Handleiding AD FS installatie
Windows Server 2016

Versie: 1.0.0

Inhoudsopgave

Inleiding

In deze handleiding lees je hoe je jouw organisatie kunt aansluiten op SURFconext als Identity Provider met behulp van AD FS (in AD FS-terminologie Claims Provider genoemd).

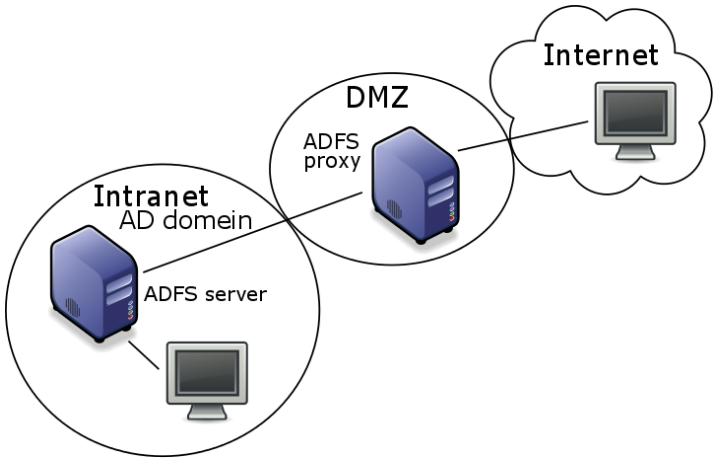
De procedure voor het aansluiten als Identity Provider bestaat uit de volgende onderdelen:

- Een AD FS serversysteem inrichten; waaronder Windows Server 2016 configureren en AD FS installeren.
- De AD FS server configureren voor aansluiting als Identity Provider (IdP) voor SURFconext.
- Een AD FS proxy inrichten indien toegang van buiten het lokale netwerk gewenst is.
- Attributen vrijgeven aan SURFconext

Deze handleiding is gebaseerd op de release van AD FS 4 zoals meegeleverd in Windows Server 2016.

Waarom een server én een proxy inrichten?

Om de AD FS-server minder kwetsbaar te maken voor aanvallen van buitenaf, moet je naast een AD FS server ook een AD FS-proxy inrichten buiten het Windows-domein. De AD FS-server moet namelijk bij voorkeur niet bereikbaar zijn van buitenaf. Je doet dit door een AD FS-proxy in te richten en deze 'voor' de AD FS-server te plaatsen. Dit houdt in dat je twee verschillende Windows Server machines moet configureren in deze setup. De proxy mag geen lid zijn van het domein en wordt bij voorkeur in de DMZ (zie verklarende woordenlijst achterin dit document) geplaatst.



De proxy zorgt ervoor dat gebruikers die niet zijn ingelogd op het (windows-)domain, via een webpagina (username/ password formulier) kunnen inloggen. Dit formulier kan aan de look-and-feel van jouw organisatie worden aangepast.

AD FS 4.0-Server inrichten

Inleiding

Dit document beschrijft de installatie van een AD FS server op Windows Server 2016. Voordat je de specifieke instellingen voor SURFconext kunt invoeren, moet je een basisinstallatie op de AD FS server uitvoeren. Hiervoor moet je onderstaande stappen doorlopen:

- Installeer en configureer Windows Server 2016.
- Voeg de AD FS software als feature toe.
- Configureer de basisinstellingen van AD FS.

Windows Server 2016 installeren en configureren

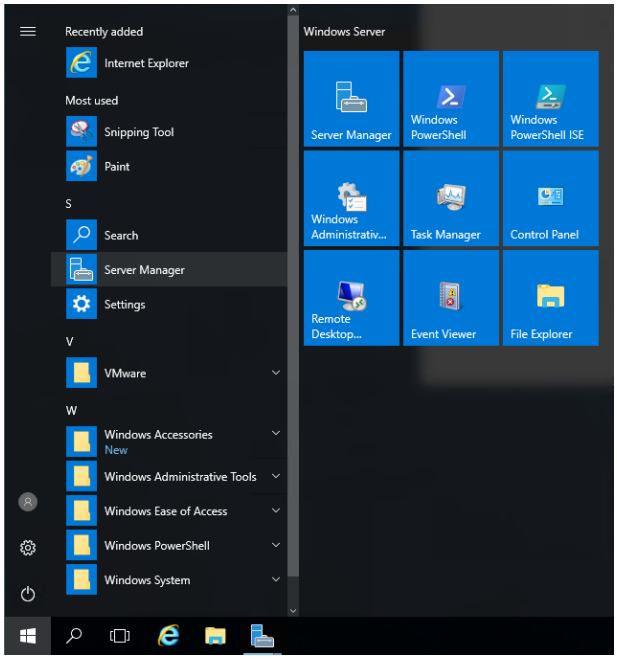
Om een AD FS 4.0-server te kunnen inrichten, moet je eerst Windows Server 2016 installeren en configureren. Deze AD FS 4.0-server dient lid te zijn van een domein. In deze handleiding installeren we de AD DS en AD FS rol op dezelfde server. Hiervoor moet je onderstaande stappen doorlopen:

- Installeer Windows Server 2016 op de server.
- Stel de tijd op de server correct in en zorg ervoor dat je deze synchroniseert met een time server (NTP).
- Neem de server op in het domein van de Active Directory waaruit de accounts voor de SURFconext federatie komen.
- Installeer een geldig certificaat voor de voorgenomen login URL in de Personal Certificate store van de Local Computer ten behoeve van veilige gegevensuitwisseling met de IdP (SSL) . Zie appendix A: Certificaat installeren.

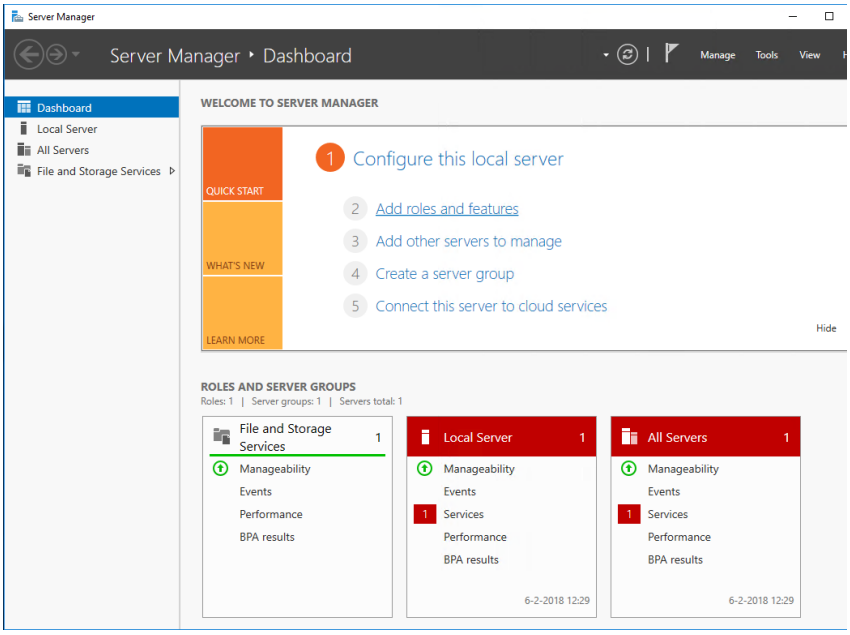
AD DS Server Rol installeren

Onderstaand gedeelte van deze handleiding is te gebruiken voor het installeren van de AD FS Server Role op Windows Server 2016

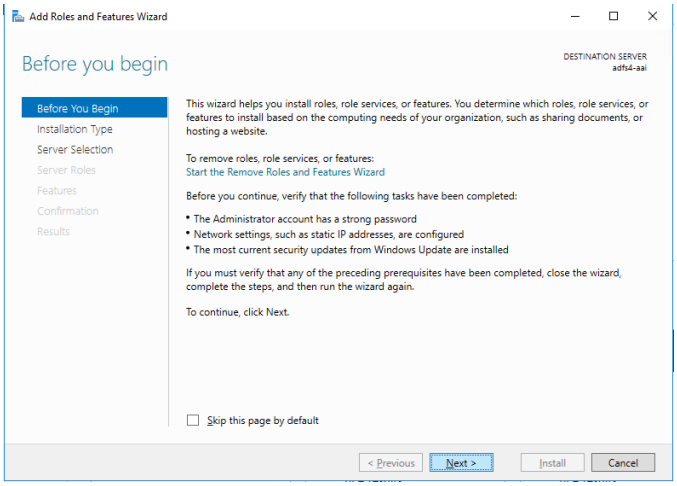
1. Start de Server Manager tool op de machine die als Domain Controller ingericht wordt.



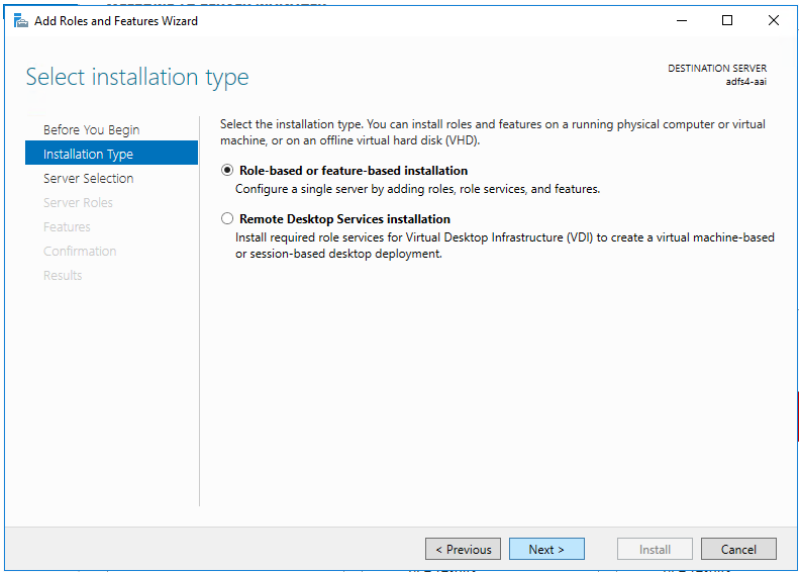
2. Klik op “Add Roles and Features”.



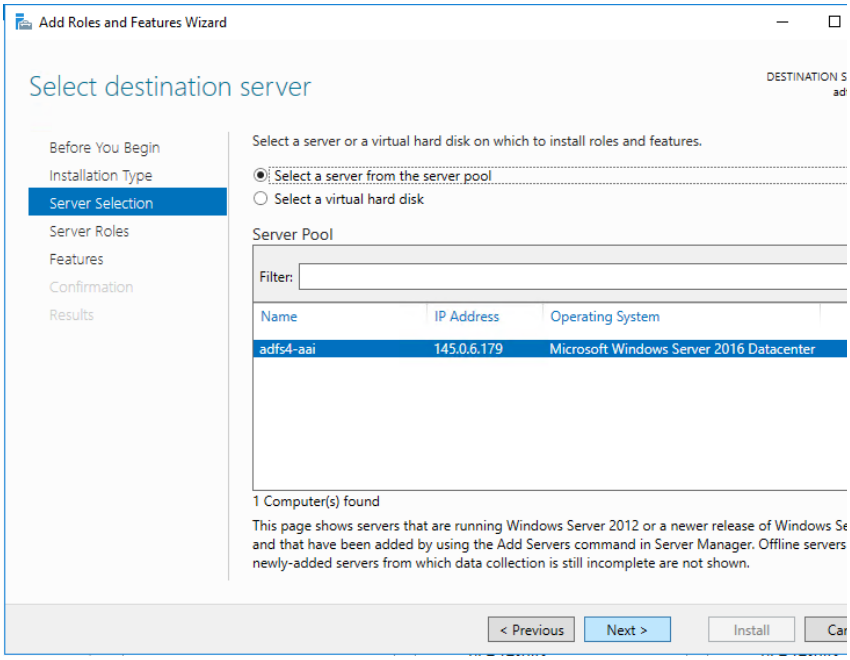
3. Klik op “Next >”



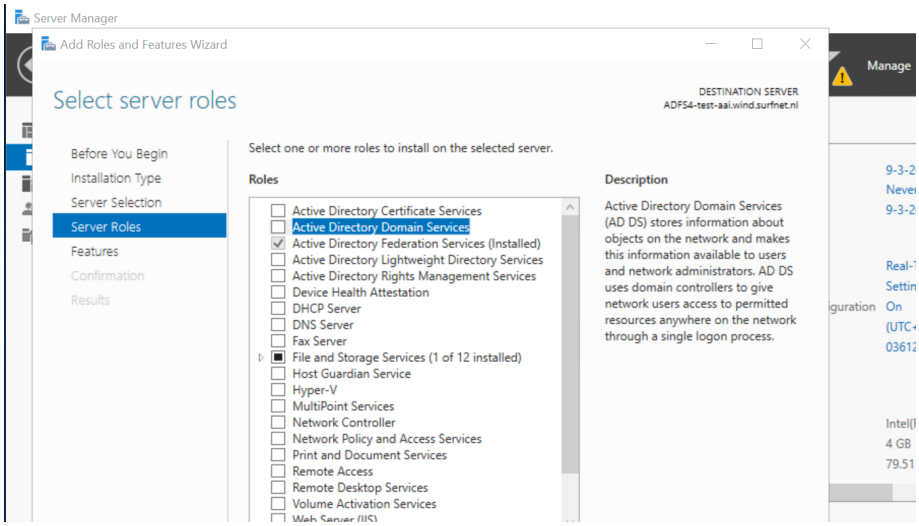
4. Klik op “Role-based or feature-based installation” en klik op “Next >”:



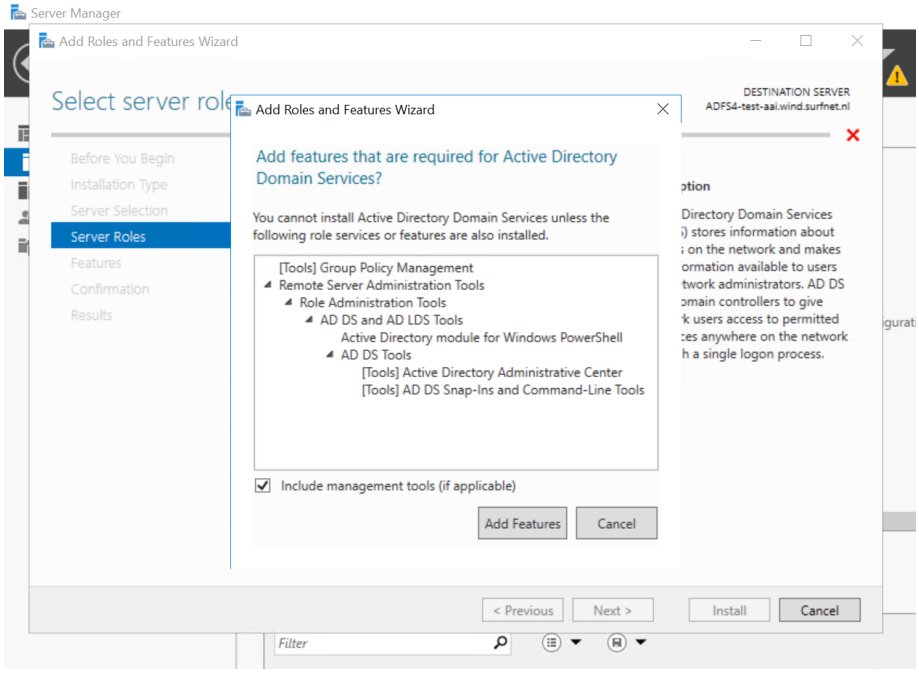
5. Selecteer “Select a server from the server pool”, kies de juiste server en klik op “Next >”:



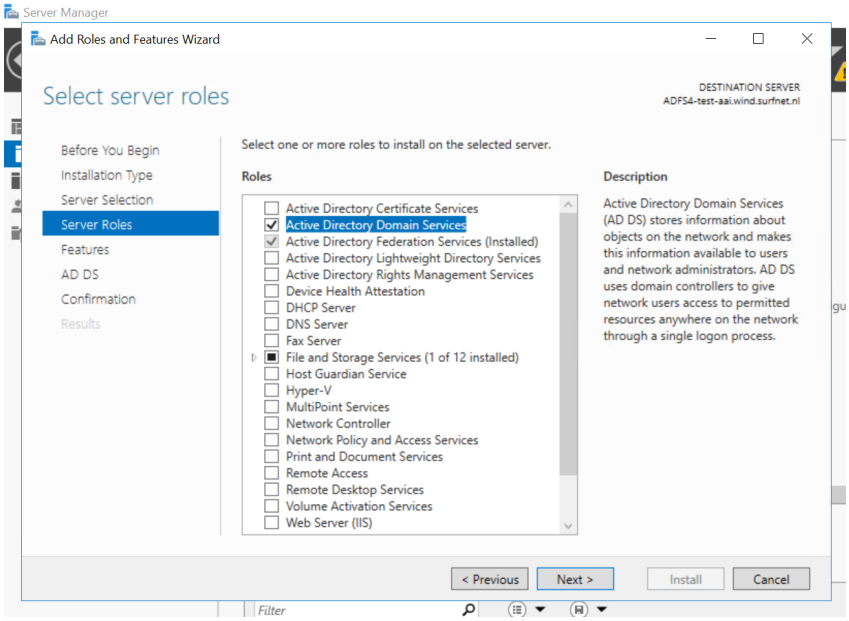
6. Selecteer Active Directory Domain Services



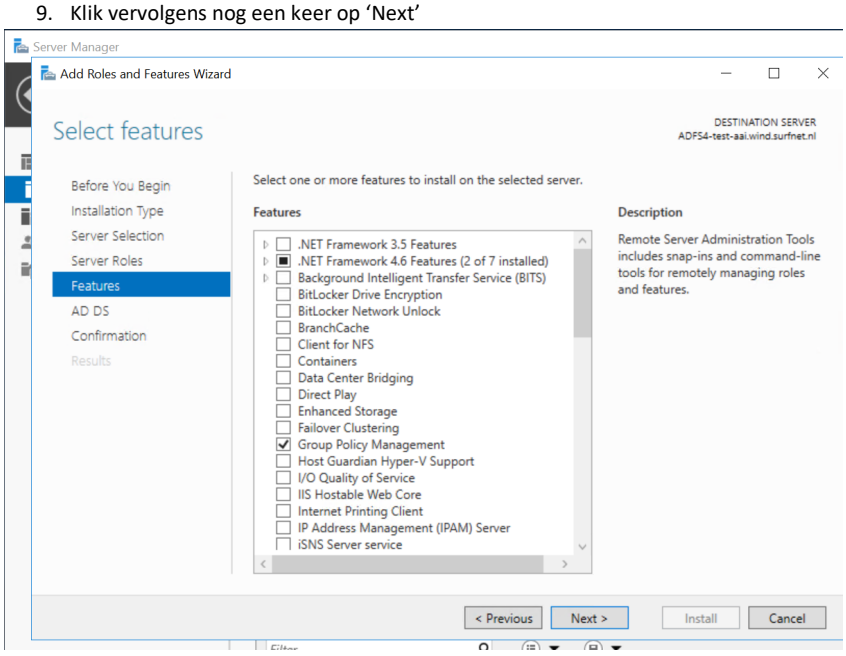
7. Klik vervolgens op ‘Add Features’



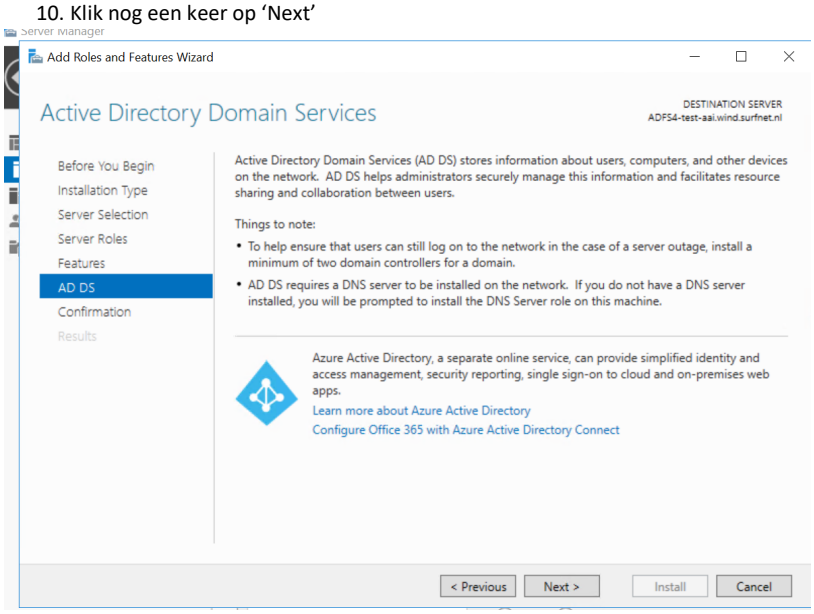
8. Klik op ‘Next’



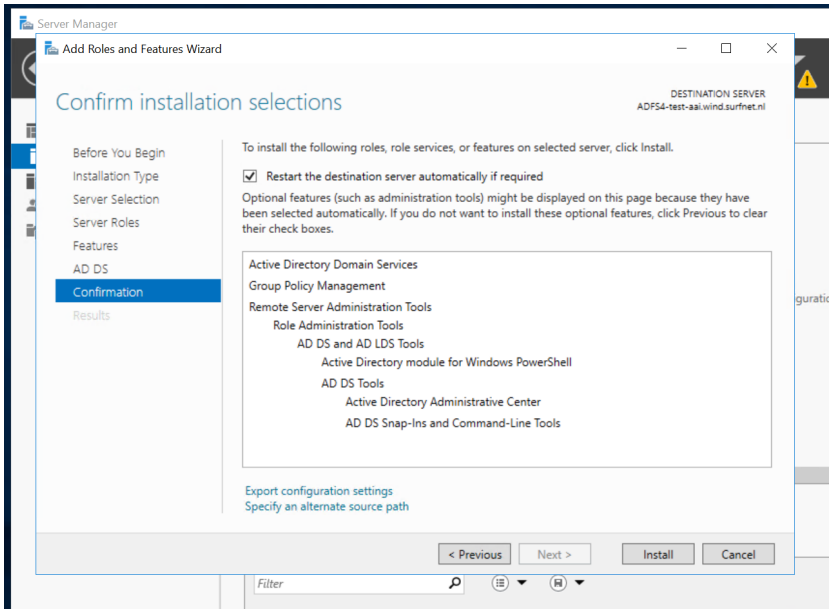
9. Klik vervolgens nog een keer op ‘Next’



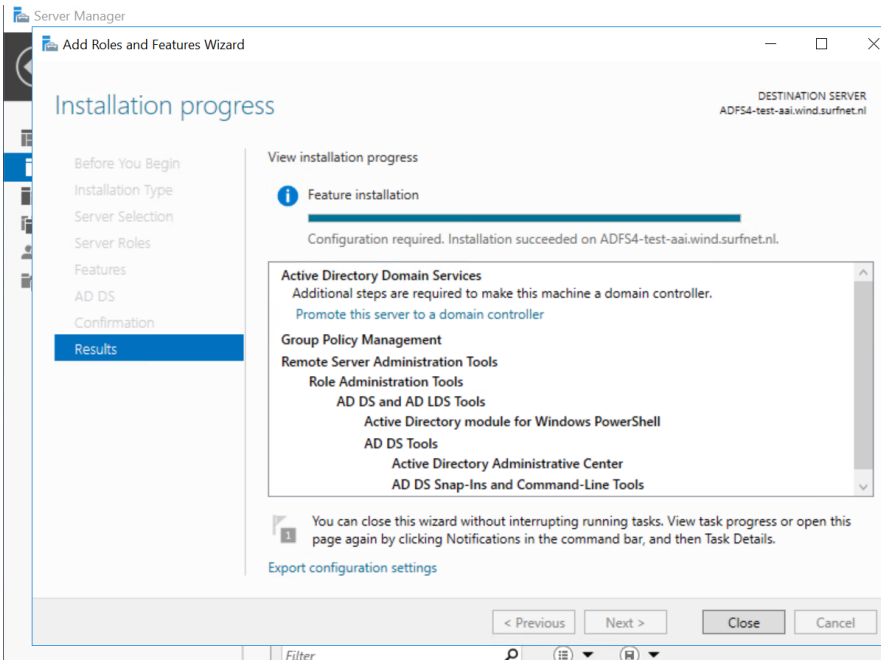
10. Klik nog een keer op ‘Next’



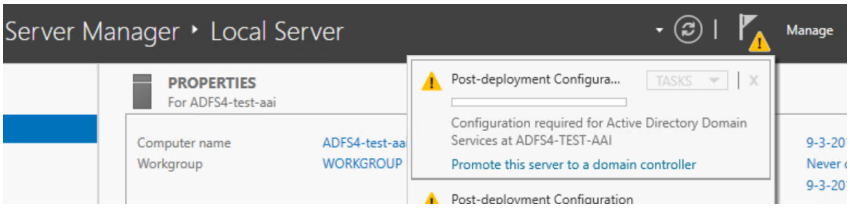
11. Vink het ‘Restart the destination server automatically if required’ vinkje aan en klik op ‘Install’.



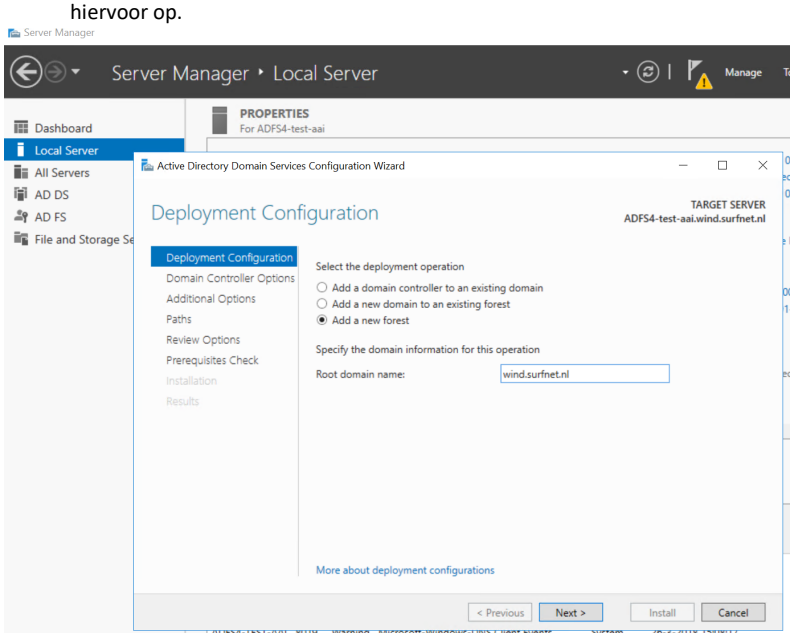
12. Klik op ‘Close’ wanneer de installatie succesvol is verlopen



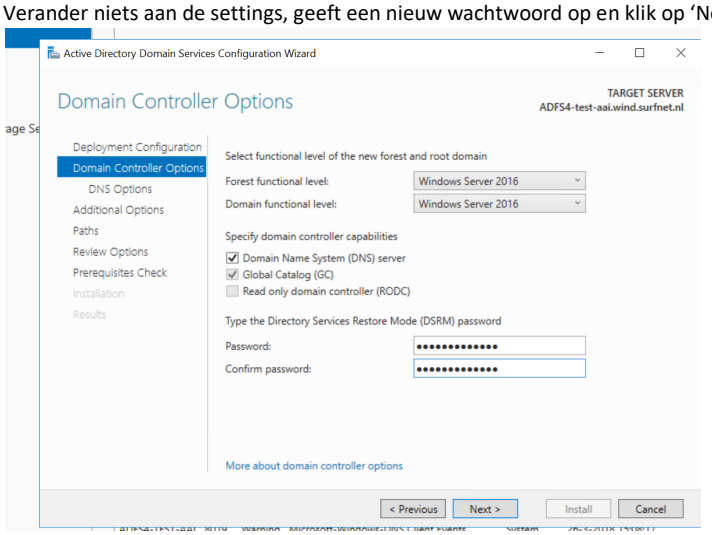
13. Klik in de Servermanager op het vlaggetje voor meldingen en kies voor de Post-deployment actie ‘Promote this server to a domain controller’



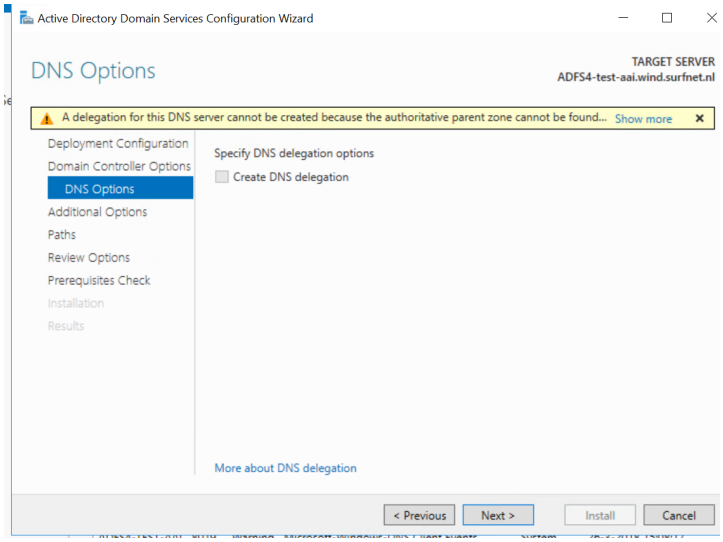
14. In deze stap kan je kiezen of de machine wordt toegevoegd aan een bestaand domein of niet. Wij kiezen er in deze stap voor om een nieuwe forest aan te maken en geven de naam hiervoor op.



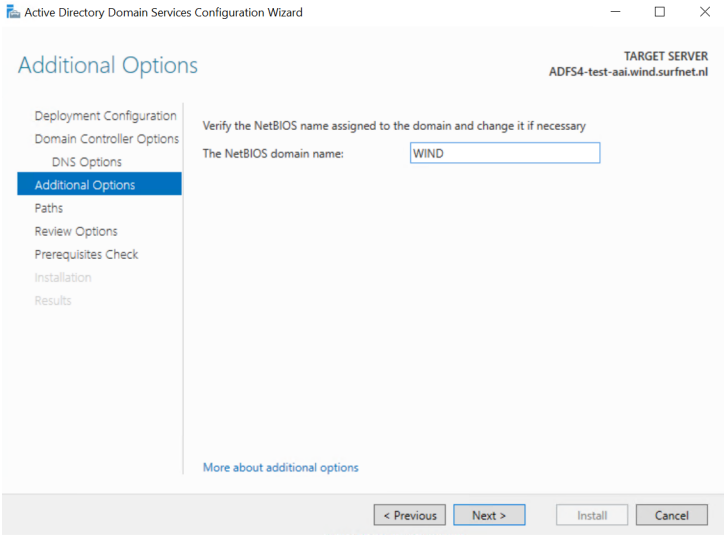
15. Verander niets aan de settings, geeft een nieuw wachtwoord op en klik op 'Next'



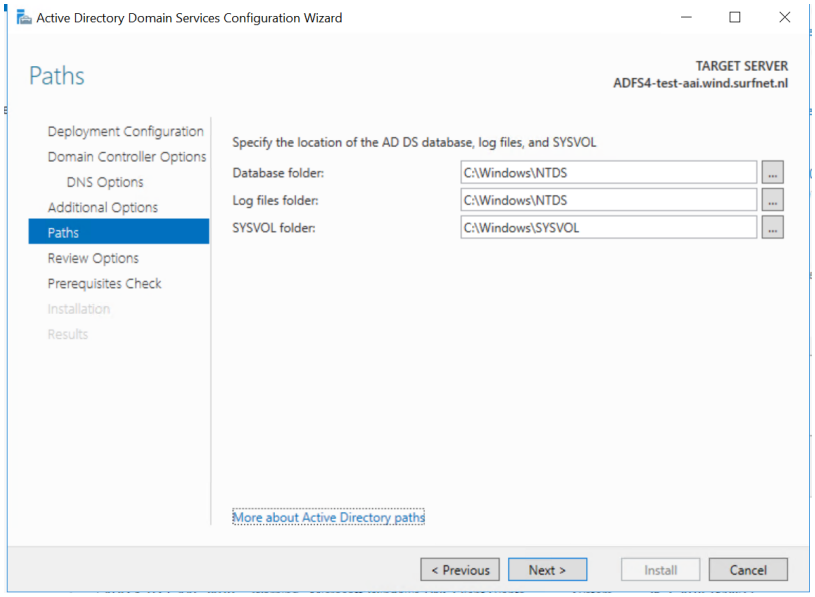
16. Klik in deze stap op ‘Next’



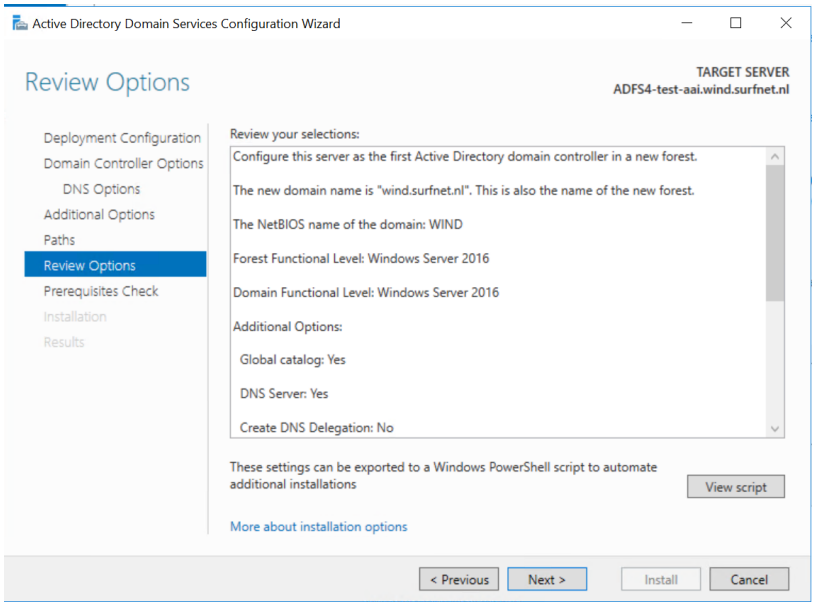
17. Controleer of de NETBIOS naam voor het domein klopt of pas hem aan naar de juiste en klik op ‘Next’



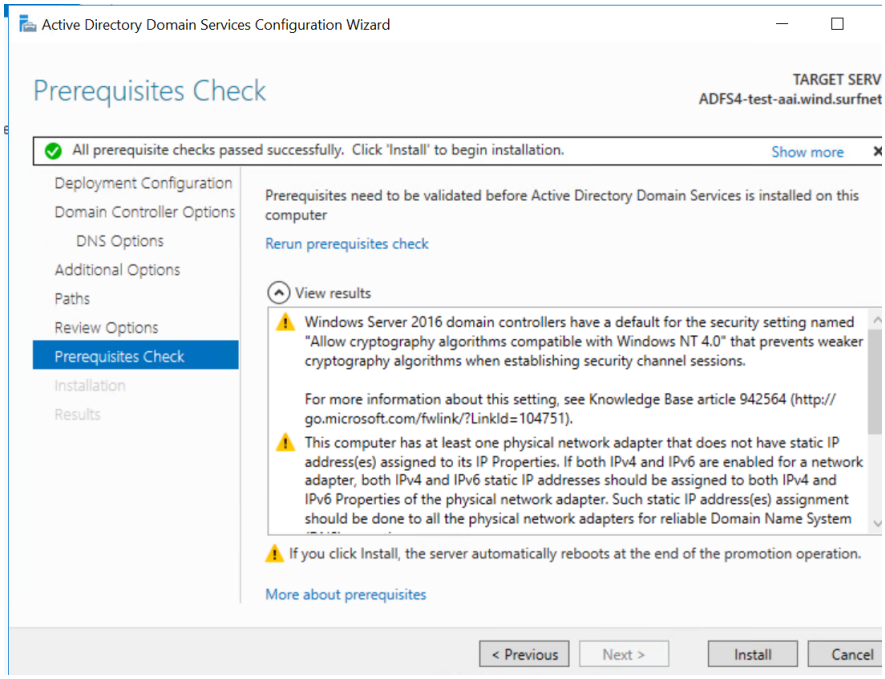
18. In deze stap kan u de diverse paden wijzigen. Wij laten deze ongewijzigd en klikken hier op ‘Next’



19. Er wordt een overzicht van de instellingen gegenereerd. Klik in deze stap op ‘Next’



20. Wij krijg een aantal warnings, die wij in deze situatie mogen en kunnen negeren. Klik in deze stap op de knop ‘Install’

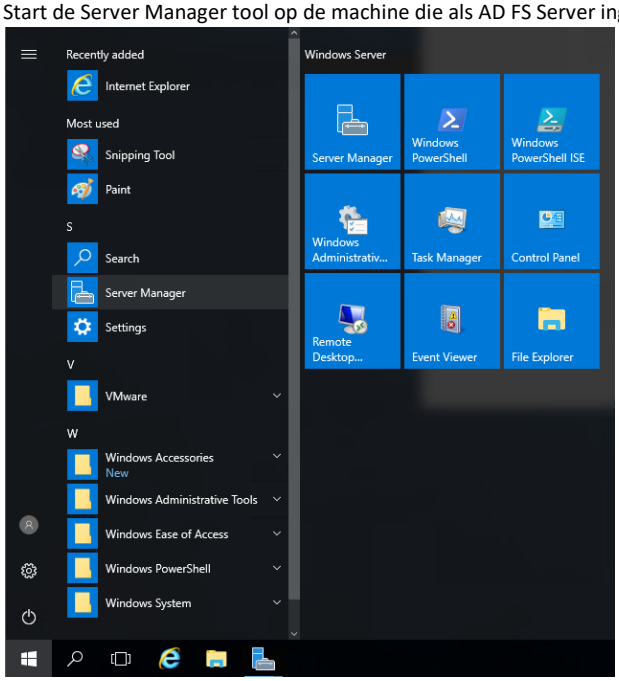


21. De server zal een keer opnieuw opstarten en vanaf nu is uw server een Domain Controller en onderdeel van een domein.

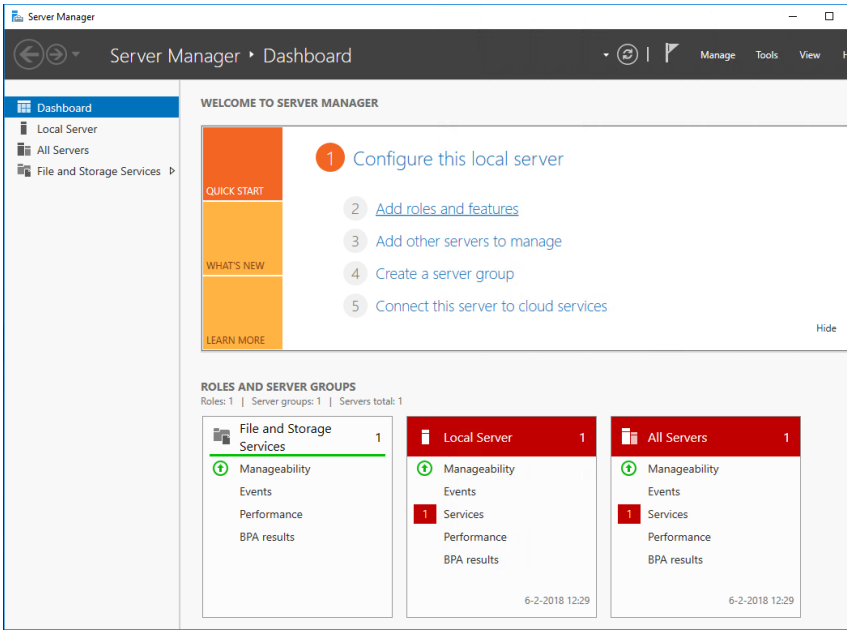
AD FS Server Software installeren

Onderstaand gedeelte van deze handleiding is te gebruiken voor het installeren van de AD FS Server Role op Windows Server 2016.

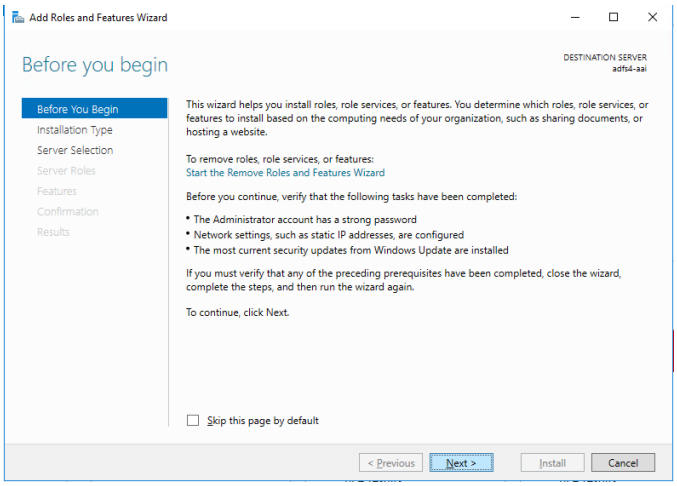
1. Start de Server Manager tool op de machine die als AD FS Server ingericht wordt.



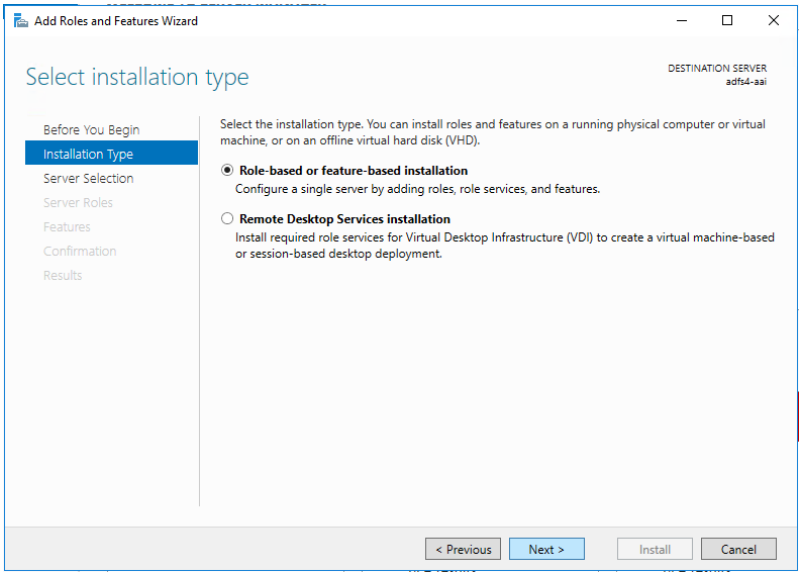
2. Klik op “Add Roles and Features”.



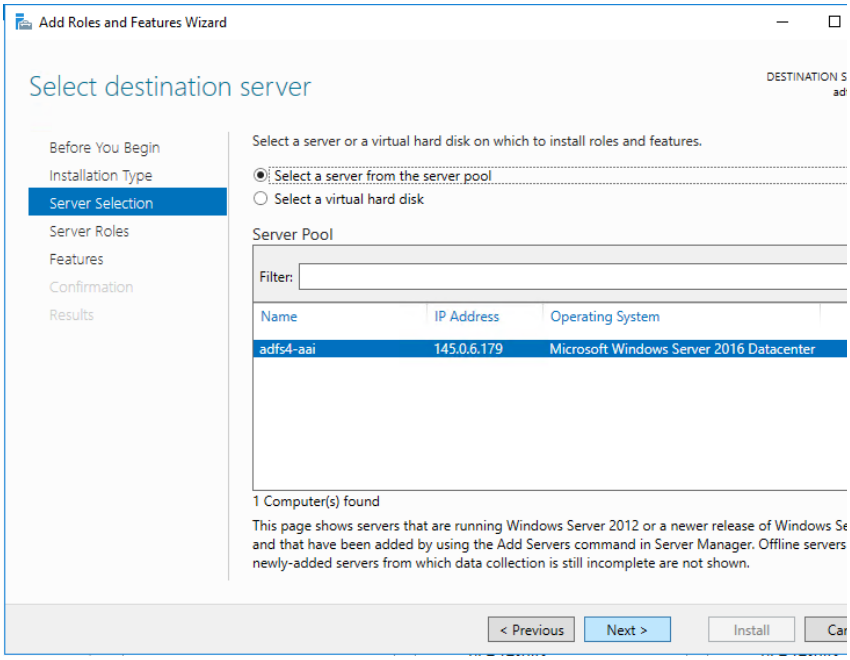
3. Klik op “Next >”



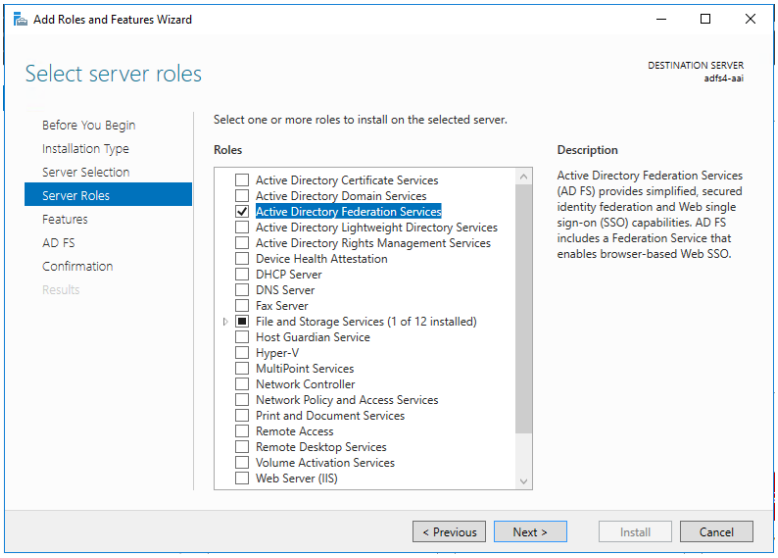
4. Klik op “Role-based or feature-based installation” en klik op “Next >”:



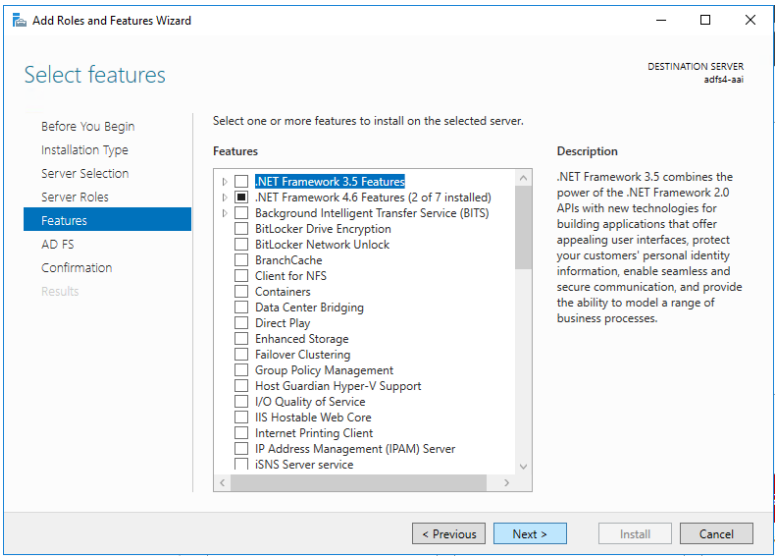
5. Selecteer “Select a server from the server pool”, kies de juiste server en klik op “Next >”:



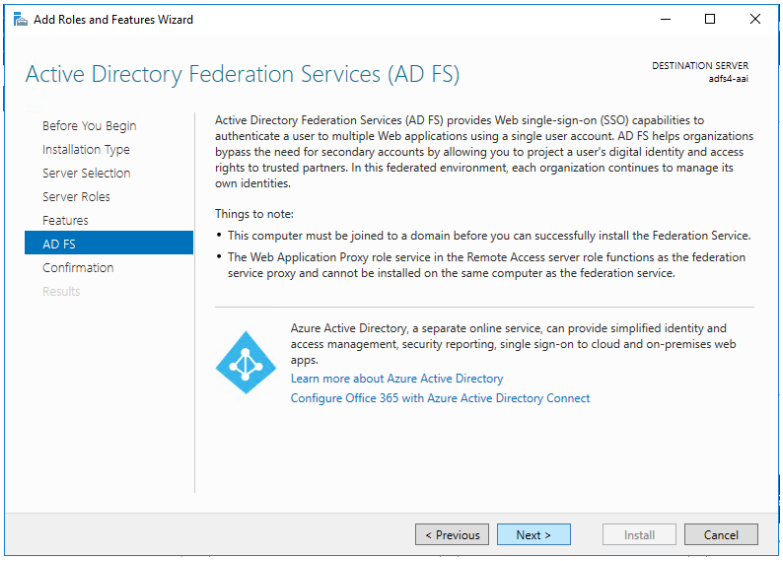
6. Selecteer “Active Directory Federation Services” en klik op “Next >”:



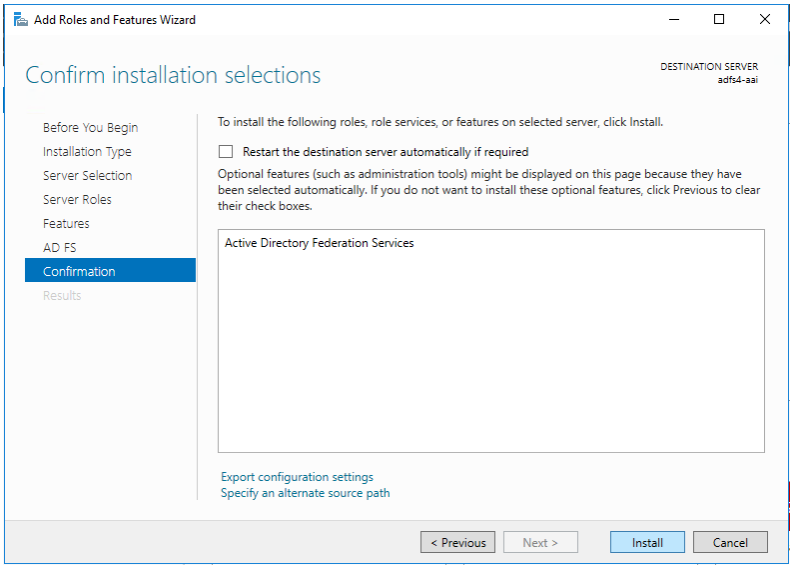
7. Klik “Next >” in het Features overzicht:



8. Klik op “Next >”:

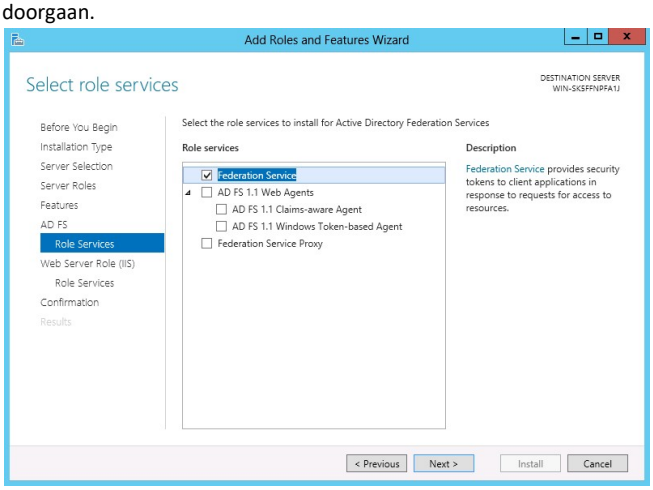


9. Klik op “Install”:

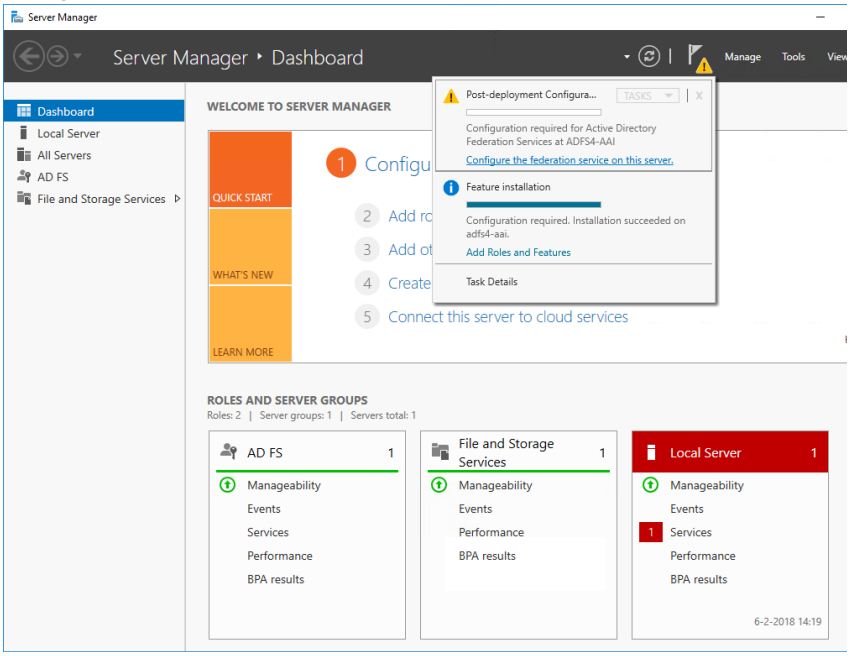


10. Wacht eventueel tot de installatie afgerond is. De wizard mag afgesloten worden, de installatie zal op de achtergrond

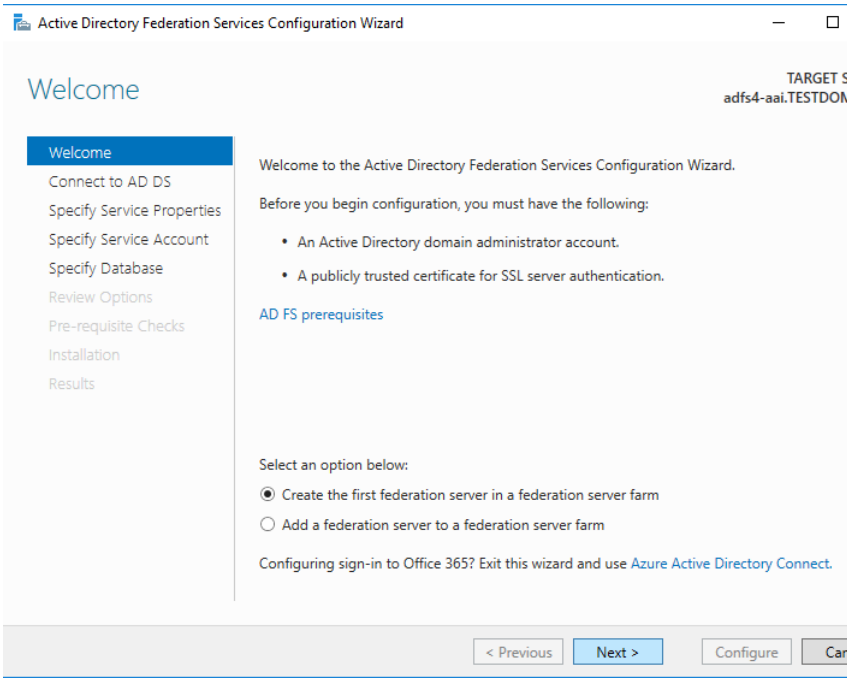
doorgaan.


Add Roles and Features Wizard
Select role services
DESTINATION SERVER
WIN-SKSFFNPFA1J
Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Role Services
Web Server Role (IIS)
Role Services
Confirmation
Results
Select the role services to install for Active Directory Federation Services
Role services
Federation Service
AD FS 1.1 Web Agents
AD FS 1.1 Claims-aware Agent
AD FS 1.1 Windows Token-based Agent
Federation Service Proxy
Description
Federation Service provides security tokens to client applications in response to requests for access to resources.
< Previous
Next >
Install
Cancel

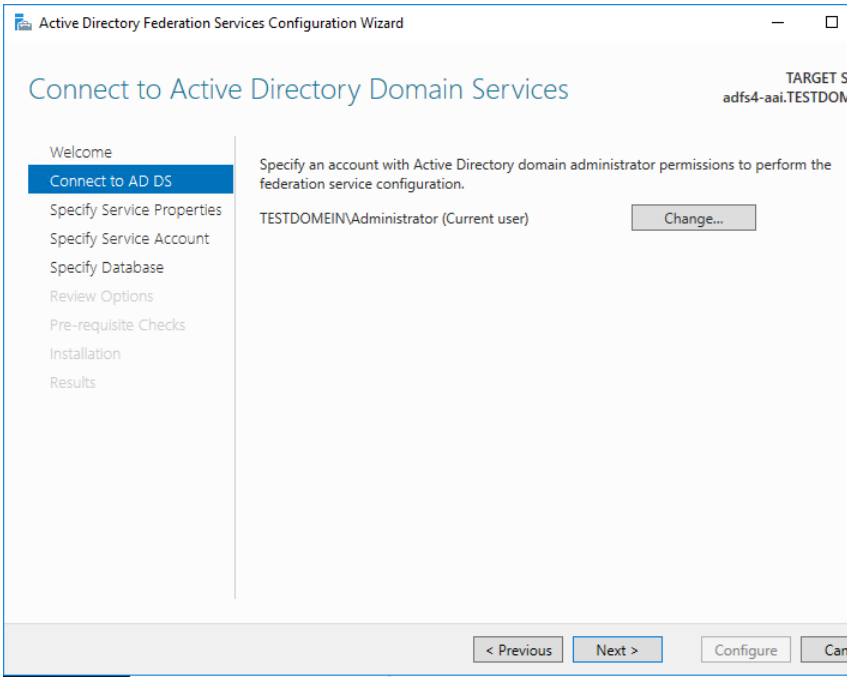
11. Als de installatie afgerond is zal er een “Post-deployment” waarschuwing “Configuration required for Federation Service at ...” verschijnen in het Server Manager Dashboard. Klik op “Configure the federation service on this server” om de installatie van AD FS te voltooien.



12. Klik “Next > “in het eerste scherm:

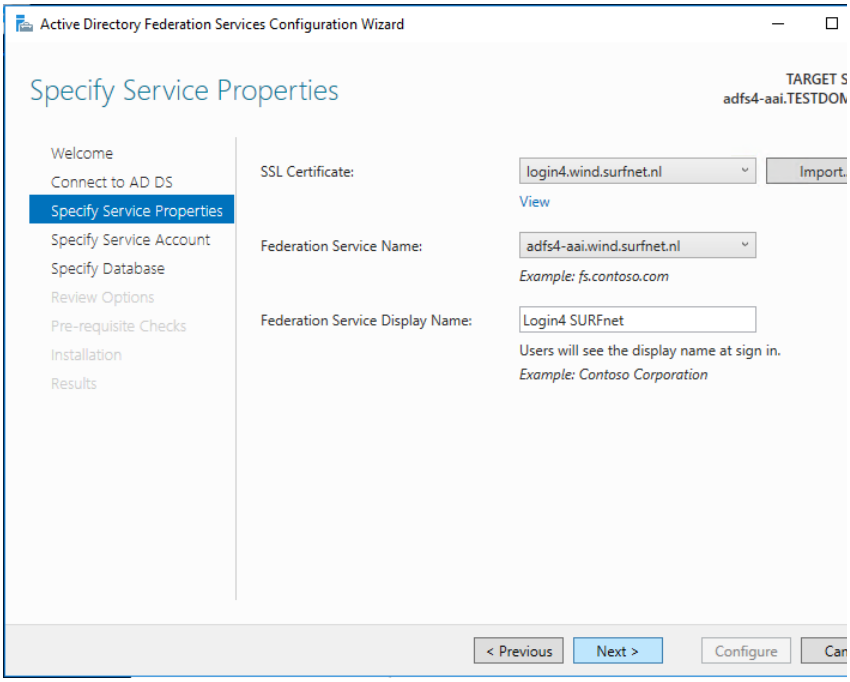


13. Kies het AD Administrator account en klik op “Next > “:

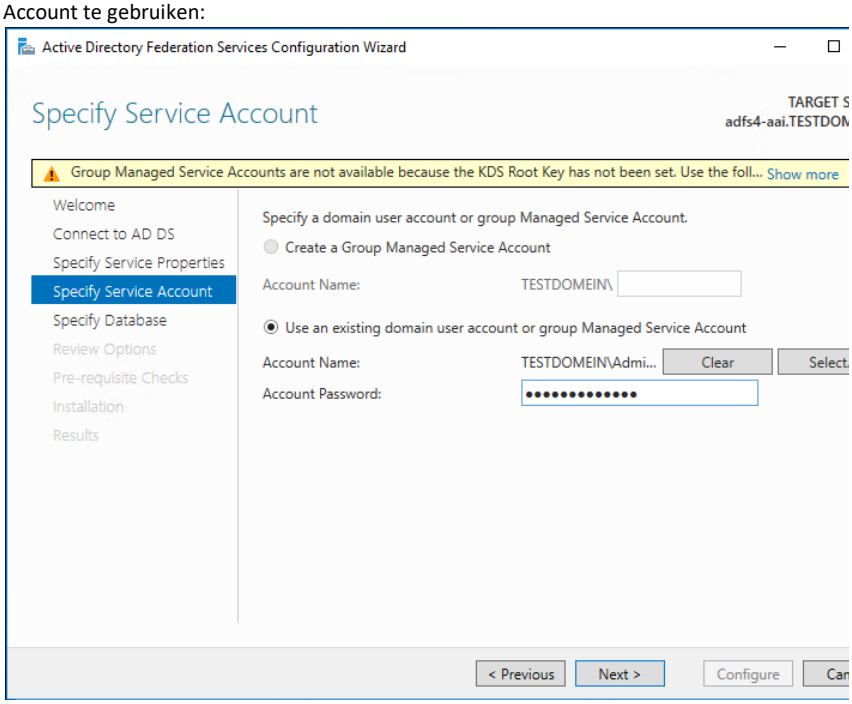


14. Kies het vooraf geïnstalleerde SSL certificaat (Appendix A) waarmee de AD FS dienst ontsloten zal worden en een handige “Displayname” bijvoorbeeld Login SURFnet). Klik op

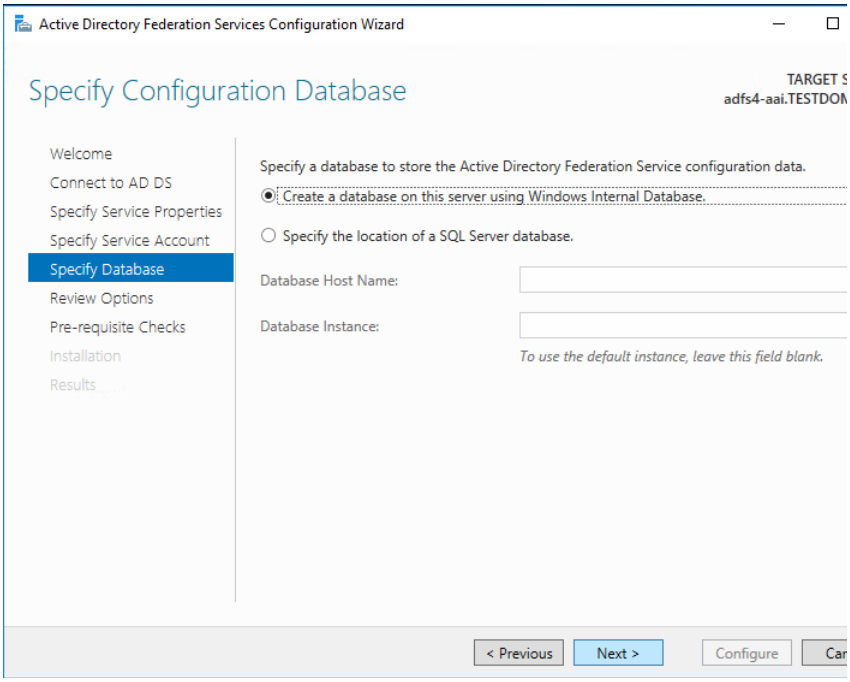
“Next >”:


Active Directory Federation Services Configuration Wizard
Specify Service Properties
TARGET S
adfs4-aai.TESTDOM
Welcome
Connect to AD DS
Specify Service Properties
Specify Service Account
Specify Database
Review Options
Pre-requisite Checks
Installation
Results
SSL Certificate:
login4.wind.surfnet.nl
Import.
View
Federation Service Name:
adfs4-aai.wind.surfnet.nl
Example: fs.contoso.com
Federation Service Display Name:
Login4 SURFnet
Users will see the display name at sign in.
Example: Contoso Corporation
< Previous
Next >
Configure
Can

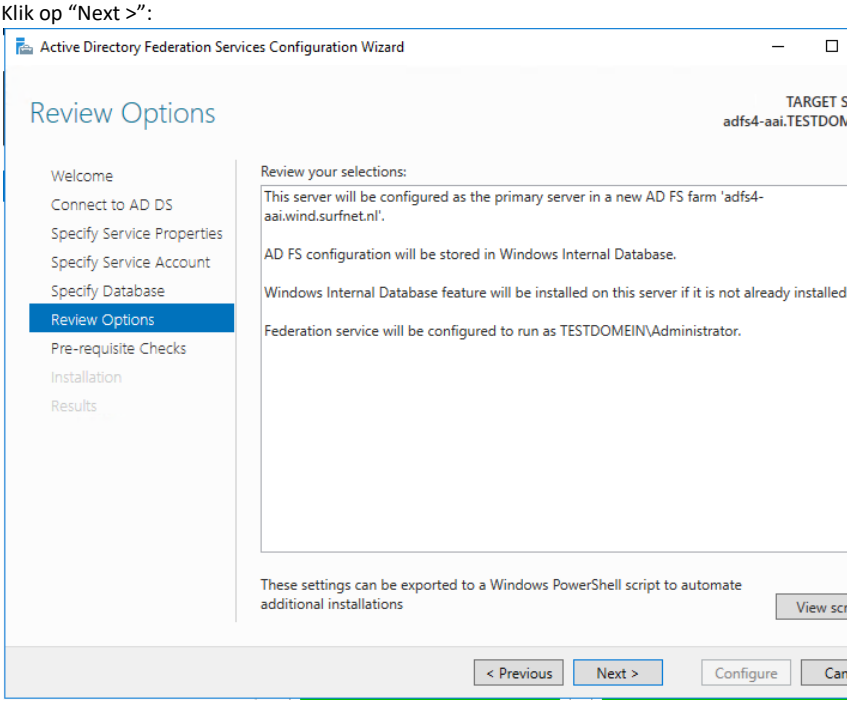
15. De waarschuwing in de gele balk kan opgelost worden door op Show more” te klikken en het voorgestelde commando “Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)” in een Powershell uit te voeren. Kies voor een eenvoudige installatie een domain Administrator account voor het installeren van de AD FS service. Uit veiligheidsoogpunt en voor de beheersbaarheid kan er voor worden gekozen om een Group Managed Service Account te gebruiken:



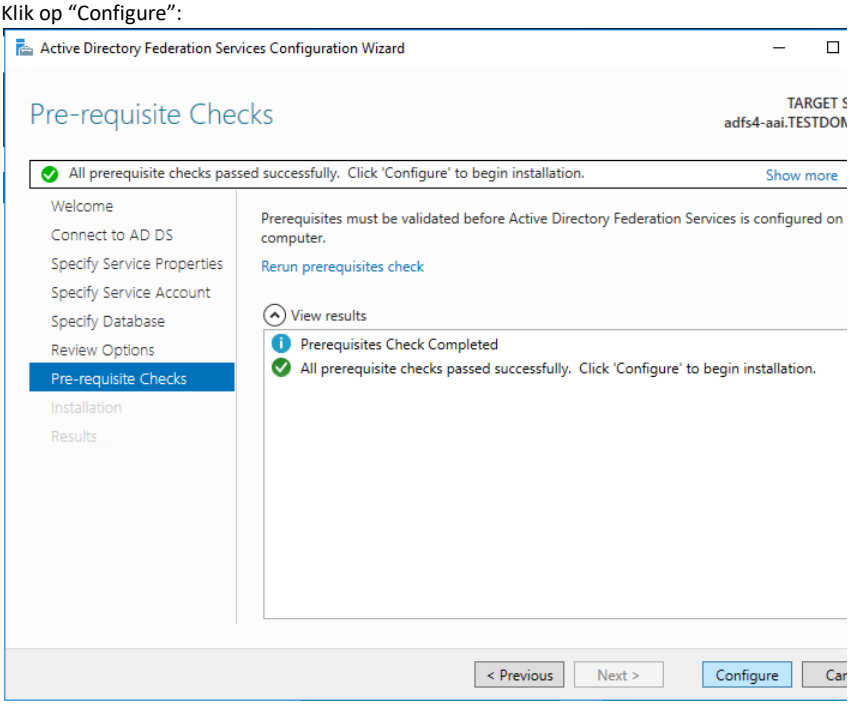
16. Selecteer “Create a database on this server using Windows Internal Database.” en klik op “Next >”:



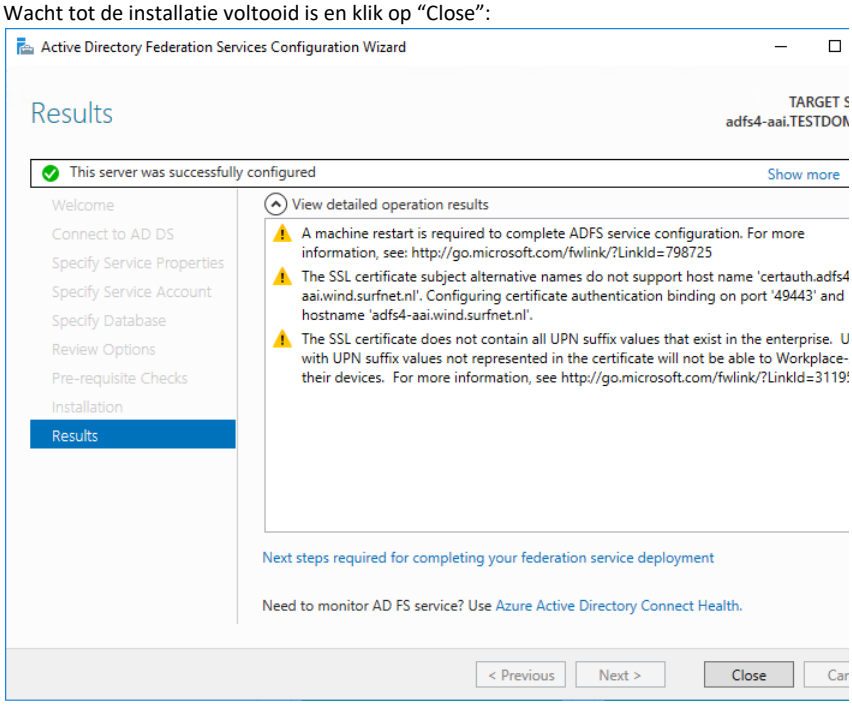
17. Klik op “Next >”:



18. Klik op “Configure”:



19. Wacht tot de installatie voltooid is en klik op “Close”:



20. Om verder te gaan zijn er claim beschrijvingen nodig. “step 4” op de wiki (https://wiki.surfnet.nl/display/services/Configure+Office+365+with+AD FS+and+SURFconext+Step-by-Step) is hierbij nodig. Open PowerShell en voer de volgende commando’s uit:

Claim description PowerShell

```
############################################## Create AD FS Claim Descriptions
##############################################
#### ADD UID CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:uid -ClaimType
urn:mace:dir:attribute-def:uid -ShortName uid -IsAccepted $false -IsOffered $false

#### ADD MAIL CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:mail -ClaimType
urn:mace:dir:attribute-def:mail -ShortName mail -IsAccepted $false -IsOffered $false

#### ADD DISPLAYNAME CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:displayName -ClaimType
urn:mace:dir:attribute-def:displayName -ShortName displayName -IsAccepted $false -
IsOffered $false
```

```
#### ADD schacHomeOrganization CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name schacHomeOrganization -ClaimType
 urn:mace:terena.org:attribute-def:schacHomeOrganization -ShortName
 schacHomeOrganization -IsAccepted $true -IsOffered $true

#### ADD eduPersonAffiliation CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:eduPersonAffiliation -
 ClaimType urn:mace:dir:attribute-def:eduPersonAffiliation -ShortName eduPersonAffiliation
 -IsAccepted $true -IsOffered $true

#### ADD eduPersonEntitlement CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:eduPersonEntitlement -
 ClaimType urn:mace:dir:attribute-def:eduPersonEntitlement -ShortName
 eduPersonEntitlement -IsAccepted $false -IsOffered $false

#### ADD employeeNumber CLAIM DESCRIPTION ####
Add-AD FSClaimDescription -Name urn:mace:dir:attribute-def:employeeNumber -ClaimType
 urn:mace:dir:attribute-def:employeeNumber -ShortName employeeNumber -IsAccepted
 $false -IsOffered $false
```

21. Step 5 in de wiki beschrijft het toevoegen van de “SURFconext Relying Party Trust”.
    Download het configuratiebestand: ClaimIssuanceRules.txt
22. De url van de metadata ($MetaDataURL) is afhankelijk op welke omgeving van SURFconext wordt aangesloten (productie-, acceptatie- (pre-productie) of testomgeving):
    a. De "productie omgeving van SURFconext" tbv productie diensten en productie IdP's; De Public SAML metadata (de entity descriptor) van de SURFconext SP Proxy voor deze omgeving staat op https://engine.surfconext.nl/authentication/sp/metadata
    b. De "acceptatie (pre-productie) omgeving van SURFconext" tbv de acceptatie van diensten en IdP's die naar de "productie omgeving van SURFconext" moeten worden omgezet. De "acceptatie (pre-productie) omgeving van SURFconext" gebruikt hetzelfde SAML endpoint met dezelfde SAML metadata als de productie omgeving van SURFconext.
       De "acceptatie (pre-productie) omgeving van SURFconext" en de "productie omgeving van SURFconext" zijn galvanisch van elkaar gescheiden wat wil zeggen dat een IdP die is aangesloten op de "productie omgeving van SURFconext" niet gekoppeld kan worden aan een dienst die is aangesloten op de "acceptatie (pre-productie) omgeving van SURFconext" en visa versa.
    c. De "test omgeving van SURFconext" tbv het aansluiten van nieuwe diensten & IdP's. Deze omgeving heeft eigen SAML endpoint en staat geheel los van de "productie omgeving van SURFconext" en de "acceptatie (pre-productie) omgeving van SURFconext".

    De Public SAML metadata (de entity descriptor) van de SURFconext IdP Proxy voor deze omgeving staat op: https://engine.connect.surfconext.nl/authentication/sp/metadata

    Zie ook: https://wiki.surfnet.nl/display/surfconextdev/Environments

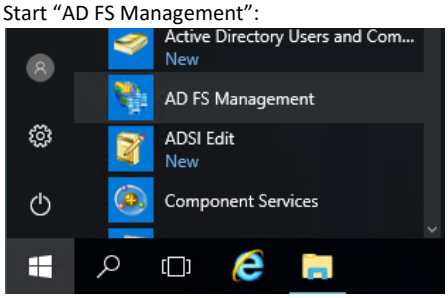
23. Kopieer onderstaande PowerShell commando's en voer deze uit nadat bij $MetaDataURL de juiste url is ingesteld (22.) en $ClaimIssuanceFile het pad naar het zojuist gedownloade bestand is ingesteld

PowerShell Create SURFconext Relying Party Trust

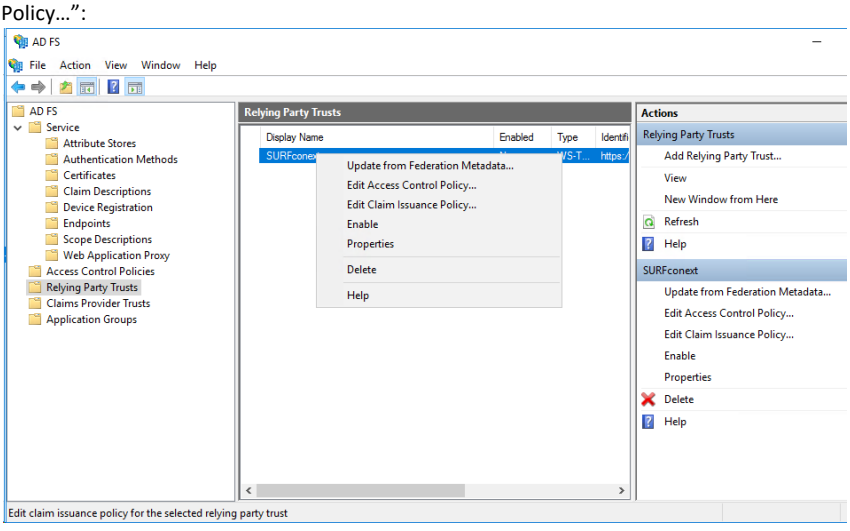
```
#### CREATE SURFCONEXT RELYING PARTY TRUST ####
$RelyingPartyTrustName = "SURFconext"
$MetaDataURL = "https://engine.surfconext.nl/authentication/sp/metadata"
$ClaimIssuanceFile = "THE LOCATION OF YOUR CLAIM ISSUANCE RULE FILE"
$ACPName = "Permit everyone"

Add-AD FSRelyingPartyTrust -Name $RelyingPartyTrustName -
MetadataUrl $MetaDataURL -IssuanceTransformRulesFile $ClaimIssuanceFile -
AutoUpdateEnabled:$true -MonitoringEnabled:$true -
AccessControlPolicyName $ACPName
```

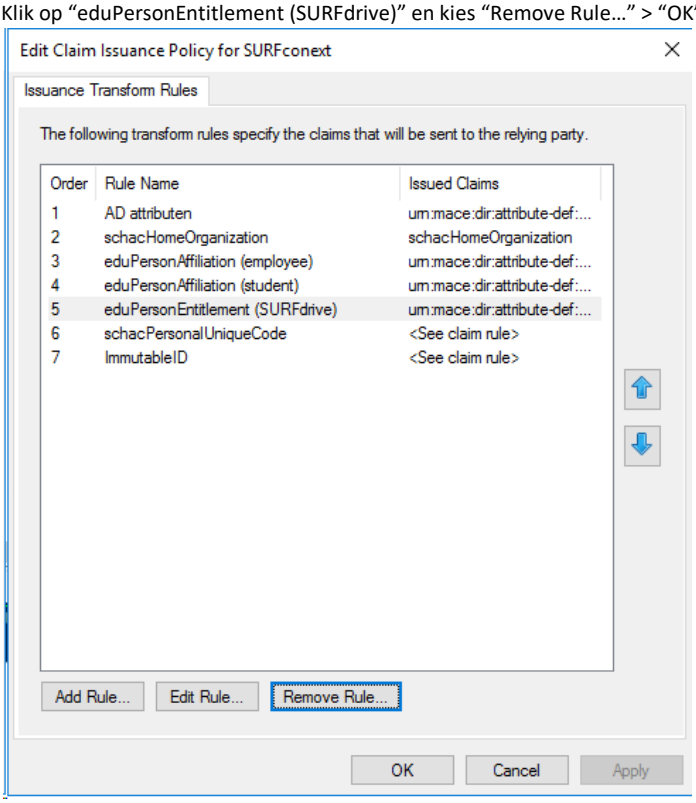
24. Start "AD FS Management":



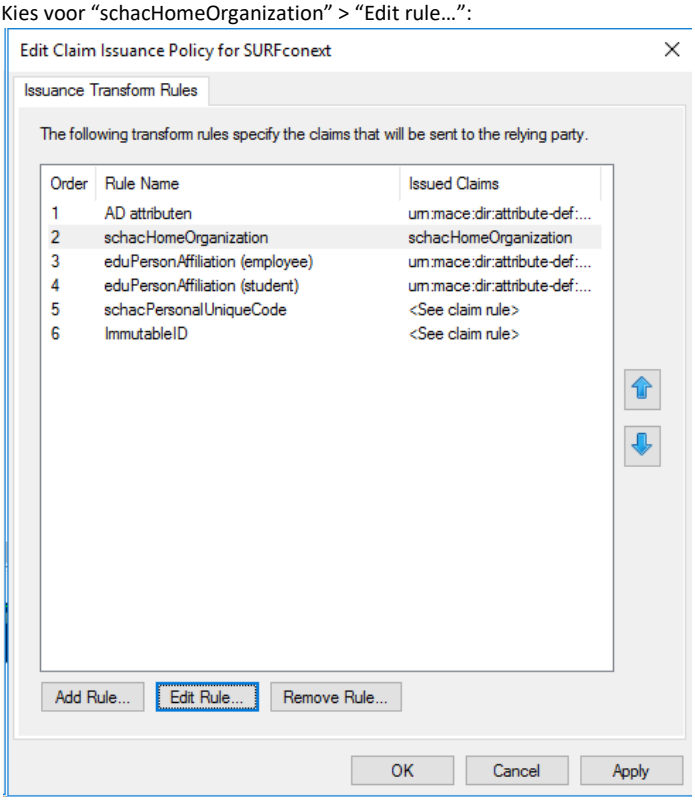
25. Ga naar "Relying Party Trust" en klik rechts op "SURFconext" > "Edit Claim Issuance Policy…":



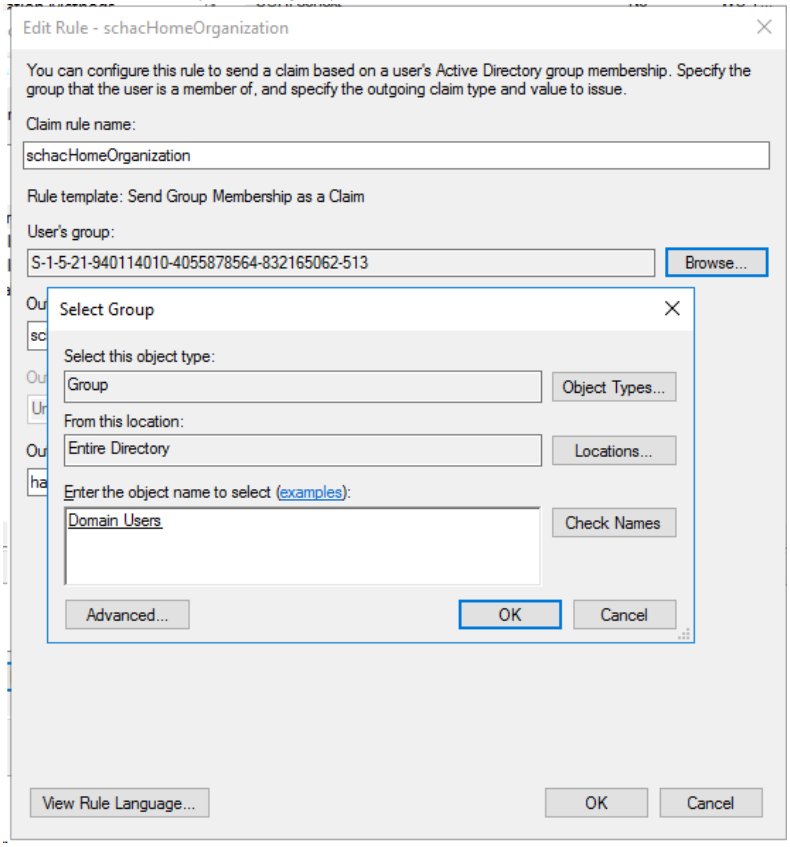
26. Klik op “eduPersonEntitlement (SURFdrive)” en kies “Remove Rule…” > “OK”:



27. Kies voor “schacHomeOrganization” > “Edit rule…”:



28. Kies voor “Browse” bij “User’s group” en vul “Domain Users” in > “OK” en weer “OK”:



29. Doe hetzelfde voor de eduPersonAffiliation Student en Employee. Vul daar bij Student de studenten AD groep in. Bij Employee de medewerkers AD groep. Indien deze AD groepen nog niet bestaan maak deze dan aan. En Klik “OK” om dit scherm te sluiten.
30. Custom claim rules
    Het kan voorkomen dat de gewenste waarde van een bepaald attribuut niet beschikbaar is in AD maar wel daaruit afgeleid zou kunnen worden. Een voorbeeld is schacPersonalUniqueCode. De vereiste syntax van dit attribuut is

    urn:schac:personalUniqueCode:nl:local:<schacHomeOrganisation>:<id_type>:<id_token>

    Let op dat de waarde een URN is en daarom moet voeldoen aan de eisen die aan een URN gesteld worden. Een belangrijke eis is dat een URN geen spaties mag bevatten.

    Bijvoorbeeld:

    urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:90210

Hiervan is het employeeid “90210” waarschijnlijk wel beschikbaar als medewerkernummer en kan het attribuut dus samengesteld worden uit de tekst

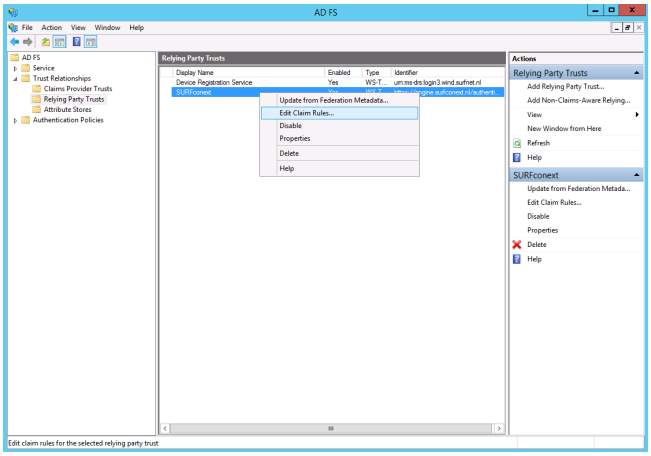
“urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:”

en bijvoorbeeld

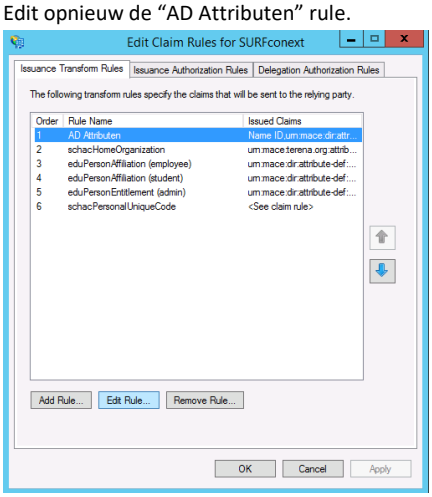
(de waarde van) het AD attribuut Employee-Number

Hiervoor kennen we de waarde van het AD attribuut Employee-Number eerst toe aan “urn:mace:dir:attribute-def:employeeNumber” en stellen daarmee later de personalUniqueCode samen.

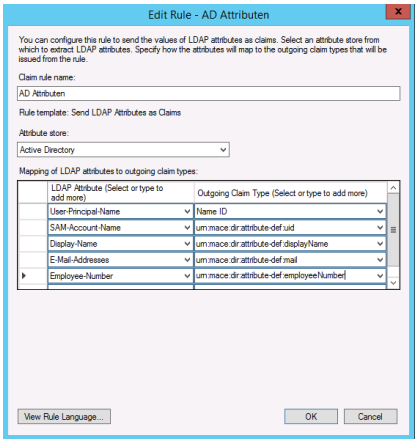
31. Edit opnieuw de Claim Rules van de Relying Party SURFconext



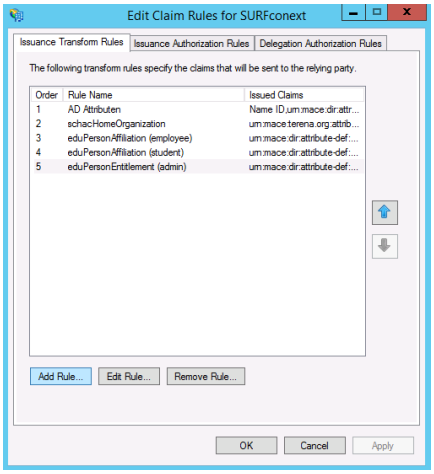
32. Edit opnieuw de “AD Attributen” rule.



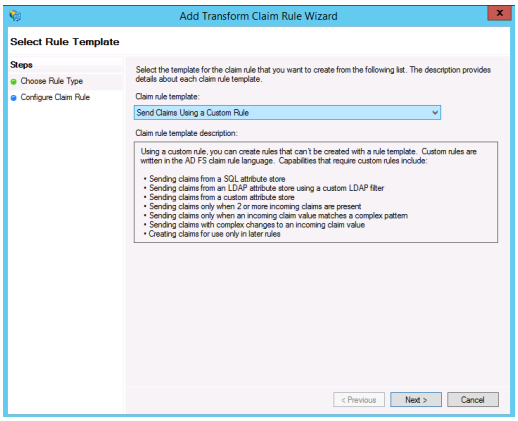
33. Voeg een regel toe die Employee-Number koppelt aan “urn:mace:dir:attribute-def:employeeNumber”.



34. Sla de rule op en voeg een Custom claim rule toe door op de “Add Rule...” knop te klikken.



35. Kies in het volgende venster voor “Send Claims Using a Custom Rule” en klik op “Next”.



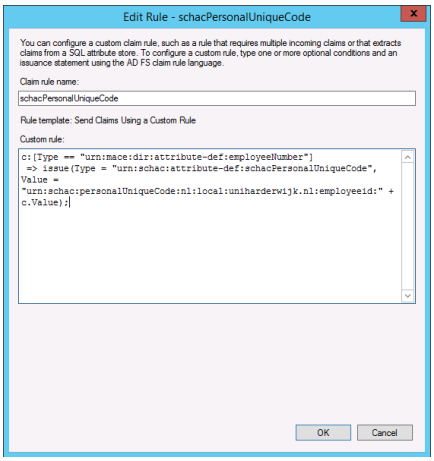
36. Geef de rule een beschrijvende naam zoals “schacPersonalUniqueCode” en creëer de gewenste attribuutsamenstelling op basis van een tekst en één of meerdere bestaande attributen.

```
c:[Type == "urn:mace:dir:attribute-def:employeeNumber"]
 => issue(Type = "urn:schac:attribute-def:schacPersonalUniqueCode", Value =
"urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:" + c.Value);
```

Bovenstaande code dient als volgt gelezen worden:

Als een attribuut van het type “urn:mace:dir:attribute-def:employeeNumber” bestaat, bewaar dit attribuut *dan* in variabele “c” *en* geef een nieuw attribuut van type “urn:schac:attribute-def:schacPersonalUniqueCode” uit met een samenstelling van de letterlijke tekst “urn:schac:personalUniqueCode:nl:local:uniharderwijk.nl:employeeid:” en de *waarde* van het attribuut in variabele “c”.

Het venster ziet er dan ongeveer zo uit:



37. Als de Rule compleet is, klik dan op “OK”.
38. Een meer geavanceerde rule, welke ook de “*schacHomeOrganization*” en de “*affiliation*” meeneemt, ziet er dan als volgt uit:

```
c1:[Type == "urn:mace:dir:attribute-def:employeeNumber"] &&
c2:[Type == "urn:mace:terena.org:attribute-def:schacHomeOrganization"] &&
c3:[Type == "urn:mace:dir:attribute-def:eduPersonAffiliation"]
 => issue(Type = "urn:schac:attribute-def:schacPersonalUniqueCode", Value = "urn:schac:personalUniqueCode:nl:local:" + c2.Value + ":" +
c3.Value + "id:" + c1.Value);
```

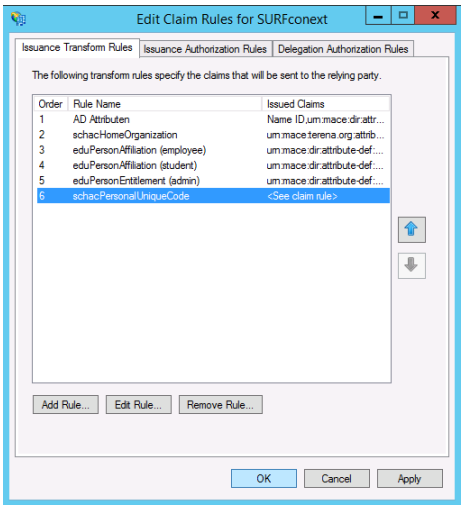
39. **eduPersonScopedAffiliation**

    Om eduPersonScopedAffiliation toe te voegen aan de ADFS claims kan de volgende Custom claims rule gebruikt worden, er vanuit gaande dat de claims "urn:mace:dir:attribute-def:eduPersonAffiliation" en "urn:mace:terena.org:attribute-def:schacHomeOrganization" zoals eerder in deze handleiding beschreven, correct gedefinieerd zijn.

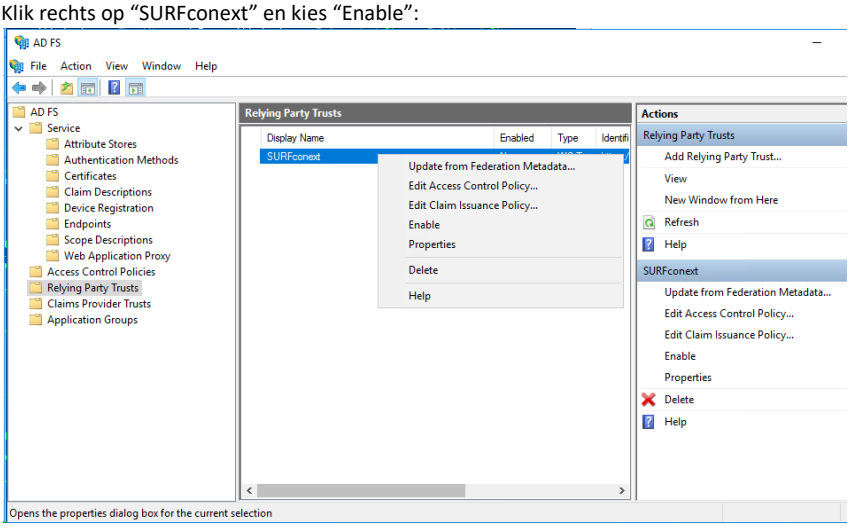
    Kies weer voor "Edit Claim rules" en "Add Rule". Kies in het volgende scherm voor "Send Claims Using a Custom Rule" en klik op "Next".
    Geef de Rule een beschrijvende naam zoals "Create eduPersonScopedAffiliation" en plak de volgende code in het "Custom Rule" venster:

    ```
    c1:[Type == "urn:mace:dir:attribute-def:eduPersonAffiliation"] &&
    c2:[Type == "urn:mace:terena.org:attribute-def:schacHomeOrganization"]
    => issue(Type = "urn:mace:dir:attribute-
    def:eduPersonScopedAffiliation", Value = c1.Value + "@" + c2.Value);
    ```

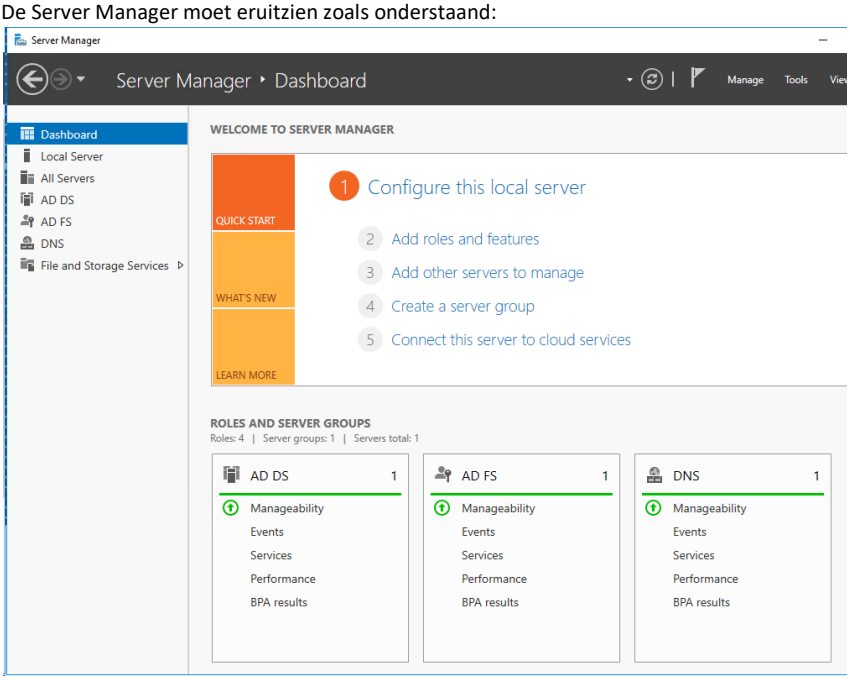
    Klik "Finish" en klik "Ok" in de "Edit Claims Rules" dialoog. Test hierna de uitgifte van het nieuwe attribuut.



40. En bewaar, als alles klopt de Claim Rules set door op “OK” te klikken.
41. Klik rechts op “SURFconext” en kies “Enable”:



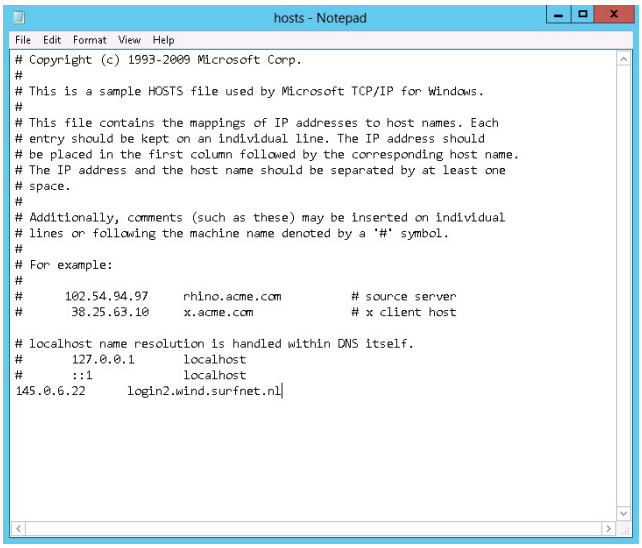
42. De Server Manager moet eruitzien zoals onderstaand:



AD FS Proxy installeren

Algemeen

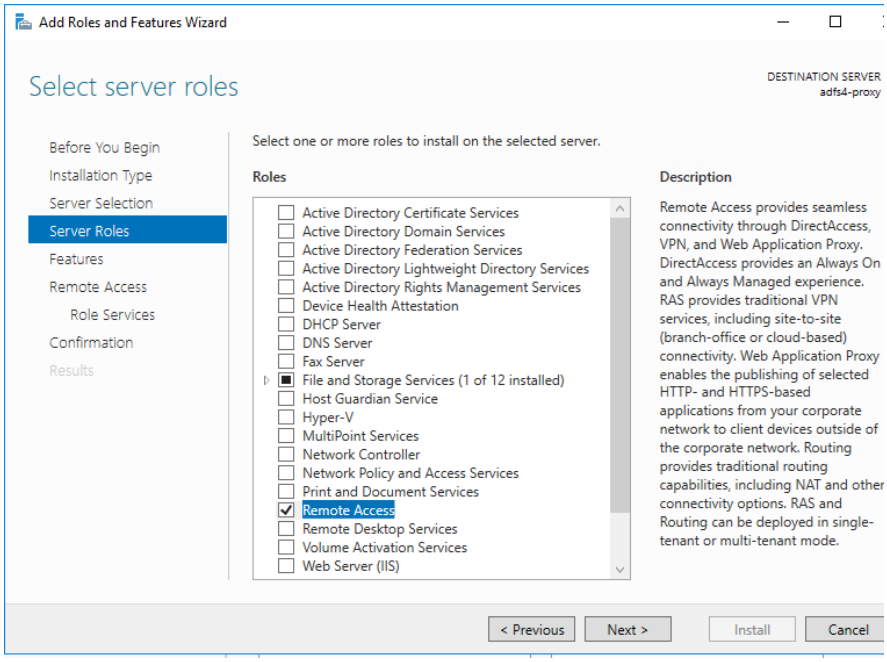
Het is belangrijk dat de AD FS Proxy de AD FS server onder de voor de AD FS service gekozen DNS naam kan bereiken. De Proxy zelf moet echter onder dezelfde naam voor de buitenwereld (het internet) bereikbaar zijn. Hiervoor kan een split-DNS (zie verklarende woordenlijst) configuratie ingericht worden. Als dat niet mogelijk is, moet de Proxy op een andere manier verteld worden wat het IP adres van de AD FS server is. Dat kan met behulp van de hosts file (C:\Windows\System32\Drivers\etc). Voeg hiervoor een regel toe met vooraan het fysieke adres van de AD FS server en daarachter de servicenaam waaronder de AD FS dienst beschikbaar is:



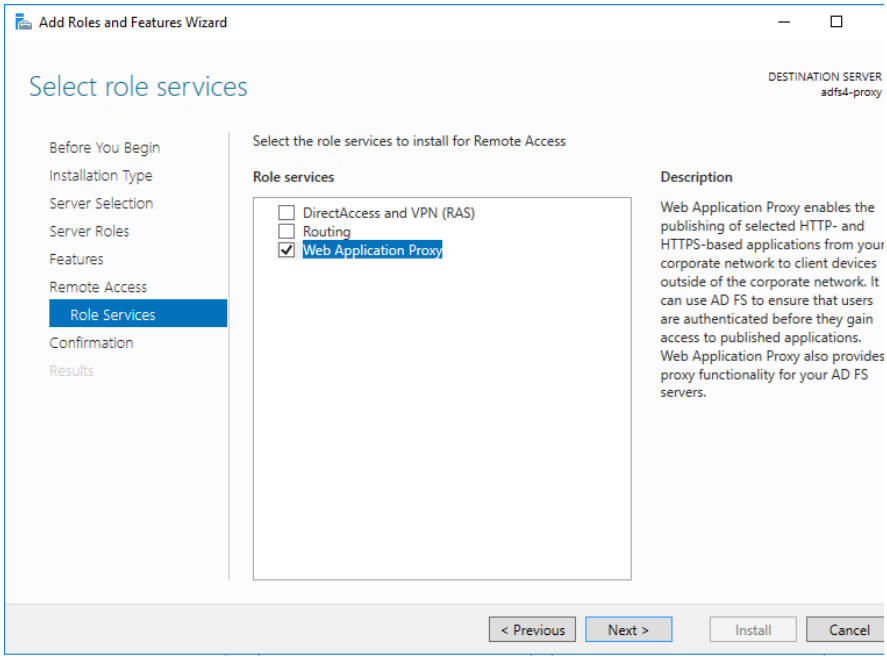
Let op: dit bestand is alleen als Administrator te bewerken. Start hiervoor een Notepad op onder “run as Adminstrator” conditie.

AD FS Proxy installeren

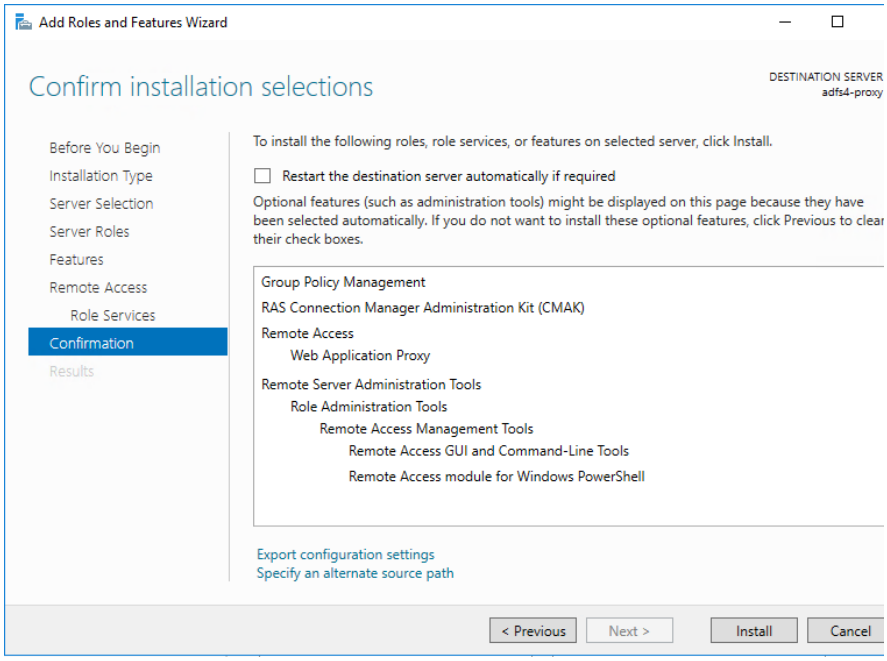
1. Kies in het Server Manager Dashboard weer voor “Add roles and features” en klik zoals hiervoor beschreven door de eerste schermen en selecteer ditmaal “Remote Access”:



2. Klik “Next >” tot je bij “Role Services” bent en kies “Web Application Proxy” > “Next >”:

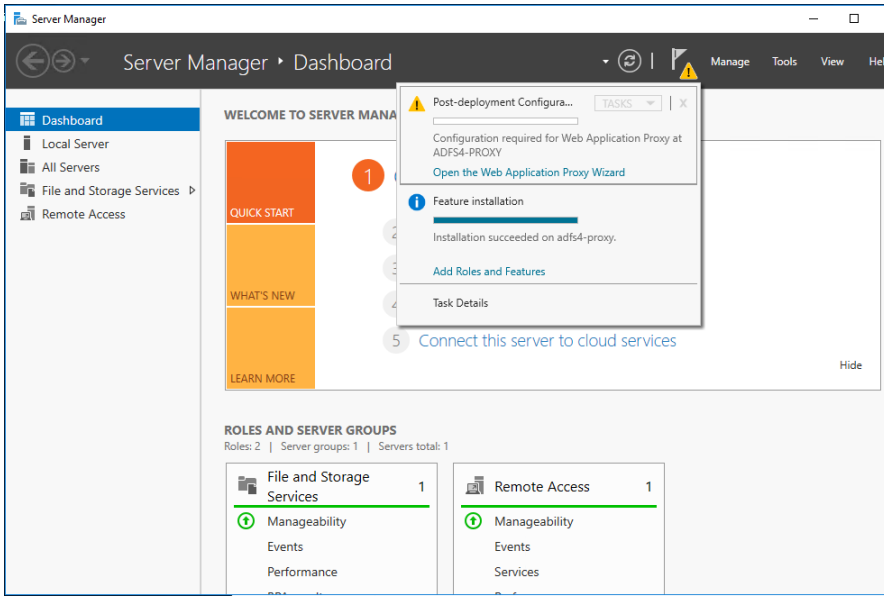


3. Klik op “Install”, wacht eventueel de installatie af en klik op “Close”:

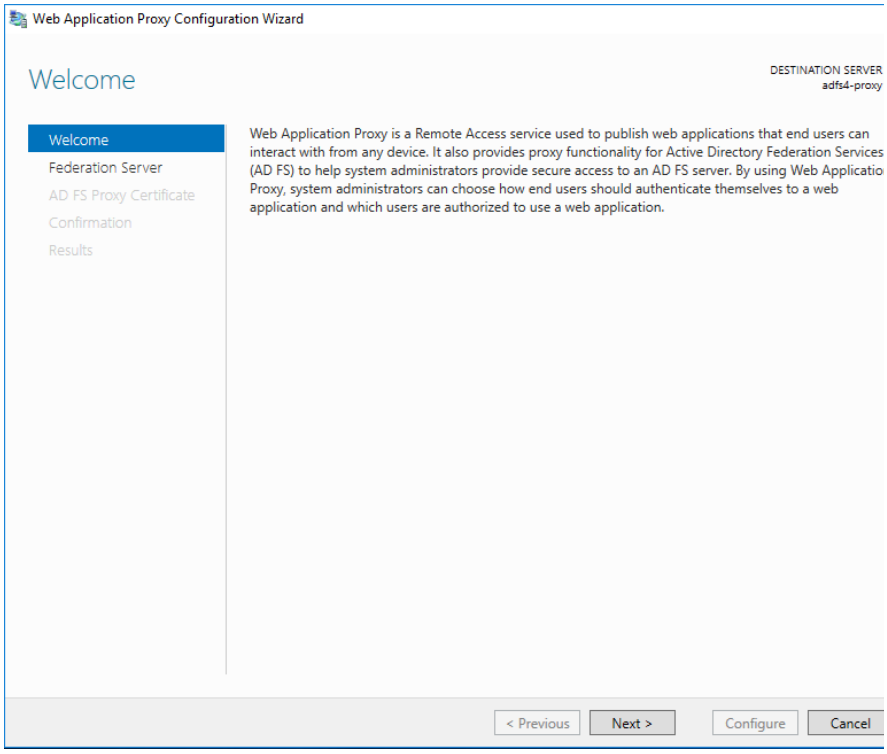


4. De Proxy configuratie vereist een geldig en werkend SSL certificaat. Installeer hiervoor eerst het SSL certificaat dat ook op de AD FS Server geïnstalleerd is door het daar bijvoorbeeld als .pfx bestand te exporteren. Zie voor de installatie van een SSL certificaat “Appendix A: Certificaat Installeren”.

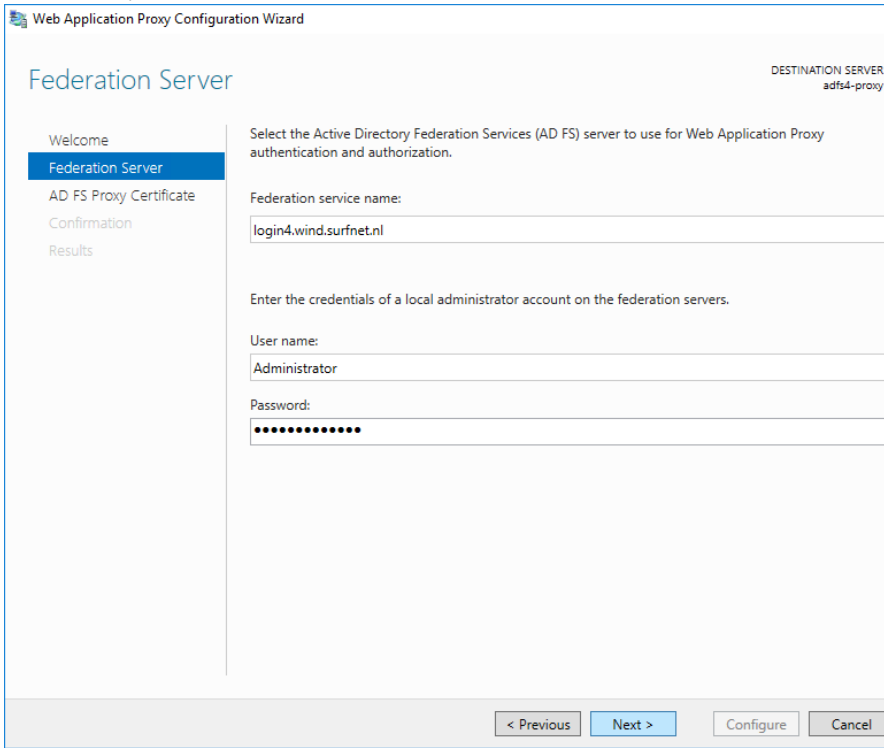
5. Na installatie verschijnt een Post-deployment alert “Configuration required for the Federation Service Proxy at ...” in het Server Manager Dashboard. Klik op deze link:



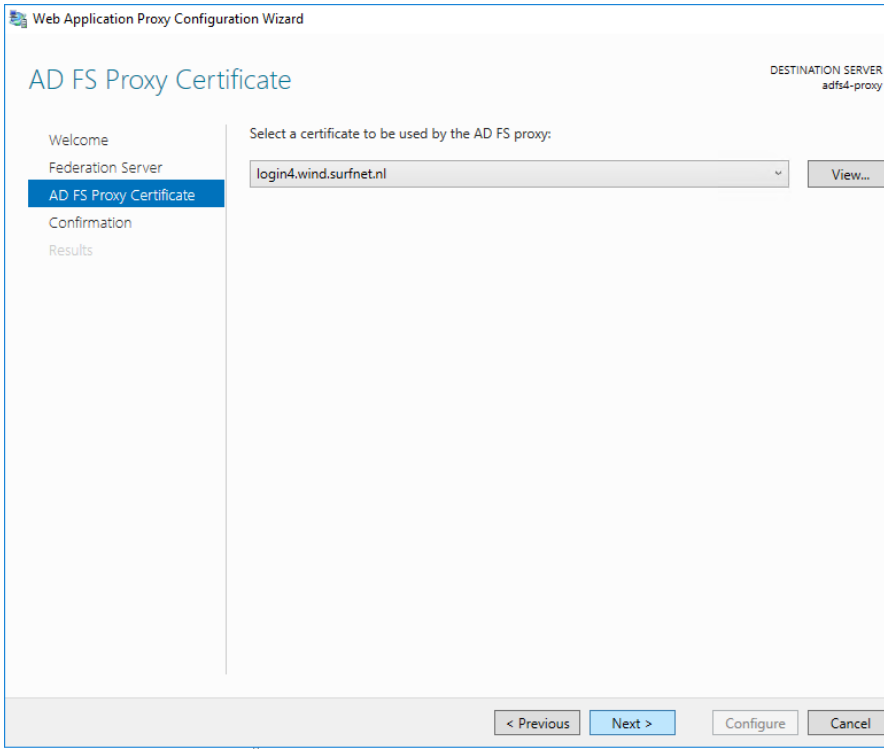
6. De “Web Application Proxy Configuration Wizard” wordt geopend, klik op “Next > “:



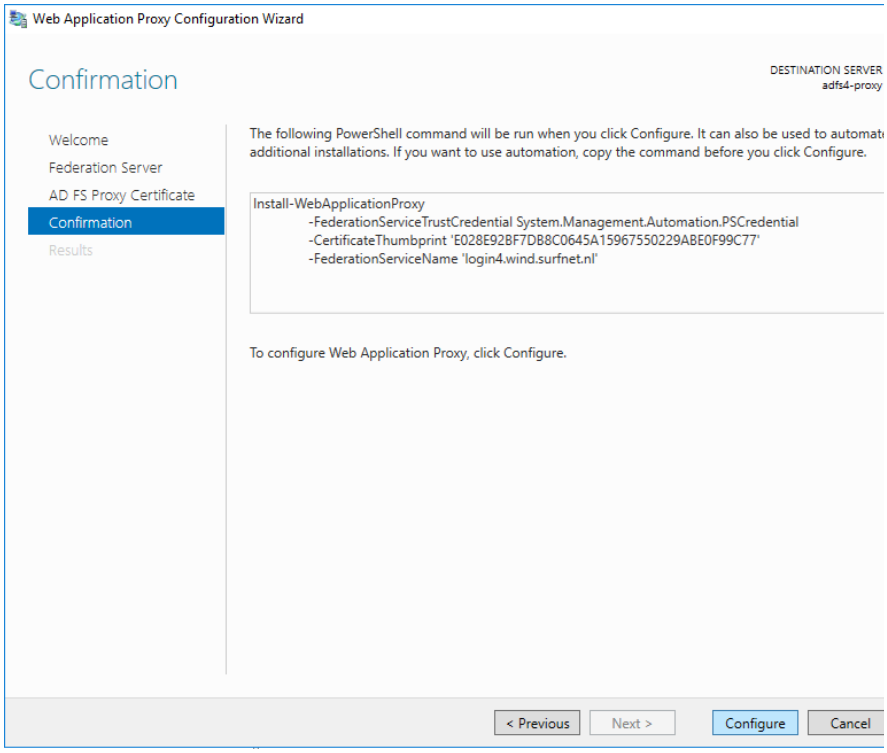
7. Kies dezelfde DNS naam als de AD FS Server voor “Federation Service Name” en vul de username en password in:



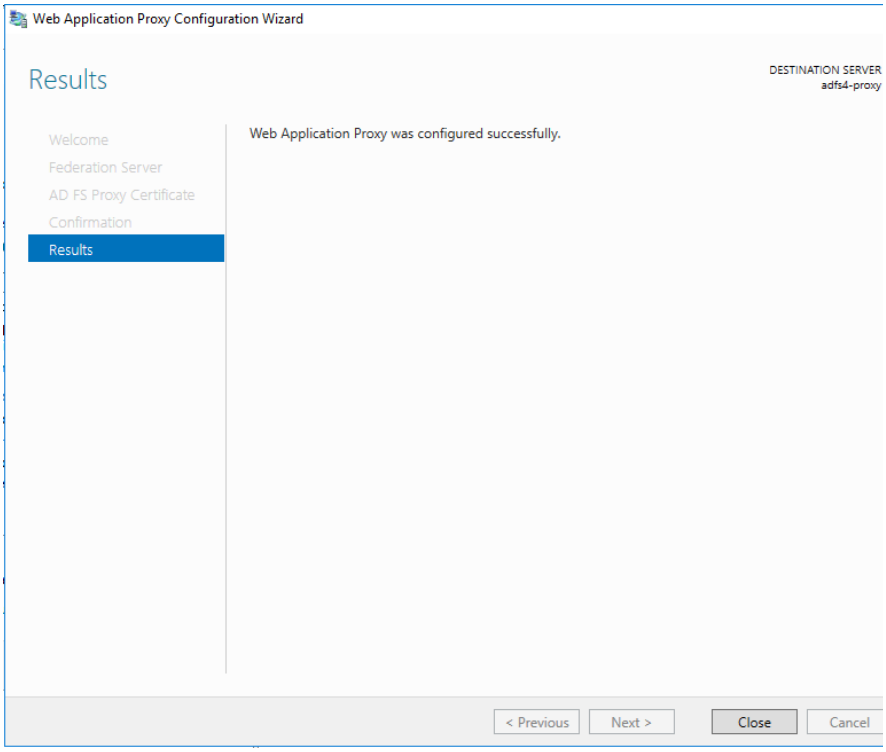
8. Selecteer het certificaat (Appendix A) en klik op “Next >”:



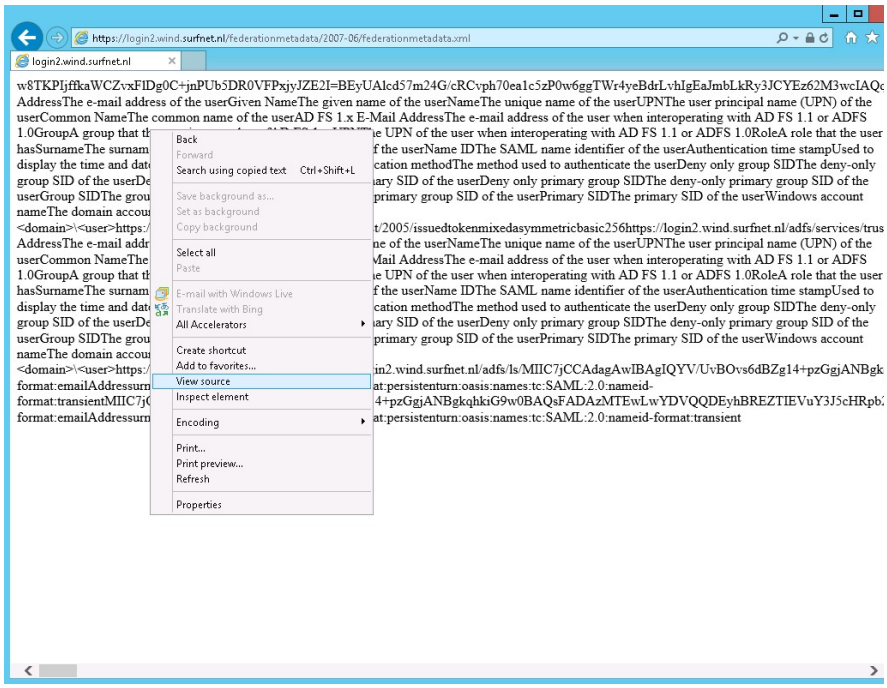
9. Klik op “Configure”:



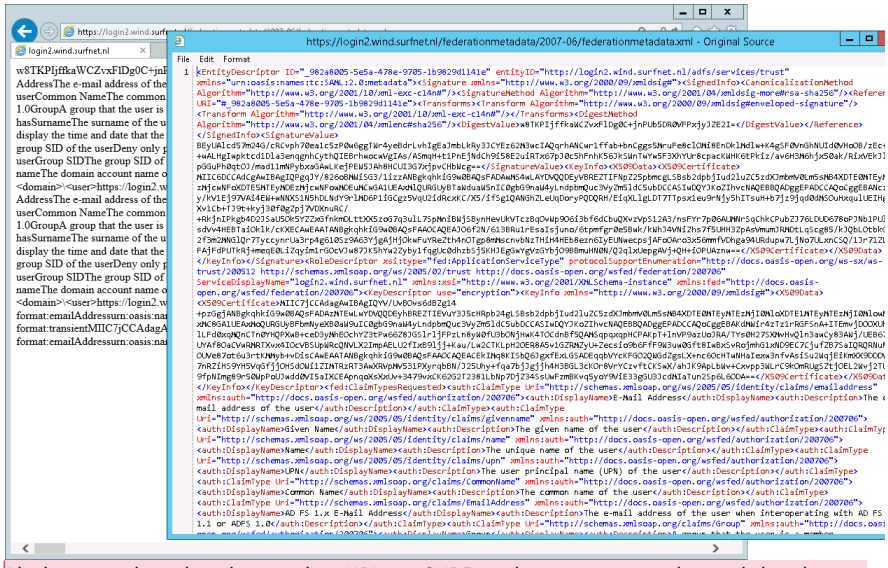
10. Klik op “Close”:



11. Surf ter controle naar de AD FS service URL (zowel vanuit een plek die op de AD FS Server uitkomt als vanaf een plek die op de Proxy uitkomt) en controleer de inhoud van de volgende URL: https://<servicenaam>/federationmetadata/2007-06/federationmetadata.xml :



12. Deze URL dient zoals hierboven te zien is een XML document te bevatten. Als de browser geen document laat zien kan met “View Source” het document in een editor getoond worden:



13. Als deze test slaagt kan de metadata URL aan SURFnet doorgegeven worden zoals beschreven in het hoofdstuk “Metadata doorgeven aan SURFnet”.
Op de AD FS Proxy is deze URL nu nog plaintext (http) beschikbaar. Dit kan geen kwaad, maar kan voor de zekerheid uitgeschakeld worden door de binding van de default site in IIS met poort 80 ongedaan te maken.

Commented [NB1]: AD FS 4.0 werkt niet meer met IIS, dus ik vraag me af of dit je gaat lukken in IIS…

Metadata doorgeven aan SURFnet

Als de AD FS server en AD FS Proxy of Web Application Proxy geïnstalleerd zijn en hun werking gecontroleerd kan de metadata URL doorgeven worden aan SURFnet. Om er voor te zorgen dat de metadata voor de Identity Provider langer houdbaar is verlengen we de duur van het Token Signing certificaat op de AD FS server eerst even door in een Powershell de volgende commando's uit te voeren:

```
Set-AD FSProperties -CertificateDuration 1825
```

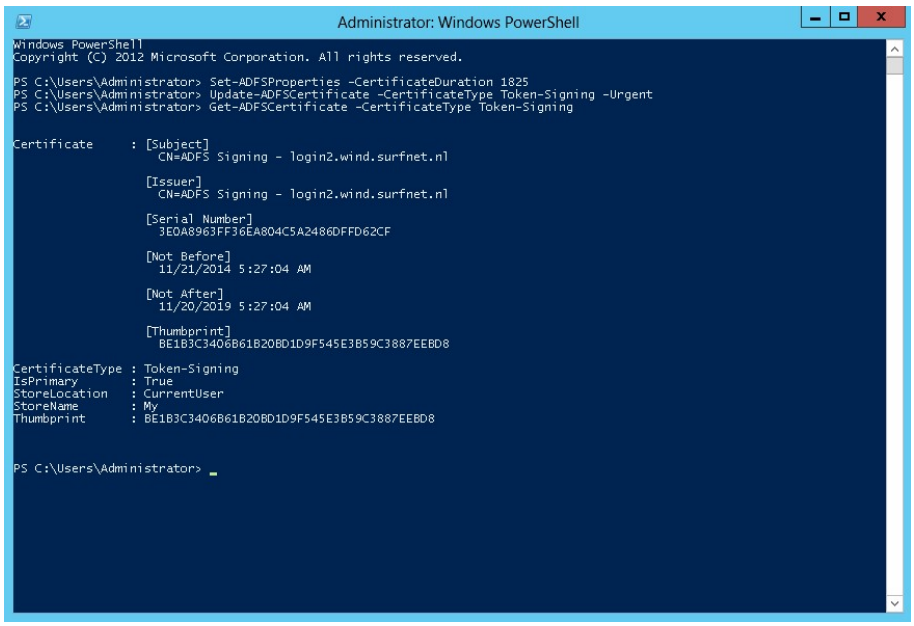
Als er nog geen andere Relying Party Trusts configuraties bestonden voor deze installatie:

```
Update-AD FSCertificate -CertificateType Token-Signing -Urgent
```

(deze worden namelijk onbruikbaar door het uitvoeren van bovenstaande commando)

en ter controle:

```
Get-AD FSCertificate -CertificateType Token-Signing
```



Het Token-Signing certificaat is nu als het goed is vijf jaar geldig.

Aanleveren Metadata

Vervolgens kan een mail naar SURFconext gestuurd worden met daarin de volgende informatie:

- Metadata URL: https://<servicenaam>/federationmetadata/2007-06/federationmetadata.xml

En alle onder deze URL genoemde extra gegevens:
https://wiki.surfnet.nl/display/surfconextdev/Vereiste+metadata

Het advies is om Appendix B door te nemen over openstaande poorten op de server.

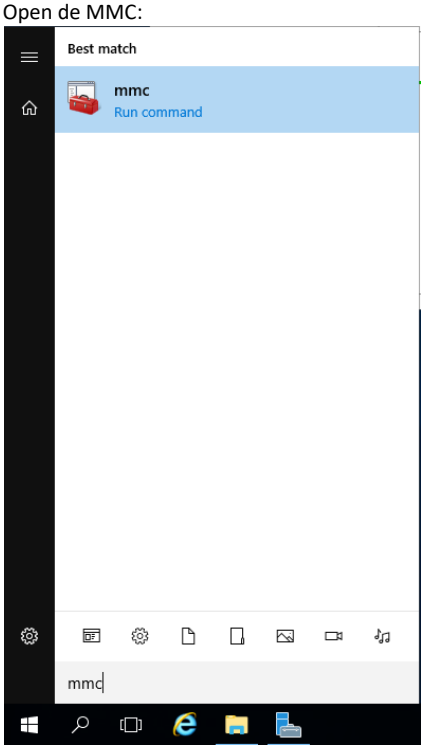
Appendix A Certificaat installeren

Deze handleiding gaat er vanuit dat het certificaat plus private key beschikbaar is in de vorm van een .pfx bestand. Als het certificaat en de private key alleen los beschikbaar zijn als respectievelijk *cert.pem* en *cert.key* met certificate chain *chain.pem*, is daar met het volgende openssl commando een *cert.pfx* bestand van te maken:

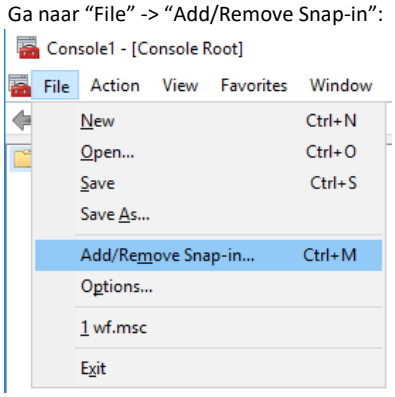
#openssl pkcs12 -export -passout pass:*123welkom* -in *cert.pem* -certfile *chain.pem* -inkey *cert.key* -out *cert.pfx*

Het cert.pfx bestand heeft nu als voorbeeld wachtwoord *123welkom*.

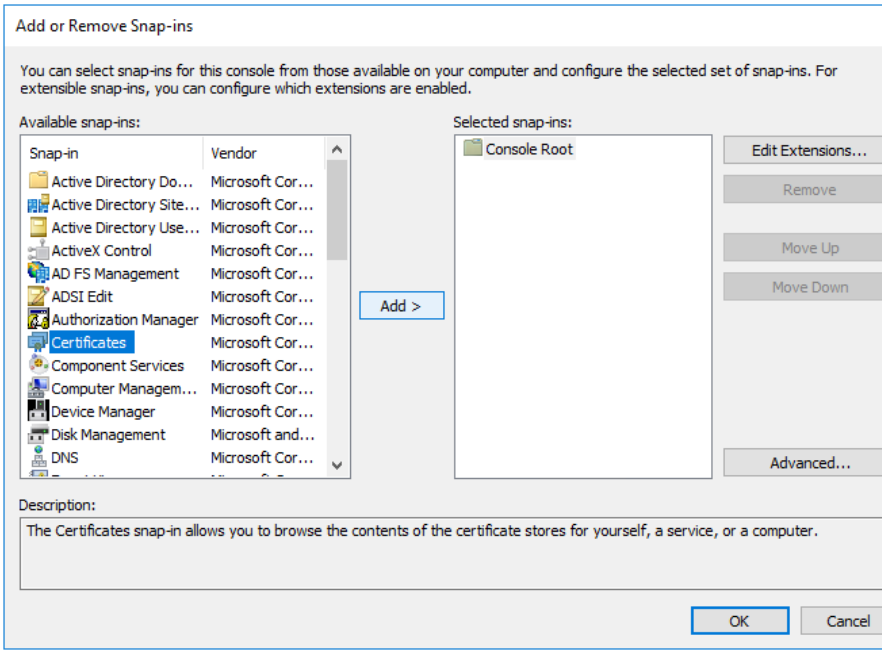
1. Open de MMC:



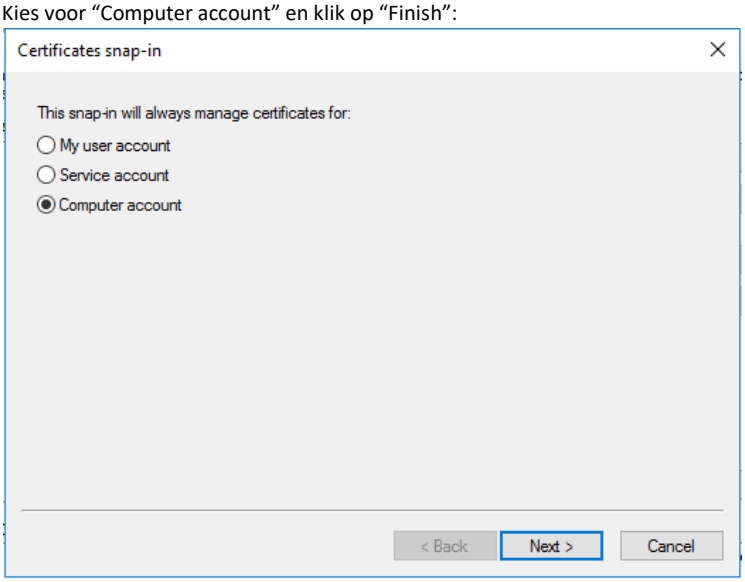
2. Ga naar “File” -> “Add/Remove Snap-in”:



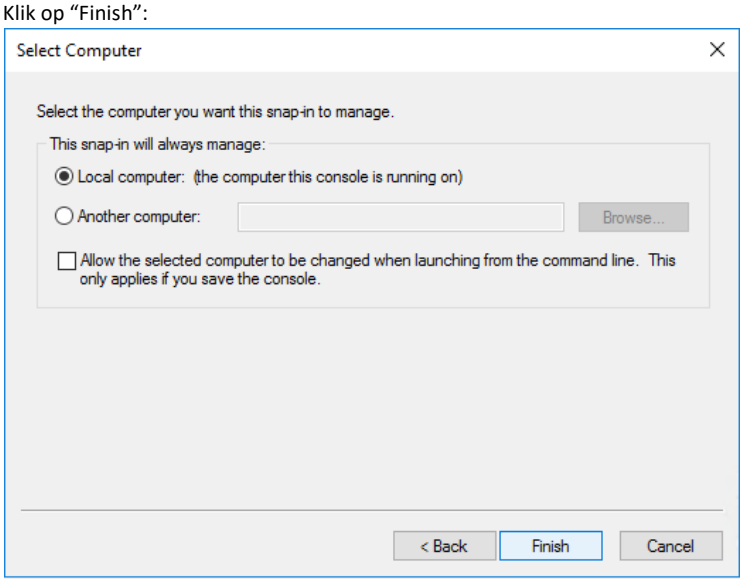
3. Klik links op “Certificates” en op “Add”:



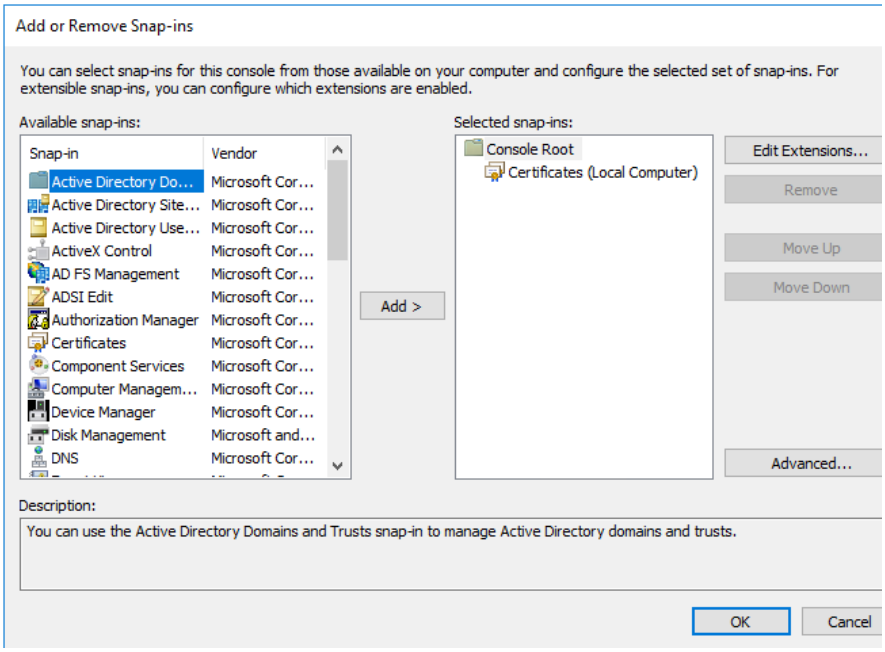
4. Kies voor “Computer account” en klik op “Finish”:



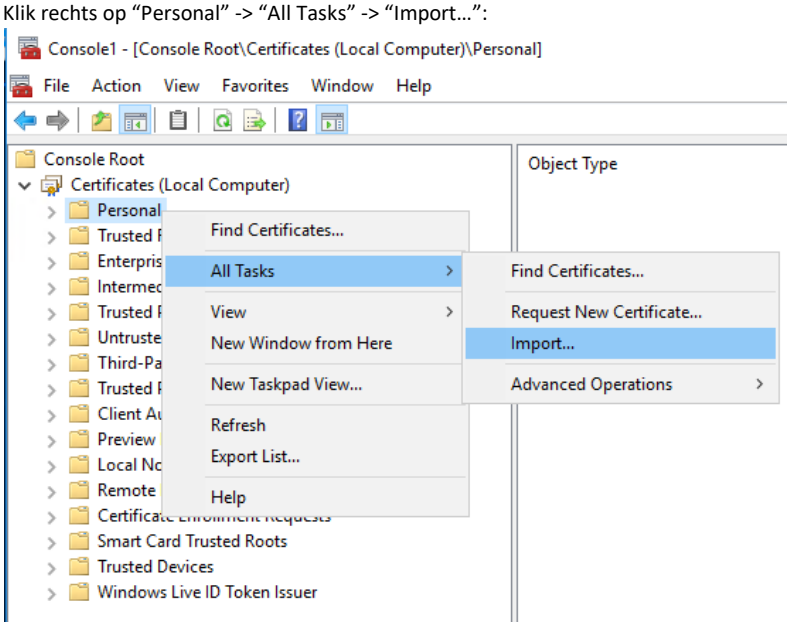
5. Klik op “Finish”:



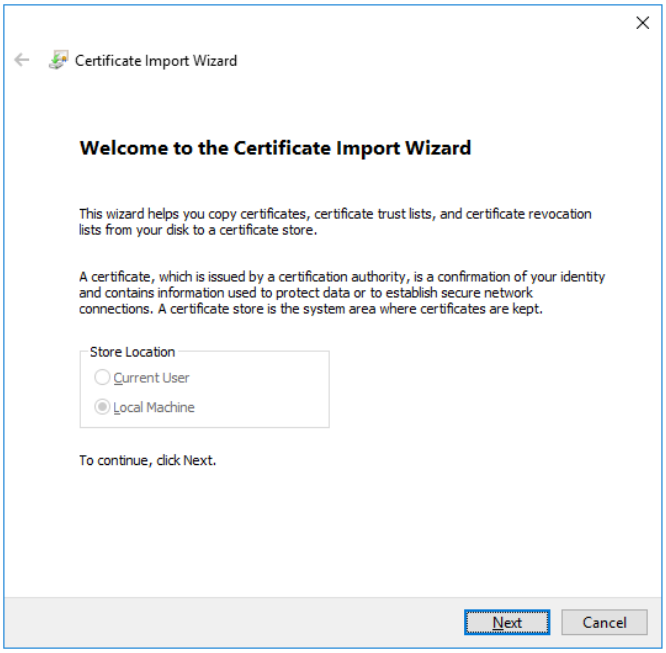
6. Klik op “OK”:



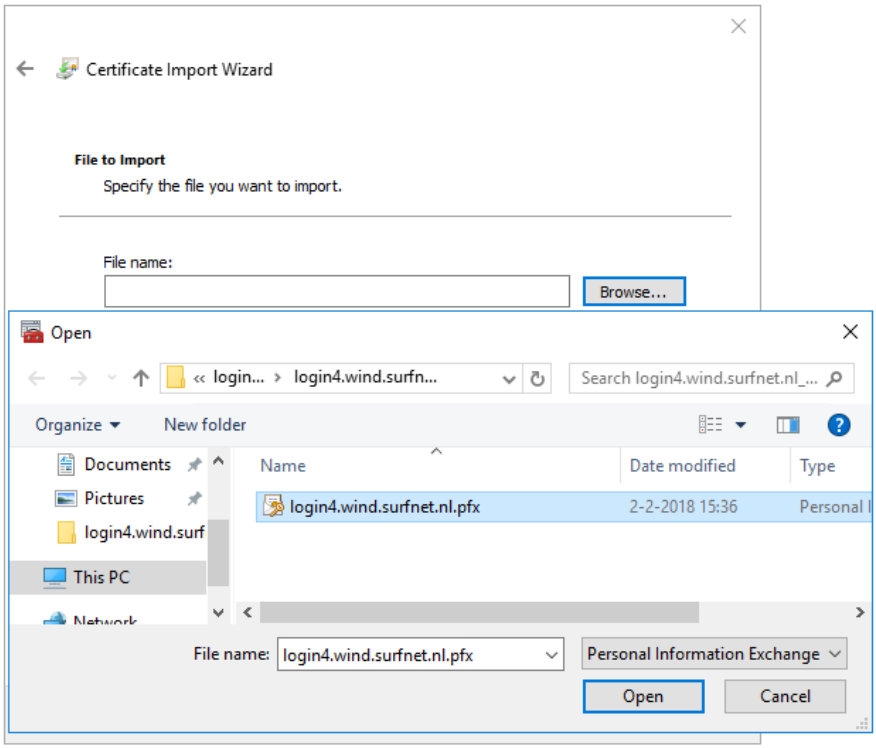
7. Klik rechts op “Personal” -> “All Tasks” -> “Import...”:



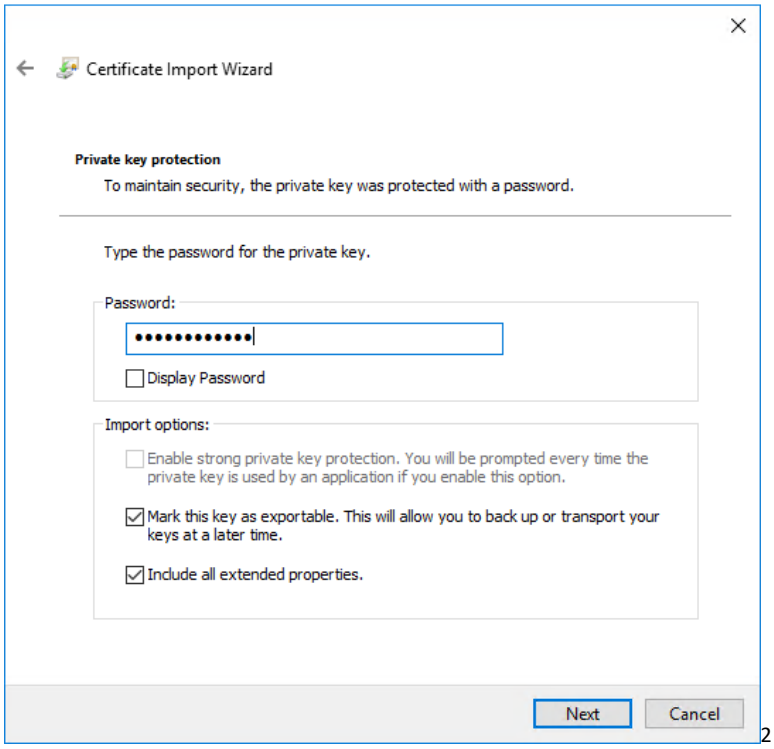
8. Klik op “Next”:



9. Klik op “Browse” en selecteer het certificaat en klik op “Next”:

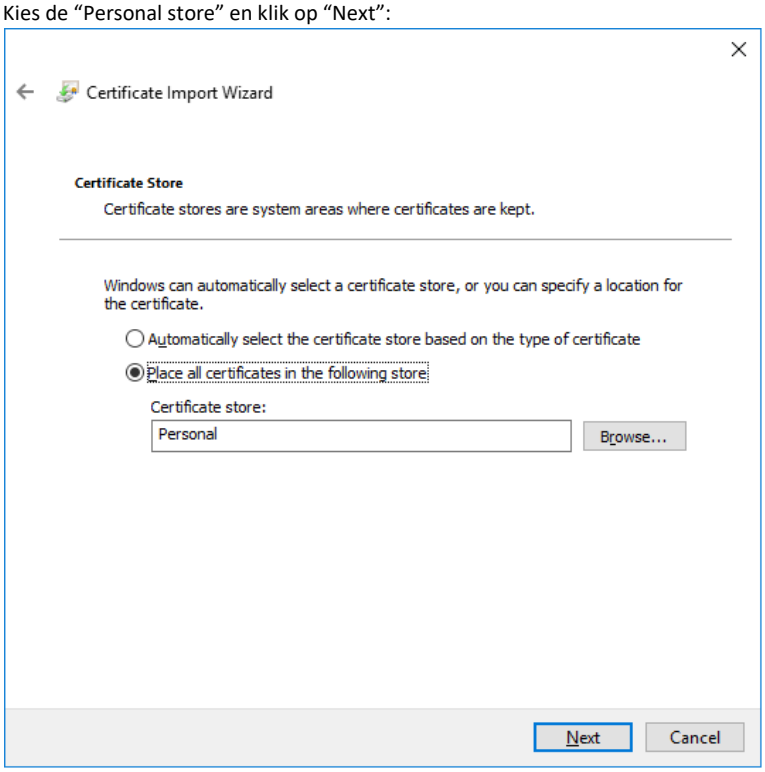


10. Vul het wachtwoord in en klik op “Next”

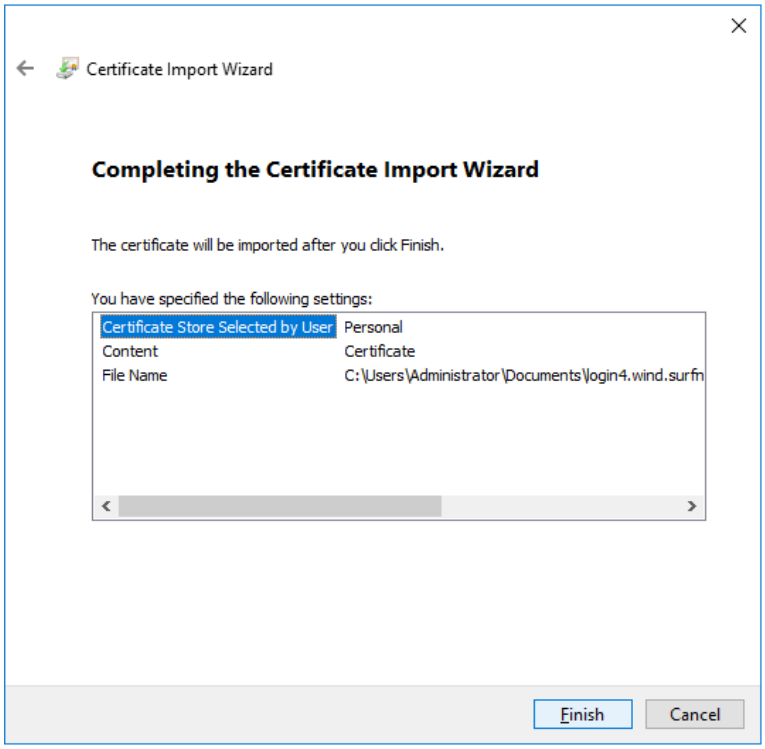


2

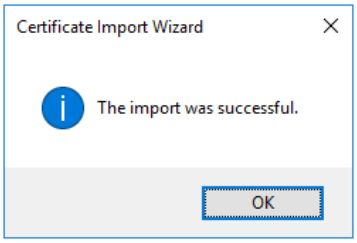
11. Kies de “Personal store” en klik op “Next”:



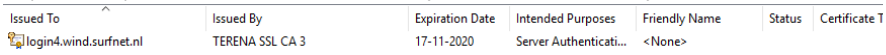
12. Klik op “Finish”:



13. Klik op “OK”:



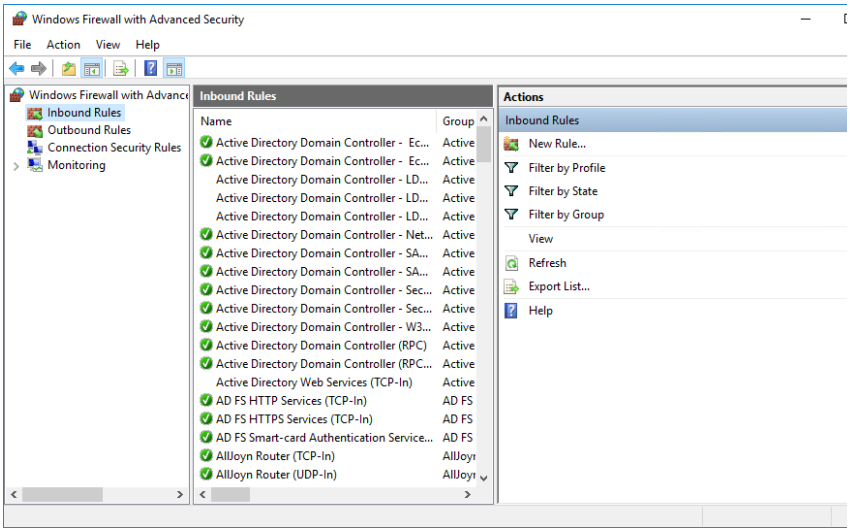
14. Controleer of het certificaat, inclusief private key, correct geïmporteerd is. Aanwezigheid van de private key is te herkennen aan het sleuteltje linksboven het icoontje van het certificaat.



Apendix B Poorten dichtzetten

1. Ga naar de AD FS server
2. Open “Windows Firewall”:

3. Ga naar “Inbound Rules”:



4. Disable de volgende regels:
    a. Active Directory Domain Controller - LDAP (TCP-In)
    b. Active Directory Domain Controller - LDAP (UDP-In)
    c. Active Directory Domain Controller - LDAP for Global Catalog (UDP-In)
    d. Acitve Directory Web Services (TCP-In)
    e. DNS (TCP, Incoming)
    f. DNS (UDP, Incoming)
5. Ga naar Outbound rules en disable de volgende regels:
    a. Xbox Game UI
6. Ga nu naar de AD FS Proxy en open daar ook Windows Firewall
7. Ga naar Outbound rules en disable de volgende regels:
    a. Xbox Game UI

Verklarende woordenlijst

DMZ

DMZ staat voor Demilitarized Zone en is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. Het externe netwerk is meestal het internet.
Een DMZ is feitelijk een andere naam voor een extranet, een gedeelte van het netwerk dat voor de buitenwereld volledig toegankelijk is.
Op het netwerksegment van de DMZ zijn meestal servers aangesloten die diensten verlenen die vanuit het interne en externe netwerk aangevraagd kunnen worden (bijvoorbeeld een webserver en/of mailserver). De DMZ dient door een firewall beschermd te worden, maar moet wel zodanig geconfigureerd worden (gaten in de firewall) dat de diensten binnen de DMZ toegankelijk blijven.
(Bron: Wikipedia)

Split-DNS

Is de een Domain Name System (DNS) implementatie waarbij verschillende verzamelingen DNS gegevens worden geleverd afhankelijk van de bron van het DNS verzoek. In de praktijk komt het er op neer dat de DNS server voor een computer binnen het intranet een private adres van de server binnen de intranet grenzen geeft en voor gebruikers van buitenaf (het internet) het adres van de server in de DMZ (zie hierboven) of de firewall/router die verbonden is met de server.