Anàlisi i implementació d'un sistema de recuperació de desastres d'una infraestructura de sistemes de dades

Juan Luis Guillen Garcia

Enginyeria Tècnica de Telecomunicacions, especialitat Sistemes Electrònics

Escola Politècnica Superior d'Enginyeria de Vilanova i la Geltrú

Universitat Politècnica de Catalunya

Resum

Aquest projecte s'inicia amb la necessitat d'una empresa, d' implementar un sistema de recuperació dels sistemes de dades (DRP). Assegurant que davant una incidència amb implicació de caiguda dels seus sistemes, es disposa d'un pla de recuperació del negoci mitjançant el desplegament d'un entorn temporal amb la disponibilitat dels principals serveis de producció.

L'objectiu del propòsit, es l'anàlisi de dues opcions per la realització de l'entorn: implantació del DRP a les infraestructures de la pròpia empresa, i implantació del nou entorn a una solució al núvol. I la seva posterior implementació.

1. Introducció

L'aturada dels serveis d'una empresa, originada per la degradació dels seus sistemes de dades, suposa pèrdues econòmiques degudes a l'aturada dels serveis oferts als seus clients.

Un sistema de recuperació de desastres, assegura una reducció del temps de la inoperativitat del negoci. Activant un entorn DRP, els departaments IT no necessiten preparar noves infraestructures i realitzar restauracions dels backups de dades. I la seva ubicació a una localització geogràfica diferent no es veu influenciada per incidents originats a les infraestructures principals. Segons les estadístiques proporcionades per la U.S. Small Business Administration [1], el 40% dels negocis que experimenten un desastre als seus sistemes es veuen obligats a tancar i un 25% tanquen durant els següent any.

A l'actualitat, els sistemes de computació al núvol, ofereixen solucions per replicar els sistemes de manera externa a les instal·lacions de l'empresa.

2. Objectius

L'objectiu principal que es desitja assolir amb la realització del projecte és la implementació d'un sistema de recuperació de desastres d'una infraestructura de dades. De forma que l'empresa on es realitza disposi d'un entorn replicat i independent que permeti la continuïtat del negoci en cas d'incident greu als sistemes de producció. Assegurant que: la producció, venta i accés als continguts, continuï estant disponibles pels clients i els empleats en un curt espai de temps.

3. Àmbit de l'aplicació

El projecte es realitzarà a l'Agència Catalana de Notícies en endavant ACN. Aquesta és una de les primeres agències de notícies digitals creades a Europa i opera a Catalunya des de l'any 1999. És pionera en l'ús de les tecnologies de la informació, el teletreball i l'organització descentralitzada aplicats a un entorn periodístic virtual.

L'ACN utilitza una tecnologia pròpia, que permet oferir un servei extremadament competitiu als abonats. La producció informativa es presenta en formats de text, àudio, fotografies i vídeo digitals incorporables tant a mitjans tradicionals com a plataformes de continguts lligades a l'actualitat, com ara Internet, telefonia mòbil, tauletes digitals i televisions publiques i estatals.

4. Estat de l'art

A l'actualitat els plans de recuperació davant desastres s'han introduït progressivament a als procediments de negoci i departaments tecnològics de les empreses. Implantar un DRP es una solució que pot garantir la continuïtat de les operacions d'una organització. Els sistemes tradicionals de backups o equips redundants operen de forma local, i no permeten disposar d'un nou entorn (infraestructura) a una localització diferent i en un temps reduït.

Pel disseny del DRP s'analitzaran dos tipus de solucions: les realitzades utilitzant les infraestructures pròpies de l'empresa o contractació del servei a proveïdors de serveis de sistemes al núvol.

Dintre de la darrera opció apareixen un ventall de diferents corporacions. Entre les més importants podem destacar Amazon (AWS), Microsoft Azure o Google. Per la realització del projecte s'ha decidit estudiar la opció d'Amazon. La pressa de decisió es basa en l'experiència de l'empresa, en ser de les primeres en oferir aquest tipus de servei i tenir la major quota de mercat[1], els preus i l'experiència de l'equip de tècnics que realitzaran el projecte en la utilització de la plataforma AWS que utilitza.

5. Disseny de la solució

Per realitzar el disseny del pla es realitzarà l'estudi de dues solucions, a fi d'implementar aquella que ofereixi un millor balanç de rendiment i despesa econòmica.

Mitjançant la pressa de requeriments del sistema es podran acotar els serveis i infraestructures necessàries per poder oferir el servei amb els mínims pactats amb la direcció de l'empresa.

Aquests son els serveis que hauran d'estar disponibles:

- El portal web de l'agència i les aplicacions que el nodreixen de contingut
- Els sistemes d'enviament de continguts automàtics als clients (aplicació gen)
- Les dades multimèdia (text, àudios, fotos i vídeos) continguts als sistemes d'emmagatzematge
- La connexió a internet dels usuaris de la seu
- El servei de ERP utilitzat pels departaments de finances i administració

S'estableixen els següents temps de resposta del pla:

- Marge de decisió per activar l'entorn de recuperació de 30 minuts
- Marge d'activació i funcionament de l'entorn de 2 hores

La figura 1, mostra mitjançant una gràfica el temps transcorregut i la disponibilitat dels serveis. Delimitant per marges les diferents etapes per les quals s'avança després de l'inici d'un incident que causa l'activació del DRP. S'observa que posteriorment a la caiguda, comença el procés d'activació del DRP i que durant el temps necessari per recuperar els sistemes, la infraestructura es veu ressentida al no disposar de totes les seves funcionalitats. La tornada a producció retorna l'estat de màxima disponibilitat.

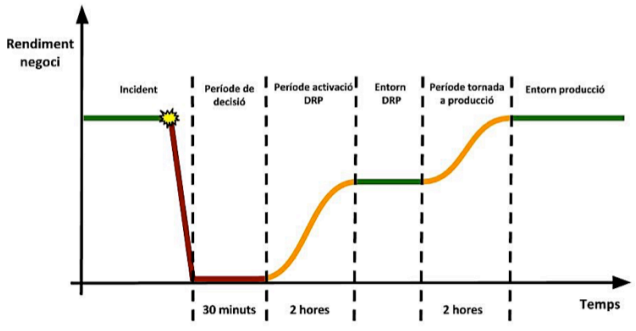

Fig. 1. *Gràfica marges activació DRP*

La solució ha de garantir el rendiment necessari per donar servei a un mínim del 70% de les pàgines vistes a la web (20.000 pàgines) i el cost anual de la solució no pot ser superior als 3.000€ anuals, sense comptabilitzar els cost dels recursos.

L'entorn a replicar es troba ubicat a un CPD d'Hospitalet, i l'empresa disposa d'un segon CPD situat a Barcelona amb hardware disponible. Aquest detall permet estudiar la opció de replicar els sistemes que necessita el DRP al poder separar geogràficament els dos entorns. Es realitzarà un estudi dels recursos utilitzats pels sistemes de producció que cal replicar. Aquestes dades ens mostraran si l'empresa pot absorbir la nova estructura i la despesa que implica implementar la solució al núvol.

Realitzant l'anàlisi dels sistemes de producció, s'arriba a la conclusió de que els requisits mínims, més importants, necessaris per realitzar el projecte assegurant l'acompliment dels objectius son:

Requisit	**Total**
CPUS	17
Memòria RAM	16Gb
Espai en disc servers	522Gb
Emmagatzematge fitxers	10 Tb
Upload/Dowload línia internet (Mb/s)	5,31 / 1,97
Pàgines diàries vistes al portal	20.000

Taula. 1. *Requeriments principals del nou entorn DRP*

Les diferents xarxes configurades als actualment son:

- 10.125.53.0/24: Servidors d'aplicacions i cabina de dades
- 10.125.55.0/24: Destinat a les bases de dades
- 172.22.72.0/24: Xarxa d'usuaris i servidors del cpd de Barcelona

Amb les dades extretes es confirma que el nou entorn es pot ser implementat al CPD secundari de Barcelona. On es disposa dels suficients recursos de hardware als servidors virtuals per instal·lar les màquines necessàries. Es compleixen els requeriments de disc (espai pels fitxers i velocitat d'escriptura i lectura similar a la cabina de producció). El hardware que s'utilitzarà per la virtualització es un servidor HP Proliant DL380p Gen8 i la cabina de dades de l'entorn del DRP es una Iomega EMC px12-400r de 28Tb d'espai en disc. Per la línia de dades de connexió a internet es disposa de l'opció de contractar una fibra de la companyia Movistar[3] . Que tot i oferir velocitats inferiors de pujada (100Mb/10Mb) a la principal (40Mb/40Mb), assegura un rendiment similar durant la major part de la jornada laboral. Aquest era el tipus de línia amb major capacitat per contractar. La despesa associada a aquesta solució de reaprofitament d'infraestructures, està centrada a aquesta línia de dades. Suposant un cost anual de 591,16€, durant el primer any, disminuint a 434,16€ els anys posteriors, al utilitzar sistemes ja adquirits amb anterioritat. Adoptar aquesta opció ajuda a l'empresa a rendibilitzar el hardware del que es propietària, durant el seu període d'amortització.

Amb les dades recopilades es procedeix a realitzar un estudi dels serveis equivalents a contractar a Amazon i el seu cost, per poder implementar la solució al núvol. Per l'anàlisi s'ha utilitzat l'eina de simulació facilitada pel mateix proveïdor. S'ha contemplat la implementació d'un total de set servidors (servei EC2) de diferents característiques segons el necessitat de les aplicacions instal·lades: 3 servidors amb alta capacitat de CPU, memòria RAM i disc ssd, 1 servidor de potència mitja i 3 servidors més reduïts en quant a recursos. Un sistema d'emmagatzematge (Servei S3) amb

capacitat suficient per contenir els continguts multimèdia actuals i estimats durant un any. Un servei de base de dades Oracle, un balancejador de càrrega i DNS (Route 53). Els càlculs es reflecteixen a la Taula 2, on l'import anual final de la solució ascendeix als 14.983€. La despesa es concentra principalment en la utilització de base de dades Oracle amb llicència i el conjunt de servidors on s'haurien d'instal·lar la resta d'aplicacions de l'ACN. La conversió utilitzada per determinar el valor final es 1$dolar=0,8€euros.

Nom del servei	**Tipus servei**	**Import**
EC2	Servidors	$182,65
RDS	Base dades	$1.041,61
S3	Emmagatzematge	$308,00
E.Load Balancing	Balancejador	$26,32
Route 53	DNS	$2,20
Total dòlars (mes)		**$1560,78**

Taula. 2. *Valoració econòmica entorn DRP a Amazon*

Per realitzar el disseny del nou entorn es realitzarà la creació de dues noves subxarxes a la seu de Barcelona, on es replicarà l'estructura i ips del cpd d'Hospitalet, amb la finalitat d'aconseguir un entorn igual que el de producció. Que pugui realitzar la sortida per la nova connexió de dades contractada i es mantingui aïllada dels equips de producció per evitar duplicitats i errors entre entorns. L'arquitectura del nou entorn queda representada pel següent esquema de la Figura 2, on es poden diferenciar les diferents xarxes que s'han d'implementar. A l'esquema es diferencien els servidors que queden aïllats a la xarxa 53 i 55, i aquells que han de comunicar-se amb totes dues. Servidors virtuals, que per les aplicacions que contenen, necessiten comunicar-se amb les bases de dades oracle. S'ha decidit utilitzar una màquina virtual amb el sistema operatiu PFSense que tindrà la funció de realitzar l'enrutament entre les diferents xarxes facilitant la replicació dels entorns i permetent l'accés des del rang 172.22.72.0/24 per administrar el nou entorn i poder accedir als servidors.

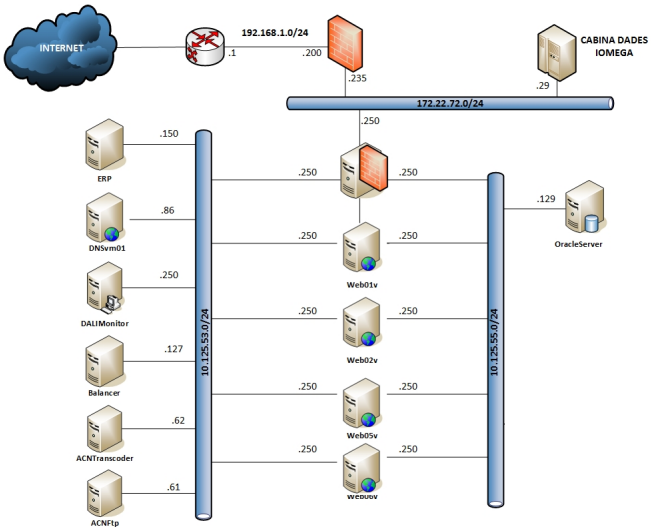

Figura 2. *Arquitectura de xarxa del nou entorn*

Per realitzar la replicació dels servidors virtuals entre entorns, es decideix utilitzar els software Veeam Backup[4], que facilita la copia i restauració de màquines. I ofereix la opció de replicar servidors. Aquesta funcionalitat s'utilitzarà per aconseguir que la base de dades estigui actualitzada en cas d'activació del DRP, al ser la màquina que experimenta més canvis constants, juntament amb la cabina de fitxers. Així s'aconsegueix clonar els servidors necessaris a l'inici del projecte, i optar a la seva actualització en cas de modificacions posteriors. Per implementar la replicació de les dades multimèdia s'ha realitzar una sèrie d'scripts que utilitzen la comanda unix "rsync"[5] amb la sintaxi: "rsync –avu \DirectoriOrigen \DirectoriDestinació", que s'executarà segons una tasca programada a un servidor Ubuntu Server 14.04. A la Figura 3 es mostra un esquema de la sincronització entre els dos entorns. On es diferencia la replicació de màquines virtuals i fitxers de la cabina.

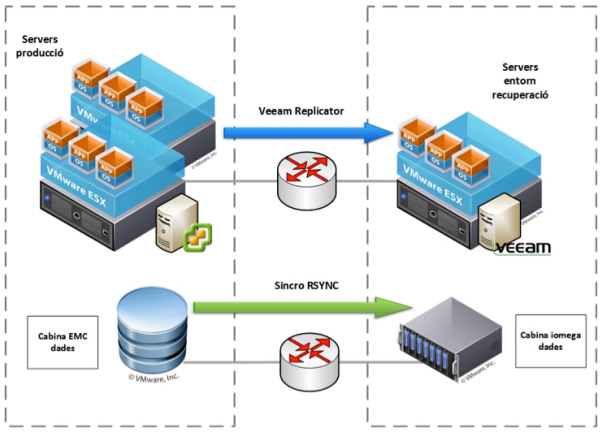

Fig. 3. *Esquema simplificat de la replicació*

Durant les proves de laboratori realitzes per comprovar la velocitat de replicació de les dades de cabina, es va detectar que el temps necessari per traspassar les dades incrementals excedien els requerits pel projecte, arribant a valors que superaven les 3hores. Originat per la necessitat d'analitzar els directoris de tota la cabina i analitzar els canvis realitzats respecte el volum del DRP. Per donar solució a aquest risc es sol·licita al departament de desenvolupament, una aplicació.

Mitjançant la qual es realitzes diverses peticions a la base de dades amb la finalitat d'extreure directament el llistat de fitxers modificats entre repliques per reduir el temps que necessita la comanda rsync per escanejar les dues cabines i rebre els diferents directoris a sincronitzar. Amb aquesta solució es redueix el temps d'execució de l'operació situant-lo als vint minuts. L'aplicació va ser desenvolupada en llenguatge Java i es programa la seva crida perquè es realitzi de manera periòdica cada quatre hores. La figura 4 mostra el circuit realitzat per aquest procés, i com s'utilitza la base de dades per actualitzar els fitxers multimèdia a la cabina Iomega.

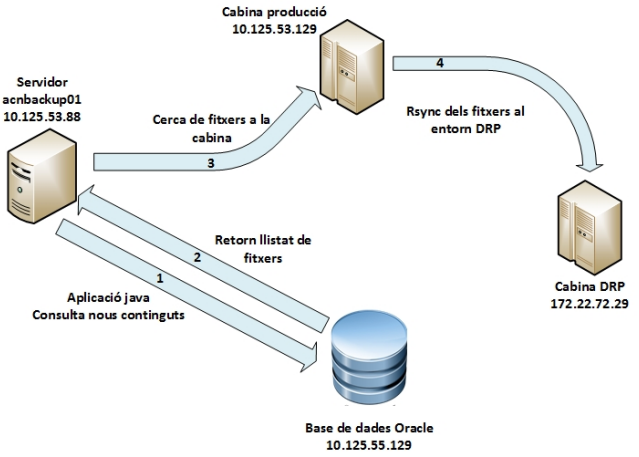

Figura 4. *Sincronització de les dades entre cabines*

L'aplicació disposa de tres mètodes diferents que ofereixen diferents opcions per sincronitzar les dades i que seran cridats pels diferents scripts de sincronització, aquests mètodes realitzats son:

- Mètode pathDaysDRP: La funció d'aquest mètode es generar un fitxer on s'escriurà la ruta de cada arxiu generat durant el període de temps, dues dates, que s'introdueix també com a paràmetre a la crida. La comanda utilitzada es: curl --data "numberDays=1&mmediaOrData=0/1" http://10.125.53.88:8080/numberDaysDRP
- Mètode pathNumberDaysDRP: El marge de dies on es realitzarà l'anàlisi s'introdueix mitjançant el nombre dels darrers N dies. Aquest es el model de la comanda : curl --data "path=/RutaOnDessar/fitxer.txt &numberDays=1&mmediaOrData=0/1" http://10.125.53.88:8080/pathNumberDaysDRP
- Mètode numberDaysDRP: Permet introduir el path per defecte on es desarà el fitxer resultant. Per fer-ho es defineix al arxiu proToDRP.properties del servei, la ruta genèrica que sempre utilitzarà quan es realitzi aquesta crida. Al igual que els altres mètodes introdueix el contingut al final del fitxer en cas de d'aquest existeixi i retorna el path on s'ha desat.

El procés de retorn als equips de producció després de la seva recuperació es centra en la restauració dels diferents servidors utilitzant el software Veeam Backup i l'script nfsRestauraDRP.sh [Nº dies]. Aquest script utilitza el mètode pathNumberDaysDRP realitzat per l'equip de desenvolupament, el qual proporcionarà el llistat d'arxius que necessita la comanda rsync per deixar les dades sincronitzades entre entorns.

El sistema de resolució de noms està contingut als servidors de producció i en cas d'incident l'accés als portals s'impossibilita. Per aquest motiu es decideix canviar la gestió dels DNS i externalitzar-los. Després d'haver realitzat estudi de la plataforma Amazon i confirmar que disposa de SLAS molt restrictius i un baix cost pel servei Route 53, es decideix moure el servei a les seves infraestructures. Afegint totes les zones dependents de l'Agència Catalana de Notícies i assegurar que en cas d'incident a l'entorn de producció, es podrà realitzar un canvi de les ips on es redireccionen les peticions i no deixarà d'oferir el servei al no trobar-se dintre de la xarxa de l'empresa.

La totalitat del procés d'activació i desactivació del DRP es troba detallada al projecte i serveix de guia perquè els tècnics responsables disposin de la documentació necessària per dur a terme l'operació en cas de necessitat.

6. Resultats aconseguits

Després de d'implementar el nou entorn i finalitzar les configuracions exposades al capítol 5 de disseny es decideix realitzar una prova simulant una caiguda real dels equips de producció.

L'inici de l'actuació es va programar per les 23:59h del dia 11 de febrer. Segons els càlculs inicials l'entorn del DRP hauria d'estar completament actiu a les 01:45h del 12 de febrer i per realitzar l'actuació es va formar un equip de dos tècnics. El sistema de DRP es va poder activar sense incidents, després de 1 hora i 30 minuts. Complint així els requeriments del projecte. Al finalitzar el procediment, tots els checks del sistema de monitorització eren correctes, i la bateria de proves realitzada a totes les aplicacions, accessos i continguts de la cabina del DRP van ser satisfactòries.

El rendiment dels servidors durant el dia de l'actuació es va trobar dintre dels marges esperats durant el disseny, els valors de CPU i RAM es van mantenir dintre la franja dels 50% i 70%, tal i com mostra la figura 5. Detectant-se pics d'utilització durant els períodes compresos entre les 10:00h i 13:30h i posteriorment entre les 18:00h i les 22:00h. Les màquines virtuals dedicades als servidors frontals i a la transcodificació de vídeos van suposar la major part de la utilització dels recursos del ESX.

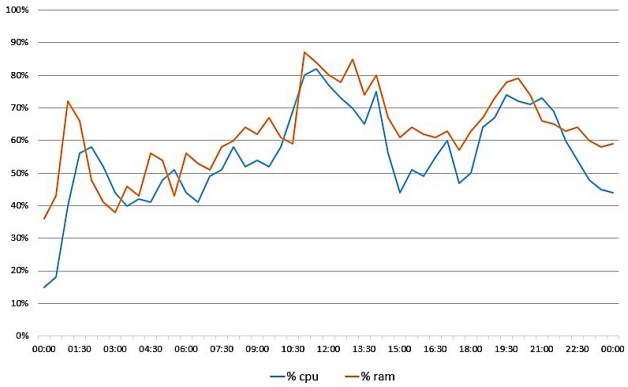

Figura 5. *Rendiment CPU i RAM del servidor durant actuació*

L'anàlisi de l'ample de banda utilitzat pel DRP, mitjançant la fibra de Movistar instal·lada, reflexa que durant tot el període al qual es va utilitzar l'entorn de recuperació, l'ample va ser consumit constantment a les franges de major activitat. L'ús total de l'ample es va reflectir en petites lentituds als enviaments automàtics que es realitzen a l'aplicació gen, però en cap moment va haver incidents relacionats amb la xarxa.

Consultant les estadístiques de l'accés al portal es detecta que la mitja de carrega de la web es trobava dintre dels valors habituals. El temps mig de càrrega del portal va ser de 1,973ms.

Durant l'actuació on es va activar el DRP del dia 12 de Febrer es va detectar un incident al rendiment del portal web de l'ACN, el qual va deixar de respondre o registrava

valors molt elevats per la seva càrrega. Aquest incident va ser degut un pic de visites i sessions al portal concentrades a les 12:00h, moment al qual es va publicar una sèrie de noticies que cobrien l'actualitat informativa que s'estava desenvolupant a la localitat d'Igualada i relacionada amb la fuita de gasos irritants a una empresa química propera a la localitat. Tal i com mostra la figura 6, les sessions establertes al balancejador pateixen un augment del 700% respecte els valors habituals pujada a la mateixa hora, situant-se entorn a les 600 sessions. A la gràfica es compara les registrades el dia 12 de febrer (DRP) i el dia 11 de febrer. Aquesta pujada de sessions concentrades en un curt espai de temps va originar errors al servidor de balanceig de la pàgina web. Es detecta que el balancejador es queda saturat i que el servei d'Apache sota el qual s'executa deixa de respondre. Originant que els tècnics necessitin reiniciar manualment l'aplicació dues vegades per recuperar el servei web als clients. Es recupera completament el servei a les 12:20h.

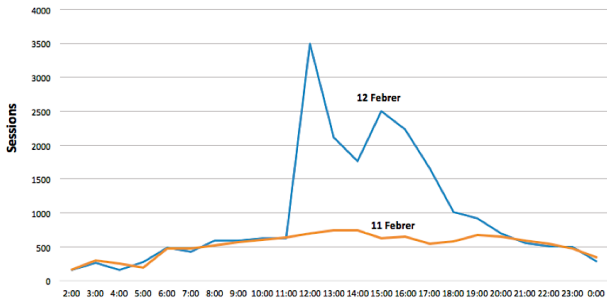

Fig6. *Nº sessions actives al balancejador*

Analitzant les estadístiques de la plataforma Google Analytics del portal es detecta períodes amb 5.000 pàgines vistes de manera puntual, la mitjana de pics anual era de 2200.

Per realitzar el càlcul del cost total del projecte, s'ha analitzat el cost aproximat associat als recursos necessaris per dur a terme el projecte i les despeses de manteniment del DRP durant el primer any. Els recursos participants son: un cap de projecte, dos tècnics de sistemes i un desenvolupador. L'import de l'alta del servei i manteniment d'un any era 591,16€, com s'analitzava al apartat 3.

Rol	**Preu/hora**	**Hores**	**Cost**
Cap de projecte	20€	30	600€
Tècnics de sistemes	12€	236	2.832€
Desenvolupador	12€	46	552€
TOTAL Recursos		**312**	**3.984€**
TOTAL Projecte			**4.575,16€**

Taula 3. *Detall del cost del projecte*

El cost final del projecte es situa en 4575,16€, on s'inclou el disseny i implementació del sistema i el primer any de manteniment. S'ha complert el requeriment inicial de realitzar un entorn de recuperació amb una despesa anual continguda i no es sobrepassa el límit de 2000€ anuals de manteniment de la nova infraestructura. L'objectiu de costos del projecte s'ha assolit.

7. Conclusions i futures vies de treball

Després de realitzar el disseny de la solució i fer el desplegament a producció, podem extreure una sèrie de conclusions del funcionament de la mateixa. Tot seguit es detallen:

- Integritat de les dades: La sincronització de la base de dades i els fitxers de contingut audiovisual no va reportar cap incident i es va realitzar correctament.
- Replicació oracle: Al optar per implementar un procés de replicació amb l'eina Veeam Backup que mitjançant les rèpliques ha permès realitzar el traspàs de la base de dades en temps propers als 20 minuts. Al ser un procés automatitzat i monitoritzat, s'ha aconseguit implementar un sistema que assegura la integritat de les dades i facilita la gestió de la replicació.
- Temps activació/desactivació del DRP: El procés necessita d'una hora i trenta minuts aproximadament, complint el requeriment inicial del projecte.
- Temps de resposta del portal: Els temps de carrega del portal van ser molt propers als habituals. La diferència no va superar els 300ms, assegurant d'aquesta manera que l'usuari no experimentés lentitud a la navegació per les notícies del portal.
- Disponibilitat web: Després de publicar la noticia del incident químic a l'Anoia es va rebre un nivell molt elevat de visitants que va afectar al rendiment del balancejador. L'incident s'hauria reproduït de forma idèntica a l'entorn de producció, perquè no va ser degut a falta de recursos o connectivitat.
- Enviament de continguts: El servei d'enviament de continguts va funcionar correctament durant l'actuació. Però es van detectar cues degudes a l'ample de banda de sortida disponible (10MB/s). Disposar d'una línia de connexió amb major ample de banda de sortida, facilitaria el procés d'entrega directa als clients reduint el temps d'espera.

L'entorn dissenyat i implementat cobreix els requeriments i necessitats de l'empresa per donar solució a una possible incidència que obligui a activar un entorn temporal on poder continuar amb les activitats de negoci.

Per facilitar l'execució s'ha redactat un runbook, el qual pot ser seguit pels tècnics. Amb aquet procediment es facilita la seva actuació al tenir totes les etapes definides i comentades de forma seqüencial. El cost de manteniment del nou entorn, fixat a l'inici amb un màxim de 2.000€ anual, s'ha rebaixat fins a una quarta part.

Tot i així es detecten punts de millora al sistema plantejat, que poden augmentar el seu rendiment i la seva resposta.

Per tal d'evitar l'incident relacionat amb el balancejador durant l'actuació, cal realitzar un estudi de rendiment del mateix per determinar si cal substituir-lo o modificar la seva configuració. S'ha començat a analitzar diferents solucions que ofereix el mercat per la implementació de balancejadors de càrrega a servidors Linux.

Una segona línia de fibra dedicada íntegrament al servei d'enviaments millorant el temps d'enviament de continguts als clients, i la resposta a la navegació del portal web. Tot i continuar dintre dels marges acceptables (diferències de 200ms) durant l'activació del DRP actual.

Cal tenir present l'escenari que presenten les solucions al núvol. Tot i suposar un increment de la despesa que no podia ser assumida pel projecte, aquest tipus de solucions estan experimentant una tendència a reduir els costos dels seus serveis. I plantegen una nova via d'implementació pels entorns de producció empresarials. Una disminució del preu associat a un increment de l'antiguitat dels sistemes actuals, i el cost de manteniment, ens apropen al canvi de la infraestructura per fer el salt a la migració al núvol.

Referències

[1] Michael Pietroforte, "Microsoft is now the number two in the cloud", https://4sysops.com/archives/microsoft-is-now-the-number-two-in-the-cloud/ (data: 21/11/2014)

[2] S. Snedaker, "Business Cotinuity and Disaster Recovery Planning for IT Professionals", Syngress, 2013, pp. 13

[3] Pàgina oficial per contractacions de línies d'empresa movistar: http://www.movistar.es/empresas/

[4] Veeam, "Veeam Backup & Replication for VMware | User Guide" , rev 7, pp.130

[5] Linux Foundation: https://refspecs.linuxfoundation.org/LSB_1.1.0/gLSB/rsync.html (data: 02/12/2014)