FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

# IMPLEMENTACIÓN DE UN SISTEMA DE MONITOREO EN EL DATA CENTER DE LA EMPRESA SEGUROS ORIENTE S.A.

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Tecnólogo en redes y telecomunicaciones.


Profesor Guía

Ing. Fabián Wladimiro Basantes Moreno

Autor

Luis Alfredo Gavilanes Rivera



Año

2016

## DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante Luis Alfredo Gavilanes Rivera, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Ing. Fabián Wladimiro Basantes Moreno

Ingeniero en Electrónica y Telecomunicaciones

CI: 1709767667

## DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se ha citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____

Luis Alfredo Gavilanes Rivera

CI: 0918295270

**AGRADECIMIENTOS**

A mi tutor por su gran labor de ayuda al realizar esta tesis.

**DEDICATORIA**

Dedico ésta tesis a mi familia, que siempre ha estado a mi lado apoyándome, a mi madre, quien en vida luchó por darme la vida y salir adelante enseñándome el valor de la honestidad, la lucha constante y el no rendirme ante las situaciones difíciles, a mi esposa, quien es mi fuerza para seguir adelante cada día.

## RESUMEN

El objetivo de esta tesis es proveer a la empresa Seguros Oriente S.A. un sistema de monitoreo capaz de monitorear los dispositivos que se encuentran en la red, este aplicativo debe ser de bajo costo, ofrecer reportaría y monitoreo en tiempo real, para lo cual se ha elegido Zabbix, basa en software libre como herramienta de monitoreo, el cual permite llenar a cabalidad los inconvenientes de la empresa los cuales han sido reportados como falta de espacio en el disco duro del servidor de datos y saturación en el enlace de red.

## ABSTRACT

The objective of this thesis is to provide the company Seguros Oriente SA a monitoring system capable of monitoring devices on the network, this application mustn’t be expensive, and would report to provide real-time monitoring, for which they have chosen Zabbix, based on free software as a tool for monitoring, allowing fully fill the drawbacks of the company which have been reported as lack of space on the hard disk and saturation data server in the network link.

**Índice**

## Índice de Figuras

**Índice de Tablas**

# Capítulo 1 Introducción y Generalidades

## 1.1. Introducción

A medida del avance tecnológico, los procesos se vuelven más complejos y la necesidad de tener mayores velocidades en la utilización de varios dispositivos que se comunican entre sí, tales como computadores, tablets, celulares, hogares inteligentes etc., se vuelve evidente. Para ello se requiere de mecanismos para interrelacionar dos o más dispositivos entre sí en un entorno de red. Estos mecanismos son conocidos como protocolos, siendo éstos normas y procedimientos que rigen el intercambio de información entre diversos dispositivos electrónicos a través de una red.

De igual manera, con mejores comunicaciones, toda empresa que posea servicios informáticos, requiere de un monitoreo constante de su tráfico en la red con el fin de mantener el servicio entrega al usuario activo y confiable.

## 1.2. Definiciones

### 1.2.1. Arquitecturas

La arquitectura de red se la puede definir como el medio más efectivo para desarrollar e implementar una conexión de dispositivos que se puedan interconectar e intercambiar información y recursos entre sí, es el “plan” con el que se conectan los elementos de una red. Esta conexión permite un correcto intercambio de datos, para lo cual debe cumplir ciertas características básicas para mantener una comunicación fiable y funcione perfectamente, estas características son:

- Calidad del servicio.
- Tolerancia a fallos.
- Seguridad.
- Escalabilidad.

**Tolerancia a fallos**

Una red tolerante a fallos es aquella que limita el impacto frente a un error de software o hardware pudiendo recuperarse de dicho error rápidamente. Por ejemplo, si se envía un mensaje y se presenta un error de enrutamiento, la red tendría que enviar inmediatamente el mismo mensaje pero por una ruta distinta de tal forma que el destinatario no perciba dicho error y reciba sin problemas el mensaje. Para aplicar este sistema se utiliza una técnica llamada redundancia que consiste en implementar varios caminos o soluciones, si uno falla, se tienen más y el mensaje siempre llegue a su destinatario.

**Escalabilidad**

Esta característica consiste en permitir el crecimiento de las redes sin repercutir en su funcionamiento.

**Calidad del servicio**

Para brindar una buena calidad de servicio se utilizan las prioridades, para que así, se gestione prioridad más alta por ejemplo a una transmisión de video que a una página web, ya que esta última no requiere tantos servicios para funcionar correctamente.

**Seguridad**

La confidencialidad de los datos es primordial a la hora de enviar mensajes a través de una red, por lo cual se implementan sistemas que protejan la información de los usuarios que viaja a través de los diferentes medios digitales. Como sistemas de seguridad, en las redes se utilizan sistemas de contraseñas cifradas, firewall, encriptadores de datos, etc.

Dentro de los tipos de arquitectura se encuentran:

- Red Centralizada
- Red Descentralizada
- Redes Distribuidas

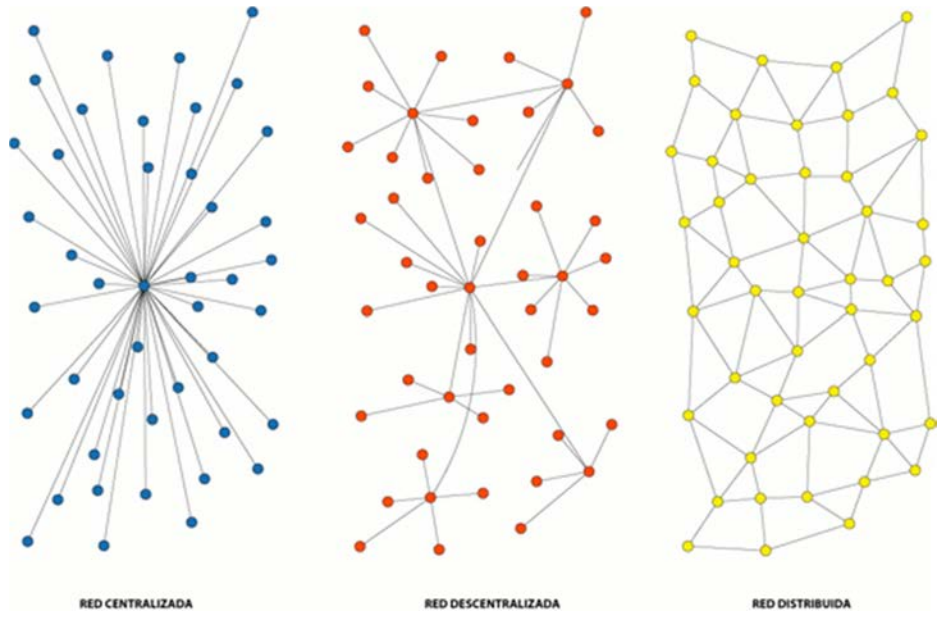



*Figura 1 Tipos de arquitectura de red.*
*Tomado de: (El Correo de las Indias, 2002)*

**Red Centralizada**

También conocida como Cliente-Servidor, y es aquella red de comunicaciones en la que todos los clientes están conectados a un servidor central, que puede ser cualquier computador que centraliza los diversos recursos y aplicaciones con los que se dispone; y que son puestos a disposición de los clientes cada vez que los requieran. Quiere decir que todas las gestiones que se realizan se concentran en el servidor, permitiendo así tener control de permisos con los archivos que son de uso público y los que son de uso restringido. La principal característica es que en este tipo de redes los roles están bien definidos y no se intercambian; los clientes en ningún momento pueden ser servidores y viceversa.

Este modelo aporta mayor seguridad, rendimiento y menores costos ya que una sola PC centraliza y distribuye toda la información, sin embargo la caiga del nodo principal provoca una pérdida de los servicios de la red.

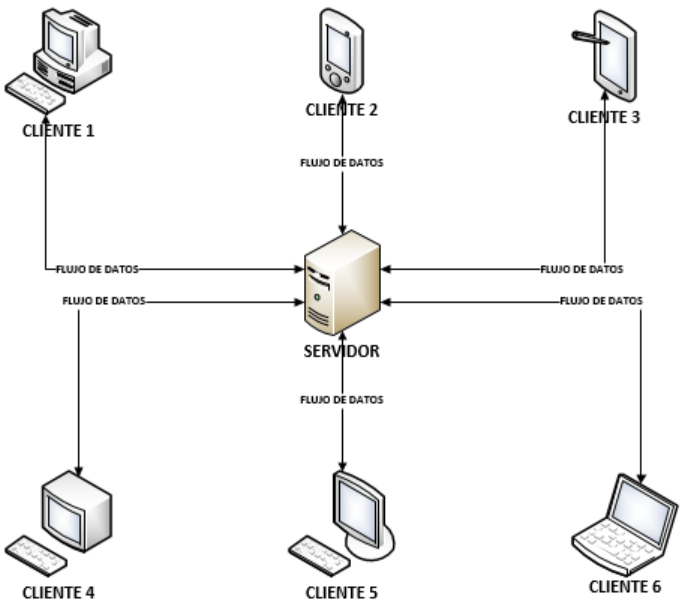



Figura 2. Flujo de Información Arquitectura Cliente – Servidor.

**Red Descentralizada**

Aparece por la interconexión de los nodos centrales de varias redes centralizadas, no existiendo un nodo central único sino un centro colectivo de nodos centrales. La caída de uno de los nodos centralizadores, provocaría la desconexión de los servicios de ese único nodo dejando intacto el servicio para los demás nodos interconectados.

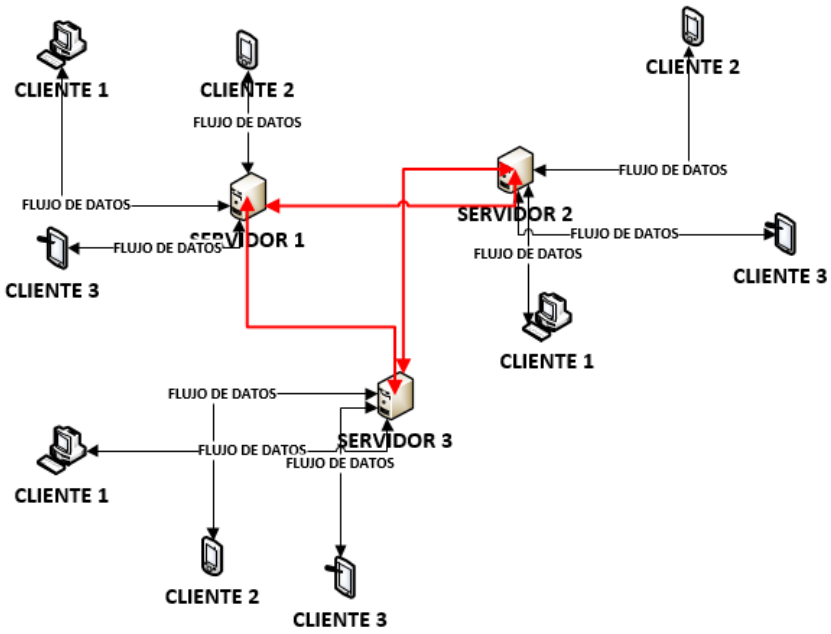



Figura 3. Flujo de Información Arquitectura Descentralizada.

**Red Distribuida**

Todos los nodos se conectan entre sí sin la necesidad de conectarse por uno o varios centros, con esto desaparece el control de permisos sobre la información que fluye por ella. La red es robusta ante la caída de nodos ya que ningún nodo es central y al no existir no genera desconexión de otro, de esta manera los

clientes pueden intercambiar roles en cualquier momento, pudiendo convertirse un cliente en servidor y viceversa.

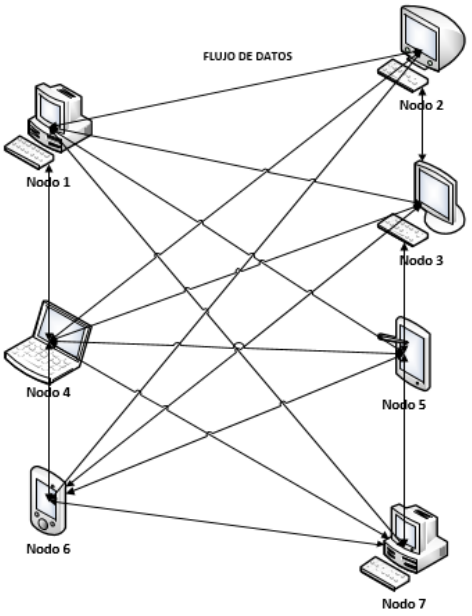



Figura 4. Flujo de Información Arquitectura Distribuida.

### 1.2.2. Ancho de Banda

El ancho de banda de una red informática se define como la cantidad máxima de información que puede fluir en un período de tiempo establecido a través de una conexión de red. El ancho de banda es finito ya que independiente de la arquitectura de la red utilizada existen límites en la transmisión de información. El ancho de banda está limitado por las tecnologías empleadas en la instalación de los medios físicos. Por ejemplo, el ancho de banda de un módem convencional tiene un límite aproximadamente de 56 kpbs por la tecnología del modem. Sin embargo, DSL utilizan los mismos cables telefónicos de par trenzado y ofrece un ancho de banda mucho mayor que los módems.

En los sistemas digitales, la unidad básica del ancho de banda es bits por segundo (bps). Por lo tanto se poden definir al ancho de banda como la cantidad de información, o bits, que puede fluir desde un lugar hacia otro en un período de tiempo determinado.

Se debe tener cuidado con las definiciones de ancho de banda y velocidad de transmisión, por ejemplo, se tiene una conexión T3 a 45Mbps y una conexión T1

a 1,544Mbps la primera conexión opera a mayor velocidad que la segunda, no obstante, si en la primera conexión sólo se utiliza una cantidad mínima de su capacidad para transportar datos, cada uno de estos tipos de conexión transportará datos a la misma velocidad. Esto es así porque la conexión T3 posee la capacidad para transportar más información en el mismo período de tiempo, y no porque tenga mayor velocidad.

Tabla 1, Unidad de Ancho de Banda.

| Unidad de Ancho de Banda | Abreviatura | Equivalencia |
|---|---|---|
| **bits por segundo** | bps | 1 bps= unidad fundamental del ancho de banda. |
| **Kilobits por segundo** | kbps | 1kbps=1000 bps |
| **Megabits por segundo** | Mbps | 1Mbps=1000,000bps |
| **Gigabits por segundo** | Gbps | 1 Gbps=1000,000,000bps |
| **Terabits por segundo** | Tbps | 1 Tbps=1000,000,000,000bps |

**Tasa de Transferencia**.

La tasa de transferencia se refiere a la medida real del ancho de banda, en un momento dado del día, usando rutas de Internet específicas, y al transmitirse un conjunto específico de datos (Gerald Aguirre & Himura Productions Inc, 2012). Generalmente, la tasa de transferencia es menor que el ancho de banda digital.

### 1.2.3. Tráfico de Red

Se puede definir al tráfico de red como la cantidad de información que atraviesa un medio físico, este puede ser cable UTP, coaxial, fibra óptica, etc., siendo medible y administrable.

El tráfico de red puede ser comparado con una autopista, cuando se tiene una cantidad menor de autos (datos) circulando por una carretera de dos carriles (ancho de banda) fluirán con mayor facilidad que teniendo la carretera saturada. Por esta razón el tráfico de red debe ser constantemente monitoreado para

prevenir un cuello de botella y garantizar el correcto funcionamiento de los servicios ofrecidos.

Existen varios tipos de tráfico de red entre ellos se tiene:

- Voz
- Datos

Esta tesis se preocupará del tráfico de una red de datos conocida como cliente – servidor, llamado así porque existe una comunicación entre un host, el cual realiza peticiones sobre un servicio a un servidor dedicado para ofrecer ciertos servicios. Mientras más alto es el tráfico en una red cliente – servidor, el servicio ofrecido se vuelve lento y el servidor pierde capacidad de respuesta ante el cliente.

Actualmente, se procura realizar análisis de tráfico de red, utilizando varios métodos, a través de herramientas que permiten determinar cuando los canales

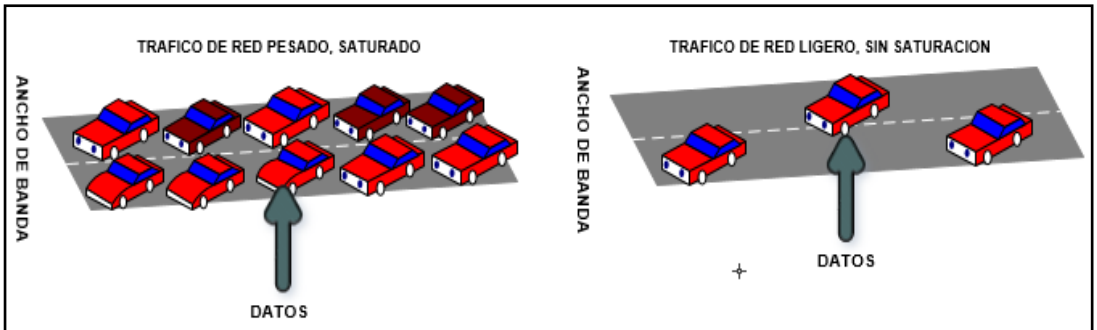



Figura 5, Canal de Red Saturado y Despejado.

de red de datos se encuentren próximos a saturarse y tomar correctivos necesarios, ésta metodología se conoce como QoS (Quality of service), siendo estándares que permiten optimizar en tiempo real el ancho de banda de la red, por ejemplo, se tiene una empresa con múltiples enlaces dedicados de datos y ofrece varios servicios, el estándar QoS nos ayuda a determinar el momento que un canal se encuentre saturado y comienza a enviar los paquetes por medio de otro canal, manteniendo el servicio activo liberando de tráfico a ciertos canales y retransmitiendo la información por los enlaces que se encuentran vacíos o con capacidad de transmisión más alta. Como se observa en el grafico siguiente

Los Estándares QoS son conocidos como RFC (Requests for Comments) “son un conjunto de informes, propuestas de protocolos y estándares de protocolos

utilizados por la comunidad de Internet. Los estándares de Calidad de servicio (QoS, Quality of Service) están definidos en las RFC publicadas por el Grupo de trabajo de ingeniería de Internet (IETF, Internet Engineering Task Force) y otros grupos de trabajo.

Las siguientes RFC tratan aspectos de QoS:
2211 : Specification of the Controlled-Load Network Element Service (especificación del servicio de elementos de red de carga controlada)
2212: Specification of Guaranteed Quality of Service (especificación del servicio de calidad garantizada)" (Estándares de QoS (RFC), 2016)
Existen dos mecanismos QoS utilizados para controlar la calidad de una red de datos:
IntServ (Integrated Services) y protocolo RSVP. El usuario solicita realiza una solicitud previa de los recursos necesarios y los routers implicados en el trayecto reservan los recursos solicitados.

DiffServ (Differentiated Services). Los paquetes son marcados por niveles de prioridad, los routers agregan y distribuyen las demandas de los usuarios, este método es el más utilizado actualmente.

**PROTOCOLOS DE RED**

Se denomina protocolo de red informática o protocolo de comunicación al conjunto de normas y criterios necesarios para comunicarse entre los diversos componentes de un sistema de redes de datos. Es decir, son estándares que determinan la manera en cual debe comenzar y terminar la conexión de datos entre los equipos electrónicos. Para que la comunicación se realice es necesario que el transmisor y el receptor tengan configurados el mismo protocolo de red, adicionalmente deben poseer una dirección IP (ver los diferentes tipos de conexión) la misma que es un numero único en cada segmento de red e identifica a cada dispositivo dentro de la misma red
Dentro de las funciones principales de los protocolos de red se encuentran la detección y corrección de errores, que realiza determinando que exista un punto

inicial y uno final en el momento de la conexión. El instante que se realiza la conexión los protocolos determinan la forma idónea de realizar transmisión de información e intercambio de datos dentro de una red.

Existen varios protocolos como son:

**TCP (Protocolo de Control de Transmisión):** protocolo orientado a comunicaciones, el cual ofrece una transmisión de datos fiable, además se encarga de ensamblar los datos que provienen de las capas superiores hacia las capas inferiores, asegurando que la transferencia de datos sea correcta.

**HTTP (Protocolo de Transferencia de Hipertexto):** Permite recuperar la información y realizar búsquedas indexadas, los mismos que admiten saltos intertextuales de forma eficiente. Por otro lado, permiten transferencia de textos de diversos formatos, no sólo HTML, fue desarrollado para resolver problemas provenientes del sistema hipermedia.

**FTP (Protocolo de Transferencia de Archivos):** Es utilizado el momento de realizar transferencias remotas de archivos, por lo general pc es el dispositivo local, mientras que el remoto es el servidor.

**SSH (Interprete de Orden Seguro):** Fue desarrollado para mejorar la seguridad de las comunicaciones de internet, para lo cual se elimina el envío de contraseñas no cifradas y codificando toda la información transferida.

**UDP (Protocolo de Datagrama de Usuario):** el protocolo de datagrama de usuario está destinado a aquellas comunicaciones que se realizan sin conexión y que no cuentan con mecanismos para transmitir datagramas. Esto se contrapone con el TCP que está destinado a comunicaciones con conexión. Este protocolo puede resultar poco confiable excepto si las aplicaciones utilizadas cuentan con verificación de confiabilidad.

**SNMP (Protocolo Simple de Administración de Red):** protocolo compartido que utiliza el protocolo PDU como mecanismo de transporte, utiliza también distintos agentes y administradores TCP/IP en lugar de clientes y servidores. El administrador se comunica por medio de la red, mientras que el agente envía la información sobre un determinado dispositivo.

**SMTP (Protocolo Simple de Transferencia de Correo):** este protocolo está compuesto por una serie de reglas que rige la transferencia y el formato de datos

en los envíos de correos electrónicos. SMTP suele ser muy utilizado por clientes locales de correo que necesiten recibir mensajes de e-mail almacenados en un servidor cuya ubicación sea remota.

**ARP (Protocolo de Resolución de Direcciones):** por medio de este protocolo se logran aquellas tareas que buscan asociar a un dispositivo IP, el cual está identificado con una dirección IP, con un dispositivo de red, que cuenta con una dirección de red física. ARP es muy usado para los dispositivos de redes locales Ethernet. Por otro lado, existe el protocolo **RARP** y este cumple la función opuesta a la recién mencionada. (Simple Organization, 2012-2015)

Con la aparición de los protocolos las organizaciones tuvieron que organizarlos en diferentes capas, las mismas que agrupan a los protocolos a cumplir funciones específicas, este conjunto de capas se denomina modelo, el primer modelo en aparecer fue el modelo OSI el mismo que consta de 7 capas y es una referencia de estudio para la compresión del modelo TCP/IP, modelo que es orientado a internet.

## 1.3. Modelos de Redes de Computadores

En los últimos siglos se han implementado nuevos tipos de Hardware y Software, antiguamente esto causaba que hubiera interferencias y pésima comunicación entre ellas, la organización que soluciono este problema fue la ISO (*International Organization for Standarization*), ellos realizaron y esquematizaron las redes, sin embargo se dieron cuenta que era necesario crear una nueva topología y un nuevo modelo. Un nuevo modelo nace en el año de 1984 con el nombre que tiene ahora, es decir modelo OSI *(Open System Interconnection*)**.**

(Ross & Kurose, 2010)(pg 55)

### 1.3.1. Modelo OSI

A finales del año 1970, la Organización Internacional de Estandarización (ISO, *con sus siglas en inglés International Organization for Standardization*) planteó que las redes de computadoras se organicen usando siete capas denominando a este modelo OSI (*Open Systems Interconnection*, Interconexiónde sistemas abiertos).

#### 1.3.1.1. Generalidades

El modelo OSI (por sus siglas en inglés *OPEN SYSTEM INTERCONECTION*) está conformado por 7 capas, las mismas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función que se realiza cuando los datos son transferidos entre aplicaciones a través de una red intermedia.

El modelo OSI fue creado con los siguientes objetivos:

- Estructura multinivel: Diseñada con la idea de que cada nivel posea funciones dedicadas a resolver partes específicas del problema de comunicación. Cada nivel superior utiliza los servicios de los niveles inferiores.
- Puertos (Ports): Entre niveles existen interfaces físicas llamadas "Ports", los que se encargan de la transmisión diferentes tipos de datos.
- Dependencias de Niveles: Cada nivel es dependiente del nivel inferior y también del superior.
- Encabezados: En cada nivel, se adjunta al mensaje una trama de control. Este elemento permite que el receptor conozca que el emisor se encuentra enviándole información. Un mensaje está constituido de dos partes: Encabezado e Información. Una vez realizado el proceso en cada capa el receptor retira los encabezados en orden inverso a como fueron incorporados en el emisor, por lo cual finalmente el usuario sólo recibe el mensaje original.

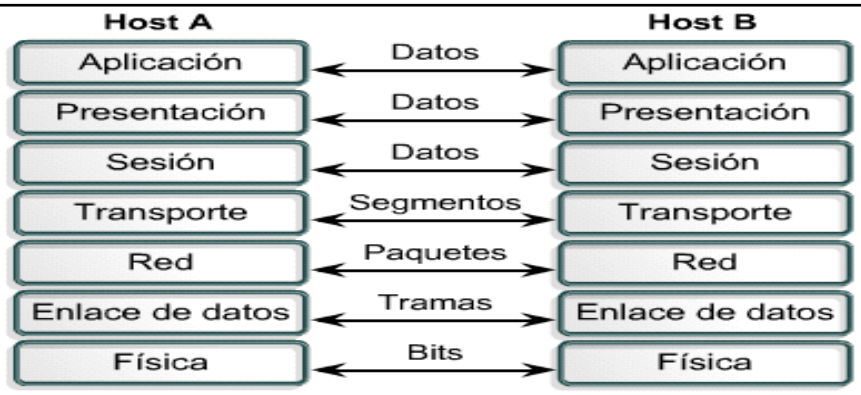



Figura 6: Protocolo de transmisión de datos.
Tomado de: (León, 2005)

**Proceso de transmisión de datos**

El modelo OSI está conformado por capas, las mismas que se las describe en orden descendente, siendo la última capa la primera en ser recibida en la transmisión de datos, como se muestran en la Figura 7

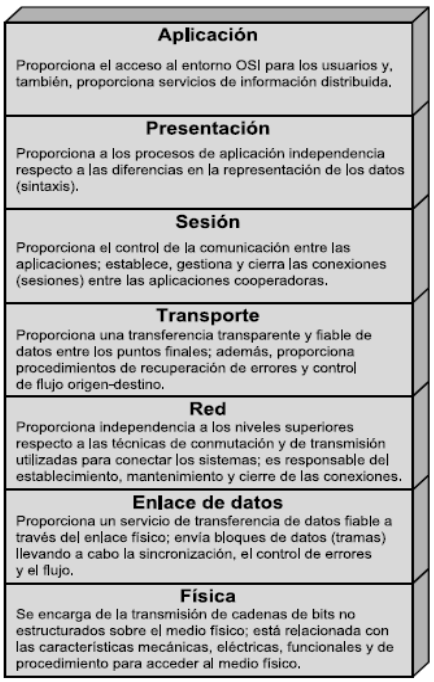



*Figura 7, Modelo OSI.*
*Tomado de: (Stallings, 2004), Pag 31*

### 1.3.1.2. Capas

**Capa física**

Esta capa es la más baja del modelo OSI, la misma que se encarga de las conexiones globales del computador, es el medio físico por la cual se transmiten los datos.

Las funciones principales de esta capa son:

- Definir el medio o medios físicos por los que se realizará la comunicación (utp, coaxial, fibra óptica) así como los materiales y componentes que se utilizaran en la transmisión de datos
- Transmitir el flujo de bits a través del medio.
- Garantizar que se realice la conexión sin asegurar la fiabilidad

**Capa de datos**

Es la encargada de realizar la transmisión de los datos sin errores, sin duplicaciones ni perdidas de paquetes, es decir que permite la transferencia confiable de los datos a través de los medios físicos.

Las funciones principales son:

- Realizar la conexión sin errores
- Control de tráfico de tramas para que no exista una transmisor innecesaria
- Detecta errores y se recupera de ellos cuando se producen en la capa física.
- Crea y reconoce los límites de la trama
- Comprobación de errores de las tramas
- Administración de accesos

En la capa de enlace de datos los paquetes se organizan en unidades llamadas tramas o también llamadas PDU, las mismas que tienen cabeceras, y que poseen dirección e información de control y una cola, que es usada para la detección de errores.

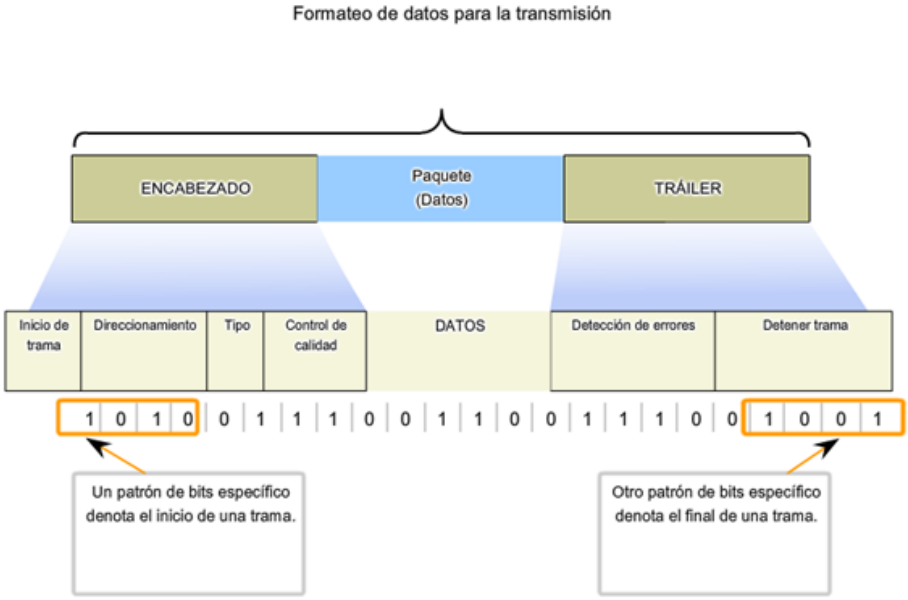



Figura 8, Tramas.

Tomado de: (Ronald Pinos, 2014)

Las **unidades de datos de protocolo**, también llamadas **PDU**, se a la forma que adopta una porción de datos en cualquier capa del modelo OSI, cada capa encapsula las PDU que recibe de la capa inferior de acuerdo al protocolo que utiliza. En cada etapa del proceso, una PDU tiene un nombre distinto para reflejar sus nuevas funciones. Existen dos clases de PDU:

- De datos, que contiene datos del usuario principal (en caso de la capa de aplicación).
- De control, que sirven para controlar el comportamiento completo del protocolo en las funciones de establecimiento y unión de la conexión, control de flujo, control de errores, etc. No contienen información alguna proveniente del nivel N+1.

Las PDU cambian de nombre en cada capa del modelo OSI como se observa a continuación:

- **Datos:** término general para la PDU que se utiliza en la capa de aplicación.
- **Segmento:** PDU de la capa de transporte.
- **Paquete:** PDU de la capa de red

- **Trama:** PDU de la capa de enlace de datos
- **Bits:** PDU de la capa física que se utiliza cuando se transmiten datos físicamente por el medio

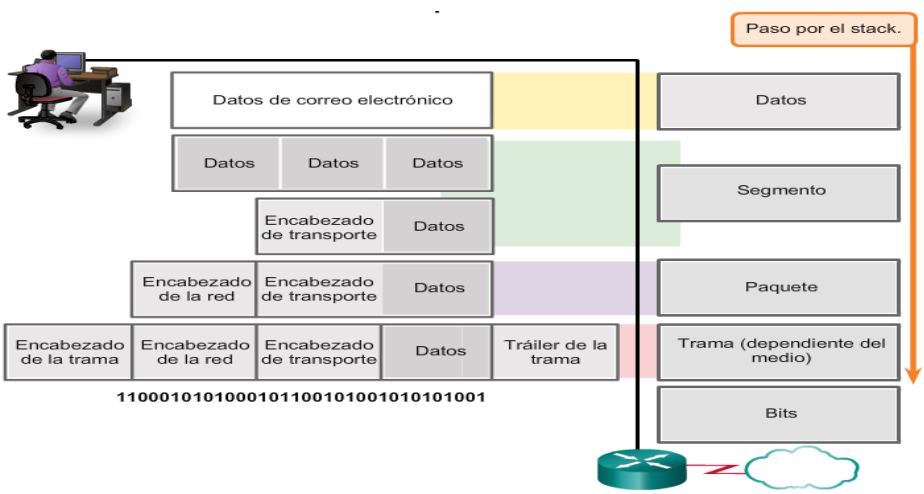



Figura 9, CAMBIO DE NOMBRE DE PDU.

Tomado de: (Itesa, s.f.)

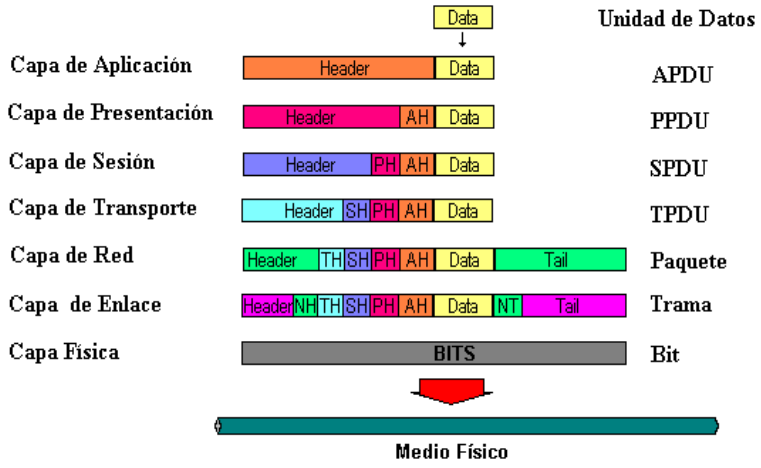



Figura 10, PDU EN CADA CAPA OSI.

Tomado de: (Wikipedia, 2015)

**CAPA DE RED**

Es la encargada de realizar el direccionamiento y proporcionar la mejor ruta para que se realice la transmisión.

Para realizar el transporte de datos se utilizan cuatro procesos básicos:

- Direccionamiento
- Encapsulamiento
- Enrutamiento
- Des encapsulamiento

Direccionamiento. Por medio de la dirección de red que es la dirección única que posee cada host para poder ser identificado en la red.

Encapsulamiento. Es el proceso de empaquetar los datos con la información de protocolos necesaria antes de que comience la transmisión de datos.

Enrutamiento. Se encarga de dirigir los paquetes al host de destino. Cada vez que un paquete toma una ruta para llegar a su destino se lo denomina salto.

Des encapsulamiento. Cuando el paquete llega al receptor, la capa de red analiza la dirección para confirmar que sea enviado al host correcto, si la dirección es correcta el paquete es des encapsulado para pasar a la siguiente capa de transmisión.

**CAPA DE TRANSPORTE**

Esta capa se encarga de proporcionar servicios de detección y corrección de errores, permite segmentación de datos y brinda el control necesario para re ensamblar las partes de los PDU de la comunicación.

Las funciones principales en la capa de transporte se encuentran:

**Segmentación y reensamblaje:** Las redes en su mayoría poseen una limitación en la cantidad de datos que se pueden incluir en una única PDU. La capa de Transporte divide los datos de la aplicación en bloques de datos con un tamaño adecuado. En el destino, ésta capa se encarga de reensambla los datos antes de enviarlos a la aplicación o servicio de destino.

**Multiplexación de conversaciones**: Pueden existir varias aplicaciones o servicios ejecutándose en cada host de la red. A cada una de estas aplicaciones o servicios se les asigna una dirección conocida como puerto para que la capa de Transporte pueda determinar con qué aplicación o servicio identificar los

datos. Además de utilizar la información contenida en los encabezados para las funciones básicas de segmentación y reensamblaje de datos, algunos protocolos de la capa de Transporte proveen (Gallegos, Capa de transporte del modelo OSI, pág. 10):

- Conversaciones orientadas a la conexión,
- Entrega confiable,
- Reconstrucción ordenada de datos,
- Control del flujo.

**CAPA DE SESION**

Proporciona mecanismos para establecer la comunicación entre dos aplicaciones finales, administrando y terminando las sesiones cuando se termine la comunicación:

La capa de sesión proporciona los siguientes servicios:

- Control del Diálogo, puede ser:
  - Full-dúplex (simultáneo en los dos sentidos)
  - Half-dúplex (alternado en ambos sentidos)
- Agrupamiento: El flujo de datos se marca para definir grupos de datos.
- Recuperación: Si ocurre algún fallo entre los puntos de comprobación, la entidad de sesión retransmite todos los datos desde el último punto de comprobación y no desde el principio.

**CAPA DE PRESENTACION**

Se encarga de la representación de la información, quiere decir que traduce los caracteres en datos reconocibles.

La capa de presentación se encarga adicionalmente de aspectos como semántica y sintaxis de los datos transmitidos haciéndose reconocible entre distintos formatos de dispositivos.

La capa de presentación se encarga de:

- Traducir entre varios formatos de datos a un formato estándar.
- Definir la estructura de datos a transmitir.
- Definir el código a usar para representar en una cadena de caracteres.

- Dar formato a la información para visualizarla o imprimirla.
- Comprimir los datos.

**CAPA DE APLICACIÓN**

Brinda los servicios de comunicación a los usuarios, es la interfaz a través de la cual los usuarios visualizan la aplicación. Esta puede ser instalada en el dispositivo o vía web, las características principales son:

- Uso compartido de recursos y redirección de dispositivos
- Acceso a archivos y recursos remotos
- Comunicación entre procesos
- Administración de la red
- Servicios de directorio
- Correo electrónica
- Terminales virtuales de red

En la Figura 11 se encuentra el proceso de comunicación de datos en el cual la línea representada con rojo son los datos a transmitir se puede ver como atraviesa cada capa desde la primera capa en la primera pila (emisor) y continua por la última capa en la segunda pila (receptor).De igual manera se puede encontrar el proceso de desempaquetado de cada capa a la derecha

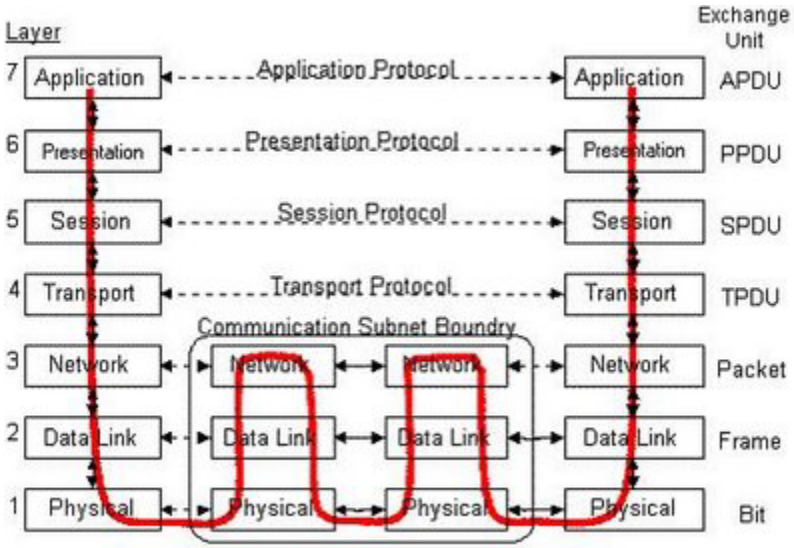



Figura 11: Capa de Aplicación del modelo OSI.

Tomado de: (Jose Solano, s.f.)

**Protocolos Utilizados en la transmisión de Datos**

El objetivo del modelo es apoyarse sobre normas para alcanzar la interoperabilidad. El modelo define sistemas, procedimientos y normas permitiendo el intercambio de información de una manera ordenada y segmentada. Los sistemas informáticos utilizan sistemas o métodos que les permiten comunicarse entre sí. Las funciones que cumple cada sistema son agrupados en capas, las capas permiten separar las diferentes funciones del proceso de comunicación de datos y evitar una complejidad demasiado grande dentro de cada capa los modelos están representados por medio de una pila.

En una capa no se define un único protocolo sino una función de comunicación de datos que puede ser realizada por varios protocolos. Siendo cada capa necesaria para que se realice la transmisión de datos en la siguiente.

Las capas superiores delegan en las inferiores los procedimientos para la transmisión de los datos a través de la red subyacente. Los datos descienden por la pila, de capa en capa, hasta que son transmitidos a través de la red por los protocolos de cada capa.

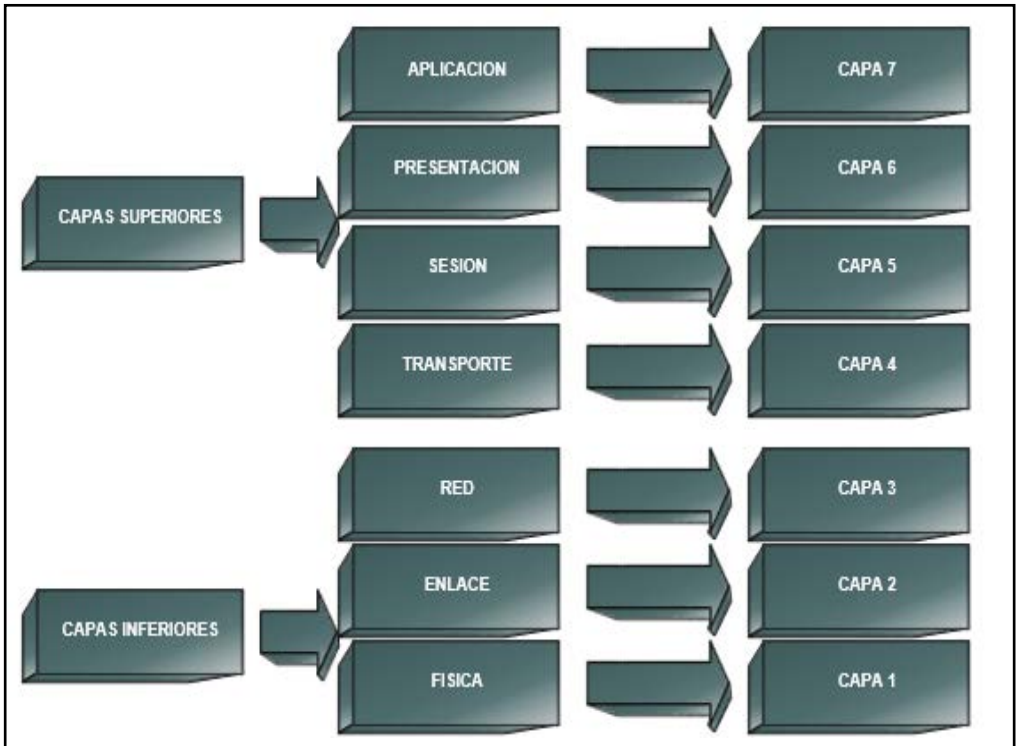



*Figura 12, Capas de Protocolos.*

**Clasificación de protocolos:**

**Orientados y No Orientados a conexión**

Los protocolos se clasifican en dos categorías según el nivel de control de datos requerido:

- **protocolos orientados a conexión**: controlan la transmisión de datos durante una comunicación establecida entre dos máquinas (por ejemplo la arquitectura Cliente-Servidor). El host receptor envía acuses de recepción durante la comunicación, por lo cual el host remitente es responsable de la validez de los datos que está enviando. TCP es un protocolo orientado a conexión.

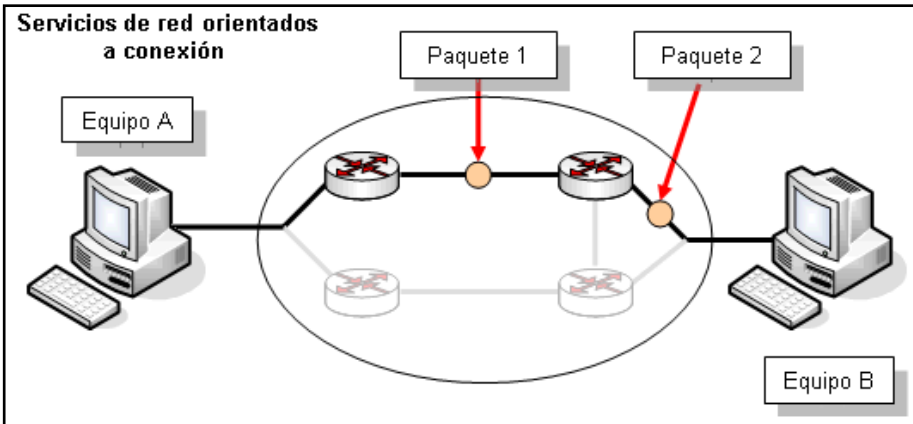



Figura 13, Servicios Orientados a Conexión.

Tomado de: (Adrformacion, 2015)

- **protocolos no orientados a conexión**: método de comunicación en el que el equipo remitente envía datos sin avisarle al equipo receptor, y éste recibe los datos sin enviar una notificación de recepción al remitente. Los datos se envían entonces como bloques

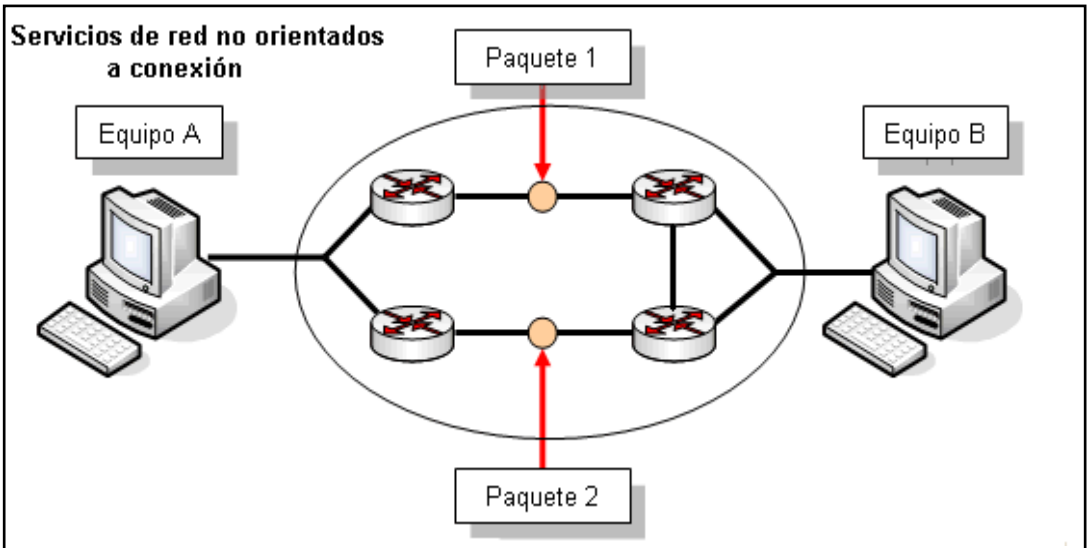



*Figura 14, Servicios no Orientados a Conexión.*
*Tomado de: (Adrformacion, 2015)*

### 1.3.2. Modelo TCP/IP

El Protocolo de Internet (IP) y el Protocolo de Transmisión (TCP), fueron desarrollados inicialmente por el informático estadounidense Vinton Cerf en el año 1973 como parte de un proyecto dirigido por el norteamericano Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPAnet) que conectaba redes de ordenadores de varias universidades y laboratorios en investigación en Estados Unidos. World Wibe Web se desarrolló en 1989 por el informático británico Timothy Berners-Lee para el Consejo Europeo de Investigación Nuclear (CERN, siglas en francés) (Alumnos, 1977).

#### 1.3.2.1. Generalidades

El TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, con diferentes sistemas operativos sobre redes de área local (LAN) y área extensa (WAN). TCP/IP propone un método de interconexión lógico de las redes físicas y define un conjunto de convenciones para el intercambio de datos. Fue desarrollado por el DARPA (Defence Advanced Research Projects Agancy), y es operacional sobre la red Internet. Este modelo se basa en el modelo OSI

El modelo TCP/IP se conforma de 4 niveles

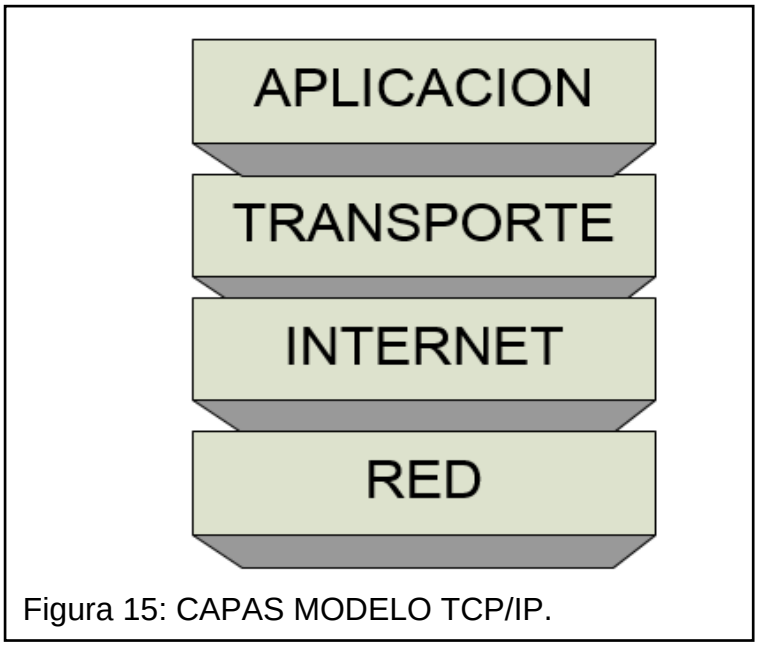



Figura 15: CAPAS MODELO TCP/IP.

### 1.3.2.2. Capas

**Capa de Red**

Es el interfaz de la red real, corresponde a la capa física y de enlace de OSI

**Capa de Internet**

Es el nivel de red del Modelo OSI. Incluye el protocolo IP, que se encarga de enviar los paquetes de información a sus destinos correspondientes.

**Capa de Transporte**

Coincide con el nivel de transporte del Modelo OSI. Los protocolos de este nivel, tales como TCP y UDP, se encargan de manejar los datos y proporcionar la fiabilidad necesaria en el transporte de los mismos.

**TCP:** significa Protocolo de Control de Transmisión es uno de los principales protocolos de la capa de transporte del modelo TCP/IP. El objetivo de este protocolo es comunicarse de manera segura realizando la comunicación de manera emisor – transmisor, más bien llamado cliente – servidor, orientado a conexión.

Las principales características del protocolo TCP son las siguientes:

- Permite colocar los datagramas nuevamente en orden cuando vienen del protocolo IP.
- Permite que el monitoreo de datos se realice en la capa de transporte liberando al router del monitoreo y así evitar la saturación de la red.
- Permite multiplexar los datos, es decir, la información que viene de diferentes aplicaciones circulen simultáneamente.

**UDP:** significa Protocolo de datagrama de usuario Protocolo no orientado a conexión, el cual no posee detección de errores y puede ser transmitido con retardo o errores durante la comunicación.

**CAPA DE APLICACIÓN**

Corresponde con los niveles OSI de aplicación, presentación y sesión.

Como ya se ha visto existe simmilitud entre las ambos modelos.

En la figura a continuacion se presenta una similitud entre ambas capas, tomando en cuenta que el modelo TCP/IP fue creado en base al modelo OSI

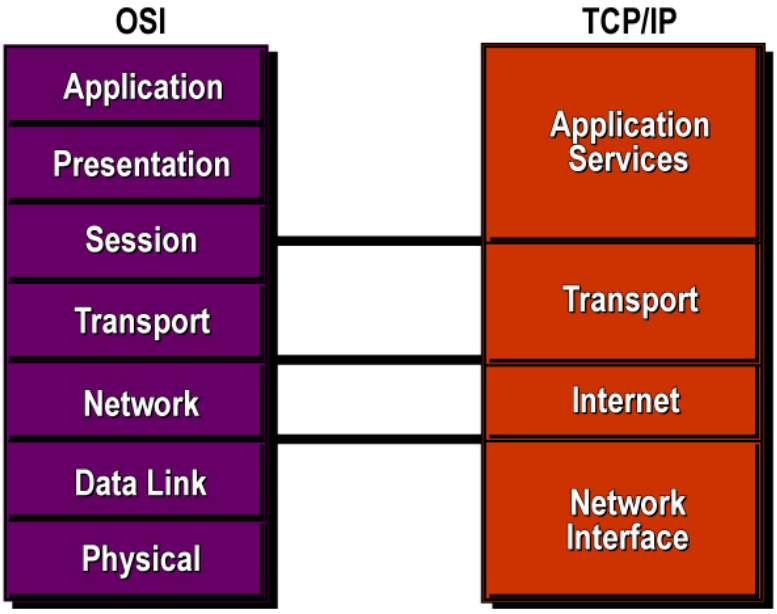



*Figura 16 Protocolo OSI y TCP/IP.*

*Tomado de: (Carol Mendoza , 2014)*

**PROTOCOLOS QUE INTERVIENEN EN AMBOS MODELOS DE TRANSMISION**

*Tabla 2, Protocolos del Modelo OSI,*

| MODELO OSI | PROTOCOLOS | MODELO TCP/IP | PROTOCOLOS |
|---|---|---|---|
| **Aplicación** | HTTP,HTTPS,DNS,SMTP,FTP,NFS | Aplicación | HTTP, SMTP, FTP, TELNET, NFS, DNS, LDAP, RLOGIN, RSH |
| **Presentación** | XDR, SMB, AFP | | |
| Sesión | TLS, SSH, TELNET, NETBIOS | | |
| Transporte | TCP, UDP, RPT, SCTP, SPX | Transporte | UDP,TCP.SCTP |
| **Red** | IP,ICMP,IGMP,ARP, RIP,OSI,IGRP,EIGRP,BGP | Internet | IP,IPV6,IPV6,ARP,ICMP |
| **Enlace de Datos** | ETHERNET, TOKEN RING, PPP, FRAME RELAY, ATM, IEEE 802.11 | Red | ETHERNET, TOKEN RING, FRAME RELAY, PPP, HDLC, CABLE COAXIAL, FIBRA OPTICA, RS 232 |
| **Físico** | COAXIAL, FIBRA ÓPTICA, RS232 | | |

## 1.4. Problemas de comunicación de red

Una red "lenta" o de bajo performance es un problema para cualquier empresa que provea servicios internos y externos, baja productividad e incluso sobrecarga de trabajo para el personal de soporte técnico.

Existen varias causas para la saturación o lentitud de una red, entre las cuales se encuentran:

- Placas de red defectuosas.
  Un problema frecuente es la presencia de nodos con placas de red defectuosas. Cuando se detectan intermitencias suelen deberse generalmente a este problema.
  En este caso el primer paso es verificar el LED de la placa de red:
- Cuando el Led se encuentra apagado puede ocurrir que el cable de conexión esté desconectado, defectuoso o no sea el correcto.
  Si la conexión a la red es correcta y la placa está adecuadamente habilitada y configurada en Windows, el siguiente paso es reemplazar la placa de red.
- Fallas en switches o routers.
  En algunos casos los problemas de la red pueden parecer inconsistentes. Por ejemplo:
  No se pierde navegación web pero el servicio de correo electrónico "se pierde", o falla otro tipo de servicios http/https. En otros casos, cuando se mantiene una buena conexión de red el acceso a Internet es imposible.
  Si se tiene conectividad local pero se ha perdido parcial o totalmente el acceso a recursos de Internet, el problema puede solucionarse reiniciando el equipo de acceso a Internet (Access point o router).
  Cuando los problemas son de conectividad local, o simplemente se trata de una red switcheada pero excesivamente lenta, el problema puede solucionarse reiniciando el switch de acceso.
- Conexión de dispositivos en "daisy chaining".
  Cuando una red requiere ser aumentada (escalada), lo más común es realizar una conexión en cascada de los switches, con lo cual puede provocar retrasos en los saltos de las conexiones entre dispositivos.
- Conflictos de IP.
  Los servicios de DHCP en general, implementa sistemas que les permiten prevenir que 2 hosts utilicen la misma dirección IP. Sin embargo, ocasionalmente cuando se asigna direcciones ips estáticas puede ocurrir que dos dispositivos tengan la misma dirección ip. Este conflicto provoca una

caída en la red.

Para solucionar este problema es necesario verificar la configuración de DHCP para asegurarse de que no haya superposición de rangos de direcciones IP con aquellas direcciones IP que se asignan estáticamente a servidores y demás dispositivos.

- Exceso de aplicaciones que operan sobre la red.

  En varias ocasiones se ejecutan aplicaciones que requieren recursos superiores a los que puede proporcionar la red, los mismos que no han sido adecuadamente previstos.

  Por ejemplo, se utilizan sistemas de información que realizan consultas frecuentes sobre bases de datos, y que las consultas a la base de datos generen congestión sobre la red en los horarios pico.

  Hay que tener presente que en la actualidad hay múltiples aplicaciones como los sistemas de VoIP hasta aplicaciones de audio y video sobre Internet que generan tráfico de cadenas de paquetes sobre UDP que tienden a ocupar todo el ancho de banda disponible.

  Una combinación de estos elementos puede volver excesivamente lenta una red FastEthernet.

  Cuando se trabaja con sistemas de Telefonía IP es preciso asegurarse antes que se cuenta con los recursos necesarios para manejar el tráfico de voz y el de datos.

*Tabla 3, Indicador de Led en Tarjeta de red*

| **COLOR LED** | **ESTADO** | **DESCRIPCION** |
|---|---|---|
| Verde | Fijo | Tarjeta de red en buen estado |
| Verde/Amarillo | Parpadeante | Conexión activa / Procesando Trafico de red |
| Apagado | Apagado | Tarjeta deshabilitada / No existe proceso activo |

### 1.4.1. Posibles soluciones al problema de saturación en una red de área local (LAN)

En base a las posibles causas sobre la saturación y lentitud de red se presenta un cuadro donde se puede encontrar las posibles soluciones para los diferentes problemas:

*Tabla 4, Posibles soluciones al problema de saturación en red de área local (LAN),*

| **PROBLEMA** | **SOLUCION** |
|---|---|
| **Placas de red defectuosas.** | Cambio de placa |
| **Fallas en switches o routers.** | Reiniciar el dispositivo / configuración correcta del dispositivo |
| **Conexión de dispositivos en "daisy chaining".** | Minimizar los switches en cascada |
| **Conflictos de IP.** | Correcta configuración del dispositivo DHCP, revisión del diagrama de red |
| **Exceso de aplicaciones que operan sobre la red.** | Segmentación correcta del ancho de banda |

# Capítulo 2. Estado actual de la Red

En el capítulo a realizar se revisara la situación actual que presenta la empresa a la cual se procederá el análisis.

## 2.1. Estado actual de la Red Empresa Oriente Seguros

La empresa Oriente Seguros (Seguros Oriente S.A.) es una empresa aseguradora fundada en 1977 en la ciudad de Quito. Es una compañía aseguradora con diferentes productos tanto empresariales como individuales tales como:

Oriente Fianzas.- La fianza existe cuando una parte garantiza a otra el cumplimiento de una obligación de un tercero, en consecuencia, es un acuerdo suscrito entre tres partes: contratista, contratante y afianzador, dentro de este paquete de producto se aseguran los ramos de Seriedad de oferta, Fiel cumplimiento de contrato, Buen uso de anticipo y materiales, garantía aduanera. (SegurosOriente, 2015)

Oriente Construcción.- Son productos creados especialmente para salvaguardar proyectos inmobiliarios y cubrir daños o pérdidas materiales que puedan sufrir la obra, daños a terceros e incluso daños corporales a sus trabajadores a consecuencia de accidentes personales dentro de este paquete de producto se aseguran los ramos de Accidentes personales y responsabilidad civil de construcción, equipo y maquinaria, todo riesgo de montaje, todo riesgo en construcción. (OrienteSegurosEmpresa, 2015)

Oriente Pymes.- Oriente Seguros ofrece a los pequeños y medianos empresarios, pólizas de seguro diseñadas para salvaguardar los bienes de propiedad y responsabilidad del asegurado, cuya indemnización le permite cubrir las pérdidas patrimoniales ocasionadas en caso de un evento accidental, súbito e imprevisto. (http://www.segurosoriente.com/productos/seguros-empresariales/seguros-pymes/). Dentro de este paquete de producto se aseguran los ramos de incendio y líneas aliadas, robo, equipo electrónico,

transporte, rotura de maquinaria, lucro cesante en incendio y rotura de maquinaria, fidelidad, responsabilidad civil.

Dentro de los productos personales o individuales se tiene:

- Oriente Hogar
- Oriente Hogar Plus
- Oriente Hogar Premium

Todos estos productos ayudan a proteger el hogar y cada uno diferencia del monto de cobertura que disponen, cada plan aplica con las coberturas de:

- Daños de estructura
- Rotura de vidrios
- Remoción de escombros
- Responsabilidad Civil
- Robo

La empresa actualmente posee un total de 150 empleados, con su matriz ubicada en Quito y una sucursal el Guayaquil por medio de las cuales ofrece servicios a clientes internos y externos como:

*Tabla 5, Oriente Seguros, Tipo de Clientes y Servicios*

| **CLIENTES INTERNOS** | **CLIENTES EXTERNOS** |
|---|---|
| Listas de clientes con riesgos de lavados de activos(RCS) | Página web |
| Listas de clientes con riesgos de lavados de activos | PBX |
| Correo electrónico | Cotizadores de productos |
| SISE(Core financiero) | |

## 2.2. Diagrama de red

En el siguiente diagrama, se muestran los servidores que serán monitoreados para que los servicios permanezcan siempre óptimos y no exista lentitud en los enlaces

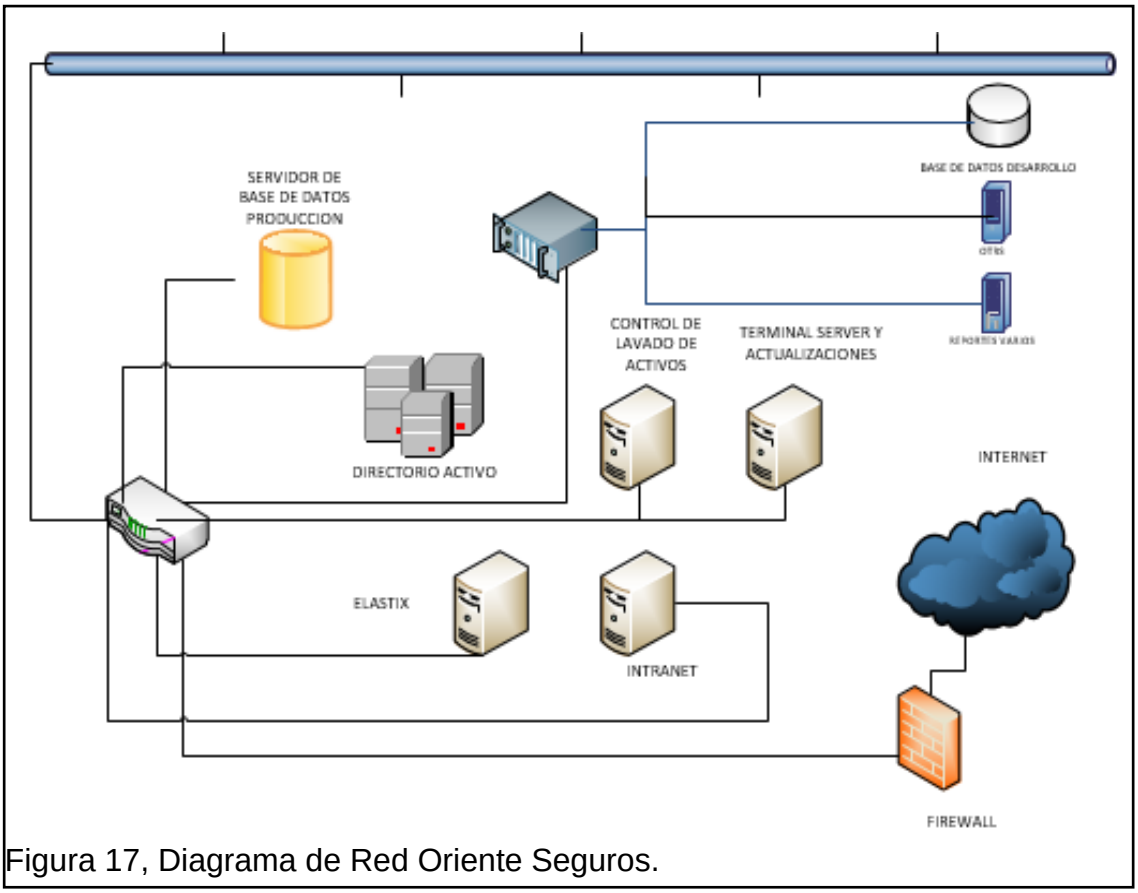



Figura 17, Diagrama de Red Oriente Seguros.

Cuenta con un data center en su oficina matriz con 10 servidores entre físicos y virtuales y cuenta con un ancho de banda de 4mb como enlace principal utilizado para datos y uno secundario de 3mb compartido entre datos y voz siendo provistos por PUNTONET .

Para los diferentes servicios se dispone de los servidores siguientes:

*Tabla 6, Servidores existentes*

| Servidor | Servicio | Tipo de servidor |
|---|---|---|
| Serverad | Directorio activo UIO | Físico |
| Srvrcs | Aplicativo web para control de lavado de activos | Físico |
| Svrb1 | Base de datos de producción | Físico |
| Svrb5 | Terminal server/actualizaciones | Físico |
| Srvotrs | Otrs | Virtual |
| Intranet | Intranet | Físico |
| Mail | Correo electrónico | Físico |
| Svrjetform | Reportes varios | Virtual |
| Dbdesarrollo | Base de datos de desarrollo | Virtual |
| Elastix | Telefonía ip | Físico |

## 2.3. Situación actual de la red de datos.

### 2.3.1. Problemática

Seguros Oriente al ser una empresa con un número grande de empleados, presenta ciertos problemas, tanto en software, hardware y redes. Los más frecuentes, los cuales son:

1.- Lentitud en la red

Como se observa el apartado anterior se posee un enlace de datos el cual soporta toda la comunicación tanto de internet como de datos en la empresa.

Durante el día se reciben llamadas alertando sobre lentitud tanto de internet como en los aplicativos de la empresa, los cuales no han sido tabulados, debido a la falta de un proceso para tal motivo.

De acuerdo al protocolo del Departamento de Sistemas, en cada alerta se verifica la lentitud de los enlaces a través del comando ping tanto a los servidores centrales como a www.google.com; una vez confirmado el problema se reporta al proveedor del enlace. El proveedor ha informado en estos eventos que la lentitud se debe a una saturación en los enlaces y que procederá a reiniciar los routers para liberar el canal de comunicación.

2.- Al poseer servidores centralizados los datos de los usuarios son respaldados en un servidor central, el mismo que debe poseer espacio suficiente para guardar la información,  es compartida como una unidad de red a cada usuario desde el servidor central. De igual manera, diariamente se reciben llamadas para notificar que no existe espacio suficiente para guardar la información En el momento que los usuarios reportan el inconveniente, se procede a liberar espacio en el servidor central; el proceso se demora aproximadamente de 20 a 30 minutos, mientras tanto, varios usuarios en la compañía no pueden guardar su información y existen pérdidas de información a todo nivel.

Se ha tomado una estimación de llamadas y correos de los usuarios de 10 llamadas diarias entre lentitud y espacio en los servidores, las mismas que no pueden ser evaluadas estadísticamente ya que no se cuenta con un sistema que permita realizar dicha estimación.

Esto complica mucho el análisis y la solución definitiva de los problemas que se suscitan en el día a día de la empresa

### 2.3.2. Diagnóstico

Los diagnósticos que se pueden dar a la problemática de la empresa no pueden catalogarse de exactos, pues la fidelidad de la estadística es baja a no contar con sistemas de monitoreo en tiempo real

1.- La saturación de la red puede deberse al mal uso que los usuarios dan al internet, entre ellos, páginas de videos y música, redes sociales, descarga de archivos, etc, así como la conexión simultanea de diferentes usuarios al momento de realizar consultas y procesos en la base de datos.

2.- Los servidores de almacenamiento pueden llenar su almacenamiento de manera acelerada por la cantidad de información que cada usuario almacena simultáneamente, siendo este un inconveniente en los servidores que no poseen una alarma en tiempo adecuada para realizar la respectiva liberación de espacio.

Cabe recalcar que todos estos procesos se los realiza manualmente o ante la llamada de los usuarios, sin existir aun una manera de prevenir estos problemas y solucionarlos antes de que sucedan.

## 2.4. Conclusión a la situación actual de la empresa

Tanto los problemas de saturación de red como de almacenamiento se solucionan manualmente por los operadores de sistemas encargados junto con los proveedores de servicios, al solventarlos en cada llamada conlleva un alto tiempo en la solución.

Actualmente la empresa no cuenta con un sistema que les permita anticiparse a los acontecimientos antes mencionados.

Con una herramienta sólida y especializada en la detección de los canales de red y almacenamiento de servidores se puede elaborar un procedimiento oportuno para realizar correctivos necesarios en los servidores y routers, para lo cual la herramienta debe ser capaz de alertar a los operadores del área de TI la saturación o el almacenamiento llegue máximo a un 80% de su capacidad, teniendo con esto un tiempo oportuno de respuesta y evitar los problemas de congestión de la red y de falta de espacio en los servidores, adicionalmente este proceso debe ser transparente para el usuario de tal manera que las quejas por parte de las diferentes áreas se reduzcan y se eleve el nivel del departamento de sistemas frente a la empresa.

# Capítulo 3. Selección del Sistema de Monitoreo

## 3.1. Introducción

Para tener los servicios de red siempre activos es necesario un monitoreo constante de la red de datos, para lo cual requerimos de un sistema automático

el cual nos alerte constantemente sobre saturación de red y componentes defectuosos que alteren los servicios que se ofrecen.

Existen varios sistemas de monitoreo, entre los cuales se encuentran sistemas altamente costosos, los mismos que ofrecen varias opciones y soporte, y, por otra parte, sistemas libres, que funcionan sobre sistemas operativos Windows o Linux, por ser un software libre no se ve atado a un costo por parte del proveedor, operando bajo licencia GPL(GENERAL PUBLIC LICENCE), la mismas que nos ahorra costos, que sea un sistema libre no significa que posee desventajas frente a sistemas pagados, únicamente el soporte se lo realiza por medio de investigación y consultas.

## 3.2. Sistemas de Software Libre

Los sistemas de software libre son aquellos que permiten modificación del código fuente a nuestra conveniencia, el mismo que no debe ser confundido con software gratuito.

### 3.2.1. Generalidades

Un software gratuito en inglés *freeware*, se define como el tipo de programa que se distribuye libremente sin costo por tiempo ilimitado, pero con ciertas restricciones de servicio y funcionalidades. Sin embargo no posee un código fuente para poderlo modificar y no puede ser vendido.

Sin embargo un Software libre “es el software que respeta la libertad de los usuarios y la comunidad. A grandes rasgos, significa que los usuarios tienen la libertad de ejecutar, copiar, distribuir, estudiar, modificar y mejorar el software. Es decir, el «software libre» es una cuestión de libertad, no de precio. Para entender el concepto, piense en «libre» como en «libre expresión», no como en «barra libre». En inglés a veces decimos «libre software», en lugar de «free software», para mostrar que no se quiere decir que es gratuito.” (Free Software Foundation, 2015), adicionalmente un software libre funciona bajo licencias GLP (General Public Licence), dentro del derecho de COPYLEFT (derecho de copia), las cuales se explicarán a continuación.

### 3.2.2. Tipos de Licencias

Las licencias son una parte importante en el desarrollo de software, por medio de ellas se puede diferenciar la distribución que tendrán los sistemas creados. Las licencias son contratos entre los desarrolladores de un software y el usuario final, en el cual se definen derechos y deberes de ambas partes tales como propiedad intelectual y derechos de autor. Es el desarrollador quien elige la licencia según la cual distribuye el software.

Existen varias licencias como son:

#### 3.2.2.1Copyleft

Se denomina copyleft a la licencia de un software libre cuyos términos de distribución no permiten a los redistribuidores restringir de ninguna forma el uso o modificación del sistema haciendo que las nuevas versiones del software se de igual manera libre.

#### 3.2.2.2. GNU GPL

Por sus siglas en inglés (GNU NOT UNIX GENERAL PUBLIC LICENCE) es la licencias más utilizada en software libre, además es la primera creada como copyleft creada por Richard Stallman fundador de la Free Software Foundation(FSF), esta licencia es se encarga de proteger los derechos de los usuarios finales tomando en cuenta los principios fundamentales de software libre (usar, estudiar, compartir y modificar) un sistema libre, esta licencia además garantiza que los trabajos derivados bajo esta licencia seguirán trabajando bajo los mismos principios de libertad antes mencionados.

Los sistemas de software libre cumplen ciertas características esenciales:

- La libertad de ejecutar el programa como se desea, con cualquier propósito, esto nos permite modificar y estudiar el código fuente sin ninguna restricción del proveedor, siendo factible adecuar a las necesidades del usuario en cualquier momento.
- La libertad de redistribuir copias para ayudar a su prójimo con lo cual se forman los llamados foros, en los cuales se comparten actualizaciones y recomendaciones encontradas por las diferentes personas que manipulan el programa para una mejora continua del software.

#### 3.2.2.3. Otras

**Software semi libre:** es aquél que no es libre, pero tiene autorización de uso, copia, distribución y modificación sin fines de lucro.

**Freeware:** es aquella licencia para programas que permiten la redistribución pero no la modificación y su código fuente no está disponible.

**Shareware:** software con autorización de redistribuir copias, pero debe pagarse después de un tiempo para continuar con su uso.

**Software privativo:** aquél cuyo uso, redistribución o modificación están prohibidos o necesitan una autorización.

**Software comercial:** el desarrollado por una empresa que pretende ganar dinero por su uso

## 3.3. Sistemas de Monitoreo de Red

Una herramienta de monitoreo de redes es esencial para asegurar el funcionamiento correcto de los sistemas informáticos y así evitar fallos en la red, también nos ayuda a optimizar la red, ya que nos facilita información detallada sobre el uso de la banda ancha y otros recursos de la red.

### 3.3.1. Generalidades

La administración de una red se basa en poseer un software que permita monitorear tanto la red como los dispositivos periféricos, routers, switchs, servidores, etc. Y que nos alerte constantemente sobre componentes lentos o defectuosos. Estas herramientas de supervisión deben enviar automáticamente alertas o activar copias de seguridad en caso de interrupciones causadas por accidentes o sobrecargas del servidor, conexiones de red u otros factores no controlados.

Estos sistemas utilizan varios métodos de monitoreo, por ejemplo, para supervisar el estado de un servidor web, el software envía peticiones HTTP para buscar una página en el servidor deseado. Para los servidores de correo electrónico, un mensaje de prueba puede ser enviado a través de SMTP y traído por protocolos IMAP o POP3. En el caso de recibir un estado negativo o fallido,

el software de monitoreo envía mensajes de alarma al personal de tecnología para realizar los correctivos necesarios y prevenir futuros inconvenientes.

Un sistema de monitoreo debe poseer ciertos aspectos básicos como son:

- Recopilación de Datos
- Sistema de alertas configurable
- Gráficos en tiempo real
- Monitoreo mediante una Interfaz Web
- Network Discovery
- Sistema de permisos
- Inventario
- Búsqueda de dispositivos
- Reportes avanzados

El sistema de monitoreo debe ser capaz de permitir optimizar la red durante los primeros meses de usos, por medio de la alertas, las mismas que deben ser notificadas incluso antes de que el usuario lo note. Otra característica importante que debe tener el sistema es la capacidad de monitoreo constante del ancho de banda de la red e indicar cuales son los dispositivos que generan una mayor cantidad de tráfico.

### 3.3.2. Arquitecturas de Gestión

La gestión de red es la rama que se ocupa de controlar el funcionamiento y mantenimiento de las redes, para lo cual se utilizan un conjunto de protocolos y técnicas que conjuntamente aplicados garantizan el mantenimiento de los sistemas y el acoplamiento a las necesidades de funcionamiento diario de los organismos que las utilizan. Los sistemas de gestión de red están diseñados para entender a la red como una arquitectura unificada, con direcciones y etiquetas asignadas a cada punto.

De esos puntos se reciben o se extraen, por medio, de protocolos específicos, información que permite tener una imagen casi permanente del funcionamiento general de la red. En los sistemas de gestión de red se deben contemplar ciertos aspectos como son:

- Actividades que permitan a los gestores de red la planificación, organización, supervisión, control y contabilidad para el uso de los servicios de la red.
- Habilidad para ser capaces de escalar el sistema cuando sea necesario.

- Técnicas para poder anticiparse, en la medida de lo posible, a los funcionamientos incorrectos que se puedan presentar en la red.

Los protocolos para la administración de redes especifican modelos para facilitar la gestión, los principales modelos de gestión de redes son los siguientes:

**Modelo OSI**

La Gestión de red a través del Modelo OSI se basa en el uso de protocolos a nivel de aplicación para el intercambio de información de gestión según el paradigma Gestor-Agente.

La Gestión de Modelo OSI consta de cuatro modelos, que son:

- **Modelo de Comunicación.-** consiste en el intercambio de información mediante los protocolos de red CMIP del nivel de aplicación.
  **Protocolo CMIP** (Protocolo de administración de información común), provee el servicio CMIS (Servicio de administración común de información), es un protocolo orientado a conexión el cual fija la comunicación entre las aplicaciones de administración y agentes permitiendo así realizar modificaciones sobre los objetos gestionados.
- **Modelo de Información.-** consiste en abstraer los recursos de la red de datos con el objetivo de gestionarla, de esta manera comienza el uso de platillas para llevar a cabo la gestión de los dispositivos.
- **Modelo Funcional.-** modelo con el cual se describe las cinco áreas en las que se divide la gestión de red:

A.- Gestión de fallos

Consiste en la detección, aislamiento y corrección de errores en el entorno OSI. Los fallos se manifiestan como sucesos particulares en la operación de un sistema.

Funciones: mantener y examinar logs de errores, aceptar notificaciones al detectar errores y reaccionar a las mismas, rastrear e identificar fallos, realizar pruebas de diagnóstico, y eliminar fallos.

B.- Gestión de configuración

Encargada de identifica y ejerce control sobre la captura de datos y los prepara para sistemas abiertos, con el fin de preparar, poner en marcha y tener en cuenta la operación continua y la terminación de servicios de interconexión.

Funciones: Establecer parámetros de control en la operación rutinaria de sistemas abiertos, asociar nombres, inicializar, cerrar, y reunir información sobre la condición actual del sistema abierto en objetos gestionados , así como cambiar la configuración de sistemas abiertos.

C.- Gestión de prestaciones

También llamada de rendimiento tiene como objetivo principal el mantenimiento a nivel de servicio que la red ofreciendo y asegurando a los usuarios operaciones eficientes en todo momento.

Funciones: Recoger datos o variables indicadoras de rendimiento, como troughput de la red, tiempos de respuesta, latencia, etc., Analizar datos para determinar niveles normales de rendimiento. Establecer umbrales, como indicadores que fijan niveles mínimos de rendimiento tolerados, Determinación de un sistema de procesado periódico de los datos de prestación de los distintos equipos, para su estudio continuado.

D.- Gestión de contabilidad

Permite establecer tasas e identificar costos correspondientes a la utilización de los recursos de la red.

Funciones: informar a los usuarios sobre costos y recursos incurridos, permite establecer límites de contabilidad y tarifar la utilización de recursos y permitir la combinación de costos cuando se invoquen múltiples recursos para alcanzar un objetivo de comunicación dado.

E.- Gestión de seguridad.

Tiene por objetivo soportar las políticas de seguridad de las aplicaciones.

Funciones: creación, supresión y control de servicios en mecanismos de seguridad, la distribución de información relativa a la seguridad, y señalización de sucesos relacionados con la seguridad.

- **Modelo de Organización.-** Parte de una estructura de red dividida en dominios de gestión.
  La división del entorno se realiza a partir de dos aspectos principales:
- Políticas funcionales por ejemplo dominios con una misma política de seguridad, contabilidad, etc.
- Otras políticas, como dominios geográficos, tecnológicos, etc.

La red se estructura en dominios administrativos, con la necesidad de establecer y mantener las responsabilidades de cada dominio.
El sistema permite que dentro de un dominio, se pueda reasignar dinámicamente el papel de gestores y agentes.

**b) Modelo TCP/IP**

**Generalidades**

El modelo TCP/IP sirve de interfaz para los operadores humanos e incluye un conjunto de aplicaciones de gestión, se comunica con uno o varios agentes (que son aplicaciones software instaladas en los recursos físicos de la red, tales como routers, hubs, etc) encargados de responder a las peticiones de información o de ejecución de acciones sobre los recursos gestionados provenientes de la estación de gestión.

**MIB**

Una Base de Información de Administración (MIB) es una colección de información que está organizada jerárquicamente. Un objeto administrado (algunas veces llamado objeto MIB, objeto, o MIB) es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Existen dos tipos de objetos administrados: Escalares y tabulares. Los objetos escalares definen una simple instancia de objeto. Los objetos tabulares definen múltiples instancias de objeto relacionadas que están agrupadas conjuntamente en tablas MIB.

Un identificador de objeto (object ID) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones.

## SNMP

### Generalidades

El Protocolo Simple de Administración de Red o SNMP pertenece a la capa de aplicación del modelo OSI que permite intercambiar información entre los dispositivos de la red, permite también, administrar, buscar y resolver problemas en la red así como planear un crecimiento posterior.

### Evolución de la seguridad proporcionada por el protocolo

Cronológicamente hablando, el primer intento serio de dotar al protocolo SNMP de un cierto grado de seguridad se corresponde con la versión denominada SNMPsec, cuyos fundamentos se definen en los RFC 1351 y 1352. Los elementos introducidos en dicha versión para mejorar la seguridad del protocolo forman la base de todas las versiones posteriores y se siguen utilizando en la actualidad.

Las principales innovaciones propuestas en la versión SNMPsec son la identificación unívoca de las entidades que participan en las comunicaciones SNMP, lo que permitirá grandes mejoras y mayor flexibilidad en cuanto al control de acceso, así como la utilización de mecanismos criptográficos para conseguir autentificación, integridad de los mensajes y privacidad.

Dicha versión introduce los siguientes conceptos:

- *Party* SNMP. Es un contexto virtual de ejecución cuyas operaciones se pueden encontrar restringidas a un subconjunto del conjunto total de operaciones permitidas por el protocolo. Un *party* involucra un identificador, una localización en la red utilizando un protocolo de transporte determinado, una vista MIB sobre la que opera, un protocolo de autentificación y un protocolo de privacidad.

- Vista sub-árbol y vista MIB. Una vista sub-árbol es un conjunto de variables de un MIB (*Management Information Base*) que tienen como prefijo un identificador de objeto común. Una vista MIB no es más que un conjunto de vistas sub-árbol.

- Política de control de acceso. Es el conjunto de clases de comunicación autorizadas entre dos *parties* SNMP o lo que es lo mismo el conjunto de mensajes del protocolo SNMP cuyo uso se permite entre dos elementos participantes en una comunicación de gestión.

- Protocolo de autentificación. Sirve al mismo tiempo para autentificar los mensajes y para poder comprobar su integridad. Se suele utilizar un mecanismo de firmas digitales, como por ejemplo el algoritmo MD5 que calcula un *digest* del mensaje. El valor obtenido se incluye entre los datos transmitidos a la hora de llevar a cabo una comunicación.

- Protocolo de privacidad. Sirve para proteger las comunicaciones contra escuchas malintencionadas. Se utiliza, por ejemplo, el algoritmo simétrico de encriptación DES (*Data Encryption Standard*).

La versión SNMPsec se adopta inicialmente con la introducción de la versión 2 del protocolo SNMP y pasa a denominarse SNMPv2p (*Party-based* SNMPv2).

Posteriormente el marco de trabajo SNMPv2, cuya definición no contiene ningún estándar en cuanto a seguridad, se asocia con otros modelos administrativos referentes a seguridad, y aparecen tres nuevas versiones del protocolo: SNMPv2c, SNMPv2u y SNMPv2.

La versión SNMPv2c (*Community-based SNMPv2*) utiliza el mismo modelo administrativo que la primera versión del protocolo SNMP, y como tal no incluye mecanismos de seguridad. Las únicas mejoras introducidas en la nueva versión consisten en una mayor flexibilidad de los mecanismos de control de acceso, ya que se permite la definición de políticas de acceso consistentes en asociar un

nombre de comunidad con un perfil de comunidad formado por una vista MIB y unos derechos de acceso a dicha vista (*read-only* o *read-write*).

La versión SNMPv2 proporciona niveles de seguridad adecuados, pero no alcanzó el necesario nivel de estandarización y aceptación por el IETF (*Internet Engineering Task Force*).

Por último, la versión denominada SNMPv2u (*User-based SNMPv2*) reutiliza los conceptos introducidos en la versión SNMPsec, introduciendo la noción de usuario. En este caso, las comunicaciones se llevan a cabo bajo la identidad de usuarios en lugar de utilizar el concepto de *party*existente en las versiones precedentes. Un mismo usuario puede estar definido en varias entidades SNMP diferentes.

**La seguridad en la versión 3 del protocolo**

La principal novedad introducida en la versión 3 del protocolo SNMP es la modularidad. En dicha versión una entidad SNMP se considera compuesta por un motor y unas aplicaciones. A su vez el motor se divide en cuatro módulos: *dispatcher*, subsistema de proceso de mensajes, subsistema de seguridad y subsistema de control de acceso.

Se observa, por tanto, que en la versión SNMPv3 se independizan los mecanismos utilizados para la seguridad (autentificación y privacidad) y para el control de acceso. De este modo, una misma entidad puede utilizar diferentes modelos de seguridad y control de acceso simultáneamente, lo que incrementa notablemente la flexibilidad y la interoperabilidad.

Se define un modelo estándar para seguridad basada en usuarios, USM (*User Security Model*) y otro para control de acceso basado en vistas, VACM (*View-based Access Control Model*). Se aprovechan los conceptos definidos en las versiones previas y al mismo tiempo la modularidad del protocolo permite la introducción de futuros modelos independientes de los actuales (J.C. Fernández J.A. Corrales y A. Otero, 2007).

**RMON (Remote Monitor)**

Protocolo utilizado para monitoreo remoto de redes, forma parte del protocolo TCP/IP, este protocolo posee ciertos sensores, los cuales son:

- Alarmas: Sirve para informar sobre cambios de características de la red, permitiendo a los usuarios configurar alarmas sobre objetos dentro de la red.
- Estadísticas: Recolecta estadísticas de la red.
- Filtros: Encargado de recolectar información filtrada de la red por medio de conectores como AND, OR y NOT.
- Computadores: Tabla basada en direcciones MAC, con información de transmisión y recepción del computador.
- Principales: Contiene información de los computadores principales previamente definidos por el usuario.
- Matriz de tráfico: Información de errores organizada en una matriz para relacionar los nodos más activos.
- Captura de paquetes: Encargado de recolectar paquetes previamente filtrados.
- Sucesos: Registro de sucesos basados en rangos definidos por el administrador de red, los cuales son, ascendente, descendente y acoplamiento de red.

**Importancia de Monitorizar una Red de Datos**

Las redes empresariales se vuelven cada vez más complejas, por lo tanto la operación de las mismas se vuelve más exigente. El tráfico de voz y datos requieren mayor demanda de recursos, requiriendo mejor estabilidad de la red, por lo cual el análisis y monitoreo de redes se ha convertido en actividades de gran importancia en todas las compañías.

El proceso para monitorizar debe ser continuo, ordenado y exacto, de esta manera en caso de problemas se toman medidas tanto preventivas como correctivas para estabilizar la red, de esta manera se mantiene un control efectivo para mejorar el desempeño de la red. Con los datos obtenidos se

realizan estadísticas para recopilar datos de problemas e irregularidades, ésta información es guardad en bitácoras, siendo utilizadas para mostrar el comportamiento de la red.

Al no poseer una adecuada herramienta de monitoreo del estado de la red y sus elementos, conlleva un costo elevado, ya que el costo de reparación y mantenimiento será mayor, por otra parte será necesario contratar más personal para el soporte de la misma. La prevención mediante respuestas anticipadas a problemas cotidianos son mecanismos de control exitosos en una red (CLAVIJO & SALAZAR, 2010, pág. 29).

## 3.4. Herramientas de Monitoreo de Red

Una herramienta de monitoreo de redes es fundamental para asegurar el funcionamiento de los sistemas informáticos y para evitar fallos en la red. Como también nos ayuda a optimizar la red, ya que nos facilita información detallada sobre el uso de la banda ancha y otros recursos de la red.

### 3.4.1. Herramientas Pagadas (No GNU)

Las herramientas de red pagadas ofrecen buenas soluciones pero a un muy alto costo el cual tiene que ser renovado mensual o anualmente, de igual manera el soporte técnico se encuentra ligado a la licencia que se compre, esto conlleva un gasto para la empresa y atados a un proveedor externo al cual se lo debe contactar para cualquier requerimiento, siendo problemático cuando se trata de fidelidad de información.

A continuación se presentan unas soluciones de monitoreo de redes licenciadas:

WHATSUP GOLD

Es una solución de gestión de redes diseñada para redes de pequeñas y medianas empresas y garantizar un crecimiento estable en el futuro.

PRTG

Es una solución avanzada de monitoreo para toda su red. Fácil de usar con una interfaz basada en Web que permite a los usuarios rápidamente auto-descubrir y configurar los dispositivos de red y los sensores que desea supervisar.

ORIONNETWORK PERFOMANCE MONITOR

Herramienta de monitoreo de red que permite acelera la detección y resolución de problemas, resuelve los problemas de desempeño de red y reduce el tiempo de inactividad, monitorea y muestra el tiempo de respuesta, la disponibilidad y el rendimiento de los dispositivos de red.

### 3.4.2. Herramientas Libre (GNU)

Por otro lado las herramientas de montero basadas en software libre proveen una serie de herramientas gratuitas y editables con las cuales se puede enriquecer nuestro sistema con diferentes aplicativos acordes a nuestro nivel de negocio sin que se vean afectados los recursos económicos de la empresa.

ZABBIX

Es un sistema que permite monitorear la capacidad, el rendimiento y la disponibilidad de los servidores, equipos, aplicaciones y bases de datos. Además ofrece características avanzadas de monitoreo, alertas y visualización, que incluso, algunas de las mejores aplicaciones comerciales de este tipo no ofrecen, Dentro de las características principales de Zabbix se puede agregar y monitorear servidores, equipos, servicios, aplicaciones específicas, dispositivos físicos como impresoras, routers, entre otros, generar reportes en tiempo real a través de gráficas, datos y alertas visuales que muestran el estado y rendimiento de los servicios y equipos monitoreados, posee adicionalmente un módulo de inventario de equipos para mantener al día la infraestructura tecnológica, mapas de la red de la empresa, configuración de notificaciones vía correo electrónico y sms, perfiles de usuarios para el uso del administrador Web, entre otras.

NAGIOS

Sistema de monitorización de redes de código abierto, que vigila los equipos y servicios que específicos, alertando cuando el comportamiento de los mismos sea inadecuado. Entre sus características principales se tiene la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

CACTI

Esta herramienta, desarrollada en PHP, provee un pooler ágil, plantillas de gráficos avanzadas, múltiples métodos para la recopilación de datos, y manejo de usuarios. Tiene una interfaz de usuario fácil de usar, así como también para redes complejas con cientos de dispositivos.

## 3.5. Análisis de los sistemas de monitoreo

Como vimos anteriormente existen diferentes sistemas de monitoreo, los cuales poseen variadas características, para lo cual se ha elaborado un cuadro con los aspectos más importantes que debe poseer un sistemas y así derivar en uno que satisfaga las necesidades de las empresas sin incurrir en costos demasiado elevados.

*Tabla 7, Cuadro Comparativo entre diferentes sistemas de monitoreo*

| NOMBRE | GRÁFICAS | INFORMES SLA | GRUPOS LÓGICOS | ESTADÍSTICAS | PREDICCIÓN DE ESTADÍSTICAS | AUTODESCUBRIMIENTO | AGENTES | SNMP | SYSLOG | SCRIPTS EXTERNOS | COMPLEMENTOS (PLUGINS) | CREACIÓN DE COMPLEMENTOS | ALERTAS (E-MAIL/JSMS) | APLICACIÓN WEB | MONITORIZACIÓN DISTRIBUIDA | MÉTODO DE ALMACENA | LICENCIA | MAPAS | SEGURIDAD | EVENTOS |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Zabbix | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si | Si | Fácil | Si | Control total | Si | SQL | GPL | Si | Si | Si |
| Nagios | Si | Si | Si | Si | Si | Si | Si | A través de plugin | Si | Si | Si | Media | Si | Sólo visualización | Si | SQL | GPL | Desconocido | Desconocido | Desconocido |
| Cacti | Si | Si | Si | Si | No | A través de plugin | Si | Si | Si | Si | Si | Media | Si | Control total | No | RRDtool y MySQL | GPL | A través de plugin (Weathermap) | Roles personalizados | No se tiene plugin |
| Ptrg | Si | Si | Si | Si | Si | Si | Snmp y Wmi | Si | Desconocido | No | Si | No | Si | Control total | Desconocido | Propietario | Freeware and Commercial | Si | Si | Si |
| Whatsup | Si | Desconocido | Si | Si | Si | Si | Si | Si | Si | No | Si | No | Si | Control total | Desconocido | Propietario | Freeware and Commercial | Si | Si | Si |
| Orion | Si | Si | Si | Si | Si | Si | Parcial | Si | Si | No | Si | No | Si | Control total | Desconocido | SQL | comercial | Si | Si | Si |

## 3.6. Justificación para la selección de la herramienta

Se observa en la tabla que el sistema de monitoreo de redes “ZABBIX” cumple con los requerimientos necesarios para un programa de esta categoría que otros no. Adicionalmente se aprecia que este al ser un programa con licencia de software libre no tiene un costo lo que representa una gran ventaja para el usuario interesado, cuenta con un diseño amigable, fácil y versátil que se acomoda fácilmente a las necesidades del usuario en general. Entre otras características o ventajas que se poden mencionar se tiene el hecho que SABBIX cuenta con una interfaz gráfica fácil y sencilla, una bitácora syslog que mantiene un registro constante de los sistemas y equipos monitoreados, cuenta además con una característica que dará al usuario la facilidad de crear scripts para general complementos externos y un método de almacenaje de datos SQL adaptable a cualquier plataforma gratuita de base de datos como mysql, postgres y mariadb

# Capítulo 4. Zabbix

## 4.1. Generalidades Zabbix

Zabbix es un sistema diseñado para monitorear la capacidad, el rendimiento y la disponibilidad de los servidores, equipos, aplicaciones y bases de datos, junto con características avanzadas de alertas y visualización, las cuales serán de gran ayuda para mantener los servicios siempre activos.

Zabbix fue creado por Alexei Vladishev y actualmente es propiedad de la compañía Zabbix SIA., la cual se encarga de actualizarlo. Es una herramienta de monitoreo de redes y dispositivos open source compatible con Unix y distribuciones Linux y posee una extensa lista de características que lo convierten en una excelente solución que sirve para prevenir saturaciones de red y problemas con servidores, convirtiéndose en una poderosa herramienta de soporte. Esta herramienta brinda una serie de facilidades para realizar diagnóstico, prevención y control de los diferentes equipos de la red, mejorando los tiempos de respuesta y garantizando mayor efectividad.

## 4.2. Características Destacadas de Zabbix

La herramienta de monitoreo Zabbix permite fácilmente controlar servidores, dispositivos de red y aplicaciones, junto con reportes estadísticos de datos de rendimiento. Dentro de las características más destacadas de Zabbix se tiene:

*Tabla 8, Características destacadas Zabbix*

| CARACTERÍSTICAS | DESCRIPCIÓN |
|---|---|
| Rendimiento | Indicadores de memoria, procesador, red, espacio en disco y procesos. |
| Supervisión sin Agente | Uso de agentes como SNMP (Protocolo simple de manejo de red) e IPMI (Plataforma inteligente de monitoreo de interfaces). |
| Dispositivos de Red | Monitoreo de la capacidad de red, estado de puertos y sistemas de energía. |

| | |
|---|---|
| Personalizar | Uso de scripts en diferentes lenguajes: Shell ,Perl, etc. |
| Built-in Java Application Server Control | Supervisión de servidores de aplicaciones Java sobre JMX directamente sin necesidad de módulos de terceros o capas de integración. |
| Monitoreo de hardware | Estadísticas de temperatura, voltaje del ventilador, y estado del disco. |

## 4.3. Ventajas de ZABBIX

Algunas son las ventajas de Zabbix, entre otras tiene la capacidad de encontrar los diferentes dispositivos de la red como servidores, impresoras y periféricos a través de diferentes protocolos como son SNMP o IMPI, además, posee un sistema de administración centralizado desde un monitor web donde se encuentran en una misma interfaz todos los dispositivos de la red.

El sistema es compatible para diferentes plataformas como son Linux, Solaris, HP-UX, AIX, Free BSD, Open BSD, OS X, Tru64/OSF1, Windows, permitiendo mantener un monitoreo constante de la red.

Para mantener la seguridad y diferentes perfiles de administración Zabbix posee un sistema de manejo de usuarios junto con una autenticación por medio de contraseñas y usuarios, cada usuario posee su perfil con accesos propios de ese usuario.

Permite diferentes formas de alertas, de las cuales las más utilizadas son a través de correo electrónico, el cual se envía automáticamente cuando los servidores cumplen un porcentaje establecido de capacidad o la red se satura a cierto nivel, el correo es enviado a la dirección de correo del operador de redes indicando el porcentaje restante de capacidad de la red o el espacio.

## 4.4. Importancia de ZABBIX

Como se mencionó anteriormente Zabbix es una herramienta de código abierto, la cual nos permite modificar el código en caso de requerirlo, así como también minimizar costos de licencias ni estar atados a un proveedor con pagos

mensuales o anuales, siendo fácil de instalar, Zabbix no requiere de una especialización para su puesta en producción, con un conocimiento básico de manejo Linux se instalará sin ningún inconveniente, de igual manera con su interfaz web fresca y amigable la configuración de Zabbix se la puede realizar a cualquier nivel, siendo administrable desde que cada dispositivo es configurado, Zabbix siempre pensando en una facilidad para los usuarios centraliza toda la información en su propia base de datos (basada también en software libre) para realizar cualquier consulta desde un solo servidor por el cual la conexión se la realiza via web desde cualquier dispositivo de la red, de esta forma se mantiene siempre monitoreado cada dispositivo agregado a su plataforma.

**PLATAFORMAS SOPORTADAS**

- Linux
- BM AIX
- FreeBSD
- NetBSD
- OpenBSD
- HP-UX
- Mac OS X
- Solaris
- Windows: 2000, Server 2003, XP, Vista, Server 2008, 7, 8, Server 2012 (Solo en los agentes)

**BASES DE DATOS SOPORTADAS**

- MySQL (5.03 en adelante)
- PostgreSQL (8.1 en adelante)
- Oracle (10g en adelante)
- SQLite (3.3.5 en adelante)

**INTERFACES WEB SOPORTADAS**

- Apache (1.3.12 en adelante)
- PHP (5.3 en adelante)

(QuasarSofrware, s.f.)

## 4.5. Elementos de Zabbix

Zabbix posee elementos los cuales permiten un correcto manejo del sistema de monitoreo de la red.

*Tabla 9, Elementos Zabbix*

| ELEMENTOS | DESCRIPCION |
|---|---|
| Agente Zabbix | Componente propio de Zabbix basado en el protocolo abierto snmp permite monitorear de manera más sencilla y en tiempo real los recursos de la red, con la ayuda de este componente instalado en los dispositivos Windows o Linux la recolección de información resulta sencilla de obtener. |
| Key | Son etiquetas utilizadas para organizar de manera eficiente el tipo de información que se va a analizar, por ejemplo el key de disco, analizara la información del disco duro de la unidad |
| Triggers | Son módulos creados por el administrador de red para evaluar cada dato recopilado de acuerdo a un ítem y a un key por ejemplo, si se crea un trigger del ítem disco que analice el key disco cuando llegue a un 80% este trigger enviara una alerta cada vez que suceda este evento |
| Items | Módulos Zabbix que recogen información de los hosts |
| Host | Equipos registrados en la consola de administración, los cuales se convierten en dispositivos a ser monitoreados |
| Servidor recolector Zabbix | Servidor principal donde se encuentra instalada la consola de administración y la |

| | |
|---|---|
| | base de datos central de Zabbix el cual sirve para recopilar la información de los dispositivos configurados ya sea con el agente propio Zabbix o con los agentes configurados por medio de snmp.<br><br>Se podrá ingresar a la consola de administración de cualquier lugar a través de la interfaz web Zabbix |

## 4.6. Funcionamiento el monitoreo

Una vez instalado el agente Zabbix en los servidores y hosts a monitorear comienza la recolección de datos, esto se lo realiza a través del protocolo snmp como se indica a continuación:

- Los dispositivos de la red previamente configurados para reportar al servidor recolector Zabbix informan al servidor recolector sobre su estado actual.
- El servidor recolector Zabbix almacena la información enviada por los dispositivos de la red.
- Los ítems recogen la información de los hosts y por medio de los keys analizan la información recolectada de cada elemento de los hosts.
- Los trigger analizan los eventos programados y realizan las acciones configuradas.
- Zabbix captura los eventos (triggers) y dependiendo de su naturaleza puede enviar alertas por correo electrónico o SMS.

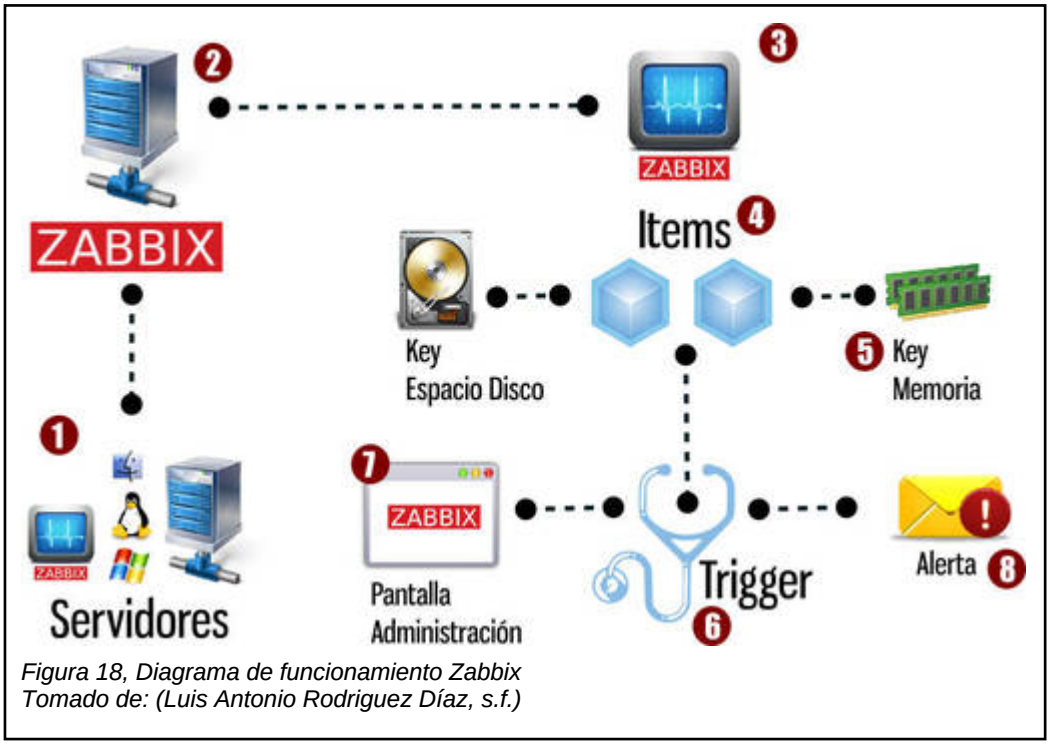



*Figura 18, Diagrama de funcionamiento Zabbix*
*Tomado de: (Luis Antonio Rodriguez Díaz, s.f.)*

## 4.7. Requisitos previos de instalación

Existen ciertos requisitos tanto de hardware como de software que se requieren para instalar correctamente Zabbix

*Tabla 10, Requisitos de Instalación Zabbix*

| **HARDWARE** | |
|---|---|
| PROCESADOR | 2 núcleos para pequeñas empresas |
| DISCO DURO | HDD 500 GB |
| MEMORIA | 4 GB mínimo |
| **SOFTWARE** | |
| SISTEMA OPERATIVO | Sistema Operativo Linux (Centos, RedHat, Fedora, Ubuntu, Suse,etc) |
| BASE DE DATOS | MySql 5.0 o superior |
| | Oracle 10g o superior |
| | PostgreSQL 8.1 o superior |
| | SqlLite 3.3 o superior |
| ENTORNO WEB | Apache 1.3 o superior |
| | PHP 5.1 o superior |

## 4.8. Instalación

Zabbix puede ser instalado en cualquier entorno Linux, sea este físico o virtual, para este ejemplo se ha utilizado la distribución Centos 6, los comandos establecidos son enfocados específicamente para esta distribución.

**Configurar reportorio YUM**

Antes de instalar Zabbix se debe configurar el repositorio rpm de Zabbix siguiendo los siguientes comandos

**CentOS/RHEL 7:**

#rpm -Uvh http://repo.Zabbix.com/Zabbix/2.2/rhel/7/x86_64/Zabbix-release-2.2-1.el7.noarch.rpm

**CentOS/RHEL 6:**

#rpm -Uvh http://repo.Zabbix.com/Zabbix/2.2/rhel/6/x86_64/Zabbix-release-2.2-1.el6.noarch.rpm

**CentOS/RHEL 5:**

# rpm -Uvh http://repo.Zabbix.com/Zabbix/2.2/rhel/5/x86_64/Zabbix-release-2.2-1.el5.noarch.rpm

**Instalar Zabbix con MySql**

Se instalarán los paquetes necesarios para la integración con mysql.

**# yum install Zabbix-server-mysql Zabbix-web-mysql Zabbix-agent Zabbix-java-gateway**

**Configuración apache**

Zabbix crea automáticamente su archivo de configuración apache **/etc/httpd/conf.d/Zabbix.conf,** pero se debe editar la zona horaria a la que se pertenece

**php_value date.timezone America/Guayaquil**

Reiniciar el servicio apache.

# service httpd restart

**Crear base de datos mysql**

Este paso crea la base de datos propia de Zabbix.

# mysql -u root -p

mysql> CREATE DATABASE Zabbix CHARACTER SET UTF8,

mysql> GRANT ALL PRIVILEGES on Zabbix.* to 'Zabbix'@'localhost' IDENTIFIED BY 'SECRET_PASSWORD',

mysql> FLUSH PRIVILEGES,

mysql> quit

Luego de crear la base de datos se debe restaurar a la instalada por Zabbix

# mysql -u Zabbix -p Zabbix < /usr/share/doc/Zabbix-server-mysql-2.2.8/create/schema.sql

# mysql -u Zabbix -p Zabbix < /usr/share/doc/Zabbix-server-mysql-2.2.8/create/images.sql

# mysql -u Zabbix -p Zabbix < /usr/share/doc/Zabbix-server-mysql-2.2.8/create/data.sql

**Iniciar servidor Zabbix**

Iniciar Zabbix con el siguiente comando

# service Zabbix-server start

Una vez iniciado se puede proceder con la instalación via web de Zabbix

**Iniciar Zabbix via web**

Para iniciar la instalación web, se debe colocar la ruta siguiente desde el buscador, cambiando el nombre del servidor.http://servidorZabbix/Zabbix/

### Página de bienvenida

Esta es la página de bienvenida de Zabbix, en la cual se muestra un resumen de los pasos a realizarse durante la instalación,  presionar next para continuar


*Figura 19, Página de Inicio Zabbix*

### Check de pre-requisitos

Se revisan si los requisitos previos como son los servicios apache, mysql, php se encuentran instalados correctamente, de ser así presionar next**.**

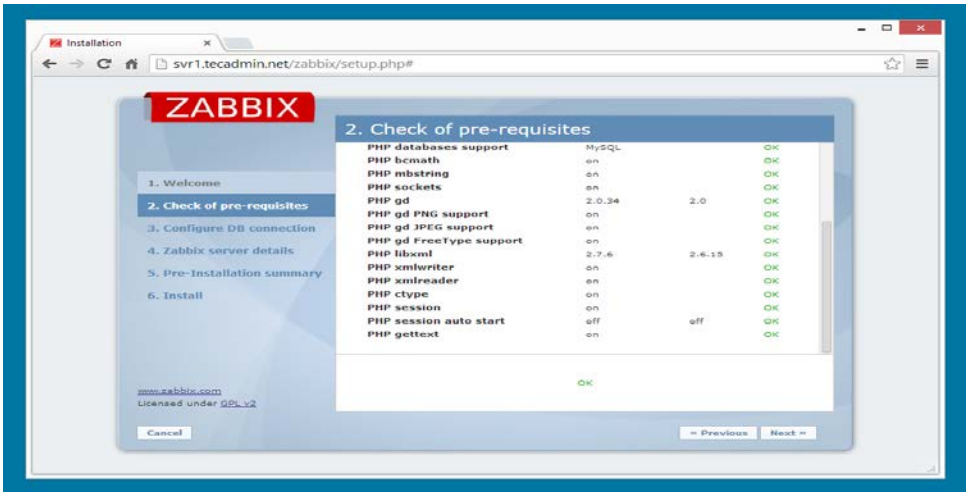



Figura 20, Lista de Requisitos Previos

### Configurar conexión DB

Ingresar los datos de la base creada anteriormente y probar dando click en **Test Connection**, si la base de datos es correcta, presentará un mensaje de OK y se puede continuar presionando en next

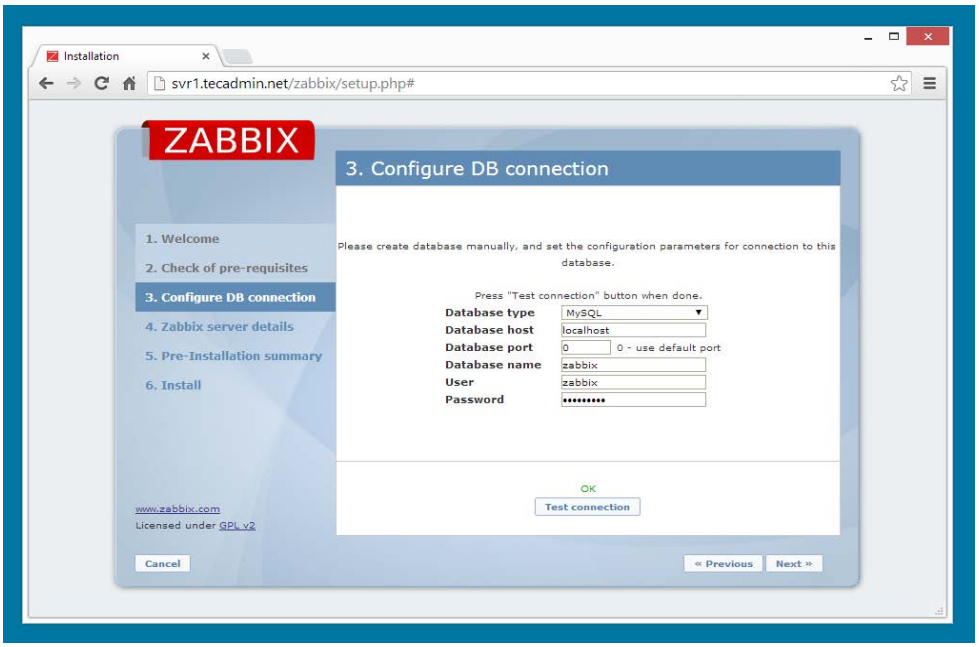



Figura 21: Configuración Base de Datos

### Detalles del servidor Zabbix

En la siguiente pantalla se debe colocar los detalles de la red como son host, puerto y nombre de dominio, los cuales serán utilizados para la conexión con los dispositivos

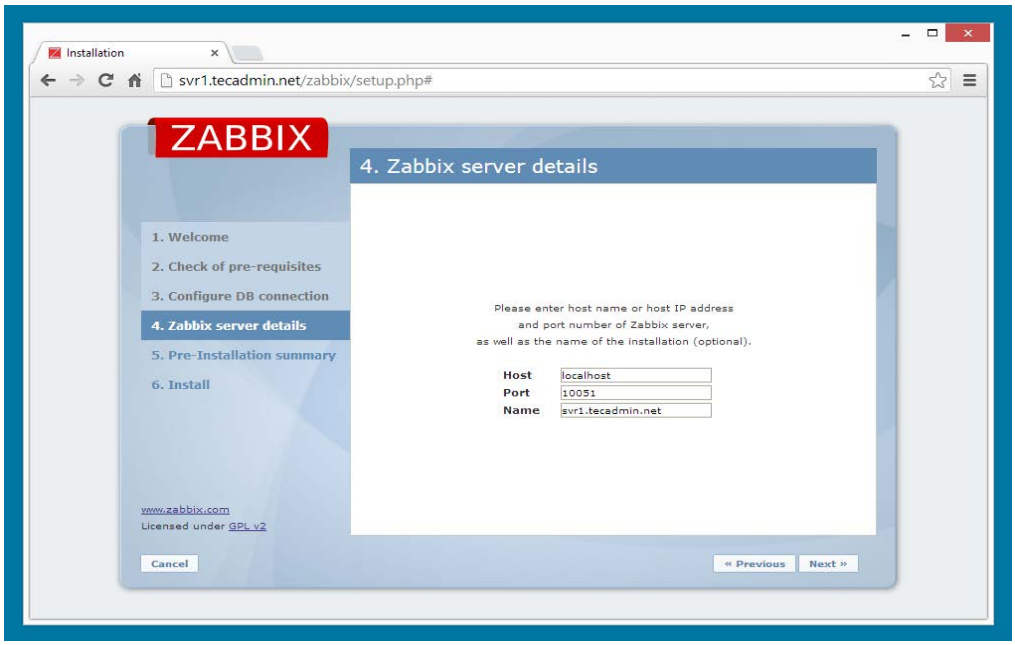



Figura 22, Detalles del Servidor Zabbix

**Resumen de preinstalación**

Esta pantalla da un resumen de la instalación que se va a realizar.

Presionar next

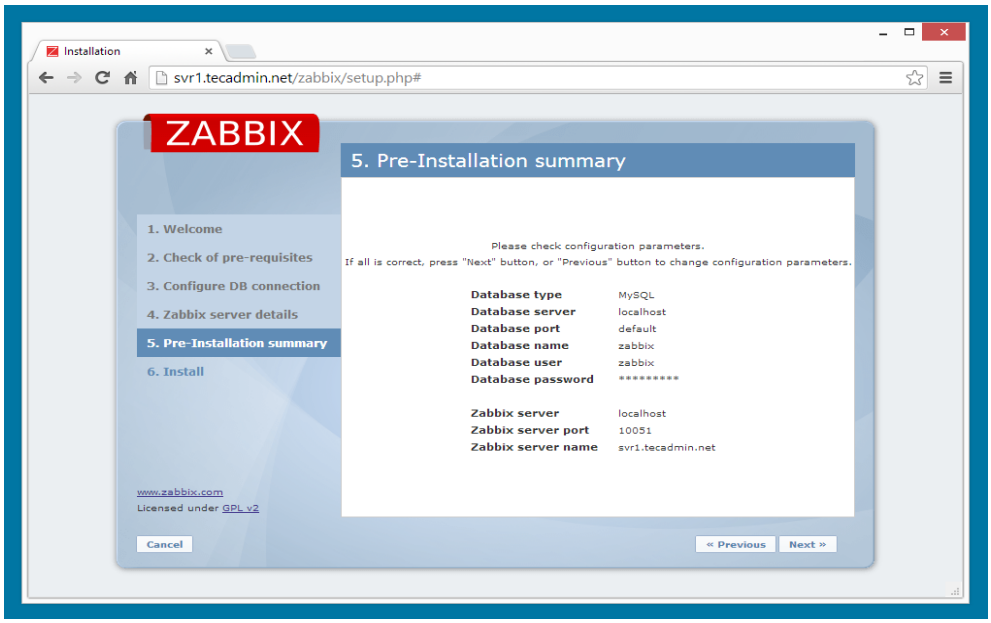



Figura 23, Resumen de Requisitos

## Instalación Zabbix

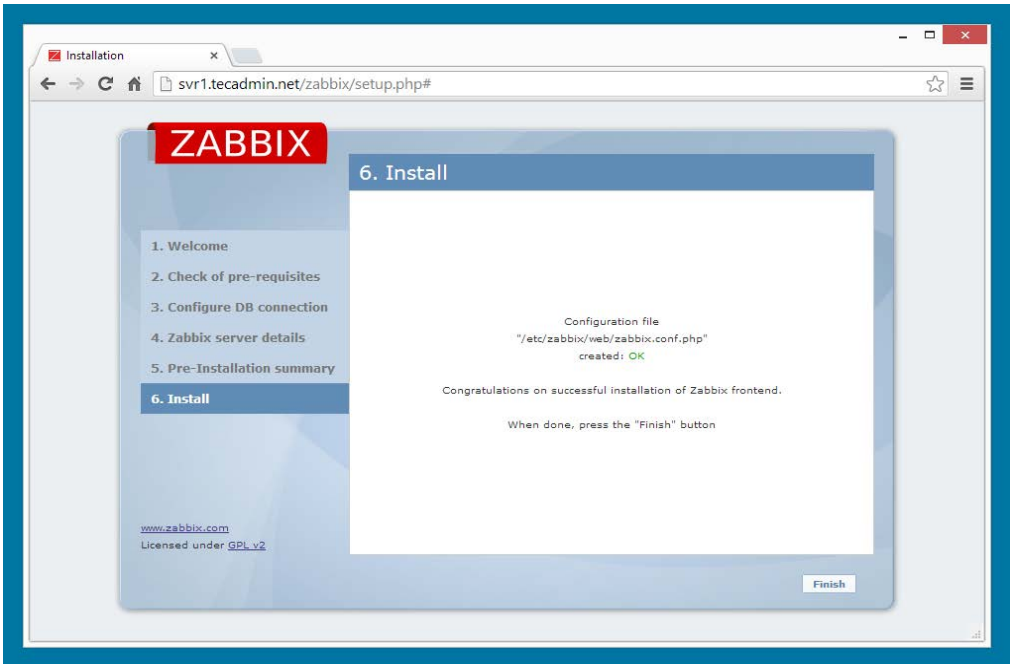



Figura 24, Pantalla de Instalación completada

**Zabbix pantalla de login**

Una vez completada la instalación se debe ingresar con las credenciales por defecto.

**Username: admin**

**Password: Zabbix**

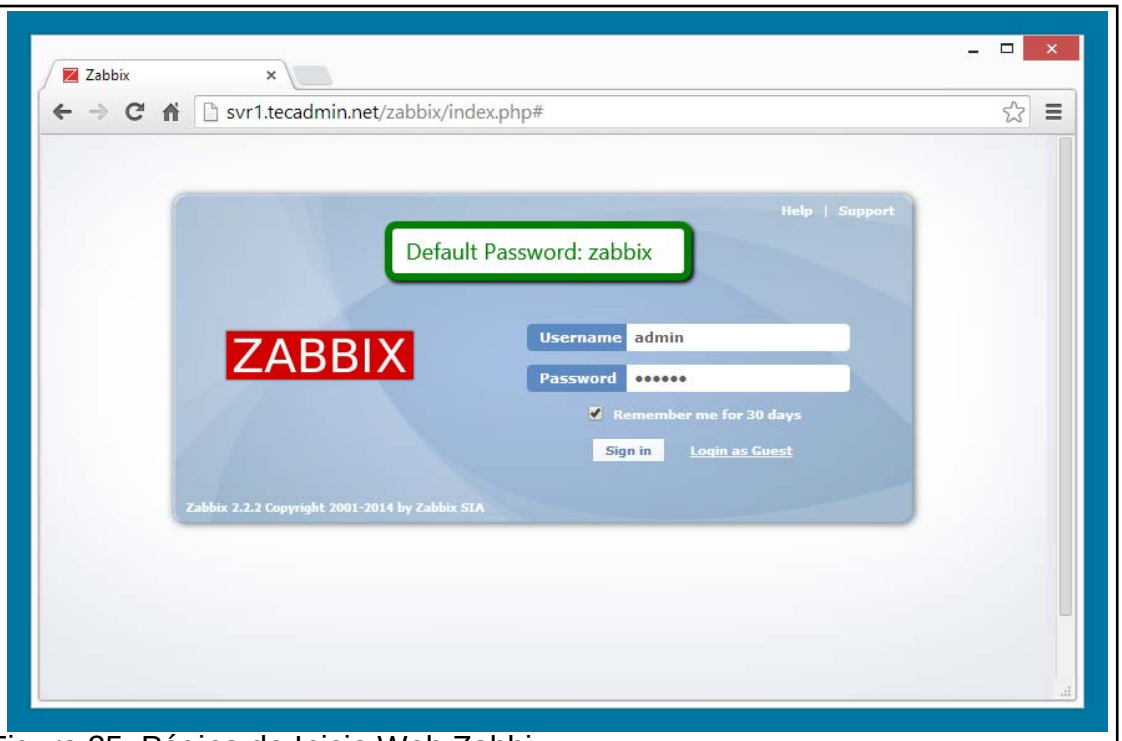



Figura 25, Página de Inicio Web Zabbix

## 4.9 Análisis de riesgos

**Problemas posibles al instalar**

1.- Al momento de crear la contraseña mysql presenta el siguiente error:

```
[root@localhost zabbix-1.8.8]# mysqladmin -u root password sesamo
mysqladmin: connect to server at 'localhost' failed
error: 'Access denied for user 'root'@'localhost' (using password: NO)'
```

Diagnóstico: El servicio mysql no se encuentra levantado, lo cual provoca que no exista conexión a la base de datos.

Solución: ejecutar el comando service mysqld start

2.- Se presentan errores en la instalación de paquetes Zabbix

Diagnóstico:

Errores al momento de instalar los paquetes se producen porque no se ha realizado una actualización del sistema y existen componentes i librerías que presentes en la actualización

Solución:

Ejecutar el comando: yum update -y

3.- Al momento de iniciar Zabbix web presenta un error de página no encontrada

Diagnóstico:

Este error se produce ya que no se han otorgado los permisos necesarios en iptables al puerto 80

Solución:

Ejecutar el siguiente comando:

iptables -A INPUT -p tcp -m tcp --sport 80 -j ACCEPT

iptables -A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT

4.- Reinicio de servicios Linux

Diagnóstico:

Cuando se reinicia servicios Linux como iptables, mysqld o httpd y el servidor es compartido todos los servicios ofrecidos a los clientes que ocupen este tipo de ser servicios Linux se detendrá durante el reinicio

Solución:

Realizar la instalación fuera de horarios laboral si se lo realiza en un servidor compartido, siendo en un servidor propio para Zabbix no hay problema en el reinicio.

**Problemas posibles al ejecutar y operar**

1. Ciertos dispositivos no aparecen en la consola Zabbix

Diagnóstico:

El servicio snmp no se encuentra bien configurado

Solución:

Revisar que los segmentos de red y puertos se encuentren bien configurados en la consola.

## 4.10. Cronogramas de instalación

**Pasos previos**

- Para instalar Zabbix se debe verificar previamente que los elementos hardware se encuentren correctos.
- Verificar que el SO Linux se encuentre actualizado (yum update -y)
- Verificar que los servicios de base de datos (mysql, postgres, etc) y aplicativos web se encuentren instalados (apache, php)

## 4.11. Cronograma

A partir del momento de la instalación se presenta el siguiente cronograma

*Tabla 11, Cronograma de Instalación*

| DESCRIPCIÓN | SEMANA 1 | | | | | SEMANA 2 | | | | | SEMANA 3 | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Dia 1 | Dia 2 | Dia 3 | Dia 4 | Dia 5 | Dia 6 | Dia 7 | Dia 8 | Dia 9 | Dia 10 | Dia 11 | Dia 12 | Dia 13 | Dia 14 |
| Preparación Servidores | X | X | | | | | | | | | | | | |
| Instalación Zabbix | | | X | | | | | | | | | | | |
| Configuración | | | X | X | X | | | | | | | | | |
| Pruebas iniciales | | | | | X | X | X | X | X | | | | | |
| Pruebas en produccion | | | | | | | | | X | X | | | | |
| Estadisticas | | | | | | | | | | X | X | X | X | X |

# Capítulo 5. Administración

## 5.1. Instalación Agentes Zabbix:

Una vez instalado el servidor Zabbix es necesario instalar el agente en los servidores que se requiera monitorear.

Para instalar los agentes Zabbix en un servidor Windows, siendo el caso actual con el que se realizan la pruebas en el servidor de almacenamiento de información (SERVERAD).

Para instalar y configurar el agente se seguirán los siguientes pasos:

1. Descargar el paquete agente de la siguiente dirección: http://www.Zabbix.com/download.php, de acuerdo al sistema requerido, en este caso se elige la opción Windows

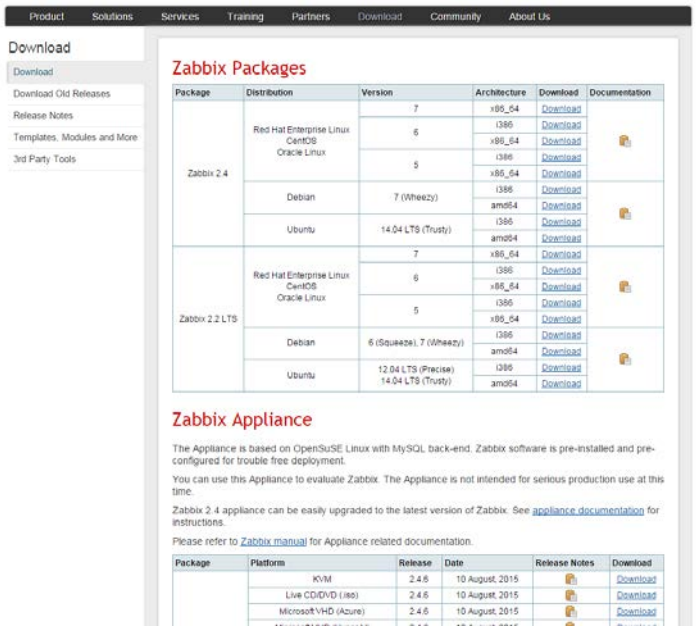



Figura 26, Descarga de paquetes Zabbix para agentes

2. Una vez descargado el paquete se lo abre en el servidor cliente que se va a monitorear con el cual se iniciará el agente de instalación Zabbix


*Figura 27, Pantalla de inicio de instalación agente Zabbix*

3. Aceptar la licencia GNU – GPL presionando la pestaña de “I accept the terms in the licence agreement”.


*Figura 28,* Aceptación *de Condiciones Generales*

4. Llenar los campos con la información requerida, luego de los cual presionar en el botón next

Zabbix Server Name: Nombre o IP del servidor Zabbix
Zabbix Server Port: Puerto destinado para la conexión con Zabbix (default)
Agent Port: Puerto del agente Zabbix (default)
Remote Command: Habilitarlo para permitir a Zabbix controlarlo remotamente desde la interfaz web

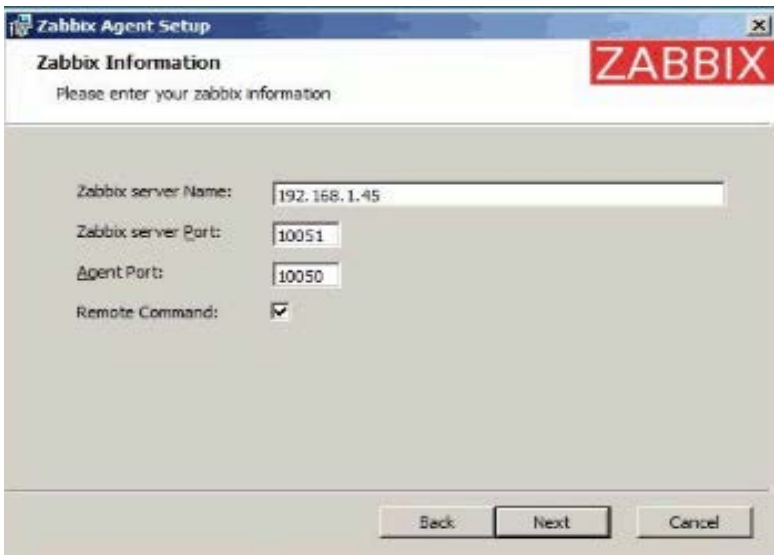



*Figura 29, Cronograma de Instalación*

5. Elegir los complementos a instalar y presionar en el botón next


*Figura 30, Pantalla de* complementos *Zabbix*

6. Presionar install para instalar el agente


Figura 31, Pantalla de confirmación para la instalación

Una vez que se ha agregado los agentes a los servidores, se controlará su funcionamiento desde el front-end web de Zabbix, para lo cual se de activar la monitorización en el servidor.

**Usuarios Zabbix**

1.- Ingresar a la opción Administrator → Users → Users

Donde se muestran los siguientes usuarios

Admin: Super-usuario Zabbix, el cual posee todos los permisos.

Guest: Usuario para invitados el cual no tiene permisos de operación.

| Alias | Name | Surname | User type | Groups | Is online? | Login | Frontend access | Debug mode | Status |
|---|---|---|---|---|---|---|---|---|---|
| Admin | Zabbix | Administrator | Zabbix Super Admin | Zabbix administrators | Yes (Wed, 04 Jan 2012 15:39:51 +0200) | Ok | System default | Disabled | Enabled |
| guest | Default | User | Zabbix User | Guests | Yes (Wed, 04 Jan 2012 15:33:42 +0200) | Ok | System default | Disabled | Enabled |

Figura 32, Pantalla de usuarios Zabbix

2.- Dar clic en Admin y cambiar la contraseña.

Como vimos en el capítulo anterior Zabbix se compone ciertos elementos como son host, trigger, agent, ítems, etc., los cuales deben ser configurados para monitorear los dispositivos.

**Registro de dispositivos (HOST)**

Un host es un dispositivo registrado que se convierte en un elemento a ser monitoreado

Para agregar un Host se debe seguir lo siguientes pasos:

1.- Ir a la opción

Configuration → Hosts.

En la cual se observa un Host llamado Zabbix Server, el mismo que corresponde al Servidor Zabbix registrado.

2.- Agregar un nuevo host, haciendo click en Create Host3.- Para lo cual se debe llenar el formulario de registro del host con la siguiente información:

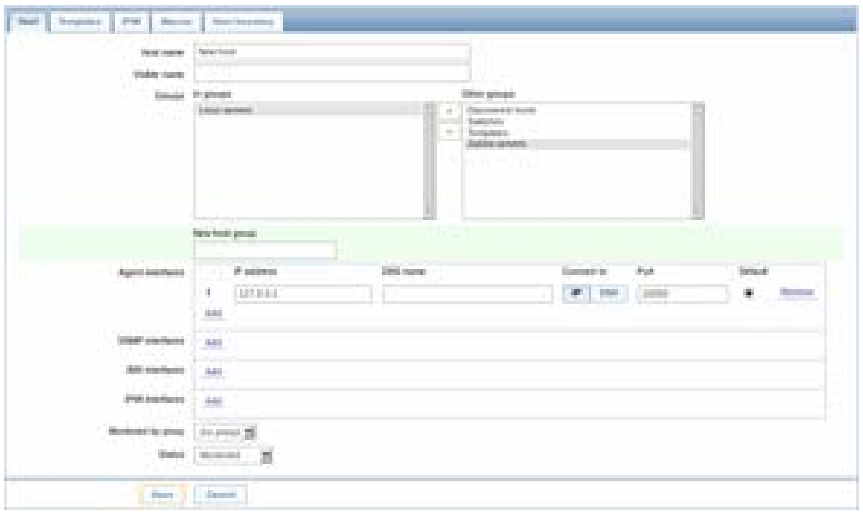


Figura 33, Registro de Hosts

La información básica que se debe ingresar es la siguiente:

**Host Name:** Nombre del host.

**Groups**: Seleccionar uno o varios grupos de la lista derecha. También se puede agregar un grupo ingresado un nombre en el campo "New host group".Los permisos de acceso se aplican por grupos y no por máquinas, por lo cual un host debe pertenecer por lo menos a un grupo.

**Dirección IP:** Ip del dispositivo instalado el agente Zabbix.

4.- Hacer clic en Save.

Configuración de ITEM

**Cada Host se encuentra compuesto por elementos llamados Items** que son **Módulos que recogen datos del Host** y son agrupados de igual manera por hosts, quiere decir que cada host tiene su propio Módulos que recogen datos Para configurar un ITEM se debe seguir lo siguientes pasos:

1.- Ir a la opción

Configuration → Hosts" y se localiza el "Host" al cual se quiere agregarle un nuevo "Item".

En el ejemplo del nuevo "Host" que se está realizando se observa que la columna de ITEMS tiene indicado "0" indicando que no existen ítems configurados Dar clikc en la opción "Create Item".

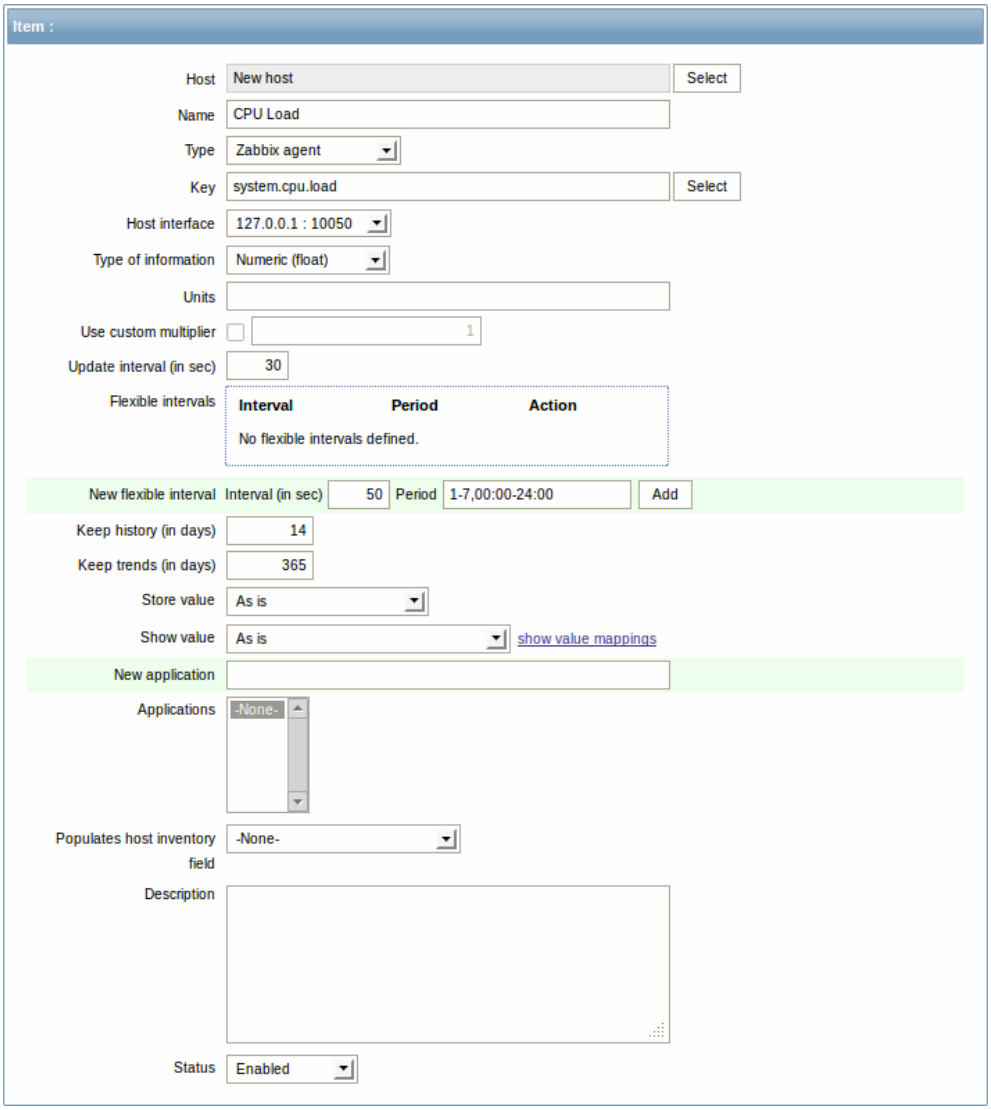



Figura 34, Items Zabbix

2.- Se debe llenar los parámetros que se necesiten para los items, al finalizar hacer clic en Save.

El nuevo item aparecerá en el apartado ITEMLIST.

Para comenzar a recolectar la información ir a:

1.- Monitoring → Latest data

2.- Dar clic en el signo **+**. La información comenzará a ser recolectada según el tiempo que se indica en el "Item".

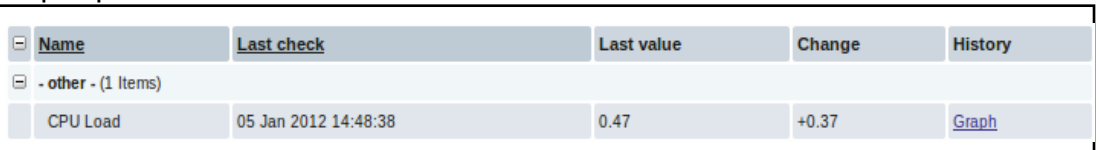



Figura 35, Pantalla de selección de sensores de monitoreo

## Triggers

**Los Trigger o disparadores son módulos encargados de** evaluar los valores recolectados por los Items con condiciones definidas por el administrador de red.

## Configuración de triggers

1.- Dar click en:

Configuration → Hosts

2.- Seleccionar el Host deseado y hacer clic en Trigger

3.- hacer click en Create Trigger

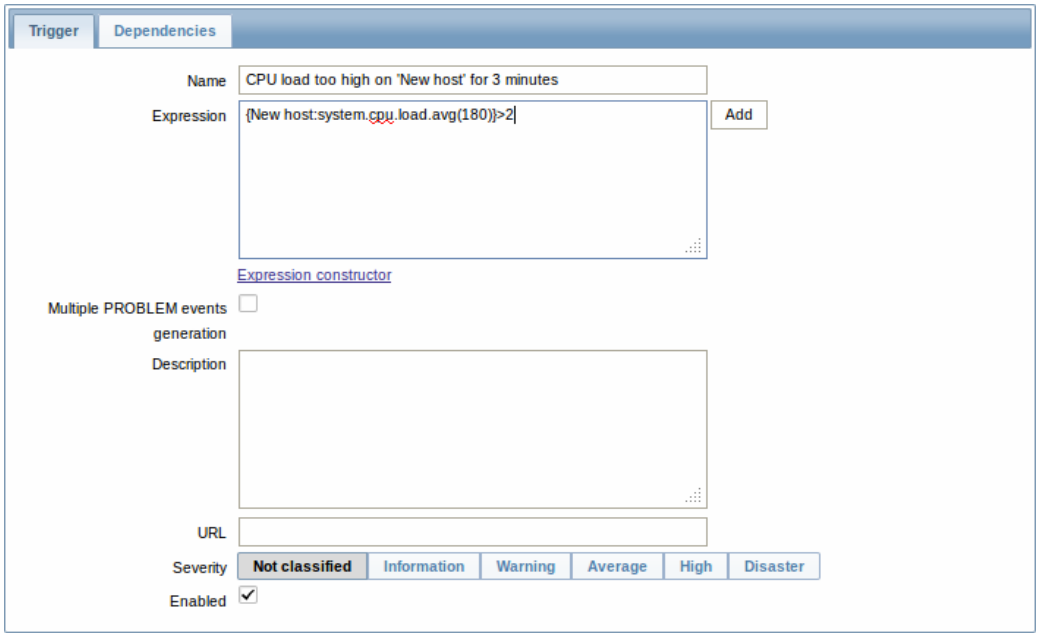



Figura 36, Triggers

**4.- Llenar la Configuración básica donde se encuentra:**

**Name:** Identificador para todas la gestiones donde se involucren los eventos relacionados.

**Expression**: Sentencia que el trigger llevara a cabo cuando se cumpla en el item

5.- Revisar el estado del Trigger, para lo cual se debe ir a:

Monitoring → Triggers.

Si el trigger se encuentra de color verde el resultado se encuentra dentro de las condiciones se indican

Si el trigger se encuentra de color rojo el resultado se encuentra fuera de las condiciones que se indican y es objeto de alerta.

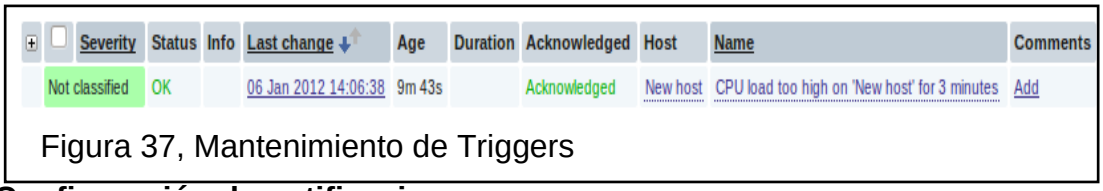



Figura 37, Mantenimiento de Triggers

**Configuración de notificaciones**

Zabbix nos permite notificar a través de "Correo Electrónico" mensajes vía "SMS" o mensajería instantánea (XMPP/JABBER).

En este caso se configura las notificaciones por correo electrónico

**Configuración de notificaciones vía E-mail**

Para configurar las notificaciones por correo electrónico se necesita parametrizar el acceso al servidor de correo electrónico.

1.- Ingresar a: Administration → Media types

2.- Click en Email en la lista Media Types

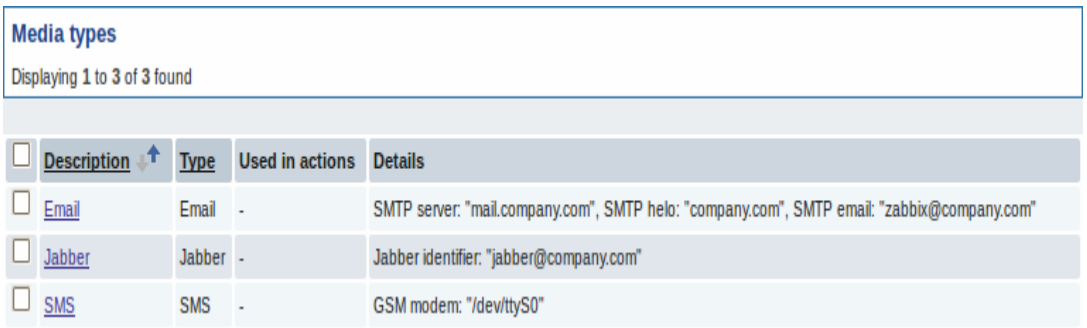



Figura 38, Tipo de Medios de Notificación

En la siguiente gráfica se muestra un ejemplo de configuración, de lo cual se debe ingresar los siguientes datos:

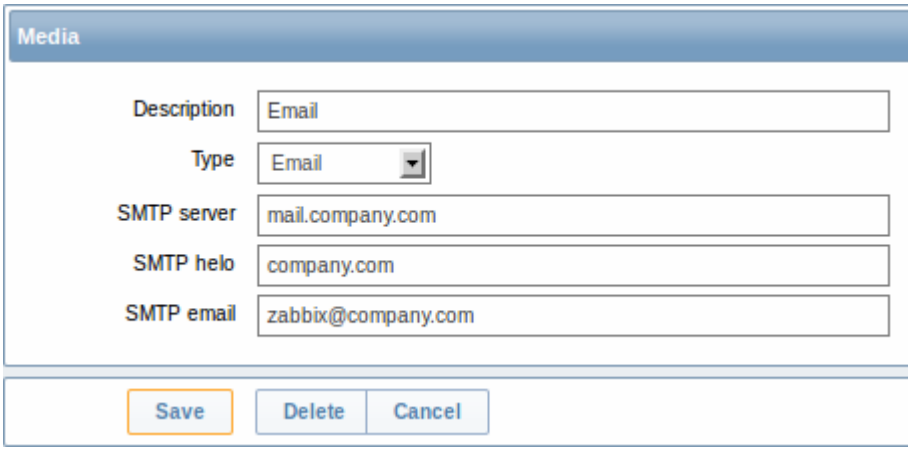



Figura 39, Ejemplo de configuración de notificaciones

**Description:** Nombre del MODULO MEDIA

**Type**: Existen tres opciones, Email, SMS and Jabber, en este caso seleccionar Email.

**SMTP Server:** Dirección ip del servidor de correo electrónico.

**SMTP helo**: Dominio del servidor de correo electrónico

**SMTP email:** Dirección de correo electrónico que se utilizará para enviar las notificaciones.

Es necesario activar el medio de notificación a los usuarios que lo utilizarán.

1.- Ir a la configuración ubicada en

Administrator → Users → Users

**Asignar la notificación al trigger**

1.- Dirigirnos a:

Configuration → Actions

2.- Seleccionar la Plantilla preconfigurada.

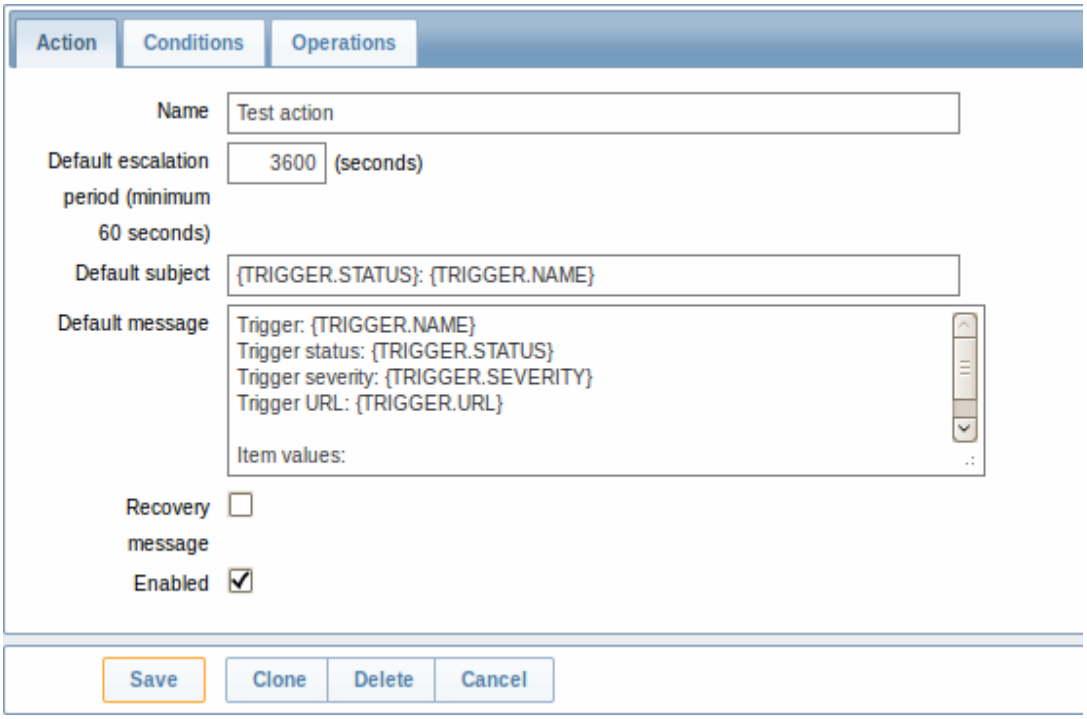



Figura 40, Asignación de notificación a trigger

**En la pantalla de configuración se encuentra lo siguiente:**

**Action:** Formulario con macros {TRRIGGER.STATUS}.Plantilla personalizable de acuerdo a las necesidades del administrador.

**Conditions:** Condiciones para las notificaciones de acuerdo a los eventos del trigger.

**Operations: Se debe agregar el usuario al que se enviaran las notificación,** es recomendable agregar el grupo Zabbix Administrators

3.- Presionar el botón Save

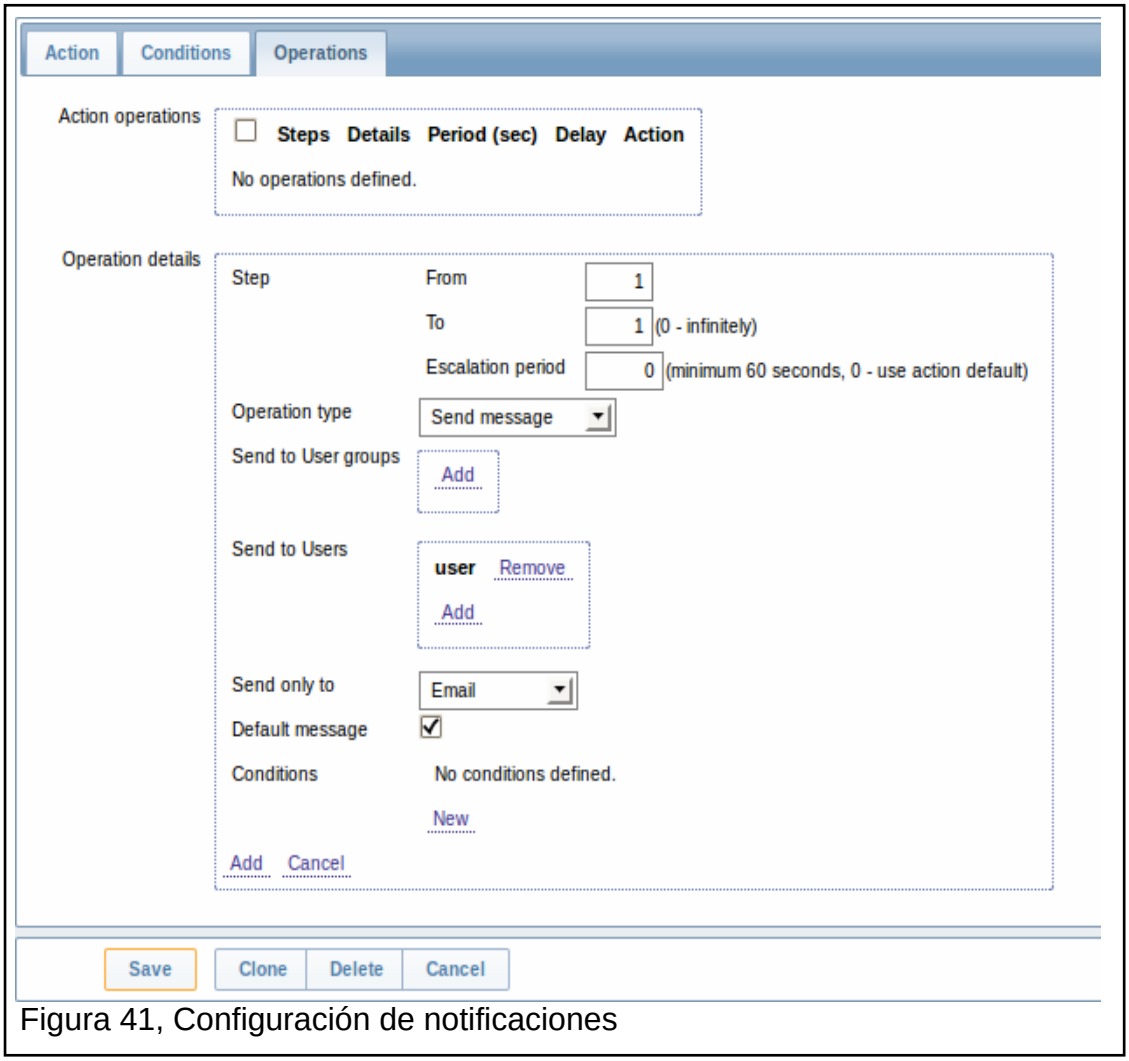



Figura 41, Configuración de notificaciones

## 5.2. MONITOREO y REPORTERIA

Zabbix ofrece una alta gama de reportes y monitorio en tiempo real, los cuales se los puede visualizar de la siguiente manera:

1.- Dirigirse a:

Monitoring donde se encuentran diferentes pestañas, una para cada tipo de reporte

Maps: Diagrama de los equipos monitoreados

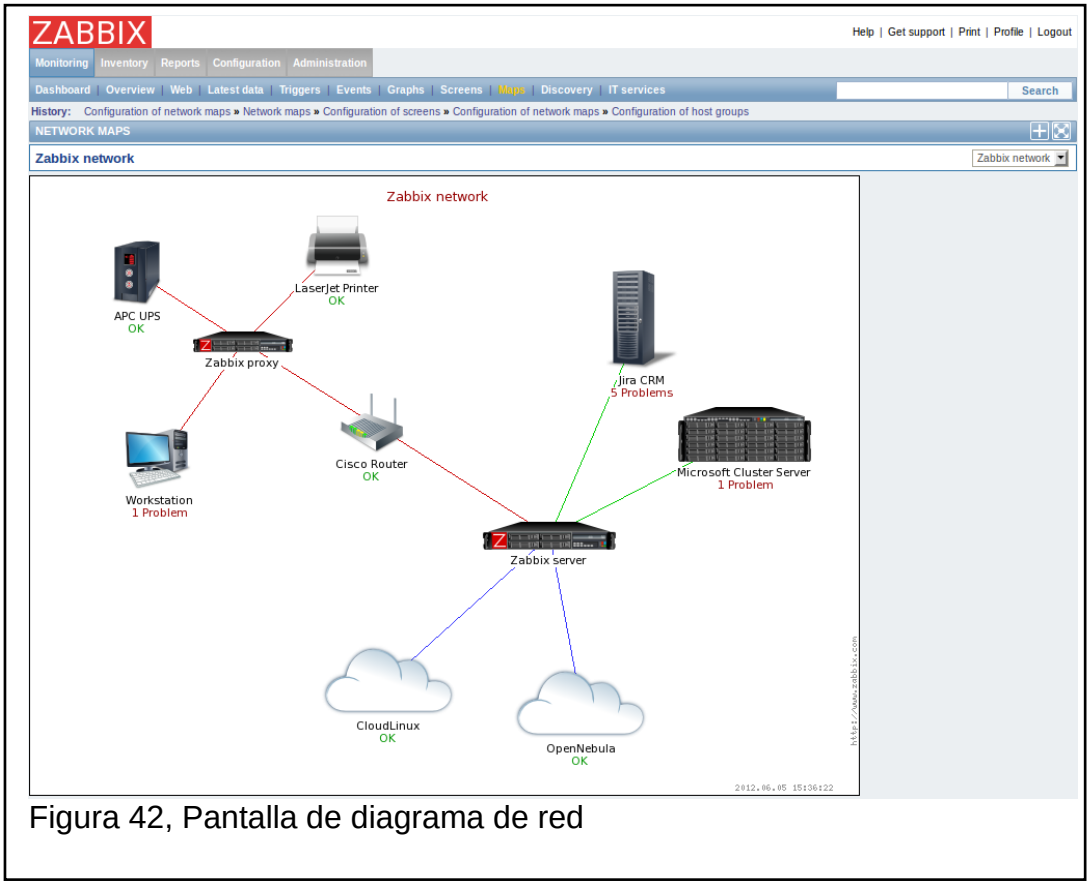



Figura 42, Pantalla de diagrama de red

Screens: Pantallas con graficas de los equipos monitoreados

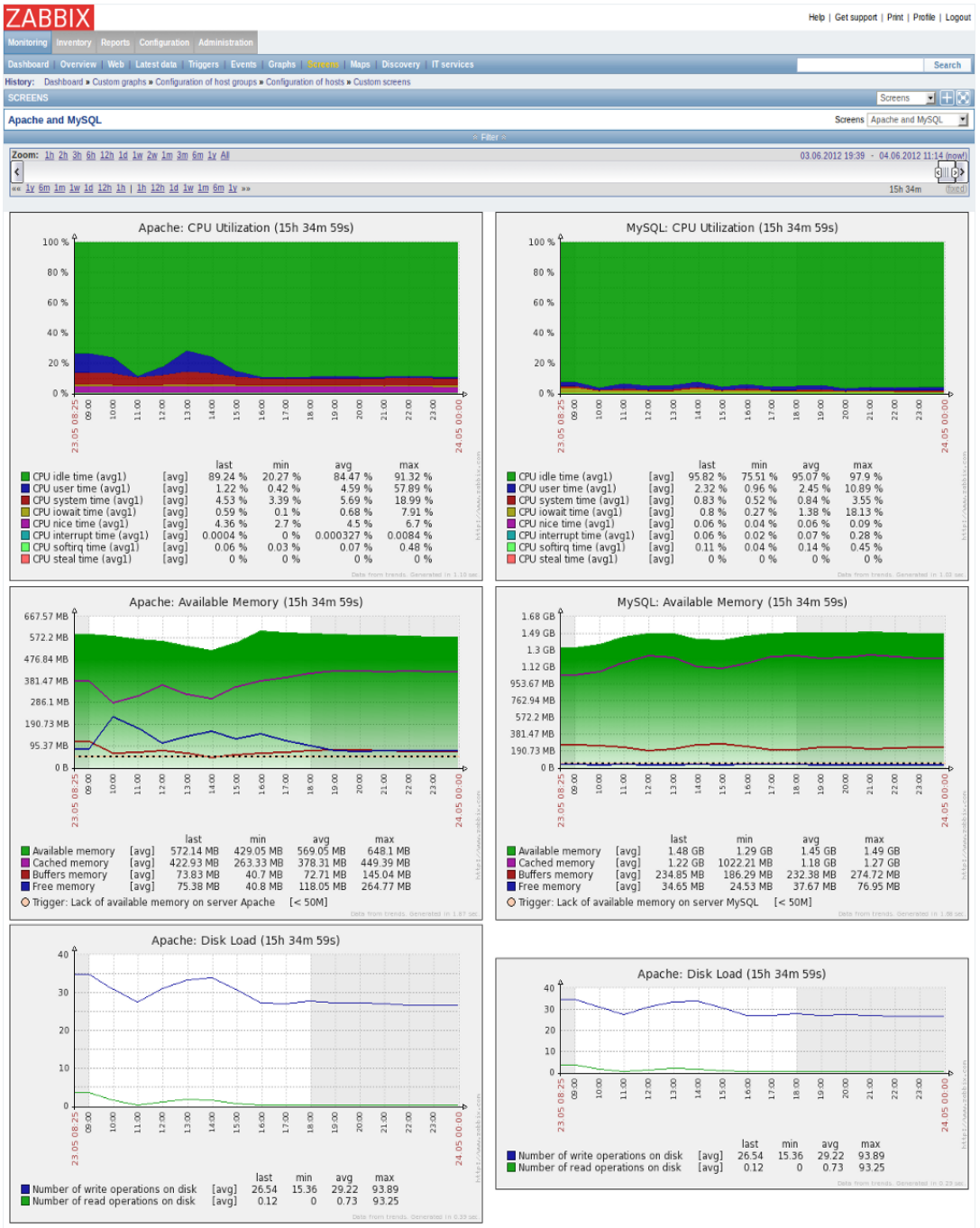



Figura 43, Screens

Events: Detalle de los eventos registrados

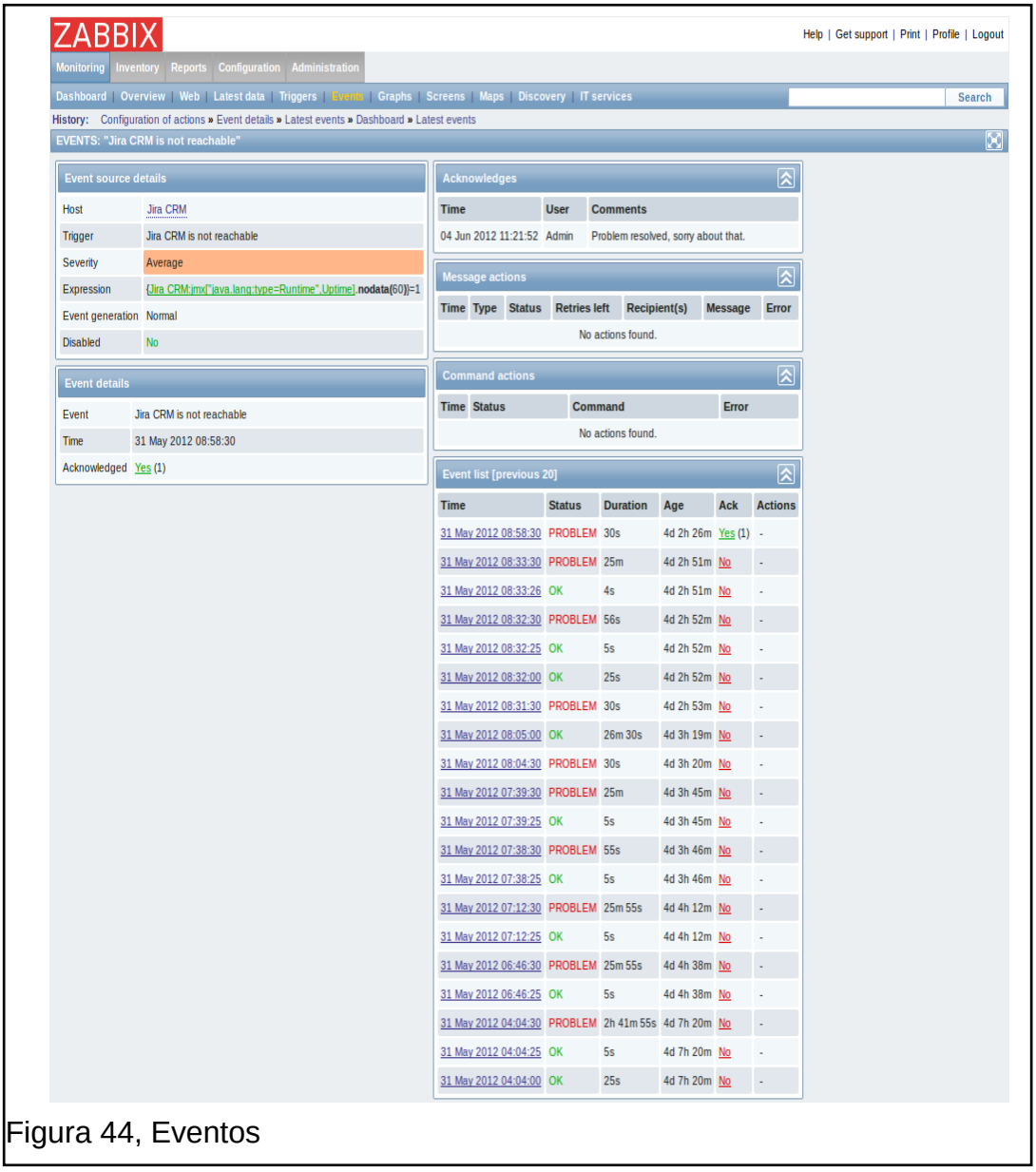



Figura 44, Eventos

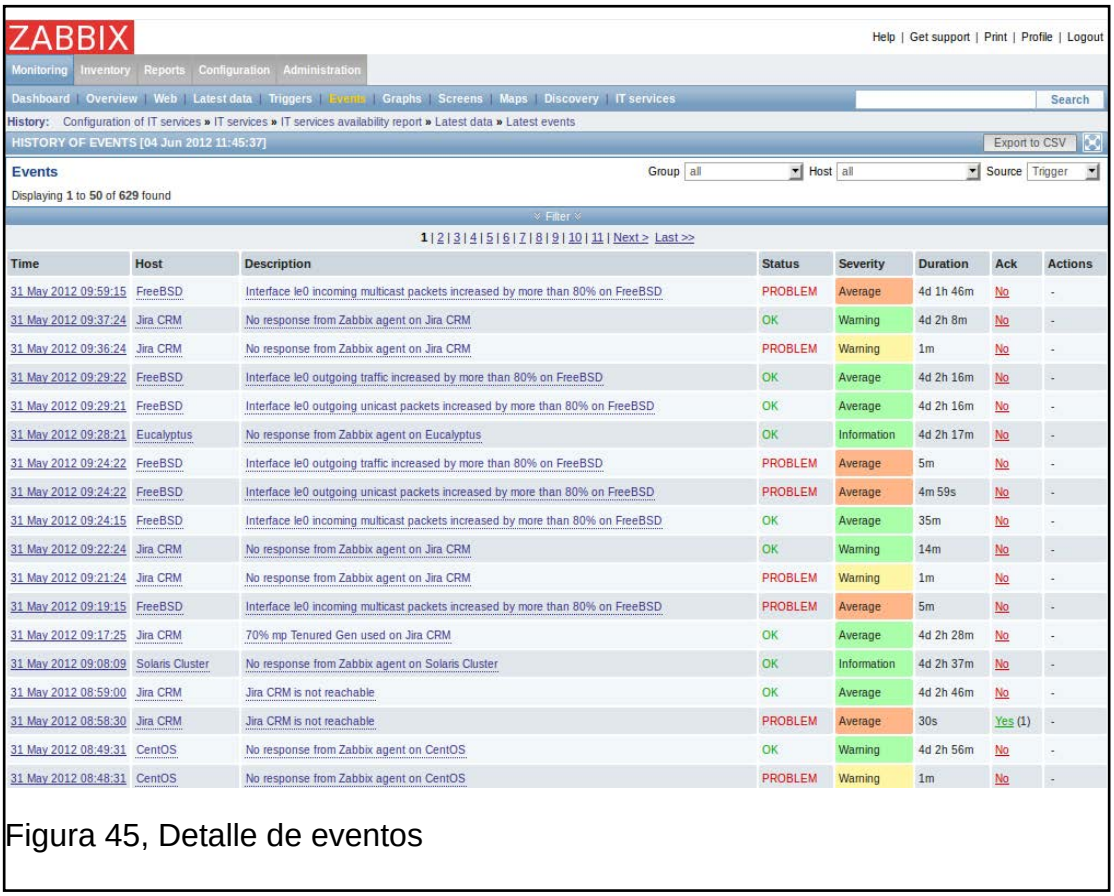



Figura 45, Detalle de eventos

Triggers: Detalle de la configuración de triggers

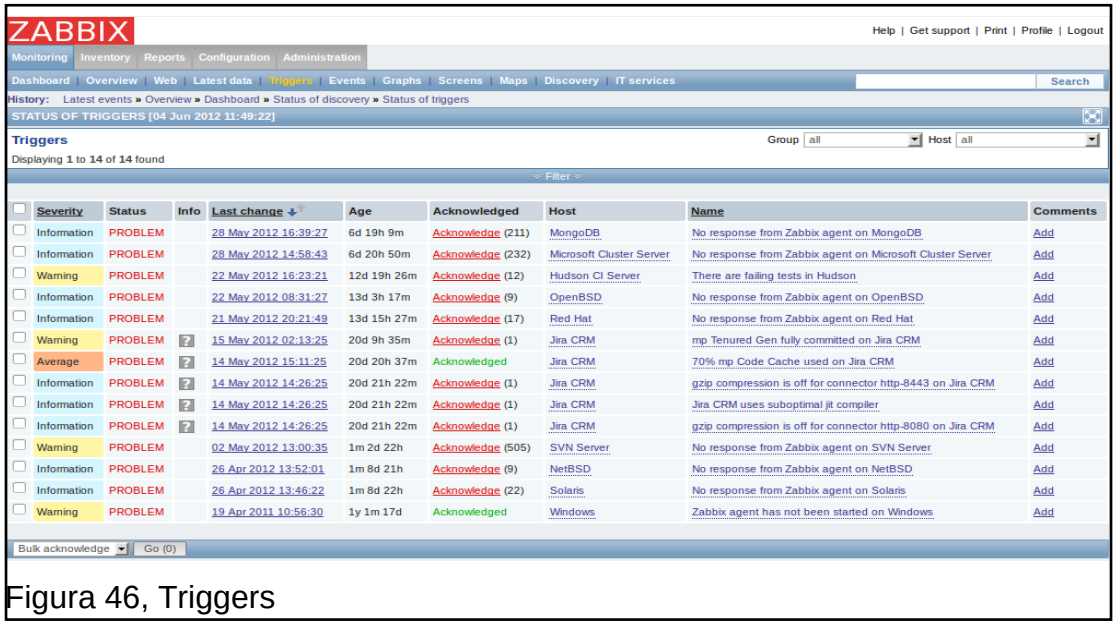
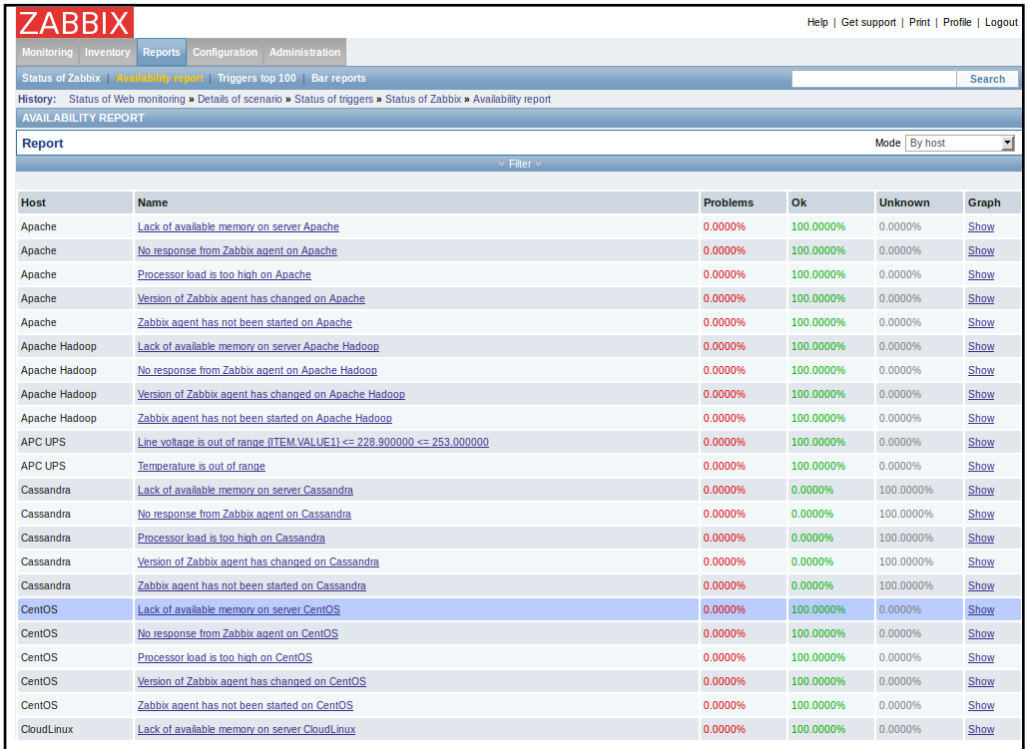



Figura 46, Triggers

También se encuentra reporte en la pestaña Reports

Availailability repots: Reportes habilitados para su visualización




| Host | Name | Problems | Ok | Unknown | Graph |
|---|---|---|---|---|---|
| Apache | Lack of available memory on server Apache | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache | No response from Zabbix agent on Apache | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache | Processor load is too high on Apache | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache | Version of Zabbix agent has changed on Apache | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache | Zabbix agent has not been started on Apache | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache Hadoop | Lack of available memory on server Apache Hadoop | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache Hadoop | No response from Zabbix agent on Apache Hadoop | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache Hadoop | Version of Zabbix agent has changed on Apache Hadoop | 0.0000% | 100.0000% | 0.0000% | Show |
| Apache Hadoop | Zabbix agent has not been started on Apache Hadoop | 0.0000% | 100.0000% | 0.0000% | Show |
| APC UPS | Line voltage is out of range {ITEM.VALUE1} <= 228.900000 <= 253.000000 | 0.0000% | 100.0000% | 0.0000% | Show |
| APC UPS | Temperature is out of range | 0.0000% | 100.0000% | 0.0000% | Show |
| Cassandra | Lack of available memory on server Cassandra | 0.0000% | 0.0000% | 100.0000% | Show |
| Cassandra | No response from Zabbix agent on Cassandra | 0.0000% | 0.0000% | 100.0000% | Show |
| Cassandra | Processor load is too high on Cassandra | 0.0000% | 0.0000% | 100.0000% | Show |
| Cassandra | Version of Zabbix agent has changed on Cassandra | 0.0000% | 0.0000% | 100.0000% | Show |
| Cassandra | Zabbix agent has not been started on Cassandra | 0.0000% | 0.0000% | 100.0000% | Show |
| CentOS | Lack of available memory on server CentOS | 0.0000% | 100.0000% | 0.0000% | Show |
| CentOS | No response from Zabbix agent on CentOS | 0.0000% | 100.0000% | 0.0000% | Show |
| CentOS | Processor load is too high on CentOS | 0.0000% | 100.0000% | 0.0000% | Show |
| CentOS | Version of Zabbix agent has changed on CentOS | 0.0000% | 100.0000% | 0.0000% | Show |
| CentOS | Zabbix agent has not been started on CentOS | 0.0000% | 100.0000% | 0.0000% | Show |
| CloudLinux | Lack of available memory on server CloudLinux | 0.0000% | 100.0000% | 0.0000% | Show |

Figura 47, Reportes Disponibles

Bar Report: Reporte de barras

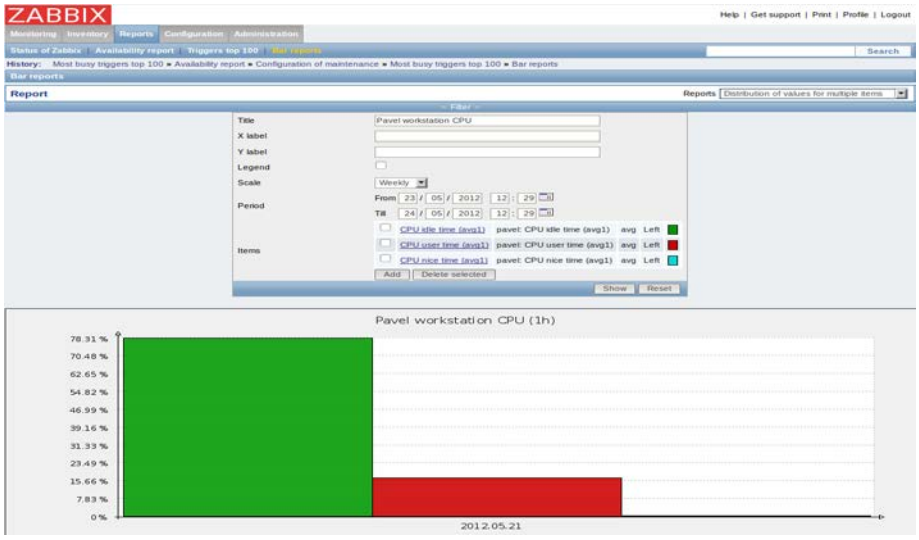



Figura 48, Reporte de Barras

## 5.3. PRUEBAS OPERATIVAS EN EL SERVIDOR

Durante la fase inicial de pruebas se hicieron pruebas en producción para garantizar el buen funcionamiento y fiabilidad de las respuestas que se esperan de Zabbix, para lo cual se han dividido los resultados de acuerdo a las problemáticas (capacidad en los servidores y rendimiento de enlace de datos) utilizando ciertos sensores para cada caso.

Para la capacidad de disco se utilizaran los siguientes sensores:

1.- Capacidad de disco

Este sensor tiene la capacidad de analizar el espacio de cada unidad de disco duro de los servidores monitoreados y por medio de graficas (barras, pastel, plano cartesiano) se puede obtener los valores reales por unidad de tiempo.

2.- Trigger

Como se explicó en el capítulo anterior los trigger tienen la capacidadde ser programados para enviar alertas cuando se cumpla ciertas condiciones, en este caso el evento programado consiste en notificar por medio de correo electrónico cuándo la capacidad de discos sea menor o igual a un 10% de su totalidad.

3.- Rendimiento

El sensor de rendimiento ofrece un análisis de procesador y memoria indicando el momento que el procesador se sature y puedan existir inconvenientes de rendimiento en los servicios que esos servidores ofrecen.

### Presentación de resultados

### Problema Reportado

El servidor de datos se satura varias veces al día y debido a la falta de espacio, actualmente esto se resuelve de acuerdo a cada llamada de los usuarios, sin embargo con el informe de reporte de Zabbix se obtiene información en línea de estos acontecimientos. De igual manera, los trigger informarán cuando el disco duro se llene hasta un porcentaje predefinido.

**Monitoreo**

**Sensor de Capacidad**

La capacidad total de la unidad C es de 136.69GB y de la unidad D es de 931.32GB

*Tabla 12, Capacidad Diaria del servidor de Datos*

| DISCO | DESCRIPCION | DIA1 | DIA2 | DIA3 |
|---|---|---|---|---|
| C | Sistema Operativo | La capacidad libre del disco es de 61.95 GB equivalente al 45.32% | La capacidad libre del disco es de 61.94 GB equivalente al 45.31% | La capacidad libre del disco es de 61.91 GB equivalente al 45.29% |
| D | Respaldos Usuarios | La capacidad libre del disco es de 123.67 GB equivalente al 13.28% | La capacidad libre del disco es de 59.67 GB equivalente al 6.31% | La capacidad libre del disco es de 82.45 GB equivalente al 8.85% |

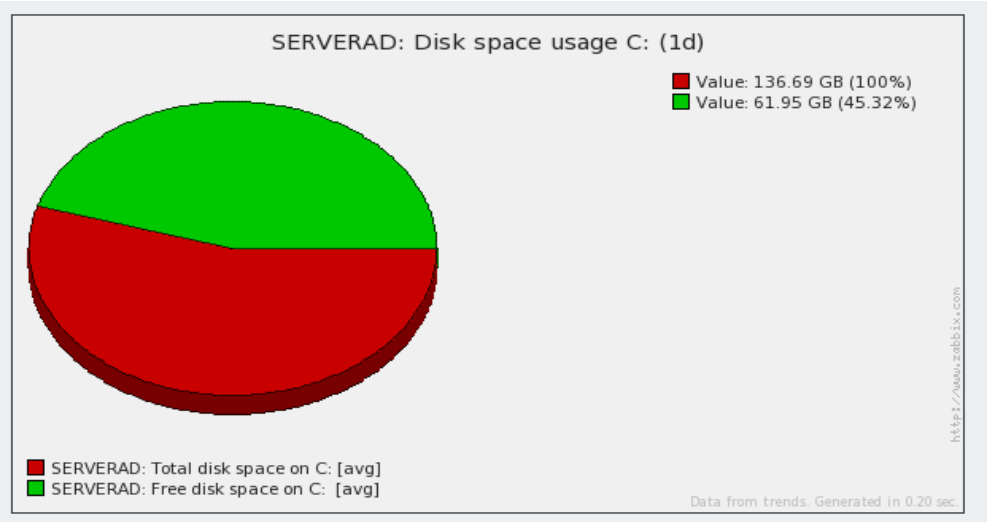



Figura 49, Capacidad Disco C Día 1

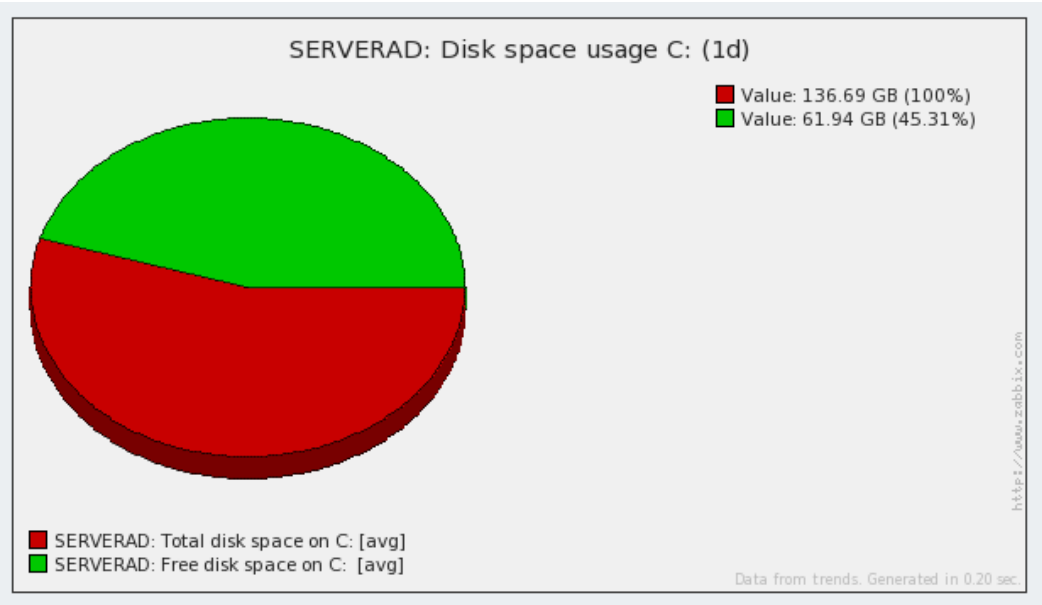



Figura 50, Imagen Disco C Día 2

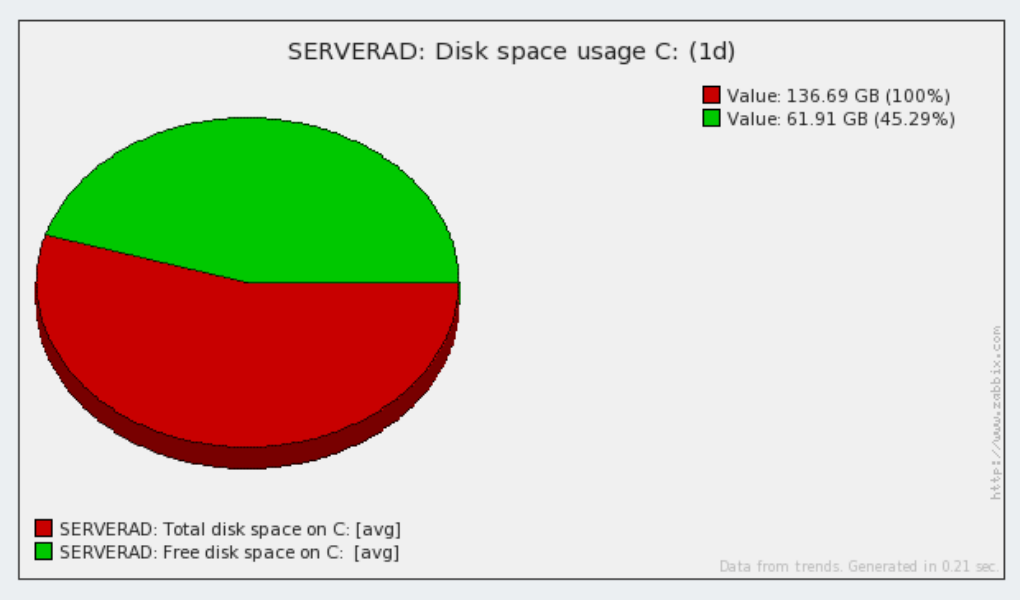



Figura 51, Imagen Disco C Día 3

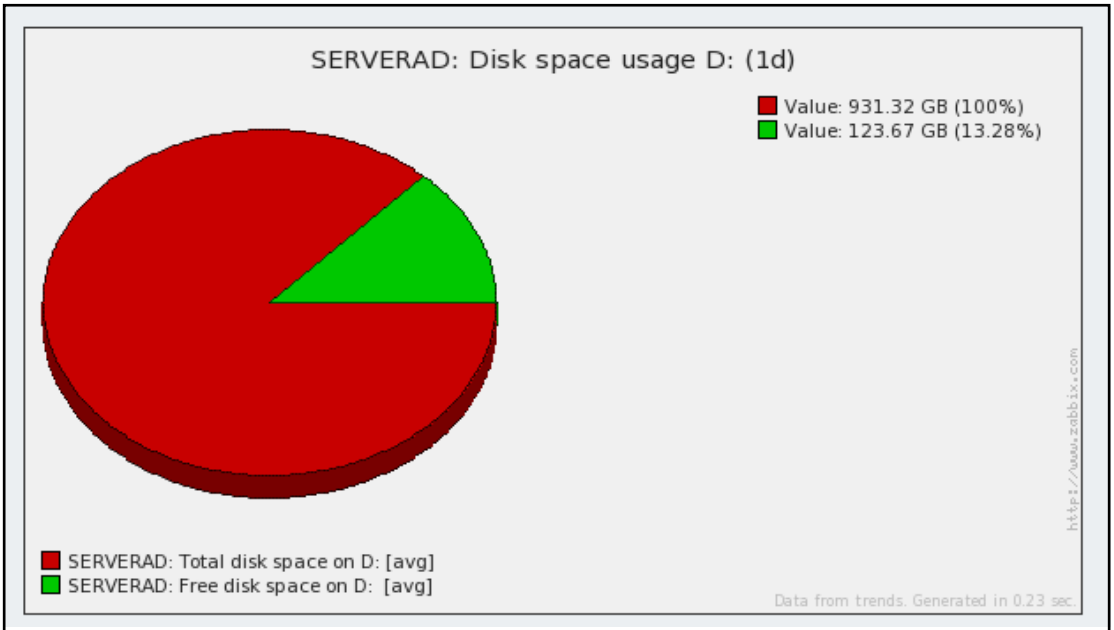



Figura 52, Imagen Disco D Día 1

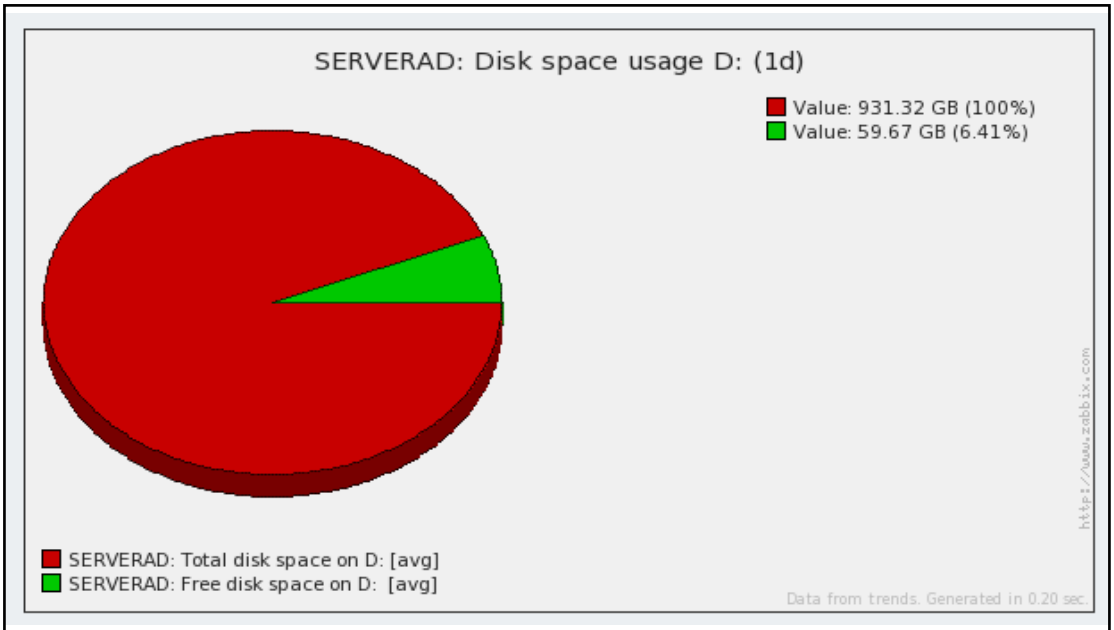



Figura 53, Imagen Disco D Día 2

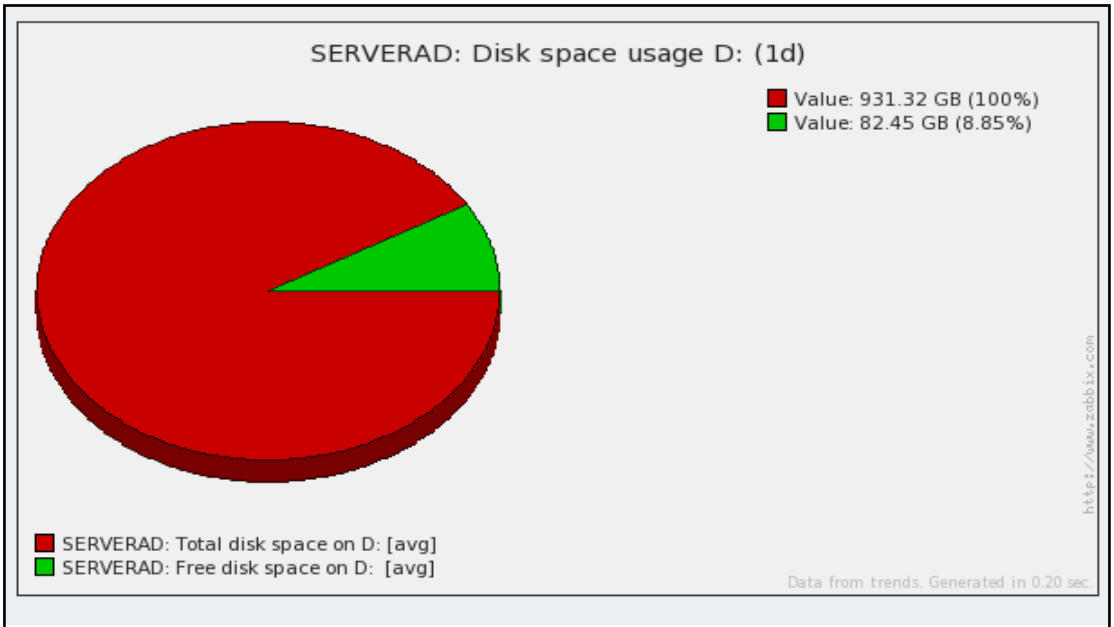



Figura 54, Imagen Disco D Día 3

**Sensor de Trigger**

La siguiente imagen presenta la configuración de los triggers los cuales alertaran a los operadores de sistemas sobre saturación en los discos duros.


Figura 55, Configuración Triggers

*Tabla 13, Activación de Triggers Diario*

| DISCO | DIA1 | DIA2 | DIA3 |
|---|---|---|---|
| C | El trigger no se activa ya que el disco tiene una capacidad libre del 45.32% | El trigger no se activa ya que el disco tiene una capacidad libre del 45.31% | El trigger no se activa ya que el disco tiene una capacidad libre del 45.29% |
| D | El trigger no se activa ya | El trigger se activa ya que | El trigger se activa ya que |

| | | | |
|---|---|---|---|
| | que el disco tiene una capacidad libre del 13.28% | el disco tiene una capacidad libre del 6.31% | el disco tiene una capacidad libre del 8.85% |

## Sensor de Rendimiento

*Tabla 14, Rendimiento Diario*

| DIA1 | DIA2 | DIA3 |
|---|---|---|
| Los procesadores se encuentran estables | Los procesadores se encuentran estables | Los procesadores se encuentran estables |

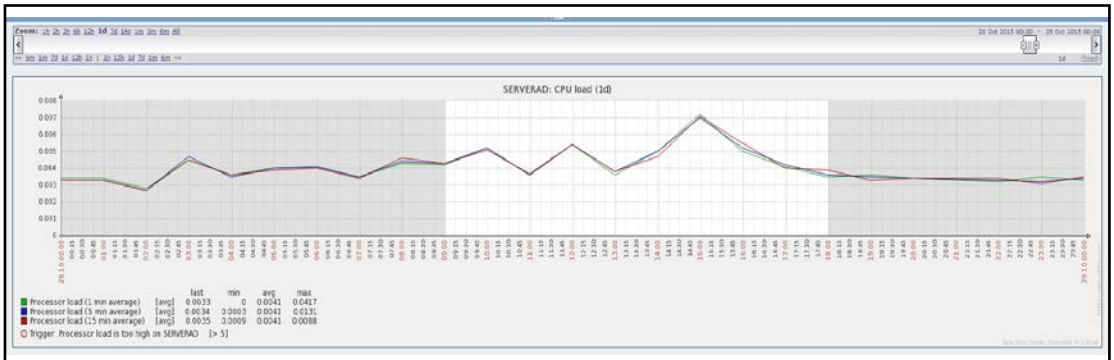



Figura 56, Rendimiento Día 1

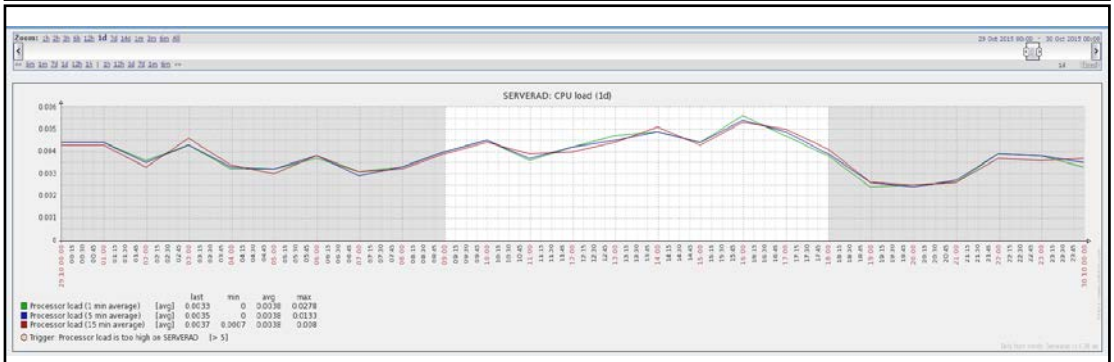



Figura 57, Rendimiento Día 2

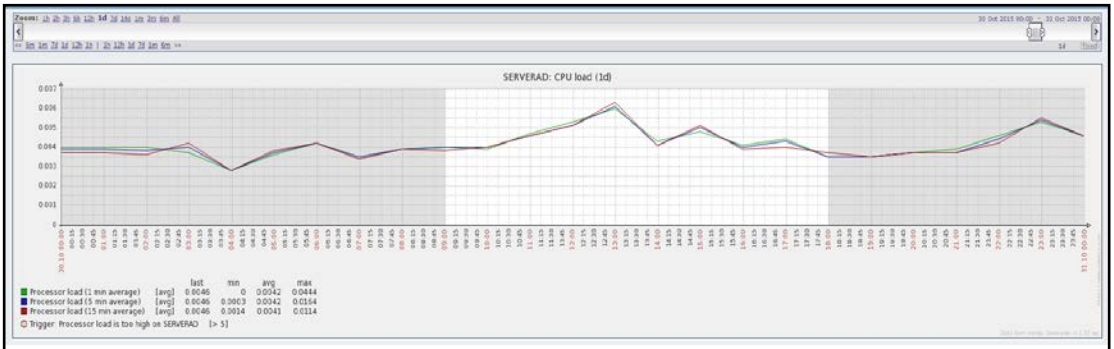



Figura 58, Rendimiento Día 3

## 5.4. Análisis de resultados

### Capacidad

Respecto a la capacidad de discos se observa que la unidad C del servidor posee una disminución constante de MB, los cuales no producen mayor alteración para el respaldo de información, sin embargo la unidad D tiene un decrecimiento de aproximadamente el 50% sobre todo en los dos primeros días, con el tercer día el decrecimiento es menor.

### Trigger

Los trigger se encuentran configurados cuando la capacidad llegue a un 10% y en cada caso, tanto el segundo día como el tercero se activa el trigger enviando alertas sobre el estado del servidor.

### Rendimiento

El rendimiento del servidor se mantiene estable durante los tres días, no existe alteraciones sobre este sensor.

### Acciones Preventivas

Cuando los trigger se activan el operador de sistemas debe revisar las alertas y liberar espacio en el servidor, sin embargo las alertas aun tardan demasiado y no son permiten liberar espacio a tiempo, para lo cual se debe aumentar el porcentaje de alertas a un 20%, con lo cual se obtendrá más tiempo para poder liberar espacio necesario.

**Análisis de Cambio**

Durante el desarrollo del problema se informó que se recibían alrededor de 10 llamadas diarias al día sobre problemas de espacio en el servidor, una vez realizado el monitoreo el índice ha reducido a 2 llamadas durante la semana, al prever que el espacio se aproxima a su capacidad máxima se realizan correctivos para liberar espacio, con lo cual los usuarios no tienen perdidas de información por espacio en disco duro.

Para el análisis de enlace de datos se utilizaran los siguientes sensores:

1.- Monitoreo de interface

Estos sensores permites revisar en tiempo real el tráfico de cualquier interfaz de red (puerto) que posea el dispositivo.

2.- Monitoreo de cpu

Este sensor permite monitorear el estado del cpu del router seleccionar

3.- Screens

Los screens nos permiten monitorear en tiempo real diferentes interfaces, permitiendo visualizar el comportamiento de la red en línea.

**Problema Reportado**

Durante el día se presenta problemas de lentitud en las aplicaciones con servicios cliente-servidor, estos enlaces se saturan y el proveedor debe reiniciar los servicios remotamente, este proceso conlleva tiempo en relazarse ya que al no existir una herramienta de monitoreo en tiempo real no se puede prever estos acontecimientos y tomar correctivos al respecto.

## Monitoreo

## Sensor de Interfaces

*Tabla 15, Monitoreo Diario de Interfaces*

| Router | Interfaz | Dia1 | Dia2 | Dia3 |
|---|---|---|---|---|
| Datos UIO | Fast Ethernet 0 | Durante el monitoreo diario se visualiza que ene l horario de la 0:00H hasta las 7:00H no existen variaciones de trafico tanto de salida como de entrada, sin embargo en el horario de 7:00H hasta las 18:00H se observa un notable aumento en la transmisión de subida. Las hora de mayor intensidad | Durante el monitoreo diario se visualiza que ene l horario de la 0:00H hasta las 7:00H no existen variaciones de trafico tanto de salida como de entrada, sin embargo en el horario de 7:00H hasta las 18:00H se observa un notable aumento en la transmisión de subida. Las hora de mayor intensidad son de 7.45H hasta las 9:00H, a partir de este momento existe un | Durante el monitoreo diario se visualiza que ene l horario de la 0:00H hasta las 7:00H no existen variaciones de trafico tanto de salida como de entrada, sin embargo en el horario de 7:00H hasta las 18:00H se observa un notable aumento en la transmisión de subida. Las hora de mayor intensidad |

| | | | | |
|---|---|---|---|---|
| | | son de 7.45H hasta las 9:00H, incluyendo un pico de subida máximo a las 17:00H | decrecimiento en la saturación del enlace, manteniéndose estable hasta las 20:00H momento en el cual empieza un pico en el canal de datos. | son de 14:00H hasta las 17:00H, manteniéndose altos los tiempos de trabajo del enlace hasta esa hora. |

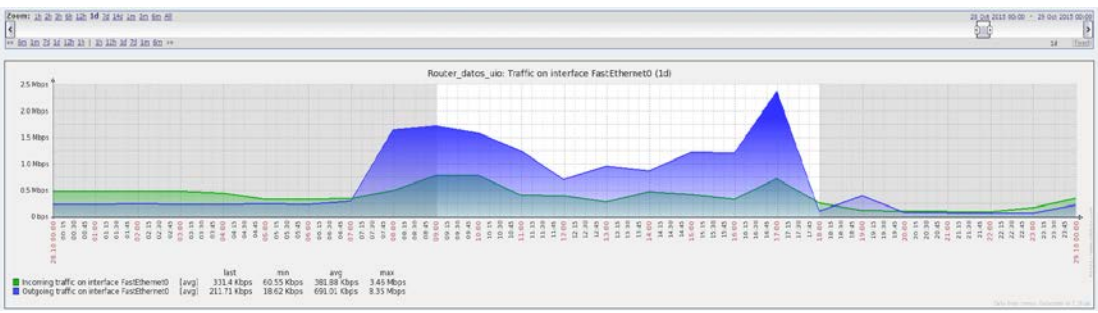



Figura 59, Enlace Router Día 1

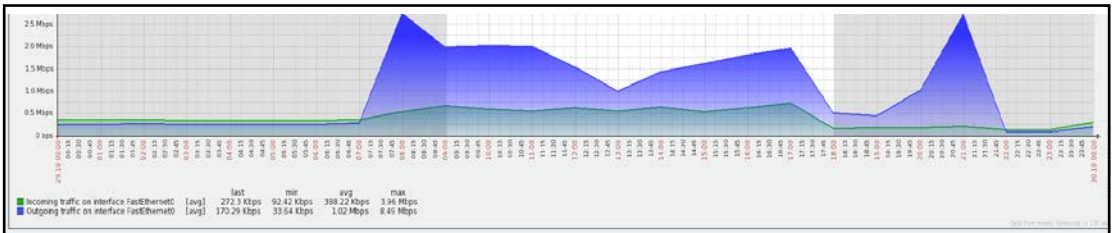



Figura 60, Enlace Router Día 2

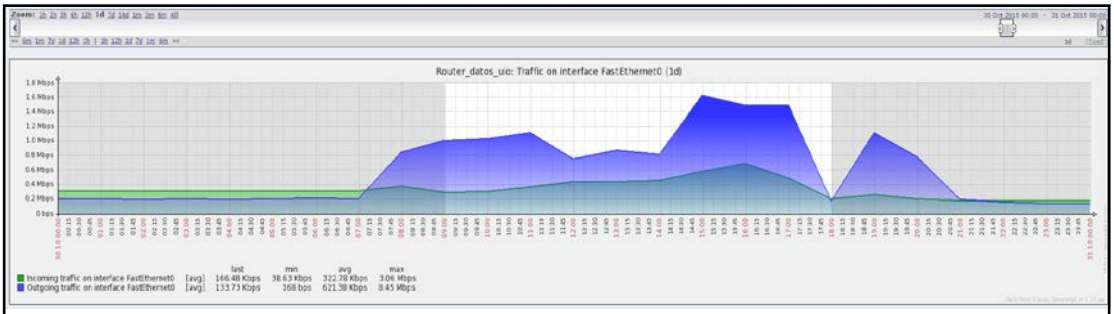



Figura 61, Enlace Router Día 3

## Sensor de CPU

*Tabla 16, Monitoreo Diario de proceso Router*

| DIA1 | DIA2 | DIA3 |
|---|---|---|
| El nivel de proceso del router no presenta mayor variación, siendo un pico máximo el 19% de su rendimiento máximo | El nivel de proceso del router no presenta mayor variación, siendo un pico máximo el 16% de su rendimiento máximo | El nivel de proceso del router no presenta mayor variación, siendo un pico máximo el 16% de su rendimiento máximo |

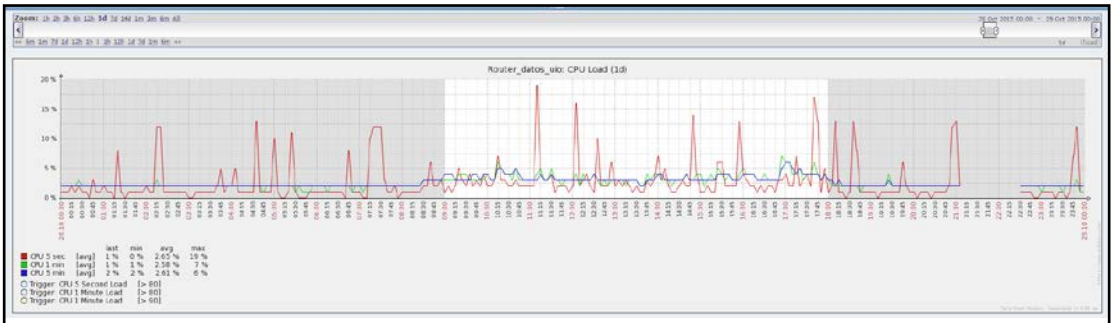



Figura 62, Proceso CPU Router Día 1

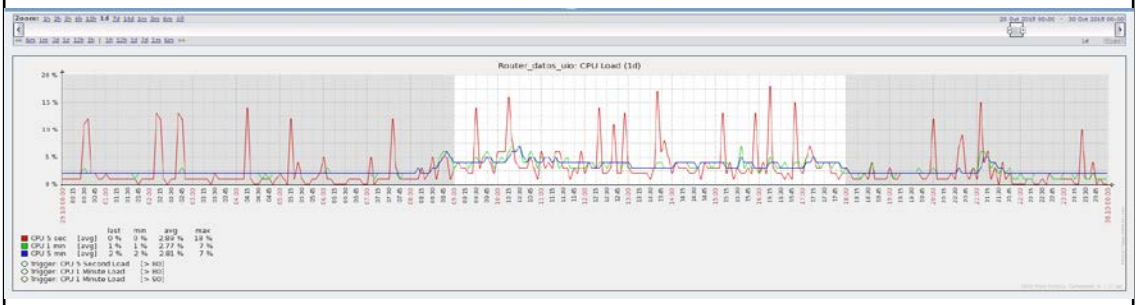



Figura 63, Proceso CPU Router Día 2


Figura 64, Proceso CPU Router Día 3

### 5.5. Análisis de resultados

En la revisión se puede determinar que el tráfico e red no se encuentra relacionado al equipo físico, ya que en los tres días pese a que existe un alto tráfico a ciertas horas el procesamiento del router no excede el 20%, el problema principal radica en la navegación que realizan los usuarios, esta navegación debe ser determinada por un sistema especializado para monitoreo de navegación y obtener resultados por pc indicando cual es la navegación diaria de los hosts y determinar las paginas o procesos que más causan tráfico de red.

**Acciones a tomar**

Las acciones que se pueden tomar para prevenir que exista aumento en el tráfico de red es bloqueando por medio de proxy la navegación y limitando el ancho de banda por departamentos.

## 5.6. CONCLUSIONES Y RECOMENDACIONES

Debido a políticas internas de la empresa no se puede realizar un análisis con un snifer como wireshark ya que es un proceso invasivo y perjudica en el rendimiento diario, de igual manera las configuraciones de los routers y switchs son informacion confidencial la cual no puede ser publicada.

La empresa Oriente Seguros cuenta con inconvenientes en los servidores tanto para capacidad de disco como para enlaces, los usuario en múltiples ocasiones se comunican con el departamento de TI para solventar sus inconvenientes, sin embargo al no contar con una herramienta de monitoreo los tiempos de respuestas son demorosos y no permiten un trabajo continuo en ciertos servicios de la empresa.

Para solventar este inconveniente se procede a instalar Zabbix, el cual con su reportaría y monitoreo permite tomar ventaja frente a estos problemas previniendo que los servidores carezcan de espacio siendo liberados en momentos oportunos, de igual manera tomando medidas de acuerdo a los enlaces de datos permitiendo identificar los horarios de mayor incidencia y saturación en los router y dispositivos de comunicaciones.

La empresa, luego del análisis por medio de Zabbix ha tomado medidas preventivas, al liberar el espacio de los discos a tiempo, de igual manera se puede elaborar políticas de permisos de internet y restricciones de datos para que los usuarios no saturen los enlaces de datos.

Con estos correctivos se ha evidenciado una notable disminución de llamadas y reportes de incidencias al departamento de IT.

# Referencias


Adrformacion. (2015). *Protocolos y el enrutamiento*. Obtenido de http://www.adrformacion.com/cursos/wserver082/leccion3/tutorial3.html

Alumnos. (9 de Junio de 1977). *HISTORIA DEL TCP/IP*. Obtenido de http://alumno.ucol.mx/al971977/public_html/tarea1s.o..htm

Alumnos. (s.f.). *HISTORIA DEL TCP/IP*. Obtenido de http://alumno.ucol.mx/al971977/public_html/tarea1s.o..htm

Carol Mendoza . (03 de 03 de 2014). *Capas del modelo OSI*. Obtenido de http://redesdearealocalmendozas.blogspot.com/

CLAVIJO, M. S., & SALAZAR, N. G. (2010). IMPLEMENTACIÓN DE ZABBIX COMO HERRAMIENTA DE MONITORIZACIÓN DE INFRAESTRUTURA. Bogota, Colombia.

El Correo de las Indias. (01 de Abril de 2002). *Topologías de red*. Obtenido de http://lasindias.com/indianopedia/topologias-de-red

Estándares de QoS (RFC), Q. (15 de Marzo de 2016). *Msdn.microsoft.com*. Obtenido de https://msdn.microsoft.com/es-es/library/cc786886(v=ws.10).aspx

Free Software Foundation. (05 de Junio de 2015). *El sistema operativo GNU*. Obtenido de http://www.gnu.org/gnu/gnu.html

Gallegos. (s.f.). *Capa de transporte del modelo OSI.* Obtenido de http://www.utp.edu.co/~fgallego/claseXcapitulo/capitulo04-capa%20de%20transporte.pdf

Gallegos. (s.f.). *Capa de transporte del modelo OSI.* Obtenido de http://www.utp.edu.co/~fgallego/claseXcapitulo/capitulo04-capa%20de%20transporte.pdf

Gerald Aguirre & Himura Productions Inc. (14 de enero de 2012). *Fundamentos de Informática*. Obtenido de Ancho de Banda: http://portalgerald.blogspot.com/2012/01/ancho-de-banda.html

Itesa. (s.f.). *Movimiento de datos en la red*. Obtenido de Encapsulación de datos: http://www.itesa.edu.mx/netacad/introduccion/course/module3/3.3.1.2/3.3.1.2.html

J.C. Fernández J.A. Corrales y A. Otero. (22 de 11 de 2007). *La seguridad en la familia de protocolos SNMP*. Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html

J.C. Fernández, J.A. Corrales y A. Otero. (22 de 11 de 2007). *La seguridad en la familia de protocolos SNMP*. Obtenido de http://www.rediris.es/difusion/publicaciones/boletin/50-51/ponencia16.html

Jose Solano. (s.f.). *Modelo OSI*. Obtenido de http://dis.um.es/~lopezquesada/documentos/IES_1213/LMSGI/curso/xhtml/xhtml22/

León, E. E. (2005). *Redes de Datos*. Obtenido de http://www.monografias.com/trabajos30/redes-de-datos/redes-de-datos.shtml

Luis Antonio Rodriguez Díaz. (s.f.). *Conoce cómo funciona Zabbix y como usarlo*. Obtenido de http://911-ubuntu.weebly.com/Zabbix_como_funciona

OrienteSegurosEmpresa. (2015). *http://www.segurosoriente.com/productos/seguros-empresariales/seguros-de-construccion/*. Obtenido de http://www.segurosoriente.com/productos/seguros-empresariales/seguros-de-construccion/

QuasarSofrware. (s.f.). *Zabbix*. Obtenido de http://www.quasarbi.com/ZABBIX.html

Ronald Pinos. (11 de 11 de 2014). *Nivel de Enlace*. Obtenido de http://ronaldpinos.blogspot.com/

Ross, K. W., & Kurose, J. F. (2010). REDES DE COMPUTADORAS. PEARSON EDUCACIÓN, S. A. 2010.

SegurosOriente. (2015). *ORIENTE FIANZAS*. Obtenido de http://www.segurosoriente.com/productos/seguros-empresariales/seguro-de-fianzas

Simple Organization. (2012-2015). *tiposde*. Obtenido de tipos de protocolos: http://www.tiposde.org/informatica/513-tipos-de-protocolos/

Stallings, W. (2004). Comunicaciones y Redes de Computadores. En W. Stallings, *Comunicaciones y Redes de Computadores* (pág. 896). Madrid: PEARSON EDUCACIÓN, S. A.

Wikipedia. (23 de 10 de 2015). *Unidad de datos de protocolo*. Obtenido de https://es.wikipedia.org/wiki/Unidad_de_datos_de_protocolo

# ANEXOS

**Instalación de Centos**

Insertar el medio de instalación en la unidad que se desea instalar.

Al iniciar la carga del SO se presentara la siguiente pantalla donde se selecciona el modo de instalación,

| Modo | Descripción |
|---|---|
| Normal | Instalación de manera grafica |
| Con Driver básico de video | Instalacion por medio de código(sin interfaz grafica) |

Iniciamos con la primera opción


Como instalar Centos 6.4 – Inicio

Cuando la instalación comienza el SO solicita verificar el medio de instalación, ésto se debe realizar si es un servidor critico o se tiene alguna sospecha de que el medio se encuentre con fallos, si es un servidor de prueba se puede omitir este paso seleccionando “Skip” y

presionando “Enter”, por otro lado si se desea realizar la verificación del medio  seleccionar “Ok” y presiona la tecla “Enter”.


Como instalar Centos 6.4 – Verificación de medio de instalación

Al iniciar la instalación de Centos se debe dar click en “Next”


Como instalar Centos 6.4 – Instalador

Se debe elegir el idioma deseado, en este caso español seleccionando “Spanish” y dar click en el botón “Next”


Como instalar Centos 6.4 – Selección de Idioma

Seleccionar la distribución del teclado que se utilices.


Como instalar Centos 6.4 – Selección de distribución de Teclado

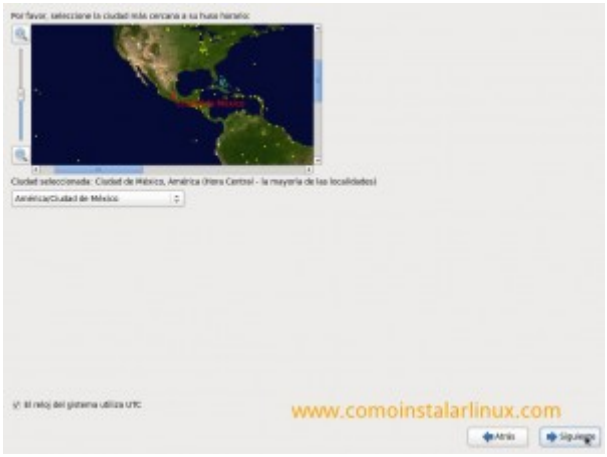
Si se dispone de un dispositivos de almacenamiento externo seleccionar “Dispositivos de almacenamiento especializados” caso contrario si solo se cuenta con discos locales seleccionar “Dispositivos de almacenamiento básicos”


Como instalar Centos 6.4 – Seleccionar tipo de almacenamiento

Especificar un nombre para el servidor y configurar la o las interfaces de red.


Como instalar Centos 6.4 – Nombre de host

Indica en el mapa o en la lista, la zona horaria del país donde se ubica el servidor.




Como instalar Centos 6.4 – Zona horaria

Ingresar una contraseña para el usuario root

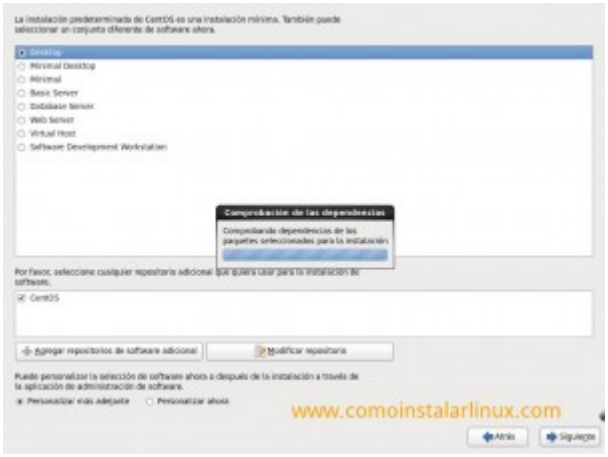

Como instalar Centos 6.4 – Contraseña de root

Para este caso se utilizará la instalación básica, la misma que ocupa todo el espacio del disco seleccionando la opción “Usar todo el espacio” y dar click en el botón “Siguiente”. Mostrando una advertencia indicando que todas las particiones del disco serán borradas y los datos eliminados.


Como instalar Centos 6.4 – Usar todo el espacio por default


Como instalar Centos 6.4 – Advertencia de borrado

Para realizar una instalación básica y rápida seleccionar “Minimal Desktop” en la que se instalará el servidor con un entorno gráfico pero sin ningún servicio, también se puede seleccionar la opción “Minimal” para instalar un servidor sin interfaz gráfica.




Como instalar Centos 6.4 – Comprobando paquetes

Luego de realizar este paso se copiarán los paquetes de software y se configurará el sistema operativo. Al terminar la instalación y configuración de los paquetes se indicará que es necesario re iniciar el servidor.


Como instalar Centos 6.4 – Instalación de paquetes


Como instalar Centos 6.4 – Reinicio del sistema

Al arrancar el sistema por primera vez luego de la instalación de Centos mostrará las siguientes pantallas en las que se debe ingresar ciertos parametros. La primera es una pantalla de Bienvenida la misma que se pasa dando click en “Al Frente”


Como instalar Centos 6.4 – Arranque de sistema instalado


Como instalar Centos 6.4 – Configuración inicial

Aceptar el acuerdo de licencia del software


Como instalar Centos 6.4 – Licencia GPL

Luego se debe crear un usuario operador el cual será diferente a root. Asignando una contraseña para su acceso

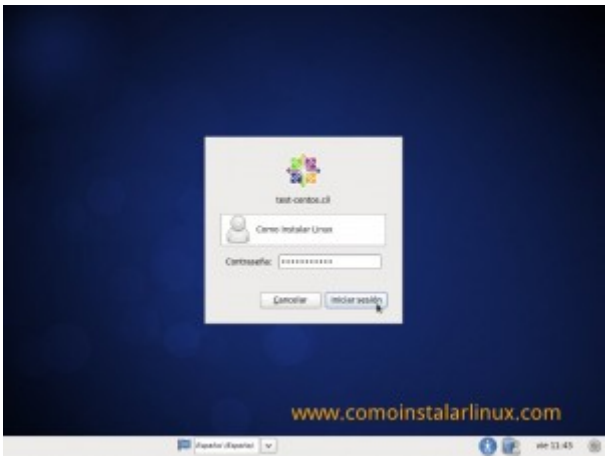

Como instalar Centos 6.4 – Crear usuario del sistema

Indicar la fecha y hora que tendrá el servidor, si se dispone de un servidor NTP para sincronizar la configuración de fecha y hora se lo debe configurar en esta pantalla.

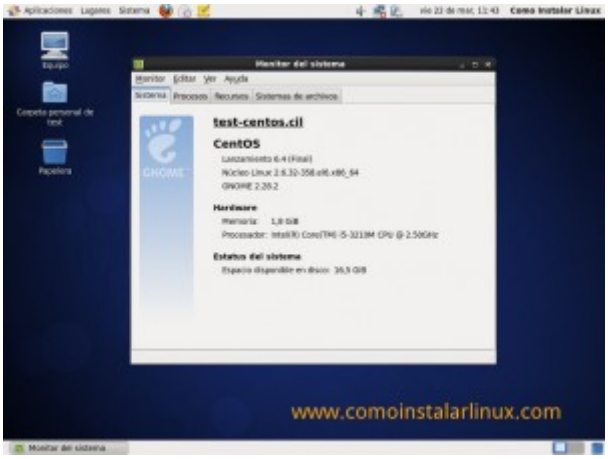

Como instalar Centos 6.4 – Fecha y hora del sistema

Por ultimo iniciar sesión con el usuario recién creado


Como instalar Centos 6.4 – Ingreso al sistema instalado




Como instalar Centos 6.4 – Ingreso de usuario y contraseña




Como instalar Centos 6.4 – Acerca de Centos 6.4

Actualizar el sistema operativo

En la ventana de terminal escribimos

**yum update –y**

INSTALAR Y CONFIGURAR LAMP

Procedemos a instalar los complementos LAMP (LIMUS-APACHE-MYSQL-PHP) necesarios para la instalación de cualquier aplicación que requiera base de datos o tenga interfaz web.

Apache

Es un web server multiplataforma open source que incluye varias características entre ellas CGI, SSL y dominios virtuales.

Para instalar apache ingresamos la siguiente línea de comando en el terminal:

# yum install httpd -y

Para iniciar el servicio apache(http) e iniciarlo automáticamente al reinicio de la pc:

# service httpd start

# chkconfig httpd on

Para realizar conexiones remotas se debe habilitar el Puerto 80(default) en el firewall o router.

Para lo cual editar el archivo /etc/sysconfig/iptables,

# vi /etc/sysconfig/iptables

Agregar la siguiente línea.

[...]

-A INPUT -m state --state NEW -m tcp -p tcp --dport 80 -j ACCEP

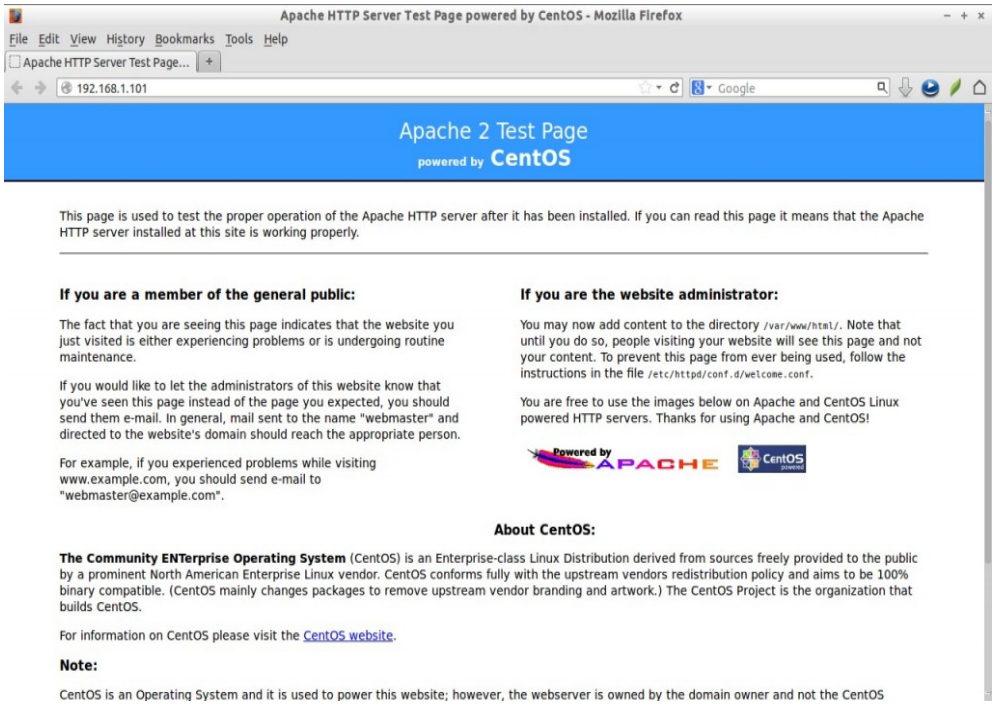
[...]

Se debe resetear el iptables:

# service iptables restart

Para comprobar que la instalación se ha realizado correctamente se debe ingresar al buscador e ingresar a la dirección siguiente

http://localhost/ o http://ip_servidor/.




MySQL

Es una herramienta de base de datos libre usualmente instalada en el conjunto LAMP.

Para instalar ingresar la siguiente línea de comandos en el terminal:

# yum install mysql mysql-server -y

Para iniciar el servicio mysql e iniciarlo automáticamente al reinicio de la pc:

# service mysqld start

# chkconfig mysqld on

Configurar la contraseña de root

Por default la contraseña de root de mysql no se encuentra configurada, sin embargo por cuestiones de seguridad se lo debe realizar.

# mysql_secure_installation

Con lo cual se desplegara el siguiente archivo en el cual se debe configurar la contraseña y seguir los parámetros recomendados en la imagen adjunta

```
NOTE: RUNNING ALL PARTS OF THIS SCRIPT IS RECOMMENDED FOR ALL MySQL
      SERVERS IN PRODUCTION USE!  PLEASE READ EACH STEP CAREFULLY!
In order to log into MySQL to secure it, we'll need the current
password for the root user.  If you've just installed MySQL, 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):     ## Press Enter ##
OK, successfully used password, moving on...
Setting the root password ensures that nobody can log into the MySQL
root user without the proper authorisation.

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

By default, a MySQL installation has an anonymous user, allowing anyone
to log into MySQL 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]     ## Press Enter ##
 ... 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]     ## Press Enter ##
... Success!
By default, MySQL 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]     ## Press Enter ##
 - Dropping test database...
 ... Success!
 - Removing privileges on test database...
 ... Success!
Reloading the privilege tables will ensure that all changes made so far
will take effect immediately.

Reload privilege tables now? [Y/n]     ## Press Enter ##
 ... Success!

Cleaning up...

All done!  If you've completed all of the above steps, your MySQL
installation should now be secure.

Thanks for using MySQL!
```

PHP

De su acrónimo (H*ypertext Preprocessor*) es un lguaje de código abierto utilizado para incluir sentencias en html

Para instalar ingresar la siguiente línea de comandos en el terminal:

# yum install php -y

Para crear se debe crear un archivo

“testphp.php” como se indica a continuacion:

```
<html>
<head>
<title>PHPTestScript</title>
</head>
<body>
<?php
phpinfo();
?>
</body>
</html>
```

Y colocar en la carpeta;

# vi /var/www/html/testphp.php

Para reinciar el servicio ingresar:

# service httpd restart