Referentiekader Tapsysteem

Status: Definitief

Versie 1.0

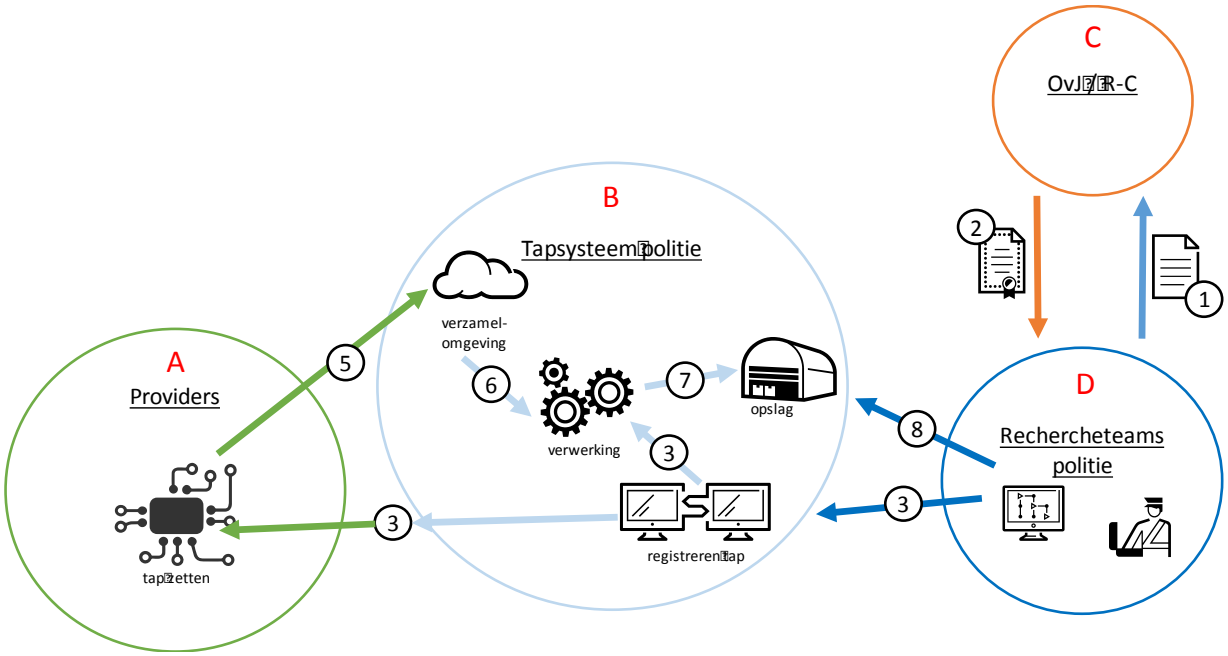
13 november 2017

Inhoudsopgave

Inleiding

Dit referentiekader vormt deel van de opdracht in het kader van het beschikbaarheidsonderzoek tapsysteem. Het referentiekader levert een nadere definitie van het begrip beschikbaarheid en doet een aantal suggesties hoe het tapsysteem beter gemonitord kan worden binnen het politiedomein. In lijn met het onderzoek staat de technische beschikbaarheid van het tapsysteem, zoals die in het onderzoeksrapport is gedefinieerd, hierin centraal. In dit referentiekader is niet gekeken naar de uitvoerbaarheid van deze monitoring binnen het huidige tapsysteem.
In de monitoring staat de beschikbaarheid van het tapsysteem centraal. Aanvullend worden enkele adviezen gegeven voor de bredere monitoring van het gehele tapproces. Bij aanvang van het onderzoek was beoogd dat het referentiekader zou dienen om de gevonden (on)beschikbaarheid van het tapsysteem weer te geven. Zoals aangegeven in Bijlage B van het onderzoeksrapport bij de beschrijving van spoor 2, is gebleken dat het huidige tapsysteem onvoldoende is ingericht om de benodigde informatie op te leveren. Om die reden is besloten dit referentiekader niet te gebruiken in het onderzoek naar het huidige tapsysteem en is het nu vooral bedoeld als mogelijke handreiking richting de toekomstige versie(s) van het tapsysteem.

Het tapproces kent een aantal stappen die van invloed kunnen zijn op de (technische) beschikbaarheid. Deze stappen staan hieronder schematisch weergegeven. De beschreven monitoring op de bredere beheersprocessen zijn afgeleiden van diverse standaarden, waaronder ITIL en ISO 20001.



Afbeelding 1 - Schematische weergave van het tapproces

Tapproces

De keten van het tapproces

Het proces van tappen wordt mogelijk door een complexe keten waarin het tapsysteem slechts een schakel is. In elk van de schakels kunnen verstoringen in principe leiden tot dataverlies. Het referentiekader richt zich op de technische infrastructuur van het tapsysteem dat onder de verantwoordelijkheid van de Nederlandse Politie valt. In het onderzoek wordt het tapproces ingedeeld in 4 fasen: zetten van de tap, ontvangst, verwerking en opslag. De in het schema weergegeven stappen van het tapproces raken deels het tapsysteem van de politie. Dit referentiekader beschrijft alleen de elementen die het tapsysteem van de politie en de technische beschikbaarheid raken.

Beschikbaarheid

Een systeem is ‘beschikbaar’ als het functioneert zoals is beoogd. Een systeem kan gedeeltelijk of volledig onbeschikbaar zijn. Dit kan al dan niet gepland gebeuren. In het onderzoek en dus ook in dit referentiekader, is uitgegaan van niet geplande verstoringen zoals gedefinieerd in het onderzoeksrapport (zie paragraaf 1.6, *Reikwijdte en beperkingen*).

Binnen de IT-dienstverlening wordt er vaak onderscheid gemaakt tussen geplande en ongeplande onbeschikbaarheid. Bij geplande onbeschikbaarheid is er sprake van onderhoud dat moet worden uitgevoerd aan systemen en infrastructuur, en dat vooraf wordt ingepland in zogenoemde onderhoudsvensters. Het is gebruikelijk om dit geplande onderhoud buiten de berekening van onbeschikbaarheid te houden. Dit betreft doorgaans een vast of een maximum aantal tijdsvensters waarbinnen het onderhoud moet worden uitgevoerd.

Niet geplande onbeschikbaarheid betreft storingen in de werking van het systeem, waardoor het systeem niet meer werkt zoals beoogd.

Daarnaast is het mogelijk dat één of enkele componenten in de keten onbeschikbaar zijn, maar door mitigerende maatregelen in de overige componenten er geen sprake is van dataverlies. De beoogde functionaliteit van de keten blijft in dat geval behouden.

De tapketen is te splitsen in vier delen:

- Het **zetten** van de tap;
- De **ontvangst** van de door de providers getapte data;
- De **verwerking** van de ontvangen data;
- De **opslag** van de ontvangen data.

Beschikbaarheid bij het zetten van de tap
Er zijn afspraken over de tijd die mag zitten tussen het uitvaardigen van een tapbevel en het daadwerkelijk effectueren van de tap. Om dit te kunnen faciliteren dient het aanvraagdeel aan een minimale beschikbaarheid te voldoen, die een afgeleide dient te zijn van die gemaakte afspraken.

Beschikbaarheid bij de ontvangst en verwerking

Gesprekken

Beschikbaarheid in dit deel betekent dat alle aangeboden gesprekken ook in het systeem binnenkomen en verwerkt worden. Theoretisch is het het eenvoudigst om te meten hoeveel gesprekken er worden aangeboden en dit te vergelijken met het aantal werkelijk ontvangen gesprekken. In de praktijk is dit niet mogelijk omdat de functionaliteit hiervoor op het huidige systeem niet bestaat en de legitimiteit ervoor ontbreekt.

Operationalisatie leidt tot de formule: alle aangeboden gesprekken, minus aantal verloren gesprekken tijdens/door gepland onderhoud, minus uiteindelijk opgeslagen gesprekken, is het aantal door storing/ongeplande onbeschikbaarheid verloren gegane gesprekken.[1]

Data

Naast ruwe data, zou het ook mogelijk moeten te zijn om te meten in hoeverre aangeboden data-producten (geordende data) ook hun weg vinden naar de opslag. Om dit te bepalen dient het mogelijk te zijn om te meten hoeveel data en dataproducten er worden aangeboden en hoeveel er daadwerkelijk worden opgeslagen. Metingen in dataproducten zijn zeer complex door de grote verscheidenheid in dataproducten en de snelle veranderingen daarin.

Beschikbaarheid bij de opslag

Beschikbaarheid in dit deel betekent in hoeverre de data die is binnengekomen en opgeslagen, beschikbaar blijft.

Aanvullende processen

De volgende processen vallen naar de letter van de opdracht buiten de scope van het onderzoek en dienen derhalve te worden gezien als aanvullende rapportagepunten.

Incidenten

Naast de bovengenoemde delen binnen de tapketen, zijn er meer algemene beheerprocessen die van wezenlijk invloed zijn op de beschikbaarheid van het tapsysteem. Zo heeft het incident managementproces ten doel om verstoringen zo snel mogelijk te herstellen. Door een goede registratie van dit proces kunnen storingen eerder worden opgemerkt, sneller worden verholpen en mogelijk worden voorkomen.

Overige processen

De overige processen zijn ook beheerprocessen, maar betreffen niet-incidentele zaken. Het doel van deze processen is het tapsysteem, inclusief de processen eromheen, goed in kaart te brengen, te beheersen en gestructureerd te verbeteren.
Het proces leverancierbeheer heeft ten doel de contractuele afspraken met leveranciers, inzichtelijk te hebben en onderdeel te laten zijn van periodieke reviews. Dit houdt in dat er met leveranciers heldere en meetbare afspraken moeten worden gemaakt en dat deze periodiek worden gemeten, gerapporteerd en besproken. Waar nodig wordt actie ondernomen.

[1] Overigens doet dit niet helemaal recht aan de complexiteit van het systeem omdat het ook kan gebeuren dat slechts een deel van een gesprek verloren gaat.

Tabel referentiekader

Nr.	Onderwerp	Doel	Benodigdheden	Rapportagepunten
1	**Beschikbaarheid**			
1.1	Beschikbaarheid bij het zetten van de taps	Het bepalen van de beschikbaarheid van het registratiesysteem om te bepalen in hoeverre tapbevelen onverwijld konden worden uitgevoerd.	1. Datum/tijd logging van de tapregistratie in het registratiesysteem 2. Logging van storingen van het tapregistratiesysteem	1. Aantal storingen in het tapregistratiesysteem 2. Duur van de storingen 3. Beschikbaarheid van het tapregistratiesysteem
1.2	Beschikbaarheid Ontvangst en Verwerking			
1.2.1	Beschikbaarheid bij ontvangst en verwerking	Het bepalen van de technische beschikbaarheid van ontvangst en verwerking om te bepalen in hoeverre tapgegevens zijn ontvangen en verwerkt.	1. Logging van storingen van het deel ontvangst en verwerking	1. Aantal storingen 2. Duur van de storingen 3. Beschikbaarheid van het deel ontvangst en verwerking
1.2.2	• Gesprekken	Het bepalen in hoeverre aangeboden gesprekken ook hun weg vinden naar de opslag.	1. Statistieken van de ontvangst server 2. Statistieken DBMS 3. Optioneel: Statistieken van alle tussenliggende componenten	1. Afwijking “Aantal gesprekken aangeboden op ontvangst server” – “Aantal opgeslagen in DBMS” = “Aantal verloren gesprekken” (– correctie voor gepland onderhoud)
1.2.3	• Data	Het bepalen in hoeverre aangeboden producten (ruwe dan wel geordende data) ook hun weg vinden naar de opslag.	1. Statistieken van de ontvangst server 2. Statistieken opslag	1. Afwijking “Statistieken ontvangst Server” – “Statistieken opslag” = “Verloren gegane data” (– correctie voor gepland onderhoud)
1.3	Beschikbaarheid opslag	Het bepalen in hoeverre opgeslagen producten (ruwe dan wel geordende data) bewaard blijven.	1. Opslag statistieken: ○ Aantal producten (data) opgeslagen ○ Aantal mutaties	1. Afwijking “Statistieken opslag aanwezig bij einde meetperiode” – “Statistieken opslag aanwezig bij begin meetperiode”

			○ Aantal producten (data) aanwezig	+/– “Statistieken mutaties” = “Verloren gegane data” (– correctie voor gepland onderhoud)

2	Incidenten			
2.1	Registratie	Ieder incident dat plaats vindt dient geregistreerd te worden. Het registreren dient op een dusdanig manier gedaan te worden, dat ieder incident geclassificeerd kan worden op urgentie en impact.	1. Inventarisatie benodigde velden 2. Kennis rondom invullen cq. afdwingen invullen van velden	1. Aantal correcte registraties
2.2	Classificatie	Ieder incident dient geclassificeerd te worden	1. Classificatieschema	1. Aantal per oorzaakcategorie 2. Duur per oorzaakcategorie
2.3	Impactbepaling	Ieder incident heeft een impact en dient als zodanig bepaald te worden	1. Tapgegevens (Type) 2. Log gegevens netwerk 3. Actuele provider storingen/werkzaamheden	1. Impact
2.4	Terugkoppeling	Alle communicatie rondom het incident moet beschikbaar zijn binnen een registratie. Het dient dus mogelijk te zijn om het incident vanuit de registratie volledig inzichtelijk te hebben.	1. Communicatiefaciliteiten vanuit incident registratiesysteem	1. Storingsrapportage

2.5	Problem	Indien er meerdere incidenten zijn die aan elkaar gerelateerd zijn, dienen deze incidenten aan elkaar gekoppeld te worden en door de problem manager opgepakt te worden.	1. Overzicht incidenten 2. Problem Manager	1. Totaal problems 2. Aantal opgelost 3. Aantal aangeduid als known problem 4. Aantal in onderzoek.
2.6	Lessons Learned	Bij het oplossen van een problem dient er gekeken te worden naar de zogenaamde Root Cause. Hierbij dient er lering getrokken te worden uit het ontstaan en het voorkomen van toekomstige verstoringen	1. Root Cause Analysis (RCA)	1. RCA + Oplossing
2.7	Opstellen van PV	Bij storingen met (potentieel) dataverlies dient er een PV opgesteld te worden	1. Aantal storingen met (potentieel) dataverlies 2. Format PV 3. Impact storing	1. Aantal PV's opgesteld t.b.v. een enkele taplijn. 2. Aantal PV's opgesteld t.b.v. meerdere taplijnen.

3	**Overige Processen**			
3.1	Capaciteitsbeheer	Om problemen ten gevolge van capaciteitstekort te voorkomen, dient er een vorm van beheer plaats te vinden.	1. Aantal taps 2. Historische gegevens over aantallen taps	1. Ontwikkelingen in aantal taps

3.2	Change Management	Om incidenten te voorkomen, dienen wijzigingen aan de systemen aangekondigd en geautoriseerd te worden door een daar toe bevoegde.	1. Status van de onderdelen van het tapsysteem 2. Problems	1. Aantal wijzigingen per onderdeel van het tapsysteem 2. Datum, tijd en aard van de wijzigingen
3.3	Configuratie Management	Het volledig in beeld hebben van alle configuratie items.	1. CMDB	1. Wijzigingen in de CMDB 2. Afwijkingen in periodieke controle
3.4	Release and Deployment management	Het gecontroleerd uitrollen van updates van zowel hardware als software mogelijk maken	1. CMDB	1. Aantal opgeloste problems
3.5	Leverancierbeheer	De leveranciers hebben een verantwoordelijkheid richting de politie. Middels deze norm dient het mogelijk te zijn om de leveranciers te houden aan deze afspraken en daar waar nodig bij te kunnen sturen.	1. SLA 2. Overzicht contractuele afspraken	1. SLR 2. Contract reviews