ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA EN SISTEMAS

"ANÁLISIS Y DISEÑO DE UNA RED DE ALTA DISPONIBILIDAD PARA CENTRALES ASTERISK BASADA EN LA TECNOLOGÍA DUNDi"

TESIS DE GRADO

Previa obtención del Título de

INGENIERO EN SISTEMAS INFORMÁTICOS

Presentado por:

GLADYS NATALI TOSCANO PALOMO

RIOBAMBA – ECUADOR

2012

AGRADECIMIENTO

Agradezco a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante toda la mi vida estudiantil.

Hoy y siempre agradezco a mi familia y en especial a mi madre que si no fuese por el su esfuerzo valentía y amor mis estudios no hubiesen sido posible.

DEDICATORIA

Dedico mi tesis con todo mi amor y cariño a mi padre y hermanos Marcelo Verónica Patricio Paola y Marisol por su ejemplo, ayuda incondicional y apoyo.

A todos mis amigos por estar junto a mi todo este tiempo donde he vivido momentos felices y tristes, siempre los llevare en mi corazón.

NOMBRE	FIRMA	FECHA
Ing. Iván Menes **DECANO FACULTAD DE INFORMÁTICA Y ELECTRÓNICA**	.....	.....
Ing. Raúl Rosero **DIRECTOR ESCUELA INGENIERÍA EN SISTEMAS**	.....	.....
Ing. Alberto Arellano **DIRECTOR DE TESIS**	.....	.....
Ing. Diego Ávila **MIEMBRO DEL TRIBUNAL**	.....	.....
LCDO. Carlos Rodríguez **DIRECTOR DPTO DOCUMENTACIÓN**	.....	.....
NOTA DE LA TESIS	.....	

"Yo Gladys Natalí Toscano Palomo, soy el responsable de las ideas, doctrinas y resultados expuestos en esta Tesis, y el patrimonio intelectual de la misma pertenecen a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

_____

Gladys Natalí Toscano Palomo

INDICE DE ABREVIATURAS

Abreviatura	Descripción
DNS	Sistema de Nombre de Dominio
	Domain Name System
IAX	Protocolo de intercambio de Asterisk
	Inter Asterisk Exchange
IAX(2)	Protocolo de intercambio Asterisk (versión 2)
LAN	Red de Área Local
	Local Area Network
NAT	Traductor de direcciones IP
	Network Address Translator
PBX(PABX)	Centrale Telefonica (Automática) Privada
	Private (Automatic) Branch Exchange
PSTN/RTB	Red de Telefonía Básica (Conmutada)
	Public Switched Telephone Network
QoS	Calidad de Servicio
RFC	Documento de Trabajo de Estandarización (Internet)
	Request For Comment
RTP	Protocolo de Tiempo Real
	Realtime Transport Protocol
SIP	Protocolo de Señalización de Sesión(es)
	Session Initiation Protocol
UDP	User Data Protocol
VoIP	Voz sobre IP

INDICE GENERAL

CONTENIDO

INDICE FIGURAS

INDICE TABLAS

CAPÍTULO I

I. MARCO REFERENCIAL

1.1 ANTECEDENTES

Actualmente, para el funcionamiento de los servicios de voz se utilizan las redes por conmutación de circuitos que son redes públicas tales como las redes RTC (Red Telefónica Pública Conmutada también llamada Red Telefónica Básica o RTB) conocida también como PSTN o RTPC que es una red analógica y ISDN o RDSI (Red Digital de Servicios Integrados), pueden servir también para el envió de datos, por medio de un módem o ADSL (Línea de Abonado Digital Asimétrica).En las empresas se puede decir que utilizan dos redes muy bien diferenciadas, una encargada del tráfico y servicios de voz y otra destinada para el tráfico de datos que se basa en la conmutación de paquetes. Con el avance de las tecnologías actuales para VoIP se tiene la capacidad de proporcionar unos servicios garantizados sobre una única red donde confluyen tráficos tanto de voz como de datos, lo

que nos lleva a afirmar que se dispone de una red multiservicio que principalmente reduce costes y ancho de banda.

Hoy en día, la mayoría de las empresas tienen su propia red telefónica convencional, diseñada sobre PBX, que soportan todos los servicios telefónicos tradicionales, estos se conectan a la RTC o RDSI para llamadas externas a teléfonos fijos o móviles y si la empresa tiene un gran volumen de llamadas y varias oficinas, éstas pueden conectarse por líneas dedicadas de alta capacidad, que le reducirán el coste considerablemente.

Otra de las características de los sistemas de comunicación en la empresa es tener su propia red de datos de área local (LAN), donde se conectan sus diversos equipos de datos. Estas redes de datos se han ido ampliando, pudiendo conectar equipos en oficinas remotas mediante la interconexión de diversas LAN, por medio de líneas dedicadas.

Este tipo de redes se conocen como VPN (Virtual Private Network). El hecho de tener dos redes independientes para comunicaciones telefónicas y de datos es algo caro e innecesario, por lo que la telefonía IP proporciona una nueva vía en el campo de las comunicaciones de la empresa.

Hoy en día se habla mucho de dos conceptos, telefonía IP y VoIP, y se tiende a utilizar ambos términos para lo mismo, cuando existe una diferencia entre ellos.

La telefonía IP se refiere a la utilización de una red IP (privada o pública, como es Internet) por la que transmitimos los servicios de voz, fax y mensajería. Esta red IP puede ser utilizada para realizar las llamadas internas de la propia empresa, así como las llamadas externas, usando, por ejemplo, Internet en lugar de la red telefónica pública conmutada.

La VoIP es la tecnología usada para el funcionamiento de la telefonía IP. VoIP gestiona el envío de información de voz utilizando IP (Internet Protocol). La información analógica vocal se transforma en paquetes digitales diferenciados que se envían por la red. Los paquetes de información de voz viajan por la red IP, del mismo modo que los datos generados por una comunicación de correo electrónico, por ejemplo. Por tanto, la telefonía IP es una aplicación inmediata de esta tecnología.

Asterisk se ha convertido en referente mundial a lo que PBX IP se refiere, muchos han sido los que han solicitado la necesidad de crear un posible clúster para Asterisk. Que permita dar soporte a los usuarios aun cuando una de las centrales pertenecientes a los nodos del clúster esté fuera de servicio.

Hasta hoy ésta ha sido una de las prioridades de Digium creador de Asterisk, por el momento se ha desarrollado un modulo llamado res_ais que permite controlar el estado de una extensión situada en otro Asterisk. Lo que restaría es propagar esta información a través del Asterisk conectados entre sí por DUNDi

Dentro del análisis de las tecnologías a utilizar se encuentra enmarcado DUNDi que permite comunicar 2 o más PBX basadas en Asterisk y así establecer la comunicación entre dos terminales VoIP unificando el plan de marcado de cada servidor PBX independiente.

La implementación de la red de alta disponibilidad se la realizara en los Laboratorios de CISCO a través de un ambiente de prueba, ya que cuenta con los equipos necesarios además de que se tiene acceso a otros recursos como por ejemplo el Internet.

Este tema de tesis se enmarca en el análisis y diseño de un clúster de Centrales Asterisk basado en DUNDi lo cual permitirá implementar una red de alta disponibilidad.

Para la parte aplicativa nos limitaremos en los siguientes módulos: La red de alta disponibilidad permitirá:

- Unificación del plan de marcado (Dial Plan)
- Garantizar la alta disponibilidad

1.2 JUSTIFICACIÓN

La VoIP es un servicio de misión crítica cuyo mayor riesgo es su interrupción. Los usuarios de telefonía IP deben gozar, por tanto, de los altísimos niveles de disponibilidad a los que están acostumbrados a recibir de la red telefónica convencional.

Por lo tanto una de las necesidades a resolver es la construcción de un sistema estable y robusto de centrales Asterisk que nos permita obtener una red de alta disponibilidad, que proporcionaría y garantizaría el servicio en un mayor porcentaje. Para lo cual se propone construir un clúster de Asterisk que permita que todo funcione correctamente aun en el caso de que uno de los nodos dejase de funcionar.

En este sentido es conseguir propagar la información de los usuarios (libres, ocupados, hablando, no disponible, etc.) entre los distintos servidores que forman el clúster. Para el funcionamiento de la red de Alta disponibilidad se proponen los siguientes módulos.

Un servidor DNS que será el encargado de proporcionar direcciones IP de las centrales a cada uno de los usuarios que ingresen a registrarse, además facilitará el balanceo de carga.

Las PBX Asterisk o el núcleo de la red, que son las centrales telefónicas y se encargarán de gestionar las llamadas en curso.

La Base de Datos en MySQL esta contendrá la información del Dial Plan o Plan de marcado, información acerca de las terminales y de los registros de llamadas.

DUNDi (Distributed Universal Number Discovery) que interviene al momento de que una extensión no se encuentre gestionada en nuestra central. Este ayudará a buscarle en distintos nodos del clúster.

1.3 OBJETIVOS

1.3.1 Objetivo General

- Analizar y diseñar una red de alta disponibilidad para centrales Asterisk basada en la tecnología DUNDi que permita el acceso de los usuarios en un mayor porcentaje.

1.3.2 Objetivos Específicos

- Estudiar las técnicas de alta disponibilidad en redes VoIP para seleccionar de acuerdo a sus ventajas y limitaciones la ideal y más adecuada para este sistema.

- Analizar la tecnología DUNDi y configurarla en cada central telefónica para establecer la comunicación punto a punto entre los nodos que forman parte de la estructura del clúster VoIP.
- Analizar la arquitectura de Asterisk para reconocer los componentes que intervienen en un sistema de Telefonía IP y la posibilidad de integrar hardware de distintas marcas y precios.
- Diseñar e implementar un Ambiente de Prueba para determinar la disponibilidad que existe en un Clúster VoIP y así comprobar el incremento porcentual de la misma.

1.4 HIPÓTESIS

La implementación de una red de alta disponibilidad para centrales Asterisk basada en la tecnología DUNDi permitirá dotar de alta disponibilidad al sistema de Telefonía IP.

Variables e Indicadores

- **Independiente**
  - **Variable:** Implementación de una red.
- **Dependiente**
  - **Variable:** Alta Disponibilidad.
  - **Indicadores:**

Tiempo de demora de la toma del control del servicio por otros Servidores del Clúster.

Tiempo de pérdida del servicio al ocurrir fallas en los Servidores.

Tiempo de demora de registro de las terminales.

CAPITULO II

II. MARCO TEORICO

CONCEPTOS IMPORTANTES PREVIOS

2.1 VOZ SOBRE IP (VoIP)

El VoIP (Protocolo de Voz Sobre Internet) o VoIP (Voice Over Internet Protocol) es una tecnología que reúne un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Internet Protocol), esto quiere decir que permite transmitir la voz en forma digital sobre redes IP, en lugar de una línea telefónica regular (o analógica), es decir convierte las señales de voz estándar en paquetes de datos comprimidos que son transportados a través de redes de datos en lugar de líneas telefónicas tradicionales.

Según Wikipedia [1]: Voz sobre Protocolo de Internet, también llamado Voz IP, VozIP, VoIP (por sus siglas en inglés), es un grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP (Protocolo de Internet).

Según Monografias [2]: La Voz sobre IP (VoIP, Voice over IP) es una tecnología que permite la transmisión de la voz a través de redes IP en forma de paquetes de datos.

Los servicios de VoIP convierten su voz en una señal digital que viaja a través de Internet. Si está llamando a un número de teléfono regular, la señal es convertida a una señal de teléfono regular antes de llegar al destino. VoIP puede permitirle hacer una llamada directamente desde una computaadora, un teléfono especial de VoIP, o un teléfono tradicional conectado a un adaptador especial.

Además, de forma inalámbrica mediante un "hotspot" en lugares tales como aeropuertos, parques y cafés le permite conectarse a Internet y puede permitir usar el servicio VoIP de forma inalámbrica.

2.2 TELEFONÍA IP

La telefonía IP es una aplicación de la tecnología de Voz sobre IP, reúne la transmisión de voz y de datos, lo que facilita la utilización de las redes informáticas para efectuar llamadas telefónicas. Además, dicha aplicación al formar una única red que es la encargada de transmitir todo tipo de

[1] *http://es.wikipedia.org/wiki/Voz_sobre_IP*
[2] *http://www.monografias.com/trabajos26/voz-sobre-ip/voz-sobre-ip.shtml*

comunicación, como es voz, datos o video, ha tomado el nombre de red convergente o red multiservicios.

Según Monografias [3]: La telefonía sobre IP que es una aplicación inmediata de la tecnología VoIP de forma que permita la realización de llamadas telefónicas ordinarias sobre redes IP u otras redes de paquetes utilizando un PC, gateways y teléfonos estándares. En general, servicios de comunicación - voz, fax, aplicaciones de mensajes de voz - que son transportada vía redes IP, Internet normalmente, en lugar de ser transportados vía la red telefónica convencional.

Abre un espacio muy importante dentro del universo que es Internet. Establece la posibilidad de estar comunicados a costos más bajos dentro de las empresas y fuera de ellas, es la puerta de entrada de nuevos servicios apenas imaginados y es la forma de combinar una página de presentación de Web con la atención en vivo y en directo desde un call center, entre muchas otras prestaciones.

2.2.1 Características

La telefonía IP surge como una alternativa económica a la telefonía tradicional, brindando nuevos servicios y una serie de beneficios económicos y tecnológicos con características especiales como:

- En comparación con la red analógica es realmente económica, solo es necesario contar con un micrófono y unos auriculares o parlantes.

[3] *http://www.monografias.com/trabajos26/voz-sobre-ip/voz-sobre-ip.shtml*

- No depende del tipo de red física que lo soporta. Permite la integración con las grandes redes de IP actuales además de poder integrarse con la red pública o PSTN.
- No depende del hardware utilizado.
- Admite ser implementado tanto en software como en hardware, con la particularidad de que el hardware supondría eliminar el impacto inicial para el usuario común.
- Permite la integración de Vídeo y TPV
- Se necesita una red activa para su funcionamiento.

2.3 PROTOCOLOS

2.3.1 Protocolos de Transporte

2.3.1.1 RTP (Real-Time Transport Protocol)

Es un protocolo desarrollado por la IETF [4] que permite transmitir información de audio y video a través de internet en tiempo real.

Este protocolo funciona sobre el protocolo de transporte UDP [5] , es decir se encapsula dentro de datagramas UDP. Al trabajar bajo UDP no garantiza la entrega de todos los paquetes al igual que su llegada al destino en el instante adecuado. La capa de aplicación se encarga de superar estos fallos en la transmisión de información. RTP no trabaja con un puerto predefinido por lo general escoge un número par elegido al azar.

---

4 (Internet Engenieering Tast Force) Es una organización abierta de normalización que contribuye a la ingeniería de Internet.

5 (User Datagrama Protocolo) Es el protocolo de nivel de transporte basado en el intercambio de datagramas. No le importa si los datos llegan con errores o no. Permite el envió de datagramas a través de la red sin establecer previamente una conexión.

2.3.1.2 RTCP (RTP Control Protocol)

Este protocolo se usa para enviar datos de control y de mediciones realizadas durante la transmisión. Para lo cual la transmisión se encapsulan dentro de mensajes RTP. La frecuencia de envío es aproximadamente cada cinco segundos. El puerto con el cual trabaja RTCP al igual que RTP no es definido, por ello escoge un número de puerto impar consecutivo en relación al seleccionado por RTP. RTCP no da ninguna clase de cifrado de flujo o de autenticación.

2.3.2 Protocolos de Señalización

2.3.2.1 SIP (Protocolo de Inicio de Sesión)

Es un Protocolo de Inicio de Sesiones creado por el IETF (Internet Engineering Task Force). Este protocolo de señalización para voz sobre IP es utilizado para iniciar, modificar y terminar Sesiones Interactivas de Comunicación Multimedia entre usuarios tales como: video, voz, mensajería instantánea y realidad virtual.

La sintaxis de las operaciones que realiza SIP son equivalentes a las realizadas por los protocolos de servicio de páginas web (HTTP) y distribución de e-mails (SMTP).

SIP para su funcionamiento trabaja en conjunto con los protocolos SDP y RTP. SDP (Session Description Protocol) se encarga de describir los parámetros de inicialización de los flujos multimedia en una sesión, es decir su función es invitar, anunciar y negociar las capacidades de una sesión multimedia en internet. RTP (Real-Time Transport Protocol) cumple con la función de transportar en tiempo real el contenido de voz y video entre los usuarios una vez establecida la sesión.

Agentes de Usuario

Los Agentes de usuario son los puntos extremos de la Sesión, estos se pueden comportar de dos modos:

Un User Agent Client (UAC) es el encargado de realizar las peticiones de servicio, mientras que el User Agent Server (UAS) es el encargado de procesar la petición recibida.

2.3.2.2 IAX(Inter-Asterisk eXchange Protocol)

Es un protocolo creado para la señalización de VoIP en Asterisk. Este protocolo es abierto para su libre desarrollo. Para control y tráfico de datos usa el puerto UDP 4569. IAX se basa en muchos estándares de transmisión de datos como SIP y RTP.

2.3.3 Protocolos de Enrutamiento Dinámico

2.3.3.1 OSPF (Open Shortest Path First)

Es un protocolo de enrutamiento jerárquico de pasarela interior, o IGP (Interior Gateway Protocol)pararedes TCP/IP, basadas en el RFC 2328.OSPF es un estándar abierto, razón por la cual está disponible en múltiples sistemas operativos como: Windows 2003 Server, Linux, Cisco IOS, etc.

2.3.3.2 RIP (Routing Information Protocol)

El protocolo RIP es un protocolo de encaminamiento dinámico de tipo IGP (Internal Gateway Protocol), utilizado por routers y equipos, para intercambiar información acerca de redes IP.

2.4 CLÚSTER

Es necesario explicar que es un clúster; un clúster consiste en un grupo de nodos (computadoras) conectados entre sí que interactúan como una sola maquina así en el caso de que uno de los nodos dejase de funcionar tomaría el control el segundo nodo, y así sucesivamente dependiendo del número de computadoras que conformen el clúster, reduciendo así considerablemente la tolerancia a fallos y caídas de servicio.

Según Ismael Olea [6]: Un clúster es un grupo de equipos independientes que ejecutan una serie de aplicaciones de forma conjunta y aparecen ante clientes y aplicaciones como un solo sistema. Los clústeres permiten aumentar la escalabilidad, disponibilidad y fiabilidad de múltiples niveles de red.
Según Eugenio Villar y Julio Gómez [7]: Un clúster es una agrupación de dos o más computadores que se encuentran interconectados y que normalmente trabajan de forma conjunta con algún propósito determinado.
Desde fuera, en la mayoría de los casos, el clúster es visto como un único equipo que ofrece unos determinados servicios.

---

[6] *Extraído de la siguiente URL, http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-cluster-computadoras/doc-cluster-computadoras-html/node8.html*
[7] *Extraído de la siguiente URL, http://www.adminso.es*

Es usual que los componentes que integran el clúster, llamados nodos, se encuentren interconectados mediante conexiones LAN (Local Area Network) de alta velocidad. El objetivo por el cual se sugiere implantar es ampliar la funcionalidad de un servidor o bien mejorar su rendimiento y/o disponibilidad. En función de las características que presente el clúster y sus objetivos, se puede mencionar los siguientes:

- **Clústeres de alta disponibilidad.** El rasgo particular de este tipo de clústeres es la compartición de un determinado servicio entre los diferentes nodos que lo componen (o un grupo de ellos), los cuales se monitorizan constantemente entre sí, de forma que se garantiza el funcionamiento ininterrumpido del servicio. Tanto si se produce un fallo hardware como si ocurre alguno en las aplicaciones o servicios que corren en el nodo que las ejecuta del clúster, las aplicaciones o servicios son migrados por el software de alta disponibilidad de forma automática a cualquiera de los nodos restantes del clúster. Una vez que el problema es subsanado, los servicios migrados pueden retornar a su ubicación original en el nodo primario (llamado así porque es el que originalmente los ejecuta). Existen diferentes configuraciones, como Activo/Pasivo (donde sólo un nodo ejecuta servicios) o Activo/Activo (todos los nodos ejecutan servicios, normalmente diferentes). La alta disponibilidad puede ser garantizada a nivel de servicio y también a nivel de datos, existiendo para cada uno numerosas herramientas en GNU/Linux tanto software como hardware.

- **Clústeres de alto rendimiento.** El propósito de este tipo es proporcionar altas prestaciones de capacidad de cómputo superior a las que pudiera ofrecer un único servidor. El ejemplo más conocido son los llamados clústeres Beowulf, en los que los nodos se encuentran localizados conjuntamente, son homogéneos y comparten una red dedicada. Normalmente

son formados cuando el tamaño del problema a resolver es inmanejable por un único servidor o cuando la máquina que podría hacerlo tiene un coste muy alto. El alto rendimiento puede ser aplicado en distintos niveles también, siendo especialmente interesante en nuestro caso enfocado a servicios –en especial en aquellos que han de soportar una mayor congestión o tráfico-. Como ejemplos de software para la implementación de clústeres de alto rendimiento podemos citar OSCAR (Open Source Cluster Application Resources), distribuido bajo la licencia GPL, o Windows HPC Server 2008 para sistemas operativos Microsoft Windows. Algunas herramientas GNU/Linux enfocadas al alto rendimiento concretamente en servicios son KeepAlived, UltraMonkey, o LifeKeeper.

- **Clústeres de balanceo de carga.** Desde el punto de vista que se mire el balanceo de carga también podría ser interpretado como una solución de alto rendimiento. Algunos de los nodos del clúster actúan como frontend del mismo y se encargan de repartir las peticiones que reciben para un servicio determinado entre otro grupo de nodos que conforman el backend del clúster. Existen soluciones también enfocadas para servicios específicos, como por ejemplo Web, FTP, DNS entre otros es decir, servicios que esperan recibir proporciones de tráfico elevadas. Por ejemplo, para telefonía IP existen varias herramientas cuya funcionalidad es la de implementar un proxy SIP (protocolo de sesión más usado en la actualidad) de alto rendimiento y muy configurable; KAMAILIO y OpenSIPS son dos de las más importantes, derivadas de la desaparecida OpenSER.

Escalabilidad y robustez son dos características que siempre deben estar presentes en un clúster. Escalabilidad tanto administrativa como en carga soportada, y robustez garantizando siempre la disponibilidad de nodos que estén activos en el clúster.

Para el presente trabajo de tesis un clúster de alta disponibilidad nos sirve perfectamente en el caso de un problema de Hardware o como en las aplicaciones o servicios que corren en el nodo que las ejecuta del clúster, nuestros clientes tendrían igualmente servicio ya que cualquiera de los nodos restantes tomaría el control como maquina primaria.

2.5 ASTERISK

Básicamente Asterisk es una plataforma software de Dominio Público (Open Software) para el desarrollo de centrales telefónicas (PBXs) y es considerado por algunos como el sistema de telefonía más flexible y extensible de los que actualmente existen en el mercado. Proporciona todas las funcionalidades de los grandes sistemas propietarios y ofrece algunas posibilidades y servicios todavía no disponibles en ellos. Además, es el más competitivo en precio.
Está sujeto a la licencia de distribución de software GPL y utiliza para su funcionamiento el sistema operativo Linux, también de libre distribución.

Fue creado por Mark Spencer como respuesta a la estrategia de la mayoría de los fabricantes de telefonía de mantener sus sistemas completamente cerrados para cautivar a sus clientes y evitar la libre competencia. Actualmente es uno de los proyectos de Dominio Público de más difusión y con una de las comunidades de usuarios y desarrolladores más activa. Además, Digium, la empresa fundada por Mark Spencer, se encuentra detrás de este proyecto soportándolo comercialmente.

2.5.1 Características

Es económico ya que utiliza la misma infraestructura de red de datos para realizar llamadas sin hacer uso de la red convencional además puede utilizar softphone que simulan a los teléfonos físicos.

Es Interoperable es decir Asterisk puede integrarse con sistemas híbridos en los que se mezclen medios tradicionales de comunicación telefónica con nuevos servicios basados en redes IP. Por lo cual se pueden aprovechar las infraestructuras ya existentes, como terminales telefónicos o líneas de comunicaciones, e integrarlas con nuevos servicios.

Tiene la capacidad de interoperar protocolos SIP, IAX, H.323, MGCP y SCCP/Skinny, así como soportar los estándares de telefonía tanto europeos como americanos.

Es flexible y tiene la capacidad de crecimiento Asterisk está formado en módulos y estructurado en capas, ofrece cuatro tipos distintos de vías o interfaces para que otras aplicaciones puedan acceder a toda la funcionalidad que ofrece. Se trata realmente de un middleware de telefonía y comunicaciones.

Tiene una gran funcionalidad ofrece un conjunto de servicios muy extenso. Por medio de una adecuada configuración se pueden establecer enrutamientos de llamadas complejos y definir estrategias de asignación de llamadas a los agentes lo que lo hace muy útil para el diseño de call centers para telemarketing o soporte de usuarios.

2.5.2 Servicios que permite implementar Asterisk

- Contestación Automática de llamadas
- Transferencia de llamadas, internas y externas.
- Desvío de llamadas si está ocupado o no contesta.
- Opción No molestar (Do Not Disturb).
- Parqueo de llamadas (Call Parking).
- Contestación de una llamada a una extensión remota.
- Llamada en espera (Hold).
- Grupos de llamada (Ring groups).
- Identificador de llamante (CallerID).
- Sistema DISA12. (método por el cual una persona externa a la oficina puede realizar llamadas a través de la centrale).
- Operadora Digital (menús interactivos y guiados).
- Música en espera y en transferencia (ficheros MP3 actualizables por el usuario).
- Captura de llamadas de forma remota (remote pickup).
- Buzones de voz (general, individuales, por grupos) protegidos por contraseña.
- Gestión de listas negras (números telefónicos con acceso prohibido).
- Salas de conferencia (2 o más terminales simultáneamente).
- Registro y listados de llamadas entrantes y salientes, con gráficas de consumo.
- Detección automática de entrada de faxes.
- Recepción de fax desde el propio sistema y posterior envío por e-mail.
- Gestión de colas de llamadas entrantes.
- Grabación de llamadas entrantes y salientes.

- Monitorización de llamadas en curso.
- Soporta videoconferencia con protocolos SIP e IAX2.

2.5.3 Servicios que implementa Asterisk

- Extensiones móviles
- Enrutamiento por Indetificador de llamada
- Mensajería SMS
- Sistema TextToSpeach
- Emitir Letras y Números
- Detección de Voz
- Llamada a tres
- Fecha y Hora
- Traducción de Codec
- Trunking
- Pasarelas VozIP
- Sistema de Buzón de Voz
- Indicador visual de mensaje no escuchado
- Indicador sonoro de mensaje no escuchado
- Mensajes del Buzón de Voz a Email
- Grupos de Buzón de Voz
- Interfaz Web de acceso al Buzón de Voz
- Identificación de llamada en Llamada en Espera
- Soporte de oficina Remoto

- ❑ Sistema de Menú en Pantalla
- ❑ Receptor de Alarmas
- ❑ Adición de Mensajes
- ❑ Autentificación
- ❑ Atención de llamada Automática
- ❑ Listas Negras
- ❑ Transferencia Ciega
- ❑ Transferencia con Consulta
- ❑ Registro de detalles de Llamada
- ❑ Reenvío de llamada en ocupado
- ❑ Reenvío de llamada en No-disponible
- ❑ Reenvío de llamada variable
- ❑ Monitorización de Llamadas
- ❑ Aparcamiento de Llamada
- ❑ Sistemas de Colas
- ❑ Grabación de llamadas
- ❑ Recuperación de Llamadas
- ❑ Enrutamiento de llamadas (DID & ANI)
- ❑ Escucha de Llamadas
- ❑ Transferencia de Llamadas
- ❑ Llamada en Espera
- ❑ Identificación de LLamada
- ❑ Bloqueo por identificación de llamada
- ❑ Tarjetas prepago

- Multiconferencia
- Almacenamiento / Recuperación en BBDD
- Integración con BBDD
- Llamada por Nombre
- Sistema de Acceso directo entrante
- Timbre personalizable
- No molestar
- E911
- ENUM
- Recepción y Envío de FAx
- Lógica de extensiones Flexible
- Listado de directorio Interactivo
- Respuesta de Voz Interactiva(IVR)
- Agentes de llamada Locales y Remotos
- Macros
- Música en Espera
- Música en Espera en transferencia
- Sistema de MP3 configurable
- Control de Volumen
- Marcador Predictivo
- Privacidad
- Protocolo de establecimiento abierto (OSP)
- Conversión de protocolo
- Captura de Llamadas

2.5.4 Productos Asterisk

Entre los productos de Asterisk se encuentra Elastix, Trixbox, Asterisknow, Asterisk@Home entre otros, el que se ha destacado por su confiabilidad modularidad y fácil uso ha sido Elastix. Lo cual ha ayudado mucho al momento de decidir que producto utilizar para el desarrollo del presente trabajo de Tesis.

2.6 ELASTIX

Elastix es un software aplicativo que integra las mejores herramientas disponibles para PBXs basados en Asterisk en una interfaz simple y fácil de usar. Además añade su Propio conjunto de utilidades y permite la creación de módulos de terceros para hacer de este el mejor paquete de software disponible para la telefonía de código abierto.

La meta de Elastix son la confiabilidad, modularidad y fácil uso. Estas características añadidas a la robustez para reportar hacen de la misma, la mejor opción para implementar un PBX basado en Asterisk. Las características proveídas por Elastix son muchas y variadas. Elastix integra varios paquetes de software, cada uno incluye su propio conjunto de características. Además añade nuevas interfaces para el control y reportes de si mismo, lo que lo hace un paquete completo.

2.6.1 Instalación Elastix

La instalación de Elastix es sumamente sencilla, hay que tomar en cuenta la versión que se va a instalar para el presente trabajo de tesis se va a instalar la versión 2.0. Ver Anexo1.

2.6.2 Características

- Soporte para VIDEO
- Soporte para Virtualización
- Interfaz Web para el usuario
- Interfaz para tarifas
- Configuración gráfica de parámetros de red
- Reportes de uso de recursos
- Opciones para reiniciar/apagar remotamente
- Reportes de llamadas entrantes/salientes y uso de canales
- Módulo de correo de voz integrado
- Interfaz Web para correo de voz
- Servidor de correo integrado incluye soporte multi-dominio.
- Interfaz web para email
- Módulo de panel operador integrado
- Módulos extras SugarCRM y Calling Card incluidos
- Sección de descargas con accesorios comúnmente usados
- Interfaz de ayuda embebido
- Servidor de mensajería instantáneo (Openfire) integrado

- ❑ Soporte Multi-lenguaje. Los lenguajes soportados incluidos son:

- Ingles	- Alemán
- Español	- Francés
- Ruso	- Rumano
- Coreano	- Esloveno
- Griego	- Portugués
- Chino	- Danés
- Polaco	- Italiano

2.6.3 Funcionalidades

- ❑ Voicemail o Buzón de voz
- ❑ Fax
- ❑ Soporte para softphones
- ❑ Consola de operador
- ❑ IVR o Recepcionista digital
- ❑ Interfase de configuración Web
- ❑ Grabación de llamadas
- ❑ Limite de tiempo
- ❑ Least Cost Routing
- ❑ Roaming de extensiones
- ❑ Email
- ❑ Llamada en espera

- Interconexión entre PBXs
- Identificador de llamadas
- Reportación avanzada
- Billing
- Extras

2.6.4 Soporte para hardware de telefonía

Elastix cuenta con un buen soporte para hardware de telefonía, contando con drivers para los principales fabricantes de tarjetas como:

- OpenVox
- Digium
- Sangoma
- Rhino Equipment
- Xorcom
- Yeastar

Elastix también soporta muchas marcas de teléfonos gracias a que los protocolos SIP e IAX que usa Asterisk lo permiten. Estos protocolos son abiertos por lo que prácticamente cualquier fabricante puede implementar un teléfono que se comunique sobre estos estándares. Algunos fabricantes de teléfonos soportados son:

- Polycom
- Atcom
- Aastra
- Linksys
- Snom
- Cisco
- Nokia
- UTstarcom

2.6.5 Protocolos que soporta

- IAX™ (Inter-Asterisk Exchange)
- IAX2™ (Inter-Asterisk Exchange V2)
- H.323
- SIP (Session Initiation Protocol)
- MGCP (Media Gateway Control Protocol
- SCCP (Cisco® Skinny®)
- Traditional Telephony Interoperability
- DTMF support
- PRI Protocols, entre otros

2.6.6 Codecs soportados

- ADPCM
- G.711 (A-Law & µ-Law)
- G.722
- G.723.1 (pass through)
- G.726
- G.729 (si se compra licencia comercial)
- GSM
- iLBC

2.6.7 Soporte para interfaces análogas

- FXS/FXO

2.6.8 Soporte para interfaces digitales

- E1/T1/J1 a través de protocolos PRI/BRI/R2

CAPITULO III

III. ESTUDIO DE TECNICAS DE ALTA DISPONIBILIDAD EN CLUSTERS VoIP.

3.1 TÉCNICAS PARA OBTENER ALTA DISPONIBILIDAD EN CLÚSTERS VOIP

En el siguiente apartado se mencionará algunas técnicas aplicables para construcción de un clúster VoIP. De esta manera dotaremos a nuestra infraestructura de red virtual de una de las características y requisitos imprescindibles que hoy en día a la hora de ofrecer servicios es fundamental como lo es la alta disponibilidad. Cada día que pasa resulta habitual encontrarnos con servicios que requerimos o que debemos proporcionar con una gran exigencia: rapidez, eficiencia, simplicidad, las 24 horas al día, los 7 días de la semana, todo el año. Es entonces cuando consideramos que ese determinado servicio (base de datos, página web, centralita VoIP, almacenamiento) debe estar continuamente

disponible, lo que implica que debamos aplicar determinadas técnicas tanto hardware como software para cumplir este objetivo.

3.1.1 Criterio de selección de la técnica de alta disponibilidad

La técnica a escoger deberá cumplir con las siguientes características:

- Respaldar y garantizar los servicios de telefonía IP.
- Mínimo tiempo de retraso al levantarse el servidor de respaldo.
- Mayor porcentaje de disponibilidad.

Cabe aclarar que para el presente trabajo de tesis se ha propuesto crear un clúster VoIP; por lo cual se ha tomado en cuenta aquellas técnicas que nos permitan realizar este cometido.

3.1.2 Heartbeat

Heartbeat es un paquete de software que fue creado por LINUX-HA, funciona de forma similar al System V o init pero en vez de una sola máquina pasaría a ejecutar los servicios en los nodos, basándose en que no le llegan respuestas estas se hacen por medio de ping y por pulsaciones del cable serie.

Esta tecnología implementa heartbeats, cuya traducción directa sería: «latidos de corazón». Funciona enviando periódicamente un paquete, que si no llegara, indicaría que un servidor no está disponible, por lo tanto se sabe que el servidor ha caído y se toman las medidas necesarias.

Dichos latidos se pueden enviar por una línea serie, por UDP o por PPP/UDP. De hecho los desarrolladores de Heartbeat recomiendan el uso de puertos serie por varias razones, entre las que destacan que están aislados de las tarjetas de red.

También incluye toma de una dirección IP y un modelo de recursos, incluyendo grupos de recursos. Soporta múltiples direcciones IP y un modelo servidor primario/secundario. Se ha probado satisfactoriamente en varias aplicaciones, como son: servidores DNS, servidores proxy de caché, servidores web y servidores directores de LVS. El proyecto LVS recomienda Heartbeat para aumentar la disponibilidad de su solución, pero no es parte de LVS.

En Linux-HA Heartbeat es un servicio de bajo nivel. Cuando un computadora se une al clúster, se considera que computadora r se ha unido al canal de comunicaciones, por lo tanto «late»; cuando sale, implica que ha dejado el canal de comunicaciones.

Cuando una maquina deja de «latir» y se considera muerto, se hace una transición en el clúster. La mayoría de los mensajes de manejo del clúster que no son heartbeats se realizan durante estas transiciones.

Los mensajes de Heartbeat se envían por todas las líneas de comunicación a la vez, de esta manera, si una línea de apoyo cae, se avisará de ese problema antes de que la línea principal caiga y no haya una línea secundaria para continuar el servicio.

Heartbeat también se preocupa por la seguridad, permitiendo firmar los paquetes con CRC de 32 bits, MD5 y SHA1. Esto puede evitar el desastre que podría provocarse si un nodo no miembro se enmascarase como nodo miembro del cluster. El problema es que el entorno donde se ejecuta

Heartbeat no debe parar nunca y con suerte ese entorno se mantendrá comunicado y funcionando durante años.

Hay varias operaciones de mantenimiento de seguridad que necesitan ser efectuadas en ese tiempo, como pueden ser cambio de claves y de protocolos de autentificación. Heartbeat está preparado para esos cambios disponiendo de ficheros para la configuración.

Heartbeat tiene el problema, si no se dispone de una línea dedicada, aunque ésta sea una línea serie, al tener un tráfico que aunque pequeño es constante, suele dar muchas colisiones con otros tráficos que puedan ir por la misma red. Por ejemplo, openMosix y Heartbeat en una misma red que no tenga gran ancho de banda no funcionan bien, sobre todo si hay bastantes nodos, pues los heartbeats se envían de cualquier nodo a cualquier nodo, por lo que podrían llegar a ser un tráfico voluminoso.

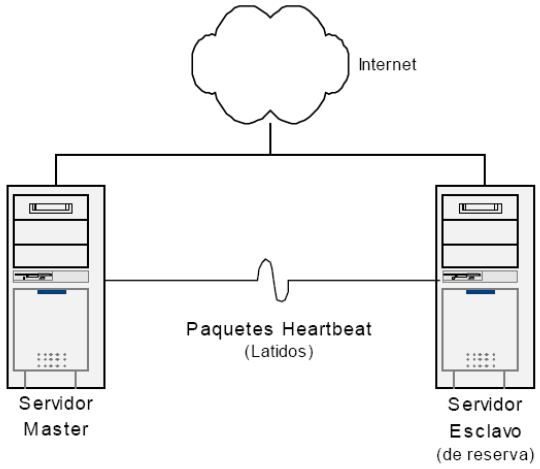


Figura III-1: Arquitectura Heartbeat.

Fuente: Arquitecturas de clustering de alta disponibilidad y escalabilidad (linux virtual server).

3.1.2.1 STONITH

STONITH son la Siglas de “Shoot The Other Node In The Head” (“ Pégale un Tiro en la Cabeza al otro Nodo”). Es una técnica usada por Heartbeat que se asegura de que un servidor supuestamente

muerto no interfiera con el funcionamiento del cluster, en caso de no implementarse bien esta técnica, podría dar lugar a que el cluster no funcione.

A grosso modo STONITH consiste en que el servidor secundario nota que el primario no funciona, y este le haría un DDOS al primario para asegurarse de que ha sido un falso positivo y tomaría el nodo secundario el control.

3.1.2.2 FUNCIONAMIENTO

Según Marcos Martínez Jiménez y Gabriel Bergés Pujol [8]:el funcionamiento de Heartbeat se basa en el envío y recepción de señales enviadas por los demonios de Heartbeat que se ejecutan en ambas máquinas, a estas señales se les conocen como "latidos".

La diferencia entre el servidor maestro y el esclavo, radica en la prioridad que tienen para ofrecer un servicio. Aquí, el esclavo solo ofrecerá el servicio cuando deje de escuchar los latidos del maestro durante periodo de tiempo determinado, pasado el cual se supondrá que el servidor maestro dejó de funcionar.

Una vez que el esclavo vuelva a escuchar los latidos del maestro, este tomará el control nuevamente, a menos que dentro de la configuración de Heartbeat se haya colocado la directiva auto_failback en off. Esta directiva puesta en off, quiere decir que si la máquina que era maestro vuelve a funcionar, ya no retomará el control del servicio, sino se convertirá en la nueva esclava.

El maestro y esclavo pueden comunicarse por medio de dos interfaces, el puerto serial (RS-232) o las tarjetas Ethernet.

Heartbeat implementa una serie de tipos de latidos:

---

[8] *Extraído de: Arquitecturas de clustering de alta disponibilidad y escalabilidad (linux virtual server), acade (lvs). [en línea]*

- Bidirectional Serial Rings.
- UDP/IP Broadcast, UDP/IP Multicast.
- Pings especiales Heartbeat para routers.

Heartbeat es el encargado de inicializar o detener el servicio al cual se le quiere prestar en alta disponibilidad. Este servicio es prestado a través del uso de una única IP en ambas máquinas, que en realidad no es más que la dirección IP Virtual (VIP). A esta VIP se le considera como un recurso.

Aquí ambas máquinas, tanto la esclava como la maestra, tienen una dirección IP propia y también comparten la VIP. Cuando Heartbeat lanza el servicio a prestarse, se activa la VIP en esa máquina.

Cuando se produce un fallo en la máquina que presta el servicio se le conoce como failover. Cuando el maestro vuelve a estar activo se le conoce como failback.

3.1.3 DUNDi

DUNDi ™ (Distributed Universal Number Discovery) es un sistema de localización de gateways para el acceso a los servicios de telefonía. Utiliza un esquema punto a punto y, a diferencia de ENUM que es estrictamente jerárquico por que se basa en DNS, DUNDi no requiere ninguna arquitectura de red en particular ni un esquema jerárquico cliente servidor.

En otras palabras DUNDI es capaz de consultar los contextos de otros equipos para encontrar una ruta hacia determinado número. Un contexto es una colección de extensiones.

DUNDi en realidad no realiza una llamada como tal, ya que no es un protocolo de señalización VoIP; más bien el recibe y proporciona la información necesaria para poder contactar a los equipos independientemente del protocolo VoIP que sea usado.

DUNDi fue inventado por Mark Spencer, quien también desarrolló Asterisk, núcleo de la telefonía en Elastix, por lo tanto es de esperar que la integración con este ultimo sea completamente transparente así como su compatibilidad impecable.

Para que DUNDi funcione se debe conocer al menos un peer quien a su vez, si no puede responder al requerimiento, puede delegar la consulta a un peer conocido por él, y así hasta que se encuentre a un peer que tenga una respuesta al número consultado (aunque este parámetro es configurable con TTL).

Un ejemplo típico de la utilidad de DUNDi es en una empresa multi-sede, en la cual cada sede tiene su propio equipo con Elastix. Cada equipo puede publicar sus extensiones y si uno de los equipos pregunta, por ejemplo, ¿dónde está el numero 456? la consulta se enviara directa o indirectamente a todos los servidores, y el servidor que tenga esa extensión responderá algo como IAX2/usuario:clave@1.2.3.4/456.

Aunque cada equipo tenga asignado un rango de extensiones o una serie de números, DUNDI resultará útil, ya que no intentara comunicarse con el equipo si la extensión no esta creada, aunque este en su rango de extensiones.

3.1.3.1 Aplicaciones de DUNDi

Básicamente, DUNDI nos permite crear una red P2P de centrales, donde cada una “publica” los números de teléfono de los que es responsable así como sus extensiones locales, números para la que es la ruta de menor coste, etc.

Ejemplo típico es el de la empresa multi-sede. Cada sede publica sus extensiones propias, de forma que el de centrales de la red pueda localizarlas. Esta consulta se enviaría, directa o indirectamente, a todas las centrales de la red DUNDI. La central que tenga esa extensión responderá algo como "tengo esa extensión, y la central que hizo la consulta utilizará esa información para realizar la llamada a través de la línea de datos a coste 0.

Otro ejemplo de uso. Supongamos dos sedes de la misma empresa en diferentes localizaciones, Riobamba y Quito, y un usuario de la sede Riobamba llama a un teléfono de Quito. En el caso de que tengamos tarifa plana en las líneas telefónicas de Riobamba, esta llamada no tendrá coste, pero ¿y si no tenemos tarifa plana en todas las líneas?. DUNDI pregunta a todas las centrales de la red cual tiene como número local un número de Quito, la centrale de Quito responde "yo lo tengo" y la central de Riobamba, efectúa la llamada a través de las líneas telefónicas de Quito a precio de llamada local.

En el caso de que las sedes están en diferentes países. El ahorro ya pasa a ser muy importante.
Aunque DUNDI, básicamente solo pregunta "por donde puedo llamar", su aplicaciones son altisimas, y nos proporciona grandes ventajas en el presente trabajo de tesis.

El protocolo DUNDi utiliza por defecto el puerto 4520/UDP. Habrá que abrirlos en los firewalls. Es independiente de IAX, es decir, la cadena de conexión devuelta en una consulta puede hacer referencia a cualquier tipo de canal (IAX2, SIP, H323, etc), aunque normalmente se usa el IAX2.

3.1.3.2 Clúster VOIP con DUNDi

Para este trabajo de tesis, no se tendrán centrales en distintas redes, sino todas en la misma red y todas gestionando las mismas extensiones. De esta forma, se utilizará DUNDi para establecer la comunicación entre ellas y puedan anunciarse, en este caso, no las extensiones que gestionan, ya que son las mismas, si no las extensiones que están registradas en el momento de la llamada. Esto se debe a que hace uso de DNS SRV, por tanto, a la hora de asignarnos dirección IP, puede asignar diferentes direcciones por lo que los usuarios se encontrarán en centrales distintas.

Cuando un usuario llame a una extensión que gestione su misma central, no habrá problema ya que la llamada se conoce como "llamada local" y sería directa. En caso de pertenecer a una central diferente, será cuando se aplique la consulta DUNDi al resto de centrales para saber en cuál se encuentra y poder gestionar la llamada entre ambas.

3.1.4 Definición de parámetros para evaluación.

Los parámetros que a continuación se definen para realizar el estudio comparativo de las técnicas de alta disponibilidad están basados en los requerimientos del usuario final, los usuarios intermitentes, y según el criterio de la autor de la tesis.

Tabla III.I : Determinación de los criterios de Comparación.

Parámetros	Concepto
Configuración	Cada técnica tiene su propia manera de estructurar sus procedimientos y la utilización de un determinado mecanismo.
Soporte Criptografico	Para asegurar la confidencialidad en el establecimiento de la llamada telefónica mediante el uso de una clave cifrada.
Aprendizaje	Una documentación insuficiente o un soporte inadecuado al usuario pueden hacer que un usuario abandone o descarte el uso.
Escalabilidad	Es la propiedad deseable de una red que indica su habilidad para extender o hacerse más grande sin perder calidad en los servicios ofrecidos, es decir nos da una idea del comportamiento del sistema cuando se incrementa el número de procesadores.
Calidad de Servicio	Es la capacidad de dar un buen servicio, es decir garantizar la realización de una llamada en un tiempo dado.

Los parámetros generales que se ha tomado en cuenta para desarrollar el estudio comparativo se dividen en variables que serán evaluadas de acuerdo a una tabla de ponderación.

3.1.5 Ponderación.

Cada variable se evalúa de acuerdo a las siguientes posibles interpretaciones, a estas se les ha asignado un peso que va en un rango de 0 a 5 que se muestra en la tabla a continuación.

Tabla III.II : Tabla de Ponderación.

Ponderación					
Cualitativa				Porcentaje (%)	Cuantitativa
Fácil	Excelente	Eficiente	Cumple Totalmente	>=80 y < =100	5
Medio Fácil	Muy bueno	Medio Eficiente	Cumple	>=60 y < 80	4
Normal	Bueno	Limitado	Limitado	>=40 y < 60	3
Medio difícil	Regular	Medio deficiente	Casi no cumple	>=20 y < 40	2
Difícil	Malo	Deficiente	No cumple	< 20	1
No Aplica	No Aplica	No Aplica	No Aplica	0	0

A cada variable se la define y se establece la comparación entre DUNDi y Heartbeat, los datos fueron obtenidos mediante la investigación, pruebas realizadas y la experiencia que se ha adquirido al probar cada una de estas técnicas.

Parámetro de Configuración

En la siguiente tabla se define a cada una de las variables que se le ha considerado para el parámetro de configuración.

Tabla III.III : Variables del parámetro Configuración.

Variables	Concepto
Facilidad de instalación	La capacidad del producto del software para ser instalado en un ambiente específico.
Nivel gráfico	El poseer una interface grafica para la instalación.

Facilidad de Instalación

La instalación de DUNDi se realiza a bajo nivel, mediante el uso de comandos propios de Linux, es por esa razón que es necesario tener un amplio conocimiento de los mismos, por lo tanto se califica como Normal.

La instalación de Heartbeat se realiza a bajo nivel al igual que la anterior, por la misma causa toma la misma calificación como Normal.

Nivel Gráfico

Gracias a la interface propia de Elastix 2.0, DUNDi puede ser manipulado desde dicha interface, esto facilita en parte la configuración y monitoreo por esa razón tiene una calificación de Bueno.

Heartbeat no tiene interface alguna, la configuración y monitoreo siempre se realiza a bajo nivel, su calificación es de Malo.

Tabla III.IV : Comparación Variables del parámetro de Configuración.

	Configuración			
Variables	**DUNDi**		**HEARTBEAT**	
Facilidad de instalación	Normal	3	Normal	3
Nivel gráfico	Bueno	3	Malo	1
	Total	6	**Total**	4

Tomando el valor más alto que es 6 corresponde al 60 % para el parámetro de configuración cuando se utiliza DUNDi. Mientras que para Heartbeat se tiene un 40 %. Se aplica una regla de 3 para conocer los porcentajes en cada caso en particular.

Para DUNDi:

$$\frac{6 * 100}{10} = 60\ \%$$

Para Heartbeat:

$$\frac{4 * 100}{10} = 40\ \%$$

El proceso de instalación para DUNDi es mucho más alto que Heartbeat ya que para Heartbeat se necesita tener conocimientos más avanzados.

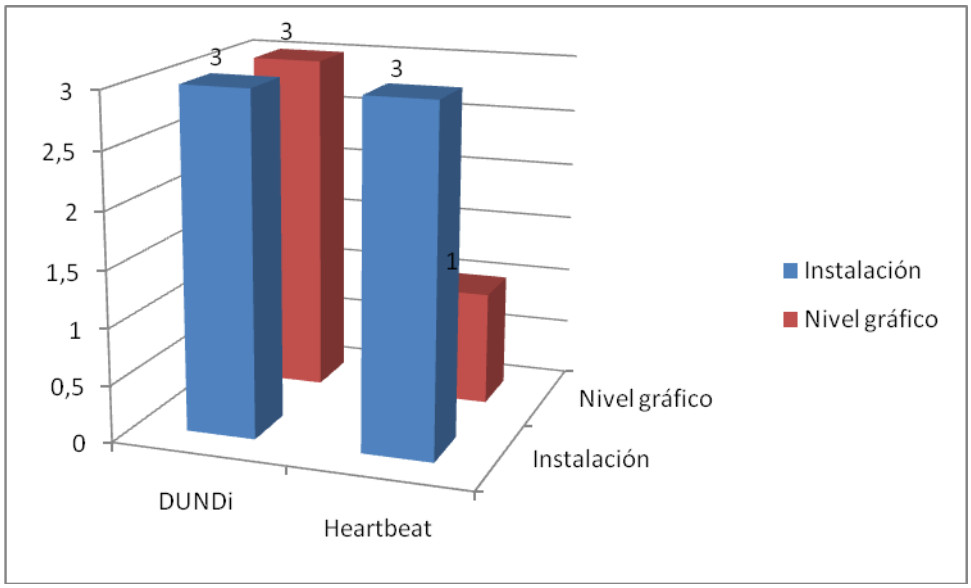


Figura III-2: Gráfico parámetro configuración

En la Figura III-2, se observa que DUNDi posee los valores más altos que Heartbeat sobretodo en el nivel gráfico.

Soporte Criptográfico

En la siguiente tabla se define a cada una de las variables que se le ha considerado para el parámetro Soporte Criptográfico.

Tabla III.V : Variables del parámetro Soporte Criptográfico.

Variables	Concepto
Cifrado	Los sistemas de clave simétrica utilizan una misma clave para cifrar y descifrar de forma que tanto el emisor como el receptor deben ponerse de acuerdo previamente en la clave a utilizar
RSA	Algoritmo de reducción criptográfico.
MD5	Algoritmo asimétrico cifrador de bloques**,**
SHA1	

RSA

DUNDi utiliza el algoritmo de cifrado RSA que es un sistema criptográfico de clave pública, se en el problema de la factorización de números enteros, será seguro mientras no se conozcan formas rápidas de descomponer un numero grande en producto de primos.

La calificación que se le atribuye es Bueno. Heartbeat no utiliza este algoritmo criptográfico.

MD5

Heartbeat utiliza el algoritmo de cifrado MD5 que es un algoritmo de reducción criptográfico. A pesar de su amplia difusión actual, la sucesión de problemas de seguridad detectados, plantea una serie de dudas acerca de su uso en un futuro. Por lo tanto la calificación que recibe es Bueno.

SHA1

Heartbeat utiliza el algoritmo de cifrado SHA1 es un sistema de funciones hash criptográficas. Ha sido examinado muy de cerca por la comunidad criptográfica pública, y no se ha encontrado ningún ataque efectivo. Por lo cual la calificación que toma es Excelente.

A continuación se muestra la tabla con los pesos correspondientes a cada una de los algoritmos de encriptación.

Tabla III.VI : Variables del parámetro Soporte Criptográfico.

	Soporte Criptográfico			
Variables	**DUNDi**		**HEARTBEAT**	
RSA	Bueno	3	No aplica	0
MD5	No aplica	0	Bueno	3
SHA1	No aplica	0	Excelente	5
	Total	3	**Total**	8

Tomando el mayor valor que es 8 se deduce que Heartbeat tiene mejor soporte criptográfico ya que utiliza un algoritmo criptográfico seguro.

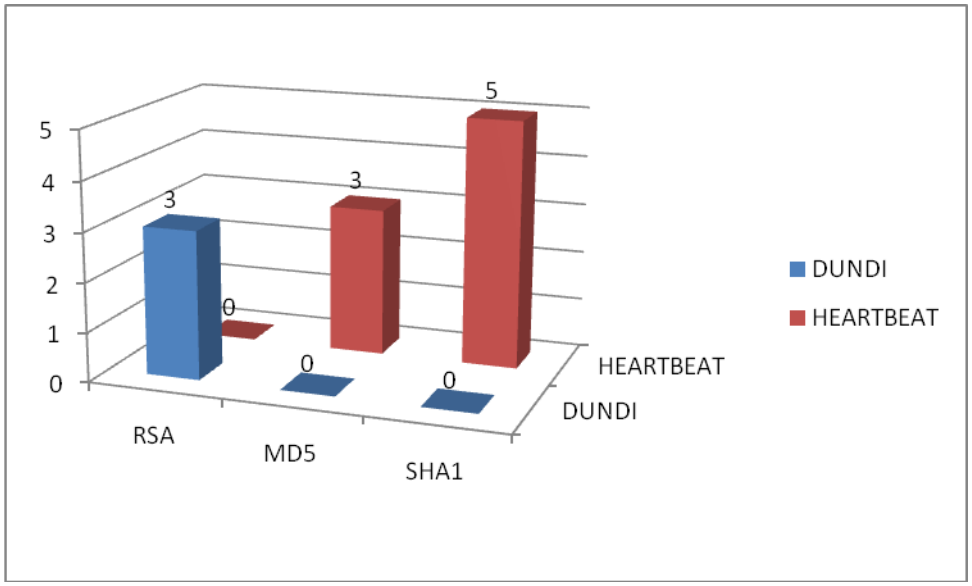


Figura III-3: Gráfico parámetro configuración

Como se ve en la Figura III-3 SHA1 que es el sistema criptográfico que utiliza Heartbeat supera a RSA y MD5.

Parámetro de Aprendizaje

En la siguiente tabla se define a cada una de las variables que se le ha considerado para el parámetro de Aprendizaje.

Tabla III.VII : Variables del parámetro Aprendizaje.

Variables	Concepto
Documentación	Para un correcto desempeño debe existir en medios de consulta como Internet, manuales, tutoriales, ejemplos prácticos
Soporte	Debe existir ayuda en línea, foros

Documentación

Para la búsqueda de fuentes de información para DUNDi se suman sin filtrar 673.000 páginas en 0,54 segundos y la búsqueda para resultados en español 13.000 páginas en 0,58 segundos.

La valoración se realiza haciendo un promedio entre la información filtrada y no filtrada.

DUNDi

$$\frac{673.000 * 13.000}{2} = 343000$$

Para la búsqueda de fuentes de información para Heartbeat se suman sin filtrar 6.260.000 páginas en 0,54 segundos y la búsqueda para resultados en español 50.000 páginas en 0,21 segundos [9].

Heartbeat

$$\frac{6.260.000 * 50.000}{2} = 3.155.000$$

[9] *http://www.google.com* 20/12/2011

El valor más alto es 3.155.000, el cual corresponde al 100 % de la información existente para Heartebeat, por lo tanto se hace una asignación cumplimiento total, para determinar el valor de DUNDi se realiza una regla de 3.

DUNDi

$$\frac{343.000 * 100}{3.155.000} = 10.87\%$$

Soporte

Para valorar esta variable se toma como dato la información obtenida al realizar una búsqueda en internet de los foros y ayudas para DUNDi y Heartbeat.

La tabla que a continuación se muestra contiene las direcciones y temas existentes en foros

Tabla III.VIII : Información acerca de foros y ayuda en línea.

FOROS Y AYUDA EN LÍNEA			
DUNDi		**Heartbeat**	
Dirección	**Tema**	**Dirección**	**Tema**
http://www.elastix.org/index.php/en/component/kunena/53-trucos/10183-usando-dundi-en-elastix-o-en-un-asteriskfreepbx.html	Usando DUNDi en Elastix	http://www.alcancelibre.org/staticpages/index.php/como-cluster-heartbeat-centos	Configurar Heartbeat
http://www.ecualug.org/2008/09/14/blog/filipok/usando_dundi_en_elastix_o_en_un_asteriskfreepbx	DUNDi	http://www.linuxespanol.com/ftopic23987.php	Heartbeat y DRBD
http://elajonjoli.org/node/11	Certificado de Encriptación	http://foro.powers.cl/viewtopic.php?f=1&t=230116	Heartbeat
		http://www.openecuador.org/modules/newbb/viewtopic.php?topic_id=149&forum=6	Guia para configurar un cluster
		http://foros.ovh.es/showthread.php?t=9194	DRBD
		http://www.pdaexpertos.com/foros/viewtopic.php ?t=22339	Controles

Se toma el valor máximo de 6 que corresponde al 100 % y es de Heartbeat para conocer la valoración porcentual de DUNDi se realiza una regla de 3.

DUNDi

$$\frac{3 * 100}{6} = 50\ \%$$

Parámetro de Escalabilidad

En la siguiente tabla se define a cada una de las variables que se le ha considerado para el parámetro de Escalabilidad.

Tabla III.IX : Variables Parámetro Escalabilidad.

Variables	Concepto
Carga	Se refiere al incremento de nodos a red telefónica.

Carga

El nuevo nodo que forme parte de la red con DUNDi se debe crear cada una de las extensiones existentes en el sistema es por eso que tiene una calificación de Cumple, ya que se puede incrementar nuevos nodos pero esto tomaría tiempo y recursos.

Para Heartbeat el incremento de un nuevo nodo es más simple ya que los datos se replicarían automáticamente cuando sincronice con el servidor del cual se obtenga los datos.

Tabla III.X : Comparación variables del parámetro Escalabilidad

	Escalabilidad			
Variables	**DUNDi**		**HEARTBEAT**	
Carga	Cumple	4	Cumple Totalmente	5
	Total	4	**Total**	5

Tomando el valor más alto que es 5 esto equivale al 100% de Escalabilidad y corresponde a Heartbeat, para conocer el porcentaje de DUNDi realizamos una regla de 3.

DUNDi

$$\frac{4 * 100}{5} = 80\ \%$$

A continuación se muestra la gráfica correspondiente a la variable carga.

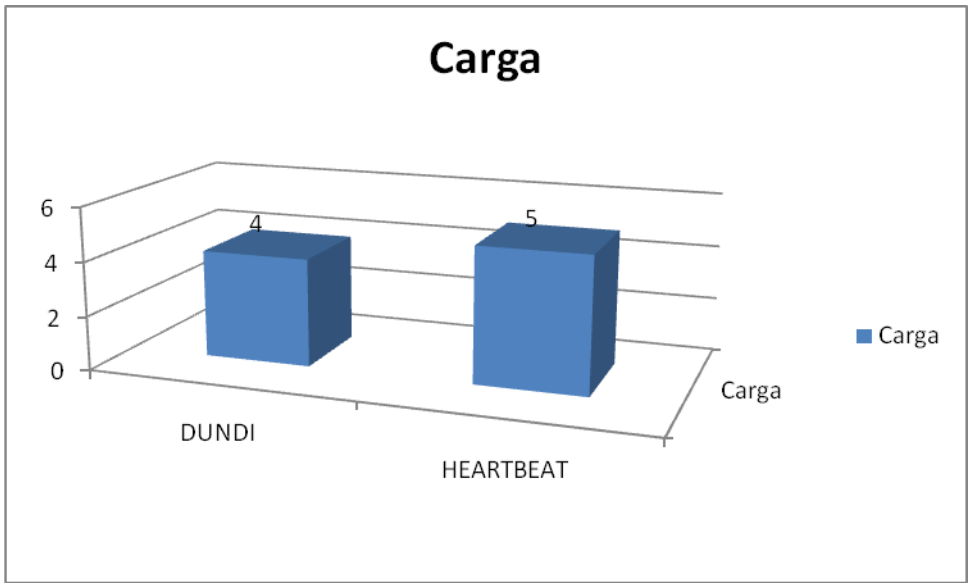


Figura III-4: Gráfico parámetro escalabilidad

Como se ve en la Figura III-4 Heartbeat supera a DUNDi en escalabilidad.

Parámetro Calidad de Servicio

En la siguiente tabla se define a cada una de las variables que se le ha considerado para el parámetro de Calidad de Servicio.

Tabla III.XI : Variables parámetro Calidad de Servicio.

Variables	Concepto
Creación de Extensiones	Determina como se debe registrar las extensiones en los servidores que conforman el clúster
Autenticación después de caída del servicio	Tiempo que demora en autentificarse una terminal después de haber perdido el control el servidor activo.
Puesta en marcha del servidor esclavo	Determina cuanto tiempo demora en tomar el control el servidor esclavo.

Creación de Extensiones

En DUNDi la creación de las extensiones se realiza en cada uno de los nodos que conforman el clúster; por lo tanto se le califica esta acción como deficiente.

En cuanto a Heartbeat para registrar una nueva extensión, es necesario crearla en el nodo que esté actuando como principal y automáticamente será replicada en el servidor secundario; por lo tanto se le califica como eficiente.

Autenticación después de caída del servicio

En DUNDi la autentificación después de la caída del servicio, no se realiza de forma automática se necesita de una acción manual, por lo cual no aplica para ser evaluada.

En Heartbeat la autentificación es automática transcurrido un tiempo, por lo tanto se lo califica como eficiente.

Puesta en marcha del servidor esclavo

En DUNDi los nodos que conforman el clúster permanecen activos, cuando un nodo deja de estar activo se le asigna una nueva IP a todas las extensiones que se encontraba dando servicio dicho servidor, pero es necesario reiniciar las terminales para que se identifique cual es el nuevo servidor que les ofrecerá el servicio. Por lo tanto se le califica como deficiente.

En Heartbeat el servidor esclavo toma el control y las terminales lo reconocen automáticamente. Por lo tanto se lo califica como Eficiente.

Tabla III.XII : Comparación variables del parámetro Calidad de Servicio.

	Calidad de Servicio			
Variables	**DUNDi**		**HEARTBEAT**	
Creación de Extensiones	Deficiente	1	Eficiente	5
Autenticación después de caída del servicio	No aplica	0	Eficiente	5
Puesta en marcha del servidor esclavo	Deficiente	1	Eficiente	5
	Total	2	**Total**	15

Tomando el valor más alto que es 15 corresponde al 100% de calidad de servicio y pertenece a Heartbeat. Para conocer el valor porcentual de DUNDi se aplica una regla de 3.

DUNDi

$$\frac{2 * 100}{15} = 13.33\ \%$$

A continuación se muestra la grafica que corresponde a esta comparación del parámetro calidad de servicio.

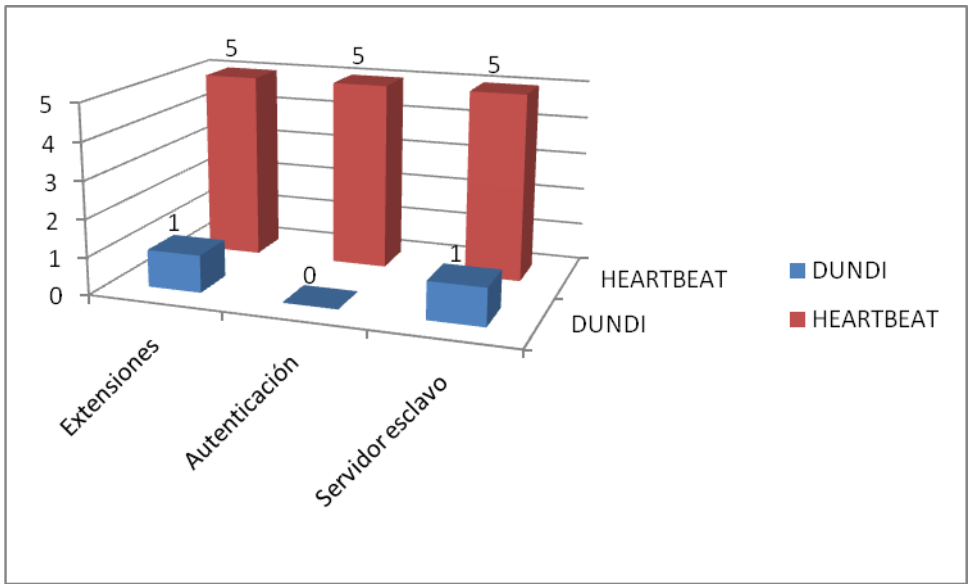


Figura III-5: Gráfico parámetro calidad de servicio**.**

Como se observa en la Figura III-5 los resultados obtenidos muestran que Heartbeat supera con un 100 % sobre DUNDi que obtuvo apenas 13.33 % esto nos indica que la implementación de la red de alta disponibilidad se lo realizara con Heartbeat.

CAPITULO IV

IV. DISEÑO E IMPLEMENTACIÓN DE UNA RED DE ALTA DISPONIBILIDAD EN UN AMBIENTE DE PRUEBA.

MODELO DUNDI

4.1 ESQUEMA GENERAL

En el presente capitulo se dará a conocer todos los módulos efectuados para la realización del presente trabajo de tesis.

En lo que se refiere a hardware, se ha hecho uso de varias máquinas para poder simular la red. Como se pretende crear un clúster de centrales Asterisk, de momento basta con utilizar tres equipos, puesto que la red a implementar será una red de pruebas y por otra parte se va a necesitar una máquina para los servidores DNS y DHCP. Finalmente, serán necesarios algunos terminales para realizar las pruebas de llamadas.

Se puede observar que el número el número de equipos es elevado y puede no ser fácil disponer de tal cantidad, por lo que se recomienda hacer uso del software VMWare Worstation versión 7.0. Este programa nos permite crear tantas máquinas virtuales como nos permita el equipo donde se encuentra instalado. Este programa se instalaró en un equipo portátil AMD Turion X2 64 de doble núcleo a 2,1 GHz y 4GB de memoria RAM,. El sistema operativo que correrá en dicha máquina será Windows 7 Ultimate.

Se ha utilizado dos máquinas para las centrales, dos más para los servidores DNS con sistema centOS 5.0 y unterminal, por lo que se ha creado cuatro máquinas virtuales. Las características físicas de estas máquinas pueden variar debido a que dependen, en parte, al hardware disponible en el equipo físico donde se encuentran instaladas, por lo que por ejemplo, la memoria RAM, puede variar de unas a otras.

Es muy importante comentar en este punto que a las máquinas virtuales, se puede cargar y editar archivos via ftp, haciendo uso del software Filezilla client. Para facilitar la digitación de comandos y líneas de código la configuración de éstas se hará de forma remota vía SSH con Putty.

Las centrales, como cabe de esperar, usarán el software Elastix , en este caso la versión 2.0 y asterisk-addons-1.6.1.1 para el uso de bases de datos MySQL. Para consultar su instalación, puede consultarse los ANEXOS. Los servidores DNS utilizarán el software BIND 9.0, como ya se comentó en apartados anteriores, esto sobre la plataforma Linux en la distribución de centOS 5.0.

4.2 Descripción de los módulos de prueba desarrollados

4.2.1 Terminales

Los terminales serán los encargados de permitirnos realizar las llamadas. Podrán ser teléfonos físicos, conocidos como hardphone, se dispone de Teléfonos IP CISCO y Grandstream o en su defecto programas informáticos que cumplen la misma función, llamados softphone (por ejemplo X-Lite, Zoiper). Un requisito que deben cumplir estos teléfonos para que funcionen en la red diseñada es que tienen que tener soporte para DNS SRV y el protocolo SIP esto es elemental para los terminales.

A continuación se explicará de forma puntual las características y configuración del Teléfono IP CISCO 7912 y Grandstream.

4.2.2 Teléfonos IP

La configuración de los teléfonos IP CISCO y GRANDSTREAM se mostrará en el Anexo 2.

4.2.3 Servidor DNS

Se ha visto la necesidad de instalar un servidor DNS primario conocido también como Maestro y uno secundario o esclavo. Esto ya que como se requiere que exista Alta disponibilidad, en el caso

de que nuestro servidor DNS dejase de funcionar el esclavo empezaría a actuar, de tal manera que la red no deje de trabajar.

A continuación se explicará de forma concreta la funcionalidad que el servidor DNS presentará en la red de alta disponibilidad.

La necesidad de un servidor DNS en la presente tesis tiene como objeto la resolución de una dirección IP, no se hará el uso que generalmente se da a un servidor de resolución de nombres, de forma explícita para la resolución de nombres. Su uso será DNS SRV, el mismo que mantienen estabilidad y también abre la posibilidad para utilizar tu propio dominio, sin importar el dominio del servicio del SIP que estás utilizando.

Los expedientes del recurso del DNS SRV indican cómo encontrar los servicios para los varios protocolos. Éste describe a uno de los registros de DNS (conocido como SeRVice en inglés) que nos permite anunciar los servicios que ofrece nuestro dominio, en nuestro caso SIP.

Descrita la explicación anterior, se puede afirmar que el servidor DNS es el encargado de suministrar las direcciones IPs de las centrales a todos aquellos terminales sean estos softphones o teléfonos IP que deseen registrarse y de esta manera establecer la conexión a la red telefónica.

De tal manera que como es éste quien gestiona las direcciones, se puede además conseguir fácilmente un balanceo de carga, es decir, podemos decidir a qué central se le asignará mayor carga de procesos a la hora de recibir registros, ya sea, por ejemplo, porque tenga mayor capacidad de procesamiento o porque nos interese tener liberada una de las centrales por consumo de recursos.

Para realizar la configuración del servidor DNS se usará BIND (Berkeley Internet Name Domain) el más común en internet sobre sistemas Unix, en nuestro caso montado sobre una plataforma Centos.

Para realizar el trabajo de forma grafica, se ha usado una herramienta de configuración de sistemas accesible vía web usada también sobre GNU/Linux y otros sistemas Unix. Webmin está escrito en Perl y se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, servicios, archivos de configuración, entre otroa, así como configurar modificar y controlar muchas aplicaciones libres, como el servidor DNS, DHCP, MySQL entre otros. En el Anexo 3 se explica de forma más detallada la configuración del servidor DNS y DN SRV.

4.2.4 Base de Datos MySQL

Se ha desarrollado una Base de Datos sobre MySQL, ya que un requerimiento importante es la creación de nuevas extensiones. Dado que en cualquier momento el administrador, se verá en la necesidad de crear una nueva extensión. Esto se logra haciendo uso la tecnología Realtime.

En este modulo se explicará todo a cerca de la aplicación basado en RealTime. Esta tecnología permite realizar modificaciones en la configuración de la central Elastix basada en Asterisk sin necesidad de recargarlo nuevamente. Esto es posible realizar gracias a que ciertos módulos permiten ser configurados desde una Base de Datos.

La Base de Datos se ha creado en cada una de las centrales esto es una gran ventaja ya que en el caso de que una de las centrales pare sus procesos, cualquier otra central tenga la capacidad de

tomarse a cargo las extensiones que esta gestiona. A continuación se explicará la configuración para Asterisk utilizada para Realtime.

4.2.5 Asterisk Realtime

Se ha implementado realtime, ya que en el momento de realizar modificaciones, crear extensiones, etc. No haya necesidad de recargar Asterisk. En primer lugar se indicará la forma de instalar el CDR en una base de datos que se denomina "Asterisk". Para esto se ha instalado MySQL en las centrales Asterisk y las librerías libmysqlclient15-dev y libmysqlclient15off para facilitar la instalación se usó la herramienta Webmin. Se explica de manera más detalla en el Anexo 4.

4.3 DUNDi

A este punto se ve necesario explicar el por qué se ha optado por la tecnología DUNDi, este un tecnología diseñada por el creador de Asterisk Mark Spencer. Su objetivo en un principio era crear sistemas distribuidos de Asterisk en una red peer-to-peer, donde los clientes y servidores no cumplen roles fijos, lo que realmente se trató es tener centralitas Asterisk es distintos puntos de la red y conseguir que los usuarios de unas y otras se llamasen entre sí.

En el presente trabajo de investigación, las centrales telefónicas son nodos que forman un clúster pero que gestionan diferentes extensiones en un momento dado, cuando esto sucede DUNDi se encarga de establecer la llamada entre distintas centrales, de manera segura, y haciendo uso la encriptación RSA.

Elastix está basada en Asterisk y como ya sabemos, es una central de telefonía que permite el uso de la tecnología VoIP, siendo Asterisk la plataforma actual más extendida en este campo. En este apartado se explicará cómo deben ser configuradas las centrales para su correcto funcionamiento.

4.3.1 Configuración

En la siguiente configuración de DUNDi se demuestra cómo se hace la distribución del plan de marcado en 4 equipos con la mencionada tecnología, además se puede afirmar que de esta manera nuestro sistema se convierte totalmente escalable, así que eso es lo que se hará continuación.

4.3.2 Ambiente de prueba

Escenario

Se configurarán cuatro equipos con los siguientes datos, cada uno de estos datos pertenecen a las cuatro centrales o nodos del clúster respectivamente.

Tabla IV.XIII : Direcciones IP y MAC de las centrales.

Nombre de equipo	Dirección IP	MAC
pc1.telefonicanet.com	172.30.124.201	00:0C:29:DA:73:F8
pc2.telefonicanet.com	172.30.124.202	00:0C:29:42:02:00
pc3.telefonicanet.com	172.30.124.203	00:0C:29:76:5A:B5
pc4.telefonicanet.com	172.30.124.204	00:0C:29:18:E2:45

dundi.conf

Este es el archivo es donde se especifica las características propias de la central y se da a conocer a las demás centrales. A continuación se generar este archivo desde el principio, sección por sección:

Sección [general]

En esta sección del archivo se define su propia identificación en la nube DUNDi, así como las opciones globales, también se ha rellenado los campos con los datos reales de los equipos (MAC, etc.):

Para pc1.telefonicanet.com:

```
[general]
department=CENTRAL01
organization=Cisco
locality=Riobamba
stateprov=Chimborazo
country=EC
email=info@telefonicanet.com
phone=+593-0000000
; Aqui podemos definir en que red va a escuchar dundi
bindaddr=0.0.0.0
; El puerto en el que va a escuchar, por defecto 4520
port=4520
; Aqui nos identificamos con nuestra MAC address
entityid= 00:0C:29:DA:73:F8
; El numero de consultas que hará DUNDI hasta alcanzar una extensión
ttl=32
; Finaliza las conexiones fallidas
autokill=yes
```

Los archivos completos de la configuración del archivo dundi.conf se presentan en el (Anexo 5)

Sección [mappings]

En esta sección lo que se ha hecho es definir nuestra respuesta a una consulta hacia determinado número que tengamos localmente. Desde esta etiqueta empieza el mapeo de los contextos DUNDi con los contextos presentes en el servidor Asterisk.

La sintaxis para definir los contextos es:

```
[mappings]
; dundi_context => local_context,weight,tech,dest[,options]]
```

- dundi_context: El contexto DUNDi que se quiere compartir con los demás nodos de la red DUNDi.
- local_context: El contexto local definido en el plan de llamadas donde se configuran las rutas o extensiones que se quieren compartir.
- weight: El peso que damos a las rutas que compartimos. Si son extensiones locales se pone 0, si son rutas por la cuales no tenemos una conexión directa o de alta calidad ponemos un número más alto. Al momento de hacer una solicitud si para el mismo número requerido existen distintas rutas, se escogerá la ruta con menor peso.
- tech: Protocolo usado para la conexión entre servidores Asterisk (se usará IAX2)
- dest: Cuando se hace una solicitud desde el servidor B y se encuentra una ruta en el Servidor A, el Servidor A usará esta destinación para recibir la llamada. Simplificando: se crea un user en el iax.conf del servidor Asterisk A y dest representa los paramentos para conectarse a ese user y a través de la conexión recibir las llamadas del servidor B

- options: Son las distintas opciones que se pueden añadir por cada contexto DUNDi:
  - nounsolicited – Llamadas de cualquier tipo que no sean solicitadas no son permitidas en esta ruta
  - nocomunsolicit – Llamadas comerciales no solicitadas no son permitidas en esta ruta
  - residential – El numero es de una residencia
  - commercial – El numero es de una empresa
  - mobile – El numero es un celular
  - nopartial – No se harán búsquedas por números que no sean completos

Este contexto se comparte a otros peers, es decir a las Centrales de Telefonía IP adyacentes.

La ruta definida para las centrales será:

```
[mappings]
priv => exten_SIP,0,IAX2,dundi:${SECRET}@192.168.137.161/${NUMBER},nopartial
```

Los valores de ${NUMBER} y ${SECRET} se reemplazaran automáticamente, según el número que se consulte y la clave aleatoria que se haya generado en ese momento.

Peers

Para finalizar con la configuración del archivo dundi.conf se definen las centrales Asterisk con las se va a tener una conexión directa.

- AA:BB:CC:11:22:33: MAC address de la tarjeta de red de Servidor Asterisk B con el que se crea la conexión

- model: Puede ser:
  - inbound: recibe solamente solicitudes.
  - outbound: solo efectúa solicitudes pero no las recibe.
  - symmetric: recibe y efectúa solicitudes.
- host: direccion IP o nombre de dominio del servidor Asterisk B.
- inkey: clave RSA usada para autenticarse con el servidor Asterisk B.
- outkey: clave RSA usada por el Servidor Asterisk B para autenticarse con el Servidor Asterisk A.
- include: incluye esta conexión para todas las solicitudes efectuadas en el Servidor Asterisk A.
- permit: se definen los contextos DUNDi a los que tendrá acceso este nodo.
- qualify: se controlará periódicamente que la conexión con el nodo esté activa.

A continuación se va a definir los PEERS que consultaran y serán consultados (con la opción symmetric), esto lo realizamos así:

Para pc1.telefonicanet.com:

```
; Identificamos al servidor 2 (CENTRAL02) por su entityid
[00:0C:29:42:02:00]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL02
host=172.30.124.202
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 3 (CENTRAL03) por su entityid
[00:0C:29:76:5A:B5]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL03
host=172.30.124.203
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 4 (CENTRAL04) por su entityid
[00:0C:29:18:E2:45]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL04
host=172.30.124.204
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
```

iax_custom.conf

Es el momento en el que se puede añadir el usuario dundi al archivo iax_custom.conf.

Aquí se procede a definir la configuración de la troncal; como DUNDI va a hacer todo el trabajo de enviar la cadena exacta de como contactarlos solo creamos un usuario que recibe las llamadas autenticadas de la nube DUNDi. Se añaden las siguientes líneas.

En pc1.telefonicanet.com, en pc2.telefonicanet.com, en pc3.telefonicanet.com y en pc4.telefonicanet.com:

```
[dundi]
type=user
context=ext_DUNDi
dbsecret=dundi/secret
; Podemos restringir ciertos codecs para mejorar la calidad
; de voz, o dar prioridad al ancho de banda (con gsm o g729)
disallow=all
allow=ulaw
allow=alaw
allow=gsm
```

Importante definir el parámetro **context** con el valor del contexto (ext_DUNDi) que se ha definido en nuestro plan de marcado.

sip_general_additional.conf

Este archivo contiene la configuración por defecto de todos los usuarios y "peers". Se encuentra anexado en el sip.conf normalmente es donde se configuran los usuarios sip locales, es decir, las extensiones que gestionaría la centralita. Es por esta razón que hay que considerar ciertos puntos

interesantes de configuración en este fichero, ya que está vinculado estrechamente con el protocolo SIP. Para esto se tomará en cuenta ciertos detalles importantes en la configuración.

Aquí se indicará la configuración basada en DNS SRV, DNS es una forma de configurar una dirección lógica para que pueda ser resuelta. Esto permite que las llamadas sean enviadas a diferentes lugares sin necesidad de cambiar la dirección lógica. Usando el DNS SRV se ganan las ventajas del DNS mientras que deshabilitándolo no es posible enrutar llamadas en base a nombre de dominios. Conviene tenerlo activado, por tanto se pone la directiva:

```
srvlookup=yes
```

Con esto Asterisk podrá resolver el controlador de protocolo SIP para un dominio a través de los registros DNS SRV y el servidor SIP confirmará que el URI SIP existe realmente en la central y enviará la solicitud. Esto hará que Asterisk se comporte de una manera más unificada.

sip_custom.conf

Al utilizar DUNDi, se marca el objetivo de anunciar sólo los usuarios registrados en la base de datos de nuestra central, se implantará la siguiente sentencia.

```
sipregistration=ext_local_SIP
```

Esta sentencia creará un contexto con nombre ext_local_SIP y creará una entrada de tipo Noop() por cada extensión que se registre esto servirá principalmente para anunciar en nuestra red DUNDi que ese usuario está registrado en la centralita y que por tanto puede gestionar la llamada. De la igual forma, cuando dicho usuario se desconecte de la central, se eliminará la presente entrada del contexto.

extensions.conf

Por último se configura el archivo extensions.conf, este contiene el plan de llamadas o Dialplan.

Para lograr la integración con la base de Datos en Realtime debemos crear el contexto "[internal]" que es el contexto que se usa para las extensiones.

Teniendo en cuenta que cuando un número no es encontrado en el plan de marcado local se usa el contexto [lookup_to_DUNDi], y la configuración debe ser exactamente la misma en los cuatro servidores:

En el archivo extensions.conf, añadimos los siguientes contextos:

```
[ext_DUNDi]
exten => _X.,1,Goto(ext_local_SIP,${EXTEN},1)
[context_internal]
include => lookup_to_DUNDi
include => ext_local_SIP
```

Aquí definimos los contextos personalizados para que DUNDI mapee nuestra extensiones, así como una macro para hacer las búsquedas en otros equipos (lo que evita loops) y la sentencia para redirigir las llamadas (switch).

```
[lookup_to_DUNDi]
switch => DUNDi/priv
[ext_local_SIP]
; Esta es la contexto que llamamos desde el contexto [lookup_to_DUNDi]
; Tambien evita que hayan loops en las consultas dundi.
;switch => Realtime/sipfriends
exten => _X.,1,Dial(SIP/${EXTEN})
exten => _X.,2,Hangup
```

Certificados de encriptación

DUNDi usa certificados de encriptación RSA para compartir los planes de marcado, además por que las respuestas a una consulta incluyen las claves de las troncales (aunque es dinámico).

Usaremos la misma clave para la comunicación entre todos los servidores, así que el primer paso es generar los certificados de encriptación uno de los equipos (en este ejemplo en SRV01):

```
# cd /var/lib/asterisk/keys
astgenkey -n SERVERS-DUNDI
```

Ahora necesitamos compartir los certificados entre los dos servidores; esto es para que cada uno pueda des-encriptar al otro.

Aplicar la configuración

Para que los cambios se hagan efectivos podemos ejecutar el comando:

```
# amportal restart
```

O

```
# Service asterisk restart
```

Ahora cada extensión que creemos en Asterisk con Realtime se añadirá al contexto [ext_SIP] el cual está incluido en extensions.conf que va a usar DUNDi para indicar que extensiones tenemos localmente.

Si nosotros tenemos la extensión responderemos con los datos para la comunicación hacia esa extensión; esos datos a su vez los interpreta el servidor que está preguntando y usa la función switch que pusimos en el archivo extensions.conf para comunicarse con la extensión local.

4.4 Pruebas del clúster de Alta Disponibilidad con DUNDi

Para probar la configuración establecida para el clúster virtual de alta disponibilidad se ha considerado a bien analizar el comportamiento del mismo ante tres sucesos diferentes que provocan la puesta en marcha de registros de extensiones en los diferentes nodos virtuales del clúster : apagado de un nodo activo, caída del servicio Asterisk y saturación de un nodo.

4.4.1 Escenario 1. Apagado del nodo activo

En este suceso, con el apagado del nodo activo en el que se encuentran actualmente registrado un grupo de extensiones en ejecución podemos simular algunas situaciones reales como la pérdida de

suministro eléctrico, daño físico en el servidor en el que tenemos alojado ciertos clientes o simplemente un apagado del sistema forzado por motivos fundados en operaciones de mantenimiento (para instalación o actualización de software adicional, reparar o sustituir algún elemento hardware del servidor, etc.).

A continuación se ve paso a paso como ha sido realizada esta prueba.

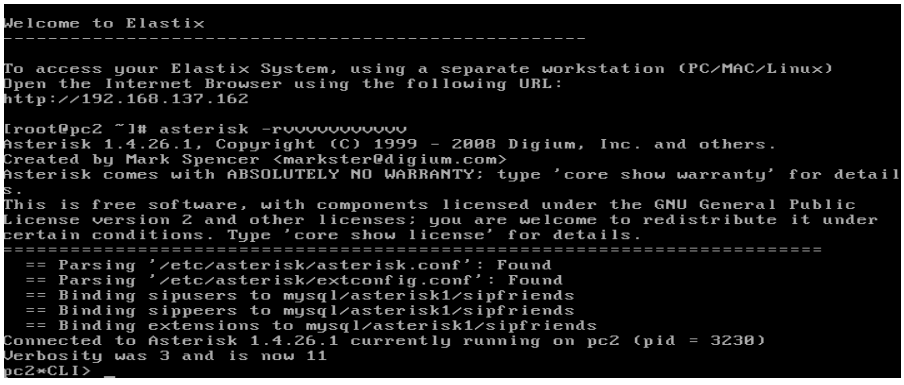
1. Puesta en marcha de los dominios o nodos. Ingresamos los datos del login,

2. Comprobamos que efectivamente el servicio Asterisk han sido iniciados de forma correcta en cada nodo.

   En el caso de la dirección IP lo hacemos ejecutando el comando **ifconfig** y observando que efectivamente el alias eth0:0 con la dirección 192.168.137.161 ha sido activada.

3. Ingresamos al modo CLI de Asterisk ejecutando la siguiente línea,

   Esto para entrar a la consola y si se quiere más detalle de lo que está pasando agreguenle v, mientras más v, mas verbosidad habrá.



4. Se procede a registrar los softphone en cada servidor, se ha utilizado X-Lite, a continuación se muestra el proceso de registro con el mencionado softphone.

Damos clic derecho sobre la pantalla, y presionamos configuración de cuentas SIP “SIP Account Settings” en ingles.

Figura IV-6: Softphone X-lite.

Ingresados los datos de la cuenta se registrará en la central a la cual le asigne el servicio DNS dada por el registro DNS SVR.

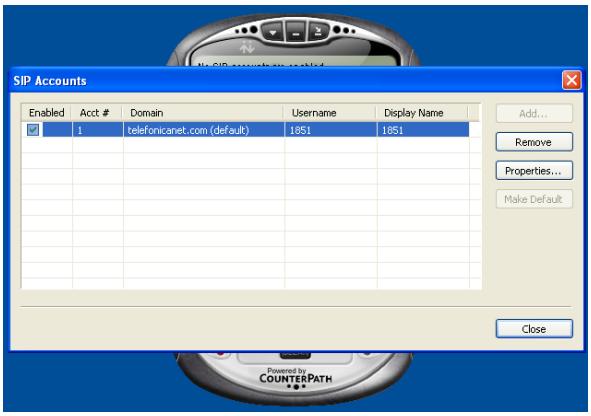


Figura IV-7: Registro de cuenta en el Softphone X-lite**.**

5. Transcurrido el tiempo del registro de extensiones en el presente nodo, se puede observar como se ha registrado.

Por medio de la consola nos damos cuenta que la extensión “1851” fue registrada en el nodo que tiene como **hostname** “*pc2*”.

```
    -- Registered SIP '1851' at 192.168.137.190 port 9032
    -- Added extension '1851' priority 1 to sipregistration
    -- Saved useragent "X-Lite release 1104o stamp 56125" for peer 1851
Really destroying SIP dialog 'NDNmMmU3NjhjZjBjYmVjNTRkNDViNDk3ZDBkZTQ3NDM.' Meth
od: REGISTER
    -- Remote UNIX connection
    -- Remote UNIX connection disconnected
```

Esto denota que se le fue asignada una extensión al nodo *pc2* del cluster VoIP.

6. Procedemos con el apagado del nodo activo (*pc2*) y posterior comprobación del traslado de los servicios. Para apagarlo simplemente ejecutamos el comando poweroff, simulando así las diferentes situaciones reales comentadas anteriormente.

```
    -- Registered SIP '1851' at 192.168.137.190 port 31108
    -- Added extension '1851' priority 1 to sipregistration
    -- Saved useragent "X-Lite release 1104o stamp 56125" for peer 1851
Really destroying SIP dialog 'OGRjMjUwZjczNzYxNmYyNTVhYWJjZDg0YWVjZmIxNjI.' Meth
od: REGISTER
```

Al ejecutar el apagado del nodo *pc2* reconoce que éste ha dejado de estar disponible (fallo de uno de los nodos del clúster) y automáticamente los servicies DNS asignan una nueva dirección IP a esa terminal para que la misma vuelva a registrarse después de un *Reboot*.

Se puede decir entonces que la tecnología DUNDi a este punto tiene deficiencia al no poder establecer la comunicación entre las terminales después de apagar un nodo del cluster, a menos que se conecte y desconecte los softphone o en el caso de los teléfonos IP se los reinicie.

A continuación el tiempo de asignación de la nueva IP.

Tabla IV.XIV : Tiempo de Asignación de una nueva dirección IP.

Prueba #	Tiempo(seg)
1	97,63
2	84,9
3	84,03
4	86,12
5	88,72
6	84,35
7	84,93
8	85,49
9	87,51
10	84,75
11	88,88
12	82,17
Promedio	86,62

La siguiente figura nos muestra de forma grafica el tiempo que demora en ser asignada una nueva IP a una terminal después de apagar el nodo activo, se tomo datos de diferentes pruebas.

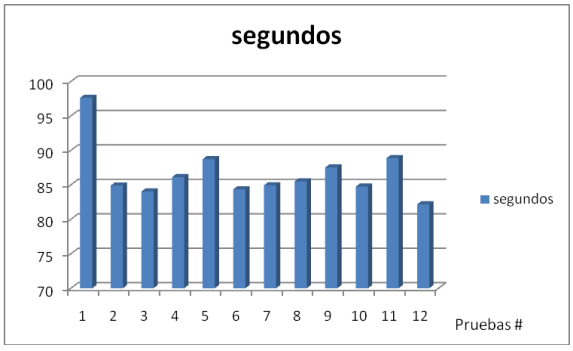


Figura IV-8: Grafico de la Tabla IV.XIV **.**

4.4.2 Escenario 2. Caída del servicio

En esta segunda prueba vamos a provocar la caída del servicio Asterisk y observar cómo reacciona el sistema de red ante este evento dependiendo. El inicio de la prueba es exactamente igual que en el caso anterior, poniendo en marcha los dos nodos pc1 y pc2 que forman el cluster VoIP. De igual manera, el grupo de extensiones son registradas e iniciadas con éxito.

Con la deficiencia de volver a registrar manualmente las extensiones en los softphone y en el caso de los teléfonos IP conectar y desconectar el cable de red o un *Reboot* que permite la comunicación en cada punto.

Tabla IV.XV : Tiempo de Asignación de una nueva dirección IP.

Prueba #	Tiempo(seg)
1	86,4
2	79,9
3	81,56
4	78,23
5	85,05
6	75,45
7	80,43
8	78,69
9	80,58
10	82,28
11	89,24
12	77,39
Promedio	**81,27**

La siguiente figura nos muestra de forma grafica el tiempo que demora en ser asignada una nueva IP a una terminal después de la caída del servicio, se tomo datos de diferentes pruebas y se tiene un tiempo de 81,27 segundos para asignar un nuevo nodo a la terminal.

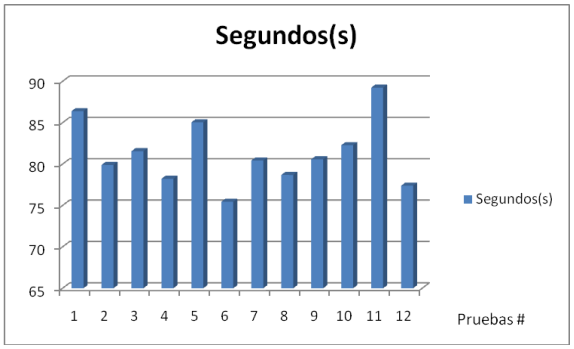


Figura IV-9: Gráfico de la Tabla IV.XV **.**

4.4.3 Interpretación del Escenario 1 y 2

Después de las pruebas realizadas se puede decir que la tecnología DUNDi, tiene dificultad al momento de la autentificación después de la caída del servicio en alguno de los nodos del cluster, esto dificulta la disponibilidad del servicio, es por eso que a continuación se muestra un nuevo modelo donde se utilizará otra técnica como es Heartbeat para solventar las deficiencia que nos da DUNDi.

MODELO HEARTBEAT

4.5 ESQUEMA GENERAL

Después de haber desarrollado diversos conceptos que serán necesarios para el modelo a diseñar, necesitamos conocer qué componentes tiene este modelo.

4.5.1 Componentes

- **Terminales**

  Este componente es el encargado de representar a los clientes que en este caso serán los softphone o teléfonos IP.

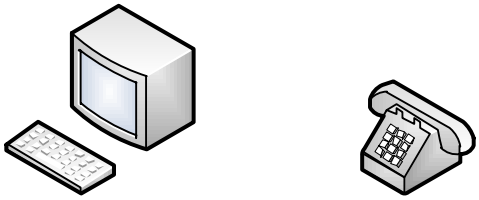


Figura IV-10: Terminales (Softphone y Teléfonos IP) **.**

- **Servidores DNS y DHCP**

  El primer componente será el encargado de resolver el servidor que tenga el rol principal y el segundo componente será el encargado de asignar una dirección IP a los terminales.

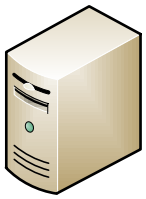


Figura IV-11: Servidor DNS **.**

- **Centrales telefónicas Asterisk**

  Este componente será el encargado de representar a los servidores reales, es decir, a los Servidores donde se encuentran las centrales telefónicas.

Figura IV-12: Servidor Asterisk **.**

- **Red Ethernet**

  El siguiente componente será el encargado de representar el tipo de enlace y/o tecnología de red a utilizar, es decir, Ethernet.

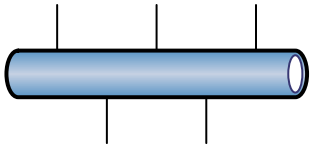


Figura IV-13: Red Ethernet **.**

4.5.2 Diseño de la Arquitectura del Clúster.

La arquitectura del clúster propuesta, es una arquitectura de dos capas, las cuales separaran a los servidor DNS, servidor DHCP y servidores Asterisk , brindando alta disponibilidad. Estas capas son:

Capa 1: Servidores DNS Y DHCP

La primera capa es la destinada a los servidores DNS y DHCP. En esta capa habrá dos servidores brindando el mismo servicio en distinto tiempo, dependiendo del rol que tenga, es decir si el servidor máster tiene algún fallo inmediatamente el servidor esclavo toma el control.

Básicamente esta capa se encarga de mostrar al clúster como una sola maquina al resto de terminales.

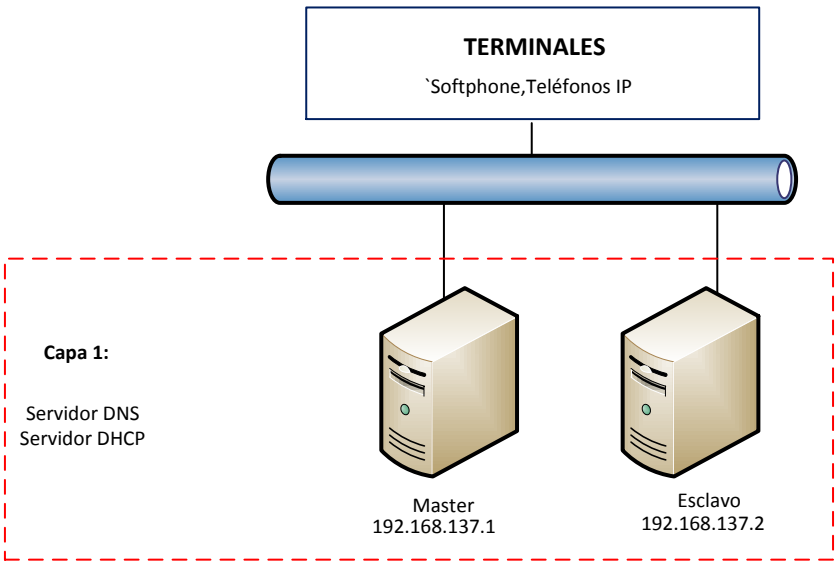


Figura IV-14: Capa 1 (Modelo Heartbeat) **.**

Capa 2: Servidores Asterisk

La segunda capa es la destinada a los servidores Asterisk. En esta capa se utilizará una configuración Activa / Pasiva. Esto brindará alta disponibilidad. Aquí tendremos dos Servidores Asterisk, en los cuales uno será el principal o activo y el segundo será el secundario o pasivo. En el servidor activo (o principal) es al cual se accederá.

El servidor pasivo (o de respaldo) replicará todos los datos del servidor principal. Cuando el servidor principal falle, el servidor de respaldo tomará el control, siendo totalmente transparente para los terminales. Cuando el servidor principal se recupere, este sincronizará sus datos con el servidor que se ha vuelto el activo.

En cuanto a la replicación de los datos, para mantener los datos sincronizados de los servidores principal a los secundarios, se hará uso de DRBD que se adapta al modelo de clúster Activo / Pasivo.

Como sabemos, DRBD es un dispositivo de bloque para almacenamiento replicado, donde el servidor Activo y/o principal será en el cual se pueden escribir los datos, y en el Servidor Pasivo o Secundario se replicarán todos los datos escritos en el principal. La replicación se da por cada recurso de DRBD. Este modelo servirá tanto para estos Servidores, los cuales podrán tener varios recursos de DRBD almacenando diferentes tipos de datos.

Pero, para que el servidor de respaldo pueda tomar el control cuando ocurra un fallo en el servidor principal, necesitamos de Heartbeat. Aquí, Heartbeat se encargará de monitorear ambos servidores para detectar fallos y así poder pasar el control del Servidor Activo al Servidor de Respaldo cuando ocurra un fallo. Heartbeat también se encargará de ejecutar DRBD, Asterisk y demás servicios según corresponda, en el servidor que asume el control.

Un esquema de esta capa lo podemos ver a continuación:

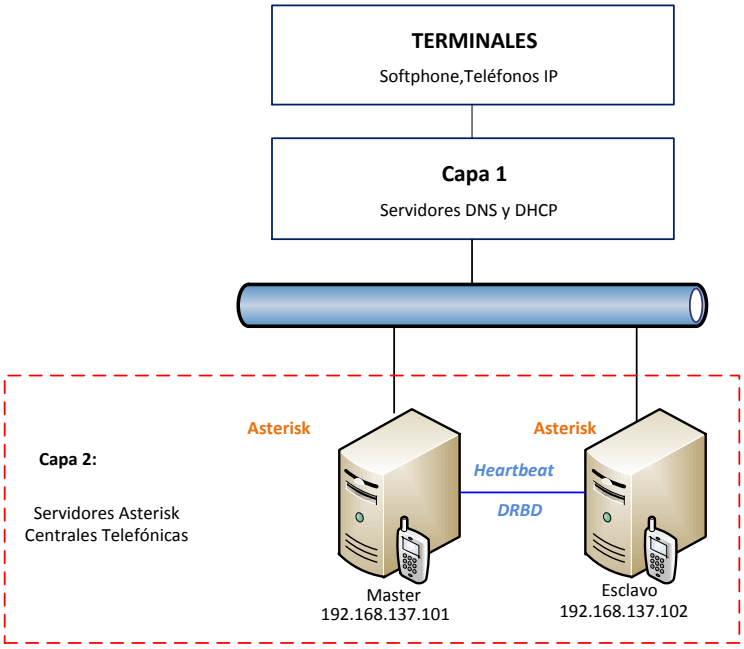


Figura IV-15: Capa 2 (Modelo Heartbeat) **.**

Pero la replicación de datos, al ser por medio de la red, puede crear un gran tráfico en la red y esto podría aumentar el consumo de ancho de banda, lo cual causaría que haya mucha latencia. Esto afectará el correcto funcionamiento de la red y de los demás servicios que se encuentran trabajando, como la transferencia de archivos.

Para solucionar esto, es necesario conectar directamente tanto ambos Servidores. Es decir, se tiene que hacer un enlace punto a punto entre los Servidores Asterisk. Esta solución hará posible que la replicación de datos se haga solo entre esos dos servidores y no utilice el ancho de banda de toda la red, sino utilizará el enlace punto a punto por el cual están conectados. Esto requerirá de una tarjeta de red adicional.

En realidad no es necesario tener un grupo separado de servidores. Es decir, podríamos brindar ambos servicios, de archivos y Asterisk, en el mismo par de servidores. Esto es posible si el hardware en el que se implementan es muy potente y puede resistir toda esa carga, pero es recomendable tener servidores separados para brindar cada servicio.

Por motivos demostrativos se utilizará este modelo, donde solo un par de servidores brindará ambos servicios, el Servidor de Archivos y Asterisk. Aquí, cada servicio utilizará un recurso de DRBD. Es decir, NFS utilizará un recurso de DRBD y Asterisk utilizará otro recurso de DRBD, que pueden ser tanto una partición en el disco duro, como otro disco duro.

Esquema

Ahora que ya hemos visto todas las capas del modelo, tenemos que ver cómo es que todos los servidores se comunican, para ser totalmente transparentes para los clientes. Es decir, debemos saber cómo es que cada grupo de servidores se van a identificar en la red y para que cada grupo aparezca ser como un solo servidor frente a los clientes.

Para hacer posible que los clientes vean a todo el modelo como si fuese un solo servidor, se hace necesaria la utilización de IPs Virtuales (VIPs). Aquí, solo se necesitarán una VIP por todo el conjunto de servidores de las Capas 1 y 2.

Aquí, cada servidor tendrá una dirección IP propia, que deberán estar en la misma subred. En las capas 1 y 2, es decir en los balanceadores y los servidores reales, se compartirá una IP Virtual. A esta IP la llamamos la VIP.

En la capa de almacenamiento, también cada servidor de archivos tendrá su propia dirección IP, pero a su vez. Esto lo podemos apreciar en la siguiente imagen:

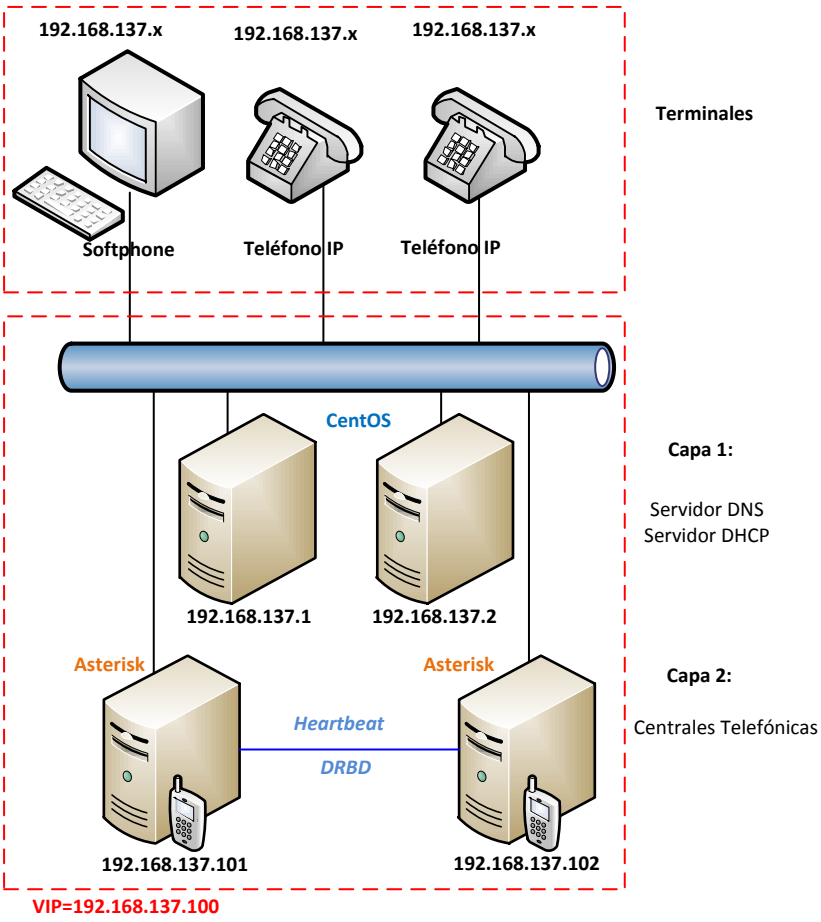


Figura IV-16: Esquema (Modelo Heartbeat) **.**

Esto hace posible que el clúster sea visto como un único nodo por cada cliente de tal forma que solo se pueda acceder, por medio de la VIP, al servicio que implementa el clúster.

Es decir, aquí los clientes ingresarán a la central por un nombre de dominio, que resolverá el servidor DNS cada vez que el nombre de dominio sea solicitado, como por ejemplo, el dominio

www.telefonicanet.com puede resolver la IP de la central con rol principal por ejemplo 192.168.137.101 ó 192.168.137.102

4.5.3 Estimación de Costos de la Red

La información necesaria para elaborar las tablas con la estimación de costos fueron obtenidas casi en su totalidad de la empresa TELET de la ciudad de Ambato, debido a la facilidad que este medio proporciona para acceder a los productos que, cumpliendo con las características requeridas, satisfagan las diferentes necesidades de los usuarios, quienes pueden decidir de esta gama de productos, considerando la funcionalidad del equipo y el precio.

Los principales elementos a considerar en la estimación de costos son:

- Compra de equipo
- Instalación
- Calibración y puesta en marcha

Costos De Equipos Y Accesorios

De acuerdo al sistema de red establecido para el sistema de telefonía IP y de sus requerimientos se dimensionan los siguientes equipos y sus características que posee el servidor para garantizar un buen servicio, para llevar a cabo la implementación.

Tabla IV.XVI : Costo de Equipos y Accesorios.

CANTIDAD	DESCRIPCION	PRECIO UNITARIO(USD)	PRECIO TOTAL(USD)
3	PC'S INTEL CORE I3	650	1950
1	GATEWAY GRANDSTREAM	290	290
1	SWITCH TP-LINK 8 PUERTOS	100	100
4	CONVERTIDOR ATA'S GRANDSTREAM	85	340
12	PATCH CORD	5	60
2	TARJETA INTERFACES FXO	850	1700
6	TELEFONOS PANASONIC	16	96
		SUBTOTAL	**4536**

Costo de Instalación

Para justificar el precio de configuración asignado en la proforma, se realiza el desglose de los costos asociados a la implementación del sistema de telefonía IP.

Tabla IV.XVII : Costos de Instalación.

CANTIDAD	DESCRIPCION	PRECIO UNITARIO(USD)	PRECIO TOTAL(USD)
1	CONFIGURACION SERVIDOR CENTOS	200	200
1	CONFIGURACION SERVIDOR ASTERISK	500	500
1	CONFIGURACION GATEWAY GRANDSTREAM	50	50
4	CONFIGURACION ATA'S GRANDSTREAM	25	100
		SUBTOTAL	**850**

Costo Total Del Proyecto

La Tabla presenta el costo total para la futura implementación, este costo es un precio referencial que puede variar, pero muestra una idea del capital que se necesita.

Tabla IV.XVIII : Costo total del Proyecto.

DESCRIPCION	**PRECIO TOTAL(USD)**
Equipos	4536
Instalación, calibración y puesta en marcha	850
SUBTOTAL	**5386**

Como resultado se obtiene el costo total de 5.386 dólares, para llevar a cabo la implementación del prototipo de telefonía IP presentado para la empresa descrita en el Capítulo I.

CAPITULO V

V. EVALUACION DEL MODELO DE ALTA DISPONIBILIDAD.

5.1 Evaluando: Centrales Telefónicas

5.1.1 Escenario 1: Apagando Normalmente la Central con rol principal

Esta prueba consistió en apagar y/o reiniciar normalmente el servidor que está teniendo un rol principal dentro de la Capa 2. Aquí, al apagar el servidor maestro, el servidor secundario tendrá que entrar en acción y volverse el nuevo principal, tomando el control del servicio.

En esta prueba, se tomó el tiempo, en segundos, que el servidor de respaldo demoró en tomar el control total del servicio. Esta prueba nos sirvió para evaluar el nivel de disponibilidad del servicio en la Capa 2.

El resultado de las pruebas se encuentra a continuación:

Tabla V.XIX : Tiempo Escenario 1.

Prueba #	Resultado
1	46,97
2	51,93
3	47,36
4	48,16
5	50,23
6	48,63
7	49,56
8	51,25
9	49,85
10	47,32
11	46,78
12	50,82
Promedio	48,75

La siguiente figura nos muestra de forma grafica el tiempo que demora en tomar el control el servidor esclavo o secundario y lo hace en un tiempo promedio de 48,75 segundos.

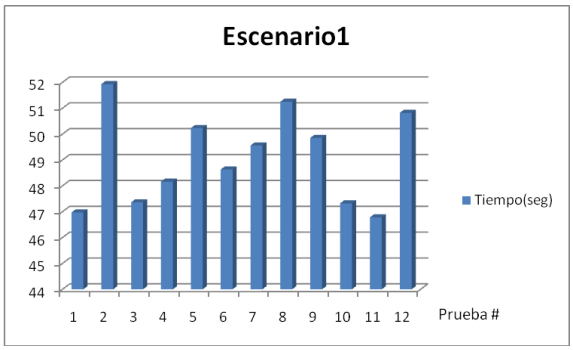


Figura V-17: Gráfico Tabla V.XIX**.**

Tomando el control Normalmente el servidor maestro.

Tabla V.XX : Tiempo de toma de control por el servidor principal.

Prueba #	Resultado
1	59,37
2	49,09
3	47,93
4	50,45
5	53,56
6	48,95
7	49,46
8	50,45
9	52,23
10	49,43
11	48,12
12	50,04
Promedio	50,75

La siguiente figura nos muestra de forma grafica el tiempo que demora en tomar el control nuevamente el servidor principal y lo hace en un tiempo promedio de 50,75 segundos.

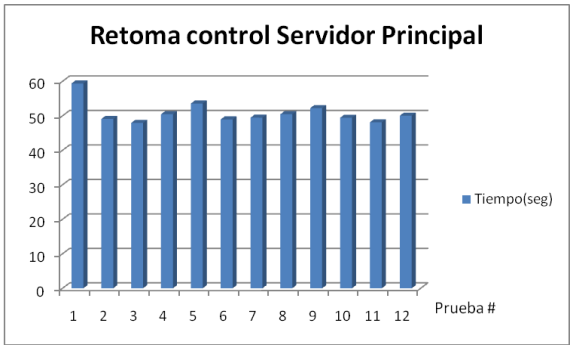


Figura V-18: Gráfico Tabla V.XX**.**

Tiempo de autenticación de los terminales al servidor

Tabla V.XXI : Tiempo de autentificación de las Terminales.

Prueba #	Resultado
1	38,26
2	35,81
3	36,1
4	35,67
5	35,16
6	35,4
7	35,47
8	35,04
9	35,28
10	35,32
11	40,76
12	32,13
Promedio	35,87

La siguiente figura nos muestra de forma grafica el tiempo que demora en autentificarse las terminales y lo hace en un tiempo promedio de 35,87 segundos.

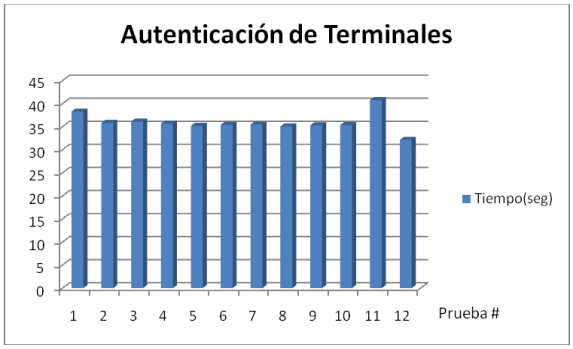


Figura V-19: Gráfico Tabla V.XXI**.**

5.1.2 Escenario 2: Fallas en el Servidor Principal

Esta prueba consistió en simular que el servidor principal ha sufrido alguna falla, que puede haber sido tanto en software como hardware, y/o se hayan apagado o reiniciado abruptamente.
Aquí también se midió el tiempo, en segundos, que el servidor de respaldo tardó en tomar el control total del servicio.

El resultado de las pruebas se muestra a continuación:

Tabla V.XXII : Tiempo de toma de control por el servidor pasivo.

Prueba #	Resultado
1	50,97
2	51,93
3	53,36
4	50,16
5	50,23
6	48,63
7	49,56
8	51,25
9	49,85
10	47,32
11	46,78
12	49,25
Promedio	51,13

La siguiente figura nos muestra de forma grafica el tiempo que demora tomar el control el servidor pasivo o secundario al momento de que ocurra algún fallo como puede ser el corte de suministro eléctrico u otro y lo hace en un tiempo promedio de 51,13 segundos.

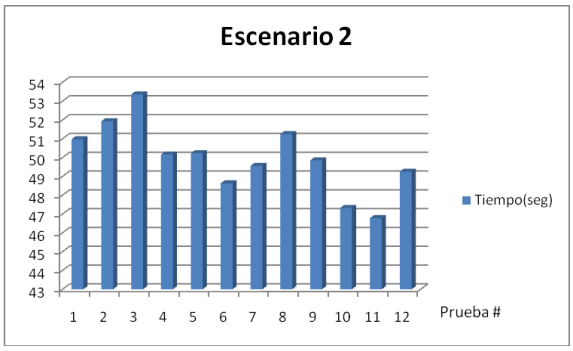


Figura V-20: Gráfico Tabla V.XXII**.**

5.1.3 Escenario 3: Fallas en la Red o Tarjeta de Red

Esta prueba consistió en simular que el segmento de red y/o tarjeta de red del servidor principal han sufrido alguna falla por lo cual el servidor secundario tuvo que tomar el control de los recursos. Como en las pruebas anteriores, también se midió el tiempo, en segundos, que el servidor de respaldo tardó en tomar el control total del servicio.

El tiempo es el cual el servidor de respaldo se demoró en tomar el control del servicio, una vez que la red y/o tarjeta de red del servidor principal falló.

El resultado de esta prueba se ve a continuación:

Tabla V.XXIII : Tiempo de toma de control por el servidor pasivo ante falla en la red.

Prueba #	Resultado
1	48,14
2	44,09
3	45,46
4	42,56
5	49,89
6	40,05
7	44,96
8	43,65
9	45,30
10	46,96
11	48,48
12	45,26
Promedio	45,40

La siguiente figura nos muestra de forma grafica el tiempo que demora tomar el control el servidor pasivo o secundario al momento de que ocurra algún fallo en la tarjeta de red y lo hace en un tiempo promedio de 45,40 segundos.

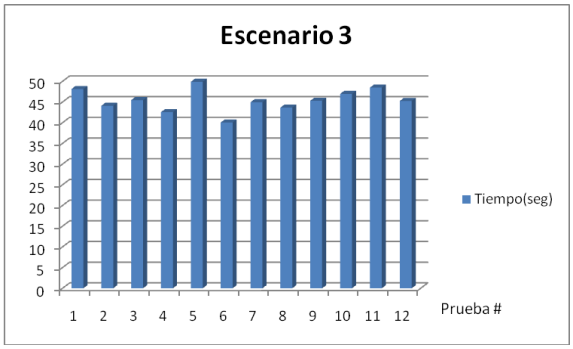


Figura V-21: Gráfico Tabla V.XXIII**.**

Interpretación de Resultados de la Capa 2

Gracias a los resultados del Escenario 1 (Tabla V.XIX), se pudo determinar que cuando se apaga y/o reinicia el servidor principal, se tiene un promedio de 48,75 segundos en el que el servidor esclavo de respaldo se demora en detectar la caída del servidor principal, y en tomar el control del servicio.

De acuerdo a los resultados de la (Tabla V.XX), se pudo determinar que cuando el servidor principal toma nuevamente el control lo hace en un promedio de 50,75 segundos.

De acuerdo a los resultados de la (Tabla V.XXI), se pudo determinar que cuando las terminales se registran, se tiene un promedio de 35,87 segundos en que tarda en registrarse en el servidor que toma el control en un momento determinado.

Gracias a los resultados del Escenario 2 (Tabla V.XXII), se pudo determinar que cuando hay una falla en el servidor principal que cause el apagado o reiniciado abrupto de este, se tiene un promedio de 51,13 segundos en el cual el servidor de respaldo se demora en tomar el control del servicio.

Gracias a los resultados del Escenario 3 (Tabla V.XXIII), con el Tiempo 1 se pudo determinar que cuando hay una falla de red y/o en la tarjeta de red del servidor principal, que cause su exclusión de la red momentáneamente, se tiene un promedio de 45,40 segundos en el cual el servidor de respaldo se demora en tomar el control del servicio.

Todas estas pruebas validan al indicador de "Tiempo de demora de la toma del control del servicio por otros Servidores del Clúster". Evaluando los tiempos promedio, y según la Tabla de disponibilidad de un servicio, se puede determinar que la Capa 1, de servidores Asterisk, del modelo se encuentran en una Alta Disponibilidad aproximada al 99.999%. Pero, cabe resaltar que estos resultados fueron obtenidos sin tener tráfico de red de peticiones de los clientes, es decir, no habían peticiones por el servicio. También podemos deducir que esta capa es tolerante a fallos, ya

que se elimina el punto único de fallos teniendo un servidor de respaldo que, con diferentes pruebas, demostró que toma el control del servicio en caso que el servidor principal falle.

5.1.4 Escenario 4: Detectando las fallas de los Servidores DNS (Capa 2)

Este Escenario consistió en simular que el servidor DNS sufrió alguna falla, que pueden haber estado relacionadas tanto a hardware como software, y que hayan causado que el servidor se apaguen o reinicien de manera abrupta.

En esta prueba se mide el tiempo en que el servidor de Asterisk activo se demoró en detectar la caída de el servidor DNS mas el tiempo en que el servidor DNS estaba activo nuevamente.

Los resultados los tenemos a continuación:

Tabla V.XXIV : Tiempo de demora del servidor DNS cuando ocurre un fallo

Prueba #	Tiempo(seg)
1	1,81
2	1,87
3	1,79
4	1,78
5	1,78
6	1,86
7	1,79
8	1,82
9	1,83
10	1,84
11	1,81
12	1,80
Promedio	1,82

La siguiente figura nos muestra de forma grafica el tiempo que demora cuando el servidor DNS presenta algún fallo y lo hace en un tiempo promedio de 1,82 segundos.

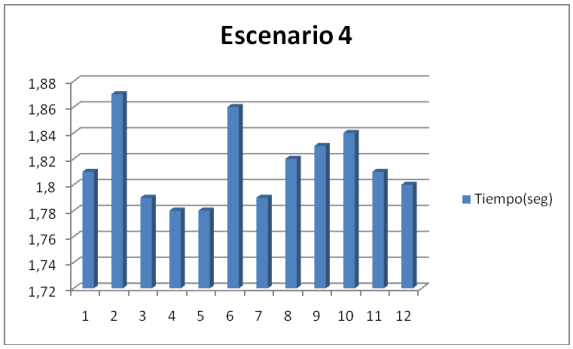


Figura V-22: Gráfico Tabla V.XXIV**.**

Interpretación de Resultados de la interacción de las Capas 1 y 2

Gracias a la Prueba 4 (Tabla V.XXIV), pudimos determinar que el tiempo que se demoró en detectar la falla de alguno de los Servidor DNS de la Capa 1 mas el tiempo que el Servidor DNS demoró en estar disponible para brindar el servicio, una vez que ha sido inicializado nuevamente. este tiempo fue un promedio de 1,82 segundos, Cabe resaltar que este tiempo puede variar según la cantidad de servicios que inicializan cada tipo de servidor. Este tiempo valida al indicador "Tiempo de recuperación del servicio al ocurrir fallas en los Servidores."

Resumen de los Escenarios de Pruebas

A continuación una tabla resumida con los datos de los diferentes escenarios de pruebas.

Tabla V.XXV : Tabla resumida de Escenarios de Pruebas.

	Escenario			
	1	2	3	4
Prueba #	Tiempo(seg)	Tiempo(seg)	Tiempo(seg)	Tiempo(seg)
1	46,97	50,97	48,14	1,81
2	51,93	51,93	44,09	1,87
3	47,36	53,36	45,46	1,79
4	48,16	50,16	42,56	1,78
5	50,23	50,23	49,89	1,78
6	48,63	48,63	40,05	1,86
7	49,56	49,56	44,96	1,79
8	51,25	51,25	43,65	1,82
9	49,85	49,85	45,30	1,83
10	47,32	47,32	46,96	1,84
11	46,78	46,78	48,48	1,81
12	50,82	49,25	45,26	1,80
Promedio	**48,75**	**51,13**	**45,40**	**1,82**

Interpretación de Resultados

Podemos deducir el modelo Heartbeat es tolerante a fallos, ya que se elimina el punto único de fallos teniendo un servidor de respaldo que, con diferentes pruebas, demostró que toma el control del servicio en caso que el servidor principal falle.

En la tabla anterior se puede observar los tiempos que demora en cada uno de los Escenarios de prueba, es así que en el Escenario 1 se tiene un tiempo de 48,75 segundos que demora hasta que el servidor secundario tome el control, el Escenario 2 se tiene un tiempo de 51,13 segundos que demora hasta que el servidor secundario tome el control, el Escenario 3 se tiene un tiempo de 45,40

segundos que demora hasta que el servidor secundario tome el control y en el Escenario 4 se tiene un tiempo de 1.83 segundos que demora el servidor Asterisk en reconocer y restablecer la conexión cuando uno de los servidores DNS a caído.

5.2 Comprobación de la hipótesis de la investigación realizada.

5.2.1 Planteamiento de la Hipótesis

"La implementación de una red de alta disponibilidad para centrales Asterisk basada en la tecnología DUNDi permitirá dotar de alta disponibilidad al sistema de Telefonía IP ".

El término "disponibilidad" hace referencia a la probabilidad de que un servicio funcione adecuadamente en cualquier momento.
En este punto se ve necesario definir a que se considera alta disponibilidad en el presente trabajo de tesis.

5.2.2 Alta Disponibilidad

La alta disponibilidad consiste en una serie de medidas tendientes a garantizar la disponibilidad del servicio, asegurando que el servicio funcione durante las veinticuatro horas.
Es decir la alta disponibilidad se considera a la capacidad de ofrecer un servicio cuando el servidor que lo ofrece deja de funcionar.

Cuando un servidor deja de funcionar el servicio se deja de ofrecer, pero la alta disponibilidad se refiere a que por más de que este servidor deje de funcionar, el servicio se siga ofreciendo, ya que otro servidor puede tomar el control del servicio que se ofrece.

Según José Ángel de Bustos Pérez [10]: La alta disponibilidad es ofrecida por todos los Clústeres que posean lo siguiente:

- Correcta configuración del clúster.
- Redundancia de Hardware, que implica la red, almacenamiento, fuentes de alimentación.
- Redundancia del Sistema Eléctrico.

La disponibilidad se expresa con mayor frecuencia a través del índice de disponibilidad (un porcentaje) que se mide dividiendo el tiempo durante el cual el servicio está disponible por el tiempo total. Según José Angel de Bustos Pérez nos dice que la disponibilidad se clasifica de acuerdo a la regla de los 9's.

Tabla V.XXVI : Tabla de disponibilidad

Disponibilidad	
Disponibilidad del Servicio	**Tiempo de caída**
99%	3,7 días
99,9%	8,8 horas
99,99%	52,7 minutos
99,999%	5,3 minutos
99,9999%	31,5 segundos

[10] *Extraído de, utilizacion y administracion avanzadas de sistemas gnu/linux y aplicaciones de software libre para estudiantes universitarios. clustering y alta disponibilidad en gnu/linux. http://www.ibiblio.org/pub/linux/docs/LuCaS/Manuales-LuCAS/doc-curso-salamanca-clustering/html/clustering-ha.html*

Fundamentada en la tabla anterior, se considera para evaluar que la red tenga Alta disponibilidad en el presente trabajo de tesis, los valores porcentuales de disponibilidad a partir del 99,99%. Es decir solo aquellos valores en tiempo que se encuentren con una disponibilidad de Servicio a partir del 99,99% o más será considerado como alta disponibilidad.

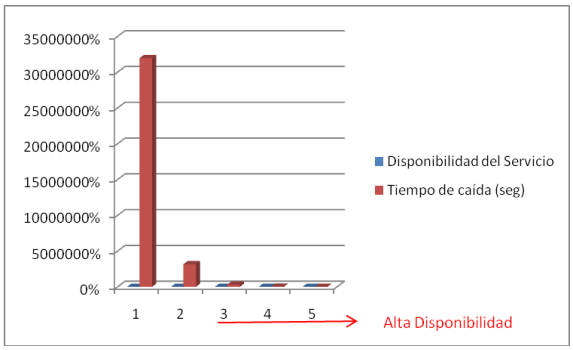


Figura V-23: Gráfico Tabla V.XXVI**.**

5.2.3 Evaluación Indicadores

Para la comprobación de la hipótesis se evalúan los siguientes indicadores tanto para DUNDi como para Heartbeat.

Tabla V.XXVII : Tabla de Indicadores

Siglas	Descripción
TD	Tiempo de demora de la toma del control del servicio por otros Servidores del Clúster
TP	Tiempo de pérdida del servicio al ocurrir fallas en los Servidores
TR	Tiempo de demora de registro de las terminales

5.2.4 Ponderación para Indicadores

Para cada rango de tiempo se asigna un valor cuantitativo, la suma de estos en cada uno de los indicadores tanto para DUNDi como para Heartbeat nos ayudará a determinar cuál tiene mayor peso. De esta manera se aceptara la hipótesis o se negará la hipótesis.

Tabla V.XXVIII : Tabla de Indicadores

Ponderación		
Tiempo	**Porcentaje (%)**	**Cuantitativa**
(0-20)seg	>=80 y < =100	5
(21-40)seg	>=60 y < 80	4
(41-60)seg	>=40 y < 60	3
(61-80)seg	>=20 y < 40	2
(81-100) seg	< 20	1
No Aplica	0	0

5.2.5 Valoración de la disponibilidad en los modelos de DUNDi y Heartbeat

Con los resultados obtenidos de las pruebas realizadas tanto para DUNDi como para Heartbeat se procede a valorar cuantitativamente de acuerdo a la Tabla V.XXVIII a cada uno de los indicadores.

El mayor resultado que se obtenga de la suma de los indicadores muestra cual es el modelo que tiene alta disponibilidad.

Tabla V.XXIX : Disponibilidad en DUNDi vs Heartbeat

	DISPONIBILIDAD					
	DUNDi			Heartbeat		
Pruebas #	**TD**	**TP**	**TR**	**TD**	**TP**	**TR**
1	1	5	0	3	5	4
2	1	5	0	3	5	4
3	1	5	0	3	5	4
4	1	5	0	3	5	4
5	1	5	0	3	5	4
6	1	5	0	3	5	4
7	1	5	0	3	5	4
8	1	5	0	3	5	4
9	1	5	0	3	5	4
10	1	5	0	3	5	4
11	1	5	0	3	5	4
12	1	5	0	3	5	4
Total	12	60	0	36	60	48
Suma Total	**62**			**144**		

5.2.6 Decisión

Se concluye que se rechaza la hipótesis ya que no se puede medir uno de los indicadores y por lo tanto el resultado en DUNDi que es 62 es bastante inferior al de Heartbeat que es 144 por lo cual se deduce que no se puede obtener alta disponibilidad con DUNDi.

5.2.7 Comprobación de alta disponibilidad con Heartbeat

Al demostrar que Heartbeat es la mejor opción para diseñar una red de alta disponibilidad para centrales Asterisk, es necesario comprobar si se encuentra en el rango de alta disponibilidad de la Tabla V.XXVI de disponibilidad.

A continuación se muestra el promedio de cada escenario de pruebas realizadas para Heartbeat con su equivalente porcentual en disponibilidad

Tabla V.XXX : Tabla resumida de Escenarios con la Disponibilidad.

Escenario	Promedio	Disponibilidad (%)
1	48,75	99,999
2	51,13	99,999
3	45,4	99,999
4	1,82	99,9999
PROMEDIO	36,775	**99,999**

Evaluando los tiempos promedio, y según la Tabla V.XXVI de disponibilidad de un servicio. se puede determinar que los servidores Asterisk, del modelo Heartbeat se encuentran en una Alta Disponibilidad aproximada al 99.999%.

Podemos decir que la mejor opción y la mejor adaptable para una red de alta disponibilidad es el modelo de Heartbeat, ya que además de las ventajas que tiene sobre el modelo de DUNDi este también puede ser adaptable a otras tecnologías de almacenamiento y de Base de Datos.

CONCLUSIONES

Se ha demostrado que al implementar un sistema para telefonía IP tolerante a fallos con DUNDi no se obtiene alta disponibilidad ya que al ocurrir algún fallo en el servidor que se encuentra proporcionando el servicio, las terminales no logran registrarse automáticamente, sino que se necesita reiniciar las terminales para que estas reconozcan al nuevo servidor que se les fue asignado para establecer la comunicación.

Con DUNDi cada uno de los nodos que se encuentra conectados entre si propagan la información del estado de cada una de las extensiones, esto ayuda a la comunicación entre los nodos que forman parte de la estructura del clúster VoIP.

Asterisk permite integrar dispositivos de distintas marcas y precios como CISCO y Grandstream, convertidores ATA, Gateway, softphones entre ellos X-lite y Zoiper, entre otros, esto gracias a la arquitectura de Asterisk.

De acuerdo al estudio realizado acerca de las técnicas de alta disponibilidad en redes VoIP, Heartbeat es la mejor herramienta para dar alta disponibilidad a un servicio, en este caso Asterisk; ya que siendo un software libre se adapta a las necesidades del cliente y proporciona un clúster evitando en lo más mínimo la pérdida del servicio de telefonía. Esto se ve reflejado en la utilización de un servidor de respaldo que entrará en acción cuando ocurra alguna falla en el servidor principal, tomando el control del servicio.

Con Heartbeat, la adquisición de la IP se produce en menos de un segundo. DRBD se re-configura en casi 35 segundos y luego dependiendo de la plataforma de hardware y la complejidad de las aplicaciones que se ejecuten en Asterisk puede tardar entre 10-15 segundos para que Asterisk se ponga en marcha en el servidor secundario, se sincronizan los archivos de configuración y está listo para procesar las llamadas en un promedio de 48,75 segundos .

El modelo implementado en un Ambiente de Prueba haciendo uso de DRBD junto con Heartbeat optimiza en un 99.999% la disponibilidad de la solución; puesto que se crea una partición virtual la misma que será compartida entre los servidores que se realice el clustering.

RECOMENDACIONES

Es recomendable tener un modelo de red de alta disponibilidad donde adaptar el modelo propuesto. Así, al contar con una red de alta disponibilidad, se asegura también que el servicio esté siempre disponible cuando ocurran fallas en los diversos segmentos de la red, donde se encuentre implementado el modelo.

Se recomienda utilizar enlaces Ethernet punto a punto entre los Servidores Asterisk, para que la replicación de datos se realice por medio de este enlace. Así, nos aseguramos de separar el tráfico de red producido por el acceso a los datos, del tráfico producido por la replicación de datos. Además, al ser un enlace dedicado, se evitan las colisiones de los paquetes al momento de hacer la replicación de los datos, en este caso se utilicen hubs en vez de switches. También nos aseguramos que los servidores se monitoreen entre ellos por medio del enlace punto a punto y no por medio de la red, lo cual podría generar mayor tráfico. Gracias a esto, los servidores se seguirán monitoreando aún si ocurre alguna falla de red.

La utilización de múltiples tarjetas de red, le permitirá a los servidores adaptarse a diferentes modelos de red de alta disponibilidad, entre ellas, las redes con enlaces redundantes. Esto también incluye la utilización de enlaces eléctricos de respaldo. Este modelo es motivo de una próxima investigación.

RESUMEN

El presente documento tiene como objetivo el análisis y diseño de una red de alta disponibilidad para centrales Asterisk basada en la tecnología DUNDi que será desarrollada en los Laboratorios de la Academia CISCO de la Escuela Superior Politécnica de Chimborazo.

La investigación se realizó con el método deductivo con el cual se estudio las técnicas de alta disponibilidad en redes VoIP y se propuso una solución que consiste en un modelo activo / pasivo basado en Heartbeat como la mejor opción para mantener servicios de alta disponibilidad, este modelo hace uso de un Servidor Maestro y un Servidor Esclavo que forman la Capa 2, un Servidor DNS y DHCP que se encuentran en la Capa 1 y los terminales que son Teléfonos IP, convertidores ATA Grandstream y softphones; todos estos equipos se encuentran en una red Ethenet mediante cables UTP cat 5e con conectores RJ45.

Los resultados muestran que existe un tiempo promedio de demora de 36,775 segundos hasta que sistema se recupere después de que haya ocurrido algún fallo, esto equivale a una alta disponibilidad del 99,999% según la tabla de disponibilidad.

Se concluye entonces que Heartbeat es la mejor herramienta para dar alta disponibilidad al servicio Asterisk; pues es un sistema tolerante a fallos y proporciona un clúster evitando en lo más mínimo la pérdida del servicio.

Se recomienda la utilización de múltiples tarjetas de red esto permitirá a los servidores adaptarse a diferentes modelos de red de alta disponibilidad, entre ellas, las redes con enlaces redundantes.

SUMMARY

This study allows us choosing the best technique for obtaining high availability IP telephony networks.

It intended to decrease the risk of a prolonged interruption in telephone network, for which is proposed for a stable and robust core Asterisk that allows us to obtain a high availability network.

the main goal is to analysis and design a highly available network core based Asterisk DUNDi technology, which will develop at the Laboratory of CISCO Academy Polytechnic School of Chimborazo.

It was used the deductive method to study the techniques of high availability VoIP networks and to propose a solution of a model asset/liability based on Heartbeat as the best option to maintain high availability services. this model uses a Master and a Slave server that form the Layer 2, a DNS server, and DHCP are on Layer 1, and the terminals are IP phones, softphones and Grandstream ATA drives; all these equipments are on a network Ethernet by Cat 5e UTP cables with RJ45 connectors.

the result show a turnaround time of 36.775 seconds until the system recovers after a failure has occurred; this equals high availability of 99.999% availability per table.

It concluded that, Heartbeat is the best tool to provide high availability by running Asterisk; it is a fault tolerant system and provides a cluster in the least prevent the loss of service.

Using multiple network cards, which will allow to the servers to adapt them to different models of high availability network, including networks with redundant links, were recommended.

GLOSARIO

B

BIND (Berkeley Internet Name Domain)

Servidor DNS más común para sistemas Unix, el cual resuelve los nombres de hosts en la red a direcciones numéricas y viceversa

C

Canal

Vía o medio utilizado para comunicar un mensaje.

CentOS

Es una libre y disponible distribución de Linux que se basa en Linux Red Hat Enterprise Linux RHEL.

Clustering

Es la facultad que tienen varias máquinas para realizar una tarea como si se tratase de una sola máquina, siendo esto tranparente para las maquinas clientes.

D

DHCP (Dynamic Host Configuration Protocol)

Protocolo utilizado para la configuración dinámica y está encargado de asignar, de forma automática, direcciones IP a los hosts de una red de computadoras.

DNS (Domain Name Server)

Servidor de Nombres de Dominios, se encarga de convertir nombres de dominio en direcciones IP.

T

Telefonía

Sistema telefónico en el que la conexión entre el aparato portátil y la central se realiza mediante ondas hercianas.

DRBD (Distributed Replicated Block Device)

Traducido es un Dispositivo de Bloque Distribuido y Replicado, este dispositivo se asemeja a un disco duro, es el encargado del almacenamiento de los datos en clústeres de alta disponibilidad, replicando sobre una red.

E

Ethernet

Es un estándar de transmisión de datos para redes de área local para computadoras, que define el acceso al medio.

Failback

Es el proceso que permite devolver el control del servicio a un servidor, sistema o red, a su estado original, una vez que se recuperó de alguna falla.

Failover

Es la facultad para dar el control de un servicio a un servidor, sistema o red redundante o de respaldo, de forma automática, cuando ocurre alguna falla.

G

GPL (General Public License)

Licencia Pública General, fue creada por la Free Software Foundation para proteger la libre distribución, modificación y uso de Software Libre.

H

Heartbeat

Software que se encarga de monitorear dos o más máquinas destinadas a mantener servicios de alta disponibilidad en un modelo activo / pasivo, dando el control del servicio a la máquina en estado pasivo en caso ocurra alguna falla en la activa.

HTTP (HyperText Transfer Protocol)

Protocolo de Transferencia de Hipertexto, es el protocolo estándar para la transmisión de páginas Web.

IP (Dirección)

Número que identifica de manera lógica a un computador dentro de una red de computadoras, que utiliza el protocolo IP.

K

Kernel

Núcleo de los Sistemas Operativos GNU/Linux.

L

LAN (Local Area Network)

Red de Área Local, es una red de computadoras de tamaño medio, disperso dentro de un edificio o hasta dentro de una ciudad.

Linux

Es un Sistema operativo, también conocido como GNU/Linux, basado en UNIX, distribuido bajo la licencia GPL, siendo este Software Libre.

Linux-HA

Proyecto que provee un framework de alta disponibilidad, con Heartbeat como su componente básico.

M

MAC (Media Access Control)

Dirección de Control de Acceso al Medio, es un identificador de 48 bits que identifica, de manera única, a una tarjeta de red

MySQL

Sistema Gestor de Bases de Datos.

S

SO

Sistema Operativo.

STONITH (Shoot The Other Node In The Head)

Modalidad de Fencing que consiste en apagar o reiniciar algún servidor para asegurarse de que libere los recursos que tiene asignados.

Switch

Es un dispositivo de interconexión de redes de computadoras, que interconecta dos o más segmentos de red.

U

UNIX

Sistema operativo portable, multitarea y multiusuario.

URL (Uniform Resource Locator)

Localizador Uniforme de Recursos, es una secuencia de caracteres que se usa para nombrar recursos de Internet para su localización, de acuerdo a un formato estándar para los diversos protocolos utilizados en Internet como HTTP, FTP, etc.

V

VIP (Virtual IP Address)

Dirección IP Virtual, es una dirección IP que puede ser asignada a un conjunto

de computadores dentro de un clúster.

ANEXOS

ANEXO 1

INSTALACIÓN Y

CONFIGURACIÓN DE ELASTIX

ANEXO 1.

INSTALACIÓN Y CONFIGURACIÓN DE ELASTIX

Descargar: asterisk-addons-1.4.13.tar.gz

Pag. http://downloads.asterisk.org/pub/telephony/asterisk/

Descarga Elastix 2.0

http://sourceforge.net/projects/elastix/files/Elastix%20PBX%20Appliance%20Software/2.0/Elastix-2.0.0-i386-bin-29Oct2009.iso/download

Mysql servidor.

user: root

password: eLaStIx.2oo7

fpt

user: root

password: 123456

elastix

user: admin

password: palosanto

webmin

user: root

password: 123456

{ dbname=asteriskcdrdb
password=eLaStIx.asteriskuser.2oo7}
res_mysql.conf

```
;
; Sample configuration for res_config_mysql.c
;
; The value of dbhost may be either a hostname or an IP address.
; If dbhost is commented out or the string "localhost", a connection
; to the local host is assumed and dbsock is used instead of TCP/IP
; to connect to the server.
;
[general]
dbhost = 127.0.0.1
dbname = asteriskrealtime
dbuser = asteriskuser
dbpass = eLaStIx.asteriskuser.2oo7
;dbport = 3306
;dbsock = /tmp/mysql.sock
```

ANEXO 2

PASOS PARA LA CONFIGURACIÓN DE TELEFONIA IP CISCO

ANEXO 2.

PASOS PARA LA CONFIGURACIÓN DE TELEFONIA IP CISCO

Teléfono IP CISCO 7912

Figura 4: Teléfono IP CISCO 7912.

Descripción de las características del Teléfono IP 7912

Tabla VIII : Características del teléfono IP CISCO 7912.

N.	Características	Función
1	Modelo del teléfono	Indica el modelo del teléfono IP CISCO
2	Pantalla LCD	Presentan información tales como el estado de la llamada, número de teléfono y las etiquetas de las teclas programables de función soft-keys.
3	Teclas programables	Activan las funciones presentadas en sus correspondientes etiquetas.

4	Botones de navegación	Permiten desplazarse por el texto y seleccionar las funciones que aparecen en la pantalla. Ofrece acceso directo al menú de navegación rápida cuando el teléfono está colgado.
5	Botón de menú	Proporciona acceso a los servicios que ofrece el teléfono.
6	Botón de retención	Para poner la llamada activa en espera. También reinicia una llamada en espera.
7	Teclado	Funciona como en un teléfono tradicional.
8	Botón de volumen	Sube o baja el volumen del teléfono. También controla el volumen del timbre (si el teléfono está colgado).
9	Auricular con indicador luminoso	Sube o baja el volumen del teléfono. También controla el volumen del timbre (si el teléfono está colgado).

Teclas programables

Este teléfono IP Cisco dispone de teclas programables que activan las funciones que aparecen en la parte inferior de la pantalla LCD. Las teclas varían en función del estado del aparato. Las teclas programables se usan para iniciar las funciones que aparecen en las correspondientes pestañas de la pantalla LCD.

A continuación se muestra una lista con las teclas programables del Teléfono IP Cisco 7912G. Las funciones varían dependiendo de la configuración del sistema.

Tabla IX : Teclas programables del teléfono IP CISCO 7912.

Tecla	**Función**
<< ó >>	Para desplazarse al editar caracteres
Acct	Consulte con el administrador acerca de la utilización de esta tecla.
RetroLl.	Indica que la línea está libre.
Cancela	Anula la última selección.
DsvInc.	Desvía todas las llamadas.

Elimina	Elimina el historial de la agenda.
Confrn	Establece una conferencia.
Eliminar	Elimina el número seleccionado.

Tabla X : Teclas programables del teléfono IP CISCO 7912 (continuación).

Tecla	**Función**
DND	Activa la función "no molesten".
Abajo	Disminuye el contraste de la pantalla LCD.
EdtMarc	Selecciona un número y active el cursor para modificarlo.
FinLlam.	Finaliza la llamada en curso
Salir	Para abandonar la selección en curso
Flash	Activa el indicador luminoso del suricular para llamadas a 3 y llamadas en espera.
CaptGr.	Para atender llamadas entrantes en un número de teléfono que forma parte de un grupo determinado.
Login	Acceso a servicios que requieren de un PIN para su activación. Consulte al administrador de su sistema para el uso de esta tecla.
Message	Para acceder al buzó del voz.
Monitor	Para pasar de la escucha a través del auricular al altavoz y al modo manos libres.
Monoff	Para pasar de la escucha a través del altavoz alauricular y seguir hablando.
Más	Para desplazarse por opciones adicionales (utilice el botón Mas, por ejemplo, para localizar la tecla DND)
Mute	Activa o desactiva el silenciador.
Llamar	Abre una nueva línea para realizar una llamada.
Ok	Para confirmar la selección.
Park	Envía la llamada a una extensión desde la cual puede ser recuperada.
Captur	Para responder a llamadas dirigidas a otra extensión.
Reprod.	Reproduce una muestra del timbre
ReLlam.	Vuelve a marcar el último número marcado.
Guardar	Consulte al administrador para el uso de esta tecla.
Resume	Returna a una llamada activa.
Guardar	Guarda el último cambio.
Busca	Inicia una búsqueda en el directorio local.

Selecci.	Selecciona la opción resaltada en pantalla.
Config.	Acceso a la configuración del teléfono para tonos de llamada, contraste de la pantalla y volumen del timbre.
Trnsf.	Para transferir las llamadas a un número alternativo.
Arriba	Incrementa el contraste de la pantalla LCD.

Elementos

A continuación se especifica los elementos necesarios para la configuración de un Teléfono IP sobre una central Asterisk. Es importante configurar el tipo de protocolo que se usará, en los teléfonos CISCO los teléfonos CISCO se configurará el protocolo SIP. Los elementos que se necesitan son:

- Un Teléfono IP CISCO SIP 7912
- Y un servidor dhcp, para que la dirección ip sea asignada al teléfono de forma dinámica.

Configuración teléfono CISCO SIP 7912

Configuración por medio de la pantalla LDC

La siguiente configuración se realizara mediante interface web, en la barra de direcciones se ingresa la dirección ip correspondiente al teléfono IP Cisco (ejemplo 172.30.124.167), en **SIP Parameters** se procede a crear la extensión.

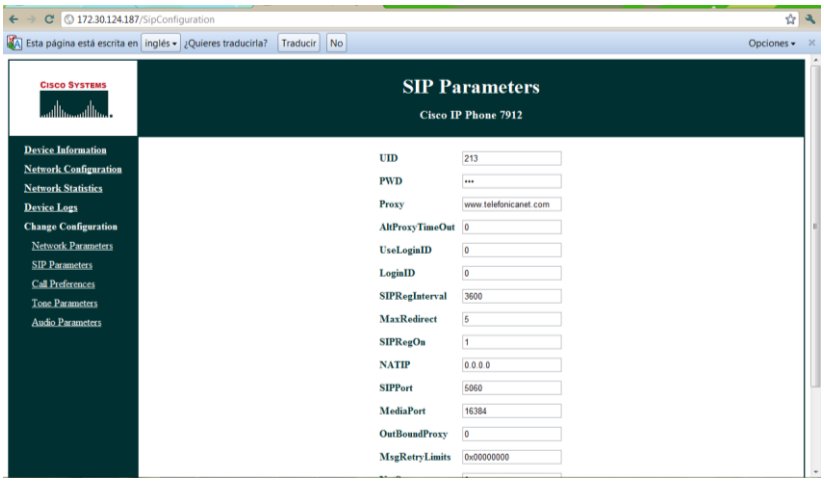


Figura 5: Registro de parámetros SIP en el Teléfono IP CISCO.

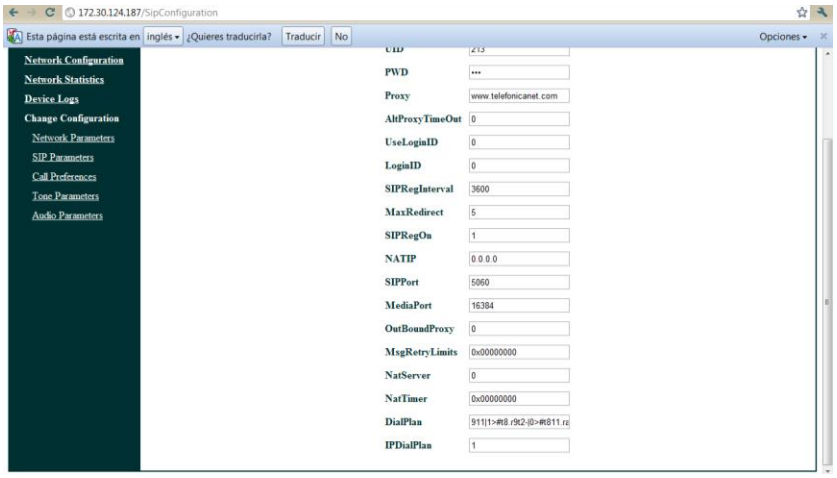


Figura 6: Registro de parámetros SIP en el Teléfono IP CISCO (continuación).

Para realizar una llamada:

Se puede utilizar cualquiera de los métodos que se indican a continuación:

- Se descuelga el teléfono y se marca un número.
- Se puede pulsar **Llamar** y luego marcar un número.

- Otra forma es pulsando **ReLlam.**.
- Y la úlitma forma es marcar el número sin descolgar el auricular y, a continuación, pulsar **Marcar** o descolgar el auricular..

Para realizar una llamada al último número marcado

- Se descuelga el teléfono y se pulsa la tecla de rellamada.
- Ó se pulsa el botón de servicios y luego se navega hasta la opción de " Llamadas enviadas" a continuación se seleccione el número que desea marcar.

Para poner una llamada en espera

- Basta con pulsar **Reten.**.
- Y para volver a recuperar la llamada en espera se vuelve a pulsar **Reten.**.

Para silenciar una llamada

- Se debe pulsar en **Mute**.
- Para desactivar el silencio se debe volver a pulsar Mute o, si utiliza la función de silencio y la de manos libres, simplemente descuelgue el auricular.

Para gestionar las llamadas en espera

- Para seleccionar entre varias llamadas en espera en la misma línea, utilice el botón **Reten.**.

Para realizar una conferencia telefónica

1. Durante una llamada, pulse **Confrn.**. Al hacerlo se abre una línea automáticamente y el primer interlocutor pasa a modo "en espera".
2. A continuación llame a otro número.
3. Cuando se establece la llamada, vuelva a pulsar **Confrn.** para añadir al nuevo interlocutor a la conferencia.

Nota: Cuando el que origina la llamada cuelga, termina la conferencia teléfonica.

Para ajustar el volumen del timbre

- Pulse Up o Down Volume con el teléfono colgado. Para ajustar el volumen de la llamada en curso.

Para ajustar el volumen de la llamada en curso

- Pulse Arriba o Abajo Volumen mientras utiliza el teléfono.

Para transferir llamadas

Existen dos modos de transferencia de llamadas a otro número:

- Transferencia "a ciegas": redirige la llamada directamente, sin hablar con la persona a la que se transfiere la misma.
- Transferencia "con consulta": redirige la llamada después de haber hablado con la persona a la que se va a transferir.

Para transferir una llamada:

1. Durante la llamada, pulse Trnsf.. La llamada activa se pone en espera.
2. Marque el número al que desea transferir la llamada.
3. Para realizar una transferencia "a ciegas":
   - Cuelgue cuando oiga la señal de línea.

   Para realizar una transferencia "con consulta":
   - Cuando la persona a la que desea transferir la llamada contesta, pulse Trnsf. y, a continuación, cuelgue.

Nota: Si no se transfiere la llamada, pulse Resume para volver a la llamada original.

4. Para cancelar un intento de transferencia de llamada y volver a tener en línea a la persona que ha llamado, pulse **Reten.**.

Para desviar todas las llamadas

1. Pulse **DsvInc.**. Se oye una señal sonora de confirmación.

2. Marque el número al que desee desviar todas las llamadas.

   Márquelo exactamente como lo haría si quisiera realizar una llamada; con todos los prefijos necesarios.
3. Se actualizará la pantalla del teléfono para indicar que se ha desviado la llamada.
4. Pulse almohadilla (#). Se actualizará la pantalla del teléfono para indicar que se ha desviado la llamada.
5. Para cancelar el desvío de llamadas, pulse **DsvInc.**.

Para escuchar los mensajes del buzón de voz, configurar el teléfono y utilizar la agenda

1. Pulse **Menu**.
2. Utilice el botón Navigation para desplazarse por las opciones:
   a. Pulse **1** para escuchar los mensajes y siga las instrucciones de la operadora.
   b. Pulse **2** para acceder a la agenda y para ver las llamadas perdidas, recibidas y enviadas. –
   c. Pulse **3** para acceder a la configuración del aparato: ajuste del contraste, volumen del timbre, tipo de timbre.
3. Utilice el botón Navegación para desplazarse por las opciones.
2. Para seleccionar una opción, pulse **Selecci.**.
4. Si desea regresar al menú precedente, pulse Salir.

Activación de la función de “no molesten” (**DND**)

Para recibir un aviso visual e información de las llamadas sin que suene el teléfono, utilice el **DND**. La línea se mostrará ocupada y las llamadas se tratarán como en los casos normales sin respuesta.

- Pulse Mas para localizar la tecla **DND**.
- Pulse la tecla **DND**.

Para utilizar la función Captura de Llamada

- Pulse **Captur.**.
- Marque la extensión del teléfono IP Cisco que está sonando

El control de la llamada se transferirá a su aparato.

Para atender una llamada procedente de un teléfono que forma parte de un grupo determinado, puede utilizar uno de los métodos que se exponen a continuación:

- Pulse **CaptGr.**. Si sólo hay un grupo definido en todo el sistema CallManager Express, el control de la llamada se transfiere a su teléfono.
- Si el teléfono que está sonando y el suyo pertenecen al mismo grupo, pulse asterisco (*) para transferir el control de la llamada a su aparato.
- Si el teléfono que está sonando y el suyo pertenecen a grupos distintos, marque el número del grupo al que pertenece el teléfono que está sonando para transferir el control de la llamada a su aparato.

Almacenamiento y recuperación de llamadas aparcadas

Puede recurrir al aparcamiento de llamadas si desea almacenar una llamada para recuperarla desde otro teléfono del sistema Cisco CallManagerExpress (por ejemplo, un teléfono de la oficina de otra persona o de una sala de conferencias).

El aparcamiento de llamadas es una función especial que el administrador del sistema puede configurar en su teléfono.

Para Almacenar una llamada activa con aparcamiento de llamadas:

Durante una llamada, seleccione más > Aparcar. En la pantalla del teléfono se mostrará el número especial para aparcar llamadas en el que se almacenará la llamada. Pulse el botón de transferencia, seguido del número especial de aparcamiento presentado por el sistema.

Recuperar una llamada Aparcada: Marque el número en el que se aparcó la llamada desde cualquier teléfono IP de Cisco en su red para recuperarla.
Nota: Dispone de un período de tiempo limitado para recuperar la llamada aparcada antes de que vuelva a sonar en su destino original.

Pregúntele al administrador del sistema el valor de este tiempo limitado.

Función de difusión de mensajes

El servicio de difusión de mensajes proporciona un método para enviar mensajes de audio a grupos de teléfonos IP que hayan sido previamente designados por el administrador del sistema como destinatario de estos mensajes. La comunicación es unidireccional y los mensajes no pueden ser contestados. Para utilizar la función de difusión de mensajes, haga lo siguiente:

1. Seleccione una línea disponible levantando el auricular y espere el tono de llamada.
2. Marque el número del grupo de difusión. Este número debe ser proporcionado por el administrador del sistema.

Cada uno de los teléfonos IP que han sido configurados como pertenecientes al grupo de difusión, y que no estén ocupado en ese momento, responde automáticamente en modo manos libres, y la

pantalla muestra la identidad del llamante.

Cuando el iniciador de la difusión cuelga el auricular, los teléfonos retornan a su estado normal.

Personalización de tonos de llamada

El usuario puede seleccionar el tono de llamada utilizad de entre los configurados por el administrador y que estén disponibles en el sistema de Call Manager Express. Para ello, acceder al menú de configuración del teléfono a través del botón de configuración.

Navegar por las opciones de configuración del teléfono hasta la opción de RingList y seleccionar el tono deseado de entre los disponibles.

PASOS PARA LA CONFIGURACIÓN DEL TELÉFONO IP GRANDSTREAM

Teléfono GRANDSTREAM Budge Tone-201

Presiona el botón Menú del teléfono IP GRANDSTREAM, con el botón que indica la flecha hacia abajo recorre hasta la opción 2 y presiona nuevamente el botón Menú.

En la pantalla LCD se visualiza una dirección IP que fue asignada por el servidor DHCP en mi caso se me ha asignado la dirección 172.30.124.183, para continuar con la configuración, se registrará una extensión configurada anteriormente en la PBX Asterisk.

Accedemos mediante un Cliente Web que puede ser un navegador (Google Chrome, Mozilla Firefox, Internet Explorer, etc.).

En el navegador Google Chrome en la barra de direcciones e ingresado la dirección IP 172.30.124.183.

User: admin

Password: admin

Figura 7: Login en el Teléfono IP GRANDSTREAM.

Se ha Ingresado los datos de la extensión de la siguiente manera

Si no se posee un servidor de DNS, en SIP server se ingresa la IP de la central Asterisk, (por ejemplo: 172.30.124.202). El DNS que yo he configurado reconoce el dominio www.telefonicanet.com.

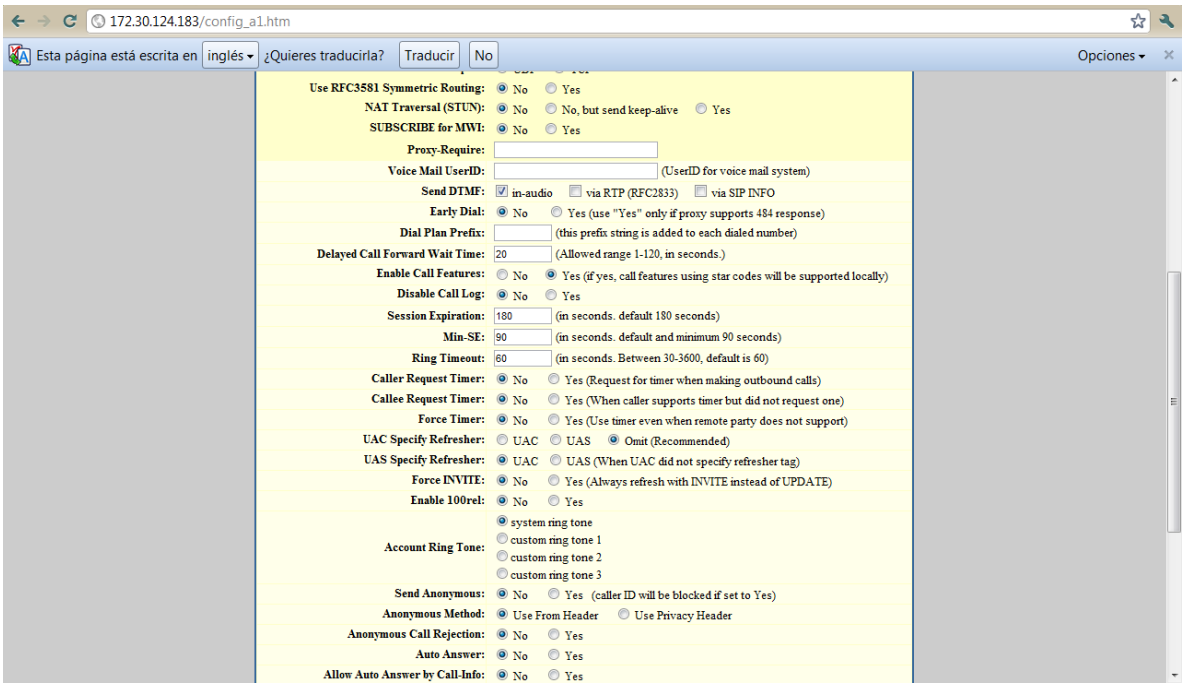


Figura 8: Registro de cuenta en el Teléfono IP GRANDSTREAM (continuación).

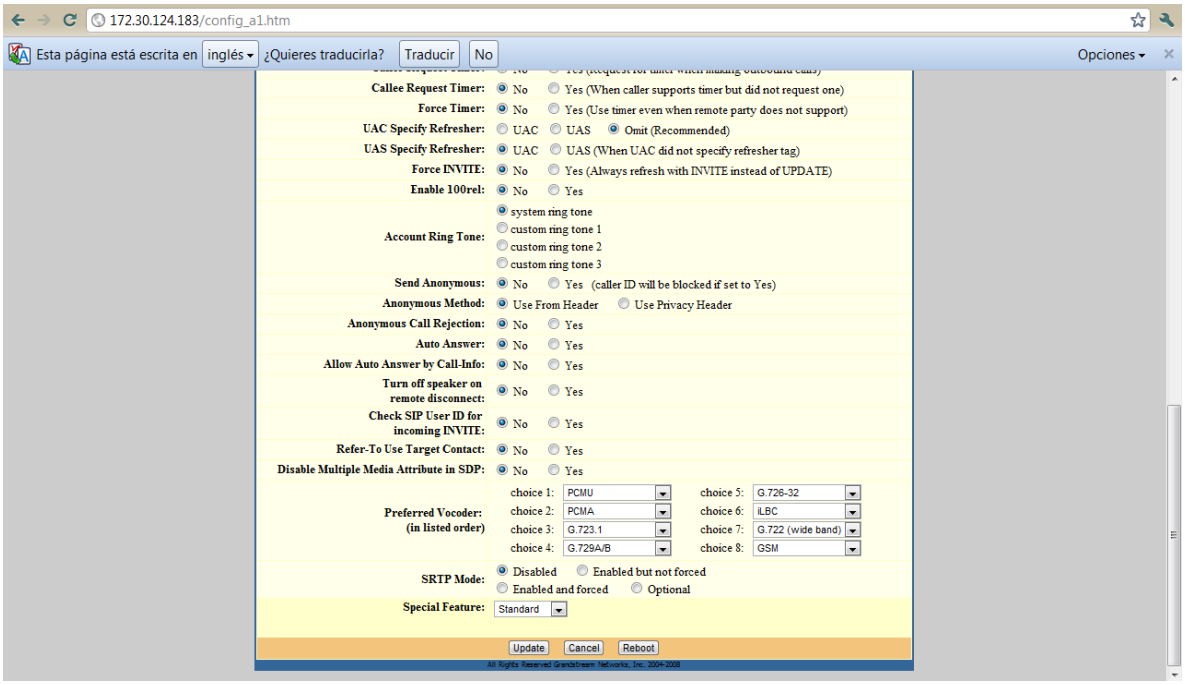


Figura 9. Registro de cuenta en el Teléfono IP GRANDSTREAM (continuación).

Se acepta las modificaciones clicleando Update.

Nuevamente ingresamos el password (“admin”).

Finalmente se ha registrado la extensión en el teléfono IP GRANDSTREAM Budge Tone-201.

ANEXO 3

CONFIGURACIÓN DE DNS SRV

ANEXO 3.

CONFIGURACIÓN DE DNS SRV

Lo primero a realizar es la creación de una zona en este punto se modificará el archivo de configuración que se conoce como named.conf.

Este archivo ubicado en el directorio /etc es el archivo de configuración principal de DNS ya que contiene la ubicación y parámetros de los demás archivos de configuración, en él se indican todas las zonas a las cuales dará servicio el servidor DNS, entre otras funciones. Este archivo contiene dos tipos de secciones:

Opciones " **options** ": Indica el directorio donde se encuentran otros archivos de configuración y algunas otras opciones.

Zonas " **zone** ": Pueden existir varias zonas por archivo, estas zonas definen los dominios (telefonicanet.com) y redes "networks" (172.30.124.0) sobre los que se mantiene información.

A continuación se muestran las líneas de configuración del dominio, los archivos de configuración completos se pueden ver en los ANEXOS. Para observar este apartado se ha ingresado mediante interface grafica de Webmin en **Edit Config File** de la zona.

```
options {
        directory "/etc";
        pid-file "/var/run/named/named.pid";
        };
zone "telefonicanet.com" {
        type master;
        file "/var/named/telefonicanet.com.hosts";
        notify yes;
        allow-update {
                none;
                };
        allow-transfer {
        172.30.124.101
                };
        };
```

La zona configurada será el dominio dentro de la red, conocido como telefonicanet.com. Zone indica el nombre del dominio que estamos configurando, el resto son sus detalles. Type master indica que es el servidor principal de la zona. Si fuera un servidor secundario tendríamos que poner "type slave".

```
zone "telefonicanet.com" {
        type slave;
        file "/etc/bind/db";
        master {
        172.30.124.100
        };
        };
```

La razón de la existencia de ambos no es en estricto rigor pero es tremendamente conveniente en el caso de que el primario dejase de funcionar. La línea file indica qué fichero contiene los datos de la zona. Este fichero se debe encontrar en el directorio /var/named.

Por último, allow-update indica desde qué equipos se pueden realizar actualizaciones dinámicas, en nuestro caso se permitirá realizarlas hacia el host 172.30.124.101.

En estos ficheros tendremos que poner direcciones IP y no nombres porque el sistema de resolución aun no está activo.

Ahora tenemos que introducir una configuración inicial de la zona. Este fichero ha de contener todos los registros de recurso asociados a dicha zona.

Tipos de registros de DNS

Tabla XI: Tipos de registros de DNS.

	Tipo	**Nombre**	**Función**
Zona	SOA	Start Of Authority	Define una zona representativa del DNS
	NS	Name Server	Identifica los servidores de zona, delega subdominios
Básicos	A	Dirección IPv4	Traducción de nombre a dirección
	AAAA	Dirección IPv6 original	Actualmente obsoleto
	A6	Dirección IPv6	Traducción de nombre a dirección IPv6
	PTR	Puntero	Traducción de dirección a nombre
	DNAME	Redirección	Redirección para las traducciones inversas IPv6
	MX	Mail eXchanger	Controla el enrutado del correo
Seguridad	KEY	Clave pública	Clave pública para un nombre de DNS
	NXT	Next	Se usa junto a DNSSEC para las respuestas negativas
	SIG	Signature	Zona autenticada/firmada
Opcionales	CNAME	Canonical Name	Nicks o alias para un dominio
	LOC	Localización	Localización geográfica y extensión
	RP	Persona responsable	Especifica la persona de contacto de cada host
	SRV	Servicios	Proporciona la localización de servicios conocidos
	TXT	Texto	Comentarios o información sin cifrar

Es necesario definir un registro de recurso que es el que hará funcionar todo la estructura de la red de alta disponibilidad, el registro de recursos SRV; permite utilizar varios servidores para un único dominio DNS, para mover servicios desde un host a host fácilmente y designar algunos hosts como servidores. Localizan servidores que proporcionen un servicio basado en TCP/IP mediante una única operación de consulta DNS. Gracias a este registro es por el cual se puede establecer un balanceo de carga en las centrales en uno de sus parámetros. Se muestra a continuación el fichero de registros DNS.

```
$ttl 38400
telefonicanet.com.          IN      SOA     dns0.telefonicanet.com.
cisco.telefonicanet.com. (
                            1293935335
                            10800
                            3600
                            604800
                            38400 )
IN NS dns0
telefonicanet.com.          IN      A       192.168.137.100
dns0 IN  CNAME telefonicanet.com.
www.telefonicanet.com. IN CNAME         telefonicanet.com.
pc1 IN    A         192.168.137.161
pc2 IN    A         192.168.137.162
pc3 IN    A         192.168.137.163
pc4 IN    A         192.168.137.164
telefonicanet.com.          IN      NS      telefonicanet.com.
dns0.telefonicanet.com.     IN      CNAME   telefonicanet.com.
_sip._udp.telefonicanet.com. 300 IN SRV 0 1 5060 pc1.telefonicanet.com.
_sip._udp.telefonicanet.com. 300 IN SRV 0 1 5060 pc2.telefonicanet.com.
_sip._udp.telefonicanet.com. 300 IN SRV 0 1 5060 pc3.telefonicanet.com.
_sip._udp.telefonicanet.com. 300 IN SRV 0 1 5060 pc4.telefonicanet.com.
```

Los registros de tipo A son aquellos que aportan la dirección IP de una máquina, en este caso cada una de estas centrales, conocidas por el nombre pc1, pc2, pc3 y pc4. Las dos últimas sentencias son pertenecientes al registro SRV. Para razonar mejor su funcionalidad, se hará una explicación más puntualizada de esta sentencia.

Formato del registro de recursos SRV

El registro de recursos SRV tiene código de tipo DNS, a continuación se muestra la siguiente sintaxis:

```
Servicio.Protocolo.Nombre TTL clase SRV Prioridad Peso Puerto destino.
```

Cada uno de los estos campos que se usan en el registro de recursos SRV tienen como objetivo lo siguiente:

Servicio (_sip): Nombre simbólico de la información solicitada de servicio, Pueden llamarse localmente sólo servicios definidos localmente. Servicio no distingue entre mayúsculas y minúsculas. Para los servicios conocidos, se define en el documento RFC 1700. Si no se define en el documento RFC 1700 un nombre de servicio conocido, en su lugar se puede utilizar un nombre creado por el usuario. Si el RFC 1700 asigna un nombre para un servicio indicado en este campo, el nombre definido en RFC es el único nombre que se puede utilizar pero solo se lo utilizará localmente.

Protocolo (._udp): TCP y UDP son en este momento los valores más útiles para este campo, Se puede utilizar cualquier protocolo de transporte nombrado en RFC 1700, aunque cualquier nombre definido por números asignados o localmente, se puede utilizar (como en servicio). Distingue mayúsculas de minúsculas e indica el tipo de protocolo de transporte.

Nombre (telefonicanet.com.): Dominio que hace referencia este registro de recursos a. El registro de recursos SRV es único en que el nombre buscado no es este nombre. Es diferente con relación a otros tipos de registro DNS en que no se utiliza para realizar búsquedas o consultas.

TTL: Especifica el tiempo máximo que otros servidores DNS y aplicaciones deben mantener en caché ese registro. Si el valor es 0, entonces no se mantiene ningún caché y los cambios que se realicen en el registro se registrarán en el momento. Cuando se decide el tiempo TTL, se debe tener en cuenta cuan a menos se cambiará el record (registro). Por el caché, los cambios en un registro DNS no alcanzarán toda la red hasta que el TTL no haya expirado. Si se quieren cambios rápidos, debe elegirse un TTL bajo.

Clase: Es un entero de 16 bits que define la clase del Resource Record.

Prioridad (0): Es la prioridad de este host de destino. El campo de prioridad determina la prioridad de uso de los datos del registro. Los clientes siempre usan el registro SRV con el menor valor de prioridad numeradas en primer lugar. El intervalo es 0-65535.

Peso (1): Se lo considera como un mecanismo de equilibrio de carga. Al seleccionar un host de destino entre las que tienen la misma prioridad, la posibilidad de tratar este uno primero debe ser proporcional a su peso. Pesos mayores se debería dar una proporcionalmente mayor probabilidad de

que se está seleccionada. El intervalo es 0-65535. En el caso de no requerir equilibrio de carga se asignará 0.

Puerto (5060): Puerto de este host de destino de este servicio. El intervalo es 0-65535. Esto es a menudo como especificado en los números asignados, pero no es necesario.

Destino: se define el nombre de dominio DNS de los host de destino. Debe haber uno o más registros "A" para este nombre. Los implementadores deben, pero no son necesarios, para devolver los registros "A" en la sección de datos adicionales. Nombre de la compresión es que se va a utilizar para este campo. Un destino de "." significa que el servicio no está disponible en este dominio.

Si nos fijamos en los registros SRV el campo **peso** asignado es **1** esto quiere decir que no habrá preferencia por ninguno de los servidores, todos tienen igual preferencia.

ANEXO 4

CONFIGURACIÓN DE ASTERISK

EN REALTIME

ANEXO 4.

CONFIGURACIÓN DE ASTERISK EN REALTIME

Descargar asterisk-addons-1.4.13.tar de http://downloads.asterisk.org/pub/telephony/asterisk/. Al punto se ha descargado el asterisk-addons-1.4.13.tar que es un paquete que permitirá integrar a nuestra central de telefonía IP y añade cuatro funcionalidades muy importantes como son:

- Tener un registro de las llamadas en una base de datos usando MySql.
- Poder utilizar archivos MP3 para la música en espera.
- Añadir el protocolo H.323 para proveer a los usuarios con tele-conferencias que tienen capacidades de voz, video y datos sobre redes de conmutación de paquetes.
- El canal chan_mobile que nos permite conectar, via bluetooth, un celular a nuestra central y usarlo como gateway GSM y, si el celular lo soporta, envio de SMS, esta es una funcionalidad que no se ha la implementará en el presente trabajo de Tesis.

Antes de empezar tenemos que parar el servidor Asterisk y arrancar el servidor Mysql

Para hacer esto digitamos:

```
/etc/init.d/asterisk stop ó service asterisk stop
/etc/init.d/mysqld start ó service mysqld stop
```

Luego dentro del directorio /usr/src/ se descomprime el archivo asterisk-addons-1.4.13.tar.

Ingresamos al terminal y procedemos a compilar e instalar.

```
[pc1@localhost ~]$ cd asterisk-addons-1.4.13
[pc1@localhost ~]$ ./configure
[pc1@localhost ~]$ make
[pc1@localhost ~]$ make install
```

Posteriormente ir al directorio de archivos de configuración de Asterisk /etc/asterisk y editar los archivos cdr_mysql.conf y res_mysql.conf

archivo cdr_mysql.conf

```
[global]
hostname=localhost
dbname=asterisk1
table=cdr
password=123456
user=userealtime
userfield=1
port=3306
;sock=/tmp/mysql.sock
```

archivo res_mysql.conf

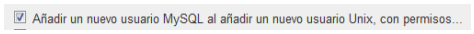
```
[general]
dbhost = 127.0.0.1
dbname = asterisk1
dbuser = userealtime
dbpass = 123456
dbport = 3306
dbsock = /var/lib/mysql/mysql.sock
```

Para habilitar esta funcionalidad, simplemente hay que disponer de una base de datos mysql, en este caso se crear una base de datos Asterisk1.

Para esto se debe crea un usuario con libre acceso a la Base de Datos.

Para eso ingresamos a Servidores y luego a Servidor de Base de Datos MySQL, con la herramienta Webmin:

Luego en **Permisos de usuario** señalamos **añadir usuario con permisos** como se indica en la figura, procedemos a crear el usuario, esto nos permitirá manipular adecuadamente la base de datos Asterisk1:



Entonces creamos la base de Datos que lleva por nombre Asterisk1.

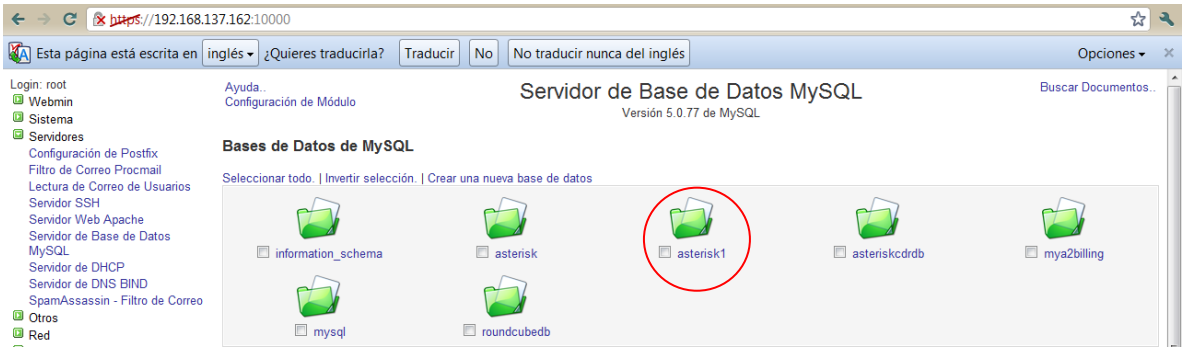


Figura 10: Servidor de base de datos MySQL.

Nuestra base de datos mysql se encuentra en la misma máquina, así que no se necesitará cambiar el hostname y dbhost. Luego se debe crear la tabla "cdr" en nuestra base de datos.

A continuación el script de la Tabla "**cdr**":

```
CREATE TABLE cdr (
 calldate datetime NOT NULL default '0000-00-00 00:00:00',
 clid varchar(80) NOT NULL default ' ',
 src varchar(80) NOT NULL default ' ',
 dst varchar(80) NOT NULL default ' ',
 dcontext varchar(80) NOT NULL default ' ',
 channel varchar(80) NOT NULL default ' ',
 dstchannel varchar(80) NOT NULL default ' ',
 lastapp varchar(80) NOT NULL default ' ',
 lastdata varchar(80) NOT NULL default ' ',
 duration int(11) NOT NULL default '0',
 billsec int(11) NOT NULL default '0',
 disposition varchar(45) NOT NULL default ' ',
 amaflags int(11) NOT NULL default '0',
 accountcode varchar(20) NOT NULL default ' ',
 uniqueid varchar(32) NOT NULL default ' ',
 userfield varchar(255) NOT NULL default ' ',
 KEY `calldate` (`calldate`),
 KEY `dst` (`dst`),
 KEY `accountcode` (`accountcode`)
 ) ENGINE=MyISAM ;
```

Finalmente reiniciar Asterisk

```
/etc/init.d/asterisk reload
```

Al ingresar a la consola para verificar si los cambios y la tabla han sido reconocidos con el comando

```
Asterisk*CLI> realtime mysql status
```

Para registrar el uniqueid, se debe recompilar asterisk-addons previamente hay que agregar al principio del archivo.

```
/usr/src/ asterisk-addons-1.4.13/cdr/cdr_addon_mysql.c
```

La línea

```
#define MYSQL_LOGUNIQUEID
```

Guardar el archivo y recompilar asterisk-addons

```
[pc1@localhost ~]$ make
```

Por último se presentará el script de la Tabla "**sipfriends**" para manejar los usuarios, peers y extensiones.

```
CREATE TABLE `sipfriends` (
 `name` varchar(40) NOT NULL default ' ',
 `type` varchar(10) NOT NULL default ' ',
 `username` varchar(40),
 `fromuser` varchar(40),
 `fromdomain` varchar(40),
 `secret` varchar(40),
 `md5secret` varchar(40),
 `auth` varchar(10),
 `mailbox` varchar(20),
 `subscribemwi` varchar(10),
 `vmexten` varchar(20),
 `callerid` varchar(40),
 `cid_number` varchar(40),
 `callingpres` varchar(20),
 `usereqphone` varchar(10),
 `language` varchar(10),
 `incominglimit` varchar(10),
 `context` varchar(40) NOT NULL default ' ',
 `subscribecontext` varchar(40),
 `amaflags` varchar(20),
 `accountcode` varchar(20),
 `musicclass` varchar(20),
 `mohsuggest` varchar(20),
 `allowtransfer` varchar(20),
 `callgroup` varchar(20),
 `pickupgroup` varchar(20),
 `autoframing` varchar(10),
 `disallow` varchar(20) default 'all',
 `allow` varchar(20),
 `maxcallbitrate` varchar(15),
 `host` varchar(40) default 'dynamic',
 `outboundproxy` varchar(40),
 `ipaddr` varchar(20) NOT NULL default ' ',
 `defaultip` varchar(20),
 `port` int(6) NOT NULL default '0',
 `fullcontact` varchar(40),
 `insecure` varchar(20),
 `qualify` varchar(15),
 `regseconds` int(11) NOT NULL default '0',
 `regexten` varchar(20),
 `regserver` varchar(20),
 `rtptimeout` varchar(15),
 `rtpholdtimeout` varchar(15),
 `rtpkeepalive` varchar(15),
 `lastms` int(11) NOT NULL default '-1',
 `setvar` varchar(200),
 PRIMARY KEY  (`name`),
 INDEX host (host, port),
 INDEX ipaddr (ipaddr, port)
) TYPE=MyISAM;
```

Al final modificamos el archivo de configuración de Asterisk para el Realtime; en el archivo /etc/asterisk/extconfigs.conf vamos a encontrar algo como:

;sipusers => odbc,asterisk

;sippeers => odbc,asterisk

La primera línea debe indicar el tipo de conexión y base de datos que estamos usando en este caso mysql, luego Asterisk es el nombre de la base de datos y sipfriends en el nombre de la tabla, obviamente cambiando estas dos líneas queda de la siguiente manera:

```
sipusers => mysql,asterisk1,sipfriends
sippeers => mysql,asterisk1,sipfriends
```

Por último recargamos la configuración de Asterisk y verificamos que toda la configuración esté bien en nuevo sistema con soporte Realtime esto significa que solo tendremos que modificar la base de datos y los cambios serán activados en línea, la información de los anexos y peers estará reflejada directamente en la tabla "**sipfriends"**.

```
/etc/init.d/asterisk reload
asterisk –rvvvvvvvvvvv
CLI> realtime mysql status
```

Se ha comprobado la conexión a Asterisk por el puerto **3306** con el usuario **userealtime.**

En este modulo se afirma que la configuración de Asterisk en realtime es decir en “tiempo real” es de gran ventaja para obtener Alta disponibilidad, con esto es posible la administración del sistema desde cualquier aplicación externa, ya que podemos almacena y acceder a la información de una base de datos, en este caso MySQL.

ANEXO 5

ARCHIVOS DE CONFIGURACIÓN

DE DUNDi

ANEXO 5.

ARCHIVOS DE CONFIGURACIÓN DE DUNDi

dundi.conf

Sección [general]

Para pc1.telefonicanet.com:

```
[general]
department=CENTRAL01
organization=Cisco
locality=Riobamba
stateprov=Chimborazo
country=EC
email=info@telefonicanet.com
phone=+593-0000000
; Aqui podemos definir en que red va a escuchar dundi
bindaddr=0.0.0.0
; El puerto en el que va a escuchar, por defecto 4520
port=4520
; Aqui nos identificamos con nuestra MAC address
entityid= 00:0C:29:DA:73:F8
; El numero de consultas que hará DUNDI hasta alcanzar una extensión
ttl=32
; Finaliza las conexiones fallidas
autokill=yes
```

Para pc2.telefonicanet.com:

```
[general]
department=CENTRAL02
organization=Cisco
locality=Riobamba
stateprov=Chimborazo
country=EC
email=info@telefonicanet.com
phone=+593-0000000
;Aqui podemos definir en que red va a escuchar dundi
bindaddr=0.0.0.0
; El puerto en el que va a escuchar, por defecto 4520
port=4520
; Aqui nos identificamos con nuestra MAC address
entityid= 00:0C:29:42:02:00
; El numero de consultas que hará DUNDI hasta alcanzar una extensión
ttl=32;
; Finaliza las conexiones fallidas
autokill=yes
```

Para pc3.telefonicanet.com:

```
[general]
department=CENTRAL03
organization= Cisco
locality=Riobamba
stateprov=Chimborazo
country=EC
email=info@telefonicanet.com
phone=+593-0000000
;Aqui podemos definir en que red va a escuchar dundi
bindaddr=0.0.0.0
; El puerto en el que va a escuchar, por defecto 4520
port=4520
; Aqui nos identificamos con nuestra MAC address
entityid= 00:0C:29:76:5A:B5
; El numero de consultas que hará DUNDI hasta alcanzar una extensión
ttl=32;
; Finaliza las conexiones fallidas
autokill=yes
```

Para pc4.telefonicanet.com:

```
[general]
department=CENTRAL04
organization= Cisco
locality=Riobamba
stateprov=Chimborazo
country=EC
email=info@telefonicanet.com
phone=+593-0000000
;Aqui podemos definir en que red va a escuchar dundi
bindaddr=0.0.0.0
; El puerto en el que va a escuchar, por defecto 4520
port=4520
; Aqui nos identificamos con nuestra MAC address
entityid= 00:0C:29:18:E2:45
; El numero de consultas que hará DUNDI hasta alcanzar una extensión
ttl=32;
; Finaliza las conexiones fallidas
autokill=yes
```

Sección [mappings]

Para pc1.telefonicanet.com:

```
[mappings]
priv => exten_SIP,0,IAX2,dundi:${SECRET}@192.168.137.161/${NUMBER},nopartial
;
; Identificamos al servidor 2 (CENTRAL02) por su entityid
[00:0C:29:42:02:00]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL02
host=172.30.124.202
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 3 (CENTRAL03) por su entityid
[00:0C:29:76:5A:B5]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL03
host=172.30.124.203
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 4 (CENTRAL04) por su entityid
[00:0C:29:18:E2:45]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL04
host=172.30.124.204
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
```

```
[mappings]
priv => exten_SIP,0,IAX2,dundi:${SECRET}@192.168.137.162/${NUMBER},nopartial
;
; Identificamos al servidor 1 (CENTRAL01) por su entityid
[00:0C:29:DA:73:F8]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL01
host=172.30.124.201
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 3 (CENTRAL03) por su entityid
[00:0C:29:76:5A:B5]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL03
host=172.30.124.203
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 4 (CENTRAL04) por su entityid
[00:0C:29:18:E2:45]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL04
host=172.30.124.204
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
```

```
[mappings]
priv => exten_SIP,0,IAX2,dundi:${SECRET}@192.168.137.163/${NUMBER},nopartial
;
; Identificamos al servidor 1 (CENTRAL01) por su entityid
[00:0C:29:DA:73:F8]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL01
host=172.30.124.201
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 2 (CENTRAL02) por su entityid
[00:0C:29:42:02:00]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL02
host=172.30.124.202
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 4 (CENTRAL04) por su entityid
[00:0C:29:18:E2:45]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL04
host=172.30.124.204
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
```

```
[mappings]
priv => exten_SIP,0,IAX2,dundi:${SECRET}@192.168.137.164/${NUMBER},nopartial
;
; Identificamos al servidor 1 (CENTRAL01) por su entityid
[00:0C:29:DA:73:F8]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL01
host=172.30.124.201
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 2 (CENTRAL02) por su entityid
[00:0C:29:42:02:00]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL02
host=172.30.124.202
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
; Identificamos al servidor 3 (CENTRAL03) por su entityid
[00:0C:29:76:5A:B5]
;permitir y realizar conexiones
model=symmetric
; IP ser servidor CENTRAL03
host=172.30.124.203
inkey=SERVERS-DUNDI
outkey=SERVERS-DUNDI
; Incluimos el contexto antes definido en la sección mappings
include=priv
permit=priv
qualify=yes
order=primary
```

iax_custom.conf

```
[dundi]
type=user
context=ext_DUNDi
dbsecret=dundi/secret
; Podemos restringir ciertos codecs para mejorar la calidad
; de voz, o dar prioridad al ancho de banda (con gsm o g729)
disallow=all
allow=ulaw
allow=alaw
allow=gsm
```

sip_general_additional.conf

```
vmexten=*97
disallow=all
allow=ulaw
allow=alaw
context=ext_local_SIP
bindaddr=0.0.0.0
srvlookup=yes
regcontext=sipregistration
rtcachefriends=yes
callerid=Unknown
notifyringing=yes
notifyhold=yes
limitonpeers=yes
tos_sip=cs3
tos_audio=ef
tos_video=af41
alwaysauthreject=yes
```

sip_custom.conf

```
sipregistration=ext_local_SIP
```

extensions.conf

```
[ext_DUNDi]
exten => _X.,1,Goto(ext_local_SIP,${EXTEN},1)
[context_internal]
include => lookup_to_DUNDi
include => ext_local_SIP
[lookup_to_DUNDi]
switch => DUNDi/priv
[ext_local_SIP]
; Esta es la contexto que llamamos desde el contexto [lookup_to_DUNDi]
; Tambien evita que hayan loops en las consultas dundi.
;switch => Realtime/sipfriends
exten => _X.,1,Dial(SIP/${EXTEN})
exten => _X.,2,Hangup
```

Certificados de encriptación

Para pc1.telefonicanet.com:

```
# cd /var/lib/asterisk/keys
astgenkey -n SERVERS-DUNDI
```

Copiar hacia pc2.telefonicanet.com:

```
[root@pc1 ~]# scp /var/lib/asterisk/keys/SERVERS-DUNDI.* \
172.30.124.202:/var/lib/asterisk/keys
```

Copiar hacia pc3.telefonicanet.com:

```
[root@pc1 ~]# scp /var/lib/asterisk/keys/SERVERS-DUNDI.* \
172.30.124.203:/var/lib/asterisk/keys
```

Copiar hacia pc4.telefonicanet.com:

```
[root@pc1 ~]# scp /var/lib/asterisk/keys/SERVERS-DUNDI.* \
172.30.124.204:/var/lib/asterisk/keys
```

Aplicar la configuración

```
# amportal restart
```

O

```
# Service asterisk restart
```

ANEXO 6

INSTALACIÓN Y CONFIGURACIÓN DE HEARTBEAT Y DRBD

ANEXO 6.

INSTALACIÓN Y CONFIGURACIÓN DE HEARTBEAT Y DRBD

A continuación se explica cómo instalar drbd y heartbeat y como configurar este servicio para tener siempre disponible un equipo servidor y en el caso de una caída del mismo que otro pueda tomar su lugar sin que el usuario cliente perciba alguna anomalía (de ser posible).

Material requerido

Hardware:
Servidores: 2 máquinas idénticas
1 GB RAM
10 HD 160 GB RAID

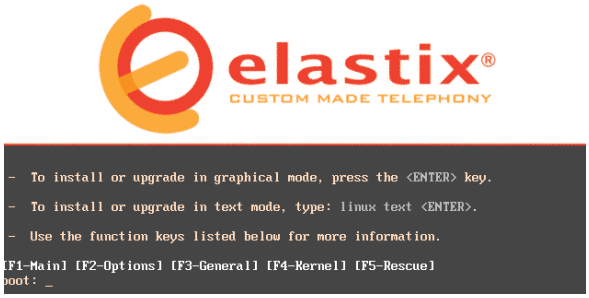
Software:
SO: CenOS 5.4, Elastix 2.0
HA: drbd8 y heartbeat

Particiones:
- 100 MB /boot ext3 primaria
- 6144 MB / ext3 primaria
- 1 GB /tmp ext3 primaria
- 3072 MB swap lógica
- 15 GB no montar

Una vez realizadas las instalaciones básicas y securizadas las máquinas, los siguientes pasos a dar serían:

Pasos que se deben realizar en los servidores primarios y secundarios.

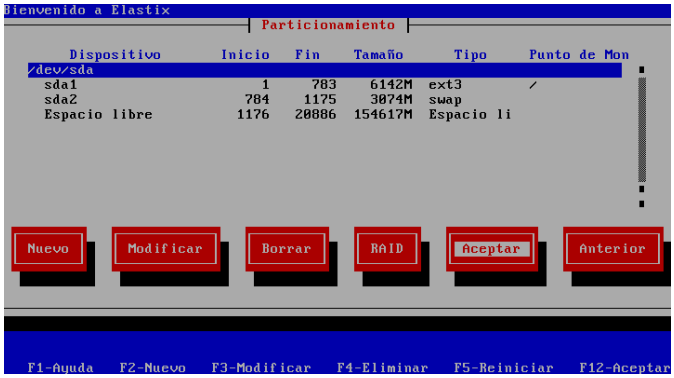
1. Arranque Elastix-2.0del CD de instalación



2. En el menú de inicio tipo "avanzado" y entrar

3. Durante la rutina de instalación elige manejar particiones manualmente duro. La siguiente es basado en un160,0GBSATA
   • Creación de raíz (/), ext3con6144MB(sda1)
   • Crear una partición swap con3072MB(sda2)

4. El resto de la rutina de instalación es estándar.



5. Después de la instalación y el arranque realizar la actualización. Actualizar el sistema operativo. Para realizar la actualización se ejecuta:
   - yum –y update

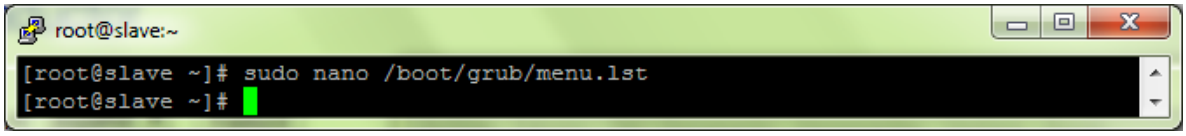
6. Asegúrese que para arrancar el fichero / boot/grum/menu.lst del kernel no-xen a menos que necesite el kernel de Xen.

http://elanalista.wordpress.com/2007/01/08/editar-menu-de-grub/

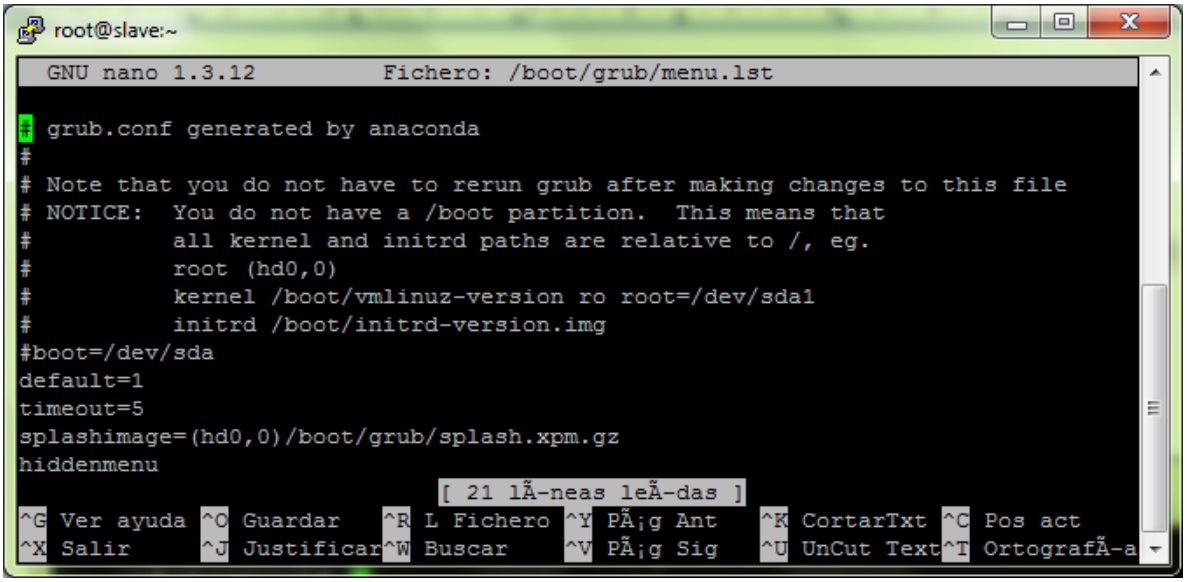
- default=1

El archivo de configuración del menú es: /boot/grub/menu.lst
Antes de hacer ningún cambio sería buena idea hacer una copia de seguridad de nuestro menú, por lo que pudiera pasar. Para ello ejecutaremos en un terminal la siguiente orden:
cp /boot/grub/menu.lst /boot/grub/menu.lst_original

Con lo que nos hará una copia del archivo menu.lst con el nombre menu.lst_original.
Ahora sí podemos empezar, abriremos el archivo de configuración usando nuestro editor de texto favorito, yo usaré nano:
nano /boot/grub/menu.lst

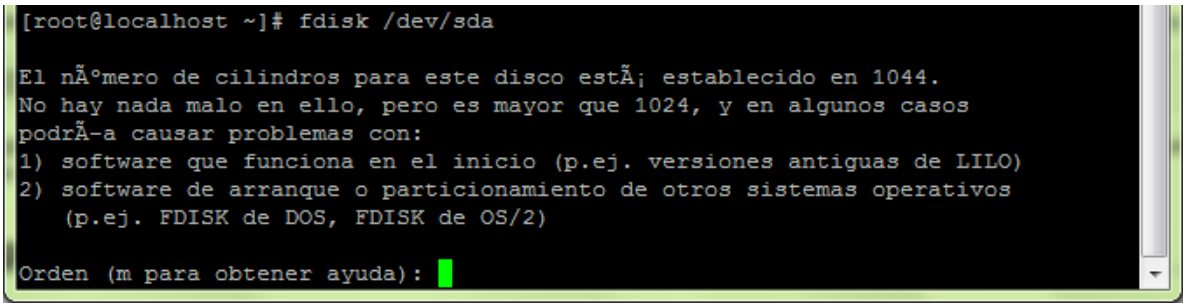


Con lo que veremos un archivo similar a este:



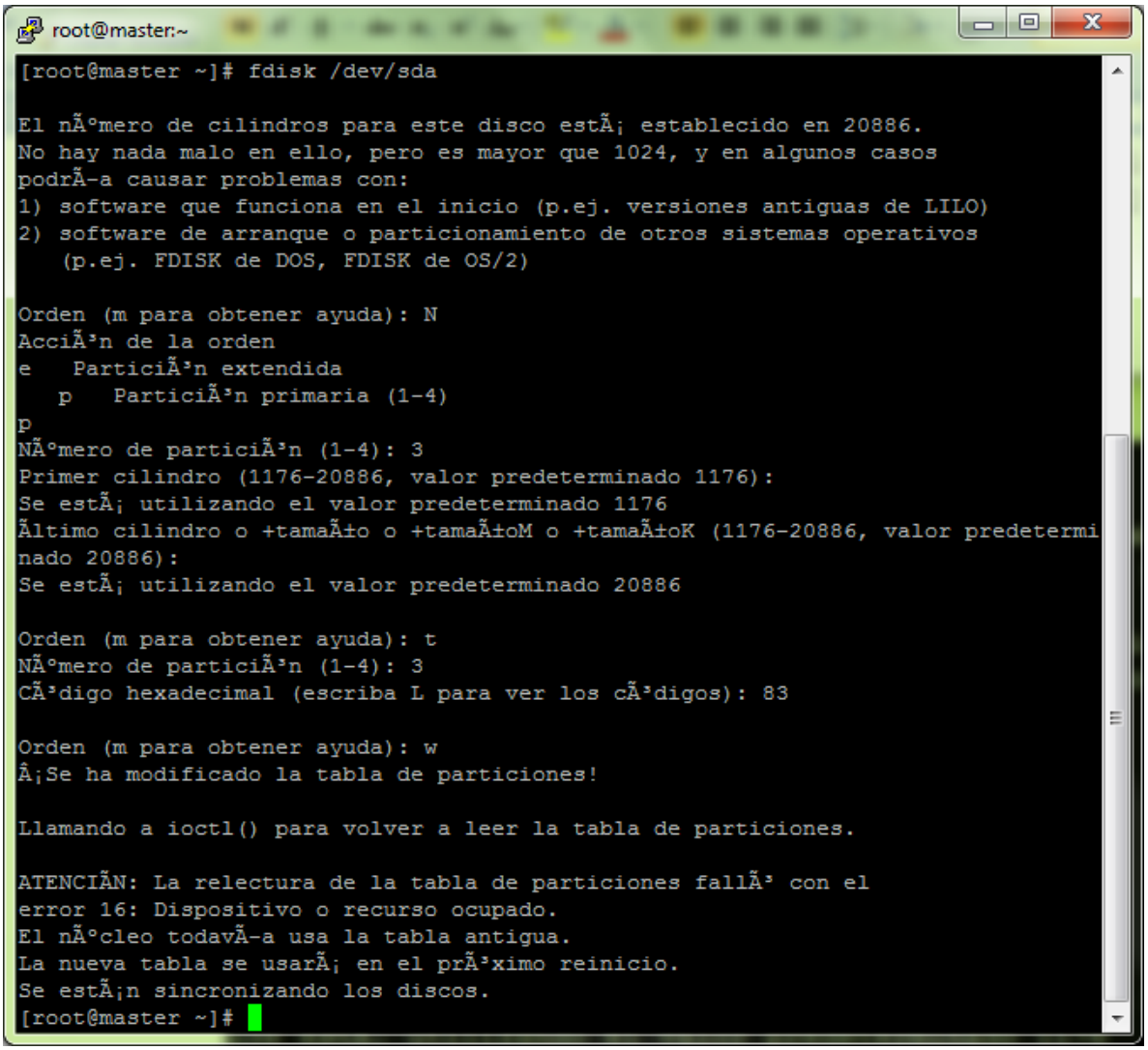
Para guardar los cambios
ctrl+x
enter
S
Enter

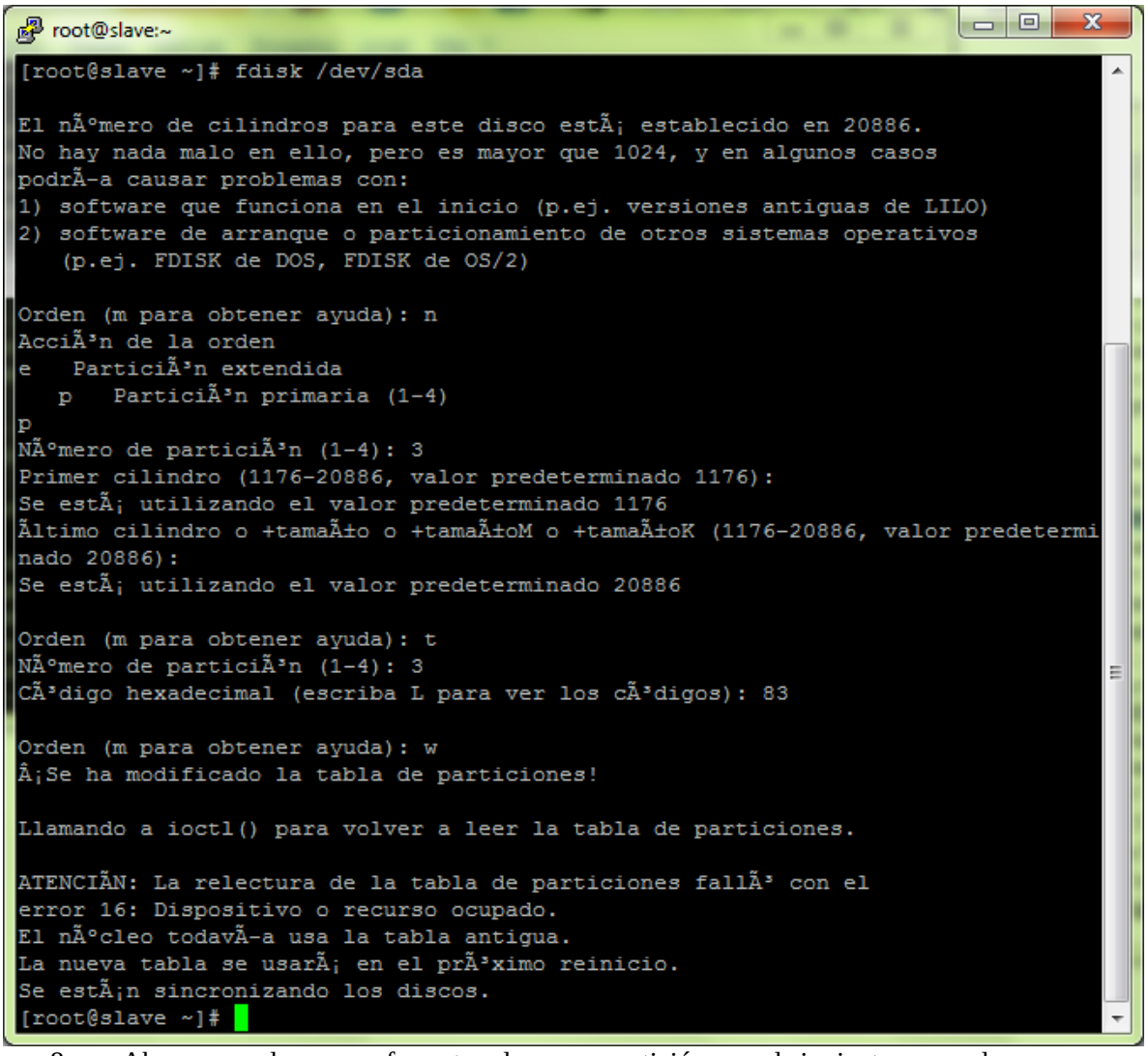
7. Ahora vamos a crear la partición que contendrá los datos que se replicaran, para esto ejecutamos el comando:
fdisk /dev/sda



Pasos

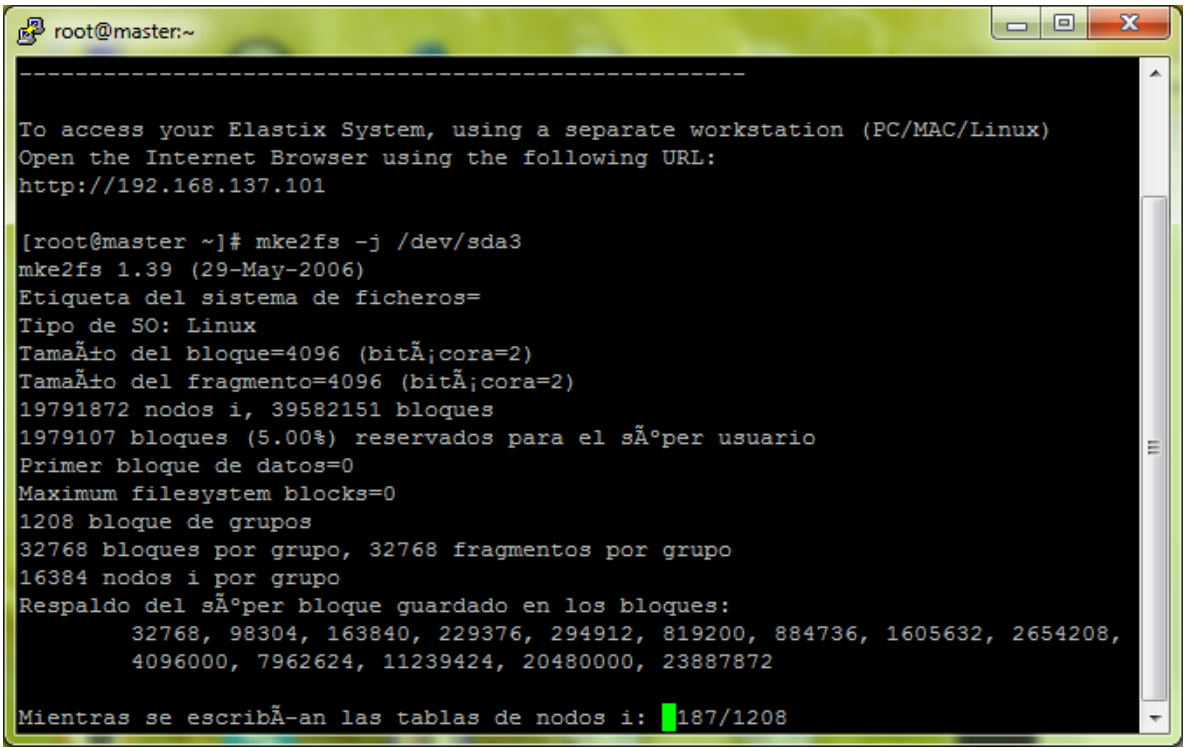
1.- Presionamos la letra n (add a new partition)
2.- Presionamos la letra p (Primarypartition)
3.- Escribimos el número 3 (Partitionnumber)
4.- Presionamos Enter un par de veces hasta que nos aparezca el Command de nuevo.
5.- Luego presionamos la letra t para cambiar el id del sistema de particiones.
6.- Escribimos la partición 3.
7.- En HEX code escribimos 83 que es la partición de Linux
8.- Por ultimo escribimos la letra w para salvar los cambios.
9.- Después reiniciamos el servidor para que la nueva tabla esté disponible.


root@master:~
[root@master ~]# fdisk /dev/sda
El nÃºmero de cilindros para este disco estÃ¡ establecido en 20886.
No hay nada malo en ello, pero es mayor que 1024, y en algunos casos
podrÃ-a causar problemas con:
1) software que funciona en el inicio (p.ej. versiones antiguas de LILO)
2) software de arranque o particionamiento de otros sistemas operativos
(p.ej. FDISK de DOS, FDISK de OS/2)
Orden (m para obtener ayuda): N
AcciÃ³n de la orden
e ParticiÃ³n extendida
p ParticiÃ³n primaria (1-4)
p
NÃºmero de particiÃ³n (1-4): 3
Primer cilindro (1176-20886, valor predeterminado 1176):
Se estÃ¡ utilizando el valor predeterminado 1176
Ãltimo cilindro o +tamaÃ±o o +tamaÃ±oM o +tamaÃ±oK (1176-20886, valor predetermi
nado 20886):
Se estÃ¡ utilizando el valor predeterminado 20886
Orden (m para obtener ayuda): t
NÃºmero de particiÃ³n (1-4): 3
CÃ³digo hexadecimal (escriba L para ver los cÃ³digos): 83
Orden (m para obtener ayuda): w
Â¡Se ha modificado la tabla de particiones!
Llamando a ioctl() para volver a leer la tabla de particiones.
ATENCIÃN: La relectura de la tabla de particiones fallÃ³ con el
error 16: Dispositivo o recurso ocupado.
El nÃºcleo todavÃ-a usa la tabla antigua.
La nueva tabla se usarÃ¡ en el prÃ³ximo reinicio.
Se estÃ¡n sincronizando los discos.
[root@master ~]#

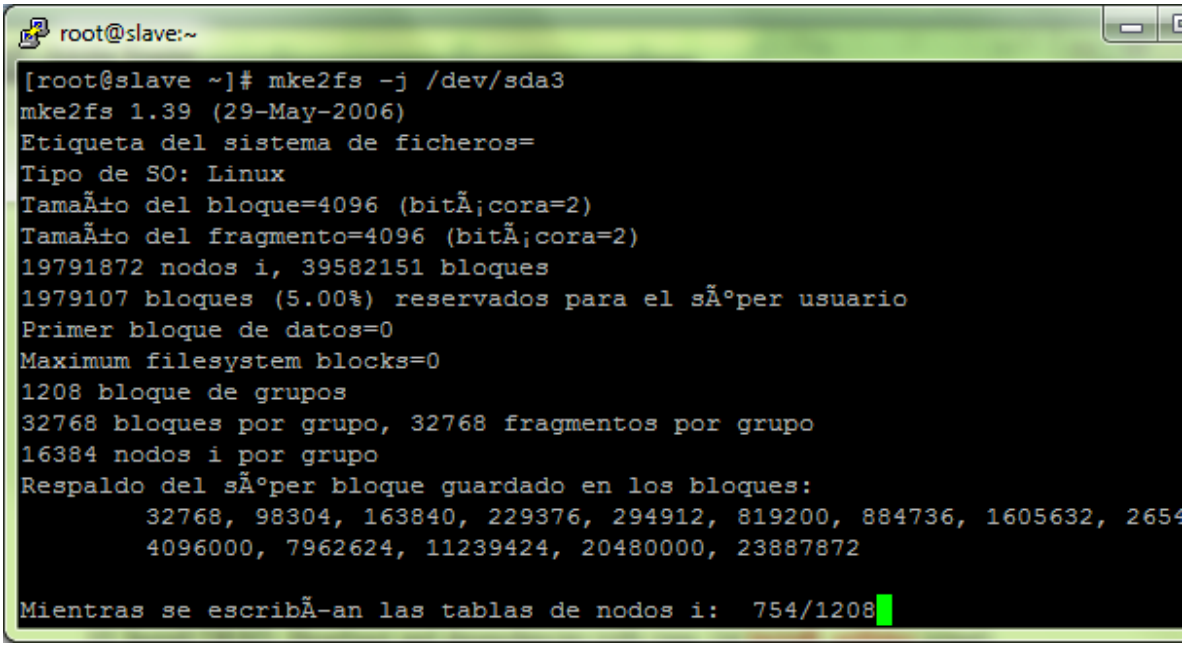


8. Ahora procederemos a formatear la nueva partición con el siguiente comando:

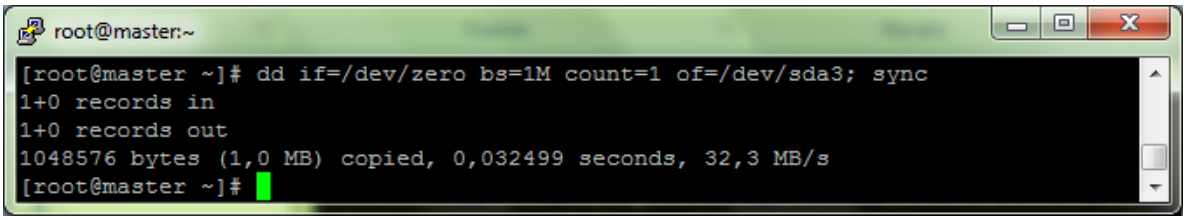
mke2fs -j /dev/sda3

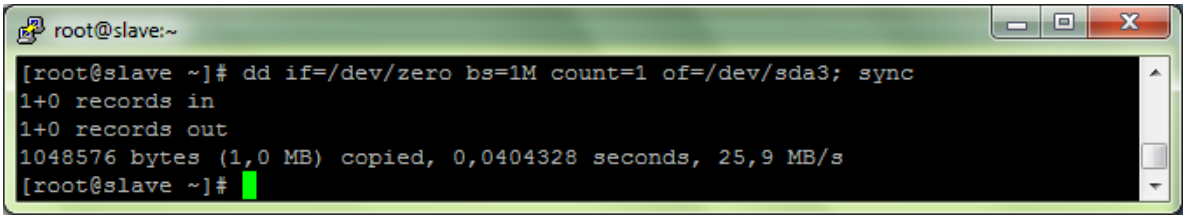


Slave



9. Ahora hay que eliminar el sistema de archivos desde el disco que acabamos de crear dd if=/dev/zero bs=1M count=1 of=/dev/sda3; sync





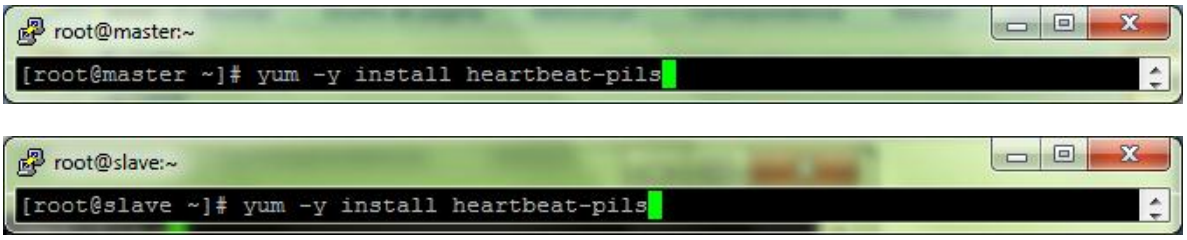
10. Instalamos DRBD, Heartbeat y dependencias con yum.

yum -y installdrbd

yum -y install kmod-drbd82

yum -y installOpenIPMI-libs

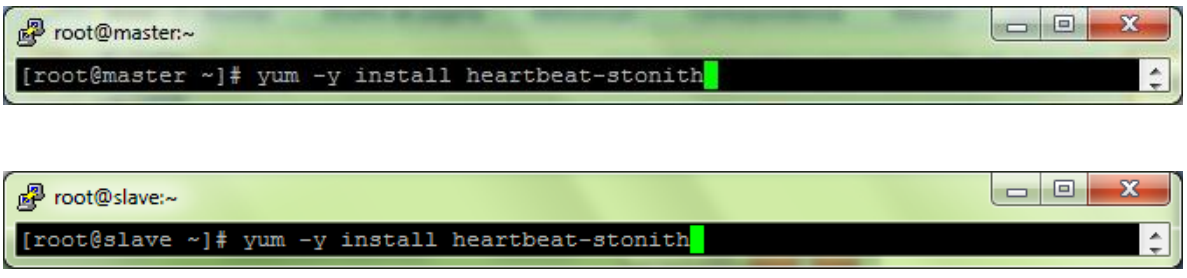
yum -y installheartbeat-pils



yum -y installopenhpi

yum -y install heartbeat

yum -y installheartbeat-stonith



11. Para garantizar la correcta nombre de host IP de la resolución se recomienda que actualice manualmente el archivo / etc / hosts para reflejar una asignación correcta de host-a-IP.

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
192.168.137.101                 master.telefonicanet.com
192.168.137.102                 slave.telefonicanet.com
127.0.0.1               master.telefonicanet.com
::1                     localhost6.localdomain6 localhost6
```

SLAVE

```
# Do not remove the following line, or various programs
# that require network functionality will fail.
192.168.137.101                  master.telefonicanet.com
192.168.137.102                  slave.telefonicanet.com
127.0.0.1               slave.telefonicanet.com
::1                     localhost6.localdomain6 localhost6
```

12. DRBD nos permite escribir la partición declarada en ambos miembros de la agrupación. En nuestro caso / dev/sda3. Para que esto suceda tenemos que crear una partición virtual llamado / dev/drbd0.

13. Editar el archivo / etc / drbd.conf en ambos servidores primarios y secundarios. drbd.conf archivo debe ser idéntico en ambos servidores.

Configuración de DRBD

Esto en ambos servidores
/etc/drbd.con

```
#
# please have a a look at the example configuration file in
# /usr/share/doc/drbd/drbd.conf
#
resource "r0" {
protocol A;
disk { on-io-error pass_on; }
startup { wfc-timeout 5; degr-wfc-timeout 3; }
syncer { rate 100M; }
onmaster.telefonicanet.com {
device /dev/drbd0;
disk /dev/sda3;
address 192.168.137.101:7789;
meta-disk internal;
        }
on slave.telefonicanet.com {
device /dev/drbd0;
disk /dev/sda3;
address 192.168.137.102:7789;
meta-disk internal;
}
   }
```

14. Antes de seguir se debe de cambiar el nombre del servidor en la interface web de Elastix

15. Ahora vamos a crear la partición virtual / dev/drdb0 en ambos servidores

    drbdadm create-md r0

```
--== This is a new installation of DRBD ==--
Please take part in the global DRBD usage count at
http://usage.drbd.org.

The counter works anonymously. It creates a random number to identify
your machine and sends that random number, along with
DRBD's version number, to usage.drbd.org.

The benefits for you are:
 * In response to your submission, the server (usage.drbd.org) will tell
you
how many users before you have installed this version (8.2.6).
 * With a high counter LINBIT has a strong motivation to
continue funding DRBD's development.

http://usage.drbd.org/cgi-
bin/insert_usage.pl?nu=16759413772803331981&git=3e69822d3bb4920a8c1bfdf7
d647169eba7d2eb4

In case you want to participate but know that this machine is
firewalled,
simply issue the query string with your favorite web browser or wget.
You can control all of this by setting 'usage-count' in your drbd.conf.

* You may enter a free form comment about your machine, that gets
used on usage.drbd.org instead of the big random number.
* If you wish to opt out entirely, simply enter 'no'.
* To count this node without comment, just press [RETURN]

--==  Thank you for participating in the global usage survey  ==--
The server's response is:

you are the 19977th user to install this version

From now on, drbdadm will contact usage.drbd.org only when you update
DRBD or when you use 'drbdadm create-md'. Of course it will continue
to ask you for confirmation as long as 'usage-count' is at its default
value of 'ask'.

Just press [RETURN] to continue:
v08 Magic number not found
v07 Magic number not found
v07 Magic number not found
v08 Magic number not found
Writing meta data...
initialising activity log
NOT initialized bitmap
New drbdmeta data block sucessfully created.
```

```
--=== Creating metadata ===--
As with nodes, we count the total number of devices mirrored by
DRBD at
at http://usage.drbd.org.

The counter works anonymously. It creates a random number to
identify
the device and sends that random number, along with
DRBD's version number, to usage.drbd.org.

http://usage.drbd.org/cgi-
bin/insert_usage.pl?nu=13574562491563078845&ru=2141960357920203354&
rs=162128494080

* If you wish to opt out entirely, simply enter 'no'.
* To continue, just press [RETURN]

success

-----------------
```

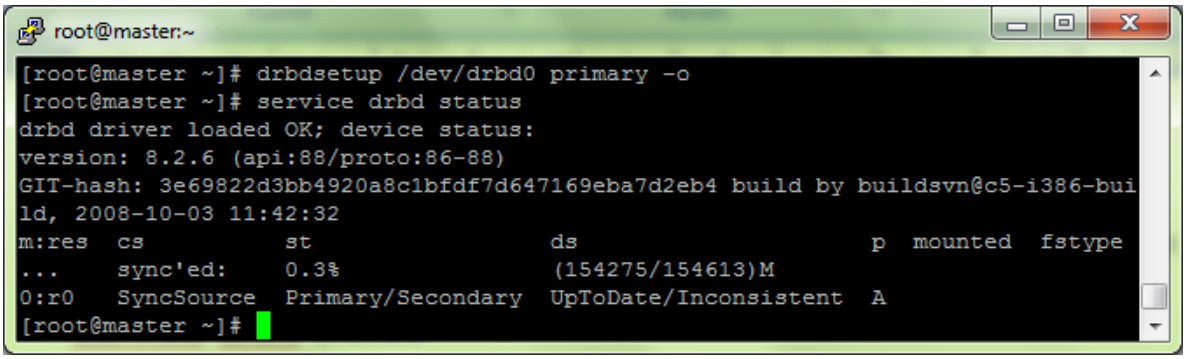
16. Inicio servicio drbd en ambos servidores para iniciar el proceso de sincronización.
    service drbd start

17. Verificar proceso de sincronización con el siguiente comando
    service drbd status

Inicialmente, ambos servidores son "secundarios". Tenemos que asignar, cual es el' principal'. Escriba el siguiente comando sólo en el servidor principal

drbdsetup /dev/drbd0 primary -o

Compruebe drbd estado de nuevo con servicio drbd estado. Usted debe obtener un estatus similar al siguiente



Podemos determinar la unción de un servidor mediante la ejecución de los siguientes

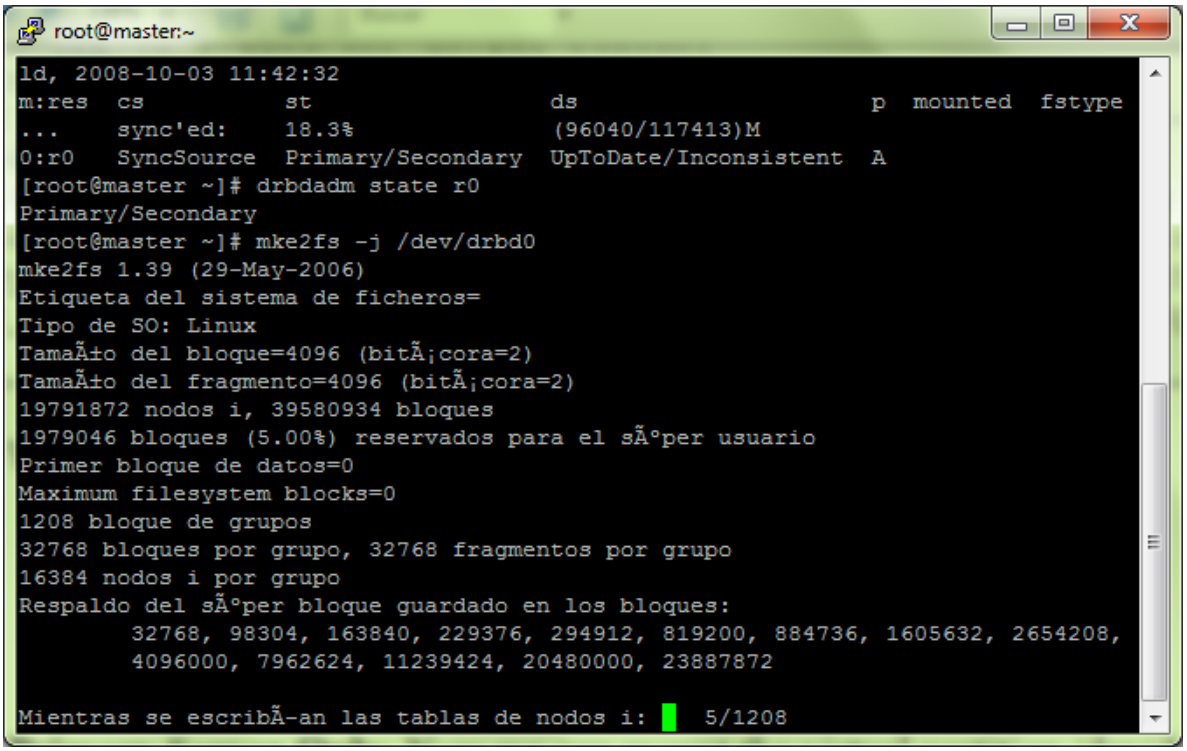
drbdadm state r0

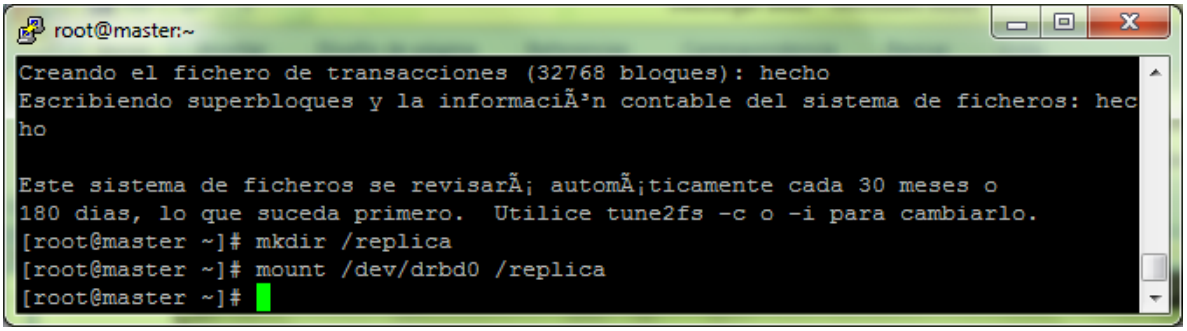
The primary server should return;

drbdadm state r0

Sólo el servidor primario: Ahora podemos montar la partición virtual /dev/drbd0, pero primero tenemos que formatear la partición con ext3 con el siguiente comando "Después de reiniciar los dos servers."

mke2fs –j /dev/drbd0
mkdir /replica
mount /dev/drbd0 /replica





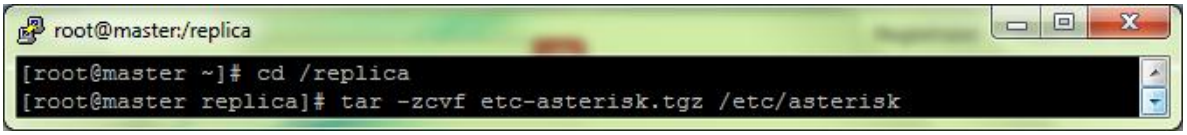
Sólo el servidor primario: Ahora vamos a copiar todos los directorios que quieres sincronizar entre los dos servidores a nuestra nueva partición, eliminar los directorios originales y crear enlaces simbólicos para reemplazarlos.
Directorios de interés;

- /etc/asterisk
- /var/lib/asterisk
- /usr/lib/asterisk
- /var/spool/asterisk
- /var/lib/mysql
- /var/log/asterisk

- /var/www

Copiar, eliminar y vincular. (O create_directories script que automatiza este paso)

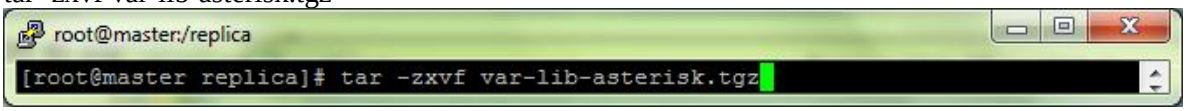
cd /replica
tar -zcvf etc-asterisk.tgz /etc/asterisk



tar -zxvf etc-asterisk.tgz

tar -zcvf var-lib-asterisk.tgz /var/lib/asterisk

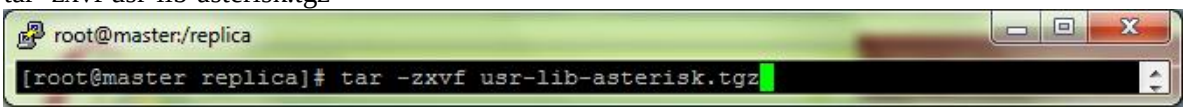
tar -zxvf var-lib-asterisk.tgz



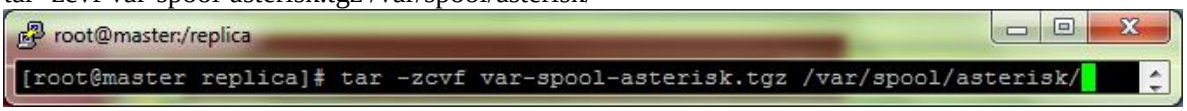
tar -zcvf usr-lib-asterisk.tgz /usr/lib/asterisk/

tar -zcvf var-www.tgz /var/www/

tar -zxvf usr-lib-asterisk.tgz



tar -zcvf var-spool-asterisk.tgz /var/spool/asterisk/



tar -zxvf var-spool-asterisk.tgz

tar -zcvf var-lib-mysql.tgz /var/lib/mysql/

tar -zxvf var-lib-mysql.tgz

tar -zcvf var-log-asterisk.tgz /var/log/asterisk/

tar -zxvf var-log-asterisk.tgz

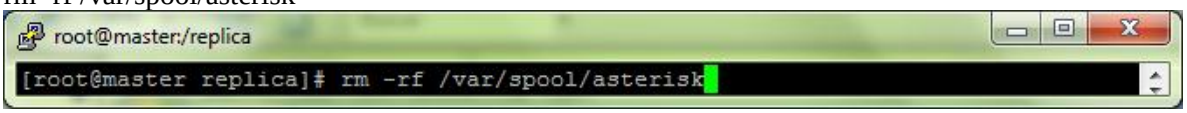
tar -zxvf var-www.tgz

rm -rf /etc/asterisk

rm -rf /var/lib/asterisk

rm -rf /usr/lib/asterisk/

rm -rf /var/spool/asterisk

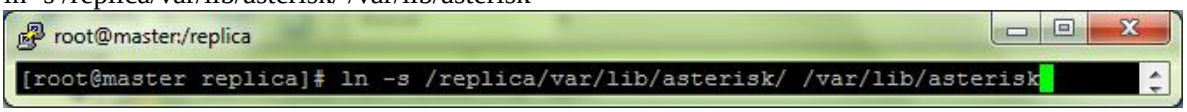


rm -rf /var/lib/mysql/

rm -rf /var/log/asterisk/

ln -s /replica/etc/asterisk/ /etc/asterisk

ln -s /replica/var/lib/asterisk/ /var/lib/asterisk

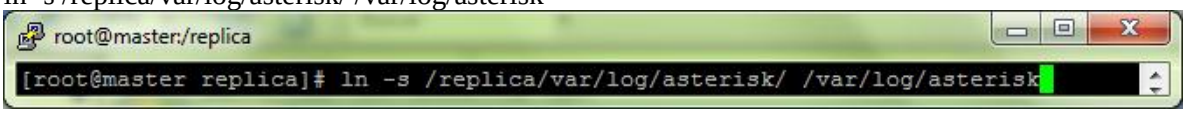


ln -s /replica/usr/lib/asterisk/ /usr/lib/asterisk

ln -s /replica/var/spool/asterisk/ /var/spool/asterisk

ln -s /replica/var/lib/mysql/ /var/lib/mysql

ln -s /replica/var/log/asterisk/ /var/log/asterisk



ln -s /replica/var/www /var/www

Configuración Heartbeat

Recuerde detener cualquier servicio que debe ser controlado por el Heartbeat.
Estos servicios serán controlados por Heartbeat en el servidor que tiene el control

chkconfig asterisk off
chkconfig mysqld off
chkconfig httpd off

Ahora tenemos que crear tres archivos de configuración:

- ha.cf
- authkeys
- haresources

Editar el archivo /etc/ha.d/ha.cf. Este es un sencillo archivo de configuración que proporciona todas nuestras funcionalidades requeridas.

En el servidor master:

nano /etc/ha.d/ha.cf

debugfile /var/log/ha-debug
logfile /var/log/ha-log
logfacility local0
keepalive 2
deadtime 20
warntime 10
initdead 40
udpport 694
bcast eth0 192.168.137.102
auto_failback off
node master.telefonicanet.com
node slave.telefonicanet.com

En el servidor slave:

nano /etc/ha.d/ha.cf

debugfile /var/log/ha-debug
logfile /var/log/ha-log
logfacility local0
keepalive 2
deadtime 20
warntime 10
initdead 40

udpport 694
bcast eth0 192.168.137.101
auto_failback off
node master.telefonicanet.com
node slave.telefonicanet.com
Editar el archivo / etc / ha.d / haresources. Aquí es donde se especifica que es nuestro servidor principal, el nombre de la partición DRBD vamos a montar y donde, nuestra flota dirección IP(10.1.1.3 en este ejemplo en eth1 con una máscara de subred de 24 bits) y los scripts de init.d se pondrá en marcha durante una conmutación por error o un cambio (fonulator, asterisco, mysqld,httpd)

nano /etc/ha.d/haresources

master.telefonicanet.com drbddisk::r0
Filesystem::/dev/drbd0::/replica::ext3
IPaddr::192.168.137.103/24/eth1/192.168.137.255 asterisk mysqldhttpd

Editar el archivo / etc / ha.d / authkeys. Esto proporciona un nivel de seguridad y autenticación entre los nodos.

nano /etc/ha.d/authkeys

auth 1
1 sha1 password123456

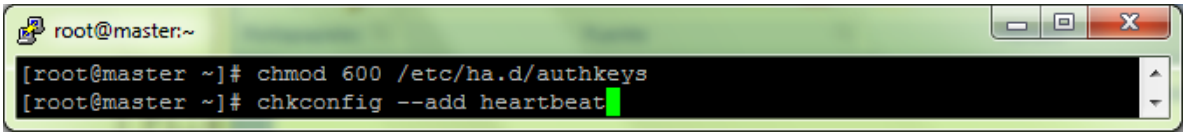
B!gb@dUndUglIp@$$werd

Cambiar permisos en el archivo / etc / ha.d / archivo authkeys

chmod 600 /etc/ha.d/authkeys

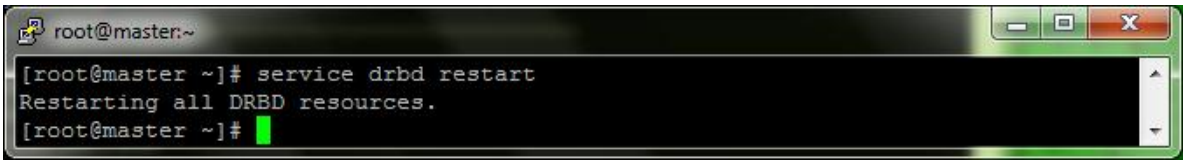
Configurar heartbeat para iniciar en el arranque

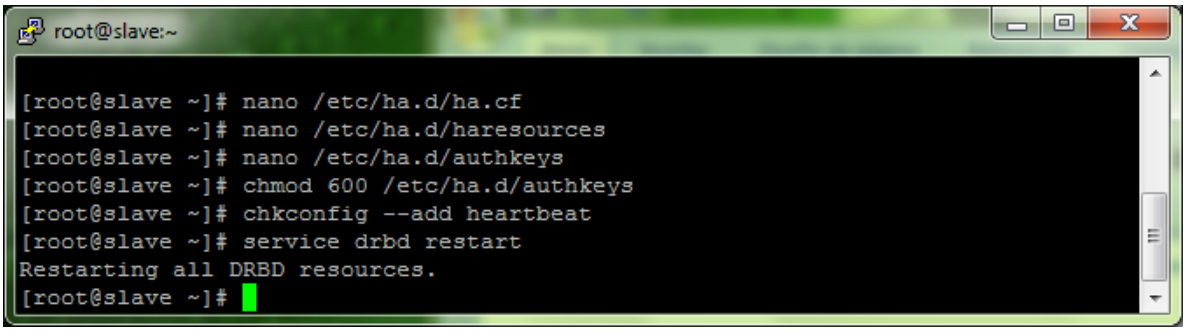
chkconfig --addheartbeat



Reinicie drbd en ambos servidores

service drbd restart





Compruebe que ambos servidores se encuentran actualmente en estado de secundaria

drbd adm state r0

- Result should be 'Secondary/Secondary' on both

Restaurar heartbeat

service heartbeat restart

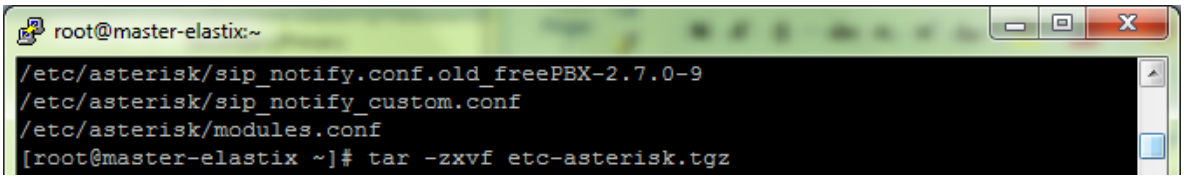
Espere un momento se vuelven a comprobar el estado de los servidores.

Procederemos a copiar dentro de /replica la data que queramos replicar, incluyendo archivos de configuración de servicios, en el caso de Elastix serian los siguientes directorios:

•/etc/asterisk
• /var/lib/asterisk
• /usr/lib/asterisk
• /var/spool/asterisk
• /var/lib/mysql
• /var/log/asterisk

A modo de ejemplo lo haremos con /etc/asterisk, así:
cd /replica
tar -zcvf etc-asterisk.tgz /etc/asterisk
tar -zxvf etc-asterisk.tgz

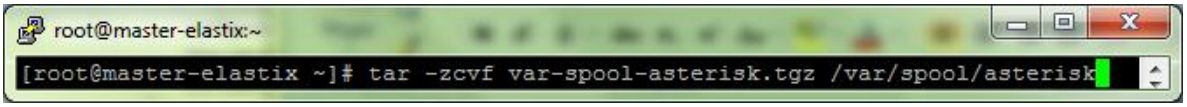
rm -rf /etc/asterisk
ln -s /replica/etc/asterisk /etc/asterisk

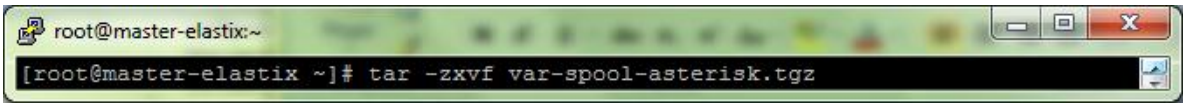


tar -zcvf var-lib-asterisk.tgz /var/lib/asterisk
tar -zxvfvar-lib-asterisk.tgz
rm -rf /var/lib/asterisk
ln -s /replica/var/lib/asterisk/var/lib/asterisk

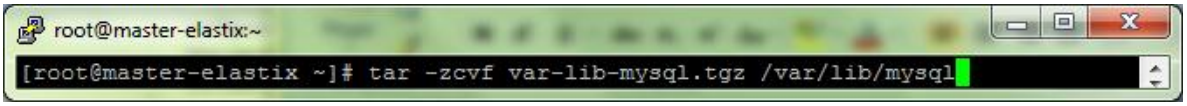
tar -zcvfusr-lib-asterisk.tgz /usr/lib/asterisk
tar -zxvfusr-lib-asterisk.tgz
rm -rf/usr/lib/asterisk
ln -s /replica/usr/lib/asterisk/usr/lib/asterisk

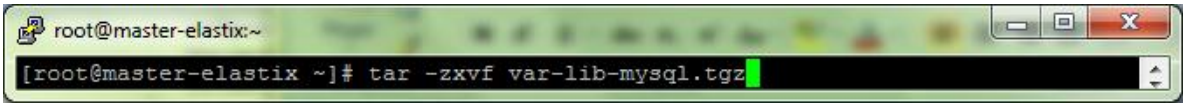
tar -zcvfvar-spool-asterisk.tgz /var/spool/asterisk
tar -zxvfvar-spool-asterisk.tgz
rm -rf/var/spool/asterisk
ln -s /replica/var/spool/asterisk/var/spool/asterisk





tar -zcvfvar-lib-mysql.tgz /var/lib/mysql
tar -zxvfvar-lib-mysql.tgz
rm -rf/var/lib/mysql
ln -s /replica/var/lib/mysql/var/lib/mysql





tar -zcvfvar-log-asterisk.tgz /var/log/asterisk
tar -zxvfvar-log-asterisk.tgz
rm -rf/var/log/asterisk
ln -s /replica/var/log/asterisk/var/log/asterisk

Recordar de reiniciar el servicio de mysql una vez finalizado este paso

service mysqld restart

service asterisk restart

service/var/lib/asterisk restart

• /var/lib/asterisk
• /usr/lib/asterisk
• /var/spool/asterisk
• /var/lib/mysql
• /var/log/asterisk

Lo mismo debemos hacer con los demás directorios.

Notas

Para declarar un nodo como primario (role)

drbdadmprimary r0
drbdsetup /dev/drbd0 primary-o

Para declara un nodo como secundario (role)

drbdadm secondary r0

Acordarse de que para declarar como secundario hay que desmontar la unida /replica) y antes de

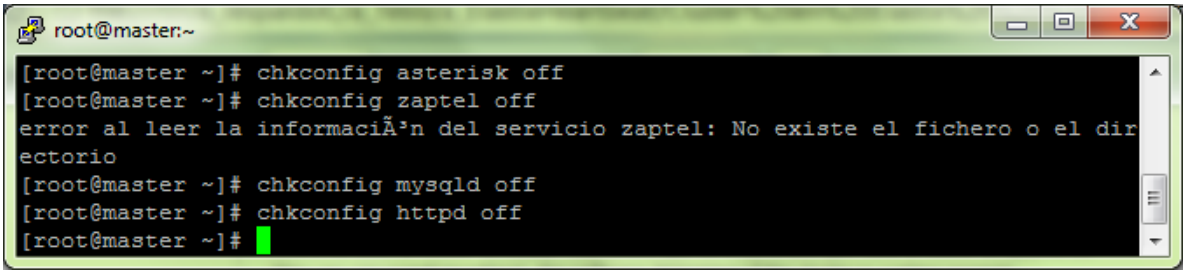
desmontarla detener el servicio de mysqld

umount /replica

Ahora se debe proceder a instalar Heartbeat, que es el software que hace el cluster propiamente.

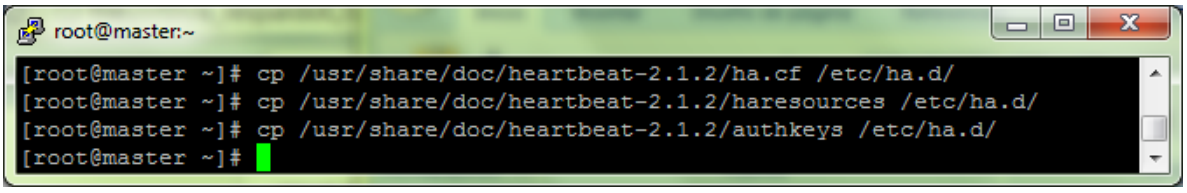
Configuracion de Heartbeat

Acordarse de apagar los servicios que se iniciaran con el heartbeat
chkconfig asterisk off
chkconfigzaptel off
chkconfigmysqld off
chkconfighttpd off



Esto se hace ya que el Heartbeat iniciara estos servicios cuando el servidor sea master. Debemos copiar los archivos de configuración de Heartbeat (http://www.linux/- ha.org/) de la documentación que viene con el paquete al directorio de configuración /etc/ha.d, asi:

cp /usr/share/doc/heartbeat-2.1.2/ha.cf /etc/ha.d/
cp /usr/share/doc/heartbeat-2.1.2/haresources /etc/ha.d/
cp /usr/share/doc/heartbeat-2.1.2/authkeys /etc/ha.d/



Ahora vamos a editar el archivo /etc/ha.d/ha.cf

cd /etc/ha.d
vi ha.cf

Y agregamos al final estas líneas:

debugfile /var/log/ha-debug
logfile /var/log/ha-log
logfacility local0

keepalive 2
deadtime 20
warntime 10
initdead 40
udpport 694
bcast eth0 # Linux
auto_failback off
node master.telefonicanet.com
node slave.telefonicanet.com

Luego el archivo /etc/ha.d/haresources
cd /etc/ha.d
viharesources

Y agregamos al final la línea:

master.telefonicanet.com drbddisk::r0 Filesystem::/dev/drbd0::/replica::ext3
IPaddr::192.168.137.2/24/eth0/192.168.137.3 asterisk mysqld httpd

Finalmente el archivo /etc/ha.d/authkeys

cd /etc/ha.d
vi authkeys

Y agregamos al final las líneas:

auth 1
1 sha1 elastix

Le damos el siguiente permiso al archivo /etc/ha.d/authkeys

cd /etc/ha.d
chmod 600 authkeys

Todos los archivos anteriores deben ser iguales en ambos servidores.

Configuramos heartbeat con soporte chkconfig, asi:

chkconfig –-add heartbeat

Ahora, antes de iniciar los servicios de heartbeat, debemos reiniciar el servicio drbd en ambos servidores, así:

service drbd restart

Verificamos que ambos servidores se encuentren en estado Secundario, así:

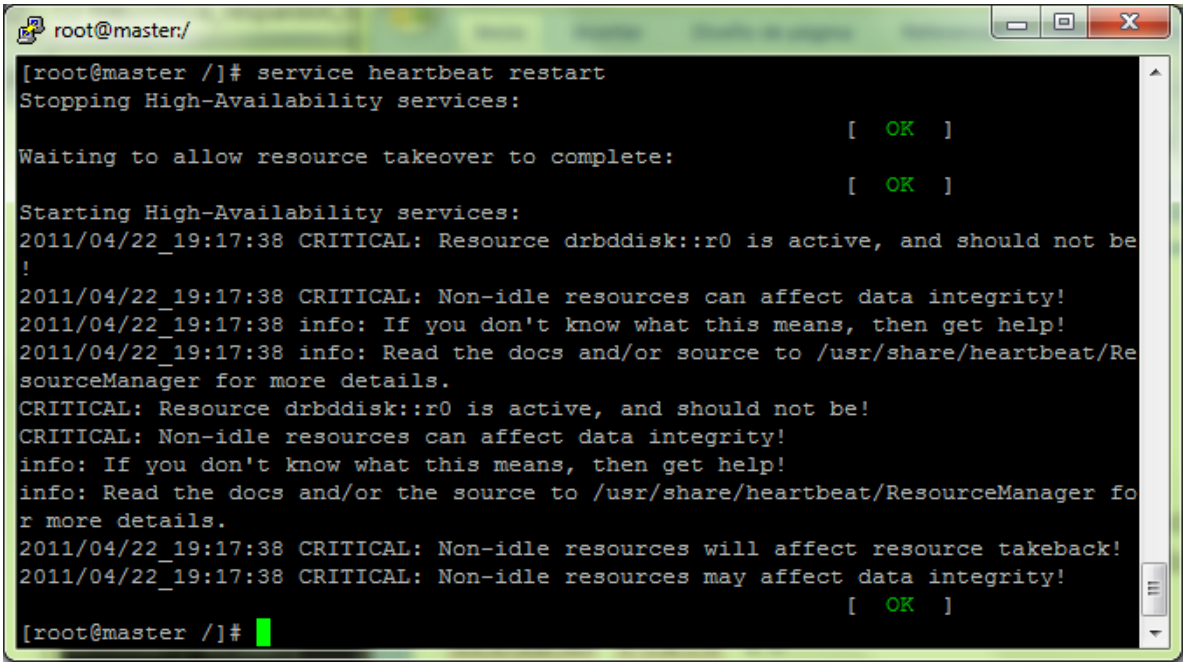
drbdadmstate r0

[root@master-elastix ~]# drbdadmstate r0
Secondary/Secondary

Si es así, procedemos a levantar el servicio heartbeat, así:

service heartbeat start

Una vez hecho esto, esperaremos unos momentos hasta que heartbeat monte la partición /replica en el servidor Primario, lo verificamos así:



drbdadmstate r0

[root@master-elastix ~]# drbdadmstate r0
Primary/Secondary

df -h

[root@master-elastix ~]# df -h
FilesystemSizeUsedAvail Use% Mountedon
/dev/hdc1 9.5G 1.5G 7.6G 17% /
tmpfs 501M 0 501M 0% /dev/shm

/dev/drbd0 9.2G 150M 8.6G 2% /replica

La partición /replica solo se montara en el servidor cuyo estado sea Primario, es decir, si por algún motivo el servidor master-elastix.com falla entonces slave- elastix.com asumirá el estado de Primario y por ende levantara la partición /replica, la cual contendrá la información replicada entre ambos equipos.

Esperar a que termine de hacer la sincronización de los dos servidores, este proceso se puede observar con el comando:

watchcat /proc/drbd

Cuanto tenemos los dos nodos en modo stand alone, con un cs:StandAlonest:Secondary/Unknownds:UpToDate/DUnknown lo más probable es que tengamos que realizar una re sincronización de la data, para ello basta con ejecutar:

En el servidor que no está UpTodate

drbdadm – –discard-my-data connectall

Luego en el servidor que esta UpToDate

drbdadmconnectall

Los nodos empezaran a re-sincronizarse, transfiriendo los datos desde el nodo con datos OK, al nodo con los datos corruptos.

chkconfig asterisk on
chkconfig mysqld on
chkconfig httpd on

ANEXO 7

MARCAS Y COSTOS DE

TELEFONOS IP

ANEXO 7.

MARCAS Y COSTOS DE TELEFONOS IP

Los teléfonos IP son dispositivos de conmutación de paquetes utilizados en la en la telefonía de voz sobre IP, los cuales son teléfonos que físicamente son normales, con apariencia tradicional donde estos incorporan un conector RJ45 para conectarlo directamente a una red IP en Ethernet, estos dispositivos no pueden ser conectados a líneas telefónicas normales, estos terminales utilizan tecnología Voz IP y normalmente pueden realizar funcionalidades avanzadas como lo es llamada en espera, transferencia de llamada, se configuran desde los menús del propio teléfono o por interfaz Web y entre otras.

Teléfono IP	Marca	Costo
	Telefono Cisco Sip Phone 3911	$102
	Grandstream Telefono Ip Gxp280 1-line Voip Sip	$108
	Telefono Ip Grandstream Gxp2000	$145,24

	Teléfono Ip Itp-5121d Samsung	$200
	Telefono Ip Linksys 2 Or 4 Lineas Ip	$250
	Telefono Sip Spa525g2 5lineas Ip Phone Lcd + Poe 2 Puertos	$475
	Telefono Cisco Sip Phone 3911	$102
	Cisco IP Phone 7912G	$150
	Ip Analog Gateway Gxw4008 Fxs	$ 388

Fuente: http://articulo.mercadolibre.com.ec/

Algunos teléfonos como lo detallamos anteriormente disponen de dos conectores RJ-45 e implementan funciones de switch, de esta forma no es necesario instalar cableado nuevo para los nuevos terminales. Los teléfonos IP en cierta forma se están pareciendo a los teléfonos móviles por los tipos de accesorios que estos traen consigo como

Fuente: http://www.hostname.cl

Adaptadores analógicos IP

Los adaptadores IP son dispositivos de conexión que permiten aprovechar los teléfonos analógicos actuales, transformando su señal analógica en los protocolos de Voz IP. Existen diferentes tipos de adaptadores entre los cuales esta el ATA, FXS17, FXO18 que son considerados como gateway IP ATA.

Adaptador para Teléfonos Analógicos (ATA)

Un adaptador para teléfonos analógicos (ATA) o a futuro, adaptadores telefónicos (TA), conectan un teléfono ordinario a una red de VoIP. Un ATA tiene un conector RJ11 (el conector de teléfono) y un RJ45 (el conector de red o Ethernet). Un ATA funciona como si fuera un adaptador FXS. Este dispositivo por un lado habla con el teléfono analógico y por el otro opera en modo digital con la red de voz IP. Los ATAs hoy en día suelen ser suelen ser más baratos y al ser más pequeños suelen ser más fáciles de "nacionalizar" en las aduanas. Otra de las ventajas de usar un hardware ATAs, es

que se puede conectar cualquier tipo de dispositivo telefónico a la red IP, por ejemplo, se pueden conectar una cabina telefónica (de monedas o tarjeta), un fax o un teléfono inalámbrico.

El Analog Telephone Adapter (ATA), es el caso más normal, tienen un conector FXS para teléfono analógico normal y envían por Voz IP a través del conector LAN, soportan SIP normalmente. En la figura siguiente, se puede describir un adaptador de los mas usados actualmente por la telefonía IP consta de dos puertos FXS con conectores RJ 11 y un puerto ethernet con un conector RJ 45 el cual se encarga de permitir el paso de la entrada de los datos para que se haga la conversión digital-análoga o viceversa, después saliendo por los dos puertos FXS para un teléfono normal con esto se logra el aprovechamiento de terminales convencionales.

Dispositivo	Marca	Costo
	Grandstream Handytone 286 Adaptador Ata Fxs - Voip	$77
	Adaptador ATA marca Linksys	$120

Fuente: http://articulo.mercadolibre.com.ec/

Softphones

Son programas que permiten llamar desde el ordenador utilizando tecnologías Voz IP, los cuales se ejecutan en estaciones o servidores de trabajo permitiendo establecer llamadas de voz sobre el protocolo IP. Este tipo de dispositivo o software de comunicación es muy esencial a la hora de no querer colocar teléfonos ni otro elemento de comunicación para esta tecnología como lo es la voz IP, en la Figura siguiente, podemos establecer los diferentes tipos softphones, los cuales son lo más

utilizados en la actualidad. Estos elementos son de gran importancia para un red de telefonía IP por que permiten la comunicación al igual que cualquier otro teléfono común, estos software o dispositivos IP permiten una reducción de costo a la hora de la implementación, por loque hay algunos elementos de estos que no tienen licencia y son software libres.

Los softphones, son una alternativa al uso de equipos dedicados (físicos) de VoIP. Estos programas funcionan en cualquier ordenador personal. El único requerimiento es tener una tarjeta de sonido en funcionamiento y estar seguro de que el cortafuegos instalado en tu máquina no está bloqueando a la aplicación.

Si se desea reducir el ancho de banda usado por las conversaciones, se puede elegir un "soft phone" que tenga soporte para el protocolo IAX2, en donde se pueda activar un codec de alta compresión.

X-Lite

Zoiper

Las características Principales de estos tipos de software de comunicaciones son:

- Integración con el entorno.
- Icono en systray, dock.
- Aviso visual de llamadas entrantes.
- Integración con plataformas de acceso y validación de usuarios (LDAP).
- Importación / Exportación de datos: libretas de contactos en XML.
- Soporte de varias conversaciones simultáneamente y en algunos casos de varias líneas

BIBLIOGRAFIA

1.- BARRIOS J., Alcance libre implementación de servidores con GNU/Linux., México - México., s. edt., 2007., Pp. 491

2.- BONILLA, M y otros., Arquitecturas distribuidas como solución a sistemas demandantes de servicios de uso crítico considerando factores de seguridad, rendimiento y disponibilidad., Colombia - Bogota., s. edt., 2011., Pp. 120

3.- LANDIVAR E., Comunicaciones unificadas con Elastix., México - México., s. edt., 2009., Pp. 256

4.- LANDIVAR E., Comunicaciones unificadas con Elastix., 2a. ed. México - México., s. edt., 2009., Pp. 218

5.- LOPEZ, J. y otros., VoIP y Asterisk : Redescubriendo la telefonía., México - México., Alfaomega., 2009., Pp. 348

6.- VAN J. y otros., Asterisk The Future of Telephony., 2a. ed. Washington - United States., O'Reilly Media., 2007., Pp. 604

7.- BIND

es.wikipedia.org/wiki/BIND

[2011/11/10]

8.- Calcular disponibilidad

http://www.availabilitydigest.com/public_articles/0101/calculating_availability.pdf

[2011/11/12]

9.- Configuración Heartbeat y BRBD.

http://support.red-fone.com/downloads/elastix/Elastix_HA_Cluster.pdf

[2011/09/11]

10.- Configurando DUNDI en Elástix

http://elajonjoli.org/node/11.

[2010/09/02]

11.- Clúster

http://es.scribd.com/doc/36757812/Cluster-de-Bajo-Costo-en-Linux

http://es.wikipedia.org/wiki/Cluster_de_computadores

http://ohem.wordpress.com/2009/07/15/clusters/

[2011/09/01]

12.- Clustering de alta disponibilidad en GNU/Linux

[2011/05/16]

13.- DRBD

http://www.drbd.org

[2011/10/03]

14.- DUNDI

http://www.dundi.com/

http://www.dundi.com/dundi.

[2010/10/13]

15.- DUNDI Enterprise configuration IAX

http://www.voip-info.org/wiki/view/DUNDi+Enterprise+Configuration+IAX.

[2010/12/17]

16.- Heartbeat + DRBD

http://www.gonzalomarcote.com/blog/?p=58

[2011/08/03]

17.- Instalación de Asterisk

1.http://www.voztovoice.org/

[2010/09/23]