# Lijst met gebruikte symbolen en afkortingen

2FA two-factor authentication

AAA Authentication, Authorization and Accounting

AD Active Directory

CA certificate authority

CIFS Common Internet File Systeml

DaaS Directory as a Service

DMZ demilitarized zone

DNS Domain Name System

ERP Enterprise resource planning

HA high availability

HTTPS HyperText Transfer Protocol Secure

IaaS Infrastructure as a Service

ICT Informatie en Communicatie Technologie

IDP identity provider

IP internetprotocol

ISO International Organization for Standardization

LDAP Lightweight Directory Access Protocol

OAuth Open Authorization

OpenID OpenID Connect

PaaS Platform as a Service

PFS perfect forward secrecy

QMP Quality Management Principles

RADIUS Remote Authentication Dial-In User Service

SaaS Software as a Service

SAML Security Assertion Markup Language

SAP Systeme, Anwendungen und Produkte in der Datenverarbeitung (bedrijf)

SLA service-level agreement

SP service provider

SSO single sign-on

URL Uniform Resource Locator

VPN virtual private network

# Omschrijving van de opzet

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



:::::::::::::::::::::::::::::::::::::::::

Gebruikers zullen aanmelden op de ShareFile en indien nodig bestanden opslaan op of ophalen van de lokale StorageZone. De ShareFile stuurt hiervoor de query’s van de gebruiker naar de content switching virtuele server (CS-VS) van de NetScaler. Vooraleer een gebruiker toegang krijgt tot de lokale StorageZone zal de CS-VS verbinding maken met de AAA virtual server (AAA-VS). Die bezit de nodige policies om te oordelen of de gebruiker recht heeft op de content binnen de StorageZone. Indien dit het geval is worden de gegevens doorgestuurd naar de load balancing virtual server (LB-VS) die het evenredig verdeeld over de beschikbare StorageZone Controllers (SZ-C). Door middel van de informatie opgegeven in de gebonden load balancing services weet die LB-VS waar hij met dit verkeer naartoe kan.

Op netwerkniveau adverteert de interne StorageZone de publieke FQDN waaronder hij bereikbaar is aan de publieke ShareFile Cloud. Wanneer die ShareFile connectie probeert te maken zal hij een DNS-query uitvoeren en het publieke IP-adres dat hieraan gekoppeld is achterhalen. Dit IP-adres is voorzien van een network address translation (NAT) regel in ICORDA’s firewall/router die naar het DMZ IP-adres van de NetScaler zijn CS-VS wijst. En zoals hierboven vermeld werd eindigt het verkeer op basis van enkele geconfigureerde policies en services uiteindelijk bij de lokale StorageZone.

# 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/of high availability)
* ShareFile Enterprise editie met sharefile.com subdomein

# NetScaler configuratie

Hier volgt de NetScaler configuratie die nodig is om de ShareFile Cloud te connecteren met de lokale opslag die eraan toegewezen wordt. Authenticatie voor de gebruikers met de lokale opslag gebeurt op de NetScaler a.d.h.v. de AD-credentials. Ook SSO kan geconfigureerd worden op de ShareFile en NetScaler, de configuratie die hier vermeld wordt maakt SSO mogelijk, door middel van het oudere SAML 2.0 en het nieuwere OAuth 2.0 framework.

## 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 te bekomen is het aangeraden om dieper in te gaan op elke component en uit te zoeken welke extra configuratie deze nodig acht.

### Content switching server

De eerste server dat geconfigureerd wordt tijdens de NetScaler voor ShareFile setup is de content switching virtuele server.

Eerst en vooral zal deze server voorzien moeten worden van een publiek IP-adres. Publiek betekent dat het gebruikt zal worden voor communicatie met het publieke internet. Om goed te functioneren zal men dus nood hebben aan een publiek herkend IP-adres dat in jouw bezit is of een DMZ IP-adres dat verbonden is met een publiek via een NAT-regel.

Buiten dat heeft de server ook nood aan een naam. De gekozen naam maakt eigenlijk niet zo veel uit, maar hou er rekening mee dat ze vooraf gegaan zal worden door de string “\_SF\_CS\_” (die staat voor ShareFile Content Switching server).

Omdat de communicatie tussen de NetScaler en het internet waardevolle en gevoelige informatie kan bevatten, is het uiteraard aangeraden om hem van een certificaat te voorzien zodat het verkeer over HTTPS kan lopen. In de volgende stap zal men dus een publiek aanvaard certificaat moeten voorzien. Dat certificaat kan een wildcard certificaat of een speciaal toegewijd certificaat zijn voor de NetScaler, zolang het maar gesigneerd is door een herkende certification authority (CA).

### Load balancing Server

In de volgende stap worden de load balancing servers toegevoegd, voor elke SZ-C die toegevoegd wordt aan de opstelling zal de NetScaler automatisch een load balancing service configureren. Ook wanneer slechts 1 SZ-C opgezet wordt zal de content switching server standaard zijn verkeer doorsturen naar een LB-VS.

Eerst en vooral moet het interne IP-adres van de lokale SZ-C (of indien deze ontdubbelt zijn Controllers) voorzien worden.

Dan krijgt men de keuze om de communicatie met die Controller over HTTP of HTTPS te laten verlopen. Indien de beste werkmethode gevolgd wordt moet men hier ook gebruik maken van een certificaat om HTTPS-verbindingen mogelijk te maken. Het gebruik van HTTPS is hier echter minder belangrijk omdat dit verkeer volledig intern verloopt, maar voor een optimale beveiliging zal opnieuw gebruik gemaakt worden van het wildcard certificaat. Dit certificaat zal op de Controller geïnstalleerd moeten worden, aangezien de NetScaler een beveiligde verbinding zal aanvragen bij de Controller en niet omgekeerd. Meer info hierover kan teruggevonden worden in de StorageZone configuratie. Aangezien dit certificaat enkel nodig is om intern verkeer te beveiligen kan hier ook een zelf gesigneerd certificaat gebruikt worden.

### Load balancing Service

Elke load balancing server is voorzien van een load balancing service. De “NetScaler voor ShareFile setup” koppelt zo een service automatisch. De service wordt voorzien van een IP-adres zodat de load balancing server weet naar waar hij het verkeer dat hij ontvangt moet sturen. In ons geval zal elke load balancing service het IP-adres van een lokale StorageZone Controller toegewezen krijgen.

### AAA-Server

In de laatste stap van de setup wordt de basis authenticatie geconfigureerd. Standaard zal hier gevraagd worden achter de AD-gegevens van de opstelling. Eerst en vooral wordt er gevraagd achter een IP-adres voor het opzetten van de AAA-VS, dit is de server die (zoals de naam reeds meedeelt) de authenticatie, autorisatie en accounting regelt, in hoofdstuk x werd er reeds meer verteld over AAA. In principe is het enkel nodig om een vrij IP-adres te geven dat binnen de netwerk range van het interne domein valt.

De NetScaler met zijn AAA-server zal dus instaan voor alle authenticatie van de gebruikers met de lokale StorageZone. Hij vervangt hier het werk dat meestal toegewezen wordt aan lokale servers en hij gebruikt de reeds bestaande AD-gegevens of tokens i.p.v. een nieuwe lokale database vol gebruikersgegevens.

De AD-gegevens die de NetScaler nodig heeft voor de authenticatie goed te laten verlopen zijn als volgt.

* Het IP-adres van de AD-server, de poort waarover die server zijn AD DNS verkeer stuurt.
* Het SSO-domein waar de AD-gegevens terug te vinden zijn.
* De Base DN (dit is de locatie in de AD waar de usergegevens terug te vinden zijn).
* AD-account met leesrechten

## Extra configuratie

### Policies

### Default policies

### LDAP-policy

**NetScaler**

Publiek IP-adres

**CS-VS**

**LB-VS**

**AAA-VS**

**SZ-C**

**SZ-C**

**StorageZone**

FQDN

Sharefile.icorda.be

**ShareFile Cloud**

icorda.sharefile.com