

UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE QUITO-CAMPUS SUR

CARRERA INGENIERÍA DE SISTEMAS

MENCIÓN (ROBÓTICA E INTELIGENCIA ARTIFICIAL)

**INVESTIGACIÓN, ANÁLISIS E IMPLEMENTACIÓN DE UN SERVIDOR
DE VIRTUALIZACIÓN DEDICADO PARA INTEGRAR UN SERVIDOR
DE CORREO ZIMBRA VIRTUALIZADO CON UN SERVIDOR
MULTITAREA ZENTYAL FÍSICO COMO CONTROLADOR DE
DOMINIO, FIREWALL Y PROXY UTILIZANDO HERRAMIENTAS
COMO TECNOLOGÍAS DE SOFTWARE LIBRE.**

HENRRY ROLANDO PADILLA CEVALLOS

DIRECTOR: RENATO CUMBAL

Quito, Junio 2012

DECLARACIÓN

Yo Henry Rolando Padilla Cevallos declaro bajo juramento que el trabajo aquí descrito es de autoría propia, por ser auspiciado por la Empresa Movidatos para su realización.

El proyecto de tesis que no ha sido previamente presentada para ningún grado o calificación profesional.

A través de la presente declaración concedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

Henry Rolando Padilla Cevallos.

No hay metas inalcanzables ni tampoco sueños imposibles de realizar, cada logro en tu vida es una meta cumplida y cada sueño realizado es un logro en la misma, los sueños que se cumplen en el camino de la vida nos ayuda a ser cada vez mejores por que lograr una meta es cumplir un ciclo en la vida.

CERTIFICACIÓN.

Certifico que el presente trabajo fue desarrollado por Henry Rolando Padilla Cevallos bajo mi dirección y el cual se ha concluido a entera satisfacción su Tesis de Grado.

Ing. Renato Cumbal.
DIRECTOR DE TESIS

Ing. Daniel Díaz.
LECTOR DE TESIS

AGRADECIMIENTO

Doy gracias a Dios por darme salud, vida, corazón para seguir adelante ya que siempre será mi guía, mi fortaleza.

A mis padres Rita y Ángel por sus consejos, valores, oportunidades, por su constante empeño en darme lo mejor para poder salir adelante cada día de mi vida.

Gracias por ser un buen ejemplo y enseñarme siempre que en la vida hay que luchar para poder conseguir mis sueños y ser feliz con nuestros seres más queridos.

A mi hermana Paola a pesar de ser tan pequeña siempre fue uno de mis grandes motivos para salir adelante, para ser su ejemplo a seguir y demostrarle que todo lo que nuestros padres nos dan cada día es valioso y ayuda de mucho para ser una buena persona en lo personal como profesional.

A mi director de tesis Renato Cumbal por su apoyo, visión y ganas de trabajar con el software libre, siempre será un gusto trabajar con su persona, gracias por el apoyo incondicional en todo el tiempo en la universidad como en el transcurso de la realización como terminación de la tesis.

A mis tíos, tías, primos, como mi gran querida abuela que siempre me han apoyado con un consejo y siempre han creído en mis capacidades como fortalezas para salir adelante.

A mis amigos, compañeros del alma que siempre fueron como unos hermanos y juntos formamos una hermosa familia de apoyo, aprendizaje y muchas experiencias universitarias en todo los niveles en la prestigiosa Universidad Politécnica Salesiana.

A mis amigos del prestigio Colegio Central Técnico con los cuales aprendí a iniciar el camino de vida profesional con los cuales en cada día de la vida del colegio supe comprender que siempre puedes salir adelante cuando tus amigos como tus padres te apoyan.

A mi novia Susana que siempre me ha brindado su apoyo, comprensión y autoestima para salir adelante en todo el transcurso de este proyecto de tesis como mi trayecto universitario.

DEDICATORIA

Presento este gran trabajo con gran orgullo a una gran mujer que Dios me dio para que siempre este a mi lado para cuidarme, apoyarme y darme todo para salir adelante: mi madre Rita, que siempre ha sido mi fortaleza, apoyo en todo el trayecto de mi vida, todo sus valores, enseñanzas, consejos en mi camino ha sido de gran valor para salir adelante.

También dedico este trabajo a mi padre, mi hermana y mi novia todos ellos han constituido en mi vida un pilar de fuerza, alegría y ganas de seguir adelante, quienes me enseñaron a alcanzar mi sueños y entender que no existe metas inalcanzables.

CONTENIDO

CAPITULO 1.

1.1. PLANTEAMIENTO DEL PROBLEMA.....	30
1.2. EMPRESA MOVIDATOS.....	30
1.3. ANÁLISIS INFRAESTRUCTURA.....	30
1.4. INFRAESTRUCTURA TECNOLÓGICA ACTUAL.....	31
1.4.1. ANÁLISIS SERVIDOR DE CORREO CORPORATIVO.....	31
1.4.2. ANÁLISIS ESTACIONES DE TRABAJO.....	32
1.4.3. ANALISIS PROTECCIÓN DE FIREWALL.....	32
1.4.4. ANÁLISIS RESTRICCIÓN COMO CONTROL PÁGINAS WEB.....	33
1.5. OBJETIVOS.	34
1.5.1. OBJETIVO GENERAL.....	34
1.5.2. OBJETIVOS ESPECÍFICOS.....	34
1.6. SERVIDORES A INTEGRAR COMO IMPLEMENTAR.....	35
Servidor de virtualización de dicado VirtualBox.....	35

Servidor de correo virtual Zimbra Collaboration Suite.....	35
Servidor multitarea Zentyal.....	35
Controlador de dominio.....	35
Firewall.....	35
Proxy.....	36
1.7. HERRAMIENTAS COMO TECNOLOGÍAS DE SOFTWARE LIBRE.....	36
1.8. PRINCIPALES SERVICIOS.....	36
CAPÍTULO 2.	
2.1. SERVIDORES LINUX.....	37
2.1.1. UBUNTU.....	37
2.1.2. CENTOS.....	37
2.2. SERVIDOR DE VIRTUALIZACION VIRTUAL BOX.....	37
2.3. VIRTUALBOX.....	38
2.4. ZIMBRA.....	39
2.4.1. PROTOCOLOS DE ENVÍO Y RECEPCIÓN DE CORREO COMO MENSAJES.....	40
SMTP, Simple Mail Transfer Protocol.....	40

POP, Post Office Protocol.....	40
IMAP, Internet Message Access Protocol.....	40
2.4.2. CARACTERÍSTICAS DE LA ARQUITECTURA DEL PRODUCTO.....	40
Flexibilidad.....	40
Libertad.....	40
Durabilidad.....	40
Bajo coste de mantenimiento.....	41
2.4.3. MÓDULOS PRINCIPALES.....	41
2.4.4. CARACTERÍSTICAS DE ADMINISTRACIÓN ZIMBRA.....	42
2.4.5. VERSIONES DEL PRODUCTO.....	43
Open Source Edition.....	43
Zimbra Collaboration Server (ZCS).....	43
Network Professional Edition (ZCS).....	44
Starter Edition.....	44
Standard Edition.....	45
Professional Edition.....	45
Zimbra Collaboration Server Appliance (ZCA).....	45
Zimbra Appliance Basic Edition.....	45
Zimbra Appliance Standard Edition.....	46
Zimbra Appliance Professional Edition.....	46
2.4.6. TIPOS DE LICENCIA.....	46

Licencias Anuales.....	46
Plurianual Licencias.....	46
Licencias Perpetuas.....	47
2.4.7. TIPOS DE USUARIO.....	47
Profesional.....	47
Standard.....	47
2.4.8. COMPARATIVO CONTRA OTRAS SOLUCIONES DISPONIBLES.....	47
Características del conector Microsoft Outlook.....	47
Alta disponibilidad.....	47
Integración.....	48
Conectores soportados, para clientes de correo electrónico.....	48
Dispositivos móviles.....	49
Sistemas operativos soportados.....	49
Simulación del coste de inversión a 3 años.....	49
2.5. SERVIDOR ZIMBRA COLLABORATION SUITE 5.0.	49
2.5.1. ARQUITECTURA DE ZIMBRA.	50
2.5.2. COMPONENTES DE LA ARQUITECTURA.....	52
Zimbra Core.....	53
Zimbra LDAP.....	53
Zimbra MTA.....	53
Zimbra Store.....	54
Zimbra SNMP	54

Zimbra Logger.....	55
El cliente web.....	55
2.5.3. EL SERVIDOR ZIMBRA.....	56
2.5.4. CLIENTE DE WEB DE ZIMBRA MANUAL PARA LOS USUARIOS.....	58
2.5.6. INSTRUCCIONES DE INGRESO EN EL SISTEMA.....	58
2.5.7. EXPLORAR LAS DIFERENTES APLICACIONES.....	59
2.5.8. CONFIGURANDO LAS PREFERENCIAS.....	60
2.5.9. ALGUNOS DETALLES IMPORTANTES DE LAS OPCIONES DE CONFIGURACIÓN.....	61
2.5.10. USANDO LAS BÚSQUEDAS RÁPIDAS.....	62
2.5.11 USANDO EL CORREO ELECTRÓNICO.....	63
Leer correos.....	64
Imprimir correos.....	65
Crear nuevo mensaje.....	65
Campo CCO.....	66
Adjuntar archivos a un mensaje.....	67
Filtros de correo.....	68
Usando la libreta de direcciones.....	68
Usando el calendario.....	69
Agendar una cita.....	70
Seleccione la opción de nueva cita.....	71

Citas recurrentes.....	71
Responder a una invitación a reunión o cita.....	71
Usando la opción de tareas.....	72
Mensajería instantánea (Messenger).....	73
Usando notas.....	73
Usando el maletín.....	73

CAPÍTULO 3.

3.1.ZENTYAL.....	73
3.1.1. SERVIDOR LINUX PARA PYMES.....	74
3.1.2. ENTORNO GRÁFICO CON EL INTERFAZ DE ADMINISTRACIÓN.....	77
3.1.3. PERFILES Y PAQUETES INSTALABLES.....	79
Zentyal Gateway.....	79
Zentyal Unified Threat Manager.....	79
Zentyal Infrastructure.....	79
Zentyal Office.....	79
Zentyal Unified Communications.....	79
Paquetes adicionales.....	80
3.1.4. SELECCIONAR MODO DE LAS INTERFACES DE RED.....	82
3.1.5. MODO DE OPERACIÓN DE USUARIOS Y GRUPOS.....	82
3.1.6. ASISTENTE DE SUSCRIPCIÓN A ZENTYAL CLOUD.....	83

3.2. PRIMEROS PASOS CON ZENTYAL	84
3.2.1. LA INTERFAZ WEB DE ADMINISTRACIÓN DE ZENTYAL	84
3.2.2. EL DASHBOARD	87
3.2.3. CONFIGURACIÓN DEL ESTADO DE LOS MÓDULOS	88
Configuración del estado del módulo.....	89
Confirmación para habilitar un módulo.....	90
Aplicando los cambios en la configuración.....	90
Guardar Cambios.....	91
Advertencia.....	91
3.2.4. CONFIGURACIÓN GENERAL	91
Contraseña.....	92
Idioma.....	92
Zona Horaria.....	92
Fecha y Hora.....	92
Puerto del interfaz de administración.....	92
Nombre de la máquina.....	93
3.3. REDES EN ZENTYAL	93
3.3.1. CONFIGURACION Y ADMINISTRACION DE LA RED	93
Configuración modo estático.....	94
Configuración de las puertas de enlace.....	94
Configuración de los servidores DNS.....	94

Diagnóstico de red.....	95
Ping.....	96
Traceroute.....	97
Resolución de nombres de dominio.....	97
3.4. LA ACTUALIZACIÓN DE SOFTWARE EN ZENTYAL.....	98
Gestión de componentes de Zentyal.....	99
Instalación de componentes.....	100
Actualización de componentes.....	101
Desinstalación de componentes.....	101
Actualización del sistema.....	102
Actualizaciones del sistema.....	103
Actualizaciones automáticas.....	103
3.5. ZENTYAL GATEWAY.....	104
3.5.1. OBJETOS DE RED.....	104
3.5.2. GESTIÓN DE LOS OBJETOS DE RED CON ZENTYAL.....	105
3.5.3. SERVICIOS DE RED.....	106
Gestión de los servicios de red con Zentyal.....	106
3.6. MANTENIMIENTO DE ZENTYAL.....	107
Actualizaciones de software de calidad.....	108
Alertas.....	108
Informes.....	108

Monitorización y gestión remotas.....	109
Actualizaciones de seguridad avanzadas.....	109
Recuperación de desastres.....	109
3.7. EVENTOS Y ALERTAS.....	109
La configuración de eventos y alertas en Zentyal.....	109
Pantalla de configuración de eventos.....	110
3.8. MONITORIZACIÓN.....	111
La monitorización en Zentyal.....	111
Carga del sistema.....	112
Uso de la CPU.....	112
Uso de la memoria.....	113
Memoria libre.....	113
Caché de página.....	113
Buffer caché.....	113
Memoria usada.....	113
Uso del sistema de ficheros.....	113
Alertas.....	114
Pantalla de configuración de los observadores de la monitorización.....	115
Pantalla de configuración de los umbrales de eventos.....	115

CAPÍTULO 4

4.1. IMPLEMENTACIÓN.....	116
4.2. INTRODUCCIÓN.....	116

Servidor de virtualización.....	116
Servidor de correo virtualizado Zimbra.....	116
Servidor multiplataforma Zentyal.....	116
4.2.1. CARACTERÍSTICAS DE LOS SERVIDORES A NIVEL DE HARDWARE...	117
Servidor Multitarea Zentyal.....	117
HP ProLiant Server ML150 G3.....	118
Características.....	118
Servidor de virtualizacion VirtualBox.....	118
Servidor virtual de correo Zimbra Collaboration Suite.....	118
HP ProLiant ML350 G6.....	118
Características.....	118
4.2.2. ESTRUCTURA ACTUAL DE RED INTERNA.....	118
Router Cisco (Telconet).....	118
Switch 3com (10/100 Mbps) de 24 puertos capa 2 (Movidatos).....	119
Router Cisco D-Link (Movidatos).....	119
Cableado estructurado categoría 5e.....	119
Estructura actual de red externa.....	119
Fibra óptica.....	119
Transiber (Telconet.).....	119
Router Cisco (Telconet).....	119
4.3. INSTALACIÓN.....	120
4.3.1. SERVIDOR DE VIRTUALIZACIÓN VIRTUALBOX.....	120

4.3.2. SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE..	122
4.4. IMPLEMENTACIÓN.....	122
4.4.1. SERVIDOR DE CORREO ZIMBRA COLLABORATION SUITE.....	122
Requerimientos.....	122
Seguridad.....	124
4.4.2. CONFIGURACIÓN DEL DNS.	125
4.4.3. ADMINISTRACIÓN DIARIA.....	132
Comandos básicos utilizados para la administración del servidor Zimbra.....	134
Comando básico para parar y arrancar Zimbra.....	135
4.5. SERVIDOR MULTIPLATAFORMA ZENTYAL.....	135
4.5.1. REQUISITOS DE HARDWARE.....	136
4.5.2. TABLA DE REQUISITOS HARDWARE.....	137
4.5.3. LA INSTALACIÓN PUEDE REALIZARSE DE DOS MANERAS DIFERENTES.....	139
4.6. CONFIGURACIÓN E INTEGRACIÓN DEL SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE.....	148
Acceso a nivel interno.....	154
Acceso a nivel externo.....	155

4.6.1. OPCIONES CONSOLA DE ADMINISTRACIÓN.	156
4.7. IMPLEMENTACIÓN, CONFIGURACIÓN E INTEGRACIÓN DEL SERVIDOR FISICO MULTITAREA ZENTYAL	159
4.7.1. CONFIGURACIÓN DE RED EN ZENTYAL	160
Tarjeta de red interna Eth0.....	160
Tarjeta de red externa Eth1.....	161
4.8. SERVICIO DE DIRECTORIO (LDAP) ZENTYAL	161
4.8.1. INTRODUCCIÓN AL SERVICIO DE DIRECTORIO (LDAP)	161
4.9. SERVIDOR LDAP CON ZENTYAL	162
4.9.1. OPCIONES DE CONFIGURACIÓN DE LDAP	162
4.10. COMPARTICIÓN DE FICHEROS Y A LA AUTENTICACIÓN ...	163
4.10.1. SERVIDOR DE FICHEROS CON ZENTYAL	163
4.10.2. COMPARTICIÓN DE FICHEROS	163
4.10.3. LISTA DE DIRECTORIOS COMPARTIDOS	164
4.10.4. AUTENTICACIÓN CON ZENTYAL	165

4.11. CONFIGURACIÓN DE PROXY HTTP CON ZENTYAL.....	166
Permitir todo.....	166
Denegar todo.....	166
Filtrar.....	166
Autorizar y filtrar, permitir todo o denegar todo.....	166
4.11.1. PROXY HTTP.....	168
4.11.2. FILTRADO DE CONTENIDOS CON ZENTYAL.....	169
4.11.3. BLOQUEAR DOMINIOS ESPECIFICADOS SÓLO COMO IP.....	172
Bloquear dominios no listados.....	172
Permitir siempre.....	172
Denegar siempre.....	172
Filtrar.....	172
4.11.4. FILTRADO DOMINIOS.....	172
4.12. CORTAFUEGOS.....	174
4.12.1. CONFIGURACIÓN DE UN CORTAFUEGO CON ZENTYAL.....	174
Interfaz externa.....	174
Filtrado de paquetes.....	174
Tráfico de redes internas a Zentyal.....	174
Tráfico entre redes internas y de redes internas a Internet.....	175
Tráfico de Zentyal a redes externas.....	175
Tráfico de redes externas a Zentyal.....	175

Tráfico de redes externas a redes internas.....	175
Esquema de los diferentes flujos de tráfico en el cortafuego.....	176
Lista de reglas de filtrado de paquetes desde las redes internas a Zentyal..	177
4.12.2. CREANDO UNA NUEVA REGLA EN EL FIREWALL.....	178
4.12.3. REDIRECCIÓN DE PUERTOS CON ZENTYAL.....	178
4.13. ZENTYAL GATEWAY.....	179
4.13.1 CONFIGURACIÓN DEL ENCAMINAMIENTO CON ZENTYAL.....	180
4.13.2. PUERTA DE ENLACE.....	180
 CAPITULO 5.	
5.1. ANALISIS Y PRUEBAS FINALES.....	181
5.2. ANÁLISIS IMPLEMENTACIÓN E INTEGRACIÓN.....	181
5.3. SERVIDOR DE VIRTUALIZACIÓN VIRTUALBOX.	181
Máquina virtual servidor de correo Zimbra Collaboration Suite.....	181
Máquina virtual servidor de contabilidad Fenix.....	181
Máquina virtual servidor Vtiger CRM.....	181
5.4. SERVIDOR MULTITAREA ZENTYAL.	182
Servidor controlador de dominio.....	182

Servidor proxy.....	182
Servidor firewall.....	182
Servidor de archivos.....	182
Servidor ftp.....	182

**5.5. ESCENARIO DE PRUEBAS SERVIDOR VIRTUAL DE CORREO
ZIMBRA COLLABORATION SUITE.....183**

**5.5.1. PRUEBAS DE FUNCIONAMIENTO EN EL SERVIDOR VIRTUALIZACION
CON VIRTUALBOX.....183**

5.5.2. MAQUINA VIRTUAL ZIMBRA COLLABORATION SUITE.....184

**5.5.3. REALIZAMOS PRUEBAS DE RESOLUCIÓN DE DOMINIO
MOVIDATOS.....184**

Buscar tipos de datos diferentes.....	185
Consultar directamente desde otro servidor de nombres.....	185

**5.6. REALIZAMOS PRUEBAS EN EL SERVIDOR MULTITAREA
ZENTYAL.....187**

**5.6.1. REALIZAMOS PRUEBAS DE LOS TRES SERVICIOS
IMPLEMENTADOS.....190**

Controlador de dominio.....	190
Firewall.....	190
Proxy.....	190

5.6.2. PRUEBAS EN EL CONTROLADOR DE DOMINIO INTEGRADO E IMPLEMENTADO.....	190
5.6.3. PRUEBAS EN EL PROXY INTEGRADO E IMPLEMENTADO.....	192
5.6.4. PRUEBAS EN EL FIREWALL INTEGRADO E IMPLEMENTADO.....	194

CAPÍTULO 6.

6.1. COLOCACIÓN EN PRODUCCIÓN Y EVALUACIÓN FINAL.....	195
6.1.1. DIAGRAMA DE LA ESTRUCTURA DE RED.....	196
6.1.2. DIAGRAMA DE LA IMPLEMENTACIÓN DE NUEVOS SERVIDORES A LA INFRAESTRUCTURA ACTUAL.....	197
6.1.3. DIAGRAMA DE LA INTEGRACIÓN DE LOS NUEVOS SERVIDORES A LA INFRAESTRUCTURA ACTUAL.....	198
6.1.4. DIAGRAMA DE COLOCACIÓN EN PRODUCCIÓN DE LOS NUEVOS SERVIDORES A LA INFRAESTRUCTURA ACTUAL.....	199
6.2. COLOCACIÓN EN PRODUCCIÓN SERVIDOR DE VIRTUALIZACION DEDICADO CON VIRTUALBOX.....	201
6.2.1. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR EN PRODUCCIÓN.....	201

6.3. COLOCACIÓN EN PRODUCCIÓN SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE.....	202
6.3.1. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR EN PRODUCCIÓN.....	202
6.4. COLOCACIÓN EN PRODUCCIÓN EL SERVIDOR FISICO MULTITAREA ZENTYAL.....	208
6.4.1. INFORMACIÓN GENERAL DEL SERVIDOR.....	208
6.4.2. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR CONTROLADOR DE DOMINIO EN PRODUCCIÓN.....	214
6.4.3. DETALLES DE LA CONFIGURACIÓN LDAP EN EL SERVIDOR DE DOMINIO MOVIDATOS.....	216
6.4.4. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR PROXY EN PRODUCCIÓN.....	218
6.4.5. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR FIREWALL EN PRODUCCIÓN.....	223
6.5. FINANCIAMIENTO.....	231
6.5.2. FINANCIAMIENTO ESTUDIANTE PADILLA CEVALLOS HENRRY ROLANDO.....	231
6.5.3 FINANCIAMIENTO EMPRESA MOVIDATOS.....	232

6.6. TERMINOLOGIA.....	233
6.7. CONCLUSIONES Y RECOMENDACIONES.	235
6.7.1. CONCLUSIONES.....	235
6.7.2. RECOMENDACIONES.....	236
6.8. BIBLIOGRAFÍA.....	238
6.8.1 DOCUMENTACIÓN DE INTERNET.....	238
6.8.2. LIBROS.....	238
6.9. CRONOGRAMA DE ACTIVIDADES.....	240
6.10. ANEXOS.....	241

RESUMEN

Esta investigación tuvo como objetivo analizar e implementar servidores Linux a nivel de infraestructura en la empresa Movidatos que ofrezcan beneficios como lo son dominio corporativo el cual tiene la función de registrar todos los respectivos usuarios como sus contraseñas y tener un registros de los equipos en el dominio para una mejor organización, bloqueo de páginas web para tener un control de acceso a nivel de internet y establecer políticas de seguridad e integridad de las funciones internas de la empresa como del empleado, cortafuegos el cual ayuda a tener seguro toda la información interna como sus aplicaciones de ataques de terceros nivel de red interna como externa, correo electrónico el cual es una herramienta muy importante para la comunicación entre personal interno como externo y desarrollo de la empresa.

El proyecto de tesis se orienta tomando en cuenta que los servicios implementados ayudara al campo empresarial a desarrollarse de una mejor manera y aun bajo costo, en la actualidad en el país alrededor del 99% de las empresas son PYMES como medianas empresas y sus presupuestos de inversión en infraestructura tecnológica como en licencias de software es limitado. Las PYMES buscan continuamente fórmulas para reducir costes y aumentar su productividad, especialmente en tiempos de crisis como el actual. La mayoría suelen operar bajo presupuestos muy escasos y con una fuerza laboral limitada.

Estas circunstancias hacen muy difícil ofrecer soluciones adaptadas a las PYMES que les aporten importantes beneficios, manteniendo al mismo tiempo las inversiones necesarias y los costes operacionales dentro de su presupuesto.

Quizás sea esta la razón por la que siendo un mercado enorme con un potencial casi ilimitado, muchos fabricantes de tecnología y software han mostrado desinterés en desarrollar soluciones que se adapten a la realidad de las PYMES.

Por lo general, las soluciones corporativas disponibles en el mercado se han desarrollado pensando en las grandes corporaciones, por lo que requieren inversiones considerables en tiempo y recursos y demandan un alto nivel de conocimientos técnicos.

En el mercado mundial de los servidores, esto ha significado que hasta ahora las PYMES han dispuesto de pocas opciones como alternativas donde elegir, consistentes por lo general en soluciones sobredimensionadas a sus necesidades reales, complejas de gestionar y con elevados costes de licencias.

Revisando la situación actual de las PYMES parece razonable considerar a Linux como una alternativa más que interesante como servidor para PYMES, puesto que técnicamente ha demostrado una calidad y nivel funcional muy elevados y su precio, gratuito, es imbatible. Sin embargo la presencia de Linux en entornos de pyme es testimonial y su crecimiento relativamente reducido.

La razón es sencilla por la siguiente, para que un servidor de empresa se adapte a un entorno de pyme necesita que sus distintos componentes estén bien integrados entre sí y que sean sencillos de administrar. Las PYMES no tienen los recursos ni el tiempo necesario para desplegar soluciones de altas prestaciones pero complejas. Así mismo, los proveedores de servicios TIC para PYMES también precisan de soluciones que consuman poco tiempo en despliegue y mantenimiento para poder ser competitivos, y las tradicionales distribuciones de Linux para servidor no cumplen con estas premisas.

PRESENTACIÓN

Este proyecto, presenta dos soluciones de gran utilidad utilizada para grandes, medianas como pequeñas empresas la primera es servidor correo electrónico como lo es Zimbra Collaboration Suite que manejan servicios como infraestructura bajo plataforma Linux Centos y la segunda es un servidor multitarea Zentyal de red unificada que puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet Gateway, gestionando las amenazas como Firewall, como servidor de dominio , como servidor de bloqueo de páginas que maneja servicios como infraestructura bajo plataforma Linux Ubuntu Server.

El proyecto se integró como implemento todo con software, herramientas como sistemas operativos basados en software libre.

En el primer capítulo se representa a la empresa en la cual se implementó el tema de tesis, se detalla el análisis de la infraestructura tecnológica, se indica los respectivos servicios a implementar como integrar en la empresa y las herramientas de software utilizadas.

En el capítulo segundo se indica las características de los sistemas operativos de Linux a utilizar como lo son la distribución Linux y Centos, las herramientas de software libre utilizadas en los respectivos servidores, analizando su arquitectura, características como servicios.

En el capítulo siguiente número tres se detallan todo lo referente al servidor multitarea Zentyal sus características, funcionalidad como servicios los cuales se encuentran en funcionamiento en producción.

En el cuarto capítulo se detalla la implementación, instalación como integración del hardware disponible para el proyecto, se indica principales recomendaciones para la

administración de las distribuciones Linux en este caso Ubuntu y Centos y los respectivos servicios implementados en cada plataforma como lo son servicios de correo con Zimbra Collaboration Suite, controlador de dominio, firewall y proxy con Zentyal.

Las pruebas finales se detallan en el capítulo cinco en el cual se realiza un análisis del servidor multitarea Zentyal y el servidor de correo Zimbra a nivel de infraestructura. Se procede a verificar el estado de los servicios de correo zimbra a nivel externo como interno, se verifica los servicios de firewall, proxy como controlador de dominio del servidor Multitarea Zentyal.

Y en el último capítulo el número seis se detallan la colocación en producción de los respectivos servidores Linux y la activación de los respectivos servicios de correo, firewall, proxy como controlador de dominio. Los cuales antes de ser integrados en producción se realizó pruebas en un ambiente de test, luego preproducción para luego colocarlos en producción. Y así realizar un análisis del comportamiento de los sistemas operativos implementados y sus respectivos servicios colocados en funcionamiento en producción conjuntamente con los clientes que consumen los diferentes servicios que proporcionan cada servidor.

CAPITULO 1.

1.1. PLANTEAMIENTO DEL PROBLEMA.

1.2. EMPRESA MOVIDATOS.

La Empresa Movidatos es una empresa legalmente constituida cuya visión de negocio es ofrecer servicios de telecomunicaciones mediante telefonía móvil, internet, planes de datos y voz conjuntamente con la empresa Movistar, entre los servicios más importantes que ofrece están los siguientes

Móvil.

- Voz
- Correo
- Internet.
- Teléfonos

Internet

- Planes pregago
- Planes pospago
- Equipos
- Asesoramiento

1.3. ANÁLISIS INFRAESTRUCTURA.

La Empresa Movidatos actualmente según el estudio realizado necesita lo siguiente para optimizar el rendimiento de trabajo de su recurso humano.

Un servidor de correo electrónico con su propia interfaz web de envío y recepción de mail con compatibilidad con dispositivos móviles.

Un servidor controlador de dominio con funcionalidad de garantizar o denegar a un

usuario el acceso a recursos compartidos o a otra máquina de la red, normalmente a través del uso de una contraseña.

Un firewall que proporciona funcionalidades de filtrado, marcado de tráfico y de redirección de conexiones.

Un servidor proxy que proporciona funcionalidades de autorizar y filtrar, permitir todo o denegar cualquier contenido web.

Por el costo que implica este proyecto con software privativo la Empresa Movidatos ha decidido auspiciar un proyecto de tesis para poder implementar los servidores como servicios mencionados anteriormente con software libre.

1.4. INFRAESTRUCTURA TECNOLÓGICA ACTUAL.

1.4.1. ANÁLISIS SERVIDOR DE CORREO CORPORATIVO.

Actualmente la Empresa Movidatos posee un servidor de correo llamado sendmail pero el mismo posee las siguientes desventajas.

Desventajas:

- El servidor de correo sendmail no posee una interfaz web para poder visualizar como utilizar el servicio de correo electrónico mediante una navegador web.
- No existe compatibilidad con dispositivos móviles, opciones de protección de antispam, antivirus, como chat interno.
- Entre las configuraciones que se puede realizar a nivel de cuentas de correo de usuario son muy limitadas.
- Es necesario utilizar un software de escritorio como Microsoft Outlook, Outlook Express, Thunderbird para poder utilizar este servidor de correo como sus servicios.

- Presenta dificultades en su mantenimiento y el alta de cuentas solo puede llevarse a cabo a través de línea de comandos.

Todas estas desventajas que se han presentado en la empresa al utilizar este tipo de servidor de correo lo cual ha provocado que las actividades de los usuarios se hagan cada vez lentas y en muchos casos ineficientes.

1.4.2. ANÁLISIS ESTACIONES DE TRABAJO.

Actualmente la Empresa Movidatos tiene en su mayoría equipos, servidores como estaciones de trabajo comunicados mediante un grupo de trabajo lo cual presenta las siguientes desventajas.

Desventajas.

- Los usuarios no pueden trabajar en un dominio corporativo con niveles de seguridad informática.
- No a todos los usuarios se puede controlar como monitorear mediante un servidor de dominio.
- Los usuarios actualmente trabajan en un perfil de administrador como usuario invitado sin control de ningún nivel de seguridad.
- Los recursos de claves de seguridad, compartición de archivos, impresoras envío recepción de correos es muy limitada, y cada vez más se corre el riesgo de que la información empresarial este sin protección.
- No se puede tener ninguna información referente al inicio de sesiones de cada usuario.
- No se puede manejar perfiles de administración a nivel de usuario como computador aplicando seguridad informática en cada uno de las estaciones de trabajo como servidores.

1.4.3. ANALISIS PROTECCIÓN DE FIREWALL.

Actualmente la Empresa Movidatos no posee un servidor que realice la función de servidor de protección como lo es un firewall, en su infraestructura posee un firewall a nivel hardware pero no es lo suficientemente seguro, lo cual causa las siguientes desventajas.

Desventajas.

- Las estaciones de trabajo pueden ser infectadas con cualquier virus lo cual con el tiempo puede causar daños en el sistema operativo del computador retrasando las actividades de los empleados de la empresa.
- La empresa solo tiene un firewall que se podría llamar Gateway de circuito electrónico que son proxy no inteligentes que solo reenvían la conexión.
- Los servidores como estaciones de trabajo están a la vista de los llamados hackers.
- El servidor de correo actual como el dominio de Movidatos podrían caer en la llamada lista negra de envío y recepción de correo por producir spam.

1.4.4. ANÁLISIS RESTRICCIÓN COMO CONTROL PÁGINAS WEB.

Actualmente la Empresa Movidatos no posee un servidor que se realice la función de bloqueo de páginas web a nivel de proxy.

Desventajas.

- El usuario puede ingresar a cualquier página de internet disminuyendo su productividad en el trabajo por revisar páginas de internet que no le interesan a la empresa.
- Al ingresar a revisar cualquier página de internet los usuarios contaminan su computador de virus conjuntamente como la red interna de la empresa.
- La red interna de la empresa sin este tipo de protección estaría expuesto a muchos fraudes a nivel de información de la empresa como información personal del usuario.

- El acceso a direcciones de internet no se puede controlar mediante una específica dirección url.
- En cada estación de estación de trabajo no se puede controlar el acceso a internet por número de IP.

Según los accesos a internet que cada usuario puede visitar no existe ningún control de navegación de internet.

1.5. OBJETIVOS.

1.5.1. OBJETIVO GENERAL.

Integrar e implementar un servidor de correo virtualizado con un servidor físico multitarea que realizara las funciones de firewall, controlador de dominio y proxy, utilizando tecnologías como herramientas de software libre como servidor de correo Zimbra y servidor multitarea Zentyal manteniendo coherencia, consistencia con los servidores predecesores y mejorando sus funcionalidades.

1.5.2. OBJETIVOS ESPECÍFICOS.

- Realizar un análisis de los servidores actuales para conocer su funcionamiento, alcance, limitaciones como estructura que se deberán tomar en cuenta en el proceso de integración e implementación del servidor Zimbra como servidor Zentyal.
- Efectuar un análisis de la factibilidad de la implementación de un nuevo servidor de virtualización de servidores, tomando en cuenta las tecnologías como herramientas a usarse, la disponibilidad y soporte de las mismas en el mercado ecuatoriano.

- Implementar e integrar la configuración de un servidor de virtualización dedicado en el cual se procede a virtualizar un servidor de correo Zimbra el cual cumplirá las funciones de servidor virtual de correo en un primer servidor proporcionado por la Empresa Movidatos.
- Implementar e integrar la configuración de un servidor multitarea Zentyal que funcionara como firewall, controlador de dominio y proxy en un segundo servidor el cual también será proporcionado por la Empresa Movidatos.
- Verificar configuraciones del servidor de virtualización dedicado como las respectivas configuraciones de servidor de correo virtual.
- Verificar configuraciones del servidor Zentyal a nivel de controlador de dominio, firewall y proxy.
- Realizar pruebas de funcionalidad a nivel de servidor como a nivel de usuario verificando la funcionalidad de los servicios de servidor de correo virtual como los servicios de servidor de controlador de dominio, firewall como proxy en una o dos estaciones de trabajo de la empresa.
- Verificar el correcto funcionamiento de los servidores en producción como estaciones de trabajo que funcionen conjuntamente con los servicios implementados con los servidores anteriormente mencionados.

1.6. SERVIDORES A INTEGRAR COMO IMPLEMENTAR.

Servidor de virtualización de dicado VirtualBox.

- Consiste en lo siguiente, para implementar dicho servidor en este caso se utilizara la distribución de Linux Ubuntu de software libre como sistema

operativo que será instalado en un servidor físico sobre el sistema operativo se instalara la herramienta de virtualización VirtualBox con la cual se creara servidores virtuales como máquinas virtuales.

Servidor de correo virtual Zimbra Collaboration Suite.

- El servidor de correo a implementar en primer instancia se procederá a virtualizar en el servidor de virtualización dedicado con sistema operativo Ubuntu y la herramienta VirtualBox, es decir se creara un servidor virtual con sistema operativo Centos Linux de software libre en VirtualBox.

Servidor multitarea Zentyal.

- Para la implementación del servidor se utilizara otro servidor físico para lo cual se instalará en dicho servidor la distribución de Zentyal de software libre cuya distribución está basado en el sistema operativo Ubuntu Server el cual contiene varios servicios que ofrece con parte de arquitectura Zentyal y los cuales se implementaran:
 - Controlador de dominio
 - Firewall
 - Proxy

1.7. HERRAMIENTAS COMO TECNOLOGÍAS DE SOFTWARE LIBRE.

Debian 6.0 Server GNU/Linux.

- Es una distribución de sistema operativo de software libre con licencia GNU que se encuentra en unas de las más estables distribuciones de Linux

CentOS 5.5 Server GNU/Linux.

- CentOS (acrónimo de Community ENTerprise Operating System) es un clon a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

Ubuntu 10.04 GNU/Linux.

- Ubuntu es un sistema operativo basado en GNU/Linux desarrollado por la comunidad de usuarios que es perfecto para computadores de escritorio, portátiles y servidores. Contiene todas las aplicaciones que necesitas: un navegador de internet, programas para texto, presentaciones y hojas de cálculo, mensajería instantánea y mucho más.

Zentyal Servidor Multitarea GNU/Linux.

- Zentyal (anteriormente conocido como eBox Platform) es un servidor de red unificada de código abierto (o una plataforma de red unificada) para las PYMEs. Zentyal puede actuar gestionando la infraestructura de red, como puerta de enlace a Internet (Gateway), gestionando las amenazas de seguridad (UTM), como servidor de oficina, como servidor de comunicaciones unificadas o una combinación de estas. Además, Zentyal incluye un marco de desarrollo (un framework) para facilitar el desarrollo de nuevos servicios basados en Unix.

Virtual Box Open source.

- Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

- Entre los sistemas operativos soportados (en modo anfitrión) se encuentran GNU/Linux, Mac OS X, Microsoft Windows, y Solaris/OpenSolaris, y dentro de ellos es posible virtualizar los sistemas operativos FreeBSD, GNU/Linux, OpenBSD, OS/2 Warp, Windows, Solaris, MS-DOS y muchos otros.

Zimbra Open source.

- Zimbra es la solución líder para correo electrónico y calendario de código abierto para empresas, proveedores de servicios, instituciones académicas y gubernamentales; ofrece un software de grupo moderno e innovador muy superior a los sistemas de software anteriores.

1.8. PRINCIPALES SERVICIOS.

Samba (Servicio de directorio).

- Es un protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que ordenadores con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

Netfilter.(Filtrado, marcado de tráfico y de redirección de conexiones).

- Netfilter es un framework disponible en el núcleo Linux que permite interceptar y manipular paquetes de red. Dicho framework permite realizar el manejo de

paquetes en diferentes estados del procesamiento. Netfilter es también el nombre que recibe el proyecto que se encarga de ofrecer herramientas libres para cortafuegos basados en Linux.

- El componente más popular construido sobre *Netfilter* es iptables, una herramienta de cortafuegos que permite no solamente filtrar paquetes, sino también realizar traducción de direcciones de red (NAT) para IPv4 o mantener registros de log. El proyecto Netfilter no sólo ofrece componentes disponibles como módulos del núcleo sino que también ofrece herramientas de espacio de usuario y librerías.

Squid.(Control de contenidos).

- Squid es un popular programa de software libre que implementa un servidor proxy y un dominio para caché de páginas web, publicado bajo licencia GPL. Tiene una amplia variedad de utilidades, desde acelerar un servidor web, guardando en caché peticiones repetidas a DNS y otras búsquedas para un grupo de gente que comparte recursos de la red, hasta caché de web, además de añadir seguridad filtrando el tráfico. Está especialmente diseñado para ejecutarse bajo entornos tipo Unix.

Dansguardian (Control de contenidos).

- DansGuardian es un software de filtro de contenido, diseñado para controlar el acceso a sitios web. Incluye un filtro de virus, importante en sistemas Windows, es usado principalmente en instituciones de educación, gobierno y empresas. Se caracteriza por su alto grado de flexibilidad y adaptación de la implementación.
- DansGuardian se instala en un ordenador (servidor) con el sistema operativo GNU/Linux, y filtrará contenidos de webs solicitadas por el resto de ordenadores (independientemente del sistema operativo que tengan instalado). Para filtrar contenido usa comparación de caracteres, filtro PICS y filtro por URL.

BIND. (Servidor de DNS).

- BIND es el servidor de DNS más comúnmente usado en Internet, especialmente en sistemas Unix, en los cuales es un Estándar de facto.

VirtualBox (Servidor virtualización).

- Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, creado originalmente por la empresa alemana innotek GmbH. Actualmente es desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

Apache + Tomcat (Servidor Web).

- Tomcat es un contenedor de servlets (es lo que se necesita para ejecutar JSP y Servlets)

Clamav (Antivirus).

- ClamAV es un software antivirus open source (de licencia GPL) para las plataformas Windows, Linux y otros sistemas operativos semejantes a Unix.

Spamassassin + DSpam (Filtro de spam).

- SpamAssassin es una utilidad de correo electrónico que intenta filtrar *spam* mediante la inspección del correo electrónico entrante y examina si contiene características de *spam*. Usa filtración bayesiana de *spam* y pruebas de red para inspeccionar el correo entrante. Las pruebas le dan una puntuación total. Si un mensaje entrante alcanza una puntuación predefinida, se descarta.

Jdk (Maquina Java).

- Java Development Kit o (JDK), es un software que provee herramientas de desarrollo para la creación de programas en Java.

MySQL (Servidor de base datos).

- MySQL es un sistema de gestión de bases de datos relacional, multihilo y multiusuario con más de seis millones de instalaciones

OpenLdap (Servidor de directorio).

- Generalmente una petición LDAP es recibida por el frontend, decodificada y luego transferida a un backend para procesamiento. Cuando el backend completa la petición, devuelve un resultado al frontend, quien luego envía el resultado al cliente LDAP. Un overlay es una pieza de código que puede ser insertada entre el frontend y el backend. Es entonces capaz de interceptar peticiones y lanzar otras acciones en ellas antes de que el backend las reciba, y puede también actuar sobre los resultados del backend antes de que éstos alcancen el frontend. Overlays tiene acceso completo a las interfaces de programación (APIs) internas del servidor slapd, y por tanto pueden invocar cualquier llamada que podrían realizar el frontend u otros backends. Múltiples overlays pueden ser usados a la vez, formando una pila de módulos entre el frontend y el backend.
- Los overlays proveen un medio simple para incrementar las funcionalidades de una base de datos sin requerir que un completo backend nuevo puede ser escrito, y permite añadir nuevas funcionalidades de manera compacta, fácilmente depurable y módulos mantenibles. Desde la introducción de la característica de overlay en OpenLDAP 2.2 muchos nuevos overlays han sido contribuidos por la comunidad OpenLDAP

Postfix (Servidor de correo SMTP).

- Postfix es un servidor de correo de software libre / código abierto, un programa informático para el enrutamiento y envío de correo electrónico, creado con la intención de que sea una alternativa más rápida, fácil de administrar y segura al ampliamente utilizado Sendmail.

CAPÍTULO 2.

2.1. SERVIDORES LINUX.

Entre las distribuciones más estables como recomendadas entre las múltiples sistemas operativos de Linux con licencia GNU de software libre se encuentran las distribuciones de Ubuntu Linux y Centos Linux que se caracterizan por su estabilidad, seguridad, rendimiento, y actualización continua de versiones con mejoras en sus características como servicios que presta cada uno de ellos.

2.1.1. UBUNTU

Ubuntu es un sistema operativo basado en GNU/Linux desarrollado por la comunidad de usuarios que es perfecto para computadores de escritorio, portátiles y servidores. Contiene todas las aplicaciones que necesitas: un navegador de internet, programas para texto, presentaciones y hojas de cálculo, mensajería instantánea y mucho más.

- Es software libre, esto quiere decir que puedes instalarlo, copiarlo, distribuirlo o modificarlo sin restricciones.
- Al estar basado en GNU/Linux es un sistema muy estable.

- Contiene la suite de oficina OpenOffice completamente compatible con MSOffice, el navegador de Internet Firefox, el programa de gráficos GIMP, el gestor de correos Evolution y más de 16,000 programas listos para instalar.

2.2.2. CENTOS

CentOS es una distribución de Linux basada en las fuentes libremente disponibles de Linux. Cada versión de CentOS es mantenida durante 7 años (por medio de actualizaciones de seguridad). Las versiones nuevas son liberadas cada 2 años y actualizadas regularmente (cada 6 meses) para el soporte de hardware nuevo esta para libre descarga como instalación de la comunidad que utiliza o implementa software libre.

2.3. SERVIDOR DE VIRTUALIZACION VIRTUAL BOX.

2.3.1. VIRTUALBOX.

VirtualBox es una aplicación que nos permite ejecutar diferentes Sistemas Operativos simultáneamente en el mismo equipo de manera virtual. La razón para usar VirtualBox es porque es libre (GNU/GPL) y porque funciona bien.

Es un software de virtualización para varias arquitecturas, creado. Por medio de esta aplicación es posible instalar sistemas operativos adicionales, conocidos como «sistemas invitados», dentro de otro sistema operativo «anfitrión», cada uno con su propio ambiente virtual.

La aplicación fue inicialmente ofrecida bajo una licencia de software privativo, pero en enero de 2007, después de años de desarrollo, surgió VirtualBox OSE (Open Source Edition) bajo la licencia GPL 2.

2.4. ZIMBRA.

Es una solución completa de correo electrónico corporativo y colaboración con Antivirus y Antispam, que se integra con Microsoft Outlook 2003/2007. En la actualidad existe una versión de código abierto, sin costo de licencias alguno, y otra versión de pago con varios componentes extras de código cerrado y con costo de licencias. Está disponible para diversas plataformas y distribuciones de Linux.

Zimbra aporta módulos nuevos para almacenar documentos, chatear con nuestros compañeros o crear contenido dentro de un bloc de notas, calendario, contactos y tareas. Es posible, integrar los llamados “Zimlets” para expandir el potencial de la solución integrándolo funciones adicionales.

La integración con móviles tipo BlackBerry, iPhone, Windows Mobile, etc, se puede realizar con interfaz de acceso web Zimbra Mobile, es posible también realizar una migración desde un entorno IMAP4, Microsoft Exchange, Lotus y también ficheros “*.pst” de Microsoft Outlook.

En la actualidad Zimbra se ha convertido en una solución de código abierto líder a nivel para todo tipo de empresa como para proveedores de servicio, centros educativos y administraciones públicas. Su éxito se basa en el uso de tecnologías de código abierto y protocolos de comunicación e intercambio de datos estándares.

El producto, está compuesto por un conjunto de servicios Linux (Courier, Openldap, Mysql, Postfix) integrados entre sí, para hacer una solución muy robusta y probada.

2.4.1. PROTOCOLOS DE ENVÍO Y RECEPCIÓN DE CORREO COMO MENSAJES.

Para lograr la conexión se definen una serie de protocolos, cada uno con una finalidad concreta.

- **SMTP, Simple Mail Transfer Protocol.**

Se utiliza para que dos servidores de correo intercambien mensajes.

- **POP, Post Office Protocol.**

Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario.

- **IMAP, Internet Message Access Protocol.**

Su finalidad es la misma que la de POP, pero el funcionamiento es diferente, ya que a diferencia de POP, los correos se mantienen en el servidor de correos.

2.4.2. CARACTERÍSTICAS DE LA ARQUITECTURA DEL PRODUCTO.

- **Flexibilidad:** Fácil personalización según las necesidades de la organización.
- **Libertad:** Uso de cualquier navegador web y de aplicaciones de escritorio tradicionales.
- **Durabilidad:** Servidor de correo electrónico y calendario extraordinariamente fiable y ampliable.
- **Bajo coste de mantenimiento:** Gestión muy sencilla, tanto mediante una interfaz gráfica como desde la consola.

2.4.3. MÓDULOS PRINCIPALES:

- **Cliente web.**

El cliente web de Zimbra es la interfaz web que el cliente puede utilizar internamente o externamente mediante cualquier navegador de internet para enviar y recibir correos y revisar los mismos.

- **Servidor.**

- El servidor de Zimbra en sus principales funcionalidades esta proporcionar acceso al correo electrónico mediante web mail, vía Mlackberry como cliente Outlook se puede integrar mediante uso de internet en cualquier teléfono móvil que tenga acceso a internet por la característica de tener su interfaz móvil.

- **Extras.**

Zimbra se integra con sus dispositivos móviles, de forma natural y sin tener que instalar aplicaciones en los terminales, gracias a la tecnología “Active Sync” y a su conector para “BlackBerry Enterprise Server”. Todos los dispositivos Windows Mobile, Android, Blackberry, iPhone, Nokia, están soportados por Zimbra.

La figura muestra las funcionalidades que ofrece Zimbra y los servicios que se ejecutan sobre este.

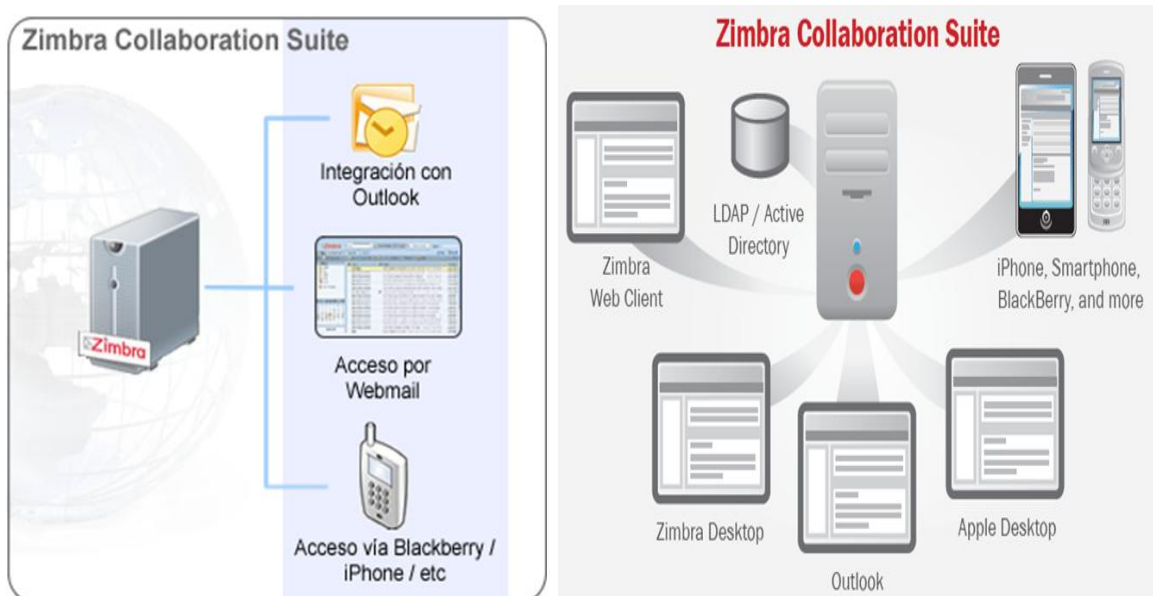


Figura 2.4.1. Zimbra Collaboration Suite.

Fuente: <http://www.altosec.com.ar/zimbra-collaboration-suite-solucion-de-groupware>

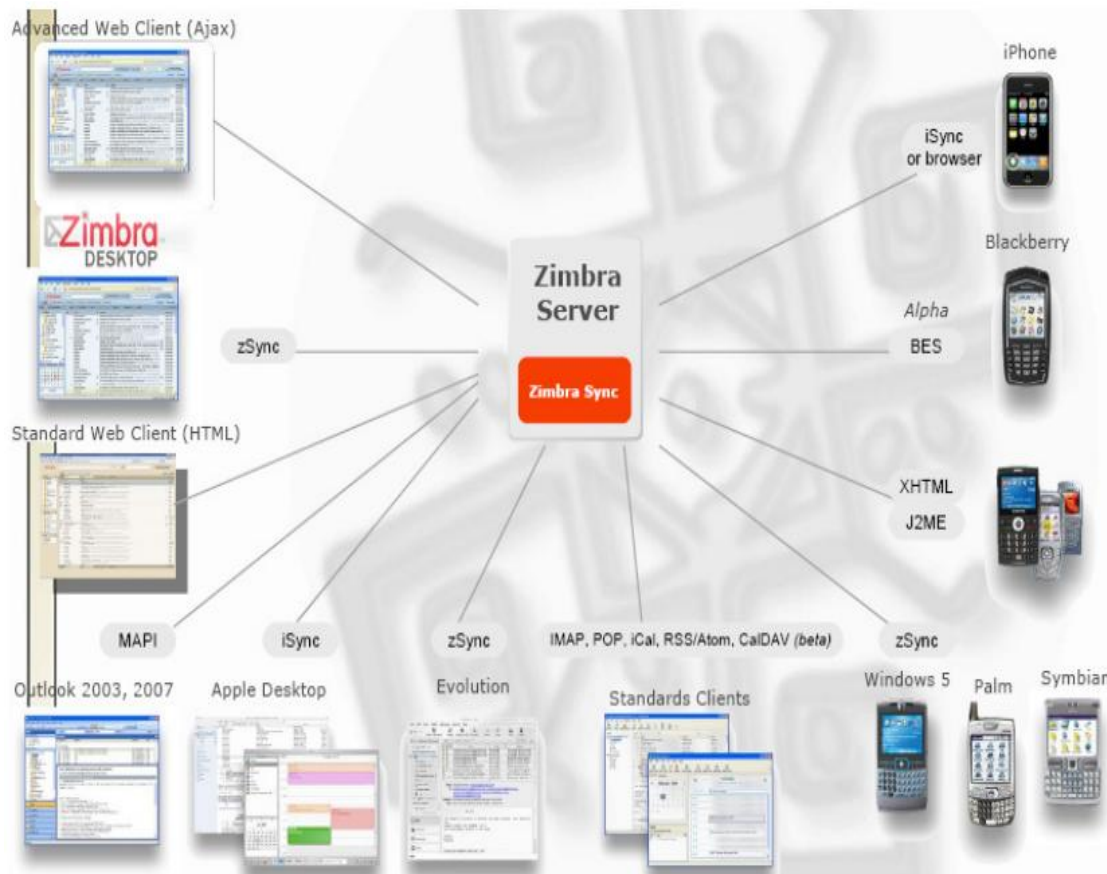


Figura 2.4.2. Zimbra Server.

Fuente: <https://agilemail.com.au/files/imagecache/preview/node/182661/zimbra-server-client-support1.png>

2.4.4. CARACTERÍSTICAS DE ADMINISTRACIÓN ZIMBRA.

Al manejar un entorno gráfico, Zimbra permite una administración más fácil de todos los servicios que ofrece:

- Administración vía Web (AJAX) o usando CLI.
- Multi dominios/multi servidor.
- Clases de Servicio.
- Antivirus y Antispam integrados.
- Monitoreo de Mensajes.
- Manejo de colas de correo.
- Clustering/HA.

- Bloqueo de adjuntos.
- Soporte para servidores Linux/Mac.

2.4.5. VERSIONES DEL PRODUCTO.

Open Source Edition.

Totalmente funcional pero con algunos recortes en el interfaz Web y en la herramienta de administración. Este producto, se ofrece sin garantías y sin opción de adquirir soporte por parte del fabricante.

Zimbra Collaboration Server (ZCS).

Edición ZCS de código abierto es un correo electrónico gratuito y es una solución de colaboración para los individuos o las organizaciones más pequeñas.

Zimbra, una administración avanzada, continuidad del negocio y sólo el correo electrónico IMAP en los escritorios y dispositivos.

Zimbra Open Source Edition, permite gestionar los correos institucionales de la empresa de manera sencilla desde una herramienta web intuitiva, Zimbra es una buena opción frente a Exchange o Lotus.

Zimbra, es una empresa líder en el mercado, la cual dispone de su versión Open Source que no requiere licenciar y ofrece características similares comparadas a un software licenciado.

Principales características:

- **Gestión de Usuarios:** Permite gestionar los usuarios de su institución, UD

podrá crear, eliminar y bloquear cuentas. También le permite al administrador ver los correos de los usuarios para evaluar la productividad de su negocio.

- **Gestión de Dominios:** Permite gestionar los diferentes dominios que tenga en el servidor, si UD tiene un nuevo dominio puede registrarlo y empezar a crear las cuentas para el nuevo dominio.
- **Monitoreo de Colas:** Permite ver las colas de correo, las cuales puedes estar corruptas o en algunos casos rechazados por el servidor destino, igualmente Zimbra desde la herramienta web le permitirá re encolar el correo.
- **Bloqueo de Adjuntos:** Permite bloquear los archivos adjuntos que UD crea conveniente, esta opción bloquear a todos los usuarios de enviar determinados adjuntos, por ejemplo archivos: .exe o .bat.
- **Reporte de Envíos:** Permite ver en gráficos la cantidad de correos enviados y recibidos de su empresa.
- **Acceso WEB:** Permite tener acceso a sus correos desde una interfaz web totalmente intuitiva, para sus colaboradores de provincia o cuando no esté en su oficina.
- **Compartir Calendario, contactos:** Permite compartir su calendario o contactos con los usuarios que UD invite, ofreciéndole accesos de edición o solo lectura.

Network Profesional Edition (ZCS).

La opción profesional, con funciones adicionales tanto en el interfaz Web, como en la herramienta de administración. Este tipo de versión, va acompañado por un soporte del fabricante y unas garantías del producto.

- **Starter Edition.**

ZCS red Starter Edition es un paquete de software sólo con 15 licencias de Professional Edition buzón de correo, además de actualizaciones de software y sólo sin la compatibilidad de Zimbra. Licencias adicionales del buzón no se puede añadir, Zimbra Mobile y Zimbra Archiving and Discovery están incluidos.

- **Standard Edition.**

- ZCS Red Standard Edition es un correo electrónico de clase empresarial y soluciones de colaboración sin límite en el número de buzones que pueden ser objeto de licencia. Zimbra Mobile y soporte Zimbra Advantage (ampliable a Premium) también están incluidos.

- **Professional Edition.**

ZCS Red Professional Edition es un correo electrónico de clase empresarial y soluciones de colaboración sin límite en el número de buzones que pueden ser objeto de licencia. Cuenta con Zimbra Mobile, Zimbra Connector para Outlook, soporte Zimbra Advantage (ampliable a Premium) y Zimbra Archiving and Discovery.

Zimbra Collaboration Server Appliance (ZCA).

- **Zimbra Appliance Basic Edition.**

ZCA Basic Edition es una solución de correo electrónico gratuito y de colaboración diseñado para el despliegue de vSphere para proporcionar una administración sin esfuerzo VMware. Se trata de un paquete de software sólo

para un máximo de 10 cuentas de correo, no es compatible Zimbra. Zimbra Mobile se incluye (sin el apoyo de BlackBerry). Licencias adicionales del buzón no se puede añadir, ni Zimbra Archiving and Discovery.

- **Zimbra Appliance Standard Edition.**

ZCA Standard Edition es un correo electrónico de la empresa y la solución de colaboración diseñada para el despliegue de vSphere para proporcionar una administración sin esfuerzo VMware. Hasta 1.000 buzones de correo pueden ser objeto de licencia y viene con soporte Advantage (ampliable a Premium) y Mobile Zimbra.

- **Zimbra Appliance Professional Edition.**

ZCA Professional Edition es un correo electrónico de la empresa y la solución de colaboración diseñada para el despliegue de vSphere para proporcionar una administración sin esfuerzo VMware. Hasta 1.000 buzones de correo pueden ser objeto de licencia y viene con soporte Advantage (ampliable a Premium). Zimbra Mobile se incluye como es Zimbra Connector para Microsoft Outlook, Zimbra Archiving and Discovery está incluido.

2.4.6. TIPOS DE LICENCIA.

- **Licencias Anuales.**

Licencias anuales renuevan cada año en base a la fecha de compra. Durante la duración de la suscripción, los clientes tienen derecho a actualizaciones de liberación mayor y menor y Zimbra Soporte Advantage o de primera calidad, el acceso al portal y mucho más.

- **Plurianual Licencias.**

Varios años las licencias renovar cada 2 o 3 años según el día de la compra y se tenía a un nivel de descuento de licencias anuales. Durante la duración de la suscripción, los clientes tienen derecho a actualizaciones de liberación mayor y menor y Zimbra Soporte Advantage o de primera calidad, el acceso al portal y mucho más.

- **Licencias perpetuas.**

Perpetua es una licencia de software permanentes para la versión principal que está comprando, además de las actualizaciones de versión menor a la misma (por ejemplo, sólo 7.xx). Apoyo Zimbra se compra ya sea anualmente o como un período de tres años, además de los costos de licencia (con el año obligatorio de primero) y le da derecho a actualizaciones de versión principal, el acceso al portal y mucho más. Licencias perpetuas ofrecen el modelo de licencias más rentables para varios años de implementación.

2.4.7. TIPOS DE USUARIO.

- **Profesional.**




Acceso a todos los módulos del sistema y con opciones de compartir carpetas de datos y uso de los conectores para MS Outlook y iSync de Mac.

- **Standard.**

Acceso a todos los módulos del sistema y con opciones de compartir carpetas de datos pero quedan excluidos de utilizar los conectores para MS Outlook y iSync de Mac.

2.4.8. COMPARATIVO CONTRA OTRAS SOLUCIONES DISPONIBLES.

Características del conector Microsoft Outlook.

Características del conector Microsoft Outlook			
Sincronización Correo	Nativo	IMAP	Nativo
Sincronización PIM	Nativo	Nativo	Nativo
Sincronización Carpetas Públicas	No disponible	Si	Si
Modo Offline / Online	Si	Si	Si
Abrir buzón de otro usuario	Si	IMAP	Si
Autoinstalable	Si	Si	Si
Autenticación Soportada	User-pass	User-pass	User-pass / Kerberos

Cuadro comparativo de las características del conector Outlook.

Figura 2.4.3. Cuadro comparativo de las características de conector Outlook.

Fuente: Comparativa de soluciones Open Source Groupware.

Alta disponibilidad.




Alta disponibilidad			
Activo / Pasivo	Si	Si	Si
Activo / Activo	No	Si	No
Balancedor de Carga	No	Si	No
Virtualización	Si	Si	Si
Almacenamiento Compartido	No	Si	No
Distribución de Servicios	Si	Si	Si

Cuadro comparativo de las opciones en alta disponibilidad

Figura 2.4.4. Cuadro comparativo de las opciones de alta disponibilidad.

Fuente: Comparativa de soluciones Open Source Groupware.

Integración.

Integración			
Coexistencia con Exchange	Si	No	Si
Integración con otro SMTP	Si	Si	Si
Integración con otro IMAP	No	Si	No
Soporte de SOAP	Si	Si	No
Soporte de RMI	No	Si	No
Soporte WebdavXML	No	Si	Si
Integración Active Directory	Si	Si	Si (modificación del Schema)
Métodos de Autenticación	ADS OpenLdap Mysql	ADS OpenLdap MailServer Mysql	ADS OpenLdap Kerberos

Cuadro comparativo de integración, tanto en infraestructuras consolidadas, como en APIs de integración con otras aplicaciones

Figura 2.4.5. Cuadro comparativo de integración.

Fuente: Comparativa de soluciones Open Source Groupware.

Conectores soportados, para clientes de correo electrónico.




Conectores para clientes de correo			
Outlook 2003 / 2007	Completa	Sólo PIM	Completa
iSync Mac	Completa	Completa	No disponible
Thunderbird	IMAP (PIM con Funambol)	IMAP (PIM con Funambol)	IMAP
KDE Kontact / Kmail	Sólo IMAP	Completa	Sólo IMAP
Novell Evolution	Completa	IMAP + Calendario	Completa

Cuadro comparativo de los conectores para diferentes tipos de clientes de correo

Figura 2.4.6. Cuadro comparativo de conectores.

Fuente: Comparativa de soluciones Open Source Groupware.

Dispositivos móviles.

Dispositivos Móviles			
Blackberry	Zimbra Mobile / Funambol / Notify Link	Funambol / O3SIS	Notify Link
Active Sync	Zimbra Mobile / Funambol / Notify Link	Funambol / O3SIS / Oxtender	Notify Link
Nokia / LG / Samsung	Zimbra Mobile / Funambol / Notify Link	Funambol / O3SIS	Notify Link
iPhone	Funambol / Notify Link	Funambol / O3SIS	Notify Link
Push Email	Funambol	Funambol / O3SIS	Funambol

Cuadro comparativo, de las diferentes soluciones ofrecidas para integración con dispositivos móviles

Figura 2.4.7. Cuadro comparativo de las diferentes soluciones.

Fuente: Comparativa de soluciones Open Source Groupware.

Sistemas operativos soportados (Sólo versiones profesionales de las soluciones).

Sistemas Operativos			
Red Hat	Si	Si	Si
Suse Novell (SLES)	Si	Si	Si
Debian	No	Si	No
Ubuntu	Si	No	No

Cuadro comparativo, de los diferentes sistemas operativos soportados

Figura 2.4.8. Cuadro comparativo de las diferentes sistemas operativos..

Fuente: Comparativa de soluciones Open Source Groupware.

Simulación del coste de inversión a 3 años.

Precios de licencias			
100 usuarios (Pago único)	4.800€	3.500€	3.990€
Suscripción de soporte 1º Año	960€	Incluido	1.200€
Suscripción de soporte 2º Año	960€	875€	1.200€
Suscripción de soporte 3º Año	960€	875€	1.200€
Total inversión 3 años con soporte	7.680€	5.250€	7.590€

Cuadro comparativo, de los precios de licencia y soporte del fabricante

Figura 2.4.9. Cuadro comparativo de los precios de licencia y soporte del fabricante..

Fuente: Comparativa de soluciones Open Source Groupware.

2.5. SERVIDOR ZIMBRA COLLABORATION SUITE 5.0.

Zimbra es una solución de nueva generación con capacidad de crecimiento en situaciones futuras, la cual ofrece dos versiones. Una versión soportada por la comunidad de software abierto (opensource) y una versión soportada comercialmente (Zimbra Network) que contiene algunas mejoras propietarias.

2.5.1. ARQUITECTURA DE ZIMBRA.

Zimbra Collaboration Suite está formada por un conjunto de componentes que trabajan juntos para formar una solución completa. El núcleo del servidor está escrito en Java, utilizándose Jetty como servidor de aplicaciones. El servidor se integra con otros sistemas como el MTA, la base de datos y los paquetes de seguridad.

El agente de transferencia de correos (Mail Transfer Agent o MTA) enruta los mensajes de correo al servidor de Zimbra. Este servicio está basado en el popular Postfix. Integrado a través de Postfix, Zimbra incorpora varios filtros de seguridad, como antivirus y antispam, entre otros.

Soporta por defecto los protocolos principales de cifrado de canal, SSL y TLS. Los filtros en el lado del servidor mediante James/Sieve.

En Zimbra Collaboration Suite hay diversos almacenes de datos para la información de los usuarios:

- OpenLDAP proporciona la autenticación.
- MySQL guarda las preferencias, metadatos de los mensajes y el sistema de ficheros guarda directamente los mensajes de correo.

Otro componente integrado en Zimbra es Lucene, un potente motor de indexación y búsquedas que permite a los usuarios y administradores buscar mensajes a través de múltiples carpetas de correo, tanto metadatos como contenidos en el cuerpo del mensaje.

En términos generales, las funcionalidades ofrecidas por Zimbra son muy similares a las de Microsoft Exchange, aunque está mejor preparado para ser utilizado por proveedores de hosting y tiene algunas características de colaboración que

Exchange no tiene. Además, una gran diferencia la marcan los bindings de SOAP que permiten integraciones de terceros que amplíen las funcionalidades de Zimbra

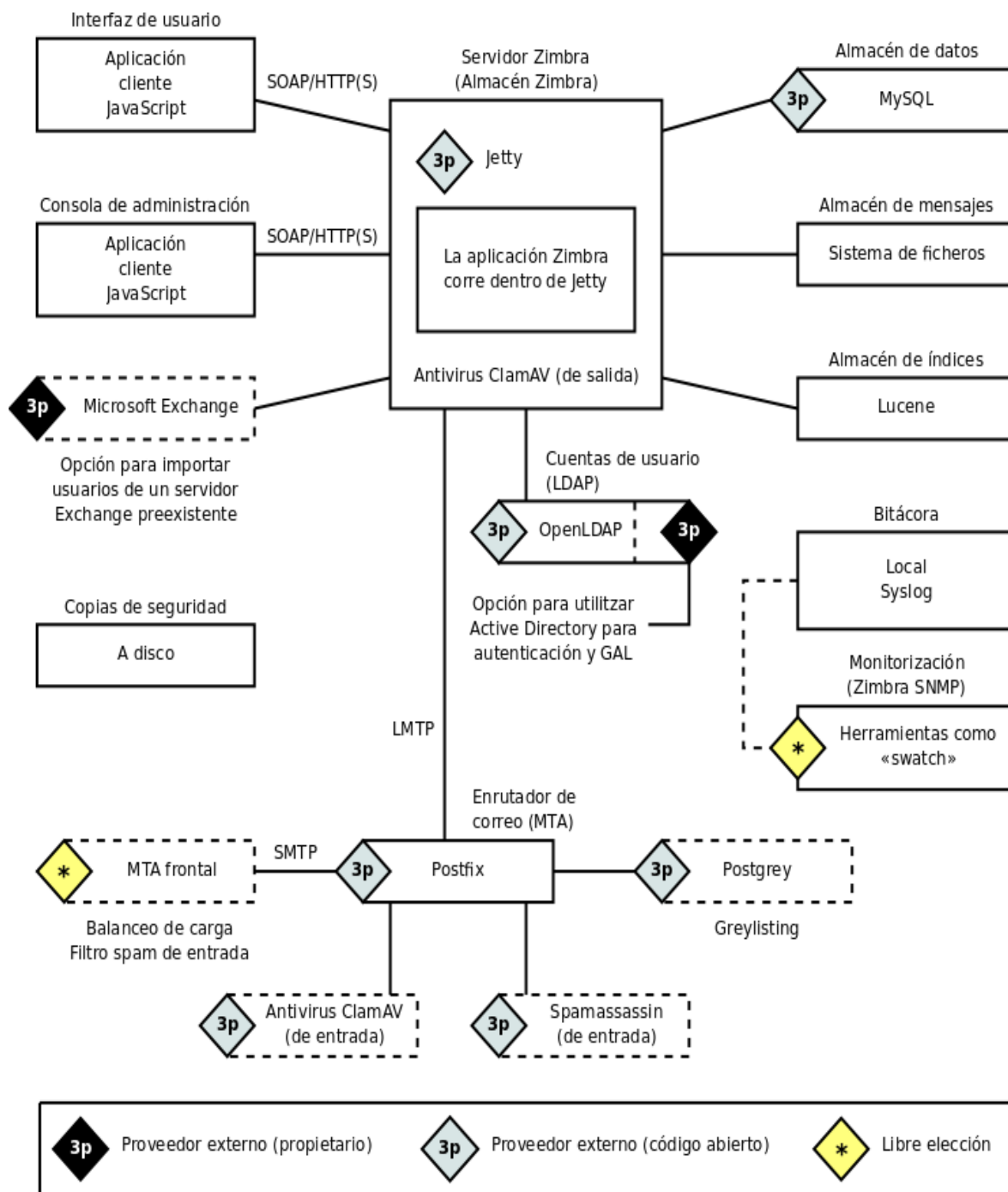


Figura 2.5.1. Arquitectura Zimbra.

Fuente: http://wiki.zimbra.com/images/f/f0/2_Overview_System_Architecture.2.1.1.jpg

2.5.2. COMPONENTES DE LA ARQUITECTURA

La arquitectura del sistema está formada por los siguientes componentes.

- **Zimbra Core**

Zimbra Core incluye las librerías, utilidades, herramientas de monitorización y ficheros básicos de configuración.

- **Zimbra LDAP**

Zimbra Collaboration Suite utiliza por defecto OpenLDAP para almacenar y gestionar el almacén de usuarios, integrando de serie el soporte para la replicación. Permite fácilmente su configuración para el uso de directorios LDAP externos, incluyendo Active Directory de Microsoft o eDirectory de Novell, entre otros.

El esquema LDAP de Zimbra está disponible por si se desea utilizarlo en una instalación LDAP ya existente, facilitando de esta manera la gestión centralizada de las cuentas de usuario de nuestra instalación. Cada cuenta tiene un identificador único de buzón de correo, que representa el punto principal de identificación en todo el sistema. El esquema de OpenLDAP ha sido modificado para adaptarlo a las necesidades de ZCS.

- **Zimbra MTA**

Uno de los componentes claves de cualquier solución de mensajería, el servidor de correo electrónico de Zimbra está formado, como es habitual, de diversas partes.

Un MTA (Mail Transport Agent) es un almacén de buzones de correo accesible por IMAP4 y POP3, con soporte para cifrado del canal mediante (SSL) unos filtros de contenidos (antivirus y antispam).

Zimbra utiliza Amavis como filtro de contenidos y, por defecto, SpamAssassin y ClamAV como filtros antispam y antivirus, respectivamente. Es posible configurarlo para que utilice cualquier otro filtro antispam, como Dspam, o antivirus. El correo se recibe mediante SMTP, se enruta mediante una tabla de transportes y se entrega al almacén de correo haciendo uso del protocolo LMTP.

- **Zimbra Store**

Zimbra Store, utilizando Jetty como contenedor de servlets, almacena el correo electrónico. Cada cuenta se configura en un servidor, y esta cuenta está asociada con un buzón de correo que contiene todos los mensajes y ficheros adjuntos.

El servidor de buzones está formado por.

- El almacén de datos.
- El almacén de mensajes.
- El almacén de índices.

Las utilidades de conversión de adjuntos a HTML.

Cada servidor de Zimbra tiene su propio almacén de datos, almacén de mensajes y almacén de índices para los buzones de ese servidor. En cuanto llega un correo, el servidor de Zimbra crea un nuevo proceso para indexar el mensaje. También se crea un hilo para la conversión de adjuntos a formato HTML, que a su vez es indexado por otro hilo.

El almacén de datos es una base de datos MySQL en la cual los identificadores de mensajes son enlazados con las cuentas de usuario. El almacén de datos relaciona el identificador del buzón con la cuenta de usuario a la que pertenece en el directorio LDAP. Esta base de datos contiene el conjunto de etiquetas definido por el usuario, las carpetas, las citas del calendario y los contactos de los usuarios, así como el estado de cada mensaje de correo (leídos, no leídos, etiquetas asociadas a cada mensaje y la carpeta en la cual reside el mensaje).

El almacén de mensajes guarda todos los mensajes y sus adjuntos en formato MIME (Multipart Internet Mail Extension). Los mensajes enviados a múltiples destinatarios dentro del mismo servidor sólo son almacenados una vez.

La tecnología necesaria para indexar y buscar la proporciona Lucene. Se mantienen índices sobre cada buzón.

- **Zimbra SNMP y Zimbra Logger.**

La instalación de ambos paquetes es opcional, pero muy recomendada. En cada servidor donde esté instalado, Zimbra SNMP recoge información periódica del estado del sistema. Además, utiliza Swatch para analizar la salida del syslog y generar los traps de SNMP.

Por su parte, Zimbra Logger instala herramientas de agregación de logs, informes y seguimiento de mensajes. Sin este paquete no se podrán utilizar las funcionalidades de seguimiento de mensajes y estadísticas del servidor de la consola gráfica de administración.

- **El cliente web**

Zimbra incorpora un cliente web que hace un uso extensivo de AJAX (Asynchronous Javascript and XML) y que se ejecuta en la mayoría de los navegadores web más habituales, como Firefox, Safari e Internet Explorer. Debido al uso intensivo de Javascript, las diferencias en la experiencia del usuario son enormes dependiendo del navegador, siendo Opera y Safari los mejores e Internet Explorer 6 el peor. En cualquier caso, el cliente web de Zimbra permite utilizar una versión sólo con HTML que es muy recomendable para equipos antiguos pero que, asimismo, ofrece una usabilidad muy buena.

El cliente web de Zimbra ofrece unas avanzadas funcionalidades, casi al mismo nivel que una aplicación de escritorio, pero con la ventaja de poder utilizarlo desde cualquier lugar y desde casi cualquier navegador. Su gestor de correo permite, entre otros.

- Agrupar los correos por conversación, ahorrando así espacio en la pantalla.
- Construir, de manera gráfica, búsquedas avanzadas y guardarlas para su posterior reutilización.
- Etiquetar contenidos, ver documentos adjuntos sin necesitar ninguna aplicación externa.

La gestión de contactos de Zimbra es muy completa, ya que soporta múltiples libretas de direcciones (tanto personales como de cuentas del sistema), compartición de contactos, autocompletado y creación de listas de distribución personales.

El calendario compartido es una de las características más destacadas de Zimbra, con capacidad para detectar, visualizar y corregir solapamientos. Permite gestión de recursos (salas de reuniones, proyectores, etc.), programación de reuniones en grupo con delegación del acceso, compartición y publicación del calendario con otros usuarios y suscripción a calendarios remotos en formato iCal.

Zimbra incorpora una gestión documental en línea. Mediante una interfaz WYSIWYG es posible crear documentos en un formato de texto tipo RTF a los que adjuntar, por ejemplo, hojas de cálculo o imágenes mediante la tecnología ALE (AJAX Linking and Embedding). Esta gestión documental puede adquirir la forma de un wiki, permitiendo que los documentos sean creados, actualizados y compartidos entre todos los usuarios.

La publicación y compartición de contenidos es homogénea en todo el sistema tanto para contactos, como para el calendario o los documentos. Esta compartición puede realizarse con usuarios internos y externos del sistema. El cliente de correo permite la gestión de varias identidades y de varias cuentas de correo, incluyendo la agregación de cuentas externas mediante POP3.

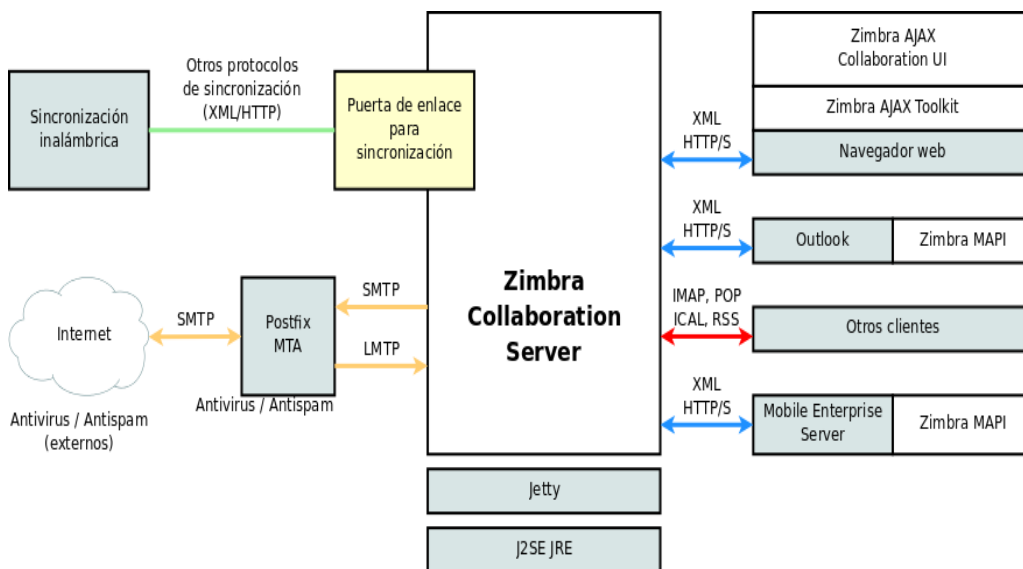


Figura 2.5.2. Zimbra Collaboration Server.

Fuente: http://linuxsilo.net/articles/zimbra/zimbra_architecture_backend.png

2.5.3. EL SERVIDOR ZIMBRA.

Zimbra Server (o Zimbra Store) es el núcleo de Zimbra Collaboration Suite. Está diseñado sobre una arquitectura extremadamente estable y modular usando tecnologías de código abierto contrastadas. Este servidor incluye soporte para

multitud de protocolos estándares que le permiten interactuar con los clientes de software más populares.

El servidor de Zimbra empaqueta todos los componentes principales en un simple instalador y utiliza, entre otras, tecnologías como Linux, Jetty, Postfix, MySQL, OpenLDAP y Lucene y soporta, entre otros, protocolos tales como SMTP, LMTP, SOAP, XML, IMAP, POP, iCal y CalDAV.

Zimbra es un servidor muy rápido y eficiente que, además, permite escalar de manera horizontal, pues cada host incluye su propio almacén de buzones de correo y de datos de configuración. Zimbra puede crecer añadiendo más máquinas con subdominios diferentes y mantener una gestión centralizada dentro del mismo dominio principal.

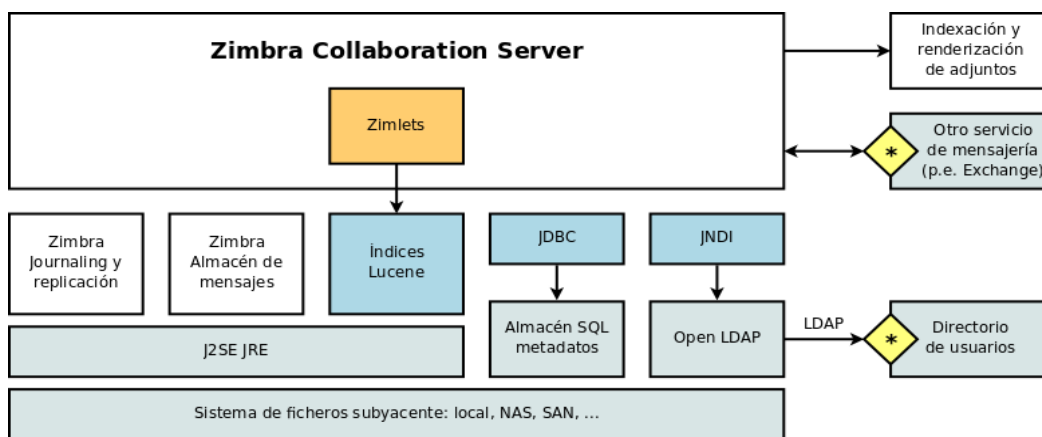


Figura 2.5.3. Zimbra Collaboration Server.

Fuente: <http://linuxsilo.net/articles/zimbra>

Zimbra, por supuesto, soporta múltiples dominios y también perfiles de usuarios, que denomina COS (Class Of Service). En estas clases de servicio se pueden definir las cuotas de almacenamiento y las características a las cuales tendrán acceso los usuarios. La siguiente lista presenta las más destacadas en su versión actual.

- Correo electrónico.

- Libreta de direcciones.
- Calendario de citas.
- Tareas.
- Documentos.
- Maletín.
- Mensajería instantánea.
- Preferencias.
- Etiquetado.
- Compartición.
- Cambio de contraseña.
- Elección de tema.
- Redacción de correos en formato HTML.
- Atajos de teclado.
- Acceso al Global Address List (GAL).
- Acceso externo por IMAP4/POP3.
- Creación de una dirección de reenvío automático del correo.
- Creación de una respuesta automática a la recepción de correos.
- Filtros de correo.
- Gestión de calendarios de grupos.
- Búsquedas avanzadas.
- Guardar búsquedas.

2.5.4. CLIENTE DE WEB DE ZIMBRA MANUAL PARA LOS USUARIOS.

Zimbra es una herramienta de colaboración que combina herramientas de correo electrónico, calendarios, libreta de direcciones. Todas estas herramientas se encuentran al utilizar el cliente de web en una misma dirección y un solo login.

2.5.5. INSTRUCCIONES DE INGRESO EN EL SISTEMA.

- Vaya a la dirección que le dio el administrador del sistema.

- Introduzca el usuario que le indicó el administrador del sistema
- Introduzca la clave que le indicó el administrador del sistema
- Escoja el tipo de cliente de web que quiere usar (Avanzado (Ajax), Normal (HTML) o Mobile).
- Clic el botón “Log In”
- Si es la primera vez que entra, cambie su clave.
- Ingrese a la pestaña “Preferencias” y luego el botón “Cambiar contraseña”. Se abrirá una nueva ventana.
- Introduzca su contraseña actual y luego la nueva contraseña dos veces.
- Clic en el botón “Cambiar contraseña” para guardar los cambios.



Figura 2.5.4. Acceso web cliente Zimbra.

Fuente: Autor tesis Henry Padilla

2.5.6. EXPLORAR LAS DIFERENTES APLICACIONES.

Debajo de los campos para buscar información en Zimbra y buscar información en Internet, aparecen los tabs con las diferentes aplicaciones que componen Zimbra: Correo, Libreta de direcciones, Agenda, Tareas, Mensajería Instantánea (MI Beta), Bloc de notas, Maletín y Preferencias.

A la izquierda usted verá su nombre y cuanto espacio está ocupando en el servidor. Si el administrador del sistema ha configurado cuotas de espacio. Se mostrará cuanto espacio está utilizando de su cuota. Debajo del nombre se muestran las carpetas y subcarpetas donde usted puede almacenar y clasificar los correos. Luego vienen las Etiquetas y los Zimlets (Aplicaciones que se usan para recibir información de otros sistemas).

Al final viene un calendario, en el que usted puede tocar una fecha para ver la agenda de ese día.

Cuando usted escoja una aplicación, aparecerá una barra de herramientas con opciones específicas para la aplicación seleccionada.

Note también que hay opciones de “Ayuda” y “Salir” en la esquina superior derecha de la aplicación.

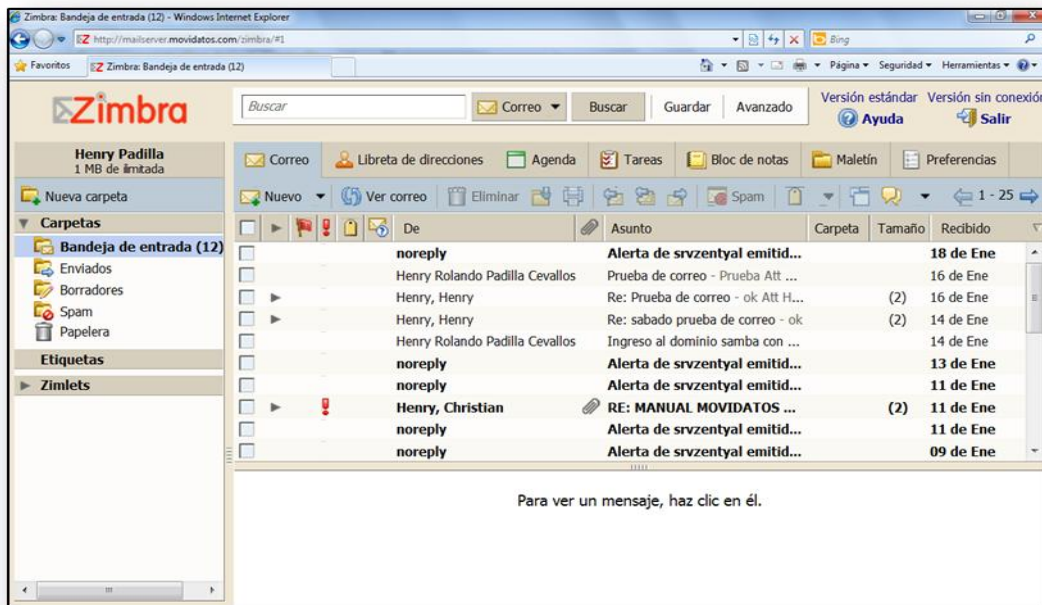


Figura 2.5.5. Acceso web cliente Zimbra.

Fuente: Autor tesis Henry Padilla

2.5.7. CONFIGURANDO LAS PREFERENCIAS

Zimbra fue instalado con la configuración por defecto, pero se puede cambiar la forma de como se ve y comporta Zimbra ajustando las opciones mostradas en el tab “Preferencias”.

Se puede revisar que la nueva barra con tabs que aparece cuando entra a esta opción.

General, correo, redactar, firmas, libreta de direcciones, cuentas, filtros de correo, agenda, mensajería instantánea, accesos directos.

Para terminar clic en “Guardar”, que se encuentra a la izquierda, encima de la barra de herramientas después de hacer cambios y antes de pasar a otra aplicación.

2.5.8. ALGUNOS DETALLES IMPORTANTES DE LAS OPCIONES DE CONFIGURACIÓN:

- **Correo:** Usted puede cargar el correo nuevo al buzón de entrada al tocar el botón “Ver Correo” cuando esté en la aplicación de Correo.

En esta opción, también puede configurar el mensaje que se desplegará cuando esté fuera de la oficina, ya sea en un viaje de negocios o por vacaciones.

Para configurar este mensaje, marque la casilla “Enviar respuesta por ausencia”, e introduzca el texto que quiera que aparezca en el correo.

Cuando vuelva de vacaciones desmarque la casilla “Enviar respuesta por ausencia”

- **Redactar:** Permite redactar mensajes con diferentes tipos de letra, colores e imágenes, escoja redactar los mensajes en HTML.
- **Firmas:** Permite crear múltiples firmas para los correos electrónicos, cada una con un nombre único.

Cuentas: Defina aquí la firma por defecto a utilizar en todos los correos. Cuando usted esté creando un nuevo correo, podrá escoger otra firma o no firmar el correo.

- **Calendario:** Al dejar marcada la opción “Siempre mostrar agenda en miniatura”, quedará activado el mini calendario a la izquierda y le permitirá ver rápidamente citas y reuniones al sobreponer el cursor en una fecha específica.
- **Accesos directos:** Le permite configurar combinaciones de teclas para ir rápidamente a las diferentes opciones.

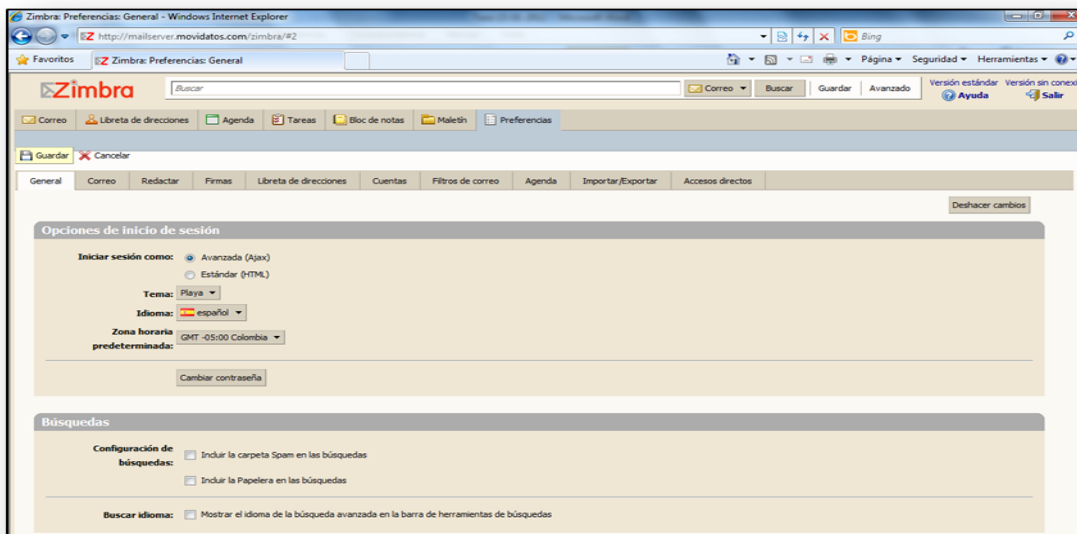


Figura 2.5.6. Opciones cliente web Zimbra

Fuente: Autor tesis Henry Padilla.

2.5.9. USANDO LAS BÚSQUEDAS RÁPIDAS.

La función para buscar información almacenada en Zimbra, está a la derecha del logo de Zimbra

Verificar el tipo de item que quiere buscar. Si no selecciona es tipo de item, la búsqueda se hará de acuerdo a la aplicación que tenga activa en el momento de la búsqueda.

Si se requiere incluir la carpeta de Spam y Basura en las búsquedas, configure las opciones apropiadas en “Preferencias General Búsquedas”.

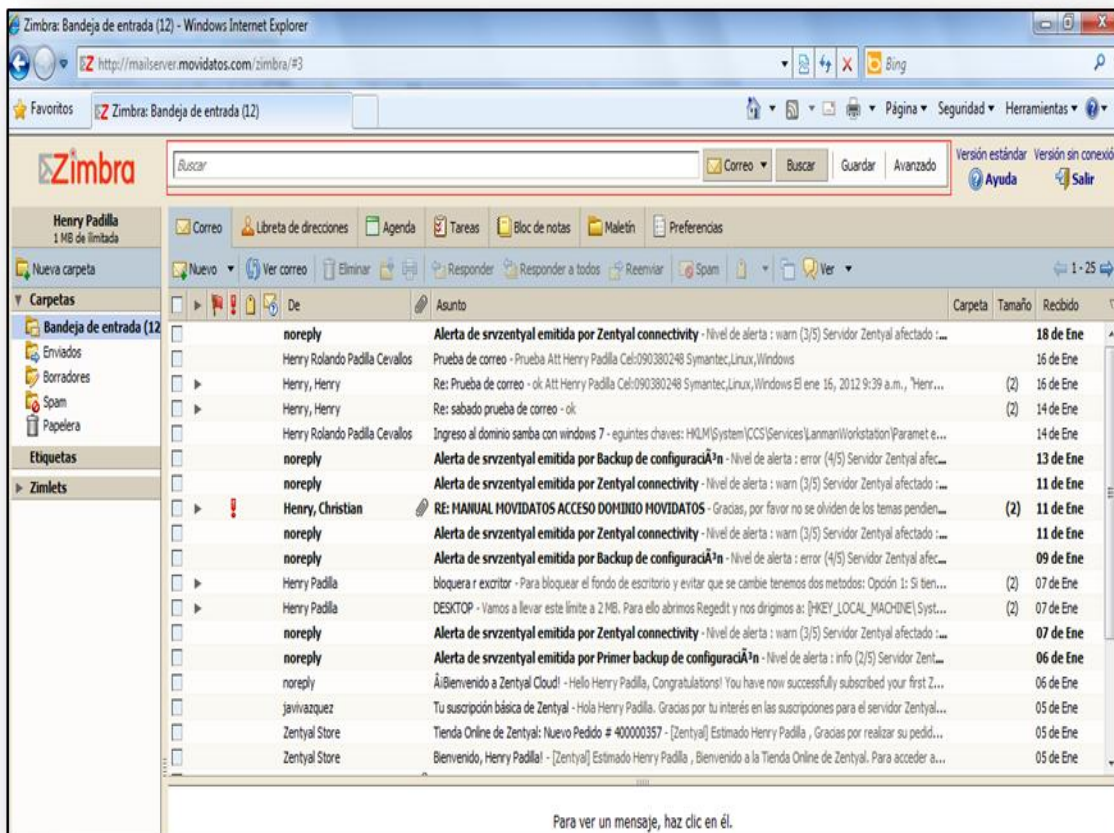


Figura 2.5.7. Cliente web Zimbra

Fuente: Autor tesis Henry Padilla.

CAPÍTULO 3.

3.1. ZENTYAL.

3.1.1. SERVIDOR LINUX PARA PYMES.

Zentyal se desarrolló con el objetivo de acercar Linux a las PYMES y permitirles aprovechar todo su potencial como servidor de empresa. Es la alternativa en código abierto a Windows Small Business Server, basado en la popular distribución Ubuntu. Zentyal permite a profesionales TIC administrar todos los servicios de una red informática, tales como el acceso a Internet, la seguridad de la red, la compartición de recursos, la infraestructura de la red o las comunicaciones, de forma sencilla y a través de una única plataforma.

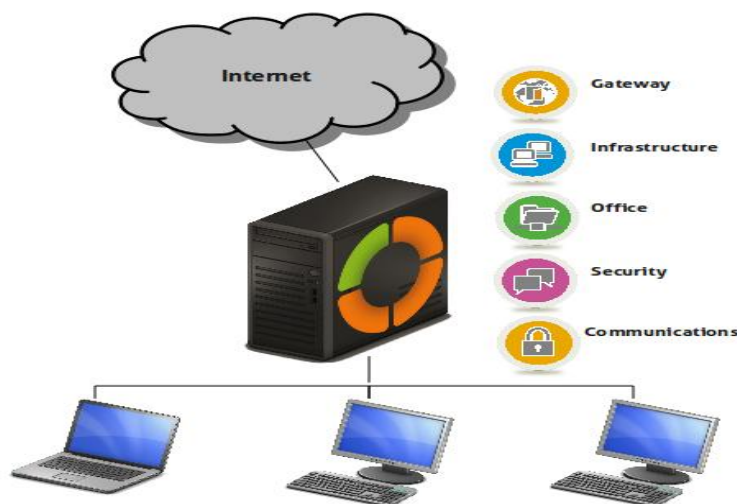


Figura 3.1.1 Zentyal sus funcionalidades.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Durante su desarrollo se hizo un especial énfasis en la usabilidad, creando una interfaz intuitiva que incluye únicamente aquellas funcionalidades de uso más frecuente, aunque también dispone de los medios necesarios para realizar toda clase de configuraciones.

Otra de las características más importantes de Zentyal es que todas sus funcionalidades, construidas a partir de una serie de aplicaciones en principio independientes, están estrechamente integradas entre sí, automatizando la mayoría de las tareas y ahorrando tiempo en la administración de sistemas. Teniendo en cuenta que el 42% de los fallos de seguridad y el 80% de los cortes de servicio en una empresa se deben a errores humanos en la configuración y administración de los mismos, el resultado es una solución no sólo más sencilla de manejar sino también más segura y fiable. Además de acercar Linux y el Software Libre a las PYMES con los importantes ahorros que ello supone, Zentyal mejora la seguridad y disponibilidad de los servicios en la empresa.

Se estima que hay más de 50.000 instalaciones activas de Zentyal, principalmente en América y Europa, aunque su uso está extendido a prácticamente todos los países del globo, siendo Estados Unidos, Alemania, España, Brasil y Rusia los países que cuentan con más instalaciones. Zentyal se usa principalmente en PYMES, pero también en otros entornos como centros educativos, administraciones públicas, hospitales o incluso en instituciones de alto prestigio como la propia NASA.

El desarrollo de Zentyal está financiado por eBox Technologies que además ofrece a las PYMES y a otros usuarios de Zentyal de todo el mundo herramientas y servicios de gestión orientados a reducir los costes de mantenimiento de la infraestructura TIC.

Estas herramientas y servicios comerciales se ofrecen a los clientes a través de las suscripciones a Zentyal Cloud, que incluyen:

- Actualizaciones del sistema con garantía de calidad.
- Notificaciones y alertas del servidor.
- Informes periódicos sobre el uso del sistema.
- Monitorización y administración centralizada de múltiples servidores Zentyal.

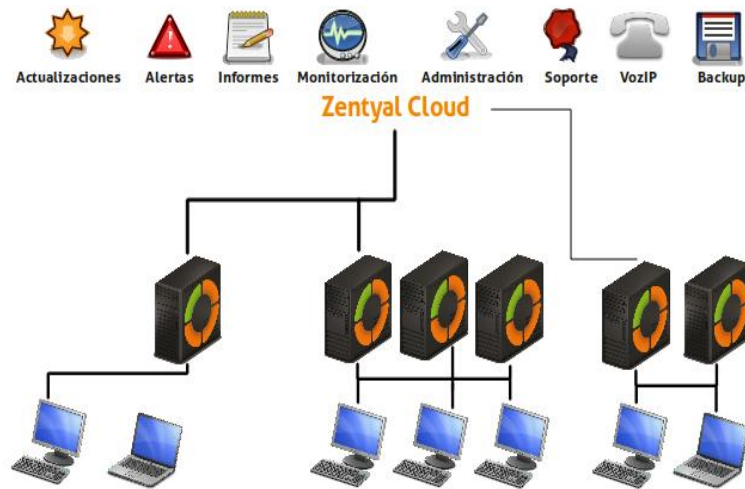


Figura 3.1.2 Zentyal Cloud.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Zentyal Cloud garantiza una red segura y actualizada a un nivel profesional con un coste reducido

Las suscripciones están dirigidas a dos tipos de clientes claramente diferenciados. Por un lado la Suscripción Profesional está dirigida a pequeñas empresas o proveedores TIC con un número reducido de servidores Zentyal que deben ser mantenidos al día, asegurando su continuo funcionamiento, que se benefician de las actualizaciones garantizadas, las alertas y los informes.

Por otra parte, la Suscripción Empresarial está dirigida a grandes empresas o proveedores de servicios gestionados que además tienen la necesidad de monitorizar y administrar múltiples instalaciones Zentyal de forma remota. Así mismo, los clientes que dispongan de una suscripción, pueden obtener acceso a suscripciones adicionales como la recuperación de desastres, actualizaciones avanzadas de seguridad o suscripciones de Zarafa.

Estas suscripciones se complementan con otros servicios adicionales como formación, despliegue o soporte técnico provistos generalmente por alguno de sus

partners certificados. Zentyal dispone de una Red Global de Partners en rápida expansión, a través de la cual consigue llevar la atención necesaria para distribuir el producto y los servicios a las PYMES de todo el mundo. El estereotipo de los partners de Zentyal son proveedores locales de servicios TIC, consultores o proveedores de servicios gestionados que ofrecen un servicio de asesoría, despliegue, soporte y/o externalización completa de la infraestructura y servicios de red de sus clientes.

La combinación entre el servidor y las suscripciones aportan unos beneficios muy importantes que se traducen en ahorros superiores al 50% del coste total de instalación y mantenimiento de un servidor para PYMES, comparando los costes de Zentyal con los de una instalación típica de Windows Small Business Server.

3.1.2. ENTORNO GRÁFICO CON EL INTERFAZ DE ADMINISTRACIÓN.

Para comenzar a configurar los perfiles o módulos de Zentyal, establece el usuario y contraseña indicados durante la instalación. Cualquier otro usuario que se pueda posteriormente al grupo admin podrá acceder al interfaz de Zentyal al igual que tendrá privilegios de *sudo* en el sistema.

Configuración inicial.

Una vez autenticado por primera vez en la interfaz web comienza un asistente de configuración, en primer lugar podría seleccionar qué funcionalidades desea incluir en nuestro sistema.

Para simplificar nuestra selección, en la parte superior de la interfaz contamos con unos perfiles prediseñados.



Figura 3.1.3 Paquetes de Zentyal instalables.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.1.3. OPCIONES Y PAQUETES INSTALABLES DE ZENTYAL.

Perfiles de Zentyal que se podría instalar según el proyecto que se desea realizar:

- **Zentyal Gateway.**

Zentyal actúa como la puerta de enlace de la red local ofreciendo un acceso a Internet seguro y controlado.

- **Zentyal Unified Threat Manager.**

Zentyal protege la red local contra ataques externos, intrusiones, amenazas a la seguridad interna y posibilita la interconexión segura entre redes locales a través de Internet u otra red externa.

- **Zentyal Infrastructure.**

Zentyal gestiona la infraestructura de la red local con los servicios básicos: DHCP, DNS, NTP, servidor HTTP, etc.

- **Zentyal Office.**

Zentyal actúa como servidor controlador de dominio como también de recursos compartidos de la red local: ficheros, impresoras, calendarios, contactos, perfiles de usuarios y grupos, etc.

Zentyal Unified Communications.

Zentyal se convierte en el centro de comunicaciones de la empresa, incluyendo correo, mensajería instantánea y Voz IP.

Entre las opciones puede seleccionar varios perfiles para hacer que Zentyal tenga, de forma simultánea, diferentes roles en la red.

También se podría instalar un conjunto manual de servicios simplemente con un clic sobre sus respectivos iconos sin necesidad de amoldarnos a los perfiles, o bien, instalar un perfil más unos determinados paquetes que también nos interesen.

Como ejemplo se indicará una instalación del perfil de Gateway únicamente.

Al terminar la selección, se instalarán también los paquetes adicionales necesarios y además si hay algún complemento recomendado se preguntará si se desea instalar. Esta selección no es definitiva, ya que posteriormente puede instalar y desinstalar el resto de módulos de Zentyal a través de la gestión de software.

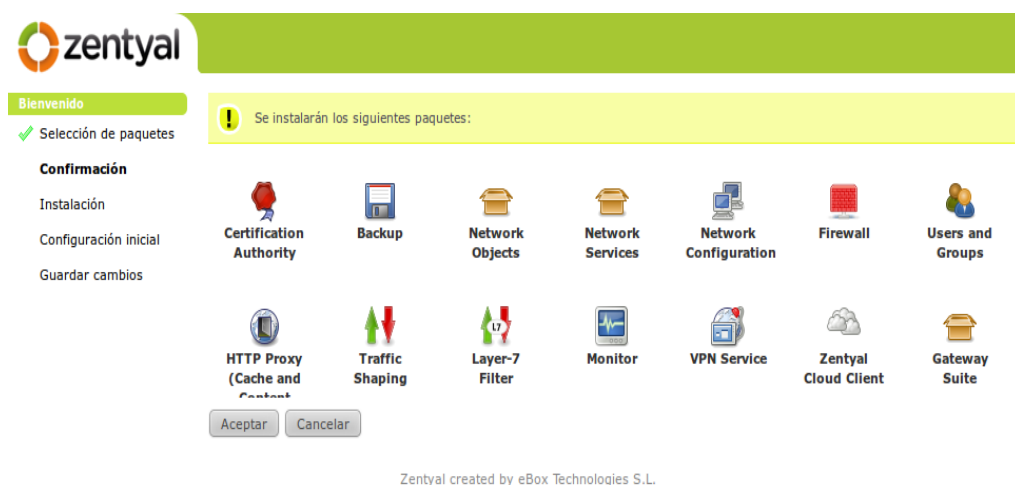


Figura 3.1.4. Funcionalidades Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Paquetes adicionales.

El sistema comenzará con el proceso de instalación de los módulos requeridos, mostrando una barra de progreso donde además se puede leer una breve introducción sobre las funcionalidades y servicios adicionales disponibles en Zentyal.

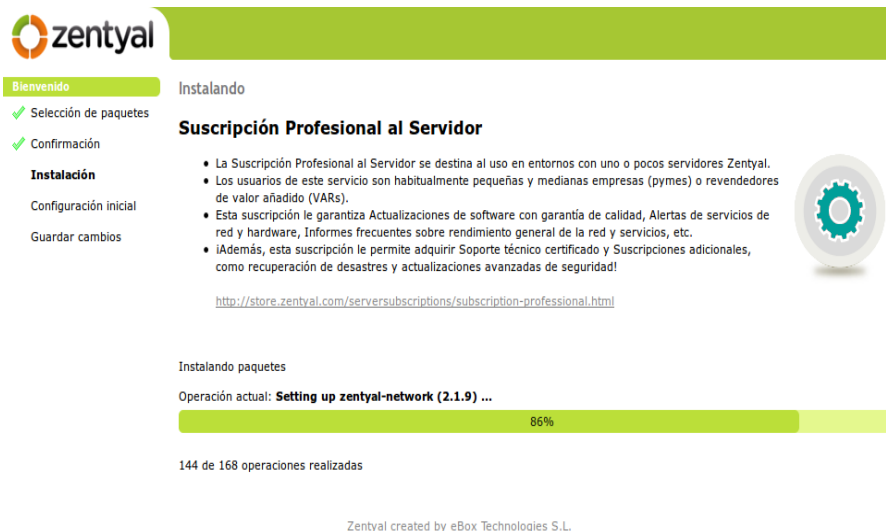


Figura 3.1.5. Instalación paquetes Zentyal.
Fuente: <http://www.zentyal.com/es/small-business-it/>

Una vez terminado el proceso de instalación el asistente configurará los nuevos módulos realizando algunas preguntas.

En primer lugar se solicitará información sobre la configuración de red, definiendo para cada interfaz de red si es interna o externa, es decir, si va a ser utilizada para conectarse a Internet u otras redes externas, o bien, si está conectada a la red local. Se aplicarán políticas estrictas en el cortafuego para todo el tráfico entrante a través de interfaces de red externas.



Figura 3.1.6. Configuración de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.1.4. SELECCIONAR MODO DE LAS INTERFACES DE RED

Según el tipo de servidor para el modo de operación del módulo *Usuarios y Grupos*. Si sólo se va a tener un servidor la mejor opción es *Servidor stand-alone*. Si por el contrario estamos desplegando una infraestructura maestro-esclavo con varios servidores Zentyal y gestión de usuarios y grupos centralizada o si se desea sincronizar los usuarios con un Microsoft Active Directory, la mejor opción es *Configuración avanzada*. Este paso aparecerá solamente si el módulo *Usuarios y Grupos* están instalados. Configurar el modo de *Usuarios y Grupos* puede tomar unos minutos.

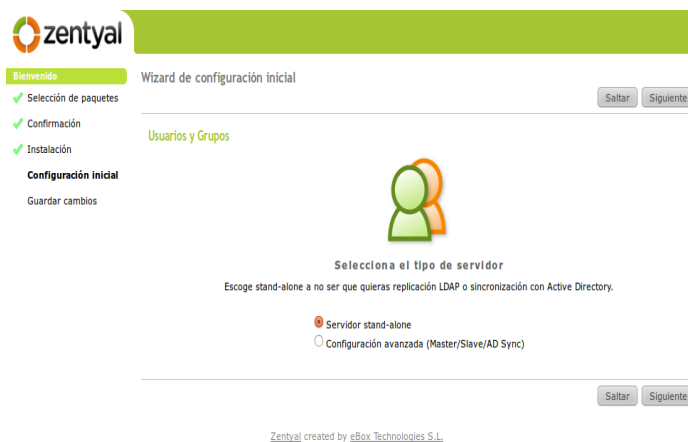


Figura 3.1.7. Configuración servidor Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.1.5. MODO DE OPERACIÓN DE USUARIOS Y GRUPOS.

El último asistente permite suscribir el servidor a Zentyal Cloud. En caso de tener una suscripción registrada tan sólo es necesario introducir los credenciales. Si todavía no tienes un usuario en Zentyal Cloud es posible registrar automáticamente una cuenta con suscripción básica gratuita.

En ambos casos el formulario solicita un nombre para el servidor. Éste es el nombre que lo identificará dentro de la interfaz de Zentyal Cloud.

Figura 3.1.8. Suscripción servidor Zentyal Cloud.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.1.6. ASISTENTE DE SUSCRIPCIÓN A ZENTYAL CLOUD.

Una vez hayan sido respondidas estas cuestiones, se procederá a la configuración de cada uno de los módulos instalados.

Figura 3.1.9. Zentyal Cloud.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Configuración inicial finalizada

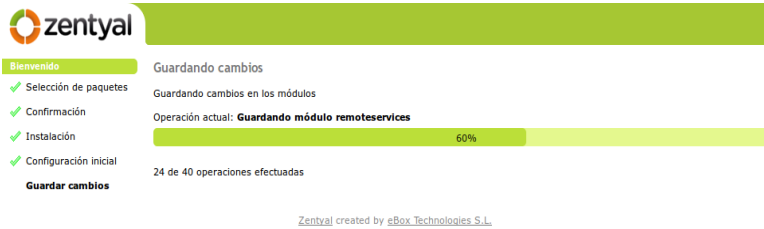


Figura 3.1.10. Zentyal Cloud.

Fuente: <http://www.zentyal.com/es/small-business-it/>

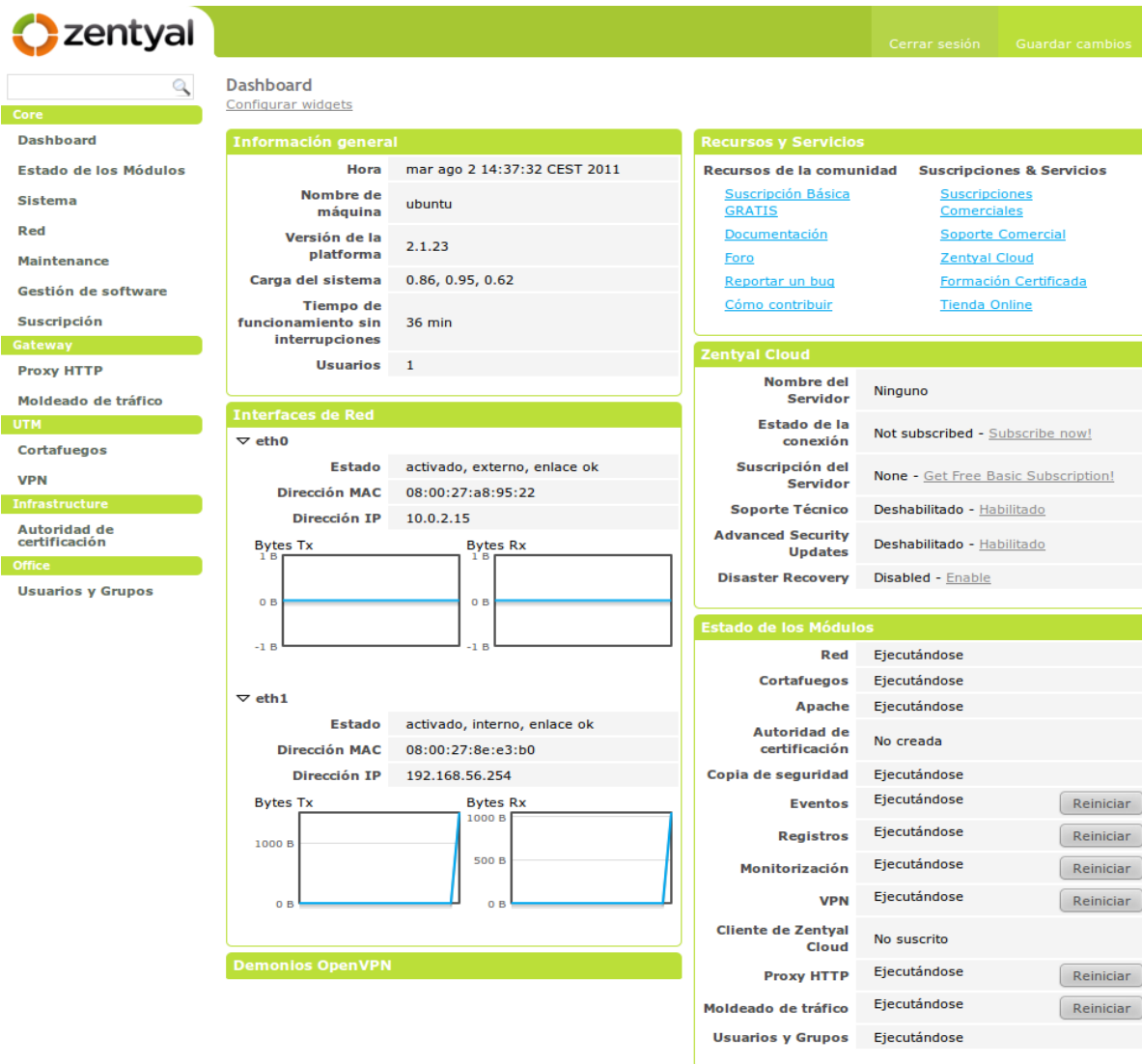


Figura 3.1.11. Zentyal Dashboard..

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.2. PRIMEROS PASOS CON ZENTYAL

3.2.1. LA INTERFAZ WEB DE ADMINISTRACIÓN DE ZENTYAL.

Una vez instalado Zentyal, se accederá a la interfaz web de administración tanto a través del propio entorno gráfico que incluye el instalador como desde cualquier lugar de la red interna, mediante la dirección `https://192.168.0.5` , donde *direccion_ip* es la dirección IP o el nombre de la máquina donde está instalado Zentyal que resuelve a esa dirección. Dado que el acceso es mediante HTTPS, la primera vez el navegador nos pedirá si confiar en un certificado digital para este sitio, para aceptar el certificado autogenerado.

Para acceder a la interfaz web se debe usar Mozilla Firefox, ya que otros navegadores como Microsoft Internet Explorer no están soportados.

La primera pantalla solicita el nombre de usuario y la contraseña, podrán autenticarse como administradores tanto el usuario creado durante la instalación como cualquier otro perteneciente al grupo admin.



Figura 3.2.1. Acceso Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Login

Una vez autenticados, aparecerá la interfaz de administración que se encuentra dividida en tres partes fundamentales.

Menú lateral izquierdo:

Contiene los enlaces a todos los servicios que se pueden configurar mediante Zentyal, separados por categorías. Cuando se ha seleccionado algún servicio en este menú puede aparecer un submenú para configurar cuestiones particulares de dicho servicio.

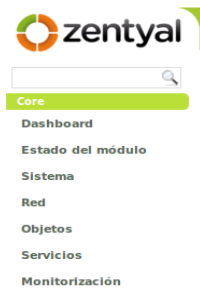


Figura 3.2.2. Panel de administración Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Menú lateral

Menú superior:

Contiene las **acciones**: guardar los cambios realizados en el contenido y hacerlos efectivos, así como el cierre de sesión



Figura 3.2.3. Menú superior Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Menú superior

Contenido principal:

El contenido, que ocupa la parte central, comprende uno o varios formularios o tablas con información acerca de la configuración del servicio seleccionado a través del menú lateral izquierdo y sus submenús.

Selecciona informe

Dominio	Informe completo	Informe resumido
Firewall		
DHCP		--
Events		
IDS		
VPN		--
Printers		--
Samba access		--
Samba virus		--
Samba quarantine		--
Proxy HTTP		

10 ▼ Página 1 

Figura 3.2.4. Servicios Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.2.2. EL DASHBOARD.

El Dashboard es la pantalla inicial de la interfaz. Contiene una serie de widgets configurables. En todo momento se pueden reorganizar pulsando en los títulos y arrastrándolos.

Pulsando en Configurar Widgets la interfaz cambia, permitiendo retirar y añadir nuevos widgets. Para añadir uno nuevo, se busca en el menú superior y se arrastra a la parte central. Para eliminarlos, se usa la cruz situada en la esquina superior derecha de cada uno de ellos.



Figura 3.2.5. Funcionamiento de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Configuración del Dashboard

Hay un widget importante dentro del Dashboard que muestra el estado de todos los módulos instalados en Zentyal.

Estado del módulo	
Red	Ejecutándose
Cortafuegos	Ejecutándose
Antivirus	Ejecutándose <input type="button" value="Reiniciar"/>
Apache	Ejecutándose
Autoridad de certificación	Disponible
DHCP	Ejecutándose <input type="button" value="Reiniciar"/>
DNS	Ejecutándose <input type="button" value="Reiniciar"/>
Copia de seguridad	Deshabilitado
Eventos	Ejecutándose <input type="button" value="Reiniciar"/>
IDS	Ejecutándose <input type="button" value="Reiniciar"/>
Registros	Ejecutándose <input type="button" value="Reiniciar"/>
Monitorización	Ejecutándose <input type="button" value="Reiniciar"/>
NTP	Ejecutándose <input type="button" value="Reiniciar"/>
VPN	Ejecutándose <input type="button" value="Reiniciar"/>
Compartir Impresoras	Ejecutándose <input type="button" value="Reiniciar"/>
RADIUS	Ejecutándose <input type="button" value="Reiniciar"/>
Ciente de Zentyal Cloud	Suscrito
Compartir ficheros	Ejecutándose <input type="button" value="Reiniciar"/>
Proxy HTTP	Ejecutándose <input type="button" value="Reiniciar"/>
Moldeado de tráfico	Ejecutándose <input type="button" value="Reiniciar"/>
Rincón del Usuario	Deshabilitado
Usuarios y Grupos	Ejecutándose

Figura 3.2.6. Estado servicios de Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.2.3. CONFIGURACIÓN DEL ESTADO DE LOS MÓDULOS.

Zentyal tiene un diseño modular, en el que cada módulo gestiona un servicio distinto. Para poder configurar cada uno de estos servicios se ha de habilitar el módulo correspondiente desde *Estado del módulo*. Todas aquellas funcionalidades que hayan sido seleccionadas durante la instalación se habilitan automáticamente.

Configuración del estado de los módulos

Módulo	Depende	Estado
Red		<input checked="" type="checkbox"/>
Cortafuegos	Red	<input checked="" type="checkbox"/>
Antivirus		<input checked="" type="checkbox"/>
DHCP	Red	<input checked="" type="checkbox"/>
DNS		<input checked="" type="checkbox"/>
Copia de seguridad		<input type="checkbox"/>
Eventos		<input checked="" type="checkbox"/>
IDS	Red	<input checked="" type="checkbox"/>
Registros		<input checked="" type="checkbox"/>
Monitorización		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>
VPN	Red, Cortafuegos	<input checked="" type="checkbox"/>
Moldeado de tráfico	Red, Cortafuegos	<input checked="" type="checkbox"/>
Usuarios y Grupos		<input checked="" type="checkbox"/>
RADIUS	Usuarios y Grupos	<input checked="" type="checkbox"/>
Compartir ficheros	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>
Proxy HTTP	Cortafuegos, Usuarios y Grupos, Antivirus	<input checked="" type="checkbox"/>
Rincón del Usuario	Usuarios y Grupos	<input type="checkbox"/>
Compartir Impresoras	Compartir ficheros	<input checked="" type="checkbox"/>

Figura 3.2.7. Configuración de módulos Zentyal.
Fuente: <http://www.zentyal.com/es/small-business-it/>

Configuración del estado del módulo.

Cada módulo puede tener dependencias sobre otros para que funcione. Por ejemplo, el módulo DHCP necesita que el módulo de red esté habilitado para que pueda ofrecer direcciones IP a través de las interfaces de red configuradas. La dependencia se muestran en la columna *Depende* y hasta que esta no se habiliten, no se puede habilitar tampoco el módulo.

La primera vez que se habilita un módulo, se pide confirmación de las acciones que va a realizar en el sistema así como los ficheros de configuración que va a sobrescribir. Tras aceptar cada una de las acciones y ficheros, habrá que guardar cambios para que la configuración sea efectiva.



Figura 3.2.8. Detalle de configuración de módulos Zentyal.
Fuente: <http://www.zentyal.com/es/small-business-it/>

Confirmación para habilitar un módulo.

Aplicando los cambios en la configuración.

Una particularidad importante del funcionamiento de Zentyal es su forma de hacer efectivas las configuraciones que se puede hacer en la interfaz. Para ello, primero se tendrán que aceptar los cambios en el formulario actual, pero para que estos cambios sean efectivos y se apliquen de forma permanente se tendrá que Guardar Cambios en el menú superior. Este botón cambiará a color rojo para indicarnos que hay cambios sin guardar. Si no se sigue este procedimiento se perderán todos los cambios que se hayan realizado a lo largo de la sesión al finalizar ésta. Una excepción a este funcionamiento es la gestión de usuarios y grupos, dónde los cambios se efectúan directamente.

Guardar Cambios.

Esta opción tiene la función de guardar todo cambio realizado en la configuración de Zentyal en sus diferentes servicios.

Advertencia.

La notificación de advertencia notifica cuando se ha ejecutado un cambio y solicita guardar o deshacer el cambio realizado en Zentyal.

Si se cambia la configuración de las interfaces de red, el cortafuego o el puerto del interfaz de administración, se podría perder la conexión teniendo que cambiar la URL en el navegador o reconfigurar a través del entorno gráfico en local.

3.2.4. CONFIGURACIÓN GENERAL.

Hay varios parámetros de la configuración general de Zentyal que se pueden modificar en Sistema › General.

The screenshot shows the Zentyal web interface. At the top, there is a green header with the Zentyal logo on the left and 'Cerrar sesión' and 'Guardar cambios' buttons on the right. Below the header is a search bar and the title 'Configuración General' with a '(show help)' link. The left sidebar contains a navigation menu with categories: Core (Dashboard, Estado de los Módulos, Sistema), Red, Mantenimiento, Gestión de software, Suscripción, Gateway, Proxy HTTP, Moldeado de tráfico, UTM, Cortafuegos, VPN, Infraestructure, and Office. The main content area is titled 'Configuración General' and contains several sections: 'Cambiar contraseña' with fields for 'Usuario' (administrador), 'Contraseña actual', 'Nueva contraseña', and 'Confirmar contraseña', and a 'Cambiar' button; 'Selección de idioma' with a dropdown menu set to 'Español' and a 'Cambiar' button; 'Zona Horaria' with dropdowns for 'Europe', 'Madrid', and a 'Cambiar' button; 'Fecha y Hora' with date and time pickers (3 / Agosto / 2011 and 20 / 1 / 5) and a 'Cambiar' button; 'Puerto TCP de la interfaz de administración' with a text input '443' and a 'Cambiar' button; and 'Cambiar nombre de la máquina' with a text input 'ubuntu' and a 'Cambiar' button.

Figura 3.2.9. Configuración general Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

- **Contraseña:**

Para cambiar la contraseña de un usuario. Será necesario introducir su nombre de *Usuario*, la Contraseña actual, la Nueva contraseña y confirmarla de nuevo en la sección Cambiar contraseña.

- **Idioma:**

Para seleccionar el idioma de la interfaz mediante *Selección de idioma*.

- **Zona Horaria:**

- Aquí para especificar nuestra ciudad y país para configurar el ajuste horario.

- **Fecha y Hora:**

Para especificar la fecha y hora del servidor, siempre y cuando no este sincronizando con un servidor de hora exterior (ver NTP).

- **Puerto del interfaz de administración:**

Por defecto es el 443 de HTTPS, pero si se desea utilizarlo para el servidor web, habrá que cambiarlo a otro distinto y especificarlo en la URL a la hora de acceder: `https://192.168.0.5: puerto/`.

- **Nombre de la máquina:**

Es posible cambiar el *hostname* o nombre de la máquina, por ejemplo. El nombre de la máquina sirve para identificarla de otras dentro de la red.

3.3. REDES EN ZENTYAL.

Zentyal puede utilizarse de dos maneras fundamentales:

- Puerta de enlace y cortafuegos de la conexión a internet,
- Servidor de los servicios en la red (o local o Internet).
- Ambas funcionalidades pueden combinarse en una misma máquina o separarse en varias, dependiendo de las características de cada despliegue.

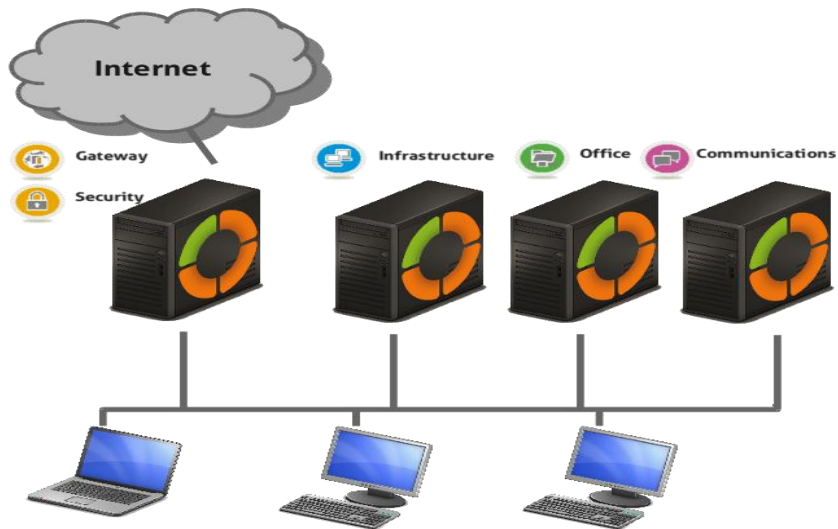


Figura 3.3.1. Funcionalidades Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.3.1. CONFIGURACION Y ADMINISTRACION DE LA RED.

A lo largo de esta documentación se verá cómo configurar Zentyal para desempeñar un papel de puerta de enlace y cortafuegos. Y por supuesto también se puede verificar la configuración en los casos que actúe como un servidor más dentro de la red.

Configuración modo estático.

Network Interfaces [\(show help\)](#)

eth0 br1

Name:

Method:

IP address:

Netmask:

Virtual Interfaces

Name	IP address	Netmask	Action
<input type="text"/>	<input type="text"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="+"/>

Figura 3.3.2. Configuración de red Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Configuración de las puertas de enlace

Puertas de enlace y Proxy ([mostrar ayuda](#))

Lista de Puertas de Enlace

[+ Añade nuevo](#)

Enabled	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Action
<input checked="" type="checkbox"/>	ADSL2	192.168.2.1	eth3	1	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	ADSL1	192.168.1.1	eth2	3	<input checked="" type="checkbox"/>	

10 ▼ Página 1

Proxy

Servidor proxy: Opcional

Puerto del proxy: Opcional

Figura 3.3.3. Configuración de puerta de enlace en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Configuración de los servidores DNS

Para que el sistema sea capaz de resolver nombres de dominio se tiene que especificar indicar la dirección de uno o varios servidores de nombres en *Red* > *DNS*.

Traductor de Servidores de Nombres de Dominio ([mostrar ayuda](#))

Lista de traductores de servidores de nombres de dominio

[+ Añade nuevo](#)

Servidor de nombres de dominio	Action
127.0.0.1	

10 ▼ Página 1

Dominio de búsqueda

Domnio: Opcional

Figura 3.3.4. Configuración servidores de DNS en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Si la conexión a Internet asigna una dirección IP dinámica y se desea que un nombre de dominio apunte a ella, se necesita un proveedor de DNS dinámico. Utilizando

Zentyal se puede configurar alguno de los proveedores de DNS dinámico más populares.

Para ello se procede a ingresar en *Red DynDNS* y se verifica el proveedor, del Servicio, Nombre de usuario, Contraseña y Nombre de máquina que se desea actualizar cuando la dirección pública cambie, sólo resta Habilitar DNS dinámico.



Dynamic DNS [\(mostrar ayuda\)](#)

Configuración

Habilitar DNS dinámico:

Servicio: DynDNS ▼

Nombre de usuario: zentyal

Contraseña: ●●●●●●

Nombre de máquina: servidor.dyndns.org

Cambiar

Figura 3.3.5. DNS dinámico en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Diagnóstico de red.

Para ver si se ha configurado bien nuestra red se puede utilizar las herramientas de Red Diagnóstico.

Ping: es una herramienta que utiliza el protocolo de diagnóstico de redes ICMP (Internet Control Message Protocol) para comprobar la conectividad hasta una máquina remota mediante una sencilla conversación entre ambas.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
PING zentyal.org (92.243.17.196) 56(84) bytes of data:
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_seq=1 ttl=55 time=78.5 ms
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_seq=2 ttl=55 time=77.5 ms
64 bytes from slurm.zentyal.com (92.243.17.196): icmp_seq=3 ttl=55 time=79.1 ms

--- zentyal.org ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 77.583/78.440/79.178/0.732 ms
```

Figura 3.3.6. Herramienta de diagnóstico ping en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Traceroute: También se dispone de la herramienta traceroute que se encarga de mostrar la ruta que toman los paquetes hasta llegar a la máquina remota determinada.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
traceroute to zentyal.org (92.243.17.196), 30 hops max, 60 byte packets
 1 192.168.1.1 0.872 ms 1.418 ms 1.733 ms
 2 87.222.134.1 32.586 ms 33.923 ms 35.107 ms
 3 10.255.16.254 34.836 ms 36.088 ms 37.327 ms
 4 212.106.217.19 44.930 ms 212.106.216.147 45.123 ms 212.106.217.3 46.211 ms
 5 212.106.216.145 45.853 ms 46.911 ms 47.792 ms
 6 212.106.216.69 82.198 ms * *
 7 212.106.216.69 82.944 ms 69.929 ms 69.502 ms
 8 217.70.176.113 78.110 ms 79.288 ms 79.288 ms
 9 217.70.176.113 79.294 ms 78.288 ms 79.299 ms
10 92.243.17.196 78.758 ms 79.218 ms 79.413 ms
```

Figura 3.3.7. Herramienta de diagnóstico tracerroute en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Resolución de nombres de dominio: Y por último también se cuenta con la herramienta de resolución de nombres de dominio que se utiliza para comprobar el correcto funcionamiento del servicio.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
;<<>> DiG 9.7.0-Pl <<>> +time=3 zentyal.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61100
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 3, ADDITIONAL: 1

;; QUESTION SECTION:
;zentyal.org.                IN      A

;; ANSWER SECTION:
zentyal.org.                727     IN      A      92.243.17.196

;; AUTHORITY SECTION:
zentyal.org.                7211    IN      NS     a.ns.joker.com.
zentyal.org.                7211    IN      NS     b.ns.joker.com.
zentyal.org.                7211    IN      NS     c.ns.joker.com.

;; ADDITIONAL SECTION:
a.ns.joker.com.            1241    IN      A      207.44.185.100

;; Query time: 1 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Sep 15 18:50:20 2010
;; MSG SIZE rcvd: 121
```

Figura 3.3.8. Herramienta de diagnóstico resolución de dominio en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.4. LA ACTUALIZACIÓN DE SOFTWARE EN ZENTYAL.

Como todo sistema de software, Zentyal Server requiere actualizaciones periódicas, bien sea para añadir nuevas características o para reparar defectos o fallos del sistema.

Zentyal distribuye su software mediante paquetes y usa la herramienta estándar de Ubuntu.

Para facilitar la tarea ofrece una interfaz web que simplifica el proceso.

Mediante la interfaz web se puede ver para qué componentes de Zentyal está disponible una nueva versión e instalarlos de una forma sencilla. También se puede actualizar el software en el que se apoya Zentyal, principalmente para corregir posibles fallos de seguridad.

Gestión de componentes de Zentyal

Al entrar en esta sección se puede verificar la vista avanzada del gestor de paquetes, que quizás ya se conoce del proceso de instalación. Esta vista se compone de tres pestañas, cada una de ellas destinadas, respectivamente, a las acciones de Instalar, Actualizar y Borrar componentes de Zentyal.

Desde esta vista se dispone de un enlace para cambiar al *modo básico*, desde el cual se instalara colecciones de paquetes dependiendo de la tarea a realizar por el servidor que se configure.

Volviendo a la vista avanzada, se puede ver detalladamente cada una de las acciones que se puede realizar.

[Ver modo básico](#)

Install Actualizar(0) Borrar

Search :

Component	Latest version	Select
Antivirus	2.1.2	<input type="checkbox"/>
DHCP Service	2.1.5	<input type="checkbox"/>
DNS Service	2.1.4	<input type="checkbox"/>
FTP	2.1.1	<input type="checkbox"/>
File Sharing Service	2.1.5	<input type="checkbox"/>
Filtro de correo	2.1.4	<input type="checkbox"/>
Groupware (Zarafa)	2.1.4	<input type="checkbox"/>
IPsec	2.1.3	<input type="checkbox"/>
Jabber (Instant Messaging)	2.1.2	<input type="checkbox"/>
Mail Service	2.1.8	<input type="checkbox"/>
Monitor de Ancho de Banda	2.1.4	<input type="checkbox"/>
NTP Service	2.1.4	<input type="checkbox"/>
PPTP	2.1.1	<input type="checkbox"/>
Portal Cautivo	2.1.8	<input type="checkbox"/>
Printer Sharing Service	2.1.4	<input type="checkbox"/>
RADIUS	2.1.1	<input type="checkbox"/>
Rincón del Usuario	2.1.4	<input type="checkbox"/>
Servidor Web	2.1.2	<input type="checkbox"/>
Sistema de Detección de Intrusiones	2.1.1	<input type="checkbox"/>
Virtualization Manager	2.1.3	<input type="checkbox"/>
Voz IP	2.1.4	<input type="checkbox"/>
Web Mail Service	2.1.2	<input type="checkbox"/>

Instalar Actualizar listado Seleccionar todo Deseleccionar todo

Figura 3.4.1. Componentes en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Instalación de componentes.

Esta es la pestaña visible al entrar en gestión de componentes. En ella se tiene tres columnas, una para el nombre del componente, otra para la versión actualmente disponible en los repositorios y otra para seleccionar el componente. En la parte

inferior de la tabla se puede ver los botones de Instalar, Actualizar lista, Seleccionar todo y Deseleccionar todo.

Para instalar los componentes que desee tan solo tiene que seleccionarlos y pulsar el botón Instalar. Tras hacer esto nos aparecerá una pantalla en la que se puede ver la lista completa de paquetes que se van a instalar, así como algunas recomendaciones que, aun no siendo dependencias necesarias, pueden aumentar las opciones de los componentes instalados o mejorarlos.

Actualización de componentes.

La siguiente pestaña, Actualizar, nos indica entre paréntesis el número de actualizaciones disponibles. Aparte de esta característica, si se visualiza esta sección, se puede ver que se distribuye de una forma muy similar a la vista de instalación, con tan solo algunas pequeñas diferencias. Una columna adicional nos indica la versión actualmente instalada y en la parte inferior de la tabla se puede ver un botón que se tiene que pulsar una vez seleccionados los paquetes a actualizar. Al igual que con la instalación de componentes, nos aparece una pantalla de confirmación desde la que puede ver los paquetes que van a instalarse.

Desinstalación de componentes.

La última pestaña, Borrar, nos mostrará una tabla con los paquetes instalados y sus versiones. De modo similar a las vistas anteriores, en ésta puede seleccionar los paquetes a desinstalar y una vez hecho esto, pulsar el botón Borrar situado en la parte inferior de la tabla para finalizar la acción.

Antes de realizar la acción, y como en los casos anteriores, Zentyal solicitará confirmación para eliminar los paquetes solicitados y los que de ellos dependen.




Actualización del sistema.


Las actualizaciones del sistema actualizan programas usados por Zentyal. Para llevar a cabo su función, el servidor Zentyal necesita diferentes programas del sistema. Dichos programas son referenciados como dependencias asegurando que al instalar Zentyal, o cualquiera de los módulos que los necesiten, son instalados también asegurando el correcto funcionamiento del servidor. De manera análoga, estos programas pueden tener dependencias también.


Normalmente una actualización de una dependencia no es suficientemente importante como para crear un nuevo paquete de Zentyal con nuevas dependencias, pero sí que puede ser interesante instalarla para aprovechar sus mejoras o sus soluciones frente a fallos de seguridad.

Para ver las actualizaciones del sistema puede ir a Gestión de Software, actualizaciones del sistema. Ahí se dispone de una lista de los paquetes que puede actualizar si el sistema no está actualizado. Si se instalan paquetes en la máquina por otros medios que no sea la interfaz web, los datos de ésta pueden quedar desactualizados, por lo que cada noche se ejecuta el proceso de búsqueda de actualizaciones a instalar en el sistema. Si se quiere forzar dicha búsqueda se puede hacer pulsando el botón Actualizar lista situado en la parte inferior de la pantalla.

Hay actualizaciones de la comunidad disponibles para los siguientes componentes del sistema:

Componente	Descripción	Versión	Actualizar
apt-transport-https	APT https transport	0.7.25.3ubuntu9.6	<input type="checkbox"/>
 libdbus-1-3	simple interprocess messaging system	1.2.16-2ubuntu4.3	<input type="checkbox"/>
 logrotate	Log rotation utility	3.7.8-4ubuntu2.2	<input type="checkbox"/>
python-apt	Python interface to libapt-pkg	0.7.94.2ubuntu6.4	<input type="checkbox"/>
apt-utils	APT utility programs	0.7.25.3ubuntu9.6	<input type="checkbox"/>
apt	Advanced front-end for dpkg	0.7.25.3ubuntu9.6	<input type="checkbox"/>
linux-image-2.6.32-33-generic	Linux kernel image for version 2.6.32 on x86/x86_64	2.6.32-33.71	<input type="checkbox"/>
 libpng12-0	PNG library - runtime	1.2.42-1ubuntu2.2	<input type="checkbox"/>
Actualizar todos los paquetes			<input type="checkbox"/>

 Esta operación puede tomar un tiempo, no se preocupe si Zentyal no responde después de presionar el botón de Actualizar.

 Actualizar


 Actualizar listado

Figura 3.4.2. Actualizaciones en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Actualizaciones del sistema.

Para cada una de las actualizaciones puede determinar si es de seguridad o no con el icono indicativo de más información. Si es una actualización de seguridad puede ver el fallo de seguridad con el registro de cambios del paquete, pulsando sobre el icono.

Si desea actualizar tiene que seleccionar aquellos paquetes sobre los que realizar la acción y pulsar el botón correspondiente. Como atajo también tiene un botón de *Actualizar todos los paquetes*. Durante la actualización se irán mostrando mensajes sobre el progreso de la operación.

Actualizaciones automáticas.

Las actualizaciones automáticas permiten al servidor Zentyal instalar automáticamente cualquier actualización disponible.

Podría activar esta característica accediendo a la página Gestión de Software, Configuración.



Figura 3.4.4. Configuración actualizaciones en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.5. ZENTYAL GATEWAY.

Las funcionalidades de Zentyal como puerta de enlace o gateway. Zentyal puede hacer la red más fiable y segura, gestionar el ancho de banda y definir políticas de conexiones y contenidos.

Hay un apartado centrado en el funcionamiento del módulo de cortafuegos, el cual nos permite definir reglas para gestionar el tráfico entrante y saliente tanto del servidor como de la red interna. Para ayudar en la configuración del cortafuego, existen dos módulos que facilitan la gestión de objetos y servicios de red.

A la hora de acceder a Internet podría balancear la carga entre varias conexiones y definir diferentes reglas para usar una u otra según el tráfico.

3.5.1. OBJETOS DE RED.

Los Objetos de red son una manera de representar un elemento de la red o a un conjunto de ellos. Sirven para simplificar y consecuentemente facilitar la gestión de la configuración de la red, pudiendo dotar de un nombre fácilmente reconocible al elemento o al conjunto y aplicar la misma configuración a todos ellos.

Por ejemplo, podría dar un nombre reconocible a una dirección IP o a un grupo de ellas. En lugar de definir la misma regla en el cortafuego para cada una de las direcciones IP, simplemente bastaría con definirla para el objeto de red que contiene las direcciones.

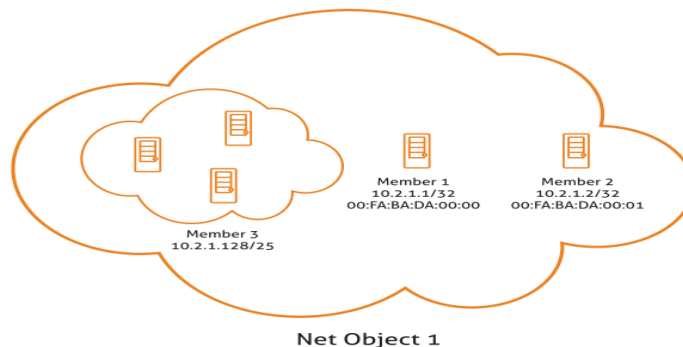


Figura 3.5.1. Objetos de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.5.2. GESTIÓN DE LOS OBJETOS DE RED CON ZENTYAL.

Para empezar a trabajar con los objetos en Zentyal, se puede acceder la sección Red, Objetos, allí puede ver una lista inicialmente vacía, con el nombre de cada uno de los objetos y una serie de acciones a realizar sobre ellos. Se pueden crear, editar y borrar objetos que serán usados más tarde por otros módulos.

Objetos [\(mostrar ayuda\)](#)

Lista de objetos

[+ Añadir nuevo](#)

Nombre	Miembros	Action
DMZ		
Guest		
IT		
Ventas		

10 ▼ Página 1

Figura 3.5.2. Objetos de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Cada uno de estos objetos se compondrá de una serie de miembros que puede modificar en cualquier momento. Los miembros tendrán al menos los siguientes valores: Nombre, Dirección IP y Máscara de red. La Dirección MAC es opcional y lógicamente sólo se podrá utilizar para miembros que representen una única máquina y se aplicará en aquellos contextos que la dirección MAC sea accesible.

Objetos > marketing [\(mostrar ayuda\)](#)

Editando miembro

Nombre:

Dirección IP: /

Dirección MAC: Opcional

Figura 3.5.3. Configuración de objetos de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Añadir un nuevo miembro

Los miembros de un objeto pueden solaparse con miembros de otros, con lo cual hay que tener cuidado al usarlos en el resto de módulos para obtener la configuración deseada y no tener problemas.

3.5.3. SERVICIOS DE RED.

Los Servicios de red son la manera de representar los protocolos (TCP, UDP, ICMP, etc) y puertos usados por una aplicación. La utilidad de los servicios es similar a la de los objetos: si con los objetos se puede hacer referencia a un conjunto de direcciones IP usando un nombre significativo, así mismo identificar un conjunto de puertos por el nombre de la aplicación que los usa.



Figura 3.5.4. Servicios de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Gestión de los servicios de red con Zentyal.

Para trabajar con los servicios en Zentyal se debe ir al menú red, servicios donde se listan los servicios existentes creados por cada uno de los módulos que se hayan instalado y los que se haya podido definir adicionalmente.

Para cada servicio se puede ver su nombre, descripción y un indicador de si es Interno o no. Un servicio es interno si los puertos configurados para dicho servicio se están usando en el mismo servidor.

Además cada servicio tendrá una serie de miembros, cada uno de estos miembros tendrá los valores: Protocolo, Puerto origen y Puerto destino. En todos estos campos se puede introducir el valor cualquiera, por ejemplo para especificar servicios en los que sea indiferente el puerto origen o un rango de puertos.

El protocolo puede ser TCP, UDP, ESP, GRE o ICMP. También existe un valor TCP/UDP para evitar tener que añadir dos veces un mismo puerto que se use en ambos protocolos, como en el caso de DNS.

Servicios [\(mostrar ayuda\)](#)

Lista de servicios

[+ Añade nuevo](#)

Nombre del servicio	Descripción	Interno	Configuración	Action
FTP	Zentyal FTP Server	<input checked="" type="checkbox"/>		
RADIUS	Zentyal RADIUS system	<input checked="" type="checkbox"/>		
any	any protocol and port	<input type="checkbox"/>		
any TCP	any TCP port	<input type="checkbox"/>		
any UDP	any UDP port	<input type="checkbox"/>		
dhcp	--	<input checked="" type="checkbox"/>		
dns	Domain Name Service	<input type="checkbox"/>		
eBox administration	Zentyal Administration Web Server	<input checked="" type="checkbox"/>		
http	--	<input checked="" type="checkbox"/>		
ldap	--	<input checked="" type="checkbox"/>		

10 ▼ Página 1 de 2

Figura 3.5.5. Servicios de red en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.6. MANTENIMIENTO DE ZENTYAL.

En Zentyal no sólo se configuran los servicios de red de manera integrada, sino que además se ofrecen una serie de características que facilitan la administración y el mantenimiento del servidor.

En este apartado se explicarán aspectos como los registros de los servicios para conocer qué ha sucedido y en qué momento, notificaciones ante incidencias o determinados eventos, monitorización de la máquina o herramientas de soporte remoto.

Además de estas herramientas de mantenimiento integradas en el servidor Zentyal, Zentyal Cloud ofrece un conjunto de servicios de suscripción que nos ayudan a automatizar las tareas de mantenimiento y gestión de nuestro servidor. Estos servicios están disponibles a través de la interfaz web de Zentyal Cloud e incluyen:

Actualizaciones de software de calidad.

Todas las actualizaciones y correcciones de errores que se suministran a través del Repositorio de Calidad Asegurada han sido extensivamente comprobadas para asegurar que no introducirán errores ni regresiones en los sistemas en producción.

- **Alertas.**

Alertas sobre el rendimiento del hardware, la disponibilidad de las redes, la actividad del proxy HTTP, la actividad del módulo de IDS, eventos en el correo electrónico y copias de seguridad.

- **Informes.**

Informes que detallan el rendimiento hardware, el uso de Internet, eventos en el antivirus, uso de las VPN, eventos IDS, uso del correo electrónico, actividad en las carpetas compartidas, impresoras y copias de seguridad.

- **Monitorización y gestión remotas.**

Monitorización del rendimiento hardware, actividad de la red, uso de la conexión a Internet y estado de los servicios.

Gestión a través del acceso remoto a los servidores, gestión de software y tareas por grupos de servidores.

- **Actualizaciones de seguridad avanzadas.**

Actualizaciones comerciales a los sistemas de Antispam, Antivirus, IDS, filtrado de contenidos y filtrado de anuncios que son aplicadas automáticamente.

- **Recuperación de desastres.**

Copia de seguridad remota de configuración y datos de usuario, con un proceso de recuperación sencillo y automatizado en caso de desastre.

3.7. EVENTOS Y ALERTAS.

La configuración de eventos y alertas en Zentyal.

El módulo de eventos es un servicio muy útil que permite recibir notificaciones de ciertos eventos y alertas que suceden en un servidor Zentyal.

En Zentyal dispone de los siguientes mecanismos emisores para la notificación de incidencias:

- Correo
- Jabber
- Registro
- RSS

Antes de activar los eventos se tiene que asegurar de que el módulo se encuentra habilitado. Para habilitarlo, como de costumbre, se debe ir al estado del módulo y seleccionar la casilla eventos.

Eventos [\(mostrar ayuda\)](#)

[Configurar eventos](#) [Configurar emisores](#)

Enabled	Nombre	Descripción	Configuración	Action
<input type="checkbox"/>	RAID	Comprueba si algún evento ha ocurrido en el subsistema RAID	Ninguna	
<input type="checkbox"/>	Log observer	Notify when a logger (VPN, POP3 proxy, Proxy HTTP, Samba quarantine, Samba access, Samba virus, Firewall, IDS, SMTP filter, VoIP, Correo, Printers) has logged something		
<input type="checkbox"/>	Estado	Comprueba si Zentyal está actualmente en activo o inactivo	Ninguna	
<input type="checkbox"/>	Espacio de almacenamiento libre	Comprobar si alguna partición no tiene espacio libre de almacenamiento		
<input type="checkbox"/>	Copia de seguridad	Comprobar si la copia de seguridad de Zentyal no se realizó correctamente.	Ninguna	
<input type="checkbox"/>	Monitorización	Notificar cuando un valor en concreto ha llegado un cierto umbral		
<input type="checkbox"/>	WAN failover	Verifique si las puertas de enlace están conectadas o desconectadas.	Ninguna	
<input type="checkbox"/>	Servicio	Comprueba si algún servicio de Zentyal no está ejecutándose cuando debería estar haciéndolo	Ninguna	

10

Figura 3.7.1. Eventos en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Pantalla de configuración de eventos.

Además, algunos eventos como el observador de registros o el observador de espacio restante en disco tienen sus propios parámetros de configuración.

La configuración para el observador de espacio en disco libre es sencilla. Sólo se debe especificar el porcentaje mínimo de espacio libre con el que desea ser notificados (cuando sea menor de ese valor).

Eventos [\(mostrar ayuda\)](#)

Configurar eventos Configurar emisores

Habilitado	Nombre	Receptor	Configuración	Action
<input type="checkbox"/>	Correo	Cuenta de correo para Admin		
<input type="checkbox"/>	Jabber	Cuenta de administrador Jabber		
<input type="checkbox"/>	RSS	Fichero RSS: Alerts		
<input type="checkbox"/>	Zentyal Cloud	Control panel		
<input checked="" type="checkbox"/>	Registro	Fichero de registro	Ninguna	

10 Página 1

Figura 3.7.2. Eventos en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

3.8. MONITORIZACIÓN.

La monitorización en Zentyal.

El módulo de monitorización permite al administrador conocer el estado del uso de los recursos del servidor Zentyal. Esta información es esencial tanto para diagnosticar problemas como para planificar los recursos necesarios con el objetivo de evitar problemas.

La monitorización se realiza mediante gráficas que permiten hacerse fácilmente una idea de la evolución del uso de recursos. Se puede acceder a las gráficas desde monitorización. Colocando el cursor encima de algún punto de la línea de la gráfica en la que se esté interesado se puede saber el valor exacto para un momento determinado.

Al elegir la escala temporal de las gráficas entre una hora, un día, un mes o un año. Para ello simplemente puede pulsar sobre la pestaña correspondiente.

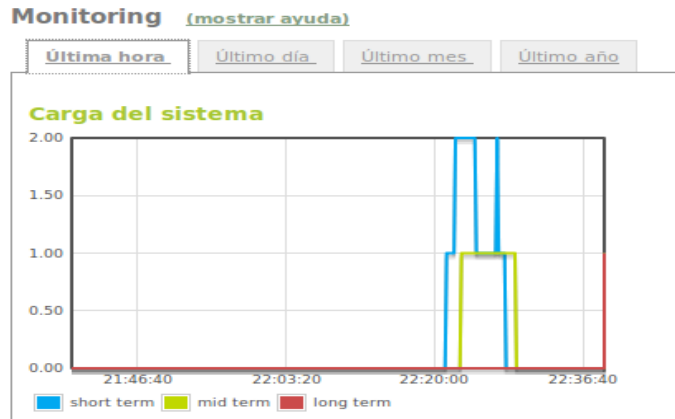


Figura 3.8.1. Monitoreo del sistema en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Carga del sistema.

La carga del sistema trata de medir la relación entre la demanda de trabajo y el realizado por el computador. Esta métrica se calcula usando el número de tareas ejecutables en la cola de ejecución y es ofrecida por muchos sistemas operativos en forma de media de uno, cinco y quince minutos.

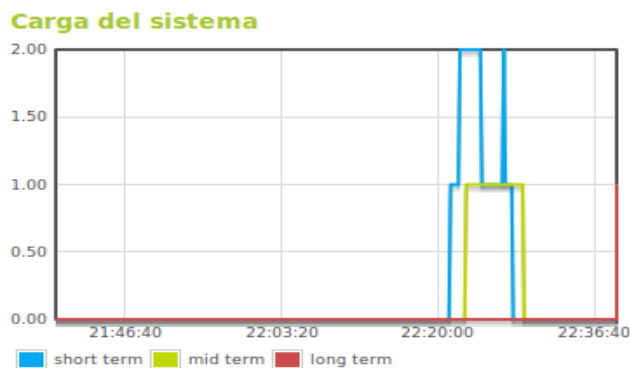


Figura 3.8.2. Monitoreo del sistema en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Uso de la CPU.

Con esta gráfica se tiene una información detallada del uso de la CPU. En caso de que se disponga de una maquina con múltiples CPUs con una gráfica para cada una de ellas.

En la gráfica se representa la cantidad de tiempo que pasa la CPU en alguno de sus estados, ejecutando código de usuario, código del sistema, esta inactivo, en espera de una operación de entrada/salida, entre otros valores.

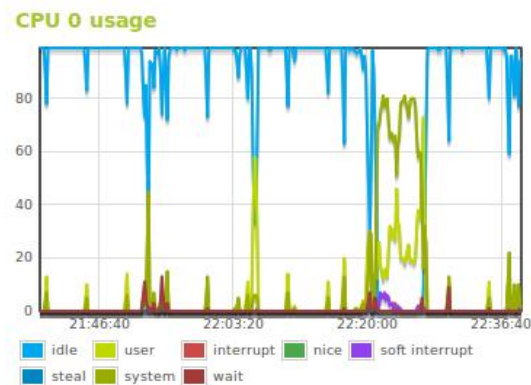


Figura 3.8.3. Monitoreo del CPU en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Uso de la memoria.

La gráfica nos muestra el uso de la memoria. Se monitorizan cuatro variables:

- **Memoria libre:**
Cantidad de memoria no usada
- **Caché de página:**
Cantidad destinada a la caché del sistema de ficheros
- **Buffer caché:**
Cantidad destinada a la caché de los procesos
- **Memoria usada:**
Memoria usada que no está destinada a ninguno de las dos anteriores cachés.

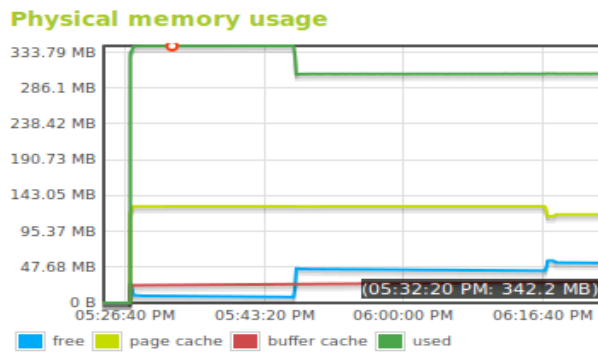


Figura 3.8.4. Monitoreo de memoria en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Uso del sistema de ficheros.

Esta gráfica nos muestra el espacio usado y libre del sistema de ficheros en cada punto de montaje.

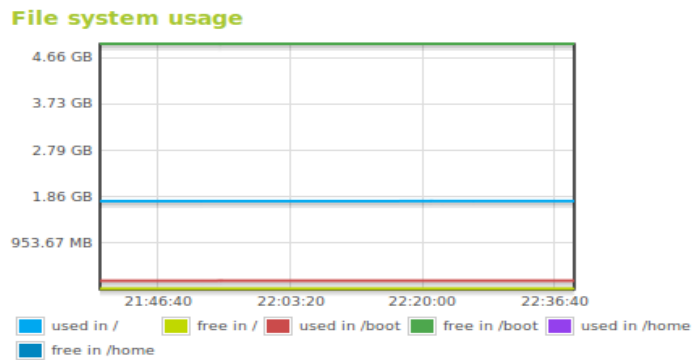


Figura 3.8.5. Monitoreo del sistema de archivos en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Alertas.

La monitorización carecería en gran medida de utilidad si no estuviera acompañada de un sistema de notificaciones que nos avisara cuando se producen valores anómalos, permitiéndonos saber al momento que la máquina está sufriendo una carga inusual o está llegando a su máxima capacidad.

Configurar observadores de monitorización

Medida	Umbral	Action
Physical memory usage		
File system usage		
CPU usage		
Carga del sistema		

10 ▼ Página 1

Figura 3.8.6. Configuración monitoreo en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Pantalla de configuración de los observadores de la monitorización.

Pulsando en la celda de configuración, se accede a la configuración de este evento. Se puede elegir cualquiera de las métricas monitorizadas y establecer umbrales que disparen el evento.

Añadiendo una nueva Umbral

Habilitado:

Mínimo para fallo:
Opcional
Establece un límite inferior para valores aceptables. Si no se especifica se toma -infinito por defecto.

Mínimo para aviso:
Opcional
Si el valor es menor que este valor y mayor que mínimo para fallo se enviará un evento de aviso

Máximo para aviso:
Opcional
Si el valor es mayor que este valor y menor que máximo para fallo se enviará un evento de aviso

Máximo para fallo:
Opcional
Establece un límite superior para valores aceptables. Si no se especifica se toma +infinito por defecto.

Invertir:
Si se habilita, el rango de valores aceptables se invierte, esto es, valores entre mínimo para fallo y máximo para fallo (mínimo para aviso y máximo para aviso) no son correctos.

Persistente:
Si se activa, un evento será emitido para cada valor fuera del rango aceptable. Si no, sólo un cambio de un valor aceptable a uno inaceptable será notificado

Ejemplar de medida:

Tipo:

Fuente de datos:

Figura 3.8.7. Umbral de eventos en Zentyal.

Fuente: <http://www.zentyal.com/es/small-business-it/>

Pantalla de configuración de los umbrales de eventos

En cuanto a los umbrales se tiene de dos tipos, de advertencia y de fallo, pudiendo así discriminar entre la gravedad del evento. Se tiene la opción de invertir, lo que hará que los valores que estén dentro del umbral sean considerados fallos y lo contrario si están fuera. Otra opción importante es la de persistente.

Una vez configurado y activado el evento se debe configurar al menos un observador para recibir las alertas. La configuración de los observadores es igual que la de cualquier evento, así que se debe seguir las indicaciones de eventos y alertas.

CAPÍTULO 4.

4.1. IMPLEMENTACIÓN.

Para la implementación de los servidores como servicios anteriormente revisados se necesita revisar el tipo de sistema operativo anfitrión, distribución de la plataforma Linux y las herramientas de software libre a utilizar.

En la implementación se tiene que revisar requisitos de hardware como software para hacer la instalación de las respectivas actualizaciones como dependencias, librerías necesarias para su funcionamiento.

4.2. INTRODUCCIÓN.

Servidor de virtualización.

Para la implementación del servidor de virtualización se procede a seleccionar el sistema operativo Linux anfitrión a utilizar y la herramienta de software libre para la creación, virtualización de servidores virtuales para lo cual se requiere lo siguiente.

Sistema operativo Linux anfitrión Ubuntu 9.10

Herramienta de software libre para la virtualización VirtualBox.

Servidor de correo virtualizado Zimbra.

Para la implementación del servidor de correo virtualizado se va a seleccionar el sistema operativo Linux anfitrión a utilizar y la herramienta de software libre para la creación para la creación de la máquina virtual para lo cual se requiere lo siguiente.

Sistema operativo Linux Anfitrión Centos 5.2.

Herramienta de software libre para la virtualización VirtualBox.

Servidor multiplataforma Zentyal.

Para la implementación del servidor multiplataforma Zentyal se va a seleccionar el sistema la distribución más actual de Zentyal a utilizar para la instalación y configuración respectiva para lo cual se requiere lo siguiente.

4.2.1. CARACTERÍSTICAS DE LOS SERVIDORES A NIVEL DE HARDWARE.

Servidor Multitarea Zentyal.

HP ProLiant Server ML150 G3



Figura 4.2.1. HP ProLiant Server ML150 G3

Fuente: <http://www.hp.com>

Características:

- Dual-Core Intel Xeon 5060 Processor (3.2 GHz, 1066 FSB)
- Intel 5000V Chipset
- 2 Embedded
- HP NC7781 Gigabit Server Adapter 10/100/1000 WOL (Wake on LAN) GB
- SAS and SATA HDD options are available
- HP Embedded SATA RAID Controller or HP 8 Internal Port SAS Host Bus Adapter with RAID

Servidor de virtualizacion VirtualBox.

Servidor virtual de correo Zimbra Collaboration Suite.

HP ProLiant ML350 G6



Figura 4.2.2. HP ProLiant ML350 G6

Fuente: <http://www.hp.com>

Características:

- Quad-Core Intel Xeon 5504 Processor
- 4 GB en ram
- Smart Array P410i Controller (RAID 0, 1 y 1+0) HD LFF.
- 16X DVD

- Tarjeta de red Dual 10/100/1000

4.2.2. ESTRUCTURA ACTUAL DE RED INTERNA.

Como parte de la infraestructura de Movidatos se tiene los siguientes dispositivos de telecomunicaciones.

Router Cisco (Telconet).

En el cual se tiene la conexión mediante Ip publica a internet, el enlace de Movidatos tiene varias Ip públicas a disponibilidad para ser usadas como en este caso una Ip publicara para el servidor de correo, una Ip publica para el firewall que funcionara con el proxy para proporcionar y controlar el acceso a internet.

Switch 3com (10/100 Mbps) de 24 puertos capa 2 (Movidatos).

El switch se lo utiliza para tener conectividad entre los equipos conjuntamente con los servidores y así todos los usuarios puedan los servicios que proporcionan los servidores implementados actualmente.

Router Cisco D-Link (Movidatos).

Este router es utilizado para proporcionar conexión de red inalámbrica a usuarios que no puedan conectarse a la red de Movidatos mediante cable.

Cableado estructurado categoría 5e.

El cableado estructura que posee la empresa es específicamente para tener una mejor calidad de envió como recepción de información y aumentar el rendimiento de los equipos como los usuarios de la empresa

Estructura actual de red externa.

La empresa Movidatos tiene actualmente como proveedor de enlace de internet a la empresa de telecomunicaciones Telconet.

La conexión de datos es proporcionada median fibra óptica para lo cual se tiene los siguientes dispositivos de telecomunicaciones que interactúan para proporcionar el servicio.

Fibra óptica.

Transiber (Telconet.)

Router Cisco (Telconet).

En el cual se establece la conexión mediante Ip publica a internet, el enlace de Movidatos tiene varias Ip públicas a disponibilidad para ser usadas como en este caso una Ip publicara para el servidor de correo, una Ip publica para el firewall que funcionara con el proxy para proporcionar y controlar el acceso a internet.

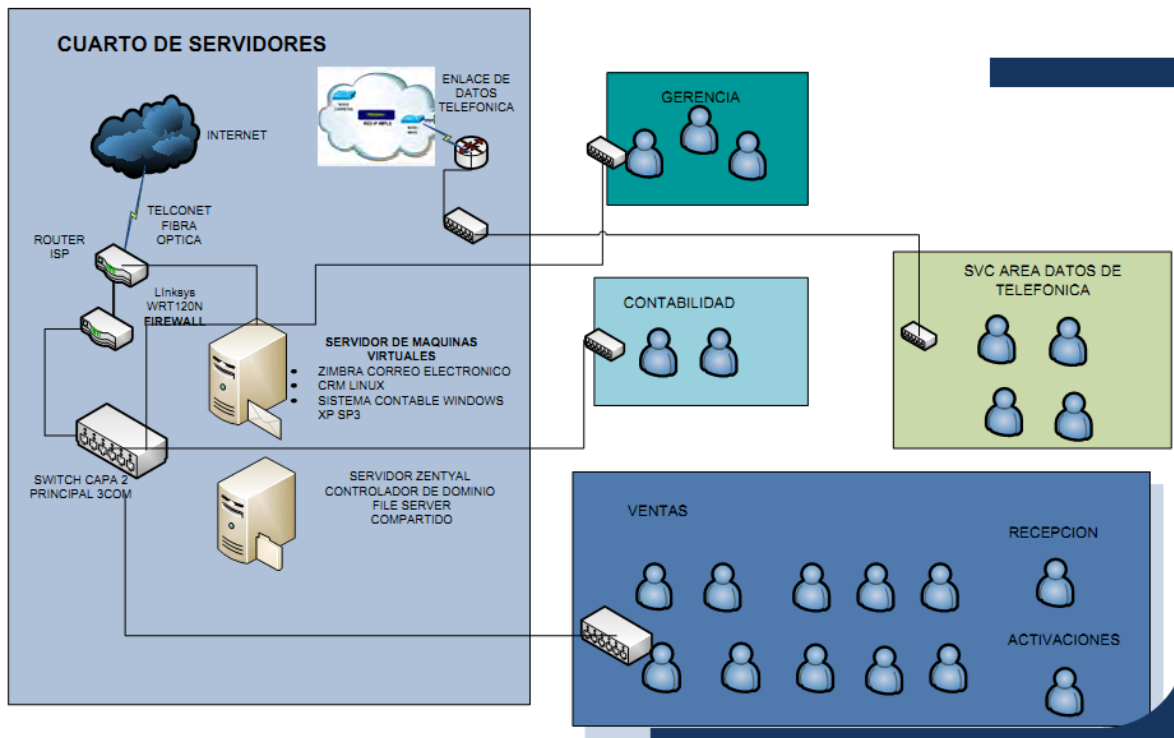


Figura 4.2.3. Estructura de red Empresa Movidatos.

Fuente: Autor tesis Henry Padilla.

4.3. INSTALACIÓN.

4.3.1. SERVIDOR DE VIRTUALIZACIÓN VIRTUALBOX.

Para la instalación del servidor de correo Zimbra se preparó el servidor hp ml 350 g6 de la siguiente manera:

- Instalación de dos módulos de memoria de 2 GB en el slot correspondiente.
- Instalación de la fuente de poder principal como la redundancia de respaldo.
- Instalación de 4 discos de 160 GB SCSI.
- Configuración de la controladora raid.
- Creación de raid 5 con 3 discos SCSI.
- Preparación de los discos para la instalación del sistema operativo.
- Cuando ya se tiene el hardware correctamente configurado se procede con la

instalación de sistema operativo base de la siguiente manera:

- Instalación de la plataforma principal en este caso sistema operativo Linux anfitrión Ubuntu 9.10.
- Luego se procede a crear las respectivas particiones del sistema operativo

Partición	Tamaño	Ubicación	Formato
Swap	4096 MB	Principio	área de intercambio
/boot	100MB - 350MB	Principio	ext2
/	8GB - 16GB	Principio	ext4
/home	Libre	Principio	ext4

Figura 4.3.1. Particiones Linux.

Fuente: Autor tesis Henry Padilla.

- Configuración zona horaria servidor, nombre servidor, servicios a instalar, red etc.
- Se continua con la instalación hasta terminar y el instalador lo indique.
- Terminamos la instalación de sistema operativo principal.
- Instalación del software que se utilizara para crear, configurar las máquinas virtuales en este caso VirtualBox.
- Configuración del software para la virtualización VirtualBox.
- Instalación de las actualizaciones como dependencias del sistema operativo principal.

4.3.2. SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE.

Para la instalación se preparó una máquina virtual utilizando el software para la virtualización VirtualBox versión libre para lo cual se procedió de la siguiente manera.

- Creación de una maquina virtual de nombre SRVMAILS.
- Preparación de la máquina virtual creación de disco de 500 Gb de almacenamiento dinámico.
- Asignamiento de 2 GB en ram para el funcionamiento del servidor.
- Habilitación y configuración de dos tarjetas de red a nivel interno interna (Eth1) y externo externo (Eth0).
- Configuración de unidad de cd para la detección de la imagen .iso que servirá para la instalación del sistema operativo principal.
- En esta máquina virtual se instaló sistema operativo Linux Centos 5.5.
- Instalación de todas las actualizaciones como dependencias necesarias para el funcionamiento de Zimbra.
- Una vez que se ha comprobado que se cumple con todos los requisitos se procede con la instalación del servidor de correo Zimbra.

4.4. IMPLEMENTACIÓN.

4.4.1. SERVIDOR DE CORREO ZIMBRA COLLABORATION SUITE.

Requerimientos.

Los requerimientos de Zimbra Collaboration Suite son, en comparación con otros productos similares, bastante bajos. Para el entorno que se va a implementar la siguiente configuración debería ser la siguiente:

Para un sistema en test se recomienda la siguiente configuración:

- CPU Intel/AMD de 32bits a 1.5 GHz o superior.
- 1 GB de RAM.
- 20 GB de espacio libre en disco minimo para el software y los logs.

- Espacio adicional para el almacenamiento del correo y las bases de datos (depende del número de cuentas y de la cuota de disco asignada a cada una).

Para un sistema en producción se recomienda la siguiente configuración:

- CPU Intel/AMD de 32 bits a 2.0GHZ o superior.
- 2 GB de RAM.
- 50 GB de disco duro para actualizaciones, logs y software, con RAID para redundancia de datos.

- Espacio de disco adicional para el almacenamiento de los buzones de correo y las bases de datos.

- Se recomiendan CPU (Central Processing Unit) de doble núcleo o superior, y preferiblemente doble CPU, pues se hará buen uso de éstos por parte de la máquina virtual de Java y por parte de Amavis, SpamAssassin y ClamAV.

Para instalaciones de más de 2000 cuentas de usuario, se recomienda CPU de 64 bits, lo que lleva a la necesidad de duplicar la RAM (mínimo 4 GB). El uso de discos SCSI es siempre recomendado frente a SATA por su fiabilidad y rendimiento. En general, y Zimbra no es una excepción, a mayor cantidad de RAM, mayor rendimiento general debido a la caché del kernel, y mayor fiabilidad.

Finalmente, el uso de una SAN o NAS, si es pertinente y económicamente posible, es siempre bienvenido dado el uso masivo que se hace del correo hoy en día y de la criticidad de este servicio en las empresas.

Por supuesto, todos estos valores son orientativos y únicamente útiles en un caso estándar. Es muy posible que sea preciso aumentarlos en función de los picos de carga que se prevean (por ejemplo si un cierto número, muy elevado, de usuarios acceden a la misma hora a comprobar el correo).

Seguridad.

Respecto de la seguridad, en la documentación de Zimbra se aconseja desactivar SELinux (del inglés, Security Enhanced Linux) y el cortafuego. Desactivar SELinux no tiene por qué suponer un problema, pero trabajar sin un cortafuego en una máquina con dirección IP pública no es algo que uno pueda o quiera permitirse. La documentación de Zimbra presupone que el servidor se encuentra tras un router que hace NAT de los puertos, pero éste no tiene porqué ser siempre el caso y, aun así, la seguridad no debe enfocarse únicamente hacia el exterior. Debido a que este tema es susceptible de largas discusiones, además de dependiente de cada caso y organización particular, por no hablar de cómo configurar en sí un cortafuego, a continuación se facilita una lista de puertos que deberán dejarse abiertos para el correcto funcionamiento de Zimbra y se deja a discreción del usuario su uso y su aplicación.

- SMTP, puerto 25 TCP.
- HTTP, puerto 80 TCP.
- HTTPS, puerto 443 TCP.
- POP3, puerto 110 TCP.
- POP3 sobre SSL (POP3S), puerto 995 TCP.
- IMAP4, puerto 143 TCP.
- IMAP4 sobre SSL (IMAPS), puerto 993 TCP.
- LDAP, puerto 389 TCP.
- LDAP sobre SSL (LDAPS), puerto 636 TCP.
- Administración de Zimbra, puerto 7071 TCP.

El acceso a los puertos 389 y 686 permite consultas al GAL de Zimbra, pero no debería abrirse al exterior (quizás filtrarlo sólo a la red local o a la IP pública del gateway/router de la oficina) pues OpenLDAP permite consultas anónimas por defecto.

Zimbra 5.0.7 es la primera versión que incluye la posibilidad de permitir sólo consultas autenticadas a LDAP sobre la IP pública, a través de SSL, y que las consultas internas se realicen por la interfaz local.

El acceso al puerto 7071 quizás quiera restringirse también a ciertas direcciones IP.

4.4.2. CONFIGURACIÓN DEL DNS.

El siguiente paso es configurar el DNS de movidatos.com para crear los registros A y MX.

- Registro de intercambio de mail MX (Mail Exchange).
- Registro de acceso A (Access Control).

Se crea un registro A con mailserver.movidatos.com que apunte a la IP pública 190.95.222.195 y luego dos entradas MX. Una entrada MX con peso 10 que apunte a mailserver.movidatos.com y otra con peso 20 que apunte al relay del backup.

La forma de configurar esto depende de con quien se tiene contratado la compra de nuestro dominio.

Si se lo tiene contratado con una tercera empresa, se pasa la información que se debe configurar en sus servidores DNS.

Toda modificación en un DNS implicará esperar 24 o 48 horas hasta que todos los DNS se actualicen.

Si se hace un nslookup al dominio, mostrará la información que se ve en la figura.

```

> set type=mx
> movidatos.com
Servidor: UnKnown
Address: 192.168.1.1

Respuesta no autoritativa:
movidatos.com MX preference = 0, mail exchanger = emailserver.movidatos.com
movidatos.com MX preference = 0, mail exchanger = mailserver.movidatos.com

movidatos.com nameserver = dns1uio.cyberweb.net.ec
movidatos.com nameserver = dns2uio.cyberweb.net.ec
mailserver.movidatos.com internet address = 190.95.222.195
emailserver.movidatos.com internet address = 190.95.222.195
dns1uio.cyberweb.net.ec internet address = 200.24.208.2
dns2uio.cyberweb.net.ec internet address = 200.24.208.1
>

```

Figura 4.4.1. Nslookup.

Fuente: Autor tesis Henry Padilla.

Lo que se consigue poniendo los pesos de 10 y 20 es que por defecto todo el correo entrante se enviará a mail.ecuadorchallenger.com.ec y solo si no responde (se cae nuestra línea de datos, nuestro Server cae o un ratón ha mordido el Ethernet) el correo se reenviará al relay de backup (servidor del proveedor que almacenará los correos hasta que se reestablezca el servidor principal) contratado en smtp.movistar.com.ec.

Si el correo se cae y va a parar todo al relay, se tiene que recoger el correo depositado en este relay más tarde, una vez que el sistema de correo vuelva a funcionar.

Para proceder a instalar Zimbra en nuestro Servidor Proliant ML 350 G6 con disco duro 500 GB y ram 4GB la cual tendrá las siguientes particiones :

```

swap    : 4 GB
/       : 100 GB
/opt    : 300 GB
/boot   : 300 MB
/home   : 20 GB
/var    : 30 GB

```

/tmp : 10 GB

/usr : 5GB

Cabe resaltar que la partición de tipo /opt debe de tener la mayor cantidad de espacio posible, ya que en esta se guardaran los BACKUP

Como ya se tiene instalado nuestro Centos, se procede a descargar Zimbra de 32 bits en el directorio previamente creado denominado paquetes.

```
[root@free paquetes]# cd /root/paquetes/
```

```
[root@free paquetes]# http://h.yimg.com/lo/downloads/5.0.18_GA/zcs-5.0.18_GA_3011.RHEL5.20090707164432.tgz
```

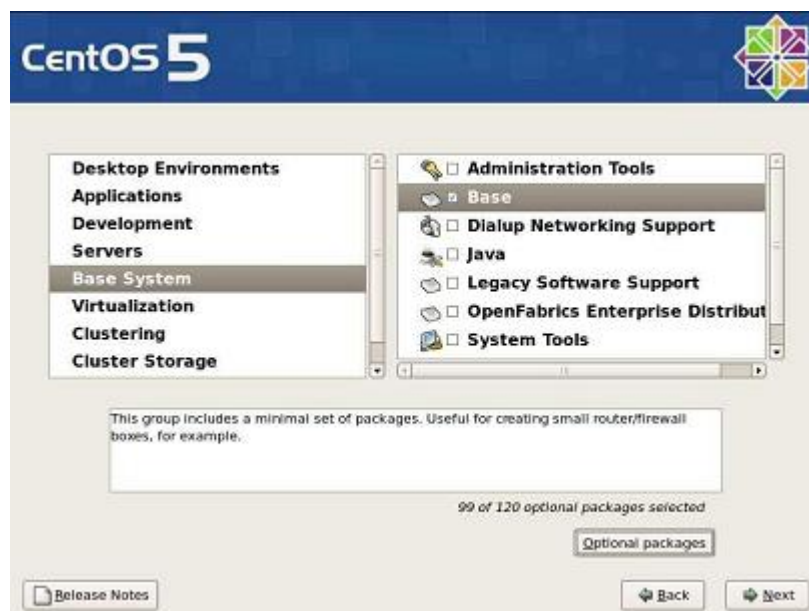


Figura 4.4.2. Instalación sistema operativo Centos Linux.

Fuente: Autor tesis Henry Padilla.

Una vez iniciado el sistema por primera vez, se utilizara el comando “ntsysv” para deshabilitar todos los servicios que no se necesite.

Por ejemplo: bluethooth, cups, firstboot, ip6tables, isdn, sendmail, iptables y yum-updatesd.

Deshabilitamos SELinux.

Para ello editamos `/etc/selinux/config` y cambiamos “SELINUX=permissive” por “SELINUX=disabled”.

Todas las sentencias deben ejecutarse como usuario root o mediante sudo, a menos que se indique lo contrario (comandos que se ejecutarán con el usuario Zimbra).

Acto seguido se procederá asegurar de que el fichero `/etc/hosts` esté configurado correctamente.

Debería tener, al menos, las dos entradas siguientes:

```
127.0.0.1 localhost.localdomain localhost
x.y.z.t mailserver.movidatos.com zimbra
```

A continuación se verificara de que los registros A y MX de la zona de DNS correspondiente al servidor estén bien configurados. Esto puede variar en función de si nos encontramos en una máquina con IP pública o en una máquina con IP privada (tras un router que haría NAT). Además, puede que se use un servidor de DNS local con vistas, o directamente uno externo. En cualquier caso, los objetivos son dos:

Estos aspectos de configuración de DNS son requerimientos de Zimbra para su instalación. Es conveniente, asimismo, tener bien configurado el registro PTR de la dirección IP donde se vaya a instalar Zimbra.

Como último paso antes de iniciar el instalador de ZCS, se instalara una serie de paquetes que son dependencias necesarias para el correcto funcionamiento (algunos son dependencias de los paquetes de Zimbra, otros son opcionales pero de facto necesarios si se desea que todas las funcionalidades de Zimbra estén activas).

También se incluyen paquetes de propósito general de instalación obligada en cualquier servidor:

```
yum install curl sudo libidn11 fetchmail libgmp3c2 libxml2 \  
libstdc++5 libstdc++6 openssl libltdl3 libssl0.9.7 libdb3 \  
libexpat1 libltdl3 libio-socket-ssl-perl libmail-imapclient-perl \  
libmail-pop3client-perl libpcre3 file psmisc libgetopt-mixed-perl \  
libmime-explode-perl sysstat rar lha arj unrar zoo nomarch cpio \  
lzop cabextract zip unzip bzip2 gzip lsof tcpdump sysstat procs \  
pstack strace
```

Se procede a descargar la última versión disponible de Zimbra. Para escribir este proyecto se ha utilizado la versión 5 de la Open Source Edition.

Tras descomprimir el archivo TGZ, se encontrara en su interior un fichero install.sh, que se tiene que ejecutar. Centos por defecto no instala SELinux pero, en el caso de que se hubiera hecho, será necesario cambiarlo a modo permissive o disabled para el correcto funcionamiento de Zimbra (SELINUX=permissive en /etc/selinux/config) y reiniciar el servidor para que el cambio surja efecto.

El instalador realizará diversas preguntas, todas muy sencillas de responder. Para unas pruebas iniciales, se recomienda instalar todos los paquetes excepto Zimbra Proxy.

```
Install zimbra-ldap [Y]  
Install zimbra-logger [Y]  
Install zimbra-mta [Y]  
Install zimbra-snmp [Y]  
Install zimbra-store [Y]  
Install zimbra-apache [Y]  
Install zimbra-spell [Y]  
Install zimbra-proxy [N]
```

Al final de la instalación se mostrará un menú de texto con varios puntos pendientes (marcados con asterisco). Será necesario corregir estos puntos antes de aplicar los cambios y terminar el proceso. Como mínimo será necesario ir a la opción 3 para establecer la contraseña de administrador y cambiar el modo del servidor web a https). El resultado final debería de ser el siguiente:

```
1. Common Configuration.
2. zimbra-ldap: Enabled
3. zimbra-store: Enabled
  * Create Admin User: yes
  * Admin user to create: admin@movidatos.com
  * Admin Password:
  * Enable automated spam training: yes
  * Spam training user: spam.n2xvfp2a@movidatos.com
  * Non-spam(Ham) training user: ham.htr37bbj@movidatos.com
  * Global Documents Account: wiki@movidatos.com
  * SMTP host:mailserver.movidatos.com
  * Web server HTTP port: 80
  * Web server HTTPS port: 443
  * Web server mode: https
  * IMAP server port: 143
  * IMAP server SSL port: 993
  * POP server port: 110
  * POP server SSL port: 995
  * Use spell check server: yes
  * Spell server URL: http://mailserver.movidatos.com:7780/aspell.php
4. zimbra-mta: Enabled
5. zimbra-snmp: Enabled
6. zimbra-logger: Enabled
7. zimbra-spell: Enabled
```

8. Default Class of Service Configuration.

r. Start servers after configuration: yes

s. Save config to file

x. Expand menu

q. Quit

A partir de este momento ya se debe ser capaz de acceder al webmail de Zimbra en:

<http://mailserver.movidatos.com>

Como nuestros servicios están corriendo satisfactoriamente entonces se puede ingresar de la siguiente manera, se tiene que ingresar desde otro equipo al administrador se coloca lo siguiente:

<https://mailserver.movidatos.com:7071/zimbraAdmin>

Se ingresa desde el mismo equipo

<https://localhost:7071/zimbraAdmin>

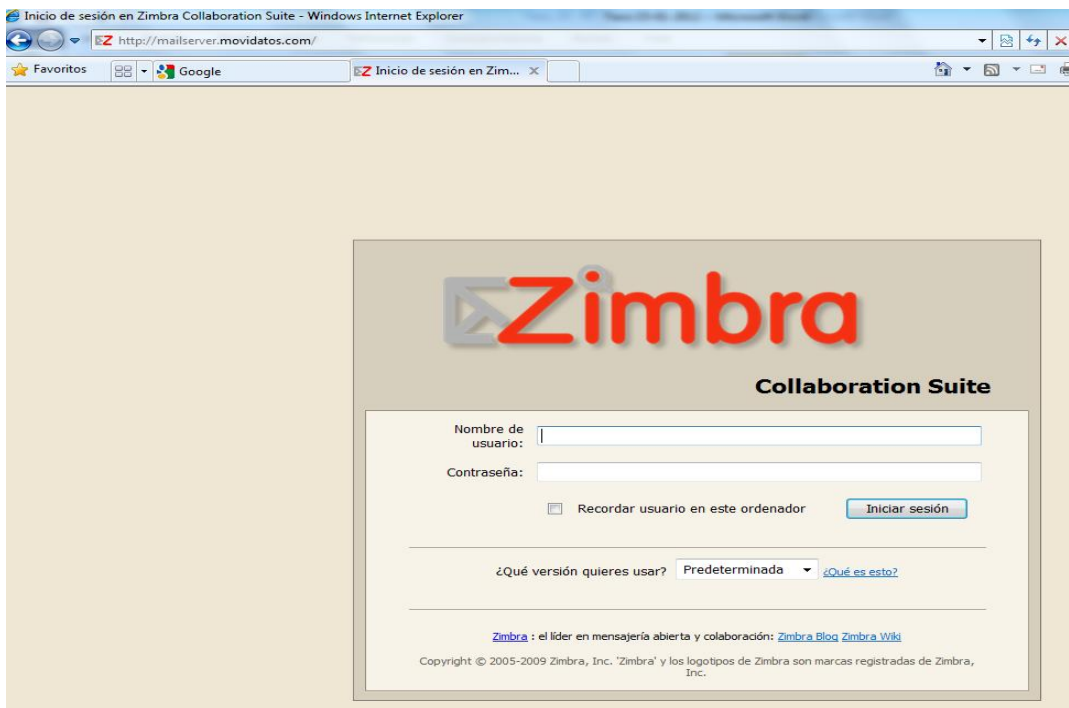


Figura 4.4.3. Acceso cliente web Zimbra Movidatos

Fuente: Autor tesis Henry Padilla.

4.4.3. ADMINISTRACIÓN DIARIA.

Zimbra es una herramienta muy completa y potente, por lo que lleva su tiempo acostumbrarse, ver de qué es capaz y empezar a sacarle verdadero provecho más allá del uso básico como servidor de correo, anotación de citas y gestión de contactos. A continuación se presentan una serie de utilidades varias que son de frecuente uso (todas deberán ejecutarse como usuario zimbra, normalmente accedido mediante *sudo su – zimbra* al hacer login:

- **zmcontrol status:** Obtener el estado de los diversos daemons que forman el sistema Zimbra.
- **zmcontrol start/stop:** Arrancar/parar el sistema Zimbra.
- **zmtlsctl [mixed|both|http|https|redirect]:** Cambiar el tipo de acceso permitido al webmail.

- **mixed:** Realizará la validación sobre HTTPS y luego volverá al modo HTTP.
- **both:** Permitirá indistintamente uno y otro.
- **redirect:** Cambiará al usuario al modo https y lo mantendrá en ese modo (recomendado).
- **http:** Forzará que se trabaje sólo sobre HTTP.
- **https:** Forzará que se trabaje únicamente sobre HTTPS (recomendado).

El fichero de configuración principal de Zimbra es `/opt/zimbra/conf/localconfig.xml`. Cualequier cambios que desee hacer sobre el sistema para que sobrevivan a las actualizaciones deberán realizarse en éste fichero y en los demás dentro del directorio `/opt/zimbra/conf`.

- **zmzimletctl listZimlets:** Mostrará un listado de los Zimlets instalados.
- **zmzimletctl deploy zimlet.zip:** Instalará el Zimlet `zimlet.zip`, que deberá encontrarse dentro del subdirectorio `/opt/zimbra/zimlets-extra/`.
- **zmlocalconfig:** Permite realizar cambios sobre la configuración local guardada en el fichero `/opt/zimbra/conf/localconfig.xml`.
- **zmprov:** Aprovisionamiento de cuentas.
- **zmprov:** es un comando que permite interactuar con casi cualquier parte del sistema desde la consola de comandos, por ejemplo para crear o borrar cuentas desde un script. Puede actuar sobre los siguientes sistemas:
 - Cuentas.
 - Calendario.
 - Configuración.

- COS (Class Of Service).
- Dominios.
- Listas de distribución.
- Buzones de correo.
- Wiki.
- Búsquedas.
- Servidores.
- Otros (misceláneos).

Los comandos de consola disponibles se encuentran en /opt/zimbra/bin. Además, un gran conjunto de utilidades del sistema en forma de scripts de Perl están disponibles en /opt/zimbra/libexec.

Comandos básicos utilizados para la administración del servidor Zimbra:

Comando básico para parar y arrancar Zimbra:

“./zmcontrol stop” y “./zmcontrol start”.

Arrancar o parar el antivirus:

“./zmavavisctl stop/start”

Arrancar o parar el servidor Web:

“./zmapachectl stop/start”.

Estos comandos son necesarios por ejemplo cuando queramos actualizar el antivirus o el certificado SSL sin necesidad de detener el servidor de correo.

En las tareas programadas de Linux se puede ver que hay varias tareas creadas para Zimbra, entre ellas, una tarea que arranca el script “zmdailyreport”. Esta genera un reporte con la cantidad de correo procesados en el día, cuantos correo han llegado a cada persona y cuantos a enviado, los errores en el MTA, etc.

Si se quiere un reporte de un mes entero, se puede modificar los parámetros startTime y endTime del script para ajuntarlo según la necesidad requerida.

También se puede hacer: “./zmlocalconfig -e

zimbra_mtareport_max_recipients=10” y “./zmlocalconfig -e

zimbra_mtareport_max_senders=10” para no hacer el reporte demasiado largo

Se puede utilizar el comando “postqueue -p” para ver la cola de correos en el MTA.

Con “./opt/zimbra/clamav/freshclam --configfile=/opt/zimbra/conf/freshclam.conf” se forza la actualización del antivirus.

4.5. SERVIDOR MULTIPLATAFORMA ZENTYAL.

Zentyal está concebido para ser instalado en una máquina (real o virtual) en este caso se procedió a realizar una instalación real en un servidor físico. Se puedan instalar otros servicios o aplicaciones adicionales, no gestionados a través de la interfaz de Zentyal, que deberán ser instalados y configurados manualmente.

Funciona sobre la distribución Ubuntu en su versión para servidores, usando siempre las ediciones LTS (Long Term Support), cuyo soporte es mayor: cinco años en lugar de tres.

4.5.1. REQUISITOS DE HARDWARE.

Zentyal funciona sobre hardware estándar arquitectura x86 (32-bit) o x86_64 (64-bit). Es conveniente asegurarse de que Ubuntu Lucid 10.04 LTS (kernel 2.6.32) es compatible con el equipo que se vaya a utilizar. Se debería poder comprobar esta información directamente del fabricante. De no ser así, se puede consultar en la lista de compatibilidad de hardware de Ubuntu

Linux, en la lista de servidores certificados para Ubuntu 10.04 LTS o buscando en Google.

Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios utilizan los servicios y de sus hábitos de uso.

Algunos módulos tienen bajos requerimientos, como Cortafuegos, DHCP o DNS, pero otros como el Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU. Los módulos de Proxy y Compartición de ficheros mejoran su rendimiento con discos rápidos debido a su intensivo uso de E/S.

Una configuración RAID añade un nivel de seguridad frente a fallos de disco duro y aumenta la velocidad en operaciones de lectura.

Si usas Zentyal como puerta de enlace o cortafuegos necesitarás al menos dos tarjetas de red, pero si lo usas como un servidor independiente, una única tarjeta de red será suficiente. Si tienes dos o más conexiones de Internet puedes tener una tarjeta de red para cada router o conectarlos a una tarjeta de red teniéndolos en la misma subred. Otra opción es mediante VLAN.

Por otro lado, siempre es recomendable tener un SAI con tu servidor.

Para un servidor de uso general con los patrones de uso normales, los requerimientos siguientes serían los mínimos recomendados:

4.5.2. TABLA DE REQUISITOS HARDWARE

Perfil Zentyal	de	Usuarios	CPU	Memoria	Disco	Tarjetas de red
Puerta de acceso	de	<100	P4 o equivalente	2G	80G	2 ó más
		100 más	Xeon Dual core o equivalente	4G	160G	2 ó más
UTM		<100	P4 o equivalente	2G	80G	1
		100 más	Xeon Dual core o equivalente	4G	160G	1
Infraestructura		<100	P4 o equivalente	1G	80G	1
		100 más	P4 o equivalente	2G	160G	1
Oficina		<100	P4 o equivalente	1G	250G	1
		100 más	Xeon Dual core o equivalente	2G	500G	1

Perfil Zentyal	de Usuarios	CPU	Memoria	Disco	Tarjetas de red
Comunicaciones	<100	Xeon Dual core o equivalente	4G	250G	1
	100 ó más	Xeon Dual core o equivalente	8G	500G	1

Si se combina más de un perfil se deberían aumentar los requerimientos. Si se está desplegando Zentyal en un entorno con más de 100 usuarios, debería hacerse un análisis más detallado, incluyendo patrones de uso, tras un benchmarking y considerando estrategias de alta disponibilidad.

Para la instalación del servidor multitarea Zentyal se preparó el servidor hp ml 150 g5 de la siguiente manera:

- Instalación de la memoria de 2 GB en el slot correspondiente.
- Instalación de la fuente de poder principal como la redundancia de respaldo.
- Instalación de 2 discos de 160 GB SCSI.
- Configuración de la controladora raid.
- Creación de raid 1+0 con 2 discos SCSI.
- Preparación de los discos para la instalación del sistema operativo.

Cuando ya se tiene el hardware correctamente configurado se procedera con la instalación de sistema operativo base de la siguiente manera:

- Instalación de la plataforma principal en este caso distribución plataforma

Zentyal 2.2 Linux anfitrión.

- Se procede a crear las respectivas particiones del sistema operativo

Partición	Tamaño	Ubicación	Formato
Swap	2048 MB	Principio	área de intercambio
/boot	350MB	Principio	ext2
/	150 GB	Principio	ext4
/home	Libre	Principio	ext4

4.5.3. LA INSTALACIÓN PUEDE REALIZARSE DE DOS MANERAS DIFERENTES.

- Usando el instalador de Zentyal (opción recomendada).
- Instalando a partir de una instalación de Ubuntu Server Edition.

En el segundo caso es necesario añadir los repositorios oficiales de Zentyal y proceder a la instalación de aquellos módulos que se deseen.

En el primer caso se facilita la instalación y despliegue de Zentyal ya que todas las dependencias se encuentran en un sólo CD o USB y además se incluye un entorno gráfico que permite usar el interfaz web desde el propio servidor.

El instalador de Zentyal está basado en el instalador de Ubuntu Server así que el proceso de instalación resultará muy familiar a quien ya lo conozca.

En primer lugar se procede a seleccionar el lenguaje de la instalación, para este ejemplo es Español.



Figura 4.5.1. Selección de idioma para instalación de Zentyal.

Fuente: http://doc.zentyal.org/es/_images

Se puede instalar utilizando la opción por omisión que elimina todo el contenido del disco duro y crea las particiones necesarias para Zentyal usando LVM o seleccionar la opción expert mode que permite realizar un particionado personalizado. La mayoría de los usuarios deberían elegir la opción por omisión a no ser que estén instalando en un servidor con RAID por software o quieran hacer un particionado más específico a sus necesidades concretas.



Figura 4.5.2. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

En el siguiente paso se elige el lenguaje que usará la interfaz de nuestro sistema una vez instalado, para ello nos pregunta por el país donde nos localizamos, en este caso Ecuador.

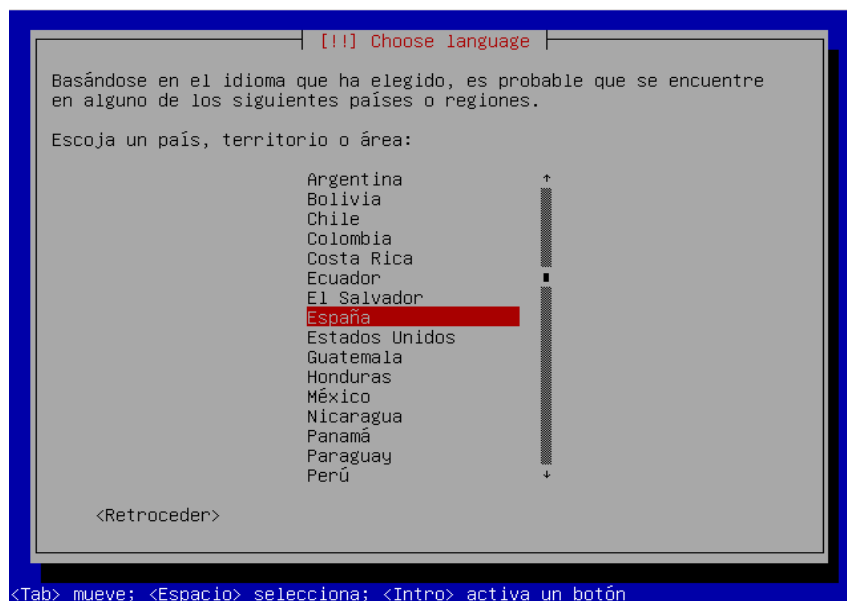


Figura 4.5.3. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

Se puede usar la detección de automática de la distribución del teclado, que hará unas cuantas preguntas para asegurarse del modelo que estamos usando o seleccionarlo manualmente escogiendo No.

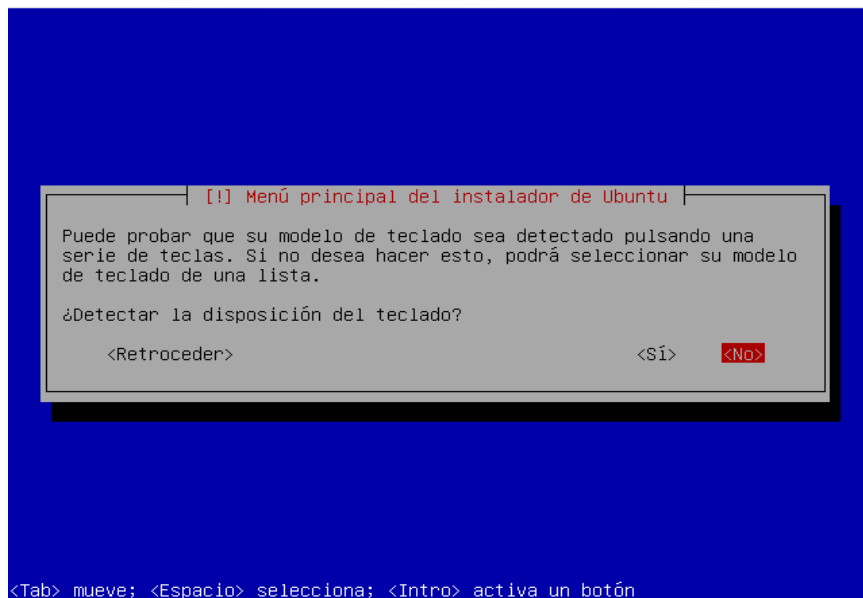


Figura 4.5.4. Instalación Zentyal
Fuente: http://doc.zentyal.org/es/_images

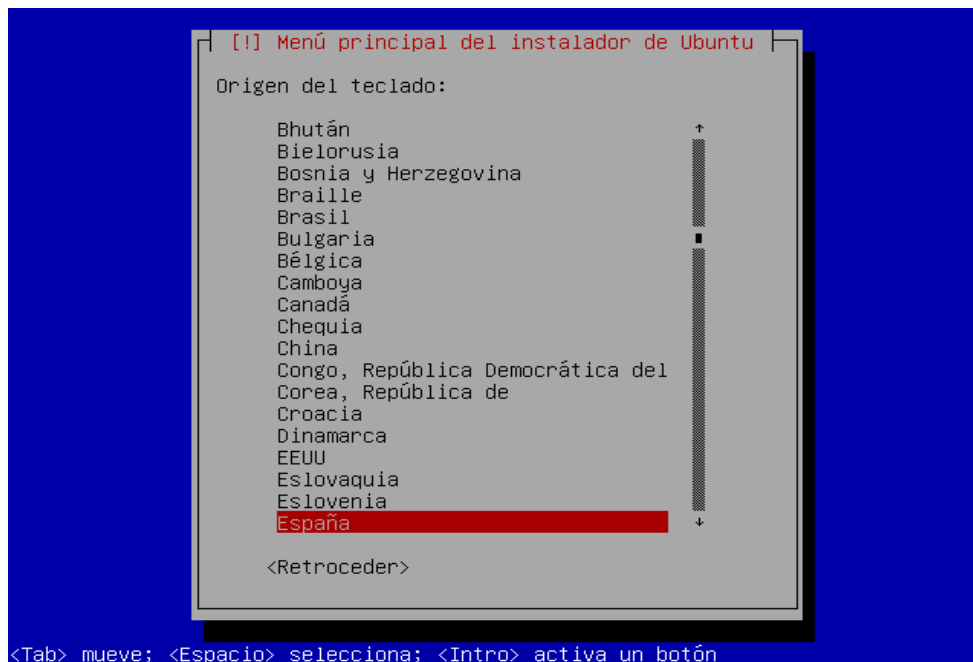


Figura 4.5.5. Instalación Zentyal
Fuente: http://doc.zentyal.org/es/_images

En caso de que dispongamos de más de una interfaz de red, el sistema nos preguntará cuál usar durante la instalación (por ejemplo para descargar actualizaciones).

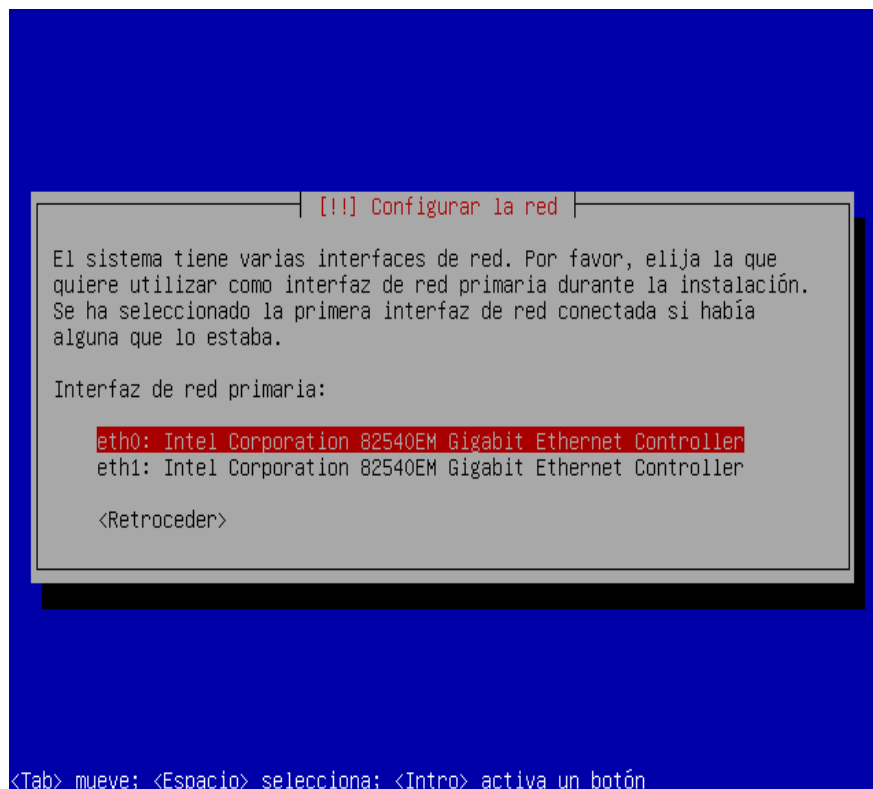


Figura 4.5.6. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

Después se procede a elegir un nombre para nuestro servidor; este nombre es importante para la identificación de la máquina dentro de la red.

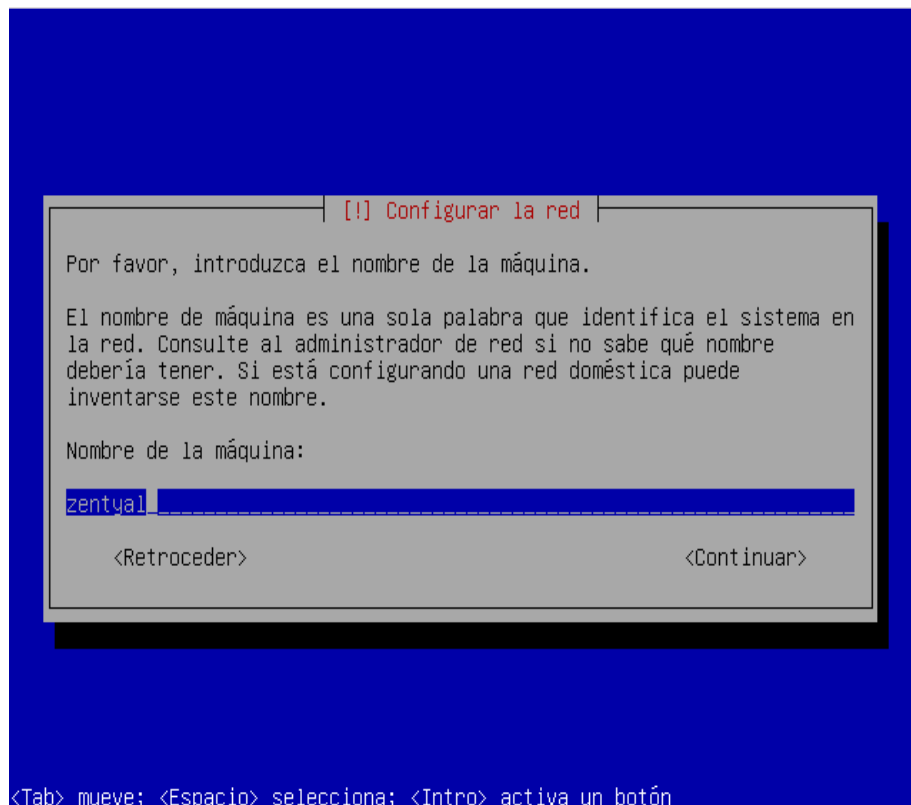


Figura 4.5.7. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

En el siguiente paso, se nos pregunta por nuestra zona horaria, que se autoconfigurará dependiendo del país de origen que hayamos seleccionado anteriormente, pero se puede modificar en caso de que sea errónea.

Una vez terminados estos pasos, comenzará la instalación que irá informando de su estado mediante el avance de la barra de progreso.

A continuación se nos pregunta por el nombre real del administrador.

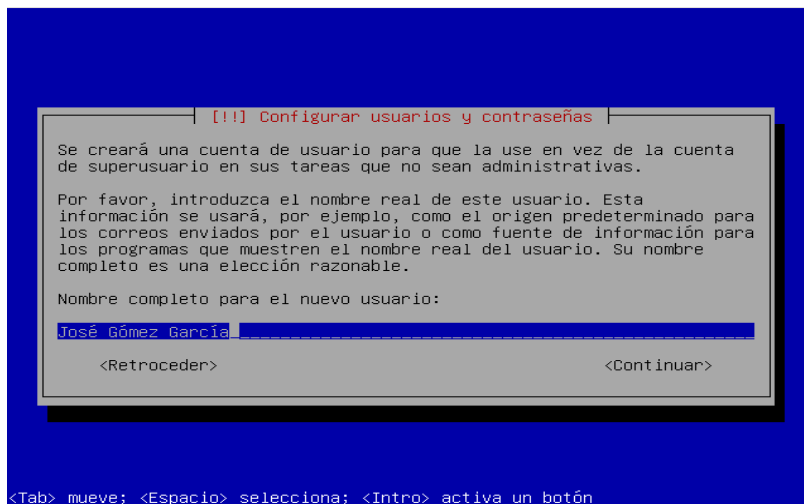


Figura 4.5.7. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

Después, habrá que indicar el nombre de usuario o login usado para identificarse ante el sistema. Este usuario tendrá privilegios de administración y además será el utilizado para acceder a la interfaz de Zentyal.

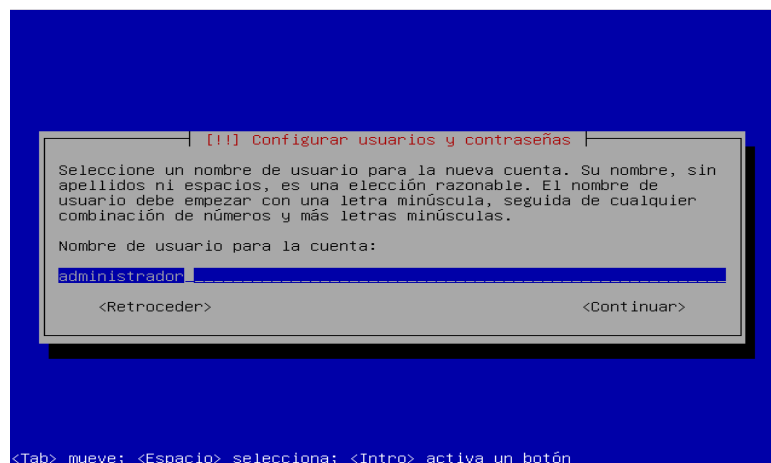


Figura 4.5.8. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

En el siguiente paso nos pedirá la contraseña para el usuario. Cabe destacar que el anterior usuario con esta contraseña podrá acceder tanto al sistema (mediante SSH o *login* local) como a la interfaz web de Zentyal, por lo que se tiene que ser

especialmente cuidadosos en elegir una contraseña segura (más de 12 caracteres incluyendo letras, cifras y símbolos de puntuación).

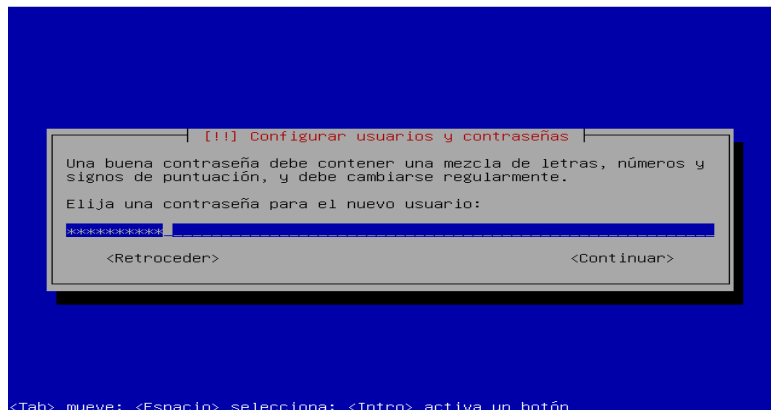


Figura 4.5.9. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images



Figura 4.5.10. Instalación Zentyal

Fuente: http://doc.zentyal.org/es/_images

Se tiene que esperar que nuestro sistema básico se instale, mientras muestra una barra de progreso. Este proceso puede durar unos 20 minutos aproximadamente, dependiendo del servidor en cada caso.

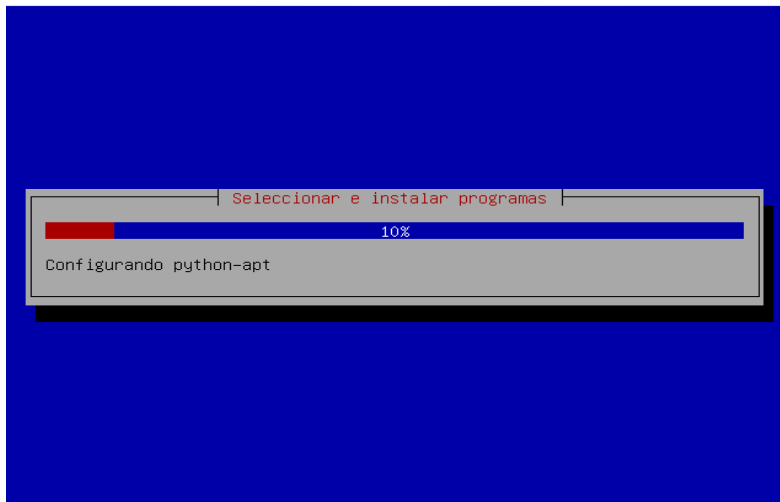


Figura 4.5.11. Instalación Zentyal
Fuente: http://doc.zentyal.org/es/_images

La instalación del sistema base está completada; ahora se procede a extraer el disco de instalación y reiniciar.

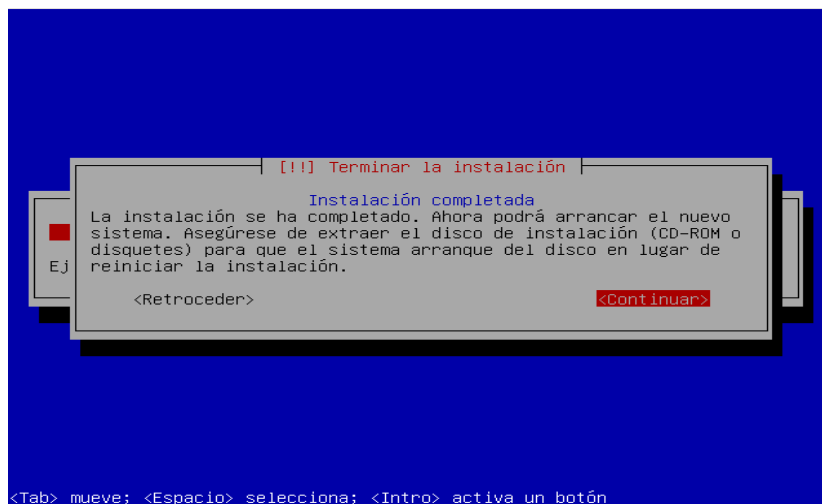


Figura 4.5.12. Instalación Zentyal
Fuente: http://doc.zentyal.org/es/_images

Nuestro sistema Zentyal está instalado.

El sistema arrancará un interfaz gráfico con un navegador que permite acceder a la interfaz de administración, y, aunque tras este primer reinicio el sistema haya iniciado

el entorno gráfico automáticamente, de aquí en adelante, necesitará autenticarse antes de que éste arranque.

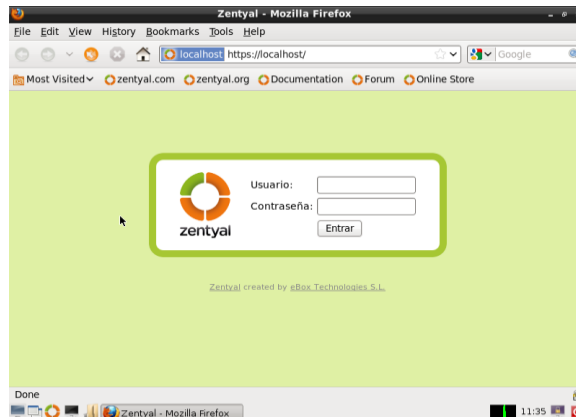


Figura 4.5.13. Acceso Zentyal

Fuente: http://doc.zentyal.org/es/_images

4.6. CONFIGURACIÓN E INTEGRACIÓN DEL SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE.

Una vez implementado e instalado el servidor de correo Zimbra en una máquina virtual con la herramienta de virtualización Virtual Box en el servidor principal de virtualización ML350 G6, se procede a configurar el servidor virtual de correo.

Las características a configurar la máquina virtual son las siguientes para su correcto funcionamiento:

Nombre maquina virtual: SRVMAIL_PRODUCION

Tipo sistema operativo: Centos 5.5

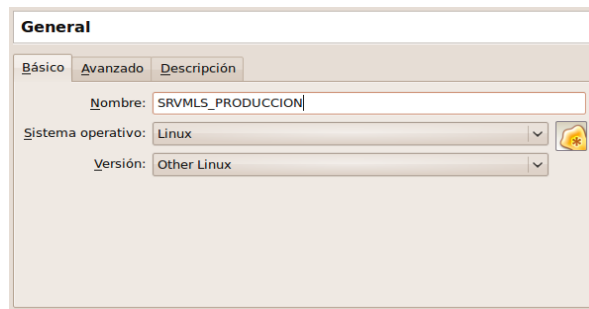


Figura 4.6.1. Configuración servidores virtuales en VirtualBox

Fuente: Autor tesis Henry Padilla

Memoria base: 2048 MB



Figura 4.6.2. Configuración servidores virtuales en VirtualBox

Fuente: Autor tesis Henry Padilla

Procesadores: 1

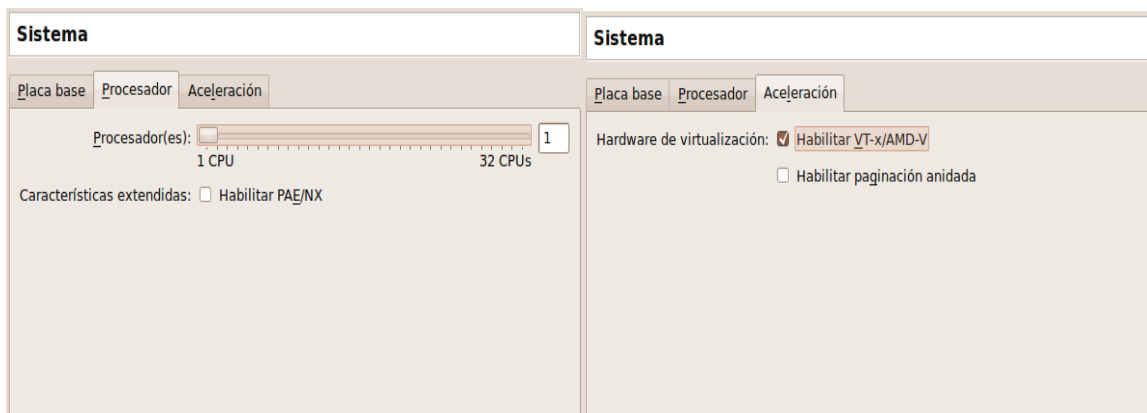


Figura 4.6.3. Configuración servidores virtuales en VirtualBox

Fuente: Autor tesis Henry Padilla

Memoria de video: 12 MB

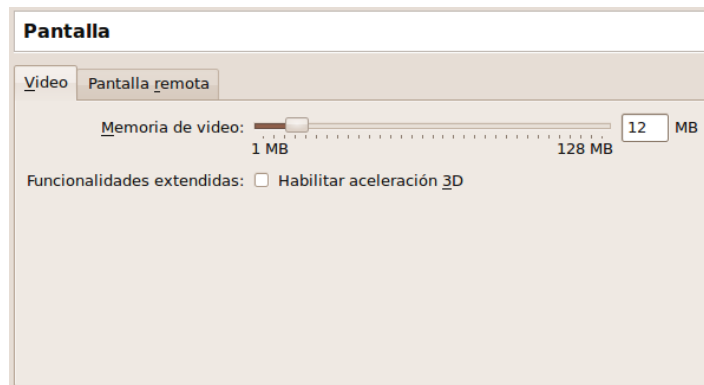


Figura 4.6.4. Configuración servidores virtuales en VirtualBox

Fuente: Autor tesis Henry Padilla

Disco Duros: Zimbra-Movidatos.vdi

Tamaño disco: 300 GB

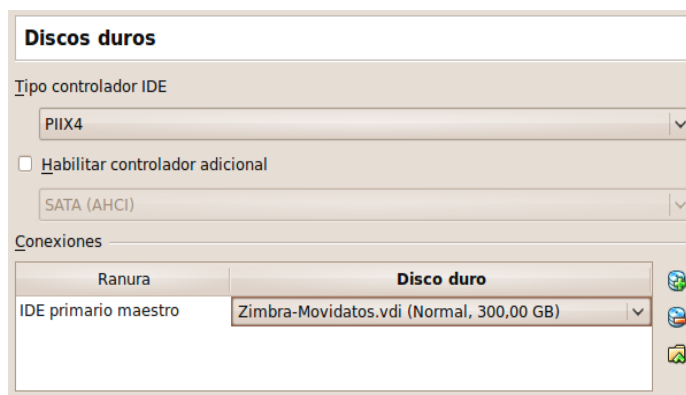


Figura 4.6.5. Configuración servidores virtuales en VirtualBox

Fuente: Autor tesis Henry Padilla

Red:

Adaptador 1: Intel PRO/100 (Adaptador puente, Eth0)

Adaptador de red para conexión de red LAN.

Adaptador 2: Intel PRO/100 (Adaptador puente, Eth1)

Adaptador de red para conexión de red WAN.

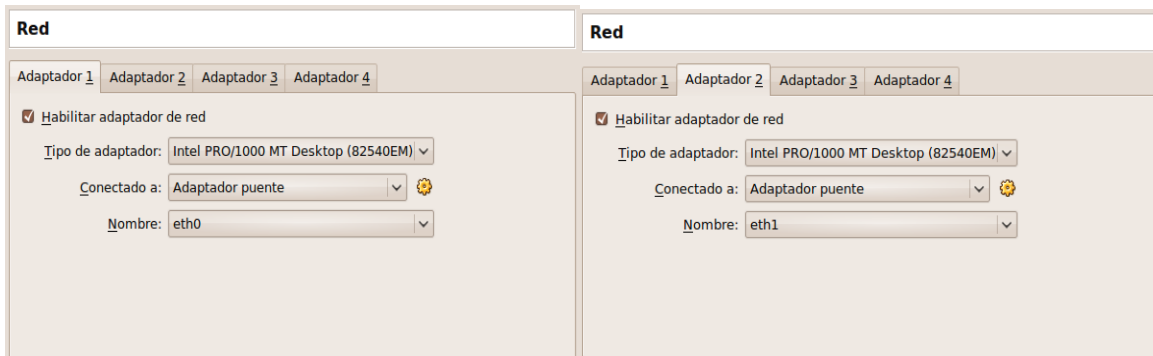


Figura 4.6.6. Configuración servidores virtuales en VirtualBox
Fuente: Autor tesis Henry Padilla

Para finalizar la configuración de la máquina virtual se procede a verificar el registró de todas las configuraciones realizadas.

Preparada la máquina virtual de Zimbra se procede a iniciar el servidor de correo virtualizado.

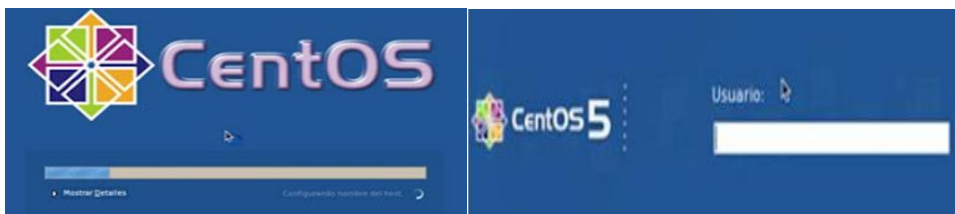


Figura 4.6.7. Configuración servidores virtuales en VirtualBox
Fuente: Autor tesis Henry Padilla

Una vez iniciado el servidor de correo Zimbra.

Luego se procede a verificar conectividad de las tarjetas de red Eth1 y Eth0 para tener acceso a la interfaz web de Zimbra desde la red interna como la red externa en la máquina virtual.

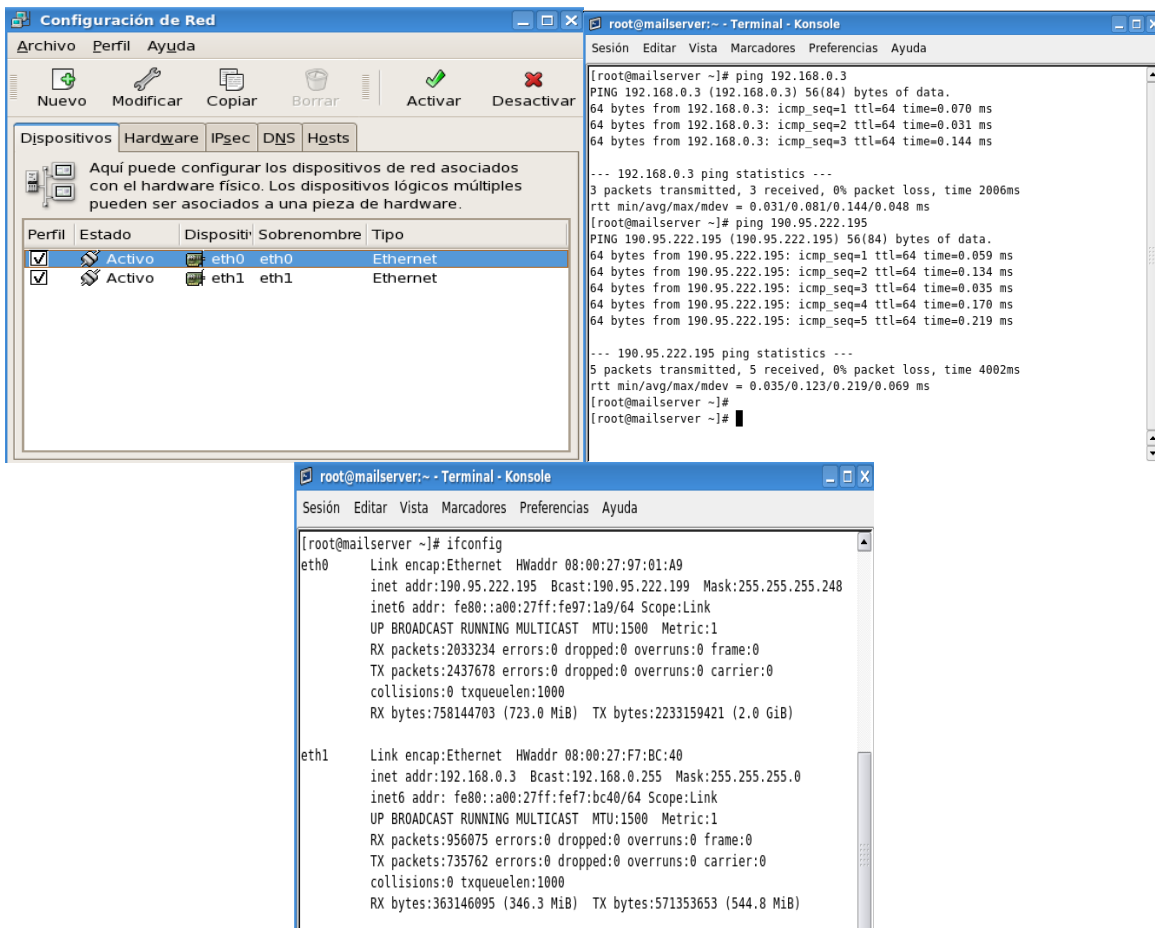


Figura 4.6.8. Tarjetas de red en VirtualBox

Fuente: Autor tesis Henry Padilla

También se tiene que verificar el estado de la instalación como implementación del servidor virtual de correo Zimbra.

Verificamos el servidor de correo Zimbra ingresando desde un terminal al usuario de administración Zimbra a nivel de consola para verificar el estado del servidor virtual.

```
zimbra@mailserver:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[zimbra@mailserver ~]$ zmcontrol status
Host mailserver.movidatos.com
    antispam           Running
    antivirus          Running
    ldap              Running
    logger            Running
    mailbox           Running
    mta               Running
    snmp              Running
    spell             Running
    stats             Running
[zimbra@mailserver ~]$ zmcontrol -v
Release 5.0.23_GA_3242.RHEL5_20100326192051 CentOS5 FOSS edition
```

Figura 4.6.9. Verificación estado servicios Zimbra

Fuente: Autor tesis Henry Padilla

A nivel de terminal se verifica el correcto estado de los siguientes servicios se zimbra:

- Antispam.
- Antivirus.
- Ldap.
- Logger.
- Mailbox.
- Mta.
- Snmp
- Spell.
- Stats.

También se verifica la correcta resolución del dominio Movidatos como la verificación del nombre del servidor.

```
zimbra@mailserver:~ - Terminal - Konsole
Sesión Editar Vista Marcadores Preferencias Ayuda
[zimbra@mailserver ~]$ zmprov gas
mailserver.movidatos.com
[zimbra@mailserver ~]$ zmprov gad
movidatos.com
```

Figura 4.6.10. Verificación del dominio de Zimbra

Fuente: Autor tesis Henry Padilla

Finalizado la verificación del estado del servidor Zimbra a nivel de terminal en Centos.

Luego se tiene que verificar el acceso a consola de administración de Zimbra vía interfaz web mediante un navegador de internet.

Acceso a nivel interno.

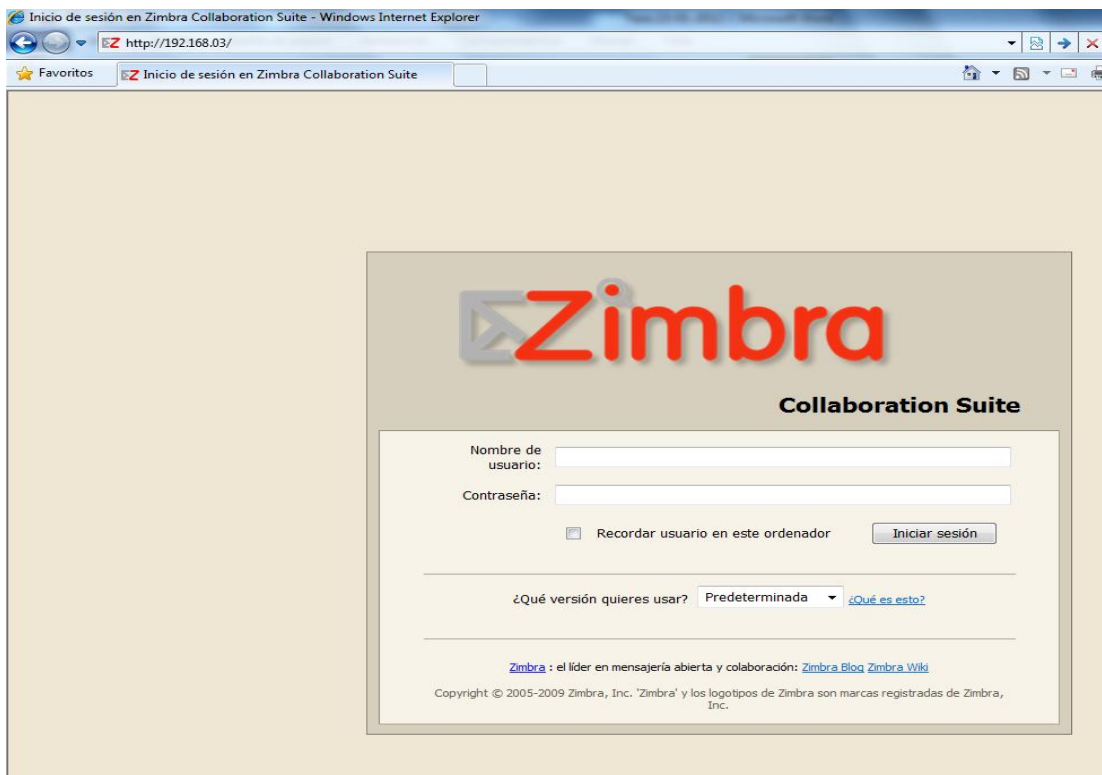


Figura 4.6.11. Acceso interno vía web Zimbra

Fuente: Autor tesis Henry Padilla

Acceso a nivel externo.



Figura 4.6.12. Acceso externo vía web Zimbra

Fuente: Autor tesis Henry Padilla

Para el acceso a la consola de administración utilizamos un nivel de acceso por puerto seguro https utilizando el puerto 7071. El acceso a la consola de administración esta soportado por el navegador de internet Firefox, safari, no está soportado para internet explorer.

https://mailserver.movidatos.com:7071



Figura 4.6.13. Acceso consola de administración Zimbra

Fuente: Autor tesis Henry Padilla

4.6.1. OPCIONES CONSOLA DE ADMINISTRACIÓN.

En el Panel de navegación el administrador tiene a su disposición las siguientes áreas:

- **Direcciones:** Se puede seleccionar configurar o editar Cuentas, Alias, Listas de Distribución y Recursos. Cuando se seleccione una función, el panel de Contenido muestra los detalles por dominio.
- **Configuración:** Funciones de servidor que pueden ser configurados, incluyendo Clases de Servicio, Dominios, Servidores, Zimlets (Complementos), Extensiones de Consola de Administración y Configuración General.
- **Supervisión:** Las funciones de monitoreo incluyen Estado del Servidor para apreciar el estado de todos los servidores y servicios instalados, y Estadísticas del servidor que muestren gráficos de barras del número de mensajes, volumen de mensajes, actividad antivirus y antispam, uso de disco, número de cuentas activas y capacidad de cuentas de correo para cada cuenta.

- **Herramientas:** En Colas de mensajes, se puede apreciar un vistazo del contenido de las colas de mensajes enviados, recibidos, activos, guardados y corruptos. En Certificados se pueden apreciar los certificados de seguridad para cada servidor.
- **Búsquedas:** Se puede crear y guardar búsquedas ejecutadas frecuentemente. Algunas búsquedas son incluidas automáticamente, como las búsquedas de todas las cuentas inactivas, las cuentas bloqueadas, cuentas de administración, y cuentas cerradas.

Además, la consola de administración de Zimbra cuenta con otros paneles de administración:

- **Panel de contenido:** Ubicado a la derecha del panel de navegación. Cuando se hace clic sobre una función en el panel de Navegación, el panel de Contenido cambia para reflejar dicha vista. Se puede abrir múltiples paneles de Contenido para una función específica. Por ejemplo, seleccionar de la lista de cuentas. Cada cuenta es abierta en una nueva pestaña detrás de la pestaña de Administración de Cuentas.
- **Barra de Herramientas:** La barra aparece encima del panel de contenido. Cuentas, Clases de Servicio, Dominios y Servidores muestran sus opciones específicas de barra de herramientas.
- **Barra de Búsqueda:** Usar la barra de búsqueda encima del panel de contenido para rápidamente buscar pos cuentas específicas, alias, listas de distribución, recursos, y dominios. Buscar Ayuda es una poderosa búsqueda unificada que localiza información en los foros, wiki y documentos de Zimbra. Clic en Búsqueda Avanzada para construir una búsqueda más avanzada.

Centro de Asistencia (Help Desk) ofrece enlaces a la documentación de Zimbra (en inglés), incluyendo las herramientas de migración.

- **Caja de Estado:** Esta es la caja en el lado inferior izquierdo de la ventana. Varios mensajes de Zimbra y la hora son mostrados aquí.

Funciones configuradas en el servidor virtual de correo Zimbra Movidatos.

- **Cuentas:** Cada dirección de correo de la cuenta, nombre a mostrar, y estado son mostrados en el panel de contenido por dominio. En Cuentas, se pueden crear y manejar cuentas de usuario, cambiar claves de acceso y ver el correo electrónico de una cuenta.
- **Alias:** Todos los alias de las cuentas son mostrados. En Alias se puede crear y administrar alias de usuario y mover alias.
- **Listas de correo:** Las listas de correo y su estado (habilitado o deshabilitado) son mostrados. Se puede crear y manejar listas de correo desde esta sección.
- **Recursos:** Se listan ubicaciones o equipos que pueden ser planificados para una cita. Se pueden crear nuevos recursos y establecer políticas para los recursos.
- **Clases de Servicio:** Todas las Clases de Servicio (COS) que pueden ser definidas son mostradas. Por lo menos, la COS por defecto es mostrada. Se pueden crear y editar COS.
- **Dominios:** Se muestran los dominios en el ambiente Zimbra. Se pueden crear y administrar dominios, establecer el modo Lista de Direcciones Global (GAL, Global Address List).

- **Servidores:** Los servidores, el nombre del host, y la descripción son mostrados. Se pueden editar y borrar registros de servidores para los servidores instalados.
- **Zimlets:** Los complementos (Zimlets) pueden ser desplegados y administrados desde la consola de administración.
- **Administración de Extensiones:** Las extensiones de administración pueden ser desplegadas y administradas desde la consola de administración.
- **Configuración General:** La configuración para las preferencias globales de seguridad, libreta de direcciones, MTA (Mail Transfer Agent), soporte para recepción de correo vía POP e IMAP, y protecciones antivirus y antispam pueden ser modificadas. Estas preferencias son utilizadas cuando las preferencias de servidor, opciones personales, y Clase de Servicio no han sido establecidas.
- **Estado del Servidor:** El estado actual de cada servidor y servicio es mostrado, incluyendo Zimbra MTA, Zimbra LDAP, Zimbra Store, SNMP y los servicios antivirus y antispam.
- **Estadísticas del Servidor:** Ambos tipos de datos, respecto a la totalidad de servidores y servidor específico acerca del volumen de mensajes recibidos, número de mensajes, actividad antivirus y antispam, y uso de disco para mensajes procesados en las últimas 48 horas, y los últimos 30, 60, y 365 días. Datos referentes a datos específicos por servidor incluyen cuota de información.
- **Cola de Mensajes:** Muestra el número de mensajes en el Agente de Transferencia Correo (MTA) que están en las colas de mensajes enviados, recibidos, activos y almacenados.

4.7. IMPLEMENTACIÓN, CONFIGURACIÓN E INTEGRACIÓN DEL SERVIDOR FISICO MULTITAREA ZENTYAL.

Una vez implementado e instalado el servidor físico multitarea Zentyal en un servidor hp ml150 g6, se procede a configurar el servidor.

Las características a configurar el servidor son las siguientes para su correcto funcionamiento:

En primer lugar se procede a verificar la configuración del arreglo raid 1+0 establecida en la instalación del sistema principal anfitrión.

Luego se procede a configurar la tarjeta de red de acceso interno como la tarjeta de red de acceso externo.

4.7.1. CONFIGURACIÓN DE RED EN ZENTYAL.

A través de red, interfaces se puede acceder a la configuración de cada una de las tarjetas de red detectadas por el sistema y se pueden establecer como dirección de red estática (configurada manualmente), dinámica (configurada mediante DHCP)

Además cada interfaz puede definirse como externa si está conectada a una red externa, normalmente Internet, para aplicar políticas más estrictas en el cortafuego. En caso contrario se asumirá interna, conectada a la red local.

Tarjeta de red interna Eth0.

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 eth1

Nombre:

Método:

Externo (WAN):

Dirección IP:

Máscara de red:

Figura 4.7.1. Configuración tarjeta de red en Zentyal.

Fuente: Autor tesis Henry Padilla

Ip interna: 192.168.0.5

Mascara: 255.255.255.0

Gateway: 192.168.0.5

Tarjeta de red externa Eth1.

eth0 **eth1**

Nombre:

Método:

Externo (WAN):

Dirección IP:

Máscara de red:

Figura 4.7.2. Configuración tarjeta de red en Zentyal.

Fuente: Autor tesis Henry Padilla

Ip externa: 190.95.222.198

Mascara: 255.255.255.248

Gateway: 190.95.222.193

Ingresado los datos de telecomunicaciones correspondientes para la conexión de red interna como externa.

Se procede a verificar las configuraciones establecidas.

Se tiene que verificar que exista conectividad entre el servidor y sus clientes, cuando este ya establecido esta conexión se procede a realizar las siguientes implementaciones como configuraciones para la integración del servidor a la infraestructura de Movidatos y sus clientes puedan utilizar sus servicios como recursos.

4.8. SERVICIO DE DIRECTORIO (LDAP) ZENTYAL.

4.8.1. INTRODUCCIÓN AL SERVICIO DE DIRECTORIO (LDAP)

Zentyal integra OpenLDAP como servicio de directorio, con tecnología Samba para implementar la funcionalidad de controlador de dominios Windows además de para la compartición de ficheros e impresoras.

Como se ha explicado, Zentyal está diseñado de manera modular, permitiendo al administrador distribuir los servicios entre varias máquinas de la red. Para que esto sea posible, el módulo de usuarios y grupos puede configurarse siguiendo una arquitectura para compartir usuarios entre los diferentes servidores.

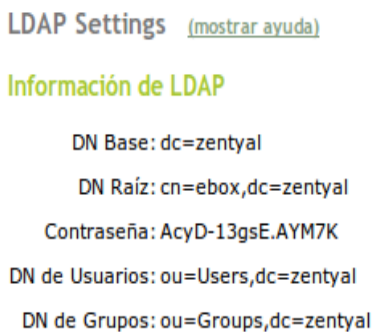
Por defecto y a no ser que se indique lo contrario en el menú usuarios y grupos, el módulo se configurará como un directorio LDAP maestro y el nombre distinguido del directorio se establecerá de acuerdo al nombre de la máquina.

4.9. SERVIDOR LDAP CON ZENTYAL

4.9.1. OPCIONES DE CONFIGURACIÓN DE LDAP

Teniendo el servidor Zentyal como maestro, desde usuarios y grupos, opciones de configuración de LDAP se puede comprobar cuál es nuestra configuración actual de LDAP y realizar algunos ajustes relacionados con la configuración de autenticación PAM del sistema.

En la parte superior se puede ver la información de LDAP.



The image shows a screenshot of the 'LDAP Settings' interface in Zentyal. At the top, it says 'LDAP Settings' with a link '(mostrar ayuda)'. Below that is the heading 'Información de LDAP'. The settings listed are: 'DN Base: dc=zentyal', 'DN Raíz: cn=ebox,dc=zentyal', 'Contraseña: AcyD-13gsE.AYM7K', 'DN de Usuarios: ou=Users,dc=zentyal', and 'DN de Grupos: ou=Groups,dc=zentyal'.

Figura 4.9.1. Datos LDAP en Zentyal.

Fuente: Autor tesis Henry Padilla

4.10. COMPARTICIÓN DE FICHEROS Y A LA AUTENTICACIÓN.

Zentyal usa Samba para implementar SMB/CIFS.

4.10.1. SERVIDOR DE FICHEROS CON ZENTYAL.

Los servicios de compartición de ficheros están activos cuando el módulo de compartición de ficheros está activo, sin importar si la función de PDC lo está.

Con Zentyal la compartición de ficheros está integrada con los usuarios y grupos. De tal manera que cada usuario tendrá su directorio personal y cada grupo puede tener un directorio compartido para todos sus usuarios.

El directorio personal de cada usuario es compartido automáticamente y sólo puede ser accedido por el correspondiente usuario.

Compartir ficheros (mostrar ayuda)

Configuración general PDC Directorios compartidos Papelera de Reciclaje

Habilitar PDC:

Nombre del dominio: ZENTYAL-DOMAIN

Nombre de Netbios: zentyal

Descripción: Zentyal File Server

Límite de cuota: Limitada a 100 Mb

Habilitar perfiles móviles:

Letra de unidad: H

Grupo Samba: Todos los usuarios

Sólo los usuarios que pertenecen a este grupo tendrán una cuenta de Samba. Sincronización ocurre cada hora.

Cambiar

Figura 4.10.1. Información servidor PDC en Zentyal.

Fuente: Autor tesis Henry Padilla

4.10.2. COMPARTICIÓN DE FICHEROS.

Se establece el dominio donde se trabajará dentro de la red local en Windows, y como nombre NetBIOS el nombre que identificará al servidor Zentyal dentro de la red Windows. Se le puede dar una descripción larga para describir el dominio.

Además se puede establecer de manera opcional un límite de cuota. Con el grupo Samba se puede opcionalmente configurar un grupo exclusivo en el que sus usuarios tengan cuenta de compartición de ficheros en vez de todos los usuarios, la sincronización se hace cada hora.

Para crear un directorio compartido, se accede a compartir ficheros, directorios compartidos y se pulsa añadir nuevo.

Compartir ficheros [\(mostrar ayuda\)](#)

Configuración general PDC **Directorios compartidos** Papelera de Reciclaje

Añadiendo un nuevo recurso compartido

Habilitado:

Nombre del recurso compartido:

Ruta del recurso compartido:
Directorio bajo Zentyal creará automáticamente el directorio compartido share.directory en /home/samba/shares
File system path permitirá compartir un directorio existente en su sistema de archivos

Comentario:

Acceso de invitado:
 Este directorio compartido no necesita de autenticación.

Figura 4.10.2. Compartición de ficheros en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

Compartir ficheros [\(mostrar ayuda\)](#)

Configuración general PDC **Directorios compartidos** Papelera de Reciclaje

recurso compartido añadida

[+ Añade nuevo](#)

Habilitado	Nombre del recurso compartido	Ruta del recurso compartido	Comentario	Acceso de invitado	Control de acceso	Action
<input checked="" type="checkbox"/>	facturas	facturas	Facturas procesadas	<input type="checkbox"/>		

10 ▼ Página 1

Figura 4.10.3. Compartición de ficheros en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.10.3. LISTA DE DIRECTORIOS COMPARTIDOS

Desde la lista de directorios compartidos se puede editar el control de acceso. Allí, pulsando en añadir nuevo, puede asignar permisos de lectura, lectura y escritura o administración a un usuario o a un grupo. Si un usuario es administrador de un directorio compartido podrá leer, escribir y borrar ficheros de cualquier otro usuario dentro de dicho directorio.



Figura 4.10.4. Compartición de ficheros en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.10.4. AUTENTICACIÓN CON ZENTYAL

Para aprovechar las posibilidades del PDC como servidor de autenticación y su implementación Samba para Linux se debe marcar la casilla habilitar PDC a través de compartir ficheros > configuración general.



Figura 4.10.5. Autenticación en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

Si la opción perfiles móviles está activada, el servidor PDC no sólo realizará la autenticación, sino que también almacenará los perfiles de cada usuario. Estos perfiles contienen toda la información del usuario, como sus preferencias de Windows, sus cuentas de correo de outlook, o sus documentos.

Cuando un usuario inicie sesión, recibirá del servidor PDC su perfil. De esta manera, el usuario dispondrá de su entorno de trabajo en varios ordenadores. Hay que tener en cuenta antes de activar esta opción que la información de los usuarios puede ocupar varios gigabytes de información, el servidor PDC necesitará espacio de disco suficiente. También se puede configurar la letra del disco al que se conectará el directorio personal del usuario tras autenticar contra el PDC en Windows.

4.11. CONFIGURACIÓN DE PROXY HTTP CON ZENTYAL.

Para configurar el proxy HTTP se tiene que ubicar en proxy HTTP, general. Para definir si el proxy funciona en modo proxy transparente para forzar la política establecida o si por el contrario requerirá configuración manual.

En este último caso, en puerto se establecerá dónde escuchará el servidor conexiones entrantes. El puerto preseleccionado es el 3128, otros puertos típicos son el 8000 y el 8080. El proxy de Zentyal únicamente acepta conexiones provenientes de las interfaces de red internas, por tanto, se debe usar una dirección interna en la configuración del navegador.

El tamaño de la caché define el espacio en disco máximo usado para almacenar temporalmente contenidos web. Se establece en tamaño de caché y corresponde a cada administrador decidir cuál es el tamaño óptimo teniendo en cuenta las características del servidor y el tráfico esperado.

Además también se debe establecer aquí la política predeterminada para el acceso al contenido web HTTP a través del proxy. Esta política determina si se puede acceder o no a la web y si se aplica el filtro de contenidos.

Puede configurarse de las siguientes maneras:

- **Permitir todo:**

Con esta política se permite a los usuarios navegar sin ningún tipo de restricciones pero todavía disfrutando de las ventajas de la caché, ahorro de tráfico y mayor velocidad.

Denegar todo:

Esta política deniega totalmente el acceso a la web. Aunque a primera vista podría parecer poco útil ya que el mismo efecto se podría conseguir con una regla de cortafuegos, sin embargo también se puede establecer posteriormente políticas particulares para objetos, usuarios o grupos, pudiendo usar esta política para denegar en principio y luego aceptar explícitamente en determinadas condiciones.

Filtrar:

Esta política permite a los usuarios navegar pero activa el filtrado de contenidos que puede denegar el acceso web según el contenido solicitado por los usuarios.

Autorizar y filtrar, permitir todo o denegar todo:

Estas políticas son versiones de las políticas anteriores que incluyen autorización. La autorización se explicará en la sección configuración avanzada para el proxy HTTP.

Proxy HTTP [\(mostrar ayuda\)](#)

Configuración General

Proxy Transparente:

Nótese que no se puede usar proxy HTTPS de forma transparente. Se necesitará añadir una regla de firewall si se habilita este modo.

Puerto:

Tamaño de los ficheros de caché (MB):

Política predeterminada:

Filter significa que las peticiones HTTP pasan por el filtro de contenidos y que podrían ser rechazados si el contenido no se considera válido.

Excepciones en la caché

[+ Añade nuevo](#)

<input type="text"/> <input type="button" value="Buscar"/>		
Dirección del nombre de dominio	Negar almacenamiento en caché del dominio	Action
miorganizacion.com	<input checked="" type="checkbox"/>	<input type="button" value="Eliminar"/> <input type="button" value="Editar"/>

10 Página 1

Figura 4.11.1. Configuración proxy en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.11.1. PROXY HTTP

Es posible indicar que dominios no serán almacenados en caché. Si se tiene servidores web locales no se acelerará su acceso usando la caché y se desperdiciaría memoria que podría ser usada por elementos de servidores remotos.

Si un dominio está exento de la caché, cuando se reciba una petición con destino a dicho dominio se ignorará la caché y se devolverán directamente los datos recibidos desde el servidor sin almacenarlos. Estos dominios se definen en Excepciones a la caché.

Tras establecer la política global, se puede definir políticas particulares para objetos de red en proxy HTTP, política de objetos. También puede elegir cualquiera de las seis políticas para cada objeto cuando se acceda al proxy desde cualquier miembro

del objeto esta política tendrá preferencia sobre la política global. Una dirección de red puede estar contenida en varios objetos distintos por lo que es posible ordenar los objetos para reflejar la prioridad. Se aplicará la política del objeto de mayor prioridad que contenga la dirección de red. Además existe la posibilidad de definir un rango horario fuera del cual no se permitirá acceso al objeto de red aunque esta opción sólo es compatible con políticas de permitir o denegar y no con políticas de filtrado de contenidos.

Política de Objeto [\(mostrar ayuda\)](#)

[Lista de objetos](#)

[+ Añade nuevo](#)

Objeto	Política	Periodo de tiempo permitido	Política de grupo	Perfil de filtrado	Action
Guest	Authorize and allow	08:00-20:00 MTW		default	
Ventas	Always allow	All time		default	
IT	Always allow	All time		default	
DMZ	Always deny	All time		default	

10 ▼ Página 1

Figura 4.11.2. Política de objetos en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.11.2. FILTRADO DE CONTENIDOS CON ZENTYAL

Zentyal permite el filtrado de páginas web en base a su contenido. Para ello, es necesario que la política global o la política particular de cada objeto desde el que se accede sean de filtrar o autorizar y filtrar.

Se pueden definir múltiples perfiles de filtrado en proxy HTTP, perfiles de filtrado pero si no hay ninguno específico aplicándose al usuario, grupo u objeto se aplicará el perfil default.

Filtrar perfiles [\(mostrar ayuda\)](#)

Lista de perfiles

[+ Añade nuevo](#)

Filtrar grupo	Configuración	Action
default		 
Ventas		 
IT		 

10 ▼ Página 1 

Figura 4.11.3. Filtrado de contenidos en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

El filtrado de contenidos de las páginas web se utiliza diferentes métodos incluyendo filtrado heurístico, tipos MIME, extensiones, listas blancas y listas negras entre otros. La conclusión final es determinar si una página o un recurso web puede ser visitado o no.

El primer filtro que se puede configurar es el antivirus. Para poder utilizarlo se debe tener el módulo de Antivirus instalado y activado. Si está activado se bloqueará el tráfico HTTP en el que sean detectados virus.

El filtrado heurístico consiste principalmente en el análisis de los textos presentes en las páginas web, si se considera que el contenido no es apropiado (pornografía, racismo, violencia, etc) se bloqueará el acceso a la página.

Para controlar este proceso se puede establecer un umbral más o menos restrictivo, siendo este el valor que se comparará con la puntuación asignada a la página para decidir si se bloquea o no. El lugar donde establecer el umbral es la sección umbral de filtrado de contenido.

Se puede desactivar este filtro eligiendo el valor desactivado. Hay que tener en cuenta que con este análisis se pueden llegar a bloquear páginas no deseadas, lo que se conoce como un falso positivo. Este problema se puede remediar añadiendo los dominios de estas páginas a una lista blanca, pero siempre existirá el riesgo de un falso positivo con nuevas páginas.

También se tiene a continuación el filtrado de extensiones de fichero, el filtrado de tipos MIME y el filtrado de dominios.

Umbral de filtrado de contenido

Usar el umbral del perfil por defecto:

Umbral: Medio ▼

Esto especifica cuán estricto es el filtro

Change

Filtrado de extensiones de fichero
Filtrado de tipos MIME
Filtrado de dominios para grupo de filtros

Usar perfil predeterminado para el filtrado de MIME

Usar configuración del perfil predeterminado:

Change

✪ Tipo MIME añadido

Configurar tipos MIME permitidos

[+ Añade nuevo](#)

Buscar

Tipo MIME	Permitir	Action
application/compress	☑	🗑️ ✎
application/gzip	☑	🗑️ ✎
audio/mpeg	☑	🗑️ ✎
audio/x-wav	☑	🗑️ ✎

10 ▼ Página 1
⏪ ⏩ ⏴ ⏵

Configurar politica para todos los tipos MIME

Permitir todos Tipos MIME:

Usar este campo para cambiar el valor de todas filas de arriba a la vez

Change

Figura 4.11.4. Filtrado de contenidos tipos MIME en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

En la pestaña de filtrado de extensiones de fichero se puede seleccionar qué extensiones serán bloqueadas. De manera similar en filtrado de tipos MIME se pueden indicar qué tipos MIME se quieren bloquear y añadir otros nuevos si es necesario, al igual que con las extensiones.

En la pestaña de filtrado de dominios se puede encontrar la configuración del filtrado basado en dominios.

4.11.3. BLOQUEAR DOMINIOS ESPECIFICADOS SÓLO COMO IP.

Esta opción bloquea cualquier página que se intente acceder especificado únicamente su dirección IP y no el dominio asociado.

Bloquear dominios no listados.

Esta opción bloquea todos los dominios que no estén presentes en la sección reglas de dominios o en las categorías presentes en ficheros de listas de dominios y cuya política no sea *ignorar*.

A continuación se tiene la lista de dominios, donde se puede introducir nombres de dominio y seleccionar una política para ellos entre las siguientes:

- **Permitir siempre:**

El acceso a los contenidos del dominio será siempre permitido, todos los filtros son ignorados.

- **Denegar siempre:**

El acceso nunca se permitirá a los contenidos de este dominio.

- **Filtrar:**

Se aplicarán las reglas usuales a este dominio. Resulta útil si está activada la opción bloquear dominios no listados.

4.11.4. FILTRADO DOMINIOS.

Filtrado de extensiones de fichero Filtrado de tipos MIME **Filtrado de dominios para grupo de filtros**

Usar perfil predeterminado para el filtrado de dominios
Usar configuración del perfil predeterminado:
Change

Configuración del filtrado de dominio
Bloquear dominios y URLs no listados:
Si esta opción está habilitada, cualquier dominio que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.
Bloquear sitios especificados sólo como IP:
Change

Reglas de dominios y URLs
[+ Añade nuevo](#)

Buscar

Dominio o URL	Política	Action
miorganizacion.com	Always allow	

10 ▼ Página 1

Ficheros de las listas de dominios para el filtrado de grupo
[+ Añade nuevo](#)

Buscar

Description	Categorías	Fichero	Action
shalla blacklist		shalla_blacklist Download	

10 ▼ Página 1

Figura 4.11.5. Filtrado de dominios en Zentyal.











Fuente: http://doc.zentyal.org/es/_images.

Para simplificar el trabajo del administrador usando listas clasificadas de dominios. Estas listas son normalmente mantenidas por terceros y tienen la ventaja de que los dominios están clasificados por categorías, permitiéndonos seleccionar una política para una categoría entera de dominios. Estas listas son distribuidas en forma de archivo comprimido. Una vez descargado el archivo, se puede incorporar a nuestra configuración y establecer políticas para las distintas categorías de dominios. Las políticas que se pueden establecer en cada categoría son las mismas que se pueden asignar a dominios y se aplican a todos los dominios presentes en dicha categoría. Existe una política adicional *Ignorar* que, como su nombre indica, simplemente ignora

la existencia de la categoría a la hora de filtrar. Dicha política es la elegida por defecto para todas las categorías.

Listado de categorías.

Domains list categories

Category	Policy	Action
adv	Always deny	
aggressive	Always deny	
astronomy	Ignore	
banking	Always allow	
bikes	Ignore	
boats	Ignore	
cars	Ignore	
chat	Always deny	
chemistry	Ignore	
cooking	Ignore	

10 Page 1 of 7

Figura 4.11.6. Filtrado de dominios en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.12. CORTAFUEGOS

4.12.1. CONFIGURACIÓN DE UN CORTAFUEGO CON ZENTYAL.

El modelo de seguridad de Zentyal se basa en intentar proporcionar la máxima seguridad posible en su configuración predeterminada, intentando a la vez minimizar los esfuerzos a realizar tras añadir un nuevo servicio.

Cuando Zentyal actúa de cortafuegos, normalmente se instala entre la red interna y el router conectado a Internet. La interfaz de red que conecta la máquina con el router debe marcarse como externo *en* red, interfaces de red para permitir al cortafuegos establecer unas políticas de filtrado más estrictas para las conexiones procedentes de fuera.

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 eth1 **eth2** eth3

Nombre:

Método:

Externo (WAN): Comprueba si estás usando Zentyal como gateway y este interfaz está conetado a tu router a Internet

Dirección IP:

Máscara de red:

Figura 4.12.1. Configuración cortafuego en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

Interfaz externa

La política para las interfaces externas es denegar todo intento de nueva conexión a Zentyal mientras que para las interfaces internas se deniegan todos los intentos de conexión excepto los que se realizan a servicios definidos por los módulos instalados. Los módulos añaden reglas al cortafuego para permitir estas conexiones, aunque siempre pueden ser modificadas posteriormente por el administrador. Una excepción a esta norma son las conexiones al servidor LDAP, que añaden la regla pero configurada para denegar las conexiones por motivos de seguridad. La configuración predeterminada tanto para la salida de las redes internas como desde del propio servidor es permitir toda clase de conexiones.



Figura 4.12.2. Configuración cortafuego en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

Filtrado de paquetes

La definición de las políticas del cortafuego se hace desde cortafuegos, filtrada de paquetes.

Se pueden definir reglas en 5 diferentes secciones según el flujo de tráfico sobre el que serán aplicadas:

- **Tráfico de redes internas a Zentyal.**

Permitir acceso al servidor de ficheros desde la red local.

- **Tráfico entre redes internas y de redes internas a Internet.**

Restringir el acceso a todo Internet o determinadas direcciones a unas direcciones internas o restringir las comunicaciones entre las subredes internas.

- **Tráfico de Zentyal a redes externas.**

Permitir descargar ficheros por HTTP desde el propio servidor.

- **Tráfico de redes externas a Zentyal.**

Permitir que el servidor de correo reciba mensajes de Internet.

- **Tráfico de redes externas a redes internas.**

Permitir acceso a un servidor interno desde Internet.

Hay que tener en cuenta que los dos últimos tipos de reglas pueden crear un compromiso en la seguridad de Zentyal y la red, por lo que deben utilizarse con sumo cuidado.

Esquema de los diferentes flujos de tráfico en el cortafuego

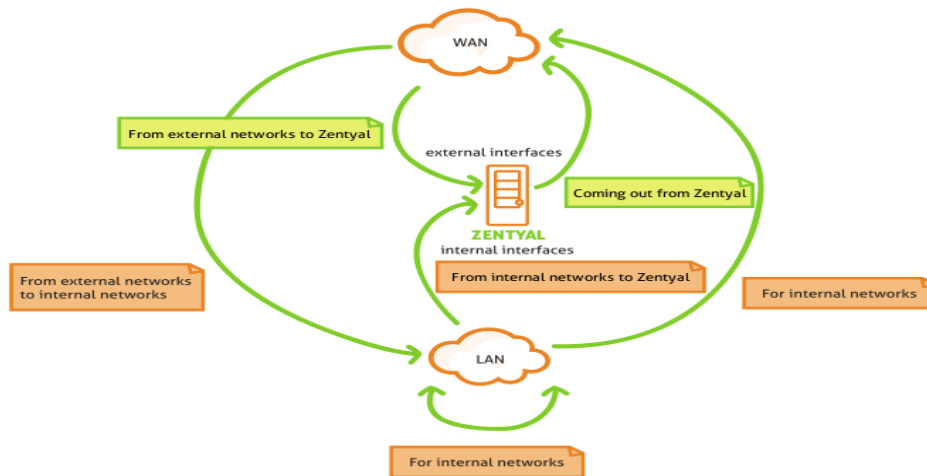


Figura 4.12.3. Cortafuego en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

Zentyal provee una forma sencilla de definir las reglas que conforman la política de un cortafuegos. La definición de estas reglas usa los conceptos de alto nivel introducidos anteriormente: los *Servicios de red* para especificar a qué protocolos y puertos se aplican las reglas y los *Objetos de red* para especificar sobre qué direcciones IP de origen o de destino se aplican.

Lista de reglas de filtrado de paquetes desde las redes internas a Zentyal

Normalmente cada regla tiene un origen y un destino que pueden ser cualquiera, una dirección IP o un objeto en el caso que queramos especificar más de una dirección IP o direcciones MAC. En determinadas secciones el origen o el destino son omitidos ya que su valor es conocido a priori; será siempre Zentyal tanto el destino en tráfico de redes internas a Zentyal y Tráfico de redes externas a Zentyal como el origen en tráfico de Zentyal a redes externas.

Además cada regla siempre tiene asociado un servicio para especificar el protocolo y los puertos (o rango de puertos). Los servicios con puertos de origen son útiles para reglas de tráfico saliente de servicios internos, por ejemplo un servidor HTTP interno,

mientras que los servicios con puertos de destino son útiles para reglas de tráfico entrante a servicios internos o tráfico saliente a servicios externos.

El parámetro de mayor relevancia será la decisión a tomar con las conexiones nuevas. Zentyal permite tomar tres tipos distintos de decisiones:

Aceptar la conexión.

Denegar la conexión ignorando los paquetes entrantes y haciendo suponer al origen que no se ha podido establecer la conexión.

Registrar la conexión como un evento y seguir evaluando el resto de reglas.

Añadiendo una nueva regla

The screenshot shows the configuration form for a new firewall rule in Zentyal. It includes the following fields and options:

- Decisión:** A dropdown menu set to "DENY".
- Origen:** A dropdown menu set to "Cualquiera".
- Destino:** Two dropdown menus, the first set to "Objeto destino" and the second set to "IT".
- Servicio:** A dropdown menu set to "ssh".
- Inverse match:** An unchecked checkbox.
- Descripción:** A text input field containing "No permitir ssh a máquinas de IT".
- Opcional:** A label in blue text below the description field.
- Buttons:** "Añadir" and "Cancelar" buttons at the bottom.

Below the "Inverse match" checkbox, there is a small explanatory text: "Si la selección inversa está marcada, la regla será aplicada cualquier servicio excepto el seleccionado".

Figura 4.12.4. Cortafuego en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.12.2. CREANDO UNA NUEVA REGLA EN EL FIREWALL.

Si se desea registrar las conexiones a un servicio, primero se tiene la regla que registra la conexión y luego la regla que acepta la conexión. Si estas dos reglas están en el orden inverso, no se registrará nada ya que la regla anterior ya acepta la conexión. Igualmente si se desea restringir la salida a Internet, primero explícitamente se tiene que negar los sitios o los clientes y luego para permitir la salida al resto, invertir el orden daría acceso a todos los sitios a todo el mundo.

4.12.3. REDIRECCIÓN DE PUERTOS CON ZENTYAL.

Las redirecciones de puertos de destino se configuran en cortafuegos, redirecciones de puertos.

Para configurar una redirección hay que establecer la interfaz donde se recibe el tráfico sobre el que se va a hacer la traducción, el destino original (que puede ser el servidor Zentyal, una dirección IP o un objeto), el puerto de destino original (que puede ser cualquiera, un puerto determinado o un rango de puertos), el protocolo y el origen (que también puede ser cualquiera, una dirección IP o un objeto).

Además se tiene que establecer la dirección IP de destino y finalmente, el puerto donde la máquina destino recibirá las peticiones, que puede ser el mismo que el original o no. Existe también un campo opcional de descripción para aclarar el propósito de la regla.

Redirecciones de puertos

Añadiendo un/a nuevo/a redirección

Interfaz: eth0

Destino original: Zentyal

Protocolo: TCP

Puerto de destino original: Puerto único 8080

Origen: Cualquiera

IP Destino: 10.10.10.10

Puerto: Otro 80

Reemplazar la dirección de origen:

Reemplaza la dirección de origen inicial de la conexión con la dirección de Zentyal. Esto puede ser necesario cuando el destino no tiene una ruta de retorno o tiene reglas de firewall restrictivas

Registro:

Registrar conexiones redirigidas nuevas

Descripción: Opcional Mi servidor web

Añadir Cancelar

Figura 4.12.5. Redirección de puertos en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

4.13. ZENTYAL GATEWAY.

En este capítulo se describen las funcionalidades de Zentyal como puerta de enlace o gateway. Zentyal puede hacer la red más fiable y segura, gestionar el ancho de banda y definir políticas de conexiones y contenidos.

Hay un apartado centrado en el funcionamiento del módulo de cortafuegos, el cual nos permite definir reglas para gestionar el tráfico entrante y saliente tanto del servidor como de la red interna.

Para ayudar en la configuración del cortafuego, existen dos módulos que facilitan la gestión de objetos y servicios de red.

A la hora de acceder a Internet se tiene que balancear la carga entre varias conexiones y definir diferentes reglas para usar una u otra según el tráfico.

4.13.1 CONFIGURACIÓN DEL ENCAMINAMIENTO CON ZENTYAL

4.13.2. PUERTA DE ENLACE

La puerta de enlace o gateway es el router por omisión para las conexiones cuyo destino no está en la red local. Es decir, si el sistema no tiene definidas rutas estáticas o si ninguna de éstas coincide con una transmisión a realizar, ésta se hará a través de la puerta de enlace.

Para configurar una puerta de enlace en Zentyal se utiliza *red*, puertas de enlace, que tiene los siguientes parámetros configurables.

Añadiendo una nueva puerta de enlace

Habilitado:

Nombre:

Dirección IP:

Interfaz: Interfaz conectada a esta puerta de enlace

Peso: Este campo solo es útil si tiene mas de un router y la función de balanceo de tráfico esta habilitada.

Predeterminado:

Figura 4.13.1. Puerta de enlace en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

- **Habilitado:**
Indica si realmente esta puerta de enlace es efectiva o está desactivada.
- **Nombre:**
Nombre por el que se puede identificar a la puerta de enlace.
- **Dirección IP:**
Dirección IP de la puerta de enlace. Esta dirección debe ser directamente accesible desde la máquina que contiene Zentyal, es decir, sin otros enrutamientos intermedios.
- **Interfaz:**
Interfaz de red conectada a la puerta de enlace. Los paquetes que se envíen a la puerta de enlace se enviarán a través de esta interfaz.
- **Peso**
Cuanto mayor sea el peso, más paquetes se enviarán por esa puerta de enlace si activamos el balanceo de tráfico.
- **Predeterminado**
Si esta opción está activada, esta será la puerta de enlace por defecto.

Puertas de enlace y Proxy [\(mostrar ayuda\)](#)

Lista de Puertas de Enlace

+ Añade nuevo

Habilitado	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Action
<input checked="" type="checkbox"/>	Gateway_Wan	190.95.222.193	eth1	1	<input checked="" type="checkbox"/>	 

10 Página 1

Figura 4.13.2. Puerta de enlace en Zentyal.

Fuente: http://doc.zentyal.org/es/_images.

CAPITULO 5.

5.1. ANALISIS Y PRUEBAS FINALES.

5.2. ANÁLISIS IMPLEMENTACIÓN E INTEGRACIÓN.

Para la implementación del servidor de correo Zimbra Collaboration Suite y Zentyal como servidor de dominio, firewall y proxy se realizó el siguiente diagrama estructural, para detallar como se integrarían estos nuevos servidores según sus sistemas operativos principales físicos como virtuales actuales de la empresa Movidatos.

5.3. SERVIDOR DE VIRTUALIZACIÓN VIRTUALBOX.

- Máquina virtual servidor de correo Zimbra Collaboration Suite.
- Máquina virtual servidor de contabilidad Fenix.
- Máquina virtual servidor Vtiger CRM

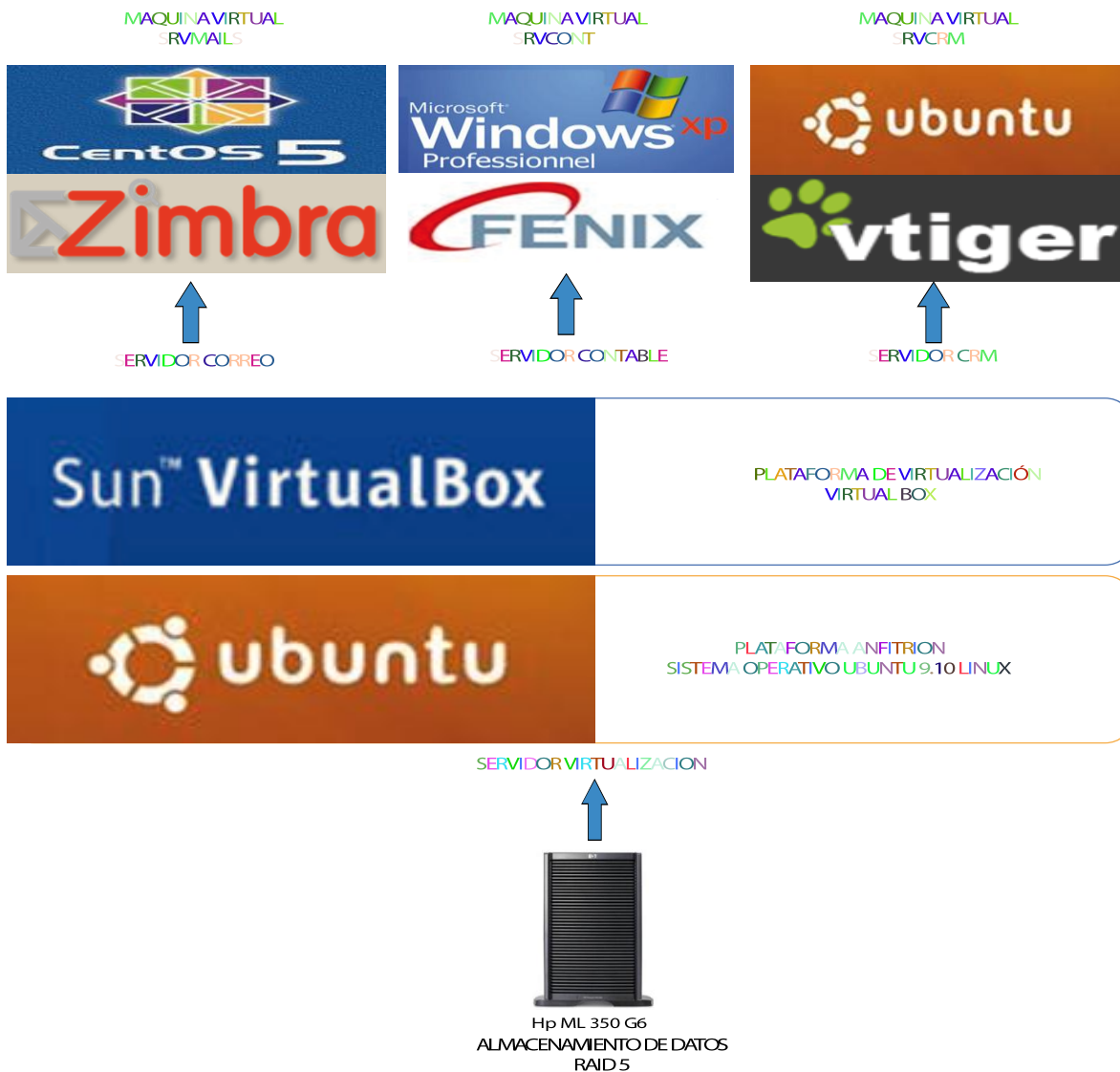


Figura 5.3.1. Plataforma de virtualización con VirtualBox.

Fuente: Autor tesis Henry Padilla.

5.4. SERVIDOR MULTITAREA ZENTYAL.

- Servidor controlador de dominio.
- Servidor proxy
- Servidor firewall
- Servidor de archivos.
- Servidor ftp.

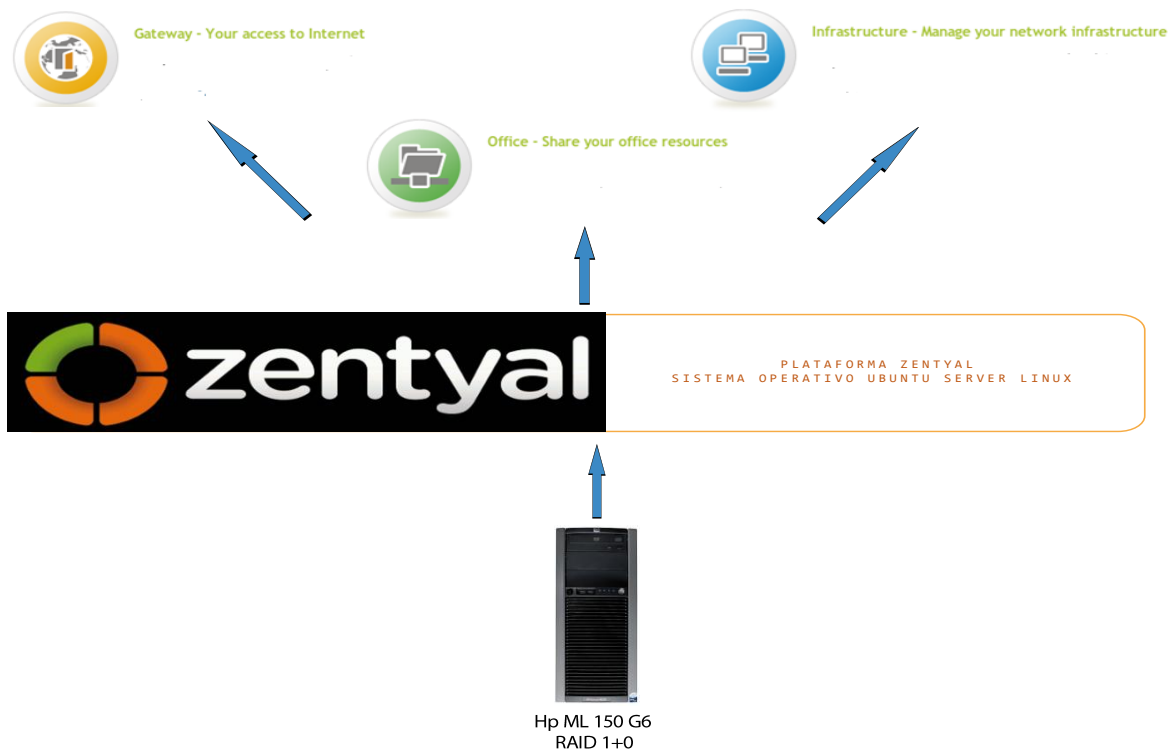


Figura 5.4.1. Plataforma del servidor Zentyal.

Fuente: Autor tesis Henry Padilla.

5.5. ESCENARIO DE PRUEBAS SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE.

Para el escenario de pruebas del servidor de correo Zimbra se realizó las siguientes pruebas.

5.5.1. PRUEBAS DE FUNCIONAMIENTO EN EL SERVIDOR VIRTUALIZACION CON VIRTUALBOX.

5.5.2. MAQUINA VIRTUAL ZIMBRA COLLABORATION SUITE.

Validación de comunicación del servidor Zimbra con el servidor principal de virtualización.

Realizamos un ping desde el servidor de virtualización hacia el servidor de correo Zimbra a nivel interno como externo.

Conectividad Eth0 a nivel interno, realizamos el respectivo ping.

Ping a la Ip a nivel lan asignado para el servidor de correo Zimbra.

```
movidatos@movidatos-desktop:~$ ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=5.20 ms
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=0.357 ms
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.445 ms
64 bytes from 192.168.0.3: icmp_seq=4 ttl=64 time=0.367 ms
64 bytes from 192.168.0.3: icmp_seq=5 ttl=64 time=0.539 ms
64 bytes from 192.168.0.3: icmp_seq=6 ttl=64 time=0.414 ms
64 bytes from 192.168.0.3: icmp_seq=7 ttl=64 time=0.416 ms
64 bytes from 192.168.0.3: icmp_seq=8 ttl=64 time=0.407 ms
64 bytes from 192.168.0.3: icmp_seq=9 ttl=64 time=0.371 ms
```

Figura 5.5.1. Verificación de comunicación a nivel interno de la red.

Fuente: Autor tesis Henry Padilla.

Conectividad Eth1 a nivel externo, realizamos el respectivo ping

Ping a la Ip a nivel wan asignado para el servidor de correo Zimbra.

```
movidatos@movidatos-desktop:~$ ping 190.95.222.195
PING 190.95.222.195 (190.95.222.195) 56(84) bytes of data.
64 bytes from 190.95.222.195: icmp_seq=1 ttl=64 time=9.17 ms
64 bytes from 190.95.222.195: icmp_seq=2 ttl=64 time=0.310 ms
64 bytes from 190.95.222.195: icmp_seq=3 ttl=64 time=0.390 ms
64 bytes from 190.95.222.195: icmp_seq=4 ttl=64 time=0.345 ms
64 bytes from 190.95.222.195: icmp_seq=5 ttl=64 time=0.272 ms
64 bytes from 190.95.222.195: icmp_seq=6 ttl=64 time=0.233 ms
64 bytes from 190.95.222.195: icmp_seq=7 ttl=64 time=0.464 ms
64 bytes from 190.95.222.195: icmp_seq=8 ttl=64 time=0.324 ms
```

Figura 5.5.2. Verificación de comunicación a nivel externo de la red.

Fuente: Autor tesis Henry Padilla.

Realizamos un ping desde el servidor de correo Zimbra hacia el servidor de virtualización a nivel interno como externo.

Conectividad Eth1 a nivel externo, realizamos el respectivo ping

Ping a la Ip a nivel wan asignado para el servidor de correo Zimbra

```
[root@mailserver ~]# ping 190.95.222.196
PING 190.95.222.196 (190.95.222.196) 56(84) bytes of data.
64 bytes from 190.95.222.196: icmp_seq=1 ttl=64 time=0.145 ms
64 bytes from 190.95.222.196: icmp_seq=2 ttl=64 time=0.156 ms
64 bytes from 190.95.222.196: icmp_seq=3 ttl=64 time=4.40 ms
64 bytes from 190.95.222.196: icmp_seq=4 ttl=64 time=0.423 ms
64 bytes from 190.95.222.196: icmp_seq=5 ttl=64 time=0.157 ms
```

Figura 5.5.3. Verificación de comunicación a nivel externo de la red.

Fuente: Autor tesis Henry Padilla.

Conectividad Eth0 a nivel interno, realizamos el respectivo ping.

Ping a la Ip a nivel lan asignado para el servidor de correo Zimbra.

```
[root@mailserver ~]# ping 192.168.0.2
PING 192.168.0.2 (192.168.0.2) 56(84) bytes of data.
64 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=8.37 ms
64 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=0.288 ms
64 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=0.557 ms
64 bytes from 192.168.0.2: icmp_seq=4 ttl=64 time=0.357 ms
■
```

Figura 5.5.4. Verificación de comunicación a nivel interno de la red.

Fuente: Autor tesis Henry Padilla.

Teniendo ya una comprobación de conectividad y repuesta entre la red interna como externa.

5.5.3. REALIZAMOS PRUEBAS DE RESOLUCIÓN DE DOMINIO MOVIDATOS.

Buscar tipos de datos diferentes

Para buscar tipos de datos diferentes dentro del espacio de nombres de dominio, utilice el comando set type en el símbolo del sistema. Por ejemplo, para consultar los datos del intercambiador de correo, escriba lo siguiente:


```

C:\>nslookup

> set q=mx
> movidatos.com
Servidor: ecuio012d02.uio.bpichincha.com
Address: 10.0.0.133

Respuesta no autoritativa:
movidatos.com MX preference = 0, mail exchanger = emailserver.movidatos.com
movidatos.com MX preference = 0, mail exchanger = mailserver.movidatos.com

movidatos.com nameserver = dns2uio.cyberweb.net.ec
movidatos.com nameserver = dns1uio.cyberweb.net.ec
mailserver.movidatos.com internet address = 190.95.222.195
emailserver.movidatos.com internet address = 190.95.222.195
dns1uio.cyberweb.net.ec internet address = 200.24.208.2
dns2uio.cyberweb.net.ec internet address = 200.24.208.1

```

Figura 5.5.5. Resolución de nombres de dominio.

Fuente: Autor tesis Henry Padilla.

Consultar directamente desde otro servidor de nombres

Para consultar directamente otro servidor de nombres, utilice los comandos server o lserver para cambiar a ese servidor de nombres. El comando lserver utiliza el servidor local para obtener la dirección del servidor al que se desea cambiar, mientras que el comando server utiliza el servidor predeterminado actual para obtener la dirección.

```

C:\>nslookup

> server 190.95.222.195
Servidor predeterminado: mailserver.movidatos.com
Address: 190.95.222.195

```

Figura 5.5.6. Resolución de nombres de dominio.

Fuente: Autor tesis Henry Padilla.

Hay muchas otras opciones, si por ejemplo el modo de consulta se lo puede colocar a “any” para que nos de toda la información posible (con “q=any” o “type=any”).

```

> set q=any
> movidatos.com
Servidor: puntonet.ec
Address: 200.105.225.2

Respuesta no autoritativa:
movidatos.com MX preference = 0, mail exchanger = emailserver.movidatos.com
movidatos.com MX preference = 0, mail exchanger = mailserver.movidatos.com
movidatos.com
    primary name server = uio.movidatos.com
    responsible mail addr = nsadm@bellsouth.com.ec
    serial = 2009042103
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 86400 (1 day)
movidatos.com nameserver = dns2uio.cyberweb.net.ec
movidatos.com nameserver = dns1uio.cyberweb.net.ec

movidatos.com nameserver = dns2uio.cyberweb.net.ec
movidatos.com nameserver = dns1uio.cyberweb.net.ec
mailserver.movidatos.com internet address = 190.95.222.195
emailserver.movidatos.com internet address = 190.95.222.195
dns1uio.cyberweb.net.ec internet address = 200.24.208.2
dns2uio.cyberweb.net.ec internet address = 200.24.208.1

```

Figura 5.5.7. Resolución de nombres de dominio.

Fuente: Autor tesis Henry Padilla.

Despliega toda la información posible acerca del dominio movidatos.com

En otras ocasiones la necesidad de saber a qué dominio pertenece cierta IP pública, simplemente con poner la IP el servidor DNS nos hace un DNS inverso:

```

> set type=ptr
> movidatos.com
Servidor: puntonet.ec
Address: 200.105.225.2

movidatos.com
    primary name server = uio.movidatos.com
    responsible mail addr = nsadm@bellsouth.com.ec
    serial = 2009042103
    refresh = 10800 (3 hours)
    retry = 3600 (1 hour)
    expire = 604800 (7 days)
    default TTL = 86400 (1 day)

```

Figura 5.5.8. Resolución de nombres de dominio.

Fuente: Autor tesis Henry Padilla.

Pero esto a veces no funciona o los datos no son fiables (no es lo normal), esto ocurre cuando el propietario de la IP pública no tiene almacenada ninguna información PTR o incluso puede tener información falsa (no es lo normal), pero esta información PTR es un tanto informal y no da la información necesaria en la mayoría de los casos, en el caso que tengamos necesidad de saber desde donde viene (localización) las consultas de determinadas IPs sospechosas o incluso la información del propietario hay una utilidad mucho más potente que usa el protocolo whois.

5.6. REALIZAMOS PRUEBAS EN EL SERVIDOR MULTITAREA ZENTYAL.

Validación de conectividad interna como externa de las tarjetas de red servidor Zentyal.

Conectividad Eth0 a nivel interno, realizamos el respectivo ping.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data:
64 bytes from 192.168.0.5: icmp_seq=1 ttl=64 time=0.061 ms
64 bytes from 192.168.0.5: icmp_seq=2 ttl=64 time=0.057 ms
64 bytes from 192.168.0.5: icmp_seq=3 ttl=64 time=0.060 ms

--- 192.168.0.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 1998ms
rtt min/avg/max/mdev = 0.057/0.059/0.061/0.006 ms
```

Figura 5.6.1. Diagnóstico de red en Zentyal.

Fuente: Autor tesis Henry Padilla.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.  
64 bytes from 192.168.0.3: icmp_seq=1 ttl=64 time=5.04 ms  
64 bytes from 192.168.0.3: icmp_seq=2 ttl=64 time=0.335 ms  
64 bytes from 192.168.0.3: icmp_seq=3 ttl=64 time=0.404 ms  
  
--- 192.168.0.3 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2000ms  
rtt min/avg/max/mdev = 0.335/1.928/5.045/2.204 ms
```

Figura 5.6.2. Diagnóstico de red en Zentyal.

Fuente: Autor tesis Henry Padilla.

Conectividad Eth1 a nivel externo, realizamos el respectivo ping.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
PING 190.95.222.198 (190.95.222.198) 56(84) bytes of data.  
64 bytes from 190.95.222.198: icmp_seq=1 ttl=64 time=0.062 ms  
64 bytes from 190.95.222.198: icmp_seq=2 ttl=64 time=0.057 ms  
64 bytes from 190.95.222.198: icmp_seq=3 ttl=64 time=0.058 ms  
  
--- 190.95.222.198 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 1998ms  
rtt min/avg/max/mdev = 0.057/0.059/0.062/0.002 ms
```

Figura 5.6.3. Diagnóstico de red en Zentyal.

Fuente: Autor tesis Henry Padilla.

Verificación de ruta de conectividad.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
traceroute to 192.168.0.5 (192.168.0.5), 30 hops max, 60 byte packets
 1  192.168.0.5  0.067 ms  0.014 ms  0.013 ms
```

Figura 5.6.4. Traceroute en Zentyal.

Fuente: Autor tesis Henry Padilla.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
traceroute to 190.95.222.198 (190.95.222.198), 30 hops max, 60 byte packets
 1  190.95.222.198  0.067 ms  0.013 ms  0.013 ms
```

Figura 5.6.5. Traceroute en Zentyal.

Fuente: Autor tesis Henry Padilla.

5.6.1. REALIZAMOS PRUEBAS DE LOS TRES SERVICIOS IMPLEMENTADOS

- Controlador de dominio.
- Firewall.
- Proxy.

5.6.2. PRUEBAS EN EL CONTROLADOR DE DOMINIO INTEGRADO E IMPLEMENTADO.

Herramientas de Diagnóstico de Red

Ping

Máquina:

Traceroute

Máquina:

Resolución de Nombre de Dominio

Nombre de dominio:

Salida

```
; <<>> DiG 9.7.0-Pl <<>> +time=3 movidatos.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 21988
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;movidatos.com.                IN      A

;; AUTHORITY SECTION:
movidatos.com.                10800  IN      SOA     uio.movidatos.com. nsadm@bellsouth.com.ec. 2009042103 10800 3600 10800 0

;; Query time: 3 msec
;; SERVER: 200.93.216.2#53(200.93.216.2)
;; WHEN: Sat Feb 11 15:38:53 2012
;; MSG SIZE rcvd: 93
```

Figura 5.6.6. Resolución de dominios en Zentyal.

Fuente: Autor tesis Henry Padilla.

Registrando los equipos al dominio de Movidatos.

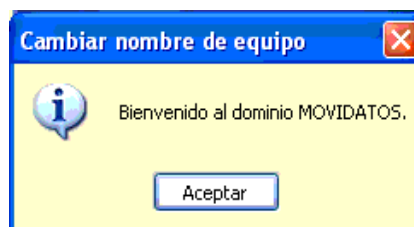
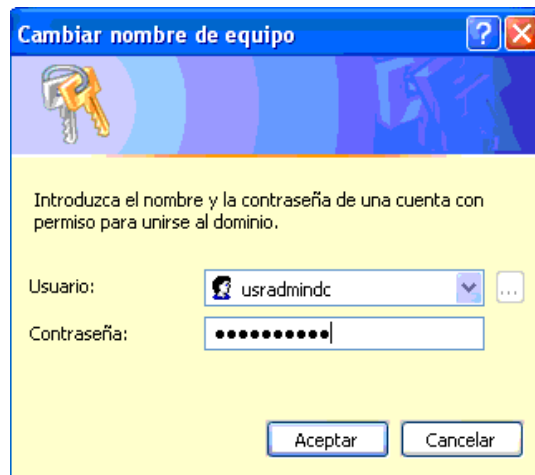
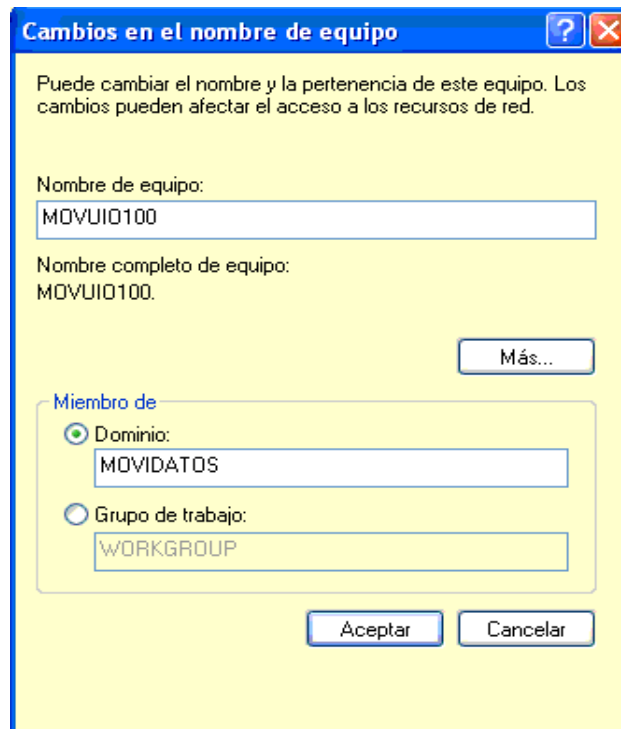


Figura 5.6.7. Ingreso equipos al dominio de Movidatos
Fuente: Autor tesis Henry Padilla.

Ingresando al dominio Movidatos.

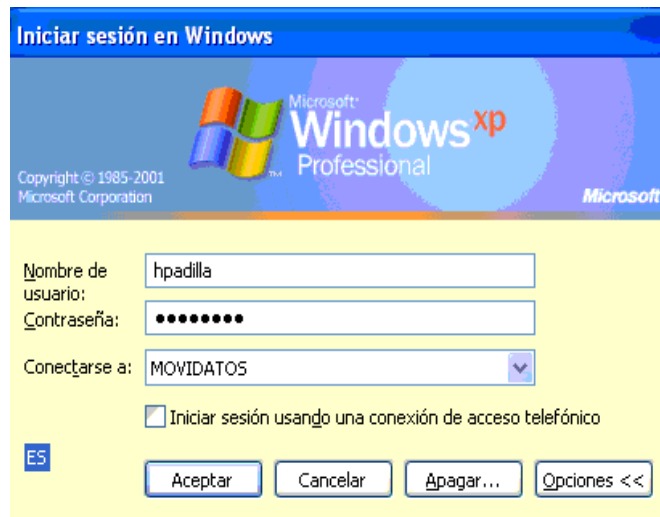


Figura 5.6.8. Ingreso equipos al dominio de Movidatos

Fuente: Autor tesis Henry Padilla.

5.6.3. PRUEBAS EN EL PROXY INTEGRADO E IMPLEMENTADO.

Objetos de red creados para configurar el acceso como bloqueo de páginas web para cada área de la empresa Movidatos.

Objeto_Proxy_Grupo_Administrativo
Objeto_Proxy_Grupo_Contabilidad
Objeto_Proxy_Grupo_Gerencia
Objeto_Proxy_Grupo_RRHH
Objeto_Proxy_Grupo_Recepcion
Objeto_Proxy_Grupo_Sistemas
Objeto_Proxy_Grupo_Svc
Objeto_Proxy_Grupo_Ventas_Guayaquil
Objeto_Proxy_Grupo_Ventas_Quito

Figura 5.6.9. Objetos de red Zentyal para Movidatos

Fuente: Autor tesis Henry Padilla.

Grupo de filtrado de dominios como urls para configurar el acceso como el bloqueo de páginas web según su dominio o url por área o por usuario según la necesidad de la empresa.

Filtrado_Grupo_Gerencia
Filtrado_Grupo_Recepcion
Filtrado_Grupo_Invitado
Filtrado_Grupo_Administrativo
Filtrado_Grupo_Ventas
Filtrado_Grupo_Contabilidad
Filtrado_Grupo_Sistemas
Filtrado_Grupo_Svc

Figura 5.6.10. Objetos de red Zentyal para Movidatos

Fuente: Autor tesis Henry Padilla.

Resultado final cuando el proxy del servidor Zentyal actúa con las funciones de proxy para el bloqueo de páginas web.

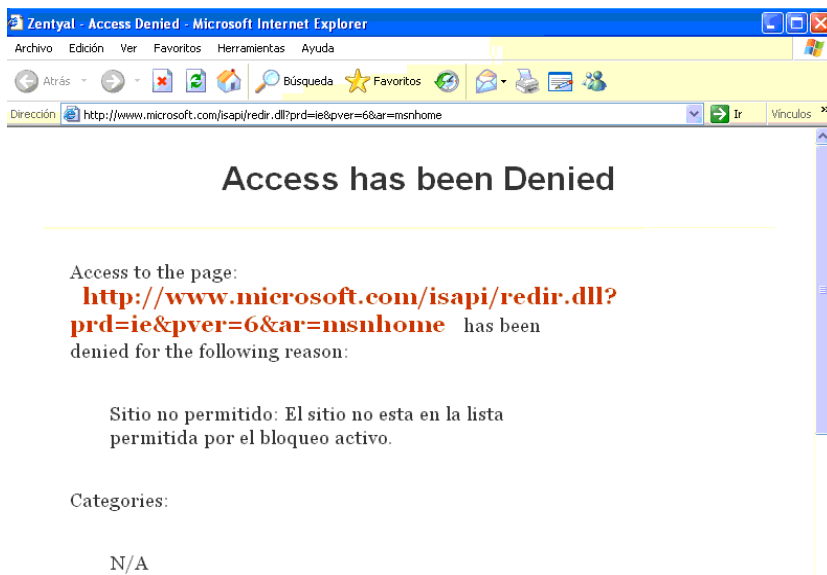


Figura 5.6.11. Funcionalidad bloqueo proxy.

Fuente: Autor tesis Henry Padilla.

5.6.4. PRUEBAS EN EL FIREWALL INTEGRADO E IMPLEMENTADO.

Redirección de puertos en el firewall.



Nombre									
Objeto_Acceso_Usrssh									
Interfaz	Destino original	Puerto de destino original	Protocolo	Origen	IP Destino	Puerto	Registrar	Descripción	Action
eth0	192.168.0.4/32	22	TCP/UDP	192.168.0.1/32	192.168.0.4	Mismo	<input checked="" type="checkbox"/>	Conexion usuario ssh SRVCONT	 

Figura 5.6.12. Funcionalidad del cortafuego en zentyal.

Fuente: Autor tesis Henry Padilla.

Control de acceso desde la red interna hacia aplicaciones como servicios como externos que utilizan internet.

Los objetos de red a configurar son los siguientes en los cuales vamos a registrar las direcciones Ips como puertos que vamos a utilizar para conexión desde el servidor Zentyal para utilizar los servicios previamente configurados utilizando la red interna como externa según las reglas a configurar.

Servicios [\(mostrar ayuda\)](#)

Lista de servicios

[+ Añade nuevo](#)



















<input type="text"/> <input type="button" value="Buscar"/>				
Nombre del servicio	Descripción	Interno	Configuración	Action
FTP	Zentyal FTP Server	<input checked="" type="checkbox"/>		 
Mail system	Zentyal Mail System	<input checked="" type="checkbox"/>		 
ManageSieve	protocol for editing SIEVE filters	<input checked="" type="checkbox"/>		 
Messenger Gmail	Mail Messenger Externo Gmail	<input type="checkbox"/>		 
Messenger Hotmail	Mail Messenger Externo Hotmail	<input type="checkbox"/>		 
Messenger Yahoo	Messenger Externo Yahoo	<input type="checkbox"/>		 

Figura 6.4.30. Configuración de servicios en Zentyal.

Fuente: Autor tesis Henry Padilla.

Servicios > Messenger Gmail

Configuración de servicio

+ Añade nuevo

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	443
TCP/UDP	cualquiera	5222

Figura 6.4.31. Configuración de puertos de Messenger Gmail.

Fuente: Autor tesis Henry Padilla.

Servicios > Messenger Hotmail

Configuración de servicio

+ Añade nuevo

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	1503
TCP/UDP	cualquiera	5004:65535
TCP/UDP	cualquiera	1863
TCP/UDP	cualquiera	3389
TCP/UDP	cualquiera	6901

Figura 6.4.32. Configuración de puertos de Messenger Hotmail.

Fuente: Autor tesis Henry Padilla.

Configuración de servicio

+ [Añade nuevo](#)

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	5001
TCP/UDP	cualquiera	5000
TCP/UDP	cualquiera	5055

Figura 6.4.33. Configuración de puertos de Messenger Yahoo.

Fuente: Autor tesis Henry Padilla.

Decisión	Origen	Destino	Servicio
✘	Objeto_grupo_Sistemas	Cualquiera	Messenger Hotmail
✘	Objeto_grupo_Sistemas	Cualquiera	Messenger Gmail
✘	Objeto_grupo_Sistemas	Objeto_Bloqueo_Correos_Externos	any
✘	Objeto_grupo_Sistemas	Objeto_Bloqueo_Messenger_Externo	any
✘	Objeto_grupo_Ventas_Quito	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Ventas_Guayaquil	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Svc	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Recepcion	Objeto_Bloqueo_Messenger_Externo	any TCP

Figura 5.6.13. Control de acceso a messengers externos.

Fuente: Autor tesis Henry Padilla.

El objeto de red de nombre Objeto_Bloqueo_Messenger_externo lo puede utilizar para registrar los puertos que utiliza el Messenger externo para funcionar y así poder bloquear el acceso a los respectivos usuarios que no deberían tener acceso a estos servicios por internet por resolución de políticas de seguridad de la empresa.

Reglas de filtrado desde las redes externas a Zentyal

Estas reglas te permiten controlar el acceso desde redes externas a servicios que corren en tu máquina Zentyal.



Debes saber que añadiendo reglas a esta sección puedes estar comprometiendo la seguridad de tu red, permitiendo el acceso desde redes no confiables. Por favor, hazlo sólo si sabes lo que estás haciendo.

[Configurar reglas](#)

Reglas de filtrado desde las redes externas a las internas

Estas reglas te permiten controlar el acceso desde redes externas a redes internas



Debes saber que añadiendo reglas a esta sección puedes estar comprometiendo la seguridad de tu red, permitiendo el acceso desde redes no confiables. Por favor, hazlo sólo si sabes lo que estás haciendo.

Figura 5.6.14. Reglas de firewall en Zentyal.

Fuente: Autor tesis Henry Padilla.

CAPÍTULO 6.

6.1. COLOCACIÓN EN PRODUCCIÓN Y EVALUACIÓN FINAL.

Finalizado la revisión de configuraciones en el servidor principal de virtualización, servidor de correo virtual Zimbra Collaboration Suite, servidor multitarea Zentyal y realizado las pruebas correspondientes a nivel de red, hardware, software como aplicación instalada.

Verificamos la estructura de la implementación integrada en la infraestructura de la Empresa Movidatos mediante los siguientes diagramas.

6.1.1. DIAGRAMA DE LA ESTRUCTURA DE RED.

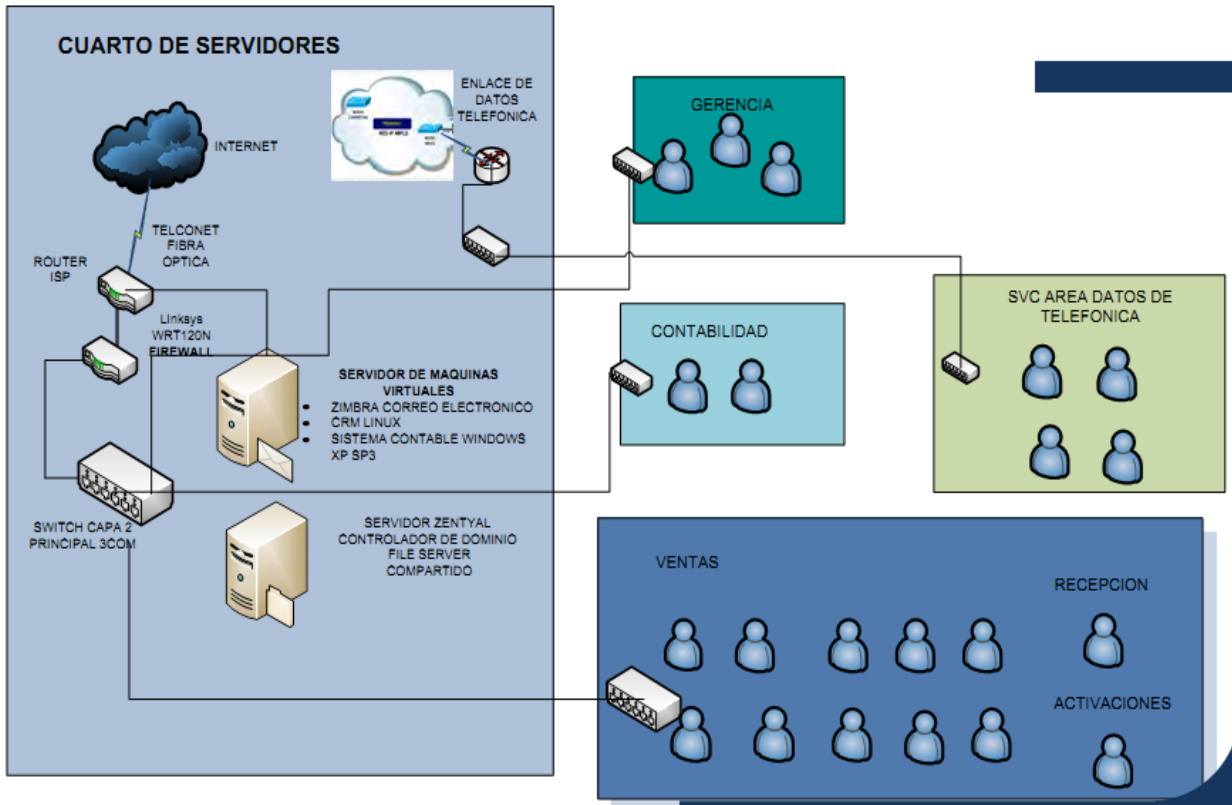


Figura 6.1.1. Estructura de red Empresa Movidatos..

Fuente: Autor tesis Henry Padilla.

6.1.2. DIAGRAMA DE LA IMPLEMENTACIÓN DE NUEVOS SERVIDORES A LA INFRAESTRUCTURA ACTUAL.

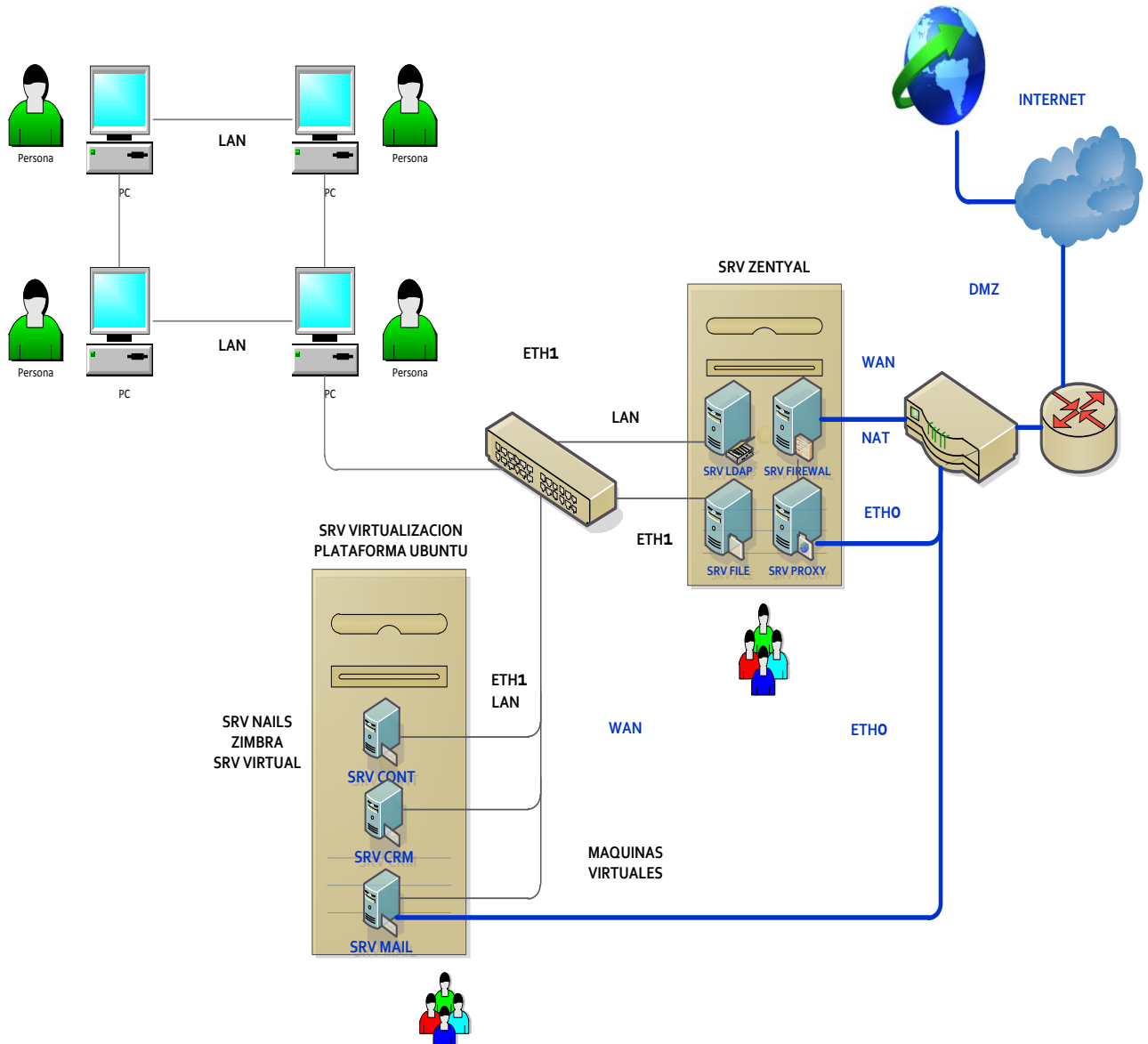


Figura 6.1.2. Implementación nueva infraestructura de Empresa Movidatos.

Fuente: Autor tesis Henry Padilla.

6.1.3. DIAGRAMA DE LA INTEGRACIÓN DE LOS NUEVOS SERVIDORES A LA INFRAESTRUCTURA.

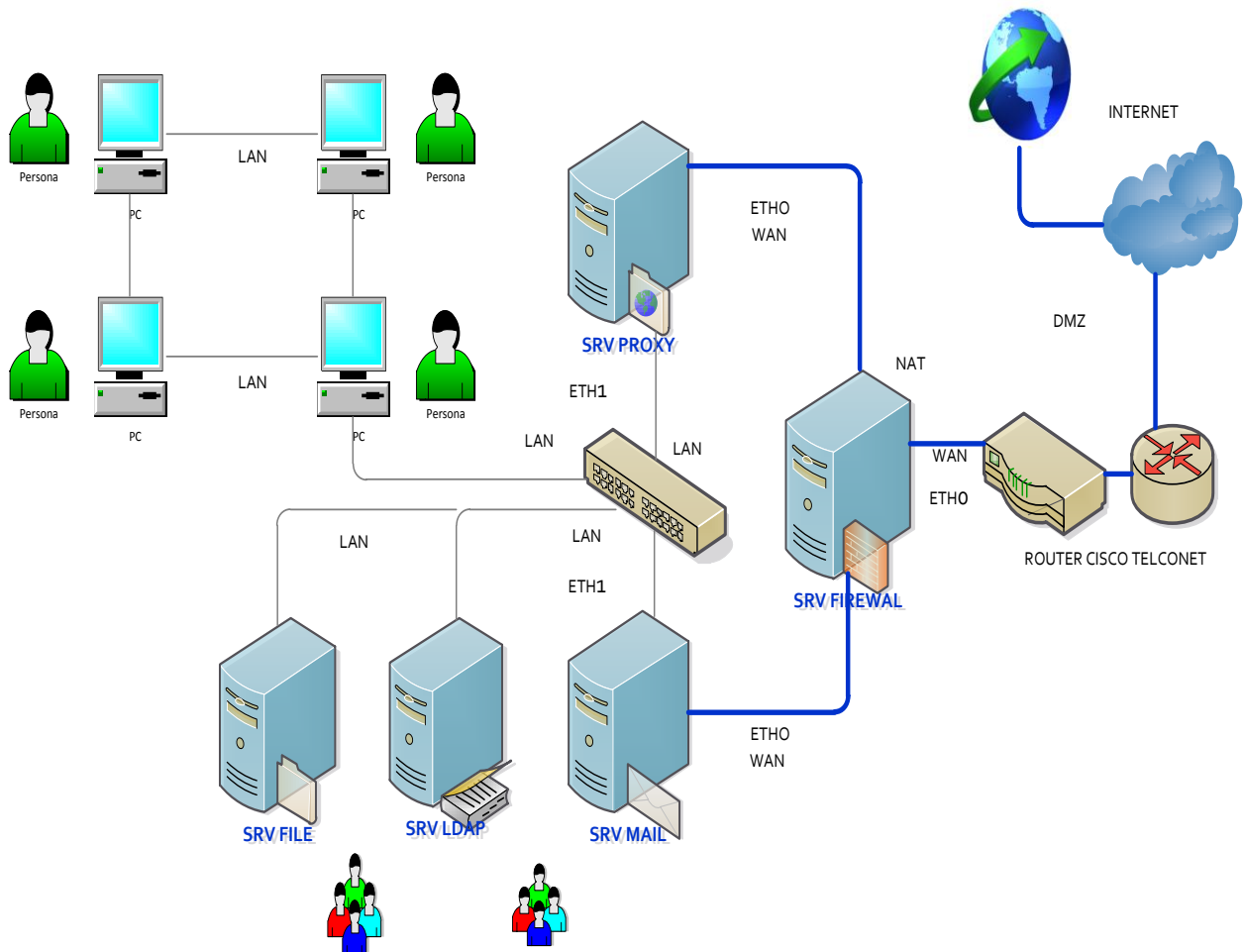


Figura 6.1.3. Implementación nueva infraestructura de Empresa Movidatos.

Fuente: Autor tesis Henry Padilla.

6.1.4. DIAGRAMA DE COLOCACIÓN EN PRODUCCIÓN DE LOS NUEVOS SERVIDORES A LA INFRAESTRUCTURA ACTUAL.

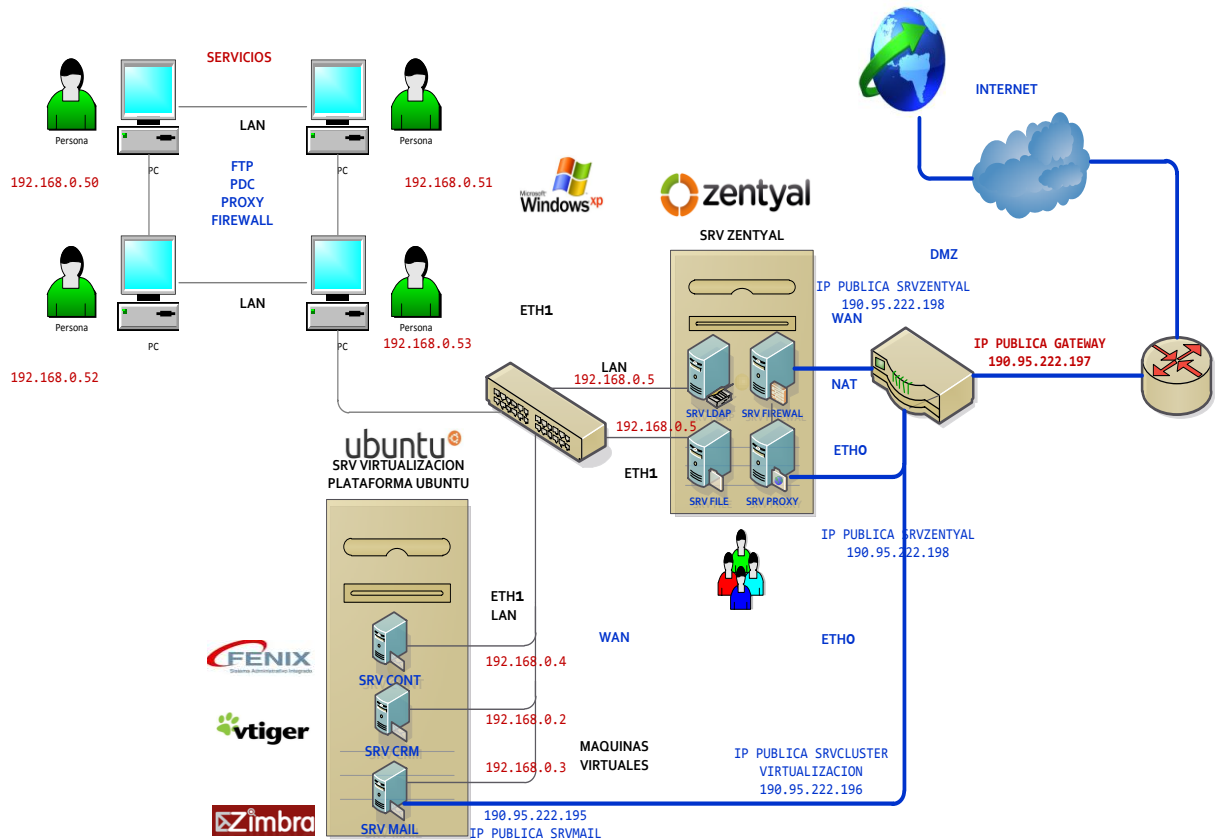
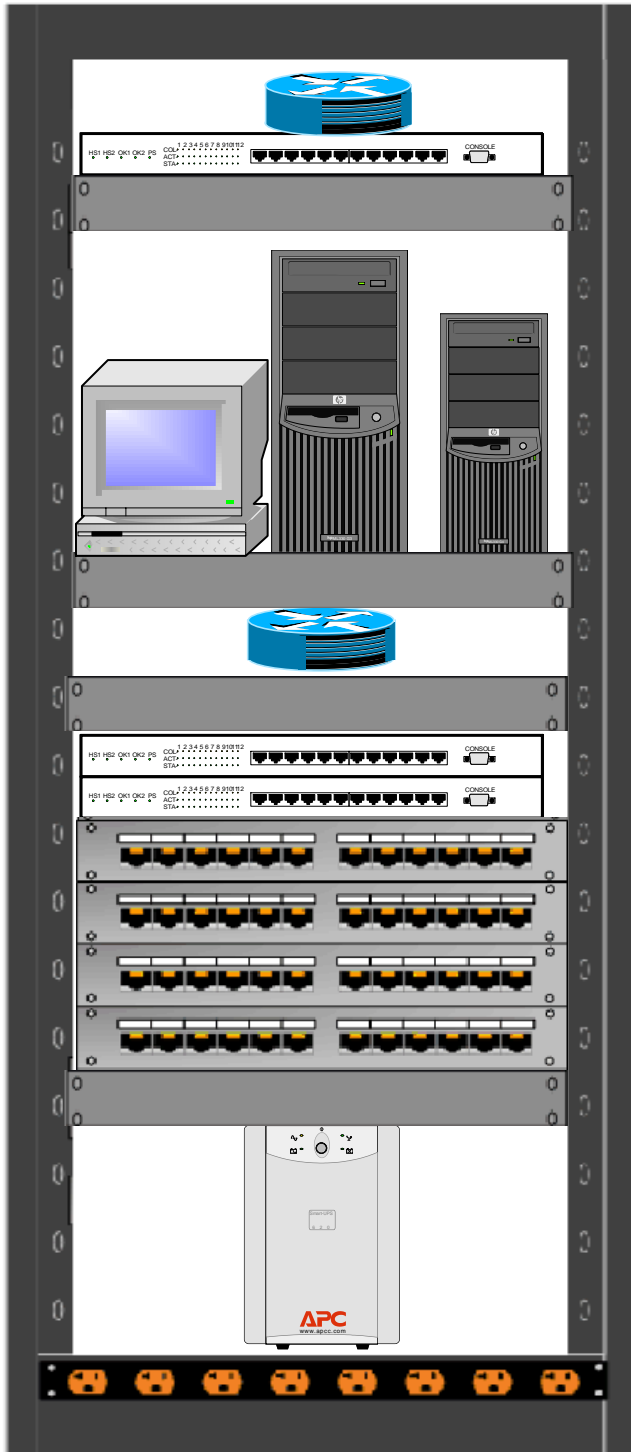


Figura 6.1.4. Implementación nueva infraestructura de Empresa Movidatos.

Fuente: Autor tesis Henry Padilla.



Router Cisco Telefonica

Servidor Zimbra

Servidor Zentyal

Router Cisco Telnet

Switch 3com conexión datos/internet

Panel conexiones

Ups

Conexiones electricas

Figura 6.1.5. Armario servidores.

Fuente: Autor tesis Henry Padilla.

6.2. COLOCACIÓN EN PRODUCCIÓN SERVIDOR DE VIRTUALIZACIÓN DEDICADO CON VIRTUALBOX.

6.2.1. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR EN PRODUCCIÓN.

Histórico del comportamiento del procesamiento, memoria como la red en el servidor.

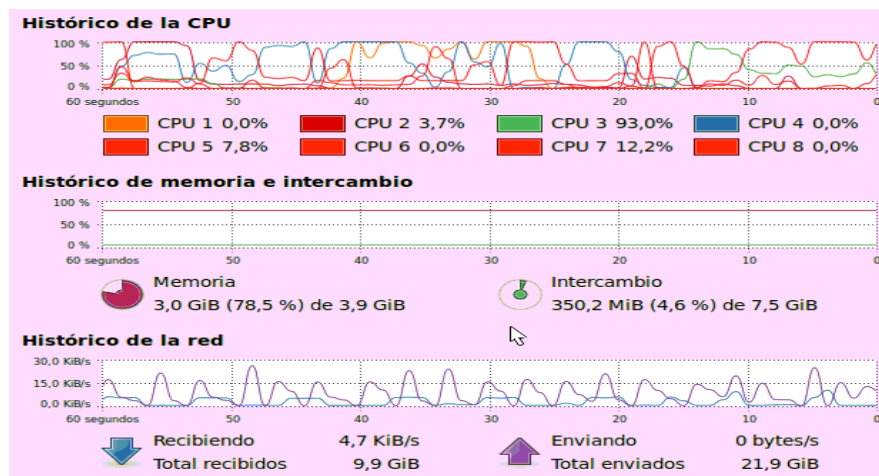


Figura 6.2.1. Comportamiento servidores.

Fuente: Autor tesis Henry Padilla.

Información de las diferentes particiones realizadas en el servidor y el espacio disponible en cada una de ellas.

Sistemas de archivos				
Dispositivo	Directorio	Tipo	Total	Libre
/dev/cciss/c0d0p7	/	ext4	18,3 GiB	15,9 GiB
/dev/cciss/c0d0p1	/boot	xfs	473,8 MiB	437,9 MiB
/dev/cciss/c0d0p9	/home	ext4	80,9 GiB	11,3 GiB
/dev/cciss/c0d1p1	/media/Respaldos Movida	ext4	134,5 GiB	39,2 GiB
/dev/cciss/c0d0p6	/tmp	ext4	9,2 GiB	3,2 GiB
/dev/cciss/c0d0p5	/var	ext4	18,3 GiB	17,9 GiB

Figura 6.2.1. Sistema de archivos.

Fuente: Autor tesis Henry Padilla.

Directorio	Tipo	Total	Libre	Disponible	Usada	
/	ext4	18,3 GiB	15,9 GiB	15,0 GiB	2,4 GiB	14 %
/boot	xfst	473,8 MiB	437,9 MiB	437,9 MiB	35,9 MiB	7 %
/home	ext4	80,9 GiB	11,3 GiB	7,2 GiB	69,6 GiB	90 %
/media/Respaldos Movida	ext4	134,5 GiB	39,2 GiB	32,4 GiB	95,4 GiB	74 %
/tmp	ext4	9,2 GiB	3,2 GiB	2,7 GiB	6,0 GiB	68 %
/var	ext4	18,3 GiB	17,9 GiB	17,0 GiB	427,2 MiB	2 %

Figura 6.2.2. Sistema de archivos.

Fuente: Autor tesis Henry Padilla.

Información de las máquinas virtuales que se encuentran en producción y las que están en pruebas de post producción.

En esta imagen se puede encontrar la nomenclatura de las máquinas virtuales correspondiente a los servidores y equipos virtuales.



Figura 6.2.3. Servidores como máquinas virtuales en VirtualBox.

Fuente: Autor tesis Henry Padilla.

6.3. COLOCACIÓN EN PRODUCCIÓN SERVIDOR VIRTUAL DE CORREO ZIMBRA COLLABORATION SUITE

6.3.1. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR EN PRODUCCIÓN.

En la consola de administración de Zimbra Collaboration Suite ingresando como administrador se puede verificar el estado de cada uno de los servicios que forman parte del servidor de correo los mismos se pueden revisar en la siguiente imagen.

Servidor	Servicio	Hora
mailserver.movidatos.com ▼ ✓	✓ stats	21 de Feb 2012 11:24 (datos antiguos)
	✓ spell	21 de Feb 2012 11:24 (datos antiguos)
	✓ snmp	21 de Feb 2012 11:24 (datos antiguos)
	✓ mta	21 de Feb 2012 11:24 (datos antiguos)
	✓ mailbox	21 de Feb 2012 11:24 (datos antiguos)
	✓ logger	21 de Feb 2012 11:24 (datos antiguos)
	✓ ldap	21 de Feb 2012 11:24 (datos antiguos)
	✓ antivirus	21 de Feb 2012 11:24 (datos antiguos)
	✓ antispam	21 de Feb 2012 11:24 (datos antiguos)

Figura 6.3.1. Estado servicios servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

En la consola de administración están definidas las siguientes funciones para cada una de las cuentas de usuario para su funcionamiento.

Funciones destacadas

- Correo
- Libreta de direcciones
- Agenda
- Tareas
- Bloc de notas
- Maletín
- Messenger
- Preferencias

Funciones generales

- Etiquetado
- Compartir
- Cambiar contraseña
- Cambiar temas de la interfaz
- Redactar en HTML
- Los alias de las teclas rápidas
- Acceso a la Libreta de direcciones
- Autocompletado desde GAL

Funciones de correo

- Prioridad del mensaje
- Marcado
- Acceso IMAP
- Acceso POP3
- Acceso externo IMAP
- Acceso POP externo
- Permitir al usuario especificar una dirección de reenvío

Funciones de la agenda

- Agenda del grupo

Funciones de mensajería instantánea

- Alertas

Funciones de búsqueda

- Búsqueda avanzada
- Búsquedas guardadas
- Preferencia de búsqueda inicial

Figura 6.3.2. Opciones de configuración cuentas de correo.

Fuente: Autor tesis Henry Padilla.

Cada una de las funciones configuradas en la consola de administración del servidor interactúa con los siguientes servicios para su funcionamiento.



Figura 6.3.3. Servicios activados Zimbra.

Fuente: Autor tesis Henry Padilla.

Ya colocado el servidor en producción en la consola de administración se puede verificar los siguientes parámetros de forma gráfica.

El número de mensajes según el número de cuentas creadas en el servidor por un tiempo de 48 horas, 30 días, como 60 días y así verificar el trabajo del servidor para realizar una análisis de rendimiento en memoria como en procesamiento.

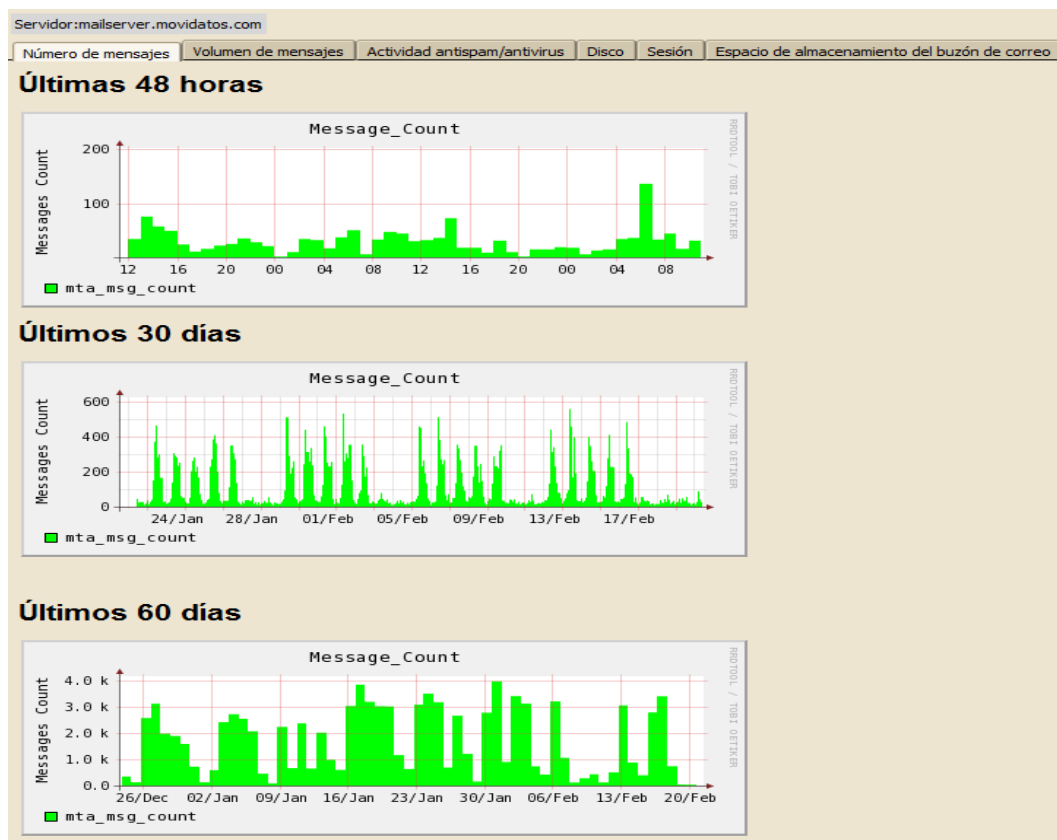


Figura 6.3.4. Estadísticas número de mensajes en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

El volumen de los mensajes según los destinatarios ya sea por el tamaño del mensaje o el número de personas que reciben el mismo mensaje se puede verificar de forma gráfica el volumen de los mismo en un tiempo de 40 horas, 30 días, como 60 días para realizar un análisis de cantidad de mails que se envía su tamaño y el número de destinatarios.

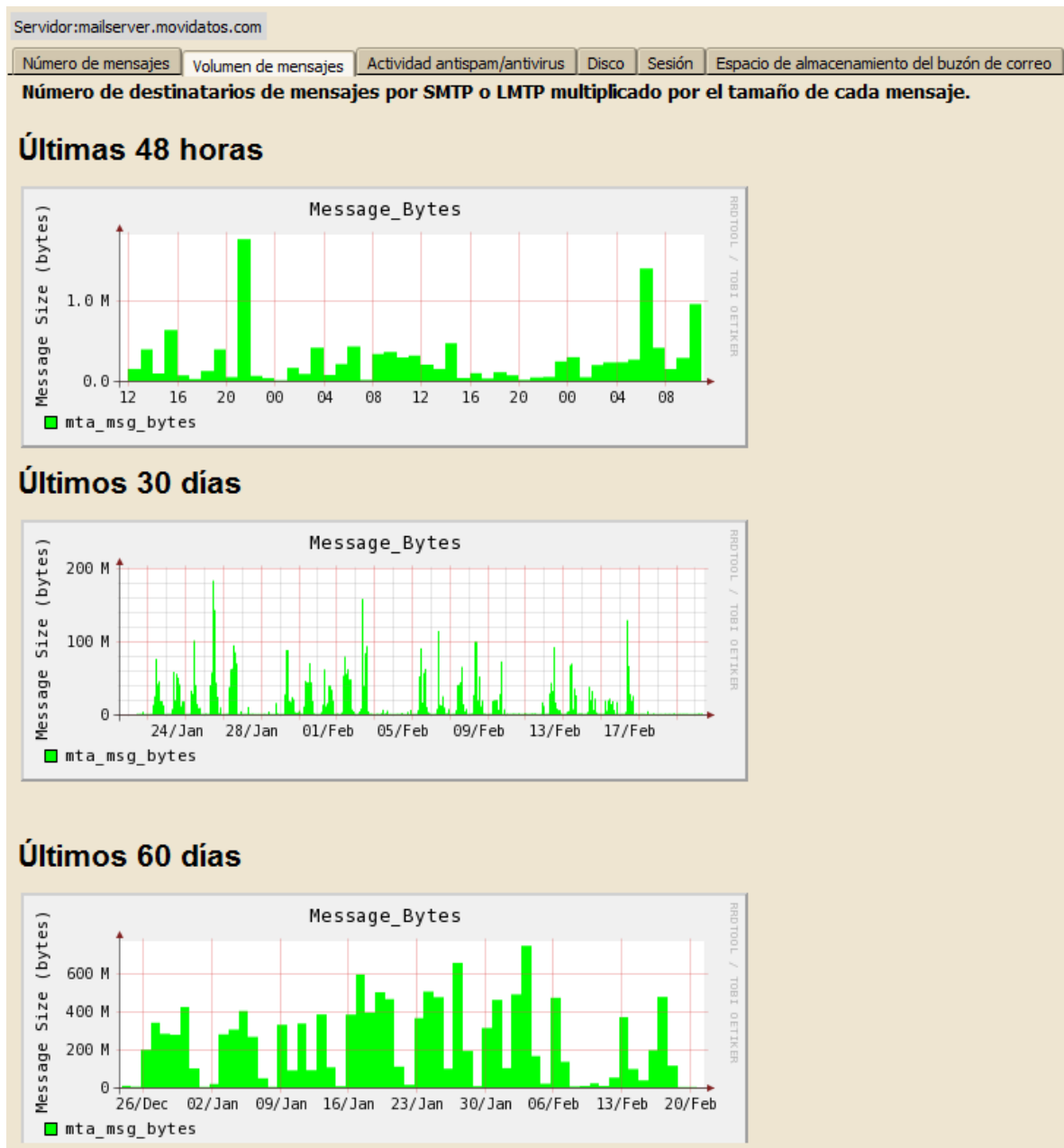


Figura 6.3.5. Estadísticas volumen de mensajes en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

En el proceso de envío y recepción de mails existe un servicio de actividad de antispam como antivirus los cuales interactúan para controlar que cada uno de los correos que se envían como los que se reciben no tengan el riesgo de contraer un virus como provocar spam y que el dominio de Movidatos pueda caer en listar negras por estar enviando y recibiendo correos infectados.

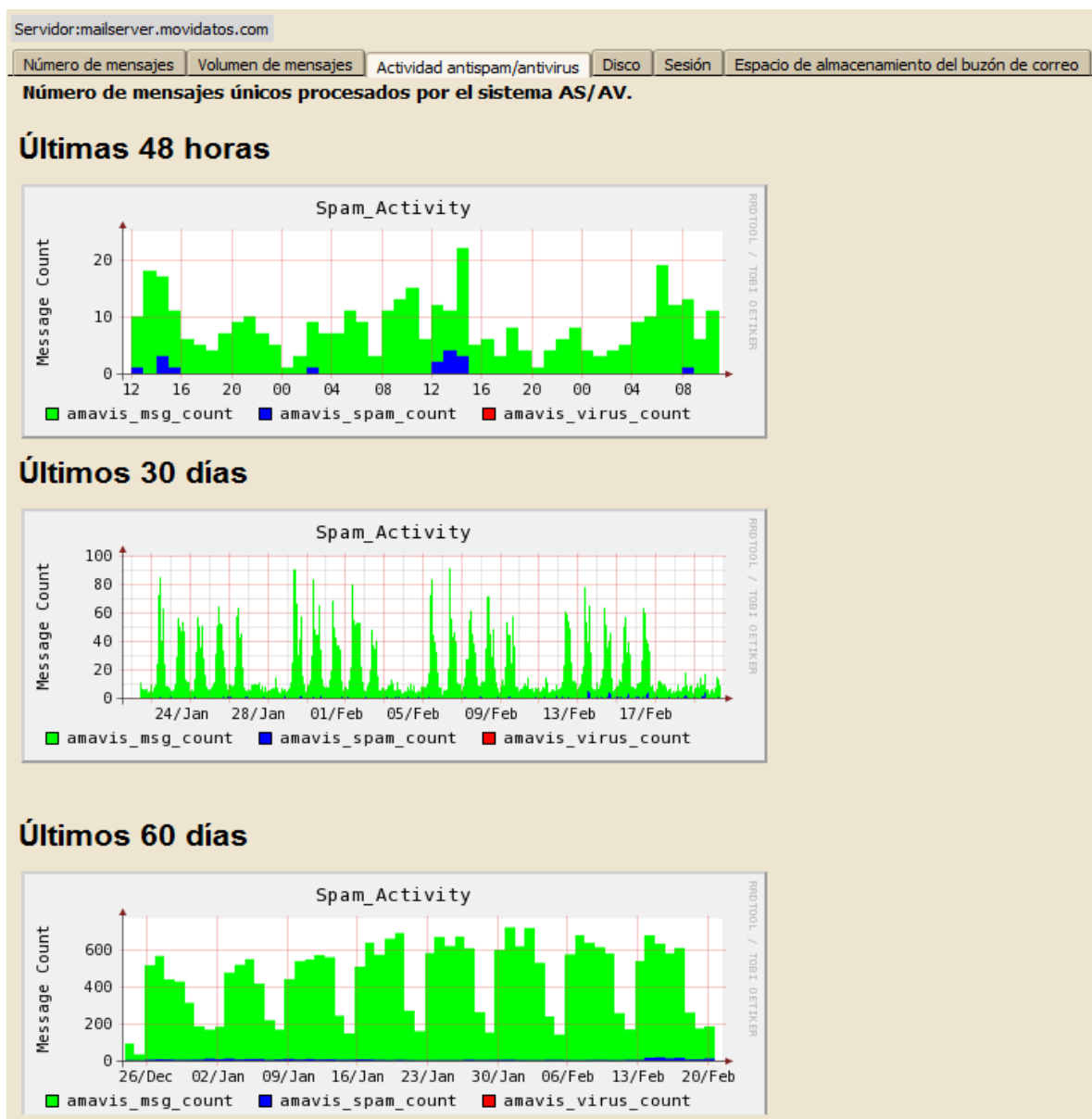


Figura 6.3.6. Estadísticas niveles de spam en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

Según los detalles de mails enviados como recibidos en el volumen de mails según la estadística grafica se puede revisar la gráfica del crecimiento del disco en el último mes.

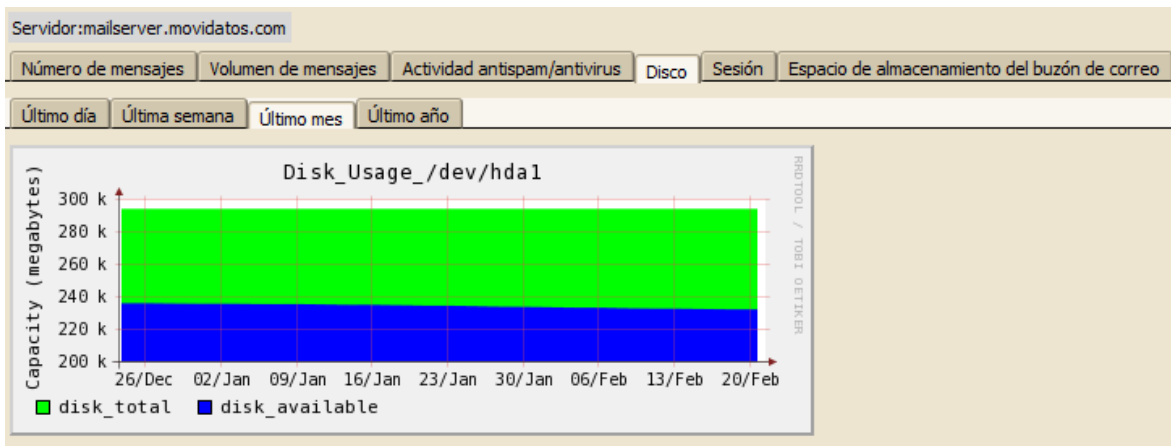


Figura 6.3.7. Estadísticas disco en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

En la consola de administración se puede revisar el número de sesiones mediante aplicación web, secciones de administrador como sesiones IMAP.

Server: mailserver.movidatos.com

Navigation: Número de mensajes | Volumen de mensajes | Actividad antispam/antivirus | Disco | Sesión | Espacio de almacenamiento del buzón de correo

Número total de sesiones activas: 9

Filters: Sesiones de la aplicación web (0) | Sesiones del administrador (1) | Sesiones IMAP (8)

Nombre de cuenta	ID de sesión	Fecha de creación	Hora de último inicio de sesión
andres.lopez@movidatos.com	242572	02/19/2012 02:13:37	02/21/2012 11:41:41
cristian.fallos@movidatos.com	237528	02/14/2012 15:22:31	02/21/2012 11:42:36
david.paschoa@movidatos.cc	237526	02/14/2012 15:21:01	02/21/2012 11:39:15
gabriela.ante@movidatos.com	242570	02/19/2012 02:13:37	02/21/2012 11:41:44
gabriela.teran@movidatos.com	242571	02/19/2012 02:13:37	02/21/2012 11:41:45
maria.gomez@movidatos.com	242008	02/18/2012 07:58:23	02/21/2012 11:42:36
pablo.ruiz@movidatos.com	243679	02/20/2012 13:01:19	02/21/2012 11:39:59
renato.teran@movidatos.com	242569	02/19/2012 02:13:37	02/21/2012 11:41:42

Figura 6.3.8. Sesiones IMAP en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

Tipo	Dirección de correo	Nombre mostrado	Estado	Hora de último inicio de sesión	Descripción
	administrativo@movidatos.com	Administrativos Movidatos	Puede recibir correo	No se inició sesión	Grupo Administrativos Movidatos
	callcenter@movidatos.com	CallCenter Movidatos	Puede recibir correo	No se inició sesión	Grupo CallCenter Movidatos
	gerentes@movidatos.com	Gerente Movidatos	Puede recibir correo	No se inició sesión	Grupo Gerentes Movidatos
	servicioalcliente@movidatos.com	Servicio al Cliente Movidatos	Puede recibir correo	No se inició sesión	Grupo Servicio al Cliente Movidatos
	ventas@movidatos.com	Ventas Movidatos	Puede recibir correo	No se inició sesión	Grupo Ventas Movidatos

Tipo	Nombre	Nombre mostrado	Estado	Hora de último inicio de sesión	Descripción
	admin@movidatos.com		Activo	02/21/2012 11:24:38	
	henry.padilla@movidatos.com	Henry Padilla	Activo	02/14/2012 12:27:54	

Figura 6.3.9. Sesiones IMAP en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

Para el funcionamiento de cada uno de los servicios que utiliza Zimbra Collaboration Suite se tiene que tener un certificado de vigencia de funcionamiento el cual se procede a renovar cada año.

Nombre del servidor: mailserver.movidatos.com

Certificado para el servicio de Zimbra ldap:

Asunto: /C=US/ST=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Emisor: /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Días de validación: Jan 14 17:29:35 2012 GMT - Jan 13 17:29:35 2013 GMT
Nombre alternativo de asunto:

Certificado para el servicio de Zimbra mailboxd:

Asunto: /C=US/ST=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Emisor: /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Días de validación: Jan 14 17:29:35 2012 GMT - Jan 13 17:29:35 2013 GMT
Nombre alternativo de asunto:

Certificado para el servicio de Zimbra mta:

Asunto: /C=US/ST=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Emisor: /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Días de validación: Jan 14 17:29:35 2012 GMT - Jan 13 17:29:35 2013 GMT
Nombre alternativo de asunto:

Certificado para el servicio de Zimbra proxy:

Asunto: /C=US/ST=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Emisor: /C=US/ST=N/A/L=N/A/O=Zimbra Collaboration Suite/OU=Zimbra Collaboration Suite/CN=mailserver.movidatos.com
Días de validación: Jan 14 17:29:35 2012 GMT - Jan 13 17:29:35 2013 GMT
Nombre alternativo de asunto:

Figura 6.3.10. Certificado digital en el servidor Zimbra.

Fuente: Autor tesis Henry Padilla.

6.4. COLOCACIÓN EN PRODUCCIÓN EL SERVIDOR FISICO MULTITAREA ZENTYAL.

Para el monitoreo del servidor multitarea Zentyal en producción se tiene un panel principal en el cual se puede revisar las siguientes características de su funcionamiento.

6.4.1. INFORMACIÓN GENERAL DEL SERVIDOR.

Zentyal Cloud



Para servicios completos de nivel empresarial, obtén una suscripción [Profesional](#) o [Empresarial](#). Estas ofrecen actualizaciones con Aseguramiento de la Calidad, Alertas, Informes y monitorización y gestión centralizada de tus servidores Zentyal

Detalles de suscripción de Zentyal

Nombre de usuario o dirección de correo: henry.padilla@movidatos.com

Nombre del servidor: srvzentyal

Elige un nombre para tu servidor que sea un nombre de subdominio válido

[Desuscribir](#)

[Server subscription info](#)

[QA software updates](#)

[Alerts](#)

[Reports](#)

Server name: srvzentyal

Server subscription: Unknown

Subscription renovation date: Unlimited

Central monitoring & management: Disabled

Figura 6.4.1. Información general servidor Zentyal..

Fuente: Autor tesis Henry Padilla.

Dashboard

[Configurar widgets](#)

Información general	
Fecha y hora	mar feb 21 12:02:33 ECT 2012
Nombre de máquina	srvzentyal
Versión de la plataforma	2.0.21 (2.0.22 disponible)
Carga del sistema	0.37, 0.53, 0.53
Tiempo de funcionamiento sin interrupciones	44 days, 16:16
Usuarios	0

Figura 6.4.2. Información general servidor Zentyal.

Fuente: Autor tesis Henry Padilla.

Información funcionamiento de red.

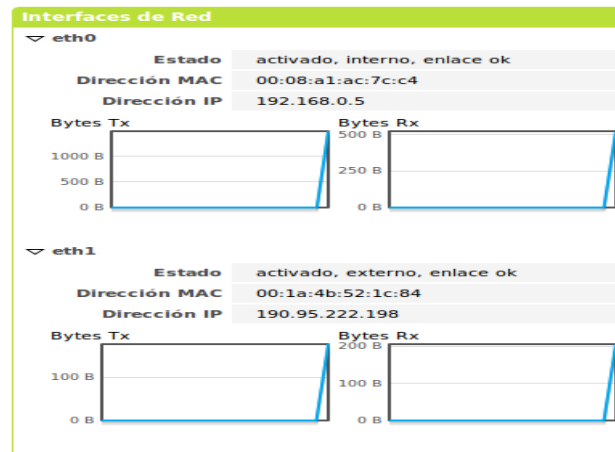


Figura 6.4.3. Funcionamiento de red servidor Zentyal.

Fuente: Autor tesis Henry Padilla.

Zentyal Cloud el cual es una suscripción básica la cual sirva para monitorear los servicios del servidor desde cualquier conexión o enlace de internet.

Zentyal Cloud	
Server name	srvzentyal
Connection status	Conectado
Server subscription	Basic
Technical support	Disabled - Enable
Actualizaciones de Seguridad Avanzadas	Disabled - Enable
Recuperación de Desastres	Configuration backup enabled - Latest conf backup: Wed, 15 Feb 2012 22:15:44 +0100

Figura 6.4.4. Zentyal Cloud.

Fuente: Autor tesis Henry Padilla.

Información referente a los módulos configurados y su estado de los mismos en el servidor multitarea Zentyal.

Configuración del estado de los módulos

Módulo	Depende	Estado
Red		<input checked="" type="checkbox"/>
Cortafuegos	Red	<input checked="" type="checkbox"/>
Antivirus		<input checked="" type="checkbox"/>
DHCP	Red	<input type="checkbox"/>
DNS		<input checked="" type="checkbox"/>
Copia de seguridad		<input checked="" type="checkbox"/>
Eventos		<input checked="" type="checkbox"/>
IDS	Red	<input checked="" type="checkbox"/>
Registros		<input checked="" type="checkbox"/>
Filtro de correo	Red, Antivirus, Cortafuegos	<input checked="" type="checkbox"/>
Monitorización		<input checked="" type="checkbox"/>
NTP		<input checked="" type="checkbox"/>

Figura 6.4.5. Estado de módulos configurados en Zentyal.

Fuente: Autor tesis Henry Padilla.

VPN	Red	<input checked="" type="checkbox"/>
Moldeado de tráfico	Red, Cortafuegos	<input checked="" type="checkbox"/>
Usuarios y Grupos		<input checked="" type="checkbox"/>
Servidor Web		<input checked="" type="checkbox"/>
Voz sobre IP	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>
FTP	Usuarios y Grupos	<input checked="" type="checkbox"/>
Jabber	Usuarios y Grupos	<input checked="" type="checkbox"/>
Correo	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>
RADIUS	Usuarios y Grupos	<input checked="" type="checkbox"/>
Compartir ficheros	Red, Usuarios y Grupos	<input checked="" type="checkbox"/>
Proxy HTTP	Cortafuegos, Usuarios y Grupos, Antivirus	<input checked="" type="checkbox"/>
Rincón del Usuario	Usuarios y Grupos	<input checked="" type="checkbox"/>
Webmail	Correo, Servidor Web	<input checked="" type="checkbox"/>
Groupware	Correo, Servidor Web	<input checked="" type="checkbox"/>
Compartir Impresoras	Compartir ficheros	<input checked="" type="checkbox"/>

Figura 6.4.6. Estado de módulos configurados en Zentyal.

Fuente: Autor tesis Henry Padilla.

En la gráfica se puede revisar el detalle de uso de disco en el servidor Zentyal.

Uso de disco

/dev/md0	
Propiedades de la partición	
Montado en	/
Tipo	ext4
Opciones	rw,errors=remount-ro,usrquota,grpquota,acl

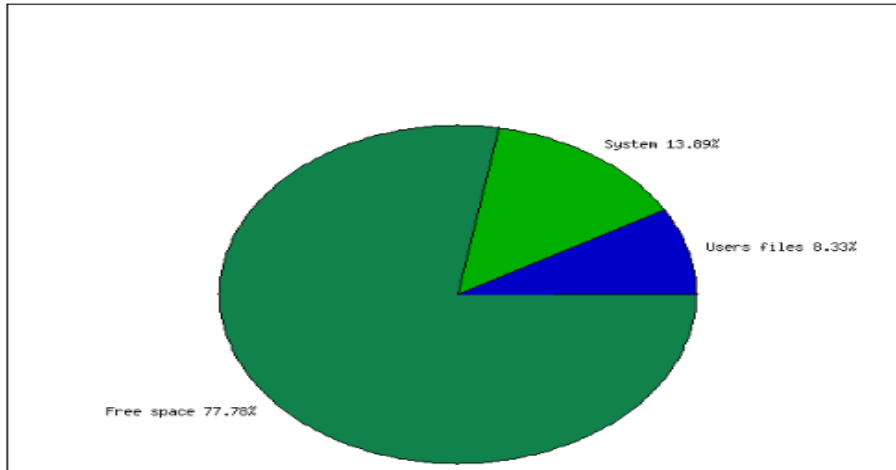


Figura 6.4.7. Uso de disco en Zentyal.

Fuente: Autor tesis Henry Padilla.

Para colocación en producción del servidor multitarea Zentyal se implementó como configuro un arreglo raid 1 +0 a nivel de software para tener redundancia de información de un disco a otro con todo lo implementado como integrado en el servidor.

RAID

/dev/md0		/dev/md1
Propiedades del vector		
Estado	activo	
Tipo	RAID 1	
Dispositivos RAID activos	2	
Dispositivos RAID activos necesarios	2	
Tamaño en bloques	148436928	
Número de dispositivo RAID	Dispositivo	Estado
0	/dev/sda1	funcionando
1	/dev/sdb1	funcionando

Figura 6.4.8. Estado de arreglo de disco 1 + 0 en Zentyal.

Fuente: Autor tesis Henry Padilla.

RAID

Propiedades del vector		
Estado	activo	
Tipo	RAID 1	
Dispositivos RAID activos	2	
Dispositivos RAID activos necesarios	2	
Tamaño en bloques	7851968	
Número de dispositivo RAID	Dispositivo	Estado
0	/dev/sda2	funcionando
1	/dev/sdb2	funcionando

Figura 6.4.9. Estado de arreglo de disco 1 + 0 en Zentyal.

Fuente: Autor tesis Henry Padilla.

Listado de los principales servicios internos que tiene el servidor en producción.

Lista de servicios

[+ Añade nuevo](#)

Nombre del servicio	Descripción	Interno	Configuración	Action
FTP	Zentyal FTP Server	<input checked="" type="checkbox"/>		
Mail system	Zentyal Mail System	<input checked="" type="checkbox"/>		
ManageSieve	protocol for editing SIEVE filters	<input checked="" type="checkbox"/>		
POP Transparent proxy	POP transparent proxy	<input checked="" type="checkbox"/>		
POP3	POP3 protocol	<input checked="" type="checkbox"/>		
RADIUS	Zentyal RADIUS system	<input checked="" type="checkbox"/>		
Voz sobre IP	Zentyal VoIP system	<input checked="" type="checkbox"/>		
any	any protocol and port	<input type="checkbox"/>		
any TCP	any TCP port	<input type="checkbox"/>		
any UDP	any UDP port	<input type="checkbox"/>		

10 Página 1 de 3

Figura 6.4.10. Lista de servicios en Zentyal.

Fuente: Autor tesis Henry Padilla.

Monitoreo del rendimiento del sistema de archivos como el uso de CPU del servidor en producción.



Figura 6.4.11. Monitoreo en Zentyal.

Fuente: Autor tesis Henry Padilla.

Monitoreo del rendimiento del uso de memoria en el servidor en producción.

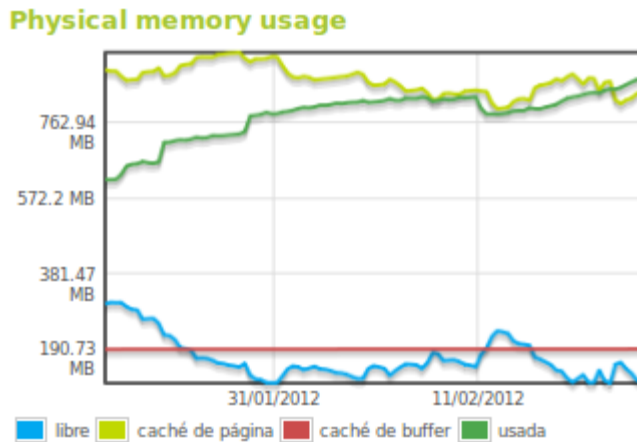


Figura 6.4.12. Monitoreo memoria en Zentyal.

Fuente: Autor tesis Henry Padilla.

6.4.2. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR CONTROLADOR DE DOMINIO EN PRODUCCIÓN.

En el panel principal de monitoreo de Zentyal se puede verificar el número de usuarios conectados al dominio Movيدات como los recursos compartidos que está utilizando del servidor de archivos.

En el servidor de dominio que forma parte del servidor multitarea Zentyal se creó los usuarios los cuales van a pertenecer a un grupo determinado según su respectiva área.

Usuarios

<input type="text"/> <input type="button" value="Buscar"/>		
Nombre	Nombre completo	Editar
alopez	Andres Lopez	
calban	Carlos Alban	
chrodriguez	Christian Rodriguez	
csumba	Carmen Sumba	
dcarvajal	Daniela Carvajal	
dpasochoa	David Pasochoa	
drosero	Darwin Rosero	
dzambrano	David Zambrano	
ecastro	Elizabeth Castro	
egallardo	Edwin Gallardo	
fguerrero	Fabian Guerrero	
gante	Gabriela Ante	
gteran	Gabriela Teran	
hpadilla	Henry Rolando Padilla Cevallos	
hreinoso	Henry Reinoso	
ialban	Ivonne Alban	
jandrade	Jacqueline Andrade	
jfrancis	Joel Francis	
jrojas	Jhoana Rojas	
jvalle	Julio Valle	




























lchicaiza	Luis Chicaiza	
lperalta	Luis Peralta	
malban	Monica Alban	
mbustos	Monica Bustos	
mjgomez	Maria Jose Gomez	
mproanio	Mario Proanio	
mvasquez	Marco Vasquez	
nquinchanegua	Nohora Quinchanegua	
palban	Paola Alban	
pmorales	Paola Morales	
pruiz	Pablo Ruiz	
rburnano	Rodrigo Burbano	
rcumbal	Renato Cumbal	
rrodriguez	Rosy Rodriguez	
rteran	Renato Teran	
sredroban	Santiago Redroban	
usradmindc	Usuario Servidor Controlador Dominio	
usradministrativo	Usuario Generico Administrativo	
usradminpc	Usuario Generico Administrador Equipos	
usrcontabilidad	Usuario Generico Contabilidad	
usrecepcion	Usuario Generico Recepcion	
usrgerencia	Usuario Generico Gerencia	
usrinvitado	Usuario Generico Ingreso Invitados	
usrrhh	Usuario Generico RRHH	
usr sistemas	Usuario Generico Sistemas	
usrventas	Usuario Generico Ventas	
vgonzalez	Vinicio Gonzalez	

Figura 6.4.13. Usuario configurados en el dominio Movidatos.

Fuente: Autor tesis Henry Padilla.

Como se indicó anteriormente cada usuario va pertenecer a un grupo determinado según su área en el dominio configurado de nombre Movidatos, cada usuario al ingresar como dominio corporativo va a pertenecer a un grupo específico con

políticas de seguridad como recursos de acceso archivos, red, internet, páginas web etc. según la necesidad de la empresa

Grupos

Nombre	Descripción	Editar
Grupo_Administrador_Dominio	Administrador Controlador Dominio	
Grupo_Departamento_Administrativo	Departamento Administrativo	
Grupo_Departamento_Contabilidad	Departamento Contabilidad	
Grupo_Departamento_Gerencia	Departamento Gerencia	
Grupo_Departamento_RRHH	Departamento RRHH	
Grupo_Departamento_Recepcion	Departamento Recepcion	
Grupo_Departamento_SVC	Departamento Servicio Cliente	
Grupo_Departamento_Sistemas	Departamento Sistemas	
Grupo_Departamento_Ventas	Departamento Ventas	
Grupo_Usuarios_Genericos	Usuarios Genericos Movidatos	

10 Página 1 

Figura 6.4.14. Grupos configurados en el dominio Movidatos.

Fuente: Autor tesis Henry Padilla.

6.4.3. DETALLES DE LA CONFIGURACIÓN LDAP EN EL SERVIDOR DE DOMINIO MOVIDATOS.

LDAP Settings [\(mostrar ayuda\)](#)

Información de LDAP

DN Base: dc=svrzentyal

DN Raíz: cn=ebox,dc=svrzentyal

Contraseña: .U5U170DmLXXaJ8w

DN de Usuarios: ou=Users,dc=svrzentyal

DN de Grupos: ou=Groups,dc=svrzentyal

Opciones de configuración PAM

Habilitar PAM:

Hacer que los usuarios LDAP tengan cuenta en el sistema.

Shell por defecto:











Este cambio se aplicará únicamente a los usuarios creados a partir de ahora.

Figura 6.4.15. Información LDAP en Zentyal.

Fuente: Autor tesis Henry Padilla.

Lista de traductores de servidores de nombres de dominio

[+ Añade nuevo](#)

Servidor de nombres de dominio		Action
192.168.0.1	  	
200.93.216.2	   	
200.93.216.5	  	





10 ▼ Página 1    

Figura 6.4.16. Servidores de nombres de dominio en Zentyal.

Fuente: Autor tesis Henry Padilla.

Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) | [PDC](#) | [Directorios compartidos](#) | [Papelera de Reciclaje](#) | [Antivirus](#)

Habilitar PDC:

Nombre del dominio:

Nombre de Netbios:

Descripción:

Límite de cuota: Limitada a ▼ Mb

Habilitar perfiles móviles:

Letra de unidad: H: ▼

Grupo Samba: Todos los usuarios ▼
Sólo los usuarios que pertenecen a este grupo tendrán una cuenta de Samba. Sincronización ocurre cada hora.

Figura 6.4.17. Compartición de ficheros en Zentyal.

Fuente: Autor tesis Henry Padilla.

Compartir ficheros [\(mostrar ayuda\)](#)

[Configuración general](#) | [PDC](#) | [Directorios compartidos](#) | [Papelera de Reciclaje](#) | [Antivirus](#)

Longitud mínima de contraseña: Limitada a ▼ caracteres

Caducidad de la contraseña: Deshabilitado ▼

Forzar historial de contraseñas: Deshabilitado ▼

Figura 6.4.18. Parámetros contraseñas usuarios del dominio.

Fuente: Autor tesis Henry Padilla.

Compartir ficheros

Cuenta de Compartición de Ficheros o de PDC:

Compartir ficheros [\(mostrar ayuda\)](#)

Habilitado	Nombre del recurso compartido	Ruta del recurso compartido	Comentario	Acceso de invitado	Control de acceso	Action
<input checked="" type="checkbox"/>	Registro Activaciones Ventas	Registro_Activaciones_Ventas	Departamento Ventas	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Contabilidad 2011	Contabilidad_2011	Departamento Contabilidad	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Analisis Comisiones	Analisis_Comisiones	Departamento Contabilidad	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Documentos Portabilidad	Documentos_Portabilidad	Documentos Ventas	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Reliquidaciones 2011	Reliquidaciones_2011	Departamento Contabilidad	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Historico Contabilidad	Historico_Contabilidad	Departamento Contabilidad	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Historico Ventas General	Historico_Ventas_General	Departamento Ventas	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Comisiones 2011	Comisiones_2011	Departamento Contabilidad	<input type="checkbox"/>		
<input checked="" type="checkbox"/>	Bodega	Bodega	Departamento Contabilidad	<input type="checkbox"/>		

Figura 6.4.19. Compartición de ficheros.

Fuente: Autor tesis Henry Padilla.

6.4.4. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR PROXY EN PRODUCCIÓN.

Para proceder a bloquear el acceso a páginas web de internet se crearon objetos de red los cuales tienen su respectivos miembros en este caso serían las direcciones Ip de cada usuario asignada en su computador.

Proxy HTTP [\(mostrar ayuda\)](#)

Configuración General

Proxy Transparente:

Nótese que no se puede usar proxy HTTPS de forma transparente. Se necesitará añadir una regla de firewall si se habilita este modo.

Puerto:

Tamaño de los ficheros de caché (MB):

Política predeterminada:

Filter significa que las peticiones HTTP pasan por el filtro de contenidos y que podrían ser rechazados si el contenido no se considera válido.

Figura 6.4.20. Proxy en Zentyal.

Fuente: Autor tesis Henry Padilla.

Filter Profiles > Filtrado_Grupo_Contabilidad [\(mostrar ayuda\)](#)

Filtrar virus

Usar antivirus:

Umbral de filtrado de contenido

Usar el umbral del perfil por defecto:

Umbral:

Esto especifica cuán estricto es el filtro

Usar perfil predeterminado para la extensión de filtrado

Usar configuración del perfil predeterminado:

Configurar extensiones de ficheros permitidas

[+ Añade nuevo](#)

Determinar política para todas las extensiones

Permitir todas extensiones:

Usar este campo para cambiar el valor de todas filas de arriba a la vez

Filtrar virus

Usar antivirus:

[Cambiar](#)

Umbral de filtrado de contenido

Usar el umbral del perfil por defecto:

Umbral: Desactivado

Esto especifica cuán estricto es el filtro

[Cambiar](#)

[Filtrado de extensiones de fichero](#)

[Filtrado de tipos MIME](#)

Filtrado de dominios para grupo de filtros

Usar perfil predeterminado para el filtrado de dominios

Usar configuración del perfil predeterminado:

[Cambiar](#)

Configuración del filtrado de dominio

Bloquear dominios y URLs no listados:

Si esta opción está habilitada, cualquier dominio que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP:

[Cambiar](#)

Configuración del filtrado de dominio

Bloquear dominios y URLs no listados:

Si esta opción está habilitada, cualquier dominio que no esté en la sección *Reglas de dominios*, ni en *Ficheros de listas de dominios* debajo será prohibido.

Bloquear sitios especificados sólo como IP:

[Cambiar](#)

Reglas de dominios y URLs

[+ Añade nuevo](#)

<input type="text"/> Buscar		
Dominio o URL	Política	Action
192.168.0.3	Siempre permitir	
aulaclic.es	Siempre permitir	
bancodelpacifico.com	Siempre permitir	
bancoguayaquil.com	Siempre permitir	
bce.fin.ec	Siempre permitir	
cabinas.net	Siempre permitir	
ccpp.org.ec	Siempre permitir	
computrabajo.com.ec	Siempre permitir	
es.wikipedia.org	Siempre permitir	
google.com.ec	Filtrar	

Figura 6.4.21. Filtrado de contenido, dominios y ficheros.

Fuente: Autor tesis Henry Padilla.

Lista de objetos

[+ Añade nuevo](#)

Nombre	Miembros	Action
Objeto_Acceso_Usrssh		 
Objeto_Control_Red_Dmz_Gye		 
Objeto_Control_Red_Lan		 
Objeto_Control_Red_Wan		 
Objeto_Proxy_Grupos_Activaciones		 
Objeto_Proxy_Grupos_Administrativo		 
Objeto_Proxy_Grupos_Contabilidad		 
Objeto_Proxy_Grupos_Gerencia		 
Objeto_Proxy_Grupos_RRHH		 
Objeto_Proxy_Grupos_Recepcion		 

Lista de objetos

[+ Añade nuevo](#)

Nombre	Miembros	Action
Objeto_Proxy_Grupos_Sistemas		 
Objeto_Proxy_Grupos_Svc		 
Objeto_Proxy_Grupos_Ventas_Guayaquil		 
Objeto_Proxy_Grupos_Ventas_Quito		 

10  Página 2 de 2    

Figura 6.4.22. Objetos de red en Zentyal.

Fuente: Autor tesis Henry Padilla.

Cada objeto de red tiene como referencia el grupo de usuarios del dominio según su área para proceder con el bloqueo de páginas web según su dominio o número de ip que se encuentran en la dmz.

Lista de perfiles

[Añade nuevo](#)

Filtrar grupo	Configuración	Action
default		 
Filtrado_Grupo_Gerencia		 
Filtrado_Grupo_Recepcion		 
Filtrado_Grupo_Invitado		 
Filtrado_Grupo_Administrativo		 
Filtrado_Grupo_Ventas		 
Filtrado_Grupo_Contabilidad		 
Filtrado_Grupo_Sistemas		 
Filtrado_Grupo_Svc		 

Figura 6.4.23. Perfiles de red en Zentyal.




















Fuente: Autor tesis Henry Padilla.




Cada dominio de página web registrado para el bloqueo tiene la opción de configurar el acceso como permitir, denegar o filtrar según los requerimientos corporativos como las necesitadas del usuario y de la empresa.

Ejemplo de una regla de acceso a específicas páginas de internet al objeto de red del grupo de contabilidad.

Reglas de dominios y URLs




















[+ Añade nuevo](#)





Dominio o URL	Política	Action
192.168.0.3	Siempre permitir	 
aulaclic.es	Siempre permitir	 
bancodelpacifico.com	Siempre permitir	 
bancoguayaquil.com	Siempre permitir	 
bce.fin.ec	Siempre permitir	 
cabinas.net	Siempre permitir	 
ccpp.org.ec	Siempre permitir	 
computrabajo.com.ec	Siempre permitir	 
es.wikipedia.org	Siempre permitir	 
google.com.ec	Filtrar	 

10 ▼ Página 1 de 3    

Reglas de dominios y URLs









[+ Añade nuevo](#)

Dominio o URL	Política	Action
google.es/maps	Always allow	 
iess.gob.ec	Always allow	 
lacamaradequito.com	Always allow	 
movidatos.com	Always allow	 
mrl.gob.ec	Always allow	 
pichincha.com	Always allow	 
policiaecuador.gob.ec	Always allow	 
produbanco.com	Always allow	 
sbs.gob.ec	Always allow	 
secap.gob.ec	Always allow	 

10 ▼ Página 2 de 3    

Reglas de dominios y URLs

[+ Añade nuevo](#)

Dominio o URL	Política	Action
sri.gov.ec	Always allow	 
supercias.gov.ec	Always allow	 
translate.google.es	Always allow	 
tributacionposgradog.galeon.com	Always allow	 





10 ▼ Página 3 de 3    

Figura 6.4.24. Reglas de acceso a dominios y urls.



Fuente: Autor tesis Henry Padilla.





6.4.5. DETALLE DEL COMPORTAMIENTO DEL SERVIDOR FIREWALL EN PRODUCCIÓN.

Puertas de enlace y Proxy [\(mostrar ayuda\)](#)

Lista de Puertas de Enlace

[+ Añade nuevo](#)

Habilitado	Nombre	Dirección IP	Interfaz	Peso	Predeterminado	Action
<input checked="" type="checkbox"/>	Gateway_Wan	190.95.222.193	eth1	1	<input checked="" type="checkbox"/>	 

10 ▼ Página 1    

Interfaces de Red [\(mostrar ayuda\)](#)

eth0 eth1

Nombre:

Método: ▼

Externo (WAN):

Dirección IP:

Máscara de red: ▼

eth0 eth1

Nombre: eth1

Método: Estático

Externo (WAN):

Dirección IP: 190.95.222.198

Máscara de red: 255.255.255.248

Cambiar

Figura 6.4.25. Tarjetas de red lan y wan.

Fuente: Autor tesis Henry Padilla.

Para la implementación del servidor multitarea Zentyal se configuró la opción de las tarjetas de red eth0 y eth1 como sus puertas de enlace para la tarjeta de red interna como la externa, para realizar la función de NAT para que los usuarios puedan navegar por internet mediante el servidor Zentyal.

El servidor Zentyal para proporcionar acceso a internet actúa como firewall mediante la configuración de las respectivas tarjetas de red interna como externa realizando NAT.

Es decir se tiene configurado una IP interna para la red LAN y una IP externa para la red WAN para que todos los usuarios puedan navegar en internet mediante el servidor Zentyal y así poder controlar el acceso a internet mediante el proxy realizando las siguientes acciones como son permitir, filtrar, denegar el acceso a direcciones de internet por dominio o por dirección IP.

Para la verificación del funcionamiento del servidor Zentyal en producción se colocó la configuración de la siguiente manera el origen va a ser cualquiera para utilizar un determinado servicio, es decir cualquier equipo va a poder utilizar el servicio especificado en las configuraciones del servidor.

Objetos [\(mostrar ayuda\)](#)

Lista de objetos

[+ Añade nuevo](#)

Nombre	Miembros	Action
Objeto_Acceso_Usrssh		
Objeto_Bloqueo_Correos_Externos		
Objeto_Bloqueo_Messenger_Externo		
Objeto_Control_Red_Dmz_Gye		
Objeto_Control_Red_Lan		
Objeto_Control_Red_Wan		
Objeto_Limitacion_Ancho_Banda		
Objeto_Proxy_Grupo_Activaciones		
Objeto_Proxy_Grupo_Administrativo		
Objeto_Proxy_Grupo_Contabilidad		

10 ▼ Página 1 de 2

Lista de objetos

[+ Añade nuevo](#)

Nombre	Miembros	Action
Objeto_Proxy_Grupo_Gerencia		
Objeto_Proxy_Grupo_RRHH		
Objeto_Proxy_Grupo_Recepcion		
Objeto_Proxy_Grupo_Sistemas		
Objeto_Proxy_Grupo_Svc		
Objeto_Proxy_Grupo_Ventas_Guayaquil		
Objeto_Proxy_Grupo_Ventas_Quito		

10 ▼ Página 2 de 2








































Figura 6.4.26.Objetos de red para control de acceso..

Fuente: Autor tesis Henry Padilla.

Filtrado de paquetes > Redes internas

Configurar reglas

+ [Añade nuevo](#)

Decisión	Origen	Destino	Servicio	Descripción	Action
✗	Objeto_Proxy_Grupo_Ventas_Quito	Objeto_Bloqueo_Messenger_Externo	any TCP	--	  
✗	Objeto_Proxy_Grupo_Ventas_Guayaquil	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_Svc	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_Recepcion	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_RRHH	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_Administrativo	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_Activaciones	Objeto_Bloqueo_Messenger_Externo	any TCP	--	   
✗	Objeto_Proxy_Grupo_Ventas_Guayaquil	Objeto_Bloqueo_Correos_Externos	any TCP	--	   
✗	Objeto_Proxy_Grupo_Svc	Objeto_Bloqueo_Correos_Externos	any TCP	--	   
✗	Objeto_Proxy_Grupo_Recepcion	Objeto_Bloqueo_Correos_Externos	any TCP	--	   






10  Página 1 de 2    

Figura 6.4.27. Filtrado de paquetes de acceso interno.

Fuente: Autor tesis Henry Padilla.

Filtrado de paquetes > Redes internas [\(mostrar ayuda\)](#)

Configurar reglas

+ [Añade nuevo](#)













Decisión	Origen	Destino	Servicio	Descripción	Action
✗	Objeto_Proxy_Grupo_RRHH	Objeto_Bloqueo_Correos_Externos	any TCP	--	   
✗	Objeto_Proxy_Grupo_Activaciones	Objeto_Bloqueo_Correos_Externos	any TCP	--	   
✗	Objeto_Proxy_Grupo_Ventas_Quito	Objeto_Bloqueo_Correos_Externos	any TCP	--	   
































Figura 6.4.28. Filtrado de paquetes de acceso interno.

Fuente: Autor tesis Henry Padilla.

Filtrado de paquetes ▶ Desde redes internas hacia Zentyal [\(mostrar ayuda\)](#)

Configurar reglas

[+ Añade nuevo](#)

Decisión	Origen	Servicio	Descripción	Action
✘	Cualquiera	ldap	--	   
↑	Cualquiera	ntp	--	   
↑	Cualquiera	dns	--	   
↑	Cualquiera	dhcp	--	   
↑	Cualquiera	tftp	--	   
↑	Cualquiera	http	--	   
↑	Cualquiera	ssh	--	   
↑	Cualquiera	eBox administration	--	  






10  Página 2 de 2    

Figura 6.4.29. Filtrado de paquetes desde redes internas hacia Zentyal.

Fuente: Autor tesis Henry Padilla.

En la opción de firewall del servidor Zentyal se tiene la opción del filtrado de paquetes desde redes externas hacia Zentyal definiendo un origen que en este caso sería la dirección ip de un equipo de la red interna de la empresa y un destino que sería la dirección ip de un servidor determinado para usar un específico servicio.

Las reglas de filtrado de paquetes añadidas por servicios de Zentyal están configuradas para que según el servicio a utilizar desde cualquier red externa pueda ser controlado mediante el proxy del servidor especificando el puerto como el servicio a utilizar, y se procede a configurar la decisión si se acepta el acceso o petición o se deniega, según el requerimiento.

Servicios [\(mostrar ayuda\)](#)

Lista de servicios

[+ Añade nuevo](#)

Nombre del servicio	Descripción	Interno	Configuración	Action
FTP	Zentyal FTP Server	<input checked="" type="checkbox"/>		
Mail system	Zentyal Mail System	<input checked="" type="checkbox"/>		
ManageSieve	protocol for editing SIEVE filters	<input checked="" type="checkbox"/>		
Messenger Gmail	Mail Messenger Externo Gmail	<input type="checkbox"/>		
Messenger Hotmail	Mail Messenger Externo Hotmail	<input type="checkbox"/>		
Messenger Yahoo	Messenger Externo Yahoo	<input type="checkbox"/>		

Figura 6.4.30. Configuración de servicios en Zentyal.

Fuente: Autor tesis Henry Padilla.

[Servicios](#) > [Messenger Gmail](#)

Configuración de servicio

[+ Añade nuevo](#)

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	443
TCP/UDP	cualquiera	5222

Figura 6.4.31. Configuración de puertos de Messenger Gmail.

Fuente: Autor tesis Henry Padilla.

Servicios > Messenger Hotmail

Configuración de servicio

+ [Añade nuevo](#)

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	1503
TCP/UDP	cualquiera	5004-65535
TCP/UDP	cualquiera	1863
TCP/UDP	cualquiera	3389
TCP/UDP	cualquiera	6901

Figura 6.4.32. Configuración de puertos de Messenger Hotmail.

Fuente: Autor tesis Henry Padilla.

Servicios > Messenger Yahoo

Configuración de servicio

+ [Añade nuevo](#)

Protocolo	Puerto origen	Puerto destino
TCP/UDP	cualquiera	5001
TCP/UDP	cualquiera	5000
TCP/UDP	cualquiera	5055

Figura 6.4.33. Configuración de puertos de Messenger Yahoo.

Fuente: Autor tesis Henry Padilla.

Decisión	Origen	Destino	Servicio
✘	Objeto_grupo_Sistemas	Cualquiera	Messenger Hotmail
✘	Objeto_grupo_Sistemas	Cualquiera	Messenger Gmail
✘	Objeto_grupo_Sistemas	Objeto_Bloqueo_Correos_Externos	any
✘	Objeto_grupo_Sistemas	Objeto_Bloqueo_Messenger_Externo	any
✘	Objeto_grupo_Ventas_Quito	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Ventas_Guayaquil	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Svc	Objeto_Bloqueo_Messenger_Externo	any TCP
✘	Objeto_grupo_Recepcion	Objeto_Bloqueo_Messenger_Externo	any TCP

Figura 6.4.34. Bloqueo de acceso a los diferentes Messenger externos.

Fuente: Autor tesis Henry Padilla.

Redirecciones de puertos

Lista de puertos redirigidos

[+ Añade nuevo](#)


Interfaz	Destino original	Puerto de destino original	Protocolo	Origen	IP Destino	Puerto	Registrar	Descripción	Action
eth0	192.168.0.4/32	22	TCP/UDP	192.168.0.1/32	192.168.0.4	Mismo	<input checked="" type="checkbox"/>	Conexion usuario ssh SRVCONT	

Figura 6.4.34. Redirecciones de puertos en Zentyal.

Fuente: Autor tesis Henry Padilla.

6.5. FINANCIAMIENTO.

**6.5.1. FINANCIAMIENTO ESTUDIANTE PADILLA CEVALLOS
HENRRY ROLANDO.**

Derecho de matrícula.	\$ 200 Dólares.
Presentación de tesis.	\$ 200 Dólares.
Servicio de internet.	\$ 180 Dólares
Impresiones.	\$ 200 Dólares.
Transporte.	\$ 100 Dólares.
Servidor de dominio, firewall, y proxy con Zentyal.	\$ 600 Dólares.

(Servidor financiado por el estudiante en un 50 % del valor total de \$ 1200 Dólares).

Subtotal 1: \$ 1480 Dólares.

6.5.2. FINANCIAMIENTO EMPRESA MOVIDATOS

Servidor de correo virtual Zimbra. \$ 2500 Dólares.

(Servidor HP Proliant ML350 G6 proporcionado por la Empresa Movidatos.)

Servidor de dominio, firewall, y proxy con Zentyal. \$ 600 Dólares.

(Servidor financiado por la Empresa Movidatos en un 50 % del valor total de \$ 1200 Dólares).

Subtotal 2: \$ 3100 Dólares.

Total: \$ 4580 Dólares

6.6 TERMINOLOGIA.

DNS: Domain Name System (Sistema de nombre de dominios).

HTTP: HyperText Transfer Protocol (Protocolo transferencia hipertexto).

HTTPS: HyperText Transfer Protocol Secure (Protocolo transferencia hipertexto seguro).

HTML: HyperText Markup Language (Lenguaje de marcas de hipertexto).

IMAP: Internet Message Access Protocol (Protocolo de acceso a mensajes de internet).

LDAP: Lightweight Directory Access Protocol (Protocolo ligero de acceso a directorios).

LMTP: Local Mail Transfer Protocol (Protocolo de transporte local de correo).

MTA: Mail Transfer Agent (Agente de transferencia de correo).

MAPI: Messanging Aplication Programing Interface.

NAT: Network Access Translation (traducción de dirección de red).

POP: Post Office Protocol.

RAM: Memoria de acceso aleatorio.

SMTP: Simple Mail Transfer Protocol (Protocolo de simple transferencia de correo).

SSL: Secure Sockets Layer (Protocolo de capa de conexión segura).

SNMP: Protocolo simple de administración de red.

SRP: Server Routing Protocol (Protocolo de enrutamiento del servidor).

TLS: Transport layer security (Seguridad de la capa de transporte).

ZCS: Network Profesional Edition.

ZCB: Controlador de Zimbra para dispositivos celulares.

BIND: Servicio de resolución de nombres de dominio

NTP: Servicio de sincronización de hora

HTTP APACHE: Servicio de publicación de páginas web

VSFTPD : Servicio de Transferencia de ficheros

NETFILTER: sistema de cortafuegos

IPROUTE2: Introducción al encaminamiento o routing

SQUID : Servicio de Proxy HTTP

6.7. CONCLUSIONES Y RECOMENDACIONES.

6.7.1. CONCLUSIONES.

Todo proyecto de infraestructura antes de implementarlo tiene que ser sujeto a un análisis previo de su estructura, a nivel de red, plataformas, tipos de servicios como servidores implementados en producción.

Para integrar un nuevo servidor a producción se tiene que realizar en primer lugar pruebas en test de todos los servicios como plataforma a implementar para luego colocar en producción.

En el proceso de integración como implementación de uno o varios servidores a granja de servidores de una empresa se tiene que realizar la respectiva documentación del tipo hardware como software que se utilizó, para en un futuro realizar un control de cambios.

Realizar un diagrama de la infraestructura de red actual cuando se finalice la implementación como integración de los respectivos servidores, en la cual tiene que constar el diagrama de telecomunicaciones como dispositivos y hardware que se utilizó para el proyecto indicando las respectivas plataformas y servicios integrados.

Una vez realizado las respectivas pruebas en test realizando pruebas en conjunto con la infraestructura actual realizamos análisis del servidor en un ambiente de pre producción para verificar su funcionalidad según los servicios y sus prestaciones hacia el usuario y su desempeño como servidor.

En la pre producción de los respectivos servidores se tiene que establecer seguridades a nivel de red interna como externa mediante un respectivo firewall, tomando muy en cuenta si el equipo va estar conectado a la red externa mediante una dirección ip pública.

6.7.2. RECOMENDACIONES.

Para la implementación de servidores de correo se tiene que verificar donde se encuentra alojado el respectivo dominio como registros MX y registros A, para proceder a promover a un nuevo servidor de correo el dominio de correo respectivo, tomar en cuenta el tiempo que se demora en replicar los registros del dominio para que apunten hacia el nuevo servidor.

Establecer niveles de seguridad a nivel de puertos en la infraestructura, es decir se tiene que abrir solo los puertos de comunicación utilizados por las diferentes aplicaciones como servicios de correo, proxy, dominio utilizados, los demás puertos por seguridad tienen que estar cerrados.

Para implementaciones de servidores de alta disponibilidad se tiene que establecer seguridades redundantes como lo son configuración de discos en RAID, tener disco espejo si en algún momento llega a fallar un disco, fuentes redundantes, respaldos de máquinas virtuales en caso de tenerlas, enlaces de comunicación de respaldo.

Para implementar nuevos servidores a la infraestructura de un empresa se tiene que implementar un servidor de pruebas en un ambiente de test antes de colocar servidores en producción realizado un proceso de pre producción, verificando el funcionamiento del servidor a nivel de plataforma como servicios y el funcionamiento como rendimiento de su hardware respectivo.

6.8. BIBLIOGRAFÍA.

6.8.1. DOCUMENTACIÓN DE INTERNET.

<http://www.zimbra.com/training>

<http://www.zimbra.com>

<http://www.elblogderigo.info/2009/07/03/video-tutorial-instalacion-y-configuracion-de-zimbra/>

<http://www.zimbra.com>

<http://www.ubuntu-es.org/node/96029>

<http://www.lacosox.org/sites/default/files/ManualUsuarioZimbraVersionZCS>

<http://www.zimbra.com/community/documentation.html>

6.8.2 LIBROS.

- Zentyal preparación para el examen de certificación.
Zentyal Certified Associate (ZeCA).

Zentyal para administradores de redes versión 2.0.

Autor: Zentyal Formación.
- Manual Linux.
Autor: Álvaro Alea.
- Manual de usuario de Zimbra
IEFPS

Autor: Erika Mari

Dinamizador TIC
- Software libre.

Autor: Josep Jorba Esteve.

- Instalación de CentOS 5.
Autores: Pablo Sanz Mercado - Remo Suppi Boldrito.
- Manual zimbra collaboration suite.
Autor: Verónica Mora.
- Zimbra como solución libre a un servidor de correo.
Autor: Alejandro Moreno.
- Introducción a Linux.

Autor: C.Torrelaguna, 5828027 – Madrid.

Dirección general de educación.

Formación profesional e innovación educativa.

6.9. CRONOGRAMA DE ACTIVIDADES.

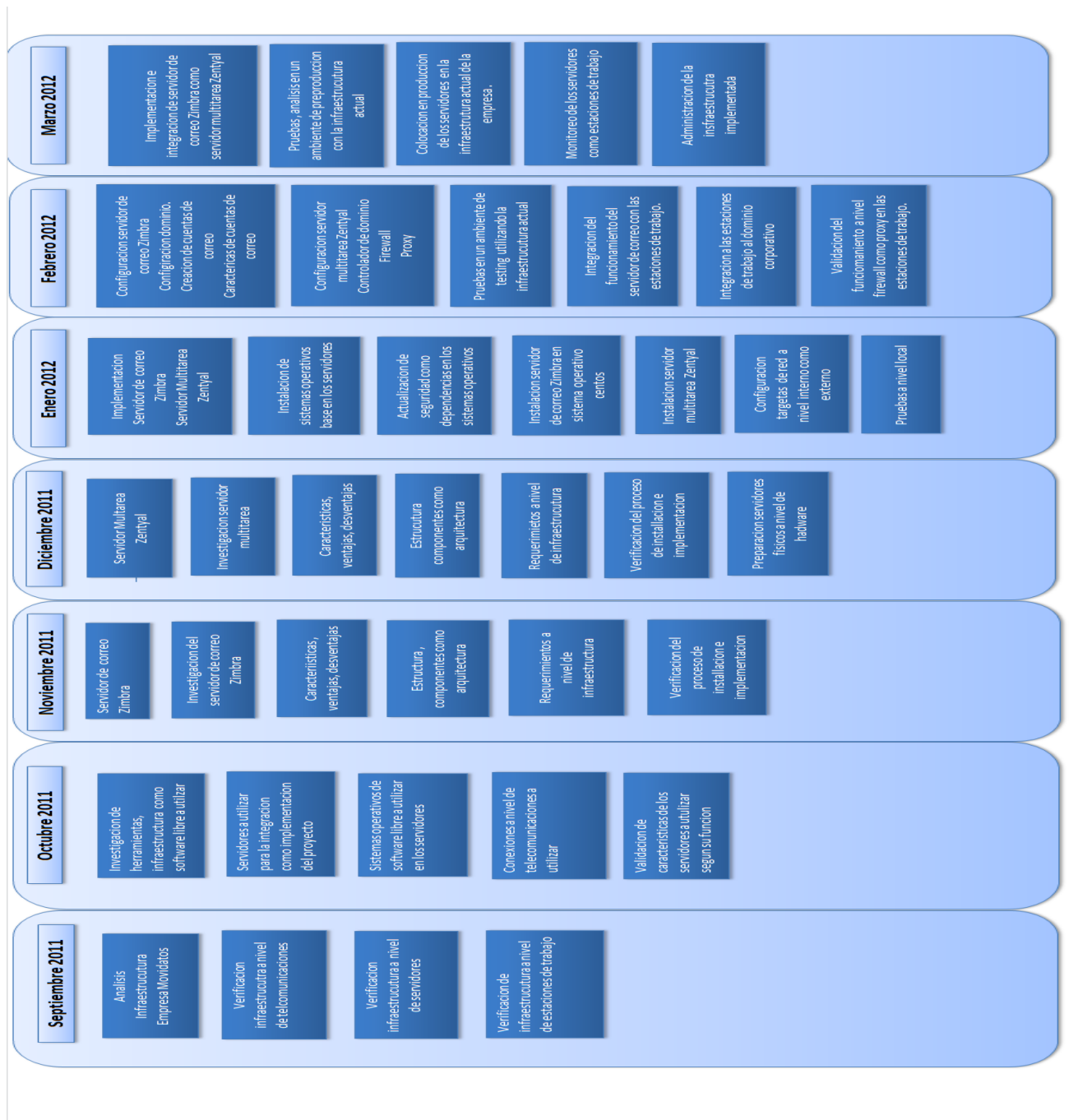


Figura 6.9.1. Cronograma actividades.

Fuente: Autor tesis Henry Padilla.

6.10. ANEXOS.

6.10.1. IMPLEMENTACIÓN FTP EXTERNO COMO INTERNO.

Servidor FTP [\(mostrar ayuda\)](#)

Opciones generales de configuración

Acceso anónimo:

Configura los permisos para el directorio /srv/ftp

Directorios personales:

Activa el acceso FTP de cada usuario a su directorio /home

Figura 6.10.1. Servidor FTP.

Fuente: Autor tesis Henry Padilla.

Dirreccion de acceso externo:

<ftp://hpadilla@190.95.222.198>

Dirreccion de acceso interno:

<ftp://hpadilla@192.168.0.5>

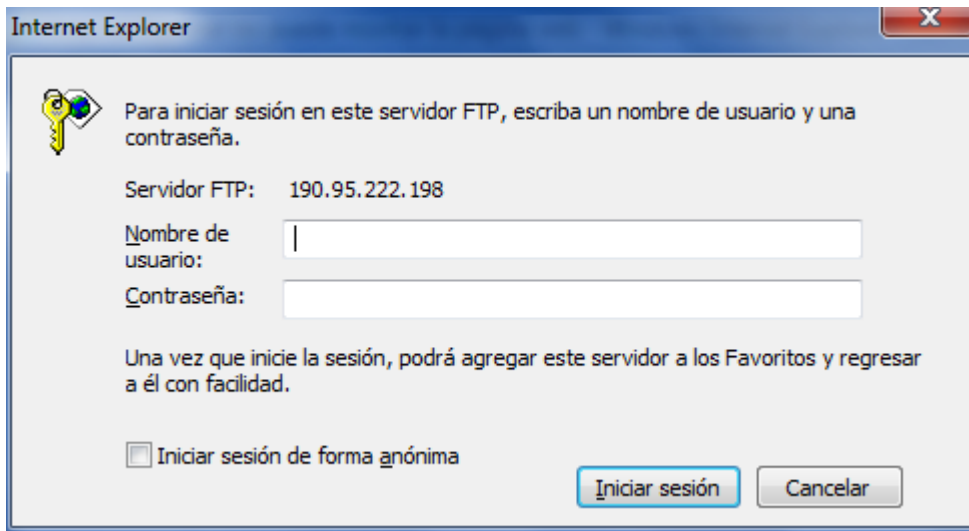


Figura 6.10.2. Acceso Servidor FTP.

Fuente: Autor tesis Henry Padilla.

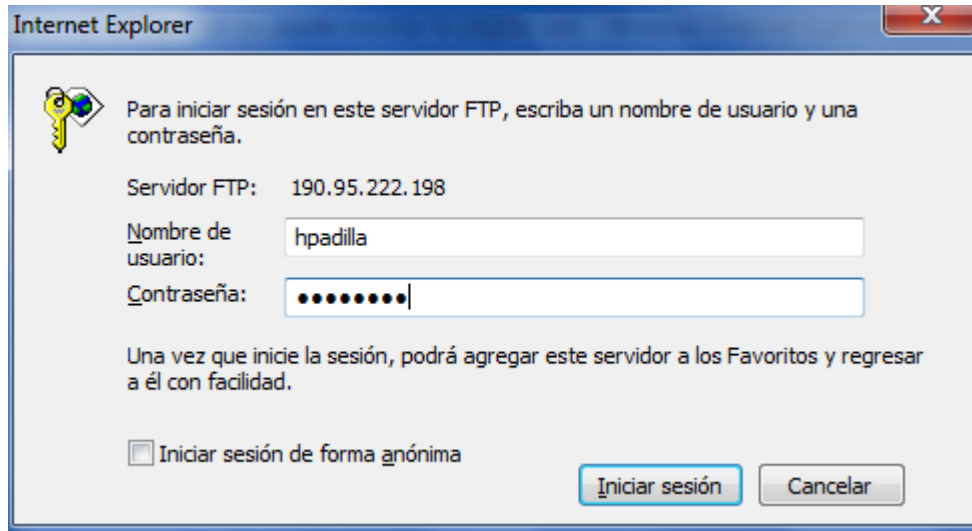


Figura 6.10.3. Acceso Servidor FTP.

Fuente: Autor tesis Henry Padilla.

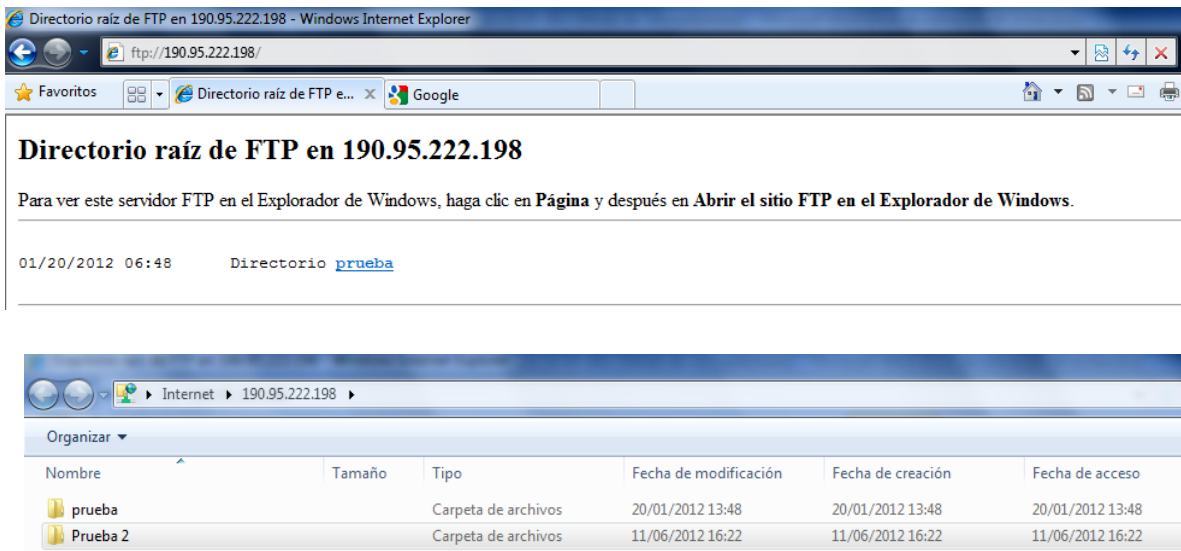


Figura 6.10.4. Acceso Servidor FTP.

Fuente: Autor tesis Henry Padilla.

6.10.2. DIRECTORIOS COMPARTIDOS.

Compartir ficheros [\(mostrar ayuda\)](#)

Configuración general		PDC	Directorios compartidos	Papelera de Recor
+ Añade nuevo				
<input type="text"/>		<input type="button" value="Buscar"/>		
Habilitado	Nombre del recurso compartido	Ruta del recurso compartido	Comentario	
<input checked="" type="checkbox"/>	Registro Activaciones Ventas	Registro_Activaciones_Ventas	Departamento Ventas	
<input checked="" type="checkbox"/>	Contabilidad 2011	Contabilidad_2011	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Análisis Comisiones	Análisis_Comisiones	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Documentos Portabilidad	Documentos_Portabilidad	Documentos Ventas	
<input checked="" type="checkbox"/>	Reliquidaciones 2011	Reliquidaciones_2011	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Historico Contabilidad	Historico_Contabilidad	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Historico Ventas General	Historico_Ventas_General	Departamento Ventas	
<input checked="" type="checkbox"/>	Comisiones 2011	Comisiones_2011	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Comisiones 2011	Comisiones_2011	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Bodega	Bodega	Departamento Contabilidad	
<input checked="" type="checkbox"/>	Servicio al cliente	Servicio_Cliente	Departamento Servicio Cliente	

Habilitado	Nombre del recurso compartido	Ruta del recurso compartido	Comentario
<input checked="" type="checkbox"/>	Historico Comisiones	Historico_Comisiones	Departamento Contabilidad
<input checked="" type="checkbox"/>	Descuentos Telefonica 2011	Descuentos_Telefonica_2011	Departamento Administrativo
<input checked="" type="checkbox"/>	Reportes Ejecutivos Ventas	Reportes_Ejecutivos_Ventas	Departamento Ventas

Figura 6.10.5. Directorios compartidos en dominio Movidatos.

Fuente: Autor tesis Henry Padilla.