<https://www.youtube.com/playlist?list=PLZw_fXxI6L51dB6hD03-MAX8cBc7FqR6l>

Contents

[IIS asennus 1](#_Toc105740655)

[Oletushakemiston vaihto 1](#_Toc105740656)

[Salattu https yhteys 2](#_Toc105740657)

[DNS konfigurointi web palvelinta varten 5](#_Toc105740658)

[Forward Lookup Zone 5](#_Toc105740659)

[Reverse Lookup Zone 7](#_Toc105740660)

[Aliakset 9](#_Toc105740661)

[Forwarders ja Interfaces 10](#_Toc105740662)

[Redirection eli uudelleenohjaus 11](#_Toc105740663)

[Useampi sivusto ja Host Headerit 11](#_Toc105740664)

[IIS Intranet Sivusto 12](#_Toc105740665)

[Directory Browsing / hakemistolistaus 15](#_Toc105740666)

[VirtualHostit / Autentikaatio vain toiselle sivulle 17](#_Toc105740667)

# IIS asennus

IIS on WWW palvelin eli sen avulla voidaan ylläpitää eli hostata verkkosivuja jota käyttäjät voivat sitten käyttää yrityksen sisäisessä verkossa tai ulkopuoliset voivat ottaa siihen yhteyden Internetin kautta.

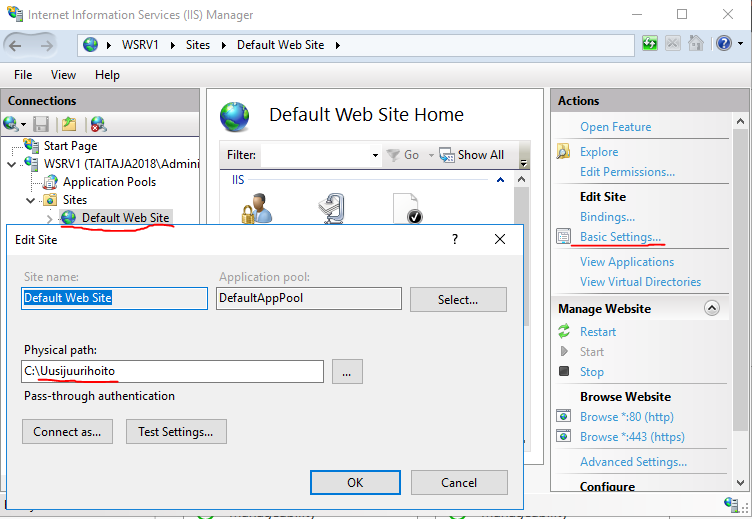
Add roles and features -> IIS.

IIS Managerin saat auki kun avaat Server Managerin -> Tools -> Internet Information Services

# Oletushakemiston vaihto

Tässä esimerkissä C:\ asemalle on luotu Uusijuurihoito niminen kansio josta tehdään uusi oletushakemisto nettisivullemme. Kyseisessä kansiossa sijaitsee index.html (tämän joudut itse tekemään – ota huomioon että tiedostopäätteet ovat näkyvissä) niminen tiedosto, joka sisältää meidän nettisivumme. **Kaikki www-palvelimet avaavat oletuksena index.html tiedoston**, jos sellaista ei ole, tulee ongelmia!

**Tarvittaessa luo kokonaan uusi index.html tiedosto oletushakemistoon. Varmista, että kansion hallinnassa on näkyvissä tiedostopäätteet. Muuten luomastasi tiedostosta tulee index.html.txt eikä se toimi nettisivuna.**

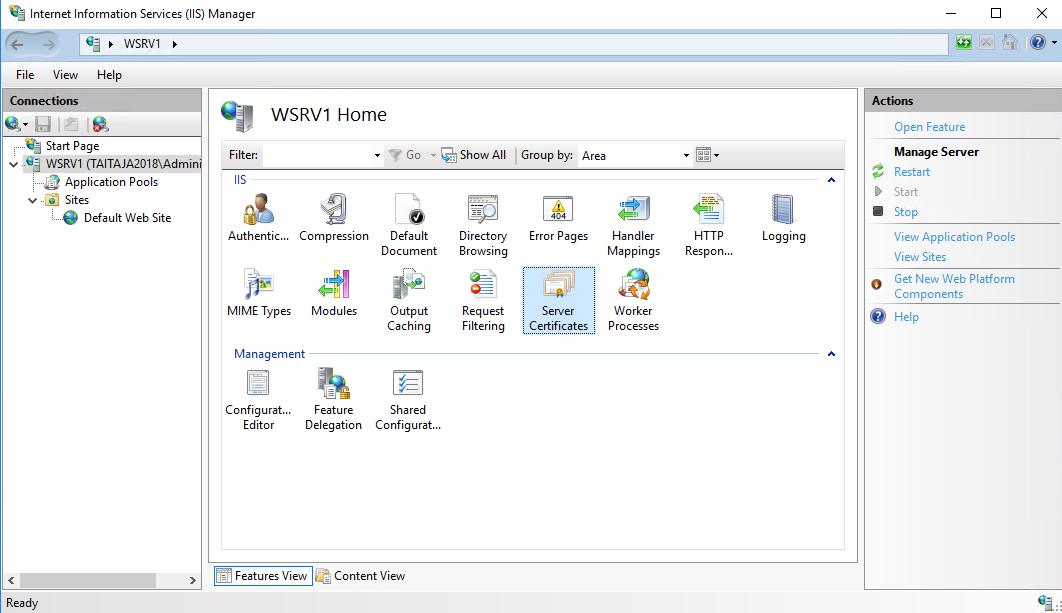


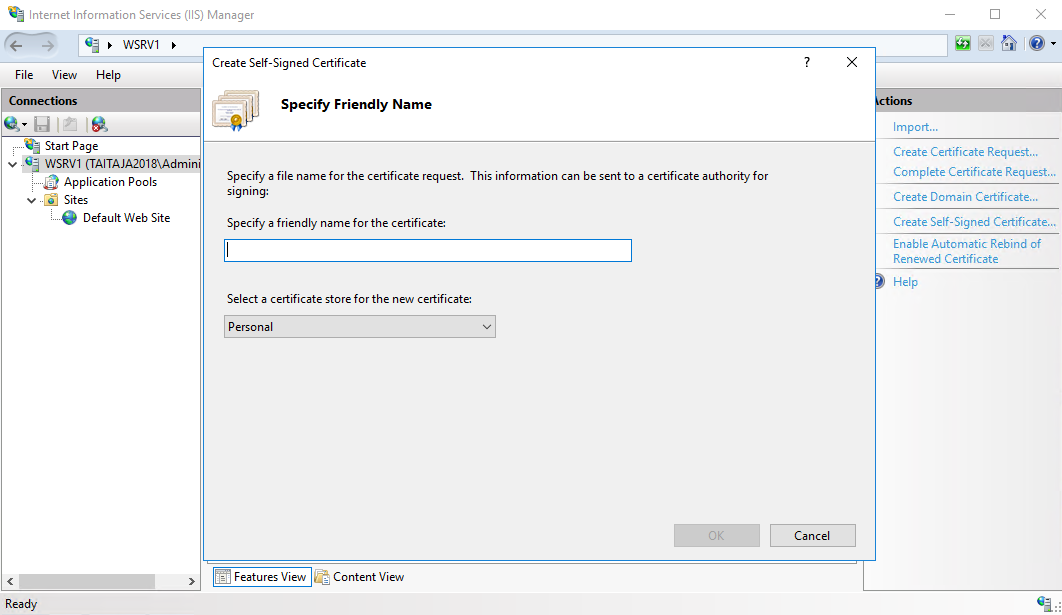
# Salattu https yhteys

Tässä tehty sertifikaatti on ns. self-signed certificate. Niitä käytetään pääasiassa testausvaiheessa. Kun oikeaan WWW-palvelimeen (tai muuhun palveluun) halutaan suojattu yhteys, tulisi hankkia virallinen sertifikaatti viralliselta taholta, kuten godaddy.com tai comodo.com. Usein tällaisista sertifikaateista ei tarvitse murehtia, jos WWW-sivut sijaitsevat webbihotellissa tai pilvipalvelussa.

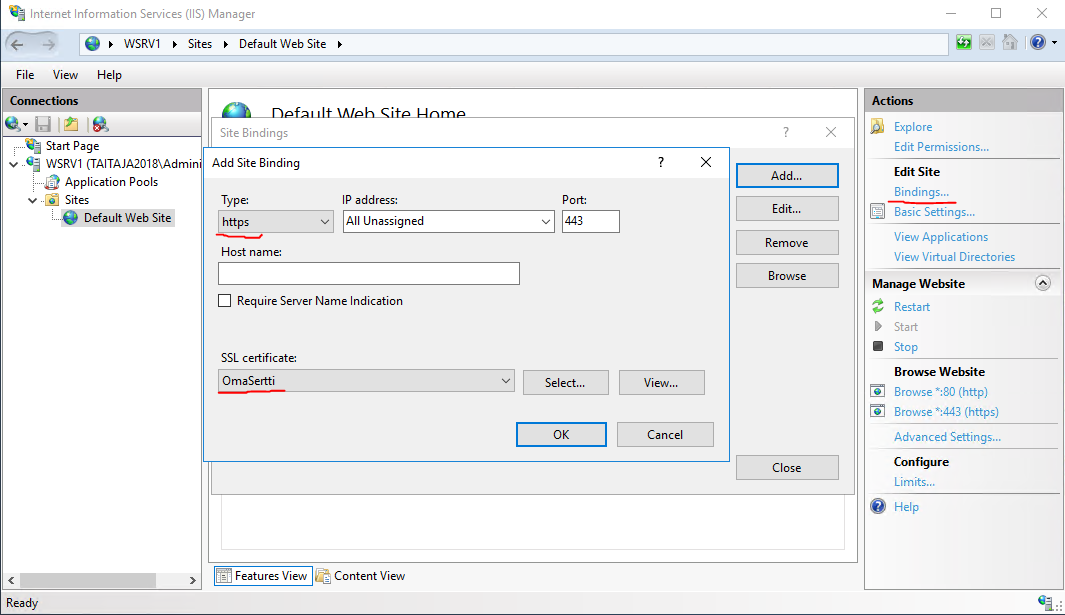
Sertifikaatteja voi tehdä myös itse hyödyntämällä Windows Serverin Certificate Authority palvelua. Tällöin voit luoda virallisen sertifikaatin yrityksen sisäisille laitteille, jotta ne luottavat esimerkiksi sisäiseen intrapalvelimeen. Luonnin jälkeen tämä sertifikaatti tulee jakaa yrityksen tietokoneille vielä.

IIS managerin pääikkunasta pääset tekemään Server Certificates eli sertifikaatteja.



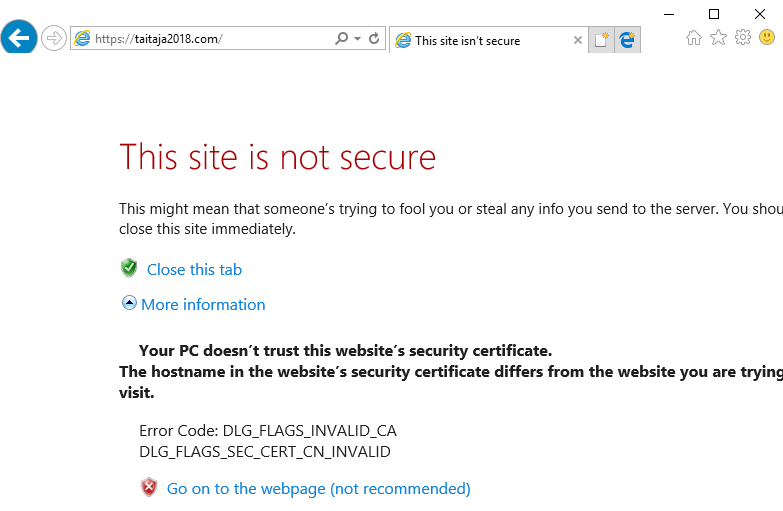


Luo Self-Signed Certificate ja anna sille jokin nimi ja tee siitä Web-Hosting.

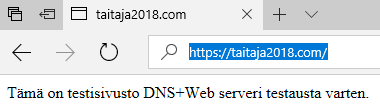


Valitse oma sivustosi (Sites) -> Bindings -> Add... -> valitse kuvan mukaiset asetukset ja valitse luomasi sertifikaatti.

Koska sertifikaatti on itse luotu selaimet valittavat siitä esim. Seuraavalla tavalla:



Varsinaisen sertifikaatti pitäisi hankkia taholta joka niitä myöntää. Meidän testaamista varten self-signed certificates riittävät kuitenkin. Alla kuva sivustosta jolla on salatulla yhteydellä:



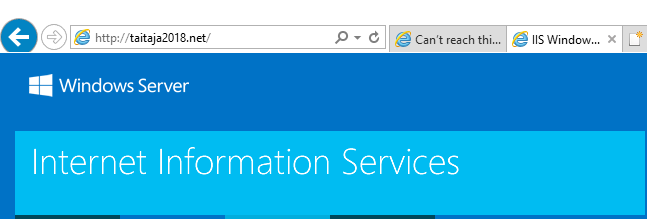
# DNS konfigurointi web palvelinta varten

DNS on palvelu jolla saadaan ohjattua nimet, kuten [www.yle.fi](http://www.yle.fi) johonkin IP-osoitteeseen kuten 52.85.47.74.

Oletuksena on, että sinulla on jo asennettuna AD DS ja DNS. Tässä esimerkissä DNS nimi/toimialueen nimi on taitaja2018.net.

DNS nimissä [www.taitaja2020.fi](http://www.taitaja2020.fi) olisi domain-osoitetta. [www.taitaja2020.fi/kuvat](http://www.taitaja2020.fi/kuvat) ”kuvat” kohta ei ole enään DNS tehtävä, vaan se tulee www palvelimelta, jolla sijaitsee sellainen kansio oletushakemistossa.

Asenna Web server (IIS) palvelimeen. Heti asennuksen jälkeen sivun taitaja2018.net tulisi toimia.

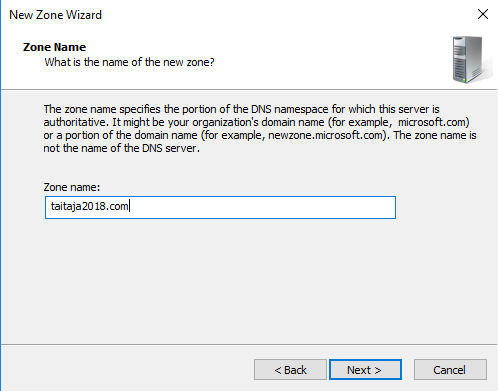


Web serverin sisältöä voi muokata palvelimesta polusta C:\inetpub\wwwroot. Sivusto, joka avataan oletuksena on nimeltään index.html. Joten voit luoda sinne sellaisen ja siihen mitä sisältöä haluatkaan.



# Forward Lookup Zone

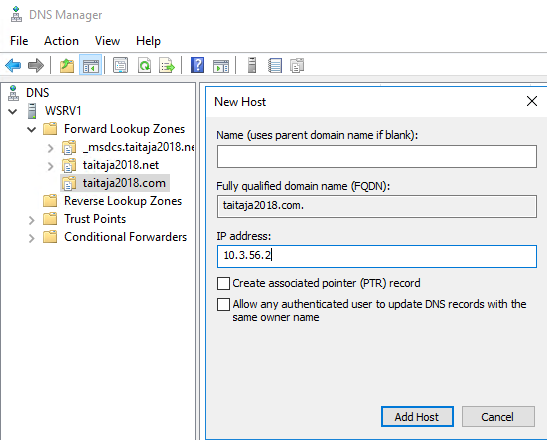
Jos haluat että sama sivu aukeaa myös osoitteesta taitaja2018.com tulee sinun tehdä sellainen zone DNS palveluun. Avaa DNS Manager ja luo uusi Forward Lookup Zone. Käytä oletusasetuksia, mutta laita Zone Name: kohtaan taitaja2018.com tai muu haluamasi nimi.

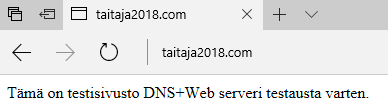


Luo taitaja2018.com zoneen uusi Host (A) recordi. Tämä recordi vastaa osoitetta taitaja2018.com

Näin määritetään IP-osoite 10.3.56.2 vastaamaan nimeä taitaja2018.com.

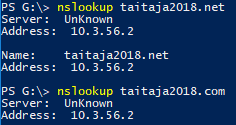
**HUOM! Saat tässä samassa yhteydessä tehtyä myös Reverse Lookup Zonelle PTR tietueen. Laita täppä kohtaan Create associated pointer (PTR) record. Varmista kuitenkin, että PTR tietue tuli Reverse Lookup Zoneen!**





# Reverse Lookup Zone

DNS asetuksia on hyvä testata myös komentoriviltä käyttäen nslookup työkalua.

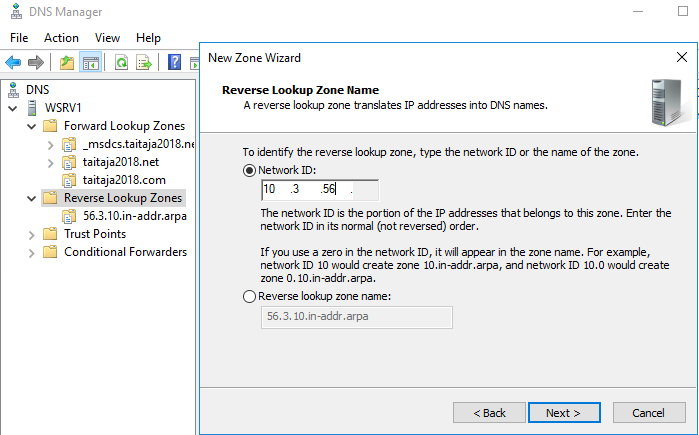


Kuvassa DNS näyttäisi toimivan ainakin Forward Lookup Zone kohdalta. **Unknown kohdat johtuvat kuitenkin siitä, että emme ole konfiguroineet Reverse Lookup Zoneja**. Reverse Lookup Zonet muuttavat nimet IP-osoitteiksi.

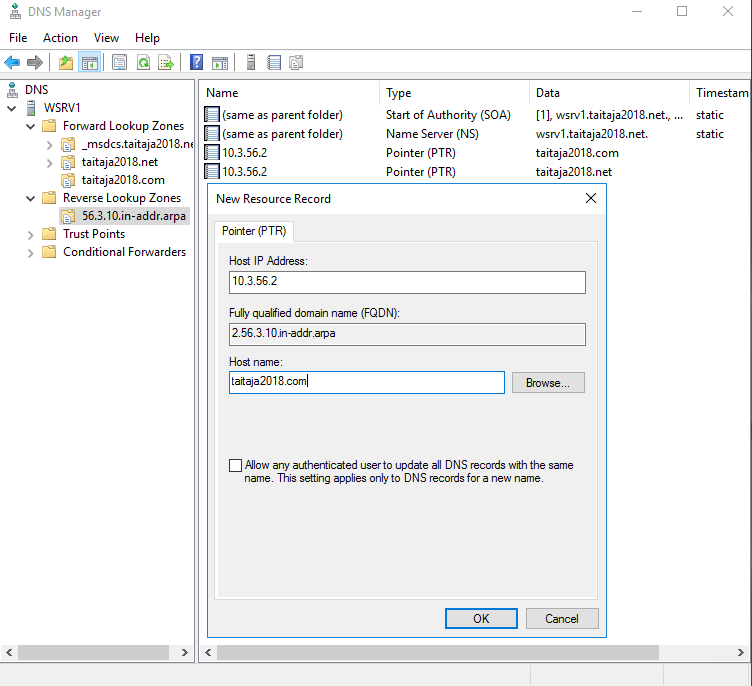
Reversen voi myös testata alla olevan kuvan mukaisesti. Eli sitä ei löydy lainkaan, koska ei sitä ole konfiguroitukaan.



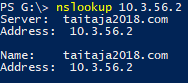
Luo uusi Reverse Lookup Zone. Käytä oletusasetuksia mutta Network ID: kohtaan aseta oman verkkosi osoite. Tässä on käytetty 10.3.56 verkkoa.

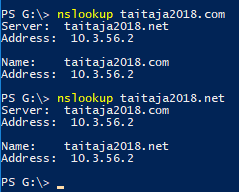


Sitten luo Reverse Lookup Zonelle kaksi pointer recordia. Näillä määritetään että IP-osoite 10.3.56.2 = taitaja2018.com / taitaja2018.net



Testataan toiminta uudestaan nslookupilla. Ei ole Unknown kohtia enään eikä valituksia Non-existent domain.

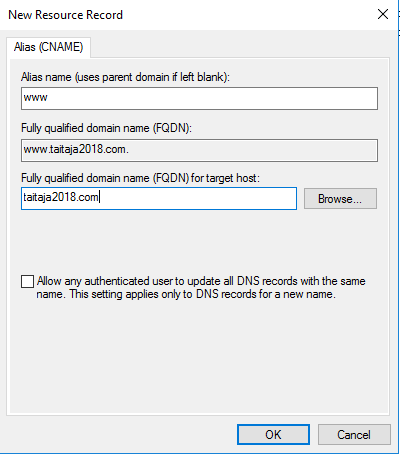
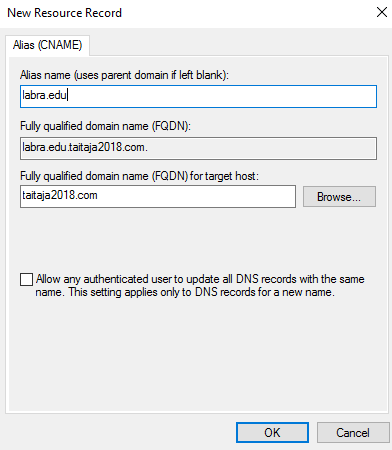




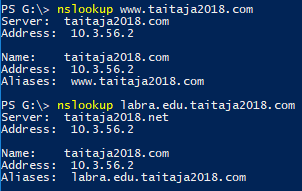
# Aliakset

Joskus voidaan haluta, että useampi osoite vie samaan paikkaan. Esim. Että www.taitaja2018.com ja labra.edu.taitaja2018.com vievät molemmat osoitteeseen taitaja2018.com.

Tällöin voidaan käyttää Alias recordeja eli CNAME. CNAME luodaan Forward Lookup Zoneen.

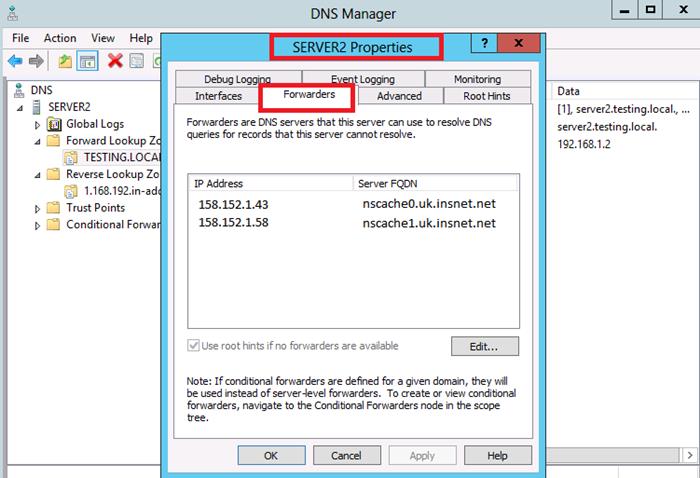
 

Testataan toiminta nslookupilla:



# Forwarders ja Interfaces

Voit määrittää mihin Windowsin DNS lähettää DNS kyselyt, joihin se ei osaa vastata määrittämällä ulkoisen DNS palvelimen IP-osoitteen Forwarders välilehdellä kuvan mukaisesti:



Samasta ikkunasta, Interfaces välilehdeltä voit määrittää mitä palvelimen verkkokortteja DNS palvelin kuuntelee.

# Redirection eli uudelleenohjaus

Uudelleenohjauksen avulla voit ohjata IIS jonkin sivuston toiselle sivulle. Esimerkiksi jos käyttäjä muodostaa yhteyden osoitteeseen hyriataitaja.local, se uudelleenohjattaisiin osoitteeseen skillsfinland.fi.

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/httpredirect/>

<https://www.supportsages.com/how-to-enable-http-redirection-in-iis-servers/>

# Useampi sivusto ja Host Headerit

IIS avulla voit ylläpitää useampaa sivustoa samalla palvelimella. Eli IIS voisi sisältää sivut hyriataitaja.local sekä taitajawindows.fi. Tämä onnistuu hyödyntämällä IIS Host Headers (Host Name) toimintoa. Toimiakseen ne vaativat myös DNS hyödyntämistä.

Ensiksi luo DNS:ään kaksi eri Zonea, toinen hyriataitaja.local ja toinen taitajawindows.fi. Luo molempien Zonejen alle A-tietueet, jotka osoittavat palvelimen IP-osoitteeseen, jolla IIS sijaitsee.

Sitten seuraa seuraavan linkin ohjeita, ja luo kaksi sivustoa IIS:ään ja hyödynnä Site Bindings toimintoa. Siinä tärkeä kenttä on Host name, johon tulee kirjoittaa verkkosivuston osoite, kuten hyriataitaja.local. IP-osoitteeksi voi laittaa IIS palvelimen IP-osoitteen.

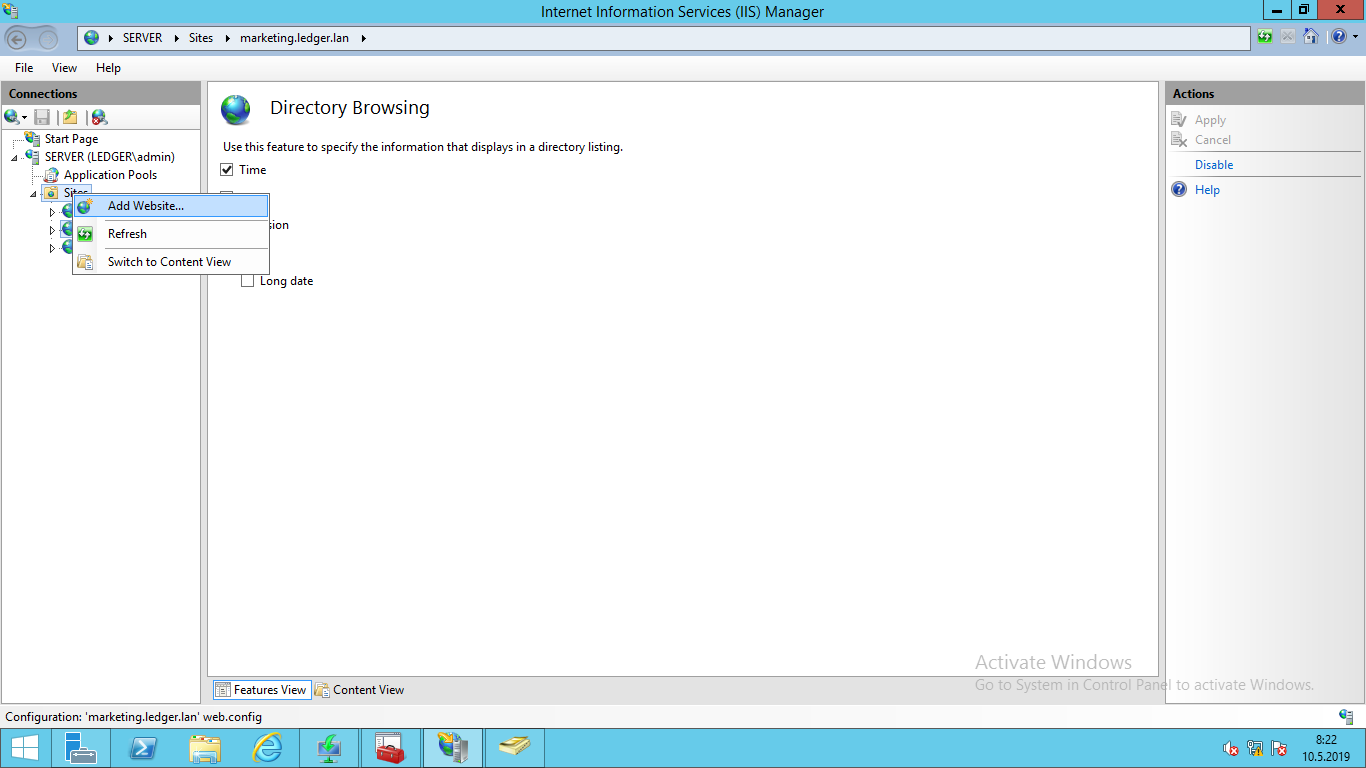
<https://docs.ukfast.co.uk/operatingsystems/windows/iis/hostheaders.html>

# IIS Intranet Sivusto

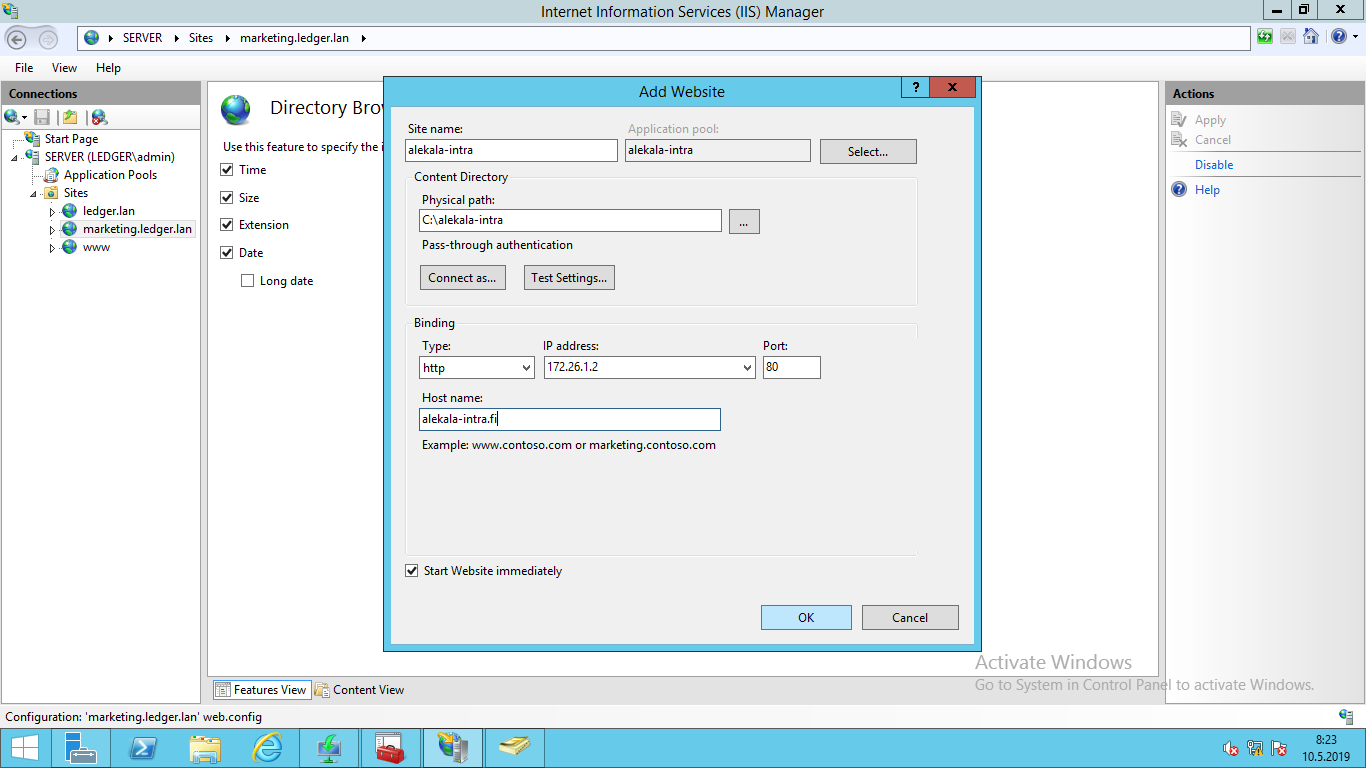
Aleksi Sievälä TITI17BR

Tässä ohjeessa tehdään intrasivusto jota voi käyttää vain marketing ryhmään kuuluvat käyttäjät.

Luodaan uusi IIS-sivusto:

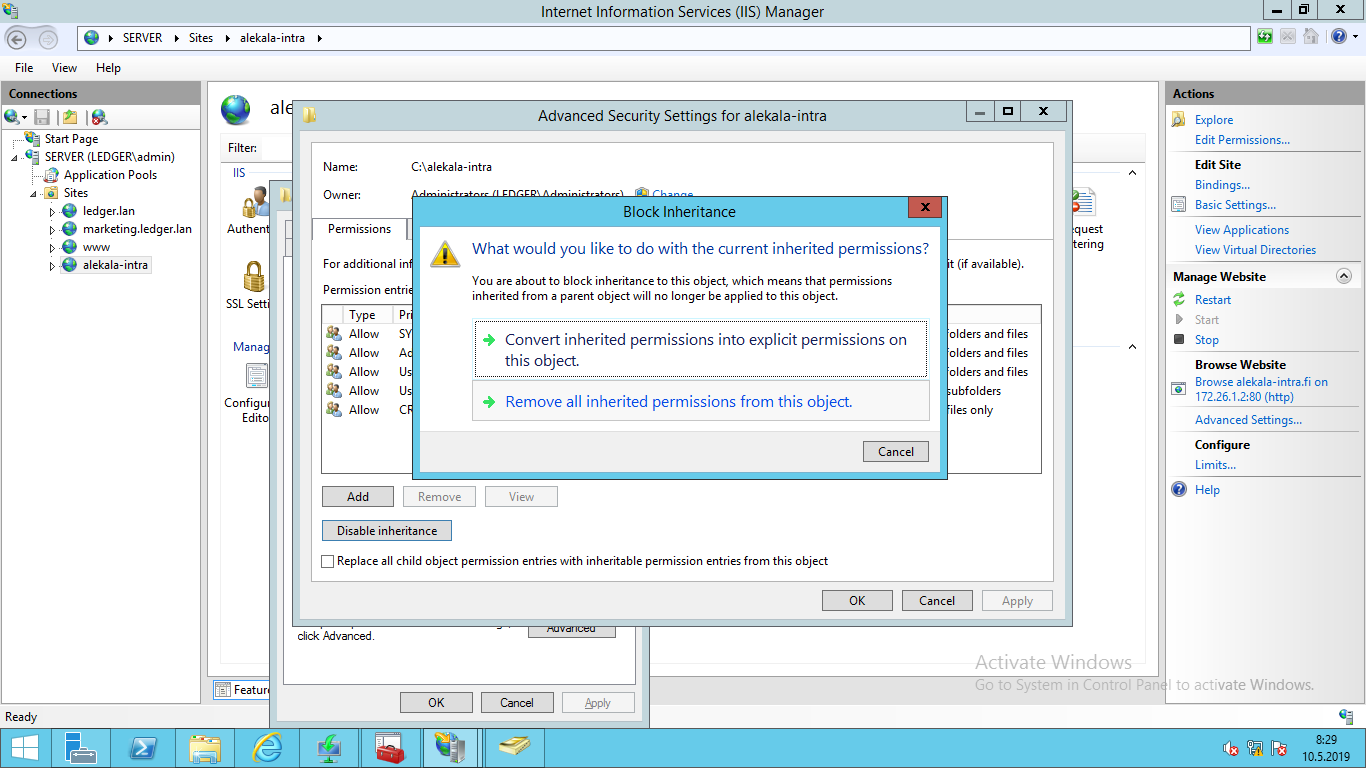


Sivuston asetukset:

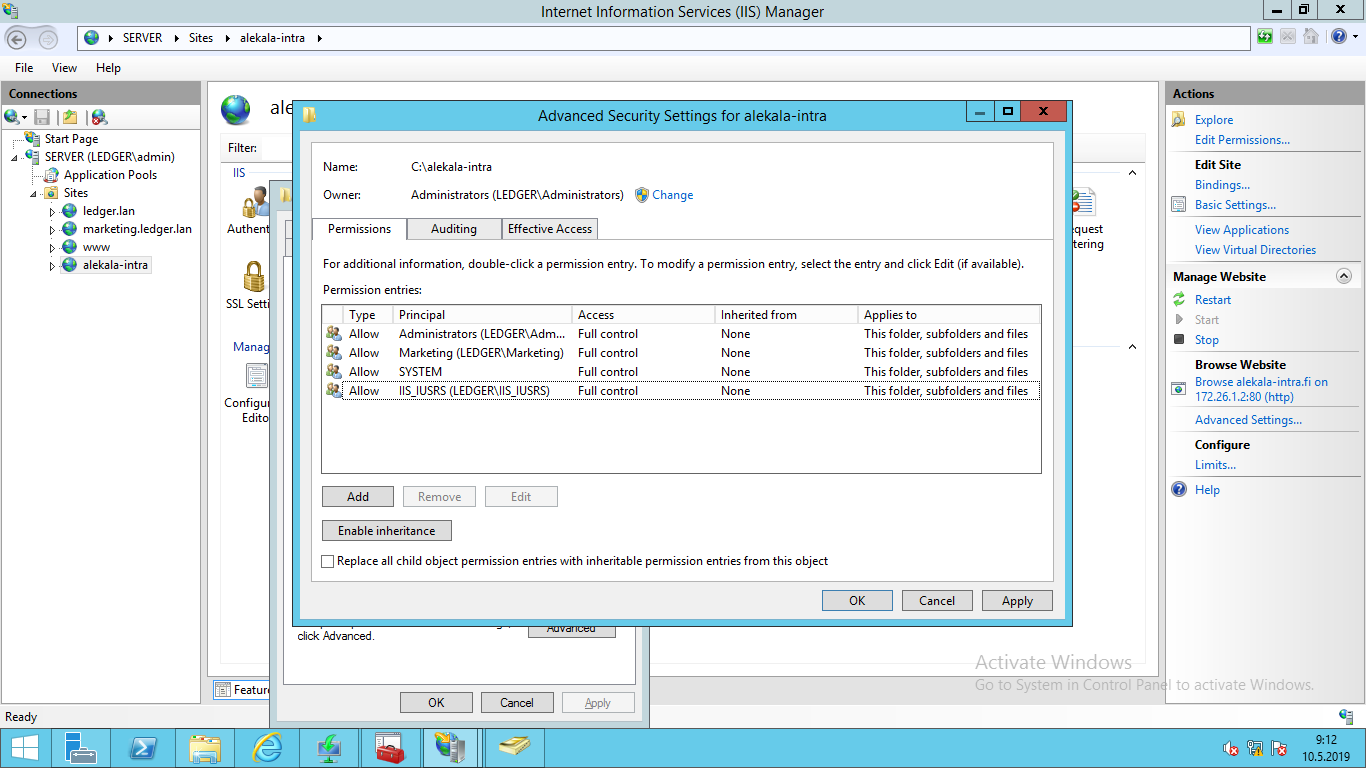


Poistetaan kansion alkuperäiset oikeudet:

IIS > Edit Permissions... > Security > Advanced > Disable inheritance > Remove all inherited permissions from this object.

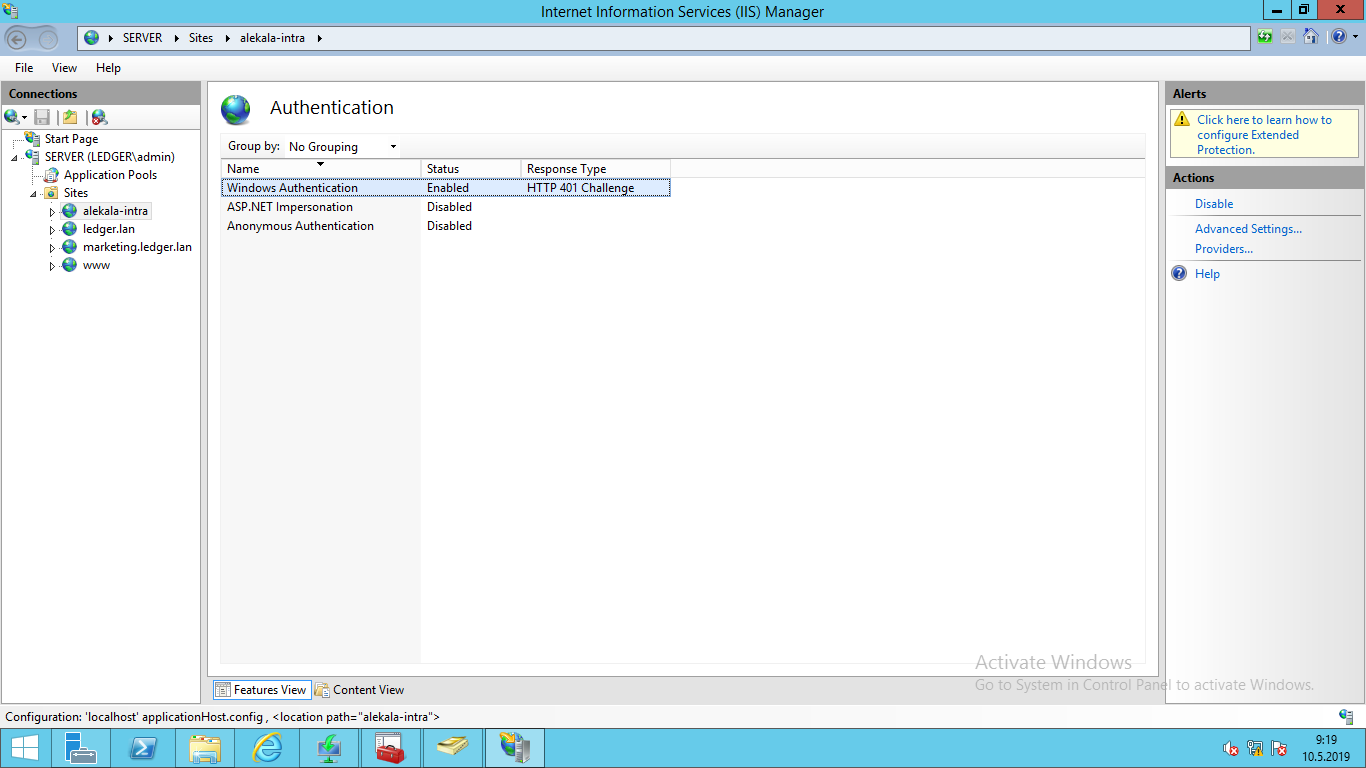


Lisätään uudet oikeudet (Marketing-oikeuksien tilalle voit laittaa haluamasi intra-jäsenet):



**HUOM!** IIS\_IUSRS ja SYSTEM-käyttäjille tulee antaa täydet oikeuden toimivuuden takaamiseksi.

Valitaan autentikointi tavat:



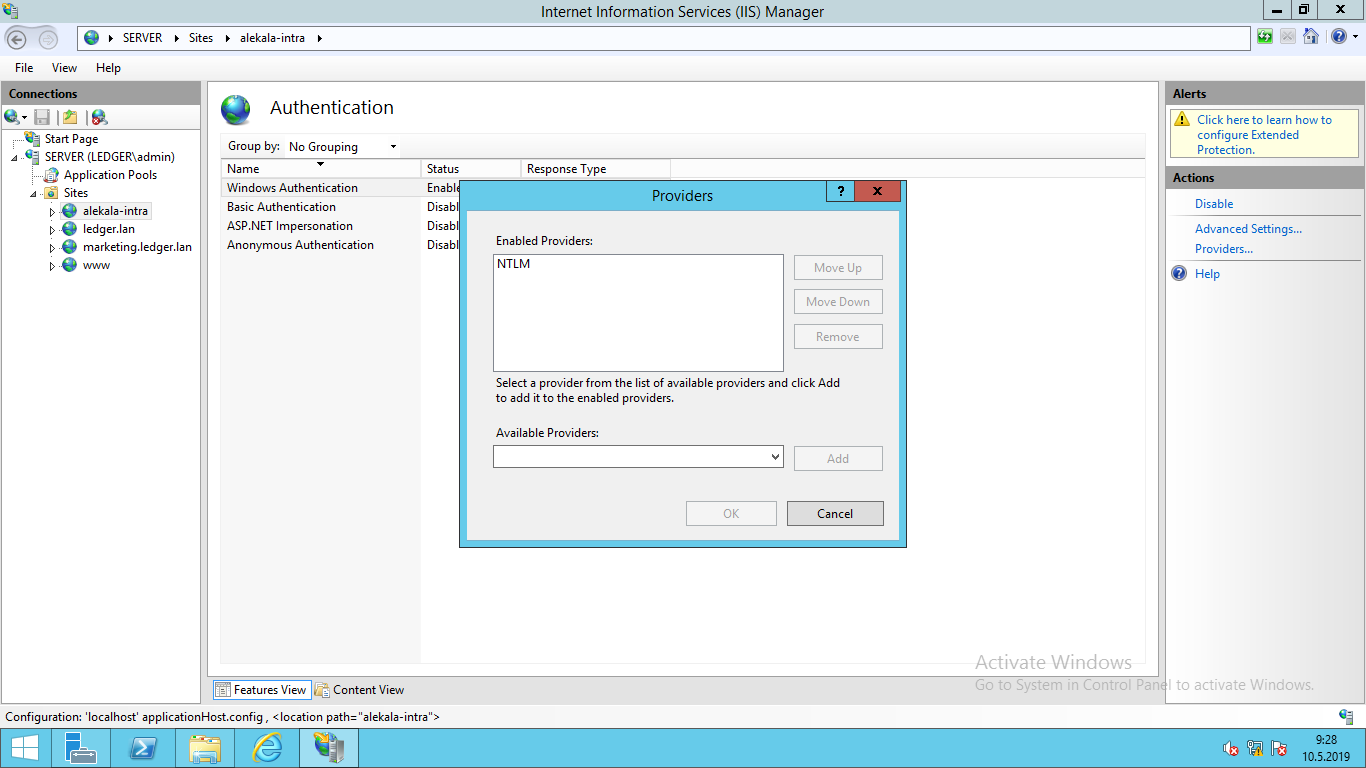
Jos Windows Authentication **EI** ole asennettu, voit asentaa sen Powershell komennolla:

**Install-WindowsFeature Web-Windows-Auth**

Saman ominaisuuden saa myös asennettua Add Roles and Features-ominaisuuden kautta.

Poistetaan turhat asetukset:

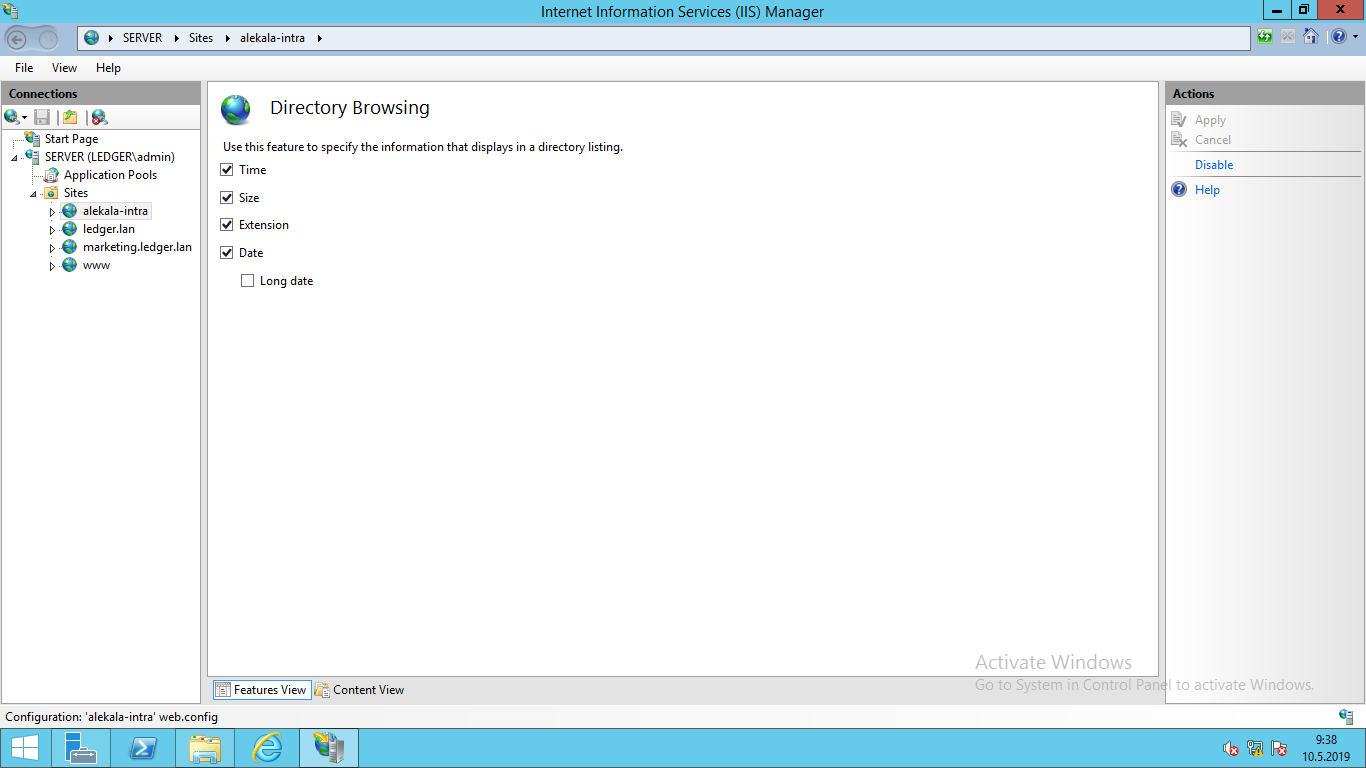
IIS > Sivustosi > Authentication > Providers > Negotiate > Remove



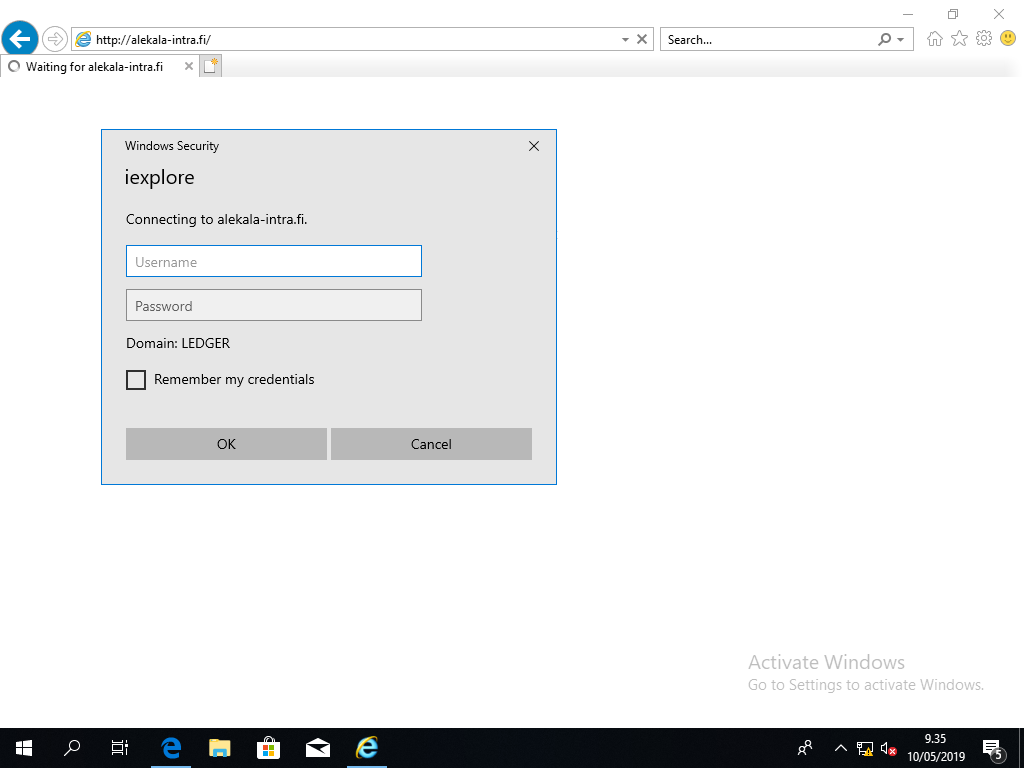
# Directory Browsing / hakemistolistaus

Jos verkkosivuille halutaan myös Directory Browsing, eli tiedostolistaus käyttöön:

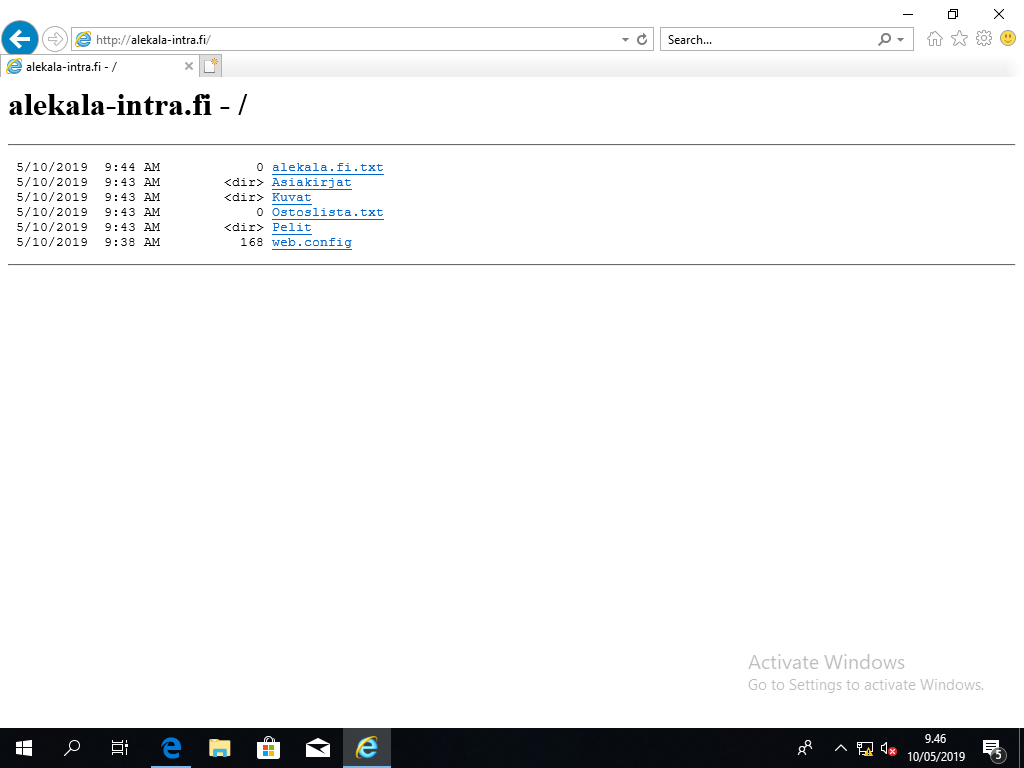
IIS > Sivustosi > Directory Browsing > Enable



Nyt verkkosivuille mentäessä pyydetään autentikaatiota, johon kelpaa tässä tapauksessa Marketing-ryhmän jäsenten tunnukset:



Kun tunnukset on annettu, saamme tiedostolistauksen:

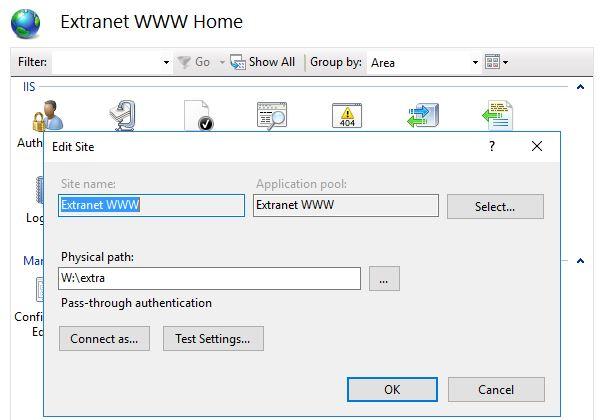


# VirtualHostit / Autentikaatio vain toiselle sivulle

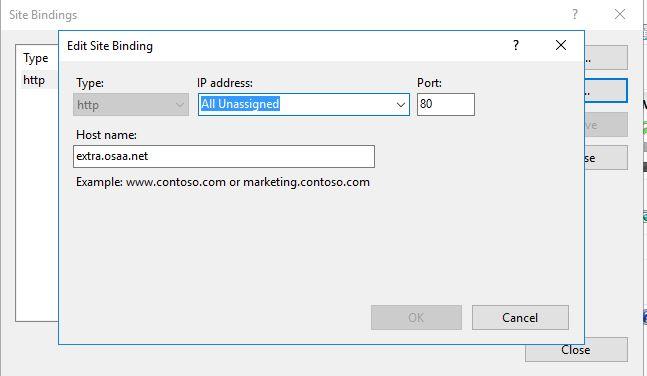
Tehnyt Roope Lajas TITI17AR

Tässä ohjeessa laitetaan toimimaan extra.osaa.net sivusto, joka toimii vain extra nimisellä käyttäjällä.

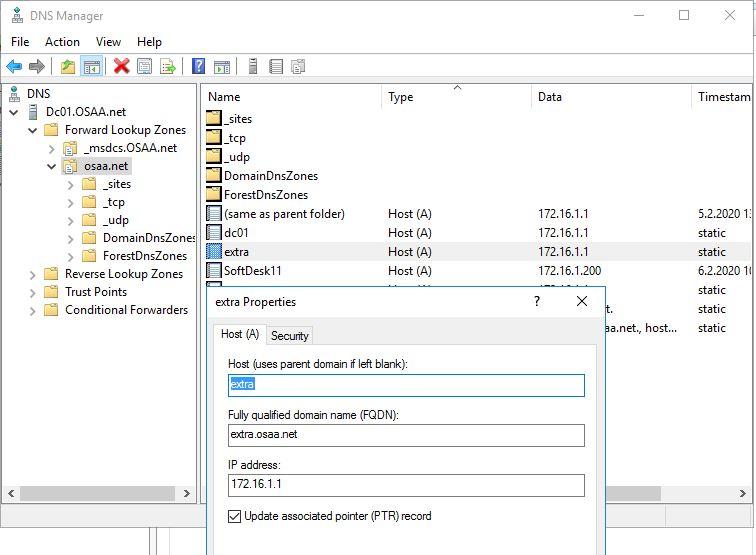
Aluksi luo AD Users and Computers extra niminen käyttäjä ja anna sille salasana. Luo IIS uusi sivusto extra sivua varten. Määritä sen fyysisen polku vaadituksi.



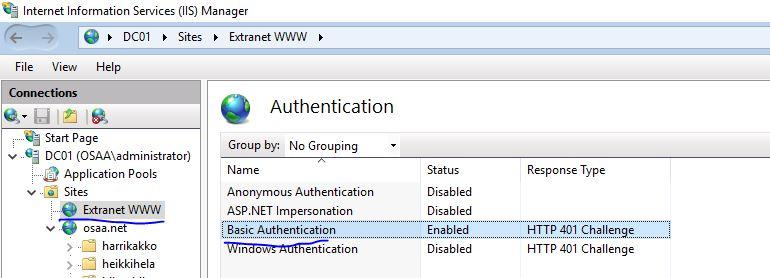
Aseta sille myös Host Nameksi extra.osaa.net:



Koska IIS käytetään Host Name toimintoa tulee meidän tehdä myös vastaava tieto DNS puolelle. Eli tee DNS managerissa osaa.net forward lookup zonen alle uusi A-tietue nimeltään extra jonka IP-osoite on palvelimen IP.



Asenna IIS palveluun Basic Authentication lisäosa Add roles and Features kautta. Sammuta IIS Manager ikkuna ja avaa se uudestaan. Ota käyttöön Basic Authentication extra sivustolle:



Kun teet näin. Sinulla olisi käytössäsi osaa.net sivusto joka toimii aivan normaalisti sekä extra.osaa.net joka vaatii autentikaation ja sijaitsee eri polussa.

Tämä on siis IIS tapa saada VirtualHostit toimimaan.