Microsoft

Exchange

Sadržaj

Uvod

Microsoft Exchange je u osnovi mail server, koji podržava POP, IMAP, web klijente, kao i svoj klijent Outlook. Ali kada bi kao proizvod Exchange bio samo mail server, to bi bio vrlo skup i kompliciran izbor za korisnike.

Exchange omogućuje korisnicima da razmjenjuju informacije pomoću Outlooka ili Outlook Web Accessa, dakle omogućuje suradnju među korisnicima. Primjeri takve suradnje su održavanje zajedničkih lista adresa kojima svaki korisnik može pridodati vlastite adrese, dogovaranje sastanaka, te razmjenjivanje ostalih tipova informacija preko public foldera ili dopuštanjem pristupa vlastitim folderima u mailboxu. Također može se koristiti za smještaj baze Outlook formi.

Exchange je server-based aplikacija te se zasniva na Active Directory infrastrukturi. Zato je nepraktična za pojedinačne korisnike i male firme kojima je jeftinije rješenje, recimo shareware POP server. Exchange je puno teže konfigurirati od takvog jednostavnijeg rješenja, naročito ako se ukjuče neke napredne opcije poput Outlook Web Access. Exchange se tako čini prekompleksan za male firme, ali ta kompleksnost posjeduje funkcije koje su važne za povezivanje nekoliko tisuća Exchange korisnika.

Povijest Exchangea

rane 1990-te : Program Microsoft Mail smatramo prethodnikom Exchangea

1993 : Prvi put se pojavljuje program sa nazivom Exchange , te se prva verzija označava sa brojem 4.0 - tada još nije komercijalni proizvod, već je prodavan samo "velikim" korisnicima; Exchange je Microsoftov odgovor na Lotusov proizvod. Ta prva verzija nije user friendly niti admin friendly, glavne karakteristike su kompleksnost, te mnogo problema. Takav proizvod je bio koristan samo velikim kompanijama.

1996 Q1 : Exchange 4.0 izlazi u prodaju kao komercijalni proizvod za male korisnike. Nova funkcija koju podržava Exchange je CDO - collaboration data objects, tada nazvan OLE (Object Linking & Embeded) Messaging s kojim je dopušteno drugim proizvodima da pristupe Exchangeu.

1997 Q1 : Izlazi verzija Exchange 5.0. OLE Messaging se sada zove Active messaging. Dodan je Outlook Web Access koji daje korisnicima mogućnost da preko interneta provjeravaju poštu, tj. da se mogu spojiti na svoj mail server preko weba kao kod mail klijenta te omogućuje slanje i čitanje maila.U to vrijeme Lotus Notes je i dalje dominantan komercijalni mail proizvod.

1997 Q4 : Izlazi verzija Exchange 5.5 sa poboljšanim Outlook Web Access i poboljšanom podrškom za internet. Sa ovom verzijom Exchange je po prvi put postao ozbiljan mail proizvod

1998 : Exchange je prodavaniji proizvod od Lotus Notesa.

31.8.2000 : Izlazi verzija Exchange 2000. Glavna promjena je da Active Directory infrastruktura zamjenjuje Directory Service.

2003 : Izlazi verzija Exchange 2003.

Verzije Exchangea 2000

Exchange 2000 Server : Namijenjena malim i srednje velikim organizacijama. Glavna karakteristika je ograničenost pohrane podataka na 16 GB.

Exchange 2000 Enterprise Server : Ova verzija nije samo mail server već i program koji omogućuje messaging i suradnju među korisnicima. Ovoj verziji su dodane funkcije kao što je Public Folders ili četverosmjerni active/active clustering. Nema ograničenja za količinu pohranjenih podataka, te je omogućeno particioniranje pohrane podataka.

Exchange 2000 Conferencing Server : Prodaje se kao zaseban proizvod. Omogućuje voice, data, video conferencing, te daje mogućnost administratorima da alocira resurse.

Verzije Exchangea 2003

Exchange 2003 Standard Edition : Namijenjena malim i srednjim kompanijama. Ograničena je pohrana podataka (16 GB).

Exchange 2003 Enterprise Edition : Namijenjena velikim kompanijama. Omogućuje stvaranje višestrukih baza podataka i grupa za pohranu podataka na jednom serveru. Omogućava pohranu do 16 TB podataka. Podržava clustering sa 8 nodova (ako je instaliran Windows Server 2003 Enterprise Edition).

Glavne osobine Exchangea 2003

- Integracija Active Directory
  - integriranost u Active Directory directory servis u Windows 2000 i Windows 2003
  - korištenje system access control lists u Windows 2003 za sigurniju komunikaciju
- Skalabilna arhitektura baza podataka

    - do 16 GB u jednoj mailbox bazi podataka, do 20 takvih baza podataka po serveru
    - višestruke baze podataka na jednom serveru
- Mogućnost korištenja na računalu na kojem su već instalirane prijašnje verzije Exchangea.
- Poboljšana sigurnost
    - brojne antispam mogućnosti
    - Virus Scanning API 2.5
    - podrška za Internet Information Services 6.0 u Windows 2003
- Podrška za mobilne uređaje
- Integracija sa Outlook 2003
...

MS Active Directory servis

Od verzije Exchange 2000, Exchange više nema svoj directory servis, već se kompletno oslanja na Active Directory.

Što je to Active Directory?

Active Directory je directory servis Windowsa 2000, koji hijerarhijski sprema informacije o objektima (korisnici, printeri,...) u mreži i te informacije čini dostupnima administratoru, korisnicima ili aplikacijama. Koristeći AD mreža i objekti u mreži su organizirani u konstrukcije poput domene, stabla (x domena = stablo) i šume (x stabala = šuma). Pošto AD radi na osnovi standardnih protokola moguć je pristup AD-u ostalih aplikacija koji sa baziraju na istim protokolima.

Koje su koristi od Active Directory ?

- Integracija sa DNS-om – AD koristi Domain Name System, internet standardni servis koji prevodi imena računala u numeričku IP adresu, što omogućuje identifikaciju i uspostavljanje veze među računalima u TCP/IP mrežama.
- korisnik može pomoću search komande brzo pronaći objekte u mreži. Pronalaženje informacija je optimizirano korištenjem globalnog kataloga
- AD je moguće proširiti/nadograditi, npr. mogu se dodati nove klase objekata ili osobine samih objekata
- grupna načela – npr. određuju čemu korisnik može pristupiti, te se ta načela primjenjuju na sva računala
- skalabilnost – kombiniranje višestrukih domena u stabla, višestrukih stabala u šume
- replikacija informacija - u svakom trenutku su sve informacije dostupne na svim računalima
- sigurnost – svakom objektu se može odrediti kontrola pristupa
- interoperabilnost sa drugim directory servisima

Directory (spremište podataka) je hijerarhijska struktura koja sprema informacije o objektima u mreži. U objekte spadaju serveri, printeri, korisnici, domene, servisi, itd. Npr. direktorij sadrži podatke o korisniku (ime, prezime, mail adresa, telefonski broj,...).

Directory Servis je u stvari izvor informacija direktorija i uz to servis kojim se informaciju daju na korištenje administratorima, korisnicima ili aplikacijama. Directory servis je transparentan, tj. korisnik ne zna gdje se informacija koju trenutno koristi fizički nalazi. Primjer DS je servis koji dopušta drugim korisnicima na mreži da pristupe podacima (npr. mail adresi) nekog drugog korisnika.

MS Exchange je primjer korištenja directory servisa koji omogućuje korisnicima da potraže druge korisnike,te komuniciraju putem e-pošte.

Integracija DNS i AD

DNS i AD koriste ista imena domena za različite nazivne prostore. AD povezuje imena domena objekata sa zapisima objekata pomoću LDAP (Lightweight Directory Access Protocol) poziva u AD bazi podataka. Da bi AD klijent locirao server koristi se DNS-om, tj. koristi se DNS-om kao lokator servisom, tj. pretvara imena domene ili servisa u IP adrese. DNS je potreban za rad AD-a. Dakle :

- AD domene i DNS domene koriste iste hijerarhijske strukture (npr. microsoft.com je i DNS i AD domena);
- DNS zone se mogu spremiti u AD;
- AD klijenti koriste DNS za lociranje domenskih kontrolera.

Domenski kontroler je računalo koje ima instalirane Windows 2000 sa već instaliranim i namještenim Active Directory servisom. Na početnom DK se automatski stvara «Globalni Katalog» (svaka šuma mora imati barem jedan GK). GK omogućuje logiranje u mrežu AD klijentima (svi objekti – printeri , korisnici – moraju imati referencu u GK), te pretraživanje svih domena, kao da je jedna velika domena.

Interoperabilnost

Organizacije obično koriste široku paletu proizvoda koji moraju raditi zajedno. Active Directory podržava veliki broj standarada, te je time omogućena komunikacija sa ostalim Microsoft proizvodima, ali i proizvodima ostalih proizvođača.

- LDAP protokol je industrijski standard za pristup direktorijima. Kod AD je LDAP primarni protokol za pristup direktorijima koji omogućuje dodavanje, modificiranje i brisanje podataka u AD, kao i pozivanje i ispitivanje podataka iz AD. LDAP definira kako klijent može pristupiti podacima u direktoriju i izvoditi operacije na podacima.

- ADSI (AD Service Interface) – omogućuje pristup AD otkrivajući objekte iz direktorija kao COM (Component Object Model) objekte

- LDAP C API

Active Directory i Exchange komuniciraju pomoću servisa zvanog Active Directory Connector, koji omogućuje dvosmjernu sinhronizaciju. ADC mapira objekte i njihove osobine kada sinhronizira podatke između dva direktorija.

Forestprep i Domainprep

Prije instaliranja Exchange servera na računalo potrebno je obaviti neke preinake na Windows 2000 instalaciji. Shema Active Directorya mora biti proširena, te se moraju izdati dozvole korisniku ili grupi korisnika koji će prvi instalirati Exchange server. Na svakoj domeni koja

će biti Exchange ili mail server, moraju biti napravljene dvije sigurnosne grupe, koje dozvoljavaju administrativne mogućnosti. Za ovu pripremu služe dva programa : Forestprep i Domainprep. Glavna funkcija ovih programa je da razdvajaju instalaciju Exchangea na zadaće koje ovise o razini potrebne dozvole koje administrator posjeduje.

Forestprep obavlja sve zadaće za koje je potrebna Enterpriseadmin ili Schemaadmin dozvola, zbog toga što mijenja samu konfiguraciju Active Directorya. Forestprep proširuje shemu AD da uključuje specifične informacije vezane uz Exchange. Također kreira objekte, te daje Exchange administrator dozvolu tim objektima. Forstprep imenuje Exchange organizaciju te odgovarajuće objekte. Forestprep se pokreće samo jednom u jednoj Windows 2000 šumi.

Domainprep obavlja sve zadaće za koje je potrebna Domainadmin dozvola. Domainprep je potrebno pokrenuti jednom u svakoj domeni koja sadrži Exchange server. Domainprep stvara grupe i dozvole potrebne da Exchange server čita i modificira atribute korisnika. Domainprep stvara 2 nove domene :

- Exchange Domain Servers grupa : sadrži accounte svih Exchange servera u domeni. Koristi se za Recipient Update Service (koji služi za stvaranje i modificiranje address lista)
- Exchange Enterprise Servers grupa : sadrži sve Exchange Domain Server grupe u organizaciji.

Domainprep također stvara Public Folder spremište u AD. Objekti iz Public Foldera egzistiraju izvan tog spremišta, pa Domainprep stvara te objekte u spremištu svake domene.

<u>Kako Exchange komunicira sa AD</u>

Exchange koristi tri directory access komponente u komunikaciji sa AD :

-Directory Service Access

-Directory Service Proxy

-Categorizer

DSAccess je komponenta jezgre Exchangea koja je implementirana u fileu DSACCESS.DLL. Svrha ove komponente je da kontrolira kako ostale Exchange komponente pristupaju Active Directory-ju. DSAccess otkriva topologiju AD i radi listu dostupnih directory servera kojima se

služe ostale komponente. Također sadrži memory cache koji smanjuje broj LDAP poziva komponenti prema AD serverima. Dakle u E2000 DSAccess je centralni mehanizam koji određuje topologiju AD, otvara odgovarajuće LDAP veze zaobilazi greške u serveru.

DSProxy je Exchange komponenta implementirana u fileu DSPROXY.DLL. Funkcije DXProxy-a su : da emulira MAPI address book servis i proxy zahtjeve prema AD serveru, te služi kao mehanizam kojim Outlook direktno pristupa AD serverima.

Categorizer je komponenta koja izvlači informacije iz headera poruke kako bi u AD pronašla odgovarajuće mjesto gdje će poruka biti poslana. Npr. kod SMTP adrese x@y.com Categorizer će identificirati server na kojem taj korisnik ima mailbox, te će odrediti put kojim će poruka doći do servera. Categorizer također određuje limite koje poruka može imati i to svakom korisniku posebno.

Kako Exchange određuje opterećenje na AD serveru

Pomoću DS Topology kalkulatora je moguće odrediti koliko opterećenje može podnijeti AD server uzimajući slijedeć faktore u obzir :

- topologija Exchange-a,
- resursi servera,
- broj korisnika,
- protokoli u upotrebi,
- količina emailova koja prolazi kroz sustav

Struktura Mailbox direktorija

Većina interakcije između korisnika i Exchangea se provodi preko programa MS Outlook, email klijenta. Outlook stvara direktorije od kojih su mnogi vidljivi korisniku, ali i direktorije koji su nevidljivi korisniku a koji su potrebni za operacije između Outlooka i Exchangea, koje korisnik ne kontrolira (skrivene direktorije možemo gledati pomoću Exchange Database View programa – mdbvu.exe, korisno za brisanje temporary fileova koji se nagomilaju vremenom).

Kada administrator u Exchangu stvori korisnika-objekt, može uključiti opciju kojom je taj korisnik «mailbox-enabled». Time korisnik dobiva svoj «poštanski sandučić» na Exchange serveru. Mailbox se stvori tek kada se korisnik prvi put logira na server.

Svaki protokol koji Exchange podržava stvara vlastite direktorije. Kao primjer ćemo uzeti direktorije koje Exchange napravi kada MAPI klijent pristupi Outlooku :

- Common Views : ako korisnik promjeni izgled Outlooka, podaci o novom izgledu će se naći ovdje
- Deferred Action (odložene/odgođene akcije) : npr. ako je korisnik postavio Outlook da kod svake primljene poruke se izvrši akcija kojom će se ta poruka maknuti na neko drugo mjesto, ta akcija neće biti obavljena sve dok korisnik nije logiran. To tada ta akcija će biti u ovom direktoriju.
- Finder : ovaj direktorij je aktivan kada korisnik izabere Search funkciju u Outlooku. Stvara se poddirektorij Search Results, a rezultati koji zadovoljavaju tražene kriterije se kopiraju u Finder direktorij.
- Schedule : ovdje se drže informacije vezane za Schedule+, koje se mogu prebaciti u Calendar direktorij (vremena sastanaka ???)
- Shortcuts : sadrži poruke vezane za Favorites
- Spooler Queue
- IPM Subtree : sadrži poddirektorije koji su vidljivi Outlook korisniku (ovdje se nalazi većina informacija koje unosi korisnik (pošta,...) :

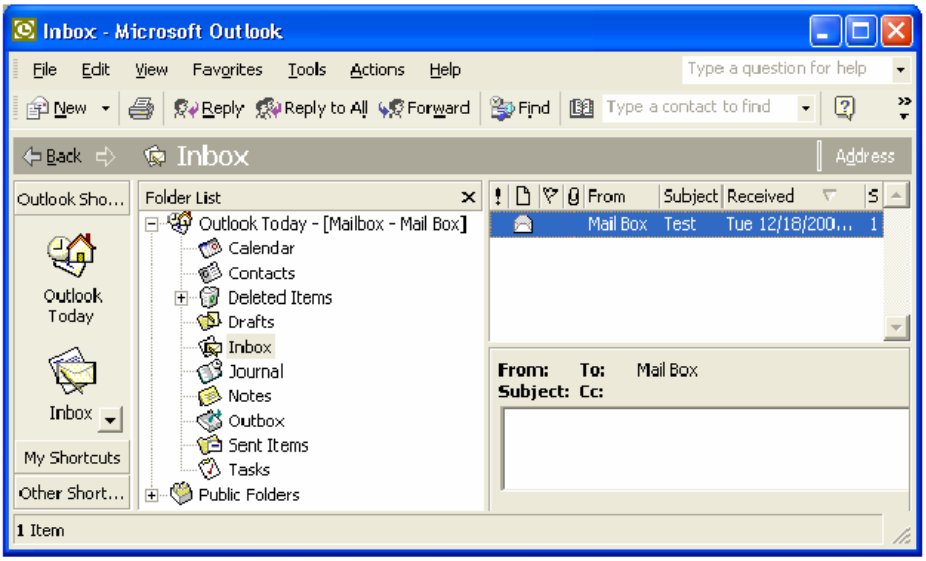


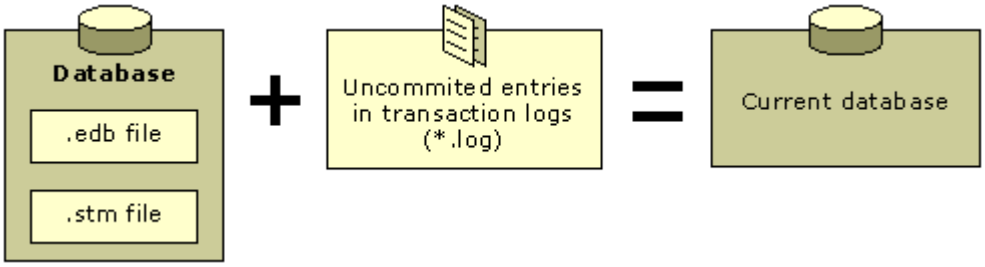
Figure 1 The IPM Subtree folders as they appear in Outlook

  - Calendar : svi podaci vezani uz sastanke
  - Contacts : sve informacije vezane uz kontakte
  - Deleted Items : izbrisane informacije, koje ostaju ovdje dok ih korisnik ne obriše (ili ih program automatski obriše)
  - Drafts : nedovršene poruke koje korisnik još ne želi poslati
  - Inbox : Outlook automatski sprema sve poruke koje su došle u Mailbox u ovaj direktorij. Sadrži poddirektorije :
    - Rules : korisnik može automatizirati akcije koje će se primjeniti na poruke i kada korisnik nije logiran
    - Views : korisnikov odabir prikaza poruka
  - Journal
  - Notes
  - Outbox : temporary direktorij za poslane poruke
  - Sent Items : po defaultu Outlook ovdje napravi kopiju poslane poruke
  - Tasks
  - Views : korisnik može mijenjati prikaz direktorija za lakše snalaženje (npr. boje)
- Freebusy data : informacije o sastancima (kada je korisnik na raspolaganju)
- Reminders : sadrži poruke koje sadrže podsjetnike

Struktura baza podataka u Exchangeu

Za administratora Exchange servera jedna od najbitnijih stvari je poznavati strukturu baza podataka.

Ovo je primjer za jednu storage grupu:



Kao što vidimo baza podataka se sastoji od tri filea :

- .edb file : sadrži sve direktorije, tablice, indexe o porukama, te MAPI poruke i attachmente
- .stm file : sadrži sve podatke skinute s Interneta u svom originalnom formatu
- .log fileovi : sadrži zapise o svim porukama u storage grupi. Pruža toleranciju za grešku u slučaju greške u bazi podataka. Log fileovi imaju fiksnu veličinu od 5 MB.
- edb.chk file : prati koji zapisi u log fileu moraju biti ponovno pokrenuti u slučaju greške
- .srs file: omogućava kompatibilnost sa Exchange 5.5
- .kms file : služe za sigurnost i enkripciju

Backup podataka u Exchangeu

Koristi se ntbackup.exe iz Windowsa, koji daje 4 opcije backupa za Exchange :

- full backup : backupira cijeli Web Storage System i log fileove, te briše logove koji su nepotrebni (određeno u .chk fileu)
- copy backup : isto kao i full, samo ne briše log fileove
- incremental backup : backupira log fileove (određeno u .chk fileu), te ih zatim obriše
- differential backup : isto kao i incremental, samo ih ne obriše

Outlook Web Access

MS Outlook Web Access je integrirana komponenta Exchangea.

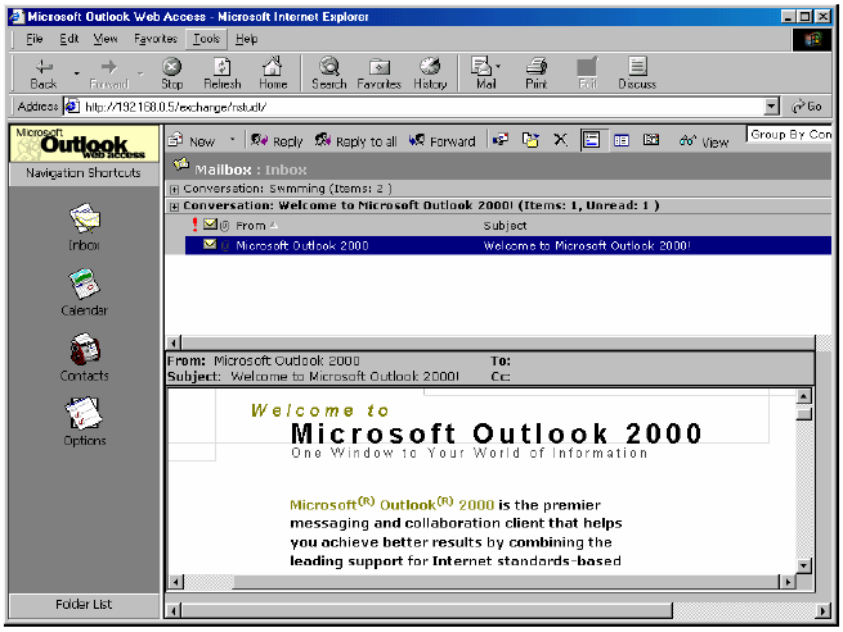


Figure 1 Outlook Web Access Using Internet Explorer 5.0

Prva verzija Exchangea sa OWA je bila verzija 5.0. OWA nije napravljen da zamijeni Outlook, već da omogući korisniku obavljanje samo osnovnih funkcija (dakle, OWA je «osiromašena» verzija Outlooka) :

Feature	***Outlook 2000***	***Outlook Web Access 2000***	***Outlook Web Access 5.5***
Basic features			
E-mail	Yes	Yes	Yes
Calendaring	Yes	Yes	Yes
Contacts	Yes	Yes	Yes
Tasks	Yes	No	No
Access to embedded objects	Yes	Yes	No
Rich text	Yes	Yes	Yes
HTML	Yes	Yes	No
Drag-and-drop editing	Yes	Yes with Internet Explorer 5.0	No
Shortcut menus	Yes	Yes with Internet Explorer 5.0	No
Offline use	Yes	No	No
Journal	Yes	No	No
Printing templates	Yes	No	No
Advanced features			
Delegate access to mailbox	Yes	Yes (read-only)	No
Timed delivery	Yes	No	No
Expiration	Yes	No	No
Spelling checker	Yes	No	No
Reminders	Yes	No	No
Outlook rules	Yes	No	No
Single sign-on	Yes	Yes*	No

* Not available with front-end and back-end server configurations.

OWA je napravljen tako da može raditi s bilo kojim browserom, ali naravno najbolje radi sa MS Internet Explorerom.

OWA 5.x je koristio Active Server Pages (ASP) za komunikaciju sa Exchange serverom koji je koristio CDO 1.2 i Messaging Aplication Programming Interface (MAPI). Time je broj korisnika bio ograničen. OWA u Exchange 2000 više ne koristi MAPI za komunikaciju sa Mailboxom, te ne koristi ASP za pristup klijentu. I dalje se koristi Http, a OWA je sada dio MS Web Storage System, te koristi Internet Information Services (IIS) samo za primanje zahtjeva, koje daje prosljeđuje WSS-u. ISS koji je dio Windowsa 2000, prima HTTP zahtjeve browsera i šalje HTTP odgovore sa Exchange servera ili OWA. Kada korisnik u Web browser upiše npr. http://owa.microsoft.com/exchange, klijent će prikazati korisnikov mailbox. Isto tako drugi folderi se mogu pristupiti dodavanjem npr. /calendar gornjem URL-u.

U najnovijoj verziji OWA 2003 dodane su još mnoge nove mogućnosti od kojih je najvažnija podrška za mobilne uređaje (Pocket PC,...). Ostale novosti su :

- povećana sigurnost (S/MIME podrška, zaštita od spama, blokiranje attachmenta)
- poboljšan user interface
- veća brzina (podrška GZip kompresije)
- podrška za mobilne uređaje (xHTML, cHTML, HTML, i-Mode), wireless,...

SMTP i Exchange 2000

E2000 koristi SMTP za interno dostavljanje pošte između Exchange servera i routing grupa, te za dostavljanje pošte izvan Exchange organizacije.

SMTP je internet standard za transportiranje i dostavljanje e-pošte. SMTP specifikacija se nalazi u RFC 2821 i RFC 2822. SMTP se oslanja na TCP za preciznu dostavu podataka preko mreže. U Windowsima 2000 SMTP servis je dio Internet Information Service i pokreće se komandom Inetinfo.exe. Kada je Exchange instaliran na računalo, proširuje funkcionalnost SMTP komponente :

- SMTP servisom sada upravlja Exchange System Manager

- implementira podršku za Link State Information
- dodaje podršku za Exchange Installible File System
- određuje diskovni prostor gdje se poruke šalju na čekanje
- poboljšava kategorizaciju poruka

Primanje pošte u E2000, u default konfiguraciji je moguće ako :

- postoji stalna veza na Internet (Dialup treba dodatna podešavanja)
- vanjski DNS server za našu domenu mora pokazivati na naš mail server
- naš mail server mora biti dostupan ostalim serverima na internetu
- police primanja moraju biti dobro podešene (npr. za primanje pošte od x@y.com polica mora sadržavati @y.com)

Primanje pošte kroz Exchange 2000 server protječe na sljedeći način:

1. SMTP server koji šalje poštu ispituje DNS kako bi locirao IP adresu primateljevog SMTP servera

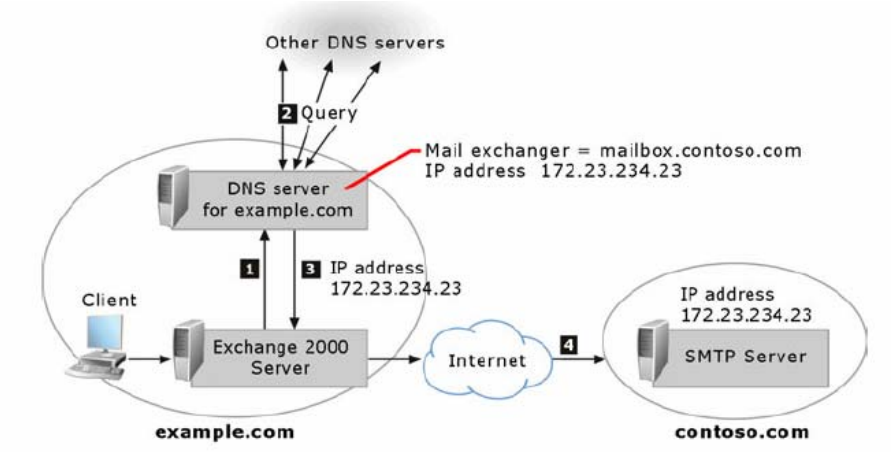


Figure 3 How Exchange uses DNS to resolve external IP addresses

2. zatim preko porta 25 uspostavlja komunikaciju između servera (na Exchange serveru primateljev SMTP server je virtualni SMTP server koji je za to određen)
3. SMTP server prihvaća poštu samo ako je namijenjena primatelju sa te domene. Primatelji su definirani u polici primatelja (osim ako nije omogućen relay)
4. zatim virtualni SMTP server određuje način na koji će dostaviti poštu. Exchange locira primatelja u Active Directoryju, te određuje koji će server obaviti dostavu

5. na kraju virtualni SMTP server koristi interni mehanizam da dostavi poštu do određenog servera

Za slanje pošte (ako postoji stalna veza na Internet) Exchange koristi 2 glavne metode : koristi DNS direktno da kontaktira udaljeni mail server, ili provodi poštu kroz «pametnog hosta» koji preuzima odgovornost oko DNSa i dostave pošte.

Slanje pošte preko Exchange servera protječe na sljedeći način:

1. interni korisnik šalje poštu primatelju na udaljenoj domeni
2. virtualni SMTP server ispituje dali je primateljeva adresa na globalnom popisu. Ako nije Exchange određuje da je pošta namijenjena udaljenoj domeni
3. ako je potrebno Exchange server dostavlja poštu pripadnom virtualnom SMTP serveru
4. virtualni server koristi IIS metabazu da odredi metodu slanja pošte
5. virtualni SMTP server na Exchange serveru tada koristi DNS da potraži IP tražene domene, te zatim pokuša dostaviti poštu; ili proslijedi poštu do «pametnog hosta» koji preuzima odgovornost za dostavljanje pošte

Virtualni SMTP Server je u osnovi proces ili server, koji služi i za primanje i služi kao klijent za slanje pošte. Određen je posebnom kombinacijom IP adrese i broja porta. Standardni virtualni SMTP server koristi sve raspoložive IP adrese na serveru te port 25 za dolazeće poruke. Jedan fizički server može biti host više virtualnih servera. Za konfiguraciju virtualnih servera koristi se Exchange System Menager. U njemu možemo konfigurirati IP adrese i portove koje ćemo koristiti, relay restrikcije, sigurnost (TLS – Transport Layer Security – implementacija SSL),...

Spajanje POP3 i IMAP klijenata na Exchange

Najkorišteniji i najpopularniji način za primanje pošte je preko POP3 protokola. Post Office Protocol (POP) dozvoljava čitanje i skidanje pošte sa servera. Opisan je u RFC 1939. Pomoću POP se pošta ne može slati, već se za to koristi SMTP. POP se oslanja na TCP za točnu dostavu podataka preko mreže.

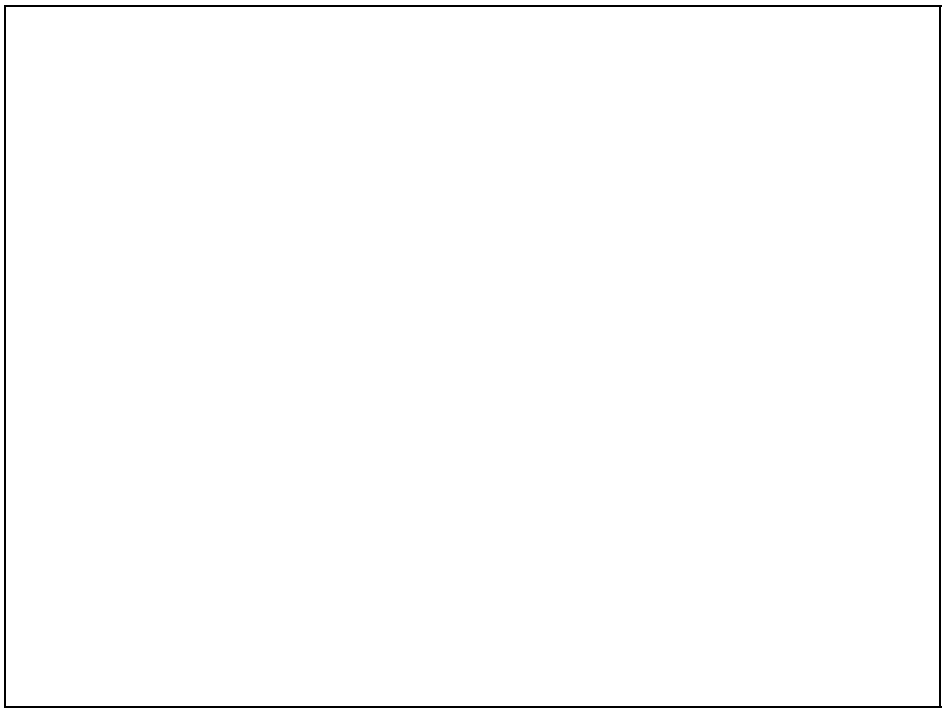
Exchange pruža mogućnost korištenja POP3 usluge za lokalnu mrežu i za udaljene korisnike. Najveći problem pri korištenju POP3 protokola u prošlosti je bio nemogućnost podešavanja opcije za ostavljanje pošte na serveru kod starijih verzija email klijenata. U slučaju da je korisnik skidao poštu sa nekog udaljenog računala, kada bi se vratio na vlastito računalo pošta bi mu bila nedostupna. Zbog toga je IMAP protokol bio popularniji od POP protokola. Današnji POP3 klijenti dopuštaju odabir, želimo li da skinuta pošta ostane na POP3 serveru, te zato POP3 ponovno postaje popularan, naročito među korisnicima koji zahtijevaju samo osnovne email funkcije (Inbox - Outbox). IMAP dopušta upotrebu svih funkcija email klijenta (Calendar, Contacts, Drafts, Journal, ...). Interactive Mail Access Protocol (IMAP) dopušta korištenje pošte i mailboxa na udaljenom serveru. Trenutna verzija IMAP je verzija IMAP4. IMAP je opisan u RFC 2060. Kao i POP ne pruža mogućnost slanja pošte, već se za to koristi SMTP. IMAP je složeniji i moćniji od POP protokola. IMAP se također oslanja na TCP za točnu dostavu podataka preko mreže.

Razlozi za korištenje POP3 protokola su :

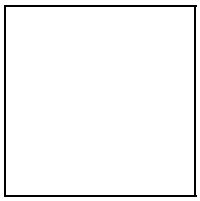
- svi email klijenti podržavaju POP3 protokol
- većina korisnika ima iskustva sa POP3 protokolom
- POP3 veze se mogu zaštititi TLS enkripcijom
- POP3 zahtjeva manje resursa sa strane servera, jer nije potrebno stalno održavati vezu, već samo povremeno provjeravati stanje
- korisnik može odabrati da ne želi zadržati poštu na POP3 serveru, te se time štedi diskovni prostor na serveru

Konfiguriranje Exchangea za korištenje POP3 protokola:

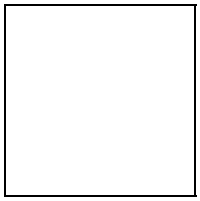
1. Kod najnovije verzije Exchange 2003, POP3 servis je onemogućen po defaultu, pa ga je potrebno pokrenuti, te postaviti da se uključuje automatski, ako želimo koristiti POP3 protokol.



2. Zatim je potrebno zatražiti Web certifikat, da bismo mogli koristiti TLS zaštićenu vezu.



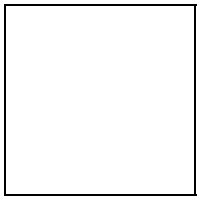
3. Tada možemo konfigurirati naš virtualni POP3 server, te namjestiti opciju da server zahtijeva TLS enkripciju za svu nadolazeću poštu.



4. Pošto POP3 služi samo za primanje pošte, za slanje pošte koristimo SMTP. Korisnik može koristiti SMTP server svog ISP-a kada je na udaljenom računalu. Ako to nije moguće, onda je potrebno stvoriti vlastiti SMTP server.

Implementacija NNTP-a u Exchange

NNTP je protokol namijenjen transportu netnews i usenet poruka među računalima. Definiran je u RFC 977. Newsgrupe su javni forumi na kojima se raspravlja o – svemu i svačemu ?, te su zato dobri izvori informacija. Organizacije zato mogu imati koristi ako dopuste svojim zaposlenima da koriste newsgrupe. Mogu na svako računalo instalirati neki NNTP klijent (npr. Gravity), ali tako ne mogu kontrolirati sadržaj newsgrupa koje zaposlenik koristi. Zbog toga su mnoge organizacije zabranile korištenje NNTP kroz njihov firewall.
Korištenjem Exchangea kao NNTP klijenta dobiva se mogućnost kontrole sadržaja, određivanja tko može gledati newsgrupe, te tko može postati na newsgrupe. Jedini uvjet koji se mora ispuniti je imati pristup nekom izvoru newsgrupa. Potrebno je samo dodati server u postavkama Exchange System Managera, te namjestiti kojim grupama želimo imati pristup.



Key Managment Service u Exchangeu 2000

Key Managment Service (KMS) je jedna od najbitnijih mogućnosti Exchangea vezana uz sigurnost. KMS koristi servis za certifikate Windowsa 2000, te zato nije potrebno tražiti dodatni Certification Authority (CA) za njegov rad. CA Windowsa 2000 obavlja sve operacije sa certifikatima, te sa održavanjem Certificate Trust List (CTL).

Kada korisnik želi izdati digitalni certifikat preko KMS-a, KMS koristi certifikate izdane sa strane Windows 2000 servisa za certifikate, za stvaranje para ključeva. Par ključeva se sastoji od javnog ključa (koji je smješten u Active Directory, te je dostupan svim korisnicima), te privatni

ključ, koji je smješten u enkriptiranoj bazi podataka, koja se nalazi na Key Managment serveru. Privatni ključ je dostupan samo korisniku kojem je izdan.
Točnije je reći da se u stvari kreiraju dva para ključeva :

- prvi par je kreiran od strane KMS-a, te se koristi za enkripciju poruka
- drugi par je kreiran od strane Outlooka, te služi digitalnom potpisivanju

Dakle zadatak KMS-a je pružiti mogućnost enkripcije i digitalnog potpisivanja podataka. Kada nam pošiljatelj pošte želi poslati poruku, on će iskoristiti naš javni ključ, pomoću kojeg će enkriptirati poruku. Tako smo mi jedini koji možemo pomoću našeg privatnog ključa dekriptirati poruku. Kod digitalnog potpisivanja, pošiljatelj koristi svoj privatni ključ za potpisivanje, a onda svoj javni ključ da potvrdi potpisivanje. Digitalni potpis u nekoj poruci, sadrži dio same poruke, te time možemo potvrditi da je poruka stigla u originalnom stanju.

Za mogućnost korištenja potrebno je imati samo jedan certifikat (obično Enterprise Root certifikat).

Ako korisnik izgubi svoj privatni ključ, administrator samo mora pokrenuti Recover Keys akciju. Korisnik će dobiti poruku za ponovno pokretanje izrade ključa.

KMS koristi razne algoritme za enkripciju, čiji izbor ponajprije ovisi o geografskoj lokaciji, te verziji Outlooka :

- If you have users running Outlook 97 or older, select an algorithm under Microsoft Exchange 4.0/5.0 encryption:

Algorithm	Description
DES (North America only)	Data Encryption Standard. The default selection, DES, is a 56-bit strength algorithm used for content encryption.
CAST-64 (North America only)	A 64-bit strength algorithm.
CAST-40	For use outside of North America. Similar to CAST-64, except that keys are only 40 bits long.

- If you have users running Outlook 98 or later versions, select an algorithm under S/MIME encryption:

Algorithm	Description
3DES (North America only)	Known as "triple DES," this is the strongest encryption available in Exchange and is the recommended option. It is the default encryption method for S/MIME.
DES (North America only)	Data Encryption Standard. DES is a 56-bit strength algorithm used for content encryption.
RC2-128 (North America only)	Provides keys that are 128-bits in length. Note that messages encrypted with 128-bit keys require more time and processing to decrypt.
RC2-40	For use outside of North America. Similar to RC2-128, except that

	keys are only 40 bits long.

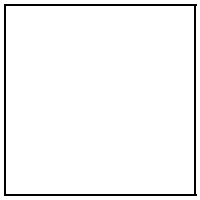
Exchange 2000 Clusters

Za stvaranje Exchange 2000 clustera koristimo program Windows Clustering koji je dio Windowsa 2000 Enterprise i Datacenter Server verzije. Exchange automatski pri instalaciji detektira da se instalira na cluster. Exchange koristi sljedeće mogućnosti Windows Clusteringa :

- Shared Nothing Architecture
- Resource DLL
- Grupe
- Resurse

Logički serveri stvoreni od strane Exchange clustera zovu se Exchange virualni serveri. Exchange virtualni server je cluster grupa, kod koje ako jedno računalo u sistemu se sruši, onda drugi node preuzme sve zadaće srušenog računala, kojemu korisnici pristupaju koristeći isto ime servera. Exchange minimalno zahtjeva:

- statičnu IP adresu
- ime mreže
- više fizičkih diskovnih prostora
- Exchange 2000 System Attendant resurse



Klijenti se spajaju na cluster istim načinom kao i kad se spajaju na obični Exchange server.

Table 2 Exchange 2000 Server components and their cluster functionality

Simple Mail Transfer Protocol (SMTP)	Provides connections to client computers and is dependent on the Exchange store.

Exchange clusteri ne podržavaju :

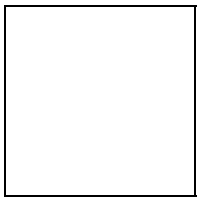
- Active Directory Connector
- Chat Servis
- MS Exchange 2000 Conferencing Server
- Instant Messaging
- Key Managing Service
- Exchange Connector
- NNTP

U clusteru od dva noda imamo slijedeću konfiguraciju :

- svaki nod ima dvije statične IP adrese (javnu i privatnu), te jedni NetBios ime
- sam cluster ima jednu statičnu IP adresu i jedno NetBios ime
- svaki Exchange virtualni server ima jednu statičnu IP adresu i jedno NetBios ime

Exres.dll je dll vezan uz resurse Exchangea 2000. Exres.dll komunicira sa odgovarajućim Exchange komponentama. Exres manipulira resursima, prijavljuje greške, te druge funkcije.

Najvažniji fizički disk u clusteru se zove Quorum Disk Resource. On se brine o konfiguraciji informacija u Quorum logu, cluster database checkpointu, te resource checkpointima. Također služi kao stalni diskovni prostor pri padovima sistema. Zbog toga svi nodovi moraju biti povezani sa ovim diskom.



Tako Quorum spriječava stvaranje višestrukih clustera. Quorum sadrži posljednju osvježenu verziju konfiguracijske baze podataka u obliku logova i checkpoint fileova.

Konfiguracije clustera:

- 2-node Active/Active : kada jedan nod padne, drugni nod preuzima funkcije prvoga. Time se smanjuju performanse clustera. Svaki nod u ovoj konfiguraciji sadrži barem jedan virtualni server.
- 2-node Active/Passive : sastoji se od primarnog i sekundarnog noda. Tako primarni podržava sve klijente, dok drugi služi kao dedicated server, koji je spreman za korištenje kada se primarni sruši. Tako ne dolazi do pada performansi. U ovoj konfiguraciji smije postojati samo jedan virtualni server u clusteru. Ova konfiguracija je preporučena.

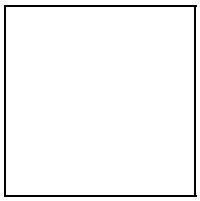


Figure 4 Example two-node Exchange 2000 cluster

Kada koristimo Windows 2000 Datacenter Server možemo koristiti do 4 noda :

- 4-node Active/Passive sa 3 aktivna noda : 3 virtualna servera (1 po nodu) + dedicated server koji preuzima posao ako jedan server padne
- 4-node Active/Passive sa 2 aktivan noda : 2 virtualna servera (1 po nodu) + 2 dedicated servera koji pruzimaju posao ako server padne. Ovo je sigurnija konfiguracija.

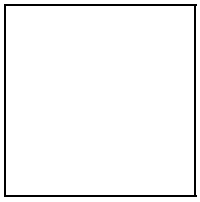


Figure 5 **Example four-node Exchange 2000 cluster**

Pitanja

1. Što je MS Exchange ?
2. Što je Active Directory ?
3. Što je directory ?

4. Struktura mailbox direktorija ?
5. Struktura baze podataka ?
6. Koje protokole podržava Exchange ?
7. Što je to Key Managment Service ?
8. Konfiguracije clustera ?

Linkovi (literatura)

http://www.microsoft.com/windows2000/server/evaluation/business/addatasheet.asp

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/ad/windows2000/deploy/projplan/default.asp

http://techtutorials.com/tutorials/exchange/exchange2000.shtml

http://www.microsoft.com/exchange/evaluation/overview

http://www.swinc.com/resource/exch_faq_sec3.htm

http://www.msexchange.org/tutorials/ms_exchange_server_5_5

http://www.microsoft.com/exchange/evaluation/features/default.asp

http://www.msexchange.org/tutorials/Exchange_Server_2003

http://www.msexchange.org/tutorials/ms_exchange_server_2000

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/library/utda.asp

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/library/exchcptc.asp

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/library/e2kowa.asp

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/library/me2kmfs.asp

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2000/proddocs/library/confsmtp.asp

http://www.microsoft.com/technet/prodtechnol/exchange/exchange2003/proddocs/library/admingde.asp