

Wprowadzenie do IIS

- Czym jest IIS. Internet Information Services to wydajny serwer sieci Web, jak również hosting aplikacji i usług. Obejmuje aplikacje napisane w różnych technologiach, takich jak ASP.NET, PHP, Python, Node.js itp.
- IIS wyróżnia się budową modułową, serwer Web składa się z około 40 składników (IIS7), dzięki czemu administrator może wybrać tylko te, które są wymagane. Sprzyja to również zmniejszeniu liczby ataków.
- W Windows Server 2016, IIS jest w wersji 10.0.14393.0, w Windows Server 2019 - w wersji 10.0.17763.0, a w Windows Server 2022 - w wersji 10.0.20348.0. Wszystkie te wersje IIS posiadają Internet Information Services (IIS) Manager, osobną konsolę MMC dla konfiguracji serwera sieci Web firmy Microsoft.

Architektura

- Internet Information Services (IIS) 7.0 zapewnia architekturę przetwarzania żądań, m.in.:
 - usługa, Windows Process Activation Service (WAS), która umożliwia używania protokołów innych niż HTTP i HTTPS dla stron Przykładowe protokoły
 - WAS umożliwia hostowanie aplikacji, które komunikują się poprzez protokół TCP/IP.
 - Protokół Named Pipes może być wykorzystywany przez aplikacje w celu komunikacji międzyprocesowej na jednym komputerze lub między komputerami w sieci lokalnej.
 - Usługa Message Queuing umożliwia komunikację między aplikacjami, które działają w różnych czasach lub w różnych systemach komputerowych.
 - Silnik, który umożliwia dodawanie i usuwanie wybranych modułów
 - Komponenty: listeners - HTTP.sys, usługi - World Wide Web Publishing Service (WWW service) i Windows Process Activation Service (WAS)

Detektory protokołów (Protocol Listeners)

- Detektory protokołów (Protocol Listeners) odbierają specyficzne żądania, wysyłają je do IIS w celu przetworzenia i zwracają odpowiedź do żądającego. Przykładowo jeżeli przeglądarka klienta wysłała żądanie otwarcia strony WWW, HTTP listener, HTTP.sys odbiera żądanie i wysyła je do IIS. IIS przetwarza żądanie i wysyła odpowiedź do klienta.
- W standardzie HTTP.sys wspiera protokoły HTTP i HTTPS.
- Żeby wspierać usługi i aplikacje, które używają protokołów innych niż HTTP i HTTPS, możemy użyć technologii Windows Communication Foundation (WCF). WCF posiada listener adapters, które zapewniają odpowiednie funkcjonalności dla obsługi innych protokołów. Więcej informacji o WCF na - [Windows Communication Foundation](#).

Hypertext Transfer Protocol Stack (HTTP.sys)

- HTTP „nasłuchiwanie” są częścią podsystemu sieciowego, który jest zaimplementowany jako sterowniki urządzeń na poziomie jądra w systemach operacyjnych i nazywa się to HTTP protocol stack (HTTP.sys). HTTP.sys nasłuchuje żądań HTTP requests z sieci, wysyła do IIS w celu przetworzenia i wysyła odpowiedź zwrotną.
- W IIS 6.0, HTTP.sys był zastąpiony Windows Sockets API (Winsock), który był komponentem na poziomie użytkownika.

HTTP.sys zapewnia następujące korzyści:

- Buforowanie w trybie jądra. Żądania odpowiedzi z pamięci podręcznej są obsługiwane bez przełączania do trybu użytkownika.
- Kolejowanie żądań w trybie jądra. Żądania powodują mniejsze obciążenie związane z przełączaniem kontekstu, ponieważ jądro przekazuje żądania bezpośrednio do poprawnego procesu roboczego. Jeśli żaden proces roboczy nie jest dostępny do przyjęcia żądania, kolejka żądań trybu jądra wstrzymuje żądanie, dopóki proces roboczy go nie odbierze.
- Wstępne przetwarzanie i filtrowanie zabezpieczeń.

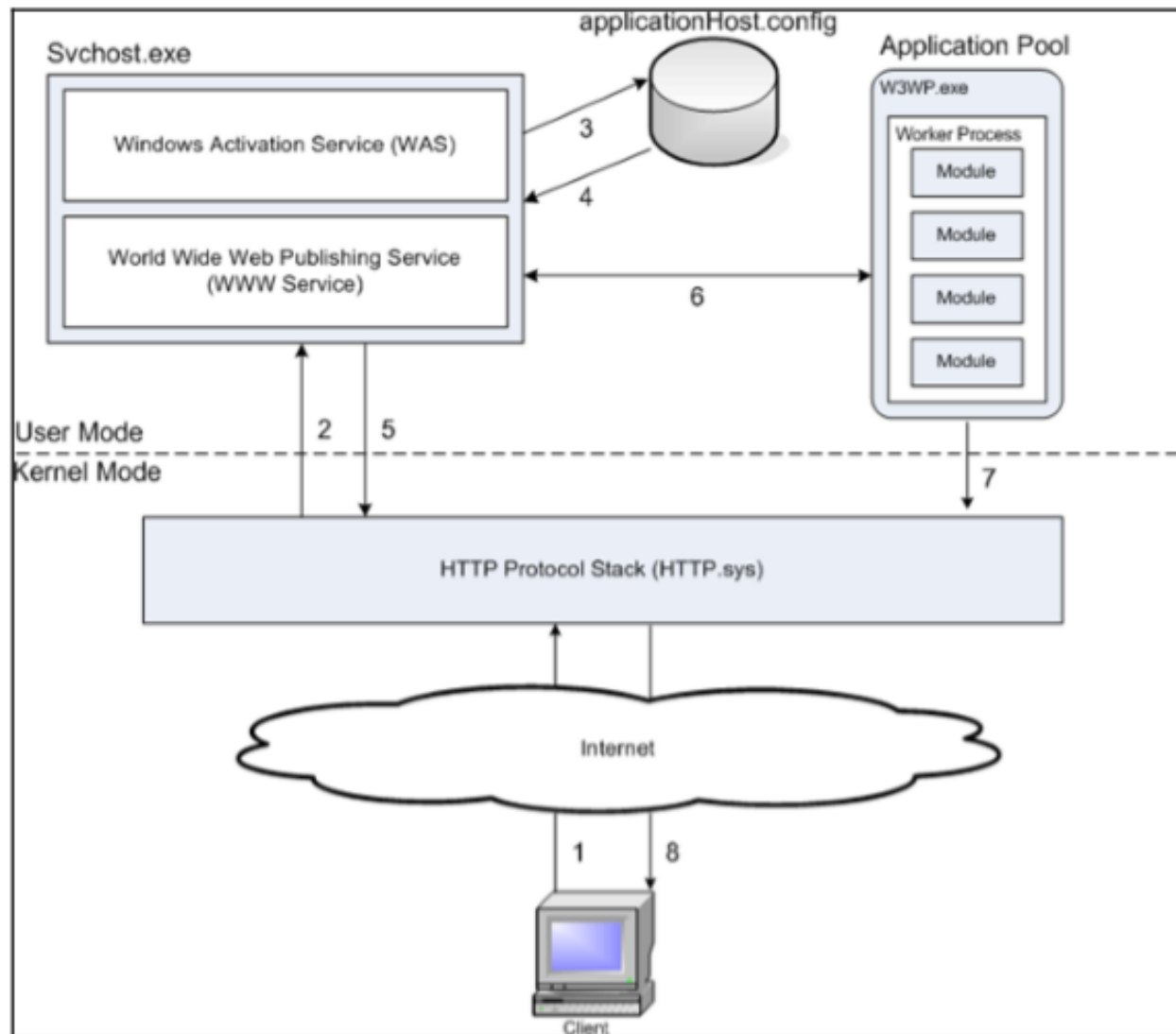
Windows Process Activation Service (WAS)

- Jest odpowiedzialny za zarządzanie procesami aplikacji internetowych, które są hostowane na serwerze.
- Używa tej samej konfiguracji i modelu przetwarzania jak dla HTTP
- WAS obsługuje uruchamianie, zatrzymywanie, monitorowanie oraz ponowne uruchamianie procesów aplikacji w zależności od zapotrzebowania.
- Usługa ta jest integralną częścią infrastruktury IIS, zapewniając elastyczność i skalowalność w obsłudze różnych aplikacji internetowych.
- Opcjonalnie można uruchomić WAS bez startowania WWW Service jeśli nie jest potrzebna funkcjonalność HTTP.
- Aby uzyskać informacje o adapterach nasłuchiwania WCF i hostowaniu aplikacji WCF w IIS za pomocą WAS, zobacz [Hosting in WCF](#).

World Wide Web Publishing Service (WWW service)

- Usługa World Wide Web Publishing Service, znana również jako WWW service, jest główną usługą zarządzającą serwerem WWW działającym na systemie Windows.
- WWW service zarządza cyklem życia serwera WWW, w tym uruchamianiem, zatrzymywaniem i zarządzaniem witrynami internetowymi hostowanymi na serwerze.
- WWW Service jest odpowiedzialny za konfigurację HTTP.sys, update HTTP.sys przy zmianach w konfiguracji, i informowanie WAS kiedy pojawi się żądanie w kolejce.
- WWW Service zbiera informacje do liczników.
- Nie uległo to zmianie w późniejszych wersjach IIS, w tym w Windows Server 2016, 2019 i 2022.

Integracja IIS 10.0 z Windows Server 2016



Przetwarzanie żądań HTTP w IIS7

1. Gdy przeglądarka klienta inicjuje żądanie HTTP dotyczące zasobu na serwerze sieciowym, HTTP.sys przechwytuje żądanie.
2. HTTP.sys kontaktuje się z WAS w celu uzyskania informacji ze sklepu konfiguracji.
3. WAS żąda informacji o konfiguracji ze składnicy konfiguracji applicationHost.config.
4. Usługa WWW otrzymuje informacje o konfiguracji, takie jak pula aplikacji i konfiguracja witryny.
5. Usługa WWW używa informacji konfiguracyjnych do skonfigurowania HTTP.sys.
6. WAS uruchamia proces roboczy dla puli aplikacji, do której wysłano żądanie.
7. Proces roboczy przetwarza żądanie i zwraca odpowiedź do HTTP.sys.
8. Klient otrzymuje odpowiedź.

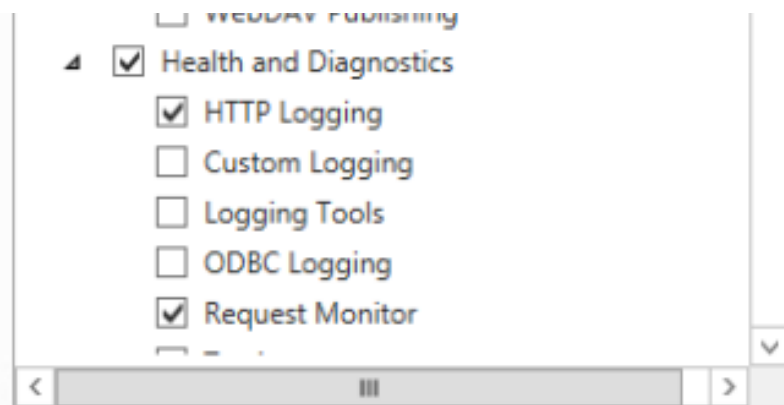
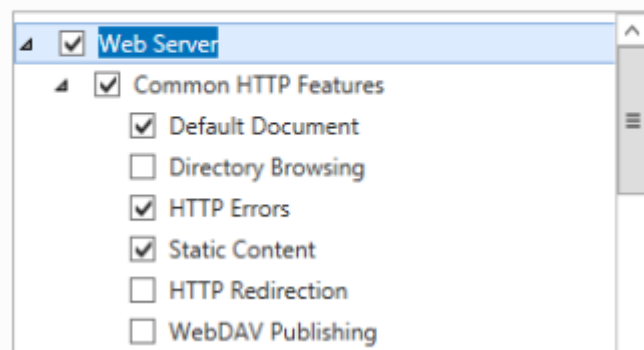
IIS7 - 10 jako serwer stron WWW

Instalacja

- Server Manager, gdzie wybrać należy „Add Roles” i następnie zaznaczyć właściwe składniki.
- Zaznaczając rolę IIS, użytkownik musi wyrazić zgodę na doinstalowanie opcji związanych z Windows Process Activation Service. Są one niezbędne do działania IIS.
- Następnym krokiem instalacji jest wybór składników, spośród kilkudziesięciu IIS7, które faktycznie mają być zainstalowane. Można zainstalować wszystkie, jeżeli ktoś chce eksperymentować.

Select the role services to install for Web Server (IIS)

Role services



IIS7 - 10 jako serwer stron WWW

Instalacja w cmd

- Wpisz cmd w pasku wyszukiwania, a najwyższym wynikiem powinien być wiersz polecenia.
- Kliknij Uruchom jako administrator.
- Wpisz polecenie

`DISM /online /enable-feature /featureName:IIS-DefaultDocument /All`
i naciśnij Enter.

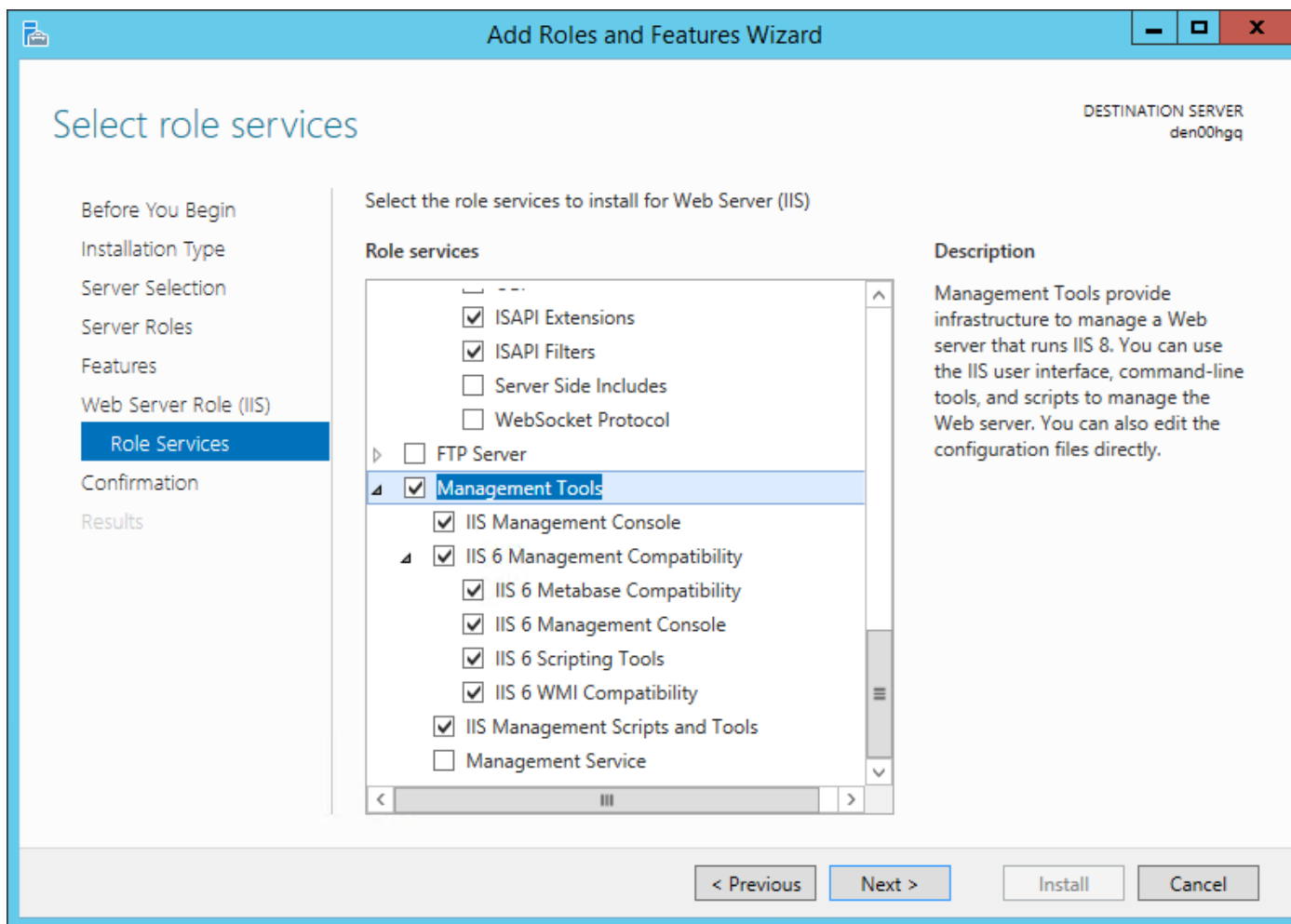
Instalacja w PowerShell

- Wpisz polecenie cmdlet

`Enable-WindowsOptionalFeature -Online -FeatureName IIS-WebServerRole -NoRestart`
i uruchom je.

Zobaczysz początek paska postępu.

Po zakończeniu sprawdź, czy usługi IIS są zainstalowane i działają.



1. Web Server

Główna funkcjonalność serwera internetowego, zaznaczana automatycznie. Wszystkie serwerowe opcje są elementami tego głównego węzła.

2. Typowe funkcje protokołu HTTP (Common HTTP Features)

Zaznaczana automatycznie funkcjonalność serwera jest związana ze statycznymi stronami.

- **Static Content (Zawartość statyczna)**. Włączyć. Opcja pozwalająca na publikowanie stron. Z punktu kogoś, kto chciałby opublikować swoje strony, jest to opcja najważniejsza. Teoretycznie wystarczyłaby tylko ona, ale tak skonfigurowany serwer byłby bardzo nieciekawym.
- **Default Document (Dokument domyślny)**. Włączyć. Opcja pozwala na podanie strony html w sytuacji, kiedy użytkownik wpisze w przeglądarce tylko adres serwera. Przykładowo, pełny adres strony Microsoft to <http://www.microsoft.com/en/us/default.aspx>. Nikt jednak tak nie pisze, zamiast tego podając w przeglądarce tylko <http://www.microsoft.com/>. Aby serwer wiedział, którą stronę podać, jak użytkownik o żadną nie zapyta – należy zaznaczyć tę opcję.

- **Directory Browsing (Przeglądanie katalogów).** Włączyć, jeżeli tylko może się przydać. Opcja pozwala na przeglądanie plików w katalogu. Zamiast ładnej strony wyświetlana jest lista plików, a kliknięcie na jakiś plik, otwiera go już w jego właściwej postaci. Należy pamiętać, że opcję tę można później włączać i wyłączać dla każdego katalogu oddzielnie, co zostanie omówione w dalszej części artykułu. Zazwyczaj przyjmuje się, że inne niż celowe i przemyślane pokazanie komuś zawartości katalogu jest istotnym naruszeniem powszechnie przyjętych standardów bezpieczeństwa serwera WWW.
- **HTTP Errors (Błędy HTTP).** Włączyć. Opcja pozwala na wysyłanie do klienta własnych komunikatów błędu, jeżeli z jakiegoś powodu błąd się pojawi. Typową sytuacją (i komunikatem) błędu jest odwołanie do nieistniejącej strony.
- **HTTP Redirection (Przekierowanie HTTP).** Włączyć. Opcja pozwala na przekierowanie klienta w inne miejsce, w praktycznie niezauważalny dla niego sposób. Może to być bardzo użyteczne na przykład przy zmianach w strukturze stron.
- **Application Development (Tworzenie aplikacji).** Zaznaczana automatycznie. Zestaw opcji wspierających aplikacje internetowe.

- **ASP.** Włączyć lub wyłączyć w zależności od sytuacji. ASP jest standardem skryptów uruchamianych po stronie serwera IIS. Formalnie nie jest to statyczna strona WWW, więc wypadałoby wyłączyć. Praktyka pokazuje jednak, że nawet statyczne strony na tyle często mają format ASP, że wyłączenie może uniemożliwić ich publikację.
- **CGI.** Wyłączyć. Stary, ale stale żywy sposób zapewniania dynamicznej treści stron internetowych. Kompletne zapytanie od klienta przekazywane jest jako parametr podawany przy uruchomieniu zapisanego na dysku pliku *.EXE. Wynik działania programu *.EXE odsyłany jest jako odpowiedź dla klienta. Każde otwarcie strony to uruchomienie aplikacji, na czym cierpi wydajność. Z drugiej strony, prostota mechanizmu sprawia, że aplikacje CGI są nadal tworzone w dziesiątkach różnych języków programowania.
- **ISAPI Extensions (Rozszerzenia ISAPI).** Wyłączyć. Bardzo wydajny mechanizm tworzenia dynamicznych stron. Cały kod generujący stronę zapisany jest w podłączonej do IIS bibliotece DLL. Efektem jest bardzo szybka praca, jednak strony tak tworzone zazwyczaj bardzo ciężko się rozwija, utrzymuje i aktualizuje.

- **ISAPI Filters (Filtry ISAPI).** Wyłączyć. ISAPI Filters są rozszerzeniami serwera IIS pozwalającymi na obsługę przychodzących zgłoszeń nim trafią one do właściwego serwera. temu, można na przykład stworzyć bibliotekę, która zablokuje wszystkie żądania niezgodne z RFC.
- **Server Side Includes (Włączanie Strony Serwera).** Wyłączyć. Stara i prosta metoda tworzenia zawartości stron, poprzez łączenie zawartości różnych plików. Przykładowo, dla każdej wyświetlanej strony jej stopka jest pobierana z pliku stopka.txt i dopiero wtedy całość jest wysyłana do klienta jako jeden spójny kod HTML.
- **ASP.NET.** Wyłączyć. Bardzo cenna opcja pozwalająca na uruchamianie najnowocześniejszych aplikacji internetowych.
- **NET Extensibility (rozszerzalność .NET).** Wyłączyć. Pozwala na rozszerzanie funkcjonalności IIS7.

3. Monitorowania stanu serwera (Health and Diagnostics)

- Zaznaczana automatycznie. Zestaw opcji służących do monitorowania stanu serwera.
- **HTTP Logging (Rejestrowanie zdarzeń)**. Włączyć. Opcja pozwala na zapisywanie na dysku plików z informacjami o odwołaniach do stron. Pliki takie umożliwiają później analizę odwiedzin i śledzenie błędów.
- **Logging Tools (Narzędzia Logowania)**. Włączyć. Są to dodatkowe narzędzia pozwalające na zarządzanie logami systemowymi.
- **Request Monitor (Monitorowanie żądań)**. Wyłączyć. Opcja pozwalająca na śledzenie zapytań, co w praktyce, dla statycznych stron jest zbędne.
- **Tracing (Monitorowanie)**. Wyłączyć. Opcja pozwala śledzić zapytania. Co w praktyce dla statycznych stron jest zbędne.
- **Custom Logging (Niestandardowe logowanie)**. Wyłączyć. Opcja pozwala na tworzenie własnych metod logowania zapytań. Wymaga niemałych umiejętności i nie wnosi nic cennego w przypadku statycznych stron.
- **ODBC Logging (Logowanie ODBC)**. Wyłączyć, chyba że włączenie jest uzasadnione. Opcja pozwala na zapisywanie informacji o zapytaniach do bazy danych zamiast do plików. Dane takie są łatwiejsze do późniejszej analizy dzięki mechanizmom SQL.

4. Bezpieczeństwo (Security)

Zaznaczane automatycznie. Zestaw opcji pozwalających na dostosowanie metod, którymi klient może potwierdzić swoją tożsamość.

- **Basic Authentication (Podstawowe uwierzytelnianie).** Raczej wyłączyć. Włączyć, jeżeli do części stron dostęp mają mieć tylko wybrani użytkownicy a inne metody nie działają. Ta metoda autentykacji jest dostępna w każdej przeglądarce, jednak jej wadą jest stosunkowo prosta możliwość podsłuchania haseł.
- **Windows Authentication (Uwierzytelnianie Windows).** Raczej wyłączyć. Włączyć, jeżeli do części stron dostęp mają mieć tylko wybrani użytkownicy z lokalnej sieci LAN. Metoda autentykacji opiera się na uwierzytelnianiu systemu. Dzięki temu, użytkownik zalogowany do domeny automatycznie może się przedstawić serwerowi.
- **Digest Authentication (Uwierzytelnianie skrótu).** Włączyć, chyba że wszystkie strony na serwerze WWW przeznaczone są dla całego świata. Jeżeli jest konieczne uwierzytelnianie użytkowników, to opcja wydaje się najbezpieczniejsza.
- **Client Certificate Mapping Authentication (Autentykacja mapowania certyfikatu klienta).** Wyłączyć dopóki się nie zrozumie, jak to działa. Bardzo bezpieczny sposób uwierzytelniania, jednak jego złożoność sprawia, że włączać tę opcję powinni tylko doświadczeni administratorzy, znający już dobrze serwer IIS.

4. Bezpieczeństwo (Security)

- **IIS Client Certificate Mapping Authentication (Autentykacja mapowania certyfikatów klienta w usłudze IIS)**. Wyłączyć dopóki się nie zrozumie, jak to działa. Bardzo bezpieczny sposób uwierzytelniania, jednak jego złożoność sprawia, że włączać tę opcję powinni tylko doświadczeni administratorzy, znający już dobrze serwer IIS.
- **URL Authorization (Autoryzacja URL)**. Raczej wyłączyć, chyba że strony WWW mają złożony schemat uprawnień określających dopuszczonych użytkowników. Opcja pozwala na powiązanie uprawnień do stron z grupami do których należy użytkownik. Dzięki tej funkcji można określać, które adresy URL są dostępne publicznie, a które wymagają autoryzacji. Jest to istotne narzędzie w zarządzaniu bezpieczeństwem i dostępem do zasobów hostowanych na serwerze WWW.
- **Request Filtering (Filtrowanie żądań)**. Włączyć. Opcja ta podłącza do IIS filtry, które są w stanie zapobiec wielu typowym atakom. Dzięki tej funkcji można definiować reguły filtrowania, które określają, które żądania są dozwolone, a które są blokowane na podstawie różnych kryteriów, takich jak typy plików, rozszerzenia, metody HTTP, ciągi zapytań i inne.
- **IP and Domain Restrictions (Ograniczenia IP i domen)**. Włączyć. Dzięki tej opcji można zarządzać uprawnieniami poprzez określenie, które adresy IP mają zakaz (lub pozwolenie) dostępu do stron.

5. Wydajność (Performance)

Zaznaczane automatycznie. Zestaw dwóch opcji związanych z kompresją przesyłanych danych.

- **Static Content Compression (Kompresja treści statycznych).** Włączyć.
Opcja powoduje, że odwiedzana strona jest kompresowana, zapisywana w skompresowanej postaci i od tej pory w takiej właśnie postaci wysyłana do klienta. Dzięki temu, znacząco zmniejsza się obciążenie łącza.
- **Dynamic Content Compression (Kompresja treści dynamicznych).** Wyłączyć.
Analogiczna jak dla Static Content Compression możliwość kompresji stron, jednak dla zawartości dynamicznej. Zastosowanie tej opcji powoduje, że każda odwiedzana strona, za każdym razem jest kompresowana przed wysłaniem do klienta, co znacząco obciąża procesor. Jest to funkcja, która umożliwia kompresowanie treści generowanych dynamicznie przez serwer WWW działający na IIS, takich jak strony internetowe generowane przez aplikacje internetowe, pliki ASP.NET, PHP, i inne. Kompresja treści dynamicznych pomaga zmniejszyć rozmiar danych przesyłanych przez sieć, co przyspiesza czas ładowania stron internetowych i zmniejsza zużycie przepustowości sieciowej.

6. Narzędzia zarządzania (Management Tools).

Zaznaczane automatycznie. Zestaw opcji związanych z narzędziami administracyjnymi IIS.

- **IIS Management Console (Konsola zarządzania IIS).** Włączyć. Opcja odpowiada za instalacji konsoli zarządzającej serwerem IIS. Za pomocą konsoli zarządzania IIS można tworzyć witryny internetowe, konfigurować ustawienia serwera, zarządzać aplikacjami internetowymi, przeglądać dzienniki zdarzeń i wiele innych.
- **IIS Management Script and Tools (Skrypty i narzędzia zarządzania IIS).** Włączyć. Narzędzia administracyjne obsługiwane z linii poleceń. Nawet, jeżeli nie są potrzebne od razu, to nigdy nie wiadomo, kiedy mogą się przydać.
- **Management Service (Usługa Zarządzania).** Wyłączyć. Włączyć tylko w sytuacji, gdy serwerem administruje równocześnie wiele osób, każda odpowiadająca tylko za swój serwer wirtualny. Usługa Zarządzania (Management Service) w IIS umożliwia zdalne zarządzanie serwerem WWW działającym na IIS za pomocą narzędzi administracyjnych, takich jak Internet Information Services (IIS) Manager, Web Deploy, PowerShell itp. Ta usługa pozwala administratorom na zdalny dostęp do konfiguracji i zarządzania serwerem WWW bez konieczności bezpośredniego dostępu do maszyny, na której jest uruchomiony serwer WWW.

7. Zgodność IIS6 (IIS6 Management Compatibility).

Zaznaczane automatycznie. Opcje wykorzystujące mechanizmy z poprzedniej wersji serwera IIS.

- **IIS6 Metabase Compatibility (Zgodność z metabazą IIS6).** Wyłączyć.
Zgodność z metabazą IIS6 nie powinna być używana bez wyraźnej potrzeby.
- **IIS6 WMI Compatibility (Zgodność z WMI IIS6).** Wyłączyć.
Zgodność z interfejsami WMI dla IIS6 nie powinna być używana bez wyraźnej potrzeby.
- **IIS6 Scripting Tools (Narzędzia skryptowe IIS6).** Wyłączyć.
Narzędzia do zarządzania IIS przez wiersz poleceń zostały zastąpione nowymi aplikacjami.
- **IIS6 Managment Console (Konsola zarządzania IIS 6.0).** Wyłączyć.
Konsola zarządzająca z poprzedniej wersji serwera. Użyteczna wyłącznie dla SMTP i FTP.

8. Usługa publikowania FTP (FTP Publishing Service).

Zaznaczane automatycznie. Dwie opcje pozwalające na uruchomienie i zarządzanie serwerem FTP

- **FTP Server (Serwer FTP).** Wyłączyć. Serwer dołączony do wersji RC1 nie zachęca do użycia. Ponadto, funkcjonalność FTP osiągnana jest innymi, wydajniejszymi i bezpieczniejszymi mechanizmami.
- **FTP Management konsole (Konsola zarządzania FTP).** Wyłączyć. Konsola zarządzająca FTP nie jest potrzebna jeżeli nie został zainstalowany serwer FTP.

Po ostatecznym potwierdzeniu, system wykona instalację wybranych opcji potwierdzając zakończenie komunikatem „Installation succeeded”

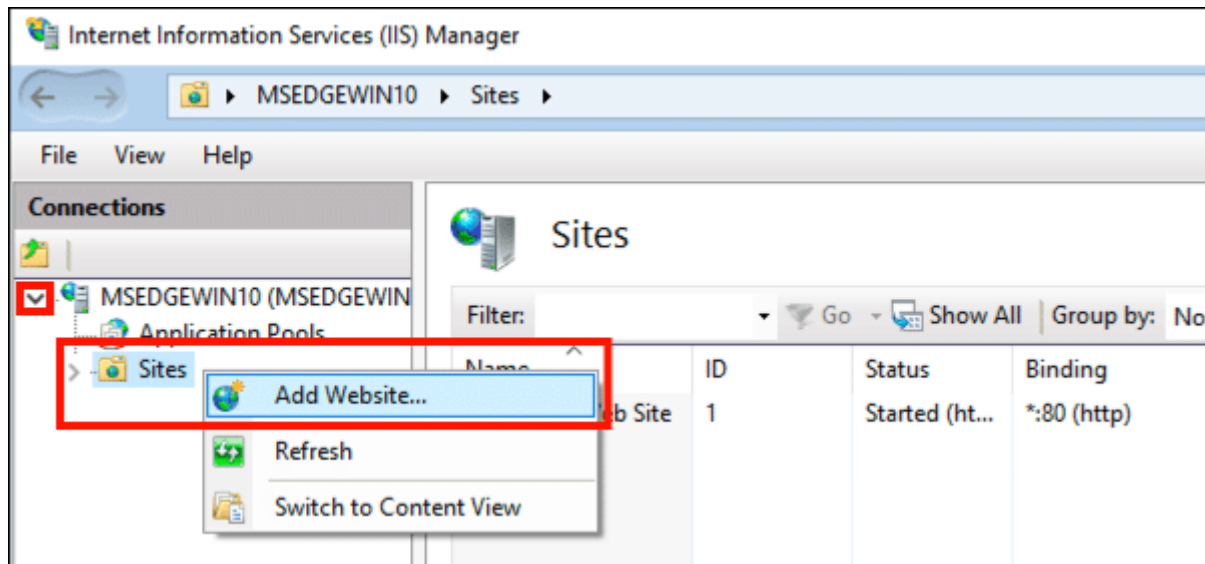
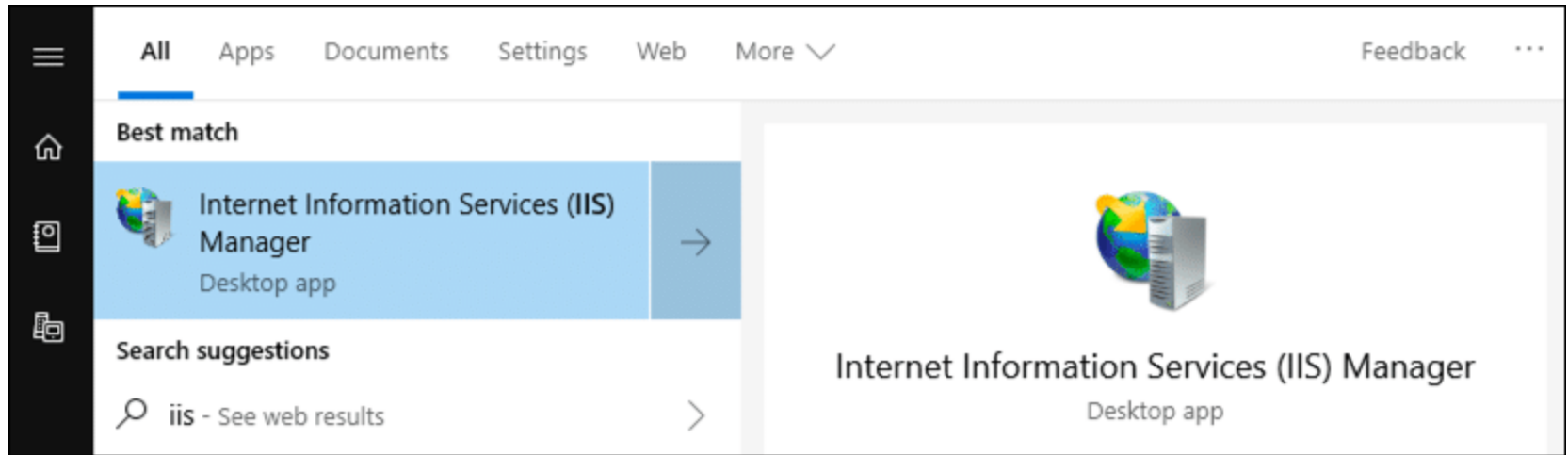
Konfiguracja IIS7 - 10

- Po zakończeniu instalacji, na pierwszy rzut oka nic nowego się nie pojawia. Jeżeli jednak sprawdzi się otwarte porty TCP/IP od razu widać, że serwer już działa.

```
C:\Users\Administrator>netstat -an | findstr /i ":80 "  
TCP      0.0.0.0:80      0.0.0.0:*      LISTENING  
TCP      [::]:80        [::]:*        LISTENING
```

- Jak widać, serwer nasłuchuje na porcie 80 nie tylko na wszystkich adresach IPv4 (0.0.0.0), ale i na adresach IPv6 ([::]).

IIS Manager



Konfiguracja IIS7 - 10

W menu Start znajdują się narzędzia administracyjne, wybrane podczas instalacji.

Podstawowym narzędziem jest Internet Information Server (IIS) Manager.

Po uruchomieniu z lewej strony konsoli wyświetlana jest struktura w postaci drzewa. Wybierając elementy drzewa, zarządzać można różnymi funkcjonalnościami serwera.

Aby zainstalować IIS Manager, należy włączyć opcję Konsola zarządzania IIS podczas instalacji.

W przypadku Windows Server 2016, 2019 i 2022 nie ma znaczących różnic w funkcjonalności IIS Managera.

IIS Manager to podstawowe narzędzie do zarządzania serwerem IIS.

Za pomocą IIS Managera można wykonywać następujące czynności:

1. Zarządzać witrynami i aplikacjami internetowymi.
2. Konfigurować ustawienia serwera, takie jak adresy IP, porty, protokoły, certyfikaty SSL, itp.
3. Zarządzać aplikacjami internetowymi, takimi jak ASP.NET, PHP, itp.
4. Zarządzać usługami internetowymi, takimi jak FTP, SMTP, itp.
5. Monitorować wydajność serwera i aplikacji internetowych.
6. Zarządzać użytkownikami i rolami.
7. Tworzyć i zarządzać kopiami zapasowymi i przywracaniem.
8. Zarządzać zgodnością z poprzednimi wersjami serwera IIS.

Najlepsze praktyki dla IIS (Best Practices)

- Należy skonfigurować opcje dostępne z poziomu serwera, a dopiero później dostępne z poziomu witryny. Dzięki takiemu podejściu każda nowa witryna odziedziczy ustawienia i już w chwili utworzenia będzie poprawnie skonfigurowana i gotowa do pracy.
- Sprawdzającym się w praktyce podejściem jest ustawienie właściwości na poziomie całego serwera na poziom maksymalnie bezpieczny. Jeśli gdzieś taki poziom przeszkadza w funkcjonowaniu serwisów WWW, można go rozluźnić dla danego serwisu. Pozwala to na stworzenie nowego serwisu, który wymaga rozluźnienia uprawnień na tyle, żeby działał poprawnie, co jest stosunkowo łatwo sprawdzić. W przeciwnym razie każdy serwis działałby poprawnie, ale wymagałby każdorazowo sprawdzenia zabezpieczeń.

Poziom serwera

Z poziomu zarządzania całym serwerem, użytkownik ma do dyspozycji opcje start, stop oraz restart. Uruchamiają one i zatrzymują cały serwer HTTP. Oczywiście jest, że zatrzymany serwer nie udostępnia w sieci stron WWW.

Uwierzytelnianie (Authentication)

Opcje dostępne w tym widoku zależą bezpośrednio od wybranych w czasie instalacji metod uwierzytelniania. Oprócz sugerowanej metody „Digest”, pojawia się metoda „Anonymous Authentication”.

- W przypadku metody „Digest” dostępne jest okno konfiguracyjne, w którym można zmienić parametr Realm. Wartość tego parametru wyświetlana jest użytkownikowi razem z pytaniem o hasło i zawierać powinna jakiś czytelny opis serwera lub strony.
- W przypadku metody „Anonymous”, najważniejszym parametrem jest nazwa konta, którym IIS się posługuje, odczytując strony z dysku. Domyślnie, wartość parametru jest równa IUSR i to ta grupa musi mieć prawa odczytu do katalogów, w których znajdują się pliki html.

Kompresja (Compression)

Kompresja zawartości statycznej ma na celu „spakowanie” zawartości stron i wysyłanie jej w takiej postaci do klienta. Aby nie przeprowadzać kompresji przy każdym żądaniu, dane kompresowane są raz i zapisywane na dysku.

Ustawiając parametry kompresji, Administrator ma do możliwość zdefiniowania:

- Włączenia lub wyłączenia kompresji;
- Minimalnego rozmiaru pliku, który jest poddawany kompresji. Pliki bardzo małe nie zyskują na kompresji na tyle dużo, żeby operacja taka była opłacalna;
- Katalogu, w którym przechowywane są skompresowane dane;
- Limitu objętości skompresowanych danych na dysku. Limit ustawiany jest per pula aplikacji, ale dla typowego serwera statycznych stron każdy site ma jedną swoją pulę.

Domyślny dokument (Default Document)

Ponieważ użytkownik woli wpisywać w przeglądarce adres serwera zamiast pełnej ścieżki do dokumentu, serwer musi wiedzieć, jaką stronę ma wysłać do przeglądarki w sytuacji, kiedy użytkownik nie poprosi o żadną konkretną.

Dane domyślnej strony ustawiane są właśnie w sekcji „Default Document”.

- Dla każdego wirtualnego katalogu (o czym dalej) możliwe jest zdefiniowanie listy domyślnych dokumentów. Lista ta przetwarzana jest od pierwszej do ostatniej pozycji. Jeżeli dokument wymieniony na liście istnieje na serwerze - jest wysyłany do klienta. Jeżeli nie istnieje - przetwarzany jest kolejny wpis na liście. Jeżeli wpis nie został znaleziony, sprawdzane jest zezwolenie na przeglądanie katalogu, a jeżeli przeglądanie również nie jest możliwe - wysyłany jest kod błędu mówiący, że tego katalogu nie wolno przeglądać.
- Poprzez interfejs IIS Manager możliwa jest zmiana kolejności dokumentów domyślnych, ich dodawanie i usuwanie. Dostępna w sekcji „Actions” opcja **Disable** w ogóle wyłącza funkcjonalność domyślnego dokumentu dla danego katalogu wirtualnego.
- W praktyce bardzo rzadko zdarza się, żeby właściciel stron WWW nie chciał publikować domyślnego dokumentu. Ponieważ przyjęte standardy określają kilka zwyczajowo stosowanych nazw, najlepszym rozwiązaniem wydaje się umieszczenie całej listy typowych nazw dokumentów, co w IIS jest ustawione domyślnie. W takiej sytuacji, każdy katalog ma szansę wyświetlać poprawnie swój domyślny dokument.

Przeglądanie katalogów (Directory Browsing)

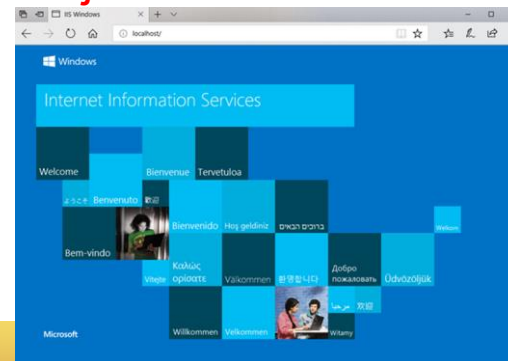
Opcja Directory Browsing odpowiada za uprawnienia do przeglądania katalogów serwera. Może zdarzyć się, że działanie takie będzie potrzebne. Należy jednak przyjąć, że jest to sytuacja wyjątkowa. Dlatego na poziomie serwera należy wyłączyć przeglądanie katalogów i lokalnie, w konkretnych katalogach włączać tylko wtedy, kiedy jest to potrzebne. Włączenie tej opcji sprawia, że użytkownik serwera widzi znajdujące się na nim pliki zamiast stron internetowych.

- Serwer IIS najpierw sprawdza obecność domyślnego dokumentu i dopiero kiedy go nie znajdzie, pozwala na przeglądanie katalogu. W opcjach IIS Manager dotyczących przeglądania katalogów określić można, które z widocznych na rysunku parametrów pliku (data, czas, rozmiar i rozszerzenie) są wyświetlane.

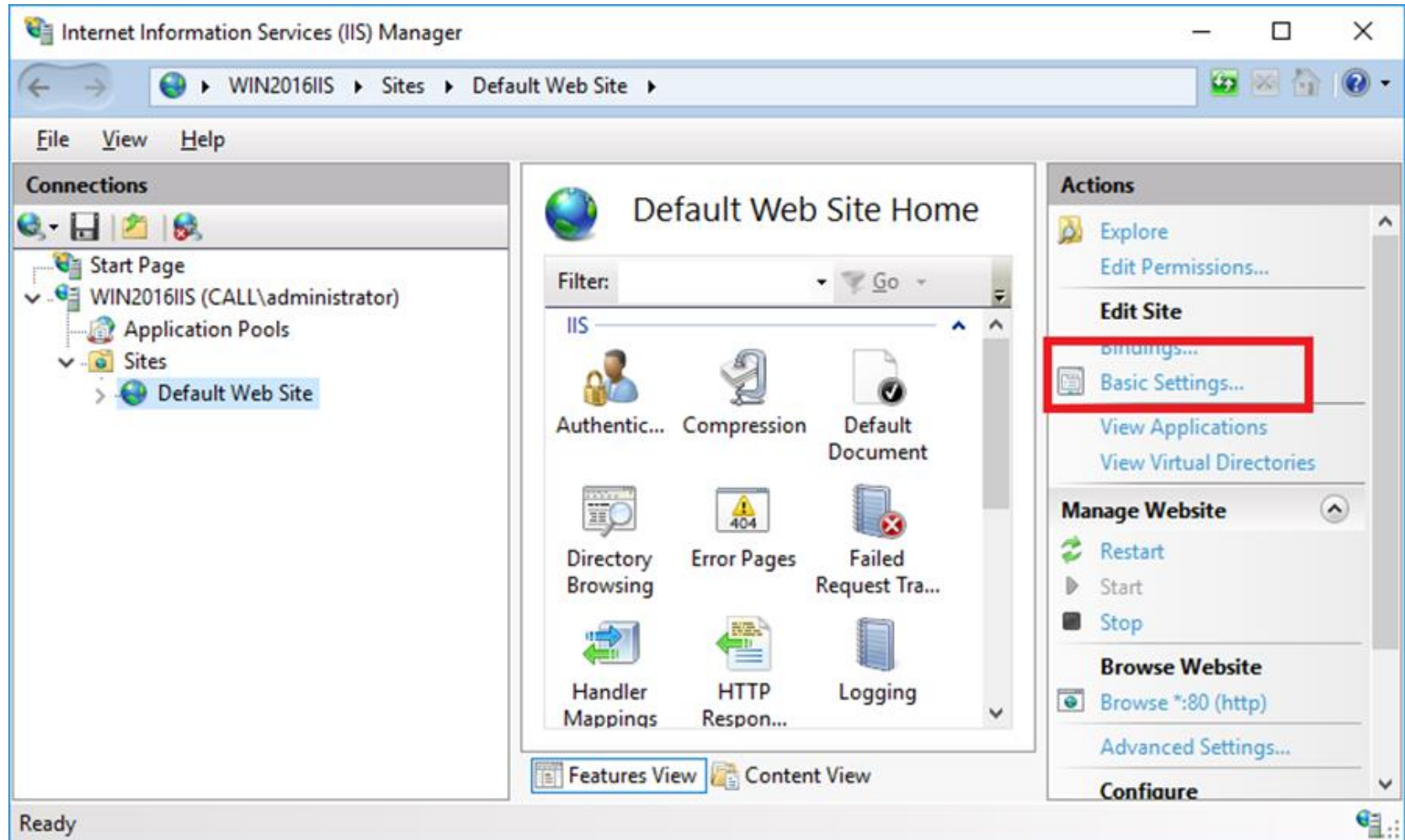
Należy pamiętać, że nieuzasadnione wyświetlanie katalogów serwera uznawane jest za poważne naruszenie reguł bezpiecznej konfiguracji.

Index of /

	Name	Last modified	Size	Description
	signup.php	2015-01-04 12:51	760	
	test.html	2015-01-04 13:24	843	
	test.php	2015-01-04 13:05	166	



Directory Browsing



Strony błędów (Error Pages)

Protokół HTTP określa, że dla każdego zapytania od klienta, w odpowiedzi zwracanej z serwera powinien się znaleźć kod liczbowy mówiący, jakiego rodzaju jest to odpowiedź. W normalnych warunkach kod ten ma numer 200 i oznacza, że wszystko poszło dobrze. Istnieją jednak sytuacje, kiedy serwer nie może odpowiedzieć na żądanie klienta. W takim przypadku, to właśnie kod błędu informuje o tym, co naprawdę się wydarzyło.

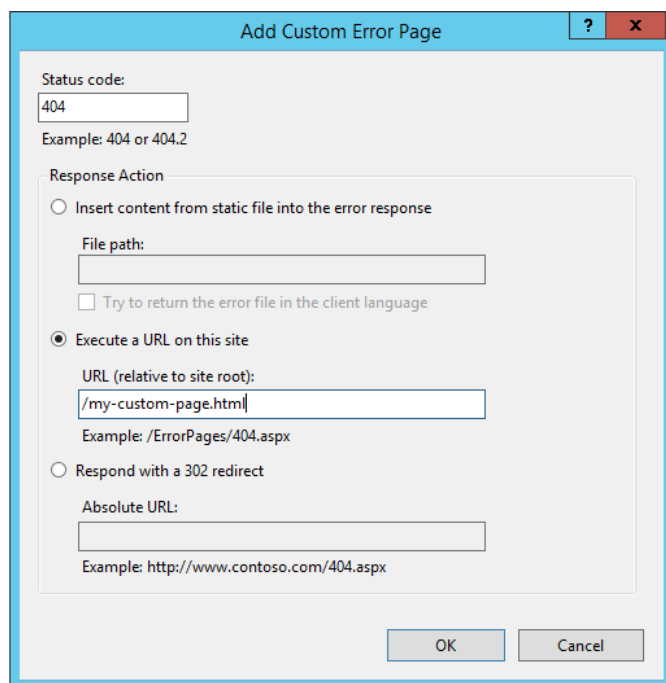
Kody błędów są ustandaryzowane i opisane w dokumencie RFC 2616, sekcja 10. "Status Code Definitions". W przypadku błędu, serwer może zamiast samego kodu wysłać również jakieś dane.

Przykładowo, błąd 404 mówi klientowi, że na serwerze nie ma tej strony, o którą zapytał. Zamiast posłać samo 404 i liczyć, że przeglądarka zrozumie komunikat, serwer może na przykład wyświetlić stronę, na której będzie opisana struktura portalu, dzięki czemu klient łatwo trafi tam, gdzie chciał.

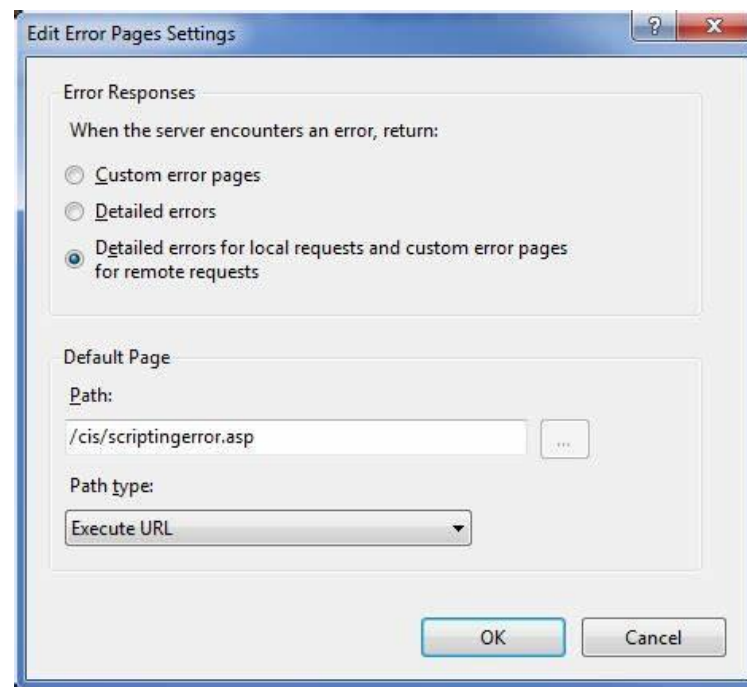
Strony błędów (Error Pages)

Administrator ma następujące możliwości:

- Wstawić tekst z pliku. Może to być na przykład „szanowny kliencie, nie ma u nas na serwerze takiej strony”. Co ciekawe, mając klientów mówiących różnymi językami, można określić, że odpowiedź wysyłana jest w języku właściwym dla danego klienta.
- Wykonać skrypt lub aplikację na serwerze.
- Przekierować klienta na inną stronę, nawet na stronę na innym serwerze.



The 'Add Custom Error Page' dialog box is shown. It has a title bar with a question mark and a close button. The 'Status code' field contains '404', with an example '404 or 404.2' below it. Under 'Response Action', three options are listed: 'Insert content from static file into the error response' (unselected), 'Execute a URL on this site' (selected), and 'Respond with a 302 redirect' (unselected). The 'File path' field is empty. The 'URL (relative to site root)' field contains '/my-custom-page.html', with an example '/ErrorPages/404.aspx' below it. The 'Absolute URL' field is empty, with an example 'http://www.contoso.com/404.aspx' below it. 'OK' and 'Cancel' buttons are at the bottom.



The 'Edit Error Pages Settings' dialog box is shown. It has a title bar with a question mark and a close button. Under 'Error Responses', the text 'When the server encounters an error, return:' is followed by three radio button options: 'Custom error pages' (unselected), 'Detailed errors' (unselected), and 'Detailed errors for local requests and custom error pages for remote requests' (selected). Under 'Default Page', the 'Path' field contains '/cis/scriptingerror.asp', with a browse button (three dots) to its right. The 'Path type' dropdown menu is set to 'Execute URL'. 'OK' and 'Cancel' buttons are at the bottom.

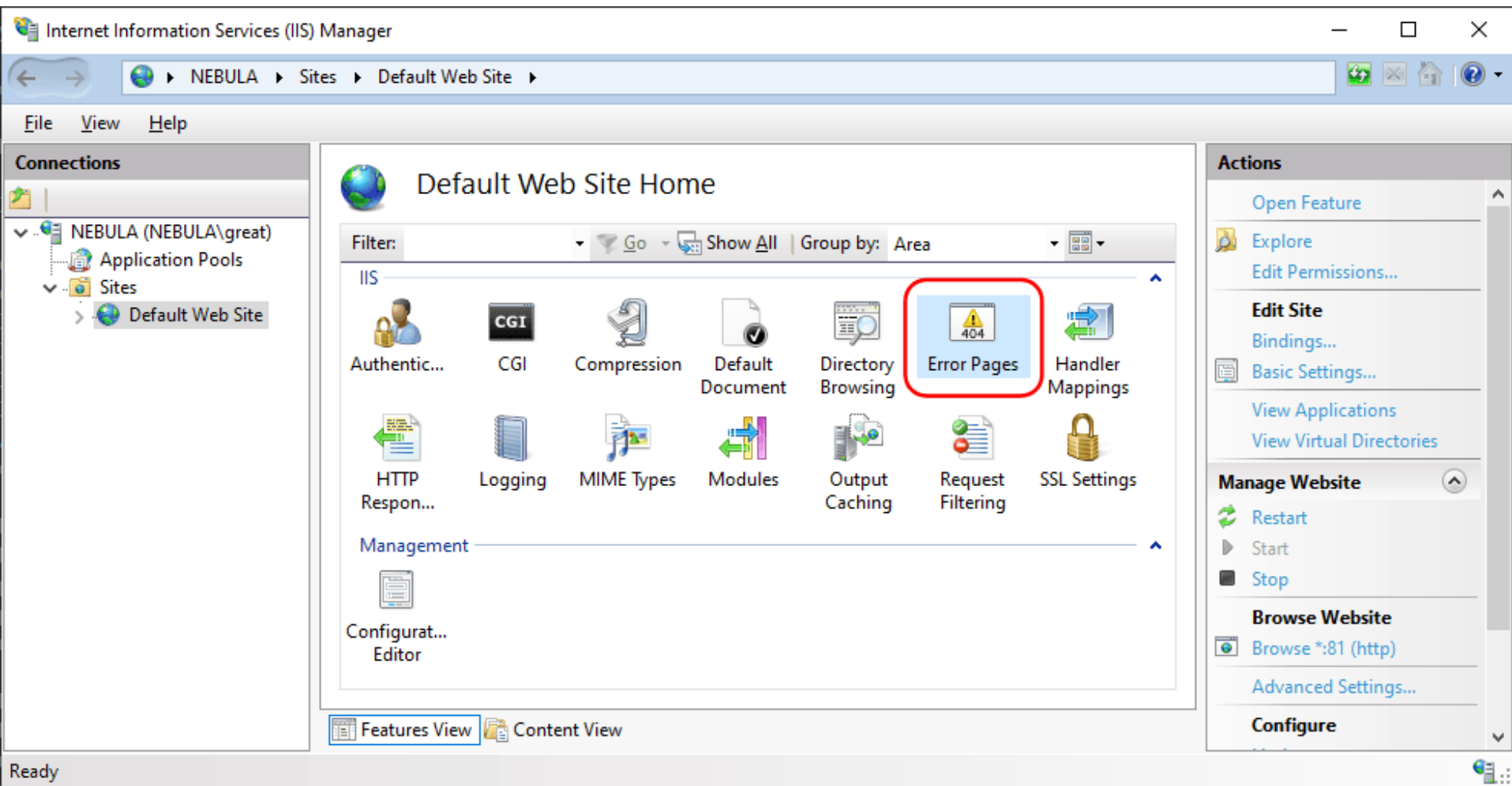
Strony błędów (Error Pages)

Okno konfiguracji strony błędów w IIS na Windows Server 2016, 2019 i 2022 pozwala na dostosowanie wyglądu i treści stron błędów, które są wyświetlane użytkownikowi, gdy wystąpi błąd.

Aby skonfigurować strony błędów, należy wybrać serwer lub witrynę w IIS Manager, a następnie wybrać opcję Error Pages. W oknie konfiguracji można zdefiniować, jakie strony błędów mają być wyświetlane dla różnych kodów błędów HTTP.

Można również zmienić wygląd i treść stron błędów, aby lepiej pasowały do stylu i wymagań witryny.

Strony błędów (Error Pages)



Mapowanie obsługi (Handler Mappings)

Opcja odpowiada za specjalną obsługę niektórych zapytań. W przypadku standardowego serwera udostępniającego strony WWW najpraktyczniejszym podejściem jest pozostawienie wszelkich ustawień z wartościami domyślnymi.

Przekierowanie HTTP (HTTP Redirect)

Opcja pozwalająca na odesłanie klientowi kodu (301, 302 lub 307) mówiącego, że danej zawartości należy poszukać gdzie indziej. Przekierowanie dla całego serwera zazwyczaj mija się z celem, ale dla poszczególnych katalogów czasem trzeba je zdefiniować. Klient wchodzący na daną stronę zostanie automatycznie skierowany w miejsce określone przez administratora IIS.

Nagłówki odpowiedzi HTTP (HTTP Response Headers)

Wraz z treścią strony (i omówionym już kodem liczbowym) serwer HTTP może przesłać do klienta wiele dodatkowych informacji. Jedną z nich są nagłówki. Definiuje się je w sekcji HTTP Response Headers. Nagłówki można dowolnie definiować według własnych potrzeb lub skorzystać z dwóch predefiniowanych. Potrzeba wstawienia własnych nagłówków jest tak egzotyczna, że nie warto się na niej skupiać. Należy tylko zapamiętać, że jest to wykonalne.

Predefiniowane nagłówki dotyczą za to opcji, które mogą się przydać:

- **utrzymywanie aktywności (http keep-alive)** - nagłówek mówiący przeglądarce, że nie powinna się rozłączać z serwerem. Zyskiem jest to, że przy kolejnym odwołaniu do serwera, system klienta nie będzie musiał od nowa zestawiać sesji TCP. Zmniejsza się dzięki temu ilość przesłanych danych i zwiększa prędkość. Opcja ta jest domyślnie włączona.
- **zawartość wygasa (Content expires)** - nagłówek mówiący przeglądarce, kiedy treść strony będzie już nieaktualna. Można podać konkretną datę lub „nigdy”, lub „jak tylko ją pobierzesz, to będzie nieaktualna”. Dzięki temu nagłówkowi, przeglądarka wie, czy ponowne żądanie danych ze strony stroną może być obsłużona na podstawie danych zgromadzonych w cache przeglądarki czy musi opierać się na informacjach pobranych z serwera. Dopóki nie jest to czymś konkretnym uzasadnione, najlepiej pozostawić nagłówek content expires wyłączony.

IPv4 Address and Domain Restrictions

Czasem zdarza się, że właściciel stron internetowych chce ograniczać dostęp do nich na podstawie informacji o adresie IP użytkownika.

Od IIS7 jest to możliwe i istnieją dwa scenariusze:

- Administrator pozwala wchodzić wszystkim oprócz wskazanych (Black list),
- Administrator nie pozwala wchodzić nikomu oprócz tych, których wskaże (white list).

Rodzaj podejścia zależeć musi od konkretnej sytuacji i dla każdego wirtualnego katalogu może być ustawiony indywidualnie.

Zmiana polityki dostępu (Black list czy white list) możliwa jest po wybraniu opcji „Edit Feature Settings”.

Z wyjątkiem bardzo specyficznych sytuacji, zarządzanie dostępem na podstawie adresu IP powinno nie być wykonywane na poziomie całego serwera. Pomijając trudności z późniejszym znalezieniem przyczyn błędów, ograniczenie takie można próbować omijać, więc nie powinno być traktowane jako ważna linia obrony serwera.

Logging

Logowanie zapytań jest jedną z najważniejszych rzeczy w dobrze skonfigurowanym serwerze. Nawet, jeżeli logi nie wydają się dzisiaj potrzebne, na pewno w przyszłości zdarzy się tak, że trzeba będzie do nich sięgnąć.

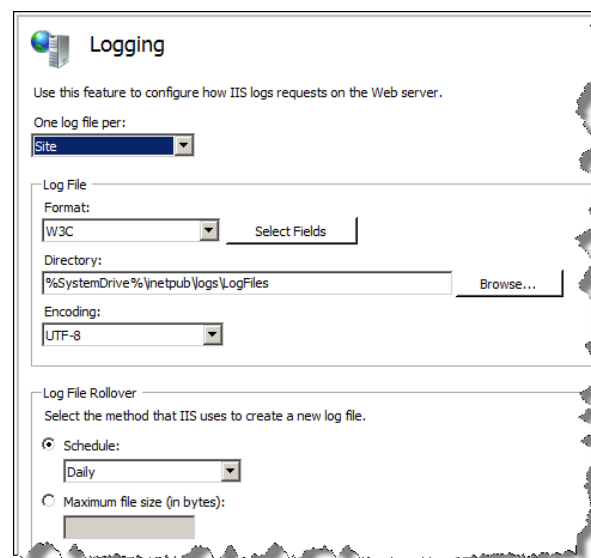
Opcje dostępne po włączeniu logowania przez administratora:

- **Poziom logowania** (One log file per). Log można zbierać jeden dla całego serwera IIS lub oddzielnie dla każdego serwera wirtualnego (o czym dalej). Domyślne ustawienie zakłada, że każdy serwer wirtualny ma oddzielny log i wydaje się to sensowne.
- **Format logu**. Najbardziej typowym formatem jest W3C czyli format, z którym zgodne są praktycznie wszystkie serwery internetowe, niezależnie od tego czy pochodzą z Microsoft, czy nie. Przy pomocy przycisku „Select Fields” wybrać można, które parametry żądania są zapisywane w pliku logu a które nie.
- **Katalog**. Miejsce, w którym zapisywane są logi.
- **Kodowanie znaków narodowych**. Domyślna opcja UTF-8 jest mniej uniwersalna, ale na pewno pozwoli na zapisanie każdego znaku narodowego z chińskimi i japońskimi łącznie.
- **Sposób tworzenia nowego pliku (rotacja)**. Opcja ta wskazuje, jak często ma być tworzony nowy plik z logami. Dostępne wartości to: co godzinę, codziennie, co tydzień i co miesiąc. Ponadto, nowy plik można zakładać wtedy, gdy stary osiągnie założony rozmiar (minimum 1048576 bajtów) lub cały czas zapisywać log do jednego pliku. Ostatnia opcja określa kiedy jest koniec dnia i nadeszła pora na założenie nowego pliku. Czy jest to o północy lokalnego czasu czy czasu UTC.

Logging

Ustawiając parametry logowania, nie wolno zapomnieć o dwóch istotnych faktach:

- Logi serwera WWW nie są małe. Miesiąc działania średnio odwiedzanego serwera to 300MB. Rok - prawie 4GB. Jeżeli serwer obsługuje wiele serwerów wirtualnych, nietrudno wyobrazić sobie, że po prostu zabraknie na nie miejsca. I tu pojawia się problem, ponieważ logi serwera IIS7, domyślnie znajdują się na dysku systemowym. A jeżeli systemowi zabraknie miejsca na dysku, to skutki mogą być bardzo smutne. Remedium może być albo umieszczenie logów na dedykowanym dysku albo stworzenie automatu (na przykład opartego na Task Scheduler), który stare logi będzie archiwizował i usuwał.
- W logach serwera WWW zapisywany jest czas. Czas ten nie jest czasem lokalnym! To czas uniwersalny czyli UTC, przesunięty o godzinę w stosunku do polskiego. Jeżeli odwołanie do strony miało miejsce w południe czasu polskiego, to w logach zostanie zapisana godzina 11:00. Należy o tym pamiętać.



Rodzaje plików (Mime Types)

Tabela typów plików informuje serwer jaki nagłówek ma wysłać w przypadku żądania pliku z danym rozszerzeniem. Na podstawie tego nagłówka przeglądarka wie, co z plikiem zrobić. Zasadniczo, należy przyjąć, że póki administrator nie jest pewny tego, co robi, opcje te powinien omijać. Szczególnym przypadkiem są pliki, których rozszerzenie nie pojawia się na liście. W takiej sytuacji możliwe jest, że serwer odpowie, że dany plik nie istnieje.

Moduły (Modules)

W sekcji tej wymienione są załadowane przez IIS moduły. To właśnie te moduły obsługują zapytania do serwera i ich lista zależy od wybranych podczas instalacji opcji. Dopóki ktoś nie jest w stu procentach pewny, co robi, to listę tę powinien traktować jako informację przeznaczoną tylko do odczytu i zbyt głęboko w niej nie grzebać.

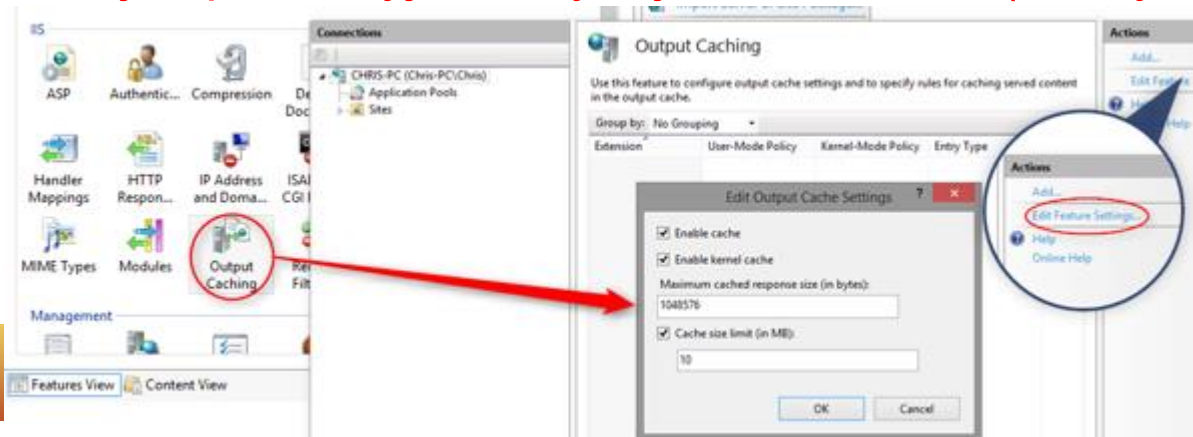
Buforowanie danych wyjściowych (Output Caching)

Buforowanie danych wyjściowych ma na celu przyspieszenie ich wysyłania do klienta HTTP. W IIS Manager definiować można jakie parametry ma mieć buforowania dla każdego typu plików oddzielnie.

Oczywiście, zdefiniować daje się również domyślna polityka buforowania. Warto wiedzieć, że dla buforowania można ustawiać polityki typu:

- Buforuj dopóki zawartość nie zostanie zmieniona;
- Buforuj na zadany czas;
- Nie buforuj.

W praktyce, eksperymenty z buforowaniem warto prowadzić tylko tam, gdzie wszystko inne działa już perfekcyjnie i wydajność serwera (nie łącza!) nie jest zadowalająca.



Certyfikaty (Certificates)

Sekcja „Certificates” służy do zarządzania certyfikatami, których serwer IIS7 używa do szyfrowania ruchu SSL (HTTPS).

Każdy certyfikat ma kilka istotnych pól:

- **Name (nazwa).** Pole określa nazwę certyfikatu, która pomaga administratorowi w zarządzaniu.
- **Issued To (wydany dla).** Pole podaje nazwę serwera, dla którego certyfikat został wydany. Nazwa ta zaszyta jest wewnątrz certyfikatu i nie może zostać zmieniona. Jeżeli serwer WWW udostępnia strony szyfrując je certyfikatem, którego nazwa nie jest zgodna z nazwą serwera, użytkownik zobaczy w ekranie przeglądarki komunikat o potencjalnym zagrożeniu.
- **Issued By (wydany przez).** Określa nazwę podmiotu, który wydał certyfikat. Jeżeli podmiot nie jest zaufany przez przeglądarkę klienta, zobaczy on na ekranie komunikat o potencjalnym zagrożeniu.
- **Expiration Date (data wygaśnięcia).** Definiuje termin przydatności certyfikatu do użycia. Wprawdzie po tym terminie certyfikat działa i transmisja jest szyfrowana, jednak użytkownik zobaczy w ekranie przeglądarki komunikat o potencjalnym zagrożeniu.
- **Certificate Hash (wynik funkcji skrótu).** Niedługi ciąg znaków, który zmienia się całkowicie nawet przy najdrobniejszej modyfikacji certyfikatu. Dzięki skrótowi można prosto porównać czy dwa pozornie identyczne certyfikaty są naprawdę tym samym czy jednak się różnią między sobą.

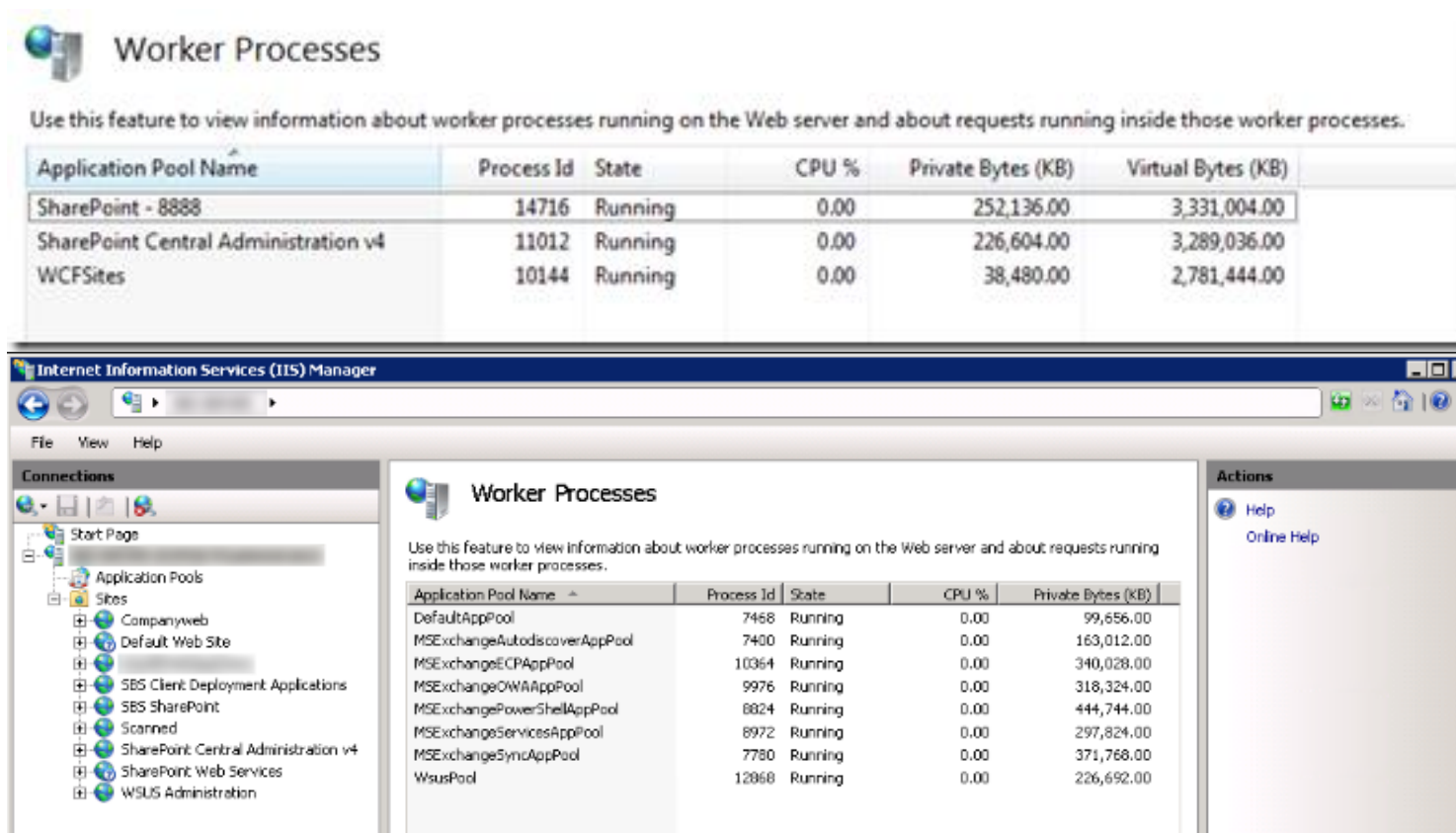
Certyfikaty (Certificates)

Serwer IIS może pozyskać certyfikaty SSL z czterech źródeł:

- Z pliku w formacie PFX. Plik taki chroniony jest zazwyczaj hasłem i jest to opcja najczęściej stosowana, kiedy ktoś już certyfikat posiada. Podczas importu dostępna jest opcja „Allow this certificate to be exported” (Zezwól na eksport tego certyfikatu) która pozwala na wykonanie kolejnych kopii takiego certyfikatu.
- Poprzez opcję „Create Self Signed Certificate” (Utwórz certyfikat samopodpisany). Certyfikat generowany jest natychmiast, ma roczną ważność a nazwa w certyfikacie jest taka sama jak nazwa FQDN serwera.
- Poprzez Online Certification Authority (Online Certyfikujący Organ Wydający Certyfikaty). W ten sposób można utworzyć certyfikat dla całej domeny i później łatwo przyznawać go poszczególnym hostom. Wymaga to jednak działającego w sieci CA.
- Poprzez Certificate Request (Żądanie certyfikatu). Sposób ten jest najczęściej stosowany, jeżeli potrzebny jest certyfikat do zastosowania w Internecie. Procedura składa się z kilku kroków: najpierw należy przy pomocy linku „Create Certificate Request” (Utwórz żądanie certyfikatu) wygenerować plik z żądaniem certyfikatu i zapisać go w pliku na dysku. Plik ten należy przesłać do Certification Authority (Organ Wydający Certyfikaty). CA generuje na podstawie pliku certyfikat i odsyła go do żądającego. Plik z certyfikatem należy zapisać na serwerze i wgrać go do IIS poprzez użycie opcji „Complete Certification Request” (Zakończ żądanie certyfikatu).

Proces roboczy (Worker Process)

- Ponieważ działanie serwera opiera się na działaniu wielu procesów roboczych obsługujących docierające serwerów wirtualnych żądania, istnieje okno pozwalające na zobaczenie aktywnych procesów, ich czasu działania, obciążenia procesora i zajętości pamięci.



Worker Processes

Use this feature to view information about worker processes running on the Web server and about requests running inside those worker processes.

Application Pool Name	Process Id	State	CPU %	Private Bytes (KB)	Virtual Bytes (KB)
SharePoint - 8888	14716	Running	0.00	252,136.00	3,331,004.00
SharePoint Central Administration v4	11012	Running	0.00	226,604.00	3,289,036.00
WCFSites	10144	Running	0.00	38,480.00	2,781,444.00

Internet Information Services (IIS) Manager

File View Help

Connections

- Start Page
- Application Pools
- Sites
 - Companyweb
 - Default Web Site
 - SBS Client Deployment Applications
 - SBS SharePoint
 - Scanned
 - SharePoint: Central Administration v4
 - SharePoint: Web Services
 - WSUS Administration

Worker Processes

Use this feature to view information about worker processes running on the Web server and about requests running inside those worker processes.

Application Pool Name	Process Id	State	CPU %	Private Bytes (KB)
DefaultAppPool	7468	Running	0.00	99,656.00
MSExchangeAutodiscoverAppPool	7400	Running	0.00	163,012.00
MSExchangeECAppPool	10364	Running	0.00	340,028.00
MSExchangeOWAAppPool	9976	Running	0.00	318,324.00
MSExchangePowerShellAppPool	8824	Running	0.00	444,744.00
MSExchangeServicesAppPool	8972	Running	0.00	297,824.00
MSExchangeSyncAppPool	7780	Running	0.00	371,768.00
WsusPool	12068	Running	0.00	226,692.00

Actions

- Help
- Online Help

Opcja SSL

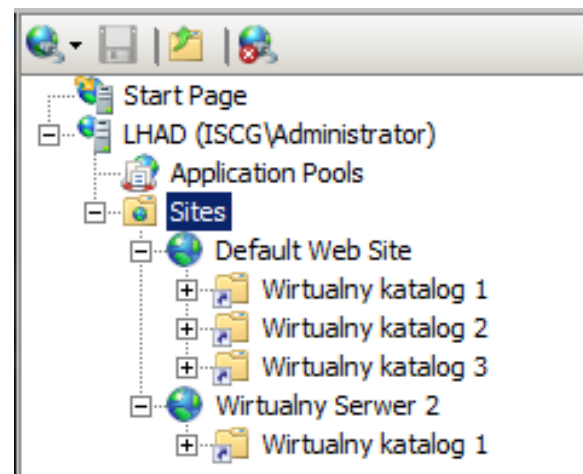
Opcja ta dostępna jest jedynie w ustawieniach wirtualnych serwerów i katalogów. Nie jest dostępna dla całego serwera IIS.

Zaznaczenie checkboxu oznacza, że dla danego obiektu dozwolony będzie jedynie dostęp przez HTTPS. Aby opcja była aktywna, obiekt musi być wcześniej skonfigurowany tak, żeby istniało powiązanie (binding) z HTTPS.

Serwery i katalogi wirtualne

Aby zrozumieć działanie serwera IIS7, konieczna jest wiedza na temat tego, jak wygląda wewnątrz jego struktura. W IIS7 ma ona trzy poziomy:

- Serwer IIS;
- Serwery wirtualne (Sites);
- Katalogi wirtualne (Virtual Directories).



Serwer wirtualny

Serwer wirtualny (zwany często „**site**”) jest przez użytkowników z sieci widziany jako samodzielny serwer WWW. Na pierwszy rzut oka wcale nie widać, że kilka adresów WWW działa na tym samym komputerze. Każdy ma swój adres, swoją stronę domyślną, swoje ustawienia itp. Warto zastanowić się, jak to możliwe, że na jednym komputerze dostępne są serwery pod wieloma nazwami.

Jest to możliwe na trzy różne sposoby:

- Serwer IIS ma wiele adresów IP i każdy serwer wirtualny ma przydzielony swój adres. Dzięki temu żądanie strony, przychodząc do IIS7, kierowane jest do właściwego serwera wirtualnego, który je obsługuje. Rozwiązanie to wymaga wielu adresów IP przypisanych do serwera. Przez to w sieci Internet sprawdza się dość słabo, natomiast świetnie działa w serwerach udostępniających strony tylko dla sieci LAN.

Serwer wirtualny

- Serwer IIS nie ma tylu adresów IP, ile ma serwerów wirtualnych, ale każdy serwer wirtualny działa na własnym porcie TCP/IP. W efekcie strony mają adresy `http://mojastrona.pl:1234/` itp. W sieci LAN działa to poprawnie, ale w Internecie wielu klientów nie będzie mogło skorzystać ze strony ze względu na filtrowanie ruchu przez rozmaite firewalle. Poza tym, adres taki jest mniej elegancki, a jak ktoś zapomni podać numer portu, to trafi na zupełnie inny serwer wirtualny i w efekcie inne strony.
- Serwer IIS ma jeden adres IP a wszystkie serwery wirtualne używają portu 80. Rozwiązanie takie używa tzw. host headers. Przeglądarka internetowa, komunikując się z serwerem WWW, poza pytaniem o stronę wysyła dane na temat tego, z jakim serwerem chciałaby się połączyć. Serwer IIS wykrywa takie żądanie i kieruje je do tego serwera, który ma przypisany odpowiedni host header. Ten sposób jest w chwili obecnej najczęściej spotykany w Internecie. W sieci LAN również działa to bardzo dobrze.

Serwer wirtualny

Aby utworzyć nowy serwer wirtualny, należy z menu kontekstowego serwera wybrać opcję „Add Web Site”.

W oknie konfiguracyjnym należy wypełnić odpowiednie pola:

- Site name oznacza nazwę wirtualnego serwera. Tak, jak chce ją widzieć administrator IIS, żeby łatwo poznać, który to site. „Mój serwer testowy” albo „serwer dla uciążliwych klientów” są nazwami jak najbardziej akceptowalnymi, ponieważ klient w przeglądarce nie widzi tej nazwy.
- Application pool i przycisk Select nie mają praktycznie zastosowania w przypadku statycznych stron WWW.
- Physical Path (ścieżka fizyczna) oznacza lokalizację, w której na dysku komputera znajdują się pliki *.html mające być serwowane jako strony WWW.
- Connect as pozwala na wybranie konta, którym posłuży się IIS, żeby odczytać pliki z dysku. W normalnych warunkach, do czasu naprawdę dobrego poznania założeń bezpieczeństwa w systemach Windows, najlepiej pozostawić tam wartość domyślną.

Serwer wirtualny

Sekcja „Bindings” (powiązania) definiuje metody, którymi ma kierować się IIS7, żeby przesłać żądanie do tego właśnie serwera wirtualnego.

Ustawić można protokół HTTP lub HTTPS, adres IP serwera wirtualnego (domyślnie są to wszystkie adresy serwera IIS), port TCP oraz host header.

- Jeżeli serwer IIS ma obsługiwać tylko jeden serwer wirtualny, wskazane jest pozostawienie wartości domyślnych. Można wprawdzie wybrać HTTPS zamiast nieszyfrowanego HTTP, ale w takiej sytuacji, konieczne jest posiadanie certyfikatu, nabytego jedną z opisanych w niniejszym artykule metod. Jeżeli nie jest to konieczne (nie są planowane wirtualne serwery rozróżniane przez host headers), to nie należy podawać żadnej wartości host header, ponieważ może to prowadzić do niezrozumiałych na pierwszy rzut oka sytuacji, kiedy serwer IIS nie chce obsłużyć połączenia.
- Checkbox na końcu okna dialogowego określa czy tak stworzony serwer wirtualny ma być uruchomiony natychmiast po utworzeniu, czy też utworzony i pozostawiony jako nieaktywny.
- Warto zwrócić uwagę, że jeżeli parametry (a dokładniej bindings czyli powiązania) serwera wirtualnego są takie, że IIS nie będzie mógł określić, gdzie przekierować ruch - pojawi się ostrzeżenie.

Server wirtualny

Add Web Site [?] [X]

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

☒ Start Web site immediately

Sites

Filter: Go Group by: No Grouping

Name	ID	Status	Binding	Pat
Default Web Site	1	Started (http)	*:80 (http)	%S
Wirtualny Server 2	2	Started (http)	*:81 (http)	c:V

Add Web Site [?] [X]

Site name: Application pool:

Content Directory

Physical path:

Pass-through authentication

Binding

Type: IP address: Port:

Host name:

Example: www.contoso.com or marketing.contoso.com

Add Web Site [?] [X]

 The binding '*:80:' is assigned to another site. If you assign the same binding to this site, you will only be able to start one of the sites. Are you sure that you want to add this duplicate binding?

Wirtualny Katalog

W ramach jednego serwera wirtualnego możliwe jest utworzenie katalogów wirtualnych. Katalog taki, to część przekazywana w zapytaniu HTTP do serwera po nazwie hosta. Przykładowo, w zapytaniu `http://mojeforum.firma.pl/admin` - parametr `admin` definiuje katalog wirtualny. Katalog może wskazywać na inną ścieżkę fizyczną niż wirtualny serwer oraz mieć inny sposób uwierzytelniania.

Warto też przyzwyczaić się, do traktowania serwera wirtualnego jako katalogu wirtualnego o pustej nazwie, zlokalizowanego na tym serwerze. Aby utworzyć katalog wirtualny, z menu kontekstowego wirtualnego serwera należy wybrać „Add Virtual Directory” i w wyświetlonym oknie dialogowym podać nazwę i ścieżkę fizyczną. Dodatkowo, zmienić można parametry uwierzytelniania.

Należy wiedzieć, że jeżeli nie jest potrzebna inna ścieżka fizyczna, inny sposób uwierzytelniania, ani inne pozostałe parametry nie różnią się od parametrów serwera wirtualnego – tworzenie wirtualnego katalogu nie jest niezbędne. W takiej sytuacji, lepiej w folderze zawierającym pliki *.html utworzyć podfolder i w nim umieścić zasoby. Z punktu widzenia użytkownika przeglądarki, nie widać różnicy czy wyspecyfikowana w URL ścieżka odwołuje się do faktycznie istniejących na dysku katalogów, czy do katalogów wirtualnych.

Rady dla początkujących

- Po instalacji serwera IIS należy na tym samym komputerze wejść na stronę <http://localhost>. Powinna się otworzyć strona powitalna. Jeżeli się nie otwiera – trzeba wrócić do instalacji i dokładnie sprawdzić wybrane opcje;
- Jeżeli serwer ma mieć tylko jeden serwer wirtualny, należy wgrać pliki html do katalogu `c:\inetpub\wwwroot` i przestawić domyślną stronę na właściwą. Po tej operacji należy sprawdzić czy <http://localhost> działa poprawnie i pokazuje nową stronę;
- Jeżeli serwer IIS ma mieć kilka serwerów wirtualnych, należy ich katalogi fizyczne umieścić w katalogu `c:\inetpub\wwwroot` lub umieścić w innym miejscu (ale nie na pulpicie ani w dokumentach!) i ustawić im prawa takie, jak ma `c:\inetpub\wwwroot`. Dopiero później do tych folderów należy skopiować (nie przenieść!) pliki html;
- Na początku nie należy eksperymentować z host headers, póki nie opanuje się wszystkich innych opcji. Warto pamiętać, że dla ustawionego host header nie zadziała link <http://localhost>. Do lokalnych testów host header, najprościej dodać stosowny wpis w pliku hosts. Jeżeli brzmi to niejasno, naprawdę lepiej wcześniej doczytać niż rozpoznawać działanie host headers w IIS metodą prób i błędów;

Rady dla początkujących

- Każdą wprowadzoną zmianę należy testować. Po jednej na raz. Dzięki temu możliwe będzie wychwycenie ustawienia, przy którym coś nie działa;
- Jeżeli serwer wirtualny przestał działać i nie wiadomo dlaczego, być może najprostszą metodą jest wyłączenie go i stworzenie nowego o właściwych parametrach;
- Warto pamiętać, że IIS7 ma mechanizmy backup i odtwarzania całej konfiguracji. Wprawdzie w chwili pisania niniejszego artykułu, dostępna wersja nie oferowała tego przez GUI i konsolę zarządzającą, to jednak poprzez zarządzanie z linii poleceń (omówione poniżej) można łatwo backup wykonać. Dzięki temu, w razie nieudanego eksperymentu, zawsze można wrócić do poprzedniego, działającego stanu.

Linki

http://www.microsoft.com/poland/technet/article/art0106_01.mspx

- IIS Home Page (Get Started \ Learn)

<http://www.iis.net/default.aspx?tabid=1>