



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

The screenshot shows the URKUND web interface. The browser address bar displays a secure URL. The page header includes the URKUND logo and the user name 'Oriando Philco Asqui (orlando.philco)'. The main content area is divided into two sections: document details on the left and a list of sources on the right.

Documento: Tesis_Gilego_Monitoreo_v2_Rev_26-08-2018.docx (41238865)

Presentado: 2018-08-07 08:05 (-06:00)

Presentado por: orlando.philco_78@hotmail.com

Recibido: orlando.philco.ucsg@entanalysis.arkund.com

Mensaje: TESIS Guillermo Vega. [Mostrar el mensaje completo](#)

14 de estas 22 páginas, se componen de texto presente en 1 fuentes.

Lista de fuentes:

Categoría	Enlace/nombre de archivo
	http://repositorio.ucsg.edu.ec/bitstream/33173673/1/T-UCSG-PR5-ING-OS-42.pdf
	Tesis diego vifian.docx
	https://www.ceris.es/blog/rimo-tan-simple-el-nombre-indica
	Tesis_Leonardo_Rodriguez.docx

SISTEMA DE POSGRADO

MAESTRIA EN TELECOMUNICACIONES

TEMA:

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

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.....	XI
ÍNDICE DE TABLAS	XIII
Resumen.....	XIV
Abstract	XV
Capítulo 1: Descripción del proyecto de intervención.	2
1.1. Introducción	2
1.2. Antecedentes.....	2
1.3. Definición del problema	3
1.4. Justificación del Problema a Investigar.....	3
1.5. Objetivos.....	4
1.5.1. Objetivo General:.....	4
1.5.2. Objetivos específicos:.....	4
1.6. Hipótesis.....	4
1.7. Metodología de investigación.	4
Capítulo 2: Fundamentación Teórica	6
2.1. Introducción al monitoreo de la red	6
2.2. Elección entre una herramienta de monitoreo gratuita frente a una de pago.	6
2.2.1. Herramientas de monitoreo gratuitas	7
2.2.1.1. Cacti.....	7
2.2.1.2. Nagios.....	8
2.2.2. Herramientas de monitoreo de pago	9
2.2.2.1. Pandora FMS.....	9
2.2.2.2. ManageEngine.....	10
2.2.2.3. Orion – SolarWinds.....	11
2.3. SNMP	12
2.3.1. Monitorización SNMP por Polling	13
2.3.2. Monitorización SNMP por Traps.....	15
2.3.3. OID y MIB.....	16

2.4.	Diferencias entre las distintas versiones de SNMP.	17
2.4.1.	SNMP v1	17
2.4.2.	SNMP v2	18
2.4.3.	SNMP v3	18
2.5.	Tipos de mensajes enviados en SNMP	19
2.6.	Criterios para la selección adecuada de una solución de monitoreo de red	20
2.6.1.	Elección de la mejor alternativa.....	20
Capítulo 3: Instalación y Configuración de las herramientas de monitoreo Cacti y Nagios.....		22
3.1.	Instalación y configuración de la herramienta Cacti	22
3.2.	Instalación y configuración de Nagios	25
Capítulo 4: Resultados y Análisis de las herramientas de red utilizadas		30
4.1.	Análisis y resultados de la herramienta Cacti	30
4.2.	Análisis y resultados de la herramienta Nagios	36
Referencias Bibliográficas.....		45
Anexos.....		50
Anexo I.	Instalación y Configuración de Cacti	50
Anexo II.	Instalación y Configuración de Nagios	60

ÍNDICE DE FIGURAS

Capítulo 2:

Figura 2.1: Software de Monitoreo Pandora FMS.....	9
Figura 2.2: Software de monitoreo OpManager	10
Figura 2.3: Software de monitoreo Orion de Solarwinds.....	11
Figura 2.4: Consulta SNMP v2 realizada a un router Cisco.....	14
Figura 2.5: MIB obtenida al realizar una consulta SNMP con v3	14
Figura 2.6: MIB obtenida al realizar una consulta SNMP con v3	14
Figura 2.7: Instalacion de snmptrapd.....	15
Figura 2.8: Estructura de una MIB	16
Figura 2.9: Object identifier de una MIB.....	17
Figura 2.10: PDU de un mensaje SNMP	17
Figura 2.11: PDU del protocolo SNMPv3.....	19
Figura 2.12: Comparativa entre las diferentes herramientas analizadas	21

Capítulo 3:

Figura 3.1: Panel principal de la herramienta instalada	23
Figura 3.2: Configuración del protocolo SNMP	24
Figura 3.3: Elección de cacti spine	24
Figura 3.4: Configuración del envío de notificaciones.....	25
Figura 3.5: Página principal de nagios.....	27
Figura 3.6: Pestaña de visualización para el monitoreo de hosts	27
Figura 3.7: Pestaña de visualización para el monitoreo de servicios de hosts	28
Figura 3.8: Archivos de configuración para la herramienta nagios	28

Capítulo 4:

Figura 4.1: Agrupación de equipos monitoreados.....	31
Figura 4.2: Monitoreo de equipos Windows y Linux.....	31
Figura 4.3: Consumo en tiempo real de una interfaz	32
Figura 4.4: Estado normal de un host en la herramienta cacti.....	32

Figura 4.5: Estado de recovery de un host en la herramienta cacti	33
Figura 4.6: Host alarmado dentro de la herramienta cacti	33
Figura 4.7: Saturación del ancho de banda	34
Figura 4.8: Incremento de los tiempos de latencia debido a saturación	34
Figura 4.9: Configuración para la visualización de una gráfica en especifico.....	35
Figura 4.10: Patrón de monitoreo para un host específico.....	35
Figura 4.11: Envío de alarmas al personal encargado de la administración de la red.....	36
Figura 4.12: Monitoreo realizado en la herramienta nagios	37
Figura 4.13: Monitoreo de disponibilidad de un dispositivo.....	37
Figura 4.14: Monitoreo por servicio de un dispositivo	38
Figura 4.15: Reporte de disponibilidad de un dispositivo monitoreado	38
Figura 4.16: Análisis del reporte de disponibilidad de un dispositivo monitoreado.....	39
Figura 4.17: Análisis del reporte de disponibilidad de un dispositivo monitoreado.....	40
Figura 4.18: Envío de notificaciones de la herramienta Nagios	41

ÍNDICE DE TABLAS

Capítulo 2:

Tabla 2.1: Mensajes enviados entre el NMS y el agente 19

Capítulo 3:

Tabla 3.1: Archivos de configuracion para nagios 29

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 Administración 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 eligió, características de los servidores en los cuales se alojaron 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, pérdida 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 preestablecido.

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 Información de Gestión) y OIDs (Object Identifiers - Identificador de Objeto) de los equipos a ser monitoreados.

Cacti es una herramienta muy útil que cuenta con plantillas para algunos fabricantes, equipos, servicios, además de que permite la elaboración de plantillas 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 Administración 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 decisión 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 analizarán Pandora FMS, ManageEngine y Orion de SolarWinds.

2.2.2.1. Pandora FMS

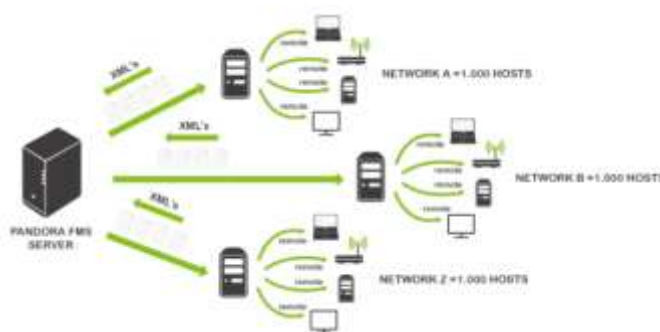


Figura 2.1: Software de Monitoreo Pandora FMS

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

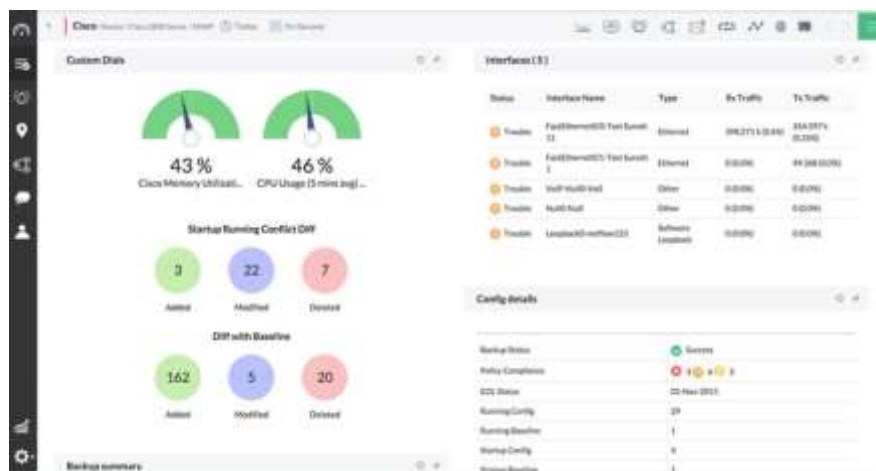


Figura 2.2: Software de monitoreo OpManager

Fuente: (ManageEngine, 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

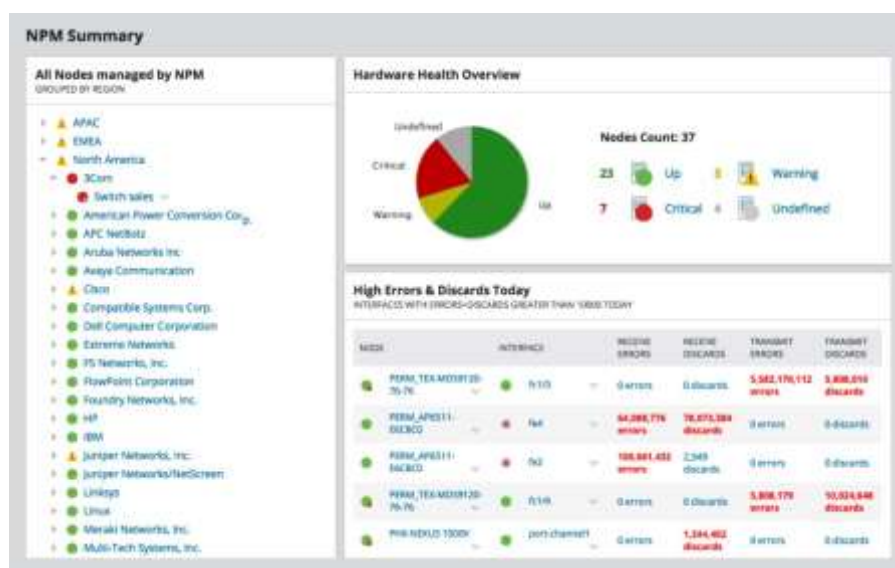


Figura 2.3: Software de monitoreo Orion de Solarwinds

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 implementación 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 específica 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.

```

SNMPv2-MIB::sysDescr.0 = STRING: Cisco IOS Software, C181X Software (C181X-ADVISERVICERSK9-M), Version 12.4(15)T14, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2010 by Cisco Systems, Inc
Compiled Tue 17-Aug-10 19:35 by prod_ral_bam
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.9.1.641
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (269240847) 211 days, 14:53:29.47
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING:
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 78
SNMPv2-MIB::sysOidLastChange.0 = Timeticks: (0) 0:00:00.00
SNMPv2-MIB::sysCRID.1 = OID: SNMPv2-SMI::enterprises.9.7.129
SNMPv2-MIB::sysCRID.2 = OID: SNMPv2-SMI::enterprises.9.7.115
SNMPv2-MIB::sysCRID.3 = OID: SNMPv2-SMI::enterprises.9.7.265
SNMPv2-MIB::sysCRID.4 = OID: SNMPv2-SMI::enterprises.9.7.112
SNMPv2-MIB::sysCRID.5 = OID: SNMPv2-SMI::enterprises.9.7.106
SNMPv2-MIB::sysCRID.6 = OID: SNMPv2-SMI::enterprises.9.7.47
SNMPv2-MIB::sysCRID.7 = OID: SNMPv2-SMI::enterprises.9.7.122
SNMPv2-MIB::sysCRID.8 = OID: SNMPv2-SMI::enterprises.9.7.135
SNMPv2-MIB::sysCRID.9 = OID: SNMPv2-SMI::enterprises.9.7.43
SNMPv2-MIB::sysCRID.10 = OID: SNMPv2-SMI::enterprises.9.7.37
SNMPv2-MIB::sysCRID.11 = OID: SNMPv2-SMI::enterprises.9.7.92
SNMPv2-MIB::sysCRID.12 = OID: SNMPv2-SMI::enterprises.9.7.53
SNMPv2-MIB::sysCRID.13 = OID: SNMPv2-SMI::enterprises.9.7.54
SNMPv2-MIB::sysCRID.14 = OID: SNMPv2-SMI::enterprises.9.7.52
SNMPv2-MIB::sysCRID.15 = OID: SNMPv2-SMI::enterprises.9.7.33
SNMPv2-MIB::sysCRID.16 = OID: SNMPv2-SMI::enterprises.9.7.186
SNMPv2-MIB::sysCRID.17 = OID: SNMPv2-SMI::enterprises.9.7.128
SNMPv2-MIB::sysCRID.18 = OID: SNMPv2-SMI::enterprises.9.7.425
SNMPv2-MIB::sysCRID.19 = OID: SNMPv2-SMI::enterprises.9.7.269
SNMPv2-MIB::sysCRID.20 = OID: SNMPv2-SMI::enterprises.9.7.121
SNMPv2-MIB::sysCRID.21 = OID: SNMPv2-SMI::enterprises.9.7.44
SNMPv2-MIB::sysCRID.22 = OID: SNMPv2-SMI::enterprises.9.7.202
SNMPv2-MIB::sysCRID.23 = OID: SNMPv2-SMI::enterprises.9.7.264
SNMPv2-MIB::sysCRID.24 = OID: SNMPv2-SMI::enterprises.9.7.33
SNMPv2-MIB::sysCRID.25 = OID: SNMPv2-SMI::enterprises.9.7.492
SNMPv2-MIB::sysCRID.26 = OID: SNMPv2-SMI::enterprises.9.7.130
SNMPv2-MIB::sysCRID.27 = OID: SNMPv2-SMI::enterprises.9.7.116
SNMPv2-MIB::sysCRID.28 = OID: SNMPv2-SMI::enterprises.9.7.91
SNMPv2-MIB::sysCRID.29 = OID: SNMPv2-SMI::enterprises.9.7.399
SNMPv2-MIB::sysCRID.30 = OID: SNMPv2-SMI::enterprises.9.7.212
SNMPv2-MIB::sysCRID.31 = OID: SNMPv2-SMI::enterprises.9.7.126
SNMPv2-MIB::sysCRID.32 = OID: SNMPv2-SMI::enterprises.9.7.127
SNMPv2-MIB::sysCRID.33 = OID: SNMPv2-SMI::enterprises.9.7.64
SNMPv2-MIB::sysCRID.34 = OID: SNMPv2-SMI::enterprises.9.7.123

```

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>
-I 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>
-I 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 recpte los traps enviados por los equipos para su revisión.

Los traps se los pueden receptor 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
```

```
Dependencies resolved
-----
Package             Arch           Version           Repository        Size
-----
Installing          x86_64
net-snmp-libs       1:5.7.3-01.el7_3.2
Transaction Summary
-----
Install 3 Package
Total download size: 186 k
Installed size: 431 k
Downloading packages:
net-snmp-libs-1:5.7.3-01.el7_3.2.x86_64.rpm
Running transaction check
Running transaction test
Transaction test successful
Warning: RPMdb altered during installation
Installing : 1:net-snmp-libs-5.7.3-01.el7_3.2.x86_64
Verifying  : 1:net-snmp-libs-5.7.3-01.el7_3.2.x86_64
Installed:
net-snmp-libs.x86_64 1:5.7.3-01.el7_3.2
Complete!
```

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.

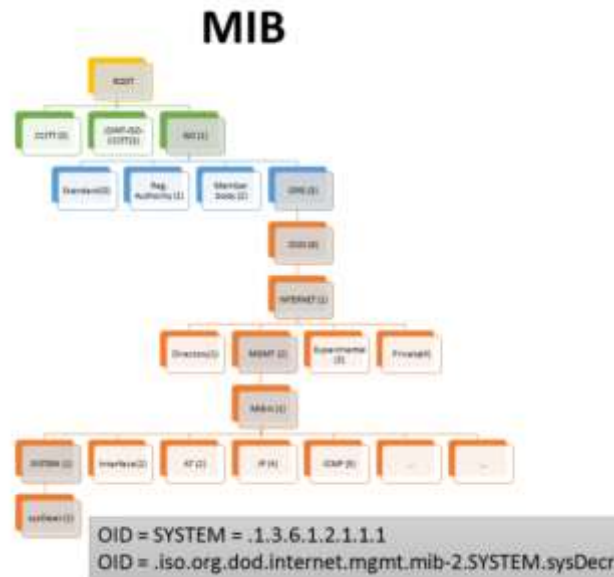


Figura 2.8: Estructura de una MIB

Fuente: (INCIBE, 2017)

La MIB se encuentra estructurada en una jerarquía, la cual permite el correcto orden de cada objeto que este siendo monitoreado, así 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.

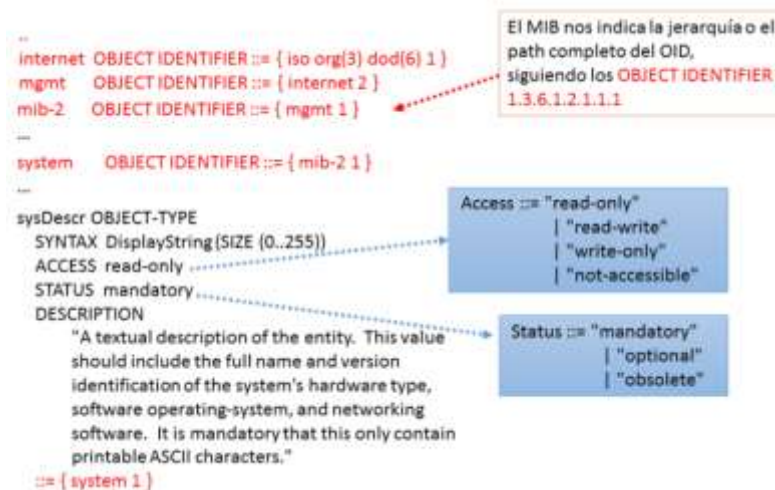


Figura 2.9: Object identifier de una MIB

Fuente: (INCIBE, 2017)

El PDU (Protocol Data Unit – Unidad de Datos de Protocolo) de un mensaje SNMP esta compuesto 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 tenía que realizar en reiteradas ocasiones 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 leídos dentro de la MIB, brindando con esto una pequeña barrera de seguridad al protocolo.

2.4.2. SNMP v2

En esta versión se modifican algunos campos de la PDU, permitiendo la implementación de nuevas funcionalidades como son GetBulkRequest e InformRequest, así 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 Administración de Red) por sus siglas en inglés 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 pérdida 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.

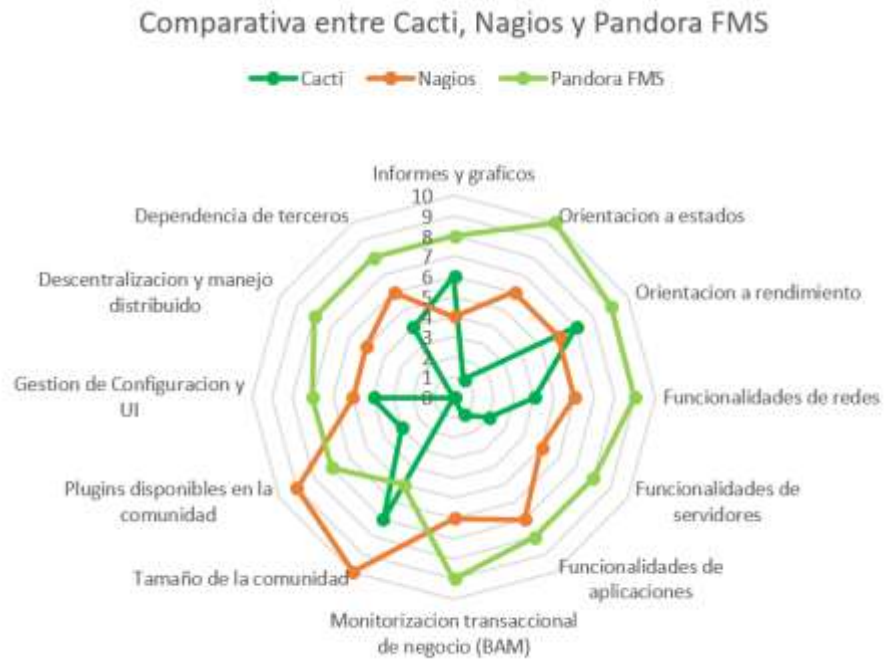


Figura 2.12: Comparativa entre las diferentes herramientas analizadas

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

The screenshot shows the Cacti configuration interface for Mail/Reporting/DNS. The settings are as follows:

Setting	Value
Server Base URL	http://192.168.14.12/cacti
Test Email	<input type="checkbox"/>
Mail Services	SMTP
Ring Mail Server	Yes
From Email Address	<input type="text"/>
From Name	<input type="text"/>
Word Wrap	120
SMTP Hostname	192.168.14.14
SMTP Port	25
SMTP Username	<input type="text"/>
SMTP Password	<input type="password"/>
SMTP Security	None
SMTP Timeout	10

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 prerequisites 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

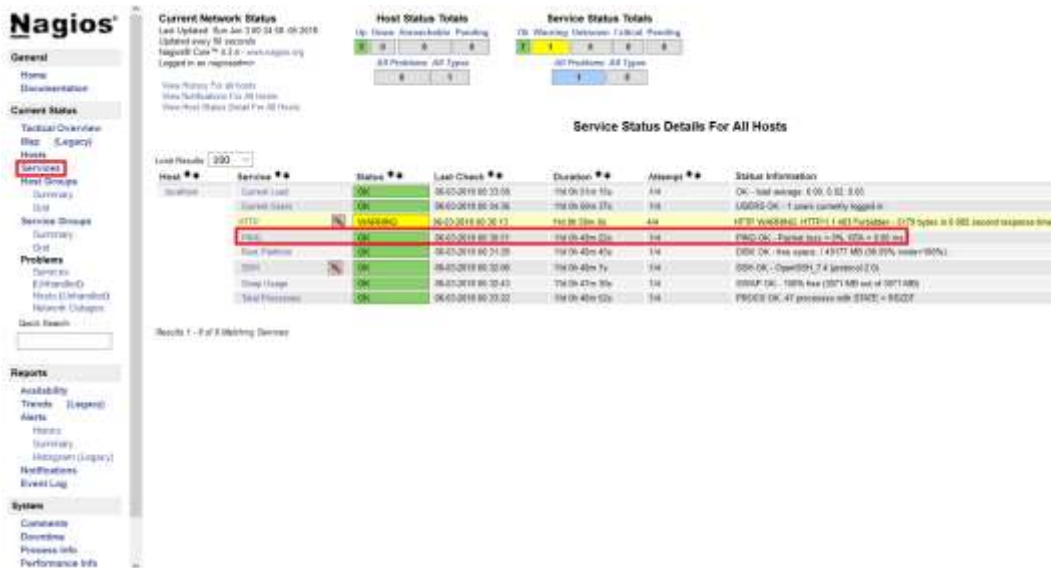


Figura 3.7: Pestaña de visualización para el monitoreo de servicios de hosts

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-rw-r-- 1 root root 50 May 22 23:41 httppasswd.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-rw-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-r-- 1 nagios nagios 1312 May 22 23:30 resource.cfg
1143159 -rw-rw-r-- 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 así 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.

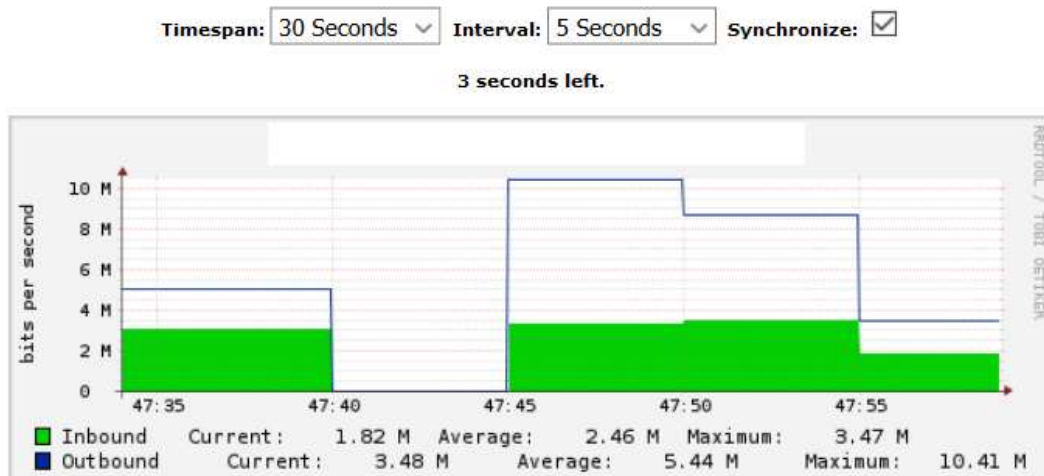


Figura 4.3: Consumo en tiempo real de una interfaz

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).

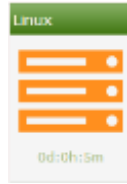


Figura 4.5: Estado de recovery de un host en la herramienta Cacti

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.

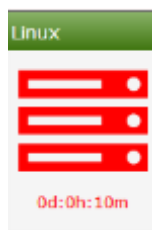


Figura 4.6: Host alarmado dentro de la herramienta cacti

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.

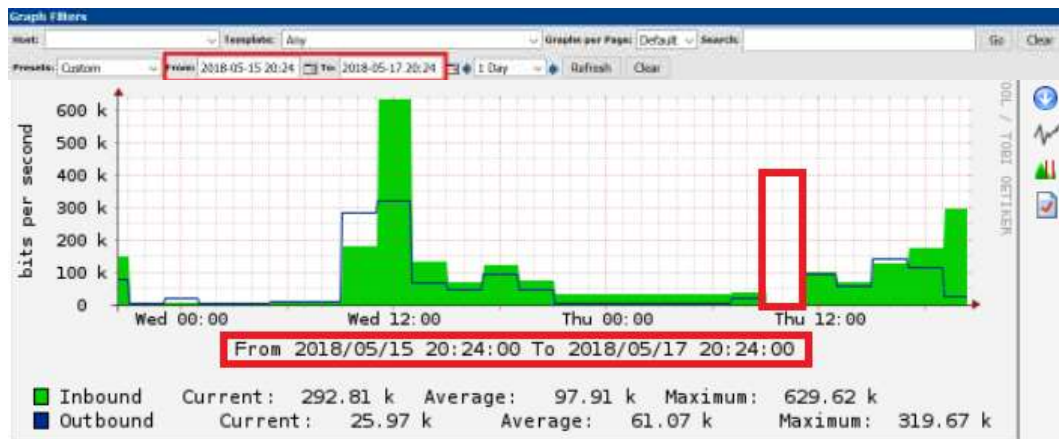


Figura 4.9: Configuración para la visualización de una gráfica en específico

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.

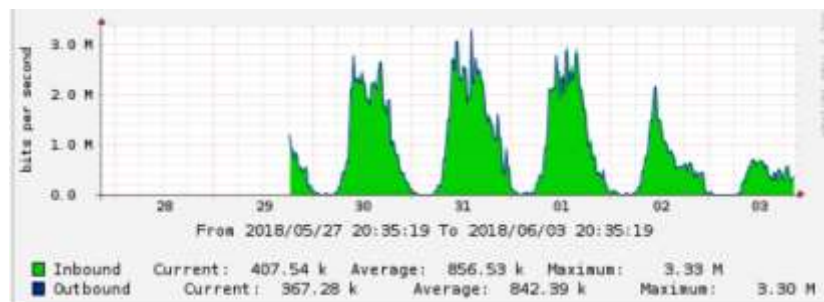


Figura 4.10: Patrón de monitoreo para un host específico

Fuente: El autor

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

Service Status Details For All Hosts

Load Results:

Host**	Service**	Status**	Last Check**	Duration**	Attempt**	Status Information
Card05-7	Current Load	OK	07-17-2018 18:28:26	0d 1h 28m 56s	114	OK - load average: 0.90, 0.01, 0.35
	Current Users	OK	07-17-2018 18:29:25	0d 1h 29m 55s	114	USERS OK - 1 users currently logged in
	HTTP	CRITICAL	07-17-2018 18:30:26	0d 1h 29m 56s	44	connect to address 192.168.14.11 and port 80: No data to host
	PING	OK	07-17-2018 18:30:32	0d 0h 30m 31s	114	PING OK - Packet loss = 0%, RTT = 0.34 ms
	Host Partition	OK	07-17-2018 18:32:21	0d 1h 25m 1s	114	DISK OK - free space: 149019 MB (95.98% used=308%)
	SSH	OK	07-17-2018 18:32:30	0d 0h 27m 33s	114	SSH OK - OpenSSH_7.4 (protocol 2.0)
	Disk Usage	OK	07-17-2018 18:33:41	0d 1h 28m 1s	114	SWAP OK - 300% free (3071 MB out of 3071 MB)
	Total Processes	OK	07-17-2018 18:33:44	0d 1h 28m 53s	114	PROCS OK - 99 processes with STATE = RSZDT

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.

Step 3: Select Report Options

Report Period:

If Custom Report Period:

Start Date (Inclusive):

End Date (Inclusive):

Report time Period:

Assume Initial States:

Assume State Retention:

Assume States During Program Downtime:

Include Soft States:

First Assumed Host State:

First Assumed Service State:

Backtracked Archives (To Scan For Initial States):

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.

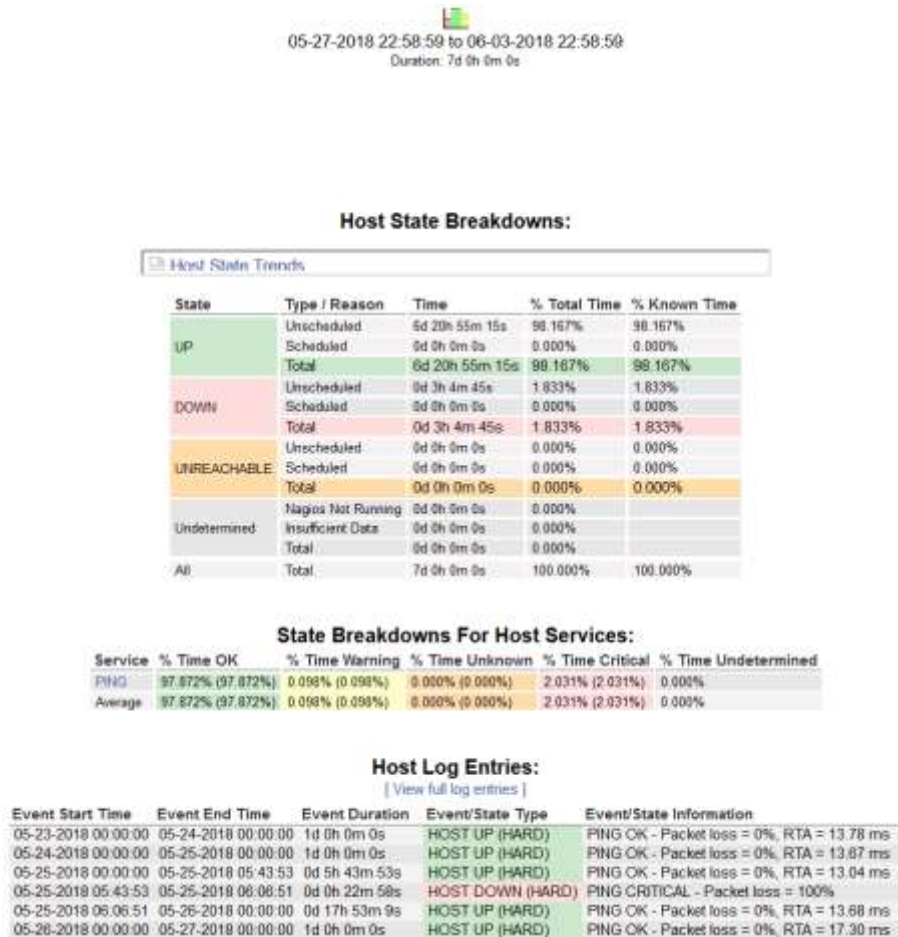


Figura 4.16: Análisis del reporte de disponibilidad de un dispositivo monitoreado

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.

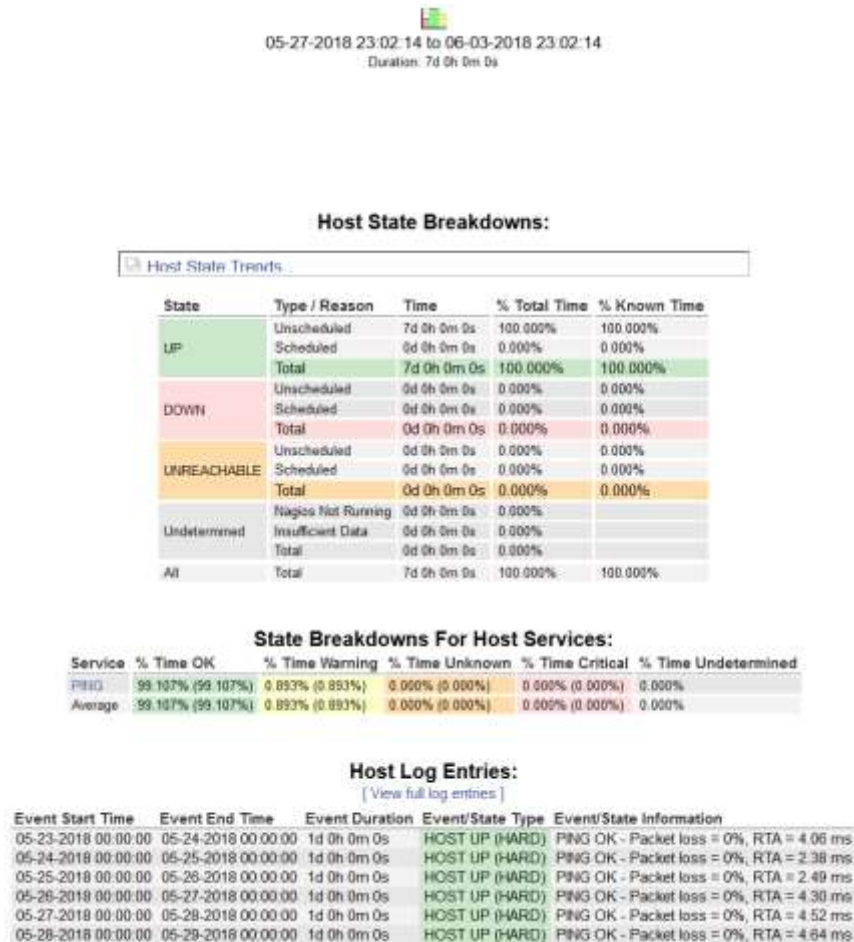


Figura 4.17: Análisis del reporte de disponibilidad de un dispositivo monitoreado

Fuente: El autor

La herramienta permite realizar la configuración para el envío 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: Envío 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 intuitivas, 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 encriptación 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 creación 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

Este es el programa que se ejecuta como proceso en el background en los equipos remotos y procesa las peticiones de ejecución de comandos del plugin check_nrpe del equipo donde esta Nagios40

O

OID

Object Identifiers 21

OSI

Open System Interconnection 26

P

PDU

Unidad de Datos de Protocolo..... 31

PHP

Es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML..... 37

ping

Packet Internet Groper

Herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión 34

plugin

Complemento 46

poller

Sondeo 36

R

recovery

Restablecimiento..... 46

RRDTool

Round Robin Database Tool 21

S

SHA

Secure Hash Algoritm 33

SLA	
Service Level Agreement	16
SMB	
Bloque de Mensajes del Servidor	
Es un protocolo de uso compartido de archivos de red.	48
SMTP	
Simple Mail Transfer Protocol	40
SNMP	
Simple Network Management Protocol	XIV
ssh	
Secure Shell	
Es un protocolo de administración remota que permite a los usuarios	
controlar y modificar sus servidores remotos a través de Internet.	
.....	23
T	
template	
Plantilla.....	45
TI	
Tecnología de la información	36
U	
udp	
User Datagram Protocol.....	26
upgrade	
Incremento	44
USM	
User-based Security Model	33
W	
web	
Red o Internet	
Programa que se lo visualiza en un navegador	36

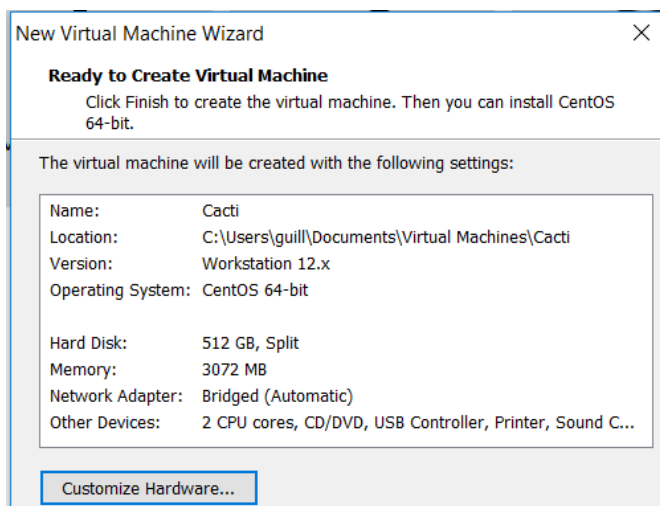
Anexos

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

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

```
CentOS Linux 7 (Core)
Kernel 3.10.0-862.el7.x86_64 on an x86_64

cacti login: root
Password:
Last login: Sun May 20 21:00:32 on tty1
[root@cacti ~]# yum -y update_
```

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.

```
root@cacti~
login as: root
root@192.168.1.118's password:
Last login: Sun May 20 22:23:20 2018
[root@cacti ~]# yum -y install httpd httpd-devel
```

```

Dependencias Resueltas
-----
Package Arch Version Repository Size
Installing:
httpd x86_64 2.4.18-02.el7.centos base 2.7 M
httpd-devel x86_64 2.4.18-02.el7.centos base 195 K
Installing for dependencies:
apr x86_64 1.4.9-3.el7.4.1 base 103 K
apr-devel x86_64 1.4.9-3.el7.4.1 base 109 K
apr-util x86_64 1.3.2-4.el7 base 92 K
apr-util-devel x86_64 1.3.2-4.el7 base 75 K
expat-devel x86_64 2.1.2-2.el7 base 88 K
expat-devel-devel x86_64 2.1.2-2.el7 base 210 K
nghttp-devel x86_64 1.1.0-10.el7_3 base 57 K
httpd-tools x86_64 2.4.18-02.el7.centos base 89 K
libdb-devel x86_64 5.3.21-28.el7 base 36 K
mailmap noarch 2.1.41-2.el7 base 31 K
openssl-devel x86_64 2.0.18-15.el7_3 updates 822 K

Transaction Summary
-----
Install 2 Packages (+11 dependent packages)

Total download size: 4.7 M
Installed size: 37 M
Is this ok [y/N]: y

```

Instalación de Apache

- Instalación de MariaDB y sus dependencias

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

```

Dependencias Resueltas
-----
Package Arch Version Repository Size
Installing:
mariadb-server x86_64 10.5.5-2.el7 base 11 M
Installing for dependencies:
bc1c4db x86_64 1.0.5.58-2.el7 base 8.7 M
pwi-Compress-Base-File2 x86_64 2.182-3.el7 base 32 K
pwi-Compress-Base-File x86_64 1.2.181-4.el7 base 57 K
pwi-DB-MySQL x86_64 4.222-4.el7 base 185 K
pwi-DBI x86_64 1.827-4.el7 base 822 K
pwi-Data-Dumper x86_64 2.185-3.el7 base 47 K
pwi-DB-Connector x86_64 2.142-2.el7 base 140 K
pwi-Net-Database noarch 0.48-3.el7 base 51 K
pwi-PLRPC noarch 0.2020-14.el7 base 38 K

Transaction Summary
-----
Install 1 Package (+5 dependent packages)

Total download size: 21 M
Installed size: 328 M
Is this ok [y/N]: y

```

Instalación 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
```

```

Dependencias Resueltas
-----
Package Arch Version Repository Size
Installing:
php x86_64 5.4.16-45.el7 base 1.4 M
php-cli x86_64 5.4.16-45.el7 base 2.7 M
php-common x86_64 5.4.16-45.el7 base 545 K
php-devel x86_64 5.4.16-45.el7 base 692 K
php-gd x86_64 5.4.16-45.el7 base 128 K
php-intl x86_64 5.4.16-45.el7 base 255 K
php-mbstring x86_64 5.4.16-45.el7 base 255 K
php-mysql noarch 5.1.8-8-21.el7 base 287 K
Installing for dependencies:
autoconf noarch 2.69-11.el7 base 703 K
autoconf-noarch noarch 1.13.4-3.el7 base 678 K
libpng x86_64 3.8.12-1.el7 base 89 K
libzip x86_64 3.12.1-9.el7 base 48 K
nd x86_64 1.4.18-10.el7 base 256 K
pcre-devel x86_64 8.39-17.el7 base 492 K
pwi-DBI-Database noarch 1.28-3.el7 base 352 K
pwi-DBI-Database noarch 1.32-2.el7 base 37 K
php-gd x86_64 5.4.16-45.el7 base 89 K
php-pear x86_64 5.4.16-45.el7 base 34 K
php-xml x86_64 5.4.16-45.el7 base 324 K
zip x86_64 5.1.2-18.el7 base 244 K

Transaction Summary
-----
Install 9 Packages (+12 dependent packages)

Total download size: 9.2 M
Installed size: 38 M
Is this ok [y/N]: y

```

Instalación de PHP

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 ~]# rpm http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
--2018-05-20 22:50:24-- http://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
Resolving dl.fedoraproject.org (dl.fedoraproject.org) ... 219.132.181.23, 219.132.181.24, 219.132.181.25
Connecting to dl.fedoraproject.org (dl.fedoraproject.org)|219.132.181.23| 80: connected.
HTTP request sent, awaiting response... 200 OK
Length: 15066 (15K) [application/x-rpm]
Saving to: 'epel-release-latest-7.noarch.rpm'

100% |-----| 15.00K -- -0/s 1s 0.1s

2018-05-20 22:50:24 (119 KB/s) = 'epel-release-latest-7.noarch.rpm' saved [15066/15066]

[root@cacti ~]# rpm -ivh epel-release-latest-7.noarch.rpm
warning: epel-release-latest-7.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 3526da5b: NOKEY
Preparing...
Updating / installing...
 1: epel-release-7-11
```

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 mirror usa.mia.mir
 * epel mirror espoch.mia.ec
 * extras mirror usa.mia.mir
 * updates mirror usa.mia.mir

repo id                               repo name                               status
base/7/x86_64                          CentOS-7 - Base                         9.811
epel/x86_64                              Extra Packages for Enterprise Linux 7 - x86_64 12,542
updates/7/x86_64                        CentOS-7 - Updates                       291
epelset: 25,182                          CentOS-7 - Updates                       539
```

Verificación del repositorio instalado

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

```
[root@cacti ~]# yum install cacti cacti-spine
```

Package	Arch	Version	Repository	Size
Dependencies Resolved				

Installing:				
cacti	x86_64	1.1.27-1.el7	epel	8.9 K
Installing the dependencies:				
libmnl	x86_64	2.0.10-1.el7	epel	38 K
libnftnl	x86_64	1.0.3-1.el7	base	37 K
libnl3	x86_64	3.2.25-1.el7	base	53 K
Transaction Summary				

Install 1 Package (+4 Dependent packages)				
Total download size: 7.8 K				
Installed size: 28 K				
Is this ok [y/N]:				

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

```
[root@cacti ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 3
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> create database cacti;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> GRANT ALL ON cacti.* TO cacti@localhost IDENTIFIED BY 'cacti';
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> FLUSH privileges;
Query OK, 0 rows affected (0.00 sec)

MariaDB [(none)]> quit
bye
```

Configuración de la base de datos cacti con el usuario cacti

- Instalación 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  = 'cacti';
$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 así 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:



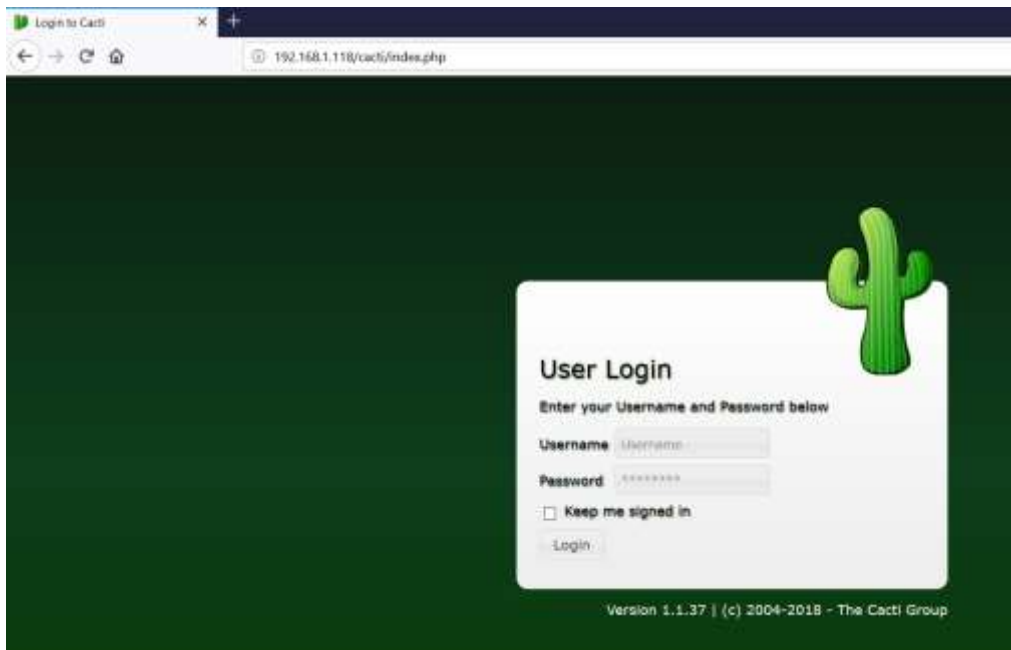
Acceso a la herramienta via http

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.

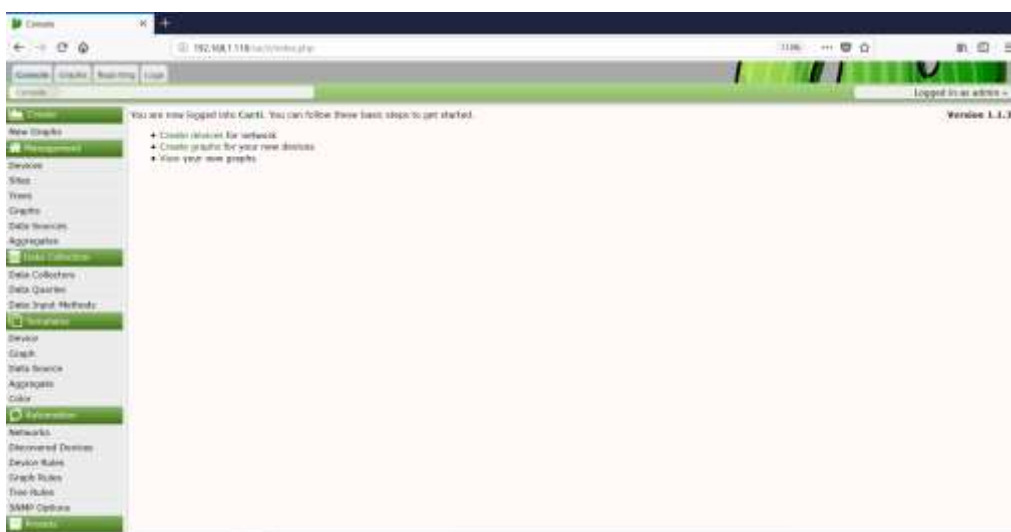
max_connections	151	>= 100	Depending on the number of logins and use of spare data collectors, MySQL will need many connections. The calculation for sparis is: $total_connections = total_processors * (total_threads + script_servers + 1)$, then you must leave headroom for user connections, which will change depending on the number of concurrent login accounts.
max_heap_table_size	128M	>= 128M	If using the Cacti Performance Booster and choosing a memory storage engine, you have to be careful to flush your Performance Booster buffer before the system runs out of memory table space. This is done two ways, first reducing the size of your output columns to just the right size. This column is in the tables <code>poller_output</code> and <code>poller_output_backup</code> . The second thing you can do is allocate more memory to memory tables. We have arbitrarily chosen a recommended value of 10% of system memory, but if you are using 300 GB of disks, or have a smaller system, you may agree this recommendation or choose a different storage engine. You may see the expected consequences of the Performance Booster tables under Console -> System Utilities -> View Fastest Status.
max_allowed_packet	16777216	>= 16777216	With remote polling capabilities, large amounts of data will be synced from the main server to the remote pollers. Therefore, keep this value at or above 16M.
tmp_table_size	64M	>= 64M	When executing subqueries, having a larger temporary table size, keep these temporary tables in memory.
join_buffer_size	64M	>= 64M	When performing joins, if they are below this size, they will be kept in memory and never written to a temporary file.
innodb_file_per_table	ON	ON	When using InnoDB storage it is important to keep your table spaces separate. This makes managing the tables simpler for long term users of MySQL. If you are running with this currently off, you can migrate to the per file storage by enabling the feature, and then running an alter statement on all InnoDB tables.
innodb_buffer_pool_size	681M	>= 681M	InnoDB will hold as much tables and indexes in system memory as is possible. Therefore, you should make the <code>innodb_buffer_pool</code> large enough to hold as much of the tables and index in memory. Checking the size of the <code>/var/lib/mysql/cacti</code> directory will help in determining this value. We are recommending 25% of your systems total memory, but your requirements will vary depending on your systems size.
innodb_flush_at_commit	OFF	OFF	With modern SSD type storage, this operation actually degrades the disk usage rapidly and adds a 50% overhead on all write operations.
innodb_additional_mem_pool_size	60M	>= 60M	This is where metadata is stored. If you had a lot of tables, it would be useful to increase this.
innodb_lock_wait_timeout	50	>= 50	Regular queries should not for the database to go offline to others. All these queries before they kill your system.
innodb_flush_log_at_trx_commit	2	2	Setting this value to 2 means that you will flush all transactions every second rather than at commit. This allows MySQL to perform writing less often.

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:



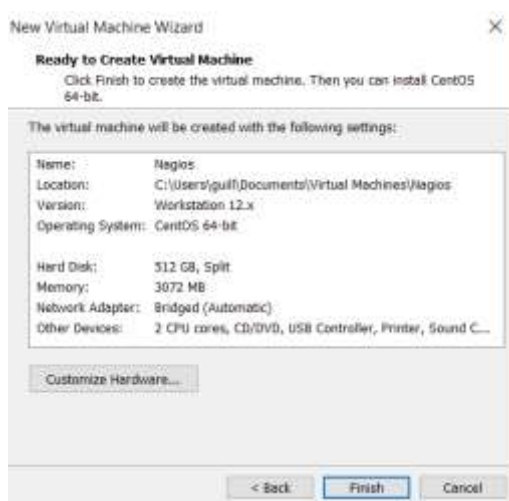
Pantalla para el ingreso de las credenciales de la herramienta



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.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-862.el7.x86_64 on an x86_64

nagios login: root
Password:
[root@nagios ~]# yum -y update
```

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.

```
[root@nagios ~]# yum install httpd
```

Package	Arch	Version	Repository	Size
Dependencies Resolved				
Installing:				
httpd	x86_64	2.4.18-0.el7.centos	base	2.1 M
Installing for dependencies:				
apr	x86_64	1.4.9-2.el7_4.1	base	103 K
apr-util	x86_64	1.5.2-6.el7	base	90 K
httpd-tools	x86_64	2.4.18-0.el7.centos	base	49 K
mailcap	noarch	2.1.41-2.el7	base	32 K

```
Transaction Summary
Install 1 Package (+4 dependent packages)
Total download size: 3.0 M
Installed size: 22 M
Is this ok [y/N]:
```

Instalacion de Apache

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

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

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

Habilitacion y opción de arranque de apache

- Instalación de MariaDB y sus dependencias.

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

Package	Arch	Version	Dependency	Size
Installing	x86_64	1:10.5.9-2.el7	base	8.7 M
Installing	x86_64	1:10.5.9-2.el7	base	11 M
Installing for dependencies:				
mysql-libs	x86_64	2.081-3.el7	base	32 k
mysql-Connector-ODBC	x86_64	1:2.500-4.el7	base	37 k
mysql-Connector-Python	x86_64	4.020-4.el7	base	149 k
mysql-Connector-Java	x86_64	1.027-4.el7	base	802 k
mysql-Connector-C++	x86_64	2.145-3.el7	base	47 k
mysql-Connector-Perl	x86_64	2.061-2.el7	base	209 k
mysql-Connector-C#	x86_64	2.080-4.el7	base	51 k
mysql-Connector-Nodejs	x86_64	2.020-14.el7	base	18 k

```

Transaction Summary
-----
Install 1 Package (+9 dependent packages)
Total download size: 21 M
Installed size: 135 M
Is this ok [y/N]:

```

Instalacion de MariaDB

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

```
[root@nagios ~]# systemctl start mariadb
```

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

Habilitacion y configuración de arranque de MariaDB

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

```
[root@nagios ~]# mysql_secure_installation
```

```

NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MariaDB
SERVERS IN PRODUCTION USE! PLEASE READ EACH STEP CAREFULLY!

In order to log into MariaDB to secure it, we'll need the current
password for the root user. If you've just installed MariaDB, and
you haven't set the root password yet, the password will be blank,
so you should just press enter here.

Enter current password for root (enter for none):
OK, successfully used password, moving on...

Setting the root password ensures that nobody can log into the MariaDB
root user without the proper authorization.

Set root password? [Y/n] Y
New password:
Re-enter new password:
Password updated successfully!
Reloading privilege tables..
... Success!

By default, a MariaDB installation has an anonymous user, allowing anyone
to log into MariaDB without having to have a user account created for
them. This is intended only for testing, and to make the installation
go a bit smoother. You should remove them before moving into a
production environment.

Remove anonymous users? [Y/n] Y
... Success!

Normally, root should only be allowed to connect from 'localhost'. This
ensures that someone cannot guess at the root password from the network.

Disallow root login remotely? [Y/n] Y
... Success!

By default, MariaDB comes with a database named 'test' that anyone can
access. This is also intended only for testing, and should be removed
before moving into a production environment.

Remove test database and access to it? [Y/n] Y
- Dropping test database...
... Success!

```

Configuración de MariaDB

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

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

Package	Arch	Version	Repository	Size
Dependencies Resolved				
Installing:				
php	x86_64	5.4.24-45.el7	base	2.9 M
php-mysql	x86_64	5.4.24-45.el7	base	221 k
Installing for dependencies:				
libicu	x86_64	4.10.1-0.el7	base	40 k
php-cli	x86_64	5.4.24-45.el7	base	2.7 M
php-common	x86_64	5.4.24-45.el7	base	885 k
php-gd	x86_64	5.4.24-45.el7	base	55 k
Transaction Summary				
Install 2 packages (+4 dependent packages)				
Total download size: 4.9 M				
Installed size: 18 M				
Is this ok [y/d/N]:				

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 dependencias necesarios para nagios.

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

Package	Arch	Version	Repository	Size
Dependencies Resolved				
Installing:				
gcc	x86_64	4.8.3-28.el7_3.1	epelbase	14 M
gd	x86_64	2.8.20-20.el7	base	144 k
gd-devel	x86_64	2.8.20-20.el7	base	75 k
net-snmp	x86_64	1.8.7.2-33.el7_3.2	epelbase	330 k
openssl-devel	x86_64	2.1.18-22.el7	base	1.3 M
xinetd	x86_64	2.3.15-13.el7	base	128 k
Installing the dependencies:				
rpm	x86_64	4.8.3-28.el7_3.1	epelbase	6.4 M
rpm-libs	x86_64	4.8.3-28.el7_3.1	base	37 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	228 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	128 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	9.9 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	308 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	1.1 M
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	478 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	7.1 M
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	37 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	289 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	66 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	39 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	805 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	14 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	29 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	55 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	26 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	173 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	32 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	98 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	173 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	32 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	122 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	189 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	77 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	12 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	1.9 M
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	203 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	705 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	epelbase	784 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	880 k
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	1.3 M
rpm-libs-devel	x86_64	4.8.3-28.el7_3.1	base	284 k

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.

```

[root@nagios ~]# curl -L -O https://s3.amazonaws.com/sourceforge.net/project/nagios/nrpe-2.x/nrpe-2.15/nrpe-2.15.tar.gz
% Total    % Received % Xferd Average Speed   Time    Time     Time  Current
           Dload  Upload   Total   Spent    Left    Speed
100 409k  100 409k    0     0  216k    0  0:00:01  0:00:01 --:--:--  216k

[root@nagios nrpe-2.15]# ./configure --enable-command-args --with-nagios-user=nagios --with-nagios-group=nagios --with-snl=/usr/local/openssl --with-ssl-lib=/usr/lib64/lib64-1
openssl

```

Configuración de NRPE

- Configuración de Apache.

```

[root@nagios ~]# htpasswd -c /usr/local/nagios/etc/htpasswd.users nagiosadmin
New password:
Re-type new password:
Adding password for user nagiosadmin

```

Configuración del acceso a apache

- Habilitación de servicios para el arranque de nagios.

```

[root@nagios ~]# systemctl daemon-reload
[root@nagios ~]# systemctl start nagios.service
[root@nagios ~]# systemctl restart httpd.service
[root@nagios ~]# chkconfig nagios on

```

Habilitación de servicios para nagios

- Restricción del acceso a nagios.

```

vim /etc/httpd/conf.d/nagios.conf

#       Order allow,deny
#       Allow from all
#       Order deny,allow
#       Deny from all
#       Allow from 127.0.0.1 192.168.1.0/24

```

Restricción del acceso a la herramienta nagios

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

```

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

```

Reinicio de servicios para iniciar nagios

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

Nagios®

Home
Documentation

Current Status

Tactical Overview
Map (Agents)
Hosts
Services
Host Groups
Services Groups
Out
Service Groups
Summaries
Out

Problems

Services
Entirehost
Hosts (Unreachable)
Network Outages

Quick Search:

Reports

Availability
Trends (Legacy)
Alerts
History
Summaries
Historians (Agents)
Notifications
Event Log

System

Comments
Downtime
Process Info
Performance Info

Nagios® Core™
✓ Daemon running with PID 82218

Nagios® Core™
Version 4.3.4
- August 24, 2017
Check for updates

Nagios XI
Easy Configuration
Advanced Reporting
Download

Nagios Log Server
Monitor and analyze
logs from anywhere
Download

Nagios Network Analyzer
Real-time network and
bandwidth analysis
Download

Get Started

- Start monitoring your infrastructure
- Change the look and feel of Nagios
- Extend Nagios with hundreds of add-ons
- Get support
- Get training
- Get certified

Quick Links

- Nagios Library (downloads and docs)
- Nagios Labs (development blog)
- Nagios Exchange (plugins and add-ons)
- Nagios Support (tech support)
- Nagios.com (company)
- Nagios.org (project)

Latest News

- Nagios Core Selected as SourceForge "Project of the Week"
- hCMA 2 Released
- Nagios Core 4.3.4 and NSCA 2.9.2 Released
- More news...

Don't Miss...

- Monitoring Log Data with Nagios** - Nagios Log Server can handle all log data in one central location
- Can Nagios monitor netflow?** - Yes! Nagios Network Analyzer can take in a variety of flow data. Learn more
- Nagios XI is Available Now!** - Easier configuration, Advanced Reporting. Download Today!

Get started on the N...
NAGIOS CORE
GET TOUR

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		
TÍTULO 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:	<p>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 Administración 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 eligió, características de los servidores en los cuales se alojaron las herramientas de monitoreo y configuración de cada una de ellas.</p>		
ADJUNTO PDF:	<input checked="" type="checkbox"/> SI	<input type="checkbox"/> NO	
CONTACTO CON AUTOR/ES:	Teléfono: +593-984149123	E-mail: gvega88p@gmail.com	
CONTACTO CON LA INSTITUCIÓN (COORDINADOR 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):			