Introduction to IIS and HTTP

Internet Information Services


Web Server

- separate product for **NT 4.0 (IIS 4.0)**
  - supports TLS/SSL with Schannel
  - metabase binary configuration database (LDAP compliant)
- first integrated within **Windows 2000 (IIS 5.0)**
  - no direct support for ASP.NET
  - limited application isolation (service or individual worker process)
- integrated with HTTP.SYS in **Windows 2003 (IIS 6.0)**
  - first XML editing of metabase
  - application pools and ASP.NET integration
  - shared content storage
- strictly XML configuration in **Windows 2008 (IIS 7.0)**
  - HTTPS in kernel mode
  - modular architecture and request pipeline
  - request filtering
  - installation with ServerManagerCmd.exe
  - kernel mode authentication, AppPoolIdentity
  - IIS Management Service
  - non-Windows FTP accounts
  - shared configuration storage
  - URL rewrite module
Web Server

- Slightly improved in Windows 2008 R2 (IIS 7.5)
  - Schannel supports AES, SHA2
  - Complex and scriptable request filtering
  - WebDAV extension
  - Full installation with PowerShell
  - Support for managed service accounts
  - FTPS

- Security improved in Windows 2012 (IIS 8.0)
  - TLS SNI for multiple certificates on a single IP address
  - Binding TLS certificates from a central PFX share
  - Support for group managed service accounts
  - Dynamic IP restrictions (DoS, x-forwarded-for)
  - CPU limits per application pool
  - FTP account lockout

- Minor improvements in Windows 2012 R2 (IIS 8.5)
  - Certificate rebinding when renewed
  - Logging custom fields

- Minor improvements in Windows 2016 (IIS 10)
  - Wildcard host headers
  - Running on Nano Server
  - HTTP/2
  - PowerShell cmdlets shadowing appcmd

IIS and HTTP.SYS

User Mode

- SSTP
- WinRM
- IPHTTPS
- Hyper-V Replication
- Reporting Services
- IIS

Kernel Mode

Certificate

HTTP.SYS
HTTP.SYS

NETSH http show servicestate

NETSTAT -ano | findstr :80

NETSH http show sslcert

Installation

- GUI Add Windows Components wizard
  - Windows 2003-
- ocsetup.exe command line
  - Windows 2003-
- GUI Server Manager
  - Web Server role
  - Windows 2008+
- ServerManagerCmd.exe
  - Windows 2008
- PowerShell Get-WindowsFeature, Add-WindowsFeature
  - Windows 2008 R2+
NET Framework versions

- v1.0 core engine
- v1.1 core engine
  - can be installed manually yet on Windows 2012 R2
- v2.0 core engine (requires installation SXS media on Windows 2012+)
  - 3.0 update + new functionality
  - 3.5 update + new functionality
- v4.0 core engine
  - 4.5 update + new functionality
  - 4.51 update + new functionality
  - 4.6 update + new functionality
  - 4.6.2, 4.7, ...

Installation paths and Default Web Site

- %windir%\System32\inetsrv
  - metabase.bin (IIS 5.0)
  - metabase.xml (IIS 6.0)
- %windir%\System32\inetsrv\config
  - applicationHost.config (IIS 7.0+)
- %systemroot%\inetpub
  - logs
  - custErr
  - wwwroot = Default Web Site
  - temp
Default Web Site (ID=1)

- By default installed
- Not always necessary (usually configuration can be finished manually if not present)
  - AD CS Web Enrollment
  - AD CS Policy/Enrollment Web Services
  - Exchange CAS server
  - AD FS before Windows 2012 R2
    - AD FS Windows 2012 R2+ has direct HTTP.SYS hosting
  - SQL Reporting Services until SQL Server 2008 R2
    - SQL RS 2008 R2 has direct HTTP.SYS hosting
  - Internet printing
- Who does not need Default Web Site
  - SharePoint 2010+
  - DirectAccess 2012+
  - AD FS and WAP on Windows 2012 R2+
  - SQL RS 2008 R2+

Post installation WF exceptions

- Inbound
- Process SYSTEM (HTTP.SYS)
- TCP 80
- TCP 443
  - although not opened
  - firewall hides (stealth) even unopened ports
HTTP

- Hypertext Transport Protocol
- Plaintext or wrapped inside TLS/SSL HTTPS
- TCP 80 or TCP 443 by default
- Request-response based nature
  - every request must contain all parameters
  - any request can hit a different farm member

Web server farms (load balancing with separate TCP connection)
Web server farms (load balancing with direct TCP connection)

Web Site

- Virtual web server
- Binding to http(s):IP:port:host
  - more web servers on the same IP:port
- Returns content from a physical disk location
**URI = URL + Query**  
**URL = Protocol + Host + URN**

- **Unified Resource Identifier**
  - **URL**
    - Protocol
    - Host (FQDN)
    - URN
  - **Query String**
    - ?ID=8&Param=Test
  - **Fragment**
    - #HTMLtagID

- **Unified Resource Name**
  - /SitePages/default.aspx
  - /Lists/Products/EditForm.aspx

- **Query String**
  - /Lists/Products/EditForm.aspx?ID=8&Param1=X;Param2=Y

- **Fragment**
  - /Wiki.aspx?ID=7#heading1 (references any id="", or <hX>, or <A name="">)

**HTTP Methods**

- GET
- HEAD
- POST

- GET If-Modified-Since, 304 Not Modified
- GET Authorization
  - Kerberos / NTLM
  - Basic
- POST
  - "postback" to the same URL
GET vs. POST method

- **GET**
  - URL (URI) encoded form parameters
  - ?, #
  - bookmarks, history, refresh + reenter
- **POST**
  - might have URL (URI) encoded parameters as well
  - mostly included inside request body
  - cannot bookmark, no history, invisible in the address bar, F5 asks to resend

URL examples

  - not an FQDN, cannot be resolved from internet
  - using FQDN, might be resolvable from internet
- http://finance/Seznam českých jmen.htm
- http://finance/Seznam%20českých%20jmen.htm
- http://finance/seznam%20%C4%8Desk%C3%BDch%20jmen.htm
- file://C:\MyPages\test.htm
  - local file only
- file://\filesrvr\WebPages\test.htm
Encoding URI and header characters

- URI and headers must be *7bit US-ASCII* only
- URI characters encoded with *%xx* in hex format
- Header data are usually encoded with Base-64
  - a-z, A-Z, 0-9, =/+
  - Ahoj Ondřejí = QWhvaiBPbmTFmWVqaQ==

Static content and returned HTMLs

- Static file
  - must have MIME type defined
- Default document
  - if not any present, tries Directory Browsing, or HTTP 403
- Directory browsing
  - if no explicit URL is specified, generates HTML with directory listing
Virtual Directories

- Folder structure from URL perspective

HTTP Status Codes

- 200 OK
- 30x redirect
  - temporary, permanent, method, not modified
- 40x client error
  - unauthorized, forbidden, bad request
- 50x server error
  - internal error, overloaded temporarily, gateway timeout

- Substatus not visible to clients by default
  - Error pages can switch to detailed errors
### 404 Not Found - substatus codes in IIS

<table>
<thead>
<tr>
<th>What</th>
<th>Error code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site not found</td>
<td>404.1</td>
</tr>
<tr>
<td>Denied by policy</td>
<td>404.2</td>
</tr>
<tr>
<td>Denied by mime map</td>
<td>404.3</td>
</tr>
<tr>
<td>No handler</td>
<td>404.4</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> URL Sequence denied</td>
<td>404.5</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Verb denied</td>
<td>404.6</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> File extension denied</td>
<td>404.7</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied by hidden segment</td>
<td>404.8</td>
</tr>
<tr>
<td>Denied since hidden file attribute has been set</td>
<td>404.9</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because request header is too long</td>
<td>404.10</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because URL doubled escaping</td>
<td>404.11</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because of high bit characters</td>
<td>404.12</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because content length too large</td>
<td>404.13</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because URL too long</td>
<td>404.14</td>
</tr>
<tr>
<td><strong>Request Filtering:</strong> Denied because query string too long</td>
<td>404.15</td>
</tr>
<tr>
<td>.NET 2.0/4.0 version not registered</td>
<td>404.17</td>
</tr>
</tbody>
</table>

### MIME/content types

- text/html
- image/jpeg
- image/png
- .doc = application/msword
- .docx = application/vnd.openxmlformats-officedocument.wordprocessingml.document
- application/pdf
Logging

- W3C log always UTC time
- Logging settings at server-level only default for new sites
- NETSH HTTP FLUSH LOGBUFFER

Static content HTTP headers
HTTP.SYS tracing

logman start httptrace -p Microsoft-Windows-HttpService 0xFFFF -o trace-output.etl -ets

logman stop httptrace -ets

tracerpt.exe trace-output.etl -of XML -o trace-output.xml

IIS Error Pages
Static content compression into TEMP
Dynamic content compressed on the fly

Compression

Use this feature to configure settings for compression of responses. This can improve the perceived performance of a website greatly and reduce bandwidth-related charges.

- [x] Enable dynamic content compression
- [ ] Enable static content compression

Compression settings server wide
Dynamic content

- Common gateway interface (CGI)
  - simple EXE producing output into stdout
- Active Server Pages (ASP)
  - since ever, still supported
- PHP
  - similar to ASP
  - third-party, yet supported since Windows 2008 R2
- NET Framework ASPX
  - various languages such as C#, VB.NET, Python
  - inline-code
  - code-behind
- ISAPI DLLs such as RPCProxy.dll with Handler Mappings
- HTTP Modules such as Exchange PowerShell or SharePoint SPRequestModule
Classic ASP error messages

Custom and ASP.NET developer errors

- Error html vs. IIS detailed errors
  - can be customized
  - or if missing, generic error message as pure text is returned
  - or errorMode="Detailed"
- ASP.NET detailed errors: mode="Off"

```xml
<configuration>
  <system.web>
    <customErrors mode="On|Off|RemoteOnly" />
  </system.web>
  <system.webServer>
    <httpErrors errorMode="Detailed" />
  </system.webServer>
</configuration>
```
WAS, W3SVC and HTTP.SYS

Some events from WAS: 

1. A process serving application pool 'portal AppPool' terminated unexpectedly. The process id was 2508. The process exit code was '0x1'.
2. Application pool 'portal AppPool' is being automatically disabled due to a series of failures in the process(es) serving that application pool.
AppPool recycling and Rapid Fail Protection

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Time-out (minutes)</td>
<td>20</td>
</tr>
<tr>
<td>Idle Time-out Action</td>
<td>Terminate</td>
</tr>
<tr>
<td>Load User Profile</td>
<td>False</td>
</tr>
<tr>
<td>Maximum Worker Processes</td>
<td>1</td>
</tr>
<tr>
<td>Ping Enabled</td>
<td>True</td>
</tr>
<tr>
<td>Ping Maximum Response Time</td>
<td>90</td>
</tr>
<tr>
<td>Ping Period (seconds)</td>
<td>30</td>
</tr>
<tr>
<td>Shutdown Time Limit (seconds)</td>
<td>90</td>
</tr>
<tr>
<td>Startup Time Limit (seconds)</td>
<td>90</td>
</tr>
</tbody>
</table>

**Rapid-Fail Protection**

- "Service Unavailable" Response Type: HttpLevel
- Enabled: True
- Failure Interval (minutes): 5
- Maximum Failures: 5
- Include this recycle type in the recycle config file.
- Include this recycle type in the recycle config file.

**Recycling**

- Disable Overlapped Recycle: False
- Disable Recycling for Configuration Changes: False
- Generate Recycle Event Log Entry: True
- Private Memory Limit (KB): 0
- Regular Time Interval (minutes): 1740

**IISRESET + /noforce**

```cmd
C:\>iisreset /status
Status for Windows Process Activation Service ( WAS ) : Running
Status for World Wide Web Publishing Service ( W3SVC ) : Running
C:\>iisreset /restart
Attempting stop...
Internet services successfully stopped
Attempting start...
Internet services successfully restarted
C:\>
```
Limits

- **TCP/IP stack driver limit**
  - HKLM\System\CurrentControlSet\Service\TCPIP\Parameters
    - TcpNumConnections = DWORD = 0 - 16 777 214

- **Web site limits**
  - http.sys

- **Apppool limit**
  - http.sys
Limits

- **ASP.NET limits**
  - httpRuntime - executionTimeout

---

Limits

- **ASP.NET limits**
  - machine.config
  - processModel – maxWorkerThreads, maxIoThreads
Service code isolation

Isolation

<table>
<thead>
<tr>
<th>Domain</th>
<th>Account</th>
<th>Network Password</th>
<th>Groups</th>
<th>Local Isolation</th>
<th>Network Isolation</th>
<th>Kerberos PAC Validation</th>
<th>OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>NT AUTHORITY</td>
<td>SYSTEM</td>
<td>automatic 30 days</td>
<td>Administrators</td>
<td>no</td>
<td>MACHINE$</td>
<td>no</td>
<td>2000</td>
</tr>
<tr>
<td>NT AUTHORITY</td>
<td>Network Service</td>
<td>automatic 30 days</td>
<td>Users</td>
<td>no</td>
<td>MACHINE$</td>
<td>no</td>
<td>XP</td>
</tr>
<tr>
<td>NT AUTHORITY</td>
<td>Local Service</td>
<td>no</td>
<td>Users</td>
<td>no</td>
<td>anonymous</td>
<td>no</td>
<td>XP</td>
</tr>
<tr>
<td>NT SERVICE</td>
<td>&lt;serviceName&gt;</td>
<td>automatic 30 days</td>
<td>Users</td>
<td>yes</td>
<td>MACHINE$</td>
<td>no</td>
<td>Vista 2008</td>
</tr>
<tr>
<td>IIS APPPOOL</td>
<td>&lt;appPoolName&gt;</td>
<td>automatic 30 days</td>
<td>Users</td>
<td>yes</td>
<td>MACHINE$</td>
<td>no</td>
<td>Vista 2008</td>
</tr>
<tr>
<td>&lt;domain&gt;</td>
<td>&lt;userName&gt;</td>
<td>manual</td>
<td>Users</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>2000</td>
</tr>
<tr>
<td>&lt;domain&gt;</td>
<td>&lt;managedSvcAccount&gt;</td>
<td>automatic 30 days</td>
<td>Users</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>7 2008 R2</td>
</tr>
<tr>
<td>&lt;domain&gt;</td>
<td>&lt;groupSvcAccount&gt;</td>
<td>automatic 30 days</td>
<td>Users</td>
<td>yes</td>
<td>yes</td>
<td>no</td>
<td>8 2012</td>
</tr>
</tbody>
</table>
AppPool identity

- appcmd list apppool /text:*

Group Managed Service Account (gmsa)

# on DC
New-AdServiceAccount
  -Name web-finance
  -DnsHostName finance.gopas.virtual
  -PrincipalsAllowedToRetrieveManagedPassword gps-wfe1$,gps-wfe2$

# on each WFE
Add-WindowsFeature RSAT-AD-PowerShell
Install-AdServiceAccount
HTTP authentication

- HTTP authentication
  - no logoff
  - Windows offers SSO
- Cookie-based application authentication with forms-based logon page
  - smaller network footprint than Kerberos
  - cookie expiration
  - cookie sharing with state server

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>SSO</th>
<th>Windows</th>
<th>Third party</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous</td>
<td>nothing from client</td>
<td>no</td>
<td>impersonates IUSR by default should use application pool identity instead</td>
<td>yes</td>
</tr>
<tr>
<td>Basic</td>
<td>clear-text</td>
<td>no</td>
<td>any</td>
<td>yes</td>
</tr>
<tr>
<td>Windows NTLM</td>
<td>hashed</td>
<td>yes</td>
<td>any</td>
<td>?</td>
</tr>
<tr>
<td>Windows Kerberos</td>
<td>encrypted</td>
<td>yes</td>
<td>AD domain</td>
<td>??</td>
</tr>
<tr>
<td>Windows Negotiate</td>
<td>Kerberos or NTLM</td>
<td>yes</td>
<td>any with NTLM AD domain with Kerberos Windows 2000+ with Kerberos</td>
<td>???</td>
</tr>
<tr>
<td>Digest</td>
<td>hashed</td>
<td>no</td>
<td>Windows XP+ Windows 2003 DC</td>
<td>yes</td>
</tr>
<tr>
<td>TLS client certificate</td>
<td>encrypted mutual</td>
<td>yes</td>
<td>any</td>
<td>yes</td>
</tr>
</tbody>
</table>
SSO from IE/Edge/Chrome

- IE, Edge, Chrome respect Windows Internet Settings
  - Local Intranet zone

- http://portal
- *.gopas.virtual

SSO from Firefox (no *.wildcard support)
NTLM loopback check

- Loopback access with NTLM on alias
  - LSASS has the same NTLM token with different server name in cache

- HKLM\System\CCS\Control\LSA\MSV1_0
  - `BackConnectionHostNames` = `MULTI_SZ`

- HKLM\System\CCS\Control\LSA
  - `DisableLoopbackCheck` = DWORD = 1

Kerberos

- AppPool user/comuters account
  - `System, Network Service, AppPoolIdentity`
  - domain `user` account

- servicePrincipalName
  - http/portal
  - http/portal.gopas.virtual

SETSPN -a "http/portal" svc-web
SETSPN -a "http/portal.gopas.virtual" svc-web
Forms authentication

- Plain-text authentication
- Cookies based further access
  - expiration in the browser
  - expiration on the server
  - explicit log-out available
- Customizable user interface
- Implemented in ASP.NET code logic
  - might be exposed in GUI or might not

HTTP cookies

- Name=Value; Name=Value; ...
- Path=/subPath
  - limited to a subpath
- Domain=.gopas.cz
  - can enable cookie from a subdomain to go to other third-level subdomains
- Max-Age=[seconds]
Request blocking

- Windows Firewall
  - source IP addresses
- IP address and domain name restrictions
  - IP address/range/network
  - domain names require DNS PTR reverse lookup
  - Proxy mode on Windows 2012+
- Dynamic IP restrictions
  - logging only mode: sc-status = 200, sc-substatus = 502
- Request filtering (no regex)
  - extensions, size of URL and payload, methods, URL pattern, query string pattern, hidden segment (/segment/ or /file.name exactly), header patterns and patterns by .ext (the Rules)
  - use Hidden segments in collisions like /bin/ and /binary/ to block "bin" sequence

Double escaping and high-bit characters

- URL part only, not considered in query strings
  - only the query and/or fragments

- http://%70 %6F %72 %74 %61 %6C /username.aspx
- http://%25 %37 %30 %25 %36 %46 %25 %37 %32 %25 %37 %34 %25 %36 %31 %25 %36 %43 /username.aspx

- + or % after de-escaping in URL is blocked
Proxy mode with Dynamic IP restrictions

- Requests coming over proxies
- X-Forwarded-For: client, first-proxy, second-proxy, last-proxy
- Must make the proxy addresses trusted as Allowed IP entries
  - source IP address of the TCP connection is the last-proxy
  - client IP from the X-Forwarded-For is untrusted

Proxy mode (static/dynamic IP restrictions)
Proxy mode (static/dynamic IP restrictions)

Client -> Proxy 
Proxy IP 
Web 

Proxy mode (static/dynamic IP restrictions)

Client -> Proxy 
Proxy IP 
Web 

X-Forwarded-For 
Blocked Client IP
Transport Layer Security

- Standard cryptographic protocol for secure transmissions
  - RSA/DSA/EC, RC4, DES, AES, MD5, SHA1, …
- Encryption and server identity authentication
  - HTTPS, SStP, IPHTTPS, LDAPS, SQL, RDPS, SMTPS, Hyper-V replication, 802.1x EAP, IPSec IKEExt
- Client certificate authentication
- Requires public key certificate on the server

SSL vs. TLS vs. DTLS

- SSL 2.0 (1995) - Windows 2000+
  - MITM can downgrade cipher suite to 40-bit
  - MAC hashes can be downgraded to 40-bit
- SSL 3.0 (1996) - Windows 2000+
  - Support for DH, Fortezza key exchanges
  - Support for non RSA certificates
- TLS 1.0 (1999) - Windows 2000+
  - Security same as SSL 3.0
  - Protocol not compatible with SSL 3.0
  - IETF and US FIPS standard
  - More recent standards offering SHA2 and ECDH suites
  - Can fallback to TLS 1.0 without TCP RST
- DTLS 1.0 (based on TLS 1.0) and 1.2 (based on TLS 1.2) - Windows 8/2012
  - Update available for Windows 7/2008 R2 (KB2574819)
  - UDP datagram based communications such as RDP-UDP
Secure / insecure

- Insecure
  - SSL 2.0, SSL 3.0
  - DES, MDx, SHA1, RC4
- Must have for compatibility reasons
  - TLS 1.0
- Good
  - TLS 1.1, TLS 1.2, ...

Current secure algorithms and support

- since Windows 7 and Windows 2008 R2
  - AES, SHA2 (SHA-256, SHA-384, SHA-512), RSA 2048, ECDH
  - TLS 1.1+

- certificates
  - must contain Subject Alternative Name (SAN)
  - all names must be present in SAN
  - public CAs do not issue non-public DNS domains
What we do not want

- SHA-1 (weak at 80/63bit currently)
  - 2017-01-01T00:00:00 Windows stops accepting SHA-1 leaf certificates???
- RC4 (non-FIPS, some limited exploits, rumors, MS not recommended, RFC 7465 prohibited since Feb2015)
- MD5, MD4 (non-FIPS)
- RSA 1024
- SSL 2.0, SSL 3.0 (prone to attacks)

Do not confuse signature with thumbprint
Disable SSL 2.0

- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
  - \PCT 1.0
  - \SSL 2.0
    - \Client
      - Enabled = DWORD = 0
    - \Server
      - Enabled = DWORD = 0
  - \SSL 3.0
    - \Client ...

Enable TLS 1.1 and TLS 1.2

- HKLM\System\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols
  - \TLS 1.1
  - \TLS 1.2
    - \Client
      - Enabled = DWORD = 1
      - DisabledByDefault = DWORD = 0
    - \Server
      - Enabled = DWORD = 1
      - DisabledByDefault = DWORD = 0
Automatic (re)binding

- IIS manual setting
- Windows 2012 R2+ with automatic rebind if enabled

PowerShell (re)binding

```powershell
$servername = 'portal'
dir Cert:\LocalMachine\My | ? { ($_.Issuer -ne $_.Subject) -and ($_.DnsNameList -contains $servername) -and ($_.NotBefore -lt [DateTime]::Now) -and ($_.NotAfter -gt [DateTime]::Now) -and ($_.HasPrivateKey) -and (~not $_.Archived) -and ($_.Extensions["2.5.29.37"]).EnhancedKeyUsages["1.3.6.1.5.5.7.3.1"] -ne $null } | Sort -Desc NotAfter | Select -First 1
```
Change TLS allowed suites and order

Windows XP/2003 - TLS/SSL cipher suites (no AES)

TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_DHE_DSS_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_DHE_DSS_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
TLS_RSA_EXPORT_WITH_NULL_MD5
TLS_RSA_WITH_NULL_SHA

SSL_RSA_WITH_RC4_128_SHA
SSL_RSA_WITH_3DES_EDE_CBC_SHA
SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA
SSL_RSA_WITH_RC4_128_MD5

27.5.2019
Windows 7/2008 R2 TLS v1.1 cipher suites (AES/EC/SHA2)

- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P384
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P384

Validate your TLS server

- http://www.ssllabs.com
SSL enforcement vs. HTTP 403 error

Redirects

- 302 normal redirect
- 301 permanent change
  - browsers can update cache, bookmarks and links
- 307 temporary change
- Always create separate site for the redirects!
- Switch anonymous authentication to use AppPoolIdentity
- NTFS permissions Read for IIS APPPOOL\redirapppool

- Redirecting with including query string
  - https://finance$S$Q + exact destination
Client started HTTP and 302 redirect

Client started HTTP and HTTPS links `<a href>`
MITM attack with HTTPS strip (SSL strip)

Client → HTTP → Attacker → HTTPS → Server

### Strict-Transport-Security (HSTS)

Client

HTTP GET /uri.htm
Host: www.gopas.cz

```
HTTP 200 OK
HTML: ...
Strict-Transport-Security: max-age=3600;
includeSubDomains;
<a href="https://www.gopas.cz/link2.htm">
<img src="https://www.gopas.cz/pic1.png">
```

Cache

HTTP GET link1.htm
Host: www.gopas.cz
More web servers on a common IP address - single host header

Client

TLS tunnel
IP: Port

www.gopas.cz

HTTP GET /uri.htm
User-Agent: Internet Explorer
Accept-Language: cs-cz
Host: www.gopas.cz

Server Certificate: www.gopas.cz
IP: 10.10.0.37:443

WebSite

More web servers on a common IP address - different host headers on Windows 2008 R2

Client

TLS tunnel
IP: Port

HTTP GET /uri.htm
Host: www.gopas.cz

Server Certificate: www.gopas.cz
IP: 10.10.0.37:443

WebSite

HTTP GET /uri.htm
Host: www.sevecek.com

X
Host header vs. wildcard certificate on Windows 2008 R2

Server Name Indication (SNI) with Windows 7 (IE7) and Windows 2012+
Network Load Balancing

- Browser client
- GUI web service client
- Client IP1, Port1
- NLB Ethernet switch
- Web1
- Web2
- Web3
- IP1, IP NLB
- https://www.gopas.cz
- https://bi
- NLB Ethernet switch
- GUI web service client
- Client IP2, Port2
- DB
- \FS content
- \FS config
- State server
- Client IP3
- State server
- IP NLB
- NLB notes #1

**NLB notes #1**

Network Load Balancing Manager

<table>
<thead>
<tr>
<th>Network Load Balancing Clusters</th>
<th>Host configuration information for hosts in cluster <a href="http://www.gopas.cz">www.gopas.cz</a> (10.10.0.201)</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.gopas.cz">www.gopas.cz</a> (10.10.0.201)</td>
<td>Host (Interface) Status Dedicated IP address</td>
</tr>
<tr>
<td>GPS-WFE1(Prague)</td>
<td>Converged 10.10.0.22</td>
</tr>
<tr>
<td>GPS-WFE2(Prague)</td>
<td>Converged 10.10.0.23</td>
</tr>
</tbody>
</table>

**www.gopas.cz(10.10.0.201) Properties**

- Cluster IP configuration:
  - IP address: 10.10.0.201
  - Subnet mask: 255.255.0.0
  - SSL internet name: www.gopas.cz
  - Network address: 0x040c:0a-00:03
- Cluster operation mode: Multicast
NLB notes #2 (dedicated vs. cluster IPs)

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Prague:

  Connection-specific DNS Suffix : 
  Link-local IPv6 Address : fe80::0123:dc0::
  IPv4 Address : 10.10.0.22
  Subnet Mask : 255.255.0.0
  IPv4 Address : 10.10.0.201
  Subnet Mask : 255.255.0.0
  Default Gateway : 10.10.0.1

  IPv4 Address : 10.10.0.23
  Subnet Mask : 255.255.0.0
  IPv4 Address : 10.10.0.201
  Subnet Mask : 255.255.0.0
  Default Gateway : 10.10.0.1

NLB notes #3 (or create a new zone)
NLB notes #4 (on both nodes manually)

```
C:\> notepad c:\Windows\system32\drivers\etc\hosts

hosts · Notepad
File Edit Format View Help

127.0.0.1 www.gopas.cz
```

Testing load balancing

- HTTP response headers (IIS server level)
  - add custom header: NLB-Node: severName

- HTTP response headers (web-site level)
  - temporarily disable Connection keep-alive
Testing load-balancing with PowerShell
Invoke-WebRequest

Central shared IIS configuration

- Manual config
  - windows features
    - Add-WindowsFeature ...
  - group managed service accounts registration
    - Install-AdServiceAccount ...
  - SSL certificates
    - netsh http show sslcert
    - Netsh http add sslcert

- What does not work
  - additional HTTP headers per server
PHP integration

- install PHP
  - download PHP
  - download VC 201x redistributable
- Add-WindowsFeatures Web-CGI
- register Handle Mapping per site
  - *.php -> PHP-CGI.exe
- allow the PHP-CGI.exe in server CGI restrictions
## PHP integration

### ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

<table>
<thead>
<tr>
<th>Description</th>
<th>Restriction</th>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Server Pages</td>
<td>Allowed</td>
<td>%windir%\system32\netsrv\asp.dll</td>
</tr>
<tr>
<td>ASP.NET v2.0.50727</td>
<td>Allowed</td>
<td>%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll</td>
</tr>
<tr>
<td>ASP.NET v2.0.50727</td>
<td>Allowed</td>
<td>%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll</td>
</tr>
<tr>
<td>ASP.NET v4.0.30319</td>
<td>Allowed</td>
<td>%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll</td>
</tr>
<tr>
<td>ASP.NET v4.0.30319</td>
<td>Allowed</td>
<td>%windir%\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll</td>
</tr>
<tr>
<td>PHP engine server enabled</td>
<td>Allowed</td>
<td>C:\PHP\php-cgi.exe</td>
</tr>
</tbody>
</table>