



Ministerie van Infrastructuur en Waterstaat

Standaard Platform - Aansluitvoorwaarden Containerized Applicaties

Versie 2.0

Datum	29-03-2018
Status	Definitief

Colofon

Versie 2.0

Contactpersoon SP Cloudservices
Beheer.SP@minienm.nl

Ministerie van Infrastructuur en Waterstaat
Hoofddirectie Financiën, Management en Bedrijfsvoering
Directie Concern Informatievoorziening
Rijnstraat 8
Postbus 20906
2500 EX Den Haag

Auteurs SP Cloudservices

Inhoud

Historie	Fout! Bladwijzer niet gedefinieerd.
1	Inleiding6
1.1	Identificatie6
1.2	Leeswijzer6
1.3	Doelgroep6
1.4	Disclaimer6
1.5	Referenties6
2	Componenten8
2.1	Images8
2.2	Componentenbibliotheek8
2.3	Maatwerk applicaties.....9
2.4	Release management10
2.5	Infrastructuur10
3	Applicaties12
3.1	Services.....12
3.2	Stacks12
3.3	Configuratie.....13
4	Beveiliging14
4.1	Wet- en regelgeving14
4.2	Netwerктоegang14
4.3	Testing15
4.4	Logging15
4.5	Monitoring16
4.6	Back-up/restore16
4.7	Patches.....16
4.8	Acceptatie17
4.9	Productie en Beheer.....17

1 Inleiding

1.1 Identificatie

Dit document beschrijft de aansluitvoorwaarden voor de uitrol van “containerized applicaties” op het Standaard Platform (SP).

1.2 Leeswijzer

Hoofdstuk 2 beschrijft het aanleveren van componenten.

Hoofdstuk 3 beschrijft het uitrollen van applicaties op basis van aangeleverde componenten.

Hoofdstuk 4 beschrijft aansluitvoorwaarden op het gebied van beveiliging.

1.3 Doelgroep

De doelgroep van dit document bestaat uit SP-kanten, -brokers en leveranciers die containerized applicaties willen uitrollen/hosten op het SP.

1.4 Disclaimer

Containerization is een open standaard die een verregaande vereenvoudiging van applicatie-uitrol, -test en -beheer met zich meebrengt [Open Container Initiative, Cloud Native Computing Foundation]. Het is een nieuwe SP-eigenschap die is toegevoegd op basis van de principes [Minimum Viable Product] en “digitaal is permanent bèta” [Rapport Maak Waar]. Dit betekent dat nog niet alle (interactieve beheer) functionaliteiten volledig zijn uitontwikkeld. Het betekent ook dat klant/broker en leverancier rekening moeten houden met wijzingen in de aansluitvoorwaarden op korte termijn, alsook wijzigingen in de onderliggende containertechnologie zelf. Het laatste wordt mede ingegeven door de zich snel aanpassende containertechnologie zelf. Een belangrijke wijziging waar leveranciers rekening mee moeten houden is een toekomstige inspanningsverplichting voor een mogelijke “upgrade” van Docker Swarm naar Kubernetes.

De eerste “containerized applicaties” gaan mede hierom “gecontroleerd in productie met verhoogde dijkbewaking”. Er wordt vanuit SP Cloudservices extra beheer- en beveiligingsaandacht aan containerized applicaties geschonken; dit in samenwerking met klant/broker en leverancier.

1.5 Referenties

In dit document wordt gerefereerd naar verschillende documenten:

Referentie	Document
AVG	https://autoriteitpersoonsgegevens.nl/
BIR	https://www.noraonline.nl/wiki/BIR_(Baseline_Informatiebeveiliging_Rijksdienst)

Referentie	Document
Centraal Aansluitpunt	Diverse SP documentatie; raadpleeg SP Cloudservices
Cloud Native Computing Foundation	https://www.cncf.io/
CSR	https://en.wikipedia.org/wiki/Certificate_signing_request
DKIM-record	https://nl.wikipedia.org/wiki/DomainKeys_Identified_Mail
DMZ	https://nl.wikipedia.org/wiki/Demilitarized_zone_(informatica)
Docker	https://www.docker.com/what-docker
Docker Best Practices	https://docs.docker.com/develop/develop-images/dockerfile_best-practices/
Docker Compose	https://docs.docker.com/compose/
Docker Placement Constraints	https://docs.docker.com/engine/swarm/services/#placement-constraints
Docker Stack	https://docs.docker.com/engine/reference/commandline/stack/
Docker Swarm	https://docs.docker.com/engine/swarm/
Kubernetes	https://kubernetes.io/
Let's Encrypt	https://letsencrypt.org/
Minimum Viable Product	https://en.wikipedia.org/wiki/Minimum_viable_product
MX-record	https://nl.wikipedia.org/wiki/MX-record
Niet-destructieve wijzingen	https://blog.arkency.com/2014/04/the-biggest-obstacle-to-start-with-continuous-deployment/
Open Container Initiative	https://www.opencontainers.org
OTS	https://en.wikipedia.org/wiki/Commercial_off-the-shelf
OWASP	https://www.owasp.org
OWASP HSTS	https://www.owasp.org/index.php/HTTP_Strict_Transport_Security_Cheat_Sheet
PKI-o	https://www.pkioverheid.nl/
Rapport "Maak Waar"	https://www.rijksoverheid.nl/documenten/rapporten/2017/04/18/rapport-van-de-studiegroep-informatiesamenleving-en-overheid-maak-waar
SP Beleid Acceptabel Gebruik	SP Beleid Acceptabel Gebruik 1p0.pdf
SPF-record	https://nl.wikipedia.org/wiki/Sender_Policy_Framework
SSL Labs	https://www.ssllabs.com
The Twelve Factor App	https://12factor.net

2 Componenten

Het SP ondersteunt componenten op basis van [Docker] containertechnologie.

2.1 Images

Componenten worden als Docker Images gerealiseerd.

Eis	Omschrijving
CNA001	Componenten worden als Docker images gerealiseerd. Vooralsnog worden alleen Linux-gebaseerde images met “courante open source componenten” ondersteund. Onder “courante open source componenten” wordt verstaan: algemeen toegepaste-, veelgebruikte- en actueel onderhouden “frameworks” en “runtimes”. Onder de noemer “componenten” wordt verstaan: generiek herbruikbare componenten, applicatiespecifieke componenten, maatwerk applicaties en “Off The Shelf” systemen [OTS].
CNA002	Images worden gerealiseerd conform [Docker best practices]. Deze best practices omvatten onder andere beveiliging en het beperken van de grootte van de image files.
CNA003	Applicaties voldoen aan de principes van [The Twelve-Factor App]. Zodat deze door het SP op generieke wijze kunnen worden geschaald en hoog-beschikbaar kunnen worden uitgerold. De leverancier geeft in het technisch ontwerp aan hoe de “Twelve Factors” zijn toegepast.

2.2 Componentenbibliotheek

Componenten (Docker Images) worden aangeleverd naar een SP Componentenbibliotheek (private Docker Registry).

Eis	Omschrijving
CNA004	De SP Componentenbibliotheek bevat verschillende soorten componenten. De volgende componenten worden onderscheiden: • Generiek herbruikbare SP-componenten. Dit zijn Docker images waarvan het onderhoud, technisch beheer en ondersteuning naar derden onder de verantwoordelijkheid van SP Cloudservices valt. • Generiek herbruikbare Leverancierscomponenten. Dit zijn Docker images waarvan het onderhoud, technisch beheer en ondersteuning naar derden onder de verantwoordelijkheid van de leverancier valt. • Applicatiespecifieke Leverancierscomponenten. Dit zijn Docker images waarvan het onderhoud, technisch beheer en ondersteuning binnen de eigen applicatie onder de verantwoordelijkheid van de leverancier valt. In voorkomende gevallen kunnen generiek herbruikbare leverancierscomponenten worden verheven tot generiek herbruikbare SP-componenten. In dat geval wordt SP Cloudservices verantwoordelijk voor doorontwikkeling en beheer.

Eis	Omschrijving
	De leverancier blijft te allen tijde aansprakelijk voor het daadwerkelijk gebruik van componenten in applicaties.
CNA005	Nieuwe images zijn gebaseerd op reeds aanwezige images in de SP Componentenbibliotheek, of op images uit het publieke domein. De selectie van images uit het publieke domein wordt in overleg met SP Cloudservices bepaald en goedgekeurd.
CNA006	Nieuwe images worden aangeleverd door deze te pushen naar de SP Componentenbibliotheek. De SP Componentenbibliotheek is een private Docker Registry die wordt gehost door SP Cloudservices.
CNA007	Aangeleverde images worden door SP Cloudservices gevalideerd. Images kunnen om (beveiligings)redenen worden afgekeurd.

2.3 Maatwerk applicaties

Voor maatwerk applicaties gelden de volgende specifieke aansluitvoorwaarden.

Een aantal aansluitvoorwaarden uit een vorige versie van het SP is in dit document komen te vervallen. Dit betreft alle “niet-functionele eisen” waarvoor klant/broker en leverancier zelf verantwoordelijk voor worden geacht. Tevens wordt een aantal van de eisen reeds ingevuld door de in dit document gestelde eis van de [The Twelve Factor App].

Eis	Omschrijving
CNA008	Omgevingsspecifieke configuratie. Deze wordt door de leverancier in aparte gestandaardiseerde configuratiebestanden aangeleverd. Hiermee kan de applicatie over meerdere omgevingen worden uitgerold, zonder wijzingen in de applicatie zelf. Het formaat van de bestanden wordt in overleg met SP Cloudservices vastgesteld.
CNA009	Database wijzingen. Voor relationele DBMS worden database migratiescripts in een Docker image zelf afgehandeld. Bij voorkeur wordt uitgegaan van [Niet-destructieve wijzingen], zodat de applicatie “blijvend voorwaarts” kan worden uitgerold in plaats van te moeten worden teruggedroefd in het geval van migratieproblemen.

2.4 Release management

Eis	Omschrijving
CNA010	De naamgeving van Docker Images voldoet aan een vastgestelde naamgevingconventie. De volgende naamgevingconventie is van toepassing: <SP Docker Registry URL>/ <klantnaam of organisatie>/ <applicatiedomein of organisatie-unit>/ <componentnaam of applicatiennaam>: <versie> De <SP Docker Registry URL> refereert naar de SP Componentenbibliotheek. Voor voorbeelden, raadpleeg SP Cloudservices.
CNA011	Images worden op individuele basis geversioneerd. Zodat nieuwe versies op individuele wijze in gebruik kunnen worden genomen. Het upgraden naar nieuwe versies van herbruikbare images dient door de desbetreffende leverancier te worden aangestuurd. In het geval van herbruikbare SP-images wordt dit door SP Cloudservices zelf aangestuurd.

2.5 Infrastructuur

Eis	Omschrijving
CNA012	DNS. Het testen van een applicatie kan binnen een VPN-, of op internet plaatsvinden. Indien test binnen VPN (geleverd door SP): • Klant/broker kiest zelf een subdomein van "external-cloud.nl". • SP Cloudservices levert een interne DNS waarmee dit gerealiseerd wordt. • Aanbevolen wordt om het subdomein zoveel mogelijk te laten lijken op het uiteindelijke productiedomein. Indien test op internet: • Klant/broker kiest zelf een domein in samenwerking met de eigen DNS-provider. • Het publieke IP-adres waar dit domein op moet worden aangesloten wordt geleverd door SP Cloudservices. Voor productie: • De klant/broker kiest zelf een domein, in samenwerking met de eigen DNS-provider. • Subdomeinen van "minienw.nl" kunnen worden geleverd door SP Cloudservices. • Het publieke IP-adres waar de DNS-entry op moet worden aangesloten wordt geleverd door SP Cloudservices.

Eis	Omschrijving
CNA013	Servercertificaat. Webapplicaties en APIs worden door een load balancer ontsloten middels HTTPS. SP Cloudservices is verantwoordelijk voor de load balancer. Indien test binnen VPN: • Er wordt gebruik gemaakt van een SP test-certificaat (self-signed). • Het certificaat wordt door SP Cloudservices op de load balancer geplaatst. Indien test op internet: • Er wordt gebruik gemaakt van een [Let's Encrypt]. • Dit certificaat wordt door browsers standaard vertrouwd ("groen slotje"), omdat Let's Encrypt gebruik maakt van automatische certificaatuitgifte op basis van domeinvalidatie. • Het certificaat wordt door SP Cloudservices op de load balancer geplaatst. Voor productie: • Er wordt gebruik gemaakt van een [PKI] certificaat. • De klant/broker dient dit certificaat zelf aan te vragen bij een eigen certificaatprovider. Dit vindt plaats met een [CSR] die door SP Cloudservices wordt geleverd. • Indien gebruik wordt gemaakt van het domein "minienw.nl", kan SP Cloudservices het bijbehorende PKI certificaat aanvragen. • Het certificaat door SP Cloudservices op de load balancer geplaatst.
CNA014	Client certificaten en "trust". APIs worden, indien niet "open", met dubbelzijdig SSL ontsloten. Voor test worden zowel PKI- als SP client certificaten vertrouwd, zodat leveranciers niet worden gedwongen tot het gebruik van PKI client certificaten in een minder beveiligde omgeving (zoals bijvoorbeeld een eigen ontwikkel-PC). SP client certificaten dienen bij SP cloudservices te worden aangevraagd. Voor productie worden alleen PKI certificaten vertrouwd. Deze certificaten dienen door de afnemers van de door de klant/broker ontsloten API, zelf te worden aangevraagd bij een eigen certificaatprovider.
CNA015	Klantspecifiek maildomein. Indien gebruik wordt gemaakt van een klantspecifiek maildomein, dient klant/broker in samenwerking met SP Cloudservices zorg te dragen voor het plaatsen van corresponderende [DKIM-], [SPF-] en [MX-records] op de DNS.
CNA016	eHerkenning en DigiD. Indien gebruik wordt gemaakt van eHerkenning en DigiD, dient klant/broker in samenwerking met SP Cloudservices zorg te dragen voor het inregelen van de juiste certificaten/makelaars etc.

3 Applicaties

Applicaties worden samengesteld door middel van “service-composities” en worden naar een OTAP-omgeving uitgerold door middel van “stacks”.

3.1 Services

Applicaties bestaan uit service-composities. Deze worden samengesteld met [Docker Compose].

Eis	Omschrijving
CNA017	Services worden samengesteld met Docker Compose. Primair worden alleen op Linux gebaseerde services ondersteund.
CNA018	Services worden samengesteld uit images uit de SP Componentenbibliotheek. Deze services worden door het SP “opgespind” naar draaiende containers.

3.2 Stacks

Applicaties bestaan uit service-composities. Deze worden uitgerold met [Docker Stack].

Eis	Omschrijving
CNA019	Services worden met Docker Stack uitgerold naar een Docker cluster. Met Docker Stack worden de Docker Compose bestanden uitgerold naar een Docker cluster. Er wordt vooralsnog uitgegaan van [Docker Swarm]. De leverancier dient rekening te houden met een inspanningsverplichting voor een toekomstige upgrade naar [Kubernetes].
CNA020	De leverancier rolt uit naar “test”. De leverancier gebruikt Docker Stack om services vanuit de eigen ontwikkelomgeving uit te rollen naar test (TST) en acceptatie (ACC). Hiervoor dient gebruik te worden gemaakt van een VPN-verbinding en van een beveiligde Docker commandline interface (CLI) door middel van client-certificaten. Beide worden door SP Cloudservices ter beschikking gesteld.
CNA021	De SP-beheerder haalt images op van test naar productie. Dit gebeurt op aanwijzen van leverancier. In de toekomst kan deze handeling worden uitgevoerd door een applicatiebeheerder in plaats van de SP-beheerder.
CNA022	De applicatiebeheerder rolt uit naar productie. De applicatiebeheerder gebruikt een beheeromgeving om services uit te rollen naar pre-productie (PRE) en productie (PRD).

3.3 Configuratie

Voorafgaand en na uitrol van applicaties dient omgevingsconfiguratie te worden uitgerold.

Eis	Omschrijving
CNA023	De leverancier levert in overleg met SP gestandaardiseerde omgevingsconfiguratie op, zodat deze vooraf kan worden uitgerold. Deze omgevingsconfiguratie betreft Docker networks, -volumes, -configs en -secrets.
CNA024	De leverancier levert in overleg met SP gestandaardiseerde omgevingsconfiguratie op, zodat deze achteraf kan worden uitgerold. Deze omgevingsconfiguratie betreft bijvoorbeeld WSO2-IS Service Providers.

4 Beveiliging

Applicaties die op het SP worden uitgerold, moeten veilig zijn.

4.1 Wet- en regelgeving

Applicaties moeten voldoen aan wet- en regelgeving.

Eis	Omschrijving
CNA025	Applicaties voldoen aan de [BIR].
CNA026	Applicaties voldoen aan de [AVG].
CNA027	Applicaties voldoen aan de voorwaarden [SP Beleid Acceptabel Gebruik].

4.2 Netwerkt toegang

Applicaties dienen op veilige wijze benaderd te worden.

Eis	Omschrijving
CNA028	De applicatie wordt via een Load Balancer op internet ontsloten. De Load Balancer wordt door SP Cloudservices geleverd. Deze load balancer: • Bevindt zich in een apart netwerksegment [DMZ], zodat het netwerk van de applicatie zelf niet direct op internet toegankelijk is. • Verleent toegang tot de eindgebruiker, maar verbiedt toegang tot applicatiebeheer. • Ondersteunt alleen de netwerkprotocollen HTTP en HTTPS, op de standaardpoorten 80 en 443; elk HTTP-verzoek wordt omgezet in een verzoek voor HTTPS [OWASP HSTS]. • Verbiedt toegang door middel van SSH, zodat kwaadwillenden geen toegang kunnen krijgen tot draaiende VMs of containers. • Benadert de applicatie op poort 80.
CNA029	De applicatie wordt via een Reverse Proxy ontsloten. De leverancier richt deze reverse proxy in, op basis van een generiek herbruikbaar SP-component. De reverse proxy publiceert buiten het Docker netwerk alleen poort 80 over HTTP. De reverse proxy dient binnen het Docker cluster te worden gebruikt voor automatische service discovery.
CNA030	Alle containers in de applicatie zijn aangesloten op de Reverse Proxy. Deze containers ontsluiten zelf geen poorten buiten het Docker netwerk.

4.3 Testing

Applicaties dienen te worden getest op beveiliging, zodat veiligheid op het SP is gegarandeerd.

Eis	Omschrijving
CNA031	Docker Images worden door SP Cloudservices nagezien door middel van een “software component analyse”. Indien er zich fouten voordoen, dan worden deze in overleg door de leverancier opgelost.
CNA032	Docker Images worden door SP Cloudservices continue getest op algemeen bekende kwetsbaarheden (“Common Vulnerabilities Exposures”/CVEs). Indien er zich fouten voordoen, dan worden deze in overleg door de leverancier opgelost.
CNA033	Functionele- en performance tests worden door leverancier uitgevoerd in test (TST). Indien er zich fouten voordoen, dan worden deze door de leverancier opgelost. Performance tests in TST dienen slechts als bewijs dat de tests werken. De daadwerkelijke metingen vinden plaats in acceptatie (ACC) of preproductie (PRE).
CNA034	Functionele- en performance tests worden door leverancier aangeleverd aan applicatiebeheer. De tests worden samen met omgevings specifieke configuratie in aparte gestandaardiseerde configuratiebestanden aangeleverd. Hiermee kunnen de tests over meerdere omgevingen worden uitgerold, zonder wijzingen in de tests zelf.
CNA035	Functionele- en performance tests worden door applicatiebeheer uitgevoerd in acceptatie (ACC) en productie (PRE en PRD). Zodat de applicatie geaccepteerd- en in productie genomen kan worden. Indien er zich fouten voordoen, dan worden deze in overleg door de leverancier opgelost. Naast het uitvoeren van automatische tests door applicatiebeheer, kan de klant/broker zelf ook nog optioneel handmatig gedocumenteerde tests uitvoeren.
CNA036	Beveiligingstests worden in overleg met SP Cloudservices uitgevoerd. Indien er zich applicatieve fouten voordoen, dan worden deze in overleg opgelost.

4.4 Logging

Draaiende applicaties worden gelogd.

Eis	Omschrijving
CNA037	De leverancier draagt zorg voor logging naar de console. Zodat deze kan worden aangesloten op centraal logmanagement.
CNA038	De leverancier draagt zorg voor logfile rotating. Zodat de “storage” niet volloopt. Logfile rotating is van toepassing op alle applicatieve logfiles die zich binnen het cluster bevinden.

4.5 Monitoring

Draaiende applicaties worden gemonitord.

Eis	Omschrijving
CNA039	De leverancier geeft aan hoe services kunnen worden aangesloten op de monitoring tooling van het SP. Dit betreft minimaal het aanbieden van een applicatieve "Health Check URL" (/health) en een "Metrics URL" (/metrics).

4.6 Back-up / restore

Draaiende containers kunnen worden vervangen. Productiedata wordt gewaarborgd. Blue/green switches zijn eenvoudig uit te voeren.

Eis	Omschrijving
CNA040	Er wordt gebruik gemaakt van Docker Volumes. De leverancier maakt gebruik van Docker volumes, zodat deze een container-herstart overleven.
CNA041	Containers die verwijzen naar Docker Volumes maken vooralsnog gebruik van [Docker Placement Constraints]. In een later stadium komt deze eis te vervallen, zodra het SP volume-drivers naar centrale storage (buiten het Docker cluster) ondersteunt.
CNA042	In overleg met klant / broker wordt door SP Cloudservices een periodieke back-up van de productiedata gemaakt. Standaard wordt uitgegaan van back-ups op basis van Docker volumes. De leverancier geeft aan welke storagebehoefte een applicatie heeft.
CNA043	Op verzoek van klant / broker wordt door SP Cloudservices een restore uitgevoerd.

4.7 Patches

Het container "Host OS" en de container images worden op regelmatige wijze gepatched zodat deze aan de laatste beveiligingsstandaarden voldoen.

Eis	Omschrijving
CNA044	SP Cloudservices patcht het "host OS" van het Docker cluster. De leverancier dient rekening te houden met periodieke patches. Deze worden door SP Cloudservices aangekondigd en worden op geleidelijke wijze op de omgevingen van de OTAP-straat toegepast.
CNA045	De leverancier van een image draagt zorg voor het patchen van het image. Security patches worden zo snel mogelijk doorgevoerd. Dit wordt nader gespecificeerd in een SLA.

4.8 Acceptatie

Eis	Omschrijving
CNA046	Afspraken m.b.t. acceptatie worden door SP Cloudservices en leverancier gezamenlijk vastgesteld in een separate Dienstverleningsovereenkomst (DVO).
CNA047	Het document [Beheerst naar Beheer] wordt als richtlijn gebruikt.

4.9 Productie en Beheer

Eis	Omschrijving
CNA048	Het uitrollen van een applicatie naar productie is een separate beheertaak. Nadere afspraken worden door SP Cloudservices en klant/broker gezamenlijk vastgesteld in een separate Dienstverleningsovereenkomst (DVO).
CNA049	De applicatiebeheerder is namens de klant / broker verantwoordelijk voor het correcte gebruik van productiedata. Nadere afspraken worden door SP Cloudservices en klant/broker gezamenlijk vastgesteld in een separate Dienstverleningsovereenkomst (DVO).