ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DISEÑO E IMPLEMENTACIÓN DEL CLÚSTER DE LINUX PARA ALTA DISPONIBILIDAD EN ALMACENES PYCCA S.A. A TRAVÉS DE UN ENLACE DE RADIOFRECUENCIA DE 5 GHZ”

TRABAJO DE TITULACIÓN

Previo a la obtención del Título de:

MAGISTER EN TELECOMUNICACIONES

GREGORY SAÚL APOLO MARURI

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTOS

Mis más sinceros agradecimientos a Dios y la Virgen María por darme salud y sabiduría para poder continuar mis estudios e ir alcanzando las metas que me propongo en la vida.

A mi Familia quienes me han apoyado y acompañado constantemente en cada una de mis decisiones y me han dado la fortaleza para continuar, experimentando que todo proyecto que uno se proponga se puede alcanzar.

Un especial agradecimiento a mi tutor el Ing. Rayner Durango E., Msig por su paciencia, dedicación y conocimientos invaluables para este proyecto.

DEDICATORIA

El presente proyecto lo dedico a mis padres John y Janeth, motores principales de mi vida quienes me han enseñado la perseverancia, su amor y apoyo incondicional para que pudiese culminar este proyecto.

A Almacenes Pycca S.A. por permitirme crecer en el ámbito profesional brindándome la oportunidad de plasmar día a día mis conocimientos dentro de su infraestructura.

A mis profesores de la tercera promoción de la MET quienes me brindaron sus conocimientos, y son pilares fundamentales para que éste trabajo de titulación pueda desarrollarse exitosamente.

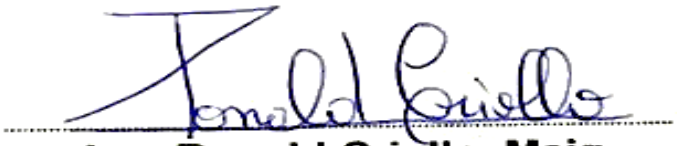
TRIBUNAL DE EVALUACIÓN

Ph.D. César Martín

PRESIDENTE SUBDECANO DE LA FIEC

Ing. Rayner Durango E., Msig

DIRECTOR TRABAJO DE TITULACIÓN

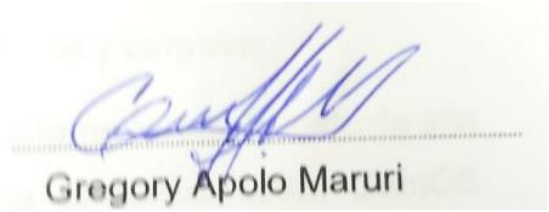


Ing. Ronald Criollo, Msig

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y doy mi consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual".



RESUMEN

El presente proyecto busca resolver el alto riesgo que presenta tener un único servidor principal en la infraestructura de sistemas de la tienda matriz de Almacenes Pycca S.A. Los servicios que dicho servidor provee son los de Motor de base de datos MySQL, servicio de recursos compartidos SAMBA, monitores web de ventas usando Apache; estos servicios son usados por los equipos de punto de venta (POS) y los computadores de uso administrativo y operativo de la tienda. En los cuartos de cómputo de tiendas a nivel nacional, se ha experimentado incidentes de tipo eléctrico que han provocado que fuentes de poder, tarjetas madre, tarjetas de red y discos duros se averían, además de incidentes de software como fallos en el sistema operativo (Kernel Panic), corrupción de los datos de archivos y carpetas.

Se ha recomendado analizar, diseñar e implementar un sistema clúster remoto de alta disponibilidad cuyos nodos trabajarán bajo el sistema operativo Linux CentOS conectados remotamente entre el centro de cómputo principal y el centro de cómputo secundario separados a una distancia de 1.2 km conectados a través de un enlace de Radiofrecuencia punto a punto implementado con Radios Ubiquiti Rocket M5 a una frecuencia de 5 GHz. A pesar que los centros de cómputo se encuentran entre las calles 9 de octubre y Boyacá, y entre las calles Boyacá y Piedrahita respectivamente y con diversos obstáculos en la línea de vista, la versatilidad de dicho enlace logra obtener un ancho de banda de hasta 216 Mbps, escenario óptimo para establecer una comunicación entre los elementos del clúster remoto.

Se realizó un monitoreo exhaustivo de la conmutación de datos, y de la sincronización de la información entre ambos nodos con sus repositorios de almacenamiento, además se realizaron pruebas al clúster alterando manualmente sus elementos para de esa forma evaluar su comportamiento al presentarse un Failover o un Split-Brain, por otro lado se procedió a hacer un Switchover alternando el rol de nodo primario entre los dos nodos para proceder a realizar mantenimientos o actualizaciones a los nodos. Todas las pruebas resultaron exitosas y el clúster provee los servicios sin interrupción.

ÍNDICE GENERAL

CAPÍTULO 1

1. DESCRIPCIÓN DEL PROBLEMA.

En este capítulo se describe la situación actual de la infraestructura de sistemas en las tiendas de Almacenes Pycca S.A., además se expone detalladamente la problemática que se busca solucionar con el presente proyecto, junto con su justificación; adicionalmente se exponen los objetivos específicos y generales del proyecto y la propuesta del esquema de solución.

1.1 Antecedentes.

Almacenes Pycca S.A., es una empresa comercializadora de productos para el hogar, constituida en el mercado ecuatoriano hace más de 60 años. Actualmente cuenta con más de 30 tiendas distribuidas a nivel nacional. [1]

Cada tienda cuenta con varios dispositivos y equipos de cómputo que toman el rol de clientes, a su vez un equipo de cómputo que actúa como Servidor local el cual provee servicio de base de datos MySQL, servicio Web Apache y servicio de archivos compartidos Samba.

Durante los últimos años se han registrado eventos de distinta naturaleza tales como fallas de energía eléctrica, corrupción de la integridad de la información, fallos en almacenamiento de datos, etc., que han provocado que el servidor quede inoperante, logrando así que los servicios que dicho servidor provee estén inaccesibles.

1.2 Planteamiento del problema y escenario de la aplicación.

Por tratarse de una estructura centralizada al momento en que falla el servidor del almacén se ve afectado el funcionamiento de todos los procesos informáticos de la tienda. En ocasiones levantar los servicios que provee el servidor principal toma minutos, horas e incluso días.

En casos más extremos ha sido necesario enviar personal especializado de sistemas a reparar el servidor o configurar un nuevo equipo para suplir el servidor averiado.

Los tiempos de una posible inactividad muchas veces son elevados, provocando deficiencias en el servicio al cliente, que acarrean pérdidas económicas para Almacenes Pycca S.A.

A continuación se muestra en la Tabla 1 una comparación que describe el tiempo aproximado que toma solucionar los distintos tipos de fallos informáticos, dependiendo en que región del Ecuador se encuentra la tienda.

Localidad / Avería	Guayaquil	Quito	Provincias Costa	Provincias Sierra
Disco principal	4h	5h	7h	9h
Disco secundario	3h	4h	6h	8h
Tarjeta Madre	5h	6h	7h	9h
Fuente de Poder	3h	4h	6h	8h
Tarjeta de Red	5h	6h	7h	9h

Tabla 1: Fallo vs Tiempo de Solución

1.2.1 Esquema de infraestructura computacional actual.

La tienda Matriz de Almacenes Pycca S.A. ubicada en la ciudad de Guayaquil entre las calles Boyacá y 9 de Octubre [1], cuenta con una infraestructura computacional homogénea con todas las tiendas de la empresa, la cual dispone de un equipo servidor principal con sistema operativo Linux CentOS 6.7 de 64 Bits, equipos de comunicación switches LAN, un router principal provisto por el proveedor de enlace de datos de última milla, siendo este mismo configurado con el rol de ser el gateway de toda la subnet del almacén; un promedio de 4 computadoras que toman el rol de puntos de venta (POS).

Los puntos de venta están configurados con el sistema operativo Linux CentOS 6.2 de 32 Bits donde se configura el sistema de facturación llamada POS 3 desarrollado por nuestro personal de desarrollo en el departamento de sistemas.

También contamos que equipos de cómputo que juegan el rol de PCs administrativas y operativas, las mismas que son utilizadas por el Gerente, Secretaria y Sub-Administradora, personal de bodega y servicio al cliente de la tienda, estas computadoras tienen instalado el sistema operativo Windows 7 de 32 Bits y permanentemente están conectados a los servicios que provee el servidor principal del Almacén.

1.2.2 Exposición detallada del problema actual.

A nivel de Hardware los servidores principales cuentan con dos discos de almacenamiento, el primero aloja el Sistema Operativo Linux CentOS 6.7 de 64 Bits y los archivos binarios de los servicios de Samba, Apache y MySQL, este es un disco de estado sólido (SSD) de 240 GB de capacidad y su dimensión es de 2.5”, en el segundo disco se alojan los datos compartidos a los que los equipos cliente acceden a través del protocolo SMB(Samba); es un disco rígido metálico de 1 TB de capacidad y su dimensión es de 3.5’’.

Estos equipos se encuentran protegidos en gabinetes metálicos que ofrecen seguridad de acceso físico, estos gabinetes son llamados rack de servidores, gracias a este esquema de implementación el equipo servidor recibe poca manipulación humana; por la repentina variación de voltaje de energía eléctrica que suele presentarse en las tiendas, hemos agregado mayor protección a esta infraestructura con supresores de pico y fuentes de poder ininterrumpida (UPS); pero a pesar de estas protecciones, estos inconvenientes han provocado que los servidores se vayan deteriorando, afectando así los discos duros, fuente de poder y placa base.

En ciertas ocasiones esto ha provocado que el servidor se encuentre en un estado de inactividad por lapsos extensos de tiempo, en otras ocasiones han provocados daños permanentes e incluso hemos registrado pérdida de datos críticos tanto de configuraciones de los equipos como de información transaccional y operativa de los clientes.

Se han tomado medidas como respaldar la información cada cierto tiempo, ya sea en un disco externo o a su vez en un recurso compartido de red [2]. Este mecanismo solventa en cierto porcentaje como una solución tras sufrir un fallo en el sistema informático, la desventaja de este mecanismo es el tiempo que toma la restauración de la información y de los servicios que ofrece el servidor, ya que mientras mayor es la cantidad de información a restaurar, mayor es el tiempo que toma dejar operativo el servidor, se han registrado restauraciones de equipos servidor que han durado desde unas horas hasta un día.

Respecto a la seguridad del sistema, también se ha tomado en cuenta que el contar con un único servidor principal en la infraestructura crea asimismo un único punto de fallo, siendo una vulnerabilidad bastante crítica, incluso podría ser considerado un objetivo de ataques tipo de denegación de servicio (DoS), o de incluso un ataque tipo MySQL Injection.

1.3 Justificación.

El presente proyecto busca fortalecer la infraestructura de las tiendas de Almacenes Pycca S. A., evitando que sea un blanco para ataques cibernéticos, que dejen inoperativo al servidor principal, o que deje de proveer los servicios computacionales debido a daños físicos o lógicos.

Luego de analizar un muestreo de las ventas por hora de todas las tiendas, tomamos como muestra a la Matriz en Guayaquil, considerada la tienda de mayor ingreso en ventas.

Una hora sin sistema en la tienda matriz en un mes de alto número de transacciones como es diciembre tendría un costo de pérdida de aproximadamente entre $4,000 a $5,000 USD; la información contable detallada la podrá encontrar en el Anexo A1.

La Tabla 2 muestra un resumen de las ventas por hora, registradas el día lunes 22 de diciembre del 2014 en la Tienda Matriz de Pycca.

Almacén Matriz Centro		
Hora	**Total por Hora**	**Total Acumulado**
10:00	$1,968	$1,968
11:00	$6,197	$8,165
12:00	$9,243	$17,408
13:00	$8,251	$25,659
14:00	$8,885	$34,544
15:00	$9,425	$43,969
16:00	$11,844	$55,813
17:00	$12,285	$68,098
18:00	$16,410	$84,508
19:00	$17,329	$101,837
20:00	$19,545	$121,382
21:00	$12,642	$134,024
22:00	$6,974	$140,998
23:00	$347	***$141,345***

Tabla 2: Tabla Ventas por Hora

La misma tienda en un mes de mediano número de transacciones como el mes de Julio, el ingreso económico por hora es aproximadamente del 50% menos.

El alcance de estas fallas en el servidor han llegado a intervenir incluso en el ámbito de gestión de operaciones en servicios al cliente. Existen costos que no pueden verse reflejados directamente en unidades monetarias.

Pero los procesos que no pueden ser realizados durante estas horas de inactividad dan como resultado ventas que no llegan a concretarse, créditos que no pueden otorgarse a personas que son clientes potenciales, e incluso la atención a clientes que buscan la solución de algún reclamo o devolución de productos se ve interrumpida.

La Tabla 3 muestra el número de atenciones a usuarios recibidas la primera semana de diciembre del 2014.

Alm. Matriz	**Total**	**8h – 13h**	**13h – 18h**	**18h – 22h**
01-DIC	562	147	249	166
02-DIC	587	111	296	180
03-DIC	469	27	315	127
04-DIC	603	166	298	139
05-DIC	424	130	176	118
06-DIC	484	121	268	95
07-DIC	463	68	299	96
Total Semanal	**3592**			

Tabla 3: Atención a Usuarios por Hora

Mediante el presente proyecto se aspira lograr los siguientes resultados:

- Contar con una infraestructura más robusta y con redundancia de información en dos equipos diferentes en la tienda matriz de Pycca S.A., ayudando así a garantizar la alta disponibilidad de los servicios provistos por el servidor principal en caso de presentarse una falla técnica o ataque cibernético en dicho equipo.
- Minimizar el nivel de vulnerabilidad con la que actualmente cuenta la infraestructura de cómputo en las tiendas de Almacenes Pycca S.A. Debido a que cuenta con tan sólo un servidor en la tienda, lo que representa un único punto de fallo, capaz de provocar que una tienda ralentice sus actividades o en ciertos casos las paralice, al momento de presentarse una falla técnica o un ataque cibernético.
- Conservar óptimos niveles de atención al cliente, al momento de que exista una falla en el servidor principal, evitando se presenten retrasos en tiempos de atención al cliente, y además precaver que puedan realizarse todas las operaciones que el cliente necesite al momento de solicitar asistencia en la ventanilla de servicios.
- Disponer a Almacenes Pycca S.A. de una solución que pueda desplegarse en todas sus tiendas a nivel nacional, fortaleciendo de esa manera su infraestructura de cómputo, garantizando la continuidad de los servicios informáticos.

1.4 Modelo propuesto para la solución del problema.

Para poder reducir los tiempos de falta de disponibilidad de los servicios que provee el servidor principal de las tiendas, se va a implementar el proyecto de clúster de servidores remotos con sistemas operativos Linux, con el cual se desea proveer una alta disponibilidad del servicio de MySQL, con el fin de ofrecer ininterrumpidamente el servicio de base de datos para las cajas y así reducir el impacto negativo que se obtiene actualmente al momento de presentarse una falla en el servidor primario.

En base a los conocimientos adquiridos en las materias dictadas en la Maestría de Telecomunicaciones, resaltando las materias de Seguridad en Redes y Sistemas, Redes de Datos y Enlaces de Radiofrecuencia; han motivado a proponer el presente trabajo de titulación en busca de diseñar e implementar una solución a la problemática presentada en las tiendas de Almacenes Pycca.

La documentación se la desarrollará siguiendo los lineamientos aprendidos en la materia de Métodos de Investigación Científica.

En una vista macro de la metodología a utilizarse en el presente proyecto se puede detallar que se llevarán a cabo los siguientes procesos:

- Descripción de conceptos básicos del Clúster de Linux y los componentes que se utilizarán dentro de la empresa.
- Diseño de la infraestructura de sistemas del proyecto a ser implementado, detallando los equipos y las interconexiones de redes.
- Dimensionamiento detallado del alcance a cubrir del proyecto, considerando el despliegue principal en la matriz de Pycca y en las 5 tiendas más importantes de Pycca.
- Detalles del despliegue técnico en la implementación del proyecto, detallando todos los recursos tecnológicos a usar, tanto en software y hardware.
- Documentación del Linux Clúster junto con sus matrices de pruebas, etapas de puesta en producción y registros de los resultados.
- Descripción del enlace de radiofrecuencia que se implementará para la conectividad de los centros de cómputos remotos.

En el presente proyecto se usará un clúster de tipo alta disponibilidad (High Availability Cluster), ya que se busca proveer continuamente los recursos de servicio de Bases de Datos MySQL, de las carpetas compartidas Samba y de los WebServices de Apache, en el caso que el nodo principal se vuelve inoperativo luego de un ataque cibernético o una falla en el hardware.

Dicho clúster estará configurado entre los sitios remotos centro de cómputo principal y centro de cómputo secundario, ubicados a 1.2 km de distancia, en las calles Boyacá y 9 de Octubre el Principal y el Secundario en Escobedo entre Montalvo y Padre Aguirre; conectados entre sí por medio de un enlace de radiofrecuencia, usando radios Ubiquiti Nanostation M5 a una banda de 5 GHz.

El alcance que tiene el presente proyecto, es el diseño, la implementación y la evaluación de un clúster para sistemas operativos Linux en el almacén matriz principal de Pycca S.A. y proponer la implementación de clúster de Linux en las 5 tiendas más importantes a nivel nacional.

Entre los elementos diferenciadores a ser implementados en el presente proyecto de titulación, podemos destacar el uso de una red LAN de velocidad de 10 Gbps en cobre, en la redes de Clientes, Servidores e iSCSI para los almacenamiento de datos. Para lograr esto se utilizarán switches Netgear de capa 3 de velocidad de 10 Gbps y cableado de Cobre Categoría 7a.

A nivel de sistema operativo, se implementará el Clúster bajo una arquitectura de 64 bits en Linux y un Kernel 2.6.32 bajo la distribución de CentOS versión 6.7.

Para la configuración del sistema de alta disponibilidad se utilizará el conjunto de programas (STACK) de administración y configuración de clúster, conformado por Corosync, CMAN y Pacemaker; una vez implementados ofrecen excelente control y supervisión de la operatividad del clúster.

En cuanto almacenamiento de datos se refiere, se utilizará dos equipos NAS de la Marca Synology modelo DS2015xs, estos equipos estarán conectados a una red de alta velocidad de 10 Gbps, para que a través del protocolo ISCSI puedan proveer discos virtuales (LUNs) a los servidores miembros del clúster. Además tendrán una conexión de red directa entre ellos, lo cual nos permite crear una replicación directa de la información entre los NAS, esta protección adicional nos brinda una contingencia de una perdida de información ante la presencia de fallos en los discos duros de cualquiera de los dos dispositivos.

La sincronización de las tablas y bases de datos entre los nodos del clúster se realiza usando una plataforma de replicación llamada Replicación de Dispositivos de Bloque (DRBD), la cual nos ayuda a certificar que los datos están 100% replicados entre los nodos del clúster.

Cuando en el mercado se habla de soluciones de clúster para centros de cómputo suele detallarse soluciones integrales bajo una marca o empresa.

Por citar un ejemplo en HP se ofrece un producto HP Cluster Platform 3000, un clúster en el que todos los elementos que lo componen son de la misma marca, desde los nodos hasta las interconexiones de red, y los repositorios de almacenamiento; una solución muy buena y certificada, pero sus costos son muy elevados.

El presente proyecto busca convertirse en una solución de tipo heterogénea, con la finalidad de integrar equipos y elementos de distintas marcas y modelos, buscando que el costo de la solución sea bajo y no crear ataduras respecto a que los elementos sean de una marca y modelo específicos, a su vez se configura una arquitectura abierta a múltiples marcas y modelos en hardware y en software.

1.5 Objetivos del proyecto.

Tomando en consideración que Almacenes Pycca S.A. es una empresa que cuenta con una infraestructura de sistemas que va a la vanguardia de la tecnología, para este proyecto contaremos con equipos bastante robustos para el rol de nodos del clúster, así también como equipos de redes de datos de velocidades de 10 Gbps.

El alcance de este proyecto es poder brindar una redundancia de equipos y servicios a la tienda matriz de Almacenes Pycca S.A., y a su vez proponer el despliegue de la solución a las 5 tiendas más importantes que tiene la cadena.

Teniendo en cuenta lo expuesto, y luego de detallar la problemática que está cursando la empresa, el presente proyecto busca como objetivo principal:

- Reducir los tiempos de inactividad de los servicios que provee el servidor principal en las tiendas de Almacenes Pycca S.A., al momento de presentarse una falla técnica o un ataque cibernético.

Los objetivos específicos que planteamos en el presente proyecto son los siguientes:

- Reducir los tiempos de ausencia de los servicios tecnológicos al momento de presentarse una falla o ataque cibernético en el nodo principal del clúster en Almacenes Pycca S.A.
- Crear un proceso de redundancia de la información almacenada en el nodo principal sincronizada en línea entre los repositorios de almacenamiento de ambos nodos.
- Proponer la distribución progresiva de equipos físicos de redundancia en las 5 tiendas más importantes a nivel nacional de Almacenes Pycca S.A., para que en un periodo de 12 meses se ejecute la creación de Linux Clúster en cada una de esas sucursales.
- Sugerir a Pycca S.A. la política de despliegue de redundancia de servidores aplicando Clústeres para Sistemas Operativos Linux, en la apertura de nuevos almacenes de tipo Almacén Senior.
- Demostrar con indicadores obtenidos en los registros del clúster, el desempeño del presente proyecto basado en tiempos de “uptime” de los servicios provistos por el Clúster de Linux en Almacenes Pycca S.A.

CAPÍTULO 2

2. MARCO TEÓRICO.

A continuación se describe los conceptos estudiados para la realización del presente proyecto, toda la metodología de Clúster y sus elementos, estructuras y conectividad, los servicios que el servidor principal provee y los equipos clientes quienes utilizan estos servicios.

Además se describe el concepto y recursos que utiliza el clúster entre sitios remotos, en el cual se describe la estructura de radiofrecuencia utilizada y la sincronización de los datos entre sitios remotos.

2.1 Definición del Clúster de Linux.

Un clúster de computadoras o clúster computacional consta de una agrupación de dos o más computadoras, que siendo administrados bajo un software trabajan en conjunto para realizar una tarea [3].

Los clúster son desarrollados e implementados en busca de cumplir dos grandes objetivos que son mejorar el desempeño de procesamiento y la disponibilidad de los servicios [4].

2.2 Elementos de un sistema Clúster de Linux.

Los computadores usados dentro de un clúster de cómputo son llamados Nodos y regularmente los clúster están conformados con Nodos homogéneos respecto a su hardware y software interconectados entre ellos a través de redes de alta velocidad LAN y siempre uno de los nodos actuando como servidor principal quien administra los procesos que deberán ejecutar los nodos restantes.

2.3 Tipos de Clúster de Linux.

Los clústeres desplegados en sistemas operativos Linux se pueden clasificar en cuatro diferentes tipos: [3]

- Clúster de almacenamiento. [3]
- Clúster de alta disponibilidad. [3]
- Clúster de balanceo de carga. [3]
- Clúster de alto desempeño. [3]

En ciertos proyectos de diferentes ámbitos se han usado una combinación de tecnologías de clúster para obtener el resultado del proyecto. [3]

A continuación brindaré una breve descripción de cada uno de los tipos de clúster.

Clúster de Almacenamiento

Este tipo de clúster simplifica la administración de almacenamiento para un sistema de archivos compartidos.

Todos los nodos del clúster usan un único almacén de datos pudiendo escribir y leer el contenido en todo momento.

Con este tipo de clúster dejamos de necesitar las copias redundantes de datos de aplicaciones y nos simplifica la recuperación de respaldos de información y recuperación de desastres. [3]

Clúster de Alta Disponibilidad

Este tipo de clúster busca proporcionar una disponibilidad continua de los servicios que provee el clúster, logra hacerlo eliminando los puntos únicos de fallo y migrando los servicios del clúster que se vuelve inoperativo hacia otro nodo que esté operativo.

El clúster de alta disponibilidad siempre responde como un solo servidor para los clientes, manteniendo la integridad de los datos, por lo tanto uno de los miembros siempre tiene el control sobre los otros miembros del clúster.

Los clústeres de alta disponibilidad también son conocidos como clúster de conmutación por error (Failover Cluster). [3]

Clúster de Balanceo de Carga

Este tipo de clúster usa los nodos del clúster para equilibrar la carga de los requerimientos, lo realiza enviando paralelamente peticiones de servicios entre todos los nodos.

Una vez que un nodo se vuelve inoperativo y no puede seguir procesando requerimientos el clúster distribuye toma la carga de solicitudes destinadas a dicho nodo y las distribuye equitativamente a los otros nodos del clúster.

Esta solución de clúster es muy conveniente si al pasar el tiempo se desea escalar de desempeño, a mayor carga se incrementan los nodos. [3]

Clúster de Alto Rendimiento

Este tipo de clúster utiliza simultáneamente todos los nodos del clúster para realizar cálculos y que las aplicaciones trabajen en paralelo mejorando así el desempeño de las aplicaciones y servicios que ofrece el clúster.

Los clúster de alto desempeño también son conocidos como clúster computacionales o grid computing.

En el proyecto de Diseño e Implementación del Clúster de Linux para Alta Disponibilidad en Almacenes Pycca S.A. a través de un enlace de radiofrecuencia de 5 GHz se usará el tipo de clúster de alta disponibilidad, ya que se busca proveer la continua disponibilidad el servicio de Bases de Datos MySQL a pesar de que un nodo se vuelve inoperativo luego de un ataque cibernético o una falla en el hardware. [3]

2.4 Configuración de un sistema Clúster de Linux.

Los sistemas clúster de alta disponibilidad permiten que los servicios computacionales se encuentren siempre disponibles para los requerimientos de clientes incluso en caso de presentarse un fallo, dado que las solicitudes se direccionan automáticamente al nodo que se encuentre activo y listo para procesar las solicitudes.

Por estas características el presente proyecto implementará un clúster de alta disponibilidad.

La primera función del clúster de alta disponibilidad es comunicar entre sí a los nodos, monitorizando continuamente su estado y detectando fallos. Para poder realizar aquello es habitual usar un canal específico para la comunicación, la cual puede ser una red IP independiente o una conexión serie, de manera que la misma no se vea afectada por problemas de seguridad o rendimiento. Además utiliza una técnica llamada Heartbeat.

La segunda función es administrar los servicios ofrecidos por el clúster, teniendo la capacidad de migrar dichos servicios entre diferentes servidores como respuesta a un fallo.

Para llevar a cabo esta función es necesario realizar seguimientos a nivel de recursos o servicios y detectar el fallo de los mismos, donde el Administrador será quien configure la periodicidad del monitoreo y las acciones que se deberán llevar a cabo. Este proceso se conoce como Monitoreo de Recursos. Cabe recalcar que el término recurso en este contexto se aplica a cualquier componente físico o lógico, administrable en un clúster y que solo se puede alojar en un nodo a la vez, el cual o los cuales son provistos a los servicios para que realicen una tarea específica.

El administrador también podrá definir la preferencia de nodos, la cual ayuda a distribuir los servicios entre los diferentes servidores de acuerdo al hardware y según interese para obtener el resultado ideal del clúster. En caso de presentarse un fallo los servicios pueden ser migrados de inmediato al siguiente nodo disponible o incluso intentar levantarlo en el mismo nodo principal.

El tiempo de inactividad por el posible fallo es mínimo y el clúster continuará proporcionando el correspondiente servicio.

En el caso de que un nodo del clúster esté funcionando de manera incorrecta, el clúster hará uso del Fencing.

También se procederá a configurar el mecanismo llamado Quórum, el cual sirve como testigo para poder comprobar el estado de todos los nodos que componen el Clúster en todo momento y ayuda a determinar cuál es el nodo activo y el nodo pasivo.

Entre las soluciones disponibles para la implementación y administración de clúster, encontramos un stack (agrupación) de tres aplicaciones llamadas Pacemaker, CMAN y Corosync. Las cuales se encargan de supervisar el estado de cada uno de los miembros del clúster, de la transmisión de mensajes de estado entre los miembros y de las operaciones del clúster respectivamente. Gracias a su versatilidad, esta agrupación será utilizada para la implementación del presente proyecto.

Heartbeat. Actualmente se conoce con este nombre a la capa de mensajería de clúster. Sin embargo, hasta la versión 2.1.4 comprendió las funcionalidades de administrador de recursos locales, infraestructura “plumbing”, STONITH, agentes de recursos y administrador de recursos de clúster, actualmente desarrollado de manera independiente bajo el nombre de Pacemaker. Es un demonio que provee los servicios de infraestructura de clúster a sus clientes, los cuales son comunicación y membresía. Necesita combinarse con un administrador de recursos de clúster (CRM) para mantener alta disponibilidad. Pacemaker es el CRM preferido para clústeres que se basan en Heartbeat. [4]

Corosync Clúster Engine. Es un sistema de comunicación de grupo con características adicionales que permiten implementar alta disponibilidad dentro de las aplicaciones. Se derivó del proyecto OpenAIS y está bajo la licencia New BSD. [4]

Entre las características que ofrece se puede mencionar un modelo de comunicación de grupo con garantías de sincronización virtual que permite replicar el estado de las máquinas, un administrador de disponibilidad simple que reinicia los procesos de las aplicaciones en caso de fallo, configuración y estadísticas de base de datos en memoria que proporcionan la capacidad de establecer, recuperar, y recibir notificaciones de cambio de información y por último un sistema de quorum que notifica a las aplicaciones cuando el quórum se ha logrado o se ha perdido. [4]

CMAN. Es un administrador de clúster basado en el núcleo, que se distribuye a todos los nodos. Consta de dos partes. La primera de ellas se encarga de administrar la conexión y maneja la membresía, mensajería, quórum, notificaciones de evento y transiciones. La segunda parte maneja los grupos de servicios. Si un nodo no transmite un mensaje durante un tiempo preestablecido, CMAN lo removerá del clúster e informará lo sucedido a los otros componentes de la Infraestructura de clúster para que realicen las acciones necesarias. También mantiene un registro del quórum del clúster mediante el control de la cuenta de los nodos. Si más de la mitad de los nodos están activos el clúster tiene quórum, pero si tan solo la mitad o menos de la mitad están activos, el clúster no tiene quórum y la actividad se detendrá. [5]

Pacemaker. Es un software de código abierto que administra los recursos del clúster. Fue desarrollado a partir del 2004, por Red Hat y Novell, y recibe además apoyo de Linbit y la comunidad open source en general. Soporta varios stack de mensajería como Heartbeat, Corosync y CMAN y además varios escenarios de implementación, desde clústeres de 2 nodos hasta configuraciones de clústeres de 16 nodos. Supervisa además el sistema para manejar fallos tanto de hardware como de software, y en el caso que se llegue a dar algún fallo recuperará automáticamente la aplicación en una de las máquinas restantes del clúster, mediante algoritmos avanzados que determinarán cuál es el lugar más apropiado. [5]

El formato de configuración interna de Pacemaker es XML, el cual es ideal para las máquinas pero poco comprensible para los seres humanos. Debido a esto, desarrolladores de la comunidad han creado interfaces gráficas e interfaces de línea de comando que permitan la configuración del clúster sin tener que usar de manera directa XML. [4]

2.5 Servicio MySQL en Linux.

MySQL es un sistema de código abierto, multihilo y multiusuario que administra bases de datos relacionales, también llamados RDBMS por sus siglas en inglés Relational DataBase Management System.

Gracias a su característica de ser Multihilo puede procesar varias consultas en paralelo y por ser Multiusuario puede ser usado al mismo tiempo por varias personas u otros sistemas de cómputo. A diferencia de otros modelos como Jerárquico y de Red, el modelo Relacional usado por MySQL almacena todos los datos en relaciones, y como cada relación es un conjunto de datos, el orden en el que estos se almacenen no tiene relevancia, eso ofrece un gran beneficio para los usuarios ya que se vuelve más fácil de entender y usar.

Existen muchos tipos de bases de datos, desde un simple archivo hasta sistemas relacionales orientados a objetos. MySQL utiliza múltiples tablas para almacenar y organizar la información. MySQL fue escrito en C y C++ y se destaca por su amplia adaptación a diferentes entornos de desarrollo, permitiendo su interacción con los lenguajes de programación más utilizados como PHP, Perl y Java además su integración con los sistemas operativos más importantes del mercado Windows, Linux y Mac.

También es muy destacable, la condición de open source de MySQL, que hace que su utilización sea gratuita e incluso se pueda modificar con total libertad, pudiendo descargar su código fuente. Esto ha favorecido en su desarrollo y continuas actualizaciones y mejoras para hacer de MySQL una de las herramientas más utilizadas por los programadores orientados a Internet.

2.5.1 Ataques a MySQL.

Existen varios tipos de ataques con los que es posible dejar inoperativo a un sistema de bases de datos MySQL, a continuación estudiaremos tres de los más comunes:

- Ataque de Fuerza Bruta
- MySQL Injection
- DoS MySQL

El objetivo de los ataques MySQL Injection y Fuerza Bruta es el obtener las credenciales de usuarios que puedan ser autenticados en la base de datos y con dichos usuarios poder realizar modificaciones a los datos que el sistema de bases de datos MySQL contiene, la diferencia de ambos radica en la manera como lo realizan. En cambio el ataque de tipo DoS MySQL busca lograr que el Servidor sea incapaz de continuar brindando el servicio de base de datos a los clientes que envían requerimientos de consultas a las Bases de Datos.

Ataque de Fuerza Bruta

Este ataque se caracteriza por hacer uso de la vulnerabilidad que representa que un servidor tenga configurado el Puerto de MySQL abierto a peticiones, nos referimos al comúnmente conocido puerto 3306. Usando herramientas como MEDUSA, un programa que puede ser encontrado fácilmente en la red o también incluido en la suite de Hacking llamado Backtrack o Kali, esta herramienta va a realizar una conexión al puerto 3306 con parámetros que el atacante configure, por ejemplo en la siguiente línea estamos conectándonos al puerto 3306 de un host (192.168.0.111) en el cual previamente verificamos que tiene el puerto abierto.

Definiendo que el usuario será ROOT (el superusuario de Linux) y las claves a probar serán tomadas de un listado de palabras almacenadas en un archivo de texto llamado easy-passwords.txt.

#medusa –h 192.168.0.111:3306 –u root –P /root/Desktop/easy-passwords.txt –M MySQL –f –b

Con esta línea el programa MEDUSA realizará la prueba de conexión hasta que todas las palabras contenidas en el diccionario hayan sido probadas. En caso de que la clave del usuario ROOT coincida con una de las palabras guardadas en el archivo se mostrará en pantalla algo similar al siguiente mensaje:

ACCOUNT FOUND: [MySQL] Host: 192.168.0.111 User: root Password: abc123 [SUCCESS]

De esa forma el atacante podrá ingresar a un Sistema de base de datos MySQL con una autenticación positiva y podrá hacer uso de los datos que contiene el servidor.

MySQL Injection

La inyección de MySQL es la técnica usada por usuarios maliciosos con la que pueden inyectar comandos o sentencias de tipo SQL a través de un entrada de página web, estos comandos SQL inyectados pueden alterar la integridad de las bases de datos e incluso poner en peligro la seguridad de una aplicación web.

Por citar el siguiente ejemplo, en una página web realiza una solicitud a la base de datos y ésta es modificada con una sentencia SQL:

txtUserId = getRequestString("UserId");

*txtSQL = " SELECT * FROM Users WHERE UserId = 105 or 1=1" + txtUserId;*

En dicha sentencia existe un comodín que es siempre Verdadero ‘1=1’ lo cual extraerá todas las filas de una tabla.

Existen ataques más peligrosos en los que podrían incluir un DROP TABLE en la sentencia lo cual eliminaría una tabla y esto provocaría pérdida de información importante del sistema de base de datos.

DoS MySQL

Ataque de denegación de servicio de MySQL, existen muchos factores por los cuales pueden desencadenar una negación al servicio MySQL como un exceso de conexiones, un alto uso del servicio, un MySQL no optimizado, un ataque concurrente externo de DoS, una explotación (xploit) exitosa podría permitir a los usuarios provocar una denegación de servicio colgando para siempre un proceso de escucha en el socket (host:puerto) y que no haga nada más con lo cual todos los demás clientes no serán capaces de emitir consultas en tablas y futuros clientes que soliciten una base de datos de conexión no serán capaces de conectarse.

2.5.2 Protecciones de MySQL.

En este subcapítulo describiremos las soluciones que serán implementadas en este proyecto en busca de proteger el Clúster de Alta Disponibilidad para el Servicio de Bases de Datos MySQL de las amenazas expuestas en el subcapítulo anterior.

Protección para ataques de Fuerza Bruta

En el presente proyecto se ha considerado proteger del ataque restringiendo por direccionamiento IP las estaciones cliente que tienen permitido conexiones hacia el servidor, no se usará el parámetro ‘%’ el cual permitirá que el servidor pueda recibir conexiones desde cualquier equipo con cualquier dirección IP.

Se registrarán las direcciones IP o el rango de equipos permitidos a conectarse en el sistema de base de datos. Adicionalmente se configura el parámetro max_user_connections de MySQL con valor de 3, permitiendo así un máximo de 3 conexiones por usuario o por IP, de esta manera un ataque de fuerza bruta no tendría efecto.

Protección para ataques de MySQL Injection

Considerando que estos ataques son para la obtención de información o actualización de información enviando consultas directamente al servicio de base de datos MySQL implementaremos un módulo bastante robusto llamado MySQL Firewall, con el cual nos brinda la posibilidad de monitorear, alertar y bloquear las actividades de las bases de datos que no estén autorizadas, estas pueden ser SELECT dirigidos a las tablas de usuarios de MySQL, con los cuales podrían obtener las credenciales de usuarios autorizados.

Por otro lado como este ataque es muy común recibirlo vía Web, se va a sugerir como requerimiento al departamento de desarrollo que las páginas webs transaccionales que conlleven a realizar algún tipo de conexión a MySQL sean revisadas y en los casos necesarios reescribir el código para que el mismo servicio Apache interpretando el código escrito no pueda procesar una sentencia SQL escrita por un usuario en la barra de direcciones como parámetro de la página web.

Protección para ataques de DoS MySQL

Para proteger el sistema de base de datos MySQL del clúster propuesto en este proyecto de un ataque de denegación de servicio se ha instalado y configurado un programa llamado Fail2Ban, este programa nos da la posibilidad de alertar de una actividad sospechosa y de poder bloquear automáticamente los requerimientos provenientes de una dirección IP específica con parámetros muy específicos.

Este programa constantemente está leyendo los Registros (Logs) del Sistema Operativo y al verificar que una dirección IP solicita una alta concurrencia de conexiones en una fracción de tiempo muy corta él automáticamente agrega dicha dirección IP en su Lista Negra (Blacklist) y a partir de ese momento toda petición que provenga de esa IP simplemente será rechazada a nivel de Sistema Operativo de tal manera tal requerimiento no pasará a ocupar un recurso del servidor de base de datos MySQL.

Adicionalmente se procederá a sugerir al Área de TI de Almacenes Pycca S.A. que en el Firewall de Red perimetral se agregue protección adicional para evitar estos ataques en caso de ser necesarios.

2.6 Servicio Apache en Linux.

Apache es un servidor web de código abierto bajo licencia GPL el cual implementa el protocolo HTTP para la creación de páginas web y de servicios web, es multiplataforma por lo que puede ser implementado en plataformas Mac, Windows y Unix (Linux, BSD, etc.).

Es el Servidor Web más utilizado a nivel mundial, muy robusto y destacado por su rendimiento, cuenta con soporte de seguridad SSL y TLS (HTTPS), puede realizar autenticación de datos usando SGDB, brinda soporte para los lenguajes de desarrollo web más comunes como Perl, PhP, Python y TCL.

Un servidor web está diseñado para transferir datos de hipertexto, es decir, páginas web estáticas o dinámicas con todos sus elementos (textos, widgets, banners, imágenes, etc.). Su tarea principal es la de procesar las peticiones de páginas web o de servicios web solicitadas al servidor y gestionar su entrega o denegación de acuerdo a políticas de seguridad.

Su desarrollo comenzó en 1995 basado en el código NCSA HTTPd 1.3, jugó un papel fundamental en el desarrollo de la World Wide Web. En la actualidad el servidor web Apache es desarrollado dentro del proyecto HTTP Server (httpd) de la Apache Software Foundation.

Las funcionalidades que debe cumplir son las de atender eficientemente la concurrencia de peticiones web solicitadas al servidor, controlar los errores de recursos no encontrados (Error 404), registrar todo la gestión del servidor web, inscribiendo peticiones recibidas, peticiones rechazadas y errores del servidor web y una de las características más importantes es la de poder configurar un Hosting Virtual basado en IPs o en nombres.

2.6.1 Ataques a Apache.

Ataques DoS

DoS o Denial of Service (Denegación de Servicio), Es un ataque a un sistema de servidores o red que causa que un servicio o recurso sea inaccesible a usuarios legítimos. Los ataques DoS obstruyen las comunicaciones entre los usuarios y el servidor afectado, impidiendo que continúen funcionando los servicios.

El flujo masivo de peticiones a través del protocolo TCP/IP al servidor y los ataques de fuerza bruta provocan el colapso de la red, o la saturación del servidor en cuestión.

Un método de ataque común consiste en la saturación del equipo al cual se apunta con solicitudes de comunicaciones externas, de modo que ese equipo no pueda responder al tráfico legítimo o lo haga lentamente y se presente como efectivamente no disponible.

Tales ataques usualmente conducen a una sobrecarga del servidor. Los equipos expuestos a ellos suelen necesitar el reinicio para poder funcionar de manera correcta nuevamente.

Los objetivos de los ataques DoS son los servidores web y su propósito consiste en que no se encuentren disponibles para los usuarios durante un período determinado.

DNS Poisoning

Este tipo de ataque busca tener la oportunidad de poder inyectar nombres de tipo DNS falsos en el cache del DNS de tu servidor.

Logrando así poder pasar por legitima y autentica cualquier información falsa, los usuarios que intentan acceder a los sitios web envenenados podrían descargar virus o gusanos en lugar del contenido que originalmente estuvo alojado.

Lo realizan basándose en una vulnerabilidad encontrada en el servidor o a través de servidores poco confiables, alojando así en el caché DNS por un cierto período de tiempo estos falsos registros y permitiendo a los atacantes escribir respuestas DNS de dirección IP solicitadas.

Ataque Slowloris

El ataque Slowloris se basa en un programa que permite que un único computador pueda dejar inoperativo el Servidor Web de un servidor remoto.

Este programa intenta realizar varias conexiones hacia el servidor web del servidor al cual se desea dejar inoperativo y las dichas conexiones las mantiene abiertas el tiempo que le sea posible mantenerlas, usa un mínimo de ancho de banda ya que envía una petición parcial y periódicamente, envía peticiones agregando cabeceras HTTP incompletas lo cual no concluye la petición. Por consiguiente el Servidor Web Apache mantendrá estas conexiones abiertas llenando su pool de conexiones concurrentes.

Esto provoca que eventualmente deniegue conexiones adicionales de clientes legítimos, liberar conexiones auténticas, retornar respuestas de tiempo agotado y por último llegar a encontrarse inoperativo.

2.6.2 Robustecimiento de Apache.

En el siguiente subcapítulo estudiaremos las soluciones que van a ser implementadas en el proyecto de Clúster Linux para Almacenes Pycca S.A. con el fin de mitigar los posibles ataques al que está expuesto el Servidor Apache descritas en el subcapítulo anterior.

Protección de Apache para ataques de DoS

Con el objetivo de evitar ataques de tipo DoS contra nuestro sistema Clúster Linux vamos a activar un módulo importante de Apache llamado mod_evasive, con el cual nos va a permitir que al momento de detectar un ataque DoS conseguiremos redirigir el tráfico de las peticiones ilegítimas hacia un error 403 lo que hará que estos clientes reciban un mensaje de recurso prohibido (Forbidden).

Internamente, se realiza la detección creando una tabla hash dinámica de direcciones IP y las URL, denegando a las IPs que cumplan una de las siguientes condiciones:

- Mandar peticiones a la misma página muchas veces por segundo.
- Hacer más de 'N' peticiones concurrentes al mismo nodo por segundo.
- Hacer peticiones estando registrado en una lista negra o lista de bloqueo (blacklisting).

Protección de Apache para Envenenamiento de DNS

Con el fin de proteger a nuestro Servidor Web Apache de un ataque de Inyección DNS vamos a hacer uso de un módulo llamado mod_spamhaus. Este módulo nos permite bloquear o denegar el acceso web a dirección IP particulares identificadas como direcciones SPAM.

Gracias a que utiliza un servicio de DNSBL (DNS-Blackhole List) logra identificarlas y detiene la retransmisión del SPAM generadas a través de inyección DNS en formularios web.

Como protección adicional el módulo de mod_spamhaus nos permite bloquear los ataques http DDoS generados por los bots.

A pesar de que regularmente este módulo no se encuentra instalado por defecto en la implementación de un Servidor Web Apache una vez instalado y configurado el modulo realiza consultas a spamhaus.org y aprovecha las principales listas:

- Lista SBL o Lista de Bloqueo Spamhaus.
- Lista XBL o Lista de Bloqueo Exploits.

Spamhaus.org y DNSBL.info son sitios web donde brindan el servicio de base de datos de IPs calificadas como SPAM o peligrosas, pudiendo así comprobar el estado de lista negra de una dirección IP basándose en registros DNS.

Protección de Apache contra Slowloris

Para poder proteger nuestro Servidor Web Apache de un ataque de tipo Slowloris vamos a hacer uso de un módulo llamado mod_qos.

Este módulo previene los ataques Slowloris dando diferentes niveles de prioridad categorizando a las diferentes peticiones HTTP recibidas en el Servidor.

El módulo mod_qos tiene la potencia de poder determinar qué petición debe servirse y cuál no y así mismo las que si van a ser atendidas este módulo le determinará con la prioridad con la que será procesada, así evita el uso indiscriminado de los recursos del Servidor.

Dicho módulo mod_qos regularmente no viene instalado por defecto en la implementación del Servidor Web Apache, pero una vez instalado y configurado el módulo recopila la información de diferentes atributos de los paquetes HTTP tales como:

- URL de la petición.
- Cabeceras de peticiones y respuestas HTTP.
- Dirección IP.
- Código de respuesta HTTP.
- Datos históricos basados en la sesión del usuario.
- Número de peticiones concurrentes al servidor.
- Número de conexiones TCP concurrentes.

Con esta información el módulo mod_qos lograr crear su tabla de prioridades de atención a los requerimientos, y a todas las peticiones que se caractericen por tener el comportamiento de los paquetes enviados por Slowloris los deja para el final en sus prioridades o simplemente los corta y no los procesa.

2.7 Servicio Samba en Linux.

Samba es una suite de aplicaciones para Unix (Linux) de tipo Open Source bajo la licencia GPL/GNU que ofrece interoperabilidad estándar con Windows, ofreciendo servicios de archivos e impresión estables, seguros y veloces para los clientes que usen el protocolo SMB/CIFS, pudiendo integrarse en ambientes de Directorio Activo, Servidores y Equipos de Escritorio Unix (Linux).

Su desarrollo es basado en una implementación de código abierto del protocolo Server Message Block (SMB) lo que permite que puedan compartir recursos como archivos, carpetas e impresoras entre redes Windows, Unix (Linux) y Mac.

Entre sus principales características podemos señalar que Samba puede unirse a un dominio Active Directory usando protocolos LDAP y Kerberos, soporte de idiomas internacionales para los nombres de archivos usando Unicode, e incluso puede funcionar como un controlador de dominio primario (PDC).

Los servicios que Samba puede ofrecer son los siguientes:

- Compartir sistemas de archivos.
- Compartir impresoras instaladas en el servidor a clientes Unix (Linux), Windows y Mac.
- Asiste en la navegación de la red (con o sin NetBIOS).
- Autentificar clientes haciendo login contra un dominio Windows.
- Asistir como un servidor de resolución de nombres Windows Internet Name Service (WINS).
- Actuar como un Backup Domain Controller (BDC) para un PDC basado en Samba.

La suite Samba consta de dos servicios (llamados demonios en Linux) que proporcionan los recursos compartidos a clientes SMB a través de la red, los demonios son SMBD y NMBD.

SMBD, este servicio permite la compartición de archivos e impresoras sobre una red SMB y proporciona autenticación de acceso para clientes SMB. NMBD, este servicio busca los recursos y clientes usando el protocolo Windows Internet Name Service (WINS), y ayuda mediante un visualizador de recursos de red.

En la amplia evolución del Servicio Samba entidades importantes como Microsoft también han contribuido con su desarrollo poniendo a disposición su definición de SMB, documentación del Common Internet File System (CIFS) y del Public Request for Comments (RFC), lo que ha agregado interoperabilidad de protocolos entre sistemas operativos. Para futuras versiones el nuevo nombre de Samba será el protocolo CIFS por tal razón en la actualidad el protocolo es escrito como SMB/CIFS.

2.7.1 Ataques a Samba.

Retransmisión SMB

Este tipo de ataque es de Intermediario o Men In The Middle (MITM), y es realizado usando dos programas especiales SMBRelay y SMBRelay2, los mismos que tienen la capacidad de llevar a cabo ataques contra equipos remotos. Los programas toman ventaja del protocolo SMB que se encuentra dentro del NETBIOS, el mismo que es usado por cualquier usuario que comparte una carpeta o archivo a través de la red LAN.

Dentro de la comunicación de la LAN los hashes de contraseñas son intercambiados entre los clientes y el servidor, en ese momento SMBRelay recibe una conexión sobre el puerto UDP 139 y 445 y retransmite los paquetes intercambiados por el cliente y el servidor y los modifican (excepto para la negociación y autentificación), luego de conectarse y autentificarse el equipo es desconectado.

SMBRelay creará una nueva dirección IP virtual y de este modo podrá ser utilizada por cualquiera de las funciones de red de Windows. Los atacantes remotos pueden utilizar la dirección IP durante tanto tiempo como el equipo se encuentre conectado.

El programa SMBRelay2 trabaja bajo el mismo principio de SMBRelay, excepto que emplea los nombres de NetBIOS en lugar de las direcciones IP.

Ambas pueden llevar a cabo ataques de tipo MITM, los cuales permiten a los atacantes remotos leer, insertar y modificar mensajes intercambiados entre dos extremos de la comunicación sin ser advertidos.

Los equipos expuestos a esta clase de ataques dejan de responder o se reinician inesperadamente.

2.7.2 Fortaleciendo a Samba.

Como se explica en el punto 2.7.1. Un ataque "Men in The Middle" (MITM) puede suplantar a un servidor de confianza y, por tanto, obtener privilegios de acceso al dominio mediante el envío de datos de replicación o autorización maliciosa.

El impacto para Samba es particularmente importante en los casos en los que el servicio de replicación Samba DRS contacta a otro DC que solicita la replicación de contraseñas de usuario, ya que éstas podrían ser controladas por el atacante.

Para contrarrestar esta vulnerabilidad se realizó una actualización de versión de Samba a la versión 4.1.1 la cual cuenta con el parche de seguridad Heimdal Kerberos.

En esta versión de Samba tenemos el parámetro de configuración "client signing = required" lo cual nos permite habilitar el cifrado en Samba, el cual proporciona cifrado de extremo a extremo de los datos SMB y protege los datos de ocurrencias de interceptación de redes no confiables.

Puede implementar el cifrado SMB con el mínimo esfuerzo, pero puede requerir pequeños costes adicionales para software o hardware especializado. El cifrado SMB puede configurarse por recurso compartido o para el servidor de archivos completo y puede habilitarse para una variedad de escenarios donde la transferencia de datos por redes no confiables.

2.8 Clústeres entre Sitios Remotos.

Los Clúster entre sitios remotos o también llamados Geo-Cluster son cada vez más requeridos en nuestro mercado, ya que las empresas en crecimiento se han visto en la necesidad de proveer al 100% de tiempo los servicios que ofrecen, y al momento que querer cubrir el riesgo que existe de mantener un centro de cómputo único es el escenario ideal para implementar Geo-Cluster.

Estos clúster remotos van desde centros de cómputos a distancias de metros hasta separados por distancias de países y continentes, casos en que el rol de software de sincronización y los enlaces de telecomunicaciones juegan el papel más importante ya que sin ellos los sistemas clúster serían inoperativos.

Por otro lado el clúster de sitios remotos o también llamados Geo-Cluster son también clasificados debido a su configuración.

Multi-Site Cluster, este término puede referirse a varios tipos de configuraciones de clúster. Los más comunes son los clústeres multi-sitio de recuperación de desastres (Multi-Site Disaster Recovery Cluster) y los clústeres elásticos (Stretch Cluster). Los Multi-Site Disaster Recovery Cluster se admiten con la advertencia de que la operación de conmutación por error de sitio a sitio se realiza manualmente por el administrador del clúster. Solamente ciertas configuraciones del Stretch Cluster pueden ser soportadas en este escenario. [5]

Multi-Site Disaster Recovery Cluster, este escenario de clúster comprende a su vez dos clúster completamente diferentes, cada uno configurado en los sitios remotos consecutivamente. Estos clústeres suelen tener la misma configuración, con uno activo y el otro pasivo (y a veces apagado). Si falla el sitio principal, el sitio secundario se activa manualmente y se hace cargo de todos los servicios. El almacenamiento compartido se debe replicar desde el sitio principal al sitio de respaldo mediante la replicación basada en array.

Durante una conmutación por error de sitio, el administrador del clúster debe alternar primero la direccionalidad de la replicación de almacenamiento para que el sitio de copia de seguridad se convierta en el principal. Estos pasos no pueden ser automatizados, ya que en caso de presentarse intermitencias en la red podría provocar que se dé un cambio entre sitio principal y el de respaldo de forma no controlada. [5]

Stretch Cluster, Los clúster elásticos están diseñados para soportar la pérdida tanto de uno como de todos los miembros en un sitio. Esto puede ser un desafío por una serie de razones:

- Un gran porcentaje de miembros del clúster podría perderse simultáneamente.
- La pérdida de conectividad con todos los miembros en un sitio determinado puede ser más probable porque la conectividad de red y de almacenamiento de sitio a sitio suele ser menos redundante, más cara y menos confiable que la conectividad de un único sitio.
- Se requiere algún método de replicación de almacenamiento multi-sitio para que los datos de servicios agrupados sigan estando disponibles después de la pérdida del sitio. [5]

Un Clúster Elástico es aquel que comprende una infraestructura única y una membresía que abarca todos los sitios. La pertenencia al clúster se divide lógicamente en dos grupos para que los servicios de clúster puedan continuar con una interrupción mínima cuando un grupo entero fracasa o se convierte en inaccesible. Si hay almacenamiento compartido, se replica mediante mecanismos de replicación de hardware o software para que cada grupo tenga acceso a una réplica. Los grupos están típicamente, pero no necesariamente, en diferentes ubicaciones físicas, a menudo con una interconectividad de comunicación reducida y un retraso mayor en comparación con un único sitio. [5]
Los siguientes son algunos ejemplos de lo que califica como un grupo de estiramiento:

- Múltiples chasis físicos conectados donde ningún chasis tiene la mayoría de los nodos del clúster.
- Los miembros del clúster que se encuentran en la misma sala o centro de datos pero no están todos conectados al mismo conmutador en 1 salto.
- Miembros de clúster que se encuentran en diferentes sitios físicos conectados por enlace de sitio físico.

2.8.1 Enlaces de Radiofrecuencia.

Para el presente proyecto se implementa un enlace de Radiofrecuencia usando equipos Ubiquiti Modelo Rocket M5 en una banda de 5 GHz a una distancia de 1.2 km. Estos equipos han demostrado ser robustos en hardware experimentado tiempo de vida prolongado de más de 6 años.

Soporta velocidades de hasta 150 Mbps TCP / IP real. Es ideal para despliegue de enlaces punto a punto (PtP), Punto a multipunto (PtMP), Aplicaciones airMAX. En anchos de banda maneja: 2, 3, 5, 8, 10, 20, 25, 30 dbm. Tiene un montaje integrado, por lo que la instalación no requiere herramientas especiales. [6]

Las Radios Ubiquiti Rocket M5 cuentan con Tecnología airMAX con la cual nos proporciona rendimiento, capacidad y escalabilidad para enlaces de alta velocidad y de clase operadora.

El protocolo TDMA asigna dinámicamente tiempo a los clientes activos y proporciona un mayor rendimiento de inmunidad al ruido en comparación con el convencional 802.11 CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance).

Los AP (Access Point) con esta tecnología pueden recorrer varios kilómetros de distancia. Debido a que las estaciones no pueden sentirse mutuamente, diseñado para aplicaciones al aire libre, el protocolo TDMA resuelve el problema del "nodo oculto".

El AP divide el canal inalámbrico en ranuras de tiempo y asigna una ranura de tiempo predeterminada a cada estación conectada. Esto elimina esencialmente la posibilidad de que las estaciones transmitan al mismo tiempo, eliminando así las colisiones de recepción en el AP. [7]

Lo cual nos ayuda a certificar que los datos transmitidos a través de estas radios llegará en tiempos muy cortos, ideal para que el Heartbeat del clúster sea efectivo.

Como se puede apreciar en la Figura 2.1 los Radios Ubiquiti Rocket M5 tienen un tamaño compacto de 160 mm x 80 mm x 30 mm, a pesar de sus dimensiones tienen una gran potencia de trasmisión y soportan años de operatividad de enlaces de radiofrecuencia ininterrumpida.

Figura 2.1 Radio Ubiquiti Rocket M5

Reseña de Radioenlaces de 5 GHz

El estándar 802.11a creado por la IEEE en el año de 1999, cuenta con 12 canales sin solapamiento, 8 para red inalámbrica en banda de 5 GHz y 4 para conexiones punto a punto.

Para las subportadoras de 802.11a puede ser utilizada una de las siguientes formas de modulación: BPSK, QPSK, 16-QAM y 64-QAM. Utiliza la modulación Multiplexación por División de Frecuencias Ortogonales, OFDM por sus siglas en ingles Orthogonal Frequency Division Multiplexing, la cual permite transferir múltiples datos a una velocidad máxima teórica de 54 Mbps, en la práctica velocidades de 30 Mbps. [8]

La señal OFDM utilizada para 802.11 comprende 52 subportadoras. De estos 48 se utilizan para la transmisión de datos y cuatro se demandan como subportadoras piloto. La separación entre las subportadoras individuales es de 0,3125 MHz. Esto resulta del hecho de que el ancho de banda de 20 MHz está dividido por 64.

Aunque sólo se usan 52 subportadoras, ocupando un total de 16,6 MHz, el espacio restante se utiliza como banda de protección entre los diferentes canales. [9]

El estándar 802.11b y 802.11a se crearon al mismo tiempo, pero debido a su mayor costo el 802.11a se encuentra generalmente en los enlaces de radiofrecuencia de negocios, mientras que la 802.11b tiene más acercamiento al cliente final del mercado nacional; otra característica que los diferencia es que las señales que utilizan 802.11a tienen más dificultad para penetrar en las paredes y otras obstrucciones que las señales que utilizan 802.11b. Ambos estándares utilizan frecuencias diferentes, por lo cual son incompatibles entre sí, a pesar de eso en el mercado se ofrecen dispositivos híbridos con ambos estándares, pero la realidad es que estos dispositivos cuentan con dos módulos separados y cada uno gestiona un estándar a la vez. [10]

2.8.2 Replicación de Dispositivos de Bloque.

Como lo habíamos mencionado en el apartado Modelo propuesto para la solución del problema, la sincronización de la información entre los nodos del clúster juega uno de los papeles más importantes y fundamentales en la constitución del clúster entre sitios remotos, ya que debemos asegurarnos que la información esté actualizada permanentemente en todos los nodos del clúster, este trabajo será realizado gracias al desempeño de la Replicación de Dispositivos de Bloque o también llamado DRBD por sus siglas en inglés Distributed Replicated Block Device.

DRBD es una replicación síncrona a nivel de bloque de kernel que sirve para construir bloques de clúster con recurso no compartidos, para lo cual sólo tendrá que instalar las utilidades de gestión de espacio de usuario de DRBD (normalmente denominadas drbd-utils, drbd8-utils o similar). [11]

Este software es capaz de sincronizar la información entre dispositivos de almacenamiento de datos a través de sus bloques de almacenamiento, es decir no sincroniza archivos o carpetas, replica los bloques físicos escritos en un dispositivo de almacenamiento hacia otro.

Gracias a este mecanismo podemos replicar la información de un almacenamiento a otro incluso si los archivos están siendo utilizados por un software, en concreto podemos sincronizar los archivos de base de datos MySQL incluso si estos están siendo usados por el motor del servicio de base de datos MySQL.

Si un Usuario está siendo uso de un archivo de un recurso compartido por SAMBA este será replicado de un dispositivo de almacenamiento a otro sin ningún problema.

Para los clúster remotos la aplicación de la sincronización a través de DRBD es esencial, la configuración consta del HeartBeat de Alta disponibilidad en los dos sitios remotos, con una conexión con rutas IPv4 entre los que puede variar desde unos pocos Mbps hasta 10Gbps dependiendo de la carga I/O impuesta a los nodos del clúster.

Se pueden distribuir varios servicios a través de los clúster con tan sólo tener que replicar los datos entre los nodos para tener un Failover rápido en caso de que se caiga un sitio. [12]

CAPÍTULO 3

3. ANÁLISIS Y DISEÑO DE LA SOLUCIÓN.

En este capítulo se expone la planificación operativa del proyecto luego de haber analizado la factibilidad de implementación del mismo con los recursos disponibles.

Para el desarrollo del análisis del sistema propuesto en este Proyecto se tomó como referencia el trabajo realizado por Katherine Estefanía Campos Bustos y José Luis Vera Chávez en el Informe de Proyecto de Graduación titulado "DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE ALTA DISPONIBILIDAD USANDO CLÚSTER Y VIRTUALIZACIÓN DE SERVIDORES WEB Y DE BASES DE DATOS PARA LAS APLICACIONES DE LA FIEC". Ya que en su estudio se analizó el Stack Pacemaker, CMAN y Corosync para la administración de Clúster se decidió tomar el stack propuesto y potenciarlo con equipos más robustos y una infraestructura de redes más sólida y protegida.

3.1 Análisis del sistema clúster de Linux del proyecto.

En cuanto a los equipos servidor a usar en este proyecto utilizaremos servidores HP ProLiant de sexta generación con sistema operativo Linux CentOS 6.7 de 64 bits.

Redes LAN de velocidades de 10 Gbps entre los equipos cliente y servidores y también para la conexión iSCSI del almacenamiento de datos de los servidores.

Como ya revisamos en el Subcapítulo 2.8 del presente documento, se estudió los tipos de clúster de sitios remotos según la configuración de cada uno.

Para la implementación del presente proyecto se configura un Multi-Site Stretch Cluster, ya que los nodos miembros que conforman el clúster se encuentran separados geográficamente en dos centros de cómputos respectivamente y estarán conectados a través de un enlace de radiofrecuencia dedicado.

Para este proyecto haremos uso de un enlace de radiofrecuencia con frecuencia de 5 GHz existente entre los centros de cómputo principal y secundario el cual usa Radios Ubiquiti Rocket M5.

Como revisamos en el Subcapítulo 2.8.1 los enlaces de radiofrecuencia de 5 GHz son óptimos para la implementación de este proyecto por el ancho de banda que nos ofrecen y además tienen la ventaja de que los canales están menos saturadas que las de 2.4 GHz.

Cada canal tiene mayor ancho de banda lo que también influye en la velocidad de transmisión.

La principal desventaja es que presentan mayores problemas al atravesar objetos sólidos, con lo cual se hace imprescindible que al ubicar las antenas tengamos visión directa entre ellas, de lo contrario aumentará notablemente la atenuación de la señal redundando en una peor calidad de transmisión de los datos.

3.2 Descripción técnica de los equipos a usar en el proyecto.

Nodos

Los nodos del clúster se comunican usando una interfaz de paso de mensajes y son los elementos principales de un sistema clúster [13].

Son los computadores que están conectados entre sí, a través de software y de una red de alta velocidad para comportarse como uno solo.

Son utilizados especialmente para mejorar el rendimiento y/o la disponibilidad que un único sistema no puede alcanzar. [5]

Además de ser una alternativa económica y que puede funcionar de manera similar a costosos sistemas de alta potencia y disponibilidad.

Los nodos a utilizarse en este proyecto son dos servidores Marca HP modelo ProLiant DL360 G6.

Como se puede apreciar en la Figura 3.1 estos equipos son de tipo Rack de medidas de 1U, además cuentan con las siguientes características [14]:

- 2 CPU Intel Xeon E5504 / 2 GHz Quad-Core.
- RAID 5 500GB Sandisk SSD.
- Memoria RAM 32 GB DDR3 SDRAM 1333 MHz.
- 3 NIC Gigabit Ethernet.
- Sistema Operativo Linux CentOS 6.7 x64 Bits.
- Fuente de Poder Redundante Doble.

Figura 3.1 Servidor HP ProLiant DL360 G6

Almacenamiento

El almacenamiento de los datos del clúster es uno de los elementos más importantes del sistema, y debe estar disponible para todos los nodos miembros del Clúster en todo momento.

Para el presente proyecto el almacenamiento de datos estará provista por equipos de Marca Synology Modelo DS2015xs, como se puede apreciar en la Figura 3.2 este dispositivo cuenta con un diseño moderno con medidas de 157 mm x 340 mm x 233 mm, las bandejas de discos cuentan con seguridad individual para evitar la manipulación de los discos.

Además cuenta con las siguientes características [15]:

- Procesador Quad Core Alpine AL514 1.7 GHz
- Memoria RAM 8 GB

Figura 3.2 NAS Synology DS2015xs

Como elemento diferenciador en el Almacenamiento del clúster se ha implementado un Clúster de Alta Disponibilidad formada entre dos NAS Synology, para lo cual se han obtenido dos de similares características, ambos formarán un único servidor iSCSI que proveerá discos virtuales a ambos nodos del Clúster, de tal manera obtenemos protección redundante en el almacenamiento de datos.

En la Figura 3.3 podemos apreciar el Administrador de Alta Disponibilidad de Synology, el cual indica el estado de salud de ambos dispositivos, los roles de cada uno, y desde el cual podemos realizar las tareas operativas al clúster formado por los dos dispositivos NAS.

Figura 3.3 Administrador Clúster Synology

Redes

Para la descripción de esta sección hemos dividido las redes en dos grupos, las redes LAN y las redes WAN. Las Redes LAN contemplan las conexiones locales de los servidores dentro del centro de cómputo.

Por otro lado las redes WAN contemplan las conexiones realizadas por las antenas de radiofrecuencia entre los centros de cómputo.

Redes LAN

Los nodos del clúster cuentan con 3 interfaces de red, asignado respectivamente a la red LAN de Pycca, Red iSCSI de Almacenamiento, Red de HeartBeat de Clúster.

Como elemento innovador en esta categoría se realizó una mejora cambiando las tarjetas de velocidad de 1 Gbps que viene equipado el servidor, por las tarjetas de Intel modelo X520 de velocidad de 10Gbps.

Como se puede apreciar en la Figura 3.4 estas tarjetas son de tipo PCI Express y además cuentan con la nueva tecnología CRC de Intel la cual puede proveer integridad de datos superior con un mínimo de impacto en el transporte de datos en la red (throughput) [16].

Figura 3.4 Tarjeta de Red Intel X520

Para que exista conmutación a la velocidad de 10Gbps es necesario también mejorar los conmutadores de red.

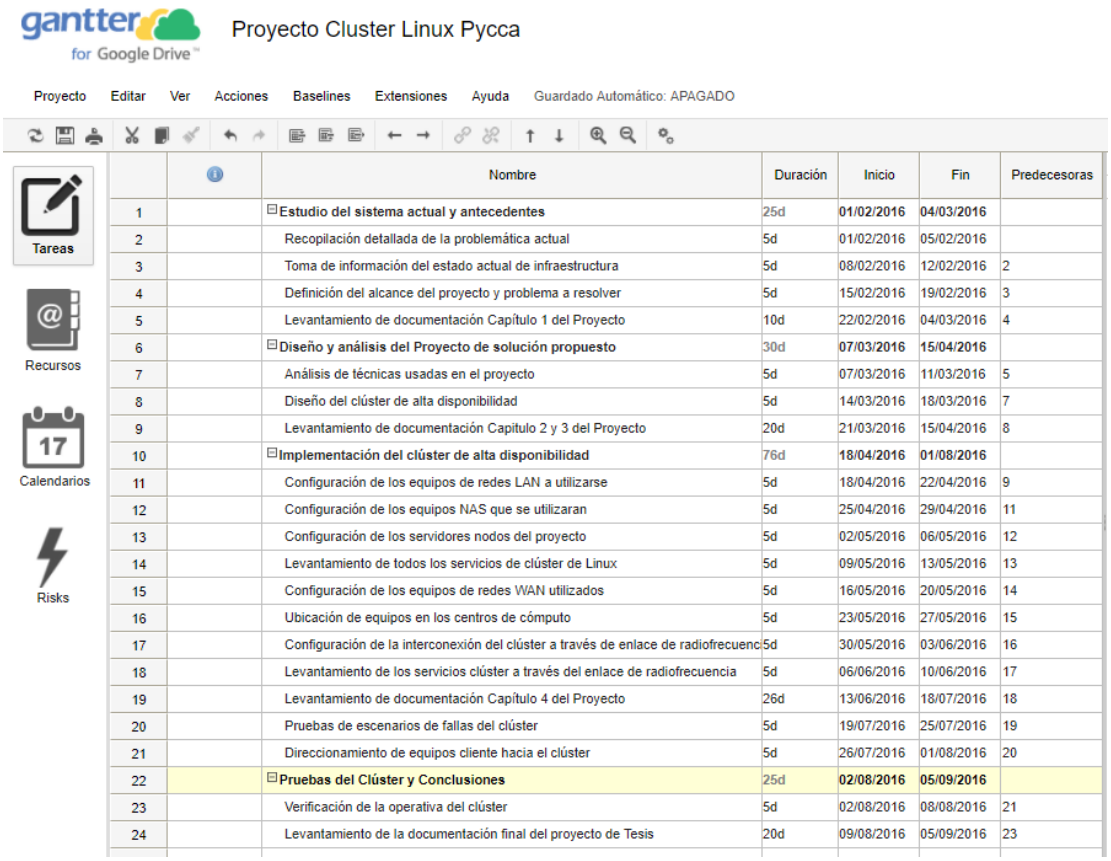
Para lo cual se adquirieron dos Switch de marca Netgear modelo ProSafe XS712T, los cuales proveen conmutación a velocidad de 10Gbps, como se puede apreciar en la Figura 3.5 el Switch es de tipo Rack, tiene 1 U de medida y 12 puertos de red, 10 dedicados a conectores RJ45 y dos que pueden ser usados con SFP o con RJ45 [17].

Figura 3.5 Switch Netgear XS712T

El cable de red UTP que se utiliza para la implementación de este proyecto es cable de cobre de red UTP Categoría 7 con conectores tipo RJ45.

3.3 Cronograma del Proyecto.

A continuación en la Figura 3.6 se detallan los procesos que fueron realizados para llevar a cabo este proyecto, agrupados por etapas, en un cronograma con fecha y duración estimada.



		Nombre	Duración	Inicio	Fin	Predecesoras
1		**Estudio del sistema actual y antecedentes**	25d	**01/02/2016**	**04/03/2016**	
2		Recopilación detallada de la problemática actual	5d	01/02/2016	05/02/2016	
3		Toma de información del estado actual de infraestructura	5d	08/02/2016	12/02/2016	2
4		Definición del alcance del proyecto y problema a resolver	5d	15/02/2016	19/02/2016	3
5		Levantamiento de documentación Capítulo 1 del Proyecto	10d	22/02/2016	04/03/2016	4
6		**Diseño y análisis del Proyecto de solución propuesto**	30d	**07/03/2016**	**15/04/2016**	
7		Análisis de técnicas usadas en el proyecto	5d	07/03/2016	11/03/2016	5
8		Diseño del clúster de alta disponibilidad	5d	14/03/2016	18/03/2016	7
9		Levantamiento de documentación Capitulo 2 y 3 del Proyecto	20d	21/03/2016	15/04/2016	8
10		**Implementación del clúster de alta disponibilidad**	76d	**18/04/2016**	**01/08/2016**	
11		Configuración de los equipos de redes LAN a utilizarse	5d	18/04/2016	22/04/2016	9
12		Configuración de los equipos NAS que se utilizaran	5d	25/04/2016	29/04/2016	11
13		Configuración de los servidores nodos del proyecto	5d	02/05/2016	06/05/2016	12
14		Levantamiento de todos los servicios de clúster de Linux	5d	09/05/2016	13/05/2016	13
15		Configuración de los equipos de redes WAN utilizados	5d	16/05/2016	20/05/2016	14
16		Ubicación de equipos en los centros de cómputo	5d	23/05/2016	27/05/2016	15
17		Configuración de la interconexión del clúster a través de enlace de radiofrecuenc	5d	30/05/2016	03/06/2016	16
18		Levantamiento de los servicios clúster a través del enlace de radiofrecuencia	5d	06/06/2016	10/06/2016	17
19		Levantamiento de documentación Capítulo 4 del Proyecto	26d	13/06/2016	18/07/2016	18
20		Pruebas de escenarios de fallas del clúster	5d	19/07/2016	25/07/2016	19
21		Direccionamiento de equipos cliente hacia el clúster	5d	26/07/2016	01/08/2016	20
22		**Pruebas del Clúster y Conclusiones**	25d	**02/08/2016**	**05/09/2016**	
23		Verificación de la operativa del clúster	5d	02/08/2016	08/08/2016	21
24		Levantamiento de la documentación final del proyecto de Tesis	20d	09/08/2016	05/09/2016	23

Figura 3.6 Cronograma del Proyecto

3.4 Diseño del sistema Clúster de Linux del proyecto.

A continuación, en la Figura 3.7 se puede observar un diagrama donde se muestra el Diseño del Sistema Clúster de Alta Disponibilidad propuesto para este proyecto, posterior a eso una explicación del mismo.

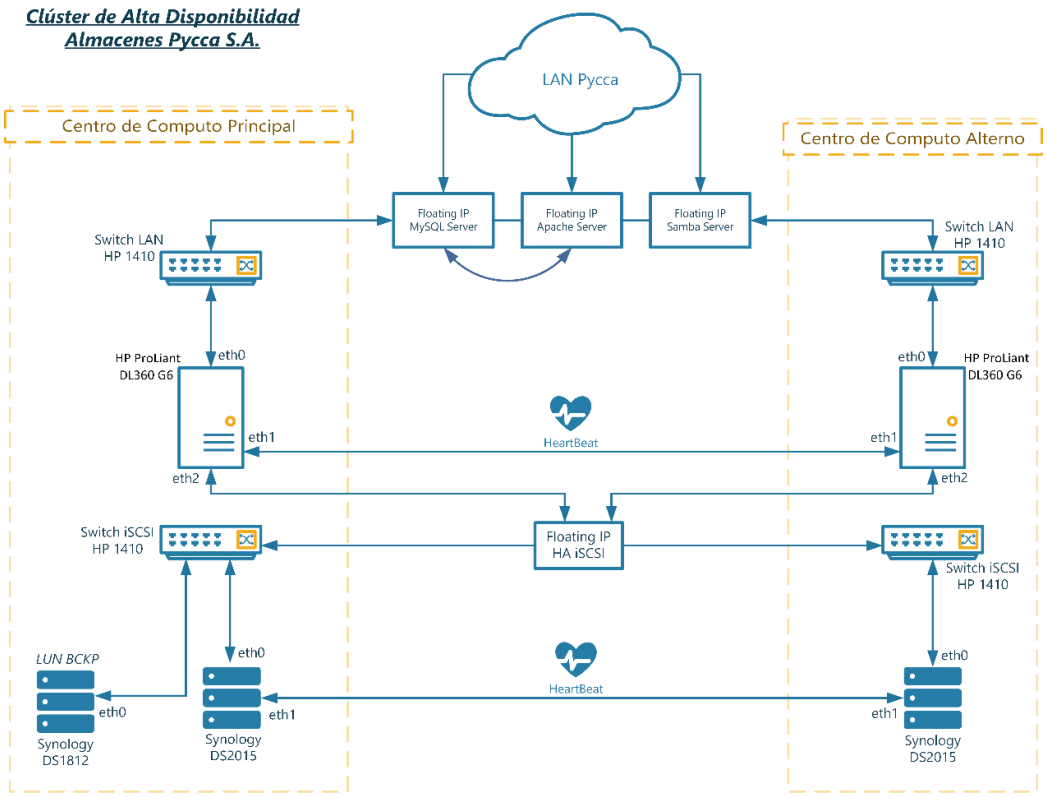


Figura 3.7 Diseño Clúster Alta Disponibilidad

Con este proyecto se busca proveer de una alta disponibilidad de los servicios que el clúster provee, para lo cual se ha diseñado un sistema con el cual se obtiene una redundancia en la transmisión de los datos y la disponibilidad de los nodos a pesar de una falla en uno de los centros de cómputo. Usando el enlace de radio frecuencia se obtienen conectividad entre ambos sitios ofreciendo así una IP flotante a la cual los clientes accederán a obtener sus servicios.

En cuanto a los repositorios de datos también contamos con un clúster de datos y los servidores nodos del clúster acceden al repositorio protegido por el clúster Synology

3.4.1 Infraestructura de Red WAN del Clúster.

En este subcapítulo se describe el diseño de la red WAN del clúster la cual está conformado esencialmente por los equipos de Radiofrecuencia Ubiquiti, a continuación un gráfico donde se describe la conexión WAN.

Como se puede apreciar en la Figura 3.8 el enlace que comunica los dos centros de cómputo el principal y el alterno está compuesto por dos radios Ubiquiti Rocket M5.

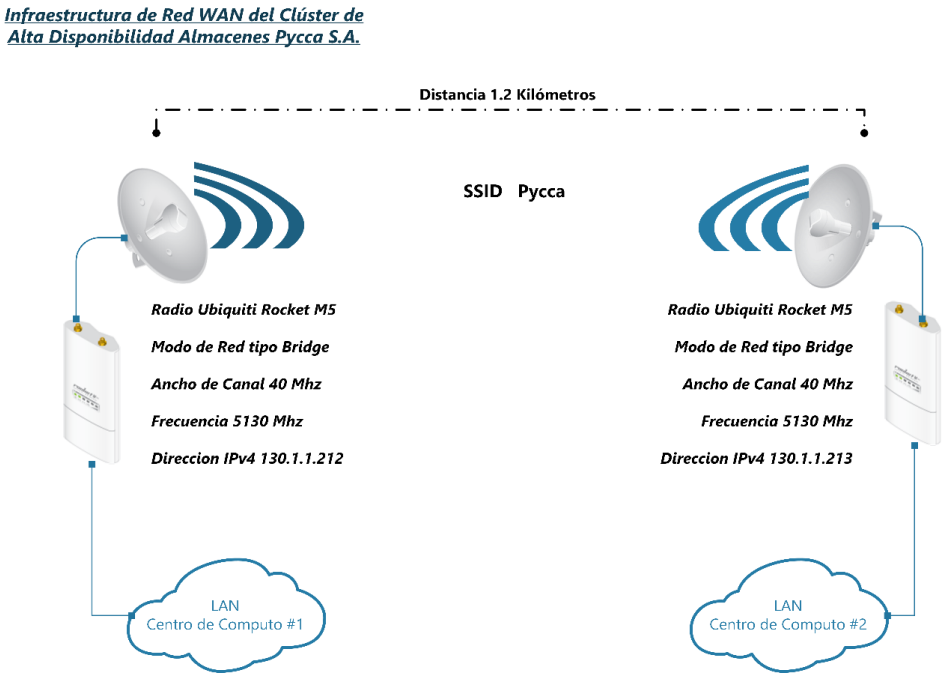


Figura 3.8 Diseño Red WAN del Clúster

Estos equipos nos dan la versatilidad que necesitamos ya que son poderosos al momento de establecer un enlace incluso con obstáculos en la línea de vista.

Usando la frecuencia de 5 GHz nos brinda un ancho de banda suficiente para que el Clúster tenga tiempos de interconexión óptimos para su operación.

La Figura 3.9 es un extracto sacado del informe elaborado para la ARCOTEL, donde se pueden verificar los detalles técnicos del enlace de radiofrecuencia, detalles tales como altura, potencia, GPS, etc.

Agencia de Regulación y Control de las Telecomunicaciones

APÉNDICE 1

INFORMACIÓN TÉCNICA DE USO DE FRECUENCIAS DEL ESPECTRO RADIOELÉCTRICO

DRE

SERVICIO DE RADIOCOMUNICACIONES: FIJO TERRESTRE - ENLACES DE MODULACIÓN DIGITAL DE BANDA ANCHA

ENLACE PUNTO-MULTIPUNTO 3

CARACTERISTICAS DEL ENLACE:

Banda de Frecuencias (MHz)	Tipo de Operación	Número de Estaciones Fijas	Tarifa Mensual (USD)
2400 MHz – 2483,5 MHz	OFDM	5	26,71

CARACTERISTICAS DE LAS ESTRUCTURAS:

No.	Código	Provincia	Cantón	Ciudad, Calle No. / Localidad	Latitud	Longitud
1	SNB0717	GUAYAS	GUAYAQUIL	BOYACA 1205 Y 9 DE OCTUBRE,	02°11'28,33" S	79°53'02,40" W
2	SMB1933	GUAYAS	GUAYAQUIL	C.C. SAN MARINO,	02°10'10,03" S	79°53'56,09" W
3	SNB2616	GUAYAS	GUAYAQUIL	BOYACA Y PIEDRAHITA,	02°11'07,00" S	79°52'56,00" W
4	SNB2622	GUAYAS	GUAYAQUIL	BOYACA Y COLON,	02°11'46,02" S	79°53'06,04" W
5	SEB013028	GUAYAS	GUAYAQUIL	PYCCA SUCRE, SUCRE 521 Y BOYACA,	02°11'44,08" S	79°53'07,05" W

CARACTERISTICAS DE LA ESTACION CENTRAL:

Indicativo	Estructura	Antena	Gan. de Ant (dBi)	Azimut de Ant. (°)	Pol.	Altura Base-Ant.(m)	Equipo	Potencia (mW)	RNI
HD126742	SNB0717	UBIQUITI NETWORKS NANOSTATION 2	10,00	325,40	V	33,00	UBIQUITI NETWORKS NANOSTATION 2	398,00	

CARACTERISTICAS TECNICAS DE LAS ESTACIONES (4):

Indicativo	Estructura	Antena	Gan. de Ant (dBi)	Azimut de Ant. (°)	Pol.	Altura Base-Ant.(m)	Equipo	Potencia (mW)	Dist. (Km)	RNI
HD126743	SMB1933	UBIQUITI NETWORKS NANOSTATION 2	10,00	145,40	V	6,00	UBIQUITI NETWORKS NANOSTATION 2	398,00	2,93	
HD126744	SNB2616	UBIQUITI NETWORKS NANOSTATION 2	10,00	196,69	V	30,00	UBIQUITI NETWORKS NANOSTATION 2	398,00	0,69	
HD126745	SNB2622	UBIQUITI NETWORKS NANOSTATION 2	10,00	11,70	V	6,00	UBIQUITI NETWORKS NANOSTATION 2	398,00	0,56	
HD126746	SEB013028	UBIQUITI NETWORKS NANOSTATION 2	10,00	16,33	V	15,00	UBIQUITI NETWORKS NANOSTATION 2	398,00	0,51	

Figura 3.9 Informe Técnico ARCOTEL

Establecido óptimamente el enlace, con la herramienta propietaria de Ubiquiti Networks podemos controlar los niveles de los indicadores necesarios para verificar que la conexión WAN es ideal para establecer el HeartBeat del clúster óptimo.

En la Figura 3.10 podemos apreciar el panel de Monitoreo de la Radio donde se verifica las Tasas de Transferencias TX 216 Mbps y RX 180 Mbps; Potencia –47 / -46 dBm; Ancho de Canal 40 MHz, etc.

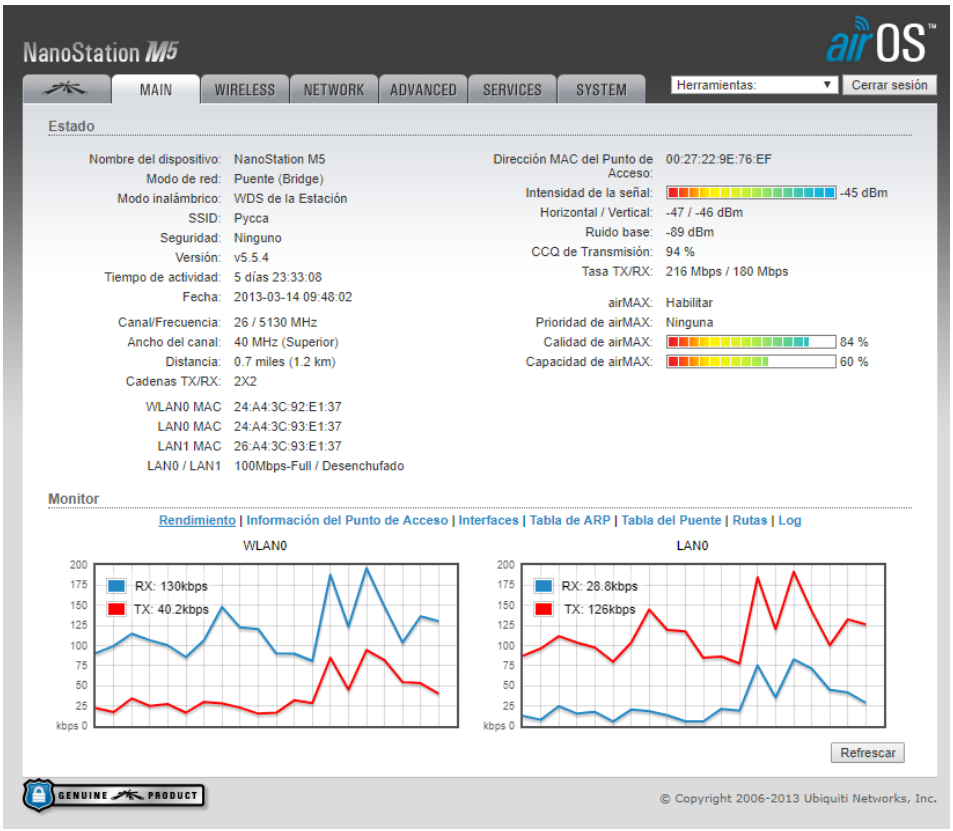


Figura 3.10 Monitor del Radioenlace WAN

3.4.2 Infraestructura de Red LAN del Clúster.

En el presente apartado describe el equipamiento que se configura para las conexiones del núcleo del clúster en cada uno de los centros de cómputo; cada Nodo cuenta con 3 interfaces de red de 10 Gbps de velocidad.

La Figura 3.11 es una representación gráfica de las interconexiones que tienen cada uno de los nodos miembros del clúster, la primera interfaz del servidor (eth0) se encuentra conectada a un Switch Netgear XS712T que pertenece a la red LAN de Pycca, y será esta interfaz la que reciba los requerimientos de los clientes.

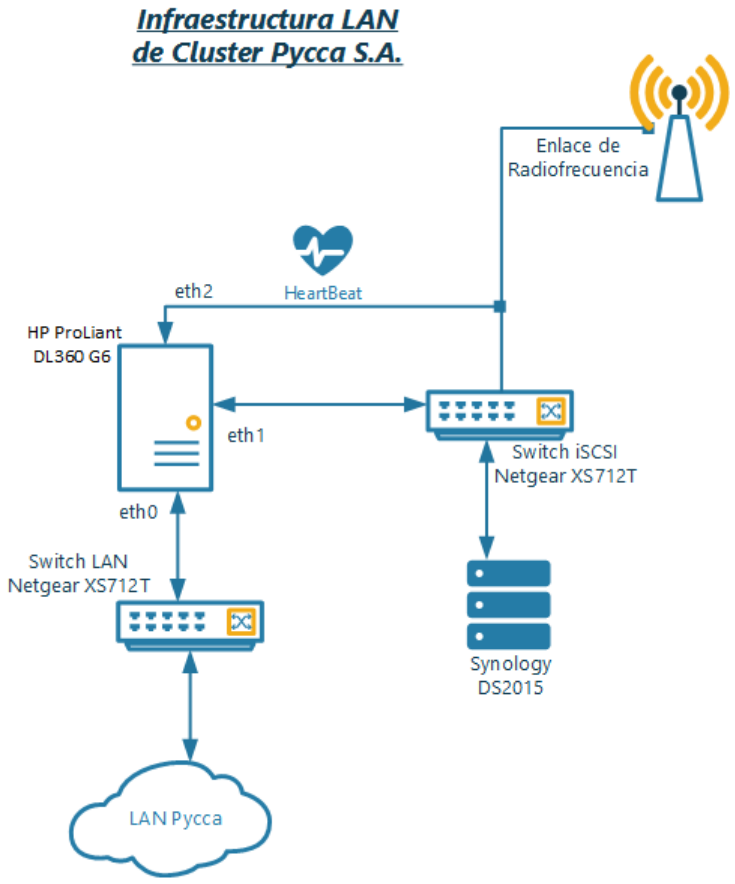


Figura 3.11 Infraestructura LAN del Clúster

La segunda interfaz (eth1) se conecta a un segundo Switch Netgear XS712T que pertenece a la red exclusiva de almacenamiento iSCSI, esta interfaz tendrá conexión directa con los NAS y utilizara el enlace de radiofrecuencia para poder comunicarse con el segundo NAS concurrentemente; y la tercera interfaz (eth2) se utilizara para establecer el HeartBeat entre ambos nodos del clúster, se utilizara el enlace de radiofrecuencia para enviar los mensajes de estados de salud de un Nodo a otro.

La red de datos corporativa de la empresa Pycca también llamada LAN Pycca, para la cual usaremos la interfaz eth0 asignada a la subnet 130.1.0.0/16.

La red de repositorio de almacenamiento o también llamada Red iSCSI por el protocolo que es usado para asignar los discos duros virtuales al Nodo, para esta subnet se asigna la interfaz eth1 a la subnet 192.168.0.0/24.

La red de HeartBeat, es la red de datos que utilizamos para intercomunicar los dos Nodos del clúster exclusivamente y a través de ellos se envían los mensajes de estados de los elementos del clúster y además la sincronización de los repositorios de almacenamiento, red asignada 192.168.2.100/24.

3.4.3 Infraestructura e Interconexión del Clúster.

Se ha buscado que la conectividad de cada uno de los recursos físicos del Clúster sea eficaz y de ser posible se cuente con redundancia, para que el sistema tenga siempre disponibles los elementos para el óptimo funcionamiento, para lo cual se ha configurado los nodos de la siguiente manera; como se describe en la Figura 3.12, los repositorios de almacenamiento se asignan a los Nodos a través del protocolo iSCSI, en una red de datos exclusiva para el almacenamiento de datos.

Además se ha configurado una protección adicional creando alta disponibilidad de NAS conectándolos entre sí, de tal manera los Nodos apuntan a una IP flotante creada del clúster de NAS, y cada Nodo ubicado en los centros de cómputo tendrá acceso a sus discos todo el tiempo.

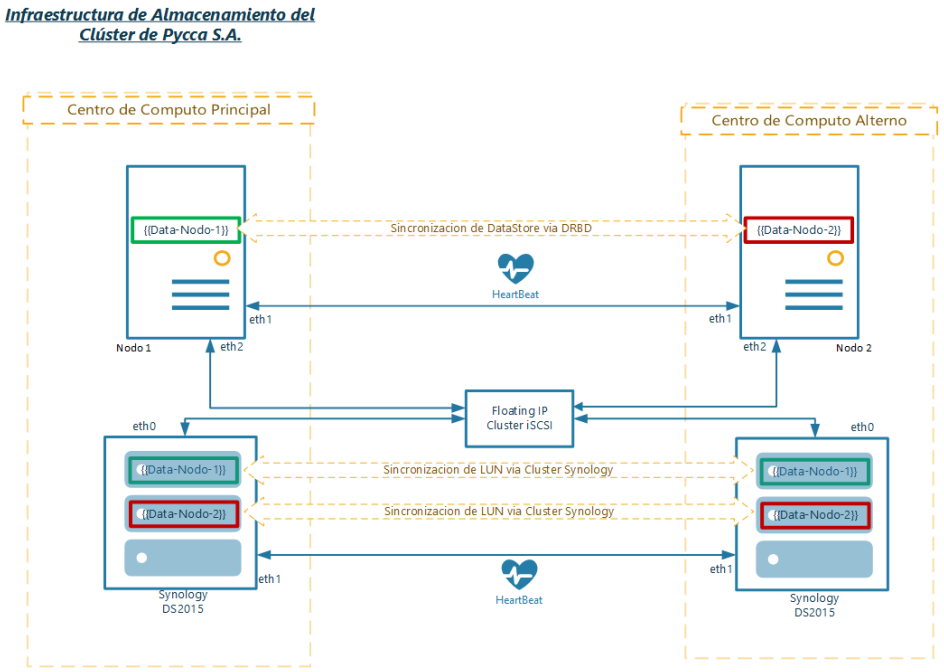


Figura 3.12 Interconexión Almacenamiento Clúster

Tanto el HeartBeat y la red iSCSI entre ambos centros de cómputo son comunicados a través del enlace de radiofrecuencia por lo cual se ha configurado ambos equipos en modo puente.

Con lo que se obtiene una comunicación directa al mismo nivel de subred y ambos nodos pueden transmitir mensajes de estados entre ellos y la sincronización de los repositorios de datos.

Como vimos en el subcapítulo 3.4.1 este enlace nos provee una tasa de transferencia TX de 216 Mbps y un RX de 180 Mbps, escenario óptimo para que la transmisión del HeartBeat sea exitosa, en caso de que la tasa de transferencia disminuya podría provocar que el clúster se comporte de manera errónea.

3.4.4 Ubicación de los equipos que componen el proyecto.

La contingencia que se busca en este proyecto tiene el alcance de cubrir fallas experimentadas por cualquiera de los elementos del clúster, por tal razón hemos ubicado 50% de los elementos del clúster en cada uno de los centros de cómputo respectivamente, separados a 1.2 km de distancia, de tal manera si el centro de cómputo principal que se muestra en la Figura 3.13 se ve afectado por algún problema eléctrico o de otra naturaleza que provoque que dicho centro de cómputo quede inoperativo empieza a procesar el centro de cómputo secundario mostrado en la Figura 3.14 de manera inmediata.

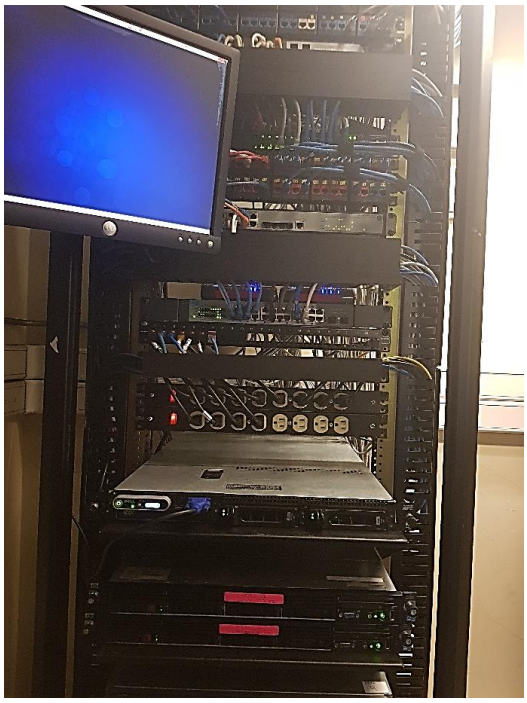


Figura 3.13 Nodo Principal

En la Figura 3.14 se puede observar la ubicación del Nodo secundario del clúster, este nodo cuenta con todos los elementos necesarios para procesar los requerimientos del clúster en el momento que el nodo primario falle.

Figura 3.14 Nodo Secundario

Uno de los elementos importantes del Clúster es el NAS Synology DS2015xs que se puede apreciar en la Figura 3.15, que es utilizado para que los Nodos obtengan su repositorio de almacenamiento, el cual está ubicado en el gabinete principal protegido por un UPS para controlar fallas eléctricas y variaciones de voltaje.

Figura 3.15 NAS Synology DS2015xs+

Como elementos innovadores del clúster se ha utilizado las Radios de marca Ubiquiti Modelo Rocket M5 de frecuencia de 5 GHZ, estas son utilizadas para el enlace de radiofrecuencia que conecta ambos centros de cómputo, el principal con el secundario. Estas radios están ubicadas en unas torres de metal construidas en la terraza de cada una de las localidades, como se puede apreciar en la Figura 3.16, en el Edificio Matriz de Pycca ubicado entre las calles 9 de Octubre y Boyacá, tenemos una torre de 33 metros de Altura, por otro lado en la edificación de contingencia ubicado entre las calles Boyacá y Piedrahita tenemos una torre de 30 metros de Altura.

Figura 3.16 Torre Radioenlace Clúster

CAPÍTULO 4

4. IMPLEMENTACIÓN DE LA SOLUCIÓN.

En esta sección se describe el proceso de implementación del clúster, las configuraciones de todos los elementos del mismo, y la verificación de la correcta ejecución de los servicios en el Clúster.

4.1 Configuración de los equipos del Clúster de Linux.

Como primer paso de la implementación del proyecto vamos a proceder a configurar cada uno de los dispositivos que conforman el clúster, tanto como los nodos con su sistema operativo y sus servicios, equipos de comunicaciones, y equipos de almacenamiento.

4.1.1 Preparación de los Nodos del Clúster.

Los servidores que formarán parte del clúster conocidos como nodos van a ser preparados con el sistema operativo Linux CentOS 6.7 de 64 Bits en modo Minimal Server, con lo cual se instalarán con los paquetes necesarios para que el sistema operativo se encuentre operativo sin problemas. Posterior a eso se instalarán los paquetes necesarios para la realización de este proyecto, tanto los paquetes de los servicios que proveerá el clúster y los paquetes que servirán para configurar el clúster.

Como primer punto se instalan los paquetes de configuración y administración del clúster, el Stack de Pacemaker, CMAN y Corosync.

Posterior a la instalación del Stack de clúster se instalarán los paquetes necesarios para los repositorios de datos a través de iSCSI y la configuración necesaria para la asignación de sus discos a través del protocolo de red.

Como parte de la sincronización de los datos se instalarán los paquetes binarios del programa DRBD, el cual de manera semisincrónica transportará los datos del repositorio de almacenamiento principal al secundario.

A continuación se procede a instalar los paquetes necesarios para los servicios que el clúster va a proveer, motor de base de datos MySQL, Recursos compartidos Samba y Recursos Web Apache.

Culminado la etapa de instalación de los paquetes y programas necesarios se procede a configurar con el programas **#crm** el Stack de Clúster para que él sea quien administre todos los recursos y los servicios de ambos nodos y de todo el clúster en sí mismo.

El lector podrá encontrar los comandos detallados del proceso de configuración en el Anexo B del documento, sin embargo a continuación mostramos el resultado final de la configuración del Stack del Clúster:

crm(live)configure# show

node nodo1

node nodo2

*primitive p_drbd_mysql ocf:linbit:drbd *

*params drbd_resource=cluster_res.res *

*op monitor interval=15s *

meta

*primitive p_fs_mysql Filesystem *

params device="/dev/drbd1" directory="/var/lib/mysql_drbd" fstype=ext4

*primitive p_ip_mysql IPaddr2 *

params ip=130.1.49.20 cidr_netmask=16 nic=eth0

*primitive p_mysql mysql *

*params binary="/usr/libexec/mysqld" config="/etc/my.cnf" datadir="/var/lib/mysql_drbd/data" pid="/var/run/mysqld/mysqld.pid" socket="/var/lib/mysql/mysql.sock" user=mysql group=mysql additional_parameters="--bind-address=130.1.49.20" pid-file="/var/run/mysqld/mysqld.pid" *

*op start interval=0 timeout=120s *

*op stop interval=0 timeout=120s *

*op monitor interval=20s timeout=30s *

meta

group g_mysql p_fs_mysql p_ip_mysql p_mysql

*ms ms_drbd_mysql p_drbd_mysql *

meta master-max=1 master-node-max=1 clone-max=2 clone-node-max=1 notify=true

colocation c_mysql_on_drbd inf: g_mysql ms_drbd_mysql:Master

order o_drbd_before_mysql inf: ms_drbd_mysql:promote g_mysql:start

*property cib-bootstrap-options: *

*have-watchdog=false *

*dc-version=1.1.15-5.el6-e174ec8 *

*cluster-infrastructure=cman *

*stonith-enabled=false *

no-quorum-policy=ignore

*rsc_defaults rsc-options: *

resource-stickiness=200

4.1.2 Configuración de equipos de redes LAN y WAN.

Como primer paso básico en la configuración de los equipos de red procedemos a la identificación de los equipos en la red, en base la dirección TCP/IPv4 de cada uno de los elementos, tanto los nodos en la LAN como las Radios en la WAN.

Red LAN

La Tabla 4 muestra el direccionamiento IP de la red LAN de Almacenes Pycca, seguido se detalla la Tabla 5 que presenta el direccionamiento IP de la red de almacenamiento de datos iSCSI y finalmente la Tabla 6 presenta el direccionamiento de la red de HeartBeat, configurada para la comunicación entre los dos Nodos exclusivamente.

Hostname Nodo	Red LAN Pycca 130.1.0.0/16
nodo1.public.cluster	130.1.49.21
nodo2.public.cluster	130.1.49.22
cluster.public.cluster	130.1.49.20

Tabla 4: Direccionamiento IP LAN Pycca

Hostname Nodo	Red iSCSI Pycca 192.168.0.0/24
nodo1.iscsi.cluster	192.168.0.21
nodo2.iscsi.cluster	192.168.0.22

Tabla 5: Direccionamiento IP iSCSI

Hostname Nodo	Red HeartBeat Pycca 192.168.2.0/24
nodo1.private.cluster	192.168.2.101
nodo2.private.cluster	192.168.2.102

Tabla 6: Direccionamiento HeartBeat

Red WAN

Las radios utilizadas para el proyecto fueron configurados en tipo Bridge, la Tabla 7 describe el direccionamiento IP de la Red WAN configurado en el Radioenlace.

Hostname Radio	Red LAN Pycca 130.1.0.0/16
radio1.cluster	130.1.1.212
radio2.cluster	130.1.1.213

Tabla 7: Direccionamiento IP Radioenlaces

El lector del presente documento podrá encontrar en el Anexo B las configuraciones realizadas en cada una de las radios.

4.1.3 Configuración de los Equipos Clientes del Clúster.

Las dos categorías principales de equipos clientes del Clúster son las cajas o también llamados puntos de venta, y los equipos administrativos del almacén.

Los equipos de Caja son computadoras equipados con sistema operativo Linux CentOS 6.2 32 bits operados por Cajeras utilizadas para la atención a clientes para realizar la venta y cobro de productos.

Estos equipos utilizan dos servicios del servidor de manera esencial, el motor de base de datos MySQL y los archivos compartidos a través de Samba, en la configuración de las cajas para encaminar sus peticiones al Clúster se actualizó una tabla local llamada **posconfig** ubicada en el motor de base de datos MySQL local de la caja, cambiando la IP del servidor anterior 130.1.1.110 a la IP del clúster 130.1.49.20.

Así mismo se cambió la configuración del archivo **fstab** local de la caja, el cual buscaba los recursos compartidos del servidor 130.1.1.110 y ahora busca los archivos compartidos en el clúster 130.1.49.20.

Con estos cambios en la configuración los aplicativos de la Caja para realizar la venta y cobro de productos enviarán sus solicitudes hacia el Clúster.

Los equipos administrativos de la tienda los cuales son operados por el Gerente de la Tienda, la Secretaria de la Tienda y el personal de Bodega; estos tres equipos utilizan como sistema operativo Windows 7 de 32 Bits y utilizan tres recursos del servidor, el Motor de bases MySQL, los recursos compartidos y el motor de páginas web Apache para monitoreo en línea de las estadísticas de venta.

Para proceder con el nuevo enrutamiento de solicitudes de los equipos administrativos hacia el clúster se modificó archivos de configuración o también llamadas archivos INI por el tipo de extensión que utilizan.

Los archivos modificados son: **indigo.ini, ventas.ini, reportes.ini,** estos archivos contienen la dirección IPv4 del servidor al cual van a establecer la conexión para operar, se realizó el cambio de la IP 130.1.1.110 a la IPv4 del clúster 130.1.49.20.

Con esta nueva configuración los equipos administrativos enviarán sus peticiones hacia el clúster para usar los servicios y recursos necesarios para gestionar.

4.2 Implementación del Clúster de Linux.

Luego de haber configurado cada uno de los nodos del clúster con sus respectivos servicios y recursos como son MySQL, Apache y Samba, y para la operativa del clúster el stack de Pacemaker, cman, y Corosync, continua la etapa de orquestar el arranque y sincronización de cada uno de los recursos para el correcto funcionamiento del clúster, ya que el orden en el cual deben levantarse los servicios es esencial para el funcionamiento del mismo.

De manera general lo que se busca es que el orden en que los servicios deben ser levantados es el siguiente:

1) El Sistema operativo CentOS de 64 bits que es la base de operaciones del Nodo, junto con todo el direccionamiento IP configurado para las 3 redes en la que va a operar, HeartBeat, LAN y iSCSI.
2) El servicio iSCSI el cual nos ayuda a que los Nodos se conecten al NAS para que los LUNs sean asignados y que los mismos sean configurados como los repositorios de almacenamiento usados por los servicios.
3) Los recursos de operación del clúster o también llamado STACK del clúster los programas Pacemaker que ayuda a la comunicación entre los nodos, CMAN quien se encarga de enviar mensajes de estado entre los nodos y el Quorum, y Corosync el cual administra los servicios que el Clúster va a proveer a través de una IP flotante o también llamada IP del Clúster.

4) El servicio DRBD que utilizamos para la sincronización de los repositorios de almacenamiento.
5) Los servicios que ofrece el Clúster, el Motor de base de datos MySQL, el servicio Web de Apache y el servicio de recursos compartidos Samba.

De manera que se pueda garantizar la integridad y sincronización de los datos del clúster. Para lograr esto luego de haber instalado y configurado cada uno de los programas necesarios hacemos configuraciones en las reglas de arranque del sistema operativo **inittab** e **init.d,** donde configuramos que servicio arranca previo a otro.

4.3 Monitoreo y Revisión del funcionamiento del clúster de Linux.

Una vez que el sistema clúster se encuentra operativo y está gestionando los requerimientos solicitados por los equipos cliente el administrador debe revisar que los requerimientos están siendo gestionados de manera correcta y que los elementos del clúster se encuentren en línea y operando para lo cual vamos a utilizar dos programas ejecutados en línea de códigos llamados **pcs** y **drbd-overview** respectivamente.

Como podemos ver en la Figura 4.1, al ejecutar el comando **#pcs status** nos brinda una visión general del estado del clúster a nivel de software, verificando el estado de los equipos nodos, de los servicios utilizados para la operación del clúster y de los recursos que el clúster provee.

#pcs status (este comando puede ser ejecutado en cualquier nodo miembro del clúster)

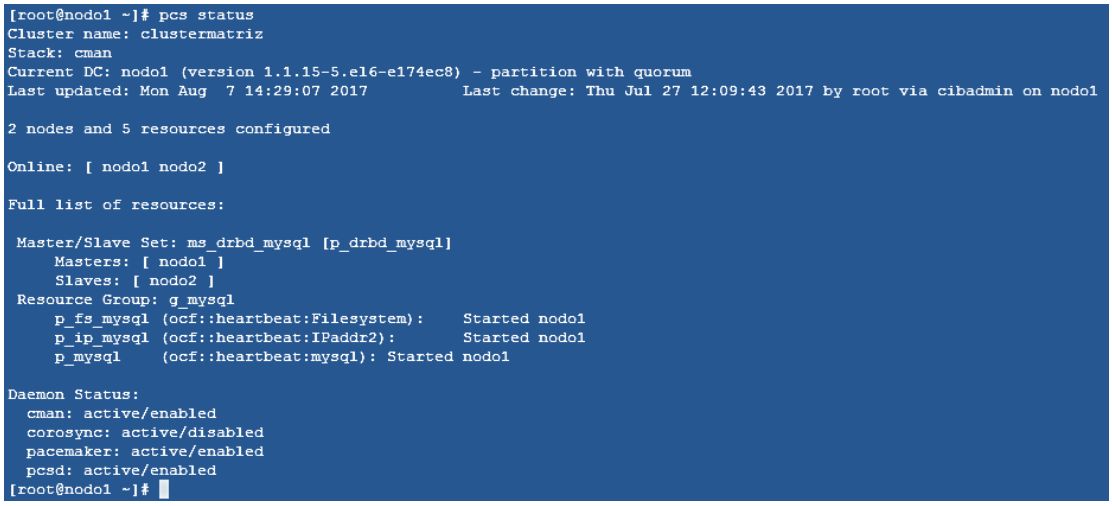


Figura 4.1 Monitoreo del Clúster (PCS)

Observamos el nombre asignado al clúster **clustermatriz** y su características, está asignado con un quorum para monitoreo permanente de los datos de los nodos, la cantidad de los nodos asignados al clúster y su estado **[nodo1 nodo2 online].**

Muestra también los recursos que debe controlar como el de sincronización de discos **DRBD** y así mismo muestra cual es el nodo que actúa como master y secundario en la replicación y como datos adicionales muestra el estado de los servicios usados por el clúster.

Otros comandos esenciales para el monitoreo del clúster son los usados para verificar la sincronización de los dos repositorios de almacenamiento tanto el asignado al nodo 1 como al nodo 2.

Los comandos a usar son **drbd-overview** y el comando **cat /proc/drbd,** con los cuales podemos observar el estado real en línea de la sincronización.

La Figura 4.2 muestra la sincronización en línea, entre los repositorios de almacenamiento principal hacia el secundario, mostrando los porcentajes de progreso, velocidad de copiado y estatus de ambos repositorios.

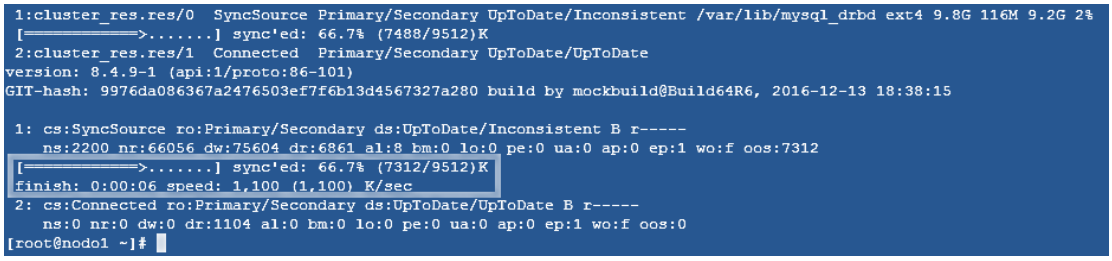


Figura 4.2 Monitoreo sincronización (DRBD)

CAPÍTULO 5

5. PRUEBAS Y ANÁLISIS DE RESULTADOS.

En el siguiente capítulo se describen las pruebas de desempeño realizadas al Clúster de Alta Disponibilidad, los procesos de control y verificación, y el análisis de los resultados obtenidos, todas estas pruebas realizadas en un ambiente de producción dentro de la infraestructura de Almacenes Pycca S. A.

5.1 Pruebas del Clúster de Linux.

Una vez que hemos verificado que el Clúster de Alta Disponibilidad se encuentra operativo y procesando los requerimientos de los equipos cliente, se procede con tres pruebas importantes donde se logra simular y medir el desempeño del sistema clúster en caso de presentarse un fallo.

5.1.1 Failover.

El Failover es un estado del clúster, en el cual se experimenta un fallo crítico de un nodo o de algún elemento esencial del mismo, el cual provoca que los recursos que ofrece el clúster sean migrados desde el nodo principal al nodo secundario.

Regularmente se da cuando el nodo principal sufre una falla a nivel de hardware, ya sea falla eléctrica o daño de un elemento físico del equipo, esto provoca que su operación quede interrumpida.

En la Figura 5.1 podemos observar a nivel de registros como la sincronización de repositorios de datos (DRBD), determina interrumpida la sincronización de los datos y cierra la conexión.

Con lo cual da por terminado el clúster de sincronización y se desencadenan la migración de recursos entre los nodos.

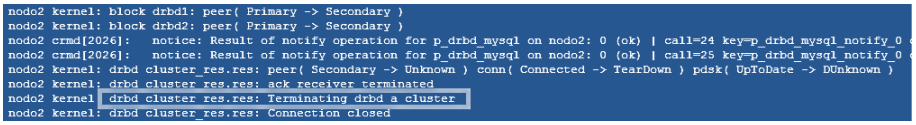


Figura 5.1 Failover DRBD

A partir de este momento el nodo secundario pasa a ser el nodo principal del clúster, adquiriendo todos los recursos del sistema, siendo asignados al nodo secundario el rol de servicios.

La IP flotante del clúster y el rol master con el quorum del sistema clúster de alta disponibilidad. Una vez configurado el nodo secundario como principal empieza a procesar todos los requerimientos de los equipos cliente.

En la Figura 5.2 se puede observar el status del clúster, el cual indica que el Nodo 2 es asignado como Nodo principal del clúster.

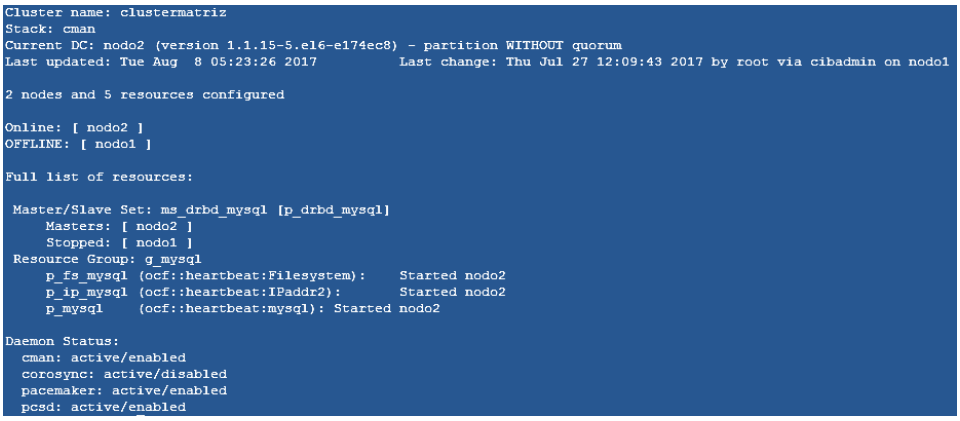


Figura 5.2 Failover satisfactorio

5.1.2 Switchover.

El Switchover es una técnica utilizada por los administradores del sistema clúster, que consiste en migrar los recursos entre los nodos del clúster de manera manual y controlada; regularmente esta técnica se utiliza para brindar mantenimiento a los equipos, o realizar actualizaciones necesarias de manera coordinada.

El proceso consiste en enviarle la orden al nodo primario que detenga todos los servicios necesarios que el clúster utiliza para operar, lo cual coacciona a que todos los recursos sean migrados al nodo secundario.

El programa que es utilizado para este proceso es el PCS, con los parámetros expuestos a continuación: **#pcs cluster stop nodo1** [5]

Una vez ejecutado el comando, los recursos son asignados al nodo secundario y el administrador podrá realizar los trabajos necesarios en el nodo primario.

Para reintegrar el nodo primario al clúster, se debe levantar los servicios necesarios para que el nodo pueda ser miembro del clúster, utilizando el mismo programa PCS con el que fue retirado del sistema, adicionando los siguientes parámetros: **#pcs cluster start nodo1.** [18]

5.1.3 Split-Brain.

Un estado que puede presentarse durante el funcionamiento del clúster es el escenario de Split-Brain. Consiste en que ambos nodos intentan adquirir el rol de nodo primario y procesar los requerimientos de los equipos cliente.

Una de las posibles causas para que se genere este escenario es la pérdida de conexión entre los nodos y la falta de sincronización del Quorum. Lo cual provoca que el clúster se divida, y cada una de las particiones de nodos, asuma que es única, e intenta asignarse los recursos del clúster asimismo y además activar los servicios del clúster.

En la Figura 5.3 se puede observar de qué manera se asienta en los archivos de registro del Nodo 1 que se ha detectado la presencia de un estado de Split-Brain en el Clúster y que los requerimientos de los clientes serán rechazados.

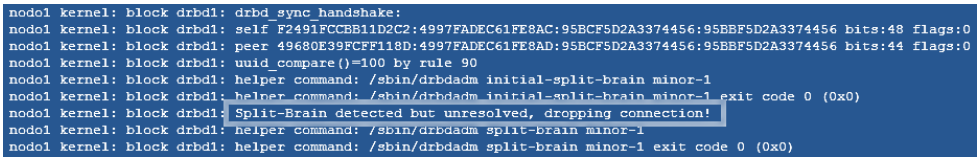


Figura 5.3 Detección de Split-Brain

Cuando el escenario de Split-Brain es detectado debe ser solucionado manualmente por el administrador del clúster. De manera conceptual se debe tomar la decisión de forzar a que uno de los nodos actúe como secundario, para que los datos que sean diferentes versus el nodo primario sean descartados, una vez establecida la jerarquía el clúster comenzara a sincronizar nuevamente los datos desde el nodo primario al nodo secundario. Por tal motivo esta acción no debe ser automática, ya que el administrador debe evaluar el rol de cada uno de los nodos bajo las condiciones presentadas. En la Figura 5.4 se puede observar en el registro del Nodo 1 como el clúster ha sido recuperado tras presentarse el escenario de Split-Brain, posterior a esta operación el clúster volverá a estar operativo y los datos sincronizados entre sus nodos.

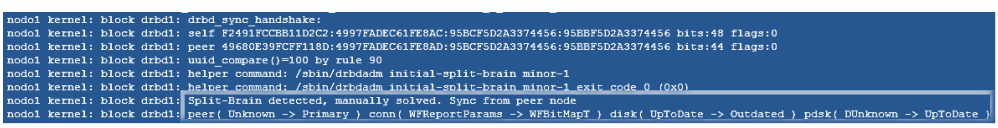


Figura 5.4 Split-Brain Solucionado

5.2 Análisis de resultados

Durante la etapa de análisis de resultados se utiliza la herramienta Wireshark, una aplicación que brinda la posibilidad de analizar los paquetes de red en tiempo real, además de permitir analizar individualmente los protocolos y bytes trasmitidos en la red de datos.

Haciendo uso de esta herramienta, en la Figura 5.5 se muestra como se registra a nivel de bytes la retransmisión fallida de los mensajes de estado entre los nodos, el sistema clúster intenta realizar este proceso a cada momento, desde el nodo principal al nodo secundario y viceversa.

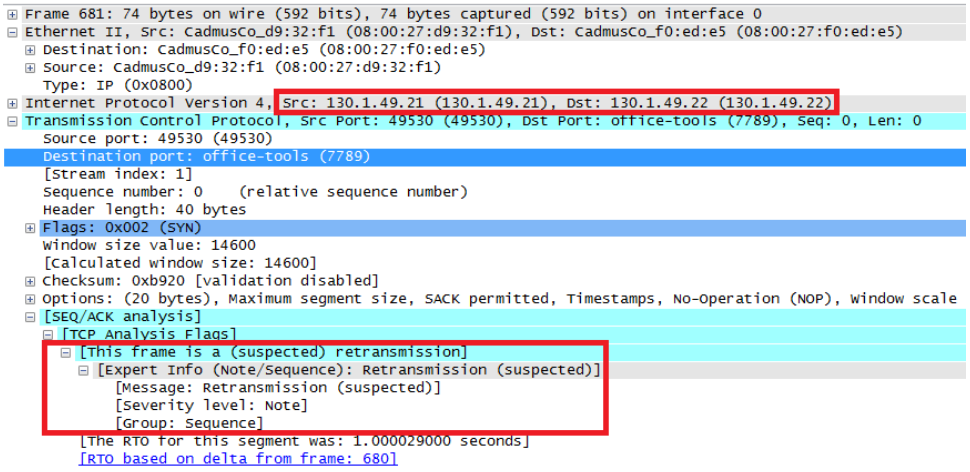


Figura 5.5 Retransmisión fallida Clúster

Luego de que los paquetes de retransmisión son catalogados como fallidos, el sistema clúster determina que el nodo principal está fuera de línea.

Tal como se muestra en la Figura 5.6, el nodo secundario registra que el nodo principal esta inoperativo.

Figura 5.6 Nodo Principal Offline

Posterior a esto se inicia la migración de los recursos desde el nodo principal al nodo secundario.

Hemos registrado que el tiempo que toma realizar este traspaso de rol entre el nodo primario al secundario, tiene una duración de aproximadamente 5 segundos. Una duración de tiempo ínfimo en comparación a los valores presentados en la Tabla 1: Fallo vs Tiempo de Solución, donde se detallan los tiempos aproximados de solución ante la presencia de un fallo informático.

CONCLUSIONES Y RECOMENDACIONES

Con la implementación del presente proyecto se ha logrado alcanzar el objetivo principal el cual es reducir el tiempo de inactividad de los servicios que provee el clúster de alta disponibilidad a un tiempo máximo de 5 segundos en el escenario de presentarse una falla tanto física como de software en el nodo principal del clúster.

Gracias a esto los equipos cliente como son los Puntos de Venta (POS) y los computadores administrativos no experimentan en ningún momento la interrupción de los servicios necesarios para su operativa diaria, las ventas no se han visto interrumpidas y tampoco las atenciones al cliente, con los cual la experiencia de usuario se ha mantenido de manera óptima.

El enlace de radiofrecuencia responde de manera eficaz y sin interrupciones, los indicadores de Tasas de Transferencias TX 216 Mbps y RX 180 Mbps; Potencia de –47 / -46 dBm; Ancho de Canal 40 MHz descritos en el subcapítulo 3.4.1 verifica que dicho radioenlace nos provee del recursos suficiente para que el HeartBeat entre ambos nodos sea eficaz y la sincronización de los datos realizada a través de la herramienta DRBD y configurada de tipo Semisincrónica nos ha asegurado que la información se encuentre integra en ambos extremos del clúster.

Esta solución ha sido aceptada gratamente con la administración de almacenes Pycca y a si mismo se ha sugerido el despliegue de la misma en varias tiendas de la cadena empresarial, en especial se ha sugerido la implementación para las tiendas más importantes de Almacenes Pycca.

Las redes de telecomunicaciones de las Tiendas de Almacenes Pycca son heterogéneas entre sí, determinado por su ubicación geográfica e instalaciones, algunas utilizan enlaces de Radiofrecuencia, otras Fibra Óptica, algunas con redundancia de anillo en Fibra Óptica otras con redundancia en enlaces de Radiofrecuencia e incluso con Proveedores diferentes, por consiguiente la capacidad de cómputo de los servidores depende de la demanda.

Por lo cual se recomienda la continuidad de este proyecto implementándolo en escenarios donde se involucre proteger tiendas remotas de mayor distancia y con recursos más limitados, principalmente porque brindar el soporte a tiendas muy alejadas de la matriz se vuelve proporcionalmente complicado, a mayor distancia de separación de la tienda matriz el soporte es menos frecuente. Así mismo en cuanto a telecomunicaciones se recomienda implementar clúster más complejos utilizados anillos de fibra de última milla para las tiendas que no tengan línea de vista ya que se encuentren en ciudades separadas.

BIBLIOGRAFÍA

[1] Pycca S.A., «Info Pycca,» [En línea]. Available: https://www.pycca.com/nuestra-empresa/quienes-somos.

[2] NeoStuff, «Revista de Tecnología,» [En línea]. Available: https://www.neostuff.net/respaldar-informacion-disco-externo-almacenamiento-la-nube/.

[3] Red Hat Inc, «Red Hat Cluster Suite,» 2007. [En línea]. Available: https://www.centos.org/docs/5/html/Cluster_Suite_Overview/index.html.

[4] M. Resman, CentOS High Availability, BIRMINGHAM - MUMBAI: Packt Publishing, 2015.

[5] K. E. Campos Bustos y J. L. Vera Chavez, «Diseño e implementación de una solución de alta disponibilidad usando clúster y virtualización de servidores web y de bases de datos para las aplicaciones de la FIEC,» Escuela Superior Politecnica del Litoral ESPOL, Guayaquil, 2015.

[6] Ubiquiti Networks, «Radio Rocket M Base Station,» [En línea]. Available: https://www.ubnt.com/downloads/datasheets/rocketm/RocketM_DS.pdf.

[7] Ubiquiti Networks, «Tecnologia airMAX,» [En línea]. Available: https://dl.ubnt.com/datasheets/airmax/UBNT_DS_airMAX_TDMA.pdf.

[8] IEEE, «IEEE 802.11a Standard,» [En línea]. Available: http://ieeexplore.ieee.org/servlet/opac?punumber=4140841.

[9] IEEE, «OFDM for Optical Communications,» [En línea]. Available: http://ieeexplore.ieee.org/document/4785281/.

[10] IEEE, «Implementation of IEEE 802.11a Wireless LAN,» [En línea]. Available: http://ieeexplore.ieee.org/document/4682256/.

[11] LINBIT, «MySQL High Availability on Pacemaker Cluster Stack,» [En línea]. Available: https://www.linbit.com/en/resources/technical-publications/108-applications/528-mysql-high-availability-on-the-pacemaker-cluster-stack/.

[12] LINBIT, «Data Replication across Geo-Clusters via DRBD,» [En línea]. Available: https://www.linbit.com/en/resources/102-disaster-recovery/613-data-replication-across-geo-clusters-via-drbd-8/.

[13] Linux Journal, «Xen Virtualization and Linux Clustering,» [En línea]. Available: http://www.linuxjournal.com/article/8812.

[14] Hewlett Packard Enterprise, «HP ProLiant DL360 G6 Server,» [En línea]. Available: http://h20564.www2.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-c01711627.

[15] Synology Inc., «DS2015xs+ Datasheet,» [En línea]. Available: https://global.download.synology.com/download/Document/DataSheet/DiskStation/15-year/DS2015xs/Synology_DS2015xs_Data_Sheet_esn.pdf.

[16] Intel Corporation, «Ethernet X520,» [En línea]. Available: https://www.intel.la/content/dam/doc/product-brief/ethernet-x520-server-adapters-brief.pdf.

[17] Netgear Inc., «ProSAFE 10-Gigabit Ethernet Smart Managed Switches,» [En línea]. Available: http://www.downloads.netgear.com/files/GDC/datasheet/en/XS712T-XS728T.pdf.

[18] ClusterLabs, «Cluster Pacemaker,» [En línea]. Available: http://clusterlabs.org/doc/en-US/Pacemaker/1.1/html/Clusters_from_Scratch/_perform_a_failover.html.

[19] Alcance Libre, «CentOS Cluster Heartbeat,» [En línea]. Available: http://www.alcancelibre.org/staticpages/index.php/como-cluster-heartbeat-centos.

[20] Alcance Libre, «Llave Publica SSH,» [En línea]. Available: http://www.alcancelibre.org/staticpages/index.php/como-ssh-clave-publica.

[21] LINBIT, «iSCSI Highly Available with DRBD,» [En línea]. Available: https://www.linbit.com/en/resources/technical-publications/100-storage/548-highly-available-iscsi-with-drbd-and-pacemaker/.

ANEXOS

Anexo A: Datos Estadísticos del Escenario actual

1. Tabla de Ventas por Hora en las Tiendas de Almacenes Pycca – año 2014

		CENTRO	ROTONDA	POLICENTRO	SUR	SAN MARINO	MALL DEL SOL ANEXO
10:00	525	89	1	0	0	0	0
11:00	11,253	1,819	896	455	835	75	0
12:00	33,004	7,550	3,191	2,182	2,825	327	6
13:00	51,281	11,281	4,012	3,368	5,086	931	402
14:00	67,033	14,331	4,553	4,328	6,241	1,188	402
15:00	80,153	16,326	5,529	5,549	7,215	1,480	699
16:00	102,898	22,619	6,282	6,962	9,903	2,288	699
17:00	127,901	27,421	7,360	8,268	12,334	2,635	702
18:00	155,805	34,753	10,205	10,012	14,970	3,100	1,189

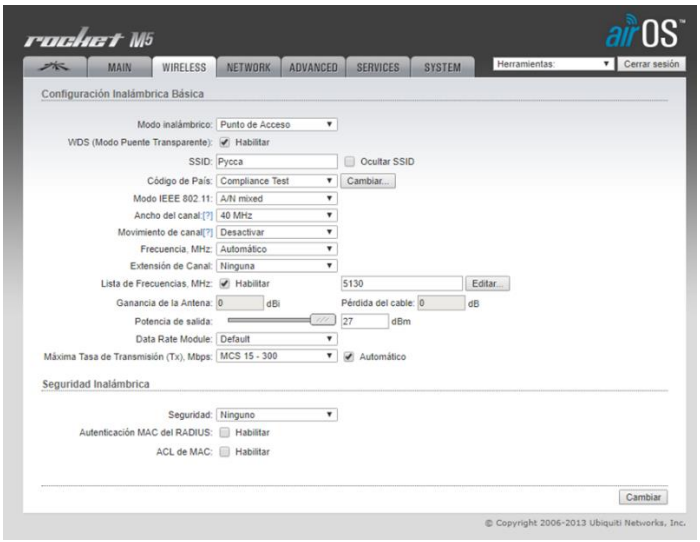
2. Tabla de cantidad de Atenciones a usuarios en el área de Crédito Pycca

06-DIC	484	0	5	17	42	57
07-DIC	463	0	0	7	21	40
TOTAL	***3,592***	***0***	***41***	***212***	***237***	***280***
Almacén						
01-DIC	562	0	2	36	69	40
02-DIC	587	0	8	34	24	45
03-DIC	469	0	0	27	0	0
04-DIC	603	0	18	64	35	49
05-DIC	424	0	8	27	46	49

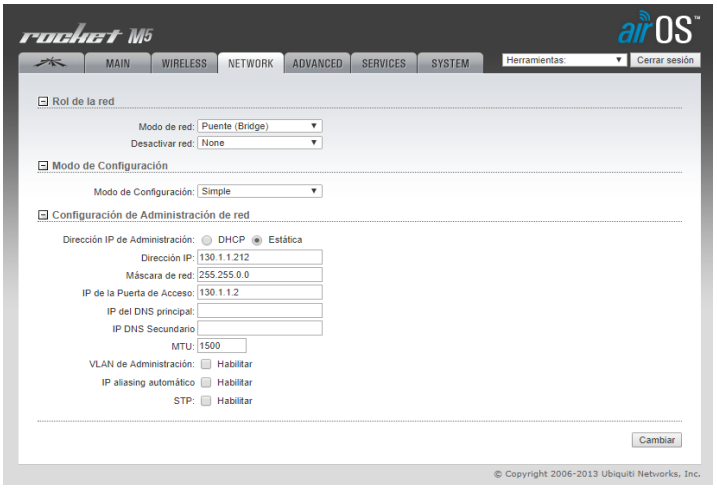
Anexo B: Procesos de Instalación y configuración de archivos

3. Configuración del enlace de Radiofrecuencia

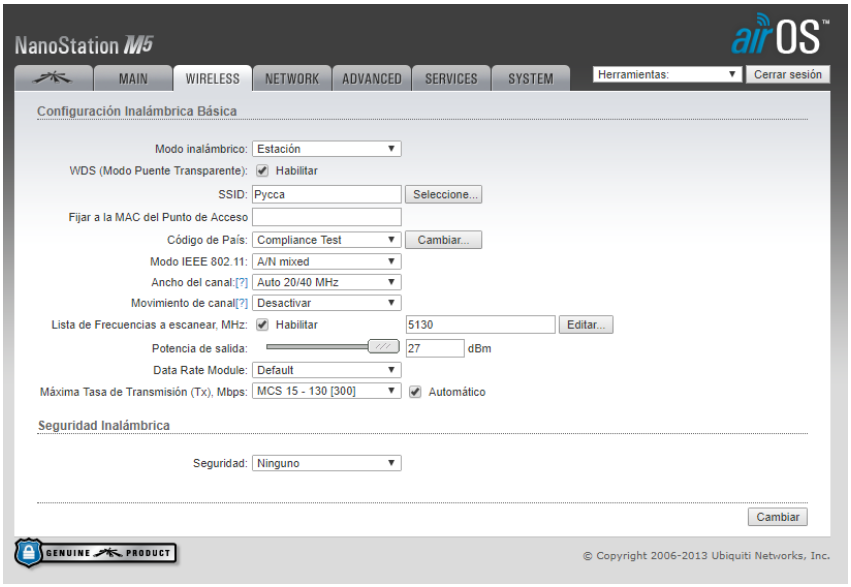
3.1. Configuración del espectro radioeléctrico de la Radio #1



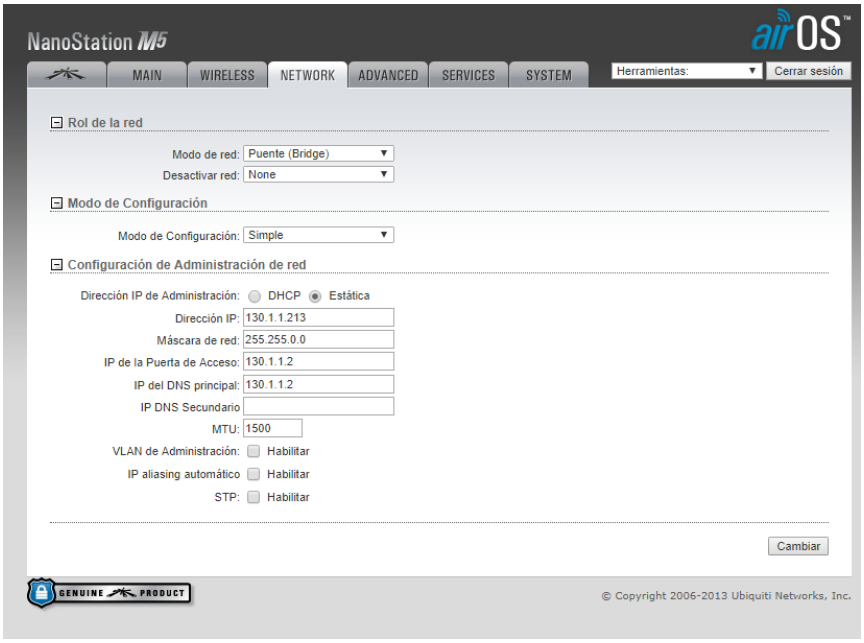
3.2. Configuración de la red LAN en la Radio #1



3.3. Configuración del espectro radioeléctrico de la Radio #2



3.4. Configuración de la red LAN en la Radio #2



4. Configuración del Stack del Clúster

```
## Creación Recurso DRBD
primitive p_drbd_mysql ocf:linbit:drbd \
params drbd_resource="clusterdb_res.res" \
op monitor interval="15s"
ms ms_drbd_mysql p_drbd_mysql \
meta master-max="1" master-node-max="1" \
clone-max="2" clone-node-max="1" \
notify="true"

##Creación Recurso FileSystrem
primitive p_fs_mysql ocf:heartbeat:Filesystem \
    params device="/dev/drbd1" directory="/var/lib/mysql_drbd" \
        fstype="ext4"

## Creación de Recurso IP Clúster MySQL
primitive p_ip_mysql ocf:heartbeat:IPaddr2 \
    params ip="130.1.49.20" cidr_netmask="16" nic="eth0"
```

```
## Creación de Recursos Motor MySQL
primitive p_mysql ocf:heartbeat:mysql \
 params binary="/usr/sbin/mysqld" \
 config="/etc/my.cnf" \
 datadir="/var/lib/mysql_drbd/data" \
 pid="/var/run/mysqld/mysql.pid" \
 socket="/var/lib/mysql/mysql.sock" \
 user="mysql" group="mysql" \
 additional_parameters="--bind-address=130.1.49.20" \
 op start timeout=120s \
 op stop timeout=120s \
 op monitor interval=20s timeout=30s

## Agrupando Recursos MySQL
crm(live)configure# group g_mysql \
 p_fs_mysql p_ip_mysql p_mysql

## Asignando Motor MySQL dentro del DRBD
colocation c_mysql_on_drbd inf: g_mysql ms_drbd_mysql:Master

## Orden de Arranque de Servicios
order o_drbd_before_mysql inf: ms_drbd_mysql:promote g_mysql:start

## Guardar y Salir
commit && exit
```