OSIGURAVANJE VISOKE DOSTUPNOSTI I SIGURNOSTI EXCHANGE SERVERA

Velović, Dorian

Master's thesis / Specijalistički diplomski stručni

2019

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Algebra University College / Visoko učilište Algebra**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:225:109879

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-03-29**

ALGEBRA VISOKO UČILIŠTE

Repository / Repozitorij:

Algebra Univerity College - Repository of Algebra Univerity College

zir.nsk.hr

dabar DIGITALNI AKADEMSKI ARHIVI I REPOZITORIJI

VISOKO UČILIŠTE ALGEBRA

DIPLOMSKI RAD

OSIGURAVANJE VISOKE DOSTUPNOSTI I SIGURNOSTI EXCHANGE SERVERA

DORIAN VELOVIĆ

Zagreb, rujan 2019.

Predgovor

Rad posvećujem svojim roditeljima.

Prilikom uvezivanja rada, Umjesto ove stranice ne zaboravite umetnuti original potvrde o prihvaćanju teme diplomskog rada kojeg ste preuzeli u studentskoj referadi

Sažetak

U ovom radu opisat će se značajke Exchange Servera 2016, koje osiguravaju visoku dostupnost pozadinskih i pristupnih servisa. Također će se na primjeru objasniti visoka dostupnost baza sa podacima, te kako uz jednostavne korake kreirati razne politike za kontrolu tijeka klasificiranih informacija unutar poduzeća. Usporedba između implementacije on-prem i cloud rješenja u smislu budžeta biti će analizirana.

Ključne riječi: visoka dostupnost, klasificirani podaci

Abstract

Exchange Server 2016 high availability and security features will be described in this final thesis. High availability in terms of background (mailbox) services and access services. Failover will be analyzed in the example when one mailbox server fails. Also, implementation of DLP policies for securing classified data will be described on the example and which solution between on-premise and cloud is more likely to be implemented in different organization sizes.

Key words: high availabillity, classified dana

Sadržaj

1. Uvod 1

2. SMTP protokol 2

3. Razvoj Exchange servera kroz godine 6

3.1. Exchange 4.0 6

3.2. Exchange 5.0 6

3.3. Exchange 2000 6

3.4. Exchange 2003 7

3.5. Exchange 2007 8

3.6. Exchange 2010 10

3.7. Exchange 2013 11

3.8. Exchange 2016 12

4. Visoka dostupnost mailbox baza 14

4.1. Osiguravanje visoke dostupnosti mailbox baza 14

4.2. Planiranje rješenja u skladu sa SLA ugovorom 15

4.3. Konfiguracija i planiranje DAG grupa 16

4.4. Konfiguracija i kreiranje File Share Witness-a 17

4.5. Konfiguracija i kreiranje kopija baza podataka 19

4.6. Planiranje i održavanje *site*-resilient DAG grupa 21

4.7. Testiranje failovera i switchovera između DAG grupa 21

4.7.1. Database switchover 21

4.7.2. Server switchover 22

4.7.3. Datacenter switchover 22

5. Visoka dostupnost servisa klijentskog pristupa 23

5.1. Planiranje proxy-a ... 23
5.2. Planiranje *site*-resilient imenskih prostora ... 24
5.3. Planiranje certifikata ... 27
6. Visoka dostupnost transportnih servisa ... 28
6.1. Shadow Redundancy ... 29
6.2. Safety Net ... 32
6.2.1. Ponovno slanje poruka iz Safety Net-a ... 32
6.2.2. Ponovno slanje poruka iz Shadow Safety Net-a ... 33
7. Sigurnost i usklađenost Exchange infrastrukture ... 34
7.1. DLP rješenja ... 34
8. Testiranje visoke dostupnosti ... 39
9. Testiranje sigurnosti ... 42
10. Izbor između Exchange on-premise i Exchange Online ... 44
Zaključak ... 46
Popis kratica ... 47
Popis slika ... 48
Popis tablica ... 49
Literatura ... 50

1. Uvod

Vođenje poduzeća ili obavljanje posla, bez korištenja elektroničke pošte (engl. e-mail) je nezamislivo. E-mail sustavi su jedan od najkritičnijih komponenata poduzeća, te stoga iziskuju neprekidan rad ili barem, sa najmanjim mogućim prekidom rada. Najpoznatiji software za izmjenu e-mailova je Microsoftov Exchange server, koji je, za razliku od ostalih e-mail servera, jednostavniji za korištenje, te sadrži napredne funkcionalnosti poput kalendara, listi zadataka, dijeljenje datoteka, te kontakte. U ovom radu opisat će se i demonstrirati primjerima najbolje prakse za dizajn implementacije za osiguravanje visoke dostupnosti najpoznatijeg e-mail sustava – Exchange server 2016. Inačica servera 2016 omogućuje visoku dostupnost tehnologijom „Failover Cluster“. Osim visoke dostupnosti, pisat će se o sigurnosti Exchange-a, budući da su e-mailovi najčešći medij preko kojeg napadači šalju razne maliciozne napade.

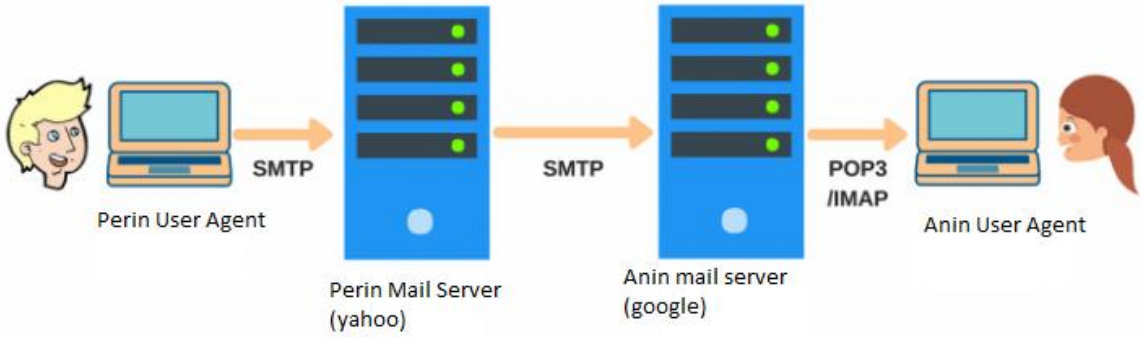
2. SMTP protokol

Što se zapravo događa kada se pošalje e-mail i klikne na tipku „Pošalji“? Kako se e-mail isporuči u željeni mailbox? Originalni opis funkcionalnosti SMTP (eng. Simple Mail Transfer Protocol) protokola, zaslužnog za slanje e-mailova, prikazan je u RFC 821 iz 1982. godine. Opširnija verzija tog dokumenta opisana je u dokumentu RFC 5321. RFC dokumenti su većinom opširni i teški za čitanje, pa ću protokol opisati u nastavku na primjeru slanja e-maila između dva korisnika. Komponente uključene u razmjenu poruke su:

User agent – Desktop ili web aplikacija na privatnom ili poslovnom računalu, koja dohvaća poruke sa mail servera, te služi za slanje poruka prema mail serveru.

Mail server – Udaljeni poslužitelj na kojemu su pohranjeni poštanski sandučići za svakog od korisnika u toj domeni. Primjerice yahoo.com ima svoje poslužitelje, dok google.com ima svoje.

Pod predpostavkom da prvi korisnik ima e-mail adresu pero@yahoo.com, dok drugi ana@gmail.com, te Pero šalje Ani poruku.



Proces slanja poruke demonstrirat ću kroz korake:

1) Pero otvara svoju desktop ili web aplikaciju, utipkava Aninu e-mail adresu, te joj šalje poruku

2) Mail aplikacija otvara sesiju sa serverom, pohranjuje sastavljenu poruku na server, te ju stavlja u red čekanja za slanje (eng. queue)

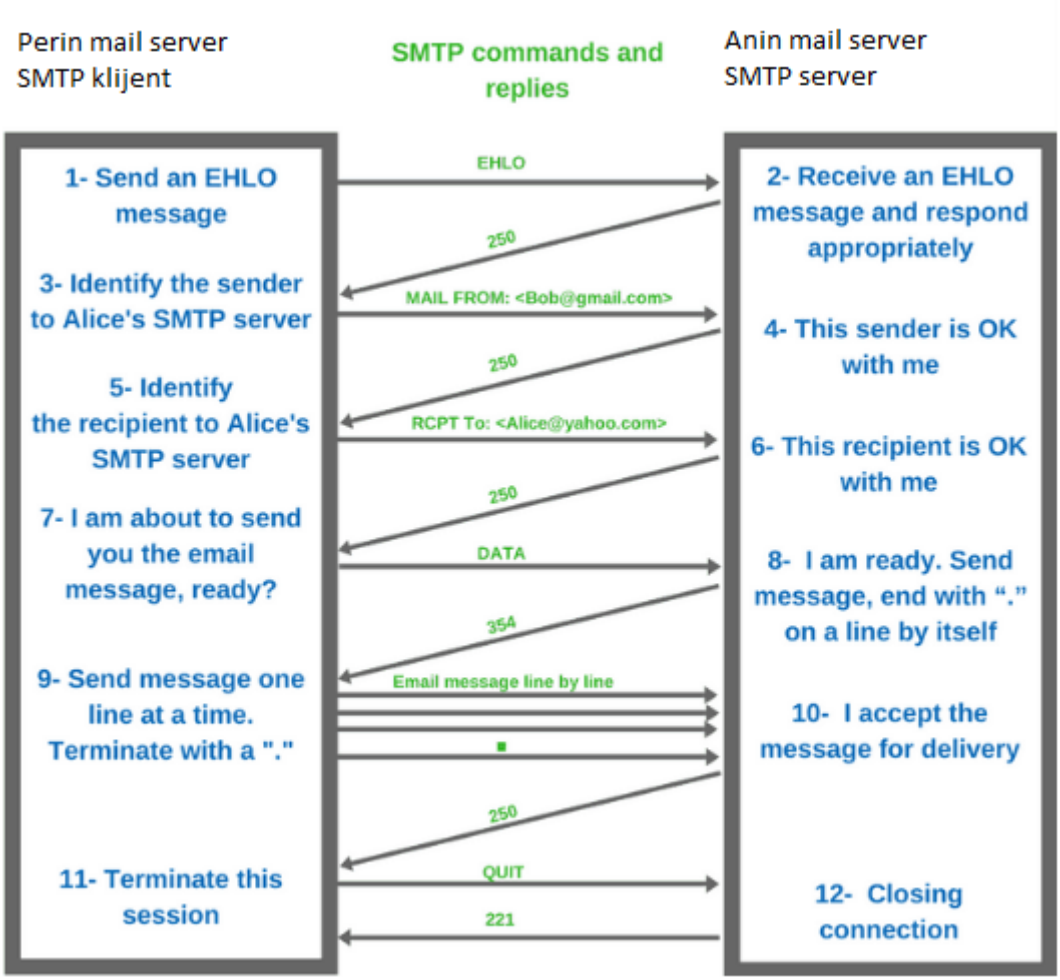
3) Yahoo mail server primjećuje da je poruka u redu čekanja spremna za slanje. Prije nego što ustanovi gdje mora poslati poruku, server dijeli e-mail adresu na domenski i korisnički dio. Kada bi domenski dio odgovarao yahoo domeni, ta poruka ne bi izlazila iz sustava, a s obzirom da se radi o vanjskog domeni, SMTP klijent šalje upit prema DNS serveru za MX zapisom domene google.com. Nakon što mu DNS server vrati upit sa IP adresom google mail servera, Yahoo server otvara konekciju prema google mail serveru. U ovom koraku SMTP protokol održava komunikaciju između dva mail servera. U opisanom scenariju Perin mail server (Yahoo) bit će u ulozi SMTP klijenta, dok Anin (Google) u ulozi SMTP servera

4) Nakon inicijalnog SMTP handshake-a između yahoo i gmail servera, SMTP klijent šalje poruku

5) Anin mail server zaprimi poruku, te s obzirom da je namijenjena Ani, pohranjuje ju u njen poštanski sandučić

6) Nakon što Ana otvori svoju mailing aplikaciju, poruka sa servera na kojem je njen poštanski sandučić se preuzme lokalno na njeno računalo.

U prijašnjim koracima spomenut je SMTP handshake. To je uspostava TCP konekcije na koji SMTP server odgovara kodom 220. Nakon što SMTP klijent dobije poruku 220, handshake počinje. Funkcija handshake-a je identifikacija klijenta i servisa koje klijent podrđava. U nastavku slijedi dijagram, koji prikazuje sve događaje handshakea[3]:



1) U prvom koraku, Perin mail server šalje EHLO (Hello) paket, na što server odgovara sa kodom 250

2) Kao odgovor na EHLO poruku, kod 250 potvrđuje primitak EHLO poruke, te u istoj poruci šalje podržane servise. Bitno je da klijent i server raspolažu istim servisima kako bi mogli komunicirati

3) Nakon što je upoznavanje gotovo, SMTP klijent šalje poruku oblika "MAIL FROM: <pero@yahoo.com>"

4) SMTP server, kao potvrdu na to šalje poruku 250, što bi značilo da nema problema sa tim pošiljateljem

5) Nakon potvrde pošiljatelja, SMTP klijent šalje poruku oblika "RCPT TO: <Ana@google.com>".

6) SMTP server porukom 250 potvrđuje, da je Ana vlasnik poštanskog sandučića u google mailbox bazi, te sa tim završava handshake dio.

7) Prije nego što počne razmjena tijela poruke, SMTP klijent pošalje komandu „DATA“, te očekuje odgovor 354 od SMTP servera, što bi značilo da je server spreman primiti tekst poruku.

8) Razmjena tijela poruke se odvija se dok SMTP klijent ne pošalje točku '**.**', koja označava kraj poruke. Kao u prijašnjim koracima, SMTP server odgovara porukom 250, kao potvrda primitka završetka teksta poruke.

9) Za kraj komunikacije SMTP klijent šalje poruku „QUIT“, na što server odgovara kodom 221 i tu završava proces slanja e-maila između dva SMTP servera.[4]

3. Razvoj Exchange servera kroz godine

3.1. Exchange 4.0

U uvodu je spomenuto što je Exchange i čemu služi, a u nastavku će se opisati njegov razvoj kroz godine. Sve je počelo davne 1996 godine sa inačicom Exchange 4.0. Te je godine Internet polako postajao dostupan javnosti, a „AltaVista“ je bio popularni pretraživački alat. Exchange je bio jedna od prvih aplikacija koja je uistinu iskoristila čari interneta i kolaboracije među ljudima. Ova verzija se instalirala na Windows NT Server 3.51.

3.2. Exchange 5.0

Već godinu kasnije, 1997. javnosti je postala dostupna verzija Exchange server 5.0. Bio je to veliki dan za Microsoft, pošto je u ovoj verziji, po prvi puta postala dostupna Exchange administratorska konzola i integrirani pristup SMTP mrežama. Zajedno sa ovom verzijom servera, izašla je i klijentska aplikacija „Exchange Client“, iako je to bila jedina verzija iste. Nakon nekoliko mjeseci, Microsoft je objavio Enterprise i Standard verziju Exchange servera 5.5. Razlika je bila u limitima baze podataka. Standard verzija je podržavala do 16 GB, dok je Enterprise verzija podržavala do 16 TB. U ovoj verziji „Outlook client“ je zamijenio „Exchange client“, te je ta inačica tako otišla u povijest. Ova verzija servera se instalirala na Windows NT Server 4.0. Također bitno je spomenuti, da se u vrijeme Exchange-a 5.0, prvi puta pojavila OWA (Outlook Web Access), prva verzija web klijenta za pristup Exchange poštanskom sandučiću (engl. *mailbox*)[4].

3.3. Exchange 2000

Exchange server 2000 ili v6.0, kodno nazvana „Platinum“, objavljena je u jesen 2000. godine. Prva je to verzija, koja je bila kompletno ovisna o (engl. *Active Directory*, skraćeno AD). Prevladala je mnoga ograničenja prethodnih verzija, kao što su povećanje maksimalnih veličina baza podataka, te broj servera u klasteru sa 2 na 4. Mnogi su korisnici odgađali migraciju na Exchange 2000 zbog toga što je zahtijevao korištenje AD-a, te je stoga predstavljao velike izazove za korisnike. Ova verzija je zahtijevala minimalnu verziju Windows Server 2000.[5]

3.4. Exchange 2003

U rujnu 2003. godine, pod kodnim imenom „Titanium“, objavljena je verzija 2003 ili v6.5, te je zahtijevala instalaciju na Windows serveru 2000 SP4 ili Windows serveru 2003, iako su neke od značajki samo radile na novijem Windowsu. Prijelaz sa ranijih verzija Exchange-a na 2003 je bila lakši nego kod prethodne verzije, stoga su korisnici Exchange-a 5.5 čekali ovu verziju za nadogradnju, te tako preskočili „Platinum“. Exchange 2003 i Windows server 2003, odnosno AD 2003 je nudio mnoga poboljšanja u fleksibilnosti i performansama. Klastering servis je prvi puta predstavljen u „Titanium-u“. Neke od novih funkcionalnosti su:

- **Filtriranje konekcija**: Blokiranje E-mailova prema IP adresama prema raznim blacklistama
- **Filtriranje primatelja**: Blokiranje E-mailova poslanih prema ručno definiranim primateljima na serveru. Ova značajka je zaustavljala spamere od nagađanja primatelja.
- **Filtriranje pošiljatelja**: Iskorištavanja SPF DNS zapisa za potvrdu pošiljatelja.

Exchange 2003 je prva verzija u kojoj su predstavljene dvije role – „Front-End“ i „Back-End“. Uloga „Front-End“ servera je bila posluživanje OWA i IMAP/POP3 klijenata, dok je „Back-end“ rola bila namijenjena SMTP komunikaciji i pristupu mailbox bazama podataka. Kao i prethodna, ova inačica Exchange servera je također dolazila u Standard i Enterprise paketu. Razlike su prikazane na tablici (Tablica 3.1)[6].

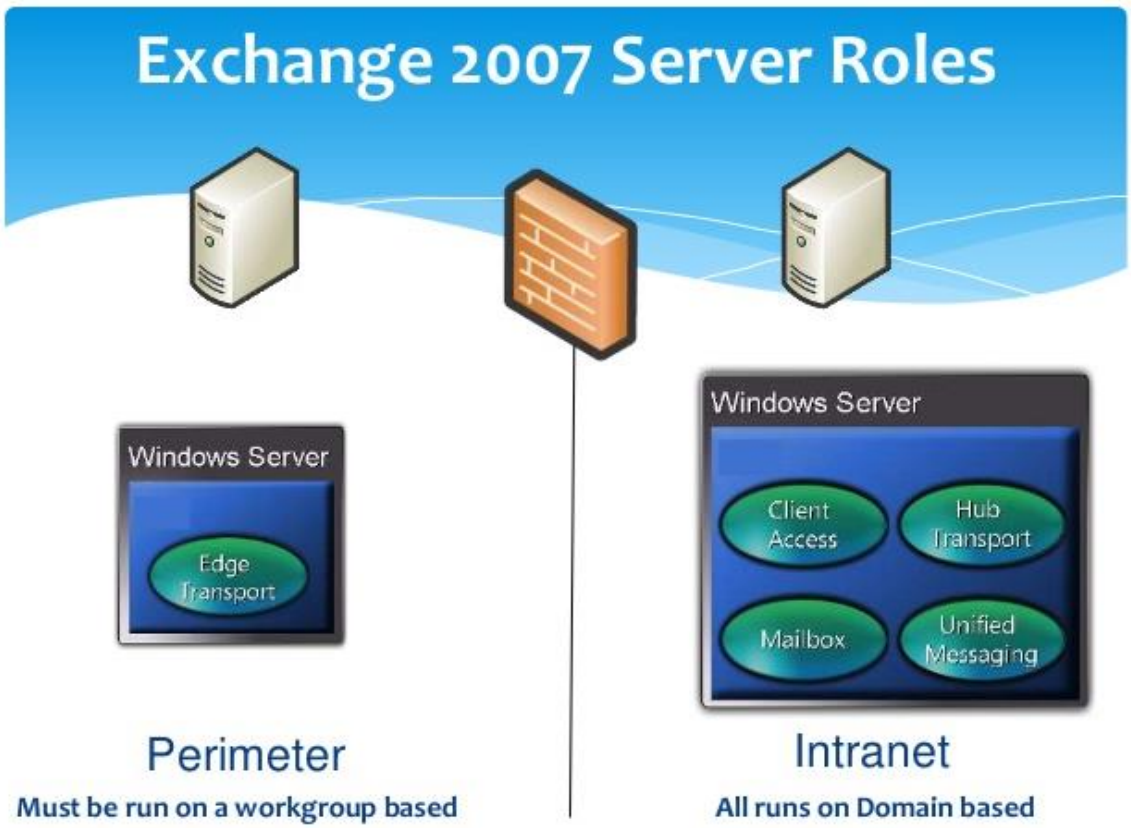
Značajka	**Standard**	**Enterprise**
Podržani broj (engl. *storage*) grupa	1	4
Podržani broj baza podataka po storage grupi	2	4
Individualna veličina baze podataka	16 GB	16 TB
Podržavanje klasteringa	NE	DA

Tablica 3.1 Prikaz razlika Standard i Enterprise verzije Exchange-a 2003

3.5. Exchange 2007

Inačica (koja se nije zvala sukladno godini u kojoj je objavljena), je Exchange server 2007, kodnog imena E12 (Exchange 12 ili v8), izdana je zimi 2006. godine. E12 se može instalirati samo na 64-bitnu verziju Windows servera. U ovoj verziji predstavljen je koncept 5 serverskih rola, te Back-end i Front-end koncept se više ne primjenjuje. Svaka od rola ima svoje mjesto instalacije (kao što je prikazano na slici 2.1) i svoju ulogu u infrastrukturi, a te su role slijedeće[8]:

- **Mailbox** – koristi se za skladištenje e-mailova i „public foldera“ krajnjih korisnika
- **Hub Transport** – odgovoran za usmjeravanje e-mailova do sljedećeg hopa i filtriranje e-mailova između mailbox-a (čak i ako se nalaze na istim serverima)
- **Client Access** – Slična funkcionalnost kao Front-end rola kod „Titaniuma“, omogućuje klijentske konekcije na mailboxe sa drugih protokola (POP3, IMAP), kao i konekcije pomoću mobilnih uređaja protokolom ActiveSync.
- **Edge Transport** – Rola koja se instalira na server na perimetarskoj mreži, te je odgovoran za higijenu i sigurnost poruka
- **Unified Messaging** – Omogućuje korisnicima pristup e-mailovima, kontaktima i kalendarima, putem telefona



Slika 3.1 Role Exchange servera 2007

Osim novih rola za servere, uvedene su i neke od novih funkcionalnosti:

- **Exchange Management Shell** - predstavljen je sa ovom verzijom Exchange-a. Izgrađen je na temeljima Powershell tehnologije sa Windows servera i omogućuje upravljanje istim operacijama koje imamo u EMC-u, sa podrškom bulk (više repetitivnih operacija sa sličnim parametrima) operacija.
- **Transportna pravila** – Pravila koja se primjenjuju na e-mailove, prema kojima se donosi odluka o tome što napraviti sa e-mailom. Na primjer, mogu se dodati potpisi na kraju tijela e-maila, kod odlaznih poruka ili riječi u subjekt e-maila kada poruka dolazi sa određenog pošiljatelja.
- **Poboljšano korištenje kalendara i unified messaging-a**
- **Povećana maksimalna veličina baze na 16TB**
- **Povećan broj maksimalnih storage grupa i bazi po serveru**

3.6. Exchange 2010

Exchange server 2010, izdan u proljeće 2009. godine, donio je sa sobom brojne nove funkcionalnosti (u usporedbi sa prijašnjom verzijom), što je i potvrđeno nagradom „InfoWorld's 2011 Award“. S obzirom na široki spektar administrativnih poslova, povećala se potreba za različitim vrstama administracije. Samim time bila je potrebna separacija i delegacija prava. Predstavljen je (engl. „*Role Based Access Control“*, skraćeno RBAC) pomoću kojeg, se može korisnicima dati prava, da si sami podešavaju opcije kroz web bazirano sučelje. U nastavku su dodatne značajke, koje su došle sa ovom inačicom Exchange servera[9]:

DAG (Database Availability Group) – omogućuje visoku dostupnost baza podataka (kao što je prikazano na slici 2.2), a u 3. poglavlju se nalazi više informacija o DAG-u.

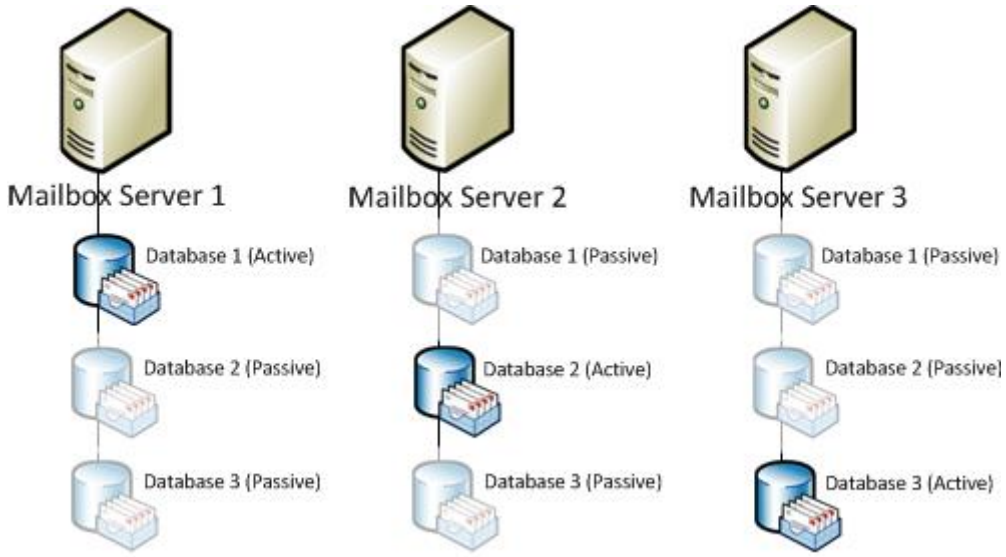
CAS (Client Access Server) – visoka dostupnost klijentskog pristupa kroz CAS polja, koji se sastoji od više CAS servera iz iste AD lokacije (engl. *site*-a), sa jednim imenskim prostorom.

Mailbox server rola može se kombinirati sa CAS – u Exchange 2007, mailbox server rola se nije mogla kombinirati sa drugim rolama. Exchange Server 2010 dolazi sa tom funkcionalnošću i može se kombinirati sa CAS ili/i sa Hub rolom.

RPC Client Access – uvođenjem ove značajke, svi Outlook klijenti se spajaju na svoje mailbox-e preko CAS servera.

Personalna arhiva – implementira se sekundarni mailbox za potrebe arhiviranja. Sekundarni mailbox se najčešće pohranjuje u bazi koja je na drugim, jeftinijim diskovima.

Shadow Redundancy – značajka koja štiti e-mailove u tranzitu, tako što Hub transport server odgađa brisanje poruke iz reda čekanja (engl. queue), sve dok mu sljedeći server u lancu isporuke, ne odgovori potvrdno da je poruka poslana na sljedeći korak u lancu (engl. *next hop*).



Slika 3.2 Shematski prikaz DAG-a

3.7. Exchange 2013

Exchange 2013 je donio „Exchange admin center“ (EAC), jedinstvenu upravljačku konzolu, koja je optimizirana za on-premise, cloud ili hibridni model (engl. *deployment-a*). EAC je zamijenio „Exchange Management Console“ (EMC) sa Exchange-a 2010 i „Exchange Control Panel“ (ECP), iako se termin ECP i dalje koristi za virtualni direktorij EAC-a. Neke od značajki EAC-a su:

- **Izlistani prikaz** – novi prikaz objekata je izbacio ograničenja, koja je imao ECP, jer je prikazivao samo 500 objekata, te ako objekt koji tražimo nije bio na listi, morali smo koristiti opcije filtriranja. Ovaj prikaz ima limit na 20 000 objekata, što je zasigurno dovoljno da nađemo objekt koji nas zanima. Također dodano je sortiranje po stranicama
- **Dodavanje stupaca u listu primatelja** – može se ručno odabrati koje podatke o primaocu želimo prikazati na listi
- **Sigurnost ECP virtualnog direktorija** – može se limitirati pristup EAC-u prema mjestu pristupanja (sa interneta ili intraneta)
- **RBAC editor** – RBAC se sada može podešavati unutar EAC-a

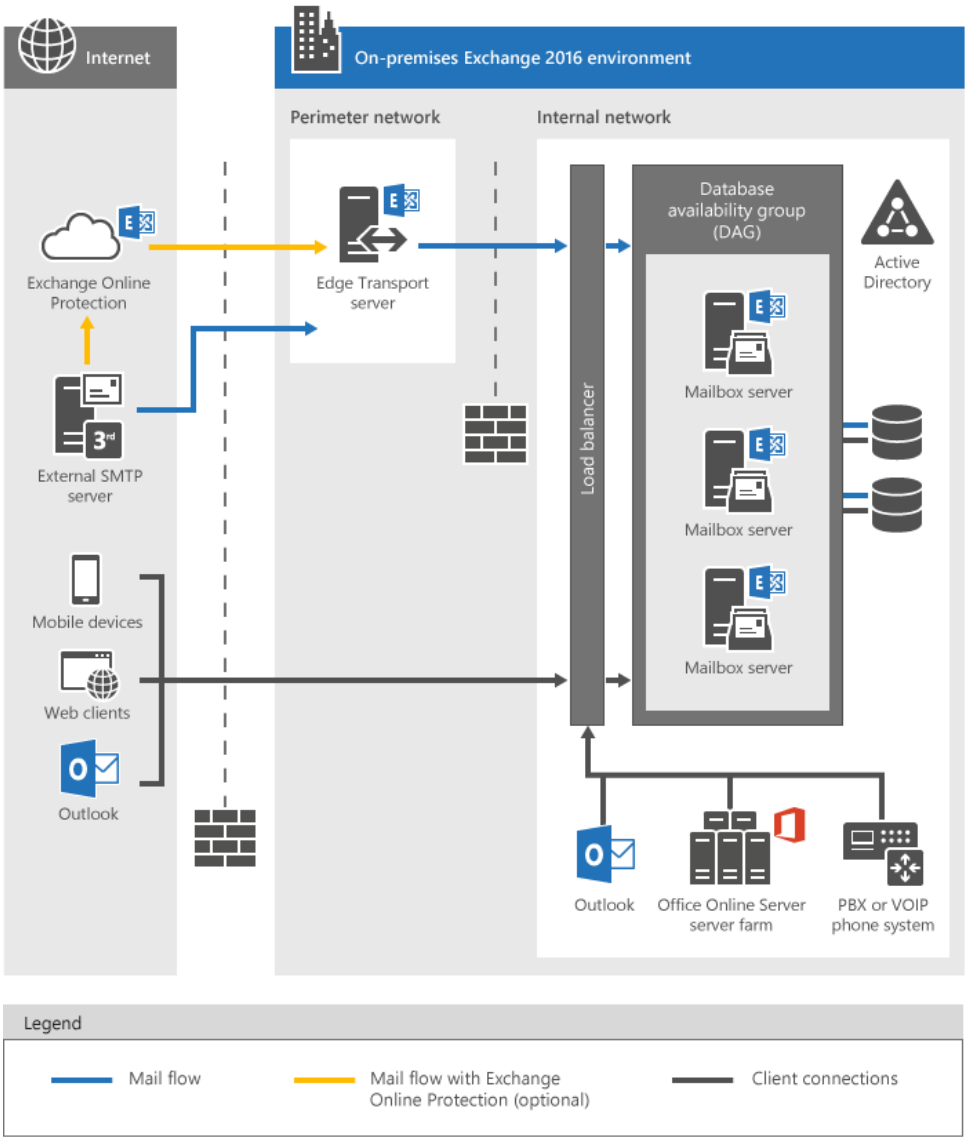
Prijašnje verzije Exchange-a su bile optimizirane prema tehnološkim ograničenjima toga vremena. Na primjer, tijekom razvoja verzije 2007, ograničenje je bilo procesorska snaga.

Da bi se to izbjeglo, arhitektura je podijeljena u role, koje su omogućivale skaliranje kroz razdvajanje servera. Međutim, role u verzijama 2007 i 2010 bile su čvrsto povezane, što je imalo mnogo loših strana kao što su zahtijevanje istih verzija, AD *site*-ova, skupih L7 (engl. *loadbalancer-a)* i kompleksnost imenskog prostora. U današnje vrijeme procesorska snaga je jeftinija i više se ne smatra ograničenjem. Stoga, ciljevi dizajna su bili pojednostavljenje skaliranja, iskorištavanja hardware-a i izolacija potencijalnih točaka prekida. U ovoj verziji Exchange-a postoje 3 role: Client Access, Mailbox i Edge transport. Mailbox server rola se sastoji od client access protokola, transport servisa i mailbox baze podataka. Client access server omogućuje autentikaciju, preusmjerenja i proxy servise i ne obavlja nikakve operacije nad podacima. Sve operacije i aktivnosti izvršavaju se na mailbox serveru.[10]

3.8. Exchange 2016

Najnovija verzija Exchange-a dolazi sa brojnim inovativnim značajkama, kojima je glavni fokus na kolaboraciji, te praksama koje se implementiraju kroz mnoge organizacije današnjice. Uvedene su neke arhitekturne promjene za veću brzinu, povezanost i izvođenje raznih operacija.

Exchange 2016 se lakše konfigurira i deploy-a nego prijašnje verzije sustava, što je velika olakšica za administratore. Prva bitna promjena je ukidanje Client Access Server role, koja u ovoj verziji postoji kao servis na serveru sa Mailbox rolom. Glavni razlog tome je mogućnost ispada raznih komponenti servera. Uzmimo za primjer, da imamo Exchange 2013 organizaciju sa pet servera od kojih su 2 CAS-a te 3 Mailbox servera. U slučaju ispada jednog CAS servera, sav se klijentski promet mora preusmjeriti na jedini CAS server, što povećava trošenje resursa istog, te u konačnici povećava rizik od ispada. Kod Exchange 2016 infrastrukture, u slučaju ispada jednog od servera, klijentski se promet jednoliko preusmjeruje na preostala 4 servera, te je zagušenje servera vidno manje. Osim toga, za iste performanse infrastrukture nije potrebno koristiti 5 servera, već je moguće sa manjim brojem, te u slučaju ispada, oporavak je znatno brži. U nastavku je na slici (Slika 3.3) prikazana shema Exchange 2016 infrastrukture te tijek poruka[11].



Slika 3.3 Shematski prikaz Exchange 2016 infrastrukture

Nadalje, kako bi konekcije i re-konekcije bile brže, Exchange 2016 potpuno prelazi na „MAPI over HTTP“ protokol, te tako MAPI preko HTTP-a postaje zadani protokol korisničkih konekcija. U slučajevima kada klijent ne podržava MAPI, koristit će „RPC over HTTP“ protokol.

U prijašnjim verzijama, MAPI protokol se također koristio, međutim enkapsuliran u RCP paket, koji je na kraju omotan u HTTP zahtjev. Tako kompleksan način slanja zahtjeva, znači duže vrijeme spajanja. RPC enkapsulacija je izostavljena u ovoj verziji Exchange servera, te je cijeli proces konekcije pojednostavljen i brži, a kao dodatni bonus, HTTP zaglavlje sadrži samo značajne podatke[12].

4. Visoka dostupnost mailbox baza

Arhitektura Exchange servera je dizajniranja u smjeru pružanja visokih performansi i dostupnosti mailbox servisa sa minimalnim troškom. Microsoft je, da bi to postigao, investirao u poboljšanje mehanizama upravljanja sustavima za pohranu podataka (engl. *storage*). Dobro dizajnirana infrastruktura je samostojeća, te u slučaju konfiguracije sa visokom dostupnošću, može biti otporna na razne scenarije ispada rada komponenata ili čak cijelih sustava.

4.1. Osiguravanje visoke dostupnosti mailbox baza

Mailbox baze podataka, koje se nalaze samo na jednom Exchange poslužitelju, osjetljive su na prekid rada ukoliko nastupi kvar bilo koje komponente servera. Kako bi smanjili rizik od prekida rada zbog jedne ključne točke (eng. Single point of failure), mailbox baze podataka mogu se konfigurirati sa visokom dostupnošću (engl. database availability group - DAG u nastavku) načinu rada. DAG je model visoke dostupnosti u infrastrukturi Exchange servera.

DAG se može sastojati od najviše 16 servera, koji međusobno repliciraju kopije mailbox baza kroz sve servere u DAG grupi. DAG nam omogućuje visoku dostupnost, te štiti bazu podataka od software-skih grešaka, korupcije podataka, ispada rada nekih od hardwerskih komponenti servera i ostalih dijelova u podatkovnim centrima. Jedan Exchange server može biti dio samo jednog DAG-a, a svi DAG partner serveri moraju imati instaliranu istu verziju Exchange servera, te kombinacija dviju verzija nije podržana. U scenarijima migracije sa ranije verzije servera na višu, potrebno je kreirati novi DAG i mailbox baze podataka, te potom premjestiti mailboxe iz starog DAG-a u novi.

Exchange DAG nije clustering aplikacija, međutim koristi komponente i značajke role „Windows failover cluster“. Klaster se automatski kreira i konfigurira kod dodavanja prvog partner servera u DAG okruženje. „Failover clustering“ radi na principu quoruma, koji se manifestira kao proces glasovanja, u kojem se odlučuje, treba li server koji je DAG partner, ostati dostupan ili ne. Da bi se osigurala „većina“, odnosno quorum, DAG radi u jednom od dva modela glasovanja:

- **Node Majority quorum mode** – koristi se kod neparnog broja DAG partnera. Svaki partner ima jedan glas u procesu glasovanja. Podaci o quorumu su zapisani na lokalni disk svakog DAG partnera.
- **Node and File Share Majority quorum mode** – koristi se kod parnog broja DAG partnera. U ovom modu implementira se FSW (File share witness) server koji odlučuje kako će proces glasovanja završiti. U poglavlju 3.4. nalazi se više informacija o FSW.

Kada je sva konfiguracija završena, te su sve mailbox baze podataka visoko dostupne, odnosno, postoje kopije baza podataka na svim replikacijskim partnerima, aktivna baza može se aktivirati na bilo kojem drugom serveru partneru koji sadrži kopiju mailbox baze. To se postiže na jedan od dva načina:

- **Switchover** – radnja koju administrator izvršava ručno, te uključuje premještanje aktivne baze podataka na drugi partner server. Switchover može biti ciljan na neki server ili DAG može automatski odlučiti, koju bazu aktivirati na temelju posebnih parametara o kojima ću govoriti kasnije.
- **Failover** – radnja koju DAG izvršava se automatski kao odgovor na ispad. Na primjer, automatski failover se dešava u trenutku ispada neke od komponenti servera, u kojem server prestaje sa radom.

Premještanje aktivne baze podataka, u stvari ne uključuje fizičko premještanje podataka. Bitno je naglasiti da su sve kopije baze podataka uvijek u sinkronizaciji, stoga svaka baza sadrži iste podatke. Premještanje aktivne baze podataka uključuje (engl. *dismount-anje*) aktivne baze, te (engl. *mount-anje*) pasivne baze. Tada pasivna baza postaje aktivna. Ovaj proces zove se još i „aktivacija kopije baze podataka“. Cijeli proces je gotov u svega nekoliko sekundi, te nema utjecaja na krajnje korisnike koji koriste „Outlook“ ili „Outlook on the web“.[1]

4.2. Planiranje rješenja u skladu sa SLA ugovorom

Neplanirani ispad sustava nije jedini razlog implementacije DAG-a, odnosno korištenja visoke dostupnosti. Exchange infrastruktura trebala bi biti dizajnirana u skladu sa poslovnim zahtjevima, te pripremljena za scenarije ispada sustava ili planiranog održavanja. Planirano održavanje servera, mrežne opreme u podatkovnim centrima, dijelovi su normalnih IT

operacija, te bi se trebale obavljati barem jednom mjesečno, kako bi software bio ažuriran (engl. Up to date).

Planiranje dizajna infrastrukture može, također, biti u skladu sa SLA ugovorom. Na primjer, u SLA ugovoru imamo definirani postotak dostupnosti 99% za e-mail servise. Kada to skaliramo na višu razinu to je 43.8 minuta ispada godišnje. Toliko vremena može oduzeti jedna instalacija sigurnosnih zakrpi, te ne preostaje mjesta za neplanirane ispade, koje bi također trebalo uzeti u obzir kod planiranja.

Kao što se može vidjeti iz prethodnog primjera, definiranje SLA ugovora je vrlo bitna stavka kod planiranja dizajniranja visoko dostupne infrastrukture.

4.3. Konfiguracija i planiranje DAG grupa

Novo kreirani DAG nema niti jednog partnera, stoga se moraju naknadno dodati. DAG se može sastojati od 1 do 16 servera, međutim, da bi se mailbox baza podataka smatrala visoko dostupnom, moraju postojati barem dvije kopije iste.

Za pripremu instalacije DAG-a, potrebno je instalirati Exchange mailbox server rolu na više servera, sa istim hardwareskim specifikacijama, uključujući iste veličine nazive volumena. Za uspješnu replikaciju podataka između baza u DAG grupi, svi DAG partneri moraju imati istu putanju do mailbox baze na svom lokalnom disku. Na primjer, ako je na jednom serveru baza smještena na lokaciji D:\DB01, isti folder mora postojati na svakom partneru.

Prije verzije Exchange-a SP1, bilo je potrebno kreiranje „Cluster Network Object“ objekta u AD-u, koji je bio poveza sa IP adresom (CAAP – cluster administrative access point). Taj se objekt koristio za povezivanje sa drugim upravljačkim alatima i aplikacijama, koje se povezuju na Failover Cluster i na sami DAG. U novoj verziji Exchange server 2016, CNO i CAAP nije potrebno kreirati. To uvelike smanjuje administraciju, te umanjuje rizik od ispada. Microsoft je odlučio koristiti (engl. *ipless*) iz iskustva sa problemima u Exchange online okruženju, koji su većinom bili uzrokovani konfliktom IP adresa.

Za kreiranje DAG-a koristiti se New-DatabaseAvailabilityGroup powershell *cmdlet* (naziv za Powershell komande). Svakom DAG-u mora se dodijeliti unikatno ime, te adresu FSW servera. FSW server može biti bilo koje podržane verzije Windows Servera, što bi u ovom trenutku značilo Windows Server 2008 R2 ili noviji. „Witness server“ može biti i domain controller, iako se to ne preporuča, jer bi u tom slučaju, morali dodati Exchange „Trusted

Subsystem“ grupu u administratorsku grupu za cijelu AD domenu. Također, mora se navesti parametar „filesystem“ ukoliko volumeni imaju ReFS filesystem.

```
[PS] C:\>  New-DatabaseAvailabilityGroup -name ALGEBRA_DAG -WitnessServer ZG-DC01 -FileSystem ReFS
```

Nakon što se kreira DAG grupa, potrebno je u nju dodati partnere, a potom Exchange automatski instalira „Windows Failover Cluster“ komponentu, instalira klaster i konfigurira FSW. Dodavanje servera u DAG, izvršavamo sljedećim powershell cmdletom:

```
[PS] C:\>  Add-DatabaseAvailabilityGroup -Identity ALGEBRA_DAG -MailboxServer ZG-EXCH01
```

Za dodavanje više partnera, ponovimo isti cmdlet za drugi server. Kako bi provjerili status novo kreiranog DAG-a, izvršimo cmdlet:

```
[PS] C:\>  Get-DatabaseAvailabilityGroup -Identity ALGEBRA_DAG -Status | Format-list
```

Parametar „Format-List“ koristi se kako bi vidjeli sve atribute DAG-a, te WitnessServer i WitnessDirectory atributi govore gdje je lociran FSW.

4.4. Konfiguracija i kreiranje File Share Witness-a

Bitna stavka kod deployment-a DAG-a, je implementacija File Share Wintess-a. Svi DAG-ovi imaju „Wintess server“ definiranu dijeljenu lokaciju, međutim, kao što je prethodno navedeno, samo DAG-ovi sa parnim brojem partnera rade u načinu glasovanja „Node and File Share Majority“. Takav pristup omogućuje iskorištavanje „Witness servera“ u svakoj situaciji kada glasovanje treba nastupiti. Na primjer, u slučaju serverskih održavanja, DAG sa 2 partnera mora isključiti jednog. To bi značilo da je 50% od ukupnog broja partnera ugašeno, te se quorum ne može postići. U takvim situacijama nastupa FSW koji se broji kao dodatni glas u procesu glasovanja. U protivnom, kada se quorum ne uspije održati, DAG se smatra ugašenim iako je jedan od partnera aktivan. Za FSW je bitno da bude aktivan kada dođe do glasovanja, ali inače nije potreban za normalne operacije DAG-a. Također, nije potrebno osigurati visoku dostupnost FWS pomoću DFS ili sličnih značajki redundancije.

U scenarijima sa više DAG-ova, FWS se može podesiti na isti server, s tim da je najbolja praksa, da se direktorij nazove po imenu DAG-a.

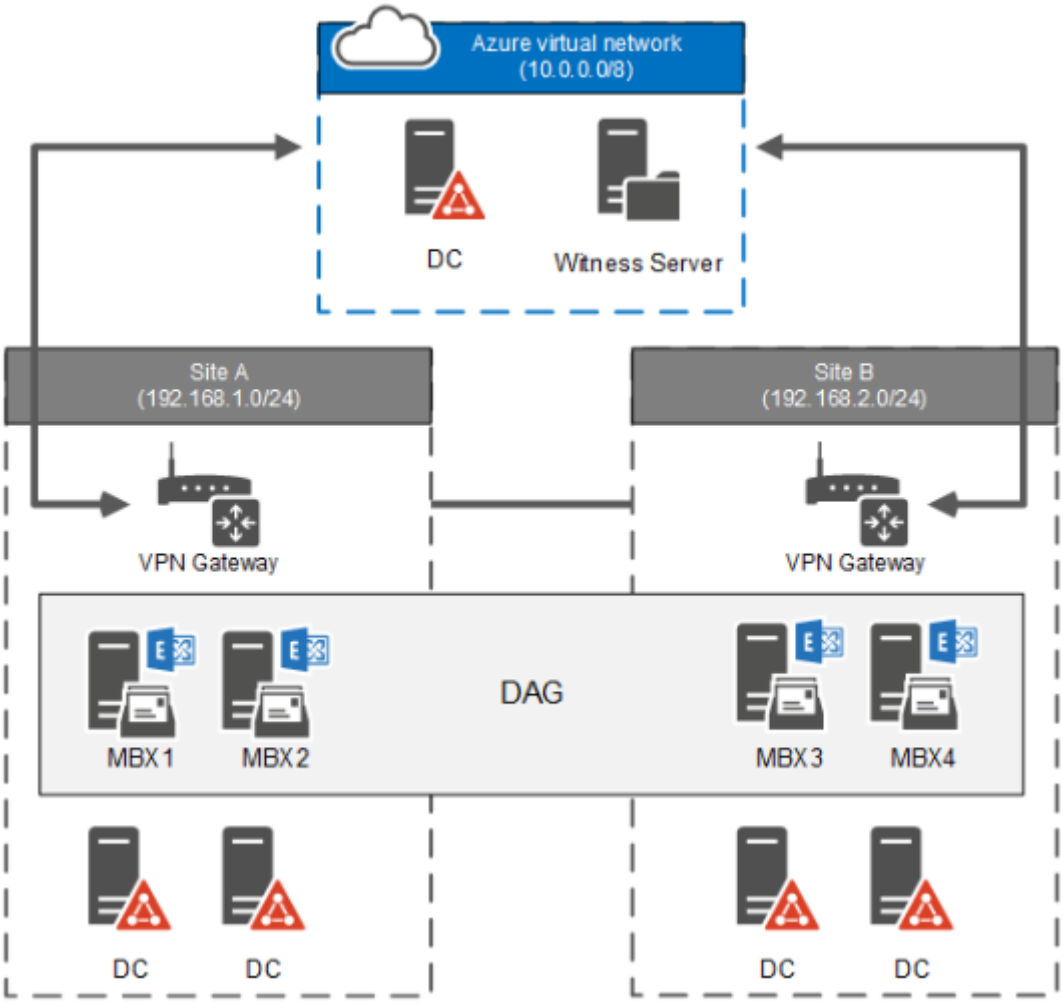
Uzimajući u obzir važnost uloge FSW, se mora pažljivo birati gdje ćemo ga smjestiti. Za DAG-ove smještene u istom podatkovnom centru, FSW se mora smjestiti tamo gdje ispad

jedne komponente neće izolirati FWS od oba DAG partnera. Quorum nije moguć ukoliko DAG partneri ne mogu komunicirati između sebe i u isto vrijeme sa FSW.

Kod scenarija sa više podatkovnih centara, FSW bi se trebao smjestiti u *site*-u koji smatramo primarnim. Drugim riječima, ako dođe do ispada WAN linka, mora se razmisliti koji od *site*-ova bi htjeli održati dostupnim.

Jedan od mogućih scenarija je smještanje FSW na treću lokaciju, s tim da svaka od lokacija mora imati nezavisnu konekciju sa ostale dvije lokacije. S tim smo osigurali da ispad jednog WAN linka, ne izolira više podatkovnih centara u isto vrijeme. Ovakav pristup omogućuje failover u situaciji ispada bilo kojeg podatkovnog centra, dok u situaciji kada imamo FSW na primarnoj lokaciji, ispad te lokacije značio bi gubljenje quoruma, što bi rezultiralo ispadom DAG-a. U takvim situacijama, potrebna je intervencija administratora.

S druge strane, ako se ne može imati treći podatkovni centar, moguće je smjestiti FSW na treću lokaciju u Azure VM. Nezavisni link između svih lokacija je i dalje ključan, kao i domain controller na lokaciji u Azuru kao što prikazuje Slika 4.1.



Slika 4.1 Shematski prikaz infrastrukture na dvije lokacije sa FSW u Azuru

4.5. Konfiguracija i kreiranje kopija baza podataka

Tek kada je Exchange server dodan u DAG, svaka mailbox baza koja se nalazi na tom serveru, postaje također dio DAG-a. Bitno je napomenuti, da baza nije visoko dostupna sve dok DAG ne sadrži barem dva partnera između kojih se vrši replikacija.

Za dodavanje servera u DAG grupu koristi se *cmdlet* Add-MaiboxDatabaseCopy i specificiramo ime servera. Nakon što je server dodan u DAG, započinje proces zvan „seeding“ koji kopira sadržaj baze i transakcijskog loga sa servera koji je trenutno aktivan na novo dodani server.

```
[PS] C:\>  Add-MaiboxDatabaseCopy -Identity DB01 -MailboxServer ZG-EXCH01
```

Proces „seeding“ je uglavnom dobra opcija, iako ga u nekim scenarijima želimo odgoditi, do primjerice vikenda. Odgoda seedinga se može napraviti u situacijama u kojima bi mrežni promet mogao zagušiti mrežu. Odgodu seedinga aktiviramo sa „-SeedingPosponed $True“

parametrom kod pokretanja Add-MaiboxDatabaseCopy cmdleta. U praksi ta bi se opija koristila ovisno o tome gdje se kopira baza (interno ili preko WAN linka), te u kojem trenutku se radi kopiranje. U najboljim praksama svako održavanje kao i skaliranje odrađuje se van radnog vremena, pa stoga se u većini slučajeva ova opcija ne koristi. Osim u izvanrednim situacijama koruptiranja baze i potrebe za kreiranjem nove.

Nakon dodavanja novog servera, svaka baza na njemu dobije parametar AP (Activation preference). Inicijalna baza dobije AP 1, a prva kopija baze dobije vrijednost 2 itd. AP služi administratorima da bi podesili baze koje bi se trebale aktivirati u slučaju failovera ili switchovera. Baze sa manjim brojem imaju prednost. AP se može modificirati cmdletom:

```
[PS] C:\> Set-MailboxDatabaseCopy -Identity DB01\ZG-EXCH01 -
ActivationPreference 2
```

Pregled stanja raspoređenosti se baza može pregledati cmdlet-om

```
[PS] C:\> Get-MailboxDatabaseCopyStatus * -Server ZG-EXCH01
```

```
[PS] E:\>Get-MailboxDatabaseCopyStatus -Server MMEM010 | Sort Nam
e | FT Name, Status, CopyQueueLength, ReplayQueueLength -AutoSize

Name                Status CopyQueueLength ReplayQueueLength
----                ------ --------------- ----------------
MDB10\MMEM010      Mounted               0                0
MDB11\MMEM010      Mounted               0                0
MDB12\MMEM010      Mounted               0                0
MDB13\MMEM010      Mounted               0                0
MDB14\MMEM010      Mounted               0                0
MDB15\MMEM010      Mounted               0                0
MDB16\MMEM010      Healthy               0                1
MDB17\MMEM010      Healthy               0                1
MDB18\MMEM010      Healthy               0                0
MDB19\MMEM010      Healthy               0                0
MDB20\MMEM010      Healthy               0                1
MDB21\MMEM010      Healthy               0                1
RMDB20\MMEM010 Dismounted               0                0
```

Slika 4.2 Prikaz statusa kopija baza

Zapisi sa statusom „Mounted“ označavaju baze koje su aktivne na specificiranom serveru, dok „Healthy“ prikazuju pasivne kopije.

4.6. Planiranje i održavanje *site*-resilient DAG grupa

Kako bi uvelike povećali visoku dostupnost naše DAG infrastrukture, proširujemo ih na podatkovne centre na različitim fizičkim lokacijama. Svrha je osiguravanje dostupnosti čak i u situacijama ispada cijelog podatkovnog centra. Termin koji se krositi za ovakve implementacije je „Size-resilient DAG“. U *site*-resilient DAG modelu, najbitnija stavka je da je round trip time (RTT – vrijeme koje je potrebno paketu da dođe do odredišne lokacije i nazad) manji od 500ms. Nimalo manje bitan parametar je dobar bandwidth (širina pojasa), koji osigurava neprekidnu replikaciju podataka između DAG partnera.

Svaki podatkovni centar bi u najboljoj praksi trebao biti u svom Active Directory *site*-u. Također, svaka lokacija bi trebala imati svoj IP subnet, u protivnom, Exchange smatra da su svi serveri unutar subneta na istoj lokaciji, iako su fizički odvojeni. Jedna od bitnijih *site*-aware (lokacijski svjesna) odluka Exchange servera je shadow redundancy. Shadow redundancy je značajka koja služi za kopiranje poruka koje su trenutno u tranzitu na drugi Exchange server na drugom *site*-u. Također, značajke poput Safety-Net i Shadow Safety-Net kopiraju poruke koje su uspješno dostavljene u mailboxe, na mailbox bazu podataka u drugom *site*-u. Koristeći navedene značajke, osigurava se da se poruke ne izgube ukoliko dođe do ispada cijelog podatkovnog centra.

4.7. Testiranje failovera i switchovera između DAG grupa

Razliku između failovera i switchovera objasnio sam ranije a sada ću objasniti razliku između 3 tipa swithovera.

4.7.1. Database switchover

Database switchover je proces u kojem se trenutna aktivna mailbox baza unmounta, te druga kopija baze postaje aktivna. Ova situacija može se desiti unutar jednog podatkovnog centra ili između dva. Database switchover se može napraviti kroz Exchange Admin Center (EAC) ili kroz Powershell.

Cmdlet za prebacivanje baze je Move-Activemailboxdatabase.

```
[PS] C:\>  Move-Active-mailboxDatabase DB01 -ActivateOnServer ZG-EXCH01 -
MountDialOverride:None
```

MountDialOverride parametar služi kako bi otkazali aktivacije baze, sve dok se određeni broj transakcijskih logova ne replicira, odnosno dok se red čekanja (eng. *queue lenght*) ne smanji do određenog broja. Postoje 4 opcije:

- **None** – koristi se predefinirana opcija sa tog mailbox servera
- **GoodAvailability** – predefinirana vrijednost, baza će postati aktvina ako je queue lenght 6 ili manje
- **BestAvailability** – baza će postati aktivna ako je queue lenght 12 ili manje
- **Lossless** – baza će postati aktivna ako nema nedostajućih logova.

4.7.2. Server switchover

Server switchover je proces u kojem se sve aktivne baze koje su na jednom serveru unmountaju, te se aktiviraju na drugim serverima.

Cmdlet je sličan kao i kod database swithcovera, jedina je razlika što ne specificiramo bazu podataka.

```
[PS] C:\>  Move-Active-mailboxDatabase -ActivateOnServer ZG-EXCH01
```

4.7.3. Datacenter switchover

U *site*-resilient infrastrukturi moguć je automatski switchover, odnosno failover, međutim, kao što je prije navedeno, potrebne su barem 3 lokacije. Ako nemamo infrastrukturu sa 3 lokacije, aktivacije baza kroz 4 koraka, mora se ručno napraviti:

- Terminiranje djelomično aktivnog podatkovnog centra
- Potvrđivanje preduvjeta i ispravnosti rada sekundarne lokacije
- Aktivacija mailbox servera na sekundarnoj lokaciji
- Aktivacija servisa klijentskog pristupa za sekundarnu lokaciju

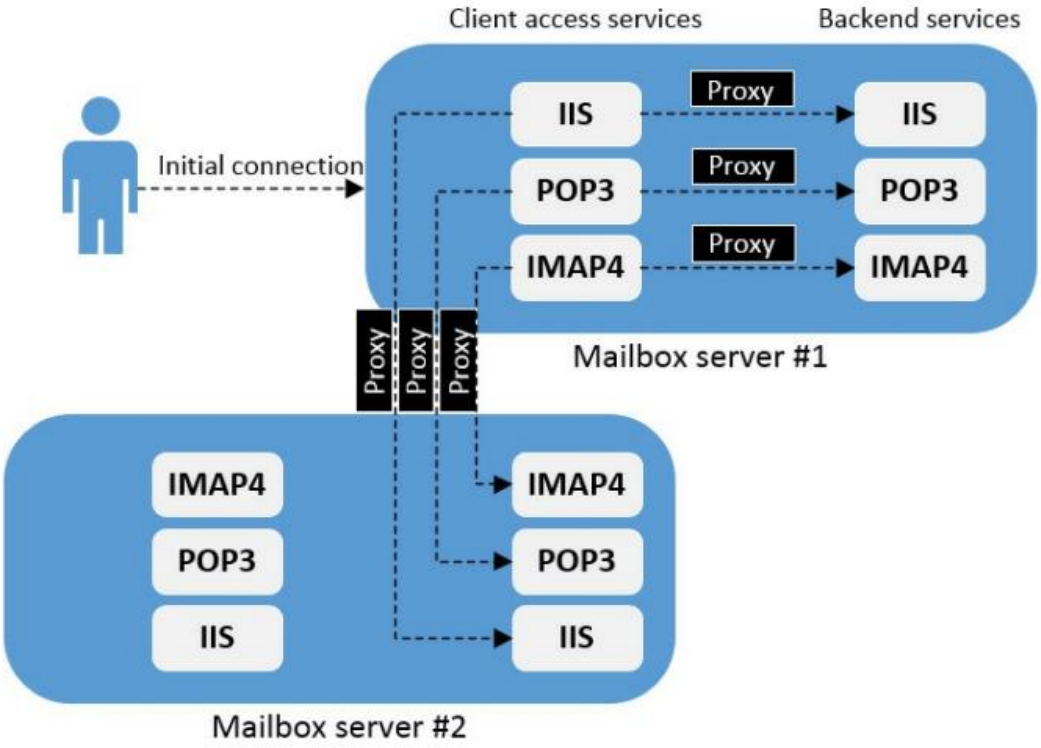
5. Visoka dostupnost servisa klijentskog pristupa

Uloga Exchange administratora je upravljanje raznim tehnologijama, od kojih, su neke (engl. *backend*), te takve nisu vidljive krajnjem korisniku. Na primjer diskovi, te njihova organizacija. Sa druge strane imamo (engl. *frontend*) tehnologije, koje krajnji korisnik primijeti u slučaju loše konfiguracije ili ispada rada. Na primjer, u slučaju isteka certifikata za klijentski pristup krajnji korisnik dobije grešku ili upozorenje u aplikaciji.

Servisi klijentskog pristupa uključuju sve tehnologije koje pružaju klijentima, odnosno krajnjim korisnicima, uslugu pristupa servisima povezanim sa Exchange serverom, najčešće e-mailom. Neke tehnologije su bitne za sve scenarije, na primjer, pravilno upravljanje certifikatima, dok su neke manje korištenije, ali ne i manje bitne (POP3 ili IMAP4).

5.1. Planiranje proxy-a

Budući da je mailbox rola zadužena za odrađivanje klijentskog pristupa, operacija *proxy* se također, dešava na serveru sa mailbox rolom. Pogledom na sliku (Slika 5.1), vidi se da bez obzira gdje se korisnikov mailbox nalazi, konekcija je uvijek *proxy*-rana prema backend servisima od strane servisa klijentskih pristupa (Client Access Services). Bez obzira na to, radi li se to na lokalnom ili na udaljenom serveru.



Slika 5.1 Rad *proxy-ranja* u Exchange-u 2016

5.2. Planiranje *site*-resilient imenskih prostora

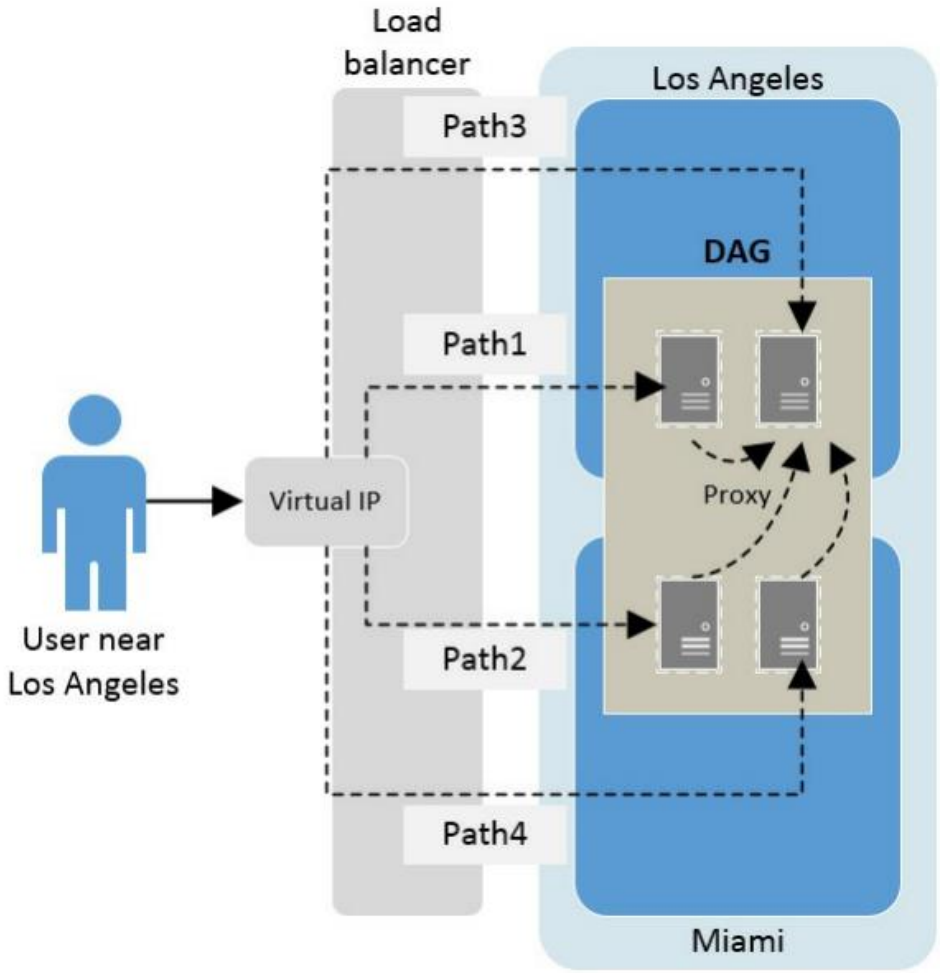
U prijašnjim verzijama Exchange-a bilo je potrebno konfigurirati nekoliko imenskih prostora, osobito za *site*-resilient slučajeve. U Exchange-u 2010, *site*-resilient konfiguracija imenskog prostora izgledalo bi ovako:

- mail.diplomski.hr - imenski prostor primarnog podatkovnog centra
- mail2.diplomski.hr - imenski prostor sekundarnog podatkovnog centra
- mailpri.diplomski.hr - redundantni imenski prostor za OWA u primarnom podatkovnom centru
- mailsec.diplomski.hr - redundantni imenski prostor za OWA u sekundarnom podatkovnom centru
- rpc.diplomski.hr - imenski prostor za RPC pristup u primarnom podatkovnom centru
- rpc2.diplomski.hr - imenski prostor za RPC pristup u sekundarnom podatkovnom centru
- mailsec.diplomski.hr – transportni imenski prostor
- autodiscover.diplomski.hr – imenski prostor za autodiscover

Osim brojnih imenskih prostora i kompleksnosti, bilo je potrebno konfigurirati certifikate za svaki od njih, što je činilo konfiguraciju klijentskog pristupa još kompliciranijom. Exchange 2013 je smanjio broj imenskih prostora na dva, te se takva konfiguracija koristi do današnjeg dana. Dva konfiguracijska imenska prostora su sljedeća:

- autodiscover.diplomski.hr
- mail.diplomski.hr

RPC se više ne koristi što je jedan od razloga smanjenja broja imenskih prostora. Drugi razlog je taj, što su klijentski zahtjevi proslijeđeni (engl. *redirected*) ili (engl. *proxied*) prema mailbox serveru, koji poslužuje aktivnu kopiju baze u kojoj se nalazi korisnikov mailbox. (Slika 3.1) prikazuje proces konekcije u slučaju jedinstvenog imenskog prostora koji se rasprostranjuje kroz dvije lokacije. Korisnik se može povezati na svoj mailbox koristeći četiri moguće putanje. U svakoj situaciji u kojoj korisnik napravi konekciju prema serveru koji ne sadrži njegov mailbox, ta konekcija se *proxy*-ra dalje do servera koji sadrži aktivnu kopiju baze u kojoj je mailbox.



Slika 5.2 Jedan imenski prostor sa četiri različite putanje kroz dvije lokacije

Kao što je i prije navedeno, zbog uporabe *proxya* više nije potrebno koristiti dva imenska prostora za svaku lokaciju (iako je u nekim situacijama bolje koristiti zasebne imenske prostore). Zaključno, *site*-resilient konfiguraciju se može postići na sljedeća dva načina:

Uporabom jednog imenskog prostora – Ovaj model je prikazan na slici (Slika 5.2). Nedostaci ovog modela su to što krajnji korisnici mogu imati bolje korisničko iskustvo ovisno o lokaciji s koje pristupaju servisu. Na primjer, ako je korisnik u blizini Los Angelesa, te ga *loadbalancer* preusmjeri na server koji je na Miami lokaciji, a njegov mailbox je na lokaciji u Los Angeles podatkovnom centru, konekcija je *proxy*-rana nazad u Los Angeles. U takvim situacijama je očito da će neki korisnici imati brži odziv od ovih iz navedenog primjera.

Uporabom dediciranog imenskog prostora po *site*-u – ovaj model veže korisnika za jedan site u kojem mu se nalazi mailbox, te koristi drugi site jedino u slučaju *failovera*.

5.3. Planiranje certifikata

Certifikati su kritična komponenta Exchange infrastrukture, te mogu znatno utjecati na korisničko iskustvo kada su pogrešno konfigurirani. Prilikom instalacije, kreirani su osobno potpisani (engl *self-signed*) certifikati, te su oni dostatni za pozadinske mailbox servise. Međutim, certifikati za klijentski pristup trebali bi biti izdani od treće strane (engl. *third party*), kako bi bili vjerodostojni. Može se reći da je planiranje certifikata povezano sa planiranjem imenskih prostora, zbog toga što su certifikati vezani za puno domensko ime ili FQDN (fully qualified domain name). Razlikujemo dva načina konfiguracije certifikata; jednostavni i kompleksni, a razlike su sljedeće:

- **Jednostavna konfiguracija** – koriste se samo dva FQDN-a, jedan za autodicover i jedan za sve ostalo, a oba FQDN-a može se povezati sa jednim certifikatom. U situacijama razdvojenog DNS-a, ova konfiguracija je poželjna.
- **Kompleksna konfiguracija** – koristi se više FQDN-ova. Postavlja se pitanje zašto bi netko koristio kompleksnu konfiguraciju? Kompleksna konfiguracija koristi se iz više razloga. Jedan od njih je nedostatak razdvojenog DNS-a ili korištenje više domenskih imena koja su vezana za fizičke geografske lokacije. Kod ove konfiguracije, potrebno je koristiti više certifikata, što zadaje mnogo više posla oko planiranja i održavanja.

Jedna od metoda za pojednostavljenje konfiguracije certifikata je korištenje univerzalnog (engl. *wildcard*) certifikata. Takav certifikat se može koristiti za sve FQDN-ove u domeni. Na primjer, može se koristiti certifikat *diplomski.com za sve pod-domene (mail-eu.diplomski.com, mail-us.diplomski.com, autodiscover.diplomski.com itd.). Problem kod ovog pristupa je sigurnosne prirode. U slučajevima neovlaštenog pristupa, napadač može iskoristiti univerzalni certifikat na svojoj malicioznoj stranici, te tako napraviti štetu organizaciji. Uzimajući u obzir sve navedeno, kod planiranja certifikata najbolje prakse bile bi sljedeće:

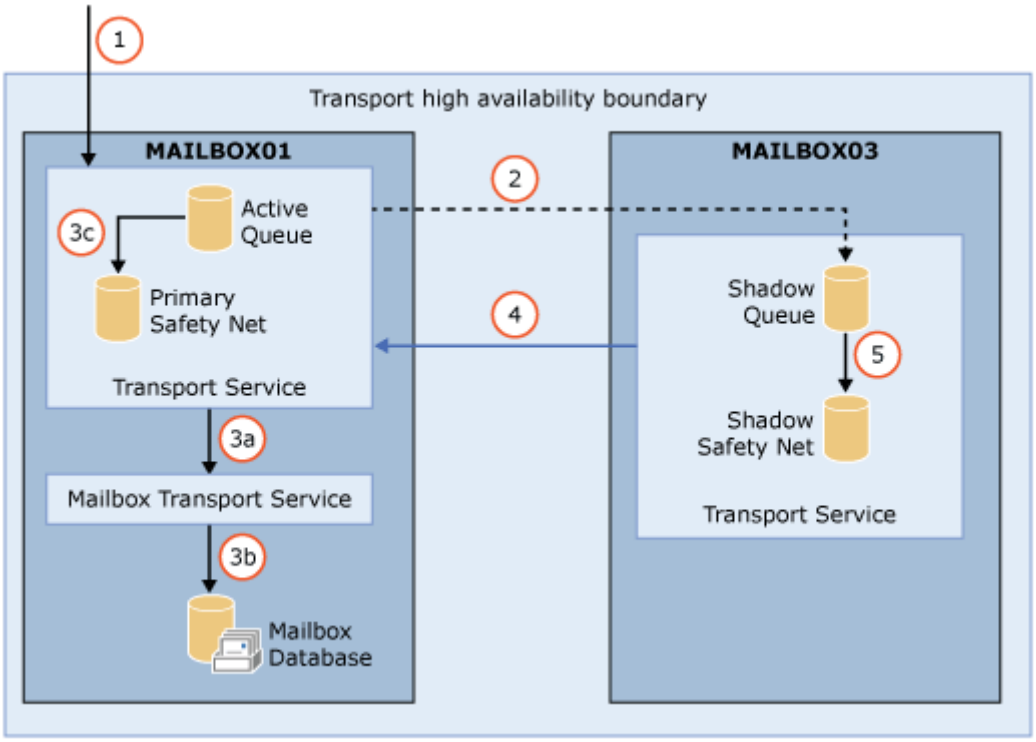
- Koristiti third party certifikate
- Jedan certifikat za sve (jednostavna konfiguracija)
- Koristiti certifikat koji ističe kroz tri do pet godina
- Koristiti certifikat koji podržava više domenskih imena

6. Visoka dostupnost transportnih servisa

Exchange administratori susreću se sa raznim tehnologijama, koje zajedno omogućuju kolaboracijske funkcionalnosti. Međutim, transportni servisi zaslužni su za promet poruka između komponenti, servera ili organizacija, te su stoga najbitniji dio cijele infrastrukture. U slučaju prekida rada transportnih servisa u trenutku slanja e-maila, taj e-mail bi bio izgubljen zauvijek da nema značajki visoke dostupnosti „Safety Net“ i „Shaddow redundancy“. Glavne značajke za poboljšanje visoke dostupnosti uključuju:

- Shadow redundancy kreira redundantnu kopiju poruke na drugom serveru prije nego što transportni servis prihvati poruku.
- Safety Net pohranjuje poruke koje je transportni servis uspješno procesirao na serveru sa mailbox rolom

Sljedeći dijagram (Slika 6.1) predstavlja pregled visoke dostupnosti transportnih servisa na Exchange serveru



Slika 6.1 Visoka dostupnost transportnih servisa

1) Mailbox server imena MAILBOX01 prima poruku od drugog SMTP servera

2) Prije nego što prihvati i potvrdi poruku, MAILBOX01 otvara SMTP konekciju na drugi mailbox server MAILBOX03, te taj server kreira kopiju poruke (engl. *Shadow copy*). Server MAILBOX01 je primarni server, a MAILBOX03 je (engl. *Shaddow server*)
3) Transportni servis na MAILBOX01 procesira primarnu poruku
    a. Na ovom primjeru korisnikov mailbox je lociran na serveru MAILBOX01, stoga transportni servis prenosi poruku do lokalnog Mailbox Transport servisa.
    b. Mailbox Transport servis dostavlja poruku u lokalnu mailbox bazu podataka.
    c. MAILBOX01 izrađuje notifikaciju namijenjenu MAILBOX03 serveru o uspješnoj isporuci poruke, te premješta poruku u lokalni Primary Safety Net
4) MAILBOX03 periodično ispituje primarni server o notifikaciji za uspješnu isporuku poruke.
5) Nakon što MAILBOX03 utvrdi postojanje notifikacije o uspješnoj isporuci poruke, premjesti shadow poruku u Shadow Safety Net

Poruka je zadržana u primarnom i *shadow* Safety Net spremniku, ovisno o konfiguriranoj opciji. Ukoliko se desi ispad servera, odnosno failover, primarni Safety Net ponovno pošalje poruku, a u slučaju da MAILBOX01 nije dostupan, isto odradi Shadow Safety Net na serveru MAILBOX03.[1]

6.1. Shadow Redundancy

Značajka iz naslova se prvi puta pojavljuje u Exchange verziji 2010, a glavna joj je zadaća bila redundantno kopiranje poruka u tijeku prije nego li su isporučene u korisnikov mailbox. Na Hub Transport serveru postojala je baza poruka koje su u protoku, te se zbog ove značajke poruke nisu brisale sve dok nije došla potvrda od sljedećeg servera u lancu o uspješnoj isporuci. Ukoliko potvrda nije isporučena, Hub Transport Server je ponovno poslao poruku. S obzirom da u Exhcnage 2016 infrastrukturi, ne postoji Hub Transport rola, već servis, ovaj proces se odvija na serveru sa mailbox rolom. Međutim, poruka se redundantno kopira, prije nego li se verificira primatelj poruke.

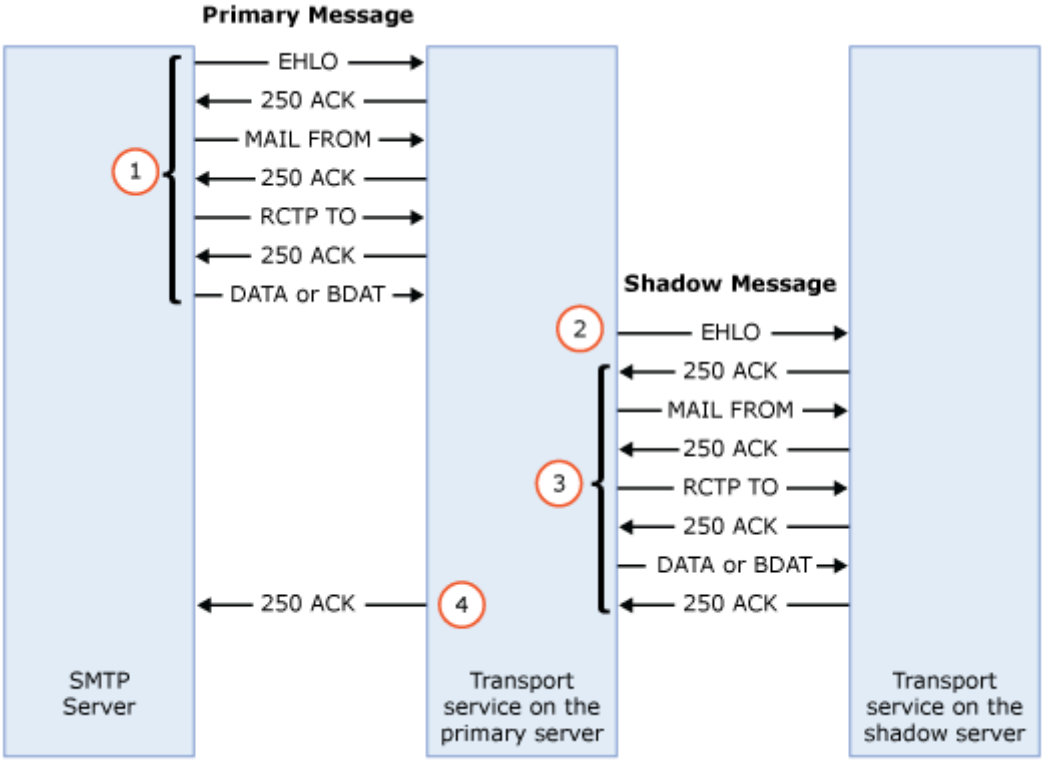
[1]https://docs.microsoft.com/en-us/exchange/mail-flow/transport-high-availability/transport-high-availability?view=exchserver-2019

“Shadow Redundancy” je predefinirano aktivirana opcija, međutim, da bi bila funkcionalna, potrebno je imati više mailbox servera u infrastrukturi. Ukoliko mailbox server nije dio DAG-a, drugi mailbox server mora biti unutar iste lokacije (engl. site), a kada se koristi DAG, onda se redundanta poruka kreira na udaljenoj lokaciji.

Značajka se može aktivirati ili deaktivirati sljedećim cmdletom:

```
Set-TransportConfig -ShadowRedundancyEnabled $true/$false
```

Glavni cilj Shadow Redundancy-a je dupliranje svake poruke u tranzitu unutar granica visoke dostupnosti. Gdje je i kako poruka kopirana, ovisi o tome odakle je poruka došla i gdje joj je sljedeća destinacija. U slučaju kada poruka dolazi izvan granica visoke dostupnosti (DAG ili AD site kod rješenja bez korištenja DAG-a), mailbox server procesira poruku na jednak način, bez obzira na to iz kakvog je okruženja server pošiljatelj odakle je pristigla poruka, te je li pristigla iz visoko dostupnog okruženja. Mailbox server će napraviti redundantnu kopiju poruke sve dok je ova značajka aktivirana, te ju poslati na drugi server (shadow server), prije nego li potvrdi primatelja poruke serveru pošiljatelju. Slika 6.2 prikazuje način rada ovog procesa.



Slika 6.2 Proces dupliranja poruka

1) Server pošiljatelj (SMTP Server na slici) otvara SMTP konekciju prema transport servisu na primarnom mailbox serveru.
2) Dok je sesija između SMTP servera i primarnog servera još uvijek aktivna, primarni server otvara SMTP sesiju prema transport servisima na shadow serveru, kako bi kreirao redundantnu kopiju poruke. Razlikujemo dva slučaja kod odabira shadow servera:
    a. U slučaju kada je primarni server dio DAG-a, odabrani shadow server je unutar istog DAG-a, ali preferirano na drugoj lokaciji. Ova se opcija može podesiti parametrom *ShadowMessagePreference* u naredbi Set-TransportService, te osim predefinirane opcije (*PreferRemote*), mogu se koristiti još *RemoteOnly* i *LocalOnly*
    b. Kada primarni server nije dio DAG-a, shadow server mora biti unutar iste AD lokacije.
3) Primarni server kopira poruku na transport servis na udaljenom mailbox serveru, te udaljeni server potvrđuje primitak poruke koja tada postaje shadow poruka.
4) Nakon što je shadow server obavijestio primarni server o primitku poruke, SMTP sesija prema SMTP serveru pošiljatelju se zatvara.

Tijekom pokušaja kreiranja redundantne kopije, može doći do timeout-a između primarnog i shadow servera ili primarnog i servera pošiljatelja. U slučaju timeout-a prije kreiranja shadow poruke, poruka se može procesirati bez obzira na timeout ili primarni server može odbiti procesiranje poruke, ovisno o opciji definirana parametrom RejectMessageOnShadowFailure ($True/ $False) naredbom Set-TransportConfig.

Nakon što je shadow poruka kreirana, rad shadow redundancy-a tek počinje. Primarni i shadow server moraju ostati u kontaktu kako bi se nadzirao status poruke. Primarni server dobije potvrdu od sljedećeg servera u lancu da je poruka uspješno dostavljena, te potom ažurira „Discard status“ listu. „Discard status“ je poruka koja sadrži zapise stanja redundantnih poruka koje se nadziru. Ukoliko je poruka uspješno dostavljena, redundantna kopija se više ne treba čuvati u „shadow redundancy-u“, te je premještena u „Safety Net“, a više o tome objasnit ću u sljedećem poglavlju. Shadow server periodično otvara SMTP sesiju prema primarnom serveru, kako bi saznao informacije o statusima nadziranih redundantnih poruka, te kao odgovor dobije „Discard status“ poruku, ovisno o sadržaju, ažurira svoj *shadow queue*. „Discard status“ poruke su pohranjene na disku, kako bi ostale

nepromijenjene u slučaju ispada servera, što se ne bi ostvarilo da su pohranjene u memoriji.[13]

6.2. Safety Net

Ova značajka je prvi put predstavljena u verziji Exchange 2007 pod imenom „*dumpster*“, a od verzije Exchange 2013 zove se Safety Net.

Za razliku od Shadow Redunancy-a, značajki koja čuva kopije poruka u tranzitu, Safety Net je zaslužan za očuvanje redundantnih kopija e-mailova koji su uspješno procesirane i poslane u mailbox bazu podataka. Safety Net proces počinje gdje Shadow Redunandcy završava. Zamislimo situaciju u kojoj imamo DAG sa dva servera, a aktivna kopija sa novim porukama se još nije replicirala na pasivnu u trenutku kada server sa aktivnom kopijom iznenadno postane nedostupan. Kada bi aktivirali, do tada pasivnu bazu, nove poruke bile bi izgubljene. Safety Net omogućuje ponovno slanje poruka na pasivnu bazu.

Primarni „Safety Net“ se nalazi na mailbox serveru, čiji je transportni servis procesirao primarnu poruku. To može značiti da je poruka dostavljena na Mailbox Transport Delivery servis na destinacijskom mailbox serveru ili je prenesena (engl. *relayed*) kroz „Hub“ lokaciju prema destinaciji. Nakon što primarni server procesira primarnu poruku, poruka je premještena iz čekanja isporuke u primarni Safety Net na istom serveru. Shadow Safety Net se nalazi na Shadow serveru. Nakon što shadow server dobije potvrdu da je primarni server uspješno poslao poruku, shadow poruka se premješta iz shadow čekanja u Shadow Safety Net. Poruka se čuva u Safety Netu ovisno o parametru *SafetyNetHoldTime*, a predefinirana vrijednost je 2 dana.

6.2.1. Ponovno slanje poruka iz Safety Net-a

Komponenta „Active Manager“ koja je dio MRS-a (Microsoft Exchange Replication Service) zadužena je za upravljanje DAG-om i kopijama baza podataka, kao i za ponovno slanje poruka iz Safety Neta. Postoje dva scenarija u kojima se dešava ponovno slanje poruka:

- Nakon automatskog ili ručnog failover-a mailbox baza podataka u DAG-u
- Nakon aktivacije zakašnjele mailbox kopije baze podataka

Zakašnjela kopija (engl. *Lagged database copy*) je pasivna kopija baze koja ne sadrži najnovije promjene, zbog toga što je odgođena replikacija. Glavni preduvjet za uspješno ponovo slanje poruka je da je vrijeme zadržavanja poruka u Safety Netu dulje od najstarije poruke koja još nije replicirana.

6.2.2. Ponovno slanje poruka iz Shadow Safety Net-a

Ponovno slanje poruka iz Shadow Safety Neta-a je kao i kod Safety Neta-a potpuno automatizirano i ne zahtijeva nikakve administratorske radnje. Sljedeći scenarij opisuje interakciju prethodno spomenutih značajki tijekom ponovnog slanja poruke:

1) „Active Manager“ zatraži ponovno slanje poruka iz Safety Net-a za određeni vremenski interval (na primjer od 13 do 16 sati). Međutim, Mailbox server koji sadrži primari Safety Net je imao neplanirani ispad, te „Active manager“ neuspješno pokušava kontaktirati primarni server sljedećih 12 sati.
2) Nakon 12 sati, „Active Manager“ šalje upit svim mailbox serverima u granicama visoke dostupnosti u potrazi za Safety Net-om koji sadrži zatražene poruke u vremenskim intervalima od 13 do 16 sati. Shadow Safety Net odgovori na upit, te ponovno šalje poruke.

Kada Shadow Safety Net odgovori na upit, poruke koje su ponovno poslane su samo određene poruke iz zadane mailbox baze podataka u zatraženom vremenskom intervalu. Spomenuta ograničenja sprječavaju neke od potencijalnih problema sa ponovnim slanjem poruka koje su već poslane ili sa pretjeranom iskorištavanjem serverskih resursa. Neke od bitnih značajki poruka koje su pohranjene u Shadow Safety Net-u su[13]:

- Shadow Safety Net nema informaciju o tome gdje je primarni server poslao poruku
- Shadow Safety Net sadrži samo informacije iz omotnice originalne poruke, te nema informacije o stvarnim primateljima poruke (u slučaju kad je primatelj distribucijska grupa koja zahtjeva ekspanziju primatelja)

7. Sigurnost i usklađenost Exchange infrastrukture

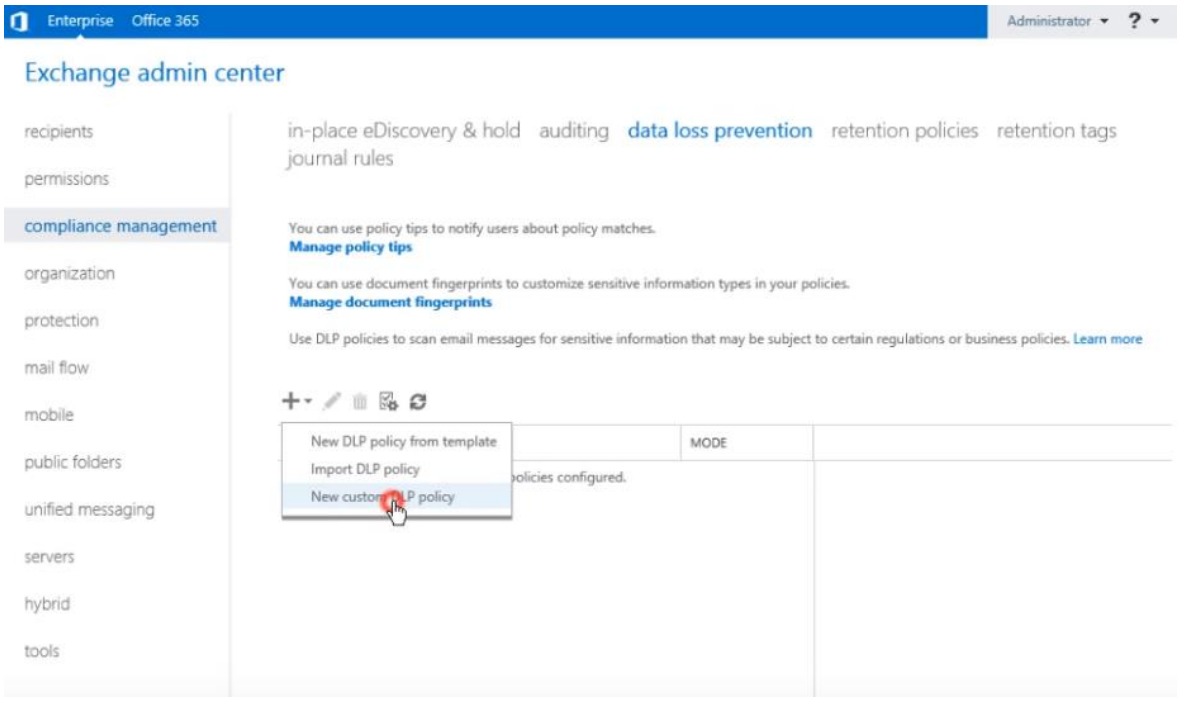
7.1. DLP rješenja

„Data Loss Prevention“ ili DLP je jedna od značajki Exchange servera koja omogućuje ili sprječava namjerno ili ne namjerno izlaganje povjerljivih informacija, kao što su osobni podaci ili podaci bankovnih računa koji se ne bi smjeli slati preko poruka. DLP koristi mehanizam koji analizira sadržaj poruke i privitaka poruka. Pravila koja definiramo ovom značajkom zovu se DLP politike, te ukoliko poslana poruka „izazove“ (engl. *triggers*) politiku, ona se može ponašati na tri načina:

- Zabilježena u logove, bez dodatnih akcija
- Korisniku se prilikom pisanja poruke može pojaviti upozorenje
- Poruka može biti potpuno blokirana

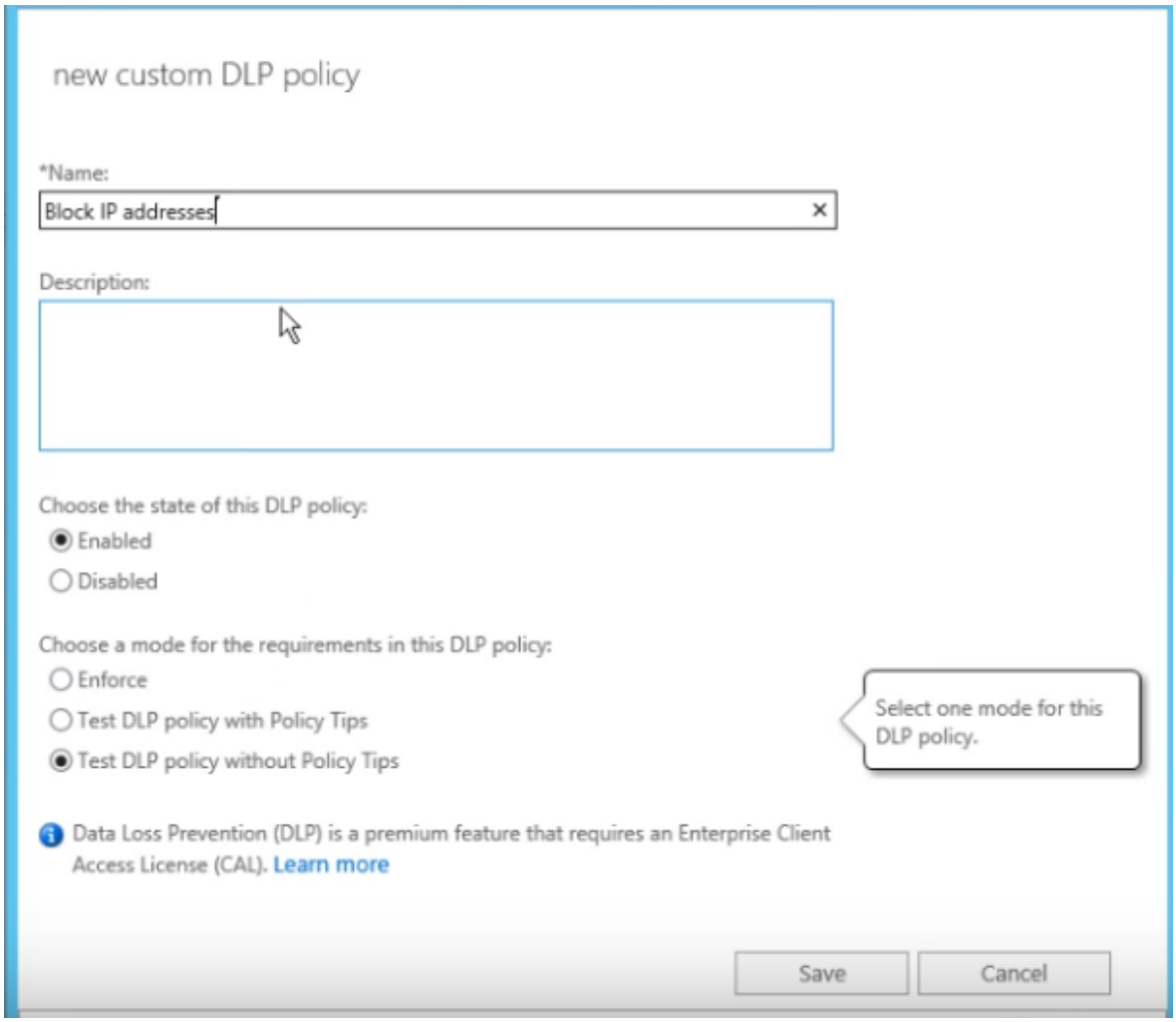
Sustav prepoznaje osjetljive informacije na temelju uzorka regularnih ekspresija u kombinaciji sa ključnim riječima i postotkom poklapanja sa uzorkom. Na primjer, brojevi kreditnih kartica su 16-znamenkasti, međutim sustav neće označiti svaki 16-znamenkasti string kao osjetljivu informaciju. Kako bi se sa sigurnošću moglo utvrditi radi li se o kreditnoj kartici, sustav će provjeriti jesu li brojevi odvojeni razmacima ili povlakama, te je li u blizini znamenki datum koji označava istek kartice. Također, ključne riječi poput „VISA“ ili „AMEX“ ulaze u kombinaciju provjere. Ukoliko se bilo koja od navedenih provjera uspostavi točnom, za svaku se podiže skor. Što je skor veći, to je veća vjerojatnost da se radi o podacima kreditne kartice.[2]

Za kreiranje DLP politiku, na „Exhange admin centar“ konzoli mora se otići pod „Complience management“ i zatim „Data loss policy“ kao što prikazuje slika 7.1. Na padajućem izborniku „Add“ ikone, imamo opciju kreiranja DLP politike iz predloška ili kreirajne nove politike.



Slika 7.1 Prikaz kreiranja DLP politike u Exchange admin centru

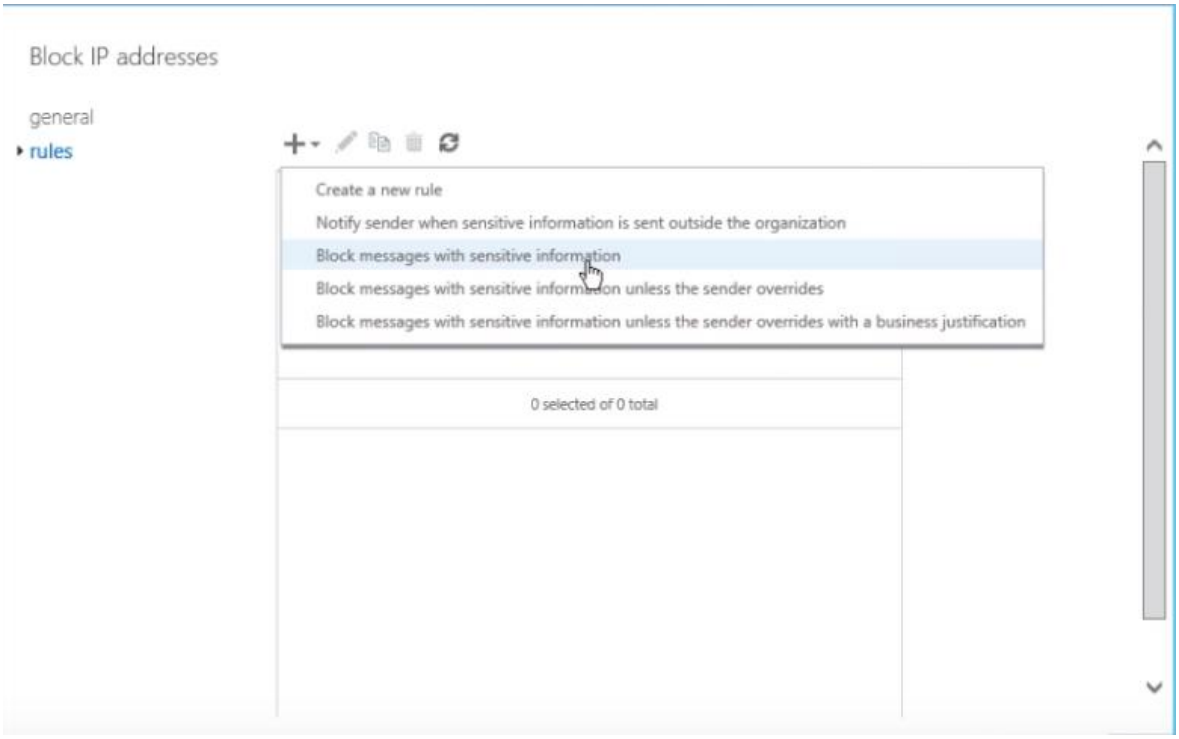
Na novootvorenom prozoru upisuje se ime politike, status, te način rada. Politiku se može prisilno primijeniti, ali ju može se i testirati pomoću „Policy Tips“. Ta opcija upozorava korisnika o osjetljivim podacima u sadržaju e-maila. U praksi bi se politika testirala pomoću „Policy Tips“ opcije, te prisilno primjenjivala nakon što zadovolji potrebe organizacije. Ostala konfiguracija parametara odrađuje se nakon kreirajna same politike.



Slika 7.2 Prikaz prozora „New custom DLP policy“

Nakon što je DLP politika kreirana, konfigurira se dvoklikom na nju. Primjećuje se da se pojavio novi konfiguracijski dio „Rules“. To je skup pravila koje se može individualno konfigurirati i svrstati pod istu politiku. U praksi, kod globalnih organizacija, DLP politike se segmentiraju po državi ili regiji. Potom se unutar njih, kreiraju prilagođeni rulovi iz razloga što identifikacijski brojevi (poput OIB-a ili sl.) se u većini država, razlikuju po strukturi. Odabirom „Block messages with sensitive information“ otvorit će se novi prozor na kojem može se podesiti parametre prema kojima će se ponašati „rule“ unutar politike. Kreiranje rulova ovisi o tome koja vrsta podataka se smatra klasificiranom unutar organizacije. Primjer sa slike 7.4 prikazuje politiku koja blokira slanje klasificiranih podataka, u ovom slučaju IP adresa. Postoje razni predefinirani uzorci prema kojima politika blokira slanje informacija. Neki od njih su: ABA Routing Number, Credit Card Number, International Banking Account Number (IBAN), IP Address, SWIFT Code, Taiwan

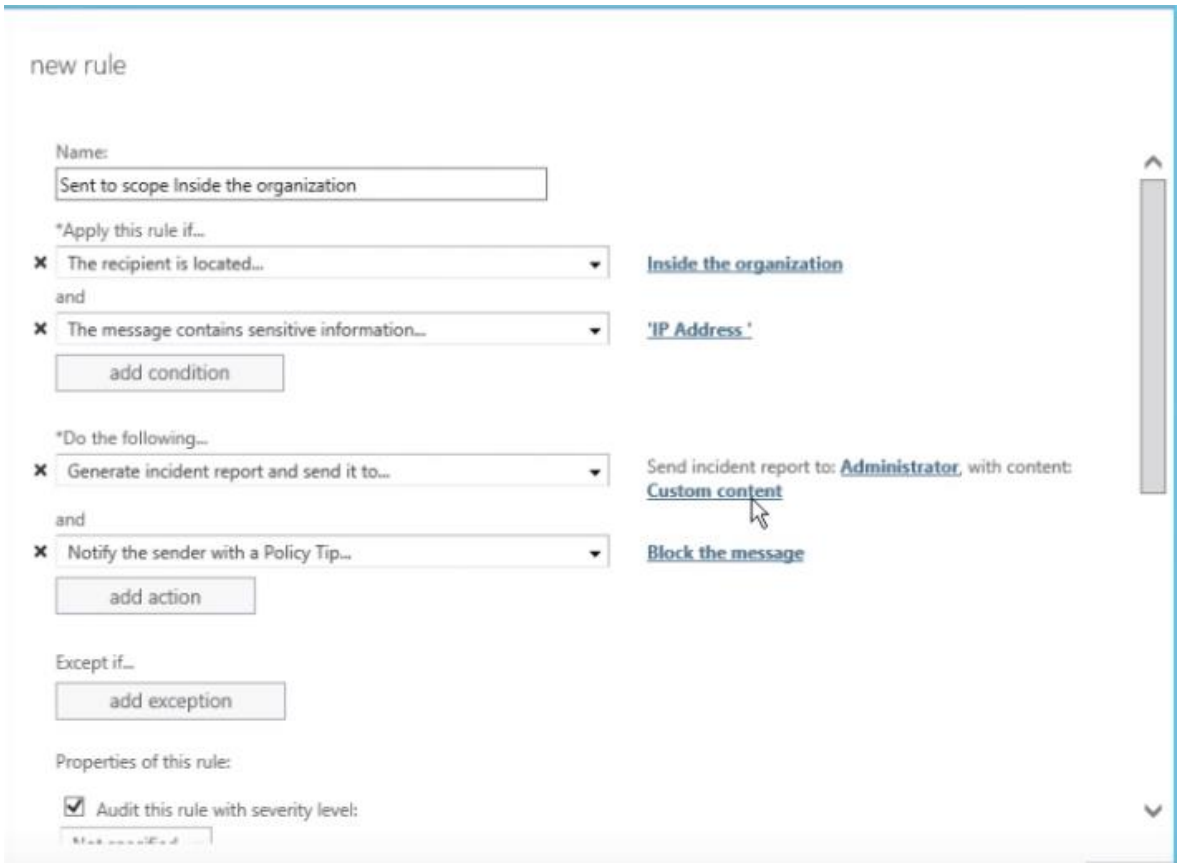
National ID, Taiwan Passport Number, U.K. Driver's License Number, U.S. Social Security Number (SSN) i brojni drugi.



Slika 7.3 Odabir opcije „Block messages with sensitive information“

Kod otvaranja novog prozora mogu se odabrati upravo spomenute uzorke, te odabrati što želimo napraviti kada se ispuni odabrani uvjet. Rule se može konfigurirati sa opcijom overide, a u tom slučaju pošiljatelj može zanemariti upozorenje i nastaviti sa slanjem poruke. Overide se može konfigurirati tako da u predmet poruke upišemo ključnu riječ, te dodamo u „except if“ polje.

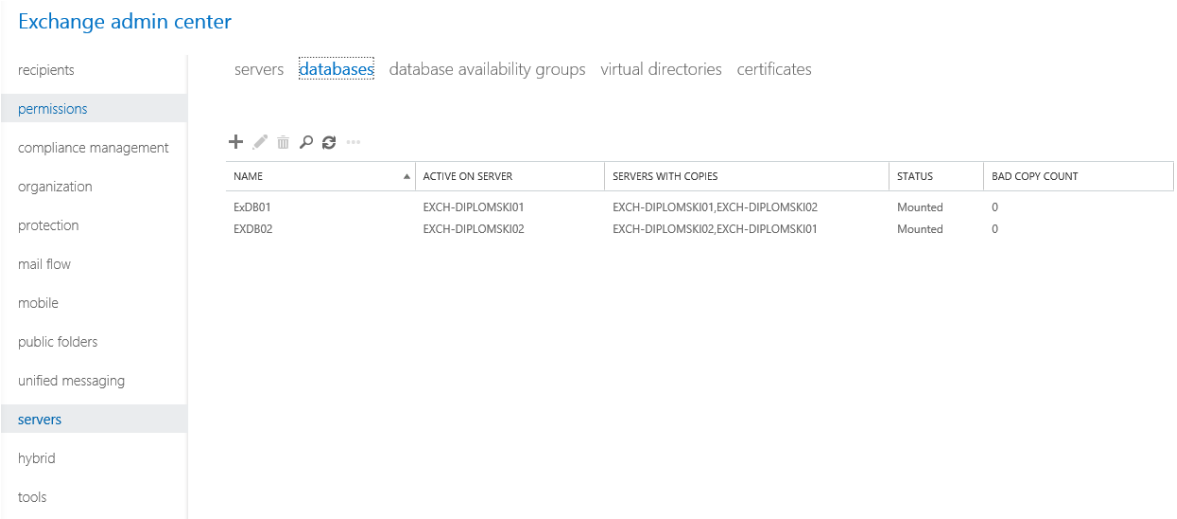
DLP politike se mogu koristiti za identifikaciju, monitoriranje i zaštitu klasificiranih informacija. Njihova svrha je uskladiti zaposlenike (koji rade sa klaisficiranim informacijama) sa definiranim pravilima, ali bez da se ometa njhov rad. U tom slučaju koriste se „Policy Tips“, koji podižu svijest i educiraju zaposlenike o politikama organizacije.



Slika 7.4 Izgled finalne DLP politike

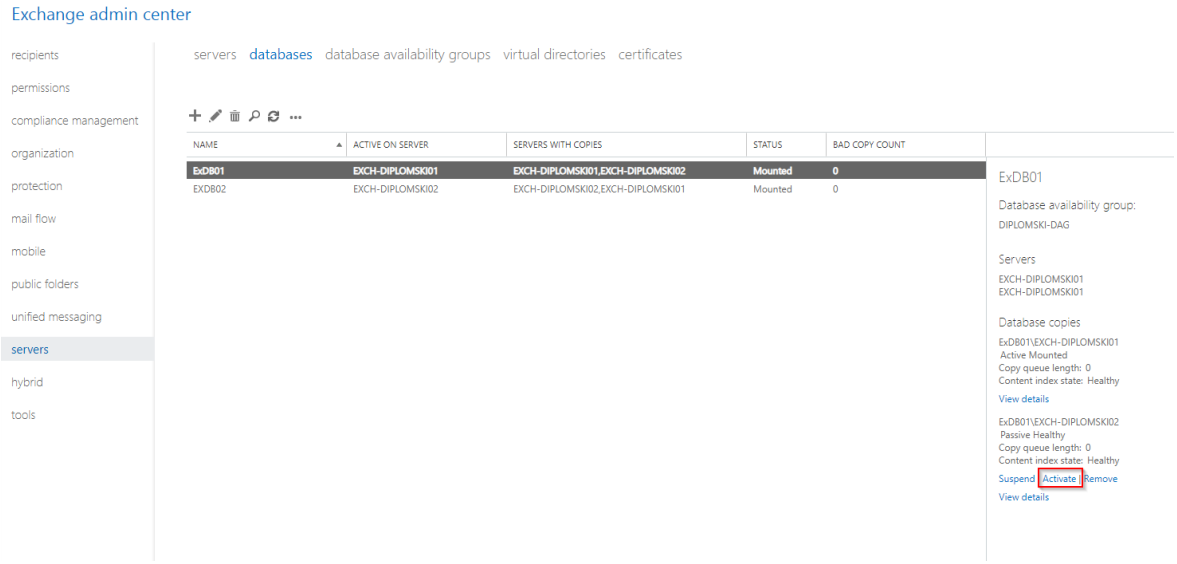
8. Testiranje visoke dostupnosti

U nastavku će se na primjeru opisati kako funkcionira database switchover, odnosno što se dešava ukoliko server sa mailbox rolom postane nedostupan. U scenariju, Exchange infrastruktura se sastoji od dva Exchange servera, te dvije mailbox baze. Na svakom od servera je akrivna jedna mailbox baza, dok je druga baza u pasivnom modu. Testni mailbox se nalazi na bazi ExDB02.



Slika 8.1 Pregled statusa baza

Kako bi se testirao failover, odnosno swithcover, aktiviranjem pasivne kopije baze ExDB01 (koja je trenutno aktivna na serveru **EXCH-DIPLOMSKI01)** na serveru **EXCH-DIPLOMSKI02** simulira se ispad servera **EXCH-DIPLOMSKI01** na kojem se nalazi testni mailbox**.** Za aktivaciju pasivne baze potrebno je u EAC konzoli kliknuti na Activate, kao što prikazuje slika 8.2.



Slika 8.2 Aktivacija pasivne baze

Prije nego što se aktivira baza, napravit će se test slanjem e-maila, te izmjeriti koliko je vremena potrebno e-mailu da se dostavi u normalnim uvjetima, te usporediti sa vremenom potrebnim u situaciji failovera. Kako bi se vidjelo koliko je vremena potrebno e-mailu da se isporuči, uzet će se zaglavlje e-mail poruke, te se kopirati u Microsoftov online servis – Message Header Analyser. Prema zaglavlju, u normalnim uvjetima potrebno je manje od sekunde da se poruka isporuči.

Summary

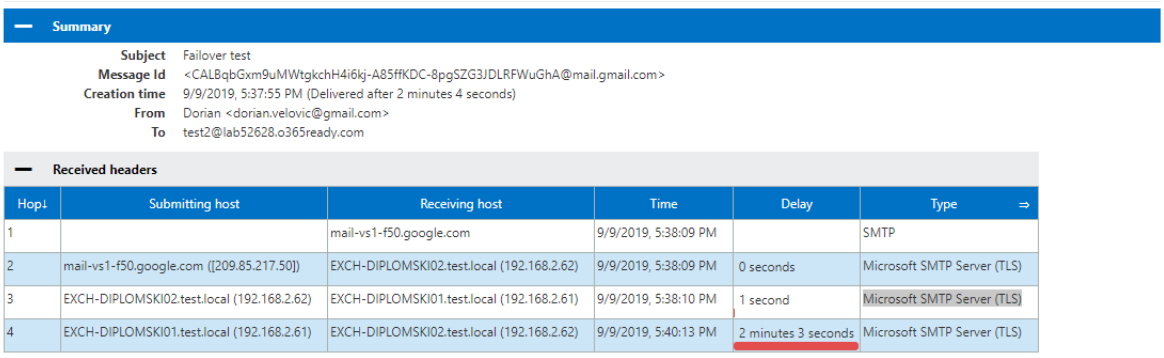
Subject Test
Message Id <CALBqbGxN-HdW9PAfg=dEy9eE77dCFtLEP2LNN-=1etyE8wheVQ@mail.gmail.com>
Creation time 9/9/2019, 5:06:24 PM (Delivered after -2 seconds)
From Dorian <dorian.velovic@gmail.com>
To test2@lab52628.o365ready.com

Received headers

Hop↓	Submitting host	Receiving host	Time	Delay	Type ⇒
1		mail-ua1-f53.google.com	9/9/2019, 5:06:37 PM		SMTP
2	mail-ua1-f53.google.com (209.85.222.53)	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	9/9/2019, 5:06:34 PM	-3 seconds	Microsoft SMTP Server (TLS)
3	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	9/9/2019, 5:06:34 PM	0 seconds	Microsoft SMTP Server (TLS)
4	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	9/9/2019, 5:06:35 PM	1 second	Microsoft SMTP Server (TLS)

Slika 8.3 Analiza zaglavlja poruke

Sada će se provjeriti kolko je poruci potrebno da se dostavi, kada u trenutku slanja iste, baza bude u stanju aktivacije na drugi node.



Summary

Subject	Failover test
Message Id	<CALBqbGxm9uMWtgkchH4i6kj-A85ffKDC-8pgSZG3JDLRFWuGhA@mail.gmail.com>
Creation time	9/9/2019, 5:37:55 PM (Delivered after 2 minutes 4 seconds)
From	Dorian <dorian.velovic@gmail.com>
To	test2@lab52628.o365ready.com

Received headers

Hop	Submitting host	Receiving host	Time	Delay	Type
1		mail-vs1-f50.google.com	9/9/2019, 5:38:09 PM		SMTP
2	mail-vs1-f50.google.com ([209.85.217.50])	EXCH-DIPLOMSKI02.test.local (192.168.2.62)	9/9/2019, 5:38:09 PM	0 seconds	Microsoft SMTP Server (TLS)
3	EXCH-DIPLOMSKI02.test.local (192.168.2.62)	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	9/9/2019, 5:38:10 PM	1 second	Microsoft SMTP Server (TLS)
4	EXCH-DIPLOMSKI01.test.local (192.168.2.61)	EXCH-DIPLOMSKI02.test.local (192.168.2.62)	9/9/2019, 5:40:13 PM	2 minutes 3 seconds	Microsoft SMTP Server (TLS)

Slika 8.4 Analiza zaglavlja poruke u situaciji failovera

Vidi se da je poruci u trenutku failovera bilo potrebno 2 minute i 3 sekunde da se isporuči na mailbox servis, te konačno u korisnički mailbox. Uzimajući u obzir da se u praksi tolerira kašnjenje mailova do 10 minuta. Ovaj rezultat je pozitivan te dokazuje koncept aktivacije baza u prihvatljivom intervalu. U produkcijskoj okolini rezultati bi mogli biti drugačiji zbog količine podataka u mailbox bazama.

9. Testiranje sigurnosti

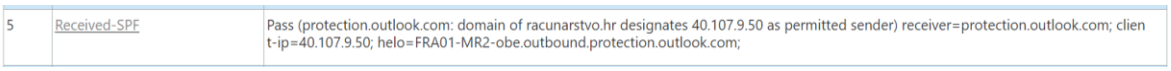
U nastavku će se testirati sigurnost Exchange-a uporabom SPF (eng. Sender Policy Framework) koji je oformljen kao standard 2014. godine pod IETF-om. SPF zapis je DNS zapis tipa TXT koji se dodaje u domensku zonu (SMTP domenu). U zapisu su defirnirane IP adrese, spektar adresa ili domenskih imena koje su autorizirane za slanje e-mailova sa te domene. Sljedeća slika prikazuje kako izgleda SPF zapis



Slika 9.1 Primjer SPF DNS zapisa

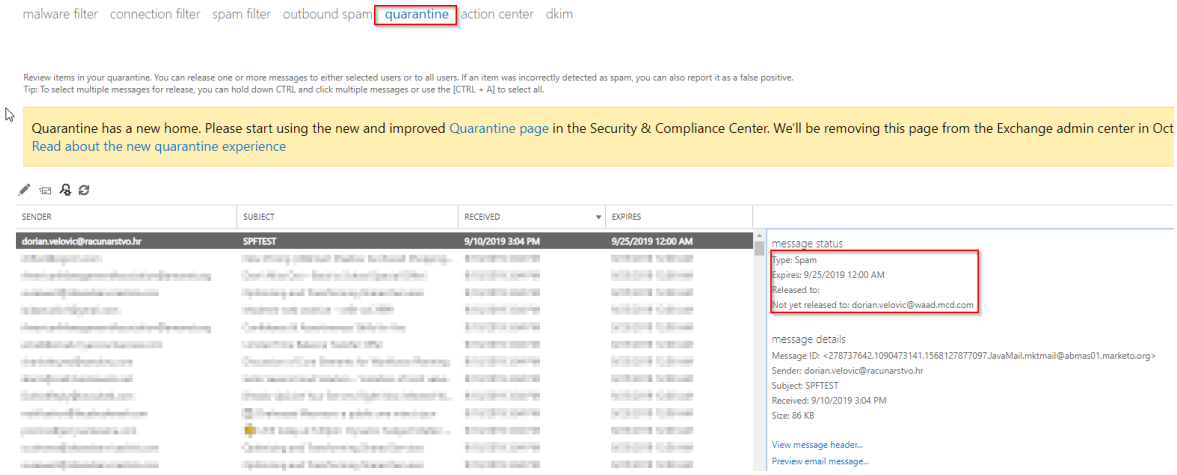
SPF-a se predefinirano provjerava prilikom svakog maila u Exchange Online Protection subskripciji te se se dešava u trenutku kada e-mail server dobije poruku. Također, provjera se može napraviti pomoću transportnog rula. SPF provijera funkcionira na način da na temelju polja „envelope from“ u zaglavlju e-maila, mail server radi DNS TXT upit prema toj domeni, te ukoliko kao rezultat dobije adresu s koje je poslan taj mail, označuje poruku kao SPF=pass. Ukoliko IP adresa s koje je mail došao nije na listi IP adresa u SPF zapisu, poruka se označuje kao SPF=fail, te se na temelju te informacije poruka može smjestiti u karantenu, izbrisati ili dostaviti u mailbox primaoca.

Za potrebe testiranja poslat će se legitiman e-mail na sustav u kojem je implementiran Exchange Online Protection. U headeru poruke se jasno vidi da je SPF test prošao te je poruka dostavljena.



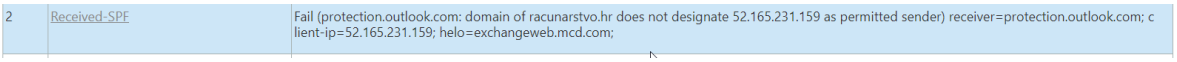
Slika 9.2 Uspješni SPF test

Kako bi se demonstrirao neuspješni SPF test, poslat ću e-mail sa SMTP relay-a, te će se kao pošiljatelja staviti adresa sa domene racunarstvo.hr. Dostavljena poruka je završila u karanteni sa razlogom SPAM kao što prikazuje sljedeća slika 9.3.



Slika 9.3 Prikaz poruke u karanteni

Kada se ode na „View message header“ može se vidjeti i jedan od razloga zašto je poruka završila u karanteni kao što prikazuje slika 9.4.



Slika 9.4 Neuspješni SPF test

10. Izbor između Exchange on-premise i Exchange Online

Mnogim organizacijama e-mail je primarni način komunikacije, te je stoga posjedovanje messaging platforme je neizbježno. Sa sve većom prisutnošću oblaka (eng. Clouda), mnoge organizacije svoje poslovanje okreću u tom smjeru. No, je li to zbilja isplativo? Na tu odluku utječu mnogi parametri kao i veličina organizacije. Jedan od glavnih razloga prebacivanja u cloud je trošak licenci i hardware-a. Za manje firme (do 100 korisnika), potrebna su barem dva fizička servera sa 2 x 1TB RAID 1 podatkovnog prostora, cijene oko 100 000,00 kn. Također, za servere treba kupiti licence, jer Exchange radi samo na Windows server operativnom sustavu. Takve licence koštaju oko 5000,00 kn svaka. Licenca za svakog usera (CAL) košta oko 400,00 kn po korisniku, a za standardnu verziju Exchange-a oko 5000,00 kn. Na Exchange mora biti implementiran certifikat koji košta oko 500,00 kn godišnje. Svu tu opremu potrebno je napajati, ali ću to izostaviti za potrebe ove usporedbe. Osim troškova za infrastrukturu servere je potrebno održavati. Pod održavanje spadaju mjesečne zakrpe i razne instalacije novih verzija sustava (eng. upgrade). Takvi zahvati mogu biti kompleksni, te ukoliko se ne izvode pravilno, utječu na pouzdanost sustava.

Sa druge strane, cloud rješenje umanjuje sve navedene brige. Licenca za svakog usera u Exchange Online Plan 1 rješenju košta oko 20,00 kn mjesečno. Drugi benefit je taj što se ne mora brinuti o kupnji hardware-a i licenci. Pouzdanost je još jedna stavka o kojoj ne mora voditi briga jer Microsoft garantira 99,99% dostupnosti servisa. U Exchange Online okruženju, briga oko ažuriranja i instalaciji novih verzija sustava je na pružatelju usluge. S obzirom da je Exchange Online produkt baziran na pretplati, dodavanje i brisanje korisnika ne zahtjeva dodatne naplate, dok u on-premise okruženju to nije slučaj. Uzmimo za primjer organizaciju koja iznenada počne loše poslovati, te izgubi velik broj zaposlenika. U tom se slučaju njihove licence ne mogu vratiti. U nastavku je tablica izračuna troška i usporedbe dviju navedenih načina implementacije messaging platforme za organizacije. Vidljivo je da je on-prem rješenje u prednosti tek sa više od 500 korisnika, uz napomenu da u izračun nije uključena električna energija, te bi u realnoj situaciji ta brojka bila puno veća.

##############################	50 Cloud	50 on-prem	100 Cloud	100 on-prem	500 Cloud	500 on-prem	1000 Cloud	1000 on-prem
Exchange online plan 1 (5 godina)	6,000.00	-	120,000.00	-	600,000.00	-	1,200,000.00	-
Broj servera	-	2.00	-	2.00	-	3.00	-	4.00
Broj baza po serveru	-	2.00	-	2.00	-	4.00	-	4.00
Trošak hardwarea	-	100,000.00	-	100,000.00	-	200,000.00	-	250,000.00
Windows server licence	-	10,000.00	-	10,000.00	-	15,000.00	-	20,000.00
Exchange licence	-	5,000.00	-	5,000.00	-	10,000.00	-	10,000.00
Exchange CAL	-	20,000.00	-	40,000.00	-	200,000.00	-	400,000.00
Exchange certifikati - godišnje	-	500.00	-	500.00	-	500.00	-	500.00
Ukupno nakon 5 godina	6,000.00	137,500.00	120,000.00	157,500.00	600,000.00	427,500.00	1,200,000.00	682,500.00
Mjesečno	100.00	2,290.00	2,000.00	2,625.00	10,000.00	7,125.00	20,000.00	11,375.00

Tablica 110.1 Izračun troška u kunama

Zaključak

Microsoft Exchange Server 2016 je skalabilna platforma za razmjenu e-mail poruka, koja dokazuje da Microsoft i dalje pruža rješenja korisnicima koji radije posjeduju on-premise rješenje. Jedna od njegovih najvećih prednosti je mogućnost održavanja sustava sa 0% prekida usluge. Globalnim organizacijama je to veoma bitno, jer u svakom trenutku uslugu koristi veliki broj korisnika. Zbog toga što se referencira na Site objekte u Active Directoryu, Exchange server omogućuje krajnjim korisnicima da se autenticiraju na njima geografski najbliži server. Osim što nudi skalabilnost, Exchange server omogućuje sigurnu komunikaciju, te vrlo lako sprječava izlaganje klasificiranih informacija izvan organizacije DLP politikama.

Popis kratica

ATM	*Asynchronous Transfer Mode*	asinkroni način prijenosa
ISDN	*Integrated Services Digital Network*	digitalna mreža integriranih usluga
SMTP	*Simple Mail Trasport Protocol*	protokol za komunikaciju
DNS	*Domain Namin System*	imenički servis
MX	*Mail Exchanger*	DNS zapis za mail server
TCP	*Transport Control Protocol*	komunikacijski protokol
AD	*Active Directory*	aktivni direktorij
OWA	*Outlook Web Access*	web mail aplikacija
EMC	*Exchange Management Center*	web sučelje za administraciju
RBAC	*Role Based Access Control*	kontrola pristupa pomoću rola
CAS	*Client Access Server*	server koji prima http konekcije
RPC	*Remote Procedure Call*	sistemski poziv
DAG	*Database Availability Group*	grupe visoke dostupnosti
FQDN	*Fully Qualified Domain Name*	puno domensko ime

Popis slika

Slika 3.1 Role Exchange servera 2007 9

Slika 3.2 Shematski prikaz DAG-a 11

Slika 3.3 Shematski prikaz Exchange 2016 infrastrukture 13

Slika 4.1 Shematski prikaz infrastrukture na dvije lokacije sa FSW u Azuru 19

Slika 4.2 Prikaz statusa kopija baza 20

Slika 5.1 Rad *proxy-ranja* u Exchange-u 2016 24

Slika 5.2 Jedan imenski prostor sa četiri različite putanje kroz dvije lokacije 26

Slika 6.1 Visoka dostupnost transportnih servisa 28

Slika 6.2 Proces dupliranja poruka 30

Slika 7.1 Prikaz kreiranja DLP politike u Exchange admin centru 35

Slika 7.2 Prikaz prozora „New custom DLP policy“ 36

Slika 7.3 Odabir opcije „Block messages with sensitive information“ 37

Slika 7.4 Izgled finalne DLP politike 38

Slika 8.1 Pregled statusa baza 39

Slika 8.2 Aktivacija pasivne baze 40

Slika 8.3 Analiza zaglavlja poruke 40

Slika 8.4 Analiza zaglavlja poruke u situaciji failovera 41

Slika 9.1 Primjer SPF DNS zapisa 42

Slika 9.2 Uspješni SPF test 42

Slika 9.3 Prikaz poruke u karanteni 43

Slika 9.4 Neuspješni SPF test 43

Popis tablica

Tablica 2.1 Prikaz razlika Standard i Enterprise verzije Exchange-a 2003..... 7

Literatura

[1] CUNINGHAM,SVIDERGOF *Designing and Deploying Microsoft Exchange Server 2016*

[2] CLIFTON, L *Mastering Microsoft Exchange Server 2016*

[3] *https://datatracker.ietf.org/doc/rfc821/*

[4] https://datatracker.ietf.org/doc/rfc5321/

[5] *https://en.wikipedia.org/wiki/History_of_Microsoft_Exchange_Server*

[6] *https://www.slideshare.net/bedekarpm/brief-32579920*

[7] *https://sherpasoftware.com/blog/microsoft-exchange-history-lesson/*

[8] *https://www.itprotoday.com/email-and-calendaring/exchange-server-2007-new-features*

[9] *https://searchitchannel.techtarget.com/tip/New-features-in-Microsoft-Exchange-Server-2010*

[10] *https://www.techrepublic.com/article/understand-storage-groups-and-stores-in-exchange/*

[11] *https://docs.microsoft.com/en-us/exchange/new-features/new-features?view=exchserver-2019*

[12] *http://techgenix.com/whats-new-microsoft-exchange-2016/*

[13] *https://docs.microsoft.com/en-us/exchange/mail-flow/transport-high-availability/transport-high-availability?view=exchserver-2019*

„Pod punom odgovornošću pismeno potvrđujem da je ovo moj autorski rad čiji niti jedan dio nije nastao kopiranjem ili plagiranjem tuđeg sadržaja. Prilikom izrade rada koristio sam tuđe materijale navedene u popisu literature ali nisam kopirao niti jedan njihov dio, osim citata za koje sam naveo autora i izvor te ih jasno označio znakovima navodnika. U slučaju da se u bilo kojem trenutku dokaže suprotno, spreman sam snositi sve posljedice uključivo i poništenje javne isprave stečene dijelom i na temelju ovoga rada“.

U Zagrebu, 9.7.2019.