B-1 - NetScaler configuratie guide (NS12)

Voor ShareFile met lokale StorageZone

Omschrijving van de opzet

Opzetten van een Citrix ShareFile met een lokale storage zone door middel van NetScaler met AAA-functionaliteit.



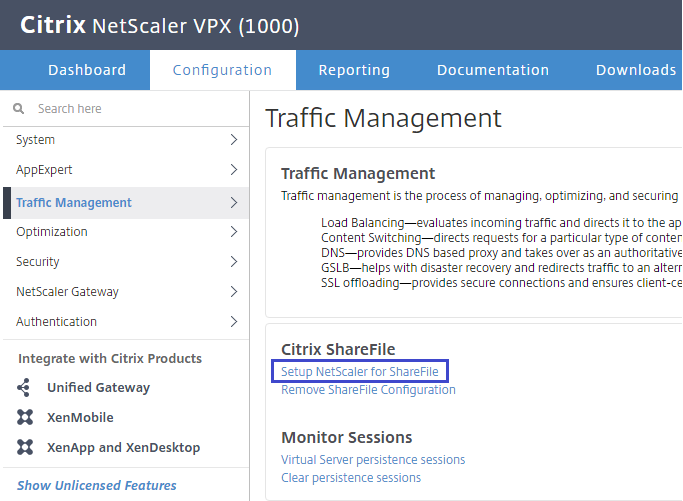
*De opstelling; “Citrix ShareFile met lokale storage zone door middel van NetScaler met AAA-functionaliteit”.*

Vereisten en randvoorwaarden

* Werkende NetScaler VPX (NS10.5 of hoger is aangeraden) (2 indien high availability nodig is)
* Geldig publiek aanvaard certificaat
* Publiek IP-adres en DNS-naam (2 indien high availability nodig is)
* Active Directory (AD) en account met leesrechten
* Interne StorageZone Controller (2 indien nood aan load balancing en high availability)
* ShareFile Enterprise editie met sharefile.com subdomein

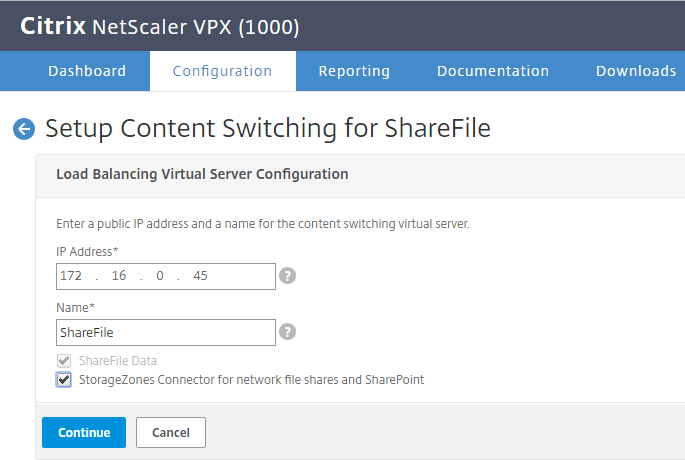
Standaard NetScaler voor ShareFile setup (NS10.5 of hoger)

Sinds NS versie 10.5 is NetScaler is voorzien van een ingebouwde “NetScaler voor ShareFile setup”. Die standaard setup is geen verplichting, maar biedt een grote hulp indien een basissetup voldoet.



Ga naar het configuratie tabblad in de NetScaler VPX GUI interface.

Navigeer naar traffic management en klik op zet NetScaler op voor ShareFile.

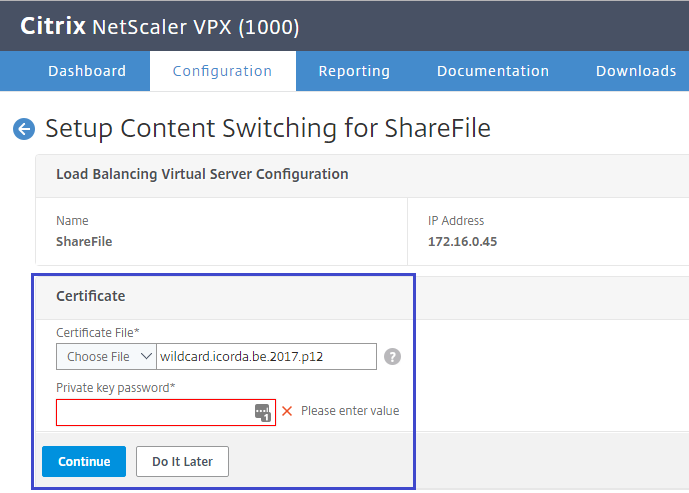
Content switching virtuele server (CS-VS)

Vul het IP-adres in dat gebruikt zal worden om de NetScaler (en achterliggende StorageZone) van buitenaf te bereiken. Dit kan een DMZ IP-adres zijn indien ze correct voorzien wordt van een NAT regel naar een publiek IP-adres.

Geef de content switching virtuele server een naam. De gekozen naam maakt niet zo veel uit, maar hou er rekening mee dat ze voorafgegaan zal worden door de string “\_SF\_CS\_” (die staat voor ShareFile content switching server).

Vink de ShareFile Data en StorageZones Connector selectievakjes aan.

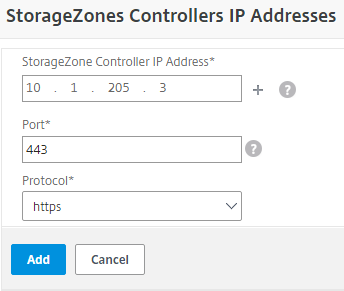
Klik op volgende.



Importeer een certificaat uit NetScaler, of uit de lokale serveropslag.

Indien het certificaat beveiligd is met een wachtwoord dient u dat vervolgens in te vullen.

Klik op volgende

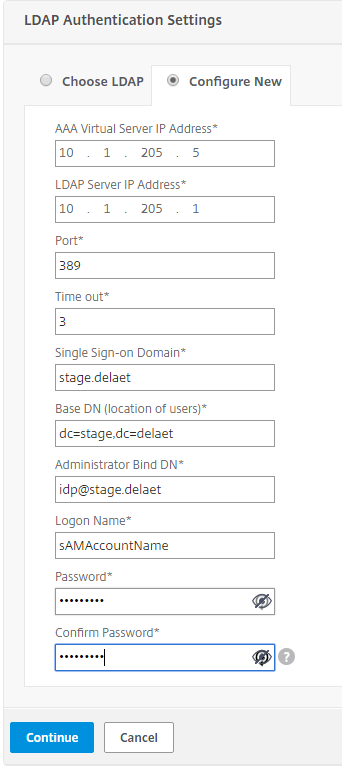
StorageZone (SZ) & load balancing virtuele server (LB-VS)

Kies voor het toevoegen van een nieuwe StorageZone Controller.

Voorzie het IP-adres van de StorageZone Controller server.

Volgens de beste praktijken wordt er gekozen voor HTTPS over poort 443. Hou er rekening mee dat in dit geval een certificaat moet voorzien worden op de StorageZone Controller server (in de IIS-Manager). Dat certificaat mag zelf gesigneerd zijn.

Klik op toevoegen

AAA virtuele server (AAA-VS)

Configureer een nieuw LDAP policy onder de LDAP-authenticatie.

Geef een IP-adres op voor de AAA-VS.

Geef het IP-adres van de lokale AD-server op (dat mag een primaire of secundaire server zijn).

Geef de correcte poort op waarover het AD-verkeer intern verloopt (standaard is dat 389).

Geef het SSO-domein op, standaard zal dat hetzelfde zijn als het AD-domein.

Vul de Base-DN in (dat is de plaats in AD waar de users zich bevinden).

Geef een AD-account met leesrechten op als Administrator Bind DN. Voorzie bij voorkeur een serviceaccount waarvan het wachtwoord niet meer zal veranderen in plaats van een Administrator account. Hier kan gerust een nieuw account voor aangemaakt worden.

Als inlognaam wordt meestal gekozen voor het oudere “sAMAccountName” of het nieuwere “userPrincipalName”. De eerste wordt ook ondersteund door pre Windows 2000 machines.

Standaard zal de NetScaler voor ShareFile setup gebruik maken van basic policies. Aangezien die verouderd zijn en afgekeurd worden, raadt Citrix aan om ze om te zetten in advanced policies. Dit kan gemakkelijk gedaan worden door het volgende commando in te geven in de command line interface van NetScaler en achteraf de nieuwe configuratie in te laden.



Klik op volgende.

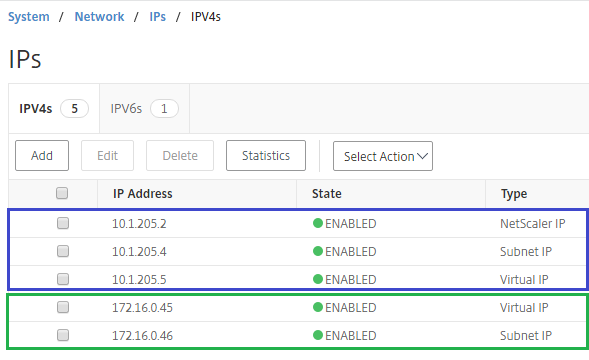
Klik op finish.

Extra configuratie

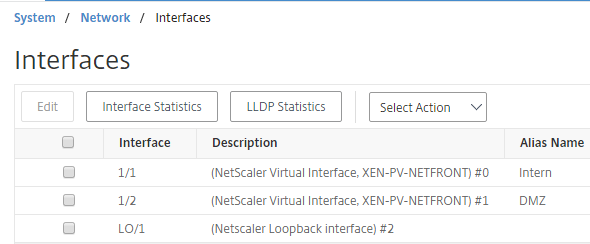
Verder er nog wat geconfigureerd worden alvorens NetScaler correct zou functioneren. Daar bovenop zijn er opties die toegevoegd kunnen worden, maar niet verplicht voor de werking van de opstelling.

Netwerkinstellingen

Navigeer naar systeem 🡪 netwerk onder het configuratie tabblad.

*IP-adressen*

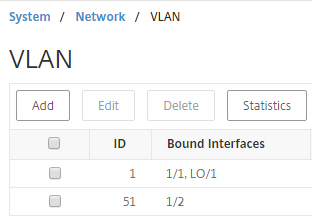
Onder het menu-item “IPs” bevinden zich de IP-adresse die reeds aangemaakt werden tijdens het doorlopen van de setup. Hier moet nog een subnet IP-adres aan toegevoegd worden dat de communicatie van de NetScaler met het internet regelt. Dit subnet IP-adres moet zich in hetzelfde subnet bevinden als het adres van de CS-VS. Voor elk subnet waarin de NetScaler actief is zal zo een subnet IP-adres voorzien moeten worden. Standaard vraagt NetScaler vanaf de eerste opstart al achter een intern subnet adres. Indien dat nog niet geconfigureerd werd, moet er één aangemaakt worden voor de interne communicatie tussen NetScaler en andere componenten van de setup.

*Interfaces*

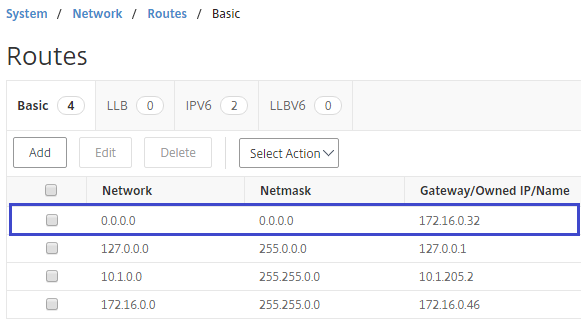
Onder het menu-item “Interfaces” zouden reeds 3 interfaces voorzien moeten zijn.

1. De loopback interface
2. Een interface voor het interne netwerk
3. Een interface voor de DMZ

Het is mogelijk om ze van aliassen te voorzien indien gewenst.

*Virtual local area network (VLAN)*

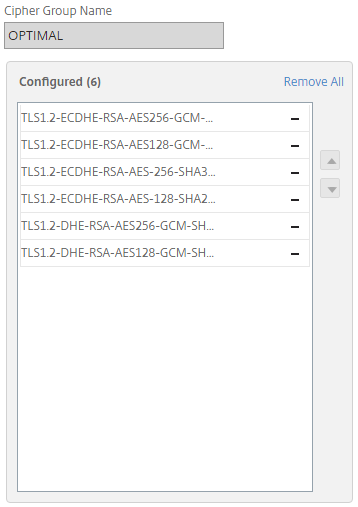
Onder het menu-item “VLANs” kunnen VLAN’s gecreëerd worden. Indien bepaalde interfaces die verbonden zijn met de AD DNS-server, StorageZone controller of gateway zich bevinden in een VLAN moet dit ook in NetScaler aangemaakt worden. Vergeet niet van de passende interfaces te binden aan het correcte VLAN-nummer tijdens de configuratie.

*Routes*

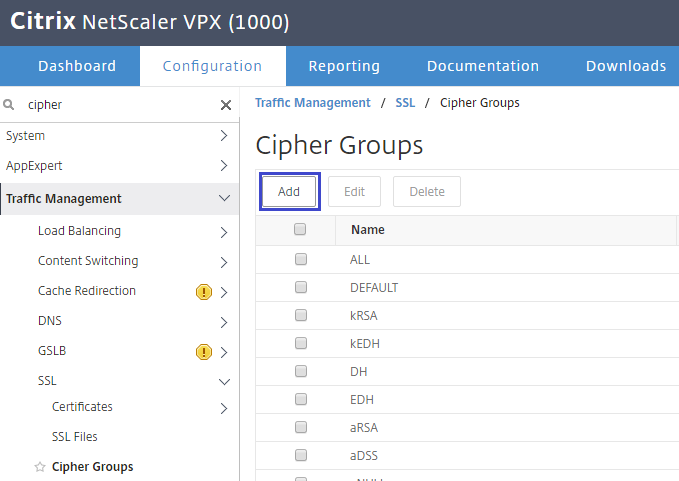
Onder het menu-item “Routes” kunnen routes aangemaakt worden zodat NetScaler weet waar hij IP-verkeer naartoe moet sturen. Standaard zal voor alle gekend IP-adressen (die tijdens de configuratie aan bod kwamen) reeds een route aangemaakt zijn. Er moet enkel nog een default route voorzien worden dat al het ongekende IP-verkeer naar het internet stuurt. De default route krijgt 0.0.0.0 als IP-adres en subnet masker en de default gateway van de DMZ als gateway adres.

Cipher suites (optioneel)

Om de kans op succesvolle aanvallen op het netwerkverkeer te minimaliseren is het aangeraden om enkel de veiligste SSL-verbindingen toe te laten. Om enkel gebruik te maken van veilige algoritmes moet er een Cipher groep gecreëerd worden. Hier volgt een voorbeeld van een zelf gemaakte optimale Cipher groep.



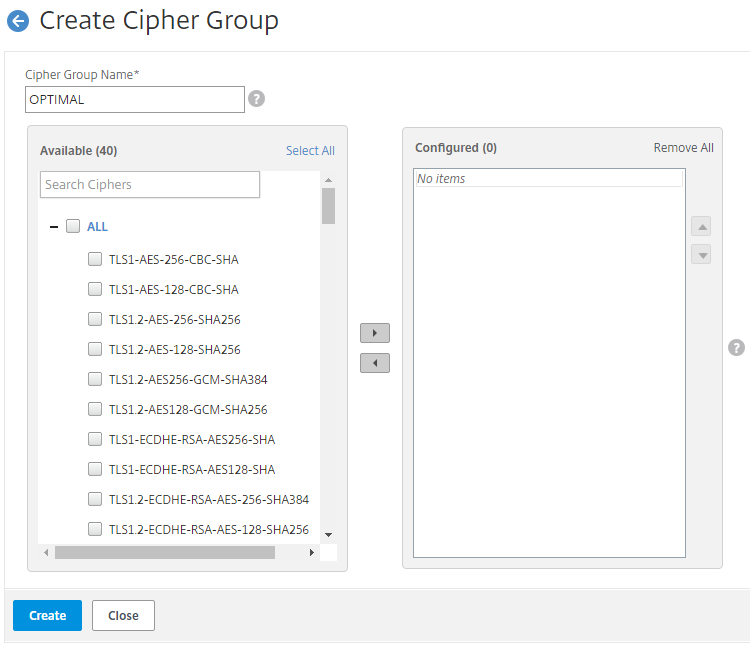
Navigeer naar traffic management, klik op SSL en dan ‘Cipher Groups’.

****

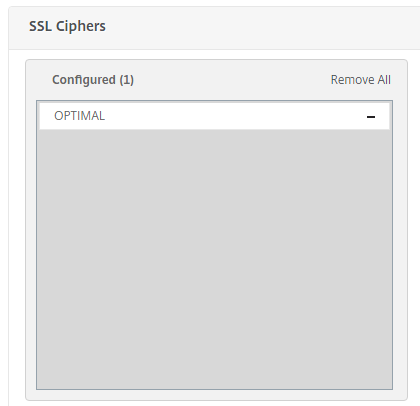
Voeg een nieuwe Cipher groep toe.

Geef de nieuwe Cipher groep een passende naam.

Begin met het toevoegen van Cipher suites.



Voeg de nodige Cipher suites toe door ze aan te vinken. (Onder de ‘ALL’ groep kunnen alle ondersteunde Cipher suites teruggevonden worden).



Link de Cipher suites aan de virtuele servers. Verwijder ook de default Cipher suite die er standaard aan toegewezen was.

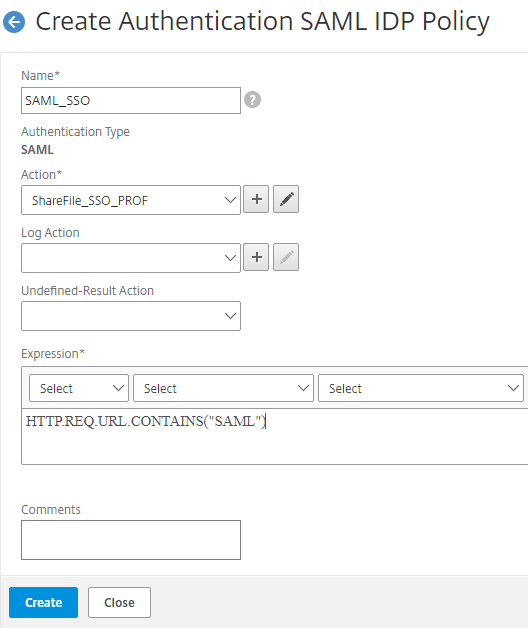
Single sign-on (SSO) (optioneel)

In deze opstelling wordt er reeds geconnecteerd met de StorageZone door middel van de AD-gegevens, SSO is dus al aanwezig. Het kan toch handig zijn om te weten hoe SAML 2.0 en OAuth 2.0 geconfigureerd worden in NetScaler. SAML kan namelijk ook gebruikt worden om aan te melden op ShareFile met diezelfde AD-gegevens. OAuth kan dan weer gebruikt worden voor SSO in externe applicaties die aan ShareFile gekoppeld worden.

*SAML 2.0*

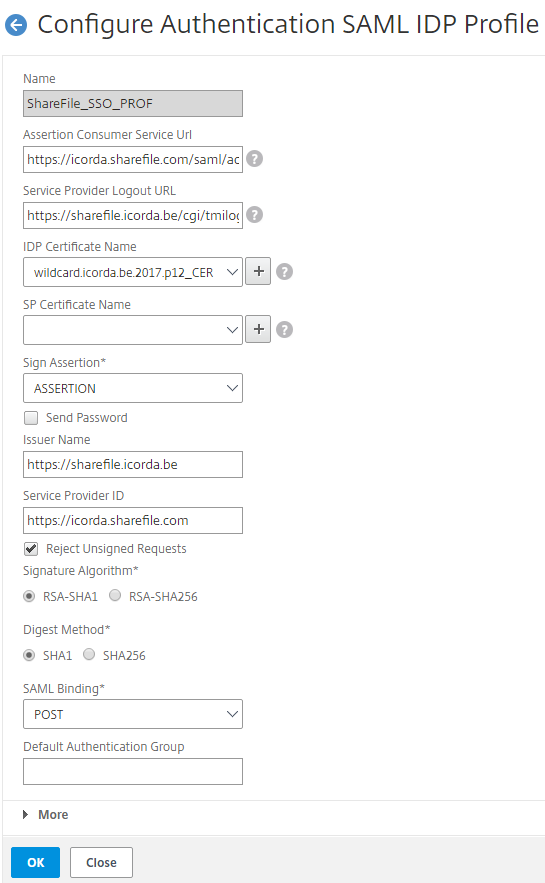
Navigeer naar security 🡪 AAA – Application traffic 🡪 policies 🡪 authenticatie 🡪 geavanceerde policies 🡪 SAML IDP.

Ga naar het policies tabblad en druk op toevoegen om een SAML IDP policy aan te maken.



Geef een expressie op in de vorm van “HTTP.REQ.URL.CONTAINS(“SAML”)”.

Druk op het plus icoon om een actie (SAML IDP Profile) toe te voegen aan de policy.



Geef het ShareFile subdomein gevolgd door “/saml/acs” op als Assertion Consumer Service URL.

Als logout URL kan het publieke adres van de NetScaler gebruikt worden gevolgd door “cgi/tmilogout”.

Gebruik het certificaat van de CS-VS als IDP certificaat voor SAML.

Het certificaat dat ShareFile aanmaakt na de SSO configuratie is het SP certificaat dat hier thuishoort. Zie de ShareFile configuratie guide hiervoor.

NetScaler Gateway (indien van toepassing)

Indien NetScaler als gateway gebruikt wordt in de opstelling, moet een NetScaler Unified Gateway (UG) aangemaakt worden.

Deze Gateway zal automatisch beschikbaar zijn als een CS-VS, de content switching policies kunnen dus evengoed aan deze UG gebonden worden om dezelfde setup werkend te krijgen.

B-2 - StorageZone Configuratie Guide

Voor ShareFile

Omschrijving van de opzet

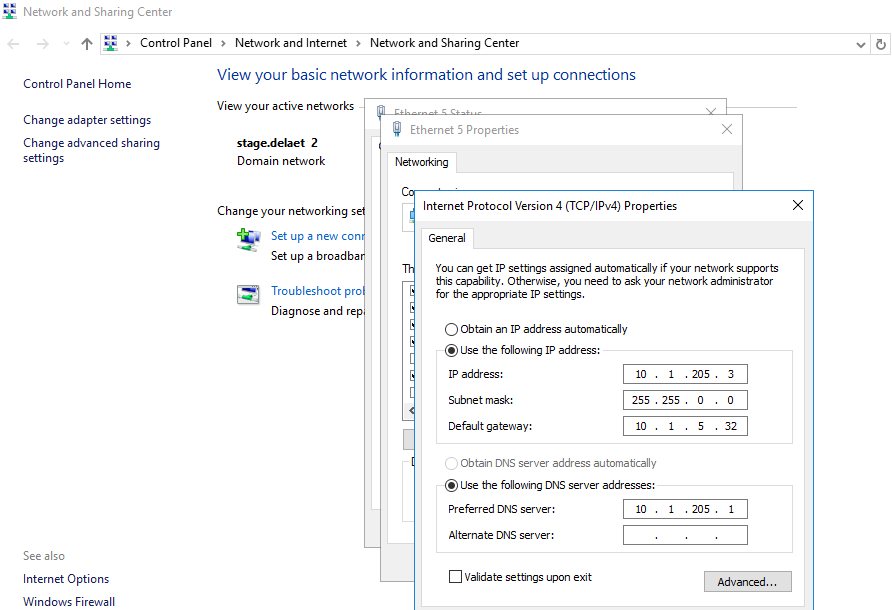
Opzetten van een Citrix ShareFile met een lokale storage zone door middel van NetScaler met AAA-functionaliteit.



*De opstelling; “Citrix ShareFile met lokale storage zone door middel van NetScaler met AAA-functionaliteit”.*

Netwerkconfiguratie

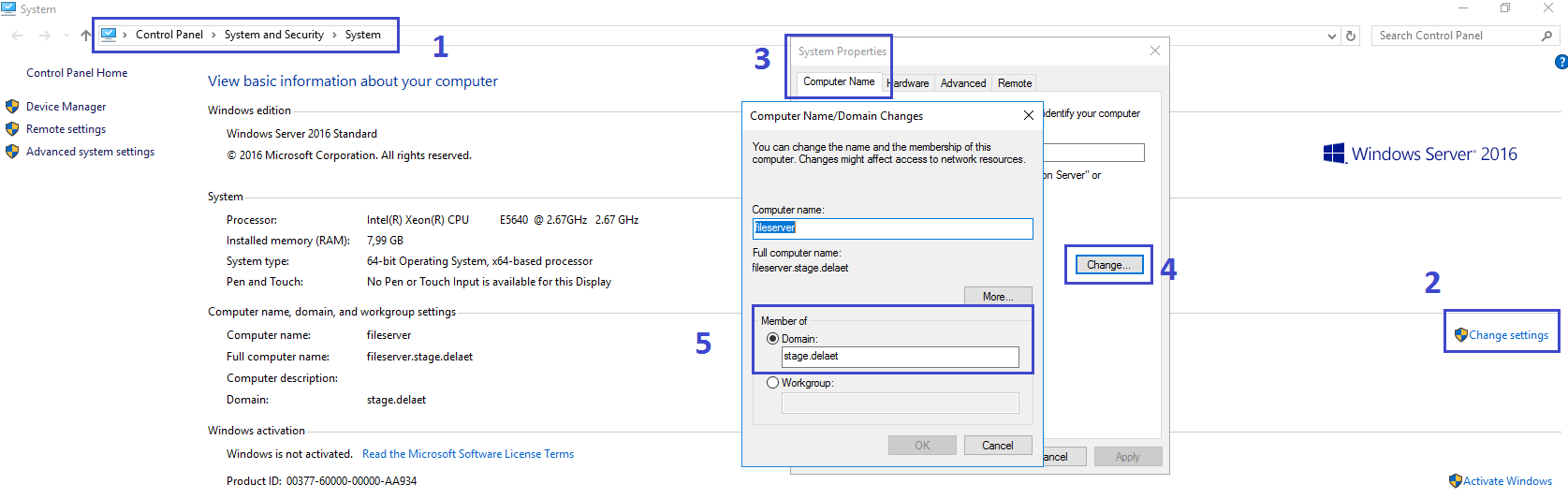
De volgende netwerkinstellingen moeten aangepast worden op de StorageZone-Controller (SZ-C) om de communicatie met de AD DNS-server en de NetScaler correct te laten verlopen.



Voorzie hem van hetzelfde subnet als de NetScaler en AD-server.

Voorzie hem van een statisch IP-adres.

Gebruik de correcte DNS-server.



Voeg hem toe aan het AD-domein.

Server Manager

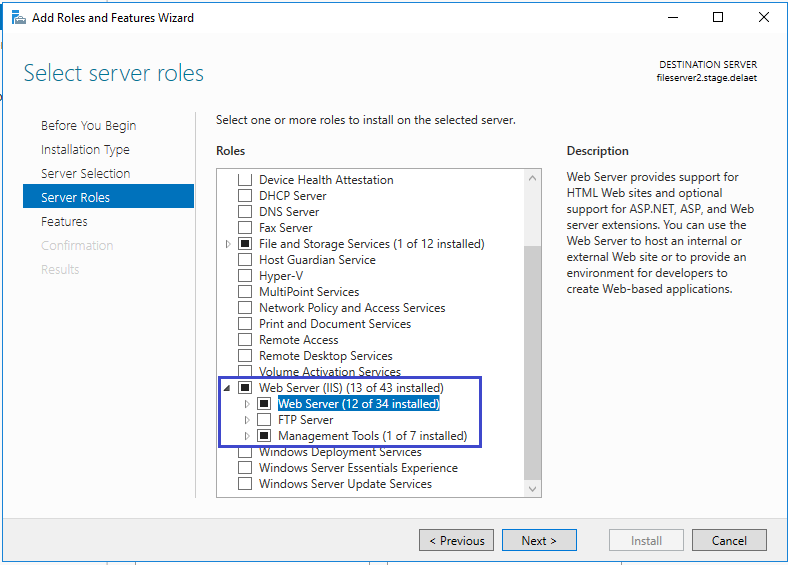
Een deel van de storage zone configuratie gaat door in Server Manager. De Internet Information Services (IIS) server role moet geïnstalleerd worden zodat de SZ-C over HTTPS bereikt kan worden als een web server. Bovendien moet er ASP.NET ondersteuning zijn voor het configuratiescript.

Een certificaat zal toegevoegd moeten worden om HTTPS-communicatie tussen NetScaler en SZ-C mogelijk te maken. Er zal ook een HTTPS-binding voor de default website aangemaakt moeten worden.

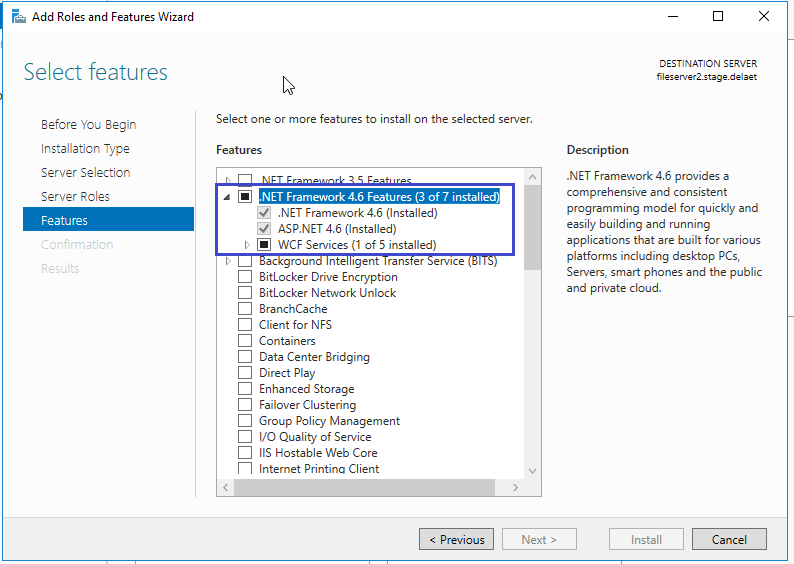
Server rollen en functies

Binnen Server Manager, ga naar “beheer” en druk op “toevoegen van rollen en functies”.

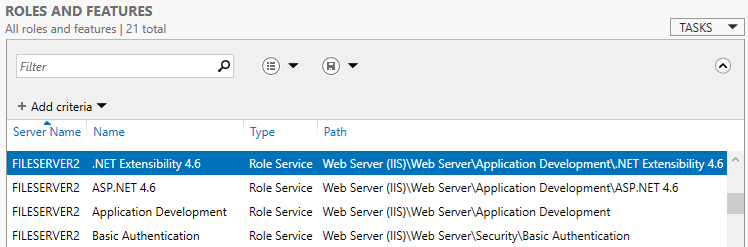
Selecteer de huidige server.



Selecteer de Web Server (IIS) rol, zie de blauwe kader in bovenstaande figuur. Druk op volgende.



Selecteer de meest recente .NET framework functie, zie de blauwe kader in bovenstaande figuur. Druk op volgende.



Selecteer basis authenticatie en de meest recente ASP.NET service. Druk op volgende.

Druk op finish.

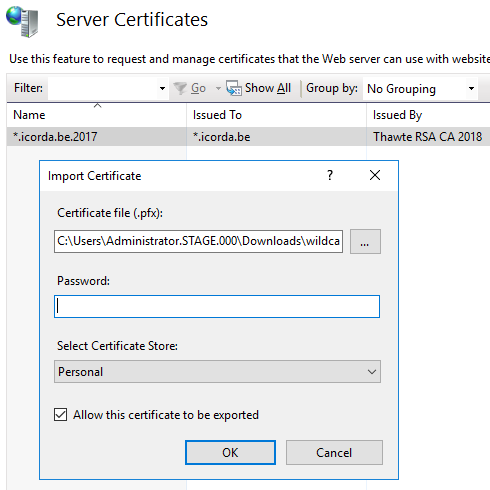
IIS Manager

Binnen Server Manager, ga naar “tools” en druk op “Internet Information Services (IIS) Manager”.

Druk op de huidige server.

Ga naar de server certificaten.

Klik op importeer.



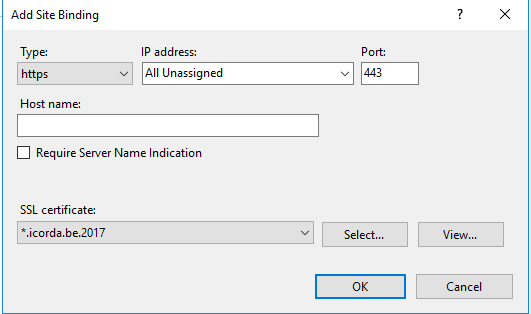
Selecteer een wildcard of een zelf gesigneerd certificaat.

Geef het juiste wachtwoord op indien het importeren van het certificaat beveiligd is.

Kies voor de personal certificatenstore en sta toe dat het certificaat geëxporteerd wordt zoals in de afbeelding hierboven.

Ga naar sites, standaard website.

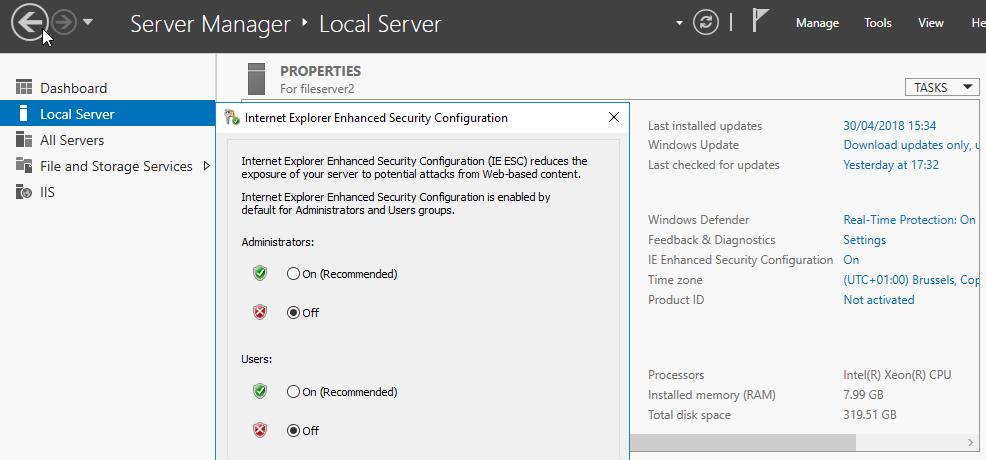
Klik op bindingen.



Voeg een site binding toe van het type HTTPS, met poort 443 en selecteer het vooraf geïmporteerd certificaat zoals zichtbaar op de afbeelding hierboven kan zien.

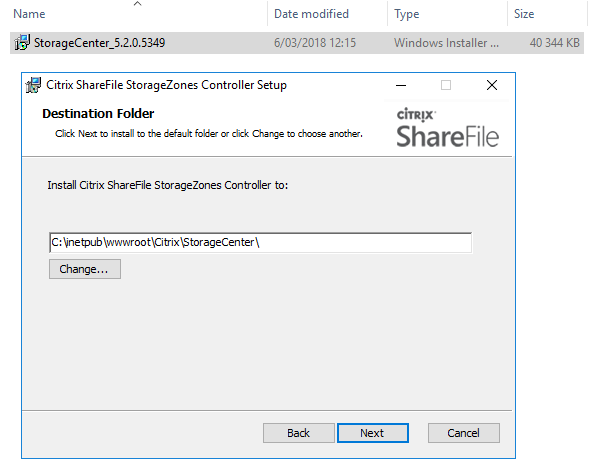
StorageZone-Controller (SZ-C)

Binnen Server Manager, ga naar de lokale server.



Schakel de Internet Explorer versterkte beveiligingsconfiguratie uit in eigenschappen.

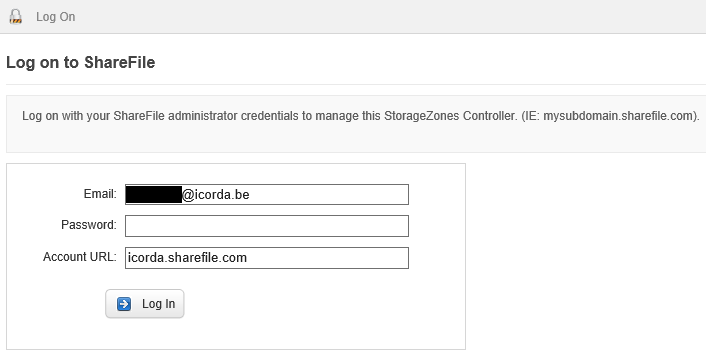
Haal het meeste recente SZ-C installatiebestand van de Citrix website. In deze opstelling werd SZ-C versie 5.2 gebruikt.



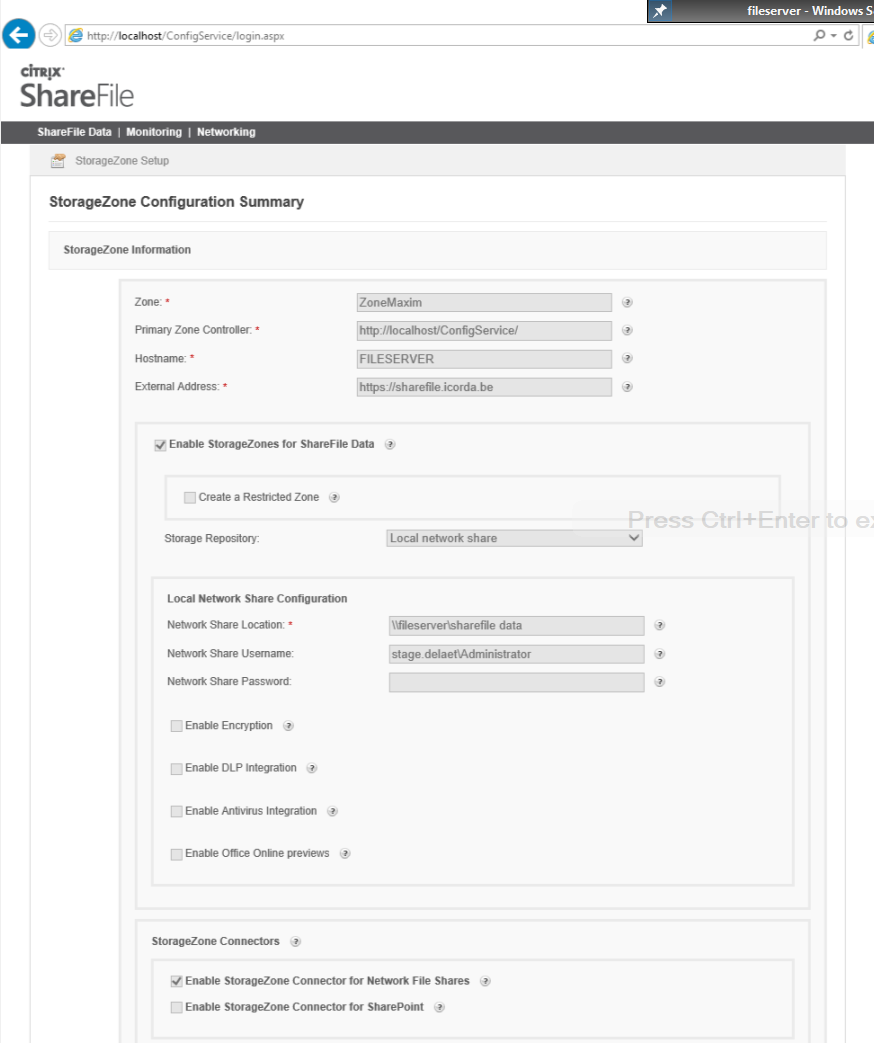
Installeer de zone met het .EXE-bestand. Kies de standaardinstellingen. De zone zal in de wwwroot folder van de webserver geïnstalleerd worden, zodat ze bereikbaar is over het internet.

Start de computer opnieuw op.

Browse naar het “ConfigService/admin.aspx” script op de lokale webserver met een internetbrowser.



Meldt aan met een ShareFile account dat administratorrechten bezit. Vul de ShareFile account URL in, dit subdomein is standaard van de vorm “bedrijfsnaam.sharefile.com” zoals in de afbeelding hierboven.



Kies voor een nieuwe lokale StorageZone (SZ).

Geef de SZ een naam, deze zonenaam verschijnt in ShareFile.

De primaire SZ-C moet naar het script verwijzen.

Vul de hostname van de SZ-C in.

Geef het externe adres van de NetScaler zijn CS-VS op.

Check of het selectievakje “SZ voor ShareFile data” aangevinkt is.

Kies voor een lokale netwerkshare als opslagplaats.

Geef de locatie van die netwerkshare op volgens de uniform naming convention schrijfwijze.

Geef het gebruikersnaam en wachtwoord op van een account met ‘full control’ rechten op de netwerkshare.

Indien gewenst kan encryptie ingeschakeld worden.

Selecteer de optie voor het ontgrendelen van de SZ-C voor netwerkshares.

Indien gewenst kunnen bepaalde paden binnen de share toegestaan of geblokkeerd worden.

Geef een wachtwoord op, dit wachtwoord wordt gebruikt indien encryptie ingeschakeld zou worden. Het wachtwoord moet goed bewaard worden, het wordt opnieuw gevraagd indien er extra Controllers opgezet worden voor deze zone.

Extra StorageZone Controllers

Maak een tweede Windows server aan en doorloop alle stappen vermeld onder “netwerkconfiguratie” en “Server Manager”.

Doorloop de installatie van de SZ zoals vermeld onder “StorageZone-Controller” en meldt aan op dezelfde manier.

Kies ditmaal voor het toetreden tot een bestaande SZ en kies voor de reeds aangemaakte zone.



Vul de hostname van de primaire SZ-C in.

Vul de hostname van de huidige secundaire SZ-C in.

Geef het externe IP-adres van de NetScaler zijn CS-VS opnieuw in.

Geef hetzelfde wachtwoord als bij de configuratie van de primaire Controller op.

Hou er echter rekening mee dat in een praktische omgeving ook de netwerkshare ontdubbelt moet worden over verschillende fileservers alvorens de lokale gegevens volledige redundant zijn. Dit wordt praktisch meestal bereikt door gebruik te maken van Windows DFS zoals dat in hoofdstuk 4.2.3 reeds vermeld werd.

# B-3 - ShareFile configuratie guide

Op ShareFile valt er niet veel te configureren. Na de SZ-configuratie werd reeds meegedeeld aan de ShareFile Cloud via welk adres de zone bereikbaar is.

## SSO

Het is wel nog mogelijk van SAML SSO te voorzien om aan te kunnen melden op de ShareFile zonder telkens de nodige gebruikersgegevens te moeten voorzien. De configuratie hiervan kan teruggevonden worden in de administrator instellingen bij het login & security policy.





Vul het ShareFile subdomein URL gevolgd door de string “/saml/info” in als ShareFile issuer.

Vul als IDP issuer de externe URL van de NetScaler in.

Vul dit adres aan met “/saml/login” en “/cgi/tmilogout” respectievelijk voor de standaard login en logout pagina’s van NetScaler.

Kopieer het *certificaat gedeelte* (dat is het eerste tekstgedeelte van het certificaat, zonder de sleutels die daarop volgen) van het certificaat dat gebruikt wordt door de CS-VS. Gebruik dit voor het X.509 certificaat dat ShareFile nodig heeft voor de SAML-authenticatie met NetScaler.

Optioneel kan je aangeven of SSO verplicht nodig is om aan te melden op de ShareFile Cloud. In dat geval zal elke verbruiker verplicht via SAML moeten aanmelden en kan dit niet meer manueel gedaan worden.

Je kan kiezen of het certificaat verzonden wordt in een POST of een REDIRECT.

Het is aangeraden om de authenticatie web gebaseerd te laten verlopen, NetScaler ondersteunt deze methode het best.

In deze opstelling wordt gebruik gemaakt van de sAMAccountName voor authenticatie, dit is een vorm van Integrated Windows Authentication (IWA). Kies voor een minimale vergelijking bij de authenticatie.

Voltooi de configuratie.

Open de configuratie opnieuw om het certificaat dat ShareFile voor SAML gegenereerd heeft te kopiëren. Dit is het ISP certificaat dat thuishoort in de NetScaler configuratie. Zie de NetScaler configuratie guide hiervoor.