Modelo administrativo para gestión de servidores Linux, implementando mecanismos de seguridad y tecnologías de software libre orientadas a la alta disponibilidad

Administrative model for managing Linux servers, implementing security mechanisms and open source technologies high availability oriented

MANUEL GUILLERMO FLÓREZ BECERRA
M.Sc en informática Universidad Industrial de Santander
Profesor Escuela de Ingeniería de Sistemas e Informática
Universidad Industrial de Santander
mgflorez@uis.edu.co
Bucaramanga, Colombia

ALEXANDER BARBOSA AYALA
Ingeniero de Sistemas.
Universidad Industrial de Santander
alexanderbarbosaayala@gmail.com
Bucaramanga, Colombia

ELKIN DARÍO MUÑOZ DUARTE
Ingeniero de Sistemas.
Universidad Industrial de Santander
elkin.dmd@gmail.com
Bucaramanga, Colombia

Fecha de recibido: 07/03/2012
Fecha de aceptado: 15/12/2012

RESUMEN

Este artículo describe el proceso de administración en servidores Linux, desde una perspectiva administrativa organizacional, usando procedimientos basados en tecnologías de software libre orientadas a la alta disponibilidad e implementación de mecanismos de seguridad para conservar la integridad de los recursos informáticos.

PALABRAS CLAVE: administración, alta disponibilidad, backup, clúster, corosync/OpenAIS, DRBD, pacemaker, CRM

ABSTRACT

This article describes the management process on Linux server, from an organizational management perspective, using procedures based on free software technologies aimed at high availability and implementation of security mechanisms to preserve the integrity of computer resources

KEYWORDS: administration, backup, clúster, corosync/OpenAIS, DRBD, high availability, pacemaker, CRM.

1. INTRODUCCIÓN

La administración de servidores es una labor que con el tiempo se hace cada vez más compleja, a medida que las organizaciones crecen también crecen sus componentes hardware y software. Es necesaria una visión a nivel organizacional para realizar una administración consolidada mediante la implementación de herramientas especializadas que tengan en cuenta la seguridad e integridad de la información, los mecanismos de control adecuados y la administración eficiente de recursos informáticos.

Los clústeres son una tecnología comúnmente aplicada para diferentes propósitos dependiendo de la actividad computacional a realizar; básicamente es un conjunto de computadoras que usan componentes de hardware comunes y presentan un comportamiento de unidad simulando un ambiente de una sola computadora.

En la EISI (Escuela de Ingeniería de Sistemas e Informática) de la UIS (Universidad Industrial de Santander) se dispone de servidores y servicios para un entorno educativo, de profesores, estudiantes y comunidad académica que requiere de estos en forma continua y permanente.

Al combinar la gestión administrativa con tecnologías orientadas a la alta disponibilidad y seguridad, es posible generar un ambiente confiable para satisfacer estos requerimientos de servicios académicos.

2. MARCO TEÓRICO

2.1 Clúster

La evolución del clúster, según sus usos, comprende desde la programación distribuida hasta la implementación de servicios en un entorno de alta disponibilidad [1].

Los servicios provistos de acuerdo a la orientación de la organización son:

- Alto rendimiento (High Performance Computing Clúster, HPCC), proveen un gran rendimiento a nivel de la velocidad en que se procesan los datos [2].

- Alta disponibilidad (High Availability, HA), establecer una infraestructura donde se mantengan los servicios de manera permanente independientemente de la caída de nodos [3].

- Balanceo de carga (Load Balancing), distribuir la carga de los diferentes elementos computacionales en una red de trabajo, mediante un balanceador de carga (Load Balancer) [4].

La composición de un clúster viene dada por los siguientes elementos:

- Nodos
- Sistema operativo instalado
- Protocolos de comunicación
- Servicios a disponer
- Dispositivos de almacenamiento
- Aplicaciones para el entorno del clúster
- Middleware, para establecer comunicación entre las diferentes aplicaciones que conforman el clúster.

2.2 Sistemas Operativo Debian

Es una distribución Linux, coherente a la filosofía del núcleo Linux y de GNU bajo licencia GPL (General Public Licence), la versión 6 fue lanzada el 6 de febrero de 2011 [5] y ha sido seleccionada como SO (Sistema Operativo) base para la implementación de la alta disponibilidad, no solo por ser uno de los sistemas operativos más utilizados en el mundo como servidor web [6], sino también por ser estable, versátil a nivel de mantenimiento e instalación de herramientas, bajo consumo de recursos, gran soporte y documentación.

2.3 Clúster de Alta Disponibilidad

Para mantener los servicios y la información crítica fuera de un punto único de fallo SPOF (Single Point Of Failure), es necesario la implementación de un clúster de alta disponibilidad; estos son agrupaciones de dos o más servidores que trabajan simultáneamente compartiendo información y servicios tales como el servidor web *Apache*, el gestor de base de datos *MySQL*, sistemas de ficheros, sitios web y otros, existiendo una comunicación permanente entre los servidores que permite reaccionar ante cualquier evento imprevisto [7] mediante una infraestructura de elementos redundantes, como volúmenes compartidos y configuración de interfaces de red extra.

2.4 DRBD (Distributed Replicated Block Device)

El DRBD es una herramienta bajo licencia GPL que permite la duplicación de un dispositivo a través de una red asignada para apoyo de clústeres de alta disponibilidad [8].

Cada uno de los componentes instanciados presenta un rol primario o secundario; el primario puede ser usado sin restricciones de lectura y escritura a diferencia del secundario, el cual para mantener la coherencia en el caché, no tiene acceso completo.

2.5 Corosync/OpenAIS

OpenAIS, es un software con licencia Open Source, que provee una interfaz de clúster a nivel de mensajería basándose en el estándar de alta disponibilidad AIS (Application interface Specification) [9]; AIS es un API (Application Programming Interface), para el sistema de comunicación en el clúster, mediante el uso de middleware y aplicaciones de servicio [10]. Corosync además de proveer un sistema de comunicación presenta características adicionales de sincronía virtual, reinicio de procesos, configuración y estadísticas en una base de datos y un sistema de agrupación de aplicaciones [11].

2.6 Pacemaker

Es un software bajo licencia GPL para la gestión de los servicios del clúster de alta disponibilidad, con el apoyo de la infraestructura de clúster que se asigne (Heartbeat o Corosync/OpenAIS), brindando una interfaz para la detección y recuperación de los nodos ante cualquier fallo a nivel de recursos [12].

2.7 Estado del Conocimiento

La implementación de sistemas de alta disponibilidad, surge principalmente con el propósito de mitigar el problema de la pérdida del servicio por eventos inesperados. Dependiendo del entorno para el cual se pretende implementar, han sido desarrolladas una amplia variedad de herramientas informáticas para la gestión de clústeres, tanto en versiones pagas como gratuitas.

Actualmente se implementan sistemas de alta disponibilidad a nivel empresarial donde el flujo de datos desde y hacia los servidores deben estar disponibles continuamente, siendo los sistemas en estado redundante y la infraestructura middleware dispuesta, los que hacen viable este tipo de servicios. Compañías como IBM® e Intel® se encuentran a la vanguardia en soluciones empresariales de Alta disponibilidad y sistemas de almacenamiento [13] [14], destacándose, el mantenimiento, concurrencia y monitoreo, de las funciones de alta disponibilidad para los servicios y el uso de tecnologías de almacenamiento personalizadas como RAID1 [15], en donde se dispone completamente el disco duro para el modo espejo.

Uno de los trabajos con mayor reconocimiento a nivel mundial, en el que se usó el conjunto de herramientas Pacemaker/Corosync, se encuentra en Deutsche Flugsicherung GmbH (DFS)[16], compañía del sector privado, encargada del tráfico aéreo en Alemania, donde se implementó el sistema de control del tráfico aéreo, construido bajo el sistema operativo SUSE® Linux Enterprise Server, trabajando como soporte a la infraestructura del sistema de procesamiento de datos de los radares[17]. Las especificaciones del hardware en el cual opera el sistema mencionado no han sido descritas por motivos de confidencialidad de la compañía propietaria del sistema.

3. ALTA DISPONIBILIDAD

3.1 Servicios disponibles

En la EISI mediante el clúster de alta disponibilidad y apoyados en las herramientas Apache [18], Mysql [19], Tomcat (módulo para paginas dinámica con contenidos Java)[20] , PHP (Hypertext Pre-processor) [21] y JAVA [22] se proveen diversos servicios como: Aulas virtuales de MeiWeb (Material Educativo Informático en la Web) y Moodle (Module Object-Oriented Dynamic Learning Environment o Entorno Modular de Aprendizaje Dinámico Orientado a Objetos), para docentes y alumnos, bases de datos, sitios web para estudiantes realizando proyecto de grado, además, se proyecta ofrecer a la comunidad académica servicios de computación en la nube mediante maquinas virtuales implementadas sobre el clúster.

3.2 Configuración

Un clúster de alta disponibilidad tiene diferentes modalidades de infraestructura: *N+1*, *N a N*, *split-site*; *Activo/Pasivo*; en esta última, uno de los nodos mantiene los servicios y los sistemas de archivos compartidos y el otro se mantiene las réplicas en espera ante un caso de fallo.

Para la creación del clúster se usaron dos servidores, previo a un estudio, se seleccionó el software *DRBD*, *Pacemaker* y *Corosync/OpenAIS* para conformar el stack de aplicaciones de alta disponibilidad. La Figura 1 muestra la infraestructura planteada y la manera como se encuentra configurado el clúster de alta disponibilidad para el entorno de trabajo.

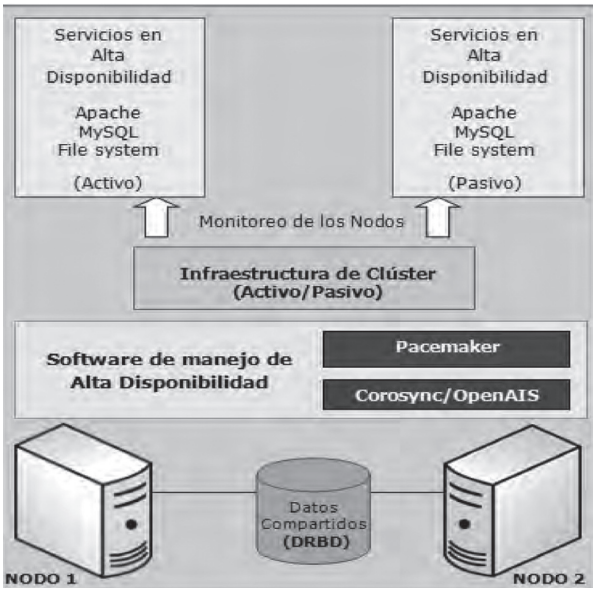

Figura 1. *Esquema del clúster de alta disponibilidad.*

Las anteriores herramientas, en conjunto, permiten el funcionamiento del clúster de alta disponibilidad; los siguientes parámetros deben considerarse para el montaje del clúster:

- Entre los nodos debe existir un enlace de red redundante debidamente configurado.
- El archivo */etc/network/interfaces* debe configurarse incluyendo una sub-interfaz de red con una dirección IP que pertenezca a la misma red del enlace redundante, donde se apoya el clúster para la comunicación entre nodos.
- El servicio de *corosync* debe estar configurado, para que se inicialice ante un reinicio del sistema.
- La llave de autenticación de corosync, generada en uno de los nodos, se envía por el protocolo de comunicación *SSH* hacia el otro nodo.
- El archivo de configuración de corosync, en ambos nodos, debe tener en la opción *bindnetaddr*, la dirección de red para los ajustes configurados en la interfaz redundante.
- Deshabilitar la propiedad *stonith*, dentro del clúster de alta disponibilidad, para no delimitar el uso de los servicios en los nodos a nivel de los nodos implementados [23].
- Crear el sistema de ficheros para el volumen que se dispondrá en modo espejo, teniendo en cuenta, que en el nodo esclavo debe existir otro volumen con la misma capacidad.
- Instanciar de manera correcta el recurso para *DRBD*, especificando para cada uno de los host el dispositivo, el disco, el socket y los metadatos.
- Uso del *CRM* (Cluster Resource Manager) para configuración de cada uno de los servicios a disponer en el clúster de alta disponibilidad, entre los que se resaltan, el sistema de archivos, la base de datos y el servidor web.

3.3 Pruebas de funcionamiento

Para evaluar la efectividad del clúster en producción se realizaron pruebas en maquinas reales y maquinas virtuales, estas últimas se lograron con el uso del software de virtualización *VirtualBox* [24], tanto las máquinas virtuales como las reales, fueron configuradas con características similares en cuanto al sistema operativo, software instalado, configuraciones de las herramientas para la entrega de servicios y esquema de particiones. Una vez establecido y configurado el canal de comunicación en los nodos que integran el clúster, estos se reconocen permanentemente por la red mediante un monitoreo automático constante.

Se estudiaron dos fenómenos que pueden ocurrir en el evento de un fallo, donde una de dichas anormalidades es consecuencia de la otra, siendo estas:

- El tiempo de promoción, para que el nodo secundario pase a primario ante una caída del nodo maestro.
- El tiempo de estabilización, para que el clúster vuelva a la normalidad en términos de disponer de manera correcta los roles activo y pasivo en los nodos.

La tabla 1 muestra cada una de las pruebas realizadas para ese tiempo de promoción y la tabla 2 evidencia cada ensayo para el tiempo de estabilización en los escenarios planteados; cada dato tiene implícito un error como consecuencia de los siguientes factores: a) la velocidad de respuesta del otro nodo a través del canal de comunicación, b) el instrumento de medición, c) la velocidad a la hora de finalizar o empezar la toma de las medidas.

Analizando los datos obtenidos en el escenario de las maquinas virtuales, se tiene una media de aproximadamente 16 segundos para la promoción y la estabilización, considerándose aceptable ya que es un tiempo relativamente pequeño; respecto a la desviación de 8 segundos para la promoción y 7 segundos para la estabilización también es aceptable, considerando el factor del error en la medida como fundamento para aprobarlos. A nivel de maquinas reales, se nota un cambio mínimo del tiempo de promoción con una

media de aproximadamente 13 segundos y un tiempo de estabilización de aproximadamente 15 segundos; esto se puede atribuirle al hecho de que el canal de comunicación entre ambos equipos es dedicado, la desviación de aproximadamente 6 segundos para la promoción y 5 segundos para la estabilización, también se encuentra dentro del rango de aceptabilidad; considerando estas medidas se puede inferir que el clúster de alta disponibilidad implementado cumple el requisito fundamental de brindar permanentemente los servicios hacia los usuarios.

Tabla 1. *Tiempo de promoción, paso de un nodo secundario a primario.*

Maquinas Virtuales		Maquinas Reales	
No. Toma	Tiempo de Estabilización (s)	No. Toma	Tiempo de Estabilización (s)
1	11,61	1	8,47
2	11,70	2	10,18
3	15,21	3	14,06
4	11,08	4	9,50
5	40,46	5	12,37
6	9,75	6	15,24
7	15,26	7	11,19
8	13,52	8	10,23
9	15,85	9	16,96
10	14,45	10	15,74
11	15,78	11	20,91
12	19,05	12	21,62
13	14,75	13	18,03
14	15,01	14	25,71
15	17,60	15	19,17
Media	16,07	Media	15,29
Desviación	6,95	Desviación	4,93

s = segundos.

Tabla 2. *Tiempo de estabilización, reincorporación de un nodo al clúster.*

Maquinas Virtuales		Maquinas Reales	
No. Toma	Tiempo de Promoción (s)	No. Toma	Tiempo de Promoción (s)
1	8,63	1	6,42
2	10,55	2	9,67
3	10,9	3	12,47
4	10,4	4	7,91
5	11,54	5	8,59
6	19,57	6	6,51
7	9,33	7	13,83
8	9,36	8	12,41
9	27,33	9	10,35
10	9,48	10	7,34
11	18,77	11	20,67
12	8,93	12	18,93
13	21,86	13	23,55
14	29,33	14	14,48
15	33,63	15	27,26
Media	15,97	Media	13,36
Desviación	8,22	Desviación	6,28

s = segundos.

4. MODELO ADMINISTRATIVO

Finalizada la etapa de configuración para la gestión de los servicios, se debe establecer una estructura fuerte al sistema consolidado a nivel de políticas administrativas y de seguridad [25][26].

4.1 Seguridad

Es Considerado como un proceso de vigilancia permanente, los aspectos que abarcan este componente del modelo administrativo son:

- Hardware: Con el fin de mitigar riesgos y amenazas ante ingresos no autorizados, es necesario el aseguramiento por contraseña del *BIOS* (Basic Input/Output System) y disponer de un espacio restringido a terceros, con llaves físicas para la apertura de gabinete y el frontal de los equipos, para que las modificaciones en el esquema base de operación sean realizados únicamente por el administrador.
- Sistema Operativo: Ningún equipo que se comunica en una red o que sea visible por internet es completamente seguro, es pertinente realizar actualizaciones del sistema, rectificando huecos de seguridad del software, pero verificando previamente que no se afecten las aplicaciones, herramientas y configuraciones previas.
- Software: Los errores más comunes en una herramienta son de *overflow* (desbordamiento) y *exploits* (explotación de una vulnerabilidad); es importante asegurar las aplicaciones a nivel de su configuración sin vulnerar la funcionalidad mediante un monitoreo permanentemente.
- Servidor web Apache: Configurar de manera adecuada cada uno de los módulos que compone la herramienta, define la seguridad funcional

de esta; deben establecerse el dominio web, los tiempos de respuesta, tiempos de sesión, puertos a disposición, la ruta del directorio raíz, los permisos de los directorios disponibles en el servidor web y mantener un control de privilegios. Para el cifrado de los datos, se usó la herramienta libre *OpenSSL*, que opera en la capa de transporte e incluye librerías de encriptación del protocolo *SSL* (Secure Socket Layer) y del protocolo *TLS* (Transport Layer Security) [27]; cuando se trata de una empresa, el certificado digital debe ser comprado a una entidad certificadora,

- Gestor de base de datos MySQL; Es altamente recomendable realizar la administración de las bases de datos mediante una interfaz de línea de comandos, evitando herramientas gráficas; a cada una de las bases de datos creadas se les debe asignar un usuario para asegurar la independencia en la gestión de las mismas.
- Lenguaje PHP: En el archivo de configuración tener en cuenta: tiempos de sesión para las solicitudes, tiempos de vida tras inactividad, tiempo de expiración de una solicitud, período de vida para la cookie de navegación, deshabilitar variables globales e inhabilitar ataques por inyección SQL.
- Alta disponibilidad: La configuración de modo *Activo/Pasivo*, es uno de los aspectos clave en cuanto a seguridad, ya que la información se encuentra disponible únicamente en el nodo primario, dejando al nodo secundario como respaldo ante una posible condición de error; además, el enlace de red redundante habilita un canal dedicado y aislado de la interfaz que se comunica por la internet.
- Accesos por red: El acceso remoto para realizar labores de configuración, mantenimiento y monitoreo requiere del aseguramiento de puertos, ya que es a través de estos donde se accede al sistema; contar con un Cortafuegos o Firewall es importante para definir aquellos puertos a los cuales se le limitará el acceso. Configurando las reglas en el Cortafuegos *Iptables*, incluido en el sistema operativo se puede gestionar el tráfico de red.

4.2 Usuarios y grupos

La gestión de usuarios se ha basado en roles acorde a la asignación de permisos; los roles identificados para esta gestión son:

- Administrador: Este usuario es independiente del root, posee permisos necesarios sobre los archivos y programas para realizar funciones críticas; debido al nivel de privilegios otorgados, no es conveniente que todos los programas sean ejecutados o asociados a este usuario.
- Usuario de acceso: Dispone de acceso remoto para escalar hacia cuentas de usuario sin acceso remoto pero con mayores privilegios. Su rango de operación se limita a su propio directorio.
- Usuario de servicios: Controla las funciones del servicio asignado, dando orden a las actividades administrativas.
- Usuarios jaula: Permite que los usuarios que requieran un servicio web, en desarrollo o en producción, tengan acceso a realizar modificaciones en su propio directorio raíz mediante el uso del protocolo *SFTP*.

4.3 Recursos

Además de disponer del clúster de alta disponibilidad, los recursos instalados en los equipos requieren ser gestionados de manera periódica, se deben considerar otros factores que pueden impedir la funcionalidad del sistema, incluyendo los errores humanos. Las acciones que permiten recuperar el sistema considerando este tipo de fallas son:

- Copias de seguridad del sistema: el sistema operativo es el software fundamental, es donde se tienen las configuraciones y las herramientas software para el funcionamiento y correcta prestación de los servicios; mantener un respaldo del SO y de las particiones permite que ante algún error ya sea humano o daño permanente en alguno de los recursos se pueda volver a un estado anterior. Los respaldos se deben realizar en diferentes momentos guardándolos en forma de bitácora en discos internos del sistema y discos externos
- Copias de seguridad de los servicios: Los servicios ofrecidos a los usuarios están sujetos a errores y fallos, que con frecuencia suceden por equivocación humana; es pertinente establecer un esquema de respaldos periódicos como manera de mitigar el problema. Se dispuso un modelo de backups basado en incrementales diarios, respaldos de aquellos archivos con modificaciones posteriores al del día anterior, y un backup completo por semana, copia de todos los archivos que se encuentran dentro del directorio a respaldar, ver Figura 2; estos backups se realizan a horas no laborales para conservar la integridad en la información; como plan de contingencia se mantiene una copia externa, fuera del lugar físico en el que se alojan los equipos. Los

backups completos se crean de manera lineal estilo de bitácora; los incrementales en forma circular sobre-escriben los de la semana anterior.

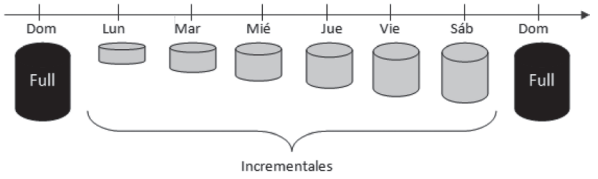

Figura. 2. *Esquema de respaldos periódicos.*

- Revisión de logs del sistema: El sistema operativo guarda registros de los servicios que se ejecutan, es importante que se realice un monitoreo de los eventos que ocurren, para la toma de decisiones y actuar de manera correcta y oportuna al momento de detectar un comportamiento no esperado. Con el apoyo del software *Logwatch*, cuya licencia es de libre distribución, se realiza un chequeo recopilando los eventos del sistema [28].

4.4 Automatización de tareas administrativas

Mediante el uso de scripts Shell y el servicio cron, Linux posibilita la automatización de tareas, desde generar respaldos hasta notificar la caída de un nodo; esta automatización se puede realizar para que las tareas se ejecuten a ciertas horas y fechas donde además de ganarse eficiencia para la gestión de actividades cotidianas se puede asegurar que la ejecución se realicen correctamente al no estar sujeta a fallos humanos.

4.5 Mantenimiento

Tanto el software como el hardware cambian de manera dinámica, por una parte el software se actualiza mediante parches o nuevas versiones, mientras que el hardware presenta deterioros por desgaste, provocado por el uso constante y paso del tiempo. Es importante estar preparado para cualquier fallo y mantener de manera periódica un apoyo técnico a nivel de esquemas de mantenimiento preventivo y correctivo.

4.6 Administración del clúster de alta disponibilidad

El clúster de alta disponibilidad necesita ser monitoreado constantemente para visualizar procedimientos o fallas que se pueden producir a la hora de gestionar o manejar servicios, para ello se dispone de la interfaz de línea de comandos CRM (Cluster Resource Manager), apropiada con instrucciones para mantener un completo control sobre el clúster. Paralelamente usando una tarea automatizada de notificaciones sobre la caída de algún nodo, es posible mantener el control sobre el clúster y asegurar que los servicios se mantendrán disponibles.

4.7 Gestión administrativa

El esquema de funcionamiento de los servidores, a nivel operativo, se basa en el modelo cliente-servidor; la información se encuentra centralizada en los servidores y los usuarios acceden a tales contenidos comunicándose por medio de una red [29], para que esta operatividad se efectúe en un contexto **organizacional**, se han seguido los siguientes principios administrativos [30]:

- Planeación: Realizar planteamientos referentes a expectativas de funciones organizacionales y acciones a futuro.
- Organización: Tomar los objetivos generados en el proceso de planeación y distribuir las actividades según se considere necesario para cumplir el propósito establecido.
- Ejecución: Puesta en marcha de las propuestas establecidas en la planeación y la organización.
- Control: Regular las actividades ejecutadas para que estas se encuentren dentro del marco operacional establecido en la organización.

Aplicando estas directivas, se puede generar un ciclo administrativo en el cual se propicie un entorno de trabajo de optimización continua, en el que las diferentes actividades organizacionales se realicen de manera eficaz y eficiente [31]. La Figura 3, representa el modelo planteado para los procesos internos de la organización.

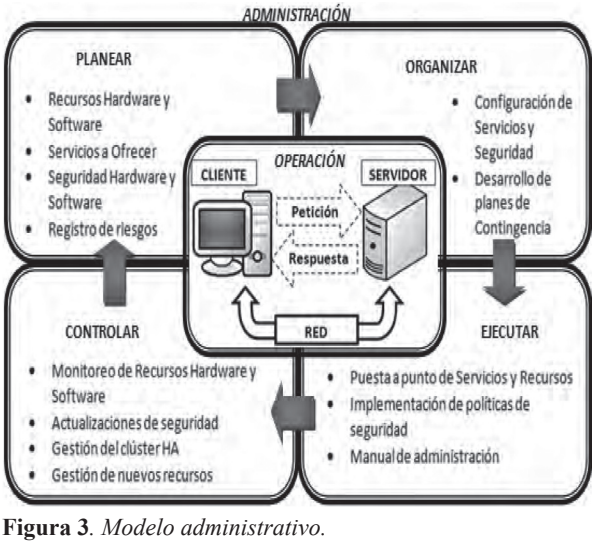

Figura 3. *Modelo administrativo.*

4.8 Validación

El proceso de validación del modelo se realizó simulando, durante un ´periodo de dos meses, el entorno de producción bajo una red local, realizando monitoreo sobre la infraestructura descrita, observando el funcionamiento del clúster antes de su paso al entorno de producción para asegurar la correcta prestación del servicio, desarrollando pruebas de vulnerabilidad de la seguridad, accesos no autorizados, administración del clúster, solicitudes de cliente en equipos ajenos a la red y tareas automatizadas.

Terminada la fase de validación por simulación y después de comprobar que la infraestructura construida cumplía con las funcionalidades establecidas, se realizó la configuración y montaje del clúster en el CENTIC (Centro de Tecnologías de Información y Comunicación de la UIS) con nuevos servicios computacionales en alta disponibilidad para la EISI; los servicios prestados a los usuarios se han mantenido consistentes y estables demostrando su correcto y permanente funcionamiento desde la fecha de implementación en Noviembre de 2011 hasta el presente confirmando los resultados de la validación anterior. La administración del clúster se mantiene gestionada de acuerdo al ciclo administrativo planteado, generando continuamente nuevas concepciones de arquitectura hardware y servicios a implementar.

5. NORMATIVIDAD

Establecer un conjunto de normas referentes a la actividad presente en los equipos que indique de manera pertinente los alcances y restricciones de uso y gestión, sirve para que los usuarios a nivel general tengan conciencia de los límites a los que está sujeta su actividad. Se ha realizado dicha normatividad, con el fin de propiciar un ambiente de trabajo organizado para dar un uso adecuado a los recursos y promover la responsabilidad.

5.1 Normas y políticas

Ser administrador del sistema, implica la realización de actividades que en algunos casos puede comprometer la operación del sistema; los lineamientos que debe seguir este usuario se estipulan en un contrato de confidencialidad en el cual se compromete a realizar su trabajo bajo las políticas de seguridad establecidas preservando la información sensible y dando soporte a usuarios que requieran uso de los servidores. El resto de usuarios que tienen acceso a los equipos, deben realizar sus labores de acuerdo a las normativas de uso asociadas a su rol dentro de los servidores mediante la aceptación y firma de un acuerdo de uso de los servicios.

6. CONCLUSIONES

El proceso administrativo de servidores que trabajan a través de una infraestructura de clúster de alta disponibilidad, es una tarea compleja que se puede realizar con el uso de diferentes aplicativos software, teniendo en cuenta la manera como se configuran y se gestionan en el sistema; mediante la implementación de políticas y mecanismos de seguridad se provee confiabilidad e integridad para mantener un ambiente administrativo organizado. Con la automatización de actividades básicas, se libera al administrador de ejecutar tareas repetitivas y le permite atender otros factores como el mejoramiento de la seguridad, políticas de administración, monitoreo de la eficiencia del clúster, escalabilidad de servidores y servicios que permitan el crecimiento de los recursos computacionales académicos.

Este modelo administrativo muestra un sistema confiable a nivel de prestación de servicios web, que ante fallas de algún nodo puede reaccionar de manera automática conservando la integridad de la información del usuario final.

En contraste con las diferentes soluciones existentes en el mercado, se demuestra que con el apoyo de tecnologías de software libre se puede lograr implementar una infraestructura con un sistema administrativo condicionado al entorno de producción, generando innovación a nivel de uso de estas tecnologías que aportan mejoras en la prestación de servicio dentro de la institución y mostrar a la sociedad, en especial a la Colombiana, que el uso de software libre se adapta fácilmente a un entorno de producción, además es apoyado por una gran comunidad que mantiene un soporte constante.

En general, un sistema está sujeto a fallos desde el momento en que se pone a disposición en un entorno de producción; con las herramientas y los procedimientos descritos, es posible solucionar este tipo de problemas. Mediante un proceso administrativo organizado se logra ofrecer un servicio óptimo acorde al ambiente que va dirigido tal como lo evidencia el clúster de alta disponibilidad, conformado por los servidores Sistemas y Delfín en la EISI de la UIS actualmente en producción y total funcionamiento.

7. AGRADECIMIENTOS

Agradecimientos a la Universidad Industrial de Santander y a la Escuela de Ingeniería de Sistemas e Informática por su apoyo permanente.

Agradecimientos a la fundación Raúl Ocazionez y al grupo MEIWEB, que han brindado su apoyado significativo en esta labor investigativa y práctica.

8. REFERENCIAS

[1] Sitio web de clusters. Disponible: http://www.clusters.nom.es/ [citado 7 de Enero de 2012]

[2] Sitio web de la comunidad Linalco. Disponible: http://www.linalco.com/hpcc-cluster-de-calculo-alto-rendimiento-linux.html [citado 7 de Enero de 2012]

[3] P. Clavijo. *Clusters de Alta Disponibilidad*. Disponible: http://www.lintips.com/?q=node/119 [citado 7 de Enero de 2012]

[4] Sitio web de la comunidad Linux virtual server. Disponible: http://kb.linuxvirtualserver.org/wiki/Load_balancing [citado 7 de Enero de 2012]

[5] Sitio web de la comunidad Debian. Disponible: http://www.debian.org/ [citado 7 de Enero de 2012]

[6] M. Gelbmann. *Debian is now the most popular Linux distribution on web servers*. Disponible: http://www.w3techs.com/blog/entry/debian_is_now_the_most_popular_linux_distribution_on_web_servers [citado 7 de Enero de 2012]

[7] J. Paredes. *Alta disponibilidad para Linux*. Disponible: http://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/paredes/pdf/LinuxHA.pdf [citado 8 de Enero de 2012]

[8] Sitio web del proyecto DRBD de la comunidad linbit. Disponible: http://www.drbd.org/ [citado 9 de Enero de 2012]

[9] Sitio web del proyecto Openais. Disponible: http://www.openais.org/ [citado 7 de Enero de 2012]

[10] Sitio web de la comunidad Service Availability. Disponible: http://www.saforum.org/Service-Availability-Forum:-Application-Interface-Specification~217404~16627.htm [citado 9 de Enero de 2012]

[11] Sitio web del proyecto Corosync. Disponible: http://www.corosync.org/ [citado 9 de Enero de 2012]

[12] Sitio web del proyecto Pacemaker. Disponible: http://www.clusterlabs.org/wiki/Pacemaker [citado 9 de Enero de 2012]

[13] Intel®. *High Availability Server Clustering Solutions*. Disponible: http://www.intel.com/design/network/papers/25157401.pdf [citado 24 de Noviembre de 2012]

[14] L. Spainhower. *High Availability for e-business*. Disponible:http://www.dependability.org/wg10.4/meeting38/08-Spain.pdf [citado 24 de Noviembre de 2012]

[15] Sitio web de Intel. Disponible: http://www.intel.com/support/sp/chipsets/imsm/sb/cs-009337.htm#raid1 [citado 24 de Noviembre de 2012]

[16] Sitio web de DFS. Disponible: http://www.dfs.de/dfs/internet_2008/portal/english/start/index.html [citado 20 de Diciembre de 2012].

[17] Sitio web de novell. Disponible: http://www.novell.com/success/dfs.html. [citado 20 de Diciembre de 2012]

[18] Sitio web del proyecto Apache. Disponible: http://www.apache.org/ [citado 20 de Febrero de 2012]

[19] Sitio web del proyecto MySQL. Disponible: http://www.mysql.com/ [citado 20 de Febrero de 2012]

[20] Sitio web del proyecto Tomcat. Disponible: http://tomcat.apache.org/ [citado 20 de Febrero de 2012]

[21] Sitio web del proyecto PHP. Disponible: http://www.php.net/ [citado 20 de Febrero de 2012]

[22] Sitio web del proyecto JAVA. Disponible: http://www.java.com/ [citado 20 de Febrero de 2012]

[23] D. Muhamedagic. *Fencing and Stonith*. Disponible: http://www.clusterlabs.org/doc/crm_fencing.html [citado 9 de Enero de 2012]

[24] Sitio web del proyecto VirtualBox. Disponible: https://www.virtualbox.org/ [citado 20 de Febrero de 2012]

[25] A. Barisani, T. Bader, S. Biles, C. Clark, R. Chiesa, P. Endres, R. Feist, A. Ghirardini, J. Ho, M. Ivaldi, D. Lavigne, S. Presti, C. Low, T. Miller, A. puccetti. *Hacking Exposed Linux: Linux Security Secrects & Solutions*. 3rd ed. ISECOM, McGraw-Hill, 2008

[26] E. Nemeth, G. Snyder, T. R. Hein, B. Whaley. *Unix and Linux Systems Administration Handbook*. 4th ed. Pearson Education, Inc., 2011.

[27]Sitio web del proyecto OpenSSL. Disponible: http://www.openssl.org/ [citado 10 de Enero de 2012]

[28]Sitio web del proyecto Logwatch. Disponible: http://sourceforge.net/projects/logwatch/ [citado 10 de Enero de 2012]

[29] A. S. Tanenbaum. *Redes de Computadoras*. 4th ed.

Pearson Education de México, 2003.

[30] I. Chiavenato. *Teoría general de administración*. Elsevier, Río de Janeiro, 2001.

[31] E. M. Fernández. *Introducción a la gestión (Management)*. Ed. Universidad Politécnica de Valencia, 1991.