



UNIVERSIDAD TÉCNICA DE AMBATO

**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E
INDUSTRIAL**

**CARRERA DE INGENIERÍA EN SISTEMAS
COMPUTACIONALES E INFORMÁTICOS**

TEMA:

**“SISTEMA DE ANÁLISIS Y CONTROL DE RED DE DATOS & VoIP PARA
EL GOBIERNO PROVINCIAL DE TUNGURAHUA”**

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN:

Redes de Computadoras

AUTOR: Franklin Edmundo Escobar Vega
TUTOR: Ing. David Omar Guevara Aulestia Mg.

Ambato - Ecuador
Diciembre, 2015

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

“SISTEMA DE ANÁLISIS Y CONTROL DE RED DE DATOS & VoIP PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA.”, del señor Franklin Edmundo Escobar Vega, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Diciembre de 2015

EL TUTOR

Ing. David O. Guevara A., Mg.

AUTORÍA

El presente trabajo de investigación titulado: “SISTEMA DE ANÁLISIS Y CONTROL DE RED DE DATOS & VoIP PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA”. Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Diciembre 2015

Franklin Edmundo Escobar Vega

CC: 0503474827

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, Diciembre de 2015

Franklin Edmundo Escobar Vega

CC: 0503474827

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. K. Renato Urbina e Ing. Jaime Ruiz, revisó y aprobó el Informe Final del trabajo de graduación titulado “SISTEMA DE ANÁLISIS Y CONTROL DE RED DE DATOS & VoIP PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA”, presentado por el señor Franklin Edmundo Escobar Vega de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. Vicente Morales L., Mg.

PRESIDENTE DEL TRIBUNAL

Ing. K. Renato Urbina
DOCENTE CALIFICADOR

Ing. Jaime Ruiz
DOCENTE CALIFICADOR

DEDICATORIA

A Dios, por haberme permitido llegar hasta este punto y haberme dado la salud, la sapiencia, la paciencia, la constancia, para lograr mis objetivos, además de su infinita bondad y amor.

A Mi Padre Edmundo, al mejor de los padres por nunca dejar de apoyarme y ser un ejemplo para mí de lucha constancia, perseverancia ante las adversidades de la Vida, por estar en todo momento a mi lado, por ser el mejor.

A mi Madre Yolanda, por ser la persona que ha depositado en mí todos valores de la vida, por compartir día tras día tú amor, comprensión y ternura hacia mí.

A mi Hermana Carmen del Rocío, por ser mi amiga, la persona que siempre esta ahí para apoyarme en las buenas, en las malas y más aún por que siempre seremos inseparables querida hermana.

A ti, que me escuchas en Tú corazón, te dedico este triunfo por que siempre serás una de las personas más importantes de mí Vida.

Franklin Edmundo Escobar Vega

AGRADECIMIENTO

Agradezco de la manera más sincera a mi tutor de Tesis, Ingeniero David Guevara A., por haber compartido, sus bastos conocimientos, su manera de trabajar, la persistencia, sobre todo la paciencia y motivación que han inculcado en mí la responsabilidad académica para tener una formación profesional completa, de lo cual quedo agradecido y siempre tendrá en mí un voto de admiración hacia su persona.

Al Departamento de TI del Honorable Consejo Provincial de Tungurahua en especial a los Ingenieros Francisco López Administrador del Área de TI, Ricardo Domínguez encargado del Área de Redes, por haberme dado la oportunidad trabajar con excelentes profesionales, por la apertura, el tiempo, los conocimientos para llegar a concluir mi tesis.

A mis grandes amigas y amigos, en especial a Cristian por ayudarme con las dudas que nunca faltó para concluir mi tesis, por el tiempo, la paciencia, y por sus conocimientos compartidos gracias por todo.

A todos mis maestros que a lo largo de mi carrera Universitaria en la FISEI han dejado huella con sus enseñanzas, conocimientos para dejar en alto de dónde somos y hacia dónde vamos.

Franklin Edmundo Escobar Vega

ÍNDICE

APROBACIÓN DEL TUTOR	ii
AUTORÍA	iii
DERECHOS DE AUTOR	iv
APROBACIÓN COMISIÓN CALIFICADORA	v
Dedicatoria	vi
Agradecimiento	vii
Introducción	xix
CAPÍTULO 1 El problema	1
1.1 Tema de Investigación	1
1.2 Planteamiento del problema	1
1.3 Delimitación	2
1.4 Justificación	3
1.5 Objetivos	4
1.5.1 General	4
1.5.2 Específicos	4
CAPÍTULO 2 Marco Teórico	5
2.1 Antecedentes Investigativos	5
2.2 Fundamentación teórica	7
2.2.1 Políticas de la Gestión de Redes.	7
2.2.2 Monitoreo de Redes.	9
2.2.3 Objetivos del Monitoreo de Redes	9
2.2.4 Arquitectura de la Administración y Monitoreo de Redes .	9
2.2.5 Enfoque del Monitoreo.	11
2.2.6 Clasificación de Procesos de Monitoreo	11
2.2.7 Monitoreo Activo	11

2.2.8	Monitoreo Pasivo	11
2.2.9	Elementos involucrados en la Administración y Monitoreo de Red	13
2.2.10	SNMP (Simple Network Management Protocol - Protocolo Simple De Administración De Red)	14
2.2.11	EL PROTOCOLO SNMP	15
2.2.12	Proceso de envío de un Mensaje de SNMP	15
2.2.13	Versiones de SNMP	16
2.2.14	BASE DE INFORMACIÓN DE GESTIÓN (MIB)	17
2.2.15	Especificaciones de la Base de Información de Gestión (MIB)	17
2.2.16	Grupos de la Base de Información de Gestión (MIB)	18
2.2.17	Estructura de la Base de Información de Gestión (MIB)	19
2.2.18	Base de Información de Gestión II (MIB-II)	20
2.2.19	Notación de Sintaxis ASN.1(Abstract Notation One).	21
2.2.20	Servidor	21
2.2.21	Punto de Acceso Inalámbrico (WAP o AP)	22
2.2.22	Conmutador o Switch	22
2.2.23	Cortafuegos o Firewall	23
2.3	Propuesta de Solución	23
CAPÍTULO 3 Metodología		24
3.1	Modalidad Básica de la investigación	24
3.2	Población y muestra	24
3.3	Recolección de información	24
3.4	Procesamiento y análisis de datos	24
3.4.1	Procesamiento de la Información	24
3.5	Desarrollo del Proyecto	25
3.6	Análisis de Datos	25
CAPÍTULO 4 Desarrollo de la propuesta		27
4.1	Establecidos los puntos críticos de la Red de Datos & VoIP se podrá diseñar mecanismos para obtener información detallada de la Red Informática.	27
4.2	Determinar las herramientas Open Source que cumplan los requerimientos específicos para el monitoreo adecuado de la Red de Datos & VoIP.	29
4.3	Realizar un modelado de escenarios de carga crítica en la Red de Datos y Analizar los datos obtenidos.	40

4.4	Implementar la herramienta Open Source en los equipos en Producción del HGPT.	70
4.5	Tomar desiciones adecuadas para resolver problemas que se observan en la Red de Datos & VoIP.	80
4.6	Optimizar los recursos de Red de Datos & VoIP del Gobierno Provincial de Tungurahua.	80
	CAPÍTULO 5 Conclusiones y Recomendaciones	82
5.1	Conclusiones	82
5.2	Recomendaciones	83
	Bibliografia	84
	ANEXOS	88

ÍNDICE DE TABLAS

1	Mensajes utilizados en SNMP.	15
2	Niveles de Registro de un MIB	20
3	Cuadro Cualitativo de Herramientas para el Monitoreo de Redes.	35
4	Cuadro Cualitativo de Herramientas para el Monitoreo de Redes.	36
5	Criterio de Evaluación[1].	37
6	Cuadro Cuantitativo de Herramientas para el Monitoreo de Redes.	38
7	Cuadro Cuantitativo de Herramientas para el Monitoreo de Redes.	39
8	Tabla de Sistemas Operativos.	41
9	Tabla de Sistemas Operativos Virtualizados.	42
10	Tabla de Características de Sistemas Operativos Virtualizados.	42
11	Tabla de Configuración de VirtualHost.	43
12	Tabla de Configuración de Usuario Anonymous.	44
13	Tabla de Configuración de WordPress.	44
14	Tabla de Configuración de Archivo Dnsmasq.	45
15	Tabla de Servidores en Producción del HGPT.	73

ÍNDICE DE FIGURAS

1	Representación de los bloques para un modelo de políticas simple[2].	8
2	Elementos principales de un modelo de gestión de red basado en políticas[2].	8
3	Arquitectura de la Administración de Redes[3].	10
4	Componentes de la Administración y Monitoreo de Redes[3]. . . .	13
5	Arquitectura del Modelo SNMP [4].	14
6	Estructura MIB[3].	19
7	Puntos Críticos en la Red de Datos & VoIP del HGPT.	28
8	Topología de Red del HGPT, para la Simulación de la Carga Datos.	40
9	Escenario de Simulación de Carga de Datos para el HGPT.	41
10	Configuración de Iptables.	45
11	Configuración de Finalizada de Espacio Final.	47
12	Instalación de Sistema Operativo en Modo Gráfico.	47
13	Programas a Instalar.	48
15	Interfaz de Debian 7 i386.	49
14	Instalación Completa del Sistema Operativo.	49
16	Configuración Servicio SNMP - SNMPOPTS.	50
17	Configuración del Archivo Servicio SNMPD.	51
18	Configuración del Archivo SNMPD en el Cliente CentOS.	52
19	Instalar Protocolo SNMP en Windows.	53
20	Configuro Capturas de SNMP en Windows.	53
21	Configuro Seguridad SNMP en Windows.	54
22	Interfaz de Instalación de Zenoss.	55
23	Configuración para Funcionamiento de Zenoss.	55
25	Pantalla DashBoard de Zenoss.	56
24	Agregar Dispositivos.	56
26	Agregar Dispositivos a Monitorear.	59
27	Dispositivos de forma Manual.	59
28	Dispositivos Agregados.	60
29	Agregar Múltiples Dispositivos.	60

30	Descubrimiento de Dispositivos.	61
31	Dispositivos Agregados.	61
32	Descripción del Dispositivos	62
33	Agregar Usuarios.	63
34	Configuración de Usuarios.	64
35	Usuario y Email.	64
36	Configuración para Alerta de Correo Electrónico.	65
37	Configuración de Alerta de Usuario.	65
38	Añadir Alerta.	66
39	Definir ID para la Alerta.	66
40	Configuración de Alerta de Usuario.	67
41	Añadir servicio a Http.	67
42	Lista de Dispositivos.	68
43	Servicio Http.	68
44	Estado del servicio http en CentOS.	69
45	Verificar el servicio http en CentOS.	69
46	Verificar el servicio http en CentOS.	70
47	Alerta de Correo Electrónico.	70
48	Ingreso a Zenos.	71
49	Consola de Eventos del HGPT.	71
50	Historial de Eventos.	72
51	Historial de Eventos.	72
52	Transmisión de paquetes en la BBNR.	74
53	Transmisión de Paquetes en la BBNR.	75
54	Error en la Transmisión de Paquetes en la BBNR.	75
55	Uso del Sistema de Archivos raíz en el Servidor Web de Mapas.	76
56	Uso del Sistema de Archivos del Servidor Web de Mapas.	76
57	Carga de Datos hacia el Servidor Web de Mapas.	77
58	Carga de Datos hacia el Servidor de Recursos Hídricos.	78
59	Uso del CPU en el Servidor de Recursos Hídricos.	78
60	Uso de Memoria en el Servidor de Recursos Hídricos.	79
61	Lectura y Escritura en Disco del Servidor de Recursos Hídricos.	79

Resumen

El análisis de la Red de Datos y VoIP del Honorable Gobierno Provincial de Tungurahua se procedió a realizar la entrevista a los Ingenieros: Francisco López Jefe de TI, Ricardo Dominguez encargado del Área de Redes, de esta manera se logro tener el conocimiento necesario del funcionamiento actual y de la infraestructura de TI del HGPT.

Mediante el análisis de la entrevista se logró levantar los requerimientos y establecer los puntos críticos de la Red de Datos y VoIP del HGPT, a nivel Gerencial de Sistemas, de la misma manera a nivel de Red Datos y VoIP, lo cual ayuda acertadamente al cumplimiento de los requerimientos necesitados por la entidad mencionada.

En cuanto a la determinación de las Herramientas Open Source idóneas para el monitoreo de Redes se analizó varias en las cuales se observó las diferentes presentaciones de cada una de ellas, teniendo como mejor herramienta para el monitoreo Zenoss, esta herramienta es una aplicación de monitoreo de código abierto es una plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope.

Una vez implementada herramienta Zenoss en el escenario de Datos de carga crítica el cual consta diferentes servicios, se logró apreciar el consumo de recursos de la Red de Datos Local, analizado los datos se implementó en un servidor Debian con la herramienta Zenoss en el Departamento de TI del Honorable Gobierno Provincial de Tungurahua, lo cual ayuda a tener el monitoreo de los equipos en producción en tiempo real.

Abstract

The analysis of the Data Network and VoIP Honorable Gobierno Provincial de Tungurahua proceeded to conduct the interview Engineers: Francisco Lopez Head of IT, Ricardo Dominguez Area Network Manager, achieving in this way have the necessary knowledge of the current operation and infrastructure of HGPT.

By analyzing the interview raise achievement requirements and establish the critical points of the Data Network and VoIP HGPT, Systems management level, just as at the level of Network Data and VoIP, which helps accurately compliance requirements needed by the named entity.

As for determining the best Open Source tools for monitoring networks in which several different presentations of each was analyzed and observed, with the best tool for Zenoss monitoring, this tool is a monitoring application Open Source, which is a platform for network management and server based on the Zope application server.

Once deployed Zenoss tool on the stage of critical load data which has different services, we were able to appreciate the resource consumption of local area network, data analyzed was implemented on a Debian server with the Zenoss tool in the Department iT “Honorable Gobierno Provincial de Tungurahua”, which helps to keep the monitoring equipment in real-time production.

Glosario de Términos

- SNMP Protocolo simple de monitoreo de Redes, usado para administrar la configuración de dispositivos de red en una estación de trabajo.
- MIB Base de Información de Administración es una colección de información que ordena en forma de árbol donde se registran las variables a monitorear.
- OID Identificador de Objetos, el cual lleva una única llave para seleccionar un dispositivo.
- ASN1 Notación de Sintaxis Abstracta 1 es el lenguaje utilizado para definir tipos de datos.
- Agente SNMP Programa que permite a un dispositivo responder a solicitudes SNMP.
- Solicitud SNMP Solicitudes enviadas o recibidas por una entidad administradora estas pueden ser Get, Set Trap, etc.
- BER Reglas Básicas de Codificación es un conjunto de reglas para traducir valores ASN1 a un flujo de octetos para transmitir por la red.
- NMS Red de administración de la estación de red encargada de gestionar varios dispositivos de red.
- PDU Protocolo de Unidad de datos define la estructura de la información que va a ser enviada por la red.
- ALERTA Poner alerta o avisar de un peligro o de una amenaza.
- DESCUBRIMIENTO Define al proceso por el cual la información del sistema reúne información sobre los dispositivos de la infraestructura. Los resultados de los descubrimientos se utilizan para rellenar el modelo.
- PROTOCOLO Protocolo de red se utiliza en el contexto de la informática para nombrar a las normativas y los criterios que fijan cómo deben comunicarse los diversos componentes de un cierto sistema de interconexión. Esto quiere decir que, a través de este protocolo, los dispositivos que se conectan en red pueden intercambiar datos.

- ARQUITECTURA INFORMÁTICA Es el diseño conceptual y la estructura operacional fundamental de un sistema de Computadora. Es decir, es un modelo y una descripción funcional de los requerimientos y las implementaciones de diseño para varias partes de una computadora, con especial interés en la forma en que la unidad central de proceso (UCP) trabaja internamente y accede a las direcciones de memoria. También suele definirse como la forma de seleccionar e interconectar componentes de hardware para crear computadoras según los requerimientos de funcionalidad, rendimiento y costo.
- OSI Siglas que significan Open Systems Interconnection o Interconexión de Sistemas Abiertos. Es un modelo o referente creado por la ISO para la interconexión en un contexto de sistemas abiertos. Se trata de un modelo de comunicaciones estándar entre los diferentes terminales y host. Las comunicaciones siguen unas pautas de siete niveles preestablecidos que son Físico, Enlace, Red, Transporte, Sesión, Presentación y Aplicación.
- ICMIP El Protocolo de administración de información común (CMIP) es un protocolo de administración de red que define la comunicación entre las aplicaciones de administración de red y la gerencia de los agentes.
- TCP/IP Es una denominación que permite identificar al grupo de protocolos de red que respaldan a Internet y que hacen posible la transferencia de datos entre redes de ordenadores. En concreto, puede decirse que TCP/IP hace referencia a los dos protocolos más trascendentes de este grupo: el conocido como Protocolo de Control de Transmisión (o TCP) y el llamado Protocolo de Internet (presentado con la sigla IP).
- LAMP (Linux-Apache-MySQL- PHP/Python/PERL). El término hace referencia al sistema creado por la conjunción de esas aplicaciones libres (de código abierto). Este grupo de aplicaciones generalmente son usados para crear servidores web.
- DNS El sistema de nombres de dominio, más comúnmente conocido por sus siglas en inglés como Domain Name System o DNS, es básicamente es el encargado de traducir las complicadas series de números que conforman una dirección IP en palabras que el usuario pueda recordar fácilmente.
- DISPONIBILIDAD La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben

acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

- PLUGIN es aquella aplicación que, en un programa informático, añade una funcionalidad adicional o una nueva característica al software. En nuestro idioma, por lo tanto, puede nombrarse al plugin como un complemento.

INTRODUCCIÓN

El presente Trabajo Estructurado de Manera Independiente denominado: "SISTEMA DE ANÁLISIS Y CONTROL DE RED DE DATOS & VoIP PARA EL GOBIERNO PROVINCIAL DE TUNGURAHUA" para un mejor entendimiento, se lo ha dividido en los siguientes capítulos:

CAPÍTULO I denominado "EL PROBLEMA", identifica el problema de la Red de Datos y VoIP del Honorable Gobierno Provincial de Tungurahua HGPT, una justificación de la implantación de un modelo funcional y de políticas de administración en el sistema de transmisión actual, además del establecimiento de objetivos que plantean opciones para mejorar la gestión que realizan los administradores de red.

CAPÍTULO II denominado "MARCO TEÓRICO", muestra las investigaciones previas que sirven de soporte a la investigación, la información de estudios similares anteriormente realizados, además de los aspectos conceptuales que sustentan el tema en general, y el conjunto de conceptos y fundamentos teóricos que han sido analizados en base al problema establecido.

CAPÍTULO III denominado "METODOLOGÍA", define el tipo de investigación que ha sido desarrollada, el tratamiento de los procesos que señala la modalidad de investigación, así mismo se presenta el tipo de análisis de los datos según el tipo de investigación.

CAPÍTULO IV denominado "DESARROLLO DE LA PROPUESTA", determina una extensa información sobre el tema investigado en donde se detalla los puntos críticos, se determina conceptualmente la herramientas a ser analizadas, el modelado de escenarios, conceptos sobre las herramientas, los servicios, instalación, manipulación de la Herramienta Open Source Zenoss.

CAPÍTULO V denominado "CONCLUSIONES Y RECOMENDACIONES", expone de forma clara y concisa las consideraciones mas relevantes que se han

obtenido al finalizar el proyecto, además se indican recomendaciones que servirán de apoyo para el desarrollo del mismo.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

“Sistema de Análisis y Control de Red de Datos & VoIP para el Gobierno Provincial de Tungurahua”.

1.2. Planteamiento del problema

El mundo actualmente enfrenta a drásticos cambios y a una evolución permanente, ante lo cual es indispensable actualizar los procedimientos usados, a fin de efectivizar la utilización de recursos, haciendo que los sistemas organizacionales sean más robustos, sin embargo a más de la fiabilidad y robustez del hardware es necesario el buen diseño de ambos, la omisión de ello implica repercusiones negativas a las empresas, sean estas públicas o privadas, generando complicaciones tales como el aumento de costos no previstos, la disminución del nivel de servicio organizacional y el deterioro del ambiente laboral, esto debido a que no se cuenta con los recursos adecuados, que permitan evaluar y diagnosticar el tráfico de la red produciendo una crisis en su desempeño, e interrupciones de importantes servicios del negocio.

El monitoreo de red se va constituyendo en una labor continua, esto debido a que la infraestructura de red requiere de una permanente supervisión de todos los componentes que intervienen en el complejo proceso de transmisión de datos; componentes tales como: switches, routers, firewall, servidores, tarjetas de red, computadores, dispositivos móviles, etc., con el propósito de conocer oportunamente situaciones críticas como interrupciones de servicios, ataques a dispositivos, tráfico anómalo o comportamientos dentro de la red que requieren de la intervención del encargado para evitar colapsos o saturaciones que puedan poner en riesgo la continuidad del servicio.

Según Ariel Armijos Guevara, en su artículo menciona, que en el Ecuador la mayoría de la empresas carecen de un efectivo monitoreo de sus redes, en tal

razón se puede determinar que las empresas no tienen sistemas o herramientas de seguridad robustas que le permitan monitorear y gestionar de manera rápida y oportuna cuando estas reciban ataques por agentes externos que buscan llevarse información valiosa de la empresa [5].

Ante lo cual se ven imposibilitados a tener un adecuado control de sus redes, pues no están en la capacidad de realizar un exhaustivo monitoreo del tráfico de red y mucho menos de contar con un eficiente historial de eventos de sucesos, esto ha determinado que no se puedan identificar de manera rápida las posibles causas y fallas de los servicios, lo que conlleva a la búsqueda de solución tardías y como consecuencia al colapso de la red, todo esto debido no solo a la escasez de recursos sino también al desconocimiento de los métodos y técnicas actualmente utilizadas para tal efecto.

La mayoría de Gobiernos Provinciales de nuestro país actualmente no cuentan con una herramienta que permita mantener un constante control y vigilancia de toda la red. El Gobierno Provincial de Tungurahua no es la excepción pues si bien es cierto cuenta con una adecuada estructuración de Red Interno lamentablemente carece de un eficiente sistema que permita monitorear, diagnosticar y establecer las posibles soluciones que podrían presentarse como anomalías propias de una Red, ocasionando el empleo innecesario de equipos lo que da origen a grandes pérdidas económicas pues se incrementan los costos de mantenimiento debido a la disminución significativa del espacio de almacenamiento y al consumo inadecuado el ancho de banda.

1.3. Delimitación

Área Académica:

Redes y Hardware.

Línea de Investigación:

Tecnologías de la Información.

Sub Línea de Investigación:

Redes de Computadoras.

Delimitación Espacial:

La presente investigación se realizará en el Gobierno Provincial de Tungurahua.

Delimitación Temporal:

La presente investigación se desarrollará en 6 meses posteriores a la aprobación del proyecto por parte del H. Concejo Directivo de la Facultad de Ingeniería en

Sistemas, Electrónica e Industrial.

1.4. Justificación

El presente proyecto involucra aspectos eminentemente relacionados con los conocimientos adquiridos, los mismos que posteriormente serán puestos en práctica a nivel profesional, en tal razón, la investigación es de gran interés, pues también permitirá tomar decisiones eficientes y consecuentemente disminuir el empleo de recursos ciertamente innecesarios en el Gobierno Provincial de Tungurahua.

La realización del presente proyecto evidencia su gran importancia, debido a que el Departamento de Sistemas del Gobierno Provincial de Tungurahua actualmente carece de un adecuado monitoreo de sus Datos & VoIP, ante lo cual se puede observar una significativa disminución del tráfico de datos procesados por dicha Institución diariamente, en tal virtud se plantea la propuesta de implementar una herramienta Open Source.

Así también se podrá promover el uso de herramientas Open Source en el Gobierno Provincial de Tungurahua, con el afán, de innovar el esquema tradicional manejado hasta la actualidad, esto atendiendo al decreto presidencial mismo que textualmente dispone “Establecer como política pública para las Entidades de la Administración Pública Central la utilización de Software Libre en sus sistemas y equipamientos informáticos”.

Se beneficiará por una parte el Gobierno Provincial de Tungurahua ya que mejorará los tiempos de ejecución de los procesos internos y por otra parte la ciudadanía en general pues se observará mayor fluidez en los trámites realizados en dicha entidad, así también se podrá satisfacer los requerimientos establecidos por el Departamento de Sistemas en el Área de Redes para el cumplimiento de sus diferentes actividades.

Evidentemente el impacto de este proyecto será positivo pues la ejecución del mismo permitirá minimizar el empleo de recursos y optimizar los tiempos aplicando conocimientos perfectamente fundamentados y con la suficiente argumentación científica, en tal virtud tendrá una gran utilidad práctica porque además permite plantear una alternativa de solución al presente problema.

Este proyecto es factible realizar pues se cuenta con toda la predisposición de

los involucrados es decir autoridades y funcionarios, lo cual manifiesta su interés por el mejoramiento continuo y la optimización de los servicios prestados por tan importante dependencia del estado, así también se cuenta con los medios necesarios para la correcta implementación y aplicación de esta herramienta de análisis y control de Redes.

1.5. Objetivos

1.5.1. General

Establecer un Sistema de Análisis y Control de Red de Datos & VoIP para la optimización de los recursos informáticos empleados en el Gobierno Provincial de Tungurahua.

1.5.2. Específicos

- Analizar el estado actual de la Red Datos & VoIP del Gobierno Provincial de Tungurahua.
- Establecer los puntos críticos de la Red de Datos & VoIP del Gobierno Provincial de Tungurahua.
- Determinar herramientas Open Source más idóneas para el monitoreo adecuado de la Red de Datos & VoIP del Gobierno Provincial de Tungurahua.
- Realizar un modelado de escenarios de carga crítica en la Red de Datos del Gobierno Provincial de Tungurahua.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Con el aparecimiento de la Informática, la evolución y revolución tecnológica se han fusionado también diferentes áreas científicas-tecnológicas, como son los Sistemas Informáticos y las Redes de Comunicación, en vista de ello las necesidades de incrementar y mejorar el uso de redes de información ha provocado que la administración, control y monitoreo de las mismas sea un factor predominante en el campo de las comunicaciones entre los diferentes Sistemas Informáticos, es por ello necesario la utilización de una herramienta, que posibilite el monitoreo y administración adecuada del tráfico de datos en redes LAN.

El trabajo de grado desarrollado por Luis Alberto Del Pozo Guevara aborda el problema que genera la necesidad de disponibilidad de redes basada en un monitoreo que ayude a manejar más eficientemente el ancho de banda de la red interna de la organización evitando o minimizando el uso de aplicaciones no permitidas a través de esta. Dicho problema es más crítico ya que con el desarrollo de la Internet, el mercado globalizado y crecimiento tecnológico de la empresas, más el gran volumen de información que fluye a través de estas, las organizaciones deben estar más preparadas para asegurar que la información que fluye a través de su red, así como sus aplicaciones, tengan una mayor disponibilidad y performance frente aplicaciones no deseadas que pueden estar circulando por la red [6].

Por lo expuesto anteriormente se evidencia el nivel de importancia de este tema pues ha sido de gran utilidad no solo para diagnosticar el estado actual de los sistemas de monitoreo de redes en otros países sino también para tomar medidas necesarias y respectivas en caso de presentarse anomalías, y consecuentemente proporcionar un mejor servicio minimizando el impacto en las operaciones de cada una de las organizaciones tanto públicas como privadas incrementando cada vez más la fiabilidad del hardware.

Así también en la Revista Electrónica manifiesta, la gestión de redes se extiende más allá de su conocimiento global lógico, a nivel técnico se debe disponer de una documentación del entramado y la forma más fiel de representar configuración de red es seguir paso a paso la interconexión entre los equipos que la componen y ofrecer la visión real de las instalaciones. Existen plataformas de gestión integradas con aplicaciones en común como el Protocolo Sencillo de Administración de Redes (SNMP) para la administración de redes estándar utilizadas en Internet [7].

En consecuencia el protocolo SNMP, tiene gran importancia en la Gestión de la Redes, pues permite la comunicación de un administrador con un agente, es decir define el formato y el significado de los mensajes que intercambian, permite de esta manera monitorear y controlar redes que operan sobre TCP/IP, así también capturar y alterar información de la red, para su posterior diagnóstico y corrección de problemas en la red.

El artículo tomado de IEEE LATIN AMERICA TRANSACTIONS, Arquitectura de referencia de gestión de red basada en políticas para un Entorno Integrado 3G-WLAN, manifiesta, por lo general, los modelos de gestión de red tradicionales están principalmente enfocados en el monitoreo y no en el control, y por lo tanto no se pueden cubrir las necesidades de este nuevo entorno de red heterogéneo. La gestión de red basada en políticas se presenta como una solución viable a estos nuevos retos. Esta tecnología de gestión está enfocada en la generación de un entorno de gestión de red autónomo que permita la operación de los recursos de red mediante la definición de una serie de reglas que dinámicamente configuradas puedan alcanzar ciertas metas y reaccionar en forma automática a los diferentes entornos de operación[2].

Un adecuado modelo de gestión de red en las organizaciones hará del monitoreo una tarea menos complicada y más eficientemente evitando como consecuencia el empleo de recursos innecesarios (humanos y económicos); y minimizando el uso de aplicaciones no permitidas a través de esta, lo que facilitará también su crecimiento tecnológico mediante un óptimo procesamiento del volumen de información que fluye a través de estas, obteniendo una mayor disponibilidad y performance frente aplicaciones no deseadas que pueden estar circulando por la red.

Por último haciendo referencia al Artículo desarrollado por Ariel Armijos Gueva-

ra y Luis Villamar Lavay alumnos de la Carrera de Licenciatura en sistemas de información gerencia de la Escuela Superior Politécnica del Litoral, manifiestan que uno de los temas más importantes son los datos y la información sensible que tenemos en nuestra empresa mismos que pueden ser usados como ayuda para a mejorar la rentabilidad de la misma[5].

Se hace referencia a la importancia de establecer estrategias y métodos que materialicen las políticas de seguridad que tiene las empresas, de esa manera podremos optimizar el uso eficiente de los sistemas de información y de redes, todo esto considerando que son entes importantes para el adecuado procesamiento de datos entre las diferentes áreas o dependencias de una empresa.

2.2. Fundamentación teórica

2.2.1. Políticas de la Gestión de Redes.

En los últimos años se han realizado esfuerzos para generar un modelo de gestión de red basado en políticas. Una política es un conjunto de directivas o reglas especificadas por el administrador para gestionar ciertos aspectos de los resultados deseados de las interacciones entre usuarios, entre aplicaciones, y entre usuarios y aplicaciones. Las políticas proporcionan las guías para especificar cómo los diferentes elementos de red, por ejemplo enrutadores, conmutadores, servidores, cortafuegos, deberían manejar el tráfico generado por los diferentes usuarios y aplicaciones. Cada política está formada, como mínimo, por una cláusula de condición y una cláusula de acción[8]. Si la cláusula de condición es verdadera entonces las acciones definidas en la cláusula acción son ejecutadas. La Figura 1 presenta las clases y relaciones que definen la semántica de la construcción de bloques de representación de políticas. Los bloques de una política definen un conjunto de eventos que sirven como activadores de la ejecución de la política, además de un conjunto de condiciones que debe de cumplir el evento y las acciones a llevar a cabo si las condiciones se cumplen[2].



Figura 1: Representación de los bloques para un modelo de políticas simple[2].

La Figura 2 muestra la arquitectura de políticas definida por el IETF y las entidades principales que la componen. La herramienta de gestión de políticas es el componente utilizado por el administrador de red para definir el conjunto de políticas que estarán activas en la red. Todas las políticas generadas por la herramienta de gestión se almacenan dentro de un contenedor de políticas (PR – Policy Repository). Los dispositivos responsables de la aplicación y ejecución de las diferentes políticas se conocen como Punto de Aplicación de Política (PEP – Policy Enforcement Point).

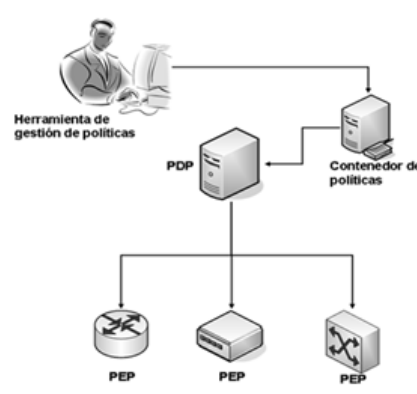


Figura 2: Elementos principales de un modelo de gestión de red basado en políticas[2].

Las políticas a ser aplicadas en cada uno de los elementos gestionados son seleccionadas por un elemento intermediario conocido como Punto de Decisión de Política (PDP – Policy Decision Point), el cual se comunica con el PR mediante algún protocolo como LDAP[9] y es responsable de interpretar las políticas almacenadas en el PR y proporcionar respuesta a las peticiones realizadas por el PEP. El PDP es el elemento principal de la arquitectura definida por el IETF y se encarga de desempeñar tres tareas básicas: realizar la consulta de las políticas

existentes en el contenedor, llevar a cabo la traducción de cada política al formato específico del dispositivo y distribuirlas a los PEPs de acuerdo a las peticiones realizadas. La comunicación entre el PDP y el PEP se lleva a cabo mediante el protocolo COPS (Common Open Policy Service)[10].

2.2.2. Monitoreo de Redes.

Monitoreo de una red activa de comunicaciones sirve para diagnosticar problemas y recopilar estadísticas por la administración y ajustamiento de la red.

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de cómputo son actividades de gran relevancia para brindar un buen servicio a los usuarios. De esto se deriva la importancia de contar con un esquema capaz de notificarnos las fallas en la red y de mostrarnos su comportamiento mediante el análisis y recolección de tráfico. A continuación se habla sobre los enfoques activo y pasivo de monitoreo y sus técnicas, de esta manera se crea una estrategia de monitoreo incluyendo la definición de métricas y la selección de las herramientas[11].

2.2.3. Objetivos del Monitoreo de Redes

- Identificar la Información a monitorear.
- Diseñar mecanismos para obtener la información necesaria.
- Utilizar la información obtenida dentro de las distintas áreas funcionales de la administración de red.
- Tomar nuevas medidas sobre aspectos de los protocolos, colisiones, fallas, paquetes, etc.
- Almacenar la información obtenida en Base de Información de gestión para su posterior análisis.
- De análisis, obtener conclusiones para resolver problemas concretos o bien para optimizar la utilización de la red.

2.2.4. Arquitectura de la Administración y Monitoreo de Redes

La mayoría de las arquitecturas para la administración de redes utilizan la misma estructura y conjuntos básicos de relaciones. Las estaciones terminales, como los sistemas de cómputo y otros dispositivos de la red, utilizan un software que le permite enviar mensajes de alerta cuando se detecta algún problema. al

recibir estos mensajes de alerta las entidades de administración son programadas para reaccionar, ejecutando una o varias acciones que incluyen la notificación al administrador, al cierre del sistema, y un proceso automático para la posible reparación del sistema.

Las entidades de administración también pueden registrar la información de las estaciones terminales para verificar los valores de ciertas variables. Esta verificación puede realizarse automáticamente o ejecutada por algún administrador de red[3].

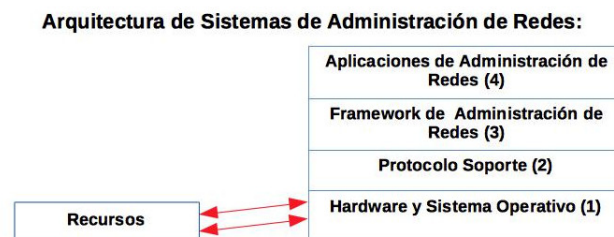


Figura 3: Arquitectura de la Administración de Redes[3].

- Hardware y el Sistema Operativo
- Protocolo de soporte, en el cual incluye:
 - Capas por debajo de la capa de aplicación en OSI, UDP/IP en Internet.
 - Protocolos de administración tales como SNMP, CMIP.
 - Conversión de diferentes protocolos y multi-protocolos que soporte protocolos heterogéneos.
 - Provee la base de varias aplicaciones de administración de redes:
 - Funciones de agente y administración.
 - Soporte de bases de datos tales como las base de datos relacionales y orientadas a objetos para almacenar datos de muchas funciones de administración de redes y soporte para aplicaciones.
 - Funciones de administración de redes, tales como configuración y administración de fallas.
 - Provee un mercado muy amplio y que tiene un potencial alto de producir aplicaciones innovadoras tales como aplicaciones de administración de negocios, aplicaciones de fácil uso para facilitar la tarea del administrador y aplicaciones de diagnóstico de fallas[3].

2.2.5. Enfoque del Monitoreo.

Existen, al menos, dos puntos de vista para abordar el proceso de monitorear una red: el enfoque activo y el enfoque pasivo. Aunque son diferentes ambos se complementan.

2.2.6. Clasificación de Procesos de Monitoreo

2.2.7. Monitoreo Activo

Este tipo de monitoreo se realiza inyectando paquetes de prueba en la red, o enviando paquetes a determinadas aplicaciones midiendo sus tiempos de respuesta. Este enfoque tiene la característica de agregar tráfico en la red. Es utilizado para medir el rendimiento en una red.

Técnicas del Monitoreo Activo

Basados en ICMP.

- Diagnosticar problemas en la red.
- Detectar retardo, pérdida de paquetes.
- RTT.
- Disponibilidad de host y redes.

Basados en TCP.

- Tasa de transferencia.
- Diagnosticar problemas a nivel aplicación.

Basados en UDP.

- Pérdida de paquetes en un sentido (one-way)
- RTT (traceroute)

2.2.8. Monitoreo Pasivo

Este enfoque se basa en la obtención de datos a partir de recolectar y analizar el tráfico que circula por la red. Se emplean diversos dispositivos como sniffers, ruteadores, computadoras con software de análisis de tráfico y en general dispositivos con soporte para snmp, rmon y netflow. Este enfoque no agrega tráfico en

la red como lo hace el activo. Es utilizado para caracterizar el tráfico en la red y para contabilizar su uso[11].

Técnicas de monitoreo pasivo

Solicitudes remotas

Mediante SNMP

Esta técnica es utilizada para obtener estadísticas sobre la utilización de ancho de banda en los dispositivos de red, para ello se requiere tener acceso a dichos dispositivos. Al mismo tiempo, este protocolo genera paquetes llamados traps que indican que un evento inusual se ha producido.

Otros métodos de acceso

Se pueden realizar scripts que tengan acceso a dispositivos remotos para obtener información importante para monitorear. En esta técnica se pueden emplear módulos de perl, ssh con autenticación de llave pública, etc.

Captura de tráfico

Se puede llevar a cabo de dos formas: 1) Mediante la configuración de un puerto espejo en un dispositivo de red, el cual hará una copia del tráfico que se recibe en un puerto hacia otro donde estará conectado el equipo que realizará la captura; y 2) Mediante la instalación de un dispositivo intermedio que capture el tráfico, el cual puede ser una computadora con el software de captura o un dispositivo extra. Esta técnica es utilizada para contabilizar el tráfico que circula por la red.

Análisis de Tráfico

Se utiliza para caracterizar el tráfico de la red, es decir, para identificar el tipo de aplicaciones que son más utilizadas. Se puede implementar haciendo uso de dispositivos probe que envíen información mediante RMON (Remote Network Monitoring - Norma basada en SNMP para informar diversas condiciones de red. RMON tiene 10 grupos diferentes de administración que proporciona información detallada sobre una red.) o a través de un dispositivo intermedio con una aplicación capaz de clasificar el tráfico por aplicación, direcciones IP origen y destino, puertos origen y destino, etc.

Flujos

También utilizado para identificar el tipo de tráfico utilizado en la red. Un flujo es un conjunto de paquetes con:

- La misma IP origen y destino
- El mismo puerto TCP origen y destino
- El mismo tipo de aplicación.

Los flujos pueden ser obtenidos de ruteadores o mediante dispositivos que sean capaces de capturar tráfico y transformarlo en flujos. También es usado para tareas de facturación (billing)[11].

2.2.9. Elementos involucrados en la Administración y Monitoreo de Red

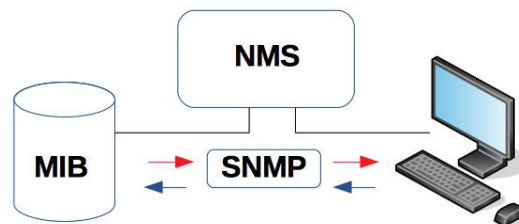


Figura 4: Componentes de la Administración y Monitoreo de Redes[3].

En donde:

- MIB (Base de Información Gestionada o del Ingles Management Information Base) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.
- NMS (Sistema de Gestión de Red o del Ingles Network Management System) que es una combinación de hardware y software utilizado para controlar y administrar una red de ordenadores o redes.
- SNMP (Protocolo Simple de Administración de Red o del inglés Simple Network Management Protocol) es un protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento[4].

2.2.10. SNMP (Simple Network Management Protocol - Protocolo Simple De Administración De Red)

El Protocolo simple de administración de redes (SNMP, Simple Network Management Protocol) es un protocolo ubicado en la capa siete del modelo OSI, facilita la administración de los equipos en la red, permitiendo a los administradores supervisar, encontrar y resolver problemas de una manera mucho más fácil y cómoda. El protocolo SNMP se ha convertido en un estándar de gestión de red sobresaliente y la mayoría de los equipos de interconexión (switches, routers, hubs, puentes) dispositivos de encaminamiento, estaciones de trabajo y Pcs ofrecen agentes SNMP para ser gestionados tal como se observa en la figura 5[3].

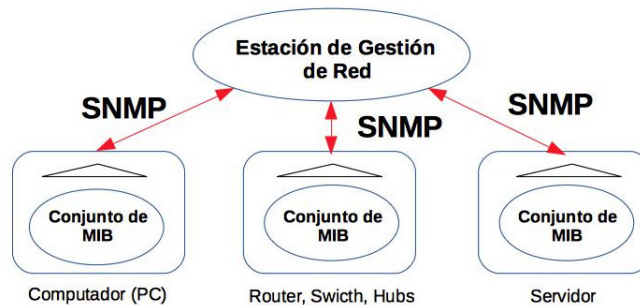


Figura 5: Arquitectura del Modelo SNMP [4].

SNMP proporciona un método de administración de hosts de redes como switch, puentes, enrutadores y equipos de servidor o estaciones de trabajo desde un equipo central donde se ejecuta software de administración de redes. SNMP realiza servicios de administración mediante una arquitectura distribuida de sistemas de administración y agentes. Puesto que la administración de redes es fundamental para la administración de recursos y auditoría, SNMP puede utilizarse para:

- Configurar dispositivos remotos.
- La información de configuración puede enviarse a cada host conectado a la red desde el sistema de administración.
- Supervisar el rendimiento de la red.
- Puede hacer un seguimiento de la velocidad de procesamiento y el rendimiento de la red, y recopilar información acerca de las transmisiones de datos.
- Detectar errores en la red o accesos inadecuados.

- Puede configurar las alarmas que se desencadenarán en los dispositivos de red cuando se produzcan ciertos sucesos.
- Cuando se dispara una alarma, el dispositivo envía un mensaje de suceso al sistema de administración. Entre las causas más frecuentes de alarma se incluye el cierre y reinicio de un dispositivo, un error de un vínculo detectado en un enrutador y un acceso inadecuado.
- Auditar el uso de la red.
- Puede supervisar el uso general de la red para identificar el acceso de un grupo o usuario, y los tipos de uso de servicios y dispositivos de la red.

2.2.11. EL PROTOCOLO SNMP

Está basado en el modelo Administrador/Agente, y utiliza un conjunto limitado de comandos y mensajes como lo indica la Tabla 1:

Tabla 1: Mensajes utilizados en SNMP.

Comando	Acción
Get-request	Solicita el valor de una variable de estado
Get-next-request	Solicita la siguiente variable
Get-bulk-request	Obtiene una tabla de valores de variables
Set-request	Actualiza una o más variables
Inform-request	Descripción de la MIB local
SNMPV2-trap	Informe de interrupción

Elaborado por: El Investigador.

2.2.12. Proceso de envío de un Mensaje de SNMP

El envío de mensajes SNMP se realiza por medio del siguiente proceso:

- Transmisión
 - Se constituye UPD
 - Se involucra el servicio de autenticación con la dirección de transporte.
 - Se construye el mensaje SNMP.
 - Se codifica.
- Recepción
 - Comprobación sintáctica.
 - Verificación de la versión utilizada.

- Autenticación, verifica si falla.
- Proceso de petición.
 - Mensaje SNMP
- Mensaje SNMP <—> Datagrama UPD
- Disminuye el procesado de mensajes y complejidad del agente[3].

2.2.13. Versiones de SNMP

Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

SNMP en su última versión (SNMPv3) posee cambios significativos con relación a sus predecesores, sobre todo en aspectos de seguridad, sin embargo no ha sido mayoritariamente aceptado en la industria[12].

SNMP v1

Esta versión fue muy simple y utiliza como método la autenticación basada en comunidades. Se define por arquitectura, física (gestor-agente), en la aparte de seguridad introduce el cifrado con clave pública y firma digital. La forma sencilla de autenticarse en esta versión por el método de comunidades son tipos de mensaje como: get, get-next , get-response , set-request y trap no tiene ninguna seguridad implementada[3].

- Fue diseñado a mediados de los 80.
- Lograr una solución temporal hasta la llegada de protocolos de gestión de red con mejores diseños y más completos.
- Se basa en el intercambio de información de red a través de mensajes (PDU's).
- No era perfecto, además no estaba pensado para poder gestionar la inmensa cantidad de redes que cada día iban apareciendo.

SNMP v2

Esta versión contiene mejoras en cuanto a SNMP v1, ha mejorado en los tipos de datos y operaciones, pero sigue quedando corto en cuanto a seguridad[3].

- Definida en 1993 y revisado en 1995
- Añade mecanismos de seguridad.

- Mayor detalle en la definición de las variables.
- Se añaden estructuras de la tabla de datos para facilitar el manejo de los datos.
- No fue más que un parche, es más hubo innovaciones como los mecanismos de seguridad que se quedaron en pura teoría, no se llegaron a implementar.

SNMP v3

Ofrece autenticidad e integridad utilizando claves de usuarios y mensajes con huellas digitales también ha mejorado en la privacidad al cifrar los mensajes y valida temporalmente sincronizando relojes y una ventana de 150 segundos con chequeo de secuencia[3].

- Desarrollado en 1998.
- A esta versión se le agregan los mecanismos de seguridad que no se llegaron a implementar en la versión anterior, los cuales son:

Integridad del Mensaje: asegura que el paquete no haya sido violado durante la transmisión.

Autenticación: determina que el mensaje proviene de una fuente válida.

Encriptación: encripta el contenido de un paquete como forma de prevención.

2.2.14. BASE DE INFORMACIÓN DE GESTIÓN (MIB)

Un MIB define un modelo conceptual de la información requerida para tomar decisiones de administración de red. La información que la MIB incluye tiene número de paquetes transmitidos, número de conexiones intentadas, datos de contabilidad entre otros [13].

Así también se puede decir que es una base de datos de objetos administrados que son accesibles por el agente y manipulados vía SNMP para lograr la administración de la red, es una información jerárquica estructurada en forma de árbol de todos los dispositivos gestionados en una red[3].

2.2.15. Especificaciones de la Base de Información de Gestión (MIB)

La MIB define tanto los objetos de la red operados por el protocolo de administración de red, como las operaciones que pueden aplicarse a cada objeto. La MIB no incluye información de administración para las aplicaciones Telnet,

FTP o SMTP, debido a los inconvenientes que se presentan al instrumentar aplicaciones de este tipo para la MIB por parte de las compañías fabricantes[13].

Para definir una variable u objeto para la MIB es necesario especificar lo siguiente:

Sintaxis: Especifica el tipo de variable, u valor entero, etc.

Acceso: Especifica el tipo de permiso como: Leer, leer y escribir, escribir, no accesible.

Estado: Define si la variable es obligatoria u opcional.

Descripción: Describe textualmente a la variable.

2.2.16. Grupos de la Base de Información de Gestión (MIB)

La MIB-1 define 126 objetos de administración, divididos en los siguientes grupos:

- Grupo de Sistemas

Usado para registrar información del sistema, por ejemplo:

Compañía fabricante del sistema.

Tipo de software.

Tiempo que el sistema ha estado operando.

- Grupo de Interfaces

Registra la información genérica acerca de cada interfaz de red, como el número de mensajes erróneos en la entrada y salida, el número de paquetes transmitidos y recibidos, el número de paquetes de broadcast enviados, MTU del dispositivo, etc.

- Grupo de traducción de dirección

Comprende las relaciones entre direcciones IP y direcciones específicas de la red de deben soportar, como la tabla ARP, que relaciona direcciones IP con direcciones físicas de la red LAN.

- Grupo IP

Almacena información propia de la capa IP, como datagramas transmitidos y recibidos, conteo de datagramas transmitidos y recibidos, conteo de datagramas erróneos, etc. También contiene información de variables de control que permite a las aplicaciones remotas ajustar el TTL (Time To Live) de omisión de IP y manipular las tablas de ruteo de IP.

- Grupo TCP

Este incluye información propia del protocolo TCP, como estadísticas del número de segmentos transmitidos y recibidos, información acerca de conexiones activa como dirección IP, puerto o estado actual.

- Grupo ICMP Y UDP

Lo mismo que el grupo IP y TCP.

- Grupo EGP

Este grupo se requieren sistemas (ruteadores) que soporten EGP (Protocolo de Gateway o Salida Exterior)[13].

2.2.17. Estructura de la Base de Información de Gestión (MIB)

Los objetos que guardan en la MIB tiene un identificados único. Este identificador de objeto se llama (OID) es una secuencia de números enteros no son negativos y están separados por puntos que salen de un árbol estandarizado mundialmente conformado ramas y nodos como lo indica la figura 6[3].

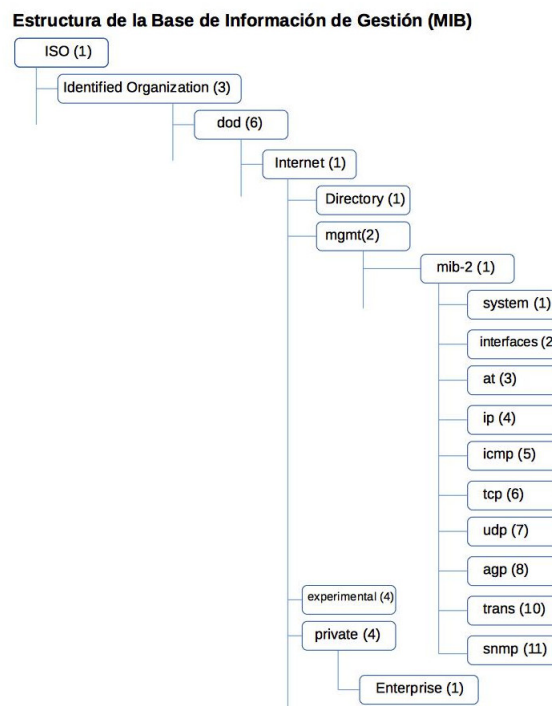


Figura 6: Estructura MIB[3].

Tiene 8 niveles de registro que son:

Tabla 2: Niveles de Registro de un MIB

GRUPO	VARIABLE	SIGNIFICADO
System (sys)	sysUpTime	Tiempo desde el Ultimo arranque.
Interfaces (intf)	ifNumber	Número de Interfaces.
Interfaces (intf)	ifInErrors	Número de paquetes entrantes en los que el agente ha encontrado error.
Address Translation(add trs)		Número de paquetes recibidos.
Internet Protocol (ip)	ipInReceives	
Internet Control Message (icmp)	icmpInEchos	Número de solicitudes ICMP.
Transmission Control Protocol (tcp)	tcpInSegs	Número de paquetes TCP.
User Datagram Protocol (udp)	udpInDatagrams	Número de datagramas UDP recibidos.

Elaborado por: El Investigador.

Las MIB están escritas utilizando las sintaxis ASN.1. Esta es utilizada para descubrir estructuras de datos que se definen para guardar la información de gestión. Luego que definimos las estructuras se debe definir la sintaxis de transferencia, para saber la forma en la que van hacer transmitidas los datos en la red; a esto se le conoce como las reglas de codificación básicas (BER). Es la codificación utilizada para la transmisión de información escrita en sintaxis ASN.1 a otras aplicaciones mediante una sintaxis que define y permite definir el formato de cómo se van a enviar los datos[3].

En el ASN.1 se definen tres tipo de objetos:

1. Tipos (Types) —> define nuevas estructuras de datos y comienzan en mayúsculas.
2. Valores (Values) —> son variables de un tipo y se escriben en minúsculas.
3. Macros —> usadas para cambiar la gramática y son escritas en mayúsculas.

2.2.18. Base de Información de Gestión II (MIB-II)

La MIB-II se crea para extender los datos de administración de red empleados en redes Ethernet y WAN (Wide Area Network) usando ruteadores para un enfoque a múltiples medios de administración en redes LAN y WAN[13].

Se agregan dos grupos:

- Grupo de Transmisión

Soporta múltiples tipos de medios de transmisión, como cable coaxial, cable UTP, cable de fibra de óptica y sistemas T1/E1.

- Grupo SNMP

Incluyen estadísticas sobre el tráfico de red SNMP.

2.2.19. Notación de Sintaxis ASN.1(Abstract Notation One).

La estructura de información de gestión Internet utiliza el estándar abstract para una información estructurada conocida como mensajes, es decir ASN.1 define elementos básicos del lenguaje y proporciona reglas para combinar estos elementos en los mensajes.

La ASN.1 especifica una gran cantidad de tipos de datos para diferentes aplicaciones, de los cuales, se tomaran en cuenta aquellos tipos de datos que se pueden ser utilizados en la definición de objetos de las MIBs. La ASN.1 define tipos básicos de datos, tales como enteros o caracteres y tipos nuevos de datos que están basados en combinaciones de los tipos básicos.

Se debe diferenciar dos términos que son estandarizados, la sintaxis abstracta la cual especifica la notación de los datos por medio del código ASN.1, y la sintaxis de transferencia la cual permite convertir las definiciones ASN.1, en un patrón de bits para que se puedan transmitir a los elementos de red, median la utilización de las reglas de codificación básica llamada BER(Basic Encoding Rules). Las reglas de codificación básicas son utilizadas para convertir la información de la MIB en formato que pueda ser entendido por el agente[14].

2.2.20. Servidor

El término servidor se dice a la aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia. Los servidores se pueden ejecutar en cualquier tipo de computadora, incluso en computadoras dedicadas a las cuales se les conoce individualmente como "El Servidor". En la mayoría de los casos una misma computadora puede proveer múltiples servicios y tener varios servidores en funcionamiento. La ventaja de montar un servidor en computadoras dedicadas es la seguridad. Por esta razón la mayoría de los servidores son procesos daemon diseñados de forma que puedan funcionar en computadoras de propósito específico.

Los servidores operan a través de una arquitectura cliente-servidor. Los servidores son programas de computadora en ejecución que atienden las peticiones de otros programas, los clientes. Por tanto, el servidor realiza otras tareas para beneficio de los clientes. Ofrece a los clientes la posibilidad de compartir datos, información y recursos de hardware y software. Los clientes usualmente se conectan al servidor a través de la red pero también pueden acceder a él a través de la computadora donde está funcionando. En el contexto de redes Internet Protocol (IP), un servidor es un programa que opera como oyente de un socket.

Comúnmente los servidores proveen servicios esenciales dentro de una red, ya sea para usuarios privados dentro de una organización o compañía, o para usuarios públicos a través de Internet. Los tipos de servidores más comunes son servidor de base de datos, servidor de archivos, servidor de correo, servidor de impresión, servidor web, servidor de juego, y servidor de aplicaciones.

2.2.21. Punto de Acceso Inalámbrico (WAP o AP)

Un punto de acceso inalámbrico (WAP o AP: Wireless Access Point) en redes de computadoras es un dispositivo que interconecta dispositivos de comunicación alámbrica para formar una red inalámbrica. Normalmente un WAP también puede conectarse a una red cableada, y puede transmitir datos entre los dispositivos conectados a la red cable y los dispositivos inalámbricos. Muchos WAPs pueden conectarse entre sí para formar una red aún mayor, permitiendo realizar "roaming" (itinerancia).

2.2.22. Conmutador o Switch

Un conmutador o switch es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes de red, pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las redes de área local.

2.2.23. Cortafuegos o Firewall

Un cortafuegos (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas.

Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través del cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuegos a una tercera red, llamada «zona desmilitarizada» o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un cortafuegos correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

2.3. Propuesta de Solución

Establecer una aplicación de monitoreo de Red de Datos & VoIP para el Gobierno Provincial de Tungurahua, utilizando el protocolo SNMP (Simple Network Management Protocol), a fin de poder analizar y controlar eficazmente el procesamiento de datos.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la investigación

El presente trabajo tiene las siguientes modalidades:

Modalidad de Campo

La investigación tendrá la modalidad de campo porque el investigador acudirá al lugar en donde se producen los hechos para obtener información relacionada con los objetivos del trabajo de grado. Las técnicas a ser utilizadas serán: entrevistas y la observación.

Modalidad Bibliográfica o Documentada

La investigación bibliográfica tendrá como propósito fortalecer la investigación se recurrirá a obtener investigación teórica de diferentes autores obtenidas en fuentes secundarias (Libros, revistas especializadas, publicaciones, internet, otros) y de ser necesario fuentes de información primaria a través de documentos válidos y confiables.

3.2. Población y muestra

La presente investigación por su característica no requiere población ni muestra, por tal motivo no se aplica.

3.3. Recolección de información

Para la recolección de la Información se usará diferentes metodologías como son entrevistas al personal que está a cargo del departamento de Sistemas del Gobierno Provincial de Tungurahua en especial al personal encargado del Área de Redes.

3.4. Procesamiento y análisis de datos

3.4.1. Procesamiento de la Información

Para el procesamiento de la información se realizará las siguientes actividades:

- Recolección de la información mediante la investigación en documentos electrónicos referentes al tema.
- Revisión de la información recogida.
- Análisis de los datos.
- Lectura de artículos relacionados con la investigación presentada.
- Interpretación de los resultados mediante gráficos, cuadros para analizar e interpretar y por último redactar una síntesis de los resultados.

3.5. Desarrollo del Proyecto

Para el desarrollo del presente proyecto se realiza a cabo los siguientes aspectos:

- Identificar los recursos de Red de Datos & VoIP a monitorear en el Gobierno Provincial de Tungurahua.
- Establecidos los puntos críticos de la Red de Datos & VoIP se podrá diseñar mecanismos para obtener información detallada de la Red Informática.
- Determinar las herramientas Open Source que cumplan los requerimientos específicos para el monitoreo adecuado de la Red de Datos & VoIP.
- Realizar un modelado de escenarios de carga crítica en la Red de Datos y Analizar los datos obtenidos.
- Implementar la herramienta Open Source en los equipos en Producción del HGPT.
- Tomar desiciones adecuadas para resolver problemas que se observan en la Red de Datos & VoIP.
- Optimizar los recursos de Red de Datos & VoIP del Gobierno Provincial de Tungurahua.

3.6. Análisis de Datos

Identificar los recursos de Red de Datos & VoIP a monitorear en el Gobierno Provincial de Tungurahua.

Esta actividad consiste en analizar minuciosamente las entrevistas aplicadas al Jefe de TI, y al encargado del Área de Redes del HGPT., esto con el propósito

de lograr identificar de mejor manera los recursos de Red de Datos & VoIP a monitorear en el Gobierno Provincial de Tungurahua. (Ver Anexo N°1).

CAPÍTULO 4

Desarrollo de la propuesta

En el presente se analiza la capacidad funcional de la Red de Datos & VoIP del Gobierno Provincial de Tungurahua, para posteriormente evaluar el desempeño de cada una de ellas, y de esta manera poder emitir informes oportunos y verídicos sobre los diferentes escenarios de redes; lo cual indudablemente facilita la toma de decisiones oportunas a la hora de su implementación, y en consecuencia permitiendo un estable tráfico de Datos y garantizando estabilidad en el proceso comunicativo del H. Gobierno Provincial de Tungurahua.

4.1. Establecidos los puntos críticos de la Red de Datos & VoIP se podrá diseñar mecanismos para obtener información detallada de la Red Informática.

Una vez empleados todos los métodos investigativos necesarios se pudo identificar de forma clara los recursos de Red de Datos & VoIP, del Gobierno Provincial de Tungurahua, posteriormente se procedió a detallar uno a uno los puntos considerados críticos de la Red de Datos & VoIP del HGPT. Para lo cual fue necesario realizar una entrevista debidamente estructurada al Jefe de TI y al encargado del Área de Redes del Gobierno Provincial de Tungurahua, esto con el propósito de obtener la información necesaria sobre las principales falencias de la red a nivel General de Sistemas y a Nivel de Red de Datos y de Red VoIP, todos estos datos se pueden observar en el Anexo N° 2.

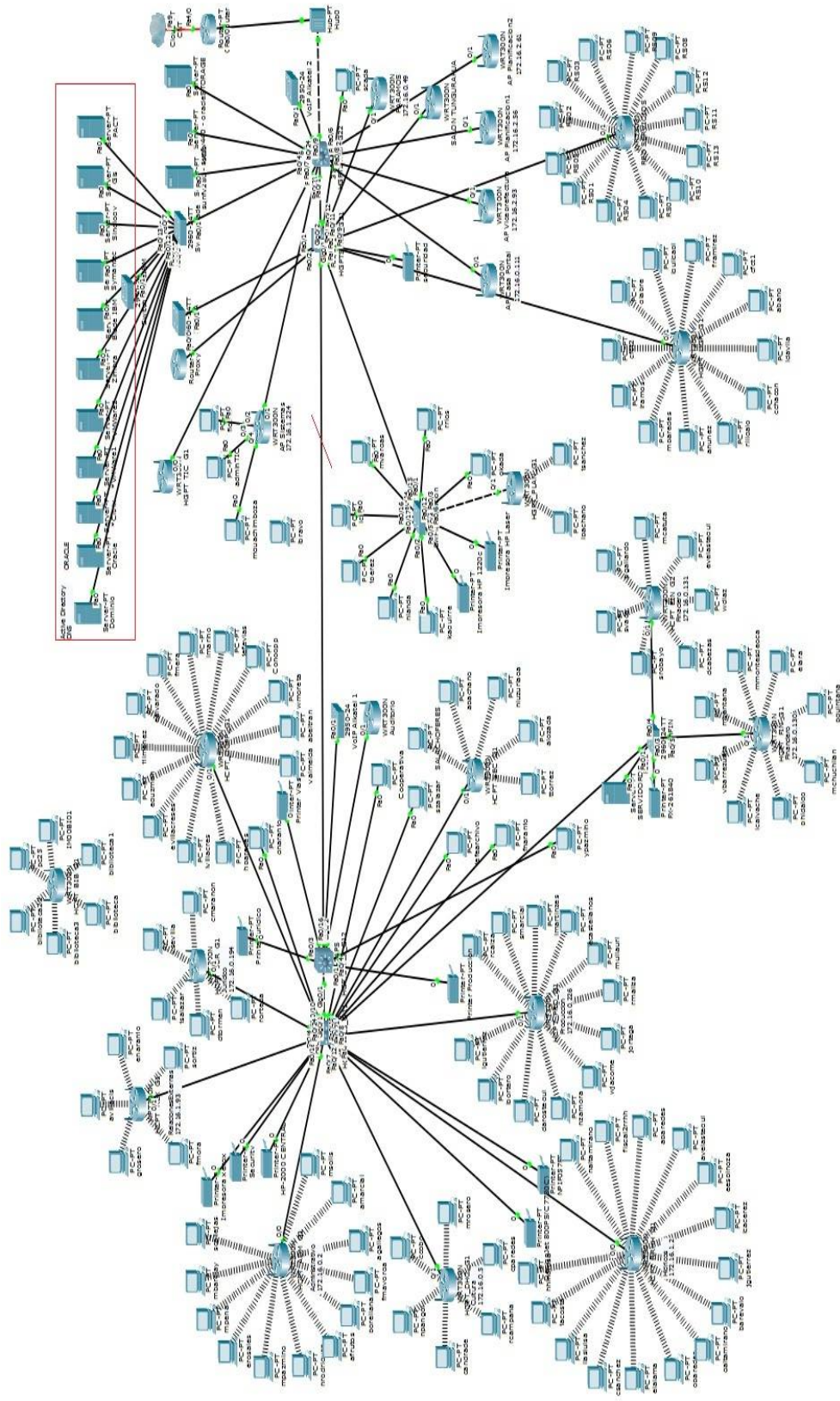


Figura 7: Puntos Críticos en la Red de Datos & VoIP del HGPT.
 Elaborado por: Departamento de TI del Honorable Gobierno Provincial de Tungurahua.

4.2. Determinar las herramientas Open Source que cumplan los requerimientos específicos para el monitoreo adecuado de la Red de Datos & VoIP.

Se determinó las herramientas Open Source que cumplan los requerimientos específicos para el monitoreo adecuado de la Red de Datos & VoIP, para ello es necesario realizar un análisis de factibilidad a fin de seleccionar las herramientas mas idóneas para cumplir los requerimientos planteados para el presente proyecto y observando de manera detallada sus principales características así como sus ventajas y desventajas, finalmente se tomó en cuenta diferentes herramientas Open Source las cuales nos ofrecen múltiples opciones entre las que se destacan: Cacti, Monitorix, Ntop, Zabbix y Zenoss.

- Cacti

Cacti es una completa herramienta de solución para la generación de gráficos en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad para gráficas que poseen la aplicación RRDtool. La herramienta, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Posee una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos[15].

Cacti representa gráficamente los datos almacenados en la RRD: uso de conexión a internet, datos como temperatura, velocidad, voltaje, número de impresiones, etc. La RRD es utilizada para almacenar y procesar datos recolectados vía SNMP. En definitiva, para hacer uso de una RRDtool, lo que se necesita es un sensor para medir los datos y poder alimentar al RRDtool con esos datos. Entonces, la RRDtool crea una base de datos, almacena los datos en ella, recupera estos datos y basándose en ellos, Cacti crea gráficos en formato PNG[15].

- Monitorix

Monitorix una herramienta bajo licencia libre y está disponible para Linux y FreeBSD. Su objetivo es ofrecer un panel de control sencillo, personalizable a través de un único fichero de configuración en texto plano, que permite realizar un detallado seguimiento mediante completas gráficas a los parámetros y servicios del sistema que más interese.

Monitorix utiliza bases de datos Round Robin (RRD) como backend para el almacenamiento de los datos recogidos. Esto le permite mantener un histórico del comportamiento del sistema y ofrece la posibilidad de consultar la información tanto en tiempo real como del periodo de tiempo que se requiera. Otra característica muy interesante de Monitorix es que se puede configurar una instancia a través de la cual se accede a todas las demás instaladas en los sistemas monitorizados.

- Ntop

Ntop facilita la labor de diagnóstico de la red. Ntop es una herramienta de monitorización de red en la que prima la presentación de informes de los datos recogidos sobre la recolección de paquetes de red[16]. Se puede destacar las siguientes características de ntop las cuales son:

- Es un proyecto de software libre.
- Su interfaz es web y muy intuitivo.
- Dispone de gran variedad de informes: informes globales de carga de red, de tráfico entre elementos, de sesiones activas de cada elemento, etc.
- Detecta posibles paquetes perniciosos.
- Permite exportar los datos a una base de datos relacional MySQL para su análisis.
- Es capaz de analizar datos proporcionados por dispositivos de red que soporten NetFlow y sFlow.
- Es un software multiplataforma (Windows, Linux, *BSD, Solaris y MacOSX) y muy fácil y rápido de instalar[17].

- Zabbix

Zabbix es una herramienta para monitorear los recursos de un equipo en forma remota que consume pocos recursos, permite centralizar la información en un servidor que permite visualizar el monitoreo de múltiples hosts. Zabbix es un software que controla numerosos parámetros de una red y la integridad de los servidores. Zabbix utiliza un mecanismo de notificación flexible que permite a los usuarios configurar alertas basadas en correo electrónico para cualquier evento[18].

Este permite una reacción rápida a los problemas del servidor. Todos los informes Zabbix y estadísticas, así como los parámetros de configuración se acceden a través de una interfaz basada en web. Un front-end basado en web se asegura que el estado de la red y la salud de los servidores se puede apreciar desde

cualquier lugar. Zabbix es libre de costo. Zabbix se escribe y se distribuye bajo la GPL General Public License versión 2. Esto significa que su código fuente se distribuye libremente y disponible para el público en general. El soporte es gratuito y comercial está disponible y realizado por la empresa Zabbix[18].

- Zenoss

Zenoss es una aplicación de monitoreo de código abierto, es una plataforma para la gestión de red y servidores basada en el servidor de aplicaciones Zope. Liberado bajo la Licencia Pública General de GNU (GPL) versión 2, Zenoss Core provee una interfaz web que permite a los administradores de sistemas, monitorear la disponibilidad, inventario/configuración, desempeño y eventos.

Sus principales funciones son dejar a la vista la configuración de red, la supervisión de la actividad de red, la gestión de la ocurrencia de eventos y la alarma. De forma automática, Zenoss permite visualizar las relaciones entre cada elemento de la red. Entre los protocolos utilizados, se encuentran SNMP, WMI y Telnet/SSH. Cada técnica de modelado produce una diversa riqueza de la información en el modelo. SNMP a menudo proporciona la más completa información del modelo, y SSH/Telnet se suele utilizar para aumentar el modelado cuando un agente SNMP no da una información crítica sobre alguna pieza específica. Los datos se registran en una base de datos exportable a XML, y el seguimiento de la actividad de la red se hace a través de tests SCMP y TCP programados[19].

La administración de Zenoss se realiza desde una interface web lo que simplifica la tarea a personas novatas en la aplicación y posibilita la configuración de la herramienta prácticamente sin la necesidad de modificar archivos de configuración. Zenoss permite realizar monitoreo de sistemas operativos Windows y Linux prácticamente sin la necesidad de instalar agentes en los sistemas operativos. Es la herramienta de monitorización elegida por earthweb como uno de los diez proyectos más innovadores de software libre. La aplicación y todas sus características están preparadas para funcionar bajo un entorno de software libre, como son las distribuciones Linux, pero también trabaja en plataformas Unix y sistemas Mac. Mención aparte sobre Windows; aunque Zenoss no fue diseñado para trabajar en él, es totalmente compatible y utilizable en este sistema.

La implementación en Windows es posible gracias a la simulación que ofrece la aplicación VMplayer, que permite hacer funcionar Zenoss con todas sus características en los sistemas operativos de Microsoft[19].

Por lo expuesto anteriormente, se detalla la tabla comparativa, con el propósito de poder observar de mejor manera cada una de las características de las herramientas antes mencionadas, determinando en consecuencia de forma pormenorizada sus características / criterios:

- NOMBRE DEL PRODUCTO

El nombre del software.

- INFORMES SLA IP

Soporte de Cisco IP Acuerdo de Nivel de Servicio mecanismo.

- AGRUPACIÓN LÓGICA

Soporta la organización de los anfitriones o dispositivos que supervisa en grupos definidos por el usuario.

- TRENDING

Proporciona una tendencia de datos de la red a través del tiempo.

- PREDICCIÓN DE TENDENCIAS

El software cuenta con algoritmos diseñados para predecir futuras estadísticas de la red.

- DETECCIÓN AUTOMÁTICA

El software detecta automáticamente los hosts o dispositivos de red que está conectado.

- SIN AGENTE

El producto no se basa en un agente de software que deben ejecutarse en los ejércitos es la vigilancia, por lo que los datos pueden ser empujados de nuevo a un servidor central. "Con el apoyo" significa que un agente puede ser utilizado, pero no es obligatorio. Un SNMP demonio no cuenta como un agente.

- SNMP

Capaz de recuperar e informar sobre SNMP estadísticas.

- SYSLOG

Capaz de recibir e informar sobre Syslogs .

- PLUGINS

Arquitectura del software basado en una serie de 'plugins' que proporcionan funcionalidad adicional.

- ACTIVADORES / ALERTAS

Capaz de detectar violaciones de umbral en datos de la red, y alerta al administrador de alguna forma.

- APLICACIÓN WEB

Se ejecuta como una aplicación basada en web.

No: No hay interfaz basada en la web para este software.

Viendo: los datos de la red se pueden ver en una interfaz gráfica basada en la web.

Reconociendo: Los usuarios pueden interactuar con el software a través de la interfaz basada en web para reconocer alarmas o manipular otras notificaciones.

Informes: informes específicos sobre los datos de red se pueden configurar por el usuario y se ejecutan a través de la interfaz basada en web.

Control total: TODOS los aspectos del producto se pueden controlar a través de la interfaz basada en la web, incluyendo tareas de mantenimiento de bajo nivel, tales como la configuración del software y las actualizaciones.

- DISTRIBUTED MONITORING

Capaz de aprovechar más de un servidor para distribuir la carga de la supervisión de la red.

- INVENTARIO

Mantiene un registro de hardware y / o software de inventario para los anfitriones y los dispositivos que supervisa.

- LOS DATOS MÉTODO DE ALMACENAMIENTO

Método principal utilizado para almacenar los datos de la red que supervisa.

- LICENCIA

Licencia publicado bajo (por ejemplo, GPL , la licencia BSD , etc.).

- MAPAS

Características mapas de red gráficos que representan los anfitriones y los dispositivos que SUPERVISA, Y LOS VÍNCULOS ENTRE ELLOS.

- CONTROL DE ACCESO

Características de seguridad a nivel de usuario, lo que permite a un administrador para impedir el acceso a determinadas partes del producto en una base por usuario o por papel.

- IPV6

Soporta monitoreo IPv6 hosts y / o dispositivos, que reciben datos de IPv6, y que se ejecutan en un servidor habilitado para IPv6. Soporta comunicación utilizando IPv6 al agente SNMP a través de una dirección IPv6.

ANÁLISIS DE FACTIBILIDAD

Con el propósito de poder determinar de forma cualitativa la factibilidad de la aplicación de la herramienta mas idónea se realiza la evaluación de cada una de ellas para lo cual se les asignará una calificación y posteriormente se procederá a determinar su grado de conveniencia para el proyecto considerando de manera especial sus principales ventajas.

Tabla 3: Cuadro Cualitativo de Herramientas para el Monitoreo de Redes.

Nombre	Informes de SLA IP	Agrupación Lógica	Trending	Predicción de Tendencias	Detección Automática	Sin Agente	SNMP	Syslog	Plugins	Activadores / Alertas	Aplicación Web
Cacti	Si	Si	Si	Si	Vía Plugin	Si	Si	Si	Si	Si	Control Total
Monitorix	No	No	Si	Si	No	No	Si	No	Si	Si	Visualización
Ntop	No	No	Si	No	No	Apoyado	Si	No	Si	Si	Visualización
Zabbix	Si	Si	Si	No	Si	Apoyado	Si	Si	Si	Si	Control Total
Zennos	Si	Si	Si	Si	Si	Apoyado	Si	Si	Si	Si	Control Total
Nombre	Informes de SLA IP	Agrupación Lógica	Trending	Predicción de Tendencias	Detección Automática	Sin Agente	SNMP	Syslog	Plugins	Activadores / Alertas	Aplicación Web

Elaborado por: El Investigador.

Tabla 4: Cuadro Cualitativo de Herramientas para el Monitoreo de Redes.

Nombre	Distributed Monitoring	Inventario	Plataforma	Método de Almacenamiento	Licencia	Mapas	Control de Acceso	IPv6	Ultima Fecha de Lanzamiento
Cacti	Si	Si	PHP	RRDtool, MySql	GPL	Enchufar	Si	Si	2014 - 11
Monitorix	Desconocido	Desconocido	Perl	RRDtool	GPL	Desconocido	No	Si	2014 - 5
Ntop	Si	Desconocido	PHP	MySql	GPL	Desconocido	No	Si	20142 - 8
Zabbix	Si	Si	C, PHP	Oracle, MySql, PostgreSQL, IBM, DB2, SQLite	GPL	Si	Apoyado	Si	2015 - 04
Zennos	Si	Si	Python, Java	ZODB, MySql, RRDtool	Libre Core GPL, Empresa Comercial	Si	Apoyado	Si	2014 - 4
Nombre	Distributed Monitoring	Inventario	Plataforma	Método de Almacenamiento	Licencia	Mapas	Control de Acceso	IPv6	Ultima Fecha de Lanzamiento

Elaborado por: El Investigador.

CRITERIO DE EVALUACIÓN

A fin de asignar un parámetro el cual nos permitirá calificar e identificar a la herramienta mas idónea se opto por evaluarlas según el siguiente detalle:

Tabla 5: Criterio de Evaluación[1].

Calificación	Parámetros de Evaluación
1	Muy Malo
2	Malo
3	Bueno
4	Muy Bueno
5	Excelente

Elaborado por: El Investigador.

Tabla 6: Cuadro Cuantitativo de Herramientas para el Monitoreo de Redes.

Nombre	Informes de SLA IP	Agrupación Lógica	Trending	Predicción de Tendencias	Detección Automática	Sin Agente	SNMP	Syslog	Plugins	Activadores / Alertas	Aplicación Web
Cacti	1	3	3	4	3	2	5	4	4	5	4
Monitorix	0	0	3	4	0	0	5	0	4	5	4
Ntop	1	3	3	0	3	1	1	1	4	5	4
Zabbix	1	3	3	0	5	1	5	4	4	5	4
Zennos	1	3	3	4	5	1	5	4	4	5	4
Nombre	Informes de SLA IP	Agrupación Lógica	Trending	Predicción de Tendencias	Detección Automática	Sin Agente	SNMP	Syslog	Plugins	Activadores / Alertas	Aplicación Web

Elaborado por: El Investigador.

Tabla 7: Cuadro Cuantitativo de Herramientas para el Monitoreo de Redes.

Nombre	Distributed Monitoring	Inventario	Plataforma	Método de Almacenamiento	Licencia	Mapas	Control de Acceso	IPv6	Total
Cacti	2	5	1	1	3	1	3	4	55
Monitorix	2	0	1	1	3	0	3	4	39
Ntop	2	1	2	1	3	3	3	4	45
Zabbix	2	5	2	2	3	3	3	4	59
Zennos	2	5	3	3	4	3	3	4	67
Nombre	Distributed Monitoring	Inventario	Plataforma	Método de Almacenamiento	Licencia	Mapas	Control de Acceso	IPv6	Total

Elaborado por: El Investigador.

Según los parámetros obtenidos en el cuadro anterior en el que se da un grado de ponderación del 1 al 5 siendo el parámetro 1 la calificación menos factible para el proyecto y el 5 el mas factible se puede concluir por una parte la herramienta Zennos se ajusta de mejor manera a los requerimientos del cliente pues evidencia prestaciones significativas desde el punto de vista práctico, así también se puede notar que la herramienta Monitorix a su vez claramente muestra características excesivamente básicas lo cual evidentemente dificulta el grado de familiarizaron entre el usuario y la herramienta, dificultando en consecuencia su entendimiento e interpretación de datos.

4.3. Realizar un modelado de escenarios de carga crítica en la Red de Datos y Analizar los datos obtenidos.

Realizado el análisis de factibilidad de las herramientas para el monitoreo de la red del HGPT, se modela la red de datos del Honorable Gobierno Provincial, se virtualiza los diferentes Sistemas Operativos con su respectivos servicios, como se la observar en la figura 8.

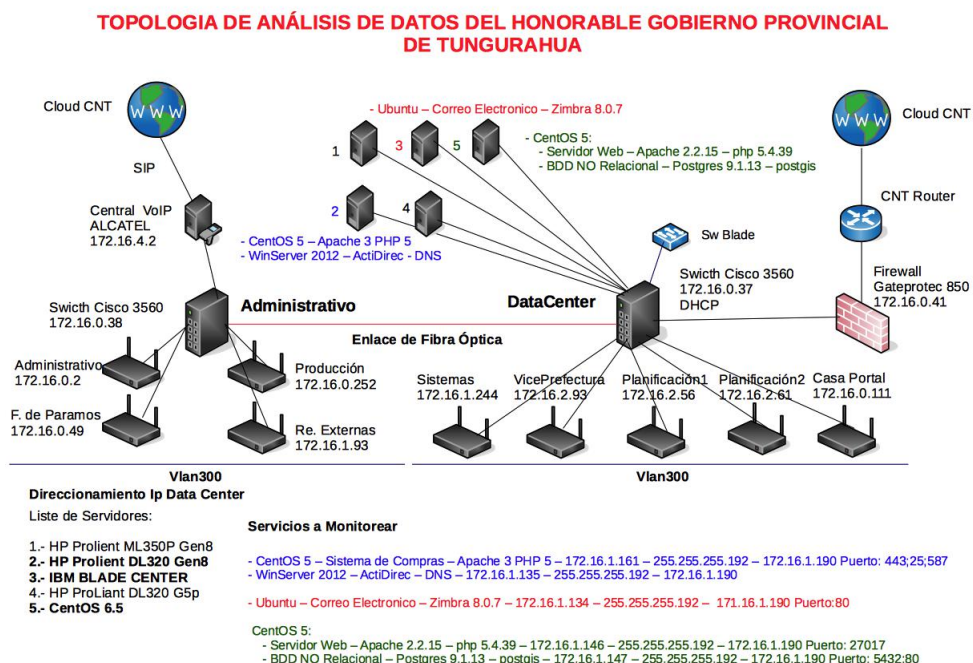


Figura 8: Topología de Red del HGPT, para la Simulación de la Carga Datos.
Elaborado por: El Investigador.

Servidores a virtualizar con las siguientes características como lo indica la tabla 8.

Tabla 8: Tabla de Sistemas Operativos.

Nº	Sistema Operativo	Función	Servicios	Dirección IP	Máscara de Red	Puerta de Enlace
1	CentOS 5	Sistema de Compras	Apache 3 - Php 5	172.16.1.161	255.255.255.192	172.16.1.190
2	Windows Server 2012 R2	Control de Usuarios	Active Directory - DNS	172.16.1.135	255.255.255.192	172.16.1.190
3	Ubuntu Server	Correo Electrónico	Zimbra	172.16.1.134	255.255.255.192	172.16.1.190
4	CentOS 5	GIS HGPT	Apache 2.2.25 - Php 5.4.39	172.16.1.146	255.255.255.192	172.16.1.190

Elaborado por: El Investigador.

Topología de Red Lan para análisis de Datos del HGPT, como se observa en la figura 9.

ANÁLISIS DE DATOS DEL HONORABLE GOBIERNO PROVINCIAL DE TUNGURAHUA

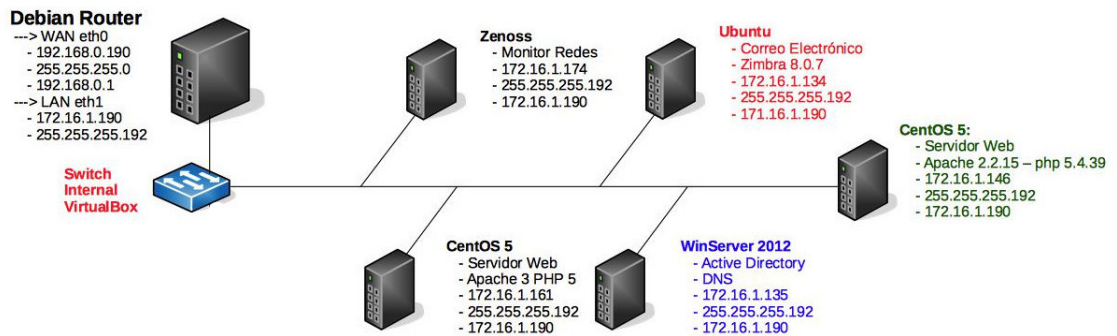


Figura 9: Escenario de Simulación de Carga de Datos para el HGPT.

Elaborado por: El Investigador.

Configuración de Sistemas Operativos

Definido el escenario para la Carga de Datos, se procede a virtualizar los diferentes Sistemas Operativos con sus respectivos servicios. Las máquinas a virtualizar son alojadas en Oracle VirtualBox, como se observa en la tabla 9 en la cual se describe: Sistema Operativo, Función, Servicios y su Direccionamiento IP.

Tabla 9: Tabla de Sistemas Operativos Virtualizados.

Nº	Sistema Operativo	Función	Servicios	Dirección IP	Máscara de Red	Puerta de Enlace
1	CentOS 5	Servidor LAMP	BDD Apache	172.16.1.161	255.255.255.192	172.16.1.190
2	Windows Server 2012 R2	Control de Usuarios	Active Directory - DNS	172.16.1.135	255.255.255.192	172.16.1.190
3	Ubuntu Server	Correo Electrónico	Zimbra	172.16.1.134	255.255.255.192	172.16.1.190
4	CentOS 5	Servidor LAMP	Apache 2.2.25 / Php 5.4.39	172.16.1.146	255.255.255.192	172.16.1.190
5	Debian 7	Monitoreo	Snmp	172.16.1.174	255.255.255.192	172.16.1.190
6	Debian 8	Router para la LAN	Iptables	LAN - eth0 - 172.16.1.190	255.255.255.192	-
				WAN - eth1 - 192.168.0.190	255.255.255.0	192.168.0.1

Elaborado por: El Investigador.

De esta forma se instala los SO los cuales van a ser necesarios para la carga de datos.

Tabla 10: Tabla de Características de Sistemas Operativos Virtualizados.

Sistema Operativo - Características	CentOS 5	Windows Server 2012 R2	Ubuntu Server 14.10	CentOS 5	Debian 7 Monitoreo	Debian 8 Router
Disco Duro	5,8 Gb.	25 Gb.	38 Gb.	5,8 Gb.	15 Gb.	1,9 Gb.
Memoria RAM	1002 Mb.	2 Gb.	1,4 Gb.	1002 Mb.	1,7 Gb.	500 Mb.
Swap	2015 Mb.	348 Mb.	1,4 Gb.	2015 Mb.	603,636 Mb.	134 Mb.
Entorno Gráfico	Xfce 4	Metro	Lxde	Gnome 2.1.6.0	Gnome 3.4.2	Mininal
Interfaces de Red	eth0	Adaptador de Red	eth0	eth0	eth0	eth0 - eth1

Elaborado por: El Investigador.

Configuración de Servicios

- CentOS

En los Sistemas Operativos Centos 5 se instala un servidor LAMP (Linux, Apache, MySql o MariaDb, Perp, Php o Phytion), la cual se usa para un Servidor Web.

El alojamiento del contenido esta sobre WordPress, a continuación se describe la configuración e instalación del mismo.

- Instalar Apache: `yum install httpd`

- Configurar Apache: Ingresar a la terminal con privilegios de usuario root, ubicar el directorio: `“/etc/httpd/conf/”`; editar el archivo de configuración `“httpd.conf”` en el cual se modifica las siguientes lineas: `Listen 80`; `ServerName localhost`, quitar los comentarios y guardar las modificaciones. Activar el servicio con el comando `“chkconfig httpd on”`, para finalizar reiniciar la máquina.

- Instalar Php: `yum install php php-mysql`

- Configurar VirtualHost: para la configuración abrir el directorio `“/var/www/html”`; y dentro del mismo crear otro directorio con la instrucción `“mkdir -p midominio1.com/public_html”`

Para la configuración se elige `AllowOverride None` por `All`, `NameVirtualHost *:80`, en el cual se quita los comentarios. En la tabla número 11 se observa la configuración del VirtualHost:

Tabla 11: Tabla de Configuración de VirtualHost.

Configuración de VirtualHost	
ServerAdmin	webmaster@midominio1.com
DocumentRoot	/var/www/midominio1.com/public_html/
SeverName	www.midominio1.com
ServerAlias	midominio1.com
ErrorLog	logs/lamp.hgpt-error_log
CustomLog	logs/lamp.hgpt.local-access_log common

Elaborado por: El Investigador.

Por último se reinicia el servicio `“service httpd restart”`.

- Instalación de MySQL: `yum -y install mysql mysql-server`

- Configuración: MySQL la configuración consta de los siguientes parámetros, primero ubicar el directorio:

`“/usr/bin/mysql_secure_installation/”`

al presionar enter su selección debe estar en `“YES”` de esa manera se ingresa el nuevo password el cual es: `“server123”`, confirmar el password: `“server123”`; en la tabla 12 se visualiza la configuración del usuario Anonymous elegir la siguiente configuración:

Tabla 12: Tabla de Configuración de Usuario Anonymous.

Configuración de Usuario Anonymous	
Remove Anonymous user?[Y/N]	Yes
Disable root login remote ? [Y/N]	Yes
Remove test databse and access to it? [Y/N]	Yes
Reload privilegie tables now? [Y/N]	Yes

Elaborado por: El Investigador.

Una vez configurado el usuario Anonymous crear la base de datos para el CMS WordPress, se ingresa a MySQL con el siguiente comando: “mysql-u root-p” ingresar la clave definida anteriormente: server123, crear la Base de Datos y dar los permisos necesarios para su correcto funcionamiento:

- Create User userw@localhost;
- SET PASSWORD FOR userw@localhost=PASSWORD ('lamp132');
- GRANT ALL PRIVILEGES ON wordpress.* TO userw@localhost IDENTIFIED BY 'lamp123';
- FLUSH PRIVILEGES;
- exit

- Instalación de WordPress:

Ingresar al directorio “/var/www/html/wordpress” al que se le hace una copia del archivo “wp_config_sample.php” a “wp_config.php” para configurar las siguientes líneas, a observar en la tabla 13:

Tabla 13: Tabla de Configuración de WordPress.

Configuración de WordPress	
DB_NAME:	wordpress
DB_USER:	userw
DB_PASSWORD:	server123
DB_HOST:	localhost

Elaborado por: El Investigador.

Una vez editado el archivo guardar los cambios e iniciar la instalación de WordPress.

- Debian Router

En la configuración del router se instala Debian 8 minimal, el complemento adicional a instalar es el servidor SSH en el cual se modifica las “Iptables”

lo que permite la correcta comunicación de la LAN Interna hacia la WAN, la configuración de lo mencionado anteriormente se describe en la figura 4.3:

```
#!/bin/sh
# /etc/init.d/franco
# squid server IP
#SQUID_SERVER="192.168.2.1"
# Interface connected to Internet
INTERNET="eth0"
# Interface connected to LAN
LAN_IN="eth1"
# Squid port
#SQUID_PORT="3128"
# DO NOT MODIFY BELOW
# Clean old firewall
iptables -F
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe ip_conntrack_ftp
# For win xp ftp client
#modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward
# Setting default filter policy
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
# Unlimited access to loop back
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
# set this system as a router for Rest of LAN
iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
# unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT
# DNAT port 80 request coming from LAN systems to squid 3128 ($SQUID_PORT) aka transparent proxy
#iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $SQUID_SERVER:$SQUID_PORT
# if it is same system
#iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $SQUID_PORT
# DROP everything and Log it
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP
```

Figura 10: Configuración de Iptables.
Elaborado por: El Investigador.

- Ubuntu Server 14.10

Para la instalación y configuración de Zimbra se accede como usuario “root” instalando los siguientes paquetes: “apt-get install libgmp10 libperl5.18 unzip pax sysstat sqlite3 dnsmasq”; una vez instalado los paquetes configurar el Servidor de DNS. Para la configuración de DNS modificar el archivo “hostname” el cual se encuentra en el directorio “/etc/” el mismo que se edita y se configura: “mail.hgtp.local”, cerrar y guardar los cambios. Editar el archivo “hosts” ingresar la dirección ip, el dominio “172.16.1.134 mail.hgpt.local mail”, cerrar el archivo salvando los cambios. Para configurar el archivo “dnsmasq” direccionarse al directorio “/etc/” el mismo que tiene la siguiente configuración para su funcionamiento, tal como lo muestra la tabla 14.

Tabla 14: Tabla de Configuración de Archivo Dnsmasq.

Configuración archivo DNSMASQ	
server:	172.16.1.134
domain:	hgpt.local
mx-host:	hgpt.local, mail.hgpt.local, 5
mx-host:	hgpt.local, mail.hgpt.local, 5
listen-address:	127.0.0.1

Elaborado por: El Investigador.

Salvar los cambios y reiniciar la máquina.

Descargar el paquete: “`wget https://files.zimbra.com/downloads/8.6.0_GA/zcs-8.6.0_GA_1153.UBUNTU14_64.20141215151116.tgz`”

Desempaquetar e instalar con la siguiente instrucción:

```
“tar -xvf zcs-8.6.0_GA_1153.UBUNTU14_64.20141215151116.tgz”
```

Al tener desempaquetado zimbra ingresar al directorio y buscar el archivo ejecutable, para instalarlo dígitelo la siguiente instrucción: “`./install.sh`”, de esta manera se tiene listo el Correo Electrónico Zimbra.

Virtualización del Modelado de Escenarios

Establecido el Modelado de Escenarios a ser monitoreados se crea espacios virtuales para instalar los diferentes Sistemas Operativos con sus respectivos servicios, para poder utilizar las prestaciones que ofrece Oracle VirtualBox se descarga la imagen .iso del sistema Operativo Debian i386 desde la siguiente página:

- <http://cdimage.debian.org/debian-cd/7.0.0/i386/iso-dvd/>

Al tener la distro descargada, instalar dentro de VirtualBox de Oracle de la siguiente manera:

Espacio de Trabajo de Oracle VirtualBox:

Crear el espacio de la máquina virtual y la instalación de Debian 7.0.0 i386.

Elegir “Nuevo” para Instalar el Sistema Operativo, nombrar como Debian, de esta manera automáticamente reconoce el tipo de sistema la versión si es de “64bits” ó “32bits”. El mismo que tiene los siguientes parámetros:

- Tamaño de la Memoria Virtual.
- Tamaño, tipo de Disco, si su Almacenamiento es Dinámico o tiene Tamaño Fijo, la ubicación del Disco dentro del Sistema.

La forma de establecer una correcta configuración en la máquina virtual es:

- Cambiar la configuración del adaptador de “NAT” a adaptador “PUENTE” lo cual permite un mejor desempeño en la instalación del Sistema.

Una vez realizado esto se puede decir que se creó y configuró el espacio virtual para que pueda ser instalado “Debian 7”, tal como se ilustra en la figura 11.

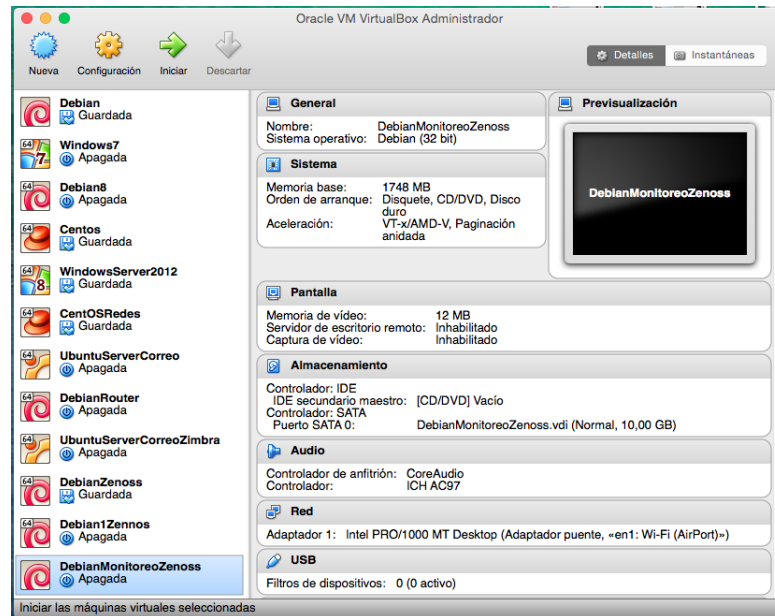


Figura 11: Configuración de Finalizada de Espacio Final.
Elaborado por: El Investigador.

Instalar Debian 7.0.0 i386 en el Espacio Virtual.

Al instalar Debian 7.0.0 de 32bits se elige el espacio virtual, el cual ubicará la imagen .iso de “Debian 7.0.0 i38.iso” dentro del sistema, al mismo que se da las siguientes configuraciones:

- Selección modo de instalación Sistema Operativo.



Figura 12: Instalación de Sistema Operativo en Modo Gráfico.
Elaborado por: El Investigador.

- Ubicación del Sistema, configuración de teclado.

- Nombre de la máquina, contraseña de super usuario.
- Se asigna un nombre al usuario.
- Zona hora para el Sistema.
- Particionamiento de Discos, se confirma los cambios escritos en el Disco.
- Configuración de paquetes usando una réplica de red, la se aconseja el Gestor de paquetes de la UNAL ubicada en Colombia.
- Configuraré Proxy de ser necesario.
- Paquetes adicionales a instalar serán: Debian desktop, SSH Server, Utilidades del sistema estándar.

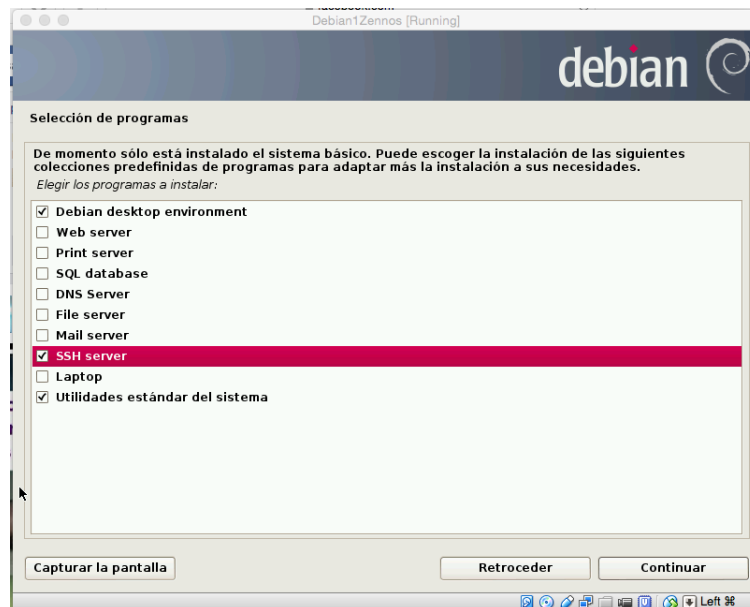


Figura 13: Programas a Instalar.
Elaborado por: El Investigador.

- Configuración del Grub.

Realizado esto se tendrá instalado Debian de manera satisfactoria.



Figura 15: Interfaz de Debian 7 i386.
Elaborado por: El Investigador.

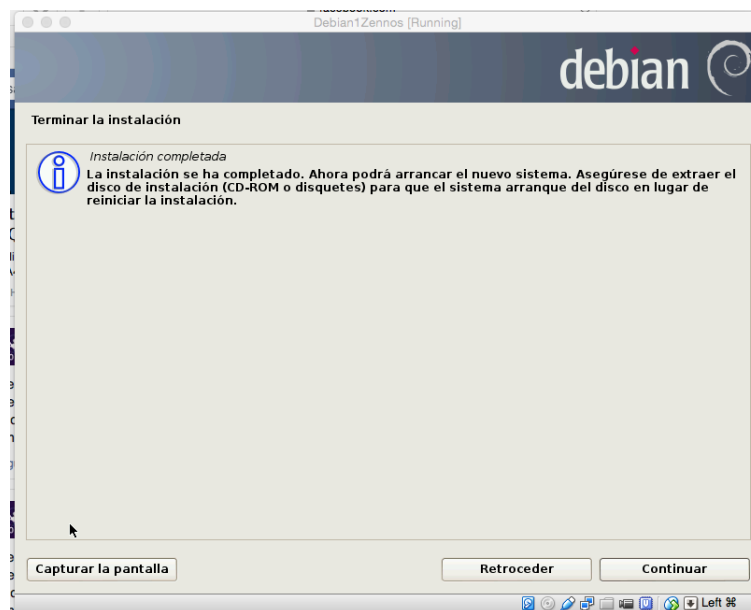


Figura 14: Instalación Completa del Sistema Operativo.
Elaborado por: El Investigador.

Configurar Protocolo SNMP en Sistemas Operativos a ser Monitoreados.

Al tener instalado el sistema operativo “Debian 7”, se procede a instalar el servicio SNMP en el servidor y en las terminales a ser monitoreadas como son: Linux y Windows.

- Instalar SNMP en Servidor Linux.

La instalación del agente SNMP Servidor en Linux Debian se lo hará de la siguiente manera:

- Se Ingresa a la terminal como usuario root.
- Para proceder a la instalación digitar: “apt-get install snmpd”.
- Realizada la instalación configurar los archivos snmp que se encuentra dentro del directorio “/etc/default/snmp”, al cual se modifica la línea de SNMPOPTS lo que permite ser escuchado por cualquier máquina.

```

# This file controls the activity of snmpd and snmptrapd
# Don't load any MIBs by default.
# You might comment this lines once you have the MIBs downloaded.
export MIBS=

# snmpd control (yes means start daemon).
SNMPDRUN=yes

# snmpd options (use syslog, close stdin/out/err).
SNMPOPTS='-Lsd -Lf /dev/null -u snmp -g snmp -I -smux -p /var/run/snmpd.pid -a -X 127.0.0.1 172.16.1.174'

# snmptrapd control (yes means start daemon). As of net-snmp version
# 5.9, master agentx support must be enabled in snmpd before snmptrapd
# can be run. See snmpd.conf(5) for how to do this.
TRAPDRUN=no

# snmptrapd options (use syslog).
TRAPDOPTS='-Lsd -p /var/run/snmptrapd.pid'

# create symlink on Debian legacy location to official RFC path
SNMPDCOMPAT=yes

```

Figura 16: Configuración Servicio SNMP - SNMPOPTS.
Elaborado por: El Investigador.

- En este caso se configura el archivo “/etc/snmp/snmpd.conf”, en donde se crea la comunidad con permiso de lectura y escritura para permitir el escaneo completo del equipo en el que nos encontramos para poder realizar la practicas y tareas necesarias como se muestra en la siguiente captura.

```
franco@monitoreo: ~
GNU nano 2.2.6 Fichero: /etc/snmp/snmpd.conf

#configuracion
rocommunity public
syslocation "PDC, Peters DataCenter"
syscontact franqex.escobar1516@gmail.com
com2sec MiRedLocal default public
group MiGrupo v1 MiRedLocal
group MiGrupo v2c MiRedLocal
#group MyRWGroup usm local
view all included .1
access MiGrupo "" any noauth exact systemview none none
#syslocation Unknown (edit /etc/snmp/snmpd.conf)
#syscontact Root (configure /etc/snmp/snmp.local.conf)
#pass .1.3.6.1.4.1.4413.4.1 /usr/bin/ucd5820stat
#view systemview included .1.3.6.1.2.1.1
#view systemview included .1.3.6.1.2.1.25.1.1
dontLogTCPWrappersConnects yes
```

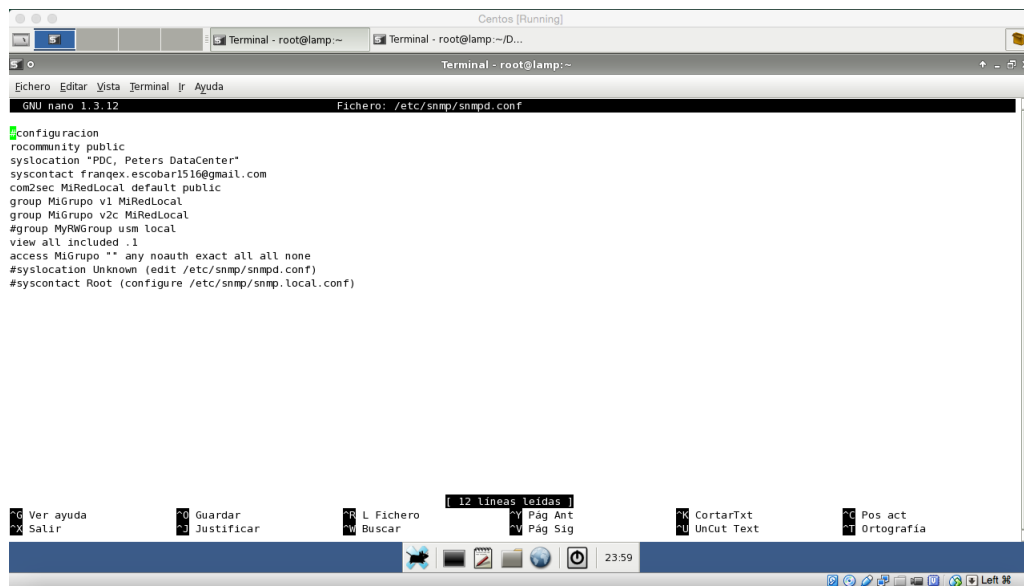
Figura 17: Configuración del Archivo Servicio SNMPD.
Elaborado por: El Investigador.

- Para verificar el servicio se ejecuta “/etc/init.d/snmpd start”, verificado esto el servicio esta en: “OK snmpd is running”.

- Instalar SNMP en Cliente Linux.

La instalación el Agente SNMP Cliente en Linux CentOS se procede de la siguiente manera:

- Se Ingresara a la terminal como usuario root.
- Para proceder a la instalación digitar: “yum install net-snmp net-snmp-utils net-snmp-lib”.
- Realizada la instalación configurar los archivos snmp que se encuentra dentro del directorio “/etc/snmp/snmpd.conf”, en donde se creara una comunidad con permiso de lectura y escritura para permitir el escaneo completo del equipo.



```
GNU nano 1.3.12 Fichero: /etc/snmp/snmpd.conf

#configuracion
rocommunity public
syslocation "PDC, Peters DataCenter"
syscontact franqex.escobar1516@gmail.com
com2sec MiRedLocal default public
group MiGrupo v1 MiRedLocal
group MiGrupo v2c MiRedLocal
#group MyRWGroup usm local
view all included .1
access MiGrupo "" any noauth exact all all none
#syslocation Unknown (edit /etc/snmp/snmpd.conf)
#syscontact Root (configure /etc/snmp/snmp.local.conf)
```

Figura 18: Configuración del Archivo SNMPD en el Cliente CentOS.
Elaborado por: El Investigador.

- Para verificar el servicio se ejecuta “service snmpd start”, verificado esto el servicio esta en OK.

- Instalar SNMP en Windows.

La instalación del servicio SNMP en Windows se la realiza de la siguiente manera:

- Se dirige a: Inicio/Panel de Control/Agregar o Quitar Programas/Activar o desactivar características de Windows., se activa el Protocolo simple de administración de redes SNMP se debe activar el Proveedor de SNMP de WMI dando en Aceptar.

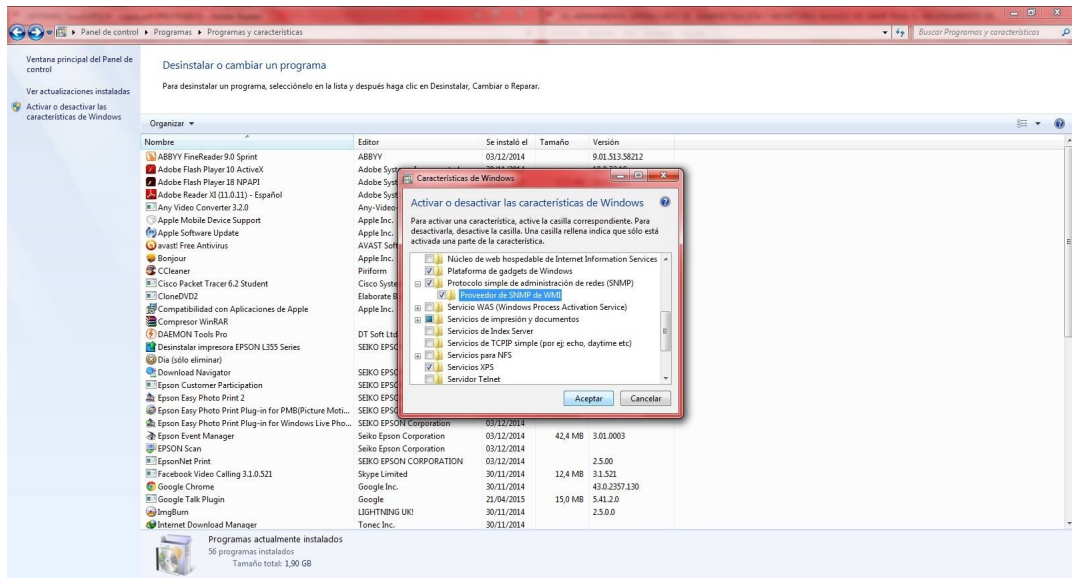


Figura 19: Instalar Protocolo SNMP en Windows.
Elaborado por: El Investigador.

- Dirigirse a Servicios de Windows donde se modifica las opciones de “Capturas”, “Seguridad”. del protocolo SNMP, aplicar los cambios y reiniciar.
- Para configurar las “Capturas” del protocolo SMNP en windows la comunidad debe estar en Public y el destino de las capturas debe ser direccionado a: 172.16.1.174.

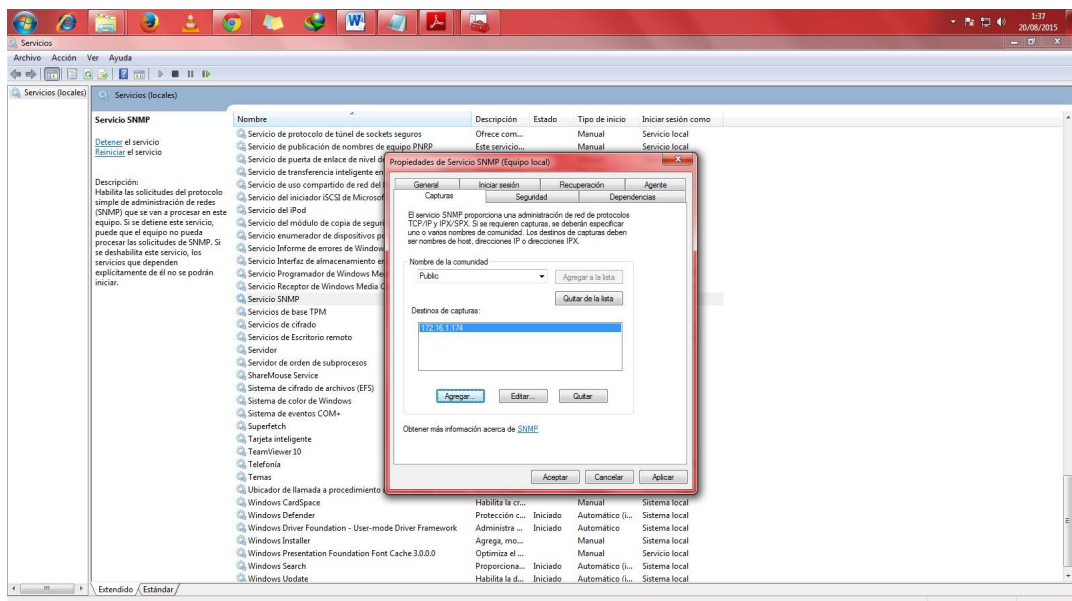


Figura 20: Configuro Capturas de SNMP en Windows.
Elaborado por: El Investigador.

- Para configurar la “Seguridad” del protocolo SMNP la comunidad debe estar

en public con permiso de “Lectura y Escritura” en el cual los debe ser habilitado aceptar paquetes SNMP de este host 172.16.1.174.

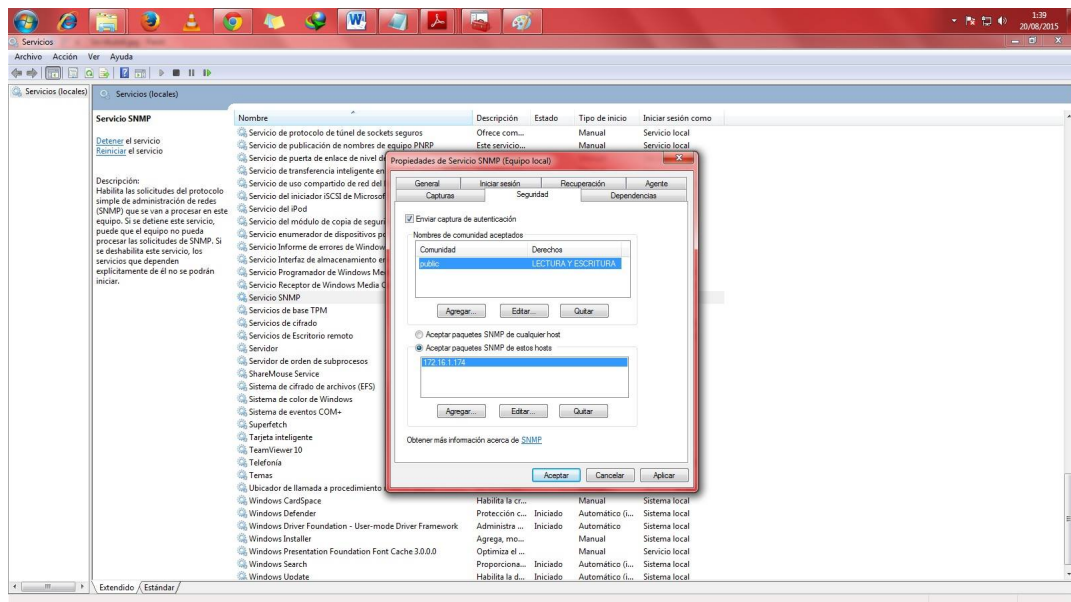


Figura 21: Configuro Seguridad SNMP en Windows.
Elaborado por: El Investigador.

Instalar Zenoss en Debian.

Para instalar la aplicación que realiza el monitoreo de la Red de Datos de HGPT “Zenoss” se sigue los siguientes pasos:

Ingreso a la Terminal con privilegios de Super Usuario para descarga de los paquetes requeridos.

Ubicarse en el Directorio del Usuario Franco: /home/franco/Descargas/. Para proceder a la descarga del paquete Zenoss.:

“wget http://sourceforge.net/projects/zenoss/files/zenoss-3.2/zenoss-3.2.1/zenoss-stack_3.2.1_i386.deb/download”, presionar enter para su descarga.

Descargado el paquete describir la carpeta “Descargas” con el comando “ls” para observar si el paquete se descargo correctamente, donde esta “zenoss-stack_3.2.1_i386.deb”.

Para la instalación del paquete utilizar el siguiente comando “dpkg -i zenoss-stack_3.2.1_i386.deb”:

Finalizada la Instalación de la aplicación Zenoss, levantar con la siguiente instrucción “/etc/init.d/zenoss-stack start” donde inician todos sus servicios.

Iniciada la aplicación “Zenoss” dirigirse al navegador de preferencia, digitar la siguiente dirección de “localhost” o la dirección ip: http://localhost/Zenoss o

http://172.16.1.172:8080 en donde se tiene la siguiente interfaz y dar click en Get Started.

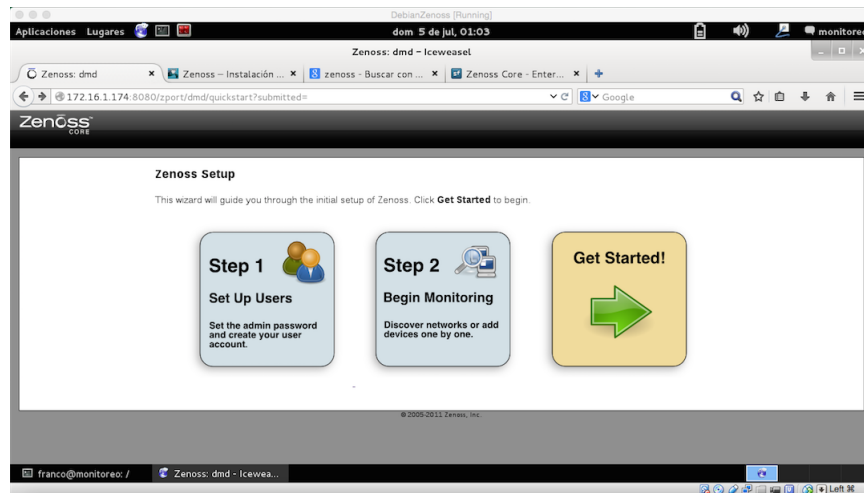


Figura 22: Interfaz de Instalación de Zenoss.
Elaborado por: El Investigador.

Realizado el paso anterior se tiene la interfaz para crear: el Usuario, la Contraseña y el Correo Electrónico. Una vez culminado este paso se observara la interfaz de Zenoss:

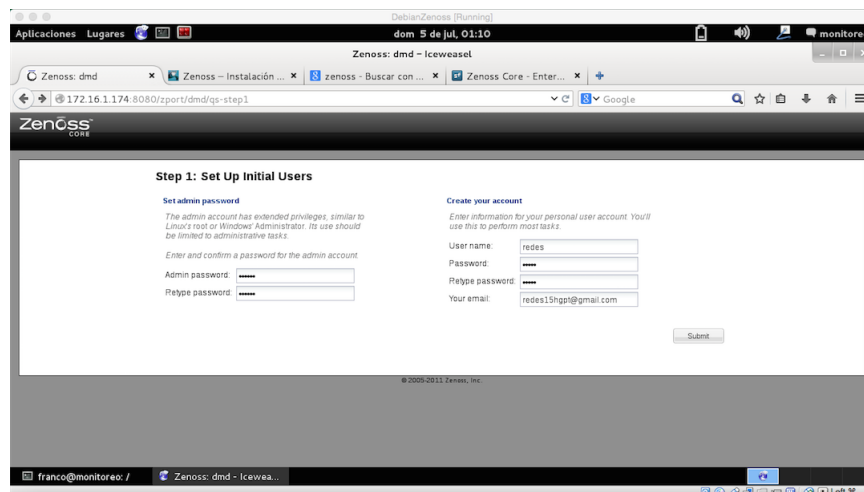


Figura 23: Configuración para Funcionamiento de Zenoss.
Elaborado por: El Investigador.

Se presenta la primera configuración que Zenoss desea realizar donde permite Agregar los dispositivos de manera manual o por auto descubrimiento:

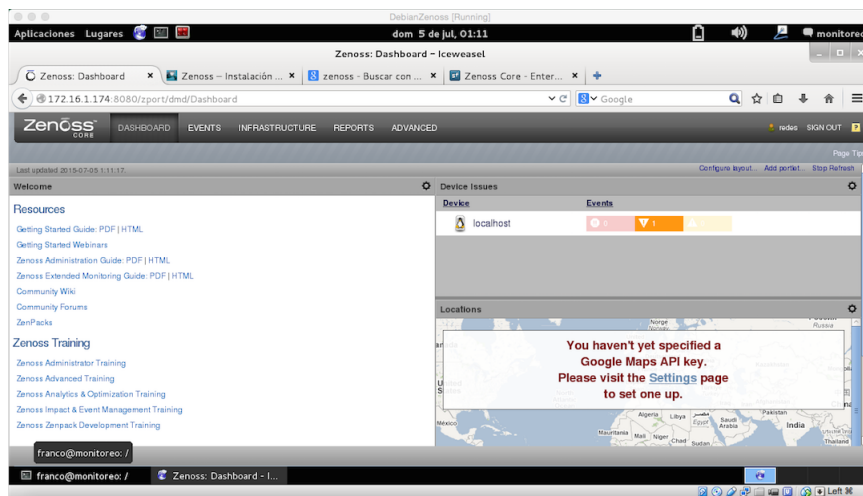


Figura 25: Pantalla DashBoard de Zenoss.
Elaborado por: El Investigador.

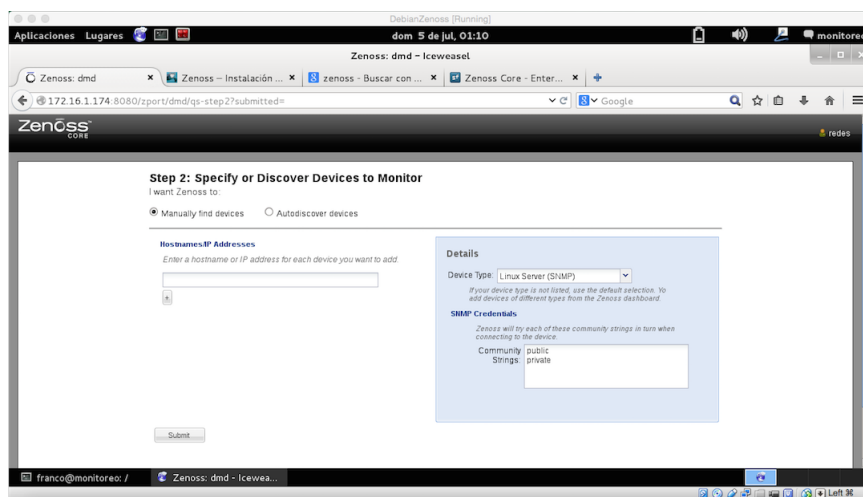


Figura 24: Agregar Dispositivos.
Elaborado por: El Investigador.

Terminado el proceso para Agregar Dispositivos de forma Manual o Autodecubrimiento, se observa el Dashboard de Zenoss; donde se manipula cada opción que ofrece la herramienta entre las que se tiene:

Administración de Zenoss

Zenoss para su administración proporciona una solución adecuada para el Monitoreo de Redes en el Área de TI, en la cual incorpora las siguientes opciones:

- Gestión de Dispositivos.
- Monitorización de Disponibilidad.
- Gráficos de Rendimiento.

- Gestión de Alertas y Usuarios.
- Arquitectura de Plugin.
- Informes de Rendimiento.

Para monitorear los activos de TI los cuales son: servidores, routers, switches, sitios web y cualesquier dispositivo que este conectado a la Red. El Dashboard de Zenoss es el lugar donde se va a pasar la mayor parte del tiempo. En donde se proporcionara un único punto de acceso al sistema de monitoreo en la cual no se requiere el conocimiento especifico del Sistema Operativo a ser usado.

■ **Gestión de Dispositivos**

En la Administración de Dispositivos en la aplicación Zenoss, se utiliza la configuración de Base de Datos de Gestión (CMDB), la cual permite agregar dispositivos de manera Manual o por Auto-descubrimiento, estos dispositivos son modelados a través del Protocolo Simple Network Mangement (SNMP), SSH (o Telnet). Zenoss organiza los dispositivos por usuarios, grupos y sistemas, uno de los conceptos más poderoso de Zenoss es clases el cual maneja la clasificación jerárquica de dispositivos.

■ **Monitorización de Disponibilidad**

Mediante el uso de ICMP y SNMP, Zenoss informa sobre la disponibilidad que tiene de los siguientes dispositivos:

- Dispositivos de Red.
- Servidores de TCP / IP y Puertos.
- Disponibilidad de URL.
- Servicios y Procesos de Windows.
- Procesos de Linux / Unix.

Los monitores de rendimiento recogen datos de serie de tiempo y proporcionan gráficas de análisis de los siguientes componentes:

- Estadísticas del Sistema de Archivos.
- CPU y uso de Memoria.
- Monitoreo de JMX para servidores J2EEE (Disponible a través de ZenPack).
- Soporte para plugins de Nagios y Cacti.

■ **Gestión de Eventos**

Zenoss supervisa gran cantidad de eventos que se dan incluyendo, syslog, disponibilidad, rendimiento de monitores, trampas SNMP, registro de eventos de Windows y scripts personalizados. Las características principales son:

- Eventos Personalizados.
- Priorización automática de Eventos.
- Eventos de Depuración.
- Correlación de Eventos.

■ **Arquitectura de Plugin**

Zenoss dispone de varias opciones y maneras para ampliar la base para su funcionamiento, los que son:

- ZenPacks.
- Plugins de Nagios.
- Plugins de Cacti.

También se puede desarrollar nuestros propios plugins.

■ **Informes del Sistema**

Zenoss empaqueta un conjunto de informes estándar el cual permite observar lo que sucede en este momento, así como lo que ha sucedido en el pasado, los informes se integran con la gestión de dispositivos, monitores de rendimiento, eventos y funciones de usuario.

Manipulación de la Herramienta

■ **Agregar Dispositivos**

Zenoss muestra los dispositivos de las redes a las que puede acceder con las diferentes referencias que estos les brinda, permitiendo al administrador de la red identificar y posteriormente administrarlo.

■ **Agregar Dispositivos Manualmente**

Para agregar dispositivos de forma Manual, en la Barra de Navegación selecciona Infraestructura, en el icono (+) donde aparece la siguiente opción:
Add a Single Device.

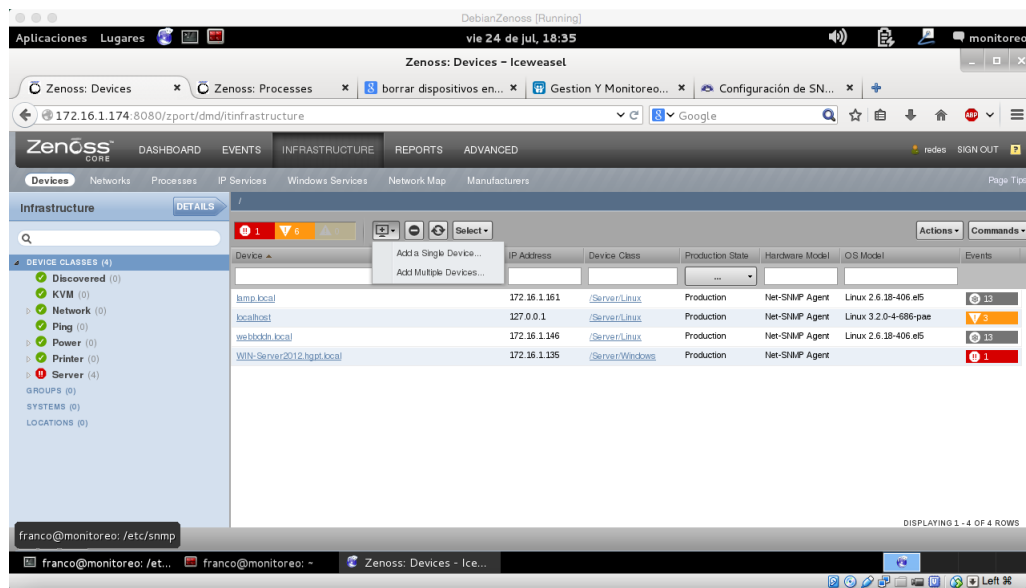


Figura 26: Agregar Dispositivos a Monitorear.
Elaborado por: El Investigador.

En esta parte se agrega la dirección Ip o el nombre del Host y sus respectivas opciones, la cuales son: Nombre o Ip, Clase de Dispositivo, Colector, Modelo. Si le damos en la opción More, agregaremos Snmp Community, Snmp Port, además la información Hardware y Software del dispositivo.

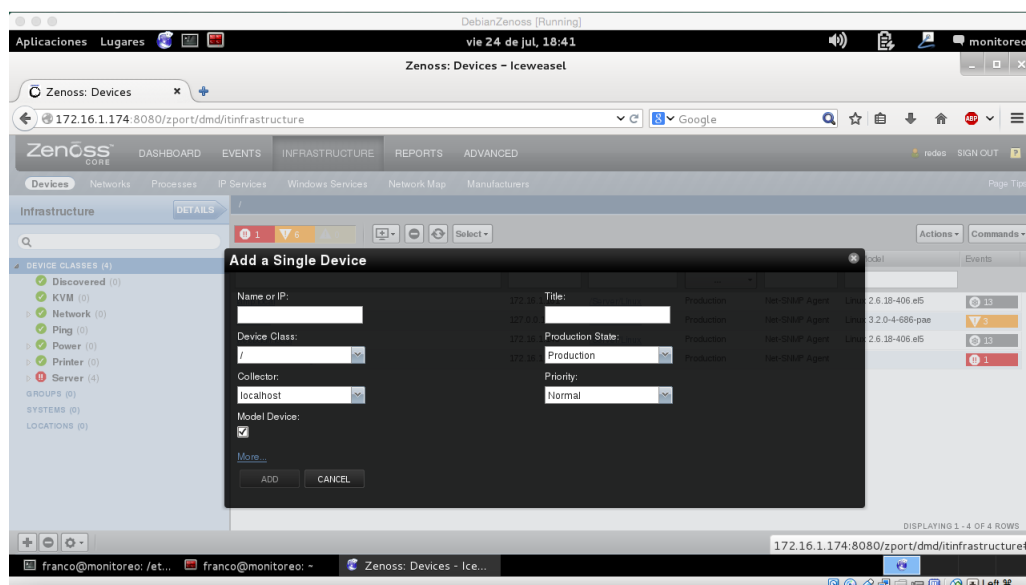


Figura 27: Dispositivos de forma Manual.
Elaborado por: El Investigador.

En la siguiente captura se observa los dispositivos Agregados.

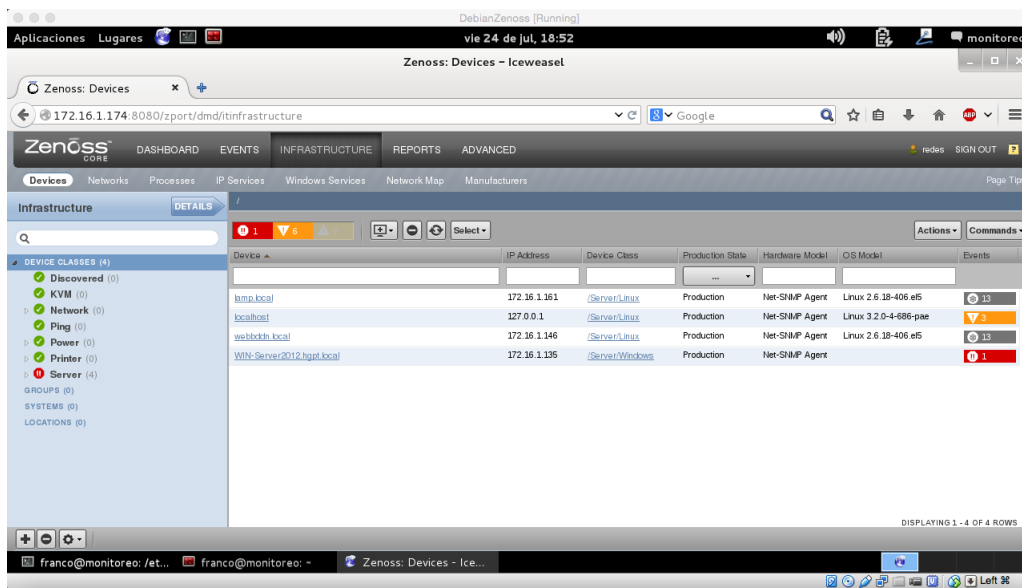


Figura 28: Dispositivos Agregados.
Elaborado por: El Investigador.

- **Agregar Múltiples Dispositivos**

Para Agregar dispositivos de forma múltiple, se ubicara en la Barra de Navegación se selecciona Infraestructura, en el icono (+) donde aparece la siguiente opción. Add Multiple Device.

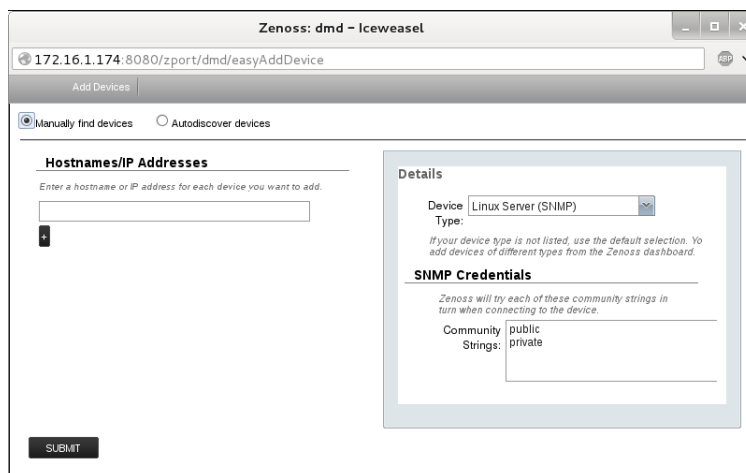


Figura 29: Agregar Múltiples Dispositivos.
Elaborado por: El Investigador.

En la ventana se observa dos opciones, las que son: Manually Find Device y Autodiscover Device. En donde se introducirán las credenciales adecuadas de configuración para el dispositivo.

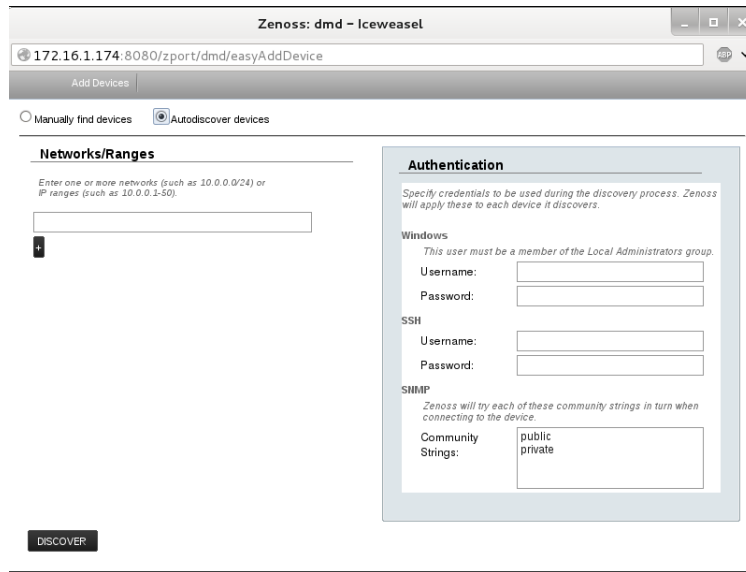


Figura 30: Descubrimiento de Dispositivos.
Elaborado por: El Investigador.

■ Trabajar con Dispositivos

Lista de Dispositivos Agregados, desde esta imagen se observa la tarea de gestión de los dispositivos; se va cal organizando en vista de árbol:

- Clase de dispositivo
- Grupo
- Sistema
- Ubicación

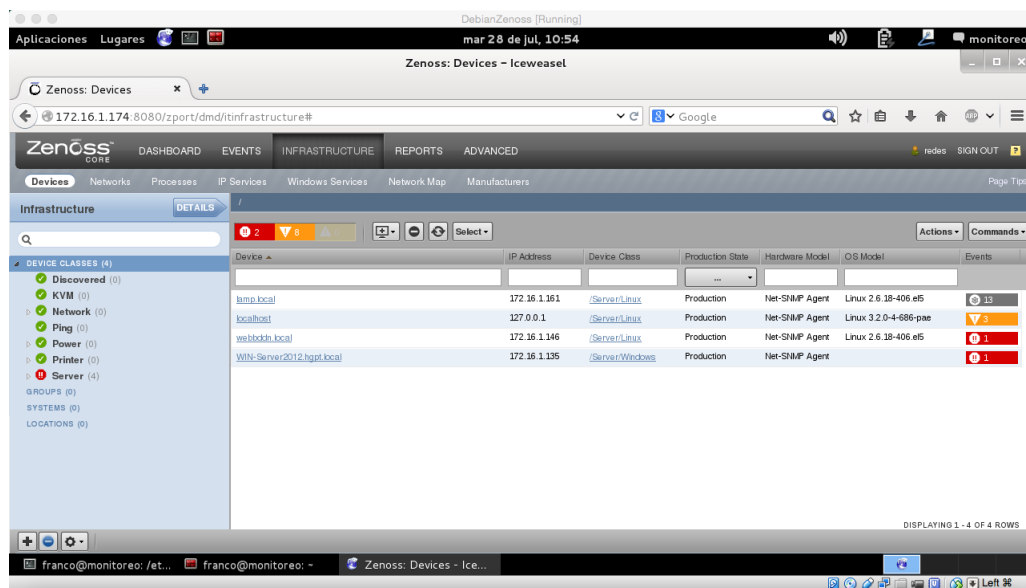


Figura 31: Dispositivos Agregados.
Elaborado por: El Investigador.

Al dar click sobre cada dispositivo se observa las opciones que tienen cada uno de ellos, en esta parte ve el “Arco iris de Eventos” el cual da el estado del dispositivo, además se observa:

- Nombre del Dispositivo
- Dirección Ip utilizada
- Estado del Dispositivo
- Estado de Producción

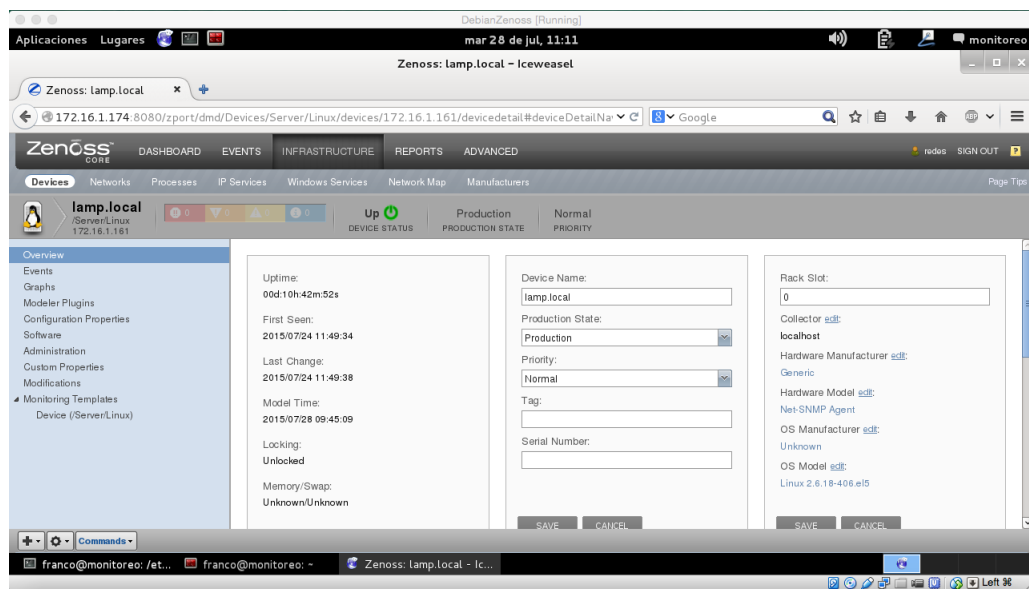


Figura 32: Descripción del Dispositivos
Elaborado por: El Investigador.

En el panel izquierdo del la herramienta se observa las diferentes opciones que se tiene en los dispositivos.

- Componentes
- Software
- Gráficas
- Administración
- Propiedades de Configuración

■ Componentes

Se observa la información que facilita sobre los diferentes dispositivos, en los que se incluye: IpService, WinService, IpRouteEntry, IpInterface, CPU, Sistema de Archivos.

- **Software**

Los datos que se obtiene en software son netamente sobre la estructura de los dispositivos mencionados.

- **Gráficas**

Por medio de las gráficas se observa el rendimiento de los dispositivos monitoreados, en el se da uso de sus opciones: Desplazamiento, Acercar / Alejar, Rango(obtener datos por periodo de tiempo).

- **Administración**

Crear, gestiona, ejecuta opciones personalizadas del usuario, a la vez determina la capacidades de administración para el dispositivo y sus funciones.

- **Propiedades de Configuración**

Establece la correcta configuración del dispositivo.

- **Monitoreo de Servicios y Alertas de Correo Electrónico**

Para las alertas de correo electrónico se crea un nuevo usuario:

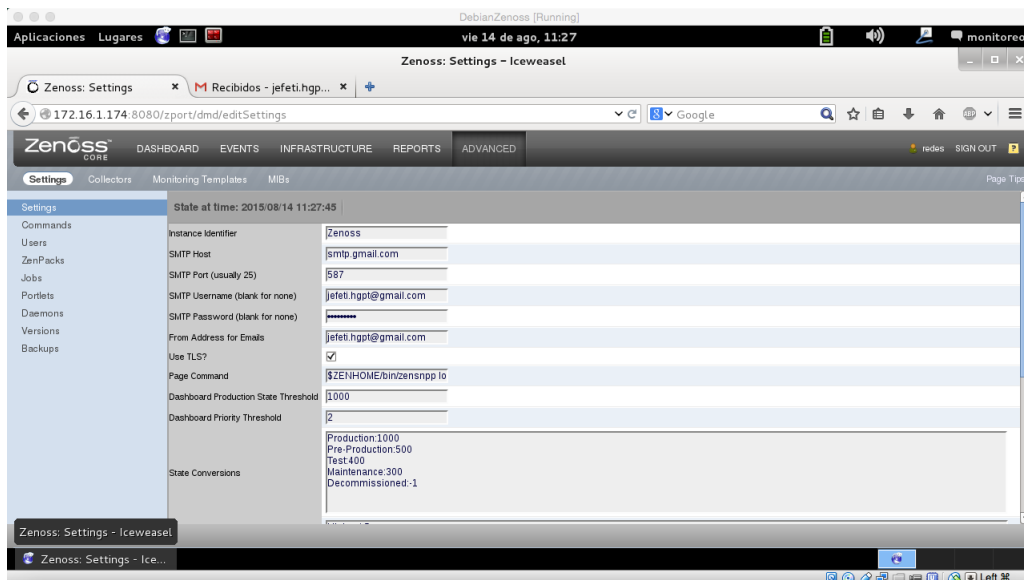


Figura 33: Agregar Usuarios.
Elaborado por: El Investigador.

Al dar click sobre usuario, en configuraciones, se podrá Agregar el usuario:

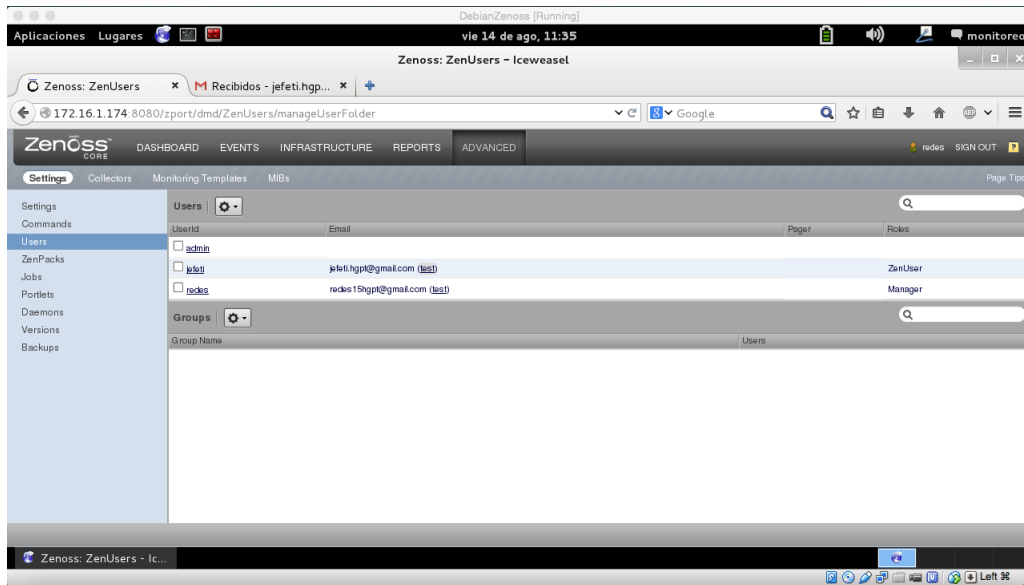


Figura 34: Configuración de Usuarios.
Elaborado por: El Investigador.

De esta manera permite la definición del nombre del usuario y el email:

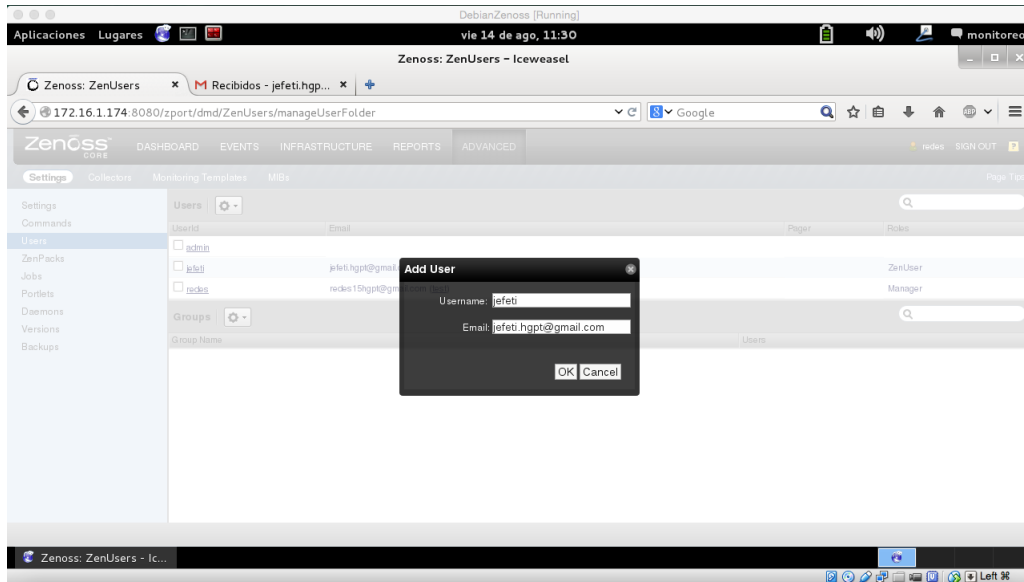


Figura 35: Usuario y Email.
Elaborado por: El Investigador.

Una vez creado el usuario se habilita el correo electrónico para recibir las alertas de los servicios de Red los cuales no están en funcionamiento, al dirigirse hacia las configuraciones se activa el puerto SMTP que es 587, el cual permite la transferencia(recepción-envío) de los correos electrónicos.

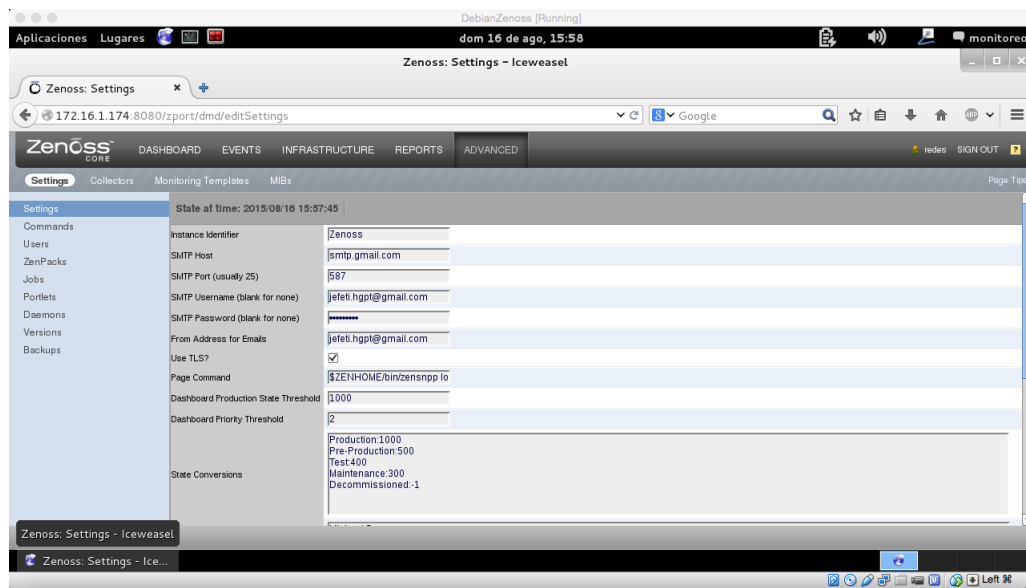


Figura 36: Configuración para Alerta de Correo Electrónico.
Elaborado por: El Investigador.

Al dar click sobre el usuario definido anteriormente “jefeti” se observa la configuración.

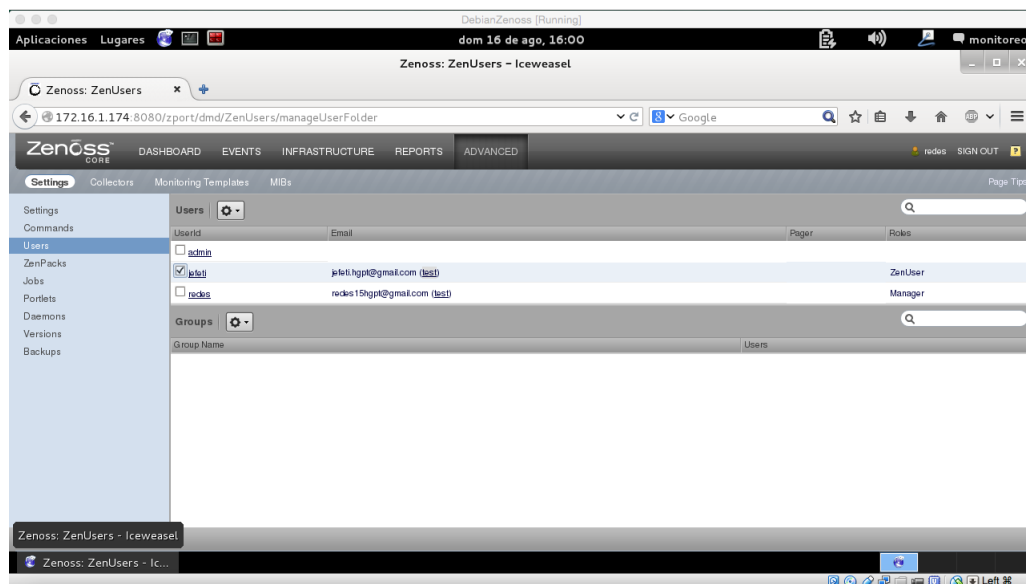


Figura 37: Configuración de Alerta de Usuario.
Elaborado por: El Investigador.

Permitiendo de esta manera ubicarse en las alertas, a las cuales se agrega una nueva regla.

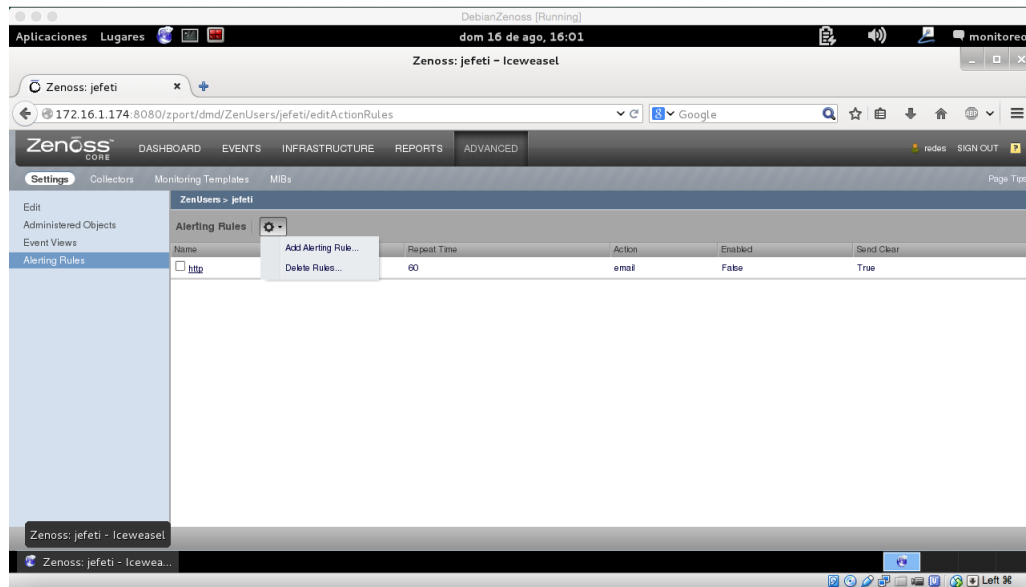


Figura 38: Añadir Alerta.
Elaborado por: El Investigador.

De esta manera se añade la alerta del protocolo de comunicación “http”.

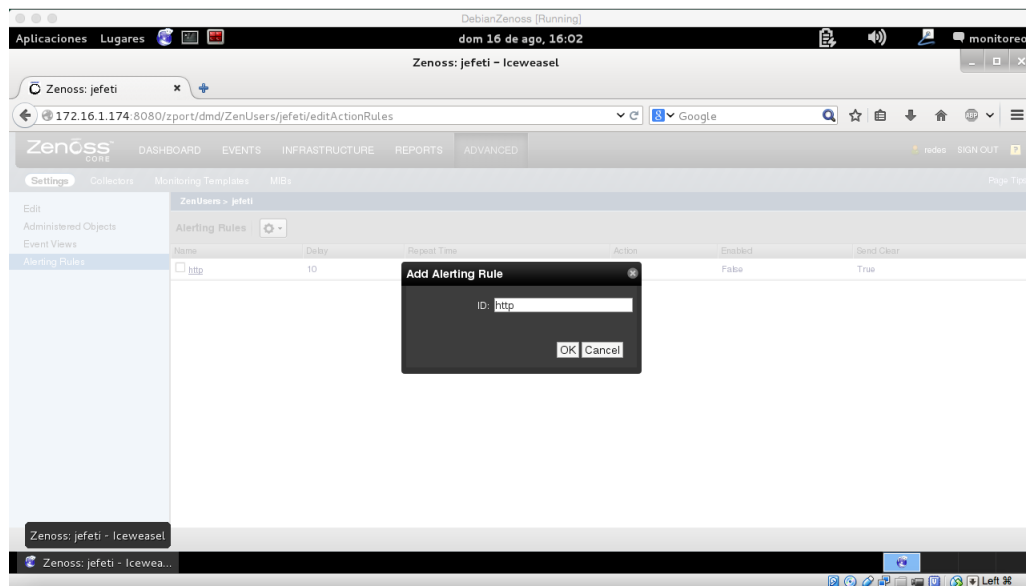


Figura 39: Definir ID para la Alerta.
Elaborado por: El Investigador.

Una vez terminado de agregar el protocolo “http” se añade las configuraciones las cuales son ID del protocolo, se habilita el tiempo de llegada de los mensajes y se procede a guardar la configuración.

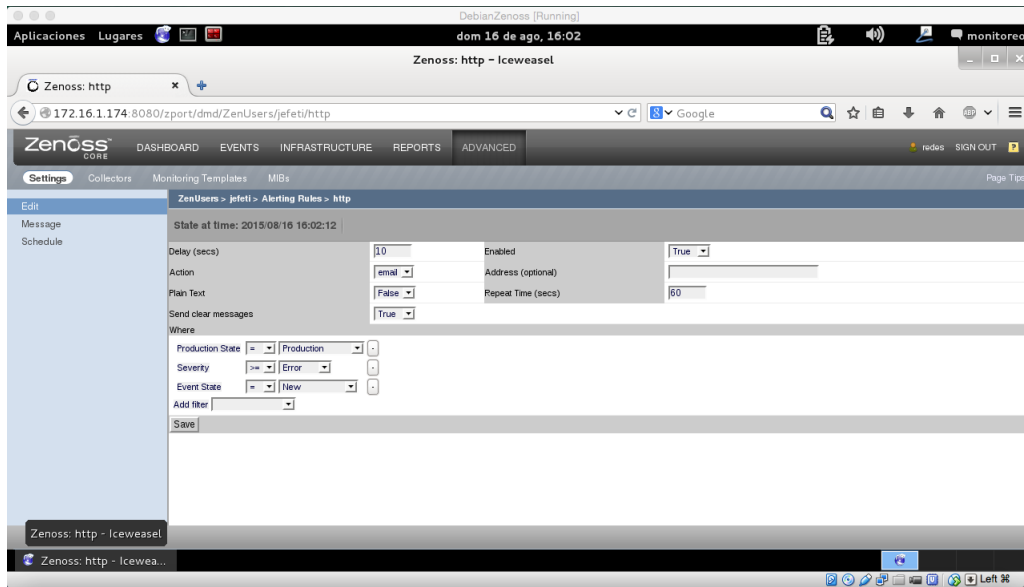


Figura 40: Configuración de Alerta de Usuario.
Elaborado por: El Investigador.

Se debe elegir en el presente caso “Service Class” y “Protocol” al cual se enviaran los datos.

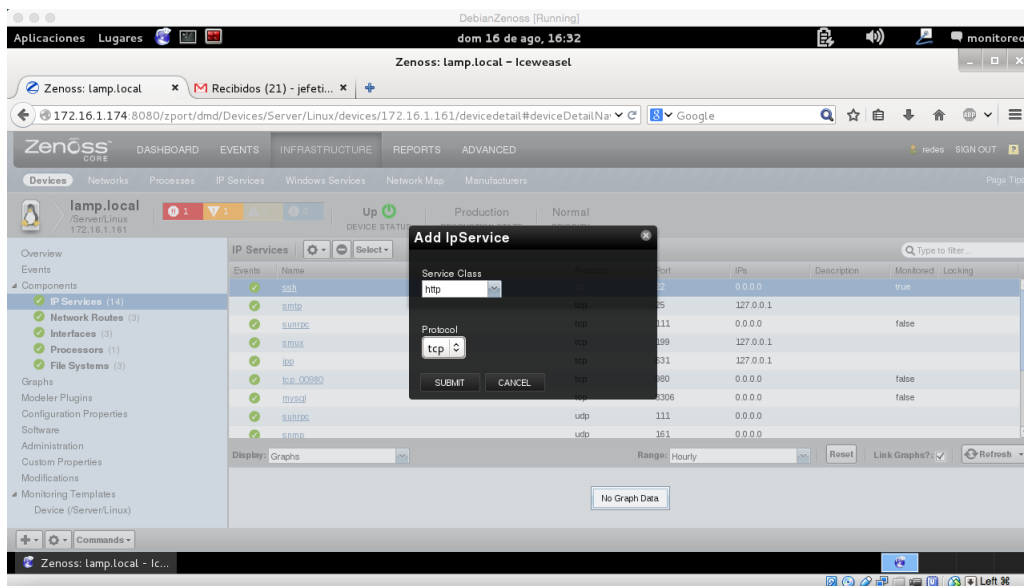


Figura 41: Añadir servicio a Http.
Elaborado por: El Investigador.

Se puede observar que al dar click sobre Infraestructura se observa los dispositivos.

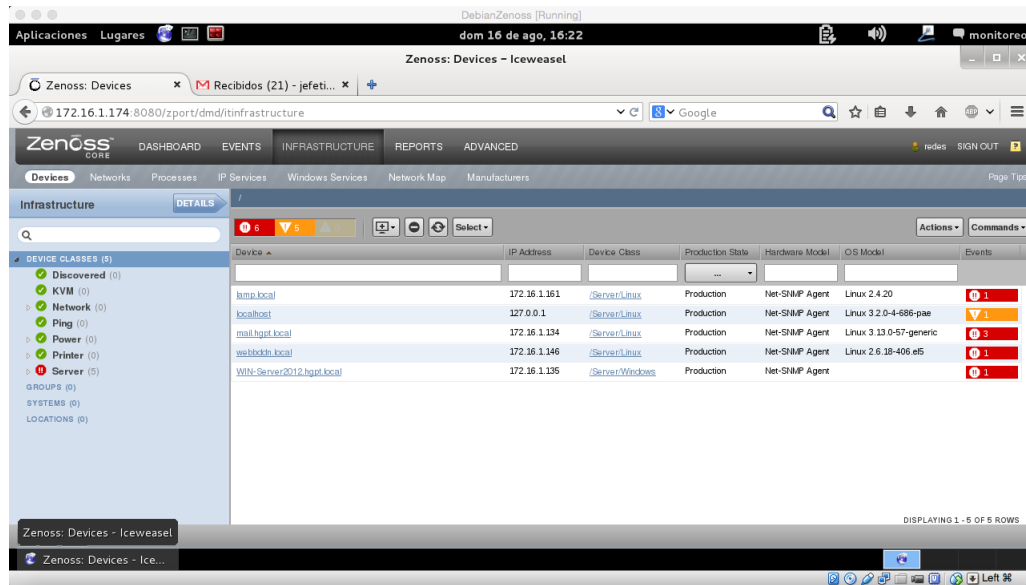


Figura 42: Lista de Dispositivos.
Elaborado por: El Investigador.

Imágenes del protocolo “http” del servidor “CentOS lamp” a monitorear.

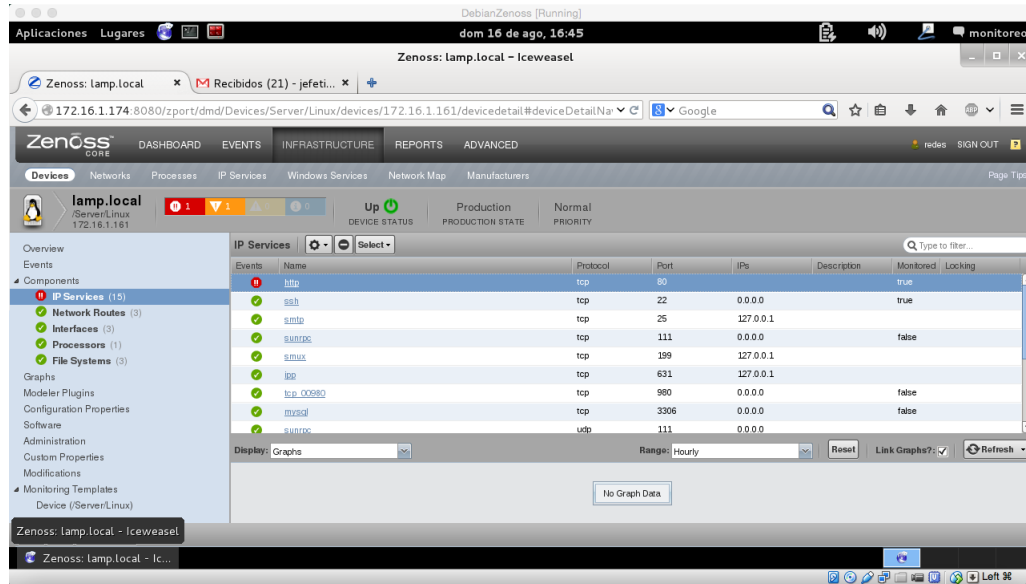


Figura 43: Servicio Http.
Elaborado por: El Investigador.

Verificar el estado de servicio “http” en la terminal del servidor “CentOS lamp”.

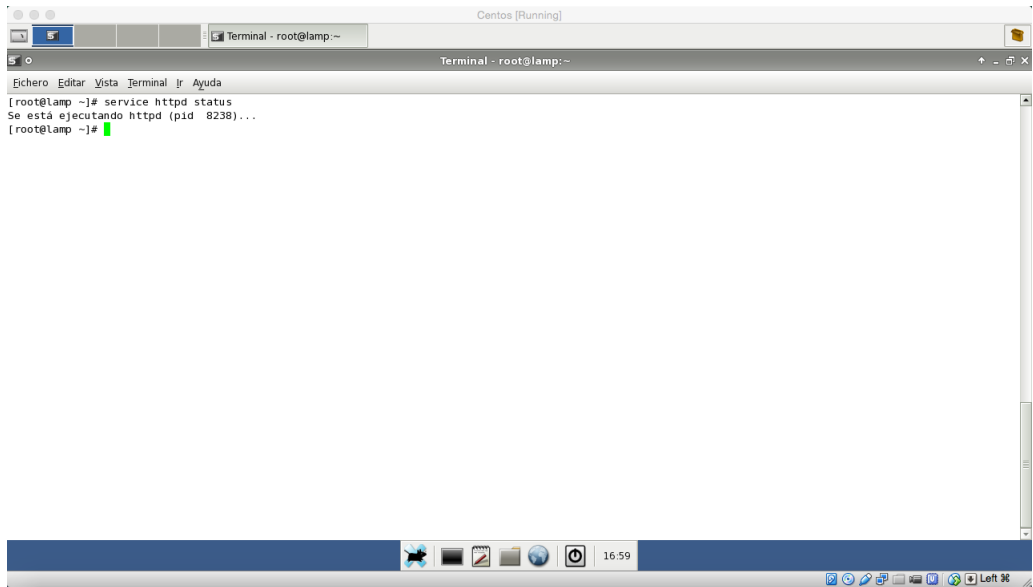


Figura 44: Estado del servicio http en CentOS.
Elaborado por: El Investigador.

Estado Inactivo del protocolo “http” en la terminal del servidor “CentOS lamp”.

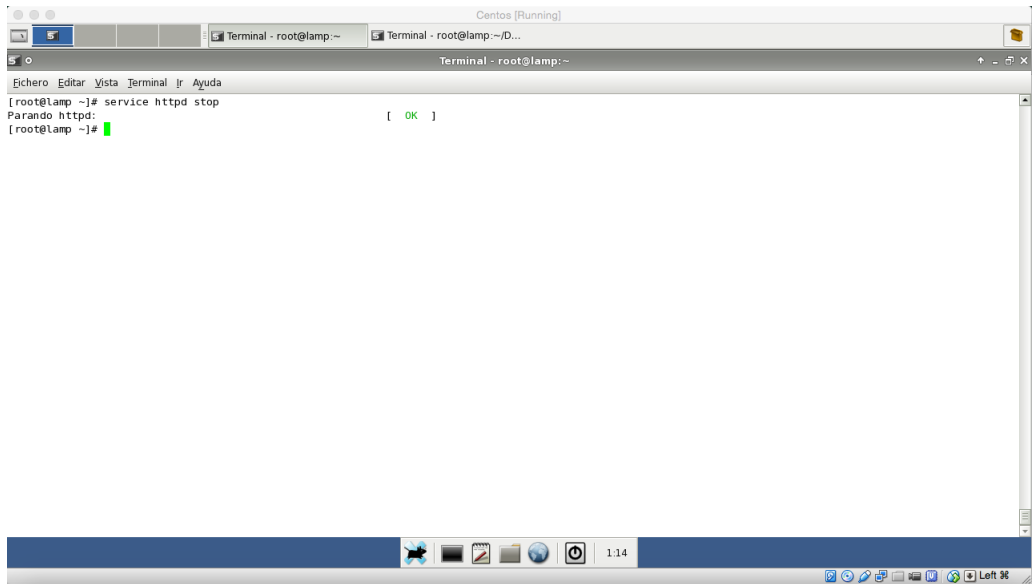


Figura 45: Verificar el servicio http en CentOS.
Elaborado por: El Investigador.

Estado Inactivo del protocolo “http” en la consola de administración Zenoss.

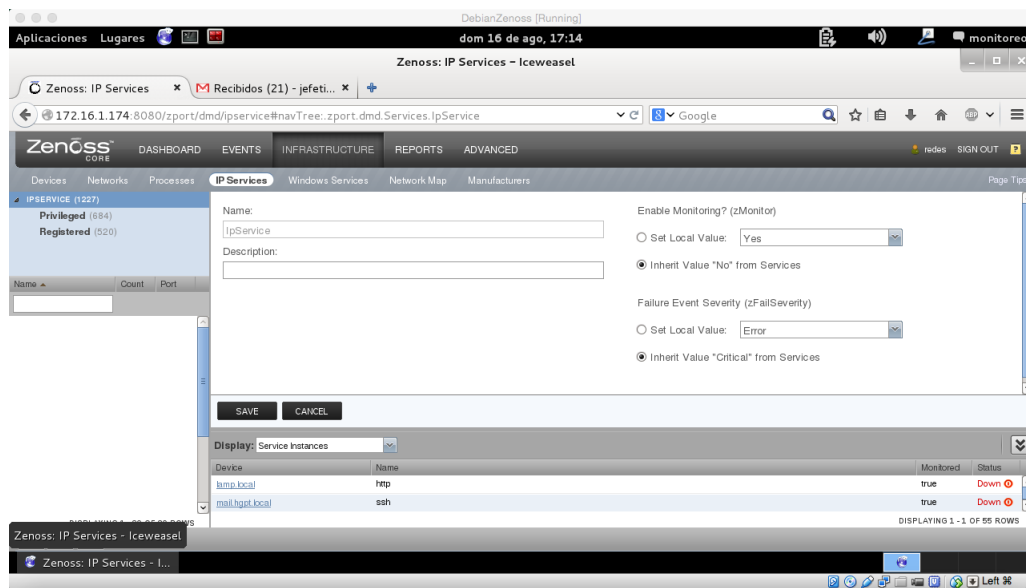


Figura 46: Verificar el servicio http en CentOS.
Elaborado por: El Investigador.

Alertas de mensajes recibidos en el correo electrónico.

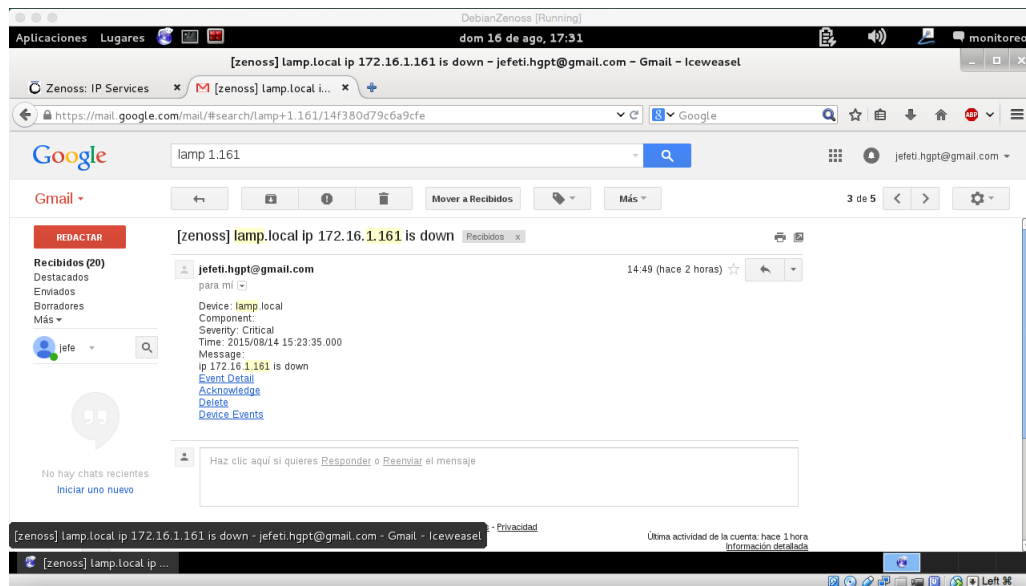


Figura 47: Alerta de Correo Electrónico.
Elaborado por: El Investigador.

4.4. Implementar la herramienta Open Source en los equipos en Producción del HGPT.

Ejecución de la Herramienta Zenoss en Producción

En la siguientes imágenes se observa la interfaz de Administración Web de la

Herramienta de Monitoreo Zenoss la cual facilita el trabajo del Administrador tanto de TI como el de Administrador de la Red del HGPT, con lo anteriormente mencionado se puede decir que esto ayudara a la reducción significativa de tiempo para la administración de los equipos concernientes al Área de TI del Honorable Gobierno Provincial de Tungurahua.

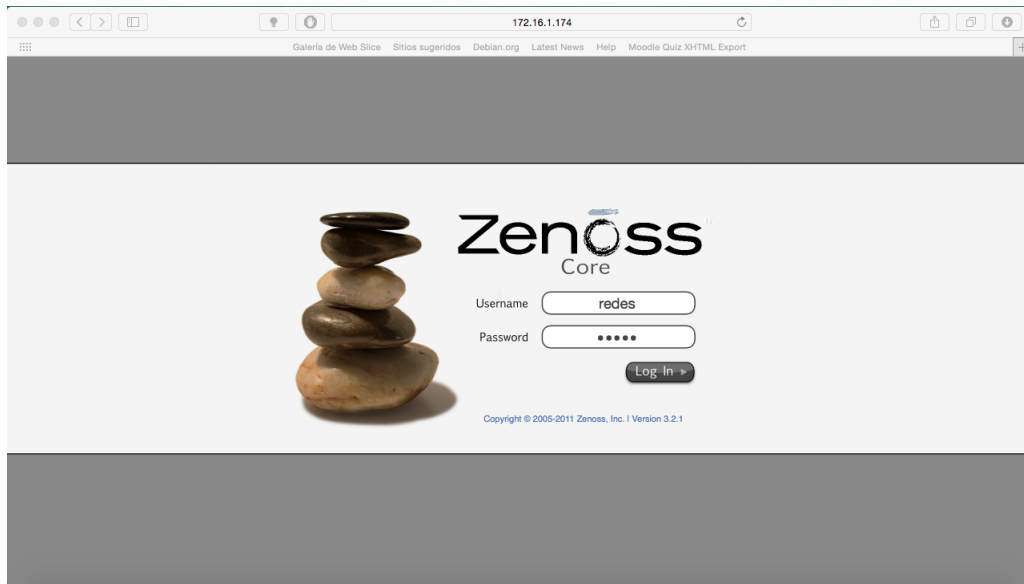


Figura 48: Ingreso a Zennos.
Elaborado por: El Investigador.

Se observa la consola de eventos:

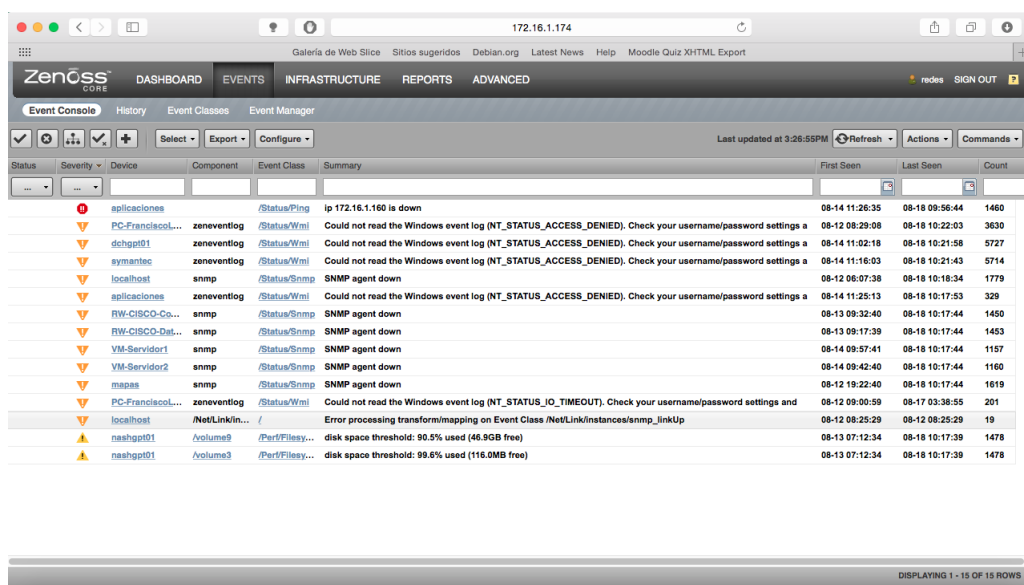


Figura 49: Consola de Eventos del HGPT.
Elaborado por: El Investigador.

El histórico de Eventos, entre otros.

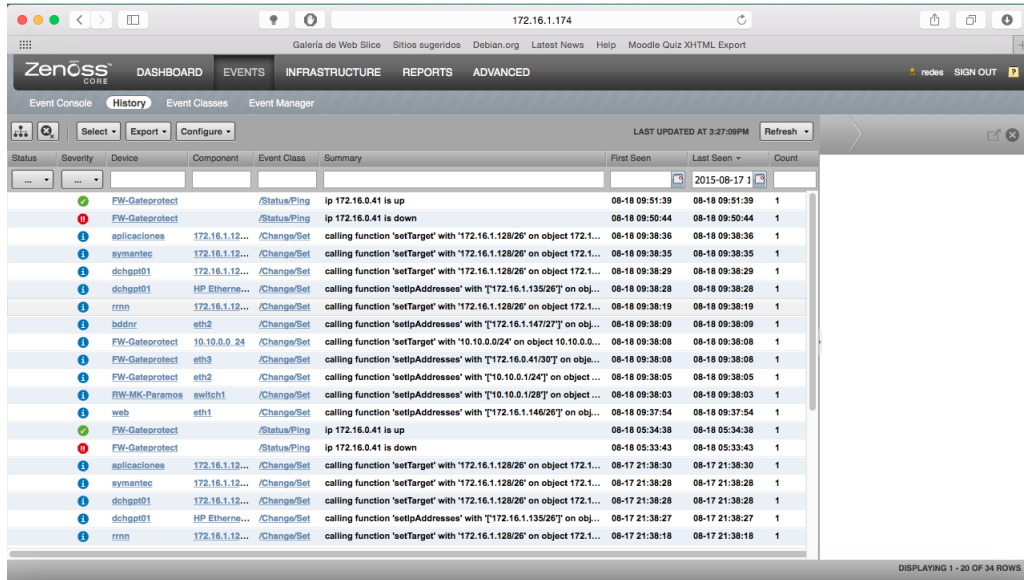


Figura 50: Historial de Eventos.
Elaborado por: El Investigador.

Dispositivos Actualmente monitoreados en producción del HGPT.

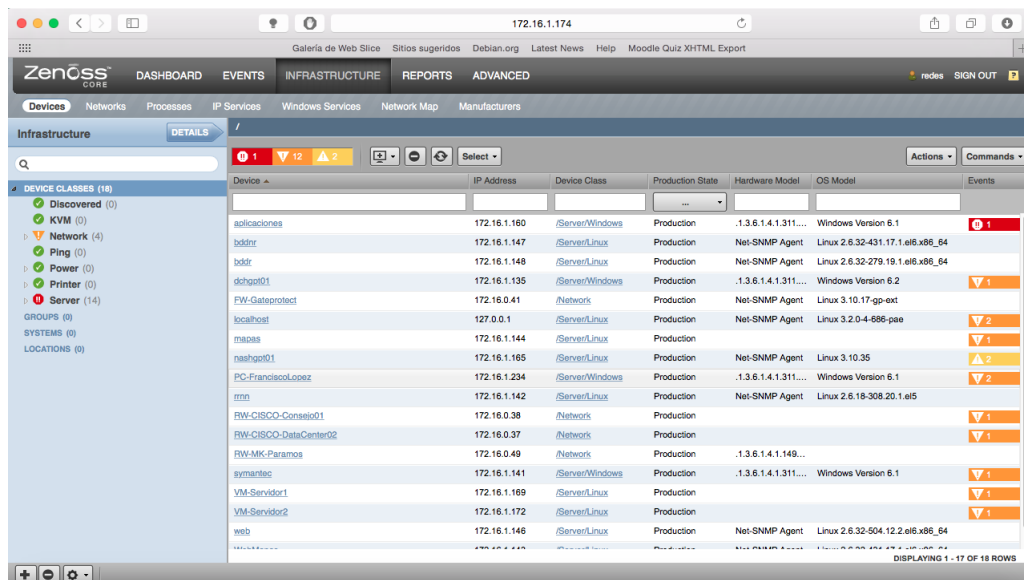


Figura 51: Historial de Eventos.
Elaborado por: El Investigador.

Equipos de TI en Producción Monitoreados del HGPT.

Los Datos recolectados de los Servidores en Producción del Honorable Gobierno Provincial de Tungurahua fueron tomados desde el día miércoles 12 de agosto

hasta el día martes 18 de agosto del presente año, los cuales constan de los siguientes parámetros monitoreados:

- Transmisión de Datos por interface de Red.
- Uso del Sistema de Archivos.
- Media de Carga al Sistema.
- Uso del CPU.
- Uso de Memoria.
- Escritura y Lectura en Disco.

De los cuales se monitorea los servidores que constan en la siguiente tabla:

Tabla 15: Tabla de Servidores en Producción del HGPT.

Servidores en Producción del HGPT:
Servidor de Base de Datos No Relacional.
Servidor Web Mapas del HGPT.
Servidor de Recursos Hídricos del HGPT.
Servidor de Web del HGPT.

Elaborado por: El Investigador.

Medición de uso de la interface de Red.

Una vez ejecutada la aplicación se procedió a tomar los de datos de la interface de Red, en este caso del Servidor de la Base de Datos No Relacional HGPT, la cual muestra el rendimiento, paquetes y errores por interface de red.

- Transmisión de Datos por interface de Red:

Se puede evidenciar claramente que las peticiones hacia la interfaz eth2 entre Martes y Domingo se mantienen en un promedio de 2 megas/sec. y en inicio de semana alcanzan un máximo de 9.30 megas/sec., a la vez que al inicio de semana hay más peticiones hacia el servidor de la BBDNR, como lo indica la figura 52.

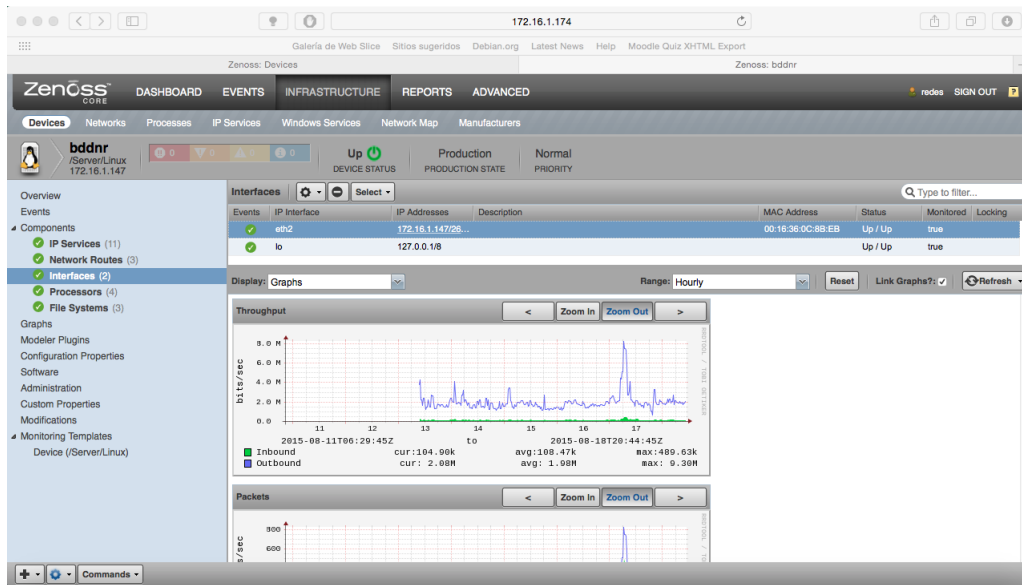


Figura 52: Transmisión de paquetes en la BBNR.
Elaborado por: El Investigador.

En la transmisión de paquetes se evidencia, las características:

- > Máxima transmisión en “INBOUND-MAX-ENTRADA”: 550.50 packets/sec.
- > Máxima transmisión en “OUTBOUND-MAX-SALIDA”: 929.94 packets/sec.
- > Media transmisión en “INBOUND-AVG-ENTRADA”: 124.28 packets/sec.
- > Media transmisión en “OUTBOUND-AVG-SALIDA”: 197.35 packets/sec.
- > Promedio actual transmisión en “INBOUND-CUR-ENTRADA”: 127.52 packets/sec.
- > Promedio actual transmisión en “OUTBOUND-CUR-SALIDA”: 204.14 packets/sec.

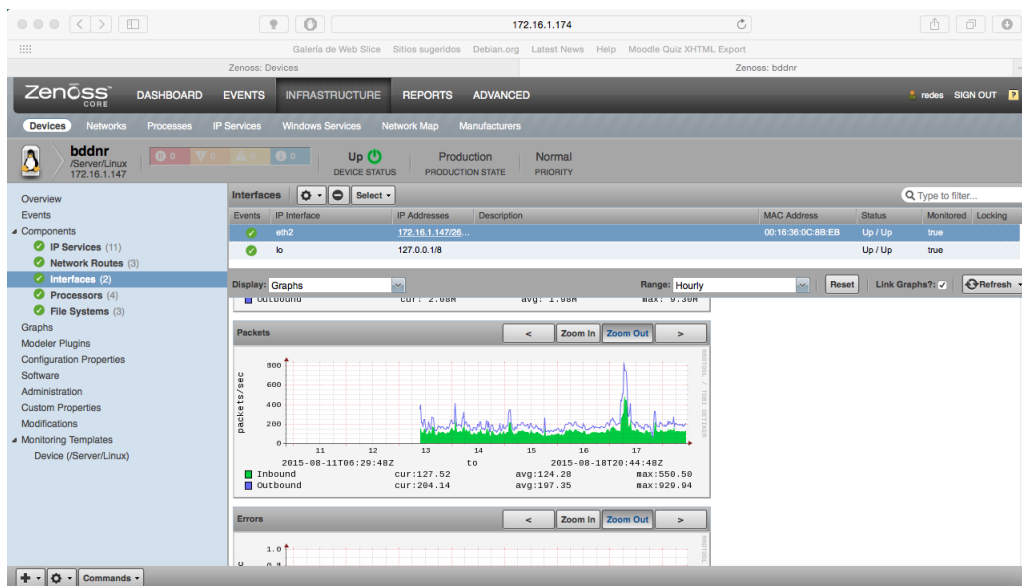


Figura 53: Transmisión de Paquetes en la BBNR.
Elaborado por: El Investigador.

En la transmisión de paquetes no existe ningún tipo de error.

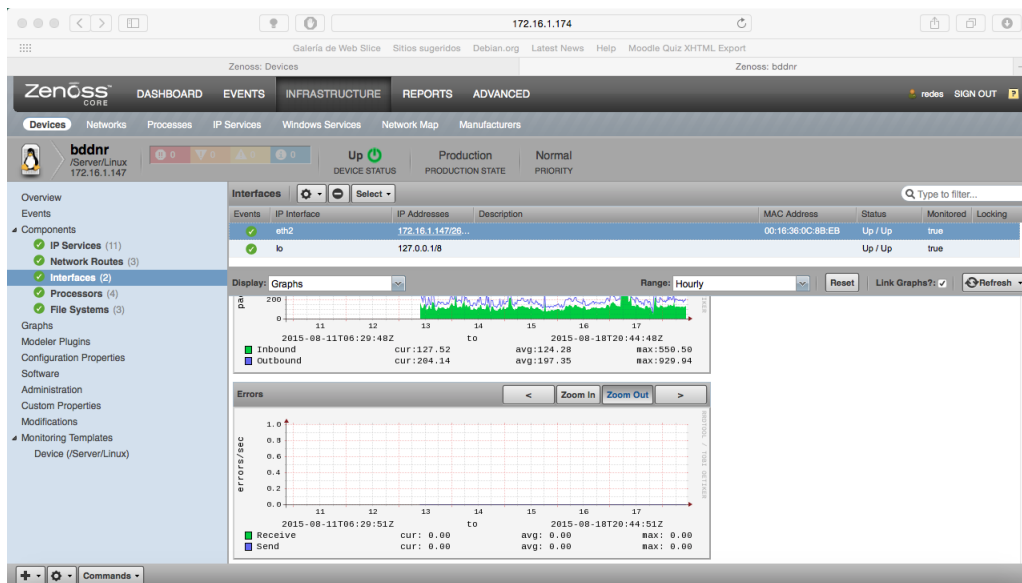


Figura 54: Error en la Transmisión de Paquetes en la BBNR.
Elaborado por: El Investigador.

Uso del Sistema de Archivos.

Una vez ejecutada la aplicación se procedió a tomar los de datos del uso del sistema de archivos, en este caso del Servidor Web Mapas del HGPT, la cual muestra las siguientes gráficas.

- Uso del sistema de archivos raíz del cual se interpreta que su uso esta en 90% del 100% esta información es útil para tomar decisiones al momento de administrar nuestros equipos de TI en el presente caso el sistema de archivos del Servidor de Web Mapas tiene que ser ampliado el disco para mejorar la capacidad almacenamiento en el servidor.

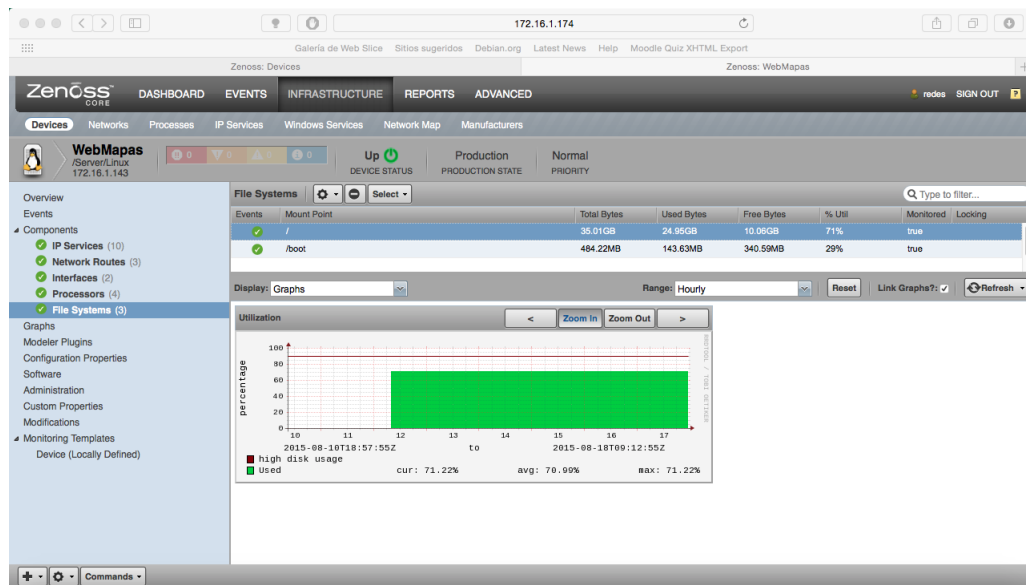


Figura 55: Uso del Sistema de Archivos raíz en el Servidor Web de Mapas.
Elaborado por: El Investigador.

- En el caso del boot no existe ningún tipo de modificación ya que se encuentra funcionando manera adecuada.

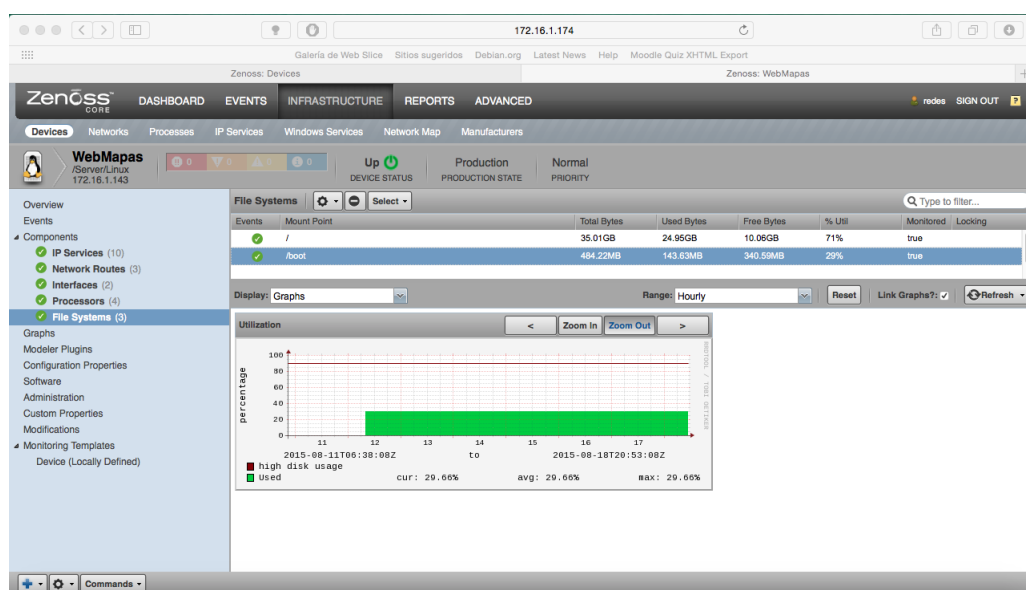


Figura 56: Uso del Sistema de Archivos del Servidor Web de Mapas.
Elaborado por: El Investigador.

- Media de Carga al Sistema.

Se puede evidenciar claramente que el Servidor de Web Mapas no tiene muchas solicitudes hacia el, ya que la mayor parte del tiempo tiene una carga mínima de 0.01 megas y esporádicamente alcanza un pico máximo de 0.53 megas.

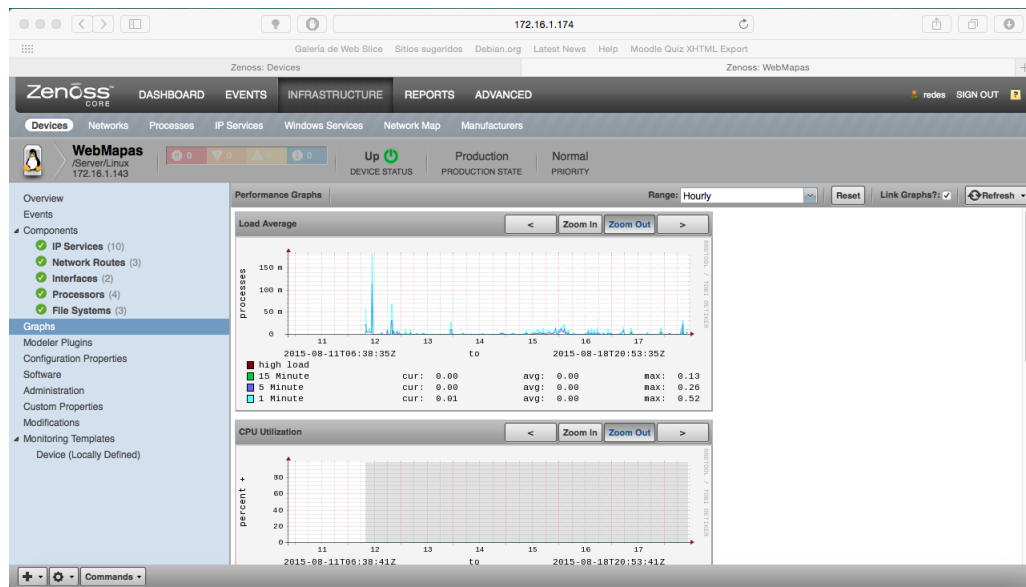


Figura 57: Carga de Datos hacia el Servidor Web de Mapas.
Elaborado por: El Investigador.

Uso del CPU, memoria, lectura y escritura en disco.

Una vez ejecutada la aplicación se procedió a tomar los de datos del uso de la media de carga, cpu, memoria, lectura y escritura en disco, en este caso del Servidor de Recursos Hídricos del HGPT, la cual muestra las siguientes gráficas.

- Media de Carga al Sistema, en esta imagen se observa que no hay ningún contratiempo y que todo esta estable.

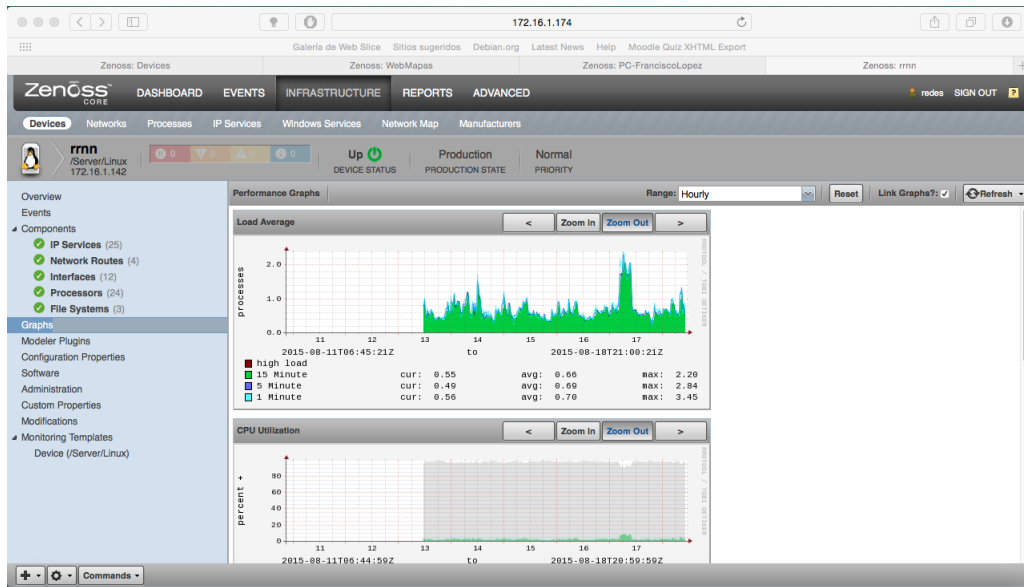


Figura 58: Carga de Datos hacia el Servidor de Recursos Hídricos.
Elaborado por: El Investigador.

- Uso del CPU, se observa que su utilización es “idle” lo cual se dice que no esta siendo usado por ningún otro programa lo cual dice que el CPU se ejecuta en prioridad baja, esto puede conllevar a que los recursos del servidor sean re asignados por motivo que se desperdician sus recursos.

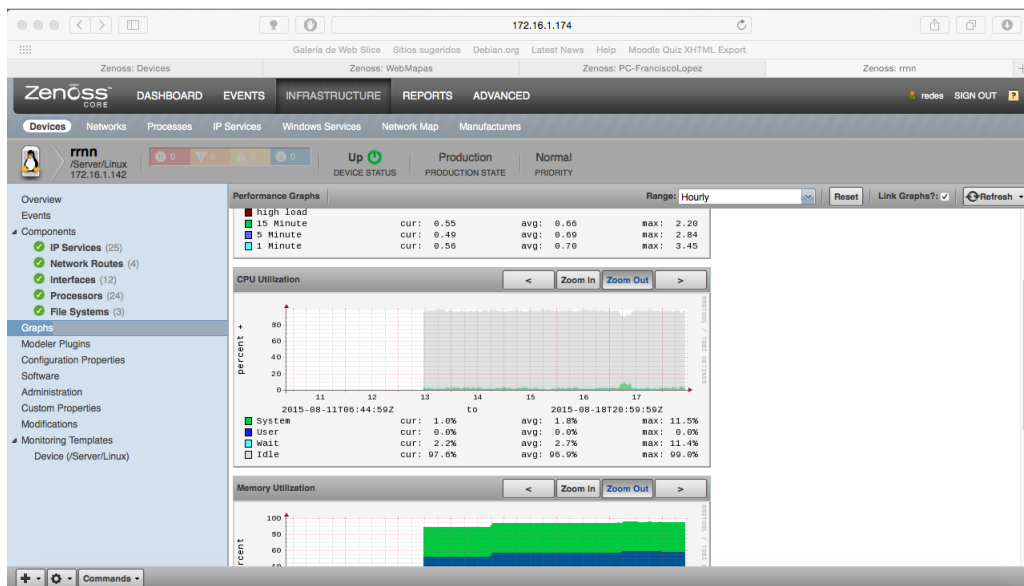


Figura 59: Uso del CPU en el Servidor de Recursos Hídricos.
Elaborado por: El Investigador.

- Uso de Memoria se describe que la memoria en uso es de un 95.6% y el buffered es de 58.8% lo cual se dice que es necesario aplicar un aumento de memoria al

Servidor.

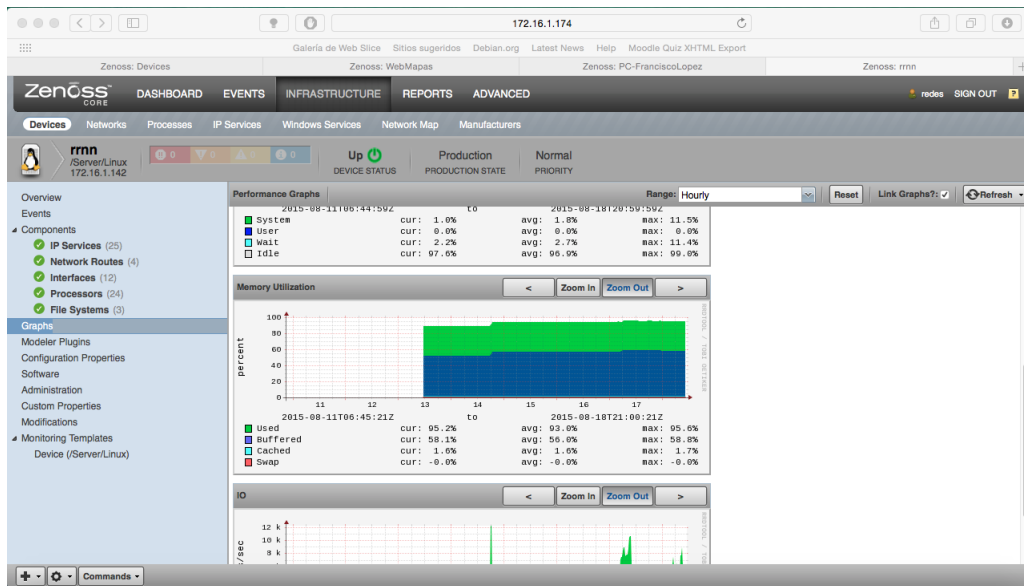


Figura 60: Uso de Memoria en el Servidor de Recursos Hídricos.
Elaborado por: El Investigador.

- Escritura y Lectura en Disco, muestra que hay mas peticiones de escritura que de lectura lo cual concuerda con el uso de la memoria ya que recibiendo más peticiones de entrada que de salida.

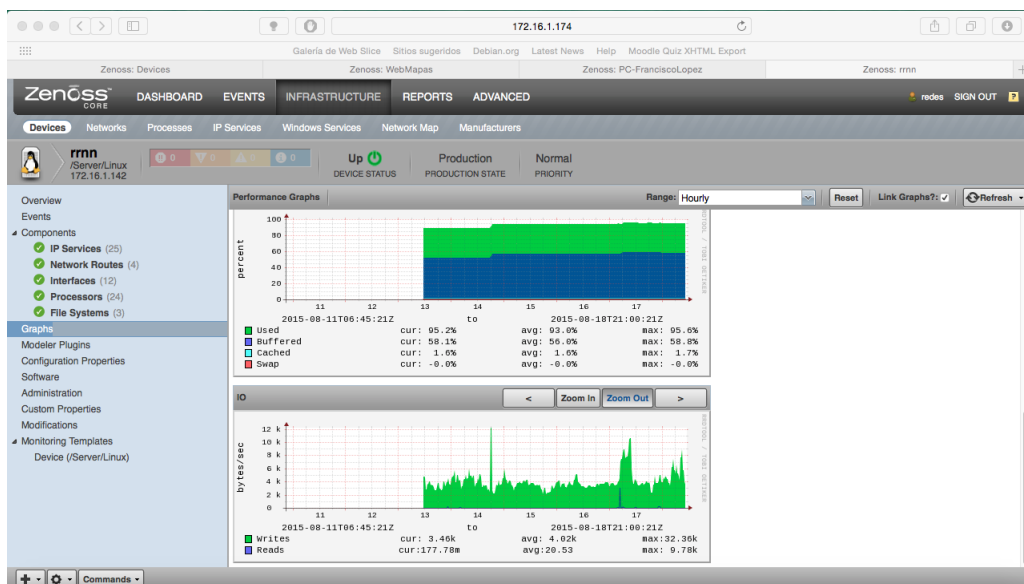


Figura 61: Lectura y Escritura en Disco del Servidor de Recursos Hídricos.
Elaborado por: El Investigador.

4.5. Tomar decisiones adecuadas para resolver problemas que se observan en la Red de Datos & VoIP.

El planteamiento para la toma de decisiones en el Honorable Gobierno Provincial de Tungurahua sobre su infraestructura en el Área de TI tanto a nivel de Talento Humano como de Recursos Informáticos da lugar a dos enfoques; por una parte se observa la gran cantidad de servidores y equipos de red lo que conlleva a la obligación de buscar la forma más idónea para supervisar la infraestructura del mismo; sustentándose en el previo análisis de las Herramientas de Monitoreo se crea un escenario local para no interrumpir los procesos de producción por ser susceptibles al monitoreo de red. Por otra parte con la implementación de la propuesta se tiene un enfoque administrativo global y con la ayuda de la herramienta implantada da lugar a una visión en tiempo real de la infraestructura de Red lo que permite tomar decisiones más acertadas tanto en recursos, problemas y sugerencias ya existentes como futuras dentro de lo concerniente a la red de datos.

Referente el Servidor de la Base de Datos No Relacional se sugiere crear otro servidor para balancear la carga de datos lo cual permite mejorar notablemente su funcionamiento.

Para el Servidor de Web Mapas se sugiere el aumentar la capacidad de sus Disco Duro ya que esta siendo usado en 80 % de su capacidad lo que conlleva a a que sus transmisión sea muy lenta.

4.6. Optimizar los recursos de Red de Datos & VoIP del Gobierno Provincial de Tungurahua.

Durante la optimización de los recursos de Red de Datos & VoIP de Honorable Gobierno Provincial de Tungurahua, da lugar al análisis de los escenarios convencionales encontrados en la actualidad para la administración, los que citan: ssh, telnet los que trabajan como interpretes de comandos, otros manejan una interfaz gráfica remota para la manipulación de los equipos como son: VNC, TeamViewer los cuales no son factibles ni viables para manipular y administrar un gran número de servidores y equipos de TI ya que consumen tiempo, son complejos en la asignación de personal en cada área a más de ello consumen recursos de Red. Concluido el análisis de los diferentes protocolos se muestra que el protocolo SNMP es el que menos recursos consume además por medio de este protocolo se logra la centralización de información en la administración de equipos de TI el cual se complementa con la utilización de la Herramienta de Monitoreo Zenoss

lo que permite visualizar la información en una consola de Administración en un entorno Web.

CAPÍTULO 5

Conclusiones y Recomendaciones

5.1. Conclusiones

- Mediante el estudio del estado actual de la red de Datos y VoIP del Honorable Gobierno Provincial de Tungurahua se pudo obtener y aseverar que no se tiene un buen control al momento de monitorear los equipos de TI ya que no se cuenta con la información centralizada lo cual genera puntos críticos en la infraestructura de red ocasionado retardos al mostrar si algún equipo TI falle.
- Los puntos críticos en la red de Datos y VoIP del Honorable Gobierno Provincial de Tungurahua se ubica en los servidores configurados por el Área de TI, puesto que con estos se manejan los datos en producción los cuales por la pérdida de información generan inconsistencias en los datos al momento de trabajar con ellos.
- Se comprobó que Zennos es un aplicación que ayuda a tener una mejor coordinación entre dispositivos y los administradores tanto de TI como de Red, lo cual proporciona un alto rendimiento al momento de administrar los diferentes dispositivos, lo que conlleva a la reducción de tiempos y a tener un alto performance al desarrollar dichas actividades.
- Con el modelado de escenarios localmente se pudo obtener una visión amplia sobre la administración de los recursos de TI a la vez de los servicios configurados, gracias a esto se determinó que la herramienta Zennos alcanza valores de alto rendimiento en el monitoreo de dispositivos, pudiendo mostrar los sucesos que tienen los recursos de TI.
- En el modelado de escenario local se pudo comprobar que para la configuración del protocolo SNMP tenga éxito en la comunicación se debe configurar correctamente los parámetros establecidos, por lo tanto configurar en windows el firewall, proveedor de SNMP de WMI y en Linux

las Iptables, el archivo de configuración snmp, snmpd, lo cual genera que Zenoss tenga un desempeño satisfactorio para su funcionamiento.

5.2. Recomendaciones

- Se recomienda al momento de utilizar Zenoss sea de manera local, mediante el navegador web, ya que de esta manera se puede consumir un menor número de recursos, que al ejecutar por escritorios remotos VNC, TeamViewer, o por interpretes de comandos SSH o TelNet, de esta manera se logrará tener un mayor performance al momento de manipular Zenoss.
- En el uso de Zenoss se recomienda tener en claro la configuración de grupo para la comunicación por medio del protocolo SNMP, gracias a esto se podrá observar y tener una comunicación exitosa al momento de monitorear los recursos de TI.
- Tener en claro los servicios instalados en nuestros servidores, en los equipos de TI y cuales de ellos se desea monitorear con Zenoss, más no olvidar en enviar la información a ser monitoreada desde la consola de administración de Zenoss.

Bibliografía

- [1] M. J. "B. González and M. Nieto, "Estudio comparativo - aplicaciones educativas gnu/linux de la upv-ehu," 2009.
- [2] J. Guerrero and A. Barba, "Arquitectura de referencia de gestión de red basada en políticas para un entorno integrado 3g-wlan," vol. 6, no. 2, p. 7, June 2008. [Online]. Available: http://www.ewh.ieee.org/reg/9/etrans/ieee/issues/vol06/vol6issue2June2008/6TLA2_15GuerreroIbanez.pdf
- [3] J. Arellano and E. Calderón, "Análisis de herramientas opensource de administración y monitoreo basado en snmp, aplicado a la red de datos del ilustre municipio de ambato." 2012. [Online]. Available: <http://dspace.espoch.edu.ec/handle/123456789/1496>
- [4] J. I. F. Bonilla, "Herramienta opensource de administración y monitoreo basado en snmp para el mejoramiento del funcionamiento de la red en speedy com cia ltda." 2013. [Online]. Available: <http://repo.uta.edu.ec/bitstream/handle/123456789/4920/t802ec.pdf?sequence=1>
- [5] A. Armijos and L. Villamar, "Sistema de gestión en seguridad informática como soporte a la toma de decisiones en respuesta a incidentes, basados en monitoreo de redes," vol. I, no. 1, p. 6, 2011. [Online]. Available: <https://www.dspace.espol.edu.ec/bitstream/123456789/14922/1/Sistema%20de%20Gestion%20en%20seguridad%20informatica%20como%20soporte%20a%20la%20toma%20de%20decisiones.pdf>
- [6] L. A. D. P. Guevara, "Herramienta integrada de monitoreo de redes para soporte de estudios de disponibilidad," 2007. [Online]. Available: http://cybertesis.urp.edu.pe/bitstream/urp/43/1/delpozo_la.pdf
- [7] R. B. Caryuly, "Protocolo snmp (protocolo sencillo de administracion de redes)," vol. III, no. 1, 2004. [Online]. Available: <http://publicaciones.urbe.edu/index.php/telematique/article/viewArticle/782/1886>
- [8] D. C. Verma, *Policy-Based Networking: Architecture and Algorithms*. New

- Riders Publishing, 2000. [Online]. Available: <http://dl.acm.org/citation.cfm?id=557650>
- [9] M. Wahl, T. Howes, and S. Kille, “Lightweight directory access protocol (v3),” 1997. [Online]. Available: <https://www.ietf.org/rfc/rfc2251.txt>
- [10] D. Durham, J. Boyle, R. Cohen, S. Herzog, R. Rajan, and A. Sastry, “The cops (common open policy service) protocol,” 2000. [Online]. Available: <http://tools.ietf.org/html/rfc2748>
- [11] C. A. V. Altamirano, “Monitoreo de recursos de red,” vol. I, no. 1, p. 11, Junio 2005. [Online]. Available: <https://julioestrepo.files.wordpress.com/2011/04/monitoreo.pdf>
- [12] . G. Valarezo and J. Simisterra, “Implementación de un sistema de gestión y administración de redes basados en el protocolo simple de monitoreo de redes snmp en la red espol-fiec,” 2011. [Online]. Available: <http://www.dspace.espol.edu.ec/handle/123456789/16202>
- [13] D. Naranjo and P. Ortega, “Desarrollo de una aplicación gráfica basado en el sistema operativo linux para el monitoreo y administración del tráfico de datos de redes lan,” 2006. [Online]. Available: <http://bibdigital.epn.edu.ec/bitstream/15000/2353/1/CD-0006.pdf>
- [14] C. A. Herrera Muñoz, “La técnica de objetos aplicada a la gestión de redes de telecomunicaciones,” 1999. [Online]. Available: <http://bibdigital.epn.edu.ec/bitstream/15000/5349/1/T1537.pdf>
- [15] T. Urban, *Cacti 0.8 beginner’s guide*. Packt Publishing Ltd, 2011. [Online]. Available: <https://www.packtpub.com/sites/default/files/39200S-Chapter-2-Using-Graphs-to-Monitor-Networks-and-Devices.pdf>
- [16] L. Deri and S. Suin, *Ntop: Beyond Ping and Traceroute*. Lungarno Pacinotti 43, Pisa, Italy.: Centro Sera, University of Pisa,. [Online]. Available: http://link.springer.com/chapter/10.1007/3-540-48100-1_21
- [17] L. Deri, R. Carbone, and S. Suin, “Monitoring networks using ntop,” in *Integrated Network Management Proceedings, 2001 IEEE/IFIP International Symposium on*. IEEE, 2001, pp. 199–212. [Online]. Available: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=918032

- [18] R. Olups, *Zabbix 1.8 network monitoring*. PACKT Publishing Ltd, 2010. [Online]. Available: <https://www.ebooks-it.net/ebook/zabbix-1-8-network-monitoring>
- [19] M. Badger, *Zenoss Core 3. x Network and System Monitoring*. Packt Publishing Ltd, 2011. [Online]. Available: <https://www.ebooks-it.net/ebook/zenoss-core-network-and-system-monitoring>

Anexos y Apéndices

Anexo A

A.1. Entrevista

Entrevista Aplicada al Ing. Ricardo Domínguez encargado de la Administración de la Red del Gobierno Provincial de Tungurahua.

Preguntas

- 1.- ¿Cuál considera Usted que es el estado actual de la Red de Datos & VoIP del Gobierno Provincial de Tungurahua?
- 2.- ¿Cuál considera Usted que es la principal falencia de la Red actual del Gobierno Provincial de Tungurahua?
- 3.- ¿Bajo qué sistema operativo se monitorea en la actualidad a la Red de Datos & VoIP del Gobierno Provincial de Tungurahua?
- 4.- ¿De qué equipos disponen en la actualidad el Gobierno Provincial de Tungurahua para administrar su Red de Datos & VoIP?
- 5.- ¿Qué características considera necesarias incorporar a la actual Red de Datos & VoIP del Gobierno Provincial de Tungurahua?

Gracias por su amable atención.

Respuestas

Pregunta N° 1

En relación a la pregunta N° 1 el entrevistado manifiesta:

La Red de Datos del Gobierno Provincial de Tungurahua no cuenta con cableado estructurado sin embargo la Red de VoIP. si cuenta con un cableado estructurado lo que implica la utilización de AP's cual evidentemente deteriora la calidad de

comunicación entre cada uno de los departamentos.

Pregunta N° 2

En relación a la pregunta N° 2 el entrevistado manifiesta:

La principal falencia de la Red del Gobierno Provincial de Tungurahua es que actualmente no es posible realizar un eficiente Control y un adecuado Monitoreo de la Red de Datos & VoIP.

Pregunta N° 3

En relación a la pregunta N° 3 el entrevistado manifiesta:

La aplicación empleada actualmente para el monitorear la Red de Datos & VoIP del Gobierno Provincial de Tungurahua, está montada sobre el sistema operativo Debian, misma que tiene un entorno gráfico permitiendo la identificación visual de todos los equipos que componen la Red.

Pregunta N° 4

En relación a la pregunta N° 4 el entrevistado manifiesta:

El Gobierno Provincial de Tungurahua para administrar su Red de Datos & VoIP disponen en la actualidad de una gran cantidad de equipos entre los que se destacan: servidores, switch, antenas, router, teléfonos IP.

Pregunta N° 5

En relación a la pregunta N° 5 el entrevistado manifiesta:

La Red de Datos & VoIP del Gobierno Provincial de Tungurahua requiere de un análisis detallado y debidamente sustentado que permita establecer una herramienta idónea la cual garantice un adecuado Monitoreo de la Red de Datos & VoIP.

A.2. Entrevista

Entrevista Aplicada al Ing. Francisco López encargado del Departamento de Sistemas del Gobierno Provincial de Tungurahua.

Preguntas

1.- ¿Cuál considera Usted que son los puntos críticos del Área de TI del Gobierno Provincial de Tungurahua?

Gracias por su amable atención.

Respuesta

Pregunta N° 1

En relación a la pregunta N° 1 el entrevistado manifiesta:

Los puntos críticos en el Área de TI del Gobierno Provincial de Tungurahua e derivan en 3 ejes los cuales son:

- Seguridad.
- Interconexión de Sistemas.
- Equipos Informáticos.

Entrevista Aplicada al Ing. Francisco López encargado del Departamento de Sistemas del Gobierno Provincial de Tungurahua.

Preguntas

1.- ¿Cuál considera Usted que son los puntos críticos de la Red de Datos & VoIP del Gobierno Provincial de Tungurahua?

Gracias por su amable atención.

Respuesta

Pregunta N° 1

En relación a la pregunta N° 1 el entrevistado manifiesta:

- La puntos críticos de la Red de Datos & VoIP del Red del Gobierno Provincial de Tungurahua, los cuales son:

- Servidor de Dominio.
- Servidor de Correo.
- Servidor de Base de Datos.
- Firewall.
- Consola Blade Center.
- Routers de cada Edificio.

- Access Point – AP's.
- Central Telefónica VoIP Alcatel .