# NetScaler configuratie guide (NS12)

Voor ShareFile met lokale StorageZones

## Omschrijving van de opzet

Opzetten van een Citrix ShareFile met een 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)

NetScaler is voorzien van een ingebouwde “NetScaler voor ShareFile setup” vanaf versie 10.5. Die standaard setup is geen verplichting, maar het kan de configuratie veel sneller en gemakkelijker maken. Om een volledig functionele opstelling met optimale beveiligingsmaatregelen en gebruikerservaring te bekomen is het aangeraden om dieper in te gaan op elke component en uit te zoeken welke extra configuratie deze nodig acht.



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

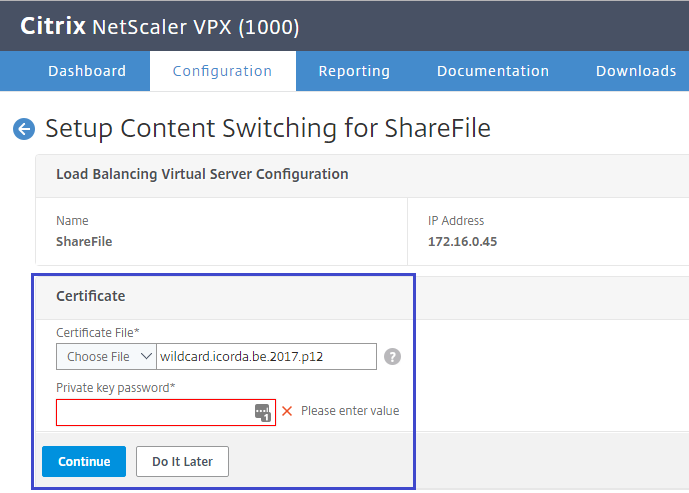
Navigeer naar traffic management en klik op “Setup NetScaler for ShareFile”.

### Content switching virtuele server (CS-VS)

Vul het correcte IP-adres in dat gebruikt wordt om van de NetScaler (en achterliggende StorageZone) van buitenaf te bereiken. Dit kan een DMZ IP-adres zijn indien ze correct geNAT wordt naar het publieke 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.



Importeer een certificaat vanuit je NetScaler of je vanop je lokale serveropslag.

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

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

Kies voor “Add New 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 StorageController server (in de default IIS-pool bijvoorbeeld). Dat certificaat mag zelf gesigneerd zijn.

### AAA virtuele server (AAA-VS)

Kies voor “Configure New” in de LDAP-authenticatie.

Geef daar als eerste een IP-adres op voor de AAA-VS, dit mag gewoon een ongebruikt intern IP-adres zijn indien hij enkel dient voor AD-authenticatie.

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

Voorzie de correcte poort 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 best 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 Logon Name wordt meestal gekozen voor het oudere “sAMAccountName” of het nieuwere “userPrincipalName”. De eerste wordt ook ondersteund door pre Windows 2000 machines. Alhoewel de schrijfwijze van een “userPrincipalName” gekender is, heeft het hier geen voordelen aangezien de AD-authenticatie automatisch.

Standaard zal de NetScaler voor ShareFile setup gebruik maken van basic policies. Aangezien deze verouderd zijn raadt Citrix aan om deze 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.



## Extra configuratie

Verder moeten er nog wat zaken geconfigureerd worden binnen NetScaler alvorens de opstelling correct zou functioneren. Er zijn tevens een aantal extra’s die optioneel kunnen toegevoegd worden aan deze opstelling, maar niet nodig zijn voor een correcte werking ervan.

### Netwerkinstellingen

Navigeer naar system 🡪 network onder het configuration tabblad.

#### IP-adressenC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_IP.png

Onder het menu-item “IPs” kan je de IP-adressen terugvinden die reeds aangemaakt werden tijdens het doorlopen van de setup. Hier moeten nog subnet IP-adressen aangemaakt worden dat de communicatie van de NetScaler naar buiten toe werkt. Voor elk subnet waarin de NetScaler actief is zal zo een subnet IP-adres moeten voorzien worden. Indien de opstelling gebruik maakt van een interne AD DNS-server en SZ, zal een intern subnet IP-adres aangemaakt moeten worden. Binnen de DMZ moet er ook een subnet IP-adres voorzien worden die de communicatie tussen NetScaler en het internet mogelijk maakt.

#### InterfacesC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_Interfaces.PNG

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

#### Virtual local area network (VLANC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_VLAN.PNG)

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 toegevoegd worden. Vergeet niet van de passende interfaces te binden aan het correcte VLAN-nummer tijdens de configuratie.

#### RoutesC:\Users\Stagair1\Documents\Stage_en_BP_2018\documentatie\NetScaler\NetScaler Config afbeeldingen\ShareFile_Routes.PNG

Onder het menu-item “Routes” kunnen routes aangemaakt worden zodat NetScaler weet waar hij het verkeer dat bestemd is voor een bepaald subnet naartoe kan sturen. Standaard zal voor alle gekend IP-adressen reeds een route aangemaakt zijn door NetScaler. Indien de nodige subnet IP-adressen aangemaakt werden zal je zien dat het verkeer bestemd voor het DMZ subnet al een route gekregen heeft naar het bijhorende subnet IP-adres. Er moet dus enkel nog een default route voor al het ongekende internetverkeer aangemaakt worden. Die route krijgt 0.0.0.0 als IP-adres en subnet masker en de passende default gateway van de DMZ als gateway adres.

### Cipher suites (optioneel)

Om de kans op succesvolle aanvallen van hackers te minimaliseren is het aangeraden om enkel de veiligste SSL-verbindingen toe te laten. Om de Virtual Servers in NetScaler te verplichten 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 door op de ‘Add’ knop te drukken.

Geef de nieuwe Cipher groep een passende naam.

Begin met het toevoegen van Cipher suites door op de ‘Add’ knop te drukken.

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

Om HTTP-verbindingen te vermijden is het ook nog mogelijk om HSTS aan te zetten in de SSL-parameters secties van de opgestelde virtuele servers (CS-VS, LB-VS, AAA-VS).

Indien gewenst kunnen SSLv3, TLSv1 en TLSv1.1 ook uitgeschakeld worden in dezelfde SSL-parameters secties.

### Single sign-on (SSO) (optioneel)

Alhoewel het in deze opstelling niet nodig is om extra configuratie uit te voeren voor het bekomen van SSO, kan het toch handig zijn om te weten hoe SAML 2.0 en OAuth 2.0 geconfigureerd worden in NetScaler. SAML en OAuth kunnen namelijk gebruikt worden voor SSO in applicaties die aan ShareFile gekoppeld worden.

#### SAML 2.0

#### OAuth 2.0

### NetScaler Gateway (indien van toepassing)