Configuratie van een internetserver

Robert La Lau

Ik leg het nog één keer uit...

Boom beroepsonderwijs · Meppel · 2020

Boom beroepsonderwijs
info@boomberoepsonderwijs.nl
www.boomberoepsonderwijs.nl

Auteur: Robert La Lau
Redactie en opmaak: Henk Pel
Titel: Configuratie van een internetserver
ISBN 978 90 372 5751 9
Eerste druk / eerste oplage

Inhoud

1 Inleiding en voorbereiding

Er zijn diverse redenen te bedenken waarom men (bedrijf of particulier) de hosting van diensten als websites en e-mail in eigen hand zou willen nemen. Er zijn evenveel redenen te bedenken waarom men dat niet zou willen.

De belangrijkste redenen om de hosting in eigen hand te houden, zijn **privacy** en **controle**. Het kan bijvoorbeeld onwenselijk zijn de zakelijke communicatie (e-mail, online helpdesk) onder te brengen bij een externe partij; ook het opslaan van klantgegevens kan een reden zijn om voor een zelf-beheerde oplossing te kiezen. Wanneer de server maatwerksoftware moet draaien, is het soms zelfs onmogelijk (of extreem prijzig) om dit bij een externe partij onder te brengen.

De belangrijkste redenen om de hosting uit te besteden, zijn **kennis** en **tijd**; beide zijn vereist voor het up-to-date houden, monitoren en back-uppen van een server. Over de beschikbare tijd voor het beheren van een server zal ieder voor zich moeten beslissen. Dit boek zal in ieder geval proberen de kennis op het vereiste niveau te brengen, en de systeembeheerder van een goed startpunt te voorzien, door deze te begeleiden bij de initiële configuratie van de server; ook zal de systeembeheerder worden voorzien van handvatten voor het vinden van aanvullende informatie.

Dit boek neemt de lezer mee van een *vanilla*-server – een server waarop alleen een besturingssysteem is geïnstalleerd, zonder verdere aanpassingen, zoals deze bijvoorbeeld door een hostingprovider wordt geleverd – naar een volledig functionele internetserver die klaar is om in bedrijf genomen te worden. De uiteindelijke server zal alle diensten leveren die verwacht mogen worden van een internetserver (DNS, mailhosting, webhosting enzovoort). Deze server is adequaat beveiligd en de systeembeheerder beschikt over de kennis die nodig is om het systeem bij te werken en te monitoren, en om backups te maken en terug te plaatsen.

1.1 Addendum

Een online addendum bij dit boek, met voorbeelden van configuratiebestanden en scripts, en links naar aanvullende informatie, is voor iedereen vrij toegankelijk op *www.librobert.net/boek/internet/addendum.*

1.2 Vrije software

Alle in dit boek beschreven software is zogenaamde *vrije software*. Dit houdt in dat voor alle software de broncode vrij beschikbaar is, en eventueel door de gebruiker gecontroleerd en zelfs aangepast zou kunnen worden vóór installatie. Velen, waaronder de auteur van dit boek, zijn ervan overtuigd dat deze openheid de efficiëntie en veilig-

heid van software ten goede komen, omdat bugs en lekken sneller gevonden, en dus ook sneller gerepareerd en gedicht zullen worden.

Hoewel *vrije software* niet per definitie betekent dat de software ook gratis beschikbaar is, is dat in het geval van de in dit boek beschreven software wel het geval. Uiteraard betekent dit niet dat donaties aan deze projecten niet op prijs gesteld worden: het overgrote deel van de ontwikkelaars van vrije software doet dit in de vrije tijd, en donaties worden niet alleen gebruikt om ontwikkelaars te helpen meer tijd aan hun project te besteden, maar ook om te betalen voor infrastructuur zoals testcomputers, webhosting enzovoort; een donatie kan helpen garanderen dat de ontwikkeling van de software die u gebruikt, kan voortbestaan op het huidige of een hoger niveau.

Vrije-softwareprojecten kunnen overigens ook vaak versterking gebruiken – niet alleen ontwikkelaars, maar ook gebruikersinterface-deskundigen, vormgevers, vertalers, schrijvers van documentatie en webcontent, systeembeheerders, moderatoren voor internetfora enzovoort.

1.3 Benodigde kennis en ervaring

Voor het volgen van de instructies in dit boek is geen uitgebreide kennis nodig van Unix. Wel is het wenselijk dat de lezer een eerste geslaagde kennismaking heeft gehad met Unix, en bekend is met concepten als de opdrachtregelinterface (*command line*) en de configuratie middels tekstbestanden, alsook met de globale directorystructuur van deze systemen. Op de werking van het besturingssysteem zelf wordt slechts beknopt ingegaan, en de lezer wordt geacht bekend te zijn met basiscommando's als **`cd`**, **`ls`**, **`cat`**, **`less`** en **`tar`**.

Aangezien het een *headless* server betreft (een server zonder monitor, toetsenbord en muis), en geen pc of werkstation, zal er geen grafische gebruikersomgeving worden geïnstalleerd.

Ik heb mijn best gedaan dit boek, zowel qua taalgebruik als qua inhoud, begrijpelijk en interessant te laten zijn voor zowel de beginnende als de meer gevorderde systeembeheerder.

Benodigde tijd en motivatie

Na het lezen van dit boek en het volgen van de instructies beschikt de lezer over een werkende internetserver. Hiermee is het werk echter niet gedaan. Elke computer behoeft monitoring en onderhoud, en voor een direct op het internet aangesloten server geldt dat meer dan voor enige andere computer. Er zal geprobeerd worden om ongeoorloofd toegang te krijgen tot de server, en het is de taak van de systeembeheerder alles in het werk te stellen de vertrouwelijkheid van de gegevens op de server te waarborgen, en te voorkomen dat de server ingezet wordt voor doeleinden waarvoor hij niet bedoeld is.

Dit boek beschrijft hoe de geïnstalleerde software up-to-date gehouden kan worden, en ook wordt een aantal tips gegeven voor de monitoring van het systeem. Al deze aanwijzingen zijn echter nagenoeg nutteloos zonder de twee belangrijkste gereedschappen van de systeembeheerder: tijd en motivatie. Het bedrijf moet ervan doordrongen zijn

dat systeembeheer geen bezigheid is die men er even bij doet; er moet structureel tijd voor ingeruimd worden, om te voorkomen dat het onderhoud op achterstand raakt en de server kwetsbaar wordt. De systeembeheerder moet zich ervan bewust zijn dat hij of zij niet altijd om 5 uur 's middags de deur achter zich dicht kan trekken; als er, bijvoorbeeld, een probleem is met de e-mail, is het zaak dat dat uiterlijk de volgende ochtend bij het begin van de werkdag is opgelost.

Ik adviseer om, na installatie en initiële configuratie, een halve werkdag per week structureel in te plannen voor het onderhoud van de server. Op een ander moment in de week kan er dan nog een uur ingepland worden voor een vlugge controle (bijvoorbeeld op vrijdag een hele ochtend voor het echte onderhoud, en dinsdagochtend een uur voor de nodige controles).

Uiteraard is de werkelijk benodigde tijd enigszins afhankelijk van het gebruik van de server. Met de hier beschreven configuratie kunnen zonder probleem tientallen websites geserveerd worden, en de e-mail afgehandeld van honderden gebruikers. In dergelijke gevallen is de kans groot dat er meer tijd nodig zal zijn. Wanneer de server daarentegen gebruikt wordt voor een enkele kleine website en de e-mail van twee of drie gebruikers, neemt het onderhoud uiteindelijk misschien niet meer tijd in beslag dan een halve werkdag per twee weken.

Maar een halve werkdag per week is een goede vuistregel voor de tijd die nodig is voor het controleren van de logbestanden, het finetunen van het systeem, het bijwerken van de software, het vergroten van de kennis en eventueel het beantwoorden van vragen van gebruikers.

Uiteraard moet in geval van nood, zoals een crash of een inbraak, de systeembeheerder *stante pede* vrijgemaakt kunnen worden voor ad-hoc-werkzaamheden.

Als bij voorbaat al duidelijk is dat deze tijd niet ingeruimd kan worden, is het waarschijnlijk beter om het onderhoud van de server aan de provider uit te besteden.

Oefenopdrachten

Om de gebruiker van deze uitgave praktisch te laten oefenen zijn per hoofdstuk opdrachten toegevoegd.

1.4 Extern account voor mail en schijfruimte

Het is aan te raden om voor de systeembeheerder (of voor het team van systeembeheerders) een extern e-mailaccount in te stellen. Wanneer een probleem optreedt dat verhindert dat de eigen server gebruikt kan worden voor e-mailafhandeling, kan dit account gebruikt worden voor communicatie met externe partijen.

Mail-accounts worden bovendien vaak geleverd met een stukje schijfruimte, dat eventueel gebruikt kan worden om gegevens op te slaan buiten de eigen infrastructuur. Hierbij kan gedacht worden aan belangrijke wachtwoorden, contactadressen enzovoort. Uiteraard dienen extern opgeslagen bestanden versleuteld te worden, en niet met een op de server opgeslagen sleutel; `zip` en `OpenDocument` kunnen beide versleuteld worden met een wachtwoord. Dit wachtwoord dient op papier bewaard te worden, zodat het bestand toegankelijk is, ook wanneer de eigen infrastructuur dat niet is.

Het is belangrijk dat partijen als de provider en het datacenter dit e-mailadres kennen en in het dossier hebben, zodat in geval van nood de communicatie direct opgepakt kan worden via dit adres, zonder dat kunstgrepen nodig zijn om deze partijen ervan te overtuigen dat dit inderdaad een geautoriseerd adres is.

Dit e-mailaccount dient ingesteld te worden om alle ontvangen e-mails ook door te sturen naar het 'normale' e-mailadres van de beheerafdeling, zodat nooit mails verloren gaan; het externe adres zal in de praktijk immers niet dagelijks gecontroleerd worden.

Aangezien dit account veelal gebruikt zal worden voor vertrouwelijke informatie, en de privacy-regelgeving in Europa strikter is dan elders, kan het wenselijk zijn een Europese provider te kiezen voor dit account. Het online addendum bij dit boek bevat een lijst met enkele voorbeelden van geschikte e-mailproviders.

Bij het vertrek van een systeembeheerder dient **altijd** het wachtwoord van dit account gewijzigd te worden.

1.5 Systeem en provider

Zowel de keuze van een systeem als de keuze van een hostingprovider zijn afhankelijk van veel factoren, waarvan een groot deel persoonlijke eisen, wensen en voorkeuren zijn. Het is dan ook niet mogelijk om een blauwdruk te geven voor de keuze van deze zaken.

Hieronder volgen enkele richtlijnen en handvatten die gebruikt kunnen worden bij het maken van deze keuzes.

Hardware

Eén van de eerste keuzes die gemaakt moeten worden bij de aanschaf van een server, is de keuze voor de te gebruiken hardware. Aan welke specificaties moet de server voldoen? Wordt het een fysieke server of een virtuele machine?

Een fysieke server of een virtuele machine?

Voordat de voor- en nadelen van fysieke servers en virtuele machines vergeleken worden, is het goed om een definitie van beide apparaten te geven.

Een fysieke server is een combinatie van hardware (moederbord, processor, geheugen enzovoort) en software (het besturingssysteem en de toepassingen). De server is aan een enkele klant toegewezen, en de beheerder of het team beheerders dat de server onder de hoede heeft, beheert de volledige server en heeft de volledige controle over die server.

Een virtuele machine bestaat alleen uit software: de 'hardware' voor de server is gevirtualiseerd en meerdere virtuele machines delen de fysieke hardware waarop de server draait. Deze fysieke hardware kan een enkele machine zijn, of een cluster machines; een zogenoemde *hypervisor* zorgt vervolgens dat de capaciteiten van de fysieke hardware worden verdeeld over de virtuele machines die erop draaien, volgens de specificaties van de beheerder van de fysieke hardware. De beheerder van de virtuele machine beheert alleen de aan hem of haar toegewezen virtuele machine(s), binnen de door de beheerder van de *hypervisor* gestelde limieten.

De virtuele machines worden ook wel *guest* (*gast*) genoemd en de hypervisor ook wel *host* (*gastheer*).

De grootste voordelen die een fysieke server biedt ten opzichte van een virtuele machine zijn de volledige privacy en controle: na de overdracht van de server, en het wijzigen van de aanwezige wachtwoorden, bepaalt de beheerder van de server wie er toegang heeft en wie niet.

Dankzij tools als *libguestfs* kan de beheerder van een hypervisor altijd toegang krijgen tot de virtuele machines onder zijn of haar hoede. Uiteraard is hiermee niet gezegd dat deze dit ook zal doen, maar de mogelijkheid moet in de overwegingen worden meegenomen, zeker als de vertrouwelijkheid van de gegevens op de server een grote rol speelt.

Wanneer de vertrouwelijkheid een minder prominente rol speelt, of de garanties van de provider voldoende vertrouwen bieden, kan deze toegankelijkheid ook een voordeel zijn: het maken en terugzetten van back-ups kan dan uitbesteed worden aan de provider, wat de systeembeheerder een hoop werk kan besparen.

Een ander voordeel van virtuele machines is het gemak waarmee ze opgeschaald en gerepareerd kunnen worden. Wanneer bijvoorbeeld het geheugen van een fysieke server het begeeft, zal de machine over het algemeen uitgezet moeten worden om het geheugen te vervangen. Wanneer de capaciteiten van een fysieke server niet langer volstaan, zal een nieuwe server samengesteld, geïnstalleerd en geconfigureerd moeten worden, om vervolgens de data van de oude naar de nieuwe server te kopiëren. Aangezien bij een virtuele machine de hardware gevirtualiseerd is, kan de beheerder van de hypervisor eenvoudig geheugen of schijfruimte toevoegen, of de processor opschalen, door de instellingen van de software aan te passen. En in het ergste geval kan de virtuele machine verplaatst worden naar een andere hypervisor, waarmee de *downtime* (onbruikbaarheid/onbereikbaarheid) beperkt wordt tot minuten.

Tot slot kan de prijs van een virtuele machine aantrekkelijker zijn dan die van een fysieke server. Enerzijds delen virtuele machines hun hardware, en hoewel over het algemeen de specificaties voor een server voor meerdere virtuele machines zwaarder zullen zijn dan die voor een enkele fysieke server, zullen de specificaties voor hardware voor tien virtuele machines zeker niet tien keer die van een fysieke machine zijn. En anderzijds kan, vanwege de eenvoudige opschaalbaarheid, met een virtuele machine voorzichtiger ingestapt worden, terwijl een fysieke server meestal met wat overcapaciteit aangeschaft zal worden, om groei op te kunnen vangen.

Wel moet hierbij opgemerkt worden dat de prijzen van fysieke servers momenteel dalen; dit is waarschijnlijk het gevolg van de marktwerking die veroorzaakt wordt door het feit dat meer en meer bedrijven overstappen naar virtuele hosting.

Minimale specificaties

Uiteraard is het onmogelijk te zeggen wat de minimale specificaties zijn voor een internetserver. Dit is sterk afhankelijk van het gebruik: een server die enorme hoeveelheden website-bezoekers en/of e-mails verwerkt, heeft andere specificaties dan een server die de e-mail verwerkt voor een bedrijf met vijf medewerkers en een enkele website host voor enige tientallen bezoekers per dag.

Algemeen kan in ieder geval gesteld worden dat de eisen vaak minder zwaar zijn dan men zou denken. Het is verleidelijk om bij de provider de krachtigste server uit de lijst te bestellen, en wanneer het budget dat toelaat kan dat zeker geen kwaad, maar nodig is dat over het algemeen niet.

Uitgaande van een server zoals beschreven in dit boek – DNS, e-mail, websites, adresboeken, kalenders en gedeelde bestanden, plus monitoring en back-up – voor een bedrijf met enige tientallen of honderd werknemers, en een paar websites met een paar duizend bezoekers per dag, moet een quadcore machine met 8 GB geheugen prima voldoen. Aangezien schijfruimte niet heel duur is, hoeft hierop niet beknibbeld te worden, maar het is goed om te bedenken dat een website meestal niet extreem veel ruimte in beslag neemt; de benodigde ruimte neemt uiteraard wel toe als veel bestanden gedeeld worden door de werknemers.

Het behoeft niet veel argumentatie dat wanneer het een server voor een gezin of familie betreft, waarop enkele tientallen mails per dag afgehandeld worden, één of twee websites draaien met hooguit enkele tientallen bezoekers per dag, en vijf tot tien personen hun mobiele telefoons synchroniseren, de goedkoopste server uit de lijst gekozen kan worden.

Besturingssysteem

De meeste systeembeheerders, waaronder de auteur van dit boek, zijn het erover eens dat Unix-systemen de geschiktste besturingssystemen zijn voor servers: ruim 70% van alle internetservers wordt bestuurd door een Unix-systeem, waarvan tenminste de helft door Linux; hieronder zijn ook de servers van Google, Facebook, Twitter en Amazon. Daarbij draaien overigens ook het International Space Station, de Large Hadron Collider, de *ground stations* van NASA en SpaceX, en de Amerikaanse nucleaire onderzeevloot op Linux.

Linux-varianten worden *distributies* of kortweg *distro's* genoemd.

Om een groot deel van het aanbod te beschrijven, en op deze manier de lezer/systeembeheerder zo vrij mogelijk te laten in zijn of haar keuze, beschrijft dit boek drie verschillende Unix-varianten:

- **FreeBSD**
  Dit is een BSD (geen Linux), en dus familie van OpenBSD, NetBSD en DragonFly BSD.
  De bij het schrijven van dit boek gebruikte versie is FreeBSD 12.0-RELEASE.
- **Debian**
  Met een eerste release in 1993 is dit een van de oudste Linux-distributies. Debian was de basis voor veel andere distro's, waaronder Knoppix, Ubuntu, Linux Mint, Kali Linux en Whonix.
  Bij het schrijven van dit boek is gebruikgemaakt van Debian 9 (Stretch).
- **CentOS**
  Deze distro is gebaseerd op Red Hat Enterprise Linux, en is daarmee onder andere familie van Fedora, CloudLinux en Oracle Linux.
  De versie die is gebruikt bij het schrijven van dit boek is CentOS 7.

Hoewel er nog vele andere varianten bestaan, en deze allemaal hun voors en tegens hebben, moet er ergens een grens gesteld worden aan het aantal dat behandeld wordt. Met deze drie systemen wordt een groot deel van het spectrum behandeld, en de sys-

teembeheerder die verder gaat, zal zonder twijfel in de loop van de tijd zijn of haar eigen voorkeur ontwikkelen, op basis van zijn of haar wensen, eisen en ervaringen. (Voor wie er belang in stelt: de auteur van dit boek prefereert FreeBSD op de server, en Gentoo Linux op de desktop.)

De kans is groot dat de systeembeheerder die dit boek leest zelf ook al een voorkeur heeft, dan wel uit ervaring, dan wel van horen zeggen. Indien dit niet het geval is, zijn de genoemde drie opties alle even valide, en zou de keuze eventueel gemaakt kunnen worden door een spelletje kop-of-munt; het leren moet ergens beginnen, en de systeembeheerder die nog een carrière voor zich heeft, krijgt zonder twijfel met alle drie deze Unix-families te maken.

Dit boek gaat bij aanvang uit van een server zoals deze geleverd wordt door een *co-locatie-provider*: het besturingssysteem geïnstalleerd, het netwerk geconfigureerd, een *root*-wachtwoord ingesteld, en over het algemeen één gebruiker aangemaakt. Wanneer dit boek gebruikt wordt bij de installatie van een thuisserver, of bijvoorbeeld een virtuele machine om te oefenen, zijn deze eerste stappen uiteraard nog niet gezet. De installatie-images van genoemde systemen, evenals voor de meeste andere Unix-varianten, ondersteunen de gebruiker bij het instellen van het netwerk en het aanmaken van de eerste gebruiker, waarmee het systeem na installatie op het niveau is dat verwacht wordt bij aanvang van dit boek.

Omdat providers vaak gebruikmaken van aangepaste images voor de installatie – bijvoorbeeld om te zorgen dat de netwerkinterfaces juist geconfigureerd worden bij het opstarten – is het niet met zekerheid te zeggen welke software al geïnstalleerd is op de nieuwe server. Dit boek gaat daarom uit van een nieuwe, verse installatie vanuit een image zonder aanpassingen.

Bestandssysteem

Er bestaan diverse bestandssystemen, die allemaal hun voor- en nadelen hebben, afhankelijk van de wensen van de gebruiker. Providers bieden hierin echter meestal geen keuze voor gepre-installeerde servers. Voor de server zoals gedocumenteerd in dit boek is dat geen enkel probleem; de standaardbestandssystemen (**`ext4`** voor Linux en **`UFS`** voor FreeBSD) volstaan prima. De systeembeheerder die dringende andere wensen heeft voor het gebruikte bestandssysteem, heeft waarschijnlijk nog meer wensen die niet in dit boek besproken worden.

Provider

Het selecteren van een geschikte provider begint met het vergelijken van websites van verschillende providers. Een aantal zaken om hierbij op te letten:

- Garanties voor *uptime* en bereikbaarheid
  Een onbereikbare server is nutteloos. Overigens zal geen provider *100%* garanderen, omdat dit geen ruimte laat voor onvoorziene omstandigheden.
- Back-up elektriciteit
  Komt de server in aanmerking voor elektriciteit van een noodaggregaat, in geval van een stroomstoring (en hoe lang)?
- DDoS-bescherming
  Een *DDoS*-aanval (*Distributed Denial of Service*) houdt in dat aanvallers vanuit meerdere locaties op het internet aanvragen naar de server sturen, met als doel deze onbereik-

baar te maken voor anderen (legitieme bezoekers/klanten), of deze te laten bezwijken onder de hoeveelheid werk. Een colocatie-provider kan hier bescherming tegen bieden, en biedt dit meestal aan op verschillende niveaus, tegen verschillende tarieven.

- Serviceniveau
  Staat men bij problemen 7 dagen per week, 24 uur per dag, binnen 15 minuten klaar, of is de systeembeheerder meer op zichzelf aangewezen? Op zich hoeft het geen probleem te zijn als het serviceniveau wat lager is, maar dan moet het datacenter wel in de buurt zijn, zodat het geen al te groot obstakel is om de server zelf te bezoeken.
- Fysieke toegang
  Als het nodig kan zijn de server af en toe te bezoeken, dan moet het deurbeleid van het datacenter dusdanig zijn dat de systeembeheerder 24 uur per dag toegang heeft, en bij voorkeur zonder afspraak vooraf.

Het is een goed idee om tijdens deze selectie ook per e-mail en telefoon vragen te stellen aan de provider. Dit is een eenvoudige manier om de responsetijden te testen.

Uiteraard zal later geverifieerd moeten worden dat deze beloften ook in het contract weerspiegeld worden.

In de overwegingen betreffende de keuze van een provider kan ook meegenomen worden dat de privacyregelgeving in Europa strenger is dan in het overgrote deel van de rest van de wereld. Bedrijven die gegevens opslaan van Europese gebruikers en kiezen voor een Amerikaanse provider zijn in ieder geval verplicht te verifiëren dat de gekozen provider gecertificeerd is volgens het *Privacy Shield*-programma.
Bovendien kan het interessant zijn zich te realiseren dat landen als Zwitserland, Duitsland, Tsjechië en IJsland geen wetten kennen die een systeembeheerder kunnen verplichten wachtwoorden of sleutels over te dragen.

Tot slot is het belangrijk dat de provider een *remote console* biedt. Een *remote console* biedt de systeembeheerder de mogelijkheid om via het internet contact te maken met het netwerk van de provider, en vanuit dat netwerk direct op de console van de server in te loggen, alsof hij of zij zich met toetsenbord en scherm bij de server bevindt. Hiermee beschikt de systeembeheerder over een achterdeur in het geval van bijvoorbeeld netwerkproblemen op de server (vrijwel iedere systeembeheerder heeft zichzelf weleens buitengesloten tijdens het configureren van de firewall). Zonder deze *remote console* zou de systeembeheerder bij netwerkproblemen naar het datacenter toe moeten, om de problemen via de console op te lossen. Een remote console wordt ook wel *KVM over IP* (*Keyboard, Video, Mouse over Internet Protocol*) of *IPMI* (*Intelligent Platform Management Interface*) genoemd.

Configuratie van de BIOS of de UEFI

Vanwege de grote verscheidenheid aan instellingen voor *BIOS* en *UEFI* is het onmogelijk ze hier allemaal te behandelen. Met een paar aanwijzingen en een beetje gezond verstand moet het echter voor elke systeembeheerder mogelijk zijn de BIOS of UEFI goed te configureren.

De provider kan vertellen hoe men van afstand toegang krijgt tot de BIOS- of UEFI-instellingen (of tot het virtuele equivalent daarvan in het geval van een virtuele machine).

Stel de machine in om zichzelf automatisch in te schakelen na een stroomstoring. Het is vervelend als de stroom uitvalt en de machine daardoor ook uitgaat. Maar het is nog veel vervelender als de machine daarna niet vanzelf weer opstart. Ga ervan uit dat de provider, in het geval van een stroomstoring, grotere prioriteiten heeft dan een beheerder naar uw server te sturen om de schakelaar om te zetten.

Stel geen *boot*-wachtwoord in. Als de server na een stroomstoring vanzelf weer opkomt, is het niet praktisch als hij vervolgens op een wachtwoord wacht om het besturingssysteem op te starten.

Stel wel een wachtwoord in om toegang te krijgen tot de instellingen van de BIOS of UEFI. Wanneer deze instellingen niet beveiligd zijn met een wachtwoord, is het voldoende om een *reboot* af te wachten of te forceren, om ze allemaal weer ongedaan te maken. Sla dit wachtwoord veilig maar vindbaar op; u zult dit zo weinig nodig hebben, dat u het gegarandeerd vergeten bent als het zover is.

Schakel zaken als USB, de parallelle poort en de CD of DVD uit. Een server heeft al deze zaken niet nodig, maar iemand met kwade bedoelingen kan ze gebruiken om toegang tot de server te krijgen.

Inloggen op de nieuwe server

Na het selecteren van de hardware en de provider, en het instellen van de BIOS/UEFI, is het tijd om voor de eerste keer in te loggen op de nieuwe server. In de documentatie van de provider is terug te vinden hoe dit bij uw provider werkt.

Waarschijnlijk heeft de provider *SSH-toegang* op de server geconfigureerd. Indien dit het geval is, zal de provider ook documenteren hoe toegang verkregen kan worden via SSH; het configureren van de *SSH-server* en het inloggen via SSH worden in een later hoofdstuk van dit boek uitgebreid behandeld.

Het is ook mogelijk dat toegang alleen toegestaan is via de eerder besproken remote console. Ook in dit geval zal de provider de toegang documenteren. Wanneer het een thuisserver of een virtuele machine op de pc betreft, is er uiteraard geen sprake van een remote console, maar kunnen gewoon het toetsenbord en het scherm gebruikt worden.

Om niet te veel op de zaken vooruit te lopen, is het voorlopig nog acceptabel om in te loggen met de gebruikersnaam *root* (*administrator*). In een volgend hoofdstuk zal directe toegang tot dit account uit veiligheidsoverwegingen geblokkeerd worden.

Op een standaard Debian-installatie is direct inloggen op het *root*-account al geblokkeerd. De mogelijkheid bestaat dat de provider deze blokkering ongedaan heeft gemaakt bij de installatie van de server. Indien dit niet het geval is, log dan in met de gemaakte/verstrekte gebruikersnaam, en gebruik vervolgens het commando **`su -`** (**es uu spatie min Enter**) om te schakelen naar het *root*-account; het systeem vraagt dan om het wachtwoord van *root*.

Tik **`exit`** om terug te gaan naar het account van de 'gewone' gebruiker.

Tik **`exit`** om uit te loggen van de server.

1.6 Gebruikte namen en adressen

In dit boek wordt een internetserver geconfigureerd. Voor een op een netwerk aangesloten server zijn één of meer IP-adressen vereist, en één of meer domeinnamen en hostnames gewenst.

De volgende gegevens zullen gebruikt worden voor documentatiedoeleinden. U moet deze zelf aanpassen aan uw systeem; uiteraard worden deze wijzigingen waar nodig gedocumenteerd.

IP-adres

Het IP-adres van een server kan niet verzonnen worden, dit wordt toegewezen door de provider. Wanneer men zich niet houdt aan het door de provider toegewezen IP-adres is de server mogelijk niet meer bereikbaar.

Dit boek gaat ervan uit dat de provider het IP-adres **198.51.100.156** verstrekt heeft, met *netmask* **255.255.255.0**. Dit adres komt uit een gereserveerde reeks die speciaal bestemd is voor documentatie; het kan dus nooit botsen met het adres van een 'echte' server. Het *gateway*-adres dat de denkbeeldige provider heeft verstrekt, is **198.51.100.1**.

Voor een thuis- of kantoorserver kan het IP-adres wel zelf gekozen worden. Het is dan zaak het IP-adres te kiezen uit één van de IP-reeksen die gereserveerd zijn voor privégebruik, zodat het adres nooit kan botsen met een IP-adres dat op internet gebruikt wordt. Meer hierover in het hoofdstuk over netwerkconfiguratie.

Naast het IP-adres van de netwerkinterface(s) heeft iedere computer, ongeacht of het een server betreft of een pc, ook het IP-adres **127.0.0.1**. Dit adres wordt gebruikt voor netwerkverkeer van de computer naar zichzelf. Deze virtuele netwerkinterface waaraan dit adres is gekoppeld, wordt het *loopback device* genoemd.

Aangezien de implementatie van *IPv6* (*Internet Protocol versie 6*) nog niet zover is dat het noodzakelijk is voor het functioneren van een internetserver, en er geen delen van het publieke internet zijn die niet bereikbaar zijn over *IPv4*, wordt *IPv6* in dit boek niet behandeld.

Domeinnamen

Hoewel een domeinnaam niet strikt noodzakelijk is voor de werking van de server – een IP-adres is in principe voldoende – zal men over het algemeen één of meer domeinnamen aan het IP-adres willen koppelen, zodat gebruikgemaakt kan worden van herkenbare e-mail- en website-adressen. Een domeinnaam kan wel zelf gekozen worden en wordt geregistreerd bij een *registrar*, een functie die over het algemeen de provider op zich neemt. Uiteraard kan iedere domeinnaam slechts door een enkele eigenaar geregistreerd worden, dus de mogelijkheid tot registratie is afhankelijk van de beschikbaarheid van de gewenste domeinnaam.

Bij de registratie van een domeinnaam wordt gevraagd tenminste twee DNS-servers op te geven. Deze DNS-servers zijn de servers die de koppeling tussen het IP-adres en de domeinnaam registreren. Als eerste (*primaire*) DNS-server kan het adres van deze server opgegeven worden, het adres dat in de vorige paragraaf door de provider is verstrekt. Normaal gesproken zal de provider aanbieden als *secundaire DNS* te fungeren,

maar men is vrij hiervoor een andere server te kiezen; er zijn verschillende bedrijven die deze dienst gratis of tegen betaling kunnen leveren, of er kan gekozen worden voor een server die reeds in bezit is. De secundaire DNS-server kopieert zijn gegevens periodiek van de primaire DNS-server. Meer over DNS later in dit boek.

De server in dit boek verwerkt het verkeer voor de domeinnamen *example.com*, *example.edu* en *example.org*, met *example.com* als hoofddomein. Net als voor het voor deze documentatie gekozen IP-adres, geldt ook voor deze domeinnamen dat ze gereserveerd zijn voor documentatiedoeleinden; ze kunnen door niemand geregistreerd worden, en ook niet botsen met reeds geregistreerde domeinnamen.

De denkbeeldige provider, *ExampleNET*, heeft als domeinnaam *example.net*.

Een domeinnaamregistratie is altijd geldig voor een bepaalde periode, bijvoorbeeld 1 of 2 jaar. Denk eraan uw registratie te verlengen voordat deze verloopt, anders loopt u het risico dat een ander de domeinnaam wegkaapt – dan wel om hem zelf te gebruiken, dan wel om hem voor veel geld aan u terug te verkopen. Normaal gesproken ontvangt u bericht van uw provider wanneer de registratie dreigt te verlopen.
Wanneer u één of meer domeinnamen geregistreerd hebt, zult u met enige regelmaat e-mails ontvangen over de verlenging van uw registratie(s). Reageer hier alleen op wanneer u zeker weet dat het bericht afkomstig is van uw provider. Als u tekent bij een andere provider, kan deze uw domeinnaam verhuizen, en u meer in rekening brengen voor dezelfde registratie.

Hostname

Een *host* is een computer in een netwerk. Omdat namen makkelijker te onthouden zijn dan IP-adressen, krijgen computers in een netwerk ook een naam: de *hostname*. De systeembeheerder is volledig vrij in de keuze van deze hostnames; de meesten kiezen een bepaald thema, bijvoorbeeld muziekinstrumenten of namen uit televisieseries of films.

Voor dit boek is gekozen voor het thema *kleuren*. De naam van de server is *groen*. De volledige hostname (ook wel *fully qualified domain name*) is daarmee *groen.example.com*. Een eventuele volgende server zou dan *rood.example.com* kunnen heten.

Uiteraard worden verderop in dit boek ook nog *aliassen* als *www.example.com* aangemaakt.

Gebruikersnamen

Indien in voorbeelden namen van gebruikers nodig zijn, zullen daarvoor *diane* en *dimitri* gebruikt worden; de bijbehorende eigennamen zijn uiteraard *Diane* en *Dimitri*.

Gebruikersnamen worden bij conventie altijd geschreven met kleine letters, maar hoofdletters zijn ook toegestaan. Cijfers, de punt, het lage streepje en het verbindingsstreepje zijn ook toegestaan, maar gebruikersnamen mogen niet beginnen met een verbindingsstreepje. Letters met accenten zijn niet toegestaan.

1.7 Uitleg bij de Oefenopdrachten

Het boek ***Configuratie van een internetserver*** beschrijft het inrichten van een server op basis van drie verschillende Unix-varianten. Om, parallel aan het bestuderen van dit boek, zelf een virtuele server op te bouwen zijn er vanaf hoofdstuk 3 aan het eind van elk hoofdstuk hands-on oefeningen toegevoegd waarbij omwille van duidelijkheid gekozen is voor één variant. De oefeningen zijn gemaakt voor CentOS omdat deze gebaseerd is op de veelgebruikte Red Hat Enterprise-distributie, versie 7. Basiskennis van Linux is hiervoor vereist. Hoewel hoofdstuk 2 een aantal essentiële onderdelen van het Linux-systeem behandelt is dit niet voldoende om zonder voorkennis aan de **oefenopdrachten** te beginnen.

De theorie in het boek gaat uit van een volledig ingerichte server voor professioneel gebruik. Als dit de opzet is moet je vooral de theorie uit het boek stap voor stap volgen voor de door jou gekozen distributie. Om met veel essentiële zaken voor het inrichten van de server in een virtuele omgeving te oefenen zonder in de praktijk helemaal de diepte in te gaan, is het boek op de volgende wijze goed te gebruiken:

- Lees elk hoofdstuk door en bestudeer alle opties. Bekijk de in het grijs gedrukte commando's maar voer deze niet uit.
- Als de theorie van een hoofdstuk duidelijk is, ga dan naar de **Oefenopdracht** aan het eind van het hoofdstuk. Hierin staat stap voor stap vermeld welke stappen je moet volgen om tot een werkend resultaat te komen in de virtuele omgeving. Vaak zijn de commando's overgenomen uit de theorie, soms wordt hiernaar terugverwezen en soms zijn aanpassingen zodanig dat het uitvoerbaar is in de virtuele omgeving.
- Omdat we in een virtuele omgeving werken kunnen we een aantal zaken niet doen. Vanaf hoofdstuk 10 wordt SSL geïnstalleerd. Omdat dit niet lukt wordt vanaf hoofdstuk 11 alleen een aantal configuraties gemaakt die zonder SSL werken. Je hebt hierna een werkende DNS-server, een werkende webserver en een aantal databases geïnstalleerd.