Microsoft Exchange Server 2003

Radim Němec

Microsoft Certified Professional Systems Engineer

http://www.cs.vsb.cz/navrat

Agenda

- Pozice Exchange serveru na trhu
- Vlastnosti Exchange 2003
- Instalace a správa Exchange 2003
- Diskuze

Exchange na trhu podle MS

- Číslo 1 v instalované bázi se 115 milióny uživatelů
- Číslo 1 na trhu s 60% podílem
- Strategický produkt pro Microsoft

Konkurenti

- IBM Domino/Notes – hlavní rival
- Oracle – Collaboration suite
- Novell GroupWise - historie
- OpenSource ?

- Kuriozita: Ray Ozzie—tvůrce Lotus Notes je nyní chief technical officer Microsoftu.

http://www.microsoft.com/presspass/exec/ozzie/default.mspx

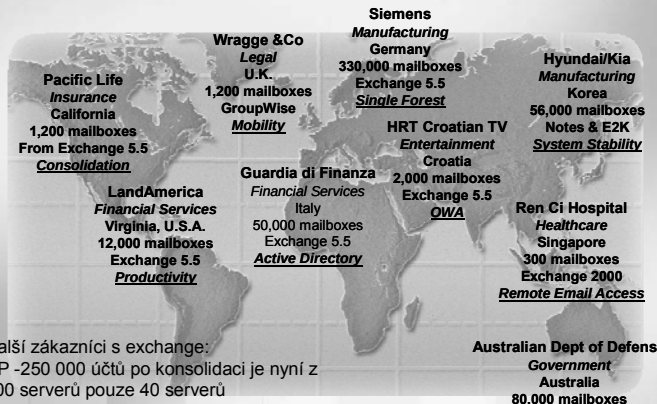
Microsoft ITG – Exchange 2003

Konsolidace Exchange Serverů do 7 oblastí

Situace dnes – konsolidované servery, clusterovaný SAN
Enabler - Office System 2003 a Exchange Server 2003

- 38 mailboxových serverů
- 90,000 e-mailových účtů
- 7 celosvětových oblastí
- 75000 uživatelů
- dostupnost 99.99 %
- 6M+ e-mailových zpráv denně

Kdo další nasazuje Exchange 2003?



Další zákazníci s exchange:
HP -250 000 účtů po konsolidaci je nyní z 300 serverů pouze 40 serverů
DHL
U nás např.: Česká pojišťovna, Indoš a další

"Siemens manages 340K desktops with Windows Server System, saves millions"

"A few years ago, Siemens supported its business with 1000 domains in a highly decentralized structure. They wanted a single, centralized Active Directory to streamline user management, email, and collaboration. Thanks to Windows Server System, Siemens has deployed a single-forest architecture and directory that simplifies and facilitates management, saves tens of millions of dollars annually, and helps Siemens to add business value that it couldn't otherwise consider. Key products are Windows Server 2003, Exchange Server 2003, Office Live Communications Server, and Office 2003 Professional."

Vlastnosti Exchange

Exchange Server 2003

Novinky	**Vylepšený přístup klientů** **Vylepšená bezpečnost** **Zlepšená správa** **Lepší ADC utility** **Nová pfMigrate utilita**
Co bylo odváto větrem	**Podpora pro real time spolupráci – přesunuto do MS Office real time communications server 2003.** **Podpora pro MS Mail a pro Lotus cc:Mail** **Mapování disku M** **Key management – nyní se používá CA W2003 serveru**

Všudypřítomná produktivita

Information Workers

Všudypřítomná produktivita	Vylepšený Outlook 2003 • **Nový uživatelský vzhled a nástroje pro správu dat** • **Podpora mobilních a vzdálených scénářů** • **Anti-Spam, Information Rights Management**
Mission Critical Dependability	Nový Outlook Web Access • **Stejný interface a mnoho stejných vlastností jako Outlook 2003** • **Více zabezpečený přístup (S/MIME, blokování HTML, automatické odhlášení)** • **Přístup přes OWA z libovolné stanice**
Snižování nákladů	Bezpečný mobilní přístup • **Podpora mobilních zařízení Windows Mobile** • **Synchronizace zařízení s Exchange Server 2003** • **Podpora mobilního procházení**

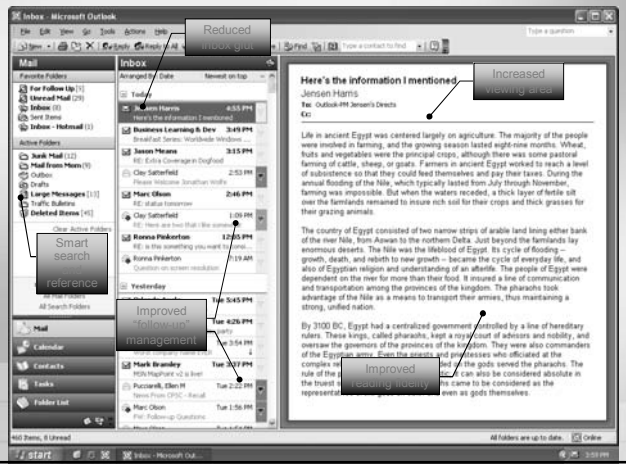
Integrace s Active Directory

Jednoduchá správa	**Správa z jednoho místa** **Automatická distribuce software** **Zjednodušené tiskové a souborové služby** **Flexibilita**
Zabezpečení	**Single sign-on k síťovým zdrojům** **Zabezpečení pracovní stanice** **Internet-ready zabezpečení serveru**
Rozšiřitelnost	**Založeno na standardech** **Otevřená rozhraní a konektory** **Silná podpora od dalších výrobců**

Vylepšený Outlook 2003

- **RPC over HTTP(S)** (bez potřeby VPN)
- **Vylepšená synchronizace**
  - **Synchronizace Smart Change**
  - **Inkrementální check-point změn při synchronizaci (ICS)**
  - **Přeskakování špatných položek**
  - **Reportování stavu před synchronizací**
- **Cache Mode** (30 – 40% less traffic)
- **Komprese MAPI** (snížení o 50 – 70%)
- **Buffer Packing**
- **Automatické řešení konfliktů**
- **Zvětšení limitů PST a OST souborů** (20 GB)
- **Vylepšené skupiny pro odeslání/přijetí**

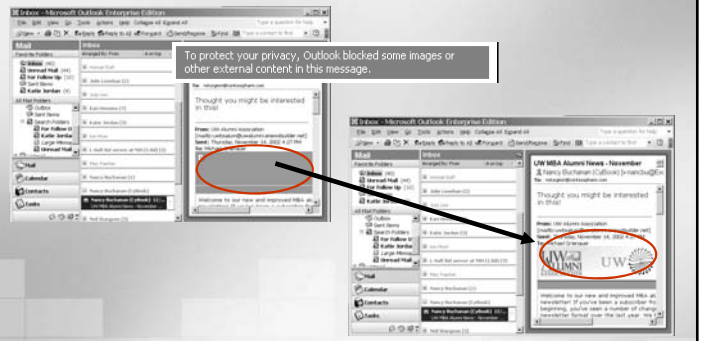
Outlook 2003: produktivní uživatelské rozhraní



Outlook 2003: ještě lepší kalendář

Outlook 2003: ještě lepší kalendář

Outlook 2003 – odstranění spamu

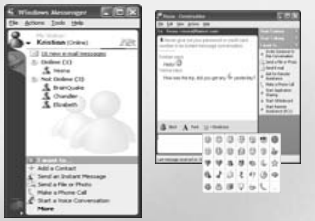


Outlook 2003 – filtrace spamu

Bezpečný mobilní přístup

- Umožnění připojení vašich mobilních pracovníků kdykoliv a odkudkoliv
- Bezpečné bezdrátové připojení
  - Pocket PC a Windows Powered Smartphone
    - Synchronizace zařízení s Exchange
      - Lokálně (přes desktop) či vzdáleně (přímo se serverem přes GSM/GPRS, Wi-Fi…)
    - Always up-to-date synchronizace s Exchange
    - Konfigurovatelnost zařízení
    - Dostupné od operátorů (Eurotel, T-Mobile) i HW výrobců (HP, Dell, Toshiba, Motorola…)
  - Bezpečné mobilní procházení informacemi
    - HTML, cHTML a WML (WAP 2.0)

Instant Messaging



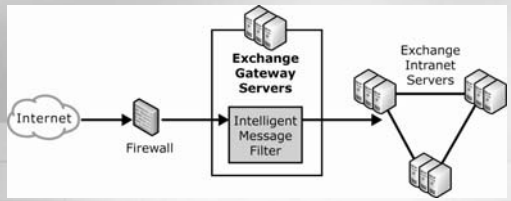
.NET Messenger Service
- Volná služba pro konzumenty
- MSN Messenger klient je stažitelný z webu
- Webově orientovaná služba používá MSN Passport pro ověření a kontrolu identity
- Možné použít také pro Pocket PC, Smart Phone a Microsoft TV

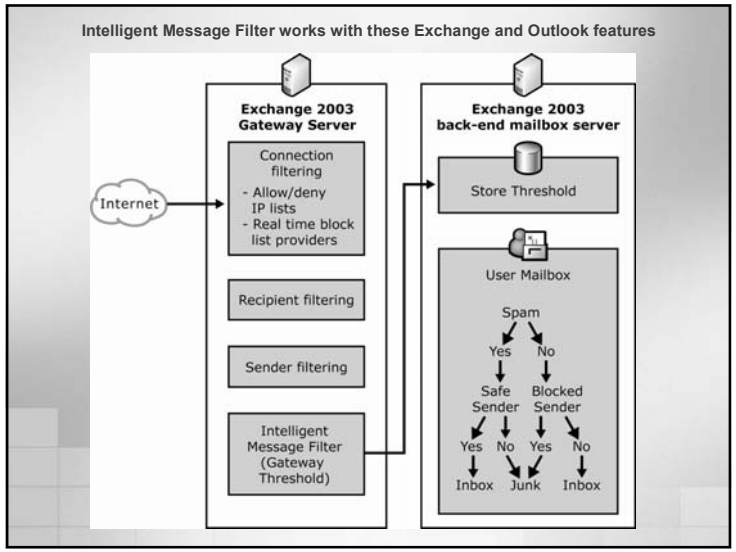
Office Live Communication Server
- Další generace podnikové IM služby
- Windows Messenger klient
- Založeno na standardu SIP protokolu
- Serverová služba, která používá Active Directory pro ověření a kontrolu identity
- Rozšířené šifrování, ověření a možnosti archivace

Microsoft Office Live Meeting
- Webová konferenční služba
- Možnost vzdálené interaktivní komunikace
- Umožňuje sdílení desktopů, aplikací nebo používání společných tabulí
- Vytváření většího počtu meetingů a optimalizace jejich zdrojů
- Snadné nasazení služby přes pobočky v rámci celé společnosti

Background Information on IMF

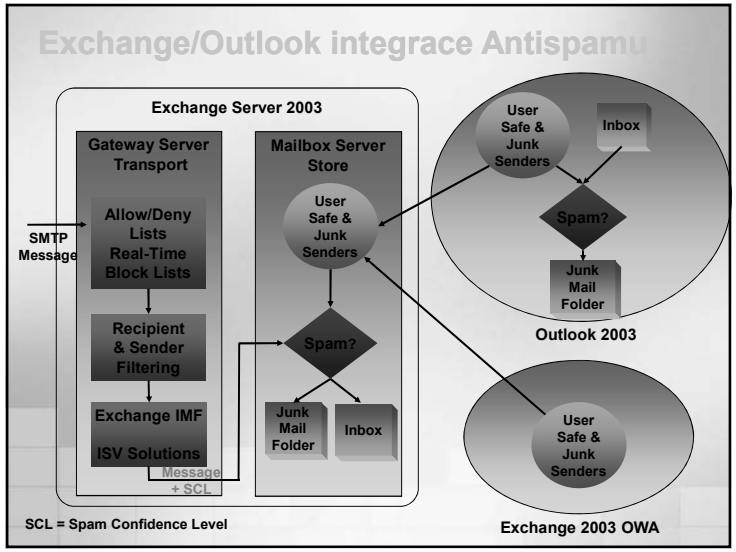
- **Hundreds of thousands** of Hotmail subscribers have volunteered to classify millions of e-mail messages as legitimate or as spam, generating more than **500,000** characteristics of spam that the SmartScreen filtering technology can track.
- With the Exchange Intelligent Message filter, Exchange 2003 customers can rate each incoming e-mail message for spam probability according to these characteristics and can use that rating to help filter spam before it reaches the user's inbox.





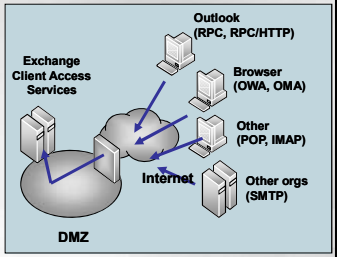
Anti-spamové technologie

- Outlook 2003
  - Seznam bezpečných a blokovaných odesilatelů, technologie SmartScreen
- Exchange 2003
  - Filtrování připojení (IP based)
  - Filtrování příjemců
  - Filtrování odesilatelů
  - Podpora ISV - Per Message Spam Rating (SCL) tagging
  - Microsoft Exchange Intelligent Message Filter
    - Na serverové straně
    - Spravován z centrální konzoly ESM

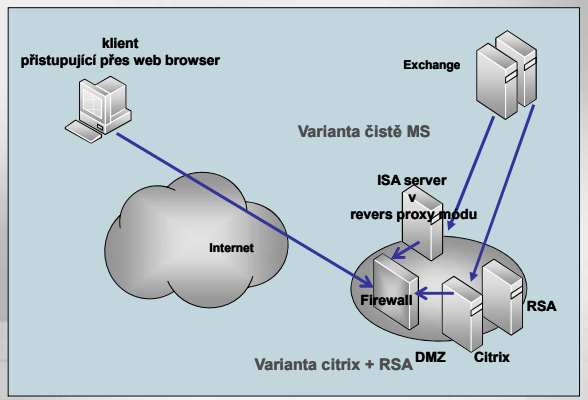


Použití Exchange spolu s ISA Serverem

- Klientské scénáře přístupu k Exchange:
  - OWA
  - OMA, ActiveSync
  - RPC/HTTP
- ISA Server 2004 poskytuje další zabezpečení pro následující scénáře:
  - Application layer inspection
  - Authentication solutions
  - Firewall protection
  - Logging and Monitoring
  - RPC filtering (pro Exchange 2000)



Možnosti vzdáleného přístupu na poštu



Produkty třetích stran

Příklady

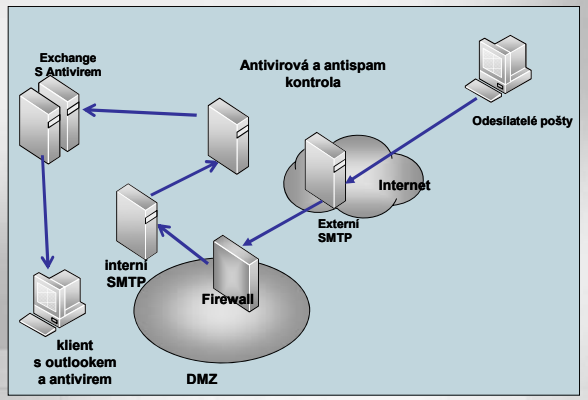
Rozšíření	Společnost
Exchange Anti-Spam	IMF (Microsoft), Symantec (Brightmail)
Exchange Anti-Virus	Trend Micro, McAfee, Symantec, CA, Sophus, Sybari, GFI, Panda, others
ISA Server Antivirus	McAfee, GFI, Panda
Intrusion Detection	ISS, GFI

Detaily viz:

http://www.microsoft.com/isaserver/partners

http://www.microsoft.com/exchange/partners

Ochrana pošty před viry a útoky

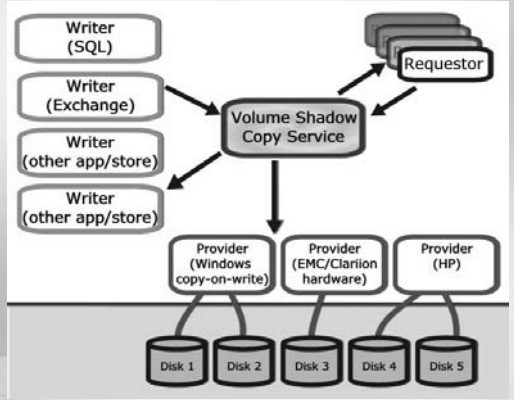


Vylepšená škálovatelnost, spolehlivost a výkon*

- Volume Shadow Copy Service (VSS) pro okamžitý Snapshot/backup
- 4 & 8 uzlový clustering
- Vylepšená správa paměti
- Vylepšení spolupráce s Active Directory
  - Ověření schématu při setupu vč. rollbacku
  - Snížení provozu při replikacích
    - Replikace položek s více hodnotami, replikace členství ve skupinách, etc…
    - > 5000 uživatelů ve skupině
- Zrychlený cluster failover
- Zlepšené replikace veřejných složek

*S Windows 2003 Serverem

VSS Basics



VSS a Exchange 2003

VSS zálohování a obnova

- Dva typy obnovy:
  - Obnova Point in time
    (obnovuje se k **času zálohy**)
  - Obnova Roll forward
    (obnovuje se k **času chyby**)
- VSS může obnovovat:
  - Na to samé místo
  - Na alternativní server či les

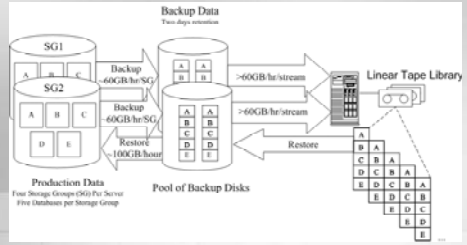
Zálohování a obnova

- Volume Shadow Copy (VSS) – Snapshot
  - Podpora software třetích stran
  - Obnova „Point in time“ nebo „Roll forward“
  - VSS může obnovovat na stejné místo nebo alternativní server

Sectors on-disk at time of snapshot (t_1)	❶❷❸❹❺❻❼❽❾❿
Sectors modified between time t_1 & t_2	❷ ❹❺ ❾
Copy replaced sectors to a side store:	❶ ❸ ❻❼❽ ❿
Recover old view (t_1) by laying snapshot ‘side store’ over current data	❶❷❸❹❺❻❼❽❾❿

Microsoft strategie zálohování

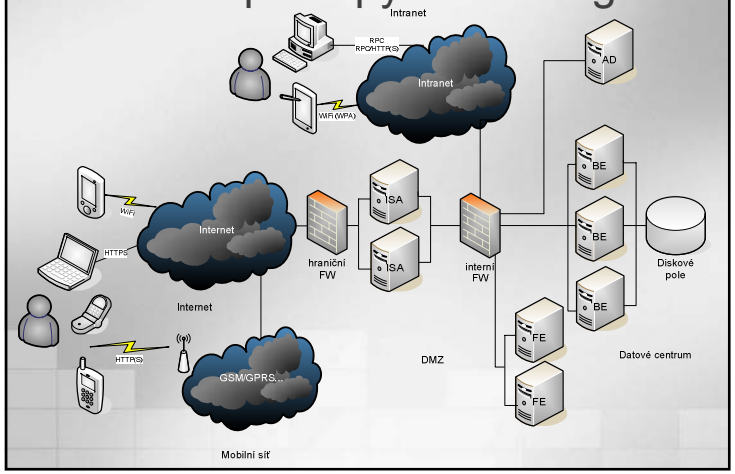
- Dvoustavová strategie zálohování
  - Primární záloha na disk
  - Na pásku pro archivaci a disaster recovery



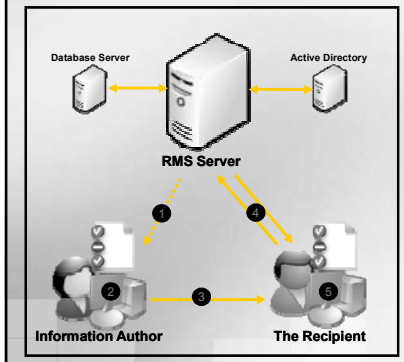
Recovery Storage Group

- Další SG speciálně pro obnovu databází
- Umožňuje okamžitou „Dial tone“ službu v případě čekání na obnovu databáze
- Umožňuje snadný přístup k jedné položce nebo mailboxu
- Využívá stávající zdroje pro obnovu databází na stejném serveru

Možné přístupy k exchange



Windows Rights Management Services (1)



1. **Author receives a client licensor certificate the “first time” they rights-protect information.**
2. **Author defines a set of usage rights and rules for their file; Application creates a “publishing license” and encrypts the file.**
3. **Author distributes file.**
4. **Recipient clicks file to open, the application calls to the RMS server which validates the user and issues a “use license.”**
5. **Application renders file and enforces rights.**

Share Information in a confidential way

Protect Sensitive Files	**Word 2003, PowerPoint 2003 Excel 2003, Windows RMS**	**•Control access to sensitive plans •Set level of access: view, change, print, etc. •Determine length of access**
Do-Not-Forward Email	**Outlook 2003 Windows RMS**	**•Keep Executive e-mail off the Internet •Reduce internal forwarding of confidential information •Templates to centrally manage policies**
Safeguard Intranet Content	**IE w/RMA, RMS SDK Windows RMS**	**•Safeguard financial, legal, HR content •Set level of access: view, print, export •View Office 2003 rights protected info**

Instalace

- Modifikace schematu:
- Setup /forestprep
- Setup /domainprep

- Admin nástroje se už nedají jednoduše spouštět z XP klienta
- Neinstalovat klienta exch a outlook na jeden poč.
- Před upgradem z w2000 na w2003 nainstalovat exchange
- Vytvořit si účet pro Exchange full administratora
- Musí být funkční AD a DNS

minimum	doporučeno
Pentium 233	Pentium 1,6 Více procesorů
256 MB RAM	3 až 4 GB RAM
W2000 SP3 W2003 server	W 2003 ent. edition

Administrátorské nástroje

- Exchange System Manger
- Active Directory Users and Computers
- Cluster Administrator
- ADSI EDit
- LDP utilita
- Active Directory Schema snap-in
- IIS snap-in
- DNS snap-in

Administrátorská oprávnění

oprávnění	**Co můžete dělat**	**Kdo by měl mít tuto roli**
Exchange full administrator	Plně administrovat Exch včetně práv.	Administrátor, který musí nastavovat a řídit přístup na email systém.
Exchange administrator	Plně spravovat exchange, ale nemůže měnit oprávnění.	Lidé zodpovědní za běžný provoz.
Exchange view only administrator	Pouze prohlížet exchange konfiguraci.	Admin, který si může prohlížet nastavení ale nesmího měnit. Vhodné pro audit.

System policies

- Systémové politiky se používají pokud je třeba konfigurovat složitejší prostředí. Pokud je jenom jeden server nejsou důležité.

Store a Storage groups

- Storage groupa zahrnuje story – tj. Db ve kterých se ukládají emaily atd.
- Entr. Server může mít 5 storage group
- Z toho jedna slouží pro obnovu
- Lepší je tvořit více malých storů pro rychlejší obnovu, backup
- Pro VIP uživatele udělejte samostatný store
- Data s různými požadavky na obnovu dávejte do různých storů.
- Každá storage skupina by měla mít vlastní vyhrazený disk pro logy.
- Uživatelé ze stejných oddělení by měli být v stejných skupinách

Zabezpečení

- Digitální podpisy
- Šifrování

Exchange a porty pro firewall

port	služba
25	SMTP
80	HTTP
88	Kerberos autent. protocol
102	MTA X.400 konektor přes TCP/IP
110	POP3
119	NNTP
135	client/server komunikace, RPC, exchange administrace
143	IMAP
389	LDAP
443	HTTP (SSL)
563	NNTP (SSL)
636	LDAP (SSL)
993	IMAP4 (SSL)
995	POP3 (SSL)
3268 a 3269	Global catalog lookups

RFC

- HTTP 1945, 2068
- SMTP 2821, 2822
- NNTP 977
- POP3 1939,1743
- IMAP4 2060
- www.rfc-editor.org/rfc.html

Administrative groups vs Routing groups

- Admin groups – skupina exch. objektů které jsou sdruženy za účelem správy a delegace oprávnění
- Může obsahovat: servery,routing groups, policies, public folders (veřejné složky)
- Routing groups – servery podle lokalit

Typy objektů

Uživatel
- Mail enabled
- Mailbox enabled

Kontakt
- Mail enabled

Skupina
- Mail enabled

Hromadné úpravy v AD

- CSVDE.exe
- LDIFDE.exe

jmenosouboru.csv →
← Jmenosouboru.ldf
AD

Různé

Skryté mailboxy
- Mailboxy na které můžete posílat zprávy ale které nejsou vidět v adresáři

Remapování účtů

Send on behalf
- Posílání zpráv v zastoupení, např. sekretářka za ředitele

Storage limits – omezení dat

- Issue warning at
- Prohibit send
- Prohibit send and receive

Nastavuje se buď individuálně nebo přes mailbox store policy.

Přesun mailboxů

- Ručně pomocí exchange task wizardu
- Pomocí utility Exmerge.exe – vhodné když je třeba přesunovat mezi různými organizacemi

Query-based distribution group

- Distribuční skupiny, které samy vytvářejí svůj obsah (členství) na základě dotazu
- Jsou dynamické, ulehčují administraci
- Servery Exchange musí mít nativní mód 2003
- Jsou náročné na výkon serveru

Omezení posílání pošty na distr. skupiny

- Skupina se může skrýt z adresáře
- Na skupinu se nastaví omezení – tj. určí se kdo na ni může posílat zprávy (které účty).

Veřejné složky – Public folders

- Slouží k umístění společných dat
- Mohou obsahovat data, kalendáře, úkoly, popř. vlastní aplikace
- Lze na ně poštu rovnou zasílat z venku i zevnitř
- Jsou přístupné i přes web
- Pozor na práva na vytváření „top level“ složek
- Nastavují se na ně oprávnění – editor, owner, reviewer, author
- Veřejné složky lze replikovat mezi servery
- Lze je full text indexovat

Připojení na exchange přes internetové protokoly pro klientský přístup

- Jaké protokoly můžeme použít: POP3,IMAP4,HTTP,NNTP,LDAP
- Front end, back end servery
- Zabezpečení komunikace mezi FE a BE - IPSec

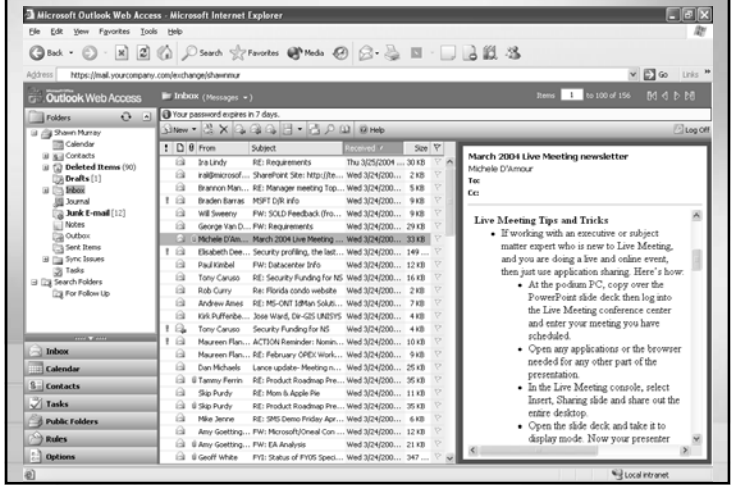
OWA – Outlook web access

- Přístup k poště přes webové rozhraní
- Dvě verze
- Premium – poskytuje všechny OWA možnosti, potřebuje MS IE 5.0 a výše
- Basic – poskytuje podmnožinu funkcí, funguje v libovolném browseru
- Doporučeno používat v kombinaci se SSL

Nový Outlook Web Access (OWA)

- Anywhere Access – vylepšená práce s Outlook Web Accessem (= přístup přes čistý webový prohlížeč)
  - Nový uživatelský vzhled jako Outlook 2003
  - Rychlejší (až o 80% rychlejší oproti předchozí verzi): komprese gZip, využití mezičasu (idle) na stahování prvků, inteligentní synchronizace
  - Bezpečný: Public/Private options, S/MIME, časované odhlášení, blokování příloh, blokování externích HTML
- Tuny nových vlastností – vše co máte rádi v Outlooku
  - Slovníky, úkoly, serverová pravidla, označení příznaku přečtení
  - Třídění a ‘type down’, zobrazení až 100 zpráv najednou
  - Vícebarevné označování příznaků, pohledy na vyhledávání
  - Podokno pro čtení na pravé straně a 2 řádky v náhledu
  - Automatické formátování HTML rámců

OWA 2003 Premium Client



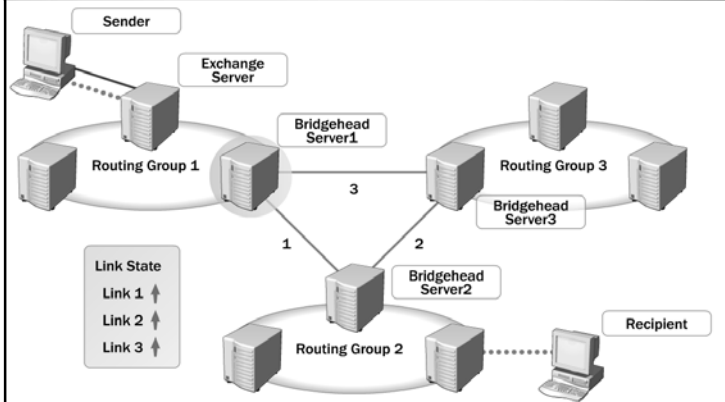
Připojení Outlooku k Exchange

- Cached – kopie uživatelova mailboxu je lokálně uložená a exchange server ji často aktualizuje. Uživatel má přístup k online zdrojům.
- Online – data jsou uložena na serveru. Uživatel má trvalý přístup k síti.
- Offline – uživatel nemá trvalý přístup k síti. Pro připojení k exchange používá dial up nebo VPN. Typický mód pro mobilní uživatele.

Routing

- Routing groups
- Routing group connector
  - Routing group connector – default konektor v rámci stejné organizace. Používá taky SMTP protokol.
  - SMTP connector – spojení mezi dvěmi routing group nebo mezi rout. group a SMTP serverem
  - X.400 connector
- Bridgehead server
  - Slouží jako server přes který ostatní z groupy komunikují s okolím

Routing



SMTP

- Jak SMTP a ESMTP funguje
- HELO, MAIL FROM:, RCPT TO:, DATA, RSET, VRFY <string>, HELP, QUIT, TURN

- DNS
  - MX záznam

    MX 10 smtp1.nwtraders.msft

    MX 20 smtp2.nwtraders.msft

Péče o data

- Exchange má dva typy logování
  - Cirkulární nebo standardní
- Data store – je možný mount a unmout
- Před tím než smažu data store je třeba přesunout uživatele na jiný
- Zálohování
  - Lze využít ntbackup nebo sw třetí strany - Veritas, CA Brightstore, Legato Networker, HP Omnibackup, IBM Tivoli atd.

Disaster recovery

- Plán záloh
- Plán pro obnovu
- Vytvoření fault tolerantního prostředí
- Pozor na SPOF
- Nezapomenout i na zálohu AD

- Data jdou obnovit do určité doby i z klienta

Denní údržba

- Kontrola event logů
- Kontrola výkonu
- Kontrola exchange front
- Kontrola backupů

Tuning výkonu

- Když má exchange server 1 GB paměti a více přidejte do boot.ini přepínač /3GB
- Tento přepínač nedávejte pokud to běží na W2000 serveru
- Pokud běží E2003 na W2003 přidejte ještě /USERVA=3030
- Nastavte registry podle MS Knowledge Base článku s ID 815372. http://support.microsoft.com/?id=815372

Defragmentace

- Online probíhá automaticky za provozu
- Offline – eseutil /d
- Ověření integrity dat - Isinteg
- Varování: pozor na to – je to nebezpečné pokud nevíte přesně co chcete. Hlavně si před tím udělejte zálohu!!!

Diskuze