# NetScaler

## Geïmplementeerde virtuele servers

Zoals ik vorige week reeds vermeld had zijn content switching en load balancing 2 basistaken van de NetScaler. De NetScaler dient dus onder andere als één/meerdere content switching en load balancing server(s). Binnenin de NetScaler moeten er dus virtuele servers gecreëerd worden, dit is allemaal heel erg versimpeld en NS12.0 (het gebruikte NetScaler OS) voorziet al het nodige in het 'configuration tabblad'.

### Content switching

De NetScaler wordt dus ook gebruikt als content switching server dat bepaalt of het inkomend verkeer doorgestuurd wordt naar de lokale StorageZones of de ShareFile Cloud. Hij zal het verkeer ook steeds bij de tripple A server laten passeren die a.d.h.v. zelf opgestelde policies beslist of die client toegang krijgt en tot welke gegevens (lees SSO). De content switching server is hier ook de '**destination server**' voor alle clients die verbinding willen maken met de data. Daarom is ze voorzien van een **DMZ IP-adres** in het Icorda domein. Na intern overleg heb ik een DMZ IP-adres gekregen, deze is gekoppeld aan een publieke DNS binnen het Icorda domein (de DNS-server is voorzien van de nodige records), en voorzien van de nodige NAT en IP-forwarding rules (tussen de publieke IP en de DMZ IP die ik kreeg  toegewezen).

### Load balancing

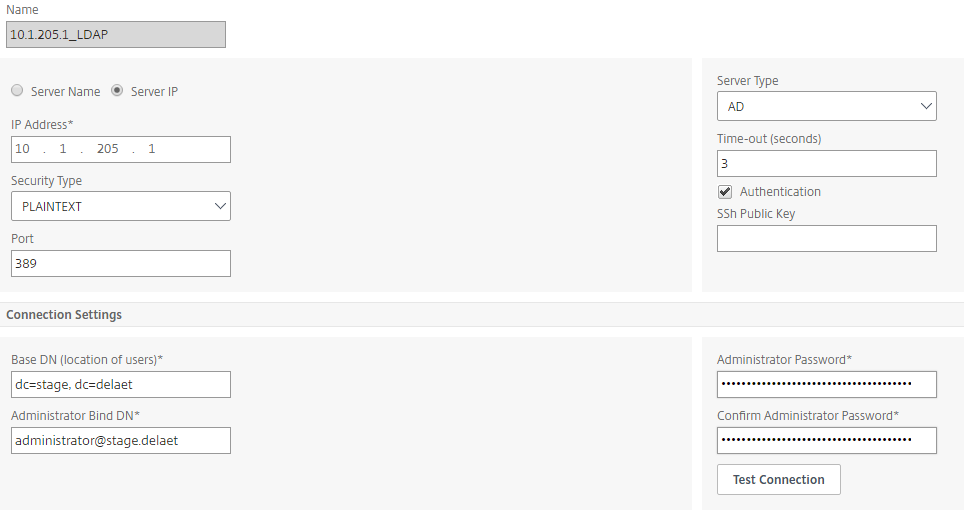
Momenteel heb ik de NetScaler voorzien van 1 SSL load balancing server. Deze zal het verkeer dat voorzien is voor de lokale StorageZone(s) evenredig verdelen over de beschikbare storage controllers (dit gaat voornamelijk over de bandwith en processing power). Op dit moment draait alles virtueel op éénzelfde IBM server en is het load balancen van minder groot belang, maar wanneer dit geheel geïmplementeerd wordt bij klanten zal dat niet meer het geval zijn, dan moet het voorzien zijn van HA over verschillende fysieke servers. (Deel 2 en 3 van de stageopdracht gaan hier dieper op in)

De virtuele load balancing server draait in de NetScaler zelf en hoeft niet voorzien te worden van een IP-adres aangezien de NetScaler (a.d.h.v. policies) weet dat het verkeerd daar langs moet lopen. De load balancing server wordt gekoppeld aan een load balancing service, dit stelt in deze opstelling de lokale StorageController(s) voor waarnaar het verkeer van de Clients hoort te lopen. Uiteraard is in mijn opstelling de 'local storage server' de StorageController voor onze lokale StorageZone. Deze service is dus wel voorzien van een IP-adres.

### AAA (Tripple A)

De tripple A authentication server is nog zo een virtuele server die op de NetScaler zelf draait. Ze heeft nood aan een ongebruikt IP-adres. Deze moet ook voorzien worden van een hoop domeingegevens (en meer) om de nodige authenticatie mogelijk te maken. De tripple A server wordt van de volgende basisinstellingen voorzien, alle andere gegevens en instellingen voor de authenticatie worden voorzien in de SSO-service dat apart geconfigureerd wordt maar samen werkt met de tripple A.

* ongebruikt intern IP-adres
* IP-adres van de domein controller
* poort waarover de DNS-communicatie met de domein controller loopt
* time out value bij communicatieproblemen
* **Single sing-on domein**
* AD locatie van de users (Base DN)
* account met administrator rechten binnen het domein
* **methode waarop de authenticatie van gebruikers word nagekeken** (hier heb ik accountnaam+ ww. gekozen, dit wordt vermeld als 'sAMAccountName')



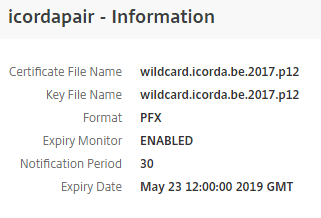
## Authenticatie & Credentials

De NetScaler is publiek bereikbaar, het verkeer van de clients naar de NetScaler moet uiteraard over een beveiligde HTTPS verbinding lopen. Daarvoor moeten er dus certificaten voorzien worden op de NetScaler. Bovendien kan een client alleen maar verbinden met de data waartoe hij rechten heeft. Voor die authenticatie wordt er gebruik gemaakt van 'Single sign-on' (SSO).

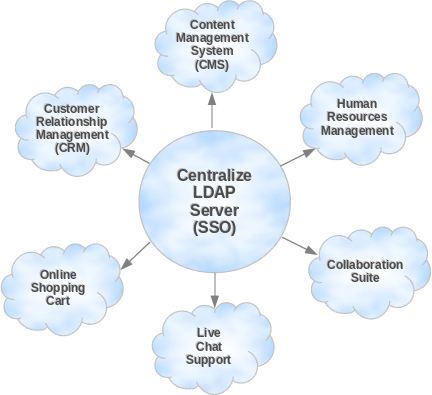
### Certificaten

Aangezien de NetScaler publiek bereikbaar is d.m.v. een URL die onder het icorda.be domein valt, moet ze voorzien worden van het **wildcard certificaat voor \*.icorda.be** om SSL-verbindingen mogelijk te maken. Alle clients die het algemene certificaat voor icorda.be vertrouwen (of alle certificaten die getrust worden door intermediate CA 'Thawte' of root CA 'DigiCert') kunnen nu een veilige verbinding met de NetScaler opzetten.

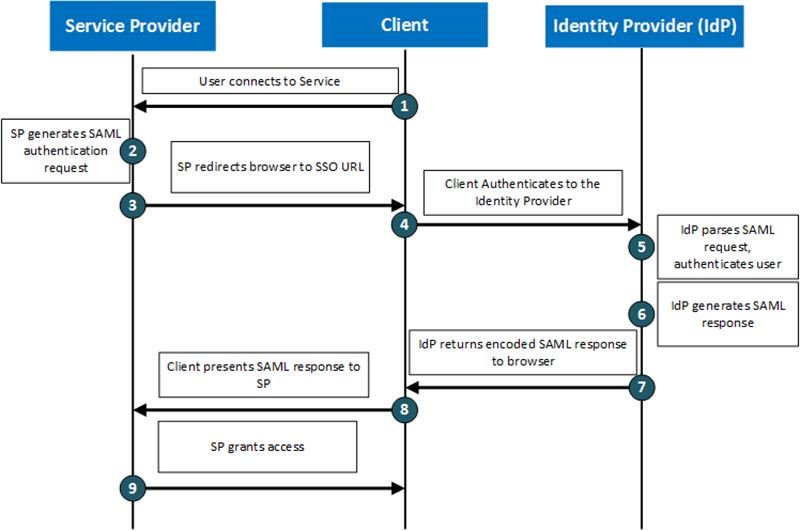
Niet alleen de wildcard- maar ook de intermediate CA- en root CA certificaten moesten hiervoor geïnstalleerd worden op de NetScaler.



### SSO



Single sign-on (SSO) is een onderdeel in deze opstelling waar ik veel tijd en onderzoek aan besteed heb. Het is een zeer interessante oplossing dat steeds meer en meer gebruikt wordt (ook in het dagelijks leven van de gewone internetgebruiker, denk aan de universele 1-click Facebook of Google login). Mijn voorkennis hierover was minimaal tot onbestaande en dit bleek ook het geval te zijn voor het merendeel van mijn collega's. Buiten het enorme potentieel voor hedendaags gebruik is het ook een heel interessant mechanisme om meer over te leren. De informatie die terug te vinden is over de werking (en zeker de configuratie) ervan is redelijk miniem. De technologie is bovendien nog steeds voor verbetering vatbaar ondanks dat het al 15 jaar bestaat. Op dit moment wordt voor SSO nog steeds (veruit) het meest gebruik gemaakt van de sterk verouderde SAML (Security Assertion Markup Language) standaard. Van de recentere OAuth (Open Authorization) en OpenID Connect standaarden is veel minder terug te vinden omdat het gebruik ervan lager ligt (ondanks de betere beveiliging en ondersteuning t.o.v. SAML). Mij leek het dan ook een uitdaging om gebruik te maken van 1 van deze nieuwere standaarden in mijn opstelling (momenteel gaat mijn aandacht naar OAuth, in principe draait OpenID ook op de OAuth standaard). **Bovendien zou ik SSO graag opnemen als een belangrijk onderwerp in mijn bachelorproef.**



Opmerking: In dit artikel wordt er over 2 verschillende domeinen gesproken (namelijk mijn intern zelf opgesteld domein waar de opstelling gebruik van maakt en het publieke Icorda domein waar alles uiteraard op draait). Om verwarring te vermeiden vermeld ik het steeds wanneer ik over het publieke Icorda domein spreek, in de andere gevallen gaat het dus om mijn Intern domein dat ik 'stage.delaet' genoemd heb.