snellere PCNY-ssd met PCIe 5.0 met 1,6 GB/s. De SK Hynix Platinum P41 is identiek aan de Solidigm P44.

- ▲ snel
- ▲ snel onder belasting

kopen in het laatste kwartaal van 2023, waar Samsung 27 procent van voor zijn rekening nam. Western Digital volgt met 21 procent, Kioxia staat met 9,5 procent op vergelijkbare hoogte met Micron (10,8%), SK Hynix (9,0%) en Kingston (10,8%). Solidigm, de voormalige flashdivisie van Intel, staat op 5,4 procent.

De fabrikanten leverden al met al 88 exabytes aan flashgeheugen met hun ssd's, waarvan Samsung verantwoordelijk was voor 30,5 procent. De ssd's van Samsung hebben daarmee een hogere capaciteit dan het gemiddelde. De capaciteit-eenhedenverhouding bij Solidigm is echter bijzonder opvallend: 12 procent van het aantal exabytes wordt gebruikt door dat bedrijf, dat momenteel de grootste ssd in zijn assortiment heeft met de 61,4 TB grote D5-P5336.

Het gaat dus goed met de gevestigde opslagfabrikanten, waarbij de prijzen eerder meer zullen stijgen dan dalen. Trendforce verwacht dat de flashprijzen met ongeveer 25 procent zullen stijgen. Iedereen die een ssd nodig heeft, moet er dan ook nu een kopen. Hopen op dalende prijzen werkt waarschijnlijk alleen in individuele gevallen.

De baas van controllerfabrikant Phison, KS Pua, waarschuwt echter al voor te hoge prijzen. Die zouden de vraag kunnen doen afnemen. Fabrikanten moeten de productie weer opvoeren en aan de vraag naar opslag voldoen, zei Pua. Hij waarschuwde halverwege vorig jaar echter ook dat de prijzen te laag waren [1]. Volgens hem had dat kunnen leiden tot insolventie van leveranciers – wat toen niet gebeurde.

Zijn waarschuwing is niet alleen gevoed door eigenbelang. Phison is namelijk een van de grootste ssd-fabrikanten ter wereld: vorig jaar kocht het bedrijf 16 exabytes aan flashgeheugen en gebruikte het om ssd's voor andere bedrijven te bouwen.

Op de International Solid-State Circuits Conference 2024 (ISSCC) presenteerde Samsung een nieuw QLC-geheugen met 280 lagen, dat naar verluidt het geheugen van alle andere fabrikanten overtreft in termen van oppervlaktedichtheid.

Het geheugen van Samsung zou 28,5 Gbit/mm² halen, bijna 25 procent meer dan het 5-bit geheugen van Intel met 23,3 Gbit/mm². Beide zijn echter nog lang niet klaar voor de markt, waar YMTC momenteel



Teamgroup TCreate Classic PCIe 4.0 DL SSD

De TCreate Classic PCIe 4.0 DL SSD van Teamgroup is de oudste ssd in deze test. Hij staat al ongeveer een jaar in de prijsvergelijkers, maar was lange tijd niet verkrijgbaar. Teamgroup gebruikt de E21T Phison-controller en flashgeheugen van Micron voor de ssd. Hij haalt daarmee typische waarden voor die combinatie van iets minder dan 5 GB/s lezen en 4,5 GB/s bij schrijven.

De Corsair MP600 Micro gebruikt vergelijkbare componenten en is daarmee iets sneller, maar ook aanzienlijk duurder. Vergeleken met de Kioxia Exceria G3 houdt de Teamgroup-ssd zijn snelheid langer vast.

- ▲ goedkoop
- ▼ traag

aan de leiding gaat met een oppervlaktedichtheid van 19,8 Gbit/mm².

VERDELEN EN SAMENVOEGEN

De voorbereidingen voor het splitsen van Western Digital in twee onafhankelijke bedrijven gaan op de achtergrond verder. Het bedrijf kondigde die splitsing enige tijd geleden aan op verzoek van een grote investeerder. De huidige CEO, David Goekeler, komt aan het hoofd te staan van het nog naamloze flashgeheugenbedrijf.

De hardeschijfactiviteiten gaan verder onder de naam Western Digital en worden geleid door Irving Tam, de huidige Executive Vice President voor de wereldwijde activiteiten.

Over de verdeling van Western Digital is op dit moment nog geen besluit genomen, dat wordt later dit jaar verwacht. De splitsing kan ook de fusiebesprekingen tussen Kioxia en het flashgeheugenonderdeel van

Western Digital nieuw leven inblazen. Onlangs sprak een van de aandeelhouders van Kioxia, de flashfabrikant SK Hynix, een veto uit tegen de fusie, maar dat lijkt niet definitief te zijn.

Een extra financiële injectie van een miljard dollar van de Japanse overheid voor het bouwen van twee extra flashfabrieken in de buurt van de Japanse steden Yokkaichi en Kitakami wordt door sommige marktwaarnemers gezien als een verdere indicatie van een op handen zijnde fusie tussen Kioxia en de flashdivisie van Western Digital.

De Japanse overheid geeft daarmee een totale subsidie van 1,63 miljard dollar, terwijl de twee bedrijven zelf van plan zijn om samen iets minder dan 5 miljard te investeren.

SSD-CONTROLLER

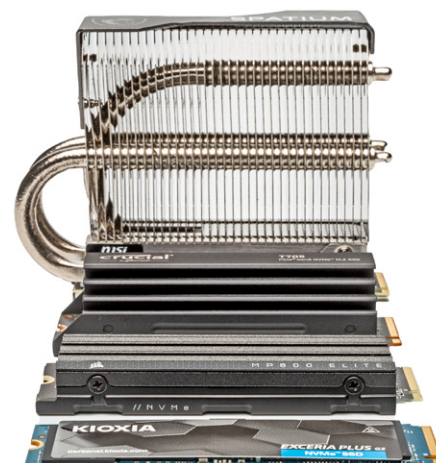
De ontwikkeling van controllers voor PCIe 5.0 is vooral gericht op een lager energieverbruik omdat de enorme koellichamen en ventilatoren van de huidige modellen mensen afschrikken ze aan te schaffen. Het huidige topmodel, de Phison E26, verbruikt tot 11,5 watt bij volledige belasting.

Phison heeft in januari echter al een zinnigere controller gepresenteerd: de E31T. Die maakt ook gebruik van PCIe 5.0, maar slechts vier NAND-kanalen. Het weglaten van DRAM-ondersteuning verlaagt ook het energieverbruik. Desalniettemin wordt verwacht dat ssd's met de E31T zonder complexe koeling lees- en schrijfsnelheden tot 10,8 GB/s zullen halen. De aangekondigde Silicon Motion SM2508 PCIe 5.0-controller hebben we nog niet aangetroffen op een ssd. Om de ontwikkelprocessen te versnellen, heeft het bedrijf zich nu opgesplitst in twee business-units: Client & Automotive Storage (CAS) en Enterprise Storage & Display Interface Solution (ESDI). Meer concurrentie is zeker goed voor de markt.

RANDZAKEN

Een X-post van yuuki-ans heeft een nieuwe ssd-fabrikant onder de aandacht gebracht: Microsoft. Hij postte een foto en wat technische gegevens van een M.2-ssd met de naam Z1000. Het flashgeheugen is afkomstig van Toshiba, het DRAM van Micron en de controller van CNEX Labs, een fabrikant die vooral actief is in de enterprisesector. Die ssd werd naar verluidt al in juni 2020 geproduceerd, dus het is onwaarschijnlijk dat Microsoft de massamarkt voor ssd's nu zal betreden.

Over Microsoft gesproken: sommige lezers hebben geprobeerd om de Microsoft Surface Pro 7+ te upgraden met een grote-



Niets tegen een ssd-heatsink, maar het model van MSI op de achtergrond met een hoogte van 72 millimeter begint wel een beetje absurd te worden.

De baas van
controllerfabrikant
Phison waarschuwt
al voor te hoge
prijzen



De Haechi H01-koeler van SK Hynix vervangt het originele ssd-deksel van de Playstation 5 en dient als ssd-koeler.



Corsair MP700 Pro

Getest in c't 4/2024 op pagina 100

- ▲ zeer snel, stille ventilator
- ▼ duur

€ 330 (2 TB, PCIe 5.0)

Updates voor de eerste PCIe 5.0-ssd's worden nog steeds maar druppelsgewijs uitgebracht



Lexar NM790

Getest in c't 1-2/2024, p.48

- ▲ goedkoop
- ▲ snel

€ 75 (1 TB, PCIe 4.0)



Micron 2400

Getest in c't 1-2/2024 op pagina 48

- ▲ relatief betaalbaar
- ▼ traag bij hoge vulstand

€ 210 (2 TB, PCIe 4.0)



Patriot VP4300 Lite

Getest in c't 1-2/2024 op pagina 48

- ▲ snel
- ▲ houdt snelheid goed vol

€ 95 (1 TB, PCIe 4.0)

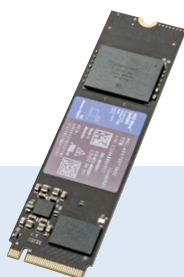


Samsung SSD 980 Pro

Getest in c't 11/2021 op pagina 50

- ▲ snel
- ▲ warmt nauwelijks op

€ 105 (1 TB, PCIe 4.0)



WD Blue SN580

Getest in c't 1-2/2024 op pagina 48

- ▲ goedkoop
- ▼ traag voor PCIe 4.0

€ 70 (1 TB, PCIe 4.0)



WD Black SN770M

Getest in c't 4/2024 op pagina 100

- ▲ snel voor een 2230-ssd
- ▼ duur

€ 205 (2 TB, PCIe 4.0)



WD Black SN850X

Getest in c't 1-2/2023 op pagina 114

- ▲ zeer snel
- ▲ houdt snelheid goed vol

€ 100 (1 TB, PCIe 4.0)

Een firmware-update beschermt de FireCuda 540 tegen oververhitting. De Seagate Download Finder heeft alleen het serienummer nodig, de tool herkent het schijfmodel zelf.

re ssd. In principe passen 2230-ssd's zoals de VP4000 Mini uit deze test erin, en met 2 TB flashgeheugen is een upgrade echt de moeite waard.

Maar dat werkt niet altijd. Net als veel andere laptopfabrikanten lijkt Microsoft een whitelist in het BIOS te hebben die alleen bepaalde ssd's toestaat. Volgens meldingen leidt het werken met een Kioxia BG5 tot frequente crashes.

Met de Transcend MTE300S moet het iets beter werken, maar ook niet stabiel. Als je wilt upgraden met een grotere ssd, kun je daarom het beste advies op verschillende forums inwinnen voordat je tot aanschaf overgaat.

Als je een Playstation 5 hebt, kun je het geheugen daarvan vrij eenvoudig upgraden: het enige wat je nodig hebt is een ssd met PCIe 4.0 en een koeler met een maximale hoogte van 8 mm boven de printplaat, want dan past de ssd onder het deksel van de PS5.

SK Hynix heeft een vervangend deksel voor de PS5 in het programma dat de ssd-koeler overbodig maakt: de Haechi 01. Die is zo dik dat hij direct op de ssd rust. Dat resulteert waarschijnlijk in een betere warmteafvoer, aangezien een conventionele ssd-koeler eerst de luchtspleet naar de originele cover moet overbruggen. De Haechi 01 is te koop vanaf 13 euro.

M.2-ssd's met PCIe 4.0 en 5.0 – benchmarks

Model	Seq. transferrates schrijven/lezen ¹ [MB/s]	Seq. transferrates volschrijven ssd ² /5 minuten ¹ [MB/s]	IOPS lezen QD=1/32/256 ³ [in duizendtallen]	IOPS schrijven QD=1/32/256 ³ [in duizendtallen]	PCMark 10 Drive Performance Consistency/ Full System Drive ⁴ [punten]
	beter ▶	beter ▶	beter ▶	beter ▶	beter ▶
Corsair MP600 Elite (2 TB)	6659/7380	1360/6666	21/401/792	66/469/1101	856/3197
Corsair MP600 Micro (1 TB)	4868/5250	1140/4865	19/337/759	66/462/989	954/2636
Crucial T705 PCIe Gen5 NVMe M.2 SSD (2 TB)	12729/14447	2080/9528	22/576/1369	79/593/1494	4568/5482
HP SSD FX700 (2 TB)	6252/7314	162/6219	21/485/665	61/192/212	663/3383
HP SSD FX900 Plus (4 TB)	6487/7432	1150/6477	21/457/672	51/593/931	1543/3589
Kioxia Exceria Plus G3 SSD (2 TB)	3981/5077	391/4004	15/262/649	66/451/943	1333/3351
MSI Spatium M570 Pro Frozr (2 TB)	11666/12362	1980/11653	22/569/1417	82/297/1485	1801/5442
Patriot VP4000 Mini (2 TB)	3978/5147	134/3786	16/212/474	67/459/877	541/2582
PNY CS3150 (1 TB)	9281/11559	1500/9290	542/1345/83	83/590/1491	1393/5422
Samsung SSD 990 Evo (2 TB)	3737/6768	1180/3738	19/441/766	58/401/669	928/3396
Silicon Power US75 (2 TB)	6668/7450	1220/6423	20/481/682	52/261/384	1104/3427
SK Hynix P41 SSD (2 TB)	6596/7383	1620/6586	20/535/1430	62/474/1168	1745/3753
Teamgroup Classic PCIe 4.0 DL SSD (2 TB)	4482/4931	899/4655	19/316/759	66/416/747	803/2487
Ter vergelijking					
Corsair MP700 Pro (2 TB)	11819/12363	1940/11808	21/486/1456	79/574/1514	3839/4935
Lexar NM790 (1 TB)	6638/7453	847/6642	21/488/687	57/287/434	1018/3451
Micron 2400 NVMe SSD (2 TB)	3225/4425	187/2515	18/369/560	61/412/570	491/2545
Patriot VP4300 Lite M.2 PCIe Gen4 x4 Gaming SSD (1 TB)	6641/7448	1160/6643	20/488/683	56/287/434	1049/3496
Samsung SSD 980 Pro (1 TB)	4953/6648	1690/4937	22/503/1020	55/505/1035	2130/2910
Western Digital WD Blue SN580 NVMe SSD (1 TB)	4129/4119	600/3976	20/247/473	61/509/617	996/3274
Western Digital WD_Black SN770M NVMe SSD (2 TB)	4895/5219	439/4756	16/244/362	75/552/526	920/3210
Western Digital SN850X (2 TB)	6681/7368	1560/6423	21/447/1181	64/519/825	1260/3682

¹ gemeten met Iometer, blok grootte 512 kB, duur: 60 s ² gemeten met H2testw ³ gemeten met Iometer, blok grootte 4 kB, duur: 60 s ⁴ i.c.m. een Asus TUF Gaming B550M-Plus (Wi-Fi) met AMD Ryzen 7 5800X en 16 GB RAM, PCIe-5.0-ssd's i.c.m. een ASRock B650 Pro met AMD Ryzen 9 7950X en 32 GB RAM

SOFTWARE-UPDATES

Samsung heeft een update uitgebracht voor zijn Windows ssd-beheertool Magician. Die heeft geen nieuwe functies, maar dicht wel een beveiligingslek. Door een bug in versie 8.0.0 van Magician konden lokale gebruikers met hogere rechten ongeautoriseerde toegang krijgen tot gegevens. Versie 8.0.1 dicht dat gat en Samsung raadt sterk aan om die nieuwe versie te installeren. Je kunt hem downloaden bij Samsung (zie de link links op deze pagina), maar ook installeren via Magician zelf.

Updates voor de eerste PCIe 5.0-ssd's tegen temperatuurgerelateerde crashes worden nog steeds maar druppelsgewijs uitgebracht. Seagate had dat voor zijn Firecuda 540 beloofd voor september vorig jaar, maar die is pas sinds eind januari beschikbaar.

Op onze Firecuda 540 werd versie SUESR010 geïnstalleerd, maar versie SUESR101 is nu beschikbaar. Controleer vooraf het serienummer van de ssd, de eenvoudigste manier daarvoor is om een SMART-tool

te gebruiken zoals CrystalDiskInfo of Hard Disk Sentinel.

CONCLUSIE

Ssd's met PCIe 5.0 lopen inmiddels tegen de limieten van de interface aan. Als veel geld wilt uitgeven aan een ssd, dan krijg je zeker een zeer snelle ssd. Belangrijker is echter dat je daar niet per se een enorm koellichaam of een ventilator voor nodig hebt.

Bij ssd's met PCIe 4.0 is het beeld wat verdeeld. Sommige halen het maximum uit de interface, andere zijn nauwelijks sneller dan goede ssd's met een PCIe 3.0-interface. Er zijn in ieder geval nog redelijk betaalbare modellen die heel goed kunnen presteren in een kantoor-pc.

De Samsung 990 Evo, die met zijn twee snelle lanes een positieve ontwikkeling zou kunnen inluiden, is ook een mooie optie: weg van de snelheidsgekke, naar wel kiezen voor voldoende snelheid met een matig energieverbruik.



www.ct.nl/softlink/2407050

M.2-ssd's met PCIe 4.0 en 5.0

Model	MP600 Elite	MP600 Micro	T705 PCIe Gen5 NVMe M.2 SSD	SSD FX700	SSD FX900 Plus	Exceria Plus G3 SSD	Spatium M570 Pro Frozr	VP4000 Mini	CS3150	SSD 990 Evo	US75	P41 SSD	Classic PCIe 4.0 DL SSD
Fabrikant, website	Corsair, corsair.com	Corsair, corsair.com	Crucial, crucial.com	HP, hp.biwin-tech.com	HP, hp.biwin-tech.com	Kioxia, kioxia.com	MSI, msi.com	Patriot, patriot-memory.com	PNY, pny.com	Samsung, samsung.nl	Silicon Power, silicon-power.com	SK Hynix, skhynix.com	Teamgroup, teamgroup inc.com
Typenummer	CSSD-F2000GBMP-600EHS	CSSD-F1000GBMP-600MCR	CT2000-T705SSD5	8U2N5-AA#ABB	7F619-AA#ABB	LSD10-Z002TG8	SPATIUMM-570PROPCle50FROZR	VP4000-M2TBM23	M280CS-3150XHS-1TB-RB	MZ-V9E2-T0BW	SP02KGBP-44US7505AY	SHP41-2000GM-2	TM8FPM-002T0C329
Capaciteit volgens fabrikant / herkend door Windows ¹	2 TB / 1863 GB	1 TB / 932 GB	2 TB / 1863 GB	2 TB / 1908 GB	4 TB / 3815 GB	2 TB / 1863 GB	2 TB / 1863 GB	2 TB / 1863 GB	1 TB / 932 GB	2 TB / 1863 GB	2 TB / 1908 GB	2 TB / 1863 GB	2 TB / 1863 GB
Interface / protocol	PCIe 4.0 x4 / NVMe 1.4	PCIe 4.0 x4 / NVMe 1.4	PCIe 5.0 x4 / NVMe 2.0	PCIe 4.0 x4 / NVMe 2.0	PCIe 4.0 x4 / NVMe 2.0	PCIe 4.0 x4 / NVMe 1.4	PCIe 5.0 x4 / NVMe 2.0	PCIe 4.0 x4 / NVMe 1.4	PCIe 5.0 x4 / NVMe 2.0	PCIe 4.0 x4 / 5.0 x2 / NVMe 2.0	PCIe 4.0 x4 / NVMe 1.4	PCIe 4.0 x4 / NVMe 1.4	PCIe 4.0 x4 / NVMe 1.4
Formfactor / montage chips / hoogte boven pcb uit	M.2 2280 / enkelzijdig / 7,1 mm	M.2 2242 / dubbelzijdig / 1,9 mm	M.2 2280 / dubbelzijdig / 17,7 mm	M.2 2280 / enkelzijdig / 1,7 mm	M.2 2280 / enkelzijdig / 1,8 mm	M.2 2280 / enkelzijdig / 1,4 mm	M.2 2280 / dubbelzijdig / 69,4 mm	M.2 2230 / enkelzijdig / 1,6 mm	M.2 2280 / dubbelzijdig / 15,3 mm	M.2 2280 / enkelzijdig / 1,2 mm	M.2 2280 / enkelzijdig / 1,4 mm	M.2 2280 / enkelzijdig / 1,4 mm	M.2 2280 / enkelzijdig / 1,5 mm
Ssd-controller / NAND-kanalen / firmware-versie	Phison E27T / 4 / ERFM11.0	Phison E5021T / 4 / ELFMH0.1	Phison E26 / 8 / PACRS5111	Maxiotek 1602A / 4 / SN14428	Maxiotek 1602A / 4 / SN12717	Phison E21T / 4 / ELFA01.2	Phison E26 / 8 / EQFM22.2	Phison E21T / 4 / ELFCM1.0	Phison E26 / 8 / CS315222	Samsung Piccolo / 4 / OB2QKXJ7	Maxiotek MAP1602A / 4 / SN11273	SK Hynix / 8 / 51060A20	Phison E21T / 4 / ELFMB0.6
Flash-fabrikant / soort flash	Kioxia / TLC	Micron / TLC	Micron / TLC	YMTC / QLC	YMTC / TLC	Kioxia / TLC	Micron / TLC	Micron / QLC	Micron / TLC	Samsung / TLC	YMTC / TLC	SK Hynix / TLC	Micron / TLC
Schrijfperformance per dag ²	658 GB	329 GB	658 GB	438 GB	1315 GB	658 GB	767 GB	247 GB	384 GB	658 GB	658 GB	658 GB	658 GB
Kans op uitval (jaar) ²	0,58 %	0,58 %	0,44 %	0,44 %	0,44 %	0,58 %	0,55 %	g.o.	0,55 %	0,58 %	0,58 %	g.o.	0,58 %
DRAM-cache ²	—	—	4 GB	—	—	—	4 GB	—	2 GB	—	—	2 GB	—
Energieverbruik ² [watt]	0,005 / 0,05 / 1,8 / 3 / 5,7	0,0025 / 0,03 / 1,5 / 3 / 5	0,144 / 0,144 / 6 / 8 / 11,5	0,0025 / 0,05 / 3,6 / 5,8 / 6,5	0,0025 / 0,05 / 3,6 / 5,8 / 6,5	0,005 / 0,05 / 2,1 / 3,6 / 5,5	0,144 / 0,144 / 6 / 8 / 11,5	0,005 / 0,05 / 1,5 / 2,4 / 5,5	0,144 / 0,144 / 6 / 8 / 11,5	0,007 / 0,08 / 7,47 / 7,47	0,726 / 0,746 / 3,6 / 5,8 / 6,5	0,005 / 0,05 / 1,5 / 3,9 / 7,5	0,005 / 0,07 / 1,92 / 2,4 / 5
Garantie	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar	5 jaar
Prijs per gigabyte	9,6 ct	10,9 ct	21,4 ct	9,1 ct	8,6 ct	6,7 ct	19,8 ct	12 ct	24,6 ct	8 ct	7,8 ct	10,4 ct	7,5 ct
Prijs	€ 180	€ 102	€ 400	€ 175	€ 330	€ 125	€ 370	€ 225	€ 230	€ 150	€ 150	€ 195	€ 140
overige capaciteiten	1 TB (€ 105)	—	1 TB (€ 205)	512 GB (€ 65), 1 TB (€ 110)	512 GB (€ 70), 1 TB (€ 115), 2 TB (€ 160)	1 TB (€ 80)	—	500 GB (€ 65), 1 TB (€ 105)	2 TB (€ 380)	1 TB (€ 110)	1 TB (€ 90), 4 TB (€ 290)	500 GB (€ 90), 1 TB (€ 115)	1 TB (€ 85)

¹ Fabrikanten rekenen met 1 GB = 1.000.000.000 byte. Voor Windows geldt echter 1 GB = 1.073.741.824 byte, de getoonde capaciteit is daardoor lager. ² volgens fabrikant
 ✓ aanwezig — niet aanwezig g.o. geen opgave

ct

LIVE

28 september 2024

Kom ook naar c't LIVE: een dag vol interessante lezingen over onderwerpen zoals security, smarthome, netwerken en meer

Bestel je kaarten op:
www.ct.nl/live



Illustratie Midjourney, c't

ENERGIEVRETENDE TAALMODELLEN

Hoe taalmodellen zoals ChatGPT in de toekomst zuiniger kunnen werken

De prestaties van de grote taalmodellen zijn zeer indrukwekkend, maar het energieverbruik ervan is dat ook. Onderzoekers buigen zich nu over dit probleem omdat het verbruik pas effectief verminderd kan worden wanneer het gedetailleerd in kaart gebracht is.

Thomas Brandstetter en Merel Atia

In het artikel 'Attention is all you need' uit 2017 presenteerden onderzoekers van Google hun eerste concept van een Transformer-model. Daarmee zetten zij de wereld van de computerlinguïstiek op zijn kop. Voorheen konden AI-algoritmes in een tekst slechts één woord tegelijk analyseren. De nieuwe modellen konden hele zinnen herkennen, wat chatbots zoals ChatGPT mogelijk maakte.

Maar er zat een addertje onder het gras. Sommige hedendaagse taalmodellen bestaan uit meer dan honderd miljard parameters. Tijdens een langdurig trainingsproces analyseren ze enorme hoeveelheden tekst. De training van GPT-3 kostte 1287 megawattuur aan energie. Dat komt ongeveer overeen met de hoeveelheid die een middelgrote kerncentrale in één uur produceert. En dat is nog maar het begin. In de eerste twee maanden na de lancering had de chatbot al 100 miljoen gebruikers aangetrokken. Volgens schattingen heeft GPT-3 elke dag 564 megawattuur extra energie nodig om zijn diensten te blijven uitvoeren.

TOENEMENDE UITSTOOT

Volgens schattingen is de informatie- en communicatietechnologie in zijn geheel nu al verantwoorde-

lijk voor twee tot vier procent van de wereldwijde uitstoot van broeikasgassen. Dat aandeel is even groot als dat van het wereldwijde luchtverkeer. Artificiële intelligentie is de nieuwe grootverbruiker in dit domein, voornamelijk dankzij taalmodellen. Die worden niet alleen steeds vaker gebruikt, maar ook steeds complexer en energie-intensiever.

‘Als je kijkt naar de groeiende vraag naar AI-diensten, lijkt het erg waarschijnlijk dat het energieverbruik de komende jaren flink zal toenemen’, zegt datawetenschapper Alex de Vries. In een publicatie in het vaktijdschrift Joule onderzocht hij het energieverbruik van taalmodellen. Omdat techbedrijven hun gegevens in het algemeen geheim houden, moest hij schattingen maken op basis van de gebruikte hardware. De bovenstaande schatting van het energieverbruik van ChatGPT is gebaseerd op het feit dat OpenAI in eerste instantie 3617 Nvidia HGX A100-servers met in totaal 28.936 gpu’s gebruikte.

Vooraf zorgwekkend is het gedachte-experiment dat De Vries aanhaalt, waarbij alle Google-vragen – dagelijks ongeveer negen miljard – worden beantwoord door een chatbot. In februari 2023 gaf Google zelf toe dat zo’n omschakeling de kosten waarschijnlijk zou vertienvoudigen. Volgens de meest pessimistische aanname in het artikel van De Vries zou dat 512.821 Nvidias A100-HGX-servers vergen met meer dan 4,1 miljoen gpu’s, die dagelijks 80 gigawattuur nodig hebben. Dat komt doordat elke server alleen al sowieso 6,5 kilowatt verbruikt. Het totaal zou ongeveer net zoveel energie verbruiken als heel Ierland, wat dertig keer meer is dan bij conventionele zoekopdrachten op trefwoorden.

Gelukkig is zo’n extreem scenario momenteel onrealistisch. Niet alleen omdat het veel tijd zou kosten om zoveel grafische kaarten te produceren, maar ook omdat het economisch onhaalbaar zou zijn. Alleen al de extra hardware zou zo’n 100 miljard dollar kosten. Volgens de Vries zouden de aanschaf- en elektriciteitskosten van de hardware, zelfs verspreid over drie jaar, de jaarlijkse winst van Google bijna volledig tenietdoen.

Bovendien zouden betere antwoorden van AI het totale aantal zoekopdrachten kunnen verminderen. Ook zijn de huidige AI-systemen nog lang niet geoptimaliseerd als het gaat om energie-efficiëntie. Toch waarschuwt de Vries voor een nonchalante houding richting artificiële intelligentie: ‘De potentiële groei laat zien dat we heel goed moeten opletten waarvoor we AI gebruiken. Het is energie-intensief en daarom moeten we het niet zomaar in allerlei dingen inbouwen waar we het misschien niet echt nodig hebben.’

EEN ENERGIEPRIJKAARTJE VOOR AI

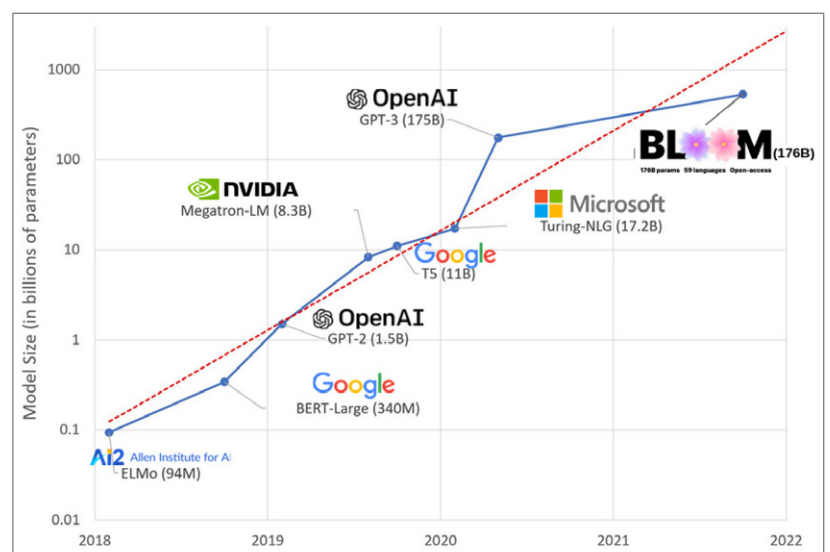
Op de milieucampus Birkenfeld van de Hogeschool van Trier zet Stefan Naumann zich met zijn team in om de grondstoffen- en energiebehoeften van AI-systemen te meten en openbaar te maken. ‘Informatie over energieverbruik is een voorwaarde om algoritmen efficiënter te maken’, zegt de professor in

duurzaamheidsinformatica. Het idee is dat aan elke dienst een energieprijkaartje gehangen wordt. Als je geïnteresseerd bent in je ecologische voetafdruk kun je meestal zonder veel moeite toegang krijgen tot de informatie over je energieverbruik, of dat nou gaat over het boeken van een vlucht of het streamen van een serie. ‘In de ideale situatie heeft de eindgebruiker van een AI-toepassing ook toegang tot die informatie,’ zegt Naumann. ‘Het zou op zijn minst mogelijk moeten zijn om er via een programmeerinterface professionele toegang tot te krijgen.’

Om het gebruik van grote systemen zoals ChatGPT beter in te schatten, voeren de wetenschappers voortdurend kleinere AI-projecten uit en meten ze het energieverbruik daar zo gedetailleerd mogelijk van. ‘Het is altijd spannend om te zien hoe de aanbieders van die systemen reageren wanneer dergelijke cijfers openbaar worden gemaakt,’ zegt Naumann. ‘Als ze reageren, is dat in ieder geval een teken dat ze ermee bezig zijn. En als ze dat niet doen, kunnen we aannemen dat het een goede schatting is of dat het verbruik in werkelijkheid veel hoger ligt.’

Onderzoekinstellingen hebben in het algemeen echter niet de infrastructuur om grote modellen zoals GPT daadwerkelijk te analyseren. ‘Dat kan snel oplopen tot honderdduizenden of miljoenen euro’s aan elektriciteitskosten,’ benadrukt Naumann. ‘Alleen de grote bedrijven zelf kunnen zich dat veroorloven.’

Een welkome uitzondering in dat verhaal is het Bloom-taalmodel, dat met zijn 176 miljard parameters op gelijke hoogte staat met GPT-3. In tegenstelling tot OpenAI hebben de makers echter besloten om het energieverbruik tijdens de bijna vier maanden durende training tot in detail te meten en te publiceren. Het model werd getraind op Nvidia A100-processors in iets meer dan een miljoen gpu-uren. Dat gebeurde met behulp van 1,6 terabytes aan gegevens in 46 menselijke talen en 13 programmeertalen. Daarbij verbruikte het volgens de ontwikkelaars 433 megawattuur.



Het aantal parameters van taalmodellen zoals GPT-3 van OpenAI is constant. Dat verhoogt ook het energieverbruik van trainingen.

AI-taalmodellen verbruiken tijdens de training enorme hoeveelheden energie. De overtollige warmte moet afgekoeld worden, zoals hier bij Google in Saint-Ghislain. Onderzoekers werken aan efficiëntere methoden om het energieverbruik te verminderen.



HARDWARE EFFICIËNTER GEBRUIKEN

De ontwikkelaars hebben ook experimenten uitgevoerd op hun servers om erachter te komen waarvoor die energie gebruikt werd. ‘Een probleem met trainingen in grote datacenters is dat de afzonderlijke computer-units zelden volledig gebruikt worden’, legt Naumann uit. Net als bij een computer die ongemerkt ingeschakeld op het bureau staat, wordt ook in die tijd energie verbruikt – zonder dat daar prestaties tegenover staan.

Uit het onderzoek van Bloom bleek dat een derde van de energie werd verbruikt aan inactieve computers. Slechts iets meer dan de helft van de energie werd daadwerkelijk gebruikt om de code uit te voeren. De rest werd besteed aan de infrastructuur van het datacenter, zoals het koelsysteem.

‘Dergelijke metingen kunnen ontwikkelaars in de toekomst helpen om hun algoritmes te optimaliseren en energie te besparen’, zegt Naumann. Naast het directe energieverbruik zijn er voor hem nog twee andere belangrijke aspecten als het gaat om verduurzaming: ‘Het is belangrijk dat de hardware ook zo lang mogelijk meegaat en niet vroegtijdig moet wor-

den vervangen door bijvoorbeeld software-updates.’ De productie ervan verbruikt namelijk ook grondstoffen en draagt bij aan de ecologische voetafdruk van artificiële intelligentie. Hoe kleiner een apparaat is en hoe minder energie het tijdens gebruik nodig heeft, des te groter de impact van de productie. ‘Bij een server die misschien 500 watt verbruikt, loont het de moeite om eerder een nieuwere generatie te kopen,’ zegt Naumann. ‘Met een smartphone is dat daarentegen bijna nooit het geval.’

Het tweede punt dat Naumann maakt is dat niet elk type elektriciteit dezelfde ecologische belasting vormt. ‘Als je energie nodig hebt, moet dat zo hernieuwbaar mogelijk zijn’, vertelt hij. Zogenaamde load-shifts kunnen daarbij helpen. Energie-intensieve taken van niet-tijdkritische processen worden aangepast aan de weersafhankelijke beschikbaarheid van hernieuwbare energie. Windturbines en zonnepaneelsystemen genereren namelijk vaak een overschot aan elektriciteit wanneer het bijzonder hard waait of de zon fel schijnt.

Idealiter wordt de artificiële intelligentie precies in zo’n tijdvenster getraind. ‘Puur technisch gezien is dat realistisch’, zegt Naumann. De ontwikkelaars zouden op die manier een tijdsbestek kunnen specificeren en dat aan de elektriciteitsleveranciers kunnen doorgeven. Bijvoorbeeld dat ze de training binnen de komende vier of twintig uur uit willen voeren. ‘Maar doe het dan wel precies wanneer de energie beschikbaar is,’ zegt Naumann. ‘Dat biedt ook een bepaalde mate aan planningszekerheid.’

STEEDS GROTERE MODELLEN

Het is echter de vraag of dat voldoende zal zijn om de ontwikkeling van AI-modellen ecologisch duurzaam te maken. De complexiteit van met name taalmodellen lijkt immers exponentieel te groeien, waardoor ook de benodigde energie voor trainingen explodeert. Het gerucht gaat dat OpenAI voor GPT-4 al tien keer zoveel parameters heeft moeten optimaliseren als voor zijn voorganger GPT-3. ‘De rekeninspanning die nodig is om AI-systemen te trainen verdubbelt



Het gebruik van energie uit hernieuwbare bronnen vermindert de negatieve impact van taalmodellen op het klimaat. Load-shifts plannen rekenintensieve processen in op momenten dat er een overschot aan zonne- of windenergie beschikbaar is.

elke paar maanden,' zegt Ralf Herbrich, hoofd van de afdeling Artificial Intelligence and Sustainability van het Hasso Plattner Instituut (HPI). 'Maar het is eigenlijk onnodig dat modellen steeds groter worden om betere voorspellingen te kunnen doen.'

In het begin is het gebruik van overgeparametriseerde modellen makkelijker voor het maken van nauwkeurige voorspellingen. Vervolgens kunnen uit die voorspellingen weer betere trainingsvoorbeelden gegenereerd worden voor andere modellen. Die redden het met minder parameters, en werken met een vergelijkbare nauwkeurigheid. 'Veel studies hebben aangetoond dat dit werkt, en nu wordt het ook routinematig toegepast,' zegt Herbrich.

Om te illustreren dat de huidige modellen niet meer hoeven te groeien, vergelijkt Herbrich de 175 miljard parameters van GPT-3 met de structuur van het menselijk brein. 'Het brein bestaat uit 86 miljard neuronen en als je elk neuron beschouwt als een enkele eenheid van code, dan hebben de taalmodellen qua orde van grootte allang de mogelijkheden van de hersenen bereikt,' zegt de onderzoeker. 'We hebben niet veel meer nodig.'

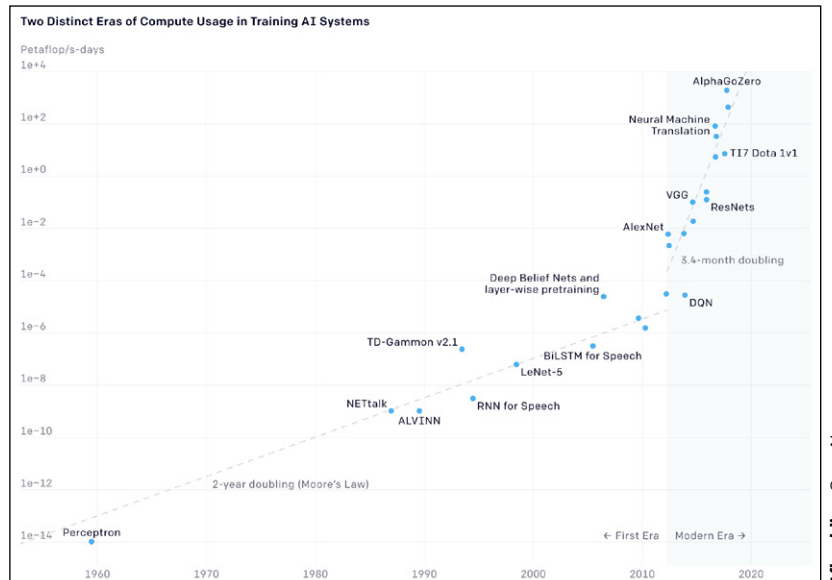
ONNAUWKEURIG IS BETER

Volgens Herbrich zijn de energiebehoefte en de bijbehorende kosten van een AI-systeem ook altijd een kwestie van economisch voordeel. 'In mijn ervaring is dat een heel natuurlijke nivellering, omdat geen enkel bedrijf op de lange termijn kan bestaan als het meer uitgeeft aan een berekening dan het verdient met het product dat het berekent.' Dat is een van de redenen waarom er momenteel intensief onderzoek wordt gedaan naar hoe de nauwkeurigheid van de rekenprocessen in een kunstmatig neuraal netwerk kan worden verlaagd zonder dat het eindresultaat merkbaar verstoord wordt.

'In het algemeen draaien AI-systemen constant op 32-bit floatingpoint-getallen, zelfs als ze uiteindelijk slechts tot één procent nauwkeurig kunnen voorspellen of er een hond of een kat op een afbeelding te zien is', merkt Herbrich op. Bovendien worden de getallen in elke laag van een diep neuraal netwerk herhaaldelijk vermenigvuldigd en opgeteld, waardoor onnauwkeurigheden zichzelf uitmiddelen. Grafische kaarten zijn simpelweg te nauwkeurig voor veel AI-toepassingen. 'Ze zijn precies en nauwkeurig, omdat we in de computerwetenschap nog niets anders nodig hebben gehad en daarom ook niets anders hebben ontwikkeld', aldus Herbrich.

Verschillende fabrikanten zijn bezig met het verbeteren van de manier waarop getallen worden gebruikt bij machine-learning. Vele kiezen voor een benadering waarbij ze verschillende formaten combineren, zoals floatingpoint-getallen met halve en enkele precisie (FP16 en FP32), en FP16 met 8-bit gehele getallen (INT8). Op die manier wordt geprobeerd om een balans te vinden tussen nauwkeurigheid en efficiëntie in machine-learning modellen.

'Nvidia doet al onderzoek naar dergelijke machines,' zegt Herbrich. 'En als uit empirisch onder-



Afbeelding OpenAI

Een nieuw tijdperk is aangebroken: volgens een onderzoek van OpenAI verdubbelde de rekenkracht die nodig is om AI-modellen te trainen tot 2012, in lijn met de Wet van Moore, nog ongeveer elke twee jaar. Nu verdubbelt dat elke drieënhalve maand.

zoek blijkt dat een bepaalde weergave van getallen energie-efficiënter is voor machine-learning, dan dat uiteindelijk leiden tot nieuwe hardware waarin dat is toegepast.' Tot die tijd zal artificiële intelligentie het echter moeten doen met de IEEE-754 standaard en de floatingpoint-getallen die daarbij horen.

De wetenschappers van het HPI werken al aan zogenaamde One-Bit-Networks om fundamentele kennis te vergaren. Die netwerken beschrijven de sterkte van de verbindingen tussen kunstmatige neuronen met behulp van slechts één bit in plaats van continue waarden. De betreffende bit bepaalt of het ene neuron het andere triggert of niet. Herbrich schat dat dit parallelle berekeningen met een factor 30 sneller kan maken. 'In bepaalde gevallen kan dat het energieverbruik met wel 95 procent verminderen, terwijl de nauwkeurigheid van de resultaten slechts met vijf procent afneemt.'

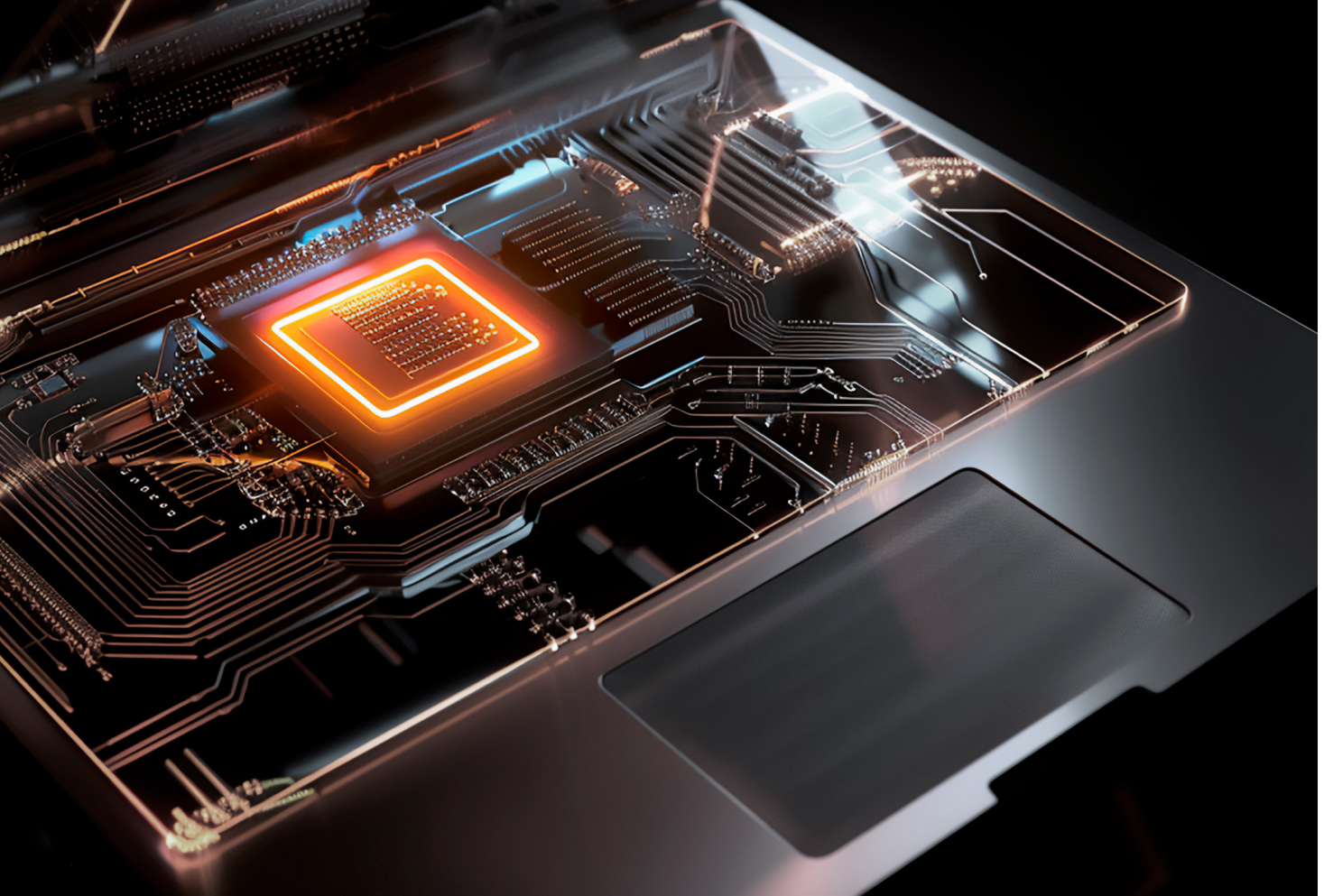
CONCLUSIE

De weg van fundamenteel onderzoek naar toepassing is lang. Maar zelfs als we vandaag de dag nog genoeg energie hebben voor artificiële intelligentie, zou het toenemende gebruik een waarschuwing moeten zijn. 'Steeds meer industrieën zullen AI gebruiken en integreren omdat het nu echt economische waarde heeft', waarschuwt Herbrich.

Daarom is het belangrijk om nu te beginnen met het een structureel besef van de kosten die gepaard gaan met de technologie. Het duurde immers ook meer dan vijf jaar van de eerste Google-modellen tot de doorbraak van ChatGPT.

'Het zal heus niet morgen zijn dat het licht uitgaat en we de keuze moeten maken tussen het aanzetten van een broodrooster of het laten draaien van ChatGPT.' Zegt Herbrich. 'Maar als we over vijf jaar nog steeds genoeg energie willen hebben, moeten we het probleem nu aanpakken.'

ct



Illustratie Midjourney, c't

OVERZICHT VAN MOBIELE CPU'S

Mobiele processors van AMD, Apple en Intel

Dankzij AI-versnellers, chiplet-structuren en hybride kernen rekenen moderne mobiele processors steeds sneller en efficiënter. Je raakt echter makkelijk het spoor bijster in het doolhof van complexe functies en cryptische modelaanduidingen. Wij helpen je de juiste chip te vinden voor jouw eisen wanneer je een laptop of mini-pc koopt.

Christian Hirsch en Alieke van Sommeren

Bij het kopen van een nieuwe laptop staan veel criteria op de checklist zoals grootte, gewicht, beeldschermresolutie en interfaces. De juiste mobiele processor is echter minstens zo belangrijk. Die bepaalt namelijk niet alleen de prestaties, maar ook de energiebehoefte en daarmee de accuduur, en hoe luid of stil de laptop is. Een verkeerde aankoop doen is zuur omdat processors vast in laptops en mini-pc's worden gesoldeerd en je ze later niet kunt vervangen.

Let daarom goed op bij de processoraanduiding bij het gewenste apparaat, zodat je geen miskoop doet met oudere en/of energievretende rommel. Het gaat minder om het hoogst mogelijke modelnummer

en meer om het aantal en type kernen, het thermische budget en de klokfrequenties.

Mobiele processors bevatten steeds meer extra functies zoals grafische, AI- en video-eenheden en controllers voor interfaces zoals PCI Express, SATA, Thunderbolt en USB. Dat bespaart kostbare ruimte voor extra chips in de steeds plattere apparaten, die fabrikanten liever gebruiken voor accu's. De mogelijkheden van een laptop zijn daarom steeds meer afhankelijk van de betreffende processor.

PERFORMANCE-KLASSEN

In tegenstelling tot desktopprocessors, waar het energieverbruik dankzij een verbinding met een stopcontact minder aandacht krijgt, zijn cpu's voor laptops en mini-pc's vooral geoptimaliseerd voor een laag energieverbruik. Daarom kunnen de verschillende series worden ingedeeld op basis van de zogenaamde Thermal Design Power (TDP, zie tabel). Dat geeft het continue verbruik onder volledige belasting aan waarvoor het koelsysteem van de laptop specifiek is ontworpen.

Die waarde is echter niet zo heel erg in beton gegoten omdat AMD en Intel apparaatfabrikanten flexi-

biliteit toestaan op dat punt, zodat de TDP binnen een bepaald bereik via de firmware te tweaken is. De Ryzen 7 8840U behoort bijvoorbeeld tot de 28W-klasse, wat af te leiden is aan de U aan het eind van de naamgeving. De configureerbare TDP (cTDP) kunnen laptopfabrikanten naar eigen inzicht instellen tussen 15 en 30 watt. Omdat de klokfrequentie onder volledige belasting op alle acht kernen wordt beperkt door de TDP, betekent dit dat twee laptops van verschillende fabrikanten op verschillende snelheden hun rekenwerk afhandelen ondanks dat ze dezelfde processor hebben. Het prestatieverschil kan oplopen tot meer dan 30 procent.

Hoewel dergelijke afwijkingen in de praktijk niet erg merkbaar zijn, vertoebelen ze wel de prestatieverschillen in grensgevallen: een hoog afgestelde Core i5 kan sneller rekenen dan een afgeknepen Core i7, die aanzienlijk duurder is.

AMD en Intel gebruiken ongeveer dezelfde naamgeving voor de prestatieklassen. De eerder genoemde U is van toepassing op de grote klasse van doorsnee mobiele cpu's met 15 tot 30 watt. Geen regel zonder uitzondering: in de 12e en 13e Core i-generatie, zoals de Core i7-1360P, staat de P voor dat TDP-niveau. De U was gereserveerd voor zwakkere chips met een maximale TDP van 15 watt.

Voor krachtigere apparaten, vooral de gaming-laptops met aparte grafische chips, gebruiken fabrikanten H-processors met 35 tot 54 watt. Veel H-chips gebruiken dezelfde halfgeleider-die als hun P/U broers en zussen. Door het hogere energiebudget kloppen de H-cpu's echter aanzienlijk sneller.

De HX-modellen zijn de toppers van AMD en Intel. De cpu-fabrikanten gebruiken daarvoor halfgeleider-

dies van desktopprocessors. Intel heeft bijvoorbeeld 24 cores in de Core i-13000HX. Bij de Ryzen 7045HX Dragon Range transplanteert AMD zelfs het chiplettrio van twee Core Complex-dies en de IO-die van de Ryzen 7000 Raphael naar de laptop. In tegenstelling tot desktopprocessors, solderen de pc-fabrikanten ze echter rechtstreeks op het moederbord.

CRYPTISCHE NAMEN

Processoraanduidingen voor mobiele chips zijn een nog groter mysterie dan voor desktopversies. Nog verwarrender dan de prestatieklassen zijn de processoraanduidingen, die soms zo inconsistent zijn dat zelfs wij diep in datasheets moeten duiken.

Apple bewijst hoe het op een klantvriendelijke manier kan. Bij diens ARM-chips, ook bekend als Apple Silicon, geeft het nummer de generatie aan. M3 is nieuwer dan M2, die nieuwer is dan M1. Daarnaast zijn er per generatie drie modelvarianten met een oplopend aantal cpu- en gpu-kernen in de volgorde M3, M3 Pro en M3 Max. De Ultra-varianten zijn alleen beschikbaar in de Mac Studio en Mac Pro desktop-pc's. Er zijn twee subversies van de M1 Pro, M2 Pro en M3 Pro, elk met een iets ander aantal cores.

Bij Intel identificeer je de cpu-generatie aan de hand van het eerste of de eerste twee cijfers. Tot eind 2023 was de Core i-familie actueel, waarvan in totaal 13 generaties verschenen. Intel gebruikt echter een nummering met vier of vijf cijfers, afhankelijk van de prestatieklasse: de Core i7-1360P behoort net als de Core i5-13600H tot de 13e generatie Raptor Lake.

Met de introductie van Meteor Lake eind 2023 heeft Intel Core i vervangen door Core Ultra en Core. De huidige mobiele cpu's met een chiplet-structuur

Huidige mobiele cpu's van AMD en Intel

Platform	Processorserie(s)	TDP	Kernen ¹	Gpu / shader-kernen	AI-unit	Procedé
AMD						
Hawk Point	Ryzen 8040HS	20 tot 54 W	6, 8	RDNA 3 / 256, 512, 768	✓	TSMC N4
Hawk Point	Ryzen 8040U	15 tot 30 W	1+3c, 2+4c, 6, 8	RDNA 3 / 256, 512, 768	✓	TSMC N4
Dragon Range	Ryzen 7045HX	45 tot 75 W	6, 8, 12, 16	RDNA 2 / 128	—	TSMC N5, TSMC N6
Phoenix	Ryzen 7040H, Ryzen 7040HS	35 tot 54 W	6, 8	RDNA 3 / 512, 768	✓	TSMC N4
Phoenix	Ryzen 7040U	15 tot 30 W	1+3c, 2+4c, 6, 8	RDNA 3 / 256, 512, 768	✓	TSMC N4
Rembrandt-R	Ryzen 7035HS	35 tot 54 W	6, 8	RDNA 2 / 384, 768	—	TSMC N6
Rembrandt-R	Ryzen 7035U	15 tot 28 W	4, 6, 8	RDNA 2 / 256, 384, 768	—	TSMC N6
Barcelo-R	Ryzen 7030U	15 W	4, 6, 8	GCN 5 / 256, 384, 512	—	TSMC N7
Mendocino	Ryzen 7020U	15 W	4	RDNA 2 / 128	—	TSMC N6
Rembrandt	Ryzen 6000H, Ryzen 6000HS, Ryzen 6000HX	35 W tot 45 W	6, 8	RDNA 2 / 384, 768	—	TSMC N6
Rembrandt	Ryzen 6000U	15 tot 28 W	6, 8	RDNA 2 / 384, 768	—	TSMC N6
Intel						
Meteor Lake-H	Core Ultra 100H	20 tot 65 W	4P+8E+2LP, 6P+8E+2LP	Xe-LPG / 896, 1024	✓	Intel 4, TSMC N5, TSMC N6
Meteor Lake-U	Core Ultra 100U	9 tot 28 W	2P+4E+2LP, 2P+8E+2LP	Xe-LPG / 384, 512	✓	Intel 4, TSMC N5, TSMC N6
Raptor Lake-HX	Core i-13000HX, Core i-14000HX	45 tot 55 W	6P+4E, 6P+8E, 8P+8E, 8P+12E, 8P+16E	Xe-LP / 128, 256	—	Intel 7
Raptor Lake-H	Core i-13000H, Core i-13000HK	35 tot 45 W	4P+4E, 4P+8E, 6P+4E, 6P+8E	Xe-LP / 384, 512, 640, 768	—	Intel 7
Raptor Lake-P	Core i-1300P	20 tot 28 W	4P+8E, 6P+8E	Xe-LP / 640, 768	—	Intel 7
Raptor Lake-U	Core i-1300U, U300, Core 100	12 tot 15 W	1P+4E, 2P+4E, 2P+8E	Xe-LP / 384, 512, 640, 768	—	Intel 7
Alder Lake-N	Core i3-N, N	6 tot 15 W	2E, 4E, 8E	Xe-LP / 128, 192, 256	—	Intel 7
Alder Lake-HX	Core i-12000HX	35 tot 45 W	4P+4E, 4P+8E, 6P+8E, 8P+8E	Xe-LP / 128, 256	—	Intel 7
Alder Lake-H	Core i-12000H	35 tot 45 W	4P+4E, 4P+8E, 6P+8E, 8P+8E	Xe-LP / 384, 512, 640, 768	—	Intel 7
Alder Lake-P	Core i-1200P	20 tot 28 W	2P+8E, 4P+8E, 6P+8E	Xe-LP / 512, 640, 768	—	Intel 7
Alder Lake-U	Core i-1200U, Pentium 8500, Celeron 7300	9 tot 15 W	1P+4E, 2P+4E, 2P+8E	Xe-LP / 384, 512, 640, 768	—	Intel 7

¹ c: compacte Zen4c-kernen

P: performance-kernen, E: efficiency-kernen, LP: Low-Power efficiency-kernen

behoren tot de Core Ultra 100U/H-serie, wat betekent dat ze slechts drie cijfers voor het modelnummer hebben. Voor goedkopere apparaten gebruikt de processorfabrikant de aanduiding Core 100 zonder Ultra. Dat zijn echter Raptor Lake Refresh-chips, die qua constructie identiek zijn aan de voorgangers van de 13e Core i-generatie en alleen iets hoger klokken.

Noch de productclassificatie Core i3, i5, i7 en Core Ultra 3, Ultra 5, Ultra 7, noch de modelaanduiding geven eenduidige informatie over technische eigenschappen zoals het aantal kernen, de klokfrequenties of hoe krachtig de geïntegreerde graphics zijn. De Core Ultra 7 155U en Core Ultra 7 155H verschillen bijvoorbeeld alleen in de laatste letter. De eerste cpu heeft echter maar twee performancekernen en een gpu met 512 shaderkernen, terwijl de tweede aanzienlijk krachtiger is met zes performancekernen en een gpu met 1024 shaderkernen.

Onze tip is daarom om altijd de productdatabase van Intel op ark.intel.com erbij te pakken voor de eigenschappen van de cpu. Die biedt ook een functie om de technische eigenschappen van verschillende processor types te vergelijken.

De processors in de laagste prijs- en prestatieklasse, waar voorheen de zwakkere mobiele cpu's van de Celeron Y/N- en Pentium Y/N-series onder vielen, moeten het bij Intel nu zonder merknamen stellen. De Alder Lake N-processors krijgen simpelweg een N plus een modelnummer, bijvoorbeeld N100. In tegenstelling tot de Core-processors missen ze de performancekernen (P-kernen) en bevatten ze alleen de zwakkere efficiency-kernen (E-kernen). Natuur-

lijk zijn ook daar uitzonderingen op: de topmodellen Core i3-N305 en Core i3-N300 mogen de Core i-merknaam dragen ondanks het ontbreken van P-cores.

Bij AMD gaf het eerste cijfer van het viercijferige modelnummer de generatie aan, dus Ryzen 4000, 5000 en 6000. Vanaf Ryzen 7000 staat het eerste cijfer bij de mobiele processors echter voor het jaar van verschijnen, dus 7 = 2023, 8 = 2024 enzovoort. De architectuurgeneratie staat nu op de voorlaatste positie: 2 = Zen 2, 3 = Zen 3 en Zen 3+, 4 = Zen 4.

De huidige cpu-kernen met Zen 4-architectuur zitten in mobiele chips uit de Ryzen 7040-, 7045- en 8040-serie. Voor budgetapparaten biedt AMD de Ryzen 7030 en 7035, die technisch nauw verwant zijn aan hun voorgangers Ryzen 5000 en 6000. Bij de Ryzen 5000U smokkelde de cpu-fabrikant de drie modellen Ryzen 3 5300U, Ryzen 5 5500U en Ryzen 7 5700U met oudere Zen 2-rekeneenheden naar binnen. Die worden ook gebruikt in de Ryzen 7020, die net als Intels N-serie alleen geschikt zijn voor laptops met 'iets meer power dan een typemachine'. Op products.amd.com staat een productdatabase voor Ryzen-cpu's, vergelijkbaar met die van Intel.

GEÏNTEGREERDE INTERFACES

De meeste kopers willen platte, lichte laptops met een lange accuduur. Moederborden worden steeds kleiner om ruimte te maken voor grotere accu's, ondanks de kleinere afmetingen van de behuizing. Mobiele processors nemen ook steeds meer functies over die voorheen door aparte chips werden uitgevoerd, in navolging van de cpu's van smartphones.

Integrated graphics

Op een paar uitzonderingen na bevatten alle moderne mobiele processors geïntegreerde grafische eenheden, ook wel geïntegreerde gpu's (IGP, ook: iGPU) genoemd. Dat geeft fabrikanten van laptops en mini-pc's de flexibiliteit om apparaten te bouwen met of zonder een extra grafische chip. AMD verwijst bijvoorbeeld naar zijn IGP's als Radeon 740M, 760M en 780M, terwijl Intel de termen UHD, Iris Xe en Arc gebruikt zonder modelnummers.

Qua structuur en architectuur zijn mobiele IGP's identiek aan hun grotere broers en zussen wat 3D- en rekenversnellers betreft, maar ze hebben veel minder rekeneenheden en moeten ook de relatief smalle geheugeninterface delen met de cpu-kernen. Daardoor zijn de 3D-prestaties vaak hooguit voldoende voor 3D-weergaven in kaartdiensten in de browser, casual games en bouwsimulaties waarbij het geen vereiste is om zo veel mogelijk fps eruit te persen [3].

De topvarianten met 700 en meer shadercores halen de benodigde framerate van 60 fps bij volledige hd-resolutie

De 3D-prestaties van de meeste iGPU's op mobiele processors zijn vaak alleen voldoende voor casual games zoals The Sims 4. Gamers moeten dus kiezen voor een laptop met een dedicated krachtige grafische chip.



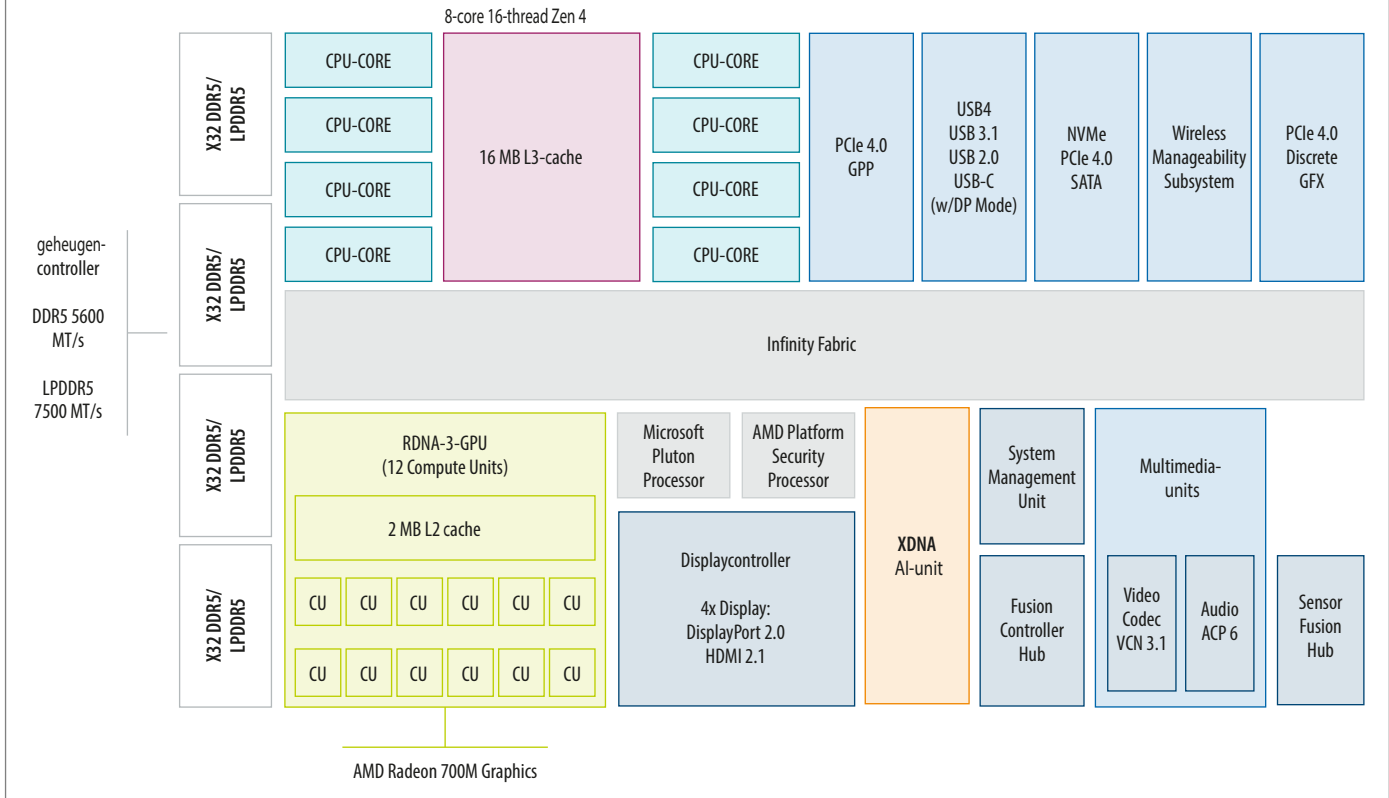
en middelhoge tot hoge kwaliteitsinstellingen, in ieder geval voor oudere eSports-titels. Apples M-serie in de Pro- en Max-varianten is een uitzondering. Qua aantal shaders en geheugenaansluiting houden de IGP's van Apple gelijke tred met de krachtige gaming console-SoC's van de Playstation 5 en Xbox Series X/S.

De Intel Core i, Core Ultra en Ryzen display-engines kunnen elk vier high-res monitoren tegelijk aansturen, dus drie ex-

tra naast het ingebouwde beeldscherm. Hoeveel aansluitingen de fabrikanten naar buiten toe beschikbaar maken als DisplayPort, HDMI en USB-C/Thunderbolt hangt echter af van het betreffende apparaat. Mobiele processors bevatten ook video-eenheden die de cpu-kernen ontlasten bij het coderen en decoderen van gangbare videoformaten zoals H.264/AVC, H.265/HEVC, VP9 en AV1, waardoor de accuduur verlengd wordt.

Function blocks bij de Ryzen 7040

Moderne mobiele processors hebben veel meer functies dan alleen cpu-kernen en grafische eenheden. Naast geïntegreerde microcontrollers voor beveiliging (Platform Security Processor & Pluton) en gespecialiseerde eenheden voor video- en audioberekeningen, hebben ze ook I/O-controllers voor PCI Express, USB en SATA. Dat bespaart ruimte en energie voor een aparte chipset. Een nieuwe functie van de Ryzen 7040 is de XDNA AI-eenheid, ook bekend als de Neural Processing Unit (NPU) of Ryzen AI, die is ontworpen om de cpu-kernen te ontlasten van die taken.



Chipsets als aanvulling op de cpu, voor extra PCIe-lanes en SATA- en usb-poorten, bestaan al jaren niet meer, behalve voor dikke gaminglaptops en mobiele workstations. De snelle en flexibele Thunderbolt-interface maakt al vier chipgeneraties lang deel uit van Intels mobiele cpu's. Bovendien zit het digitale circuitgedeelte van wifi nu in de processor, terwijl de hoogfrequente module extern blijft.

Het besturingssysteem in een moderne laptop belandt meestal op een M.2-ssd, die via vier PCIe-lanes met de cpu is verbonden, of de flashopslag zit rechtstreeks op het moederbord gesoldeerd.

SATA-poorten voor optische stations en 2,5-inch schijven sterven uit. In plaats daarvan neemt het belang van USB-C toe. Daarmee zet je niet alleen data over, maar ook DisplayPort-signalen voor externe monitors in Alt-modus en het laadt de accu van je laptop op via Power Delivery.

Thunderbolt 3 en 4 maken de bovengenoemde functies verplicht en kunnen ook PCIe-signalen verzenden via USB-C om bijvoorbeeld snel en makkelijk externe grafische kaarten aan te sluiten. Bij USB4 is, ondanks de Thunderbolt-relatie, veel daarvan (helaas) alleen optioneel [1].

Naast I/O-functies hebben mobiele processors meestal ook een gpu (zie kader), die voor veel toepassingen voldoet. Krachtigere, apart gesoldeerde grafi-

sche chips met eigen geheugen zijn de moeite waard voor 3D-games, creatieve toepassingen zoals AI en videobewerking, maar ook voor professionele software zoals CAD en wetenschappelijke berekeningen. Specialisatie zie je ook op minder prominente gebieden. AMD integreert een audiocoprocessor in Ryzen-processors, die de cpu-kernen ontlast van audio-effecten. Intel rust zijn mobiele cpu's uit met een zuinige beeldverwerkingseenheid (IPU), bijvoorbeeld om ruis uit webcambeelden te verwijderen.

AI-VERSNELLERS

Artificiële intelligentie is momenteel een toverwoord. Processorfabrikanten willen ook een graantje meepikken van de AI-hype en adverteren hun cpu's met dergelijke functies. Apple loopt daarin voorop, want de eerste generatie van de M-serie heeft al een Neural Processing Unit (NPU). Die voert de belangrijkste berekeningen uit in AI-toepassingen met datatypes met lage precisie en beheert 11 biljoen tensorberekeningen per seconde (TOPS) met 8-bit gehele getallen (INT8).

Apple was AMD en Intel voor met AI-hardware omdat de M1 ARM-processor een verdere ontwikkeling is van de Apple A14 smartphone-SoC's. Die hebben sinds 2017 AI-versnellers (Apple A11). De AI-eenheid in de M3 tikt 18 TOPS aan.

Opbouw van een Core Ultra 100 Meteor Lake

Intel vertrouwt op een chiplet-ontwerp voor de huidige Core Ultra 100 Meteor Lake-serie mobiele processors. De verschillende tiles worden niet alleen zelf geproduceerd, maar ook door TSMC. Ook hebben ze verschillende structuurgroottes. De SoC-tile bevat twee energiezuinige kernen, en de media- en display-engine. Daardoor kan de processor de cpu en gpu-tile bij lage belasting volledig loskoppelen van de voeding, bijvoorbeeld bij het afspelen van een video. De chiplets communiceren met elkaar via de onderliggende base-tile, die verbonden is met behulp van Foveros-technologie. De afstand tussen de soldeerpunten is daarbij slechts 36 micrometer.



Bij x86-processors was AMD de eerste. De fabrikant adverteert de Ryzen 7040 die begin 2023 werd gepresenteerd als Ryzen AI. De NPU maakt gebruik van de XDNA-rekeneenheden van de in 2022 overgenomen FPGA-fabrikant Xilinx, met een prestatie van 10 TOPS. De opvolgers (Ryzen 8040) zullen naar verwachting 16 TOPS halen.

De NPU van Intels Core Ultra zit met 10 TOPS op hetzelfde niveau als de Ryzen 7040. Fabrikanten adverteren vaak echter met hogere waarden van meer dan 30 TOPS voor hun processors, omdat ze de rekensnelheid van cpu, gpu en NPU bij elkaar optellen. Dat is correct als de AI-berekeningen draaien op alle drie tegelijk. De gpu is meestal sneller dan de NPU, maar verbruikt onevenredig veel energie. In de praktijk zijn er nog maar weinig toepassingen die de NPU's kunnen aanspreken. Windows 11 bevat Windows Studio Effects, dat de webcamstream tijdens videoconferenties analyseert met behulp van beeldherkenning en de achtergrond vervaagt.

HYBRIDE KERNEN

Steeds meer mobiele processors hebben verschillende typen cpu-kernen, de eerder genoemde P- en E-kernen. AMD en Intel hebben dat afgekeken van SoC's voor smartphones, waar energiebesparing de hoogste prioriteit heeft en hybride ontwerpen al lang gebruikelijk zijn. E-cores zijn niet alleen efficiënter en zwakker dan P-cores, maar nemen ook minder ruimte in op een chip, zodat er meer op passen.

De P-cores zijn ontworpen om veel instructies parallel uit te voeren en bieden een hoge rekenkracht voor vectorbewerkingen met 128- en 256-bit instructies. De E-cores hebben dezelfde functies, maar veel minder parallele eenheden. Het doel is om de energievervlindende P-cores alleen kort op te starten wanneer gebruikersinput dat vereist en ze daarna direct weer in de slaapstand te zetten, zodat de

achtergrondtoepassingen door de zuinigere E-cores kunnen worden afgehandeld. Beide kerntypes werken onder volledige belasting samen voor veeleisende toepassingen.

Apple kan de afzonderlijke software-threads efficiënter verdelen over de verschillende cpu-kernen omdat het besturingssysteem en de hardware van hetzelfde bedrijf komen. Intel bouwt in Core-processors vanaf de 12e generatie de zogenaamde Thread Director in, die moderne besturingssystemen zoals Windows 11 en Linux vanaf kernel 5.18 ondersteunen bij het verdelen van de threads [2].

Vanaf de Core Ultra bouwt Intel ook een derde core-klasse in, twee zogeheten low-power E-cores, die zich in de SoC-chiplet bevinden. Die wordt bij lage belasting dan volledig uitgeschakeld, maar dat verhoogt de complexiteit. AMD pakt het bij de drie zwakste Ryzen 7040U-processors anders aan en vervangt enkele Zen 4-cores door compactere varianten (Zen 4c), die in tegenstelling tot bij Apple en Intel dezelfde functionele eenheden hebben als de grotere. Ze zijn echter ontworpen voor lagere klokfrequenties en beslaan minder chipruimte. Door de lagere kloksnelheid vergen ze ook een lager voltage en minder energie.

Wat betreft het werkgeheugen kiezen steeds meer laptopfabrikanten voor ruimtebesparing door het LPDDR5X RAM vast te solderen in plaats van DDR5 SO-DIMM-poorten te installeren. Moderne mobiele processors kunnen daarom beide RAM-types aansturen. LPDDR5X heeft kortere signaalpaden nodig en bereikt daardoor hogere klokfrequenties.

Apple gaat nog een stap verder met zijn M-processors en integreert de geheugenchips daarin. Terwijl AMD en Intel meestal twee 64-bit geheugenkanalen aansluiten, dus in totaal 128 bit, heeft Apple er tot maximaal acht (512 bit). Dat verhoogt de doorvoersnelheid van circa 100 GB/s tot wel 400 GB/s. Dat komt vooral de 3D- en AI-prestaties van de geïntegreerde gpu ten goede.

SNELLE CHIPS

De cpu-prestaties zijn de afgelopen jaren gestaag toegenomen. Enerzijds zijn singlethread-prestaties, die belangrijk zijn voor kantoortoepassingen en web surfen, toegenomen dankzij sterkere P-cores en hogere klokfrequenties van meer dan 5 GHz. De huidige mobiele chips halen een uitstekende 1500 punten en meer met één thread bij de gratis renderbenchmark Cinebench R23, wat meer dan voldoende is voor alle toepassingsscenario's (zie de tabel). De M3-serie van Apple is de onbetwiste leider met bijna 2000 punten.

Bij rendering, videobewerking en beeldverwerking rekenen verschillende threads vaak parallel en profiteren daarom van veel cores. De prestaties zijn sterk afhankelijk van het thermische budget van de processor. Als je vaak met dergelijke toepassingen werkt, kun je het beste voor een mobiele processor in de 28W-klasse gaan met minstens 12 threads. Dat kan een processor zijn met zes cores en simultane multithreading (SMT) of een hybride chip bestaande uit twee P-cores en acht E-cores. Dergelijke cpu's

halen 9000 punten en meer bij de multithreaded-benchmark van Cinebench R23.

Zoals te zien is in de tabel, hoeft het niet altijd een gloednieuwe processor te zijn. Als je een laptop van de vorige generatie met een Core i-1200/12000 of Ryzen 6000 koopt, kun je een paar euro besparen zonder op prestaties in te boeten. Bijna alle processors hebben een turbo en kunnen hun TDP korte tijd overschrijden. Cpu-fabrikanten maken gebruik van de thermische traagheid van het koelsysteem, wat zorgt voor een merkbare snelheidsverhoging bij het gebruik van interactieve programma's.

In tegenstelling tot bij desktop-pc's kunnen de efficiëntie en prestaties van mobiele cpu's niet algemeen worden bepaald omdat dit sterk afhangt van het apparaat in kwestie. De processors in laptops hebben vaak een lagere vermogenslimiet dan die in mini-pc's, waar meer ruimte is voor grotere koelers. Het is daarom zinvol om daar testrapporten voor te lezen en te vergelijken.

VOORUITZICHTEN

Het innovatietempo bij mobiele processors ligt momenteel erg hoog. Met zijn M3 bewijst Apple dat een combinatie van krachtige kernen, krachtige geïntegreerde graphics en AI-eenheden mogelijk is met een matige energiebehoefte. Intel richt zich momenteel sterk op chiplet-ontwerpen in de mobiele sector. Core Ultra 200 Arrow Lake staat gepland voor de tweede helft van dit jaar. Er gaan geruchten dat afgezien van de Base Tile alle andere chips door TSMC zullen worden geproduceerd. Dat is een noviteit voor Intel, waar tot voor kort alles uit de eigen fabrieken moest komen – wat leidde tot jarenlange vertragingen.

Met Lunar Lake heeft Intel een tweede ijzer in het vuur. Voor die cpu's (voor zeer platte, dure laptops) heeft Intel waarschijnlijk gekeken naar Apple Sili-

con, want het LPDDR5X-geheugen is in de processor-package verwerkt. Dat maakt hogere snelheden mogelijk met kleinere afmetingen en lagere energie-eisen. Lunar Lake moet dit jaar verschijnen.

AMD lanceert binnenkort een nieuwe cpu-architectuur, Zen 5. Die zal niet alleen worden gebruikt in desktop- en serverprocessors, maar ook in mobiele chips. De laptop-cpu's, ook wel bekend als Strix Point, zullen vermoedelijk Ryzen 8050 worden genoemd en krijgen naast een krachtigere AI-eenheid ook een modernere gpu uit de RDNA 3.5-generatie.

De krachtigere Strix Halo-chip is bedoeld om de grafische kaart overbodig te maken in gaming-laptops. AMD combineert naar verluidt 16 Zen 5-kernen met krachtige RDNA 3.5 grafische kaarten met 2560 shaderkernen. Daarvoor is echter een bredere geheugeninterface nodig dan de gebruikelijke twee DDR5-kanalen met elk 64 bit. Het ontwerp van de Strix Halo lijkt daarom erg op de combinatie-processors die AMD heeft ontwikkeld voor gameconsoles zoals de Playstation 5 en Xbox Series S/X.

Last but not least bereidt Qualcomm zich voor om marktaandeel af te snoepen van de gevestigde fabrikanten. Qualcomm wil deze zomer in de aanval gaan met de snelle Snapdragon X Elite. Die heeft 12 kernen met de naam Oryon, waarvan de prestaties op hetzelfde niveau als Apples M3 zitten. Hoe succesvol de Snapdragon X Elite zal zijn, hangt echter met name af van hoeveel laptopfabrikanten bereid zijn om die cpu in hun apparaten te stoppen.

ct



www.ct.nl/softlink/2407064

Literatuur

- [1] Christof Windeck en Marco den Teuling, Supersnel USB: hoe USB 3.2 Gen 2x2, USB4 en Thunderbolt presteren, c't 12/2022, p.60
- [2] Christian Hirsch en Noud van Kruijsbergen, Hybride processors onder Windows 10 en 11 optimaal gebruiken, c't 11/2022, p.100
- [3] Christian Hirsch en Marco den Teuling, 3D- en videofuncties van de graphics van Core i en Ryzen, c't 10/2021, p.52

Performance van huidige mobiele cpu's

Processor	Fabrikant	Kernen / threads	Max. snelheid	TDP ¹	Cinebench R23 1T	Cinebench R23 MT	Cinebench R24 1T	Cinebench R24 MT
					beter ►	beter ►	beter ►	beter ►
M3 Max	Apple	12P+4E / 16	4,05 GHz	78 W	1885	23811	141	1483
Snapdragon X Elite ²	Qualcomm	12P / 12	4,3 GHz	g.o.	–	–	133	1149
Ryzen 7 7840HS	AMD	8P / 16	5,1 GHz	45 W	1676	15540	101	906
M3 Pro	Apple	6P+6E / 12	4,05 GHz	27 W	1980	15128	145	1005
Core i9-13900H	Intel	6P+8E / 20	5,4 GHz	45 W	1965	14504	113	723
Ryzen 7 7840U	AMD	8P / 16	5,1 GHz	25 W	1735	13810	105	782
M3	Apple	4P+4E / 8	4,05 GHz	20 W	1903	10479	141	746
Ryzen 7 7735U	AMD	8P / 16	4,75 GHz	28 W	1515	10392	–	–
Core Ultra 7 155H	Intel	6P+8E+2LP / 22	4,8 GHz	28 W	1745	10311	104	574
Core i5-1345U	Intel	2P+8E / 12	4,7 GHz	15 W	1544	9711	99	362
Ryzen 5 7540U	AMD	6P / 12	4,9 GHz	25 W	1536	9571	93	535
Core i7-1360P	Intel	4P+8E / 16	5,0 GHz	28 W	1684	9192	99	487
Core i7-1260P	Intel	4P+8E / 16	4,7 GHz	28 W	1675	9121	–	–
Ryzen 7 7730U	AMD	8P / 16	4,5 GHz	15 W	1469	9055	86	522
Ryzen 5 Pro 6650U	AMD	8P / 16	4,5 GHz	28 W	1462	8128	–	–
Ryzen 3 7320U	AMD	4P / 8	4,1 GHz	15 W	1111	4944	–	–
Core i3-N305	Intel	8E / 8	3,8 GHz	15 W	990	4636	–	–
SQ3 (Snapdragon 8CX Gen3)	Qualcomm	4P+4E / 8	3,0 GHz	15 W	602	3665	–	–
N100	Intel	4E / 4	3,4 GHz	6 W	814	2416	59	155

¹ TDP: Thermal Design Power, de individuele waarde hangt af van het apparaat, tijdens het korte turbowindow is hoger verbruik mogelijk ² prototype g.o. geen opgave – niet gemeten



EASY-3D-PRINT

Prusa MK4 en Bambu Lab P1S 3D-printers vergeleken

Je kunt bij een 3D-printer veel verkeerd instellen: de bedhoogte, nozzle-temperatuur, versnellingen, aanvoersnelheid en E-steps. Maar niet bij deze printers, die alle lastige waarden zelf bepalen en instellen. Daarmee wordt 3D-printen echt iets voor iedereen.

Johannes Börnsen, Pina Merkert en Marco den Teuling

De pen grijpt in het sleufgat en de spiraalveer drukt beide delen in de groef. Natuurlijk, waarom heb ik daar niet meteen aan gedacht? Kan het prototype nog gemaakt worden voor de deadline van 12 uur? Zeker, want we hebben twee 3D-printers van de laatste generatie. Die helpen niet alleen een hoop beginners, maar ook professionals hun doel twee keer zo snel te bereiken.

3D-printers produceren onderdelen sneller dan je ze met de hand zou kunnen maken. Je hebt geen werkplaats nodig en de precisie is meestal ook beter. De onderdelen moeten van kunststof zijn, maar omdat kunststoffen extreem veelzijdig zijn, is dat geen grote beperking. Wat wel jarenlang een obstakel was, was dat je uren aan die machines moest zitten prutsen tot ze überhaupt goed werkten. Het vergde veel kennis van de technologie [1]. Dat was voor c't-lezers wellicht minder een probleem, maar behalve aan werktuigbouwkundigen en technici waren 3D-printers verder aan niemand aan te bevelen.

De twee moderne printers die we hier testen moeten dat probleem verhelpen. De Prusa MK4 en de Bambu Lab P1S automatiseren bijna alles wat je fout kunt doen bij een 3D-printer. Je hoeft niet langer te weten waarom wat ze doen klopt. Gecombineerd met duidelijke instructies en geavanceerde software, krijgen beginners en professionals apparaten die meestal gewoonweg werken.

Dat geldt echter alleen voor goed ontworpen printmodellen en de makkelijke grondstof PLA. We hebben beide machines tot het uiterste gedreven qua afdrukkwaliteit. Als je wilt weten wanneer beide machines niets anders dan spaghetti produceren, hoef je alleen verder te lezen.

FUNDAMENTEEL VERSCHILLENDE

De Prusa MK4, die als zelfbouwpakket net geen 900 euro kost, en de Bambu Lab P1S van 750 euro verschillen niet alleen qua prijs, maar ook het mechanische principe, de snelheid en de werking zijn totaal verschillend.

De Prusa is de vierde versie van een ontwerp dat gebaseerd is de legendarische RepRap (Replicating Rapid Prototyper), de eerste open-hardware 3D-printer. Het printbed beweegt naar voren en naar achteren, de kop van links naar rechts en de assen waarop hij rolt kunnen omhoog bewegen. 3D-printers van dat type worden meestal bedslingers genoemd. Het voordeel van dat ontwerp ligt in het feit dat het frame uit vlakke delen kan bestaan omdat er geen zijdelingse krachten optreden tijdens de beweging. Omdat de Prusa alleen het slanke frame vereist, heeft hij geen behuizing. Die zou uit veel extra onderdelen moeten bestaan en, althans voor PLA, heeft een 3D-printer meestal geen behuizing nodig.

Bambu Lab betrad in 2022 de markt voor 3D-printers pas. Sinds kort heeft het bedrijf ook bedslingers [2], maar de meeste printers van het merk hebben een andere opbouw. De P1S gebruikt het CoreXY-principe om de printkop met lange riemen zijwaarts en heen en weer te bewegen. Twee trapeziumvormige spindels bewegen het hele printbed langzaam naar beneden. CoreXY vereist een stijf frame bovenaan voor de motoren en riemrollers. De Z-as moet onder het bed passen. Daardoor omvat het frame, dat belangrijk is voor de stabiliteit, al bijna alle onderdelen voor een behuizing. De printer is ook verkrijgbaar onder de naam P1P zonder behuizingswanden. Alleen al de stofbescherming en toegevoegde afzuiging zijn de

meerprijs echter waard. Bovendien resulteert het in een warme printruimte zonder tocht, wat eigenlijk wel nodig is voor kunststoffen zoals PETG, ASA, ABS, CPE of nylon. Daarover later meer.

OVEREENKOMSTEN

De printers hebben echter ook enkele dingen gemeen: ze hebben allebei een verwarmd printbed dat temperaturen tot 120 °C (Prusa) of tot 100 °C (Bambu Lab) kan bereiken. Het printbed is een veerstalen plaat bedekt met de kunststof PEI. Daarvan kunnen prints zonder spatel verwijderd worden. Een beetje heen en weer buigen van de plaat is meestal voldoende. Beide maken gebruik van direct-drive extruders, waarbij een motor direct op de kop het filament aanvoert. Dat ontwerp zorgt voor een zeer korte afstand tussen het aanvoerwiel en de nozzle (spuitmond), waardoor ze vrij goed overweg kunnen met flexibele kunststoffen zoals TPU. Beide hebben een volledig metalen hot-end, waarvoor de fabrikanten een maximumtemperatuur opgeven van 290 °C (Prusa) en 300 °C (Bambu Lab). Omdat de hot-ends geen teflon bevatten in het verhitte gedeelte, komen er ondanks temperaturen boven 250 °C geen giftige fluorverbindingen vrij uit het teflon. Beide printers herkennen wanneer de filamentrol leeg raakt en beide kunnen na een stroomstoring doorgaan met printen.

De slicer-software, die instructies voor de printer berekent vanuit een 3D-model in een STL- of 3MF-bestand, lijkt ook erg op elkaar. Zo'n programma splitst het model op in lagen van 0,08 tot 0,3 millimeter dikte (instelbaar) en berekent een goed pad voor de nozzle om te volgen. Prusa is jaren geleden begonnen met een fork van de opensource software Slic3r en heeft de opensource PrusaSlicer ontwikkeld tot de populairste slicer naast concurrent Cura (onderhouden door printerfabrikant UltiMaker).

Bambu Lab heeft weer een fork van PrusaSlicer gemaakt met de naam Bambu Studio, de standaardinstellingen voor de Prusa-printers vervangen door eigen machines en verschillende eigen functies toegevoegd. Beide programma's zijn zelf opensource en er zijn ook weer forks van beide – SuperSlicer is een fork van PrusaSlicer en OrcaSlicer van BambuStudio.

BEDIENING

Als je de Prusa bedient, merk je dat het bedrijf een van pioniers is op het gebied van 3D-printen. De gedrukte instructies zijn uitgebreid en geïllustreerd en de website vult ze aan met video's over installeren, onderhoud en bediening. Technische details worden goed uitgelegd en niet verborgen, zoals helaas vaak wel het geval is bij andere producten.

Prusa vraagt van haar klanten geen technische voorkennis, maar wel de interesse en bereidheid om de instructies te lezen. Dat is bijvoorbeeld merkbaar bij het instellen van de wifiverbinding. Daarvoor moet je een tekstbestand op een usb-stick bewerken. De instructies leggen dat zo gedetailleerd uit dat iedereen dat wel kan doen. Maar die manier van werken is ver verwijderd van apps die volledig intuïtief zijn.



De Prusa MK4 is een bedslinger, waarbij het printbed met werkstuk over de Y-as naar voor of achter beweegt. Het ontwerp maakt een open constructie mogelijk, wat bij bepaalde materialen nadelig is.

Sinds versie 2.7 kan PrusaSlicer dat bestand voor je maken.

De intuïtieve Bambu Lab neemt een eenvoudiger route en biedt een app die echt gebruikt kan worden met een beetje kennis van 3D-printen – zelfs zonder instructies. De app is ook veel mooier en duidelijker dan het pijltjestoetsdisplay op de printer.

We vonden de gebruiksvriendelijkheid van de Bambu Lab wat verfijnder. Dat komt deels echter ook door de privacyvriendelijke standaardinstelling op de Prusa. Hij maakt standaard geen verbinding met een netwerk en dat hoeft ook niet, want je bewaart de printopdrachten met PrusaSlicer op de bijgeleverde usb-stick en steekt die in de printer. Na een druk op de draaiknop begint de printer.



De Bambu Lab P1S is een CoreXY-printer. De motoren voor de X- en Y-as zijn bevestigd aan het frame, het printbed beweegt alleen verticaal. Dat maakt veel snellere prints mogelijk dan bij de Prusa.



Het display van de Prusa MK4 toont een overzichtelijk menu dat je bedient met de draaiknop rechts. Het printen vanaf usb-stick met de knop starten vonden we het eenvoudigst. Er is ook een webinterface.

Als je wifi activeert (alleen 2,4 GHz), kun je Prusa-Link benaderen vanuit je thuisnetwerk. Dat gaat met een webinterface die informatie toont die anders op het display zou staan. Je kunt de usb-stick dan in de printer laten zitten en bestanden via het netwerk uploaden. Dat gaat ook makkelijk via een knop in Prusa-Slicer. Maar de gegevensoverdracht is zo langzaam dat het voor grote prints sneller is om ze via de usb-stick naar de printer over te zetten.

Je kunt ook PrusaConnect activeren. Voor het instellen toont de printer een qr-code op het display, die je alleen met je smartphone hoeft te scannen. Prusa Connect is een cloudservice waarmee je vanaf elke locatie toegang tot de printer hebt. De gegevens lopen daarbij via een Prusa-server.

Als je een MK4 hebt, heb je waarschijnlijk geen probleem met het feit dat Prusa theoretisch kan zien wat de printer produceert. Zoals meestal het geval is bij clouddiensten, heeft het bedrijf waarschijnlijk wel wat beters te doen dan gebruikersgegevens te bekijken. Het is echter een goed teken dat Prusa voorrang geeft aan gegevensbescherming en je de cloudfunctie optioneel zelf moet activeren. Eigenlijk zou dat de standaardinstelling voor alle producten moeten zijn.



De Bambu Lab P1S heeft een klein maar bruikbaar display. We gaven in de praktijk de voorkeur aan de uitstekende app van de fabrikant voor het bedienen van de printer.

Bij de Bambu Lab P1S kunnen printgegevens ook worden overgebracht naar de printer, op een geheugenkaart, en gestart met de kleine pijltjestoetsen op het display. Je kunt echter zien dat Bambu Lab dat anders benadert: printer en slicer worden standaard gekoppeld aan een account bij Bambu Lab. De slicer toont dan alle huidige machineparameters van de printer en stuurt printtaken via het netwerk naar de printer, die ze zonder verdere actie start. Als de printer zich op een andere locatie bevindt, kun je de voortgang van het afdrucken volgen via een camera in de printruimte. Die stuurt om de twee seconden een beeld naar de slicer.

MULTI-MATERIAAL

Als de P1S is uitgerust met het optioneel verkrijgbare Automatic Material System (AMS), kun je met maximaal vier filamenten tegelijk printen zonder dat de filamentrol handmatig verwisseld hoeft te worden. De printer kan de kunststofdraad zelfstandig naar de printkop leiden en weer intrekken wanneer je van kleur of materiaal wisselt. Dat is bijvoorbeeld praktisch om opschriften in een andere kleur te kunnen printen. Je kunt daarmee ook makkelijk te verwijderen steunmateriaal gebruiken. De printer wisselt voor de laatste lagen tussen de steunen en het werkstuk dan naar in water oplosbaar PVA-filament. Dat is makkelijker te verwijderen van de voltooide print en resulteert in gladdere onderzijden op de ondersteunde plekken.

In de praktijk werkte de AMS in de overgrote meerderheid van de gevallen zonder problemen. Af en toe was de kracht echter niet voldoende om het materiaal betrouwbaar uit de printkop te trekken. Na een korte handmatige ingreep konden we dan verder gaan met printen. Na elke wisseling van filament moet de printer het oude filament uit de nozzle verwijderen en een paar gram materiaal door de hete spuitmond duwen totdat alleen het nieuwe filament volgt. Dat proces produceert bij elke wisseling overtollig plastic, dat als afval uit een opening aan de achterkant valt. Bovendien duurt elke wisseling ongeveer anderhalve minuut. Bij prints waarbij de AMS vaak wisselt tussen verschillende filamenten, kan de printtijd snel oplopen en er aanzienlijke hoeveelheid afval ontstaan.

Prusa heeft een systeem ontwikkeld met de naam Multi-Material-Upgrade 3 (MMU3), dat veel lijkt op de AMS. Die upgrade werkt al met de voorganger MK3S, maar met de MK4 waren er problemen door een iets andere geometrie van de nozzle. Daarom kon Prusa het MMU3-systeem voor de MK4 nog niet leveren, maar ondertussen is het wel beschikbaar.

PLA VOOR BEGINNERS

Met het standaardmateriaal PLA zijn beide printers zeer beginnersvriendelijk. De vooraf ingestelde slicer-profielen werken voor de overgrote meerderheid van de modellen die online te vinden zijn zonder aanpassingen. De printers kalibreren zichzelf automatisch zodat iedereen, ongeacht het ervaringsniveau,

in een paar uur prints van uitstekende kwaliteit van de printplaat kan halen. Als je je eigen ontwerpen maakt, moet je zoals gewoonlijk letten op overhangen en als die niet te vermijden zijn supports activeren in de slicer.

Met PETG zagen we bij de test echter al de eerste problemen in de vorm van opkrullende hoeken. Met ASA moesten we op de Prusa tientallen pogingen doen om de eerste testprints te maken zonder dat de modellen te vroeg loskwamen van de printplaat. Het onderliggende probleem is wat de 3D-print-community warping noemt. Dat wordt veroorzaakt door thermische spanningen in het object, die vooral scherpe hoeken van de printplaat omhoog doen komen en in het ergste geval zelfs scheuren veroorzaken.

PLA trekt nauwelijks krom, maar vooral nylon, ABS en zijn variant ASA hebben daar veel last van. Het materiaal PETG zit er tussenin. Warping wordt erger wanneer het temperatuurverschil tussen net geprinte en al afgekoelde lagen groter is. Daarom zal een warme printruimte, zoals in de behuizing van de Bambu Lab, het probleem verminderen. Maar zelfs daar komen prints met weinig contactoppervlak met de printplaat soms los.

Net als Prusa levert Bambu Lab een lijmstift waarmee de printplaat voor het printen kan worden bestreken. Dat hielp in veel gevallen, met ASA en ABS hadden we geen problemen met een net schoongemaakte printplaat en een opgedroogde laag haarlak (extra sterke fixatie).

Met de Prusa hebben we PETG zoals aanbevolen geprint op een gesatineerde printplaat en ASA op een printplaat met structuur. Op oppervlakken met structuur is de hechting aanzienlijk beter als de nozzle het plastic van de eerste laag goed in alle groefjes duwt. Dat gebeurde duidelijk niet met de automatisch ingestelde bedhoogte op de Prusa MK4. Er is echter een truc die kan helpen: als je de draaiknop minimaal twee seconden ingedrukt houdt nadat een print gestart is, opent een geheim menu waarin de afstand tussen nozzle en printplaat kan worden aangepast.

Met een 0,02 tot 0,03 millimeter dieper ingestelde nozzle bereikten we een aanzienlijk betere hechting zonder dat de onderste laag zichtbaar naar buiten uitliep. Ondanks die instelling raden we aan om de MK4 zonder behuizing alleen te gebruiken voor PLA en TPU. We haalden al betere resultaten met een eenvoudige behuizing van textiel.

CONCLUSIE

Zowel de Prusa MK4 als de Bambu Lab P1S vertonen niet de gebruikelijke problemen van 3D-printers zoals verstopte nozzles, vervormd of gebroken filament. Beide ontwerpen zijn zeer onderhoudsarm: schroeven hoeven pas na honderden bedrijfsuren te worden aangedraaid en de lagers gaan, als ze goed worden gesmeerd, waarschijnlijk langer mee dan de gebruikers. De automatische bedkalibratie elimineert op elegante wijze de meest voorkomende bron van fouten voor beginners en bespaart 3D-printveteranen ook vervelend handwerk.



Beide printers bieden probleemloze prints met PLA (links Bambu Lab, rechts Prusa). Zelfs veel duurdere FDM-printers kunnen dat nauwelijks beter. Met andere materialen zijn de resultaten wisselend.

Beide machines voldoen dus aan de belofte dat ze eenvoudig te gebruiken zijn voor standaard prints. Ze zijn daarbij ongeveer even moeilijk (of eigenlijk makkelijk) te gebruiken als inkjet- of laserprinters.

Dankzij het volledig metalen hot-end en de goede verwarmde printbedden is het mogelijk om te experimenteren met de meeste materialen die beschikbaar zijn voor FDM 3D-printen. Succes is echter niet gegarandeerd, want vooral door warping kunnen prints mislukken. Vooral bij de MK4 mis je daarbij een behuizing met actieve verwarming. Als je de originele behuizing erbij bestelt, kost de MK4 meer dan twee keer zoveel als de Bambu Lab P1S en zelfs aanzienlijk meer dan de X1C van Bambu Lab. De MK4-kitversie moet je daarnaast zelf opbouwen, wat volgens Prusa zo'n acht uur werk is.

Volgens ons biedt de Bambu Lab P1S een betere balans tussen prestaties en prijs. Het gebruiksgemak ligt ook hoger en het coreXY-ontwerp levert veel hogere snelheden. Prusa blinkt wel uit op het gebied van ondersteuning en biedt veel reserveonderdelen en upgradekits, ook voor oudere modellen. **ct**

Literatuur

- [1] Pina Merkert, Christoph Schmith en Marco den Teuling, Zo vind je een geschikte 3D-printer, c't 7/2023, p.70
[2] Marco den Teuling, Bambu Lab A1 mini review, c't 3/2024, p.24

Gebruiksvriendelijke 3D-printers

Apparaat	Bambu Lab P1S	Prusa MK4
Fabrikant, website	Bambu Lab, bambulab.com	Prusa Research, prusa3d.com
Bouwvolume	25,6 × 25,6 × 25,6 cm	25 × 21 × 22 cm
Afmetingen	38,9 × 38,9 × 45,8 cm	50 × 55 × 40 cm
Gewicht	13 kg	7 kg
Filament	1,75 mm - PLA, PETG, TPU, PVA, PET, ABS, ASA, PA, PC	1,75 mm - PLA, PETG, ABS, ASA, TPU, HIPS, PA, PVA, PC, PP, CPE, PVB, NGEN
Laaghoogte	0,08 tot 0,28 mm	0,05 tot 0,3 mm
Meegeleverde nozzle	0,4 mm	0,4 mm
Printplaat	Veerstaal verwijderbaar, met PEI-laag	Veerstaal verwijderbaar, met PEI-laag
Maximale bedtemperatuur	100 °C	120 °C
Maximale nozzle-temperatuur	300 °C	290 °C
Maximale printsnelheid / versnelling / flow	500 m/s / 20.000 m/s ² / 32 mm ³ /s	600 mm/s ¹ / 20.000 mm/s ² / 15 mm ³ /s
Prijs	€ 749	€ 1199 (zelfbouwkit € 889)
Prijs multimateriaal-upgrade	AMS: € 359	MMU3: € 329

¹ In de praktijk is de P1S sneller, omdat die de maximale snelheid vaker kan benutten zonder dat de printkwaliteit eronder lijdt.



MINDER KABELBENDE

27-inch 4K-monitoren met USB-C

De 27-inch beeldschermen met ultrahoge resolutie combineren een groot schermoppervlak met een compact ontwerp. De huidige beeldschermen tonen prachtige kleuren, en je sluit een pc of laptop makkelijk aan via een enkele USB-C-kabel. De prijzen beginnen al bij 350 euro.

Ulrike Kuhlmann en Alieke van Sommeren

Een 27-inch monitor biedt voldoende schermoppervlak om comfortabel te werken en toch niet te veel ruimte op je bureau in te nemen. Dat formaat monitoren is op dit moment daardoor een van de populairste monitorformaten. Voor deze test hebben we monitoren geselecteerd met een 4K-resolutie en USB-C. De schermen halen een pixeldichtheid van 163 pixels per inch (dots per inch, dpi), waarbij zelfs haviksoogen geen pixelstructuur meer zien.

ÉÉN KABEL VOOR ALLES

De geteste schermen zijn de BenQ PD2706U, de ThinkVision P27pz-30 van Lenovo, de 27UP850N van LG, de Philips Brilliance 27B1U7903 en de S27A800UJU van Samsung. Die laatste is het model uit 2021, we konden de even goed uitgeruste maar goedkopere opvolger met de toevoeging 800UJP helaas niet testen. Alle vijf hebben minstens één USB-C-ingang, die ze ten eerste gebruiken om videosignalen te ontvangen, ten tweede om een laptop van stroom te voorzien en ten derde om andere randapparatuur aan te sluiten. Ze hebben ook een usb-hub voor je toetsenbord, muis, harde schijf of webcam en laden mobiele apparaten op die zijn aangesloten via USB-C met behulp van Power Delivery (USB-PD). Een enkele kabel is dus voldoende tussen je pc of laptop en het beeldscherm.

De vijf beeldschermen kunnen in hoogte worden versteld en zijn in twee richtingen te draaien. De in-

gebouwde IPS-panels zijn ergonomisch, waardoor de beeldinhoud er vanaf de zijkant en 90 graden gedraaid hetzelfde uitziet als vanaf de voorkant.

Tot zover de overeenkomsten tussen onze vijf schermen. Ze verschillen enorm in prijs, want ze kosten tussen 350 en 1200 euro. Die verschillen zijn deels te wijten aan de kwaliteit van de ingebouwde panels en deels aan de andere functies. Naast de vele video-ingangen hebben twee beeldschermen verschillende usb-poorten en een netwerkaansluiting. Vier apparaten vertragen de overdrachtssnelheid via USB-C naar USB 2.0-snelheid bij het ontvangen van een beeldsignaal. Alleen de monitor van Philips behoudt een snelle overdrachtssnelheid dankzij Thunderbolt 4 – zelfs bij 4K met 60 Hz en 10-bit kleurenresolutie.

Geen van de vijf is geschikt voor veel-eisende games. De LG en Philips ondersteunen in ieder geval respectievelijk FreeSync en Adaptive Sync en geven vloeiende bewegingen vrij streeploos weer. De schakeltijden van de BenQ waren vergelijkbaar.

Vier van de monitoren kunnen twee signaalbronnen tegelijk op het scherm weergeven, naast elkaar (Side-by-Side, Sbs) of in elkaar (Picture-in-Picture, PiP). De BenQ en Lenovo hebben naast een usb-hub een KVM-switch voor je toetsenbord, muis en video. Daardoor kan één setje invoerapparatuur worden gebruikt voor twee aangesloten pc's. Het overschakelen gebeurt automatisch of, bij een Side-by-Side weergave, met een druk op een knop op de monitor.

MINI-LEDS VOOR HDR

De grootste kostenpost is echter de achtergrondverlichting van de schermen. Drie monitoren hebben een conventionele led-achtergrondverlichting met kleine diodes aan de rand van het scherm. Dat zijn blauw licht uitstralende diodes gecoat met groene en rode fosfor. Samen produceert het RGB-mengsel wit licht, dat door dunne folielagen zo gelijkmatig mogelijk over de achterkant van het scherm verdeeld wordt. Kleurenfilters over de RGB-subpixels maken daar uiteindelijk weer gekleurd licht van.

De twee beeldschermen van Lenovo en Philips hebben in plaats daarvan minuscule rode, groene en blauwe diodes die gelijkmatig achter het beeldscherm zijn verdeeld en waarvan het RGB-mengsel per diode driedubbel wit produceert.

De helderheid van de leds kan specifiek worden geregeld in kleine groepen: Lenovo heeft 1152 clusters, Philips zelfs 2304. Local



BenQ PD2706U

De DesignVue is ideaal om meerdere pc's naast elkaar te gebruiken. Met de ingebouwde KVM-switch kun je een toetsenbord, muis en webcam aan de gebruikte pc koppelen. Een kleine puck met een draaiwiel en vijf knoppen, die via usb aan de monitor bevestigd is, helpt bij de monitorinstellingen. Als alternatief zijn er ook knoppen aan de achterkant van het beeldscherm. De functie in het menu om inbranden te verhelpen schakelt eindeloos snel achter elkaar drie verschillende compleet grijze inhoud op het scherm – het doel is onduidelijk.

De Uniformity-functie voor een gelijkmatige verlichting beperkt de gehele helderheid en maakt het midden van het scherm iets te donker. Als de functie uitgeschakeld is, is het midden iets te helder. Over het geheel is de verlichting echter prima. De PD2706U met 10-bit kleurenresolutie reproduceert grijze gradiënten erg zuiver, kleurneutraal en zonder strepen. Alleen zeer donkere gebieden zouden iets meer verzadigd kunnen zijn.

In de USB-C-modus met gegevensoverdracht via USB 3.1 wordt de kleurresolutie teruggebracht tot 8 bit. De monitor dekt de sRGB-kleurruimte volledig af, voor DCI-P3 mist hij wat verzadiging in het groen. De PD2706U heeft drie video-ingangen en twee usb-hubs, plus een jackaansluiting aan de zijkant en twee extra usb-poorten voor het opladen van een smartphone of tablet. Alleen de netwerkaansluiting ontbreekt voor gebruik als dockingstation, dat zou je bureau helemaal netjes kunnen opruimen. Als je de beeldinhoud van twee pc's naast elkaar weergeeft, kun je hun kleurweergave onafhankelijk van elkaar aanpassen.

- ▲ KVM-switch
- ▲ net grijsverloop
- ▼ groen mist verzadiging



Lenovo ThinkVision P27pz-30

De ThinkVision-monitor van Lenovo beschikt over de nieuwste technologie met zijn local-dimming achtergrondverlichting met RGB mini-leds en maakt indruk met zeer rijke kleuren, enorme helderheid en hoge contrasten. De achtergrondverlichting heeft ook zijn schaduwkant in de ware zin van het woord: het scherm is donkerder aan de randen en wit wordt omlijst door een kader van ongeveer vijf centimeter breed in een koelere kleurtemperatuur. Het energieverbruik is het hoogste van alle hier geteste monitoren.

Het scherm toont fijne grijstinten perfect zuiver. Het biedt verschillende presets, maar in tegenstelling tot bijvoorbeeld DCI-P3 wordt de ingestelde sRGB-kleurruimte niet zuiver afgedekt. Er zitten de nodige ongebruikelijke instellingen in het menu, waaronder een die de helderheid tot pijnlijk fel opschroeft, maar ook nuttige zoals een automatische helderheidsaanpassing via de omgevingslichtsensor en een afwezigheidssensor.

De monitor staat stevig op zijn voet en heeft voldoende ingangen. Met zijn netwerkpoort en ingebouwde KVM-switch kun je de P27pz-30 gebruiken als dockingstation. In de rode sleuf in de voetplaat passen smartphones, die via USB-C-PD met 15 watt kunnen worden opgeladen. Als je het in hoogte verstelbare scherm in staand formaat zet, moet je het scherm iets omhoog zetten, anders ramelt het met een hoek op de voetplaat en laat het lelijke groeven achter.

- ▲ geïntegreerde docking
- ▲ kleuren, helderheid, contrast
- ▼ ongelijkmatige verlichting



LG 27UP850N

De monitor van LG onderscheidt zich van het gestandaardiseerde zwart van zijn concurrenten met zijn deels witte behuizing. Om ergonomische redenen is de voorkant zwart omlijst, waardoor je oog naar de beeldinhoud wordt getrokken. De monitor staat op een ruimtebesparende halvemaanvormige voet. Het scherm wiebelt al snel. Alle aansluitingen steken richting de achterkant uit in plaats van naar beneden. Als je het scherm dicht tegen de muur wilt monteren, moet je haakse stekkers aanschaffen en de lompe externe voeding ergens plaatsen.

De twee usb-poorten voor randapparatuur zijn zo bezet, LG had er wel een paar meer mogen installeren. De monitor is echter sowieso niet optimaal als dock door het ontbreken van een netwerkpoort. De 27UP850N is de enige geteste monitor die niet twee signaalbronnen tegelijk kan weergeven. De Edge-led achtergrondverlichting verlicht het scherm wat ongelijkmatig en de kleurtemperatuur in de sRGB preset is iets te warm. Afgezien daarvan dekt het scherm de volledige sRGB-range af. Als je DCI-P3 kiest als voorinstelling voor het beeld, zijn de rode en groene kleuren niet verzadigd genoeg.

De HDR effect-preset bewijst dat de monitor zeker rijkere kleuren kan produceren: rood, groen en blauw worden weergegeven met een verzadiging die overeenkomt met P3. De 27UP850N levert voorbeeldig werk met het reproduceren van fijne grijsverlopen. De schakeltijden zouden voor veel games voldoende moeten zijn en de monitor ondersteunt ook FreeSync.

- ▲ zeer goed grijsverloop
- ▼ ongelijkmatige verlichting
- ▼ karige uitrusting



Philips 27B1U7903

De Brilliance-monitor van Philips maakt gebruik van een mini-led achtergrondverlichting met meer dan 2300 dimbare zones. Helaas heeft de geavanceerde achtergrondverlichting ontsierende neveneffecten, witte beeldinhoud vertoont bijvoorbeeld parelachtige schaduwen aan de randen en wordt omgeven door een blauwgrijs kader. Philips heeft een ventilator ingebouwd om de restwarmte van de leds veilig af te voeren. Die maakt een beetje geluid bij het inschakelen, maar is daarna niet meer hoorbaar.

De helderheid kan royaal worden gevarieerd in de sRGB-modus, tot 850 cd/m² met local dimming geactiveerd. Net als bij Lenovo is er een onzinnige functie in het menu die de helderheid verhoogt naar de maximale waarde, hier heet het 'Intelligent Contrast Enhancement'. Het menu is in het algemeen verwarrend en met de knoppen aan de achterkant erg moeilijk te bedienen.

Het scherm toont subtiele grijsverlopen op een kleurneutrale en streeploze manier – dat geldt alleen niet voor zeer donkere gebieden. De 27B1U7903 dekt de sRGB-kleurruimte perfect af, de rijke kleuren zijn ook geschikt voor DCI-P3 en AdobeRGB, maar niet voor BT2020. De weergave van bewegende beelden blijft streeploos. De monitor ziet er over het geheel genomen zeer hoogwaardig uit, heeft ook een netwerkpoort en behoudt de snelle overdrachtssnelheid zelfs bij een maximale framerate en kleurresolutie dankzij Thunderbolt 4. Hij heeft een uitklapbare omgevingslichtsensor en oplaadmogelijkheden voor smartphones. Het enige wat ontbreekt is een KVM-switch.

- ▲ geïntegreerde docking
- ▲ kleuren, helderheid, contrast
- ▼ ongelijkmatige verlichting



Samsung S27A800UJU

De Viewfinity-monitor van Samsung staat stevig op zijn voet en het scherm kan soepel worden veresteld. Het scherm stuitert een beetje als je er tegenaan duwt, maar dat brengt de stabiliteit niet in gevaar. De video-ingangen van de elegante monitor zitten aan de onderkant, terwijl de aansluitingen voor usb-randapparatuur en koptelefoons richting de achterkant uitsteken.

Als je de omgevingslichtsensor activeert, verandert de kleurtemperatuur van het scherm en wordt het beeld erg warm. Als je echter de drietraps oogbeschermingsmodus gebruikt om de helderheid te verminderen, blijft de kleurtemperatuur hetzelfde. De monitor biedt geavanceerde opties voor het weergeven van twee ingangssignalen naast of in elkaar op het scherm. De USB-C-hub kan worden ingesteld om gegevens op volle snelheid naar de randapparatuur te sturen door de refreshrate te verlagen. Prima als tijdelijke oplossing, maar 30 Hz wil je niet al te lang gebruiken.

De monitor toont fijne grijstrappen zonder strepen, maar wel met wat kleurzweem. Het witte beeld lijkt een beetje troebel, het midden is te helder, grijze gebieden flikkeren een beetje. Het scherm produceert rijke kleuren en dekt DCI-P3 goed af. In de sRGB-preset vallen de primaire kleuren iets buiten de kleurendriehoek. Het bereik van het helderheidsniveau in de sRGB-modus loopt zoals aangegeven op tot 296 cd/m² – te laag voor HDR. Het energieverbruik blijft met 23 watt laag, zelfs onder de waarden die worden opgegeven voor zijn opvolger.

- ▲ elegant design
- ▲ uitgebreide weergavefuncties
- ▼ ongelijkmatige verlichting

dimming verhoogt het in-beeld contrast, oftewel het verschil tussen zeer heldere en zeer donkere beeldgebieden. Het beeld van de lcd's profiteert zichtbaar van de mini-led achtergrondverlichting, hoewel het niet in de buurt komt van het enorme contrast van organische beeldschermen (oled).

De mini-leds produceren rijkere kleuren en een hogere helderheid voor HDR-inhoud. Het aanzienlijk grotere aantal leds kost echter ook aanzienlijk meer energie. Bovendien moet de warmte die vrijkomt bij de halfgeleiderverbinding van de leds goed worden afgevoerd. Philips gebruikt daar een kleine ventilator voor, die je duidelijk kunt horen bij het inschakelen, maar niet tijdens gebruik.

CONCLUSIE

De ergonomische eigenschappen van alle vijf de schermen zijn indrukwekkend. Je hebt geen stapel

tijdschriften nodig om de juiste hoogte te vinden en het scherm verticaal gebruiken is met het IPS-paneel geen probleem. Dankzij USB-C is één enkele kabel tussen je laptop en monitor alles wat je nodig hebt.

De twee high-end monitoren met de mini-led achtergrondverlichting van Lenovo en Philips zijn aan te bevelen voor professionele beeld- en video-bewerking.

De Philips 27B1U7903 kan de aangesloten rand-apparatuur altijd op hoge snelheid gebruiken dankzij de Thunderbolt 4-aansluiting. De beeldschermen met Edge-led achtergrondverlichting zijn prima geschikt voor normaal kantoorgebruik. De 27UP850N van LG scoort punten met een goede beeldkwaliteit, maar is maar karig uitgerust. Als je twee apparaten wilt aansluiten, is de PD2706U van BenQ met KVM-switch geschikter – als dockingstation mist hij echter een netwerkaansluiting.

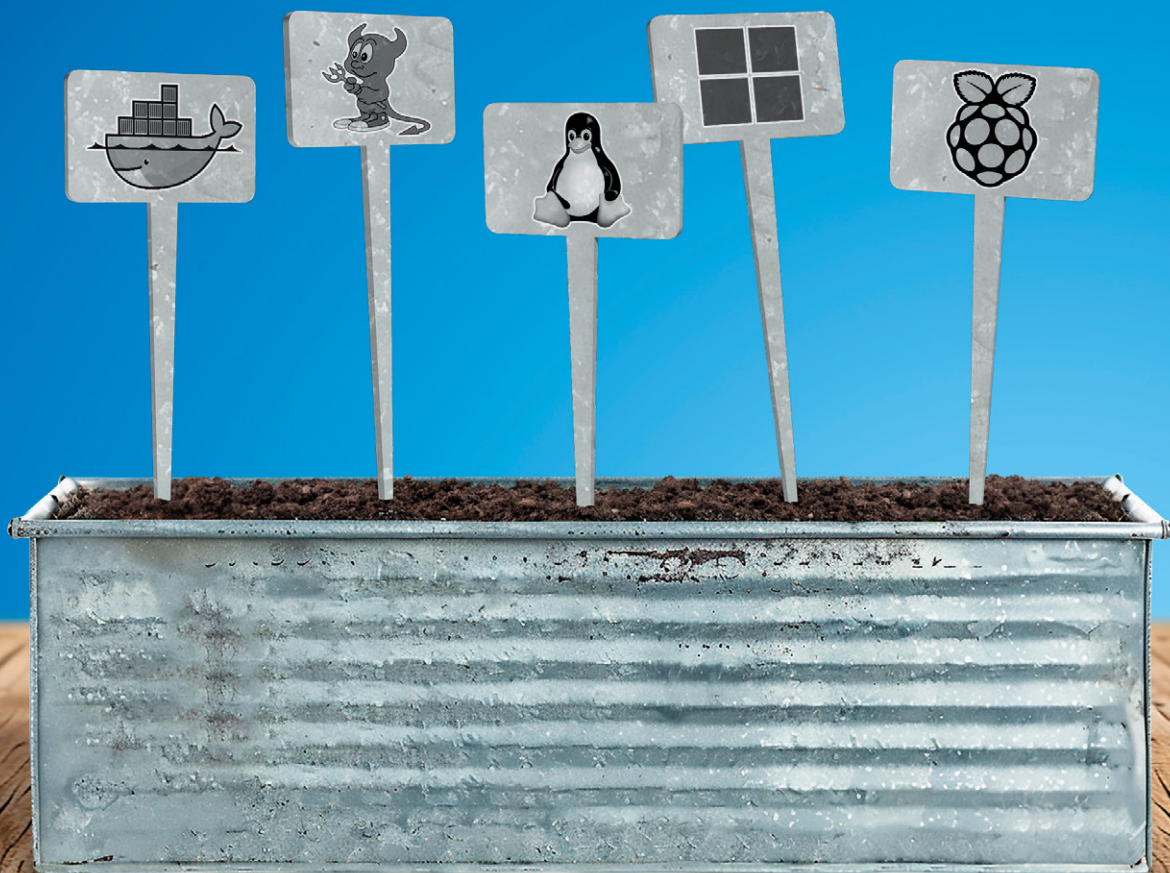


27-inch monitoren met 4K en USB-C

Model	DesignVue PD2706U	ThinkVision P27pz-30	27UP850N	Brilliance 27B1U7903	Viewfinity S27A800JU
Fabrikant	BenQ	Lenovo	LG	Philips	Samsung
Diagonaal	27" (68,29 cm)	27" (68,29 cm)	27" (68,29 cm)	27" (68,6 cm)	27" (68,6 cm)
Resolutie (beeldverhouding) / pixeldichtheid	3840 × 2160 pixels (16:9) / 163 dpi	3840 × 2160 pixels (16:9) / 163 dpi	3840 × 2160 pixels (16:9) / 163 dpi	3840 × 2160 pixels (16:9) / 163 dpi	3840 × 2160 pixels (16:9) / 163 dpi
Paneltype / maximale refreshrate	IPS / 60 Hz (mat)	IPS / 60 Hz (mat)	IPS / 60 Hz (mat)	IPS / 60 Hz (mat)	IPS / 60 Hz (mat)
HDR / kleurresolutie	DisplayHDR 400, HDR10 / 10 bit	DisplayHDR 1000, HDR10, HLG / 10 bit	DisplayHDR 400, HDR10 / 8 bit	DisplayHDR 1400, HDR10 / 10 bit	HDR10 / 8 bit
Video-ingangen	USB-C met DP, HDMI 2.0, DisplayPort 1.4	USB-C met DP, 2 × HDMI 2.1, DisplayPort 1.4	USB-C met DP, 2 × HDMI 2.0, DisplayPort P 1.4	Thunderbolt 4 / USB-C met DP, 2 × HDMI 2.0, DisplayPort 1.4	USB-C met DP, HDMI 2.0, DisplayPort 1.4
Usb-hub	✓ (3 × USB-A 3.2 Gen 1 en USB-C 3.1 Gen 1 met USB-PD)	✓ (4 × USB-A 3.2 Gen 2 and USB-C 3.2 Gen 2 met USB-PD)	✓ (2 × USB-A 3.1 Gen 1)	✓ (4 × USB-A 3.2 en Thunderbolt 4 met USB-PD)	✓ (3 × USB-A 3.1. Gen 1)
Overige aansluitingen	3,5mm-jack voor headset, micro-USB (voor remote-puck)	3,5mm-jack voor headset, gigabit-LAN, DisplayPort	3,5mm-jack voor headset	3,5mm-jack voor headset, gigabit-LAN, DisplayPort	3,5mm-jack voor headset
Bijzonderheden	remote-puck, stereospeakers, ICC-profielsync	aanwezigheidsensor, omgevingslichtsensor	stereospeakers	stereospeakers, omgevingslichtsensor	omgevingslichtsensor
Meegeleverd	kabels: power, USB-C, HDMI, DisplayPort	kabels: power, USB-C, HDMI, DisplayPort	adapter, kabels: power, USB-C, HDMI, DisplayPort	kabels: power, USB-A, Thunderbolt, HDMI, DisplayPort	kabels: power, USB-C, USB-C-naar-A, HDMI
Afmetingen (b × h × d) / gewicht	61,5 × 45-56 × 24 cm / 8,3 kg	61,5 × 46-55 × 22 cm / 6,2 kg	61 × 46-57 × 22 cm / 4,1 kg	61 × 40-52,5 × 20 cm / 9,4 kg	61 × 43,5-54,5 × 17,5 cm / 6,7 kg
Picture-in-Picture / Picture-by-Picture / KVM	✓ / ✓ / ✓	✓ / ✓ / ✓	- / - / -	- / ✓ / -	✓ / ✓ / -
VESA-mount	✓ (10 × 10 cm)	✓ (10 × 10 cm)	✓ (10 × 10 cm)	✓ (10 × 10 cm)	✓ (10 × 10 cm)
Laadperformance USB-C (Power Delivery)	90 W	140 W	90 W	90 W	90 W
Instellen: hoogte / kantelen / draaien / pivot	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / ✓
Metingen					
Contrast minimaal / uitgebreid blikveld	1123:1 (15,7 %) / 743:1 (52,5 %)	1108:1 (19,9 %) / 691:1 (58,1 %)	1075:1 (17,9 %) / 702:1 (53,7 %)	1100:1 (14,4 %) / 739:1 (49 %)	1075:1 (18,1 %) / 690:1 (55,3 %)
De ronde diagrammen geven de kijkhoekafhankelijkheid weer. Blauw bij lager, rood bij hoger contrast.					
Cirkels markeren kijkhoekintervallen van 20 graden. Idealiter is de cirkel volledig roze.					
Bereik verlichting sRGB / met local dimming	50 ... 308 cd/m ² / -	80 ... 625 cd/m ² / 1580 cd/m ²	60 ... 390 cd/m ² / -	4 ... 780 cd/m ² / 845 cd/m ²	65 ... 296 cd/m ² / -
Verbruik ¹ : stand-by / in gebruik ³ / bij volledige helderheid	0,3 W / 20,1 W / 34,3 W	0,3 W / 27,4 W / 57 resp. 135 W ⁴	0,3 W / 22,8 W / 40,5 W	0,3 W / 38,8 W / 90,3 resp. 96,5 ⁴ W	0,3 W / 23,1 W / 35 W
Beoordeling					
Contrast / kijkhoekafhankelijkheid	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕	⊕ / ⊕⊕	⊕ / ⊕
Verlichting / kleurweergave	⊕ / ⊕	○ / ⊕⊕	○ / ⊕	○ / ⊕⊕	○ / ⊕
Bediening / afwerking	⊕⊕ / ⊕	⊕⊕ / ⊕⊕	⊕ / ○	○ / ⊕⊕	⊕ / ⊕
Garantie	3 jaar	3 jaar	2 jaar	3 jaar	3 jaar
Prijs	€ 450	€ 1200	€ 350	€ 780	€ 400
⊕⊕ zeer goed ⊕ goed ○ voldoende ⊖ slecht ⊖⊖ zeer slecht ✓ aanwezig — niet aanwezig ¹ volgens fabrikant ² gemeten bij signaal-input via HDMI ³ gemeten bij 120 cd/m ² ⁴ met ingeschakelde local dimming					

KEUZEVRIJHEID

Virtualisatie – een universeel systeem voor pc's



ALLES OVER DIT ONDERWERP

- ▶ **Universeel systeem voor pc's** 78
- ▷ Introductie Proxmox VE 82
- ▷ Aan de slag met Proxmox VE 86

VMware prijst zichzelf een beetje de markt uit omdat de investeerder alleen nog abonnementen wil verkopen en daarbij producten opheft. Op veel gebieden is die virtualisatie inmiddels ook al niet meer toonaangevend. We bekijken de interessantste alternatieven: van desktopvirtualisatie met macOS-software tot de veelzijdige Proxmox-server. Veel daarvan is gratis of zelfs opensource.

Peter Siering en Marco den Teuling

Sinds VMware 25 jaar geleden virtualisatie introduceerde in de x86-wereld, draaien verschillende besturingssystemen vreedzaam naast elkaar op dezelfde hardware in virtuele machines – en dat allemaal tegelijk. Dat is praktisch voor het testen of om de efficiëntie te verhogen. Virtualisatie wordt nu ook gebruikt om pc's veiliger te maken.

Voor die tijd was dat in x86-kringen alleen mogelijke met meestal halfslachtige emulaties. Niet alleen de software (hypervisor) en de besturingssystemen die daarvoor worden gebruikt zijn daarna snel geëvolueerd, ook de pc-hardware paste zich aan.

Software in een virtuele machine draait nu nauwelijks langzamer dan op echte hardware. Alleen wanneer speciale omstandigheden vereist zijn, zoals supersnelle toegang tot gegevensdragers of grafische kaarten als coprocessors of voor 3D-games, loont het nog steeds om software niet in een virtuele machine te verpakken maar op echte hardware te draaien.

De voordelen van een virtuele machine ten opzichte van een echte pc wegen vaak zwaarder dan de nadelen: een virtuele machine is eenvoudig over te zetten naar andere hardware, eenvoudig volledig te back-uppen, je kunt de huidige status bevriezen en op een later tijdstip weer herstellen en een virtuele machine is meestal op afstand toegankelijk. Een virtuele machine is ook handig voor de beveiliging: mogelijk geïnfecteerde bestanden kunnen erin worden geopend zonder gevolgen voor de rest van het systeem – mits de virtuele machine goed afgeschermd is.

VERKLAREND OVERZICHT

In de begindagen van x86-virtualisatie draaide de applicatiesoftware in een virtuele machine alleen ongehinderd zolang het geen systeemaanroepen deed. Zodra er systeemaanroepen plaatsvonden, zoals contextwisselingen in het besturingssysteem, moest de virtualisatiesoftware die controleren en geprivilegieerde instructies emuleren om de hardware virtueel te vermenigvuldigen.

Die emulatie van de geprivilegieerde instructies die zijn gereserveerd voor het besturingssysteem vergde veel bronnen. Daarnaast moest de software binnen een virtuele machine ook typische pc-bronnen emuleren, zoals de grafische kaart, harde schijf, netwerkkaart enzovoort. Ook daar hielp aanvankelijk het emuleren van populaire pc-onderdelen, zoals een S3 grafische kaart, een AMD-netwerkkaart en een Buslogic SCSI-controller.

De virtualisatiefuncties die beschikbaar zijn in de huidige processors (Intel VT-x, AMD-V) vergemakkelijken en versnellen het uitvoeren van geprivilegi-

eerde instructies. De instructiesets en de daarmee gemaakte softwarearchitectuur zijn gevirtualiseerd. Intel en AMD hebben ook functies in hun cpu's ingebouwd om harde schijven, usb-apparaten, grafische en netwerkkaarten rechtstreeks vanuit virtuele machines aan te spreken. Dat staat bekend staat als I/O-virtualisatie (I/O staat voor input/output).

Gespecialiseerde stuurprogramma's voor harde schijven, netwerken en grafische kaarten die in de huidige besturingssystemen geïntegreerd zijn, communiceren rechtstreeks met de virtualisatiesoftware. Ze nemen een kortere weg zodat tijdrovende emulatie van pc-componenten niet langer nodig is. De gebruikelijke naam daarvoor is paravirtualisatie. Alles bij elkaar vormt dat de gemeenschappelijke basis voor de huidige x86- en ARM-hardware en besturingssystemen.

INTERACTIE

Virtualisatiesoftware voegt de afzonderlijke elementen samen tot één pakket. De gegevens op de virtuele harde schijf van een virtuele machine komen meestal terecht als bestand(en) in het bestandssysteem van de echte pc. Om een virtuele machine op een andere pc te laten draaien, bestaat het belangrijkste werk uit het daarheen overbrengen van die bestand(en). Door slim beheer van die bestanden, dat onder andere wijzigingen afzonderlijk registreert terwijl de virtuele machine draait, kunnen snapshots worden gemaakt.

Een virtuele machine is verbonden met het netwerk door de netwerkverbinding te delen met de

De juiste oplossing vinden

De veelzijdige functies van **VMware** en **VirtualBox** op de **desktop** pleiten voor het gebruik ervan onder Linux en Windows – maar dat is alleen aanbevolen als de virtualisatie van het besturingssysteem zelf uitgeschakeld kan blijven.

Als je **exotische besturingssystemen** wilt draaien, zoals OS/2, kun je het beste VirtualBox gebruiken. De emulatiefuncties voor oude pc-hardware zijn daar het meest geavanceerd en de kans dat je die oude apparaten aan de praat krijgt is groter.

macOS heeft sinds versie 12 zijn eigen virtualisatie, die niet kan worden uitgeschakeld en waarvoor

geen interface bestaat. Er is echter wel macOS-software die helpt bij het opzetten van virtuele machines, zoals UTM en VirtualBuddy.

Hyper-V is de tool bij uitstek voor **Windows** op de desktop. Beheer via de Hyper-V Manager is even wennen, maar daarna is het bijzonder eenvoudig te onderhouden.

Voor de **Linux-desktop** biedt Gnome Boxes een eenvoudige interface voor KVM. Als je het liever technischer aanpakt, kun je Virtual Machine Manager (virt-manager) of de commandline gebruiken.

Als er een Linux-server nodig is, dan is Proxmox VE het overwegen waard.

echte pc. Daar bestaan verschillende modellen voor: een virtuele machine kan zich achter de pc verbergen door middel van adresvertaling (NAT). De virtuele machine kan echter ook zelfstandig in het netwerk verschijnen. In de regel is er ook de mogelijkheid om meerdere virtuele machines in aparte virtuele netwerken te organiseren. Daardoor kun je complexe testscenario's opzetten zonder zelfs maar één netwerkkabel aan te raken.

Het toetsenbord, de muis en het scherm van een virtuele machine zijn toegankelijk via speciale software, in wiens venster de output verschijnt. Als dat venster de focus heeft, komen de toetsaanslagen als invoer in de virtuele machine terecht. Binnen bepaalde grenzen is het mogelijk om informatie via het klembord in een virtuele machine te plaatsen of informatie juist op te halen. Die manier van samenwerken werkt echter vaak slechts rudimentair.

Om uitwisseling tussen het uitvoerende systeem (host) en de virtuele machine (gast) te bevorderen, maakt virtualisatie graag gebruik van de diensten van hulpsoftware in de virtuele machine. Dat verbetert de controle over het toetsenbord en scherm door gebruik te maken van geoptimaliseerde remote-beheertechnieken. Het vergemakkelijkt het uitwisselen van bestanden door een speciale map aan te maken voor overdracht of zelfs door het slepen en neerzetten van bestanden. De hulpsoftware neemt vaak extra taken op zich en stelt de virtualisatiesoftware in staat om signalen van buitenaf naar een virtuele machine te sturen, bijvoorbeeld om de gast op een ordelijke manier af te sluiten. Of er wordt informatie van de virtuele machine naar de host gestuurd, bijvoorbeeld om het ip-adres weer te geven. In sommige gevallen heeft de hulpsoftware ook een actieve rol en helpt de cpu-klok en het geheugengebruik van virtuele machines te optimaliseren.

PRODUCTTYPEN

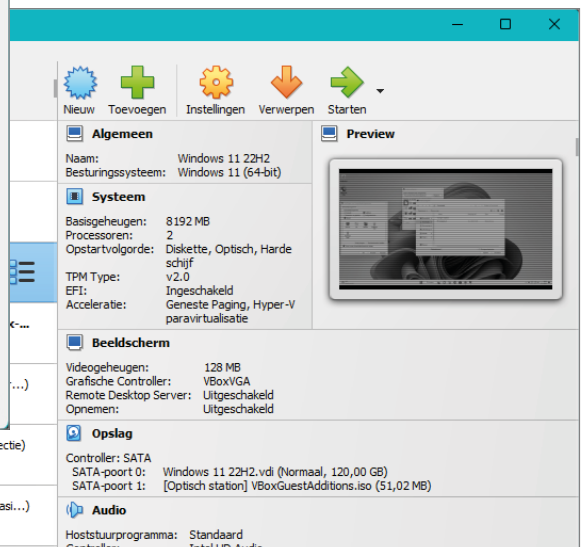
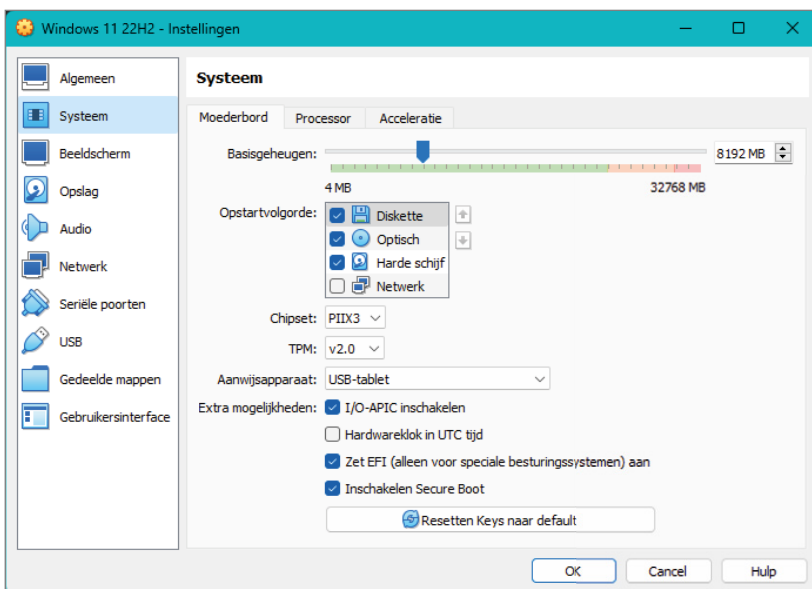
Naarmate de omstandigheden voor virtualisatie veranderden, is ook de software veranderd (zie de link op de volgende pagina voor downloads). Het klassieke product waarmee veel pc-gebruikers tegenwoordig waarschijnlijk bekend zijn, zijn desktopproducten. Die installeren zichzelf als een applicatie en breiden in het beste geval het bestaande besturingssysteem uit met systeemgerelateerde modules die als stuurprogramma's worden toegevoegd. VMware Workstation en Player werken vandaag de dag nog steeds op die manier, evenals VirtualBox.

Tegelijkertijd heeft software voor virtuele machines zijn weg gevonden naar veel gangbare besturingssystemen. Zo wordt Windows geleverd met Hyper-V. Sinds macOS versie 12 (Monterey) heeft het besturingssysteem van Apple ook virtualisatie ingebouwd. Linux-ontwikkelaars hebben hun eigen virtualisatietechnologie met de naam KVM ontwikkeld en in de kernel ingebouwd. De BSD-wereld heeft ook zijn eigen hypervisors. Die zijn vaak de beste en meest kosteneffectieve methode.

Als onderdeel van het besturingssysteem neemt virtualisatie ook nieuwe taken op zich, bijvoorbeeld voor een betere beveiliging. Bij Windows sluit Microsoft kritieke inloggegevens desgewenst op in een aparte virtuele machine.

Met de integratie van een hypervisor in besturingssystemen zijn ook twee standaarden voor paravirtualisatie- stuurprogramma's en bijbehorende services populair geworden. In de Linux-wereld en meer recentelijk bij macOS is dat VirtIO, in de Windows-wereld zijn het de integratieservices voor Hyper-V die Microsoft zelfs in de Linux-kernel heeft opgenomen. Bij BSD is er ook een soortgelijke ontwikkeling.

Het tweede type virtualisatieproducten zijn die voor servers. Ze zijn ontworpen om een groot aantal virtuele machines betrouwbaar te draaien. Ze hebben soortgelijke functies als tot nu toe genoemd, maar voegen daar geavanceerde functies aan toe om bijvoorbeeld draaiende virtuele machines van de ene server naar de andere te migreren.



Virtualisatiesoftware voor de desktop zoals Virtual-Box biedt talloze opties. Veel ervan werkt echter niet als de geïntegreerde virtualisatie van het besturingssysteem ertussen komt.

Een speciaal geval zijn x86-NAS-apparaten of sommige serverbesturingssystemen zoals Unraid en OVM. Afhankelijk van de configuratie kunnen die ook virtuele machines hosten, maar qua functies kunnen ze niet tippen aan producten die uitsluitend gericht zijn op virtualisatie.

Een typisch kenmerk van servergebaseerde virtualisatie is dat de virtuele harde schijven van de virtuele machines niet langer in bestanden eindigen. In plaats daarvan gebruiken ze blokgebaseerde opslag, zoals die wordt beheerd door een logical-volume-manager. Ze kunnen de functies daarvan dan gebruiken voor snapshots. Sommige producten gebruiken bestandssystemen met daarvoor geschikte technologie zoals ZFS of BTRFS. Alleen Hyper-V werkt voornamelijk met bestanden.

Serverproducten stappen steeds meer af van de aanpak waarbij meerdere servers een gedeeld opslagsysteem gebruiken waarop de virtuele machines zich dan bevinden en dus makkelijk van server naar server kunnen worden gemigreerd. De trend gaat in de richting van hyperconvergentie: de software zorgt ervoor dat alle servers hun opslagruimte redundant delen en een gedeelde toegang hebben tot het netwerk.

Helaas wordt de keuze aan software voor servergebruik steeds beperkter. Microsoft heeft de voorheen gratis Windows Hyper-V Server-versie sinds de 2019-editie stopgezet (maar er is ondersteuning tot 2029). Licentiekosten voor reguliere serversoftware zijn fors. VMware-investeerder Broadcom heeft de gratis ESXi-server geschrapt en verkoopt nu alleen nog dure abonnementen.

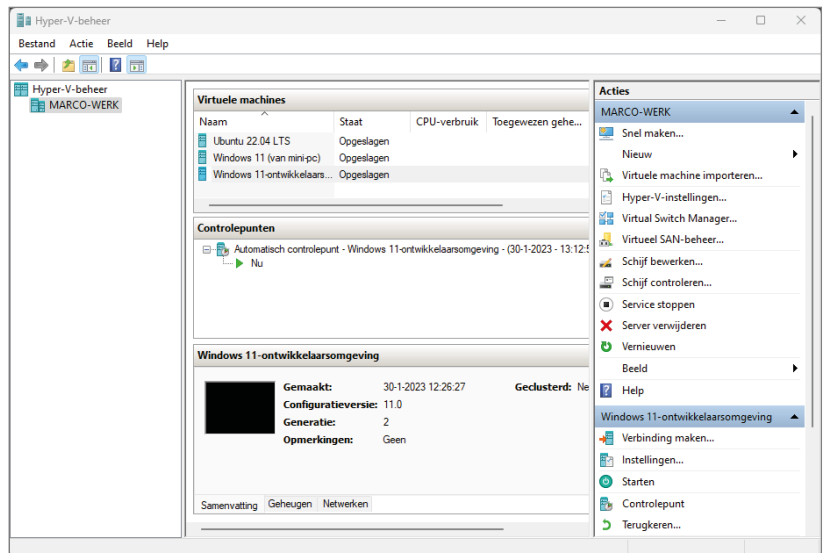
In het aanbod springt Proxmox VE eruit: het is gebaseerd op Linux en KVM, biedt een duidelijke web-interface en wordt momenteel gezien als hét alternatief voor gefrustreerde VMware-gebruikers. Aan de andere kant is het zo eenvoudig te gebruiken dat het voor sommige gebruikers een alternatief is voor de oplossingen die bedoeld zijn voor de desktop – en voor particuliere gebruikers is het dat sowieso.

In het volgende artikel staat een introductie van Proxmox VE en in het artikel erna kun je lezen hoe je met Proxmox aan de slag kunt gaan.

VERWIKKELINGEN

In de praktijk is virtualisatie minder vanzelfsprekend wanneer de wensen toenemen: de toegang tot de hardware, de werking ondanks eigen virtualisatie van het besturingssysteem en de beschikbaarheid van afzonderlijke functies hangen niet alleen af van welk product er draait, maar ook op welk besturingssysteem het actief is en wat er binnen de virtuele machines moet gebeuren.

Neem als voorbeeld de tweede editie van het Windows-subsysteem voor Linux (WSL2): wanneer dat geactiveerd wordt, maakt het gebruik van de eigen virtualisatie van het besturingssysteem. VirtualBox en VMware draaien dan alleen nog met een beperkt aantal functies en verminderde prestaties. Bij macOS is het nog extremer: virtualisatie staat altijd



De omgang met Hyper-V is even wennen, wat ook ligt aan de enigszins achterhaalde interface van de Windows Management Console.

aan en VirtualBox draait al sinds macOS 12 met de handrem erop.

Spice, dat veel wordt gebruikt in de Linux-virtualisatieomgeving, moet niet alleen de console van een virtuele machine makkelijk toegankelijk maken, maar ook usb-apparaten op de host. Dat werkt ook goed met Linux aan beide kanten. Zodra echter Windows of macOS als client gebruikt wordt, weigert de virt-viewer (oftewel remote-viewer) de toegang tot usb-apparaten.

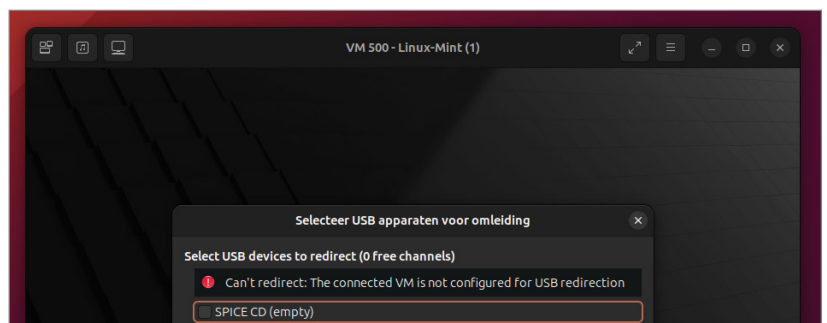
Toegang tot echte hardware vanuit virtuele machines is sowieso een lastige functie. Het kan werken, maar dat is zeker niet altijd het geval. Nvidia-stuurprogramma's controleerden bijvoorbeeld soms of ze in een virtuele machine draaiden en weigerden dan te werken. Er zitten echter vaak geen kwade bedoelingen achter beperkingen in directe hardware-toegang.

Je kunt van veel beperkingen en systeemeisen makkelijk afkomen door de virtualisatie uit te voeren op een apart apparaat dat uitsluitend voor die taak bedoeld is. Dat hoeft geen dikke pc te zijn, een mini-pc of tweedehands thin-client kan volstaan. In het volgende artikel leggen we uit wat je (daarop) van Proxmox VE kunt verwachten.

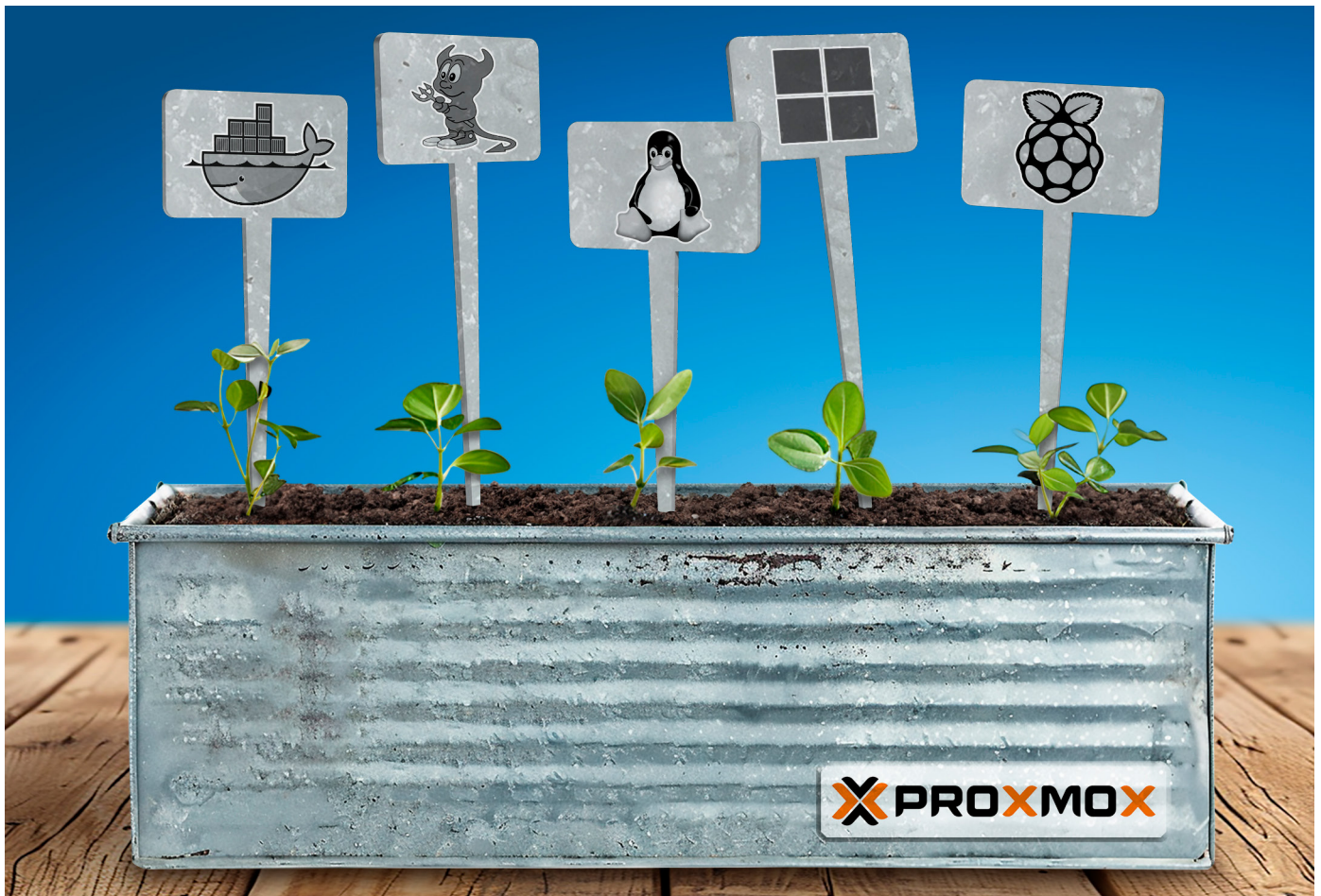
ct



www.ct.nl/softlink/2407078



Gezien de enorme verscheidenheid aan pc-besturingssystemen mag je niet verwachten dat elke functie overal werkt. Spice koppelt lokaal aangesloten usb-apparaten bijvoorbeeld alleen met een remote virtuele machine als aan beide kanten Linux wordt gebruikt én de benodigde usbredir-pakketten geïnstalleerd zijn.



Illustratie c't

WAT PROXMOX VE TE BIEDEN HEEFT

Introductie tot Proxmox VE

Proxmox VE is niet alleen een gespecialiseerde Linux-distributie voor virtualisatie op servers, maar ook interessant als je virtuele machines op je werkplek wilt gebruiken zonder een dikke en lawaaierige pc onder je bureau te hoeven hebben staan. Je kunt er ook een aantal Raspberry Pi's mee vervangen.

Peter Siering en Marco den Teuling

Linux-distributies wordt vaak verweten dat ze cryptisch zijn, maar dat is niet van toepassing op Proxmox VE. Na het installeren heb je via een webinterface toegang tot de hele wereld van virtualisatie. Je kunt virtuele machines instellen, starten, stoppen, klonen, snapshots maken, netwerkdetails configureren, schijven vergroten, back-ups maken, Proxmox-updates installeren en nog veel meer.

Via de browser krijg je ook toegang tot de console van een virtuele machine, bijvoorbeeld om een besturingssysteem te bedienen dat erin draait. Die vervanging van toetsenbord, muis en scherm is voldoende voor eenvoudig gebruik. Het kan echter niet helemaal tippen aan het gemak van desktopvirtualisatie met VMware, VirtualBox en dergelijke, omdat het standaard gebruikmaakt van het eenvoudige VNC-protocol.

MAKKELIJK WERKEN

Bij het opzetten van een virtuele machine of achteraf kun je echter een alternatief consoleverbindingsprotocol activeren: Spice. Met een Spice-client en wat hulpsoftware kun je makkelijk rechtstreeks verbinding maken met de virtuele console van een virtuele machine, zonder zelfs de Proxmox-webinterface te moeten oproepen. De handige PVE VDI Client-software, die niet van Proxmox zelf is, kun je vinden bij de link op de laatste pagina van dit artikel.

Proxmox verschilt van desktopoplossingen door de manier waarop het de virtuele harde schijven van de virtuele machines beheert. In plaats van bestanden gebruikt het standaard logische volumes, oftewel delen van bestaande partities die worden beheerd door gespecialiseerd volumebeheer. Je hoeft je daar zelf niet mee bezig te houden, maar je moet je er wel bewust van zijn.

Het type volumebeheer dat Proxmox gebruikt kan worden bepaald tijdens het installeren. De Proxmox-ontwikkelaars hebben ook ZFS ingebouwd als alternatief voor de beproefde Logical Volume Manager (LVM). Natuurlijk is het ook mogelijk om later opslag toe te voegen. Je bent niet gebonden aan de methode die je kiest tijdens het installeren, maar het is verstandig om de keuze vooraf te overwegen.

Het voordeel van ZFS: het kent incrementele snapshots. Proxmox maakt daar handig gebruik van

om wijzigingen aan virtuele schijven van de ene Proxmox-node naar de andere te repliceren. Aangezien dan alleen de gewijzigde gegevens verstuurd worden, werkt dat snel en interessant voor iedereen die meerdere Proxmox-computers als clusternodes wil gebruiken en dan virtuele machines heen en weer wil verplaatsen.

Proxmox is gebaseerd op virtualisatie in de Linux-kernel (KVM). De naam QEMU wordt in die context vaak gebruikt. Dat project, dat oorspronkelijk werd gelanceerd als een systeememulator, helpt virtualisatiesoftware vaak bij het opzetten van de benodigde pc-omgeving, zoals bij Proxmox.

WAT ZIT ERIN

De minimale uitrusting voor een Proxmox-node is een x86-pc met bruikbare virtualisatiefuncties in de processor en een ssd als gegevensopslag voor het besturingssysteem en de virtuele machines. Harde schijven zijn niet geschikt voor virtualisatie, die zijn te traag. Een mini-pc of enkele thin-clients zijn daarom prima geschikt, afhankelijk van de werklust en de inhoud van de virtuele machines natuurlijk.

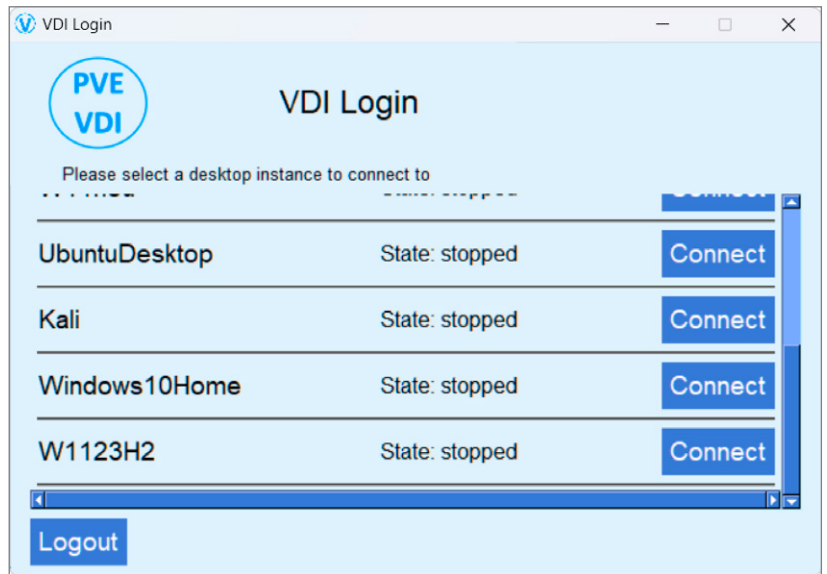
Onder de motorkap van Proxmox zit een geüpgradede Debian. De maker heeft het uitgebreid met een eigen kernel, onder andere voor ZFS-ondersteuning, uitbreidingen voor het beheren van virtuele machines (qemu-Server genaamd) en vele onderdelen die pas interessant worden bij professioneel gebruik wanneer meerdere Proxmox-nodes toegang moeten krijgen tot een gedeeld opslagsysteem of er samen een moeten vormen.

In principe is het installeren ook mogelijk op een reeds draaiend Debian-systeem. Dat kan handig zijn als Proxmox moet worden geïnstalleerd op een gehuurde server waar geen geschikte voorinstallatie wordt aangeboden en het op afstand aansluiten van een usb-stick of ISO niet mogelijk is.

Het feit dat Debian de basis vormt, is ook om een andere reden belangrijk om te vermelden: Proxmox gebruikt het Debian-pakketbeheer (APT) voor updates. Het verbergt de uitvoer ervan en eventuele vragen tijdens de installeren van de pakketten niet achter de webinterface, maar opent daar een extra browservenster voor met een tekstconsole. Daar moet je mogelijk vragen beantwoorden en kun je de voortgang zien.

Het installeren van updates en upgrades naar een volgende Proxmox-versie zijn de enige punten waar Proxmox-gebruikers zonder Linux-ambities een commandline moeten gebruiken. APT stelt daar vragen, die meestal goed beantwoord kunnen worden met het standaard antwoord. De Proxmox-ontwikkelaars bieden voorbeeldige hulp bij upgrades naar de volgende versie. Er is een programma dat controleert of aan alle eisen is voldaan en dat informatie geeft over hoe daar zo nodig aan te voldoen.

De mogelijkheden van het product groeien met elke Proxmox-versie. Slechts weinig gebruikers zullen alle functies nodig hebben. Enkele hoogtepunten: het geïntegreerde gebruikersbeheer biedt twee-factor



Met wat hulpsoftware kun je de virtuele machines bedienen vanaf een laptop of desktop-pc zonder de Proxmox-webinterface überhaupt te hoeven openen.

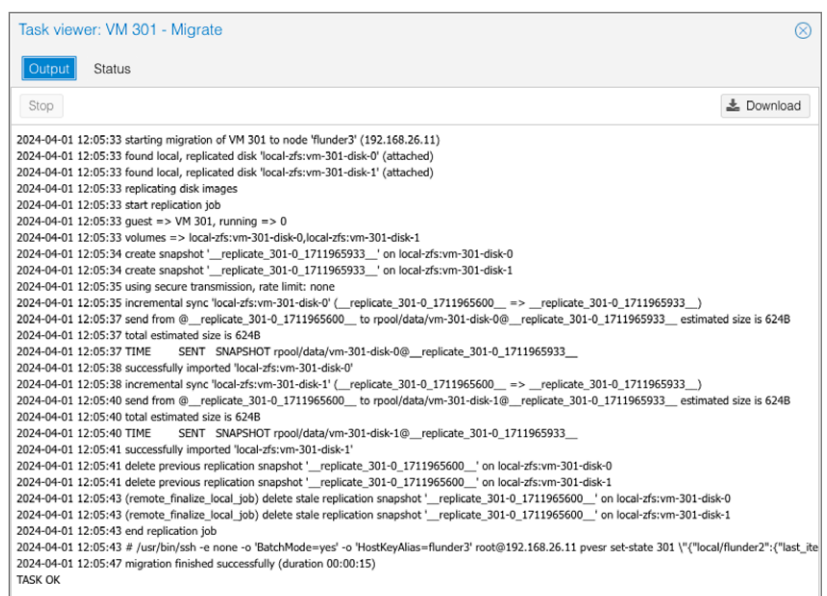
authenticatie en rollen. Het toch al handige netwerkbeheer, dat overweg kan met VLAN's en bridges, is uitgegroeid tot een volwaardige SDN-stack (Software-Defined Networking).

Proxmox werkte altijd al niet alleen met ingekapselde virtuele machines, maar staat ook het gebruik van containertechnologie toe. De ontwikkelaars vertrouwen echter niet op Docker, maar op Linux-containers (LXC), die technisch anders werken (zie het volgende artikel).

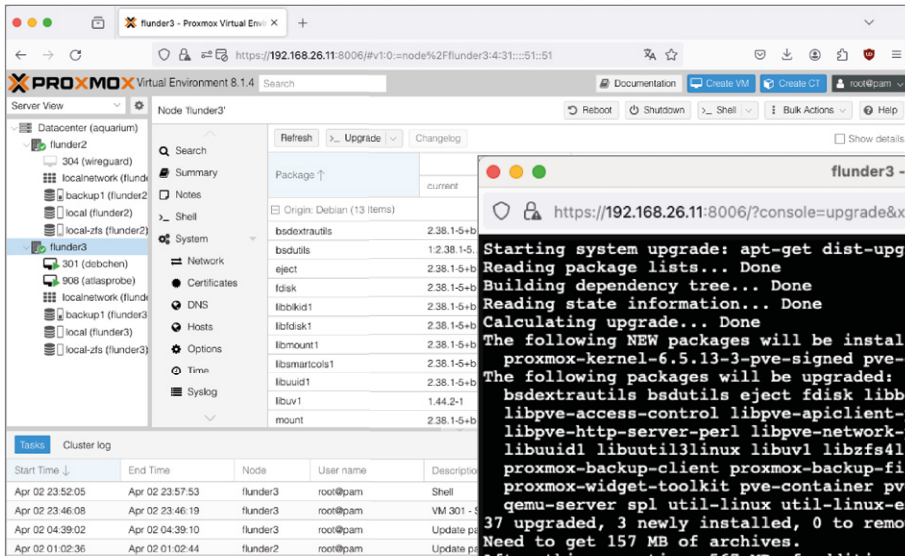
WAT KRIJG JE

Proxmox slaat op een minimale pc al een goed figuur. Het kan bijvoorbeeld virtuele machines hosten die een Raspberry Pi vervangen die je wellicht op verschillende plekken door het huis heen hebt staan voor je smarthome.

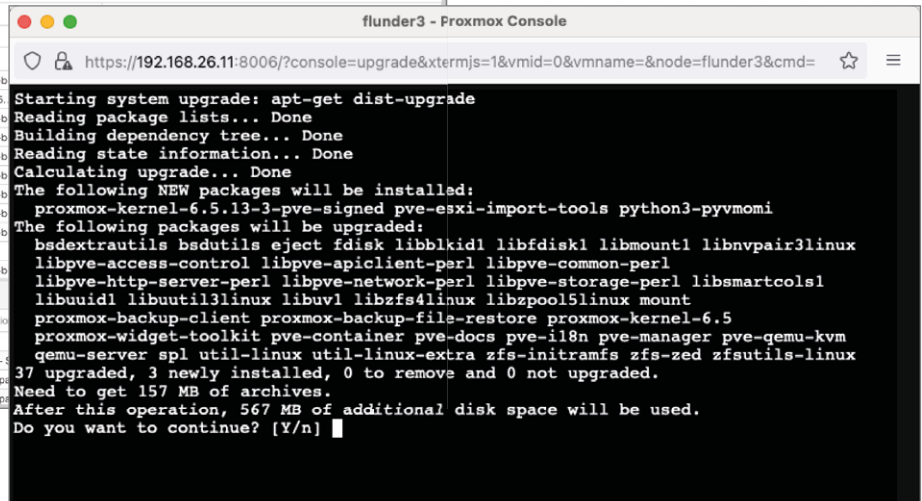
Docker-containers in een virtuele machine kunnen ook makkelijk toegang krijgen tot Zigbee-sticks



Met ZFS als opslaglocatie en ingestelde regelmatige replication schrijft Proxmox virtuele machines razendsnel van de ene clusternode naar de andere.



Voor updates en upgrades gebruikt Proxmox het Debian-pakketbeheer APT. Daarbij mag de charme van de commandline niet ontbreken.



via de functies voor het doorgeven van usb-apparaten van de host-pc naar de virtuele machines. Je hoeft alleen maar de USB-ID's in te voeren in de Proxmox-interface en de virtuele machine ziet het apparaat.

Proxmox bundelt services die om tactische redenen als aparte hosts in virtuele machines zijn opgezet om ruimte en energie te besparen: VPN-servers, back-upservers, gevirtualiseerde Ripe Atlas Probes, een Pi-hole of software-firewalls stellen geen hoge eisen aan het werkgeheugen. Een paar gigabytes of zelfs maar een paar 100 MB RAM en wat schijfruimte zijn vaak al genoeg.

Proxmox is ook goed in het aansturen van krachtige systemen om er meerdere virtuele Windows-machines op te draaien, bijvoorbeeld een testomgeving inclusief Active Directory. Of het nu gaat om Linux of Windows: je kunt groupware, mailservices, software voor de private-cloud enzovoort onderbrengen in afzonderlijke virtuele machines, zodat verschillende systeemeisen geen extra computers vergen. Extra virtuele machines zijn voldoende.

Als de eisen groeien, biedt Proxmox de mogelijkheid om meerdere servers samen te voegen tot clusters. Virtuele machines die je laat beschermen door een hoge beschikbaarheidsmodus worden automatisch overgezet naar andere nodes in het cluster. Live migratie van virtuele machines van de ene node naar de andere vergt niet noodzakelijkerwijs een gedeeld opslagsysteem. Maar dat kan met Proxmox ook: met het gedistribueerde opslagsysteem Ceph hebben meerdere nodes toegang tot een gedeelde opslag.

Wat je daadwerkelijk nodig hebt, hangt af van je wensen of eisen. Als je er alleen zeker van wilt zijn dat je geen virtuele machines verliest en de gegevens die ze bevatten, moet je zeker eens kijken naar de Proxmox Backup Server. Die is ook erg handig als je alleen af en toe virtuele machines met één muisklik van de ene naar de andere server wilt verplaatsen.

WIE ZIT ERACHTER

Het is bijna ongelooflijk hoe relaxed de makers van Proxmox zijn met het aanbieden van hun product onder AGPLv3. Iedereen kan de virtualisatie-omgeving gratis gebruiken. Iedereen die de Enterprise-pakketten met betere kwaliteitscontrole wil, die de maker aanbeveelt voor productief gebruik, kan een abonnement nemen voor 110 euro per jaar. Supportservices zijn inbegrepen vanaf 340 euro per jaar.

Volgens de eigenaars van het bedrijf heeft nog geen tiende van de beheerders van de momenteel meer dan een miljoen actieve installaties een dergelijk abonnement afgesloten. Toch zegt Martin Maurer, een van de oprichters, in een interview: 'Ons businessmodel werkt zelfs als meer dan 90 procent van de gebruikers niets betaalt.'

Proxmox is van de oprichters en dat moet zo blijven. Maurer: 'Iedereen die zijn bedrijf verkoopt heeft het vertrouwen in de toekomst ervan verloren, en/of het is een erkenning van mislukking, of ze hebben dringend geld nodig of een combinatie van al die punten. Geen daarvan is op ons van toepassing.'

Dat geeft hoop dat het bedrijf, dat sinds de oprichting in 2005 is gegroeid en momenteel een miljoenenomzet heeft, een andere koers vaart dan VMware, dat wordt geleid door investeerders. Maurer prijst hun activiteiten als 'zeer goede 'verkoopactiviteiten' door Broadcom', doelend op Broadcom's omzetting van VMware-producten naar een duur abonnementsmodel.

Het volgende artikel gaat dieper in op de wereld van Proxmox en laat zien hoe zoekende VMware-ESXi-gebruikers hun virtuele machines comfortabel kunnen veiligstellen in de relaxte Proxmox-wereld. Als je gewoon op zoek bent naar een alternatief voor de desktopvirtualisatie die je tot nu toe hebt gebruikt, heb je niet alles nodig wat dat artikel laat zien. Maar het kan ook geen kwaad.



www.ct.nl/softlink/2407082

Nieuwe Intel Xeon E-2400 servers van GIGABYTE



GIGABYTE lanceert servers aangedreven door Intel Xeon E-2400 processors en deelt updates voor de ondersteuning van 5e generatie Intel Xeon schaalbare processors

Giga Computing, een dochteronderneming van GIGABYTE, heeft een geavanceerde serie servers gepresenteerd die geoptimaliseerd zijn voor de Intel Xeon E-2400 processors. Deze servers leveren essentiële rekenkracht en zorgen voor een betrouwbare workload voor een breed scala aan enterprise- en edge computing-toepassingen – voor een indrukwekkende prijs-prestatieverhouding.

EEN NIEUWE STANDAARD

De nieuwe servers zijn ontworpen om volledig gebruik te maken van de mogelijkheden van Intel Xeon E-2400 processors. De line-up omvat de E133-X10 short depth server, op maat gemaakt voor compacte installaties om te voldoen aan de vereisten voor edge-computing.

Daarnaast zijn de R133-X10, R133-X11 en R133-X13 rackservers ontworpen voor uiteenlopende toepassingen. Met configuraties met dubbele 10GbE LAN-poorten en dual-slot-gpu's, voldoen deze servers aan een diversiteit aan budgettaire overwegingen en prestatievereisten.

DE KRACHT VAN INTEL XEON E-2400

De Intel Xeon E-2400 processors bieden verbeterde prestaties dankzij 8, 6 of 4 cores met snelheden tot 5,6 GHz. Ze ondersteunen 128 GB DDR5-4800 geheugen en hebben ECC-ondersteuning. Deze processors bieden veel uitbreidingsmogelijkheden met 16 PCIe 5.0-lanes voor gpu's. Daarnaast beschikken de processors over maximaal 24

PCIe 4.0-lanes voor extra apparaten. Vier lanes zijn direct verbonden met de cpu, de overige 20 lanes zijn gekoppeld aan de platform controller hub.

Intel Xeon E-2400 processors hebben de nieuwste Intel Server Platform Services (Intel SPS) 6 firmware, inclusief Intel Node Management-ondersteuning, wat een efficiënt en veilig serverbeheer mogelijk maakt.

NIEUWE PRODUCTLIJN

GIGABYTE's nieuwste serverproductlijn is ontworpen voor ongeëvenaarde prestaties en betrouwbaarheid. Door de kracht van de nieuwe Intel Xeon E-processors in te zetten, kunnen bedrijven de servers gebruiken om hun rekencapaciteiten te verhogen, waardoor ze efficiënter en productiever werken.

De E133-X10 short-depth edge-server is ideaal voor toepassingen die een compacte, krachtige serveroplossing vergen. De E133-X10 levert uitzonderlijke prestaties met Xeon E-2400 processors met een maximale TDP van 95 W. De E133-X10 is perfect voor allerlei edge-computing toepassingen.

De R133-X10, R133-X11 en R133-X13 rackservers vormen de kern van het serveraanbod van GIGABYTE. De servers zijn ontworpen voor veelzijdigheid in verschillende toepassingen. Ze bieden een scala aan serverconfiguraties. De R133-X10, R133-X11 en R133-X13 zijn budgetvriendelijk en geoptimaliseerd voor processors met een TDP van 95W. Dit zorgt ervoor dat bedrijven superieure verwerkingskracht kunnen krijgen zonder de grote investeringen, waardoor ze

ideaal zijn voor kleine en middelgrote bedrijven die hun IT-infrastructuur willen optimaliseren.

De R123-X00 en R113-X30 rackservers bieden kosteneffectieve en kortere chassis-infrastructuur opties voor bedrijven met een krappere budget. Ze garanderen 24/7 betrouwbaarheid op serverniveau met essentiële prestaties ter ondersteuning van bedrijfsbehoeften zoals webhosting, gegevensopslag en inzet in kleine en middelgrote ondernemingen. Het MX34-BS0-moederbord is niet alleen ontworpen voor gebruik met de R113-X30, maar biedt ook allerlei extra aangepaste opties voor het selecteren van IT-infrastructuur.

UPDATES VOOR DE NIEUWSTE GENERATIE

Tegelijkertijd met de lancering van de 5e generatie Intel Xeon Scalable-processors, zal GIGABYTE software-updates uitrollen voor de bestaande 4e generatie Intel Xeon Scalable-processors productlijn. Gebruikers kunnen op de desbetreffende productpagina's het nieuwe BIOS eenvoudig downloaden om hun producten bij te werken en om ondersteuning voor 5e generatie Intel Xeon Scalable-processors toe te voegen. Bovendien krijgen ze daarmee toegang tot nieuwe functies.

GIGABYTE's toewijding aan innovatie en hoogwaardige producten wordt weerspiegeld in deze serverproducten, die nieuwe standaarden stellen voor prestaties en efficiëntie in de serverindustrie. Terwijl bedrijven zich blijven ontwikkelen en nieuwe technologieën omarmen, blijft GIGABYTE voorop lopen en betrouwbare oplossingen bieden die organisaties in staat stellen hun doelen te bereiken.



De GIGABYTE E133-X10 server is ideaal voor toepassingen die een compacte, krachtige serveroplossing vereisen. De E133-X10 levert uitzonderlijke prestaties dankzij de Intel Xeon E-2400-processor en is perfect voor allerlei edge-computing toepassingen.



De GIGABYTE R133-serie rackservers zijn ontworpen voor een veelzijdigheid van verschillende toepassingen en zijn verkrijgbaar in een reeks configuraties, inclusief functies zoals snelle netwerkverbindingen en gpu-ondersteuning. Het zijn krachtige maar budgetvriendelijke servers, ideaal voor het MKB.



De R123-rackserver biedt een kosteneffectieve oplossing voor bedrijven met een krappere budget. Ze garanderen 24/7 betrouwbaarheid op serverniveau met essentiële prestaties ter ondersteuning van bedrijfsbehoeften zoals webhosting, gegevensopslag en inzet in kleine en middelgrote ondernemingen.



Illustratie Collage c't

MULTITALENT

Aan de slag met Proxmox Virtual Environment

Proxmox Virtual Environment is een krachtige en veelzijdige virtualisatieomgeving die je eenvoudig beheert via een webinterface. Lees hoe je Proxmox inricht, virtuele machines aanmaakt of bestaande importeert en waarop je moet letten om het productief te gebruiken.

Peter Siering en Marco den Teuling



Hoe begin ik met Proxmox, past het bij onze behoeften, hoe verplaats ik virtuele machines? Dat zijn vragen die gebruikers zich de afgelopen tijd gesteld zullen hebben, van de gezinsbeheerder en de test-administrator tot de technisch manager van een IT-team. Het opensource virtualisatieplatform Proxmox is onder geïnteresseerden al lang geen geheimtip meer. Sinds Broadcom, de nieuwe eigenaar van VMware, de gratis versie van de vSphere-hypervisor (VMware ESXi) stopzette staat het extra in de belangstelling. Zelfs buiten thuis- en testomgevingen voelen klanten zich beperkt door de herstructurering van het licentie- en productlandschap bij VMware en zijn ze op zoek naar alternatieven.

Overstappen naar Proxmox is een voor de hand liggende keuze omdat dat virtualisatieplatform inmiddels beproefd is en weinig te wensen overlaat als het aankomt op reguliere virtualisatie. Toepassingsgebieden en de benodigde hardwareconfiguraties variëren van een handvol virtuele machines op een mini-pc om Linux-distributies te testen tot virtuele machineparken op een hyperconvergent cluster in een datacenter waarop honderden productieve systemen draaien.

Wij gebruiken een virtualisatieomgeving bijvoorbeeld om malware te analyseren in een geïsoleerde Windows-machine of een Kubernetes-cluster te draaien op een netwerk van virtuele Linux-machines. Privé gebruiken we het voor allerlei taken, van smarthomebesturing tot VPN-server. Op professioneel vlak mis je bij Proxmox wellicht het automatisch verdelen van virtuele machines over een cluster afhankelijk van de belasting van de individuele nodes, en ondersteuning voor enterpriseback-ups zoals Veeam. Maar de meeste lezers zijn waarschijnlijk geïnteresseerd in Proxmox om van één computer er meerdere te maken – meestal op een aparte machine die via het netwerk beheerd kan worden.

In dit artikel zullen we ons daarom eerst concentreren op het installeren op een enkele computer. We leiden je door de webinterface en laten zien hoe je virtuele machines kunt maken, importeren en back-uppen. Dat is voldoende om vertrouwd te raken met het virtualisatieplatform. Als je grotere plannen hebt, kun je meerdere Proxmox-nodes koppelen om een cluster te vormen.

PROXMOX INSTALLEREN

Download eerst een installatiemedium van de downloadsectie van de Proxmox-website en schrijf het naar een usb-stick met behulp van een toepassing zoals Etcher (alle hulpmiddelen en downloads zijn te vinden bij de link op de laatste pagina van dit artikel). Je kunt Proxmox en zijn kernel ook installeren vanuit de Proxmox-repository op een Debian-systeem. Dat is bijvoorbeeld handig als je Proxmox wilt installeren bij een cloudprovider die het zelf niet aanbiedt.

In principe heeft Proxmox geen hoge systeemeisen. Voor testdoeleinden heb je genoeg aan 1 GB RAM en een 64-bit cpu met Intel VT- of AMD-V-functies, die ook geactiveerd moeten zijn in het UEFI-BIOS. Als je meerdere virtuele machines wilt draaien, heb je meer RAM nodig. Om apparaten zoals een grafische kaart door te geven aan een virtuele machine (PCIe-passthrough), moeten de cpu en het moederbord geschikt zijn voor IOMMU-mapping (I/O Memory Management Unit). Virtuele machines en Proxmox zelf profiteren van snelle ssd-massaopslag. Een tweede computer waarop je Proxmox Backup Server installeert wordt aanbevolen voor het back-uppen van je virtuele machines, maar daarover later meer.

Sluit een monitor, muis en toetsenbord aan op de Proxmox-host en verbind die met een netwerk waar je vanaf een andere machine toegang toe hebt. Na het opstarten vanaf de usb-stick word je begroet door de grafische installatiewizard. Accepteer de licentieovereenkomsten en selecteer vervolgens een schijf voor de installatie. Als je maar één schijf hebt die zowel Proxmox zelf als virtuele machine- en containerimages herbergt, moet je dan een belangrijke beslissing nemen.

Standaard claimt het installatieprogramma de hele schijf en stelt die in als een fysiek volume voor Linux' eigen Logical Volume Manager (LVM). Dat wordt verdeeld in de logische volumes root, swap en data. De rootpartitie wordt geformatteerd met ext4. Het datavolume gebruikt LVM-thin om ruimtebesparende snapshots mogelijk te maken.

We raden die methode aan voor de meeste gebruikers die Proxmox thuis gebruiken. Als je een cluster wilt maken van meerdere Proxmox-nodes, gebruik dan ZFS. Dat is een voorwaarde voor zogenaamde storage-replication tussen Proxmox-nodes. Snapshots van de gastsystemen worden daarbij opgeslagen op andere nodes. Dat verkort het migreren van een virtuele machine van enkele minuten tot enkele seconden. Natuurlijk kun je ook achteraf meer opslagruimte toevoegen en die instellen voor ZFS. Houd er rekening mee dat ZFS graag meer RAM gebruikt. De Proxmox-ontwikkelaars raden ten minste 8 GB aan.

Bij de volgende stap moet je het land, de tijdzone en de toetsenbordindeling opgeven als het installatieprogramma dat niet zelf heeft kunnen bepalen. Vervolgens geef je een e-mailadres en wachtwoord op voor de rootgebruiker, waarmee je standaard op de webinterface en via SSH inlogt. Het installatieprogramma moet Proxmox een ip-adres hebben gegeven via DHCP. Zo niet, pas dan nu de netwerkconfiguratie aan. Je moet voor de Proxmox-host een vast ip-adres instellen of in je router reserveren. We gaan er hier vanuit dat de hostnaam van je Proxmox-node `pve` is.

Controleer de samenvatting bij de laatste stap en start dan het installeren. Na een herstart toont Proxmox de url van zijn webinterface, bijvoorbeeld `https://192.168.1.90:8006`. Hier is de interface standaard Engelstalig, maar andere talen zoals Frans en Duits zijn beschikbaar – al is Engels sowieso handiger als je op internet naar informatie zoekt.

Open vanaf een ander apparaat in het netwerk dat adres in een browser, bevestig de uitzondering voor het zelfondertekende certificaat en log vervolgens in als root. Als de pagina niet toegankelijk is, is er waarschijnlijk een probleem met de netwerkconfiguratie. Een blik op `/etc/network/` interfaces en de Proxmox-documentatie (zie de link) kan helpen bij het oplossen van het probleem.

WEBINTERFACE

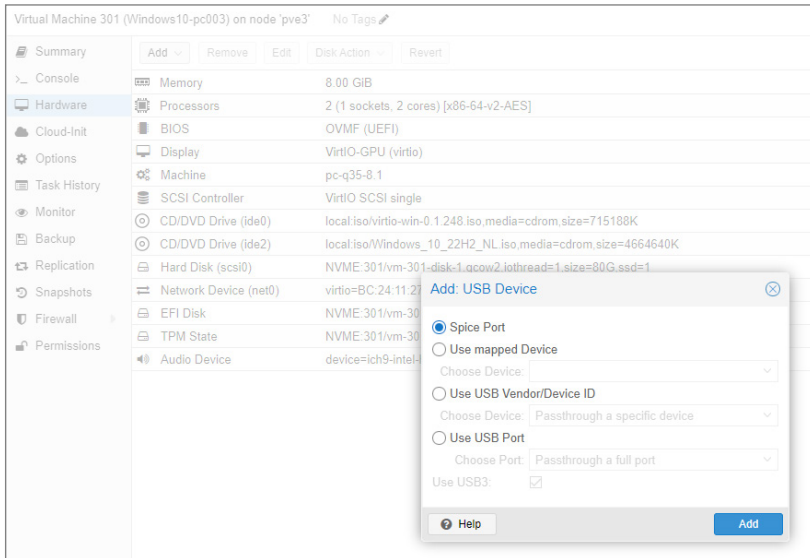
De Proxmox-webinterface bestaat uit vier gebieden. Gebruik de header bovenaan om gastsystemen aan te maken, persoonlijke instellingen te wijzigen en de node af te sluiten. Aan de linkerkant vind je een boomstructuur, die Proxmox de Resource Tree noemt, met alle computerbronnen. Het bovenste niveau is het datacenter of cluster, als je er een hebt opgezet. Op nodeniveau worden het netwerk, de opslagpools, virtuele machines en containers weergegeven. In eerste instantie bestaat je datacenter uit slechts één node, genaamd `pve`.

In het midden van de webinterface bevindt zich een dynamisch gebied dat informatie toont over de geselecteerde objecten. Het logpanel onderaan het venster geeft een overzicht van de lopende en al voltooide

The screenshot shows the Proxmox web interface for node 'pve'. The 'Status' section displays a warning: 'You get updates for Proxmox VE. The no-subscription repository is not recommended for production use.' Below this, the 'APT Repositories' section is active, showing a table of configured repositories.

Enabled	Types	URLs	Suites	Components	Options	Origin	Comment
File: /etc/apt/sources.list (4 repositories)							
<input checked="" type="checkbox"/>	deb	http://ft.p.debian.org/debian	bookworm	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	http://ft.p.debian.org/debian	bookworm-updat	main contrib		Debian	
<input checked="" type="checkbox"/>	deb	http://security.debian.org	bookworm-security	main contrib		Debian	security updates
<input checked="" type="checkbox"/>	deb	http://download.proxmox.com/debian/pve	bookworm	pve-no-subscription		Proxmox	
File: /etc/apt/sources.list.d/ceph.list (1 repository)							
<input checked="" type="checkbox"/>	deb	https://enterprise.proxmox.com/debian/ceph-quincy	bookworm	enterprise		Proxmox	
File: /etc/apt/sources.list.d/pve-enterprise.list (1 repository)							
<input checked="" type="checkbox"/>	deb	https://enterprise.proxmox.com/debian/pve	bookworm	pve-enterprise		Proxmox	

Proxmox is in principe gratis voor iedereen. Als je niet wilt betalen voor Enterprise-repository's, die intensiever geteste pakketten bevatten, moet je genoeg nemen met community-repository's.



Flexibele virtualisatiemogelijkheden: via het menu Hardware kun je onder meer usb-poorten en -apparaten of PCI-apparaten van de host (zoals een grafische kaart) aan een virtuele machine toevoegen.

taken. Een taak kan bijvoorbeeld een back-up of het herstarten van een virtuele machine zijn.

Na het inloggen waarschuwt Proxmox dat je geen abonnement afgesloten hebt. Met die ondersteuningsabonnementen, die in de goedkoopste Community-versie 110 euro per cpu-socket per jaar kosten, kan Proxmox het project verder ontwikkelen en krijg je toegang tot de Enterprise-repository's. Die bevatten pakketten die intensiever getest zijn. Professionele ondersteuning is beschikbaar vanaf 340 euro per jaar.

Als je Proxmox zonder supportabonnement gebruikt, moet je de Enterprise-repository's omruilen voor de Community-versies om updates te ontvangen. Navigeer op nodeniveau naar het menu Repositories onder Updates en deactiveer de repository's `pve` en `ceph-quincy` van `enterprise.proxmox.org`. Klik vervolgens op de knop Add. Er wordt een venster geopend waarin Proxmox opnieuw een abonnement aanbeveelt. Sluit het venster niet, maar bevestig met OK. Voeg vervolgens de repository No-Subscription toe in het vervolkeuzemenu.

Updates voor Proxmox VE kunnen worden geïnstalleerd via het menu Updates. Alle functies die in dit artikel worden uitgelegd via de Proxmox-webinterface hebben een equivalent op de commandline (zie de link op de laatste pagina).

OPSLAGRUIMTE

De resource-tree toont ten minste twee lokale storage-pools onder de pve-node, die verschillende taken vervullen. Als je voor LVM hebt gekozen tijdens het installeren, worden ze `local` en `local-lvm` genoemd. Proxmox heeft een hele reeks opslagplug-ins en onderscheidt opslag op bestands- of blokniveau (zie de link).

De lokale opslag is van het type directory, werkt op bestandsniveau en is bedoeld voor ISO-images, containersjablonen en lokale back-ups. Daarentegen is `local-lvm` een blokopslag voor de schijven van de virtuele machines en containers. Als je voor ZFS hebt ge-

kozen, staan daar `local` en `local-zfs`, die op bestands- en blokniveau werken.

Je kunt het menu Storage gebruiken (op Datacenter-niveau) om op elk moment extra opslagruimte toe te voegen, zoals remote SMB/CIFS- of NFS-shares, voor back-ups en andere content.

VIRTUELE MACHINES MAKEN

Verplaatst een ISO-bestand naar de lokale opslag om het te gebruiken als installatiemedium voor een virtuele machine. Je kunt het uploaden vanaf je lokale computer, downloaden vanaf een url of `scp` gebruiken om het te verplaatsen naar de directory `/var/lib/vz/template/iso`. Je kunt om mee te beginnen bijvoorbeeld Ubuntu Server 22.04 gebruiken als gastsysteem.

Klik op de knop 'Create VM' in de header om een wizard te openen die je begeleidt bij het maken van de virtuele machine. Geef de machine een naam, bijvoorbeeld `ubuntu-jammy-server`, en een VM-ID. Je hebt die ID nodig voor back-ups of wanneer je virtuele machines aanpast met de Proxmox-commandlinetools. Het is het beste om in een vroeg stadium na te denken over een schema voor het toewijzen van ID's, bijvoorbeeld 300 tot 400 voor virtuele testmachine's en 800 tot 900 voor productieve werking. Selecteer op het tabblad OS het ISO-bestand op de betreffende opslag als virtuele installatieschijf voor de virtuele machine en pas de overige instellingen toe. Je hoeft bij System niets aan te passen.

Indien mogelijk moet je het vakje voor de QEMU Agent altijd aanvinken en die tool later op het gastsysteem installeren. Hoe royaal je de virtuele machine voorziet van cpu, opslagruimte en geheugen hangt af van je hardware en geplande werkbelasting. Bij de optie Type onder CPU moet je een afweging maken tussen de gewenste prestaties en compatibiliteit. Het type `host`, ook bekend als `cpu passthrough`, is performanter dan een generieke cpu zoals `x86-64-v2-AES`. Dat kan echter tot problemen leiden als je virtuele machines in een cluster wilt migreren tussen nodes met verschillende processors. Op het tabblad Memory kun je de geavanceerde opties gebruiken om een minimale hoeveelheid geheugen op te geven naast het maximale geheugen. Tot slot vat de wizard de configuratie van de virtuele machine nogmaals samen.

Selecteer de virtuele Ubuntu-machine in de resource-tree en start hem. Klik op Console om VNC (Virtual Network Computing) te openen, dat dient als venster voor de machine en toetsenbord invoer doorgeeft wanneer het venster de focus heeft.

Na het installeren van een gastsysteem moet je de QEMU Agent achteraf installeren. Bij Ubuntu installeer je het pakket `qemu-guest-agent`:

```
sudo apt update
sudo apt install qemu-guest-agent
```

Afhankelijk van de distributie moet je er vervolgens voor zorgen dat de agent start bij het opstarten van het systeem:

```
sudo systemctl enable qemu-guest-agent
sudo systemctl start qemu-guest-agent
```

Bij een Debian-gastsysteem kun je die stap overslaan.

Proxmox toont dan het (de) ip-adres(sen) van de virtuele machine in het menu Summary. Het sluit virtuele machines met de guest-agent ook op een nette manier af en bereidt ze voor op back-ups en snapshots.

Om het installatieproces niet steeds opnieuw te hoeven doorlopen, bijvoorbeeld voor Ubuntu Server, kun je virtuele machines klonen of omzetten in sjablonen. Proxmox maakt onderscheid tussen volledige en gekoppelde klonen. Die laatste besparen opslagruimte, maar kunnen niet gebruikt worden over nodes heen omdat ze toegang vereisen tot de lokale opslag met de virtuele harde schijf.

De Proxmox-documentatie adviseert om virtuele machinesjablonen vrij te houden van gebruikersgegevens (zie de link). We hebben eerder beschreven hoe gastsystemen vooraf geconfigureerd kunnen worden met cloud-init en hoe je kunt voorkomen dat virtuele machines van sjablonen hetzelfde ip-adres krijgen als het sjabloon [1].

VIRTUELE WINDOWS-MACHINES

Bij de wizard voor het maken van virtuele machines moet je voor virtuele Windows-machines het type Microsoft Windows selecteren op het tabblad OS. In tegenstelling tot de meeste Linux-distributies, die stuurprogramma's voor paravirtualisatie van apparaten (VirtIO) bevatten en automatisch laden, moet je die voor virtuele Windows-machines apart installeren.

Het Fedora-project levert een ISO-image met opensource, ondertekende VirtIO-stuurprogramma's en de QEMU guest-agent (zie de link). Bewaar dat ISO-bestand in de local-storage en geef het door aan de virtuele machine. Je kunt dat meteen doen bij het maken van de virtuele machine door op het tabblad OS het vakje 'Add additional drive for VirtIO drivers' aan te vinken, of je doet dat achteraf via het menu Hardware. Vervolgens installeer je de stuurprogramma- en toolverzameling in Windows.

Voor virtuele Windows 11-machines moet je bij System ook OVMF (UEFI) selecteren in plaats van SeaBIOS en een TPM (Trusted Platform Module) en EFI Storage toevoegen. Zorg ervoor dat de installatie-ISO de hoogste prioriteit heeft bij de opstartvolgorde wanneer je voor de eerste keer opstart. Je kunt dat na het maken van de virtuele machine aanpassen bij het menu Options onder 'Boot order'.

VIRTUELE MACHINES IMPORTEREN VANUIT ESXI

Er zijn verschillende manieren om virtuele machines van een VMware ESXi-host te migreren naar Proxmox. Wat ze gemeen hebben is dat je 'verhuisdozen' moet inpakken voor de overdracht door gemounte ISO-bestanden uit te werpen, VMware-hulpprogramma's te verwijderen en de virtuele machines af te sluiten.

VMware biedt de commandolinetool `ovftool` voor het overhuizen, die je ook rechtstreeks op de Proxmox-node kunt uitvoeren. Dat bespaart bijvoorbeeld de omweg via een netwerkshare. We moesten een gratis VMware-account maken voor het downloaden. Zet het installatieprogramma op de Proxmox-node via `scp`, maak het daar uitvoerbaar en installeer `ovftool`:

```
chmod +x ./VMware-ovftool-4.6.2-22220919-lin.x86_64.bundle
./VMware-ovftool-4.6.2-22220919-lin.x86_64.bundle
```

Gebruik het volgende commando om virtuele machines als OVF-pakketten op te halen uit de ESXi-datastore:

```
ovftool vi://root@192.168.1.10/vm /var/lib/vz/template/iso
```

Vervang in het bovenstaande commando het ip-adres door dat van je ESXi-instantie en de generieke naam `vm` door de naam van je virtuele machine. Je kunt de importmap vrij kiezen, dit voorbeeldcommando gebruikt de standaardmap voor ISO-bestanden.

Virtualisatie light

Naast virtuele machines heeft Proxmox ook Linux-containers (LXC) als tweede virtualisatiemethode. Bij 'volwaardige' virtuele machines draait elk besturingssysteem zijn eigen kernel en, afhankelijk van de configuratie, moeten ook apparaten geëmuleerd worden. Containers delen de kernel daarentegen met de host. Dat vermindert de overhead en zorgt voor snellere opstarttijden. Verwar Linux-containers echter niet met Docker of andere OCI-containers (Open Container Initiative).

In zijn begin dagen was Docker gebaseerd op LXC, beide gebruiken nog steeds dezelfde kernelfuncties om containers te realiseren, maar ze vervullen verschillende toepassingsdoeleinden. Docker-images worden bewust klein gehouden en zijn ontworpen om slechts één applicatie in

de container te draaien. Linux-containers zijn juist bestemd als vervanging voor een compleet systeem. Daarom worden ze ook wel onderscheiden als applicatie- en systeemcontainers. Je vindt in een Linux-container alle diensten en toepassingen die je zou verwachten van een Linux-systeem.

Praktisch is dat Proxmox wordt geleverd met een grote voorselectie aan containersjablonen die je naar de local-storage kunt downloaden via het menu CT Templates. Je vindt daar veel populaire Linux-distributies en images van `turnkeylinux.org`. Laatstgenoemde bevatten net als Docker-containers al een applicatie zoals WordPress of een database zoals PostgreSQL.

Je kunt containers maken met de knop 'Create CT' in de header. Vanwege de ge-

meenschappelijke kernel zijn containers minder afgeschermd van de host dan virtuele machines.

Om te voorkomen dat een gecompromitteerd proces schade aanricht op de host moet je zoveel mogelijk kiezen voor unprivileged containers. Die zetten de user-ID 0 van de rootgebruiker in de container buiten de container om naar de user-ID van een gebruiker zonder privileges. Containers profiteren net als virtuele machines van Proxmox-functies zoals replicatie, migratie en high-availability en maken gebruik van dezelfde bronnen, bijvoorbeeld de netwerkconfiguratie.

Docker moet je nooit rechtstreeks op de Proxmox-host installeren, maar je kunt wel een virtuele machine als Docker-host gebruiken.

Navigeer naar de importmap en importeer de virtuele machine in Proxmox:

```
qm importovf 301 vm.ovf local-lvm
```

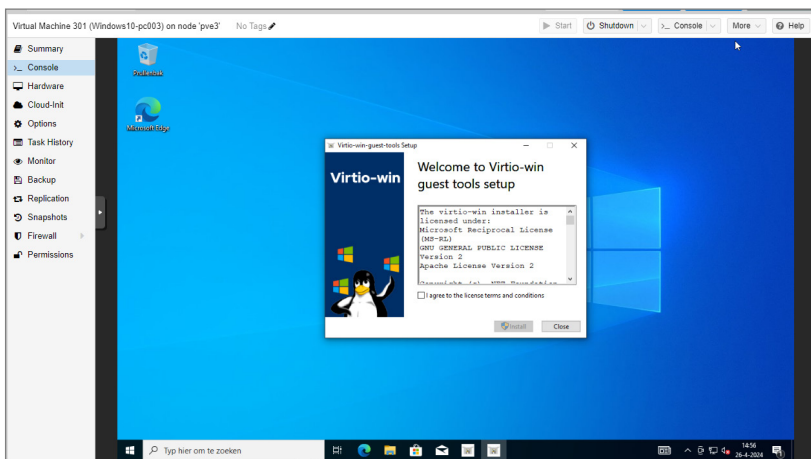
Vervang de VM-ID 301 door de gewenste VM-ID en pas de naam van het OVF-bestand aan. Je moet ook een opslag definiëren voor de virtuele harde schijf van de virtuele machine, bijvoorbeeld local-lvm. De geïmporteerde machine verschijnt dan in de resource-tree. Je kunt het OVF-bestand dan verwijderen.

Voordat je de virtuele machine de eerste keer start, moet je die voorbereiden. Dat hangt af van hoe je de virtuele machine in ESXi geconfigureerd hebt. Na een overdracht van Ubuntu Server 22.04 moesten we de firmware veranderen van SeaBIOS naar OVMF, een EFI-schijf toevoegen, een netwerkkaart (VirtIO) toevoegen en de SCSI-controller wijzigen in VirtIO SCSI single.

De virtuele machine kreeg via DHCP pas een ip-adres nadat we de nieuwe netwerkinterface met de naam enp0s19 hadden ingevoerd in het bestand /etc/netplan/00-installer-config.yaml in Ubuntu. Je moet ook altijd de QEMU guest-agent installeren en het bijbehorende vakje aanvinken bij de virtuele-machine-configuratie.

Kort voor de deadline hebben de Proxmox-ontwikkelaars een experimentele wizard voor virtuele-machinemigratie vanuit ESXi geïntegreerd in de Proxmox-webinterface. Daarvoor moet je je ESXi-datastore integreren in het menu Storage, zodat Proxmox het aanspreekt via de ESXi-API.

Selecteer vervolgens op een lijst de virtuele machine's die moeten worden geïmporteerd. Je moet hun configuratie grondig controleren en eventuele fouten eruit halen voordat je de overdracht start. Tijdens een testrun wees de wizard bijvoorbeeld vier cpu-sockets toe aan een virtuele Windows 11-machine, hoewel het vier cpu-cores hadden moeten zijn. Sommige gebruikers melden op het Proxmox-forum ook problemen met een snelheidsbeperking tijdens bulkimports. Bij de geavanceerde hostinstellingen van ESXi kun je de limiet van gelijktijdige verbindingen verhogen door de waarde bij `Config.HostAgent.vmacore.soap.maxSessionCount` te verhogen of door een 0 in te stellen om rate limiting uit te schakelen.



Voor Windows zijn in Proxmox wat extra handelingen vereist. Stuurprogramma's voor VirtIO installeer je vanuit een ISO-bestand in de virtuele machine.

Voor de nazorg gelden dezelfde tips als bij het conventioneel importeren van virtuele machines met `ovf-tool`. Meer informatie daarover is te vinden in de Proxmox-documentatie en op het communityforum.

PROXMOX-CLUSTER

In een productieve omgeving is het zinvol om meerdere Proxmox-nodes te combineren tot een cluster om virtuele machines te verdelen. Proxmox slaat de configuraties van de virtuele machines dan op in het pmxcfs-clusterbestandssysteem en synchroniseert de gegevens via het corosync-clusterprotocol. Om dat te laten werken, moeten de nodes elkaar kunnen bereiken via UDP-poorten 5405 tot 5412 voor corosync en poort 22 voor SSH.

Voor High Availability (HA), oftewel het automatisch overzetten van een virtuele machine als een node uitvalt, zijn ten minste drie nodes in het cluster nodig zodat ze het eens kunnen worden over een gemeenschappelijke procedure. Het is echter mogelijk om een extern QDevice (Quorum Device) te integreren, bijvoorbeeld een Raspberry Pi met stemautorisatie (zie de link). Omdat corosync allergisch is voor hoge latency's, kun je het clusterverkeer het beste routeren via een tweede netwerkkaart over een apart netwerk.

Bij een testrun hebben we drie Proxmox-nodes met ZFS-opslag bekabeld om een cluster te vormen. Je maakt het cluster aan via de webinterface in het gelijknamige menu op datacenterniveau. Controleer vooraf of de ip-adressen en hostnamen van alle nodes kloppen, aangezien die niet meer gewijzigd kunnen worden na toetreding tot het cluster. Na het aanmaken van het cluster toont Proxmox bij 'Join Information' informatie die je kunt doorgeven aan de andere kandidaten in het Cluster-menu. Die andere kandidaten mogen bij het toevoegen nog geen gastsystemen bevatten.

Voor het opzetten van gedistribueerde opslag met Ceph wordt netwerkhardware vanaf gigabit-ethernet aanbevolen. Om redundantie in het cluster te garanderen, zelfs zonder Ceph, kun je snapshots van virtuele machines op andere nodes bewaren (ZFS-replicatie). Dat verkort de migratietijd tussen twee nodes van enkele minuten naar enkele seconden. Navigeer daarvoor naar het menu Replication. Daar geef je een of meer doelnodes op en configureer je een interval waarmee Proxmox het volume van de virtuele machine synchroniseert. Na de eerste volledige synchronisatie worden de volgende keer alleen de wijzigingen in de gegevensstatus, ook wel delta genoemd, overgedragen.

Het feit dat je cluster voldoet aan alle eisen voor de high-availability modus (zie de link op de volgende pagina) betekent niet dat het cluster automatisch resources migreert zodra een node offline is. Daarvoor moet je de virtuele machines of containers onder de bescherming plaatsen van de High Availability Manager (`ha-manager`). Dat kan via de webinterface in het menu HA op datacenterniveau, waar je ook kunt zien of er een werkend quorum is, dus of het cluster een quorum heeft. Activeer de HA-modus via de knop Add voor alle bronnen die je tegen uitval wilt beschermen.

Afhankelijk van de werklast en het doel van de virtuele machine, kan het nuttig zijn om de gewenste status aan te passen, bijvoorbeeld started of stopped, evenals het maximale aantal pogingen tot herstarten en migreren (max. Relocate).

Als je Proxmox professioneel gebruikt, moet je er rekening mee houden dat echte high-availability ook de juiste hardware en infrastructuur vereist, zoals redundante voedingen en fail-overnetwerken. De meeste thuisgebruikers hebben waarschijnlijk genoeg aan een Proxmox-host en een back-upoplossing van waaruit de virtuele machines kunnen worden hersteld.

BACK-UPS

Met `vzdump` heeft Proxmox VE een eenvoudige en degelijke back-uptool die je kunt configureren via de webinterface of de commandline. Hij werkt goed, maar legt alle gegevens van een virtuele machine vast, dus het maakt elke keer een volledige back-up. Dat kan goed werken voor opstellingen met een paar of kleinere virtuele machines. Als je echter veel virtuele machines draait of meerdere back-ups tegelijk wilt bewaren, wordt de opslagruimte op een gegeven moment waarschijnlijk schaars.

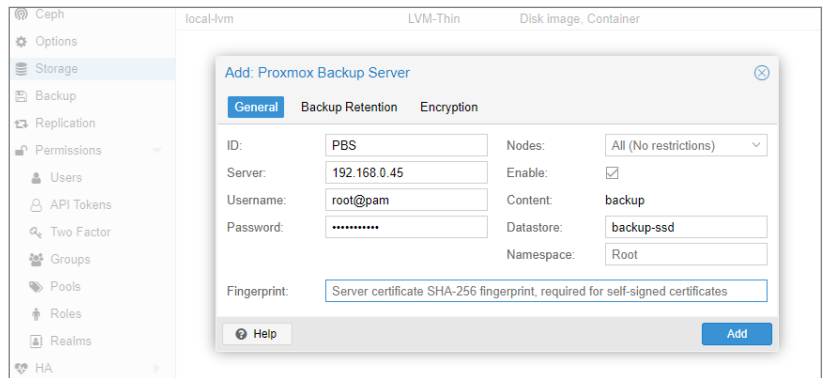
Een populaire bestemming voor `vzdump`-back-ups zijn SMB/CIFS- of NFS-shares, bijvoorbeeld op een NAS. Om dat te doen, voeg je de netwerkshare toe als bestemming in het menu Storage door op Add te klikken. Voor een NFS-share moet je een naam (ID) toewijzen, het ip-adres van de server invoeren en de geëxporteerde share, bijvoorbeeld `/mnt/backups`. Gebruik het vervolgkeuzemenu Content om de share te selecteren als bestemming voor 'VZDump backup file'. Back-uptaken, oftewel wanneer back-ups worden gemaakt van welke machine en hoe lang ze worden bewaard, worden geconfigureerd in het menu Backup in de Proxmox VE webinterface.

Proxmox maakt onderscheid tussen de back-up-modi Snapshot, Suspend en Stop voor virtuele machines. Die laatste voorkomt inconsistente gegevens, maar veroorzaakt downtime omdat de machine na het back-uppen moet worden afgesloten en opnieuw opgestart. De snapshotmodus werkt tijdens gebruik. Als de QEMU guest-agent draait, vermindert dat het risico op inconsistente gegevens. De ontwikkelaars raden de suspend-modus af, die is er alleen om compatibiliteitsredenen.

Een aparte Proxmox Backup Server, die je op een andere computer installeert, biedt meer functies dan lokale of NAS-back-ups met `vzdump`, zoals ruimtebesparende deduplicatie, incrementele back-ups en het herstellen van individuele bestanden. Je kunt het ISO-bestand gratis downloaden van de website van Proxmox.

Het installeren werkt op dezelfde manier als bij Proxmox VE en de back-upserver heeft ook een eigen webinterface voor beheer. Als eerste stap kun je overschakelen naar de community-repository's zoals bij Proxmox VE.

Als je niet afhankelijk bent van professionele functies zoals tape-archivering, hoeft je niet veel tijd te be-



Proxmox Backup Server (PBS) voeg je toe als extra storage, die je als doel voor back-ups kunt kiezen, maar het biedt veel meer functies. De fingerprint vind je in PBS.

steden aan de webinterface van Backup Server. De eenvoudigste manier om te beginnen met back-ups is om de datastore met de naam backup-data te integreren als opslag. Naast het ip-adres, de gebruikersnaam en het wachtwoord heb je ook de fingerprint van het zelfondertekende TLS-certificaat nodig. De back-upserver toont die fingerprint op het dashboard. Je kunt de back-ups aan de clientzijde versleutelen.

Back-upservers gedragen zich passief ten opzichte van je Proxmox-cluster: je configureert back-ups per virtuele machine bij de Proxmox VE-webinterface in het menu Back-ups. Proxmox VE stuurt de snapshots naar de back-upserver (push-modus). De ontwikkelaars hebben de functie voor het terugzetten van individuele bestanden van een virtuele machine verborgen in het menu Back-ups op virtuele-machineniveau. De knop voor het terugzetten van bestanden verschijnt daar alleen nadat je de back-upserver als opslag hebt geselecteerd. Je kunt ook bestanden downloaden naar je lokale machine via de bestandsbrowser.

Als je het volledige potentieel van Proxmox Backup Server wilt benutten, moet je de uitgebreide documentatie goed lezen. Het goedkoopste ondersteuningsabonnement voor Proxmox Backup Server is met 540 euro aanzienlijk duurder dan Proxmox VE. Professionele ondersteuning is beschikbaar vanaf 1040 euro per jaar.

CONCLUSIE

Je hebt de belangrijkste functies van Proxmox VE leren kennen en kunt nu aan de slag met virtualisatie. We moedigen je aan om naar hartenlust te experimenteren, want – dat is het mooie van virtuele machines – fouten kunnen meestal snel ongedaan worden gemaakt. Als je vragen hebt in de trant van 'en hoe doe ik dit of dat voor mijn specifieke toepassing', dan raden we je aan een bezoek te brengen aan het Proxmox-forum. Er is een zeer behulpzame community en veel Proxmox-ontwikkelaars zijn daar ook actief om vragen te beantwoorden. Iemand anders heeft jouw vraag misschien al eens gesteld en jij kunt profiteren van de oplossing.



www.ct.nl/softlink/2407086

Literatuur

[1] Niklas Dierking en Marco den Teuling, Infrastructuur uit code met Terraform en Proxmox, c't 10/2023, p.135



17W-PC

Bouwvoorstel voor een stille en zuinige kantoor-pc

Ons bouwvoorstel voor een kantoor-pc met een snelle Core i14000-cpu biedt ruimte aan een grafische kaart en extra opslag. We moesten ons echter in paar bochten wurmen om een laag energieverbruik voor elkaar te krijgen.

Christian Hirsch en Alieke van Sommeren

We bekijken bij het samenstellen van onze bouwvoorstellen welke functies belangrijk zijn en welke programma's je op een desktop-pc voornamelijk gebruikt. Daaruit distilleerden we een mini-pc en een krachtige gaming-pc. Maar er is ook altijd veel vraag naar een kantoor-pc in een standaard formaat behuizing.

Het oorspronkelijke idee was om het oudere bouwvoorstel van onze 13W-pc [1] te updaten en zo veel mogelijk componenten te hergebruiken. Hij had de toen actuele hexacore Core i5-12400, 16 GB DDR4 RAM en een 1TB-ssd.

Intussen heeft Intel echter nieuwe Core i's uitgebracht en DDR5-RAM is zo goedkoop geworden dat het DDR4-RAM grotendeels vervangen heeft. Door het nieuwere geheugentype was een ander moederbord nodig. Maar dat was niet de enige verandering,

want veel oude onderdelen zijn niet meer verkrijgbaar.

De 17W-pc is aanzienlijk krachtiger: met in totaal 14 cpu-kernen en 20 threads levert de Core i5-14500 niet alleen voldoende prestaties voor teksten, tabellen en e-mails, maar ook voor zwaardere taken zoals beeld- en videobewerking. Hij wordt ondersteund door 32 GB DDR5-RAM en een ssd van 1 TB. Hij start binnen 18 seconden op naar het Windows bureaublad, heeft snel 2,5 Gbit/s ethernet en Wi-Fi 6E aan boord, en Ubuntu Linux draait er soepel op. Bij dagelijkse taken staan computers veel niets te doen, ons bouwvoorstel verbruikt dan 17 watt. De voeding van 650 watt biedt echter ook voldoende reserves voor een grafische kaart om games te spelen of AI- en videoberekeningen uit te voeren.

ZUINIG PLATFORM

Bij het kiezen van de componenten hebben we ons gericht op een zo stil en zuinig mogelijke werking omdat kantoor-pc's zo onopvallend mogelijk moeten zijn. Daarom was een Intel-processor voor ons de voor de hand liggende keuze omdat het LGA1700-platform bij gedeeltelijke belasting minder energie nodig heeft dan AMD's AM5.

De keuze voor een Core i5-14500 werd relatief vroeg gemaakt, omdat die processor slechts minimaal meer kost dan de Core i5-14400, maar met acht in plaats van vier twee keer zoveel efficiency-kernen heeft voor hogere multithreading-prestaties. Vergeleken met de Core i5-12400 van de 13W-pc reikt hij 24 procent sneller bij de renderbenchmark Cinebench R23.

Het belangrijkste werk wordt gedaan door zes performance-cores met een klokfrequentie tot 5 GHz, waardoor de cpu ook goed presteert op het gebied van singlethreaded-prestaties, wat belangrijk is voor kantoor taken. Als 65W-cpu is de Core i5 14500 relatief eenvoudig te koelen. Tijdens het turbovenster van 28 seconden kan de processor tot 154 watt verbruiken.

Het moederbord is het belangrijkste onderdeel voor veel functies van een pc. Het bepaalt het aantal, type en snelheid van de interfaces en de energie-eisen. Bij het maken van onze keuze twijfelden we tussen de Gigabyte B760M Gaming X AX en de beter uitgeruste B760M AORUS Elite AX van dezelfde fabrikant, en kozen uiteindelijk voor de goedkopere van de twee.

Het was belangrijk voor ons dat het moederbord vier DIMM-slots had, zodat we later konden upgraden. We richtten ons ook op de BIOS-flashback-functie zodat je het BIOS kunt updaten zonder cpu. Via DisplayPort 1.4 en HDMI 2.0b sluit je twee monitoren met hoge resolutie tegelijkertijd aan zonder een extra grafische kaart. De 2.5 Gbit/s netwerkpoort is snel genoeg voor glasvezelinternet en het maken van backups naar je NAS. Als alternatief kan de pc verbinding maken met een netwerk via Wi-Fi 6E. Externe ssd's en smartphones sluit je aan via een USB-C-poort aan de voorkant van de behuizing.

RAM: LIEVER STABIEL DAN SNEL

Matig snel DDR5-4800 is in dit geval voldoende omdat alleen de Core i9, Core i7 en de Core i5-14600K officieel DDR5-5600 RAM ondersteunen. Dus alleen als je een krachtigere cpu installeert is het de moeite om sneller geheugen te installeren. We raden met JEDEC compatibele modules zonder XMP-profiel aan. Overklokt geheugen vereist een hoger voltage, verhoogt de energiebehoefte en kan instabiliteit veroorzaken. Omdat de geheugeneisen van moderne software blijven toenemen, hebben we de pc 32 GB RAM gegeven.

Voor de ssd blijven we de Samsung SSD 980 met PCIe 3.0-interface gebruiken, die is beproefd en getest in onze bouwvoorstellen. Het moederbord ondersteunt ook PCI Express 4.0, maar voor kantoor toepassingen hoef je geen merkbaar snelheidsverschil te verwachten.

De behuizing blijft ook hetzelfde: de Fractal Design Define 7 Mini miditower is naar verhouding compact, voorzien van stille ventilatoren en biedt onder andere een USB-C-frontpoort. De case bestaat uit twee compartimenten. Het onderste gedeelte herbergt de voeding en twee sleuven voor 3,5-inch schijven. Het moederbord zit in het bovenste gedeelte.

Aan de achterkant van de moederbordtray kunnen twee 2,5-inch ssd's gemonteerd worden.

VOEDINGSZOEKTOCHT

We moesten voor de overige componenten op zoek naar andere oplossingen. De eerder gebruikte Scythe Mugen 5 Rev. B cpu-koeler is nieuw niet meer te koop. Daarom hebben we de koeler uit de allround gaming-pc [2] gepakt. Volgens de fabrikant is de Endorfy Fortis 5 geschikt voor maximaal 220 watt, dus hij koelt de Core i5-14500 fluisterstil en heeft genoeg reserves als je het bouwvoorstel wilt uitrusten met een krachtigere cpu.

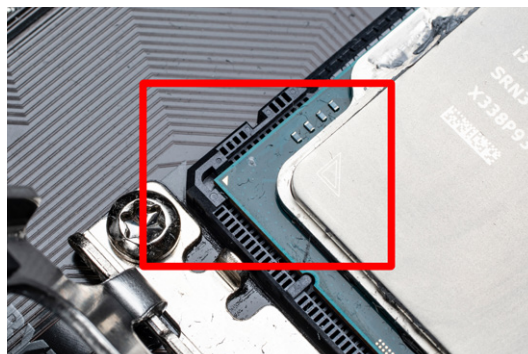
De zoektocht naar een geschikte voeding was een uitdaging. De afgelopen jaren hebben we bij onze bouwvoorstellen vaak de Seasonic Core GM-500 gebruikt, die zeer efficiënt werkt bij lagere belastingen en ook stil is. Dat zou betekenen dat dit bouwvoorstel idle slechts 13 watt zou verbruiken. Helaas heeft Seasonic de hele Core-serie stopgezet. Een opvolger zal pas aan het eind van het jaar beschikbaar zijn. Daarom hebben we verschillende voedingen uitgeprobeerd, maar we konden geen betaalbare voeding vinden die net zo zuinig en stil was.

Het best mogelijke compromis was de Seasonic G12 GM 650 Watt. Daarmee haalden we idle 16,5 watt. De ventilator maakt iets meer dan 0,1 sone geluid, maar dat is niet merkbaar – zelfs niet in zeer stille omgevingen, en zeker niet als de computer onder je bureau staat. Seasonic biedt ook een 550-watt versie uit dezelfde serie. Het prijsverschil was minimaal en dus hebben we gekozen voor de krachtigere versie. De voeding heeft voldoende reserves voor krachtigere cpu's en een grafische kaart

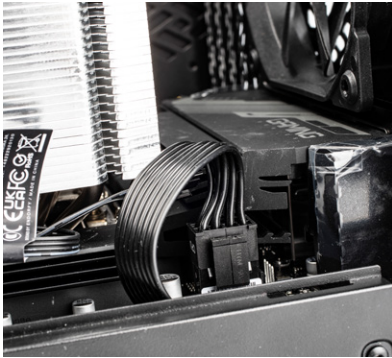
MONTAGE

Het in elkaar zetten van de 17W-pc is niet zo moeilijk zolang je de onderstaande instructies volgt. Zelfs kleine details zoals een vergeten ATX12V-plug kunnen frustratie veroorzaken als de computer de eerste keer dat je hem aanzet niet meteen opstart.

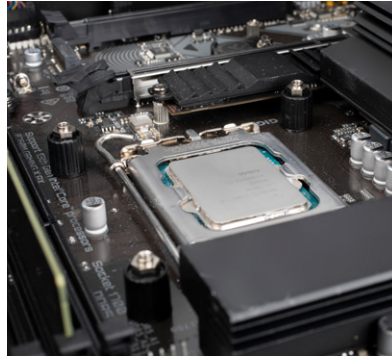
Om ervoor te zorgen dat alles soepel verloopt, moet je bij het bestellen van de onderdelen letten op de exacte productaanduidingen, zoals weergegeven in de onderdelentabel en bij de link op de laatste pagina van dit artikel. Een paar letters in de productaanduiding van het moederbord bepalen het geheugentype of een ander moederbordformaat.



De juiste uitlijning van de cpu is te herkennen aan de hoek van de heatspreider: de markering met een driehoek komt overeen met de markering in de socket.



De ATX12V-connector voor de cpu wordt vaak vergeten. Die zit wat verstopt in de bovenste hoek van het moederbord.



Zorg er bij het installeren van het montageframe van de Endorfy Fortis 5 cpu-koeler voor dat je de zwarte afstandhouders gebruikt.

Hou rekening met ongeveer een middag knutselen. Na het in elkaar zetten volgt het installeren van het besturingssysteem, de drivers en de software. Het gereedschap dat je nodig hebt zijn een kleine en een grote, liefst lange kruiskopschroevendraaier. Hoewel veel van de stappen voor zich spreken, moet je toch de instructies lezen die bij de onderdelen geleverd worden.

De eerste stap is het moederbord voorbereiden. Monteer het met het RAM, de M.2-ssd en de processor buiten de behuizing. De twee geheugenmodules gaan in de DDR5_A2- en DDR5_B2-slots. Die zijn gemarkeerd op het moederbord. Om de M.2-ssd in het M2A_CPU-slot direct naast de processor te plaatsen, moet je eerst de schroef van het koellichaam op de printplaat losdraaien. Vergeet niet de beschermfolie voor het warmtegeleidende materiaal te verwijderen voordat je het koellichaam terugplaatst.

Let er bij het plaatsen van de cpu op dat je geen van de 1700 gevoelige pinnetjes in de socket verbuigt. Draai de beugel daarvoor los zodat de socket opengaat. Laat de beschermkap op zijn plaats. Plaats vervolgens de cpu. Voor een correcte uitlijning moet de driehoek in een van de hoeken van de cpu-heat-spreader overeenkomen met de driehoek op het bevestigingsframe. Als de socket vervolgens vergrendeld is, springt de beschermkap er vanzelf af.

Bij het installeren van de cpu-koeler moet je even goed de aandacht erbij houden. Eerst moet je de backplate die bij de Endorfy Fortis 5 wordt geleverd

aan de achterkant van het moederbord bevestigen en van bovenaf vastschroeven met de vier donkerkleurige schroefbouten. Plaats vervolgens het montageframe op de bouten. Zet het vast met de vier meegeleverde schroeven. Vergeet niet de thermische pasta aan te brengen. Omdat LGA1700-processors rechthoekig zijn, raden we aan om een dunne strook langs het midden aan te brengen. De pasta wordt later verdeeld door de contactdruk van de koeler.

Nadat je de koeler met heatpipe bevestigd hebt, moet je de twee schroeven om en om vastdraaien en de ventilator bevestigen met de bevestigingsklemmen. De koeler moet vervolgens zo worden geplaatst dat de ventilator boven de geheugenmodules zit en in de richting van de I/O-aansluitingen blaast. De bijbehorende vierpolige kabel sluit je aan op de CPU_FAN-header op het moederbord.

MOEDERBORD INBOUWEN

Voordat je het moederbord, de koeler, cpu en ssd in de kast plaatst, moet je de midtower voorbereiden. Na het verwijderen van de zijpanelen, raden we aan om het deksel en de twee frames eronder te verwijderen, zoals beschreven op pagina 13 van de Define 7 Mini-handleiding. Dat maakt het daaropvolgende installeren veel eenvoudiger. Draai de twee schroeven van het voedingsdeksel los en bevestig het met vier schroeven aan de voeding. Zorg er bij het plaatsen voor dat de ventilator van de voeding naar de onderkant van de kast wijst. Er is een opening met een stoffilter.

Leg de kabels voor de 24-pins ATX-connector en de 8-pins ATX12V-connector met het label CPU achter de moederbordtray en leid ze door de uitsparingen. De ATX12V CPU-voedingsconnector zit in de linkerbovenhoek van het moederbord. Je hoeft je in ieder geval geen zorgen te maken over het I/O-panel van het moederbord, aangezien dat aan het moederbord vastzit – erg fijn. Plaats het moederbord eerst grofweg waar hij moet uitkomen. Schroef het nog niet vast, maar gebruik de ruimte om de stekkers voor de voeding, usb, audio, leds en knoppen aan te sluiten. De ventilator voor de achterste ventilator van de behuizing wordt aangesloten op de SYS_FAN3-connector in het midden van de onderrand van het moederbord. Dat is de enige manier om de ventilatorcurves op de projectpagina te volgen en de pc fluisterstil te houden. Je kunt de kabel achter de moederbordtray laten lopen.

Je hoeft de voorste ventilator in de behuizing alleen aan te sluiten als je een grafische kaart installeert. Anders zijn de koelprestaties van de achterste ventilator prima. De optionele voorste ventilator wordt aangesloten op SYS_FAN2, die verborgen zit tussen de 24-pins ATX voedingsconnector en de geheugenslots.

Draai vervolgens het moederbord vast met alle zeven schroeven en controleer alle aansluitingen nogmaals. Als je voor een grafische kaart hebt gekozen, moet je vóór het installeren de bovenste twee afdekplaatjes in de achterkant van de behuizing ver-

Bouwvoorstel 17W-pc: componenten

Component	Product	Prijs
Processor	Intel Core i5-14500 (BX8071514500)	€ 265
Cpu-koeler	Endorfy Fortis 5 (EY3A008)	€ 42
Moederbord	Gigabyte B760M Gaming X AX (B760M G X AX)	€ 160
Geheugen	2 × Crucial DIMM 16GB, DDR5-4800 (CT16G48C40U5)	€ 100
Ssd	Samsung SSD 980 1TB (MZ-V8V1T0BW)	€ 80
Voeding	Seasonic G12 GM 650W ATX (G12-GM-650)	€ 82
Behuizing	Fractal Design Define 7 Mini Black Solid (FD-C-DEF7M-01)	€ 130
	Totaal (+ verzendkosten)	€ 859 (+ € 20)

wijderen. Schroef de kaart vervolgens vast met twee kartelschroeven en sluit een of meer van de zes- of achtpins PEG-voedingsstekkers van de voeding aan. Plaats ten slotte alles in de bovenkant van de behuizing terug op zijn plek en sluit de behuizing.

LAATSTE TWEAKS

Als je alle stappen hebt doorlopen, heb je een voltooide 17W-pc. Ongeacht of je Windows 11 of Linux of beide als besturingssysteem wilt installeren, moet je het UEFI-BIOS voor het installeren updaten. Ons moederbord werd geleverd met versie F3, op het moment van schrijven was versie F8 actueel – zie de link op deze pagina. Pak de inhoud van het zipbestand uit op een usb-stick. Je kunt de firmwareset-up openen door de Del-toets in te drukken bij het opstarten van de pc. Druk op F8 om het geïntegreerde Q-Flash updateprogramma op te roepen. Om ervoor te zorgen dat de 17W-pc de door ons gespecificeerde meetwaarden haalt, moet je vervolgens de instellingen die we voor je verzameld hebben bij de link op deze pagina doorvoeren.

Als je Windows 11 gaat installeren, is ons advies om na het installeren eerst Windows Update te starten. Die installeert de drivers voor de meeste hardwarecomponenten. Dat werkt in ieder geval via LAN, maar het wifistuurprogramma zit niet in het installatiemedium van Windows. Installeer dan de stuurprogramma's voor de chipset, HID event filter, seriële I/O, wifi, bluetooth en audio handmatig via de links die we voor je hebben verzameld.

We hebben de computer zonder problemen getest met Windows 11 versie 23H2. Je kunt de prestaties vergelijken met je vorige computer met behulp van de benchmarks en meetwaarden in dit artikel.

De 17W-pc draait ook met Ubuntu 23.10 als een zonnetje. Alle hardwarefuncties zoals het overzetten van gegevens naar een snelle usb-ssd, standbymodus, 2,5 Gbit/s ethernet en wifi werken zonder problemen. Idle was het energieverbruik onder Ubuntu 20 watt, drie en een halve watt meer dan onder Windows. Door te optimaliseren met powertop, waarmee we het Link Power Management van de SATA- en PCIe-poorten activeerden, konden we dat terugbrengen tot 18 watt.

UPGRADESUGGESTIES

Met de voltooide 17W-pc krijg je een moderne alledaagse computer die je eventueel nog beter aan je behoeften kunt aanpassen door wijzigingen en toevoegingen te maken. Als je meer RAM nodig hebt, kun je dat uitbreiden tot 192 GB. Er is op het moederbord ruimte voor een extra M.2-ssd. De behuizing biedt plaats aan maximaal vier 2,5-inch ssd's of twee 3,5-inch schijven. Kaartlezers en optische drives kun je

beter aansluiten via usb. Op die manier kunnen de apparaten ook op een laptop worden gebruikt als dat nodig is.

Als de cpu-prestaties van de Core i5-14500 niet voldoende zijn, kun je zonder aarzelen een krachtigere processor met meer kernen installeren. De cpu-koeler en de voeding bieden voldoende reserves. We raden alleen de twee topmodellen Core i7-14700K en Core i9-14900K af vanwege het zeer hoge piekverbruik van 253 watt.

Je kunt een grafische kaart tot en met een GeForce RTX 4070 installeren. De eerder door ons aanbevolen PNY GeForce RTX 4070 XLR8 Gaming Verto Epic-X RGB Triple past qua lengte in de behuizing. Dat heeft tot gevolg dat de pc maximaal 427 watt verbruikt. Daarom raden we aan om de ventilator aan de voorkant dan aan te sluiten. Je kunt de juiste instellingen vinden via de link op deze pagina.

Als je echter op zoek bent naar een gaming-pc, kun je beter gaan voor de allround gaming-pc van eerder dit jaar [2]. De Ryzen 7 7800X3D met een groot level 3-cache is daar veel beter geschikt voor. Bovendien kan energievretende hardware in de grotere behuizing beter worden gekoeld.

ct



www.ct.nl/softlink/2407092

Literatuur

[1] Christian Hirsch en Daniel Dupré, Bouwvoorstel voor een 13W-pc, c't 3/2023, p.42

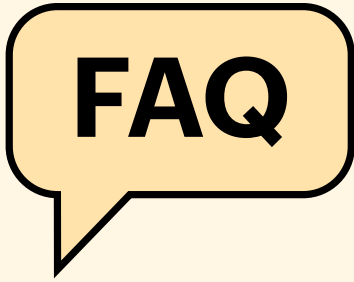
[2] Carsten Spille en Daniel Dupré, Bouwvoorstel voor een allround gaming-pc met een superefficiënte processor, c't 4/2024, p.38

Bouwvoorstel 17W-pc: technische gegevens en tests

Hardware-uitrusting	
Uitbreidings-slots (vrij)	2 × PEG (1 × PCIe 4.0 x16 (1), 1 × PCIe 3.0 x4 (1)), 1 × M.2-2280 (PCIe 4.0 x4) (0), 1 × M.2-22110/80 (PCIe 4.0 x4) (1)
Drivebays (vrij)	2 × 2,5" (2), 2 × 2,5"/3,5" (2)
Afmetingen (b × h × d) / casefans (fanregeling)	20,6 × 40,3 × 39,7 cm / 1 × 12 cm (✓)
Aansluitingen achterop	1 × HDMI 2.1, 1 × DisplayPort 1.4b, 3 × USB-A 5 Gbit/s, 5 × USB 2.0, 1 × LAN, 2 × wifi-antenne, 3 × analoge audio
Aansluitingen voor, boven, zijkant	2 × USB-A 5 Gbit/s, 1 × USB-C 10 Gbit/s, 2 × USB 2.0, 2 × analoge audio
Energieverbruik / snelheidsmetingen / audio	
Soft-off (met ErP) / energie besparen / idle	1,3 W (0,2 W) / 2,1 W / 17 W
Belast: cpu / peak	105 W / 226 W
Ssd: lezen (schrijven)	3567 (2732) MB/s
USB 3.2 Gen 1 (5 Gbit/s) / USB 3.2 Gen 2 (10 Gbit/s) type-C front: lezen (schrijven)	464 (466) / 1068 (1015) MB/s
LAN: ontvangen (zenden)	297 (298) MB/s
Wifi 5 GHz / 6 GHz: dichtbij (20 m)	1483 (307) / 1468 (277) Mbit/s
Audio: weergave / opnemen / front	⊕⊕ / ○ / ⊕⊕
Boottijd Windows 11	18 s
Linux-compatibiliteit met Ubuntu 23.10	
Idle energieverbruik (geoptimaliseerd)	20 W (18 W)
3D / LAN / wifi / audio	✓ (i915) / ✓ (r8169) / ✓ (rtw_8852ce) / ✓ (snd_hda_intel)
✓ werkt — werkt niet	
⊕⊕ zeer goed ⊕ goed ○ voldoende ⊖ slecht ⊖⊖ zeer slecht	

Bouwvoorstel 17W-pc: benchmarks en metingen onder Windows 11

Bouwvoorstel	Cinebench 2024 1T [punten]	Cinebench 2024 MT [punten]	Sysmark 30 [punten]	3DMark TimeSpy [punten]	Geluidsproductie idle / belast [sone]	Energieverbruik idle / belast / piek [watt]
	beter ▶	beter ▶	beter ▶	beter ▶	◀ beter	◀ beter
17W-pc	115	962	2145	952	0,2/0,2	17/105/226



Netwerkopslag

Netwerkopslag, ook bekend als NAS (Network Attached Storage), is hét alternatief voor iedereen die zijn bestanden niet wil toevertrouwen aan een cloudprovider. Hier de antwoorden op eventuele vragen.

Ernst Ahlers en Noud van Kruysbergen

WELKE NAS WAARVOOR?

? Er zijn honderden NAS-modellen op de markt. Hoe vind ik de juiste?

! Je kunt in de klasse rond 200 euro een systeem kopen voor je gezin of gedeelde kantoorruimte dat niet snel of uitbreidbaar hoeft te zijn. Het gaat dan om een lege NAS-behuizing met twee bays voor harde schijven. Vermijd aanbiedingen, dat gaat vaak om oudere modellen. Voor up-to-date hardware mag een model niet langer dan drie jaar op de markt zijn.

Raadpleeg bij het kiezen van harde schijven de compatibiliteitslijsten van de fabrikant, in het artikel in c't 3/2024 op pagina 60 beantwoorden we basisvragen over NAS-schijven. Als je het installeren van de schijven niet zelf wilt doen, zoek dan een winkelier die gevulde NAS-apparaten verkoopt.

Als de netwerkopslag moet functioneren als een kleine server of als een containerhost voor je eigen netwerk-services, dan moet je een model met een quad-core-processor en minstens 8 GB RAM overwegen, met uitbreidbaar RAM en slots voor M.2-ssd's. Er zijn bijna geen bovengrenzen, de grote NAS-fabrikanten bieden ook volwaardige servers voor middelgrote bedrijven.

Koop bij een NAS minstens twee usb-schijven met dezelfde capaciteit of meer als back-upmedia. Die zul je vroeg of laat nodig hebben.

1000 Mbit/s ontvangen voor een enkele transmissie. Link-aggregatie werkt vaak alleen als er meerdere overdrachten parallel lopen. Dan is het goedkoper en efficiënter om je pc's en LAN te upgraden naar 2,5 Gbit/s. Daardoor kun je de gegevensnelheid van harde schijven volledig benutten voor grote bestanden.

RAID ALS BACK-UP?

? Als ik meerdere harde schijven in een NAS stop en die als RAID koppel, dan hoef ik toch geen back-up meer te maken?

! Het maakt niet uit hoe je je NAS instelt: back-ups zijn een must! Dat is omdat de redundante RAID-configuraties 1, 5, 6 of 10 alleen helpen tegen het falen van de componenten van de massaopslag. Bedieningsfouten – oeps, verkeerde bestanden verwijderd! – worden door RAID ook gewoon overgenomen. Het biedt ook slechts beperkte bescherming tegen het overlijden van het moederbord van de NAS. Je kunt de schijven in een identiek apparaat plaatsen en hopen dat het die de RAID zonder problemen zal integreren. Het is echter veiliger en sneller om de bestanden terug te zetten vanaf een back-up dan erop te vertrouwen dat je ze van de oude NAS-schijven kunt halen.

GIGABIT- OF MULTIGIGABIT-ETHERNET?

? Wat is zinvoller, gigabit-netwerkpoorten of de duurere interfaces voor 2,5 Gbit/s?

! Neem een NAS met 2,5Gbit/s-ethernet. Het is mogelijk om twee gigabitpoorten aan de NAS-kant te combineren tot maximaal 2 Gbit/s met behulp van link-aggregatie – vroeger bekend als trunking, maar de LAN-switch moet dat ook aankunnen. Maar een pc met twee gigabitpoorten zal meestal maximaal

RAID 1 OF 5?

? Wat is logischer, RAID 1 met twee harde schijven of RAID 5 met drie?

! Dat hangt af van de gewenste opslagcapaciteit, de ontwikkeling van de elektriciteitskosten en de apparaatprijzen. Met dezelfde opslagcapaciteit zijn de schijven bij RAID 1 duurder dan bij RAID 5. Bij RAID 5 is echter het energieverbruik in rusttoestand hoger en de NAS iets duurder. Het is daarom niet mogelijk om in het algemeen te zeggen welke constellatie voor iemand gunstiger is. Je zult dat moeten uitwerken op basis van je eisen en je gebruiksgedrag (continu gebruik of de schijven frequent op stand-by).



Sockets voor M.2-cache-ssd's maken deel uit van de basisuitrusting van een moderne NAS. Het loont echter niet altijd die te vullen.

SSD'S ALS CACHE OF VOOR DATA?

? Ssd's zijn nog steeds aanzienlijk duurder dan harde schijven voor hoge capaciteiten. Wat is de beste manier om ze te gebruiken?

! Tenzij je een krachtige NAS gebruikt met 10 Gbit/s ethernet en een geschikte netwerkinfrastructuur die enorme bestanden opslaat op een ssd-RAID 5-configuratie, leveren ssd's zelden veel voordeel op. Een ssd-cache versnelt meestal alleen bepaalde toegangspatronen, zoals database-achtige benaderingen. Daarom lijkt het gebruik van ssd's het meest zinvol voor een volume waarop Docker-containers en hun bestanden staan die direct vanaf de NAS gestart worden. Een SQL-database en een cloudcontainer met veel kleine-bestandstoegangen profiteren van de veel lagere latentie van ssd's in vergelijking met harde schijven.

DESKTOP-, SERVER- OF NAS-SCHIJVEN?

? Heb ik NAS- of servermodellen nodig of zijn harde schijven voor pc's ook geschikt?

! Harde schijven voor pc's of desktops werken in een NAS, maar kunnen problemen veroorzaken bij leesfouten. Het is beter om NAS- of serverschijven te gebruiken, die defecte sectoren sneller overslaan. Dan wordt de schijf niet te vroeg als defect gemarkeerd en uit de RAID verwijderd. Bovendien zijn desktopschijven meestal niet geschikt voor continu gebruik.

SMR OF CMR?

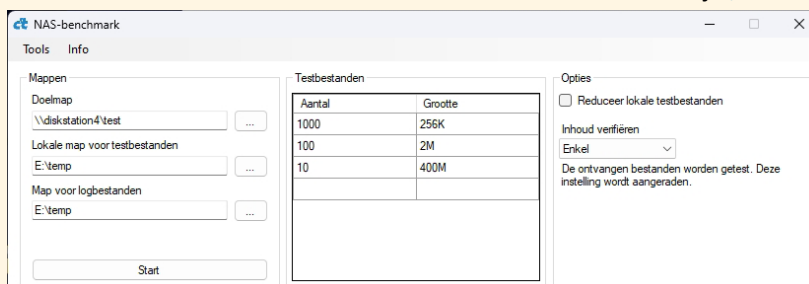
? SMR-schijven met hoge capaciteit zijn vaak goedkoper dan andere types. Kan ik die zonder problemen in een NAS plaatsen?

! Nee, het is beter om Conventional Magnetic Recording (CMR) schijven te gebruiken voor een NAS. Harde schijven met Shingled Magnetic Recording (SMR) zijn bedoeld voor archivering. Die doen er vaak veel langer over om sectoren te overschrijven dan CMR-modellen. Dat verlaagt de schrijfsnelheid enorm, vooral bij veel kleine toegangen, en een NAS gaat bij een vertraagde reactie soms uit van een schrijffout en gooit de schijf uit de RAID-array. De bescherming tegen uitval gaat dan verloren, in het ergste geval onopgemerkt als je daar geen alarm voor geactiveerd hebt.

NAS-DOORVOER METEN

? Met welke software testen jullie de prestaties van een NAS?

! We gebruiken onze eigen Windows-tool die de snelheid meet van het kopiëren van typische alledaagse bestandsets. De c't-NAS-bench (zie de link op deze pagina) schrijft drie groepen bestanden na elkaar van een RAM-schijf naar de NAS via een Windows-bestandsshare met behulp van functies van het besturingssysteem en leest ze vervolgens weer. De gebruikelijke bestandsets zijn 1000 kleine



De c't-NAS-benchmark kopieert verschillende bestandsets van en naar de NAS via de systeemfuncties van Windows. Het laat zien welke snelheden je in het dagelijks leven met verschillende bestandstypen kunt verwachten.

bestanden (256 kB), 100 middelgrote bestanden (2 MB) en 10 grote bestanden (400 MB). Bij kleine bestanden beperkt de latentie van de systeemfuncties van de besturingssystemen (Windows, NAS) de snelheid. Middelgrote bestanden laten het effect zien van de RAM-cache in de NAS tijdens het schrijven en grote bestanden laten zien wat de NAS en het netwerk kunnen bieden in termen van maximale gegevenssnelheid.

DE HARDE SCHIJVEN PERMANENT LATEN DRAAIEN?

? Moet ik de harde schijven in mijn NAS continu laten draaien? Of kunnen ze tussendoor in de slaapstand gaan om stroom te besparen?

! Er is niets dat een NAS ervan weerhoudt om het apparaat voor massaopslag na een uur inactiviteit op stand-by te zetten. Slijtage bij het opnieuw opstarten is niet langer een probleem: Western Digital specificeert zijn harde schijven bijvoorbeeld met 300.000 cycli, wat meer dan 30 jaar zou zijn als ze elk uur in slaapstand zouden gaan.

WANNEER HARDE SCHIJVEN VERVANGEN?

? De harde schijven in mijn NAS zijn al meer dan zes jaar oud. Wanneer moet ik die vervangen?

! Een absolute looptijd is niet erg zinvol. Besteed meer aandacht aan andere SMART-parameters van de harde schijven (Self-Monitoring, Analysis and Reporting Technology). Als je NAS daar een functie voor heeft, schakel die dan in. Voer de korte SMART-test minstens een keer per week uit.

Er zijn bij de SMART-waarden twee interessante parameters: Reallocated Sector Count en Offline Uncorrectable, soms met een iets andere benaming. Beide kunnen af en toe een kleine sprong vertonen, bijvoorbeeld van 0 naar 4 of van 12 naar 16 of iets dergelijks. Ten eerste hebben harde schijven geen perfecte schijfoppervlakken. Het is heel goed mogelijk dat een sector niet kan worden gelezen of geschreven. Ten tweede slijten harde schijven na verloop van tijd. Als die parameters op een harde schijf constant toenemen, oftewel bij elke SMART-uitlezing, dan moet je de schijf snel vervangen. Als je niet hebt gezorgd voor redundantie, oftewel meerdere harde schijven in RAID 1- of RAID 5-configuratie gebruikt, maak dan vaker dan normaal back-ups en wacht niet lang met vervangen.



www.ct.nl/softlink/2607096





DEUREN OPENEN

Windows krijgt een sudo-commando

Programma's uitvoeren onder Windows met administrator-rechten is met de muis meestal geen probleem, maar voor consolegebruikers was dat tot nu toe nogal omslachtig. Microsoft wil dat veranderen met het nieuwe sudo-commando.

Hajo Schulz en Noud van Kraysbergen

Een alledaags verschijnsel voor Linux-gebruikers: je voert een commando uit op de console en het systeem weigert dat uit te voeren met het argument dat er geen autorisatie is. Geen probleem: tover het commando weer tevoorschijn met de pijltjestoets, laat het dan voorafgaan door `sudo` en het werkt.

Voor Windows-gebruikers is dat niet zo eenvoudig. Dan moet je een console met administrator-rechten openen, een beveiligingsprompt van het Gebruikersaccountbeheer bevestigen en het commando daar opnieuw uitvoeren of van het vorige terminalvenster kopiëren – zelfs als je zelf een administrator bent [1]. Als je normaal gesproken geen

administrator bent, moet je ook een administrator-wachtwoord intypen.

Maar er is een oplossing op komst: Microsoft heeft aangekondigd dat het Windows ook een `sudo`-commando gaat geven in een van de volgende updates. Het is in een voorlopige versie al te bewonderen. We hebben gekeken naar wat je daarvan kunt verwachten, hoe Windows' `sudo` presteert ten opzichte van zijn Linux-naamgenoot en waar een al beschikbaar alternatief goed voor is.

WAAROM DAT ALLES?

In het verre verleden had Windows geen gebruikers-autorisaties: iedereen kon gewoon alles. Sinds Windows NT is Windows echter een multi-user besturingssysteem. Elke gebruiker heeft een eigen gebruikersaccount, waardoor privégegevens niet toegankelijk zijn vanuit andere accounts. Daarnaast wordt voorkomen dat gebruikers die (te) graag experimenteren het systeem verknoeien voor hun medegebruikers. De systeembeheerder moet echter wel toegang hebben tot alle gegevens, instellingen en programma's. Een account voor onderhouds- en con-

figuratiewerk dat alle rechten heeft (of in ieder geval kan krijgen) wordt een administratoraccount als het tot de groep Administrators behoort.

Dat concept is echter onhandig gebleken voor het typische gebruik van een privé-pc die alleen of hooguit samen met vertrouwde familieleden gebruikt wordt. Het is gewoon onhandig om opnieuw te moeten inloggen voor elke programma-installatie en elke wijziging aan de systeemconfiguratie. Veel mensen van Windows NT tot XP hebben daarom voor de makkelijke weg gekozen en zijn ook tijdens normaal gebruik lid van de administratorgroep. Dat is echter om twee redenen problematisch: ten eerste voorkomt het niet langer onbedoelde ingrepen in het systeem die de stabiliteit in gevaar kunnen brengen. En ten tweede heeft alles wat onbewust wordt gestart ook volledige systeemtoegang – en dan met name allerlei virussen, trojans en soortgelijke rotzooi.

Microsoft heeft bij Windows Vista daarom het concept van de zogenaamde ‘integrity levels’ en het bijbehorende User Account Control (UAC, Gebruikersaccountbeheer) geïntroduceerd. Het idee: zelfs leden van de administratorgroep hebben in eerste instantie alleen de rechten van normale gebruikers. Alleen als ze volledige rechten nodig hebben voor een bepaald programma of om toegang te krijgen tot systeembestanden, kunnen ze die rechten krijgen, maar dat moeten ze expliciet bevestigen. In het begin waren die constante verzoeken eerder vervelend dan nuttig, maar nu is het gebruikelijk – tenminste in de privé-sfeer – om zo’n beperkt administratoraccount te gebruiken, al is het maar omdat dit de standaard voor een nieuwe installatie is.

Grafische toepassingen kunnen vrij eenvoudig worden gestart met volledige rechten, bijvoorbeeld door te dubbelklikken op hun pictogram terwijl je de Ctrl- en Shift-toetsen ingedrukt houdt of door met de rechtermuisknop te klikken en ‘Als administrator uitvoeren’ te selecteren in het contextmenu. Microsoft heeft de liefhebbers van de Opdrachtprompt tot nu toe echter nogal nalatig behandeld bij dit concept. Je kunt een Opdrachtprompt of PowerShell starten met administratorrechten, maar je moet daar voor het intypen van het eerste commando wel over nadenken. Binnen de console hielp vroeger de constructie `runas /user:Administrator <command>`, maar het account met de naam Administrator, dat als enige niet onder UAC valt, is niet meer actief. PowerShell-gebruikers kunnen nog het commando `Start-Process` gebruiken in combinatie met de optie `-Verb` `runas` als je niet bang bent voor wat typewerk.

MICROSOFTS SUDO

Met het nieuw geïntroduceerde `sudo`-commando – de naam is afgeleid van ‘superuser do’ – zou alles nu net zo handig moeten zijn als onder Linux. Bovenal zou die tool universeel bruikbaar moeten zijn, ongeacht of je alleen de volledige rechten wilt geven aan een admin-account via een UAC-vraag of wilt overschakelen van een restricted naar een administratoraccount.

Tot nu toe is Microsofts eigen `sudo` alleen opgenomen in de Insider pre-releaseversies van Windows – om precies te zijn: vanaf build 26052. Als je het echter probeert te gebruiken, krijg je aanvankelijk een foutmelding: het commando is niet geactiveerd, dus dat moet je eerst doen bij de Ontwikkelaarsopties bij de Instellingen. Bij ‘Systeem / Voor ontwikkelaars’ staat een schakelaar genaamd ‘sudo inschakelen’. Als je daarop klikt, waarschuwt Windows dat het `sudo`-commando een beveiligingsrisico is en vraagt om bevestiging.

Als je op Ja klikt, activeer je een selectievak waarmee je kunt configureren hoe `sudo` applicaties uitvoert. De voor zichzelf sprekende optie ‘In een nieuw venster’ is voorgeselecteerd. De optie Inline heeft het tegenovergestelde effect: de output van commando’s die je uitvoert met `sudo` komt dan terecht in hetzelfde venster waarin je ze typt. Hetzelfde gebeurt bij ‘Met uitgeschakelde invoer’, maar dan verbindt `sudo` het opgeroepen programma niet met het toetsenbord. Volgens de documentatie van Microsoft is dat voor beveiligingsdoeleinden: een kwaadaardig proces dat in een consolesessie binnengeslopen is, kan dan niet stiekem valse invoer versturen naar het programma dat met verhoogde rechten draait. Zoals zo vaak het geval is, lijdt het gebruiksgemak daar echter onder: commando’s zoals `sudo cmd` en `sudo diskpart`, die verondersteld worden een interactief consoleprogramma te starten, werken niet langer omdat ze herkennen dat ze geen input kunnen ontvangen en onmiddellijk na het starten afsluiten. Als je bang bent voor het risico van de inline-modus, is het beter om de optie ‘In een nieuw venster’ optie te gebruiken.

Overigens werken commando’s als `sudo tasklist /v | more` ook met uitgeschakelde invoer, daarbij werkt alleen `tasklist` met verhoogde rechten, de console verzamelt zijn uitvoer en geeft die door aan `more`, die weer met beperkte rechten werkt en op toetsaanslagen wacht.

De inline-modi hebben op dit moment nog een bug: een programma dat aangeroepen wordt zonder verdere argumenten krijgt nog steeds een parameter mee, maar die is leeg. Programma’s reageren daar heel verschillend op: `diskpart` meldt bijvoorbeeld ‘The parameters could not be processed’ en verlaat het programma meteen weer. Zelfs `netsh` laat op die manier geen interactieve prompt zien, maar toont in plaats daarvan de netwerkconfiguratie, die meerdere schermpagina’s vult, net alsof `netsh dump` was aangeroepen.

Zoals het een consoleprogramma betaamt, kan `sudo` ook worden aangestuurd via de commandline. Het herkent onder andere de optie `config`, die de huidige modus rapporteert. Als je dat laat volgen door het argument `--enable` en `disable`, `enable`, `forceNewWindow`, `disableInput` of `normal` toevoegt, schakel je die besturingsmodus systeembreed, waarbij `normal` (of `default`) overeenkomt met de inline-instelling. Voor een enkele aanroep kan de standaardinstelling overschreven worden met `--newwindow` (of `-N` in het kort) of `--disable-input`. Verdere details krijg je met `sudo help`.

Zoals altijd als je een programma met administratorrechten wilt uitvoeren onder Windows, roept `sudo` ook het Gebruikersaccountbeheer op. Zelfs gebruikers met een account dat behoort tot de groep Administrators moeten daarom elke keer dat ze `sudo` uitvoeren Ja zeggen op 'Wilt u toestaan dat deze app wijzigingen aan uw apparaat aanbrengt' – als de UAC-schakelaar bij de Instellingen zoals aanbevolen op ten minste het derde van de vier mogelijke niveaus ingesteld is. Dat is een goede zaak om te voorkomen dat malware niet zomaar volledige rechten kan krijgen met een verborgen `sudo`-oproep.

Als je `sudo` uitvoert vanuit een gebruikersaccount met beperkte rechten, verschijnt de UAC ook weer, maar is in dat geval niet tevreden met een simpele klik op Ja. In plaats daarvan wil het de gebruikersnaam en het wachtwoord van een admin-account weten. Windows voert de gevraagde toepassing dan uit onder dat account. Dat betekent dat `sudo` aan een beperkt account geen administratorrechten geeft – dat is vanuit het beveiligingsconcept van Windows ook niet de bedoeling.

Microsoft is van plan om de broncode van `sudo` te publiceren. De speciale pagina op GitHub (zie de link op de volgende pagina) was op het moment van schrijven echter nog grotendeels leeg. Er stond alleen een script dat het makkelijker moet maken voor PowerShell-gebruikers om `sudo` te gebruiken.

GSUDO

Er zijn alternatieven voor Microsofts `sudo`. Het meest populair is waarschijnlijk het opensource programma `gsudo` van de Argentijnse ontwikkelaar Gerardo Grignoli (zie de link). Het basisidee is hetzelfde als bij `sudo`: je schrijft de programmaam voor een commando om het uit te voeren met administratorrechten. Zolang er geen Microsoft `sudo` op het systeem staat, voelt `gsudo` zich ook aangesproken door het `sudo`-commando.

Er is geen grafische configuratie voor `gsudo`, in plaats daarvan kun je de opties instellen met commando's, die allemaal beginnen met `gsudo config`.

De huidige configuratie wordt weergegeven zonder verdere argumenten. Standaard werkt `gsudo` op een manier die overeenkomt met de inline-modus van Microsofts `sudo`. De modus die een nieuw venster opent voor elk programma dat met volledige rechten wordt gestart, stel je vast in met `gsudo config New-Window.Force true`, met `false` in plaats van `true` zet je dat weer terug. Met `gsudo -n <commando>` voer je dat ene commando uit in een nieuw venster. De optie `SecurityEnforceUac Isolation true`, die in de documentatie van `gsudo` wordt omschreven als experimenteel, activeert een inline-modus zonder invoer.

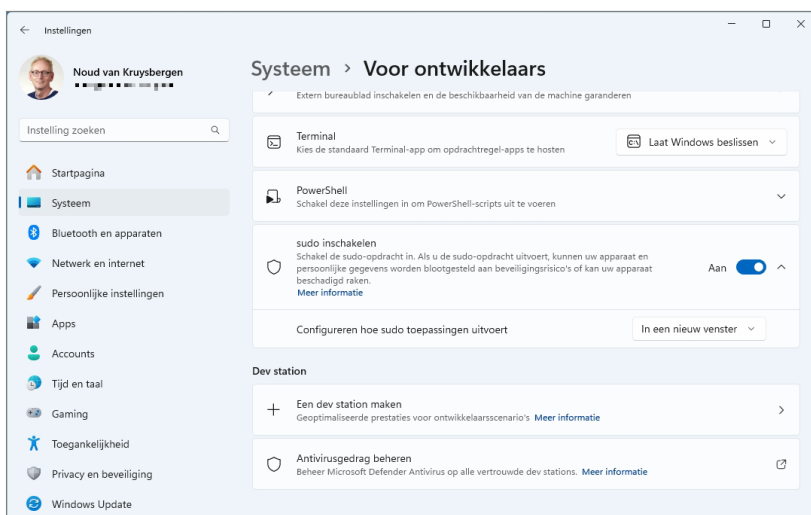
Naast de basisfuncties heeft `gsudo` ook een paar trucjes die het onderscheiden van zijn Microsoft-tegenhanger. Het feit dat `gsudo` bijvoorbeeld de rechten van de huidige actieve console sessie zonder verdere parameters verhoogt, bespaart een beetje typewerk. Als je weet wat je doet, kun je `gsudo` niet alleen gebruiken om administratorrechten te verkrijgen, maar ook die van de lokale systeemaccount via de vlag `-s` of die van de Trusted Installer met `--ti`, oftewel het account dat als enige schrijf- en verwijderrechten heeft voor Windows' eigen systeembestanden. Nogal exotisch, maar soms handig: `gsudo -i Medium <commando>` voert een commando uit met normale gebruikersrechten (`Medium`) – zelfs als je het start vanaf een administratorconsole.

Zoals gebruikelijk bij Windows activeert elke verhoging van rechten met `gsudo` ook het Gebruikersaccountbeheer. Als je je ergert aan de constante beveiligingsvragen, kun je het programma ook zo instellen dat het de bevestiging een tijdje onthoudt en overslaat: `gsudo cache on` geeft eenmaal een UAC-vraag en onthoudt de bevestiging totdat je die console sessie beëindigt of de cache uitschakelt met `gsudo cache off` of `gsudo -k`. Je kunt het programma ook zo instellen dat het elke UAC-bevestiging automatisch gedurende een bepaalde tijd onthoudt. Het commando daarvoor is `gsudo config Cache-Mode Auto`; de standaard opslagtijd is vijf minuten, maar dat kun je wijzigen met `gsudo config Cache-Duration "hh:mm:ss"`. Let op: de UAC-cache is een veiligheidsrisico en de `gsudo`-documentatie wijst er expliciet op dat je het gemak ervan betaalt met verminderde veiligheid. De cache schakelt tijdelijk het Gebruikersaccountbeheer voor de actieve console uit en programma's kunnen dan ongevraagd meer rechten krijgen.

Voor verdere beschouwingen over het onderwerp beveiliging en voor een volledig overzicht van de `gsudo`-commando's en opties, raadpleeg je de uitvoer van `gsudo help` en de online documentatie (zie de link op de volgende pagina).

SUDO ONDER LINUX

Het voorbeeld voor zowel `gsudo` als Microsofts `sudo` is het commandlinecommando `sudo`, dat gangbaar is bij Unix-achtige besturingssystemen. De basisfunctionaliteit vanuit het oogpunt van gebruikers is vergelijkbaar in beide werelden: een commando wordt



Als je `sudo` van Microsoft wilt gebruiken, moet je dat eerst activeren bij de Ontwikkelaarsopties van de Instellingen.

voorafgegaan door `sudo` om het daaropvolgende commando te kunnen uitvoeren zonder beperkingen qua rechten. In detail en vooral achter de schermen gebeuren er echter verschillende dingen. Wanneer we het in het volgende hebben over `sudo` onder Linux, omvat dat automatisch ook naamgenoten onder macOS en andere Unix-achtige besturingssystemen.

De verschillen beginnen met het feit dat er onder Linux geen concept bestaat dat overeenkomt met het Gebruikersaccountbeheer en de integriteitsniveaus van Windows. De rechten die worden toegewezen aan een gebruikersaccount zijn hetzelfde bij elke login en veranderen niet in de loop van een sessie. Daardoor logt `sudo` een gebruiker altijd in onder een ander account voor verhoogde rechten, wat standaard root is – oftewel de almachtige systeembeheerder.

Iets soortgelijks gebeurt ook onder Windows, namelijk wanneer een gebruiker die niet tot de administratorgroep behoort het `sudo`-commando uitvoert. De authenticatie werkt echter op een fundamenteel andere manier: onder Windows moet je het wachtwoord weten dat hoort bij het gewenste administratoraccount, onder Linux alleen je eigen wachtwoord. Wat in eerste instantie lijkt op openstaande schuurdeuren waardoor iedereen rootrechten kan krijgen, blijkt bij nader inzien heel slim te zijn: een beheerder kan (en moet) configureren wie `sudo` mag gebruiken en wat ze met de hogere rechten precies mogen doen. Daarvoor bestaat het tekstbestand `/etc/sudoers`, dat – je raadt het waarschijnlijk al – alleen de root-gebruiker mag bewerken. Iedereen die daar niet staat, mag `sudo` niet gebruiken. De root-gebruiker mag in geen geval zijn eigen wachtwoord opgeven.

Het valt buiten het bestek van dit artikel om de exacte structuur van het bestand uit te leggen. In een notendop: elke regel definieert eerst op wie (een gebruikersaccount of een groep) en waar (op welke hosts) de regel van toepassing is. Vervolgens definieert de regel welke identiteiten – opnieuw gebruikers of groepen – de bevoegde persoon mag aannemen via `sudo`. Tenslotte is er een lijst van reguliere expressies die specificeren hoe de gebruikte commandoregels eruit mogen zien. Het sleutelwoord **ALL** kan voor al deze punten gebruikt worden om een controle achterwege te laten.

Je kunt in het bestand `sudoers` ook specificeren of gebruikers überhaupt een wachtwoord moeten invoeren, en zo ja, hoelang `sudo` dat bewaart alvorens er opnieuw om te vragen. De standaardinstelling is 15 minuten.

De lijst van opties die `sudo` begrijpt vanuit het oogpunt van de gebruiker is lang. De belangrijkste zijn `-u` en `-g` om te bepalen welke gebruikers- of groepsidentiteit je wilt aannemen, en `-i` om een interactieve shell te starten met andere rechten. Het concept van het automatisch openen van een nieuw consolevenster voor een root-sessie is echter vreemd aan Linux' `sudo`: alle input en output van het gestarte programma, zelfs die van een nieuwe root-shell, vindt plaats in de huidige terminal. In ieder geval is `sudo` uitdrukkelijk niet bedoeld voor GUI-programma's,

SUDO(8)	System Manager's Manual	SUDO(8)
NAME		
sudo, sudoedit – execute a command as another user		
SYNOPSIS		
sudo -h -K -k -V		
sudo -v [-ABkNnS] [-g group] [-h host] [-p prompt] [-u user]		
sudo -l [-ABkNnS] [-g group] [-h host] [-p prompt] [-U user] [-u user]		
[command [arg ...]]		
sudo [-ABbEHnPS] [-C num] [-D directory] [-g group] [-h host] [-p prompt]		
[-R directory] [-r role] [-t type] [-T timeout] [-u user] [VAR=value]		
[-t -s] [command [arg ...]]		
sudoedit [-ABkNnS] [-C num] [-D directory] [-g group] [-h host]		
[-p prompt] [-R directory] [-r role] [-t type] [-T timeout] [-u user]		
file ...		
DESCRIPTION		
sudo allows a permitted user to execute a command as the superuser or another user, as specified by the security policy. The invoking user's real (not effective) user-ID is used to determine the user name with which to query the security policy.		
sudo supports a plugin architecture for security policies, auditing, and input/output logging. Third parties can develop and distribute their own plugins to work seamlessly with the sudo front-end. The default security policy is <code>sudoers</code> , which is configured via the file <code>/etc/sudoers</code> , or via LDAP. See the "Plugins" section for more information.		
The security policy determines what privileges, if any, a user has to run sudo. The policy may require that users authenticate themselves with a		
Manual page sudo(8) line 1 (press h for help or q to quit)		


In het dagelijks gebruik werkt `sudo` onder Linux meestal zonder geavanceerde opties, maar er zijn er verschillende beschikbaar voor speciale gevallen.

die andere manieren en middelen hebben om uitgebreide rechten te krijgen.

Voor een beschrijving van andere opties voor het beheer en gebruik van `sudo` onder Linux verwijzen we je graag naar de documentatie in de manpages via `man sudoers` of `man sudo`.

CONCLUSIE

Iedereen die zowel onder Linux of macOS als onder Windows regelmatig consoleprogramma's gebruikt, zal een commando als `sudo` bij die laatste erg gemist hebben. Het is dus goed dat Microsoft die tekortkoming aanpakt – en dat werd hoog tijd. Het was niet te verwachten dat dit zou resulteren in een één-op-één kopie van de gelijknamige Linux-tool, daarvoor zijn de beveiligingsarchitecturen van de twee besturingssysteemwerelden te verschillend. Hoewel Microsofts `sudo` nog alleen beschikbaar is bij de pre-release versies van Windows, heeft het al het versienummer 1.0. Het lijkt er dus op dat de beperkte reeks functies voorlopig alles is wat Microsoft op dat gebied wil leveren.

Het commando `gsudo` laat zien dat je een `sudo`-tegenhanger onder Windows met wat meer liefde kunt programmeren. Zijn UAC-cache en de mogelijkheid om programma's uit te voeren onder elk gebruikersaccount met een vrij definieerbaar integriteitsniveau maken dat de eerste keuze voor consolegebruikers – zelfs na de release van Microsofts `sudo`. Het enige addertje onder het gras: zodra de `sudo`-versie van Microsoft officieel wordt opgenomen in Windows, moet je even anders te werk gaan en `gsudo` intypen als je ook `gsudo` bedoelt, want `sudo` zal dan Microsofts versie aanroepen. 

Literatuur

[1] Axel Vahldiek, Administratorrechten in Windows 10, c't 10/2018, p.56



www.ct.nl/softlink/2407098



Illustratie Midjourney, bewerking ct

SLIMME TRAJECTCONTROLE

Waarom het HTTPS-record voor DNS nuttig is

Sinds enkele maanden werkt het internet ongemerkt eleganter dan voorheen omdat het nieuwe DNS-record HTTPS een nuttig en krachtig sturelement heeft toegevoegd voor het regelen van het dataverkeer.

Carsten Strotmann en Noud van Kruijsbergen



Het internet is net een duiventil: elke dag verschijnen er nieuwe servers, oude servers veranderen zonder aankondiging van ip-adres en niemand weet precies hoeveel internetserver er op een bepaald moment zijn. Clients zoals browsers of smartphone-apps kunnen een server echter nog steeds vinden door de wereldwijde, gedecentraliseerde DNS-database (Domain Name System) te raadplegen. Beheerders registreren daar bijvoorbeeld webservers door de vereiste gegevens in te voeren op de DNS-server die verantwoordelijk is voor hun domein.

De gegevens in de database staan bekend als resource-records (RR). Er zijn verschillende resource-records voor verschillende doeleinden. De A- en AAAA-records zijn waarschijnlijk wel enigszins bekend, dat zijn records voor respectievelijk de IPv4- en IPv6-serveradressen. Het A-record werd samen met het DNS geïntroduceerd in 1983, het AAAA-record (ook bekend als Quad-A) werd toegevoegd in 1995.

Om de paar jaar worden er nieuwe recordtypes aan het DNS toegevoegd. Bijna geen enkele heeft

echter zo'n grote invloed op het internetverkeer als het HTTPS-record dat in november 2023 gespecificeerd werd, omdat het beheerders onder meer in staat stelt om de verbindinginstellingen van browsers te beïnvloeden.

Iedereen die een website beheert of toepassingen ontwikkelt, zoals mobiele apps of web API-clients, zou daarom het nieuwe HTTPS-record nader moeten bekijken. In het volgende gebruiken we een browser als voorbeeld voor van alle clienttoepassingen.

Het HTTPS-record werd gespecificeerd door de Internet Engineering Task Force (IETF) in het document RFC 9460 [1]. Het breidt het concept van de klassieke A- en AAAA-records uit en kan die aan het begin van de dialoog tussen de applicatie en de server zelfs vervangen.

Het grote verschil tussen de adresvermeldingen en de HTTPS-vermelding is snel uitgelegd: de adresvermelding specificeert alleen het ip-adres en dus de netwerklocatie van een server, maar het HTTPS-record informeert de browser over een beleid (policy) en geeft daarmee de voorkeursparameters voor communicatie met de server op.

ENCRYPTIE-AANBEVELING

De meeste functies van het HTTPS-record zijn optioneel voor zowel de beheerder van een webservice als de ontwikkelaar van een browser, zodat men rekening kan houden met de kenmerken van de server of browser.

De eenvoudigste functie wordt gerealiseerd door eenvoudigweg de aanwezigheid van het record: dat betekent dat de server op zijn minst een met TLS versleutelde en geauthenticeerde verbinding moet aanbieden bij het tot stand brengen van contact. Het is daarom handig als de browser het DNS niet om een adresrecord vraagt, maar om het HTTPS-record voor het domein in de url voordat er een verbinding tot stand wordt gebracht. Als het DNS dan een HTTPS-record meldt, wordt er meteen een HTTPS-verbinding tot stand gebracht.

Het niet-versleutelde HTTP wordt dan uitgesloten – zelfs als HTTPS mislukt. Dat voorkomt een downgrade-aanval waarbij aanvallers de browser dwingen om het onveilige HTTP te gebruiken.

Die functie is vergelijkbaar met de oudere HTTP Strict Transport Security (HSTS, RFC 6797) [2], die ook bedoeld was om met TLS beveiligd HTTP-verkeer af te dwingen. Een paar jaar geleden maakte de technologie deel uit van browsers en konden website-beheerders de browser via HTTP-headers verzekeren dat de website in kwestie gedurende een bepaalde periode via HTTPS zou worden geleverd. Browsers sloegen de HSTS-informatie echter op in de cache en beheerders hadden daar geen controle over, dus verdween HSTS al snel naar de achtergrond.

Beheerders kunnen de geldigheid van de HTTPS-records en dus het beleid daarentegen bepalen op basis van de Time-To-Live waarde (TTL): als de TTL verloopt, verloopt de informatie in het HTTPS-record. Browsers moeten het record dan opnieuw ophalen. Beheerders behouden dus de controle over het beveiligingsbeleid en kunnen indien nodig wijzigingen aanbrengen, bijvoorbeeld TLS-encryptie afraden als dat om wat voor reden dan ook niet werkt.

PROTOCOLKEUZE

Sinds enige tijd is het moderne HTTP/3-protocol, de opvolger van HTTP/1.1 en HTTP/2, die nog steeds in gebruik zijn, beschikbaar voor het benaderen van websites. Google initieerde HTTP/3 en testte het jarenlang in de Chrome-browser, op zijn eigen zoekmachines en op YouTube, voordat de IETF het in juni 2022 specificeerde als RFC 9114 [3]. Sindsdien is HTTP/3 steeds wijder verspreid.

Het bijzondere aan HTTP/3 is dat het User Datagram Protocol (UDP) wordt gebruikt voor transport. Zijn voorgangers waren gebaseerd op het langzamere Transmission Control Protocol (TCP). Daarnaast zijn UDP en de beveiligingslaag TLS gekoppeld aan de QUIC-substructuur (RFC 8999 tot 9002), die alle HTTP/3-transmissies versleutelt.

Het url-formaat blijft echter ongewijzigd: alle versleutelde url's blijven beginnen met https://. Browsers weten daarom niet of ze de verbinding via TCP – voor HTTP/1.1 of HTTP/2 – of via UDP/QUIC voor HTTP/3 moeten opzetten. Ze maken daarom altijd een TCP-verbinding. Als de server in de HTTP-header dan de optie alt-svc voor HTTP/3 meldt, starten ze opnieuw via UDP/QUIC – dit is omslachtig en verspilt tijd. Het HTTPS-record ruimt ook daar op: de beheerder

kan de parameter Application Layer Protocol Negotiation (alpn) gebruiken om de browser te vertellen welke protocollen de server aankan [4].

In het volgende voorbeeld meldt de gezaghebbende DNS-server op verzoek van clients dat de webserver voor example.com bij voorkeur communiceert via HTTP/3 (h3). Als de client dat niet aankan, moet hij HTTP/2 (h2) gebruiken:

```
example.com. 300 IN HTTPS 1 . alpn="h3,h2"
```

HTTP/1.1 wordt in het bovenstaande voorbeeld niet expliciet genoemd, maar is impliciet opgenomen. Dat komt omdat elk url-schema een standaard set protocollen definieert die een browser kan gebruiken naast de protocollen die zijn gespecificeerd in de alpn-parameter – inclusief HTTP/1.1. Alleen met no-default-alpn worden uitsluitend de protocollen bedoeld die in het HTTPS-record worden genoemd en worden de protocollen uitgesloten die impliciet via het url-schema gedefinieerd zijn:

```
example.com. 300 IN HTTPS 1 . alpn="h3,h2"
no-default-alpn
```

ALIAS VERBETEREN

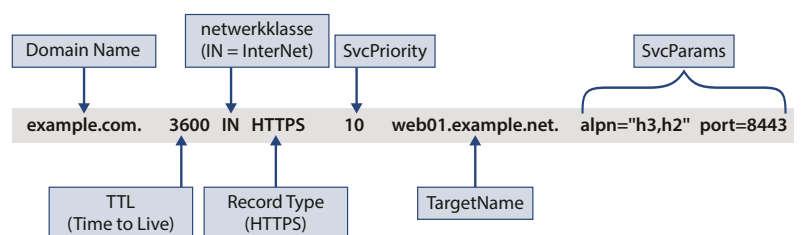
Met het HTTPS-record kunnen eindelijk aliassen worden aangemaakt voor basisdomeinen zoals example.com. Dat is met name handig voor bedrijven die hun eigen domeinen gebruiken in combinatie met gehoste diensten zoals webserver, omdat daar een dilemma bestaat: de webserver draaien onder een domeinnaam van de hoster (example.com) en de hoster heeft continu controle nodig over de bijbehorende DNS-invoer omdat de ip-adressen vaak veranderen vanwege de verdeling van de belasting en updates van de infrastructuur.

Cloudgebruikers willen daarentegen ook hun eigen domein (example.nl, basisdomein) zelf beheren (bijvoorbeeld voor MX-vermeldingen voor hun eigen mailservers).

Om toegang te krijgen tot de webserver van de hoster via het klantdomein, wil je een alias aanmaken van het basisdomein example.nl naar het basisdomein example.com van de hoster. Dat is echter niet mogelijk met de tot nu toe gestandaardiseerde alias-

Anatomie van het HTTPS-record

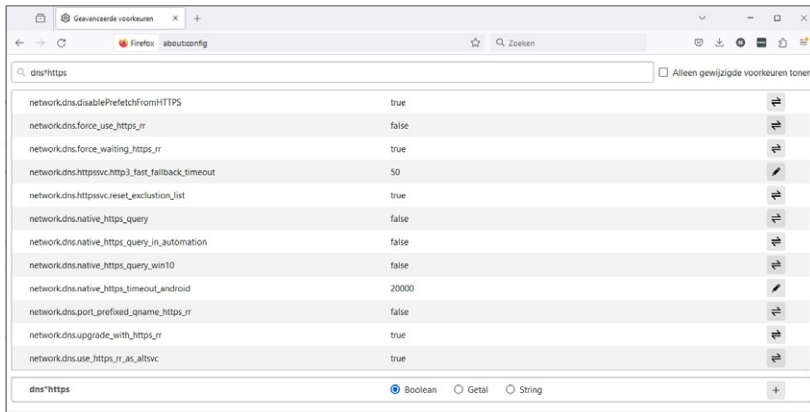
Met behulp van het HTTPS-record kunnen clients zoals browsers service-informatie ophalen uit het DNS en zo vanaf het begin door TLS beschermd communiceren of de verbinding sneller opzetten.



SvcPriority: 0 = Alias Mode
1+ = Backup Mode

TargetName: . = domain dan wel doelserver
<Domain Name> = andere doelserver

SVCParams: null of meerdere parameters in de vorm sleutel=waarde



Browsers zoals Firefox gebruiken al enige tijd het HTTPS-record. Een blik op de gedetailleerde instellingen laat zien of dat bij jou het geval is.

functies, zoals CNAME. Die zijn alleen geschikt voor subdomeinen en niet voor basisdomeinen. Sommige cloudaanbieders gebruiken daarom hun eigen, onderling incompatibele DNS-records (ANAME, ALIAS).

Het HTTPS-record is bedoeld om die wildgroei op te lossen: als de waarde van het eerste veld in het HTTPS-record (SvcPriority) 0 is, moet het tweede veld (TargetName) de aliasnaam voor de webservice bevatten. Voorbeeld:

```
example.nl. IN HTTPS 0 example.com.
```

Dat verandert de workflow: terwijl CNAME-records worden geëvalueerd door de DNS-resolver en de client het definitieve doeladres krijgt, valt het resolver van HTTPS-records onder de verantwoordelijkheid van de browser.

In die situatie kan de browser zoals gewoonlijk de ip-adressen van de doelserver opvragen (in het voorbeeld example.com). De beheerder kan dat echter verkorten en de adressen direct in het HTTPS-record noemen (meer daarover bij Serveradressen).

BACK-UPSERVERS

Back-upservers van de webservice kunnen ook worden opgegeven via de aliasvelden. Browsers gebruiken een back-upserver als de hoofdservier niet beschikbaar is. Om een of meer back-ups te definiëren, moet je een waarde groter dan 0 invoeren bij het eerste veld van het HTTPS-record (SvcPrio). Als er meerdere HTTPS-records voor hetzelfde domein zijn, kun je meerdere back-ups definiëren en de prioriteit opgeven bij het veld SvcPrio. Het veld SvcTarget bevat de hostnaam van een back-up. Voorbeeld:

```
example.com. IN HTTPS 10 backup01.example.com.
example.com. IN HTTPS 20 backup02.example.net.
example.com. IN HTTPS 30 backup03.example.nl.
```

Net als bij het MX-record voor mailservers vertegenwoordigen lagere waarden hogere prioriteiten. Een browser die het bovenstaande voorbeeldrecord krijgt, probeert eerst een verbinding tot stand te brengen met backup01.example.com. Als die niet kan worden bereikt, gaat hij naar backup02.example.net en als dat ook mislukt, naar backup03.example.nl.

Een punt in het veld SvcTarget betekent dat de hostnaam van de doelserver en het domein van het

HTTPS-record identiek zijn:

```
example.com. IN HTTPS 1 .
```

In het bovenstaande voorbeeld wordt HTTPS-record gebruikt om aan te geven dat de webservice bereikbaar is via poort 443 (HTTPS) op de server met de domeinnaam example.com.

SERVERADRESSEN

De HTTPS-vermelding vervangt in principe niet de adresvermeldingen, maar kan de bijbehorende verzoeken besparen. Normaal gesproken evalueert een browser eerst het veld SvcTarget en raadpleegt dan het DNS voor de adressen van de domeinnamen die daarin worden vermeld. De beheerder kan die stap verkorten door de adressen direct bij het HTTPS-record te benoemen. De parameters ipv4hint en ipv6hint zijn daarvoor gedefinieerd. Voorbeeld:

```
www.example.com. IN HTTPS 1 . ipv4hint=192.0.
2.20,198.51.100.80 ipv6hint=2001:db8:10::80,
2001:db8:20::443
```

Of browsers die adressen gebruiken of niet is aan de browserontwikkelaar. In plaats daarvan zouden ze zich ook aan de oorspronkelijke specificatie kunnen houden en de adressen zelf parallel kunnen opvragen aan de eerste HTTPS-verbinding die tot stand wordt gebracht. Daarom moeten beheerders normaal gesproken de A- en AAAA-records en de velden van de HTTPS-records bijwerken als ze van adres veranderen.

POORTSIGNALERING

Sommige HTTPS-servers leveren websites niet via de gebruikelijke poort 443. Om die op te halen, moet je de poort invoeren zoals in deze voorbeeld-url: https://webservice.example.nl:8000/path.

Dat is lastig. Met een beetje geluk adverteert de server op zijn minst zo'n url in het lokale netwerk met behulp van het multicast-DNS-protocol. Dat betekent dat werknemers die zijn ingelogd op een bedrijfsnetwerk alleen maar op de weergegeven servicenaam in de browser hoeven te klikken om de juiste verbinding tot stand te brengen. In de meeste gevallen ontbreekt dat echter of wordt dat niet geëvalueerd door de browser, zodat de gebruiker zowel op het internet als in het bedrijfsnetwerk de taak heeft om de juiste url in te voeren. Als de gebruiker de juiste poort niet weet, kan hij de website niet openen. Dat probleem kan ook worden omzeild met het HTTPS-record door de browser het poortnummer mee te geven:

```
webservice.example.nl IN HTTPS 1 . port=8000
```

Dat werkt zowel in bedrijfsnetwerken als op het internet en kan zelfs worden gebruikt om verschillende onafhankelijke webservices op dezelfde server onder dezelfde domeinnaam uit te voeren – zelfs met verschillende webserversoftware. Dat is bijvoorbeeld handig voor containers met een geïntegreerde webservice.

De parameter Encrypted Client Hello (ech) is nog niet geactiveerd in de huidige browsers [5], maar daar is al wel in voorzien. Die parameter is bedoeld voor een publieke sleutel waarmee browsers direct vanaf

het eerste ip-pakket versleuteld kunnen communiceren met de webserver. Details moeten nog worden gespecificeerd.

BROWSERPRAKTIJK

We hebben de eerste verzoeken voor HTTPS-records al in de zomer van 2020 waargenomen, kort voor de release van Apples besturingssystemen iOS 14 en macOS 11. Alle webtoepassingen op iPhones, macOS en macOS 11 zijn versleuteld. Alle webapplicaties op iPhones, iPads, Macs en andere Apple-apparaten, waaronder de Safari-browser van Apple, halen inmiddels HTTPS-records op bij het DNS. Daardoor werd het HTTPS-record al snel het op twee na meest voorkomende DNS-record (na adresrecords) in de DNS-resolverstatistieken.

Tegenwoordig vertrouwen de Chromium-browsers Google Chrome, Microsoft Edge, Vivaldi en Brave en de nieuwste Firefox ook op het HTTPS-record. Afhankelijk van de versie en geografische regio kunnen sommige functies gedeactiveerd zijn. Wat precies geactiveerd is, kun je vinden bij de gedetailleerde browserinstellingen. Bij Firefox vind je de HTTPS-recordinstellingen via het about:config-adres. Voer daarna de tekenreeks `dns*https` in bij het zoekveld.

HTTPS-RECORDS OPVRAGEN

Met de huidige versies van de DNS-querytools `dig` (onderdeel van BIND9), `kdig` (Knot DNS) en `unbound-host` (NLNetLabs Unbound) kan het HTTPS-record (Record Type #65) via de commandline worden opgevraagd voor analysedoeleinden: `kdig cloudflare.com https`

De `dig`-aanroep ziet er verder hetzelfde uit, de `unbound-variant` ziet er als volgt uit:

```
unbound-host -t https cloudflare.com.
```

De gevraagde gegevens zijn te vinden in het antwoordgedeelte van de uitvoer:

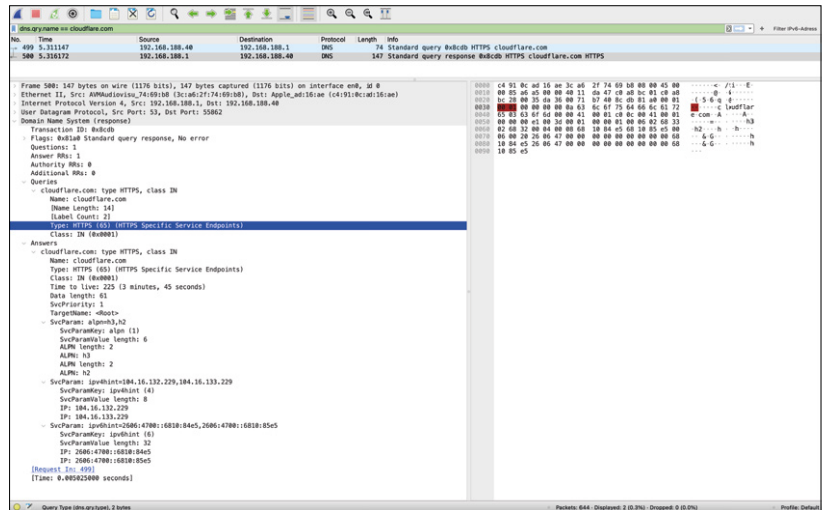
```
cloudflare.com. 294 IN HTTPS 1 . alpn="h3,h2
ipv4hint="104.16.132.229, 104.16.133.229"
ipv6hint="2606:4700::6810:84e5,2606:4700::68
10:85e5"
```

Het programma `nslookup`, dat nog steeds in sommige Linux-versies en in Windows zit, maar al lang niet meer bijgewerkt is, herkent het HTTPS-record niet en kan het niet opvragen.

HTTPS-RECORD BIJ OUDERE DNS-SERVERS

Huidige opensource DNS-servers zoals BIND 9.18, Knot-DNS 3.3.4 en PowerDNS 4.8.4 zijn zonder meer geschikt voor het HTTPS-record. Het record kan zoals gebruikelijk als tekst in de zones worden ingevoerd.

Voor commerciële DNS-producten en -diensten die nog niet ontworpen zijn voor het HTTPS-record, zoals oudere Windows DNS-servers, kan het generieke formaat voor onbekende DNS-resource-records gebruikt worden dat gespecificeerd is in RFC 3597 [6]. Om dat te doen, wordt eerst het gewenste HTTPS-record ingevoerd op een DNS-server die voor dat doel ontworpen is, zoals BIND9. Het `dig`-commando verandert in:



De Wireshark-analysetool kan worden gebruikt om te registreren hoe een client HTTPS-records aanvraagt bij het DNS en welk antwoord de geconfigureerde DNS-resolver geeft (linkerkolom, sectie Answers).

```
dig https example.com +multi +unknownformat
+noall +answer
```

Het geeft dan een uitvoer als deze:

```
example.com. 300 CLASS1 TYPE65 \# 61 (
00010000001000602683302683200040008681084E56810
85E500600202606470000000000000000000000000000
81084E526064700000000000 000000681085E5 )
```

Die uitvoer wordt dan toegevoegd aan het zonebestand van een DNS-server die niet ontworpen is voor het HTTPS-record.

Als alternatief kun je BIND9 of een andere geschikte server instellen als Hidden Primary en de gewenste HTTPS-records erin zetten. Gebruik vervolgens zonetransfer om de zone te verplaatsen naar de actieve DNS-server op het internet, bijvoorbeeld bij een DNS-hoster.

Als je DNS-verzoeken voor ongewenste inhoud zoals advertenties of malware blokkeert met behulp van DNS-filters, bijvoorbeeld met Pi-Hole of AdGuard Home, moet je naast de A- en AAAA-records ook het HTTPS-record voor de ongewenste domeinnamen blokkeren.

CONCLUSIE

Het HTTPS-record moderniseert de DNS-naamresolutie, versnelt in veel gevallen de communicatie met servers en maakt het eenvoudiger voor een beheerder om versleuteld verkeer af te dwingen.

Voor al HTTP/3 gebruiken, zouden beheerders die al HTTP/3 gebruiken, zouden moeten overwegen om het HTTPS-record te gebruiken. Maar HTTP/2-servers kunnen daar echter ook van profiteren, bijvoorbeeld door een betere beveiliging.

ct

Literatuur

- [1] Service Binding and Parameter Specification via the DNS (SVCB and HTTPS Resource Records), RFC 9460, rfc-editor.org/rfc/rfc9460
- [2] HTTP Strict Transport Security (HSTS), RFC 6797, rfc-editor.org/rfc/rfc6797
- [3] HTTP/3, RFC 9114, rfc-editor.org/rfc/rfc9114
- [4] NPN and ALPN, imperialviolet.org/2013/03/20/alpn.html
- [5] Encrypted Client Hello in Firefox Browser, wiki.mozilla.org/Security/Encrypted_Client_Hello
- [6] Handling of Unknown DNS Resource Record, rfc-editor.org/rfc/rfc3597

Concepten en ontwikkeling achter Thunderbolt

Thunderbolt wordt gebruikt om beeldschermen, externe ssd's en andere randapparatuur aan te sluiten op een laptop of pc. Thunderbolt is universele en meestal betrouwbaarder dan het zeer ingeburgerde usb – ook al gebruikt het dezelfde aansluitingen.

Lutz Labs en Alieke van Sommeren

U sb bestaat al meer dan 25 jaar, je muis en toetsenbord maken al lang dankbaar gebruik van die makkelijk aansluitmethode. Met de snellere versies van USB 3.0 en de overstap naar de type C-aansluiting is usb de universele connector geworden voor verschillende randapparaten, van beeldschermen en snelle ssd's tot de oplaadpoort voor laptops. Andere standaarden voor randapparatuur zoals Fire-Wire en eSATA zijn volledig verdrongen door usb.

De vergelijkbare Thunderbolt-interface is in de pc-sector een stuk minder gangbaar, maar Mac-gebruikers maken er al jaren gebruik van. Thunderbolt-verbindingen worden als minder storingsgevoelig beschouwd, wat vooral belangrijk is voor professionele toepassingen. Het gangbaarder zijn qua gebruik in de Mac-omgeving kan ook te maken hebben met het feit dat Apple-gebruikers eerder bereid zijn om de hogere prijzen voor Thunderbolt-apparaten te betalen.

Maar op de Mac zijn er ook veranderingen geweest: met de overgang van versie 2 naar versie 3 gebruikt Thunderbolt de type C-aansluitingen en -stekkers die nu ook gebruikelijk zijn voor usb. Hoewel er adapters zijn waarmee je Thunderbolt 2-apparaten op nieuwere aansluitingen kunt aansluiten, is het kopen van zo'n adapter alleen in een paar speciale gevallen de moeite waard. Thunderbolt-apparaten kunnen mechanisch worden aangesloten op usb-aansluitingen via de type C-stekkers en omgekeerd. Pure Thunderbolt-apparaten, zoals ssd's,

werken echter niet op de usb-poort, terwijl usb-apparaten meestal wel werken op de Thunderbolt-poort – waarover later meer.

DIT KAN THUNDERBOLT

Thunderbolt (we hebben het hierna alleen over versies 3 en hoger) gebruikt vier draden voor de gegevensoverdracht. Dat maakt het mogelijk om apparaten aan te sluiten die rechtstreeks met PCIe werken, zoals grafische kaarten en behuizingen met een PCIe-slot voor speciale insteekkaarten. Dat soort behuizingen kunnen bijvoorbeeld worden gebruikt om een insteekkaart toe te voegen aan een laptop.

De overdrachtssnelheid van Thunderbolt is 40 Gbit/s, hoewel versie 3 slechts 16 Gbit/s garandeert. Dat is nog steeds voldoende voor hoge overdrachtsnelheden omdat het overzetten van video, audio en data in pakketten wordt verwerkt die via een gemeenschappelijke drager werken. Bij usb-docking via USB-C worden de draadparen daarentegen star en inflexibel toegewezen aan de overdracht van usb-gegevens of videosignalen, ongeacht of de lijn op dat moment nodig is of restcapaciteit heeft voor iets anders.

In tegenstelling tot bij usb, waar veel dingen niet-bindende opties zijn, specificeert Thunderbolt veel wel expliciet. Thunderbolt 4 schrijft bijvoorbeeld voor dat een dergelijke poort twee 4K-monitoren met een refreshrate van 60 Hz of als alternatief een van de zeldzame 5K-monitoren met 60 Hz moet kunnen aansturen – ongeacht de gegevensoverdracht. In principe zijn refreshrates tot 120 Hz mogelijk, maar dan alleen met een 4K-monitor.

Als je meer dan één Thunderbolt-apparaat wilt aansluiten, kan dat met TB3, net als bij eerdere revisies, alleen in de vorm van een zogeheten daisy-chain: je sluit het volgende apparaat aan op de uitgang van het ene apparaat. Veel Thunderbolt-apparaten hebben daar twee type C-aansluitingen voor. Er zijn maximaal zes apparaten achter elkaar te schakelen. Elke Thunderbolt-poort levert minstens 15 watt om de aangesloten randapparaten van energie te voorzien. Apparaten die meer nodig hebben, moeten hun eigen adapter hebben.

Thunderbolt kan ook laptops opladen via een datakabel. Eenvoudige kabels kunnen tot 65 watt overbrengen, zoals bij USB-PD, terwijl kabels met een geïntegreerde marker nodig zijn voor hogere oplaadcapaciteiten. In principe is opladen via USB-PD 3.1 mogelijk tot 240 watt, maar dat heeft weinig te maken met Thunderbolt maar met de USB-C-poort.



De Thunderbolt 4-dock (onderste), die meer dan 200 euro kost, heeft slechts een paar extra functies in vergelijking met de USB-C-dock voor 50 euro (bovenop), maar ze kunnen de meerprijs waard zijn. TB4 maakt het mogelijk om snellere opslagmedia en meer beeldschermen tegelijk aan te sluiten.

Er is bij versie 4 daarentegen het een en ander veranderd. Hoewel de bruto snelheid van 40 Gbit/s hetzelfde blijft, is de gegarandeerde datasnelheid verhoogd naar 32 Gbit/s. Tegelijkertijd stijgt de beeldschermresolutie naar 8K met 60 Hz. Bovendien moet een laptop uit de slaapstand ontwakken als hij is aangesloten op een TB4-dock en er een muis of toetsenbord via het dock aangesloten is.

Thunderbolt 4 verandert ook de topologie: naast het in serie schakelen van Thunderbolt-apparaten (daisy-chaining) kun je vanuit één Thunderbolt-bron meerdere Thunderbolt 4-hubs genereren, wat ook aan usb doet denken.

Intel heeft als uitvinder van Thunderbolt heel slim ook de juiste hubchip in zijn programma zitten: de JHL8440 integreert zowel een Thunderbolt 4-hub als een usb-poort volgens versie 3.2 Gen 2 met 10 Gbit/s. Die chip zit samen met de USB-PD-chips en usb-hubs in veel Thunderbolt-dockingstations [1].

Thunderbolt is vooral bij dockingstations nuttig omdat één enkele kabel tussen de dock en een laptop voldoende is voor een comfortabele werkplek. Je muis en het toetsenbord zijn dan aangesloten op de Thunderbolt-dock, net als twee grote monitoren, de netwerkaansluiting en een snelle ssd voor je back-up – en je laptop wordt tegelijkertijd opgeladen.

Thunderbolt 5 gaat nog een stap verder, vooral op het gebied van snelheid. Die versie zal naar verwachting 80 Gbit/s halen. Geschikte apparaten zullen in de loop van dit jaar uitgebracht worden. De bandbreedtebooster is ook interessant: de controller schakelt over naar een asymmetrische modus met drie lijnen in de richting van de client en één terug. Dat levert een snelheid van 120 Gbit/s op, bijvoorbeeld voor monitorsignalen, terwijl de tegenovergestelde richting wordt ‘afgeremd’ tot 40 Gbit/s.

Net als usb is Thunderbolt compatibel met oudere versies. Apparaten gebaseerd op Thunderbolt 3 moeten daarom ook werken op de nieuwe TB5-poorten, maar alleen met een maximum van 40 Gbit/s.

THUNDERBOLT-KABELS

Thunderbolt-kabels verschillen qua schakeling niet van usb-kabels. Ze moeten echter op hogere frequenties versturen, wat betekent dat een passieve Thunderbolt-kabel ook werkt met usb-apparaten, maar er omgekeerd problemen kunnen ontstaan met een usb-kabel en Thunderbolt-apparaten.

Met Thunderbolt 3 werden actieve kabels nog steeds voorgeschreven voor kabellengtes van meer dan 50 centimeter, maar passieve kabels werkten in sommige situaties nog steeds. Thunderbolt 4 schrijft alleen actieve kabels voor bij lengtes boven de twee meter, maar in de praktijk kom je zelden kabels tegen die langer zijn dan 80 centimeter.

Voor aanzienlijk langere verbindingen bieden bedrijven als Corning optische kabels aan. Aan beide uiteinden van dergelijke kabels, die tot 50 meter lang kunnen zijn, zitten converters, waardoor de kabels alleen kunnen worden gebruikt voor eindapparaten met een eigen adapter.

Thunderbolt-kabels zijn te herkennen aan het bliksemschichtsymbool op de connectors, het versienummer staat er meestal op gedrukt. Soms staat er ook een extra aanduiding van het vermogen dat de kabel kan overbrengen, maar meestal alleen als de kabel is ontworpen voor meer dan 65 watt.

Actieve kabels zijn in het algemeen alleen geschikt voor Thunderbolt. Als ze als usb-kabel worden gebruikt, wordt de maximale snelheid verlaagd naar 5 Gbit/s, oftewel USB 3.0 (3.2 Gen 1). Net als usb is Thunderbolt ontworpen om te worden aangesloten en losgekoppeld terwijl je pc actief is.

WACHTEN OP THUNDERBOLT 5?

De huidige Thunderbolt-versie is 4, maar er zijn nog steeds overal veel TB3-apparaten te koop. Die zijn nauwelijks goedkoper dan de huidige apparatuur met TB4, dus als je een nieuwe koopt, kun je het beste kiezen voor de nieuwste versie 4. Het actief vervangen van een TB3-apparaat door een TB4-model heeft zelden zin: de snelheid is niet toegenomen, met een maximum van 40 Gbit/s in beide richtingen. De andere verschillen zitten hem in de details.

Thunderbolt 5 belooft een nog hogere snelheid en meer bandbreedte voor het aansluiten van monitoren met een hoge resolutie. Maar die overstap, die op het moment van schrijven nog niet eens beginnen is, is waarschijnlijk alleen de moeite waard als er ook echt behoefte is aan de hogere snelheid. Als je nog geen 5K-monitor of meerdere 4K-monitoren op je bureau hebt staan, is randapparatuur met ‘slechts’ Thunderbolt 3 nog meer dan prima.

ct



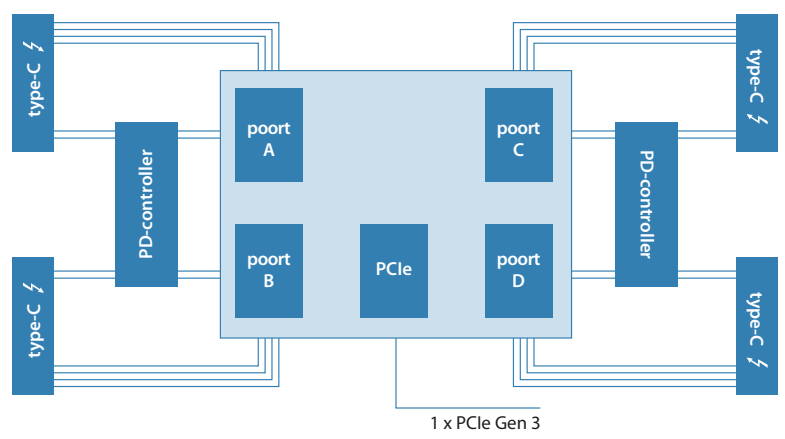
Thunderbolt-kabels zijn te herkennen aan het bliksemschichtsymbool (links). Ze zijn ook geschikt voor USB-C, maar niet andersom. De 4 geeft aan dat de kabel de datasnelheden van TB4 biedt.

Literatuur

[1] Lutz Labs en Alieke van Sommeren, Zeven docks met Thunderbolt 4, c't 8-9/2023, p.53

De opbouw van een Thunderbolt-hub

De Intel JHL8440 Thunderbolt 4-controller splitst een TB4-input en stuurt het signaal door naar drie TB4-uitgangen. De controller biedt ook een usb-poort met 10 Gbit/s (en USB 2.0) en pinnen voor verdere interne verbindingen via PCIe 3.0 x1. Fabrikanten van docks sluiten daar vervolgens LAN- en andere usb-interfaces op aan. De USB-PD-controllers voor het opladen van laptops bevinden zich tussen de Thunderbolt-aansluitingen van de controller en de type C-aansluitingen.





Illustratie Midjourney, c't

STARTSLOT VERWIJDEREN

Secure Boot en bootissues onder Linux

Secure Boot is bedoeld om bootvirussen en andere kwaadaardige code te voorkomen door het UEFI-BIOS alleen ondertekende bootloaders en kernels te laten starten. Dat geldt ook voor Linux. Als er beveiligingsproblemen opduiken, worden de handtekeningen ingetrokken via een Revocation List. De ruimte in het flashgeheugen van het BIOS is echter beperkt, daarom zijn er nieuwe technieken ontwikkeld.

Mirko Dölle en Alieke van Sommeren

De aankondiging van Microsoft in kennisbank-artikel KB5025885 dat extra kwetsbare bootmanagers vanaf begin april worden geblokkeerd, liet veel ruimte voor speculatie. Het verwijst naar de Secure Boot-kwetsbaarheid CVE-2023-

24932 aka Black Lotus, die Microsoft wil dichten in een multi-stage update. We hebben eerder al in detail beschreven wat dat betekent voor Windows-gebruikers [1]. Linux werd niet beïnvloed door Black Lotus, wat betekent dat er geen Linux-bootloaders zouden moeten opduiken in de verwachte update van de Revocation List (Secure Boot Forbidden Signature Database, DBX) van niet-vertrouwde bootloaders. Bij tests werden op sommige pc's toch vermeldingen voor Linux-bootloaders toegevoegd toen we de betreffende update handmatig uitvoerden.

We raden je ten zeerste af om die zelf te activeren. De update wordt in fase 4 pas geforceerd geïnstalleerd door Windows, wat gepland staat voor 8 oktober 2024. Dat maakt Microsofts aankondiging dat extra bootmanagers vanaf 9 april in fase 3 worden geblokkeerd des te cryptischer. Bij het testen begin april hadden we nog geen antwoord op de

vraag of Linux-systemen beïnvloed zouden kunnen worden door de aankomende extra blokkades.

Een nieuwe technologie, Secure Boot Advanced Targeting (SBAT), wordt om ruimtetechnische redenen gebruikt om de Linux-bootloaders te blokkeren die getroffen zijn door de HTTP-boot-kwetsbaarheid die begin februari 2024 werd bekend. Dat zou dus niets te maken moeten hebben met de uitsluitingen die zijn aangekondigd voor 9 april.

Omdat het niet mogelijk is om op voorhand te zeggen wat er zal veranderen en in welke mate Linux beïnvloed zal worden, geven we je een algemeen overzicht van wat Windows-updates te maken hebben met Linux-bootloaders en hoe de nieuwe Secure Boot Advanced Targeting kwetsbare bootloaders blokkeert.

KWESTIE VAN VERTROUWEN

Het Secure Boot-concept zorgt ervoor dat het UEFI-BIOS van een moederbord alleen bootloaders van een vertrouwde bron opstart. Daar worden verschillende certificaten met verschillende autorisaties voor opgeslagen in het BIOS. Bovenaan staat de Platform Key (PK) van de moederbordfabrikant. Daaronder staat de Key Exchange Key (KEK) van Microsoft, waarmee Microsoft geautoriseerd is om nieuwe certificaten en checksums te importeren, eventueel naast die van de hardwarefabrikant. Je kunt beide lijsten onder Linux opvragen met

```
sudo fwts uefidump - | less
```

uit het gelijknamige softwarepakket. De lijst is verdeeld in verschillende blokken, verwante delen zijn altijd even ver ingesprongen. Aan het begin staat de naam van het blok. De Platform Keys zijn bijvoorbeeld te vinden onder PK op de alfabetisch gesorteerde lijst, de Key Exchange Keys onder KEK.

Om een computer te kunnen certificeren voor Windows, moet de fabrikant ook twee certificaten leveren als Authorised Signatures (DB): Microsoft Windows Production PCA 2011 en Microsoft Corporation UEFI CA 2011. Als Secure Boot actief is, mag het BIOS alleen bootloaders uitvoeren die zijn ondertekend met een van de certificaten uit de DB. Soms is daar ook een certificaat van de hardwarefabrikant te vinden, en de fabrikant kan ook andere certificaten opslaan – bijvoorbeeld van Linux-distributies.

In de praktijk worden de meeste computers geleverd of gebruikt met Windows, dus je hoeft daar geen moeite voor te doen. De certificaten die op je computer zijn opgeslagen kun je vinden in de uitvoer van fwts in de sectie db.

Onder Boot0000 kun je zien welke bootloader je UEFI-BIOS als eerste opgeslagen heeft, Boot0001 kan een tweede bevatten enzovoort. Onder Info: vind je een duidelijke naam, zoals Windows Boot Manager, en onder Path: het pad naar de EFI-partitie (EFI System Partition, ESP) samen met de bestandsnaam. Standaard koppelt Linux de EFI-partitie onder /boot/efi zodat je de handtekening en integriteit van de Windows-bootloader kunt contro-

leren met het commando:

```
sudo sbverify /boot/efi/EFI/Microsoft /Boot/  
bootmgr.efi
```

Je kunt te weten komen met welk certificaat de bootloader is ondertekend met de extra parameter --list vóór de bestandsnaam.

VOORUITDENKEND

De minimalistische EFI-loader Shim is ontwikkeld om te voorkomen dat elke wijziging aan Grub opnieuw moet worden beoordeeld en gecertificeerd door Microsoft. Linux-distributies voegen hun eigen certificaat toe en dienen Shim vervolgens in bij Microsoft voor certificering. In plaats van het Windows-productiecertificaat te gebruiken, ondertekent Microsoft dergelijke bootloaders van derden altijd met het UEFI CA-certificaat. Het distributeurcertificaat in Shim stelt Canonical bijvoorbeeld in staat om Ubuntu's Grub, kernel en kernelmodules op elk gewenst moment zelf te ondertekenen. Als een Shim eenmaal ondertekend is, kan die soms jarenlang gebruikt worden. Installatiemedia voor Ubuntu 20.04 LTS hadden nog steeds de Shim van Ubuntu 18.04.

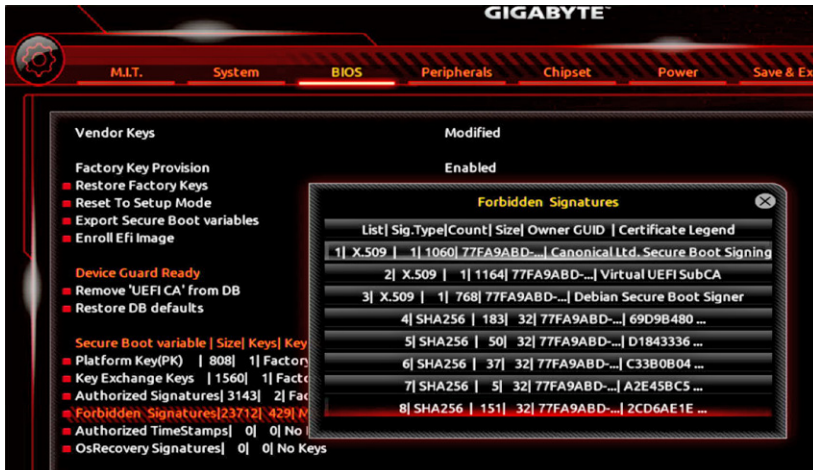
Microsofts Windows-bootloader, Shim en Grub bevatten soms echter ook fouten waardoor niet-ondertekende bootloaders of kernels geladen kunnen worden. De Revocation List DBX is beschikbaar in het UEFI-BIOS om dergelijke onveilige bootloaders achteraf te kunnen blokkeren. De checksums van bootloaders die als onveilig worden herkend, moeten op die lijst worden opgeslagen.

De huidige Revocation List kan worden gedownload van het UEFI-forum en wordt soms ook bijgewerkt door hardwarefabrikanten tijdens BIOS-updates, zodat er in een nieuwe pc al meer dan honderd items zijn opgeslagen

Verdere checksums worden toegevoegd via updates van besturingssystemen, bijvoorbeeld met de Windows-update van 9 augustus 2022, waarna de Linux-installatiemedia van verschillende distributies niet meer opstartten. Niet alle fouten betroffen Shim: Microsoft blokkeerde ook Shims die defecte Grub-bootloaders startten, ondertekend door de betreffende distributeur. Er zijn ook updates voor de blacklist onder Linux. Die worden geïnstalleerd via fwupd als onderdeel van de reguliere pakketupdates.

Het UEFI-BIOS accepteert echter alleen Revocation Lists van vertrouwde bronnen waarvan het certificaat is opgeslagen op de lijst met Key Exchange Keys. Daarom voert Ubuntu bijvoorbeeld ook Canonicals master CA-certificaat daar in tijdens het installeren op systemen met Secure Boot ingeschakeld en niet alleen op de DB-lijst die bootloaders autoriseert.

De DBX-update beschreven in KB5025885, die uiterlijk in oktober 2024 door Windows geforceerd geïnstalleerd moet worden, bevat opnieuw honderden checksums: dit keer voornamelijk van Windows bootloaders die defect zijn. En door de HTTP-kwets-



De zwarte lijst voor deze computer is al aangegroeid tot 429 vermeldingen. We vonden in totaal meer dan 600 verschillende vermeldingen.

baarheid die in februari bekend werd, zouden er weer talloze Shims op de blacklist moeten worden gezet, waardoor het krap wordt in de DBX-database. Volgens de Shim-ontwikkelaars zit er op veel moederborden slechts 32 kB BIOS flashgeheugen.

GRENSOVERSCHRIJDEND

Je kunt erachter komen hoe groot de Revocation List al is geworden onder Linux met het commando `sudo ls -l /sys/firmware/efi/efivars/dbx-*`. Op een van onze laptops, waarop Windows 10 zonder de optionele update uit KB5025885 was geïnstalleerd naast Ubuntu 22.04 LTS, was de DBX-lijst al meer dan 13 kB groot. Je kunt met `dbxtool` uitvinden hoeveel geblokkeerde entries hij bevat:

```
dbxtool -l | wc -l
```

Het resultaat op de laptop was 272 vermeldingen. Op een pc met Ubuntu 22.04 LTS, waarop nooit iets anders dan Ubuntu geïnstalleerd was, vonden we slechts 186 vermeldingen. Dat veranderde drastisch nadat we daar Windows 10 op installeerden en de update beschreven in KB5025885 activeerden: het DBX-bestand zwol toen aan tot meer dan 24 kB en 429 vermeldingen.

AFSLANKKUUR

Om niet nog meer ruimte te gebruiken, zijn de Shim-ontwikkelaars niet van plan om de Shims die getroffen worden door het HTTP-gat te deactiveren via extra vermeldingen in de Revocation List, maar om in plaats daarvan Secure Boot Advanced Targeting (SBAT) te gebruiken, wat Shim al enige tijd ondersteunt. Het belangrijkste verschil is dat SBAT geen constant groeiende lijst is zoals de DBX-database, maar dat waarden steeds opnieuw worden vervangen om ruimte te besparen.

De aanpak van de DBX-database om simpelweg nieuwe items aan de bestaande toe te voegen, voorkomt effectief dat iemand een verouderde Revocation List importeert en zo bootloaders die al lang geblokkeerd zijn weer inschakelt. De SBAT-ontwikkelaars willen daarentegen in staat zijn om de en-

tries in de SBAT-lijst voortdurend aan te passen en, indien mogelijk, in te korten. Om ervoor te zorgen dat niemand een oude SBAT-lijst kan importeren, gebruiken ze de EFI Variable Time Based Authenticated Write Access: de tijdstempel van de handtekening van de nieuw te importeren lijst wordt gecontroleerd. De uitwisseling vindt alleen plaats als die nieuwer is dan die van de bestaande lijst.

De SBAT-CSV-lijst (Comma-Separated Values) bevat informatie over SBAT zelf en over de componenten die betrokken zijn bij Secure Boot. Die omvatten de Stage 1-bootloader Shim, Grub als Stage 2-bootloader en de kernel, maar ook de firmware-update-daemon `fwupd` of een hypervisor voor systemen met virtualisatie. Elk onderdeel, een product genoemd, heeft een naam die door de ontwikkelaars is gedefinieerd, zoals `sbat`, `shim` of `grub`. Dat wordt aangevuld met de naam van de fabrikant. De Grub-bootloader van Debian Linux heeft bijvoorbeeld de productnaam `grub.debian`.

De productnaam wordt als tweede voorgescreven waarde van elke regel gevolgd door het zogenaamde generatienummer. Dat moet je niet verwarren met het versienummer. Het generatienummer is een opeenvolgend geheel getal dat alleen aangeeft hoeveel beveiligingsupdates er voor dat product al gemaakt zijn sinds het SBAT ondersteunt. Dat klinkt wellicht ingewikkeld, maar dat is het niet, zoals de volgende voorbeelden laten zien.

Voor de volledigheid: de individuele regels van de SBAT-CSV-lijst kunnen ook nog drie andere waarden bevatten, namelijk de projectnaam, zoals `grub` of `grub2` voor Grub (maar niet `grub.debian`), het exacte versienummer inclusief patchniveau, zoals `2.02-0.34.e17_2`, en een url of e-mailadres dat naar het project leidt. Hier is de volledige SBAT-informatie voor Grub van Debian:

```
grub.debian,2,Debian,grub2,2.04-13,https://
packages.debian.org/source/sid/grub2
```

NIEUWE GENERATIE

De Grub-bootloader versie 2.04-13 van het Debian-project heeft generatienummer 2 omdat die versie van Grub een beveiligingslek heeft gedicht dat voor Secure Boot bij eerdere versies relevant was. Ervan uitgaande dat het Debian project overschakelt naar Grub-versie 2.05 voor nieuwe functies, gaat de SBAT-entry er als volgt uit zien:

```
grub.debian,2,Debian,grub2,2.05-1, https://
packages.debian.org/source/sid/grub2
```

Dat is nog steeds de tweede generatie `grub.debian` component, omdat er geen Secure Boot-gerelateerde beveiligingsupdates zijn gemaakt. Of iemand de nieuwe Grub in versie 2.05-1 of versie 2.04-13 gebruikt, is irrelevant vanuit het oogpunt van beveiliging. Het generatienummer is daarom onafhankelijk van het versienummer.

Het beveiligingslek dat bij Grub leidde tot de generatiewissel van 1 naar 2 bestond niet alleen in het Debian-project. Integendeel, praktisch alle Linux-distributeurs hadden daar last van. Om te voor-

komen dat kwetsbare versies van Grub gebruikt blijven worden, werd in 2022 deze SBAT Revocation List gepubliceerd met de nieuwe Grub-builds:

```
sbat,1,2022052400
```

```
grub,2
```

De eerste regel bevat de timestamp van de SBAT-update en voorkomt dat er later een oudere versie van de Revocation List geïnstalleerd kan worden. De tweede regel verbiedt het starten van alle `grub`, ongeacht de distributeur, die niet minstens van generatie 2 zijn. Je kunt op elk moment te weten komen hoe je huidige SBAT-Revocation List eruitziet met het commando

```
mokutil --list-sbat-revocations
```

In november 2022 werden er nog twee beveiligingslekken voor verschillende distributies gedicht, waardoor alle distributeurs overstapten op generatie 3. Het Debian-project deed hetzelfde en bracht build 2.06-3~deb10u2 van Grub uit:

```
grub.debian,3,Debian,-
grub2,2.06-3~deb10u2,https://packages.debian.org/source/sid/grub2
```

De vermelding op de Revocation List werd ook bijgewerkt, zodat Grub van de tweede generatie over het algemeen niet meer opstart:

```
grub,3
```

De maintainer maakte echter een fout bij het compileren van de nieuwe Grub-pakketten: de fix voor de kwetsbaarheid CVE-2022-2601 was niet opgenomen in Debian 10 Buster, terwijl dat in die voor Debian 11 Bullseye wel het geval was. Daardoor werden Grubs van de derde generatie uitgebracht die nog steeds kwetsbaar waren. De packet-maintainer moest de bug daarom repareren en ook de generatie naar 4 verhogen. De SBAT-entry was toen:

```
grub.debian,4,Debian,-
grub2,2.06-3~deb10u3,https://packages.debian.org/source/sid/grub2
```

De officiële Revocation List stond echter nog steeds generatie 3-bootloaders toe en dus ook de kwetsbare builds voor Debian Buster. Een mogelijke oplossing zou zijn geweest om de generatie voor alle Grubs te verhogen naar 4:

```
grub,4
```

Maar dan hadden alle distributies nieuwe builds van Grub moeten publiceren waarin alleen het generatienummer was veranderd. De ontwikkelaars namen daarom genoegen met een distributiespecifieke definitie van het generatienummer en publiceerden de volgende SBAT Revocation List met Shim versie 15.8:

```
grub,3
```

```
grub.debian,4
```

Zo'n uitzondering zou ook andersom mogelijk zijn als een bepaalde distributie niet getroffen wordt door een anders wijdverspreide bug. In dat geval zou een distributiespecifieke vermelding ook een lager generatienummer kunnen hebben dan geldig is voor het algemene product. De Shim-ontwikkelaars willen daar in de toekomst ruimte besparen en zo min mogelijk uitzonderingen vermelden.

CONCLUSIE

De designfouten in Secure Boot hebben het opstartproces enorm gecompliceerd, en het is te voorzien dat er binnenkort geen bootloaders meer geblokkeerd kunnen worden via een Revocation List. Met SBAT heeft de opensource-community een eigen technologie ontwikkeld die vanaf het begin ontworpen is om ruimte te besparen en de potentie heeft om niet gestaag uit te dijen.

SBAT betekent echter niet dat distributeurs niet langer afhankelijk zullen zijn van Microsoft om Shim steeds opnieuw te laten certificeren en ondertekenen. Dat komt omdat Secure Boot nog steeds alleen bootloaders toestaat om op te starten vanaf een betrouwbare bron, en voor bijna alle hardware-fabrikanten is dat nog steeds alleen Microsoft. **ct**

Literatuur

- [1] Axel Vahldiek en Alieke van Sommeren, Naderende boot(loader)issues voor Linux en Windows, c't 6/2024, p.80

Secure Boot-geneuzel

Tijdens het ontwikkelen van Secure Boot werd al voorzien dat er ooit bootloaders zouden komen waarvan de beveiligingsproblemen pas bekend zouden worden nadat ze als betrouwbaar ondertekend waren. Daarom werd vanaf het begin in de specificatie opgenomen dat er een Revocation List (Forbidden Signature Database, DBX) in het UEFI-BIOS moet zijn, waarin de checksums van de als onveilig herkende bootloaders achteraf kunnen worden ingevoerd.

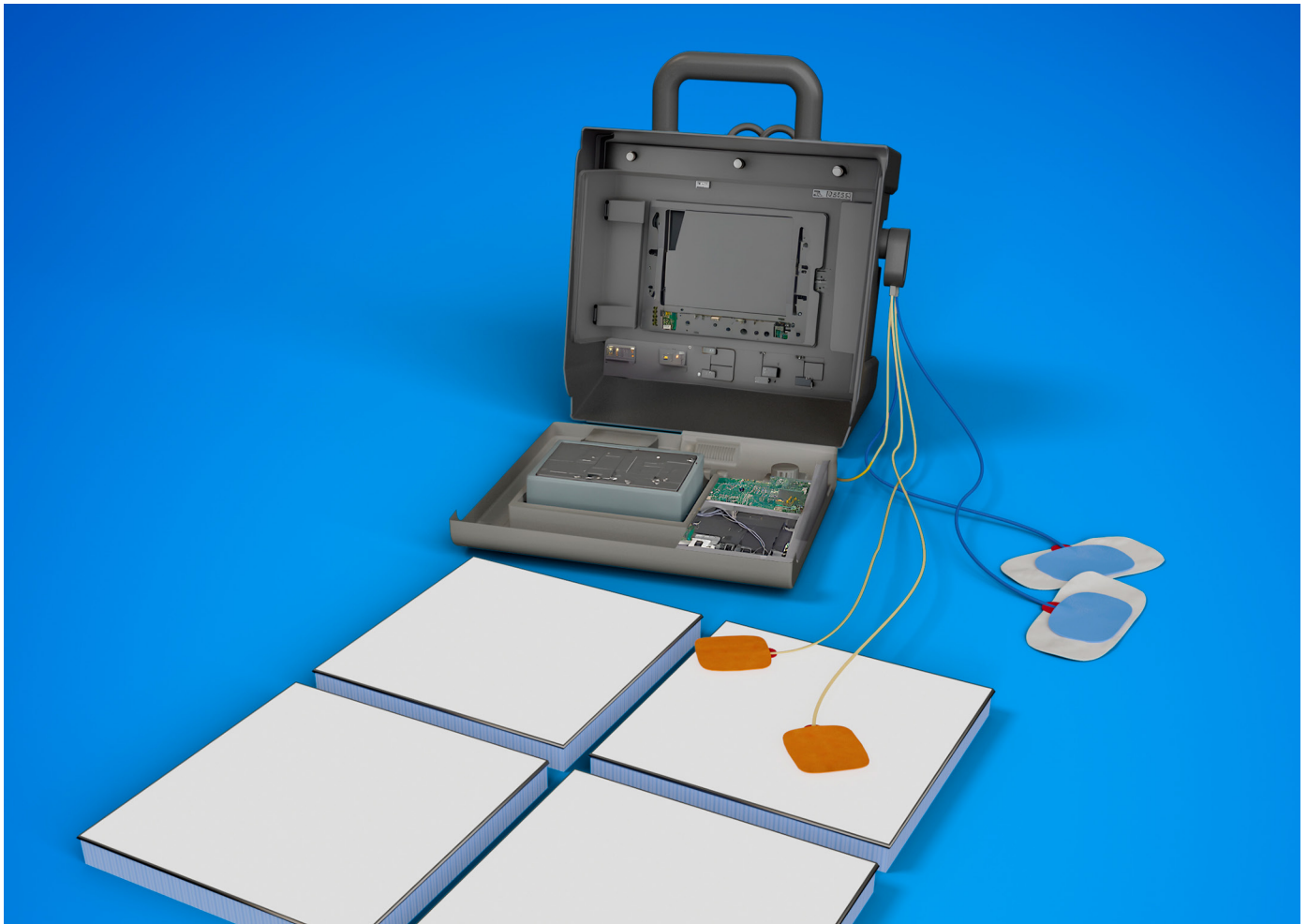
De specificatie was echter slordig en er is geen bindende specificatie voor de minimale hoeveelheid flashgeheugen die moederbord-fabrikanten in het UEFI-BIOS moeten voorzien. Volgens de Shim-ontwikkelaars is daar afhankelijk van het moederbord slechts 32 kB voor beschikbaar. Hoeveel ruimte de DBX-lijst op een bepaalde pc inneemt moet per geval worden gecontroleerd. In ons onderzoek varieerde het van minder dan 1 kB met slechts 10 vermeldingen tot meer dan 24 kB met meer dan 420 vermeldingen.

ALTIJD ONVOLLEDIG

Er is geen plausible verklaring voor de ernstige verschillen in de blacklists op de computers die we analyseerden voor [1]. Alle blokkadellijsten zouden, ongeacht het besturingsstelsel, eigenlijk hetzelfde moeten zijn – op voorwaarde dat alle

beschikbare updates geïnstalleerd zijn. Het UEFI-forum publiceert op zijn website ook het DBX-bestand dat door Microsoft is gemaakt. Desondanks vonden we pc's met tot wel 50 vermeldingen die niet in het UEFI-DBX-bestand stonden. We vroegen Microsoft, als eigenaar van de handtekeningcertificaten, ook om een volledige lijst van alle teruggetrokken bootloaders, maar kregen daar nog geen antwoord op. Verschillen in het aantal DBX-entries en de checksums tussen verschillende pc's waren bij ons onderzoek de regel, niet de uitzondering.

Dus zelfs nu, wanneer de zwarte lijsten nog in het flashgeheugen van de moederborden passen, is er geen garantie dat een pc alle gecompromitteerde bootloaders zal weigeren. Het concept heeft gefaald en het einde van die manier van werken is in zicht. Microsoft en de Shim-ontwikkelaars werken daarom aan alternatieven. Microsoft heeft een technologie ontwikkeld die vermoedelijk Code Integrity Boot Policy [1] wordt genoemd. Aan de kant van Linux is Secure Boot Advanced Targeting, kortweg SBAT, ontstaan. Terwijl het UEFI-BIOS weigert om het systeem op te starten met de DBX-entries, zijn het met Code Integrity en SBAT respectievelijk de Windows-kernel en de Linux-bootloaders Shim en Grub die herkennen dat Secure Boot niet langer gegarandeerd is en daarom weigeren.



Illustratie Moritz Reichartz

TOOLMAKER

Tips en trucs om c't-rescue-Windows uit te breiden

Volg ons achter de schermen van ons rescuesysteem, dat we eerder dit jaar presenteerden. We laten zien hoe het werkt en geven voorbeelden van hoe je het bouwpakket zelf kunt uitbreiden – je hebt immers nooit genoeg tools.

Peter Siering en Noud van Kruysbergen

We hebben de afgelopen jaren telkens een rescue-Windows uitgebracht als een bouwpakket omdat Microsoft de minimale Windows PE (Preinstallation Environment) die daarvoor als basis wordt gebruikt wel openbaar beschikbaar stelt om te downloaden, maar daar geen licenties voor uitgeeft die ons in staat stellen om het te redistribueren. Het bouwpakket voert scripts uit die geschreven zijn in een taal die ooit werd geïntroduceerd door het WinBuilder-programma.

De basis van ons rescuesysteem is een project gebaseerd op Windows PE. Dat hebben we niet zelf uitgevonden, derden ontwikkelen dat al langer. Sinds vorig jaar gebruiken we PhoenixPE als basis. Wat we

in dit artikel uitleggen is daar ook op van toepassing. Het doel van alle PE-projecten is om de Preinstallation Environment (PE), die een beperkt aantal functies heeft, te upgraden zodat het reguliere Windows-programma's kan uitvoeren.

Een typische, officiële vertegenwoordiger van zo'n PE-systeem is de omgeving die start vanaf een Windows-installatieschijf om het besturingssysteem startklaar over te brengen naar de harde schijf van een pc – vandaar de naam Preinstallation Environment. In de Windows Assessment and Deployment Kit (ADK) biedt Microsoft hulpmiddelen om dat proces te beïnvloeden. Vroege PE-projecten gebruikten dat, maar tegenwoordig werkt het bijna zonder.

Op een 'herstelstation', dat je onder Windows kunt aanmaken met de wizard met dezelfde naam, staat ook een PE-variant. Windows' eigen wizard schrijft naar een usb-stick, waar vanaf dan een aangepaste PE-omgeving gestart wordt. Die bevat echter relatief weinig programma's. Het enige interactieve element om bestanden te bekijken is de Opdracht-prompt.

Microsofts eigen PE-omgeving is erg zuinig als het gaat om de programma's die het bevat. Vaak is slechts alleen Opdrachtprompt beschikbaar. Bovendien ontbreken veel bibliotheken, waardoor sommige portable software die zonder installatie zou moeten kunnen, het niet doet. Bovendien heeft de 64-bit omgeving geen functies voor 32-bit programma's.

PE UITBREIDEN

De kunst van alle PE-projecten is om de minimale Windows-variant die in het bestand Boot.wim zit zodanig te verbeteren dat het leert om andere programma's te draaien. De projecten bereiken dat door de registersleutels aan het basissysteem toe te voegen die de software gewoonlijk verwacht, de nodige bibliotheken toe te voegen en zelfs het subsysteem uit te breiden om 32-bit programma's uit te voeren in een 64-bit omgeving (WOW64 [1]).

Om dat te doen, halen de projecten de in PE ontbrekende bestanden uit het bestand install.wim van een originele Windows-dvd en voegen die toe aan Boot.wim. Centrale onderdelen die zorgen voor een ordelijke systeemstart in een reguliere Windows-installatie worden vervangen door eigen creaties. Zo voert pecmd.exe de betreffende stappen aan en vult het startmenu. Op dezelfde manier zorgt penetwork.exe voor het netwerk.

Over de scripts: de WinBuilder die oorspronkelijk werd gebruikt, geschreven in Delphi (Borlands Pascal-IDE), had verschillende eigenaardigheden en de broncode was niet toegankelijk. Begin 2018 publiceerde Hajin Jang PEBakery, een Winbuilder-alternatief op GitHub, dat hij implementeerde in C# en uitbracht onder een GPL-licentie. Het programma heeft zich ontwikkeld tot een geweldig alternatief.

PEBakery is op de belangrijke punten volledig compatibel met Winbuilder en grotendeels vrij van eigenaardigheden. Er hoeven in bestaande scripts relatief weinig wijzigingen te worden aangebracht om ze te converteren van WinBuilder naar PEBakery. Speciale opties die PEBakery in staat stellen om bepaalde eigenaardigheden van WinBuilder na te bootsen helpen ook.

ALGEMENE STRUCTUUR

PEBakery heeft de basisstructuur van een project behouden, oftewel de manier waarop de scripts moeten worden gebundeld tot een groter geheel. Een project bestaat uit een map in Projects (zoals Projects\PhoenixPE) met daarin een bestand genaamd script.project dat het overkoepelende project beschrijft, zoals c't Emergency Windows 2024.

Alle andere scripts staan in die map of in submappen. PEBakery leest die projectboom volledig bij het opstarten en voert de instructies uit die in script.project staan. Bij c't-rescue-Windows 2024 zorgen die ervoor dat het welkomstbericht verschijnt en krijg je instructies over de bediening.

Twee andere bestanden zijn belangrijk: het bestand PEBakery.ini bevindt zich in de hoofdmap van het overkoepelende project (bijv. c:\ctrescue). Het

beschrijft de naam van het project respectievelijk de naam van de submap (PhoenixPE) en enkele andere startopties voor PEBakery.

Het tweede bestand, dat zich bevindt in c:\ctrescue\Projects\PhoenixPE, heet folder.project. Dat beschrijft verdere mappen die bij het project horen en in c:\ctrescue\Projects moeten staan – PhoenixPE stelt voor om de map MyApps te gebruiken om je eigen scripts in op te slaan die het project uitbreiden.

SCRIPTKERN

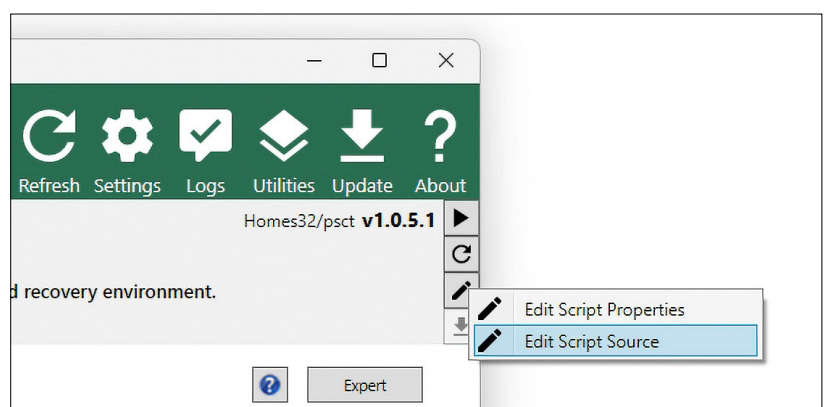
Op het eerste gezicht lijken de scripts op INI-bestanden omdat ze secties tussen vierkante haken gebruiken voor het structureren en variabelen en opties het typische formaat van een opdracht gebruiken. In feite maken onder meer onze uitbreidingen ook gebruik van die gelijkens door functies voor het bewerken van INI-bestanden op scripts los te laten om aanpassingen te maken.

De sectie [Main] beschrijft de basisgegevens van een script. Daar staat hoe het heet (Title), wat het doet (Description), wie het geschreven heeft (Author), wanneer het moet draaien (Level), of het gekozen is om te draaien (Selected), of het verplicht moet draaien (Mandatory), welke versie het is (Version) en wanneer het geschreven is (Date). Sommige regels zijn conventies, andere zijn belangrijk voor het hele project.

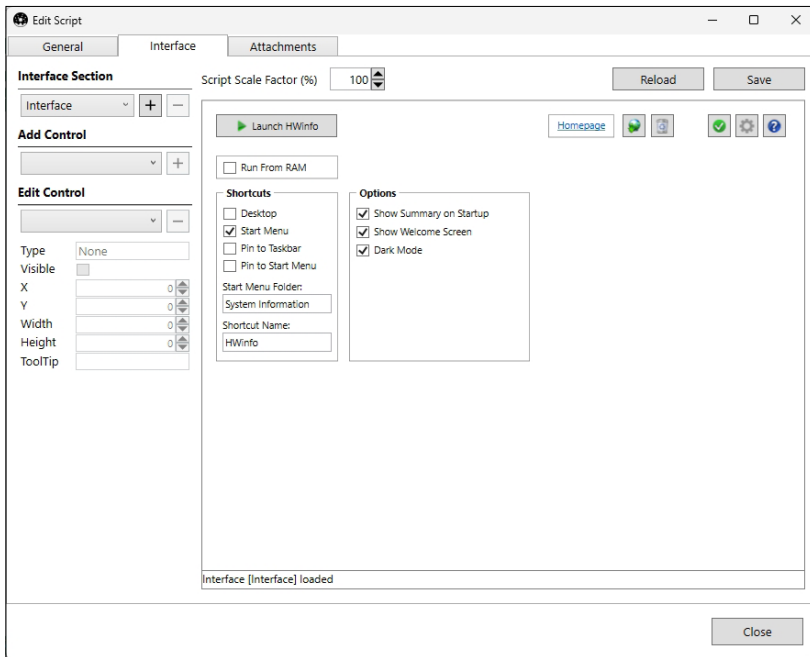
Variabelen worden vooraf toegewezen bij de sectie [Variables]. Dat is altijd handig als een script meerdere keren gegevens gebruikt die kunnen veranderen, bijvoorbeeld download-url's. Je kunt variabelen in de scripts herkennen aan het feit dat hun naam begint en eindigt met een procentteken – ze zijn vergelijkbaar met variabelen in batchbestanden, maar delen geen naamruimte en zitten elkaar dus niet in de weg.

Zowel PEBakery als WinBuilder werken met een aantal voorgedefinieerde variabelen. In %BaseDir% staat de naam van de hoofdmap, zoals c:\ctrescue, %ProjectDir% verwijst naar de projectbestanden, bijvoorbeeld c:\ctrescue\Projects\PhoenixPE. Scripts vinden hun eigen bestandsnaam via %ScriptFile%.

De bovengenoemde variabelen en nog een paar andere kunnen niet door een script veranderd wor-



Je kunt scripts vanuit PEBakery bewerken via het potloodpictogram. Het is handig om Visual Studio Code daarbij als editor te gebruiken.



Om de gebruikersinterface voor een script te maken, biedt PEBakery zijn eigen grafische editor om elementen zoals invoervelden te positioneren en het uiterlijk aan te passen.

den. Ze worden ook Fixed Variables genoemd. PEBakery definieert ze aan het begin van het project of script. Dergelijke variabelen worden ook gedefinieerd bij [Variables] in het bestand script.project en zijn altijd zichtbaar in alle scripts (Global Variables). Variabelen in een script zijn alleen daar zichtbaar.

Een script hoeft niet per se variabelen te definiëren in de sectie [Variables]. Het kan dat ook op elk willekeurig moment doen met de aanroep `Set,%-MijnVariabele%, "Mijn Tekst"` - in dit voorbeeld krijgt de variabele "Mijn Tekst" als inhoud. Als het script de optie GLOBAL met een komma aan de aanroep toevoegt, kunnen andere scripts ook toegang krijgen tot de inhoud en de variabele wijzigen. PEBakery geeft een duidelijke lijst van de variabelen in de logs.

De instructies die een script uitvoert komen terecht in een derde sectie: [Proces]. Daar kan een script de verschillende commando's die PEBakery biedt op elke gewenste manier combineren: archieven downloaden, uitpakken, bestanden kopiëren, tekstbestanden aanpassen en externe programma's uitvoeren.

Scripts kunnen het register van het rescuesysteem aanpassen, voorwaarden controleren en scriptpaden uitvoeren, WIM-bestanden bewerken, lijsten bewerken en die in loops uitvoeren. Bij uitgebreide scripts moet de auteur extra secties introduceren die een script kan aanroepen als een subroutine.

Veel scripts bevatten nog een sectie, namelijk [Interface]. Die beschrijft de gebruikersinterface, die opties weergeeft die door de gebruiker kunnen worden geselecteerd. Sommige scripts gebruiken dat om dialogen van meerdere pagina's te maken om details te definiëren, maar veel scripts kunnen het ook helemaal zonder. Niemand hoeft cryptische teksten te schrijven voor de interface: een interactieve edi-

tor voor de besturingselementen in PEBakery helpt je daarbij.

Er zijn verschillende andere secties die worden gemaakt bij het bewerken van scripts in PEBakery, bijvoorbeeld om logo's voor een script te beheren en op te slaan. Het is zelfs mogelijk om binaire bestanden te uploaden in een script. Die worden dan Text Base64-gecodeerd ingevoegd als een sectie in het gewone bestand (vergelijkbaar met bijlagen in e-mails). Het script kan toegevoegde binaire data weer uitlezen met speciale commando's.

SCRIPTVOLGORDE

De volgorde waarin PEBakery een compleet bouw pakket uitvoert hangt af van twee factoren: de ruwe volgorde wordt gegeven door Level in de [Main]-sectie. In Level 1 tot 4 worden voorbereidingen getroffen voor het basissysteem, in Level 5 voegt een project meestal programma's toe, in Level 6 worden stuurprogramma's toegevoegd, van Level 7 tot 9 wordt er opgeschoond en uiteindelijk het ISO-bestand gebouwd. Op Level 0 kunnen ontwikkelaars scripts deponeren die niet hoeven te draaien en die PEBakery niet weergeeft, maar waarvan de functies kunnen worden aangeroepen door andere scripts.

Het is gebruikelijk geworden om de namen van de afzonderlijke scriptbestanden en mappen te voorzien van driefijferige nummers binnen de levels. De sortering bepaalt de volgorde waarin PEBakery de scripts uitvoert. Veel ruimte maakt het makkelijker om daar eigen scripts tussen te plaatsen.

In principe kan een script worden uitgevoerd in de algemene context van een project wanneer je op de Build-knop drukt in het PEBakery-venster. Als alternatief kan een afzonderlijk script rechtstreeks worden gestart via de Play-knop. PEBakery voert het script dan uit, ongeacht of het is gemarkeerd als Selected in de [Main]-sectie of niet.

Het starten van een enkel script maakt het testen ervan veel eenvoudiger omdat niet altijd het hele project hoeft te draaien voordat de nieuw toegevoegde code uitgevoerd wordt. Maar scripts wijzigen bestanden in de projectboom, downloaden ze, pakken ze uit en wijzigen ze. Een script moet daarom altijd worden getest in de algehele context wanneer het afzonderlijk uitgevoerd wordt. En wel in twee situaties: één keer in een schone projectboom en één keer in een projectboom die al in gebruik is.

Een schoon script moet uitgaan van een specifieke toestand, maar altijd controleren of die bestaat. De meeste scripts controleren eerst of een bestand al gedownload is voordat ze het uitpakken. Er kunnen echter onvoorziene dingen gebeuren: als een download afbreekt, kan de uitpakstap mislukken omdat het bestand onvolledig is. Maar weinig scripts zijn voorbereid op dergelijke situaties en accepteren dat de projectrun dan wordt afgebroken met een foutmelding - om pragmatische redenen worden downloads niet gecontroleerd door checksums.

PhoenixPE, en dus ook c't-rescue-Windows, proberen tijdens een volledige projectrun de essentiële

logbestanden te bundelen in een gecomprimeerd pakket in de map Logs. Als er maar één script draait, kun je de PEBakery-logviewer gebruiken. Indien nodig toont hij de uitvoer van een script in HTML-vorm. Dat stelt je in staat om de voortgang van een zelfontwikkeld script achteraf te volgen, maar ook om te bestuderen hoe andere scripts zich gedragen. Dat laatste is essentieel om aan de slag te gaan met scripting: wat je kunt kopiëren uit andere scripts hoeft je zelf niet meer te bedenken.

SCRIPTING-FRAMEWORK

PhoenixPE biedt bovendien tools voor het genereren van scripts. Je kunt die vinden bij de projectboom in 'PhoenixPE / Toolbox / ScriptFactory'. Om een scriptraamwerk te maken, vul je gewoon de velden in en druk je op de knop Create Script. De varianten van de scripts spreken voor zich, net als de meeste velden. Een opmerking over Script Folder: dat veld bepaalt of het script ook in een andere submap wordt geplaatst in de map die is gespecificeerd door Level in de projectboom (zoals ze bestaan bij Applications).

PEBakery plaatst een nieuwe aangemaakt script direct in de projectboom. Als je een fout hebt gemaakt bij het aanmaken, moet je zelf bestanden en mappen verwijderen die door de actie in het bestandssysteem zijn aangemaakt. Daar zijn binnen PEBakery geen functies voor. PEBakery herkent dergelijke veranderingen niet automatisch. Je moet dan klikken op de Refresh-knop op de bovenste toolbar. Hetzelfde geldt als je je scripts direct aan het bestandssysteem toevoegt.

Alle bewerkingstappen voor een script zijn toegankelijk vanuit PEBakery. Dat kan op de scriptpagina of via het contextmenu in de projectboom. PEBakery biedt functies voor het bewerken van de scripteigenschappen (Edit Script Properties), het uploaden van logo's, het instellen van opties bij [Main], het ordenen van bedieningselementen voor het script en het beheer van bestandsbijlagen in mappen.

Om de broncode te bewerken (Edit Script Source) gebruikt PEBakery de bij Windows als standaard ingestelde editor als Visual Studio Code niet geïnstalleerd is. VS Code wordt sterk aangeraden, omdat er zelfs een extensie is voor PEBakery-scripts die niet alleen de taalelementen kleurrijker maakt, maar ook helpt met suggesties bij het schrijven van scripts. Dat maakt het makkelijker om de syntaxis te leren, die even wennen is.

SCRIPTVOORBEELD

Het volgende concrete voorbeeld beschrijft de stappen voor het integreren van RustDesk (een alternatief voor AnyDesk). Voordat je aan de slag gaat, moet je eerst uitproberen hoe de software zich gedraagt als je het handmatig in het rescuesysteem brengt. Kopieer het EXE-bestand naar een nieuwe map op een usb-stick die met het bouwpakket gemaakt is, start die op en start het programma. RustDesk.exe zal dan melden dat het DLL's mist. Volgens de foutmeldingen gaat het daarbij om glu32.dll en opengl32.dll.

```
[Main]
Title=RustDesk
Author=ps@ct.de
Level=5
Version=1.1.0.0
Description=Remote desktop software and open source TeamViewer
alternative
Date=2023-11-04
Selected=False
Mandatory=False

[Variables]
%ProgramFolder%="RustDesk"
%ProgramExe%="rustdesk.exe"
%DownloadURL%=https://github.com/rustdesk/rustdesk/releases/
download/1.2.3/rustd
%ConfigFile%="RustDesk2.toml"

[Process]
Echo,"Processing %ScriptTitle%..."
If,%cb_RunFromRam%,Equal,True,RunFromRam
If,%cb_AlwaysDownload%,Equal,True,DirDeleteEx,"%ProgramsCache%\%ProgramFolder%"
If,Not,ExistFile,"%ProgramsCache%\%ProgramFolder%\%ProgramExe%",Run,%ScriptFile%
FileCopy,"%ProgramsCache%\%ProgramFolder%\%ProgramExe%", "%TargetPrograms%\%Progr

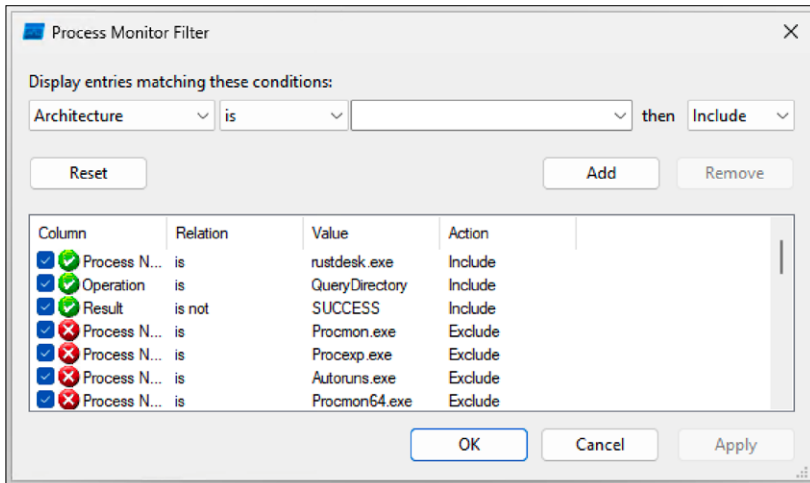
RequireFileEx,AppendList,\Windows\System32\sas.dll
RequireFileEx,AppendList,\Windows\SysWOW64\sas.dll
RequireFileEx,AppendList,\Windows\System32\opengl32.dll
RequireFileEx,AppendList,\Windows\SysWOW64\opengl32.dll
RequireFileEx,AppendList,\Windows\System32\glu32.dll
RequireFileEx,AppendList,\Windows\SysWOW64\glu32.dll
RequireFileEx,ExtractList

[DownloadProgram]
Echo,"Downloading %ScriptTitle%..."
WebDownload,%DownloadURL%, "%ProgramsCache%\%ProgramFolder%\%ProgramExe%",NOERR
If,Not,#r,Equal,200,Halt,"Download failed: The code returned was
[#r]."
```

Het hier verkort weergegeven script voor het integreren van RustDesk zit al in het bouwpakket van ons rescuesysteem.

Je kunt dan proberen die DLL's van Windows naar het rescuesysteem te kopiëren. In het ideale geval gebruik je de bestanden van een Windows-installatie met een identieke versie als degene die je aan het bouwpakket toevoegt. Het is voldoende om de DLL-bestanden te kopiëren naar de map waarin de gedownloade Rust Desk – gelukkig is het programma niet verpakt in een installatieprogramma.

Ondanks de toegevoegde DLL's start RustDesk nog niet. Het enige wat dan helpt is dieper naar de oorzaak zoeken. De Sysinternals-tool Procmon is daar zeer geschikt voor. Het registreert en toont de functie-aanroepen van een programma. Je kunt Procmon downloaden en starten terwijl het rescuesys-



Met een filter in Sysinternals Processmonitor kun je snel achterhalen welke DLL's een programma wil laden, maar blijkbaar niet kan vinden.

teem draait – het hoeft niet te worden geïnstalleerd en alle bibliotheken zitten in het rescuesysteem.

Zorg ervoor dat je na het starten van Procmon het automatisch opnemen van gebeurtenissen uitschakelt met Ctrl+E – het slaat alles op in het RAM, en dan kom je al snel ruimte tekort. Pas kort voordat je RustDesk weer probeert te starten, laat je Procmon de gebeurtenissen weer opnemen. Na de start beëindig je dat snel weer.

Maak dan een filter in Procmon om de getoonde resultaten te beperken. We vonden het handig om de Process Name te beperken tot het programma waar het om ging. RustDesk verschijnt daar in twee varianten: onder de originele naam met een lange versie-aanduiding en gewoon als rustdesk.exe. Die laatste naam is het meest nuttig. Als verdere filtercriteria gebruiken we Operation en de functie QueryDirectory en kijken we alleen naar mislukte oproepen (Result is not SUCCESS).

Met de bovenstaande criteria kun je heel snel DLL-bestanden vinden die door een programma worden gebruikt en die het nodig heeft maar niet vindt, maar die het zelf niet specifiek benoemt in een foutmelding – in het geval van RustDesk is dat het bestand sas.dll. Als je die DLL in de map naast de al genoemde DLL's zet waarin RustDesk staat, dan start de software op in het rescuesysteem en kan het op een rudimentaire manier getest worden – om er zeker van te zijn dat er geen andere bestanden ontbreken).

Dan zou je die DLL's gewoon als bestand als bijlage in het script kunnen opnemen, maar dat is om meerdere redenen niet slim. Ten eerste is dat een licentieschending: je mag bestanden uit Windows niet zomaar inbouwen – als je het bouw pakket aan anderen beschikbaar wilt stellen tenminste. Aan de andere kant moet je er dan zelf voor zorgen dat de bestanden uit een Windows-versie komen die overeenkomt met het rescuesysteem dat je gebouwd hebt.

INPAKKEN MAAR

Het installeren van RustDesk via een script is iets ingewikkelder. Uitgaande van een gegenereerd script met

de template Simple Download App, kun je het beste het script openen in een editor zoals Visual Studio, en regel voor regel doorlopen. Alle plaatsen waar je wijzigingen moet aanbrengen, zijn gemarkeerd met het commentaar `// TODO`, zoals de naam van de map die het bouw pakket moet aanmaken voor het programma.

Je zult dan snel op een gemeenschappelijk kenmerk van veel scripts stuiten: ze behandelen 32-bit en 64-bit programmaversies afzonderlijk (de TODO's vereisen bestandsnamen en download-url's voor de betreffende versie). Dat heeft vaak historische redenen. In principe zou het voldoende zijn om de 32-bit versie van een programma op te nemen in het rescuesysteem omdat het ook zal werken in een 64-bit versie van het systeem (in tegenstelling tot een reguliere PE). De 64-bit versie integreert namelijk Windows-32-On-Windows-64 (WOW64) in het rescuesysteem.

Voor het huidige bouw pakket hebben we echter besloten om alleen 64-bit versies te ondersteunen. Het hieronder beschreven RustDesk-script downloadt daarom alleen de 64-bit programmaversie en houdt geen rekening met eventuele 32-bit eigenaardigheden. Met één uitzondering: het voegt altijd de DLL's toe die nodig zouden zijn voor 32-bit programma's – niet van elk programma in het systeem is er immers ook een 64-bit versie. Zonder die truc zouden 32-bit programmaonderdelen het niet doen als ze de 32-bit DLL's niet kunnen vinden.

Regels om de door RustDesk gemiste DLL's te integreren in het rescuesysteem zijn niet opgenomen in het gegenereerde script. Voeg de gewenste regels toe bij de sectie `[Process]` tussen de commentaren `Extract` en `Settings` (zie het kader). Die zorgen ervoor dat de genoemde DLL's uit de gebruikte Windows-bron worden gehaald en tijdens het bouwen in het project geïntegreerd worden.

Met de aanroepen van `RequireFileEx,AppendList` voeg je een lijst toe om te bewerken, de laatste aanroep met `ExtractList` als tweede parameter voltooit de installatie. Op die manier halen veel scripts de originele Windows-bestanden in het rescuesysteem tijdens het bouwen. De commando's worden gedefinieerd als macro's in het project en roepen op de achtergrond functies aan die WIM-bestanden verwerken.

Om het script er mooi uit te laten zien, kun je een logo toevoegen dat bij het programma past. We hebben er een genomen uit de GitHub-repository. Om het toe te voegen, klik je op het potloodpictogram aan de rechterkant van de kop tekst van het script en ga je naar de functie Edit Script Properties. In het onderste gedeelte van het venster dat dan opent, kun je een bestand selecteren om in het script op te nemen.

De regels van het scriptbestand, die we hier niet volledig weergeven, hebben betrekking op het maken van een configuratiebestand dat RustDesk de weg wijst naar een eigen server. Je kunt de gegevens daarvan invoeren in PEBakery. Voor het integreren van RustDesk zijn verder geen andere handelingen

nodig die typisch zijn voor een script, zoals het aanmaken en instellen van sleutels in het register van het rescuesysteem.

Als je een scriptbestand wilt testen, moet je dat eerst doen in een buildmap die al de bestanden van een succesvolle run bevat. Dat zorgt ervoor dat een script in de context correct werkt. Zodra je dat gecontroleerd hebt, moet de tweede stap een test met een nieuwe buildmap zijn – dat zal ervoor zorgen dat je script ook op andere computers werkt.

SPEURWERK

Afgezien van de technische aspecten bestaat de kunst van het integreren van eigen scripts in het bouw pakket voornamelijk uit spuurwerk. In hardnekkige gevallen helpt Procmon van de Sysinternals tools. Laat Procmon het betreffende programma observeren in het rescuesysteem.

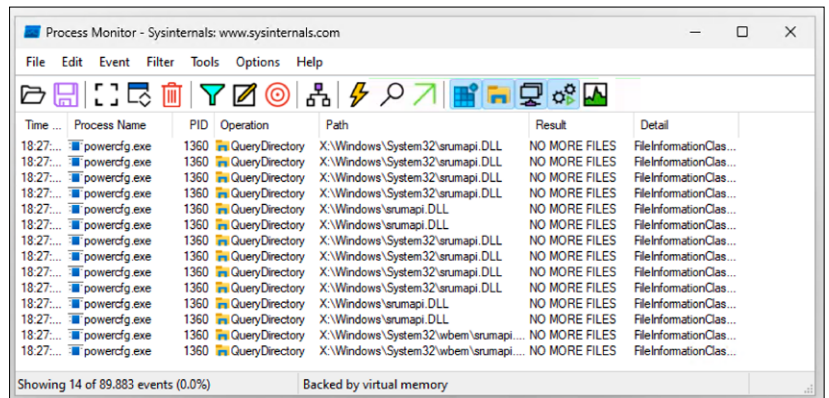
Kijk eerst naar mislukte operaties. Die mislukkingen geven vaak informatie over andere ontbrekende DLL's en registersleutels die mogelijk moeten worden toegevoegd. Het gaat hier niet om volledigheid, maar vooral om het stap voor stap identificeren van de onderdelen die echt nodig zijn.

De laatste stap naar een perfect script is dan het toepassen van de opgedane kennis. Je moet manieren vinden om uit de download van een installatiepakket de juiste bestanden te halen. De verschillende scripts in PhoenixPE en rescue-Windows gebruiken een hele reeks speciale programma's om dat te doen voor wanneer tools als 7-Zip falen. Voor sommige wordt PhoenixPE zelfs geleverd met gespecialiseerde macro's.

Houd bij dat alles de licentie in de gaten van de software die je installeert in het rescuesysteem. Gratis software, die onbeperkt mag worden verspreid, kan als bestandsbijlage aan een script worden toegevoegd – net als andere binaire en configuratiebestanden. Dat maakt het echter moeilijk voor gebruikers om programmaversies bij te werken en heeft daarom alleen zin voor tijdloze software.

Een opmerking over het integreren van nieuwe programma's in de menustructuur van c't-rescue-Windows: de scripts die je met PEBakery maakt gebruiken daar PhoenixPE's eigen methodes voor. We gebruiken een eigen aanpak om de menu's van het rescuesysteem overzichtelijker te maken. Het bestand `pecmd_links.ini`, dat je kunt vinden in de Custom-map in de buildmap in het ziparchief van het project, beschrijft de menuopties. Voeg je scripts toe analoog aan de bestaande vermeldingen.

De menuopties maken deel uit van de configuratie voor `pecmd.exe`, dat aan het begin genoemd is. Het programma start de gebruikersinterface van het rescuesysteem. Het volledige configuratiebestand bevat de vermeldingen uit `pecmd_links.ini` en `pecmd_pins.ini` (voor programma's die aan het startmenu zijn vastgemaakt, ook uit de aangepaste map) in combinatie met vermeldingen die tijdens het bouwen gegenereerd zijn. Zo is `pecmd.ini` het juiste adres voor het automatisch uitvoeren van programma's



Filters bij Process Monitor helpen om de relevante gegevens te isoleren, zoals mislukte pogingen van `powercfg /batteryreport` om andere DLL's te laden.

wanneer het rescuesysteem gestart wordt – een regel met `EXEC=` is voldoende.

Er zijn verschillende manieren om `pecmd.ini` te bewerken. De makkelijkste manier is om het te selecteren in de projectboom in PEBakery aan de linkerkant onder 'Shell \ PECMD' en dan een door de gebruiker gedefinieerd bestand toe te voegen. De knop Sample Config geeft daar een voorbeeld van. Je moet daar echter niet te veel aandacht aan besteden, want PhoenixPE-ontwikkelaar Jonathan Holmgren reorganiseert momenteel dat deel en wil af van `pecmd.exe`, dat als closed-source ontwikkeld is.

Als je het toekomstige register van het rescuesysteem wilt bewerken, is er iets belangrijks om in gedachten te houden: het bouw pakket integreert tijdelijk delen daarvan in het register van het buildsysteem. Het is belangrijk om de juiste branch aan te spreken – oftewel de subbranch die voor dat doel opgenomen is. En: in tegenstelling tot bijvoorbeeld een draaiende Windows is niet `CurrentControlSet` vereist, maar `ControlSet001`. Dat kan bijvoorbeeld handig zijn om het zoekpad (PATH) in het rescuesysteem uit te breiden voor programma's die je hebt toegevoegd.

HARDE NOTEN

Nog een tip over de 'taal' van de scripts die Winbuilder geïntroduceerd heeft: dat is even wennen. Er ontbreken bijvoorbeeld functies die bij andere scripttalen vanzelfsprekend zijn, zoals het regel-voor-regel lezen van tekstbestanden. De scripts in het bouw pakket bevatten daar creatieve oplossingen voor en in geval van twijfel kun je externe scripts gebruiken zoals batchbestanden, PowerShell en andere tools. Je kunt een taalreferentie vinden op GitHub in de PEBakery-repository's.

Een laatste aanbeveling: pak het langzaam aan. Portable software is eenvoudig te integreren, maar complexere applicaties die met stuurprogramma's of eigen services komen of daarop gebaseerd zijn, zijn moeilijk over te zetten naar de PE-wereld – dat werkt niet altijd. Maar het is natuurlijk altijd leuk om het te proberen!

Literatuur

[1] Axel Vahldiek en Daniel Dupré, 32-bit programma's in 64-bit Windows, c't 1-2/2020, p.98



www.ct.nl/ctrescuewin





INVOEGONTOEPASSINGEN

De technische verwarring rond Outlook-add-ins

Plotseling lijkt het pictogram van een Office-add-in verdwenen en in de nieuwe Outlook verschijnt hij al helemaal niet. Met het ene mailaccount werkt hij wel, met het andere niet. Er zijn al met al veel problemen met Outlook-add-ins. We onderzoeken de oorzaken en laten zien hoe je jezelf kunt helpen.

Stefan Wischner en Daniel Dupré



Al vele jaren zijn er installeerbare add-ins – of invoegtoepassingen zoals Microsoft ze ook wel noemt – waarmee je de functies van Outlook en andere Office-programma's kunt uitbreiden. Ze koppelen externe services en verbeteren workflows. De laatste tijd verdwijnen sommige echter opeens uit de menubalken of verschijnen nog maar sporadisch.

De reden daarvoor is dat Microsoft een oude maar bewezen technologie heeft stopgezet en vervangen door een nieuwe, of om preciezer te zijn: heeft aangevuld. Voorheen ondersteunden Office-programma's

extensies van beide typen. De nieuwe maakt gebruik van webtechnologie en biedt vooral een aantal voordelen voor ontwikkelaars. Voor veel gebruikers levert het echter problemen op. We onderzoeken de verwarring rondom COM-, VSTO- en web-add-ins en helpen je om add-ins te vinden die plotseling verdwenen zijn. We concentreren ons op het mailprogramma Outlook, dat in het bijzonder is getroffen, maar de problemen en oplossingen zijn voor alle Office-programma's grotendeels hetzelfde.

COM/VSTO-ADD-INS: OUDE MODELLEN

Veel add-ins voor Microsoft Office, zowel de add-ins die door softwarefabrikanten worden geleverd als de add-ins die gebruikers zelf hebben geprogrammeerd, zijn gebaseerd op de meer dan dertig jaar oude COM-architectuur. De afkorting staat voor Component Object Model en is een standaard voor communicatie tussen toepassingen. COM-add-ins kunnen worden ontwikkeld in verschillende programmeertalen, waaronder C, C++, Java en VBS (Visual Basic Script).

De opvolger van COM-add-ins wordt VSTO-add-ins genoemd, naar de gelijknamige Visual Studio-bibliotheek (Visual Studio Tools for Office), waarmee vanaf versie 2003 add-ins voor Office kunnen worden ontwikkeld met Visual Studio en .NET. Vanuit het oogpunt van de gebruiker maakt het geen verschil of een add-in op COM- of VSTO-basis is ontwikkeld – het installeren, integreren en beheren in de Office-programma's is voor beide typen identiek.

Omwille van de eenvoud wordt in dit artikel voor beide typen alleen de term COM-add-in gebruikt – dat is ook wat de relevante dialoogvensters in de Office-programma's doen.

COM-add-ins draaien alleen onder Windows, je installeert ze als aparte programma's en ze worden door de Office-programma's benaderd via DLL's, die met de add-in op het systeem worden geïnstalleerd. Het voordeel daarvan is dat DLL's erg krachtig kunnen zijn. Ze hebben ook toegang tot veel Office- en systeemfuncties en zijn daarom geschikt voor verschillende doeleinden. Dat heeft echter ook een nadeel: door hun vaak verregaande lokale rechten vormen COM-add-ins een beveiligingsrisico.

WEB-ADD-INS: ALLEEN MET EEN MICROSOFT-ACCOUNT

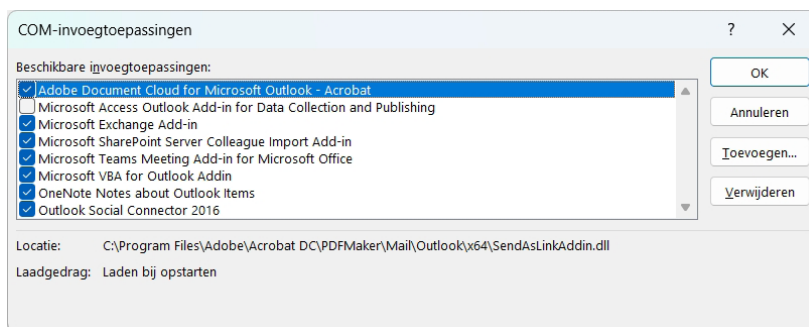
Enige tijd geleden is Microsoft gestopt met het ontwikkelen en onderhouden van COM- en VSTO-add-ins en heeft die vervangen door een nieuw type add-in gebaseerd op webtechnologieën zoals HTML, CSS en JavaScript. In zijn communicatie maakt Microsoft geen onderscheid meer tussen de twee typen, maar verwijst het altijd naar web-add-ins als het gaat over Outlook-apps, Outlook-add-ins of Office-add-ins. De 'nieuwe Outlook' die Microsoft de laatste tijd agressief promoot, kan helemaal niets met COM- en VSTO-add-ins en ondersteunt uitsluitend web-add-ins. Volgens Microsoft zal dat ook niet veranderen omdat het technisch niet mogelijk is.

Bestaande COM- en VSTO-add-ins kunnen echter wel parallel worden gebruikt in de klassieke Outlook voor Windows. Maar omdat ze apart worden geïnstalleerd en beheerd, veroorzaakt dat ook weer onnodige verwarring. Daarover zo dadelijk meer.

Het voordeel van de nieuwere web-add-ins, afgezien van de betere beveiliging, is dat ze platformafhankelijk zijn. Ze draaien in Outlook onder Windows (klassiek en nieuw), macOS en op outlook.com in een browser, zonder dat er voor elk platform een aparte versie hoeft te worden ontwikkeld.

Er zijn echter ook enkele nadelen en beperkingen ten opzichte van de klassieke COM-add-ins. Web-add-ins vergen in het algemeen bijvoorbeeld een actieve internetverbinding. Ook hebben ze geen toegang tot veel Office-programmafuncties en lokale gegevens. Je moet er bovendien rekening mee houden dat inhoud – bij Outlook bijvoorbeeld e-mails – wordt verzonden naar de servers van de add-in-provider. Dat is echter vaak het doel van de add-in, bijvoorbeeld als je berichten wilt doorsturen naar een online notitie- of projectplanningsprogramma en dus naar de cloudopslag van de betreffende aanbieder.

Het grootste probleem met web-add-ins voor Outlook is dat ze alleen werken in combinatie met een Exchange-server die geschikt is voor het web. Dat betekent meestal een mailaccount dat bij een Microsoft 365 Business-abonnement (Exchange Online) of een Microsoft-account (outlook.com, Windows Live, Hotmail, Xbox) hoort. Als je bij Outlook meerdere accounts ingesteld hebt, zijn de web-add-ins alleen beschikbaar als je een map van een Microsoft-account opent, bijvoorbeeld het Postvak IN. Zodra je overschakelt naar een ander account (IMAP, POP3), verdwijnen de pictogrammen en kun je de add-ins niet gebruiken.



Je kunt de afzonderlijke extensies in- en uitschakelen bij de opties voor COM-add-ins.

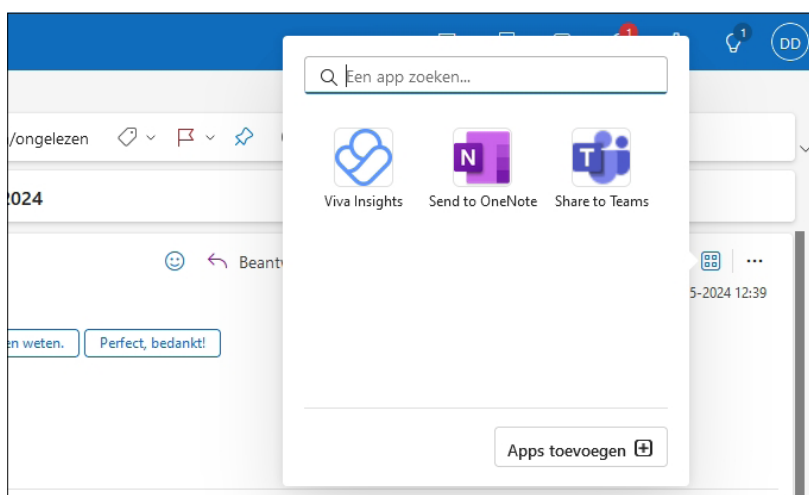
Er is geen manier om een web-add-in te laten werken met een niet-Microsoft-account. Nog meer verwarring wordt veroorzaakt door het feit dat veel – maar lang niet alle – externe leveranciers van add-ins, bijvoorbeeld voor ToDoist en Evernote, zijn overgestapt van COM-add-ins naar webadd-ins en die overstap vaak automatisch maken als onderdeel van een update voor hun programma.

WAAR IS MIJN ADD-IN?

Een van de meest voorkomende problemen met Office-add-ins is dat ze niet zichtbaar zijn, bijvoorbeeld dat ze niet verschijnen op de Outlook-werkbalk. Dat kan verschillende oorzaken hebben, afhankelijk van of de ontbrekende add-in een COM- of web-add-in is.

Als je dat niet weet, ga er dan eerst van uit dat het een COM-add-in is en open het bijbehorende beheerdialoogvenster. Klik daarvoor op 'Bestand / Opties / Invoegtoepassingen'. Er wordt een lijst geopend met alle geïnstalleerde COM-add-ins, gegroepeerd volgens actieve, inactieve en uitgeschakelde add-ins. Inactieve add-ins worden normaal gesproken door de gebruiker gedeactiveerd, terwijl uitgeschakelde add-ins door het systeem automatisch zijn gedeactiveerd omdat ze het opstarten van Outlook ernstig vertragen of het programma al eens hebben laten vastlopen. Als de ontbrekende add-in in een van de laatste categorieën valt, dan heb je de oorzaak van het probleem al gevonden.

Je kunt beide soorten gedeactiveerde add-ins weer activeren door onder de lijst op 'Start...' te klik-



In zowel de nieuwe Outlook als de browserversie van Outlook (afbeelding) heb je toegang tot add-ins via een onopvallend pictogram in de maileditor.

ken achter 'Beheren: COM-invoegtoepassingen', en de relevante vakjes in het volgende dialoogvenster aan te vinken. Als je het starten van add-ins die het Office-programma automatisch had gedeactiveerd in de toekomst wilt forceren, doe je dat bij 'Bestand / Invoegtoepassingen beheren'. In het bijbehorende dialoogvenster vind je de add-ins die het programma als problematisch beschouwt, samen met informatie over de reden en de huidige status. Elk item heeft een menu Opties waarmee je de betreffende add-in een week of een maand lang kunt uitsluiten van bewaking of onvoorwaardelijk kunt activeren.

Als de gezochte add-in niet op een van die lijsten voorkomt, zijn er twee mogelijkheden. Hij kan helemaal niet geïnstalleerd zijn, wat je dan eerst nog moet doen. Of je dat via een installatieprogramma moet doen of een nieuwe installatie, hangt af van de betreffende aanbieder.

GOED VERBORGEN WEB-ADD-INS

Het is echter ook goed mogelijk dat de ontbrekende add-in een web-add-in is en daarom helemaal niet via het COM-invoegtoepassing-beheer beheerd kan worden. Aan het pictogram van een add-in op de menubalk van Outlook kun je niet aflezen of het om een COM- of web-add-in gaat. Een indicatie voor web-add-ins is echter dat je ze meestal via de zijbalk van Outlook vindt, waar je dialoogvensters en instelingsopties opent. COM-add-ins communiceren daarentegen via dialoogvensters die typisch zijn voor het besturingssysteem.

Als je de nieuwe Outlook of de browserversie gebruikt, kom je mogelijk een bijzonderheid tegen in de gebruikersinterface: in tegenstelling tot de klassieke Outlook tonen beide geen invoegknoppen op de menubalk van de hoofdweergave. Alleen wanneer je

een bericht opent of een nieuw bericht maakt, zie je de geïnstalleerde add-ins. Voor nieuwe berichten verschijnen de add-in-pictogrammen op de werkbalk van een apart bewerkingsvenster.

Bij geopende mails zitten de knoppen soms in de rechterbovenhoek of achter het menu met drie puntjes. Aangezien de browserversie van Outlook en de nieuwe Outlook-applicatie voortdurend worden gewijzigd en verder ontwikkeld, kan de integratie van de extensies in de interface op elk moment veranderen.

Als je niet zeker weet of en welke web-add-ins überhaupt geïnstalleerd zijn, geven de verschillende Outlook-versies op verschillende manieren informatie. In de klassieke Outlook open je eerst een map die hoort bij een Exchange Online/Microsoft e-mail-account. Er verschijnt dan een knop met de tekst 'Alle apps' in het menu Start. Als je daarop klikt, wordt een webvenster geopend met de Microsoft add-in store (AppSource) al gefilterd op Outlook-extensies. Daar kun je zoeken naar add-ins en ze meteen installeren. Als je in het linkermenu op 'Mijn invoegtoepassingen' klikt, schakelt de weergave over naar de web-extensies die al geïnstalleerd zijn.

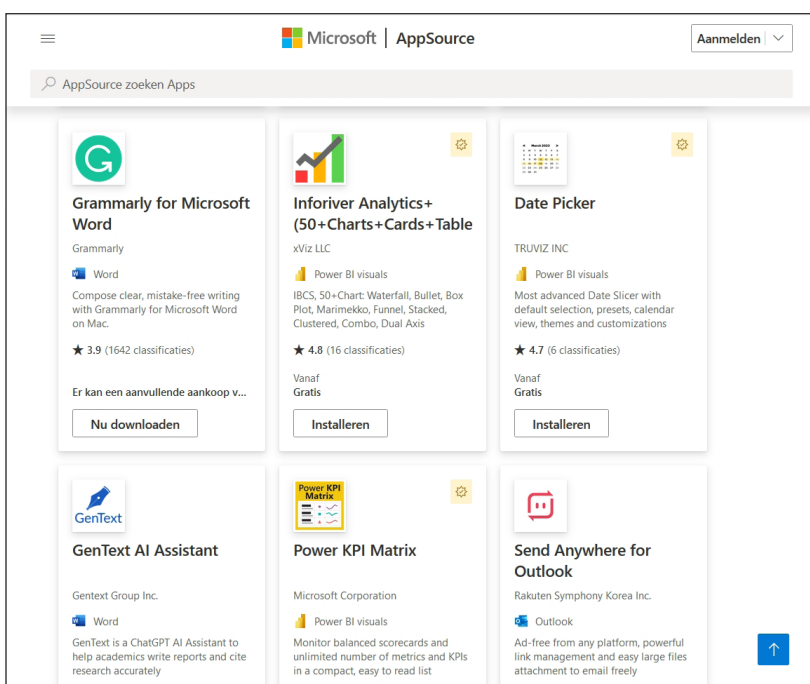
In de nieuwe Outlook is de weg naar het AppSource-venster niet veel ingewikkelder, bovendien is de manier waarop het werkt ongeveer gelijk aan de webversie van Outlook. Je moet eerst een Microsoft-mailaccount selecteren en vervolgens op een bericht klikken. Klik naast het menu met de drie puntjes in de rechterbovenhoek van het bericht op het pictogram links ervan. Het ziet er ongeveer uit als de vier op een dobbelsteen en er opent een pop-upvenster dat direct de geïnstalleerde web-add-ins opsomt. Daarnaast is er ook knop 'Invoegtoepassingen openen' waarmee je naar de AppSource-winkel wordt geleid.

DE NIEUWE OUTLOOK

Als de nieuwe Outlook, zoals Microsoft aanvankelijk communiceerde, alleen de mail-, agenda- en contactpersonen-apps van Windows 10 en 11 zou vervangen, zou het gebrek aan ondersteuning voor COM-add-ins niet zo erg zijn – die ondersteunen immers helemaal geen extensies.

Microsoft laat echter steeds vaker doorschemeren dat de nieuwe Outlook op een gegeven moment ook de klassieke client zal vervangen, waardoor ook bestaande COM-add-ins onbruikbaar zouden worden. Of dat echt gaat gebeuren valt nog te bezien. Microsoft heeft in het verleden al vaker laten zien dat het ook terug kan krabbelen als het teveel tegenwind krijgt, zoals dat bijvoorbeeld is gebeurd met Windows-tiles en het UWP-OneNote (Universal Windows Platform). Die laatste verving de klassieke OneNote korte tijd helemaal in de Office-suite, om er vervolgens weer plaats voor in te ruimen.

De overlevingskansen voor een mailclient die niet alleen zeer twijfelachtig is op het gebied van beveiliging, maar ook bestaande extensies onbruikbaar maakt en het gebruik van add-ins beperkt tot Microsoft-accounts, zijn voor veel zakelijke klanten waarschijnlijk vrij klein.



Je kunt nieuwe add-ins zoeken en installeren in Microsofts AppSource-store. Daar vind je ook de extensies die al geïnstalleerd zijn in Outlook.

SUPERMICRO

MULTI-NODE

Building Blocks



Construct Your Optimized IT Solutions with Our Twin Family of Multi-Node Servers
Featuring 3rd Gen Intel® Xeon® Scalable Processors

SMBE Belgium

+32 495 533 245
www.smbe.be
sales@smbe.be

TWP Computer

+31 20 638 9057
www.twp.nl
info@twp.nl

Server Storage Solution

+32 9 261 5310
www.s3s.be
sales@s3s.be

NCS International

+31 544 47 0000
www.ncs.nl
info@ncs.nl

ServerDirect BV

+31(0) 85-3018585
www.ServerDirect.nl
sales@serverdirect.nl



Learn More at www.supermicro.com

© Supermicro and Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries.



USB-C-PC'S

Mini-pc's voeden via USB-C

Bij laptops is het al langer gangbaar, maar er zijn nog maar erg weinig mini-pc's die via USB-C gevoed kunnen worden. Ontdek niet alleen waarom dat zo is, maar ook hoe je dat toch voor elkaar kunt krijgen.

Christof Windeck en Marco den Teuling

USB-C-voedingen met USB Power Delivery (USB-PD) zijn praktisch, veelzijdig en duurzaam. In plaats van voor elk apparaat een aparte voeding te moeten gebruiken, past één enkele op meerdere apparaten. Dat is beter voor het milieu en je zenuwen, bespaart ruimte in je bagage en biedt praktische aansluitmogelijkheden. Veel laptops kunnen via een monitor of dock met één USB-C-kabel worden aangesloten op alle randapparatuur, ethernet en voeding. Dat vermindert de kabelwarboel op het bureau.

Sommige mensen willen die flexibiliteit van USB-C ook voor hun mini-pc. Een enkele kabel zou praktisch zijn voor stationair gebruik. Met een krachtige powerbank of een USB-C-adapter voor 12 volt zou de mini-pc klaar zijn voor gebruik in de auto, camper, boot of tuinhuisje. Helaas weigeren de meeste mini-pc's de nieuwe wereld van USB-C te omarmen. We leggen de redenen daarvoor uit, maar proberen ook adapters uit om ze toch aan te sluiten op USB-C-stroombronnen.

KOSTEN EN ENERGIEVERBRUIK

Afgezien van onwil of fantasieloosheid bij fabrikanten zijn er drie belangrijke redenen waarom de meeste mini-pc's een speciale voeding hebben: kosten, energieverbruik en compatibiliteitsproblemen.

Bij USB-PD onderhandelen de source (oftewel de voeding of powerbank) en de sink (hier de mini-pc) met elkaar over welk voltage mag worden toegepast en hoeveel stroom er mag lopen. De gebruikte USB-C-kabel speelt daarbij ook een rol. USB-PD specificeert namelijk spanningsniveaus tussen 5 en 20 volt en alleen kabels met een piepkleine chip in de stekker (e-marker) mogen met meer dan 3 ampère (A) werken, namelijk 5 A. De stekkers kunnen niet meer verdragen.

Wanneer een apparaat wordt aangesloten op een USB-PD-voeding, vindt er een relatief complex communicatieproces plaats tussen de controllerchips aan beide zijden. Als de USB-C-connector niet alleen stroom moet krijgen, maar tegelijkertijd ook data- en videosignalen moet leveren, moeten de fabrikanten multiplexer-chips installeren en de firmware daarop afstemmen. Een USB-C-aansluiting met voeding die ook data- en videosignalen levert, verhoogt de kosten voor ontwikkeling en productie dan ook.

USB-C brengt ook risico's met zich mee op het gebied van compatibiliteit, waardoor de kosten voor ondersteuning en garantie toenemen. Met een te zwakke USB-C-voeding of de verkeerde USB-C-kabel



USB-C biedt verschillende mogelijkheden voor de stroomvoorziening. Hier hangt een mobiele monitor aan een powerbank, die op zijn beurt weer een mini-pc voedt. Op de eerste pagina zijn mini-pc en monitor verwisseld.



USB-C-voeding werkt ook via een USB-C-dock. In het hier getoonde voorbeeld levert dat extra kabels op omdat de monitor dan zijn beeldsignalen moet krijgen via HDMI en zijn voeding krijgt via een andere usb-kabel.

zal de mini-pc onstabiel of helemaal niet werken, waardoor veel kopers de supportafdeling bellen. En als een inferieure voeding schade veroorzaakt, dreigt er een geschil.

Een groot probleem is de voeding. Dat komt doordat moderne x86-processors in de turbomodus veel energie verbruiken. Zelfs veel 28-watt mobiele processoren kunnen kortstondig meer dan 110 watt aan. Een USB-PD-voeding van 100 watt is dan niet genoeg. Die voedingen zijn ook niet ontworpen voor snelle, sterke pulsen. Die komen bij moderne processoren met een turbomodus echter vaak voor.

Het is ook moeilijk om de energiebehoefte van andere pc-onderdelen zoals RAM, ssd, harde schijven en zelfs grafische kaarten in te schatten. Flexibel uitbreidbare mini-pc's met meerdere RAM- en ssd-slots worden daarom geleverd met redelijk krachtige voedingen. Veel NUC's met een Core i-processor hebben er een van 120 watt. Dat is meer dan wat USB-PD zonder de relatief nieuwe Extended Power Range (EPR) uitbreiding aankan. Mini-pc's voor desktopprocessors, zoals de Asrock DeskMini-serie, hebben zelfs nog meer vermogen nodig. Vaak hebben die een voeding van 180 watt nodig.

Bij laptops ligt dat anders. Daar kan de accu de stroompieken mee opvangen naast de voeding of beperkt de fabrikant het piekvermogen van de cpu omdat hij het hele systeem zelf heeft samengesteld. Voor fabrikanten van mini-pc's is het makkelijker om hun eigen voedingseenheid te leveren die is afgestemd op de prestatieklasse van de computer.

Goedkope processors zoals Intels Celeron N, Pentium Silver en N100 (Alder Lake-N) series zijn in het algemeen goed geschikt voor USB-C-voeding. Dat komt omdat ze gespecificeerd zijn met een Thermal Design Power (TDP) van slechts 6 tot 15 watt en hun turbomodus minder dan 30 watt vereist. Ze bieden ook maximaal twee geheugenslots en hebben maar een paar PCIe- en SATA-poorten. Dat betekent dat er geen extra energievreters in de pc zitten. Of om het anders te zeggen: als je een USB-C-voeding hebt, beperkt dat indirect de rekenkracht omdat de eerder genoemde goedkope processors aanzienlijk langza-

mer zijn dan krachtigere mobiele processoren en de meeste desktop-cpu's.

USB-C MINI'S

De MeLE Quieter 4C met Intel N100 (zie elders in deze c't) is een van de weinige pc's die standaard via USB-C gevoed kan worden. Asus ontwerpt ook veel versies van de ExpertCenter mini-pc-serie voor USB-C-voeding, maar vereist een 100W-voeding voor de krachtigere systemen. Dat beperkt de keuze van geschikte monitoren met USB Power Delivery. Veel monitoren kunnen via USB-C slechts 65 watt leveren, of in elk geval minder dan 100 watt, dus let daarop als je er een krachtigere mini-pc mee wilt voeden.

De grote pc-merken Dell en HP hadden enkele mini-pc's en thin-clients met USB-C-voeding in hun programma, maar dat sloeg blijkbaar niet aan – ze worden niet meer gemaakt. Dell had in 2021 de Optiplex 7090 UFF. Die was ontworpen om te worden gemonteerd in de voet van speciaal ontworpen Dell-monitoren en daarop te worden aangesloten via USB-C. In 2016 introduceerde HP al de Elite Slice business-mini met een modulair uitbreidingsconcept en USB-C-voeding, waarvan nog een tweede generatie verscheen voordat die werd stopgezet. Vanaf 2018 verkocht HP de t430 thin-client met optionele USB-C-voeding.

VREEMDE COMBINATIES

USB-C-voedingen leveren spanningen tussen 5 en 20 volt en stromen tot 5 ampère, maar niet alle combinaties daarvan. Een actueel voorbeeld is de Raspberry Pi 5: die vereist de ongebruikelijke combinatie van 5 volt en 5 ampère, die maar door heel weinig USB-C-voedingen geleverd wordt. Sommige mini-pc's vereisen meer dan 5 ampère bij 12 volt, wat simpelweg niet binnen de USB-C-specificaties valt. En niet alle USB-C-voedingen met een totale output van minder dan 60 watt gaan tot 20 volt, aangezien de combinatie van 15 volt en 3 ampère al voldoende is voor 45 watt. Veel mini-pc's zijn echter ontworpen voor 19 volt en zullen niet starten met 15 volt – zelfs als ze het met 45 watt zouden redden. Je hebt dan



Via adapterkabels met een PD-controllerchip kun je van een USB-C-voeding een spanning krijgen tussen 5 en 20 volt. Met verloopstekkers kun je dan allerlei apparaten voeden, maar dat is niet zonder risico.

een krachtigere en duurdere USB-C-voeding nodig die 20 volt kan leveren.

Veel pc-kopers zijn zich niet bewust van die details en daarom bestaat er een risico op vervelende incompatibiliteiten. Dat zou technisch opgelost kunnen worden door pc-fabrikanten de spanningsovmvormers van hun computers te laten herontwerpen voor USB-C-voeding. Dat zou voor die fabrikanten echter alleen de moeite waard zijn als ze dan de voedingseenheid zouden kunnen weglaten om kosten te besparen, maar dat zal leiden tot klachten van klanten. De meesten gaan er namelijk van uit dat ze het apparaat inclusief voeding ontvangen en er geen extra aanschaf nodig is.

Als je een mini-pc wilt voeden via USB-C, moet je de stroom- en spanningsspecificaties van beide apparaten nauwkeurig vergelijken. Dat is niet eenvoudig omdat veel USB-C-voedingen en powerbanks niet bij hun specificaties vermelden welke combinaties ze aankunnen. Je hebt ook een kabel met een e-marker nodig, zodat er meer dan 3 ampère doorheen kan. Dat soort kabels wordt vaak aangeprezen als 100watt-capabel. Let op: sommige lange kabels hebben een hoge inwendige weerstand, waardoor verliezen optreden [1].

SPANNINGSADAPTER

Sommige mini-pc's zonder eigen PD-functie die maximaal 100 watt nodig hebben, kunnen toch gevoed worden via een USB-C-voedingsbron, namelijk met behulp van een adapter. Die zijn verkrijgbaar met een geïntegreerde PD-controllerchip en verwisselbare stekkers aan de pc-zijde. Dat zijn vaak holle stekkers met een diameter van 5,5 millimeter voor de buitenste contactring voor aarde en 2,5 millimeter voor de positieve pool aan de binnenkant. Sommige adapterkabels worden geleverd met 10 of meer verwisselbare pluggen. Dat betekent dat veel andere apparaten ook via USB-C gevoed kunnen worden, bijvoorbeeld laptops zonder USB-C-aansluiting of effectapparaten voor muzikanten.

Dergelijke adapterkabels hebben vaak een kleine behuizing met een display en knop. Daarmee wordt ingesteld welk voltage de PD-chip moet aanvragen bij de USB-C-voedingseenheid. De adapters verande-

ren dus een USB-C-voeding of een powerbank in een regelbare spanningsbron.

Dat brengt risico's met zich mee: als het voltage te hoog wordt ingesteld, bestaat het risico dat de mini-pc beschadigd raakt. Bij een apparaat dat is ontworpen voor 12 volt, kan de ingangconverter doorbranden bij 20 volt. En het is denkbaar dat mini-pc's een andere polariteit nodig hebben dan de positieve pool op het interne contact. Dergelijke adapters leggen de verantwoordelijkheid dus bij de gebruiker. Het is ook belangrijk om de knop voor de spanningskeuze te beschermen tegen onbedoelde wijzigingen.

In theorie leveren USB-C-spanningsbronnen met de functie Programmable Power Supply (PPS) elke spanning tussen 5 en 20 volt in stappen van 0,1 volt. Bij twee adapters die we als voorbeeld bij Amazon hebben gekocht, konden we echter alleen 5, 9, 12, 15 of 20 volt selecteren. Ze hebben beide slechts een eenvoudige knop waarmee die niveaus stap voor stap kunnen worden doorlopen.

Veel mini-pc's (en laptops) worden geleverd met voedingen voor 19 volt. De meeste zouden zonder problemen 20 volt aan moeten kunnen, omdat dat slechts 5,2% meer is. Daar is echter geen garantie voor, dat is op eigen risico. We hebben de twee USB-C-adapters getest op vier mini-pc's. Zoals verwacht: hoe minder energie een computer verbruikt onder volledige belasting, des te beter dat werkt. Een Intel NUC11 met een Core i-processor van de elfde generatie liep vast in het BIOS. De drie andere mini-pc's met Celeron J3455 (Intel NUC-6CAYH), Celeron J4105 (Gigabyte Brix) en Intel N100 (Zotac Zbox Edge CI343) werkten daarentegen zonder problemen. Dat werkte zowel met een USB-C-voeding van 100 watt als met een 65-watt powerbank.

De werktijd op een powerbank is afhankelijk van de capaciteit ervan en het energieverbruik van de mini-pc. De mini-pc's met Celeron N, Celeron J of N100 verbruiken in ruststand tussen de 4 en 8 watt, dat wil zeggen minstens 4 tot 8 wattuur (Wh) per uur, plus het verbruik onder belasting. Een powerbank met 10.000 mAh levert idealiter 30 tot 35 wattuur, wat betekent dat 3 tot maximaal 8 uur werken mogelijk is.

CONCLUSIE

Er zijn maar weinig (mini-)pc's die standaard ontworpen zijn voor USB-C-voeding. Daarmee kunnen ze flexibel worden gevoed via een bestaande netadapter, via een powerbank of via een USB-C-monitor of -dock. Maar die aansluitmogelijkheid is blijkbaar slechts interessant voor een paar kopers en heeft te veel nadelen voor fabrikanten, want veel mini's met USB-C-voeding zijn al van de markt verdwenen. Met wat achtergrondkennis en een adapter kun je sommige bijzonder zuinige mini-pc's echter laten werken met een USB-C-voedingsbron – ook al zijn ze daar niet voor ontworpen.



Literatuur

[1] Rudolf Opitz en Marco den Teuling, USB-C kabels voor snel opladen en snelle data-overdracht, c't 12/2022, p.70



SANS

Hands-On Workshops

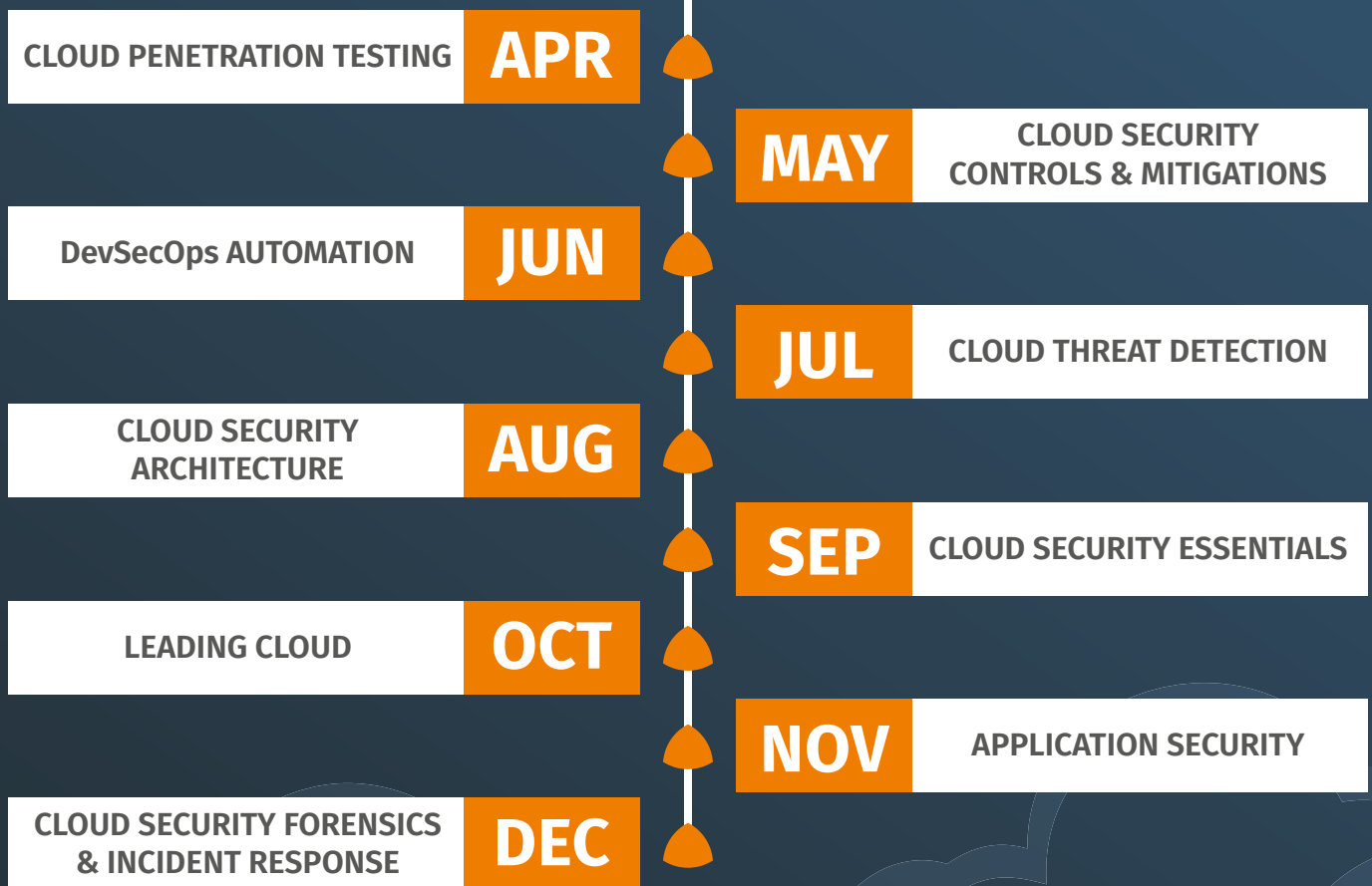
AVIATA CLOUD SOLO FLIGHT CHALLENGE

Around the World 2x

Embark on an exhilarating journey through cloud security with the Aviata Cloud Solo Flight Challenge! This FREE workshop series, built and taught by esteemed SANS faculty, is your ticket to mastering cloud security through hands-on, engaging sessions. Each monthly workshop follows the same storyline and ties directly to a specific cloud security topic, ensuring you learn the most relevant and advanced techniques in a cohesive manner. While they compliment each other, each workshop stands alone, allowing you the freedom to participate whenever you choose.

Join the crew of the cutting-edge Airborne io 24 as they navigate cloud security challenges posed by the nefarious Baron Von Herrington. Explore our session topics below:

Monthly Workshop Focus



Register Now at sans.org/ace135





Illustratie Midjourney, c't

BEVRIJDE SLEUTELS

Passkeys gebruiken met opensource tools

Passkeys bieden veel voordelen: je kunt inloggen zonder wachtwoord en loopt geen risico op phishing. Je kunt die veilige en handige aanmeldprocedure ook gebruiken met opensource tools zonder afhankelijk te zijn van Google en Apple. Dat werkt ook onder Linux.

Ronald Eikenberg en Alieke van Sommeren



Je hebt waarschijnlijk al wel eens gehoord van passkeys. Die nieuwe inlogmethode voor webdiensten en apps lost een probleem op dat iedereen heeft: wachtwoorden. Je kunt lekker makkelijk inloggen met een pincode, vingerafdruk of Face-ID zonder te hoeven goochelen met omslachtige wachtwoorden [1]. Een veelgehoord punt van kritiek is echter dat je daardoor overgeleverd bent aan de genade van grote techbedrijven.

Dat is deels waar: iedereen die wachtwoorden opslaat met Android, Apples besturingssystemen of Windows kan ze er niet meer uithalen. Er is geen exportfunctie, wat het overstappen van een iPhone naar een Android-smartphone (of omgekeerd) erg omslachtig maakt. Je moet dan nieuwe passkeys

aanmaken voor alle accounts. Bij Apple en Google worden de wachtwoorden ook altijd opgeslagen in de betreffende cloud. Zelfs als ze van tevoren versleuteld zijn, stoort veel gebruikers dat.

Maar er is een oplossing beschikbaar: omdat de moderne aanmeldingsprocedure is gebaseerd op open webstandaarden kun je in theorie dus genieten van volledige vrijheid. Dat betekent dat je passkeys kunt aanmaken met opensource tools en ze lokaal kunt opslaan of zelfs synchroniseren met een eigen server. Voor maximale veiligheid kun je passkeys opslaan op een FIDO2-stick. Die zijn ook beschikbaar in opensource versies. Dat werkt allemaal op Windows en macOS, maar is ook erg interessant voor Linux-gebruikers omdat Linux-distributies zelf nog geen passkeys kunnen beheren.

KEEPASSXC EN PASSKEYS

De eerste optie is de veelzijdige opensource wachtwoordmanager KeePassXC, die beschikbaar is voor Windows, macOS en Linux. Je hebt minimaal versie 2.7.7 nodig voor passkeys en de KeePassXC-browser-extensie voor je browser (zie de link op de laatste pagina van dit artikel). Als je KeePassXC voor de eerste

keer gebruikt, zal het je eerst vragen om een nieuwe wachtwoorddatabase aan te maken.

Om dat te doen, kies je een hoofdwachtwoord om de database mee te ontgrendelen. Maak het voldoende lang, maar zorg er wel voor dat je goed kunt onthouden. Schrijf het voor de zekerheid op een stuk papier en bewaar het op een veilige plek. Je kunt ervoor kiezen om een sleutelbestand toe te voegen of een hardware-sleutel toevoegen die challenge-response ondersteunt. Er wordt ook gevraagd naar een opslaglocatie voor het databasebestand op je computer.

Na de snelle installatie geef je de browserextensie toegang tot je wachtwoordmanager door op het tandwiel bovenaan KeePassXC te klikken en dan op Browserintegratie aan de linkerkant, en zet daarna aan de rechterkant een vinkje bij 'Browserintegratie inschakelen'. Vink vervolgens onder 'Integratie in de volgende browsers inschakelen' de browsers aan die je wilt gebruiken en klik onderaan op OK. Het lijstje bevat op dit moment Google Chrome, Firefox, Tor Browser, Edge, Chromium, Vivaldi en Brave. Klik op het pictogram van de KeePassXC-extensie in je browser en druk op de knop Verbinden om de app en je browser-extensie te koppelen.

De wachtwoordmanager zal dan opnieuw verschijnen en vragen hoe je de nieuwe verbinding wilt noemen. Voer bijvoorbeeld de naam van de browser in. Onder Linux kan het opzetten van de verbinding mislukken als je de browser als flatpack geïnstalleerd hebt. De eenvoudigste oplossing is in dat geval om de browser uit de pakketrepository's van je distributie te halen.

Zodra de verbinding tot stand gebracht is, klik je opnieuw op het pictogram van de browserextensie en vervolgens op het tandwiel om de instellingen te openen. Scroll naar beneden naar de optie Passkeys en vink het vakje 'Passkeys inschakelen' aan.

Je kunt dan aan de slag met passkeys. Voor een functietest kun je het beste een testpagina zoals WebAuthn.io gebruiken: voer daar een willekeurige gebruikersnaam in en klik op Register. Kort daarna zal KeePassXC tevoorschijn komen en vragen of je een passkey wilt aanmaken, wat je bevestigt door op de knop Registreren te klikken.

Inloggen is net zo eenvoudig. Klik op 'Try it again?' op de demopagina om terug te keren naar het inlogformulier. Klik deze keer op Authenticate. Je hoeft je gebruikersnaam niet in te voeren, want die staat al in de passkey. Zodra KeePassXC reageert, bevestig je met Authenticeren en ben je meteen ingelogd. De wachtwoordmanager gebruikt altijd de op dat moment geopende database voor je wachtwoorden. Als er meerdere bestaan, kun je kiezen.

We konden met KeePassXC met succes passkeys aanmaken voor Amazon, eBay en Google en die gebruiken om in te loggen. Er waren hier en daar wat haperingen, zoals bij het gebruik van de testpagina passkey.org. Dat is een bekend probleem waarvoor al een issue is aangemaakt bij het GitHub-project – zie de link op de laatste pagina. Gebruikers melden daar ook andere websites die problemen geven.

We gaan ervan uit dat de ontwikkelaars bezig zijn met verbeteringen. Een op het moment van schrijven onopgelost probleem is de ondersteuning voor Android, iOS en iPadOS. Er zijn veel KeePass-compatibele smartphone-apps, maar nog geen met passkey-ondersteuning.

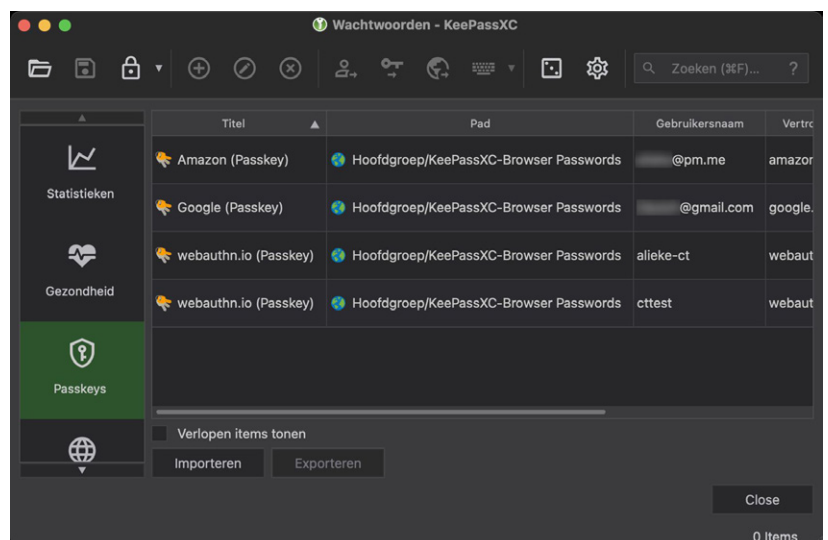
Bij KeePassXC is de beste manier om je wachtwoorden te inspecteren en beheren via 'Database / Passkeys...'. Omdat wachtwoorden en passkeys worden opgeslagen in het databasebestand op je computer, kun je ze eenvoudig kopiëren naar een andere computer of een usb-stick als dat nodig is. Synchronisatie met een tool naar keuze kan ook, bijvoorbeeld via een NextCloud of met Syncthing.

Als je een bepaalde passkey wilt delen, selecteer je die in het overzicht en gebruik je de knop Exporteren om hem op te slaan in een bestand met de extensie .passkey. Maar wees voorzichtig: de privésleutel wordt opgeslagen als platte tekst. Dat betekent dat je passkey net zo goed of slecht beveiligd is als een wachtwoord in een tekstbestand. Als je dubbelklikt op een passkey in KeePassXC en op Geavanceerd klikt, kun je de privésleutel ook bekijken door KPEX_PASSKEY_PRIVATE_KEY_PEM en Onthullen te selecteren.

EIGEN PASSKEY-CLOUD MET BITWARDEN

Een andere manier om vrij en onafhankelijk te blijven bij het gebruik van wachtwoorden is Bitwarden. Dat is vooral geschikt voor gebruik met meerdere apparaten omdat het, net als de meeste moderne wachtwoordmanagers, werkt met een synchronisatieserver. Je hebt de keuze om de cloud van de fabrikant te gebruiken of zelf een server te beheren.

De cloud van de maker is de eenvoudigste optie: installeer gewoon de browserextensie (zie de link) en maak een account aan op bitwarden.com. Passkey-ondersteuning is bij een gratis basisaccount al inbegrepen, dat is te gebruiken met een onbeperkt aantal apparaten. Dat is voor de meeste gebruikers voldoende.



Lokaal opgeslagen: KeePassXC zorgt voor het opslaan van passkeys als je de bijbehorende browserextensie installeert.

Een toegangssleutel maken op dit apparaat
 Log de volgende keer sneller in door een toegangssleutel te maken op dit apparaat.

Met toegangssleutels kun je beveiligd inloggen op je Google-account met je vingerafdruk, gezicht, schermvergrendeling of beveiligingssleutel. Toegangssleutels en beveiligingssleutels kunnen ook worden gebruikt als 2e stap als je inlogt met je wachtwoord. Bescherm je privé- en beveiligingssleutels voor schermvergrendeling, zodat alleen jij ze kunt gebruiken.

Je kunt toegangssleutels maken op je apparaten of op beveiligingssleutels. [Meer informatie](#)

Toegangssleutel maken

+ Toegangssleutel maken

Met Bitwarden is de browserextensie voldoende om passkeys te gebruiken. Je kunt ook zelf een synchronisatieserver instellen.



In tegenstelling tot KeePassXC biedt Bitwarden momenteel nauwelijks extra's voor passkeys. Meld je gewoon aan bij de browserextensie en die zal dan automatisch starten wanneer je een passkey aanmaakt op een website, waarna hem opslaat via 'Passkey als nieuwe login opslaan'. Als je al toeganggegevens voor een website opgeslagen hebt, kun je de toegangscodes aan de bestaande invoer toevoegen. Inloggen is net zo eenvoudig.

De testsite webauthn.io kun je ook weer gebruiken om te testen. Bitwarden werkt ook met de demo-site passkey.org en lijkt in het algemeen een betere compatibiliteit te bieden. Als Bitwarden niet wakker wordt wanneer je passkey-authenticatie start op een website, klik dan op 'Instellingen / Opties' bij de browserextensie en vink het vakje 'Vragen om opslaan van gebruiken van passkeys en wachtwoorden' aan.

Als je meerdere passkeys voor een website nodig hebt, omdat je er bijvoorbeeld meerdere accounts voor hebt, dan heb je meerdere entries in Bitwarden nodig. Je kunt slechts één passkey per vermelding opslaan, maar je kunt een onbeperkt aantal vermeldingen voor een website aanmaken.



Met FIDO2 sticks zoals de Nitrokey Passkey kun je ook onder Linux passkeys gebruiken met maximale beveiliging. De hardware en firmware zijn opensource.

Dat regel je meteen bij het aanmaken van een passkey door in het venster dat tevoorschijn ploft op het plusteken te klikken om een nieuwe vermelding aan te maken. Als dat niet wordt aangeboden en Bitwarden meldt dat er al een passkey voor die login bestaat, maak dan alvast een nieuwe invoer aan door op het pictogram van de browserextensie en het plusteken te klikken. Geef de extra invoer een passende naam, bijvoorbeeld 'Google <account2>', zodat je later niet in de war raakt. Je kunt ook andere gegevens invoeren zoals een klassiek wachtwoord, maar dat is voor een passkey niet nodig. Zodra je de nieuwe invoer hebt opgeslagen, kun je die de volgende keer dat je inlogt selecteren.

Het is niet zo moeilijk om zelf een Bitwarden-server op te zetten op bijvoorbeeld een Raspberry Pi of thin-client. Het opensource project Vaultwarden (zie de link op de laatste pagina) repliceert de API van de Bitwarden-server en vergt weinig resources.

Je kunt Vaultwarden bijvoorbeeld starten als Docker-container, of het jezelf makkelijk maken en het met een paar klikken installeren via de app-store van het YunoHost-serverbesturingssysteem (zie de link). Het gebruik van een eigen server heeft een voordeel ten opzichte van de Bitwarden-cloud: je wachtwoorden en passkeys blijven compleet onder je eigen hoede. Er zijn echter ook nadelen, omdat je zelf moet zorgen voor updates, back-ups en beveiliging.

PASKEYS DELEN

Als je passkeys wilt delen met andere familieleden, vrienden of collega's, maakt Bitwarden dat bijzonder eenvoudig, ook al klinkt het wel wat omslachtig. Je moet daar namelijk een organisatie voor aanmaken waaraan je andere gebruikers toevoegt. Alle passkeys en andere toeganggegevens die je in de toekomst aan die organisatie toewijst, verschijnen ook meteen bij de andere gebruikers. Dat werkt ook met het gratis account in de Bitwarden-cloud met in totaal twee personen – een eigen server heeft die beperking niet.

Om een organisatie aan te maken in de Bitwarden-cloud, open je de webkuis (vault.bitwarden.com) en klik je op '+ Nieuwe organisatie'. Voer een naam en je e-mailadres in, de rest kan op de standaardwaarden blijven staan. Nodig vervolgens iemand uit via 'Leden / + Lid uitnodigen'. Daar is alleen het e-mailadres van de persoon voor nodig. Je moet ook een gedeelde collectie selecteren (standaard Standaardverzameling).

Het nieuwe lid moet dan klikken op de link in de bevestigingsmail en de hoofdgebruiker moet de nieuwe toevoeging dan bevestigen bij de ledenadministratie. Als alles klaar is, kun je bestaande passkeys en meer naar de organisatie verhuizen. De procedure voor Vaultwarden is vergelijkbaar.

Het was op het moment van schrijven alleen mogelijk om passkeys te gebruiken op een smartphone met de bètaversie van de iOS-app. Dat gaat echter snel veranderen, want de Bitwarden-ontwikkelaars werken er met hoge prioriteit aan om passkeys naar de mobiele apps te brengen.

In elke situatie is een up-to-date besturingssysteem vereist om wachtwoordmanager-apps in een mobiele browser te gebruiken voor passkey-authenticatie. Android biedt de benodigde API's pas vanaf versie 14, iOS vanaf versie 17.

KWESTIE VAN VEILIG

Wachtwoordmanagers zijn redelijk veilig, maar hebben beperkte mogelijkheden om de geheimen van gebruikers te beschermen. Als er malware op je computer op de loer ligt, kan die proberen de privésleutels van je passkeys en je wachtwoorden uit het werkgeheugen te stelen nadat de wachtwoordmanager ze heeft ontsleuteld om ermee te kunnen werken.

FIDO2-sticks bieden meer beveiliging, maar ook weer wat minder gemak. Dat zijn speciale usb-sticks die geschikt zijn voor het aanmaken en opslaan van passkeys. In dat geval worden de privésleutels gegenereerd door een chip in de stick en kunnen ze niet worden uitgelezen. Het nadeel is dat je dus geen back-ups kunt maken en de FIDO2-stick altijd bij je moet hebben om de daarop opgeslagen passkeys te kunnen gebruiken. Dat laatste is echter geen groot probleem, want als je cookies toestaat in je browser, blijven je sessies met de meeste webdiensten zo lang openstaan als je wilt. Maar als je de stick verliest, gaan je passkeys ook verloren.

Voorstanders van opensource kunnen eens kijken naar de FIDO2-sticks van SoloKeys (zie de link op deze pagina). Ze werken met opensource firmware en de hardware valt onder de CERN Open Hardware Licentie. De SoloKeys zijn verkrijgbaar in verschillende versies met USB-A, USB-C en NFC. Een ander alternatief is de Nitrokey Passkey. Je kunt die sticks ook gebruiken op smartphones en tablets. Je hebt geen browserextensies nodig om ze te gebruiken omdat de browsers de benodigde functies al bieden. De prijzen van de hardware sleutels beginnen bij zo'n drie tientjes.

VAN NEE NAAR JA

Sommige webdiensten controleren welk besturingssysteem en welke browser je gebruikt en beslissen dan of ze je al dan niet een passkey aanbieden. Toen we dit artikel schreven, gaf het inlogscherm van Amazon bijvoorbeeld geen knop om in te loggen met een passkey weer (door Amazon wat krom vertaald als sleutelcode) als je het scherm met de Firefox-browser opriep. Dat is vooral onhandig voor Linux-gebruikers met Firefox, omdat Linux en Firefox passkeys niet ondersteunen zonder hulp van buitenaf.

Met de hierboven beschreven opties, oftewel een wachtwoordmanager of een FIDO2-stick, werkt het nog wel – zolang de webdienst ook meewerkt. Als je de user-agent van Firefox, die de browser gebruikt om zich te identificeren bij de server, verandert in Chrome, werk je daar handig omheen en kun je ook passkeys gebruiken op websites zoals amazon.nl. Dat gaat heel eenvoudig met de door Mozilla aanbevolen browserextensie User-Agent Switcher and Manager (zie de link).

Klik na het installeren op het pictogram en selecteer een browser uit de lijst, bijvoorbeeld Chrome voor Windows. Pas indien nodig de user-agent aan in de tekstregel eronder om de allernieuwste Chrome-versie in te voeren (zie de link). Klik vervolgens op 'Apply (container)' om de wijziging te activeren.

Je kunt het resultaat controleren door in Google 'my user agent' in te typen, waarna alle recente informatie direct bovenaan in een kadertje verschijnt. Om ongewenste neveneffecten te voorkomen, moet je Firefox alleen als het echt nodig is vermommen als Chrome. De browserextensie heeft daar een whitelist-modus voor, die je kunt selecteren via de opties. Als je bijvoorbeeld amazon.nl aan de whitelist toevoegt, wordt je user-agent alleen daar aangepast. Sla de configuratiewijziging op via Save onderaan de pagina.

CONCLUSIE

Als je passkeys wilt gebruiken, hoef je je zoals dit artikel laat zien niet te onderwerpen aan de grillen van Apple en Google. Je kunt ook een opensource besturingssysteem, een opensource browser en opensource tools gebruiken om zonder wachtwoord bij veel webdiensten in te loggen en de volledige controle over je passkeys te behouden.

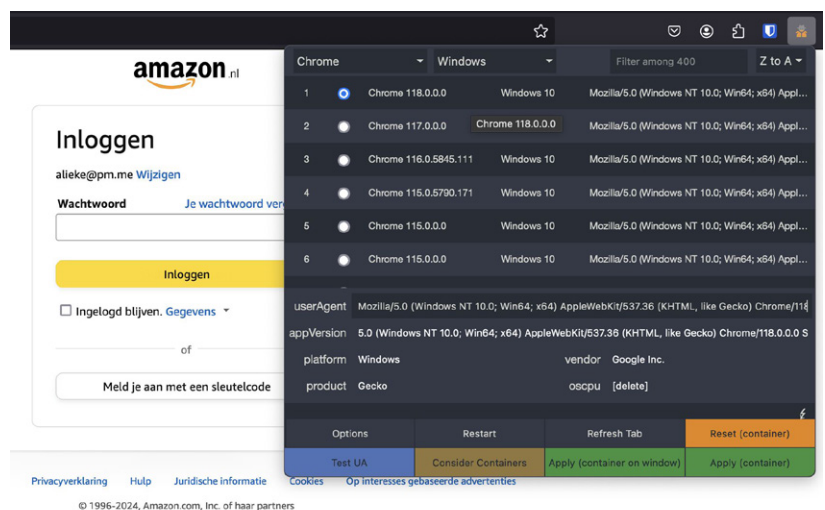
Maar die vrijheid brengt ook verantwoordelijkheid met zich mee, want jij moet nu zorgen voor de beveiliging en back-ups. In sommige situaties werkt nog niet alles vlekkeloos, vooral bij het gebruik van passkeys op Android en iOS. Maar dat zijn problemen die binnenkort opgelost moeten zijn – als je dit leest kun je hopelijk ook de Bitwarden-apps voor passkeys op smartphones en tablets gebruiken. Een geschikte KeePass-app moet vroeg of laat volgen. Dankzij FIDO2-sticks met opensource firmware kun je in de haperende gevallen alsnog passkeys gebruiken. **ct**



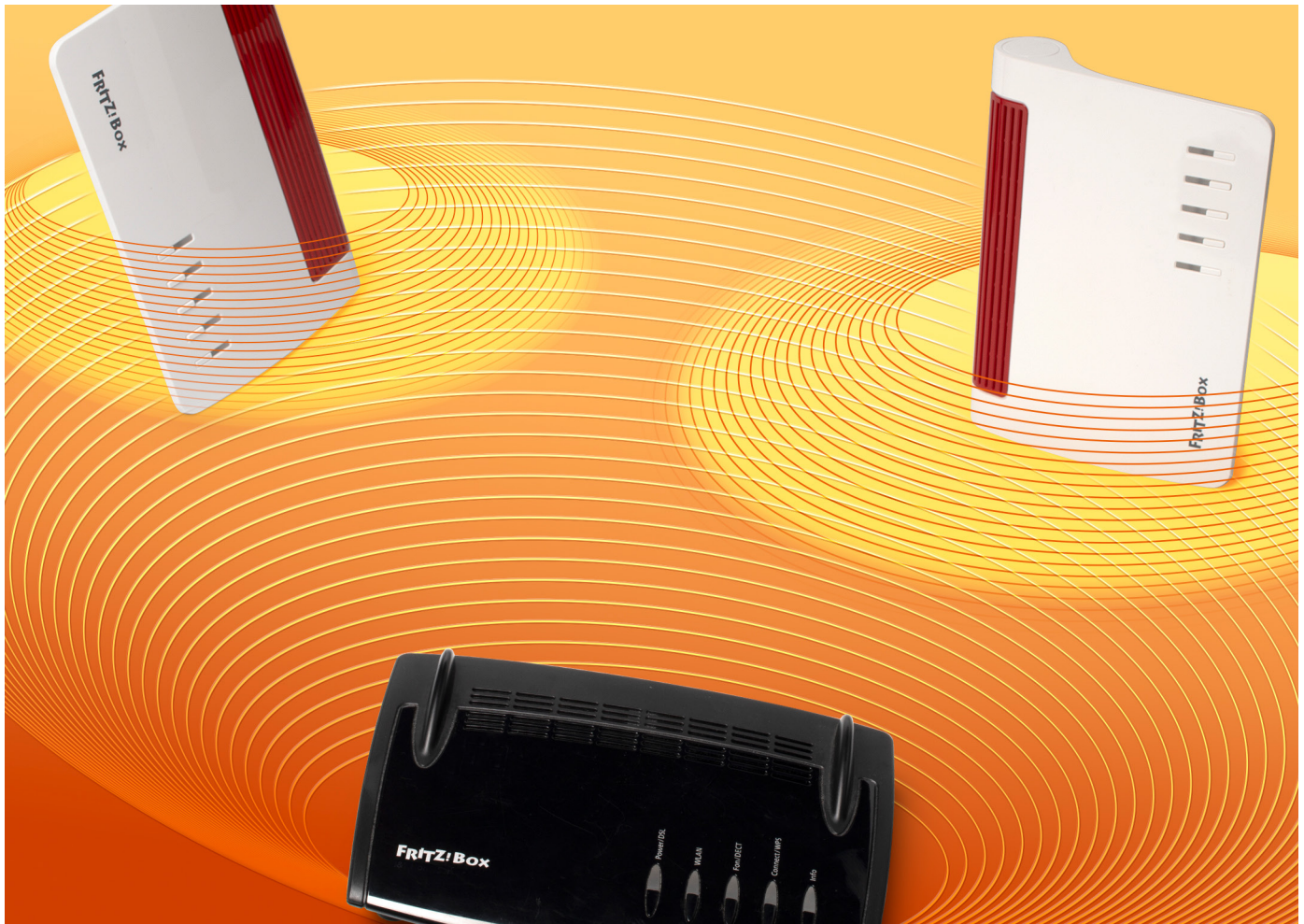
www.ct.nl/softlink/2407126

Literatuur

- [1] Kathrin Stoll en Alieke van Sommeren, Zo werken passkeys, c't 4/2023, p.64
- [2] Ronald Eikenberg en Marco den Teuling, FAQ: Passkeys: inloggen zonder wachtwoord, c't 8-9/2023, p.111



Als je Firefox zich laat identificeren als Chrome, verschijnt de passkey-knop om bij Amazon zonder wachtwoord in te loggen alsnog.



ROUTER VAN DE BUREN

Overwin de thuisnetwerkgrenzen met OpenWrt

Of het nu gaat om een netwerkcamera, NAS of netwerkprinter: er zijn apparaten die je makkelijk kunt delen met burens die je vertrouwt. De routing tussen verschillende thuisnetwerken of alleen toegang tot een paar apparaten werkt met een OpenWrt-router – zo stel je een netwerkbrug in.

Andrijan Möcker en Noud van Kruysbergen



Als jij en je burens maar weinig printen, zou het dan niet een idee zijn om een netwerkprinter te delen? Dat lijkt op het eerste gezicht moeilijk te realiseren, maar kan wellicht met een VPN-verbinding tussen de twee routers? Maar dan kunnen je burens niet printen als hun of jouw internetverbinding eruit

ligt. Je kunt echter ook niet zomaar een switch tussen de netwerken zetten, want dan ontbreekt een netwerkscheiding op layer 2. Iedereen moet immers nog steeds wel zijn eigen internetverbinding kunnen gebruiken.

De oplossing voor het probleem is een extra buurrouter die meerdere virtuele netwerken ondersteunt en in beide thuisnetwerken een eigen (LAN-) interface heeft, elk met een ip-adres van het betreffende netwerk. De router gedraagt zich in die gebieden als een client. Het gedeelde apparaat of de gedeelde apparaten worden bij elkaar in een derde subnet geplaatst waarin de buurrouter ook ip-adressen toewijst.

Of de twee thuisnetwerken ook met elkaar kunnen communiceren, is slechts een kwestie van de

configuratie van de firewall. We laten in dit artikel zien wat je nodig hebt voor een bridge tussen de netwerken en hoe je exclusieve toegang tot de gedeelde apparaten of ongehinderde routing tussen de twee thuisnetwerken kunt configureren.

Dat kan met het opensource routerbesturings-systeem OpenWrt, dat voor veel routers complexe netwerkconfiguraties mogelijk maakt – zelfs op goedkope tweedehands hardware. We gaan ervan uit dat je wat basiskennis hebt van IPv4-adressen en netwerkconfiguraties.

BENODIGDHEDEN

Voor de betrouwbaarheid en een stabiele gegevenssnelheid moeten de twee netwerken met een kabel op de bridge-router worden aangesloten, bijvoorbeeld in een gemeenschappelijke kelder. Routers met twee wifi-interfaces zouden zich kunnen aanmelden op het 2,4GHz-wifi van de ene router en het 5GHz-wifi van de andere, maar automatische kanaalwisselingen, naburige netwerken en andere storende factoren zouden dan regelmatig voor uitval kunnen zorgen.

Als je geen netwerkkabels kunt leggen, zijn eventueel aanwezige vieraderige telefoonkabels ook bruikbaar voor Fast Ethernet. De 100 Mbit/s die je daarmee kunt halen, zijn meer dan voldoende voor toepassingen zoals netwerkprinters. Lees [1, 2] om uit te vinden hoe je goedkoop netwerkkabels kunt leggen of een oude telefoonlijn kunt ombouwen.

De thuisnetwerkroulers moeten statische routes toestaan om vanuit beide netwerken toegang te hebben tot gedeelde apparaten en optioneel tot het thuisnetwerk van de burens. Die instelling informeert de thuisnetwerkrouter dat er een andere router in zijn subnet is via welke andere subnetten kunnen worden bereikt.

Voorbeeld: de eerste thuisnetwerkrouter heeft het ip-adres 192.168.175.1, de bridge-router in zijn subnet is 192.168.175.10 en het remote subnet 192.168.178.0. De route is dan 192.168.178.0/24 via 192.168.175.10. De apparaten in het subnet 175.0 hoeven daar niets van te weten: als een pakket voor het externe thuisnetwerk na configuratie aankomt op de router van het thuisnetwerk (.175.1) (bijvoorbeeld op .178.23), stuurt die het pakket naar de bridge-router (.175.10), die een tweede interface heeft in het externe subnet (zeg 178.10). Omgekeerd moet de router in het externe subnet (.178.1) ook op de hoogte zijn van de bridge-router (178.10) in zijn subnet, zodat het antwoord zijn weg terug vindt naar het andere subnet.

Statische routes zijn standaard in (semi)professionele routers, waaronder de Fritzboxen van AVM met hun FritzOS-besturingssystemen. De standaard providerrouters van KPN en Ziggo hebben die functie meestal niet. Details daarover kun je vinden in de handleiding van je apparaat.

Als beide thuisnetwerkroulers zo'n functie hebben, moet je er alleen voor zorgen dat ze verschillende subnetten gebruiken, zoals 192.168.175.0 en 192.168.178.0.

HARDWARE

We gebruiken hier een Turrís Omnia als bridge-router in dit artikel. Die wordt standaard ondersteund door OpenWrt en heeft genoeg geheugen en opslagruimte om nog jarenlang OpenWrt-updates te installeren.

De netwerkverbinding loopt via de Gigabit-poorten van de Turrís, maar Fast Ethernet-poorten zijn ook genoeg om heen en weer te routeren tussen de twee thuisnetwerken en nog wat extra hardware in de tussenwereld. De Wi-Fi 5-chip van de Omnia gebruiken we verder niet.

Je kunt voor dit project ook een andere ondersteunde router kopen. Kijk op de website van OpenWrt welke routers allemaal ondersteund worden – zie de link op de laatste pagina van dit artikel. Veel wat oudere maar wel ondersteunde routers zijn tweedehands voor een paar tientjes te koop. De website van OpenWrt geeft ook informatie over hoe je OpenWrt op de betreffende modellen moet installeren, daar gaan we hier verder niet op in. De meest recente versie van OpenWrt op het moment van schrijven is 23.05.2.

Verbind je router via een kabel met je computer en stel bij webinterface (<http://192.168.1.1>) een veilig beheerderswachtwoord in. De twee thuisnetwerken mogen nog niet verbonden zijn.

BASISINSTALLATIE

Alleen als de gebruikte subnetten elkaar niet overlappen, zal de routing tussen beide zonder problemen werken. Als beide bijvoorbeeld het standaard Fritzbox-subnet 192.168.178.0/24 gebruiken, moet je bij een van de twee thuisnetwerken een ander subnet zoals 192.168.175.0 gebruiken. Bij FritzOS vind je die instelling bij 'Thuisnetwerk / Netwerk' op het tabblad Netwerkinstellingen bij de IPv4-instellingen. Of en


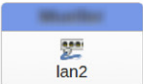
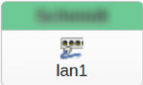


Het opensource routerbesturings-systeem staat standaard geïnstalleerd op een Turrís Omnia, maar het is op veel en ook oudere routers te installeren.

Status ▾ System ▾ Network ▾ Log out REFRESHING

Interfaces | Devices | Global network options | DSL | ATM Bridges

Interfaces

 <p>lan br-lan</p>	<p>Protocol: Static address Uptime: 1h 2m 31s MAC: 38:10:D5:6B:6E:C0 RX: 845.87 KB (7733 Pkts.) TX: 2.37 MB (7528 Pkts.) IPv4: 192.168.21.1/24 IPv6: fd4a:7194:8ddb::1/60</p>	<p>Restart Stop Edit Delete</p>
 <p>lan2</p>	<p>Protocol: DHCP client Uptime: 1h 1m 46s MAC: 38:10:D5:6B:6E:C0 RX: 2.94 MB (30444 Pkts.) TX: 45.28 KB (411 Pkts.) IPv4: 192.168.73.171/24</p>	<p>Restart Stop Edit Delete</p>
 <p>lan1</p>	<p>Protocol: DHCP client Uptime: 1h 1m 43s MAC: 38:10:D5:6B:6E:C0 RX: 2.01 MB (11099 Pkts.) TX: 481.66 KB (3838 Pkts.) IPv4: 192.168.59.132/24</p>	<p>Restart Stop Edit Delete</p>

De buurrouter heeft een virtuele interface in elk thuisnetwerk. Als de twee thuisnetwerkroueters via routes op de hoogte worden gebracht van het bestaan van de bridge, kunnen apparaten communiceren over de grenzen van hun thuisnetwerk heen.

hoe je dat bij andere routerbesturingssystemen kunt doen, vind je in de gebruiksaanwijzing van de betreffende apparaten.

Koppel na het wijzigen alle apparaten in het netwerk even los, zodat ze een ip-adres uit het nieuwe bereik krijgen. De apparaten met een vast adres moeten opnieuw worden geconfigureerd. Eenmaal geïnstalleerd, gebruikt OpenWrt het subnet 192.168.1.0/24. Als dat niet past bij je thuisnetwerkconfiguratie(s), open dan de OpenWrt-webinterface en ga naar het interface-overzicht ('Network / Interfaces'). Klik op Edit naast br-lan en verander het 'IPv4 address', bijvoorbeeld naar 192.168.21.1. Bevestig met Save en klik op 'Save & Apply' onderaan de interfacielijst.

OpenWrt waarschuwt je dat het wijzigen van het ip-adres kan leiden tot verbindingsverlies als je het verkeerd hebt ingetypt en biedt je de optie 'Apply with revert after connectivity loss'. Als je dat accepteert, wacht het systeem 90 seconden totdat je opnieuw verbinding maakt met de webinterface, anders worden de wijzigingen ongedaan gemaakt.

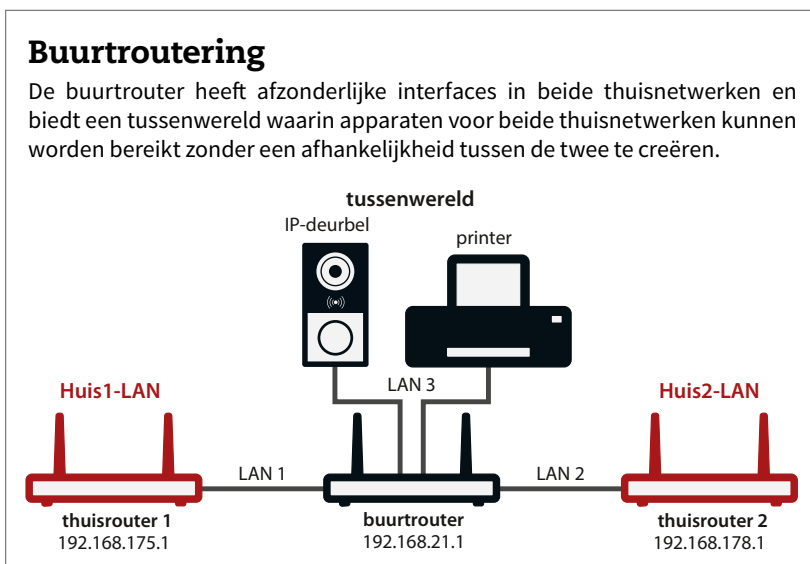
Klik op die optie en verbreek de verbinding dan kort door bijvoorbeeld de LAN-kabel los te koppelen. Zodra de verbinding hersteld is, ga je weer naar de webinterface met het nieuwe adres (192.168.21.1 in ons voorbeeld).

Als je wilt dat de buurrouter met een betekenisvolle naam in het netwerk verschijnt, verander dan de Hostname onder 'System / System'. Mocht het ooit nodig zijn om de logs te lezen, dan kan een onjuiste tijdzone verwarring veroorzaken, maar je kunt hier bij Timezone meteen de juiste instellen.

NETWERKINTERFACES

Bij de startconfiguratie worden bij OpenWrt alle LAN-poorten toegewezen aan een virtuele bridge-interface. Om de poorten meteen aan de nieuwe thuisnetwerkinterfaces toe te kunnen wijzen, moet je ze verwijderen uit de bestaande bridge-interface. Ga daarvoor naar het tabblad Devices onder 'Network / Interfaces' en klik op Configure achter br-lan.

Schakel bij het drop-downmenu 'Bridge ports' alle poorten uit die je wilt gebruiken om met andere thuisnetwerken te verbinden. In dit voorbeeld gebruiken we daarvoor de twee LAN-poorten 1 en 2, dus laat de overige poorten geselecteerd. Bevestig de instellingen en sla ze op. Sluit je computer dan aan op



Als uw netwerk uit meerdere subnetten bestaat die niet rechtstreeks met de FRITZ!Box zijn verbonden, kunt u hiervoor statische IPv4-routes in de FRITZ!Box instellen.

Let op!
Door wijzigingen op deze pagina is de FRITZ!Box mogelijk achteraf niet meer bereikbaar. Raadpleeg in ieder geval de hulp voordat u wijzigingen aanbrengt.

Actief	Netwerk ↑	Subnetmasker ↓	Gateway ↓	
<input checked="" type="checkbox"/>	192.168.21.0	255.255.255.0	192.168.59.132	 

[Nieuwe IPv4-route](#)

[Toepassen](#) [Ongedaan maken](#)

Statische routes informeren de router dat er andere subnetten zijn die bereikt kunnen worden via een andere router in zijn subnet (hier bij een Fritzbox).

een van de andere netwerkpoorten als je verbonden was via LAN 1 of 2. De webinterface is voorlopig niet meer toegankelijk via die poorten.

Je kunt dan de eerste thuisnetwerkinterface aanmaken. Ga naar het tabblad Interfaces en klik op 'Add new interface'. Geef de interface een zinvolle naam en selecteer LAN 1 of 2 bij Device.

Wat je bij Protocol moet selecteren hangt ervan af of de betreffende thuisnetwerkrouter DHCP-adresreserveringen kan maken, oftewel altijd hetzelfde ip-adres aan een apparaat kan toewijzen. Een vast ip-adres op de buurrouter is essentieel voor een statische routing, anders krijgt hij een nieuw adres wanneer de DHCP-lease verloopt en komen de pakketten niet meer aan. Als je router adresreserveringen ondersteunt, zoals het geval is bij een Fritzbox, maak dan van de interface een 'DHCP-client'. Als dat niet het geval is, selecteer dan 'Static address' om het adres zelf in te stellen. Bevestig de selectie met 'Create interface'.

Als je 'DHCP client' geselecteerd hebt, hoeft je bij het volgende venster alleen nog maar een zone toe te wijzen bij de Firewall Settings. Als je wilt dat apparaten van zowel het thuisnetwerk als de tussenwereld ongehinderd met elkaar kunnen communiceren, wijs dan gewoon de bestaande zone lan toe. Klik anders in het veld custom in het vervolgkeuzemenu, voer een willekeurige naam voor de nieuwe zone in en bevestig met Enter. Die kan dezelfde naam hebben als de interface.

Als je het adres zelf moet toewijzen (Static address), heb je bij het volgende menu een ip-adres uit het betreffende thuisnetwerk, het subnetmasker en de gateway nodig. Om het ip-adres correct toe te wijzen, controleer je eerst het DHCP-adresbereik dat is ingesteld bij de betreffende thuisnetwerkrouter.

Het handmatig ingevoerde ip-adres mag niet in dat bereik liggen, omdat sommige routers niet controleren welke adressen in het netwerk al in gebruik zijn. Dat kan leiden tot storende ip-adresconflicten. Als het DHCP-bereik bijvoorbeeld van .50 tot .200 is, kun je adressen vanaf .201 handmatig toewijzen, oftewel 192.168.178.201 voluit geschreven in ons scenario.

Het subnetmasker is voor een thuisnetwerk bijna altijd 255.255.255.0. De gateway is het adres van de betreffende thuisnetwerkrouter, meestal 1, oftewel 192.168.178.1 – de standaardinstelling van een Fritzbox.

Stel ook in dat geval een zone in op het tabblad Firewall Settings, bevestig de instellingen en pas ze toe met 'Save & Apply' – vergeet vooral dat laatste niet.

Herhaal het instellingsproces voor het tweede thuisnetwerk en diens adresbereik. Zodra beide interfaces klaar zijn, sluit je de netwerkkabels aan op de corresponderende poorten. Bij 'Status / Overview' kun je zien of er een verbinding tot stand gebracht is. Als je interfaces in de DHCP-modus geconfigureerd hebt, zouden de adressen kort daarna op de lijst moeten worden weergegeven.

FIREWALLCONFIGURATIE

Als je beide thuisnetwerkinterfaces in de lan-firewall-zone hebt gezet, hoeft je niets te veranderen bij de firewallconfiguratie. OpenWrt routeert de pakketten dan heen en weer tussen de twee thuisnetwerken en de tussenwereld zoals de bedoeling is. De webinterface is ook overal toegankelijk. Sla in dat geval de volgende tekst over tot aan de statische routes.

Als je nieuwe zones hebt aangemaakt bij het maken van de interfaces – met twee verschillende namen – moet je daar nu regels aan toewijzen: ga naar 'Network / Firewall' en klik op Edit voor de eerste nieuwe zone. Sta de zone lan toe bij de opties 'Allow forward to/from destination zones'. Herhaal dat voor de tweede zone.

Sta bij de lan-zone ook toe dat pakketten van die zone worden doorgestuurd naar de twee nieuwe zones, voor zover OpenWrt dat zelf nog niet gedaan heeft. Die configuratie geeft beide netwerken toegang tot de tussenwereld en vice versa. De buurrouter verhindert echter de communicatie tussen de twee thuisnetwerken.

Als je toch wilt dat de OpenWrt-webinterface toegankelijk is vanaf beide thuisnetwerken om latere configuratiewijzigingen te vergemakkelijken, moet je daar ook twee regels voor aanmaken. Ga naar het tabblad Traffic Rules van het firewallmenu en klik onderaan op Add. Geef de regel een naam zoals 'HTTP-Router1' en stel de zone met dezelfde naam in als de Source Zone. Selecteer bij Protocol alleen TCP. Stel 'Device (Input)' in als de Destination Zone, de Destination Port is de HTTP-standaardpoort 80. Maak die regel ook aan voor de tweede zone.

Als je liever versleutelde toegang binnen de thuisnetwerken wilt hebben, maak beide regels dan opnieuw aan voor TCP poort 443, de HTTPS-standaardpoort.



[www.ct.nl/softlink/
2407130](http://www.ct.nl/softlink/2407130)

STATISCHE ROUTES

De configuratie van de OpenWrt-buurtrouter is met het instellen van de firewall voltooid, je kunt je aandacht dan richten op de eerste thuisnetwerkrouter. Daarvoor maak je rechtstreeks verbinding met het netwerk via LAN of wifi. Als je de betreffende interface als DHCP-client hebt geconfigureerd in de OpenWrt-router, moet je eerst de reservering maken zodat het ip-adres hetzelfde blijft.

Bij FritzOS kun je dat doen door het overzicht te openen onder 'Thuisnetwerk / Netwerk' en te zoeken naar de buurtrouter op de apparatenlijst. De apparaatnaam moet de hostnaam zijn die je eerder toegewezen hebt.

Klik op het potloodje achteraan op de apparaatregel om het apparaatmenu te openen. Vink bij 'Adressen in het thuisnetwerk (IP-adressen)' de optie 'Aan dit netwerkapparaat altijd hetzelfde IPv4-adres toewijzen' aan. Noteer het toegewezen ip-adres, dat heb je nodig voor de statische route(s).

FRITZOS

De instellingen voor statische routes zijn ook te vinden in het netwerksubmenu bij FritzOS: op het tabblad Netwerkinstellingen is er een verborgen optie IPv4-routes onder 'meer instellingen'. Klik op 'Nieuwe IPv4-route'. Het IPv4-netwerk is het externe subnet dat je toegankelijk wilt maken in het thuisnetwerk – in ons voorbeeld de tussenwereld 192.168.21.0. Het subnetmasker is 255.255.255.0.

De gateway is het ip-adres van de buurtrouter in het betreffende thuisnetwerk. Dat heb je eerder ge-

definieerd tijdens de vaste toewijzing in de OpenWrt-interface of overgeschreven van de webinterface toen je de reservering aanmaakte.

Herhaal het proces voor het subnet van het naburige thuisnetwerk als je dat op dezelfde manier toegankelijk wilt maken. De gateway en het subnetmasker blijven hetzelfde.

Zodra de routes aangemaakt zijn, probeer dan de OpenWrt-webinterface in de browser te bereiken. Als je geen antwoord krijgt, maak dan opnieuw verbinding met de OpenWrt-router en controleer de firewallregels. Als alles werkt, ga dan naar het andere thuisnetwerk en maak de routes in de tegenovergestelde richting aan: configureer de reservering, noteer het ip-adres van de buurtrouter (gateway) in het thuisnetwerk en stel routes in voor de externe subnetten.

Zodra de routes op beide thuisnetwerkroulers zijn ingevoerd, zou je de tussenwereld en de thuisnetwerken met elkaar moeten kunnen bereiken – op voorwaarde dat je dat geconfigureerd hebt. Als dat niet werkt, controleer dan de routes op typefouten en de firewallinstellingen op ontbrekende zone-toewijzingen.

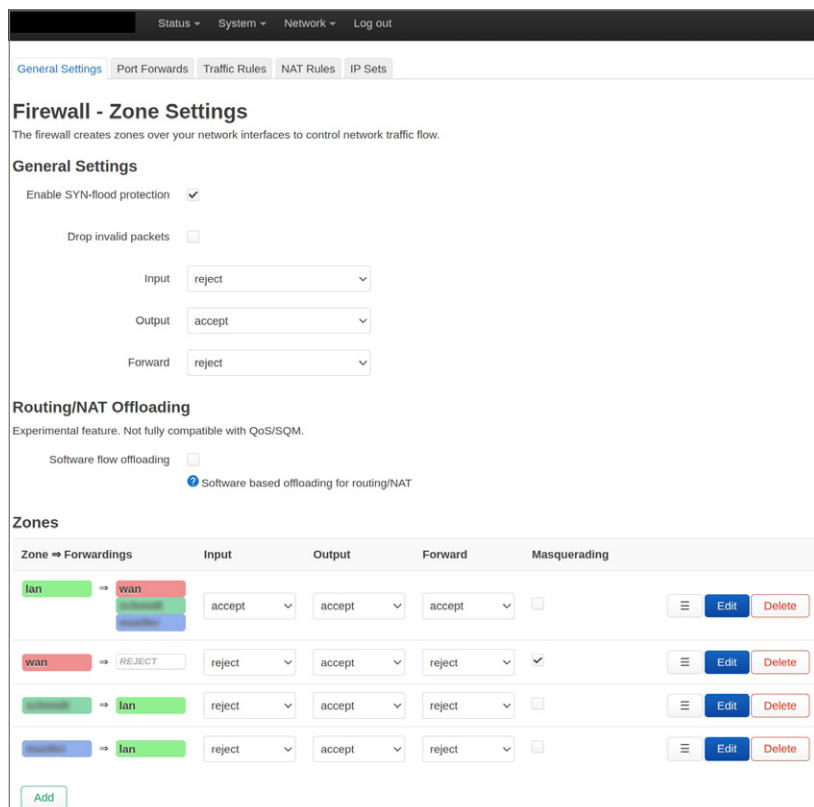
LEVEN IN DE TUSSENWERELD

Als de routers de pakketten met succes van A naar B en C sturen, kun je apparaten voor de tussenwereld aansluiten en configureren op de andere poorten van de buurtrouter.

Je moet dat doen met hardware waarvan de functie een hoge prioriteit heeft voor beide partijen, zelfs als je routing tussen beide thuisnetwerken toestaat. Als een netwerkprinter zich bijvoorbeeld in thuisnetwerk A bevindt, is hij afhankelijk van de thuisnetwerkrouter voor routing naar de andere netwerken. Alleen apparaten in de tussenwereld kunnen echt onafhankelijk bereikt worden, zelfs als een van de internettoegangspunten of routers uitvalt.

Als er andere gedeelde apparaten bijkomen, is er geen reden om niet een switch aan te sluiten. Je kunt indien nodig ook het wifi opnieuw activeren en je tussenliggende netwerk draadloos toegankelijk maken. Je vindt de configuratie daarvoor bij OpenWrt onder 'Network / Wireless'.

Tot slot moet je de configuratie downloaden onder 'System / Backup / Flash Firmware' (Generate archive) en opslaan. Daarmee kun je altijd weer terugkeren naar de laatst werkende configuratie. Dat werkt ook met vervangende apparaten van hetzelfde type, zodat je de netwerkprinter en dergelijke weer snel gebruiksklaar kunt maken als de vorige buurtrouter is gesneuveld door bijvoorbeeld een bliksem-inslag.



Bij OpenWrt is de firewall beginnersvriendelijk, een paar eenvoudige instellingen voorkomen dat de thuisnetwerken met elkaar communiceren.

Literatuur

- [1] Andrijan Möcker en Alieke van Sommeren, Netwerkbekabeling: van noodoplossing tot professioneel en duurzaam, c't 5/2021, p.84
- [2] Andrijan Möcker en Alieke van Sommeren, Goedkope snelle netwerkbekabeling voor thuis, c't 8-9/2023, p.98

DE NIEUWE NIS2-RICHTLIJN KOMT ER AAN

Uitdagingen en kansen voor organisaties

Om aan de vereisten van de nieuwe Network and Information Security richtlijn (NIS2) te voldoen, moeten organisaties zorgen dat ze sneller kunnen detecteren en sneller kunnen reageren.

Organisaties hebben zich te lang alleen gericht op het beschermen tegen en het detecteren van compromissen binnen hun eigen omgeving. Met de Network and Information Security Directive (NIS2) komt de focus te liggen op verbeterde detectie van kwaadaardige activiteiten voordat het een incident wordt. 'Beheerders van Security Operations Centers (SOC) zouden de nieuwe richtlijn als hun bondgenoot moeten beschouwen,' zegt SANS Certified Instructor Maxim Deweerdt.

Deweerd geeft al bijna tien jaar cyber defence-cursussen bij SANS, zowel vanuit een technisch als managementperspectief. Hij is gespecialiseerd in het opbouwen van een SOC-operatie en adviseert organisaties over dit onderwerp. Hij vindt dat de nieuwe richtlijn van de Europese Unie (EU) een goede stap is. 'De richtlijn versterkt de maatregelen die genomen moeten worden voor risicobeheer op het gebied van cyberbeveiliging, ze legt verplichtingen op om incidenten te melden en schetst de mogelijke sancties voor als dat niet wordt nageleefd. Deze verhoogde mate van aansprakelijkheid op bestuursniveau betekent dat er meer aandacht zal zijn voor cyberbeveiliging en snellere cyberdetectie,' aldus Deweerdt.

BESTUURLIJKE AANSPRAKELIJKHEID

SOC-leiders en organisaties die al stappen hebben genomen op basis van de vorige NIS-richtlijn of die voldoen aan andere standaarden en frameworks zoals ISO27001, hoeven zich niet al te veel zorgen te maken over de gevolgen van de NIS2-richtlijn. 'We pleiten al heel lang voor aandacht voor cyberbeveiliging op bestuursniveau,' zegt Deweerdt. 'De NIS2-regeling geeft nu expliciet een gevoel van urgentie aan het bestuur van organisaties in de vorm van directe aansprakelijkheid als ze hun verantwoordelijkheden niet opvolgen.'

De strenge NIS2-vereisten zorgen voor meer informatiedeling in individuele landen en in Europa als geheel en vragen een veel betere detectie van bedreigingen. Hoe sneller een bedreiging wordt gedetecteerd, hoe beter een organisatie kan anticiperen op het voldoen aan de wettelijke meldingsplicht.

BEVEILIGING VAN DE EU VERBETEREN

Het doel van de NIS2 is om een gemeenschappelijke cyberbeveiligingsnorm in alle Europese lidstaten te vestigen en de samenwerking op het gebied van cyberbeveiliging te vergroten. Dit geldt met name in kritieke sectoren waar een verstoring een negatieve impact kan hebben op alle burgers.

Organisaties die als essentieel worden gecategoriseerd, krijgen te maken met proactieve nalevingscontroles. Organisaties met het predicaat belangrijk krijgen hooguit te maken met beperkt reactief toezicht en dus niet met direct toezicht, tenzij er zich een significant incident voordoet.

UITDAGINGEN

NIS2 zal een bondgenoot zijn voor SOC-leiders, hoopt Deweerdt. 'Als je een SOC-manager bent in een organisatie die onder de nieuwe regelgeving valt, dan moet het hopelijk makkelijker zijn om zwakke punten te identificeren en onder de aandacht van het management te brengen. Het NIS2 geeft een goede aanleiding om ervoor te zorgen dat ze aan de richtlijn kunnen voldoen.'

VOORBEREIDEN OP NIS2

Organisaties kunnen samen met experts een uitgebreide inventarisatie van cyberbeveiligingslekken uitvoeren om zich voor te bereiden op de nieuwe richtlijn. Het advies is om te beginnen met het ISO27000-framework, het NIST CSF-framework of landspecifieke richtlijnen. Deze kunnen helpen bij het identificeren van hiaten met betrekking tot

de wettelijke verplichtingen. Besteed speciale aandacht aan onderdelen zoals de toeleveringsketen en het risicobeheer van elk framework, aangezien dit belangrijke aandachtspunten van NIS2 zijn. Het is belangrijk dat organisaties contact opnemen met hun CISO, juridische team of een NIS2-expert om op de hoogte te blijven van de manier waarop overheden de richtlijn omzetten in nationale wetgeving.

DE PERSOONLIJKE NOOT

Wat Deweerdt het liefst meegeeft als het gaat om voorbereiding op NIS2, is het belang van het opbouwen van een persoonlijke relatie met iemand bij hun lokale cyberbeveiligingsautoriteit. 'Gebruik al het advies en de informatie die deze centra geven en doe kennis op over wat de lokale autoriteit van je verwacht met betrekking tot de NIS2-richtlijn. Bekijk vervolgens alle aspecten die relevant voor de richtlijn zijn. Stel prioriteiten en maak een plan om ze aan te pakken.' Ten slotte adviseert Deweerdt om precies te weten wat de zwakke punten zijn in hun softwareomgeving en die zichtbaar te maken voor het management. 'Zeg niet alleen dat je meer budget nodig hebt, maar laat de hiaten zien en de mogelijke gevolgen als ze niet worden aangepakt.'

Alles over de NIS2-richtlijn

SANS en onze instructeurs hebben een hub gemaakt met alles wat je moet weten over de nieuwe NIS2-richtlijn, inclusief bronnen, infographics en checklists die je kunt gebruiken om jezelf en jouw organisatie voor te bereiden op de nieuwe richtlijn. Ga voor meer informatie naar:

www.sans.org/mlp/nis2/



Hotline

UPGRADEN MET C'T-WIMAGE

? Ik heb met c't-WIMage een back-up gemaakt van de huidige installatie (Windows 11 versie 23H2) op mijn pc en het is gelukt die te herstellen op een andere pc. Ik heb echter nog een andere computer met Windows 11 in de oude versie 21H2. Kan ik die oude Windows upgraden naar 23H2 met behulp van mijn c't-WIMage back-up?

! De tool c't-WIMage (zie de link op de laatste pagina van deze hotline) is exclusief ontworpen om een back-up te maken van bestaande installaties en die vervolgens terug te zetten op vrijwel alle hardware. Het herstellen is onder andere zo betrouwbaar omdat het wordt gedaan door het installatieprogramma van Windows zelf. Het denkt dat het een schone, nieuwe Windows installatie maakt, maar beseft niet dat het in plaats daarvan de back-up herstelt die c't-WIMage gemaakt heeft. Dat is de essentie c't-WIMage en is geen ingewikkelde hack, maar precies zoals Microsoft het bedoeld heeft.

Je back-up wordt dus hersteld als een nieuwe installatie. Een upgrade is technisch anders. Ter vergelijking: tijdens een nieuwe installatie partitioneert en formatteert het set-upprogramma de doelgegevensdrager, installeert er vervolgens de nieuwe Windows op en voorziet die van een bootloader die overeenkomt met de hardware. Bij een upgrade verplaatst het installatieprogramma daarentegen eerst de bestaande installatie naar een nieuwe map met de naam Windows.old, installeert dan de nieuwe Windows ernaast en probeert ten slotte alle documenten, toepassingen en instellingen van de oude installatie over te zetten naar de nieuwe. We zeggen bewust 'probeert' omdat dit niet altijd betrouwbaar werkt. Dat ondanks het feit dat het doel van de gegevensoverdracht zich in een vooraf gedefinieerde staat bevindt omdat het een nieuwe installatie is.

De gegevensoverdracht zou veel complexer zijn als je zou proberen een upgrade uit te voeren met behulp van een c't-WIMage back-up. Dat komt omdat de bestaande installatie dan eerst geïnstalleerd zou moe-

ten worden in Windows.old, en dan zou je back-up ernaast worden geïnstalleerd in plaats van een nieuwe Windows. Dan zou het installatieprogramma de taak hebben om documenten, toepassingen en instellingen over te zetten van de oude installatie naar de herstelde installatie, dus als het ware twee installaties in één te verenigen.

Dat is gedoemd te mislukken: zelfs als het resultaat opstart, is het zeer waarschijnlijk dat de overdracht fout gaat – tenminste voor individuele toepassingen en instellingen. De ware gevolgen daarvan merk je mogelijk pas na verloop van tijd. Maar wat nog belangrijker is: je documenten zijn dan een mix van de documenten die voor de upgrade bestonden en de documenten die afkomstig zijn van de back-up. In het ergste geval kan dat leiden tot gegevensverlies.

Bespaar jezelf dus de moeite om upgrades te proberen te maken met behulp van c't-WIMage back-ups. Dat kan alleen maar fout gaan.

CENTREREN MET CSS

? Af en toe moet ik CSS-bestanden op een website bijwerken, maar het lukt me maar niet om elementen correct te centreren. Zo moeilijk kan dat toch niet zijn?

! Dat is niet moeilijk, er zijn alleen talloze manieren die allemaal naar hetzelfde doel leiden. Het wordt echt ingewikkeld als je ook oude browsers wilt of moet ondersteunen.

De snelste manier om de juiste CSS-snipet te vinden is door gebruik te maken van de kleine online generator van ontwikkelaar Oliver Zheng (zie de link op de laatste pagina). Selecteer daarvoor je wensen in het online formulier, klik op 'Generate code' en kopieer de resulterende code.

VASTGESOLDEERDE MOEDERBORBATTERIJ VERVANGEN

? Ik heb een acht jaar oude mini-pc die zijn BIOS-instellingen vergeet. Ik ga er van uit dat de bufferbatterij leeg is. Die zit echter met een kabeltje vastgesoldeerd op het moederbord. Is er een manier om hem te vervangen zonder te solderen?

! De moederborden van desktop-pc's hebben meestal een vastgesoldeerde houder voor een CR2032-lithiumcel met een nominale spanning van 3 volt. Als de voeding van de pc uitgeschakeld is, zorgt die ervoor dat de realtime klok (RTC) die in de chipset is ingebouwd doorloopt en dat de buffer van het CMOS-RAM de configuratie van het BIOS onthoudt. Als de batterijspanning zakt tot onder de 2 volt, moet hij vervangen worden.

In veel laptops en mini-pc's is de bufferbatterij echter aangesloten via een kabel met twee draadjes, die vaak een propriëtaire stekker heeft of zelfs vastge-



c't-WIMage is ideaal om een bestaande Windows te verhuizen naar een andere pc. De tool kun je beter niet gebruiken om er meteen een upgrade mee te doen.

soldeerd is. Aan het andere uiteinde bungelt dan de met krimpkous geïsoleerde knoopcel. Daarvoor bestaat vaak geen geschikte vervanging.

Als alternatief kun je de twee kabeladers van de batterij doorknippen, de isolatie een stukje verwijderen en een CR2032-knoopcel in een batterijhouder aansluiten – let op de polariteit! De gesoldeerde of gedraaide contacten isoleer je vervolgens met krimpkous. Of je kunt kleine verbindingsklemmetjes gebruiken voor dunne fijnaderige geleiders zoals de Wago 222-412.

We hebben goedkope batterijhouders van Amazon geprobeerd – een zakje met 20 stuks kostte ongeveer 8 euro. Ze zien er mechanisch wat wiebelig uit, maar werken wel.



Losse houders voor CR2032-knoopcelbatterijen kunnen uitkomst bieden wanneer een oudere pc de BIOS-instellingen en de tijd vergeet.

ESP NIET PROGRAMMEERBAAR ONDER LINUX

? Ik wil met PlatformIO in Visual Studio Code een ESP-microcontroller programmeren. Op mijn Mac werkt dat prima. Nu probeer ik hetzelfde te doen op Linux, maar ik krijg steeds een time-out als ik de programmacode probeer te laden op de ESP. Wat is daar de reden voor?

! Misschien zit een ander apparaat in de weg voor de driver voor seriële usb-apparaten. We hebben dat meegemaakt bij een Linux Mint-pc: in de logs die via `dmesg` gelezen konden worden stond de melding ‘ch341-uart converter now disconnected from ttyUSB0’ en daarboven de opmerking ‘usbfs: interface 0 claimed by ch341 while ‘brltty’ sets config #1’. Blijkbaar heeft een driver voor de braille-uitvoer het apparaat in beslag genomen. Er zijn verschillende tips op internet te vinden om dat te voorkomen door de configuratieregels voor `udev` aan te passen. Je kunt dat ook doen door gewoon het relevante pakket te verwijderen met `apt-get remove --purge brltty`.

ANDROID ROOTEN: OEM-ONTGRENDELEN

? Mijn smartphone is een Essential PH-1 uit 2017 die geen updates meer ontvangt. Ik wil hem rooten en LineageOS installeren, maar dat mislukt al wanneer ik probeer de OEM-vergrendeling op te heffen. De smartphone vraagt alleen om de pincode van het apparaat en doet verder niets. Is het defect of is er een oplossing?

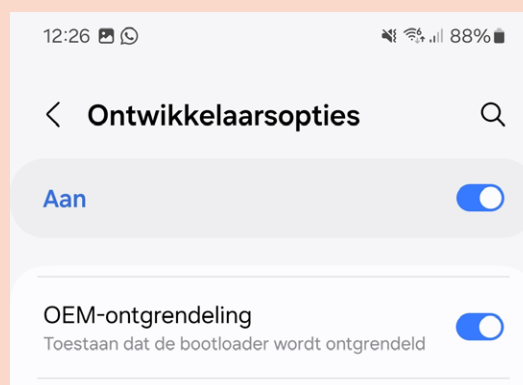
! Afhankelijk van de fabrikant kan de optie om de OEM-vergrendeling op te heffen verschillend geïmplementeerd zijn. Sommige vereisen een specifieke code of een specifieke procedure, terwijl voor anderen de ontgrendelingscode van het apparaat eigenlijk al voldoende is.

Als dat niet helpt, kan het ook voldoende zijn om de simkaart uit de smartphone te verwijderen. Dan wordt de ontwikkeldermodus weer uitgeschakeld, maar die kun je gewoon weer inschakelen: ga bij de Android-

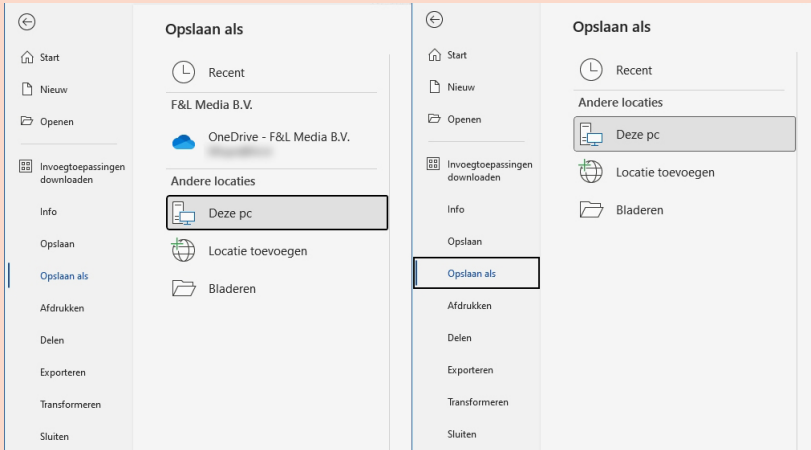
stelselinstellingen onderaan naar het menu ‘Info telefoon’ en tik zeven keer op de buildversie. Voer de pincode van het apparaat in als daarom wordt gevraagd. Bij de instellingen zal Android dan het menu-item Ontwikkelaarsopties weergeven, waar de OEM-vergrendeling eindelijk kan worden geannuleerd – misschien dat je eerst de pincode nog een keer moet invoeren. Je kunt dan de simkaart opnieuw plaatsen, de OEM-ontgrendeling blijft gehandhaafd.

ONEDRIVE VERWIJDEREN

? Ik gebruik Microsoft Office 2021 en ben niet geïnteresseerd in het opslaan van bestanden in de cloud. Hoewel ik OneDrive uit Windows verwijderd heb, krijg ik nog steeds OneDrive aangeboden als opslaglocatie in bijvoorbeeld Word onder ‘Opslaan als’. Is het mogelijk om de vermelding volledig te verwijderen?



Om een smartphone te kunnen rooten, moet je afhankelijk van de fabrikant eerst nog de OEM-ontgrendeling activeren.



Een entry in het Windows-register zorgt ervoor dat de cloudopslagbestemmingen verdwijnen uit Microsoft Office. Links de weergave 'Op slaan als' vóór en rechts ná de ingreep.

! Helaas is het daarvoor niet afdoende om de OneDrive-client uit Windows te verwijderen. De Office-programma's hebben namelijk hun eigen synchronisatiemechanisme en communiceren rechtstreeks met de OneDrive- en SharePoint-servers.

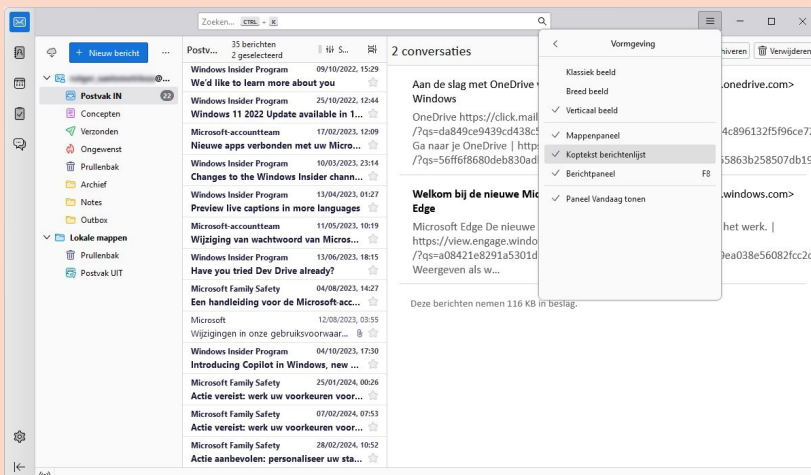
Er is geen officiële optie om de koppelingen naar OneDrive en SharePoint te verwijderen uit de Office-interface (om precies te zijn: de Backstage-weergave die verschijnt na het klikken op Bestand). Tijdens het testen met de huidige Office-programma's van Microsoft 365 en met Office 2021 bereikte een aanpassing in het register echter het gewenste effect.

Voer in het register onder HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Internet een nieuwe sleutel van het type DWORD in met de naam OnlineStorage. Wijs die een waarde toe van 1 om OneDrive te verwijderen, 2 voor SharePoint of 3 voor alle MS-services. De waarde 0 herstelt de oorspronkelijke status.

Dat gaat sneller met een PowerShell-commando:

```
Set-ItemProperty -Path "HKCU:\Software\Microsoft\Office\16.0\Common\Internet" -Name OnlineStorage -Value <waarde>
```

Vervang de laatste parameter <waarde> door het juiste



Thunderbird toont informatie zoals het aantal geselecteerde berichten nu in de koptekst van de berichtenlijst.

getal. Daardoor verlies je ook de functie 'Automatisch opslaan', die vereist dat het bestand in kwestie ook in de cloud opgeslagen wordt. Als je het toch probeert te activeren, krijg je een foutmelding dat er geen geschikte opslaglocaties gevonden zijn. We kunnen niet garanderen dat die truc met alle Office-versies werkt en dat Microsoft die manier met een update op termijn niet zal blokkeren.

PC START PLOTSELING NIET MEER OP

! Onlangs wilde een pc op ons kantoor plotseling niet meer opstarten. Alle gebruikelijke herstelmaatregelen, zoals het gebruik van Bcdboot om de opstartbestanden te herstellen, leidden tot niets.

Uiteindelijk bleek dat de CSM-bootmodus actief was bij de BIOS-instellingen, ook al stond er een Windows UEFI-installatie op de harde schijf. Nadat we die deactiveerden, startte de pc weer op. Een paar dagen later echter weer hetzelfde: de pc kon wel aangezet worden, maar na wat geratel van de dvd-drive schakelde hij kort uit en startte weer op. Dat herhaalde zich, maar Windows wilde niet opstarten. We hebben toen de CMOS-batterij vervangen, en inderdaad, na het uitschakelen van CSM-boot en het laden van de CMOS-defaults, werkte de pc weer perfect.

De verwijderde CMOS-batterij had met 3,2 volt niet te zwak hoeven te zijn – de meeste moederborden en pc's verliezen hun instellingen pas onder de twee volt – maar in dit geval was dat duidelijk de oorzaak, de pc werkt inmiddels al enkele weken weer perfect.

THUNDERBIRD GEEFT HET AANTAL MAILS NIET WEER

? Thunderbird gaf vroeger het aantal gemarkeerde mails weer op de statusbalk, maar die weergave ontbreekt sinds een tijdje bij mij.

! Sinds versie 115 Supernova hebben de Thunderbird-ontwikkelaars die informatie verplaatst naar een extra 'koptekst'. Als je die niet ziet: klik op het hamburgermenu (de drie streepjes) in de rechterbovenhoek en navigeer naar 'Beeld / Vormgeving' en activeer 'Koptekst berichtenlijst'.

IPERF3-SERVER OP ANDROID

? Ik wil mijn nieuwe smartphone gebruiken om wifibenchmarks te meten met iPerf3. Op mijn oude smartphone werkte dat met de he.net Network Tools, maar die kunnen bij Android 14 niet meer geïnstalleerd worden. Ik heb geen app kunnen vinden waarmee je een serie metingen op dezelfde doelpoort kunt maken of zonder de iPerf3-serverfunctie handmatig opnieuw te starten na elke run. Hoe doen jullie dat?

! Voor onze tests installeren we de Linux-omgeving UserLand en zetten daar een Alpine Linux-instantie op, die heel weinig geheugen nodig heeft. Een `apk-update` of `apk-upgrade` is nodig om Alpine up-to-date te brengen. Negeer alle apk-foutmeldingen die mogelijk verschijnen omdat het vanuit een onbekende omgeving werkt.

Vervolgens haal je met `apk add iperf3` de gewenste benchmark binnen, die je zoals gewoonlijk op de commandline start met `iperf3 -s`. Op die manier lukte het ons voor de test van Wi-Fi 7-basisstations (zie c't 5/2024 op pagina 60) om met een Pixel 8 een netto snelheid van meer dan 2 Gbit/s te halen.

GEEN VIDEOGELUID IN TEAMS

? Ik wil een YouTube-video laten zien in een Microsoft Teams-vergadering, maar bij het delen van het scherm streamt Teams wel de video, maar zonder geluid naar de andere deelnemers aan de videoconferentie. Wat moet ik doen om te zorgen dat de audio van de video ook hoorbaar is?

! Teams streamt normaal gesproken de audio die op je computer wordt afgespeeld niet. Je moet de schakelaar 'Geluid opnemen' in het selectievenster activeren voordat je scherm delen start.

Microsoft biedt Teams voor Linux alleen nog maar aan als webversie in de browser. Daar moet je het tabblad met de YouTube-video delen en het selectievakje 'Tabbladaudio delen' inschakelen. In beide gevallen verstuurt Teams dan ook het audiospoor en niet alleen je microfoonsignaal. De kwaliteit is echter wisselend, afhankelijk van de verbinding.

ALTERNIEVE PRINTERINKTEN

? We gebruiken op ons kantoor Canon TS 7400-inkjetprinters, waar we erg tevreden over zijn. Tot nu toe hebben we alleen originele inktcartridges van Canon gebruikt, omdat we niet kunnen inschatten hoeveel pagina's alternatieve inkt zal printen. Kan het gebruik van cartridges van andere leveranciers zoals KMP bijvoorbeeld leiden tot verlies van garantie?

! De cartridges in Canon-printers zijn combinatiecartridges met geïntegreerde printkoppen. Dat maakt die cartridges duurder, maar als er problemen zijn met verstopte spuitmondjes, hoef je alleen de betreffende cartridge te vervangen in plaats van de gehele printer.

Voor zover wij weten bieden alternatieve leveranciers zoals KMP hervulde originele cartridges aan, wat betekent dat de printkoppen al een onbepaald aantal pagina's hebben afgedrukt.

Normaal gesproken is dat geen probleem, want ze zouden makkelijk tien keer de hoeveelheid inkt die ze bevatten kunnen printen. De bubblejet-printkoppen

die Canon gebruikt, gaan gemiddeld 10.000 pagina's mee.

Als je alternatieve inkten overweegt, raden we bedrijven als KMP, Peach en Pelikan aan. Dergelijke bedrijven hebben jarenlange ervaring en bieden service en garantie. In het geval van KMP zouden de cartridges hetzelfde bereik moeten hebben als de originelen. Net als de printerfabrikanten specificeert KMP het bereik volgens de ISO/IEC 24711 standaard, wat controleerbaar is.

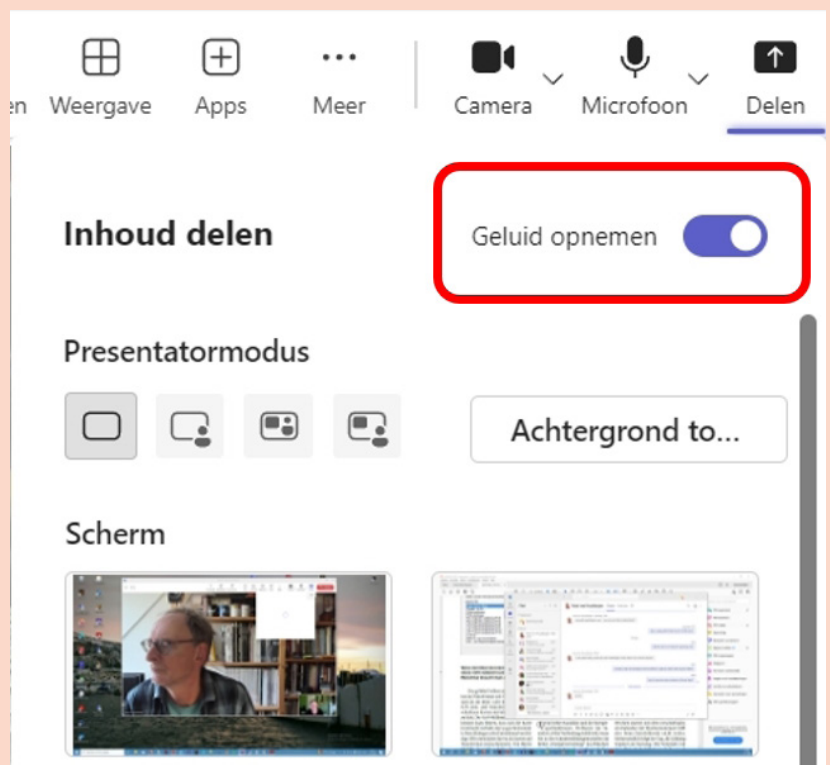
Cartridges van gerenommeerde leveranciers hebben geen invloed op de levensduur van een printer. Als een cartridge niet goed afdrukt, bijvoorbeeld omdat de geïntegreerde printkop defect is, geldt de garantie van de leverancier.

De printerfabrikanten handhaven geen algemeen garantieverlies voor de hele printer bij gebruik van inkt van derden – dat zou ook juridisch niet houdbaar zijn. Servicelocaties zullen echter controleren of er bij garantiereparaties inkt van derden gebruikt is. Aangezien jullie printers modellen zijn met combinatiecartridges die je op elk moment kunt vervangen door originele cartridges, zou dat ook geen probleem moeten zijn.

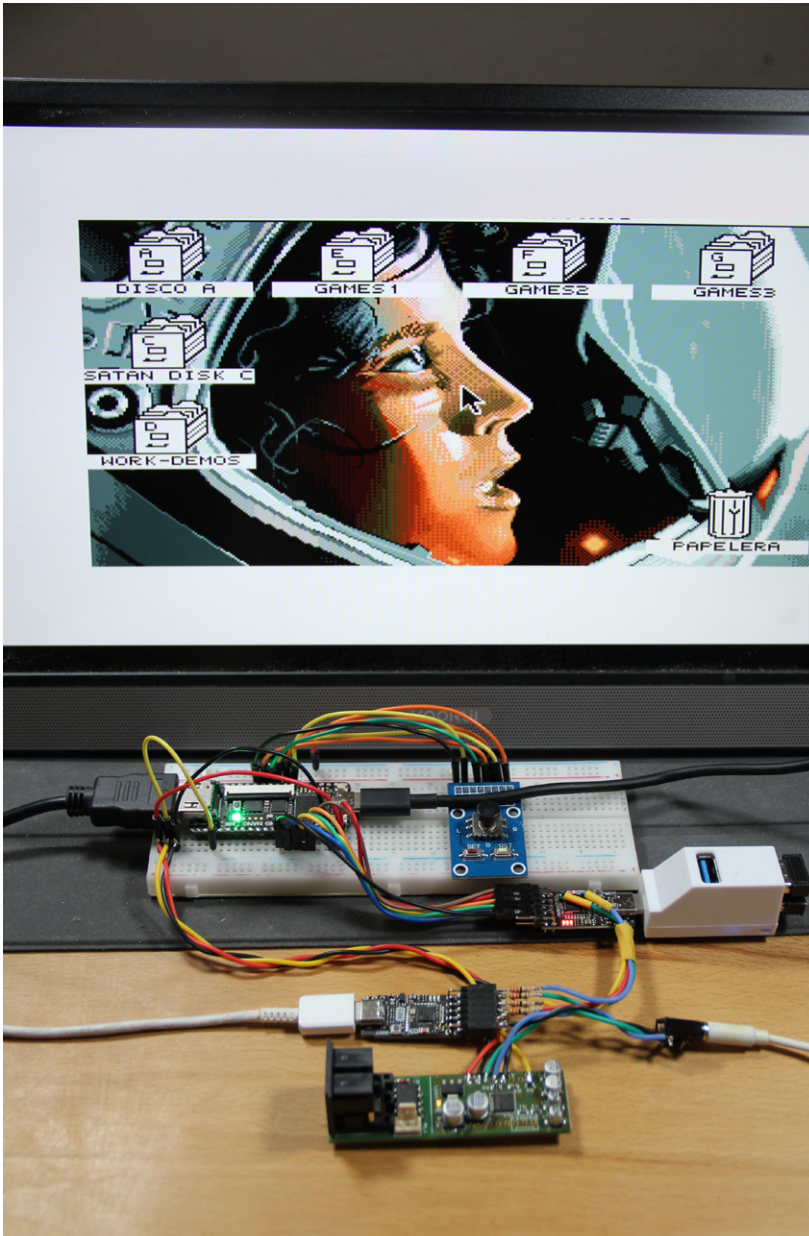
In het algemeen raden af cartridges te gebruiken van leveranciers die hun producten extreem goedkoop verkopen op Amazon of andere online aanbieders. Het interesseert ze in het algemeen niet of de informatie die ze geven correct is. Als er klachten komen over beschadigde printers, verdwijnen dergelijke leveranciers weer snel van de markt en bieden ze hun onbetrouwbare producten een paar dagen later onder een nieuwe naam weer aan. **ct**



www.ct.nl/softlink/2407136



Om ervoor te zorgen dat Teams ook het geluid van lokaal afgespeelde media naar de videoconferentie streamt, moet je de schakelaar 'Geluid opnemen' omzetten.



RETROGAMEN MET FPGA

Bouw een Atari ST na met een FPGA-board

Retrocomputers en gameconsoles die via hardware geëmuleerd zijn op FPGA-basis bieden een zeer authentieke game-ervaring. De hardware kost echter honderden euro's. We laten zien hoe dat werkt voor een Atari ST, tegen een fractie van de prijs.

Till Harbaum en Daniel Dupré

Ongeveer tien jaar geleden zag het MiST FPGA-board het daglicht. Ontwikkelaars gebruikten het om de 8-bit Nintendo Entertainment System (NES) gameconsole en de 16-bit Amiga-computer nauwkeurig hardwarematig te klonen, waaronder een replica van de Atari ST. Samen met zijn opvolger, de MiSTer-FPGA, maakte dat apparaat op FPGA gebaseerde retrocomputing populair. Dankzij de hogere prestaties kan de MiSTer zelfs PlayStation 1 3D-games draaien, net als de originele console.

Sindsdien is er herhaaldelijk gevraagd om een opvolger. De chipcrisis heeft echter ook de prijzen van FPGA's opgedreven, waardoor de vooruitzichten enige tijd lang vrij slecht waren. Een compleet MiST-systeem kost ongeveer 240 euro. Het MiSTer FPGA-board kost ongeveer 300 euro voor de minimale configuratie. Een reeds gemonteerd board in een behuizing dat ook voorzien is van extra interfaces (USB, VGA, ...) verdubbelt de prijs. De minder krachtige maar aanzienlijk goedkopere Tang Nano FPGA-boards van Sipeed zijn dan een betere optie: die zijn al vanaf 15 euro verkrijgbaar. We hebben gekeken in hoeverre ze geschikt zijn voor retrogaming.

FUNCTIONALITEIT

Field Programmable Gate Arrays (FPGA) hebben standaard geen vaste functie. Ze worden normaal gebruikt voor onderzoek en chipontwikkeling. Ze kunnen echter ook worden gebruikt om halfgeleiders van retrocomputers en gameconsoles in de vorm van cores in de FPGA-chip te simuleren. Daardoor gedraagt het board zich precies als bijvoorbeeld een echte Atari ST. Om dat te doen, verbinden ontwikkelaars de beschikbare logische poorten in de FPGA en wijzen ze functies toe zoals de cpu van de originele hardware.

In tegenstelling tot software-emulatie zijn de geheugenbenaderingen en timings bijna 'cycle exact' zoals bij de originele hardware, en is de invoer van controllers en de beelduitvoer praktisch direct, waardoor de spelervaring uiterst authentiek is.

PRESTATIES IN VERGELIJKING

De Tang Nano familie van Sipeed bestaat uit kleine printplaten in een breadboard-vriendelijk Arduino-formaat. De relatief goedkope FPGA-chips komen van het Chinese bedrijf GoWin. De eerste van die printplaten boden echter maar 1000 logische elementen en lagen daarmee ver achter op de 25.000 logische elementen van de MiST en de 110.000 elementen van de MiSTer FPGA. Om dat in perspectief te plaatsen: zelfs een voor huidige begrippen relatief zwakke 8-bit retromachine als de NES kan nauwelijks worden gerealiseerd met minder dan 5000 logische elementen. En voor de stap naar het 16-bit-tijdperk van de Super Nintendo (SNES) en Sega's Mega Drive zijn minstens 20.000 logische elementen nodig.

Na de Tang Nano-varianten 1K, 4K en 9K verscheen halverwege 2023 de 20K-variant op de markt. Dankzij de 9000 logische elementen van de 9K-versie heeft GitHub-ontwikkelaar nand2mario al een

NES-core kunnen ontwikkelen. Hij heeft zijn SNES-core in de 20K-versie geperst. Vanwege de beperkte SDRAM-grootte zullen echter niet alle games ermee werken. Een volledig ontwikkelde C64-core is al beschikbaar voor de 20K-versie (zie de link op de laatste pagina van dit artikel). Het 20K-board kost ongeveer 35 euro en beschikt naast de FPGA-chip over RAM- en ROM-geheugen. Bovendien heeft het een usb-poort voor het uploaden van je eigen cores, een HDMI-uitgang voor video- en geluidsuitvoer en een SD-kaartslot voor ROM- en diskette-images.

Het board voldoet dus aan alle eisen om een Atari ST- of Amiga-core te realiseren. De port van de Atari ST-core MiSTeryNano (voor download zie de link) gebruikt meer dan 90 procent van de 20.000 logische elementen van de FPGA en emuleert een volwaardige Atari ST. Een eenvoudige Amiga 500 is in dezelfde orde van grootte, maar zo'n core is er nog niet. Dat is waar de community om de hoek komt kijken. Als startpunt kunnen geïnteresseerden documentatie van de Amiga-core voor het MiSTer-project vinden op GitHub (zie de link). Programmeren is mogelijk met behulp van een Hardware Description Language (HDL) zoals Verilog.

De Atari ST-core is compatibel met bijna alle demo's en games van diskette-images en harde schijven. Er wordt momenteel nog gefinetuned en er wordt bijvoorbeeld gewerkt aan het reproduceren van de typische toegangsgeluiden bij het laden vanaf een diskette. Naast de Tango Nano 20K is de core ook geport naar het Tang Primer 25K en Tang Mega 138K FPGA-board.

BASIS VAN HARDWARE-KLONEN

Inmiddels zijn enkele computeronderdelen en chips bijna perfect omgezet in HDL. Bij sommige daarvan is er een complex proces aan voorafgegaan: tijdens het decappen wordt bijvoorbeeld de chipbehuizing opgelost in zuur en wordt de blootgelegde chip onder een krachtige microscoop gelegd en gefotografeerd. Door stapsgewijs verschillende chemicaliën toe te passen, worden de verschillende lagen van de chip die blootgelegd en wordt elke laag vervolgens in zogeheten die-shots vastgelegd. Als de beeldkwaliteit goed genoeg is, is het mogelijk de elektrische structuur van chips uit de foto's af te lezen en een exacte replica in HDL te formuleren. Op die manier is het bijvoorbeeld gelukt een bijna perfecte omzetting van de Motorola MC68000-cpu van de Atari ST te maken.

Inmiddels zijn er ook al delen van de Atari ST-chipset beschikbaar in een perfecte HDL-implementatie. De gegevens kwamen uit originele productie-documenten van de daadwerkelijke chips, die konden worden gereconstrueerd uit oude verzamelingen diskettes en harde schijven uit de bedrijfsomgeving van Atari. Vooral voor de Atari ST maken dergelijke 'cyclus-exacte' implementaties van de chips een aanzienlijk verschil om ervoor te zorgen dat het systeem nauwkeurig en foutloos draait.

Vindingrijke programmeurs, vooral uit de demo-scene, hebben destijds de grenzen van de Atari ST

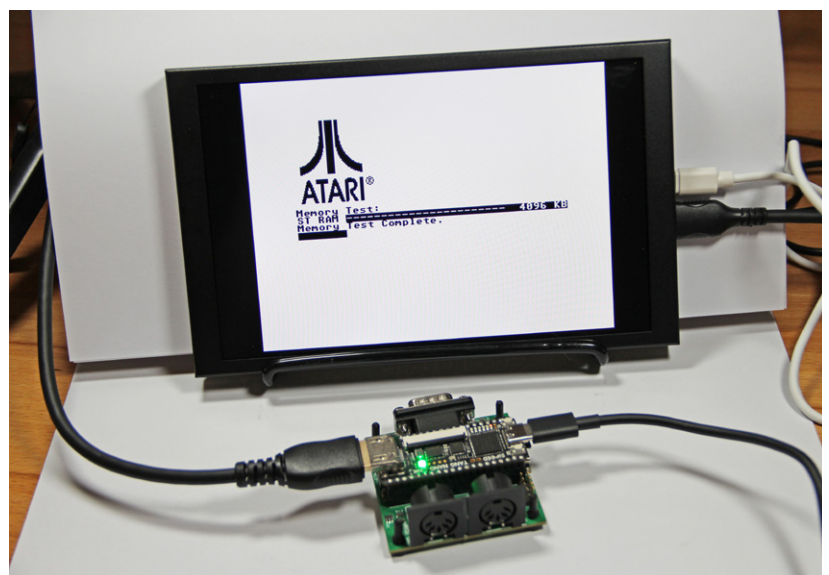
opgezocht door listig te programmeren. Het is ze op die manier gelukt om meer kleuren en een hogere resolutie te realiseren dan waar de hardware eigenlijk voor gemaakt was. Sommige van die trucs werken dankzij een op de nanoseconde-precieze uitvoering van bepaalde opdrachtreeksen. Alleen door de originele chips nauwkeurig te repliceren kunnen dergelijke listige programma's daadwerkelijk correct en zonder beeldstoringen worden uitgevoerd. Op MiST en MiSTer gebruikt de MiSTery-core die precieze chip-implementaties om een Atari ST te simuleren en de demo's foutloos af te spelen. Hier stellen we ons als doel om de MiSTery-implementatie over te zetten naar de Tang Nano 20K.

OP WEG NAAR DE ATARI ST

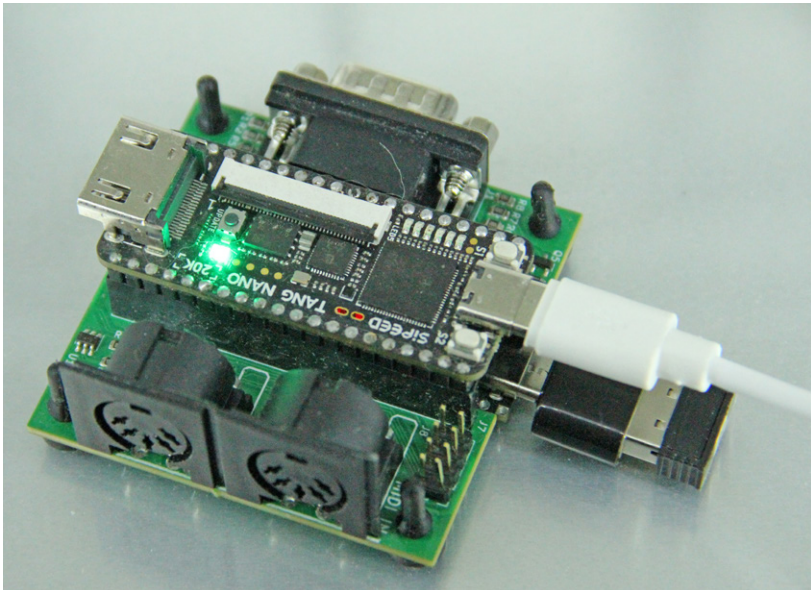
Je sluit het board via usb aan op een pc. Zoals bij een Arduino wordt de code naar het flashgeheugen geschreven. De eerste stappen met de Tang Nano 20K onder Linux zijn iets ingewikkeld. Omdat FPGA-boards nog niet ingeburgerd zijn, moet je daarvoor nieuwe wegen inslaan om de Atari ST-core aan de praat te krijgen.

Het is mogelijk om softwarevoorbeelden van de FPGA-fabrikant GoWin, bijvoorbeeld voor het uitvoeren van een testbeeld via HDMI, in de FPGA-ontwikkelomgeving GoWin IDE te genereren, maar de GoWin-software herkent het aangesloten board onder Linux niet en kan de code niet in de FPGA laden. Voor het programmeren van de Tang Nano 20k onder Linux heb je de FPGA-programmeertool openFPGA-loader project (zie de link) nodig.

Tot kort moest je het stellen zonder de GoWin Analogue Oscilloscope (GAO) tool, die een live weergave van de draaiende FPGA mogelijk maakt voor essentiële debugging. Sinds begin 2024 ondersteunt de GoWin IDE echter wel de Tang Nano 20K, zodat GAO nu ook onder Linux kan worden gebruikt. GAO is vergelijkbaar met Altera's debugtool Signaltap en de Integrated Logic Analyser van Xilinx.



Om het originele videosignaal van de gekloonde Atari ST weer te geven op een moderne flatscreen-tv of monitor, is wel een greep in de trukendoos nodig.



Handig: als je geen zin hebt om te solderen om hardware-uitbreidingen te maken, kun je je CAD-bestanden uploaden naar een online-service zoals JLCPCB en de uitbreiding volledig geassembleerd naar je toe laten sturen. Deze MIDI-adapter kost ongeveer 10 euro vanaf vijf stuks.

RAM EN ROM PROBLEMEN

Een speciaal kenmerk van de GW2AR FPGA-chip die op de Tang Nano 20K zit, is het 8 MB FPGA-interne SDRAM-geheugen. Dat is goed geschikt voor de thuiscomputers van het 16-bit tijdperk. Een Atari ST werd geleverd met maximaal 4 MB RAM.

Retro-thuiscomputers bewaren essentiële delen van hun besturingssysteem in het ROM. In de FPGA wordt het ROM-geheugen vaak gemodelleerd in het RAM. Om dat te doen, worden bij het opstarten van het systeem de vereiste gegevens automatisch van een sd-kaart geladen en wordt het geheugen tegen schrijven beveiligd zodat het zich vanaf dat moment gedraagt als ROM-geheugen.

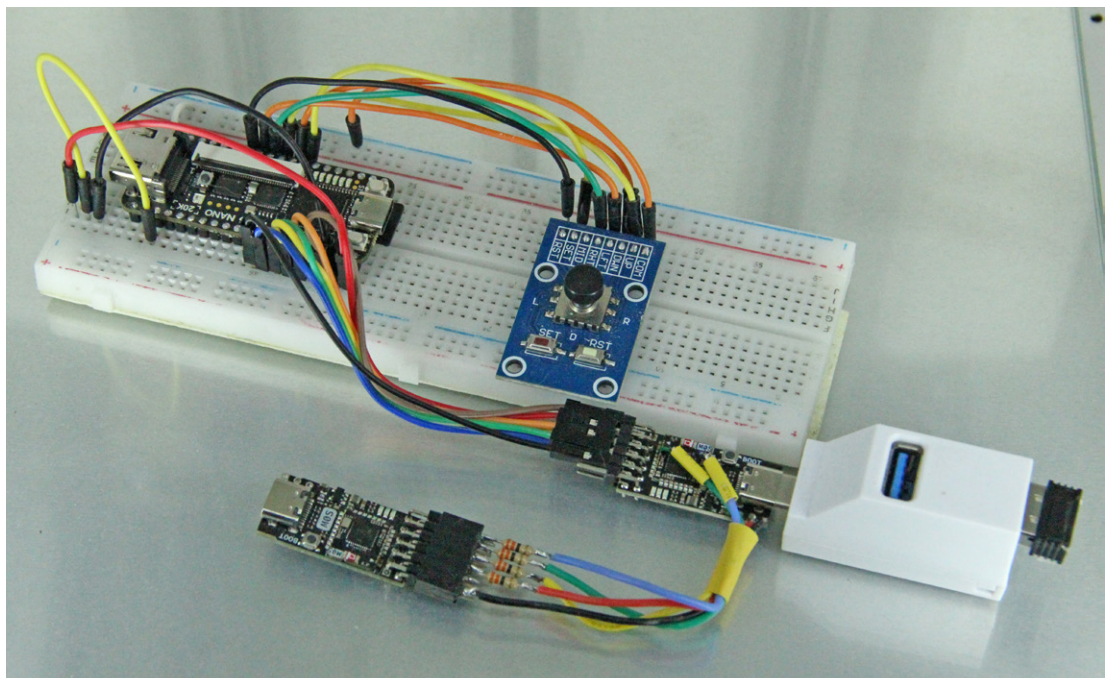
Maar er is een alternatief: de Tang Nano 20K beschikt ook over 8 MB serieel flashgeheugen, dat de FPGA bij het opstarten van het systeem initialiseert met de gegevens van de core. De FPGA-configuratie neemt minder dan 1 MB in beslag, dus er is meer dan 7 MB beschikbaar voor de core.

De Atari ST-core gebruikt 1 MB, om vier van de maximaal 256 kB grote The-Operating-System ROM-varianten (TOS-ROM) van het besturingssysteem onder te brengen. Het installeren van de ROM's werkt met dezelfde flashtools die je gebruikt om de eigenlijke FPGA-configuratie te installeren.

Het flashgeheugen van de Tang Nano is eigenlijk te langzaam voor Atari ST-standaarden. Daarom waren we in eerste instantie van plan om ervoor te zorgen dat bij het opstarten van het systeem de ROM-data gekopieerd zouden worden naar ongebruikt snel RAM-geheugen. Maar 'helaas' zijn de HDL-replica's van de Atari ST-chipset inmiddels echter zo perfect dat ze, net als de echte Atari ST, gebruik maken van het feit dat de cpu ongehinderd toegang heeft tot het ROM-geheugen, terwijl het moet coördineren met de video-uitgang bij benaderingen van het RAM.

Als je het ROM dan zou kopiëren naar het RAM, weet de chipset daar niets van af en geeft hij de cpu ongehinderd toegang tot wat eigenlijk het ROM zou moeten zijn. Het resultaat is dat in zeldzame gevallen de ROM-toegang die wordt omgeleid naar het RAM botst met de videotoeegang. Dan worden de verkeerde gegevens gelezen en crasht het systeem.

Uit de specificaties van het flashgeheugen bleek echter dat de toegang met verschillende optimalisaties kan worden versneld. De resulterende snelheidsverhoging is net voldoende voor de gespecificeerde ROM-toegang van een Atari ST en na het uitproberen waren er inderdaad geen crashes meer. De gegevens kunnen dus gewoon in het flash-ROM blijven en hoeven niet naar het snellere RAM-



De ontwikkelomgeving voor de Atari ST-core op een breadboard: links het FPGA-board Tango Nano 20K. Rechts is een mini-joystick bedraad. Rechts daaronder een MOS-dock met een usb-hub en ingeplugde draadloze ontvanger voor muis en toetsenbord. Het tweede MOS-dock in het onderste deel van de foto dient als debug-adaptor.

geheugen te worden gekopieerd. Dat resulteert in een leuk bijeffect: de volledige 8 MB RAM is beschikbaar voor de core. Geen enkele echte Atari ST beschikt over zoveel geheugen.

PROBLEMATISCHE VIDEO-UITVOER

Dankzij een bestaande codebase (zie de link) konden we via de HDMI-uitgang snel een videosignaal aan de praat krijgen, zij het in DVI-modus zonder geluid. Er is ook bestaande code op GitHub (zie de link) voor beeld- en geluidsuitvoer volgens de HDMI-standaard, die relatief eenvoudig aan te passen is. Daardoor lukte het zowel geluid als een videosignaal uit het FPGA-board te krijgen. Omdat veel retrocomputers en gameconsoles echter videomodi gebruiken die niet precies overeenkomen met de HDMI-standaard, is de juiste implementatie complex. Bij diverse tests bleef het scherm vaak zwart.

Om de Atari ST-core-videosignalen weer te geven met bijvoorbeeld 320×200 pixels in overeenstemming met de HDMI-specificaties, zou het beeldsignaal via een complex proces moeten worden omgezet. De kleine FPGA heeft daar echter niet de resources voor. Daarom hebben we voor een scan-doubler-aanpak gekozen. Die vrij eenvoudige verdubbeling van elke beeldlijn (320×400) zet de signalen om in een formaat dat dicht in de buurt komt van standaard HDMI-signalen en wordt daarom geaccepteerd door de meeste moderne monitoren en televisies. Zelfs als het videosignaal dat ermee wordt verwerkt niet volledig HDMI-compliant is, lukte het daarmee toch om een vertragsvrije en vloeiende weergave te realiseren. En dat maakt retrogaming dan erg leuk.

RANDAPPARATUUR

Naast de joysticks en gamepads hebben retro-computercores ook een muis en een toetsenbord nodig. Theoretisch kan de bestaande microcontroller

```

85 L
86 wire [5:0] leds; // control leds with positive logic
87 assign leds_n = ~leds;
88
89 wire sys_resetn;
90
91 // connect to ws2812 led
92 wire [23:0] ws2812_color;
93 ws2812 ws2812_inst (
94     clk(clk32),
95     color(ws2812_color),
96     data(ws2812)
97 );
98
99 // system values are set by the external MCU (by the user via the OSD)
100 // and used to control the system in general
101 wire [1:0] system_leds;
102 wire [1:0] system_chipset;
103 wire system_memory;
104 wire system_video;
105 wire [1:0] system_reset; // reset and coldboot flag
106 wire [1:0] system_scanlines;
107 wire [1:0] system_volume;
108 wire system_wide_screen;
109 wire [1:0] system_floppy_wprot;
110 wire system_cubase_em;
111 wire [1:0] system_port_mouse;
112 wire system_tos_slot;
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

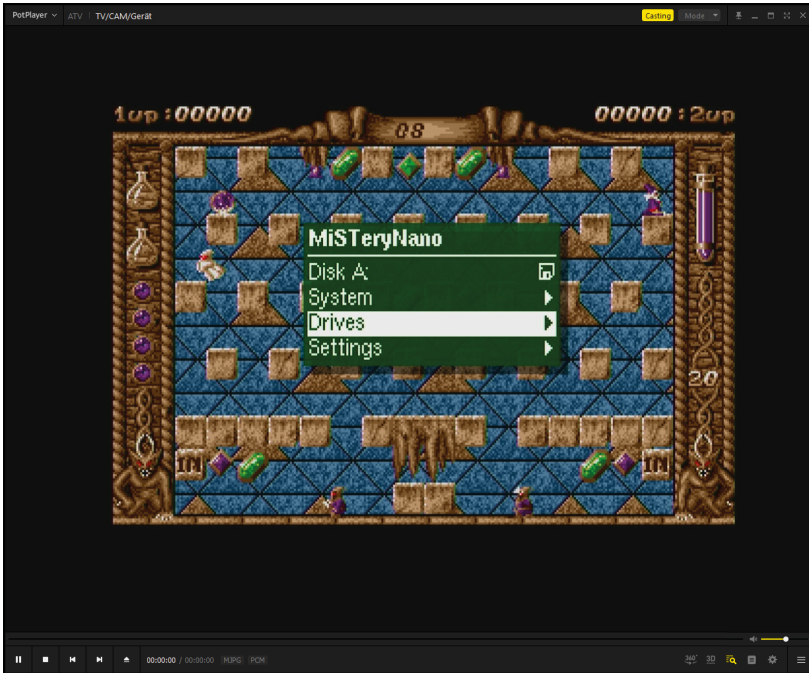
De Atari ST-core kan worden geprogrammeerd met de Hardware Description Language (HDL) Verilog.

van de Tang Nano 20K daarvoor worden gebruikt. De rekenkracht en het geheugen van deze 320 MHz RISC-V-cpu zijn daarvoor voldoende en met bluetooth, usb-host en wifi biedt hij ook de nodige interfaces.

Als je die weg bewandelt, verlies je echter de mogelijkheid om code van de pc naar de FPGA te kopiëren. Een andere optie is een extra microcontroller-board. Het M0S-dock, ook van Sipeed en te koop voor 5 euro, wordt via een jumperkabel verbonden met het FPGA-board en biedt aansluitmogelijkheden voor bijvoorbeeld een usb-muis en toetsenbord. Bovendien maakt het de bediening ook eenvoudiger door een schermdisplay te tonen over de huidige beeldinhoud. Je kunt die dan gebruiken om core-specifieke dingen zoals de RAM-grootte in te stellen of diskette-images van een sd-kaart te integreren.



Als je wilt, kun je met een beetje werk ook een uitbreidingsboard met een DE-9 connector voor originele Atari-joysticks maken.



Via het OSD-menu kun je onder andere images van diskettes selecteren om games te starten.

We hebben voor de Atari ST-core een kleine printkaart gemaakt die de thuiscomputerkloon voorziet van zijn beroemde MIDI-interfaces (zie de foto op de vorige pagina) om synthesizers via MIDI-commando's aan te sturen. In combinatie met de muzieksoftware Cubase werd de Atari ST vroeger in veel muziekstudio's gebruikt. De KiCAD-data die daarvoor nodig is, is ook op GitHub beschikbaar en kan relatief eenvoudig worden aangepast.

Als je dat toch teveel gedoe vindt, kun je de beschikbare productiegegevens gebruiken om voor relatief weinig geld kant-en-klare printplaten te bestellen via Aziatische printplaatfabrikanten zoals JLCPCB.

CONCLUSIE

Het Tang Nano 20K FPGA-board lost de belofte van het MiST-board in voor een veel lagere prijs en kan met relatief weinig moeite worden omgevormd tot

een volwaardige Atari ST en andere retrosystemen. Voor iets minder dan 40 euro heb je met de Tang Nano 20K en het MOS-dock alles wat je nodig hebt om retro-homecomputing nieuw leven in te blazen. Verdere ports, vooral van de Commodore Amiga, maar ook van verschillende andere 8-bit thuiscomputers, zijn ook beschikbaar.

MiST en MiSTer op GitHub bieden een breed scala aan volwassen oplossingen van verschillende ontwikkelaars, waarvan sommige met niet al teveel inspanning kunnen worden geport naar de Tang Nano 20K – en dat voor een klein budget. Bovendien is iedereen die geïnteresseerd is welkom om bij te dragen op GitHub.

De inspanning is zeker de moeite waard: in directe vergelijking met software-emulatie, vooral op een relatief zwakke Raspberry Pi Zero 2, scoort de FPGA-aanpak met meer overtuigende nauwkeurigheid en prestaties. In tegenstelling tot software-emulatie storen er geen processen van het besturingssysteem en hoeft het afspelen van audio en video niet via stuurprogramma's te verlopen – de originele hardware die in de FPGA is gemodelleerd, kan direct worden aangesproken zonder omwegen. De FPGA-typische precisie garandeert dus een uiterst authentieke en latencievrije retro-game-ervaring.

Vergeleken met software-emulatie is het installeren en configureren echter complexer en zijn er momenteel slechts relatief weinig cores beschikbaar voor het goedkope FPGA-board. Bovendien zijn de prestaties van de Tang Nano 20K beperkt en kunnen bijvoorbeeld de SNES en Mega Drive er niet volledig mee worden gerealiseerd.

Met de Tang Primer 25K heeft Sipeed onlangs een board op de markt gebracht met een FPGA met 25.000 logische elementen. Dat board zou met die elementen voldoende moeten zijn voor deze consoles, maar hij kost meer dan 50 euro als hij volledig is uitgerust. De Tang Mega 138K overtreft zelfs de grote FPGA van de MiSTer en kan met het optionele ingebouwde scherm ook worden gebruikt als handheld-console. Met meer dan 200 euro is hij echter ook aanzienlijk duurder.



Atari-ST-core starten op Tang Nano 20K

Om redenen van ruimte is dit slechts een korte versie van hoe je de Atari ST-core onder Windows kunt kopiëren naar het FPGA-board Tang Nano 20K, de muis en het toetsenbord kunt aansluiten via het MOS-dock en games kunt starten via diskette-images vanaf een sd-kaart.

De lange versie van dit verhaal en alle benodigde tools zijn te vinden op de GitHub-pagina van het MiSTeryNano-project

(zie de link linksonder op deze pagina).

Sluit het FPGA-board aan op een Windows-pc via usb. Gebruik de GoWin-programmeer-software om het besturings-systeem (TOS-ROM) te flashen naar adres 0x100000 van het flashgeheugen. Laad vervolgens de actuele MiSTeryNanoCare in het flashgeheugen en zet de usb-firmware over naar het MOS-dock. Sluit het FPGA-board aan

op het dock via een jumperkabel zoals beschreven op de projectwebsite. Plaats een sd-kaart met diskette-images van games in het slot van het FPGA-board. Sluit vervolgens een monitor aan via HDMI. Het bureaublad van de Atari ST zou dan op het scherm moeten verschijnen. Om diskette-images te integreren en te starten, druk je op de F12-toets op het toetsenbord. Veel plezier met het retrogamen!



www.ct.nl/softlink/2407140



Klantenservice

Wil je abonnee worden of heb je vragen over je abonnement? Op onze website vind je antwoord op de meeste vragen.



www.ct.nl/contact

Wist je dat je tegenwoordig eenvoudig zelf je adres kan wijzigen? Ga naar www.ct.nl/adreswijzigen om je nieuwe adres door te geven. Het nieuwe adres wordt vervolgens automatisch in ons systeem gewijzigd.

Telefoon

We zijn er maandag tot en met vrijdag van 09.00 tot 17.00 uur om je vragen te beantwoorden.
+31 (0)24-2027 825

E-mail

Stel je vraag per e-mail aan een van onze servicemedewerkers.
klantenservice@ct.nl

ABONNEMENTSINFORMATIE c't magazine kost € 8,99 per nummer. De abonnementsprijs is in Nederland € 79,00 en in België € 82,50 (10 nummers). Deze prijs geldt bij betaling per automatische incasso. Voor betaling via een (digitale) factuur geldt een toeslag van € 2,50. Je kunt eenvoudig een machtiging afgeven via www.magazineshop.nl/machtigen. Abonnementen worden automatisch verlengd, tenzij anders vermeld. Het opzeggen van een abonnement kan eenvoudig telefonisch via +31 (0)24 2027825 of per mail via klantenservice@ct.nl.

ct IT-magazine
voor de
liefhebber

c't is een uitgave van F&L Media B.V.

in licentie van Heise Medien GmbH & Co. KG, Hannover

Hoofdredacteur Noud van Krusbergen

Redactie Daniel Dupré, Elwin Hodžić, Alieke van Sommeren, Marco den Teuling

Met medewerking van

Ernst Ahlers, Merel Atia, Johannes Börnsen, Thomas Brandstetter, Anke Brandt, Niklas Dierking, Mirko Dölle, Liane M. Dubowy, Ronald Eikenberg, Till Harbaum, Christian Hirsch, Benjamin Kraft, Ulrike Kuhlmann, Lutz Labs, Jan Mahn, Pina Merkert, Andrijan Möcker, Rudolf Opitz, Benjamin Pfister, Hajo Schulz, Peter Siering, Carsten Spille, Carsten Strotmann, Axel Vahldiek, Christof Windeck, Stefan Wischner, Dušan Živadinović

Art Direction Nick Groenewold

Vormgeving Mylene Nales, Tom Gerrits, Lisanne Cobussen, Susan Gerbrands-Derksen, Ferry Dorresteijn en Ellen Willemsen

Sales Thijs de Hoogh +31 (0)24 2404641
tdhoogh@fnl.nl

Marketing José Snel jsnel@fnl.nl

Drukkerij Senefelder Misset Doetinchem B.V.

Vragen aan de redactie

Heb jij opmerkingen, suggesties of vragen aan de redactie? redactie@ct.nl

Nieuwsredactie / Pers

redactie@ct.nl of het onderstaande adres o.v.v. F&L Media / redactie c't
Jonkerbosplein 52, 6534 AB Nijmegen

F&L Media



COPYRIGHT Het auteursrecht op deze uitgave en de gedrukte uitgave en op de daarin verschenen artikelen wordt door de uitgever voorbehouden. De vertaalrechten berusten bij F&L Media B.V. te Nijmegen/ Nederland. Het verlenen van toestemming tot publicatie in de gedrukte uitgave houdt in dat de auteur de uitgever, met uitsluiting van ieder ander onherroepelijk machtigt de bij of krachtens de auteurswet door derden verschuldigde vergoedingen voor kopiëren te innen en dat de auteur alle rechten overdraagt aan de uitgever, tenzij anders bepaald. Niets uit deze uitgave en de gedrukte uitgave mag worden overgenomen, vermenigvuldigd of gekopieerd zonder uitdrukkelijke schriftelijke toestemming van de uitgever. De uitgever stelt zich niet aansprakelijk voor eventuele onjuistheden, welke in deze uitgave of de gedrukte uitgave mochten voorkomen.

In de volgende c't

Nummer 8-9 ligt op 16 juli thuis bij de abonnees

OVERSTAPPEN OP LINUX

Microsoft weigert het om veel computers die op Windows 10 draaien te upgraden naar Windows 11 – een goede reden om over te stappen op Linux. We kijken naar Linux Mint en Fedora Workstation, twee op zich zeer verschillende maar solide distributies. En we leggen uit hoe je de overstap kunt maken.



GAMING-LAPTOPS MET GEFORCE RTX 4070

Als je wilt genieten van 3D-games met veel details en van het scherm spatende effecten, kom je met de geïntegreerde grafische eenheden van veel laptops niet echt ver en heb je meer grafische kracht nodig. We hebben een aantal 16-inch gaminglaptops met GeForce RTX 4070 getest.

BOVENDIEN

PIMP WEBSITES MET AI

Met behulp van AI kun je websites van anderen naar wens aanpassen: nieuwe functies toevoegen, vervelende elementen verwijderen, het ontwerp verfraaien en nog veel meer. Je formuleert gewoon wat je wil en kort daarna spuugt de AI een geschikt browserscript uit.

DE GEVAREN VAN DE AI ACT

Na lang getouwtrek is de Europese AI-wet erdoor gekomen. Die AI-wet opent echter een achterdeur voor biometrische massasurveillance. Een dergelijk gebruik brengt door wiskundige en statistische wetmatigheden onredelijk hoge risico's met zich mee.

STARTVERBOD VOOR ALLE WINDOWS-BOOTLOADERS

Microsoft wilde het vertrouwen van enkele honderden Windows-bootloaders opzeggen door beveiligingsproblemen in UEFI Secure Boot, maar dat is niet langer van toepassing. Nu worden echter alle Windows-bootloaders geblokkeerd – of ze onveilig zijn of niet.



Alles over Artificiële Intelligentie online en in de winkel



Windows Praktijkhandboek online en in de winkel

Meer lezen?

Voor het laatste nieuws op ICT-gebied, extra reviews, achtergronden en IT-vacatures kun je terecht op onze website: www.ct.nl



 [linkedin.com/company/ctmagazine](https://www.linkedin.com/company/ctmagazine)

 **c't – IT-magazine voor de liefhebber**

 lezersvragen@ct.nl

Mis geen nummer meer!

Neem nu een abonnement en krijg voortaan elke uitgave van c't automatisch in je brievenbus én digitaal.

Ga naar www.ct.nl/abo

of bel gratis naar +31 (0)24 2027 825

 **IT-magazine voor de liefhebber**

Liquid Cooling

Superior Effectiveness of Liquid Cooling with Proven Deployments at Scale for Direct-to-Chip, RDHx, and Immersive Cooling Solutions



Cooling Capacity



H₂O
has
1000X
more
cooling capacity
than **Air**



Thermal Conductivity

Water
is
25X
Better
at transferring

Heat



Transport Energy

Water
requires
10X Less
Energy

to move **Heat**



SMBE Belgium

+32 495 533 245
www.smbe.be
sales@smbe.be

TWP Computer

+31 20 638 9057
www.twp.nl
info@twp.nl

Server Storage Solution

+32 9 261 5310
www.s3s.be
sales@s3s.be

NCS International

+31 544 47 0000
www.ncs.nl
info@ncs.nl

ServerDirect BV

+31(0) 85-3018585
www.ServerDirect.nl
sales@serverdirect.nl



Learn More at www.supermicro.com

© Supermicro and Supermicro logo are trademarks of Super Micro Computer, Inc. in the U.S. and/or other countries.



Copilot+ PC

A new AI era begins

ASUS

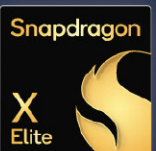


ASUS Vivobook S 15 S5507

Your First ASUS Copilot+ PC

Meet your first ASUS Copilot+ PC – the ASUS Vivobook S 15, a sleek AI-powered laptop designed for smart users. With the efficient power of its Qualcomm® Snapdragon® X Elite Processor, enjoy up to 18 hours of seamless productivity. The 3K 120 Hz ultra-large OLED display and immersive audio system are encased in a premium all-metal 1.47 cm-thin, 1.42 kg-light body for effortless mobility. Featuring a mood-setting single-zone RGB keyboard, with a dedicated Copilot key for instant AI assistance, revolutionize your work and play. Welcome to an innovative and elegant future, where AI brings you to the forefront, with no compromises.

Powered by



* Snapdragon and Qualcomm branded products are products of Qualcomm Technologies, Inc. and/or its subsidiaries.
* Product weight and specification may vary according to device configuration.