DNSadmin gebruikershandleiding

Datum laatst bewerkt:	26-05-2020
Versie:	3.02
Organisatie:	QDC Internetservices

Contact informatie

Adres:
Damlaan 11
2265 AL Leidschendam
Nederland

Telefoonnummer: +31 70 327 12 59
Fax (digitaal)**:** +31 84 836 47 06
E-mail: info@qdc.nl
Website: https://www.qdc.nl/

Inhoudsopgave

DNSadmin gebruikershandleiding 1
Inhoudsopgave 2
Inleiding 3
- Web Based Beheer 3
- Redirection Engine 3
- Beheer en Monitoring 3
- DNSSEC 3
- Meer informatie 3

Inloggen 4
- Wachtwoord vergeten 4

Het DNSadmin Dashboard 5
- Wijzigen Wachtwoord 5
- Het Records overzicht 6
- Record wijzigen 6
- Record toevoegen 7
- Verwijderen record 8

Record types 9
- A-record 9
  - Wildcard 9
- AAAA-record 9
- CAA-record 10
  - Wat is een CAA DNS Record? 10
  - Opbouw van een CAA-record 10
  - Toevoegen van een CAA-record 11
- CNAME-record 11
  - Een CNAME-record aanmaken 12
- NS-record 12
- SRV-record 13
  - Een SRV-record aanmaken in DNSadmin 13
- TXT-record 13
  - SPF 14
  - DMARC 16
  - Site verificatie 16
- URL-record 17
  - Wat is URL-forwarding 17
  - Het aanmaken van een URL-record 17
- PTR-record 19
- MX-record 19

Admin account functies 21
- Het subaccount overzicht 21
- Domeinnamen koppelen aan een subaccount 21

Uitleg van diverse begrippen 23
- Domain Name Server (DNS) 23
- TTL 23
- URL 23
- CAA-records 23
- DNSSEC 24

Inleiding

Een goed werkende DNS-infrastructuur ligt ten grondslag aan het goed functioneren van vrijwel alle diensten welke gebruik maken van het internet. Onze DNS-infrastructuur is redundant uitgevoerd op 3 verschillende VPS-servers, welke elk zijn ondergebracht op een geografisch gescheiden locatie. Zo opereren zij vanuit een eigen netwerk, om ervoor te zorgen dat zelfs bij ernstige calamiteiten in een van deze drie netwerken uw DNS blijft werken.

Web Based Beheer

Al uw domeinnamen en bijbehorende records kunnen gemakkelijk via een beveiligde website worden beheerd. Op deze website kunt u dit portaal vinden: https://dnsadmin.qdc.nl/.

Redirection Engine

Onze DNSadmin portaal biedt u de mogelijkheid om direct vanuit de interface gebruik te kunnen maken van de mogelijkheid tot het aanmaken van http-forwards middels een eigen ontwikkeld type record, het URL-record. Dit is geen officieel DNS-record, het maakt eigenlijk ook gebruik van een IP-adres middels een A-record. Het bijbehorende IP-adres is de server waarop deze Redirection Engine draait.
Hierdoor is het niet mogelijk om tegelijkertijd een URL-record en een A-record aan te maken. Wilt u toch wisselen, dan dient u eerst het oude record te verwijderen, voordat u het nieuwe record aan kan maken.

Beheer en Monitoring

Vanzelfsprekend wordt de DNS-service met behulp van onze monitoring systemen 24 uur per dag, 365 dagen per jaar in de gaten gehouden. Daarnaast zorgen wij ervoor dat de software altijd up-to-date is en u zonder technische tussenkomst gebruik kunt maken van een kwalitatief hoogwaardige DNS-infrastructuur.
Tevens worden er dagelijks diverse scans uitgevoerd om te controleren of er geen DNS-records worden gebruikt die volgens de huidige technologische standaard niet zouden mogen bestaan. Ook worden er diverse records bijgehouden, welke bijdragen aan de overall betrouwbaarheid van onze domeinnamen. Hierbij valt te denken aan SPF-records en DMARC-records, welke het systeem systematisch naloopt en eventueel toevoegt indien deze missen

DNSSEC

Voor alle domeinnamen, welke gebruik maken van onze DNS-infrastructuur, kunnen wij DNSSEC configureren. Deze extra beveiliging kan voorkomen dat kwaadwillende uw domeinnaam nabootsen door bijvoorbeeld spoofing of phishing.
Voor alle .NL, .BE en .EU domeinnamen wordt dit automatisch door ons geconfigureerd. Voor andere domeinregistraties wordt dit op verzoek afgehandeld.

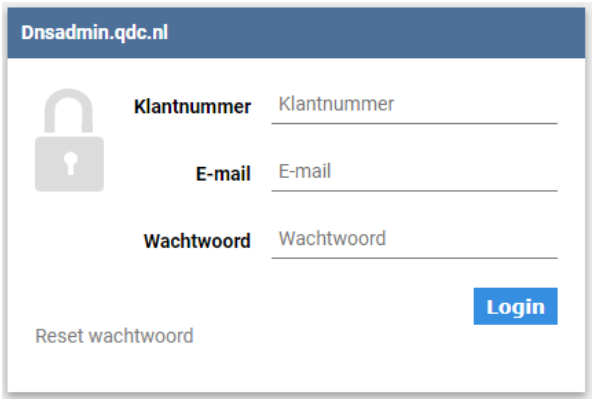
Meer informatie

Bent u geïnteresseerd in DNSadmin of wenst u meer informatie? Neem dan contact op met onze support afdeling (support@qdc.nl).
We zijn ook telefonisch te bereiken op +31 (0) 70 327 1259

Inloggen

DNSadmin is via een beveiligde verbinding bereikbaar op https://dnsadmin.qdc.nl/

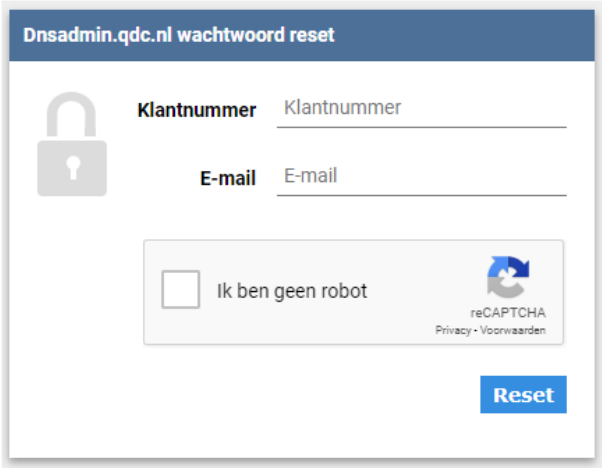
Alvorens u DNS-records kunt wijzigen en/of aanmaken moet u eerst inloggen op het systeem. Hieronder ziet u het inlogscherm.



Het **klantnummer** is gelijk aan uw klantnummer bij QDC. Het **e-mailadres** met het bijbehorende **wachtwoord** waarop uw DNSadmin account is aangemaakt, zou u per e-mail van ons ontvangen moeten hebben. Nadat uw inloggegevens correct zijn ingevuld, verschijnt het DNSadmin Dashboard.

Wachtwoord vergeten

Als u uw wachtwoord bent vergeten dan kunt u gebruik maken van de optie “Reset wachtwoord”. Het volgende scherm wordt dan getoond:



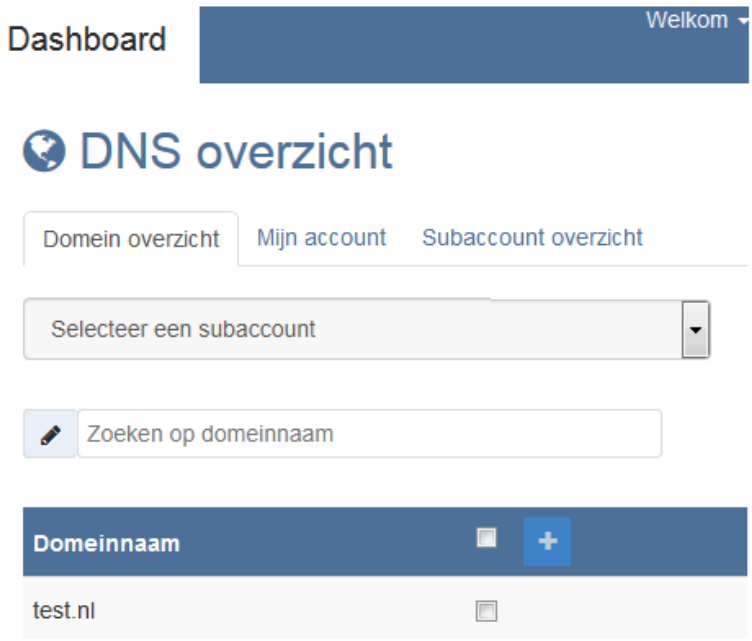
Ook hier kunt u uw **Klantnummer** en **E-mail** achterlaten. Verifieer hierna dat u geen robot bent en kies voor **Reset**. Het systeem controleert of het opgegeven E-mailadres ook overeenkomt met het bijbehorende klantnummer. Als deze overeenkomen, dan worden er instructies verstuurd om uw wachtwoord aan te passen.

Indien u na een uur nog geen instructie e-mailbericht heeft ontvangen, dan kunt u contact opnemen Stuur hiervoor een e-mailbericht naar support@qdc.nl, geef daarbij ook aan welk klantnummer en e-mailadres u heeft ingevuld. Wij controleren dan of de door u gebruikte gegevens overeenkomen met de gegevens welke in ons systeem bekend zijn. Als deze niet kloppen, dan nemen wij dat met u op. Het is ook mogelijk dat wij om meer verificatie gaan vragen, om er vanzelfsprekend voor te zorgen, dat de inloggegevens alleen bij de juiste personen terecht komen.

U kunt de bovenstaande stappen ook volgen, indien u niet langer toegang heeft tot het e-mailadres waarop uw DNSadmin account in het verleden is aangemaakt.

Het DNSadmin Dashboard

Op het hoofdscherm start u met een overzicht van alle domeinen onder uw DNSadmin-account, welke op onze DNS-servers staan. Het domein **test.nl** wordt verder in deze handleiding als voorbeeld gebruikt.



Dit DNS overzicht krijgt u ook te zien als u op een later moment kiest voor het tabblad “Domein overzicht”.

Note: Het is mogelijk dat u het tabblad “Subaccount overzicht” en het menu “Selecteer een subaccount” uit het voorbeeld hierboven niet ziet. Deze zijn namelijk alleen zichtbaar voor resellers, welke meerdere accounts hebben ondergebracht bij QDC.

Indien u ook gebruik wenst te maken van subaccounts, dan kunt u dat opnemen met onze support afdeling support@qdc.nl).

Wijzigen Wachtwoord

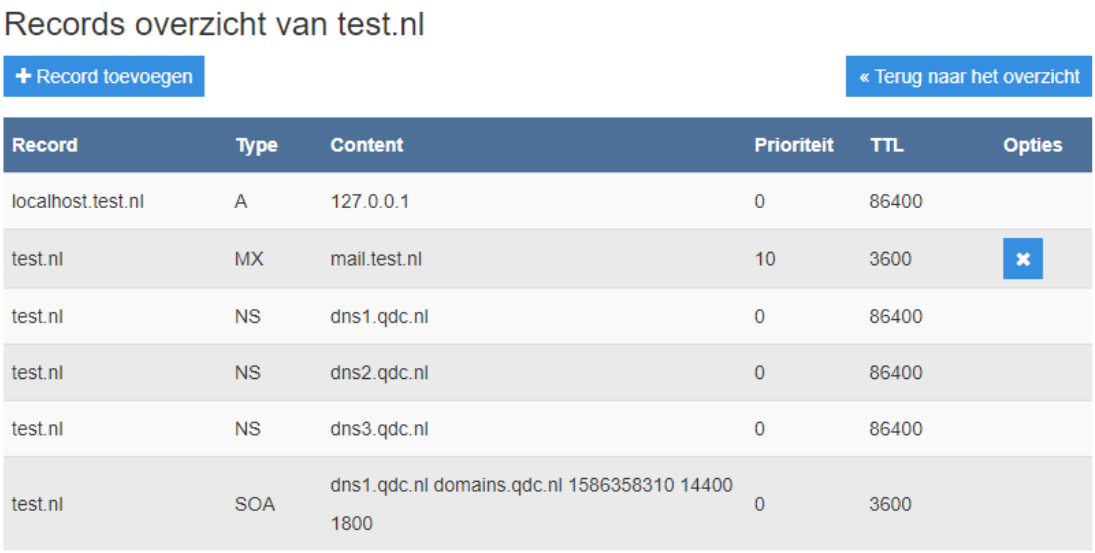
Nadat u bent ingelogd, kunt u ervoor kiezen om uw wachtwoord te wijzigen. Ga hiervoor naar het tabblad “Mijn account”. De onderstaande pagina wordt getoond.

In het bovenstaande overzicht kunt u het wachtwoord wijzigen door het huidige wachtwoord op te geven en **tweemaal** het nieuw gewenste wachtwoord op te geven. Tevens kunt u hier uw **E-mailadres** wijzigen in het veld **E-mail**.

Het Records overzicht

Als u teruggaat naar het startscherm (via de tab “Domein overzicht”), dan ziet u wederom het overzicht van de gekoppelde domeinnamen uit uw portfolio.

Indien u nu een van deze domeinnamen aanklikt, dan komt u in het **Records overzicht** van de gekozen domeinnaam.



Op het Records overzicht scherm kunt u diverse handelingen uitvoeren, zoals het wijzigen, toevoegen en verwijderen van DNS-records.

Met de button **Terug naar het overzicht** gaat u weer naar het Domein overzicht.

Record wijzigen

Door op een regel van een DNS-record te klikken, komt u op een nieuwe pagina. Hier staat het record uitgeschreven en kan het betreffende record tevens gewijzigd worden. Zo kunt u in het onderstaande voorbeeld het type record, de content (oftewel de inhoud van het record), de prioriteit en de TTL wijzigen. Tevens kan de “voorloop” van het record worden gewijzigd. In het voorbeeld is dit veld leeg, maar daar kan bijvoorbeeld ook **www** of **mail** worden opgegeven.

Let op! De records met het type NS en SOA en het localhost-record kunnen om technische redenen niet aangepast of verwijderd worden in DNSadmin. Deze zijn noodzakelijk voor de werking van een domeinnaam.

U kunt het record wijzigen door uw gewenste aanpassingen door te voeren en deze vervolgens te bevestigen met de button **Gegevens wijzigen**. In het volgende hoofdstuk over het toevoegen van een DNS-record, worden de velden extra toegelicht.

Indien u kiest voor de button **Terug naar het overzicht**, dan wordt u weer naar de pagina gestuurd met alle DNS-records van de huidige domeinnaam.

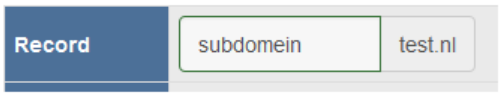
Record toevoegen

Indien er een nieuw record nodig is, dan kan er vanuit het **Records overzicht** gekozen worden voor de button **Record toevoegen**. Er wordt dan een soortgelijke pagina geopend, zoals de pagina om een record te wijzigen.
U kunt nu een nieuw record toevoegen. Voor ieder type record is dit scherm in de basis hetzelfde. Er kan echter per record een ander veld verschijnen, om uw gegevens in te vullen. Daarnaast worden er bij het toevoegen of wijzigen van een record ook controles uitgevoerd. Zo wordt er per type record een aantal tests gedaan, welke ervoor zorgen dat er in principe geen fouten kunnen ontstaan. Als voorbeeld, een exact hetzelfde record kan niet twee keer bestaan.

Bij het aanmaken van een nieuw record of het wijzigen van een bestaand record, dient u rekening te houden met het volgende:

Record: standaard wordt bij het toevoegen van een record, het nieuwe record aangebracht op het hoofddomein Dit hoofddomein staat hieronder in het grijs aangegeven en kan niet aangepast worden. Met het hoofddomein wordt hier de domeinnaam zonder voorloop bedoelt, uit het voorbeeld is dat dan alleen **test.nl**.

Wanneer u wenst dat de aanpassing op een subdomein wordt aangebracht, dan kunt u het subdomein opgeven in het veld vóór de domeinnaam. In het onderstaande voorbeeld is het dan alleen het voorvoegsel **subdomein**. Het totale record zal dan werken op **subdomein.test.nl**. Deze totale naam wordt ook aangeduid als *Hostname*. Is er geen voorloop, dan is de hostname vanzelfsprekend alleen **test.nl**.



Note: In het veld staat hier **subdomein** opgegeven zonder een punt-symbool (.) tussen het subdomein en het hoofddomein in. DNSadmin zet automatisch een punt tussen de waarde welke u opgeeft in het veld en de domeinnaam die erachter staat. Uiteraard mag u wel de punt toevoegen, ook dan wordt er automatisch slechts één punt gebruikt.

Type: Hier kunt u de verschillende soorten records selecteren, welke verschijnen als u op het “Drop Down” menu klikt. De verschillende soorten worden later in dit document toegelicht.

Content: Hier dienen de gegevens ingevoerd te worden, welke nodig zijn voor het record. Afhankelijk van het type dienen hier de bijbehorende gegevens ingevuld te worden. Ook deze gegevens worden nog toegelicht per type record.

TTL: Dit staat voor Time to Live en wordt gebruikt voor de tijd (in secondes). Deze waarde wordt gebruikt om aan te geven hoe lang een record onthouden mag worden op het internet. In de praktijk wordt dit echter niet altijd meer gebruikt, omdat veel computers en netwerken vaak zelf gebruik maken van eigen methodes, waaronder internetgeschiedenis en cache.
De waarde in het TTL-veld wordt door DNSadmin alvast voor u ingevuld, afhankelijk van het gekozen type record. Deze hoeft u in principe niet aan te passen, omdat het voor de werking van het record nauwelijks nog van invloed is.
Hoewel wij adviseren deze niet aan te passen, hebben wij deze mogelijkheid er wel in laten zitten. Wilt u deze toch wijzigen, dan dient u er rekening mee te houden dat wij de waarde hebben gelimiteerd tussen de 600 en 604800 seconden (dat is minimaal 10 minuten en maximaal 1 week). Vereist een record een lagere waarde, kies dan voor 600.

Prioriteit: Deze waarde (ook vaak afgekort tot alleen prio) kan ingevuld worden bij de record types MX en SRV. Deze waarde is ook gelimiteerd, namelijk tussen de 0 en de 65535. Indien u dit veld niet invult, dan wordt de prioriteit 0 automatisch gekozen. Hieronder staat beknopt uitgelegd, waarvoor de prioriteit gebruikt wordt:

Indien er twee records worden gemaakt met dezelfde hostname, maar met andere content, dan wordt de prioriteit geraadpleegd. Het record met de laagste prioriteit zal dan als eerst worden aangesproken. Dit kan handig zijn als er bijvoorbeeld meerdere mailservers aanwezig zijn, een hoofdserver en een server in het geval van calamiteiten (een back-up-server).
Als de hoofdserver een lagere prioriteit krijgt dan de back-up-server, dan zal alle e-mail normaliter afgeleverd worden op de hoofdserver. Mocht deze hoofdserver door een calamiteit niet meer gevonden worden op het internet, dan zullen de e-mailberichten worden afgeleverd bij de back-up-server. Zo kunt u zichzelf beter beveiligen tegen het verlies van een e-mailbericht.
Deze prioriteit zal verder ook nog toegelicht worden, bij de bijbehorende type records.

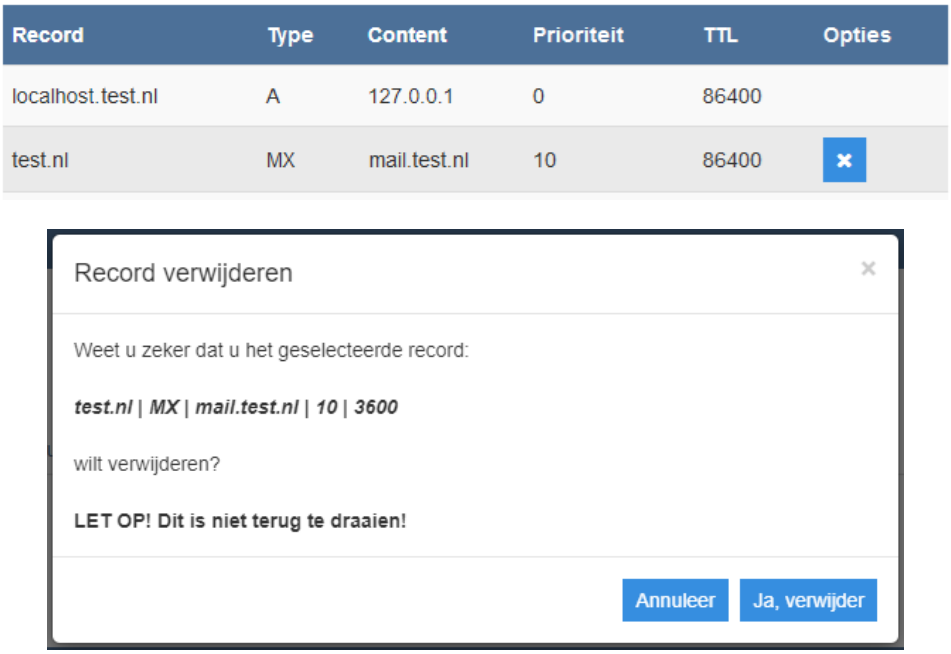
Tweede Type: Indien er gekozen wordt voor het URL-record bij type, dan veranderen de velden enigszins. Verder op in dit document wordt dit nader toegelicht.

Indien alle velden zijn ingevuld met de gewenste gegevens, dan kunt u het record toevoegen met de button Record toevoegen. Kies voor de button **Terug naar het overzicht** om terug te keren naar Records overzicht.

Belangrijk: Hou er rekening mee dat het tot 48 uur kan duren, voordat een wijziging op DNS-niveau op het gehele internet bekend is. Het kan dan ook voorkomen dat uw gewijzigd record niet direct werkt. In de praktijk gaat dit echter vaak sneller, een wijziging zou binnen enkele uren al zichtbaar kunnen zijn en soms zelfs binnen enkele minuten. Toch adviseren wij om rekening te houden met de opgegeven 48 uur.

Verwijderen record

In het **Records overzicht** kunt u ook records verwijderen. Aan de rechterkant van het overzicht staat de categorie **Opties.** Bij records welke verwijderd kunnen worden, staat een kruisje weergegeven. Als u hierop klikt wordt er een bevestiging gevraagd, voordat het record daadwerkelijk verwijderd wordt.



U kunt het verwijderen bevestigen met de button **Ja, verwijder**. U kunt er ook voor kiezen om het record te behouden, door te kiezen voor de button **Annuleer**.

Record types

Bij het aanmaken of wijzigen van de verschillende records, kunt u kiezen uit een aantal types. Deze types worden hieronder toegelicht.

A-record

Dit type wordt gebruikt als u een (sub)domeinnaam wilt laten verwijzen naar een webserver, door middel van een IP-adres (versie IPv4). Wanneer u bijvoorbeeld een internetaansluiting heeft met een vast IP-adres, dan kunt u deze koppelen aan uw (sub)domein, Zo kunt u dan bijvoorbeeld een eigen webserver draaien.

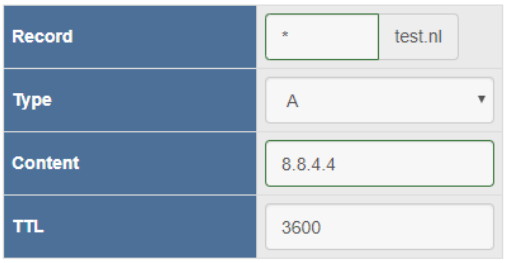
In het onderstaande voorbeeld is dit weergegeven, met als IP-adres 8.8.8.8 (een IP-adres van Google) en als hostname **webserver.test.nl**.

Record: `webserver.test.nl A 8.8.8.8`

Wildcard

In het volgende voorbeeld is een **wildcard** (*) A-record aangemaakt voor domein **test.nl** naar IP-adres 8.8.4.4 (ook een IP-adres van Google. Dit houdt in dat u via ieder willekeurig subdomein uitkomt op dit opgegeven IP-adres. Zou u bijvoorbeeld naar **computer.test.nl** of **mail.test.nl** gaan, dan komt u bij beide op IP-adres 8.8.4.4 uit. Het *-symbool vangt namelijk alle mogelijke combinaties af.

Record: `*.test.nl A 8.8.4.4`



Note: Een wildcard-record werkt alleen voor niet benoemde subdomeinen, van hetzelfde type. Indien u beide bovenstaande voorbeelden heeft aangemaakt (het **www** en het **wildcard**-record), dan werkt het wildcard record niet voor **www.test.nl**. Dit komt dan doordat het **www**-record apart benoemd is (deze verwijst naar 8.8.8.8 en niet naar 8.8.4.4). Alle apart benoemde records hebben altijd voorrang op een eventueel ingesteld wildcard-record.

Belangrijk: Wij adviseren overigens om geen gebruik te maken van een **wildcard**-record, omdat dit een negatieve invloed op de performance van uw server kan hebben. Maak hier alleen gebruik van, indien u er zeker van bent dat dit noodzakelijk is.

AAAA-record

Met de komst van de IPv6-adressen zijn er ook mogelijkheden gemaakt om deze aan domeinnamen en subdomeinen te koppelen. Hieronder staat een voorbeeld van een niet bestaand adres.

Record: `ipv6.test.nl AAAA 2a00:1450:4010:c07::5e`

Het toevoegen van een AAAA-record gaat op exact dezelfde manier als voor de hierboven beschreven stappen voor een A-record. Het verschil zit dan in het veld content, waar u een IPv6-adres dient op te geven. Ook hier is het mogelijk om een wildcard aan te maken.

CAA-record

Het CAA-record is een DNS-record dat domeineigenaren extra controle geeft over SSL-certificaten die worden uitgegeven voor diens domeinen. Hiermee kan worden aangegeven welke CA (Certificate Authority), certificaten mag uitgeven voor jouw domeinen. Het is voor domeineigenaren overigens niet verplicht het record in te vullen.

Wat is een CAA DNS Record?

Een Certificate Authority Authorization record, oftewel een CAA-record, is ontworpen om domein eigenaren de mogelijkheid te bieden om aan te geven welk CA root-certificaat gebruikt mag worden om certificaten mee te ondertekenen voor het domein in kwestie. Omdat dit certificaat toebehoort aan een bepaalde certificaat autoriteit, kan hiermee effectief aangegeven worden welke certificaten uitgegeven mogen worden voor een domein. Dit voorkomt dat het uitgeven van een certificaat door een andere CA dat de gekozen CA gedaan kan worden.

Voorbeeld: Door onderstaand record toe te voegen voor test.nl geven we aan dat certificaten voor dit domein alleen uitgegeven mogen worden door Sectigo/Comodo:

Record: `test.nl IN CAA 0 issue "comodoca.com"`

Een domeinnaamhouder kan meerdere CAA-records toevoegen aan een domeinnaam, om zo verschillende CA's toestemming te kunnen geven, om een SSL-certificaat voor de domeinnaam uit te geven. Het toevoegen van een CAA-record is niet verplicht, de controle erop door CA's is dit wel. In de praktijk betekent dit als volgt:

- Wordt er geen CAA-record gevonden bij deze controle, dan heeft dit geen gevolgen.
- Wordt er wel een CAA-record gevonden, dan wordt de gehele domeinnaam gescand op eventueel andere aanwezige CAA-records.
  Wanneer er een “match” is tussen de uitgever van het SSL-certificaat en een van deze CAA-records, dan wordt het SSL-certificaat verstrekt. Is er geen match, dan kan de uitgever geen SSL-certificaat uitgeven.

Opbouw van een CAA-record

Een CAA record is technisch als volgt opgebouwd:

Record: `Domein Flag Tag CA`

Domein: Deze is altijd gelijk aan de domeinnaam waar het SSL-certificaat voor aangevraagd wordt, er wordt dan ook geen subdomein opgegeven. Daarnaast werkt een CAA-record, welke op het “hoofddomein” is ingesteld automatisch op alle aanwezige subdomeinen. In de DNS jargon heet dit “inherited”.

Flag: De waarde die hier opgegeven wordt is in principe altijd 0, wij adviseren dan ook om geen andere waarde op te geven.

Tag: De volgende waardes kunnen hier gebruikt worden:

- issue – deze wordt gebruikt om aan te geven dat er SSL-certificaten uitgegeven mogen worden door de betreffende CA.
- issuewild – deze wordt gebruikt om aan te geven dat er enkel een wildcard certificaat uitgegeven mag worden door de betreffende CA. Andere certificaten worden niet toegestaan.
- iodef– deze wordt gebruikt om meldingen te versturen naar het vermelde e-mailadres, wanneer er een certificaatuitgifte is mislukt.

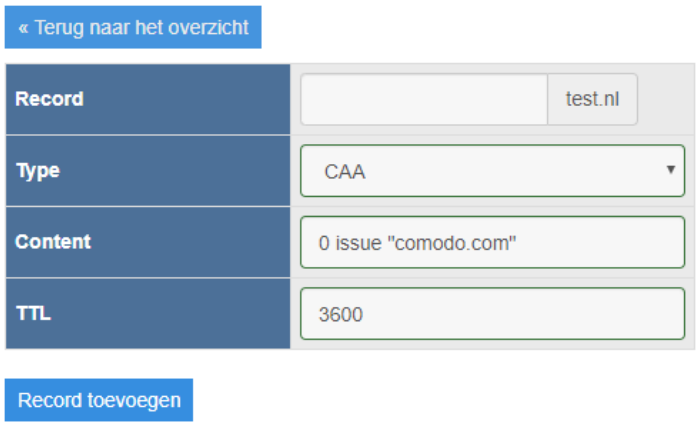
CA: Binnen deze waarde wordt de uiteindelijke CA (Certificate Authority) opgegeven. Daarnaast kan er een bepaald beleid worden opgegeven. Doordat er een CA en een beleid in de CA-waarde opgegeven kan worden, is er besloten om deze tussen quotes op te slaan. Hieronder volgen drie fictieve voorbeelden:

- Een standaard CAA-record, waarmee Comodo als CA wordt opgegeven:
  `test.nl CAA 0 issue "comodo.com"`
- Een CAA-record, waarmee Comodo als CA wordt opgegeven, maar met als beleid dat dit alleen maar EV-certificaten mogen zijn:
  `test.nl CAA 0 issue "comodo.com; policy=ev"`
- Een CAA-record, waar bijvoorbeeld een e-mailadres wordt opgegeven, welke een melding dient te ontvangen als er een mislukte poging is gedaan om een SSL-certificaat uit te geven:
  `test.nl CAA 0 iodef "mailto:abuse@qdc.nl"`

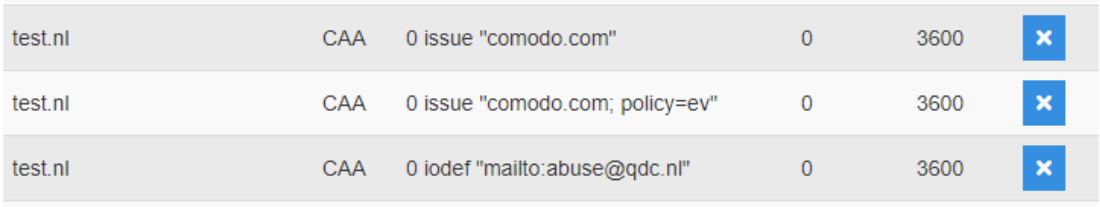
Note: Het is heel gebruikelijk dat er meerdere CAA-records worden ingevuld, wanneer een domeinnaamhouder ervoor kiest om hier gebruik van te maken.

Toevoegen van een CAA-record

Bij het toevoegen van een CAA-record dienen de volgende waardes opgegeven te worden. Het veld achter Record blijft uiteraard leeg en het type wordt op CAA gezet. Uit de bovenstaande voorbeelden wordt de eerste gekozen. Hier dienen dan de volgende waardes binnen het veld **Content** gezet dient te worden: de *Flag*, de *Tag* en de *CA*.



Voeg het record toe om het CAA-record in te stellen. In de onderstaande afbeelding zijn alle drie de voorbeelden van de CAA-records toegevoegd.



Note: Wanneer een certificaat reeds is uitgegeven, dan wordt er daarna niet meer gekeken naar eventuele CAA-records. Deze records bieden dan ook alleen bescherming tegen het aanvragen van nieuwe certificaten. Reeds uitgegeven certificaten kunnen wel gebruikt (blijven) worden op een domeinnaam, aangezien die dan al op een eerder moment zijn geverifieerd. Zo zal het toevoegen of aanpassen van CAA-records niet van invloed zijn op reeds bestaande en werkende certificaten.

CNAME-record

Een CNAME-record (of Canonical Name record) is een record dat een alias is van een andere (Canonical) hostnaam. Dit kan handig zijn in het geval er meerdere records welke verwijzen naar hetzelfde IP-adres. Dit vereenvoudigt het beheer in het geval van een wijziging van IP-adres, omdat alleen het IP-adres van het betreffende A-record gewijzigd hoeft te worden.

Belangrijk is dat een gekozen CNAME-record niet voor andere records gebruikt mag worden. Zo kan het bestaan van een A-record met de naam ftp botsen met een CNAME-record die ook als naam ftp heeft. Het wordt ook afgeraden een MX-record te verwijzen naar een CNAME-record. Een CNAME-record zou ook niet naar een andere CNAME-record moeten verwijzen.

Een CNAME-record aanmaken

Als voorbeeld willen wij het volgende CNAME-record gaan instellen:

```
Record: mail.test.eu CNAME webmail.outlook.com.
```

Geef de volgende gegevens op bij het aanmaken van een nieuw CNAME-record:

- **Record**: De naam van het subdomein. Uit het voorbeeld *mail*, vul deze in.
- **Type**: het type dient CNAME te zijn.
- **Content**: Hier wordt de hostnaam ingevuld waar het CNAME-record naar toe dient te verwijzen. In het voorbeeld is *webmail.outlook.com* gebruikt.
- **TTL**: Stel de Time To Live in, in het voorbeeld is deze niet opgegeven. Wij adviseren de standaard waarden van *3600* aan te houden.

Sla het record op met Record toevoegen en het CNAME-record is ingesteld.

mail.test.eu	CNAME	webmail.outlook.com

Let op: Het root-record (de domeinnaam zelf), mag geen CNAME-record zijn. Dit wordt dan ook niet ondersteund in ons DNSadmin portaal. Het onderstaande record kan dan ook niet worden ingesteld.

```
Foutief record: test.eu CNAME www.test.eu.
```

Over het algemeen kan de serverbeheerder (de eigenaar) van de server, waar het CNAME-record verwijst u ook een IP-adres doorgeven. Wij adviseren dan ook om het root-domein te koppelen middels dat IP-adres, door een A-record toe te voegen.

Een alternatieve oplossing hiervoor is om een URL-record aan te maken, welke verwijst naar bijvoorbeeld www.uwdomein.nl (welke wel een CNAME-record kan zijn). U kan dan het foute record van hierboven vervangen door het onderstaande record.

```
Alternatief record: test.eu URL www.test.eu.
```

Wij adviseren om in dit geval een *Redirect permanent* URL-record te kiezen. De optie *Iframe* raden wij hier af.

NS-record

Dit type records wordt gebruikt voor het aangeven van de *authorative nameservers*. Voor het hoofddomein moeten deze overeenkomen met de opgegeven nameservers bij de uitgever van het domein (de registry). Hierdoor zal het toevoegen (of wijzigen) van een NS-record geen waarde hebben, zonder dat dit ook is opgegeven bij de bijbehorende registry. Het zou zelfs kunnen voorkomen dat de domeinnaam niet meer correct functioneert, bij het wijzigen, verwijderen of toevoegen van een NS-record.

Het is wel mogelijk om NS-records aan te maken voor subdomeinen. Hou er wel rekening mee, dat de opgegeven nameserver records ook verwijzen naar een bestaande server. Die bestaande server dient dat weer geconfigureerd te worden, om als nameserver te kunnen functioneren. Anders heeft het aanmaken van een subdomein als NS-record nog geen zin.

Op dit moment is het nog niet toegestaan om zelf nameserver records aan te maken, ook niet voor subdomeinen. Een verzoek tot wijzigen of toevoegen van nameservers kunt u indienen bij de Support afdeling. Wij kunnen dan gezamenlijk kijken wat de beste oplossing hiervoor is.

SRV-record

Een SRV-record (of Service-record) kan worden gebruikt om via DNS te achterhalen welke server een bepaalde service levert voor een domeinnaam. Die server mag remote of local zijn, wat inhoudt dat de gezochte service opgevraagd kan worden op een externe server of een lokale server. Een SRV-record heeft over het algemeen de volgende notatie:

```
_Service._Protocol.Name TTL Class SRV Priority Weight Port Target
```

- Service:
  De naam van de service
- Protocol:
  Het protocol van de service (dit is vrijwel altijd TCP of UDP)
- Name:
  De domeinnaam zelf
- TTL:
  De Time To Live, uitgedrukt in secondes
- Class:
  Een standaard DNS instelling, deze staat altijd op IN
- SRV:
  Het record type, in dit geval SRV
- Priority:
  De Prioriteit van het record (hoe lager dit nummer hoe eerder dit record wordt aangesproken, van 0 tot 65535)
- Weight:
  Het gewicht van het record, wanneer er meerdere records met dezelfde prioriteit zijn (hoe lager dit nummer hoe eerder dit record wordt aangesproken, van 0 tot 65535)
- Port:
- De TCP of UDP poort waarop de service zou moeten werken
- Target:
  De hostnaam van de server welke de service biedt

Een voorbeeld van een SRV-record ziet er zo uit:

```
_sip._tcp.test.nl 86400 IN SRV 10 5 5060 sipserver.voorbeeld.com.
```

Een SRV-record aanmaken in DNSadmin

Om een eigen SRV-record aan te maken kiest u voor **Record toevoegen**. In de instructies hieronder wordt het bovengenoemde voorbeeld toegevoegd.

- Record:
  Hier komt de naam van de service en de naam van het protocol, met (over het algemeen) underscores. De waardes *_sip._tcp* staan in het voorbeeld.
- Type:
  Dit dient SRV te zijn.
- Content:
  Hier worden achtereenvolgens de *Weight*, de *Port* en de *Target* ingevuld, gescheiden door een spatie. De punt (.) achter de target is in DNSadmin niet nodig, deze wordt door DNSadmin zelf toegevoegd.
  De waardes uit het voorbeeld zijn *5 5060 sipserver.voorbeeld.com*
- Priority:
  Hier wordt de Priority ingevuld; in het voorbeeld is dat *10*
- TimeToLive:
  De Time To Live; in het voorbeeld is dat *86400*

Sla het record op met **Record toevoegen** en het SRV-record wordt ingesteld.

TXT-record

Een TXT-record is een record, welke een stukje *Tekst* bevat. Dit kan voor veel doeleinde gebruikt worden. Er zijn weinig restricties voor TXT-records, in principe kan er van alles worden opgegeven in dit record. Er zijn

echter wel verschillende mechanismes die gebruik maken van TXT-records. Enkele hiervan worden verderop beknopt omschreven.

Voor het toevoegen van een TXT-record kunt u de volgende stappen doorlopen. Er zal gebruik gemaakt worden van onderstaande voorbeeld:

```
Record: alinea.test.nl. IN TXT "Een stukje tekst voor dit domein"
```

Kies voor **Record toevoegen** om een TXT-record aan te maken. Geef de volgende gegevens op, om het voorbeeld hierboven in te stellen:

- **Record**: De naam van het subdomein. Uit het voorbeeld *alinea*, vul deze in.
- **Type**: het type dient TXT te zijn.
- **Content**: Hier wordt de gewenste waarde ingevuld, waarnaar het TXT-record dient te verwijzen. In het voorbeeld is dat *Een stukje tekst voor dit domein*, vul dit echter in zonder de quotes ("-symbool). Deze quotes worden DNSadmin zelf toegevoegd in het record.
- **TTL**: Stel de Time To Live in, in het voorbeeld is deze niet opgegeven. Wij adviseren de standaard waarden van *3600* aan te houden.

SPF

Voorheen waren er SPF-records, welke gebruikt werden om verzonden e-mail te kunnen verifiëren. Deze échte SPF-records worden nauwelijks nog gebruikt en zijn grotendeels al vervangen door TXT-records die beginnen met de waarde *v=spf1*. (De versie van het SPF / TXT-record wordt hieronder benoemd, namelijk versie 1).

SPF staat voor *Sending Policy Framework*, binnen dit record wordt aangegeven wie betrouwbare afzenders zijn van het domein. SPF wordt ook vaak vertaald naar *Sending Permitted From*, wat niet de officiële benaming is – maar wel aangeeft wat de functie is. Zoals hiervoor omschreven, het SPF-record geeft aan wie de domeinnaam allemaal opgeeft als betrouwbare afzender, van e-mailberichten.

Dit mechanisme wordt dan ook gebruikt, om spoofing en phishing tegen te gaan. Immers, als een kwaadwillende (bijvoorbeeld een hacker) e-mail verstuurd vanaf uw domeinnaam, dan kan een ontvanger denken dat u het zelf bent die de e-mail verstuurd heeft. Zo kunt u op het SPF-record van uw domeinnaam bijvoorbeeld opnemen, dat u alleen gebruik maakt van **QDC** en **Gmail**. Een hacker die uw e-mail adres nabootst vanaf bijvoorbeeld een **163.com** server, zal dan moeilijker een ontvanger bereiken. Voorwaarde hiervoor is wel dat de ontvanger controleert op SPF.

Uit dit voorbeeld zou naar voren kunnen komen dat de ontvanger een e-mail ziet vanaf een onbekende e-mailserver. De ontvangende mailserver kan er dan bijvoorbeeld voor kiezen de gehele e-mail te blokkeren. Het kan ook voorkomen dat de ontvangende e-mailserver twijfelt, in dat geval kan het ook zo zijn dat de e-mail in de ongewenste folder (spam) wordt geplaatst. Zo hoopt de ontvangende mailserver dat u als eindgebruiker extra oplet bij de e-mail, die in de spamfolder is geplaatst.

Uiteraard is het SPF-record niet het enige mechanisme waarop mailservers controleren. Spamfiltering is vaak nog vele malen complexer. Echter is een goed ingesteld SPF-record wel een goed begin, om uw eigen e-mailberichten als veilig(er) te bestempelen. Een nadeel is echter, dat er vergeten kan worden dat er een nieuwe partij e-mail namens uw domeinnaam wilt gaan verzenden. Als u bijvoorbeeld uw facturen door Exact, SnelStart of een ander administratie-platform laat afhandelen, dan kan het voorkomen dat er vergeten is die partij op te nemen in uw SPF-record. Het is dan goed denkbaar dat uw facturen bij uw klanten allemaal in de ongewenste e-mail belanden. Het nalopen en aanpassen van uw SPF-record kan in dat geval voor een vervolg mailing er wel voor zorgen dat de e-mailberichten dan in te toekomst wel netjes in de inbox van uw relaties terecht komen.

De opbouw van het SPF-record.

Zoals hierboven al kort aangegeven, wordt in het begin van het TXT-record aangegeven dat het een SPF-record betreft, door te beginnen met de waarde *v=spf1*. Hierna kunnen de volgende toevoegingen opgegeven worden.

- **a**
  Deze wordt gebruikt om een IP-adres van een hostname aan te duiden als een betrouwbare afzender. Hiervoor dient de hostname achter de a en een dubbele punt gezet te worden,

bijvoorbeeld: **a:mail.qdc.nl**. Het kan voorkomen dat er meerdere IP-adressen bestaan op de opgegeven hostname; in dat geval worden al die IP-adressen als betrouwbaar gezien.
Wordt er geen dubbele punt en hostname achter de **a** gezet, dan wordt het IP-adres (of IP-adressen) van de domeinnaam zonder voorloop aangemerkt als betrouwbaar.

- **mx**
  De waarde **mx** wordt gebruikt, om alle e-mailberichten als betrouwbaar aan te kaarten, welke worden verstuurd vanuit dezelfde mailservers als degene die genoemd zijn achter de MX-records van de domeinnaam. Net als hierboven bij de a kan er ook verwezen worden naar de MX-records van een andere domeinnaam, bijvoorbeeld **mx:anderdomein.nl**. In dat geval worden de bijbehorende mailservers, genoemd in de MX-records van de domeinnaam anderdomein.nl ook als betrouwbaar gezien.
- **ip4**
  De waarde **ip4** wordt gebruikt om e-mailberichten als betrouwbaar te markeren, welke afkomstig zijn ban het bijbehorende IP-adres. Een voorbeeld zou kunnen zijn **ip4:91.221.10.245**. Deze waarde wordt echter niet gebruikt zonder de dubbele punt (het IP-adres wordt altijd gespecificeerd). In plaats van een IP-adres mag er ook een IP-range worden opgegeven, bijvoorbeeld **ip4:91.221.150.245/32**. Zo zijn alle IP-adressen binnen die range gemarkeerd als betrouwbaar.
- **ip6**
  Net als bij ip4 worden hiermee IPv6 adressen als betrouwbaar opgegeven. Ook bij ip6 is het weer mogelijk om ranges op te geven.
- **include**
  Met een **include** waarde wordt er verwezen naar een ander **SPF-record**. Alle voorwaarden uit deze verwijzingen worden ook opgenomen (*included*) als betrouwbaar. Hier wordt veel gebruik van gemaakt, omdat veel mail-providers één (of meerdere) includes maken en deze doorgeven aan hun gebruikers.

Note: in sommige gevallen wordt er gevraagd een extra plus (het +-symbool) voor de gekozen waarde te zetten, om aan te geven dat de waarde geaccepteerd wordt. Dit is echter niet verplicht, zonder de plus werken de opgegeven waardes ook.

Een SPF-record wordt afgesloten (uitzonderingen daargelaten, zie alternatieve waardes) met een van de onderstaande waardes. Hiermee wordt aan de ontvangende mailserver doorgegeven, wat deze zou moeten doen met e-mailberichten welke niet voldoen aan de opgegeven waardes uit het SPF-record. Let er wel op, dat de SPF-controle alleen uitgevoerd wordt, als de ontvangende mailserver hier ook op controleert. Daarnaast kan (zoals eerder aangegeven) de ontvangende mailserver ook zelf nog (extra) mechanismes hebben, welke de SPF-records (en de uitkomst van de SPF-verificatie) overrulen.

- **~all**
  De waarde **~all** staat bekend als softfail. Als een e-mailbericht wordt verzonden door een server, welke niet voldoet aan de SPF-verificatie, dan wordt aangegeven dat het e-mailbericht mogelijk onbetrouwbaar is. Veelal resulteert dit, dat het bericht dan in de map met ongewenste e-mail (spam) afgeleverd wordt.
- **-all**
  De waarde **-all** staat bekend als hardfail. Als een e-mailbericht wordt verzonden door een server, welke niet voldoet aan de SPF-verificatie, dan wordt aangegeven dat het e-mailbericht altijd onbetrouwbaar is. Veelal resulteert dit, dat het bericht verwijderd wordt en helemaal niet aan zal komen bij de uiteindelijke ontvanger.
- **+all**
  De waarde **+all** geeft aan dat alle e-mailberichten geaccepteerd mogen worden. Het gebruik van deze waarde zorgt er eigenlijk voor, dat de gehele SPF-verificatie uitgevoerd wordt, maar dat elk e-mailbericht alsnog geaccepteerd mag worden. Wij adviseren om deze waarde dan ook niet te gebruiken.
- **?all**
  Als laatste is er nog de **?all** waarde. Hiermee wordt aangegeven dat er geen SPF-validatie uitgevoerd hoeft te worden. Ook hier worden dan alle e-mailberichten vanaf ongeautoriseerde servers toch toegelaten. Wij adviseren tevens om deze waarde niet te gebruiken, behalve voor bijvoorbeeld het zoeken naar problemen met het afleveren van uw e-mailberichten. Door de SPF-verificatie tijdelijk uit te zetten, kan er wel gecontroleerd worden of e-mail dan ineens wel wordt afgeleverd. Hieruit zou dan kunnen blijken dat er iets niet goed is geconfigureerd in het SPF-record.

Alternatieve waardes

Er bestaan nog meer waardes in SPF-records, welke hier niet omschreven gaan worden. De volgende drie waarden worden sporadisch nog wel eens gebruikt: **exists, redirect** en **exp**. Indien u een van deze waardes wenst te gebruiken, dan verzoeken wij u om dat op te nemen met de server beheerder van uw SMTP-server of mailserver. Zij kunnen u assisteren om een correct SPF-record op te bouwen met deze waarden erin verwerkt.

DMARC

DMARC staat voor *Domain-based Message Authentication, Reporting and Conformance*. Het is een policy in een DNS-record waarmee je aangeeft dat er gebruik gemaakt wordt van SPF en/of DKIM. Het wordt ook vaak gebruikt als toevoeging op SPF (en DKIM).

In een DMARC-record kunnen ook aanwijzingen worden opgenomen voor de ontvanger, over wat er eigenlijk moet gebeuren als bijvoorbeeld de SPF-verificatie faalt. DMARC wordt intussen al gebruikt door onder andere Gmail, Hotmail, Facebook, Microsoft, Yahoo, PayPal en AOL.

Net als bij de SPF-records wordt een DMARC-record ook als TXT-record opgenomen in de DNS-zone van een domeinnaam. Deze begint dan met **v=DMARC1**, waarmee wordt aangegeven dat het een DMARC-record is, met versie 1. Daarnaast wordt er (veelal) gebruik gemaakt van een subdomein, genaamd *_dmarc*.

Over het algemeen volgt daarna het beleid (de *policy*, vandaar de p), wat bijvoorbeeld opgevolgd dient te worden als de SPF-verificatie faalt. Voorbeelden zijn: **p=none** (doe niets), **p=reject** (weiger het e-mailbericht) of **p=quarantaine** (zet het e-mailbericht in de map ongewenst). Elke waarde wordt afgesloten met een puntkomma (het ;-symbool). Het record zal er dan ongeveer zo uit komen te zien:

```
Record: _dmarc.test.nl. IN TXT "v=DMARC1; p=none;"
```

Net als bij SPF geldt hier dat de gewenste policy niet per se uitgevoerd wordt door de ontvangende mailserver. Een goed ingestelde mailserver heeft zoals eerder benoemd ook eigen mechanismes om te bepalen of een e-mailbericht binnengehaald wordt, in de spamfolder gezet wordt, of in zijn geheel geweigerd wordt. De DMARC-instructie is slechts een (dringend) advies aan de ontvangende mailserver.

Voor het instellen van een DMARC-record adviseren wij u, om aan de serverbeheerder van de SMTP-server te vragen, hoe deze eruit moet komen te zien. Deze kunt u dan aan QDC doorsturen, zodat die op uw domeinnaam geïnstalleerd kan worden (of u configureert deze zelf in DNSadmin op uw domeinnaam). Gebruikt u een SMTP-server van QDC, dan zorgen wij ervoor dat het DMARC-record correct wordt ingesteld. Hier is wel een uitzondering voor domeinnamen, welke niet op onze nameservers draaien. Hiervoor kunnen wij wel de instructies doorgeven.

Site verificatie

Het kan voorkomen dat er een website aan een domeinnaam gekoppeld dient te worden, maar dat de website eigenaar vereist dat u aan kan geven dat u de eigenaar bent van dat domein. Zij kunnen dan vragen om een *Site verification* toe te voegen als TXT-record op uw domeinnaam. Zo verzekert de uitgever van de website zich ervan, dat u de eigenaar van de domeinnaam heeft (eigenlijk is het een verificatie, om te zien of u toegang heeft tot de DNS-zone van de domeinnaam).

Hieronder staat een fictief voorbeeld van zo een verificatie-record, wat gezien kan worden als een soort wachtwoord.

```
test.nl. IN TXT "google-site-verification=4-8Q0m6vQ7FMXDprkdfUf_7Qvc8"
```

URL-record

Een URL-record is eigenlijk niet echt een DNS-record. QDC heeft deze samen met onze leverancier ontwikkeld, om URL-forwarding mogelijk te maken. Hiermee kan een **hostname** doorgestuurd worden naar een vooraf ingestelde URL. De term URL staat voor **Uniform Resource Locator**, maar is beter bekend als *Webadres*. De URL kunt u terugvinden in de adresbalk van uw browser, begint met http of https.

Zoals hierboven gezegd, is het URL-record geen “echt” record. Het is eigenlijk een A-record, welke verwijst naar een door ons ingerichte forwarding server. Deze server stuurt vervolgens de bezoeker van de hostname door naar de ingestelde URL. Een dergelijke forward kan echter ook op andere manieren worden ingesteld dan op DNS-niveau. Zo kan dit op bijvoorbeeld op een webserver geregeld worden of het kan in een website zelf ingesteld worden.

Wat is URL-forwarding

URL-forwarding houdt in dat een domeinnaam of een subdomein (hostnaam) naar een (bestaande) URL verwezen wordt. Bezoekers hoeven hierdoor geen moeilijke of lange URL’s te onthouden: de bezoekers zetten gewoon de domeinnaam (met of zonder subdomein) in de webbrowser en deze zal automatisch het juiste adres vinden en weergeven. Dit uiteraard wel met de kanttekening dat de opgegeven URL bestaat en bereikbaar is.

URL-forwarding bij QDC kan op drie manieren worden ingesteld: met frame of zonder frame; zonder frame (redirect) kan dan tijdelijk of permanent. Wanneer er forwarding wordt ingesteld met frame, dan zal in de webbrowser het ingetypte adres blijven staan. Het ‘frame’ houdt stand, alle onderliggende pagina’s worden ingeladen, zonder dat deze zichtbaar worden in de adresbalk van de webbrowser. Bij een redirect forwarding zal de uiteindelijke URL / de doellocatie wel worden weergegeven in de adresbalk.

Een tijdelijke of een permanente redirect
Er zijn twee soorten redirects in te stellen, een permanente of een tijdelijke (temporary). De permanente redirect wordt ook wel een 301 redirect genoemd. Deze wordt over het algemeen het meest gebruikt. Bij een permanente redirect worden zoekmachines op de hoogte gebracht van de doorverwijzing. Wanneer er een permanente redirect gebruikt wordt, dan zullen zoekmachines (waaronder Bing, Yahoo en Google) de inhoud van de website beter kunnen indexeren.
De tijdelijke redirect wordt ook wel een 302 redirect genoemd. Het betreft hier een tijdelijke verwijzing, bijvoorbeeld een alternatieve actiepagina of een pagina met een melding dat de website in onderhoud is. De zoekmachines gaan er bij een tijdelijke redirect van uit, dat de oorspronkelijke pagina op korte termijn weer zal functioneren. In principe wordt er tegen zoekmachines verteld, dat de tijdelijke verwijzing niet geïndexeerd hoeft te worden. In de praktijk wordt de tijdelijke redirect niet veel gebruikt. De 302-redirect wordt bijvoorbeeld wel gebruikt voor webmail of inlogportalen, waarvan de eigenaar niet per se wilt dat deze te vinden zijn in een zoekmachine.

De term temporary suggereert dat er een tijdelijk verwijzing actief is. Er is echter geen standaard welke voorschrijft wanneer een redirect permanent of tijdelijk is, maar een termijn van 2 maanden wordt vaak aangehouden. Korter dan twee maanden is dan tijdelijk en langer is permanent; QDC raadt deze termijn ook aan als richtlijn.

Het aanmaken van een URL-record

Kies voor **Record toevoegen** om een URL-record aan te maken. Geef de volgende gegevens op, om het voorbeeld hierboven in te stellen, begin met het selecteren van het Type (URL):

- **Record**: De naam van het subdomein. Deze mag ook leeg zijn.
- **Type**: het type dient URL te zijn, kies deze bij voorkeur als eerste.
- **URL**: Hier kiest u als eerst voor **http:**// of **https:**// (hou er wel rekening mee, dat https wel moet werken voor de opgegeven URL, anders krijgen de bezoekers geen website te zien maar een foutmelding).
  Achter de keuze geeft u de rest van de gewenste URL op.
- **Type**: Hier kan gekozen worden voor het gewenste type: Iframe, Redirect permanent of Redirect temporary.
- **TTL**: Stel de Time To Live in, wij adviseren de standaard waarden van *3600* aan te houden.

Belangrijk!
Het is binnen DNSadmin niet mogelijk om een A-record en een URL-record aan te maken voor hetzelfde (sub)domein. Ook is een URL-record niet te wijzigen, naar een ander type record. In het geval dat u de forwarding wilt wijzigen naar (bijvoorbeeld) een A-record, dan dient u als eerste het URL-record te verwijderen. Ook andersom geldt hetzelfde. Een URL-record kan alleen aangemaakt worden voor een bepaald (sub)domein, als er nog geen A-record (of CNAME-record) bestaat. Deze dienen dan eerst verwijderd te worden.

PTR-record

Een PTR-record (of Pointer Record) staat ook bekend als een 'reverse record' of rDNS-record. Een PTR-record koppelt een IP-adres aan een hostnaam, in plaats van een hostnaam aan een IP-adres zoals met een A-record.

Als je een (eigen) mailserver hebt, dan is het verstandig ook een PTR-record aanmaken. Een PTR-record zet een IP-adres om in een hostnaam. Waar zou dat goed voor zijn? Mailservers controleren (soms) of de verzendende server van een e-mailbericht zich wellicht als een andere server voordoet, dan dat deze werkelijkheid is. Door de aanwezigheid van een PTR-record kan de ontvangende server controleren of de verzendende server bijvoorbeeld inderdaad de opgegeven mailserver is. Hieronder staat een voorbeeld van zo een fictief PTR-record:

```
Record: 166.227.79.212.in-addr.arpa 86400 IN PTR mail.qdc.nl
```

Het IP-adres wordt omgezet in een hostnaam. De mailserver groet elke server met EHLO (of HELO) mail.qdc.nl. Wanneer de ontvangende mailserver controleert op een PTR-record, vraagt deze het IP-adres van de hostnaam op, controleert of deze overeenkomt met het IP-adres waarmee de verbinding is gemaakt en doet daarna een reverse lookup op het IP-adres om te kijken of ook daar de hostnaam weer terugkomt. Is dit niet het geval, dan zal het e-mailbericht geweigerd kunnen worden.

Een PTR-record wordt in principe aangevraagd bij de provider en eigenaar van het IP-adres. Dit komt doordat de eigenaar van een IP-adres tevens verantwoordelijk is voor de reverse lookup zone. Daarnaast is het ook alleen mogelijk, als het een uniek (en vaak ook een vast) IP-adres is. Bij een gedeeld IP-adres zal de PTR vaak verwijzen naar iets van *shared.qdc.nl*. Een eigen uniek adres kan je vaak wel laten verwijzen naar een unieke hostname (bijvoorbeeld *kantoor.qdc.nl*).

Het aanmaken van een PTR-record is toegankelijk gemaakt in de DNS omgeving, enkel wordt dit niet ondersteund doordat QDC geen eigenaar is van de IP adressen. Daarnaast heeft het aanmaken hiervan ook vaak niet het gewenste resultaat. Wij adviseren dan ook om hier geen gebruik van te maken.

Wenst u toch een PTR-record te gebruiken, dan verwijzen wij u door naar de eigenaar van het IP-adres.

MX-record

Bij dit type record staat MX voor *Mail eXchange*. Dit type record wordt gebruikt om uw domeinnaam (of een subdomein) naar een (of meerdere) mailserver(s) te laten verwijzen. In ons volgende voorbeeld is er een MX-record aangemaakt voor *mail.test.nl*.

Door de aanwezigheid van dit record, wordt het internet verteld dat alle mail verzonden naar **@test.nl* wordt afgehandeld door de mailserver *mail.test.nl*. **Let op**: Er moet ook altijd een A-record (of een AAAA-record, echter werken nog niet alle providers met IPv6) zijn naar de naam van uw mailserver. Als deze niet bestaat, dan kan de mailserver niet gekoppeld worden aan een IP-adres. De e-mailberichten kunnen dan ook niet worden afgeleverd op de genoemde mailserver. Zie hieronder een voorbeeld, van hoe een mailserver correct staat ingesteld in DNSadmin, met een bijbehorend A-record.

mail.test.nl	A	91.221.150.245
test.nl	MX	mail.test.nl

Deze twee records behoren dan bij het onderstaande voorbeeld

```
Record: mail.test.nl. IN A 91.221.150.245
Record: test.nl. IN MX PRIO 10 mail.test.nl
```

Zoals hierboven aangegeven, kunnen er meerdere MX-records op dezelfde domeinnaam (of subdomeinnaam) geconfigureerd worden. Mede daarom dient er bij een MX-record ook een *Prio* (prioriteit) meegegeven te worden. Hier telt, hoe lager de Prio, hoe eerder het record wordt aangesproken. Is de

prioriteit van twee records hetzelfde? Dan wordt een van de genoemde MX-records *at random* aangesproken. Dit kan handig zijn om als soort “load balancer” op te treden, indien een mailserver erg druk is.

Verschillende waardes bij de prioriteiten kan echter handig zijn, om bijvoorbeeld gebruikt te kunnen maken van een noodserver (ofwel een fallback server). Als de eerste server (behorende bij het MX-record met de laagste prioriteit) tijdelijk niet beschikbaar is, dan zal een e-mailbericht afgeleverd worden bij het MX-record die daarop volgt. Dit kan net zo lang doorgaan, totdat de laatste MX-record is benaderd én ook niet gevonden kon worden. In dat geval wordt het e-mailbericht uiteindelijk gezien als “niet bezorgd” (undeliverable).

Admin account functies

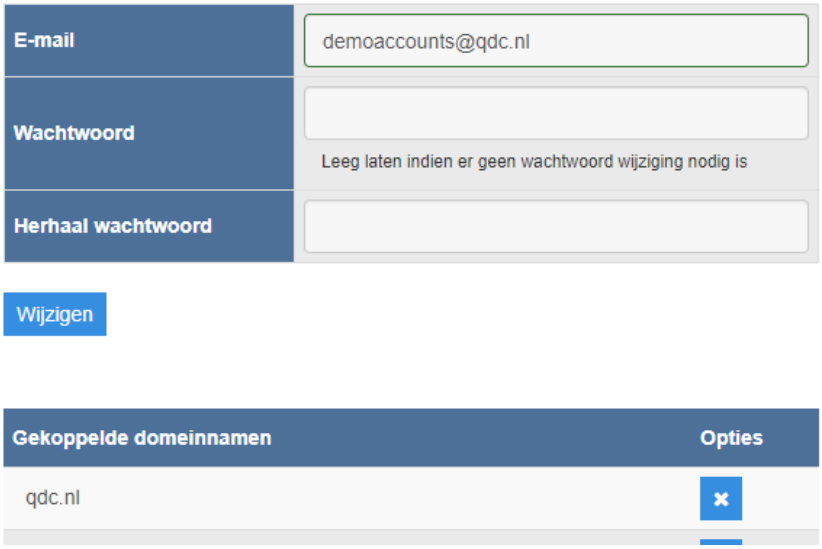
Indien u een admin account heeft, dan zijn er extra functies mogelijk binnen DNSadmin. Dit is te herkennen aan het extra tabblad **Subaccount overzicht** welke alleen zichtbaar is voor *admin accounts*. Heeft u dit tabblad niet, maar bent u wel geïnteresseerd om met subaccounts te werken? Dan kunt u dat met QDC opnemen.

Het subaccount overzicht

Als dit tabblad gekozen wordt, dan wordt er een overzicht getoond van alle subaccounts, welke gekoppeld zijn aan uw admin account (het hoofdaccount). Deze zijn gesorteerd op het door u opgegeven e-mailadres. Tevens kunt u de subaccounts verwijderen met het kruisje achter het E-mailadres en onder de Opties.

Let op: Momenteel kunt u zelf nog geen subaccounts aanmaken. U kunt deze wel verwijderen. Heeft u per ongeluk een subaccount verwijderd, dan kan QDC een nieuwe subaccount voor u aanmaken. Dat kan dan uiteraard wel met hetzelfde e-mailadres als het verwijderde account. Het nieuwe account is dan helaas niet langer gekoppeld aan de domeinnamen, welke voorheen gekoppeld waren. Dit zal opnieuw gekoppeld dienen te worden. Daarnaast zal het nieuwe account ook altijd initieel een nieuw wachtwoord ontvangen.

Door op het e-mailadres van een subaccount te klikken, wordt er een overzicht getoond van het gekozen subaccount.



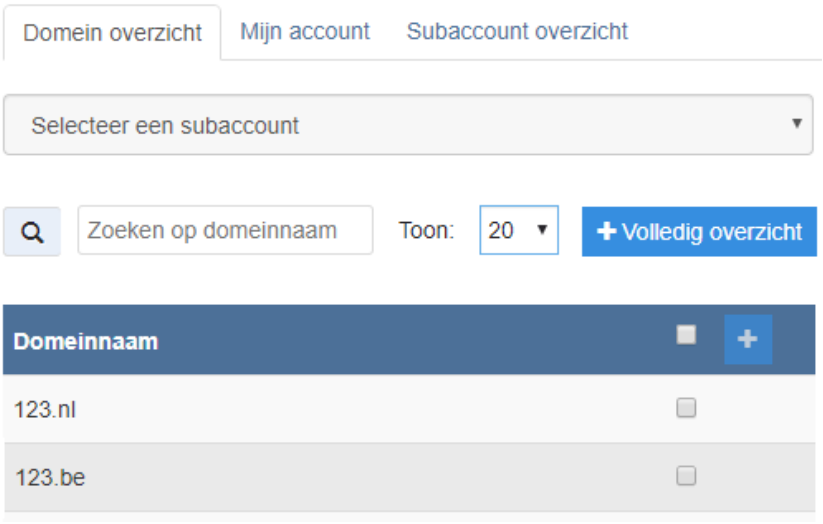
In dit overzicht kan het e-mailadres en het wachtwoord gewijzigd worden, van het subaccount. Zo kan de admin gebruiker de wachtwoorden van de subaccounts beheren. Zoals aangegeven, hoeft het wachtwoord niet per se te wijzigen als het e-mailadres wel gewijzigd wordt. Bevestig de wijziging van het e-mailadres en of het wachtwoord (vergeet deze niet te herhalen) door te kiezen voor de knop **Wijzigen**.

Onder het gedeelte om de gegevens van het subaccount te wijzigen, staat een overzicht van de gekoppelde domeinnamen. De domeinnamen, waar het subaccount toegang tot heeft, worden hier getoond. Om de toegang tot een domeinnaam in te trekken, kunt u gebruik maken van het X-symbool achter de domeinnaam, onder de **Opties**.

Als u hiervoor kiest, dan volgt er een bevestigingsverzoek of u de domeinnaam daadwerkelijk wilt ontkoppelen. Deze kunt u dan bevestigen of annuleren.

Domeinnamen koppelen aan een subaccount

Indien er een of meerdere domeinnamen gekoppeld dienen te worden aan een domeinnaam, dan kunt u de volgende stappen doorlopen. Ga hiervoor eerst naar het hoofdoverzicht van uw (admin) account.



Het bovenstaande scherm wordt getoond. Als admin account ziet u de extra mogelijk *Selecteer een subaccount* – als dropdown menu. U kunt hierop klikken en een subaccount kiezen, welke toegang mag hebben tot de hierna geselecteerde domeinnamen.

Gebruik vervolgens de zoekfunctie om de gewenste domeinnaam op te zoeken, meerdere domeinnamen is ook mogelijk. Selecteer vervolgens de domeinnamen, door een vinkje te zetten in het kleine selectievakje, achter de domeinnamen.

Indien u de gewenste domeinnamen heeft geselecteerd, veranderd de kleur van het plus-symbool enigszins. Deze knop kunt u nu aanklikken, om de gewenste domeinnamen te koppelen. Eerst volgt er nog een bevestigingsverzoek, waarmee de keuze nog ongedaan gemaakt kan worden.

Tip: Indien het gewenste subaccount niet voorkomt, dan kan het zijn dat deze niet (meer) bestaat. U kunt dan een verzoek indienen bij QDC om het subaccount alsnog aan te maken.
Staat de gewenste domeinnaam niet in het overzicht van de domeinnamen? Ook dan kan het zo zijn, dat deze niet op de nameservers van QDC aanwezig is; óf dat de domeinnaam (nog) niet gekoppeld is aan het hoofdaccount (het admin account). Ook daarvoor kunt u een verzoek indienen bij QDC, zodat er gezamenlijk gekeken kan worden of de domeinnaam toegevoegd kan worden.

Uitleg van diverse begrippen

Domain Name Server (DNS)

Op het internet wordt data steeds tussen servers uitgewisseld, welke allemaal werken op een of meerdere IP-adressen. Een IP-adres is een uniek getal waaronder u op internet bekend bent (bijvoorbeeld 8.8.8.8 voor een IPv4 adres). Domain name servers beheren welke hostnamen aan welke IP-adressen gekoppeld zijn, met daarbij nog een aantal varianten op verschillende types.

TTL

Hieronder staat uitgebreider toegelicht, waarvoor TTL staat.

Wanneer een gebruiker een domeinnaam intikt in een browser, dan zal er een *lokaal* geconfigureerde DNS-server het overeenstemmende IP-adres op het internet opzoeken. Dit IP-adres wordt dan gecached door die *lokale* name server, zodat er niet nogmaals een connectie gevraagd hoeft te worden met dat domein om het IP-adres op te zoeken.
De periode dat de DNS-informatie in de cache blijft, kan worden bepaald door gebruik te maken van de opgegeven waarde bij de TTL (Time To Live). Als hier gebruik van gemaakt wordt, dan zal dit stukje *cache* na afloop van de TTL verwijderd worden (in dit stukje cache stond dan welk IP-adres er bij de domeinnaam hoorde). Hierna zal er bij een nieuw verzoek naar dezelfde domeinnaam, opnieuw gezocht moeten worden naar het bijbehorende IP-adres.

Uiteraard kan het ook voorkomen dat een computer zelf ook bijhoudt welke IP-adressen corresponderen bij diverse domeinnamen; of een browser houdt zelf een stukje internetgeschiedenis bij. Naast deze computers kan deze taak ook nog eens worden bijgehouden door routers of modems in het netwerk. Soms kan het dan ook helpen om af en toe uw internetgeschiedenis en cache van uw computers, programma's en netwerken te legen (ook wel flush genoemd).

Afhankelijk van het type record staat de TTL bij ons op 600 (10 minuten) of 86400 (24 uur). Voor een goede werking van de DNS adviseren wij deze instellingen niet aan te passen.

URL

URL staat voor Uniform Resource Locater. Een URL is een gestructureerde naam die verwijst naar een begrijpelijk stuk data. Een URL bestaat uit een protocol, domeinnaam en eventueel een poortnummer.

https://	www.test.nl	443
Protocol	Domeinnaam test.nl	poortnummer

Een URL is het adres wat bijvoorbeeld in uw webbrowser in de adresbalk wordt getoond.

CAA-records

Een Certificate Authority Authorization record, oftewel een CAA DNS record, is ontworpen om domein eigenaren de mogelijkheid te bieden om aan te geven welk CA root certificaat gebruikt mag worden om certificaten mee te ondertekenen voor het domein in kwestie. Omdat dit certificaat toebehoort aan een bepaalde certificaat autoriteit, kan hiermee effectief aangegeven worden welke certificaten uitgegeven mogen worden voor een domein. Dit voorkomt dat het uitgeven van een certificaat door een andere CA dat de gekozen CA gedaan kan worden.
Elke uitgever van SSL-certificaten is verplicht om te controleren of een domeinnaam een CAA-record heeft. Als er in de DNS van een domeinnaam een of meerdere CAA-records aanwezig zijn, dan dient een van deze records (of het enige record) aan te geven dat de SSL-uitgever het domein ook mag beveiligen. Alleen dan kan de uitgever van het SSL-certificaat het domein ook daadwerkelijk beveiligen.
Indien er in de DNS van een domeinnaam geen gebruik gemaakt wordt van een of meerdere CAA-records, dan kan een SSL-uitgever altijd een certificaat uitgeven.

DNSSEC

DNSSEC (DNS Security Extensions) is een techniek, welke voor een extra beveiliging zorgt voor de bezoekers van uw domeinnaam.

DNSSEC voegt een digitale handtekening toe aan de DNS-informatie. Doordat er gecontroleerd wordt of deze digitale handtekening klopt, weet een bezoeker zeker dat wanneer jouw site bezocht, ook echt jouw site getoond wordt (en niet een andere site, bijvoorbeeld een phishing site). Daarnaast werkt deze beveiliging ook voor het e-mailverkeer van de beveiligde domeinnaam.

Onze nameservers steunen DNSSEC, zodat in principe alle domeinnamen hiermee beveiligd kunnen worden. Voor bijna alle domeinnamen (voornamelijk .NL, .BE en .EU) welke door QDC zijn geregistreerd, verzorgen wij dat de DNSSEC beveiliging wordt aangezet.
Maakt u gebruik van onze nameservers, maar zijn de domeinnamen niet bij QDC geregistreerd? Dan kunt u alsnog gebruik maken van DNSSEC. U kunt met ons opnemen, hoe u dat aangeeft bij uw registry.

Maakt u geen gebruik van onze nameservers, maar zijn uw domeinnamen wel bij QDC geregistreerd? Dan kunnen wij u wellicht ook assisteren met het beveiligen van die domeinnamen met DNSSEC. Ook dan kunnen wij gezamenlijk de domeinnamen proberen te beveiligen. Het is dan echter wel van belang dat de gekozen nameservers DNSSEC ondersteunen.