Domena i strefa publiczna

Rejestrator, dostawca DNS, odnowienia, blokady, rekordy, DNSSEC i CAA.

- Domena i strefa publiczna: rejestrator, dostawca DNS, odnowienia i blokady
- Rekordy publiczne Zielonej, DNSSEC i CAA

Domena i strefa publiczna: rejestrator, dostawca DNS, odnowienia i blokady

Poziom: podstawy

Dotyczy: domena zielona.example, rejestrator (dla .pl partner NASK), Azure DNS, deSEC i Cloudflare jako warianty, Azure CLI 2.x, dig, whois, GLPI, stan na 26 października 2026

Czas: ~30 min

Domena to zasób firmy jak umowa najmu: ma właściciela, termin, opłatę i kogoś, kto pilnuje odnowienia. Strona rozdziela trzy role, które często myli się w jedną (rejestr, rejestrator, dostawca DNS), uzasadnia, gdzie trzymamy strefę `zielona.example`, i zbiera to, co musi być spisane, żeby domena nie wygasła ani nie została przeniesiona bez naszej wiedzy.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu domenę `zielona.example` mamy u rejestratora, a strefę publiczną w Azure DNS, w tej samej subskrypcji co `edge-az01` (grupa zasobów `rg-dns`). Wariant bez Microsoftu to strefa w deSEC albo w Cloudflare, opisany w tabeli niżej; rekordy i procedury na kolejnych stronach są w nim takie same, różni się tylko narzędzie do ich zmiany.

Skróty użyte na tej stronie (22)

Skrót	Co znaczy
ACME	Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku
API	Application Programming Interface: sposób, w jaki programy rozmawiają ze sobą
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu
DKIM	DomainKeys Identified Mail: cyfrowy podpis wiadomości e-mail
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

Skrót	Co znaczy
DNS-01	sposób potwierdzenia domeny w ACME: urząd certyfikacji każe opublikować jednorazowy rekord TXT _acme-challenge i sprawdza go w DNS; działa bez portu 80 i pozwala na certyfikat wieloznaczny
DNSSEC	DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona
FAQ	Frequently Asked Questions: zbiór najczęściej zadawanych pytań z odpowiedziami
GLPI	Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01
HTTP-01	sposób potwierdzenia domeny w ACME: urząd certyfikacji pobiera jednorazowy plik z adresu /.well-known/acme-challenge/ na porcie 80 naszego serwera
ICANN	Internet Corporation for Assigned Names and Numbers: organizacja założona w 1998 roku, która ustala zasady dla domen globalnych i akredytuje rejestratorów
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
NASK	Naukowa i Akademicka Sieć Komputerowa: państwowy instytut badawczy, który prowadzi rejestr domen .pl i przyjmuje zgłoszenia przez rejestratorów (partnerów)
RDAP	Registration Data Access Protocol: następca WHOIS, zwraca dane o domenie (rejestrator, daty, statusy) w uporządkowanym formacie JSON; dla domen globalnych źródło rozstrzygające od 28 stycznia 2025
REST	sposób budowania API przez zwykłe żądania HTTP (GET, POST) zamiast osobnego protokołu
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
TTL	Time To Live: czas życia rekordu lub danych
TXT	typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej
WHOIS	stary protokół i polecenie do sprawdzania, kto i u jakiego rejestratora ma domenę, kiedy ona wygasa i jakie ma blokady

Fiszka

Polecenia `dig` i `whois` wykonujemy z dowolnego Linuksa, najlepiej spoza sieci Zielonej, żeby nie trafić w wewnętrzną strefę na `dc01` (split-brain). Polecenia `az` wykonujemy w Azure Cloud Shell albo na stacji administratora po `az login`, kontem z rolą właściciela grupy zasobów `rg-dns`.

TYLKO ODCZYT

Odczyt serwerów nazw domeny: dig NS

```
dig +short NS NazwaDomeny
```

Pokazuje, które serwery odpowiadają za domenę, czyli gdzie naprawdę leży strefa. Gdy wynik nie zgadza się z tym, co mamy w panelu dostawcy DNS, zmiany w panelu nie mają żadnego skutku.

Przykład:

```
ns1-07.azure-dns.com.
ns2-07.azure-dns.net.
ns3-07.azure-dns.org.
ns4-07.azure-dns.info.
```

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **dig** = domain information groper: odpytywanie DNS

TYLKO ODCZYT

Odczyt rekordu SOA strefy: dig SOA

```
dig +noall +answer SOA NazwaDomeny
```

SOA to „metryczka” strefy: główny serwer, adres administratora, numer wersji i czasy. Pole na końcu to czas, przez który inni pamiętają odpowiedź „nie ma takiej nazwy”.

Przykład (poglądowy; numer wersji i czasy w SOA ustawia dostawca DNS, swoje odczytujemy w portalu albo tym poleceniem):

```
zielona.example.␣3600␣IN␣SOA␣ns1-07.azure-dns.com. azuredns-hostmaster.microsoft.com. 1 3600
300 2419200 300
```

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **dig** = domain information groper: odpytywanie DNS

TYLKO ODCZYT

Porównanie odpowiedzi wszystkich serwerów nazw: dig @serwer

```
for ns in $(dig +short NS NazwaDomeny); do echo "$ns"; dig +short SOA NazwaDomeny @"$ns"; done
```

Każdy serwer z listy NS powinien podać ten sam rekord SOA. Różnica oznacza, że jeden z serwerów jest stary albo obcy, na przykład po przenosinach strefy od rejestratora.

□□ TYLKO ODCZYT

Odczyt daty wygaśnięcia i statusu domeny: whois

```
whois NazwaDomeny
```

Szukamy pól z datą odnowienia albo wygaśnięcia (w rejestrze `.pl` „renewal date”, w domenach globalnych „Registry Expiry Date”), nazwy rejestratora, statusów blokad (`clientTransferProhibited` w domenach globalnych) i stanu DNSSEC. Dla domen globalnych źródłem rozstrzygającym jest od 28 stycznia 2025 roku protokół RDAP, a klasyczny `whois` bywa niepełny; układ pól zależy od rejestru.

□□ **DNSSEC** = DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona · **RDAP** = Registration Data Access Protocol: następca WHOIS, zwraca dane o domenie (rejestrator, daty, statusy) w uporządkowanym formacie JSON; dla domen globalnych źródło rozstrzygające od 28 stycznia 2025 · **whois** = who is: wypisuje dane o domenie z rejestru, czyli rejestratora, daty utworzenia i wygaśnięcia, serwery nazw i statusy blokad

□□ ZMIENIA SYSTEM

Utworzenie strefy publicznej w Azure DNS: az network dns zone create

```
az network dns zone create --resource-group NazwaGrupyZasobow --name NazwaDomeny
```

(gdzie `NazwaGrupyZasobow` to grupa przeznaczona tylko na strefy DNS, w Zielonej `rg-dns`)

Tworzy pustą strefę z rekordami SOA i NS. Strefa nie działa w internecie, dopóki u rejestratora nie wpiszemy jej serwerów nazw.

□□ **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **az** = Azure CLI: narzędzie chmury Microsoftu

□□ TYLKO ODCZYT

Odczyt serwerów nazw nadanych strefie: az network dns zone show

```
az network dns zone show --resource-group NazwaGrupyZasobow --name NazwaDomeny --query nameServers --output tsv
```

Te cztery nazwy przepisujemy do panelu rejestratora jako serwery DNS domeny.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **az** = Azure CLI: narzędzie chmury Microsoftu

KLIKAMY W INTERFEJSIE

Zmiana serwerów nazw u rejestratora: panel rejestratora

```
Panel rejestratora → Domeny → NazwaDomeny → Serwery DNS (delegacja) → Własne serwery nazw → cztery nazwy z Azure DNS → Zapisz
```

Nazwy pozycji menu różnią się między rejestratorami, sens jest ten sam: domena przestaje wskazywać DNS rejestratora i zaczyna wskazywać naszego dostawcę.

DNS = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

ZMIENIA SYSTEM

Nadanie uprawnień do jednej strefy: az role assignment create

```
az role assignment create --assignee IdAplikacji --role "DNS Zone Contributor" --scope IdStrefy
```

(gdzie `IdAplikacji` to identyfikator konta aplikacji, którego używa Traefik albo skrypt, a `IdStrefy` to pełny identyfikator strefy z `az network dns zone show --query id`)

Konto automatu dostaje prawo zmiany rekordów tylko w tej strefie, a nie w całej subskrypcji. Dokumentacja klienta ACME lego dla dostawcy `azuredns` opisuje też węższy wariant: odczyt strefy i zapis tylko rekordów `_acme-challenge`.

ACME = Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku · **az** = Azure CLI: narzędzie chmury Microsoftu · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

KLIKAMY W INTERFEJSIE

Wpis domeny w rejestrze zasobów: GLPI

```
pomoc.zielona.example → Management → Domains → Add → nazwa, data wygaśnięcia,
rejestrator, osoba odpowiedzialna → Records: NS, MX
```

W GLPI moduł domen przechowuje nazwę, datę wygaśnięcia i powiązane rekordy. Nazwy pól w naszej wersji GLPI sprawdzamy w interfejsie, a sam wpis zastępuje karteczkę z datą odnowienia.

ZRZUT EKRANU DO UZUPEŁNIENIA

Zrzut do uzupełnienia: ekran Management → Domains w GLPI na `pomoc.zielona.example` z domeną `zielona.example`, widoczną datą wygaśnięcia i rekordami NS z Azure DNS w zakładce Records.

GLPI = Gestionnaire Libre de Parc Informatique: otwarty system do zgłoszeń, inwentarza i bazy wiedzy IT; w Zielonej działa w kontenerze na docker01 · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP

Z życia wzięte

Z ŻYCIA WZIĘTE

Czwartek, 14:30. Tomek chce dodać rekord dla nowego sklepu i loguje się do panelu rejestratora, gdzie od lat „była strefa”. Dodaje rekord, czeka godzinę, a `dig` z telefonu nadal nic nie pokazuje. Okazuje się, że rok wcześniej strefę przeniesiono do Azure DNS, a w panelu rejestratora została jej martwa kopia, której nikt już nie pyta. Od tego dnia w panelu rejestratora wisi notatka „strefa jest w Azure DNS, rg-dns”, a pierwsza komenda Tomka przy każdym rekordzie to `dig +short NS`.

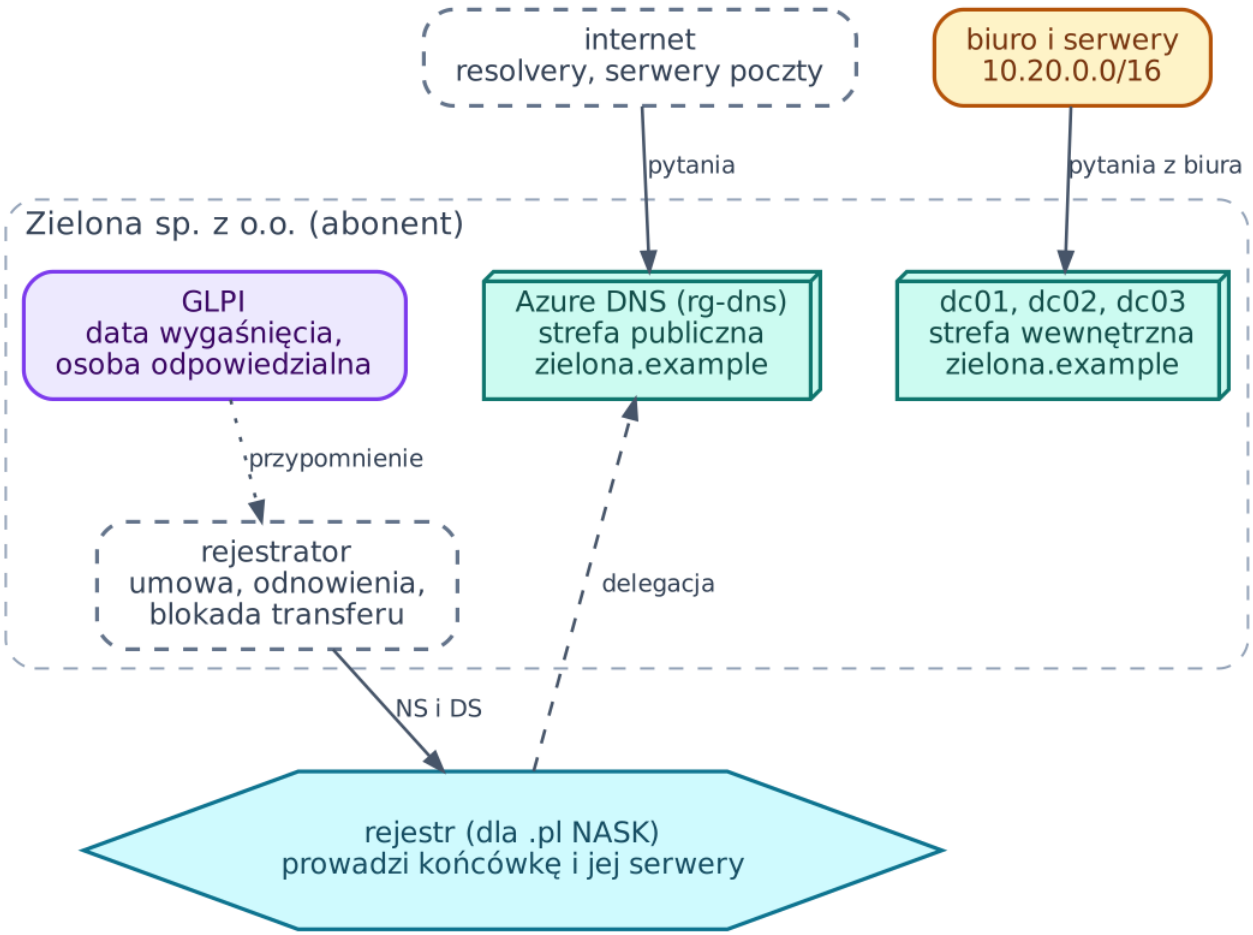
Jak to działa

Rozwiń: jak to działa pod spodem

Pojęcie: strefa publiczna. Zbiór rekordów DNS domeny, który widzi cały internet. Leży na serwerach nazw dostawcy DNS, a rejestr końcówki wie tylko, które to serwery (rekordy NS) i, przy DNSSEC, jaki jest odcisk klucza strefy (rekord DS).

Pojęcie: delegacja. Wpis w strefie nadrzędnej, który mówi „za tę domenę odpowiadają tamte serwery”. Delegację zmieniamy u rejestratora, a rejestrator przekazuje ją do rejestru. Bez zmiany delegacji nowy dostawca DNS może mieć idealną strefę, której nikt nie zobaczy.

Trzy role często siedzą w jednej firmie, dlatego łatwo je pomylić. Rejestr (dla `.pl` NASK) prowadzi końcówkę, rejestrator sprzedaje nam domenę i przekazuje do rejestru delegację i rekord DS, a dostawca DNS trzyma strefę i odpowiada na pytania. Rejestrator może być jednocześnie dostawcą DNS, ale nie musi, i w Zielonej nie jest.



Rysunek 1. Trzy role wokół domeny: rejestr .pl prowadzi końcówkę, rejestrator przekazuje delegację i rekord DS, dostawca DNS trzyma strefę publiczną, a wewnętrzna strefa na dc01 i dc02 to osobny świat dla biura (kliknięcie otwiera pełny rozmiar)

Gdzie trzymamy strefę zielona.example

Strefę publiczną możemy trzymać w kilku miejscach. O wyborze decydują cztery rzeczy: czy dostawca ma interfejs API do zmiany rekordów (potrzebny do certyfikatów przez DNS-01 i do przełączania przy awarii łącza), czy podpisuje strefę DNSSEC, jak krótki TTL pozwala ustawić i czy uprawnienia da się zawęzić do jednej strefy.

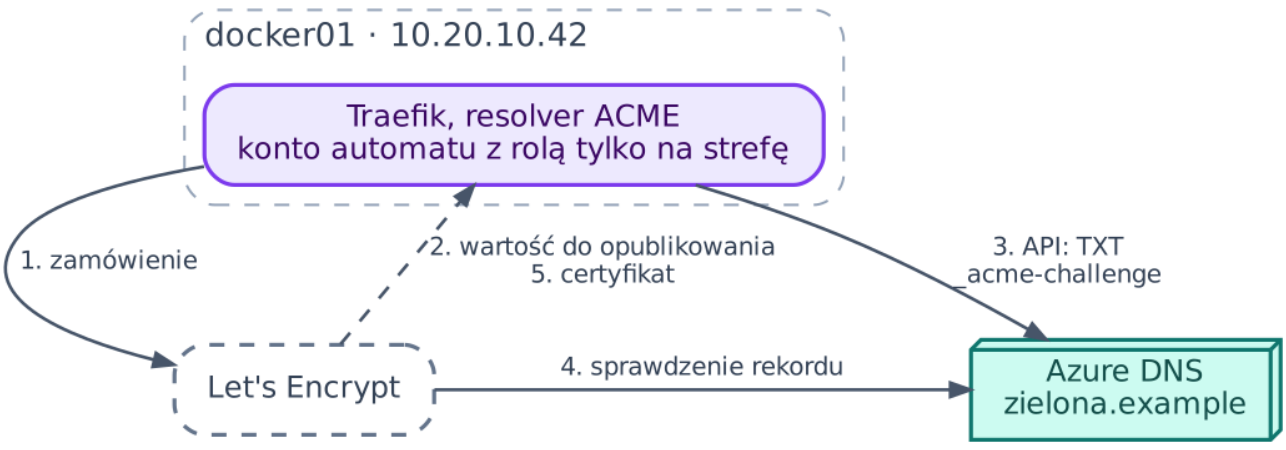
Gdzie	API i DNS-01	DNSSEC	Najkrótszy TTL	Uwagi
DNS rejestratora	zależnie od firmy, często brak	zależnie od firmy	zależnie od firmy	najprościej na start, ale bez API nie zautomatyzujemy certyfikatów ani przełączania
Azure DNS	tak (Azure CLI, PowerShell, REST, dostawca `azuredns` w lego i Traefiku)	tak, ogólnie dostępne od lutego 2025	dowolny, ustawiamy sami	uprawnienia przez role Azure na strefę, brak transferów strefy, opłata za strefę i zapytania według cennika Azure
deSEC (organizacja non-profit z Berlina)	tak, tokeny ograniczone do domeny albo rekordu	tak, domyślnie dla każdej strefy	3600 s, wyjątki na prośbę do wsparcia	bez opłat, bez Microsoftu; krótki TTL dla `vpn` wymaga wyjątku
Cloudflare DNS	tak, tokeny ograniczone do strefy	tak, włączane jednym przełącznikiem	60 s w planach innych niż Enterprise	plan bezpłatny wystarcza dla samego DNS
własny serwer na `dc01` albo BIND w DMZ	tak (RFC 2136)	tak, ale klucze pilnujemy sami	dowolny	wystawia kontroler domeny albo kolejny serwer do internetu, jedno łącze to jeden punkt awarii

Wybieramy Azure DNS z trzech powodów. Zielona ma już subskrypcję z `edge-az01`, więc nie dochodzi nowy dostawca ani nowe konto z MFA. Strona Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate potrzebuje rekordu `vpn` z TTL 300 sekund i zmiany przez API przy awarii, a deSEC domyślnie tego nie da. Wreszcie Traefik na `docker01` umie pobierać certyfikaty przez DNS-01 od Azure DNS, co przyda się, gdy usługa nie jest wystawiona na porcie 80.

Wariant bez Microsoftu to deSEC (gdy krótki TTL nie jest potrzebny albo dostaniemy wyjątek) albo Cloudflare. Dla obu Traefik ma gotowych dostawców DNS-01, a reszta tej książki działa bez zmian. Strefy publicznej nie stawiamy na `dc01`: kontroler domeny nie powinien odpowiadać internetowi, a jego strefa `zielona.example` służy biuru, jak opisuje DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain.

> ⚠ Azure DNS nie obsługuje transferów strefy, a w jego dokumentacji nie znaleźliśmy aktualizacji dynamicznych według RFC 2136: rekordy zmieniamy przez portal, Azure CLI, PowerShell albo REST API. Poddomenę `ddns.zielona.example` z wariantu dynamicznego DNS na stronie o łączach obsługujemy więc albo osobnym serwerem z RFC 2136 (delegacja rekordem NS), albo skryptem, który zmienia rekord przez API. Decyzję zostawiamy autorowi strony o łączach.

Pojęcie: DNS-01. Sposób, w jaki urząd certyfikacji (na przykład Let's Encrypt) sprawdza, że panujemy nad domeną: każe opublikować rekord TXT `_acme-challenge.nazwa` z jednorazową wartością. Działa bez otwierania portu 80 i jako jedyny pozwala na certyfikat wieloznaczny, ale wymaga API u dostawcy DNS.



Rysunek 2. Certyfikat przez DNS-01: Traefik na docker01 prosi Let's Encrypt o certyfikat, dostaje wartość, zapisuje ją przez API w Azure DNS jako rekord TXT _acme-challenge, a urząd sprawdza rekord i wystawia certyfikat (kliknięcie otwiera pełny rozmiar)

Dziś Traefik w Zielonej pobiera certyfikaty przez HTTP-01 na porcie 80, jak opisuje Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01. Przejście na DNS-01 i skracanie ważności certyfikatów opisuje strona Certyfikaty publiczne i ACME: Let's Encrypt z DNS-01, skracanie ważności i step-ca; ta strona daje jej strefę z API i konto z wąskimi uprawnieniami.

Domena jako zasób firmy

Domenę gubi się zwykle nie przez atak, tylko przez zaniedbanie: wygasa karta płatnicza, przypomnienie przychodzi na skrzynkę osoby, która odeszła, albo nikt nie pamięta hasła do konta u rejestratora. Poniższa lista to minimum, które spisujemy raz i przeglądamy co roku przed audytem.

Co	Jak w Zielonej	Dlaczego
Abonent	Zielona sp. z o.o., nie osoba prywatna	domena należy do firmy, także po odejściu pracownika
Konto u rejestratora	konto firmowe na adres `domeny@zielona.example` i drugi adres poza tą domeną, MFA, dwóch administratorów, hasło i kody odzyskiwania w Vaultwardenie	gdy domena nie działa, poczta w niej też nie, więc przypomnienie musi dojść gdzie indziej
Konto u dostawcy DNS	dostęp przez role Azure dla dwóch administratorów z MFA, konto automatu tylko do strefy	zmiana NS albo MX przez obcego to przejęcie poczty
Odnowienie	automatyczne, na kilka lat naprzód, faktura na firmę, data w GLPI i alarm w Zabbixie na 60 i 30 dni przed	jeden przegapiony termin wyłącza pocztę, VPN i stronę
Blokada transferu	w domenach globalnych status `clientTransferProhibited` włączony w panelu; w `.pl` transfer wymaga kodu AuthInfo od obecnego rejestratora, a dla ważnych domen rozważamy płatną usługę Registry Lock w rejestrze	utrudnia przeniesienie domeny do innego rejestratora bez naszej zgody
Kod AuthInfo i dane kontaktowe	kod generujemy tylko na czas transferu, dane kontaktowe sprawdzamy raz w roku	stary adres kontaktowy to najczęstsza droga przejęcia konta
Rejestr	wpis w GLPI (Management → Domains) i dostawcy w rejestrze dostawców ISO 27001	audytor pyta, kto, gdzie i do kiedy

> □□ Terminów odnowienia i zasad transferu nie podajemy w liczbach, bo zależą od rejestru i rejestratora. Dla domen globalnych ICANN prowadzi przegląd zasad transferu, więc szczegóły sprawdzamy w regulaminie naszego rejestratora przy każdej zmianie.

Alarm o wygasającej domenie i certyfikatach w Zabbixie opisze rozdział „Zabbix w całej Zielonej” w książce o Zabbixie. Do tego czasu raz w miesiącu sprawdzamy datę poleceniem `whois` z Fiszki.

Częste błędy

Objaw	Przyczyna	Co robimy
Rekord dodany w panelu nie działa nawet po dobie	strefę trzyma inny dostawca niż ten, w którego panelu pracujemy	`dig +short NS NazwaDomeny`, zmiany robimy tylko tam, gdzie wskazuje delegacja
Część użytkowników widzi stary adres, część nowy	jeden z serwerów NS to stary dostawca albo stara kopia strefy	porównanie SOA na każdym serwerze z Fiszki, poprawiamy delegację u rejestratora
Przypomnienie o odnowieniu nie dotarło	adres kontaktowy prywatny albo w tej samej domenie, która wygasła	adres kontaktowy firmowy i drugi poza domeną, data w GLPI i alarm
Po zmianie NS poczta przez kilka godzin trafia w próżnię	nowa strefa nie miała jeszcze kompletu rekordów (MX, SPF, DKIM)	najpierw kopiujemy i sprawdzamy całą strefę u nowego dostawcy, dopiero potem zmieniamy delegację
Domena „zniknęła” po zmianie dostawcy DNS przy włączonym DNSSEC	u rejestratora został rekord DS starego klucza	procedura DNSSEC ze strony Rekordy publiczne Zielonej, DNSSEC i CAA: DS usuwamy przed przenosinami
Traefik nie dostaje certyfikatu przez DNS-01	konto automatu nie ma roli na strefie albo wskazuje złą subskrypcję	`az role assignment list --scope IdStrefy`, log Traefika

□□ Ćwiczenia

1. Tomek mówi, że „domena jest u rejestratora”. Jakie dwie różne rzeczy może mieć na myśli i jak sprawdzamy, która jest prawdą dla `zielona.example`?

Odpowiedź

Może chodzić o rejestrację (rejestrator sprzedał domenę i przekazuje delegację do rejestru) albo o strefę (rejestrator trzyma rekordy DNS). Rejestrację widać w `whois`, a to, kto trzyma strefę, w `dig +short NS`. W Zielonej rejestrację ma rejestrator, a strefę Azure DNS.

1. Dlaczego adres kontaktowy u rejestratora nie powinien być tylko w domenie `zielona.example`?

Odpowiedź

Gdy domena wygaśnie albo jej strefa przestanie działać, poczta w tej domenie też przestaje działać, więc ostrzeżenie od rejestratora nie dojdzie. Drugi adres poza domeną (inna domena firmy albo skrzynka u innego dostawcy) przerywa to błędne koło.

1. Pan Zbigniew pyta, czemu nie trzymamy strefy publicznej na `dc01`, „skoro i tak tam jest DNS”. Dwa argumenty?

Odpowiedź

Po pierwsze kontroler domeny nie powinien odpowiadać na zapytania z internetu, bo to otwiera najcenniejszy serwer firmy na ataki. Po drugie strefa publiczna na jednym łączu Zielonej przestaje działać przy każdej awarii łącza, razem z pocztą i VPN, a dostawca DNS ma serwery w wielu miejscach.

1. Dlaczego przed zmianą delegacji u rejestratora kopiujemy całą strefę do nowego dostawcy i sprawdzamy ją zapytaniami prosto do nowych serwerów?

Odpowiedź

Bo od chwili zmiany NS internet zaczyna pytać nowe serwery. Jeżeli brakuje na nich MX, SPF albo DKIM, poczta przychodząca gubi się albo wychodząca trafia do spamu. Zapytanie `dig @nowy_serwer` pozwala sprawdzić strefę, zanim ktokolwiek z niej skorzysta.

Powiązane: Domena i DNS publiczny: od HOSTS.TXT do DMARC · Rekordy publiczne Zielonej, DNSSEC i CAA · DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain · Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate · GLPI w Zielonej: zgłoszenia, SLA i katalog usług na docker01 · Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01

Źródła (odczyt 26 października 2026): learn.microsoft.com: Azure DNS FAQ (brak transferów strefy, brak sprzedaży domen, DNSSEC), „DNS zones and records” (typy rekordów, limity TXT), „How to sign your Azure Public DNS zone with DNSSEC”; mc.merill.net AZ479465 (DNSSEC w Azure DNS ogólnie dostępny, 3 lutego 2025) · go-acme.github.io/lego, dostawca `azuredns` (metody uwierzytelniania, role) · jpmens.net, „A look at domain hosting with deSEC” (4 marca 2025: non-profit, DNSSEC domyślnie, tokeny, TTL 3600 s) · developers.cloudflare.com, TTL (60 s, 30 s w Enterprise) · icann.org, „Launching RDAP; Sunsetting WHOIS” (28 stycznia 2025) · dns.pl, historia rejestru (Registry Lock od marca 2019) · glpi-user-documentation.readthedocs.io, Management → Domains.

Rekordy publiczne Zielonej, DNSSEC i CAA

Poziom: średnio

Dotyczy: strefa publiczna zielona.example w Azure DNS, Azure CLI 2.x, dig i delv z BIND 9, Resolve-DnsName, DNSSEC, CAA według RFC 8659 i RFC 8657, stan na 26 października 2026

Czas: ~40 min

Spis wszystkich rekordów, które Zielona pokazuje internetowi, z odpowiedzią „po co jest każdy z nich", oraz dwa zabezpieczenia strefy: podpis DNSSEC, który chroni odpowiedzi przed podmianą, i rekord CAA, który mówi, kto może wystawić certyfikat dla naszych nazw. Wracamy tu przy każdej nowej usłudze widocznej z internetu i przy każdej zmianie dostawcy DNS.

ZAŁOŻENIA SCENARIUSZA

w tym ćwiczeniu poczta działa w podejściu A (MailCow na `docker01`), Zielona ma jedno stałe łącze `wan1` z adresem 203.0.113.10, a maszyna `edge-az01` (203.0.113.60) przyjmuje pocztę jako zapasowy MX według wariantu b ze strony Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate. Strona firmowa stoi u zewnętrznego hostingu pod adresem 203.0.113.80. Rekordy poczty dla Microsoft 365 i Google Workspace są na stronie SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny.

Skróty użyte na tej stronie (25)

Skrót	Co znaczy
ACME	Automatic Certificate Management Environment: protokół, którym Traefik albo certbot automatycznie zamawiają i odnawiają certyfikat w Let's Encrypt, bez ręcznego wniosku
BIND	Berkeley Internet Name Domain: najpopularniejszy serwer DNS, napisany w Uniwersytecie Kalifornijskim w Berkeley, dziś rozwijany przez ISC
CA	Certificate Authority: urząd certyfikacji, który podpisuje certyfikaty
CAA	Certification Authority Authorization: rekord DNS, który mówi, które urzędy certyfikacji mogą wystawiać certyfikaty dla domeny
CLI	Command Line Interface: praca przez wpisywanie komend w terminalu

Skrót	Co znaczy
DANE	DNS-based Authentication of Named Entities: odcisk certyfikatu serwera opublikowany w rekordzie TLSA podpisanej strefy, po którym nadawca sprawdza, że rozmawia z właściwym serwerem
DKIM	DomainKeys Identified Mail: cyfrowy podpis wiadomości e-mail
DMARC	Domain-based Message Authentication, Reporting and Conformance: reguła domeny mówiąca, co robić z mailem, który nie przeszedł SPF i DKIM
DNS	Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP
DNSKEY	rekord DNSSEC z kluczem publicznym strefy, którym resolver sprawdza podpisy jej rekordów
DNSSEC	DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona
ECDSA	Elliptic Curve Digital Signature Algorithm: podpis cyfrowy oparty na krzywych eliptycznych
MFA	Multi-Factor Authentication: logowanie drugim składnikiem, np. kodem z telefonu
MTA-STS	Mail Transfer Agent Strict Transport Security: zasada opublikowana przez domenę, że poczta do niej ma być wysyłana wyłącznie szyfrowanym połączeniem z serwerem o ustalonej nazwie
MX	Mail Exchanger: rekord DNS wskazujący serwer poczty domeny
NSEC3	rekord DNSSEC z podpisanym dowodem, że jakiejś nazwy w strefie nie ma, zapisany skrótami nazw, żeby nie dało się łatwo wypisać całej strefy
PTR	rekord DNS odwrotny: zamienia adres IP na nazwę
RFC	Request for Comments: oficjalny dokument opisujący standard internetowy, na przykład sposób działania danego protokołu; w ITIL także Request for Change, czyli wniosek o zmianę
RRSIG	rekord DNSSEC z podpisem jednego zestawu rekordów, na przykład wszystkich rekordów MX domeny
SPF	Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny
TLS-RPT	SMTP TLS Reporting: rekord _smtp._tls z adresem, na który serwery nadawców wysyłają raz na dobę raport o udanych i nieudanych szyfrowanych połączeniach z naszymi serwerami poczty (RFC 8460)
TLSA	rekord DNS, w którym domena publikuje odcisk certyfikatu swojego serwera, żeby inni mogli sprawdzić, że łączą się z właściwą maszyną (mechanizm DANE)
TTL	Time To Live: czas życia rekordu lub danych
TXT	typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC
VPN	Virtual Private Network: szyfrowany tunel do sieci firmowej

Fiszka

Odczyty robimy spoza sieci Zielonej albo pytając wprost publiczny serwer (`@1.1.1.1`), bo `dc01` odpowiada z wewnętrznej strefy. Zmiany robimy w Azure CLI kontem z prawem zapisu do strefy, w oknie zmian, a przed większą zmianą eksportujemy strefę do pliku.

□□ TYLKO ODCZYT

Odczyt rekordów poczty przychodzącej: dig MX

```
dig +short MX NazwaDomeny
```

Pokazuje serwery, do których świat wysyła pocztę dla domeny, z priorytetem (mniejsza liczba wygrywa).

Przykład:

```
10 poczta.zielona.example.
20 poczta2.zielona.example.
```

□□ **MX** = Mail Exchanger: rekord DNS wskazujący serwer poczty domeny · **dig** = domain information groper: odpytywanie DNS

□□ TYLKO ODCZYT

Odczyt rekordów tekstowych domeny: dig TXT

```
dig +short TXT NazwaDomeny @1.1.1.1
```

Rekordy TXT na samej domenie to głównie SPF i rekordy weryfikacyjne usług chmurowych. Zapytanie do `1.1.1.1` omija wewnętrzny DNS.

Przykład:

```
"v=spf1 ip4:203.0.113.10 -all"
```

□□ **TXT** = typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC · **SPF** = Sender Policy Framework: rekord DNS mówiący, które serwery mogą wysyłać pocztę domeny · **DNS** = Domain Name System: książka telefoniczna internetu, zamienia nazwy na adresy IP · **dig** = domain information groper: odpytywanie DNS

□□ TYLKO ODCZYT

Odczyt rekordów TXT w Windows: Resolve-DnsName

```
Resolve-DnsName -Name NazwaDomeny -Type TXT -Server 1.1.1.1 -DnsOnly
```

Ten sam odczyt ze stacji z Windows, bez instalowania `dig`.

Przykład:

```
Name                           Type   TTL   Section    Strings
----                           ----   ---   -------    -------
zielona.example                TXT    3600  Answer     {v=spf1 ip4:203.0.113.10 -all}
```

TXT = typ rekordu DNS przechowującego dowolny tekst, wykorzystywany między innymi do publikowania reguł SPF, DKIM i DMARC

TYLKO ODCZYT

Eksport strefy do pliku: az network dns zone export

```
az network dns zone export --resource-group NazwaGrupyZasobow --name NazwaDomeny --file-name NazwaPliku
```

Zapisuje całą strefę w formacie pliku strefy. Robimy to przed każdą większą zmianą i raz na kwartał do porównania ze strefą wewnętrzną na `dc01`.

az = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Utworzenie zestawu rekordów z krótkim TTL: az network dns record-set a create

```
az network dns record-set a create --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny --name NazwaRekordu --ttl 300
```

(gdzie `NazwaRekordu` to nazwa bez domeny, na przykład `vpn`; dla rekordu na samej domenie piszemy `@`)

Zakłada pusty zestaw rekordów z TTL 300 sekund. Gdy zestaw dodaje od razu `add-record`, dostaje TTL domyślny.

TTL = Time To Live: czas życia rekordu lub danych · **az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ ZMIENIA SYSTEM

Dodanie adresu do rekordu A: az network dns record-set a add-record

```
az network dns record-set a add-record --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny --record-set-name NazwaRekordu --ipv4-address AdresIP
```

Dopisuje adres do zestawu. Każdą nazwę, która ma adres publiczny, dopisujemy też w wewnętrznej strefie `zielona.example` na kontrolerach, inaczej biuro jej nie zobaczy.

◫◫ **az** = Azure CLI: narzędzie chmury Microsoftu

◫◫ TYLKO ODCZYT

Odczyt rekordu CAA: dig CAA

```
dig +short CAA NazwaDomeny
```

Pokazuje, które urzędy certyfikacji mogą wystawiać certyfikaty dla domeny i dokąd zgłaszać naruszenia.

Przykład:

```
0 issue "letsencrypt.org"
0 issuewild ";"
0 iodef "mailto:it@zielona.example"
```

◫◫ **CAA** = Certification Authority Authorization: rekord DNS, który mówi, które urzędy certyfikacji mogą wystawiać certyfikaty dla domeny · **dig** = domain information groper: odpytywanie DNS

◫◫ ZMIENIA SYSTEM

Dodanie rekordu CAA: az network dns record-set caa add-record

```
az network dns record-set caa add-record --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny --record-set-name "@" --flags 0 --tag issue --value "NazwaUrzedu"
```

(gdzie `NazwaUrzedu` to identyfikator urzędu z jego dokumentacji, dla Let's Encrypt `letsencrypt.org`)

Od tej chwili inne urzędy powinny odmówić wystawienia certyfikatu dla naszych nazw. Polecenie powtarzamy dla `issuewild` i `iodef`.

CAA = Certification Authority Authorization: rekord DNS, który mówi, które urzędy certyfikacji mogą wystawiać certyfikaty dla domeny · **az** = Azure CLI: narzędzie chmury Microsoftu

ZMIENIA SYSTEM

Włączenie podpisu DNSSEC strefy: az network dns dnssec-config create

```
az network dns dnssec-config create --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny
```

Podpisuje strefę. Status w portalu zmienia się na „Signed but not delegated”, bo rejestr jeszcze nie zna odcisku naszego klucza.

DNSSEC = DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona · **az** = Azure CLI: narzędzie chmury Microsoftu

TYLKO ODCZYT

Odczyt danych do rekordu DS: az network dns dnssec-config show

```
az network dns dnssec-config show --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny
```

W wyniku szukamy informacji o delegacji: Key Tag, Algorithm, Digest Type i Digest. Te cztery wartości przepisujemy do panelu rejestratora jako rekord DS.

az = Azure CLI: narzędzie chmury Microsoftu

KLIKAMY W INTERFEJSIE

Zgłoszenie rekordu DS: panel rejestratora

```
Panel rejestratora → Domeny → NazwaDomeny → DNSSEC → Dodaj rekord DS → Key Tag, Algorithm, Digest Type, Digest → Zapisz
```

Rejestrator przekazuje rekord do rejestru. Część rejestratorów przyjmuje zamiast DS cały klucz DNSKEY i sama liczy odcisk; sprawdzamy to w jego dokumentacji.

□□ **DNSKEY** = rekord DNSSEC z kluczem publicznym strefy, którym resolver sprawdza podpisy jej rekordów

□□ TYLKO ODCZYT

Sprawdzenie rekordu DS w strefie nadrzędnej: dig DS

```
dig +short DS NazwaDomeny
```

Gdy rejestr opublikuje rekord, wynik pokazuje te same cztery wartości, które przepisaliśmy.

Przykład (poglądowy):

```
40143 13 2 9C5F1A6E0B7D3C2A4F8E6D1B0C9A7E5D3B1F2E4C6A8D0B2F4E6C8A1D3B5F7E9C
```

□□ **dig** = domain information groper: odpytywanie DNS

□□ TYLKO ODCZYT

Sprawdzenie łańcucha podpisów: delv

```
delv NazwaDomeny SOA
```

`delv` z pakietu BIND sprawdza podpisy od strefy głównej aż do naszej. Pierwsza linia wyniku mówi, czy odpowiedź jest w pełni zweryfikowana.

Przykład (poglądowy):

```
; fully validated
zielona.example.□3600□IN□SOA□ns1-07.azure-dns.com. azuredns-hostmaster.microsoft.com. 3 3600
300 2419200 300
zielona.example.□3600□IN□RRSIG□SOA 13 2 3600 20261109000000 20261026000000 40143
zielona.example. ...
```

□□ **BIND** = Berkeley Internet Name Domain: najpopularniejszy serwer DNS, napisany w Uniwersytecie Kalifornijskim w Berkeley, dziś rozwijany przez ISC · **delv** = domain entity lookup and validation: polecenie z pakietu BIND, które pyta DNS i sprawdza podpisy DNSSEC od strefy głównej do odpowiedzi

□□ TYLKO ODCZYT

Sprawdzenie flagi weryfikacji u resolvera: dig +dnssec

```
dig +dnssec SOA NazwaDomeny @1.1.1.1 | grep flags
```

Flaga `ad` w odpowiedzi oznacza, że publiczny resolver sprawdził podpisy i uznał je za poprawne.

dig = domain information groper: odpytywanie DNS

TYLKO ODCZYT

Wyłączenie podpisu DNSSEC: az network dns dnssec-config delete

```
az network dns dnssec-config delete --resource-group NazwaGrupyZasobow --zone-name NazwaDomeny
```

Polecenie jest nieodwracalne. Wykonujemy je dopiero wtedy, gdy rekord DS zniknął z rejestru i minął jego TTL, inaczej resolvery sprawdzające podpisy uznają całą domenę za fałszywą.

DNSSEC = DNS Security Extensions: podpisy cyfrowe w DNS, dzięki którym można sprawdzić, że odpowiedź nie została po drodze podmieniona · **TTL** = Time To Live: czas życia rekordu lub danych · **az** = Azure CLI: narzędzie chmury Microsoftu

Z życia wzięte

Z ŻYCIA WZIĘTE

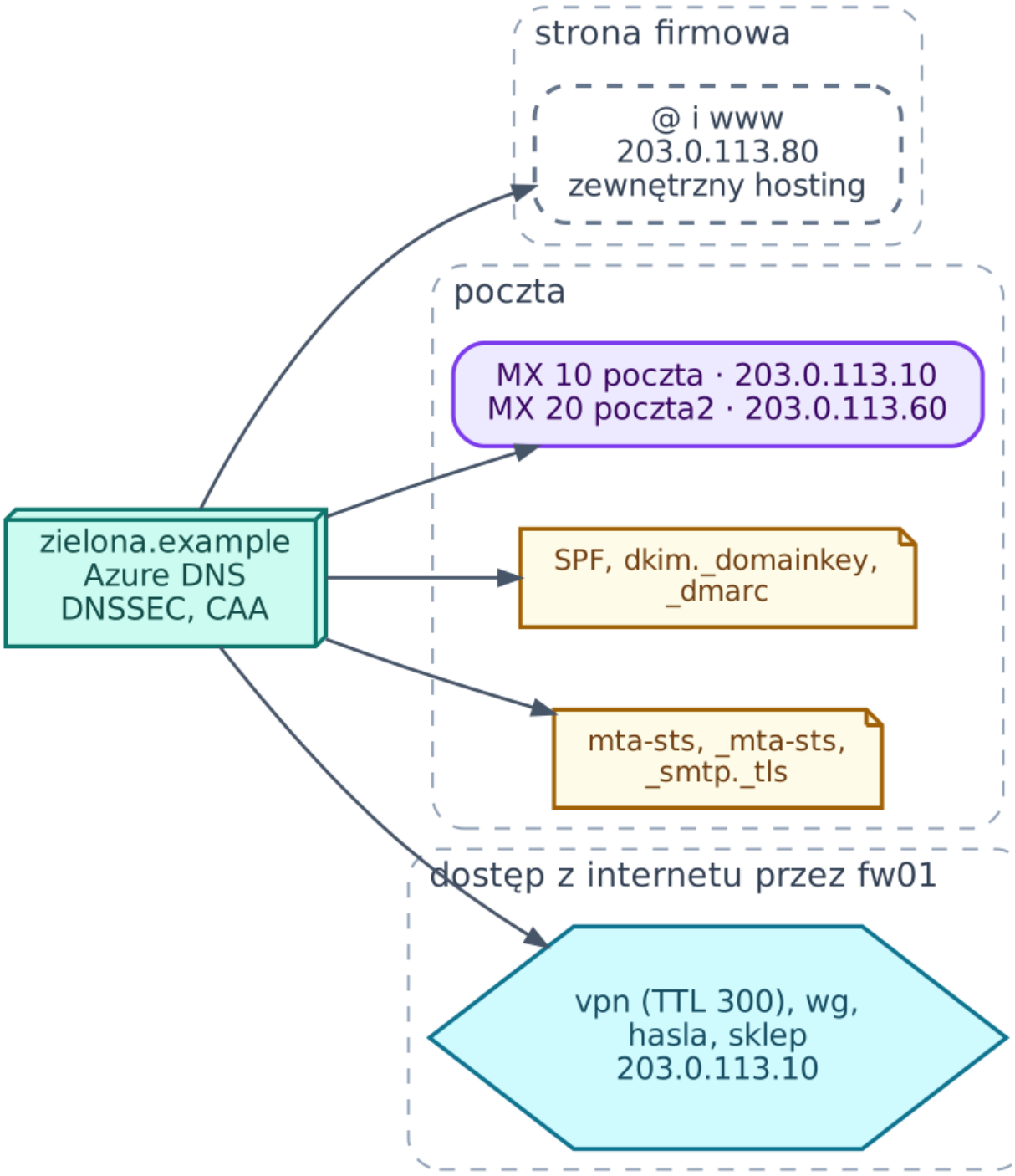
Piątek, 16:10. Tomek przenosi testowo strefę do innego dostawcy i, żeby „było czysto”, wyłącza podpis DNSSEC w Azure DNS, zostawiając rekord DS u rejestratora. Po kwadransie Kasia pisze z hotelu, że poczta nie działa, a klient z biura rachunkowego dostaje przy wysyłce do Zielonej błąd rozwiązywania nazwy. Resolvery, które sprawdzają podpisy, widzą DS bez pasującego podpisu i odpowiadają „błąd serwera” dla wszystkich nazw w domenie. Tomek włącza podpis z powrotem, ale klucz jest nowy, więc dopiero wymiana DS u rejestratora i odczekanie TTL kończą awarię po trzech godzinach.

Jak to działa

Rozwiń: jak to działa pod spodem

Rekordy publiczne Zielonej

Strefa publiczna ma tylko to, co musi być widoczne z internetu. Aplikacje wewnętrzne (`git`, `logi`, `netbox`, `pomoc`) istnieją wyłącznie w strefie wewnętrznej na kontrolerach. Każdy rekord z tabeli niżej ma za to swoją kopię w strefie wewnętrznej, czasem z adresem wewnętrznym, jak opisuje strona DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain.



Rysunek 1. Rekordy strefy publicznej zielona.example pogrupowane według usług: strona firmowa u zewnętrznego hostingu, poczta z MX 10 i MX 20, rekordy SPF, DKIM, DMARC, MTA-STS i TLS-RPT, dostęp zdalny przez fw01 oraz zabezpieczenia CAA i DNSSEC (kliknięcie otwiera pełny rozmiar)

Nazwa	Typ	Wartość	TTL (s)	Po co	Więcej
`@`	NS	cztery serwery Azure DNS	nadaje dostawca	delegacja strefy	Domena i strefa publiczna: rejestrator, dostawca DNS, odnowienia i blokady
`@`	A	203.0.113.80	3600	strona firmowa u zewnętrznego hostingu	
`www`	CNAME	`zielona.example.`	3600	ta sama strona pod adresem z `www`	
`@`	MX	`10 poczta.zielona.example.`	3600	główny serwer poczty przychodzącej	Instalacja MailCow na docker01 od zera
`@`	MX	`20 poczta2.zielona.example.`	3600	zapasowy MX na `edge-az01`	strona o łączach, wariant b
`poczta`	A	203.0.113.10	300	MailCow za `fw01`, panel i protokoły poczty	
`poczta2`	A	203.0.113.60	300	Postfix na `edge-az01`	
`autodiscover`, `autoconfig`	CNAME	`poczta.zielona.example.`	3600	automatyczna konfiguracja Outlooka i Thunderbirda	
`mta-sts`	CNAME	`poczta.zielona.example.`	3600	serwer z plikiem polityki MTA-STS	MTA-STS i TLS-RPT: szyfrowanie poczty między serwerami, a BIMI informacyjnie

Nazwa	Typ	Wartość	TTL (s)	Po co	Więcej
`@`	TXT	`v=spf1 ip4:203.0.113.10 -all`	3600	kto może wysyłać pocztę jako `@zielona.example`	SPF, DKIM i DMARC: trzy podejścia do poczty i systemy wysyłające w imieniu domeny
`dkim._domainkey`	TXT	klucz publiczny z panelu MailCow	3600	sprawdzenie podpisu DKIM	jak wyżej
`_dmarc`	TXT	polityka DMARC z adresem raportów	3600	co robić z pocztą podszytą pod domenę	Droga DMARC od p=none do p=reject z raportami parsedmarc na docker01
`_mta-sts`	TXT	`v=STSv1; id=...`	3600	sygnał, że mamy politykę MTA-STS	strona o MTA-STS
`_smtp._tls`	TXT	`v=TLSRPTv1; rua=mailto:raporty-tls@zielona.example`	3600	adres raportów o szyfrowaniu	strona o MTA-STS
`vpn`	A	203.0.113.10	300	brama VPN pracowników na `fw01`, zmieniana przy awarii łącza	strona o łączach
`wg`	A	203.0.113.10	3600	WireGuard administratorów na `wg01`	WireGuard i OpenVPN: odpowiedniki spoza FortiGate na Linuksie
`hasla`	A	203.0.113.10	3600	Vaultwarden dostępny z internetu	Instalacja Vaultwardena w Dockerze
`sklep`	A	203.0.113.10	3600	sklep B2B dla odbiorców hurtowych	w kursie AWS rekord wskazuje równoważnik obciążenia w chmurze

Nazwa	Typ	Wartość	TTL (s)	Po co	Więcej
`@`	CAA	`0 issue "letsencrypt.org"`, `0 issuewild ";"`, `0 iodef "mailto:it@zielona.example"`	3600	kto może wystawić certyfikat	niżej

Dwa rekordy żyją poza naszą strefą. Rekord PTR dla 203.0.113.10 (nazwa `poczta.zielona.example`) ustawia operator łącza, a dla 203.0.113.60 ustawiamy go właściwością `ReverseFqdn` adresu publicznego w Azure. Rekord DS leży w strefie nadrzędnej i zmieniamy go tylko przez rejestratora.

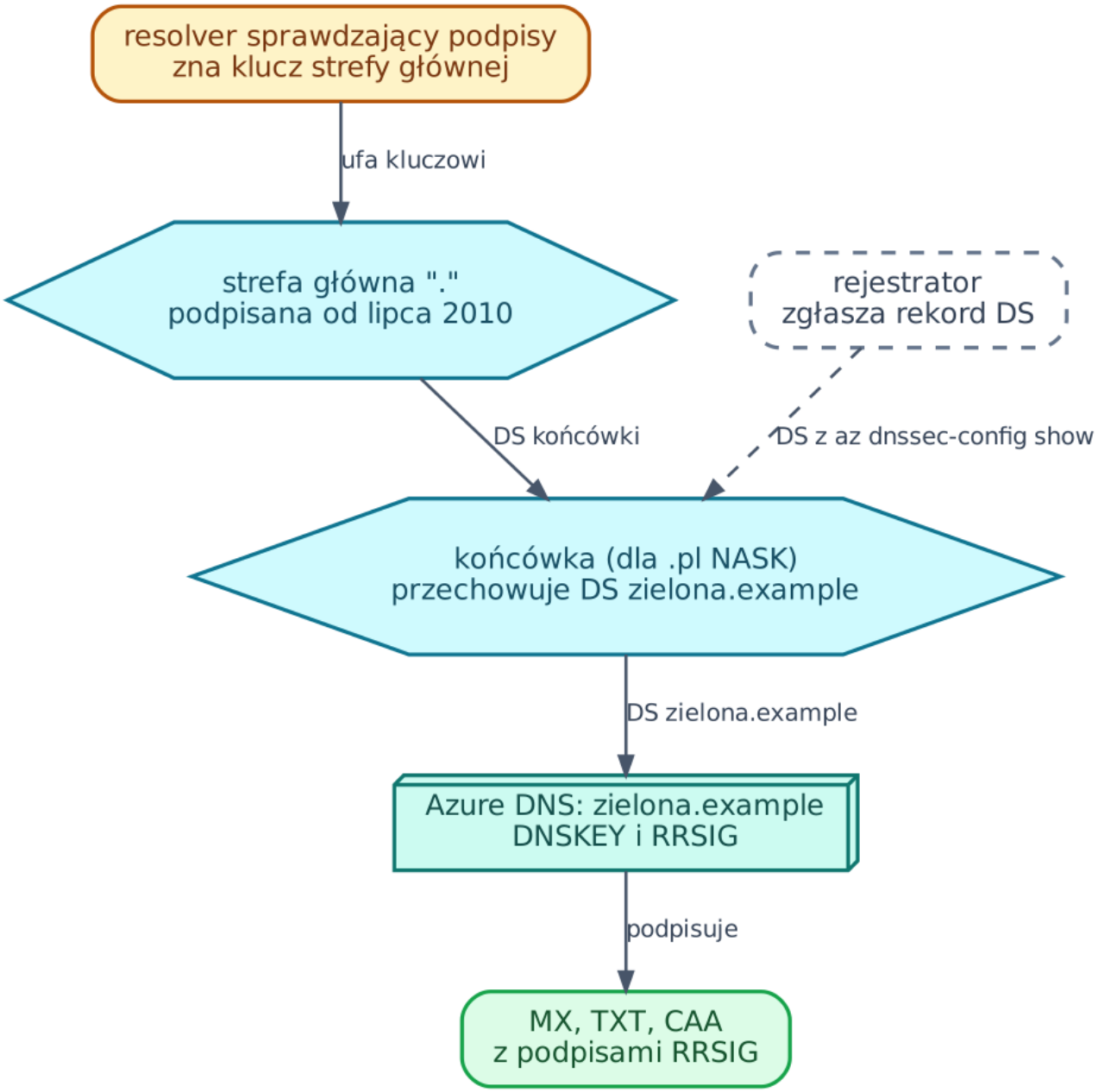
> Krótki TTL 300 sekund mają tylko nazwy, które przełączamy przy awarii (`vpn`, `poczta`, `poczta2`). Pozostałe mają 3600 sekund: krótszy TTL nic im nie daje, a mnoży zapytania i opóźnia odpowiedzi.

DNSSEC: podpis pod odpowiedzią

Pojęcie: DNSSEC. Dodatek do DNS, w którym strefa podpisuje swoje rekordy kluczem prywatnym, a pytający sprawdza podpis kluczem publicznym. Odpowiedź podmieniona po drodze nie ma ważnego podpisu i resolver, który sprawdza podpisy, ją odrzuca.

Pojęcie: łańcuch zaufania. Strefa główna internetu jest podpisana od lipca 2010 roku, a jej klucz znają resolvery. Strefa główna podpisuje odcisk klucza końcówki (rekord DS), końcówka podpisuje odcisk naszego klucza, a nasz klucz podpisuje nasze rekordy. Brakujące albo złe ogniwo przerywa łańcuch.

Strefa podpisana ma kilka nowych rodzajów rekordów, które dodaje sam dostawca: DNSKEY (klucze publiczne strefy), RRSIG (podpis przy każdym zestawie rekordów) i NSEC3 (podpisany dowód, że jakiejś nazwy nie ma). Nasza praca to włączenie podpisu i jeden rekord DS u rejestratora. Przykład w dokumentacji Azure DNS pokazuje algorytm 13, czyli ECDSA na krzywej P-256 z SHA-256, taki sam jak domyślny w deSEC.



Rysunek 2. Łańcuch zaufania DNSSEC: resolver zna klucz strefy głównej, strefa główna podpisuje DS końcówki, końcówka przechowuje DS zielona.example zgłoszony przez rejestratora, a Azure DNS podpisuje rekordy MX, TXT i CAA kluczem strefy (kliknięcie otwiera pełny rozmiar)

Kolejność kroków przy włączaniu i wyłączaniu podpisu jest najważniejszą rzeczą na tej stronie.

Czynność	Kolejność	Co się stanie przy odwrotnej kolejności

Włączenie	podpis u dostawcy, odczyt DS, DS u rejestratora, sprawdzenie `delv`	DS przed podpisem: domena przestaje działać dla resolverów sprawdzających podpisy
Wyłączenie	usunięcie DS u rejestratora, odczekanie TTL rekordu DS w strefie nadrzędnej, wyłączenie podpisu	podpis wyłączony przy żywym DS: awaria jak w scenie wyżej
Zmiana dostawcy DNS	wyłączenie DNSSEC według wiersza wyżej, przenosiny strefy i zmiana NS, nowy podpis i nowy DS	stary DS przy nowym dostawcy: domena znika

Dlaczego Zielona podpisuje strefę publiczną, skoro strefy wewnętrznej nie podpisuje? Na zewnątrz ochrona trafia tam, gdzie atak ma sens: rekord MX i klucze DKIM decydują, dokąd idzie poczta i czy przejdzie kontrolę. Podpis jest też warunkiem DANE, czyli rekordów TLSA, którymi serwer nadawcy może sprawdzić certyfikat naszego serwera pocztowego, a Exchange Online od października 2024 roku obsługuje DANE dla poczty przychodzącej, które działa tylko w domenach podpisanych DNSSEC. Rejestr `.pl` przyjmuje domeny z DNSSEC od grudnia 2011 roku; sprawdzamy tylko, czy nasz rejestrator przekazuje rekordy DS.

CAA: kto może wystawić certyfikat

> **Pojęcie: CAA (Certification Authority Authorization).** Rekord, w którym właściciel domeny wymienia urzędy certyfikacji uprawnione do wystawiania certyfikatów dla jego nazw. Od 8 września 2017 roku każdy publiczny urząd musi go sprawdzić przed wystawieniem certyfikatu. Urząd szuka rekordu najpierw na pełnej nazwie, potem coraz wyżej w drzewie, więc rekord na `zielona.example` obejmuje też `poczta.zielona.example`, jeżeli ta nie ma własnego.

Wpis	Znaczenie	Zielona
`0 issue "letsencrypt.org"`	ten urząd może wystawiać zwykłe certyfikaty	Traefik na `docker01` pobiera certyfikaty z Let's Encrypt
`0 issuewild ";"`	nikt nie wystawia certyfikatów wieloznacznych	publicznego certyfikatu `*.zielona.example` nie potrzebujemy
`0 iodef "mailto:it@zielona.example"`	dokąd urząd może zgłosić próbę naruszenia	skrzynka zespołu IT, z której GLPI robi zgłoszenie
`accounturi=...` w wartości `issue`	tylko konto ACME o tym adresie może dostać certyfikat (RFC 8657)	na później, po decyzji o DNS-01 w książce o PKI
`validationmethods=dns-01` w wartości `issue`	urząd może sprawdzać domenę tylko wskazanym sposobem	na później, jak wyżej

Let's Encrypt już honoruje parametry `accounturi` i `validationmethods`, a głosowanie SC098v2 w CA/Browser Forum czyni je obowiązkowymi dla wszystkich publicznych urzędów od marca 2027 roku. Przypięcie do konta ACME chroni przed przejęciem domeny przez kogoś, kto na chwilę przejmie ruch na porcie 80, ale gdy zgubimy plik konta Traefika (`acme.json`), nowe konto nie dostanie certyfikatu, dopóki nie zmienimy rekordu. Dlatego wprowadzamy je razem z kopią tego pliku.

> ⚠ Każda usługa, która sama wystawia certyfikat dla naszej nazwy, musi mieć swój urząd w CAA. Gdy na przykład plik polityki MTA-STS wystawimy w usłudze hostingowej z certyfikatem zarządzanym, dopisujemy jej urząd (sprawdzamy w dokumentacji usługi, który to jest), inaczej certyfikat dla `mta-sts.zielona.example` nie powstanie. Certyfikaty wewnętrzne z `CA-Zielona` CAA nie dotyczy.

Microsoft 365 i Google Workspace nie wystawiają certyfikatów dla naszych nazw przy samej poczcie, więc w podejściach B i C rekord CAA zostaje taki sam. Nowy wpis dodajemy dopiero wtedy, gdy któraś usługa (strona, sklep w chmurze, hosting polityki) ma dostać certyfikat na nazwę w `zielona.example`.

Częste błędy

Objaw	Przyczyna	Co robimy
Z internetu nazwa działa, z biura nie	rekord dodany tylko w strefie publicznej	dopisujemy go w strefie wewnętrznej na `dc01`
Cała domena nie odpowiada dla części odbiorców, inni nie widzą problemu	rekord DS nie pasuje do klucza strefy, a część resolverów sprawdza podpisy	`delv NazwaDomeny SOA`, porównujemy DS z `dnssec-config show`, poprawiamy DS u rejestratora
Status w Azure DNS stoi na „Signed but not delegated”	rekord DS nie dotarł do rejestru	`dig +short DS NazwaDomeny`, sprawdzamy zgłoszenie u rejestratora
Traefik nie dostaje certyfikatu, w logu `CAA record ... prevents issuance`	urząd nie jest wymieniony w CAA albo `accounturi` wskazuje inne konto	poprawiamy wpis `issue`, przy zmianie konta ACME zmieniamy `accounturi`
Certyfikat wieloznaczny odrzucony	`issuewild ";"` zabrania wszystkim	świadoma decyzja: dopisujemy urząd w `issuewild` albo zostajemy przy certyfikatach na pojedyncze nazwy
Zmiana adresu `vpn` przy awarii działa dopiero po godzinie	rekord miał TTL 3600, obniżony za późno	TTL 300 ustawiamy co najmniej dobę przed planowaną próbą

□□ Ćwiczenia

1. Ola prosi o publiczny adres dla `git.zielona.example`, „żeby działało z domu”. Co sprawdzamy, zanim dodamy rekord do strefy publicznej?

Odpowiedź

Czy usługa naprawdę ma być widoczna z internetu, czy wystarczy VPN. Strefa publiczna pokazuje światu, co mamy, a Gitea z danymi firmy w internecie wymaga MFA, aktualizacji i reguły na `fw01`. Domyślnie zostawiamy ją w strefie wewnętrznej, a dostęp z domu dajemy przez VPN.

1. W jakiej kolejności wyłączamy DNSSEC przed przenosinami strefy do innego dostawcy i dlaczego?

Odpowiedź

Najpierw usuwamy rekord DS u rejestratora, potem czekamy, aż minie jego TTL w strefie nadrzędnej, i dopiero wtedy wyłączamy podpis i przenosimy strefę. Odwrotna kolejność zostawia w rejestrze odcisk klucza, którego nikt już nie używa, i resolvery sprawdzające podpisy odrzucają całą domenę.

1. Dlaczego rekord CAA na `zielona.example` chroni też `poczta.zielona.example`?

Odpowiedź

Urząd szuka rekordu CAA od pełnej nazwy w górę drzewa i zatrzymuje się na pierwszym znalezionym. `poczta.zielona.example` nie ma własnego rekordu, więc obowiązuje rekord z `zielona.example`.

1. Pani Halina pyta, czy DNSSEC „zaszyfruje jej pocztę”. Co odpowiadamy?

Odpowiedź

Nie. DNSSEC niczego nie szyfruje, tylko podpisuje odpowiedzi DNS, żeby nikt nie podmienił po drodze adresu serwera pocztowego. Szyfrowanie poczty między serwerami wymuszają MTA-STS albo DANE, a DANE potrzebuje właśnie podpisanej strefy.

Powiązane: Domena i strefa publiczna: rejestrator, dostawca DNS, odnowienia i blokady · DNS w praktyce: strefy w AD, przekazywanie warunkowe, scavenging i split-brain · Łącza operatora: światłowód, radiolinia, LTE i 5G oraz przełączanie na FortiGate · MailCow: codzienna praca z domenami, skrzynkami i spamem · Reverse proxy w Dockerze: Traefik przed wszystkimi aplikacjami na docker01

Źródła (odczyt 26 października 2026): learn.microsoft.com: „DNS zones and records” (CAA, DS i TLSA w strefach podpisanych), „How to sign your Azure Public DNS zone with DNSSEC” (statusy, algorytm 13 w przykładzie), dokumentacja `az network dns dnssec-config` (create, show, delete) · rfc-editor.org: RFC 8659 (CAA, listopad 2019, wspinanie po drzewie, `issue`, `issuewild`, `iodef`), RFC 8657 (`accounturi`, `validationmethods`) · archive.cabforum.org, Ballot 187 (8 września 2017) · community.letsencrypt.org, „ACME CAA Extensions to Become Mandatory” (SC098v2, marzec 2027, Let's Encrypt już egzekwuje) · bleepingcomputer.com, Exchange Online inbound DANE z DNSSEC (28 października 2024) · dns.pl, historia rejestru (DNSSEC w .pl od grudnia 2011) · jpmens.net, deSEC (ECDSAP256SHA256).