

Issue TC025 Aanvullende maatregelen voor verbeteren robuustheid centrale systemen

Status	Vastgesteld		
Versienummer	2.0	Versiedatum	11 december 2015
Documentnaam	TC025 Robuustheid_v2.0		

Behandeld door de Technische Commissie

Raakt aan	Kleinverbruik	Grootverbruik	Wholesale
Elektriciteit	X	X	
Gas	X	X	

Impact op keten	Ja/Nee
Codewijziging	Nee
Berichten	Nee
Ketenprocessen	Nee

Mogelijke impact marktrollen en EDSN	Ja/Nee
LV	Ja
PV	Ja
MV	Ja
RNB	Ja
LNB	Ja
EDSN	Ja

Vastgesteld door NEDU op	9 december 2015
	SR 2015
Invoering in markt per	(Update uiterlijk 1 april 2016)

Contact	
Technische Commissie	TC@edsn.nl

Management samenvatting

Dit issue betreft de aanvullende maatregelen voor het verder verbeteren van de robuustheid van de centrale systemen waardoor de kans op uitval van service-request's in de centrale systemen wordt geminimaliseerd.

Uitval van service-request's is tijdens het NMM project onderkend. Voor deze uitval zijn in het NMM project work-around's geïntroduceerd. Na invoering van het NMM zijn deze work-around's opgevolgd door een zgn. roll-back mechanisme. Dit roll-back mechanisme maakt de centrale systemen robuuster: in geval van een time-out op de middleware vindt er een roll-back plaats op de back-end.

De uitval van deze service-request's is door het roll-back mechanisme verholpen doordat de transactie wordt gestopt en er geen service-response wordt geretourneerd. Momenteel vindt er nog wel uitval van service-request's plaats door de session-time-out van de service dispatcher (een component tussen de webserver en de middleware). Tevens vindt er uitval van service-request's plaats door een tijdsvenster risico bij de controle van de time-out status door de back-end.

Er zijn aanvullende maatregelen uitgewerkt voor een structurele oplossing voor het minimaliseren van de uitval van service-request's in de centrale systemen:

- verhogen van de session-time-out van de service dispatcher naar 85 seconden¹. Indien na 85 seconden de service dispatcher geen service-response heeft ontvangen, wordt er een foutmelding (SOAP Fault), geïnitieerd door de service dispatcher, naar de aanvrager (de indiener van de service-request) geretourneerd;
- controle van back-end op de aanwezigheid van de corresponderende time-out notification. Indien aanwezig, wordt de service-request afgehandeld en wordt de service-response naar de aanvrager geretourneerd.

Het realiseren van deze aanvullende maatregelen heeft voor de aanvrager impact op:

1. de session-time-out instellingen van de web services bij de aanvrager, deze session-time-out moet verlengd worden tot minimaal 90 seconden;
2. het initiëren van de juiste "retry" actie door de aanvrager als gevolg van een ontvangen foutmelding (SOAP Fault) op de service-request. Door uitbreiding van het aantal SOAP Faults is het voor de aanvrager duidelijk welke "retry" actie moet worden uitgevoerd na ontvangst van de betreffende SOAP Fault.

¹ De max. session time voor het afhandelen van het service-request door de back-end wijzigt niet, deze blijft 45 seconden!

Situatieschets:

Uitval van service-request's is tijdens het NMM project onderkend. Voor deze uitval zijn in het NMM project work-around's geïntroduceerd. Na invoering van het NMM zijn deze work-around's opgevolgd door een robuuste oplossing met een zgn. roll-back mechanisme.: in geval van een time-out op de middleware vindt er een roll-back plaats op de back-end. Om een goede afhandeling bij de aanvrager te bewerkstelligen dient deze kennis te hebben van welke soort time-out tussen hem en de verwerkende back-end is opgetreden om de juiste vervolgacties te kunnen uitvoeren.

Daarnaast zijn een aantal ondersteunende maatregelen ingevoerd:

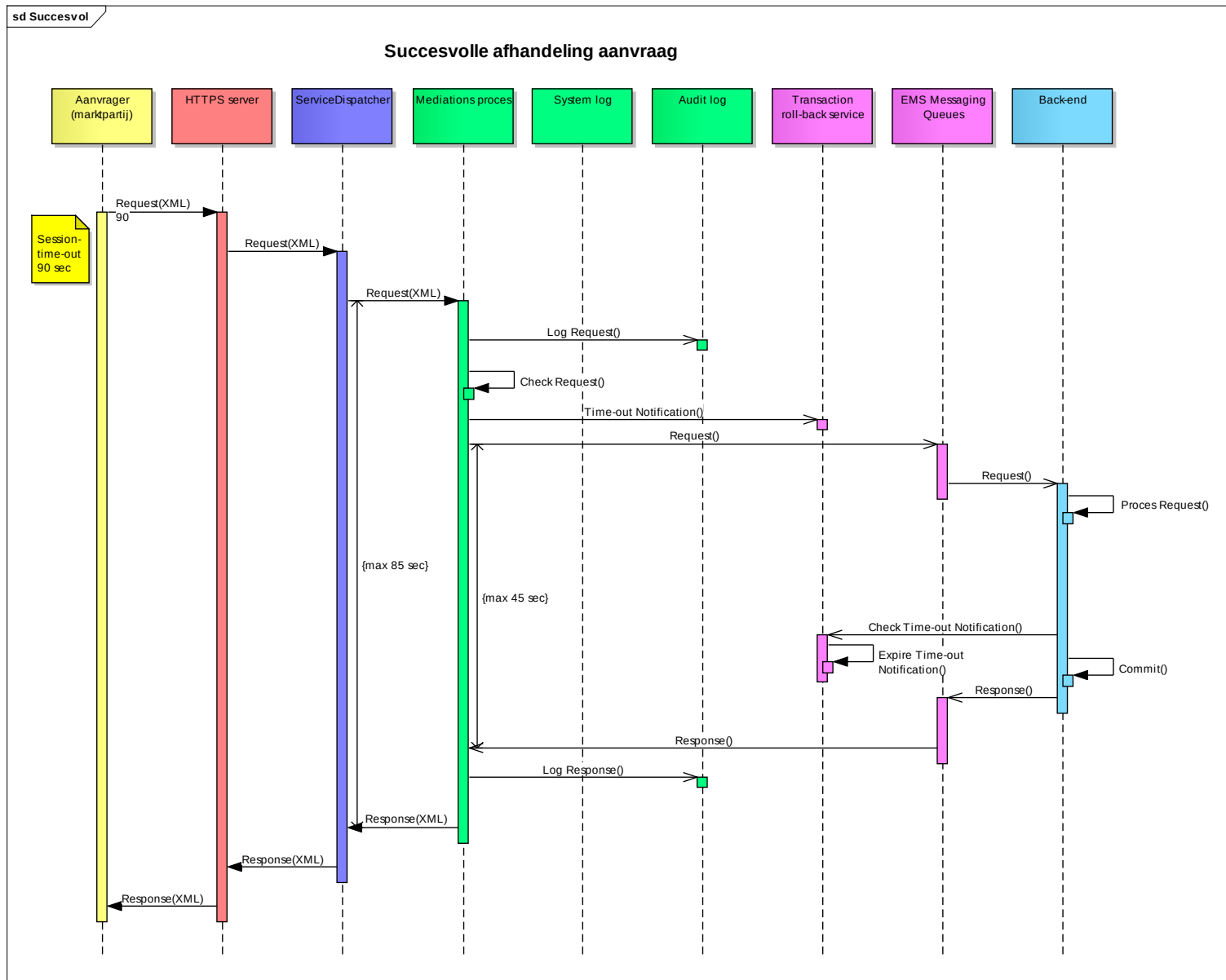
1. Session-time-out instelling op de service dispatcher (figuur 1)

De session-time-out van de service dispatcher dient te worden opgehoogd naar 85 seconden². Indien na 85 seconden de service dispatcher geen service-response heeft ontvangen, wordt er een SOAP Fault, geïnitieerd door de service dispatcher, naar de aanvrager geretourneerd. Elk service-request op de service dispatcher heeft bovendien een "expire time" van 40 seconden. Binnen die tijd moet het service-request door de middleware in behandeling zijn genomen. Indien dat niet het geval is, wordt de service-request gestopt en wordt er een SOAP Fault, geïnitieerd door de service dispatcher, naar de aanvrager geretourneerd.

2. Tijdsvenster risico controle time-out door de back-end en commit (figuur 1)

De middleware publiceert voor elke muterende service-request's een corresponderende Time-out Notification op de generieke Transaction roll-back service queue. Deze Time-out Notification heeft een configureerbare "expire time" van 40 seconden. De back-end controleert, voor de commit op de database, op de aanwezigheid van de corresponderende Time-out Notification op de Transaction roll-back service queue. Indien deze Time-out Notification beschikbaar is, zal de back-end de commit op de database uitvoeren en de service-response retourneren. De session-time-out op de middleware is 45 seconden zodat de service-response aan de aanvrager kan worden geretourneerd. Daarmee is de service-request vanuit technisch oogpunt succesvol afgehandeld. Mocht het onwaarschijnlijke geval zich voordoen dat de back-end meer tijd nodig heeft voor de commit (meer dan 5 seconden), dan wordt dit gesignaleerd op de Volledigheid Van Verwerking (VTV) rapportages en wordt het alsnog handmatig gecorrigeerd.

² De max. session time voor het afhandelen van het service-request door de back-end wijzigt niet, deze blijft 45 seconden!



Figuur 1: session-time-out instelling op de service dispatcher en tijdsvenster risico controle time-out door de back-end

TC025: Aanvullende maatregelen voor verbeteren robuustheid centrale systemen

Vraag:

Hoe kunnen we de servicegebruikers van de juiste informatie voorzien om na een time-out tussen hem en het verwerkende centrale systeem de juiste actie te kunnen laten ondernemen?

Overwegingen

Als een servicegebruiker een time out ervaart kan deze door meerdere oorzaken zijn veroorzaakt. Hierbij kan de backen nog niets hebben gedaan of de gevraagde actie al deels (en dus met roll-back tot niets) of al geheel hebben uitgevoerd. De verschillende situaties vergen een andere actie van de servicegebruiker om tot juist herstel te komen.

Op de centrale systemen is idempotentie ingevoerd: eenzelfde serviceaanvraag met dezelfde UUID geeft gegarandeerd hetzelfde resultaat (dus als dat al was aangemaakt dan staat dat al 'klaar', was er nog niks aangemaakt krijg je ook niks terug).

Oplossing:

Foutmeldingen (SOAP Fault, tabel 1)

De aanvrager ontvangt foutmeldingen indien een service-request niet kan worden afgehandeld. In veel gevallen ontvangt de aanvrager nu een SOAP Fault van het type 3. Deze SOAP Fault wordt in de huidige opzet voor verschillende soorten fouten gebruikt, waarbij ook verschillende "retry" acties vereist zijn. Daarmee is het voor de aanvrager niet duidelijk welke "retry" actie de aanvrager moet initiëren. Door de SOAP Faults in onderstaande tabel te gaan hanteren, is het voor de aanvrager duidelijk welke "retry" actie moet worden uitgevoerd na ontvangst van de betreffende SOAP Fault. De groen gemarkeerde SOAP Faults zijn nieuw of gewijzigd ten opzichte van de huidige implementatie.

Error Code	ErrorText	ErrorDetails	Opmerking	Advies
1	Database fout	<geen>	Een transactie kan niet worden doorgevoerd vanwege het feit dat zich een database probleem voordoet.	Opnieuw aanbieden met een nieuwe UUID ("retry" mechanisme incl. "time to wait"). Indien deze "retry" faalt, dan escaleren ³ .
2	XML Schema validatie fout	<details van XML Schema validatie fout>	De aangeboden XML bericht valideert niet tegen het bijbehorende XML Schema.	Aangeboden XML bericht is op syntax afgewezen en dient door de aanvrager gecontroleerd te worden. Na controle en correctie opnieuw aanbieden met een nieuwe UUID.
3	Systeem fout	<geen>	Het systeem is niet in staat om het bericht te verwerken.	Opnieuw aanbieden met een nieuwe UUID. Indien deze "retry" faalt, dan escaleren ³ .

³ Geadviseerd wordt om in dat geval contact op te nemen met EDSN Beheer.

TC025: Aanvullende maatregelen voor verbeteren robuustheid centrale systemen

Error Code	ErrorText	ErrorDetails	Opmerking	Advies
4	Security fout	<geen>	Een aangeboden transactie wordt om security redenen niet verwerkt.	Controle security door aanvrager. Na controle en correctie opnieuw aanbieden een nieuwe UUID.
5	Time-out	<geen>	Een aangeboden transactie wordt vanwege een time-out niet verwerkt.	Opnieuw aanbieden met een nieuwe UUID. Het feit dat de eerste aanvraag resulteerde in een time-out kan wijzen op een verminderde performance van de back-end. Het is een best practice om in het geval van een time-out melding, het bericht nog één of twee keer opnieuw aan te bieden (met nieuwe UUID). Indien de aanvraag alsnog niet succesvol kan worden afgehandeld, is de aanbeveling om een bepaalde periode te wachten alvorens het opnieuw aan te bieden (met nieuwe UUID). Indien deze "retry" faalt, dan escaleren ⁴ .
6	Einde sessie	<geen>	Het antwoord op de aangeboden transactie kan niet worden geretourneerd vanwege einde sessie service dispatcher.	Opnieuw aanbieden met het originele UUID. Aanvrager ontvangt de eventueel gelogde melding uit de audit log (door de ingestelde idempotentie). Indien deze "retry" faalt en opnieuw resulteert in een SOAP Fault 6, dan escaleren ⁴ .

Tabel 1: uitbreiding SOAP Faults

Merk op dat het effect van de foutmeldingen 1-4 op de serviceaanvrager betekent dat zijn verzoek niet is verwerkt (maar het verzoek (bericht) zelf is wel gelogd). Bij Fouten 2 en 4 dient de aanvrager eerst controle en mogelijk aanpassingen door te voeren alvorens de aanvraag opnieuw in te dienen. Bij fouten 1 en 3 was er een verstoring aan de verwerkende kant (meestal EDSN) en dient een nieuwe aanvraag met een nieuw UUID ingediend te worden. Het gebruik van hetzelfde UUID voor deze verzoeken zal (door het idempotentie mechanisme) leiden tot het terug melden van eerder teruggegeven foutcode en dus niets opleveren.

Impact:

Foutmeldingen (SOAP Fault)

Deze aanvullende maatregel heeft impact op de "retry" actie van de aanvrager als gevolg van een ontvangen foutmelding (SOAP Fault) op een service-request. Door uitbreiding van het aantal SOAP Faults (5 en 6 worden toegevoegd) is het voor de aanvrager duidelijk welke "retry" actie moet worden uitgevoerd na ontvangst van de betreffende SOAP Fault.

⁴ Geadviseerd wordt om in dat geval contact op te nemen met EDSN Beheer.

Risico's

Aan de realisatie van de aanvullende maatregelen om uitval van service-request's verder te minimaliseren zijn de volgende risico's verbonden:

1. aanvrager (de indiener van de service-request) hanteert een (te) korte session-time-out instelling waardoor de aanvrager de HTTPS connectie verbreekt voordat de service-response kan worden geretourneerd;
2. aanvrager implementeert geen afhandeling voor de additioneel toegevoegde SOAP Fault 5 en 6;
3. aanvrager hanteert geen differentiatie bij de afhandeling van de geretourneerde SOAP Fault waardoor:
 - a. een aanvrager niet de juiste "retry" actie kan initiëren, of;
 - b. eventuele gereedstaande service-responses niet opgehaald worden.

Mitigerende maatregelen

Realisatie van de aanvullende maatregelen om uitval van service-request's verder te minimaliseren brengt risico's met zich mee waarvoor mitigerende maatregelen voor moeten worden genomen:

1. faciliteren van SOAP Fault testen waardoor het initiëren van de juiste "retry" actie kan worden getest door de aanvrager (de indiener van de service-request);
2. uitvragen session-time-out instellingen van de web services bij de aanvragers.

Invoeringsstrategie:

Invoering van de oplossing in sectorrelease 2015.

Te vervallen issues:

Geen.

Versieoverzicht:

- 0.1 eerste aanzet door Gerrit Fokkema na bespreking in overleg AG CMF op 16 mei 2014;
- 0.2 na bespreking in de TC van 11 juli 2014 en voorbespreking in de IC-Klant en SPC beide van 10 juli 2014;
- 1.0 vastgesteld door de ALV op 23 juli 2014;
- 1.1 aanpassing na bevindingen in het tetstraject op 30 oktober;
- 1.2 aanpassing na schriftelijke instemmingsronde in de TC op 3 november 2015;
- 2.0 na vaststelling van de update in de ALV van 9 december 2015.