



Sistema de Monitoreo de Infraestructura de red para el
Ministerio de Economía Familiar, Comunitaria, Cooperativa y
Asociativa (MEFCCA)

UNIVERSIDAD NACIONAL AUTÓNOMA DE NICARAGUA

UNAN-MANAGUA

RECINTO UNIVERSITARIO RUBÉN DARÍO

FACULTAD DE CIENCIAS E INGENIERÍA

DEPARTAMENTO DE TECNOLOGÍA

**TRABAJO DE SEMINARIO DE GRADUACIÓN PARA OBTAR AL TÍTULO DE
INGENIERO EN ELECTRÓNICA**



TEMA

**SISTEMA DE MONITOREO DE INFRAESTRUCTURA DE RED PARA EL
MINISTERIO DE ECONOMIA FAMILIAR, COMUNITARIO, COOPERATIVA Y
ASOCIATIVA (MEFCCA).**

AUTORES:

**BR. MAXEL ELIEZER OROZCO MENDEZ
BR ALEXIS XAVIER MONTOYA GOMEZ.**

TUTOR: MSc. MILCIADES DELGADILLO

ASESOR TECNOLÓGICO: MSc. ÁLVARO SEGOVIA AGUIRRE.

ASESOR TECNOLÓGICO: ING. GERALD M. LANZAS GARAY

MANAGUA, NOVIEMBRE 2015



DEDICATORIA

Gracias primeramente a Dios, por darme la vida y la sabiduría, por estar conmigo en cada momento de mi vida, por iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi consejeros y compañía durante todo este proceso educativo.

Mi madre Lic. Lissette Carolina Méndez García, por darme la vida, creer en mí y porque siempre me apoyaste sin importar la situación. Mamá gracias por darme una carrera para mi futuro, todo esto te lo debo a ti.

Mi padre Pedro Francisco Orozco Castro, gracias por apoyarme todos estos años se le agradece mucho por todo.

Mi abuela que es mi segunda madre Mayra García Sequeira, por quererme y apoyarme siempre, esto también se lo debo a usted.

Mi hija María Amanda Orozco García, por llenar mi corazón de alegría, amor y fortaleza para culminar con éxito esta carrera. Te quiero hija bella.

Todos aquellos familiares y amigos que no recordé al momento de escribir esto. Ustedes saben quiénes son.

“GRACIAS”

Maxel Eliezer Orozco Méndez



DEDICATORIA

Primero agradezco a Dios por darme la vida, haberme permitido llegar hasta este punto de mi carrera y mi vida, por mi salud y la esperanza de un futuro mejor. Te agradezco los obstáculos y las penas que he pasado porque de ellos he aprendido y seguido adelante cuando había perdido los ánimos de continuar. Por iluminar mi mente y acompañarme en cada decisión que he tomado. Por poner en mí camino aquellas personas que me han dado su amistad y su apoyo incondicional en momentos importantes.

Agradezco a mi papá JUAN JOSE MONTOYA BELIZ aunque su vida fue muy diferente a la mía, nunca le dieron la oportunidad de asistir a una universidad debido a la situación, el hizo todo lo posible para que yo pudiera hacerlo, para mí es un gran ejemplo de esfuerzo y de que ante las más difíciles de las pruebas de la vida es posible sonreír, por su entereza y fortaleza. Por luchar tanto para sacarnos adelante a mis hermanos nos ha enseñado que todo se puede conseguir con trabajo y esfuerzo.

Agradezco a mi mamá SANDRA DEL SOCORRO GOMEZ PAIZ que me inculco desde niño todos los valores con los que cuento. Por tu confianza, paciencia, sabiduría, y el poderme guiar en momentos difíciles de la vida. Lo que soy hoy día te lo debo gran parte a ti, te quiero.

Agradezco al resto de mis familiares que creyeron en mí y estuvieron pendiente de brindarme su ayuda en lo que estuviera a su alcance para así poderlo lograr.

A todos mis amigos y compañeros que he conocido a lo largo de mi carrera, por el esfuerzo que hicimos cada semestre luchando por llegar hasta lo más último de nuestra carrera.

“GRACIAS”

Alexis Xavier Montoya Gómez



AGRADECIMIENTOS

Para poder realizar este trabajo de la mejor manera posible fue necesario del apoyo de muchas personas a las cuales quiero agradecer.

Agradecemos grandemente y primeramente a DIOS por permitirnos llegar a la cúspide de nuestra carrera. Por darnos la salud y la sabiduría en cada momento de nuestra vida.

Agradecemos a cada uno de los profesores de la carrera de Ing. Electrónica de la Universidad Nacional autónoma de Nicaragua por habernos enseñado y compartido con nosotros sus conocimientos.

Agradecemos a MSc. Álvaro Segovia Aguirre quien fue nuestro Asesor por guiarnos y darnos sus consejos y opinión en la elaboración de este trabajo.

Agradecemos a Ing. Gerald Martín Lanzas Garay quien fue nuestro Asesor Informático por guiarnos y darnos sus consejos y opinión en la elaboración de este trabajo.

Agradecemos a MSc. Milciades Delgadillo por ser nuestro tutor, por las charlas y la paciencia en la revisión de nuestro documento.

Por último y no menos importante agradecemos a la Universidad Nacional Autónoma de Nicaragua UNAN-Managua por la formación obtenida durante el transcurso de nuestra carrera, por las experiencias vividas, alegrías, tristezas, material didáctico, por todo lo bueno y todo lo malo.

“MUCHAS GRACIAS”

Maxel Orozco

Alexis Montoya



Contenido

| | |
|---|-----------|
| CAPITULO I..... | 11 |
| 1.1 Introducción..... | 11 |
| 1.2 Justificación. | 12 |
| 1.3 Objetivos. | 13 |
| 1.3.1 Objetivo general..... | 13 |
| 1.3.2 Objetivos específicos..... | 13 |
| CAPITULO II | 14 |
| 2.1 Fundamentos de la base teórica | 14 |
| 2.1.1 Software Libre | 14 |
| 2.1.2 Características | 14 |
| 2.1.3 Gestión de red | 14 |
| 2.1.4 Monitoreo de red..... | 15 |
| 2.1.5 Protocolo Simple de Gestión de Red..... | 15 |
| 2.2 Metodología | 16 |
| 2.2.1 Entorno de Red..... | 16 |
| 2.2.2 Modelo de Organización..... | 17 |
| 2.2.3 Modelo de Información..... | 17 |
| 2.2.4 Modelo de Comunicación | 18 |
| 2.2.5 Modelo Funcional..... | 18 |
| 2.3 Herramientas | 23 |
| 2.3.1 Nagios | 23 |
| 2.3.2 Cacti..... | 24 |
| CAPITULO III | 25 |
| 3.1 Desarrollo..... | 25 |
| 3.1.1 Diseño Operativo..... | 25 |
| 3.1.2 Plan de Actividades | 28 |
| 3.1.3 Diagrama de Gantt..... | 29 |
| 3.1.4 Topología de red MEFCCA | 30 |
| 3.2 Fase Diagnóstico | 31 |
| 3.2.1 Reportes de fallas en enlace de datos..... | 33 |



| | |
|---|------------|
| 3.3 Fase Factibilidad | 35 |
| 3.3.1 Factibilidad técnica | 35 |
| 3.3.2 Factibilidad operativa | 37 |
| 3.4 Instalación de herramientas | 43 |
| 3.4.1 Instalación Debian 8.1.0 AMD x64 | 43 |
| 3.4.2 Configuraciones adicionales | 60 |
| 3.4.3 Nagios | 62 |
| 3.4.4 Cacti..... | 68 |
| 3.5 Configuración personalizada de herramientas..... | 77 |
| 3.5.1 Configuración de Nagios..... | 77 |
| 3.5.2 Configuración de Cacti..... | 86 |
| 3.6 Evaluación de sistema en ambiente controlado. | 92 |
| 3.6.1 Procedimiento para dar solución a fallas de host y servicios | 101 |
| CAPITULO IV | 102 |
| 4.1 Conclusiones | 102 |
| 4.2 Recomendaciones | 103 |
| 4.3 Bibliografía | 104 |
| 4.4 ANEXOS | 107 |
| 4.4.1 ANEXOS A | 108 |
| 4.4.2 ANEXOS B | 111 |
| 4.3.3 ANEXOS C | 115 |
| 4.3.4 ANEXOS D | 118 |



INDICE DE ILUSTRACIONES

| | |
|--|----|
| Ilustración 1: Mensaje Snmp..... | 16 |
| Ilustración 2: Sub-Sistemas del entorno de red OSIE | 17 |
| Ilustración 3: Proceso de Gestión de Fallas..... | 20 |
| Ilustración 4: Interfaz de Nagios..... | 23 |
| Ilustración 5: Interfaz de Cacti..... | 24 |
| Ilustración 6: Diagrama de Gantt..... | 29 |
| Ilustración 7: Topología de Red MEFCCA..... | 30 |
| Ilustración 8: Reporte Falla de enlace de Red MEFCCA | 33 |
| Ilustración 9: Instalación Debian paso 1 | 43 |
| Ilustración 10: Instalación Debian paso 2 | 44 |
| Ilustración 11: Instalación Debian paso 3 | 45 |
| Ilustración 12: Instalación Debian paso 4 | 46 |
| Ilustración 13: Instalación Debian paso 5 | 47 |
| Ilustración 14: Instalación Debian paso 6 | 48 |
| Ilustración 15: Instalación Debian paso 7 | 48 |
| Ilustración 16: Instalación Debian paso 8 | 49 |
| Ilustración 17: Instalación Debian paso 9 | 49 |
| Ilustración 18: Instalación Debian paso 10 | 50 |
| Ilustración 19: Instalación Debian paso 11 | 50 |
| Ilustración 20: Instalación Debian paso 12 | 51 |
| Ilustración 21: Instalación Debian pasó 13 | 52 |
| Ilustración 22: Instalación Debian paso 14 | 52 |
| Ilustración 23: Instalación Debian paso 15 | 53 |
| Ilustración 24: Instalación Debian paso 16 | 54 |
| Ilustración 25: Instalación Debian paso 17 | 55 |
| Ilustración 26: Instalación Debian paso 18 | 56 |
| Ilustración 27: Instalación Debian paso 19..... | 57 |
| Ilustración 28: Instalación Debian paso 20..... | 58 |
| Ilustración 29: Instalación Debian paso 21..... | 59 |
| Ilustración 30: Configuración tarjeta de red..... | 60 |
| Ilustración 31: Configuración de repositorios..... | 61 |
| Ilustración 32: Actualización de repositorios..... | 62 |
| Ilustración 33: Instalación de prerequisites..... | 62 |
| Ilustración 34: Creación de cuenta Nagios..... | 63 |
| Ilustración 35: Creación de grupo nagcmd..... | 63 |
| Ilustración 36: Agregando al usuario nagios al grupo nagcmd..... | 63 |
| Ilustración 37: Agregando al usuario de apache (www-data) al grupo nagcmd..... | 63 |
| Ilustración 38: Comando para extraer el archivo comprimido de nagios..... | 64 |
| Ilustración 39: Cambio hacia el directorio nagios-4.1.1..... | 64 |
| Ilustración 40: Error tras compilar e instalar la interfaz web de Nagios..... | 65 |
| Ilustración 41: Resultado de muestra de verificación de nagios.conf..... | 66 |



| | |
|---|-----|
| Ilustración 42: Configuración de contraseña de usuario root de MySQL..... | 68 |
| Ilustración 43: Elección de servidor web para configurar cacti..... | 69 |
| Ilustración 44: Elección de configuración de base de datos para cacti..... | 70 |
| Ilustración 45: Proporcionar contraseña root..... | 71 |
| Ilustración 46: Proporcionar una nueva contraseña..... | 71 |
| Ilustración 47: Verificar contraseña..... | 72 |
| Ilustración 48: Dirección web de Cacti..... | 72 |
| Ilustración 49: Cacti guía de instalación..... | 73 |
| Ilustración 50: Cacti finalización de instalación..... | 74 |
| Ilustración 51: Cacti User Login..... | 75 |
| Ilustración 52: vista general de Cacti..... | 76 |
| Ilustración 53: ID de correo electrónico real para recibir alertas..... | 77 |
| Ilustración 54: Serie de IP que tendrá acceso a nagios..... | 79 |
| Ilustración 55: Solicitud de accesos en interfaz web de Nagios..... | 80 |
| Ilustración 56: Consola administrativa de Nagios..... | 81 |
| Ilustración 57: Pestaña hosts en la consola administrativa de Nagios..... | 81 |
| Ilustración 58: Contenido más detallado de localhost..... | 82 |
| Ilustración 59: Nuevo cliente recién agregado en Nagios..... | 85 |
| Ilustración 60: Consola Cacti..... | 86 |
| Ilustración 61: Agregar nuevo dispositivo en Cacti..... | 87 |
| Ilustración 62: Agregar nuevo dispositivo en el listado..... | 88 |
| Ilustración 63: Opciones para crear gráficas..... | 88 |
| Ilustración 64: Verificación de dispositivos en Up..... | 89 |
| Ilustración 65: Filtro de Gráficos..... | 90 |
| Ilustración 66: Agregar dispositivos a la lista de Grafica Cacti..... | 91 |
| Ilustración 67: Agregando dispositivo a Default tree, mostrando todas sus gráficas..... | 91 |
| Ilustración 68: Topología de Red MEFCCA - Cortes..... | 92 |
| Ilustración 69: Mapa de red de todos los host en monitoreo..... | 93 |
| Ilustración 70: Pantalla de Resumen de reportes..... | 94 |
| Ilustración 71: Reporte de Alertas más recientes de host..... | 95 |
| Ilustración 72: Reporte General de todas las alertas de host y servicios..... | 96 |
| Ilustración 73: Pantalla de comentarios acerca de Host y Servicios..... | 97 |
| Ilustración 74: Pantalla de visualización de Configuración de host y servicios..... | 98 |
| Ilustración 75: Historial de estado del host reposerver.mefc.gob.ni..... | 99 |
| Ilustración 76: Histograma de alertas del host..... | 100 |
| Ilustración 77: Centro de Datos..... | 109 |
| Ilustración 78: Rack de Comunicaciones MEFCCA..... | 110 |
| Ilustración 79: Centro de Datos..... | 119 |



INDICE DE TABLAS

| | |
|--|----|
| Tabla 1: Plan de Actividades..... | 28 |
| Tabla 2: Cuadro comparativo de Software de Monitoreo | 36 |
| Tabla 3: Características del Ordenador de pruebas | 37 |



Resumen.

En el presente trabajo de culminación de estudios, se desarrolla un estudio de software libre Nagios, aplicación que monitorea esencialmente activos y servicios de red. Serán demostradas sus capacidades en una forma práctica, tratando de ayudar al administrador de la red a través del proceso de configuración para el uso de esta herramienta. Algunas de las características de Nagios son: monitoreo de servicios de red SMTP, POP3, HTTP, NNTP, entre otros; monitoreo de los recursos del servidor, tales como CPU, memoria, disco duros y procesos; capacidad para definir la jerarquía de la red; notificaciones inmediatas sobre problemas de red a través de correo electrónico; capacidad de tomar contramedidas de acuerdo con problemas de la red; una interfaz web con el mapa de la red en 2D y 3D, informes, gráficos e históricos. Es versátil, flexible y verifica constantemente la disponibilidad de servicios y hosts.

Palabras clave: plugin, software, hosts, monitoreo, fallas de red, Nagios.



CAPITULO I

1.1 Introducción.

El Ministerio de Economía Familiar, Comunitaria, Cooperativa y Asociativa, es una institución de carácter público que expresa la esencia de nuestro modelo socio-productivo basado en las personas, las familias y las comunidades, el desarrollo de este ministerio es políticamente estratégico y junto al de Salud y Educación constituyen sectores que determinan la vida social, política y económica del país y la Revolución.

En los últimos años la institución ha sufrido un aumento de servicios informáticos, provocado por el incremento poblacional laboral. Esta situación ha generado una serie de problemas de rendimiento en la red de datos, los usuarios acceden de manera descontrolada a los servicios informáticos ofrecidos por el ministerio, comprometiendo la estabilidad de servicios críticos de la institución. Ante estas circunstancias, el área de informática necesita herramientas de monitoreo de infraestructura de red que faciliten su administración, detección de anomalías, etc.

El trabajo de tesis titulado; “Sistema de Monitoreo de Infraestructura de Red para el Ministerio de Economía Familiar, Comunitario, Cooperativa y Asociativa (MEFCCA).”, pretende ofrecer una solución en alternativas de software libre, que no genere costos en su adquisición.

Se pretende mejorar los servicios de red permitiendo a los usuarios realizar sus asignaciones de manera eficiente mediante la herramienta Nagios, Cacti y bajo los estándares de ISO que en su serie 10165-x esquematizan la administración de los objetos y sus propiedades que corresponden a los aspectos de información de los modelos de administración de sistemas y establecen los requisitos que una empresa debe cumplir, para considerar que disponen de una Gestión de la Red basada en el concepto de administración de sistemas ([Véase Anexo D](#)).



1.2 Justificación.

En el Ministerio de Economía Familiar Comunitaria Cooperativa y Asociativa (MEFCCA) no se monitorean los servicios de red, ni a los usuarios. Debido a la inexistencia de un software de monitoreo, que satisfaga todos sus requerimientos técnicos y se adapte a su capacidad económica. Los esfuerzos del área de informática por adquirir un software propietario se han visto frenados por los altos costos de adquisición.

Por lo anteriormente expuesto, el jefe del área de informática de la institución, ha decidido implementar una herramienta de gestión de red, con licencia de software libre. Mediante el trabajo de tesis titulado “Sistema de Monitoreo de Infraestructura de red para el Ministerio de Economía Familiar Comunitaria Cooperativa y Asociativa (MEFCCA)”, este proyecto usará una herramienta informática, considerando la compatibilidad con las aplicaciones existentes, fácil manipulación mediante interfaz gráfica amigable, enviar notificaciones de incidencias, reportes exactos, entre otros.

Todo esto permitirá al área de informática obtener un software que se adapte a las características propias de la institución, facilitando la administración de la red de datos. Con la adquisición de la aplicación de monitoreo, también se beneficiaran los trabajadores, pues dispondrán de una red segura, confiable, rápida y eficiente.



1.3 Objetivos.

1.3.1 Objetivo general.

1. Desarrollar un Sistema de Monitoreo utilizando Nagios para identificar y reportar fallas de manera instantánea, en la infraestructura de red del Ministerio de Economía Familiar, Comunitario, Cooperativa y Asociativa.

1.3.2 Objetivos específicos.

1. Diagnosticar la infraestructura de red existente en el ministerio.
2. Instalar la herramienta Nagios para ser configurado como sistema de monitoreo que identifique y reporte las fallas de infraestructura de red instantáneamente.
3. Realizar pruebas controladas de la infraestructura de red con el software de monitoreo, para analizar su comportamiento en tiempo real.



CAPITULO II

2.1 Fundamentos de la base teórica

2.1.1 Software Libre

Es un programa informático que puede ser descargado desde cualquier sitio web, por lo general la adquisición de dicho software no requiere ningún costo. Según la definición de Wayner (2001, p.17) “permite a los usuarios modificar el programa y distribuir sus propias versiones. Y sobre todo obliga a compartir todo el código fuente, más que controlar o consentir”.

2.1.2 Características

Entre las características planteadas por los autores Hernández, Jiménez, González Barahona, Seoane Pascual, & Robles (2008, p.10) menciona:

- 1) Libertad para ejecutar el programa en cualquier sitio, con cualquier propósito y para siempre.
- 2) Libertad para estudiarlo y adaptarlo a nuestras necesidades. Esto exige el acceso al código fuente.
- 3) Libertad de redistribución, de modo que se nos permita colaborar con vecinos y amigos.
- 4) Libertad para mejorar el programa y publicar sus mejoras. Esto también exige el código fuente.

2.1.3 Gestión de red

Es un conjunto de herramientas que permiten la supervisión y control de la red, de forma que los diferentes dispositivos informan de su estado a un host central. De



acuerdo con la definición propuesta por Verón Piquero (2010) son herramientas que monitorean el funcionamiento de máquinas y de los servicios (servidores web, correo, etc.) que tienen instalados para avisar al administrador en caso de fallo.

En otro contexto, el autor Stallings (2005, p.263) menciona “un sistema de gestión de red está diseñado para ver a toda la red como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto y los atributos específicos de cada elemento y enlace conocido por el sistema” ([Véase anexo D](#)).

2.1.4 Monitoreo de red

El monitoreo de red permite tener el panorama de los dispositivos conectados. Romero (2013) menciona que el monitoreo de red es indispensable en la detección de los diferentes tipos de errores y eventos que puedan influir en el desempeño de la red, los elementos más comunes que se monitorean son el ancho de banda, estado físico de las conexiones, alarmas, tráfico de red y servicios (web, correo, etc.).

2.1.5 Protocolo Simple de Gestión de Red

El protocolo simple de gestión de red (SNMP) forma parte de los protocolos del nivel de aplicación del modelo TCP/IP. La conceptualización de Valdivia (2005) refiere a la arquitectura cliente-servidor para proporcionar funciones de monitorización de red mediante la búsqueda y resolución de problemas y la planeación del crecimiento de la red.

SNMP se utiliza sobre todo para supervisar dispositivos de red: conmutadores, enrutadores, servidores y equipos de escritorio. La información se envía con unos parámetros estandarizados para que los fabricantes puedan implementar este protocolo en sus dispositivos con la finalidad de efectuar el monitoreo de los equipos de red a través del protocolo SNMP que define dos elementos claves:



- NMS (network management station): son los equipos encargados de la supervisión.
- Agentes SNMP: es el componente software instalado en los equipos que se desea monitorizar. Proporcionan la información solicitada por los NMS.

El protocolo funciona por medio de una serie de mensajes, normalmente encapsulados en un paquete UDP. Las operaciones de los mensajes pueden ser de dos tipos: comandos que son operaciones con respuesta, o, notificaciones sin respuesta. SNMP v3, define una cabecera común para todos los mensajes que se envían, precedida por la Unidad de Datos de Protocolo (PDU) donde se codifican los datos del mensaje SNMP.



Ilustración 1: Mensaje Sntp

Fuente Jorquera (2010)

2.2 Metodología

2.2.1 Entorno de Red

El Entorno de red comúnmente empleado es el modelo de referencia del estándar OSI llamado OSI Environment (OSIE), es un marco de trabajo que considera diversos aspectos relacionados con la gestión de redes, incluyendo la gestión de elementos tan dispares como dispositivos de red, aplicaciones, servicios, protocolos o los propios usuarios y administradores del sistema. Trabaja con cuatro sub-modelos bien diferenciados que ayudan a desarrollar de forma separada y ordenada un sistema.

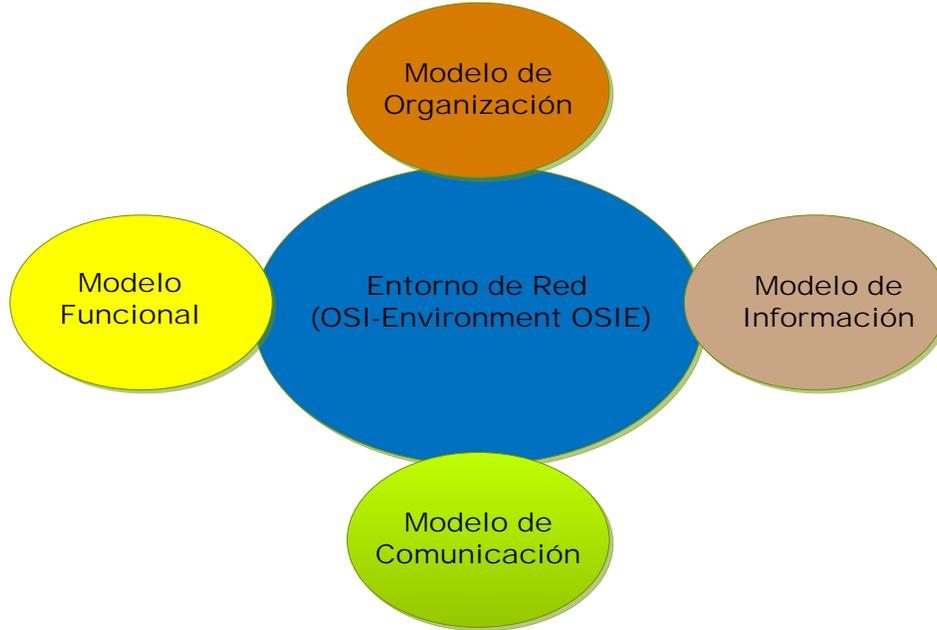


Ilustración 2: Sub-Sistemas del entorno de red OSIE

Fuente: Elaboración Propia (2015).

2.2.2 Modelo de Organización

Se describen los componentes que conforman la red los elementos a administrar, el conjunto de gestores y agentes y la relación entre estos. Al grupo de dispositivos que conforman el sistema de red y las comunicaciones que los interconecta se les denomina Entorno de Gestión (OSI Environment - OSIE). A los responsables de la gestión del sistema se les llama Entidades (System Management Application – Entity SMAE), el ultimo integrante del modelo de organización son los protocolos de red (Network Protocols - NP).

2.2.3 Modelo de Información

El sistema de gestión de redes es en sí un sistema distribuido y la información que gestiona también se distribuye entre los distintos elementos que conforman el sistema. Por ello cada una de las entidades que conforman el sistema de gestión



tendrá asociada una Base de Información de Gestión (Management Information Base – MIB). Dentro de cada dispositivo a gestionar se pueden distinguir diferentes Objetos de Gestión (Management Object - MO), cada uno de estos objetos representa un elemento de la realidad, abstrayéndonos de los detalles reales que existen en los sistemas que se gestionan, ofreciendo una visión unificada de los objetos reales.

La agrupación de todos los Objetos de Gestión conforma el MIB de la entidad. El MIB no es una base de datos al uso, que almacena y gestiona los datos que contiene, es una representación formal de los datos de gestión que virtualmente asocia un objeto del MIB a un objeto de la realidad.

De esta forma un objeto del MIB podría ser el estado de un dispositivo (Apagado o Encendido), Aplicaciones, Servicios, Usuarios, Equipos, NIC'S, Unidades de Almacenamiento, Sistemas de Archivos, Datos, Dominios.

2.2.4 Modelo de Comunicación

En el modelo de comunicaciones se definen los procesos y protocolos de comunicación utilizados por las entidades del sistema, existen tres tipos de protocolos: el de gestión, descubrimiento y los de transporte. El entorno de red OSIE, utiliza el Protocolo Simple de Gestión de Red, SNMP.

2.2.5 Modelo Funcional

A este modelo se le conoce normalmente por el acrónimo de FCAPS (Fault, Configuration, Accounting, Performance, Security). Este modelo describe cinco áreas en las que tradicionalmente se ha dividido la gestión de la red: gestión de fallos, gestión de configuración, gestión de prestaciones, gestión de contabilidad, gestión de seguridad.



El autor Jorquera (2010) indica el funcionamiento de las áreas:

1. Gestión de Fallos:

Tiene como objetivo la detección, aislamiento, corrección y registro de operaciones anormales que ocurren en el sistema. Determinar el máximo de información posible sobre los fallos es un elemento fundamental para la buena gestión. Por ello el sistema de gestión de fallos está asociado con la monitorización de los elementos del sistema, para detectar un cambio en el estado de alguno de ellos.

Otro aspecto importante a contemplar es el análisis de tendencias para poder predecir errores e intentar garantizar que la red siempre está disponible. Cuando una entidad de gestión detecta un fallo en un componente esta enviara una notificación a una entidad de control para que, en la medida de lo posible, realice las acciones pertinentes que solventen dicho fallo.

En función de la notificación recibida la entidad de control identificara el fallo producido. Es posible que un mismo fallo produzca múltiples notificaciones provenientes de entidades de gestión distintas. Es por ello que la entidad de control deberá realizar un proceso de correlación que permita asociar notificaciones relacionadas con un mismo fallo.

Una vez correlacionadas las notificaciones la entidad de control podrá tener una hipótesis del fallo producido. A partir de ese momento podrá realizar pruebas de localización para obtener más información sobre el fallo. Finalmente, localizado el fallo, la entidad de control podrá realizar las acciones correctivas pertinentes y posteriormente validar la corrección.



Ilustración 3: Proceso de Gestión de Fallas

Fuente: Elaboración Propia (2015).

2. Gestión de la Configuración

Es un conjunto de facilidades que permiten controlar, identificar, recoger y proporcionar datos de configuración a elementos gestionados. Entre las tareas relacionadas se pueden destacar la definición de información de configuración en los recursos, la modificación de las propiedades de los recursos, la definición y modificación de relaciones entre los recursos, la inicialización y terminación de servicios en red o bien la distribución de software.

Todos los cambios de hardware y software son coordinados a través de este proceso incluido la instalación de nuevas aplicaciones o equipamiento, la modificación de sistemas existentes y la eliminación de sistemas y programas obsoletos.

Según las redes incrementan su tamaño, una tarea importante es la configuración automatizada. Mediante la automatización se intenta minimizar la relación del sistema de gestión con los administradores, de forma que las tareas de administración se realicen con altos grados de autogestión.



3. Gestión de Cuentas

La tarificación o gestión de cuentas son un conjunto de procedimientos que permiten medir y gestionar el uso de determinados elementos e identificar costes por el uso de estos. El objetivo es reunir estadísticas sobre usuarios y otros elementos del sistema y su relación que el consumo de recursos que realizan: utilización de disco, consumo de memoria, tiempo de CPU, conexiones, etc.

En esta área se engloban también las operaciones de gestión de usuarios (usuarios, contraseñas y permisos) operaciones sobre equipos, servicios como realizar copias de seguridad, la sincronización y labores de inventario.

4. Gestión de Rendimiento

La gestión de rendimiento hace referencia al conjunto de procedimientos dedicado a evaluar el comportamiento de elementos gestionados y la efectividad de determinadas actividades. Entre los indicadores de prestaciones se pueden definir los que están orientados al servicio, como la disponibilidad, el tiempo de respuesta, y la fiabilidad. En cambio, otros indicadores están orientados a la eficiencia o al grado de utilización.

La gestión del rendimiento permite a los administradores planificar la red para el futuro, así como determinar la eficiencia de la red actual, en relación con las inversiones realizadas para establecerla. Algunos parámetros de red que se miden en la gestión del rendimiento son el porcentaje de utilización, las tasas de error y los tiempos de respuesta. Recolectando y analizando estos datos se pueden detectar problemas o tendencias de capacidad o fiabilidad y a que servicios está afectando.



5. Gestión de Seguridad.

Está relacionada con todos los elementos asociados a la seguridad en los recursos de red: generación, distribución y almacenamiento de claves de cifrado, información de usuarios y contraseñas, control de acceso y autorización. La gestión de seguridad no hace referencia a la propia seguridad del sistema de gestión, si no a la seguridad de los sistemas que gestiona.

En esta área se proporciona facilidades para incorporar mecanismos de seguridad contra los ataques a las comunicaciones, como protección contra interrupción del servicio, captura no autorizada de información, modificación de información o suplantación de identidad.



2.3 Herramientas

2.3.1 Nagios

Nagios es un potente sistema de monitoreo que permite a las organizaciones identificar y resolver problemas de infraestructura de TI antes que ellos afecten los procesos de negocios críticos. Diseñado con escalabilidad y flexibilidad, es una herramienta potente que permite detectar y reparar problemas, mitigar eventos futuros antes que afecten al usuario final y clientes. (NAGIOS CORE 4.1.1 (Nagios), 2015).

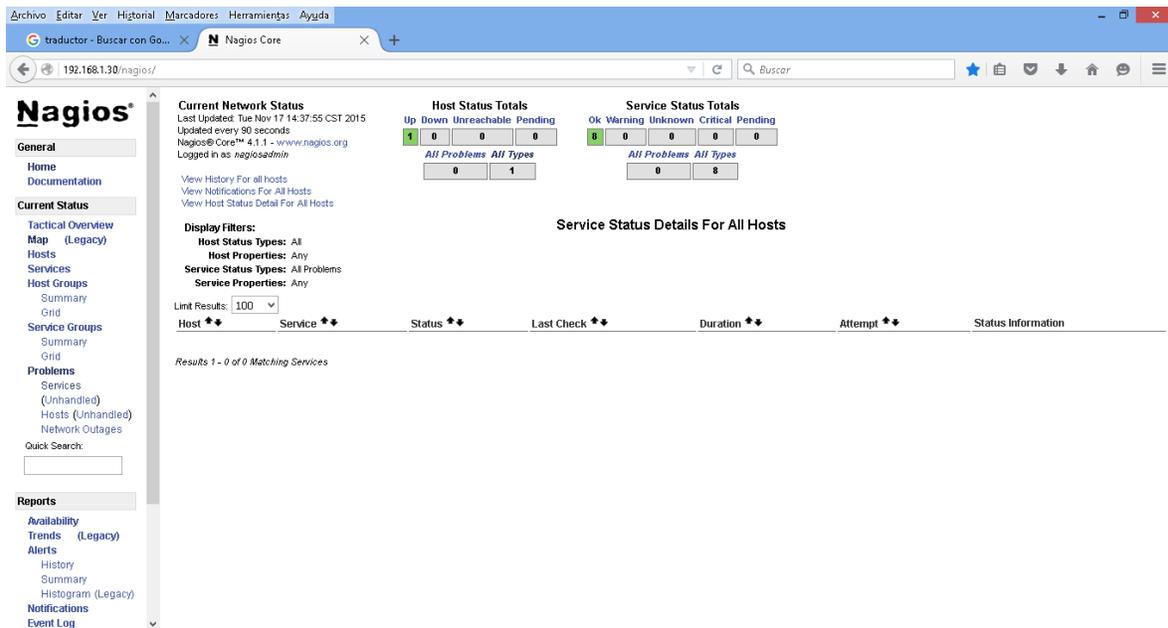


Ilustración 4: Interfaz de Nagios.

Fuente: Elaboración Propia (2015).



2.3.2 Cacti

Cacti es una interfaz completa que trabaja con una base de datos que maneja planificaciones según Round-Robin (Round Robin Database Tool - RRDtool), almacena toda la información necesaria para crear gráficos y rellenar con los datos en una base de datos MySQL. Permite escalar a un gran número de fuentes de datos y gráficos mediante el uso de plantillas; gracias a la creación de un único gráfico y el sondeo la información sobre la adición de un nuevo huésped. ((CACTI), 2015).

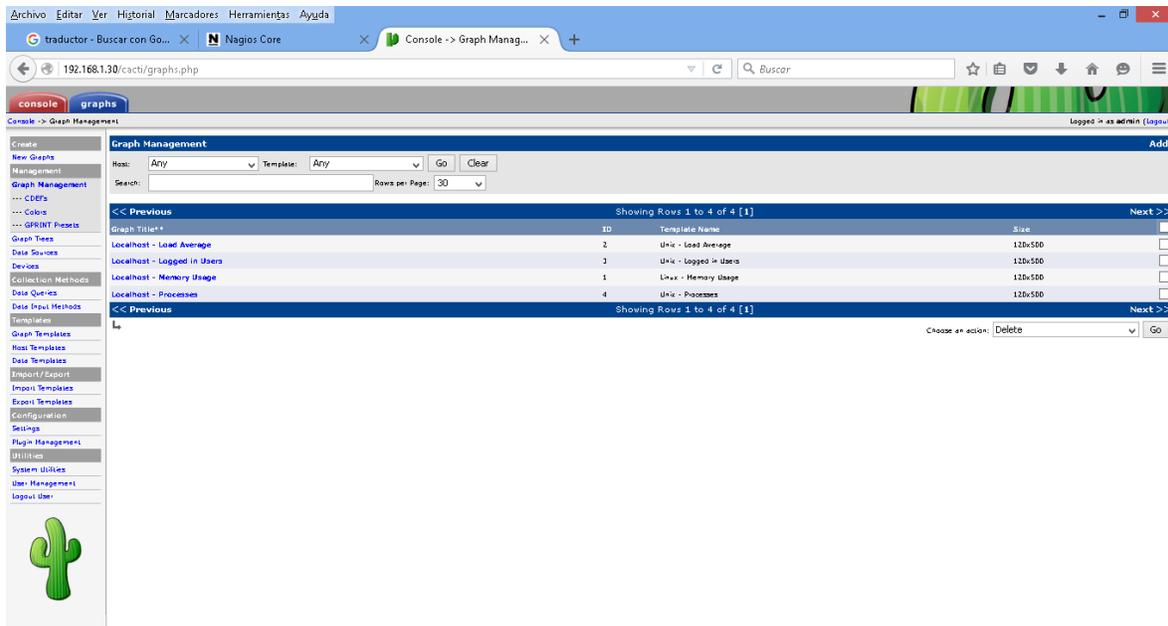


Ilustración 5: Interfaz de Cacti.

Fuente: Elaboración Propia (2015).



CAPITULO III

3.1 Desarrollo

3.1.1 Diseño Operativo.

En función del cumplimiento de los objetivos planteados, se realizó un esquema de investigación que consta de cuatro fases, a continuación se presenta la descripción del diseño operativo del proyecto.

Fase I: Diagnostico

Se aplicaron técnicas de investigación acordes a las necesidades del proyecto. Rojas Soriano (2006) señala a las técnicas de investigación como herramientas metodológicas, que permiten estructurar los procesos de esta, es decir dirigen las actividades mentales y prácticas, hacia la consecución de los objetivos formulados.

Las técnicas de recolección de información primarias, se utilizan en trabajos de pequeña envergadura, compuestas por las siguientes herramientas (observación, entrevista o cuestionario). También se utilizaron las técnicas de recolección de información secundaria, implementadas en investigaciones de carácter científico, donde se recopila información valiosa para un análisis metodológico, estadístico descriptivo e inferencial. A continuación se mencionan los instrumentos de recopilación de datos utilizados: (Otras Investigaciones, Revistas Científicas, Datos Internacionales, Información en Internet, Fuentes Internas).

Fase II: Factibilidad

Factibilidad es la posibilidad de que suceda un evento, de acuerdo con los autores Kendall & Kendall (2005), la definición de factibilidad para un proyecto de Tecnologías de la Información, va mucho más allá del uso común del término. La



factibilidad está valorada en tres formas principales; operacionales, técnicas y económicas. En este trabajo investigativo solo se hará hincapié a dos de ellas, (factibilidad técnica o tecnológica y la factibilidad operativa), debido a que las herramientas de evaluación son de código abierto.

La factibilidad técnica o tecnológica, hace referencia a las necesidades tecnológicas (hardware y software) del proyecto.

Si los sistemas existentes no pueden ser añadidos, la siguiente pregunta es si hay la tecnología existente para satisfacer las especificaciones. Si la respuesta sobre si una tecnología en particular se encuentra disponible y es capaz de satisfacer las peticiones del usuario es "sí", entonces la pregunta se convierte en económica. (Kendall & Kendall, 2005. pp.51)

La factibilidad operativa depende de las capacidades de los recursos humanos con los que se dispone para el proyecto, Kendall & Kendall (2005), opinan que al evaluar la factibilidad operacional, con mucha frecuencia hay que usar el arte de adivinar.

En este sentido la factibilidad operativa estará definida, por la destreza de los autores en labores de configuración y administración del software de monitoreo.

Fase III: Diseño

Esta fase es de vital importancia para el desarrollo de este proyecto. Se pretende crear una máquina virtual con la herramienta VMware vCenter Server V 5.5.0, con las siguientes características: 80 Gb de Disco Duro virtual, Memoria RAM de 4 Gb y 2 CPUs. Con el objetivo de instalar el sistema operativo Linux Debian-8.1.0-amd64 e instalar el software de monitoreo.



Fase IV: Implementación

En esta última fase se procederá a realizar la implementación del software de monitoreo en un entorno de red real, es decir, se monitoreara todos los segmentos de red a nivel nacional del MEFCCA. Se elegirán algunos segmentos de red para este experimento.

Documentar el comportamiento del software, para ofrecer al Área de Informática, recomendaciones y conclusiones acerca de este trabajo.



3.1.2 Plan de Actividades

En el cuadro 1, se mencionan las actividades que se llevaron a cabo en el desarrollo del trabajo, este permitirá ordenar y sistematizar la información relevante para desarrollar la investigación.

| Nombre de tarea | Duración | Comienzo | Fin |
|---|----------------|-----------------------|-----------------------|
| FASE DIAGNOSTICO | 22 días | lun 24/08/2015 | lun 14/09/2015 |
| Investigar antecedentes de la infraestructura de red del MEFCCA | 9 días | lun 24/08/2015 | mar 01/09/2015 |
| Visita a la institución | 2 días | Mie 02/09/2015 | Jue 03/09/2015 |
| Entrevista con el administrador de red | 1 día | vie 04/09/2015 | vie 04/09/2015 |
| Investigar programas de monitoreo | 5 días | sab 05/09/2015 | mie 09/09/2015 |
| Encuesta a los encargados del área de informática | 1 día | jue 10/09/2015 | jue 10/09/2015 |
| Identificar los requerimientos del programa | 4 días | vie 11/09/2015 | lun 14/09/2015 |
| FASE FACTIBILIDAD | 22 días | mar 15/09/2015 | mar 22/09/2015 |
| Factibilidad Técnica | 11 días | mar 15/09/2015 | vie 25/09/2015 |
| Factibilidad Operativa | 11 días | sab 26/09/2015 | mar 06/10/2015 |
| FASE DISEÑO | 36 días | mie 07/10/2015 | mie 11/11/2015 |
| Instalación y configuración de participación del sistema operativo GNU/Linux Debian-8.1.0-amd64 | 7 días | mie 07/10/2015 | mar 13/10/2015 |
| Instalación y configuración de software de monitoreo de red | 29 días | mie 14/10/2015 | mie 11/11/2015 |
| FASE IMPLEMENTACION | 9 días | jue 12/11/2015 | vie 20/11/2015 |
| Evaluación en ambiente real | 9 días | jue 12/11/2015 | vie 20/11/2015 |

Tabla 1: Plan de Actividades.

Fuente: Elaboración Propia (2015).



3.1.3 Diagrama de Gantt

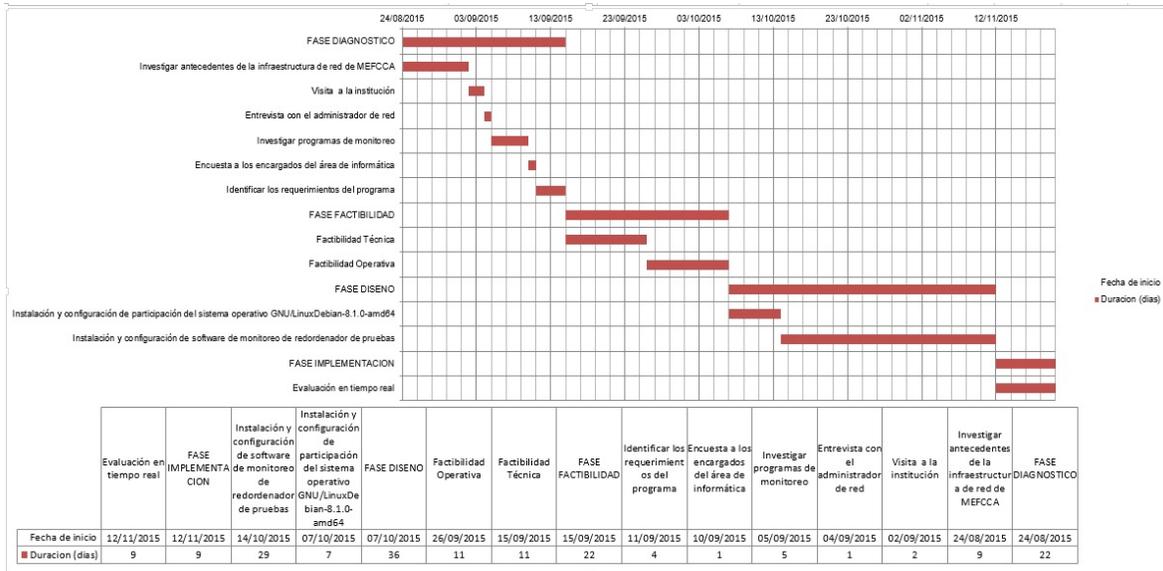


Ilustración 6: Diagrama de Gantt.

Fuente: Elaboración Propia (2015).



3.1.4 Topología de red MEFCCA

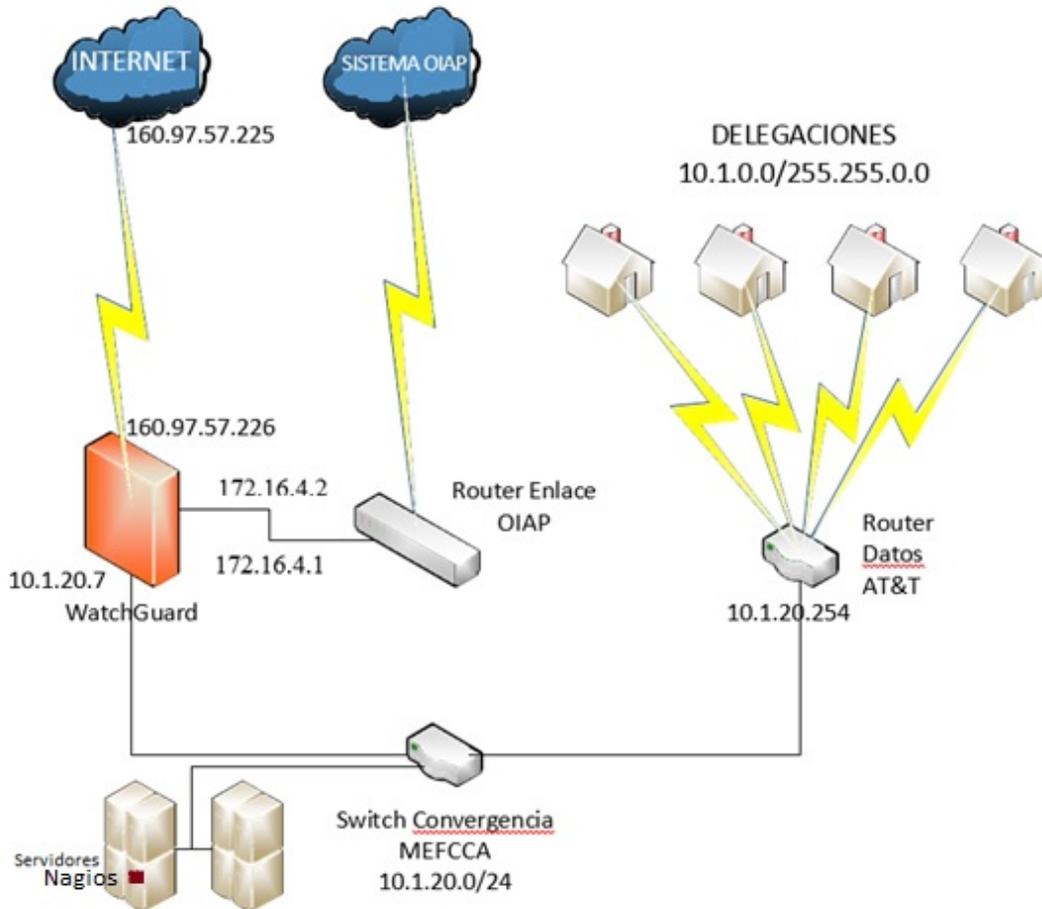


Ilustración 7: Topología de Red MEFCCA

Fuente: Elaboración Propia (2015).

Esta imagen describe la topología de red del Ministerio de Economía Familiar, Comunitaria, cooperativa y Asociativa. A como se puede apreciar. El router OIAP es que utilizamos para establecer el enlace entre el Ministerio y la empresa OIAP. El Router de datos AT&T es el que nos permite establecer enlace de datos de delegación a delegación. El equipo llamado WatchGuard funciona como Firewall y sistema de detección de intrusos (IDS- Intrusion Detection System) y por último y no menos importante tenemos el Switch de Convergencia MEFCCA, este es utilizado interconectar el Data Store (lugar donde se almacenan virtualizados los servidores), las delegaciones y el WatchGuard.



La interconexión que hay entre el WatchGuard, Router OIAP, Switch de Convergencia, Data Store y Router de datos de AT&T es mediante cable UTP. Las conexiones hacia el exterior que tiene el WatchGuard, Router OIAP, Router de Datos AT&T y las Delegaciones departamentales del MEFCCA es mediante Fibra Óptica.

3.2 Fase Diagnóstico

La etapa de diagnóstico está centrada en la búsqueda de información relevante que sirva de insumos para el desarrollo del tema, se realizaron las siguientes actividades:

Investigación de los antecedentes de la red de datos, mediante llamadas, correos electrónicos, accediendo a los sitios web de la institución y visitas al área de informática, en esta última se acordaron las fechas para desarrollar los instrumentos de recolección de información; Encuesta y Entrevista.

La entrevista fue dirigida hacia el Administrador de la red del MEFCCA, dicha herramienta estaba compuesta por catorce preguntas, obteniendo datos muy relevantes:

1. El área de informática tiene treinta servidores con discos duros divididos en dos particiones, una de cincuenta gigas para sistema operativo y programas y otra de cien gigas para respaldos, Memoria RAM cuatro gigas, dos procesadores de dos puntos cinco giga Hertz, virtualizados en VMware vSphere, centralizados en un cuarto de servidores ubicados en un Centro de Datos con climatización y seguridad.
2. Existen novecientos usuarios en la institución, el área de informática supervisa la red hasta que un usuario alerta fallas en la red al área encargada.



3. En el año dos mil catorce se implementó un software de monitoreo en modo demo Solar Wind pero no se adquirió por sus alto costo.
4. La institución ha estado presentando caídas en sus enlaces de datos en los últimos dos meses. No tienen un software de monitoreo de red, a causa del vencimiento de licencia e inversión económica que representa la adquisición de software privativo después del tiempo de prueba. El ministerio estaría dispuesto a implementar un software de monitoreo siempre y cuando este no incurra en costos adicionales.
5. La red está segmentada por delegación.



3.2.1 Reportes de fallas en enlace de datos

Hoja de reporte de enlace caído, elaborado por el proveedor de servicio de internet y enviado al responsable del área de redes del MEFCCA.



Ilustración 8: Reporte Falla de enlace de Red MEFCCA

Fuente: AT & T (2015).



Posteriormente se investigaron programas de monitoreo con licencia Software Libre, se eligió dos software de monitoreo, la elección estuvo basada en recomendaciones del asesor informático Ingeniero Gerald Martin Lanzas Garay.

Se realizaron a su vez otra entrevista semi-estructurada al área de informática, conformada por un grupo de cuatro personas. El instrumento estaba compuesto por preguntas abiertas, para recopilar la mayor cantidad de información por los entrevistados.

El entrevistado podía escribir sus opiniones que el considerara. A continuación, se muestran los resultados:

- 1) Conocen de aplicaciones de Monitoreo de Red tales como Nagios y Cacti en el área de Informática.
- 2) Se sienten más identificados con el software libre por su gratuidad, fácil resolución de problemas y buena seguridad. Aunque también los entrevistados reconocen que el software propietario es intuitivo para el uso del usuario por el uso frecuente del mismo.
- 3) No hay aplicaciones de Monitoreo de Red predilectas por los encuestados.
- 4) Las características que más le agradan de las aplicaciones de software libre, a nuestros encuestados son, gratuidad, soporte técnico, no necesita antivirus, alternabilidad. Código fuente disponible y uso Fácil.
- 5) Los entrevistados respondieron que han utilizado una de las aplicaciones de estudio, la cual es Cacti, también se mencionó Wireshark y nmap como programa de software libre.
- 6) Los encuestados mencionaron que las características más importantes son, el reporte incidencias inmediatamente, muestre los horarios picos, alerte cuando llegue al 70 % de su capacidad, optimice los recursos de la red, aplicación multiplataforma, Soporte Técnico, Reportes fácil, interfaz gráfica intuitiva, aplicación confiable y flexible, aplicación robusta y que almacene reportes en base de datos.



3.3 Fase Factibilidad

3.3.1 Factibilidad técnica

En el análisis de los datos adquiridos por la (Encuesta Semi-Estructurada), se evidencio que el área de informática conoce las aplicaciones que se proponen como el software de monitoreo de red, para el Área de Informática. Las herramientas de monitoreo: Nagios, Cacti.

Tomando en consideración los resultados arrojados por los encuestados, las principales características técnicas en las aplicaciones de monitoreo de red son:

- Reporte de ancho de banda.
- Manejo de Estadísticas (Muestra Horarios Picos).
- Alertas cuando llega al 70% de su capacidad, mediante SMS, emails, u otros métodos.
- Reportes de fácil entendimiento.
- Consume pocos recursos.
- Interfaz gráfica intuitiva.
- Aplicación confiable y flexible.
- Almacene los reportes en una base de datos.
- Aplicación gratuita.
- Soporte técnico.
- Aplicación robusta.



A continuación, se muestra un cuadro comparativo, entre las aplicaciones y los requisitos técnicos del Área de Informática.

Cuadro Comparativo entre los Requisitos Técnicos y las Herramientas de Monitoreo de red

| Requisitos Técnicos del Área de Informática | Nagios | Cacti |
|---|--------------|-------|
| Reporte de Ancho de Banda | SI | SI |
| Manejo de Estadísticas (muestre Horarios Picos) | SI | NO |
| Alertas cuando llega al 70% de su capacidad, mediante SMS, emails, u otros métodos. | SI | NO |
| Reportes de fácil entendimiento. | SI | SI |
| Interfaz gráfica intuitiva. | SI | SI |
| Aplicación confiable y flexible. | SI | SI |
| Almacene los reportes en una base de datos. | SI (plugins) | SI |
| Aplicación gratuita, GPL | SI | SI |
| Soporte Técnico | SI | NO |
| Aplicación Robusta | SI | NO |

Tabla 2: Cuadro comparativo de Software de Monitoreo

Fuente: Elaboración Propia (2015).

El cuadro comparativo evidencia que el software Cacti, no cumple con cuatro de los diez requerimientos técnicos mencionados por los encuestados. Por otra parte, las herramientas de monitoreo Nagios cumplen con todos los requisitos.



3.3.2 Factibilidad operativa

El software de monitoreo de red, Nagios y Cacti, serán instalados en los servidores del MEFCCA, se especificará una máquina virtual que albergue el sistema operativo Linux para servidores y se configurarán las aplicaciones de monitoreo, para realizar el monitoreo de red del ministerio.

Las características de la máquina virtual son las siguientes:

| Características de Hardware y Software | | | |
|--|-------------|-----------------------------|-------------------------------|
| Disco duro | Memoria RAM | Procesador | Sistema Operativo |
| 80 Giga Byte | 4 Giga Byte | Dos procesadores de 2.5 GHz | Linux Debian 8.1.0 AMD x64 |

Tabla 3: Características del Ordenador de pruebas.

Fuente: Elaboración propia (2015).

Se creará una máquina virtual, para que pueda ser instalada la distribución de Linux, de acuerdo a VMware vCenter Server (Versión 5.5.0) los pasos para crear la máquina virtual son:

Abrir VMware VSphere Client y seleccionamos:

Create a new virtual machine: Permite crear una nueva máquina virtual. En este proceso es posible elegir qué hardware virtual se desea, por ejemplo, cuántos vCPUs, memoria RAM, disco, sistema operativo, entre otros. Posteriormente se debe instalar un sistema operativo y finalmente como mejor práctica instalar también las VMware Tools.

Select a name and Folder

Dar un nombre a la máquina virtual, en este caso nuestro nombre será **redmon**.



Estas son las mejores prácticas con respecto al nombre:

- No usar espacios.
- Crear un estándar para nombrar máquinas virtuales sencillas, que tenga en cuenta el propósito y el ambiente de las mismas.

A continuación, seleccionar un folder. Tener presente que el folder debe ser creado previamente en la vista de “VMs and Templates”.

Nota:

- El máximo número de caracteres soportados en el nombre de una VM son 80.
- No puede haber máquinas virtuales con el mismo nombre en un mismo folder.
- Puede haber dos máquinas virtuales con el mismo nombre en un mismo Datacenter Virtual.
- Puede existir una VM con el mismo nombre de otra, si la segunda se encuentra en otro contenedor, como un folder.

Select a compute resource

Seleccionaremos en dónde ubicar la máquina virtual en un Pool de Recursos llamado **Desarrollo**.

Select Storage

A continuación, seleccionaremos la política de almacenamiento de la máquina virtual “VM Storage Policy” y el datastore VMFS o NFS en donde se almacenará el folder y archivos de la VM.

- VM Storage Policy: Permite definir en qué almacenamiento deberá correr la máquina virtual.
- Name: Seleccionar el datastore en donde se desea almacenar el folder y archivos de la máquina virtual.



Select Compatibility

El Hardware Virtual de una VM se puede definir como aquellos componentes de software que realizan funciones similares a los componentes de hardware físico. VMware a través de los años ha trabajado con distintas versiones de Hardware Virtual. El Hardware Virtual define qué características tendrá la máquina virtual en cuanto a procesamiento, RAM, video, USB, discos, etc.

VMware recomienda trabajar con la última versión de Hardware Virtual, la cual en la vSphere 5.5 es el número 10. Esta versión proporciona el mejor desempeño y soporta de las últimas características de vSphere, tales como soporte de SATA (AHCI), discos virtuales de hasta 62TB de tamaño, soporte para vGPUs de AMD e Intel, entre otras.

Las opciones que se podrán encontrar durante la creación de la máquina virtual son:

- ESX/ESXi 3.5 and later: Seleccionar esta opción si se desea crear una VM con versión de Hardware Virtual 4. Los Hypervisors soportados con esta versión son 3.5, 4.0, 4.1, 5.0, 5.1 y 5.5.
- ESX/ESXi 4.0 and later. Seleccionar esta opción si se desea crear una VM con versión de Hardware Virtual 7. Los Hypervisors soportados con esta versión son 4.0, 4.1, 5.0, 5.1 y 5.5.
- ESXi 5.0 and later: Seleccionar esta opción si se desea crear una VM con versión de Hardware Virtual 8. Los Hypervisors soportados con esta versión son 5.0, 5.1 y 5.5.
- ESXi 5.1 and later: Seleccionar esta opción si se desea crear una VM con versión de Hardware Virtual 9. Los Hypervisors soportados con esta versión son 5.1 y 5.5.
- ESXi 5.5 and later: Seleccionar esta opción si se desea crear una VM con versión de Hardware Virtual 10. A la fecha el único Hypervisors soportado es 5.5.

Select Guest OS

En este punto del Wizard es posible definir qué sistema operativo y versión se instalará en la máquina virtual en nuestro caso usaremos Linux Debian 8.1.0 AMD x64. Con base en esta elección, VMware elegirá algunas configuraciones, como el



adaptador de almacenamiento virtual (Bus Logic Parallel, LSI Logic Parallel, LSI Logic SAS y VMware Paravirtual).

Customize hardware

Este es el paso final. Se podrá configurar el Hardware Virtual de la VM, tales como:

CPU

- CPU: Aquí se define el número de sockets virtuales (Number of virtual sockets).
- Cores per socket: El número de cores por socket.

Memoria

- RAM: Configurar qué memoria será aprovisionada para esta máquina virtual.

El tamaño máximo de RAM de una máquina virtual está dado por la versión de hardware virtual. Por ejemplo, en vSphere 4.1 y hardware virtual 7, es de 256 GB. En vSphere 5.0, 5.1 y 5.5 (virtual hardware versión 8,9 y 10 respectivamente), la memoria máxima es de 1TB.

Nota: Una máquina virtual puede tener más memoria de la que físicamente existe.

- Disco
- New Hard Disk: Tamaño del disco.

En vSphere 5.5, el tamaño máximo del disco es de 62TB. En versiones previas se soporta hasta un tamaño de 2TB.

Nota: No se puede crear un disco virtual más grande que el storage que lo contiene.

- Location: Seleccionar el datastore en dónde se ubicará el disco de la máquina virtual. Es muy recomendable almacenar esto en datastore compartido, permitiendo así la compatibilidad de los servicios distribuidos de VMware.



- Red

En este punto de la creación de la máquina virtual es posible crear el adaptador de red virtual de la VM. Una máquina virtual podrá tener hasta 10 tarjetas de red virtual o vNIC. Las propiedades de red son las siguientes:

- New Network: Elegir el grupo de puertos de máquina virtual para conectar esta VM.
- Adapter Type: Dependiendo del tipo y versión de OS seleccionado para esta máquina virtual, VMware permitirá configurar cualquiera de los siguientes tipos de adaptadores de red virtual:
 1. Flexible (VLANCE o VMXNET)
 2. E1000
 3. E1000E
 4. VMXNET2
 5. VMXNET3
 6. SR-IOV passthrough

El sistema operativo seleccionado fue Debian 8.1.0 AMD x64, lanzada el 08 de junio de 2015, esta distribución fue escogida por los conocimientos y la familiaridad de los autores de este proyecto, con respecto a otras distribuciones.

Las características del sistema operativo Debian 8.1.0 AMD, son:

1. Apache 2.4.10
2. Asterisk 11.13.1
3. GIMP 2.8.14
4. Una versión actualizada del entorno de escritorio GNOME 3.14
5. Colección GNU Compiler 4.9.2
6. Icedove 31.6.0 (una versión de Mozilla Thunderbird sin marca)
7. Iceweasel 31.6.0esr (una versión sin marca de Mozilla Firefox)



8. KDE Plasma Workspaces y KDE Aplicaciones 4.14.2
9. LibreOffice 4.3.3
10. Linux 3.16.7-ckt9
11. MariaDB 10.0.16 y MySQL 5.5.42
12. Nagios 3.5.1
13. OpenJDK 7u75
14. Perl 5.20.2
15. PHP 5.6.7
16. PostgreSQL 9.4.1
17. Python 2.7.9 y 3.4.2
18. Samba 4.1.17
19. Tomcat 7.0.56 y 8.0.14
20. Xen Hypervisor 4.4.1
21. El entorno de escritorio Xfce 4.10

Y otros más de 43.000 paquetes de software listos para usar, construida de casi 20.100 paquetes fuente.

Con esta amplia selección de paquetes y su tradicional apoyo a la arquitectura amplia, Debian se queda una vez más fiel a su objetivo de ser el sistema operativo universal.



3.4 Instalación de herramientas

En esta etapa de nuestro trabajo procederemos a la explicación de cómo es la instalación de Debian, los requerimientos previos a la instalación del software de monitoreo (Nagios y Cacti), para el desarrollo del sistema de monitoreo de red a implementar.

3.4.1 Instalación Debian 8.1.0 AMD x64

1. Iniciamos la instalación de debían seleccionando la opción **Install** y luego presionamos enter para ir al siguiente paso

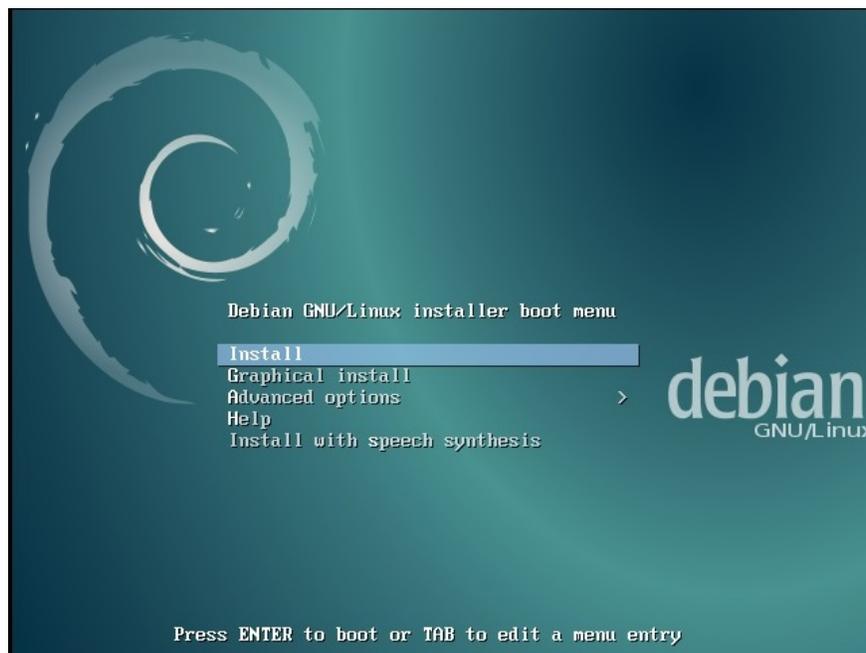


Ilustración 9: Instalación Debian paso 1

Fuente: Elaboración Propia (2015).



2. Seleccionamos el idioma de instalación del Sistema operativo:
Spanish. Presionar la tecla enter para continuar.

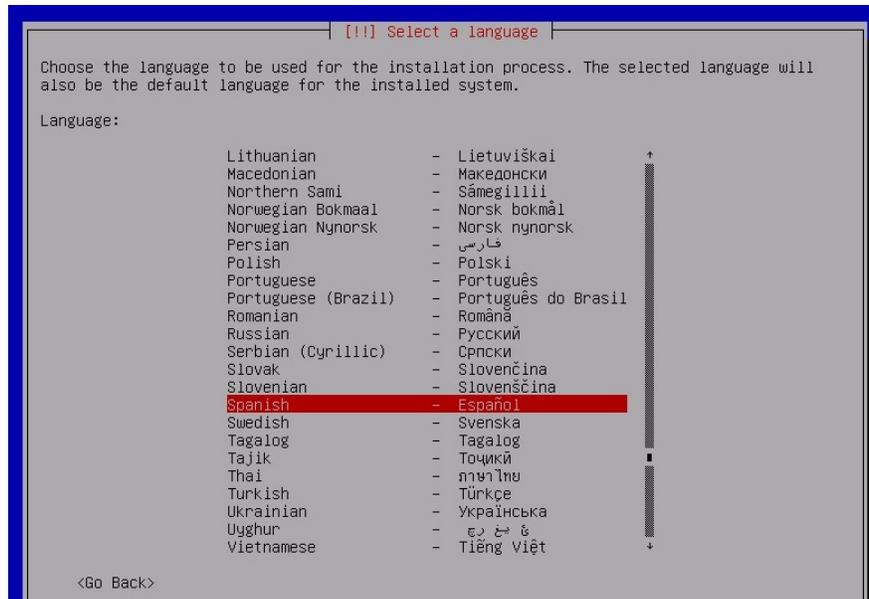


Ilustración 10: Instalación Debian paso 2

Fuente: Elaboración Propia (2015).



3. Seleccionamos nuestra ubicación, **Nicaragua**. Esta se utilizara para fijar la zona horario. Presionar la tecla enter para continuar.

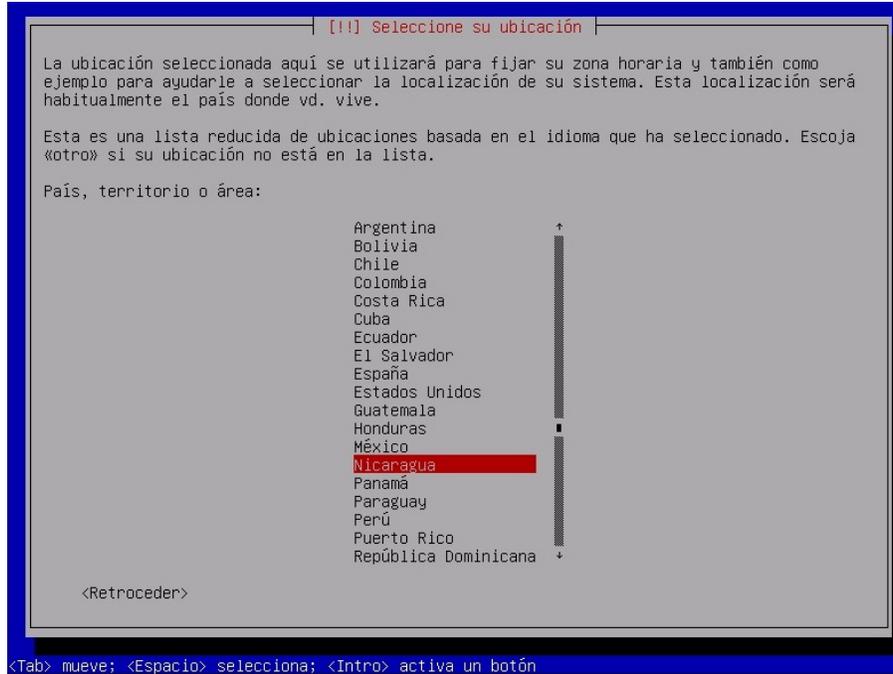


Ilustración 11: Instalación Debian paso 3

Fuente: Elaboración Propia (2015).



4. Elegimos la configuración de nuestro teclado: **Latinoamericano**.
Presionar la tecla enter para continuar.

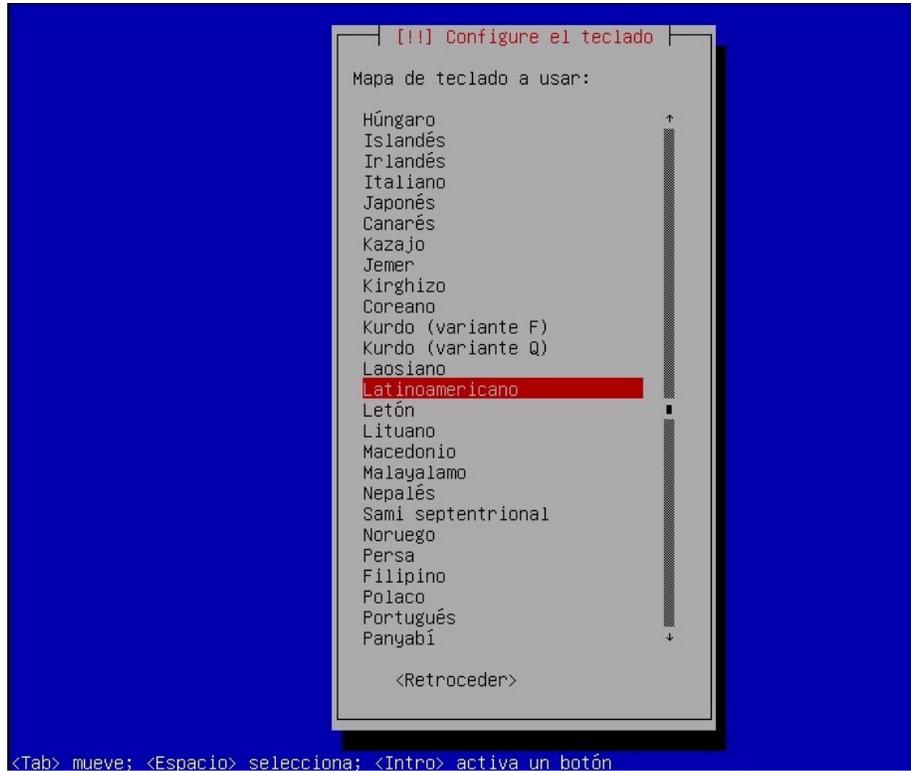


Ilustración 12: Instalación Debian paso 4

Fuente: Elaboración Propia (2015).



5. Seguimos con la configuración de la red. El nombre de la máquina debe de ser una sola palabra que identificara el sistema en la red.

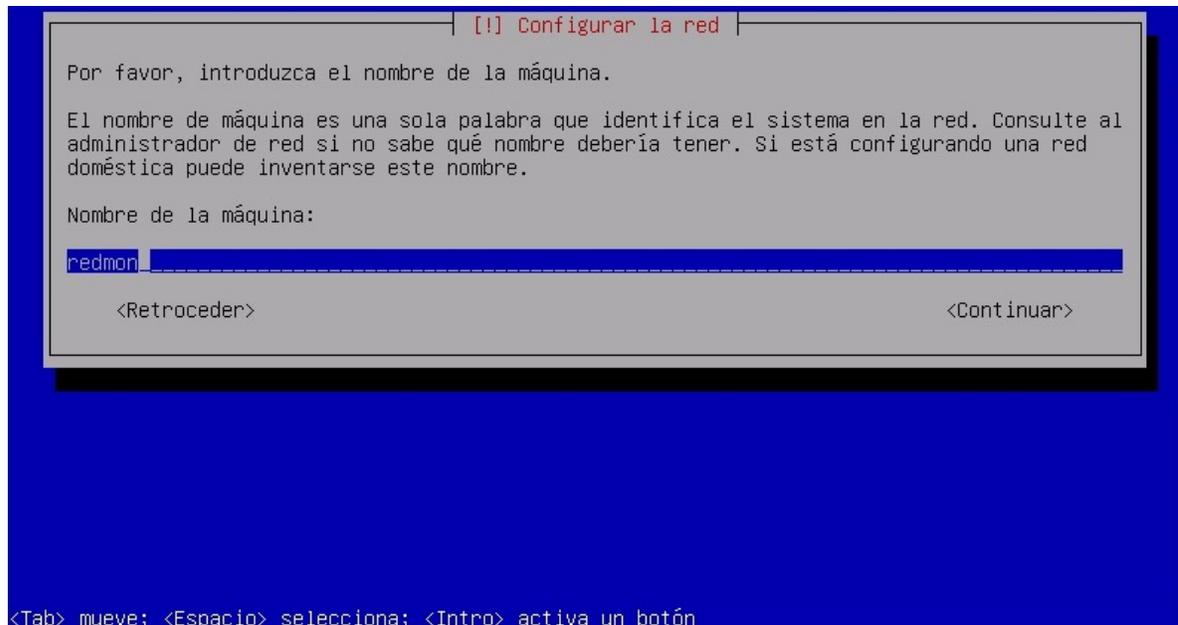


Ilustración 13: Instalación Debian paso 5

Fuente: Elaboración Propia (2015).



6. En este paso escribimos el nombre del dominio de la red

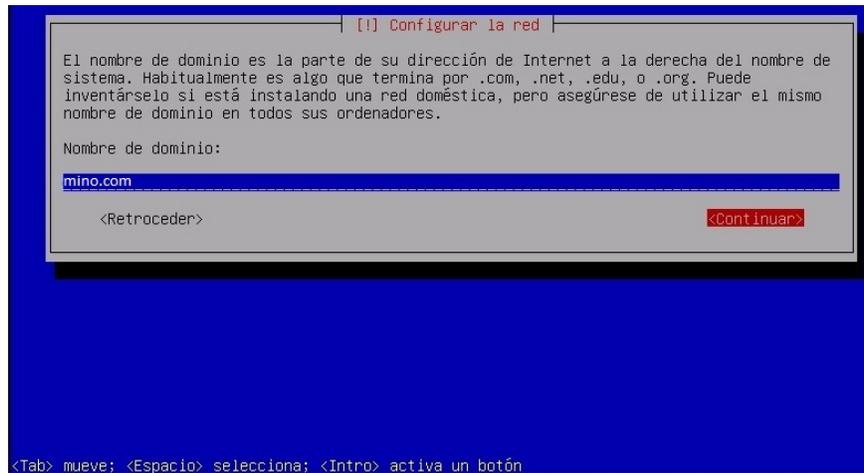


Ilustración 14: Instalación Debian paso 6

Fuente: Elaboración Propia (2015).

7. Módulo de configuración usuarios y contraseñas, Definición de clave para superusuario (root), la cuenta de administración de sistema

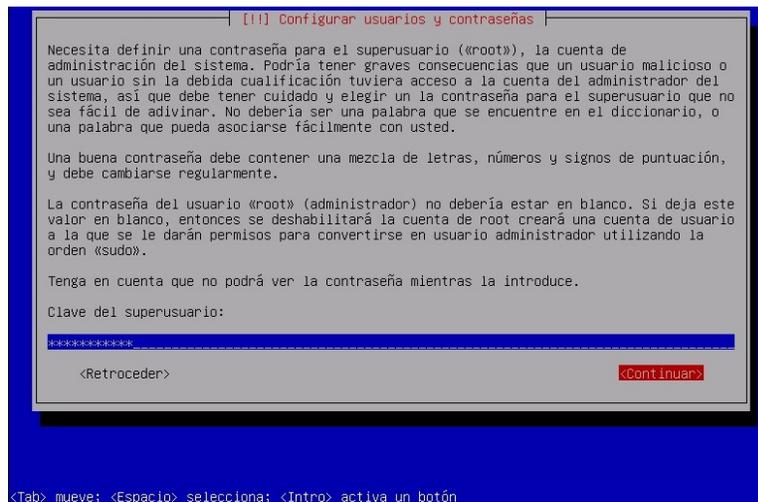


Ilustración 15: Instalación Debian paso 7

Fuente: Elaboración Propia (2015).



8. Validación de la clave de supersuario anteriormente ingresado

[!] Configurar usuarios y contraseñas

Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Ilustración 16: Instalación Debian paso 8

Fuente: Elaboración Propia (2015).

9. Creación de cuenta de usuario para usarse en vez de la cuenta de superusuario en las tareas que no sean administrativas.

[!] Configurar usuarios y contraseñas

Se creará una cuenta de usuario para que la use en vez de la cuenta de superusuario en sus tareas que no sean administrativas.

Por favor, introduzca el nombre real de este usuario. Esta información se usará, por ejemplo, como el origen predeterminado para los correos enviados por el usuario o como fuente de información para los programas que muestren el nombre real del usuario. Su nombre completo es una elección razonable.

Nombre completo para el nuevo usuario:

Max

<Retroceder> <Continuar>

<Tab> mueve; <Espacio> selecciona; <Intro> activa un botón

Ilustración 17: Instalación Debian paso 9

Fuente: Elaboración Propia (2015).



10. Contraseña del usuario

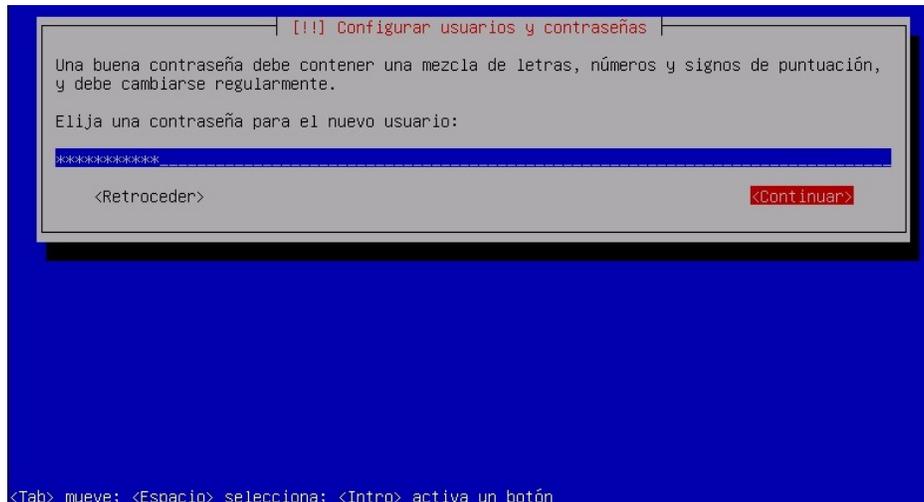


Ilustración 18: Instalación Debian paso 10

Fuente: Elaboración Propia (2015).

11. Confirmación de Contraseña

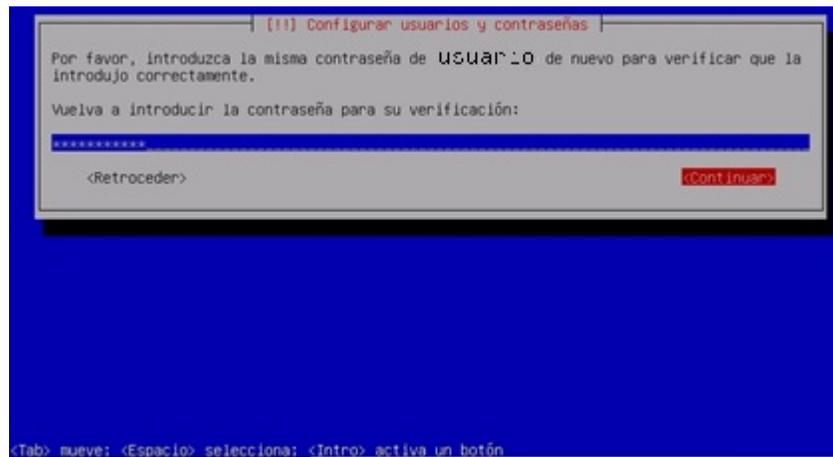


Ilustración 19: Instalación Debian paso 11

Fuente: Elaboración Propia (2015).



12. Particionado de discos. En este paso tenemos el resumen de las particiones y puntos de montajes que tiene configurado actualmente. Elegimos la opción que se aprecia resaltada en pantalla y luego presionamos enter.

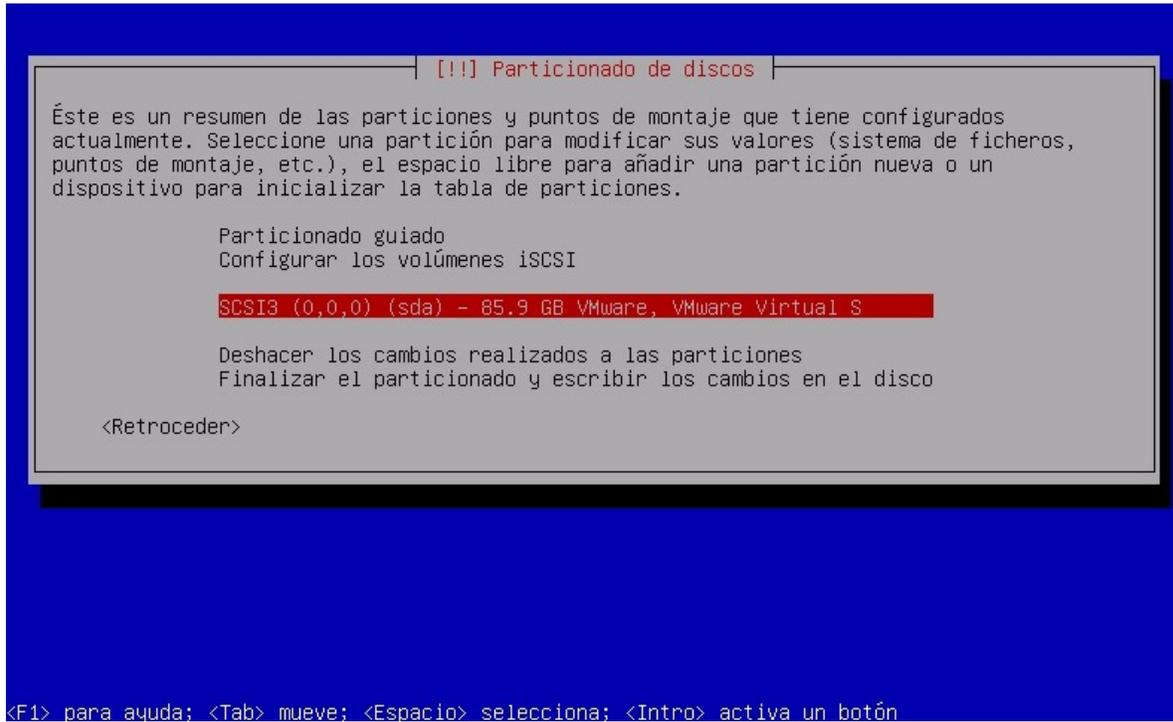


Ilustración 20: Instalación Debian paso 12

Fuente: Elaboración Propia (2015).



13. En esta opción vamos a crear una nueva tabla de partición vacía en este dispositivo.

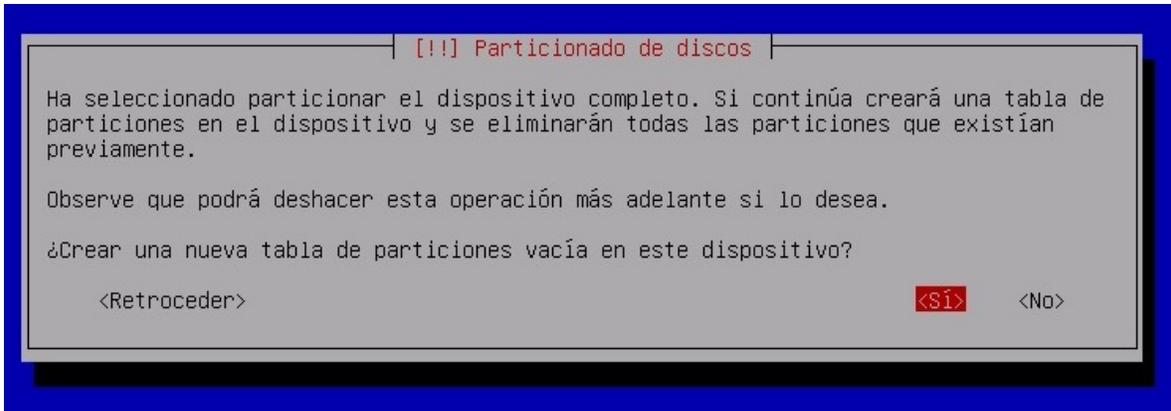


Ilustración 21: Instalación Debian pasó 13

Fuente: Elaboración Propia (2015).

14. En este paso como se muestra en pantalla vamos a seleccionar el espacio libre para añadir las particiones en donde vamos a montar nuestro sistema.

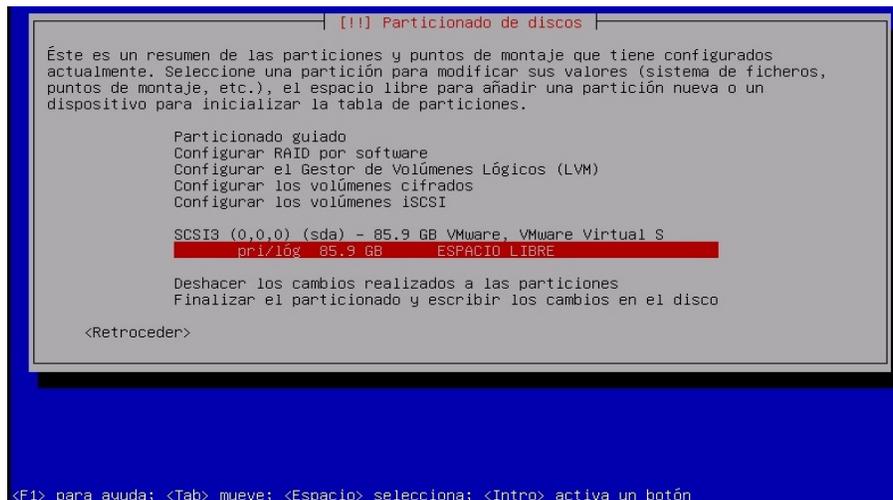


Ilustración 22: Instalación Debian paso 14

Fuente: Elaboración Propia (2015).



15. En la ilustración veintisiete podemos apreciar como quedaran configuradas nuestras particiones para el montaje del sistema operativo que contendrá el sistema de monitoreo de infraestructura de red.

```
[!!] Particionado de discos

Éste es un resumen de las particiones y puntos de montaje que tiene configurados
actualmente. Seleccione una partición para modificar sus valores (sistema de ficheros,
puntos de montaje, etc.), el espacio libre para añadir una partición nueva o un
dispositivo para inicializar la tabla de particiones.

Particionado guiado
Configurar RAID por software
Configurar el Gestor de Volúmenes Lógicos (LVM)
Configurar los volúmenes cifrados
Configurar los volúmenes iSCSI

SCSI3 (0,0,0) (sda) - 85.9 GB VMware, VMware Virtual S
#1 primaria 30.0 GB f ext4 /
#2 primaria 51.9 GB f ext4 /home
#3 primaria 4.0 GB f intercambio intercambio

Deshacer los cambios realizados a las particiones
Finalizar el particionado y escribir los cambios en el disco

<Retroceder>

<F1> para ayuda; <Tab> mueve; <Espacio> selecciona; <Intro> activa un botón
```

Ilustración 23: Instalación Debian paso 15

Fuente: Elaboración Propia (2015).



16. En este paso estamos confirmando las particiones que quedaran definidas en el disco duro.

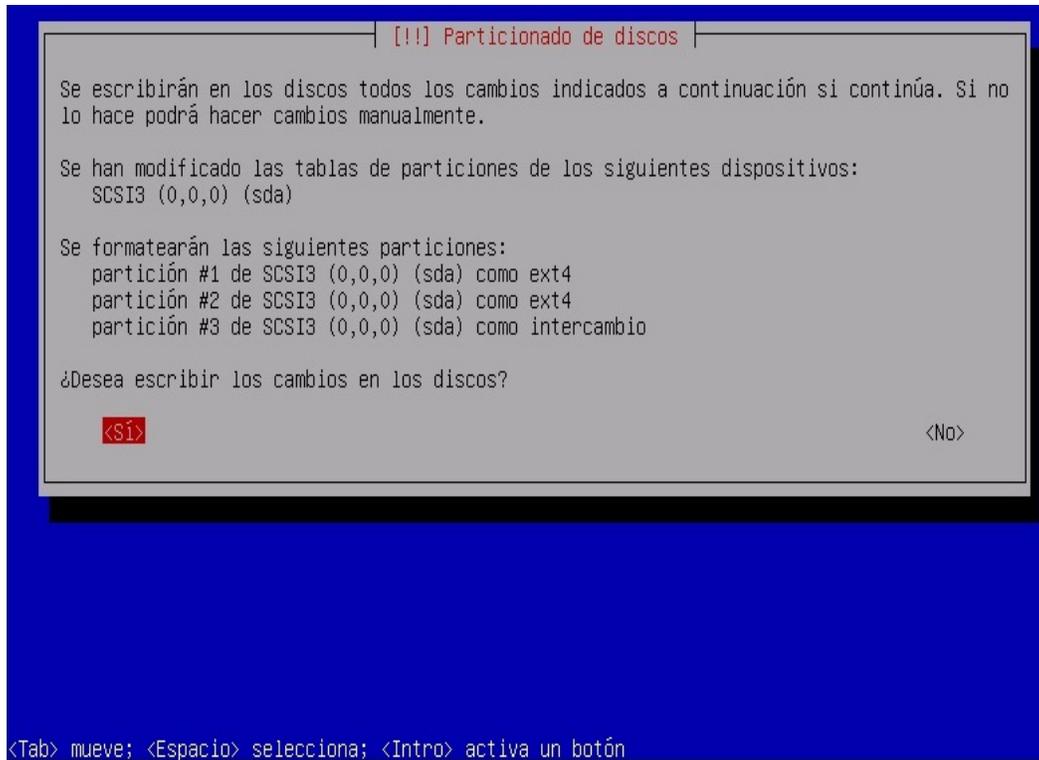


Ilustración 24: Instalación Debian paso 16

Fuente: Elaboración Propia (2015).



17. Selección de programas. Aquí estamos definiendo la instalación de las colecciones predefinidas de programas para adaptar más la instalación de nuestras necesidades. Elegiremos únicamente SSH server y utilidades estándar del sistema.

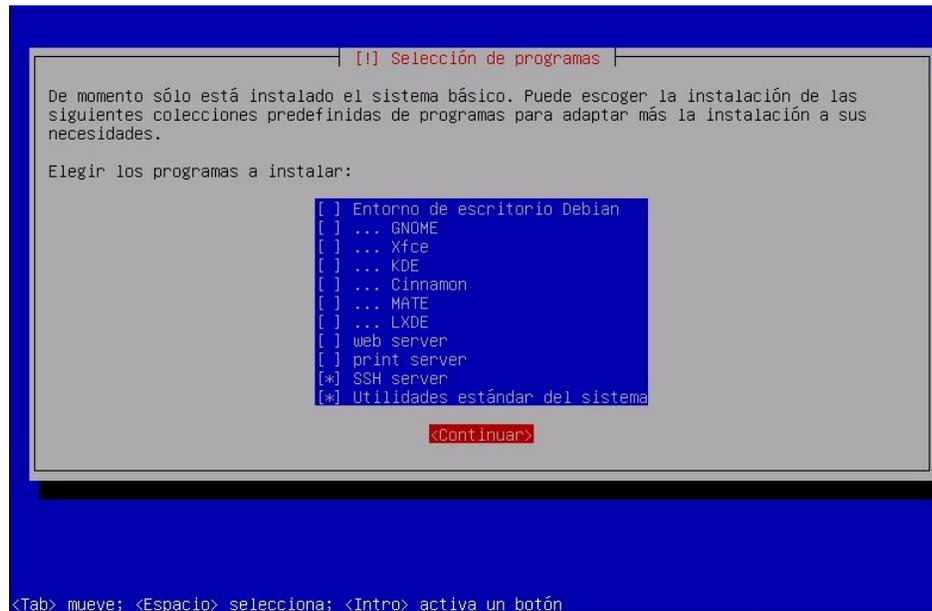


Ilustración 25: Instalación Debian paso 17

Fuente: Elaboración Propia (2015).



18. Este paso es muy importante porque vamos a permitir la instalación del GRUB de arranque.

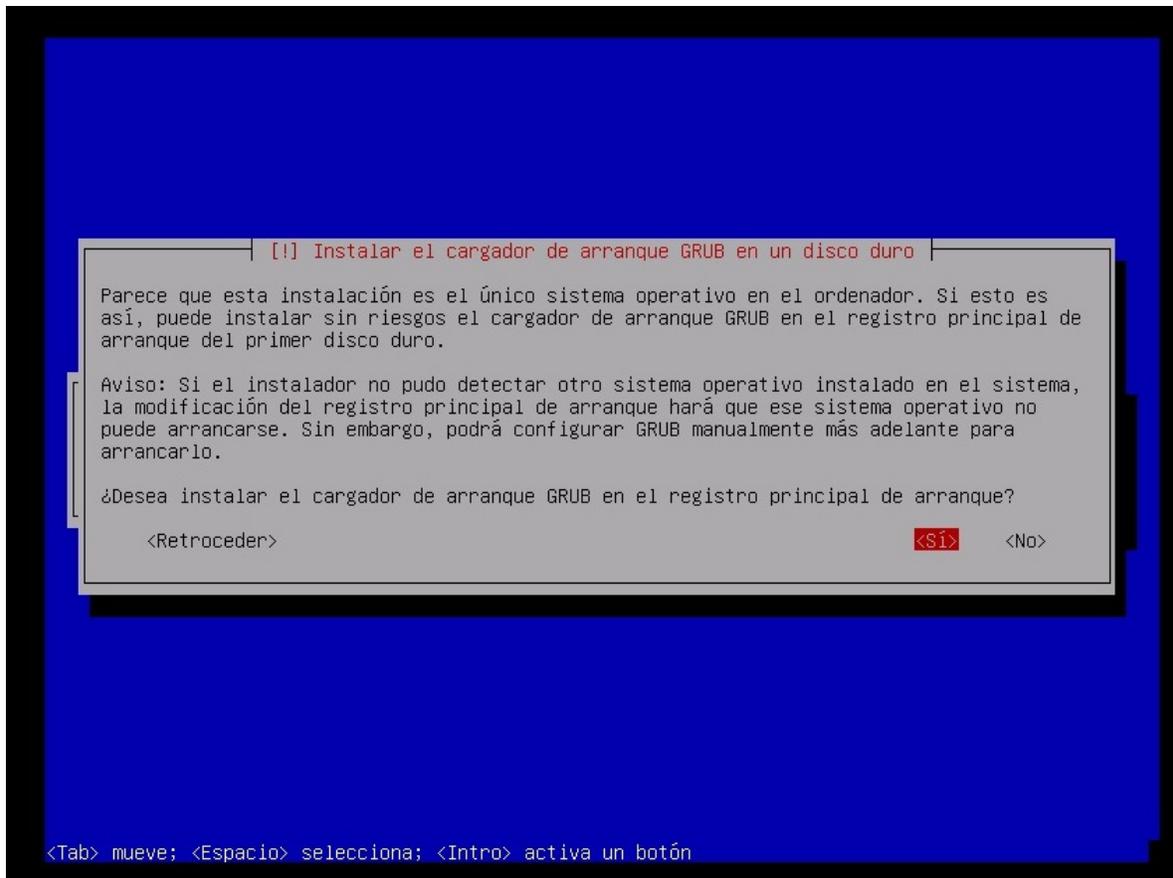


Ilustración 26: Instalación Debain paso 18

Fuente: Elaboración Propia (2015).



19. En la ilustración treinta y uno se muestra el dispositivo donde vamos a instalar el cargador de arranque GRUB.

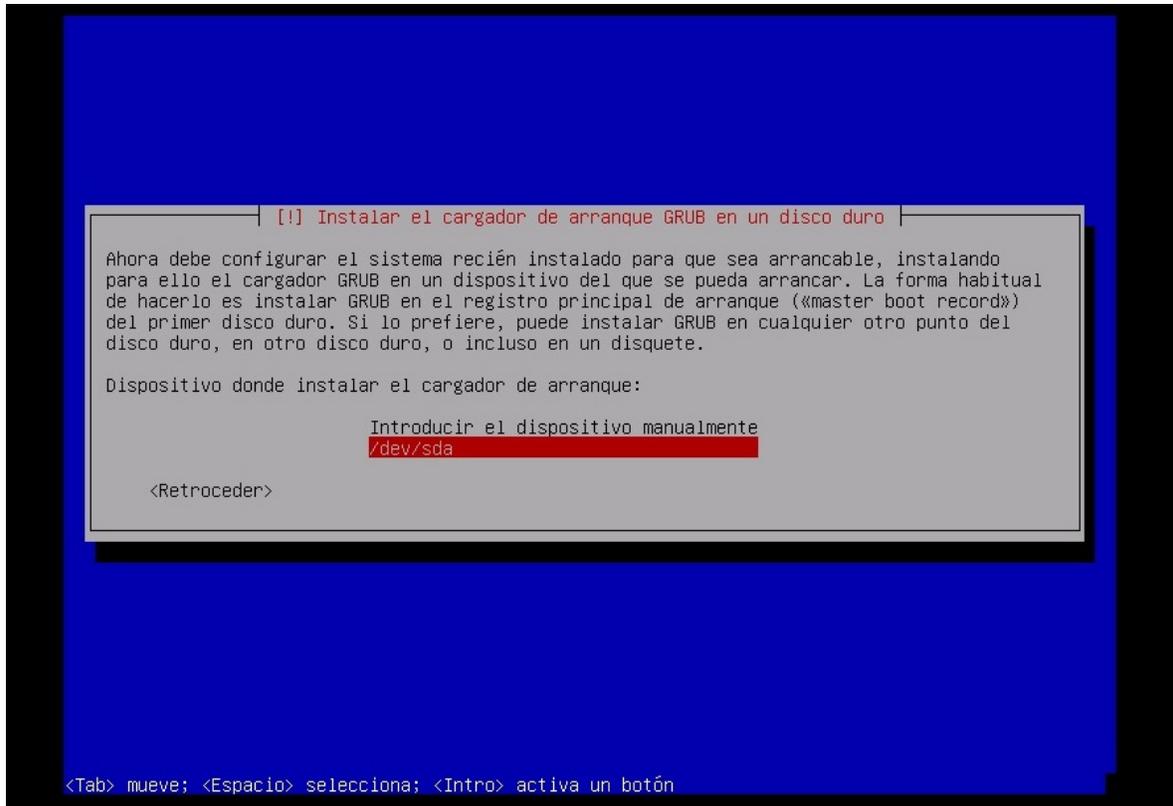


Ilustración 27: Instalación Debian paso 19.

Fuente: Elaboración Propia (2015).



20. Finalización de instalación SO. Podemos apreciar en la figura treinta y dos que la instalación de a completado.

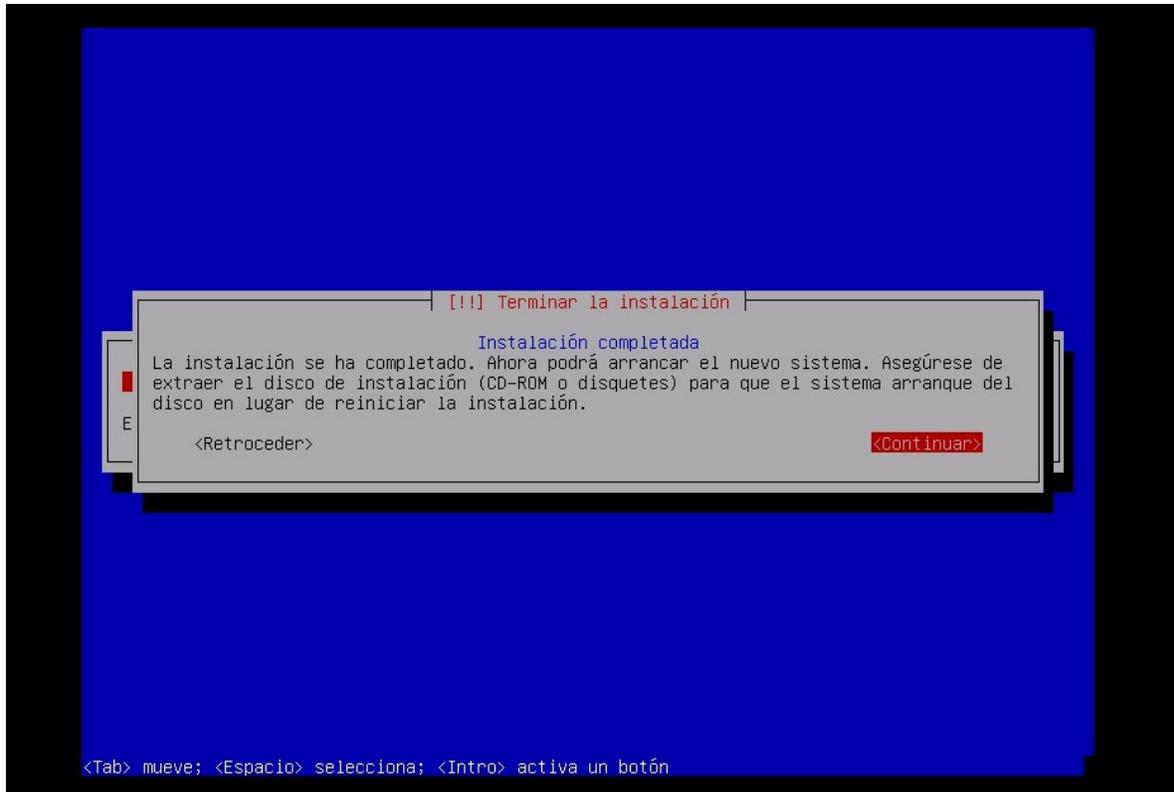


Ilustración 28: Instalación Debian paso 20.

Fuente: Elaboración Propia (2015).



21. Una vez ya instalado el sistema operativo se reinicia la máquina virtual y verificamos el login con el superusuario.

```
Debian GNU/Linux 8 redmon tty1

redmon login: root
Password:
Linux redmon 3.16.0-4-amd64 #1 SMP Debian 3.16.7-ckt9-2 (2015-04-13) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@redmon:~# _
```

Ilustración 29: Instalación Debian paso 21.

Fuente: Elaboración Propia (2015).



3.4.2 Configuraciones adicionales.

Vamos a cambiar la configuración de la tarjeta de red asignándole una dirección ip estática a como se muestra en la ilustración treinta y cuatro. Usaremos el siguiente comando: **nano /etc/network/interfaces**. Una vez editado guardamos y cerramos el archivo.

```
GNU nano 2.2.6 Fichero: /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug eth0
iface eth0 inet static
address 192.168.1.30
netmask 255.255.255.0
gateway 192.168.1.254
up route add -net 0.0.0.0 netmask 0.0.0.0 gw 192.168.1.7 metric 1
up route add -net 192.168.0.0 netmask 255.255.0.0 gw 192.168.1.254 metric 1

[ 18 líneas leídas ]
^G Ver ayuda ^O Guardar ^R Leer Fich ^Y Pág Ant ^K CortarTxt ^C Pos actual
^X Salir ^J Justificar ^W Buscar ^V Pág Sig ^U PegarTxt ^T Ortografía
```

Ilustración 30: Configuración tarjeta de red.

Fuente: Elaboración Propia (2015).

Reiniciamos el demonio networking para que nos actualice la configuración de la tarjeta de red, esto se hace con el comando: **service networking restart**.

Debido a que en la institución hay un servidor de repositorios, es necesario agregar a nuestra configuración este servicio. Esto lo realizaremos con el siguiente comando: **nano /etc/apt/apt.conf.d/01proxy.conf**. Por motivos de seguridad de la institución no se podrán plasmar en este documento el contenido del archivo **01proxy.conf**.



Adicional a esta configuración debemos agregar algunos repositorios externos en el archivo **sources.list** ubicado en la carpeta **/etc/apt**, y comentando las primeras cuatro líneas. A continuación se describe como quedara el archivo.

```
GNU nano 2.2.6      Fichero: /etc/apt/sources.list      Modificado
#_
# deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary-1 2015$
#deb cdrom:[Debian GNU/Linux 8.0.0 _Jessie_ - Official amd64 DVD Binary-1 20150$
#deb http://security.debian.org/ jessie/updates main contrib
#deb-src http://security.debian.org/ jessie/updates main contrib

# jessie-updates, previously known as 'volatile'
# A network mirror was not selected during install.  The following entries
# are provided as examples, but you should amend them as appropriate
# for your mirror of choice.
#
# deb http://ftp.debian.org/debian/ jessie-updates main contrib
# deb-src http://ftp.debian.org/debian/ jessie-updates main contrib
# Proposed updates
deb http://ftp.fr.debian.org/debian/ jessie-propused-updates main contrib noq-f$
# Oficiales
deb http://ftp.fr.debian.org/debian/ jessie main contib non-free
deb-src http://ftp.fr.debian.org/debian/ jessie main contrib non-free
# seguridad
deb http://security.debian.org/ jessie/updates main contrib non-free
deb-src http://security.debian.org/ jessie/updates main contrib non-free
# jessie-updates, previous known as 'volatile'
deb http://ftp.fr.debian.org/debian/ jessie-updates main contrib non-free
deb-src http://ftp.fr.debian.org/debian/ jessie main contrib non-free
# Multimedia
deb http://deb-multimedia.org/ jessie main non-free
deb-src http://deb-multimedia.org/ jessie main non-free
# Backport
deb http://http.debian.net/debian jessie-backports main contrib non-free
deb-src http://http.debian.net/debian jessie-backports main contrib non-free_

^G Ver ayuda  ^O Guardar   ^R Leer Fich ^Y Pág Ant   ^K CortarTxt ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág Sig   ^U PegarTxt  ^T Ortografía
```

Ilustración 31: Configuración de repositorios.

Fuente: Elaboración Propia (2015).



A continuación, descargaremos la lista de paquetes desde los repositorios y las actualizaremos para obtener las versiones más nuevas de los paquetes y sus dependencias con el comando: **apt-get update**.

```
root@redmon:~# apt-get update_
```

Ilustración 32: Actualización de repositorios.

Fuente: Elaboración Propia (2015).

3.4.3 Nagios

Antes de iniciar la instalación de Nagios debemos tener instalado los siguientes prerequisites:

- build-essential
- libgd2-xpm-dev
- apache2-utils
- unzip
- unrar

Descripción de como instalar los paquetes antes mencionados

```
root@redmon:~# apt-get install build-essential libgd2-xpm-dev apache2-utils unzi  
p unrar_
```

Ilustración 33: Instalación de prerequisites.

Fuente: Elaboración Propia (2015).



Creación de usuario y grupo Nagios

Creando un nuevo usuario Nagios y estableciendo contraseña de usuario.

```
root@redmon:~# useradd -m nagios
root@redmon:~# passwd nagios
Introduzca la nueva contraseña de UNIX:
Vuelva a escribir la nueva contraseña de UNIX:
passwd: contraseña actualizada correctamente
root@redmon:~#
```

Ilustración 34: Creación de cuenta Nagios.

Fuente: Elaboración Propia (2015).

Creación de un nuevo grupo **nagcmd** para permitir comandos externos que se presentarán a través de la interfaz web. Debemos agregar tanto el usuario nagios y el usuario apache al grupo.

```
root@redmon:~# groupadd nagcmd
```

Ilustración 35: Creación de grupo nagcmd.

Fuente: Elaboración Propia (2015).

```
root@redmon:~# usermod -a -G nagcmd nagios
```

Ilustración 36: Agregando al usuario nagios al grupo nagcmd.

Fuente: Elaboración Propia (2015).

```
root@redmon:~# usermod -a -G nagcmd www-data
```

Ilustración 37: Agregando al usuario de apache (www-data) al grupo nagcmd.

Fuente: Elaboración Propia (2015).



Descarga de Nagios y plugins

Visitar la página de descarga de Nagios, y obtener la última versión. Cuando se redactó este documento la última versión era la 4.1.1.

<https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.1.1.tar.gz>

También descargar el plugins de Nagios. Plugins de Nagios le permiten controlar hosts, dispositivos, servicios, protocolos y aplicaciones con Nagios

<http://nagios-plugins.org/download/nagios-plugins-2.1.1.tar.gz>

Instalación de Nagios y Plugins

Ir al folder donde se descargó nagios y extraerlo usando el siguiente comando:

```
root@redmon:/home/tux# tar xzf nagios-4.1.1.tar.gz
```

Ilustración 38: Comando para extraer el archivo comprimido de nagios.

Fuente: Elaboración Propia (2015).

Cambiarse hacia el directorio nagios-4.1.1

```
root@redmon:/home/tux# cd nagios-4.1.1/
```

Ilustración 39: Cambio hacia el directorio nagios-4.1.1.

Fuente: Elaboración Propia (2015).



Ejecutar los siguientes comandos uno por uno, desde la terminal para compilar e instalar Nagios.

```
./configure --with-command-group=nagcmd
```

```
make all
```

```
make install
```

```
make install-init
```

```
make install-config
```

```
make install-commandmode
```

Instalación de interfaz web de Nagios

Ingresa el siguiente comando para compilar e instalar la interfaz web de Nagios.

```
make install web-conf
```

Nos encontraremos con el siguiente error que se muestra en la ilustración cuarenta y cuatro.

```
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/httpd/conf.d/nagios.conf
/usr/bin/install: no se puede crear el fichero regular «/etc/httpd/conf.d/nagios.conf»: No existe el fichero o el directorio
Makefile:296: recipe for target 'install-webconf' failed
make: *** [install-webconf] Error 1
root@redmon:/home/tux/nagios-4.1.1# _
```

Ilustración 40: Error tras compilar e instalar la interfaz web de Nagios.

Fuente: Elaboración Propia (2015).



El mensaje de error anterior describe que nagios está tratando de crear el archivo **nagios.conf** dentro del directorio **/etc/httpd.conf/**. Pero, en los sistemas de Debian el archivo **nagios.conf** debe ser colocado en el directorio **/etc/apache2/sites-enabled/**.

Así que, ejecutaremos el siguiente comando en lugar de utilizar **make install-webconf**.

```
/usr/bin/install -c -m 644 sample-config/httpd.conf /etc/apache2/sites-enabled/nagios.conf
```

Verificar si **nagios.conf** está ubicado en el directorio **/etc/apache2/sites-enabled**

```
ls -l /etc/apache2/sites-enabled/
```

Resultado de muestra:

```
total 4
lrwxrwxrwx 1 root root   35 nov 25 13:37 000-default.conf -> ../sites-available/000-default.conf
-rw-r--r-- 1 root root 1679 nov 25 15:10 nagios.conf
```

Ilustración 41: Resultado de muestra de verificación de nagios.conf.

Fuente: Elaboración Propia (2015).

Crear una cuenta nagiosadmin para iniciar sesión en la interfaz web de Nagios. Es necesario recordar la contraseña asignada a esta cuenta. Se necesitará al iniciar sesión en la interfaz web de Nagios.

```
htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
```



Reiniciamos Apache para que la nueva configuración surta efecto.

```
service apache2 restart
```

Instalación de Plugins de Nagios

Nos dirigimos al directorio donde fue descargado el plugin de nagios, y los extraemos.

```
tar xzf nagios-plugins-2.1.1.tar.gz
```

Luego nos cambiamos al directorio del Plugins de nagios.

```
cd nagios-plugins-2.1.1/
```

Ejecutaremos los siguientes comandos uno por uno para compilar e instalarlo

```
./configure --with-nagios-user=nagios --with-nagios-group=nagios
```

```
make
```

```
make install
```



3.4.4 Cacti

En este paso, procederemos a la instalación de la herramienta Cacti desde la consola.

```
apt-get install cacti
```

Configurando mysql-server-5.5. En este paso es recomendable la configuración de una contraseña para el usuario root (administrador) de MySQL.

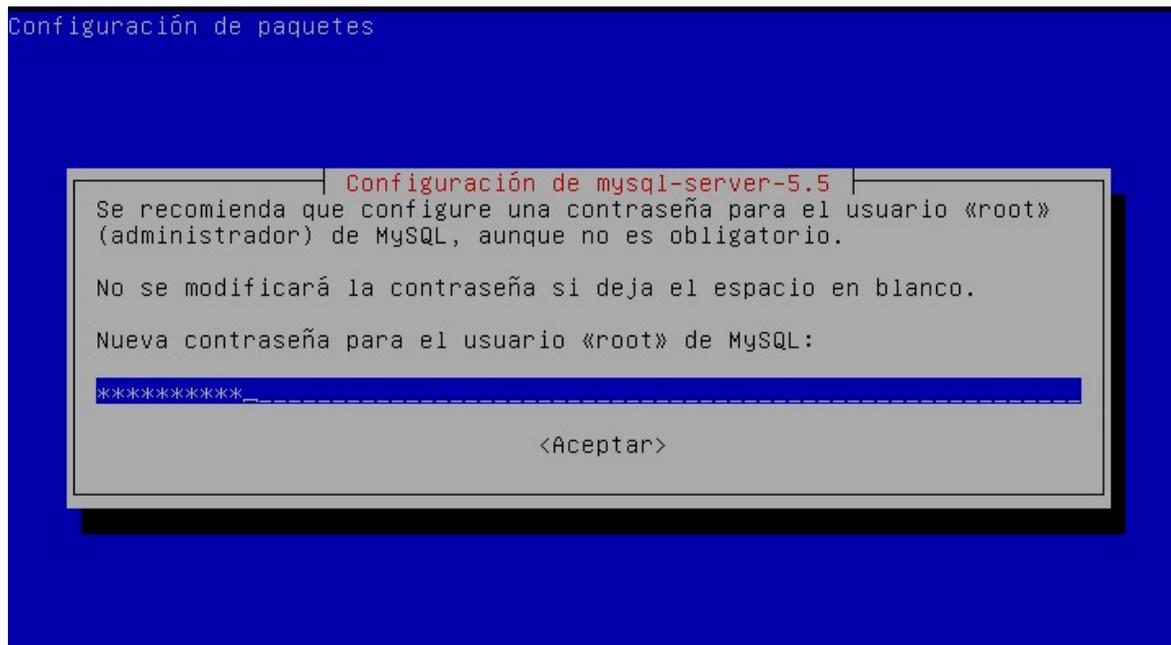


Ilustración 42: Configuración de contraseña de usuario root de MySQL.

Fuente: Elaboración Propia (2015).



Escoger el servidor web que debe configurar automáticamente para cacti, **apache2**.

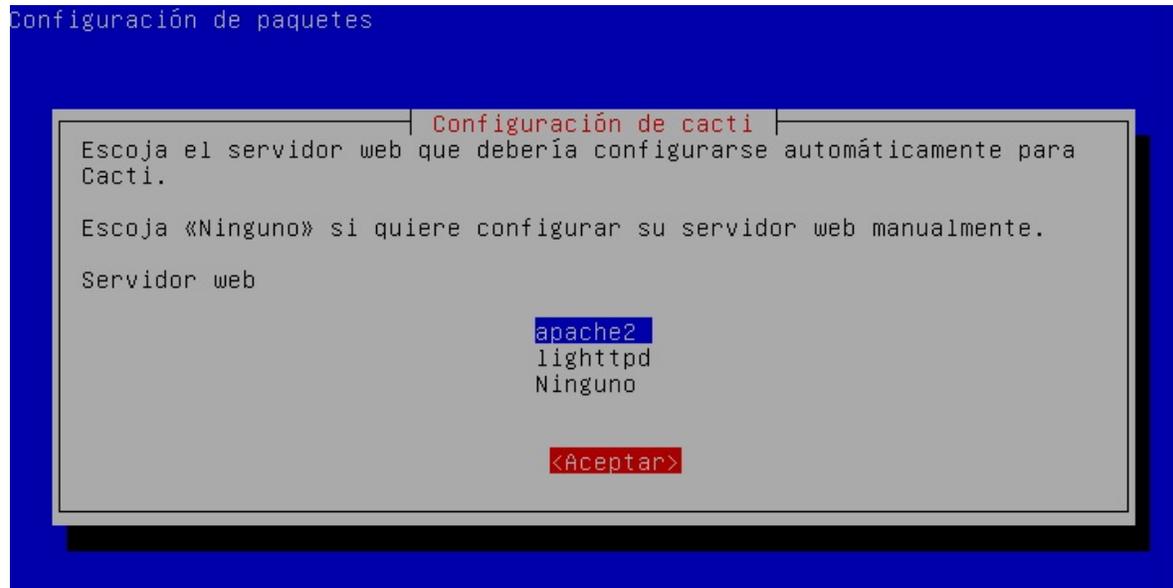


Ilustración 43: Elección de servidor web para configurar cacti.

Fuente: Elaboración Propia (2015).



Debemos tener una base de datos instalada y configurada para cacti antes de poder utilizarlo. Es por ello que vamos a gestionarlo con dbconfig-common.

Elija <Sí> y oprima <ENTER> para continuar.

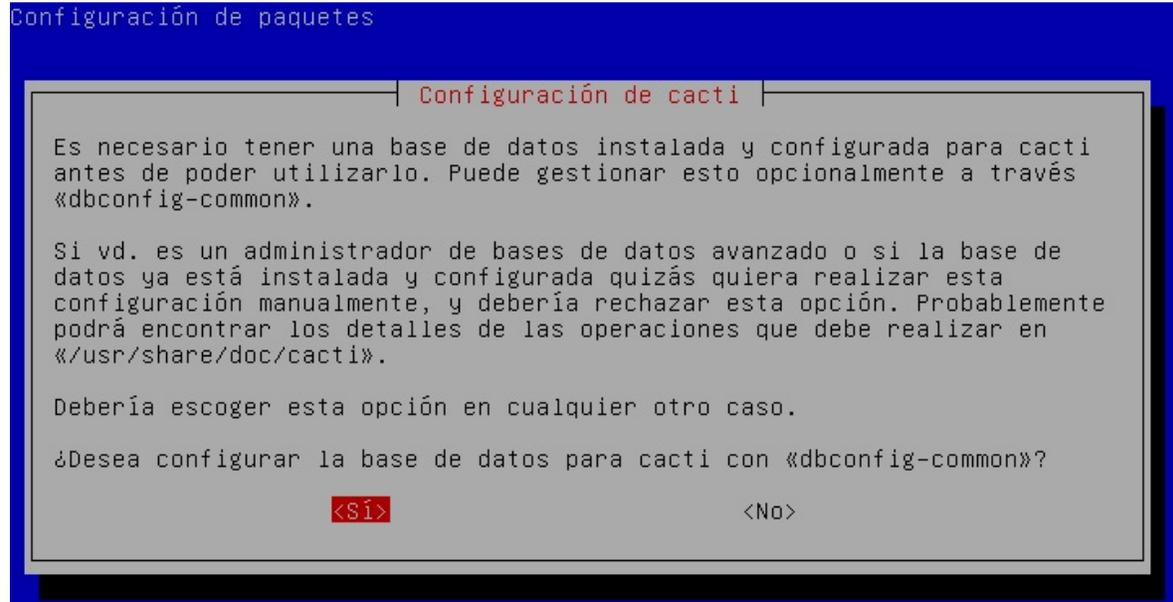


Ilustración 44: Elección de configuración de base de datos para cacti.

Fuente: Elaboración Propia (2015).



Proporcionar la contraseña root que se usó anteriormente

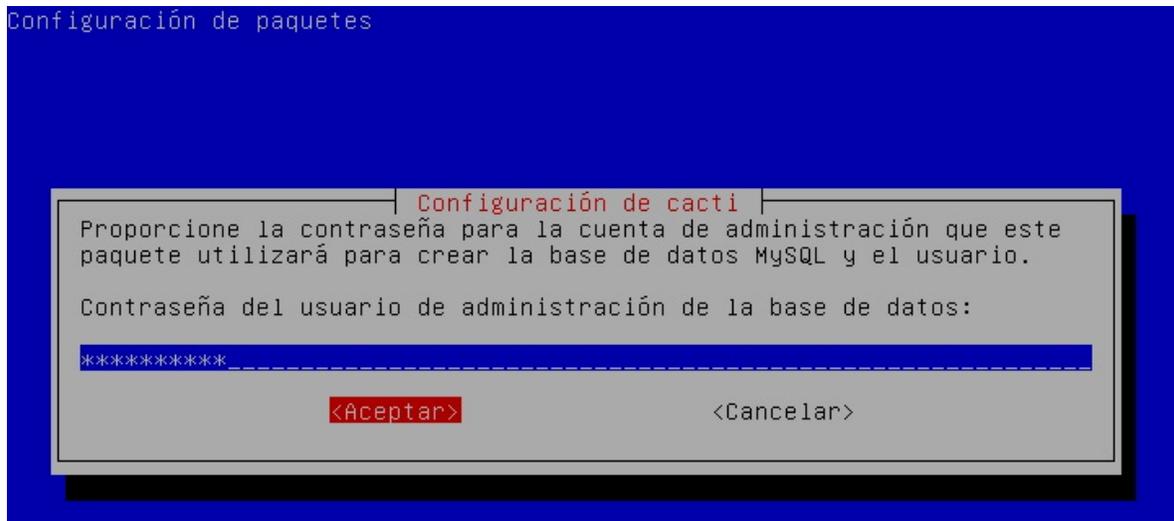


Ilustración 45: Proporcionar contraseña root.

Fuente: Elaboración Propia (2015).

Aquí se puede hacer uso de una nueva contraseña



Ilustración 46: Proporcionar una nueva contraseña.

Fuente: Elaboración Propia (2015).



Repita la clave que uso anteriormente



Ilustración 47: Verificar contraseña.

Fuente: Elaboración Propia (2015).

Ahora usaremos el navegador web para acceder a la siguiente dirección:

<http://192.168.1.30/cacti> vera lo siguiente

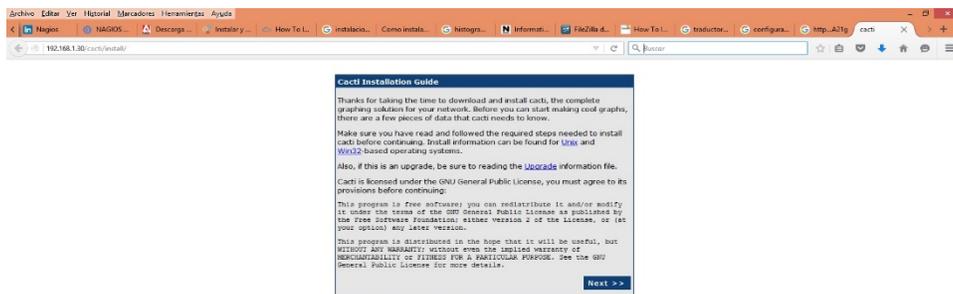


Ilustración 48: Dirección web de Cacti.

Fuente: Elaboración Propia (2015).



Elija New Install y oprima next

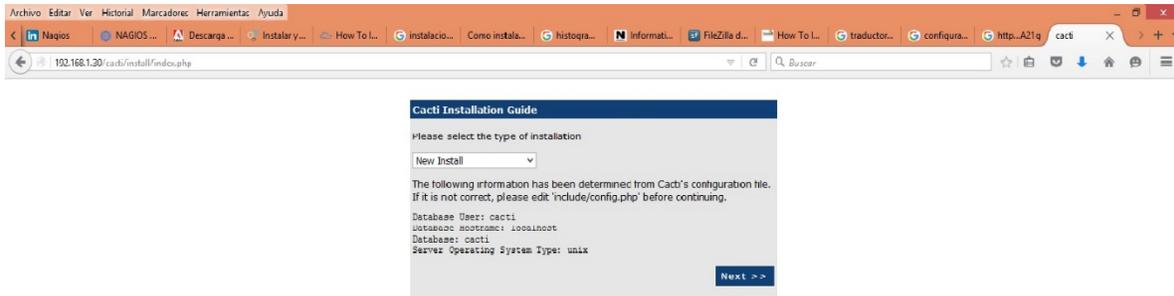


Ilustración 49: Cacti guía de instalación.

Fuente: Elaboración Propia (2015).



Con este resultado oprimir finish

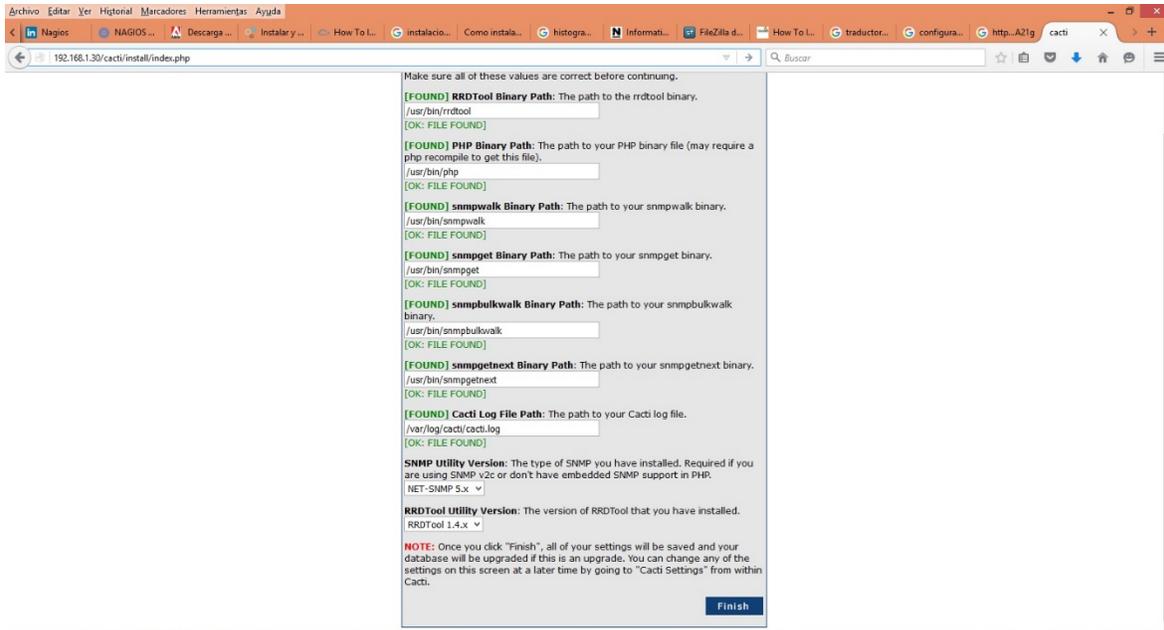


Ilustración 50: Cacti finalización de instalación.

Fuente: Elaboración Propia (2015).



Ingresar por primera vez



Ilustración 51: Cacti User Login.

Fuente: Elaboración Propia (2015).



Vista general del ambiente web de Cacti.

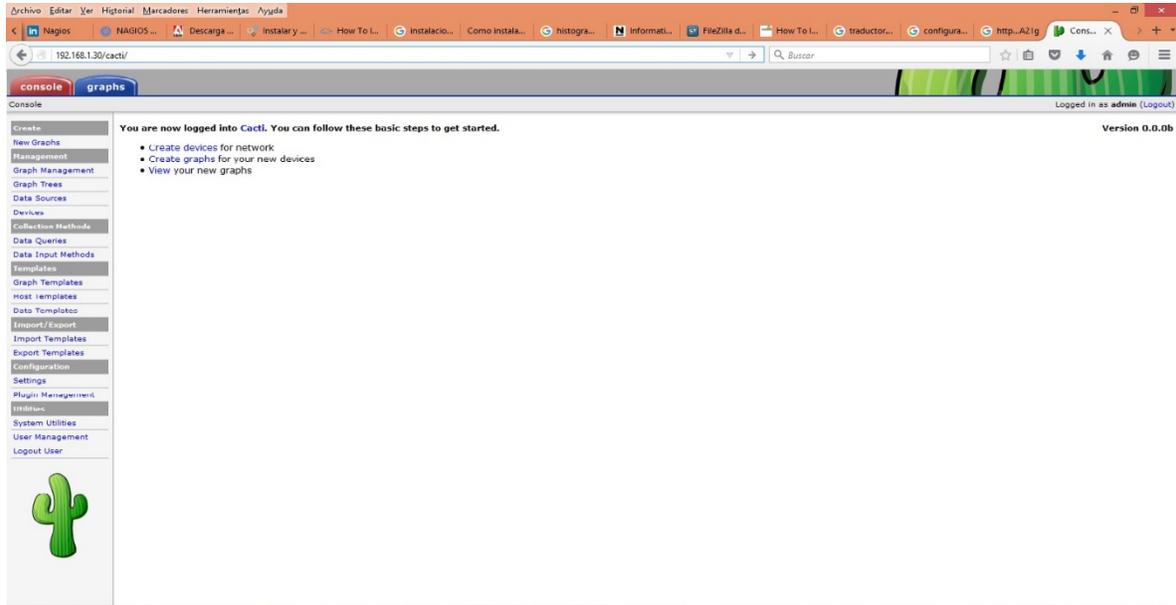


Ilustración 52: vista general de Cacti.

Fuente: Elaboración Propia (2015).



3.5 Configuración personalizada de herramientas

3.5.1 Configuración de Nagios

Los archivos ejemplo de configuración de Nagios se pueden encontrar en el siguiente directorio `/usr/local/nagios/etc`. Estos archivos de ejemplo deberían funcionar bien para empezar con Nagios. Sin embargo, si quieres, tendrás que poner tu ID de correo electrónico real para recibir alertas.

Para ello, editaremos el archivo de configuración `/usr/local/nagios/etc/objects/contacts.cfg` con el comando **nano** y cambiaremos la dirección de correo electrónico asociada a la definición de contactos `nagiosadmin` a la dirección que nos gustaría utilizar para recibir las alertas.

```
nano /usr/local/nagios/etc/objects/contacts.cfg
```

```
#####  
# Just one contact defined by default - the Nagios admin (that's you)  
# This contact definition inherits a lot of default values from the 'generic-co$  
# template which is defined elsewhere.  
  
define contact{  
    contact_name      nagiosadmin           ; Short name of$  
    use               generic-contact      ; Inherit defau$  
    alias             Nagios Admin        ; Full name of $  
  
    email             meorozco@economiafamiliar.gob.ni    $  
    }  
  
#####  
#####  
#  
# CONTACT GROUPS
```

Ilustración 53: ID de correo electrónico real para recibir alertas.

Fuente: Elaboración Propia (2015).



Y editaremos las siguientes líneas para acceder a la consola administrativa nagios desde una serie de IP en particular.

Acá, queremos permitir el acceso administrativo de nagios a solamente desde la serie 192.168.0.0/24.

```
nano /etc/apache2/sites-enabled/nagios.conf
```

Comentaremos las siguientes líneas:

```
# Order allow,deny
```

```
# Allow from all
```

Descomentar las siguientes líneas y agregar la serie de IP que queremos que tenga acceso al sistema:

```
Order deny,allow
```

```
Deny from all
```

```
Allow from 127.0.0.1 192.168.1.0/24
```



```
GNU nano 2.2.6  Fichero: /etc/apache2/sites-enabled/nagios.conf  Modificado

Options ExecCGI
AllowOverride None
<IfVersion >= 2.3>
  <RequireAll>
    Require all granted
#    Require host 127.0.0.1

    AuthName "Nagios Access"
    AuthType Basic
    AuthUserFile /usr/local/nagios/etc/htpasswd.users
    Require valid-user
  </RequireAll>
</IfVersion>
<IfVersion < 2.3>
#  Order allow,deny
#_  Allow from all
  Order deny,allow
  Deny from all
  Allow from 127.0.0.1 192.168.0.0/24

^G Ver ayuda  ^O Guardar  ^R Leer Fich  ^Y Pág Ant  ^K CortarTxt  ^C Pos actual
^X Salir      ^J Justificar ^W Buscar    ^V Pág Sig  ^U PegarTxt  ^T Ortografía
```

Ilustración 54: Serie de IP que tendrá acceso a nagios.

Fuente: Elaboración Propia (2015).

Habilitar sobre escritura de Apache y los módulos de cgi:

a2enmod rewrite

a2enmod cgi

Reiniciamos el servicio apache

service apache2 restart



Revisaremos alguna sintaxis de error en el archivo nagios.conf

```
/usr/local/nagios/bin/nagios -v /usr/local/nagios/etc/nagios.cfg
```

Si no encontramos errores, entonces iniciamos el servicio y hacemos que este se inicie automáticamente en cada boot del sistema operativo.

```
service nagios start
```

```
In -s /etc/init.d/nagios /etc/rcS.d/S99nagios
```

Acceso a Nagios desde la interfaz web

Abriremos nuestro navegador web y navegaremos hacia <http://192.168.1.30/nagios> e ingresaremos el nombre de usuario como **nagiosadmin** y su contraseña la cual fue creada en los pasos iniciales de la instalación de nagios.

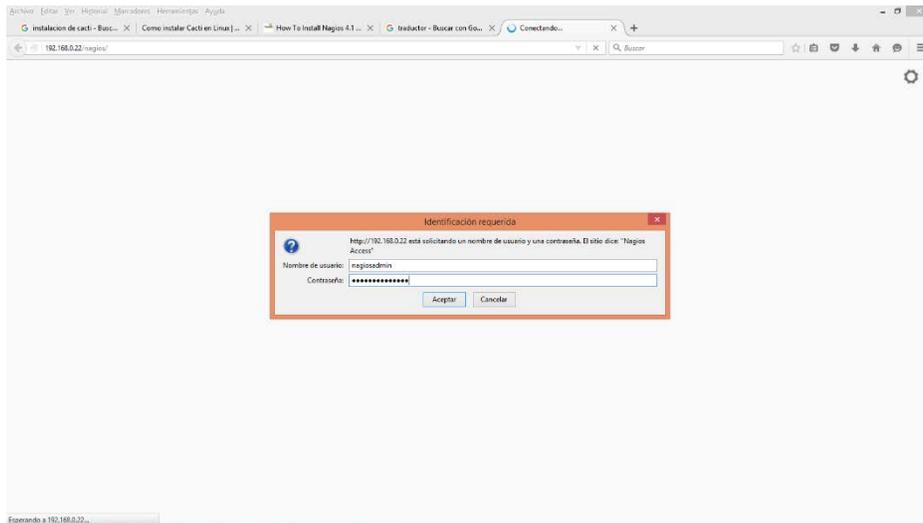


Ilustración 55: Solicitud de accesos en interfaz web de Nagios.

Fuente: Elaboración Propia (2015).



Así es como se verá la consola administrativa Nagios:



Ilustración 56: Consola administrativa de Nagios.

Fuente: Elaboración Propia (2015).

Clic en la sección “**Hosts**” en el lado izquierdo de la consola. Veremos allí que no hay ningún host supervisando por el servidor Nagios. No hemos añadido anfitriones todavía. Por lo tanto, simplemente supervisa a localhost solamente.

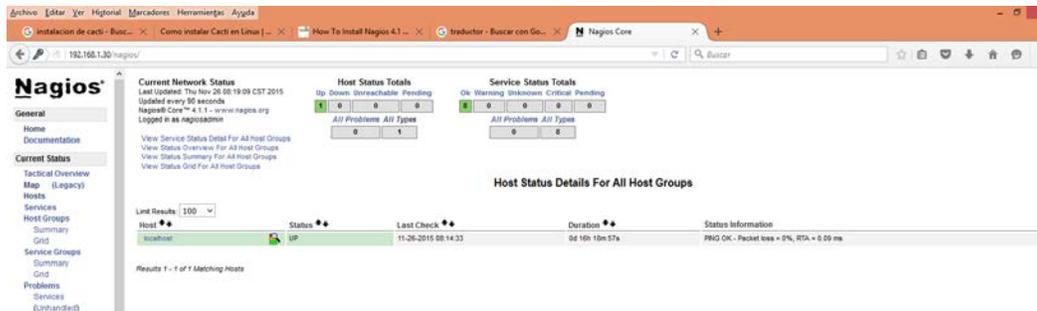


Ilustración 57: Pestaña hosts en la consola administrativa de Nagios.

Fuente: Elaboración Propia (2015).



Damos clic en localhost para mostrar más contenido:

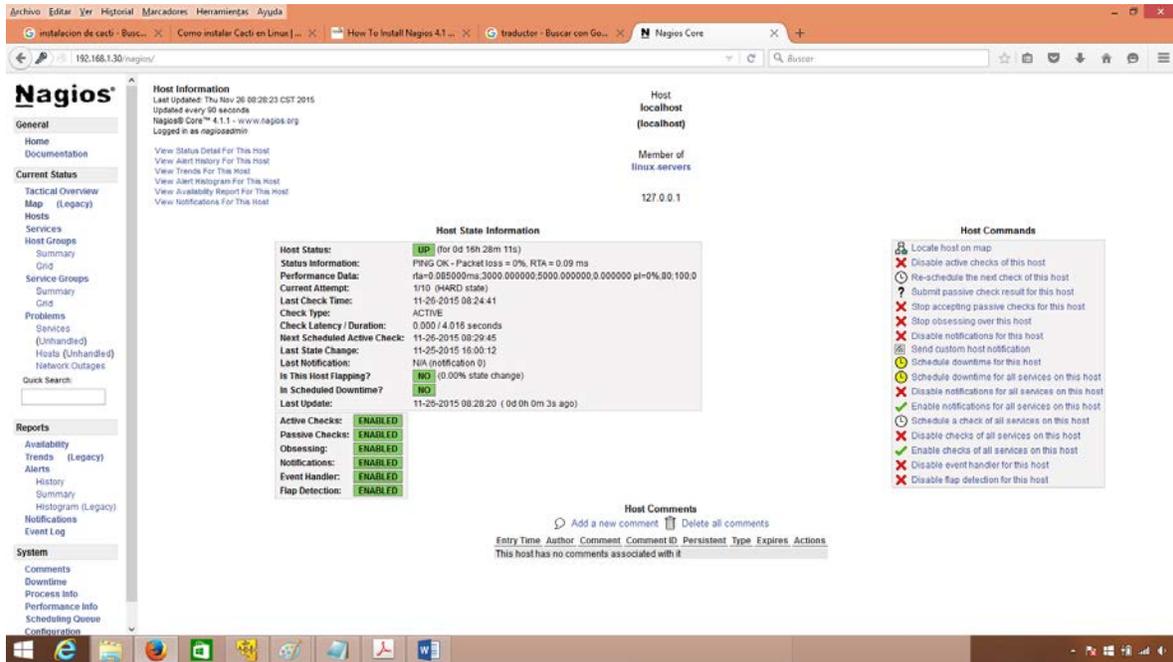


Ilustración 58: Contenido más detallado de localhost.

Fuente: Elaboración Propia (2015).

Esto es todo. Ya hemos instalado y configurado Nagios Core en Debian 8.1.0 AMD x64.

Añadir objetivos de monitoreo de servidor de Nagios

Ahora, vamos a añadir algunos clientes para monitorear servidor Nagios.

Instalaremos los paquetes en los sistemas cliente "nrpe" y "nagios-plugins":

```
apt-get install nagios-nrpe-server nagios-plugins
```



Configuración Objetivos de Monitoreo

Editamos el archivo nrpe.cfg que está ubicado en /etc/nagios/

```
nano /etc/nagios/nrpe.cfg
```

Agregamos la dirección IP de nuestro Nagios:

```
allowed_hosts=127.0.0.1 192.168.1.30
```

Iniciar el servicio nrpe a como se muestra con el siguiente comando:

```
/etc/init.d/nagios-nrpe-server restart
```

Ahora, volvemos a nuestro servidor de Nagios, y añadir los clientes (en el archivo de configuración. Para hacer eso, editamos el archivo:

```
/usr/local/nagios/etc/nagios.cfg
```

```
nano /usr/local/nagios/etc/nagios.cfg
```

Descomentar la siguiente línea:

```
cfg_dir=/usr/local/nagios/etc/servers
```



Crearemos un directorio llamado “servers” dentro de la ruta “/usr/local/nagios/etc”.

```
mkdir /usr/local/nagios/etc/servers
```

Crearemos un archivo de configuración con la meta de monitorización (cliente):

```
nano /usr/local/nagios/etc/servers/clients.cfg
```

Agregar las siguientes líneas:

```
define host{  
use                linux-server  
host_name          reposerver.economiafamiliar.gob.ni  
alias              server  
address            192.168.1.22  
max_check_attempts 5  
check_period       24x7  
notification_interval 30  
notification_period 24x7  
}
```



Acá, 192.168.1.22 es la dirección IP de mi cliente nagios y
reposer.economiafamiliar.gov.ni es el nombre del sistema cliente.

Finalmente reiniciamos el servicio Nagios.

```
/etc/init.d/nagios restart
```

```
O
```

```
Service nagios start
```

Esperamos unos segundos y refrescaremos la consola de administración nagios en el navegador y vamos a la sección " Hosts " en el panel izquierdo.

Ahora, el cliente recién añadido será visible allí. Hacemos clic en el host para ver si hay algo mal o cualquier alerta que tenga.

The screenshot shows the Nagios Core web interface. The browser address bar displays '192.168.1.30 /nagios/'. The left sidebar contains a navigation menu with 'Hosts' highlighted. The main content area shows the configuration for the host 'reposer.economiafamiliar.gov.ni'. A red box highlights the host name and IP address. The 'Host State Information' section shows the host is 'UP' (for 0d 0h 2m 29s+). The 'Host Commands' section lists various actions like 'Disable active checks of this host' and 'Schedule downtime for this host'. The 'Host Comments' section is empty.

Ilustración 59: Nuevo cliente recién agregado en Nagios.

Fuente: Elaboración Propia (2015).



3.5.2 Configuración de Cacti

Agregar un dispositivo

En **console>devices** aparece el listado de los dispositivos que se están monitoreando. Por defecto Cacti ya trae incluido al propio sistema huésped que se puede ver con el nombre de localhost.

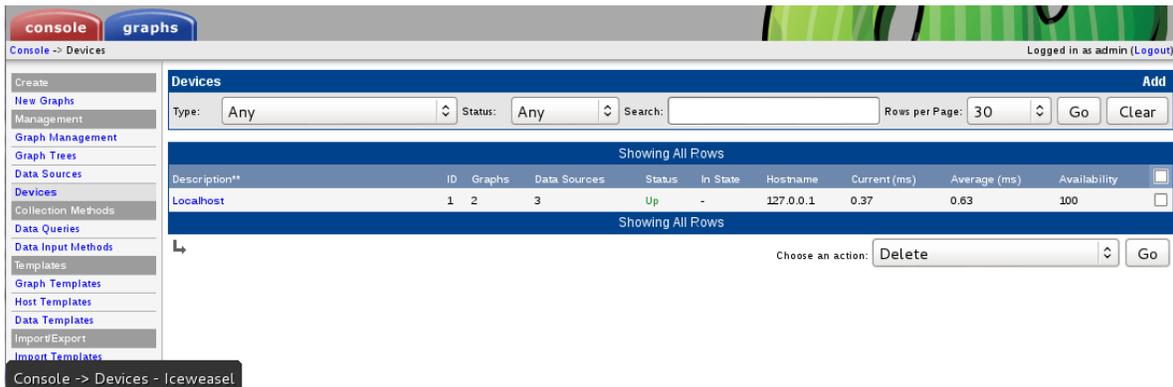


Ilustración 60: Consola Cacti.

Fuente: Elaboración Propia (2015).



Para dar de alta un nuevo dispositivo presionar Add y aparecerá una pantalla en donde agregar los datos SNMP del nuevo dispositivo.

| Device [new] | |
|--|---------------------------------------|
| General Host Options | |
| Description Give this host a meaningful description. | TP-LINK |
| Hostname Fully qualified hostname or IP address for this device. | 192.168.100.1 |
| Host Template Choose the Host Template to use to define the default Graph Templates and Data Queries associated with this Host. | Generic SNMP-enabled Host |
| Number of Collection Threads The number of concurrent threads to use for polling this device. This applies to the Spine poller only. | 1 Thread (default) |
| Disable Host Check this box to disable all checks for this host. | <input type="checkbox"/> Disable Host |
| Availability/Reachability Options | |
| Downed Device Detection The method Cacti will use to determine if a host is available for polling. <i>NOTE: It is recommended that, at a minimum, SNMP always be selected.</i> | SNMP Uptime |
| Ping Timeout Value The timeout value to use for host ICMP and UDP pinging. This host SNMP timeout value applies for SNMP pings. | 400 |
| Ping Retry Count After an initial failure, the number of ping retries Cacti will attempt before failing. | 1 |
| SNMP Options | |
| SNMP Version Choose the SNMP version for this device. | Version 2 |
| SNMP Community SNMP read community for this device. | public |
| SNMP Port Enter the UDP port number to use for SNMP (default is 161). | 161 |
| SNMP Timeout The maximum number of milliseconds Cacti will wait for an SNMP response (does not work with php-snmp support). | 500 |
| Maximum OID's Per Get Request Specified the number of OID's that can be obtained in a single SNMP Get request. | 10 |
| Additional Options | |
| Notes Enter notes to this host. | |

Ilustración 61: Agregar nuevo dispositivo en Cacti

Fuente: Elaboración Propia (2015).

Agregando un dispositivo TP-LINK

En donde dice “description” poner un nombre descriptivo, en “Hostname” poner la ip, en “Host Template” elegir la plantilla que más describa el dispositivo que se quiere agregar, si no se está seguro usar “Generic SNMP-enabled Host”. En la sección llamada “SNMP options” configurar las opciones para que coincidan con las de tu dispositivo SNMP, normalmente los valores de Port, Timeout y Maximum OID’s per request se dejan por defecto.



Una vez agregado, el dispositivo estará en el listado de dispositivos(**Console>Devices**) y tendrá leyenda de Status Unknown, esto es debido a que todavía no hemos agregado una fuente de datos para graficar. Dar clic en el dispositivo y seleccionar la opción de “Create graphs for this Host”

TP-LINK (192.168.1.1) [*Create Graphs for this Host](#)
[*Data Source List](#)
[*Graph List](#)

SNMP Information
System: 1.4.0 Build: 110922 Rel: 38122n
Uptime: 1700296 (0 days, 4 hours, 43 minutes)
Hostname: TP-LINK
Location: Bar
Contact: Max

Device [edit: TP-LINK]
General Host Options

Description
Give this host a meaningful description.

Ilustración 62: Agregar nuevo dispositivo en el listado.

Fuente: Elaboración Propia (2015).

Aparecerá una pantalla en donde se mostrarán diferentes opciones para crear gráficas. Si SNMP está correctamente configurado en la sección Data Query [SNMP] existirá un listado de interfaces disponibles para graficar. Seleccionar las interfaces que se quieran y el tipo de gráfica y dar clic en crear.

Si no aparecen interfaces dar clic en el círculo verde para forzar una nueva consulta SNMP, si esto no funciona verificar la configuración SNMP del dispositivo.

New Graphs for [TP-LINK (192.168.1.1) Generic SNMP-enabled Host]

Host: Graph Types: [*Edit this Host](#)
[*Create New Host](#)

Graph Templates
Graph Template Name:
Create:

Data Query [SNMP - Interface Statistics] Showing All Items

| Index | Status | Description | Type | Speed | Hardware Address | |
|-------|--------|-------------|------|-----------|-------------------|-------------------------------------|
| 1 | Up | eth0 | 6 | 100000000 | F8:D1:11:2D:B8:FF | <input type="checkbox"/> |
| 2 | Down | eth0.2 | 6 | 100000000 | F8:D1:11:2D:B8:FF | <input type="checkbox"/> |
| 3 | Down | eth0.3 | 6 | 100000000 | F8:D1:11:2D:B8:FF | <input type="checkbox"/> |
| 4 | Down | eth0.4 | 6 | 100000000 | F8:D1:11:2D:B8:FF | <input type="checkbox"/> |
| 5 | Up | eth0.5 | 6 | 100000000 | F8:D1:11:2D:B8:FF | <input type="checkbox"/> |
| 6 | Up | atm0 | 37 | 0 | F8:D1:11:2D:B9:00 | <input checked="" type="checkbox"/> |
| 7 | Down | dsl0 | 94 | 0 | | <input type="checkbox"/> |
| 8 | Down | atm0 | 37 | 0 | | <input type="checkbox"/> |
| 9 | Down | cpc0 | 49 | 0 | | <input type="checkbox"/> |

Select a graph type:

Ilustración 63: Opciones para crear gráficas.

Fuente: Elaboración Propia (2015).



Ya con las gráficas creadas para el nuevo dispositivo, después de 5 minutos, tiempo suficiente para que el poller se haya ejecutado, el estado del mismo deberá cambiar a **UP**, de lo contrario verificar que SNMP funciona correctamente.

Dispositivos en Up

| Devices | | | | | | | | | | Add | |
|-------------------|-----|---------|--------------|---------|----------|----------------|--------------|--------------|--------------|--------------------------|----|
| Type: | Any | Status: | Any | Search: | | Rows per Page: | 30 | Go | Clear | | |
| Showing All Rows | | | | | | | | | | | |
| Description** | ID | Graphs | Data Sources | Status | In State | Hostname | Current (ms) | Average (ms) | Availability | | |
| Localhost | 1 | 2 | 3 | Up | - | 127.0.0.1 | 0.36 | 0.52 | 100 | <input type="checkbox"/> | |
| TP-LINK | 3 | 1 | 1 | Up | - | 192.168.100.1 | 118.15 | 118.15 | 100 | <input type="checkbox"/> | |
| Showing All Rows | | | | | | | | | | | |
| Choose an action: | | | | | | | | | | Delete | Go |

Ilustración 64: Verificación de dispositivos en Up.

Fuente: Elaboración Propia (2015).



Sección de gráficas

La sección de gráficas de Cacti sirve para tener un listado de gráficas y de dispositivos que se quieran mostrar. Esta lista se configura de forma manual, de tal forma que aunque se creen nuevos dispositivos éstos no aparecerán en el listado hasta que se hayan agregado a la lista. Por defecto viene agregado el dispositivo localhost. Cuando se agrega un dispositivo también se agregan automáticamente todas sus gráficas.

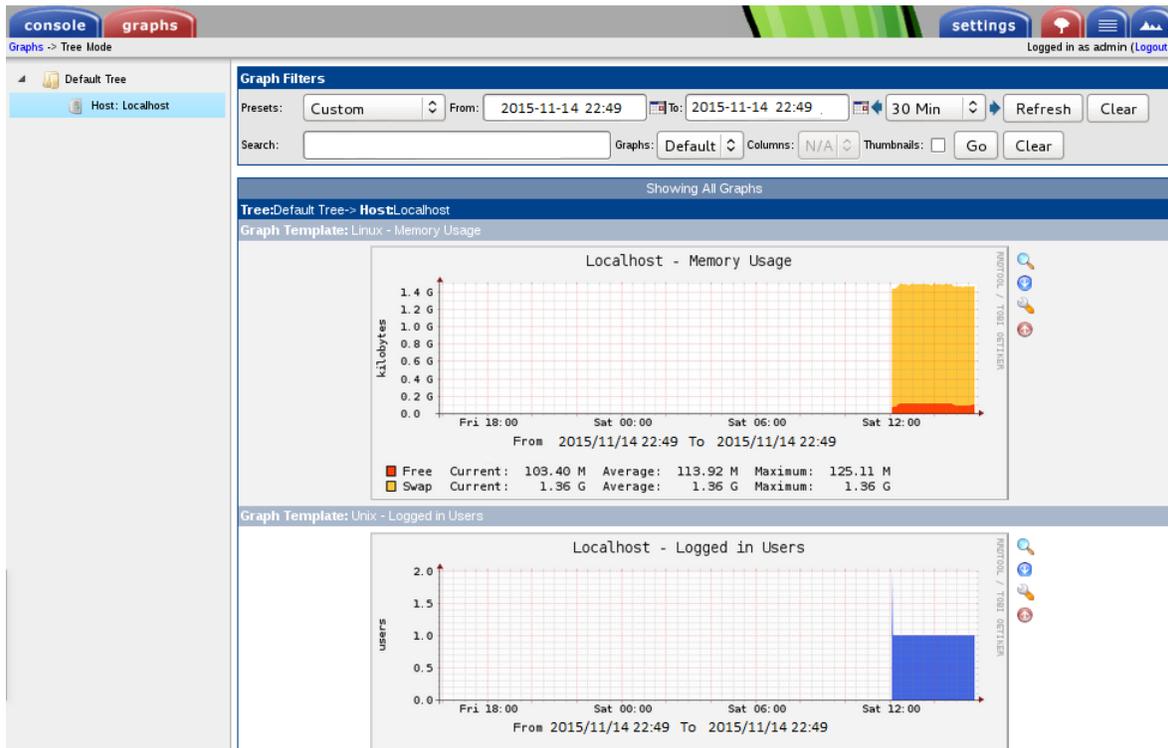


Ilustración 65: Filtro de Gráficos.

Fuente: Elaboración Propia (2015).



Para agregar el dispositivo creado anteriormente a la lista de gráficas ir a **Console> Graph trees> Default Tree** y en la sección de **Tree Items** presionar **Add**. Aparece una pantalla como la siguiente:

Console -> Graph Trees -> (Edit) -> Graph Tree Items Logged in as admin (Logout)

Tree Items

Parent Item: Choose the parent for this header/graph. [root]

Tree Item Type: Choose what type of tree item this is. Host

Tree Item Value

Host: Choose a host here to add it to the tree. TP-LINK (192.168.100.1)

Graph Grouping Style: Choose how graphs are grouped when drawn for this particular host on the tree. Graph Template

Round Robin Archive: Choose a round robin archive to control how Graph Thumbnails are displayed when using Tree Export. Hourly (1 Minute Average)

Cancel Create

Ilustración 66: Agregar dispositivos a la lista de Grafica Cacti.

Fuente: Elaboración Propia (2015).

En Tree Item Type elegir Host y en Host elegir el dispositivo que se quiere agregar a la lista. Presionar “create” para finalizar. Ahora, en la sección de gráficas dentro de “Default tree” deberá aparecer el dispositivo agregado mostrando todas las gráficas que éste tenga:

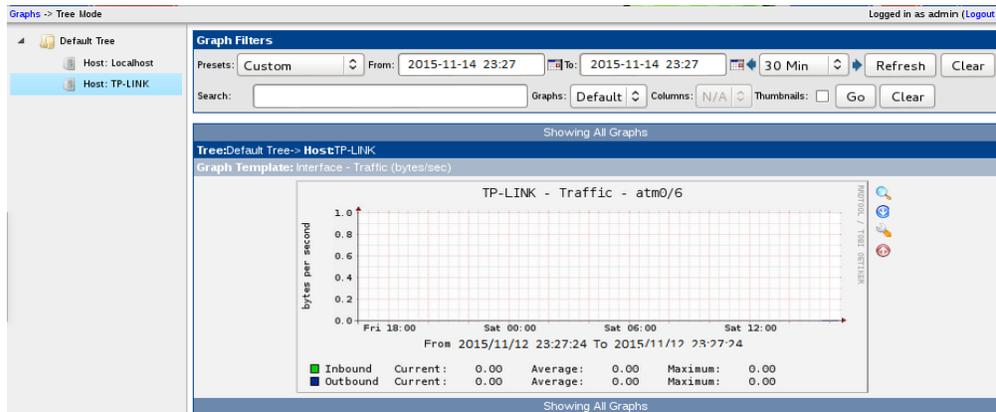


Ilustración 67: Agregando dispositivo a Default tree, mostrando todas sus gráficas.

Fuente: Elaboración Propia (2015).

Esperar unos minutos para que las gráficas muestren algo de información, y listo.



3.6 Evaluación de sistema en ambiente controlado.

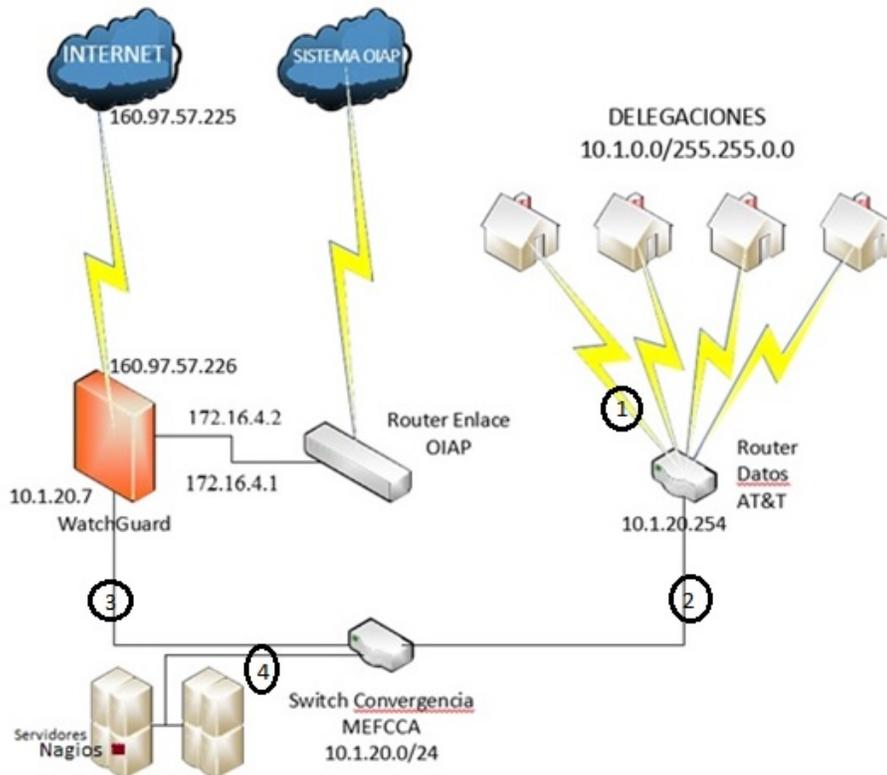


Ilustración 68: Topología de Red MEFCCA - Cortes.

Fuente: Elaboración Propia (2015).

En la topología de red del Ministerio de Economía Familiar efectuamos varios cortes, con el fin de analizar qué sucedería si en uno de esos puntos falla la comunicación hacia la herramienta de monitoreo Nagios.

Si efectuamos un corte en el punto número uno, se verá en el Software de monitoreo que el enlace se encuentra caído. Al realizar un corte en el punto número dos, observaremos que todos los enlaces se encuentran en estado inactivo o Down. Si ejecutamos un corte en el punto tres, no se observará falla alguna. Y para finalizar si se produce un corte en el punto cuatro, encontraremos que todos los host y enlaces estarán en estado inactivo o inalcanzable



Para evaluar el funcionamiento de nuestro sistema de monitoreo utilizaremos el host `reposer.mefc.gov.ni`.

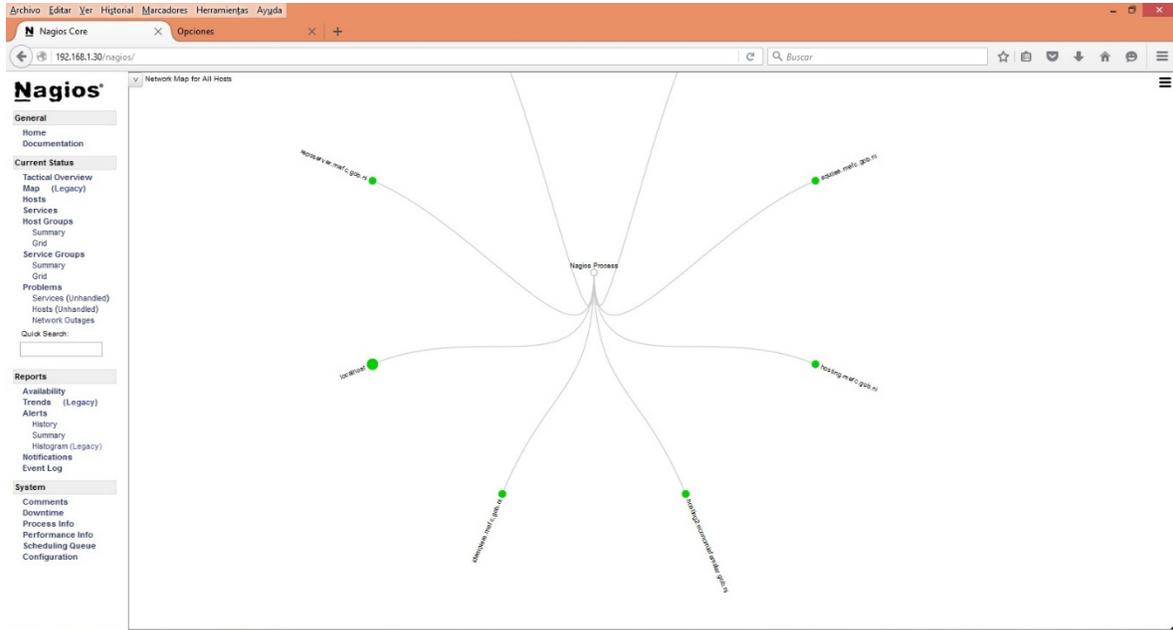


Ilustración 69: Mapa de red de todos los host en monitoreo

Fuente: Elaboración Propia (2015).

La ilustración 68 muestra el mapa de red de todos los hosts que están siendo monitoreados en este momento. Se puede apreciar que cada host tiene su nombre para identificarlo y a su vez una luz verde que indica que está en estado activo y si cambia a rojo es que este tiene una falla.



Sistema de Monitoreo de Infraestructura de red para el
Ministerio de Economía Familiar, Comunitaria, Cooperativa y
Asociativa (MEFCCA)

Ilustración 70: Pantalla de Resumen de reportes

Fuente: Elaboración Propia (2015).

Desde esta pantalla podemos elaborar distintos tipos de reportes de las fechas que el administrador del sistema lo requiera. Entre los reportes que puedes elaborar son: Las ultimas 25 alertas del host, Las 25 últimas alertas de servicios que se han producido, limitando por grupos de host, servicio, alertas leves y alertas graves.



La lámina siguiente es un ejemplo de los reportes que podemos elaborar desde la pantalla de resumen de reportes. En este caso el reporte que aparece acá es el de las alertas más recientes desde 01 de enero 2015 hasta 01 Enero 2016.

The screenshot shows the Nagios Core web interface. The main content area displays the 'Most Recent Alerts' report for the period from 01-01-2015 00:00:00 to 01-01-2016 00:00:00. The report shows 5 matching alerts. The table below summarizes the data:

| Time | Alert Type | Host | Service | State | State Type | Information |
|---------------------|------------|-----------------------|---------|-------|------------|--|
| 12-03-2015 20:11:18 | Host Alert | repositor.mefc.gob.ni | NIA | UP | SOFT | PING OK - Packet loss = 0%, RTA = 0.85 ms |
| 12-03-2015 20:10:14 | Host Alert | repositor.mefc.gob.ni | NIA | DOWN | SOFT | CRITICAL - Host Unreachable (192.168.1.22) |
| 12-03-2015 20:09:11 | Host Alert | repositor.mefc.gob.ni | NIA | DOWN | SOFT | CRITICAL - Host Unreachable (192.168.1.22) |
| 12-03-2015 19:58:56 | Host Alert | repositor.mefc.gob.ni | NIA | UP | SOFT | PING OK - Packet loss = 0%, RTA = 0.88 ms |
| 12-03-2015 19:57:52 | Host Alert | repositor.mefc.gob.ni | NIA | DOWN | SOFT | CRITICAL - Host Unreachable (192.168.1.22) |

Ilustración 71: Reporte de Alertas más recientes de host

Fuente: Elaboración Propia (2015).



Sistema de Monitoreo de Infraestructura de red para el
Ministerio de Economía Familiar, Comunitaria, Cooperativa y
Asociativa (MEFCCA)

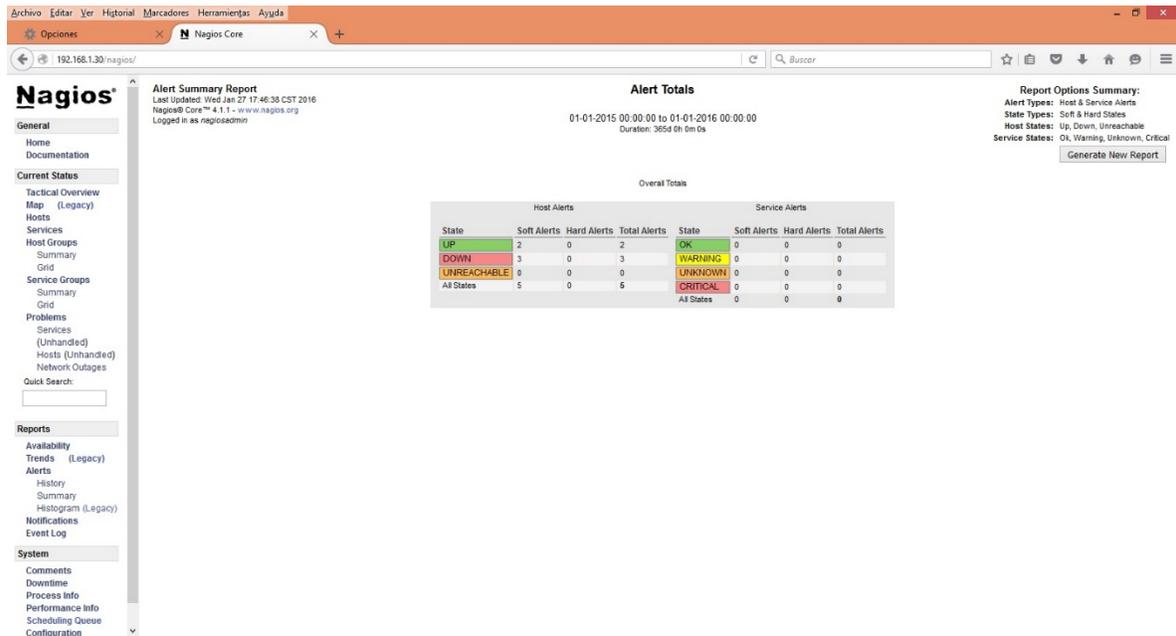


Ilustración 72: Reporte General de todas las alertas de host y servicios

Fuente: Elaboración Propia (2015).

Este reporte es uno de los más generales pero completo porque describe las alertas de host y servicios, estados activos, inactivos, inalcanzables, alertas leves, alertas graves, total de alertas, estado correcto, peligroso, desconocido y estado crítico de los servicios.



Sistema de Monitoreo de Infraestructura de red para el
Ministerio de Economía Familiar, Comunitaria, Cooperativa y
Asociativa (MEFCCA)

All Host and Service Comments
Last Updated: Wed Jan 27 17:58:18 CST 2016
Updated every 30 seconds
Nagios Core™ 4.1.1 - www.nagios.org
Logged in as nagiosadmin

[Host Comments | Service Comments]

Host Comments
Add a new host comment

| Host Name | Entry Time | Author | Comment | Comment ID | Persistent | Type | Expires | Actions |
|-----------------------|---------------------|--------------|--|------------|------------|------|---------|---------|
| reposever.mefc.gob.ni | 12-03-2015 20:12:01 | Nagios Admin | Este server se apago por motivos de prueba | 2 | Yes | User | N/A | |

Service Comments
Add a new service comment

| Host Name | Service | Entry Time | Author | Comment | Comment ID | Persistent | Type | Expires | Actions |
|-------------------------------|---------|------------|--------|---------|------------|------------|------|---------|---------|
| There are no service comments | | | | | | | | | |

Ilustración 73: Pantalla de comentarios acerca de Host y Servicios.

Fuente: Elaboración Propia (2015).

En esta pantalla podemos ver y elaborar comentarios acerca de cualquier alerta, es decir, si por ejemplo apagamos un servidor por mantenimiento, dejamos un comentario para dejar presente que estamos apagando este dispositivo por motivos de mantenimiento.



Sistema de Monitoreo de Infraestructura de red para el
Ministerio de Economía Familiar, Comunitaria, Cooperativa y
Asociativa (MEFCCA)

The screenshot shows the Nagios Core web interface. The top navigation bar includes 'Archivo', 'Editar', 'Ver', 'Historial', 'Marcadores', 'Herramientas', and 'Ayuda'. The browser address bar shows '192.168.1.30/nagios/'. The main content area is titled 'Configuration' and shows the 'Hosts' configuration page. The table below lists the configured hosts and their services.

| Host Name | Alias/Description | Address | Importance (Host) | Importance (Host + Services) | Parent Hosts | Max. Check Attempts | Check Interval | Retry Interval | Host Check Command | Check Period | Obsess Over | Enable Active Checks | Enable Passive Checks | Check Freshness | Freshness Threshold | Default Contacts/Groups | Notification Interval | First Notification Delay | Notification Options |
|----------------------------------|--------------------|---------------|-------------------|------------------------------|--------------|---------------------|----------------|------------------|--------------------|--------------|-------------|----------------------|-----------------------|-----------------------|---------------------|-------------------------|-----------------------|--------------------------|---|
| Router_Del_Managua | Router_Del_Managua | 192.168.11.1 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery, Flapping, Downtime |
| equites.mefc.gov.ni | equinventory | 192.168.1.161 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| hosting.mefc.gov.ni | hosting | 192.168.1.17 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| hosting2.economiafamiliar.gov.ni | hosting2 | 192.168.1.9 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| idempire.mefc.gov.ni | idempire | 192.168.1.27 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| localhost | localhost | 127.0.0.1 | 0 | 0 | 10 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 2h 0m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| reposever.mefc.gov.ni | reposever | 192.168.1.22 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | admins | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery |
| wip.mefc.gov.ni | wip.mefc.gov.ni | 192.168.1.7 | 0 | 0 | 5 | 0h 5m 0s | 0h 1m 0s | check-host-alive | 24x7 | Yes | Yes | Yes | No | Auto-determined value | | | 0h 30m 0s | 0h 0m 0s | Down, Unreachable, Recovery, Flapping, Downtime |

Ilustración 74: Pantalla de visualización de Configuración de host y servicios.

Fuente: Elaboración Propia (2015).

Dentro de la pantalla de configuración se logra percibir que están presente todos los host, descritos de la siguiente manera: Nombre de Host, Descripción Alias, Dirección IP, Importancia (host), Importancia (host y servicios), Hosts Primario, chequeo máximo de intentos, intervalo de chequeo, intervalo de reintento, Comando de chequeo de host, periodo de chequeo, chequeo activo habilitado, chequeo pasivo activo, refrescar, límite de refrescamiento, contacto o grupo por defecto, intervalo de notificación, primer retraso de notificación y opciones de notificaciones



En esta imagen podemos observar el estado histórico del host desde Noviembre a Diciembre del año 2015. Podemos apreciar que hemos perdido un cero coma cero (0.007%) de los paquetes de datos, equivalente en tiempo real a tres minutos con once segundos. Debemos de mencionar que esta caída fue a propósito con el fin demostrar que el sistema si detecta las fallas.

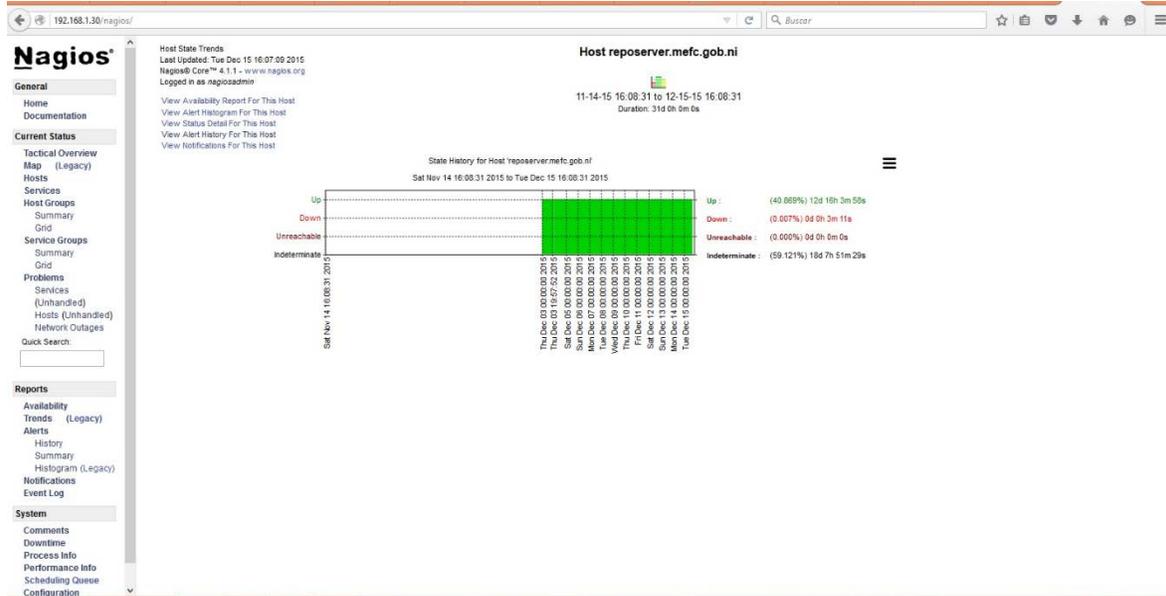


Ilustración 75: Historial de estado del host reposer.mefc.gov.ni

Fuente: Elaboración Propia (2015).



Y para finalizar la prueba controlada mostraremos el histograma de alertas del host. Como podemos apreciar en la ilustración 75, se enviaron tres alertas por falla del host y dos alertas informando que el host ya está nuevamente en servicio.

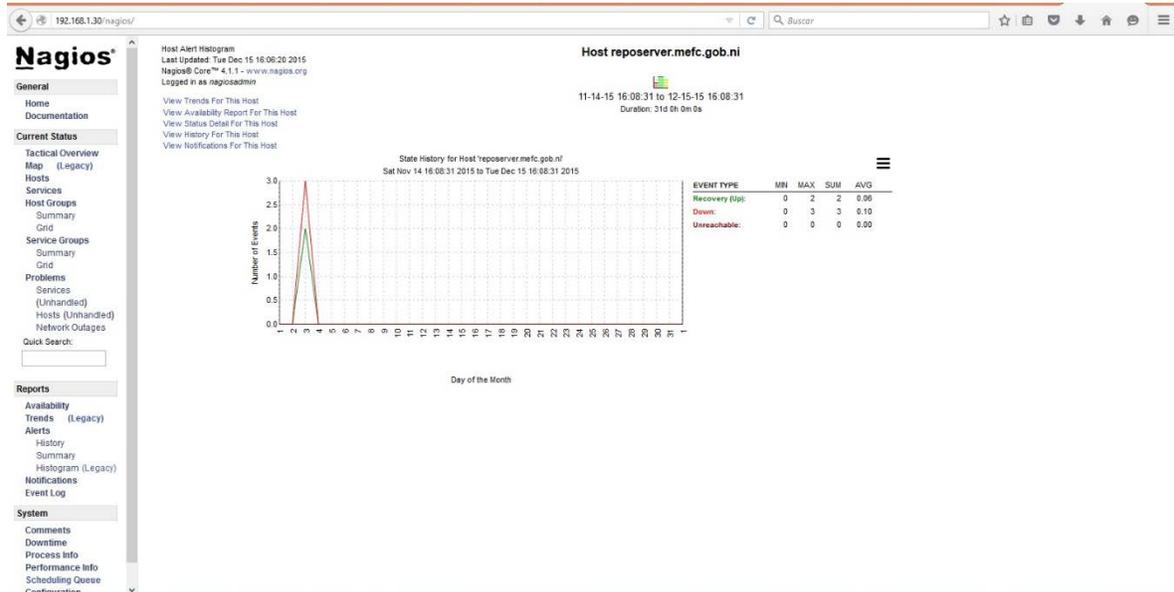


Ilustración 76: Histograma de alertas del host

Fuente: Elaboración Propia (2015).



3.6.1 Procedimiento para dar solución a fallas de host y servicios

El sistema de monitoreo Nagios está siendo administrado por el personal de infraestructura y redes. Si la herramienta detecta una alerta de servicio el personal encargado verifica el estado de la alerta. Si la alarma es positiva, se analiza a que se debió el fallo e inmediatamente se notifica vía correo electrónico indicando tiempo estimado de solución del problema. Posterior a la notificación, se comienza a reparar la falla del servicio. Una vez arreglado el problema se informa nuevamente que la falla ha sido superada, al mismo tiempo que dejaremos dentro de la herramienta de monitoreo un comentario de servicio indicando motivos de falla y solución, detallando fecha-hora en que inicio y finalizo la alerta.

Ahora bien, si el sistema identifica una alerta de host (estado inactivo o inalcanzable) el personal de redes procede a verificar si la alerta es real. Si es así se investiga si la falla es debido a problemas eléctricos o de transporte. Si el problema es eléctrico, solamente se notifica a la dirección informática que el sitio se encuentra sin energía eléctrica, esperando a que se restablezca el servicio eléctrico para verificar una vez más si el host vuelve a su estado activo. En el caso de que la falla sea por transporte de datos, se procede a enviar una notificación vía correo electrónico al proveedor de servicios de internet. Luego el proveedor verifica el tipo de problema y notifica vía correo electrónico asignando un número de ticket único, con el nombre de la sucursal que es afectada, en que zona está ubicada, la prioridad con que será atendido el caso y el estado del ticket. Sucesivamente se recibirá otro correo electrónico del proveedor, indicando que el host ha sido restablecido y que el ticket queda abierto temporalmente. Seguido, el personal encargado de infraestructura y redes verifica en la herramienta de monitoreo que el host este activo; de ser así se procede a elaborar un informe detallado del problema y su solución, apoyándose de los reportes que se generan en la herramienta de monitoreo Nagios.



CAPITULO IV

4.1 Conclusiones

En el trabajo de tesis se elaboró un diagnóstico de la situación actual de la infraestructura de red de datos del MEFCCA, mediante los instrumentos de recolección de información como: la observación in situ, entrevistas al jefe del área de informática, con la finalidad de evidenciar las necesidades técnicas del área en relación a las herramientas de monitoreo de red.

La herramienta Nagios fue configurada exitosamente bajo las normas ISO 10165-1, 10165-2, 10165-4, de tal manera que está identificando y reportando las fallas de la infraestructura de red de forma inmediata. Tras efectuar pruebas controladas de la infraestructura de red con el software de monitoreo hemos podido analizar su comportamiento en tiempo real por lo tanto podemos decir que el sistema de monitoreo es funcional.

En definitiva, la herramienta Nagios en conjunto con Cacti es un software óptimo de monitoreo de red, para el Ministerio de Economía Familiar, Comunitaria, Cooperativa y Asociativa, por sus características principales: elaboración de reportes, generación de alertas, monitoreo de múltiples segmentos de red y software libre.



4.2 Recomendaciones

Implementar el monitoreo de la infraestructura de red del Ministerio de Economía Familiar, Comunitaria, Cooperativa y Asociativa (MEFCCA) por parte del área de informática, con el propósito de administrar eficaz y eficientemente la red y recursos alineado a la normas ISO-IEC 7498, ISO-20000.

Realizar capacitación al personal de informática en el uso de la herramienta de monitoreo Nagios, para adiestrarlo en las tareas de monitorización tanto a nivel de hardware (espacio en disco, porcentaje de uso de CPU, memoria, procesos, etc.) como a nivel de software (agente SNMP, alertas, etc.).

Al momento de efectuar este trabajo el Ministerio se encontraba en el proceso de cambio de proveedor de servicio de internet (ISP- Internet Service Provider), por lo que se le recomienda una vez finalizado esto, agregar los routers de cada sitio a la herramienta de monitoreo para darles seguimiento.



4.3 Bibliografía

Cacti. (2015, Octubre).What is Cacti? Recuperado el 13 de octubre de 2015, de http://www.cacti.net/what_is_cacti.php

Hernández Sampieri, R., Fernández Collado, C., & Pilar Baptista, L. (2006).

Metodología de la Investigación. (4ª. ed.). México DF:
McGrawHill Interamericana.

Hernández, J. M., Jiménez, D. M., González Barahona, J. M., Seoane Pascual, J.,

& Robles, G. (2007). Introducción al Software libre. (2ª. ed.). Barcelona: Fundación UOC.

Jorquera, D. M. (2010). Difusión Masiva de Información en los modelos de Gestión de Redes, Aplicación a los Servicios de Alta Disponibilidad sobre Internet: Modelo de Gestión de Redes. Tesis doctoral no publicada, Universidad de Alicante, San Vicente de Raspeig, España.

Kemp, J. (2008). Monitor Libre. Linux Magazine, (41), 20-22.

Kendall, K. & Kendall, J. (2005).Análisis y Diseño de Sistemas. (6ª. ed.) . México: Pearson Education.

Landeau R. (2007). Elaboración de trabajos de investigación. Caracas: editorial Alfa



Nagios. (2015, Febrero). Nagios. Recuperado el 20 de noviembre de 2015, de <http://www.nagios.org/>

Rojas Soriano, R. (2006). Guía Para Realizar Investigaciones Sociales. ed.).México: Plaza y Valdés Editores

Romero, J. L. (2013). Administración, monitoreo y seguridad de redes con software libre. Recuperado el 13 de octubre de 2015, de www.linuxmaya.com

Valdivia, C. (2005). Sistemas informáticos y redes locales. Madrid: Ediciones Paraninfo.

Verón piquero, J. (2010). Prácticas de redes. España: Visión libros.

Wayner, P. (2001). La ofensiva del software libre: cómo Linux y el movimiento del software libre se impusieron frente a los titanes de la alta tecnología. Buenos Aires: Ediciones Granica, S.A.

Stallings, W. (2005). Wireless Communications and Networks. (2a.ed.). New Jersey: Pearson Education.

Ubuntu. (2015, Septiembre). How to install Nagios 4.0.1 (Monitoring Tool) in Ubuntu 13.10 server (Saucy Salamander) Recuperado el 07 de septiembre de 2015, de <http://www.ubuntugeek.com/how-to-install-nagios-4-0-1-monitoring-tool-in-ubuntu-13-10-server-saucy-salamander.html>



Debian. (2015, Septiembre). Instalar y configurar Nagios en servidor Debian 7 (Parte I) Recuperado el 07 de septiembre de 2015, de www.ochobitshacenunbyte.com/2014/04/30/instalar-y-configurar-nagios-en-servidor-debian-7-parte-i/

VMware vSphere P3 (2015, Septiembre). Instalar y fusionar Cacti y Nagios para gestionar VMware vSphere P3 Recuperado el 14 de septiembre de 2015, de <http://www.colombiavirtualizada.com/2013/09/08/cacti-nagios-ipfix-ntop-vmware-p3/>

<https://www.digitalocean.com/community/tutorials/how-to-install-nagios-4-and-monitor-your-servers-on-ubuntu-14-04>

Cacti (2015, Octubre). Como instalar Cacti en Linux Recuperado el 11 de octubre de 2015, de <http://notasdesoftware.com/2015/04/como-instalar-cacti-en-linux.html>



4.4 ANEXOS



4.4.1 ANEXOS A

Cuarto de Servidores de la Red del MEFCCA



Ilustración 77: Centro de Datos.

Fuente: Elaboración Propia (2015).

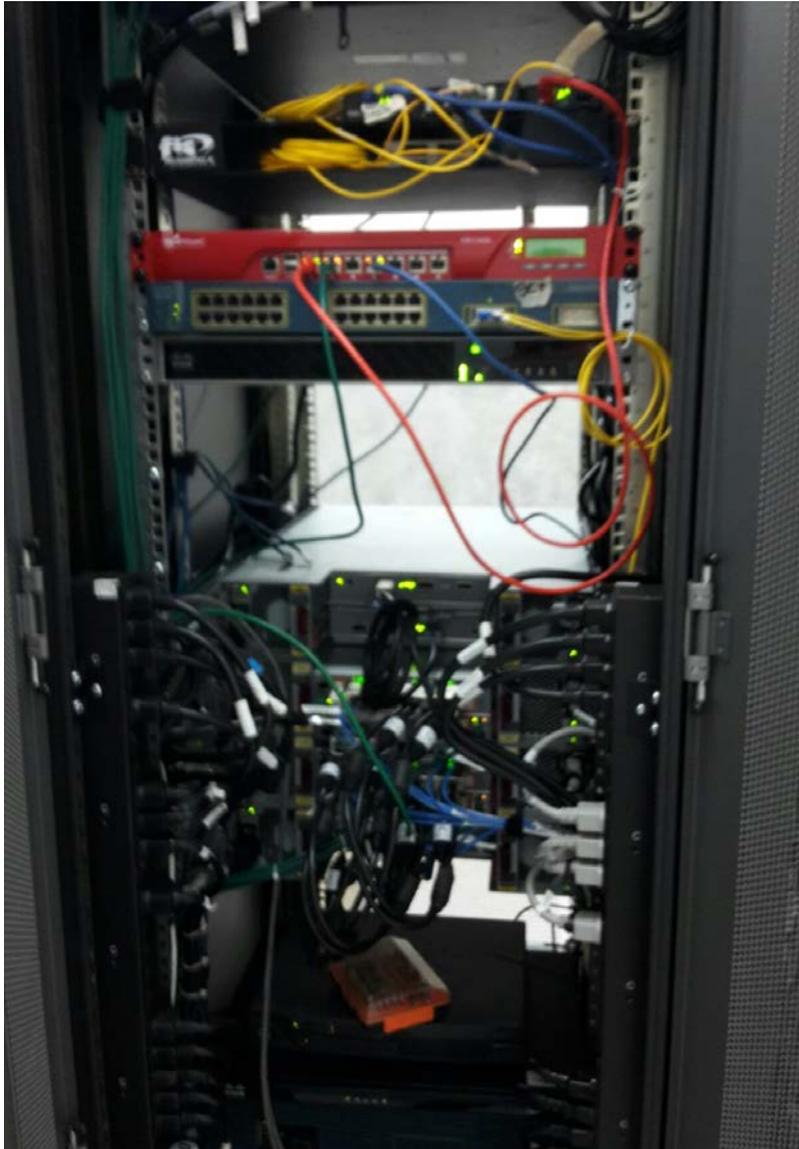


Ilustración 78: Rack de Comunicaciones MEFCCA.

Fuente: Elaboración Propia (2015).



4.4.2 ANEXOS B

Entrevista dirigida al administrador de la Red del MEFCCA



Cuestionario:

1. ¿Cuántos servidores en servicio cuenta el Ministerio de Economía Familiar, Comunitaria, Cooperativa y Asociativa en la actualidad?
2. ¿Qué sistema operativo utilizan los servidores?
3. ¿Cuáles son las especificaciones generales de los servidores?
4. Si los servidores están distribuidos ¿cuáles son las condiciones climáticas y de seguridad del local donde se albergan los servidores?
5. Además de la gratuidad del software libre ¿Cuáles son los factores, por los que el área de informática prefiere herramientas de software libre?



4.3.3 ANEXOS C

Entrevista semi-estructurada al área de informática MEFCCA



Universidad Nacional Autónoma de Nicaragua

Facultad de Ciencia

Ingeniería en Electrónica

“Sistema de Monitoreo de Infraestructura de red para el

Ministerio de Economía Familiar, Comunitario, Cooperativa y Asociativa (MEFCCA)”

Esta entrevista tiene por objetivo recopilar información acerca de sus conocimientos acerca del software libre y características específicas del software de monitoreo de red.

Estimado entrevistado, se implementaran las medidas necesarias para resguardar su información y confidencialidad, los datos recolectados serán utilizados con fines educativos en nuestro trabajo de seminario de graduación.

1. ¿Conoce o ha escuchado mencionar alguna aplicación de monitoreo de red?

2. ¿Con que tipo de software usted se siente más identificado, con el software libre o con el propietario? ¿Por qué?

3. ¿Cuáles su aplicación de monitoreo de red preferida? ¿Por qué?



4.3.4 ANEXOS D

Estándar de gestión



La gestión de red OSI, pensada inicialmente para la gestión de las propias redes OSI, debe su implantación práctica al ser adoptada por los estándares TMN (Telecommunications Management Network) como tecnología base de sus interfaces de gestión.

La arquitectura se presenta en la siguiente figura:

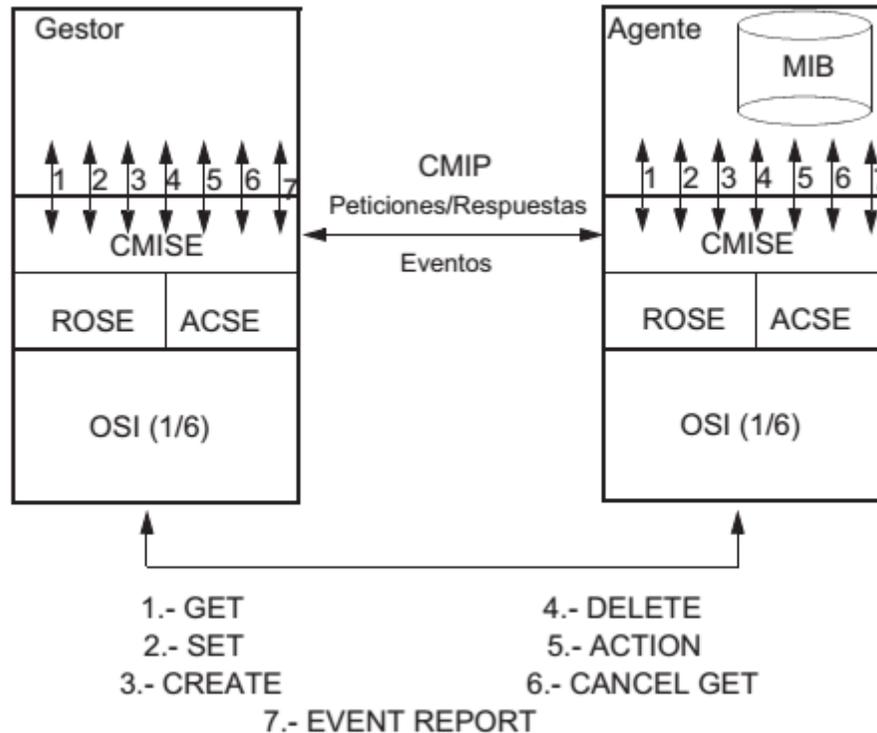


Ilustración 79: Centro de Datos.

Fuente: Facultad de Informática da Coruña (2015)

Está definida en estándares de ITU-T e ISO: •Aspectos Generales: X.700/ISO 7498-4, X.701/ISO 10040 •CMIS, CMIP: X.710/ISO 9595, X.711/ISO 9596 •Modelo de Información de Gestión: X.720/ISO 10165-1, X.721/ISO 10165-2, X.722/ISO 10165-4(GDMO) •Funciones de Gestión OSI: X.73x-4x/ISO 10164-x