WINS

DHCP

Internet Information Server

Radim Němec

Microsoft Certified Professional Systems Engineer

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

WINS

- Historie:
- Určení:
  - Zajišťuje překlad nebtios jmen na ip adresy. Jeho použití omezí broadcasty na síti.

PING IRIDIUM

dotaz na wins

vrátí se 10.1.220.6

WINS – instalace

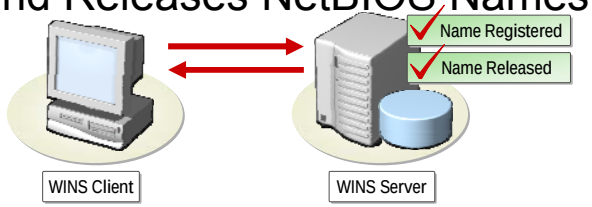
- WINS se instaluje jako služba
- Doporučuje se nainstalovat dva servery na organizaci pro zajištění dostupnosti
- Pokud je více WINS serverů nastavuje se mezi nimi replikace (PUSH, PULL)
- Databáze WINS by se měla pravidelně zálohovat a provádět její defragmentace.

What Is a NetBIOS Node Type?

A *NetBIOS node type* determines the method that a computer uses to resolve a NetBIOS name

Node type	Description	Registry value
B-node	**Uses broadcasts for name registration and resolution**	**1**
P-node	**Uses a NetBIOS name server such as WINS to resolve NetBIOS names**	**2**
M-node	**Combines B-node and P-node, but functions as a B-node by default**	**4**
H-node	**Combines P-node and B-node, but functions as a P-node by default**	**8**

How a WINS Client Registers and Releases NetBIOS Names

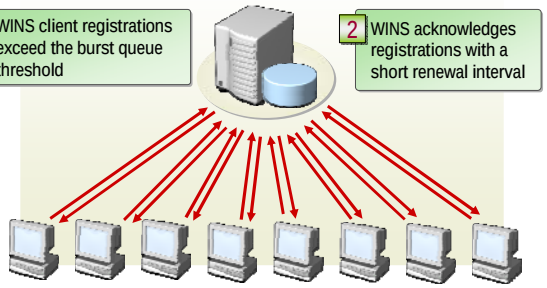


1. WINS client sends request to register
   - WINS server returns registration message with TTL value, indicating when the registration expires
2. WINS client sends request to release name
   - WINS server sends a positive name release response

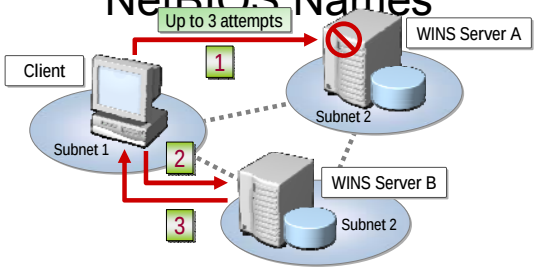
How Burst Handling Works

Burst handling allows a WINS server to handle a high number of simultaneous name registration requests

1. WINS client registrations exceed the burst queue threshold
2. WINS acknowledges registrations with a short renewal interval



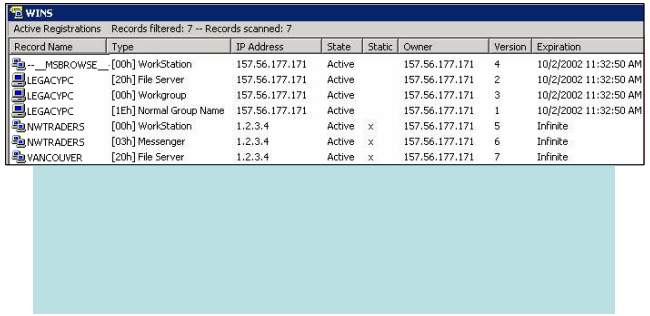
How a WINS Server Resolves NetBIOS Names



1. Client makes three attempts to contact WINS server, but does not receive a response
2. Client attempts to contact all WINS servers until contact is made
3. If name is resolved, IP address is returned to the client

Client Records

A WINS client record includes the following information:



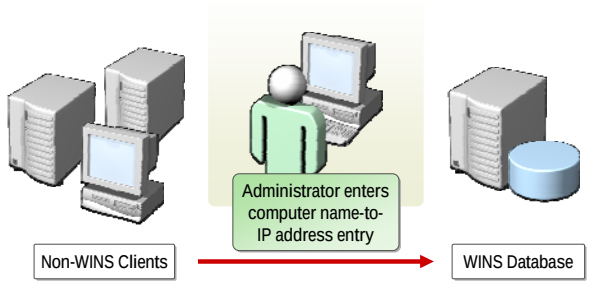
WINS

Active Registrations Records filtered: 7 -- Records scanned: 7

Record Name	Type	IP Address	State	Static	Owner	Version	Expiration
--__MSBROWSE__	[00h] WorkStation	157.56.177.171	Active		157.56.177.171	4	10/2/2002 11:32:50 AM
LEGACYPC	[20h] File Server	157.56.177.171	Active		157.56.177.171	2	10/2/2002 11:32:50 AM
LEGACYPC	[00h] Workgroup	157.56.177.171	Active		157.56.177.171	3	10/2/2002 11:32:50 AM
LEGACYPC	[1Eh] Normal Group Name	157.56.177.171	Active		157.56.177.171	1	10/2/2002 11:32:50 AM
NWTRADER5	[00h] WorkStation	1.2.3.4	Active	x	157.56.177.171	5	Infinite
NWTRADER5	[03h] Messenger	1.2.3.4	Active	x	157.56.177.171	6	Infinite
VANCOUVER	[20h] File Server	1.2.3.4	Active	x	157.56.177.171	7	Infinite

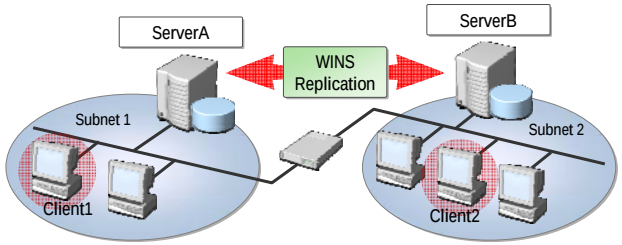
What Is a Static Mapping?

A *static mapping* is a manual entry in the WINS database



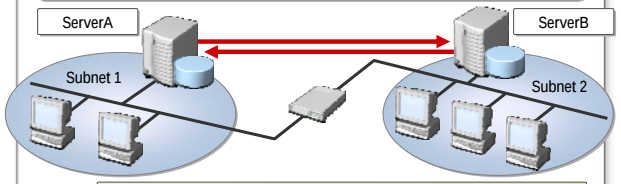
How WINS Replication Works

WINS replication occurs between two WINS servers to maintain consistent WINS data



How Push Replication Works

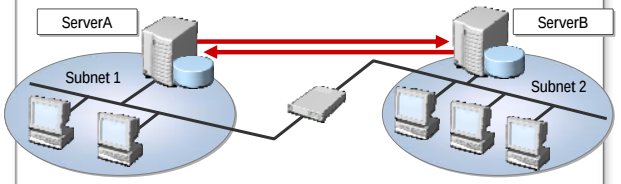
- A push partner notifies replication partners based on the number of changes in its database
- Push replication maintains a high level of synchronization



1. ServerA reaches set threshold of 50 changes in its database
2. ServerA notifies ServerB that the threshold is reached
3. ServerB responds to ServerA with a replication request
4. ServerA sends replicas of its new database entries

How Pull Replication Works

- A pull partner requests replication based on a time interval
- Pull replication limits frequency of replication traffic across slow links



1. ServerA requests database changes every 8 hours
2. ServerB sends replicas of its new database entries

What Is Push/Pull Replication?

Push/pull replication ensures that the databases on multiple WINS servers are nearly identical at any given time by:

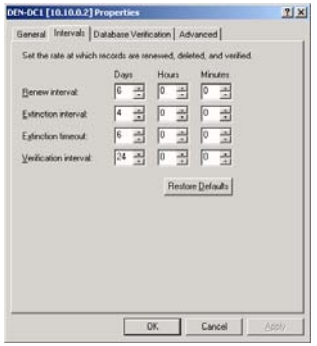
- Notifying replication partners whenever the database reaches a set threshold of changes

- And -

- Requesting replication based on a set time

How Scavenging Works

Scavenging removes extinct entries from the WINS database



Why Use DHCP?

DHCP reduces the complexity and amount of administrative work by using automatic TCP/IP configuration

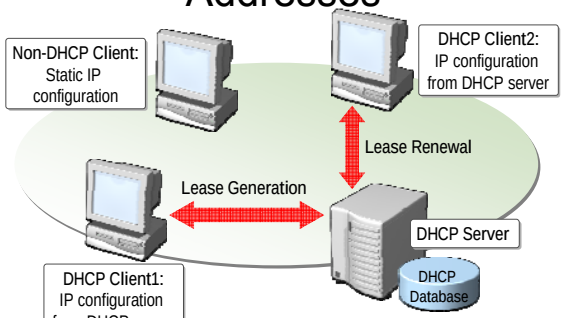
Manual TCP/IP Configuration	Automatic TCP/IP Configuration
IP addresses are entered manually	IP addresses are supplied automatically
IP address could be entered incorrectly	Correct configuration information is ensured
Communication and network issues can result	Client configuration is updated automatically
Frequent computer moves increase administrative effort	A common source of network problems is eliminated

What Is Automatic Private IP Addressing?

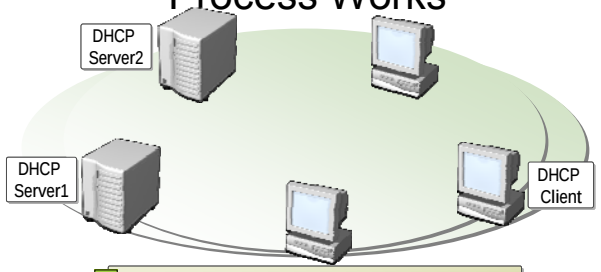
APIPA automatically self-configures addresses when there is no DHCP server available

Advantages	Disadvantages
Serves as a DHCP server failover mechanism for small networks	Forces assignment of addresses typically not used
Automatically assigns an IP address in a specific range	Conceals possible connectivity problems
	Does not work outside 169.254.x.x subnet
	Is not routable

How DHCP Allocates IP Addresses

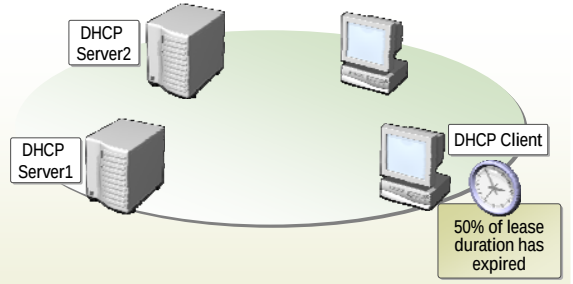


How the DHCP Lease Generation Process Works



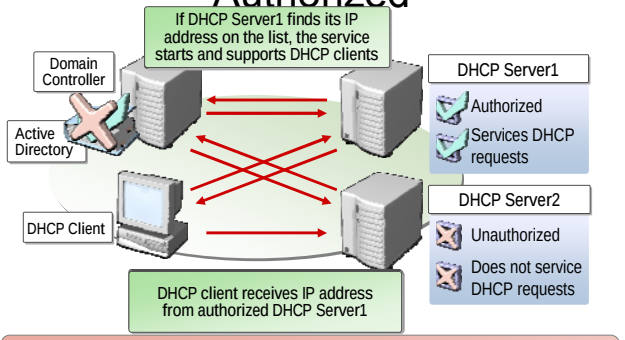
1. DHCP client broadcasts a DHCPDISCOVER packet
2. DHCP servers broadcast a DHCPOFFER packet
3. DHCP client broadcasts a DHCPREQUEST packet
4. DHCP Server1 broadcasts a DHCPACK packet

How the DHCP Lease Renewal Process Works



1. DHCP client sends a DHCPREQUEST packet
2. DHCP Server1 sends a DHCPACK packet

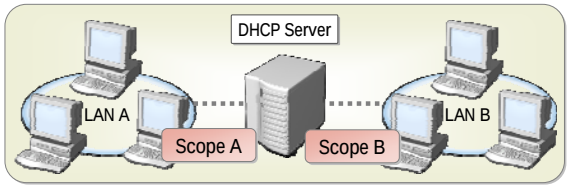
How a DHCP Server Service Is Authorized



DHCP authorization is the process of registering the DHCP Server service in the Active Directory domain to support DHCP clients

What Are DHCP Scopes?

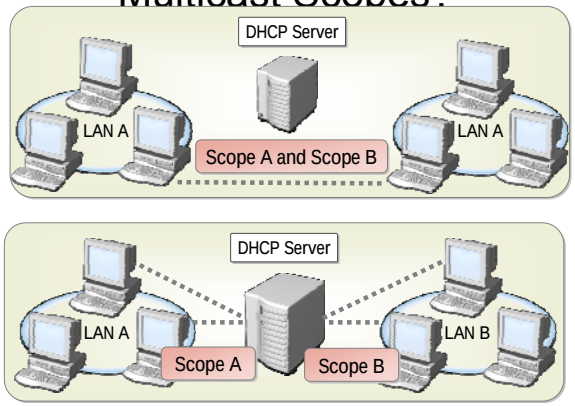
A *scope* is a range of IP addresses that are available to be leased



Scope Properties

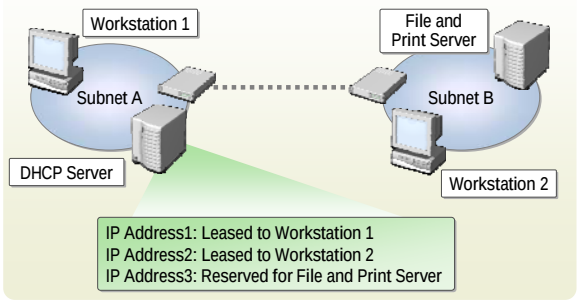
- Network ID
- Lease duration
- Scope name
- Subnet mask
- Network IP address
- Exclusion range

What Are Superscopes and Multicast Scopes?



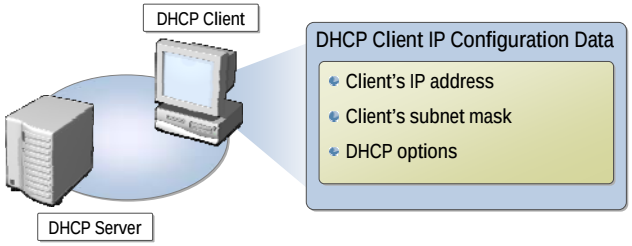
What Is a DHCP Reservation?

A *reservation* is a specific IP address, within a scope, that is permanently reserved for lease to a specific DHCP client

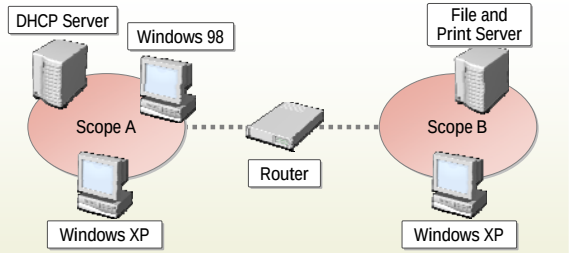


What Are DHCP Options?

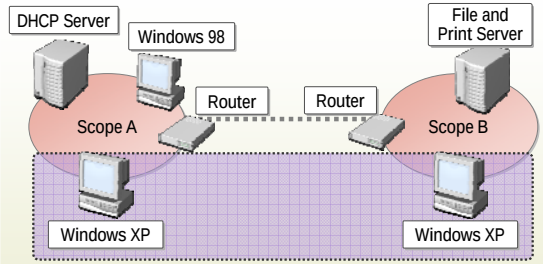
DHCP options are configuration parameters that a DHCP server assigns to clients



Reserved-Client Options Are Applied

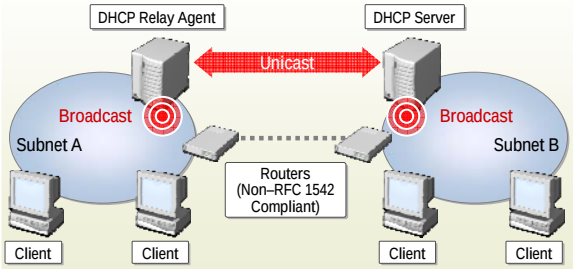


How DHCP Class-Level Options Are Applied

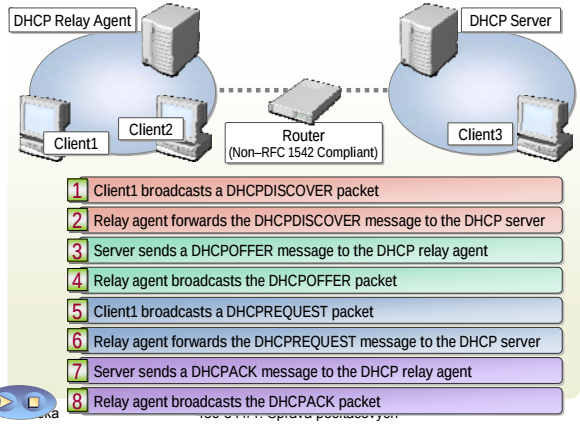


What Is a DHCP Relay Agent?

A DHCP *relay agent* is a computer or router that listens for DHCP/BOOTP broadcasts from DHCP clients and then relays those messages

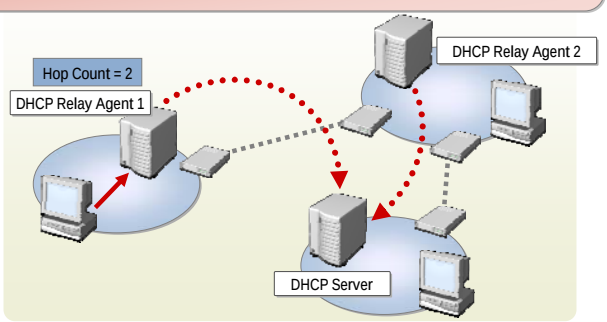


How a DHCP Relay Agent Works



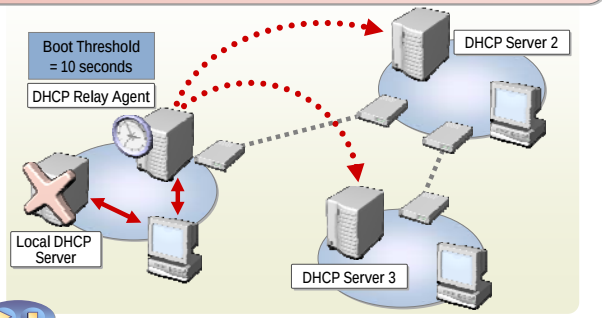
How a DHCP Relay Agent Uses Hop Count

The hop count threshold is the number of routers through which the packet can be transmitted before it is discarded



How a DHCP Relay Agent Uses Boot Threshold

The *boot threshold* is the time the DHCP relay agent will wait for a DHCP server response before forwarding the request



IIS

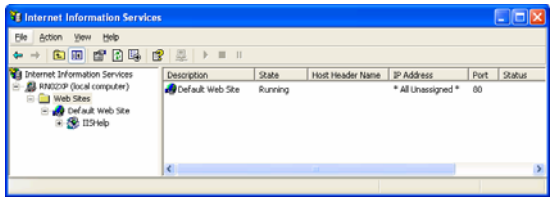
- první funkční web server 1991.
- 1992 – 50 serverů
- 2005 - 59,100,880 sajt

Apache - 40681140 (68.83%)
IIS - 12322111 (20.85%)
Sun - 1835718 (3.11%)
Zeus - 618599 (1.05%)

Porty :
– 80 Standard Web Traffic
– 443 SSL Web Traffic
– 81, 8080, … a spousta dalších, 0-65535!

IIS

Windows 2000 5.0 Windows 2003 6.0



IIS může běžet i na XP i na serveru. Použití na XP je spíše vhodnější pro vývoj nebo pro malé pracovní skupiny. Je totiž funkčně omezeno a má omezený počet připojení (10).

Xp nemá: multiple site, web site operatory, internet service manager HTML, process and bandwith throttling, limit přístupu podle jména klienta nebo IP.

IIS History

- IIS 2.0 Installed by NT 4.0
- IIS 3.0 followed by more common IIS 4.0
- Quickly gained reputation for (in)security
- IIS 5.0 Installed by Windows 2000
- Microsoft releases Hfnetchk
- Closely followed by IIS Lockdown and
- URL Scan
- IIS 6.0 Installed by Microsoft 2003 Server

Novinky v 6.0

Změna	Popis
Dva módy provozu	IIS 5.0 isolation mode Worker process isolation mode
Bezpečnost	IIS 6.0 se na serveru neinstaluje defaultně Pokud se nainstaluje je vysoce zabezpečen a defaultně v „zamčeném“ módu.
Metabase	Metabase jsou nyni dva textové soubory v xml formátu. MetaBase.xml a MBSchema.xml

XML metabase

- **XML Metabase**
  Dřívější verze ukládala svoje konfigurační nastavení do binární databáze zvané Metabase. IIS 6.0 nyní používá XML formát. XML soubory jsou prostý text takže je možné je editovat v ja66kémkoliv text editoru. Navíc má IIS 6 funkci editace za běhu. Pro aplikaci změn v konfiguraci nepotřebujete restartovat IIS, pokud neměníte schema – samostatný XML soubor který řídí strukturu záznamů do metabase.

  Tato změna podstatně urychlila start a stop IIS. Nyní je všechno rychle přístupné v XML souborech.

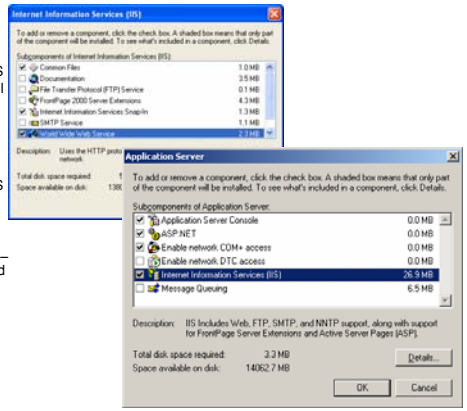
  Metabase.xml. – XML dokument s konfigurací, např. Detaily web sajt, a detaily virtuálních adresářů.
- MBSchema.xml. XML který obsahuje Metabase XML schema. Schema slouží jako kontrolní nástroj pro zajištění správných údajů v metabázi.

IIS

- **Default Lock-down Status**
  Pokud nainstalujete defaultně IIS server, nainstaluje se v „light módu“. Standardně jsou dostupné jen služby pro statický obsah (např. Htm soubory). Toto omezení funkce se nazývá: *Default Locked Down* status, a nutí adminy aby ručně přidávali ty vlastnosti které potřebují pro svoje aplikace.

IIS – instalace

Doporučený postup
- Instalovat IIS na NTFS
- Nastavit interní firewall na potřebné porty (zpravidla: HTTP, HTTPS, FTP, and SMTP), nebo jej vypnout a spoléhat na korporátní firewall
- Pokud instaluji více IIS serverů můžu použít unattended setup
- Pozor v XP je přímo v add programs - windows components – IIS. V serveru je to pod Application server



Instalace

- Vlastní server: %SystemRoot%\System32\InetSrv
- Admin aplikace: %SystemRoot%\System32\IIsAdmin
- Webové sajty:
- %SystemRoot%\InetPub
- Účty:

  IUSR_jmenopocitace – pro anonymní přístup

  IWAM_jmenopocitace – pro běh aplikací

Služby IIS

- FTP
- IIS Admin
- SMTP
- WWW Publishing service
- NNTP
- Internet printing
- BITS – background inteligent transfer
- Frontpage 2002 extension

BITS

- Background Intelligent Transfer Service
- služba která pro stahování spotřebovává nevyužitou šířku pásma, takže nezpomaluje jinou práci uživatele na internetu, a umí navázat přerušené spojení.
- Využívá ji např. Windows update

Jak provozovat více sajt na jednom serveru?

- Různé čísla portů
- Různé ip adresy
- Různé host headers (HTTP 1.1.)

Např. http://sales.com

http://research.com

Virtuální adresáře

- Virtuální adresář je adresář který odkazuje na jiné místo na stejném nebo jiném počítači.

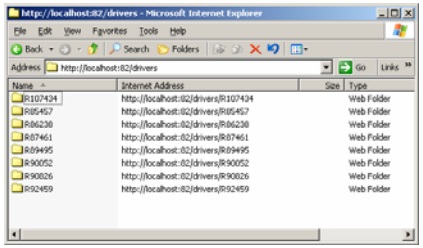
Fyzicky	Virtuálně
c:\sales	http://sales
C:\sales\marketing	http://sales/marketing
C:\sales\orders	http://sales/orders
\\Server2\customers	http://sales/customers
\\Server2\PR	http://sales/pr

UTF-8

- **Unicode Transformation Format-8 (UTF-8)**
  Dřívější verze IIS zapisovaly do logu jenom v angličtině. To byl problém pro vícejazykové sajty. IIS 6.0 to řeší podporou UCS Transformation Format (UTF) 8. Můžete nastavit *HTTP.sys* aby logoval v příslušné jazykovém formátu. Podpora UTF-8 je pro URL i pro názvy souborů. Active Server Pages (ASP) jsou podporovány rovněž. V tomto případě se unicode převádí do UTF.
- Tato podpora není pro FTP sajty.

Správa obsahu

- FTP
- Tradiční metoda
- Potřebuje další porty
- Neumí file lock soubory je nutné stáhnout a pak editovat



WebDav (Web-based Distributed Authoring and Versioning)

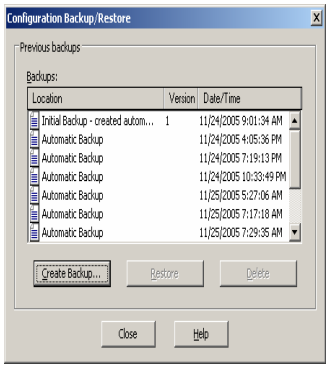
Je třeba zprovoznit na serveru
Na klientovi spustit službu webclient
U častých položek Add Network Place

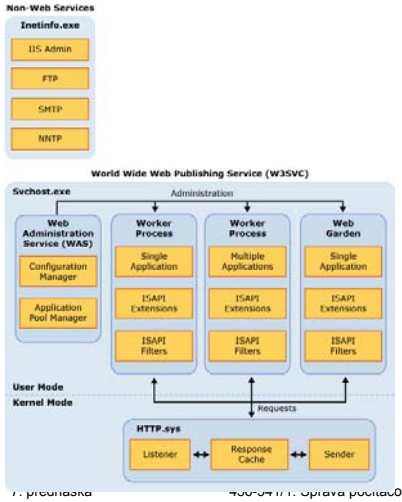
IIS – web page extensions

- ASP.NET executions
- ASP executions
- CGI and ISAPI applications
- Front Page Server Extensions 2000 and 2002
- WebDAV support for IIS directories

IIS – záloha metabase

- IIS 6.0 používá pro zálohu metabase XML soubor
- V konzole server, all task – backup/restore configuration



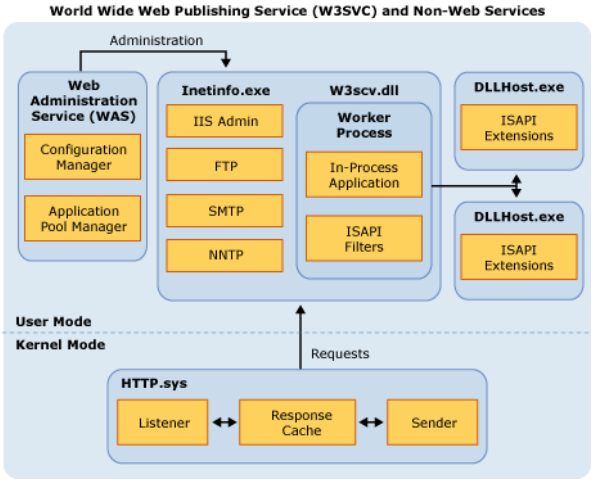


IIS 5.0 Isolation Mode

IIS 5.0 isolation mode manages application processes in a similar fashion to the process management in IIS 5.0: all in-process applications run inside Inetinfo.exe, and out-of-process applications run in separate DLL hosts. Some existing applications may not have been written to run concurrently, or store state separately from the application. Therefore, running processes in IIS 5.0 isolation mode ensures compatibility for most existing applications.

Worker Process Isolation Mode

When configured to execute in worker process isolation mode, all application code runs in an isolated environment. This design removes some of the existing bottlenecks. Worker process isolation mode allows the administrator to isolate anything from an individual Web application to multiple sites in their own self-contained World Wide Web Publishing Service (WWW service) process. This prevents one application or site from stopping another. In addition, separating applications or sites into their own process space simplifies a number of management tasks, such as restarts (independent of all other sites or applications running on the system), changing a component used by the application, debugging, monitoring counters, throttling resources, and so forth.

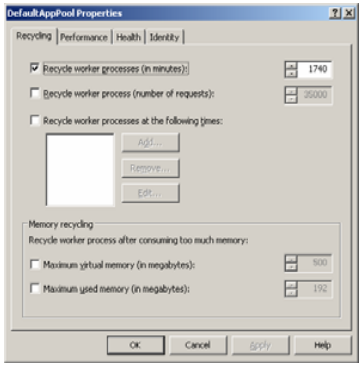


IIS

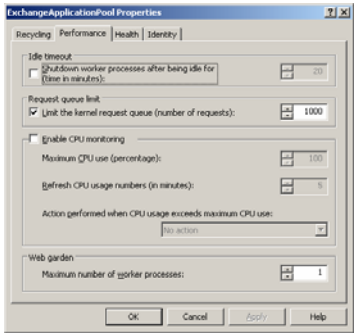
- **Health Detection**
  Automatická detekce zjednodušuje správu IIS web sajt. IIS dělá detekci pro všechny worker procesy. Což přidává další stupeň spolehlivosti web aplikací. Proces *inetinfo.exe* (IIS) pravidelně kontroluje dostupnost procesů. Interval kontroly jde nakonfigurovat. Tímto dělá IIS "*heart beat*" mezi svými worker procesy, což je něco podobného jako ping. Během každé kontroly IIS server zkouší komunikovat s worker procesy, aby se přesvědčil jestli žijí.

Application pool

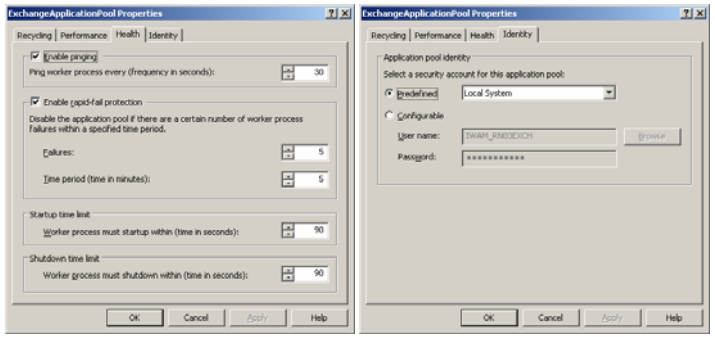
- Díky app pool běží aplikace samostatně, jedna nesestřelí ostatní procesy. Navíc běží odděleně od inetinfo
- Recycling – automatický restart
  -po čase
  -po určitém počtu požadavků
  -V určitou dobu
  -Podle paměti



App pool - Performance



App pool – Health a Identity



Web site - vlastnosti

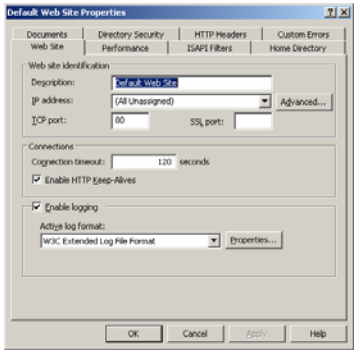
Web Site – možnosti nastavení

IP adresa

TCP port

Connection timeout

Logování – různé formáty



Web site – home directory

Home directory

Umístění stránky

Práva – čtení, zápis, spouštění skriptů, procházení adresáře

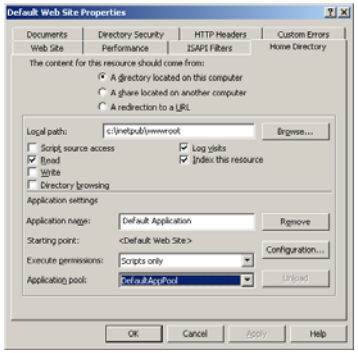
Nastavení aplikace

Jméno aplikace

Oprávnění pro spuštění

App. Pool

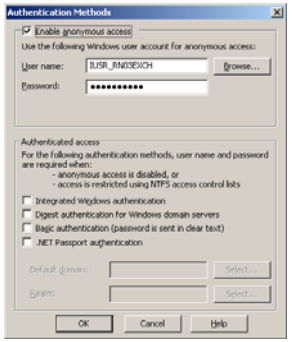
Tady se dá nastavit přesměrování na jiný web.



Autentikace

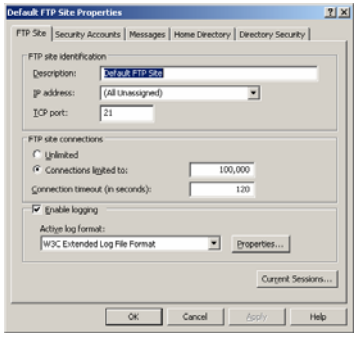
- ANONYMOUS
- BASIC – nekryptuje hesla, pouze kóduje
- INTEGRATED WINDOWS neposílá hesla, je bezpečné, nefunguje přes proxy a fw. Dva typy NTLM a Kerberos. O tom který rozhoduje browser.

  Funguje jen s IE.
- DIGEST – neposílá heslo přes síť ale jen hash, funguje přes fw i proxy, uživatel musí mít logon locally právo. V AD musí být nastaveno store password using reversible encryption (a to není bezpečné).
- .NET PASSPORT



FTP

- vždy zvážit jeho použití, pozor na odchycení hesel
- lepší je používat ftp jen pro anonymní přístup



Podpora skriptování

- IISRESET /RESTART
- IISRESET /START
- IISRESET /STOP
- Reboot, rebootonrttot,noforce,timeout,status, enable, disable

API

- ISAPI
  - Pro vývoj rozšíření IIS. Větší výkon než ASP a CGI, low-level přítup na MS Win32 API

  ISAPI extensions – runtime dll

  ISAPI filters – např. HTTP compression (nebo enkrypce dat, custom logging, custom authentication).
- ASP
- CGI

HTTPS

- Potřebujeme certifikát z certifikační autority
- Certifikát buď od vlastní CA tomu nedůvěřují venkovní klienti nebo od standardní CA jako Verisign nebo Thawte, ten je ale drahý. Lze využít i certifikát od ICA.
- CTL – cert trust list. CA kterým věříme
- CRL – cetr. Revocation list – odvolané certifikáty

Monitoring a optimalizace

- Connection limits
- HTTP compresse
- Bandwith throttling
- NLB clustering
- Web Application stress tool
- Monitoring standardními prostředky Windows – vytvořit si „baseline“
- Convlog – konverze logů

SMTP

- IIS jde nastavit jako SMTP server

Bezpečnost

- Patche a service packy
- Bezpečnostní audit
- Penetrační test
- Firewally
- IDS

Útoky

- Sociální inž. – tady helpdesk řekněte mi heslo
- Využití standard bezpečnostních konfigurací – default hesla atd.
- IP spoofing – předstírání jiné ip adresy
- Útoky na nevyužívané služby – co nepotřebuji zastavím
- Využití zadních vrátek – backdoor – cesty které jsou určeny pro přístup když jsou poškozeny původní admin účty
- Session takover – přetečením bufferu

DOS útoky

- Diskový prostor
- Šířka pásma
- Buffery – útoky na specifické porty
- CPU cykly

Port scannig

- Útočník si analýzou portů udělá přehled které služby běží a který os běží
- Nastavte firewall
- Nastavte aby vám přišlo upozornění na PS
- Zastavte zbytečné služby

Vysoká dostupnost

- Windows clustering
- Network load balancing

Securing IIS

- Run IIS Lockdown Tool
- Run URL Scan
- Remove test, development and example
- files from the public webserver
- Set NTFS ACLs on Webserver directories

IIS Lockdown Tool (2.1)

- Automatic ‘Lock Down’
- • Locks down IIS 4.0, IIS 5.0, default on 6.0
- • Express ‘lock down’ for simple web sites
- • Custom ‘lock down’ for more complex
- servers
- • Undo facility to reverse last ‘lock down’
- • URL:
- http://www.microsoft.com/technet/security/tools/l
- ocktool.mspx

IIS Lockdown Tool (2.1)…

Disable:
- Active Server Pages
- Index Server Interface
- Server Side Includes
- Internet Data Connector
- Internet Printing
- HTR Scripting

Remove:
- Sample Web Files
- Script Virtual Directory
- MSADC Directory
- WebDAV

Set Permissions on:
- Exe files
- Content Directories

URL Scan (2.5)

- ISAPI filter scans incoming HTTP requests
- Filtered based on rule set
- New rules easily added
- Default urlscan.ini suitable for static pages
- Restart service when changes made
- 404 and logged request for matched rules
- URL: http://www.microsoft.com/technet/security/tools/urlscan.mspx

URL Scan (2.5)…

Filter on:
- The request method (verb)
- File Extension
- URL Encoding
- Non ASCII characters
- Malicious character sequence
- Headers in HTTP GET

Port Reporter Tool

- Microsoft released the Port Reporter Tool in late 2004.
- Runs on; Windows 2000, XP and 2003 Server.
- Logs TCP and UDP activity:

– The ports that are used
– The processes that use the port
– Whether a process is a service
– The modules that a process loaded
– The user accounts that run a process

PortQry Tool (2.0)

- TCP/UDP Port query tool
- Released Summer 2004
- Useful for troubleshooting connectivity issues.
- Has the same functionality as fport
- Portqry –v –local
- URL: http://support.microsoft.com/default.aspx?kbid=832919

A to je vše přátelé

otázky???

IIS - podrobnosti

- **Server-gated Cryptography**
  Text-based HTTP network transmissions between a server and client can easily be compromised; therefore, whenever you need to communicate privately you must encrypt all HTTP calls and responses. Secure Socket Layer (SSL) and Transport Layer Security (TLS) are the most common encryption mechanism used on Web sites. SSL/TLS enables secure communication by encrypting the communication channel with a cipher algorithm. TLS is a later (and more secure) version of the SSL protocol.

  A further extension of SSL/TLS is Server-gated Cryptography (SGC) which has been available in a 40-bit version since version IIS 4. IIS 6.0 adds a strong 128 bit encryption mechanism to SGC. Adding SGC encryption to your applications does not require any special application code on the client machines; however, it requires a valid *certificate* at the client Web browser, which can encode and decode the data. You need a special SGC certificate to enable the SGC support built into IIS 6.0, which you can obtain by contacting a certificate authority. You add the certificate to IIS just like you'd add any other certificate. IIS 6.0 supports both 40 bit and 128 bit encryption sessions, so your old 40 bit SGC certificates are still valid in IIS 6.0. So far, financial sector applications (such as banking and other financial institutions) are the most common users of SGC

IIS - podrobnosti

- **Selectable Cryptographic Service Provider (CSP)**
  SSL/TLS offer a secure environment in which to exchange data, but they're both CPU intensive and have a negative performance impact. IIS 6.0 comes with a new feature called Selectable Cryptographic Service Provider (CSP) that lets an administrator or developer select from an optimized list of cryptography providers. A cryptographic provider provides you with an interface to encrypt communication between the server and the client. CSP is not specific to IIS and can be used to handle cryptography and certificate management.

  Microsoft implements two default security providers. Those are the Microsoft DH SChannel Cryptographic provider and Microsoft RSA SChannel Cryptographic provider. The Microsoft implementations are optimized for IIS 6.0 to provide faster communications. Windows stores the private keys for these implementations in the registry.

  The Microsoft Cryptographic API (Crypto API) for every provider contains an identical interface for all providers, so you can switch between providers to without modifying the code. Each provider creates a public and a private key to enable data communication. The private key is stored on hardware devices (such as PCI cards, Smart Cards etc.) or in the Registry. The other CSP keys can also be stored in the registry. It makes more sense to store private key as registry settings for computer access to the server. The private key is usually stored on Smart Cards and other portable devices for mobile distribution environments. (This is similar to *Plug and Play* support for devices on Windows 2000 and Windows 2003 environments.) The CSP can be configured using the "Welcome to the Web Server Certificate Wizard." To reach the wizard, select the Directory Security tab from the site's Properties dialog, and then click the Server Certificate button.

IIS - podrobnosti

- **Other New Features**
  Earlier versions of IIS (2.0 through 5.0) used a scripting host environment called Active Server Pages (ASP). IIS 6.0 uses ASP.NET language hosting instead. There are some significant advantages to the ASP.NET architecture compared to the older ASP architecture. Some of those advantages include:
- ASP.NET is based on the Microsoft.NET framework. You could write ASP code in VBScript, JScript, or any other scripting language that ran in the Microsoft Scripting Runtime host environment. You can code ASP.NET in any language compatible with the common language runtime (CLR). Currently, Microsoft's CLR-compatible languages include Visual C#, VB.NET, Jscript.NET, and J#, but languages from many other vendors are either available or under development.
- You can have code in more than one language in the same ASP.NET page. In other words, you can call a VB.NET function from a C# ASP.NET page.
- ASP code is interpreted. The runtime engine compiles the code line by line at runtime, while ASP.NET code is completely compiled in advance—not line by line. ASP.NET compiled code runs significantly faster than ASP interpreted code.
- ASP.NET gives you three levels of caching. You can cache complete pages, selected parts of the pages (called fragment caching), or by using the Caching API. Developers can use the Caching API to exert fine-grained control over caching behavior, and thus increase performance.

IIS - podrobnosti

- **New Request-processing Architecture**
  In Windows 2003 server, the HTTP stack is implemented as a kernel mode device driver called *HTTP.sys*. All incoming HTTP traffic goes through this kernel process, which is independent of the application process. IIS 6.0 itself is an application process and is external to *HTTP.sys*. Application processes run in *user mode* and the operating system functions are run in *kernel mode*. HTTP.sys is responsible for:

- Connection management—managing the database connections from the ASP.NET pages to data bases
- Caching—reading from a static cache as opposed to recompiling the ASP.NET page
- Bandwidth throttling—limiting the size of the Web requests to a Web site
- Text based logging—writing IIS information into a text log file
- In IIS 5.0, the HTTP request was handled by the IIS *inetinfo.exe* application. In IIS 6.0, *HTTP.sys* relieves IIS of request-handling responsibility. In doing so, it enhances IIS performance in the following ways.

- *HTTP.sys* enables caching (referred to as flexible caching) at kernel level so that static data can be cached for faster response time (independent of the user mode caching). You need to be careful with flexible caching. Since *HTTP.sys* is separate from IIS we may still cache old data after a IIS restart.
- *HTTP.sys* introduces a mapping concept called "application pool." Application pooling allows Web sites to run together in one or more processes, as long as they share the same pool designation. Web sites assigned to different application pools never run in the same process. A central Web site (such as a credit card verification Web site) can be accessed by all the other miscellaneous sites (such as shopping cart E- Commerce sites) by using application pooling. By using the correct application pool information *HTTP.sys* can route the HTTP traffic to the correct Web site.
- The *HTTP.sys* application pool concept increases the number of Web sites you can host host on a single machine. It also increases performance and provides more control over access to valuable IIS resources.