Redundant uitvoeren CIMS

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

Impactanalyse / Proof of Concept

Documentclassificatie: Kritiek / Strictly confidential.
Bij vragen of opmerkingen over dit document, kunt u contact opnemen met de Changemanager van Ordina.

© Copyright Ordina, 2021. Alle rechten voorbehouden

Inhoudsopgave

1 Algemene gegevens

Documentcontrole

1.1

OVERIG			
AUTEUR	5.1.2e		
NUMMER	n.v.t.		
REQUEST NUMBER RF	n.v.t.		
EIGENAAR ORDINA	5.1.2e		
WIJZIGINGSHISTORIE	Omschrijving	Versie	Datum
	Creatie	0.1	14-01-2021
	Aanvullingen	0.2	15-01-2021
	Definitief	1.0	15-01-2021
	Aanvulling	1.1	20-01-2021

Aanvraaggegevens

1.2

ALGEMEEN			
TITEL	Redundant uitvoeren van de productieomgeving van CIMS en Praeventis/Praemis		
CONFIGURATIE ITEM	☐ CBR Cliëntbeheer ☐ NHS Neonatale Hielprik Screening ☒ RVP Rijks Vaccinatie Programma ☐ VRD Voorraad ☐ VER Verrekening ☐ ALG Algemeen / diversen ☐ PSIE Prenatale Screening Infectieziekten Erytrocytenimmunisatie ☐ PMS Praemis ☒ CIMS Covid		
PRIORITEIT	Laag ☐	Middel ☒	Hoog ☐
EIGENAAR RIVM	5.1.2e 5.1.2e 5.1.2e 5.1.2e 5.1.2e		
DOCUMENTATIE	Omschrijving	Versie	Datum

2 Vraagstelling

Vanuit de klant (DVP Dienst Vaccinvoorziening en Preventieprogramma's) bestaat een vereiste om de voor de applicatie CIMS en Praeventis in gebruik zijnde servers regelmatig te voorzien van de benodigde (security-) updates. Helaas blijkt dit voor SSC Campus momenteel niet haalbaar binnen de daarvoor beschikbaar gestelde onderhoudsvensters. Daarom is het idee geopperd, om een redundante productieomgeving te bouwen, zodat de betrokken servers al dan niet tijdens kantooruren langer dan een uur offline kunnen ten behoeve van het aanbrengen van genoemde patches. Hierbij dient nadrukkelijk vermeld te worden, dat het hier dus niet gaat om een uitwijkomgeving ten behoeve van een disaster recovery scenario en evenmin om een high availibilty of scalibity solution. Verder is vooralsnog afgesproken dat de applicaties Praemis, BICIMS en Mantis buiten beschouwing blijven, omdat een langere downtime van deze applicaties in goed overleg met de eindgebruikers tot de mogelijkheden behoort.

In deze impactanalyse wordt een Proof of Concept (PoC) beschreven om bovenstaande te realiseren in de acceptatieomgeving van CIMS. Deze acceptatieomgeving wordt voldoende representatief geacht om de technische haalbaarheid van een redundante omgeving te bepalen en functioneel te testen. Op basis van de resultaten van deze PoC zal een definitief plan opgesteld dienen te worden, waarin de technische stappen in detail beschreven zijn en waarin tevens een redelijk nauwkeurig inschatting kan worden afgegeven met betrekking tot de te besteden uren en totale doorlooptijd van het realiseren van een dergelijke redundante omgeving.

Afgesproken is eveneens, dat er rekening gehouden dient te worden met het toepassen van Transparent Data Encryption (Oracle Advanced Security) in de nabije toekomst. Daarnaast wordt er in de PoC van uitgegaan dat er geen aanvullende Oracle licenties (d.w.z. andere dan momenteel in bezit) benodigd zijn; uiteraard zal het benodigde volume van de huidige licenties wel toenemen als gevolg van de in gebruikname van extra Oracle applicatie- en databaseservers. Aan de uitspraken m.b.t. benodigde licenties kunnen geen rechten ontleend worden. Het betreft een interpretatie van de wel/ niet benodigde licenties op basis van openbaar beschikbare informatie. De daadwerkelijke benodigde licenties zijn ook afhankelijk van de Oracle Master Agreement van VWS. Het RIVM is verantwoordelijk voor de aanschaf van de juiste licenties.

3.1

3 Oracle restricties

Oracle Fusion Middleware (WebLogic Server, Forms and Reports, SOA Suite)

Zoals aangegeven zal er op termijn mogelijk een verzoek komen om de databases (en back-ups daarvan) onderliggend aan de applicaties (BI)CIMS en Praeventis/Praemis te voorzien van encryptie. De daartoe geëigende technologie daarvoor is Oracle Transparent Data Encryption. Uit de documentatie van Oracle (https://docs.oracle.com/en/database/oracle/oracle-database/19/asoag/using-transparent-data-encryption-with-other-oracle-features.html) blijkt, dat deze technologie prima werkt in combinatie met Oracle Data Guard:

"You can use Oracle Data Encryption with other Oracle features, such as Oracle Data Guard"

In de volgende paragraaf zal besproken, waarom dit relevante informatie is.

Daarnaast willen we een oplossing implementeren, waarmee geen andersoortige Oracle licenties benodigd zijn dan momenteel reeds in bezit. De versie van Oracle Weblogic Server die is inbegrepen bij de licentie ten behoeve van Oracle Forms and Reports vinden we terug in de Oracle Licensing Information User Manual:

"A license to OFR includes a restricted-use license to Oracle WebLogic Server Basic or Oracle Containers for J2EE (OC4J). Use of Oracle WebLogic Server Basic or Oracle Containers for J2EE (OC4J) is restricted to running OFR applications only."

Uit de Oracle® Fusion Middleware Licensing Information User Manual blijkt eveneens dat de mogelijkheden tot gebruikmaking van de meer complexere ingebouwde technologieën licentie technisch beperkt zijn:

"A Standard Edition license provides unlimited access to most high availability features in Oracle WebLogic Server, with the exception of Cluster Support."

"Cluster Support is provided in all Oracle WebLogic Server Enterprise Edition and WebLogic Suite Edition licenses, and includes the following capabilities:

• Application failover (…)

• Cluster management and administration (…)

• Automatic and manual migration of a clustered server instance from one computer to another using Server Migration (…)

• Load balancing (…)"

Onderstaande paragraaf uit laatstgenoemd document geeft redelijk helder weer wat er volgens Oracle binnen de grenzen van de beschikbare licenties dan wel mogelijk is:

"High Availability Considerations for Oracle WebLogic Server Middle-Tier Instances
There are several ways that you can make Oracle WebLogic Server instances highly available. Each of these high availability models has specific licensing implications. These considerations are similar to the licensing considerations for the high availability features of the Oracle Database.

• Backup: In this type of recovery, Oracle WebLogic Server data/files of the primary server are stored on storage devices, such as tape media, and customers are not required to purchase additional licenses.

• Failover (also known as Active/Passive or Cold Failover Cluster): In this type of recovery, Oracle WebLogic Server nodes are configured in an Active/Passive Cluster; the first installed node acts as a primary node. If the primary node fails, one of the nodes in the cluster acts as the primary node. In this type of environment Oracle permits licensed Oracle WebLogic Server customers to run the Oracle WebLogic Server on an unlicensed spare computer for up to a total of ten separate days in any given calendar year. Any other use requires the environment to be fully licensed. Additionally, the same metric (that is, processor based, or named user based) must be used when licensing the Oracle WebLogic Server in a failover environment.

• Remote Mirroring: This method involves copying the Oracle WebLogic Server software to the secondary site and copying the changes in the primary Oracle WebLogic Server configuration and data to the secondary site. This can be accomplished through techniques such as storage based remote mirroring or host based mirroring. In the event of a failure at the primary site, the Oracle WebLogic Server on the secondary site is run using the remote storage. In this environment, Oracle WebLogic Server must be fully licensed at the primary site, and if it is ever installed and/or run at the secondary site, it must also be fully licensed there. Additionally, the same metric (that is, processor-based, or named user based) must be used to license both Oracle WebLogic Server domains."

3.2

In het oplossingsvoorstel (paragraaf 5) zal feitelijk de laatst genoemde optie (remote mirroring) in aangepaste vorm worden uitgewerkt.

Oracle Database

Uit de Oracle Database Licensing Information User Manual blijkt dat het opbouwen en actief bijwerken van een stand-by database met behulp van Oracle Data Guard mag op basis van de reeds in bezit zijnde licentie voor Oracle Database Enterprise Edition, zolang de stand-by database niet tegelijk met de primaire database geopend is (Oracle Active Data Guard); dit betekent dat er op elk moment in tijd slechts een van beide databases daadwerkelijk raadpleegbaar is.

4 Betrokken configuratie-items

In onderstaande tabel zijn alle momenteel aanwezige en bij de PoC betrokken componenten in de acceptatieomgeving van CIMS weergegeven. Hierbij moet geconstateerd worden dat de Oracle SOA Suite momenteel nog niet in gebruik is genomen en dat de daaraan onderliggende databaseschema's zich momenteel bevinden in pluggable database aofr op server rivm-cvdb-l01a; indien besloten wordt om binnen CIMS de SOA Suite daadwerkelijk in gebruik te gaan nemen, dan zullen deze schema's verhuisd moeten worden naar een aparte database.

Omgeving	Servernaam	IP -adres	OS	Omschrijving
ACCEPTATIE	rivm-cvweb-l01a	131.224.242.186	RHEL 7.6	Apache httpd
ACCEPTATIE	rivm-cvweb-l02a	131.224.242.187	RHEL 7.6	Apache httpd (intern)
ACCEPTATIE	rivm-cvapp-l01a	131.224.242.184	RHEL 7.6	Oracle Forms and Reports
ACCEPTATIE	rivm-cvapp-l02a	131.224.242.185	RHEL 7.6	Oracle WebLogic Server en ORDS
ACCEPTATIE	rivm-cvapp-l03a	131.224.242.254	RHEL 7.6	Oracle SOA Suite
ACCEPTATIE	rivm-cvdb-l01a	131.224.232.201	RHEL 7.6	Oracle RDBMS (ACIMS+ABICIMS+AOFR)

5 Oplossingsvoorstel

Met bovenstaande overwegingen in het achterhoofd, komen we tot onderstaand voorstel voor een PoC in de acceptatieomgeving van CIMS. De aanname is gedaan, dat in principe alle servers op hetzelfde moment uitgeweken zullen gaan worden.

Stappenplan:

- Klonen van alle hierboven genoemde servers binnen VMware; de nieuwe servers zullen een nieuwe nader te bepalen naam krijgen en een tijdelijk IP-adres.
- De aanwezige rules in iptables worden aangepast naar de nieuwe situatie.
- Eventuele externe connecties zullen in kaart gebracht moeten worden en daar waar nodig zullen aanvullende routes in het netwerk worden aangebracht (API gateway, VZVZ/LSP).
- Alle applicaties op de gekloonde servers worden uitgeschakeld.
- De gekloonde servers krijgen een nieuw definitief IP-adres toegekend en worden als zodanig bekend gemaakt in de interne DNS.
- De kloons van de twee webservers zullen synchroon gehouden worden met behulp van een dagelijkse cronjob, welke de inhoud van onderstaande directories kopieert (rsync) en met het commando sed de benodigde naamswijzigingen doorvoert:
    - /etc/httpd/sites-available
    - /etc/httpd/sites-enabled
    - /etc/httpd/tls

- Voor de kloons van alle Oracle Fusion Middleware applicaties geldt, dat deze gecontroleerd moeten worden op incorrecte hostnames en IP-adressen en deze zullen moeten worden aangepast; dit geldt ook voor connecties naar de relevante Oracle databases.
- Voor de kloons van alle Oracle Fusion Middleware applicaties geldt, dat hiervoor nieuwe keystores aangemaakt moeten worden met daarin certificaten met de correcte servernamen.
- Server rivm-cvapp-l01a: de voor Oracle Forms applicatie specifieke configuratie, de forms en reports zelf en de gebruikte compile-scripting worden dagelijks met behulp van een cronjob synchroon gehouden (rsync).
- Server rivm-cvapp-l02a: de kloon zal synchroon gehouden worden met behulp van een dagelijkse cronjob, welke de inhoud van onderstaande directories kopieert (rsync):
    - /ora0/acc/httpd (met uitzondering van logbestanden)
    - /ora0/acc/user_projects/domains/rvm_acceptatie/lib/
    - /ora0/acc/user_projects/domains/rvm_acceptatie/servers/AdminServer/upload
    - Mogelijk de gehele directory /ora0/acc/user_projects/domains/
- Server rivm-cvapp-l03a: de kloon zal synchroon gehouden worden met behulp van een dagelijkse cronjob, welke de inhoud van directory /ora0/acc/user_projects/domains/ kopieert (rsync).
- Server rivm-cvdb-l01a: van databases cdb1900a/acims en cdb1900c/aofr wordt een duplicate gemaakt met behulp van RMAN en wordt Oracle Data Guard en Data Guard Broker ingericht.

Opmerkingen:

- Toekomstige wijzigingen in de configuratie van de Oracle Fusion Middleware domains zullen (vooralsnog) niet automatisch worden verwerkt in de stand-by omgevingen en dienen derhalve op beide omgevingen te worden aangebracht.
- Voor de door Oracle uitgebrachte patches geldt eveneens, dat deze in zowel de primaire- als stand-by omgevingen zullen moeten worden toegepast.

6 Testplan

Stappenplan:

- Alle applicaties op de primaire servers (zoals aangegeven in de tabel) worden uitgeschakeld; de databases voorzien van een stand-by met behulp van Oracle Data Guard krijgen een switchover (geen failover!).
- Er vindt een aanpassing plaats in de interne DNS voor wat betreft de lokale in gebruik zijnde applicatie-URL's (Oracle Forms, Apex); eventueel zou er getest kunnen worden door een aanpassing in het lokale hosts-bestand op de computer/desktop van de betrokken tester.
- Alle applicaties op de stand-by servers worden opgestart en beoordeeld op eventuele technische foutmeldingen.
- Aanwezige cronjobs ten behoeve van synchronisatie van de stand-by omgevingen worden tijdelijk uitgeschakeld.

- Alle applicaties worden door nader aan te wijzen functioneel applicatiebeheerders grondig getest; alle eventuele fouten (die niet voorkomen in de primaire omgeving) worden vastgelegd en voor zover mogelijk gecorrigeerd en hertest.
- De enkel in de productieomgeving bestaande (S)FTP-server valt buiten het bestek van voorliggend document, maar functionaliteit in relatie tot deze server zal uiteindelijk wel in scope gebracht en getest moeten worden.
- Na uitvoering van voorgaande stappen zal er worden teruggeweken naar de primaire servers in omgekeerde volgorde en volgt er een globale functionele test.

Op basis van de eventuele bevindingen en wenselijkheid zal bepaald moeten worden hoe om te gaan met nieuwe releases ten tijde van een uitwijkprocedure; moet er tijdelijk een freeze worden ingesteld, wordt er direct na het voltooien van het patchproces teruggeweken?
Eventueel zal dan ook de haalbaarheid van een bidirectionele synchronisatie moeten worden bepaald en zal er moeten worden nagedacht over inrichting van back-upprocessen van de stand-by servers en applicaties/databases.

7 Urenschatting

Het aantal te besteden uren zal naar verwachting 80 uur bedragen. Hierbij is geen rekening gehouden met eventuele wachttijd, tijd voor extra overleg(gen) en extra tijd voortvloeiend uit geconstateerde bevindingen. Aangezien deze PoC een multidisciplinaire inzet vereist, zal de geschatte totale doorlooptijd langer zijn.