ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA PARA LA GESTIÓN DE LAS REDES PYMES CON TECNOLOGÍAS DE BAJO COSTO"

INFORME DE PROYECTO INTEGRADOR

Previa a la obtención del Título de:

LICENCIADA EN REDES Y SISTEMAS OPERATIVOS

MISHELL STEFANIE ABAD BROWN

GIANNELLA SOFIA MESTANZA OSORIO

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTO

“Gracias totales”.

Gustavo Cerati.

Mishell Abad Brown.

Agradezco a Dios por todas las bendiciones y la fuerza que me ha dado para llegar a donde estoy.

A mi madre que sacrificó todo para darnos lo que necesitamos, que nos ha apoyado en todo y ha sabido corregirnos cuando ha sido necesario.

A mi abuelita que desde el cielo me protege en cada paso que doy y que sé que está muy orgullosa de la persona en la que me he convertido.

A mi padre y a mis tíos que han sido incondicionales y han estado para mí cuando más los he necesitado.

A mis amigas que con gran esfuerzo estamos llegando al final de nuestro objetivo y nos hemos mantenido unidas.

A los profesores de LICRED que con sus palabras y sus consejos nos han hecho grandes profesionales y nos han enseñado valiosas lecciones.

A la Academia CISCO por el apoyo brindado en nuestro proyecto y por haber confiado en mí.

Y gracias a todos los que brindaron su ayuda en este proyecto.

Giannella Mestanza Osorio.

DEDICATORIA

A Dios, mi mamá, mi familia, amigos y a todos aquellos que estuvieron conmigo durante todo este tiempo.

Mishell Abad Brown.

Dedico este trabajo a Dios, por permitirme llegar a este momento. A mi Madre por todo su apoyo y su cariño incluso cuando hemos tenido nuestras diferencias. A mi sobrinito/a que está en camino. A mis tíos y abuelos que han sido como unos segundos padres. A mis profesores por toda la sabiduría que me han transmitido para mi carrera profesional

Giannella Mestanza Osorio.

TRIBUNAL DE EVALUACIÓN

Ing. Ronald Criollo	**Ing. Robert Andrade**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, me (nos) corresponde exclusivamente; y doy (damos) mi (nuestro) consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

_____ _____

Mishell Stefanie Abad Brown Giannella Sofia Mestanza Osorio

RESUMEN

Este proyecto es acerca del diseño e implementación de un sistema de gestión de redes que se basará en tecnología de bajo costo, para que las PYMES en Ecuador puedan implementar.

En la realización de este proyecto diseñamos una solución utilizando una consola que trabaje con software libre; esta se encargará de supervisar o vigilar el estado y el comportamiento de la red para mitigar los problemas más comunes que tienen las empresas, como lentitud o pérdida de conexión; lo que causa molestias al usuario pérdidas a nivel del negocio.

ÍNDICE GENERAL

CAPÍTULO 1

1. ANTECEDENTES Y JUSTIFICACIÓN

1.1 Antecedentes

Uno de los principales problemas con los que nos encontramos es que la mayoría de las empresas no consideran la importancia de implementar algún sistema de gestión de red, en especial las pequeñas y medianas empresas (PYMES), ya que piensan que al contar con un diseño de infraestructura sencillo no es necesario monitorear la red, por lo que descartan el uso de estas herramientas.

Los principales problemas que se presentan en las redes de las pequeñas y medianas empresas son:

- Pérdida de conexión.
- Lentitud al momento de navegar.
- No se puede acceder a los servicios y programas de la empresa.
- No se asigna o distribuye correctamente el ancho de banda.
- No se lleva un control sobre el estado de los equipos de red.

Al no contar con un sistema pueden aparecer paulatinamente problemas de retardo y conectividad; o podrían aparecer de manera eventual sin previo aviso en respuesta a cargas enormes generadas dentro de la red debido a alguna transferencia de datos entre usuarios o por fallas a nivel de hardware, ralentizando la ejecución de procesos y la comunicación en sí.

Son incontables los escenarios en los que es transcendental contar con herramientas que nos permitan estar al tanto del desempeño de la red. Desde el punto de vista de los administradores, el mantenimiento y monitoreo es un práctica constante que se debe considerar para evitar pérdidas de conectividad y un mal uso de los recursos.

Por lo que las herramientas de gestión podrían avisarle al administrador cuando es necesario realizar algún cambio en la infraestructura o en la configuración,

para de esta manera aumentar el rendimiento, mejorando el desempeño y principalmente la escalabilidad a futuro de la red.

1.2. ANÁLISIS DEL PROBLEMA

1.2.1 Análisis de la red

Las empresas PYMES en el Ecuador al contar con clientes externos requieren que sus sistemas se encuentren disponibles y operativos la mayor parte del tiempo, ya que al no estarlo generan desconfianza en el cliente y debido a que muchas veces los pedidos deben realizarse con entrega inmediata algunos se ven obligados a buscar otras empresas, generando así una gran pérdida monetaria para la compañía.

1.2.2 Diagrama de red

Al ser una PYME de bajo costo, su estructura de red básicamente se conforma de un enrutador principal, un conmutador de capa 3, tres conmutadores conectados en cascada, un enrutador inalámbrico y un servidor con el que el administrador se encarga de gestionar y administrar las cuentas de los trabajadores de la compañía. La empresa puede contar con otros servidores, pero en nuestro escenario de prueba utiliza almacenamiento web para las cuentas de correo electrónico. Como ejemplo puede observar la figura 1.1.

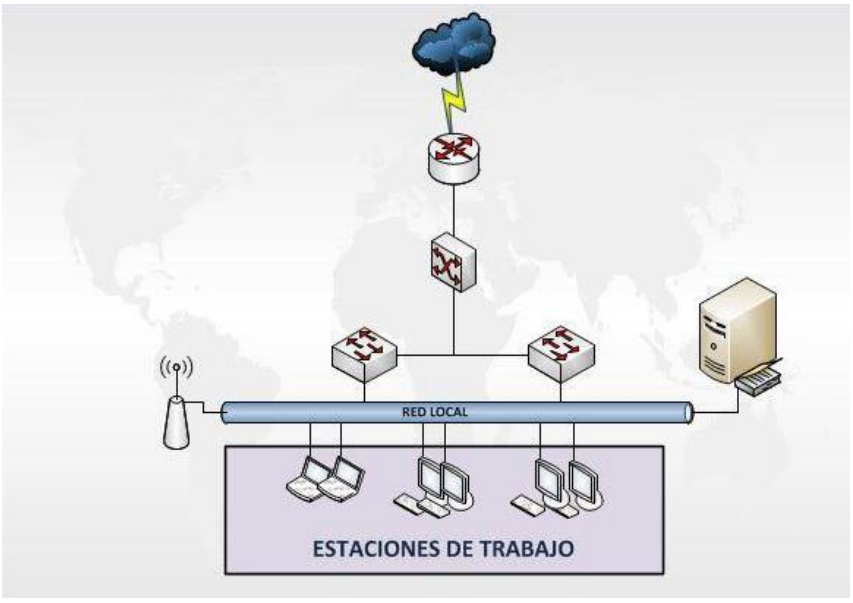


Fig. 1.1. Diagrama de red de una PYME

1.2.3 Servicios/protocolos manejados por la empresa

La empresa cuenta con solo un servidor el cual maneja el servicio de directorio de Windows, mejor conocido como Active directory, pero además la empresa cuenta con varios protocolos de red manejados por sus diferentes servicios, lo cual logra que la red se encuentre operativa y que son parte de lo que la consola de gestión se encargará de monitorear para poder recoger información acerca del funcionamiento de la red y así poder asegurar una mayor disponibilidad.

Algunos de los protocolos manejados por la empresa son:

- **DNS** para resolver nombres de dominio a direcciones IP y localizar servidores de correo de cada dominio.
- **DHCP** para asignar direcciones dinámicas a los usuarios que se conectan con las laptops al enrutador inalámbrico.
- **SNMP** estándar para la gestión de redes, la empresa maneja la versión 3.
- **SMTP/POP3** para el envío y recepción del correo electrónico.
- **UDP/TCP** para la comunicación de la red de la empresa.

- **Kerberos/LDAP** utilizados por el servidor Active directory.
- **ICMP** para verificar que un dispositivo este alcanzable.
- **SSH** para la conexión remota y segura a otro equipo de red.

1.2.4 Desempeño actual de la red

La empresa tiene 3 años de funcionamiento y en ese tiempo ha mantenido un mantenimiento de hardware anual para evitar el incorrecto funcionamiento de los mismos. Sin embargo en el último semestre se ha observado, por parte de los usuarios, que existe lentitud y pérdida en la conexión durante las horas críticas de trabajo, generando así molestias al momento de la comercialización ya que no pueden acceder a sus sistemas.

1.2.5 Problemas existentes en la red

Durante los años que llevan operando se observa que no tienen un control mensual o trimestral sobre el rendimiento y desempeño de los equipos de red, así como un registro de los servicios que están consumiendo más ancho de banda y cuáles son las horas donde se genera mayor tráfico, para así poder optimizar su infraestructura. El administrador de red recibe quejas de los usuarios sobre la lentitud de la conexión o incluso que no pueden acceder a ciertos sistemas de la compañía, el tiempo que le toma al administrador encontrar y solucionar el posible problema genera pérdidas monetarias, un sistema de gestión de redes ayudaría a mitigar estos problemas de manera eficaz.

1.3 Gestión de redes

Podemos definir a la gestión de redes como la actividad de controlar y supervisar los diferentes recursos de red que existen en una empresa, cuyo objetivo principal es el de mantener y garantizar la operatividad continua con un mínimo costo.

Integra distintos dispositivos en un solo sistema de gestión fácil de usar y de aprender ya que cuenta con una única interfaz de usuario.

El administrador podrá estar al tanto de cuando se sobrepase algún límite establecido para los recursos, por medio de alarmas que se podrán visualizar en la página web del aplicativo y también se enviarán notificaciones al correo electrónico o al celular previamente configurado.

Permite que desde el centro del gestor se acceda a cualquier punto de la red y así poder administrar y/o actuar en caso de que se produzca algún fallo en el sistema sin necesidad de ir físicamente al punto y así minimizar el porcentaje de pérdidas para la empresa en caso de que exista alguna perdida de conexión en la red.

Planificar, organizar, controlar, mantener, evaluar e integrar son unas de las ventajas del uso de un sistema de gestión. [1]

1.3.1 Importancia de la gestión de redes

Como mencionamos anteriormente, la gestión de red tiene un papel importante para el correcto desempeño de sus sistemas, algunas de las razones son:

- La cantidad de información que maneja la red es cada vez mayor.
- Con el avance tecnológico los recursos requieren ser gestionados para trabajar de una forma más eficiente.
- Los sistemas de gestión son soportados por cualquier tipo de red.
- Incrementa la disponibilidad de mis sistemas.
- Disminuye los costos.
- Aumenta la calidad del servicio que pueda brindar su negocio o empresa.
- La operación se vuelve automatizada.

1.3.2 Elementos administrables de una red

Se puede definir como elementos administrables de una red a cualquier equipo o servicio existente en la misma tales como:

Dispositivos de red:

- Servidor
- Enrutador
- Enrutador inalámbrico
- Computador
- Laptop
- Impresora
- Conmutador
- Hub

Servicios:

- TCP
- ICMP
- HTTP
- DNS
- DHCP
- keberos
- SMTP
- FTP
- POP3
- IMAP
- Uptime
- UDP

Con los sistemas de gestión podemos estar al tanto del estado de forma automatizada de cada uno de los recursos previamente mencionados y mantener un mejor control en la red sobre los servicios que consumen

mayor ancho de banda. También podremos saber si algún equipo se encuentra saturado o si es necesario tomar acciones, ya sea preventivas o correctivas para así asegurar un correcto funcionamiento e incluso mejorar el rendimiento actual de la estructura de red.

1.3.3 Métodos de la gestión de red

En toda red es necesario que la información sobre cada elemento sea actualizada constantemente y las medidas que usemos para identificar problemas y/o fallos nos ayudan a crear un historial o documentar el comportamiento de la red.

Los métodos más significativos para la gestión de red son:

- **Proactiva:** en base a un historial que contiene patrones sobre la conducta y crecimiento se planea realizar mejoras en la red para mantener o mejor su desempeño y así mitigar daños o fallos.
  Se debe tener en cuenta todos los detalles ya sean de balanceo de carga, configuraciones, segmentos clientes y servidores.

- **Reactiva:** Identificar y solucionar fallos o inconvenientes que se presenten en la red, minimizando tiempos de inoperatividad.

Es necesario llevar un balance entre estos métodos, ya que son necesarios para que la red crezca de manera óptima y se mantenga funcional, esto quiere decir que mientras mi red vaya creciendo no genere molestias a los usuarios por tiempos de pérdida o lentitud en la conexión.

1.3.4 Tipos de problemas

Podemos clasificar los problemas que se presentan en nuestra red en dos tipos:

1. **Aislados:** básicamente es una falla, hace que la red deje de operar como lo hace normalmente, por lo general se asocia con la forma reactiva de gestionar la red.

2. **Recurrentes:** fallos que se presentan regularmente en la red y cambian su conducta, se asocia con la forma proactiva de gestionar la red.

La rapidez con la que se resuelva el problema que se presente en la red varía con el uso de la herramienta de monitorio.

1.4 SOFTWARE LIBRE

Se considera "libre" al software que permite al usuario realizar cambios o mejoras a su configuración y ajustarlo a su necesidad.

En otras palabras es un software de dominio público y no hacen uso de licencias.

1.4.1 Importancia de usar software libre

En la actualidad el uso de software libre es importante para todo tipo de empresa desde una multinacional hasta las microempresa ya que brinda:

- **Autonomía en tecnología:** se pueden personalizar los programas para cubrir las diferentes necesidades del usuario.
- **Seguridad:** se puede utilizar múltiples herramientas para conocer lo que está pasando en la red.
- **Estandarización:** ya que es producido con especificaciones tecnológicos libres y públicos conocidos como "estándares abiertos".
- **Integración:** Integra sistemas y ayuda al intercambio de datos.
- **Independencia en proveedores:** cuando usamos software propietario se crea una dependencia con el proveedor, se depende de el para realizar actualizaciones en el sistema.
- **Economía:** Para las empresas que recién empiezan o para países que no cuentan con muchos recursos el uso e implementación de este tipo de software es de suma importancia.

1.4.2 Ventajas de usar software libre

Entre las ventajas del uso de software libre tenemos:

- Bajo costo
- Estabilidad
- Cuenta con apoyo y soporte por parte de la comunidad
- Una gran variedad de herramientas.
- Existen actualizaciones continuas
- Eficiente
- Diverso
- Beneficio social y en tecnología al país.
- Facilidad de corrección de errores.
- Fácil de traducir a múltiples idiomas.

1.4.3 Desventajas de usar software libre

Entre las desventajas más significativas tenemos:

- No tiene garantía
- No tiene mucha publicidad
- Algunas de los programas no son compatibles con la plataforma.
- Ciertos programas son difíciles de instalar.
- Interfaz gráfica poco amigable para el usuario.
- Menor compatibilidad a nivel de hardware
- El usuario debe tener conocimiento sobre la configuración del software.

1.5 ANÁLISIS DE LAS HERRAMIENTAS DE GESTION

A continuación describiremos brevemente algunas de las herramientas más populares en el mercado para poder seleccionar la mejor opción a implementar en este proyecto.

1.5.1 SNMP

Protocolo simple de administración de red, los administradores de red pueden administrar equipos de red y diagnosticar cualquier problema que se presente en la red. [2]

Cuenta con un supervisor que es el que permite al administrador realizar peticiones de control, en cambio, los agentes se encuentran por cada interfaz y a través de ellos se recopila la información de los objetos.

Todos los elementos relacionados con el comportamiento de los equipos se almacenan en una base llamada MIB (base de datos de información de administración), la comunicación entre en supervisor y los agentes permiten recolectar los objetos requeridos en la MIB.

SNMP es independiente del protocolo, se puede implementar tanto en UDP o TCP aunque en la mayoría sea UDP, los puertos que usan son 161 para transmisión normales y 162 para mensajes tipo trap.

Los mensajes son:

- **GetRequest:** recoge por medio de listas valores de los objetos.
- **GetNextRequest**: recorre una tabla de objetos cuando ya se haya usado.
- **GetRequest.** Solicita a un agente cambiar valores.
- **GetResponse:** el agente usa este mensaje para responder alguna petición anterior.
- **GetBulkRequest:** es parte de SNMPV2 y SMNPV3, es mucho más rápido ya que en un solo mensaje puede solicitar la totalidad de la tabla.
- **InformRequest:** envía información sobre objetos administrados usando TCP, y se enviará hasta que reciba un acuse de recibo.
- **Trap**: reporta cambios y condiciones, Su formato PDU es diferente

La arquitectura se basa en los siguientes elementos:

- **Equipos administrados:** dispositivos en la red que contienen los objetos administrados ya sea a nivel de hardware, configuración o datos estadísticos.
- **Agentes:** hace referencia al aplicativo que permite la administración, es responsable de la transmisión de datos en formato SNMP.
    - **Obtener (get):** recupera datos del agente.
    - **Colocar (put):** establece valores de los objetos en el agente.
    - **Captura (trap):** notifica sucesos importantes al agente.
- **Sistema de administración de red (NMS):** terminal por el cual se llevan a cabo las tareas para la administración y supervisión.

Versiones de SNMP

Con el paso del tiempo salieron nuevas versionas para optimizar el uso de SNMP.

SNMPV1:

Diseñado en los 80s, fue diseñado como medida temporal hasta que se desarrollara otros protocolos de gestión más completos por lo cual no iba a poder administrar la gran cantidad de redes que fueron apareciendo, se basa en UDP.

Permite el intercambio de gestión de información entre los dispositivos de redes,

La seguridad se basa en algo llamado comunidades que está definida por una contraseña y un ACL.

SNMPV2:

Definido en los 90s, se integraron mecanismos que permitan la seguridad, mayor detalle en la definición de variables, estructuras de tablas, básicamente fue un parche para prevenir la congestión de red por medio de los (GetBulk e informs) y la asistencia remota con (RMON).

Es compatible con SNMPV1.

SNMPV3:

Nacido en 1998, se añadieron mecanismos de seguridad que no se implementaron en sus antecesores como:

- **Integridad del mensaje:** verifica que la información no haya sido dañada.
- **Autenticación:** provenga de una fuente confiable.
- **Cifrado:** asegura el contenido del paquete para prevenir violaciones.

Añade con mensajes SNMP tanto v1 como v2 en una cabecera adicional. [2]

1.5.2 Herramientas de Monitorización

Estas herramientas se ejecutan en segundo planos como demonios (programas que se ejecutan en segundo plano) o servicios, que recolectan eventos y que pueden iniciar sus propias comprobaciones, por medio de herramientas que diagnostiquen lo que está sucediendo en la red y que actúen de manera programada.

A continuación explicaremos un poco de las más populares en el mercado:

1.5.2.1 Nagios

Software libre de código abierto, que permite la supervisión de dispositivos y servicios informáticos más popular del momento.

Diseñado especialmente para que los administradores de red puedan mantenerse al tanto de lo que ocurre en su red y conocer cuando existe algún fallo mucho antes de que el usuario final lo note.

Nos permite tomar decisiones importantes de infraestructura como:

- Realizar un registro de los reportes y tendencias.
- Analizar la red y el tráfico que se maneje.
- Supervisar la red dependiendo de los reportes.
- Justificar la importancia de actualizar la red.

Por medio de alarmas le avisa al administrador de redes cuando existe algún problema o fallo en la red basándose en los parámetros previamente establecidos.

Trabaja bajo un esquema cliente-servidor por medio de una ejecución de polling periódico de supervisión de recursos usando agentes y servicios sin usar agente sobre el sistema del cliente.

Si existiera algún error, envía una notificación ya sea vía email, SMS entre otros a los administradores informando lo ocurrido.

Fácilmente de integrar con programas de terceros para un mejor servicio.

Algunas de las características que vigila Nagios son:

- **Servicios:** SMTP, POP, POP3, HTTP, HTTPS, SNMP, ICMP, FTP, entre otros.
- **Hardware:** Procesador, memoria RAM, espacio del disco duro, estado de puertos, total de procesos.
- Control de servicios pasivos generados por las aplicaciones externas.
- Permite desarrollar de manera fácil al administrador sus propios agentes.
- Identificar de manera rápida caídas de servicios.
- Configurar tiempos de notificación.
- Interfaz web que permite la gestión del estado de la red.

Ventajas:

- Mejorar la productividad.

- Mitigar problemas.
- Registros y alarmas de incidentes.
- Relaciona e integra sectores adjuntos.

Permite definir las políticas de notificación basándose en combinaciones: Contactos y listas, dispositivos y grupos, servicios y grupos y horarios definidos.

En la interfaz gráfica tenemos los siguientes estados**:**

- **Warning**: cuando se está por llegar al límite o debe de ser revisado.
- **Critical**: es prioridad y de urgencia ser revisado y atendido.
- **Unknown**: cuando ocurre algún evento que no es identificado.

Nagios, cubre todas las necesidades de manera sencilla, se adapta a los cambios, se puede integrar con scripts y software externo, aparte es un software libre por lo que no se cancela ningún valor por concepto de licencia. [3]

1.5.2.2 Zabbix

Una herramienta de monitoreo que permite supervisar servidores, servicios y dispositivos de red, lanzado bajo los términos de GNU versión 2, es software libre.

Zabbix ofrece vigilancia para las redes LAN y WAN, se configura en un servidor y se encarga de recopilar información. Proporciona una interfaz web, en la cual se puede observar de manera gráfica todos los datos que recolecta la herramienta. [4]

1.5.3 Herramientas de Diagnóstico

Las herramientas de diagnóstico son herramientas activas con las que se puede probar conectividad y comprobar que un equipo sea alcanzable y esté disponible. [1]

Software que permite supervisar y en ciertos casos poder controlar la correcta funcionalidad del estado físico de los equipos de red.

Nos mantiene al tanto del estado de:

- Procesador.
- Memoria RAM.
- Disco duro.
- Tarjeta de red.
- Temperatura.
- Rendimiento.
- Transferencia de datos.

1.5.4 Herramientas de Desempeño

Nos dice como la red maneja el flujo de datos, el congestionamiento, son causados por sobrecargas que son transitorios en los recursos. Mientras llegue más tráfico a un enrutador el desempeño de la red decae. [1]

Son un prerrequisito para la gestión de una red, los tipos de herramientas de desempeño son:

- **Servicio:**
  - Disponibilidad: a mayor disponibilidad mayor costo (redundancia).
  - Tiempos de respuesta: procesamiento de los equipos, números de procesos en ejecución. (tiempos tanto del usuario como del sistema).
  - Precisión: análisis de las tendencias a fallos para asegurar la integridad de los datos.
- **Eficiencia:**
  - Throughput: número de sesiones, tasa óptima de transferencia.
  - Uso: evitar cuellos de botella y congestión.

1.5.4.1 Netflow

Protocolo diseñado por Cisco Systems para poder recoger datos sobre el tráfico IP, el uso de un colector pasivo no permite ver todos los flujos que existan en la red, solo la vera desde el punto de red donde se encuentra, sin embargo alivia la carga de generar y exportar los flujos al dispositivo principal. [5]

1.5.4.2 MRTG

Multi Router Traffic Grapher, Herramienta que permite supervisar la carga de tráfico de interfaces de red que genera informes en formato HTML y gráficas que proveen una representación visual de la evolución del flujo en un periodo de tiempo.

MRTG trabaja junto con SNMP que es el protocolo que proporciona los datos que han pasado por las interfaces de entrada y de salida que es tratada de manera adecuada para realizar los informes, usualmente se hace uso de scripts que supervisan la maquina local.

Su funcionamiento se basa en ejecución de un demonio o invocado desde las tareas que se programan en el cron, de manera predeterminada recopila datos de los equipos y ejecuta los scripts cada cinco minutos.

Al principio MRTG consultaba, procesaba y generaba los informes y las gráficas sin embargo en las últimas versiones, la información se almacena y es gestionada por RRDtool la cual genera los reportes.

Escrita en Perl, trabaja bien tanto en GNU/Linux como en Windows, así como las herramientas antes mencionadas MRTG es de código abierto y libre quiere decir que es licenciado mediante GPL.

Beneficios de MRTG:

- Uso adecuado de ancho de banda

- Proyección de crecimiento
- Identificar los programas que corren en la red
- Identificar que procesos se pueden ejecutar en horarios fuera de oficina

En si es una herramienta para poder representar de manera gráfica los datos que recopila SNMP.

Contiene paquetes que permite analizar los enlaces, extraer las características para luego modificarlos para ajustarse a las necesidades.

Permite recolectar datos del tráfico a nivel:

- Diario
- Semanal
- Mensual
- Anual

Cuenta con una interfaz web principal que contiene los gráficos de los detalles de las interfaces, permite tener una visión general de los que está pasando en la red. [7]

CAPÍTULO 2

2. DISEÑO DE LA POSIBLE SOLUCIÓN

2.1 CONSOLA DE MONITOREO.

La consola permite que los usuarios observen:

- **Sistemas y servicios de red:**
  Que se encuentren disponibles para que el usuario siempre pueda hacer uso de ellos.
- **Recursos de red:**
  Que los recursos de red se encuentren operativos y que permitan expandir la red.
- **Desempeño:**
  Conocimiento de los tiempos y tasas máximas de transmisión.
- **Cambios y configuraciones:**
  Se lleva un registro de cambios que se realizan en la red.

Usted podrá conocer el rendimiento y desempeño en tiempo real de la infraestructura de red de su empresa por medio de una consola la cual cuenta con un sistema de gestión de redes.

Con esta información se puede llevar un registro para fines estadísticos que nos permita conocer las tendencias a fallos que se presenten y sus soluciones.

Podrá mantener un mejor control y administración de sus recursos y servicios, garantizando la disponibilidad, escalabilidad, fiabilidad y desempeño.

2.1.1 Características del sistema operativo de la consola

Ya que nuestra solución debe ser de bajo costo para evitar una mayor inversión por parte de las PYMES, el sistema operativo a usar debe ser código abierto para evitar pagar costos de licenciamiento, por lo que hemos optado por usar una distribución GNU/Linux.

Además por temas de compatibilidad con el software de monitoreo en el que se basa nuestro diseño de solución propuesto se debe instalar el software de monitoreo en debían o una distribución basada en debían.

2.1.2 Software de monitoreo de la consola.

Como herramienta de monitorización hemos optado por Nagios, en lugar de zabbix, ambos son código libre pero consideramos que Nagios es mejor, ya que proporciona gran versatilidad para consultar múltiples aspectos de un sistema de red, el administrador recibe alertas cuando los parámetros requeridos sobrepasan el límite establecido ya sea por correo electrónico o mensajes SMS y aunque no genera gráficos como Zabbix, se le pueden agregar pluggins como es el caso de NagiosGraph. En la figura 2.1 podemos observar el comando para la descarga.

Fig. 2.1 Instalación Nagios

NagiosGraph nos será de gran ayuda, ya que nos permite graficar diagramas periódicos sobre los parámetros configurados en la página de Nagios y además es mucho más amigable que los gráficos que ya vienen en otros softwares de gestión. En la figura 2.2 se puede observar como descargar este complemento.

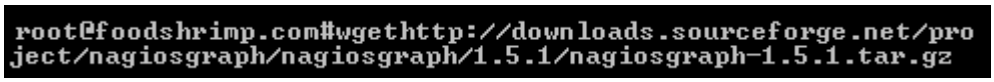


Fig. 2.2 Instalación NagiosGraph

Como herramienta de gestión de redes, SNMP cumple mejor con los requerimientos que se presentan en las PYMES; ya que, a diferencia de NETFLOW, me muestra información en tiempo real del flujo viajando a través de su red e información del CPU y memoria utilizada, permitiendo

así al administrador poder determinar cuándo es necesario comprar más memoria para los equipos o cambiar de proveedor de internet. Además no consume mucho espacio en el disco, por lo que el sistema no se volverá lento por la instalación de este software. En la figura 2.3 se observa como instalar el paquete SNMP.

Fig. 2.3 Instalación SNMP

Además para poder realizar un correcto monitoreo del servidor Active Directory que maneja la empresa, vamos a instalar NRPE ya que este complemento nos permite poder recolectar los datos a monitorear del equipo Windows de forma remota.

También instalamos MRTG para poder tener una mejor visión del tráfico que circula por nuestras interfaces de red, y mantener un registro de este para poder graficar su evolución. En la figura 2.4 se observa como instalar este paquete.

Fig. 2.4 Instalación MRTG

2.1.3 Características de hardware de la consola

El hardware donde estará montado nuestro sistema de gestión puede ser una computadora de escritorio, una laptop o un ordenador de placa reducida. No es necesario conectarle monitor, teclado o mouse ya que una vez configurada se puede acceder por medio de la página web, para ver el tráfico que se está monitorizando, o por SSH para realizar cambios en configuración.

2.2 UBICACIÓN DE LA CONSOLA

La consola irá conectada en el dispositivo núcleo principal de la red para un mejor monitoreo o supervisión de la misma.

Conectada al dispositivo principal tendríamos una visión más general de lo que pasa en la red y evitamos la supervisión de tráfico innecesario o equipos en redes vecinas. Como ejemplo puede observar la figura 2.5.

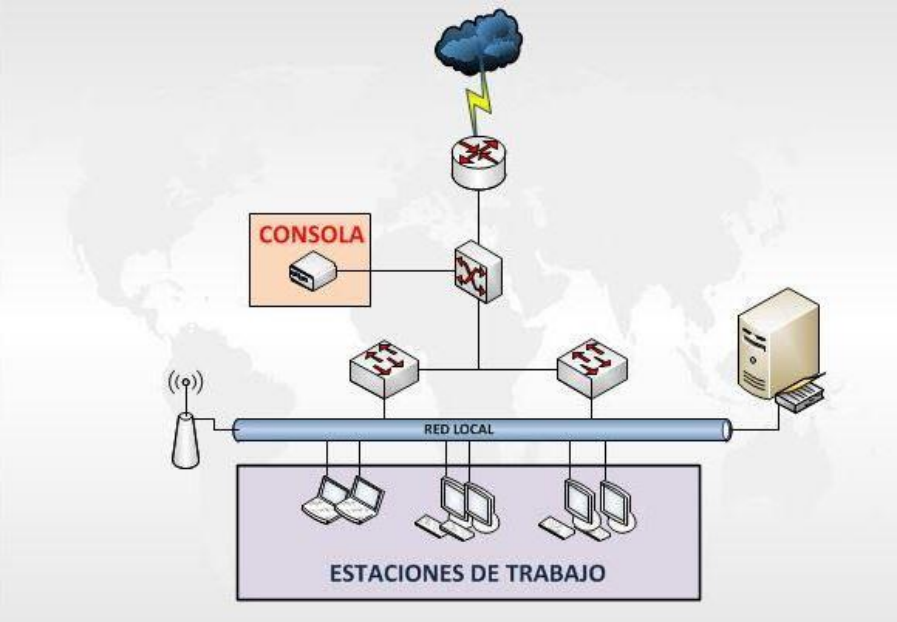


Fig. 2.5. Diagrama de red con la consola

2.3 ANÁLISIS TÉCNICO Y PLAN DE TRABAJO

A continuación presentaremos el presupuesto que necesitaría invertir una PYME para poder implementar nuestro modelo de sistema de gestión y así poder cubrir las necesidades y disminuir en un 99.9% los problemas que la empresa presentaba.

2.3.1 Presupuesto

Debido a que nuestra solución se basa en ofrecer opciones a nivel de software libre nuestra proforma sería la siguiente:

Cantidad	Detalle	Total
Servicios profesionales		
	Implementación	$1,000.00
	Capacitación	$1,000.00
	Total	
	Los precios incluyen IVA	**$2,000.00**

Tabla 1: Presupuesto

Se puede realizar cambios sobre los servicios que se están controlando totalmente gratis durante el primer mes desde la instalación, luego tendrá un valor adicional dependiendo de la complejidad del cambio a realizar.

2.3.2 Plan de trabajo

Basándonos en los requerimientos de las PYMES ecuatorianas elaboramos un plan de trabajo que se muestra a continuación:

	Nombre de tarea	Duración	Comienzo	Fin	Nombres de los recursos
1	**Configuración de la consola**	**6 días**	**mar 8/25/15**	**mar 9/1/15**	**Mishell Abad**
2	Instalación del sistema Operativo	1 día	mar 8/25/15	mar 8/25/15	
3	Instalación de software de gestión	1 día	mié 8/26/15	mié 8/26/15	
4	Configuración de los parametros	2 días	jue 8/27/15	vie 8/28/15	
5	Configuración de correo y pluggings	2 días	lun 8/31/15	mar 9/1/15	
6	**Implementación de solución propuesta**	**5 días**	**mié 9/2/15**	**mar 9/8/15**	**Giannella Mestanza**
7	Pruebas generales	2 días	mié 9/2/15	jue 9/3/15	
8	Cambios a realizarse (opcional)	2 días	vie 9/4/15	lun 9/7/15	
9	Revisiones finales	1 día	mar 9/8/15	mar 9/8/15	
10	**Entrega del proyecto**	**1 día**	**mié 9/9/15**	**mié 9/9/15**	**Mishell Abad**
11	Entrega acta E/R	1 día	mié 9/9/15	mié 9/9/15	
12	**Capacitación (opcional)**	**5 días**	**lun 9/14/15**	**vie 9/18/15**	**Giannella Mestanza**
13	Capacitación teorica	2 días	lun 9/14/15	mar 9/15/15	
14	Pruebas fisicas	3 días	mié 9/16/15	vie 9/18/15	

Fig. 2.6. Diagrama de Gantt

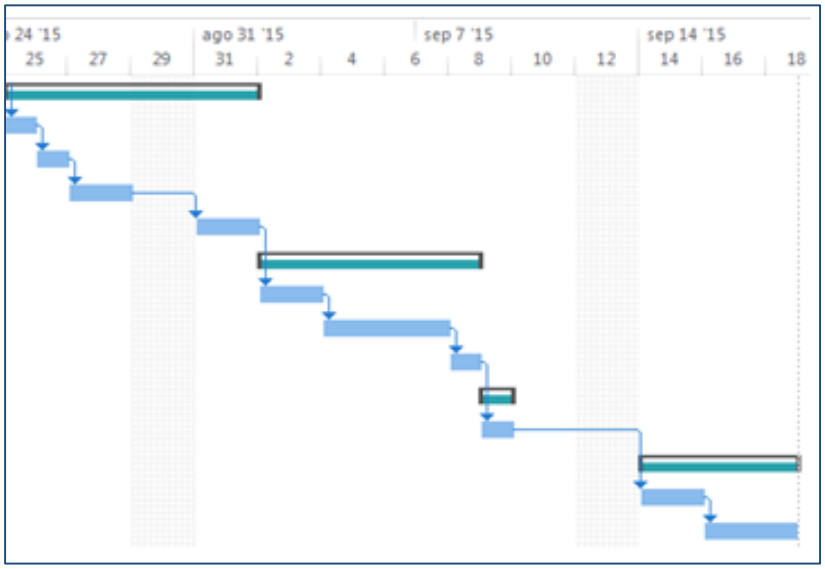


Fig. 2.7. Diagrama de Gantt

Lo primero será comenzar con la configuración del equipo, es decir la instalación y configuración del sistema operativo así como de la herramienta de gestión y todos los complementos o servicios que se requieran para el correcto funcionamiento de la consola, esto se llevará a cabo en un transcurso de seis días.

Luego, procederemos con la etapa de implementación de la consola en la empresa, en este periodo de tiempo de cinco días se realizarán las pruebas finales y el cliente podrá solicitar cambios de configuración en caso de ser necesario.

Una vez culminada la etapa de instalación y pruebas generales, se hace entrega del proyecto al cliente.
Nosotros también ofrecemos un periodo de capacitación para el personal que trabajará con el sistema de gestión, dicho valor se contempla dentro del presupuesto previamente presentado y el cliente puede decidir la fecha en la que desea recibirla.

CAPÍTULO 3

CAPITULO 3: PRUEBAS Y RESULTADOS OBTENIDOS

3.1 AMBIENTE DE PRUEBAS

Para la implementación de este proyecto, nuestro ambiente de prueba cuenta con los siguientes sistemas:

Hardware:

- Raspberry Pi.
- 512MB RAM.
- 16GB SD.
- HDMI.
- 10/100 BaseT Ethernet.
- (2) USB 2.0.
- 3.5 mm audio out Jack.
- Broadcom BCM2835 700MHz ARM1176JZFS.
- Fuente de alimentación vía el zócalo microUSB.
- Dimensiones: 85,6 x 53,98 x 17 mm.

Software:

Sistema Operativo:

- Raspbian.

Software de gestión:

- Nagios.
- SNMP.
- NagiosGraph.

3.2 RESULTADOS DE LA CONFIGURACIÓN

En la siguiente imagen podemos observar que los host que configuramos en las consolas están disponibles para ser monitoreados por Nagios:

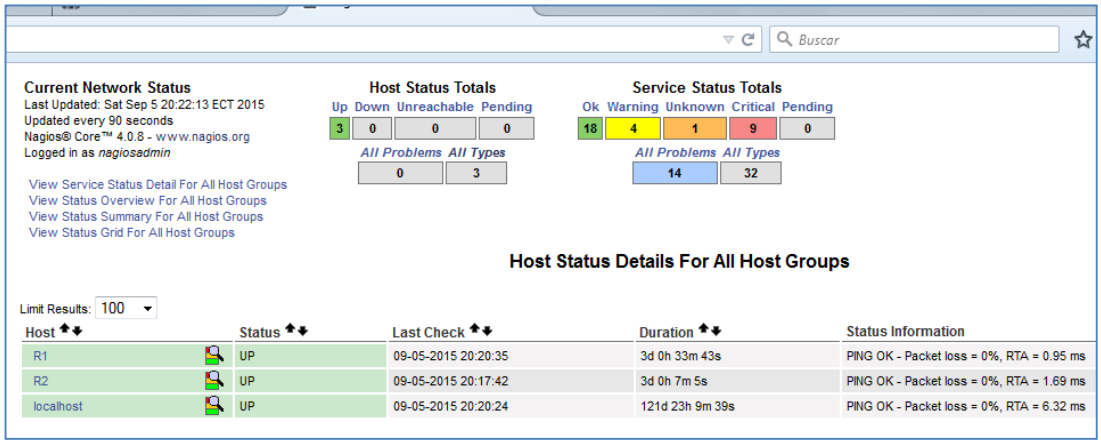


Fig.3.1 Host

Generando un poco de tráfico obtuvimos algunas alertas con diferentes estados, la imagen que se muestra a continuación detalla el tipo de servicio o aspecto y el host que está siendo supervisado junto con su estatus.

Por ejemplo, podemos notar que la carga del CPU de los 3 dispositivos se encuentra por entrar dentro del umbral de critico por lo que su estatus es warning, se representa por el color amarillo, Así mismo observamos que se encuentra en estado warning el servicio HTTP, sin embargo para que le llegue un correo al administrador el estatus debe ser crítico, se caracterizar por el color rojo, en la imagen se presenta una alarma de root partion que se encuentra en un estado crítico.

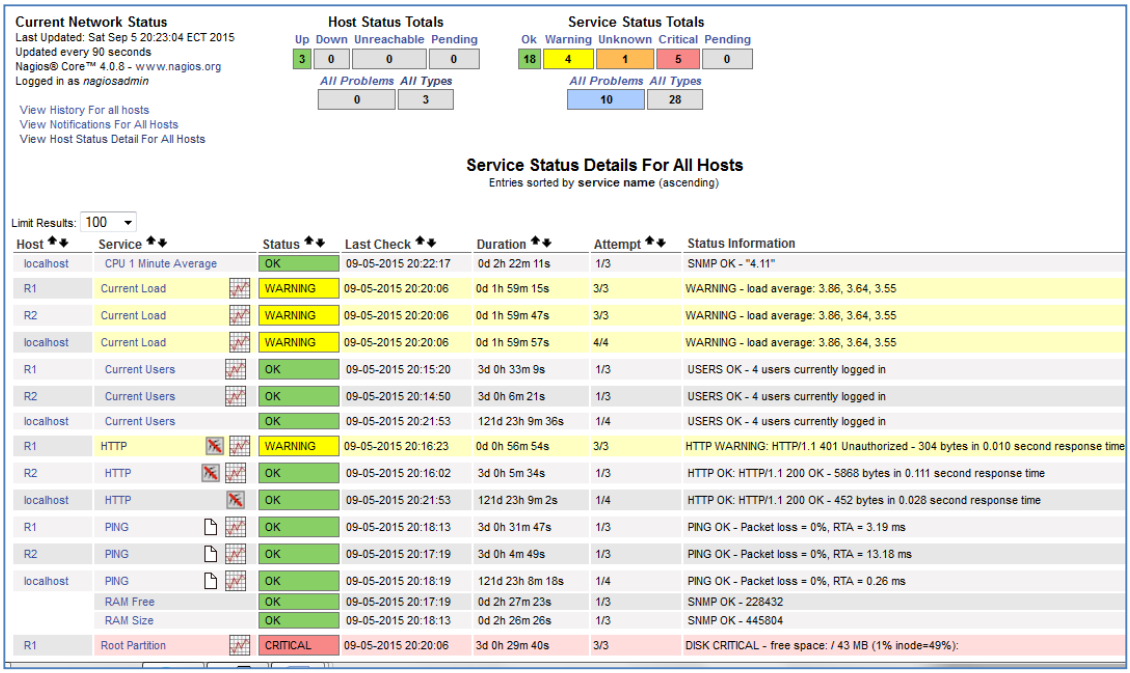


Fig.3.2 Service

En la siguiente imagen observamos que sigue la saturación de file system; como prueba no se terminó de configurar SNMP para monitoreo de disponibilidad y se muestra una alarma de color naranja cuyo estatus es desconocido, significa que Nagios está tratando de monitorear la disponibilidad de ese recurso sin embargo no se logra exitosamente.

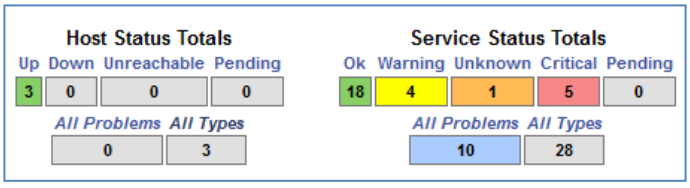
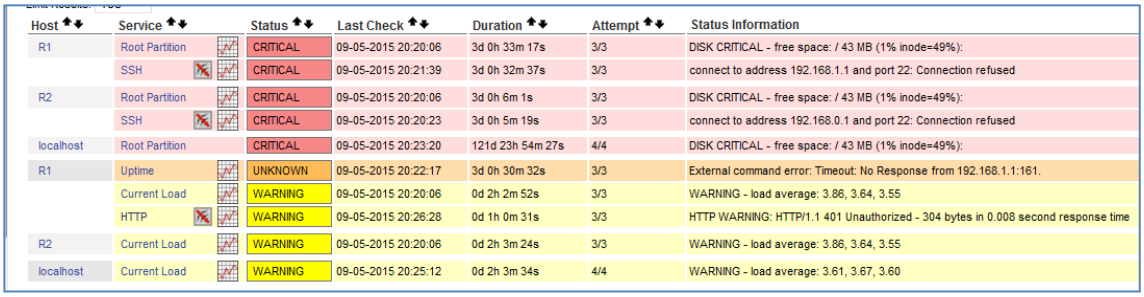


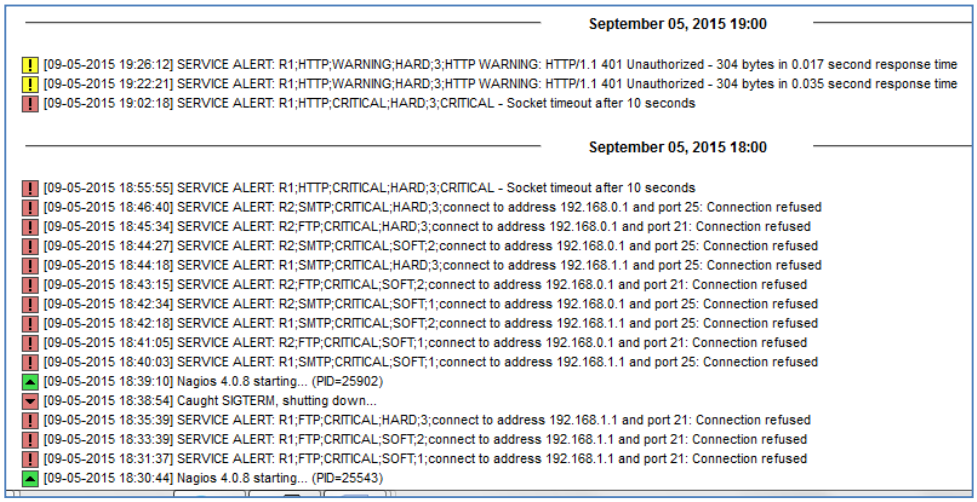
Fig.3.3 Status



Host	Service	Status	Last Check	Duration	Attempt	Status Information
R1	Root Partition	CRITICAL	09-05-2015 20:20:06	3d 0h 33m 17s	3/3	DISK CRITICAL - free space: / 43 MB (1% inode=49%):
	SSH	CRITICAL	09-05-2015 20:21:39	3d 0h 32m 37s	3/3	connect to address 192.168.1.1 and port 22: Connection refused
R2	Root Partition	CRITICAL	09-05-2015 20:20:06	3d 0h 6m 1s	3/3	DISK CRITICAL - free space: / 43 MB (1% inode=49%):
	SSH	CRITICAL	09-05-2015 20:20:23	3d 0h 5m 19s	3/3	connect to address 192.168.0.1 and port 22: Connection refused
localhost	Root Partition	CRITICAL	09-05-2015 20:23:20	121d 23h 54m 27s	4/4	DISK CRITICAL - free space: / 43 MB (1% inode=49%):
R1	Uptime	UNKNOWN	09-05-2015 20:22:17	3d 0h 30m 32s	3/3	External command error: Timeout: No Response from 192.168.1.1:161.
	Current Load	WARNING	09-05-2015 20:20:06	0d 2h 2m 52s	3/3	WARNING - load average: 3.86, 3.64, 3.55
	HTTP	WARNING	09-05-2015 20:26:28	0d 1h 0m 31s	3/3	HTTP WARNING: HTTP/1.1 401 Unauthorized - 304 bytes in 0.008 second response time
R2	Current Load	WARNING	09-05-2015 20:20:06	0d 2h 3m 24s	3/3	WARNING - load average: 3.86, 3.64, 3.55
localhost	Current Load	WARNING	09-05-2015 20:25:12	0d 2h 3m 34s	4/4	WARNING - load average: 3.61, 3.67, 3.60

Fig.3.4 Problems

Como el raspberry no tiene mucha capacidad de almacenamiento trabajando solo con la memoria de 16GB solo se lograba guardar logs de un solo día, mientras llegaban nuevas alertas y se generaban más logs los anteriores erran borrados. Para solucionar este inconveniente de memoria, podemos agregar un disco duro externo y configurar para que los logs sean guardados allí o inclusive almacenarlos en la nube o un servidor por medio de ftp.



September 05, 2015 19:00

[09-05-2015 19:26:12] SERVICE ALERT: R1;HTTP;WARNING;HARD;3;HTTP WARNING: HTTP/1.1 401 Unauthorized - 304 bytes in 0.017 second response time
[09-05-2015 19:22:21] SERVICE ALERT: R1;HTTP;WARNING;HARD;3;HTTP WARNING: HTTP/1.1 401 Unauthorized - 304 bytes in 0.035 second response time
[09-05-2015 19:02:18] SERVICE ALERT: R1;HTTP;CRITICAL;HARD;3;CRITICAL - Socket timeout after 10 seconds

September 05, 2015 18:00

[09-05-2015 18:55:55] SERVICE ALERT: R1;HTTP;CRITICAL;HARD;3;CRITICAL - Socket timeout after 10 seconds
[09-05-2015 18:46:40] SERVICE ALERT: R2;SMTP;CRITICAL;HARD;3;connect to address 192.168.0.1 and port 25: Connection refused
[09-05-2015 18:45:34] SERVICE ALERT: R2;FTP;CRITICAL;HARD;3;connect to address 192.168.0.1 and port 21: Connection refused
[09-05-2015 18:44:27] SERVICE ALERT: R2;SMTP;CRITICAL;SOFT;2;connect to address 192.168.0.1 and port 25: Connection refused
[09-05-2015 18:44:18] SERVICE ALERT: R1;SMTP;CRITICAL;HARD;3;connect to address 192.168.1.1 and port 25: Connection refused
[09-05-2015 18:43:15] SERVICE ALERT: R2;FTP;CRITICAL;SOFT;2;connect to address 192.168.0.1 and port 21: Connection refused
[09-05-2015 18:42:34] SERVICE ALERT: R2;SMTP;CRITICAL;SOFT;1;connect to address 192.168.0.1 and port 25: Connection refused
[09-05-2015 18:42:18] SERVICE ALERT: R1;SMTP;CRITICAL;SOFT;2;connect to address 192.168.1.1 and port 25: Connection refused
[09-05-2015 18:41:05] SERVICE ALERT: R2;FTP;CRITICAL;SOFT;1;connect to address 192.168.0.1 and port 21: Connection refused
[09-05-2015 18:40:03] SERVICE ALERT: R1;SMTP;CRITICAL;SOFT;1;connect to address 192.168.1.1 and port 25: Connection refused
[09-05-2015 18:39:10] Nagios 4.0.8 starting... (PID=25902)
[09-05-2015 18:38:54] Caught SIGTERM, shutting down...
[09-05-2015 18:35:39] SERVICE ALERT: R1;FTP;CRITICAL;HARD;3;connect to address 192.168.1.1 and port 21: Connection refused
[09-05-2015 18:33:39] SERVICE ALERT: R1;FTP;CRITICAL;SOFT;2;connect to address 192.168.1.1 and port 21: Connection refused
[09-05-2015 18:31:37] SERVICE ALERT: R1;FTP;CRITICAL;SOFT;1;connect to address 192.168.1.1 and port 21: Connection refused
[09-05-2015 18:30:44] Nagios 4.0.8 starting... (PID=25543)

Fig. 3.5 Alerts History

3.3 RESULTADOS CON NAGIOSGRAPH

Como mencionamos anteriormente con NagiosGraph logramos que los gráficos del comportamiento de los recursos sean más amigables a la vista del

administrador o personal encargado, a continuación se presenta los resultados del monitoreo de CPU. Se presentan reportes por día, semana y mes.

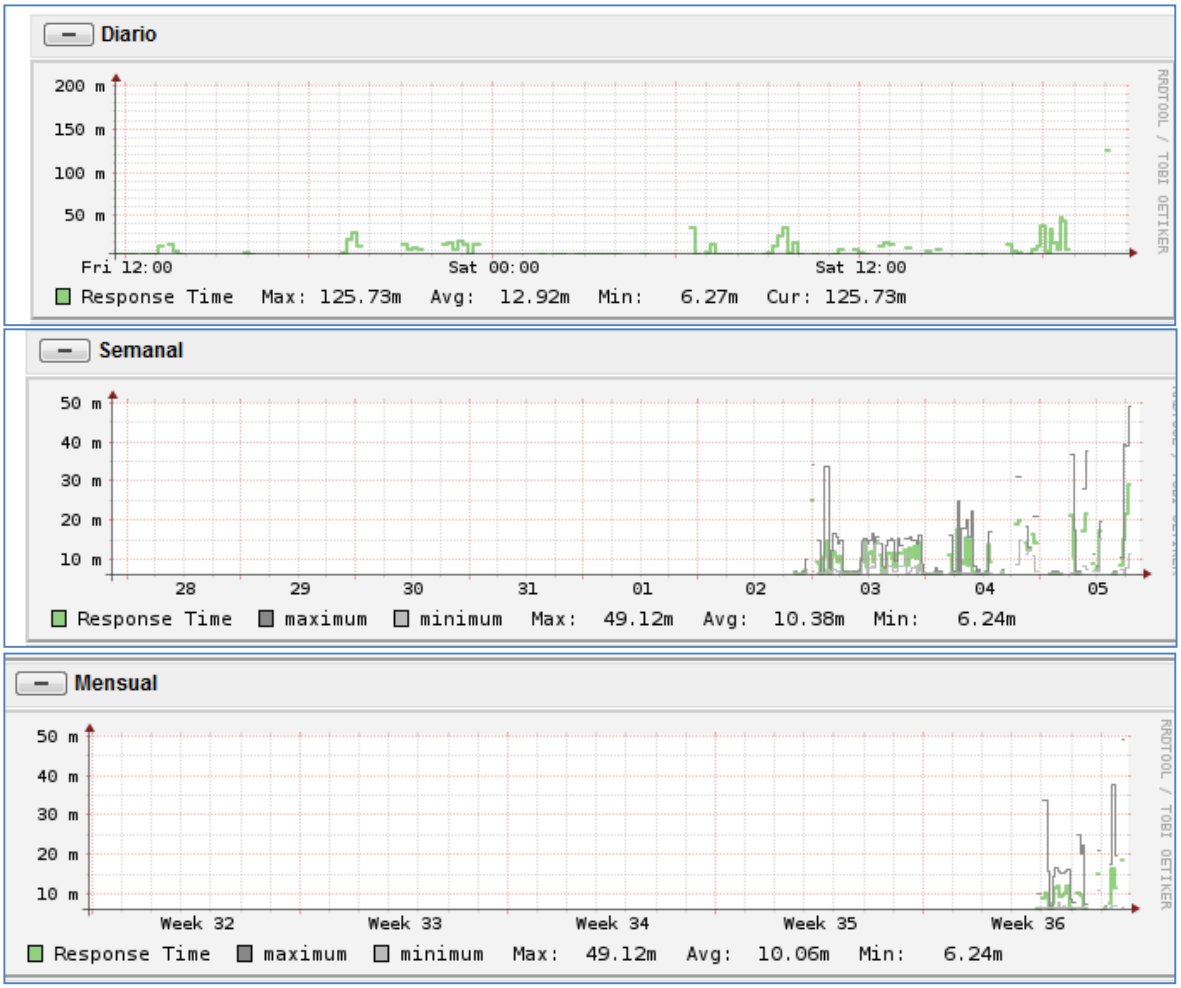


Fig. 3.6 Pestaña NagiosGraph

Para facilitar al administrador la supervisión de los recursos y servicios, realizamos pruebas con NagiosGraph para presentar dentro de la alarma un icono el cual muestra los gráficos diarios de manera más rápida.

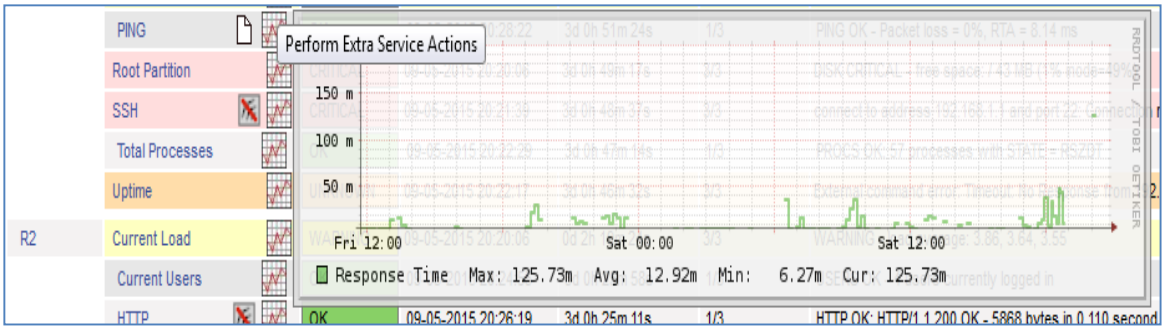


Fig. 3.7 Reporte NagiosGraph

3.4 NOTIFICACIONES AL CORREO

Nagios te permite configurar una dirección de correo electrónico para poder enviar notificaciones de alerta al administrador de red y así de esta forma poder solucionar cualquier problema oportunamente.

La siguiente imagen muestra el formato de los correos que le llegan a la persona encargada de supervisar y administrar la herramienta.

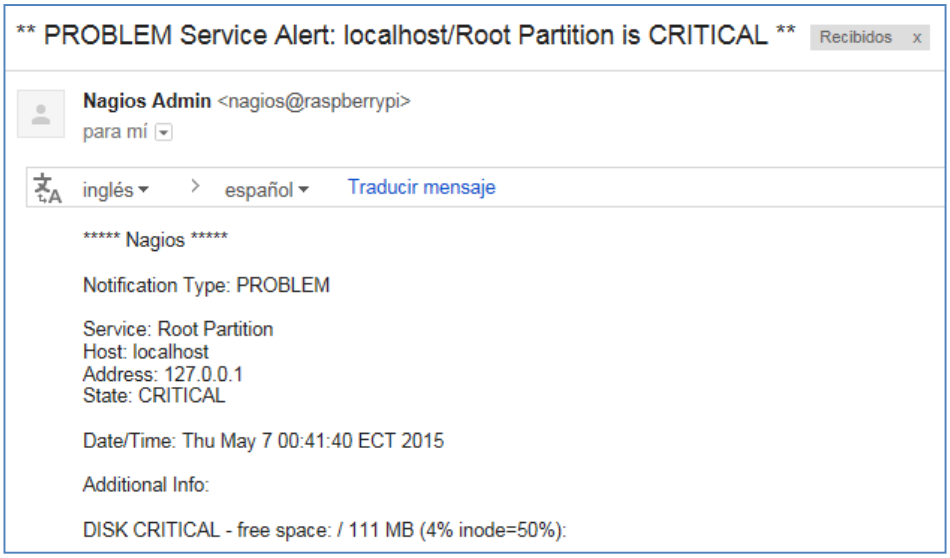


Fig. 3.8 Notificaciones vía correo

CONCLUSIONES Y RECOMENDACIONES

Al finalizar el periodo de implementación concluimos que:

1. La herramienta de gestión Nagios puede ser fácilmente implementado en una red grande o pequeña.
2. Al no tener costo representa una gran ventaja sobre todo para las empresas pequeña que recién están comenzando en el mercado ecuatoriano y quieran reducir costos.
3. Es una herramienta eficiente, eficaz y versátil, ya que nos permite configurar cualquier tipo de dispositivo que se encuentre presente dentro de la red de la empresa.
4. Es de gran ayuda para el administrador al momento de llevar un historial del comportamiento de los equipos que existen en la red.

Se recomienda lo siguiente:

1. Trabajar con distribuciones que sean basadas en debían por concepto de compatibilidad con Nagios.
2. Hacer uso del complemento NagiosGraph para poder obtener mejores gráficos del comportamiento de la red.
3. Aprovechar los beneficios de Nagios como herramienta de monitoreo por medio de la integración con otros protocolos de gestión como SNMP u otras herramientas de monitoreo como MRTG.

BIBLIOGRAFÍA

[1] NSRC, (2015, mayo 22), Gestión de redes, [Online]. Disponible en:http://www.eslared.org.ve/walc2012/material/track3/gestion-de-redes.pdf.

[2] Sourceforge, (2015, mayo 26), Net-SNMP, [Online]. Disponible en:http://net-snmp.sourceforge.net/.

[3] Nagios, (2015, junio 22), Nagios, [Online]. Disponible en:https://www.nagios.org/about/overview/.

[4] Zabbix,(2015, Mayo 26), Zabbix, [Online], Disponible en: http://www.zabbix.com/features.php

[5] NFSEN, (2015, mayo 26), Netflow/NFSEN,Netflow/ NfSen[Online]. Disponible en: http://nfsen.sourceforge.net/.

[6] Networkuptime, (2015, mayo 26), Netflow, [Online]. Disponible en: http://www.networkuptime.com/tools/netflow/.

[7] Oetiker, (2015, mayo 26), MRTG, [Online]. Disponible en:http://oss.oetiker.ch/mrtg/.

[8] Nessus, (2015, mayo 28), Tenable Nessus Security, [Online]. Disponible en:http://www.tenable.com/products/nessus/select-your-operating-system.

[9] NSRC, (2015, mayo 28), Básicos de Linux, [Online]. Disponible en:https://nsrc.org/workshops/2014/walc/raw.../wiki/.../basicos-de-linux.pdf

[10] Sourceforge, (2015, julio 22), Nagiosgraph, [Online]. Disponible en: http://nagiosgraph.sourceforge.net.

ANEXO A

A.1 CONFIGURACIÓN DE RED

Para poder tener conexión a internet en debían necesitamos configurar la tarjeta de red.

1. Abrimos un Terminal.
2. Entramos al archivo de configuración de red. */etc/network/interface*.
3. Configuramos para que sea de manera estática.
4. Configuramos los dns en el archivo */etc/resolv.conf.*
5. Reiniciamos la interfaz de red.

Con esto se obtiene nuestra consola trabajando con Raspbian.

A.1.2 INSTALACIÓN DE NAGIOS

Los pasos para la instalación de Nagios son:

1. Descargamos todos los paquetes que necesitaremos para poder instalar Nagios correctamente.
2. Creamos 2 grupos.
3. Creamos un usuario administrador.
4. Agregamos un el usuario al grupo de administradores.
5. Descargamos la última versión de Nagios y Extraemos los archivos

   #wget http://prdownloads.sourceforge.net/sourceforge/nagios/nagios-4.0.8.tar.gz
6. Creamos 2 carpetas:
   - Stylesheets
   - images
7. Comenzamos con la compilación de los archivos:

   #./configure --prefix=/usr/local/nagios --with-nagios-user=nagios --with-nagios-group=nagios --with-command-user=nagios --with-command-group=nagcmd

   #make all

   #make install

#make install-init
#make install-config
#make install commandmode
#make install-webconf

8. En caso de error [install-webconf]:
   #/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/conf-available/nagios.conf
   #ln -s /etc/apache2/conf-available/nagios.conf /etc/apache2/conf-enabled/nagios.conf

9. Descargamos los pluggins necesarios para que Nagios funcione correctamente y extraemos los archivos:
   #wget https://www.nagios-plugins.org/download/nagios-plugins-2.0.3.tar.gz
10. Comenzamos la compilación de los archivos:
    #./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl=/usr/bin/openssl --enable-perl-modules --enable-libtap
    #make all
    #make install

A.1.3 CONFIGURACIÓN APACHE

1. Se edita el archivo apache2.conf:
   #nano /etc/apache2/apache2.conf
   Include sites=enabled/
   Server Name localhost
   #a2enmod rewrite
   # a2enmod cgi
2. Reiniciamos apache.
3. Copiar los eventhandles.
4. Abrir el navegador y escribir:
   ipnagios/Nagios/

ANEXO B

B.1 CONFIGURACIÓN NRPE

1. Descargamos los paquetes y extraemos los archivos:

   #wget http://kent.dl.sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz

2. Necesitamos instalar:

   #apt-file

3. Para encontrar la ruta donde se encuentra las librerías utilizamos:

   #apt-file search libssl | grep ibssl-dev

4. Como se tiene problemas con la carpeta de librerías openssl necesitamos otra ruta:

   # ./configure --with-ssl=/usr/bin/openssl --with-ssl-lib=/usr/lib/x86_64-linux-gnu

   Cambiar la ruta por la que le dice el comando utilizado en el paso anterior.

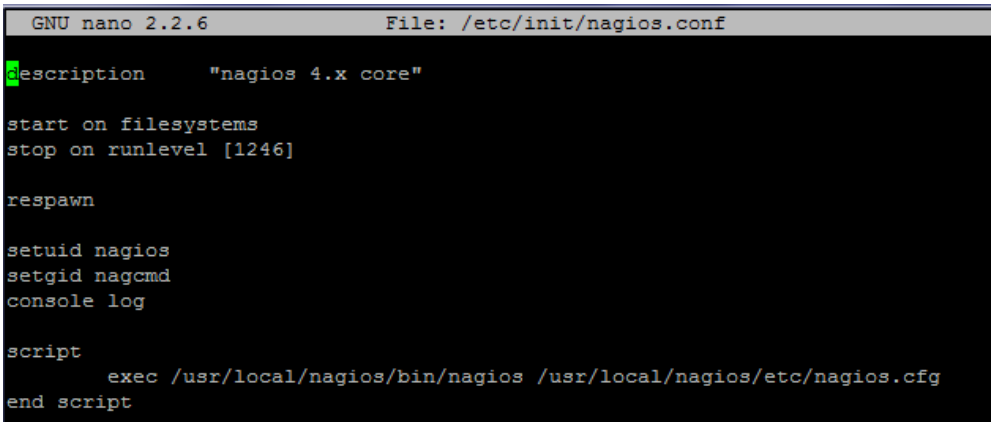
5. Compilamos:

   #make all

   #make install

6. Modificar el upstart script como se muestra en la siguiente imagen:

   #nano /etc/init/Nagios.conf



B.2 CONFIGURACIÓN NAGIOSGRAPH

Descargamos los paquetes y extraemos los archivos:

#wget http://downloads.sourceforge.net/project/nagiosgraph/nagiosgraph/1.5.1/nagiosgraph-1.5.1.tar.gz

1. Chequear que todos los pr-requisitos se encuentren instalados.
2. En la configuración de servicios agregamos:

   action_url /nagiosgraph/cgi-bin/show.cgi?host=$HOSTNAME$&service=$SERVICEDESC$&geom=1000x200' onMouseOver='showGraphPopup(this)' onMouseOut='hideGraphPopup()' rel='/nagiosgraph/cgi-bin/showgraph.cgi?host=$HOSTNAME$&service=$SERVICEDESC$
3. Editamos o creamos el archivo:

   #vim /usr/local/nagios/share/ssi/common-header.ssi
4. Agregamos:

   <script type="text/javascript" src="/nagiosgraph/nagiosgraph.js"></script>
5. Reiniciamos el servicio.

B.3 CONFIGURACIÓN SNMP EN NAGIOS

1. Descargamos los paquetes:

   #apt-get install snmp snmpd

2. Editar el archivo:

#nano /etc/default/snmp

#SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -smux -p /var/run/snmpd.pid 127.0.0.1'

SNMPDOPTS='-Lsd -Lf /dev/null -u snmp -I -p /var/run/snmpd.pid localhost'

3. Configurando el archivo:

#nano /etc/snmp/snmpd.conf

#rocommunity public *red y mascara de la red*

#rocommunity public *localhost*

B.4 CONFIGURACIÓN MRTG EN NAGIOS

1. Se descarga y se extrae los paquetes.
2. Se compila e instala.

#../configure –prefix=/usr/local/mrtg-2

#make

#make install

3. Copiamos la información de Nagios.
4. Creamos un carpeta para los archivos y gráficos que se gerarán.
5. Configurar MRTG para que use esta nueva carpeta.
6. Incluimos al comienzo del archivo el directorio de trabajo para el funcionamiento de MRTG.
7. Lo iniciamos

env LANG=C /usr/bin/mrtg /usr/local/nagios/etc/mrtg.cfg

8. Creamos una página principal HTML.
9. Configuramos un cron cada 5 minutos
10. En el menú agregamos lo siguiente para poder acceder a los gráficos que nos brinda MRTG:

```
<li><a href="/nagios/stats" target="<?php echo
$link_target;?>">MRTG stats</a></li>
```

ANEXO C

C.1 CONFIGURACIÓN SERVICIOS A MONITOREAR

1. Debemos definir qué servicios vamos a monitorear en el archivo commands.cfg:
   Vamos a definir el servicio http:

   ```
   define command {
   name check_http
   command_name check_http
   command_line $USER1$ / check_http –I $HOSTADDRESS$ $ARG$
   }
   ```

2. En el archivo donde definimos los equipos agregamos:
   ```
   define service{
   use generic-service
   host_name R1
   service_description HTTP
   check_command check_http
   }
   ```

Así con cada servicio que vayamos a supervisar.

C.2 CONFIGURACIÓN DE EQUIPOS A MONITOREAR

1. Definimos el equipo a monitorear en routers.cfg

   ```
   define host {
   use generic-host
   ```

host_name R1
alias R1
address *Ipdelequipo*
check_period 24x7
retry_interval 1
check_interval 5
max_check_attempts 10
check_command check-host-alive
notification_period 30
notification_interval 120
notification_options d,u,r
contact_groups admins
register 0
}

2. En el archivo nagios.cfg agregamos en nuevo archivo de configuración.
   Cfg_file=/usr/local/nagios/etc/objects/routers.cfg

Así mismo para todos los equipos que vayamos a supervisar.

ANEXO D

D.1 CONFIGURACIÓN NOTIFICACIONES VIA WEB

1. Editamos el archivo contact.cfg:

```
define contact{

contact_name      nagiosadmin   ;

use                  generic-contact

alias                 Nagios Admin  ; Full name of user

email                 admin@foodshrimp.com
```

```
        service_notification_period             24x7
        host_notification_period                24x7
        service_notification_options  w,u,c,r,f
        host_notification_options d,u,r,f
        service_notification_commands notify-service-by-email
        host_notification_commands notify-host-by-email
}
```