UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO PARA EL ANÁLISIS DE LA DISPONIBILIDAD, CAPACIDAD, CALIDAD Y LATENCIA DE ENLACES CORPORATIVOS DE ÚLTIMA MILLA

AUTOR:

Ing. Guillermo Eduardo Vega Picon

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

M. Sc. Manuel de Jesús Romero Paz

Guayaquil, 26 de octubre del 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por el Magíster **Guillermo Eduardo Vega Picón** como requerimiento parcial para la obtención del Grado Académico de Magíster en Telecomunicaciones.

Guayaquil, 26 de octubre del 2018

TUTOR

_____

M. Sc. Manuel de Jesús Romero Paz

DIRECTOR DEL PROGRAMA

_____

M. Sc. Manuel de Jesús Romero Paz

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, Ing. Guillermo Eduardo Vega Picón

DECLARO QUE:

El trabajo de titulación "**Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla**", previa a la obtención del grado Académico de Magíster, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros conforme las citas que constan en el documento. Consecuentemente este trabajo es mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del trabajo de titulación del Grado Académico en mención.

Guayaquil, 26 de octubre del 2018

EL AUTOR

_____

Ing. Guillermo Eduardo Vega Picón

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, Ing. Guillermo Eduardo Vega Picón

Autorizo a la Universidad Católica de Santiago de Guayaquil, la publicación, en la biblioteca de la institución del trabajo de titulación de Maestría titulado: "**Implementación de un sistema de monitoreo para el análisis de la disponibilidad capacidad, calidad y latencia de enlaces corporativos de última milla**", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

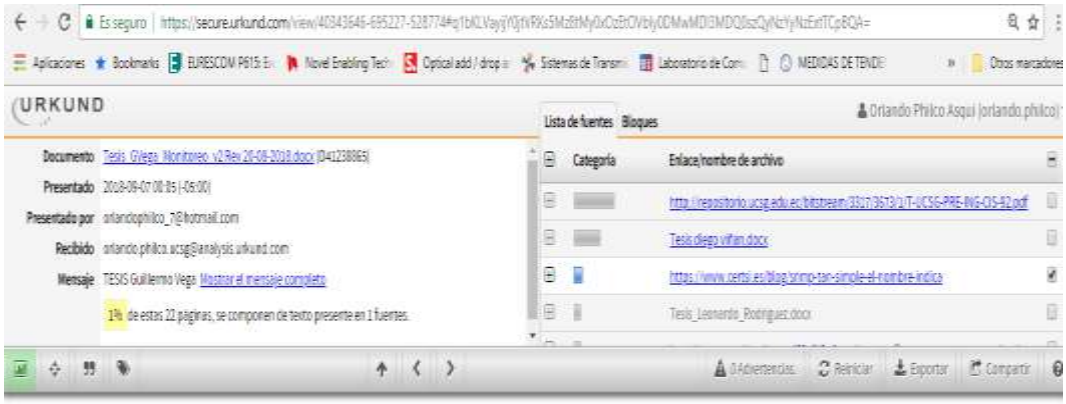
Guayaquil, 26 de octubre del 2018

EL AUTOR

_____

Ing. Guillermo Eduardo Vega Picón

REPORTE URKUND



SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

TEMA:

IMPLEMENTACION DE UN SISTEMA DE MONITOREO PARA EL ANALISIS DE LA DISPONIBILIDAD, CAPACIDAD, CALIDAD Y LATENCIA DE ENLACES CORPORATIVOS DE ULTIMA MILLA

AUTOR:

Ing. Guillermo Eduardo Vega Picon

Trabajo de titulacion previo a la obtencion del grado de Magister en Telecomunicaciones

TUTOR: M. Sc. Manuel de Jesús Romero Paz

Dedicatoria

El presente trabajo de titulación va dedicado a mis padres,
Por su apoyo incondicional durante esta etapa de estudios,
A Dios y a la Virgen por bendecirme y permitirme,
Culminar con éxito un peldaño más en mi vida

Agradecimientos

Agradezco a toda la gente que participo de una u otra manera,
De este logro, así como a mis profesores, tutor,
Quienes han sido pilares fundamentales para,
Obtener un logro más en mi vida, de igual forma,
Un agradecimiento inmenso a mis padres por ser mis guías,
Y brindarme un aporte esencial para lograr con éxito la maestría.

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

MSc. Manuel Romero Paz
TUTOR

f. _____

MSc. Manuel Romero Paz
DIRECTOR DEL PROGRAMA

f. _____

MSc. Luis Córdova Rivadeneira
REVISOR

f. _____

MSc. Orlando Philco Asqui
REVISOR

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

Capítulo 2:

Capítulo 3:

Capítulo 4:

ÍNDICE DE TABLAS

Capítulo 2:

Capítulo 3:

Resumen

En este trabajo de investigación, se realiza el análisis de diferentes herramientas de monitoreo tanto de pago como gratuitas, para poder determinar e implementar un sistema de monitoreo, que brinde los parámetros necesarios para mantener una infraestructura de red operativa y disponible para los usuarios. Se realiza un análisis y comparación de las principales herramientas de pago que existen en el mercado y las de monitoreo gratuitas que existen en la actualidad, luego se analiza el protocolo SNMP (Simple Network Management Protocol – Protocolo Simple de Administracion de Red), el cual es el principal mecanismo de comunicación entre el sistema de monitoreo y los equipos a ser monitoreados, para poder implementar un sistema de monitoreo adecuado. Luego se procede a realizar la implementación de las herramientas elegidas, analizando cada una de ellas.Por último se realiza la evaluación y se analizan los beneficios que cada una de las herramientas de monitoreo implementadas brinda, para poder contar con un sistema de monitoreo correctamente implementado. En la sección de anexos, se explican los pasos que se siguieron, para poder realizar la implementación y configuración de cada una de las herramientas de monitoreo elegidas, se indican parámetros importantes como que tipo de sistema operativo se eligio, características de los servidores en los cuales se alojaran las herramientas de monitoreo y configuración de cada una de ellas.

Palabras Clave: Cacti, Nagios, Monitoreo, Tecnologia, SLA, Enlaces.

Abstract

In this research work, the analysis of different monitoring tools, both free and paid, is carried out in order to determine and implement a monitoring system that provides the necessary parameters to maintain a network infrastructure that is operational and available to users. An analysis and comparison of the main payment tools that exist in the market and the free monitoring tools that currently exist are performed, then the SNMP protocol (Simple Network Management Protocol) is analyzed, which It is the main communication mechanism between the monitoring system and the equipment to be monitored, in order to implement an adequate monitoring system. Then we proceed to implement the chosen tools, analyzing each of them. Finally, the evaluation is made and the benefits that each of the monitoring tools implemented are analyzed, in order to have a properly implemented monitoring system. . In the annexes section, the steps that were followed are explained, in order to perform the implementation and configuration of each of the chosen monitoring tools, important parameters are indicated such as what type of operating system was chosen, characteristics of the servers in which will be the monitoring and configuration tools of each of them.

Key Words: Cacti, Nagios, Monitoring, Technology, SLA, Links.

Capítulo 1: Descripción del proyecto de intervención.

En el presente proyecto de intervención, se realizará la implementación de un sistema de monitoreo de equipos de red basado en el protocolo SNMP, para realizar la captura de datos utilizando herramientas gratuitas, esto con el fin de cumplir los acuerdos de nivel de servicio SLA (Service Level Agreement – Acuerdo de Nivel de Servicio), analizando los parámetros de disponibilidad, latencia, capacidad y calidad en los enlaces de última milla.

1.1. Introducción

El crecimiento de una empresa se basa principalmente en la disponibilidad de los servicios y sistemas que la componen, es por esto por lo que el monitoreo de los mismos es una tarea fundamental dentro de la misma, ya que se puede obtener información importante como inestabilidad, lentitud, perdida de servicio, lo cual afecta la imagen y credibilidad de una institución.

Debido a ello es importante realizar un monitoreo de la red, con el fin de tener los servicios siempre activos, o poder reaccionar proactivamente ante un evento que pueda suscitarse, es importante cumplir con los parámetros de SLA establecidos entre un proveedor y un cliente, para esto es necesario contar con herramientas de monitoreo ya sean estas de pago o gratuitas.

1.2. Antecedentes

Gracias a la información actualizada y a los avances que existen en los diferentes temas de monitoreo, se puede realizar el estudio y análisis

de algunas herramientas ya sean gratuitas o de pago para poder controlar y optimizar una red.

De igual manera, el avance de las diferentes versiones del protocolo SNMP permiten realizar el monitoreo y gestión de la red de una manera mucho más segura, evitando de esta forma posibles ataques de seguridad que puedan afectar el funcionamiento de la red.

1.3. Definición del problema

La existencia de intermitencias o interrupciones del servicio a nivel de enlaces de última milla exige el análisis de estos con el fin de poder contrarrestarlos o minimizarlos de forma adecuada, por este motivo es necesario evitar o erradicar las pérdidas de comunicación a nivel de red, mediante un análisis de parámetros específicos que afectan los enlaces de comunicaciones.

1.4. Justificación del Problema a Investigar.

Los diferentes problemas que se generan dentro de una empresa al presentarse inconvenientes de comunicaciones, pueden generar pérdidas económicas altas y de credibilidad para una institución, debido a la pérdida y desconexión de sus principales sistemas tales como paginas web, en el caso de ser entidades financieras las cuales son altamente transaccionales, servicios de correo interno y externo perdiendo comunicación con clientes y proveedores, servicios internos como sistemas de cobro e intranet necesarios para atender las necesidades de los clientes, para contrarrestar esto se debe contar con un sistema de monitoreo de red el cual se encuentre correctamente configurado, que permita atender las alertas que se generen de forma proactiva teniendo los sistemas siempre activos y operativos para los usuarios y clientes.

1.5. Objetivos

Los objetivos planteados para este trabajo de investigación son los siguientes:

1.5.1. Objetivo General:

Implementar un sistema de monitoreo basado en herramientas gratuitas que permitan garantizar un nivel de servicio adecuado en enlaces corporativos de última milla basados en un SLA prestablecido.

1.5.2. Objetivos específicos:

- ✓ Estudiar la necesidad de realizar el monitoreo de la red.
- ✓ Analizar la conveniencia de una herramienta gratuita o una de pago.
- ✓ Evaluar las diferentes versiones de SNMP y sus prestaciones.
- ✓ Evaluar el rendimiento de una red de acuerdo con las herramientas establecidas.

1.6. Hipótesis

La implementación de un correcto sistema de monitoreo basado en herramientas gratuitas proporcionará los indicadores necesarios para garantizar la correcta disponibilidad del servicio de telecomunicaciones brindado.

1.7. Metodología de investigación.

La metodología a ser utilizada en el presente trabajo se trata de la analítica y descriptiva debido a que se realiza un estudio y análisis de documentos científicos que analizan los protocolos ICMP (Internet Control

Message Protocol) y SNMP como medios de solución para el monitoreo de red.

Se trata de una investigación cuantitativa debido a que se realizara una interpretación de los parámetros obtenidos con las herramientas de monitoreo implementadas, los cuales serán visualizados en gráficas mostrando los porcentajes y valores para los parámetros analizados.

Capítulo 2: Fundamentación Teórica

En este capítulo se realizará un análisis de la importancia del monitoreo de la red, cuáles son las herramientas que mejor se ajustan a cada necesidad dependiendo de la función que tenga cada empresa, se analizará el protocolo SNMP v3 el cual es utilizado para el monitoreo de la red y elegido debido a la seguridad que le brinda a la misma.

2.1. Introducción al monitoreo de la red

El monitoreo de la red se vuelve una parte muy esencial dentro de una empresa o institución, ya que los sistemas deben encontrarse siempre activos y respondiendo con normalidad, la falla de alguno de los servicios que proporciona una institución puede incurrir en millonarias pérdidas de dinero o en multas impuestas por los organismos o entes de control.

Es por esto por lo que el monitoreo de la red va mejorando día a día, y continúa evolucionando con el pasar del tiempo, debido a que se vuelve un tema muy crítico para la respuesta de los sistemas, cada vez se tienen nuevas herramientas que ayudan al diagnóstico de la red y permiten evaluar y presentar un estado de esta, permitiendo con esto tomar acciones correctivas para el mejoramiento de la red.

2.2. Elección entre una herramienta de monitoreo gratuita frente a una de pago.

Se realizará el análisis de algunas de las principales herramientas utilizadas para el monitoreo de la red, analizando las diferentes alternativas de pago y gratuitas, se hará un análisis de las características

que brinda cada una de ellas y como llegar a su elección y verificar como aportan al crecimiento de una empresa.

2.2.1. Herramientas de monitoreo gratuitas

Entre las principales aplicaciones de monitoreo gratuitas se tienen las herramientas del Cacti y Nagios, las cuales son herramientas versátiles totalmente configurables que permiten la monitorización de una red.

A continuación, se estudiará cada una de ellas:

2.2.1.1. Cacti

La herramienta Cacti es de libre distribución, la cual se basa en gráficas, utiliza RRDTool (Round Robin Database Tool – Bases de datos circulares) para el manejo de gráficas siendo estas bastantes potentes y atractivas. RRDTool es una herramienta muy extendida para almacenar series de datos numéricas en escalas de tiempo. Cacti cuenta con una base de datos relacional la cual es utilizada para almacenar información sobre las gráficas, informes y demás detalles, pero en esta no se guarda o procesa información que se visualiza en las gráficas.

Es una herramienta que permite la monitorización y visualización de dispositivos conectados a una red y que tengan configurado el protocolo SNMP, con esta herramienta se logra visualizar el ancho de banda consumido, detectar congestiones o picos de tráfico, monitorear equipos o puertos de red.

La herramienta permite realizar el monitoreo de cualquier equipo que soporte el protocolo SNMP siempre y cuando se conozcan las MIBs

(Management Information Base - Base de Informacion de Gestion) y OIDs (Object Identifiers - Identificador de Objeto) de los equipos a ser monitoreados.

Cacti es una herramienta muy útil que cuenta con templates para algunos fabricantes, equipos, servicios, además de que permite la elaboración de templates a medida.

2.2.1.2. Nagios

La herramienta Nagios de igual manera es de libre distribución, la cual se basa en estados, generando alertas y alarmas cuando el comportamiento de los equipos monitoreados no es el esperado, esta herramienta ayuda monitoreando la disponibilidad de la red.

Proporcionar una alta disponibilidad en los sistemas de comunicación, es una de las tareas más complejas de los administradores de red, sin embargo, es posible brindar un servicio adecuado, al contar con una herramienta que permita detectar posibles errores o fallos para corregirlos en un tiempo prudencial.

Nagios de igual manera realiza el monitoreo de los equipos de red mediante SNMP, monitoreando parámetros como: procesamiento, disco, memoria, puertos, etc.

La herramienta en su panel frontal permite realizar el monitoreo de los equipos de red ya sea por estados o por servicios, la sección de monitoreo por estados permite verificar si un equipo se encuentra operando de manera normal, es decir, se tiene respuesta del mismo, si presenta alguna alarma o si el equipo se encuentra caído ya que no se tendría respuesta del mismo, con esto se podría analizar la disponibilidad de los equipos monitoreados.

En la sección de monitoreo por servicios se puede validar la calidad del servicio que se brinda o recibe, se pueden monitorear varios servicios tales como: ICMP, HTTP (Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto), ssh (Secure Shell – Protocolo de Administracion Remota), etc., verificando si existe alguna degradación o si se encuentran funcionando con normalidad.

Mediante el análisis de los parámetros indicados, el administrador de red puede tomar una decision para solventar los inconvenientes que se presenten dentro de la infraestructura.

También incluye una sección de informes de disponibilidad, la cual es de mucha utilidad cuando se tienen que entregar informes basados en un SLA establecido, y los parámetros deben encontrarse dentro un rango establecido en el mismo.

2.2.2. Herramientas de monitoreo de pago

Entre las principales herramientas de pago se analizaran Pandora FMS, ManageEngine y Orion de SolarWinds.

2.2.2.1. Pandora FMS

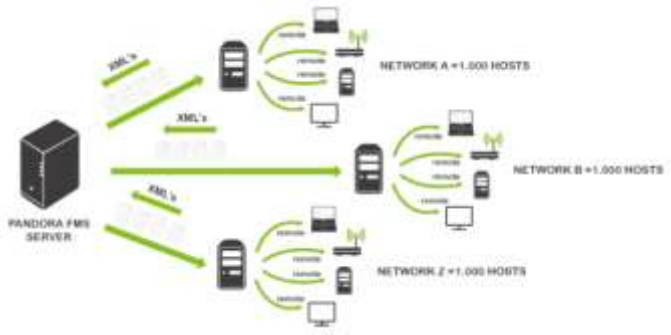


Figura 2.1: Software de Monitoreo Pandora FMS

Fuente: (PandoraFMS, 2018)

Pandora FMS es una herramienta versátil que cuenta con muchas características adicionales a las que cuentan las herramientas del cacti y nagios, esta herramienta permite un monitoreo en tiempo real de la red o conocido como Netflow, adicional permite visualizar gráficas y el estado de la red mediante el monitoreo de equipos con ping, además realiza un mapa y descubrimiento automático de la red en capa 2 y 3 del modelo OSI, también permite visualizar gráficas de consumo de tráfico de una interfaz mediante SNMP, ver tiempos de latencia o disponibilidad de un servicio.

2.2.2.2. ManageEngine

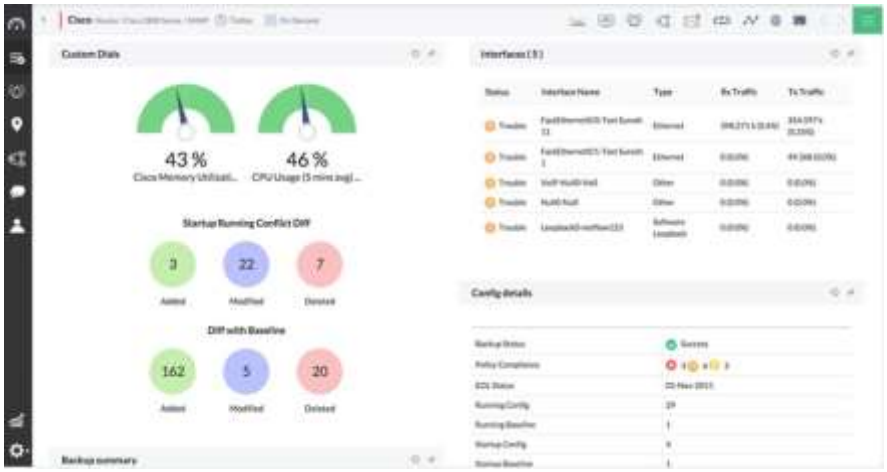


Figura 2.2: Software de monitoreo OpManager

Fuente: (ManaEngine, 2018)

Es un software popular utilizado por la mayoría de los administradores de TI, el cual hace uso de licencias freeware la cual permite evaluar la herramienta para un número limitado de equipos permitiendo en lo posterior migrar a una licencia pagada después de haber probado el producto.

La herramienta permite el monitoreo de red de la gran mayoría de equipos de red tales como: routers, switch, firewalls, servidores, para

conocer su estado y disponibilidad enviando alarmas vía correo electrónico o SMS cuando se ha detectado un problema.

La herramienta cuenta también con un set de gráficas muy útiles, y de informes para analizar el rendimiento de los equipos de red en un periodo de tiempo específico.

2.2.2.3. Orion – SolarWinds

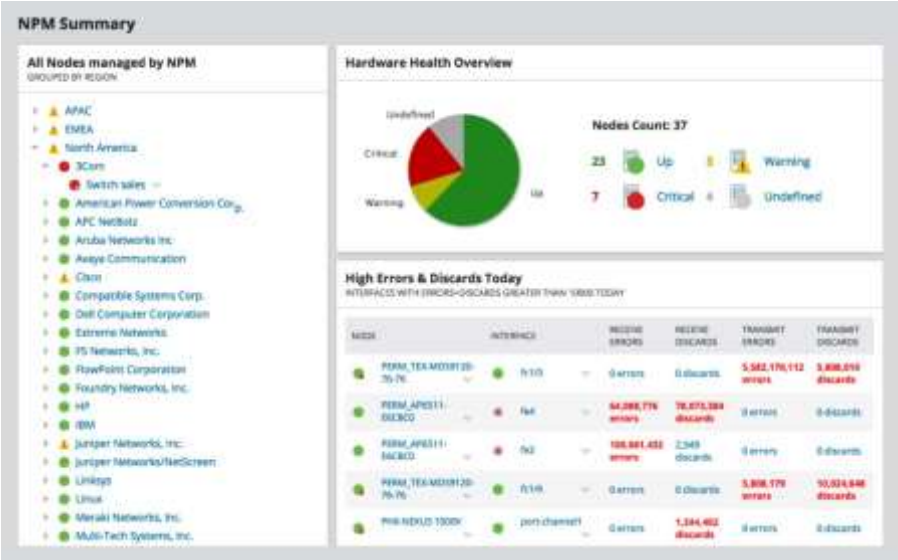


Figura 2.3: Software de monitoreo Orion de Solarwinds

Fuente: (Solarwinds, 2018)

Orion, es una herramienta de monitoreo de red de pago, la cual utiliza el módulo NPM (Network Performance Monitor – Monitoreo de Rendimiento de Red) para realizar el monitoreo de red, esta herramienta permite un periodo de evaluación de 30 días totalmente funcional, luego de este periodo se tendrá que evaluar si se desea o no adquirir la misma.

La herramienta brinda algunas características claves de monitoreo como:

- Monitorear equipos de red de varios proveedores.

- Monitoreo de flujo de rutas con NetPath.
- Análisis de desempeño mediante un panel.
- Alarmas inteligentes.

Es una herramienta bastante intuitiva y configurable, además de personalizable, la cual permite realizar el monitoreo de fallas, medir el desempeño y la disponibilidad de los equipos de red de varias marcas de proveedores mediante la detección, diagnóstico y resolución por parte de los administradores de red.

La herramienta también permite realizar el análisis de la señal wifi, así como realizar su mejoramiento mediante la implementacion de un mapa de cobertura, brinda informes de la red inalámbrica tanto de disponibilidad y puntos de acceso que sean dudosos.

Permite la creación de una línea base del desempeño de la red, estableciendo umbrales de acuerdo con parámetros históricos.

2.3. SNMP

El Protocolo Simple de Administración de Red o SNMP es un protocolo de la capa de aplicación del modelo OSI/TCP-IP (Open System Interconnection – Interconexión de sistemas abiertos) / (Transmission Control Protocol-Internet Protocol - Protocolo de Control de Transmisión-Protocolo de Internet) que utiliza los puertos UDP (User Datagram Protocol – Protocolo de Datagramas de Usuario) 161 y 162, este protocolo facilita el intercambio de información de administración entre dispositivos de red de una manera común existiendo un Gestor o controlador y un agente o controlado. Mediante los mensajes SNMP los cuales pueden ser de monitoreo o lectura (get) y de control o escritura (set) se puede supervisar el rendimiento y desempeño de la red, solventar inconvenientes y planificar un crecimiento a futuro.

El protocolo SNMP trabaja de dos maneras, la primera en la cual realiza un polling utilizando el puerto UDP 161 y la segunda mediante la cual recibe traps por el puerto udp 162, el polling consiste en realizar consultas remotas de forma activa o bajo demanda, lo cual resulta en una operación síncrona, mientras que los traps son mensajes enviados por los equipos monitoreados a una dirección especifica cuando existen cambios o eventos de forma asíncrona.

SNMP cuenta con tres versiones SNMPv1, SNMPv2 y SNMPv3, siendo la última la que brinda algunas opciones adicionales de seguridad que las anteriores dos versiones por lo que se la está utilizando cada vez más.

2.3.1. Monitorización SNMP por Polling

Este método consiste en enviar un chequeo hacia la ip de un equipo utilizando para ello la comunidad SNMP previamente configurada, la comunidad SNMP es una cadena alfanumérica, la cual añade una barrera de seguridad cuando se consulta un equipo, se puede realizar una prueba desde un equipo linux mediante el comando snmpwalk.

A continuación, se presentan dos ejemplos para consultas de snmp tanto para la versión dos y tres del protocolo.

En el servidor desde el cual se desea realizar la prueba se debe ejecutar el siguiente comando para visualizar la información que se necesita:

snmpwalk -v 2c -c <comunidad> <ip>

Obteniendo información acerca del equipo como fabricante, versión de software, estado de las interfaces, etc.

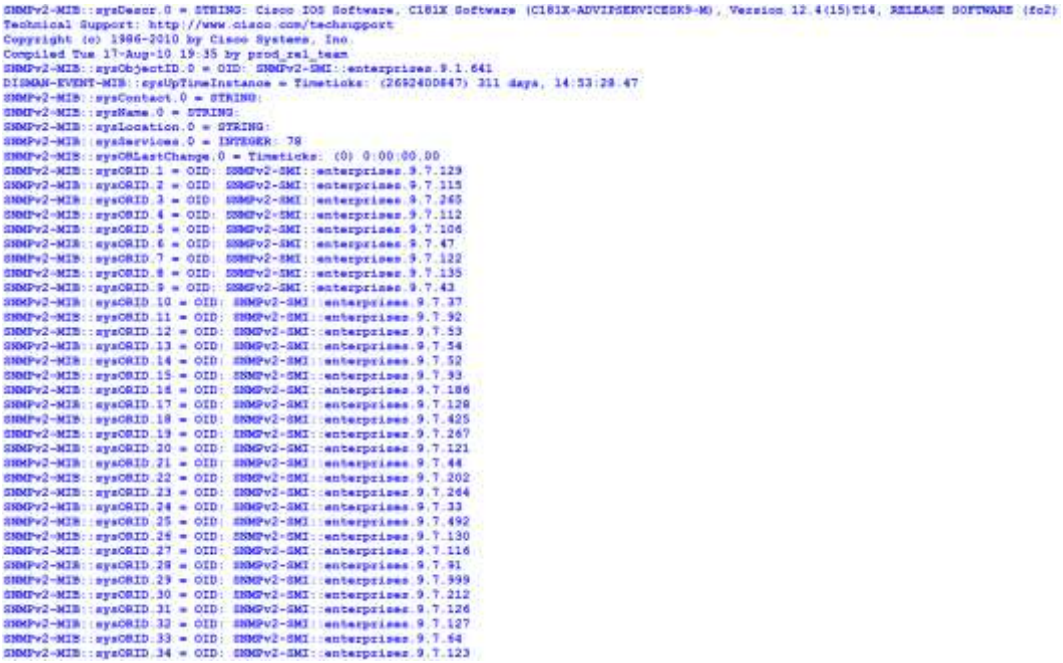


Figura 2.4: Consulta SNMP v2 realizada a un router Cisco

Fuente: El autor

La consulta snmp para la versión tres del protocolo se la realiza de la siguiente manera:

snmpgetnext -v 3 -n "" -u <usuario> -a SHA -A <clave> -x AES -X <clave> -l authPriv <ip> system

```
SNMPv2-MIB::sysDescr.0 = STRING: RouterOS RB750
```

Figura 2.5: MIB obtenida al realizar una consulta SNMP con v3

Fuente: El autor

snmpgetnext -v 3 -n "" -u <usuario> -a SHA -A <clave> -x AES -X <clave> -l authPriv <ip> sysUpTime

```
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (441100) 1:13:31.00
```

Figura 2.6: MIB obtenida al realizar una consulta SNMP con v3

Fuente: El autor

Cada una de las líneas que se visualizan al ejecutar el comando contiene un OID, el cual brinda información importante acerca del dispositivo que se está monitoreando, para entender de mejor manera los OIDs se deben instalar las MIBs de los fabricantes las cuales son librerías que traducen las cadenas numéricas obtenidas a un formato entendible.

2.3.2. Monitorización SNMP por Traps

Para trabajar con este método, se deben configurar los equipos que están siendo monitoreados para que envíen las alertas de acuerdo con las situaciones que se especifiquen, se debe contar con una herramienta que recepte los traps enviados por los equipos para su revisión.

Los traps se los pueden receptar en un sistema operativo Linux en el cual se tenga instalado el demonio snmptrapd.

Este demonio se lo puede instalar de la siguiente manera:

yum install net-snmp-utils net-snmp-libs net-snmp

Figura 2.7: Instalacion de snmptrapd

Fuente: El autor

2.3.3. OID y MIB

El OID es el principal fragmento de información, el cual identifica exactamente el valor a leer (get) o a escribir (set). Al conjunto de OID que dispone un dispositivo se lo llama MIB, el cual se asemeja a un índice en forma de árbol, en el cual se puede encontrar la información que se busca.

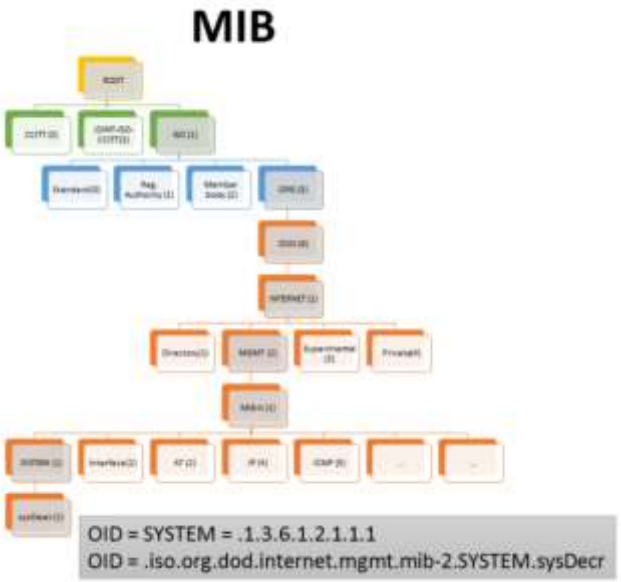


Figura 2.8: Estructura de una MIB

Fuente: (INCIBE, 2017)

La MIB se encuentra estructurada en una jerarquía, la cual permite el correcto orden de cada objeto que este siendo monitoreado, asi como evitando que estos se dupliquen o que existan incongruencias.

A un objeto se lo puede identificar de dos maneras, la primera forma es mediante la cadena texto en la cual se indica cada objeto de la jerarquía, y la segunda mediante la cadena numérica que tiene cada eslabon del árbol de la MIB.

En la Figura 2.9 se muestra un objeto identificado por su cadena numérica.

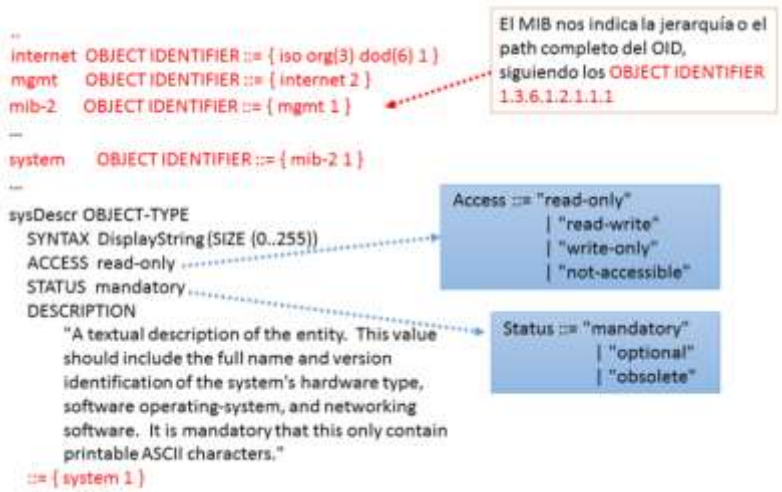


Figura 2.9: Object identifier de una MIB

Fuente: (INCIBE, 2017)

El PDU (Protocol Data Unit – Unidad de Datos de Protocolo) de un mensaje SNMP esta conmpuesto de la siguiente manera como se muestra en la Figura 2.10.

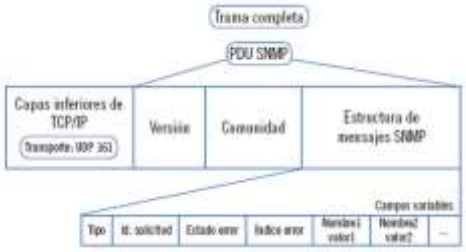


Figura 2.10: PDU de un mensaje SNMP

Fuente: (Calvo, 2015)

2.4. Diferencias entre las distintas versiones de SNMP.

A continuación, se realizará el análisis de las tres versiones del protocolo SNMP que existen en la actualidad.

2.4.1. SNMP v1

Esta versión contaba unicamente con las funciones de GetRequest, GetNextRequest, GetResponse, SetRequest y Trap, además de presentar

algunos problemas como la recolección de datos, así como la seguridad que brindaba el protocolo, por ejemplo, para obtener una tabla MIB se tenia que realizar en reiteradas ocaciones la funciones GetRequest y GetNextRequest.

Para el problema de seguridad, se podía implementar una comunidad la cual viaja en texto plano, es decir sin cifrar y asignar permisos a los objetos que van a ser leidos dentro de la MIB, brindando con esto una pequeña barrera de seguridad al protocolo.

2.4.2. SNMP v2

En esta version se modifican algunos campos de la PDU, permitiendo la implementación de nuevas funcionalidades como son GetBulkRequest e InformRequest, asi como el mejoramiento de las funciones que existían en la versión uno.

La funcionalidad de GetBulkRequest permite obtener grandes volúmenes de información, evitando de esta manera tener que realizar continuamente las funciones GetRequest y GetNextRequest.

La funcionalidad de Inform Request permite enviar un acuse de recibo entre el NMS (Network Management System - Sistema de Administracion de Red) por sus siglas en ingles y el agente.

2.4.3. SNMP v3

La versión tres del protocolo resuelve de gran manera el problema de seguridad que existía en las anteriores versiones, añadiendo parámetros de encriptación y autenticación para poder realizar el monitoreo.

Se añade un campo dentro de la PDU del protocolo, al cual se lo conoce como USM (User-based Security Model – Modelo de Seguridad de Usuario), el cual permite el acceso a la información mediante usuario y clave, así como la autenticación.

La integridad de la información se la garantiza mediante huellas digitales generadas con una función de hash, ya sea con MD5 (Message Digest) o con SHA (Secure Hash Algoritm).

A continuación, en la Figura 2.11 se muestra la PDU del protocolo SNMPv3.

Figura 2.11: PDU del protocolo SNMPv3

Fuente: (Calvo, 2015)

2.5. Tipos de mensajes enviados en SNMP

Los tipos de mensajes que se envían entre el agente y el NMS ya sea para polling o traps son los siguientes:

Tabla 2.1: Mensajes enviados entre el NMS y el agente

Mensaje	Sentido	Operacion
GetRequest	NMS ➔Agente	Lectura
GetNextRequest	NMS ➔Agente	Lectura
GetResponse	Agente ➔ NMS	Respuesta
SetRequest	NMS ➔Agente	Escritura
GetBulkRequest	NMS ➔Agente	Lectura
Inform Request	NMS ➔ NMS Agente ➔ NMS	Notificacion
Trap	Agente ➔ NMS	Notificacion

Fuente: (Calvo, 2015)

2.6. Criterios para la selección adecuada de una solución de monitoreo de red

El monitoreo de red es un tema que va mucho más allá de verificar los consumos de ancho de banda, analizar la perdida de paquetes o comprobar los tiempos de latencia, primero se debe conocer si existe conectividad de un punto a otro lo cual se lo verifica con el ping (Packet Internet Groper).

Otras de las bondades con las que debe contar un sistema de monitoreo es poder tener la capacidad de trabajar con flujos de red conocido como NetFlow, visualizando de esta manera en tiempo real el consumo de la red.

Las herramientas deben manejar históricos de los eventos generados durante los monitoreos, así como la capacidad para poder gestionarlos, además de brindar al personal dedicado al monitoreo las alarmas necesarias para comenzar a identificar un problema que se este generando.

El manejo de alarmas puede recibirse mediante correo electrónico, o por un mensaje de texto, al contar los sistemas de monitoreo con estas facilidades permite al personal encargado de monitorear la red enfocarse en mejoras u otras implementaciones para el bien del negocio.

2.6.1. Elección de la mejor alternativa

Existen varias herramientas de monitoreo como las ya mencionadas, ya sean gratuitas o de pago, depende muchas veces del presupuesto que una empresa tenga asignado a invertir en el fortalecimiento de su parte tecnológica para elegir cada una de ellas, si lo que se desea es una herramienta gratuita que cumpla con la parte de

monitoreo de red, informes y alarmas se puede trabajar con las herramientas de Cacti y Nagios, las cuales han sido elegidas para la implementación y análisis de los diferentes indicadores establecidos en este trabajo de investigación.

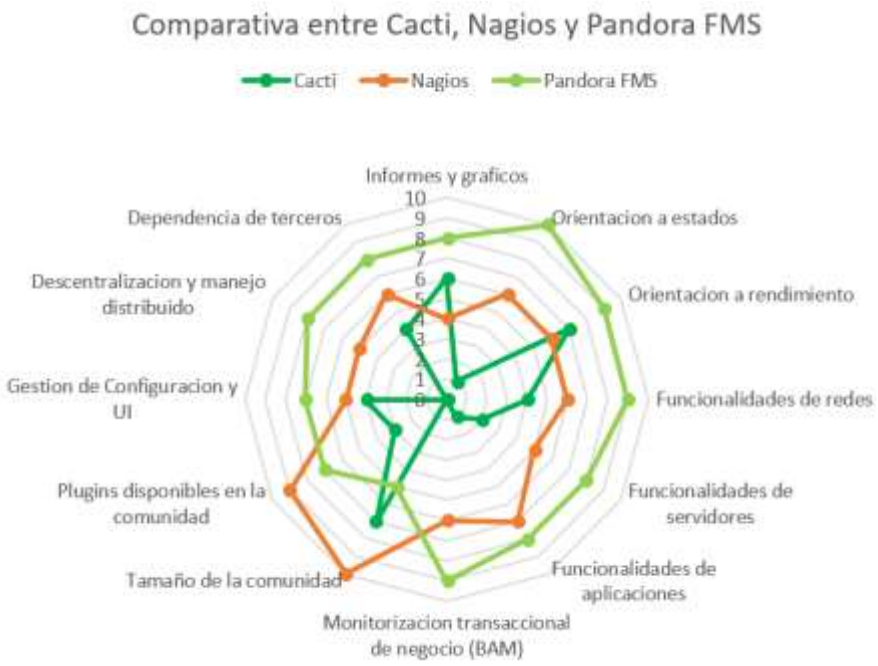


Figura 2.12: Comparativa entre las diferentes herramientas analizadas

Fuente: El Autor

Capítulo 3: Instalación y Configuración de las herramientas de monitoreo Cacti y Nagios

A continuación, se presentarán los requisitos que son necesarios para la instalación y configuración de las herramientas seleccionadas, así como su despliegue para entornos empresariales.

3.1. Instalación y configuración de la herramienta Cacti

La herramienta Cacti es una herramienta de monitoreo web y una solución de monitoreo gráfica para negocios de TI (Tecnología de la Información). Cacti permite realizar un sondeo de servicios en un intervalo regular creando gráficas mediante la utilización de RRDtool.

La instalación de la herramienta se la ha realizado en la distribución de Linux denominada CentOS 7 (Community ENTerprise Operating System), la cual se la utiliza en entornos empresariales debido a su excelente rendimiento en servidores.

La instalación de la herramienta se la realizara utilizando los repositorios de Linux, es necesario contar con algunos paquetes adicionales para su correcto funcionamiento, estos paquetes se los pueden descargar de igual manera utilizando los repositorios de Linux.

La herramienta se basa en un poller (sondeo), el cual realiza un monitoreo de los equipos ingresados de forma secuencial, este poller presenta un buen rendimiento para una red pequeña de alrededor 20 a 25 equipos, este rendimiento se lo puede optimizar instalando un plugin llamado cacti-spine el cual abre múltiples hilos de conexión por cada poller que se esté realizando, con esto la carga del sistema mejora de gran manera sin llegar a saturarlo.

Los paquetes requeridos por Cacti para su implementación son los siguientes:

- **Apache** – Es un servidor web en el cual se visualizarán los gráficos de red creados por PHP (Hypertext Preprocessor) y RRDTool.
- **MySQL** – Es un servidor de base de datos en el cual se almacenará la información del cacti.
- **PHP** – Un script para la creación de gráficos usando RRDTool.
- **PHP-SNMP** – Se trata de una extensión de PHP para SNMP con la cual se accederá a los datos.
- **NET-SNMP** – El protocolo SNMP que permitirá el manejo de los datos de la red.
- **RRDTool** – Es una herramienta de base de datos, que permite el manejo y recuperación de datos en el tiempo como carga de CPU, red, ancho de banda, etc.

Los pasos para realizar la instalación de la herramienta pueden ser consultados en el Anexo I del presente trabajo de investigación.

Luego de haber instalado la herramienta de monitoreo, se visualiza la pantalla principal, la cual consta de los paneles que se muestran en la siguiente figura:

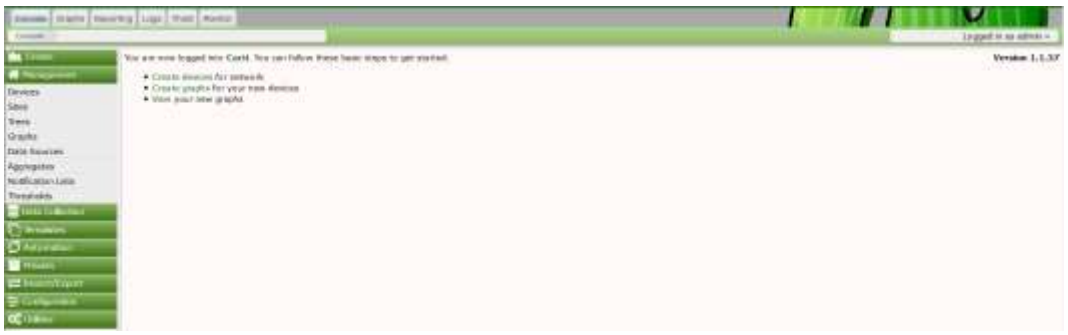


Figura 3.1: Panel principal de la herramienta instalada

Fuente: El autor

Las principales ventanas de la herramienta son las que se muestran a continuación en la cual se realiza la configuración SNMP, spine, envío de notificaciones.

Figura 3.2: Configuración del protocolo SNMP

Fuente: El autor

Figura 3.3: Elección de cacti spine

Fuente: El autor

Figura 3.4: Configuración del envío de notificaciones

Fuente: El autor

3.2. Instalación y configuración de Nagios

La herramienta de nagios es un software libre bajo la licencia de GPL2 (General Public License v2.0 – Licencia Pública General v2.0), el cual permite realizar el monitoreo centralizado de los equipos de red utilizando protocolos como ICMP y SNMP, etc. con el cual se puede llegar a conocer el estado de carga de CPU, espacio en disco, memoria, estado de los puertos de red, generando alarmas cuando se presentan condiciones no deseadas.

La visualización de la herramienta se la realiza vía web utilizando un navegador, en el cual se incluye información sobre el estado de los servicios que se hayan definido, así como la disponibilidad de los equipos y una lista en la cual se detallan la lista de host y problemas presentados.

El monitoreo de servicios se lo puede realizar por cualquier de los siguientes protocolos que se definen a continuación:

- SMTP (Simple Mail Transfer Protocol - Protocolo para Transferencia Simple de Correo)
- HTTP
- FTP (File Transfer Protocol – Protocolo de Transferencia de Archivos)
- ICMP

De acuerdo con las respuestas obtenidas a cada una de estas consultas, se puede llegar a conocer el estado de los servicios definidos para los hosts monitoreados.

La información de los equipos se la puede obtener mediante el protocolo SNMP, para esto es necesario que el equipo a ser monitoreado cuente con el protocolo activo, y permita la configuración de este.

También se puede obtener información de un equipo utilizando un agente llamado NRPE (Nagios Remote Plugin Executor), el cual es un aplicativo de Nagios que debe ser instalado en un servidor con las plataformas Linux, Windows, Mac y otras distribuciones Linux/Unix. El agente permite la definición de comandos internos, con los cuales se puede realizar el monitoreo de elementos locales del sistema a través de la ejecución de plugins.

Para la instalación de la herramienta se deben contar con los siguientes prerrequisitos los cuales se detallan a continuación:

- Apache
- MySQL
- PHP
- PHP MYSQL

Los pasos para realizar la instalación de la herramienta pueden ser consultados en el Anexo II del presente trabajo de investigación.

Luego de haber instalado la herramienta de monitoreo, se visualiza la pantalla principal la cual consta de los paneles que se muestran en la siguiente figura:

Figura 3.5: Página principal de nagios

Fuente: El autor

Figura 3.6: Pestaña de visualización para el monitoreo de hosts

Fuente: El autor

Figura 3.7: Pestaña de visualización para el monitoreo de servicios de hosts

Fuente: El autor

Para realizar la configuración de la herramienta, se debe acceder a los siguientes directorios /usr/local/nagios/etc y /usr/local/nagios/etc/objects, en los cuales se encuentran varios archivos que desempeñan varias funciones para la manipulación de la herramienta.

```
1143128 -rw-rw-r--. 1 nagios nagios 12999 May 22 23:30 cgi.cfg
1143158 -rw-rw-r--. 1 nagios nagios 12999 May 22 23:22 cgi.cfg~
1143140 -rw-r--r--. 1 root   root      50 May 22 23:41 htpasswd.users
1143127 -rw-rw-r--. 1 nagios nagios 44816 May 22 23:30 nagios.cfg
1143157 -rw-rw-r--. 1 nagios nagios 44816 May 22 23:22 nagios.cfg~
1139316 -rw-r--r--. 1 nagios nagios  7988 May 22 23:38 nrpe.cfg
34663573 drwxrwxr-x. 2 nagios nagios  4096 May 22 23:30 objects
1143129 -rw-rw----. 1 nagios nagios  1312 May 22 23:30 resource.cfg
1143159 -rw-rw----. 1 nagios nagios  1312 May 22 23:22 resource.cfg~

34634993 -rw-rw-r--. 1 nagios nagios  7696 May 22 23:30 commands.cfg
34663575 -rw-rw-r--. 1 nagios nagios  7696 May 22 23:22 commands.cfg~
34634994 -rw-rw-r--. 1 nagios nagios  2138 May 22 23:30 contacts.cfg
34663576 -rw-rw-r--. 1 nagios nagios  2138 May 22 23:22 contacts.cfg~
34634996 -rw-rw-r--. 1 nagios nagios  5379 May 22 23:30 localhost.cfg
34663578 -rw-rw-r--. 1 nagios nagios  5379 May 22 23:22 localhost.cfg~
34634998 -rw-rw-r--. 1 nagios nagios  3069 May 22 23:30 printer.cfg
34663580 -rw-rw-r--. 1 nagios nagios  3069 May 22 23:22 printer.cfg~
34634999 -rw-rw-r--. 1 nagios nagios  3252 May 22 23:30 switch.cfg
34663581 -rw-rw-r--. 1 nagios nagios  3252 May 22 23:22 switch.cfg~
34634992 -rw-rw-r--. 1 nagios nagios 10595 May 22 23:30 templates.cfg
34663574 -rw-rw-r--. 1 nagios nagios 10595 May 22 23:22 templates.cfg~
34634995 -rw-rw-r--. 1 nagios nagios  3178 May 22 23:30 timeperiods.cfg
34663577 -rw-rw-r--. 1 nagios nagios  3178 May 22 23:22 timeperiods.cfg~
34634997 -rw-rw-r--. 1 nagios nagios  3991 May 22 23:30 windows.cfg
34663579 -rw-rw-r--. 1 nagios nagios  3991 May 22 23:22 windows.cfg~
```

Figura 3.8: Archivos de configuración para la herramienta nagios

Fuente: El autor

En la Tabla 3.1, se indican los parámetros que se pueden configurar en los archivos para poder agregar servicios y hosts para ser monitoreados por la herramienta.

Tabla 3.1: Archivos de configuración para Nagios

Archivo - Directorio	Función
/usr/local/nagios/etc/nagios.cfg	Archivo para la configuración principal de nagios
/usr/local/nagios/etc/cgi.cfg	Archivo para la configuración de la consola web de nagios
/usr/local/nagios/etc/objects	Directorio que contiene una serie de configuraciones de diversos objetos base como comandos (commands.cfg), contactos (contacts.cfg), dispositivos o servidores (printer.cfg, switch.cfg) y otras definiciones de servicios o hosts (templates.cfg, timeperiods.cfg).
/usr/local/nagios/etc/conf.d/	Directorio vacío por defecto en el cual se realiza la creación de archivos .cfg propios para tener los hosts por separado

Fuente: El autor

Capítulo 4: Resultados y Análisis de las herramientas de red utilizadas

4.1. Análisis y resultados de la herramienta Cacti

Luego de haber implementado la herramienta de monitoreo Cacti, la cual permite realizar el análisis de la capacidad, y latencia de los enlaces corporativos, parámetros que están siendo analizados en el presente trabajo de investigación, se va a realizar el análisis de ésta.

El análisis de la capacidad de los enlaces es un parámetro muy importante, ya que, con este parámetro, se puede llegar a conocer si un enlace se encuentra saturado o no, al encontrarse saturado se corre el riesgo de brindar un mal servicio tanto a los usuarios internos como externos, ya que existirán perdidas de paquetes, lo cual ocasionara intermitencia dentro de la red, lo cual repercutirá en que los sistemas no se conecten y puedan trabajar de una manera adecuada. De igual manera cuando se presenta saturación de los enlaces, los tiempos de latencia se incrementan, y al encontrarse un enlace saturado, debe analizarse la opción de realizar un upgrade (incremento) del ancho de banda del enlace que se encuentre afectado.

El análisis de la latencia se lo realiza mediante el protocolo ICMP con el cual se puede saber si un equipo presenta algún problema, o si un enlace se encuentra saturado.

La herramienta permite realizar la agrupación de los equipos monitoreados de la forma en la que se desee, para llevar un control adecuado de la red.

En la Figura 4.1 se pueden observar dos agrupaciones que se han realizado a los equipos monitoreados, logrando con esto realizar un mejor monitoreo de la red y mantener un orden adecuado de la misma.

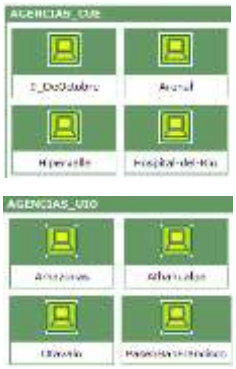


Figura 4.1: Agrupación de equipos monitoreados

Fuente: El Autor

De igual manera se han monitoreado equipos Windows y Linux lo cual se lo puede observar en la Figura 4.2, creando un template (plantilla) para cada uno de ellos, con esto pueden ser visualizados de mejor manera y asi se mantiene un agrupamiento organizado de los equipos.

Figura 4.2: Monitoreo de equipos Windows y Linux

Fuente: El autor

La herramienta de igual manera permite configurar un plugin (complemento), para poder observar una gráfica en específico, como se lo muestra en la Figura 4.3.

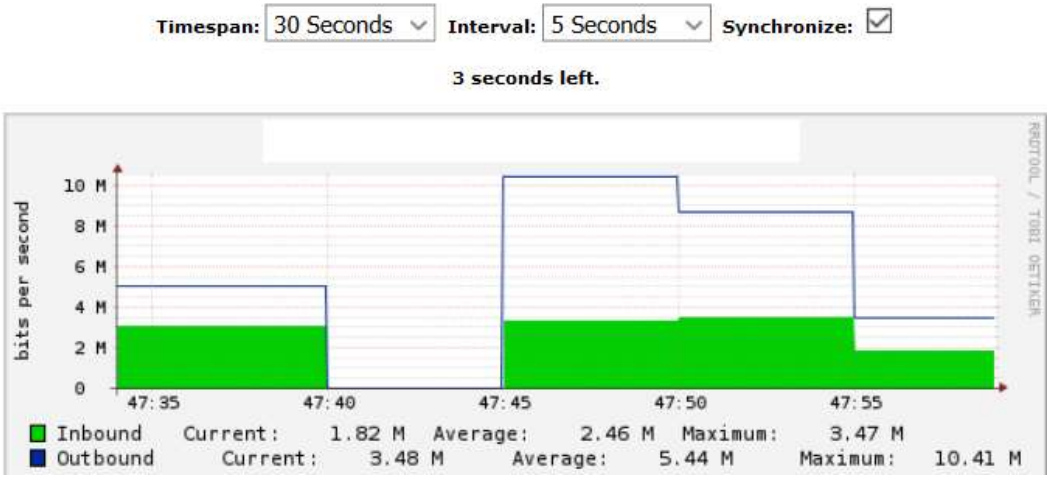


Figura 4.3: Consumo en tiempo real de una interfaz

Fuente: El autor

Existen tres estados que pueden llegar a presentarse en los hosts que están siendo monitoreados, en la Figura 4.4 se muestra un equipo que esta siendo monitoreado el cual se encuentra en color verde lo que indica que el dispositivo no presenta inconvenientes.

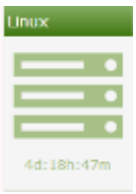


Figura 4.4: Estado normal de un host en la herramienta Cacti

Fuente: El autor

En la Figura 4.5, se muestra el color en el que se pone un host monitoreado, cuando este esta retornando de un estado alarmado hacia un estado normal, a este estado se lo conoce como “recovery” (restablecimiento).

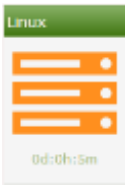


Figura 4.5: Estado de recovery de un host en la herramienta Cacti

Fuente: El autor

En la Figura 4.6 se muestra un host en estado alarmado, el color que adopta el host monitoreado es rojo y puede deberse a una o varias de las siguientes situaciones:

- En enlace se encuentra saturado, por lo que los tiempos de latencia se elevan provocando que el host pase a un estado alarmado.

- Se perdió comunicación con el dispositivo monitoreado por lo que no se recibe una respuesta de ICMP, en estos casos se debe verificar si existen problemas eléctricos en el lugar, o sino reportarlo al proveedor de última milla ya que debe existir algún tipo de inconveniente.

- Otro motivo por el cual un host puede alarmarse, es porque la ip del dispositivo monitoreado fue cambiada, o las configuraciones para el protocolo SNMP fueron modificadas, en estos casos se debe actualizar la ip o configuraciones según sea el caso.

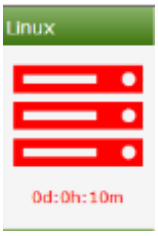


Figura 4.6: Host alarmado dentro de la herramienta cacti

Fuente: El autor

A continuación, se muestra un ejemplo en el cual se verifica que un enlace se encuentra saturado, en estos casos se debe analizar si se realiza el incremento de ancho de banda del canal, o si la saturación puede ser controlada mediante algún mecanismo.

En la Figura 4.7, se puede evidenciar que existe una transferencia de archivos entre dos equipos mediante el protocolo SMB (Server Message Block – Bloque de Mensajes del Servidor), lo cual está ocasionando una saturación del enlace.

Figura 4.7: Saturación del ancho de banda

Fuente: El autor

Lo cual genera que los tiempos de latencia hacia el equipo monitoreado se incrementen, como se puede apreciar en la Figura 4.8.

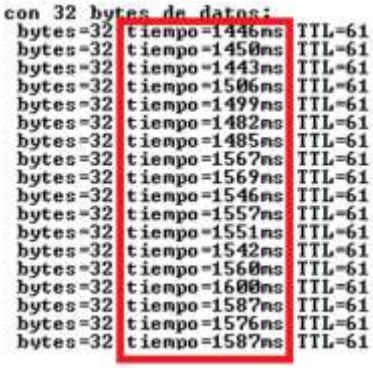


Figura 4.8: Incremento de los tiempos de latencia debido a saturación

Fuente: El autor

La herramienta, permite visualizar el tráfico generado o consumido por un dispositivo en un periodo de tiempo determinado, según se desee analizar.

En la Figura 4.9, se muestra una gráfica de monitoreo durante un periodo de tiempo seleccionado, se puede evidenciar en la gráfica que existió intermitencia en el servicio, esto se lo nota debido a que la gráfica

no es continua, lo cual genera una alerta para analizar que sucedió con ese enlace durante ese periodo de tiempo.

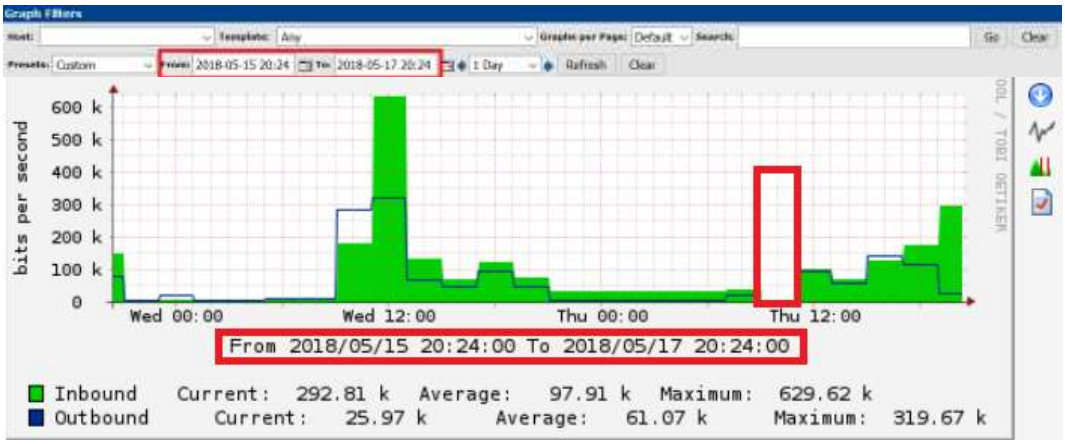


Figura 4.9: Configuración para la visualización de una gráfica en especifico

Fuente: El autor

Es muy importante realizar el análisis de la red que se esté monitoreando, ya que muchas de las veces las gráficas de monitoreo presentan patrones muy parecidos para un dispositivo monitoreado, como se lo puede apreciar en la Figura 4.10 , al verse este patrón afectado se debe identificar qué tipo de problema se está presentando en ese equipo.

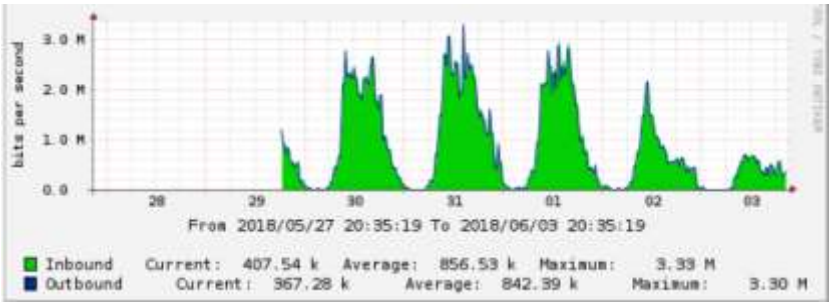


Figura 4.10: Patrón de monitoreo para un host especifico

Fuente: El autor

El envío y configuración correcto de alarmas de igual manera es muy necesario para poder identificar que esta sucediendo con la red, esto permite que el personal que esta a cargo de la administración de esta no este únicamente centrado en el monitoreo, y de esta manera se puedan realizar mejoras continúas a la infraestructura de red.

Figura 4.11: Envío de alarmas al personal encargado de la administración de la red

Fuente: El autor

4.2. Análisis y resultados de la herramienta Nagios

Luego de haber implementado la herramienta de monitoreo nagios, la cual permite realizar el análisis de disponibilidad y calidad de los enlaces corporativos, parámetros que están siendo analizados en el presente trabajo de investigación, se va a realizar el análisis de esta.

Los parámetros de disponibilidad o denominados uptime y los de calidad son muy importantes para la verificación de los SLA's, el parámetro de disponibilidad que entrega la herramienta, es de mucha utilidad para verificar si el proveedor o proveedores están cumpliendo con el acuerdo establecido, así como la calidad del enlace, el cual puede ser analizado en el apartado services de nagios para verificar si existe intermitencia en los enlaces, pérdidas de paquetes, saturación y con esto buscar una solución a un problema presentado y validar si la incidencia es atribuida al cliente o al proveedor.

La herramienta permite organizar los dispositivos monitoreados de diferentes formas, esto con el fin de mantener un orden adecuado, en la Figura 4.12 se muestra el monitoreo que realiza nagios.

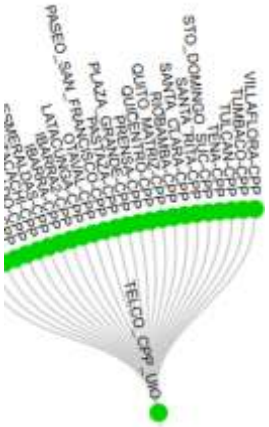


Figura 4.12: Monitoreo realizado en la herramienta nagios

Fuente: El autor

En el apartado denominado “host” se puede visualizar el estado de los dispositivos monitoreados, así como el último chequeo realizado por la herramienta, y el tiempo de disponibilidad desde la última incidencia presentada.

Figura 4.13: Monitoreo de disponibilidad de un dispositivo

Fuente: El autor

En la sección denominada “services”, se puede verificar el estado del servicio que está siendo monitoreado por la herramienta, validar si estos se encuentran funcionando correctamente, o si existen pérdidas de paquetes con el fin de solventar problemas que se presenten con los enlaces.

Figura 4.14: Monitoreo por servicio de un dispositivo

Fuente: El autor

La herramienta permite el ingreso al apartado de disponibilidad dentro de la sección “reportes”, para poder analizar cualquier dispositivo que se necesite, indicando el rango de fecha que se desee examinar, con el fin de detectar problemas en caso de presentarse o realizar un monitoreo rutinario.

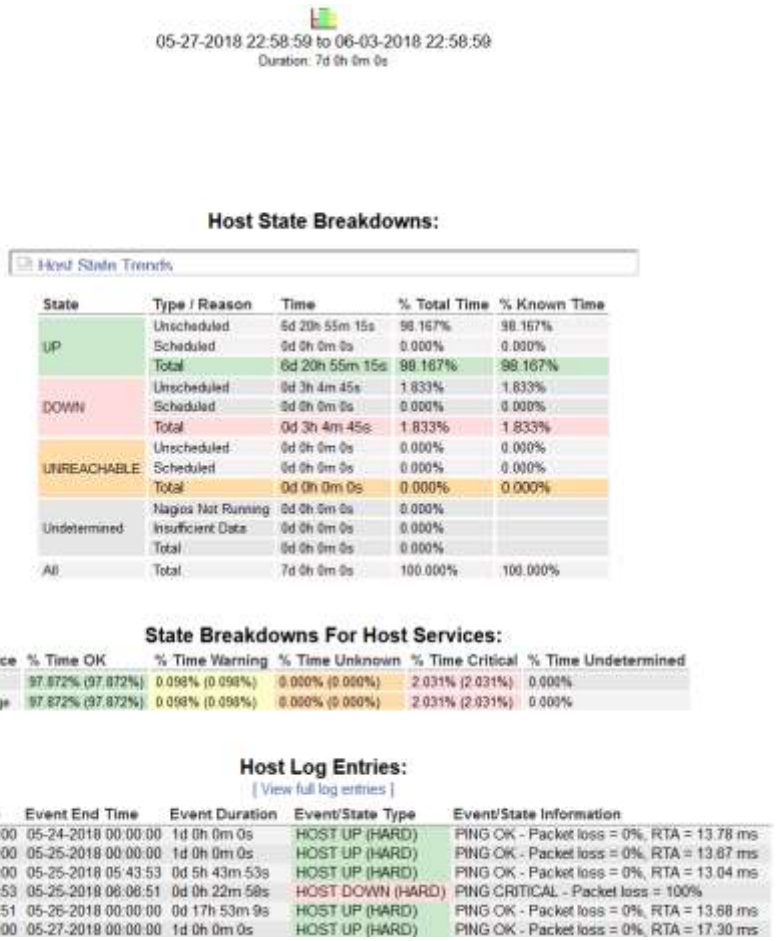
Figura 4.15: Reporte de disponibilidad de un dispositivo monitoreado

Fuente: El autor

En la Figura 4.16, se puede visualizar el porcentaje de disponibilidad que tuvo un dispositivo para los últimos siete días, el cual indica que tuvo un 98.167% de disponibilidad o uptime y un 1.833% de tiempo fuera o downtime.

De igual manera en la misma Figura 4.16, se muestra el comportamiento del servicio de ping realizado hacia ese dispositivo, verificando que respondió el equipo con normalidad un 97.872%, mientras que estuvo en estado de alerta en un porcentaje de 0.098%, y en estado

crítico o sin respuesta paso un 2.031%, los diferentes estados analizados se deben a los cambios presentados en los tiempos de respuesta de ping, validando con esto la calidad del enlace.



05-27-2018 22:58:59 to 06-03-2018 22:58:59
Duration: 7d 0h 0m 0s

Host State Breakdowns:

Host State Trends

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	6d 20h 55m 15s	98.167%	98.167%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	6d 20h 55m 15s	98.167%	98.167%
DOWN	Unscheduled	0d 3h 4m 45s	1.833%	1.833%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 3h 4m 45s	1.833%	1.833%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	97.872% (97.872%)	0.098% (0.098%)	0.000% (0.000%)	2.031% (2.031%)	0.000%
Average	97.872% (97.872%)	0.098% (0.098%)	0.000% (0.000%)	2.031% (2.031%)	0.000%

Host Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
05-23-2018 00:00:00	05-24-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.78 ms
05-24-2018 00:00:00	05-25-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.67 ms
05-25-2018 00:00:00	05-25-2018 05:43:53	0d 5h 43m 53s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.04 ms
05-25-2018 05:43:53	05-25-2018 06:06:51	0d 0h 22m 58s	HOST DOWN (HARD)	PING CRITICAL - Packet loss = 100%
05-25-2018 06:06:51	05-26-2018 00:00:00	0d 17h 53m 9s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 13.68 ms
05-26-2018 00:00:00	05-27-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 17.30 ms

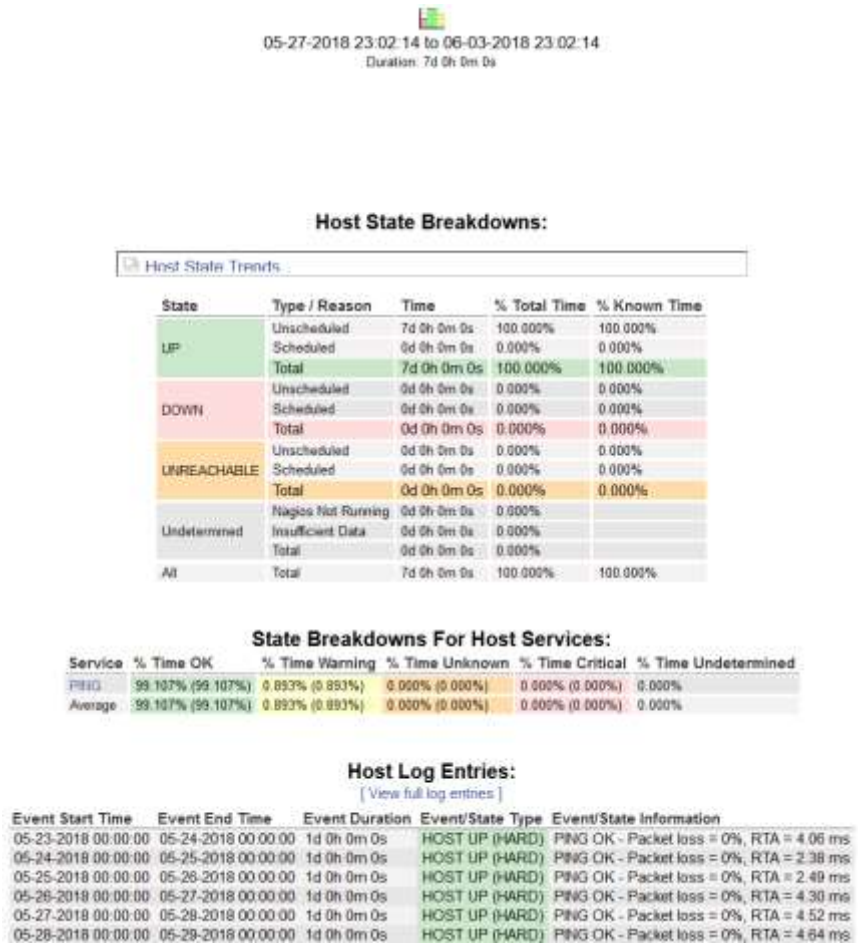
Figura 4.16: Análisis del reporte de disponibilidad de un dispositivo monitoreado

Fuente: El autor

En la Figura 4.17, se puede observar que existe un porcentaje de disponibilidad del 100% del dispositivo analizado, por lo que no se presentaron problemas durante los últimos siete días que están siendo analizados.

En la sección “services” de la misma Figura 4.17, se puede verificar la calidad del enlace del dispositivo, la cual indica que el ping respondió con normalidad un 99.107%, mientras que estuvo en estado alerta en un 0.893%, lo cual pudo ocurrir debido a que el tiempo de latencia del ping

se incrementó por momentos, debido a saturación del enlace o inestabilidad en el mismo, esto no influyo en una pérdida de servicio como lo indica el parámetro de disponibilidad.



05-27-2018 23:02:14 to 06-03-2018 23:02:14
Duration: 7d 0h 0m 0s

Host State Breakdowns:

Host State Trends

State	Type / Reason	Time	% Total Time	% Known Time
UP	Unscheduled	7d 0h 0m 0s	100.000%	100.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	7d 0h 0m 0s	100.000%	100.000%
DOWN	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
UNREACHABLE	Unscheduled	0d 0h 0m 0s	0.000%	0.000%
	Scheduled	0d 0h 0m 0s	0.000%	0.000%
	Total	0d 0h 0m 0s	0.000%	0.000%
Undetermined	Nagios Not Running	0d 0h 0m 0s	0.000%	
	Insufficient Data	0d 0h 0m 0s	0.000%	
	Total	0d 0h 0m 0s	0.000%	
All	Total	7d 0h 0m 0s	100.000%	100.000%

State Breakdowns For Host Services:

Service	% Time OK	% Time Warning	% Time Unknown	% Time Critical	% Time Undetermined
PING	99.107% (99.107%)	0.893% (0.893%)	0.000% (0.000%)	0.000% (0.000%)	0.000%
Average	99.107% (99.107%)	0.893% (0.893%)	0.000% (0.000%)	0.000% (0.000%)	0.000%

Host Log Entries:

[View full log entries]

Event Start Time	Event End Time	Event Duration	Event/State Type	Event/State Information
05-23-2018 00:00:00	05-24-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 4.06 ms
05-24-2018 00:00:00	05-25-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 2.38 ms
05-25-2018 00:00:00	05-26-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 2.49 ms
05-26-2018 00:00:00	05-27-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 4.30 ms
05-27-2018 00:00:00	05-28-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 4.52 ms
05-28-2018 00:00:00	05-29-2018 00:00:00	1d 0h 0m 0s	HOST UP (HARD)	PING OK - Packet loss = 0%, RTA = 4.64 ms

Figura 4.17: Análisis del reporte de disponibilidad de un dispositivo monitoreado

Fuente: El autor

La herramienta permite realizar la configuración para el envio de notificaciones cuando se presente una alarma en específico, y de esta manera se pueda saber que está sucediendo para solventar el inconveniente que se presente.

Figura 4.18: Envio de notificaciones de la herramienta Nagios

Fuente: El autor

Conclusiones y Recomendaciones

Conclusiones

1. Se analizó la necesidad de realizar el monitoreo de red dentro de las empresas, y como esta tarea ayuda de gran manera a reducir las afectaciones que se presentarían al tener enlaces con alarma, adicional se verificó que gracias al monitoreo de red se puede evitar caer en grandes multas impuestas por los entes de control al encontrarse un servicio caído.

2. Se realizó el análisis de las herramientas de monitoreo gratuitas, frente a las de pago, verificando que las herramientas de pago son mas intiuitivas, de fácil instalación, y son mas amigables al usuario, también cuentan con soporte, sus precios varían dependiendo de la necesidad y tamaño de la red que se va a monitorear; por otro lado las herramientas de monitoreo gratuitas requieren que el administrador tenga un conocimiento avanzado de la misma, asi como manejo del sistema operativo en el cual se instalaron el cual es Linux para poder implementarlas.

3. Se determinó que el principal mecanismo para obtener la información necesaria para la herramienta monitoreo es el protocolo SNMP, con el cual se envían mensajes entre el agente y el servidor para verificar el estado de los equipos monitoreados, se analizaron las diferentes versiones del protocolo siendo la mas segura la versión tres del mismo, debido a los algoritmos encripción con los que cuenta, también se ha utilizado la versión dos del protocolo debido a que algunos equipos como Windows o Linux aun no cuentan con la versión tres del mismo.

4. Las herramientas de monitoreo Cacti y Nagios implementadas, brindan las métricas necesarias para poder realizar el análisis de una red y saber que esta ocurriendo con la misma, con la herramienta Nagios se evalúan los parámetros de calidad y disponibilidad, mientras que con la herramienta Cacti se evalúan los parámetros de latencia y capacidad, logrando con esto el administrador de red solventar los problemas que se presenten y de esta manera se pueda mantener una red estable.

5. De acuerdo a un SLA establecido, las herramientas de monitoreo implementadas permiten corroborar si los enlaces se encuentran funcionando dentro de lo normal o caso contrario cobrar las multas del servicio según sea el caso.

Recomendaciones

1. Para la administración de los sistemas de monitoreo, se deben manejar claves seguras, las cuales deben ser distribuidas únicamente al personal encargado.

2. Para realizar la actualización de versión de la herramienta o parche al sistema operativo, se debe realizar un backup de la herramienta de monitoreo, o realizar un clon del servidor en el caso de trabajar en un ambiente virtual.

3. Implementar una herramienta de monitoreo desde cero, en la cual se conozcan todos sus componentes, y se los puedan manipular como se desee, para obtener una herramienta propia que luego pueda ser distribuida.

4. En base a la creacion de la herramienta de monitoreo, se puede llegar a implementar una empresa la cual brinde servicios de monitoreo, pudiendo extenderse a largo plazo.

5. Realizar convenios con empresas, que distribuyan o programen software de monitoreo, con el fin de poder aplicar los conocimientos adquiridos dentro de las mismas.

Referencias Bibliográficas

- Anicas, M. (s.f.). *DigitalOcean*. Obtenido de https://www.digitalocean.com/community/tutorials/how-to-install-nagios-4-and-monitor-your-servers-on-centos-7
- Calvo, A. L. (2015). *Gestión de redes telemáticas.*
- Cavassa, F. (2009). *SAYA COMUNICACIONES S.A.C*. Obtenido de IDG COMUNICACIONES: https://cioperu.pe/articulo/17462/7-herramientas-gratuitas-que-toda-red-necesita/?p=6
- Dinangkur, K., & Lavlu, S. (2009). *Cacti 0.8 Network Monitoring.*
- INCIBE. (2017). *Certsi*. Obtenido de https://www.certsi.es/blog/snmp-tan-simple-el-nombre-indica
- Jens, R. (2010, Actualizado 2017). Introducing SNMP.
- ManaEngine. (2018). *Op Manager*. Obtenido de https://www.manageengine.com/latam/network-monitoring/
- Manzano, J. (2017). *PandoraFMS Monitoring Blog*. Obtenido de https://blog.pandorafms.org/es/cumplimiento-sla/
- Manzano, J. (2017). *PandoraFMS Monitoring Blog*. Obtenido de https://blog.pandorafms.org/es/informes-sla/
- Martínez Tobar, H. (s.f.). *Apuntes Técnicos*. Obtenido de https://hmartineztobar.es/blog/guia-de-instalacion-y-configuracion-de-cacti-en-centos7/
- Mauro, D., & Schmidt, K. (2005). *Essential SNMP.*

- PandoraFMS. (2018). *PandoraFMS Enterprise*. Obtenido de https://pandorafms.com/es/soluciones/monitorizacion-de-redes/
- Saive, R. (s.f.). *TecMint*. Obtenido de https://www.tecmint.com/install-cacti-network-monitoring-on-rhel-centos-6-3-5-8-and-fedora-17-12/
- Solarwinds. (2018). *SolarWinds*. Obtenido de https://www.solarwinds.com/es/orion
- Valdivia Miranda, C. (2014). *Redes telemáticas.*
- Velasco , J. (2011). *HIPERTEXTUAL*. Obtenido de https://hipertextual.com/archivo/2011/01/diez-herramientas-esenciales-administrar-sistemas/

Glosario

F

FTP

File Transfer Protocol 40

G

GPL2

General Public License 39

H

http

Hypertext Transfer Protocol

Es el protocolo de comunicación que permite las transferencias de información en internet..... 23

I

ICMP

Internet Control Message Protocol 19

M

MD5

Message Digest..... 33

MIB

Management Information Base 21

N

NMS

Network Management System 32

NPM

Network Performance Monitor..... 25

NRPE

Nagios Remote Plugin Executor

T

U

W

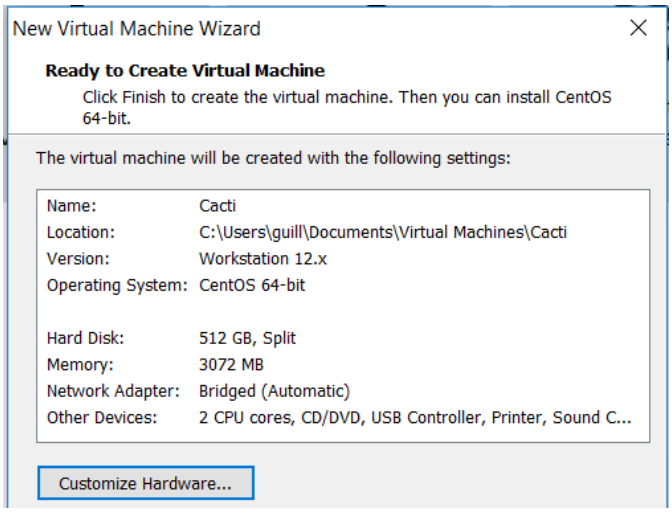
Anexos

Anexo I. Instalación y Configuración de Cacti

La descarga del sistema operativo CentOS, se la realizara desde la página oficial para esta distribución de Linux.

La instalación del sistema operativo se la puede realizar en un entorno virtual o físico, siendo el entorno virtual el más idóneo debido a sus capacidades de respaldo y seguridad que brinda frente a entornos físicos, ya que si el medio físico en el cual se encuentra instalada la herramienta sufriera algún tipo de daño se perdería toda la información y monitoreo.

Para el despliegue de la herramienta se realizará la creación de una máquina virtual, en la cual se alojará el sistema operativo en la plataforma de VMware, para después proceder con la instalación de la herramienta de monitoreo.



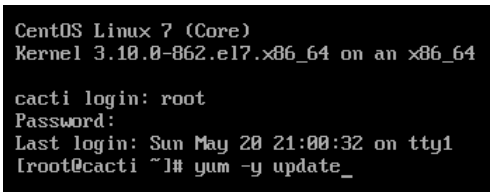
Configuración de la máquina virtual

Posterior a la configuración de la máquina virtual, se realiza la configuración para la distribución de CentOS elegida, los principales parámetros a elegir son: el tipo de servidor del que se trata, la

configuración de la tarjeta de red, creación y configuración de usuarios para el sistema.

Configuración de CentOS

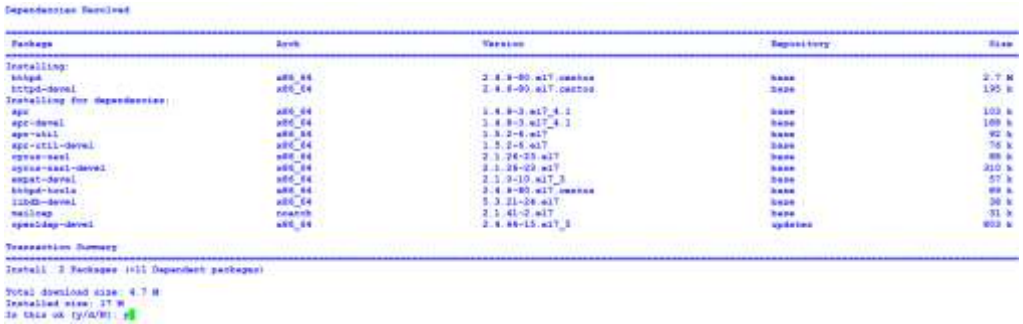
Despues de haber instalado el sistema operativo, lo primero que se tiene que realizar es la actualización del mismo de la siguiente manera:



Actualización del sistema operativo

Una vez que el sistema operativo se encuentra actualizado y listo, se procede a realizar la instalación de la herramienta cacti, con cada uno de los componentes necesarios.

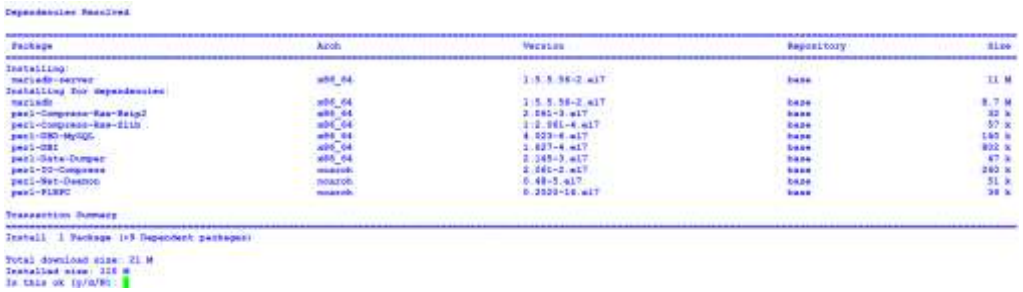
- Instalación de Apache y sus dependencias.



Instalación de Apache

- Instalación de MariaDB y sus dependencias

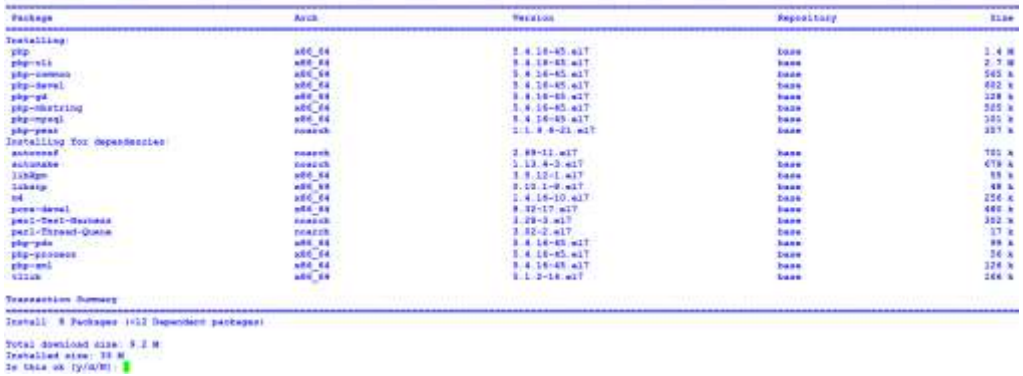
```
[root@cacti ~]# yum install mariadb-server
```



Instalacion de MariaDB

- Instalación de PHP y sus dependencias

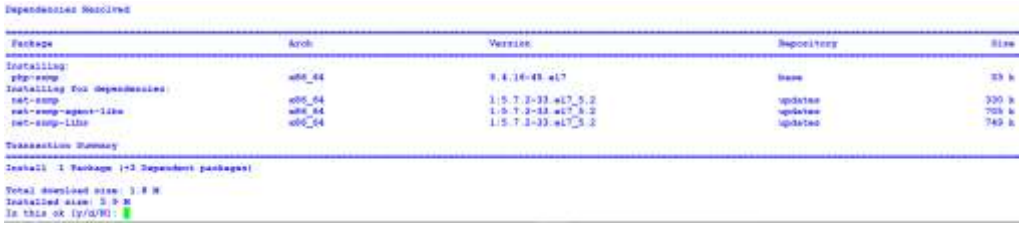
```
[root@cacti ~]# yum install php-mysql php-pear php-common php-gd php-devel php php-mbstring php-cli
```



Instalación de PHP

- Instalación de PHP-SNMP y sus dependencias

```
[root@cacti ~]# yum install php-snmp
```



Instalación de PHP-SNMP

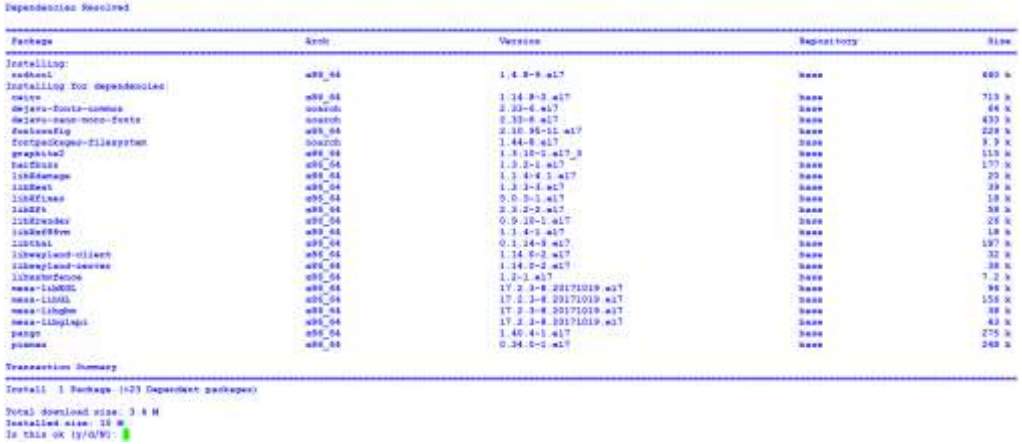
- Instalación de NET-SNMP y sus dependencias

```
[root@cacti ~]# yum install net-snmp-utils net-snmp-libs
```

Instalación de NET-SNMP

- Instalación de RRDTool y sus dependencias

```
[root@cacti ~]# yum install rrdtool
```



Instalación de RRDTool

Luego de haber instalado todo el software necesario para Cacti, se los tiene que inicializar uno a uno como se muestra en la siguiente imagen:

```
[root@cacti ~]# systemctl start httpd.service
[root@cacti ~]# systemctl start mariadb.service
[root@cacti ~]# systemctl start snmpd.service
```

Inicio de servicios instalados

De igual manera se realiza la configuración para que estos servicios se inicien conjuntamente con el sistema operativo al ser este encendido.

```
[root@cacti ~]# systemctl enable httpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@cacti ~]# systemctl enable mariadb.service
Created symlink from /etc/systemd/system/multi-user.target.wants/mariadb.service to /usr/lib/systemd/system/mariadb.service.
[root@cacti ~]# systemctl enable snmpd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/snmpd.service to /usr/lib/systemd/system/snmpd.service.
```

Configuración de servicios al encenderse el servidor

Para la instalación de cacti se debe habilitar el repositorio EPEL como se muestra a continuación:

```
[root@cacti ~]# wget http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
--2018-05-20 22:50:34--  http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
Resolving dl.fedoraproject.org (dl.fedoraproject.org)... 209.132.181.23, 209.132.181.24, 209.132.181.25
Connecting to dl.fedoraproject.org (dl.fedoraproject.org)|209.132.181.23|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15080 (15K) [application/x-rpm]
Saving to: 'epel-release-latest-7.noarch.rpm'

100%[======================================================================>] 15,080      --.-K/s   in 0.1s

2018-05-20 22:50:34 (119 KB/s) - 'epel-release-latest-7.noarch.rpm' saved [15080/15080]

[root@cacti ~]# rpm -ivh epel-release-latest-7.noarch.rpm
warning: epel-release-latest-7.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 352c64e5: NOKEY
Preparing...                          ################################# [100%]
Updating / installing...
   1:epel-release-7-11                ################################# [100%]
```

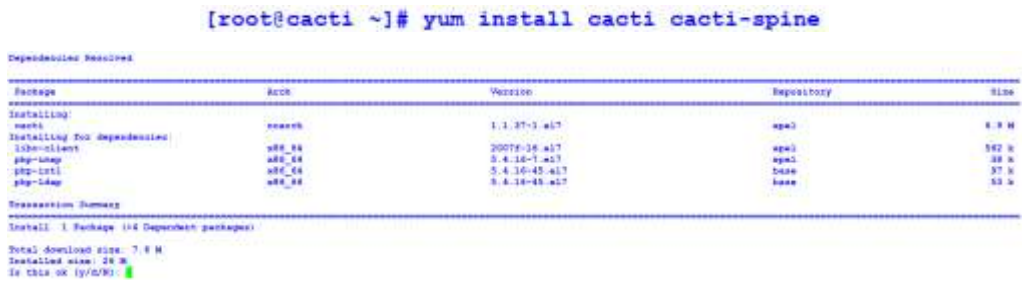
Configuración del repositorio EPEL

Luego de realizar la instalación del repositorio, se procede con su validación como se muestra a continuación:

```
[root@cacti ~]# yum repolist
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.uce.edu.ec
 * epel: mirror.espoch.edu.ec
 * extras: mirrors.uce.edu.ec
 * updates: mirrors.uce.edu.ec
repo id                                                repo name                                                status
base/7/x86_64                                          CentOS-7 - Base                                          9,911
epel/x86_64                                            Extra Packages for Enterprise Linux 7 - x86_64           12,542
extras/7/x86_64                                        CentOS-7 - Extras                                          291
updates/7/x86_64                                       CentOS-7 - Updates                                         539
repolist: 23,283
```

Verificación del repositorio instalado

Posterior a la instalación del repositorio se realiza la instalación de cacti y cacti spine.



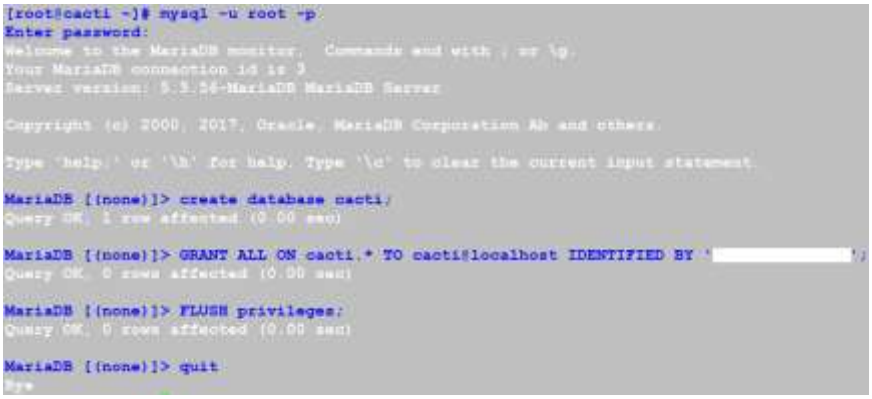
Instalación de cacti y cacti-spine

A continuación, se realizará la configuración del servidor MySQL para la instalación de Cacti, se realizará la configuración del password para MySQL, en la cual se realizará la creación de una base de datos llamada cacti con el usuario cacti.

```
[root@cacti ~]# mysqladmin -u root password
```

Configuración de la clave para MySQL

- Creación de la base de datos cacti



Configuración de la base de datos cacti con el usuario cacti

- Instalacion de las tablas de cacti en MySQL.

```
[root@cacti ~]# rpm -ql cacti | grep cacti.sql
/usr/share/doc/cacti-1.1.37/cacti.sql
[root@cacti ~]# mysql -u cacti -p cacti < /usr/share/doc/cacti-1.1.37/cacti.sql
Enter password:
```

Instalación de las tablas de cacti dentro de MySQL

La configuración de MySQL para cacti se la realizara dentro del siguiente archivo, y se deben configurar los parámetros que se indican a continuación:

```
[root@cacti ~]# vim /etc/cacti/db.php
```

Archivo de configuración para MySQL

- Quedando el archivo configurado de la siguiente manera:

```
<?php
/*
 +-------------------------------------------------------------------------+
 | Copyright (C) 2004-2018 The Cacti Group                                 |
 |                                                                         |
 | This program is free software; you can redistribute it and/or           |
 | modify it under the terms of the GNU General Public License             |
 | as published by the Free Software Foundation; either version 2          |
 | of the License, or (at your option) any later version.                  |
 |                                                                         |
 | This program is distributed in the hope that it will be useful,         |
 | but WITHOUT ANY WARRANTY; without even the implied warranty of          |
 | MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the           |
 | GNU General Public License for more details.                            |
 +-------------------------------------------------------------------------+
 | Cacti: The Complete RRDtool-based Graphing Solution                     |
 +-------------------------------------------------------------------------+
 | This code is designed, written, and maintained by the Cacti Group. See  |
 | about.php and/or the AUTHORS file for specific developer information.   |
 +-------------------------------------------------------------------------+
 | http://www.cacti.net/                                                   |
 +-------------------------------------------------------------------------+
*/

/* make sure these values reflect your actual database/host/user/password */

$database_type     = 'mysql';
$database_default  = 'cacti';
$database_hostname = 'localhost';
$database_username = 'cacti';
$database_password = '          ';
$database_port     = '3306';
$database_ssl      = false;

/* when the cacti server is a remote poller, then these entries point to
 * the main cacti server.  otherwise, these variables have no use.
 * and must remain commented out. */

#$rdatabase_type     = 'mysql';
#$rdatabase_default  = 'cacti';
#$rdatabase_hostname = 'localhost';
#$rdatabase_username = 'cactiuser';
#$rdatabase_password = 'cactiuser';
#$rdatabase_port     = '3306';
#$rdatabase_ssl      = false;
```

Configuración del archivo para MySQL

Para el acceso a la herramienta cacti, se realizará la configuración de la regla de firewall al servidor, para permitir el acceso por el puerto 80, tal como se muestra a continuación:

```
[root@cacti ~]# firewall-cmd --permanent --zone=public --add-service=http
success
[root@cacti ~]# firewall-cmd --reload
success
```

Configuración de la regla de acceso por el puerto 80

La configuración del servidor apache se la realizara dentro dentro del siguiente archivo:

```
[root@cacti ~]# vim /etc/httpd/conf.d/cacti.conf
```

Quedando el archivo de configuración de la siguiente manera, luego de esto se debe reiniciar el servicio de apache para que los cambios tomen efecto:

```
Alias /cacti    /usr/share/cacti

<Directory /usr/share/cacti/>
        <IfModule mod_authz_core.c>
                # httpd 2.4
                Require all granted
        </IfModule>
        <IfModule !mod_authz_core.c>
                # httpd 2.2
                Order deny,allow
                Deny from all
                Allow from localhost
        </IfModule>
</Directory>
```

```
[root@cacti ~]# systemctl restart httpd.service
```

Configuración del servidor apache

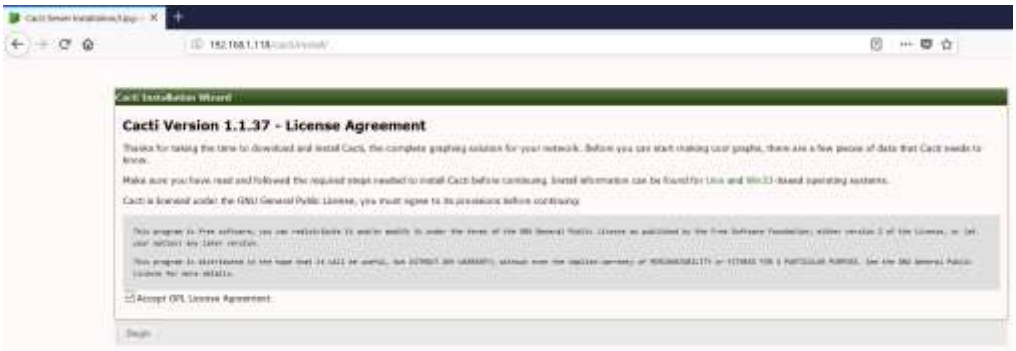
Se habilita el cron de cacti para que el polling se realice cada cinco minutos.

```
[root@cacti ~]# vim /etc/cron.d/cacti
```

```
*/5 * * * *     cacti   /usr/bin/php /usr/share/cacti/poller.php > /dev/null 2>&1
```

Ajustes del Cron de Cacti

Una vez que se tienen instalados los componentes asi como el cacti, se debe acceder via http a la ip de nuestro servidor de la siguiente manera para proceder con la configuración final de la herramienta:

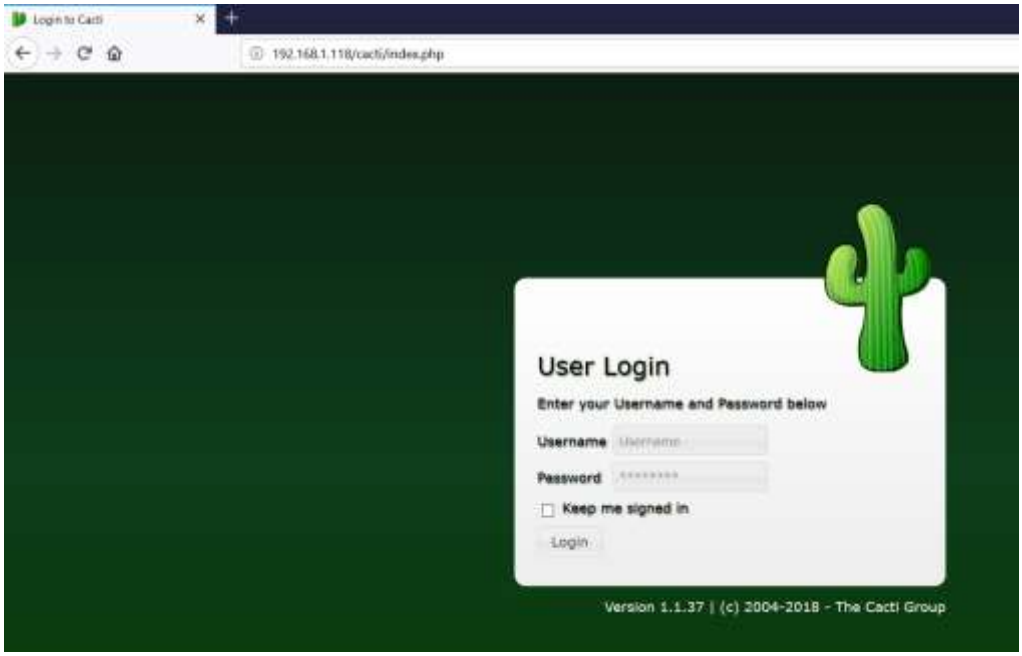


Acceso a la herramienta via http

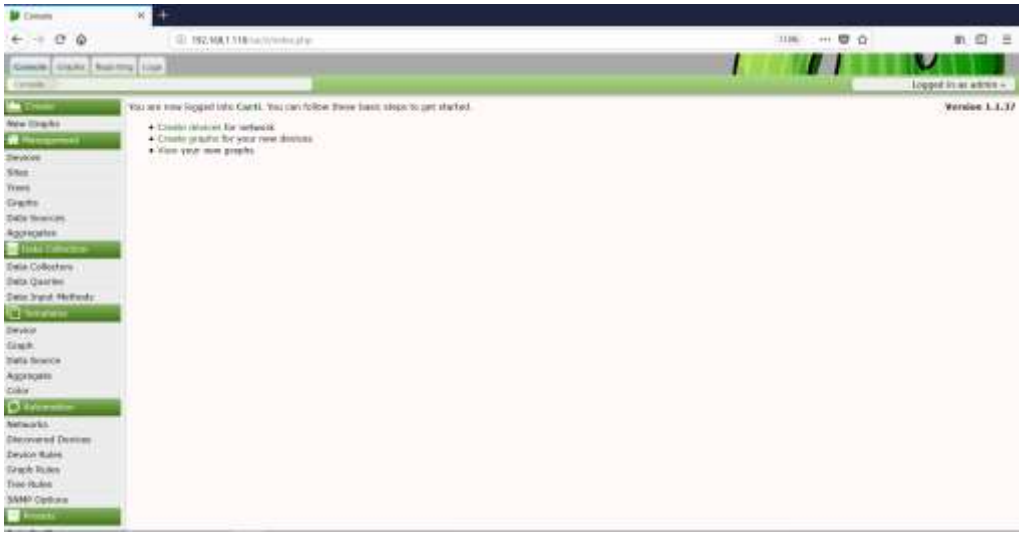
Para continuar con la instalacion final de la herramienta, se deben verificar que todos los parametros que solicita cacti, se encuentren accesibles y se encuentren dentro de los valores recomendados como se muestra en la siguiente imagen.

Parametros de configuración de la herramienta Cacti

Luego de realizar la instalación final, se deberán ingresar las credenciales configuradas, para después poder visualizar la pantalla principal de la herramienta de monitoreo, como se muestra a continuación:



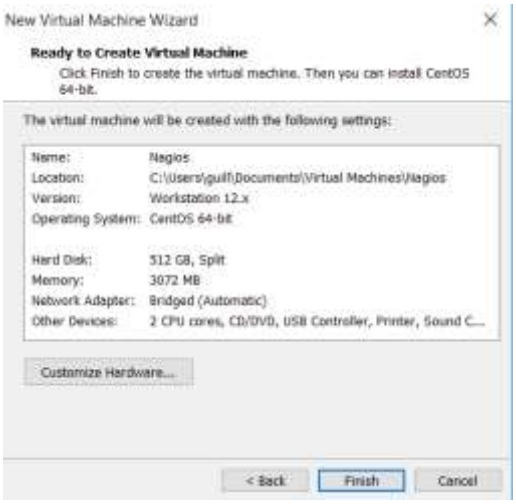
Pantalla para el ingreso de las credenciales de la herramienta



Pantalla principal de la herramienta cacti

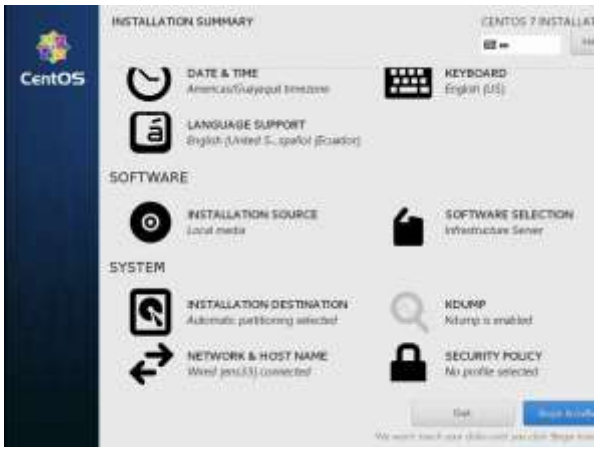
Anexo II. Instalación y Configuración de Nagios

Para la instalación de la herramienta de monitoreo nagios, se realizará el despliegue de una máquina virtual con las siguientes características:



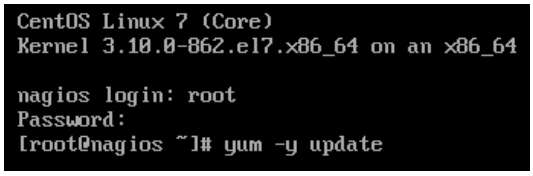
Configuración de la maquina virtual

Se deben realizar las configuraciones de la tarjeta de red para el servidor, así como la elección del tipo de servidor y demás parámetros solicitados para la instalación y proceder con la misma.



Configuración de los parámetros de configuración del sistema operativo

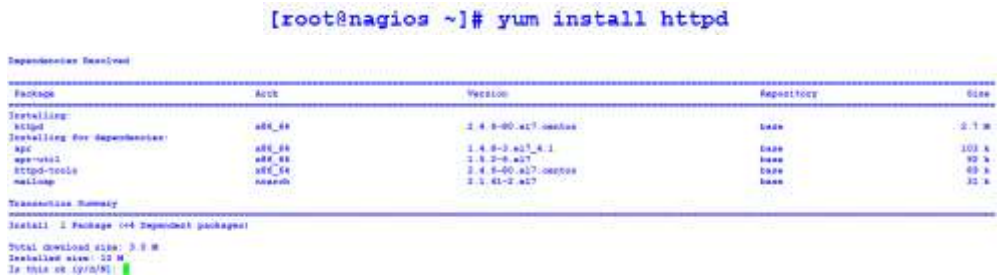
Luego de la instalación del sistema operativo, se procede con la actualización de este, así como los paquetes y dependencias.



Actualización del sistema operativo instalado

Para la instalación de la herramienta nagios, se deben instalar algunos componentes previos, los cuales se indican a continuación:

- Instalación de apache y sus dependencias.

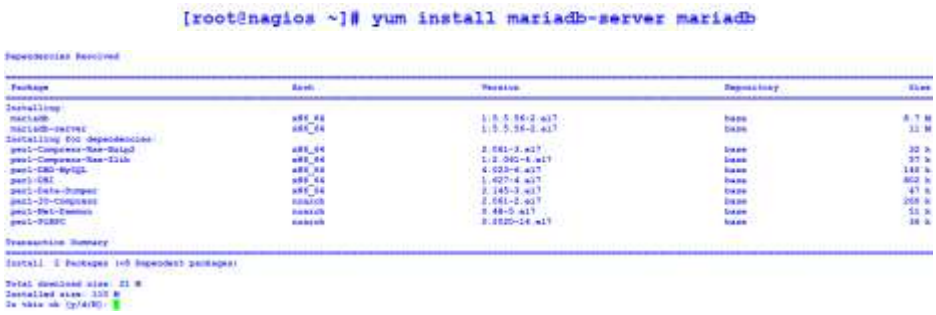


Instalacion de Apache

- Habilitación del servicio de apache, y configuración de arranque conjuntamente con el sistema operativo.

Habilitacion y opción de arranque de apache

- Instalación de MariaDB y sus dependencias.



Instalacion de MariaDB

- Habilitación del servicio de MariaDB y configuración de arranque conjuntamente con el sistema operativo.

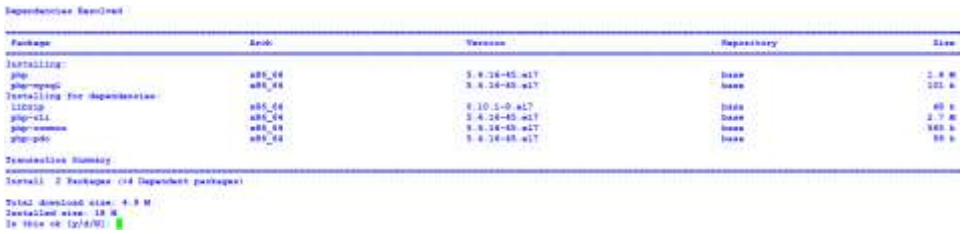
Habilitacion y configuración de arranque de MariaDB

- A continuación, se muestra la configuración realizada a MariaDB.

Configuración de MariaDB

Se procede con la instalación y habilitación de PHP, asi como de sus dependencias.

```
[root@nagios ~]# yum install php php-mysql
```



Instalación de PHP

Se realiza el reinicio del servicio de apache, para que pueda interactuar con php luego de haber sido instalado.

```
[root@nagios ~]# systemctl restart httpd.service
```

Reinicio del servicio de Apache

Se habilitan los puertos http y https al servidor, para permitir las conexiones por el puerto 80 y 443.

```
[root@nagios ~]# firewall-cmd --permanent --zone=public --add-service=http
success
[root@nagios ~]# firewall-cmd --permanent --zone=public --add-service=https
success
[root@nagios ~]# firewall-cmd --reload
success
```

Configuración del firewall del servidor

- Instalación de paquetes y dependecias necesarios para nagios.

```
[root@nagios ~]# yum install gcc glibc glibc-common gd gd-devel make net-snmp openssl-devel xinetd unzip
```

Instalación de paquetes necesarios para nagios

Para levantar el servicio de nagios, se realizará la creación del usuario nagios, así como del grupo nagcmd, posterior a esto el usuario creado será añadido al grupo creado.

```
[root@nagios ~]# useradd nagios
[root@nagios ~]# groupadd nagcmd
[root@nagios ~]# usermod -a -G nagcmd nagios
```

Creación del usuario y grupo para nagios

Se realiza la descarga de la última versión estable de nagios de la siguiente manera:

```
[root@nagios ~]# curl -L -O https://assets.nagios.com/downloads/nagioscore/releases/nagios-4.3.4.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 10.5M  100 10.5M    0     0   318k      0  0:00:34  0:00:34 --:--:--  173k

[root@nagios nagios-4.3.4]# ./configure --with-command-group=nagcmd
```

Descarga de nagios

- Instalación de los plugins de nagios.

```
[root@nagios nagios-4.3.4]# curl -L -O http://nagios-plugins.org/download/nagios-plugins-2.2.1.tar.gz
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100 2664k  100 2664k    0     0   268k      0  0:00:09  0:00:09 --:--:--  226k

[root@nagios nagios-plugins-2.2.1]# ./configure --with-nagios-user=nagios --with-nagios-group=nagios --with-openssl
```

Descarga de plugins de nagios

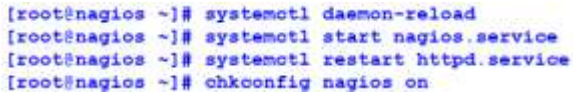
- Instalación de NRPE.

Configuración de NRPE

- Configuración de Apache.

Configuración del acceso a apache

- Habilitación de servicios para el arranque de nagios.

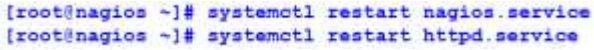


Habilitación de servicios para nagios

- Restricción del acceso a nagios.

Restricción del acceso a la herramienta nagios

- Reinicio de los servicios para que los cambios tengan efecto.



Reinicio de servicios para iniciar nagios

Finalmente se tiene la herramienta instalada, a continuación, se muestra su panel principal:

Página principal de la herramienta nagios

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Guillermo Eduardo Vega Picon**, con C.C: # **0104555313** autor/a del trabajo de titulación: **Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla,** previo a la obtención del título de **Magíster en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 26 de octubre de 2018

f. _____

Nombre: **Guillermo Eduardo Vega Picon**

C.C: **0104555313**

Presidencia de la República del Ecuador

Plan Nacional de Ciencia, Tecnología, Innovación y Saberes

SENESCYT
Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TESIS/TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Implementación de un sistema de monitoreo para el análisis de la disponibilidad, capacidad, calidad y latencia de enlaces corporativos de última milla.		
AUTOR(ES)	Guillermo Eduardo Vega Picon		
REVISOR(ES)/TUTOR	MSc. Orlando Philco Asqui; MSc. Celso Bohórquez Escobar / MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
PROGRAMA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	26 de octubre de 2018	**No. DE PÁGINAS:**	**80**
ÁREAS TEMÁTICAS:	Herramientas de monitoreo, Pandora FMS, ManageEngine, Orion – SolarWinds, Monitoreo, Mensajes, Enlaces		
PALABRAS CLAVES/ KEYWORDS:	Cacti, Nagios, SNMP, SLA, OID y MIB		

RESUMEN/ABSTRACT:
En este trabajo de investigación, se realiza el análisis de diferentes herramientas de monitoreo tanto de pago como gratuitas, para poder determinar e implementar un sistema de monitoreo, que brinde los parámetros necesarios para mantener una infraestructura de red operativa y disponible para los usuarios. Se realiza un análisis y comparación de las principales herramientas de pago que existen en el mercado y las de monitoreo gratuitas que existen en la actualidad, luego se analiza el protocolo SNMP (Simple Network Management Protocol – Protocolo Simple de Administracion de Red), el cual es el principal mecanismo de comunicación entre el sistema de monitoreo y los equipos a ser monitoreados, para poder implementar un sistema de monitoreo adecuado. Luego se procede a realizar la implementación de las herramientas elegidas, analizando cada una de ellas.Por ultimo se realiza la evaluación y se analizan los beneficios que cada una de las herramientas de monitoreo implementadas brinda, para poder contar con un sistema de monitoreo correctamente implementado. En la sección de anexos, se explican los pasos que se siguieron, para poder realizar la implementación y configuración de cada una de las herramientas de monitoreo elegidas, se indican parámetros importantes como que tipo de sistema operativo se eligio, características de los servidores en los cuales se alojaran las herramientas de monitoreo y configuración de cada una de ellas.

ADJUNTO PDF:	☒ SI	☐ NO
CONTACTO CON AUTOR/ES:	**Teléfono:** +593-984149123	**E-mail:** gvega88p@gmail.com
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Romero Paz Manuel de Jesús	
	Teléfono: +593-994606932	
	E-mail: manuel.romero@cu.ucsg.edu.ec	

SECCIÓN PARA USO DE BIBLIOTECA	
Nº. DE REGISTRO (en base a datos):	
Nº. DE CLASIFICACIÓN:	
DIRECCIÓN URL (tesis en la web):	