Alta disponibilitat amb Centreon

Carlos Burgos López

Resum— Actualment les empreses compten amb sistemes informàtics els quals han d'estar en actiu les 24 hores del dia i els 365 dies de l'any. Això ens fa pensar que aquests equips han de ser monitoritzats, d'una manera bastant precisa i sense cap tipus d'interrupció. L'objectiu d'aquest treball és el desenvolupament d'un entorn de monitorització amb alta disponibilitat. Per arribar a complir aquest objectiu, explicarem com podem garantir que aquests equips són monitoritzats de manera continua, sense cap tipus d'interrupció. Primerament, determinarem quina és la millor col·locació de l'equip de monitorització dins de la xarxa, analitzarem quins són els punts clau del sistema per garantir el funcionament continu. Tenint en compte que els entorns de monitorització es creu que són entorns poc importants i es proporcionen pocs recursos pel seu muntatge, intentarem minimitzar-los, per tal d'ajustar-nos el màxim a la realitat. Per finalitzar, podrem veure com amb la implantació d'un sistema d'aquest tipus podem treure molt de partit a la monitorització i ens pot arribar a determinar si els sistemes estan funcionant correctament o si necessiten un relleu imminent.

Paraules clau— Centreon, Pacemaker, Corosync, DRBD, MySQL, CentOS, Cluster, Nagios, monitorització, virtualització, Business Intelligence

Abstract— Nowadays, companies have complex computer systems, must be active 24 hours per day and 365 days per year. This situation suggests these computer equipments, should be monitored, working uninterrupted and in accurate manner. The purpose of this work is the development of a monitoring environment with a high availability. To get this objective, we will explain how we can ensure that these devices are monitored continuously, uninterrupted. Firstly, we have to determine the best placement for the monitoring equipment in the network, then analyze the main points to ensure continuous operation. Knowing the general opinion of the unimportance of monitoring environment, and having not many resources for their assembly, we have to minimize them to adjust the process at the real situation. Finally, we can see how the implementation of this kind of system, can be usefull for the monitoring and also determine the proper operation of the systems, or if they need an imminent replacement.

Keywords— Centreon, Pacemaker, Corosync, DRBD, MySQL, CentOS, Cluster, Nagios, monitoring, virtualization, Business Intelligence

1 Introducció

Actualment, els sistemes d'informació es consideren sistemes imprescindibles en la vida quotidiana de qualsevol ciutadà. Focalitzant-nos en les empreses, l'aturada d'un sol sistema produeix que els treballadors quedin sense poder treballar, ocasionant això una greu pèrdua econòmica per l'empresa implicada, ja que no poden fer tasques sense els sistemes que emmagatzemen la informació. Si això ho extrapolem per empreses que tenen el 100% del seu negoci online, l'aturada de serveis implica el tancament de l'empresa, aspecte inadmissible per a moltes elles. Per la qual cosa, la monitorització d'aquests sistemes, per preveure errades dels entorn i poder-les mitigar, podrà evitar problemes més greus.

Els entorns de monitorització més sofisticats permeten aplicar eines de Business Intelligence(BI) per tal de determinar el rendiment del equips i dels serveis associats.
Per tant, els entorns de monitorització estant començant a cobrar una importància alta dins de les corporacions, ja que són els ulls dels administradors de sistemes. Degut a la importància d'aquests entorns ens plantegem el muntatge d'un entorn de monitorització amb Centreon. Ens marquem els següents objectius:

- Disseny d'una infraestructura de monitorització eficient que permeti una redundància de tasques.
- Instal·lació del sistema de monitorització Centreon.
- Instal·lació i configuració de l'alta disponibilitat.
- Anàlisis dels checks afectats per la implantació de l'alta disponibilitat.

- *E-mail de contacte: carlos.burgos@e-campus.uab.cat*
- *Menció realitzada: Tecnologies de la Informació.*
- *Treball tutoritzat per: Josep Maria Basart Muñoz (dEIC)*
- *Curs 2013/14*

A continuació es troben els apartats, estat de l'art; els sistemes de monitorització Nagios i Centreon; avantatges i inconvenients de la virtualització; instal·lació i configuració de l'alta disponibilitat; anàlisi de checks conflictius; resultats; conclusions; futures línies de treball; agraïments; bibliografia i els apèndixs.

2 Estat de l'art

Fa un temps, les grans empreses no disposaven de gran quantitat de recursos informàtics per a la seva gestió i funcionament, de manera que, el plantejament d'un sistema de monitorització de la infraestructura TIC era impensable.

Conforme ha anat avançant la tecnologia ha permès aut matitzar tasques i aportar moltíssimes millores. Aquestes millores han produït que actualment els entorns TIC de les empreses o industries han passat a ser un aspecte clau pel funcionament i gestió. Per la qual cosa, els sistemes de monitorització d'aquests entorns comencen a semblar una figura imprescindible per la gestió i control dels entorns. Tot i que pot semblar un aspecte molt evident, aquest canvi es complicat d'incorporar a les empreses ja que els entorns de monitorització no són visibles per l'usuari final i en moltes ocasions es presta més importància a altres aspectes.

Cal remarcar que una vegada implantat el sistema de monitorització i es mostra la seva utilitat, aquest passa a tenir una figura imprescindible pels administradors de sistemes, ja que els sistemes de monitorització passen a ser els ulls dels administradors. Podem trobar entorns de tot tipus, de pagament, lliures i suportats per fabricants. Els més populars poden ser Nagios, Centreon, Zabbix, Xymon, Zenoss, entre altres. S'ha vist que aquests sistemes poden arribar a recollir informació molt elaborada de manera que una vegada s'està acostumat a la seva utilització és molt complicat treballar sense. Degut a la seva importància, cal garantir el seu funcionament i la seva estabilitat per poder treure un rendiment òptim. Actualment, aquest sistemes s'estan començant a utilitzar per avaluar el funcionament del negoci de manera que una petita aturada en aquests entorns suposa l'obtenció de valors erronis que poden produir errades decisives en el desenvolupament de l'activitat empresarial. Tots aquests sistemes es mostren com entorns extremadament importants, però cap d'ells aporta una estructura fàcil per poder implantar una alta disponibilitat del propi sistema, per evitar aturades inesperades.

3 Els sistemes de monitorització Nagios i Centreon

En aquesta secció s'explicarà els coneixements bàsics de Nagios i Centreon per tal de poder aconseguir els objectius marcats.

3.1 Funcionament de Nagios

Nagios[1] és una plataforma de monitorització que aporta una visibilitat global de l'estat dels sistemes. Aquest sistema de monitorització utilitza el paradigma de client servidor per tal de dur a terme la monitorització. És capaç de monitoritzar sistemes Windows, Linux, Solaris i també utilitza el protocol Simple Network Management Protocol(SNMP), entre molts altres, per monitoritzar equips. De manera que ens permet monitoritzar a nivell de sistema i a nivell hardware l'estat dels equips de la nostra corporació.

Per tal de poder definir quins seran els nostres punts crítics pel funcionament del sistema, és necessari saber de quina manera funciona el sistema, quins protocols utilitza i de quina manera ho gestiona internament.

El que realitza un sistema de monitorització simple, és executar uns checks preprogramats als sistemes que es volen monitoritzar, per avaluar si el seu estat és correcte i si el funcionament també ho és. En cas que l'estat sigui correcte, únicament torna a programar un check per tornar avaluar el sistema minuts més tard. En cas que es detecti qualsevol anomalia, es mostra una alerta a l'entorn i s'avisa de diferents maneres a l'administrador del sistema implicat, ja sigui enviant un e-mail, enviant un Tweet, enviant un SMS, fent una trucada, entre altres mètodes. Tota aquesta gestió es realitza mitjançant l'eina de monitorització i sense l'actuació de cap argument extern. Per la qual cosa, en el nostre cas Nagios, es capaç de gestionar tot això.

Per gestionar-ho, utilitza un esquema molt simple, únicament té un procés nucli que s'encarrega d'anar programant tots els checks, posteriorment avaluant les respostes i prenent decisions. Per altra banda, te els serveis de monitorització NRPE i NSCA, entre altres, que s'encarreguen d'executar el check a l'equip remot i retornar el resultat d'una forma comprensible per Nagios. També decideix si cal enviar notificacions o no i de quin tipus. Únicament decideix si cal o no enviar notificació, posteriorment passa la tasca d'enviament al servei corresponent, de manera que el temps de decisió és mínim. El nucli de Nagios pot arribar a ser molt complex però únicament necessitarem unes nocions bàsiques per poder gestionar-lo de forma correcta. El nucli, com hem explicat anteriorment, només gestiona tasques i pren les decisions, per tant és totalment aliè al funcionament de la resta de serveis. Amb això vull dir que si Nagios intenta enviar un check a un equip i es troba que l'agent NRPE del propi host Nagios està aturat retornarà un error com si el problema fos de l'equip client quan realment no és així. Això, ens fa veure que la implantació de l'alta disponibilitat no serà senzilla, ja que Nagios no integra tot un conjunt de processos coordinats a la perfecció, sinó que integra mòduls que fan les tasques desitjades. Per la qual cosa, serà necessari garantir tots aquest punts de forma independent per garantir el funcionament de l'aplicació.

A la *Figura 1* podem veure gràficament els aspectes explicats i es pot apreciar com Nagios integra una sèrie de configuracions per tal de poder fer tota la gestió esmentada.

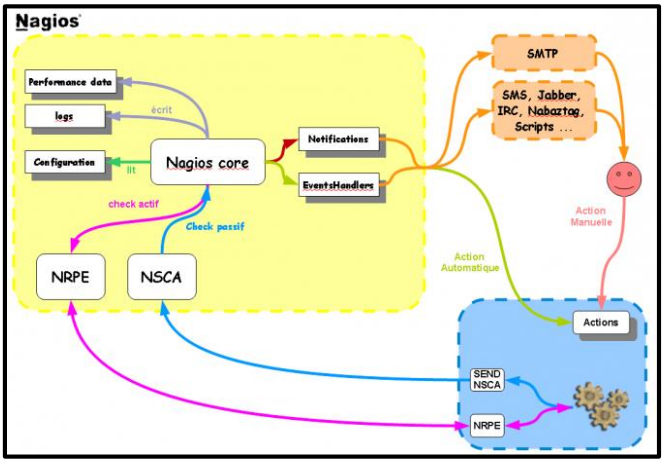


Figura 1. Esquema funcionament Nagios

3.2 Funcionament de Centreon

Pel que fa al funcionament de Centreon[2] és molt similar al de Nagios, degut el fet que es tracta d'una ampliació de Nagios, el qual integra certes millores que ara descriurem.

L'estructura de Centreon consta d'una base de dades MariaDB en la qual s'emmagatzema tot el conjunt de resultats recollits en els checks, un servei CentreonCore el qual s'encarrega del funcionament de la gran millora que aporta Centreon, una monitorització distribuïda amb diferents Nagios distribuïts en diversos equips però amb una única gestió central. També integra un servei CentreonStorage encarregat de recol·lectar les dades i inserir-les a base de dades, i per últim un servei Ndo2DB el qual escriu a base de dades els resultats obtinguts a la resta de Nagios distribuïts.

En aquest escenari de monitorització distribuïda, els equips que únicament integren Nagios s'anomenen Pollers i els equips que gestionen tota la configuració són nodes Centrals. Com podem veure el funcionament és molt similar a Nagios degut el fet que la plataforma implementa Nagios per la monitorització, i el funcionament d'aquest no ha estat modificat.

A la *Figura 2* podem observar tots els aspectes explicats anteriorment, es pot veure també que entre el node central i els pollers existeix una sincronització de dades imprescindible pel funcionament, cal dir que aquesta sincronització es realitza en moments puntuals, en determinades tasques que es realitzen a nivell d'administració i per tant l'administrador del sistema controla i supervisa.

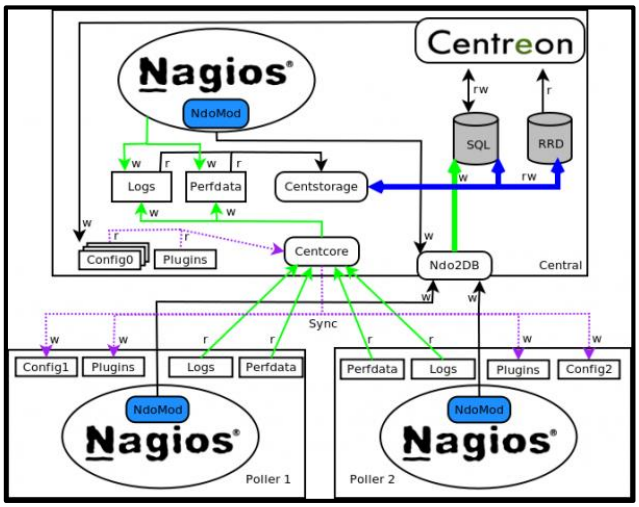


Figura 2. Esquema funcionament Centreon

Pel que fa a l'escriptura a base de dades per part dels Pollers es realitza mitjançant un servei Ndo, aquest servei el que realitza és la generació d'un fitxer amb un conjunt de marques temporals i des del node central s'avalua per tal de poder fer les insercions pertinents. A la *Figura 3* podem veure amb més detall tot el procés d'escriptura a base de dades per part dels Pollers.

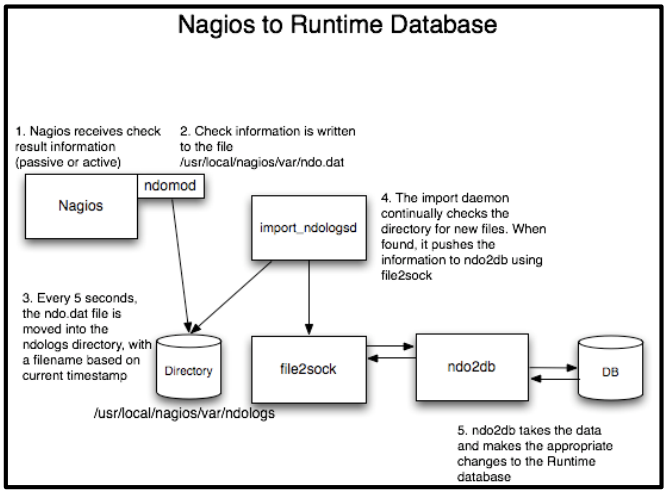


Figura 3. Funcionament servei Ndo

Cal remarcar que aquesta tasca es totalment transparent i amb una configuració correcte del servei Ndo les dades s'actualitzen correctament.

Centreon, internament, gestiona una sèrie de sessions per tal de poder accedir a la interfície web que integra. Aquestes sessions s'emmagatzemen a base de dades i també en forma de fitxer.

Les principals diferencies entre Centreon i Nagios són que Centreon va un pas més enllà i proporciona una interfície web no únicament per monitoritzar com fa Nagios sinó que també per gestionar l'entorn de monitorització. A part,

també integra gràfiques de tipus RRD i permet extreure informes de disponibilitat. Com hem dit anteriorment, permet fer una monitorització distribuïda que ens serà molt profitosa en casos en els que tinguem una gran quantitat d'equips que monitoritzar, ja que, els sistemes de monitorització es sobrecarreguen en gran mesura quan s'executen checks molt complexos o afegim una gran quantitat d'equips.

4 AVANTATGES I INCONVENIENTS DE LA VIRTUALITZACIÓ

Per tal de dur el projecte per bon camí la virtualització juga un paper imprescindible. El disseny de xarxa que s'explicarà més endavant i els dos equips implicats en el muntatge del sistema no necessàriament poden estar a l'abast de tothom. Amb un sistema de virtualització podem aprofitar molt més els recursos de l'equip físic i distribuir-los entre els diferents equips virtuals, en funció dels requeriments en cada moment.

En el nostre escenari, necessitem muntar dos equips idèntics de manera que els assignarem un vCPU a cada un i 1 GB de memòria RAM per equip. A més a més el propi sistema de virtualització ens proporciona poder fer una imatge de l'estat de l'equip virtual en el moment que desitgem. Aquest recurs, ens permet fer una instal·lació pas a pas de l'entorn amb copies de seguretat prèvies. En cas de tenir problemes, es pot tornar a l'estat anterior en menys de 5 minuts. Això aporta una tranquil·litat que permet treballar amb seguretat i sense assumir riscos.

En entorns més complexos i sofisticats, el fet de tenir els equips virtualitzats, permeten alta disponibilitat a nivell d'equip. Això vol dir que en cas que l'equip físic que conté els equips virtuals tingui problemes, mou tots els equips virtuals a un altre equip físic. Això assegura encara més la disponibilitat dels equips, reduint les errades del sistema de monitorització a nivell dels propis serveis.

Tots els aspectes explicats anteriorment, suposen avantatges, però també existeixen inconvenients. Els sistemes de virtualització requereixen estar instal·lats sobre equips potents amb característiques d'alt rendiment. També, en aquest model de treball tots els equips virtuals depenen d'un únic equip físic, de manera que un problema en un equip físic pot ocasionar molts problemes a diferents equips virtuals. Si el moviment d'equips virtuals explicat anteriorment no funciona correctament, realment la caiguda de serveis pot arribar a ser molt important. Un altre inconvenient és la falta d'experiència dels usuaris. No es habitual la utilització de sistemes de virtualització i això produeix que usuaris poc experimentats puguin tenir errades que en un futur poden arribar a ser molt greus. També, estem afegint un nou tipus de sistema al nostre entorn, de manera que requereix un manteniment i unes actualitzacions periòdiques, això afegeix feina extra d'administració que cal tenir en compte.

Tot i els inconvenients, els avantatges són molt superiors i més en el nostre cas, on no disposem d'un gran entorn, de manera que per desenvolupar el projecte utilitzarem un entorn de virtualització a petita escala. Per tal que ens aporti algunes de les millores descrites. Com per exemple la possibilitat de fer imatges com a copia de seguretat.

5 INSTAL·LACIÓ I CONFIGURACIÓ DE L'ALTA DISPONIBILITAT

En aquesta secció s'explicarà totes les decisions preses durant la implantació de l'alta disponibilitat i es detallaran aspectes de configuració de les eines utilitzades.

5.1 Disseny de xarxa

Per tal de poder fer una monitorització precisa cal fer una col·locació correcta de l'entorn de monitorització dins de la xarxa a monitoritzar. Per tal de localitzar l'equip a la zona idònia de la xarxa, podem dividir l'entorn de xarxa local en dues zones, la zona desmilitaritzada(DMZ) i la xarxa d'usuaris. Ambdues xarxes estan separades entre si per un firewall, el qual únicament permet el trànsit imprescindible en ambdós sentits. Aquesta restricció ens permetrà aplicar una seguretat extra als equips dels usuaris i als servidors, ja que únicament es poden establir les connexions imprescindibles per fer servir els serveis que proporcionen els servidors. A la zona DMZ es troben tots els servidors de la corporació que tenen serveis publicats a Internet o serveis substancialment vulnerables a atacs. També es col·loca un segon nivell de seguretat de xarxa. Els servidors de la DMZ tenen un altre firewall el qual controla la sortida i entrada de trànsit cap a Internet. Això proporciona un primer nivell de seguretat que evita un gran nombre d'atacs als servidors més exposats a Internet.

El sistema de monitorització es un servei que únicament el volem per monitoritzar i aportar-nos informació dels nostres equips que tenim a la xarxa. De manera que aquests serveis no han d'estar publicats a Internet, és un aspecte poc comú i perillós si es publiquen, ja que poden arribar a proporcionar informació de la nostra estructura de xarxa. Podem trobar entitats que subcontractin serveis de monitorització, llavors pot ser que els sigui necessari fer aquesta publicació, però parlem de casos molt concrets i poc recomanables. Per la qual cosa l'aspecte més comú és no tenir-ho publicat a Internet. Això ens fa pensar que la seva localització perfecte seria la LAN d'usuaris. Però si ho pensem detingudament, cada vegada que cal monitoritzar un equip implica la modificació de regles al firewall intern ja que els equips a monitoritzar es troben la gran majoria a la DMZ, produint això un gran increment de feina en l'administració dels dispositius de xarxa. Ja que per cada equip a monitoritzar, caldria autoritzar l'accés als ports implicats en la monitorització des de la xarxa d'usuaris fins a l'equip en qüestió de la DMZ.

Per aquest motiu decidim ubicar Centreon a la DMZ, però impedim l'accés al servei des de dominis públics, únicament es pot accedir internament. A la *Figura 4* es pot veure el plantejament de xarxa explicat.

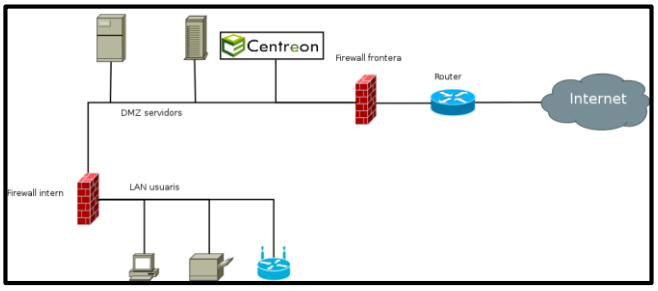


Figura 4. Esquema de xarxa

Cal tenir en compte que aquesta ubicació produirà que si hem de monitoritzar un equip de la xarxa d'usuaris, serà necessari obrir les connexions al firewall intern. Aquestes situacions seran mínimes i ens estalviaran molta feina d'administració del firewall intern. D'aquesta manera també ens assegurarem que si vulneren cap servidor de la DMZ no pugui propagar la infecció cap a la xarxa d'usuaris.

5.2 Instal·lació Centreon

Per fer la instal·lació descarreguem una imatge ISO de la pàgina oficial de Centreon, la qual integra un sistema operatiu amb Centreon preinstal·lat de manera que ens facilita la tasca d'integració amb el sistema operatiu i ens podem centrar molt més en la implantació de l'alta disponibilitat. Aquesta distribució la proporciona l'empresa desenvolupadora de Centreon, Merethis, i l'anomena Centreon Enterprise Server(CES). Bàsicament és una distribució CentOS 6 amb un instal·lador molt intuïtiu de Centreon i amb una sèrie d'eines que faciliten la monitorització dels equips.
Centreon permet dues arquitectures molt similars:

- Centreon Broker: El qual integra Centreon amb el protocol BBDO.
- Centreon Nagios: El qual integra Nagios amb el protocol ndo.

La segona opció esta en vies d'extinció ja que va ser el primer mètode que va emprar Centreon per la monitorització degut a la seva descendència de Nagios. Actualment s'està seguint una línia més independent i s'està desvinculant del projecte Nagios sense perdre la filosofia d'aquest. Com és important desenvolupar el projecte en una plataforma continuista, fem la instal·lació de Centreon Broker. Aquesta decisió implica l'estudi dels processos que funcionen en aquest tipus d'arquitectura els quals són molt semblants a la de Nagios però amb petites diferencies que aporten més estabilitat a la plataforma. Una vegada presa aquesta decisió, cal seguir el procés d'instal·lació descrit a l'apèndix A1, això ens permetrà finalitzar la instal·lació del sistema i complir un dels objectius marcats.

5.3 Identificació dels punts crítics

Per tal de poder redundar els serveis i poder garantir una fiabilitat de la plataforma cal identificar els processos clau en el funcionament de l'entorn. D'aquesta manera podrem decidir quin és el millor mètode per tal d'establir redundància en cadascun dels aspectes. En l'estudi del funcionament de Centreon, tal com es descriu a l'apartat 3.2 d'aquest mateix article, podem veure que existeixen dues tasques ben independents entre elles:

- Emmagatzematge de dades a base de dades.
- Execució dels checks, procés nucli del sistema.

Per tant, aquests dos aspectes caldrà redundar-los com sigui possible, amb tot el que comporti.

Un altre aspecte a remarcar és que Centreon es basa en la sincronització de configuracions entre nodes de monitorització. Nosaltres només ens centrarem en la redundància del node central de la plataforma, però no cal obviar aquest punt, ja que ambdós nodes necessiten tenir les mateixes configuracions i dades per evitar problemes de sincronisme. Per tant, també cal garantir els següents punts:

- Redundància de sessions d'usuari.
- Redundància de configuracions entre nodes centrals.

Una vegada decidits els quatre punts claus a redundar ens centrarem, primerament en la part de base de dades, posteriorment passarem a redundar el procés nucli i per últim mirarem de replicar les configuracions i sessions entre nodes.

5.4 Clusterització Base de Dades

Per tal de redundar les bases de dades, cal revisar amb quins entorns de bases de dades estem treballant, quines alternatives ens proporcionen i si són realment útils pel nostre objectiu.

Centreon ens proporciona una base de dades MariaDB[3], en la qual existeixen models de clusterització. MariaDB es tracta d'un fork de MySQL, per tant també permet la utilització d'aquests tipus de clústers. MariaDB en si es tracta d'un projecte bastant nou actualment, per aquest motiu la continuïtat dels projectes de clusterització són dubtosos. Per la qual cosa, optem per investigar els mètodes que poden existir per redundar les dades amb MySQL[4], els quals també podrem aplicar a MariaDB.

Ens interessa obtenir una replicació que sigui senzilla de mantenir i no aporti dificultats a l'administració de la plataforma.
Podem trobar dos mètodes:

- Replicació
- Clusterització

La replicació consisteix en copiar les dades d'un node a un altre mitjançant un mètode de parseig de logs. D'aquesta manera, aconseguim tenir dues bases de dades idèntiques en dos nodes diferents. Aquest model permet tenir una redundància master-slave que ens permet fer un canvi de base de dades. En cas de problemes amb el servidor, però presenta un petit inconvenient, degut el fet que el mètode de replicació que utilitza el canvi de rols de master → slave i slave → master no es senzill i en moltes ocasions produeix problemes de replicació. Un altre problema, és que la replicació no és atòmica, per la qual cosa una actualització al node master no implica que la base de dades slave contingui les mateixes dades, pot tenir un temps de diferència i això també produeix problemes. Per això, aquest darrer punt ens fa descartar la replicació com a possible alternativa, ja que si no podem garantir l'atomicitat de les operacions a tots dos nodes l'aplicació pot donar problemes molt seriosos.

La clusterització sembla que pot ser una altra solució, aquesta però garanteix l'atomicitat de les operacions i independitza les dades de l'administració. Tot i això, aquest model requereix com a mínim 3 nodes per tal de fer la implantació. Segons el que vam explicar a l'inici de l'article als entorns de monitorització s'acostuma a proporcionar pocs recursos, de manera que la implantació de 3 nodes, únicament per la replicació de les dades, és un aspecte insostenible, per tant també descartem aquesta opció.

Veient que a nivell del servei de base de dades no podem garantir la replicació degut a la complexitat o al mètode de replicació, decidim baixar de nivell i centrar-nos en la replicació dels fitxers que contenen les dades i les estructures que MariaDB interpreta. Fent una simple copia cada cert temps no ens era suficient, degut el fet que l'entorn pot produir problemes en qualsevol moment i això podria produir que les dades no fossin iguals a ambdós nodes, ocasionant la pèrdua de dades.

Partim que no disposem de cap entorn que ens pugui garantir la replicació a nivell hardware mitjançant un RAID, implantem Distributed Replicated Block Device(DRBD)[5] DRBD és un sistema que ens permet muntar un RAID software mitjançant la xarxa. En el nostre cas ens és molt útil fer la implantació d'un RAID 1 o mirroring per tal de replicar les dades dels discos que contenen les dades de MariaDB.

A la imatge de la *Figura 5* es pot veure, esquemàticament, com DRBD fa un clonatge de les dades mitjançant la xarxa i ens garanteix que una base de dades i l'altre tenen les mateixes dades. Per fer el clonatge, es configuren dos discos virtuals als servidors, els quals contindran les dades que MariaDB gestiona. Es defineix un dels discos com a disc master i es demana fer la copia d'un a l'altre. Per tal que la copia sigui ràpida és recomanable tenir una interfície de xarxa dedicada, això permetrà que es pugui aprofitar l'ample de banda al 100%[6].

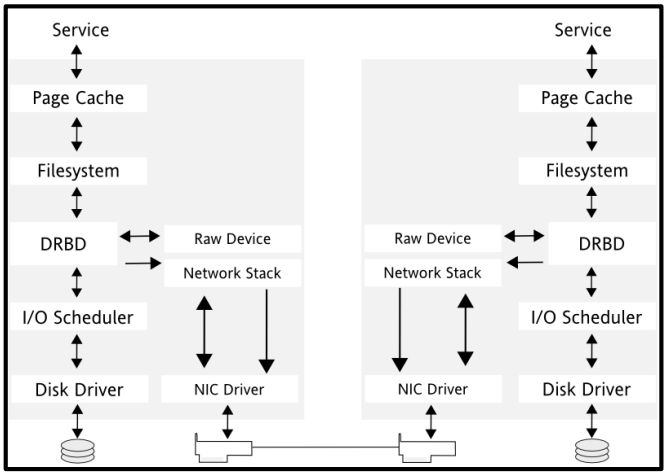


Figura 5. Esquema DRBD

Una vegada finalitzada la primera copia, la sincronització de les dades és automàtica i no produeix grans problemes. Aquest sistema però, no ens permet accedir a les dades des del node slave. Això implica que ens caldrà controlar correctament el muntatge i desmuntatge dels discos en cas de caiguda del node master i també l'arrencada i aturada del servei de base de dades. Tot aquest control ho explicarem més endavant amb la clusterització de serveis. Les configuracions aplicades en la sincronització DRBD les podeu trobar a l'apèndix A2.

5.5 Clusterització serveis Centreon

Tal com hem dit anteriorment, es necessari dur un control dels serveis que Centreon utilitza per fer la monitorització i per fer l'emmagatzematge a base de dades. Per dur a terme aquest control del clúster, utilitzarem Corosync i Pacemaker[7]. Pacemaker és el controlador de serveis, detecta si els serveis estan operant amb normalitat o tenen problemes i gestiona l'aturada i arrencada. Corosync en canvi verifica si els nodes tenen comunicació i estan actius. A la *Figura 6* podeu veure com esta estructurada la jerarquia entre Corosync i Pacemaker.

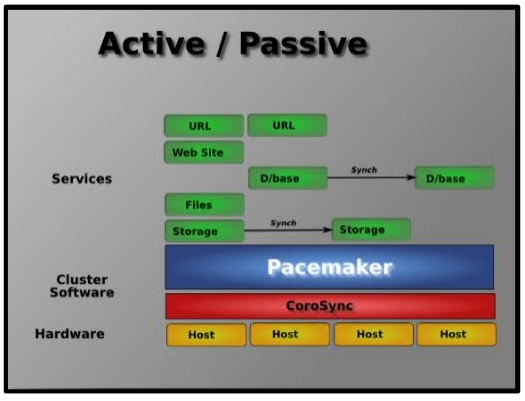


Figura 6. Estructura Pacemaker + Corosync

A l'apartat 5.3, hem pogut veure que és necessari controlar el procés nucli per tal que no realitzi checks innecessaris ja que no tindrà la possibilitat d'emmagatzemar les dades perquè la base de dades estarà aturada. El servei que gestiona tot el nucli de Centreon s'anomena "centcore". Per altra banda, el servei encarregat d'executar els checks s'anomena "cbd". També caldrà controlar el servei de base de dades, així com el muntatge i desmuntatge de la unitat DRBD.

Per tal que els equips que es monitoritzen i els usuaris que utilitzen la interfície web no hagin de validar contínuament a quina IP han d'accedir, s'afegeix una adreça IP Virtual(VIP) a la configuració de Pacemaker perquè la pugui anar transferint entre nodes segons el node que estigui proporcionant el servei. Això ens evitarà haver de verificar contínuament a quina IP cal accedir per veure la interfície web de Centreon. Per tal que Corosync pugui controlar correctament la latència entre nodes, l'escenari ideal és utilitzar una interfície dedicada a tal efecte. Independent de la que utilitza DRBD i la resta de serveis.

Pacemaker i Corosync són eines que tenen multitud de paràmetres de configuració que faciliten la tasca d'administració a multitud de plataformes clusteritzades, val a dir que molts d'aquests paràmetres en entorns petits com és el nostre cas no tenen sentit.

Pacemaker integra una opció anomenada "quorum" la qual s'encarrega de verificar que tots els nodes es posen d'acord en el moment de prendre una decisió. En un escenari com el nostre amb dos nodes aquesta opció no té sentit, ja que les decisions es prenen de forma independent. Si un node s'atura, l'altre ha de decidir per si sol agafar el rol de master. Per tant, deshabilitem aquesta opció. També integra una opció anomenada STONITH (Shoot The Other Node In The Head), la qual atura un node en cas que estigui donant problemes al clúster. En el nostre cas com és un entorn amb dos nodes no ens interessa que si el node master dona problemes amb el clúster s'aturi, és més eficient monitoritzar els problemes, no aturar el node i fer una revisió en cas de detectar problemes. Aquesta opció igual que l'anterior són útils en entorns amb més de dos nodes, per la qual cosa aquesta també la desactivem.

En aquest punt, ja tenim identificats els serveis i quines opcions de Pacemaker no ens interessen. Per tal d'identificar els nodes els assignem un nom, en el meu cas el node que actuarà la gran majoria de temps com a node master l'he anomenat "mortadelo" i el node que actuarà com slave l'he anomenat "filemon". Una vegada identificats el nodes, cal definir quin serà l'ordre d'arrencada dels serveis, ja que aquesta tasca la realitzarà el propi Corosync i no pas el sistema. Per la qual cosa, deshabilitem l'arrencada dels serveis del sistema. L'ordre adient per l'arrencada de serveis seria primer de tot arrencar el dispositiu DRBD, després arrencar la base de dades, posteriorment arrencar els serveis de Centreon, continuar amb el servei web i per últim assignar la VIP per tal que els usuaris puguin accedir a la interfície web. Per tal d'establir una jerarquització dins de l'entorn, he configurat a Pacemaker perque en cas que hi hagi caiguda del node "mortadelo" transfereixi tots els serveis a "filemon". Si posteriorment el node "mortadelo" recupera, "filemon" transferirà novament els serveis al node primari. A l'apèndix A3 es poden veure les configuracions aplicades per tal que tot el que he explicat anteriorment funcioni correctament.

Amb aquestes darreres configuracions ja tenim un altre objectiu aconseguit, el clúster funciona i en cas de caiguda d'algun servei es transfereixen tots els serveis a l'altre node.

5.6 Sincronització de dades

Centreon, en el seu funcionament habitual genera uns fitxers de configuració que posteriorment transfereix als Pollers corresponents per monitoritzar els servidors configurats. Aquests fitxers es troben a un directori del sistema, per tal que tots dos nodes comptin amb aquestes configuracions s'ha afegit una tasca, la qual cada 5 minuts clona les dades d'un servidor a l'altre. Aquesta copia es fa amb "rsync" un eina que proporciona una copia de fitxers eficient. Per tal que no hi hagi problemes en el copiat, s'han generat un parell de claus SSH a cada node i s'han copiat d'un node a l'altre per autoritzar l'accés sense password.

D'altra banda, la interfície web emmagatzema una sessió cada vegada que algú es connecta. Per evitar que l'usuari detecti el tall de servei es fa un copiat de sessions mitjançant rsync novament. Les sessions s'emmagatzemen al directori "/var/lib/php/session/" i a base de dades. Per la part de base de dades, no ens hem de preocupar, degut el fet que fem el clonatge amb DRBD. A l'apèndix A4 podem veure de quina manera fem la configuració.

Aquesta copia es fa amb rsync[8] i no amb DRBD, perquè DRBD esta pensat per fer un clonatge de discos i no pas un clonatge de directoris, com es tracta de dades que no ocupen massa espai s'ha optat per aquesta opció.

6 ANÀLISI DE CHECKS CONFLICTIUS

Després de tenir enllestit tot el muntatge d'alta disponibilitat, alguns checks no funcionen correctament degut a les configuracions establertes en els checks. Aquest sistemes realitzen dos tipus de checks:

- Checks Actius: Els quals s'executen quan el procés nucli ho indica, de manera que hi ha una comanda de Centreon cap a l'equip monitoritzat i una resposta en sentit contrari per tal que Centreon ho pugui avaluar.
- Checks Passius: Són els checks que no s'executen des de Centreon sinó que estan programats a l'equip monitoritzat i únicament hi ha una

resposta des de l'equip monitoritzat cap a Centreon.

Aquests darrers checks en moltes ocasions s'executen a cabines de discos o sistemes encastats els quals no es poden modificar i únicament permeten aquesta monitorització pròpia. Cal dir que estan en des ús i els darrers models de cabines de discos o equips encastats acostumen a permetre els checks actius.

Amb els checks actius no hauríem de tenir problemes ja que únicament hem de fer-nos càrrec que l'equip monitoritzat accepti la monitorització des de la IP de clúster. Però amb els checks passius caldrà revisar que cada equip monitoritzat està enviant les notificacions dels seus propis checks a la IP del clúster, ja que sinó no ens adonarem dels problemes perquè Centreon es totalment transparent a aquesta configuració, únicament espera un informació del client si no la rep obviarà que el sistema es troba en condicions optimes.

7 RESULTATS

Prèviament a determinar les conclusions obtingudes, cal remarcar que hem aconseguit uns resultats satisfactoris respecte els objectius marcats.

Les versions de les aplicacions utilitzades són les darreres que proporciona la distribució de linux CentOS 6.5, ja que hem intentat fer una instal·lació el màxim estàndard possible per facilitarne el manteniment i configuració.

Finalment el que hem muntat ha estat el següent:

- Nom de l'equip: Mortadelo, Centreon 2.5.0, Base de dades MariaDB 5.5.35, Pacemaker 1.1.10, Corosync 1.4.1, DRBD 8.3, rol primari
- Nom de l'equip: Filemon, Centreon 2.5.0, Base de dades MariaDB 5.5.35, Pacemaker 1.1.10, Corosync 1.4.1, DRBD 8.3, rol secundari

També hem pogut arribar a avaluar quins són els checks que ens donarien problemes després de la implantació de l'alta disponibilitat i proposar solucions per evitar aquest tipus de problemes. Cal dir que el treball ha estat desenvolupat en un entorn virtualitzat per la qual cosa ens ha facilitat molt les tasques i hem pogut aprendre molt respecte aquest tipus d'entorns.

A la *Figura 7* podem veure quin ha estat l'escenari final. Tenim una base de dades redundada amb DRBD, i tots els serveis controlats per Corosync i Pacemaker. El color vermell indica que els serveis estàn en mode passiu i el color verd indica mode Actiu.

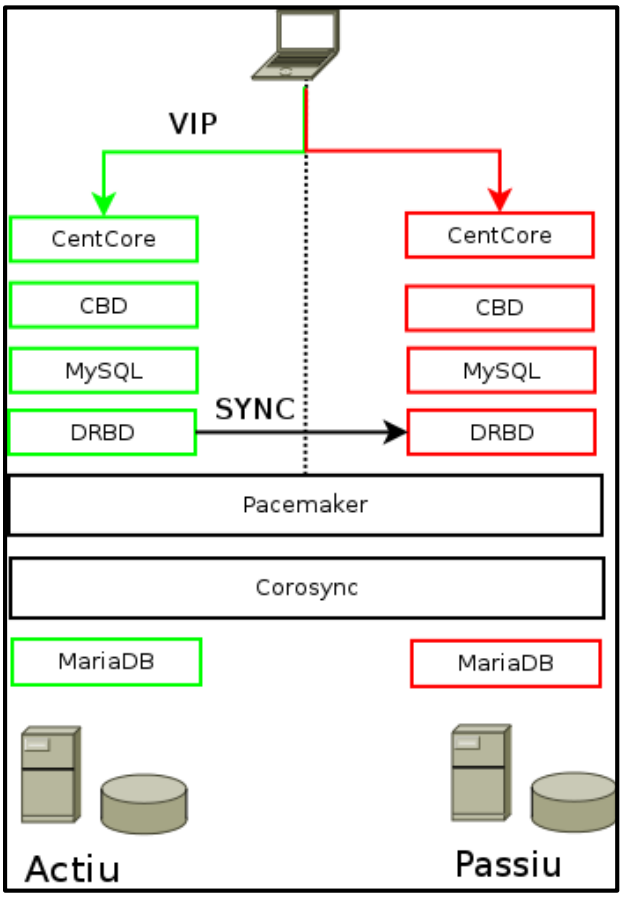


Figura 7. Resultat final

8 CONCLUSIONS

Aquest treball ens ha permès una implementació amb garanties d'un sistema de monitorització Centreon. Durant aquest treball s'ha intentat reduir a la mínima expressió els recursos necessaris per dur a terme el muntatge, ja que habitualment no és possible disposar d'un gran nombre d'equips per un entorn de contingència. Per la qual cosa, s'ha optat per utilitzar software que proporciona la redundància i no pas altres mètodes, com podria ser, per exemple, una desvinculació de la base de dades dels equips de monitorització o entorns de clúster més complexos que requereixen més manteniment i supervisió.

Per altra banda, la utilització d'un entorn virtual ens ha permès aportar moltes avantatges al desenvolupament i al manteniment de la plataforma. En entorns més complexes pot arribar aportar moltes més millores que no pas en un entorn reduït com el nostre cas. Mitjançant l'entorn virtualitzat hem pogut anar fent copies de seguretat periòdiques amb el propi entorn. En cas de problemes podíem fer una marxa enrere en qüestió de minuts. També amb pocs recursos ens ha fet possible fer el disseny de xarxa presentat ja que en entorns domèstics aquest plantejament pot ser una mica complex.

Aquesta solució, ens proporciona un entorn amb pocs recursos redundats i amb garanties de funcionament, el qual ens pot permetre aplicar certes eines de Business Intelligence i en cas de caiguda dels equips no produir ni la més mínima afectació al negoci, ni a les seves estratègies valoratives. Per la qual cosa, les aplicacions que portin a terme aquest tipus de valoració dels entorns informàtics poden arribar a proporcionar molts beneficis a les empreses, les quals podran valorar si és necessari l'actualització, millora o modificació dels actuals entorns. D'aquesta manera, podran prendre decisions empresarials amb més fiabilitat i garantint que els entorns avaluadors no han tingut problemes, proporcionen dades correctes i perfectament fiables.

Deixant de banda els aspectes de Business Intelligence, aquestes eines de monitorització acostumen a ser els ulls dels administradors de les plataformes, de manera que, en el moment que aquestes eines deixen de funcionar suposen un gran problema ja que no se sap amb certesa si hi ha problemes amb els entorns i si els usuaris poden fer les tasques sobre aquests. Això, pot produir que els problemes siguin detectats amb molt més retard del que s'espera i en cas que sigui un problema de gran importància pot arribar a bloquejar l'activitat de l'empresa. Per aquests fets, considerem que aquests sistemes són imprescindibles en grans entorns i no es poden permetre errades.

Tot i que els entorns de monitorització juguen un rol imprescindible per l'administració de sistemes, les empreses desenvolupadores d'aquest tipus d'aplicacions es centren en proporcionar moltes més funcionalitats a les aplicacions però no pas en facilitar la possibilitat de crear un entorn redundat com el que hem presentat. Aquest aspecte passa desapercebut fins que et trobes sense sistema de monitorització i cal buscar solucions ràpides.

Amb aquest projecte hem pogut veure que es una bona alternativa la utilització de la virtualització, ja que ens ha facilitat molt les tasques. Respecte a la implantació de l'alta disponibilitat podem dir que no és una tasca fàcil ja que implica moltes hores de treball i configuració però una vegada enllestit, el seu funcionament és correcte i ens pot arribar a evitar molts problemes. Per últim, els checks no han complicat massa la tasca d'adaptació, però cal tenir-ho en compte perquè cal fer les petites modificacions descrites per tal de que funcionin correctament.

9 Futures línies de treball

Per donar més continuïtat aquest treball es podrien dur a terme investigacions sobre l'aplicació d'eines de Business Intelligence sobre Centreon i valorar si l'alta disponibilitat realment és aplicable i útil amb la integració d'aquestes eines.

Per altra banda, també seria necessari valorar quin tipus de copies de seguretat sobre el nou entorn serien les més adients, ja que, cal recordar que estem treballant amb motors de bases de dades bloquejant de manera que mentre s'aplica una copia de seguretat l'aplicació pot quedar interrompuda durant el temps de copia. Això es un aspecte bastant crucial ja que la base de dades amb el temps es fa bastant gran.

Aquests sistemes venen previstos d'eines per monitoritzar, però no tenen en compte eines de documentació o ticketing. Un aspecte molt interessant seria la investigació de possibles eines que facilitin la documentació i ticketing dels elements monitoritzats i proporcionar una forta integració amb Centreon.

Existeix una eina anomenada Nagvis que proporciona una visió més real de la monitorització que proporciona Centreon, actualment però la integració web amb les darreres versions és nul·la. Per la qual cosa el disseny d'un connector amb l'aplicació Nagvis seria molt important.

Una altre possible línia seria la investigació de noves eines de monitorització i valorar si implementen una sistema de monitorització en alta disponibilitat, si és més complex implementar-ho i si hi ha cap alternativa millor que Centreon en aquest aspecte.

Agraïments

Aquest treball m'agradaria agrair-lo al meu tutor Josep Maria Basart que m'ha recolzat en tot moment marcant-me les pautes i ajudant-me en tot el que podia.

També m'agradaria agrair el recolzament dels meus companys de classe durant tot el decurs del grau, especialment els meus companys de pràctiques Manuel, Albert, David, Nahuel, entre altres, ja que hem après coses mútuament.

El departament del dEIC el qual he tingut en la gran majoria d'assignatures i ha sigut capaç de transmetre els coneixements necessaris per arribar a fer un treball d'aquest tipus.

I per últim, agrair a la meva família i amics el recolzament continu des del primer dia a la universitat fins a l'entrega d'aquest treball. Ja que sense ells tot això hauria estat molt més complicat.

Bibliografia

[1] Documentació oficial Nagios 3.0[En línia], Recuperat el 3 de Març de 2014, http://nagios.sourceforge.net/docs/3_0/toc.html

[2] Companyia Merethis, Documentació oficial Centreon [En línia]. Recuperat el 21 d'Abril de 2014, http://documentation.centreon.com/docs/centreon/en/latest/release_notes/index.html

[3] MariaDB Documentation[En línia], Recuperat el 21 d'Abril de 2014, https://mariadb.com/kb/en/mariadb-documentation/
[4] MySQL 5.0 reference manual[En línia], Recuperat el 3 de Març de 2014, http://dev.mysql.com/doc/refman/5.0/es/replication.html
[5] The DRBD User's guide[En línia], Recuperat el 21 d'Abril de 2014, http://www.drbd.org/users-guide-8.3/
[6] Configurando un clúster de alta disponibilidad con Heartbeat/DRBD[En línia], Recuperat el 3 de Març de 2014, http://wiki.centos.org/es/HowTos/Ha-Drbd
[7] Beekhof, Andrew, Clusters from scratch ed. 5 (2012)[En línia], Recuperat el 3 de Març de 2014, http://clusterlabs.org/doc/en-US/Pacemaker/1.1-crmsh/html/Clusters_from_Scratch/index.html
[8] Gómez López, Julio; Gil Montoya, Francisco; Villar Fernàndez, Eugenio Eduardo; Méndez Cirera, Francisco; *Administración avanzada de sistemes informaticos* (2010), Ra-Ma

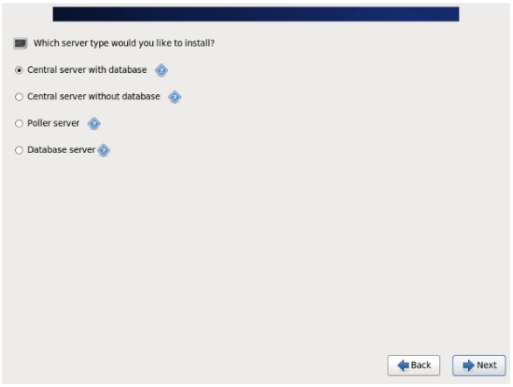
APÈNDIXS

A1. PROCÉS D'INSTAL·LACIÓ DE CENTREON

Per començar carreguem la imatge de Centreon Enterprise Server que podem descarregar de la web del desenvolupador Merethis. I seguim els següents passos:

1. Seleccionem un tipus d'instal·lació gràfica. Això ens carregarà una interfície intuïtiva la qual ens ajudarà durant tot el procés d'instal·lació.
2. Seleccionem una instal·lació de Centreon amb la base de dades incorporada al propi equip.

3. Seleccionarem com a engine de Centreon, Centreon Engine i Broker. Apareix una altra opció que actualment està quedant obsoleta.



4. Posteriorment ens demanarà configuracions típiques com password de l'usuari root, configuració de la sincronització horària, molt important que sigui correcte, configuració de xarxa de l'equip i format que donarem als discos. Tots aquests aspectes són a elecció de l'instal·lador, simplement cal complir els mínims requeriments que remarca Centreon a la seva plana web.

Una vegada enllestits aquests punts, deixarem que acabi l'instal·lador ens demanarà reiniciar l'equip i ja tindrem un equip amb Centreon Enterprise Server instal·lat.

A2. INSTAL·LACIÓ I CONFIGURACIÓ DRBD

Per fer la instal·lació de DRBD cal afegir un nou repositori que no porta integrat CentOS i una vegada instal·lat el servei, fer la carrega del mòdul del kernel. Aquestes accions cal fer-les a tots dos nodes

```
rpm -Uvh http://www.elrepo.org/elrepo-release-6-6.el6.elrepo.noarch.rpm
yum -y install drbd83-utils kmod-drbd83
modprobe drbd
```

Una vegada tenim el mòdul carregat afegim la següent configuració al fitxer "/etc/drbd.d/clusterdb.res", això ens permetrà configurar la sincronització entre nodes.

```
resource clusterdb
 {
 startup {
 wfc-timeout 30;
 outdated-wfc-timeout 20;
 degr-wfc-timeout 30;
 }
net {
 cram-hmac-alg sha1;
 shared-secret sync_disk;
 }
syncer {
 rate 10M;
 al-extents 257;
 on-no-data-accessible io-error;
```

```
}
on drbd1 {
device /dev/drbd0;
disk /dev/sdb1;
address 192.168.1.8:7788;
flexible-meta-disk internal;
}
on drbd2 {
device /dev/drbd0;
disk /dev/sdb1;
address 192.168.1.9:7788;
meta-disk internal;
}
}
```

Posteriorment caldrà crear el dispositiu virtual i arrencar el servei a tots dos nodes. El servei cal arrencar-lo a tots dos nodes a la vegada ja que s'estableix comunicació entre els equips.

```
drbdadm create-md clusterdb
service drbd start
```

A partir d'aquest punt en endavant únicament s'executaran les comandes al node primari. Per tal de formatar el dispositiu i sincronitzar les dades caldrà executar les següents comandes:

```
drbdadm -- --overwrite-data-of-peer primary all
mkfs.ext4 /dev/drbd0
mount /dev/drbd0  /var/lib/mysql
```

Per tal de validar si el dispositiu ha sincronitzat correctament cal monitoritzar el fitxer "/proc/drbd" fent una comanda 'cat' fins que indiqui que els dispositius estan "UpToDate". Una vegada veiem això voldrà dir que els discos poden veure les mateixes dades.

A3. INSTAL·LACIÓ I CONFIGURACIÓ PACEMAKER I COROSYNC

Per instal·lar Corosync i Pacemaker cal executar el següent a tots dos nodes:

```
yum install pacemaker ccs cman pcs resource-agents
```

Una vegada finalitzada la instal·lació cal fer la configuració, aquestes tasques únicament cal executar-les des de un dels nodes ja que el servei de clúster s'encarrega de transferir-les i configurar-les a l'altre node.

```
ccs -f /etc/cluster/cluster.conf --createcluster centreon
ccs -f /etc/cluster/cluster.conf --addnode mortadelo
ccs -f /etc/cluster/cluster.conf --addnode filemon
ccs -f /etc/cluster/cluster.conf --addfencedev pcmk agent=fence_pcmk
ccs -f /etc/cluster/cluster.conf --addmethod pcmk-redirect mortadelo
ccs -f /etc/cluster/cluster.conf --addmethod pcmk-redirect filemon
ccs -f /etc/cluster/cluster.conf --addfenceinst pcmk mortadelo pcmk-redirect port=mortadelo
ccs -f /etc/cluster/cluster.conf --addfenceinst pcmk filemon pcmk-redirect port=filemon
echo "CMAN_QUORUM_TIMEOUT=0" >> /etc/sysconfig/cman
service cman start
service pacemaker start
pcs property set stonith-enabled=false
pcs property set no-quorum-policy=ignore
```

Amb aquestes configuracions afegim cada node al clúster i configurem els ports per defecte, perquè es puguin comunicar de forma estàndard els dos nodes. Posteriorment, com em dit deshabilitem les opcions de Quorum i STONITH.

Des d'aquest punt en endavant ens queda configurar tots els serveis que estaran clusteritzats i de quina manera ho estaran. Per tal de fer la tasca molt més fàcil, hem creat 3 grups. El grup httpd, el qual esta format pel recurs VIP i el servei Apache, el segon grup format per DRBD i MySQL i per últim els serveis de Centreon, aprofitem per configurar l'ordre d'arrencada dels grups en l'ordre que hem indicat, el mateix odre en que hem definit els grups. Afegim primer els serveis de Apache:

```
pcs resource create VirtualIP ocf:heartbeat:IPaddr2 ip=192.168.1.7 cidr_netmask=32 op monitor interval=30s
pcs resource create HTTPD ocf:heartbeat:apache configfile=/etc/httpd/conf/httpd.conf op monitor interval=30s
pcs resource group add group_httpd VirtualIP HTTPD
pcs constraint location group_httpd prefers mortadelo=INFINITY
```

Afegim en segon lloc els serveis de DRBD i MySQL:

```
crm configure
primitive drbd_mysql ocf:linbit:drbd params drbd_resource="clusterdb" op monitor interval="15s" op start timeout="240s"
primitive fs_mysql ocf:heartbeat:Filesystem params device="/dev/drbd0" directory="/var/lib/mysql" fstype="ext4"
ms ms_drbd_mysql drbd_mysql meta master-max="1" master-node-max="1" clone-max="2" clone-node-max="1" notify="true"
primitive mysqld ocf:heartbeat:mysql params binary="/usr/bin/mysqld_safe" config="/etc/my.cnf" user="mysql" group="mysql" log="/var/log/mysqld.log"
```

```
pid="/var/run/mysqld/mysqld.pid"          data-
dir="/var/lib/mysql"   socket="/tmp/mysql.sock"
op monitor interval="60s" timeout="60s" op start
interval="0" timeout="180" op stop interval="0"
timeout="240"
group group_mysql fs_mysql mysqld meta migra-
tion-threshold="5"
colocation   mysql_on_drbd   inf:   group_mysql
ms_drbd_mysql:Master
order mysql_after_drbd inf: ms_drbd_mysql:pro-
mote group_mysql:start
pcs constraint location ms_drbd_mysql prefers
mortadelo=INFINITY
pcs constraint order start group_mysql then
start group_httpd
```

Per últim afegim els serveis de Centreon:

```
crm configure primitive centcore ocf:heart-
beat:anything params user="centreon" bin-
file="/usr/bin/perl"              cmdline_opti-
ons="/usr/share/centreon/bin/centcore        --
logfile=/var/log/centreon/centcore.log --seve-
rity=error --config=/etc/centreon/conf.pm" op
monitor interval="10" timeout="20s" depth="0"
crm configure primitive cbdrrd ocf:heart-
beat:anything params user="centreon-broker" bin-
file="/usr/sbin/cbd" cmdline_options="/etc/cen-
treon-broker/central-rrd.xml"
crm configure primitive cbdbroker ocf:heart-
beat:anything params user="centreon-broker" bin-
file="/usr/sbin/cbd" cmdline_options="/etc/cen-
treon-broker/central-broker.xml"
pcs resource group add group_centreon centcore
cbdrrd cbdbroker
pcs constraint location group_centreon prefers
mortadelo=INFINITY
```

Amb aquesta darrera configuració ja tenim el clúster actiu.

A4. SINCRONITZACIÓ SESSIONS I CONFIGURACIONS

Per tal de fer la copia de sessions i de configuracions ens aprofitem de una eina que porten integrada els sistemes operatius Linux anomenada crontab, aquesta eina permet fer una programació d'execució de tasques. De manera que nosaltres l'aprofitarem per programar la copia cada 5 minuts. Per tal de programar-ho cal afegir les següents línies a crontab.

```
rsync -aq --include 'sess*' --exclude '*' --de-
lete                        /var/lib/php/session/
root@192.168.1.9:/var/lib/php/session/

rsync    -aq    --include    'sess*'    --delete
       /usr/share/centreon/filesGeneration/*
       root@192.168.1.9:/usr/share/centreon/fi-
       lesGeneration/
```