Jak nakonfiguruji záznamy DNS pro poštovní server?

Účel

Pro poštovní server jsou nezbytné různé typy záznamů DNS. V zájmu zajištění hladké výměny e-mailů a udržení dobré pověsti poštovního serveru vás tento článek provede nastavením jednotlivých typů záznamů DNS.

Prostředí

> V zařízení NAS je nainstalována a nastavena Synology MailPlus Server nebo Synology Mail Server .

Řešení

Jak služba DNS spolupracuje s poštovním serverem

DNS je zkratka pro „Domain Name System“. Jedná se o systém, který překládá názvy domén internetových serverů s jejich podkladovými IP adresami.

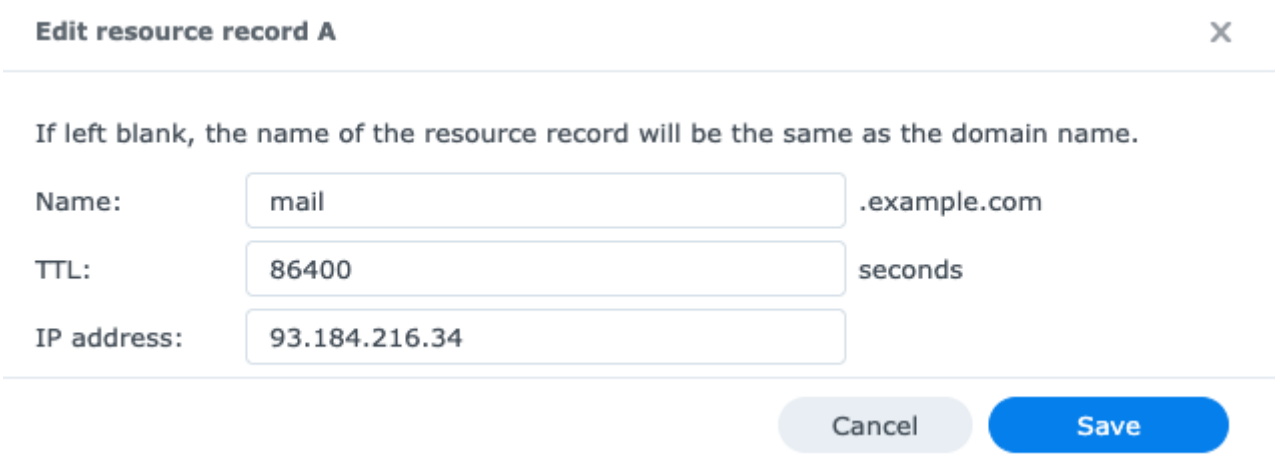
Pro správné odesílání a přijímání e-mailů je klíčové nakonfigurovat záznamy DNS **MX** a **A** tak, aby se s vaším serverem mohly spojit jiné poštovní servery přes Internet. K dispozici jsou také záznamy DNS pro ověřování jako **SPF**, **DKIM**, **DMARC** a **TLSA**, které chrání před nevyžádanou poštou a krádeží identity.

Záznam A

Záznam A nebo záznam adresy mapuje doménu nebo subdoménu na její IP adresu. Umožňuje koncovým uživatelům zadat název domény čitelný pro člověka, zatímco počítač může zpracovat IP adresu, která se za tímto názvem nachází.

Nasměrujte záznam A na IP adresu svého zařízení Synology NAS.

Podívejte se například na následující obrázek:

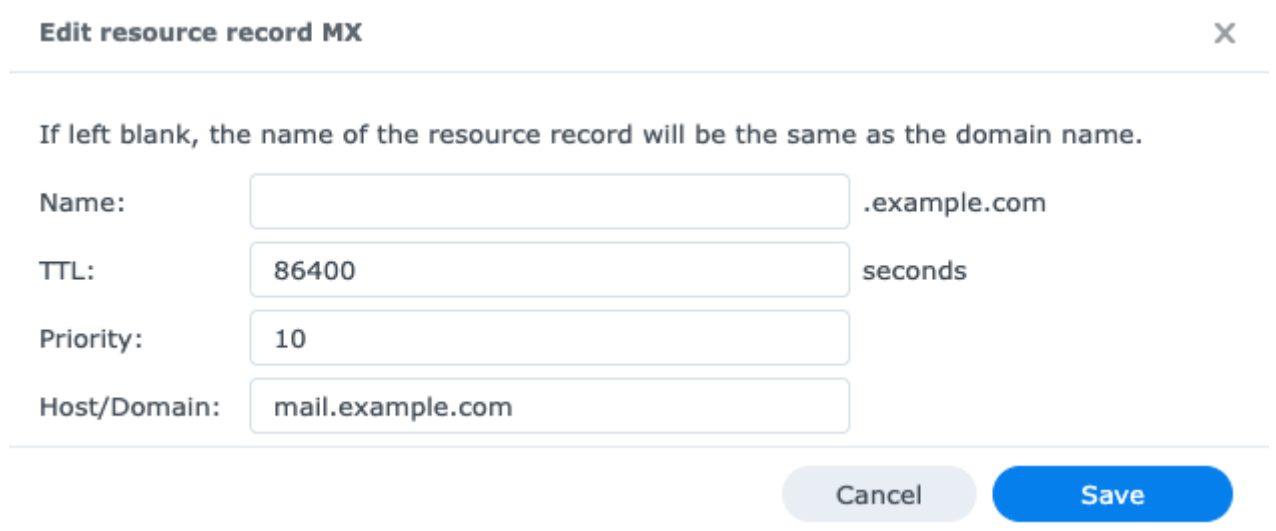


Záznam MX

Záznam MX nebo záznam služby Mail Exchanger uvádí, které poštovní servery přijímají e-maily jménem domény a kam mají být e-maily odeslané do vaší domény směrovány prostřednictvím SMTP (Simple Mail Transfer Protocol).

Každý záznam MX obsahuje název hostitele a prioritu. Název hostitele udává, kam mají být e-maily doručovány, zatímco číslo priority udává pořadí, ve kterém se mají poštovní servery používat. Nižší číslo znamená vyšší prioritu.

Chcete-li zajistit, aby e-mailová adresa jako „alex@example.com“ fungovala, musíte pro doménu „example.com“ nastavit záznam MX, jak je znázorněno na následujícím obrázku:



Záznam SPF

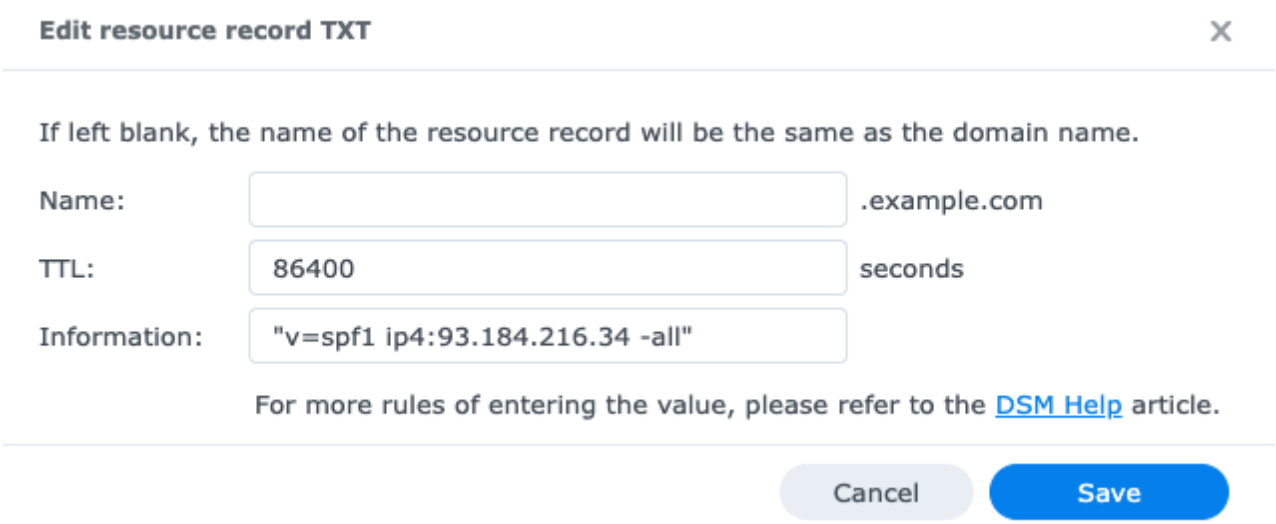
Záznam SPF nebo záznam rámce zásad odesílatele pomáhá předcházet e-mail spoofing tím, že určuje servery, které mohou odesílat e-maily jménem domény.

Základní záznam SPF je záznam TXT, který obsahuje značky a hodnoty uvedené v následující tabulce. Další informace o syntaxi záznamu SPF se nacházejí na tomto webu.

Tag	Hodnota	Příklad
`v`	Verze SPF. Prozatím používejte verzi „spf1“.	`v=spf1`
`ip4`	IP adresa autorizovaného poštovního serveru. Musí se jednat o adresu nebo rozsah IPv4 ve standardním formátu.	`ip4:93.184.216.34`
`all`	Tato hodnota určuje, zda mají přijímající servery odmítat zprávy od neoprávněných odesílatelů.	• `-all` : Zamítne a zahodí. [1] • `~all` : Povolí, ale označí jako podezřelé.

Pokud je název domény „example.com“ a IP adresa je „93.184.216.34“, záznam SPF může být ve výše uvedeném formátu:

- Název: `example.com`
- Informace: `v=spf1 ip4:93.184.216.34 -all`



Záznam DKIM

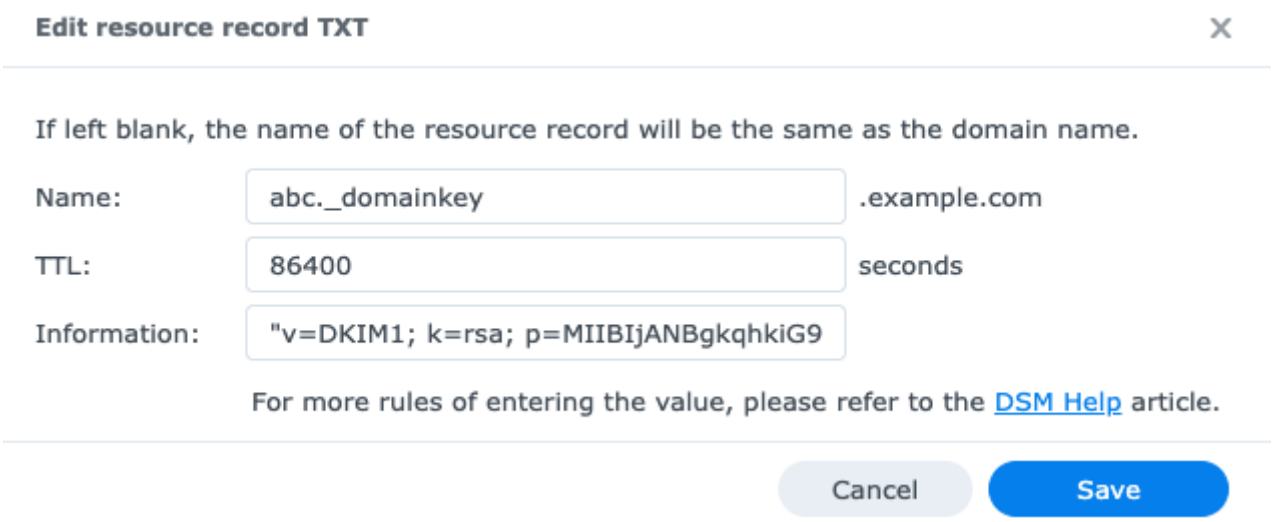
DKIM je zkratka pro DomainKeys Identified Email. DKIM připojením digitálního podpisu ke každému odchozímu e-mailu umožňuje ověřit, zda je e-mail skutečně autorizován vlastníkem domény.

Před konfigurací DKIM vygenerujte veřejný klíč pro poštovní server v následujících umístěních:

- **MailPlus Server** > **Doména** > **Upravit** > **Obecné** > **Rozšířené**
- **Mail Server** > **Zabezpečení** > **Ověření**

Po vygenerování klíče můžete začít se záznamem DKIM. Záznam DKIM se přidá jako záznam TXT v následujícím formátu:

	Formátovat	Příklad
Název	`DKIM selector prefix ._domainkey.your domain name`	`abc._domainkey.example.com`
Informace	`v=DKIM1; k=rsa; p=DKIM public key`	`v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQE`



Záznam DMARC

DMARC, což je zkratka pro Domain-based Message Authentication, Reporting, and Conformance, určuje, co se stane s e-mailem, který neprojde kontrolou SPF a DKIM. Díky funkci hlášení služby DMARC

může vlastník domény získat přehled o e-mailovém provozu a lépe tak detekovat spoofingové útoky.

Záznam DMARC je záznam TXT, který obsahuje následující značky a hodnoty:

Tag	Hodnota	Příklad
`v`	Verze DMARC. Prozatím používejte verzi „DMARC1“.	`v=DMARC1`
`p`	Zásady vynucované u neověřených e-mailů.	• `p=none` : Pouze monitory.[2] • `p=quarantine` : Odešle do karanténní poštovní schránky. • `p=reject` : Zamítne a zablokuje.
`pct`	Procento e-mailů, které mají být vynuceny zadanými zásadami.	`pct=100` (tj. 100 % e-mailů bude monitorováno, umístěno do karantény nebo odmítnuto.)
`rua=mailto`	E-mailová adresa pro příjem přehledů.	`rua=mailto:postmaster@example.com`

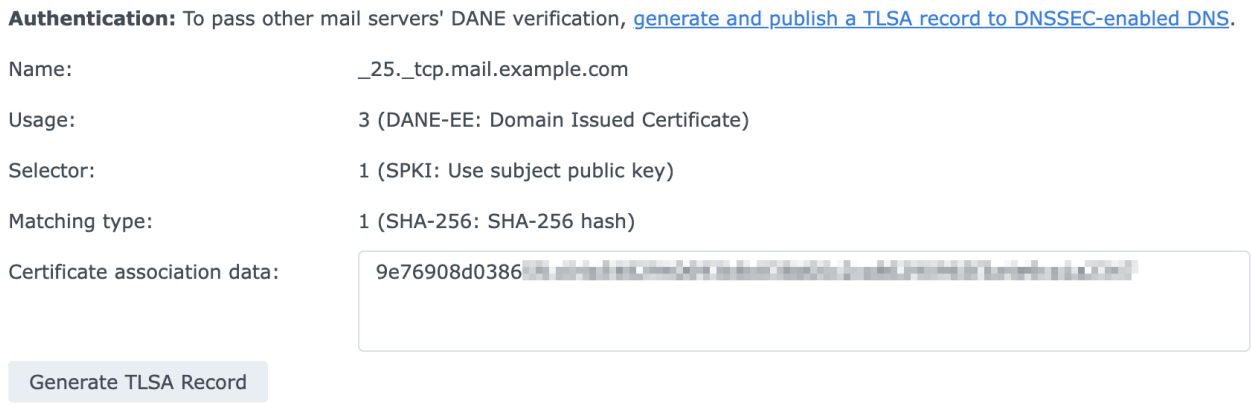
Pokud je název domény „example.com“, záznam DMARC může být ve výše uvedeném formátu:

- Název: `_dmarc.example.com`
- Informace: `v=DMARC1; p=none; pct=100; rua=mailto:postmaster@example.com`

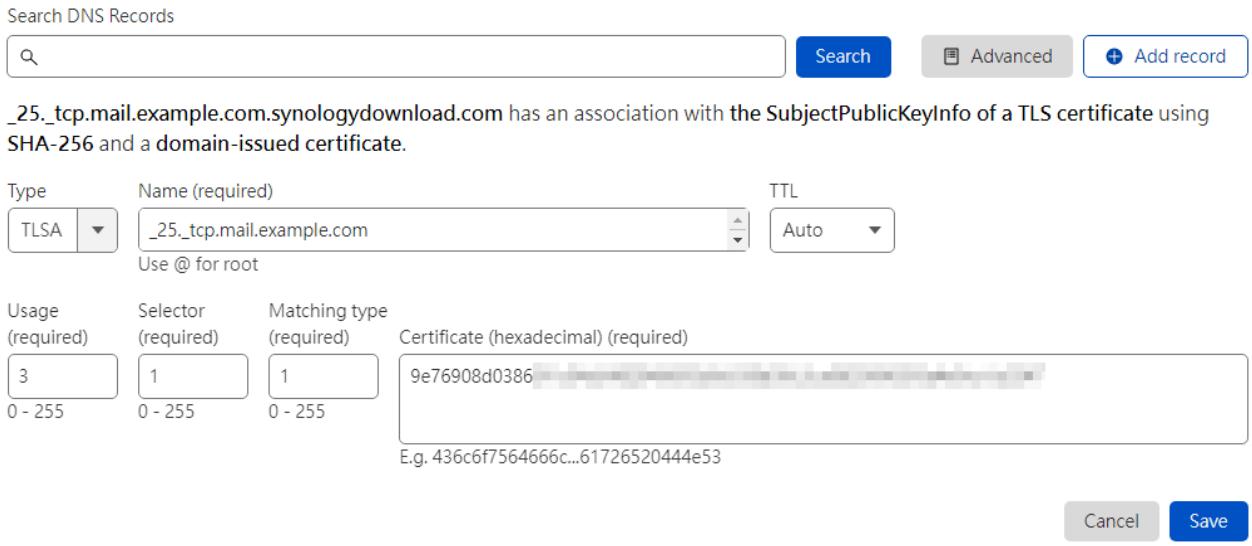
Záznam TLSA

Záznam TLSA (Transport Layer Security Authentication) přidruží certifikát serveru TLS k názvu domény, kde se záznam nachází. Pokud jiný poštovní server používá při doručování e-mailů do MailPlus Server protokol DANE, ověří záznam TLSA MailPlus Server. Bez tohoto záznamu MailPlus Server projít ověřením a vy možná nebudete moci přijímat e-maily odeslané z tohoto konkrétního poštovního serveru.

Záznam TLSA lze vygenerovat pomocí online generátoru nebo vestavěného generátoru služby MailPlus (v části **Zabezpečení** > **Ověření** > **DANE**).



Poté nasaďte záznam TLSA do veřejného serveru DNS.



Poznámky:

1. `-all` je doporučená možnost, protože dokáže lépe zajistit, aby e-maily pocházely od autorizovaného odesílatele.
2. `p=none` je dobrý výchozí bod pro analýzu toků e-mailů, ale jedná se o volnou zásadu, která nebude blokovat žádné podezřelé zprávy. Po určité době povolení SPF, DKIM a DMARC doporučujeme změnit nastavení na `p=quarantine` , abyste byli lépe chráněni před podvržením domény.

3. Příklady a obrázky v tomto článku slouží pouze pro demonstrační účely. Skutečné rozhraní závisí na jednotlivých poskytovatelích DNS. Pokud máte problémy s konfigurací záznamů DNS, požádejte o pomoc poskytovatele domény.