Stavíme poštovní server – 16 (záložní server)

23. 3. 2010 | Lukáš Jelínek | Sítě | 15252×

Může se stát, že je poštovní server nějakou dobu nedostupný – například když je umístěn uvnitř sítě firmy a přestane fungovat internetové připojení. Pro takové případy se často používá záložní server, který nemá úložiště pošty se schránkami, ale může poštu dočasně přebírat k pozdějšímu doručení na hlavní poštovní server.

Obsah

Když nejde doručovat poštu

link
Je-li hlavní poštovní server umístěn uvnitř firemní sítě, není až tak úplně vyloučeno, že bude občas nedostupný z Internetu. Internetové připojení není nikdy stoprocentně spolehlivé, navíc mohou nastat situace, kdy bude třeba kvůli nějakým stavebním pracím odpojené. Totéž, i když s menší pravděpodobností, se může stát i u serveru umístěném v perfektně zajištěném datovém centru – už třeba proto, že je potřeba provést nějaké práce přímo na tomto serveru.

Za běžných okolností se až tolik neděje, protože odesílající servery ponechají zprávy, které se nepodařilo doručit (kvůli nedostupnosti cílového serveru), ve svých frontách. To ale platí jen v případě, že jsou tyto servery správně nakonfigurované a že během této doby neselžou. Navíc pokud nedostupnost cílového serveru trvá déle, pokusy o opětovné doručení se opakují ve stále delších intervalech, takže i po obnovení dostupnosti serveru může trvat i řadu dalších hodin, než jsou zprávy doručeny.

Z uvedených důvodů (tedy přesunutí nedoručených zpráv „do vlastní moci“ a zajištění rychlého doručení po obnovení dostupnosti) se používají záložní servery, které zprávy přijmou namísto serveru hlavního a ponechají je ve své frontě potřebnou dobu. Po obnovení dostupnosti hlavního serveru je ihned tomuto serveru předají. Záložní server může být jeden, nic však nebrání tomu, aby jich bylo i více.

Problém s dostupností hlavního poštovního serveru lze samozřejmě řešit také tak, že je těchto hlavních serverů více a udržují si synchronizované úložiště. Tím lze zajistit přístup k nově doručeným zprávám i v době, kdy primární server není k dispozici. To je ale záležitost oproti řešení pomocí záložního serveru řádově složitější.

Jeden záložní server může obecně sloužit pro větší počet hlavních serverů. Typicky se to využívá třeba tak, že ISP poskytuje jeden nebo více záložních serverů svým zákazníkům pro případ nefunkčnosti jejich připojení.

Poštovní servery v DNS

link

Poštovní servery pro doručování do určité domény jsou v DNS identifikovány pomocí MX záznamů. Každý takový záznam obsahuje – kromě adresy serveru – také prioritu. Čím menší číslo, tím je priorita vyšší (na absolutní hodnotě však nezáleží). Doručující server by měl vždy začít od serveru s nejvyšší prioritou a případně (při neúspěchu; tím je myšlena nedostupnost, případně dočasná chyba, nikoli chyba trvalá) postupně zkoušet i servery s prioritou nižší. Pokud má stejnou prioritu více serverů, měly by být zkoušeny všechny se stejnou pravděpodobností (tj. například metodou *round-robin* nebo náhodně).

Chování správně nakonfigurovaného poštovního serveru tedy vypadá tak, že provede DNS dotaz na MX záznamy a pak postupuje podle priorit jednotlivých záznamů. Primární (hlavní) server bude mít

prioritu např. 10, záložní server 100 – proto se nejprve zkusí hlavní server a teprve při neúspěchu server záložní. Pokud neexistují MX záznamy, má odesílající server zkusit ještě A (resp. AAAA u IPv6) záznamy, ale to není běžná situace a nemá to v kontextu řešení záložního serveru žádný zvláštní význam.

Špatně implementované nebo nakonfigurované servery mohou volit pořadí serverů jiné, proto je pro správné fungování pošty žádoucí, aby, když už existuje MX záznam pro jeden či více záložních serverů, tyto servery správně fungovaly (nelze-li to zajistit, pak je lepší příslušné záznamy zrušit).

Existuje však ještě jedna situace, kdy jsou servery voleny ve špatném pořadí. Dělají to mnohé nástroje spammerů, a to dokonce záměrně. U záložních serverů se totiž očekává slabší ochrana než u serverů hlavních, proto spammeři mnohdy cílí právě na MX záznamy s nižší prioritou. Řešení je dvojí – buď záložní servery vůbec nepoužívat (což ale v případě, kdy jsou k používání dobré důvody, zrovna moc řešení není), anebo je zabezpečit tak, aby to spammeři neměli jednoduché.

Konfigurace programu Postfix

link

Záložní server nemá poštovní schránky – jeho jediným úkolem je přijímat zprávy a zadržovat je do doručení na hlavní server (případně je vracet, pokud doručit nejdou). Nemá tedy ani úložiště pošty, nepotřebuje žádnou službu pro přístup ke schránkám ani k autentizaci uživatelů (ledaže by měl sloužit i k odesílání pošty, to však nebývá úkolem záložních serverů). Tím se situace zjednodušuje, dokonce – jak se vzápětí ukáže – může záložní server fungovat i zcela autonomně, bez potřeby přístupu do databáze domén.

Samotná změna konfigurace tak, aby server vystupoval jako záložní, je velmi jednoduchá (viz dále). Bohužel, to není jediná věc, kterou je potřeba vyřešit. Musí se totiž zajistit i již zmíněná ochrana proti

spamu, a to nejlépe způsobem co nejpodobnějším tomu, který je použit na hlavním serveru. O tom ale až později – nejprve je potřeba záložní server zprovoznit. Tady je základní podoba konfiguračního souboru `main.cf`:

```
myhostname = postak-zalozni.moje.domena
myorigin = $mydomain
mynetworks = 127.0.0.0/8

smtpd_sender_restrictions =
    permit_mynetworks,
    reject_non_fqdn_sender,
    reject_unknown_sender_domain,
    permit

smtpd_recipient_restrictions =
    permit_mynetworks,
    reject_non_fqdn_recipient,
    permit_mx_backup,
    reject

smtpd_helo_required = yes
disable_vrfy_command = yes
```

Tato konfigurace je velmi podobná té, která se vyskytovala na počátku seriálu, konkrétně u serveru pro odesílání zpráv. Parametr `myhostname` musí být shodný s názvem uváděným v MX záznamech směřujících na tento server (viz dále). `myorigin` je doména pro zprávy odesílané (tak jako dříve), `mynetworks` určuje „vlastní sítě“ (zde jen lokální stroj).

Restrikce na odesílatele jsou podobné těm používaným dříve, tedy povoluje se příjem z vlastních sítí, odmítá příjem chybně určených adres a neexistujících domén. U restrikcí na příjemce je ale zásadní změna. Povolen je totiž příjem z vlastních sítí a dále pak (po odmítnutí chybných adres příjemců) pro domény, pro které tento server slouží jako záložní (`permit_mx_backup`).

Jak `permit_mx_backup` funguje? Povolí příjem pro domény, u kterých existuje neprimární MX záznam obsahující tento server, a dále pak domény explicitně uvedené jako `relay_domains` (zde žádné nejsou, proto se to neuplatní). Možná to zní trochu složitě, ale ve skutečnosti to složité není. Stručně řečeno, pokud pro danou doménu existuje MX záznam směřující na tento server a současně pro tuto doménu existuje alespoň jeden MX záznam s větší prioritou, je zpráva přijata.

Lze si to ukázat na příkladu. Doména `moje.domena` bude mít záznam ukazující na server `postak.moje.domena` s prioritou 10 a záznam ukazující na server `postak-zalozni.moje.domena` (čili na tento server) s prioritou 20. Zprávy pro doménu `moje.domena` tedy server přijme. Doména `jina.domena` však bude mít jen jediný MX záznam, a sice ukazující na `postak-zalozni.moje.domena` s prioritou 5. Zprávy nebudou tímto serverem přijímány.

Úskalí a možná řešení

link

Uvedená konfigurace má jednu zásadní výhodu a současně i jedno úskalí. Výhoda tkví v tom, že se vůbec není potřeba starat o to, pro které domény server funguje jako záložní – všechny potřebné informace si server sám získá z DNS. Velmi výhodné je to v situacích, kdy záložní server provozuje někdo jiný než server primární. Není potřeba nijak řešit předávání informací při změně v nastavení MX záznamů.

Úskalí spočívá v tom, že si příslušné MX záznamy může každý nastavovat, jak chce. Proto, když někdo touží po záložním serveru, může si prostě nějaký nastavit – a pokud se tento server nebrání, bude jako záloha sloužit. A uvedená konfigurace je právě taková. Nijak se nebrání tomu, aby si server úplně kdokoliv nastavil jako záložní a využíval jeho systémové prostředky ke svému užitku.

Protože by se málokomu takový stav zamlouval, je potřeba nalézt vhodné řešení, které bude umožňovat ochranu serveru při zachování maximálního komfortu. Jedním z řešení je přidat do konfigurace tento řádek:

```
permit_mx_backup_networks = 85.207.0.0/16
```

Uvedený parametr omezuje využití serveru jako záložního na případy, kdy jsou primární servery (MX záznamy s nejvyšší prioritou) v definovaných sítích. Například tak ISP může zajistit, aby jeho záložní poštovní server směli využívat jen jeho zákazníci (mající jím přidělené IP adresy) pro primární servery umístěné za jím poskytovaným připojením.

Druhá možnost je testovat domény explicitně, což může být použito samostatně nebo v kombinaci s předchozí metodou. Pro samostatné použití se místo `permit_mx_backup` použije `permit_auth_destination` a domény jsou dostupné pomocí parametru `relay_domains` (viz dále). Parametr `permit_mx_backup_networks` se nepoužije. Pro kombinované použití se ponechá parametr `permit_mx_backup`, `permit_mx_backup_networks` se nastaví podle potřeby a další domény se uvedou pomocí `relay_domains`.

Domény, pro něž má server sloužit jako záložní, se definují pomocí `relay_domains`. Je to úplně stejné, jako když si hlavní server zjišťuje domény, do nichž doručuje. Lze tedy použít obyčejný seznam přímo přiřazený do parametru, ale také kteroukoli z široké škály metod podporovaných konkrétní instalací serveru (čili obecně různé databáze, LDAP, externí službu dostupnou přes TCP…). Takové řešení je vhodné pro případy, kdy se poskytuje záložní server pro primární server umístěný kdekoliv na Internetu.

další strana článku…

Kapitoly článku

2. Stavíme poštovní server – 16 (záložní server): Příkaz ETRN
3. Stavíme poštovní server – 16 (záložní server): Greylisting

Nejčtenější články posledního měsíce

Týden na ITBiz: V Evropě se letos očekává pokles prodeje serverů
Týden na ITBiz: Elektronové můstky umožňují sdílení energie mezi vrstvami polovodičů
Jaderné noviny – přehled za leden 2023

Nejkomentovanější články posledního měsíce

všechny statistiky »

Seriál Stavíme poštovní server (dílů: 17)

Stavíme poštovní server – 1 (Postfix) (první díl)
<—« Stavíme poštovní server – 15 (sdílení, ACL)
»—> Stavíme poštovní server – 17 (optimalizace výkonu)
Stavíme poštovní server – 17 (optimalizace výkonu) (poslední díl)

Související články

SPAM – greylisting ve firmě
Mailserver s odvirováním pošty
DKIM – podepisujeme e-maily na serveru
Spam: naučte se bránit
MessageWall - kladivo nejen na spam
Jsme na dovolené - automatická odpověď

Další články z této rubriky

PowerDNS – přívětivý a jednoduchý DNS server
Bootování ze sítě: pxelinux a kořenový adresář na NFS
Těžký život Do Not Track
OpenAFS – servery
Architektura IPv6 – konfigurace adres a objevování sousedů (2)

Hodnocení: 100 %

špatné • dobré
Nástroje: Tisk bez diskuse

23.3.2010 12:11 kolcon | skóre: 15 | blog: kolcon
Re: Stavíme poštovní server – 16 (záložní server)
a nestacilo by na tom zaloznim serveru proste nastavit relay_host ?

23.3.2010 17:28 Luk | skóre: 47 | blog: Kacířské myšlenky | Kutná Hora
Re: Stavíme poštovní server – 16 (záložní server)
Jde o to, co znamená to "prostě nastavit". Bez kombinace s restrikcemi to nejde, jinak z toho bude open relay se všemi důsledky. Kromě toho je zbytečné to nastavovat, když záložní server ví, kam má zprávy předávat (dozví se to z MX záznamů). Pokud navíc záložní server slouží více primárním serverům, ani to nastavit nejde, protože jsou ty servery různé.

Šifrování je absolutní nutnost a pomáhá chránit před nekalými živly

Je mozne nejakym podobnym zpusobem postavit ne jen zalozni, ale duplicitni mail server takovy, ze v pripade vypadku primarniho prevezme v plne siri jeho ulohu (vcetne uzivatelskych uctu, stavajicich dat a podobne), a to idealne transparentne, bez nutnosti prekonfigurovat MUA? Tahove high-availibility reseni. Dekuji za odpoved.

23.3.2010 17:42 Luk | skóre: 47 | blog: Kacířské myšlenky | Kutná Hora
Re: Stavíme poštovní server – 16 (záložní server)
Bez nutnosti překonfigurovávat MUA to bude docela problém. Buď by musely být DNS záznamy s TTL=0 (nebo hodně nízkou hodnotou) a spoléhat se na to, že si to cachující servery nebudou vykládat po svém. Pak by se musely odněkud ty DNS záznamy měnit podle dostupnosti serverů. Druhá možnost je z to z IP adresy uvedené v DNS to tunelovat jinam, ale to už se zavádí single point of failure (když selže, selže všechno). Samozřejmě duplicitní server postavit

lze, s uživatelskými účty není problém (ať už jsou v databázi, přes LDAP, případně souborově). Zbývá vyřešit jediný problém, a to je úložiště. Pokud bude vzdálené (v technologickém smyslu) a transparentně synchronizované mezi různými geografickými místy, opět to není až tak velký problém.

Šifrování je absolutní nutnost a pomáhá chránit před nekalými živly

26.3.2010 08:06 tomfi | skóre: 19
Re: Stavíme poštovní server – 16 (záložní server)
Sakra, to jsem nějak zaspal dobu... myslel jsem, že standardně lze pro účely "sdílení" IP použít vrrp, carp, různé formy natu alá load-balancing atd... ale co, možná i to DNS někdo považuje za failover technologii, i když je to trochu podle hesla "když to nezvládnu nastavit na serveru tak ten problém přenesu jinam (na klienta) :D"

Vždyť jsou to jen jedničky a nuly ...

26.3.2010 08:49 petr_p | skóre: 59 | blog: pb
Re: Stavíme poštovní server – 16 (záložní server)
Problém je ve sdílení IP. K čemu mi je cluster, když se k němu klient nedostane.

26.3.2010 12:40 Luk | skóre: 47 | blog: Kacířské myšlenky | Kutná Hora
Re: Stavíme poštovní server – 16 (záložní server)

> standardně lze pro účely "sdílení" IP použít vrrp, carp, různé formy natu alá load-balancing atd.

To lze, ale jen v případě, že jsou cílové servery v jedné síti. Pokud jsou v různých sítích (nejlépe geograficky vzdálených), pak je to mnohem problematičtější. Nevím jak obecně ve světě, ale mám pocit, že tady v Česku jsou problémy zasahující celý telehouse nebo jeho velkou část (ať už souvisí s napájením, s routery nebo něčím jiným) dost časté na to, aby high availability řešení s tímto mělo počítat.
Šifrování je absolutní nutnost a pomáhá chránit před nekalými živly

Pripada mi to zbytecne, muze mi nekdo rici v cem je vyhoda mit MX backup ? kdyz v pripade nedostupnosti mailserveru zustava nedorucena posta ve spoolu na smtp serverech po dobu peti dnu (default) se je postak snazi co 30 minut odeslat.

24.3.2010 12:53 Luk | skóre: 47 | blog: Kacířské myšlenky | Kutná Hora
Re: Stavíme poštovní server – 16 (záložní server)

> Pripada mi to zbytecne, muze mi nekdo rici v cem je vyhoda mit MX backup ?

Je samozřejmě pravda, že "nejlepší léta" záložních serverů jsou už pryč, protože spolehlivost internetových připojení je dnes už taková, že většinou záloha není potřeba. Nicméně někdo se může rozhodnout, že záložní server používat bude.

> kdyz v pripade nedostupnosti mailserveru zustava nedorucena posta ve spoolu na smtp serverech po dobu peti dnu (default) se je postak snazi co 30 minut odeslat.

Na tohle nelze až tolik spoléhat. Jednak těch 5 dnů je opravdu jen default a nikdo nebrání správci nějakého serveru tu dobu zkrátit třeba na 1 den. Dále neplatí to tvrzení o 30 minutách. Jednak velmi záleží na konkrétním serveru, jeho chování a konfiguraci (např. Postfix standardně doručovací pokusy opakuje v prodlužujících se intervalech). Současně je potřeba brát v úvahu zatížení konkrétních serverů, takže i kdyby byl interval 30 minut, v reálu to může být podstatně víc. Proto se někdo může rozhodnout, že bude raději používat záložní server, který má ve své moci. Další možností je, že záložní server poskytuje ISP v rámci připojení (v ceně služby) a s předem definovanými parametry chování.
Šifrování je absolutní nutnost a pomáhá chránit před nekalými živly

Trochu mi není jasné fungování v případě graylistingu. Pokud mi (ač normálně dostupný) primární server odpoví z důvodu graylistingu, že je dočasně out, nebude se to odesílající server snažit doručit na ten záložní? Když na něm bude graylisting také asi se vrátí s dalším pokusem zas na primární, takže to asi zafunguje, ale nebude to dělat nějakou neplechu?

26.3.2010 17:02 Luk | skóre: 47 | blog: Kacířské myšlenky | Kutná Hora
Re: Stavíme poštovní server – 16 (záložní server)

> Pokud mi (ač normálně dostupný) primární server odpoví z důvodu graylistingu, že je dočasně out, nebude se to odesílající server snažit doručit na ten záložní?

Může se pokoušet (nevím, jak který poštovní software vyhodnocuje různé dočasné chyby a jak na ně konkrétně reaguje).

> Když na něm bude graylisting také asi se vrátí s dalším pokusem zas na primární, takže to asi zafunguje, ale nebude to dělat nějakou neplechu?

Může se tím prodloužit doba doručení. Ovšem vzhledem k tomu, že u greylistingu je obecně problém s tím, že doba doručení pro první komunikaci může být dlouhá (a podle toho, jak moc to vadí, je potřeba rozhodovat, zda greylisting nasadit), za až tak moc velký problém to nepovažuji.
Šifrování je absolutní nutnost a pomáhá chránit před nekalými živly