Uvod v Windows Server 2003, Standard Edition

Cilji

Ugotoviti ključne lastnosti posameznih platform družine Windows Server 2003 Razumevanje prednosti uporabe Windows XP Professional na omrežju Windows Server 2003

Razumevanje lastnosti strežniškega operacijskega sistema Windows Server 2003

Planiranje modela omreženja z Windows Server 2003

Razumevanje protokolov, ki so najbolj primerni za Windows Server 2003

Izvajanje TCP/IP na Windows Server 2003

Računalnikove vloge (Computer Roles) Družina Windows Server 2003

Windows Server 2003, Standard Edition

Datotečne in tiskalne storitve

Varna internetna povezljivost

Centralizirano opravljanje omrežnih sredstev

Podpira do 2 procesorja na računalnikih SMP

Lahko imamo do 4 GB pomnilnika RAM

Windows Server 2003, Web Edition

Podpira do 2 procesorja

Uporablja do 2 GB pomnilnika RAM

Optimiz iran za izvajanje Microsoft Internet Information Services

Ne more upravljati sredstev omrežja preko gostiteljska aktivnega imenika (“ ActiveDirectory”)

Windows Server 2003, Enterprise Edition

Podpira do 8 procesorjev

Podpira do 32 GB za računalnike x86 in do 64 GB za računalnike Itanium

Omogoča gruče z do 8 računalniškimi vozli

Podpira “ hot-add memory ”

Nudi “ Non-Uniform Memory Access ” (NUMA) in “ Microsoft Metadirectory Services ”

Windows Server 2003, Datacenter Edition

Podpira 8 do 32 proces orjev

Možnost gruč z 8 računalniškimi vozli

Uporaba do 64 GB za računalnike x86 in 128 GB za procesorje Itanium

Podpira “ hot-add memory ”

Načrtovan za aplikacije z velikimi podatkovnimi bazami

Windows XP Professional

Odjemalec (klijent) je računalnik, ki dostopa do sredstev drugega računalnika .

Delovna postaja (workstation) je računalnik z lastno CP E .

XP Professional je delovna postaja – odjemalec, ki je najbolj kompatibilna z Windows Server 2003

Zagotavlja nizko “ total cost of ownership ” (TCO)

Avtomatsko nameščanje in konfiguracija, krmiljena z Windows Server 2003

Kompatibilnost z upravljalsko bazo “ Active Directory ”

Lastnosti Windows Server 2003

Centralizirana administracija in upravljanje s sredstvi

Varnost

S kalabilnost in kompatibilnost

Zanesljivost in porazdeljivost

Strpnost do napak in reševanje

Centralizirana administracija in upravljanje s sredstvi

Servis “ Active Directory ” (aktivni imenik) upravlja s sredstvi omrežja .

Do o bje ktov, hranjenih v Aktivnem imeniku lahko vsi uporabniki preprosto dostopajo .

Obje kti so združevani v enote, domene, drevesa, gozde in lokacije (units, domains, trees, forests, sites) .

Daljinska administracija sistema preko ene centralne lokacije

Varnost

Dovoljenja za datoteke in direktorije

Varnostne politike

En kripcija in overovljenje (authentication)

Pregled dogodkov (Event auditing)

Upravljanje s strežnikom in orodja za nadzor

Skalabilnost in kompatibilnost

Razširljivost na večprocesorske sisteme

Podpora povezave več uporabnikov

Do 15 . 000 v izvedbi “ Standard Edition ”

Kompatibilnost z različnimi operacijskimi sistemi in platformami

IBM, Novell, UNIX, Linux, Banyan, DEC, Macintosh

Zanesljivost

Jedro (k ernel) teče v privilegiranem režimu

Legacy applications se izvajajo na virtualnem DOS stroju

Podpora sočasnim programom (m ultitasking)

Več programov lahko poteka sočasno

Predkupnost (p reemptive multitasking) loči pomnilne naslovne prostore posameznih programov

Podpora večnitnim programom

Zmožnost večkratnega sočasnega izvajanja delov programske kode

Porazdeljivost

Računalniške funkcije so lahko porazdeljene med različnimi računalniki

Uporaba “ Distributed Component Object Model ” (DCOM)

Programske komponente lahko komunicirajo preko omrežja .

Programske aplikacije so lahko združene preko več računalnikov .

Strpnost do napak in reševanje

Reševanje pri izpadov trdih diskov preko RAID

Zaščita pred izgubo podatkov s pomočjo rezervnih kopij (backup)

Reševanje pri napakah v konfiguraciji sistema

Zaščita pri izpadih električnega napajanja

Napredno opozarjanje o sistemskih in aparaturnih problemih

Načrtovanje modela omreženja z Windows Server 2003

Omrežja so komunikacijski sistemi, ki povezujejo računalnike in njihova sredstva .

Fizična povezava je z ožičenjem ali z brezžičnimi napravami

Omrežja so lahko lokalna ali globalna

Windows Server 2003 izvaja dva tipa omrežij .

Omreženje “ Peer-to-peer ” razprši administracijo med vsemi člani .

Omreženje, temelječe na strežniku, centralizira administracijo omrežja .

Omreženje med enakovrednimi računalniki (“Peer-to-peer”)

Namenjeno do 10 računalnikom

Le zmerna omrežna varnost

Uporabniki sami upravljajo s svojimi konti.

Ni centraliziranega pomnenja podatkov

Ni centraliziranega nadzora administracije

Pomanjkanje upravljanja z uporabniki in kritičnimi datotekami

Nezmožnost centralnega shranjevanja rezervnih kopij pomembnih datotek

Slabši odzivni časi pri souporabi sredstev

Omrežja, osnovana na strežniku

Uporabniki se za dostop do sredstev prijavijo (log in) le enkrat.

Boljša varnost zaradi upravljanja s strežnikom

Člani souporabljajo datoteke

Souporaba tiskalnikov in drugih sredstev

Zmožnost elektronske pošte preko strežnika elektronske pošte

Hramba aplikacij na centralni lokaciji

Rokovanje z varnostnimi kopijami (backups) planirano in izvajano s centralne lokacije

Pri souporabi sredstev lahko opoštevamo delovne navade podskupin.

Bolj učinkovito ažuriranje programske opreme

Proto koli za omrežni model z Windows Server 2003

Protokol je skupina komunikacijskih navodil za :

Oblikovanje podatkov v pakete in okvirje

Prenos paketov in okvirjev po omrežjih

Interpret acija paketov in okvirjev na točki sprejema

Najbolj pogosto uporabljen je “ Transmission Control Protocol/ Internet Protocol (TCP/IP) ” .

Uporaba pri spletnih komunikacijah

Načrtovan kot odprt standard

Povezuje računalnike, na katerih teče večina OS

Protokoli na Windows Server 2003

TCP/IP je privzeto nameščen na Windows Server 2003

Tudi IP v6 in IPX (NWLink)

NetBEUI ni več podpiran

Družina protokolov TCP/IP

TCP/IP je v resnici družina protokolov, ki ji pravimo ***“Internet Protocol Suite”***

Družina vsebuje protokole za nizko nivojsko naslavljanje in posredovalne funkcije (TCP in IP), kot tudi protokole za določene funkcije v zgornjih plasteh, kot na primer elektronska pošta in prenos datotek (SMTP and FTP)

Transmission Control Protocol

Nudi “ connection-oriented ” komunikacijo

Zagotavlja, da so paketi posredovani v pravem zaporedju in s pravo vsebino

Krmili pretok podatkov glede na promet v omrežju

Posluša komunikacijske zahtevke in vzpostavlja seje

Rokuje s prenosom in sprejemom podatkov

Zapira seje prenosa

Internet Protocol

Nudi spletno naslavljanje

Usmerja podatke preko različnih omrežij

Usmerjevalnik (router) bere IP naslove in posreduje pakete ustreznemu omrežju .

Rokuje s fragmentiranimi paketi

Connectionless

Temelji na TCP za zagotavljanje “ connection- oriented communication ”

IP - Internet Protocol

IP nudi naslavljanje na nivoju omrežja

Nudi tudi fragmentacijo in ponovno združevanje paketov

Servisi TCP

TCP nudi zagotovljeno posredovanje tako, da vzpostavi “*virtualno povezavo*” med pošiljateljem in prejemnikom. Taki virtualni povezavi pravimo “between socket.”

IP naslavljanje

Vsaka naprava v omrežju IP je razpoznavna po enostranskem naslovu, ki mu pravimo ***IP-address.***

Naslovi so 32 bitni in razdeljeni v 4 osem- bitne oktete.

IP naslovi

Dolgi 32-bit ov , s 4 polji desetiških vrednosti, ki predstavljajo 8-bit ne dvojiške oktete

Primer : 10000001.00000101.00001010.01100100 ustreza v desetiški obliki 129.5.10.100

Razdeljeno v identifikator omrežja in identifikator naprave glede na naslednje dejavnike :

Velikost lokalnega omrežja (LAN)

Ali je LAN razdeljen na manjša omrežja

Tip prenosa

Klasifikacija IP naslovov

Razred	Območje	# omrežij	# računalnikov
A	0 - 127	27	6,777,216
B	128 - 191	6,384	65,534
C	192 - 223	2,097,152	254

IP naslovi (nadaljevanje)

Tipi prenosov

Unicast: Pošlje strežnik vsakemu klijentu, ki pošlje zahtevek

Multicast: Pošlje strežnik enkrat (sočasno) vsem klijentom, ki to zahtevajo

Broadcast: Pošlje strežnik vsem na omrežju

Subnet masks

Prikazuje razred naslova

D eli omrežje na podomrežja

Primer : Subnet mask za naslove razreda A: 255.0.0.0

Maske podomrežij (Subnet Masks)

Podomrežja (Subnetting)

Pogosto je število vozlov, ki jih podpira ena IP podmaska, preveliko za posamezno organizacijo (na primer 65534 vozlov za eno podmasko razreda B). Organizacija lahko razbije število v manjše kose.

Subnetting je deljenje omrežnega števila enega razreda A, B ali C v manjše kose.

Subnetting a Class B

O naslovih IP ...

127.0.0.0 ne sme uporabljati nobeno omrežje .

127.0.0.1 je naslov " loopback " .

Določeni naslovi so rezervirani za privatno uporabo v omrežju (glej tabelo 1-2).

Omrežne številke ne moremo dodeliti računalnikom .

Najvišja številka v omrežju je rezervirana za sporočila " broadcast " .

Statično in dinamično naslavljanje

Stati čno naslavljanje dodeljuje računalniku stalnen, edinstven naslov .

Omogoča administratorju direkten nadzor

Uporabno za nadzor omrežja

IP naslove moramo pomniti v primerni podatkovni bazi

D inamično naslavljanje dodeli računalniku IP naslov vsakokrat, ko ga prijavimo .

Najem za določeno časovno obdobje

Uporaba " Dynamic Host Configuration Protocol " (DHCP) ,

Privzeti " Gateway "

IP naslov omrežnega usmerjevalnika, ki povezuje na druga omrežja

U porabljamo, ko je ciljni računalnik na drugem omrežju

Imena IP

IP naslovi so morda lahko za računalnike, ljudje pa raje uporabljamo imena.

http://www.fri.uni-lj.si raje kot http://193.2.104.250

To naredimo z:

Tabelami "Host lookup" na vsakem stroju

- ali -

Strežnikom "Domain Name Server" (DNS)

Datoteka "Hosts"

Na posameznih računalnikih lahko za preslikavanje IP naslovov v imena uporabimo tekstovno datoteko

Z milijoni računalnikov na spletu je take datoteke težko vzdrževati.

Resolucija imena

Ljudje torej računalnike običajno naslavljamo z imenom in ne z IP naslovi.

TCP/IP uporablja pri povezovanju IP naslove.

NetBIOS imena uporabljajo stari sistemi.

Za resolucijo uporabimo Windows Internet Naming Service (WINS) ali datoteke LMHosts.

Imena računalnikov uporabljamo za računalnike v omrežjjih, ki uporabljajo "" Domain Name System" (DNS).

Za resolucijo uporabimo "Dynamic Domain Name System" (DDNS).

Domain Name System

DNS je porazdeljena podatkovna baza, ki vsebuje imena oziroma naslove vseh računalnikov, ki so dosegljivio na spletu.

Posebni strežni računalniki, imenovani "***name-servers*** " imajo nalogo pomnenja tabel za preslikavo DNS imen v IP naslove.

Pri MS Windows so zapisi DNS lahko integrirani v ***Aktivnem imeniku***

Hierarhija DNS

Domenski strežniki najvišjega nivoja so za arpa, com and edu itd.

Posamezne organizacije vzdržujejo lokalne imenske strežnike

Fizični naslovi in protokol za resolucijo naslova

Vsak računalnik ima fizični naslov, ki je definiran z njegovo omrežno kartico "network interface card" (NIC).

Fizičnemu naslovu pravimo naslov "media access control" (MAC).

TCP/IP temelji na naslovih IP in MAC.

Naslove dobimo s pomočjo protokola "Address Resolution Protocol" (ARP).

ARP medpomnilnik (cache) vsebuje že ugotovljene in statične MAC naslove.

ARP pošlje paket, ki zahteva naslov MAC, če ta ni v medpomnilniku.

Address Resolution Protocol

Da lahko ena naprava pošilja drugi, moda pošiljatelj poznati fizični ali MAC naslov prejemnika.

Vsaka naprava vzdržuje medpomnilnik ***ARP Cache***, v katerem pomni prej ugotovljene naslove lokalnega omrežja.

Če je naslov neznan, pošlje računalnik "**ARP** broadcast" da bi ugotovil naslov.

IzvajanjeTCP/IP na Windows Server 2003

Je privzeto nameščen na Windows Server 2003

Lahko ga namestimo kot katerikoli drugi protokol

Konfiguriranje TCP/IP

Izbira o statičnega ali dinamičnega naslavljanja .

Za usmerjevalnike, strežnike in za sledenje omrežnim problemom .

Stati čno naslavljanje lahko izvedemo ročno, vendar pozor na napake!! .

Windows Server 2003 podpira avtomatično naslavljanje .

Automatic Private IP Addressing (APIPA)

D inamično naslavljanje z uporabo strežnika DHCP

Automatsko naslavljanje privatnih IP

V "Protocol Properties" izberi možnost "Obtain an IP address automatically".

Če ni na voljo strežnika DHCP, je naslov IP dodeljen v območju 169.254.0.1 to 169.254.255.254.

Računalnik lahko komunicira le z drugimi, avtomatsko konfiguriranimi računalniki na istem omrežju.

Prepreči avtomatsko konfiguriranje preko registra (registry), vendar bodi previden.

Dinamično s pomočjo strežnika DHCP

Namesti in konfiguriraj en strežnik DHCP.

DHCP olajša administracijo z dodeljevanjem:

IP naslova

Subnet mask

Privzete gateway

DNS strežnika

V "Protocol Properties" izberi "Obtain an IP address automatically".

Souporaba datotek na Windows

Ena od osnovnih uporab strežnika "Window server" je kot ***datotečni strežnik (file server)*** – centralizirano pomnenje datotek preko "***shares***".

Preglej "My Network Places"

NET USE

\\servername\sharename

C$, D$ itd – **Text body indent** administrative shares

Povzetek

Platforme Windows Server 2003

Standard Edition

Web Edition

Enterprise Edition

Datacenter Edition

Značilnosti Windows Server 2003

S kalabilnost

Učinkovitost

Dve vrsti modelov omreženja

Peer-to-peer

Osnovano na strežniku

TCP/IP

Privzet protokol, nameščen na Windows Server 2003

Zahteva ga " Active Directory "

Serija protokolov in služnostnih programov (utilities)

Omogoča komunikacijo med lokalnimi in globalnimi omrežji

IP naslavljanje

Za vsak računalnik edinstven naslov

Sestavlja ga identifikator omrežja in identifikator računalnika

Dodeljena mu je tudi maska " subnet mask "

Konfiguriranje naslovov IP

Stati čno

Automati čno z uporabo APIPA ali dinamičnega naslavljanja preko DHCP

Namestitev WS Server 2003Standard Edition

Cilji

Priprava na namestitev Windows Server 2003

Razlaga in izvedba različnih namestitvenih metod Windows Server 2003, kot na primer spremljana in nespremljana (attended, unattended) in nadgradnje

Namestitev in upravljanje "service packs"

Kako tvorimo "Automated System Recovery set"

Reševanje problemov pri nameščanju

Kako odstranimo Windows Server 2003, Standard Edition

Priprava na namestitev

Spoznajmo zahtevke za aparaturno opremo in kompatibilnost .

Izberemo datotečni sistem .

Izberemo način licenciranja .

Določimo, katere protokole bomo namestili .

Določimo članstvo v domeni ali delovni skupini " workgroup " .

Zahtevki za aparaturno opremo

Kompatibilnost aparaturne opreme

Preveri HCL za Windows Server 2003.

HCL je " hardware compatibility list " in jo najdemo na spletnih straneh Microsoft.

Pri komponentah pazi na logotip "Designed for Windows Server 2003".

Če je potrebno, nadgradi BIOS.

Ugotovi verzijo BIOS.

Pri proizvajalcu preveri, kako je s kompatibilnostjo in ali nudi datoteke za nadgradnjo.

Določimo opcije za particije diska

Vzpostavitveni (setup) program ugotovi trenutne particije.

Setup predstavi možnosti za razdelitev trdega diska na particije.

Create a new partition on an unpartitioned hard disk.

Only create the operating system partition during Setup.

Add other partitions with Disk Management later.

Create a new partition on a partitioned hard disk.

Install on an existing partition.

Delete an existing partition.

Pri nadgradnji iz "WS Server" preveri particije z " Disk Management Snap-in".

Opcije particij na disku

Izbira datotečnega sistema

Datotečni sistemi vplivajo na format diska.

Windows Server 2003 podpira FAT16, FAT32 inNTFS.

Priporočljiv je NTFS, saj ima napredne značilnosti, kot:

Varnost in enkripcija

Kompresija datotek

Podpora POSIX

Indeksiranje

NTFS je nujen za uporabo Active Directory.

Še o datotečnih sistemih

Uporabi konverzijski program za prehod iz FAT32 na NTFS po namestitvi.

Izbira načina licenciranja

C lient access license (CAL).

CAL da odjemalcu dovoljenje za povezavo z računalnikom z Windows Server 2003.

Dva načina licenciranja :

Na strežnik

Na sedež

"Na sedež" je bolj primerno za organizacije z enim strežnikom .

Izbira protokola

Privzeta namestitev protokola :

TCP/IP s predpostavko strežnika DHCP

Uporablja večina omrežij

Dodatne protokole lahko konfiguriramo po namestitvi .

Windows Server 2003 oziroma Windows XP Professional ne podpirata NetBEUI.

Pred nadgradnjo je potrebna konverzija na TCP/IP.

Določitev članstva

Delovna skupina (Workgroup)

Podati moramo ime delovne skupine .

Domena (Domain)

P odati moramo DNS ime domene .

Tvoriti moramo računalniški konto .

Na voljo moramo imeti en domenski kontroler in en strežnik DNS.

Pregled namestitve

Metode

CD

Omrežje

Nadgradnja

Brez spremljave (Unattended)

Namestitvene datoteke

Winnt za CD-ROM ali namestitev preko omrežja oziroma za operacijske sisteme Windows, predhodnike "Windows 95"

Winnt32 za operacijske sisteme "Windows 95" oziroma novejše od njega

Pri Windows NT moramo imeti "Service Pack 5" ali novejšega.

Stikala (Switches)

Winnt in Winnt32 podpirata prilagoditev namestitve s pomočjo stikal.

/s

Določa lokacija namestitvenih datotek

/a

Sproži "accessibility options"

/checkupgradeonly

Preverja kompatibilnost

/?

Pomoč v ukaznih vrsticah

Namestitev z uporabo CD

Preveri, ali računalnik (boot) s CD.

Vstavi namestitveni CD v pogon .

Ugasni računalnik .

Vklopi računalnik in tako sproži zagon s CD.

Nega programa .

Namestitev preko omrežja

Kopiraj namestitvene datoteke na gostiteljski računalnik.

Na gostiteljskem računalniku najprej naredi souporaben direktorij (shared network folder).

Souporabni direktorij na gostiteljskem računalniku naj ima dovoljenje za branje.

S ciljnega računalnika se poveži s souporabnim direktorijem.

Poženi Winnt.exe oziroma Winnt32.exe in pri tem navedi zaželena stikala.

Sledi namestitvenim navodilom.

Nadgradnja z obstoječega operacijskega sistema

Možne so nadgradnje z naslednjih operacijskih sistemov:

Windows NT Server 4.0 (ki ima Service Pack 5 ali novejši)

Windows 2000 Server

Koraki nadgradnje:

Zaženemo obstoječi operacijski sistem.

Vstavimo namestitveni CD.

V namestitvenem zaslonu izberemo med možnostmi nadgradnje.

Obdržimo obstoječe nastavitve in aplkacije.

Namestitev brez spremljanja

Običajno jo izvajamo pri namestitvi preko omrežja

Pred namestitvijo specificiramo množico parametrov v datoteki z odgovori .

Datoteka z odgovori vsebuje odgovore na vprašanja, ki jih sicer dobivamo med nameščanjem .

Med nameščanjem ne pride do spraševanja po licenci .

Izvajanje spremljane namestitve preko CD

Računalnik zaženemo s CD "Standard Edition".

Postopek namestitve je podoben pri vseh metodah.

Prva faza namestitve:

Preglej datoteke za konfiguriranje in nalaganje.

Oglej si sporazum za licenco (license agreement).

Preglej trdi disk in ugotovi OS, particije in datotečne sisteme.

Izberi particijo in datotečni sistem.

Izbrana particija bo formatirana v skladu z izbranim datotečnim sistemom.

Izvajanje spremljane namestitve preko CD (nadaljevanje)

Druga faza namestitve zahteva od uporabnika:

Nastavitev jezika, datuma, časa in omrežja

Registracijsko številko (Product Key)

Način licenciranja

Ime računalnika, Konto administratorja in njegovo geslo

Članstvo v domeni ali delovni skupini (Domain, workgroup)

Konec namestitve.

Namestitev in registracija izbranih komponent.

Namestitev elementov začetnega menuja (Start menu).

Pomnenje nastavitev in izbris začasnih (temporary) datotek.

Izvedba nespremljane namestitve

Tvorimo datoteko z odgovori.

Uporabimo urejevalnik besedil ali namestitveni čarovnik (Setup Manager Wizard).

Možnost z uporabo datoteke z odgovori pri zagonu

Datoteko z odgovori shranimo na disketo kot "Winnt.sif".

Računalnik zaženemo s CD.

Po prvem namestitvenem zaslonu vstavimo disketo.

Možnost za specifikacijo komponent

Tvorimo datoteko "Cmdlines.txt", ki naj jo uporabimo z odgovorno datoteko.

Uporabimo program Sysprep.exe ali Syspart.exe za kloniranje strežniških operacijskih sistemov.

Nadgradnja Windows NT Server in domene

Dve metodi:

Najprej nadgradimo članske strežnike.

Najprej nadgradimo domenske kontrolerje.

Navodila

Planiraj nadgradnjo v časih z najmanjšim dostopom.

Naredi kopije vsakega strežnika in "registry".

Naredi "emergency repair disk".

Če najprej nadgrajujemo domenske kontrolerje:

Vzamemo kot rezervno kopijo en BDC. **(backup domain controller??)**

Najprej nadgradimo PDC. **(Primary domain controller??)**

Nadgradnja Windows NT Server in domene (nadaljevanje)

Namestitveni koraki:

Sproži Winnt32.exe.

Med nameščanjem izberi nadgradnjo (Upgrade) in obdrži obstoječe nastavitve.

Nadgradi aktivni imenik s čarovnikom za namestitev "Active Directory".

Po namestitvi pretvori domeno v način bodisi "Windows 2000 native" bodisi "Windows .NET".

Namestitev in upravljanje " Service Pack "

Z Microsoftove spletne strani skopiraj zadnji service pack.

Redno preverjaj posodobitve (updates) in tako popravljaj varnostne probleme in izboljšuj performanco.

Pregledaj dokumentacijo o namestitvenih postopkih in problemih.

Izvedi popolno varnostno kopiranje (backup) strežnika.

Opozori klijente o planiranih namestitvah.

Po namestitvi dokumentiraj probleme in rešitve.

Tvorba " Automated System Recovery Set "

Zbirka ASR komponent za reševanje sistema:

Rezervne kopije vseh sistemskih datotek (najmanj 1.5 GB)

Rezervna kopija sistemskih nastavitev (približno 1.44 MB)

ASR ne dela rezervnih kopij aplikacijskih podatkov.

ASR narediš z uslužnostnim programom “Backup”.

Novo zbirko ASR naredi pred vsako pomembno spremembo na strežniku.

Dodajanje protokolov

Namestitev novih gonilnikov

Reševanje problemov pri nameščanju

Največ namestitvenih problemov je povezanih z aparaturno opremo in gonilniki naprav.

Precej problemom se lahko izognemo s testiranjem aparaturne opreme in izvajanjem diagnostike že pred namestitvijo.

Rešitve problemov najdemo s pomočjo dokumentacije.

Kako odstranimo Window Server 2003, Standard Edition

Naredimo rezervno kopijo pomembnih podatkov.

S pomočjo CD zaženemo nov operacijski sistem.

Računalnik lahko zaženemo tudi s CD za Windows Server 2003 in izstopimo iz nameščanja (Setup) potem, ko zbrišemo particijo

Računalnik ponovno zaženemo.

Izberemo brisanje oziroma formatiranje particije, kjer je bil nameščen stari operacijski sistem.

Namestimo nov operacijski sistem.

Povzetek

Naloge pred namestitvijo:

Preverimo kompatibilnost aparaturne opreme preko HCL.

Določimo konfiguracijo sistema.

Metode namestitve:

CD-ROM

Omrežje

Nadgradnja

Iz “Windows NT Server 4.0” s “Server Pack” ali novejšim, ali iz “Windows Server 2000 Server”

Nespremljana (unattended)

Namestitev avtomatiziramo s tvorbo datoteke z odgovori.

Nadgradnja domene Windows NT 4.0:

Začnemo s članskimi strežniki ali z domenskimi kontrolerji.

PDC moramo najprej nadgraditi.

Za odstranjevanje znanih problemov moramo namestiti “Service pack”.

Po namestitvi tvorimo zbirko ASR.

Odstranitev Windows Server 2003:

Ponovno preuredimo particije in formatiramo trdi disk.

Namestimo nov operacijski sistem.

Konfiguriranje in upravljanje z aparaturno opremo

Osnovna orodja

Čarovnik za dodajanje naprav – PNP

Upravnik naprav (Device Manager)

Profili aparaturne opreme

Podpisovanje gonilnikov (Driver Signing)

Konfiguriranje operacijskega sistema

Fino uglaševanje

Performančne opcije

Razvrščanje procesorja in uporaba pomnilnika

Navidezni (virtualni) pomnilnik

Pomnilnik za omrežno performanco

Okoljske spremenljivke (Environment variables)

Opcije pri zagonu in reševanju (Startup and recovery)

Opcije pri različnih vrstah napajanja (Power options)

Proto koli

Dodatne komponente Windows Server 2003

Namestitve s pomočjo orodja “ Add or Remove Programs ”

Uporabimo pri večini komponent, tako na primer za “ Web Application Server ” in za omrežne servise

Windows Server 2003 Registry

Kompleksna podatkovna baza, ki vsebuje vse podatke, ki jih o strežniku potrebuje operacijski sistem

5 osnovnih ključev

HKEY_LOCAL_MACHINE

Podatki o vseh aparaturnih komponentah

HKEY_CURRENT_USER

Podatki o namestitvi namizja za uporabnika, ki je trenutno logiran na konzoli strežnika

HKEY_USERS

Podatki o profilu vseh uporabnikov, logiranih na računalnik

HKEYS_CLASSES_ROOT

Podatki za asociacijo podaljškov datotek s programi

HKEY_CURRENT_CONFIG

Podatki o trenutnih profilih aparaturne opreme

Vsebina registra (nadaljevanje)

Bolj podrobno razdeljena na podključe in vhode

Vhodi

Trije deli:

Ime

Tip podatka

Konfiguracijski parameter

Trije formati podatkov:

DWORD je šestnajstiški

String je tekstovni podatek

Binary sta dve šestnajstiški vrednosti

Kaj so “ Administrative Tools ” ?

Pogosto uporabljana orodja za administracijo:

Active Directory Users and Computers

Active Directory Sites and Services

Active Directory Domains and Trusts

Computer Management

DNS

Remote Desktops

Namestimo in izvedemo oddaljeno administracijo

Kako namestimo “Administrative Tools”

Kaj je MMC?

Kaj je MMC

Kako tvorimo lasten MMC

Vaja : Konfiguriranje administrativnih orodij

Tvorba lastnega MMC , ki vsebuje naslednje :

Computer Management (lokalno)

Computer Management (sosednji računalnik)

Active Directory Users and Computers

Shranimo kot MMC na C:\MOC\ lasten MMC.msc

Reševanje problemov pri nameščanju in konfiguriranju administrativnih orodij

Konfiguriranje okolja Windows Server 2003

Cilji

Namestitev in konfiguracija naprav

Konfiguriranje okolja operacijskega sistema vključno s performančnimi opcijami, razporejanjem procesorja, uporabo pomnilnika, okoljskimi spremenljivkami, opcijami za zagon in reševanje, opcijami za napajanje in protokoli.

Razumevanje registra (registry) in uporabe urejevalnika registra (Registry Editor)

Konfiguriranje naprav

Naprave vključujejo :

Disk ovne pogone in CD pogone

Disk ovne krmilnike

Omrežne kartice (n etwork adapters)

Tipkovnice, monitorje, miške ipd.

Nameščanje in konfiguracija novih naprav z naslednjimi orodji :

Plug and Play

Čarovnikom za dodajanje naprav

Plug and Play (PnP)

A vtomatsko zazna in konfigurira novo nameščene naprave

Skoraj splošno podpiran

Da bi lahko PnP deloval , mora biti :

Vgrajen v napravo

BIOS ciljnega računalnika ga mora omogočati (enable)

Vgrajen mora biti v jedro operacijskega sistema računalnika

Čarovnik za dodajanje naprav

Kliče operacijski sistem, da naj uporabi PnP za odkrivanje novih naprav .

Namesti nove, PnP kompatibilne naprave in gonilnike naprav .

Razrešuje probleme, ki bi jih lahko imeli z obstoječimi napravami .

Do njega dostopamo preko nadzornega panoja (Control Panel) .

Konfiguriranje in upravljanje z napravami

Upravnik naprav (Device Manager)

Preverja konflikte med sredstvi

Pregleduje in spreminja lastnosti naprav

Profili naprav

Zbirka navodil, ki povedo operacijskemu sistemu, katere naprave naj požene in katere nastavitve naprav naj uporabi

Podpisovanje gonilnikov (Driver Signing)

Digitalni podpis, ki ga Microsoft za overovitev kompatibilnosti vključi v gonilnik in sistemske datoteke

Konflikti med sredstvi

Sredstva strežnika vključujejo :

Interrupt request (IRQ) line

Kanal za komunikacijo s CPE

Pri računalnikih s tehnologijo Intel tipično 15 IRQ lin ij

Naslov I/O

Naslov v pomnilniku, preko katerega prihaja do prenosa podatkov med komponento in procesorjem

Re zervirano območje pomnilnika

Konflikti med sredstvi (nadaljevanje)

Video prikazovalnik, vsak diskovni pogon, vsaka vrata, zvočna kartica, vsi uporabljajo posvečen IRQ.

Vsaka naprava potrebuje za izvajanje vhodno izhodnih operacij rezervirane naslove v pomnilniku.

Do konfliktov med sredstvi pri nameščanju novih naprav.

Za določanje in razreševanje konfliktov med napravami uporabimo “Device Manager “.

Profili naprav

Privzet profil naprav je tvorjen med nameščanjem Windows Server 2003.

V profilu je omogočena (enabled) vsaka nameščena naprava .

Za prenosne računalnike je pogosto ustvarjenih več profilov .

Z orodjem “ Device Manager ” za vsako lokacijo omogočimo ali onemogočimo določene naprave .

Podpisovanje gonilnikov

Pri nepodpisanih gonilnikih imamo tri možnosti:

Prezremo

Opozorilo (privzeta nastavitev)

Blokiramo

Podpis gonilnika nastavimo na opozorilo (warn) ali blokiranje (block)

Sistemska nastavitev naj privzeto velja za vse uporabnike

Podpisovanje gonilnikov velja tudi za vse nove namestitve programske opreme

To lahko prepreči zamenjavo (overwriting) sistemskih datotek

Podpisovanje gonilnikov (nadaljevanje)

Sistemske datoteke, ki smo jih pomotoma zamenjali, lahko restavriramo s sistemskim orodjem "System File Checker"

Lahko ga nastavimo, da se sproži pri zagonu sistema

Lahko ga ročno sprožimo z ukazom "sfc /scannow"

Uporabiti ga smemo le, ko drugi uporabniki niso logirani

Sigverif pregleda datoteke, če imajo podpise gonilnikov, vendar jih ne zamenja

Uporabimo ga lahko tudi, ko so drugi uporabniki logirani

Rezultate zapiše v datoteko z imenom sigverif.txt

Konfiguriranje operacijskega sistema

Performančne možnosti

Razporejanje procesorja in uporaba pomnilnika

Navidezni pomnilnik

Pomnilnik za performaso omrežja

Okoljske spremenljivke

Možnosti pri zagonu in reševanju

Možnosti pri napajanju

Proto koli

Razporejanje procesorja in uporaba pomnilnika

Razporejanje procesorja

Krmilimo, kako je procesor dodeljen programom

Privzeto velja " Background services "

Vsi programi dobivajo enak procesorski čas

Uporaba pomnilnika

Krmilimo, koliko pomnilnika je dodeljenega programom, koliko pa funkcijam strežnika

Privzeto velja " System cache "

Računalnik deluje kot omrežni strežnik

Navidezni pomnilnik

Za širjenje kapacitete RAM uporabljamo diskovni pomnilnik

Ko RAM prekoračimo, obravnavamo navidezni pomnilnik, kot da bi tam bil RAM

Uporabljamo tehniko ostranjevanja

Strani so podatkovni bloki, ki jih premikamo iz RAM v navidezni pomnilnik

Na računalnikih Pentium so bloki veliki 4 KB

Strani so kopirane nazaj v RAM, ko jih potrebujemo

Na disku imamo posebno datoteko za ostranjevanje "paging file", kjer je alociran navidezni pomnilnik

Navidezni pomnilnik

Začetna in največja velikost datoteke za ostranjevanje

Začetna velikost naj bo najmanj 1.5 velikosti RAM

Maksimalna velikost naj bo dvakratna začetna velikost

Datoteke za ostranjevanje ne smemo dati v zagonsko particijo (boot partition)

Datoteko za ostranjevanje damo na vsak disk (razen v zagonsko particijo)

Pri zrcaljeni množici (mirrored set) oziroma zvezku damo datoteko za ostranjevanje na glavni disk

Datoteke za ostranjevanje ne damo na "stripe set" oziroma zvezek ali na zvezek "RAID-5"

Performanca omrežja

Pomnilnik je razdeljen na funkcije strežnika in na omrežne povezovalne funkcije

Funkcije strežnika uporabljajo RAM in ostranjevanje

Aplikacijski programi , tiskanje , trenutno tekoči servisi

Omrežne povezovalne funkcije uporabljajo le RAM

Število uporabniških povezav v danem času

Če je pomnilnik zaseden , preveri omrežne pomnilniške parametre

Okoljske spremenljivke

Sistemske okoljske spremenljivke

Definirane s strani operacijskega sistema

Uporabljajo vsi uporabniki

Uporabniške okoljske spremenljivke

Definirane za vsakega uporabnika

Spremenljivke so nastavljene v naslednjem zaporedju:

Sistemske

Spremenljivke v autoexec.bat (razen spremenljivk poti (path))

Uporabniške

Spremenljivke poti (path variables) v autoexec.bat

Zagon in reševanje

Možno je spreminjanje datoteke Boot.ini

Boot.ini lahko spremenimo tudi ročno

Nudi navodila, kako se rešimo pri sistemskem izpadu

Zapisovanje dogodkov v sistemski log

Pošiljanje administrativnih opozoril

Zapisovanje razhroščevalnih (debug) podatkov v datoteko

Avtomatski zagon računalnika po sistemskem izpadu

Preprečimo avtomatski zagon, če hočemo zagotoviti delo na sistemu pred logiranjem uporabnikov.

Možnosti za napajanje

Privzeta shema napajanja je "Always On"

Monitor se izklopi po 20 minutah neaktivnosti

Trdi disk je stalno vklopljen

Privzeta nastavitev za gumb za izklop je "Shut down"

Režim "Standby" izklopi komponente računalnika, vendar nič ne zapiše na trdi disk

Režim "Hibernate" terja daljši čas za nadaljevanje, vendar zapiše na trdi disk

Neprekinljivo napajanje (UPS, Uninterruptible power supply)

V primeru Izpada električne energije zagotavlja baterijsko napajanje za omejen čas

Protokoli

NWLink IPX/SPX/NetBIOS kompatibilen prenosni protokol

Namestimo, če uporabljamo računalnike, starejše od NetWare 5.x

Konfiguriramo omrežno številko in"frame type"

Če imamo več kot en "frame type", moramo konfigurirati vsakega od njih.

Če se povezujemo na računalnik s sistemom NetWare kot strežnikom, določimo za vsak "frame type" interno omrežno številko.

AppleTalk

Ni potrebno konfigurirati "frame type" in omrežne številke

Dodatne komponente Windows Server 2003

Namestitev s pomočjo orodja "Network Connections"

QoS Packet Schedule

Nivoji zagotovljene dostave podatkovnihpaketov

Server Advertising Protocol (SAP)

Protokol, kompatibilen za klijente NetWare

Internet Connection Protocol

Uporabimo, če internetno povezavo souporablja več računalnikov

Namestitev s pomočjo orodja "Add or Remove Programs"

Uporabimo za največ komponent, kot so strežnik spletnih aplikacij ali omrežne storitve

Register Windows Server 2003

Kompleksna podatkovna baza, ki vsebuje vse podatke, ki jih operacijski sistem potrebuje o strežniku

Primeri:

Podatki o vseh aparaturnih komponentah

Podatki o nameščenih servisih Windows Server 2003, od katerih servisov so le-ti odvisni in v katerem vrstnem redu so pognani

Podatki o profilih uporabnikov in skupinski politiki

Podatki o trenutni in zadnje znani namestitvi, ki uporabljena pri zagonu računalnika

Register Windows Server 2003

Konfiguracijski podatki o uporabljani programski opremi

Podatki o licencah za programsko opremo

Konfiguracija parametrov nadzornega panoja (Control Panel)

Urejevalnik registra (Registry Editor) poženemo z izvajanjem Regedt32 ali Regedit

Za delo z registrom, moramo biti previdni

Omejimo dostopne pravice na določene administratorje

Spreminjanje stvari naj bo kot zadnja možnost

Pogosto delajmo varnostne kopije registra

Nikdar ne kopirajmo registra z enega sistema na drugega

Vsebina registra

Ključ

Kategorija ali oddelek podatkov

Pet osnovnih ključev (root keys) oziroma poddreves (subtrees) tvori primarno kategorijo v registru:

HKEY_LOCAL_MACHINE

HKEY_CURRENT_USER

HKEY_USERS

HKEY_CLASSES_ROOT

HKEY_CURRENT_CONFIG

Podključ

Ključ nižjega nivoja, ki vsebuje vhode ali podključe

Skupini podključev pravimo "roj" (hives)

Vsebina registra (nadaljevanje)

Vhod (Entry)

Podatkovni parameter, asociiran s karakteristikami programske ali aparaturne opreme pod danim ključem oziroma podključem

Primer: ErrorControl:REG_DWORD:0

Trije deli:

Ime

Podatkovni tip

Konfiguracijski parameter

Trije formati podatkov:

DWORD je šestnajstiški

String je tekstovni podatek

Binary sta dve šestnajstiški vrednosti

Korenski ključi registra

HKEY_LOCAL_MACHINE

Podatki o vseh aparaturnih komponentah

Korenski ključi registra (nadaljevanje)

HKEY_CURRENT_USER

Podatki o namestitvi namizja za (na konzoli strežnika) trenutno logirani konto

HKEY_USERS

Podatki o profilih vseh uporabnikov, ki so logirani na računalnik

HKEYS_CLASSES_ROOT

Podatki, ki asociirajo podaljške datotek s programi

HKEY_CURRENT_CONFIG

Podatki o trenutnih profilih aparaturne opreme

Povzetek

Windows Server 2003 nudi vrsto orodij za prilagoditev in optimizacijo strežnika kot za razreševanje problemov.

Sodobne računalniške naprave in operacijski sistemi podpirajo "Plug and Play" za avtomatsko detekcijo novo nameščenih naprav.

Nove naprave lahko dodajamo z opcijo "Add Hardware", konfiguriramo in upravljami s pomočjo orodja "Device Manager"

Podpisovanje gonilnikov omogoča blokiranje namestitve gonilnikov in drugih komponent, ki jih še ni testiral in odobril Microsoft.

Vedno uglasimo strežnik za najboljšed obnašanje tako, da konfiguriramo razporejanje procesorja in pomnilnika, navidezni pomnilnik in pomnilnik, uporabljan za omrežna orodja.

Načrtujmo tudi okoljske spremenljivke, zagon sistema in reševanje (recovery), možnosti napajanja in dodatne protokole.

Večino komponent Windows Server 2003 namestimo z orodji "Network Connections" in "Add or Remove Programs"

Register (registry) vsebuje podatke o konfiguraciji sistema, kar pa lahko zelo previdno spreminjamo z urejevalnikom registra bolje z možnostmi v nadzornem panoju "Control Panel"

Uvod v Aktivni imenik in upravljanje kontov

Cilji

Razlaga namena Aktivni imenik (Active Directory) in njegovih ključnih lastnosti

Opis vsebnikov (containers) v aktivnem imeniku

Razumevanje upravljanja uporabniških kontov

Razlaga urnosti in izvajanje skupinske varnosti

Izvajanje profilov uporabnikov

Kaj je " Directory Service " ?

Identificira sredstva

Nudi konsistenten način za: poimenovanje,opisovanje,lociranje,dostop,upravljanje,varovanje

Zakaj aktivni imenik?

Servis, ki hrani podatke o vseh omrežnih sredstvih

Centralizirano upravljanje omogoča hitro iskanje in dostop do sredstev

Terminologija aktivnega imenika

Uvod v aktivni imenik

Hierar hična organizacija elementov nudi možnost nadzora dostopa uporabnikov

Na voljo " Windows 2000 Server " in " Server 2003 "

Strežniki Windows NT uporabljajo podatkovno bazo SAM (Security Account Manager)

Aktivni imenik je v primerjavi s SAM izboljšava :

Nudi popolno upravljanje vseh sredstev

Omogoča zapisljive kopije na vseh domenskih kontrolerjih

Terminologija aktivnega imenika

Objekt

Omrežno sredstvo (Network resource), definirano v domeni

Ima posebne atribute in lastnosti

Vsebnik (Container)

Objekt, ki vsebuje druge objekte

Domena

Osnovni vsebovalnik, ki vsebuje skupino objektov - sredstev

Krmilnik domene (Domain controller,DC)

Strežnik Windows 2003, ki vsebuje polno kopijo podatkov aktivnega imenika

Aktivni imenik je porazdeljen

Porazdeljenost pomeni, da je podatkovna baza AD razdeljena na **directory partitions**

Vsaka particija vsebuje

Shemo celotnega gozda

Konfiguracijo gozda (metadata)

Razdelke imenika po domenah (aktualni objekti)

Omogoča razdelitev in porazdelitev delov podatkovne baze AD zaradi bolj učinkovitega omrežja, predvsem za..

Hitrejše logiranje

Zmanjšanje prometa pri replikacijah

Vsak DC ima podatkovno bazo **Ntds.dit**, ki pomni podatke AD (aktivnega imenika).

Replikacije aktivnega imenika

Kopije Multimaster

Vsaka sprememba na enem DC se skopira (replication) na druge DC

Če en DC izpade, ni vidne prekinitve omrežja

Kopiranje lahko nastavimo na določene intervale namesto takojšnjega kopiranja, ko pride do spremembe

Omrežni promet zaradi kopiranj lahko zmanjšamo s:

Kopiranjem posameznih lastnosti namesto celotnih kontov

Kopiranjem, osnovanim na hitrosti omrežnih povezav

Bolj pogosto kopiramo preko lokalne mreže (LAN), kot preko globalne (WAN)

Replikacije aktivnega imenika

Replikacija *je način, kako se spremembe v aktivnem imeniku posredujejo med vsemi domenskimi krmilniki (DC, domain controllers) v gozdu (forest).*

AD replikacija je **multi-master** replikacija

Noben domenski krmilnik ni "glavni". Vsak DC je zapisljiv (writable) in lahko sprejme posodobitve podatkov.

Konflikti med posodobitvami se rešujejo po principu "zmaga zadnji pisalec"

Latenca – Zavedati se moramo, da je za to, da posodobitve dosežejo vse DC v gozdu, potreben čas. V danem trenutku se lahko zgodi, da aktivni imenik ni konsistenten.

Namestitev aktivnega imenika

Windows 2003 server naj postane DC z namestitvijo aktivnega imenika

Za spopolnjenje namestitve mora biti na voljo strežnik DNS

Shema (schema)

Shema je opis (ali slika ali diagram) struktur podatkovne baze.

Shema aktivnega imenika (Active Directory schema) določa razrede objektov, kot so uporabniki, skupine, računalniki, domene itd.

Shema aktivnega imenika je razširljiva. Stvari lahko dodajamo!

Shema

Definira razrede objektov in njihove atribute, ki jih lahko vsebuje aktivni imenik

Vsak razred objektov vsebuje globalno edinstven identifikator (globally unique identifier, GUID)

Edinstveno število, pridruženo imenu objekta

Razred objektov ima lahko zahtevane in dodatne atribute

Vsakemu atributu je dodana številka verzije in datum tvorbe ali spremembe

Omogoča posodobitve za le dane vrednosti v vseh domenskih kontrolerjih (DC)

Windows Server 2003 ima več privzetih razredov objektov

Globalni katalog

Medtem ko vsak domenski krmilnik vsebuje polno repliko za svojo domeno, drži strežnik z globalnim katalogom (**global catalogue server)** omejeno množico atributov za vse objekte v celotnem gozdu.

Na primer: Atribute, ki so najbolj pogosto iskani

Ali potrebni za logiranje

Tako zagotavlja hiter dostop do podatkov za avtentikacijo in druga povpraševanja in iskanja. Klijentu ni potrebno skakati od strežnika do strežnika preko več domen, da bi dobil iskan podatek iz imenika.

Globalni katalog:Pomni podatke vseh objektih v gozdu (forest).Popolne kopije objektov v lastni domeni in delne kopije objektov iz drugih domen.Overovlja uporabnike, ko se logirajo

Nudi vpogled in dostop do vseh sredstev v vseh domenah

Nudi kopiranje ključnih elementov aktivnega imenika

Zaradi hitrejšega dostopa vzdržuje kopijo najbolj pogosto uporabljanih atributov objektov.

Imenski prostor (namespace)

Logično področje na omrežju, ki vsebuje servise imenika in imenovane objekte.Izvaja resolucijo imen preko strežnika DNS v imenskem prostoru DNS.Aktivni imenik mora imeti možnost dostopa do strežnika DNS, ki je na omrežju. DNS in imenski prostor aktivnega imenika sta lahko na istem računalniku ali pa sta porazdeljena med več strežniki.

Dve vrsti imenskih prostorov:

Pri enovitem imenskem prostoru (contiguous namespace) vsebuje objekt-otrok (child object) ime starševskega objekta (parent object)

Pri razdeljenem imenskem prostoru objekt-otrok ne vsebuje imena starševskega objekta

Vsebovalniki v aktivnem imeniku

Hierar hični elementi, urejeni v drevesno strukturo.Vsebovalniki v aktivnem imeniku vključujejo :

Gozdove (Forests)

Drevesa (Trees)

Domene (Domains)

Organizacijske enote (Organizational units)

Položaje (Sites)

Gozdovi

Vsebovalnik najvišjega nivoja, ki v skupnem razmerju vsebuje eno ali več dreves.

Drevesa lahko uporabljajo deljen imenski prostor

Vsa drevesa uporabljajo isto shemo

Vsa drevesa uporabljajo isti globalni katalog

Dom ene omogočajo administracijo skupno združenih objektov

Med domenami velja dvosmerno prehodno zaupanje

Razmerja zaupanja

Dvosmerno zaupanje

Člani vsake domene imajo dostop do sredstev druge domene

Prehodno zaupanje (transitive trust)

Če si zaupata A in B in če si zaupata B in C, si avtomatsko zaupata tudi A in C

Prehodno razmerje zaupanja Kerberos

Dvosmerno prehodno zaupanje, ki uporablja varnostne tehnike Kerberos

Zaupanje gozdov (Forest trust)

Kerberos prehodno zaupanje med korenskimi domenami gozdov pri gozdovih Windows Server 2003

Drevesa

Vsebujejo eno ali več domen, ki imajo skupno razmerje/.Domene so v enovitem imenskem prostoru in so lahko v hierarhiji.Vse domene souporabljajo del njihovega imenskega prostora.Starševske domene in domene-otroci so v Kerberos prehodnem razmerju zaupanja.Vse domene uporabljajo isto shemo za vse tipe skupnih objektov.Vse domene uporabljajo isti globalni katalog

Domena

Primar ni vsebovalnik skupine objektov

Nudi particijo za pomnenje objektov, ki imajo skupno razmerje

Parti cije odražajo upravljalna in varnostna razmerja

Vzpostavlja skupino podatkov, ki naj bi bila kopirana iz enega domenskega krmilnika (DC) na drugega

Pospešuje upravljanje z množico objektov

Tvorba organizacijske enote

Kaj je organizacijska enota ?

Hierarhični modeli organizacijske enote

Imena, povezana z organizacijskimi enotami

Kako tvorimo organizacijsko enoto

Organizacijska enota

Tvorba skupin objektov znotraj domene

Omogoča delegiranje strežniških administrativnih vlog

Skupine objektov glede na upravljalske naloge

Nudi možnost administracije objektov s skupinskimi politikami (Group Policies)

Skupine objektov s podobnim varnostnim dostopom

Je lahko vgnezdena znotraj drugih organizacijskih enot

Kaj je organizacijska enota ?

Organizira objekte v domeni.Omogoča delegiranje administrativnega nadzora.Poenostavlja upravljanje sredstev, združenih v skupine

Hierarhični modeli organizacijske enote

Imena, povezana z organizacijsko enoto

Kdaj premikamo domenski objekt ?

Kako premaknemo domenski objekt

Položaj (site)

Grupira objekte glede na fizično lokacijo zaradi ugotavljanja najhitrejših poti med klijenti in strežniki ter med domenskimi krmilniki.

Odraža eno ali več med seboj povezanih podomrežij

Uporabljamo za replikacijo domenskih krmilnikov

Vzpostavlja redundantne poti med domenskimi krmilniki

Koordinira replikacijo med položaji z mostičnim strežnikom (bridgehead server)

Omogoča klijentu dostop do fizično najbližjega krmilnika domene

Je sestavljen iz dveh tipov objektov:

Strežniki

Konfiguracijski objekti

Navodila za vsebnike

Aktivni imenik naj bo čimbolj preprost, njegovo strukturo planirajmo še pred njegovo izvedbo.Implementirajmo čim manjše število domen.Na večini majhnih omrežij uvedimo le eno domeno.Ko neka organizacija načrtuje svojo reorganizacijo, uporabimo organizacijske enote, ki naj odražajo njeno strukturo .Tvorimo le toliko organizacijskih enot, kolikor je nujno potrebnih

Navodila za vsebnike (nadaljevanje)

Ne tvori aktivnega imenika z več kot 10 nivoji organizacijskih enot (najbolj primerno 1 ali 2 nivoja).Uporabi domene kot razdelke v gozdih in tako označi povezane konte in sredstva, ki jih upravljamo s skupinskimi in varnostnimi politikami.Uporabi več dreves in gozdov le, če je nujno potrebno.Uporabljaj položaje (sites) tam, kjer imamo več podomrežij in geografskih lokacij. Tako izboljšamo performanse logiranja in replikacij.

Upravljanje z uporabniškimi konti

Okolje za vzpostavitev in upravljanje kontov

S pomočjo samostojnega strežnika brez aktivnega imenika:

Uporabimo orodje “Local Users and Group”

V domeni z nameščenim aktivnim direktorijem:

Uporabimo orodje “Active Directory Users and Computers”

Upravljalske naloge:

Tvorba konta

Blokiranje, omogočanje in preimenovanje konta

Premik konta

Resetiranje gesla

Brisanje konta

Lažje blokiramo star konto, ga preimenujemo in spet omogočimo, kot pa da konto zbrišemo in tvorimo novega

Brisanje konta

Konte, ki niso več v uporabi, zbrišemo

Tako zagotavljamo lažje upravljanje s konti

Zmanjšamo izpostavljenost varnostnim tveganjem

Ko je konto zbrisan, je zbrisan tudi GUID in ne bo več uporabljen

Upravljanje s skupinami

Skupine (groups)

Vgrajene (built-in), Vnaprej določene (predefined) in posebne (special) skupine

Delokrog skupine

Delokrog skupine (**scope of a group)** določa območje za dostop objektov aktivnega imenika.

V bistvu to pomeni:

Kje je skupina vidna

Katere uporabnike in skupine lahko ta skupina vključuje

Tipi skupin glede na delokrog:

Lokalne (Local) – le člani samostojnega strežnika

Domenske lokalne (Domain local) – Vidne v eni domeni, lahko vključujejo druge tipe skupin

Globalne – Vidne v gozdu. Vključujejo le uporabnike in skupine iste domene

Univerzalne – Vidne v gozdu, vsebujejo lahko kateregakoli uporabnika ali skupino

Kaj so skupine ?

Lastnosti skupin

Splošne

Spreminjanje opisa , delokroga in tipa skupine ter elektronskih naslovov za porazdeljeno skupino

Člani

Dodajanje ali brisanje članov skupine

Članstvo

Dodajanje ali brisanje članstva skupine v drugi skupini

Upravnik (kdo jo upravlja)

Vzpostavitev konta ali skupine, ki upravlja s skupino

Lastnosti “član” in “članstvo”

Uvedba lokalnih skupin

Uporabimo na samostojnih strežnikih, ki niso del domene

Uporabimo tudi na članskih strežnikih v domeni

Delokrog je omejen le na lokalni strežnik

Skupine razdeljene na osnovi varnostnega dostopa do lokalnega strežnika

Tvorba z orodjem za lokalne uporabnike in skupine

Pravila lokalne skupine

Uvedba domenskih lokalnih skupin

Uporaba v eni domeni ali za upravljanje sredstev v določeni domeni

Daje globalnim in univerzalnim skupinam iz iste domene dostop do sredstev

Običajno vstavimo v ACL, tako imajo njegovi člani dostop do sredstev

Access control list (ACL) je seznam varnostnih privilegijev za določeni objekt

Delokrog je domena, v kateri je skupina

Lahko jo pretvorimo v univerzalno skupino, če:

ni v njej drugih domenskih lokalnih skupin

je domena v režimu Windows Server 2003

Kaj so domenske lokalne skupine?

Kaj so globalne skupine ?

Uvedba globalnih skupin

Naj bi vsebovale uporabniške konte iz ene domene

Upravljanje skupinskih kontov v domeni. Ti konti naj imajo tako dostop do sredstev v isti domeni in v drugih domenah

Dostop do sredstev v drugih domenah skozi članstvo v drugih globalnih, domenskih lokalnih ali univerzalnih skupinah

Lahko vsebuje uporabniške konte in druge globalne skupine iz domene, v kateri je bila stvorjena

Lahko jo pretvorimo v univerzalno skupino z enakimi omejitvami, kot jih ima domenska lokalna skupina

Kaj je gnezdenje skupin?

To je dodajanje skupine kot člana druge skupine

Funkcionalni nivoji

Določeni so z verzijo Windows na strežnikih v domeni – NT, 2000, 2003

Domenski funkcionalni nivoji

Windows 2000 Mixed

Windows 2000 Native

Windows 2000 Interim

Windows 2003

Funkcionalni nivoji gozda

Windows 2000

Windows Server 2003 Interim

Windows 2003

Nadgradnja funkcionalnih nivojev prinaša napredne zmožnosti

Funkcionalni nivoji domene

Določa jih tip strežnikov v domeni

Trije načini funkcijskih nivojev:

Windows 2000 mixed mode

Kombinacija strežnikov NT, 2000 in 2003

Windows 2000 native mode

Le strežniki 2000 in 2003

Windows 2003 mode

Le strežniki 2003

Privzeti način je ali mešani ali “native”

Način spreminjamo s pogovornim oknom “Raise Functional Level”

Kaj so funkcionalni nivoji domene?

Uvedba univerzalnih skupin

Uporabimo za nudenje lažjega dostopa do sredstev vseh domen v gozdu

Članstvo lahko vsebuje uporabniške konte, globalne skupine in univerzalne skupine z vsake domene

Nudi možnost lahkega upravljanja varnosti posameznih kontov

Poenostavlja dostop, če imamo več domen

Če hočemo narediti univerzalno skupino, moramo domeno pretvoriti v režim “Windows Server 2003”

Kaj so univerzalne skupine ?

Navodila za varnostne skupine

Uporabljaj globalne skupine za pomnenje kontov kot članov.Gnezdenje globalnih skupin naj bo minimalno.Konti naj imajo dostop do sredstev tako, da postane njihova globalna skupina član drugih skupin.Uporabljaj domenske lokalne skupine za zagotavljanje dostopa do sredstev znotraj določene domene.Izogibaj se vnašanju kontov v domenske lokalne skupine.Uporabi univerzalne skupine za zagotavljanje prostranega dostopa do sredstev tako, da jih vstaviš v sezname ACL

Kje tvorimo skupine

Skupine lahko tvorimo v korenski domeni gozda, poljubni drugi domeni ali organizacijski enoti.Izberi domeno ali organizacijsko enoto in tvori v njej skupino glede na administrativne zahteve skupine

Primer:

Če ima vaš imenik več organizacijskih enot, vsaka od teh pa ima različnega administratorja, lahko globalne skupine tvoriš v teh organizacijskih enotah

Navodila za imenovanje skupin

Strategije skupin

Dober primer uporabe lokalnih skupin

Uporabimo, ko želimo zagotoviti dostop do sredstev v eni domeni.Damo dostop do sredstev lokalnim ali domenskim lokalnim skupinam.Uporabnike damo v globalne skupine.Globalne skupine damo v lokalne skupine

Dober primer uporabe univerzalne skupine

Uporabimo, ko zagotavljamo dostop do sredstev v več domenah/Damo dostop do sredstev univerzalni skupini/Uporabnike damo v globalno skupino/Globalno skupino damo v univerzalno skupino

Zakaj dodelimo upravnika skupini ?

Zato, da:

Vemo, kdo je odgovoren za skupine

Upravniku skupine delegiramo pooblastila za dodajanje uporabnikov ali brisanje uporabnikov s skupine

Porazdelimo administrativno odgovornost

Uporaba privzetih skupin

Privzete skupine na članskih strežnikih .Privzete skupine v aktivnem imeniku.Kdaj uporabiti privzete skupine.Varnostna vprašanja za privzete skupine.Sistemske skupine

Privzete skupine za članske strežnike

Privzete skupine v aktivnem imeniku

Kdaj uporabimo privzete skupine

Privzete skupine so :

tvorjene med namestitvijo operacijskega sistema ali pri dodajanju servisov, kot na primer aktivni imenik ali DHCP

avtomatično dodeljena množica pravic uporabnikov

Uporabi privzete skupine za :

nadzor dostopa do souporabljanih sredstev

delega cijo določene administracije znotraj domene

Varnostni premisleki za privzete skupine

Uporabnika damo v privzeto skupino le, če smo prepričani, da mu želimo dati uporabniške pravice in dovoljenja, ki so tej skupini dodeljene v aktivnem imeniku; sicer raje naredimo novo varnostno skupino

Iz izkušenj sledi, da je najbolje, če uporabniki privzetih skupin uporabljajo "Run as"

Sistemske skupine

Sistemske skupine predstavljajo v različnem času različne uporabnike

Sistemskim skupinam lahko dodeljujemo uporabniške pravice in dovoljenja, ne moremo pa spreminjani ali gledati članstva

Pri sistemskih skupinah ne uporabljamo delokrogov skupin (g roup scopes)

Ko se uporabniki logirajo ali dostopajo do posameznih sredstev, so avtomatsko dodeljeni sistemskim skupinam

Razprava: Primerjava uporabe privzetih skupin ali tvorbe novih skupin

Dobre izkušnje za upravljanje skupin

Kako tvorimo skupino

Vaja: Tvorba in upravljanje skupin

Tvorba globalnih in lokalnih skupin

Imenovanje skupin glede na dogovor poimenovanja

Dodajanje članov skupinam

Vaja : Tvorba skupin

Tvorba skupin z uporabo uporabnikov in računalnikov v aktivnem imeniku

Tvorba skupin preko ukazne vrstice z orodjem "dsadd"

Demonstracija : Members and Member Of

Demonstracija, kako uporabljamo lastnosti " Members " in " Member Of "

Kako določimo skupine, katerih uporabnik ima članstvo (member of)

Kako dodajamo in odstranjujemo člane iz neke skupine

Vaja : Upravljanje članstva skupin

Dodajanje uporabnikov v globalno skupino

Strategije za uporabo skupin

Strategija za uporabo skupin v eni domeni

Kaj je gnezdenje skupin ?

Skupinske strategije

AGDLP strategija uporabe skupin

Razprava: Uporaba skupin v eni domeni

Vaja: Dodajanje globalnih skupin v domenske lokalne skupine

Kaj je sprememba delokroga (scope) ali tipa skupine?

Sprememba delokroga

Global nega v univerzalnega

Dom ensko lokalnega v univerzalnega

Univer zalnega v globalnega

Univer zalnega v domensko lokalnega

Sprememba tipa skupine

"Security " v " distribution "

"Distribution " v " security "

Kako spremenimo delokrog ali tip skupine

Vaja: Sprememba delokroga in tipa skupine

Spremenimo delokrog skupine (group scope) iz globalnega v domensko lokalnega

Spremenimo "security group" v "distribution group"

Implementacija uporabniških profilov

Local user profile

Shranjen v lokalnem računalniku

Več uporabnikov lahko uporablja isti računalnik in vzdržuje poosebljene nastavitve

Roaming profile

Se naloži na odjemalca s strežnika

Uporabnik ima na voljo iste nastavitve, ne glede na to, na katerem računalniku se logira

Mandatory profile

Shranjeni na strežniku

Uporabnik lahko spreminja, ne more pa shranjevati nastavitev

Upravljanje uporabnikov in računalniških kontov

Pregled

Tvorba uporabniških kontov

Tvorba računalniških kontov

Sprememba lastnosti uporabniških in računalniških kontov

Tvorba predloge za uporabniški konto

Omogočanje in odklepanje uporabniških in računalniških kontov

Reseti ranje uporabniških in računalniških kontov

Lociranje uporabniških in računalniških kontov v aktivnem imeniku

Pomnenje povpraševanj (queries)

Tvorba uporabniških kontov

Kaj je uporabniški konto?

Imena, združena s konti domenskih uporabnikov

Navodila za dogovor poimenovanja uporabniških kontov

Vstavljanje uporabniških kontov v hierarhijo

Opcije za gesla uporabniških kontov

Kdaj zahtevamo spremembo gesel

Kako tvorimo uporabniške konte

Dobri primeri za tvorbo uporabniških kontov

Kaj je uporabniški konto ?

Imena, združena z domenski uporabniškimi konti

Navodila za tvorbo poimenovanja uporabniških kontov

Postavljanje uporabniških kontov v hierarhijo

Možnosti gesel za uporabniške konte

Kdaj zahtevati ali omejevati spremembe gesel

Kako tvorimo uporabniške konte

Vaja : Tvorba uporabniških kontov

Tvorba lokalnega uporabniškega konta s pomočjo orodja "Computer Management"

Tvorba domenskega konta z uporabo "Active Directory Users and Computers"

Tvorba domenskega uporabniškega konta s pomočjo "Run as"

Tvorba domenskega uporabniškega konta s pomočjo "dsadd"

Napotki za tvorbo uporabniških kontov

Kaj je računalniški konto ?

Identifi cira računalnik v domeni

Nudi način avtentikacije in nadzora računalniškega dostopa do omrežja in domenskih sredstev

I meti ga mora vsak računalnik, ki uporablja :

Windows Server 2003

Windows XP Professional

Windows 2000

Windows NT

Kako naredimo računalniški konto ?

Varnost

Avtentikacija

IPSec

Nadzor

Upravljanje

Značilnosti aktivnega imenika:

Programsko razvijanje

Upravljanje z namizjem

"Hardware and software inventory through SMS"

Kje v domeni tvorimo računalniške konte

Opcije računalniških kontov

Kako naredimo računalniški konto

Vaja : Tvorba računalniškega konta

Tvorba računalniškega konta s pomočjo "Active Directory Users and Computers"

Tvorba računalniškega konta s pomočjo "dsadd"

Spreminjanje lastnosti uporabniških in računalniških kontov

Kdaj spremeniti lastnosti uporabniških in računalniških kontov

Lastnosti, vezane na uporabniške konte

Lastnosti, vezane na računalniške konte

Kako spremeniti lastnosti uporabniških in računbalniških kontov

Kdaj spremeniti lastnosti uporabniških in računalniških kontov

Lastnosti, vezane na uporabniške konte

Lstnosti, povezane z računalniškimi konti

Kako spremenimo lastnosti uporabniškega ali računalniškega konta

Vaja: Spreminjanje lastnosti uporabniškega in računalniškega konta

Tvorba šablone za uporabniški konto (User Account Template)

Kaj je "šablona za uporabniški konto (User Account Template)?

Katere lastnosti so v šabloni?

Navodila za tvorbo šablon za uporabniške konte

Kaj je šablona za uporabniški konto?

Šablona za uporabniški konto je uporabniški konto, ki vsebuje lastnosti, ki naj bi jih imeli uporabniki s skupnimi zahtevami

Šablone za uporabniški konto večajo učinkovitost tvorbe uporabniških kontov s standardiziranimi konfiguracijami

Katere lastnosti so v šabloni?

Napotki za tvorbo šablon za uporabniške konte

Kako tvorimo šablono za uporabniški konto

Vaja : Tvorba šablone za uporabniški konto

Omogočanje in blokiranje uporabniških in računalniških kontov

Zakaj omogočamo in blokiramo uporabniške in računalniške konte?

Kako blokiramo in omogočamo uporabniške in računalniške konte

Kaj so zaklenjeni uporabniški konti?

Kako odklenemo računalniške konte

Zakaj omogočamo in blokiramo uporabniške in računalniške konte?

Kako blokiramo in omogočamo uporabniške in računalniške konte?

Kaj so zaklenjeni računalniški konti ?

Prag zaklepanja konta:

Določa število ponesrečenih poskusov vstopa

Hekerjem preprečuje ugibanje uporabniških gesel

Konto lahko preseže prag s prevelikim številom ponesrečenih poskusov vstopa:

Pri vstopnem postopku

Pri ohranjevalniku zaslona, zaščitenem z geslom

Ko dostopamo do omrežnih sredstev

Kako odklenemo uporabniško geslo

Vaja: Blokiranje in omogočanje uporabniških kontov

Reset iranje uporabniških in računalniških kontov

Kdaj resetiramo gesla

Kako resetiramo gesla

Kdaj resetiramo računalniške konte

Kako resetiramo računalniške konte

Kdaj resetiramo uporabniška gesla

Geslo resetiramo, če ga uporabnik pozabi

Po resetiranju gesla, uporabnik nima več dostopa do določenih podatkov, med drugim:

Elektronske pošte, ki je enkriptirana z javnim ključem uporabnika

Internetnih gesel, ki so pomnjena na računalniku

Datotek, ki jih je uporabnik zakodiral (enkriptiral)

Kako resetiramo uporabniška gesla

Kdaj resetiramo računalniške konte

Računalniške konte resetiramo, če :

Se računalnikom ne uspe avtentizirati na domeno

Morajo biti gesla sinhronizirana

Kako resetiramo računalniške konte

Vaja : Reset iranje gesla za uporabniški konto

Lociranje uporabniškega in računalniškega konta v aktivnem imeniku

Tipi iskanja

Kako iščemo objekte aktivnega imenika

Kako iščemo z običajnimi povpraševanji

Uporaba posebnih povpraševanj

Tipi iskanja

Osnovni kriteriji iskanja vsebujejo:

Tip objekta

Lokacijo

Splošne vrednosti, povezane z objektom, kot na primer ime in opis

Kako iščemo objekte aktivnega imenika

Kako uporabimo običajno povpraševanje

Uporaba posebnih vprašanj

Vaja : Lociranje uporabniških in računalniških kontov

Locirajte uporabniške in računalniške konte, ki izpolnjujejo določeni kriterij

Shranjevanje povpraševanj

Kaj je shranjeno povpraševanje ?

Kako tvorimo shranjeno povpraševanje

Kaj je shranjeno povpraševanje ?

Kako tvorimo shranjeno povpraševanje

Vaja: Tvorba shranjenih povpraševanj

Tvorite shranjeno povpraševanje za računalniški konto

Vaja : Upravljanje uporabniških in računalniških kontov

Tvorite uporabniške in računalniške konte

Premaknite uporabniške in računalniške konte

Omogočite uporabniške konte

Kaj so dovoljenja (permissions) ?

Dovoljenja določajo tip dostopa, zagotovljen uporabniku, skupini, računalniku ali objektu

Dovoljenja uvedemo za objekte, kot so datoteke, direktoriji, souporabljani direktoriji (shared folders) in tiskalniki

Dovoljenja dodelimo uporabnikom in skupinam v aktivnem imeniku ali na lokalnem računalniku

Kaj so standardna in posebna dovoljenja?

Povzetek

Aktivni imenik (Active Directory)

Storitev, ki nudi način upravljanja s sredstvi na omrežju

Objekt

Večina osnovnih komponent v aktivnem imeniku

Določimo jih z množico podatkov, ki ji pravimo shema

Globalni katalog

Pomni podatke o vseh objektih

Replicira ključne objekte

Avtentizira logiranje uporabnikov

Imenski prostor (namespace)

Uporablja imenski prostor DNS namespace za resolucijo imen

Aktivni imenik zahteva uporabo strežnika DNS

Povzetek

Hierarhija aktivnega imenika

Gozdi, drevesa, domene, organizacijske enote in lokacije (sites)

Načrtovanje aktivnega imenika

Struktura naj bo čimbolj preprosta

Uporabniški konti

Poosebljanje lastnosti kontov

Upravljalske naloge obsegajo blokiranje, omogočanje, preimenovanje, premikanje in brisanje kontov

Upravljanje z varnostjo skupin

Lokalne, domensko lokalne, globalne in univerzalne skupine

Uporabniški profili

Uporabljamo jih za poosebljanje kontov

Upravljanje tiskanja na Windows Server 2003

Cilji

Osnovni pojmi, kako deluje tiskanje na omrežju, kako deluje tiskanje preko interneta

Namestitev lokalnih in souporabljanih (shared) tiskalnikov

Konfiguriranje tiskalnih lastnosti "Window Server 2003"

Konfiguriranje omrežnega in internetnega tiskanja

Upravljanje s posli tiskanja

Reševanje pogostih problemov pri tiskanju

Osnovni pojmi

Lokalni tiskalnik

Lokalno povezan na računalnik

Omrežni tiskalnik (network print device)

Omrežni tiskalnik za souporabo (shared network printer)

Tiskanje preko interneta

Tiskalni odjemalec (print client)

Računalnik ali aplikacija, ki sproži tiskanje (print job)

Tiskalni strežnik (print server)

Računalnik oziroma strežna naprava, ki nudi souporabo tiskalnika

Kaj je lokalni tiskalnik in kaj omrežni tiskalnik?

Osnovni pojmi (nadaljevanje)

Tiskanje v ozadju (spooling)

Datoteke za tiskanje pomni na posebnem delu diska, dokler niso izpisane

Razbremeni računalnik za obravnavo drugih zahtevkov

Vsebuje DLL, podatkovne datoteke in programe, ki jih uporablja tiskanje

Gonilnik tiskalnika (printer driver)

Vsebuje konfiguracijske podatke in nudi navodila za oblikovanje

Je lociran na strežniku, lahko pa je tudi na odjemalcu

Implementacija lokacij tiskalnikov

Kaj so lokacije tiskalnikov ?Zahteve za implementacijo tiskalne lokacije.Dogovori za poimenovanje lokacij tiskalnikov.Kako konfiguriramo lokacije tiskalnikov.Kako nastavljamo lokacije tiskalnikov.Kako locirati tiskalnike

Kaj so lokacije tiskalnikov ?

Lokacije tiskalnikov omogočajo uporabnikom iskanje in povezovanje s tiskalniki v njihovi bližini.V aktivnem imeniku je IP podmaska predstavljena kot objekt " subnet " , ki vsebuje atribut lokacije, ki ga uporabljamo pri iskanju tiskalnikov.Aktivni imenik uporablja ta atribut lokacije kot tekstovni niz za prikaz lokacije tiskalnika

Zahteve za implementacijo lokacije tiskalnika

Dogovori za poimenovanje lokacij tiskalnikov

Kako konfiguriramo lokacije tiskalnikov

Kako nastavimo lokacijo tiskalnikov

Kako lociramo tiskalnike

Vaja: Implementacija lokacij tiskalnikov

Kako poteka tiskanje

Kako poteka tiskanje v okolju Windows Server 2003

Kako poteka tiskanje

Programska aplikacija tvori datoteko za tiskanje (print file)

Aplikacija komunicira z GDI (Graphics Device Interface)

Tiskalno datoteko oblikuje s krmilnimi znaki (control codes)

Istočasno je taka datoteka zapisana v "spooler" odjemalca kot "spool file"

"Remote print provider" s klicem oddaljene procedure (RPC) pokliče ciljni omrežni tiskalni strežnik

Ko je strežnik pripravljen, je datoteka posredovana tiskalnemu servisu na ciljnem strežniku

Kako poteka tiskanje (nadaljevanje)

Omrežni tiskalni strežnik uporablja 4 storitve za prevzem in obdelavo datoteke za tiskanje:

Usmerjevalnik (router)

Ponudnik tiska (print provider)

Izvajalec tiska (print processor)

Print monitor

Ko oddaljeni ponudnik tiskanja pokliče strežnik, ta pokliče svoj usmerjevalnik v sklopu servisa "Print Spooler"

Usmerjevalnik usmeri tiskalno datoteko ponudniku tiskanja,ta pa jo shrani kot "spool file"

Kako poteka tiskanje (nadaljevanje)

Med pripravo datoteke "spool file" ponudnik tiskanja sodeluje z izvajalcem tiskanja (print processor) pri oblikovanju datoteke s pravilnimi tipi podatkov

Ko je "spool file" izoblikovana, jo "print monitor" pošlje na tiskalnik

Kaj je tiskalnik v ozadju (Print Spooler) ?

Izvršljiva datoteka, ki upravlja proces tiskanja, kar vsebuje :

Poišče lokacijo pravega gonilnika za tiskalnik

Naloži gonilnik

Kliče v visokonivojske funkcije tiskanja v ozadju

Planira naloge za tiskanje

Prejme datoteke za tiskanje, jih shrani na trdi disk, nato jih pošlje tiskalniku, ko je ta pripravljen

Zakaj bi spremenili lokacijo tiskalnika v ozadju?

Lokacijo tiskalnika v ozadju (print spooler) spremenimo zaradi :

Izboljšanja performans

Reševanja problemov s prostorom na disku

Zmanjšanja fragmentacije zagonske particije (boot partition)

Zagotavljanja varnosti

Upravljanja z diskovnimi kvotami

I zboljšanja zanesljivosti

Kako spremenimo lokacijo tiskalnika v ozadju

Vaja: Spremenimo lokacijo tiskalnika v ozadju

Spremenite lokacijo tiskalnika v ozadju (print spooler) in spremembo preverite

Kako poteka tiskanje preko interneta

Nameščen in aktiviran mora biti IIS

Odjemalec se z uporabo spletnega brkljalnika poveže s strežnikom IIS

Brkljalnik pošlje tiskalno datoteko na GDI

Oddaljeni "print provider" s pomočjo klica oddaljene procedure (RPC) in z uporabo HTTP pokliče IIS

HTTP prenese IPP (Internet Printing Protocol)

IPP vsebuje klic oddaljene procedure (RPC) in podatke za tiskanje

Strežnik HTTP sodeluje s servisi "spooler" pri posredovanju datoteke tiskalniku

Namestitev lokalnih in souporabnih (shared) tiskalnikov

Souporabljani tiskalnik je lahko na kateremkoli računalniku z najmanj Windows95 oziroma strežniku

Tiskalnik, ki bo souporabljan, najprej konfiguriramo kot lokalni tiskalnik, nato pa omogočimo njegovo souporabo (shared printer)

Sopuporabne tiskalnike lahko povežemo na omrežje na različne načine:

Strežniki

Delovne postaje

Strežne naprave za tiskanje (print server devices)

Namestitev lokalnih in souporabnih (shared) tiskalnikov (nadaljevanje)

Zahteve za tiskalni strežnik:

Dovolj RAM za obdelavo dokumentov

Dovolj prostora na disku za "spooled documents"

Tiskalniki, ki jih namestimo s čarovnikom "Add Printer", so privzeto souporabni in objavljeni v aktivnem imeniku

Tiskalnike, ki jih namestimo s "Plug and Play", moramo konfigurirati za souporabo po namestitvi

Kako namestimo omrežni tiskalnik in vzpostavimo njegovo souporabo

Vaja : Namestitev in souporaba tiskalnikov

Namestite in souporabite en lokalni in en omrežni tiskalnik

Kaj so dovoljenja za souporabljane tiskalnike?

Zakaj spreminjati dovoljenja souporabljanih tiskalnikov?

Omejevanje dostopa do tiskalnika izbranim uporabnikom

Primer : Vsem navadnim uporabnikom oddelka damo nizkonivojska dovoljenja, vodjem pa visokonivojska. To omogoča tako navadnim uporabnikom kot vodstvu tiskanje dokumentov, le vodstvo pa lahko spreminja status dokumentov, ki so bili poslani v tisk .

Preprečevanje dostopa do tiskalnika izbranim uporabnikom

Primer : Nekaterim članom skupine dovolimo tiskati dokumente, drugim pa to onemogočimo in jih silimo, da uporabljajo drug tiskalnik .

Kako upravljamo dostop do tiskalnikov

Vaja: Upravljanje dostopa do tiskalnikov z dovoljenji za souporabo

Nastavljanje dovoljenj tiskalnikov, ki omogočajo skupini upravljanje z dokumenti

Nastavljanje dovoljenj tiskalnikov, ki dajejo skupini operaterska dovoljenja

Kaj je gonilnik tiskalnika (Printer Driver)?

Programska oprema, ki jo uporabljajo računalniški programi pri komunikaciji s tiskalniki

Preslika podatke, ki jih pošilja računalnik, v ukaze, ki jih razume tiskalnik

Sestavljajo ga naslednji tipi datotek:

Kako namestimo gonilnike tiskalnikov

Kako dodajamo gonilnike tiskalnikov za druge odjemalske operacijske sisteme

Vaja: Upravljanje z gonilniki tiskalnikov

Namestili bomo gonilnik tiskalnika

Konfiguriranje tiskanja na Windows Server 2003

Splošni podatki o tiskalniku (General printer information)

Souporaba tiskalnika (Printer sharing)

Nastavitev vrat tiskalnika (Printer port setup)

Razvrščanje tiskalnika in napredne možnosti (Printer scheduling and advanced options)

Varnost (Security)

Nastavitve naprave (Device settings)

Souporaba tiskalnika

Omogoči ali prepreči souporabo tiskalnika

Določi ime za souporabo

Objava tiskalnika v aktivnem imeniku

Dodatni gonilniki:

Za dodajanje novih tipov odjemalcev

Nameščanje gonilnikov, da se avtomatsko naložijo k uporabnikom pri prvi povezavi

Avtomatsko posodabljanje gonilnikov (po Windows 98)

Specifikacija vrat

Specificira vrata tiskalnika

Vzpostavi dvosmerno tiskanje

Dvosmerna komunikacija med tiskalnim strežnikom in programsko aplikacijo

Konfiguriranje "printer pooling"

2 ali več enakih tiskalnikov na tiskalnem strežniku

Povečuje kapaciteto tiskanja

Gumb "Add port" ima privzete nastavitve vrat

Local port rokuje s tiskanjem, posredovanem lokalnim vratom tiskalnika ali v datoteko

LPR port prenaša datoteke za tiskalnike, navezane na računalnike z OS UNIX, DEC, VAX, ali IBM mainframes, pa tudi s teh računalnikov kot klijentov na Windows Server 2003

Standard TCP/IP port uporabimo za tiskalnike, ki temeljijo na TCP/IP in so povezani v omrežje preko omrežnih kartic ali preko tiskalnih strežnikov

Konfiguriranje vrat (Configure Port)

Za vrata LPR lahko nastavimo čas "Port timeout"

Planiranje tiskanja in napredne možnosti

Planiranje (scheduling)

Dolgotrajne posle omejimo na ure izven delovnega časa

Nastavljanje prioritete tiskanja

Možnosti tiskanja v ozadju

Največkrat izberemo možnost "Spool print jobs and Start printing immediately"

Če so strani pomešane, začenjamo tiskati šele, ko je v ozadnju natisnjena zadnja stran

Direktno na tiskalnik pišemo le v nujnih primerih

Planiranje tiskanja in napredne možnosti (nadaljevanje)

Dokumente, ki se ne ujemajo, zadržimo

Sistem primerja nastavitev tiskalnika z nastavitvijo dokumenta

Zadržanih poslov ne natisnemo, dokler jih uporabnik ne sprosti

Natisnemo dokumente v ozadju (spooled documents)

Omogočimo izpis dokumentov v ozadju ne glede na prioriteto

Obdržimo natiskane dokumente

Po izpisu iz ozadja dokumente zadržimo

Omogočimo napredne značilnosti tiskanja

Omogočimo posebne značilnosti določenih tiskalnikov

Planiranje tiskanja in napredne možnosti (nadaljevanje)

Privzeto tiskanje

Specificira privzete nastavitve tiskanja, ki veljajo, dokler jih ne prekrijejo kontrolne kode in tiskane datoteke

Gumb "Separator Page"

Pred začetkom vsakega dokumenta bo prazna stran

Uporabno v velikih pisarnah za zagotavljanjeresetiranja formatiranja med posameznimi posli in za ločevanje dokumentov

Planiranje tiskanja in napredne možnosti (nadaljevanje)

Gumb "Print Processor" specificira tiskalni procesor in enega od naslednjih tipov podatkov:

RAW

Brez dodatnega formatiranja

RAW (FF dodan na koncu)

Na konec datoteke dodan "Form feed"

RAW (FF auto)

Form feed dodamo, če še ne obstoja

NT EMF

Prenosljivost omogoča "Enhanced metafile data type"

TEXT

Formatirano v skladu s standardom ANSI

Kaj so prioritete tiskalnika ?

Kako nastavimo prioritete tiskalnika

Vaja: Nastavljanje prioritet tiskalnika

Planiranje razpoložljivosti tiskalnika

Kdaj planiramo razpoložljivost tiskalnika

Navodila za planiranje razpoložljivosti tiskalnika

Kako planiramo razpoložljivost tiskalnika

Kdaj planiramo razpoložljivost tiskalnika

Planiranje razpoložljivost tiskalnika za tiskanje dolgih dokumentov ali dokumentov posebne vrste

Upoštevajmo planiranje razpoložljivosti tiskalnika :

Čez dan preusmerimo tiskanje dolgih dokumentov na tiskalnik, ki izpisuje izven delovnega časa

Nastavljanje različnih tiskalnikov kot isto tiskalno napravo in konfiguriranje posameznega tiskalnika, da bo razpoložljiv ob drugem času

Primer: en tiskalnik je razpoložljiv čez dan, drugi ponoči (skupaj torej 24 ur na dan)

Navodila za planiranje razpoložljivosti tiskalnika

Kako planiramo razpoložljivost tiskalnika

Vaja : Planiranje razpoložljivosti tiskalnika

Konfigurirajte razpoložljivost tiskalnika

Konfiguriranje varnosti

Privzeta dovoljenja

Administrators, server operators, print operators

tiskanje, upravljanje s tiskalniki, upravljanje z dokumenti

Skupina Everyone

tiskanje

Creator Owner

Upravljanje z dokumenti

Napredne varnostne možnosti

Nastavljanje posebnih dovoljenj za tiskalnik

Dodajanje ali brisanje skupine ali uporabnika za varovan dostop ali negacijo tega

Nastavljanje nadzora tiskalnika

Nastaviti moramo skupinsko politiko ali privzeto varnostno politiko domene

Imejmo lastništvo nad tiskalnikom

Poglejmo trenutna dovoljenja uporabnika ali skupine

Konfiguriranje nastavitev naprave

Konfiguriranje nelokalnega ali internetnega tiskalnika

Uporabimo čarovnik "Add Printer"

Možnosti za izbiro tiskalnika:
Najdemo tiskalnik v aktivnem imeniku
Poiščemo (Browse) ali vnesemo UNC tiskalnika
Vnesemo URL za internet ali lokalno omrežje
Ko smo oddaljeni tiskalnik namestili na domenskem krmilniku, lahko daljinsko upravljamo s "shared printer properties"

Upravljanje s tiskalnimi posli (Print Jobs)

Uporabniki z dovoljenji za tiskanje:
Posredujejo tiskalne posle tiskalniku
Ustavijo, nadaljujejo in ponovno poženejo tiskanje svojih dokumentov
Prekinejo tiskanje svojih dokumentov
Uporabniki z dovoljenji nza upravljanje z dokumenti:
Posredujejo tiskalne posle tiskalniku
Ustavijo, nadaljujejo in ponovno poženejo tiskanje katerihkoli dokumentov
Prekinejo tiskanje katerihkoli dokumentov

Nadzor posameznih tiskalnih poslov

Dostop do posameznih dokumentov v tiskalni vrsti
Nadaljevanje, ponovni zagon ali brisanje tiskanja dokumenta
Dostop do lastnosti dokumenta
Planiranje izbranih poslov
Prioriteto poslov lahko spremenimo od privzete 1 do višje prioritete (največ 99)

Reševanje običajnih problemov s tiskanjem

Lahko je prišlo do težav s tiskalnikom v ozadju (Print Spooler service)
Servis tiskalnika v ozadju ustavimo in ponovno zaženemo
Najprej opozorimo uporabnike, ker bodo uvrščeni posli zbrisani
Preverimo, da je pognan servis RPC in nastavljen na avtomatski start
Preverimo, če delujeta " Server service " in " TCP/IP Print Server service "

Tiskalne banke (Printing Pools)

Kako konfiguriramo Printing Pool

Vaja : Upravljanje tiskanja

Nameščanje tiskalnikov
Tvorba " printing pool "
Nastavljanje prioritete tiskalnika in planiranje njegove razpoložljivosti
Povzetek
Windows 2003 Server lahko konfiguriramo za nudenje lokalnega ali omrežnega tiskanja
Omrežno tiskanje poteka z uporabo HTTP in "Internet Printing Protocol"
Lokalne in souporabne tiskalnike namestimo s čarovnikom "Add Printer", ki se nahaja v kontrolnem panoju
Lastnosti, povezane s tiskalnikom, omogočajo konfiguriranje splošnih podatkov o tiskalniku, souporabe tiskalnika, nastavitve vrat tiskalnika, planiranja tiskalnika, varnosti, naprednih možnosti in gonilnika naprave
Povzetek

Nelokalni ali internetski tiskalnik namestimo s čarovnikom "Add Printer"
Tako lahko upravljamo z lastnostmi tiskalnika preko strežnika
Upravljanje s tiskalnikom
Ustavljanje in nadaljevanje tiskanja
Nastavitev privzetega tiskalnika
Brisanje, ustavljanje, nadaljevanje posameznih tiskalnih poslov
Nastavitev prioritet tiskanja
Težave s tiskanjem lahko rešujemo na več načinov, tudi s ponovnim zagonom servisa "Print Spooler"

Konfiguriranje in upravljanje podatkovnih medijev
Cilji
Razumevanje pomnilnih možnosti Windows Server 2003 vključno z osnovnimi (basic) in dinamičnimi diski
Upravljanje diskov in reševanje problemov s particijami, zvezki in montiranimi pogoni
Konfiguriranje in upravljanje zvezkov RAID za toleranco do napak
Varnostno kopiranje diskov
Restavracija podatkov na disku
Pogled na trdi disk
Particije diska
Celotno pomnilno področje diska je običajno razdeljeno regije, ki jim pravimo "particije diska"

Master Boot Record
Majhno področje na začetku diska, namenjeno ' upravljanju ' particij diska

S e k tor številka 0 je znan kot " Master Boot Record " (zelo pomembno !)

Format MBR
MBR je razdeljen na tri področja :
bootstrap loader program
Tabela particij
MBR podpis (i.e., 0x55, 0xAA)

Pomnilne možnosti Windows Server 2003

Osnovni (b asic) disk
Uporablja tradicionalne particije diska
Vsebuje primarno particijo, razširjeno (extended) part ticijo in logične pogone
D inamični d isk

Ne uporablja tradicionalnih particij
Nudi fleksibilnost v številu zvezkov (volumes) na disk
Osnovni diski
Particije
Rezervirajo skupino sledi in sektorjev na disku z namenom, da jih lahko uporabi določen datotečni sistem
Formatiranje
Tvorba tabele s podatki o datotekah in direktorijih za dani datotečni sistem
RAID
Skupina standardov za podaljševanje življenja diskov in preprečevanje izgube podatkov
Osnovni diski lahko uporabljajo RAID nivojel 0, 1 in 5

Osnovni diski (nadaljevanje)

Proge diskov (disk Striping)
Zmožnost razprostiranja podatkov preko več diskov ali zvezkov (volumes)
Zmanjšuje obrabo diskov
Zrcaljenje diskov (disk mirroring)
Tvorba slike vseh podatkov z originalnega diska na rezervnem disku (backup disk)
Rezervni disk oživi le, če izpade originalni disk
Diski, ki jih dodajamo na računalnik z "Windows Server 2003", so avtomatsko konfigurirani kot osnovni (basic) diski
Particije na osnovnih diskih so lahko primarne ali razširjene (extended)
Primarne particije
Osnovni diski morajo imeti najmanj eno primarno particijo, lahko pa imajo do 4 particije
Primarna particija je tista, s katere lahko zaženemo operacijski sistem
Lahko jo uporabimo tudi v druge namene, na primer za pomnenje datotek v drugačnem datotečnem formatu
Natančno ena primarna particija mora biti označena kot aktivna
Aktivna particija je tista, na kateri išče računalnik aparaturno specifične datoteke za zagon operacijskega sistema
Tej particiji pravimo tudi "sistemska particija"

Sistemske in zagonske particije in zvezki

Sistemski zvezek oziroma particija vsebuje aparaturno odvisne datoteke (Ntldr, Boot.ini, Ntdetect.com), potrebne za nalaganje Windows.

Zagonski (boot) zvezek oziroma particija vsebuje sistemske datoteke operacijskega sistema Windows, ki so locirane v direktorijih %Systemroot% in %Systemroot%\System32.

Razširjene (extended) particije

Naredimo jih s prostorom, ki še ni bil dodeljen particijam
Omogočajo, da osnovni disk prekorači omejitev na 4 particije
Po tvorbi lahko tako particijo delimo dalje v logične pogone (logical drives)
Logične pogone nato formatiramo in jim dodelimo črkovne oznake
Zagonsko particijo (boot partition) lahko namestimo na primarno ali na razširjeno particijo
Zagonska particija vsebuje datoteke operacijskega sistema in to v direktoriju \Windows

RAID Structure

RAID – multiple disk drives provides **reliability** via **redundancy**.

RAID is arranged into six different levels.
Several improvements in disk-use techniques involve the use of multiple disks working cooperatively.
Disk striping uses a group of disks as one storage unit.
RAID schemes improve performance and improve the reliability of the storage system by storing redundant data.
Mirroring or *shadowing* keeps duplicate of each disk.
Block interleaved parity uses much less redundancy.

RAID Levels

Množice zvezkov in prog (Volume and Stripe Sets)

Volume set
Dve ali več particij združimo tako, da izgledajo kot en zvezek z enotno črkovno oznako
Stripe set
Dva ali več kombiniranih diskov
Proge za Raid nivo 0 ali 5
Kompatibilni z množicami, tvorjeni pod operacijskim sistemom NT
Če disk izpade, ne moremo tvoriti novih množic
Dinamični diski
Zmožnost vzpostavitve velikega števila zvezkov na enem disku
Zmožnost širitve zvezkov na dodatne fizične diske
Podpirajo nivoje RAID 0, 1 in 5
Lahko jih formatiramo za datotečne sisteme FAT16, FAT32 in NTFS
Po izpadu toka ali izklopu jih lahko reaktiviramo
Nudijo boljše upravljanje diskov kot osnovni diski

Konfiguracije dinamičnih diskov

Dinamične diske razpoznavata operacijska sistema Windows 2000 in Windows Server 2003
Terminologija dinamičnih diskov uporablja zvezke (volumes) namesto particij oziroma množic (sets)
Pet tipov zvezkov:
Preprosti zvezki (Simple volumes)
Speti zvezki (Spanned volumes)
Zvezek s progo (Striped volumes)
Zrcaljeni zvezki (Mirrored volumes)
Zvezki Raid-5

Preprost zvezek (Simple Volume)

Cel disk ali del diska, ki je vzpostavljen kot dinamični disk
Možnost razširitve zvezka z nerazporejenim prostorom
Lahko razširimo z do 32 sekcijami na istem disku
Ne nudi tolerance napak

Spet zvezek (Spanned Volume)

2 do 32 diskov, ki jih obravnavamo kot en zvezek

Uporabno za kombiniranje več manjših delov prostora na disku ali za kombiniranje majhnih diskov

Zvezke, formatirane za NTFS lahko razširjamo

Če eden od diskov spetega zvezka izpade, je nedostopen celoten zvezek

Če zbrišemo del spetega zvezka, je zbrisana celotna diskovna množica (disk set)

Zvezek s progo (Striped Volume)

Pravimo mu tudi RAID nivo 0

Podaljša življenje trdih diskov z enakomernim razpostiranjem podatkov preko 2 do 32 pogonov

Izboljša performance diska

Enake količine podatkov v blokih velikosti 64 KB zapisujemo v vrstah na vsak disk

Primerno za velike podatkovne baze in replikacijo podatkov

Podatke izgubimo, če izpade eden ali več diskov

Upravljanje diska

Naloge

Vpogled v podatke o disku

Tvorba in brisanje particij in zvezkov

Pretvorba osnovnega diska v dinamični disk

Reševanje problemov z diskom

Orodja

Disk Management

Disk Defragmenter

Check Disk

chkdsk

Tvorba particij

Ko tvorimo particijo, pustimo najmanj 1 MB prostora za pretvorbe iz osnovnega diska v dinamičnega

Organiziraj pomnilne enote s particijami

Tako na primer imej operacijski sistem v ločeni particiji, podatke pa v drugi. Tako podatke zaščitiš

Particijo lahko formatiramo med njeno tvorbo ali kasneje

Zvezek na dinamičnem disku, formatiran z orodjem "Disk Management" lahko formatiramo le za NTFS

Pretvorba osnovnega diska s particijami v dinamični disk

Tvorba zvezkov – izbira novega zvezka

Montiranje pogona

Montiran pogon se prikaže kot mapa in dostopamo do njega s potjo tako kot do drugih map (direktorijev)

Montiramo lahko osnovne ali dinamične diske, CD-je ali pogone Zip

Mapi lahko dodajamo druge pogone

Tako zmanjšamo število črk za označevanje uporabljenih pogonov

Uporabno za pomnenje domačih direktorijev

Dostop iz podatkovnih baz za olajšanje dostop uporabnikov in tvorbo rezervnih kopij

Uporaba orodja Disk Defragmenter

Diski postopoma postanejo fragmentirani

Datoteke se shranjujejo na prvo prosto področje na disku

Dostop do datoteke lahko zahteva branje z različnih lokacij na disku

Disk Defragmenter

Analizira diske in tvori poročila

Locira fragmentirane direktorije in datoteke in jih prestavi na celovite lokacije na fizičnem disku

Disk zelo zasedenega strežnika defragmentiraj enkrat na eden do dva tedna

Uporaba orodja " Check Disk "

Pregleda diske za slabe sektorje in napake v datotečnem sistemu

Uporabljamo ga, ko uporabniki ne dostopajo do sistema

Dve možnosti:

Avtomatično odpravljanje napak v datotečnem sistemu

Popravi vse napake v datotečnem sistemu

Pregled in poskus reševanja pri slabih sektorjih

Vključuje vse zgoraj

Tudi najde in fiksira slabe sektorje ter reši vse podatke, ki jih lahko prebere

Uporaba orodja chkdsk

Orodje sprožimo v ukazni vrstici. Omogoča iskanje napak na disku

Se avtomatsko zažene ob zagonu, če zagonski proces odkrije, da je tabela za alociranje datotek (ali kakšne datoteke) pokvarjen

Preveri lahko FAT16, FAT32, NTFS ali njihove kombinacije

Izgubljene podatke lahko reši v datoteko (Filexxx.chk)

S stikali mu lahko določimo nekatere parametre

Strpnost do napak (Fault Tolerance)

Zmožnost, da se sistem mehko reši v primeru programskih ali aparaturnih napak oziroma izpadov

Windows Server 2003 nudi toleranco do napak preko programskega RAID

RAID ni nadomestilo za regularno tvorbo rezervnih kopij

Podatke zapiše na več kot le en pogon

Ob izpadu enega pogona lahko dostopimo do podatkov na enem od preostalih pogonov

Zvezki RAID

RAID nivo 0

Proge brez druge redundance

RAID nivo 1

Zrcaljenje diska (disk mirroring) s podvajanjem podatkov na rezervnem disku na istem krmilniku oziroma adapterju

Dupleks diska (disk duplexing) s podvajanjem diska na rezervnem disku na drugem krmilniku oziroma adapterju

Dostop za pisanje je počasnejši od dostopa za branje

Če uporabimo več kot tri zvezke, je ta nivo dražji od drugih RAID nivojev

RAID zvezki (nadaljevanje)

RAID nivo 2

Polje diskov s progami in podatki za popravljanje napak (error-correction)

RAID nivo 3

Kot nivo 2, toda podatki za popravljanje napak (error correction data) so napisani le na en disk

RAID nivo 4

Kot nivo 2, z verificiranjem kontrolne vsote (checksum)

Kontrolna vsota (checksum) je vsota bitov v datoteki, kar omogoča verifikacijo, če datoteka ni bila spremenjena (corrupt)

Server 2003 ne podpira RAID nivojev 2 do 4

RAID

Redundant Array of Inexpensive Disks

RAID zvezki (nadaljevanje)

RAID nivo 5

Nudi proge (striping) , popravljanje napak (error correction) in preverjanje kontrolne vsote (checksum) po vseh diskih

Uporablja več RAM kot drugi nivoji RAID

Zahteva polje najmanj 3 diskov

Ista garancija podatkov kot pri zrcaljenju, vendar počasnejše

Če izpade več kot en disk, so podatki zgubljeni

RAID Level 5

Primerjava RAID 0, 1 in 5

RAID 0 ne nudi tolerance do napak in ga v nekaterih primerih zato ne priporočamo

Zagonske in sistemske datoteke lahko namestimo na RAID nivo 1, ne pa na RAID nivo 5

RAID nivo 1 uporablja dva trda diska, RAID nivo 5 uporablja tri do 32 diskov

Implementacija RAID 1 je glede na pomnilno kapaciteto dražja od RAID 5

RAID nivo 5 zahteva več spomina glede na RAID nivo 1

Uporaba zvezka s progami (RAID nivo 0)

Pri diskovnih pogonih zaradi enakomernega obremenjevanja

Poveča performanso diska v primerjavi z drugimi metodami konfiguriranja dinamičnih diskovnih zvezkov

Uporabimo ga v primerih, ko imamo podatke pomnjene drugje in potrebujemo hiter dostop do sekundarnega pomnilnika

Uporaba zrcalnega zvezka (RAID nivo 1)

Kot zrcalne zvezke vzpostavimo le dinamične diske

Ena od najbolj zanesljivih oblik tolerance do napak

Čas za tvorbo in osveževanje podatkov je zaradi zrcalnega diska podvojen

Hitrost branja diska je enaka kot pri enem disku

Sistemske in zagonske datoteke imamo lahko na zrcalnem zvezku

Uporaba zvezka RAID-5

Uporablja parnostne bloke na vseh diskih. Podatki na teh so pomnjeni v vrstah blokov. Vsak blok ima 64 KB.

Parnost se obravnava z Boolovo logiko

Parnostni blik je vedno v vrstici *n* diska *n*, pri čemer je *n* številka diska

Počasnejši od zvezka s progami

Potrebuje več spomina kot zrcaljenje ali preproste proge

Velikost pomnilnega prostora je $1/n$, pri čemer je n število fizičnih diskov v zvezku

Primerjava programskega RAID in aparaturnega RAID

Aparaturni RAID je neodvisen od operacijskega sistema

Aparaturni RAID je dražji od programskega, zato pa nudi naslednje prednosti:

Hitrejše branje in pisanje

Zmožnost dajanja zagonskih in sistemskih datotek na različne nivoje RAID

Zmožnost "vroče zamenjave" ("hot-swap") pokvarjenega diska brez izklapljanja strežnika

Več možnosti za reševanje okvarjenih podatkov in kombiniranje različnih nivojev RAID

Rezervne kopije diskov (disk backup)

Kopiranje s traku na strežniku

Trakovi pomnijo več podatkov

Ne obremenjujemo dodatno omrežja

V primeru okvare traku lahko kopiramo z drugega traku

Assurance that the registry is backed up

Kopiranje na omrežju

Lahko shranjujemo na en rezervni medij, kar poenostavlja administracijo

Ne moremo kopirati registra (registry)

Povečujemo promet na omrežju

Možnosti tvorbe rezervnih kopij

Normalni "backup"

Kopiranje celotnega sistema

Spreminja atribut "archive" vsake datoteke

Inkrementalni "backup"

Kopiramo le nove oziroma spremenjene datoteke

Kopiramo le datoteke z atributom "archive"

Odstranjuje atribut "archive"

Diferencialni "backup"

Podoben inkrementalnemu, vendar ne odstrani atribut "archive"

Hitrejša obnova v primerjavi z inkrementalnim

Možnosti tvorbe rezervnih kopij (nadaljevanje)

"Copy backup"

Kopiramo le izbrane datoteke in direktorije

Atribut "archive" ostaja nespremenjen

Ne vpliva na regularne postopke tvorbe rezervnih kopij

Dnevni "backup

Kopiramo le datoteke, ki so bile spremenjene na dan rezervnega kopiranja

Atribut archive"" se ne spremeni

Dodatna orodja v čarovniku "Backup or Restore"

Planirajmo avtomatsko izvajanje rezervnih kopiranj

Podatke restavriramo iz izmenljivih medijev

Povzetek

Windows Server 2003 podpira dve različni konfiguraciji diskov:

Osnovni (basic) diski so kompatibilnimi s starejšimi operacijskimi sistemi, rokovanje z njimi je skromno

Dinamični diski omogočajo bolj izčrpno upravljanje diskov, ki vključuje preproste (simple) spete (spanned) zvezke, zvezke s progami (striped), zrcaljenjem (mirrored) in zvezke RAID-5

Orodje "Disk Management" omogoča grafičen vpogled v diskovno konfiguracijo

Z orodjem "Disk Management" tvorimo particije na osnovnih diskih ali zvezke na dinamičnih diskih.

Povzetek

Montiranje pogona omogoča, da prihranimo pri dodeljevanju črk pogonom in dostop do pogona preko mape.

Planirajmo regularno defragmentacijo diskov z orodjem "Disk Defragmenter"

Uporabljajmo orodji "Check Disk" in "chdsk" za iskanje in popravljanje težav z diski

RAID nudi toleranco do napak za trde diske našega strežnika

Windows Server 2003 podpira RAID nivoje 0, 1 in 5

RAID nivo 0, poznan tudi kot "striping" (progast) ne nudi toleratemveč le podaljšanje življenske dobe diskov

Povzetek

Z zrcaljenjem ali dupleksiranjem diska (RAID nivo 1) so isti podatki zapisani v particijo obeh diskov, vključenih v zrcaljenje

Z nivojem RAID 5 se podatki zapisujejo v najmanj 3 diske v blokih po 64 KB

Toleranco do napak dosežemo s podatki o parnosti

Za regularno tvorbo rezervnih kopij pomembnih podatkov in sistemskih datotek z orodjem "Backup"

Uporabljamo trakove, CD-R, CD-RW in pogone ZIP

Možnost "restore" v orodju "Backup" omogoča restavracijo celotnega strežnika, posameznega diskovnega pogona, posamezne direktorije na disku ali le posamezne datoteke

Datotečni sistemi, Datoteke,Souporaba datotek

Cilji

Uporaba Windows 2003 kot datotečnega ali tiskalnega strežnika

Upravljanje zaščite datotek in direktorijev

Konfiguriranje souporabnih direktorijev in dovoljenj souporabe

Ugotavljanje veljavnih dovoljenj in reševanje zaščitnih konfliktov

Kako implementirati profile uporabnikov in domače direktorije

Nameščanje in konfiguriranje tiskalnikov

Upravljanje nadzora nad datotekami in direktoriji z uporabo dovoljenj NTFS

Najprej nekaj o zaščiti objektov

Kaj je NTFS?

Dovoljenja NTFS datotek in direktorijev

Kaj se dogaja z NTFS dovoljenji pri kopiranju in premikanju datotek in direktorijev?

Kaj je dedovanje NTFS dovoljenj?

Kako kopirati ali brisati dedovana dovoljenja?

Dobra praksa upravljanja dostopa do datotek in direktorijev s pomočjo dovoljenj NTFS

Kako upravljati dostop do datotek in direktorijev s pomočjo dovoljenj NTFS

Najprej nekaj o zaščiti objektov

Vsak objekt ima seznam kontrole dostopov (access control list, ACL) za upravljanje souporabe sredstev

Dostop je nadzorovan z zaščitnimi tehnikami:

Atributi

Dovoljenja

Nadzor

Lastništvo

Atributi datotek

Atributi so dediščina starejših operacijskih sistemov DOS

Hranimo jih med podatki v zaglavju datoteke

Datoteka jih ima ne glede na dovoljenja uporabnika za to datoteko

Atributi datotek (nadaljevanje)

FAT ima za datoteke in direktorije tri atribute:

Read-only

Hidden

Archive

NTFS atributi vključujejo

Index

Compress

Encrypt

Dovoljenja datotek in direktorijev

Dovoljenja za kontrolo dostopa do datoteke/direktorija s strani uporabnika ali skupine

Odkljukamo dovoljenja ali zapreke

Če ne odkljukamo nič, uporabnik nima dostopa

Če odkljukamo zapreko, je dostop blokiran, ne glede na dovoljenja drugih

Podedovana dovoljenja

Dovoljenja starševskega objekta veljajo za objekte-otroke

Glej sive kvadratke (ne moremo odkljukati)

Standardna dovoljenja za datoteke oziroma direktorije (pri sistemu NTFS)

Posebna dovoljenja

Napotki za dovoljenja

Direktorij \Windows zaščitimo pred splošnimi uporabniki

Direktorije s programskimi aplikacijami zaščitimo pred uporabniki, dovolimo pa jim izvajanje (Read & Execute, Write)

Tvorimo javno uporabljane direktorije za splošen dostop, razen za administrativne naloge (Modify)

Uporabniki naj imajo poln nadzor nad svojimi lastnimi direktoriji

Iz zaupnih direktorijev odstranimo dostop za splošne skupine (Everyone in Users)

Vedno se nagibajmo na stran prevelike zaščite

Konfiguriranje sledenja nadzora (auditing) nad direktoriji in datotekami

Z nadzorom sledimo aktivnosti nad direktorijem ali datoteko

Direktoriji in datoteke Windows Server NTFS omogočajo nadzor nad katerokoli obliko posebnih dovoljenj

Sledimo lahko vsaki obliki dostopa glede na uspeh ali neuspeh poskušanja

Nastavimo politiko nadzora (auditing policy) na popoln nadzor objekta

Uporabimo orodje "Domain Security Policy"

Kaj je NTFS?

NTFS je datotečni sistem, ki nudi :

Zanesljivost

Zaščito na nivoju datotek in direktorijev

Izboljšano upravljanje rasti pomnilnih medijev

Večkratna uporabniška dovoljenja

Dovoljenja za NTFS datoteke in direktorije

Kaj se dogaja z NTFS dovoljenji pri kopiranju in premikanju datotek in direktorijev?

Kaj je dedovanje NTFS dovoljenj?

Kako kopiramo ali odstranimo dedovana dovoljenja

Dobra praksa upravljanja dostopa do datotek in direktorijev s pomočjo dovoljenj NTFS

Kako upravljati dostop do datotek in direktorijev s pomočjo dovoljenj NTFS

Vaja: Upravljanje dostopa do datotek in direktorijev z NTFS dovoljenji

Ugotavljanje veljavnih dovoljenj (Effective Permissions)

Kaj so veljavna dovoljenja nad NTFS datotekami in direktoriji?

Kako ugotoviti veljavna dovoljenja nad NTFS datotekami in direktoriji

Učinki kombinacije NTFS dovoljenj in dovoljenj souporabnih direktorijev (Shared Folder)

Kako ugotovimo veljavna dovoljenja pri kombinaciji dovoljenj NTFS in dovoljenj souporabnih direktorijev

Kaj so veljavna dovoljenja nad NTFS datotekami in direktoriji?

Dovoljenja so kumulativna

Dovoljenja za datoteke so ločena od dovoljenj za direktorije

Zapora (d eny) prekrije vsa dovoljenja

Prevzemanje lastništva

Razprava: Nastavljanje NTFS dovoljenj

Kako ugotoviti veljavna dovoljenja za NTFS datoteke in direktorije

Vaja: Ugotavljanje veljavnih dovoljenj za NTFS datoteke in direktorije

Učinki kombinacije NTFS dovoljenj in dovoljenj souporabnih direktorijev (Shared Folder)

Kako ugotovimo veljavna dovoljenja pri kombinaciji NTFS dovoljenj in dovoljenj souporabnih direktorijev (Shared Folder)

Vaja: Ugotavljanje veljavnih dovoljenj pri kombinaciji NTFS in "Shared Folder" dovoljenj

Ugotovite valjavna NTFS dovoljenja

Ugotovite dovoljenja souporabnega direktorija

Upravljanje dostopa do souporabnih datotek s pomočjo "Offline Caching"

Kaj so "offline" datoteke?

Kako so sinhronizirane "offline" datoteke

Možnosti predpomnenja (caching) "offline file"

Kako uporabljamo "offline" predpomnenje

Kaj so "offline" datoteke ?

"offline" datoteke predstavljajo zmožnost upravljanja z dokumenti, ki uporabnikom nudi konsistenten "online" in offline" dostop do datotek

Prednosti uporabe "offline" datotek:

Podpora mobilnim uporabnikom

Avtomatska sinhronizacija

Prednosti performans

Prednosti tvorbe rezervnih kopij

Kako so sinhronizirane "offline" datoteke

Odklopljeni od omrežja

Windows Server 2003 sinhronizira omrežne datoteke z lokalno kopijo datotek

Uporabnik dela z lokalno kopijo datoteke

Logirani na omrežje

Windows Server 2003 sinhronizira "offline" datoteke z omrežno verzijo datotek

Če smo datoteko spreminjali na obeh lokacijah

Uporabnik odloči, katero verzijo bo uporabil. Lahko pa eno od datotek preimenuje in obdrži obe verziji

Možnosti predpomnenja (Caching) "offline" datotek

Kako uporabljamo "Offline Caching"

Vaja : Uporaba " Offline Caching "

Tvorite souporaben direktorij (shared folder) brez predpomnenja (caching) dokumentov ali programov

Omogočite ročno predpomnenje dokumentov

Vaja: Upravljanje dostopa do sredstev

Tvorba skupin

Konfiguriranje NTFS zaščite
Konfiguriranje zaščite souporabnega direktorija
Konfiguriranje "offline" nastavitev
Konfiguriranje lastništva direktorijev in datotek
Direktoriji so najprej last konta, ki jih je tvoril
Lastniki direktorija lahko spreminjajo dovoljenja za direktorije
Lastništvo lahko spremenimo le, če imamo polna dovoljenja ali dovoljenje "Take Ownership"
Skupina administratorjev lahko prevzame nadzor od katerikoli skupine ne glede na dovoljenja
Upravljanje dostopa do souporabnih direktorijev
Kaj so souporabni direktoriji (Shared Folders)?
Kaj so administrativni uporabni direktoriji (Administrative Shared Folders)?
Kdo lahko dostopa do souporabnih direktorijev?
Kako tvorimo souporabne direktorije
Kaj so objavljeni souporabni direktoriji (Published Shared Folders)?
Kako objavljamo souporabne direktorije
Dovoljenja souporabnih direktorijev
Kako nastavljamo dovoljenja na souporabnih direktorijih
Kako povezujemo souporabne direktorije
Kaj so souporabni direktoriji (Shared Folders)?
Kopiranje souporabnega direktorija
Originalni souporabni direktorij je še vedno souporaben, kopija direktorija pa ne več
Premik souporabnega direktorija
Direktorij ni več souporaben
Skrivanje souporabnega direktorija
Dodaj $ za imenom souporabnega direktorija
Uporabniki lahko dostopajo do souporabnega direktorija s tipkanjem UNC, na primer, \\server\secrets$
Kaj so administrativni souporabni direktoriji?
Kdo ima dostop do souporabnega direktorija?
Windows Server 2003 domenski krmilnik (DC)
Skupina "Administrators"
Skupina "Server Operators"
Članski strežnik ali samostojni strežnik z operacijskim sistemom Windows Server 2003
Skupina "Administrators"
Skupina "Power Users"
Tvorba souporabnih direktorijev
Da bi direktorij postal dostopen za druge uporabnike v omrežju, nastavimo direktoriju lastnost "***share***

Souporabne (shared) direktorije lahko skrijemo:
Takoj za imenom dodamo znak $
Dovoljenja souporabe
Kako tvorimo souporaben direktorij

Kaj so objavljeni souporabni direktoriji (Published Shared Folders)?
Objavljen souporabni direktorij je objekt souporabnega direktorija v aktivnem imeniku
Odjemalci lahko v aktivnem imeniku iščejo souporabne direktorije, ki so objavljeni
Odjemalcem ni potrebno poznati ime strežnika, da bi se povezali s souporabnim direktorijem
Kako objaviti souporabni direktorij
Dovoljenja souporabnega direktorija
Kako nastavimo dovoljenja za souporaben direktorij

Kako se povežemo na souporabne direktorije
Vaja: Upravljanje dostopa do souporabnih direktorijev
Tvorba souporabnih direktorijev
Testiranje dovoljenj za branje souporabnega direktorija
Testiranje dovoljenj za polni nadzor souporabnega direktorija
Ugotavljanje veljavnih dovoljenj
Upoštevati moramo lokacijo datotek in direktorijev
Nova datoteka podeduje dovoljenja njenega direktorija
Datoteke, kopirane v direktorij na istem zvezku, podedujejo dovoljenja novega direktorija
Datoteke, ki jih premaknemo v direktorij na istem zvezku, obdržijo svoja originalna dovoljenja
Datoteke, ki jih premaknemo na drug zvezek, podejujejo dovoljenja novega direktorija

Reševanje konfliktov z zaščito
Zavihek "Effective Permissions" računa članstvo skupine in dedovanje dovoljenj

Datotečni in tiskalni servisi

Souporaba tiskalnika
Več uporabnikov lahko souporablja en tiskalnik
Souporabni direktoriji
Dajejo uporabnikom možnost shranjevanja dokumentov na strežnik – kot v svoje domače direktorije
U porabniški profili
Dajejo uporabnikom konsistentno namizje in centralno upravljajo konfiguracije
Souporaba tiskalnika
Souporabni tiskalnik (shared printer) je lahko na kateremkoli strežniku ali računalniku z najmanj Windows 95

Souporabne tiskalnike lahko povežemo na omrežje na različne načine:

Strežniki
Delovne postaje (workstations)

Strežne tiskalne naprave
Namestitev souporabnega tiskalnika
Souporaben tiskalnik konfiguriramo tako, da je najprej navezan na strežnik kot lokalni tiskalnik, nato pa omogočimo njegovo souporabo

Zahteve za tiskalni strežnik:
Dovolj RAM za obdelavo dokumentov
Dovolj prostora na disku za pomnenje dokumentov , tiskanih v ozadju

Tiskalniki, ki jih namestimo s pomočjo čarovnika "Add Printer", so privzeto souporabni in objavljeni v aktivnem imeniku

Tiskalnike, ki so nameščeni s pomočjo "Plug and Play", moramo za souporabo konfigurirati po namestitvi
Konfiguriranje souporabnega tiskalnika
Nastavitev tiskalnika spremenimo v zavihkih v pogovornem oknu "Printer properties":
Splošni podatki o tiskalniku
Souporaba tiskalnika
Nastavitev vrat tiskalnika
Planiranje tiskanja in napredne možnosti
Zaščita
Nstavitve naprave
Implementacija domačih direktorijev (Home Folders)
Tvorimo direktorij, kot na primer "USERS" ali "HOME"

Dodelimo dovoljenja za branje

Nastavimo souporabo direktorija

Pri "properties" vsakega uporabnika v zavihku "profile" dodelimo v rubriki "Home Folder" bodisi "Connect" bodisi "Local Path":
\\servername\sharename\%username%
Implementacija uporabniških profilov
Tvorimo direktorij, na primer "PROFILES"

Dodelimo dovoljenja za branje

Direktorij naj bo souporaben

Pri lastnostih vsakega uporabnika v zavihku "profile" dodelimo za "profile Path"
\\servername\sharename\%username%

Priključitev računalnika v domeno

Računalniki uporabnikov in operacijskimi sistemi Windows 2000 in XP se pridružijo (join) domeni.

Pridružitev (joining) tvori računalniški konto (computer account) v aktivnem imeniku. Računalniški konto je dodan bodisi:

at the end user workstation while joining the domain (must have domain admin username and password).

via Active Directory Computers and Users before hand.
"Offline " datoteke
Predpomnijo souporaben direktorij na disku odjemalca, tako da lahko dostopamo do njega tudi brez omrežne povezave

Ko povezavo obnovimo, pride do sinhronizacije spremenjenih datotek z omrežno verzijo datotek
Objavljanje souporabnega direktorija v aktivnem imeniku
Tako postanejo objekti hitro dostopni uporabnikom preko aktivnega imenika
Omogoča replikacijo podatkov o objektih na domenskih krmilnikih (DC)
Omogoča odjemalcem hitrejšnje iskanje
Za Windows 2000 in XP uporabimo aktivni imenik
Za starejše MS Windows namestimo"Directory Service Client "
Lahko objavimo za souporabo za:
Dostop znotraj domene
Upravljanje organizacijskih enot in nastavitve dostopa
Konfiguriranje " Web Sharing "
Namestitev "Internet Information Services" (IIS) izvedemo v zavihku "Web Sharing"
Porazdeljen datotečni sistem (distributed file system)
Souporabni direktoriji na omrežju lahko izgledajo kot hierarhija direktorijev
To poenostavlja dostop uporabnikov
Pri replikaciji souporabnih direktorijev imamo možnost tolerance izpadov
Uporabljamo Microsoftov servis "File Replication"
S porazdelitvijo dostopa do direktorijev med več strežniki dosežemo uravnovešenje bremena
Izboljšan je dostop do internetnih in intranetnih lokacij
Rezervno kopiranje iz ene množice glavnih direktorijev
Primer DFS (porazdeljenega datotečnega sistema)
DFS Model i in topologija
Samostojni in **domensko osnovani** modeli
Samostojni
Brez aktivnega imenika
DFS direktoriji niso povezani na druge računalnike
Domensko osnovani
Dostopni le članom domene
Izkoriščajo prednosti aktivnega imenika

Imajo večnivojsko hierarhično strukturo

Lahko implementirajo toleranco do izpadov in uravnovešenje bremena

Koren DFS (DFS root)

Glavni vsebnik (container) v aktivnem imeniku, ki vsebuje povezave na souporabne direktorije

Direktoriji iz vseh domenskih računalnikov so prikazano, kot če bi bili v klavnem direktoriju

DFS povezave (DFS links)

Dostopna pot med korenom DFS in souporabnimi direktoriji

Replica sets (targets)

Zbirka souporabnih direktorijev, ki je replicirana na enem ali več strežnikih v domeni

Konfiguriranje diskovnih kvot

NTFS nudi možnost vzpostavljanja diskovnih kvot

Onemogoča uporabnikom zapolnitev diskov

Z opozorili o omejitvah kvot pomaga uporabnikom upravljanje z diski

Sledi potrebe po diskovnih zmogljivostih glede na posamezne uporabnike. To omogoča planiranje vnaprej

Nudi administratorju strežnika podatke, kdaj se uporabniki bližajo omejitvi kvot

Kaj je to UNC

One definition of "UNC (Universal Naming Convention) name" (from the Windows 2000 on-line Glossary) reads as follows: "A full Windows 2000 name of a resource on a network . It conforms to the *\\servername \sharename* syntax, where *servername* is the server's name and *sharename* is the name of the shared resource. UNC names of directories or files can also include the directory path under the share name with the following syntax: *\\servername \sharename \directory \filename* ."

Upravljanje omrežnih servisov

Windows Server 2003

Cilji

Implemen nacija Microsoft DHCP

Implement acija Microsoft DNS

Implement acija Microsoft WINS

Namestitev in konfiguriranje " Internet Information Services "

Konfiguriranje strežnika Telnet

Microsoft DHCP

Protokol v družini TCP/IP

Uporaba s servisi DHCP za odkrivanje prisotnosti novih omrežnih klijentov in dodeljevanje IP naslovov takim klijentom

Strežnik DHCP ima dodeljeno območje naslovov

Celovitemu območju naslovov pravimo "scope" (obseg)

V enem DHCP strežniku je možnih več obsegov, kar naj odraža strukturo podomrežij oziroma segmente omrežja

Vsak naslov velja določeno časovno obdobje

Microsoft DHCP (nadaljevanje)

En strežnik DHCP lahko podpira do 1000 obsegov in 10.000 DHCP klijentov

To je priporočilo Microsoft, ne pa omejitev

Možnost avtomatske registracije "forward and reverse lookup zone records" s strežnikom DNS

Ko strežnik DHCP dodeli nov IP naslov, avtomatsko posodobi strežnik DNS

DCHP namestimo z orodjem "Add and Remove Programs"

Networking service in Windows components

Konfiguriranje strežnika DHCP

Vzpostavimo en ali več obsegov celovitih naslovnih območij

Pri konfiguraciji vsakega obsega podamo IP naslove strežnikov DNS

Vsak obseg aktiviramo

Avtoriziramo strežnik DHCP

To je varnostni ukrep, ki naj zagotovi skrbno rokovanje z naslovi IP

Konfiguriramo strežnik DHCP in njegove klijente tako, da bodo zapisi DNS avtomatsko posodabljani

Priporočeno, ne pa zahtevano

Konfiguriranje avtomatske DNS registracije

Preverimo, da je strežnik DHCP vzpostavljen tako, da avtomatsko registrira IP naslove, ki jih predaja

Preverimo, da je strežnik DHCP vzpostavljen za tipe klijentov na našem omrežju

Za strežnike samo s klijenti Windows 2000, XP ali Server 2003 dinamično osvežujemo zapise le, če to zahtevajo klijenti

Sicer DNS zapise vedno dinamično osvežujemo

Za strežnike s klijenti Windows 95, 98 ali NT dinamično osvežujemo zapise za klijente, ki osvežitve niso zahtevali

Microsoft DNS

Nudi imenski prostor DNS (DNS namespace)

Preslikava imena računalnikov v IP naslove in IP naslove v imena računalnikov

DNS strežnik, najbolj kompatibilen z aktivnim direktorijem

Nudi DNS replikacijo skozi aktivni direktorij

DNS strežniki morajo imeti statične IP naslove

Namestitev podobna kot pri drugih komponentah Windows, na primer kot pri DHCP

Namestimo pred namestitvijo aktivnega direktorija

DNS cone

Particija, ki vsebuje zapise o sredstvih v tabeli "lookup"

Cona "Forward lookup"

Vsebuje zapise z imeni računalnikov, ki povezujejo računalniška imena z IP naslovi

Avtomatsko tvorjena za domenski krmilnik (DC, domain controller) v domeni

Zapis "Host address (A) resource record" je za IPv4

Zapis "Host address (AAAA) resource record" je za IPv6

En strežnik ima lahko več "forward lookup zones"

DNS cone (nadaljevanje)

Cona "Reverse lookup"

Vsebuje zapis "PTR" (pointer)

Vsebuje povezave iz IP naslovov na imena računalnikov

Ko namestimo DNS, se ne konfigurira avtomatsko

Jo lahko uporabljamo pri nadzoru omrežja s podatni o IP naslovih

Tvorimo cono "reverse lookup" pred tvorbo conskih zapisov " DNS forward lookup"

Ko tvorimo cono " forward lookup", se lahko avtomatsko tvori ustrezen PTR zapis cone "reverse lookup"

Uporaba protokola za dinamično osveževanje DNS

Omogoča avtomatično osveževanje podatkov na strežniku DNS v koordinaciji z DHCP

Prihrani administratorju precej časa

Preverimo, da je DNS konfiguriran za uporab " DNS dynamic update protocol"

Naj bodo osvežitve varne. Zato naj osveževanje izvajajo le pooblaščeni klijenti

Strežniki DHCP morajo tudi biti registrirani za izvajanje DNS registracije

DNS Repli kacija

Primarni DNS strežnik

To je glavni strežnik za neko cono

Vse spremembe cone moramo narediti na tem DNS strežniku

Sekundarni DNS strežnik

Vsebuje kopijo podatkovne baze o coni primarnega DNS strežnika

Ne uporabljamo ga za spreminjanje

Služi kot rezerva v primeru izpada primarnega strežnika

Omogoča raznje glavnega strežnika

Zmanjšuje zasičenost

DNS Repli kacija (nadanjeljeva)

En DNS strežnik je lahko glavni za več domen

En DNS strežnik je lahko sekundarni strežnik za več primarnih strežnikov

En DNS strežnik je lahko primarni strežnik za eno cono in sekundarni strežnik za drugo cono

Če uporabljamo aktivni direktorij z dvema ali več domenskimi krmilniki (DC), vzpostavimo servise DNS na najmanj dveh DC in tako omogočimo replikacijo multimaster

Nudi omrežju neprekinjene servise DNS

Reševanje težav z DNS

Prepričajmo se, da so pognani servisi strežnika DNS in klijenta DNS in da je bil na DNS strežniku vzpostavljen njihov avtomatski zagon

Nastavitve preverimo z orodjem " Computer Management "

Status ni podatki

"Startup type box " mora biti nastavljen na " Automatic "

Microsoft WINS

Automatično registrira omrežne klijente, ki uporabljajo NetBIOS

Tvori podatkovno bazo, ki jo lahko izprašujejo drugi omrežni klijenti, ki želijo locirati nek računalnik

Namestitev je podobna kot pri DHCP in DNS

Tipično uporabi privzete nastavitve konfiguracije

Lahko ga konfiguriramo za replikacijo z drugimi WINS strežniki v domeni

Pri težavah se prepričajmo, če je WINS pognan, lahko pa zaustavimo in s ponovnim pogonom ponovno inicializiramo servis.

Microsoft Internet Information Services

Omogočajo, da se Windows Server 2003 obnaša kot Web strežnik in ponuja spletne strani

Vključeni so na namestitvenem CD za Windows Server 2003

Vključen je "Internet Server Application Programming Interface" (ISAPI)

Skupina datotek DLL, ki so aplikacija in filtri

Aplikacija omogoča povezovanje drugih programov in pospešuje izvajanje programov

Filtre uporabljamo za avtomatsko proženje programov

Microsoft Internet Information Services (nadaljevanje)

IIS vsebuje servise World Wide Web

IIS strežnik lahko deluje kot SMTP, NNTP in FTP strežnik

Windows Server 2003 nudi:

Arhitektura "Privileged-mode"

Zmožnost tolerance do napak

Dostop do podatkovne baze s pomočjo gonilnikov " IIS Open Database Connectivity" (ODBC)

IIS je kompatibilen z varnostnimi tehnikami, kot so MPPE, IPSec inSSL enkripcija

Namestitev IIS

Windows Server 2003 nameščen na računalnik

TCP/IP nameščen na gostitelju IIS

Dostop do ISP

IP naslov, "subnet" maska, IP naslov "**Text body indent** gateway"

Dovolj prostora na disku za IIS in datotekespletnih strani

Disk formatiran za datotečni sistem NTFS zaradi boljših performans in varnosti

Imenujemo metodo resolucije

Virtual ni direktorij

URL formatted address that provides an Internet location for an actual physical folder on a Web server

URL format consists of the server name, an alias for the virtual directory, and the file name

Used to access and publish Web documents

Create a virtual directory using the Virtual Directory Creation Wizard in the IIS Manager

Configure security and other options using the properties tab

Upravljanje in konfiguriranje IIS Web strežnika

Application pools

Groups similar Web applications for management

SMTP virtual server

Manages Internet e-mail

NNTP virtual server

Manages newsgroup services

Web service extensions

For compatibility with FrontPage

Enables the use of other extensions, such as Active Server pages and Internet printing

Upravljanje in konfiguriranje IIS Web strežnika (nadaljevanje)

Web sites

Manages multiple Web sites from one administrative Web server

One **Text body indent** Web site is automatically set up

Has several configuration parameters, including directory security with authentication access options

The **Text body indent** is anonymous access

Windows Media Services

Provides streaming media services

Streaming mode allows audio and video to begin playing as soon as received

Separate from the IIS component

Enables a Web server to serve voice and video multimedia applications

Install using Add/Remove Windows Components after IIS is installed

Strežnik Telnet

Protocol in TCP/IP suite that enables a client to act as a terminal to access a server

Particularly useful for non-Windows clients

Requires the following:

Telnet Server running on Windows Server 2003

Microsoft Telnet Client or another version of Telnet on the client computer

Server and client must be configured for TCP/IP

User must have a user account and supply the account name and password when logging in

Strežnik Telnet

Uses NTLM authentication to protect server access

Windows Server 2003 Telnet Server Service can be started in two ways:

Through the Computer Management tool

From the Command Prompt window:

Start telnet by typing "telnet servername"

View a command prompt window on the server

Enter "telnet /?" to view telnet command information

Povzetek

DHCP is a work-saving protocol because it enables IP addresses to be leased dynamically

Configuring DHCP involves configuring scopes, which are ranges of IP addresses from which addresses are leased to clients

Plan to configure DHCP to dynamically update DNS

Part of configuring DNS involves forward and reverse lookup zones

Povzetek

Configure Dynamic DNS to enable automated IP address registration in coordination with a DHCP server

Plan to set up two or more DNS servers on most networks and to integrate DNS with Active Directory for DNS replication and load balancing

If your network uses NetBIOS naming, install WINS

To implement a Web server, install Internet Information Services

Povzetek

Create IIS virtual directories to enable multiple users to publish on a Web site

Plan to configure each Web site to control client timeout, server bandwidth, number of connections, and authentication

Install Windows Media Services to enable a Windows 2003 Server, including one configured with IIS, to provide streaming multimedia

If you have users, such as UNIX computers, that need to connect using Telnet, configure Windows 2003 as a Telnet Server

Konfiguriranje

Remote Access Services

Cilji

Razumevanje "Remote Access Services" v "Windows Server 2003"

Konfiguriranje Remote Access Services

Implementacija virtualnega privatnega omrežja

Reševanje problemov pri Remote Access Services in namestitvah virtualnih privatnih omrežij

Povezava oddaljenih uporabnikov preko "Terminal Services"

Uvod v oddaljeni dostop

Oddaljen dostop danes pogosto uporabljamo

Telekomunikacije in poslovna potovanja

Windows Server 2003 omogoča strežniku, daq deluje tudi kot strežnik za oddaljen dostop

Strežnik za oddaljen dostop (Remote Access Services (RAS) server) postane tako, da uporabi "Routing and Remote Access Services" (RRAS)

Istočasno lahko opravlja tudi normalne strežniške funkcije

Uporabnik lahko dostopa do strežnika RAS preko telefona ali preko interneta ali intraneta

Uporaba "Microsoft Remote Access Services"

Podpira naslednje operacijske sisteme odjemalcev:

MS-DOS, Windows 3. in 3.11

Windows 95, 98 in ME

Windows NT in 2000 (vse platforme)

Windows Server 2003 inXP Professional

Podpira naslednje tipe povezav:

Asinhroni in sinhroni modemi

Komunikacije "Null modem"

Kabelski modemi

Klicne in najete telefonske linije

Uporaba "Microsoft Remote Access Services" (nadaljevanje)

T-carrier lines

Posvečena najeta telefonska linija za hitrosti do 44.736 Mbps

DSL (digital na abonirana linija)

Te hnologija, ki uporablja napredne modulacijske tehnike na navadnih telefonskih linijah za hitrosti do 60 Mbps

ISDN (Integrated Services Digital Network)

Tele komunikacijski standared za posredovanje podatkov po digitalnih telefonskih linijah s trenutno omejitvijo 1.536 Mbps

Frame Relay

WAN komunikacijska tehnologija, ki temelji na izmenjavi paketov in virtualnih povezavah za hitrosti do 45 Mbps

Uporaba "Microsoft Remote Access Services" (nadaljevanje)

X.25

Starejši protokol z izmenjavo paketov za povezavo omrežij s hitrostmi do 2.048 Mbps

Kompatibilnost z naslednjimi protokoli za prenos po omrežju in oddaljeni dostop

TCP/IP

IBX

NetBEUI

SLIP, CSLIP

PPP, PPTP, L2TP

Implemenacija protokolov za oddaljeni dostop

Protokoli za oddaljeni dostop (remote access protocols) prenašajo vgrajene omrežne pakete preko WAN povezave

Paket je oblikovan za omrežni prenosni protokol, najbolj pogosto TCP/IP

Serial Line Internet Protocol (SLIP)

Stari protokol za oddaljene komunikacije

Obsežno zaglavje (header) paketa povečuje "režijo"

Ne podpira omrežne avtentikacije

Namenjen le asinhroni komunikaciji

Ne podpira večkratnih plasti omrežnih povezav

Konfiguriranje "Remote Access Services"

Compressed Serial Line Internet Protocol (CSLIP)

Podoben SLIP, vendar pred pošiljanjem paketa komprimira podatke v zaglavju

Point-to-Point Protocol (PPP)

Podpira več omrežnih protokolov

Avtomatsko posreduje sočasne komunikacije z več omrežnimi plastmi

Podpira sinhrone in asinhrone komunikacije

Podpira avtentikacijo povezav

Konfiguriranje "Remote Access Services" (nadaljevanje)

Point-to-Point Tunneling Protocol (PPTP)

Dopolnjuje PPP tako, da omogoča oddaljene komunikacije preko interneta, intraneta ali VPN

Layer Two Tunneling Protocol (L2TP)

Podoben PPTP, omogoča pa posredovanje na osnovi naslavljanja MAC in naslavljanja IP

PPP je najbolj pogosto uporabljan protokol za oddaljeni dostop

Imamo ga na odjemalskih računalnikih z Windows 95 ali novejšimi operacijskimi sistemi

Konfigiriranje strežnika za oddaljeni dostop (Remote Access Server)

Povezuje modeme neposredno v omrežje ali preko strežnika za dostop

Vzpostavimo strežnik Windows kot strežnik RAS

Konfiguriramo pravilne protokole za povezave preko telefona

Konfiguriramo "DHCP relay agent"

Konfiguriramo protokole Multilink in Bandwidth Allocation"

Konfiguriramo "RAS security"

Vzpostavimo telefonsko in oddaljeno povezavo

Konfiguriramo RAS na odjemalskih računalnikih

Namestitev RAS

Uporabimo orodje "Routing and Remote Access"

Izberemo "Remote access" (telefonski klic ali VPN)

Če je na voljo, uporabimo strežnik DHCP za avtomatsko naslavljanje IP, sicer uporabimo APIPA

Če vzpostavljamo večkratne RAS strežnike, standardizirano avtentikacijo in politike dostopa ali zmožnosti "accounting", uporabimo strežnik RADIUS

Izogibajmo se uporabi strežnika RAS kot usmerjevalnika (router)

Konfiguriranje RAS

Konfiguriranje agenta "DHCP Relay"

Ko je nek RAS strežnik konfiguriran za uporabo DHCP, moramo RAS strežnik določiti za agenta "DHCP relay"

Podamo IP naslov strežnika DHCP

Konfiguriramo "hop count"

Maksimalno število usmerjevalnikov, ki jih lahko neko IP obvestilo prečka preko odjemalca, strežnika RAS in strežnika DHCPr

Nastavimo "boot threshold"

Čas odziva, dan lokalnemu DHCP strežniku, preden se povežemo z nekim oddaljenim DHCP strežnikom

Konfiguriranje protokola "Multilink in Bandwidth Allocation"

Multilink združuje dva ali več komunikacijskih kanalov tako, da izgledajo kot en širok kanal (aggregated links)

Must be implemented in both client and server

Bandwidth Allocation Protocol (BAP) uporabljamo z Multilink in tako zagotavljamo povezavo z dovolj veliko hitrostjo oziroma pasovno širino

Povezave po potrebi dinamično opuščamo ali dodajamo

Bandwidth Allocation Control Protocol (BACP)

Podobno kot BAP, vendar v primeri dveh ali več odjemalcev z enako pasovno širino izbere prednostnega

Konfiguriranje varnosti RAS

Dostop uporabniških kontov je varovan z zaščito, določeno s politiko skupin (group policy) ali politiko varnosti domene

Dodatne varnostne možnosti vsebujejo:

Konfiguriranje politike oddaljenega dostopa

Konfiguriranje varnosti pri klicnem dostopu

Konfiguriranje odjemalcev in protokolov odjemalcev

Politika oddaljenega dostopa (Remote Access Policy)

Pogoji

Množica atributov, ki so primerjani z atributi tipa povezave

Če se vsi pogoji ujemajo, se preverjajo dovoljenja

Dovoljenja

Dostop uporabniškega konta

Dovoljenja politike oddaljenega dostopa

Če dovoljenja so, se preveri nastavitve profila

Profile

Primerjajo se nastavitve, kot je avtentikacija, enkripcija, časovne omejitve

Konfiguriranje profila za oddaljeni dostop (Remote Access Profile)

Avtentikacija in enkripcija

V profilu za oddaljeni dostop lahko izberemo možnost avtentikacije ali enkripcije ali oboje

Strežnik RAS se usklajuje za avtentikacijo z odjemalcem, dokler ne najde delujoče metode avtentikacije

Tipi enkripcije:

IPSec je množiva komunikacijskih in enkripcijskih standardov, temelječa na IP in tvorjena preko IETF

MPPE je dvotočkovna (end-to-end) tehnika enkripcije, ki uporablja posebne, od 40 do 128 bitne ključe

DES uporablja med dvema postajama tajni mključs. Trojni DEC uporablja tri ključe, sestavljene v en dolg ključ

Konfiguriranje telefonske povezave

Konfiguriranje varnosti "callback" pri uporabniškem kontu

No callback

Strežnik dovoli dostop pri prvem poskusu klica

Set by caller

Število, uporabljeno za "callback", ponujeno s strani oddaljenega računalnika

Always callback to

Število je shranjeno na strežniku

Konfiguriranje klicnih povezav za strežnik

Konfiguriranje odjemalčevih klicnih povezav na RAS

Implemenacija virtualnega privatnega omrežja (Virtual Private Network, VPN)

Virtualna privatna omrežja (VPN) uporabljajo za varen prenos podatkov preko javnega omrežja protokole LAN in "tunelske" protokole

Učinkovito za lokalne povezave

VPN tvorijo enkriptirani tunel:

Vzpostavitev PPP povezave z ISP

Vzpostavitev druge povezave s trežnikom VPN

Odjemalec in strežnik se uskladita, kako bodo podatki enkapsulirani in enkriptirani

Vzpostavitev strežnika VPN

Namestitev in konfiguriranje strežnika VPN s pomočjo orodja "Routing and Remote Access"

Vzpostavitev lastnosti strežnika VPN

Konfiguriranje VPN kot usmerjevalca

Tvorba politike oddaljenega dostopa za VPN in nastavitev profilov

Identično tistom na strežniku RAS

Konfiguriranje števila vrat za povezavo WAN

Tako WAN Miniport (PPTP) kot WAN Miniport (L2TP)

Odpravljanje težav pri nameščanju RAS in VPN

Aparaturne rešitve:

Za razreševanje problemov in konfliktov med sredstvi uporabimo "Device Manager"

Preverimo kabelske in telefonske povezave za zunanje naprave

Preverimo povezave računalniških kartic in kartice po potrebi premestimo

Stenske povezave testiramo ločeno od modemskih povezav

Preverimo konfiguracije v zunanjih DSL napravah

Odpravljanje težav pri nameščanju RAS in VPN (nadaljevanje)

Programske rešitve, če ni povezav

Preverimo, če je omogočen RAS ali VPN

Preverimo konfiguracije vrat, TCP/IP in DHCP

Če uporabljamo RADIUS, preverimo, če je nameščen IAS

Preverimo, če sta politika oddaljenega dostopa in profil konsistentna s potrebami uporabnika

Programske rešitve, če so omejitve v povezavah

Preverimo klicne povezave, ime uporabniškega konta in uporabniška dovoljenja

Preverimo, če ima konto odjemalca klicni dostop, pravilno nastavitev "callback" in kompatibilne modeme

Terminal Services

Terminalski strežniki omogočajo odjemalcem izvajanje storitev in programskih aplikacij na strežniku namesto na odjemalcu

Dostop omogočajo skoraj vsem odjemalskim operacijskim sistemom

Uporabljamo lahko cenene tanke odjemalce

Tenki odjemalci uporabljajo preproste operacijske sisteme

Centraliziran nadzor, kako uporabljamo programe

Terminal Services (nadaljevanje)

Pri namestitvi Terminal Services namestimo tudi "Terminal Services Licensing" za odražanje števila uporabniških licenc

Za strežnike brez starejših aplikacij omogočimo polno varnost

"Terminal Services" upravljamo z orodjem "Terminal Services Manager"

Konfiguriranje Terminal Services

Za konfiguriranje lastnosti oddaljenih povezav uporabimo orodje "Terminal Services Configuration"

Za vsako kartico NIC v strežniku konfiguriramo eno povezavo

Nastavitev dovoljenj

Polna kontrola, dostop uporabnikov, dostop gostov, posebna dovoljenja

Avtentikacijo nastavimo na "none" ali na "standard Windows"

Nastavimo enkripcijo

Kompatibilno z odjemalcem, skladno z FIPS, visoko ali nizko

Konfiguriranje Terminal Services (nadaljevanje)

Konfiguriramo povezavo na oddaljeno namizje

Za dostop odjemalcev do namestitvenih datotek tvorimo "shared folder"

Odjemalci lahko dostopajo do tega direktorija in poženejo namestitveni program

Konfiguriranje licenciranja

Aktiviramo strežnik

Za aktiviranje licenc se povežemo z Microsoft

Namestitev aplikacij na Terminal Server

Oporabimo orodje "Add or Remove Programs "

Povzetek

Windows 2003 Server, ki je konfiguriran za storitve RAS, omogoča odjemalcem oddaljen dostop do strežnika ali do omrežja strežnikov

Oddaljen dostop do omrežja Windows Server 2003 lahko izvedemo preko telefonskih linij, preko internetnih povezav in preko usmerjevalnikov (routers)

Promet preko telefonskih linih izvajamo preko PPP

Promet preko interneta ali VPN izvajamo s protokoli PPTP in L2TP

Povzetek

Razpoložljivost in varnost strežnikov RAS in VPN upravljamo s pomočjo politik oddaljenega dostopa (remote access policies)

Strežnik VPNkonfiguriramo s podobnimi koraki kot pri konfiguriranju strežnika RAS

Isti strežnik je lahko konfiguriran za nudenje storitev RAS in VPN

V primeri težav pri povezovanju RAS in VPN moramo preverjati tako aparaturno kot programsko opremo

Povzetek

"Terminal Services" omogočajo uporabnikom dostop do strežnika in poganjanje aplikacij na tem strežniku

Za "Terminal Services" konfiguriramo vsako omrežno kartico (NIC) z lastnostmi za oddaljen dostop

Vključno z nastavitvami za varnost, logiranje, odjemalca in okolja

Uporabniki dostopajo do terminalskega strežnika tako, da namestijo na strani odjemalca programsko opremo za oddaljeno povezavo z namizjem (remote desktop connection)

Varnost in Windows Server 2003

Pregled varnosti in Windows Server 2003

Kaj so uporabniške pravice ?

Primerjava uporabniških pravic in dovoljenj

U porabniške pravice, dodeljene vgrajenim skupinam

Kako dodelimo uporabniške pravice

Kaj so uporabniške pravice ?

Primerjava uporabniških pravic in dovoljenj

Uporabniške pravice, dodeljene vgrajenim skupinam

Kako dodelimo uporabniške pravice

Vaja: dodeljevanje uporabniških pravic

Odstranjevanje uporabniške pravice in preverjanje, če je to bilo izvedeno

Dodajanje uporabniške pravice in preverjanje, če je to bilo izvedeno

Uporaba varnostnih šablon za zaščito računalnikov

Kaj je varnostna politika (Security Policy)?

Kaj so varnostne šablone (Security Templates)?

Kaj so nastavitve v varnostnih šablonah?

Kako naredimo lastno varnostno šablono

Kako uvozimo varnostno šablono

Kaj je varnostna politika ?

Kaj so varnostne šablone ?

Kaj so nastavitve varnostnih šablon ?

Kako tvorimo lastno varnostno šablono

Kako uvozimo varnostno šablono

Vaja: Uporaba varnostnih šablon za zaščito računalnikov

Tvorba varnostne šablone

Uvoz varnostne šablone na GPO

Testiranje varnostne politike računalnika

Kaj je orodje "Security Configuration and Analysis?

Kako testiramo zaščito računalnika

Orodje "Security Configuration and Analysis"

Kako testiramo zaščito računalnika

Vaja: Testiranje računalniške zaščite

Tvorba lastne varnostne šablone (security template)

Analiziranje nastavitve zaščite na računalniku z nastavitvami zaščite v prilagojeni zaščitni šabloni

Konfiguriranje nadzora (Auditing)

Kaj je nadzor (auditing)?

Kaj je politika nadzora (Audit Policy)?

Tipi dogodkov za nadzor

Napotki za planiranje politike nadzora

Kako omogočimo politiko nadzora

Kako omogočimo nadzor datotek in direktorijev

Kako omogočimo nadzor objektov aktivnega imenika

Dobra praksa za konfiguriranje nadzora

Kaj je nadzor (auditing) ?

Nadzor sledi aktivnostim uporabnika in operacijskega sistema in zapisuje izbrane dogodke v varnostne zapise (security logs)

Kaj je politika nadzora (Audit Policy)?

Varnostna politika določa varnostne dogodke, o kotarih bo poročano administratorju omrežja

Varnostno politiko vzpostavimo za:

Sledenje uspešnim ali propadlim dogodkom

Minimiziranje nepooblaščene uporabe sredstev

Vzdrževanje zaposa o aktivnosti

Varnostne dogodke beležimo v varnostne zapise (security logs)

T ipi dogodkov za nadzorovanje

Logiranje kontov

Upravlja nje kontov

Dostop do servisov imenika

Logiranje

Dostop do objektov

Sprememba politike

Uporaba privilegijev

Sledenje procesom

Sistem

Napotki za planiranje politike nadzora

Kako omogočimo politiko nadzora

Kako omogočimo nadzor datotek in direktorijev

Vaja : Omogočanje (vklop) nadzora datotek in direktorijev

Kako omogočimo (vklopimo) nadzor za objekte aktivnega imenika

Vaja: Vklop nadzora organizacijske enote

Dobra praksa konfiguriranja nadzora

Upravljanje z varnostnimi zapisi

Kaj so "Log Files"?

Pogosti varnostni dogodki

Naloge, povezane z upravljanjem datotek z varnostnimi zapisi (Security Log Files)

Kako upravljamo s podatki v datotekah z varnostnimi zapisi

Kako gledamo na dogodke v varnostnih zapisih

Kaj so " Log Files " ?

Pogosti varnostni dogodki

Naloge, povezane z upravljanjem datotek z varnostnimi zapisi

Kako upravljamo s podatki v datotekah z varnostnim zapisom

Kako gledamo dogodke v varnostnem zapisu

Vaja : Upravljanje s podatki v datotekah z varnostnim zapisom

Konfiguriranje lastnosti varnostnega zapisa

Pregled dogodkov, zapisanih v datoteki z varnostnim zapisom

Vaja: Upravljanje z varnostnimi nastavitvami

Tvorba prilagojene varnostne šablone

Preverjanje konfiguracije računalnika v primeri s prilagojeno varnostno šablono

Uporaba prilagojene varnostne šablone s pomočjo skuopinske politike (Group Policy)

Nadzor zaščite organizacijske enote

Cilji

Razumevanje uporabe skupinske politike (Group Policy)

Varovanje "Windows Server 2003" z varnostnimi politikami

Upravljanje varnosti s pomočjo "Security Templates Snap-in"

Konfiguriranje varnosti klijentov s pomočjo politik Windows Server 2003

Konfiguriranje zakodiranega datotečnega sistema (Encrypting File System)

Uvod v skupinsko politiko (Group Policy)

Skupinska politika v Windows Server 2003 omogoča standardizirano delovno okolje za klijente in strežnike

Razvili so jo iz konceptov sistemske politike pri NT Server 4.0

Nudi več zmožnosti od sistemske politike

Lahko jo razširimo preko več domen na eli kolaciji

Nastavimo za več okolij

Je bolj varna, ker uporabniki ne morajo spreminjati politik

Dinamične posodobitve in konfiguracija, ki odraža tekoče potrebe

Značilnosti skupinske politike

Vzpostavimo jo lahko za lokacijo, domeno, organizacijske enote ali lokalni računalnik

Ne moremo je vzpostaviti za vsebovalnike, ki niso organizacijske enote (Cannot be set for non-OU folder containers)

Nastavitve politike za skupine pomnimo v objektih "Group Policy objects" (GPO)

Vsak GPO ima edinstveno ime in GUID

Imamo lokalne in ne-lokalne GPO

Če imamo več GPO, je njihov učinek inkrementalen

Vrstni red je: lokalno, privzeta domena, položaj (site), organizacijska enota (OU)

Skupinsko politiko (Group Policy) lahko vzpostavimo tako, da vpliva na uporabniške konte, na računalnike ali na oboje

Ko osvežimo skupinsko politiko, stare politike odstranimo ali osvežimo za vse klijente

Varovanje Windows Server 2003 s pomočjo varnostnih politik

Varnostne politike (Security policies) so podmnožica skupinske politike (Group Policy)

Nekatere pogosto uporabljane varnostne politike

Politike kontov (Account policies)

Politika kontrole (Audit policy)

Pravice uporabnikov

Varnostne opcije

IP varnostne politike

Lahko jih konfiguriramo z naslednjimi orodji

Orodje "Domain Security Policy" za domeno ali lokalni računalnik

"Group Policy Object Editor Snap-in" je najbolj funkcionaleny

Orodje "Active Directory Users and Computers" uporabimo za domeno ali organizacijsko enoto

Vzpostavljanje politik kontov

Politike kontov (account policies) najdemo v naslednji poti " Group Policy " :

Computer Configuration, Windows Settings, Security Settings

Opcije politike kontov

Varnost gesla (password security)

Prenehanje kontov (account lockout)

Varnost Kerberos

Opcije varnosti gesla

Uveljavljanje zgodovine gesla

Zahteva od uporabnikov, da izberejo nova gesla, ko spreminjajo gesla

Največja starost gesla

Nastavi maksimalni čas do poteka gesla

Običajno 45 do 90 dni

Najmanjša starost gesla

Najmanjša dolžina gesla

Najmanj 7 znakov za "močno geslo"

Geslo mora izpolnjevati zahtevo po kompleksnosti

Filtriranje zahtevkov za gesla

Pomnenje gesel s pomočjo reverzibilnega kodiranja

Opcije za zapiranje kontov

Trajanje zapore konta

Lahko določimo v minutah, koliko časa je določen konto zaprt potem, ko je bilo izvedeno določeno število neuspelih poskusov logiranja

Nivo zapore konta (account lockout threshold)

Določimo lahko omejitev za število neuspelih logiranj

Reset števca zapore konta po

Določimo lahko število minut med dvema zaporednima neuspešnima poskusoma logiranja. S tem poreprečimo, da ne bi bil konto prehitro odklenjen

Varnost Kerberos

Vključuje uporabo listkov (tickets), ki si jih izmenjujeta klijent, ki zahteva dostop, in strežnik oziroma aktivni direktorij, ki zagotavlja dostop

Distribucijski center ključev (DC ali strežnik) pomni konte uporabnikov in gesla

Računalnik-klijent pošlje ime konta in geslo distribucijskemu centru ključev

Distribucijski center pošlje začasno dovoljenje (temporary ticket), ki zagotavlja dostop do strežnika "ticket-granting server"

"ticket-granting server" pošlje servisno dovoljenje "service ticket" za čas, dokler traja logiranje (logon session).

Varnostne možnosti Kerberos

Uveljavlja omejitve logiranja uporabnikov

Varnot Kerberos je privzeta

Najdaljši čas veljavnosti servisnega dovoljenja

Maksimalni čas (v minutah), ko dovoljenje (omogoča dostop do določenega servisa v eni seji

Najdaljši čas veljavnosti uporabniškega dovoljenja

Maksimalni čas (v urah), ko lahko dovoljenje uporabljamo v enoviti seji za dostop do računalnika ali domene

Najdaljši čas za za obnovitev uporabniškega dovoljenja

Maksimalno število dni, ko lahko obnovimo isto Kerberos dovoljenje vsakokrat, ko se logiramo

Največja toleranca za sinhronizacijo računalniškega časa

Največ koliko minut čaka klijent na sinhronizacijo njegove ure

Vzpostavitev politik kontrole (audit policies)

Upravljanje s konti

Dostop do servisa direktorija in objektov

Dogodki ob logiranju ali zapuščanju konta in lokalnega računalnika

Spremembe politike in uporaba privilegijev

Sledenje procesom in sistemski dogodki

K onfiguri ranje uporabniških pravic

Uporabniške pravice omogočajo kontu ali skupini izvajanje določenih nalog, kot na primer:

Dostop do strežnika

Tvorba kontov

Upravljanje funkcij strežnika

Dodelujmo uporabniške pravice skupinam namesto posameznim uporabniškim kontom

Člani skupine podedujejo uporabniške pravice skupine

Konfiguriranje varnostnih opcij

Več kot 65 specializiranih varnostnih opcij, razdeljenih v naslednje kategorije

Konti (a ccounts)

Pregled (a udit)

Naprave (d evices)

Domenski krmilnik (d omain controller)

Član domene (d omain member)

Interaktivno logiranje (i nteractive logon)

Omrežni klijent MS (Microsoft network client)

Dostop do omrežja (n etwork access)

Konfiguriranje varnostnih opcij (nadaljevanje)

Varnost omrežja (network security)

Konzola za reševanje (recovery console)

Izklop (shutdown)

Sistemsko kodiranje (system cryptography)

Sistemski objekti (system objects)

Sistemske nastavitve (system settings)

Opcije v vsaki kategoriji so specializirane glede na kategorijo

Uporaba varnostnih politik IP (IP Security Policies)

IPSec nudi varne komunikacijske in kodirne standarde za vse aplikacije, osnovane TCP/IP in za komunikacijske protokole

Proces IPSec

Računalniki izmenjujejo potrdila za avtentikacijo prejemnika in pošiljatelja

Podatki so kodirani na omrežni kartici (NIC, Network Interface Card) oddajajočega računalnika, ko so oblikovani v IP paket

Konfiguracijska orodja IPSec

Orodje "Domain Security Policy"

"IPSec Policies Management Snap-in"

Uporaba varnostnih politik IP (nadaljevanje)

Vloge IPSec

Klijent (le odgovor)

Ko se klijent poveže z Windows Server 2003 z uporabo IPSec, ta odgovori z uporabo komunikacije IPSec

S trežnik (želi varnost)

Ko je Windows Server 2003 kontaktiran ali začne komunikacijo, privzeto uporablja IPSec

Če klijent, ki odgovarja, ne podpira IPSec, preklopi strežnik v nekodiran način (clear mode)

Varni strežnik (Secure Server) (terja varnost)

Windows Server 2003 odgovarja le z uporabo komunikacije IPSec

Varnostne šablone (Security Templates Snap-in)

Uporabne, ko imamo večkratne skupinske politike (group policies) ali pa več organizacijskih enot (OU) souporablja isto skupinsko politiko

Varnost nastavimo za naslednje

Konte in lokalne politike

Politike sledenja dogodkov (Event log tracking policies)

Omejitve skupin

Varnost dostopa do servisov

Varnost registra

Varnost datotečnega sistema

Tvorba nove šablone za varnost

Prepričajmo se, če še ne obstaja privzeta šablona za varnost, ki bi nam ustrezala

Nameščena morajo biti "Group Policy Object Editor Snap-in" in "Security Templates Snap-ins"

Preko "Security Template's Action menu" tvorimo novo šablono

Konfiguriramo nastavitve

S pomočjo "Security Configuration and Analysis Snap-in" vnesemo (import) novo šablono v skupinsko politiko

Privzete varnostne šablone (Text body indent Security Templates)

Nudijo kompatibilne nastavitve za Server 2003 in NT

compatws

Nastavijo privzeto zaščito za domenske krmilnike (DC) ali korenske domene

DC security, rootsec

Nastavijo maksimalno zaščito za domenske krmilnike Windows Server 2003 ali računalnike (workstations), ki dostopajo do Windows Server 2003

hisecdc, hisecws

Nudijo priporočeno varnost na domenskih krmilnikih ali odjemalskih računalnikih (client workstations)

securedc, securews

Nudijo varnost "out of the box"

setup security

Konfiguriranje zaščite odjemalca

Nudi izboljšanje varnosti

Zagotavlja konsistentno delovno okolje v organizaciji

Ko se odjemalec logira na strežnik oziroma omrežje, se varnostne politike uporabijo na odjemalcu

Primeri uporabe:

Preusmeritev map (folder redirection) za občutljive podatke

Upravljanje z ikonami namizja s ciljem, da se aplikacije prožijo na vseh odjemalcih enako

Ročno konfiguriranje politike za odjemalce

Uporabimo "Group Policy Object Editor Snap-in"

Uporaba vnaprej pripravljenih administrativnih šablon

Eni skupinski politiki lahko dodamo več šablon

Objavljanje in dodeljevanje programov

Uporabniki lahko zaradi večje produktivnosti in varnosti uporabljajo iste programe z enakimi programskimi nastavitvami

Objavljanje aplikacij zajema nastavitve programov preko skupinskih politik. Tako lahko odjemalci nameščajo programe iz centralnega distribucijskega strežnika

Dodeljevanje aplikacij zajema konfiguriranje politike tako, da posamezne programske aplikacije avtomatsko prožimo preko bližnjice na omizju

Uporabimo pogovorno okno "Software Installation Properties" med "User Configuration Software Settings"

Re zultirajoča množica politike

Nova možnost, vključena v Windows Server 2003

Administratorju poenostavlja implementacijo skupinskih politik in odpravljanje težav

Dva načina:

"Planning mode" tvori poročilo in nudi rezultate predlaganih sprememb politike

"Logging mode" tvori poročilo, ki temelji na trenutnih politikah in nudi spremembe rezultirajoče politike

Konfiguriranje enkriptiranega datotečnega sistema

EFS (encrypted file system) konfigurira edinstven privatni ključ, ki mje vezan na konto uporabnika, ki je enkriptiral direktorij ali datoteko

Ščiti podatke pred nepooblaščeno uporabo

Za konfiguriranje enkripcije datoteke ali direktorija uporabimo ukaz "cipher" v ukazni vrstici

Če v ukazu ne podamo nobenih parametrov, je prikazan status enkripcije tekočega direktorija

Povzetek

Skupinska politika (Group Policy) omogoča standardizacijo uporabe strežnika in odjemalskih računalnikov na omrežju

Varnostne politike so del skupinske politike in jih konfiguriramo za zaščito uporabnikov in sredstev

Politike kontov konfiguriramo za organizacijske enote, domene, lokacije in lokalne računalnike

Password policies, account lockout policies, and Kerberos authentication policies

Politike nadzora (audit policies) uporabljamo za sledenje dostopa do sredstev, kot so direktoriji, datoteke ali uporabniški konti

Politike uporabniških pravic (user rights policies) omogočajo tvorbo specifičnih varnostnih nadzorov privilegijev in logiranj

Povzetek

Varnostne možnosti so specializirane za konte, nadzor, naprave, domenske krmilnike, logiranje, odjemalce, omrežni dostop, omrežno varnost in druge aktivnosti

Za tvorbo privzetih varnostnih nastavitev ali za tvorbo različnih objektov skupinskih politik za različne organizacijske enote, domene ali lokacije uporabimo "Security Templates Snap-in"

Boljši nadzor nad aktivnostmi odjemalcev ročno konfiguriramo administrativne šablone ali uporabimo vnaprej pripravljene administrativne šablone (ali oboje)

Upravljanje, kako odjemalci uporabljajo aplikacije, dosežemo z objavljanjem in dodeljevanjem aplikacij

Pri planiranju skupinskih politik in odpravljanju težav uporabljamo "Resultant Set of Policy Snap-in"

S pomočjo ukaza "cipher" v ukaznem oknu fino uglasimo uporabo enkriptiranega datotečnega sistema

Nadzor strežnika in omrežja

Cilji

Razumevanje pobembnosti nadzora strežnika

Servisi za nadzor strežnika

Procese in performanso nadzorujemo z orodjem "Task Manager "

Vse vrste sistemskih elementov nadzorujemo z orodjem "System Monitor"

Konfiguriranje zapisov performans (performance logs) in opozoril za nadzor sistema

Za nadzor performans omrežja uporabljamo orodje "Network Monitor"

Za nadzor in upravljanje uporabljamo "SNMP Service"

Uvod v nadzor strežnika

Zakaj nadzorujemo

Preventiva problemov, preden sploh pride do njih

Diagnostika obstoječih problemov

Vzpostavljanje testov (benchmarks) za primerjanje podatkov, ki smo jih dobili z nadzorom, s predvidenimi performansami

Disk, CPE, pomnilnik, odzivni časi omrežja

Počasna, tipična in zelo obremenjena uporaba strežnika in omrežnih sredstev

Nadzor servisov strežnika

Dostop do servisov strežnika

Odpremo orodje "Computer Management"

Okno s servisi ima 5 kolon

Name

Description

Status

Started, Paused, or blank

Startup Type

Automatic (most services), manual, or disabled

Log On As

Services usually log on to the Local System

Reševanje problemov s servisi

Probleme s servisi ugotavljamo z orodjem "Services"

Preverimo stanje servisa, ki smo ga pognali ali je bil sprožen avtomatsko

Če je potrebno, ga spet sprožimo

Previdni moramo biti, da pri ustavljanju servisa

Preveriti moramo odvisnosti (Dependencies) servisa in pogledati, ali zaustavitev servisa vpliva na druge servise

Servis prekinemo (da ne nudi več storitev in da ga lahko uporablja ta čas le administrator oziroma operater strežnika

Uporaba orodja " Task Manager "

Z njim nadzorujemo in upravljamo sredstva strežnika

Ap likacije

Proces i

Obnašanje v realnem času

Obnašanje omrežja

U porabniki

Nadzor aplikacij

Zavihek "Applications" prikazuje vse aplikacije (tasks, naloge), ki smo jih pognali na konzoli strežnika

Možnosti akcije:

Konec naloge, prehod na drugo nalogo, proženje nove naloge (End Task, Switch To, New Task)

Statusna vrstica prikazuje podatke o procesih

Desni klik na posamezno aplikacijo odpre naslednje možnosti:

Switch To, Bring To Front, Minimize, Maximize, End Task, Go to Process

Nadzor procesov

Zavihek "Processes" prikazuje seznam vseh procesov, ki jih uporabljajo vse aplikacije

Posamezen proces lahko ustavimo

Posameznemu procesu lahko spremenimo prioriteto

O procesu imamo na voljo nsalednje podatke:

Nastavljanje prioritet

Osnovna prioriteta (base priority class) je interno nastavljena v aplikaciji

Administrator strežnika lahko prioriteto spremeni v

Normalno (0)

nizko(-2)

Pod normalno (-1)

Nad normalno (+1)

visoko (+2)

Realni čas(+15)

To uporabljamo previdno, saj lahko proces prevlada na strežniku

Nadzor performans realnega časa

Zavihek "Performance" prikazuje podatke o zasedenosti CPE in pomnilnika

Uporaba CPE

Oporaba strani datotek (page file use)

Ročice (handles)

Niti

Nadzor omrežnih performans

Zavihek "Networking" omogoča nadzor omrežnih performans na vseh omrežnih karticah (NIC), nameščenih na strežniku

Prikazuje uporabo omrežja

Prikazuje omrežno performanso preko vsakega NIC adapterja

Tako lahko ugotovimo, če je s katerim od adapterjev problem

Lahko služitudi za opozarjanje o visoki obremenitvi omrežja(80% do 100%)

Nadzor uporabnikov

Zavihek "Users" podaja seznam uporabnikov, ki so v danem trenutku logirani

Uporabnika lahko odjavimo

Pred tem se zaprejo vse odprte datoteke

Uporabnika odvežemo, če se je povezava z njim "obesila"

Uporaba orodja " System Monitor "

Zajem sistemskih podatkov

"System Monitor" uporabljamo za nadzor komponent, kot je trdi disk, pomnilnik, procesorji, "disk caching", sproženi procesi in "page files"

Nadzorujemo objekte sistemskega monitorja

Za vsak objekt imamo enega ali več števcev, ki jih lahko nadzorujemo

Števci imajo statusni podatek

Če moramo nadzorovati več različnih elementov istega objektnega tipa, lahko instance asociiramo s števcem

Pogledi sistemskega monitorja

Graph

Diagram poteka objekta

Črte v različnih barvah predstavljajo posamezne objekte

Histogram

Palični diagrami (bar charts) kažejo posamezne objekte v različnih barvah

Na dnu zaslona so prikazani posamezni števci skupaj z legendo posameznih barv

Report

Podatki na zaslonu so prikazani številčno in jih lahko izvozimo v poročilo

Nadzor komponent sistema

Pogosto nadzorujemo štiri objekte skupaj z njim dofeljenimi števci

Procesor

% Procesorskega časa kaže, ali je strežnik zelo obremenjen, sklepamo lahko, ali moramo zmanjšati obremenitev oziroma povečati zmožnosti

% prekinitvenega časa kaže, da imamo morda problem aparaturne narave

Interrupts/sec lahko opozarja, da je omrežni promet pretiran

Dolžina čakalne vrste (processor queue length) lahko nakazuje, da moramo obremenitev procesorja porazdeliti

Pomnilnik

Disk

Omrežni vmesnik

Diskperf

Diskperf je orodje za ukazno vrstico. Z njim nadzorujemo stanje števcev trdega diska

Konfiguriranje performančnih zapisov in opozoril

Do orodja "Performance Logs and Alerts" pridemo preko menuja "Administrative tools"

Performančni zapisi (performance logs) sledijo performančne podatke v danem časovnem obdobju

Zapisi števcev predstavljajo sledenje posnetkov nadzorovanih objektov sistema v danih časovnih intervalihs

Možni so tudi zapisi posameznih dogodkov in vsebujejo le instance, ko do dogodka pride

Alarme (alerts) uporabljamo za ugotavljanje nastopa različnih problemov in opozarjanje kontov ali skupin

Tvorba zapisov števcev (counter logs)

V rubriki "Performance Logs and Alerts" izberemo možnost "Counter Logs and Alerts"

Nov zapis poimenujemo in dodamo števce

Zapisi števcev zasedajo prostor na disku in upočasnijo sistem

Pri ne več kot 4 urnem zapisovanju uporabimo 15 sekundne intervale

Za daljše zapise povečamo časovne intervale in velikost zapisne datoteke (log file size)

Zapisovanje lahko ročno ustavimo in ponovno poženemo

Dodamo lahko druge objekte in števce

Tvorba zapisov sledi (trace logs)

Dokumentirajo nastop določenih dogodkov v danem časovnem obdobju

Uporabno pri ugotavljanju ponavljajočih se problemov

Pretirana obremenitev strežnika na omrežju

Raziskovanje napak strani

Nadzorujemo bolj omejeno število elementov kot pri zapisu števcev

Tvorba alarmov (alerts)

Alarm tvorimo z opcijo "Alert" v rubriki "Performance Logs and Alerts"

V rubriki "New Alert Settings" vnesemo ime alarma

Izberemo objekt, števec ali instanco

Če hočemo nadzorovati vse procese, izberemo kot instanco "Select _Total"

Ko pride do problema, lahko skupina "Administrator" prejme sporočilo

Na primer, ko je CPE 100% obremenjen

Uporaba orodja " Network Monitor "

Reden nadzor omrežja je pomemben, saj so lahko spremembe omrežnih pogojev pogoste

Orodje "Network Monitor" lahko tvori zapise omrežnih aktivnosti in lovi okvirje in pakete

Namestimo ga z orodjem "Add/Remove Programs"

"Network Monitor Driver" omogoči omrežnim karticam (NIC) računalnika zbiranje statističnih podatkov o obnašanju omrežja

Namestimo ga z "Network Connections"

Lovljenje omrežnih podatkov

Procent uporabe omrežja

Statistika, zajeta v danem časovnem obdobju, statistika NIC, statistika omrežne postaje

Naslovi omrežnih postaj

Okvirji in bajti na sekundo

Podatki o prenosih

Prenosi na sekundo

Broadcast, unicast, in multicast prenosi

Podatki o napakah

Konfiguriranje orodja "Network Monitor"

Upravljanje dogodkov konfiguriramo z nastavitvijo filtrov za lovljenje določenih dogodkov

Dva tipa lastnosti filtrov:

Service Access Point (SAP) specificira omrežni proces, ki mora na cilju sprejeti okvir (frame)

ETYPE je 2.bajtna koda za tip protokola, ni pa del standarda Ehernet

Nadzorujemo lahko eno ali obe lastnosti

Nastavitev omrežnih testov (network benchmarks) za nadzor obremenitve

% Uporabe mreže

Okvirji (frames), Broadcast in Multicasts na sekundo

Uporaba servisa SNMP

Uporaben za upravljanje omrežja, ki temelji na TCP/IP

Sastavljajo ga sistemi za upravljanje in agenti, ki jih lahko za administrativne in varnostne namene združujemo v skupnosti

Skupnost souporablja servis

Ime skupnosti uporabljamo kot primitivno geslo, uporabljano med računalniki

Promet SNMP lahkonadzorujemo z orodjem "Network Monitor"

Konfiguriranje servisa SNMP

Servis SMNP in " SNMP Trap Service " konfiguriramo za uporabo z orodjem " Network Monitor "

Preko imena računalnika ali naslova IP/IPX dodamo imena skupnosti

Konfiguriramo zavihek " Traps "

Določa cilj pošiljanih "trap"-obvestil ", ki temeljijo na določenih dogodkih

Povzetek

Za dobro razumevanje strežnikov na našem omrežju in tipične performanse omrežja uporabljamo nadzor sistema in omrežja

Orodje "Computer Management" omogoča nadzor sistemskih servisov in ugotavljanje, ali je pri tem kaj problemov

Servis ponovno sprožimo

Preverimo odvisnosti

Aplikacije, procese, performanse sistema in omrežja ter logirane uporabnike nadzorujemo z orodjem "Task Manager"

Problematično aplikacijo ali proces ustavimo

Odjavimo "obešene" povezave uporabnikov

Vse tipe sistemskih im mrežnih aktivnosti nadzorujemo z orodjem "System Monitor"

Prikaz lahko prilagodimo, podatke lahko shranimo v datoteko

Povzetek

Zapis performans omogoča zajemanje in shranjevanje sistemskih podatkov v določenih trenutkih ali intervalih

Podatke o performansah mreže zbiramo z orodjem "Network Monitor", ki ga namestimo skupaj z gonilnikom "Network Monitor driver"

Servis SNMP omogoča omrežnim agentom zbiranje mrežnih performančnih podatkov, kar lahko nato uporabljajo programi za upravljanje mreže

Upravlja in konfigurira določene omrežne naprave

Terminal Server in MS Windows Server 2003

Pregled

Koristi uporabe " Terminal Server "

Značilnosti na strani klijenta

Značilnosti na strani strežnika

Dovoljenja Terminal Server

Razvoj ustanove

Izboljšanje licenciranja

In še...

Koristi uporabe Terminal Server

Značilnosti na strani odjemalca

Remote Desktop Protocol (RDP) v 5.2

Full client included with Windows XP

Full (.MSI), MMC and Web (ActiveX®) downloads

No separate Connection Manager

Automatic reconnects

Client resource redirection features

Resource redirection

Slow link performance optimizations

Značilnosti na strani odjemalca *(nadaljevanje)*

Remote Desktop Web Connection

Remote Desktops Administration Tool

Značilnosti na strani odjemalca *(nadaljevanje)*

Specify Computer, User name, Password, and Domain

Save settings

Značilnosti na strani odjemalca *(nadaljevanje)*

From 256 color to True Color (24 bit)

Resolution to 1600 x 1200

Full screen capabilities

Značilnosti na strani odjemalca *(nadaljevanje)*

Audio output

Windows key combos

Disk drives and printers (local and network)

Serial devices

Smart card

Time Zone

Clipboard (+files)

Značilnosti na strani odjemalca *(nadaljevanje)*

Launch entire desktop or specific application

Značilnosti na strani odjemalca *(nadaljevanje)*

Network and Performance Improvements

Increased network bandwidth savings over RDP 5.0

Remote "experience" turns off wallpaper, visual styles, etc., depending on network connection

Auto-reconnect

128-bit bidirectional encryption

Backward compatible with RDP 5.0 and RDP 4.0

Demo

Povezava na Terminal Server

Značilnosti na strani strežnika

Remote Desktop for Administration provides Console redirection—can now connect to console session

"SERVERNAME /console" or "mstsc.exe /console"

Can establish two connections plus one console connection

Can use Remote Assistance to share a session between administrators

At console, session is locked—shows user who connected to console as user who locked the console

Remote Desktops Administration Tool

Značilnosti na strani strežnika (nadaljevanje)

Privzeto nameščen na vseh platformah Windows Server 2003, vendar onemogočen

Spremeniti moramo zavihek "Remote" v "System properties"

Lahko ga omogočimo ali onemogočimo s pomočjo orodja "Windows Management Instrumentation" (WMI) ali "Windows Management Instrumentation Command (WMIC)"

RDToggle

Značilnosti na strani strežnika (nadaljevanje)

Režim " Terminal Server mode " , prej " Terminal Server Application mode "

Lahko namestimo " Terminal Server " z orodjem " Add/Remove Programs " ali " Manage Your Server "

Lahko namestimo med nenadzorovano namestitvijo (unattended installation)

TS Session Directory with Load-Balancing

Značilnosti na strani strežnika (nadaljevanje)

Varnostne značilnosti

Remote Desktop Users Group

Security Policy Editor

128- bitna enkripcija

Kompatibilnost FIPS

Politike omejevanja programov (Software Restriction Policies)

License Server Security Group

Dovoljenja za oddaljeno povezavo

Podpora pametnih kartic (Smart Card)

Dovoljenja Terminal Server

Poln nadzor

Dostop uporabnikov

Dostop gostov

Novo v Windows Server 2003 : "Remote Desktop Users group"

Ni privzetih članov

Dovoljenja lokalnih in mrežnih servisov omogočajo:

Povpraševanje podatkov o seji

Pošiljanje obvestil drugi seji

Dovoljenja "Terminal Server": Poln nadzor

Povpraševanje podatkov o seji

Spreminjanje parametrov povezave

Končanje seje

Oddaljeni nadzor sej drugih uporabnikov

Logiranje na sejo na strežniku

Odjava uporabnika s seje

Pošiljanje obvestil seji drugega uporabnika

Povezava na drugo sejo

Odklop neke seje

Uporaba virtualnih kanalov, kar omogoča dostop s stržnega programa na naprave odjemalcev

Dovoljenja "Terminal Server": Dostop uporabnika

Logiranje na sejo na strežniku

Povpraševanje podatkov o seji

Movezava na drugo sejo

Dovoljenja "Terminal Server": dostop gostov

Log iranje na sejo na strežniku

Ko dodamo dovoljenjem za servise terminala novega uporabnika ali skupino, je privzeto omogočen le dostop kot gost

Demo nstracija

Prikaz nastavitev Terminal Server

Enterprise Deployment: upravljanje

Nastavitve politike novih skupin

Obsežna množica politik

Tako nastavitve računalnika kot uporabnika

Control permissions via Remote Desktop Users group through "Restricted Groups" in Security Templates MMC snap-in

Nov dobavitelj WMI

Fully Read/Write

Nearly all Terminal Server Settings: Terminal Server Config, APIs, and Command Lines

Alias support for WMIC: RDAccount; RDPermissions; RDToggle; RDNic

Enterprise Deployment: Provisioning

Use Group Policy to populate Remote Desktop Users

Assign applications to the Computer

Best to have the Terminal Server machines in an Organization Unit

Will install at reboot

No per-user install supported

Use WMI and Group Policy to configure server

Session timeouts, time zone, redirection, encryption level, session directory, and so on

License mode only through WMI

Enterprise Deployment: Upgrading from Windows 2000

Can mix Windows 2000 and Windows Server 2003

Licensing

A Windows Server 2003 License Server can issue both Windows 2000 TSCALs and Windows Server 2003 Terminal Services Client Access Licenses (TSCALs)

License Servers do not have to be on a Domain Controller

Some parameter differences on upgrade vs. clean install:

App Compat Security

User Access Rights

Color Depth
Redirection Settings
Enterprise Deployment: Monitoring with Microsoft Operations Manager
Terminal Server management included in base product
Monitors critical functions
System availability, resources, events, and so on
Session count, session traffic
CPU and RAM per session and global
Izboljšanje licenciranja
Terminal Server License Service is required
Grace period of 120 days
Terminal Servers do not supply licenses
May be deployed on Member Servers or Domain Controllers
Terminal Servers use Broadcast or Active Directory enumeration
New User Client Access License (User TSCAL)
External Connector for External Users (TS-EC)
Consistency with Microsoft's New Software Licensing Framework
Transition Plan for OS Equivalency Removal in Microsoft Windows 2003 Server Terminal Server
http://www.microsoft.com/licensing/resources/terminal_services.asp
Izbira tipa licenciranja
Device TSCAL
Permits one device to access the server software
Any user can access the device
Most useful when devices are shared (Call center, shift-work environments)
User TSCAL
Permits one user to access the server software
Any device can be used by the user (only one device at a time)
Most useful when users roam the network (mobile sales force with work PCs, home PCs, wireless PDAs)
External Connector License (TS-EC)
Allows access for an unlimited number of external (customers, partners, etc.) users or devices
Access is limited to one Terminal Server per TS-EC
Modeli licenciranja
Remote Desktop for Administration does not require a license
2 connections (including console)
Per Server mode
TSCALs represent incoming connections
Assigned to a specific Terminal Server
Limits that server's maximum concurrent connections
Per Device or Per User mode
TSCALs represent total number of active devices, active users, or combinations of devices and users
Can be used to access all Terminal Servers

No limit to the number of devices accessing a single Terminal Server
Povzetek
Koristi uporabe " Terminal Server "
Značilnosti na strani klijenta
Značilnosti na strani strežnika
Dovoljenja Terminal Server
Razvoj ustanove
Izboljšanje licenciranja
In še...
Reference
Terminal Server Community Site http://www.microsoft.com/windows.netserver/community/centers/terminal/
Common Questions / FAQ
Newsgroups
White papers
What's New in Terminal Server
Session Directory in Load Balancing Scenarios
Resource Kit Deployment Guide
Deploying Terminal Server Applications via the Web
Terminal Server Scaling
Remote Desktop Performance
Geek Notes (GN): Terminal Server Enhancements in Microsoft Windows Server 2003
GN - Remote Desktop Protocol (RDP) 5.1 Client
New version of RDP that ships with Windows XP
Backward compatible with RDP 5.0 and RDP 4.0
Adds new functionality to client
Specification made available to ISVs
Allows developers to write applications against RDP
Applications may be written for non-Windows clients and utilize RDP 5.1
Also ships as part of Windows CE Platform Builder 4.0
GN - Remote Desktop Client Functionality
Windows XP Pro/Windows XP Home
Remote Desktop client built in
Programs > Accessories > Communications > Remote Desktop Connection or mstsc.exe
GN - Remote Desktop Client Functionality
Increased color depth and resolution support
May be limited by server configuration
Server can be configured to limit maximum color depth regardless of client settings
GN - Remote Desktop Client Functionality
Audio redirection
Keyboard shortcuts
Connection of drives, printers, serial ports upon connection to terminal server

GN - Remote Desktop Client Functionality
More connection speed options
UI configuration including themes, animations, backgrounds, etc.
GN - Remote Desktops Administration Tool
Installed with Adminpak.msi or on any Windows Server 2003 product
Collects remote connections in a single convenient interface
GN - Other Client Features
Auto-reconnect
Group Policy integration
Time Zone Redirection
Controlled by Group Policy on the server
Client Time Zone + Server Time = Session Time
If connecting from a Windows XP or Windows Server 2003 client, can log on to terminal session by using a smart card
Can utilize even with Windows 2000 Terminal Servers
GN - Remote Desktop Connection Software
Installs client portion of Remote Desktop on Windows 95, Windows 98, Windows 98 SE, Windows Millennium Edition, Windows NT 4.0 or Windows 2000
Windows Installer Package
Can be deployed via Group Policy
http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp
GN - New Terminal Server Functionality
Remote Administration mode installed Console redirection- can now connect to console session
"SERVERNAME /console" or "mstsc.exe /console"
Can establish two connections plus one console connection
Can use Remote Assistance to share a session between administrators
Remote Desktops administration tool
At console, session is locked—shows user who connected to console as user who locked the console
GN - Enterprise Deployment
Lockdown Strategies
Group policy to restrict access/views
Separate OU for Terminal Server
Loop-back to create terminal service-specific policies
See Q274478
ACLs always matter
Software Restriction Policy (SAFER)
Restrict what runs—Replaces AppSec
Allow/Block **Text body indent** and per application
Applied by policy to computer or users
Exempt Administrator through object or selection
GN - Win64

32 Bit Apps
Substantial memory penalty from Windows on Windows
64 Bit Apps
Limited selection
Scaling similar to 32 on 32
CPU limited
Win64 not usually recommended for Terminal Server
GN - Win Server 2003 Licensing
Simplified Usage
TSL Wizard redesigned to improve usability
TSL mode can be setup in unattended setup
Per Device / User
As per Windows 2000 SP3
CAL required for every connection
GN - Licensing: Not Optional
License Service is always required
Grace period provides time for this (~120 days)
Terminal Server never supplies licenses
Discovery
Broadcast in workgroup or Windows NT 4 domain
Active Directory enumeration in Windows 2000/Windows Server 2003 domain
New – Optional registry key – specify multiple computer names
Like Q239107 (Establishing Preferred License Server), but now works for multiple names
Licensing server may be deployed on any server
Not required to be deployed on a domain controller
Discovered automatically for enterprise licensing server, not domain
GN - More Licensing
Secure licensing mode
Off by **Text body indent**
Controlled via Group Policy
"Terminal Server Licensing" local group
Both Terminal Servers and License Servers
Re-issuance is automatic
Recommended high availability configuration
Per Device: Two License Servers
LS1: 1,000 CALs installed
LS2: Zero CALs installed
LS1 is used until catastrophe, then LS2 issues temporary licenses
Per Session – CALs should be distributed
GN - Additional Management Features
License Manager Wizard Improvements

Remote Desktop for Administration

Remote Desktop MMC Snap-in

Terminal Services Manager Improvements

Remote Connection Permissions

Other enhancements

Time Zone Redirection

Load Management

Reševanje problemov

Cilji

Razvoj splošnih strategij reševanja problemov

Reševanje težav pri zagonu

Restavriranje stanja sistema in "back-up"

Restavriranje izpadlega sistemskega zvezka

Uporaba orodja "Event Viewer" pri reševanju problemov

Reševanje varnostnih težav z uporabo "Security Configuration and Analysis Snap-in"

Reševanje težav s povezovanjem

Daljinska administracija strežnika

Študijski primer 1

Eden od strežnikov se je sesul ! Kje naj najprej pogledamo, kaj se je zgodilo in kateri so prvi koraki in orodja, ki naj jih uporabimo ?

Študijski primer 2

Vodja oddelka za trženje želi sprožiti novo akcijo in je ves paničen ! Nekateri delavci njegovega oddelka se ne morejo logirati, nekaterim pa ne uspe dostopiti do določenih direktorijev, ki so bili zanje pripravljeni. Izgleda tudi, da je nekdo prišel do podatkov v tajnem direktoriju . Kakšni naj bodo naši ukrepi ?

Študijski primer 3

Zaradi električne prenapetosti se na strežniku, na katerem imamo tudi podatke, pojavljajo problemi. Prikazuje obvestilo, da ni sistemskega diska in med zagonom se obesi. Kakšne tehnike in orodja naj uporabimo za rešitev tega problema

Splošne strategije reševanja problemov

Razumevanje, kako interaktirajo strežniki in omrežje

Usposabljanje uporabnikov, da bodo znali pomagati razreševati probleme

Reševanje problemov korak za korakom

Sledenje problemom in rešitvam

Razumevanje, kako interaktirajo strežniki in omrežje

Tvorimo omrežne diagrame

Mainframes, mini računalniki in strežniki

Delovne postaje in omrežni tiskalniki

Omrežne naprave

Tele komunikacijske povezave

Oddaljene povezave

Grajenje lokacij

Zbiramo teste (benchmarks)

Usposabljanje uporabnikov za pomoč

Shraniti delo ob prvem znaku težav

Ko nastopi težava, zapisovanje podatkov o težavi

Poročanje o vseh protololarnih podatkih, vključno z obvestili o napakah

Takojšnje poročanje o težavi preko telefona ali zvočne pošte

Izogibamo se pošiljanju elektronskih pošt o nujnih težavah

Reševanje problemov korak za korakom

Postavljamo prava vprašanja za pridobivanje čimveč podatkov

Zapisujemo obvestila o napakah, takoj ko se pojavijo ali o njih poroča uporabnik

Začnimo s preprostimi rešitvami

Ugotovimo, če ima enake težave še kdo drug

Redno pregledujemo zapise o dogodkih na Windows Server 2003 glede znakov o problemu

Pri razreševanju težav uporabljamo filtriranje na "System Monitor" in "Network Monitor"

Preverjamo prekinitve napajanja

Sledenje problemom in rešitvam

Vzdržujemo zapis vseh omrežnih problemov in njihovih rešitev

Podatkovna baza

Sistem namizne pomoči (Help Desk system)

Zapis uporabljamo za kasnejšo referenčno uporabo, kot orodje za učenje in kot indikator nastopajočih problemov

Vzdržujemo zapis sprememb na sistemu

Služi kot referenca drugim administratorjem

Reševanje problemov pri zagonu

Pogosti vzroki problemov pri zagonu

Izpad diskovnega pogona s sistemskimi in zagonskimi datotekami

Pokvarjena particijska tabela, zagonska datoteka ali " Master Boot Record "

Napaka pri branju diska (disk read error)

Prvi korak je poskus ponovnega zagona

Je pogosto uspešen pri branju začasnih podatkov na disku, napakah v pomnilniku, nesinhroniziranih registrih ali problemih s krmilnikom diska

Reševanje z uporabo režima "Safe Mode"

Režim "safe mode " zažene strežnik z najbolj splošnimi privzetimi nastavitvami in le s servisi, potrebnimi za osnovno konfiguracijo

Do tega režima dostopimo s pritiskom na tipko F8 med zaganjanjem računalnika

Vsebuje več naprednih možnosti za reševanje različnih problemov, vezanih na :

Spremenjeno konfiguracijo strežnika

Nove programe ali gonilnike

Reševanje zagonskih težav z "Automated Recovery Set"

Restavrira " disk signatures " , zvezke in particije in sistemske datoteke, potrebne za zagon računalnika

Uporablja predhodno tvorjen " ASR set ", ki smo ga naredili z orodjem "b ackup "

Nato namestimo Windows Server 2003 in izvedemo restavracijo sistema

Proces restavracije uporablja medij s predhodno tvorjenim " backup "

Reševanje s pomočjo "Recovery Console"

Omogoča zagon v Windows Server 2003 preko ukazne vrstice in:

odpravo kakšne težave z diskom

kopiranje kritičnih datotek nazaj na strežnik

zagon nekega servisa

Formatiranje nekega pogona

Zaženemo s CD Windows Server 2003" ali iz nameščanja

Na voljo je po namestitvi v menuju "Advanced Options"

Splošni namigi za odstranjevanje težav pri zagonu

Reševanje zagonskih problemov s "stop" obvestili

"Back-Up" in restavriranje podatkov o stanju sistema

Podatki o stanju sistema imajo nekaj kritičnih elementov

Sistemska in zagonska datoteka, aktivni imenik, mapa Sysvol, Register, podatki COM+, DNS cone, "certificate" podatki, "server cluster" podatki

Vse podatke o stanju sistema moramo kopirati tako kot kot skupino kot z lokalnega računalnika

V orodju "Backup" izberemo možnost "System State" in tako zagotovimo, da so shranjene zaščitene sistemske datoteke

V zavihku "Advanced Backup Options" izberemo avtomatski "backup" sistemskih zaščitenih datotek

Restoring a Failed System Volume

Replace the failed hardware

Install Windows Server 2003 on the new drive

Use the Backup utility to restore the system state data and all other data, using the most recent backup tapes

Do additional restores if using differential or incremental backups

Uporaba in konfiguriranje orodja "Event Viewer"

Zapisi dogodkov (event logs) vsebujejo zapise vseh tipov dogodkov na strežniku

Sistem

Varnost

Aplikacije

Servis Directory

Servis DNS

Servis replikacije datotek

Pogled na zapis dogodkov

Resnost dogodka označujejo ikone

Informacijsko obvestilo vsebuje modro črko i v belem krogu

Opozorilno obvestilo vsebuje črni "!" v rumenem simbolu

Obvestilo o napaku vsebuje beli "x" znotraj rdečega kroga

"Event Viewer" lahko poženemo v rubriki "Administrative Tools, Computer Management" lahko pa kot "MMC snap-in"

Zapisi vsebujejo podatke o vseh dogodkih

Filtriranje dogodkov

Vsi zapisi dogodkov imajo možnost filtriranja, kar olajša hitro lokalizacijo problema

Dogodke lahko filtriramo po naslednjih kriterijih

Tip dogodka, izvor in kategorija

ID dogodka

Uporabnik in računalnik, povezan z dogodkom

Datum in čas

Vzdrževanje zapisov dogodkov

Velikost zapisa naj bo dovolj velika, da ne bo prehitro napolnjen

Velikost zapisa (log size) nastavimo maksimalno

Redno preverjamo nastavitve

Redno brišemo posamezne zapise, preden so napolnjeni

Uporabimo možnost "clear" ali "overwrite"

Ko je zapis zapolnjen, avtomatsko uporabimo prekrivanje najstarejših dogodkov

Uporabimo možnost prekrivanja (overwrite) dogodkov, ki so starejši kot x dni

Zapise hranimo kot datoteke s podaljški .evt, .txt, ali .csv

Reševanje problemov z varnostjo

Pri varnostnih politikah smo morda kaj spregledali

Varnostne zahteve se s časom morda spreminjajo

Za nadzor in analizo varnosti uporabimo orodje "Security Configuration and Analysis"

Tvori podatkovno bazo za konfiguriranje strežnika in izvajanje varnostnih preverjanj

Lahko ga uporabljamo periodično za analiziranje politike

Spremembe izvajamo na osnovi naraščanja potreb strežnika

Reševanje problemov s povezavami

Moduli TCP/IP in TCP/IP-kompatibilni operacijski sistemi imajo pogosto vgrajena orodja za reševanje težav z IP

ipconfig lahko najde podvojene naslove IP

Subnet maska bo "0.0.0.0"

ping lahko preverja prisotnost drugega TCP/IP računalnika

netstat lahko preverja, če je računalnik oziroma strežnik uspešno vzpostavil TCP/IP povezavo

Če vsebuje "network and sent data" 0 bajtov, se je seja morda "obesila"

Oddaljena administracija strežnika

Oddaljeni dostop lahko izvedemo iz drugega poslopja, od doma ali med potovanjem

Omogočimo ga v zavihku "System Properties Remote"

Oddaljeni odjemalec namizja (Remote Desktop client)

Uporabimo klicno linijo preko strežnika RAS ali VPN

Konfiguriramo zelo močno geslo

Oddaljena pomoč

Nastavimo skupinsko politiko (Group Policy)

Do strežnika dostopamo iz računalnika z Windows XP

Povzetek

Redno tvorimo rezervno kopijo podatkov o stanju sistema in zaščitenih sistemskih podatkov za primer težav, kot jih na primer predstavlja okvarjena zagonska particija oziroma zvezek

Razumeti moramo, kako restavriramo okvarjen zvezek vključno s podatki o stanju sistema in sistemskimi zaščitenimi datotekami. Bodimo torej pripravljeni vnaprej

Navadimo se redno oporabljati "Event Viewer" kot orodje nadzora in rteševanja problemov

Configurirajmo zapise dogodkov (event logs) tako, kot ustrezajo potrebam naše organizacije

Študij primera 1 -odgovor

Najprej iščimo navodila z iskanjem "stop" obvestil in njihovim zapisovanjem pred poskusom ponovnega zagona.

Stop obvestilo " Data_Bus_Error" lahko pomeni, da je okvarjen pomnilnik. Stop obvestilo lahko tudi narekuje naslednji korak, še posebno če se računalnik noče ponovno zagnati.

Zaženemo preko "Recovery Console" in poženemo diagnostiko za lociranje slabega pomnilnika.Če sistem lahko zaženemo, odpremo "Event Viewer" in pregledamo predvsem sistemski zapis (system log), pregledamo pa zaradi morebitnih drugih navodil tudi druge zapise.

Študij primera 2 - odgovor

Študij primera 2 Varnost je osnovna skrb vodje oddelka. Najprej je potrebno razrešiti varnostne probleme na strežniku, na primer s pomočjo "Group Policy Object Editor Snap-in" ali z orodjem "Security Configuration and Analysis". Zaslediti moramo tudi, kdo dostopa do podatkov v tajnem direktoriju. Za ta dit+rektorij konfiguriramo nadzor (auditing) omogočimo "audit policy" in v varnostnem zapisu (security log) preverimo dogodke o dostopu do direktorija. Z orodjem "Security Configuration and Analysis" tvorimo podatkovno bazo in nato izvedemo analizo. V zapisu analize preverimo konfiguracijske podatke in ugotavljamo možne varnostne probleme, vključno s pravicami in drugimi varnostnimi podatki. Lahko tudi pregledamo dovoljenja za tajni direktorij.Ker so direktoriji s tržnimi podatki verjetno zaupne narave, je smiselno nadaljevati nadzor teh direktorijev in redno preverjati rezultate nadzora oziroma varnostne zapise.

Študij primera 2 – odgovor - nadaljevanje

Pregledamo varnostne pravice na strežniku, na primer z uporabo urejevalnika " Group Policy Object Editor Snap-in" ali orodja "Security Configuration and Analysis".

Konfiguriramo nadzor za tajni direktorij, omogočimo "audit policy" in preverjamo dogodke o dostopu do direktorija v varnostnem zapisu (security log).

Začnemo lahko tako, da tvorimo podatkovno bazo z orodjem "Security Configuration and Analysis" in nato izvedemo analizo te podatkovne baze. Preverimo vse konfiguracijske podatke in varnostni zapis ter tako iščemo možne varnostne probleme vključno s pravicami in drugimi varnostnimi podatki.

Preverimo dovoljenja za tajni direktorij.

Ker so lahko direktoriji s tržnimi podatki zaupne narave, je smiselno nadaljevati nadzor in redno preverjati rezultate nadzora in varnostni zapis.

Študij primera 3 - odgovor

Računalnik poženemo v "Recovery Console" in poženemo fixboot in fixmbr. Morda kaj od tega pomaga.

Preko "Recovery console" poženemo chkdsk ali pa poženemo "Safe Mode" ter poskusimo odstraniti težave z okvarjenimi datotekami.

Če so sistemske datoteke mše okvarjene, poskusimo spet zagon v režimu "Safe Mode" in restavriranje podatkov o stanju sistema ter sistemskih zaščitenih datotek.

Poskusimo restavracijo s pomočjo "ASR set".

Če je okvara razširjena, poskusimo restavracijo celotnega zvezka.

Če je disk okvarjen, ga zamenjamo in izvedemo potrebne restavracije.

Avtomatizacija administracije Windows Server 2003

Understanding Windows Automation

Computer Management Tasks

Disk and File Management Tasks

Security and Network Management Tasks

IIS 6.0 Tasks

Advanced Scripting Tools

Understanding Windows Automation

Windows Automation Essentials

Automation and Security

Working with VBScript

Security Best Practices

Computer Management Tasks

Client Management

Server Management

Inventorying and Reporting

Registry Management

Other Computer Management Tasks

Disk and File Management Tasks

File, Disk, and Volume Management

File Server Management

Security and Network Management Tasks

General Network and Server Management Tasks

Security Management Tasks

Service Management Tasks

User Account Management Tasks

Login Script Tasks

IIS 6.0 Tasks

IIS Web Site Management Tasks

FTP and SMTP Site Management Tasks

General IIS Management Tasks

Advanced Scripting Tools

User Interface and Databases

Wrapper Script.