Internet Information Services i Server Name Indication

Pored Hyper-V virtualizatora serverskih i desktop OS-ova, na što smo svojevremeno skrenuli pozornost, Desetka raspolaže s još jednim u osnovi serverskim "komadom" softvera – ***Internet Information Services*** (dalje: IIS). Za razliku od Hyper-V, koji ima neka ograničenja u odnosu na serversku inačicu, IIS Desetke identičan je onome iz Windows Server 2016 distribucije. Microsoft time nastoji privući što više developera kako bi razvijali web aplikacije za Windows OS, što je svakako sretna okolnost i za druge korisnike Desetke, jer oni agilniji & znatiželjniji imaju na rasplaganju kvalitetan i lako upravljiv Web / FTP / SMTP server.

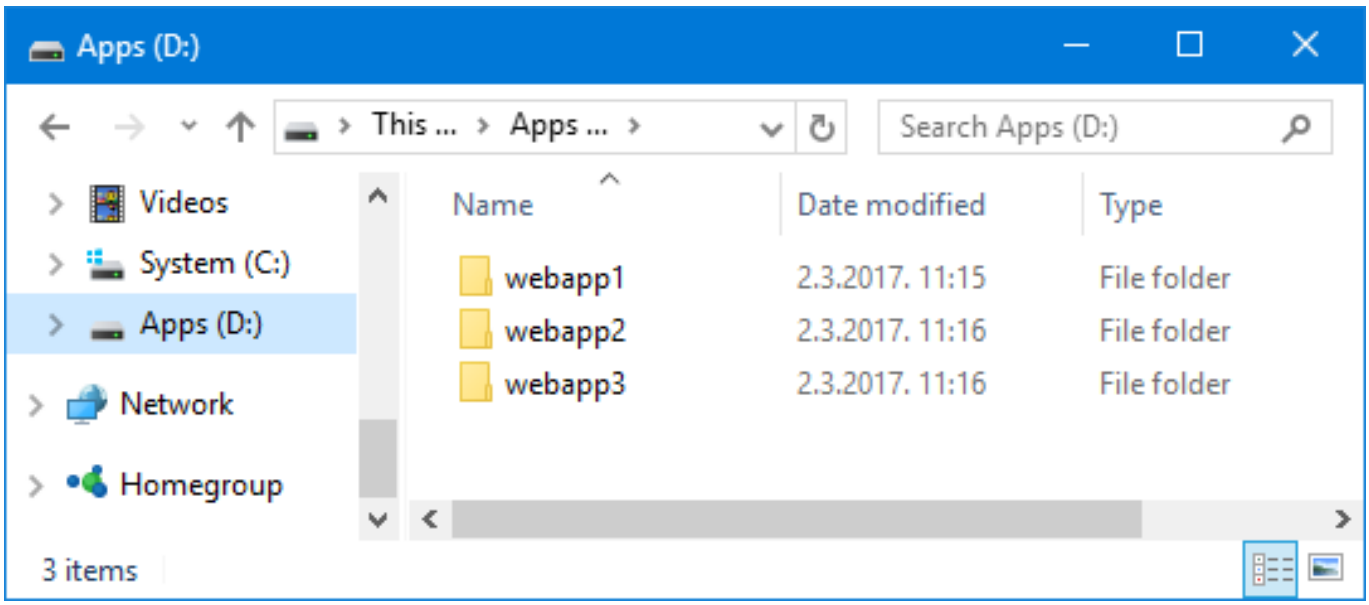
Iskoristit ćemo Desetkin IIS za upoznavanje sa ***Server Name Indication*** (dalje SNI) značajkom. SNI je spasonosna opcija kad moramo podizati nekoliko web usluga na jednoj IP v4 adresi, ujedno TLS enkripcijom štiteći vjerodajnice i podatke. Epitetom „spasonosna“ nimalo ne pretjerujemo, naime, kako znamo, kritično je stanje s raspoloživošću slobodnih javnih IP v4 adresa, pa je nužno što bolje iskoristiti svaku pojedinačnu. S druge strane, zbog imperativa sigurnosti, HTTPS pristup web resursima postao je de facto standard, pa se podižu isključivo TLS-om štićena web rješenja različitih mrežnih imena i domenskih sufiksa... time se značajno umanjuje primjenjivost digitalnih certifikata tipa Wildcard i Subject Alternative Name.

Dakle, iskoristit ćemo sretnu okolnost što na Desetki imamo IIS 10 pa ćemo podići tri web usluge na jednoj IP v4 adresi i TCP 443 portu, ali s individualiziranim certifikatima pomoću kojih se te usluge predstavljaju vanjskom svijetu i štite razmjenu podataka. To možemo zahvaliti SNI značajki, naime, ona omogućuje serveru obradu klijentovog zahtjeva za spajanje na određenu uslugu prije tzv. SSL/TLS handshakea i aktiviranja enkripcije podataka.

Očekujemo da imate:

- dvije radne stanice – „serverska“ mora biti Windows 10 Professional ili Enterprise, u domeni ili stand-alone; klijentska može biti kakvagod, Windows ili Linux;
- full administratorska prava na Desetki (isključite UAC);
- dostatnu dozu koncentracije i istraživačkog duha, posebno ako ste „tanki“ sa IIS-om ili poslužiteljskim certifikatima, jer jednim člankom ni izdaleka ne možemo pokriti sve tehničke aspekte i varijacije ove teme.

Mape za naša buduća web mjesta kreirat ćemo na volumenu namijenjenom za web sadržaje. Ne samo da je preglednije nego je i usklađeno s jednim od važnijih ***best practices*** savjeta: stopirati Default Web Site, a strukturu web mjesta napraviti na zasebnom volumenu. Naredna slika pokazuje tri mape kreirane u glavnom direktoriju diska D.

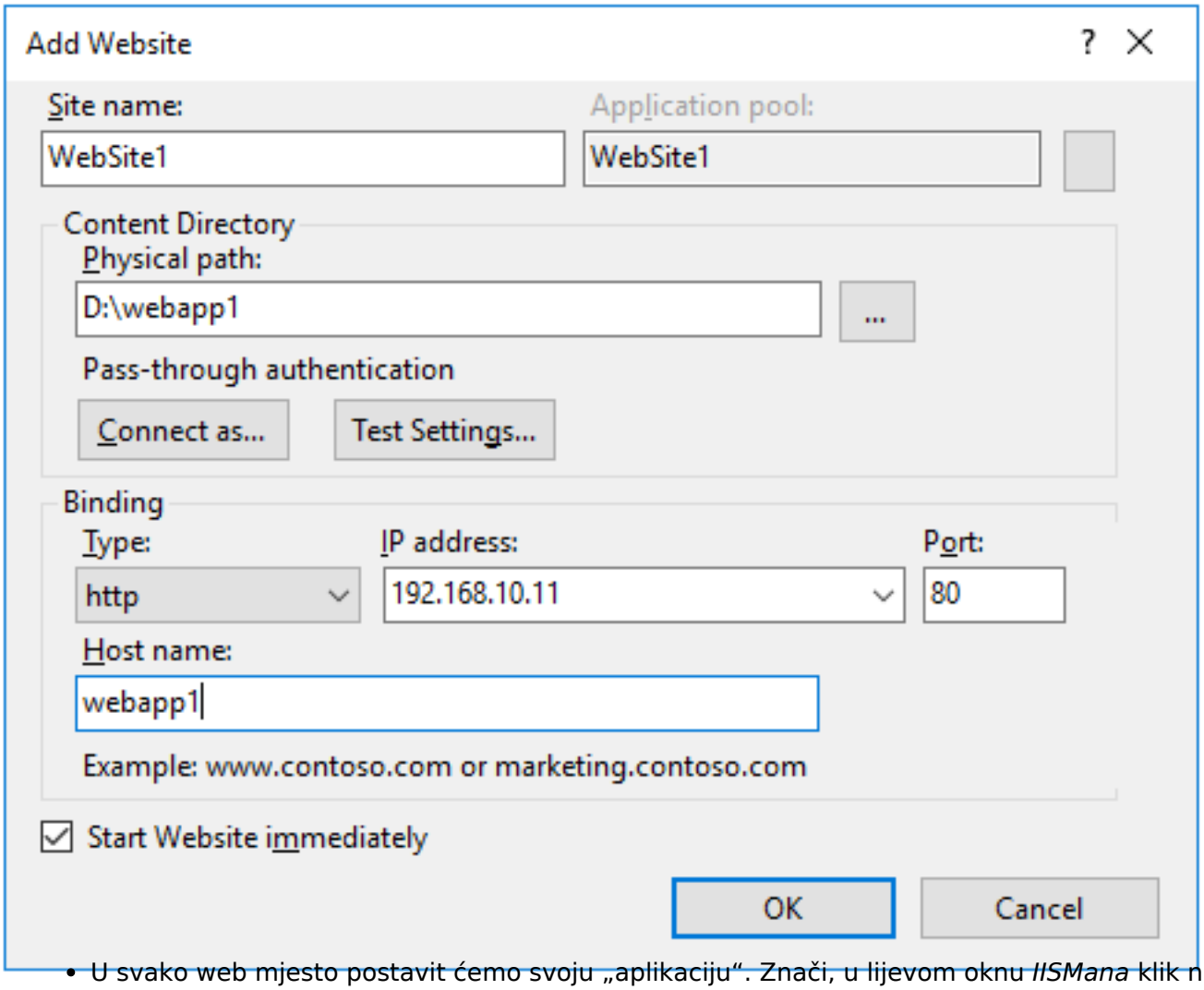


Trenutno su sve te mape prazne. Moramo u svaku od njih instalirati web aplikaciju. Tu smo na skliskom terenu, jer ako ne poznajemo dobro IIS kao web server i nemamo jasnu spoznaju kako postaviti neku *.NET ili PHP aplikaciju, primjenom web aplikacije možemo si toliko zakomplicirati situaciju da ćemo naposljetku izgubiti fokus. Bit ćemo stoga pragmatični, svaka naša „aplikacija“ sastojat će se od jedne obične tekstualne datoteke. Srećom, IIS prihvaća takav web sadržaj te, nama podjednako važno, dopušta mu anonimni pristup.

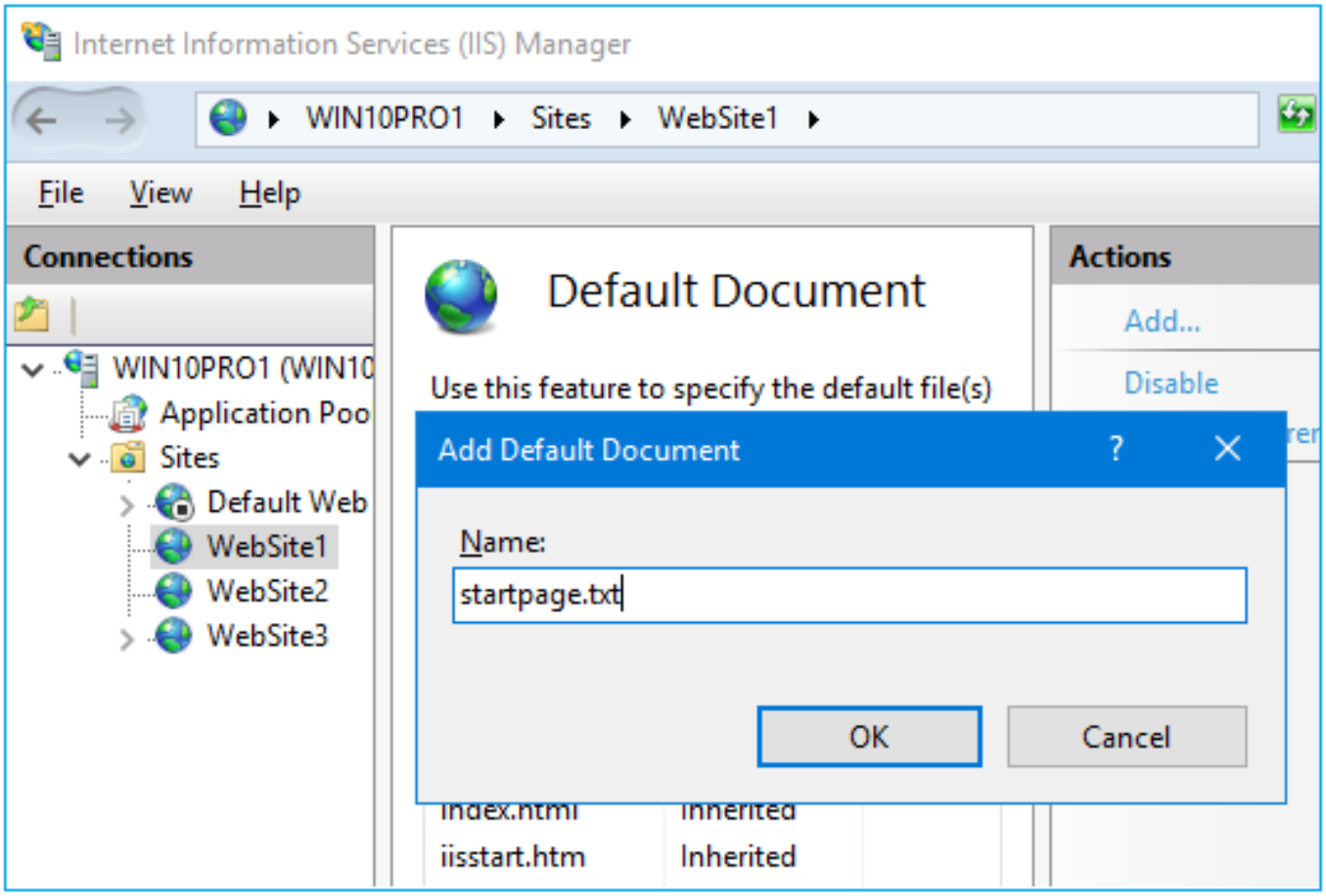
- Otvorimo Notepad, upišemo nešto poput *** OVO JE WEB MJESTO 1 *** i spremimo tekst kao startpage.txt u prvu mapu.
- Isto ponovimo za preostale mape, mijenjajući pritom broj u gornjem izrazu.

Instalaciju IIS-a odradit ćemo posredstvom appleta *Programs and Features*. Nakanismo li ozbiljnije istražiti IIS isplati se instalirati sve raspoložive module, ali za praktičnu proradu teme ovog članka sve što treba učiniti je jedan jedini klik ispred stavke *Internet Information Services*, potom još klik na gumbu Start za pokretanje instalacije... naposljetku iz *Administrative Tools* pozovemo *IIS Manager* i krenemo s poslom. Sve što slijedi možemo odraditi i iz komandne linije ali, didaktički gledano, IISMan kao GUI alat svakako je bolji izbor.

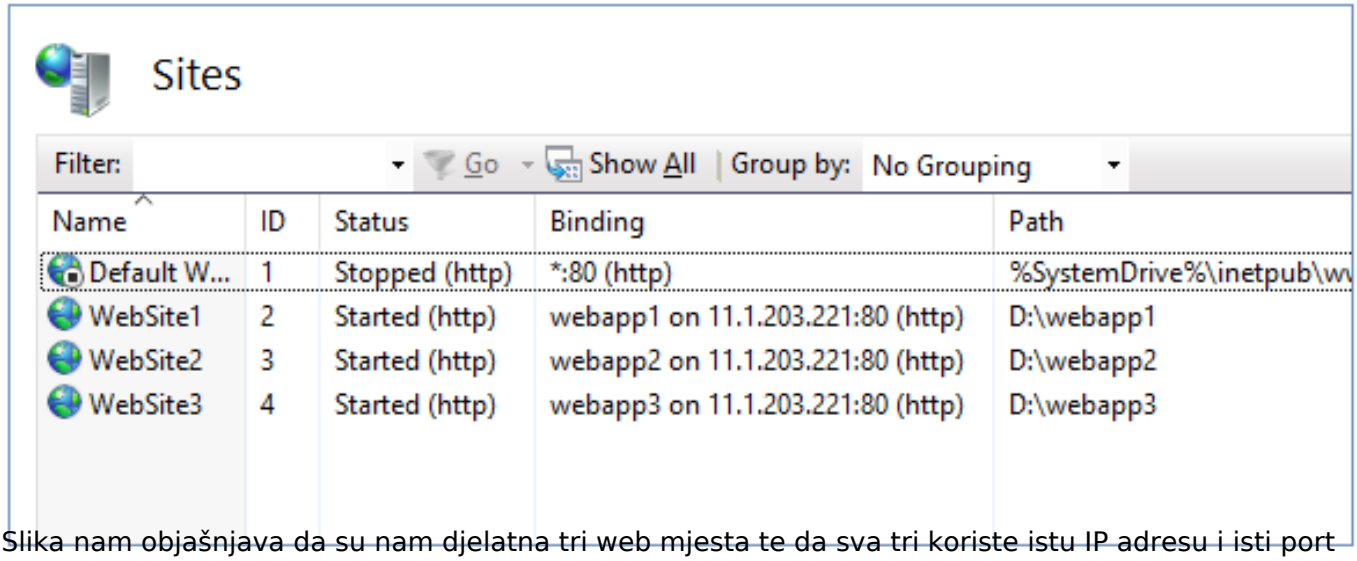
- U lijevom oknu *IIS Mana* označimo *Default Web Site*, potom u desnom oknu klik na naredbi Stop.
- U lijevom oknu *IIS Mana* klik na *Sites*, iz desnog okna pozovemo naredbu *Add Website* i popunimo polja za prvo web mjesto, kako pokazuje naredna slika Isti postupak primijenit ćemo za preostale siteove, samo mijenjamo redne brojeve u izrazima „WebSite“ i „webapp“.



- U svako web mjesto postavit ćemo svoju „aplikaciju“. Znači, u lijevom oknu *IISMana* klik na *WebSite1*, u srednjem oknu dvoklik na *Default Document* pa u desnom oknu klik na naredbi *Add*. Upišemo kako je na slici i potvrdimo. Možemo postojeće defaultne stranice izbrisati, ali i ne moramo, samo je važno da startpage.txt bude prvonavedena u popisu.



- Kliknemo li u lijevom oknu IISMana na stavci Sites, u srednjem ćemo vidjeti ovakvu situaciju:



Slika nam objašnjava da su nam djelatna tri web mjesta te da sva tri koriste istu IP adresu i isti port TCP 80. To je moguće zato jer im se razlikuju mrežna imena (hostname). Riječ je o dobro poznatom pravilu da svako web mjesto definiraju parametri: IP adresa, TCP port i mrežno ime, pa je potrebno promijeniti barem jedan od tih parametara kad hoćemo na istom web serveru imati nekoliko web mjesta.

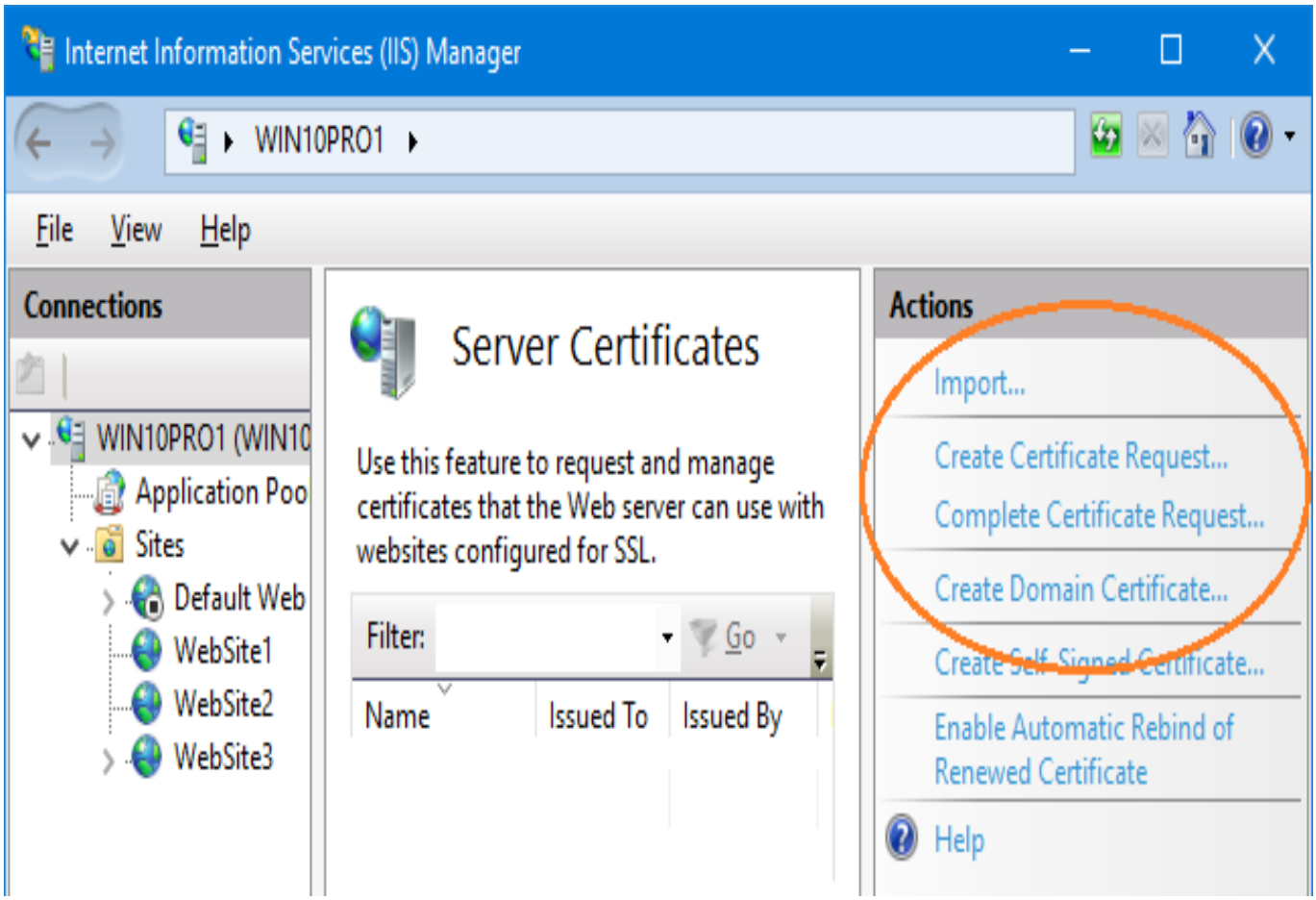
Prije nego što krenemo s konfiguriranjem značajke Server Name Indication (SNI), uvjerit ćemo se da naša web mjesta (tj. „aplikacija“ startpage.txt) već sada normalno funkcioniraju. Sjednemo za susjednu radnu stanicu i u njenu Hosts datoteku upišemo mrežna imena siteova / aplikacija:

11.1.203.221 webapp1
11.1.203.221 webapp2
11.1.203.221 webapp3

Možemo rabiti i FQDN, tada ćemo pripaziti kako oblikujemo Common name u poslužiteljskim (web server) certifikatima, vidi niže.
Iz IE-a ili Chromea http-om se spojimo na webapp1, i dalje. Naše „aplikacije“ se odazivaju, dakako, i na red je došao kompliciraniji dio teme – primjena digitalnih cetifikata kao preduvjet aktiviranja SNI značajke.

Važno je u lokalni repozitorij certifikata Desetke instalirati ne samo poslužiteljske (web server) certifikate za naše usluge, nego i certifikate svih CA koji tvore tzv. „certificate chain“ konkretne PKI infrastrukture od koje uzimamo poslužiteljske certifikate. Ukoliko ovdje zapnete, zaguglajte, samo jedna napomena: kad jednom dobijete potrebne certifikate, za upravljanje njima najbolje je rabiti Desetkinu mmc konzolu Certificates.

Što se tiče poslužiteljskih certifikata, IISMan raspolaže s nekoliko naredbi za naručivanje i uvoz takvih digitalnih isprava, prisutne su na narednoj slici.

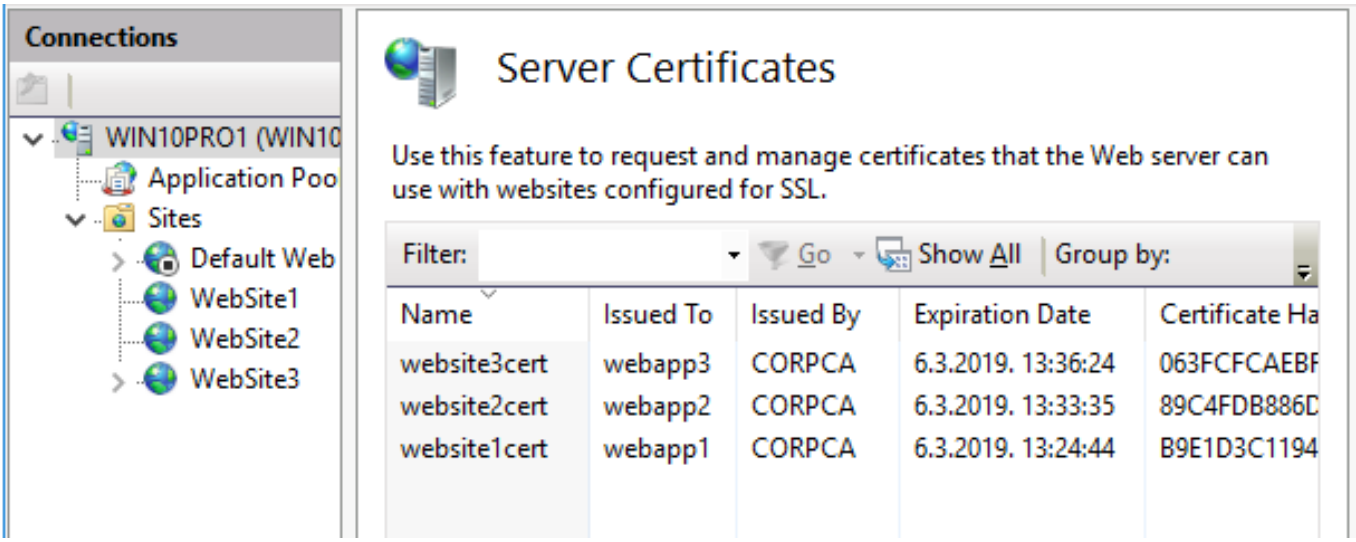


Ukoliko je naša Desetka članica Windows domene, a u toj domeni imamo Enterprise Certification Authority, dočepati se potrebih nam certifikata je jednostavno - pozovemo naredbu Create Domain Certificate te pratimo poruke na ekranima. U polje Common name moramo upisati mrežno ime web mjesta onako kako smo ga maloprije definirali kroz Hosts datoteku, ostalo možemo varirati.

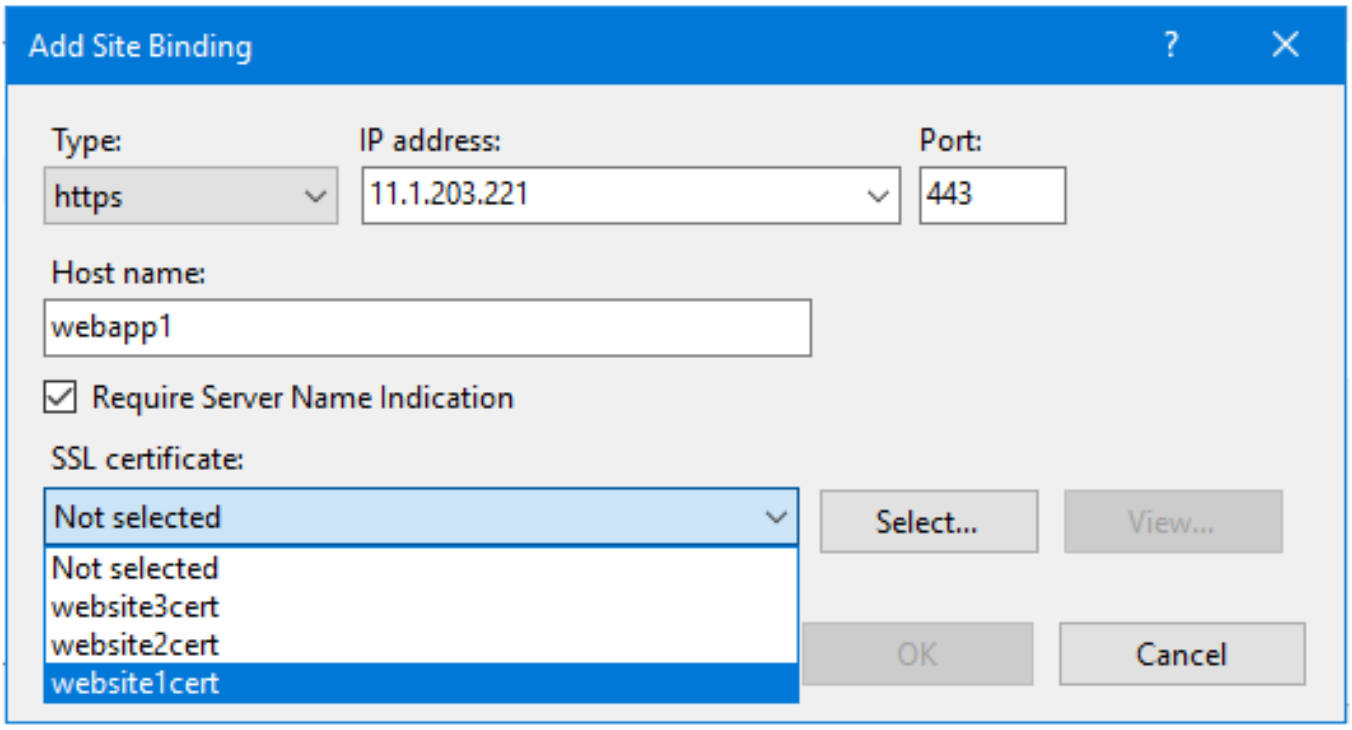
Više pozornosti treba posvetiti naredbi Import i duetu Create/Complete Certificate Request. Te naredbe rabimo kad naš IIS server nije član domene, ili jest ali nemamo domenski PKI, što su u praksi zastupljenije situacije. Koje ćemo radnje konkretno poduzeti ovisi o značajkama PKI implementacije

od koje želimo dobiti certifikate. Mala pomoć ako zahtjev za certifikatom stvaramo iz IISMana naredbom Create Certificate Request: CA instanci moramo dostaviti taj zahtjev u .txt fomatu (čisti tekst); kad od CA dobijemo odgovor tipa .cer, ne rabimo naredbu Import nego Complete Certificate Request. Naredba Import nam je korisna ako nam je certifikat isporučen kao .pfx ili .p12 paket (dakle, zajedno sa privatnim ključem).

Uvođenje certifikata u IIS mora završiti kako pokazuje naredna slika, uzeta s Desetke koja nije član domene, ali je dobila certifikate od domenske PKI hijerarhije. Common name (njega rabimo kad preglednikom pristupamo web aplikaciji) u koloni je Issued To, kolona Name je namijenjena adminima IIS-a.



Sad smo spremni postaviti svako web mjesto na HTTPS i uključiti SNI značajku. Krećemo s prvim sajtom: označimo ga u lijevom oknu IISMana, potom u desnom oknu klik na naredbi Bindings, pa klik na gumbu Add. U okviru poput ovoga na narednoj slici postavimo novu vezu (binding) za taj site.



Identičan zahvat primijenimo i na preostala web mjesta, mijenjamo samo redni broj imena u polju Hostname te biramo odgovarajući certifikat. Nakon toga možemo s pomoćne radne stanice svakoj „aplikaciji“ pristupiti HTTPS-om, što znači da nam je primjena SNI značajke uistinu omogućila smještaj nekoliko aplikacija na istu IP adresu i defaultni TLS port web servera. Živjeli! :o)

Sljedeći korak je nametnuti HTTPS pristup: u IISManu označimo web mjesto, dvoklik na appletu *SSL Settings,* uključimo *Require SSL* te, naposljetku, potvrdimo klikom na naredbi *Apply* u desnom oknu.

I sada imamo paradoksalnu situaciju: podigli smo zaštićenu konekciju k našim aplikacijama, ali svatko im može pristupiti jer je aktivan Anonimni pristup! O tome ćemo drugom prilikom, jer ovaj članak je već sada zaista predugačak.

sri, 2017-03-08 11:07 - Ratko Žižek**Kuharice:** Windows [1]
Kategorije: Servisi [2]
Vote: 0

No votes yet

Source URL: https://sysportal.carnet.hr/node/1728

Links
[1] https://sysportal.carnet.hr/taxonomy/term/18
[2] https://sysportal.carnet.hr/taxonomy/term/28