Migrace poštovních služeb z prostředí On-Premise do cloudového řešení Office365

Bc. Jaroslav Hanák

Diplomová práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2017/2018

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Jaroslav Hanák**
Osobní číslo:	**A16268**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**kombinovaná**
Téma práce:	**Migrace poštovních služeb z prostředí On-Premise do cloudového řešení Office 365**
Téma anglicky:	**The Migration of On-Premise Office Services to Cloud Office 365**

Zásady pro vypracování:

1. **V teoretické části vysvětlete princip funkčnosti poštovních služeb.**
2. **Formou rešerše popište možnosti poskytování poštovních služeb.**
3. **V praktické části vytvořte návrh migrace poštovních služeb z Exchange On-Premis do cloudového řešení Office 365 spolu s migrací uživatelů.**
4. **Následně vytvořte návrh aplikačního monitoringu oblastí Exchange On-Premise a Office 365 Exchange Online.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **CLIFTON, Leonard. Mastering microsoft exchange server 2016. Indianapolis, IN: John Wiley, 2016. ISBN 978-1119232056.**
2. **RUEST, Danielle a Nelson RUEST. Virtualizace: podrobný průvodce. Brno: Computer Press, 2010. ISBN 978-80-251-2676-9.**
3. **GREVE, David a Loryan STRANT. Microsoft Office 365: exchange online implementation and migration. New Edition. Birmingham: Packt Pub, 2012. ISBN 978-184-9685-863.**
4. **CORNELISSEN, Bob, Paul KEELY, Kevin GREENE, Ivan HADZHIYSKI, Sam ALLEN a Telmo SAMPAIO. Mastering system center 2012 operations manager: principy, metodiky, architektury. Indianapolis, IN: [2013], 2012. Management v informační společnosti. ISBN 978-111-8128-992.**
5. **BRUCKNER, Tomáš. Tvorba informačních systémů: principy, metodiky, architektury. Praha: Grada, 2012. Management v informační společnosti. ISBN 978-80-247-4153-6.**

Vedoucí diplomové práce:	**doc. Ing. Jiří Gajdošík, CSc.** Ústav bezpečnostního inženýrství
Datum zadání diplomové práce:	**8. prosince 2017**
Termín odevzdání diplomové práce:	**28. května 2018**

Ve Zlíně dne 8. prosince 2017

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....

podpis diplomanta

ABSTRAKT

Diplomová práce reflektuje problematiku e-mailové komunikace a migrace poštovních služeb mezi On-Premise poštovním systémem a cloudovým řešením společnosti Microsoft. Práce vysvětluje přenos e-mailových zpráv po Internetu. Popisuje vybrané poštovní systémy. Dotýká se také zabezpečení e-mailové komunikace.

Práce dále popisuje návrh a implementaci synchronizace mezi lokální Active Directory a Azure Active Directory. Významnou část práce tvoří výběr a návrh na provedení migrace poštovních služeb z Microsoft Exchange On-Premise do cloudového řešení Exchange Online. Vybraný scénář je prakticky testován.

Praktická část práce dále vytváří návrh na aplikační monitorování jak Microsoft Exchange 2016 On-Premise řešení, tak Exchange Online spolu s Azure Active Directory.

Klíčová slova: e-mail, komunikace, Microsoft Exchange 2016, Exchange Online, Office 365, Azure, System Center Operations Manager

ABSTRACT

The diploma thesis reflects the issue of e-mail communication and migration of e-mail services between On-Premise e-mail system and Microsoft cloud solution. The work explains the transmission of e-mail messages over the Internet. Describes selected e-mail systems. It also affects the security of e-mail communications.

The work also describes the design and implementation of synchronization between local Active Directory and Azure Active Directory. An important part of the work is the selection and design of the migration of e-mail services from Microsoft Exchange 2016 On-Premise into the Exchange Online Cloud solution. The selected scenario is practically tested.

The practical part of the thesis also creates a proposal for application monitoring both Microsoft Exchange 2016 On-Premise solution and Exchange Online together with Azure Active Directory

Keywords: e-mail, communications, Microsoft Exchange 2016, Exchange Online, Office 365, Azure, System Center Operations Manager

Děkuji doc. Ing. Jiřímu Gajdošíkovi, CSc. za přínosné rady při vedení mé diplomové práce. Děkuji také své přítelkyni a rodičům, za podporu a trpělivost, kterou mi během studia poskytovali.

OBSAH

ÚVOD

Záměrem práce bylo zpracovat problematiku e-mailové komunikace, popis různých poštovních architektur, včetně přesunu e-mailových schránek z poštovního systému, který je umístěn v On-Premise do cloudového řešení Office 365 od společnosti Microsoft, a nichž by došlo k jakékoliv ztrátě dat s minimálním výpadkem pro koncové uživatele. Výstupem práce je vytvoření úspěšného návrhu pro migraci poštovních služeb do cloudového prostředí Office 365. Návrh je vytvořen pro devadesát e-mailových schránek.

Spolu s návrhem migrace poštovních služeb, byl také zpracován návrh na vytvoření aplikačního monitorování a to jak poštovního systému Microsoft Exchange 2016 On-Premise, tak Exchange Online. V rámci cloudových služeb dojde k návrhu, také k návrhu monitorování služby Azure Active Directory.

E-mailová komunikace je pro většinu organizací důležitá, proto veškeré operace na úrovní poštovních systémů lze považovat za kritické. A pokud nebudou e-mailové schránky naší domény dostupné, může to znamenat ztrátu lukrativního obchodu, anebo minimálně nebude organizace vypadat, tak profesionálně, jako ostatní organizace, které nemají s e-mailovou komunikací žádný problém. Proto je nutné veškeré operace na úrovní poštovního systémů důkladně promyslet a naplánovat.

V dnešní době není poštovní systém zodpovědný pouze za posílání a přijímaní e-mailů. Dnes je to databáze obsahující veškeré schůzky, kontakty, úkoly, a mnoho dalšího. Proto je nutné tento systém neustále aktualizovat a umožnit uživatelům přístup k nejnovějším funkcím a držet krok s okolním světem. Nyní již nelze odepřít snahu velkých firem vytvářející tyto systémy o přesun veškerých služeb do Cloudu. A proto se již například firma Microsoft, která je dodavatelem sofistikovaného poštovního systému Microsoft Exchange Server, snaží se přesvědčit stávající organizace o přesun, alespoň částečně do cloudového prostředí, tím, že některé funkce nabízí pouze uživatelům, kteří mají své e-mailové schránky v prostředí Exchange Online.

Práce popisuje veškeré dostupné migrační scénáře ze systému Microsoft Exchange Server On-Premise do Exchange Online, včetně snahy o výběr nejvhodnějšího scénáře, dle požadavků koncových uživatelů. Obsahem práce je také návrh na vytvoření synchronizace mezi lokální adresářové službě Active Directory a Azure Active Directory.

Možnosti cloudových služeb především od společnosti Microsoft se neustále mění, proto je reálně možné, že za několik měsíců bude možné zvolit nový migrační scénář, který by stanoveným požadavkům vyhovoval více. Proto se v této práci pracovalo s možnostmi, které jsou aktuálně dostupné v dokumentaci od společnosti Microsoft.

I. TEORETICKÁ ČÁST

1 ELEKTRONICKÁ POŠTA

Pošta byla do nedávna spojena pouze s dopisy, obálkami a společnostmi, které sloužily pro přenos fyzického dopisu od adresáta k příjemci. S příchodem sálových počítačů došlo v roce 1965, k výměně informace o čase mezi uživateli, pracujících na stejném sálovém počítači. Tato skutečnost, lze považovat za první elektronickou poštu. S nástupem internetu se stala elektronická pošta veřejně známou a zvyšovala se její popularita. [1]

V současnosti se lze setkat s pojmy jako e-mail nebo jen zkráceně mail. Samotná zkratka vychází z anglického slova electronic mail. E-mail jako takový, zcela nenahradil klasickou poštu, nicméně elektronická pošta patří mezi častý způsob komunikace, jak mezi firmami, tak celkově celou společností. [1]

1.1 E-mail

Electronic mail, patří mezi nejviditelnější služby, které zaměstnanci v oblasti informačních technologií zprostředkovávají. Z pohledu uživatele, který e-mail využívá je použití jednoduché, ale proces v momentě odeslání elektronického dopisu je složitější a prochází několika operačními procedurami, které běžný uživatel nevidí. [2]

1.1.1 Historie

Dle zjištěných informací historie elektronické pošty se datuje k roku 1965. Svým způsobem se dá e-mail považovat za starší než ARPANET či Internet. Na samotném začátku e-mailové komunikace si ještě nedokázal nikdo představit, že bude e-mail fungovat jako nějaký přehledný adresář elektronických dopisů, kdy mimo poštu obsahuje, náš elektronický diář, veškeré pracovní či nepracovní schůzky, připomínky, adresář obsahující telefonní čísla adresy a mnoho dalších služeb. Tehdy šlo pouze o předání souboru. Dotyčný příjemce po přihlášení viděl soubor obsahující zprávu, kterou odesílatel zaslal. Lze si to, představit tak, že šlo například o stejnou věc, jako když necháme vzkaz na stole vybraného příjemce. [1]

Ještě, než došlo k vzájemnému propojení více počítačů, zprávy se předávali pouze mezi uživateli na jednom počítači. S příchodem síťování, kdy mohly počítače vzájemně komunikovat, si tvůrci tohoto systému kladli otázku „Jakým způsobem rozeznáme, že tento e-mail má dorazit tomuto adresátovi?“. Bylo nutné vyřešit, jakým způsobem pošleme zprávu v „obálce“ a komu ji budeme vlastně adresovat. Stejně jako u fyzických dopisů, které posíláme poštou, musíme znát adresu příjemce. To se pokusil vyřešit Ray Tomlinson, který

zvolil znak „@“, sloužící pro přenos zpráv z jednoho počítače na druhý. Vznikl standard, který popisoval syntax, jak psát adresy pro správný přenos zaslané zprávy. První je jméno uživatele a poté, jméno počítače, **uživatel@název-pc**. V anglickém jazyce, lze tento znak přeložit jako **at** (u, při, na) nebo případně jako salamander. V českém jazyce se setkáme s pojmem zavináč. [1]

V roce 1974, týkající se období ARPANETU. Uživatelů, kteří e-mail využívali, byli v řádech stovek. Již, zde lze vidět, jakým došlo k vývoji v této oblasti. Jednalo se o vojenské uživatele, kteří pracovali pro Armádu Spojených států. [1]

S příchodem Internetu, a nástup osobních počítačů, chtěli i běžní uživatelé e-mail využívat. Vznikali takzvaní Off-line čtenáři, což znamená, že si lidé stáhli poštu z poštovního serveru v momentě, kdy byli připojení k Internetu, a jakmile měli poštu uloženou ve svém počítači, mohli si poštu číst, a hlavně připravit odpověď a v momentě, kdy chtěli poštu odeslat, stačilo se jen připojit k internetu a odeslat. Tato funkčnost existuje u některých aplikací dodnes. V minulosti to bylo spojené s vysokými poplatky za připojení k Internetu. [1]

V současnosti, přesto, co všechno internet v současnosti nabízí, e-mail zůstává jako jedna z nejdůležitějších služeb. Dle studie společnosti Radicati Group, která vznikla v lednu 2017, popisuje, že 3,7 bilionů uživatelů na internetu využívají e-mail. To znamená, že přibližně 54 % obyvatel na planetě používá e-mail. Pro porovnání, k jakému dochází vývoji, tak v roce 2009 stejná společnost vytvořila stejnou studii, kdy uvádí, že e-mail využívá 1,9 biliónů uživatelů. Společnost Radicati Group, předpokládá, že v roce 2021 dosáhne na služby e-mailu 4,1 biliónů uživatelů. [1]

2 FUNKČNOST E-MAILOVÉHO SÝSTEMU

Fungování poštovních služeb je založeno na několika částech celého systémů. Jádro funkčnosti poštovních služeb je stejné i s ohledem, kdo daný poštovní systém vytvářel. Existuje několik komponentů, které se mohou lišit názvem, ovšem princip fungování zůstává stejný. Tato pravidla jsou definována na základě dokumentů, které se zabývají nejrůznějšími aspekty fungování na Internetu, včetně chování poštovních služeb. Jedná se pouze o doporučení. V případě definování protokolů jsou tyto dokumenty brány, jako závazné standardy. Tyto dokumenty jsou označovány anglicky Request For Comment, zkráceně RFC.

2.1 E-mailová zpráva

Dokument RFC822 popisuje e-mailovou zprávu, jako text, který je rozdělen na dvě části. První část je hlavička a druhá tělo. Dokument popisuje především hlavičku, jak by měla vypadat. Tělo zprávy nijak nevymezuje, je ovšem nutné, aby hlavička byla před tělem, a tyto dvě části musí být rozděleny. Nejméně jedním prázdným řádkem. [3]

Hlavička zprávy, kterou popisuje jako sled položek, které jsou nazvány jako pole hlavičky. Jednotlivé položky musí začínat na novém řádku. Jednotlivé položky jsou označovány klíčovým slovem, které definuje význam položky. Zmíněné označování položek, sebou nese výhodu pro programy, které dané hlavičky musí analyzovat. Klíčové slovo je ukončeno dvojtečkou a poté následuje samotná hodnota. [3]

Mezi základní položky hlavičky patří položka, kde je uveden například odesílatel, příjemce, předmět zprávy. Dále se, ale může jednat o rozšířené položky hlavičky, které jsou označovány písmenem X-. Zde záleží na výrobci daného poštovního systému, nebo dokonce na samotném uživateli, jaké položky bude chtít. Je nutné brát zřetel, aby se rozšířené položky hlavičky nijak nepodobaly těm základním definovaným, podle dokumentu RFC 822. Pro příklad může rozšířená položka hlavičky vypadat takto „X-Mailer: Microsoft Outlook 16.0“, která určuje, jakým programem byla zpráva vytvořena. V tomto případě se jednalo o program Microsoft Outlook 2016. [3]

Položka hlavičky	Význam
From ?utf-8?q?Jaroslav_Han=C3=A1k?= <Hanak@seznam.cz>	Jméno odesilatele
Received: from email.seznam.cz with SMTP (192.168.0.51/16.2); Sat, 31 Mar 2018 12:22:22 +0200	Počítač email.seznam.cz předal tuto zprávu počítači hanak.cz
Return-Path: Hanak@seznam.cz	Údaj o zpáteční cestě k autorovi dopisu
Received: by hanak.cz (Exchange 16.00583) id 456565; Sat, 31 Mar 2018 12:22:22 +0200	Počítač hanak.cz převzal tuto zprávu
Date: Sat, 31 Mar 2018 12:22:22 +0200	Datum a čas, kdy byla zpráva předána k odeslání
From: "Hanak Jaroslav Seznam"	Odesilatel
Message-Id: <3nK.RcjF.10Ftpmw LXow.1Qsn0z@seznam.cz>	Identifikátor zprávy
Reply-To: hanak@seznam.cz	Kam mají být odesílány odpovědi
To: jaroslav@hanak.cz	Adresát
Subject: Jak to jde?	Předmět zprávy

Tabulka 1 – Hlavička e-mailu

2.2 Protokoly

E-mailové protokoly jsou sada pravidel, které pomáhají klientovi správně přenést informaci z a do poštovního serveru. Mezi tyto protokoly se řadí protokol SMTP, POP, IMAP.

2.2.1 SMTP

Protokol byl vyvinut již v roce 1982. Cílem Simple Mail Transfer Protocol (SMTP) je spolehlivě přenášet e-mailové zprávy. SMTP je nezávislý na konkrétním přenosovém subsystému a požaduje pouze spolehlivý uspořádaný datový kanál. Jedná se o přenos přes Transmission Control Protocol (TCP). Pro SMTP je určen autoritou IANA port 25. Na tomto portu komunikují poštovní servery. V případě, kdy autentizovaný uživatel odesílá email skrze poštovní server, využívá se port 587. Důležitou vlastností SMTP je schopnost přenášet e-mailové zprávy přes více sítí, tato schopnost je označována jako „SMTP mail relaying“. Protokol SMTP nabízí příkazy, na základě, kterých komunikuje poštovní server s dalším poštovním serverem. Příklad takovéto komunikace, lze vidět za využití protokolu Telnet. Jedná se o zkratku „teletype network“, tento protokol umožnuje uživatele vzdálené připojení ke vzdálenému počítači pomocí textového uživatelského rozhraní a na základě příkazů SMTP příkazů. [4]

Připojení přes telnet na server mail.domain.loc na port 25:

„telnet mail.domain.loc 25“

220 mail.domain.loc Microsoft ESMTP MAIL Service ready at Sat, 31 Mar 2018 15:33:27 +0200

Po připojení, lze vidět číslo 220, jedná se o SMTP kód, který vyjadřuje, že je SMTP služba připravena. Další informace uvádí jméno serveru, které je doplněno o informaci, že podporuje Extended Simple Mail Transfer Protocol (ESMTP). A poslední informací je datum a čas, kdy se k serveru připojujeme. Pro zobrazení příkazu, které poštovní server nabízí, je nutné napsat ESMTP příkaz „EHLO“. V případě, že by se jednalo o server, který by podporoval pouze příkazy SMTP, tak by bylo nutné napsat příkaz „HELO“. V případě, protokolu ESMTP se jedná o rozšíření klasického SMTP, který podporuje více příkazů. I v tomto případě, lze vidět, že poštovní systém Microsoft Exchange podporuje ESMTP. [5]

220 mail.domain.loc Microsoft ESMTP MAIL Service ready at Sat, 31 Mar 2018 15:33:27 +0200

EHLO

250-mail.domain.loc Hello [172.31.254.81]
250-SIZE 37748736
250-PIPELINING
250-DSN
250-ENHANCEDSTATUSCODES

250-STARTTLS
250-X-ANONYMOUSTLS
250-AUTH NTLM LOGIN
250-X-EXPS GSSAPI NTLM
250-8BITMIME
250-BINARYMIME
250-CHUNKING
250 XRDST

Po zadání příkazu „EHLO“, lze vidět možné funkce, které tento server nabízí. Začátek řádku vždy začíná SMTP kódem 250, který znamená, že požadovaná akce poštovního serveru je v pořádku. Jméno serveru s jeho IP adresou je uvedeno za tímto SMTP kódem. Parametrem SIZE, určuje server maximální velikost e-mailové zprávy v bytech, v tomto tedy 36 MB. [6]

Možnost PIPELINING, znamená, že existuje možnost zaslat několik příkazů za sebou, aniž by musel uživatel čekat na odpověď každého příkazu. [6]

Příkaz DSN patří mezi ESMTP příkazy, který umožní oznámení o stavu doručení. Funkce ENHANCEDSTATUSCODES uvádí, že server disponuje rozšířenými kódy o stavu. STARTTLS umožnuje šifrování spojení pomocí TLS. [6]

X-ANONYMOUSTLS, AUTH NTLM LOGIN, X-EXPS GSSAPI NTLM uvádí, jaké dostupné ověření vůči serveru je k dispozici. 8BITMIME uvádí možnost odesílat zprávy v 8 bitovém kódování, výchozí protokol SMTP využívá 7 bitové kódování. BINARYMIME, umožnuje binární kódování obsahu. Parametr XRDST je k dispozici, jelikož se jedná o poštovní systém Microsoft Exchange Server, a slouží k rozšíření protokolu pro komunikaci a cílového směřování. [6]

Zmiňované možnosti, které server nabízí prostřednictvím telnetu, je možno upravovat, podle přání administrátora a možnostech poštovního serveru.

2.2.2 POP

Pokud SMTP slouží k doručení e-mailových zpráv do poštovní schránky uživatele, která se nachází na poštovním serveru. Post Office Protocol slouží k tomu, aby se daný uživatel mohl k e-mailu, který byl určen jeho adrese dostat. Jedná se o stahování e-mailových zpráv z poštovního serveru na klienta. Jedná se aplikační protokol, který pracuje na principech TCP/IP připojení. [7]

Server naslouchá na portu 110	Klient	Význam
	Otevírání spojení	Klient otevírá relaci
+OK POP3 server ready <1257879899@domain.loc>		Server odpovídá, s tím, že služba POP3 je připravena
	User hanak	Jméno uživatele
+OK User Accepted		Uživatel je přijat
	PASS heslo.123	Vložení hesla
+OK Pass Accepted		Potvrzení hesla
+OK hanaks mail has 1 message (120 octests)		Sdělení, že v poštovní schránce se nachází jeden e-mail
	STAT	Potvrzení
+OK 1 message (120 octests)		Posílání zprávy
1 120		
.		
	QUIT	Příkaz pro ukončení
+OK Exchange POP3 server singing off		Server, ukončuje relaci, a čeká na další připojení
	Uzavření spojení	Klient potvrzuje ukončení relace

Tabulka 2 – Průběh POP3 komunikace

Nyní se využívá protokol POP3, který funguje na portu 110, pro nešifrovaný přenos, tzn., že lze sledovat komunikace v plain-textu. Pokud je nutné šifrovat komunikaci, používá se port 995. [8]

Pro zobrazení nových e-mailů je nutné se přihlásit a novou e-maily stáhnout. Stejné je to s odesláním e-mailů, pro odeslání je nutné se přihlásit a vynutit odeslání e-mailu. Proto je

nevýhodou, pokud chceme o novém příchozím e-mailu vědět okamžitě s tím, že dostaneme notifikaci na telefon, notebook či cokoliv jiného.

Mezi programy, které využívají, možnost připojení k poštovní schránce jsou například Microsoft Outlook, Thunderbird, Eudora atd…

2.2.3 IMAP

Obdobně jako u protokolu POP3 se využívá e-mailový klient, například Microsoft Outlook, Apple Mail, Thunderbird. Ovšem oproti POP3, který se ve své podstatě řadí mezi jednodušší protokoly vzdálené správy, nabízí IMAP daleko více možností. Mezi tyto možnosti se řadí možnost hledání pošty přímo na serveru, kde je uložena poštovní schránka uživatele, přesouvání pošty do uživatelsky vytvořených složek. Ačkoliv je u protokolu POP3 možnost pracovat pouze off-line a připojit se pouze v případě stáhnutí nové pošty či odeslání, IMAP nabízí práci jak off-line, tak on-line, Tzn., že uživatel dostane notifikaci ihned po obdržení e-mailové zprávy do svého poštovní schránky. Nejnovější verze tohoto protokolu se označuje, jako IMAP4. Pro IMAP s podporou TLS je vyhrazen port TCP 993, bez podpory TLS je to port TCP 143. [9][8]

2.3 Komponenty poštovního systému

Poštovní systém se skládá z programů, které hrají roli ať už v posílání, čtení či přijímání e-mailových zpráv.

2.3.1 Mail Transport Agent

Jedná se o software, který zajišťuje přepravu elektronické pošty v Internetu. Někdy označován, jako Mail Transfer Agent nebo Message Transfer Agent. Mezi nejznámější MTA patří Microsoft Exchange Server, Postfix, Sendemail, Exim a mnoho dalších. [9]

Přijímá zprávy od softwarového programu MUA (Mail User Agent), a následně je směřuje a předává do cílového MTA. [9] [10]

Tento program se také zabývá bezpečnostními otázkami, zdali má odmítnout či přijmout e-mail, a pokud zprávu odmítne z jakéhokoliv důvodu, tak se také musí postarat o informování odesílatele, že byl e-mail zablokován. V případě, že jedna e-mailová schránka má více e-mailových adres, tzn. má více aliasů, je nutné určit, že tento tvar e-mailové adresy patří konkrétnímu uživateli. Může se jednat o přeposílaní e-mailů. V případě, že MTA příjme e-mail, který nebyl určen tomuto MTA, splní funkci přeposlání správnému MTA.

Tyto funkce může MTA provádět bez autentizace odesílatele, jedná se o otevřené e-mailové přenášení anglicky Open Relay, této možnosti významně využívá Spam. Proto je vhodné nakonfigurovat MTA, tak aby se klient MUA musel vůči MTA autentizovat. [10]

2.3.1.1 Elektronická poštovní schránka – Mailbox

Fungování e-mailu je založeno na použití poštovních schránek, oproti běžným poštovním schránkám, které vlastní každý dům. Jsou tyto schránky elektronické. Takzvané elektronické poštovní schránky, anglicky Mailbox. [10]

Jedná se o prostor na disku, do kterého poštovní systém vkládá elektronickou poštu. Každý uživatel poštovního systému má privátní schránku. Jakmile poštovní systém příjme e-mail, který je určen příjemci, který má Mailbox v jeho systému, vloží tuto zprávu do této schránky. [10]

Uživatel poté může danou zprávu číst, obecně tyto schránky dovolují poštu mazat, tisknout, přeposílat, vytvořit koncept a později odeslat, lze hledat specifické E-maily. Každým novějším systémem jsou přidávány nové funkce, které může uživatel využít. [10]

2.3.2 Mail Delivery Agent

V momentě, kdy MTA přijme e-mail, přichází na řadu software, který zajišťuje doručení e-mailů do určených poštovních schránek uživatelů (MDA). Provádí činnosti, mezi které patří filtrování virů v e-mailu, spamu, a dále slouží k posílání, potvrzení o přečtení, přeposílaní e-mailů skupinám či uživatelům. Nejběžnější činností MDA je připojení do uživatelovy poštovní schránky, kde uloží příchozí e-mail. [9] [10]

2.3.3 Mail Access Agent

V případě, že je e-mail odeslán uživateli. Program Mail Delivery Agent (MDA) uloží zprávu na pevný disk vzdáleného poštovního serveru. Uživatelé ve většině případů nemají právo k přímému přihlášení na daný poštovní server, i když tyto servery obsahují poštovní schránky uživatelů. Je proto nutné vyřešit jakým způsobem se uživatelé do svých schránek mohou dostat z lokálního softwarového programu, který je anglicky označován jako Mail User Agent (MUA), tento program slouží k práci s elektronickou poštou. Zde na řadu přichází Mail Access Agent - software, který běží na vzdáleném serveru, slouží k zajištění přístupu uživatelů do svých poštovních schránek. Uživatel se tedy autentizuje vůči MAA serveru. Po úspěšném ověření má uživatel k dispozici svou poštu, jakým protokolem putuje

pošta ze serveru ke klientovi, záleží na možnostech MAA, zda daný protokol ovládá. Uživatel se může přihlásit k MAA a číst poštu pouze ze serveru, tzn., nevytváří se mu na lokálním klientu žádný soubor obsahující e-maily nebo naopak dojde k přihlášení k serveru MAA. Klient si poštu stáhne k sobě na lokální stanici a po stažení se ze serveru odpojí. Pokud se jedná o řešení poštovních služeb prostřednictvím produktu Microsoft Exchange Server, tak je nutné říci, že tento produkt v sobě obsahuje jak software MTA, MDA, tak také MAA. Tyto tři softwarové komponenty jsou schopny fungovat na jediném Windows serveru. [9][10]

2.3.4 Mail User Agent

Softwarový program, díky kterému může uživatel nakládat se svou poštovní schránkou. MUA musí být nakonfigurován s MTA k tomu, aby byl uživatel schopný skrz tento program odesílat e-maily. Následně musí být správně nakonfigurován s komponentou MAA, proto aby byl MUA schopen načítat elektronickou poštu a uživatel byl schopen číst se svými e-maily. Historicky existovala varianta, kdy MUA přistupoval přímo do poštovní schránky, bez připojení skrze MAA. Mezi tyto programy patří zejména Microsoft Outlook, Thunderbird. Jedná se o programy, které uživatel nainstaluje na koncové zařízení a skrze něj spravuje svou poštovní schránku. Existují některé MUA, mezi které se řadí Gmail, Yahoo, Hotmail nejsou nainstalovány lokálně na koncovém zařízení, ale jsou na webovém serveru. Uživatelé těchto služeb se dostávají ke svým poštovním schránkám pomocí webového prohlížeče. [9][10]

2.3.5 Mail Submission Agent

V minulosti uživatel odesílal e-maily pouze skrze MUA přímo do MTA, který zprávu odeslal. Toho ovšem mohl využít uživatel a odesílat e-maily, které nemusí být legální. Proto může být nasazen Mail Submission Agent (MSA), který je umístěn mezi MUA a MTA. MSA je v podstatě jen další MTA, který je nakonfigurován jiným způsobem. Mezi jeho činnosti patří čištění e-mailů, které zahrnují přidání či opravení záhlaví. Přidává automatické podpisy, dle politiky firmy, je schopen skenovat viry. A následně posílá e-mail na odchozí MTA. [9][10]

2.4 Proces posílání a přijímaní e-mailu na Internetu

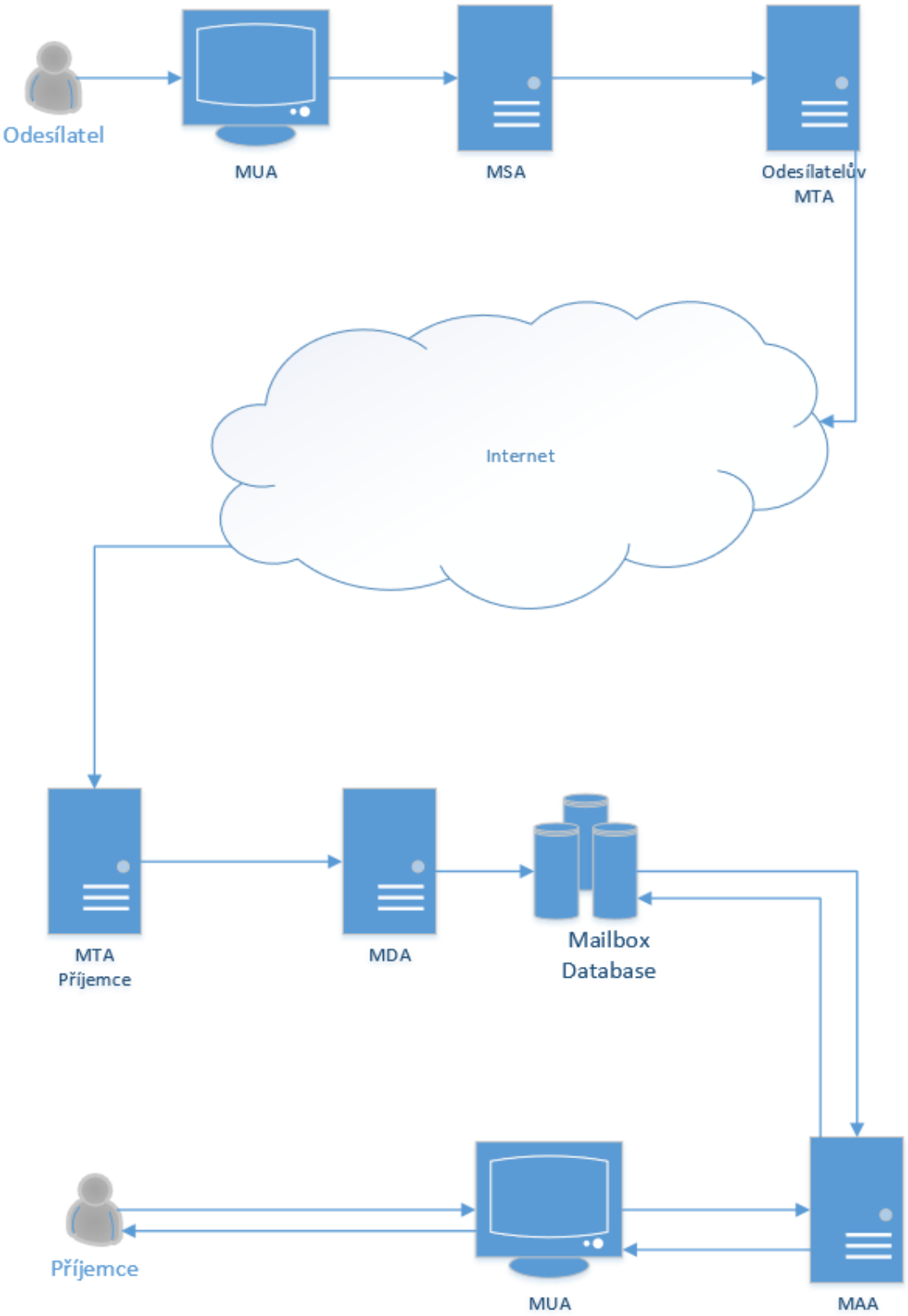
Proces již začíná u uživatele, kdy vytvoří e-mail, napíše předmět této zprávy a vybere příjemce, kterým daná zpráva bude zaslána, a to vše pomocí programu MUA. V momentě

kdy zvolí možnost Odeslat, MUA zpravidla přidá do hlavičky zprávy další informace a odešle zprávu na MSA, který tuto zprávu skenuje a v případě nutnosti upraví e-mail a poté odesílá na MTA. Dalším krokem je odeslání z MTA na MTA. Je možné, že než z odchozího MTA dojde zpráva na MTA příjemce, projde zpráva mezi vícero MTA. Proto každé MTA přidá do hlavičky zprávy informaci o tom, že zpráva prošla tímto MTA a díky tomu můžeme přesně určit, jakou cestou zpráva putovala. [10]

Jakmile dojde e-mail správnému MTA, ve kterém je poštovní schránka příjemce zprávy je zpráva předána MDA, který může zprávu filtrovat, přeposílat, třídit do různých složek a na závěr doručena do poštovní schránky uživatele. [10]

V případě, že odesílatel posílá e-mail více příjemcům v rámci jedné organizace dojde zpráva na MTA příjemců pouze jednou.

Jakmile e-mail dorazí do poštovní schránky, je majitel této schránky určitým způsobem informován. Příjemce využije MUA, kterým se daným způsobem autentizuje vůči MAA a v případě úspěšného ověření je schopen zprávu načíst ve svém MUA a přečíst. [10]



Obrázek 1 – Přenos SMTP zprávy [13]

2.4.1 Domain Name System and Mail Exchanger

V předchozí kapitole je zmíněno, jak se z Mail User Agenta odesílatele dostane do Mail user Agenta příjemce. Jak, ale Mail Transport Agent přijde na to, že tento Mail Transport Agent patří této doméně.

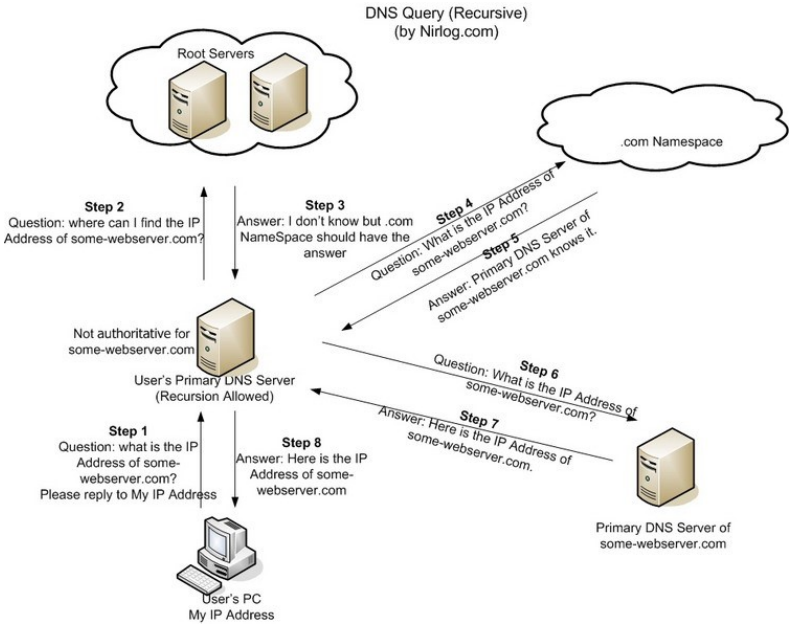
Pro zjištění IP adresy, na kterou má odesílající server e-mail odeslat, se využívá systém DNS a z tohoto systému se zjišťují záznamy typu MX. Odesílající server zjistí MX záznam, díky kterému určí, na kterou IP adresu bude zaslán e-mail. Může se jednat o poštovní server nebo firewall, který příchozí e-maily přeposílá na poštovní servery uvnitř dané domény. Záleží na každé doméně, jak má řešenou tuto problematiku.

2.4.1.1 Domain Name System (DNS)

Hlavní rolí DNS je překlad jmen na IP adresy, z důvodu, aby mohla fungovat síťová komunikace.

Pro příklad, pokud napíšeme do webového prohlížeče adresu https://tescosw.cz. Webový prohlížeč pomocí DNS vyhledá tento název a určí IP adresu serveru, ke kterému se má připojit. V tomto případě se jedná o doménu tescosw.cz.

DNS server obsahuje databázi těchto záznamů, díky kterým je schopen přeložit jméno na IP adresu. Ovšem není schopen udržovat databázi všech záznamů, které jsou dostupné na Internetu, proto jsou záznamy, které nemá v databázi distribuovány mezi mnoha servery DNS navzájem. Existuje hierarchie serverů, která má několik úrovní od 0 do 127, první úroveň patří kořenovému serveru. Poté se dělí větve na jednotlivé domény. Zjednodušené schéma řešení dotazů vypadá takto. [11] [12]



Obrázek 2 – Princip DNS [51]

2.4.1.2 Mail Exchanger

V případě zadání adresy https://tescosw.cz do prohlížeče, tak získáme IP adresu serveru, ke kterému se máme připojit. V případě, že odesíláme e-mail na adresu @tescosw.cz znovu do tohoto procesu vstupuje DNS server. Odesílající poštovní server vyhledá záznam MX v DNS v následujícím pořadí. Podívá se na autoritativní DNS server, patřící doméně tescosw.cz. Mezi autoritativní DNS servery se řadí ty servery, které trvale udržují záznamy k dané doméně. Dotáže se tohoto serveru na záznamy MX. DNS server vyhledá záznamy typu MX a zjistí jejich IP adresy. [12]

Záznamy lze vyhledat prostřednictvím programu nslookup.exe, který je k dispozici v operačních systémech Windows.

V případě domény microsoft.cz je dotaz na MX záznamy následující:

Non-authoritative answer:
tescosw.cz MX preference = 45, mail exchanger = edge15.tescosw.cz
tescosw.cz MX preference = 35, mail exchanger = edge14.tescosw.cz

Na prvním místě je uveden název domény, poté následuje priorita. To proto, kdyby doména obsahovala více serverů, na které je možno e-mail odeslat, a to z důvodu vysoké dostupnosti. Pravidlem je, že nejmenší preference znamenají nejvyšší prioritu. Pokud tento server v případě domény tescosw.cz, edge14.tescosw.cz nebude schopen navázat komunikaci. Vstupuje

do tohoto procesu druhý záznam, edge15.tescosw.cz. parametr mail exchanger určuje server, na který se bude e-mail zasílat. Stále se jedná o slovní název s tím si již DNS systém poradí jako v případě zadaní adresy https://tescosw.cz do webového prohlížeče. IP adresu serveru edge14.tescosw.cz, lze jednoduše zjistit prostřednictvím programu ping.exe. [12]

2.5 Zabezpečení e-mailové komunikace

Existuje mnoho způsobu a doporučení jak chránit e-mailové zprávy. Chránit se proti spamu, malwaru, spoof e-maily. Jelikož v oblasti poštovních serverů je převážná část komunikace v režimu klient server závislá na protokolech HTTPS či SMTP, a služby poštovního serveru jsou publikované do Internetu, je problematika zabezpečení poštovních serverů velmi důležitá. [14]

2.5.1 Zabezpečení SSL/TLS

Transport Layer Security TLS a Secure Socktes Layer SSL, jsou šifrovací protokoly, které jsou určeny k zabezpečení komunikace v síti pomocí bezpečnostního certifikátu určeným pro šifrování připojení mezi počítači. TLS nahrazuje vrstvu SSL, většina poštovních serverů využívá protokol TLS k šifrování připojení mezi poštovními servery. Jakmile dojde k vytvoření šifrovaného spojení, všechna data jsou odeslána prostřednictvím tohoto připojení a jsou přenesena zašifrovaným kanálem. Pokud je e-mailová zpráva odeslána prostřednictvím šifrovaného připojení TLS, nemusí být tato e-mailová zpráva nutně šifrována. Je to důvodem toho, jelikož TLS nešifruje e-mailovou zprávu, ale pouze připojení. [14] [15]

Ovšem například Exchange Online, dokáže šifrovat samotnou e-mailovou zprávu, jedná se o technologii Office Message Encryption. [15]

V rámci vyjednávání k vytvoření HTTPS relace mezi serverem a klientem dojde k dohodě o nejvyšší použitelné verzi protokolu SSL/TLS. Protokol SSL byl přejmenován na TLS, které existují ve verzích TLS 1.0, TLS 1.1, TLS 1.2 a budoucnu TLS 1.3. [14]

2.5.1.1 Kryptografie

Obvykle se při využití HTTPS komunikace konstatuje, že jde o komunikaci šifrovanou. To může vyvolat dojem, že co je šifrované, tak je bezpečné. To ovšem nemusí být pravda, v případě, kdy se využije k zašifrování prolomený kryptografický algoritmus, který útočník dokáže dešifrovat, de facto v reálném čase. [14]

V oblasti HTTPS se využívá mix kryptografických algoritmů v rámci symetrického a asymetrického šifrování, hashovacích algoritmů a algoritmů určených pro výměnu klíčů. [14]

V rámci bezpečnosti by měly být zakázané všechny kryptografické kombinace, anglicky nazýváno „Cipher Suite“, které obsahují RC2, RC4 atp. Naopak za prokazatelně bezpečné algoritmy jsou například AES, SHA-2, RSA, Diffe-Hellman následně by se měla zapnout funkce Forward Secrecy pro pravidelnou obměnu klíčů využitých v relacích. [14]

2.5.1.2 Certifikát

V případě využití SSL/TLS je nutné na straně serveru a případně na straně klienta důvěryhodný certifikát, díky kterému se ověří identita. Tento certifikát je také nositelem veřejného klíče, který je využit pro kryptografické operace. Úroveň využití kryptografie by měla být alespoň SHA256 a SHA2048. Z hlediska poštovního serveru, je administrátor nucen vytvářet žádosti na nové certifikáty, případě obnovu certifikátu. [14]

2.5.2 Sender Policy Framework

Často označováno zkratkou SPF, jedná se o validační systém, který slouží k ochraně před spamem. Princip je dán tím, že ověřuje IP adresu odesílatele. Z toho vychází to, že pomůže administrátorům určit, které servery mohou za danou doménu odesílat e-mailové zprávy. Pro aktivování této ochrany je nutné vytvořit TXT záznam ve veřejném DNS. Server tedy pomocí DNS záznamu určí, zda je e-mailová zpráva z příslušné adresy pro danou doménu schválena. Tato problematika je popsána například v RFC 7208. [16]

Příklad takového TXT záznamu lze zjistit pomocí nslookup.exe

Nslookup –type=TXT tescosw.cz
tescosw.cz text = "v=spf1 a mx -all"

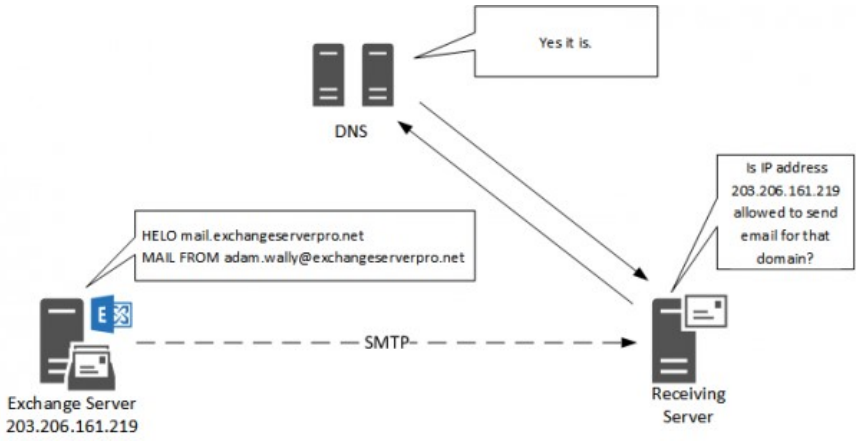
Příkazem nslookup, se vyhledají záznamy TXT pro doménu tescosw.cz, výsledkem je tedy záznam tescosw.cz text=“vspf1 mx -all“, lze vidět verze SPF a následně hodnota mx-all. To znamená, že všechny IP adresy uvedeny v MX záznamech pro danou doménu mohou za tuto doménu zasílat e-mailové zprávy. Pro zjištění konkrétních IP adresy v MX záznamech je například možné zadat tento příkaz.

Nslookup –type=MX tescosw.cz

tescosw.cz MX preference = 45, mail exchanger = edge15.tescosw.cz
tescosw.cz MX preference = 35, mail exchanger = edge14.tescosw.cz

Pro zjištění IP adresy serveru edge15.tescosw.cz a edge14.tescosw.cz, stačí například využít příkaz ping.

Ping edge15.tescosw.cz
Pinging edge15.tescosw.cz [94.124.184.167]
Ping edge14.tescosw.cz
Pinging edge14.tescosw.cz [94.124.184.131]



Obrázek 3 – Princip SPF [17]

2.5.3 Domain Keys Identified Mail

Zkráceně DKIM, vychází z technologie od společností Cisco Systéms a Yahoo. Jedná se o rozšíření, které nijak nezasahuje do poštovního systému je s ním naopak plně kompatibilní. Princip spočívá v přidání hodnoty DKIM-Signature do hlavičky. Jedná se o elektronický podpis generovaný SMTP serverem odesílatele. [18]

Na rozdíl od klasických podpisů e-mailových zpráv, v případě technologie DKIM nemusí koncový uživatel nic řešit. Veřejná část klíče je uložena ve veřejném DNS v podobě TXT záznamu. Díky tomu může příjemce prostřednictvím DNS získat a ověřit pravost přijaté e-mailové zprávy. Tento klíč je uložen ve speciální subdoméně, která začíná nesrovnatelným selektorem a následuje povinnou části _domainkey. Tento selektor je vždy uveden v hlavičce zprávy, hned za znakem s=. [18]

Nevýhodou SPF, je že svazuje doménu odesílatele s konkrétními IP adresami, ze které mohou odcházet e-mailové zprávy. DKIM, tedy využívá elektronický podpis, a přeposílání jednou podepsané pošty, nijak princip neporušuje.

3 MOŽNOSTI POSKYTOVÁNÍ POŠTOVNÍCH SLUŽEB

Na trhu existuje mnoho produktů, které zajištují odesílaní či přijímaní e-mailů. V současné době to, ale již není pouze o odesílání a přijímání, dnes se jedná o spoustu další funkcí, které tyto produktu nabízejí. Může se jednat o online archivování své pošty, vytváření schůzek, a porovnávat, zda daný kolega je v daný čas schopen se schůzky zúčastnit nebo již má ve svém kalendáři nějakou událost a proto mi aplikace doporučí jiný termín.

V době notebooků, chytrých telefonů, tabletů, chytrých hodinek je možnost spravovat e-mailové schránky de facto ze všech dostupných zařízení. Je pravidlem, že uživatelé dostanou v reálném čase upozornění, že jim přišel nový e-mail, že schůzka bude již za patnáct minut. Pro příklad, pokud aplikace spravující e-mailovou schránku má přístup k údajům o poloze telefonu, může nám doporučit nejbližší cestu a navigovat nás až do místa plánované schůzky.

Jsou k dispozici varianty, kdy chceme využívat poštovní systém na operačním systému Windows nebo varianta, kdy se jedná o open source systémy na operačním systému Linux. Další možností může být Cloud Computing. Jedná se o využití hardwaru, aplikací, uložišť, služeb, které jsou dostupné vzdáleně. Plusem této možnosti je, že administrátor firmy, která využívá tuto možnost, nemusí instalovat, aktualizovat či starat se o samotné datacentrum. Znamená to, že přístup k citlivým datům má třetí osoba. Poté už záleží na konkrétním subjektu, zda toto riziko podstoupí či nikoliv.

Mezi nejdůležitější věcí v rámci rozhodování, zda využít Cloudových služeb či se spoléhat na řešení On-Premise je rozhodnout, kde jsou data konkrétního subjektu ve větším bezpečí.

Z hlediska On-Premise řešení je největším plusem kontrola nad kritickými daty firmy. Ovšem pokud má IT oddělení pevný rozpočet, a případě, že bude nutné investovat nemalé finanční prostředky do zabezpečení firmy. Může vzniknout pro danou firmu komplikace, zda investuje do nákupu hardwaru, softwaru a licencí k danému softwaru nebo nebude investovat a podstoupí bezpečnostní riziko.

Nejen z tohoto důvodu je trendem dnešní doby pracovat v takzvaném hybridním řešení, kdy aplikace jsou umístěné v datacentru firmy, zatím co uživatelé přesouvá do Cloudu.

Cloud jako takový, sebou nese spoustu výhod, ale přináší také rizika, která je nutné vyhodnotit v rámci analýzy vyhodnocování rizik. V rámci této analýzy se budou rizika lišit

v závislosti na citlivosti dat a na tom, jak je účinný bezpečnostní systém provozovatele Cloudových služeb. Jelikož se jedná o sdílenou infrastrukturu, je cílem pro mnoho útočníků.

Pokud vznikne zranitelnost na vrstvě infrastruktury, platforem, aplikací ovlivní to všechny vrstvy bez výjimky. Dle zprávy od Cloud Security Alliance z roku 2016, vyšlo, že jediná část zranitelnosti či špatná konfigurace mohou vést k ohrožení celého Cloudu.

Údaje uživatelů jsou tak, uloženy na schváleném místě obou stran, neznáme koncovému uživateli. Pokud jsou data v jiném státě či kontinentě mohou podléhat místním zákonům. Proto je důležité komunikovat a domluvit se s poskytovatelem Cloudových služeb, docílit dostatečného zabezpečení.

Z pravidla poskytovatelé těchto služeb investují více prostředků do zabezpečení infrastruktury a zavádějí vyšší úroveň bezpečnostních kontrol. Tito poskytovatelé mají výhodu v tom, že se zprostředkovávají služby více subjektům, rychleji se od nich učí a následné poznatky mohou uplatnit pro ostatní zákazníky.

Smlouva mezi zprostředkovatelem a zákazníkem se musí zabývat bezpečnostními riziky a způsobem jejich pokrytí, určit kdo bude mít přístup k uživatelským datům. Všechny tyto dohody jsou zapsány do Service-level agreement, případně do jiné smlouvy.

3.1 On-Premise

Mezi hlavní výhody tohoto řešení je větší kontrola a lepší dostupnost. Firma se může cítit sebevědoměji, pokud má veškeré data na svém hardwaru, který spravují její zaměstnanci. Pokud bude firma chtít některá data okamžitě získat, v případě, že využívá Cloudové řešení může být toto problém. Mezi největší dodavatelé On-Premise řešení patří společnost Microsoft se svým Microsoft Exchange Serverem, IBM a IBM Notes/Domino, Kerio Technologies a jejich KerioConnect.

3.1.1 Microsoft Exchange

Nejedná se pouze o e-mail server, ale také kalendářový server vytvořen společností Microsoft. Tento produkt funguje pouze na operačním systému Windows Server. Exchange podporuje protokoly SMTP, POP, IMAP, ale také proprietární protokol MAPI a EAS. [2]

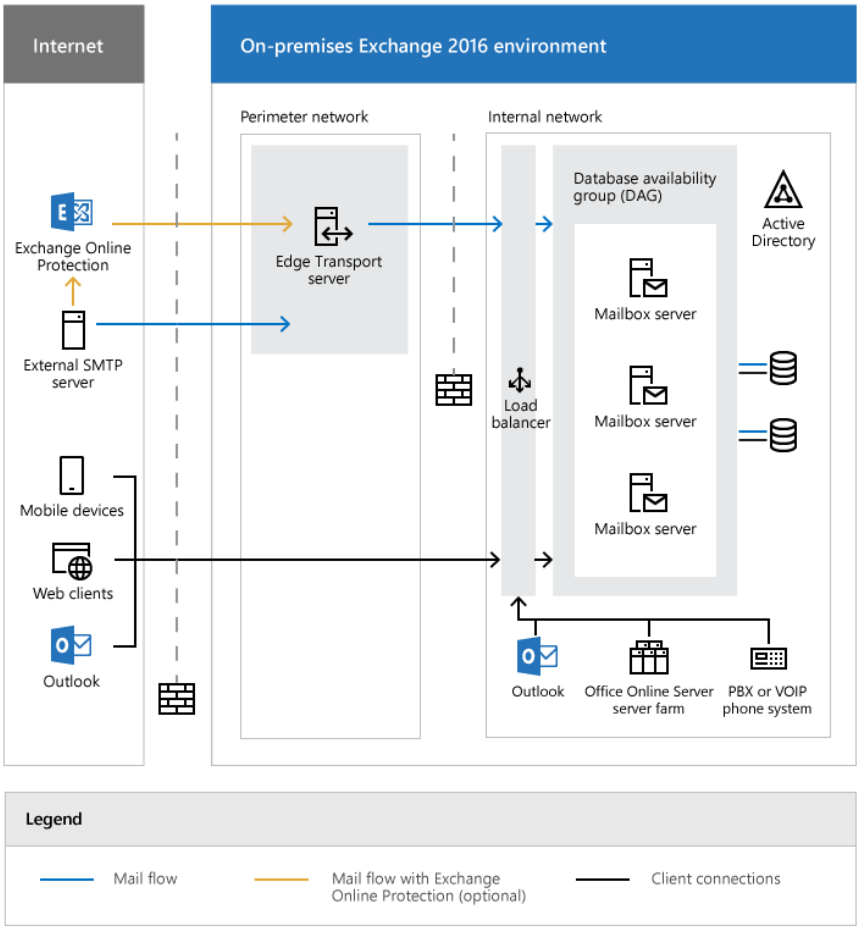
Nejnovější verzí je Microsoft Exchange Server 2016, jedná se o osmou verzi. V předchozí verzi se Microsoft Exchange Server 2013 rozděloval na roli Client Access a Mailbox. V nynější verzi mluvíme pouze o Mailbox roli. [2]

3.1.1.1 Architektura On-Premise Exchange 2016

Hlavní rolí je Mailbox, další rolí, kterou Exchange nabízí je role Edge Transport. Jedná se o hraniční server, ve většině případů v demilitarizované zóně, sloužící k odesílání a přijímaní pošty. Jedná se tedy o externí SMTP provoz. Edge je schopen filtrovat obsah zprávy, a na základě stanovených pravidel e-maily nepropouštět na Mailbox server. Plní funkci anti-spamu. [2] [19]

Exchange 2016 využívá architekturu jednoho bloku, který poskytuje e-mailové služby pro řešení na všechny velikosti. Od malých organizací po velké nadnárodní společnosti. [2] [19]

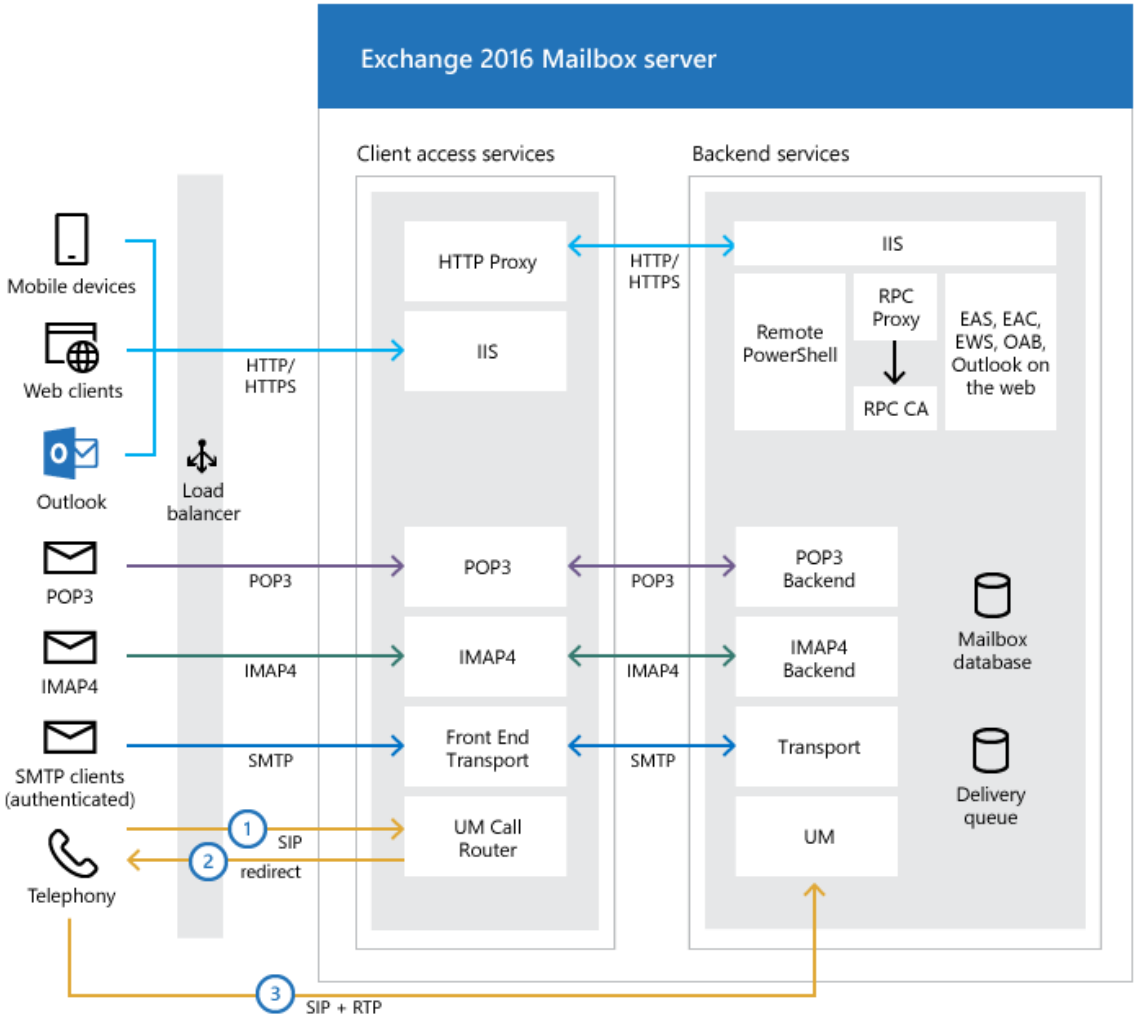
Mailbox servery poskytují transportní služby, které slouží ke směrování pošty. Dále obsahují databáze poštovních schránek, které zpracovávají a vykreslují data. Dále služby klientského přístupu, které přijímají klientská připojení. Tyto služby se nazývají Front End služby a jsou odpovědné za směřování nebo předávání připojení odpovídajícím Back End službám, které jsou také obsahem mailbox serveru. Principem je, aby se klienti nepřipojovali napřímo k těmto Back End službám. [2] [19]



Obrázek 4 – Architektura Microsoft Exchange 2016 [19]

3.1.1.2 Client Access Protocol Architecture

Jedná se o služby přístupu na Exchange server, které jsou odpovědné za přijetí všech forem připojení klienta. Tyto služby, které se nazývají jako Client Access Services (Front End), dále předávají tyto přijaté připojení na cílové Backend Services (Back End). Tyto Back End služby se mohou nacházet na místním serveru nebo na serveru vzdáleném, závislé na to, kde je aktivní kopie e-mailové schránky uživatele.[2][19]

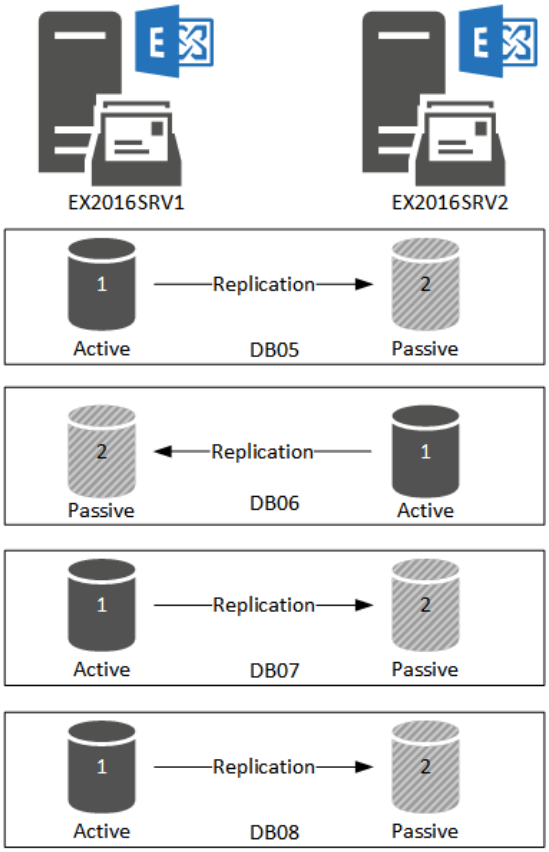


Obrázek 5 – Klientský přístup k Microsoft Exchange 2016 [19]

Protokol využívaný klientem, bude také sloužit k předání mezi Frontend službou a Backend službou. V případě, že se klient připojí pomocí HTTP protokolu, mailbox server využije protokol HTTP k předání na požadavku na cílový mailbox server. V případě, že klient využívá POP nebo IMAP protokol bude předávající protokol POP nebo IMAP. [19]

3.1.1.3 Database Availability Group

Database Availability Group (DAG), je základní komponentou Mailbox serveru, která slouží k vysoké dostupnosti, a síťové odolnosti. Jedná se o skupinu maximálně šestnácti Mailbox serverů, které hostí skupinu databází. Poskytují automatickou obnovu na úrovni databáze v případě poruchy individuálních Mailbox serverů či databází. Jedná se o databáze o aktivní a pasivní, vždy může být jen jedna databáze aktivní. Aktuálnost všech databází se provádí pomocí replikace, kdy aktivní databáze předává nové data pasivním. [2][20]



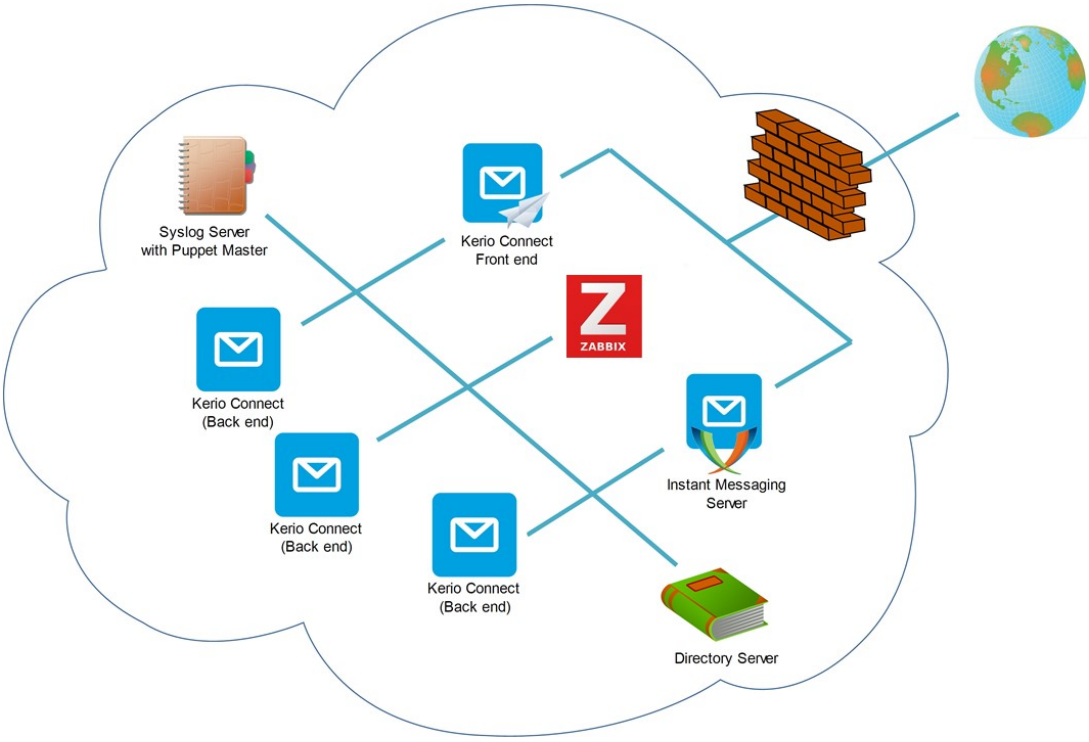
Obrázek 6 – Princip Database Availability Group [20]

3.1.2 Kerio Connect

Kerio Connect, je dostupný jako alternativa k Microsoft Exchange Server. Stejně jako Exchange Server nabízí podporu pro protokoly POP, IMAP, EAS, MAPI. Označuje se za méně náročný na správu oproti MS Exchange. Existuje varianta KerioConnect Cloud, kdy se využívá Cloudových služeb, případně možnost KerioConnect On-Premise.

3.1.2.1 Architektura

KerioConnect nabízí možnost „Single Server“, kdy stačí pouze jeden server. Může se jednat o virtuální nebo fyzický server, operační systém může být Windows Server nebo Linux. Jedná se o řešení, kdy jsou všechny komponenty nainstalovány na jednom serveru. Stejně jako Exchange Server rozlišuje služby na Backend a Frontend. Nově je k dispozici varianta „Multi-Server“, určen větším organizacím, jelikož zajistí vyšší výkon. Jedná se o modulární řešení. [21]



Obrázek 7 – Architektura Kerio Connect [22]

Schéma popisuje architekturu poštovních služeb KerioConnect v rámci modelu „Multi-Server“. Požadavek klienta, vždy dorazí nejprve na Frontend služby, jelikož KerioConnect podporuje Instatn Messaging, je možné, aby požadavek dorazil první na tuto komponentu. Komponenta IM, umožňuje sledovat Free/Busy stav uživatelů. Jedná se o možnost zasílat zprávy v reálném čase, jedná se o tzv. Chat. Oproti e-mailové komunikaci, má IM výhodu v rychlejší komunikace, kdy je zpráva doručena v rámci stovek milisekund. Požadavek dále putuje na Backend služby, kde dojde k předání do uživatelovy e-mailové schránky, v případě IM dojde k zobrazení v klientu určeným pro IM. V případě, že uživatel není k dispozici, dojde k uložení historie konverzace do jeho poštovní schránky. [21][22]

Kerio Connect podporuje stejně jako MS Exchange MUA Outlook, Thunderbird, a mnoho dalších. [21]

3.2 Cloud

Varianta, která je trendem dnešní doby, a to nijak bez důvodu. Cloudové řešení umožňuje využívat poštovních služeb, aniž by se organizace musela spravovat poštovní servery. Odpadá, tak nutnost aktualizovat poštovní software, operační systém, na kterém tento software funguje. Infrastruktura je tedy spravována třetí stranou, je vhodné a doporučené, pokud to dodavatel řešení umožňuje monitorovat infrastrukturu, na které funguje náš poštovní server. Ale také monitorovat samotný software. Mezi největší dodavatelé tohoto řešení je firma Microsoft v rámci řešení Office365, který obsahuje mimo poštovní služby, také souborové služby, služby pro IM, služby pro správu intranetu, adresářové služby a mnoho dalších.

3.2.1 Exchange Online

Jedná se o produkt v rámci balíku služeb Office365. Exchange Online je e-mailový server v cloudu, který mimo jiné zajišťuje synchronizaci kalendářů, kontaktů, úkolů a hlasové služby. To znamená, že oproti Microsoft Exchange On-Premise, kde jsou data uložena na hardwaru v našem datacentru na našem hardwaru, v případě Exchange Online jsou data uložena v datacentrech Microsoftu. Exchange Online umožňuje prakticky nepřetržitý přístup k e-mailům ze všech zařízení, které jsou připojeny k Internetu. V rámci synchronizace e-mailů využívá proprietární protokol EAS, jedná se o protokol Exchange ActiveSync Exchange Online disponuje ochranou proti malware a spamu. K dispozici je také podpora šifrování zpráv. [23]

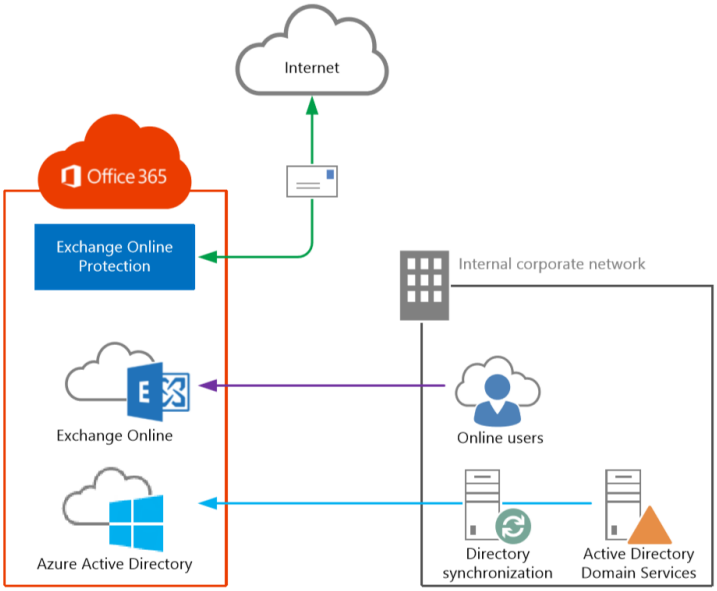
Datacentra hostící Exchange Online, jsou v rámci Evropské Unie v Irsku, Nizozemsku Rakousku a Finsku. V případě, že v rámci smlouvy určíme, že se nacházíme na území EU, je smluvně dané, že organizace bude využívat tyto datacentra. Dle smlouvy Microsoft uvádí dostupnost služeb 99,99%. Velikosti poštovních schránek se udávají v rámci předplatného v rozmezí 50-100 GB na uživatele. [23][24]

3.2.1.1 Architektura

Lze využít několika scénářů, které Office 365 nabízí. Je možné využívat pouze Exchange Online nebo lze využít Exchange On-Premise spolu s Exchange Online. Toto řešení se nazývá Hybridní.

3.2.1.1.1 Exchange Online

Řešení, ve kterém se využívá pouze poštovního server Exchange Online. Nabízí obdobné funkce jako Exchange On-Premise 2016. Z pohledu správy serveru a instalací aktualizací provádí pouze zaměstnanci Microsoftu. K dispozici je i Exchange Online Protection, jedná se o anti-spamovou a anti-malware ochranu. V případě, že organizace již má adresářové služby v rámci On-Premise a chceme, aby uživatelé, kteří jsou již v On-Premise Active Directory využívali poštovních služeb Exchange Online. Je nutné provést synchronizaci Active Directory a Azure Active Directory, kdy dojde k synchronizaci objektů v interním Active Directory, taktéž dojde k synchronizaci hesel. Výsledkem bude, že uživatelé jsou jak v On-Premise Active Directory tak v rámci Office 365. [25]



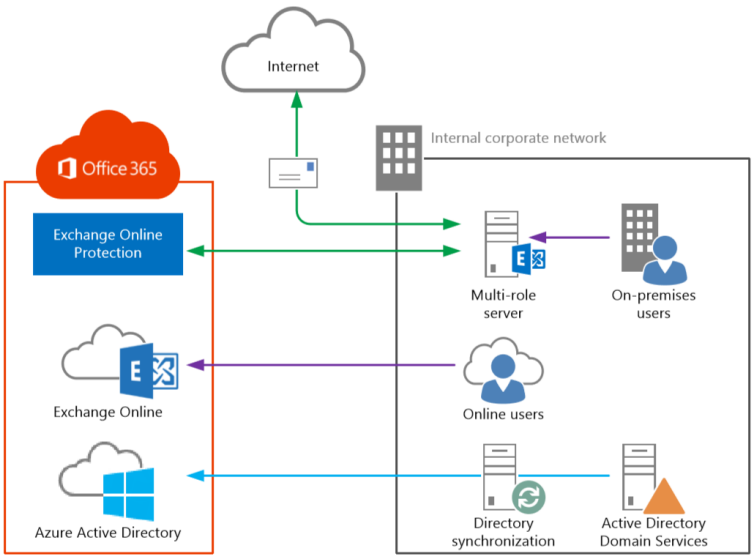
Obrázek 8 – Architektura Exchange Online [25]

Exchange Online Protection, poskytuje ochranou funkci. Pomáhá chránit e-mailovou komunikaci, včetně ochrany proti nebezpečným přílohám v e-mailové zprávě. Každá e-mailová příloha prochází anti-malwarovou analýzovou v reálném čase, která využívá

techniky učení počítače k vyhodnocení obsahu. V případě zjištění nebezpečné přílohy, dojde k umístění do určeného místa tzv. komory, ještě před odeslání příjemci. EOP, taktéž poskytuje ochranu proti škodlivým odkazům prostřednictvím skenování obsahu. Ke zkoumání dochází v reálném čase, kdy na ně uživatel klikne. Pokud je odkaz nebezpečný, uživatel dostane upozornění, a dojde k zablokování cílové URL. Oproti řešení On-Premise, nabízí Office 365 lepší a podrobnější reporty, takže správci mohou vidět, kteří uživatelé chtějí navštívit nebezpečné webové stránky. Reporty jsou k dispozici na webových stránkách Office 365, případně lze nastavit notifikační kanál, kdy report dostane vybraný uživatel. [26]

3.2.1.1.2 Exchange Hybrid

V tomto řešení, jsou některé e-mailové schránky hostované v Exchange On-Premise řešení a některé v Exchange Online. Z toho vychází, že se stále využívá On-Premise infrastruktury spolu s infrastrukturou Microsoftu. Přesuny z On-Premise do Exchange Online se provádí, dle přání administrátora. Může se jednat o jednotlivé přesuny nebo o skupiny uživatelů, kteří budou migrováni. Hybridní nasazení může sloužit jako přechodný krok, než dojde k úplnému přesunu uživatelů do Exchange Online. K nasazení je nutné mít k dispozici Exchange On-Premise server, Microsoft Office 365, nainstalovaný Hybrid Configuration Wizard na některém serveru v On-Premise infrastruktuře a naimplementovanou Azure Active Directory synchronizaci s interním Active Directory, jedná se o stejný případ, kdy využíváme poštovní služby pouze prostřednictvím Exchange Online. [25]



Obrázek 9 – Hybridní řešení Exchange Online [25]

II. PRAKTICKÁ ČÁST

4 NÁVRH ŘEŠENÍ MIGRACE POŠTOVNÍCH SLUŽEB

Migrovat e-mailové schránky do Office 365 je možné mimo Exchange On-Premise migrovat, také z jiných e-mailových systémů. Sami uživatelé si mohou svoje vlastní e-maily, kontakty či další informace z poštovní schránky naimportovat do schránky hostované v Office 365.

Ještě před samotnou migrací je vhodné nastudovat informace o omezeních a osvědčených postupech pro implementaci Exchange Online.

4.1 Výchozí stav

V popisovaném návrhu již existují e-mailové schránky uživatelů v On-Premise infrastruktuře, migrace se bude týkat pouze jedné domény v rámci celého lesa Active Directory, ve kterém je několik domén. Jedná se o poštovní systém založený na architektuře Microsoft Exchange Server 2016, v infrastruktuře se nacházejí dva poštovní servery, které se jmenují EXCH11.domena.loc, EXH12.domena.loc.

Celkem bude migrováno 90 poštovních schránek.

4.1.1 Technické specifikace poštovních serverů

Jméno serveru: EXCH11.domena.loc

Operační systém: Windows Server 2016

Verze Microsoft Exchange: Microsoft Exchange CU9, 15.01.1466.003

Procesor: 2x Intel(R)Xeon(R) CPU E5-2650v3 @2.30GHz

Operační paměť:24 GB

Diskové uložiště: 100GB (systémový disk)

Databázový disk: 500 GB (DB01_16)

Databázový disk: 500 GB (DB02_16)

Jméno serveru: EXCH12.domena.loc

Operační systém: Windows Server 2016

Verze Microsoft Exchange: Microsoft Exchange CU9, 15.01.1466.003

Procesor: 2x Intel(R)Xeon(R) CPU E5-2650v3 @2.30GHz

Operační paměť:24 GB

Diskové uložiště: 100GB (systémový disk)

Databázový disk: 500 GB (DB01_16)

Databázový disk: 500 GB (DB02_16)

Název Database Availability Group: DAG_2016

4.2 Cílový stav

Cílem je vytvořit návrh na úspěšnou migraci poštovních služeb uživatelů do prostředí Office 365. Tudíž veškeré e-mailové schránky, určené k migraci, budou hostované v Exchange Online, provoz SMTP bude směřovat na servery v Cloudu, nejprve na Exchange Online Protection a poté na Exchange Online.

Ještě před migrací bude vytvořena synchronizace mezi lokální Active Directory a Azure Active Directory, aby se uživatelé mohli přihlásit v interní síti se stejnými přihlašovacími údaji jako při přihlášení do Cloudu.

4.3 Azure Active Directory Synchronizace

Vytvoření synchronizace umožní uživatelům v lokální Active Directory využívat stejné uživatelské účty, jak pro přihlášení k prostředkům v lokální síti, tak pro přihlášení v Cloudu. Bude tedy umožněno jednorázové přihlášení. Tohoto se dá využít v momentě, kdy je uživatel přihlášen ke klientovi v lokální síti pod účtem, který je v lokální Active Directory a spustí aplikaci Outlook, díky této synchronizaci nebude muset pro úspěšné přihlášení zadávat přihlašovací údaje, podmínkou je, aby měl již svou poštovní schránku přesunovou v Exchange Online. Jelikož dojde k synchronizaci, bude účet v lokální Active Directory, tak v Azure Active Directory.

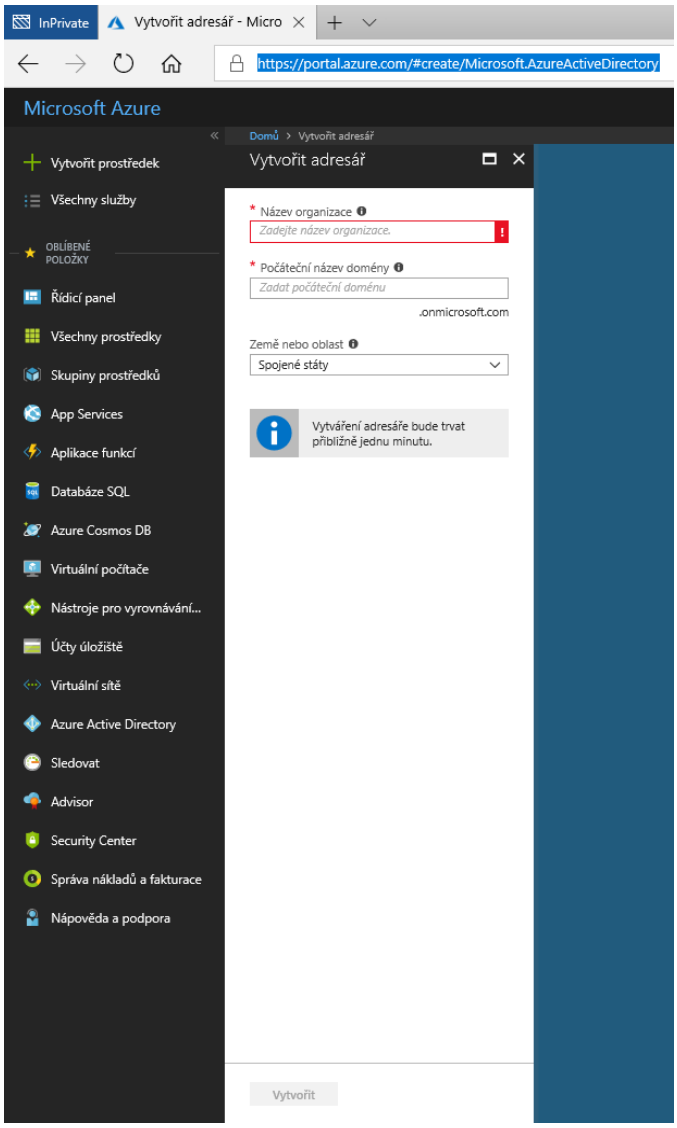
4.3.1 Vytvoření Azure AD Tenantu

Anglickým slovem tenant se označuje zástupce organizace v Azure Active Directory. Tenant je vyhrazená instance služby Azure Active Directory, kterou organizace vlastní. Vytvoření partnerství se může provést tím, že se organizace registruje ke cloudové službě Microsoftu,

může se jednat o Office 365, Microsoft Intune, Azure. Každý tentant se od ostatních tenantů odlišuje a je od nich oddělený.[27]

Tenant obsahuje uživatelé organizace a informace o nich, jako například hesla, data uživatelského profilu, obsahuje skupiny a informace o členech dané skupiny. [27]

Vytvoření se provádí na stránkách https://portal.azure.com/, po vytvoření účtu je nutné zadat název organizace a název domény. [27]

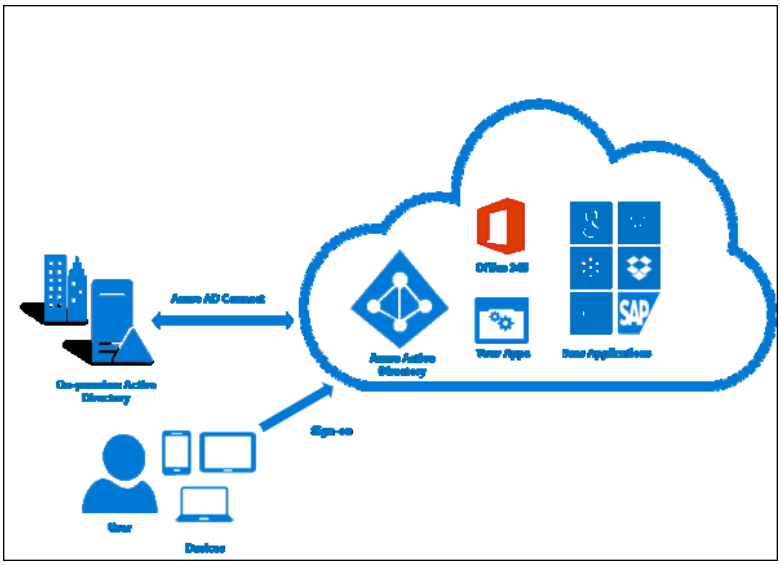


Obrázek 10 – Vytvoření Azure Active Directory tenantu

4.3.2 Integrace Active Directory a Azure Active Directory

Integrace mezi Active Directory a Azure Active Directory je bezplatná služba. K integraci se využívá program AD Connect. [27]

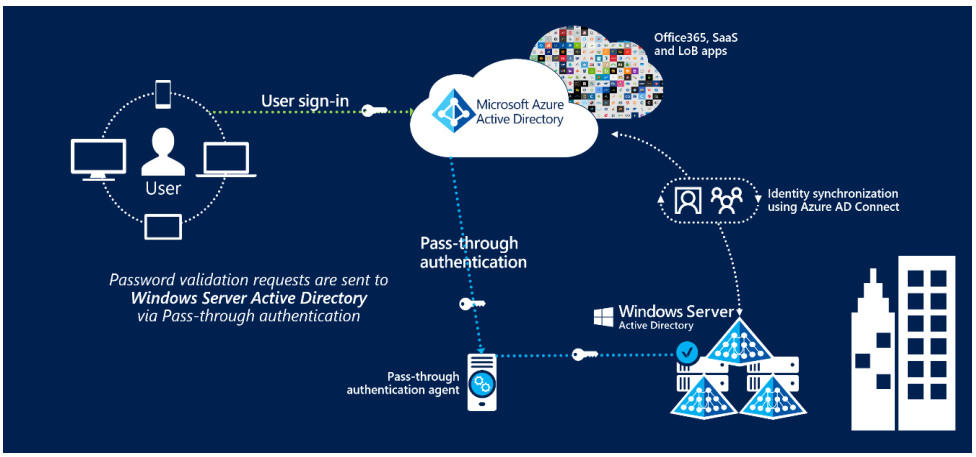
Tím, že bude provedena integrace místních adresářů, se službou Azure AD, budou uživatelé pod jednou identitou schopni přistupovat ke cloudovým službám Office 365. Azure AD Connect nahrazuje starší nástroje pro integraci identity, jako například DirSync či Azure AD Sync.



Obrázek 11 – Integrace Azure Active Directory [29]

4.3.2.1 Autentizace pomocí Azure AD pass-through

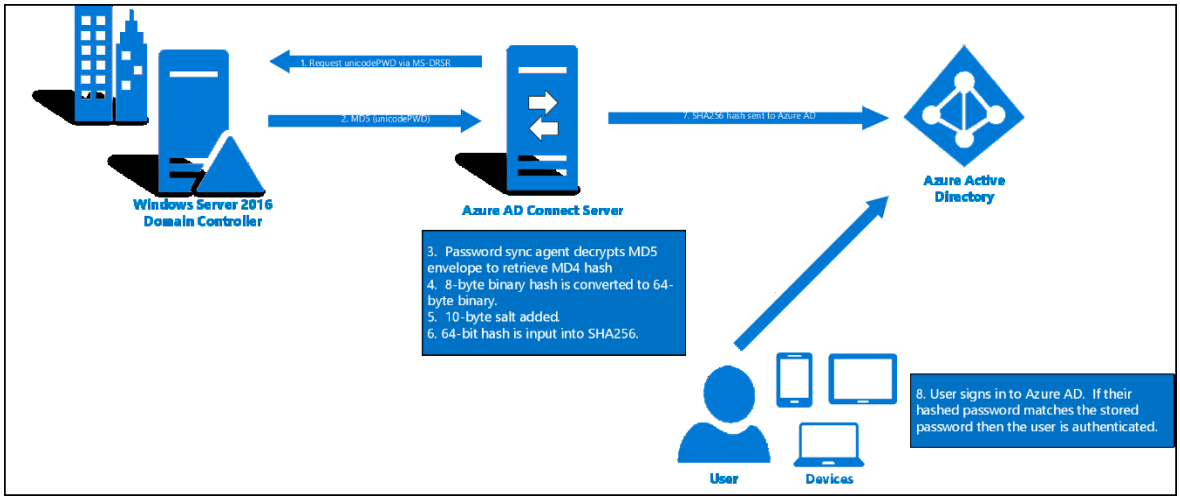
Pass-through autentizace zajišťuje možnost ověřování vůči Azure AD stejnými přihlašovacími údaji, jako v interním Active Directory. Z toho vychází, že uživatel má stejné heslo pro přihlášení v interní infrastruktuře, tak při přihlášení do cloudových aplikací. Při přihlášení uživatele prostřednictvím Azure AD, se přihlašovací údaje ověří vůči internímu Active Directory. Způsob ověřování hesel mezi interní Active Directory a Azure Active Directory je založen na synchronizaci hodnoty hash. [28]



Obrázek 12 – Autentizace pomocí Azure AD pass-through [28]

4.3.2.1.1 Synchronizace hash hesel v Azure AD

Active Directory Domain Services ukládá hesla uživatelů ve formě hash otisku skutečného hesla. Hodnota hash je výsledkem jednosměrné matematické funkce, jedná se o hashovací algoritmus. Výsledkem je hodnota, která se již nedá vrátit zpět na skutečné heslo uživatele. [29]



Obrázek 13 – Synchronizace hash hesel [29]

V synchronizačním přenosu se nesynchronizují hesla v prosté textové verzi. Přenáší se pouze hash otisky hesel uživatelů. [29]

Uživatel se ověří vůči Azure Active Directory, nikoliv vůči interní Active Directory. Hesla v Azure Active Directory jsou ve formátu hash SHA256, jedná se o výraznější bezpečnost než hesla uložená v interním Active Directory. Hodnota SHA256 nelze být dešifrována, není možné se přihlásit do interního Active Directory a vydávat se validního uživatele v útoku „pass-the-hash“. [29]

4.4 Office 365

Po úspěšné integraci mezi Active Directory a Azure Active Directory, je možné spustit migraci poštovních schránek. Nejprve je ovšem vhodné pořídit licence určené uživatelům. Přehled licencí je uveden v následující tabulce.

Název licence	Aplikace Office, které jsou součástí	Služby, které jsou součástí	Cena za uživatele na měsíc
Office 365 Business Premium	Outlook, Word, Excel, PowerPoint, OneNote, Access	Exchange Online, OneDrive, SharePoint, Skype pro firmy, Microsoft Teams	10,50 Euro
Office 365 Business Essentials	Nejsou součástí	Exchange Online, OneDrive, SharePoint, Skype pro firmy, Microsoft Teams	4,20 Euro
Školní licence			
Office 365 A1	Pouze Online: Outlook, Word, Excel, PowerPoint Aplikace: OneNote	Exchange Online, Onedrive, SharePoint, Skype pro firmy, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync	Zdarma
Office 365 A3	Aplikace: Outlook, Word, Excel, PowerPoint, OneNote, Publisher, Access	Exchange Online, OneDrive, SharePoint, Skype pro firmy, Teams, Sway, Forms, Streams, Flow, PowerApps, School Data Sync, Bookings	2,50 Euro pro studenty 3,20 Euro pro pedagogický sbor a zaměstnance
Office 365 A5	Aplikace: Outlook, Word, Excel, Power-Point, OneNote, Publisher, Access	Exchange Online, OneDrive, SharePoint, Skype pro firmy, Teams, Sway, Forms, Stream, Flow, PowerApps, School Data Sync, Bookings, Power BI	5,90 Euro pro studenty 7,90 Euro pro pedagogický sbor a zaměstnance

Tabulka 3 – Přehled licencí Office 365 [30] [31]

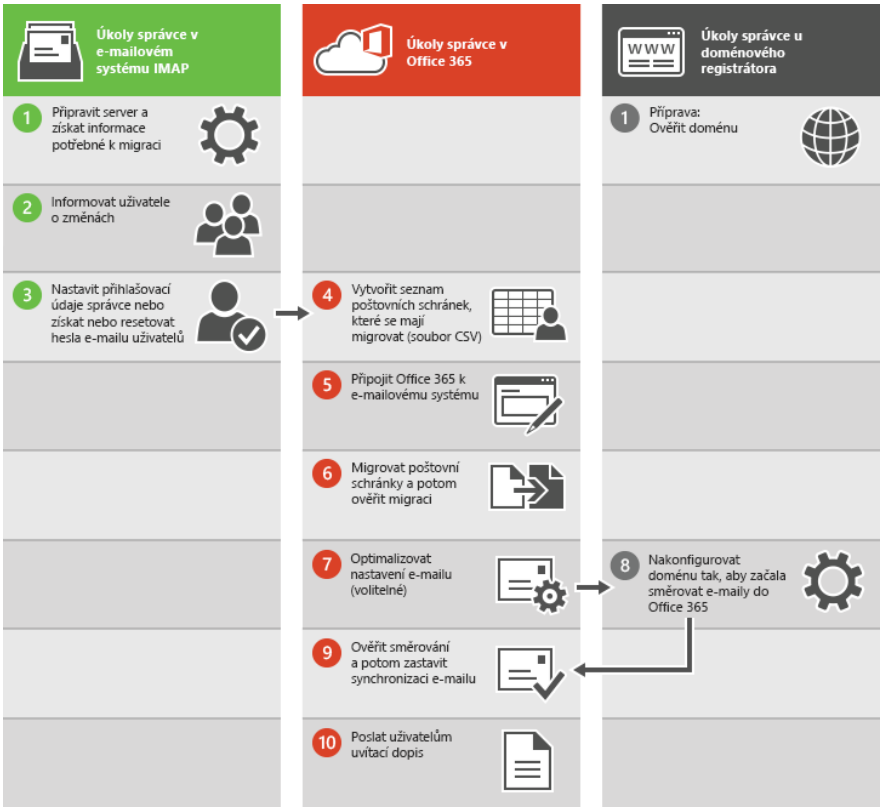
4.5 Možnosti provedení migrace poštovních služeb

Organizace je schopna přesunovat poštovní schránky z Exchange On-Premise do Exchange Online a naopak. Dochází k přesunu e-mailových zpráv, kontaktů, kalendářů, upozornění. Mezi hlavní faktory při rozhodování, kterou variantu migrace vybrat, je současný poštovní systém a jeho vlastnosti. Kolik schránek chceme migrovat, respektive velikost dat, která budeme přesouvat. Zda firma chce být v koexistenci mezi stávajícím On-Premise systémem a Exchange Online, nebo zda se chce On-Premise zbavit.

4.5.1 IMAP

Migrace e-mailů s podporou protokolu IMAP. Tato možnost nepodporuje koexistenci se stávajícím řešením. Největší nevýhodou je to, že dochází k migraci pouze k položkám, které jsou uloženy ve složce Doručená pošta, z toho vychází, že nedochází k migraci kalendářů,

kontaktů, úkolů. Dodatečně je uživatel schopen si tyto data přesunout sám. Při migraci IMAP se v Exchange Online nevytvoří automaticky poštovní schránka, je nutné před migrací poštovní schránku pro každého uživatele vytvořit, tzn. přiřadit mu příslušnou licenci. Není nutné synchronizovat interní Active Directory s Azure Active Directory. Maximální počet migrovaných položek je 500 000 e-mailů. Maximální velikost jednoho e-mailu je 35 MB. [32]



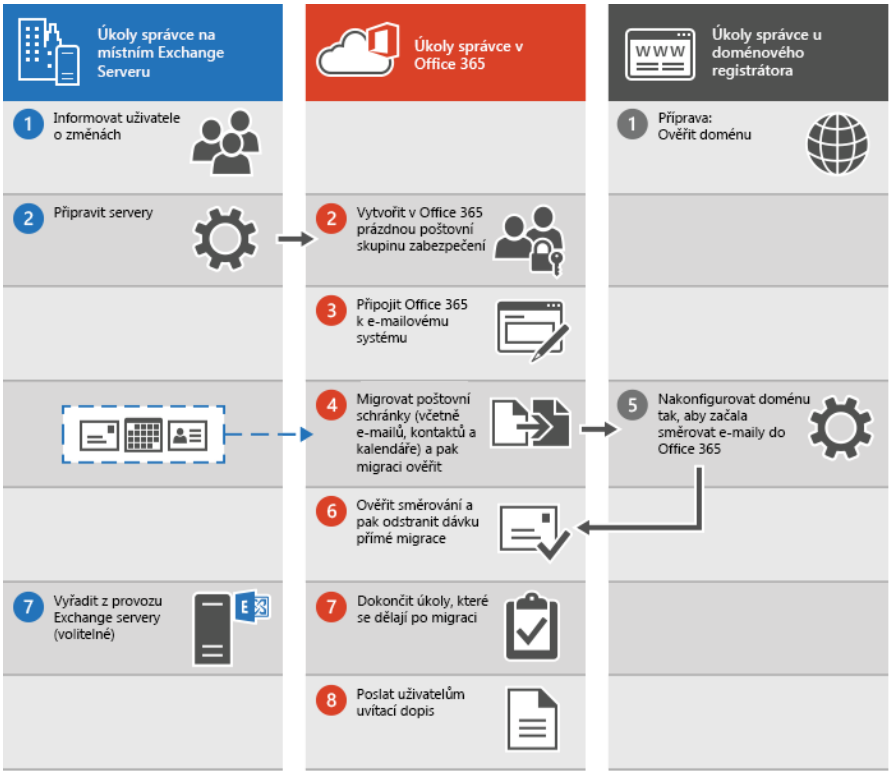
Obrázek 14 – Migrace IMAP [32]

4.5.2 PST

Předpokladem je schopnost poštovního systému vyexportovat poštovní schránku do formátu pst. Tímto způsobem se migrují e-maily, kalendář, kontakty, úkoly. Existují dvě varianty pro importování pst souborů, první je import přes internet. Využívá se služby importu Office 365, kdy je nejprve nahrát pst soubory do Azure Blob Storage a následně naimportovat do schránek uživatelů. Druhá varianta je, poslání zašifrovaných disků kurýrem do odběrového místa Microsoftu. Této varianty se využívá, zejména pokud je nedostatečná šířka pásma, latence a nejde ani dočasně navýšit. Maximální velikost disku je 10 TB. Pro nakopírování se využívá nástroj WAImportExport.exe, disk musí být šifrován BitLockerem. Cena za jeden GB je 2 USD. [33]

4.5.3 Přímá migrace do Office 365

Jedná se o jednorázovou migraci. Podmínkou je verze Microsoft Exchange minimálně 2003. Tento typ migrace je určen pro přesun maximálně 2000 poštovních schránek. Ovšem Microsoft doporučuje přenést pouze 150 poštovních schránek. Dojde k migraci všech poštovních schránek v organizaci, takže nelze selektovat koho migrovat. Migrace probíhá pomocí protokolu Outlook Anywhere. Je nutný důvěryhodný SSL/TLS certifikát. Podmínkou je, že neexistuje synchronizace Active Directory mezi Azure Active Directory, identity tato migrace vytváří sama, problém vzniká, že nedojde k synchronizaci hesel. Administrátor, který provádí migraci, musí mít plný přístup do všech poštovních schránek. V prostředí Office je nutné, aby byla ověřena doména a určilo se, že jsme vlastníci domény. Po úspěšné migraci je nutné překlopit MX záznamy Autodiscover. Uživatelé si budou muset vytvořit nový profil v Outlooku, a to samé platí i pro ActiveSync. Po všech krocích je nutné, aby měli uživatelé přiřazenou patřičnou licenci. [34]



Obrázek 15 – Příma migrace [34]

4.5.4 Fázová migrace do Office 365

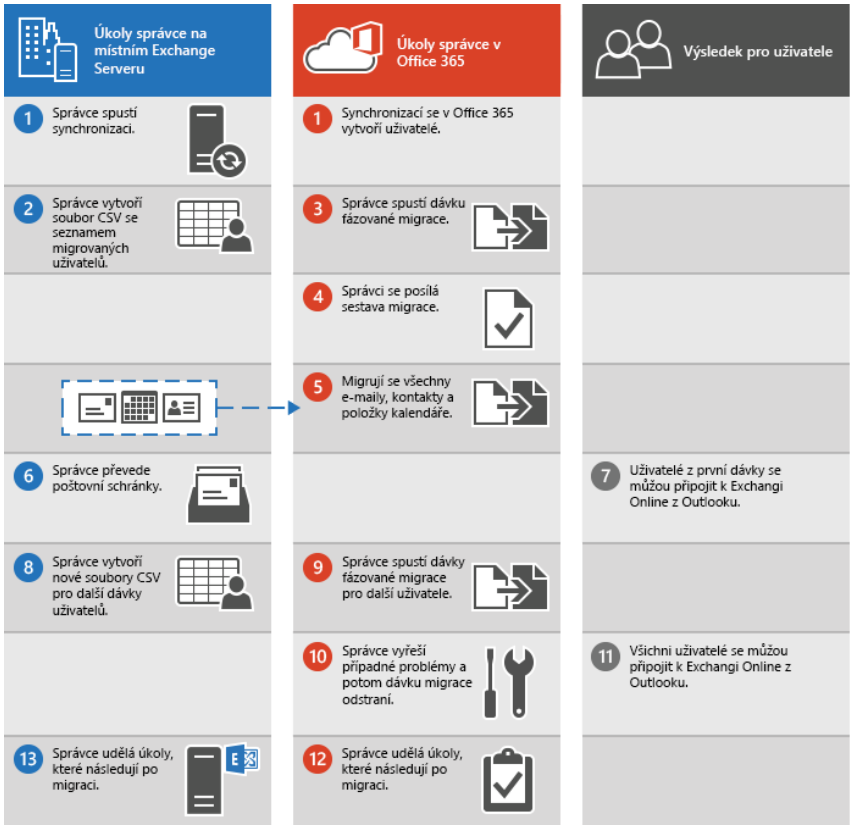
Tento typ migrace podporuje pouze Microsoft Exchange Server 2003 a novější. Migrace je určena pro migraci více než 2000 poštovních schránek. Jedná se o migrací ve fázích nikoliv

o jednorázovou migraci, jako u přímé migraci. Migrace probíhá pomocí protokolu Outlook Anywhere, je nutný důvěryhodný SSL/TLS certifikát. Administrátor, který migruje poštovní schránky, tak je stejně jako u přímé migrace nutné, aby měl plný přístup do všech přesouvaných schránek. Dále je nutné ověřit doménu v Office 365. Oproti přímé migrace je nutné provést synchronizaci uživatelů pomocí Azure AD Connect. Po úspěšné synchronizaci adresářů, je nutné, aby administrátor vytvořil CSV soubor, který bude obsahovat e-mailovou adresu uživatelů, kteří budou migrováni, jejich heslo a parametr, zda si uživatel bude muset změnit heslo, po prvním přihlášení. Příklad takového souboru vypadá takto, jedná se o textový soubor, který lze upravit v programu Notepad.exe v jedné dávce může být pouze 100 uživatelů: [35]

EmailAddress,Password,ForceChangePassword

hanak@domena.loc,Pa$$w0rd,False
administrator@domena.loc,Pa$$w0rd1,True [35]

Poté je nutné vytvořený soubor vložit do průvodce fázové migrace. Po úspěšné migraci musí dojít k překlopení MX záznamů a Autodiscover. To samé platí i pro přímou migraci, dále je nutné vytvořit uživatelům nový Outlook profil a stejně, tak i pro ActiveSync.[35]

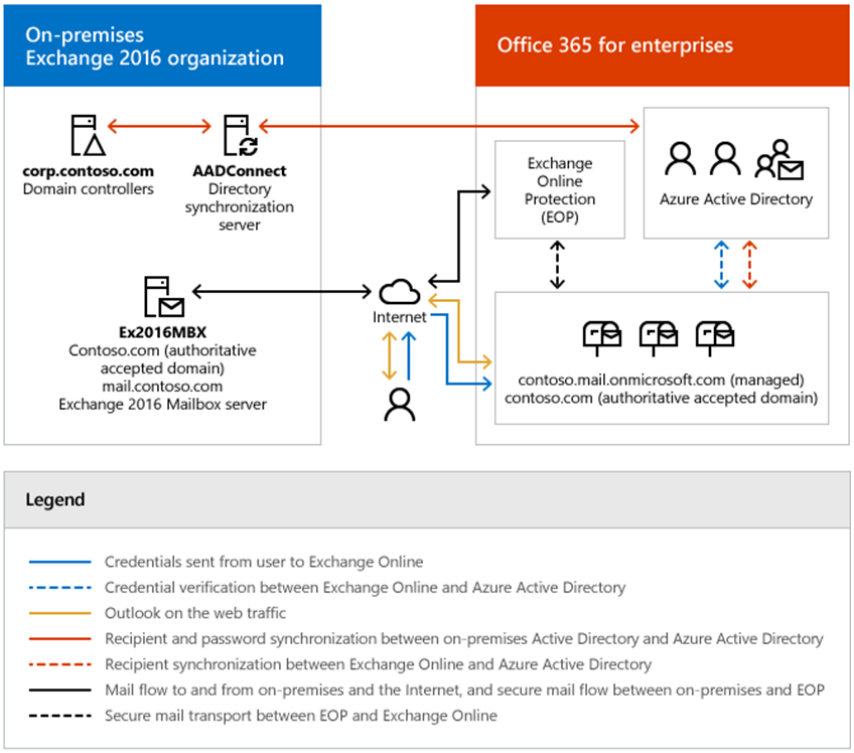


Obrázek 16 – Fázová migrace [35]

4.5.5 Exchange Hybrid

Nejnovější typ migrace, určen pouze pro Microsoft Exchange 2010 a novějším. Před migrací je nutné provést synchronizaci mezi Active Directory a Azure Active Directory, například pomocí pass-through. Využívá Mailbox Replication Service (MRS), tato služba je určena pro migraci mezi poštovními schránkami, které jsou umístěny v různých organizacích nebo Office 365. Proto je nutné povolení této funkce v případě hybridní migrace do Office 365. Povolení probíhá na Client Access serveru. Mezi Exchange Online a Exchange On-Premise nesmí být žádná SMTP gateway, jedinou výjimku má Edge Server. Existuje jedna webová konzole pro On-Premise řešení a Exchange Online, jedná se o nejkvalitnější formu koexistence. Směřování e-mailou mezi Exchange Online a On-Premise je bezpečně a považuje se jako vnitřní provoz. Jedná se o sdílenou SMTP doménu, uživatelé vidí navzájem Free/Busy statusu. Administrátor může určit, že pošta pro danou doménu bude přijímaná On-Premise prostředím nebo Online, záleží na MX záznamu. Není nutné vytvořit nový Outlook profil.

Pro vytvoření tohoto typu migrace je nutné stažení aplikace Microsoft Office 365 Hybrid Configration Wizard, který provede konfiguraci Exchange On-Premise a Exchange Online prostředí pro hybridní migraci. Aplikaci je nutné nainstalovat na serveru, který se nachází v On-Premise doméně. Aplikace vytvoří konektory určené k odesílání v Exchange Online a Exchange On-Premise. Podmínkou je důvěryhodný SSL/TLS certifikát. [36]



Obrázek 17 – Exchange Hybrid řešení [36]

4.5.5.1 Transport Layer Security a Hybrid Exchange Server

V případě hybridního nasazení musí Exchange Server On-Premise ověřit službu Exchange Online pomocí certifikátu zabezpečení, aby mohlo docházet k odesílání e-mailových zpráv příjemcům, kteří mají své e-mailové schránky v Exchange Online. Proto musí být tyto certifikáty nainstalovány na všech On-Premise Exchange Serverech. [37]

Tento certifikát musí být zakoupen z důvěryhodné certifikační autority třetích strany. Minimální požadavky na tento certifikát je uveden v následující tabulce.

Služba	Navrhované plně kvalifikované jméno	Pole v certifikátu
SMTP	domena.loc	Subject name
Autodiscover	Pole určující externí Autodiscover FQDN Exchange Serveru 2013 nebo Exchange Serveru 2016, například autodiscover.domena.loc	Subject alternative name
Přenos	Pole učrující externí FQDN shodující Edge Transport Server, například edge.domena.loc	Subject alternative name

Tabulka 4 – Požadavky na certifikát [38]

4.5.5.2 Migrace SMTP provozu

Je nutné konfigurovat veřejné DNS servery, kde dojde k úpravě MX záznamů, nové záznamy bude odkazovat na poštovní server Exchange Online. [39]

Primární SMTP název	Typ DNS záznamu	Priorita MX	Cíl
Domena.loc	MX	0	Domenaloc.mail.protection.outlook.com

Tabulka 5 – Mail Exchanger záznam v DNS [39]

Záznam odkazuje na Exchange Online Protection Server a poté dojde ke směřování na Exchange Online Server.

Pro kontrolu je nutné otevřít Windows příkazovou řádku a příkazem:

Nslookup -type=MX domena.loc

Získáme výsledek:

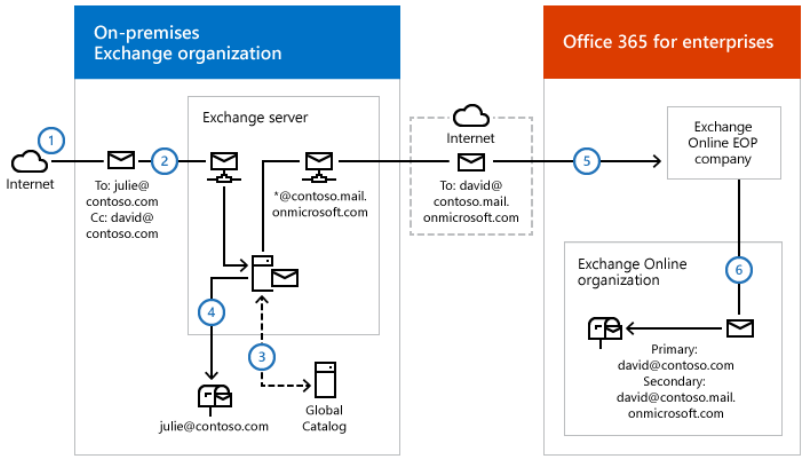
Server: dns.corp.domenaloc.com
Address: 192.168.1.10

Non-authoritative answer:
Domena.cz MX preference = 0, mail exchanger = domenaloc.mail.protection.outlook.com

domenaloc.mail.protection.outlook.com internet address = 216.32.181.10

Tímto příkazem ověřujeme, zda je pro doménu domena.loc MX záznam směřující na server 216.32.181.10.

V případě, že organizace, chce přijímat poštu určenou doméně, kterou migruje serverem Microsoft Exchange On-Premise je nutné v MX záznamu uvést IP adresu On-Premise serveru. [39]



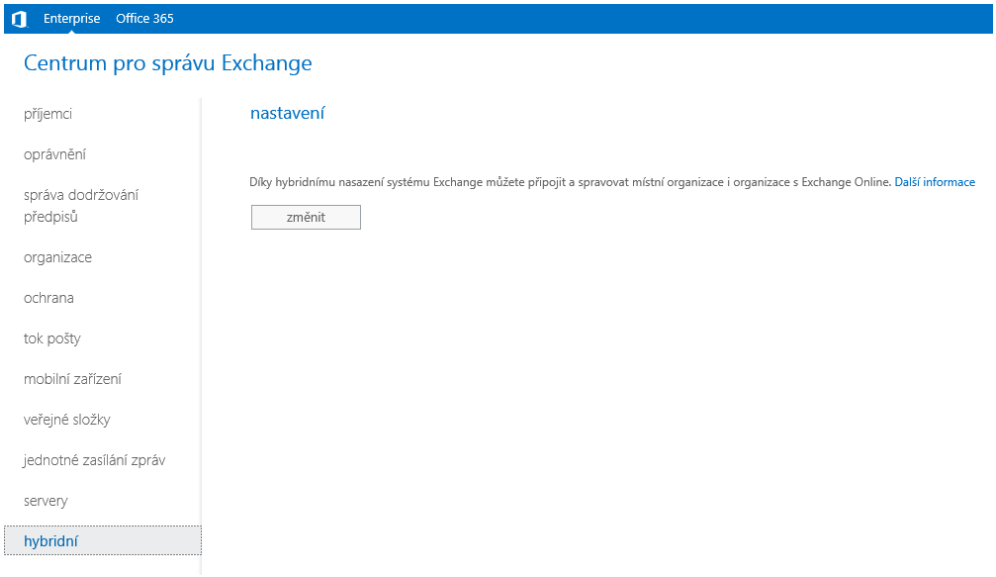
Obrázek 18 – Vybrané směřování pošty v rámci hybridního scénáře [39]

4.6 Výběr optimálního řešení

Pokud On-Premise řešení již spravuje několik domén a pouze jedna doména bude migrována do Exchange Online a organizace využívá Microsoft Exchange Server 2016 je nejvhodnější variantou hybridní migrace. Díky, které dojde k minimálnímu výpadku poštovních služeb. Pouze bude nutné restartovat aplikaci Outlook, jakmile dojde k dokončení migrace.

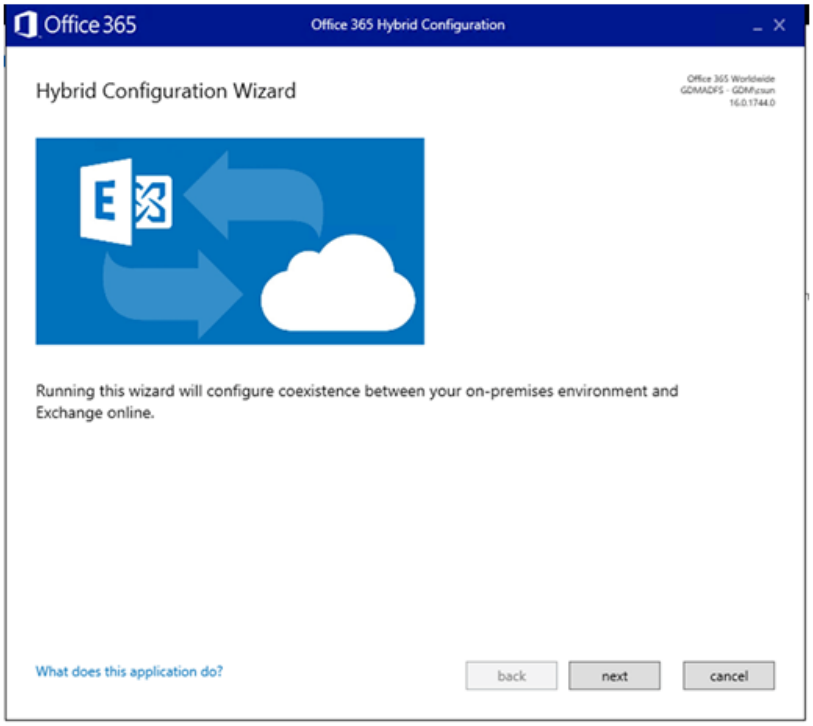
4.6.1 Migrace Hybrid

Pro hybridní migraci je nutné nainstalovat program, který nakonfiguruje oba poštovní servery. Instalátor lze stáhnout v konzoli Exchange Control Panel.



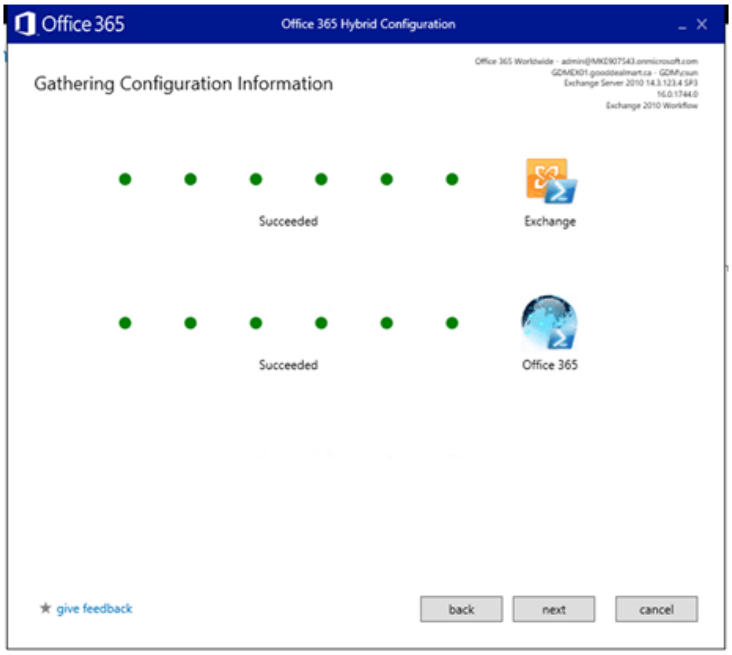
Obrázek 19 – Stažení Hybrid Configuration Wizard z prostředí ECP

Po stáhnutí spustitelného programu je nutné, nainstalovat na PC v doméně.



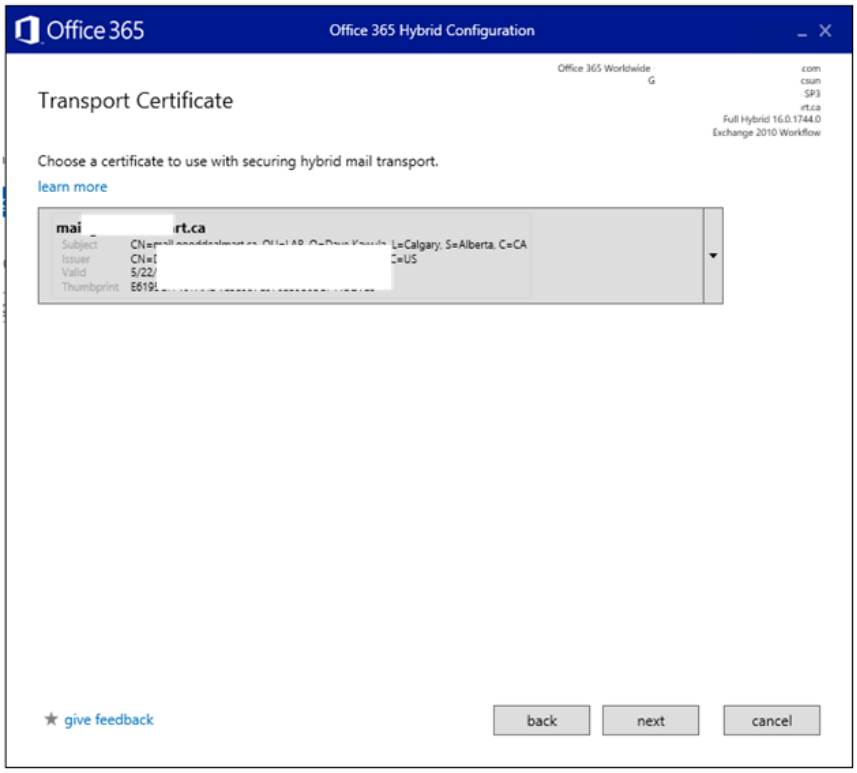
Obrázek 20 – Průvodce pro nastavení Hybridní konfigurace [40]

V průvodci je nutné zadat přihlašovací údaje administrátora On-Premise Exchange Serveru, ale také administrátora Exchange Online. Po zadání přihlašovacích údajů se aplikace bude připojovat do Exchange Online pro vytvoření konektorů, to samé platí pro Exchange On-Premise. V případě Exchange On-Premise je nutné vybrat Exchange On-Premise servery, které budou provádět migraci. V případě, že se průvodce nebude moci připojit k Office 365, je vhodné zkontrolovat konfiguraci firewallu, zda provoz neblokuje. Aplikace se připojuje pomocí protokolu HTTPS, číslo portu 443. [40]



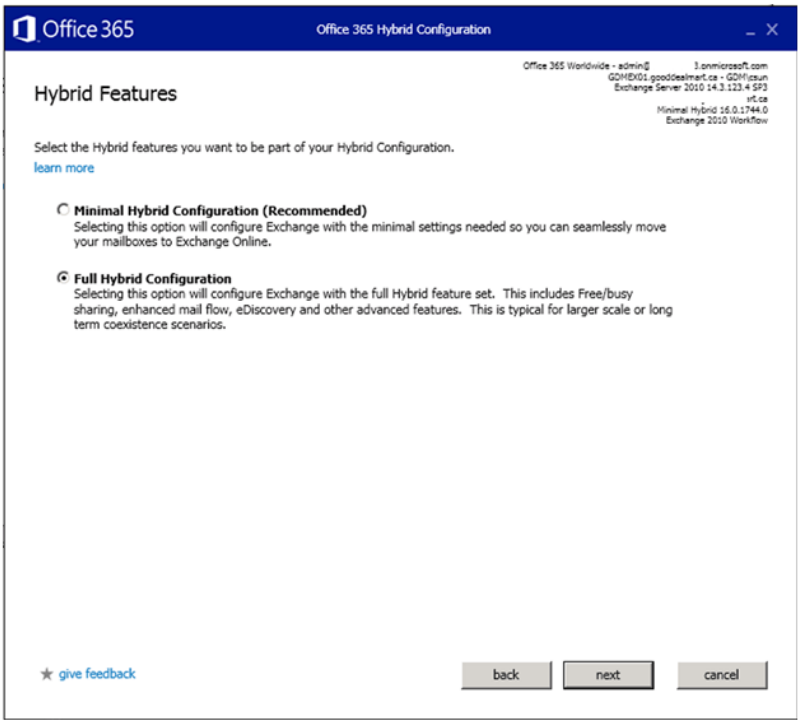
Obrázek 21 – Registrace k Exchange Online a Exchange On-Premise [40]

Po vybrání místního Client Access serveru je nutné vybrat transportní certifikát, který bude využíván k zabezpečení hybridního e-mailového provozu. Certifikát musí být důvěryhodný a vydán veřejnou certifikační autoritou například DigiCert. [40]



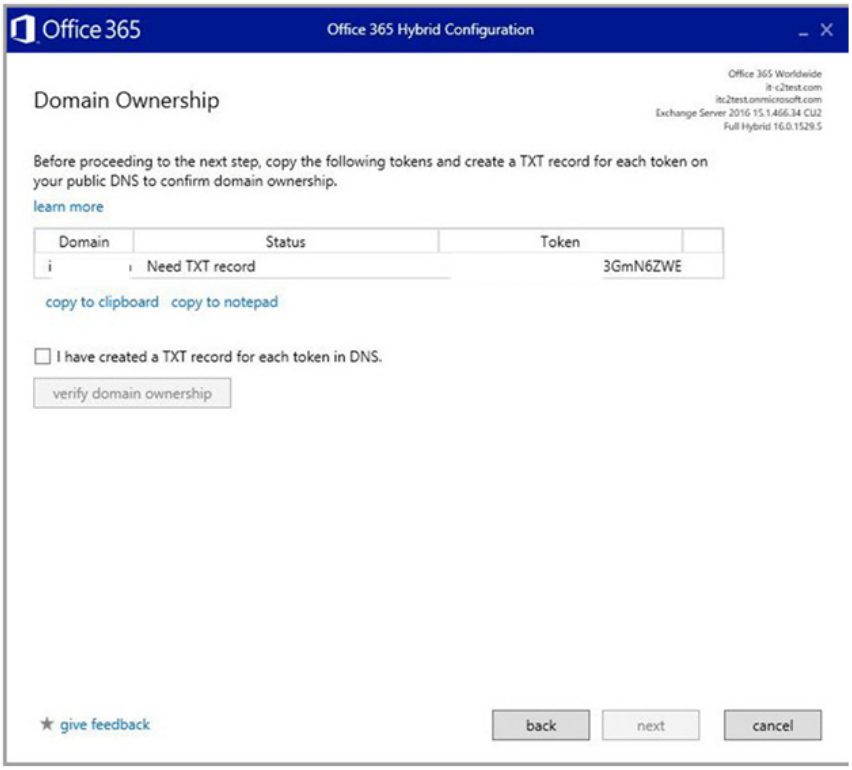
Obrázek 22 – Výběr transportního certifikátu [40]

Po úspěšném připojení je nutné vybrat možnost minimální hybridní konfigurace nebo plné hybridní konfigurace. V případě minimální konfigurace nebude k dispozici sdílení statusu Free/Busy, TLS zabezpečený tok e-mailových zpráv mezi Exchange On-Premise a Exchange Online, automatické přesměrování aplikace Outlook on the web a ActiveSync pro migrované uživatele. Tato varianta je určena pro malé či střední organizace, která potřebuje bezproblémovou migraci. Plná konfigurace všechny tyto služby zajišťuje proto je vhodnější plná konfigurace. [40]



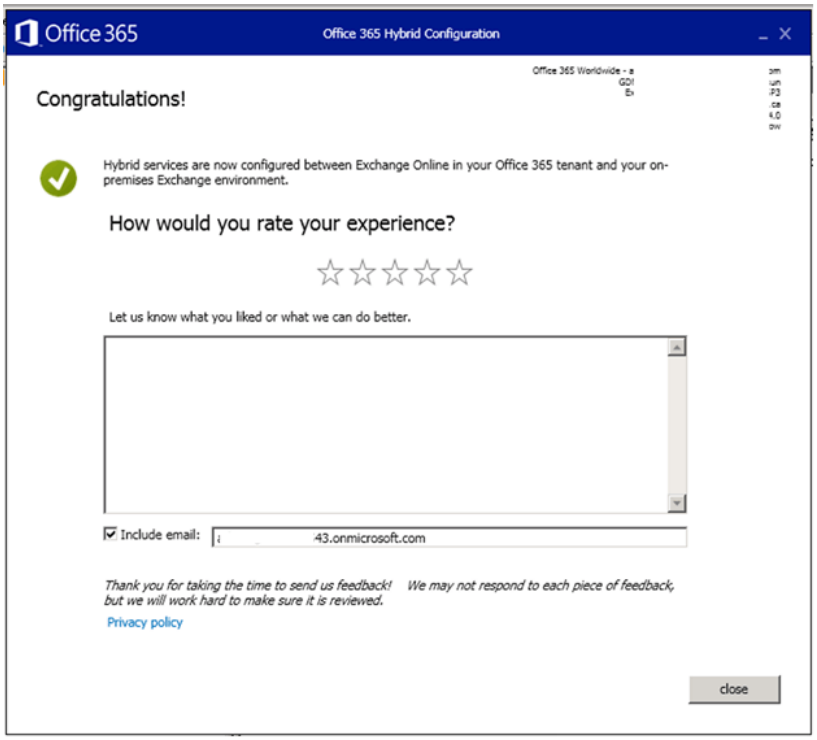
Obrázek 23 – Výběr plné hybridní konfigurace [40]

Následně pro správnou funkčnost statusu Free/Busy, je nutné zapnout Federation Trust. Pro zapnutí průvodce vygeneruje TXT záznam, který administrátor vloží na veřejný DNS server. [40]



Obrázek 24 – Generování TXT záznamu [40]

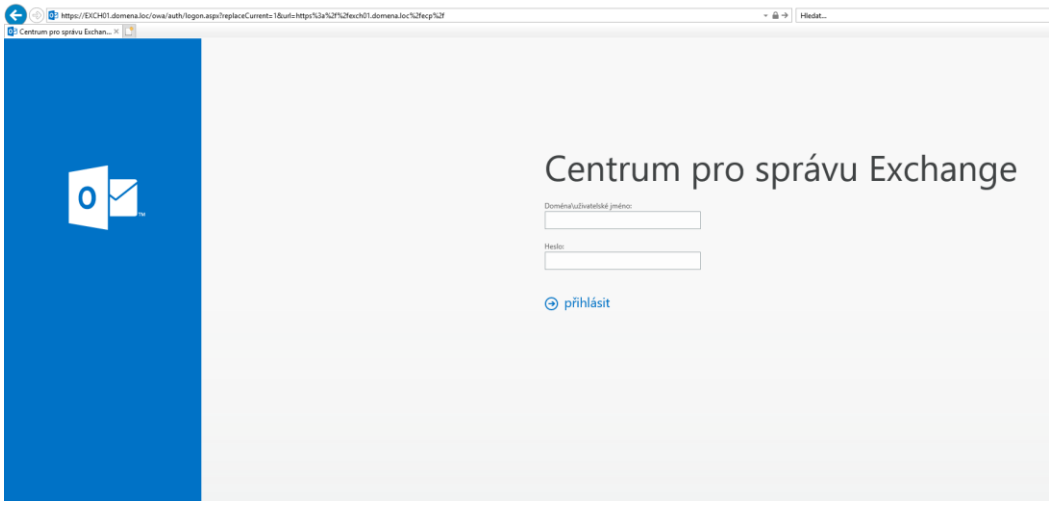
Po dokončení průvodce oznámí, že konfigurace dopadla úspěšně.



Obrázek 25 – Ukončení hybridní konfigurace [40]

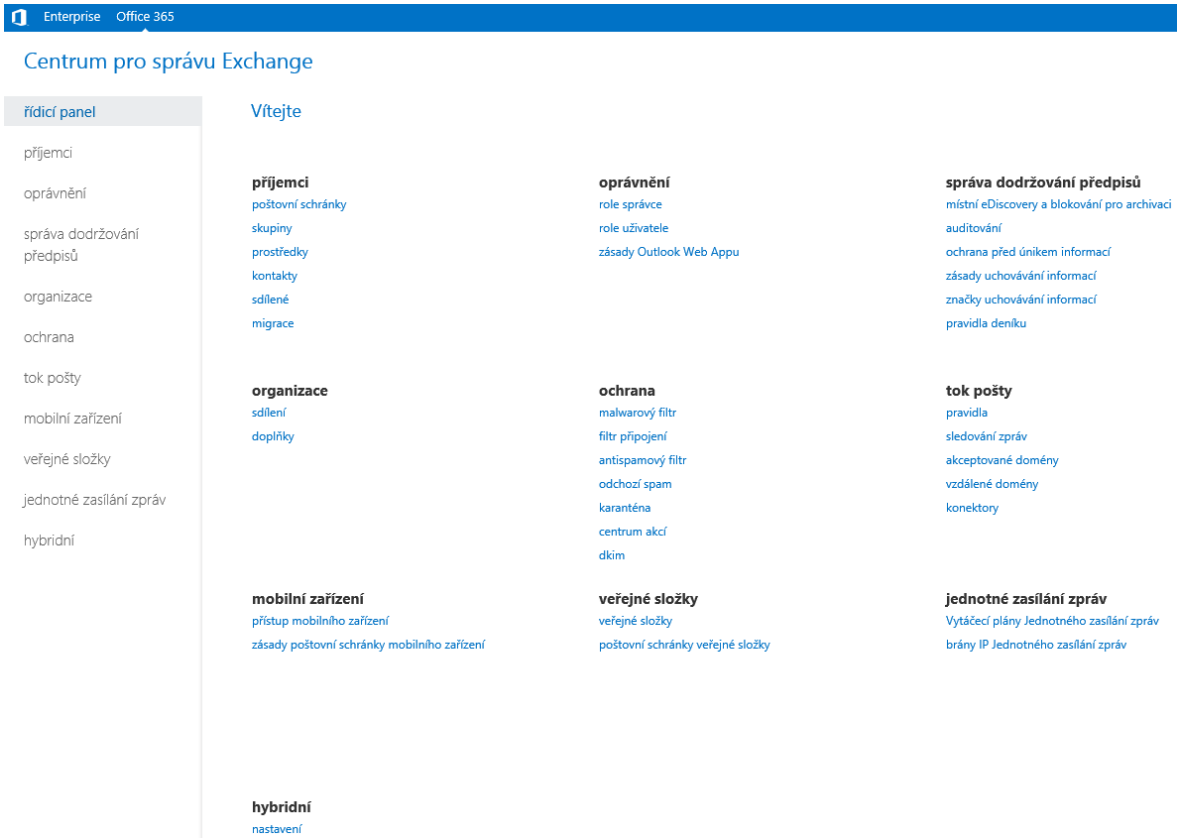
4.6.1.1 Vytvoření migrační dávky

K vytvoření migrační dávky je možné využít dvou řešení. První je prostřednictvím webového prohlížeče a druhým je prostřednictvím konzole PowerShellu. Uživatelsky příznivější je vytvoření dávky přes webový prohlížeč, zde je nutné se přihlásit do Exchange Command Center, prostřednictvím například, https://www.Exch01.domena.loc/ECP. [41]



Obrázek 26 – Přihlášení do centra pro správu Exchange

Po přihlášení pod uživatelem, který má administrátorská práva pro práci s Microsoft Exchange Serverem, zvolit kartu hybrid, kde je možné zapnout, vypnout nebo editovat nastavení stávajícího nastavení hybridního řešení. Díky hybridnímu řešení je možné spravovat Exchange On-Premise a Exchange Online pomocí jedné webové konzole, a to po přihlášení jen vybrat záložku Office 365, tím se lze dostat do správy Exchange Online. Při prvním pokusu pro přihlášení k Exchange Online je nutné zadat přihlašovací údaje administrátora Exchange Online. [41]



Obrázek 27 – Úvodní strana centra pro správu Exchange

Naopak karta pro správu Exchange On-Premise je nutné mít označenou kartu Enterprise.

Pro vytvoření migrační dávky je nutné přihlásit se do Exchange Online, a pomocí řídícího panelu zvolit možnost migrace. Po zvolení možnosti migrace, lze vidět stávající migrační dávky, mazat je anebo vytvářet nové pomocí tlačítka plus. Při zvolení je možné zvolit možnost migrovat do Exchange Online nebo migrovat z Exchange Online. [41]

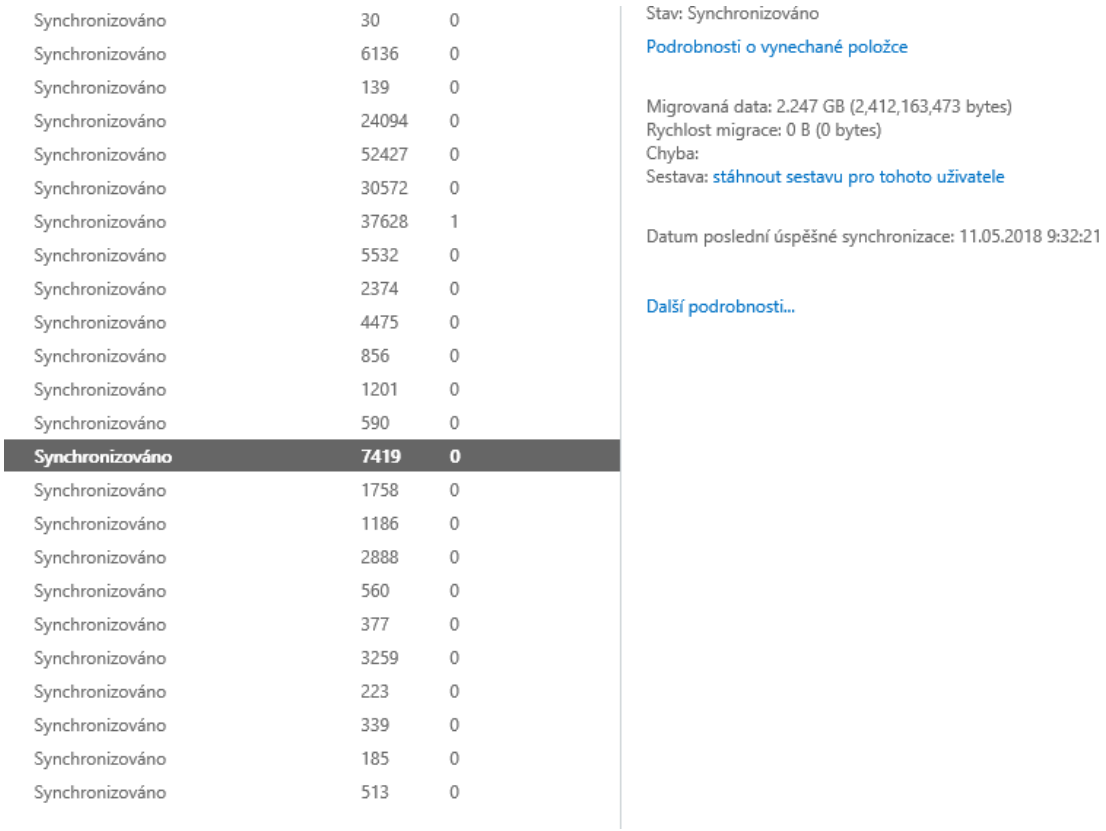
Vytvoření migrační dávky do Exchange Online, nabízí možnosti Vzdálená migrace, tato možnost se využívá v případě hybridního nasazení. Další možností je Fázová migrace, Přímá migrace, migrace IMAP. [41]

V případě, že se se jedná o hybridní nasazení, je nutné vybrat možnost vzdálené migrace. V dalším kroku dojde k vybrání poštovních schránek z Exchange On-Premise, kteří budou migrováni. Je možné ručně vybrat, případně lze vložit soubor CSV, kde bude seznam e-mailových adres uživatelů. Příklad obsahu, takového textového souboru CSV: [42]

EmailAddress

Administrator@domena.cz
HanakJ@domena.cz
LysakovaM@domena.cz

V následujícím kroku je potvrzení vzdáleného koncového bodu, jedná o plně kvalifikovaný název domény serveru Exchange On-Premise, na kterém běží Mailbox Replication Service Proxy. Poté se pojmenuje název migrační dávky, název cílové domény pro doručení, ta bude ve tvaru domenacz.onmicrosoft.com. V posledním kroku se určí, komu přijde informační e-mailová zpráva o dokončení migrační dávky. Dále se určí, zda migrační dávka má začít hned po dokončení nebo bude zapnuta ručně. Podobně je to i u dokončení migrační dávky. [41]



Obrázek 28 – Migrační dávka

4.6.1.2 Konfigurace koncových zařízení

V momentě, kdy dojde k úspěšné migrační dávce, a uživatel se bude chtít přihlásit prostřednictvím webových stránek. Tak ho původní Outlook on the web přesměruje na stránky https://outlook.com/owa/domena.cz, na kterých se může pomocí e-mailové adresy a hesla přihlásit do své poštovní schránky.

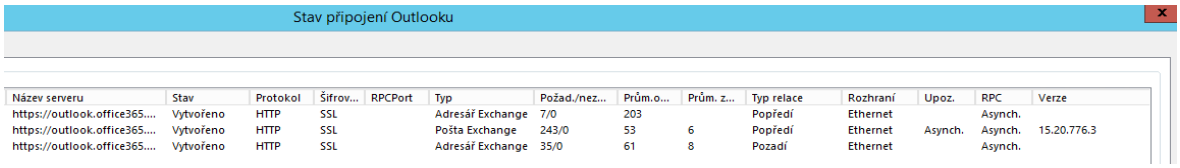
V případě, že uživatel využívá aplikaci Outlook pro správu e-mailů, tak během přesunu je schopen normálně pracovat. Ovšem po dokončení migrace je vyzván k restartovaným aplikace.

Po restartu aplikace se klient pokusí připojit k On-Premise Autodiscover názvu. Exchange On-Premise vrátí atribut RouteRoutingAddres, jelikož se jedná o Office 365 poštovní schránku, bude ve tvaru alias@domenacz.mail.onmicrosoft.com. Klient tedy využije tuto adresu k druhému pokusu Autodiscover, pomocí vyhledání DNS vůči jménu autodiscover.domancz.mail.onmicrosoft.com. Nejprve se pokusí navázat HTTPS připojení, ovšem to se nepodaří, proto se pokusí navázat http připojení, bez zaslání přihlašovacích údajů. Dojde k přesměrování na autodiscover-s.outlook.com a k úspěšné konfiguraci klienta, například aplikace Outlook.

4.6.2 Kontrola

Migrace je možná provádět v určených dávkách, pokud dojde k migraci celkem devadesáti poštovních schránek. Rozdělí se na šest dávek po patnácti uživatelích, před každou dávkou dojde k e-mailovému upozornění, které bude obsahovat informace o tom, že dojde k migraci uživatelovy schránky, předpokládány čas dokončení, návod pro správnou konfiguraci klientů.

Po potvrzení úspěšnosti migrace dojde k pokračování další dávky. Každý uživatel potvrdí funkčnost e-mailové schránky, tím, že odešle testovací e-mail administrátorovi. Pokud e-mailová schránka nebude funkční, v informačním e-mailu před migrací bude uvedeno telefonní číslo, na které uživatel zavolá, pokud poštovní schránka nebude funkční.



Obrázek 29 – Konfigurace aplikace Outlook

Po potvrzení všech uživatelů dojde ke změně MX záznamů, aby došlo ke změně SMTP provozu. Kontrolu administrátor provede pomocí Windows příkazové řádky, a také pomocí portálu https://testconnectivity.microsoft.com, který otestuje funkčnost připojení do Outlooku, funkčnost ActiveSync, testování příchozích a odchozí e-mailových zpráv.

4.7 Harmonogram

		1. měsíc																													
		1. týden				2. týden						3. týden					5. týden					6. týden					7. týden					
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
Klíčové aktivity	Vytvoření Azure Tenant																														
	Implementace Azure Active Directory Synchronizace																														
	Zakoupení licencí pro Exchange Online																														
	Instalace Hybrid Configration Wizard																														
	Migrace uživatelů do Exchange Online																														
	Kontrola funkčnosti přesunutých uživatelů																														
	Změna MX záznamů																														

Tabulka 6 – Harmonogram provedení migrace

4.8 Aplikační monitoring

Monitoring je klíčový prvek úspěšného nasazení Microsoft Exchange. Microsoft Exchange, jako takový obsahuje funkci monitoringu jednotlivých služeb, který sám nabízí. Spolu s produktem System Center Operations Manager, zkráceně SCOM, tvoří komplexní monitoring, díky kterému je administrátor informován v případě vzniku problému na některém z poštovních serverů. Existuje mnoho další monitorovacích platforem, jako například Zabbix, který je oproti SCOM open source.

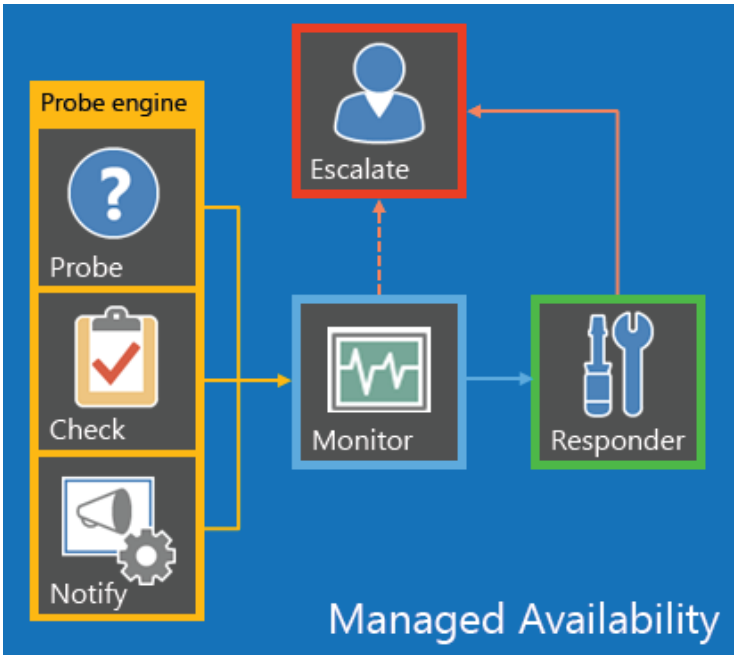
SCOM je vyvíjen firmou Microsoft stejně jako Microsoft Exchange, a i proto slibuje vysokou podporu, pro monitorování poštovního serveru. [43]

4.8.1 Správa dostupnosti

Od verze Microsoft Exchange Server 2013 přibyla komponenta Managed Availability, což se dá přeložit jako správa dostupnosti. Tato komponenta se stará o monitorování a obnovování částí infrastruktury, na kterých je závislá funkčnost poštovního serveru. Správa dostupnosti je schopna problémy, které objeví sama vyřešit. [44]

Mezi hlavní aspekty monitorování je dostupnost, zkušenost a odezva. Příkladem může být využití, pomocí webového prohlížeče do portálu Outlook on the Web (OWA). [44]

Dostupnost je myšleno v tomto případě načtení stránky pro přihlášení do e-mailové schránky. Pokud se nenačte, vznikne výstraha, a problém se dále eskaluje. V případě, že se stránky OWA načtou a uživatel se úspěšně přihlásí, ale dojde k tomu, že se nenačtou určité prvky webové stránky nebo uživatel není schopen číst své e-mailové zprávy. Znamená to, že je narušena zkušenost. Poslední částí je odezva vyjadřuje, jak rychle dojde k vykreslení schránky. Tyto tři aspekty vyjadřují uživatelskou zkušenost. [44]



Obrázek 30 – Princip správy dostupnosti [44]

4.8.1.1 Komponenty správy dostupnosti

Správa dostupnosti byla implementována od verze Microsoft Exchange 2013, jak pro roli Klientského přístupu, tak pro Mailbox. Od verze Microsoft Exchange 2016 pouze v roli Mailbox.

Mezi komponenty se řadí sonda, monitor, respondent. Činností sondy je provádění měření na poštovním serveru. Monitor obsahuje logiku, která určuje, co považujeme za zdravé. Poslední komponenta nazvána respondent, v případě zjištění nezdravého stavu, se pokusí opravit danou věc. Provede první obnovovací operace. V případě neúspěšného pokusu o uzdravení, eskaluje problém dále v případě využití SCOM, dojde k vyvolání upozornění v konzoli. Pak záleží na konfiguraci monitoringu, zda v případě nového upozornění dojde k notifikování administrátora SMTP kanálem případně SMS. [44]

4.8.2 Exchange On-Premise

Operace administrátora v rámci základního monitorovaní Microsoft Exchange Serveru jsou:

- Kontrola, zda není na poštovním serveru vytvořena fronta e-mailů, které nemohou být odeslány či doručeny.
- Kontrola volného místa na discích, kde je uložena databáze či systém.
- Kontrola, zda správně funguje hygiena zpráv a je aktuální.
- Provedení denních záloh a jejich kontrola.

- Sledování Eventlogu na poštovních serverech, kontrola zda nevznikla upozornění, chyby, cokoliv co může být považováno za neobvyklou aktivitu.
- Sledování výkonu poštovních serverů
- Kontrola komponent v rámci Exchange Management Shell [2]

V rámci Exchange Management Shell, spustit několik příkazů, které dokáži vypsat stav daného poštovního serveru. Mezi tyto příkazy patří:

Test-ServiceHealth, který ověří, zda služby určené k poštovnímu serveru jsou ve stavu spuštěno.

Pro Mailbox Server roli jsou klíčové tyto služby:

- IISAdmin, jedná se o službu, která umožnuje serveru spravovat metabázi služby IIS. Pokud tato služba není spuštěna, server nebude schopen konfigurovat SMTP či FTP protokol.
- MSExchangeADTopology, tato služba poskytuje informace o topologii služby Active Directory několika komponentám Microsoft Exchange Serveru.
- MSExchangeDelivery, přijímá SMTP zprávy od služby Microsoft Exchange Transport, na lokálních či vzdálených poštovních serverech a následně je přenese do místní poštovní schránky pomoci RPC.
- MSExchangeIS, spravuje databáze poštovních schránek na serveru. Zdali tato služba neběží, místní poštovní databáze nejsou k dispozici.
- MSExchangeMailboxAssistants, provádí zpracování poštovních schránek v databázi na pozadí.
- MSExchangeRepl, poskytuje funkci replikace databází poštovních schránek v Database Availability Groups.
- MSExchangeRPC, správa klientských RPC připojení pro Microsoft Exchange Server.
- MSExchangeServiceHost, poskytuje hostitelskou službu pro Microsoft Exchange Server komponenty.
- MSExchangeSubmission, přijímá RPC zprávy z lokální databáze poštovních schránek a předá je prostřednictvím SMTP protokolu službě Microsoft Exchange Transport, na lokálních případně na poštovních serverech.
- MSExchangeThrottling, poskytuje správu pracovního zatížení klienta, které omezuje míru uživatelských operací, jedná se o tzv. škrcení uživatele.

- MSExchangeTransportLogSearch, dává možnost vzdáleného vyhledávání transportních souborů, které se využívá například při hledání zpráv.
- W3Svc, služba určena k publikování webových stránek.
- WinRM, služba vzdálené správy systému Windows. [45]

Pro roli klientského přístupu se jedná o tyto důležité služby:

- IISAdmin,
- MSExchangeADTopology,
- MSExchangeIMAP4, předává IMAP4 klientské připojení ze serveru klientského přístupu, na IMAP4 službu, která běží na Mailbox serveru.
- MSExchangeMailboxReplication,
- MSExchangePOP3, předává POP3 klientské připojení ze serveru klientského přístupu, na POP3 službu, která běží na Mailbox serveru.
- MSExchangeRPC,
- MSExchangeServiceHost,
- W3Svc,
- WinRM. [45]

Pro roli Hub Transport jsou kritické tyto služby:

- IISAdmin,
- MSExchangeADTopology,
- MSExchangeEdgeSync, replikuje konfigurační data, data příjemců mezi Mailbox serverem a Active Directory Lightweight Directory Services na podepsaných Edge Transport serverech přes zabezpečený LDAP kanál. V případě, že se nevyužívá Edge Server, není tato služba důležitá.
- MSExchangeServiceHost,
- MSExchangeTransport, zprostředkovává SMTP server a transportní zásobník.
- MSExchangeTransportLogSearch,
- W3Svc,
- WinRM [45]

Dalším příkazem může být Test-MapiConnectivity, který ověří, zda jsou všechny databáze poštovních schránek připojeny a dostupny. Příkazem Get-MailboxDatabaseCopyStatus,

zjistíme, zda jsou všechny kopie databází a obsahové indexy v pořádku. Pomocí příkazu Test-ReplicationHealth, lze zjistit, zda všichni členové DAG mají funkční replikaci. Důležitým příkazem je Get-ServerComponentHealth, který spouští i SCOM v rámci aplikačního monitoringu. Tento příkaz slouží ke zjištění zdraví jednotlivých komponent: [43]

- ServerWideOffline
- HubTransport
- FrontendTransport
- Monitoring
- RecoveryActionsEnabled
- AutoDiscoverProxy
- ActiveSyncProxy
- EcpProxy
- EwsProxy
- ImapProxy
- OabProxy
- OwaProxy
- PopProxy
- PushNotificationsProxy
- RpsProxy
- RwsProxy
- RpcProxy
- UMCallRouter
- XropProxy
- HttpProxyAvailabilityGroup
- ForwardSyncDaemon
- ProvisioningRps
- MapiProxy
- EdgeTransport
- HighAvailability
- SharedCache
- MailboxDeliveryProxy

- RoutingUpdates
- RestProxy
- DefaultProxy
- Lsass
- RoutingService
- E4EProxy
- CafeLAMv2
- LogExportProvider [46]

Zmíněné příkazy, které se zadávají pomocí Exchange Management Shell, je vhodné vložit do skriptu, který bude jednotlivé příkazy spouštět v daný čas. A výsledek vložit do souboru a uložit na disk, případně výsledný report zaslat na zmíněné e-mailové adresy.

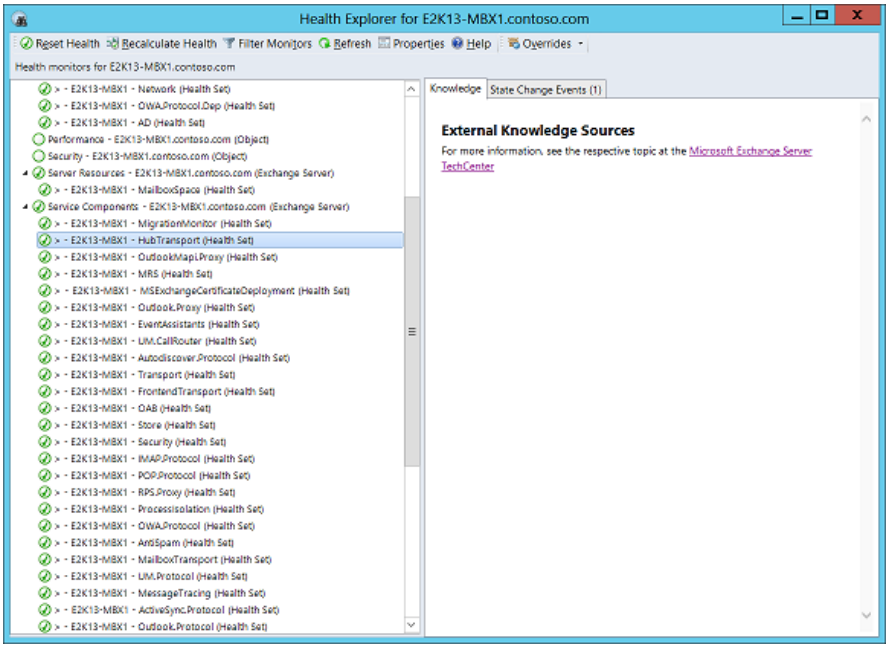
4.8.2.1 Konfigurace System Center Operations Manager

Microsoft Exchange dokáže monitorovat sám sebe. V případě doplnění o System Center Operations Manager, je administrátor schopen zvýšit úroveň monitorování. Pomocí SCOM je možné v jedné konzoli vidět schémata, grafy, historická data, upozornění a mnoho dalších. Pomocí tohoto softwaru je administrátor schopen konfigurovat eskalační kanály. [43]

SCOM je určen k aplikačnímu monitoringu, jedná se řešení od firmy Microsoft. Princip funkčnosti je založen na importování Management balíčků. Jedná se o XML soubory, které určují, jakým způsobem se monitoruje daná komponenta. Management balíček se může starat o monitorování souborového systému, o monitorování TMG, spoustu dalších věcí, dokonce je možné si i vytvořit vlastní balíček, který bude vytvořen na míru daného prostředí. [43]

V případě monitoringu Microsoft Exchange 2016, je nutné stáhnout balíček Microsoft Exchange 2013 Management pack. Jedná se o balíček určen pro starší verzi, ovšem vývojáři Microsoft Exchange oznámili, že nedojde k aktualizaci tohoto balíčku, jelikož mezi Microsoft Exchange 2013 a Microsoft Exchange 2016 není velký rozdíl. [43]

Balíček tedy obsahuje konfiguraci monitorů a pravidel, které budou monitorovat Microsoft Exchange Server. Dále obsahuje šablony, pro reportování informací, které se týkají poštovního serveru. [43]



Obrázek 31 – Health Explorer Microsoft Exchange v prostředí SCOM [43]

Monitory mohou hlídat například, volné místo na discích daného serveru, stav služeb klíčových pro funkčnost poštovního serveru. V případě, že se monitorována služba zastaví, dokáže SCOM pomocí monitoru službu znovu nastartovat a přitom je možné nastavit, zda má být administrátor notifikován. Jelikož znalost toho, že se daná služba neustále zastavuje, může znamenat daleko větší problém, a proto může problém řešit a těmto potencionálním problémům předejít.

Pravidla, zaznamenávají data a SCOM je díky tomu schopen vytvářet uživatelsky definované grafy.

4.8.2.2 Návrh monitorování Exchange On-Premise

Samotná instalace Microsoft Exchange On-Premise, dokáže monitorovat sám sebe. Ale výstupy tohoto monitorování budou dostupné pouze v aplikačním event logu.

Náplní administrátora bude na denní bázi, sledování aplikačního eventu, kontrola front na poštovních serverech, kontrola výkonu serveru, studování denních reportů, ve kterých bude uveden stav komponent poštovního serveru, průběh zálohy poštovních schránek, stav databází a Database Availability Group.

Dále bude naimplementován System Center Operations Manager, kde dojde k instalaci SCOM agentů na poštovní servery, díky tomu dojde k monitorování na úrovní operačního softwaru, k tomu aby byl k dispozici monitorování poštovního serveru, je nutné

naimportovat management balíček, který je ve formátu xml. Obsahuje monitory, pravidla a reporty týkající se Microsoft Exchange Server. V případě vzniku upozornění bude probíhat následný scénář.

Administrátor získá informaci prostřednictvím SMTP kanálu e-mailovou zprávu a vzniklém problému, v případě, že se problém nevyřeší do dvou hodin, dostane informaci pohotovost prostřednictvím SMS zprávy a e-mailem. Pokud po třech hodinách nedojde k vyřešení problému, dostane informaci vedoucí projektu e-mailovou zprávou a SMS zprávou. Tento eskalační proces bude uveden u všech monitorů a pravidel určených poštovním serverům.

4.8.3 Exchange Online

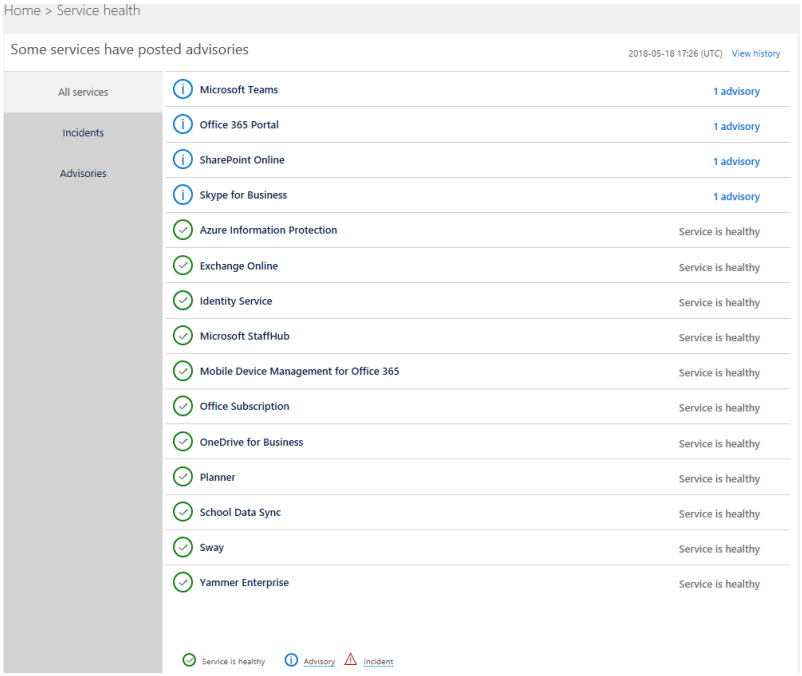
Monitorování celkového výkonu a stavu poštovních schránek v Exchange Online je významnou věcí administrátora. Není to jen o tom, aby šlo odeslat a přijímat e-maily, je nutné sledovat kapacitu jednotlivých e-mailových schránek, monitorování spamu a malwaru. Je nutné sledovat samotnou službu Exchange Online v rámci Office 365, pro samotnou funkčnost Exchange Online je také nutná funkčnost integrace služby Azure Active Directory s lokální Active Directory.

V rámci administrátorského centra Office 365, je možno přehledně sledovat „zdravotní stav“ veškerých služeb v rámci Office 365. V případě vzniku určitých incidentů, takový incident může vypadat takto:

Název:	EX134550 - Email delays
Dopad na uživatele:	Users were experiencing email delays.
Aktualizováno:	2018-04-23 20:15 (UTC)
Začátek:	2018-04-20 08:17 (UTC)
Konec:	2018-04-20 16:30 (UTC)
Zpráva:	User Impact: Users were experiencing email delays. More info: Our telemetry indicates that impact affected email sent over the internet. The impact to intra-tenant email appears to have been less severe. Final status: Further investigation confirmed that a fiber responsible for Azure data center to data center connectivity was severed which resulted in Office 365 email delays. The fiber was repaired and we've worked directly with some impacted customers to confirm impact remediation. Scope of impact: Impact was specific to a subset of users who were served through the affected infrastructure. Start time: Friday, April 20, 2018, at 8:17 AM UTC End time: Friday, April 20, 2018, at 4:30 PM UTC Preliminary root cause: A fiber responsible for Azure data center to data center connectivity was severed which resulted in Office 365 email delays. Next steps: We're reviewing our monitoring services to look for ways to reduce detection time and more quickly restore service. We’re reviewing our infrastructure for improved performance and potential automated recovery options to reduce or avoid similar impact in the future. This is the final update for the event.

Tabulka 7 – Příklad incidentu v rámci Exchange Online

Dále je možné vidět různá oznámení, například, že není možné v rámci Outlook on the Web přistoupit ke sdílené schránce. Pokud je možné vidět stav služby jako zdravá, znamená to, že služba funguje správně.



Obrázek 32- Stav služeb v Office 365

4.8.3.1 Integrace s lokální Active Directory

V rámci administrátorského centra Office 365, je možné sledovat „zdravotní stav“ konektoru pro integraci s místní Active Directory. Lze vidět název organizace, kolik domén je ověřené v Office 365, čas poslední integrace mezi Azure AD a lokální AD, zda je zapnuta synchronizace hesel, kdy naposledy proběhla synchronizace hesel, verze synchronizačního klienta, servisní účet určen pro synchronizaci.

Následně, lze sledovat samotnou službu Microsoft Azure, a to z veřejně přístupného webu, zde je možné vidět stav veškerých služeb po celém světě anebo po přihlášení do tenantu organizace a sledovat stav služby, týkající se pouze dané organizace.

4.8.3.2 Exchange Online PowerShell

Dále je možné, stejně jako v případě Microsoft Exchange On-Premise, monitorovat Exchange Online v rámci Windows PowerShell. Pro připojení do Exchange pomocí PowerShell, je nutné přistupovat z operačních systému Windows 7, Windows 8.1, Windows 10, Windows Server 2012 nebo 2012 R2, Windows Server 2016, Windows Server 2008. Následně je potřeba mít nainstalován .NET Framework 4.5. Poté vložit následující příkazy do PowerShell: [47]

Vložení přihlašovacích údajů administrátora Office 365 do proměnné UserCredential	$UserCredential = Get-Credential
Vložení nové PowerShell relace Microsoft Exchange do proměnné Session, která se bude připojovat na https://outlook.office365.com	$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic -AllowRedirection
Dojde k importu relace Session	Import-PSSession $Session

Tabulka 8 – Přihlášení prostřednictvím PowerShell [47]

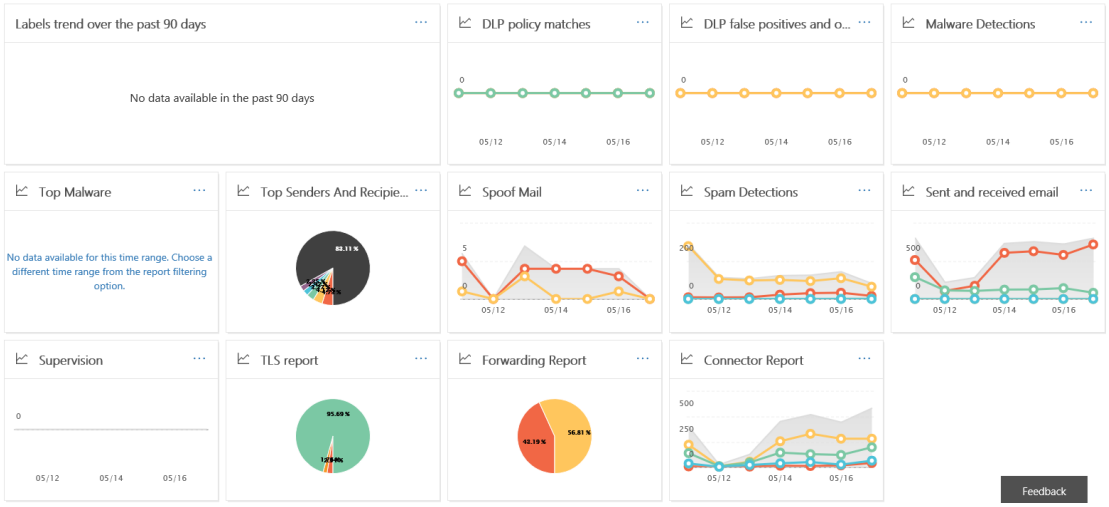
Poté existuje cirka pět set příkazů, které se týkají Exchange Online, Exchange Online Protection služeb. Příkazy jsou podobné jako příkazy určené pro Microsoft Exchange Server On-Premise, ovšem nejsou k dispozici příkazy týkající se stavu komponent poštovního serveru, stav služeb na daném serveru.

4.8.3.3 Exchange Online Protection

Pro větší ochranu proti škodlivému softwaru či spamu, lze využít Exchange Online Protection. Jedná se o dobře zásobený nástroj pro sledování provozu Exchange Online. Ve výchozím stavu je Exchange Online Protection pro poštovní schránky v rámci Exchange Online zapnuto. Díky tomu existuje další zdroj informací pro administrátora. EOP je schopen fungovat jako anti-spamová, anti-malwarová ochrana, ale také zprostředkovává data pro vytváření reportů. [26]

EOP obsahuje řadu šablon pro reportování, které jsou dostupné v administrátorském centru Office 365. Pomocí této komponenty, lze identifikovat podezřelé spam a malware e-mailové zprávy. [26]

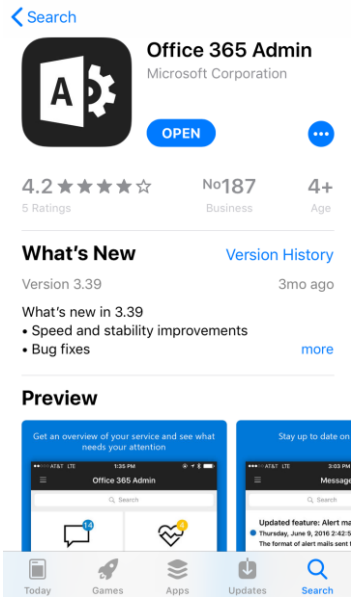
Přehled těchto indikátorů, lze zobrazit v Security&Compliance centru. Jednotlivé grafy je možné zobrazit podrobněji a filtrovat, dle vyhovujících podmínek. Jedná se o grafy Data Loss Prevention (DLP), které pomáhají identifikovat a chránit citlivé informace v rámci organizace. [48]



Obrázek 33 - Security&Compliance centrum

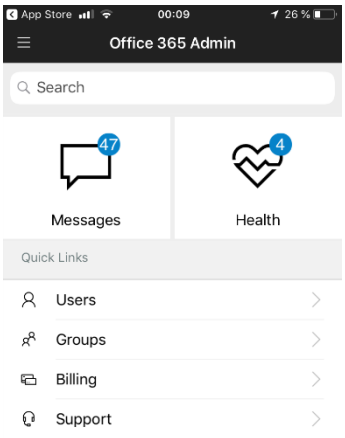
4.8.3.4 Mobilní aplikace Admin Office 365

Tato mobilní aplikace umožňuje spravovat Office 365 odkudkoliv, stáhnout lze z App Store, Google Play, Windows Store. Díky této aplikace, lze přijímat oznámení v reálném čase, přidávat uživatele, editovat uživatelské účty, kontaktovat podporu Office 365. Pomocí této aplikace, tedy administrátor rychle zjistí, zda je s danou službou nějaký problém, tato oznámení lze editovat. Proto administrátor Exchange Online nastaví, že chce primárně přijímat zprávy týkající se služby Exchange Online. Výhodou je i to, že lze vytvářet, odstraňovat uživatelské účty, přiřazovat jim licence, upravovat jejich údaje. V aplikace je možné sledovat vytvořené migrační dávky a jejich stav, a nastavit upozornění v případě dokončení nebo v momentě vzniklého problému. Pro úspěšnou instalaci aplikace stačí navštívit jeden z obchodů aplikací. Pro příklad na App Store, lze zdarma stáhnout tuto aplikaci a nainstalovat. Podmínkou je 114 MB volného místa na iOS zařízení, operační systém minimálně iOS 8.0. Aplikace je kompatibilní s iPhonem, iPadem a iPodem touch.



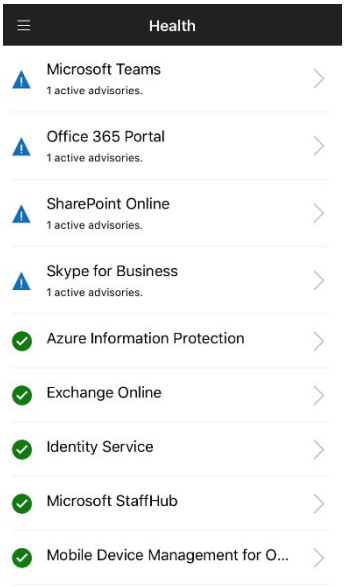
Obrázek 34 – Aplikace Office 365 Admin v App Store

Po úspěšné instalaci a spuštění aplikace, je nutné zadat přihlašovací údaje, ve kterých musí být uvedena e-mailová adresa a heslo administrátora. Po úspěšném přihlášení dojde k přesměrování na úvodní stránku aplikace, ve které si lze vybrat z možností, přečtení zpráv, zobrazení stavu služeb.



Obrázek 35 – Úvodní strana v aplikace Office 365 Admin

V případě zobrazení stavu služeb, je k dispozici přehled služeb, které jsou v rámci Office 365 k dispozici a jejich stav. V případě nějakého oznámení či incidentu, lze zobrazit detailní zprávu.



Obrázek 36 – Stav služeb v aplikaci Office 365 Admin

4.8.3.5 Návrh monitorování Exchange Online

Po úspěšné migraci uživatelů je nutno vyřešit kapitolu monitorování služeb Office 365, jelikož administrátor potřebuje vědět, zda je něco v nepořádku a uživatelé nebudou moci pracovat. Nevýhodou cloudových služeb oproti On-Premise řešení je ta, že administrátor není schopen sledovat samotný stav serverů, které zprostředkovávají běh služeb, proto nemůžu samotný administrátor ovlivnit, zda daný problém vyřeší či nikoliv. V Office 365 pouze sleduje stav služeb a může v případě problému kontaktovat klientskou službu, kde ohlásí daný problém.

Administrátor nastaví pravidelná zasílání reportů, odsouhlaseným příjemcům. Nejprve tedy bude přijímat samotný administrátor, vedoucí projektu a pohotovost. V centru pro administrátory v sekci Security&Compliance, nastavíme notifikace SMTP kanálem na stanovené příjemce. Dále v sekci, kde se uvádí „zdravotní stav“ služeb, v případě oznámení dojde k odeslání administrátorovi a vedoucímu projektu. V případě vzniku incidentu dojde k odeslání administrátorovi, vedoucímu projektu a pohotovosti.

Dále v portálu Azure, dojde k nastavení notifikací v případě problému se službou Azure, v případě vzniku oznámení bude stejně jako u Office 365 administrátor a vedoucí projektu. Jakmile vznikne incident, budou kontaktovány všechny tři složky.

Administrátor, vedoucí projektu a pohotovost bude mít na svých pracovních telefon stáhnutou aplikace Office 365 Admin, kde budou přihlášeni pomocí svých účtu s danými

právy v prostředí Office 365. Budou mít nastavené okamžité upozornění v případě změny stavu služby.

ZÁVĚR

V teoretické části byl vypracován princip funkčnosti poštovních služeb, došlo k popisu vybraných poštovních systémů. Práce se nejvíce zabývá produkty Microsoft, jelikož produkty od společnosti Microsoft, patří mezi velmi rozšířené a jsou v praxi velmi využívané.

Během popisu jednotlivých systému bylo popsáno řešení obrany proti spamu, neověřeným odesílatelům. Bylo doporučeno vytvořit Sender Policy Framework, společně s Domain Keys Identified Mail, nutno konstatovat, že jde pouze o snahu minimalizovat rizika. Jelikož dochází k neustálému prolomování kryptografických algoritmů. Proto je reálné, že toto opatření v budoucnu již nebude aktuální, je tedy nutné neustále sledovat vývoj této problematiky.

Bylo vypracováno navržení scénáře, podle zadaných požadavků zadavatele na migraci e-mailových schránek uložených v poštovním systému Microsoft Exchange 2016 On-Premise do prostředí Exchange Online. Dále byl zpracován návrh na vytvoření synchronizace mezi lokální adresářovou službou Active Directory a Azure Active Directory.

Podle požadavků byla vybrána synchronizační metoda Pass-through pro synchronizaci lokálních a cloudových adresářových služeb. Bylo vytvořeno praktické řešení tohoto typu synchronizace, během vytvoření synchronizace nedošlo k žádnému problému a uživatelské účty byly úspěšně synchronizovány. Testování jednorázového přihlášení proběhlo v pořádku.

Po implementaci synchronizace adresářových služeb, došlo k výběru vhodného migračního scénáře. Pro migraci poštovních služeb byl vybrán Hybridní scénář, jelikož nejvíce odpovídal požadavkům. Implementace tohoto řešení proběhlo úspěšně.

Bylo provedeno testování výsledků tohoto návrhu migrace poštovních služeb. Testování proběhlo na úrovni přihlášení do portálu Office 365, do Outlook on the Web, do aplikace Outlook na počítači v lokální síti. Přihlášení probíhalo jednorázovou autentizací. Proběhlo testování odeslání, přijímaní e-mailových zpráv, jak v rámci interní, tak externí domény. V případě vytváření schůzek pomocí aplikace Outlook, bylo testováno sdílení Free/Busy statusu, které dopadlo úspěšně.

Na závěr bylo navrženo řešení monitorování jak Microsoft Exchange 2016 On-Premise, tak Exchange Online, spolu s Azure Active Directory. Došlo k vytvoření eskalačního scénáře

v případě vzniku problému. Mezi eskalační kanály byl stanoven SMTP, pro e-mailovou komunikaci spolu s SMS kanálem.

SEZNAM POUŽITÉ LITERATURY

[1] The Inventor of Email: The History of Email [online]. 701 Concord Avenue Cambridge MA 02138 USA: International Center for Integrative Systems, 2018 [cit. 2018-05-21]. Dostupné z: http://www.inventorofemail.com/history_of_email.asp

[2] CLIFTON, Leonard. Mastering microsoft exchange server 2016. 2. Indianapolis, IN: John Wiley, 2016. ISBN 978-1-119-23205-6.

[3] H. CROCKER, David, ed. RFC822: Standard for ARPA Internet Text Messages. W3.org [online]. Dept. of Electrical Engineering: University of Delaware, Newark, DE 19711, 1998 [cit. 2018-05-21]. Dostupné z: https://www.w3.org/Protocols/rfc822/

[4] B. POSTEL, Jonathan. SIMPLE MAIL TRANSFER PROTOCOL. IETF Tools [online]. Fremont, California 94538 USA: Association Management Solutions, 2013 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc821

[5] Use Telnet to test SMTP communication on Exchange servers. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/bb123686(v=exchg.160).aspx

[6] SMTP Commands and Definitions. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2005 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/aa996114(v=exchg.65).aspx

[7] SIEMBORSKI, R. The Post Office Protocol (POP3). IETF Tools [online]. Fremont, California 94538 USA: Network Working Group, 2007 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc5034

[8] Configuring TLS and SSL for POP3 and IMAP4 Access. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2009 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/aa997149(v=exchg.141).aspx

[9] CRISPIN, M. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. IETF Tools [online]. Fremont, California 94538 USA: Network Working Group, 2003 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc3501

[10] POLLOCK, Wayne. Email Infrastructure. Wayne Pollock's Home Page [online]. Tampa Florida, USA: Wayne Pollock, 2006 [cit. 2018-05-21]. Dostupné z: http://wpollock.com/AUnix2/EmailSetup.htm#Internet

[11] MOCKAPETRIS, P. DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION. IETF [online]. Fremont, California 94538, USA: Association Management Solutions, 1987 [cit. 2018-05-21]. Dostupné z: https://www.ietf.org/rfc/rfc1035.txt

[12] PARTRIDGE, Craig. MAIL ROUTING AND THE DOMAIN SYSTEM. IETF [online]. Fremont, California 94538, USA: Association Management Solutions, 1986 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc974

[13] POLLOCK, Wayne. How Mail Works on the Internet. In: Wayne Pollock's Home Page [online]. Tampa Florida USA: Wayne Pollock, 2006 [cit. 2018-05-21]. Dostupné z: http://wpollock.com/AUnix2/EmailSetup.htm#Internet

[14] KNOTEK, Miroslav. Exchange Server 2013/2016: zabezpečujeme SSL/TLS. Optimalizovane IT [online]. Praha: KPCS, 2017 [cit. 2018-05-21]. Dostupné z: http://www.optimalizovane-it.cz/bezpecnost-a-identita/exchange-server-2013/2016-zabezpecujeme-ssl/tls.html

[15] How Exchange Online uses TLS to secure email connections in Office 365. Support Office 365 [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://support.office.com/cs-cz/article/how-exchange-online-uses-tls-to-secure-email-connections-in-office-365-4cde0cda-3430-4dc0-b489-f2c0736c929f?ui=cs-CZ&rs=cs-CZ&ad=CZ

[16] CRISPIN, M. INTERNET MESSAGE ACCESS PROTOCOL - VERSION 4rev1. IETF Tools [online]. Fremont, California 94538 USA: Network Working Group, 2003 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc3501

[17] KUALA, Budak. Sender Policy Framework (SPF). In: Notes Budak Kuala [online]. USA: Budak Kuala, 2013 [cit. 2018-05-21]. Dostupné z: http://notes.budakkuala.com/antispam/sender-policy-framework/

[18] CROCKER, ED., D. DomainKeys Identified Mail (DKIM) Signatures. IETF [online]. Fremont, California 94538, USA: Internet Engineering Task Force (IETF), 2011 [cit. 2018-05-21]. Dostupné z: https://tools.ietf.org/html/rfc6376

[19] Exchange 2016 architecture. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/jj150491(v=exchg.160).aspx

[20] CUNNINGHAM, Paul. Introduction to Exchange Server 2016 Database Availability Groups. Practical 365 [online]. USA: Practical 365, 2015 [cit. 2018-05-21]. Dostupné z: https://practical365.com/exchange-server/exchange-2016-database-availability-groups/

[21] Kerio Connect. Kerio [online]. Austin, TX 78701 USA: Kerio Connect, 2017 [cit. 2018-05-21]. Dostupné z: http://www.kerio.com/products/kerio-connect/server

[22] Kerio Connect Multi-Server. Kerio [online]. Austin, TX 78701 USA: Kerio Connect, 2018 [cit. 2018-05-21]. Dostupné z: https://manuals.gfi.com/en/kerio/connect/content/kerio-connect-multi-server/kerio-connect-multi-server-1667.html

[23] Exchange Online. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/jj200580(v=exchg.150).aspx

[24] Kde jsou umístěná vaše data?. Microsoft Trust Center [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://products.office.com/cs-CZ/where-is-your-data-located?ms.officeurl=datamaps&geo=Europe#Europe

[25] Exchange Online setup with an Exchange hybrid deployment. Support Office 365 [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/en-us/article/exchange-online-setup-with-an-exchange-hybrid-deployment-87c4eac6-f7fa-42c5-b449-efb1311f9fe4

[26] Exchange Online Protection. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/jj723137(v=exchg.150).aspx

[27] How to get an Azure Active Directory tenant. Microsoft Azure [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-howto-tenant

[28] User sign-in with Azure Active Directory Pass-through Authentication. Microsoft Azure [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-pass-through-authentication

[29] Implement password hash synchronization with Azure AD Connect sync. Microsoft Azure [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnectsync-implement-password-hash-synchronization

[30] Get the most from Office with Office 365. Microsoft Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://products.office.com/en/compare-all-microsoft-office-products?tab=2

[31] Get Office 365 free for your entire school. Microsoft Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://products.office.com/en/academic/compare-office-365-education-plans

[32] What you need to know about migrating your IMAP mailboxes to Office 365. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/en-us/article/what-you-need-to-know-about-migrating-your-imap-mailboxes-to-office-365-3fe19996-29bc-4879-aab9-5a622b2f1481

[33] Use network upload to import your organization's PST files to Office 365. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/en-us/article/use-network-upload-to-import-your-organization-s-pst-files-to-office-365-103f940c-0468-4e1a-b527-cc8ad13a5ea6#ID0EABAAA=How_it_works

[34] Přímá migrace do Office 365. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/cs-cz/article/přímá-migrace-do-office-365-9496e93c-1e59-41a8-9bb3-6e8df0cd81b4

[35] Co je potřeba vědět o fázované migraci e-mailu do Office 365. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/cs-cz/article/co-je-potřeba-vědět-o-fázované-migraci-e-mailu-do-office-365-7e2c82be-5f3d-4e36-bc6b-e5b4d411e207?ui=cs-CZ&rs=cs-CZ&ad=CZ

[36] Exchange Server Hybrid Deployments. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/jj200581(v=exchg.150).aspx

[37] How Exchange Online uses TLS to secure email connections in Office 365. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/en-us/article/how-exchange-online-uses-tls-to-secure-email-connections-in-office-365-4cde0cda-3430-4dc0-b489-f2c0736c929f

[38] Certificate requirements for hybrid deployments. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/library/hh563848(v=exchg.150).aspx

[39] Transport routing in Exchange hybrid deployments: Route incoming Internet messages through your on-premises organization. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/jj659050(v=exchg.150).aspx

[40] Introducing the Microsoft Office 365 Hybrid Configuration Wizard. You Had Me At Ehlo: The Microsoft Exchange Team Blog [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2015 [cit. 2018-05-21]. Dostupné z: https://blogs.technet.microsoft.com/exchange/2015/09/04/introducing-the-microsoft-office-365-hybrid-configuration-wizard/

[41] Move mailboxes between on-premises and Exchange Online organizations in hybrid deployments. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/o365e_hrcmoverequest_fl312271(v=exchg.150).aspx

[42] Learn more about .csv migrations. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/cs-CZ/library/ms.exch.eac.LearnMoreMigrationImportCsv(EXCHG.150).aspx?v=15.20.797.11&l=1&s=BPOS_S_E15_0

[43] BOB CORNELISSEN ... [ET AL.]. Mastering System Center 2012 Operations Manager. 2. Indianapolis, Ind: Wiley, 2013. ISBN 978-111-8238-424.

[44] Understanding how Exchange Server 2013 Management Pack reports system health. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2015 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/dn195910(v=exchg.150).aspx

[45] Overview of Exchange 2016 services. TechNet [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/ee423542(v=exchg.160).aspx

[46] Server Component States in Exchange 2013. You Had Me At EHLO: The Microsoft Exchange Team Blog [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2013 [cit. 2018-05-21]. Dostupné z: https://blogs.technet.microsoft.com/exchange/2013/09/26/server-component-states-in-exchange-2013/

[47] Connect to Exchange Online PowerShell. Microsoft Docs [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2017 [cit. 2018-05-21]. Dostupné z: https://docs.microsoft.com/en-us/powershell/exchange/exchange-online/connect-to-exchange-online-powershell/connect-to-exchange-online-powershell?view=exchange-ps

[48] Office 365 Security & Compliance Center. TechNet: Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2016 [cit. 2018-05-21]. Dostupné z: https://technet.microsoft.com/en-us/library/dn876574.aspx

[49] Office 365 Admin Mobile App. Support Office [online]. 1 Microsoft Way, Redmond, WA 98052, USA: Microsoft Headquarters, 2018 [cit. 2018-05-21]. Dostupné z: https://support.office.com/en-us/article/office-365-admin-mobile-app-e16f6421-2a1a-4142-bf9d-9846600a060a

[50] WATERS, Ian, David GREVE a Loryan STRANT. Microsoft Office 365 – Exchange Online Implementation and Migration - Second Edition [online]. 2. 35 Livery Street Birmingham, B3 2PB, UK.: Published by Packt Publishing, 2016 [cit. 2018-05-21]. ISBN 978-1-78439-552-0. Dostupné z: https://www.microsoft.com/en-us/store/p/microsoft-office-365-exchange-online-implementation-and-migration-second-edition/fgqpf3h0q7sd

[51] DNS Amplification Attack: Normal DNS query (Recursive). Nirlog [online]. UK: Niranjan Kunwar, 2006 [cit. 2018-05-21]. Dostupné z: http://nirlog.com/wp-content/uploads/2006/03/dns-recrussion-big.jpg

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AD	Active Directory.
SMTP	Simple Mail Transfer Protocol.
TCP	Transmission Control Protocol
POP	Post Office Protocol
IMAP	Internet Message Access Protocol
MTA	Mail Transport Agent
MDA	Mail Delivery Agent
MUA	Mail User Agent
MAA	Mail Access Agent
MSA	Mail Submission Agent
DNS	Domain Name System
MX	Mail Exchanger
TLS	Transport Layer Security
SSL	Secure Layer Security
HTTPS	Hyper Text Transfer Protocol Secure
SPF	Sender Policy Framework
DKIM	Domain Keys Identified Mail
MAPI	Messaging Application Programming Interface
EAS	Exchange ActiveSync
CAS	Client Access Server
EOP	Exchange Online Protection
PST	Personal Storage Table
SCOM	System Center Operations Manager
OWA	Outlook on the Web

XML Extensible Markup Language

MBX Mailbox

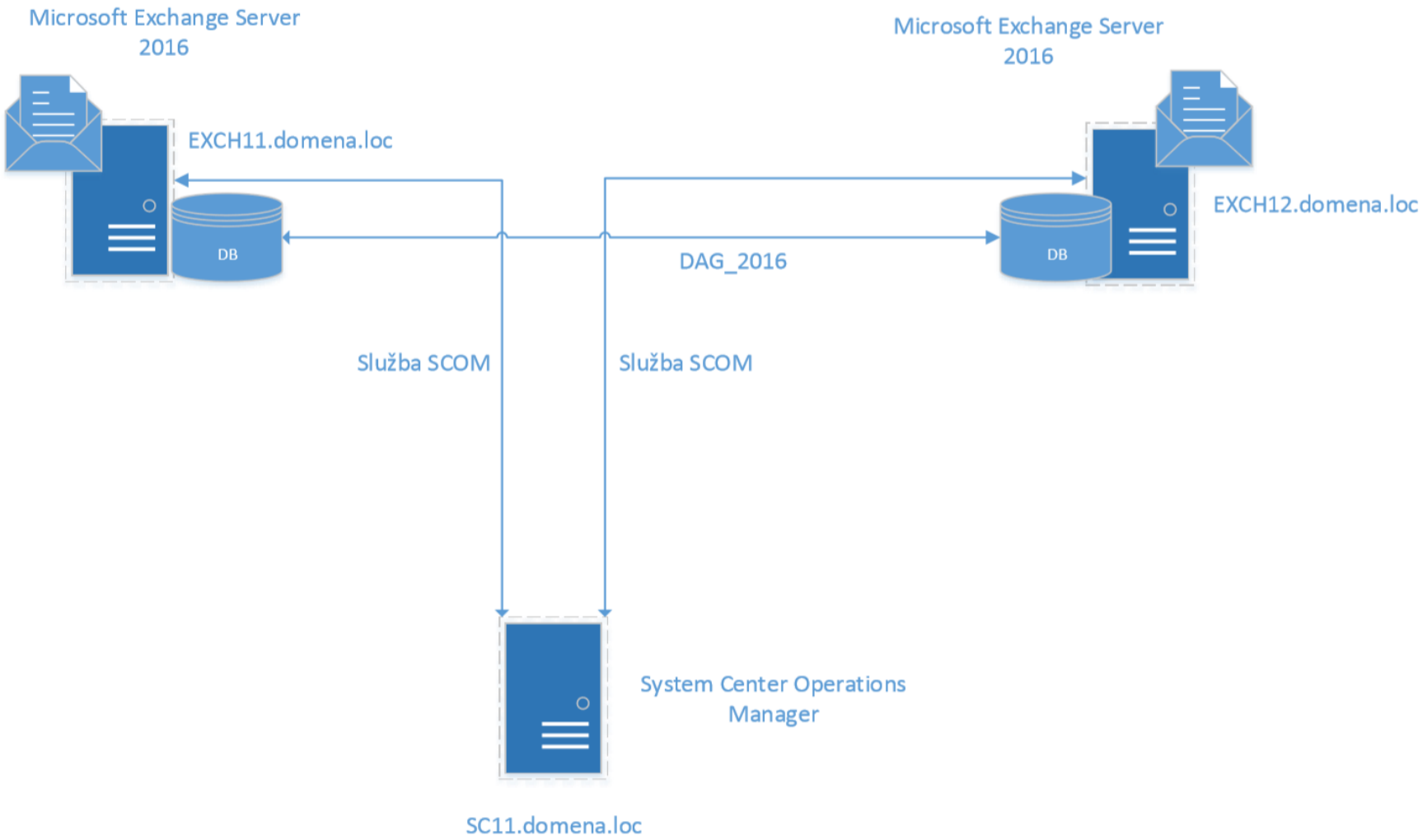
DAG Database Availability Group

SEZNAM OBRÁZKŮ

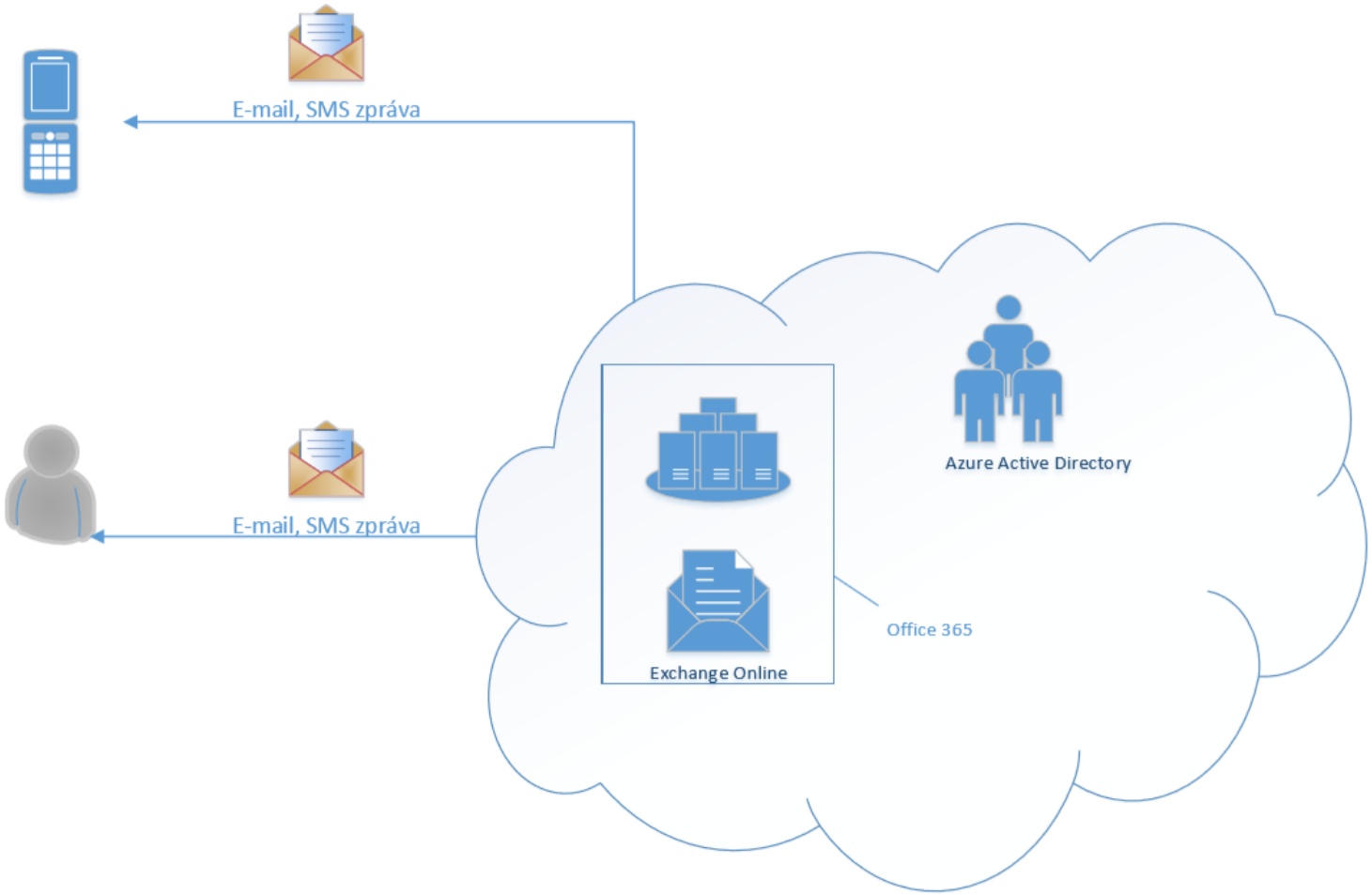
SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA P I: SCHÉMA ARCHITEKTURY MONITOROVÁNÍ ON-PREMISE



PŘÍLOHA P II: SCHÉMA ARCHITEKTURY MONITOROVÁNÍ CLOUD ŘEŠENÍ



PŘÍLOHA P III: NOTIFIKAČNÍ SCÉNÁŘ V PŘÍPADĚ VZNIKU INCIDENTU