

UNIVERSIDAD SAN FRANCISCO DE QUITO

Colegio de Ciencias e Ingenierías

**Implementación de Balanceo de Carga de Microsoft Exchange 2013
mediante equipos del fabricante F5 Networks en la empresa Nube Digital**

Marcelo Francisco Mena Lalama

Fausto Vasco, MBA, Director de Tesis

Tesis de grado presentada como requisito
para la obtención del título de Licenciado en Redes y Sistemas Operativos

Quito, agosto de 2015

Universidad San Francisco de Quito

Colegio de Ciencias e Ingenierías

HOJA DE APROBACIÓN DE TESIS

Implementación de Balanceo de Carga de Microsoft Exchange 2013 mediante equipos del fabricante F5 Networks en la empresa Nube Digital

Marcelo Francisco Mena Lalama

Fausto Vasco, MBA
Director de la tesis

Edwin Arévalo, Ing.
Revisor de la Tesis

Ney Acosta, Ing.
Revisor de la Tesis

César Zambrano, Ph.D.
Decano del Colegio de Ciencias e
Ingenierías

Quito, agosto de 2015

© DERECHOS DE AUTOR

Por medio del presente documento certifico que he leído la Política de Propiedad Intelectual de la Universidad San Francisco de Quito y estoy de acuerdo con su contenido, por lo que los derechos de propiedad intelectual del presente trabajo de investigación quedan sujetos a lo dispuesto en la Política.

Asimismo, autorizo a la USFQ para que realice la digitalización y publicación de este trabajo de investigación en el repositorio virtual, de conformidad a lo dispuesto en el Art. 144 de la Ley Orgánica de Educación Superior.

Firma: _____

Nombre: Marcelo Francisco Mena Lalama

C. I.: 171481783-8

Lugar: Quito

Fecha: agosto de 2015

DEDICATORIA

Este trabajo de tesis, lo dedico de todo corazón primeramente a mis padres y hermanas, que siempre me han apoyado para cumplir mis metas y han estado pendientes de cada uno de mis pasos. Segundo, a mis hijos, para que sea un ejemplo a seguir y ellos puedan alcanzar todas sus metas y obtengan muchos logros siempre. También, lo dedico a mi esposa y compañera de vida, quien me ha apoyado durante mi trayectoria en la Universidad y durante el desarrollo de este trabajo. Finalmente, una dedicatoria especial a Elizabeth Rosero, mi mejor amiga, que siempre me ha apoyado en todos los temas de estudio, trabajo y aprendizaje en los que hemos desempeñado juntos.

AGRADECIMIENTOS

Agradezco a mis profesores, docentes y compañeros de la USFQ por las buenas enseñanzas, el excelente trato y la amistad durante mi carrera. También un agradecimiento eterno a mis padres por haber confiado en mí en todo momento y por darme una educación tan completa y en una institución tan prestigiosa, a mis hermanas por apoyarme en todo momento y presionarme siempre para mejorar y seguir adelante. Agradezco también a mi esposa, por estar siempre a mi lado en las buenas y en las malas durante mi carrera en la Universidad San Francisco de Quito y durante la elaboración de mi trabajo de tesis. Y deseo agradecer a Dios, por darme la salud y la fuerza para lograr cumplir con un sueño tan importante como graduarme.

RESUMEN

En el mundo de hoy, nos enfrentamos a una demanda tecnológica y de servicios web extremadamente alta, por lo que la mayoría de empresas busca maneras de mejorar su infraestructura y otorgar un mejor servicio a sus clientes de forma inmediata, segura y eficaz, teniendo en cuenta siempre la alta disponibilidad, velocidad y seguridad en sus herramientas de trabajo como lo es el correo electrónico.

Mediante esta implementación, se ha mejorado la infraestructura tecnológica del cliente para el envío y recepción de correo mediante una solución escalable de manera transparente, así como facilitar el mantenimiento de los servidores de correo electrónico, para llegar al punto de literalmente eliminar el fuera de servicio al cliente final que ocupa los servicios de correo electrónico de la empresa que solicita esta solución.

Implementando el balanceo de carga del servicio de correo electrónico con un equipo de características específicas para la distribución de carga de forma equitativa, se ha logrado balancear la carga de transacciones de manera distribuida y eficaz a dos servidores de la aplicación de correo electrónico que componen esta solución, para mejorar el servicio y satisfacción de todos los clientes que consumen este servicio, utilizando un certificado digital seguro para una conexión encriptada y realizando un registro de conexiones en los Logs del sistema de balanceo, para mayor facilidad al momento de solventar un problema de ser necesario.

ABSTRACT

In today's world, we are facing an extremely high demand of technology and services; therefore, the majority of companies look for ways to improve their infrastructure and provide their customers with a better service in an immediate, secure and optimal way, keeping always in mind the high availability, fast response and security in their tools such as the e-mail.

Thanks to this deployment, the customer's technological infrastructure for sending and receiving mail has improved, with a transparent scalable solution, as well as the easiness of maintenance of the e-mail servers, getting to a point where the down time of the service being used by the users or the customer requesting this solution has been reduced to a very minimum.

By deploying the load balancing of the e-mail service with a load balancing device, the customer requesting the solution has achieved the even and effective distribution of requests into two different servers which form this solution, in order to improve the service and satisfaction to all the users consuming this service, with the use of a signed digital certificate for a secure encrypted connection, and by recording all the connection logs in the load balancing system, for an easier way of solving a problem when necessary.

TABLA DE CONTENIDO

HOJA DE APROBACIÓN DE TESIS.....	3
© derechos de autor.....	4
Dedicatoria.....	5
Agradecimientos	6
Resumen.....	7
Abstract	8
Tabla de contenido	9
ILUSTRACIONES	11
TABLAS.....	13
1. Introducción.....	14
1.1 Antecedentes.....	15
1.2 Objetivos.....	16
1.2.1 Objetivo General.....	16
1.2.2 Objetivos Específicos.....	16
1.3 Hipótesis	16
1.4 Justificación	16
2. Contexto y marco teórico.....	19
2.1 Servidores	19
2.1.1 Definición	19
2.1.2 Componentes de un servidor	19
2.2 Virtualización.....	20
2.2.1 Definición	20
2.2.2 Virtualización del Servidor	20
2.3 Balanceo de Carga	21
2.3.1 Definición	21
2.3.2 Clúster de servidores	21
2.3.3 Balanceador F5.....	21
2.3.4 TMOS	22
2.3.5 BIG-IP	23
2.3.6 Local Traffic Manager	23
2.3.7 Proxy	23
2.3.8 Full Proxy	23
2.3.9 Elementos de sistema F5.....	24
2.3.9.1 Host Name	24
2.3.9.2 Management Port IP Address.....	24
2.3.9.3 Archive.....	24
2.3.9.4 SSL Certificate	24
2.3.10 Elementos de red F5	25
2.3.10.1 Vlan	25
2.3.10.2 Host	25
2.3.10.3 Interface	25
2.3.10.4 Self IP Address.....	26
2.3.10.5 Routes	26
2.3.11 Elementos de balanceo F5	27
2.3.11.1 Node	27

2.3.11.2	Pool Member.....	28
2.3.11.3	Pool	28
2.3.11.4	Virtual Server	28
2.3.11.5	iRule.....	29
2.3.11.6	Health Monitor.....	30
2.3.11.7	Profile.....	30
2.3.11.7.1	Algoritmos de Balanceo F5	31
2.3.12	Protocolos de comunicación.....	32
2.3.13	Componentes del servicio.....	32
2.3.13.1	Diagrama de red.....	32
2.3.13.2	Centro de datos.....	33
2.3.13.3	Enrutador.....	33
2.3.13.4	Red.....	34
2.3.13.4.1	Redes LAN	34
2.3.13.4.2	Redes WAN.....	35
2.3.13.5	Rack.....	35
2.3.13.6	Raid	35
3.	Metodología.....	37
3.1.1	Plan de implementación de la solución.....	37
3.1.2	Fases de implementación del proyecto	37
3.1.2.1	Estudios preliminares.....	37
3.1.2.2	Recopilación de información.....	38
3.1.2.2.1	Entrevista.....	38
3.1.2.2.2	Entrega directa de documentación.....	41
3.1.2.3	Análisis y Diseño	43
3.1.2.4	Desarrollo y ejecución	45
3.1.2.5	Implementación y Pruebas	45
3.1.2.5.1	Implementación	46
3.1.2.5.1.1	Diagrama de Red	46
3.1.2.5.1.2	Configuración de los elementos básicos del sistema F5	47
3.1.2.5.1.3	Configuración de elementos de red.....	49
3.1.2.5.1.4	Configuración de elementos de balanceo.....	52
3.1.2.5.2	Pruebas.....	63
3.1.2.6	Mantenimiento	65
3.1.3	Verificación de la Hipótesis	65
4.	Análisis de Resultados.....	67
5.	Conclusiones y Recomendaciones	75
5.1.1	Conclusiones	75
5.1.2	Recomendaciones.....	76
6.	Referencias Bibliográficas.....	78

ILUSTRACIONES

Ilustración 1. Vista externa del Cloud Center de Telconet (Telconet S.A., 2015)	39
Ilustración 2. Vista interna del Cloud Center de Telconet (Telconet S.A., 2015).....	39
Ilustración 3. Representación del enlace de internet desde ruteador de borde de Telconet.....	39
Ilustración 4. Rack HP modelo 10642 (DSI Server Racks, Inc, 2015).....	40
Ilustración 5. Servidor blade HP ProLiant BL460c Gen8 (Hewlett-Packard Development Company, L.P., 2015).	40
Ilustración 6. Diagrama lógico de Red para Exchange 2013 (Villavicencio, 2015).....	42
Ilustración 7. Uso de CPU	42
Ilustración 8. Uso de Memoria RAM	43
Ilustración 9. Troughput.....	43
Ilustración 10. Diagrama final de solución F5.....	46
Ilustración 11. Configuraciones del sistema F5	47
Ilustración 12. Configuración de puerto de administración.....	48
Ilustración 13. Configuración de direccionamiento IP de administración.....	48
Ilustración 14. Configuración de Host Name	48
Ilustración 15. Configuración de Zona Horaria	48
Ilustración 16. Configuración de claves de acceso	48
Ilustración 17. Configuraciones de nueva VLAN.....	49
Ilustración 18. VLANs.....	50
Ilustración 19. Creación de Self IPs.....	50
Ilustración 20. Self IPs.....	51
Ilustración 21. Creación de Rutas Estáticas	51
Ilustración 22. Ruta de Default Gateway	52
Ilustración 23. Creación de un nodo	53
Ilustración 24. Nodos	53
Ilustración 25. Creación de un Pool.....	54
Ilustración 26. Pools.....	54
Ilustración 27. Miembros de Pools	55
Ilustración 28. Ingreso de Certificado SSL al sistema F5.....	56
Ilustración 29. Ingreso de Certificado SSL al sistema F5.....	56
Ilustración 30. Client SSL profile	57
Ilustración 31. Server SSL Profile.	57
Ilustración 32. Perfil SSL de cliente	58
Ilustración 33. Perfil SSL de servidor.....	58
Ilustración 34. iRule.....	59
Ilustración 35. Propiedades generales de un Virtual Server	59
Ilustración 36. Configuraciones de un Virtual Server	60
Ilustración 37. Recursos de un Virtual Server	61
Ilustración 38. Virtual Servers	61
Ilustración 39. Cambio de Default Gateway servidor CAS #1	61
Ilustración 40. Cambio de Default Gateway servidor CAS #2.....	62
Ilustración 41. Creación de archivo de respaldo.....	62
Ilustración 42. Prueba de comunicación ICMP desde F5 a CAS Server #1	63
Ilustración 43. Prueba de comunicación ICMP desde F5 a CAS Server #2.....	63
Ilustración 44. Prueba de comunicación ICMP desde F5 a Default Gateway (Firewall)	63
Ilustración 45. Prueba de conectividad desde Microsoft Outlook 2013	64
Ilustración 46. Prueba de conectividad desde explorador Web - OWA	64

Ilustración 47. Balanceo equitativo de conexiones a servidores CAS	67
Ilustración 48. Estadísticas de pérdida de paquetes	68
Ilustración 49. Encriptación entre Cliente y Equipo F5.....	68
Ilustración 50. Encriptación entre Equipo F5 y Servidores CAS	69
Ilustración 51. Archive – Respaldo de configuración final	69
Ilustración 52. Quejas por calidad de servicio	70
Ilustración 53. Tiempo fuera de servicio	71
Ilustración 54. Conexiones hacia el Virtual Server de correo electrónico.....	71
Ilustración 55. URIs accedidas por los clientes	72
Ilustración 56. Distribución de peticiones hacia los miembros del pool	72
Ilustración 57. Países desde donde se realizan las conexiones	72
Ilustración 58. Direcciones IP desde donde se conectan los clientes	73
Ilustración 59. Estadísticas de conexiones y throughput	74

TABLAS

Tabla 1. Características de equipo F5 4200s	45
Tabla 2. Mejoras en quejas por calidad de servicio y tiempo fuera de servicio	70

1. INTRODUCCIÓN

La empresa Nube Digital, fue introducida en el mercado tecnológico desde el año 2013 y está respaldada por Compuequip DOS quienes tienen experiencia en este mercado por más de 25 años. Nube Digital, ofrece los servicios de infraestructura y plataformas tecnológicas, con el respaldo de una mesa de ayuda local, de forma virtual en la nube tecnológica con comunicaciones a través del internet.

Debido al rápido crecimiento de la empresa, ésta se vio obligada a mejorar su infraestructura de servidores de correo electrónico para así proveer un mejor servicio, debido a que con su previa infraestructura, no lograba cubrir a cabalidad la demanda de los usuarios de esta aplicación. Por esta razón, decidió proceder con el despliegue de nueva infraestructura física y virtual, tomando en cuenta la necesidad de proveer un servicio de acceso rápido, seguro y sobre todo de alta disponibilidad, para lo cual implementó dos servidores virtuales de Exchange 2013 y un equipo físico de balanceo de carga para realizar la distribución de carga, administrar los certificados digitales y sobre todo para distribuir la carga de todas las peticiones a la aplicación, de manera equitativa y eficiente.

El despliegue de Exchange se encuentra sobre un servidor virtualizado en una plataforma de VMware e instalado sobre sistema operativo Windows Server 2012. Los equipos balanceadores de carga utilizados poseen un sistema operativo propietario del fabricante con un Kernel de Redhat versión 2.6.32-220.el6.f5.x86_64. Para la encriptación entre el cliente final y el balanceador, al igual que entre cada balanceador y los servidores, se utiliza un certificado digital de 2048 bits emitido por GoDaddy.com, Inc.

La configuración y despliegue de la solución de distribución equitativa de la carga enviada a los servidores de correo electrónico se realizó de forma manual en el balanceador, para desplegar solamente la aplicación por los puertos requeridos y mediante las

características solicitadas por Nube Digital, para también manejar la seguridad a nivel de los servidores balanceados.

1.1 Antecedentes

Nube Digital es una empresa Ecuatoriana situada en la ciudad de Quito que cuenta con el respaldo de Computadores y Equipos DOS, líderes en el mercado tecnológico con más de 25 años de experiencia. Su objetivo principal es el de brindar soporte tecnológico e infraestructura a empresas que no cuentan con la capacidad de mantener su propia plataforma tecnológica, de tal manera que puedan contar con una mejor infraestructura y tecnología. Para respaldar la calidad en su servicio, ofertan soluciones tecnológicas y una mesa de servicios local con la cual se puede brindar un servicio permanente a sus usuarios, manteniendo costos bajos.

La empresa se cataloga como una empresa Escalable, ya que cuenta con arquitectura independiente, de tal manera que sus actualizaciones de red, procesamiento y almacenamiento son expandibles. Cabe recalcar la seguridad en su almacenamiento de datos, ya que su red es monitoreada constantemente con el fin de brindar estabilidad a sus clientes en el manejo de información. Entre sus principales servicios están: correo electrónico, servicio de software, mensajería unificada, video conferencias, respaldo de información, escritorios remotos, seguridad electrónica, infraestructura de servicios, SAP Administrativo, consultorías entre otras (Nube Digital, 2014).

A finales del 2014, debido al crecimiento de la empresa y por la demanda de usuarios de correo electrónico, se ve la necesidad de aumentar su capacidad de rendimiento y tiempos de respuesta, al igual que una mejora en los niveles de servicio en base al mercado tecnológico ecuatoriano. Bajo esta premisa la empresa decidió implementar una solución de

alto rendimiento y disponibilidad, mejorando así los servicios de Microsoft Exchange con un servidor adicional y un equipo físico F5 de balanceo de carga de la aplicación, para servir de forma óptima a todos los usuarios finales quienes demandaban una mejor calidad de servicio (Villavicencio, 2014).

1.2 Objetivos

1.2.1 Objetivo General

El objetivo general de este trabajo de tesis es permitir el uso de toda la infraestructura actual de la empresa Nube Digital mediante la inclusión de un clúster de alta disponibilidad de equipos balanceadores de carga físicos de marca F5 Networks, que permita mejorar el servicio de correo electrónico de forma inmediata y además permita un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo.

1.2.2 Objetivos Específicos

- a) Identificar los problemas actuales de la aplicación de correo electrónico.
- b) Establecer necesidades específicas de mejoras en el servicio de correo electrónico.
- c) Implementar una solución de alta disponibilidad y rendimiento de correo electrónico.
- d) Monitorear el funcionamiento correcto de la solución.

1.3 Hipótesis

¿La implementación de un clúster de equipos de balanceo de carga F5 permite mejorar el servicio de correo electrónico de forma inmediata y además permite un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo?

1.4 Justificación

La empresa Nube Digital contaba con una solución básica de Microsoft Exchange 2013, compuesta por un solo servidor virtual instalado sobre el sistema operativo Windows

Server 2012, que receptaba las peticiones del usuario final de forma directa y sin validar protocolos avanzados de comunicación. Tampoco contaba con una administración óptima de la encriptación de datos mediante la gestión de certificados digitales por parte de un equipo intermedio entre el usuario final y el servidor.

Otro inconveniente que enfrentaba la empresa, era la indisponibilidad parcial y esporádico del servicio de correo electrónico, incumpliendo así los acuerdos de nivel de servicio ofertados en sus negociaciones, por lo que se veía impactada la calidad y credibilidad de su servicio.

Este problema inició, por la falta de recursos del servidor de Microsoft Exchange 2013 instalado, que no lograba abastecer a los requerimientos de todos los usuarios del servicio de correo electrónico, provocando así la insatisfacción de algunos usuarios por la pérdida de mensajes electrónicos.

Para tratar de solventar de manera inmediata su falta de recursos con un solo servidor, instalaron un segundo servidor virtual de Microsoft Exchange, con las mismas características del inicial. Sin embargo, nuevamente se enfrentaban a otro problema; no había forma de que ambos equipos funcionen al mismo tiempo para responder las peticiones de correo electrónico de sus usuarios ya que las pruebas de balanceo de carga por software a través de la red, no funcionaban correctamente, impidiendo así una solución de alta disponibilidad. Al analizar más a detalle la razón del problema en el balanceo de Microsoft por Network Load Balancer (NLB), se identificó que las tarjetas de red utilizadas en los equipos de forma virtual, conectadas al switch de capa 2 del cliente, impedían el funcionamiento del balanceo NLB de Microsoft debido a la incompatibilidad de una configuración virtual en una sola tarjeta de red asignada con el tipo de switch utilizado, por lo que la única manera de realizar una distribución de la carga y poder utilizar los dos servidores de Microsoft Exchange desplegados hasta el momento, era mediante el uso de un hardware para balanceo de carga.

Por ende, esto causó que solo uno de los servidores provea el servicio a la vez, y aunque facilitaba de alguna manera los cambios en políticas y configuraciones, existía aún tiempos altos de fuera de servicio de la aplicación de correo electrónico e insatisfacción de sus usuarios.

Una vez seleccionado el tipo de balanceador de carga a utilizar, el dispositivo Local Traffic Manager del fabricante F5 Networks, se identificó además otro tipo de ventajas y bondades que venían pre-establecidas en las configuraciones básicas del hardware.

La implementación de los dispositivos F5, en su mayoría, prometen solventar el tipo de inconvenientes que al momento enfrenta la empresa Nube Digital.

Se espera que al desplegar esta tecnología, se logre el fortalecimiento de la infraestructura de correo electrónico mediante el uso al 100% de los dos servidores de correo electrónico actualmente instalados, así como el crecimiento transparente en el momento que el cliente decida incluir más servidores en su granja, en un corto o mediano plazo, sin causar ninguna indisponibilidad y brindando siempre un servicio completamente disponible, seguro y eficaz hacia los clientes.

Además permitirá un crecimiento paulatino, controlado y monitoreado, para que la empresa siga escalando en el mercado de la nube tecnológica con todos sus servicios además del correo electrónico, ya que el equipo balanceador de F5 Networks, permite la configuración de balanceo de varias aplicaciones, de forma personalizada cada una para un rendimiento óptimo en base a las características de cada aplicación, así también como el control de la seguridad en la capa 7 o de aplicaciones del modelo OSI.

2. CONTEXTO Y MARCO TEÓRICO

2.1 Servidores

2.1.1 Definición

Servidor es un ordenador o máquina informática que presta sus servicios a otras entidades o dispositivos como personas u ordenadores llamadas clientes, suministrando además todo tipo de información (APR, 2015).

2.1.2 Componentes de un servidor

Microprocesador: es el chip principal o cerebro de un servidor, que se encarga de realizar todas las operaciones matemáticas y lógicas requeridas para el procesamiento de los datos. Generalmente un servidor cuenta con un conjunto de chips que forman una estructura conformada hasta por 16 microprocesadores instalados e interconectados entre sí.

Adicionalmente, cada microprocesador cuenta con dos o más núcleos.

Memoria RAM: es la memoria de acceso rápido o aleatorio que almacena de manera temporal la información necesaria para que la computadora funcione. Si existe poca memoria RAM, el servidor utilizará espacio en el disco duro para simularla pero este funcionará más lento. Dependiendo del tipo de servidor, estos pueden alojar hasta 128 Gigabytes (GB) de memoria RAM.

Placa del sistema o tarjeta principal: Es donde todos los dispositivos internos del servidor se interconectan además de los puertos de comunicación, ranuras de expansión para tarjetas y conectores de disco duro y otros elementos.

Disco duro: es un dispositivo de almacenamiento magnético, donde se encuentra la mayor cantidad de información del ordenador, incluyendo el sistema operativo, las aplicaciones, los archivos generados por el usuario, etc. Actualmente pueden llegar a tener varios Terabytes (TB) de capacidad.

Unidad de disco óptico: es una bahía donde generalmente se instala un lector de discos CD o DVD para poder acceder a los programas o las aplicaciones e instalarlas en el servidor.

Fuente de poder: Es el dispositivo encargado de suministrar la alimentación eléctrica a los elementos internos. La fuente de poder un servidor común soporta hasta 700 vatios y es más resistente que la de un ordenador común para poder resistir estar encendida todo el tiempo. La mayoría de servidores posee 2 fuentes redundantes para tener alta disponibilidad y no apagarse en caso de falla de una de las dos fuentes.

Sistema operativo: Es el programa o software principal para gestionar todas las tareas ejecutadas por el usuario y encargado de reconocer dispositivos y ejecutar las aplicaciones dedicadas (Informática Moderna, 2015).

2.2 Virtualización

2.2.1 Definición

“Virtualización es la creación de una versión virtual (en lugar de real) de algo, como un sistema operativo, un servidor, un dispositivo de almacenamiento o recursos de red” (Rouse, 2010).

“La tecnología de virtualización aumenta la eficiencia en su centro de datos ya que permite que los servidores x86 actuales ejecuten múltiples aplicaciones y sistemas operativos” (VMware, 2015).

2.2.2 Virtualización del Servidor

“La virtualización del hardware implica utilizar software para crear máquinas virtuales (VM) que emulan un host físico. Esto crea un entorno de sistema operativo independiente que es, lógicamente, aislado del servidor host. Al ofrecer varias máquinas virtuales a la vez, este enfoque permite que varios sistemas operativos corran simultáneamente en una única máquina física” (Microsoft, 2012).

2.3 Balanceo de Carga

2.3.1 Definición

Balanceo de carga es la división de cantidad de trabajo que un ordenador debe realizar, entre dos o más ordenadores similares, de tal manera que se logre ejecutar mayor cantidad de trabajo en el mismo tiempo, obteniendo mayor velocidad de respuesta a los usuarios. El balanceo de carga puede ser implementado con equipos de hardware, mediante software, o una combinación de ambos. Generalmente, el balanceo de carga es la razón principal para la creación de clústeres de servidores (Funk, 2015).

2.3.2 Clúster de servidores

Un clúster se forma de la unión de varios servidores que trabajan como uno sólo, para poder mejorar el rendimiento de la aplicación o programas albergados en cada servidor que compone el clúster.

Aunque generalmente los servidores que componen el clúster poseen las mismas características, a veces se puede tener un clúster compuesto con servidores de diferentes características y recursos, siempre y cuando alberguen las mismas aplicaciones y/o programas.

Para gestionar los diferentes servidores que componen el clúster, es necesario una herramienta de gestión o un elemento de hardware o software como un balanceador de carga (OpenLazarus, 2014).

2.3.3 Balanceador F5

Un balanceador de carga F5 es un dispositivo que actúa como un reverse proxy y distribuye el tráfico de la red o de aplicaciones hacia uno o más servidores. Los balanceadores son utilizados para incrementar la capacidad (usuarios concurrentes) y la confiabilidad de las aplicaciones. Estos mejoran el desempeño en general de las aplicaciones, minimizando la carga sobre los servidores en cuanto a la administración y el mantenimiento

de las sesiones de aplicaciones y de la red, así también como por la ejecución de tareas específicas de las aplicaciones.

Los balanceadores de carga generalmente se agrupan en dos categorías: de capa 4 y de capa 7. Los balanceadores de capa 4 actúan en base a datos encontrados en los protocolos de las capas de red y de transporte (IP, TCP, FTP, UDP). Los balanceadores de capa 7 distribuyen las peticiones en base a los datos encontrados en los protocolos de la capa de aplicación como HTTP.

Las peticiones son recibidas por cualquiera de los dos tipos de balanceadores de carga y son distribuidas hacia un servidor en particular en base a un algoritmo configurado.

Los balanceadores de capa 7 pueden distribuir mayor cantidad de peticiones en base a datos específicos de aplicación como HTTP headers, cookies, o datos dentro del mismo mensaje de la aplicación como el valor de un parámetro específico.

Los balanceadores de carga garantizan la fiabilidad y disponibilidad de las aplicaciones mediante un monitoreo de salud de aplicaciones y solamente enviando peticiones hacia los servidores y aplicaciones que pueden responder de manera oportuna (F5 NETWORKS, 2015).

2.3.4 TMOS

La base de un sistema BIG-IP desde el punto de vista del Software es el Sistema Operativo de Gestión del Tráfico (TMOS®) por sus siglas en inglés (F5 Networks® Traffic Management Operating System®). TMOS es un sistema operativo de tiempo real, orientado a eventos, diseñado específicamente para redes de distribución de aplicaciones. Mediante TMOS, se puede configurar todas las funciones básicas de ruteo y conmutación del sistema BIG-IP, así también como ciertas mejoras como clústeres, roles de usuarios, y particiones de administración. Sobre el TMOS, se ejecutan una serie de módulos independientes que pueden ser configurados como el LTM (F5 Networks, 2015).

2.3.5 BIG-IP

El término BIG-IP, como se lo denomina hoy en día, en realidad no es acrónimo de nada. Es más un juego de palabras respecto al protocolo TCP/IP. La porción ‘BIG’ representa el hecho de que el dispositivo presenta una dirección IP virtual como la puerta de entrada hacia diferentes dispositivos que se encuentran detrás de este, es decir, haciendo esta IP más ‘grande’ que una dirección IP normal (Griffin, 2005).

2.3.6 Local Traffic Manager

También llamado LTM, es el módulo más popular ofertado por F5 Networks. El verdadero poder del LTM está en que es un Full Proxy, permitiendo el aumento de conexiones del lado del cliente y del servidor. Además, toma decisiones de balanceo de carga, para mantener la disponibilidad, desempeño y persistencia de las aplicaciones balanceadas (Geraci, 2014).

2.3.7 Proxy

El significado literal de proxy es procurador. En informática, un proxy es básicamente otro computador o sistema que sirve como intermediario para las que las solicitudes de internet sean procesadas. Al conectarse a través de uno de estos equipos, el computador envía peticiones al proxy server, el cual procesa las mismas y responde el resultado esperado. De esta forma, es el salto intermedio entre la máquina del cliente final y el resto de computadores en internet (Gilbert, 2014).

2.3.8 Full Proxy

No todos los proxies son full proxies y es necesario realizar una distinción entre estos, al momento de tomar decisiones respecto a una arquitectura para un centro de datos.

Un full proxy mantiene dos tablas de sesiones separadas – una en el lado del cliente y otra en el lado del servidor. Es decir, existe una capa de aislamiento ‘espacio de aire’ entre

los dos, al interno del proxy. Esto permite la aplicación de perfiles específicos para cada lado del proxy, y así poder manipular o mejorar el comportamiento del tráfico y conexiones en el lado del cliente así como en el lado de los servidores (MacVittie, 2011).

2.3.9 Elementos de sistema F5

2.3.9.1 Host Name

El Host Name es el nombre del equipo F5 en formato FQDN es decir, un nombre de dominio completo, por ejemplo myf5.com.ec (F5 NETWORKS, 2015).

2.3.9.2 Management Port IP Address

Una dirección IP es una dirección de Protocol de Internet (Internet Protocol Address) que actúa como un identificador para un ordenador o dispositivo sobre una red TCP/IP. Las redes que utilizan el protocolo de comunicación TCP/IP, enrutan los mensajes en base a la dirección IP de destino.

El formato de una dirección IP se escribe en 4 grupos de números en el sistema binario, separados por puntos. Cada grupo de números va desde el 0 al 255. (Beal, 2015).

Todo equipo F5 posee la dirección IP de administración por defecto 192.168.1.245 que sirve para poder acceder tanto a la interfaz WEB como a la consola de comandos CLI (F5 NETWORKS, 2015).

2.3.9.3 Archive

Un elemento de tipo 'archive' se refiere a una copia de respaldo de los datos de configuración del equipo F5. Este repositorio se guarda en la forma de un set de configuración de usuario (UCS) por sus siglas en inglés (F5 NETWORKS, 2015).

2.3.9.4 SSL Certificate

Un SSL certificate o certificado digital seguro en español, es un elemento que el sistema BIG-IP presenta hacia otro dispositivo en la red para propósitos de autenticación. Un

certificado SSL puede ser un certificado auto-firmado o un certificado de un CA de confianza.

Cuando el software del sistema BIG-IP es instalado, la aplicación incluye un certificado SSL auto-firmado llamado Default. Un certificado auto-firmado es un mecanismo de autenticación que es creado y autenticado por el sistema en el cual reside (F5 Networks, 2015).

2.3.10 Elementos de red F5

2.3.10.1 Vlan

Una Vlan es un subconjunto lógico de hosts en una red de área local (LAN) por sus siglas en inglés, que operan en el mismo segmento de direcciones IP.

Para que una Vlan funcione correctamente en los segmentos de direcciones IP asignados, se debe asignar una o varias interfaces del dispositivo BIG-IP, donde serán conectados los cables hacia los dispositivos dentro del mismo segmento para cada caso respectivamente (F5 NETWORKS, 2015).

2.3.10.2 Host

El término 'host' es utilizado en diferentes contextos. En cuanto al protocolo de internet respecta, este término representa cualquier ordenador o equipo que posee dos vías de acceso o comunicación hacia otros computadores en el Internet (Rouse, 2005).

2.3.10.3 Interface

Las interfaces en un sistema BIG-IP son los puertos físicos utilizados para conectar el dispositivo F5 a otros dispositivos en la red.

Estos dispositivos pueden ser ruteadores, dispositivos de capa 2, servidores de destino, entre otros. A través de sus interfaces, el sistema BIG-IP puede reenviar el tráfico hacia y desde otros dispositivos en la red (F5 Networks, 2015).

2.3.10.4 Self IP Address

Una dirección self IP, es una dirección IP en el sistema BIG-IP que está asociada con una Vlan, para acceder a hosts en esa Vlan. En virtud de su máscara de red, una dirección self IP representa un espacio de direcciones, es decir, un rango de direcciones IP que abarcan a los diferentes hosts en cada Vlan asociada, en lugar de una sola dirección de host.

Las direcciones self IP sirven dos propósitos:

Primero, cuando se envía un mensaje a un servidor de destino, el sistema BIG-IP utiliza las direcciones self IP de sus Vlans, para determinar la Vlan específica en la cual reside el servidor de destino del mensaje. Por ejemplo, si una Vlan ‘Interna’ tiene la dirección self IP de 10.10.10.100, con una máscara de 255.255.255.0, y la dirección IP del servidor de destino es 10.10.10.20 (con máscara de 255.255.255.255), el sistema BIG-IP reconoce que la dirección IP del servidor se encuentra dentro del rango de la dirección self IP de la Vlan ‘Interna’, por ende, envía el mensaje hacia esa Vlan. Siendo más específicos, el sistema BIG-IP envía el mensaje hacia la interface asignada a esa Vlan. Si más de una interface está asignada a esa Vlan, el sistema BIG-IP toma ciertos pasos adicionales para determinar la interface correcta, como la revisión de la tabla de ruteo de capa 2.

Segundo, una dirección self IP puede actuar como la ruta por defecto para cada servidor de destino en la Vlan correspondiente. En este caso, la dirección self IP de una Vlan aparece como la dirección IP de destino en la cabecera del paquete cuando un servidor envía una respuesta hacia el sistema BIG-IP (F5 Networks, 2015).

2.3.10.5 Routes

Su traducción al español es ruta. Se define como la información que es utilizada para tomar la decisión respecto a cómo enviar un paquete para que éste llegue a su red de destino deseado (InetDaemon, 2013).

En base a las capacidades de ruteo (Capa 3) y las necesidades de procesar tráfico de aplicaciones de usuario (para balanceo de carga y monitoreo de salud) y también tráfico de administración, el sistema BIG-IP procesa dos tipos de rutas:

- Rutas de Administración

El sistema BIG-IP almacena y recupera información de las rutas de administración o gestión. Las rutas de Administración son rutas que el sistema BIG-IP utiliza para reenviar paquetes a través la interface de gestión.

- Rutas TMM

El sistema BIG-IP almacena y recupera información de las rutas del switch TMM. Las rutas del switch TMM son rutas que el sistema BIG-IP utiliza para reenviar tráfico a través de las interfaces del switch TMM (interfaces asignadas a Vlans), en lugar de la interface de administración (F5 Networks, 2015).

2.3.11 Elementos de balanceo F5

2.3.11.1 Node

Un node se traduce al español como nodo. Un Nodo es un objeto lógico en el sistema BIG-IP que identifica la dirección IP de un recurso físico o virtual en la red. Una característica importante de los nodos es su asociación con monitores de salud. Tal como un miembro de pool, los nodos pueden ser asociados con monitores de salud como una forma de determinar el estado del servidor. Sin embargo, un monitor de salud para un miembro de pool reporta el estado del servicio corriendo en el dispositivo, mientras que un monitor de salud asociado con un nodo, reporta el estado del dispositivo mismo.

La diferencia entre un nodo y un miembro de pool es que el nodo está designado por una dirección IP solamente (10.10.10.10), mientras que la designación del miembro de pool incluye una dirección IP y un puerto de servicio (10.10.10.10:80) (F5 Networks, 2015).

2.3.11.2 Pool Member

Un pool member o miembro de pool, es un objeto lógico que representa un nodo físico o virtual (servidor) en la red (F5 Networks, 2015).

2.3.11.3 Pool

Un load balancing pool o pool de balanceo de carga traducido al español, es un grupo de dispositivos lógico, como servidores web, que se agrupan para recibir y procesar tráfico. En lugar de enviar tráfico del cliente a la dirección de destino especificada en la petición del cliente, el LTM envía la petición a cualquiera de los servidores que son miembros de ese pool. Esto ayuda a distribuir la carga de forma eficaz sobre los recursos de los servidores.

Cuando se crea un pool, se deben asignar los miembros de ese pool (F5 Networks, 2015).

2.3.11.4 Virtual Server

Un Virtual Server es un objeto de gestión de tráfico en un sistema BIG-IP que está representado por una dirección IP y un servicio (puerto de conexión). Los clientes en una red externa pueden enviar tráfico de aplicación hacia un virtual server, el cual direcciona el tráfico de acuerdo a las instrucciones de la configuración. El principal propósito de un virtual server es a menudo el balancear la carga del tráfico a lo largo de un pool de servidores en una red interna. Los virtual servers incrementan la disponibilidad de recursos para el procesamiento de las solicitudes del cliente.

Los virtual servers no solamente distribuyen el tráfico a lo largo de múltiples servidores. Ellos también gestionan varios tipos de tráfico de maneras diferentes, dependiendo de las necesidades de la gestión del tráfico. Por ejemplo, un virtual server puede habilitar compresión en datos de peticiones HTTP mientras ésta pasa a través del sistema BIG-IP, o descifrar y re-criptar conexiones SSL y verificar certificados SSL. Para cada tipo de tráfico, como TCP, UDP, HTTP, SSL, SIP, y FTP, un virtual server puede aplicar un

grupo completo de configuraciones, para afectar la forma en que el sistema BIG-IP gestiona ese tipo de tráfico.

Un virtual server puede también habilitar persistencia de sesión para un tipo de tráfico específico. A través de un virtual server, se puede configurar persistencia para sesiones HTTP, SSL, SIP, MSRDP, entre otras.

Por último, a un virtual server se puede aplicar una iRule, la cual es un código escrito por el usuario, para inspeccionar y direccionar conexiones individuales en formas específicas. Por ejemplo, se puede crear una iRule que busque en el contenido de una conexión TCP, una serie de caracteres específico y si lo encuentra, direcciona al virtual server, el envío de la conexión a un pool o miembro de pool específico (F5 Networks, 2015).

2.3.11.5 iRule

Una iRule es una característica poderosa y flexible de los dispositivos BIG-IP, basados en la arquitectura exclusiva de F5. Las iRules proveen un control sin precedentes para manipular y gestionar directamente cualquier tráfico de aplicación IP. Las iRules utilizan una sintaxis de escritura de código fácil de aprender y permite personalizar como interceptar, inspeccionar, transforman y direccionar tráfico de aplicación entrante y saliente (Pruitt, 2007).

Una iRule es un código que se escribe para que conexiones individuales sean direccionadas a un pool diferente al definido por defecto en un virtual server. Las iRules permiten especificar de forma más directa, el destino al cual se desea enviar el tráfico. Al utilizar iRules, se puede direccionar el tráfico no solamente a otros pools, pero también a miembros de pool individuales y específicos, a otros puertos de comunicación y a URIs específicas (F5 Networks, 2015).

2.3.11.6 Health Monitor

Se puede configurar al sistema BIG-IP para monitorear la salud y el desempeño de ciertos nodos o servidores que son miembros de un pool de balanceo de carga. Los monitores verifican las conexiones sobre los miembros de pool y nodos. Un monitor puede ser monitor de salud o monitor de desempeño, designados para validar el estado de un pool, miembro de pool, o nodo, de manera periódica en un intervalo definido. Si el miembro de un pool o un nodo que está siendo validado, no responde dentro del período de tiempo especificado, o el estado de un miembro de pool o nodo indica que el desempeño está degradado, el sistema BIG-IP puede re-direccionar el tráfico hacia otro miembro de pool o nodo.

Algunos monitores están incluidos como parte del sistema BIG-IP, mientras otros monitores son creados por el usuario. Los monitores que forman parte del sistema BIG-IP, son llamados monitores pre-configurados. Los monitores creados por el usuario se llaman monitores personalizados (F5 Networks, 2015).

2.3.11.7 Profile

El sistema BIG-IP LTM, puede administrar tráfico de red específico de aplicaciones en una variedad de formas, dependiendo de los protocolos y servicios que están siendo utilizados. Por ejemplo, se puede configurar al sistema BIG-IP para compresión de datos en las respuestas HTTP, o se puede configurarlo para autenticación de certificados SSL antes de pasar la petición hacia el servidor de destino.

Para cada tipo de tráfico que se desea manejar, el sistema BIG-IP contiene herramientas de configuración que se pueden utilizar para controlar de manera inteligente el comportamiento del tráfico. Estas herramientas se denominan perfiles (profiles en inglés). Un perfil es una herramienta de configuración provista por el sistema que mejora la capacidad de gestión del tráfico específico de aplicaciones. Es decir, un perfil es un objeto que contiene configuraciones que pueden ser manipuladas y cambiadas por el usuario, con valores por

defecto, para controlar el comportamiento de cierto tráfico de red en particular como las conexiones HTTP. Después de configurar un perfil, se lo debe asociar con un virtual server. De esta manera, el virtual server procesa el tráfico de acuerdo a los valores especificados en el perfil. Al utilizar perfiles, se mejora el control sobre la gestión del tráfico de red, y las tareas de gestión de tráfico se vuelven más fáciles y eficientes.

Se pueden asociar múltiples perfiles a un mismo virtual server. Por ejemplo, se puede asociar un perfil TCP, un perfil SSL y un perfil HTTP al mismo virtual server (F5 Networks, 2015).

2.3.11.7.1 Algoritmos de Balanceo F5

Uno de los perfiles más importantes de los equipos balanceadores F5 es el método o algoritmo de balanceo de carga.

A diferencia del balanceo tradicional mediante software como el sistema NLB de Microsoft, F5 brinda varios algoritmos de balanceo, que se adaptan a cada configuración de servidores de cualquier aplicación. Los métodos de balanceo van desde el más simple llamado Round Robin, es decir, balanceo aleatorio enviando una petición a la vez a cada servidor de la granja, tal como lo hace NLB, hasta el método más complejo y completo que analiza el comportamiento de la aplicación y de los servidores que la albergan (F5 Networks, 2015).

Algunos de los algoritmos más importantes son:

Observed: Este algoritmo trabaja de tal manera que analiza el comportamiento de los servidores de aplicaciones y mide el tiempo de respuesta de una solicitud, y la velocidad de entrega de la misma para tomar la decisión de balanceo entre los servidores.

Ratio: Este algoritmo de balanceo, distribuye las conexiones hacia los Servidores, en base a la relación de pesos definidos en cada uno de estos servidores. Este es un método de

balanceo estático, que basa la distribución en relación de pesos definidos de manera estática, proporcionales a la capacidad de los servidores.

Observed: Con el método de balanceo Observed, la distribución de carga está basada en un ranking de acuerdo al número de conexiones. Los nodos que poseen un mejor promedio de menos número de conexiones reciben una mayor proporción de conexiones. Este algoritmo también realiza un seguimiento al número de conexiones de capa 4 hacia cada nodo a lo largo del tiempo y crea un peso para el balanceo de carga hacia cada nodo.

Este es un método de balanceo dinámico, por lo que trabaja bien en cualquier tipo de ambiente incluso si los servidores tienen diferente tipo de recursos entre sí. (F5 Networks, 2015)

2.3.12 Protocolos de comunicación

“Se trata del conjunto de pautas que posibilitan que distintos elementos que forman parte de un sistema establezcan comunicaciones entre sí, intercambiando información.

Si nos centramos en las computadoras, el protocolo de comunicación determina cómo deben circular los mensajes adentro de una red. Cuando la circulación de la información se desarrolla en Internet, existen una serie de protocolos específicos que posibilitan el intercambio” (Definicion.de, 2015).

2.3.13 Componentes del servicio

2.3.13.1 Diagrama de red

Un diagrama de red es utilizado en telecomunicaciones informáticas, para ilustrar el gráfico de una red. Este tipo de diagrama es particularmente útil para ingenieros y diseñadores de redes, para la recopilación de la documentación detallada de la red. Generalmente, un diagrama de red usualmente consiste de una red formada por grupos o sistemas interconectados. El alcance de un diagrama de red simple puede ser una aplicación

única, una familia de aplicaciones o inclusive una empresa completa (Janalta Interactive Inc., 2015).

2.3.13.2 Centro de datos

Un data center o centro de datos son instalaciones que centralizan las operaciones y equipamiento IT, y donde se almacena, administra y difunde sus datos. Los centros de datos albergan los sistemas más críticos de una red y son vitales para la continuidad de las operaciones del día a día. Consecuentemente, la seguridad y confiabilidad de los centros de datos y su información es una prioridad muy alta para las organizaciones (Palo Alto Networks, 2015).

Los centros de datos son infraestructuras físicas o virtuales utilizadas por las empresas para albergar computadoras, servidores, sistemas de red, y otros componentes para las necesidades de tecnología informática de las compañías, que normalmente incluyen el almacenamiento, procesamiento y disponibilidad de grandes cantidades de datos de misión crítica para los clientes, en una arquitectura cliente/servidor.

Un centro de datos o datacenter, a menudo requiere extensivos sistemas redundantes de suministro de energía, sistemas de refrigeración, conexiones de red redundantes y sistemas de seguridad basados en políticas, para la ejecución y administración de las aplicaciones más críticas e importantes de las empresas (Stroud, 2015).

2.3.13.3 Enrutador

Un router o enrutador, es un dispositivo que reenvía los paquetes de datos a lo largo de las redes. Un router está conectado al menos a dos redes, comúnmente dos LANs o WANs, o una LAN y su red de ISP. Los routers están ubicados en las puertas de enlace, los lugares en los que dos o más redes se conectan.

Los routers utilizan cabeceras y tablas de reenvío de datos para determinar el mejor camino para la transmisión de paquetes, y utilizan protocolos como ICMP para comunicarse entre sí y configurar la mejor ruta entre dos hosts (Beal, 2015).

Los routers son dispositivos de hardware que toman los paquetes entrantes, los analizan, los mueven a otras redes, convierten los paquetes a otras interfaces de red, interrumpen el paquete, direccionan a los destinos apropiados, y realizan otras acciones relacionadas a la red (Computer Hope, 2015).

2.3.13.4 Red

Una red o network en inglés, consiste en dos o más computadoras que están enlazadas para compartir recursos (como impresoras y lectores digitales), intercambiar archivos, o permitir comunicaciones electrónicas. Las computadoras de una red pueden estar vinculadas mediante cables, líneas telefónicas, ondas de radio, satélites, o haces de luz infrarroja.

Existen dos tipos de redes comunes: Redes LAN y redes WAN (Winkelman, 2013).

2.3.13.4.1 Redes LAN

Una red de área local (LAN) o Local Area Network, es una red que se limita a un área relativamente pequeña. Generalmente limitada a un área geográfica como un laboratorio, escuela, o edificio.

Las computadoras conectadas a una red, son categorizadas como servidores o estaciones de trabajo. Los servidores generalmente no son utilizados por las personas directamente, sino que se ejecutan continuamente para proveer servicios al resto de ordenadores (y los usuarios) en la red. Los servicios provistos pueden incluir impresión y envío de faxes, publicación de software, almacenamiento y uso compartido de archivos, mensajería, almacenamiento y recuperación de datos, control de acceso completo (seguridad) a los recursos de la red, entre otros (Winkelman, 2013).

2.3.13.4.2 Redes WAN

Una red a área amplia (WAN) o Wide Area Network, conecta redes en áreas geográficas grandes, como ciudades, países, o el mundo entero. Cableado transoceánico dedicado o enlaces satelitales pueden ser utilizados para conectar este tipo de redes globales.

Al utilizar una WAN, las escuelas en una ciudad como Florida se pueden comunicar con lugares como Tokio en cuestión de segundos, sin la necesidad de enormes pagos de facturas de teléfono. Dos usuarios en diferentes partes del mundo, con estaciones de trabajo equipadas con micrófonos y cámaras web, podrían mantener una teleconferencia en tiempo real. Una WAN es complicada. Ésta utiliza multiplexores, puentes y routers para conectar redes locales y metropolitanas a las redes de comunicación global como el Internet. Una WAN, no aparece tan diferente a una LAN para los usuarios comunes (Winkelman, 2013).

2.3.13.5 Rack

Un rack para computadoras o simplemente llamado rack, es una estructura de metal utilizada para sostener y mantener varios dispositivos de hardware como servidores, discos duros, módems y otros equipos electrónicos. Algunos pueden referirse a un rack como 'LAN o mueble de red' ya que se asemeja a una estructura de estantería donde los componentes pueden ir unidos verticalmente o apilados uno sobre otro.

Generalmente, los dispositivos individuales son ajustados en la parte delantera del rack mediante tornillos o tuercas, aprovechando las tiras de metal con agujeros espaciados para acomodar los dispositivos a la altura deseada y por lo general el espacio entre cada agujero es de 1,75 pulgadas, que son medidos en U o unidades (QuinStreet Inc., 2015).

2.3.13.6 Raid

Es el uso de múltiples discos duros para desempeño y confiabilidad.

RAID es una solución que fue desarrollada originalmente para el mercado de servidores de red como un medio para crear almacenamiento de gran tamaño a un bajo costo.

En esencia, se necesitarían varios discos de bajo costo, para ponerlos juntos mediante un controlador, para proveer una sola unidad de gran capacidad de almacenamiento. RAID es el acrónimo para ‘redundant array of inexpensive drives or disks’, que traducido al español significa arreglo redundante de discos de bajo costo. Para lograr obtener esto, software especializado y controladores fueron necesarios para permitir que los datos sean separados entre varios discos (Kyrnin, 2015).

Los discos incluidos en el arreglo, se denominan miembros del arreglo. Los discos pueden ser combinados en el arreglo de diferentes maneras, las cuales se conocen como niveles de RAID. Cada nivel de RAID tiene sus propias características de tolerancia a fallos, desempeño y capacidad (www.ReclaiMe.com, 2015).

3. METODOLOGÍA

3.1.1 Plan de implementación de la solución

Para el despliegue de esta solución se tomaron en cuenta diferentes elementos como las necesidades por parte del cliente, alcance y objetivos a cumplir, limitaciones y resultados esperados.

Se definió cada fase del proyecto de tal manera que se pueda evaluar el cumplimiento de cada una de estas, para de esa forma llegar al resultado deseado y completar el proyecto a satisfacción del cliente.

La metodología del proyecto se basa en las siguientes fases:

- Estudios preliminares
- Recopilación de Información
- Análisis y diseño
- Desarrollo y ejecución
- Implementación y Pruebas
- Mantenimiento (Kenneth E. Kendall, 2005)

3.1.2 Fases de implementación del proyecto

3.1.2.1 Estudios preliminares

Durante esta fase se mantienen reuniones con el personal de la empresa Nube Digital expertos en el servicio de correo electrónico, para realizar una observación del estado actual del servicio de correo electrónico.

Igualmente se definen los objetivos del proyecto y los procedimientos para el levantamiento de la información relevante para la solución deseada.

Es muy importante llegar a entender y conocer todos los componentes actuales del servicio tanto en la parte de hardware, software y personal involucrado.

3.1.2.2 Recopilación de información

En esta fase, se logró recolectar toda la información relacionada con el servicio actual de correo electrónico como diagramas de red, características de los servidores de correo electrónico, características de las máquinas virtuales donde se instalaron los servidores, características del sistema operativo, recursos asignados a cada servidor, de tal manera que sirvan como el punto inicial para la solución final de correo electrónico.

Los datos recopilados fueron obtenidos mediante una entrevista al experto del servicio de correo electrónico y por la entrega directa de documentación previamente recopilada por parte del administrador de este servicio.

3.1.2.2.1 Entrevista

Mediante este método de obtención de información, se logró determinar los diferentes componentes de la infraestructura donde se encuentra configurado el servicio de correo electrónico y el flujo completo del funcionamiento de esta aplicación. A continuación se detalla cada elemento del servicio de correo electrónico de la empresa Nube Digital obtenido en esta entrevista:

- Centro de Datos

El lugar donde se encuentra físicamente el equipo donde están instalados los dos servidores virtuales de Microsoft Exchange 2013 está ubicado en la ciudad de Guayaquil, en el centro de datos de Telconet Cloud Center, ubicado en la Avenida 11 NO, el cual es el primer Centro de Datos Categoría TIER IV en Latinoamérica, razón por la cual fue elegido como el lugar de almacenamiento de los equipos físicos de la empresa, por tener la mejor calificación y estándares de calidad en el Ecuador (Telconet S.A., 2015). En las ilustraciones 1 y 2 a continuación, se puede apreciar el espacio físico externo e interno del data center de Telconet en Guayaquil donde se encuentran físicamente los equipos de hardware que pertenecen a Nube Digital.



Ilustración 1. Vista externa del Cloud Center de Telconet (Telconet S.A., 2015)



Ilustración 2. Vista interna del Cloud Center de Telconet (Telconet S.A., 2015)

- Enlace de internet

Para la comunicación entre el mundo exterior y la infraestructura de la empresa Nube Digital, es necesario el uso de un enlace de internet que permita la entrada y salida de paquetes. En el caso de esta infraestructura, el enlace a internet es administrado por Telconet, que se lo maneja mediante un enrutador donde se conecta la infraestructura de Nube Digital como se aprecia en la ilustración 3 a continuación:

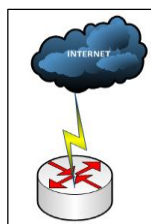


Ilustración 3. Representación del enlace de internet desde ruteador de borde de Telconet

- Rack para servidores

En el caso de los equipos de Nube Digital, el rack o bastidor utilizado es de marca HP modelo 10642, tiene una capacidad para 42 unidades y sostiene un peso máximo total de 1363 Kg. Las medidas de este bastidor son de 200,4 cm de altura, 60,9 cm de ancho y 123,8 cm de profundidad (42U, 2012). Se puede apreciar en la ilustración 4 a continuación, la imagen del rack utilizado por los equipos de Nube digital.



Ilustración 4. Rack HP modelo 10642 (DSI Server Racks, Inc, 2015)

- Servidor físico

El equipo físico donde se encuentran configurados los servidores virtuales de Microsoft Exchange 2013, es un servidor blade HP ProLiant BL460c Gen8 como se observa en la siguiente ilustración 5. Este es un servidor de doble zócalo y cuenta con 2 procesadores Intel® Xeon® E5-2660 v2 (10 núcleos, 2,2 GHz, 25 MB, 95 W), 196 GB de memoria RAM tipo 2R x4 PC3-14900-13 y 2 unidades de disco duro tipo SAS SFF de conexión en caliente de 15k rpm (Hewlett-Packard Development Company, L.P., 2015).



Ilustración 5. Servidor blade HP ProLiant BL460c Gen8 (Hewlett-Packard Development Company, L.P., 2015).

- Servidor virtual

Cada servidor virtual donde está instalado Microsoft Exchange 2013, está instalado sobre la plataforma de virtualización VMware 5.5, con una asignación de almacenamiento de 250GB configurados en Raid 5, y 12GB de memoria RAM cada servidor virtual. Cada servidor está instalado con el sistema operativo Windows Server 2012.

Además, existen dos servidores virtuales para el buzón de correo, igualmente instalados con sistema operativo Windows Server 2012, sobre la plataforma VMware 5.5, con una asignación de almacenamiento de 2TB en 4 particiones de 500Gb cada servidor virtual configurado en Raid 5, y con 12 GB de memoria RAM.

3.1.2.2 Entrega directa de documentación

Mediante este método de obtención de información, misma que fue entregada por parte del gerente de operaciones de la Compañía, se logró determinar de forma más profunda y detallada, la composición lógica del servicio de correo electrónica de Nube Digital, así como identificar el uso real de recursos de uno de los servidores de Exchange que estaba siendo utilizado antes de la implementación del hardware para balanceo de carga.

- Diagrama de red

En el diagrama de red entregado por el cliente, se puede observar de manera lógica, la composición y conectividad de los elementos que forman parte del servicio de correo electrónico de Nube Digital. Este insumo es muy importante para poder determinar la conectividad entre cada equipo involucrado en la solución, así también como el nuevo esquema a ser definido para la inclusión de los nuevo dispositivos físicos, en este caso dos equipos de balanceo de carga F5 4200s. El diagrama de red donde se muestra la estructura actual de equipos de Nube Digital, se muestra en la ilustración 6 a continuación:

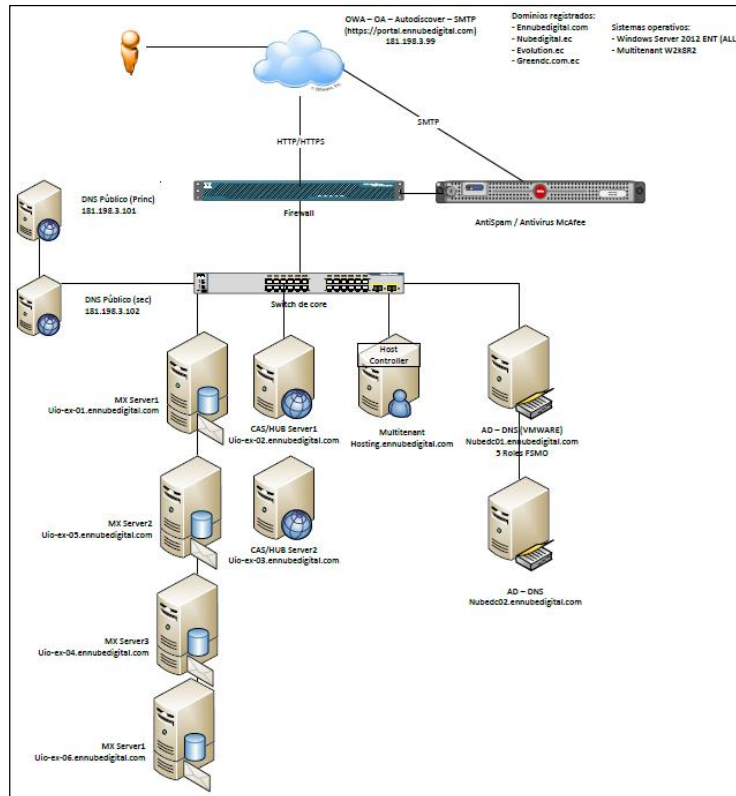


Ilustración 6. Diagrama lógico de Red para Exchange 2013 (Villavicencio, 2015)

- Estadísticas de uso de recursos de servidor de Exchange

En las ilustraciones a continuación, se puede evidenciar el uso de CPU, memoria RAM y throughput del servidor de Exchange activo previo a la implementación de balanceo de carga mediante hardware:

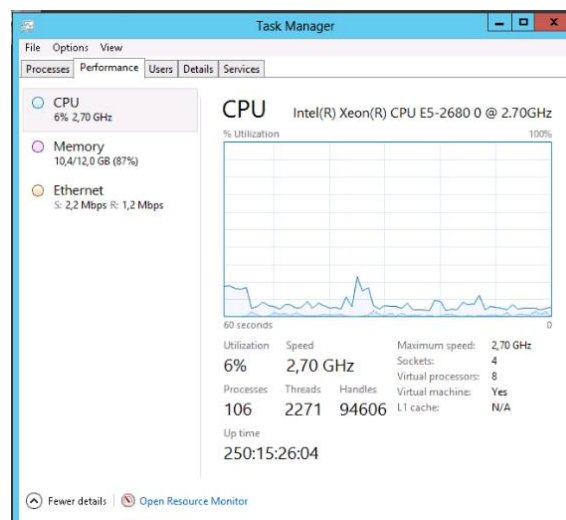


Ilustración 7. Uso de CPU

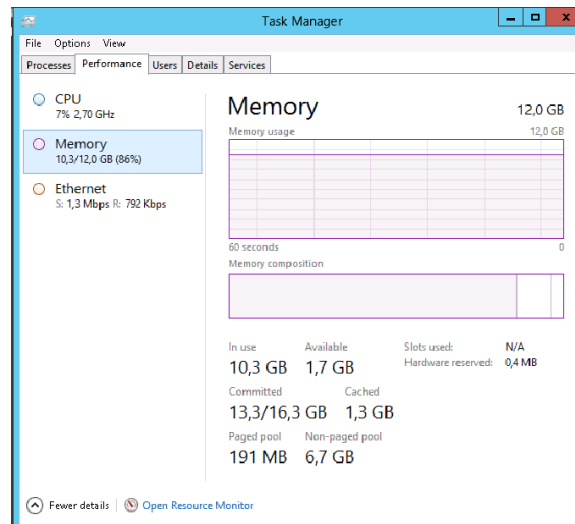


Ilustración 8. Uso de Memoria RAM

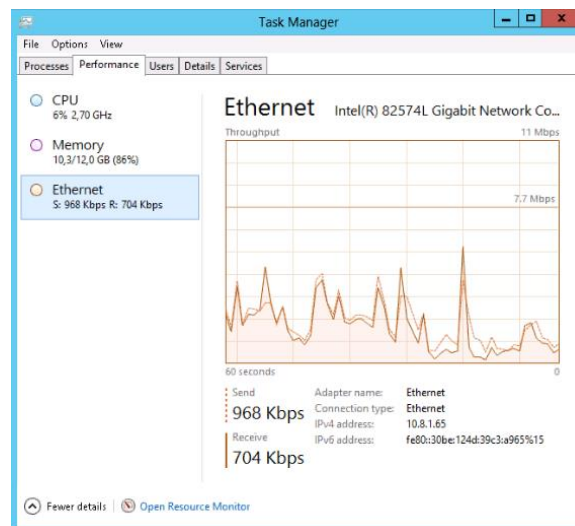


Ilustración 9. Troughput

3.1.2.3 Análisis y Diseño

Durante esta etapa del proyecto, se estructura toda la información obtenida en la recolección de información, y se diseña el plan a seguir para la implementación del proyecto. Se prepara un flujo de procesos a seguir, se definen alcances y limitaciones del proyecto y se identifican todos los recursos a ser utilizados.

El análisis de la información y el diseño del plan de implementación de este proyecto han sido encaminados al cumplimiento de objetivos específicos y del objetivo general, para la comprobación de la hipótesis de este trabajo de tesis.

Es necesario tomar en cuenta el diagnóstico inicial de antecedentes de la empresa:

- Nube Digital es una empresa de tecnología que busca la mejora continua con herramientas de última generación, para el desempeño óptimo de sus aplicaciones y servicios como el correo electrónico, considerando que esta aplicación mantiene un uso alto para las comunicaciones internas y con clientes.
- Debido a la alta demanda de servicios, se vio la necesidad de mantener una alta disponibilidad, confiabilidad y seguridad de los servicios ofertados, para mejorar la satisfacción del cliente actual y entrar en nuevos mercados.
- Una de las limitaciones de este proyecto es la ubicación del centro de datos donde se almacenan los equipos de Nube Digital, debido a la tardanza en la solución a los problemas cuando estos se presentan.

Finalmente, los recursos a utilizarse dentro de este proyecto son:

- Recurso humano
 - Implementador del proyecto
 - Gerente de operaciones de Nube Digital – Entrevistado
 - Operadores
 - Clientes
- Recurso material
 - Servidor físico
 - Servidores virtuales
 - Internet
 - Balanceadores F5

- Certificado digital
- Cableado
- Recursos financieros
 - Todos los recursos financieros fueron provistos por la empresa
Compuequip DOS como parte de uno de los servicios ofertados a Nube Digital.

3.1.2.4 Desarrollo y ejecución

En esta fase se coordinan todos los recursos humanos y materiales de acuerdo a lo establecido en el Plan de Implementación de la solución, con el propósito de obtener la documentación y resultados, mismos que han sido plasmados a lo largo de este documento, demostrando el proceso que fue seguido paso a paso para el desarrollo del proyecto, al igual que los resultados finales y éxitos del despliegue de la solución.

3.1.2.5 Implementación y Pruebas

Para la implementación y pruebas de esta solución de correo electrónico para el cliente Nube Digital, se realizó la adquisición de dos equipos F5 4200s, cuyas características se pueden observar en la siguiente tabla 1:

Memoria RAM	16 GB
Disco Duro	500 GB
Puerto Ethernet	8
Puerto de Fibra	2
Conexiones por segundo capa 4	300000
Peticiones por segundo en capa 7	850000
Peticiones HTTP por segundo en capa 4	2500000
Máximo de conexiones concurrentes capa 4	10000000
Throughput capa 4 y 7	10 Gbps

Tabla 1. Características de equipo F5 4200s

3.1.2.5.1 Implementación

La implementación de la solución para mejora y escalamiento del servicio de correo electrónico de la empresa Nube Digital, se la debe ejecutar con la configuración de varios elementos de los equipos F5 que se aglomeran en tres grupos principales como son:

- Elementos básicos del sistema
- Elementos de red
- Elementos de balanceo de carga

3.1.2.5.1.1 Diagrama de Red

El siguiente diagrama de red, muestra claramente la solución final de alta disponibilidad de balanceo de carga implementada en la empresa Nube Digital, mediante los equipos de balanceo de carga de F5 Networks, conectados a los diferentes equipos del cliente involucrados en esta solución:

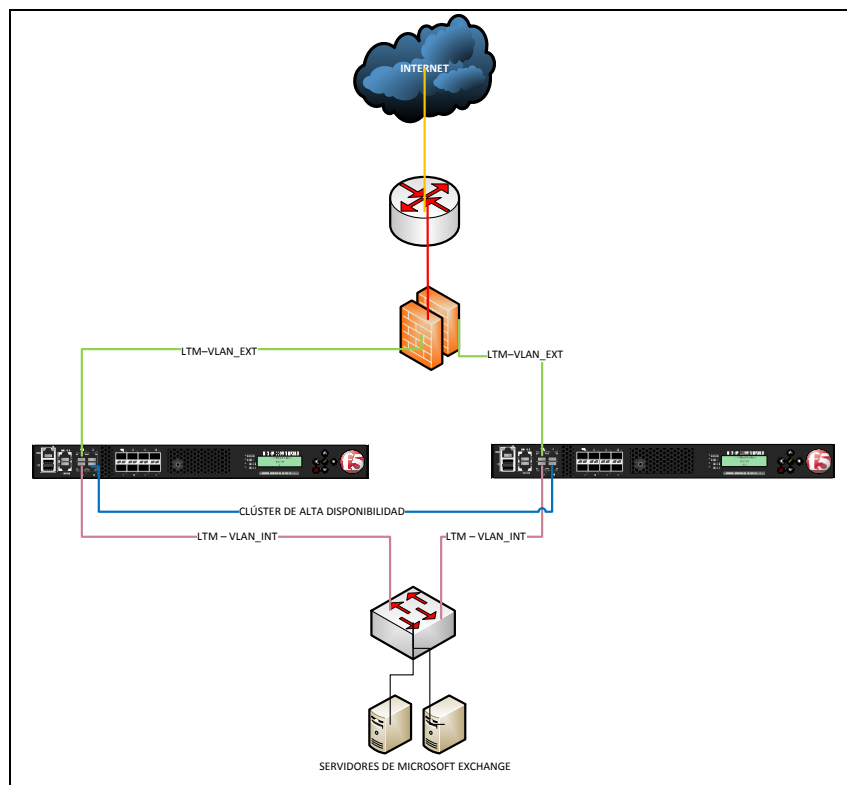


Ilustración 10. Diagrama final de solución F5

3.1.2.5.1.2 Configuración de los elementos básicos del sistema F5

La fase de implementación inicia con la configuración de los siguientes elementos del sistema de cada balanceador F5:

- Puerto de administración
- Dirección IP de administración, máscara de subred y su respectiva ruta de default Gateway.
- Host Name o nombre del equipo en nomenclatura FQDN
- Zona horaria
- Claves de acceso de usuarios admin y root

Para realizar la configuración de sistema de los elementos antes mencionados, es necesario seleccionar en la parte izquierda del panel de control de la interfaz web la opción System y posteriormente el submenú Platform, como se puede apreciar en la ilustración 11 a continuación:

System >> Platform	
Configuration	
General Properties	
Management Port Configuration	<input type="radio"/> Automatic (DHCP) <input checked="" type="radio"/> Manual
Management Port	IP Address(prefix): <input type="text" value="10.4.0.115"/> Network Mask: <input type="text" value="255.255.255.0"/> <input type="text" value="255.255.255.0"/> Management Route: <input type="text" value="10.4.0.254"/>
Host Name	<input type="text" value="F5.ennubedigital.com"/>
Host IP Address	<input type="text" value="Use Management Port IP Address"/>
Time Zone	<input type="text" value="America/Guayaquil"/>
User Administration	
Root Account	Password: <input type="password" value="*****"/> Confirm: <input type="password" value="*****"/>
Admin Account	Password: <input type="password" value="*****"/> Confirm: <input type="password" value="*****"/>

Ilustración 11. Configuraciones del sistema F5

El primer paso es seleccionar el modo de configuración del puerto de administración. Para la configuración de los equipos F5 de Nube Digital, se procedió con una configuración manual como se puede apreciar en la ilustración 12 a continuación:

Management Port Configuration	<input type="radio"/> Automatic (DHCP)	<input checked="" type="radio"/> Manual
-------------------------------	--	---

Ilustración 12. Configuración de puerto de administración

El siguiente elemento que debe ser configurado es la dirección IP de administración, junto con su máscara de subred y la dirección IP de default Gateway de esa red como se muestra en la ilustración 13 a continuación:

Management Port	IP Address[prefix]:	<input type="text" value="10.4.0.115"/>	
	Network Mask:	<input type="text" value="255.255.255.0"/>	<input type="text" value="255.255.255.0"/> ▼
	Management Route:	<input type="text" value="10.4.0.254"/>	

Ilustración 13. Configuración de direccionamiento IP de administración

A continuación se procede con la asignación de un nombre en formato FQDN (Fully Qualified Domain Name) a cada equipo F5 4200s utilizado en esta implementación como se muestra en la ilustración 14:

Host Name	<input type="text" value="F5.ennubedigital.com"/>
-----------	---

Ilustración 14. Configuración de Host Name

Posteriormente, se debe seleccionar la zona horaria en el listado respectivo, que en caso de Nube Digital es América/Guayaquil como se puede observar en la ilustración 15:

Time Zone	<input type="text" value="America/Guayaquil"/> ▼
-----------	--

Ilustración 15. Configuración de Zona Horaria

Finalmente, se procede con el cambio de las contraseñas de fábrica de los usuarios del sistema admin (interfaz web) y root (línea de comandos) como se aprecia en la ilustración 16:

User Administration	
Root Account	Password: <input type="password" value="*****"/> Confirm: <input type="password" value="*****"/>
Admin Account	Password: <input type="password" value="*****"/> Confirm: <input type="password" value="*****"/>

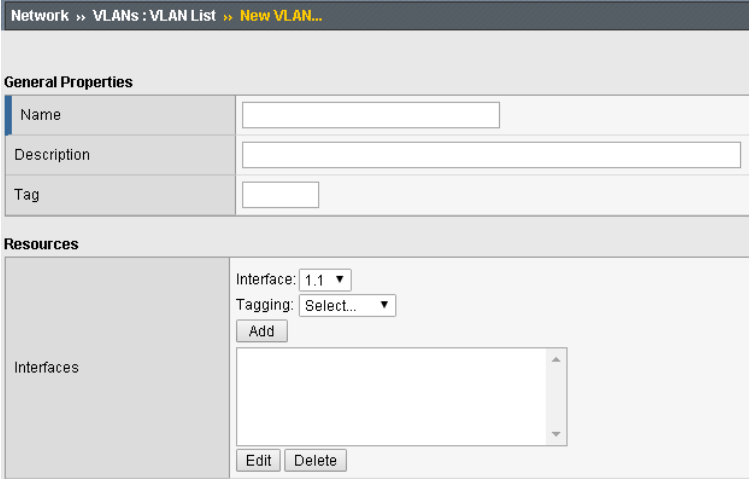
Ilustración 16. Configuración de claves de acceso

3.1.2.5.1.3 Configuración de elementos de red

En el siguiente paso del despliegue en producción de la solución de balanceo F5, se procede con la configuración de los siguientes elementos de red de cada equipo F5:

- VLANs
- Self IPs
- Routes – Default Gateway

La primera configuración que se realiza es la creación de los elementos llamados Vlan, que representan las interfaces lógicas para la comunicación entre el cliente final y cada F5 al igual que entre cada equipo F5 y los Servidores de la aplicación de correo electrónico de Nube Digital. Para la creación de una Vlan, debemos seleccionar en la parte izquierda del panel de control de la interfaz web la opción Network, seguida de la opción VLANs. Al dar clic en el botón ‘create’ vamos a observar una pantalla de interacción para ingreso de datos como se aprecia en la ilustración 17 a continuación:



The screenshot shows the 'New VLAN...' configuration page. It is divided into two main sections: 'General Properties' and 'Resources'. Under 'General Properties', there are three input fields: 'Name', 'Description', and 'Tag'. Under 'Resources', there is a list of interfaces on the left and a configuration area on the right. The configuration area includes a dropdown for 'Interface' (set to 1.1), a dropdown for 'Tagging' (set to Select...), an 'Add' button, and 'Edit' and 'Delete' buttons at the bottom.

Ilustración 17. Configuraciones de nueva VLAN

Como se observa en la ilustración 17, para crear la Vlan necesitamos ingresar un nombre de la misma, el ID de la VLAN que estamos creando y seleccionar la interfaz o Puerto donde va a estar conectado el cable de comunicación hacia esa VLAN.

Una vez que hayamos ingresado los datos respectivos, se da clic en el botón ‘Finished’ en la parte inferior de la pantalla, y la Vlan está creada. En el caso de Nube Digital

se realizó la creación de dos Vlans. Una Vlan Externa para la comunicación entre el Firewall y el F5 por donde ingresan las peticiones del cliente final y son respondidas igualmente, y otra Vlan Interna, para la comunicación entre los Servidores de la aplicación y el F5 como se muestra en la ilustración 18:

Name	Application	Tag	Untagged Interfaces	Tagged Interfaces	Partition / Path
VLAN_Externa		100	1.2		Common
VLAN_Interna		10	1.1		Common

Ilustración 18. VLANs

El siguiente paso, una vez creadas las Vlans, es la asignación de direccionamiento IP para la respectiva comunicación entre dispositivos conectados a las interfaces asignadas a cada Vlan. Para esto, debemos seleccionar en la parte izquierda del panel de control de la interfaz web la opción Network, seguida por la opción Self IPs, donde se mostrará una pantalla como se observa en la ilustración 19 a continuación:

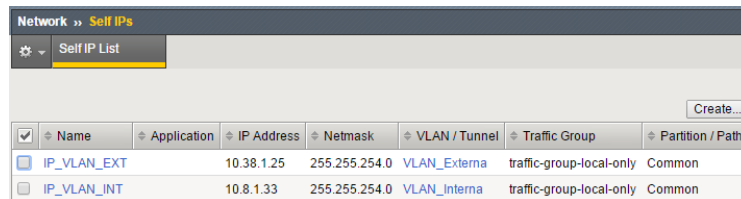
Name	<input type="text"/>
IP Address	<input type="text"/>
Netmask	<input type="text"/>
VLAN / Tunnel	http-tunnel
Port Lockdown	Allow None
Traffic Group	<input type="checkbox"/> Inherit traffic group from current partition / path traffic-group-local-only (non-floating)

Cancel Repeat Finished

Ilustración 19. Creación de Self IPs

Como se puede apreciar en la ilustración 19, cada Self IP está compuesta de un nombre, una dirección IP y su máscara de subred, igualmente se debe seleccionar la Vlan a la cual va a estar asociada, y el resto de configuraciones se las recomienda mantener por defecto.

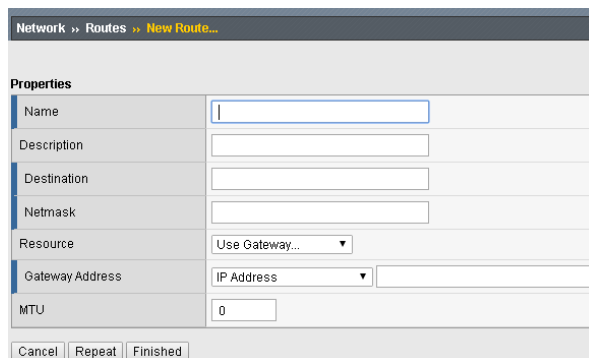
Una vez que se ingresan todos los datos de cada vlan, se da clic en el botón ‘Finished’ en la parte inferior de la pantalla y se habrán creado las Self IPs. Para el caso de Nube Digital, se procedió con la creación de dos Self IPs; es decir, una dirección IP de comunicación para cada Vlan anteriormente creada como se puede apreciar en la ilustración 20 a continuación:



<input checked="" type="checkbox"/>	Name	Application	IP Address	Netmask	VLAN / Tunnel	Traffic Group	Partition / Path
<input checked="" type="checkbox"/>	IP_VLAN_EXT		10.38.1.25	255.255.254.0	VLAN_Externa	traffic-group-local-only	Common
<input checked="" type="checkbox"/>	IP_VLAN_INT		10.8.1.33	255.255.254.0	VLAN_Interna	traffic-group-local-only	Common

Ilustración 20. Self IPs

Igualmente es necesario crear una ruta estática por defecto o también denominada default Gateway, la que permite y asegura que todas las peticiones de salida desde el equipo F5, sean direccionadas hacia el firewall siempre. Para esta configuración, se debe seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Network, seguida por la opción Routes. Es necesario dar clic sobre el botón ‘create’ en la pantalla que aparece como se puede observar en la ilustración 21:



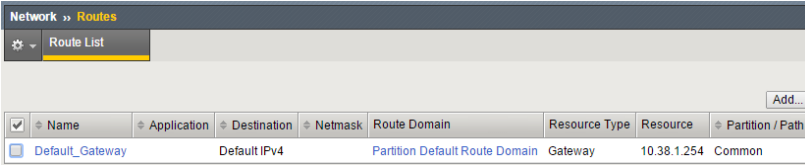
Properties	
Name	<input type="text"/>
Description	<input type="text"/>
Destination	<input type="text"/>
Netmask	<input type="text"/>
Resource	Use Gateway... ▾
Gateway Address	IP Address ▾ <input type="text"/>
MTU	0 <input type="text"/>

Cancel Repeat Finished

Ilustración 21. Creación de Rutas Estáticas

En la pantalla que aparece, se ingresa el nombre de la ruta, el destino y máscara de subred, que en este caso deberán ser los valores 0.0.0.0 y 0.0.0.0, que representan la ruta por defecto de default Gateway, y por último la dirección IP del firewall en la opción de

dirección de siguiente salto, para la creación de la ruta estática como se aprecia en la siguiente ilustración 22:



<input checked="" type="checkbox"/>	Name	Application	Destination	Netmask	Route Domain	Resource Type	Resource	Partition / Path
<input type="checkbox"/>	Default_Gateway		Default IPv4		Partition Default Route Domain	Gateway	10.38.1.254	Common

Ilustración 22. Ruta de Default Gateway

3.1.2.5.1.4 Configuración de elementos de balanceo

Al terminar la configuración de los elementos de red del equipo F5, se procede con la configuración de los siguientes elementos de balanceo, los cuales son los que permiten crear una puerta de entrada o comunicación entre el cliente final y las aplicaciones:

- Nodes
- Pools
- iRules
- Monitores
- Perfiles SSL
- Virtual Servers

En la primera configuración de balanceo, es necesario definir las direcciones IP de los servidores virtuales de correo electrónico o CAS servers, para lo cual se debe seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Local Traffic, seguida de la opción Nodes, donde aparece la pantalla de la ilustración 23 a continuación:

Ilustración 23. Creación de un nodo

En la pantalla que aparece, es necesario ingresar un nombre del servidor o nodo y su dirección IP o nombre en formato FQDN. Para el resto de configuraciones se debe mantener las de defecto. La única que se puede cambiar es la configuración del monitor del servidor, en donde F5 recomienda siempre que se mantenga un monitor simple como ‘ping’, el cual es el monitor por defecto asignado para estos elementos de balanceo. Una vez culminado el ingreso de los datos, se debe dar clic sobre el botón ‘Finished’ y se obtiene los nodos como se aprecia en la siguiente ilustración 24:

Status	Name	Application	Address	Description	Partition / Path
<input type="checkbox"/>	ex-10.ennubedigital.com		10.8.1.65	Exchange 01	Common
<input type="checkbox"/>	ex-11.ennubedigital.com		10.8.1.66	Exchange 02	Common

Ilustración 24. Nodos

El siguiente paso, es la configuración de un pool de servidores de las mismas características, en este caso un pool con dos servidores de correo electrónico. Se debe seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Local Traffic, seguida de la opción Pools, para que aparezca la pantalla que se muestra en la siguiente ilustración 25:

Ilustración 25. Creación de un Pool

En la pantalla que aparece, es necesario asignar un nombre al pool, un monitor de salud y los miembros del pool, que en este caso serán los nodos previamente creados.

También es necesario asignar un puerto del servicio. En el caso de Nube Digital se utiliza el puerto 443 para una conexión segura y encriptada mediante un certificado digital entre el cliente OWA y los servidores CAS, así como los puertos 995 y 465 para prestar otros servicios propietarios de Microsoft adicionalmente. Una vez finalizado el ingreso de datos, se debe dar clic sobre el botón 'Finished' para cada pool, y se obtienen los diferentes pools como se aprecia en la siguiente ilustración 26:

Status	Name	Application	Members	Partition / Path
	Pool_ExchangePOP3Sec		2	Common
	Pool_Exchange_Nube_Digital		2	Common
	Pool_Exchange_SMTTP_Seguro		2	Common

Ilustración 26. Pools

En la siguiente ilustración 27, se puede apreciar cada pool con los nodos o miembros de pool asignados y su respectivo puerto de servicio:

<input checked="" type="checkbox"/>	Status	Pool/Member
<input type="checkbox"/>	●	Pool_ExchangePOP3Sec
<input type="checkbox"/>	●	-- ex-10.ennubedigital.com:995
<input type="checkbox"/>	●	-- ex-11.ennubedigital.com:995
<input type="checkbox"/>	●	Pool_Exchange_Nube_Digital
<input type="checkbox"/>	●	-- ex-10.ennubedigital.com:443
<input type="checkbox"/>	●	-- ex-11.ennubedigital.com:443
<input type="checkbox"/>	●	Pool_Exchange_SMTP_Seguro
<input type="checkbox"/>	●	-- ex-10.ennubedigital.com:465
<input type="checkbox"/>	●	-- ex-11.ennubedigital.com:465

Ilustración 27. Miembros de Pools

Como se puede observar en la ilustración anterior, se realizó la creación de 3 pools que contienen a los mismos servidores de correo electrónico, pero que responden por un puerto diferente en cada caso, para proveer 3 diferentes servicios.

Previo a la creación del Virtual Server, que es el elemento final de balanceo y el que recibe directamente las peticiones de servicio desde el cliente final, es necesario la creación de dos elementos importantes que forman parte del Virtual Server. Uno de los elementos permite la encriptación de la conexión entre el cliente final y el F5, así como entre el F5 y los servidores de correo electrónico, y el otro permite el monitoreo constante de las peticiones reales entre el cliente y los servidores.

El primer elemento que debe crearse o generarse es el certificado digital. Este elemento por lo general es solicitado a una institución autorizada para emitir este tipo de elementos de forma segura y firmada. En el caso de Nube Digital, el certificado digital fue emitido por Go Daddy, Inc. En la ilustración 28 se puede observar la pantalla en donde se importa el certificado generado, al equipo F5 desde la opción System, File Management, SSL Certificate List. En la pantalla que aparece es necesario navegar en el ordenador para seleccionar el archivo emitido por Go Daddy al igual que una clave de seguridad previamente compartida por el creador del certificado:

Ilustración 28. Ingreso de Certificado SSL al sistema F5

Una vez ingresado el certificado al sistema, se puede apreciar en el listado de certificados del equipo F5 como se muestra en la siguiente ilustración 29:

<input checked="" type="checkbox"/>	Name	Contents	Common Name	Organization	Expiration	Partition / Path
<input type="checkbox"/>	Exchange	Certificate & Key	portal.ennubedigital.com		Jul 4, 2016	Common
<input type="checkbox"/>	GoDaddy_Intermediate	Certificate	Go Daddy Secure Certific...	GoDaddy.com	May 3, 2031	Common

Ilustración 29. Ingreso de Certificado SSL al sistema F5

Con este certificado digital, se procede a la creación del perfil SSL tanto de cliente como de servidor, que serán los encargados de la encriptación de las conexiones.

Se debe seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Local Traffic, Profiles y seguida de la opción SSL. Para el perfil entre cliente final y F5, se debe seleccionar la opción Client donde aparece la pantalla que se observa en la siguiente ilustración 30:

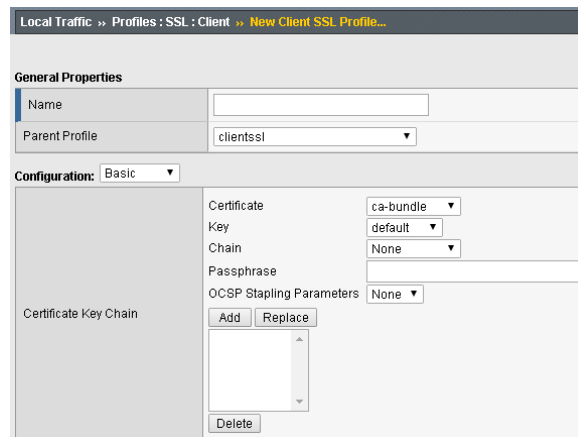


Ilustración 30. Client SSL profile

Para el perfil entre F5 y servidores, se debe seleccionar la opción Server, donde aparece la pantalla que se muestra en la ilustración 31:

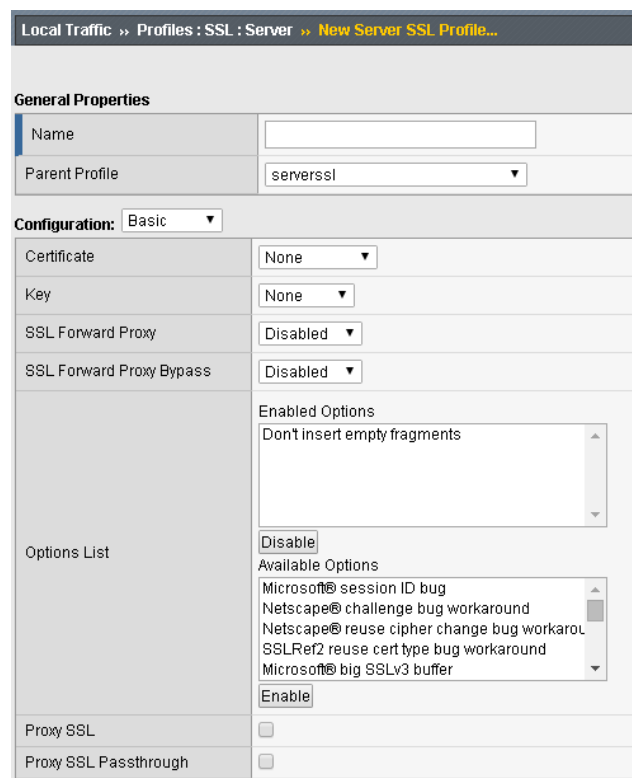


Ilustración 31. Server SSL Profile.

En ambas opciones, es necesario seleccionar el certificado digital previamente importado al sistema para obtener los perfiles que serán asignados al Virtual Server. En este caso las siguientes ilustraciones 32 y 33, muestran los perfiles generados:

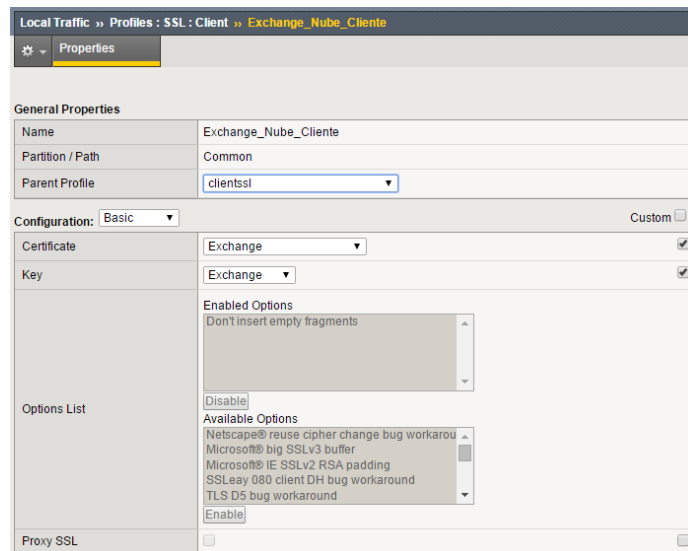


Ilustración 32. Perfil SSL de cliente

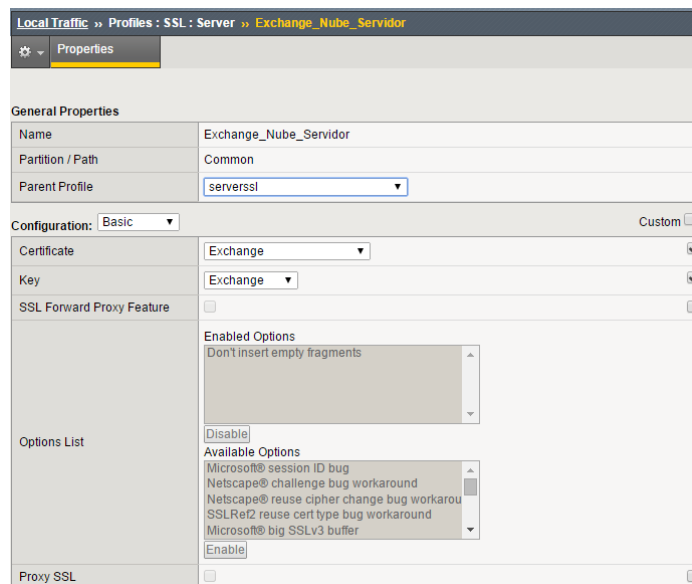


Ilustración 33. Perfil SSL de servidor

El siguiente elemento que debe ser creado previo al Virtual Server, es un script llamado iRule, que es un lenguaje de programación TCL propietario de F5. Para esto, debemos seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Local Traffic, seguida de la opción iRules, donde ingresamos el script generado, cuyo propósito es monitorear las conexiones entre los clientes finales y los servidores, manteniendo un registro de la dirección IP de origen y puerto de conexión, dirección del Virtual Server seleccionado, y también dirección y puerto del servidor de destino que atiende

la petición original. Esto se lo ingresa en la pantalla que se muestra en la ilustración 34 a continuación:

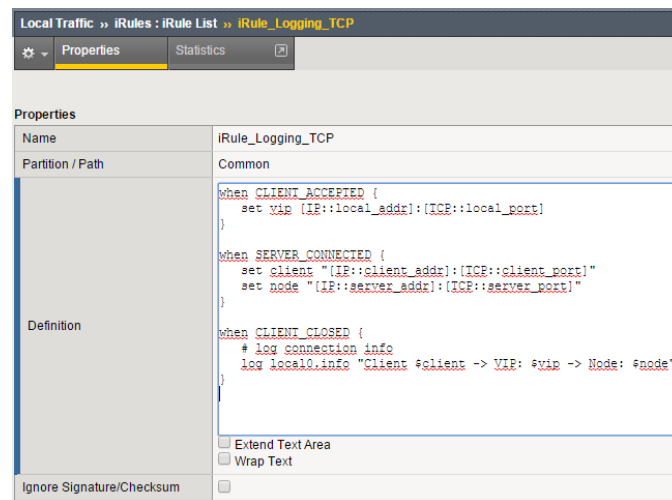


Ilustración 34. iRule

Una vez que se tiene estos elementos listos, se procede con la creación del Virtual Server al seleccionar en la parte izquierda del panel de control de la interfaz web, la opción Local Traffic, seguida de la opción Virtual Server y dar clic en el botón ‘Create’ para obtener la pantalla de ingreso de datos que se muestra por partes en las siguientes ilustraciones. La ilustración 35 muestra la parte de propiedades generales del Virtual Server:

Ilustración 35. Propiedades generales de un Virtual Server

En la ilustración anterior se debe ingresar el nombre del Virtual Server y una descripción de ser necesario. El tipo de Virtual Server que normalmente se maneja de tipo

estándar. Igualmente es necesario ingresar la IP de destino, o la que está relacionada al servicio como tal y el puerto por el que se va a recibir la petición hacia esa IP definida.

La siguiente ilustración 36 muestra la parte de configuración del Virtual Server, donde se asignan los diferentes perfiles necesarios. En este caso, los perfiles SSL previamente creados:

The screenshot displays the configuration page for a Virtual Server, titled 'Configuration: Basic'. The interface includes several dropdown menus and profile selection areas:

- Protocol:** TCP
- Protocol Profile (Client):** tcp
- Protocol Profile (Server):** (Use Client Profile)
- HTTP Profile:** None
- FTP Profile:** None
- RTSP Profile:** None
- SSL Profile (Client):** This section features a 'Selected' list (currently empty) and an 'Available' list containing: /Common, clientsssl, clientsssl-insecure-compatible, crypto-server-default-clientssl, and worm-default-clientssl. Navigation arrows (<< and >>) are present between the lists.
- SSL Profile (Server):** This section features a 'Selected' list (currently empty) and an 'Available' list containing: /Common, apm-default-serverssl, crypto-client-default-serverssl, pcoip-default-serverssl, and serverssl. Navigation arrows (<< and >>) are present between the lists.
- SMTPS Profile:** None
- Client LDAP Profile:** None
- Server LDAP Profile:** None
- SMTP Profile:** None
- VLAN and Tunnel Traffic:** All VLANs and Tunnels
- Source Address Translation:** None

Ilustración 36. Configuraciones de un Virtual Server

Por último, se debe seleccionar el pool de servidores previamente creado al igual que un método de persistencia para las conexiones generadas, y también se debe seleccionar el iRule previamente creado, en la pantalla de recursos del virtual server como se observa en la siguiente ilustración 37:

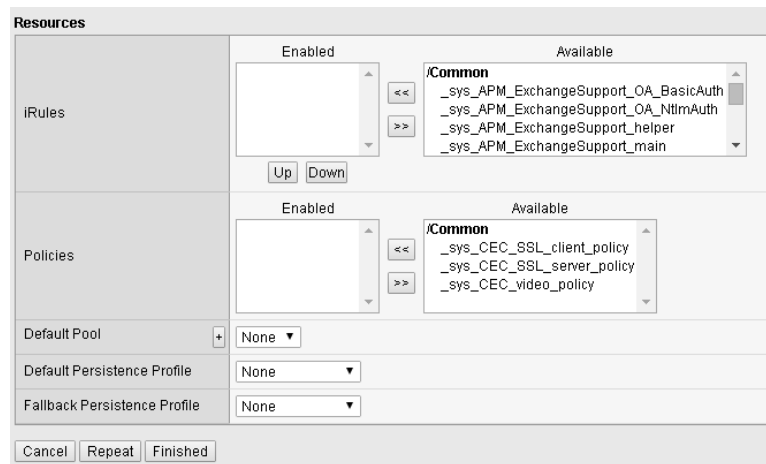


Ilustración 37. Recursos de un Virtual Server

Una vez culminada la configuración de los virtual servers, se obtiene los diferentes servicios como se puede observar en la siguiente ilustración 38:

Status	Name	Application	Destination	Service Port	Type	Resources	Partition / Path
<input checked="" type="checkbox"/>	VS_Default_Gateway		any	0 (Any)	Forwarding (IP)	Edit...	Common
<input type="checkbox"/>	VS_Exchange_Nube_Digital		10.38.1.26	443 (HTTPS)	Standard	Edit...	Common
<input type="checkbox"/>	VS_Exchange_POP3Sec		10.38.1.26	995	Standard	Edit...	Common
<input type="checkbox"/>	VS_Exchange_SMTP_Seguro		10.38.1.26	465	Standard	Edit...	Common

Ilustración 38. Virtual Servers

Para culminar el despliegue de la solución, se procede con los cambios de la dirección IP de default gateway en los servidores CAS, hacia la dirección IP configurada en la VLAN interna del equipo F5 10.8.1.33 como se muestra en las ilustraciones 39 y 40 a continuación:

```

C:\Users\exchadmin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : ex-10
Primary Dns Suffix . . . . . : ennubedigital.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ennubedigital.com

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : 
   Description . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . : 00-50-56-81-04-FB
   DHCP Enabled. . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::30be:124d:39c3:a965%15(Preferred)
   IPv4 Address. . . . . : 10.8.1.65(Preferred)
   Subnet Mask . . . . . : 255.255.254.0
   Default Gateway . . . . . : 10.8.1.33
   DHCPv6 IAID . . . . . : 302010454
   DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-1F-C3-8C-00-50-56-81-04-FB

DNS Servers . . . . . : 10.8.1.10
                       10.8.1.14
NetBIOS over Tcpip. . . . . : Enabled

```

Ilustración 39. Cambio de Default Gateway servidor CAS #1

```

(c) 2012 Microsoft Corporation. All rights reserved.
C:\Users\exchadmin>ipconfig /all
Windows IP Configuration

Host Name . . . . . : ex-11
Primary Dns Suffix . . . . . : ennubedigital.com
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . : ennubedigital.com

Ethernet adapter Ethernet:

Connection-specific DNS Suffix . : 
Description . . . . . : Intel(R) 82574L Gigabit Network Connection
Physical Address. . . . . : 00-50-56-81-56-08
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::80ac:603e:9ec3:da10%15(Preferred)
IPv4 Address. . . . . : 10.8.1.66(Preferred)
Subnet Mask . . . . . : 255.255.254.0
Default Gateway . . . . . : 10.8.1.33
DHCPv6 Iaid . . . . . : 302010454
DHCPv6 Client DUID. . . . . : 00-01-00-01-1B-30-E8-9F-00-50-56-81-56-08

DNS Servers . . . . . : 10.8.1.10
                       10.8.1.14
NetBIOS over Tcpip. . . . . : Enabled

```

Ilustración 40. Cambio de Default Gateway servidor CAS #2

Una vez que se ha culminado la configuración de todos los elementos del sistema, de red y de balanceo, se realiza una validación final de todo y se procede con la creación de un respaldo de configuraciones mediante un elemento llamado ‘Archive’ a donde se accede al seleccionar en la parte izquierda del panel de control de la interfaz web, la opción System, seguido por la opción Archive y se genera el archivo de respaldo como se muestra en la siguiente ilustración 41:

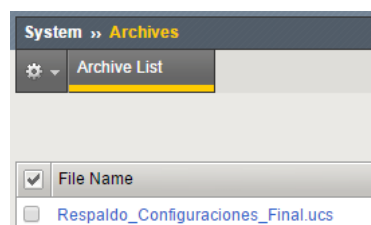
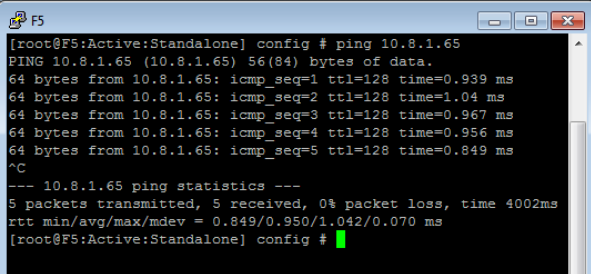


Ilustración 41. Creación de archivo de respaldo

3.1.2.5.2 Pruebas

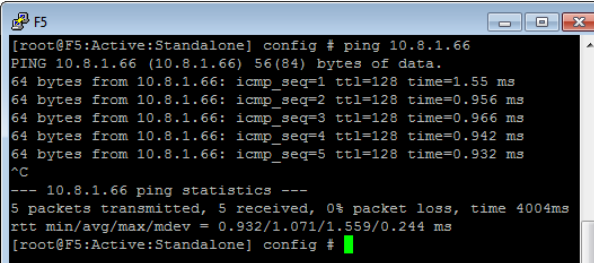
Una vez finalizada la configuración y despliegue de este proyecto, se procede a realizar las pruebas de comunicación de los equipos involucrados en la solución para el servicio de correo electrónico, así como las pruebas de acceso al servicio mediante el aplicativo Microsoft Outlook 2013 y mediante explorador Web vía OWA, para validar el correcto funcionamiento del servicio.

La primera prueba realizada es el ping desde el equipo F5 hacia los servidores de correo como se aprecia en las ilustraciones 42 y 43:



```
[root@F5:Active:Standalone] config # ping 10.8.1.65
PING 10.8.1.65 (10.8.1.65) 56(84) bytes of data.
64 bytes from 10.8.1.65: icmp_seq=1 ttl=128 time=0.939 ms
64 bytes from 10.8.1.65: icmp_seq=2 ttl=128 time=1.04 ms
64 bytes from 10.8.1.65: icmp_seq=3 ttl=128 time=0.967 ms
64 bytes from 10.8.1.65: icmp_seq=4 ttl=128 time=0.956 ms
64 bytes from 10.8.1.65: icmp_seq=5 ttl=128 time=0.849 ms
^C
--- 10.8.1.65 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.849/0.950/1.042/0.070 ms
[root@F5:Active:Standalone] config #
```

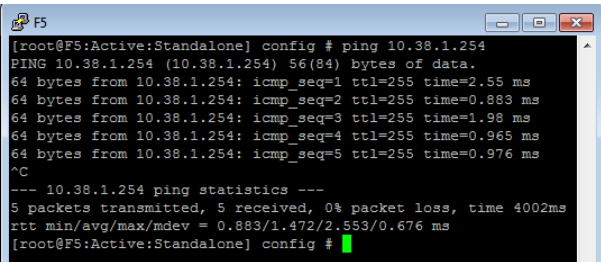
Ilustración 42. Prueba de comunicación ICMP desde F5 a CAS Server #1



```
[root@F5:Active:Standalone] config # ping 10.8.1.66
PING 10.8.1.66 (10.8.1.66) 56(84) bytes of data.
64 bytes from 10.8.1.66: icmp_seq=1 ttl=128 time=1.55 ms
64 bytes from 10.8.1.66: icmp_seq=2 ttl=128 time=0.956 ms
64 bytes from 10.8.1.66: icmp_seq=3 ttl=128 time=0.966 ms
64 bytes from 10.8.1.66: icmp_seq=4 ttl=128 time=0.942 ms
64 bytes from 10.8.1.66: icmp_seq=5 ttl=128 time=0.932 ms
^C
--- 10.8.1.66 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4004ms
rtt min/avg/max/mdev = 0.932/1.071/1.559/0.244 ms
[root@F5:Active:Standalone] config #
```

Ilustración 43. Prueba de comunicación ICMP desde F5 a CAS Server #2

La siguiente prueba realizada es el ping desde el equipo F5 hacia el default Gateway, es decir hacia el firewall, como se muestra en la ilustración 44:



```
[root@F5:Active:Standalone] config # ping 10.38.1.254
PING 10.38.1.254 (10.38.1.254) 56(84) bytes of data.
64 bytes from 10.38.1.254: icmp_seq=1 ttl=255 time=2.55 ms
64 bytes from 10.38.1.254: icmp_seq=2 ttl=255 time=0.883 ms
64 bytes from 10.38.1.254: icmp_seq=3 ttl=255 time=1.98 ms
64 bytes from 10.38.1.254: icmp_seq=4 ttl=255 time=0.965 ms
64 bytes from 10.38.1.254: icmp_seq=5 ttl=255 time=0.976 ms
^C
--- 10.38.1.254 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.883/1.472/2.553/0.676 ms
[root@F5:Active:Standalone] config #
```

Ilustración 44. Prueba de comunicación ICMP desde F5 a Default Gateway (Firewall)

La siguiente prueba a realizar es la conectividad entre el aplicativo de Microsoft Outlook 2013 instalado en un cliente, con la configuración de la cuenta de correo, que está apuntando al Virtual Server de Exchange creado en el equipos F5 como se puede observar en la ilustración 45 a continuación:

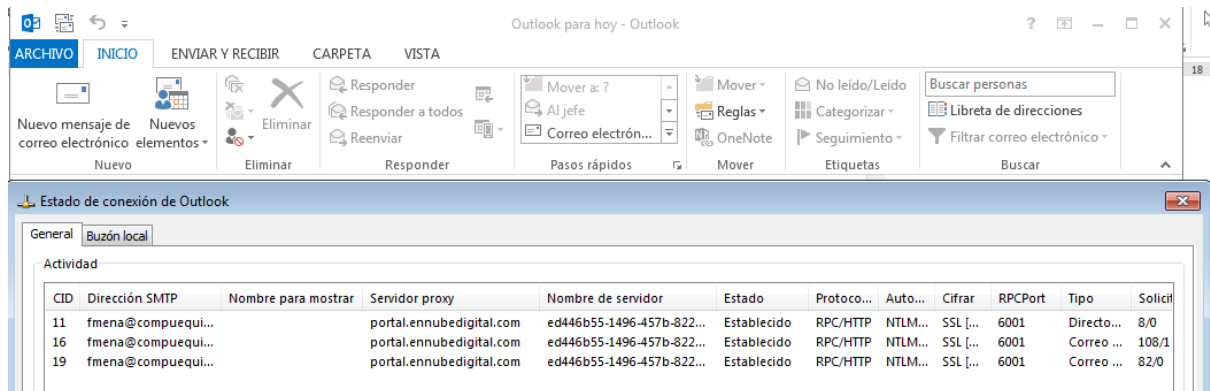


Ilustración 45. Prueba de conectividad desde Microsoft Outlook 2013

Otra prueba muy importante es la conexión desde un explorador web, hacia el Virtual Server de correo electrónico de Nube Digital. Como se puede observar en la ilustración 46, la conexión es exitosa y el servicio se encuentra operativo:

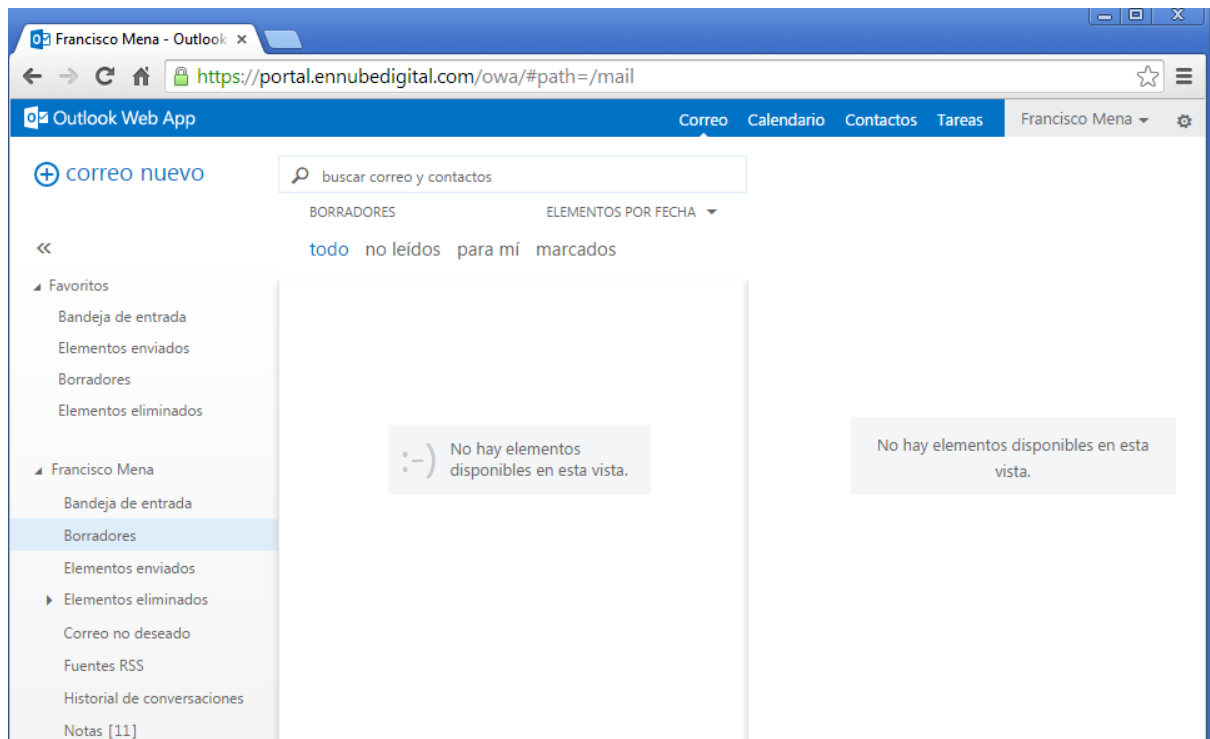


Ilustración 46. Prueba de conectividad desde explorador Web - OWA

3.1.2.6 Mantenimiento

En base al contrato de servicios entre Nube Digital y Compuequip DOS, el mantenimiento tanto preventivo como correctivo después de la implementación de este proyecto, correrá a cuenta del técnico implementador de Compuequip DOS, en base a los requerimientos o comunicaciones presentadas por parte del cliente Nube Digital.

Se realizarán dos mantenimientos físicos de cada equipo balanceador F5 por cada año de contrato, es decir desmontar del rack en el que se encuentran instalados, limpieza de cada equipo F5 externamente, eliminación de polvo externo e interno mediante una máquina sopladora de aire y comprobación de funcionamiento correcto de fuentes de poder y del sistema como tal. Igualmente, se realizarán cambios en configuraciones para solucionar problemas de rendimiento que se presenten, en base a la demanda del servicio o solicitud del cliente Nube Digital.

3.1.3 Verificación de la Hipótesis

¿La implementación de un clúster de equipos de balanceo de carga F5 permite mejorar el servicio de correo electrónico de forma inmediata y además permite un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo?

Antes de la implementación de los equipos F5, la aplicación de correo electrónico estaba siendo abastecida para todos los clientes finales, con un solo servidor de correo electrónico. Aunque se generó un nuevo servidor de correo, este no pudo ser balanceado mediante software, por temas de incompatibilidad de las tarjetas de red virtuales configuradas en los servidores físicos, por lo que de igual forma solo uno de los servidores daba el servicio a la vez. Por ende, el servicio de correo electrónico sufría caídas temporales al momento de realizar algún mantenimiento de los servidores hasta poder realizar el cambio entre ellos y ofrecer nuevamente el servicio. Esto a su vez causaba una restricción en el crecimiento del servicio de correo electrónico.

Con la implementación del clúster de balanceadores F5, al formar un pool de servidores de correo, se logró balancear el servicio entre los dos servidores que mantiene el cliente Nube Digital. Además, se logró realizar una encriptación entre las conexiones desde el cliente final hacia los servidores de correo, pero manteniendo la red de los mismos, de manera privada hacia el cliente. También se logró implementar un mecanismo de mantenimiento transparente así como la posibilidad de un crecimiento en el número de servidores de correo, como en el crecimiento del servicio propio como tal hacia más clientes, en un corto y mediano plazo, sin necesidad de adquirir un nuevo equipo de balanceo físico, y solamente generar nuevos servidores virtuales de correo electrónico. (Villavicencio, 2015).

De igual manera, al realizar la comparación del tiempo fuera de servicio del correo electrónico antes de la implementación del equipo de balanceo de carga F5, se tenía un aproximado de 1 hora de fuera de servicio, en cada ventana de mantenimiento de los equipos involucrados. Con el despliegue en producción del equipo de balanceo F5, los tiempos de fuera de servicio se han reducido a 15 segundos aproximadamente. Es decir, que el tiempo fuera de servicio ha decrecido en un 240%.

Según lo comprueba la comparación entre indicadores y estadísticas de balanceo, la implementación de un clúster de alta disponibilidad de equipos de balanceo de carga F5 si permite mejorar el servicio de correo electrónico de forma inmediata y además permite un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo.

4. ANÁLISIS DE RESULTADOS

En este capítulo se encuentran los resultados de la implementación del proyecto, así como el respectivo análisis de los mismos; que están orientados a la comprobación de la hipótesis de estudio de este proyecto.

En primera instancia, en la ilustración 47 se muestra la distribución de carga de las peticiones del servicio de correo electrónico desde los usuarios finales hacia el clúster de servidores CAS de Microsoft Exchange 2013, a través del Virtual Server configurado en cada balanceador F5, a lo largo de un mes después de la implementación.

The screenshot shows the 'Local Traffic' statistics page in F5. It includes a table with columns for Status, Pool/Member, Partition/Path, Bits (In/Out), Packets (In/Out), Connections (Current/Maximum/Total), Requests (Total), and Request Queue (Depth/Maximum Age). Three rows are visible, representing different traffic pools.

Nube													
			Bits		Packets		Connections			Requests	Request Queue		
✓	Status	Pool/Member	Partition / Path	In	Out	In	Out	Current	Maximum	Total	Total	Depth	Maximum Age
	●	Pool_Exchange_Nube_Digital	Common	703.7G	2.3T	391.4M	401.3M	161	1.5K	3.7M	30.0M	0	0
	●	-- ex-10.ennubedigital.com:443	Common	339.1G	1.1T	189.4M	198.7M	80	702	1.8M	13.0M	0	0
	●	-- ex-11.ennubedigital.com:443	Common	364.5G	1.2T	201.9M	202.5M	81	798	1.8M	17.0M	0	0

Ilustración 47. Balanceo equitativo de conexiones a servidores CAS

En la ilustración anterior, se puede observar que después de la implementación del equipo de balanceo F5, se logra realizar una distribución equitativa de carga de las peticiones de los usuarios del servicio de correo electrónico, hacia los dos servidores CAS que forman parte del clúster de esta aplicación.

Así mismo, se evidencia en la siguiente ilustración 48, que el servicio de correo electrónico se mantiene correcto y equitativo, con una cantidad mínima de pérdidas y drops de paquetes:

Packet Discards	
Maint mode virtual server or controller	0
Connection limit reached (virtual address)	0
Connection limit reached (virtual server)	0
No clientside connection	0
No virtual server, NAT or SNAT for request	6.7G
No available memory for connection	0

Packet Statistics	
Dropped Packets	333.3K
Errors Incoming	0
Errors Outgoing	0

Traffic Management CPU Usage	
Total Cycles	103.7P
Idle Cycles	2.6P
Sleep Cycles	96.0P

Ilustración 48. Estadísticas de pérdida de paquetes

El siguiente resultado obtenido, se basa en la seguridad de las conexiones entre el cliente y el equipo de balanceo F5, al igual que entre el equipo F5 y cada uno de los servidores de correo electrónico, como se aprecia en las ilustraciones 49 y 50 a continuación:

VS_Exchange_Nube_Digital							
Summary		Analytics					
Display Options							
Data Format	Normalized						
Auto Refresh	Disabled Refresh						
<< Back Clear All Statistics							
Traffic Details							
	Bits		Packets		Connections		
Type	In	Out	In	Out	Current	Maximum	Total
All	112.7G	331.5G	63.4M	95.4M	165	1.1K	799.9K
Ephemeral	0	0	0	0	0	0	0
Other	112.7G	331.5G	63.4M	95.4M	165	1.1K	799.9K
Profiles							
Select Profile	Exchange_Nube_Cliente						
Clear Profile Statistics							
Bits							
	Inbound			Outbound			
Encrypted	86.6G			291.5G			
Decrypted	81.2G			272.8G			

Ilustración 49. Encriptación entre Cliente y Equipo F5

VS_Exchange_Nube_Digital

Summary Analytics

Display Options

Data Format: Normalized

Auto Refresh: Disabled Refresh

<< Back Clear All Statistics

Traffic Details

Type	Bits		Packets		Connections		
	In	Out	In	Out	Current	Maximum	Total
All	112.7G	331.5G	63.4M	95.4M	170	1.1K	800.0K
Ephemeral	0	0	0	0	0	0	0
Other	112.7G	331.5G	63.4M	95.4M	170	1.1K	800.0K

Profiles

Select Profile: Exchange_Nube_Servidor

Clear Profile Statistics

Bits

	Inbound	Outbound
Encrypted	291.3G	86.0G
Decrypted	272.7G	81.2G

Ilustración 50. Encriptación entre Equipo F5 y Servidores CAS

Las ilustraciones anteriores, muestran los resultados favorables respecto al correcto uso de los certificados digitales SSL, y la seguridad de la transferencia de información y comunicaciones, entre el cliente final y los servidores CAS de Exchange 2013 de Nube Digital.

Otro de los resultados obtenidos en la implementación del proyecto es la configuración final de los servicios de correo electrónico en cada balanceador F5, mediante una de las características del equipo para respaldar los cambios realizados como se puede observar en la siguiente ilustración 51:

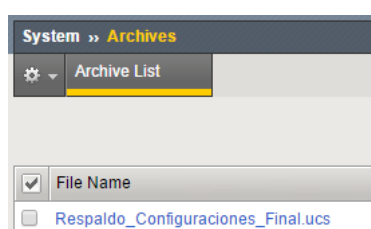


Ilustración 51. Archive – Respaldo de configuración final

Esta característica del equipo F5, permite una migración hacia cualquier otro equipo de la misma marca, en caso de ser necesario por cualquier problema que pueda presentarse.

Adicionalmente, para cumplir con los objetivos específicos planteados como parte de este proyecto de tesis, se muestra a continuación, la tabla 2, con el resumen de datos otorgada por Nube Digital:

Problema	Antes de Implementar F5	Después de implementar F5
Quejas por calidad de servicio	40%	5%
Tiempo fuera de servicio (seg.)	3600	15

Tabla 2. Mejoras en quejas por calidad de servicio y tiempo fuera de servicio

Según los datos emitidos por el cliente Nube Digital, después de la implementación de la solución de balanceo F5, se observa una mejora notable en el servicio de correo electrónico de forma inmediata y además la capacidad de permitir un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo gracias a la forma transparente de configuración de nuevos servidores de correo en el caso de ser necesarios, mediante la inclusión de miembros en el pool creado. Adicionalmente, se evidencia que existe una reducción en el tiempo fuera de servicio cuando se ejecutan ventanas de trabajo, de 1 hora (3600 segundos) a 15 segundos, lo que representa una mejora del 240%, como se puede observar en las siguientes ilustraciones 52 y 53 a continuación:

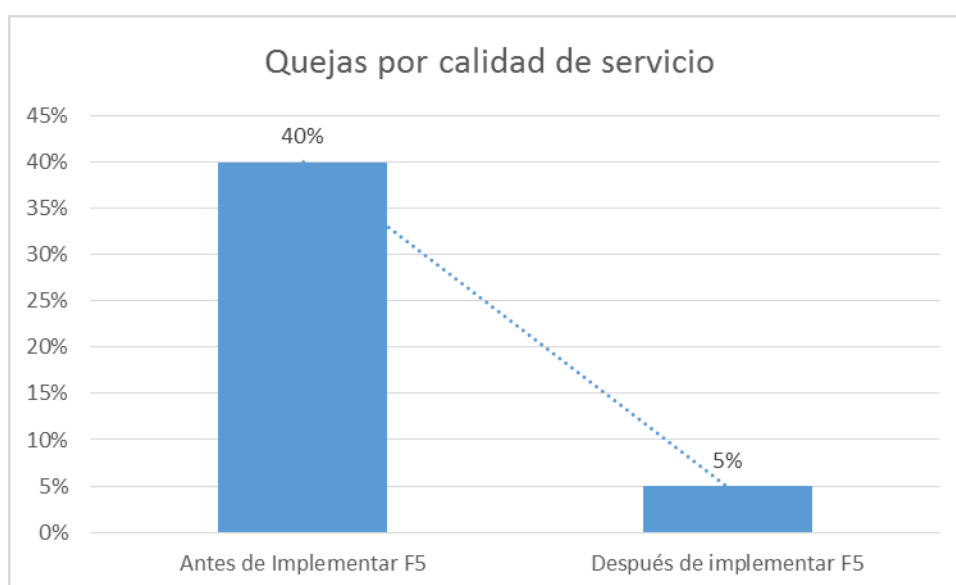


Ilustración 52. Quejas por calidad de servicio



Ilustración 53. Tiempo fuera de servicio

Finalmente, el F5 permite obtener estadísticas de comportamiento de la aplicación para el monitoreo y afinación del servicio de correo electrónico de Nube Digital como se muestra en las siguientes ilustraciones:

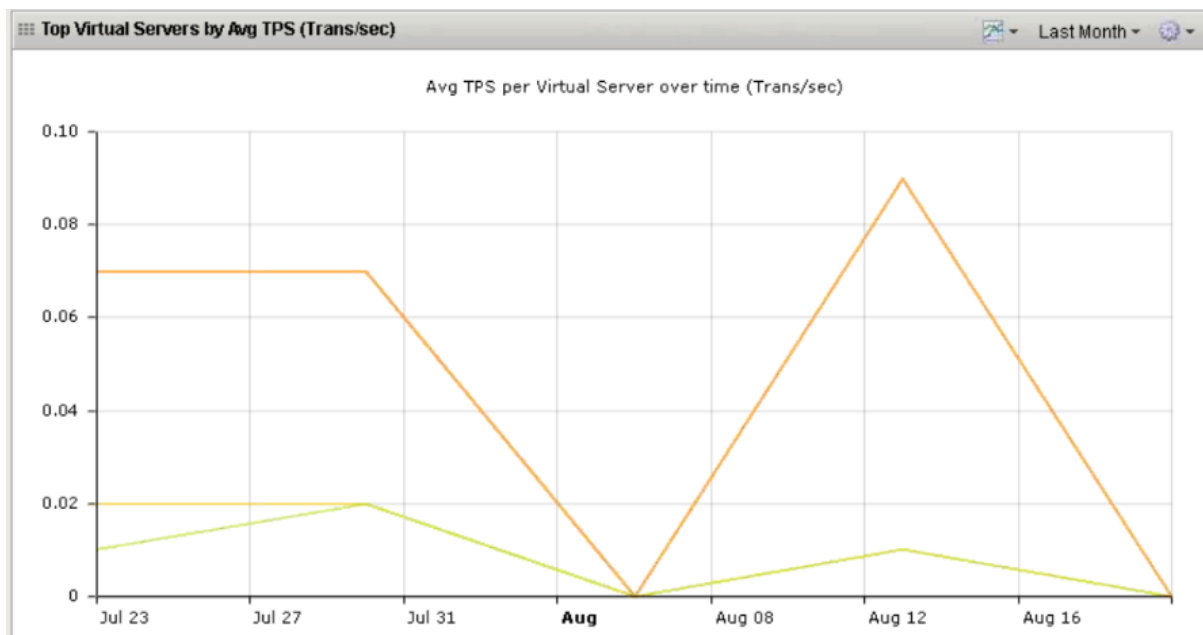


Ilustración 54. Conexiones hacia el Virtual Server de correo electrónico

Name	Avg TPS (Trans/sec)	Avg Request Throughput (bits/s)
/Microsoft-Server-ActiveSync	3.83	23,433.71
/ews/exchange.asmx	0.35	4,168.33
/EWS/Exchange.asmx	0.05	695.74
/rpc/rpcproxy.dll	0.04	156.77
/autodiscover/autodiscover.xml	0.03	261.41
/OAB/11d7bd88-d4be-4cb4-9491-6a7d12cf66eb/oab.xml	0.03	127.15
Aggregated	0.03	148.47
/ews/exchange.asmx/s/GetUserPhoto	0.03	147.09
/OAB/83898423-a78c-43ea-9ef5-313ba41e5685/oab.xml	0.03	122.32
/OAB/83898423-a78c-43ea-9ef5-313ba41e5685/7b9eee5...1085.lzx	0.02	111.36

Ilustración 55. URIs accedidas por los clientes

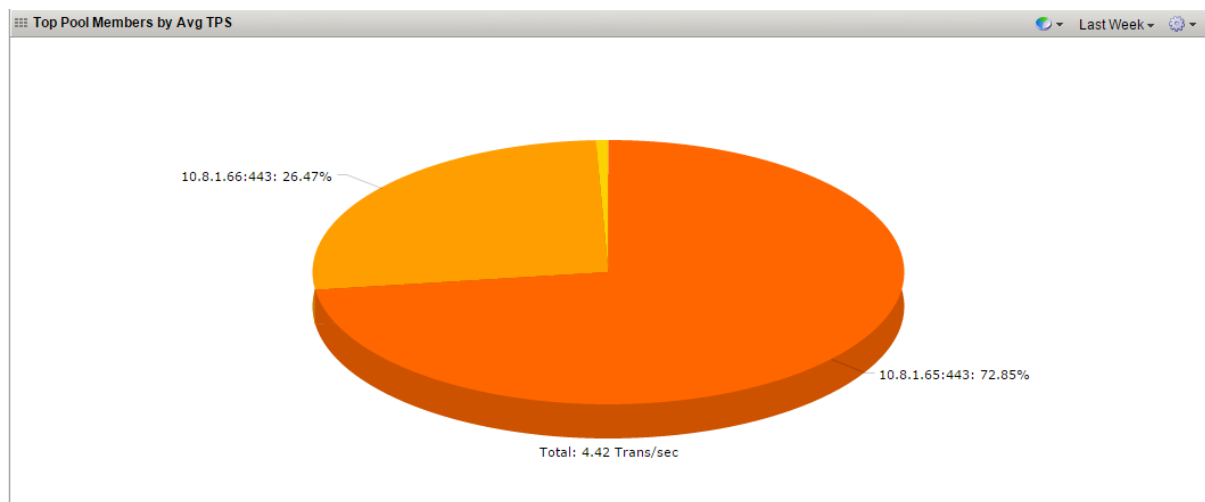


Ilustración 56. Distribución de peticiones hacia los miembros del pool

Country	Transactions
Ecuador	318646
United States	11445
United Kingdom	504
China	153
Brazil	91
Poland	75
Thailand	67
Uruguay	45
Netherlands	44
Mexico	38

Ilustración 57. Países desde donde se realizan las conexiones

Top Client IP Addresses (Day)	
54.69.110.59	13
54.200.213.161	11,187
173.198.240.115	30
179.49.1.67	2
181.39.218.50	61,347
181.39.224.29	13
181.39.250.124	18
181.112.69.83	9
181.112.70.96	2
181.112.94.253	22

Ilustración 58. Direcciones IP desde donde se conectan los clientes

En las ilustraciones anteriores, se observa a detalle, las conexiones hacia el virtual server de correo electrónico, las URIs accedidas por los clientes, los países y direcciones IP desde donde se accede a la aplicación, así como la distribución de peticiones a los miembros del pool de correo electrónico.

Además, podemos observar el comportamiento equitativo de balanceo y conexiones al correo electrónico diariamente por un período de varias semanas, en donde se evidencia el uso del servicio de manera más clara como se evidencia en las siguientes ilustraciones:



Ilustración 59. Estadísticas de conexiones y throughput

5. CONCLUSIONES Y RECOMENDACIONES

5.1.1 Conclusiones

Según el análisis de resultados después de la implementación de la solución de balanceo F5, se concluye que se han alcanzado los objetivos específicos y el objetivo general de este proyecto:

- Mediante la implementación del equipo de balanceo de carga del fabricante F5 Networks, la empresa Nube Digital ahora puede hacer uso de sus dos servidores virtuales de Microsoft Exchange, utilizando así toda su infraestructura para este propósito.
- Gracias a las bondades del balanceo de carga de F5, se puede mantener siempre una alta disponibilidad de la aplicación, mantener un registro del uso de cada servidor de Exchange, llegando incluso a identificar quien se conecta y desde que tipo de dispositivo o explorador web.
- En base al monitoreo de salud de equipos provisto por F5, se puede concluir que el tiempo fuera de servicio de la aplicación ha disminuido considerablemente, ya que en todo momento, siempre estará al menos un servidor de Exchange, respondiendo las peticiones de los clientes.
- Las conexiones entre el cliente y el servidor de Microsoft Exchange 2013, ahora son mucho más seguras, debido a la funcionalidad de full proxy de F5, lo que implica la encriptación entre el cliente y F5, y posteriormente entre F5 y los servidores, mediante certificados digitales SSL emitidos por la entidad certificadora Go Daddy Inc.
- Finalmente se concluye que la hipótesis de este proyecto es válida ya que según los resultados de las pruebas y la evidencia del servicio de correo electrónico, el clúster de equipos de balanceo F5 mejoró el servicio de correo electrónico de

forma inmediata y además permitirá un crecimiento del servicio de forma transparente y segura en un corto y mediano plazo en base a las necesidades del cliente.

5.1.2 Recomendaciones

Según el análisis de resultados, se recomienda lo siguiente:

- Realizar un seguimiento a la aplicación de correo electrónico y los elementos configurados en el equipo F5, para poder realizar las mejoras y afinaciones del caso, de manera oportuna.
- Realizar el mantenimiento preventivo de cada balanceador F5 bajo una programación adecuada y en ventanas fuera de horario laboral, para evitar problemas con la plataforma y evitar molestias a los clientes del servicio de correo electrónico.
- Adquirir un equipo F5 adicional de las mismas características del equipo actual desplegado en producción, que formará un par redundante en esquema activo pasivo, para minimizar al máximo el tiempo fuera de servicio durante mantenimientos preventivos o problemas con cualquiera de los equipos F5, y además, para mantener una alta disponibilidad en todo momento.
- Realizar respaldos de las configuraciones del equipo F5, cada vez antes y después de realizar cambios en las configuraciones de producción, para minimizar el tiempo de recuperación en caso de requerir un Rollback o un cambio de equipo F5.
- Mantener siempre actualizados los certificados digitales utilizados para encriptar la comunicación entre el cliente final y los servidores de Exchange.
- En base a las estadísticas presentadas por las herramientas visuales del equipo F5, es recomendable hacer un análisis al corto y mediano plazo, en cuanto al uso de

recursos y la disponibilidad del servicio, para considerar la inclusión de nuevos servidores de Microsoft Exchange a la granja del servicio.

6. REFERENCIAS BIBLIOGRÁFICAS

- 42U, (2012). *42U Rack Dimensions & Specifications*. Obtenido de <http://www.42u.com/42U-cabinets.htm>
- Beal, V. (2015). *IP address - Internet Protocol (IP) address*. Obtenido de http://www.webopedia.com/TERM/I/IP_address.html
- Beal, V. (2015). *router*. Obtenido de <http://www.webopedia.com/TERM/R/router.html>
- Computer Hope (2015). *Router*. Obtenido de <http://www.computerhope.com/jargon/r/router.htm>
- Definicion.de (2008-2015). *DEFINICIÓN DE PROTOCOLO DE COMUNICACIÓN*. Obtenido de <http://definicion.de/protocolo-de-comunicacion/>
- F5 Networks, Inc. (2013). *Configuration Guide for BIG-IP Local Traffic Management*. Obtenido de https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/lrm_configuration_guide_10_0_0.html
- F5 Networks, Inc. (2014). *TMOS Management Guide for BIG-IP Systems*. Obtenido de https://support.f5.com/kb/en-us/products/big-ip_ltm/manuals/product/tmos_management_guide_10_1.html
- F5 Networks, Inc. (2015). *Load Balancer*. Obtenido de <https://f5.com/glossary/load-balancer>
- Geraci, A. (2014). *GTM vs LTM – Difference between F5 Global & Local Traffic Manager*. Obtenido de <http://worldtecht.com/gtm-vs-ltm-difference-f5-global-local-traffic-manager/>
- Gilbert, B. (2014). *What Is a Proxy*. Obtenido de <https://www.whatismyip.com/what-is-a-proxy/>
- Griffin, D. (2005). *What Does BIG-IP Stand For?* Obtenido de <https://devcentral.f5.com/articles/what-does-big-ip-stand-for>
- Hewlett-Packard Development Company, L.P. (2015). *Blades de servidor HP ProLiant BL400c*. Obtenido de http://www8.hp.com/es/es/products/proliant-servers/product-detail.html?oid=5409981&jumpid=reg_r1002_eses_c-001_title_r0001#!tab=specs
- InetDaemon Enterprises. (2013). *Definition of a Route*. Obtenido de <http://www.inetdaemon.com/tutorials/internet/ip/routing/route.shtml>
- Informática Moderna (2008-2015). *EL SERVIDOR PARA REDES /SERVER*. Obtenido de <http://www.informaticamoderna.com/Servidor.htm>
- Janssen, C. (2010-2015). *Network Diagram*. Obtenido de <http://www.techopedia.com/definicion/25062/network-diagram>
- Kenneth E. Kendall, J. E. (2005). *Análisis y diseño de sistemas*. México: Pearson Educación.

- Kyrnin, M. (2015). *What is RAID?* Obtenido de <http://compreviews.about.com/od/storage/l/aaRAIDPage1.htm>
- MacVittie, L. (2011). *The Full-Proxy Data Center Architecture*. Obtenido de <https://devcentral.f5.com/articles/the-full-proxy-data-center-architecture>
- Nube Digital (2014). *Nube digital TU NUBE EN ECUADOR®*. Obtenido de <http://www.nubedigital.ec/index.html>
- OpenLazarus S.L. (2014). *Clúster de servidores, ¿qué es y cómo funciona?* Obtenido de <http://www.solingest.com/blog/cluster-de-servidores-que-es-y-como-funciona>
- Palo Alto Networks (2007-2015). *WHAT IS A DATA CENTER?* Obtenido de <https://www.paloaltonetworks.com/resources/learning-center/what-is-a-data-center.html>
- Pruitt, J. (2007). *iRules 101 - #01 - Introduction to iRules*. Obtenido de <https://devcentral.f5.com/articles/irules-101-01-introduction-to-irules>
- QuinStreet Inc. (2015). *computer rack*. Obtenido de http://www.webopedia.com/TERM/C/computer_rack.html
- Rouse, M. (2000-2015). *Host*. Obtenido de <http://searchnetworking.techtarget.com/definition/host>
- Rouse, M. (2000-2015). *load balancing. Essential Guide*. Obtenido de <http://searchnetworking.techtarget.com/definition/load-balancing>
- Rouse, M. (2010). *VIRTUALIZACIÓN, CAMINO PARA OPTIMIZAR RECURSOS*. Obtenido de <http://searchdatacenter.techtarget.com/es/definicion/Virtualizacion>
- Stroud, F. (2015). *data center*. Obtenido de <http://www.webopedia.com/TERM/D/data-center.html>
- Telconet. (2015). *Telconet la fibra del Ecuador*. Obtenido de <http://www.telconet.net/>
- VMware, Inc. (2015). *Virtualización*. Obtenido de <http://www.vmware.com/latam/virtualization>
- Winkelman, R. (1997-2013). *An Educator's Guide to School Networks*. Obtenido de <http://fcit.usf.edu/network/chap1/chap1.htm>
- www.ReclaiMe.com (2009-2015). *What is RAID?* Obtenido de <http://www.freeraidrecovery.com/library/what-is-raid.aspx>