Rijksinstituut voor Volksgezondheid
en Milieu
*Ministerie van Volksgezondheid,
Welzijn en Sport*

Van:
5.1.2e 5.1.2e 5.1.2e 5.1.2e

Aan:
5.1.2e 5.1.2e 5.1.2e 5.1.2e

A. van Leeuwenhoeklaan 9
3721 MA Bilthoven
Postbus 1
3720 BA Bilthoven
www.rivm.nl
KvK Utrecht 30276683
T 030 274 91 11
F 030 274 29 71
5.1.5@rivm.nl

**Datum**
22 april 2020

**Behandeld door**
5.1.2e 5.1.2e 5.1.2e

# memo

Hosting Infectieradar Castor-oplossing

## Achtergrond

Binnen het centrum EPI is men op zoek naar een alternatief voor de infectieradar. De infectieradar wordt ingezet in de strijd tegen het Corona virus. De infectieradar wordt gevoed doordat mensen op uitnodiging een vragenlijst invullen. De deelnemers krijgen na aanmelding wekelijks een vragenlijst die ingevuld moet worden. De verzamelde data wordt vervolgens verwerkt. Op deze manier wordt onderzoek gedaan naar de verspreiding van Corona.

De eerste versie van de infectieradar tool is na een korte tijd online gedraaid te hebben, offline gehaald omdat er security problemen met de app waren. Vanuit de IV-organisatie hebben we vervolgens een oplossing met Formdesk aangeboden en deze is nu in gebruik. Deze oplossing wordt door EPI als (te) bewerkelijk ervaren en er is een zoektocht geweest naar een geschiktere tool, die nog beter aansluit op de behoefte.

Daarbij is men uitgekomen bij de tool "Castor". Castor heeft inmiddels een offerte aangeboden, waarmee EPI akkoord is. We staan nu voor de uitdaging om deze tool op zeer korte termijn operationeel te krijgen.

Omdat per 11 mei de scholen weer open gaan, heeft EPI de sterke wens om al per 2 mei te kunnen opschalen en Castor operationeel te hebben. Ook heeft EPI de ambitie voor het aantal respondenten binnen het onderzoek opgeschroefd van 100.000 naar een veelvoud daarvan, tot wel één miljoen. Op dit moment doen binnen de Formdesk oplossing zo'n 35.000 burgers mee met dit onderzoek.

.

**Opties voor de hosting van de Castor-software**

Voor de hosting van de software zijn er drie opties geschetst:

1. Azure cloud van de leverancier (SAAS)
2. Azure cloud van het RIVM (IAAS)
3. Datacenter van het RIVM (Equinix)

**Ad 1. Azure cloud leverancier (SAAS)**

Castor heeft een aanbieding gedaan om het product voor RIVM te hosten in een Azure cloud oplossing.

Voordelen:

- Castor geeft aan binnen 5 werkdagen de applicatie beschikbaar te hebben voor load testing.
- Beperkte effort vanuit SSC-Campus om het project werkend te krijgen.
- Beperkte beheer last voor SSC-Campus.

Nadelen:

- We zetten RIVM-data in de cloud: dit geeft haken en ogen die vanuit security-optiek moeten worden getackeld (zie bijlage 1).
- Kosten voor licentie + hosting liggen zo hoog dat er aanbesteed moet worden. Contract management geeft aan dat er geen sprake meer is van een overmacht situatie, daardoor blijven de regels voor normaal aanbesteden onder rijksraamcontract gelden.
- Er is afhankelijkheid met betrekking tot beschikbaarheid van Microsoft Azure dienstverlening. Hiervoor bestaat een wachtrij, zeker voor commerciële partijen. Mogelijk kunnen we vanuit RIVM/VWS hier een voorrangspositie voor regelen.

**Ad 2. Azure cloud RIVM (IAAS)**

Dit betreft een eigen RIVM Azure cloud via Surfnet.

Voordelen:

- Geen

Nadelen:

- De RIVM Azure cloud via Surfnet is nog niet volledig ingericht en is niet gereed voor productie;
- Ook op security gebied moet er nog heel veel worden ingeregeld (zie bijlage 1)
- Behalve virtuele machines moet ook netwerk, loadbalancing en beveiliging nog worden ingeregeld.
- Er is weinig ervaring met Azure Cloud binnen SSC-Campus.
- Afhankelijkheid en wachtrij Microsoft Azure dienstverlening.
- Het gewenste tijdpad zal bij lange na niet worden gehaald.

**Ad 3. Datacenter RIVM (Equinix)**

Dit betreft hosting op onze bestaande infrastructuur met virtual machines.

Voordelen:

- Bekende hosting techniek voor SSC-Campus waar voldoende ervaring mee is.
- Beheer processen zijn ingericht en ingewerkt team (samenwerking in de keten).
- Gegevens in Rijksdatacenter (secure)
- Uitnutten eigen infra en de investeringen die hierin zijn gedaan (Robuuste Infrastructuur)

Nadelen:

- Beschikbaarheid voldoende BI-resources (deze zijn nu ingezet op andere werkzaamheden).
- Er is onbekendheid met de load die de applicatie genereert, met kans op performance problemen in de infrastructuur. Dit risico bestaat ook voor de twee eerdere opties, maar bij hosting in de cloud van de leverancier ligt de verantwoordelijkheid voor te nemen maatregelen bij de leverancier zelf.

**Gevraagd besluit**

Om het project voor de implementatie van Castor voor de Infectieradar te kunnen opstarten en nog enige kans te hebben de gewenste live-datum te kunnen behalen moet er op hele korte termijn een keuze gemaakt worden uit de bovengenoemde opties.

Optie 2 Azure Cloud RIVM valt wat mij betreft af. Deze omgeving dient eerst op een gedegen manier te worden opgetuigd en dit is niet mogelijk binnen deze "haastig en spoed" opdracht.

Optie 1 Azure Cloud Leverancier valt wat mij betreft af, omdat hiervoor eerst een aanbesteding gedaan zal moeten worden. Als deze optie wel tijdig behaald zou kunnen worden, dan leggen we veel risico's bij de leverancier (wij hebben er zelf geen omkijken naar), echter het is de vraag of het onderzoek daarbij gediend is.

Optie 3 Datacenter van het RIVM (Equinix) heeft wat mij betreft de voorkeur. De leverancier is bereid ons volop te ondersteunen in de implementatie. Bovendien hebben we ervaring opgedaan met een hoge load en hoe we dit op een goede manier kunnen managen. We houden hier zelf de volledige regie in. De data staat in een Rijksdatacenter (zie de discussie aangaande de Corona-app hoe gevoelig dit ligt). We hebben als RIVM ongeveer € 150K minder "out of pocket kosten" ten opzichte van Optie 1. En we doen waar we m.i. voor bestaan: namelijk het mogelijk maken van (RIVM) onderzoek. In de toekomst zouden wellicht ook andere onderzoeken van dit platform en onze ervaring gebruik kunnen maken.

Om de kans op het halen van de door EPI gewenste deadline zullen dan wel de voor deze noodzakelijke resources vanaf dit moment hiervoor moeten worden beschikbaar gesteld.

Bijlage 1

Advies security management SSC-Campus

Hi,

Naar aanleiding van jouw vraag **of infectieziekten radar in de publieke Cloud** gebouwd kan worden heb ik de volgende overdenkingen. Hierbij ben ik ervan uit gegaan dat het gaat om een applicatie met privacy gevoelige gegevens en dat SSC-Campus nog geen ervaring, noch sluitende contracten heeft met een Cloudleverancier.

SLM Rijk is van mening dat organisaties zelf een moeten risicoassesment uitvoeren en dan kunnen besluiten of er gebruik kan worden gemaakt van " Microsoft cloud applicaties". Het risico (reputatie, misbruik, continuiteit, AP veroordeling) ligt dan ook heel duidelijk bij de partij die ervoor kiest de cloud te gaan gebruiken.
Daarom is een risicoanalyse en waar nodig een DPIA noodzakelijk. Beide kosten veel meer tijd bij een Public Cloud oplossing dan bij een in-house oplossing.

Een dergelijke case -maar dan veel eenvoudiger- heeft eerder gespeeld: Toen het KNMI gebruik wilde gaan maken van Cloud applicaties. Toen was op basis van een risicoanalyse (kost weken tijd) het de CIO-Security die het gebruik van de Cloud door het KNMI heeft tegengehouden omdat de netwerken niet 100% gescheiden zijn waardoor het RIVM een -minimaal- risico liep. Uiteindelijk hebben de twee DG's de knoop doorgehakt en is het KNMI onder strenge voorwaarden Cloudtoepassingen gaan gebruiken. Dit onder protest van CIO-Security.

In dit geval gaat het veel verder: het gebruik van de Cloud om door het RIVM persoonsgegevens te verwerken. Het is niet te verwachten dat CIO-Security en FCC hier mee instemen., zelfs na een uitgebreide risicoanalyse en DPIA

Heel kort door de bocht: Qua Security zal het minimaal het BasisBeveilgingsNiveau2 (BBN2) nodig hebben. Daarvoor staat in het concept cloudbeleid Rijksdienst:

In een matrix overzicht:

| | Public Cloud | Hybride Cloud | Private Cloud (Bijv. Rijkscloud) | Non-Cloud/ on-premise |
|---|---|---|---|---|
| Volgens QIS: | | | | |
| BIR-BBN3 | Niet toegestaan | Niet toegestaan | Niet Toegestaan | Toegestaan, mits (1) |
| DepV gerubriceerd èn BIR-BBN2 | Niet toegestaan | Niet toegestaan | Toegestaan, mits (1,2) | Toegestaan, mits (1) |
| Niet-gerubriceerd, wèl BIR-BBN2 | Niet toegestaan, tenzij (1,3) | Niet toegestaan, tenzij (1,3) | Toegestaan, mits (1) | Toegestaan, mits (1) |
| BIR-BBN1 | Toegestaan, mits (1) | Toegestaan, mits (1) | Toegestaan, mits (1) | Toegestaan, mits (1) |

(1) Mits geldende kaders zijn toegepast.
(2) Mits verwerking van gerubriceerde gegevens vóóraf door de SG is goedgekeurd.
(3) Tenzij op basis van een samenhangende risicoanalyse voor kritieke processen en gevoelige data (conform komende brief AIVD over Nationale Veiligheid en gebruik van commerciële clouddiensten).

Daarbij geldt ook dat ook SSC-Campus hier goed naar moet kijken. Het is een uitbreiding van de infrastructuur buiten ons eigen beheerdomein. Dat betekent dat er gekeken moet worden naar contracten (ook al zal Surf dat goed geregeld hebben), communicatie tussen beheerders van de derde partij, garanties (op veel gebieden) van de derde partij aan SSC-Campus en of deze matchen met de eisen (die eerst vastgelegd moeten zijn) van de aanvrager, security, privacy etc.

Net zoals met andere leveranciers zal dat allemaal vastgelegd moeten worden, daarbij is contractmanagement, security en klantcontact betrokken.

En hoog over..... voor de toekomst:

Al met al is het gebruik van de Cloud zeker "a way to go" en kan in bepaalde gevallen best besparingen opleveren. Echter om dat nu "even" te gaan doen lijkt mij geen haalbare kaart. De normale route voor een dergelijke grote move zou volgens mij minmaal onderstaande stappen bevatten:

-Verkennende gespreken met potentiele leverancier (done)

-POC / kleine projecten zonder impact om te testen (??? Niet door SSC-Campus, niet volgens een proces?)

-Opstellen PvE

-Aanbesteding (hoeft niet als het via Surf is)

-Onderhandelingen zodat het technisch en juridisch framework klaar is.

-Opleiding medewerkers

-Testen communicatie met leveranciers, schrijven procedures, werkinstructies.

- Eerste projectje

- Lessons Learned, aanpassen bovenstaande.

- Vaststellen onder welke voorwaarden de Cloud interessant is. (rekenmodel- in house versus cloud, en dan nog hybride of alleen cloud)

- Tot slot gebruik, waarbij er rekening wordt gehouden met al gedane investeringen in de bestaande infra.

Dan zal er een overgangsperiode volgen waarbij de afgeschreven apparatuur vervangen wordt -onder voorwaarde- door apparatuur in de cloud.

Al met al geen "ram er maar even doorheen onder de noemer van Corona". Ik adviseer met klem om voor deze toepassing bestaande en bekende technologie te gebruiken en als de rust is teruggekeerd op een goede wijze naar het gebruik van de Cloud te gaan kijken.

Groeten 5.1.2e

Bijlage 2

Voor het hosten van Castor is flexibiliteit van belang. Het is nog niet duidelijk hoeveel bezoekers het platform daadwerkelijk gaat ontvangen. Vanuit EPI wordt uitgegaan tussen de 100.000 tot 1.000.000 bezoekers. Castor heeft daarom in hun aanbod van 1 april 2020 twee opties uitgebracht met hosting voorstellen in de Azure cloud.

De twee mogeijkheden die ze beschrijven in hun aanbod gaan om de volgende machines in Azure:

Mogelijkheid 1:

Bestaat uit 3 webserver met twee database server (master/slave). De databasen moeten 2500 connecties aan kunnen zodat het cluster samen 5000 gelijktijdige connecties aan kan.

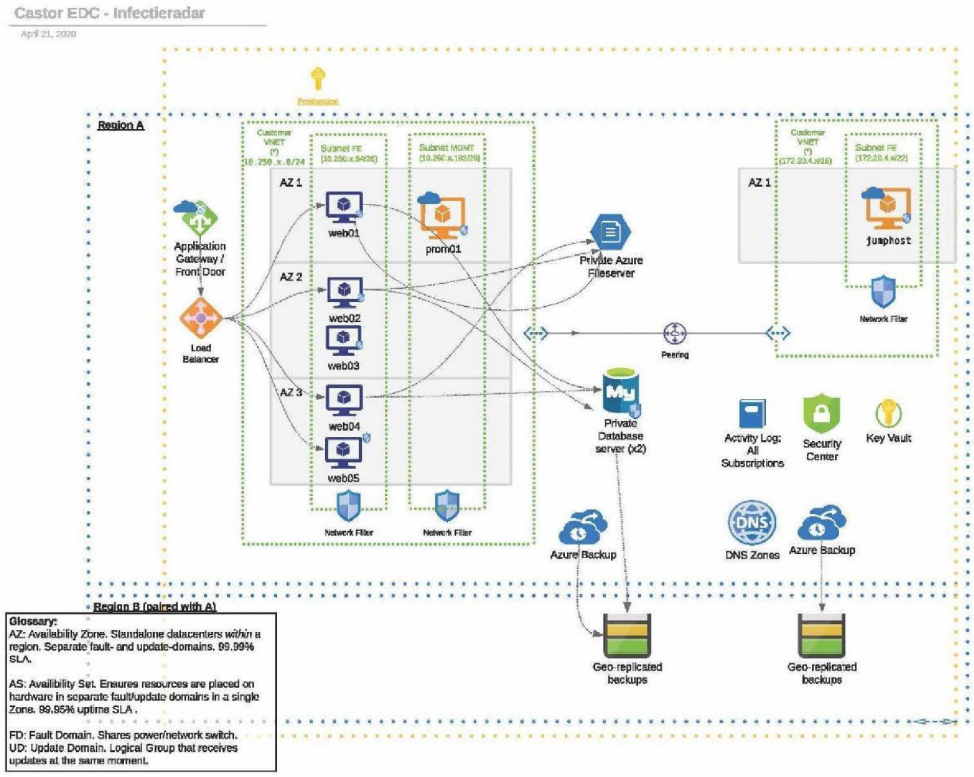
- Webserver 3 stuks, Linux Ubuntu, 4vCPU's,
- Storage 1 TB
- Database server MySQL 8 vCPU's , 1 TB opslag
- Daarbij 1 TB dataverkeer en voor de firewall rekenen ze 2 TB dataverkeer.

Mogelijkheid 2:

Bestaat uit 5 webserver met daarachter twee database machines van 64 vCPU's per machine. De verwachting is dat dit cluster in totaal 20.000 gelijktijdige gebruikers aan moet kunnen.

- Webserver 5 stuks, Linux Ubuntu, 8vCPU's
- Storage 1 TB
- Database server MySQL 64 vCPU's, 1TB opslag
- Daarbij 1 TB dataverkeer en voor de firewall rekenen ze 2 TB dataverkeer.

Systeem schets infectieradar (Castor)


Castor EDC - Infectieradar
April 21, 2020
Region A
Customer VNET (*) 10.250.x.0/24
Subnet FE (10.250.x.64/26)
Subnet MGMT (10.250.x.192/26)
AZ 1
AZ 2
AZ 3
web01
web02
web03
web04
web05
prom01
Network Filer
Network Filer
Application Gateway / Front Door
Load Balancer
Private Azure Fileserver
Peering
Private Database server (x2)
Customer VNET (*) (172.20.4.x/16)
Subnet FE (172.20.4.x/22)
AZ 1
jumphost
Network Filer
Activity Log: All Subscriptions
Security Center
Key Vault
DNS Zones
Azure Backup
Azure Backup
Geo-replicated backups
Geo-replicated backups
Region B (paired with A)
Glossary:
AZ: Availability Zone. Standalone datacenters within a region. Separate fault- and update-domains. 99.99% SLA.
AS: Availibility Set. Ensures resources are placed on hardware in separate fault/update domains in a single Zone. 99.95% uptime SLA .
FD: Fault Domain. Shares power/network switch.
UD: Update Domain. Logical Group that receives updates at the same moment.