To: (10)(2e))[(10)(2e) @politie.nl]
Cc: (10)(2e) [@dictu.nl[(10)(2e) @dictu.nl]; (10)(2e) [(10)(2e) @ctinterim.nl]
From: (10)(2e))
Sent: Thur 8/20/2020 12:10:54 PM
Subject: RE: Update t.a.v. monitoring en alarmering
Received: Thur 8/20/2020 12:10:00 PM

Top as dinsdag,
Kan je half 11 ook gelijk met mij mee aansluiten bij de weekstart van het bouwteam,

Ik zet (10)(2e) en (10)(2e) vast in de cc

Van: (10)(2e)) < (10)(2e) @politie.nl>
Verzonden: donderdag 20 augustus 2020 14:05
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: RE: Update t.a.v. monitoring en alarmering

Was echt een flitsbezoek om tempo erin te houden voor account enzo, scan pp. Moest ook direct weer weg naar midden van het land… Goed om te zien hoe het momenteel werkt in het oog van de orkaan.. ben er dinsdag van 10-12

En stuur maar door, dan krijg ik ook een beetje gevoel van de spelers op het veld…

Ciao,
(10)(2e)

Van: (10)(2e)) [(10)(2e) @minvws.nl]
Verzonden: donderdag 20 augustus 2020 13:50
Aan: (10)(2e) < (10)(2e) @p-direkt.minbzk.nl>; (10)(2e)) < (10)(2e) @politie.nl>
Onderwerp: FW: Update t.a.v. monitoring en alarmering

Hi (10)(2e) wat leuk en goed dat je er vanochtend al even bij was !!!!

Ik ga je af en toe wat mail doorsturen zodat je indruk en informatie krijgt wat er zoal speelt rond (inregelen van) dienstverlening !!

Bij deze de eerste, rond monitoring van de app en infra en middleware etc !

Grtz (10)(2e)

Van: (10)(2e) < (10)(2e) @ctinterim.nl>
Verzonden: donderdag 20 augustus 2020 09:06
Aan: (10)(2e)) < (10)(2e) @minvws.nl>
Onderwerp: Fwd: Update t.a.v. monitoring en alarmering

FYI

Begin forwarded message:

From: "(10)(2e))" < (10)(2e) @dictu.nl>
Subject: Update t.a.v. monitoring en alarmering
Date: 19 August 2020 at 19:10:00 CEST
To: "(10)(2e) >, " (10)(2e) @gmail.com'"
< (10)(2e) @gmail.com>, " (10)(2e))'" < (10)(2e) @minvws.nl>, (10)(2e)
< (10)(2e) >, " (10)(2e))'" < (10)(2e) @minvws.nl>,
" (10)(2e) @cinqict.nl'" < (10)(2e) @cinqict.nl>
Cc: " (10)(2e) @kpn.com'" < (10)(2e) @kpn.com>, (10)(2e)
< (10)(2e) @icloud.com>

Hallo allen,

Ik had jullie graag even persoonlijk gebeld om een update te geven over monitoring. Alleen gezien de tijd is dat vandaag niet gelukt. Hieronder een kort overzicht. Bij vragen graag even met mij bellen. Dit zodat ik het nu nog even kan stroomlijnen en we geen storm van mailtjes over en weer krijgen. Bij geen vragen; gelijk graag met elkaar schakelen.

Update:
Vanaf morgen gaan we een bemande operations bridge krijgen. (10)(2e) en (10)(2e) kunnen dan gewoon weer hun normale werkzaamheden oppakken.
Vanaf vrijdag gaan we stappen zetten om de monitoring te verbeteren.

Partijen en rol/actie:

1. (10)(2e)
Gaat vanaf vrijdag beginnen als (10)(2e) op het domein Monitoring & alarmering. Dit is zijn specialisme. @(10)(2e) welkom aan boord! Hij zal met een aantal van jullie contact opnemen om helder te krijgen wat nodig is. (10)(2e) is vrijdag (remote) beschikbaar en de 2 weken erop 4 dagen per week. Daarna (in week 37 t/m 39) zo'n 8 uur per week over de week verdeeld.
2. **Operations Bridge door Cinq ICT**
Vanaf donderdag 20 augustus hebben we remote support op de monitoring. Dat wordt ingevuld door Cinq ICT. (10)(2e) gaat hun instrueren (of heeft dat zelfs al gedaan) Er zullen nog wat rechten ingevuld moet (10)(2e) (10)(2e) @gmail.com', wil jij boven water krijgen welke rechten precies nodig zijn en dit via (10)(2e) regelen?
3. (10)(2e) **voor procedure/werkwijze**
(10)(2e) heeft de incident procedure onder zijn hoede. Hij stemt af wie met wie communiceert hoe we bereikbaar zijn en hoe we om gaan met acties binnen kantoortijden en acties buiten kantoortijden
4. (10)(2e)
Is vanuit CIBG kan de man waarmee geschakeld kan worden voor monitoring acties. (10)(2e) schakelt indien gewenst met andere CIBG teamleden
5. (10)(2e)
Heeft de afgelopen tijd veel gaten dichtgelopen rondom monitoring en heeft heel goed overzicht. Consulteer svp (10)(2e) waar nodig en gebruik zijn kennis en ervaring om de goede dingen te doen op dit domein
6. (10)(2e)
is de (10)(2e) aan de CIBG kant. Monitoring inhoudelijk graag regelen met (10)(2e) Andere acties zoals rechtenkwesties en dergelijke graag via (10)(2e) laten lopen.
7. (10)(2e)
is vanuit KPN (10)(2e) Graag hem betrekken / op de hoogte houden van ontwikkelingen. Afspraken naar KPN loopt in principe via (10)(2e)
8. (10)(2e)
is de (10)(2e) ((10)(2e) van Cinq ICT. Communicatie van en naar CinQ ICT loopt via (10)(2e) (10)(2e) @ (10)(2e) @cinqict.nl, wil je deze mail doorzetten naar (10)(2e) en zijn email adres met ons delen?

Hartelijke groet,
(10)(2e)

Van: (10)(2e)) <(10)(2e) @minvws.nl>
Verzonden: woensdag 19 augustus 2020 15:39
Aan: (10)(2e)) <(10)(2e) @dictu.nl>
Onderwerp: RE: monitoring en alarmering

(10)(2e) maar ik ben nu tot 16:10 in gesprek..

Van: (10)(2e)) <(10)(2e) @dictu.nl>
Verzonden: woensdag 19 augustus 2020 13:30
Aan: (10)(2e)) <(10)(2e) @minvws.nl>
CC: (10)(2e)) <(10)(2e) @minvws.nl>
Onderwerp: RE: monitoring en alarmering

Hoi (10)(2e)

Wil je me je telefoonnummer even mailen? Ik wil graag even met je bijpraten.

Dank,

(10)(2e)

Van: (10)(2e)) <(10)(2e)@minvws.nl>
Verzonden: woensdag 19 augustus 2020 13:25
Aan: (10)(2e)) <(10)(2e)@minvws.nl>; (10)(2e)) < (10)(2e) @dictu.nl>
Onderwerp: RE: monitoring en alarmering

Hi (10)(2e)

Hierbij de gegevens van (10)(2e).
Je kan met hem schakelen om uit te zoeken wat er mogelijk is.

Groeten,
(10)(2e)

Verzonden met BlackBerry Work
(www.blackberry.com)

Van: (10)(2e)) <(10)(2e)@minvws.nl>
Datum: woensdag 19 aug. 2020 8:51 AM
Aan: (10)(2e)) <(10)(2e)@minvws.nl>
Onderwerp: RE: monitoring en alarmering

Zeker.

-----Oorspronkelijk bericht-----
Van: (10)(2e)) <(10)(2e)@minvws.nl>
Verzonden: dinsdag 18 augustus 2020 17:57
Aan: (10)(2e)) <(10)(2e)@minvws.nl>
Onderwerp: FW: monitoring en alarmering

Hi (10)(2e),

Mag ik jou koppelen aan (10)(2e) (10)(2e) ?

Om te kijken wat er mogelijk is aan monitoring op middleware en applicatie niveau.

Met vriendelijke groet,

(10)(2e)
(10)(2e)
.....
Afdeling Applicatie- en servicemanagement Agentschap CIBG | Uitvoeringsorganisatie van VWS Hoftoren | Rijnstraat 50 | 2515 XP | Den Haag Postbus 16114 | 2500 BC | Den Haag .....
M (10)(2e)
@ (10)(2e)@minvws.nl
W www.cibg.nl
(10)(2e)

-----Oorspronkelijk bericht-----
Van: (10)(2e)) < (10)(2e) @dictu.nl>
Verzonden: dinsdag 18 augustus 2020 11:27
Aan: (10)(2e)) <(10)(2e)@minvws.nl>
Onderwerp: monitoring en alarmering

Hoi (10)(2e)

We komen nu in een situatie dat we meer zicht moeten hebben in onze totale oplossing. Dit zodat we op alle niveaus weten wat er speelt en we proactief acties kunnen uitvoeren. Acties om attacks tegen te gaan en acties om problemen in de techniek (infra of middelware of applicatielaag) op te lossen voordat een groot deel van het publiek problemen ondervinden en voordat het KCC of de GGD overbelast raken.

Dat vergt duidelijke en goede monitoring inclusief alarmering en follow-up.

Voor de beeldvorming: de monitoring domeinen waar we over praten zijn:
a) end 2 end monitoring
b) applicatie monitoring
c) component monitoring op netwerk, server, middelware (applicatieserver en db server)

Naast monitoring hebben we ook nodig:

d) goede dashboards
e) goed ingestelde drempelwaardes t.b.v. wanneer er een alarm af moet en wat voor urgentie het alarm heeft
f) duidelijke communicatielijnen en duidelijk wie wanneer waarvoor beschikbaar is
g) een 7x24 uur bewaking op bovenstaande
h) dagelijkse (continue) uitvoerende analyse van wat er aan de hand is
i) dagelijkse rapportage

Dit vergt veel van ALLE betrokken partijen; het bouwteam, CIBG en KPN. Belangrijk is om dit als extra opdracht op te pakken en daarnaast vandaag onderzoeken hoe we dit domein voor nu voldoende "droog" houden.

Detail info:

1 monitoring op component level (machines, CPU, disk, etc)

2 monitoring op netwerk level (porten, firewalls)

3 monitoring op basaal L4 (http requests, 500's, 200's, etc)

4 monitoring middleware (IIS, SQL server, etc)

5 application monitoring

6 end to end monitoring (en niet de gescripte onzin op privé servertjes)

7 normaal basis dashboard

8 normale warning & alarm levels

9 escalatie lijnen naar de juiste plekken _ALS_ er iets gezien wordt dat actie vereist.

10 mankracht.

11 SLA & Rapportage. Dagelijkse rapporten bandwidth, hits, requests, uniques, new users, etc, etc.

We mogen meenemen dat we nog niets gezien hebben - het begint nu pas. De mobieltjes downloaden nog _niets_ want er zijn geen TEKs. De GGDs doen nog niets - want er is niets te doen.

Dat gaat veranderen. Wat we NIET willen is een overbelaste klant contact centrum en/of (nog erger) een GGD die overbelast raakt omdat er problemen zijn op ons vlak.

Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.
De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.
The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is toegezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen. De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.
This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message. The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.
De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.
The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.
Dit bericht kan informatie bevatten die niet voor u is bestemd. Indien u niet de geadresseerde bent of dit bericht abusievelijk aan u is gezonden, wordt u verzocht dat aan de afzender te melden en het bericht te verwijderen.
De Staat aanvaardt geen aansprakelijkheid voor schade, van welke aard ook, die verband houdt met risico's verbonden aan het elektronisch verzenden van berichten.

This message may contain information that is not intended for you. If you are not the addressee or if this message was sent to you by mistake, you are requested to inform the sender and delete the message.
The State accepts no liability for damage of any kind resulting from the risks inherent in the electronic transmission of messages.

---------- Disclaimer ----------
De informatie verzonden met dit e-mailbericht (en bijlagen) is uitsluitend bestemd voor de geadresseerde(n) en zij die van de geadresseerde(n) toestemming kregen dit bericht te lezen.
Kennisneming door anderen is niet toegestaan.
De informatie in dit e-mailbericht (en bijlagen) kan vertrouwelijk van aard zijn en binnen het bereik van een geheimhoudingsplicht en/of een verschoningsrecht vallen.
Indien dit e-mailbericht niet voor u bestemd is, wordt u verzocht de afzender daarover onmiddellijk te informeren en het e-mailbericht (en bijlagen) te vernietigen.
Conform het beveiligingsbeleid van de Politie wordt e-mail van en naar de politie gecontroleerd op virussen, spam en phishing en moet deze e-mail voldoen aan de voor de overheid verplichte mailbeveiligingsstandaarden die zijn vastgesteld door het Forum Standaardisatie.
Mail die niet voldoet aan het beveiligingsbeleid kan worden geblokkeerd waardoor deze de geadresseerde niet bereikt. De geadresseerde wordt hiervan niet in kennis gesteld.

The information sent in this E-mail message (including any attachments) is exclusively intended for the individual(s) to whom it is addressed and for the individual(s) who has/have had permission from the recipient(s) to read this message.
Access by others is not permitted.

The information in this E-mail message (including any attachments) may be of a confidential nature and may form part of the duty of confidentiality and/or the right of non-disclosure.
If you have received this E-mail message in error, please notify the sender without delay and delete the E-mail message (including any attachments).
In conformity with the security policy of the Police, E-mails from and to the Police are checked for viruses, spam and phishing and this E-mail must meet the standards of the government-imposed E-mail security as set by the Standardization Forum.
Any E-mail failing to meet said security policy may be blocked as a result of which it will not reach the intended recipient. The recipient concerned will not be notified.
