PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

PERFIL DEL TRABAJO PREVIO LA OBTENCION DEL TÍTULO DE:

MASTER EN REDES DE COMUNICACIÓN

TEMA:

"ANÁLISIS E IMPLEMENTACIÓN DE UN SISTEMA INTEGRADO DE GESTIÓN, PARA LA RED DE DATOS DE LA UNIVERSIDAD ESTATAL DE BOLÍVAR MATRIZ, EN SOFTWARE LIBRE."

JAIRO L. RAMOS G.

Quito – 2016

RESUMEN

El presente trabajo de investigación presenta un estudio comparativo e implementación de un Sistema Integrado de Gestión para la red de datos de la Universidad Estatal de Bolívar matriz, en software libre, proyecto que en los diferentes capítulos desarrollados puntualiza las características y beneficios de varios sistemas de gestión. Para el desarrollo del presente proyecto se realizó un análisis criterioso de la arquitectura, funcionalidad y facilidad de configuración de los sistemas integrados de gestión OSSIM, OpenNMS y Hp Open View, los resultados de este estudio sirvieron para determinar la herramienta más adecuada para implementarlo en el Área de Redes del Departamento de Informática de la Universidad Estatal de Bolívar.

La herramienta que se escogió para la fase de implementación por sus beneficios y costos fue OSSIM, misma que al ser instalada en un computador adaptado como servidor, empezó a recolectar la información de los activos conectados a la red de datos de la UEB, así también se configuro de manera manual los servidores que prestan servicios web, mail, plataforma virtual, evaluación y el sistema académico.

En la fase de implementación, la herramienta a través de su consola de monitorización empezó a proporcionar valiosa información para la gestión de activos, también suministro una serie de eventos y alarmas a los que se encontraban expuestos los equipos y los servicios que en ellos se ejecutaban, facilitando la respuesta inmediata por parte del administrador a fin de corregir los fallos presentados.

Finalmente, este sistema integrado cuenta con un sin número de reportes acerca de la información de los activos, eventos generados y soluciones aplicadas por parte del personal técnico, esto a fin de facilitar la toma de decisiones a nivel directivo e implementar políticas acordes a las situaciones adversas presentadas.

ABSTRACT

This research paper presents a comparative study and implementation of an integrated management system for network data from the State University of Bolivar matrix, free software project in the different developed chapter's points out the features and benefits of various systems management. For the development of this project, a judicious analysis of the architecture, functionality and ease of configuration of integrated management systems OSSIM, OpenNMS and HP OpenView was performed, the results of this study were used to determine the most appropriate tool to implement it in the area Computer Networks Department of Bolívar State University.

The tool that was selected for the implementation phase for their benefits and costs was OSSIM, same as when installed on a computer adapted as a server, it started collecting information assets connected to the rad data BSU, well manually configured servers that provide web services, mail, virtual platform, evaluation and academic system.

In the implementation phase, the tool through its monitoring console began providing valuable information for asset management also supply a series of events and alarms to the equipment and services that they were executed were exposed facilitating the immediate response by the administrator to correct the failures presented.

Finally this integrated system has a number of reports about asset information, events generated and solutions applied by the technical staff, this in order to facilitate decision-making at board level and implement policies consistent with adverse situations presented.

Contenido

Índices de figuras

Agradecimiento

Agradezco a todos quienes durante este largo y arduo trabajo supieron apoyarme y guiarme, en primer lugar, a Dios por bendecir mi vida y darme la oportunidad de estar y disfrutar junto a las personas que más me aman, a la Pontificia Universidad Católica del Ecuador, por acogerme en este periodo académico, al Dr. Gustavo Chafla PhD, por su predisposición y apoyo académico antes y durante el desarrollo de la presente Tesis.

Al personal del Departamento de Informática y Comunicación de la Universidad Estatal de Bolívar, por su predisposición y colaboración con mi persona durante el desarrollo del presente proyecto.

A mi Madre quien con su perseverancia y lucha ha sido un ejemplo a seguir en mi vida, a mi hermano por su apoyo incondicional en los momentos más difíciles, a mi amada esposa Natalia por su incansable afán de alentarme, apoyarme y creer en mí y sin duda a mi gran amigo Roberto y a su Esposa, quienes con sus consejos y guía han sido un referente en mi vida personal y profesional.

Dedicatoria

El presente trabajo de investigación está dedicado a mi familia, quienes con sus consejos y amor han sido un pilar fundamental en mi vida y en el cumplimiento de mis sueños. En lo personal este proyecto está dedicado a mi hijo Miguelito, aunque no estés junto a mí físicamente, tu recuerdo vivirá por siempre en mi mente y corazón

CAPÍTULO I

1 CAPÍTULO 1: PLANTEAMIENTO DEL PROYECTO

1.1 Introducción

Este proyecto de investigación presenta el análisis e implementación de un sistema integrado de gestión en la red de datos de la Universidad Estatal de Bolívar matriz, en software libre. El fin principal es el de proporcionar una herramienta de apoyo que permita al administrador visibilizar todos los eventos adversos que ocurran en tiempo real, de tal manera que se pueda garantizar una red constantemente supervisada, permitiendo así aumentar la capacidad de detección y respuesta priorizando los sucesos según el grado de complejidad en que se producen.

Existen sistemas integrados de gestión propietarias cuyo costo de licenciamiento es muy elevado y otras Open Source con características técnicas limitadas. Este proyecto busca realizar un análisis comparativo de las mejores herramientas presentes en el mercado con el único objetivo de establecer el sistema que mejor se acople a la infraestructura de la UEB.

El Capítulo dos del presente trabajo de investigación en redes de comunicación, detalla los conceptos, así como los trabajos realizados en este campo previamente, esto permitió la comprensión del estado del arte respecto a los sistemas integrados de gestión de red. En el capítulo tres, se describe las características técnicas y funcionalidades que brinda cada sistema integrado de gestión de red, además se presenta un cuadro comparativo con la información citada a fin de determinar el sistema que más se acople a las necesidades del proyecto. Ya en el Capítulo cinco se presenta las conclusiones y recomendaciones, mismas que representa nuestra visión y experiencia presentadas en el transcurso de este proyecto. Al final del documento se encuentra el contenido Bibliográfico, mismo que sustenta el desarrollo de la investigación realizada; así también, en esta sección se detallan los anexos

con fotografías, archivos generados por el sistema e información que no incidió directamente en el desarrollo del proyecto.

1.2 Justificación

Al igual que han crecido en tamaño y capacidades, las redes también han crecido en términos de su importancia para la organización, en muchos casos la red que comprende a Internet, las intranets, correo electrónico, redes de área local (LANs), redes de área extensa (wide area networks, WANs), LANs virtuales (VLANs) y redes inalámbricas son las que sirven de soporte a las aplicaciones y transacciones a donde acceden los usuarios internos y externos para envíar y compartir información, guardando datos de clientes, productos y negocios críticos.

Es esencial garantizar la disponibilidad y la seguridad de la red, pero es bastante difícil administrar eficazmente una sola red en una organización las 24 horas, los siete días de la semana, con transparencia total y con la capacidad para seguir, responder e informar sobre los cambios de desempeño y el estado a lo largo del tiempo. Considerar entonces, cómo crece exponencialmente la complejidad en entornos empresariales distribuidos con varias LANs y WANs, y con la misma necesidad crítica de un desempeño constante. (Douglas R. Mauro y Kevin J. Schmidt, 2005)

Pero ¿Qué es lo que se administra?, pues la respuesta es todo como enrutadores, concentradores y conmutadores, estaciones de trabajo y otros dispositivos conectados a la red a través de agentes de protocolo simple de administración de redes (Simple Network Management Protocol, SNMP) y bases de administración de información (Management Information Bases, MIBs). Aplicaciones de Windows a través de agentes de administración de Windows (WMI), correo electrónico, bases de datos y archivos, cortafuego, filtros de spam y virus, las redes privadas virtuales (VPNs) y las LAN virtuales (VLANs). Si cualquiera de estos elementos falla o está

comprometido de cualquier forma, puede tener consecuencias graves. (Douglas R. Mauro y Kevin J. Schmidt, 2005)

Es aquí donde surge la necesidad de mantener un excelente funcionamiento de la red, que es la misión principal del administrador, por lo que este profesional necesitará un conjunto de herramientas integradas que le permita llevar la correcta gerencia y gestión de la red, campo en el que siempre existen muchos obstáculos que impiden el buen desempeño de los servicios, por lo tanto, el monitoreo tiene que ser una actividad primaria en la gestión de los activos y pasivos de la red de la organización.

Una plataforma de gestión es un conjunto de módulos que ofrecen una serie de servicios para administrar los diferentes componentes de una red, a diferencia de un sistema de monitoreo que únicamente se encarga de monitorear el tráfico y estatus de la red, lo cual es una característica más de un sistema integrado; y, que al existir en el mercado una infinidad de sistemas integrados de administración se hace necesario analizar cada características de las principales herramientas de administración.

La red de datos de la Universidad Estatal de Bolívar desde sus inicios es administrada por el Instituto de Tecnologías de la Información y Comunicación, cuyo Director menciona que la red se encuentra en constante crecimiento y que al no contar con una gestión centralizada no se pueden diagnosticar correctamente los problemas presentados, tal es así que la caída de servidores por el aumento de tráfico o servicios fuera de línea a causa de algún evento adverso, tardan entre dos o tres días en solucionarse, estas deficiencias hacen necesario la implementación de un sistema de gestión y monitoreo, por lo que este proyecto propone realizar un estudio comparativo de soluciones integradas de gestión de red, para así seleccionar el software más funcional y adaptarlo

a las necesidades e infraestructura de la red académica, a fin de disminuir el tiempo de diagnóstico, atención y solución de incidentes garantizando un funcionamiento fluido de la red.

1.3 Antecedentes

La gestión de redes abarca hoy en día muchos aspectos, que pueden resumirse o sintetizarse en tareas de "despliegue, integración y coordinación del hardware, software y los elementos humanos para monitorizar, probar, sondear, configurar, analizar, evaluar y controlar los recursos "de una red para conseguir niveles de trabajo y de servicio adecuados a los objetivos de una instalación y de una organización. (FUNIBER, 2017)

Actualmente existen en el mercado herramientas de monitoreo como CACTI, ZABBIX, NTOP, NAGIOS, cuya esencia fundamental es el de monitorizar y registrar el estado de varios servicios de red, servidores, y hardware de red. En la nube existen también varios trabajos de investigación realizados en base a la monitorización de servicios de red y servidores, como la de Delgadillo Rivera José Luis y García Ronquillo Leonardo Daniel, quienes basan su estudio en las herramientas anteriormente ya citadas versus Intelligent Management Center (IMC)de 3Com, (Luis & Daniel, 2017). Así también Carlos Andrés Sánchez Izurieta, implementó un sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del Cantón Baños, estudio que se basó en la instalación y configuración del sistema CACTI, (Omar & Andrés, 2016)

Sin embargo, como ya se ha mencionado en párrafos anteriores, la gestión de una red no se reduce simplemente a la actividad de monitoreo, sino también al estar al día con lo que está pasando en la red, ya sea una interrupción inesperada, una degradación del rendimiento o un ataque. Contadas son las herramientas libres o propietario que integren todas estas necesidades en

un solo componente, por lo que su implementación trae consigo altos costos para cualquier organización.

Los aspectos descritos anteriormente, han originado que se realice este estudio, cuya razón principal es el de desarrollar un análisis comparativo de los sistemas de gestión de red libres y propietarios, a fin de determinar en base a sus características y funcionalidad si son equiparables o si uno de estos es mejor que otro.

Finalmente, el resultado del presente proyecto permitirá implementar el sistema integrado de gestión que mejor se adapte a las necesidades de la red de datos de la Universidad Estatal de Bolívar.

1.4 Objetivos

1.4.1 Objetivo General

Analizar e implementar un sistema integrado de gestión, para la red de datos de la Universidad Estatal de Bolívar matriz, en software libre, con la finalidad de evitar pérdidas en los servicios prestados y lograr un adecuado control de la red.

1.4.2 Objetivos Específicos

1. Analizar el estado del arte acerca de los sistemas de gestión de red.
2. Levantar información acerca de la infraestructura de red con que cuenta la Universidad Estatal de Bolívar.
3. Analizar los requisitos técnicos y funcionales de los sistemas de gestión de red que mejor se ajusten al perfil y cumplimiento del proyecto.
4. Realización de un análisis comparativo sobre la base de los requisitos.
5. Ejecución de pruebas e implementación.
6. Elaboración de conclusiones y recomendaciones.

1.5 Estructura de la red de la UEB

La red de datos de la Universidad Estatal de Bolívar está en funcionamiento desde 1993, la misma fue creada con el objetivo de desarrollar una infraestructura basada en tecnologías avanzadas que permita integrar a las facultades, edificios administrativos y biblioteca en todo el campus universitario entre sí y con el resto del mundo, facilitando así el desarrollo de investigación, innovación y educación.

En general el fin de la red de la UEB, es actuar como soporte para el uso compartido de información de carácter educativo, científico y administrativo, además de ser un nexo con el internet.

Actualmente esta red cuenta dentro del campus universitario con siete edificios conectados:

- ✓ Facultad de Ciencias Administrativas Gestión Empresarial e Informática
- ✓ Facultad De Ciencias De La Educación, Sociales, Filosóficas Y Humanísticas
- ✓ Facultad de Ciencias de la Salud y del Ser Humano
- ✓ Facultad De Jurisprudencia Y Ciencias Políticas
- ✓ Facultad de Ciencias Agropecuarias, Recursos Naturales y del Ambiente
- ✓ Edificio Administrativo
- ✓ Biblioteca

La Unidad de Redes y Telecomunicaciones que pertenece al Instituto de Informática, ha trabajado para distribuir la señal de Internet a todas las dependencias universitarias, dentro y fuera del campus, es así que en la Facultad de Ciencias Agropecuarias y Medicina Veterinaria y las extensiones de Chimbo y San Miguel (entidades fuera del campus) cuentan con servicio de Internet por medio de enlaces inalámbricos.

El nodo central está ubicado en el Edificio Administrativo, a donde llega el enlace de fibra del proveedor CEDIA, desde aquí salen varios enlaces de fibra óptica conectando las Facultades del campus, además de varios cables UTP que comunican a los Institutos y Biblioteca General, siempre utilizando el protocolo IPv4 (Internet Protocol version 4).

1.5.1 Distribución de direcciones IP

Desde su creación en la red de la UEB se planteó la utilización del protocolo IPv4 para la comunicación de todos los departamentos que forman el campus central, además con el transcurso del tiempo de fueron implementando varias direcciones públicas para solventar las necesidades propias de la comunidad universitaria, sin que hasta la presente fecha se cuente con una planificación para la implementación del protocolo IPv6.

1.5.2 Direcciones ipv4

Las direcciones IPv4 son asignadas como se detalla en el siguiente cuadro:

DEPENDENCIAS	IP ASIGNADO
Facultad de Ciencias Administrativas Gestión Empresarial e Informática	10.0.3.1
Facultad De Ciencias De La Educación, Sociales, Filosóficas Y Humanísticas	10.0.2.1
Facultad de Ciencias de la Salud y del Ser Humano	10.0..4.1
Facultad De Jurisprudencia Y Ciencias Políticas	10.0.1.1
Facultad de Ciencias Agropecuarias, Recursos Naturales y del Ambiente	
Edificio Administrativo	
Biblioteca	
Servidor Web	190.15.128.205
Servidor Mail	190.15.128.219
Plataforma Virtual	190.15.128.200
Evaluación	190.15.128.213
Sistema Académico	190.15.128.203

La red de datos de la UEB, desde sus inicios no cuenta con una correcta planificación, su implementación se ha realizado acorde a las necesidades de cada Facultad, razón por la cual se carece de cualquier tipo de herramienta para la gestión de la red, inclusive un fallo detectado por los administradores tarda días en ser reparado.

1.5.5 Utilización actual y futura

El principal uso que se da a la red en la actualidad es su utilización para videoconferencias de tipo académico, tanto a nivel local, como a nivel internacional, debido al gran ancho de banda que se maneja en esta institución.

Por otro lado, la red se utiliza para mover grandes cantidades de información cuyo traslado tomaría mucho tiempo a nivel de la Internet comercial; además, la baja latencia también beneficia a la ejecución de escritorios remotos y aplicaciones distribuidas.

Se estima que la utilización de la red en lo que respecta a videoconferencia siga en aumento y que a esto se le sumen tráficos de *streaming* y grandes cantidades de datos para análisis científico.

1.5.6 Necesidad del centro de gestión

Este centro de gestión debe medir constantemente la utilización de la red, su rendimiento y facilitar la detección de problemas. Las herramientas a ser utilizadas es el centro de gestión deben soportar IPv4 e IPv6 siendo el primero el protocolo usado en la UEB.

Por otro lado las computadoras conectadas a la red de la UEB cuentan con diversos sistemas operativos, diferentes distribuciones de Linux y en algunos casos Windows, por ello es necesario la implementación de un sistema que sea multiplataforma; además, si bien es cierto la implementación del centro de gestión es centralizada en un servidor, es imprescindible que cualquier miembro del ITIC pueda acceder a algún tipo de información desde su ubicación; es por ello que se prefiere una interfaz que permita la administración remota.

CAPÍTULO II

2 CAPÍTULO 2: ESTADO DEL ARTE

2.1 Gestión de Redes

La gestión de redes consiste en la monitorización, el sondeo, configuración, evaluación, análisis y control de los recursos de una red para conseguir niveles de trabajo adecuados a los objetivos de una organización; mediante tareas de despliegue, integración y coordinación de hardware, software y elementos humanos. (Ecured, 2016)

Gestión de redes es la planificación, organización, supervisión y control de elementos de comunicaciones para garantizar un nivel de servicio, y de acuerdo a un coste:

- ✓ Se gestiona para garantizar un nivel de servicio a partir de una red o sistemas con recursos limitados. La gestión de red colabora con el incremento de la efectividad, la mejora de la disponibilidad y rendimiento de los elementos del sistema.
- ✓ Gestionar implica realizar una serie de actividades, entre las que destacan actividades de carácter más puntual (planificación de la propia gestión y organización de los recursos materiales y humanos para llevarla a cabo) y la operación o mantenimiento diario (supervisión y control).
- ✓ En cuanto a los recursos a gestionar, no tienen por qué ser sólo recursos de red, sino que también pueden ser servicios y aplicaciones o sistemas finales. Así, según el objeto de la gestión, se puede hablar de gestión de red (centrada en la infraestructura de red), gestión de sistemas (centrada en los sistemas de red), gestión de servicios (centrada en los servicios de red) y gestión de aplicaciones (centrada en las aplicaciones finales).

En la International Telecommnications Union se introduce el concepto de áreas funcionales de la gestión de red, es decir, qué es lo se gestiona de la red. Estas constituyen el modelo FCAPS:

- ✓ **Fault. Gestión de Fallos:** consiste en la monitorización o seguimiento del sistema gestionado con el fin de detectar posibles problemas, y las políticas de actuación en caso de fallo para recuperarse de estos problemas
- ✓ **Configuration. Gestión de Configuración:** incluye todas las tareas que tienen que ver con la recogida de información de la red, modificación del comportamiento de los dispositivos y almacenamiento de la información que determina este comportamiento. Entre estas tareas están el inventariado de la red, control de versiones, salvaguarda y restauración de la configuración de los elementos, modificación de ésta ante la detección de errores o por la necesidad de cambios administrativos, etc.
- ✓ **Accounting Gestión de Contabilidad:** tiene como objetivo medir que se hace de la red y distribuir los costes entre los distintos usuarios de acuerdo con distintas políticas.
- ✓ **Performance Gestión de Prestaciones:** consiste en realizar un seguimiento de la adecuación de la red a su propósito manteniendo la calidad de servicio deseada, mediante la obtención de estadísticas que incluyen para qué se utiliza la red y cómo de eficientemente se está utilizando.
- ✓ **Security. Gestión de Seguridad:** trata de controlar el acceso a los recursos por parte de los distintos usuarios posibles y proteger la información en tránsito. (Casteleiro)

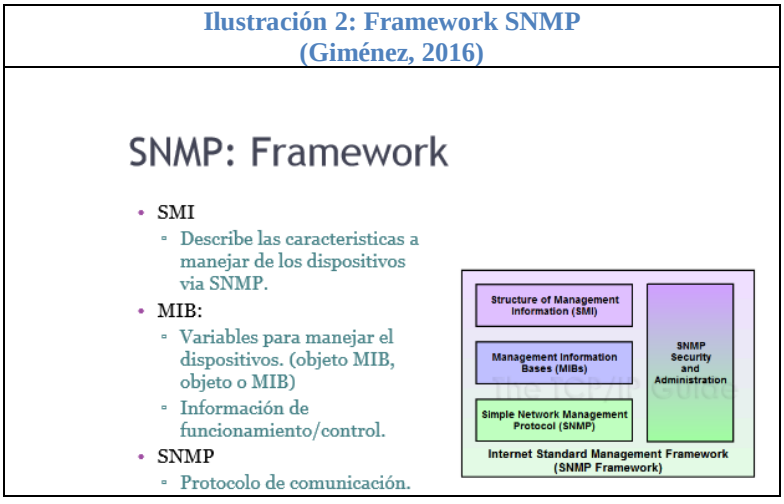
Entre los elementos de la gestión de red se encuentran: los agentes, gestores y un dispositivo administrativo; los cuales se visualizan en el siguiente gráfico. (Molero, 2010).

Ilustración 1: Elementos de la gestión de red.
(Molero, 2010)

2.1.1 Protocolo de Gestión de Redes SNMP

SNMP son las siglas de "Simple Network Management Protocol", es un protocolo que permite realizar la gestión remota de dispositivos. El predecesor de SNMP, SGMP (Simple Gateway Management Protocol) fue diseñado para administrar routers, pero SNMP puede administrar prácticamente cualquier dispositivo, utilizando para ello comandos para obtener información y para modificar la información. Este protocolo ha sido definido por la IETF, para lo cual ha publicado una serie de RFCs.

Ilustración 2: Framework SNMP
(Giménez, 2016)



Actualmente, la versión 3 (SNMPv3) es reconocida como el estándar de la IETF desde el 2004, lo principal en ella es la seguridad, por lo cual este protocolo está diseñado para proveer: Autenticación, Privacidad, Autorización y control de acceso.

Existen dos aspectos a resaltar en lo concerniente a estas versiones, el primero es que todas pueden ser soportadas de manera simultánea, como lo describe el RFC35843. Por otro lado, si bien el RFC1157 que describe el SNMPv1 está ya archivado como histórico, este protocolo es el más utilizado actualmente, a pesar de las falencias de seguridad mencionadas anteriormente. (Ríos, 2016)

2.1.1.1 Arquitectura del sistema SNMP

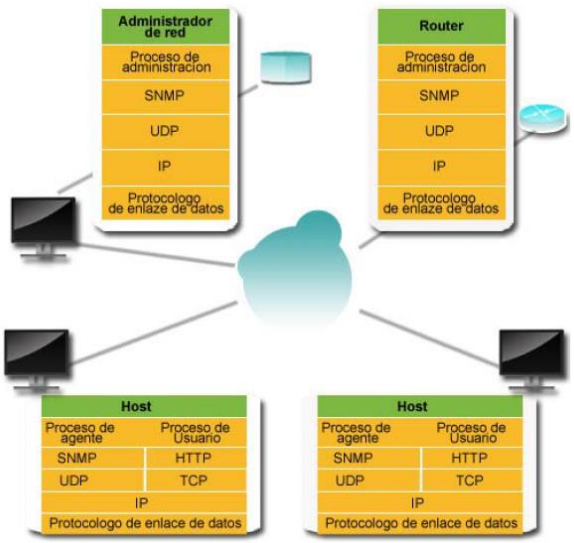
De acuerdo con el RFC 1157, la arquitectura de administración de red basada en SNMP, consta de los siguientes componentes: la estación de administración, agente de administración, base de información de administración (MIB) y protocolo de administración; los cuales se describen en el siguiente cuadro.

Ilustración 3: Elementos de la arquitectura SNMP (Molero, 2010)

Arquitectura	Descripción
Estación de administración	Es la interfaz del administrador de red que contiene un software de gestión de todo el sistema y que mantiene una base de datos llamada MIB (Base de información de administración) con un formato SMI (proporcionado por el lenguaje ASN.1).
Agente de administración	Este agente se encuentra en el dispositivo administrado, tal es el caso de un router, un switch, un computador ó bien puede ser una impresora. Este agente, ejecuta un proceso de envió de información de administración y/o de agente hacia un software de gestión de red provisto por el administrador del sistema.
Base de información de administración (MIB)	Es la base de datos jerárquicos y relacionales, organizada por objetos y sus atributos, que contiene la información que permanentemente envían los agentes de administración. Esta información se maneja a través de un formato llamado ASN.1
Protocolo de administración	Conforman el conjunto de normas que establecen la comunicación entre la estación de administración y los agentes y que ciertamente permiten llenar de datos a la base de información de administración.

En el siguiente gráfico se encuentran representados todos los elementos que intervienen en la arquitectura de SNMP, en ella se menciona al administrador de red que representa a la estación de administración, un router y dos host, que representan los procesos de administración y de agentes sobre estos dispositivos administrados, y finalmente las líneas, que representan los protocolos de comunicación a través de los cuales se hace efectivo el llenado de la MIB central que es la base de datos que recopila toda la información de administración.

Ilustración 4: Estructura del protocolo SNMP (Molero, 2010)



Cabe destacar que esta estructura de componentes, es común para todas las versiones del protocolo SNMP, tal como SNMPv1, SNMPv2 y SNMPv3. (Molero, 2010)

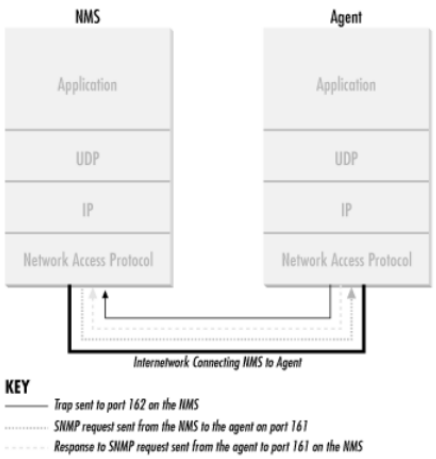
Datagrama SNMP

SNMP utiliza el User Datagram Protocol (UDP) como protocolo de transporte para pasar datos entre administradores y apoderados. UDP, que se define en el RFC 768, fue elegido sobre el Protocolo de Control de Transmisión (TCP), ya que es sin conexión; es decir, sin conexión de extremo a extremo se hace entre el agente y el SMN cuando datagramas (paquetes) se envían de ida y vuelta. Este aspecto de la UDP hace que sea poco fiable, ya que no hay acuse de recibo de datagramas perdidos en el nivel de protocolo. Todo depende de la aplicación SNMP para determinar si se pierden los datagramas y las retransmiten si así lo desea. Esto se consigue normalmente con un tiempo de espera sencillo. El NMS envía una petición de UDP para un agente y espera una respuesta, la longitud de tiempo que el NMS espera, depende de cómo está configurado, si se alcanza el tiempo de espera y el SMN no ha recibido noticias del agente, se

asume que el paquete se pierde y vuelve a transmitir la solicitud. El número de veces que el NMS retransmite los paquetes también se puede configurar.

Una estación administradora es un servidor que, por medio de un programa, realiza la gestión de los dispositivos por medio de comandos y consultas SNMP. El programa que realiza la gestión es denominado NMS (Network Management System). Por otro lado, en los elementos a administrar residen los agentes, que son los que responden los mensajes y realizan las acciones indicadas por el NMS.

Ilustración 5:Modelo de comunicación TCP / IP y SNMP (Douglas R. Mauro y Kevin J. Schmidt, 2001)



La ventaja de la naturaleza poco fiable de UDP es que requiere pocos gastos generales, por lo que el impacto en el rendimiento de su red se reduce. SNMP se ha implementado a través de TCP, pero esto es más por situaciones de caso especial en el que alguien está desarrollando un agente para un pedazo de propiedad de los equipos. (Douglas R. Mauro y Kevin J. Schmidt, 2005)

Asn.1

Abstract Syntax Notation One (notación sintáctica abstracta 1, ASN.1) es una norma para representar datos independientemente de la máquina que se esté usando y sus formas de

representación internas. Es un protocolo de nivel de presentación en el modelo OSI. El protocolo SNMP usa el ASN.1 para representar sus objetos gestionables.

SMI

SMI es sinónimo de estructura de la información administrada y representa la notación por el cual un MIB SNMP debe estar escrito. Otra forma de verlo SMI es que es la gramática para escribir MIB de SNMP. Hay dos tipos de SMI: SMIv1 y SMIv2 con SMIv1 siendo la versión anterior, por supuesto, de nuevo en 1990.

SMIv1 es la antigua notación que nadie debería utilizar más. Sin embargo, todavía hay un montón de SNMP MIBs escrito antes SMIv2 se produjo en 1993. Es por eso que los vendedores y, por tanto, mibDepot, disponen de MIB escritos en SMIv1 y SMIv2. SMIv1 está representado por las siguientes IETF RFC (Request For Comments):

- ✓ RFC 1155 de Estructura e identificación de información de gestión para redes basadas en TCP IP.
- ✓ RFC 1212 MIB Definiciones.
- ✓ RFC 1215 un convenio para la Definición de trampas.

SMIv2 es la nueva notación que se debe utilizar cuando se crea un nuevo MIB, SMIv2 está representado por las siguientes MIB:

- ✓ RFC 2576 para la convivencia entre la versión 1, versión 2 y versión 3.
- ✓ RFC 2578 para la estructura de información de Gestión de versión 2.
- ✓ RFC 2579 de los convenios para SMIv2 textual.
- ✓ RFC 2580 para Declaraciones de conformidad SMIv2.

MIB

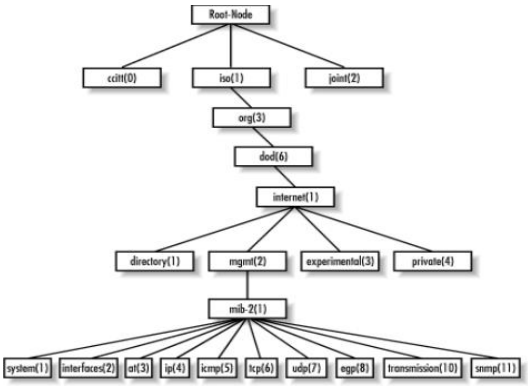
La Base de Información para Gestión (Management Information Base o MIB) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.

Es parte de la gestión de red definida en el modelo OSI, define las variables usadas por el protocolo SNMP para supervisar y controlar los componentes de una red. Está compuesta por una serie de objetos que representan los dispositivos (como enrutadores y conmutadores) en la red. Cada objeto manejado en un MIB tiene un identificador de objeto único e incluye el tipo de objeto (tal como contador, secuencia o indicador), el nivel de acceso (tal como lectura y escritura), restricciones de tamaño, y la información del rango del objeto.

Los formatos del MIB de CMIP y del SNMP se diferencian en estructura y complejidad. Los objetos de una MIB se definen usando un subconjunto del ASN.1, la versión 2 de la estructura de la información de gestión (Structure of Management Information Version 2 o SMIv2) está definida en el RFC 2578.

Los MIB tienen un formato común de modo que aun cuando los dispositivos sean de fabricantes distintos puedan ser administrados con un protocolo muy general. Las MIBs suelen ser modificadas cada cierto tiempo para añadir nuevas funcionalidades, eliminar ambigüedades y arreglar fallos. Estos cambios se han de hacer de acuerdo con la sección 10 del RFC 2578. (Cinvestav, 2016)

Ilustración 6: MIB
(Cinvestav, 2016)



2.2 Gestión Integrada

Históricamente, la gestión de red se ejecuta a través de un conjunto de software aislado, cada uno encargado de gestionar o monitorear un conjunto específico de componentes de la red.

Entonces, la solución a la administración heterogénea son los sistemas de gestión integrado, ya que permite enlazar distintos dispositivos y generar un solo sistema de gestión para toda la red y con una sola interfaz de usuario, esto nos da la posibilidad normalizar las comunicaciones mediante la utilización de protocolos de comunicación entre los elementos de la red y el centro de gestión (SNMP). Otra de sus características se destacan la normalización de la información para la gestión de redes lo que proporciona conectividad entre toda una red. (Andrés, 2017)

2.3 Software Propietario o Comercial

El software propietario se refiere a cualquier programa informático en el que los usuarios tienen limitadas las posibilidades de usarlo, modificarlo o redistribuirlo (con o sin modificaciones), o cuyo código fuente no está disponible o el acceso a éste se encuentra restringido. En el software propietario una persona física o jurídica (compañía, corporación, fundación, etc.) posee los derechos de autor sobre un software negando o no otorgando, al mismo tiempo, los derechos de usar el programa con cualquier propósito; de estudiar cómo funciona el programa y adaptarlo a las

propias necesidades (donde el acceso al código fuente es una condición previa); de distribuir copias; o de mejorar el programa y hacer públicas las mejoras (para esto el acceso al código fuente es un requisito previo). De esta manera, un software sigue siendo propietario aún si el código fuente es hecho público, cuando se mantiene la reserva de derechos sobre el uso, modificación o distribución. (Asociación para el progreso de las comunicaciones, 2017)

La herramienta de gestión integrada comercial más importante es Hp Open View, misma que será analizada más adelante.

2.3.1 Hp Open View

HP Open View es una familia de productos de software con licencia comercial muy amplia y sub-marca de HP Software. Pertenece a Hewlett-Packard Company que es uno de los principales proveedores de soluciones globales existentes en el mercado y que intenta cubrir la mayoría de las problemáticas de administración de los departamentos de TI. Existen herramientas orientadas exclusivamente a la administración del rendimiento y la disponibilidad de los sistemas. Históricamente, el nacimiento de la serie Open View fue con el producto Network Node Manager (NNM), el cual ofrecía servicios de red y GUI para otros productos que se integraban con él. Actualmente NNM se usa generalmente para administrar redes, probablemente en conjunción con otros productos como Cisco Cisco Works. A partir de 2007, tras la adquisición de Mercury Interactive Corp por parte de HP, se elimina Open View y el producto pasa a llamarse HP Operations.

La Suite de herramientas HP Open View permite el control y la gestión de la tecnología en las diferentes áreas de IT: gestión de aplicaciones, disponibilidad de dispositivos, condiciones y estado de la red, rendimiento del sistema, servicio y mantenimiento y programas de almacenamiento. En concreto, con Open View Operations (OVO), los administradores de IT pueden tener un control global desde la consola central que puede gestionar todos los recursos de IT distribuidos por la compañía. Los técnicos de sistemas pueden monitorizar, analizar y planificar recursos en entornos distribuidos, multi-fabricante, y también pueden supervisar el rendimiento de plataformas con herramientas como Open View Perfomance Agent (OVPA), Open View Performance Manager (OVPM) y Open View Performance Insight (OVPI). Cada una de estas tres herramientas, junto con la consola principal (OVO), tiene un objetivo y unas funciones y en conjunto forman la arquitectura de un sistema de monitorización. A continuación, vamos a definir cada una de ellas y sus características.

HP Open View Operations: es la consola central de eventos de HP Open View. Es independiente al resto de herramientas, ya que integra una propia arquitectura consola-agente (paquetes software) para los principales sistemas operativos del mercado y plataformas (Unix: AIX, HP-UX, Solaris, Tru64. Microsoft Windows, Linux, Novell Netware, OpenVMS, AS/400, IBM Mainframe). Existen dos versiones diferenciadas HP Operations Manager para Windows 8.10 y para Unix 8.35.

Los agentes OVO son independientes de la consola central y son un componente de activo instalado en cada equipo para informar a la consola cuando se detecta alguna situación importante, permiten monitorizar ficheros de log, ejecutar programas de control y automatización, capturar eventos SNMP (traps), recolectar métricas de rendimiento de sistema y puede tomar una acción autónoma si dicha métrica realiza un incumplimiento de un umbral, también posee interfaces

abiertas para envió de mensajes. Cualquier alerta creada también puede tener una acción asociada con ellos. Estas acciones por lo general vienen en dos formas, automáticas o iniciadas por un operador. Las acciones automáticas se ejecutarán cada vez que una alerta ocurre, mientras que las iniciadas por un operador requieren la orden explícita para la acción en concreto.

Maneja a los usuarios/operadores en su interfaz Web por privilegios o responsabilidades, lo que permite el filtrado de alarmas que son relevantes para el papel de la persona dentro de la organización, cada usuario de OVO sólo recibe mensajes de los dispositivos de su interés y que pueda tener acceso. Permite crear un mapa lógico de los componentes de la infraestructura, dando a los usuarios una mejor visión del estado de los servicios informáticos. Utiliza tecnologías como Motif en los sistemas Unix o una interfaz gráfica basada en Java para Unix o Microsoft Windows.

Es escalable e integrable, permite el manejo de una gran cantidad de dispositivos y posee integración con los otros módulos de Open View. Maneja los eventos, a los cuales permite asociar acciones, instrucciones, anotaciones y mantener un histórico para consultas y estadísticas.

Permite el empleo de plugins exteriores al núcleo del software SMART Plug-Ins (SPI) para añadir mejoras o aumentar la facilidad para el entorno existente con una rápida implementación. Un ejemplo podría ser SAS 9.2 para servidores empresariales de BI con HP Open View Operations 7.x para Windows para realizar un seguimiento a los datos de negocio y que fluye sin problemas en toda la empresa. También otro ejemplo puede ser PROGNOSIS incorpora beneficios de monitorización, filtrado y alertas en tiempo real y posibilita a los servidores NonStop incluirse en el marco de la gestión de OVO permitiendo una total visibilidad de los servidores y aplicaciones críticas de negocio.

HP Open View Performance Manager (OVPM): Esta herramienta permite visualizar información de rendimiento de los agentes de OVO y OVPA. El acceso a la información es mediante una interfaz Web (existe la posibilidad de un acceso HTML o Java).

HP Open View Performance Agent (OVPA): Es la herramienta que recolecta información de rendimiento de recursos de diferentes plataformas y/o sistemas operativos mediante los agentes OVPA, se instala localmente en cada nodo a monitorizar. A diferencia del agente de OVO, este agente permite la incorporación de nuevas métricas para recolección, configurar parámetros para el almacenamiento de datos y generar alarmas de rendimiento, que pueden integrarse a la consola de eventos de NNM y OVO.

HP Open View Performance Insight Manager (PIM): Es la herramienta que realiza los reportes de HP Open View. Permite extraer información de diferentes fuentes y protocolos (SNMP, RMON2, SQL, archivos ASCII, agentes OVO y OVPA). Posee mecanismos para definir la recolección de datos, almacenarlos en una base de datos relacional y desarrollar informes en base a estos datos. Fue comprada por HP y adapta para ser usada con los otros módulos de Open View.

Las alarmas activas son visibles en la consola de operaciones de Operation Manager en toda la infraestructura, así como el estado de los servicios que hayamos configurado. (Caballero, 2017)

Ventajas:

- ✓ Es una herramienta potente para gestionar una infraestructura IT si se combina o integra con otros productos la gama openview ya sean herramientas de ticketing (HP ServiceDesk o ServiceManager) de forma que al llegar una incidencia a la consola de OVO automáticamente se abra un tiquet para el grupo de TI interesado/afectado. También la

integración de reportes (HP Performance Manager, HP Reporter) o herramientas complementarias de monitorización (HP Network Node Manager – NNM) o monitorización sin agentes (HP SiteScope). Y, por último y quizás más recomendable la integración con los plugins SPI (Smart PlugIns) que facilitan la labor de configurar una monitorización, ya que son paquetes que llevan configurados la forma de monitorizar multitud de plataformas. (BEA, BMC, BlackBerry, Oracle, IBM WebSphere, VMWare, Unix SO, etc). (Caballero, 2017)

Inconvenientes:

- ✓ No es un producto de software libre y presenta varias desventajas, como por ejemplo el precio de la licencia, la cual tiene un precio prohibitivo para la mayoría de las empresas. Se le debe sumar un coste extra por cada agente que se desee instalar. También la poca documentación o información que hay disponible por parte del fabricante, en general la privatización de la empresa impide conocer aspectos de sus productos e incluso puede afectar al trato con los clientes de forma negativa. Podemos ver un precio estimado para el software HP Open View Network Node Manager (NNM), aunque este precio varía dependiendo de la versión y del nº de nodos a monitorizar. (Caballero, 2017)

2.4 Software Open Source

El software libre es el 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.

Un programa es software libre si los usuarios tienen las cuatro libertades esenciales:

- ✓ La libertad de ejecutar el programa como se desea, con cualquier propósito (libertad 0).
- ✓ La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera (libertad 1). El acceso al código fuente es una condición necesaria para ello.
- ✓ La libertad de redistribuir copias para ayudar a su prójimo (libertad 2).
- ✓ La libertad de distribuir copias de sus versiones modificadas a terceros (libertad 3). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones, el acceso al código fuente es una condición necesaria para ello. (Mejía, 2001)

En esta sección se presenta un conjunto de herramientas "open source", basándonos en el artículo "Network Management: Open Source Solutions to Proprietary Problems", el problema de la gestión de recursos de los sistemas en general no comprende exclusivamente la administración de redes y el tráfico en ella, ya que los administradores deben asegurar la disponibilidad y fiabilidad de los recursos en general, uso de la red, carga en ésta, etc.

El problema fundamental es tratar de dar atención a todos estos problemas en forma eficiente y segura con un bajo costo, en este contexto varias empresas ofrecen soluciones integradas para el manejo de distintos tipos de recursos, ofreciendo alta performance, correlación de eventos y altos grados de automatismo.

Un problema básico en este tipo de soluciones es el alto precio, razón por la cual surgen soluciones

alternativas que intentan reducir esos costos con herramientas que cumplan con funcionalidades básicas o de iguales características a las soluciones costosas, en este sentido es que surgen herramientas" open source" que enfocan distintos tipos de necesidades, en el caso de gerenciamiento y administración de redes. (Andrés, 2017)

En este acápite se plantea dos de las herramientas de gestión integrada más importantes, así:

- ✓ Open Source SIM
- ✓ Open NMS

2.4.1 Open Source SIM

El proyecto OSSIM consiste en una consola de seguridad central, que permite gestionar y saber el nivel de seguridad (métrica) que tiene la empresa. Se trata de un proyecto Open Source, con lo que todo el mundo puede disfrutar de él sin ningún coste, además de poder colaborar en su código para formar parte de su evolución. OSSIM engloba más de 22 herramientas de seguridad, entre ellas: IDS (Snort), detector de vulnerabilidades (Nessus), firewall (Iptables), detector de sistema operativo (Pof), monitorización en tiempo real y estadísticas (Ntop), detector de anomalías (Rrd), escaneadores (Nmap), y otros.

Todas estas utilidades son las más usadas en su categoría y todas ellas son Open Source, con lo que contamos con un gran número de personas mejorando y actualizando cada una de ellas. Pero además OSSIM no sólo consigue englobar estas herramientas, sino que la fuerza real de OSSIM reside en su motor de correlación antes mencionando, gracias al cual podemos tener una red o varias con millones de alertas de diferentes dispositivos y mediante su potente motor disponer de alarmas reales, sin falsos positivos y de manera centralizada.

Con esto conseguimos que una empresa pueda, no sólo tener un gran número de dispositivos tecnológicos, sino que además sepa en cada momento el nivel de seguridad que tiene

y el que desea tener. Gracias al motor de correlación de OSSIM conseguimos detectar entre otras cosas, virus antes incluso que los propios fabricantes de antivirus, ya que al trabajar de manera centralizada con muchas herramientas, es capaz de detectar anomalías en el funcionamiento de las máquinas, detectando nuevos virus que aún no han sido identificados por nadie. (ECURED, 2017)

OSSIM está compuesto por los siguientes elementos de software:

- ✓ Arpwatch, utilizado para detección de anomalías en direcciones MAC.
- ✓ P0f, utilizado para la identificación pasiva de OS.
- ✓ Pads, utilizado para detectar anomalías en servicios.
- ✓ Openvas, utilizado para la evaluación y correlación cruzada (Sistema de detección de intrusos vs Escaner de Vulnerabilidad)
- ✓ Snort, utilizado como sistema de detección de intrusos (IDS) como también para la correlación cruzada con Nessus.
- ✓ Spade, es un motor de detección de anomalías en paquetes. Utilizado para obtener conocimiento de ataques sin firma.
- ✓ Tcptrack, utilizado para conocer la información de las sesiones, lo cual puede conceder información útil relativa a los ataques.
- ✓ Ntop, el mismo construye una impresionante base de datos con la información de la red, para la detección de anomalías en el comportamiento.
- ✓ Nagios, utilizado para monitorear la disponibilidad de los hosts y servicios.
- ✓ nfSen, visor de flujos de red para la detección de anomalías de red
- ✓ Osiris, es un sistema de detección de intrusos basado en host (HIDS).
- ✓ Snare, colecciona los logs de sistemas Windows.
- ✓ OSSEC, es un sistema de detección de intrusos basado en hosts

- ✓ OSSIM también incluye herramientas desarrolladas específicamente para él, siendo el más importante un motor de correlación con soporte de directivas lógicas e integridad de logs con plugins. (WIKIPEDIA, 2016)

AlientVault creadora de OSSIM, actualmente compite con Intel-McAfee, IBM y HP, entre otras, opera en Europa, EE UU y Latinoamérica. Desde abril de 2010 tiene su sede social en Silicon Valley (California), donde se ha convertido en todo un referente para las *start ups* españolas que deciden cruzar el Atlántico e instalarse allí, según confiesan algunas de ellas. Más allá de la calidad de sus productos, la clave del éxito de AlientVault, según Adara Venture, es haber apostado por un equipo gestor experimentado. La joven empresa fichó a principios de 2012 a Barmak Meftah como consejero delegado y a unas 15 personas más de su equipo todos de HP. (CINCO DÍAS, 2013)

AlienVault ha desarrollado una plataforma que unifica diversas soluciones de seguridad de código abierto para facilitar un sistema de gestión centralizado para todas ellas. Algunos de sus programas, como el OSSIM, se ofrecen gratuitamente y cuentan con 160.000 descargas. Los de pago, que compran bancos, multinacionales e instituciones públicas se venden a partir de 3.600 dólares. Entre sus principales clientes figuran Telefónica, AT&T, Metro Madrid, la Agencia Espacial Europea y la NASA. (ENISA, 2016)

En la página de Alienvault (ALIENVAULT, 2017), se muestran los premios obtenidos por sus productos, así en SC Magazine como ganador del Awards 2016 Europe, en Forbes 2016 como World’s Best Cloud Companies, en Gartner como aplicación visionaria y SIEM ganadora en CYBERSECURITY 2016.

Ventajas:

- ✓ Integra diferentes aplicaciones de seguridad informática reconocidas en este campo.
- ✓ Disminuye los falso positivos y falsos negativos con la ayuda de la correlación automatizada.
- ✓ Permite realizar análisis forenses con los eventos almacenados. (Nuñez, 2008)
- ✓ Tiene soporte de una comunidad abierta mundial que se encuentra en crecimiento constante.

Inconvenientes:

- ✓ Solo se encargan de almacenar los eventos y reportarlos, no realiza ninguna acción para detener los ataques automáticamente. (Nuñez, 2008)

2.4.2 Open NMS

Es una herramienta de monitorización de Software Libre, publicada actualmente bajo la licencia GPL versión 3(GNU Public License), de las más antiguas que existen junto con Nagios y conocida como uno de los padres de este tipo de herramientas, ya que es un proyecto que se inició en 1999 por Steve Giles, Brian Weaver y Luke Rindfuss y su empresa PlatformWorks. Actualmente, la fundación The Order of the Green Polo (OGP) fundada en 2004 para administrar el proyecto, junto a The OpenNMS Group que es otra organización independiente que ofrece servicio y apoyo comercial, son las encargadas del proyecto. Ha sido premiada con varios galardones como, por ejemplo: Inforworld Best of OpenSource Software (BOSSIE), mejor software en la categoría de gestión redes en los años 2009 y 2010 o Best Systems Management

Tool de LinuxWorld en 2005 frente a otros productos, a priori favoritos, como IBM's Tivoli Intelligent Orchestrator y Novell's ZENworks 7 Linux Management.

La última versión de la herramienta disponible estable y en producción es la Versión 19, además siguen desarrollándose nuevas versiones gracias a la comunidad, que le permite seguir ofreciendo nuevas características a su producto, actualmente también trabajan en dos versiones comercial y Enterprise.

Fue diseñado para ofrecer disponibilidad y escalabilidad a decenas de miles de nodos y para ofrecer soluciones a empresas. Para ello, ponen a disposición dos tipos de soporte, el gratuito creado por la comunidad, con una wiki de información, hilos de discusión y bugs o problemas registrados en una instancia de JIRA. En el soporte comercial, incluimos un libro disponible en Amazon en lenguaje alemán por 36,90€, además del soporte profesional de OpenNMS Group, Inc que proporciona información formal a sus clientes e imparte cursos de formación en EEUU.

Es una herramienta diseñada como solución empresarial y que sigue el modelo de telecomunicaciones FCAPS para la gestión de la red. Su nombre es un acrónimo de: fallos, configuración, contabilidad, rendimiento y seguridad. Define la gestión y organización de una red mencionando la importancia de los servicios IT, ya que los empleados y clientes dependen de ellos, de su disponibilidad y rendimiento y de que los problemas puedan ser rápidamente identificados y resueltos o reparados en un tiempo lo más corto posible para evitar caídas del sistema y la consecuente la pérdida de ingresos.

Puede generar eventos y notificaciones o incluso recibirlos de fuentes externas, como por ejemplo, SNMP, syslog o TL/1. Puede procesar 125.000 mensajes de syslog por minuto de forma continua y enviar dichas notificaciones mediante e-mail, XMPP, SMS o a una aplicación de tickets que disponga de comunicación bidireccional como pueden ser JIRA, OTRS, etc. También ofrece

servicios para la gestión de los tiempos de respuesta (SLAs), como pueden ser solicitudes ICMP (ping), visitas a un puerto determinado TCP para comprobar la instancia, aplicaciones web mediante el protocolo HTTP o pruebas de comprobación de ida y vuelta de correo mediante el servicio API MTM (Mail Transport Monitor). Pudiendo generar informes detallados y representaciones gráficas sobre la disponibilidad de dichos servicios y configurar los tiempos de inactividad, a partir de los datos recogidos en la base de datos, lo cual ayuda a identificar los problemas dentro de la red.

Es una herramienta escrita en el lenguaje de programación Java, y por tanto, puede ejecutarse en cualquier plataforma con soporte para una versión de Java SDK 1.5 o superior. También existen paquetes binarios pre compilados para Linux, Windows, Solaris o Mac OS X. Requiere una base de datos PostgreSQL, aunque se está trabajando actualmente para hacer que la base de datos sea independiente de la aplicación con Hibernate, el cual es un proyecto de una librería Java ORM (object-relational mapping) o también conocido como técnica de programación para la conversión de datos en lenguajes de programación orientados a objetos, creando una base de datos de objeto virtual, pudiéndose utilizar dentro del lenguaje de programación. Su función es permitir mapear clases de Java a bases de datos relacionales mediante archivos XML, así como realizar consultas mediante llamadas SQL generadas por la propia herramienta.

Dispone de una interfaz web de usuario construida en Jetty, el cual es un servidor de aplicaciones y contenedor de servlets Java basado en HTTP desarrollado en OpenSource como parte de la fundación Eclipse y es utilizado hoy en día en productos tales como Alfresco, Apache Maven, Ubuntu, JBoss, HP OpenView, etc. También existe una integración con la herramienta de informes de Java JasperReports con el fin de crear informes de alto nivel en PDF, HTML, Microsoft Excel, etc.

Realizan una serie de comparaciones en su sitio web oficial con otros productos, ya que consideran que OpenNMS puede sustituir e incluso mejorar funcionalidades de otras herramientas sin tener una licencia privativa. Es el caso de CA eHealth Perfomance Manager, donde se argumenta que OpenNMS separa en dos demonios distintos la disponibilidad y el rendimiento, y que para la obtención de estos datos puede utilizar protocolos como HTTP(s), JMX, XMP, NSClient, JDBC y WMI entre otros, además de SNMP. También lo comparan con la herramienta HP OpenView Product Family, ya que algunos de los creadores originales de OpenNMS provienen de una compañía que era parte de OpenView, y por tanto, toman algunos conceptos, objetivos y terminologías parecidos aplicándolos a OpenNMS. Aseguran que, aunque no tienen toda la funcionalidad en el núcleo de su producto, pueden implementar el 99% de funcionalidades de HP OpenView gracias a los paquetes adicionales de código abierto (plugins). Por último, The Tivoli Netcool Suite pertenecía a la empresa Micromuse, y posteriormente fue comprado por IBM en el año 2000. Parte de la arquitectura de OpenNMS está inspirada en el producto Netcool OMNIbus, ya que poseen técnicos con experiencia y certificados en Netcool, a diferencia, de que es un producto comercializado con una licencia de software privativa. También se compara con Nagios, que sí es un producto OpenSource, y mencionan una cita que existe en la documentación de Nagios. “Note: Nagios is not designed to be a replacement for a full-blown SNMP management application like HP OpenView or OpenNMS”. Además, consideran que no es una aplicación con la que deban competir, ya que no está estructurada de la misma forma. (Caballero, 2017)

Ventajas:

- ✓ Posee un sistema de notificaciones muy flexible, ya que puede gestionarlas y enviarlas incluso a una herramienta exterior (JIRA, OTRS, etc.) centralizando así todo el mecanismo de procesos ITIL.

- ✓ Soporta y ejecuta plugins diseñados inicialmente para Nagios.
- ✓ Posee una interfaz web como demo para poder visualizar su funcionamiento sin necesidad de instalarlo y tener una idea del producto: demo.opennms.org/. (Caballero, 2017)

Inconvenientes:

- ✓ Sólo puede utilizar como gestor de base de datos PostgreSQL.
- ✓ Posee una puesta a punto para optimizar el rendimiento del sistema que requiere un nivel muy elevado de conocimientos, lo cual conlleva una serie de modificaciones y tunnings en la instalación a nivel de configuración, hardware, base de datos, sistema operativo, etc.
- ✓ Posee una interfaz web que a veces no deja claro la evaluación de los datos mostrados. Tampoco funciona correctamente con algunos navegadores como por ejemplo Mozilla Firefox. (Caballero, 2017)

2.5 Gestión integrada Open Source vs Privativa

Cuando nos enfrentamos a elegir un producto para nuestra empresa nos asaltan una gran cantidad de dudas, una de las más importantes es si debemos decantarnos por una solución Open Source o un proveedor propietario o comercial.

Ante esta pregunta, no hay una respuesta estándar que funcione para todos nosotros, la respuesta correcta la tiene únicamente el giro de nuestra empresa. Para elegir, se debe evaluar introspectivamente nuestras necesidades y encajarlas con las posibilidades que nos ofrecen las soluciones comerciales u Open Source.

Para asegurarnos de hacer la mejor decisión posible a la hora de elegir unos modelos Open Source o comercial se debe cuestionar las siguientes dudas:

¿Cuánto nos va a costar realmente?

Algunos proveedores, especialmente los comerciales o propietarios, son muy opacos con su sistema de precios, lo primero es entender la lista de precios; es importante que nos informemos bien cuál es el coste total de las licencias y del servicio, no solo tenemos que pensar en el ahora. En este punto también es esencial que pensemos que podría pasar en el futuro. ¿Cuánto costaría un upgrade? ¿Podría migrarlo en un futuro?

Es cierto, que las soluciones Open Source son mucho más transparentes en cuanto a sus precios.

¿Es demasiado complejo para nuestro equipo?

Debemos de pensar cómo nuestro equipo puede desenvolverse con el proveedor elegido. ¿Cuál va a ser el coste de aprendizaje? ¿Es fácil la instalación? ¿Es una herramienta intuitiva? La usabilidad de la plataforma es muy importante y también los recursos que podemos conseguir de la misma. Es una buena idea decantarse por un proveedor que tenga una comunidad de usuarios activa, con tutoriales, posts y artículos que ayuden a nuestros arquitectos.

¿Quién nos puede ayudar?

Es esencial prestar atención al soporte que ofrece el proveedor que elijamos. Algunos contarán con un servicio 24/7 y otros solamente nos podrán ayudar durante horas comerciales. Si nuestro negocio nunca para, nuestro soporte tampoco debería.

¿Cuáles son sus funcionalidades? ¿Son flexibles?

Algunos proveedores se quedarán cortos con las funcionalidades que ofrecen. Los proveedores comerciales suelen ganar en este aspecto, aunque algunas soluciones Open Source como OSSIM no tienen nada que envidiarles. De cualquier forma, a la hora de evaluar lo que pueden hacer tenemos que pensar en qué necesitamos-no solo ahora sino también en el futuro.

Es importante que pensemos en la flexibilidad que nos ofrece la solución. Es posible que necesitemos funcionalidades más adelante y que el proveedor que hayamos elegido no las cubra. ¡Eso sería un gran error!

¿Cuáles son las posibilidades de integración con otras soluciones?

Muchas empresas necesitan integrar sistemas heterogéneos, ¿qué facilidades nos ofrecen?; algunas soluciones nos facilitarán conectores o adaptadores que ayuden a tu equipo en la comunicación de sistemas.

Ni todas las empresas privativas, ni todas las empresas Open Source son iguales, entonces sería injusto meterlas en el mismo saco, pero es verdad que suelen contar con patrones similares y muchas coinciden en algunos aspectos. Por esta razón, Kai Wähner en InfoQ, nos ofrece esta tabla comparativa que nos ayuda a tener una idea general de como las soluciones Open Source equiparan a las comerciales a través de la integración otras características. (CHAKRAY, 2016)

Criterio	Propietario	Open Source
Dificultad de uso	Complejas con necesidad de consultores especializados.	Fáciles de usar. Podemos ponerlas en marcha en unos minutos.
Mantenimiento y monitorización	Potentes herramientas internas	Los Open Source no cuentan con herramientas tan avanzadas.
Comunidad	Aunque el soporte de pago de la empresa es muy bueno, no existe una amplia comunidad de usuarios que pueda ayudarnos	Existen grandes comunidades basadas en proyectos Open Source
Soporte	Suelen contar con un soporte 24/7 muy efectivo. Es un buen respaldo para la empresa.	En muchos casos el soporte es 24/7. El respaldo en las Open Source es menor. Lo que tampoco es ningún problema porque suelen ser más fáciles de manejar y las comunidades de usuarios suponen una gran ayuda.
Funcionalidad y flexibilidad	Cuentan con muchísimas funcionalidades. Destacan por ello, pero es verdad que a la hora de hacer cambios es menos flexible ya que dependemos de la empresa privativa para cualquier modificación. También cuentan con altos costes y largos tiempos de espera.	Las soluciones Open Source cuentan con menos funcionalidades, pero en muchas ocasiones son más que las que necesitamos. Los proveedores Open Source desatacan por la flexibilidad que ofrecen: es total.
Costes	Los costes son muchísimo mayores en comparación a las soluciones Open Source, Además, las listas de precios son complejas y opacas.	Suponen una inversión mucho menor y son mucho más transparentes y flexibles con sus políticas de precios. Por norma general, no se tiene sorpresas en los costes de nuestras soluciones Open Source.

CAPÍTULO III

3 CAPÍTULO 3: ANÁLISIS COMPARATIVO DE LOS SISTEMAS INTEGRADOS DE GESTIÓN

3.1 Criterios de análisis

Para proponer una solución que permita analizar e implementar un Sistema Integrado de Gestión de Red, el primer criterio a verificar es la ejecución de las operaciones necesarias para el desempeño de las funciones que realiza. Para esto se debe utilizar una herramienta que pueda integrar los controles de seguridad con los que cuenta la organización y de ser necesario proponer nuevos controles que fortalezcan la seguridad del sistema supervisado, dando prioridad a la función de correlación de eventos y ejecutar esta operación a un nivel que incluya una base de conocimientos, que integre estadísticas, registros de configuración, bases de datos de vulnerabilidades, así como la política de seguridad.

Esta herramienta debe proporcionar información depurada acerca de incidentes de seguridad informática a través de consolas de administración e Interfaces Gráficas de Usuario, que ayudados por adecuados procedimientos de reporte y reacción de incidentes, faciliten la toma de decisiones por parte del personal directivo en lo concerniente al manejo o mitigación de tales incidentes, además de favorecer una reacción eficiente y efectiva a los incidentes de seguridad informática que pudieran impactar sobre la Infraestructura de TI de la organización.

Una característica importante para verificar en las herramientas analizadas es que cumplan con la legislación y estándares nacionales e internacionales vigentes y también sería deseable que proporcionen acceso al código para verificar que en el proceso de integración con tecnologías existentes no afecten. Por todo lo anteriormente mencionado, en el desarrollo de este capítulo se

describirán las características básicas de algunas soluciones que nos ayudarían a implementar un Sistema Integrado de Gestión de Red adecuado a las necesidades de la infraestructura universitaria.

Como punto de partida se describirán algunas herramientas de código abierto y una herramienta propietaria donde el fabricante la presenta en formato appliance. Estas herramientas son:

- ✓ Open Source Security Information Manager (OSSIM).
- ✓ Open NMS
- ✓ HP OpenView

Para poder obtener un mejor criterio de análisis de los sistemas de Gestión de Red propuestos en nuestro proyecto de investigación, vamos a implementar cada uno de estos en un ambiente de prueba, el mismo que está constituido por 20 usuarios los cuales corresponden al área financiera de esta entidad de educación superior.

Los equipos utilizados para esta prueba son los que se describen a continuación:

- ✓ Swicht Cisco Catalyst 2960 Series.
- ✓ Equipo firewall Check Point 1140 NGTP.
- ✓ Router cisco con salida a internet por fibra.
- ✓ Un computador con servicio FTP.
- ✓ Un computador con suite Zimbra 8.0.1, para correo.

Ilustración 7: Firewall	Ilustración 8: Equipos de cómputo

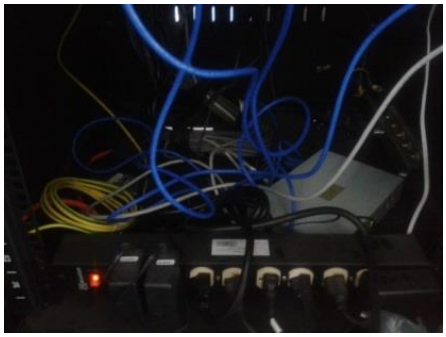
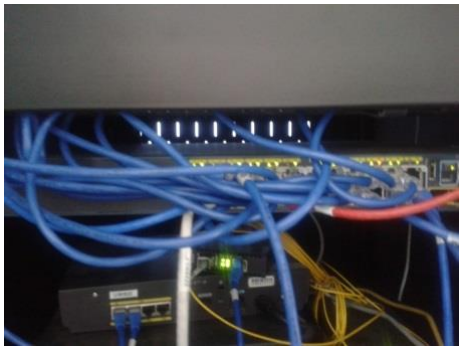



Ilustración 9: Swicht Cisco	
	

3.2 Open Source SIM

OSSIM Alienvault (Open Source Security Information Manager) es un SIEM desarrollado por Dominique Karg y Julio Casal en el año 2000, que implementa la detección y prevención de intrusiones, y la seguridad de redes en general. Este sistema funciona a partir de múltiples herramientas populares de monitoreo y seguridad de código abierto (Open Source), como Nagios, Snort, y otros, gracias a lo cual ofrece grandes capacidades y un alto rendimiento, creando así una inteligencia que traduce, analiza y organiza los datos de una forma única que la mayoría de sistemas SIEM no pueden conseguir, resultando en un diseño que gestiona, organiza y observa riesgos que los administradores pueden apreciar. (Bowling, 2010)

Esta razón los ha convertido en la primera empresa de seguridad gratuita para grandes compañías y sistemas en el mundo, de la que actualmente se descargan 40.000 copias al año, (lo

que representa el 50% de los despliegues de sistemas de seguridad del mundo), compitiendo con las grandes compañías de su negocio como IBM o McAfee. (Árbol, 2010)

Las principales características del OSSIM son:

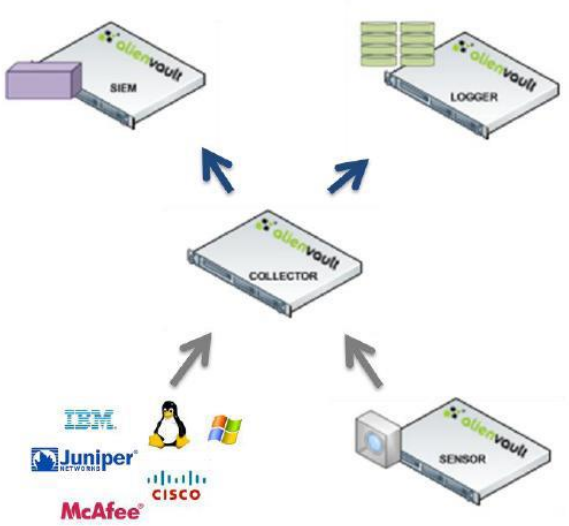
- ✓ Realiza detección a bajo nivel y en tiempo real de la actividad anómala.
- ✓ Análisis de comportamiento de red.
- ✓ Gestión de registros forenses.
- ✓ Realiza análisis del riesgo de seguridad.
- ✓ Presenta informes ejecutivos y técnicos.
- ✓ Arquitectura escalable de alto rendimiento.
- ✓ Es gratuito. (Lorenzo, 2010)

3.2.1 Arquitectura

La arquitectura que maneja OSSIM es muy parecida a la arquitectura de un SIEM descrita anteriormente, OSSIM utiliza 3 elementos básicos y un elemento adicional disponible únicamente para la versión comercial de OSSIM, llamada Alievault Profesional SIEM. (Lorenzo, 2010)

Todos estos componentes son descritos a continuación y se observan en la figura:

Ilustración 10: Arquitectura de OSSIM
(Lorenzo, 2010)



Sensores: son los encargados de recoger una amplia gama de información sobre su entorno local, procesar esta información y coordinar la detección y respuesta con el resto de la red OSSIM. Los sensores están instalados en los segmentos de red y lugares remotos, inspeccionan todo el tráfico, detectan ataques a través de diversos métodos y recolectan información sobre el tipo y forma de ataque sin afectar al rendimiento de la red. (Lorenzo, 2010)

Colectores: Los colectores reúnen los eventos generados por los sensores de OSSIM y cualquier otro sistema externo. Estos colectores clasifican y normalizan los acontecimientos antes de enviarlos al SIEM y al Logger. Con el objetivo de soportar el mayor número posible de aplicaciones y dispositivos, los colectores utilizan los Plugins Collection. Cada conector define cómo se recogen y se normalizan los eventos generados por cada dispositivo. Estos se pueden configurar mediante un archivo de configuración simple, utilizando expresiones regulares para definir el formato de cada tipo de evento. Los colectores pueden ser implementados como un sistema autónomo o ser incluidos en el sensor o dispositivo SIEM, en función de la necesidad de desempeño requerido. (Lorenzo, 2010)

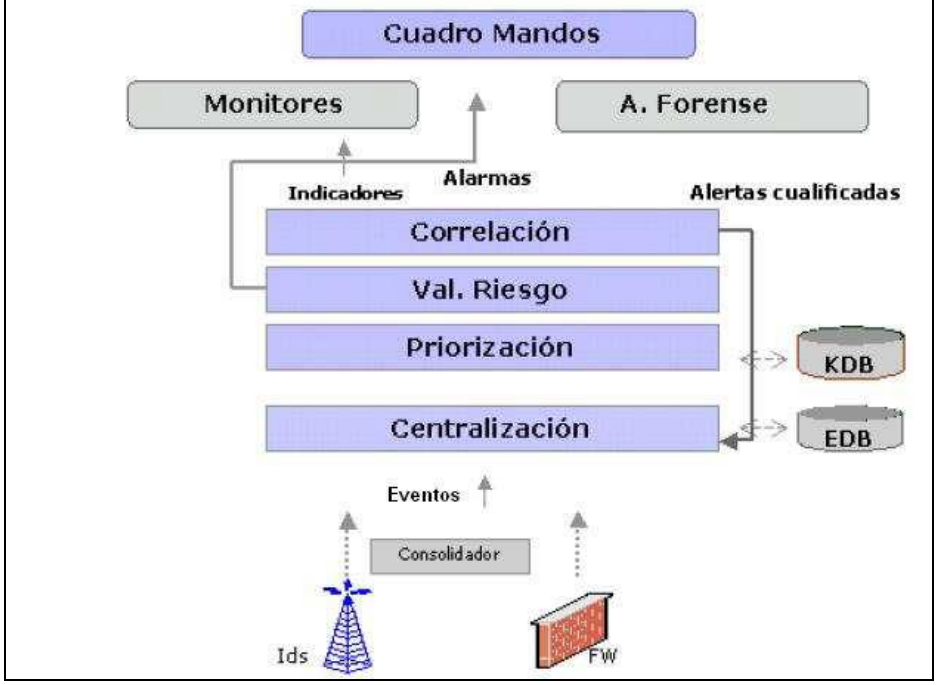
SIEM: El SIEM proporciona inteligencia y capacidades de minería de datos al sistema de seguridad, que incluye evaluación de riesgos, correlación, indicadores de riesgo, análisis de vulnerabilidad y control en tiempo real. Aquí es donde se encuentran los núcleos de reglas y de correlación que proveen la inteligencia al sistema. El SIEM también incluye una base de datos SQL (Structured Query Language) que almacena la información normalizada, lo que permite un análisis profundo de la información y capacidades de minería de datos. El SIEM está diseñado para brindar un alto rendimiento y escalabilidad hasta muchos millones de eventos por día. (Lorenzo, 2010)

Logger: El Logger almacena eventos en formato "crudo" (sin modificar) en un dispositivo de seguridad forense. Los eventos son almacenados en masa y están firmados digitalmente, asegurando su admisibilidad como prueba en un "tribunal de justicia". El Logger permite el almacenamiento de un número ilimitado de eventos con fines forenses y se incluye únicamente para la versión pagada del OSSIM. (Lorenzo, 2010)

3.2.2 Funcionalidad

Para entender que ofrece OSSIM podemos definir la funcionalidad del sistema de una forma gráfica y simplificada con los siguientes niveles:

Ilustración 11: Diagrama de Funcionalidad OSSIM
(AlientVault, 2003)



3.2.2.1 Detectores de Patrones

La mayoría de los detectores clásicos funcionan con patrones, el ejemplo más claro es el IDS o sistema de detección de intrusos, sistema capaz de detectar patrones definidos a través de firmas o reglas.

Existen otra serie de detectores de patrones incluidos en la mayoría de los dispositivos como routers o Firewalls, capaces de detectar por ejemplo escaneo de puertos, intentos de spoofing, o posibles ataques por fragmentación.

Tenemos además detectores para los eventos de seguridad de un sistema operativo, casi todos ellos incluyen su propio logger como el de Unix llamado syslog, siendo capaces de alertar de posibles problemas de seguridad.

En definitiva, cualquier elemento de la red, como un router, un puesto de trabajo, el Firewall, etc., incluye la capacidad de detección en mayor o menor medida, en nuestro sistema nos

interesa recibir los eventos de todos los sistemas críticos para de esta forma obtener uno de nuestros objetivos principales: la visibilidad de la red. (AlientVault, 2003)

3.2.2.2 Detectores de Anomalías

La capacidad de detección de anomalías es más reciente que la de patrones. En este caso al sistema de detección no tenemos que decirle que es bueno o que es malo, él es capaz de "aprender" por sí solo y alertar cuando un comportamiento difiera lo suficiente de lo que ha aprendido como normal.

Esta nueva funcionalidad ofrece un punto de vista diferente y complementario a la detección de patrones pues la naturaleza de los dos procesos es opuesta.

La detección de anomalías puede ser especialmente útil para prevenir por ejemplo ataques perimetrales, estos son en sí una anomalía continua, en la dirección, el sentido de las comunicaciones, y el camino que definen, en el flujo de datos, el tamaño, el tiempo, el horario, el contenido, etc.

Esta técnica ofrece una solución, hasta ahora irresoluble, de control de accesos de usuarios privilegiados como son los ataques internos, por ejemplo, de empleados desleales, los cuales no implican la violación de ninguna política ni la ejecución de ningún exploit. Implican sin embargo una anomalía en el uso y la forma de uso de un servicio.

Veamos otros ejemplos en los que estos detectores serían útiles:

- ✓ Un nuevo ataque del cual no existen todavía firmas podría traspasar los sistemas de detección de patrones, pero producir una anomalía clara.
- ✓ Un gusano que se ha introducido en la organización, un ataque de spamming, o el mismo uso de programas P2P, generarían un número de conexiones anómalas fácilmente detectable.

Se puede detectar así mismo:

- ✓ Usos de servicios anormales por origen y destino.
- ✓ Usos en horario anormal.
- ✓ Exceso en el uso de tráfico o conexiones.
- ✓ Copia anormal de ficheros en la red interna.
- ✓ Cambios en el sistema operativo de una máquina.

Podemos pensar que como efecto negativo estos detectores generarán un número de nuevas alertas, amplificando nuestra señal y empeorando nuestro problema (nuestro objetivo es limitar el número de alertas); sin embargo, si las tomamos como información adicional que acompaña a las clásicas alertas de patrones, permitirá cualificar y por lo tanto diferenciar aquellas que puedan implicar una situación de mayor de riesgo. (AlientVault, 2003)

3.2.2.3 Centralización / Normalización

La normalización y centralización (o agregación) tiene como objetivo unificar en una única consola y formato los eventos de seguridad de todos los sistemas críticos de la organización.

Todos los productos de seguridad poseen normalmente la capacidad de gestión centralizada a través de protocolos estándar, la agregación es por lo tanto sencilla utilizando estos protocolos.

En OSSIM normalmente se intentará no utilizar agentes y utilizar las formas de comunicación naturales de los sistemas.

La normalización implica la existencia de un “parser” o traductor que conozca los tipos y formatos de alertas de los diferentes detectores, se necesita desarrollar un trabajo de organización de la base de datos y adaptación de la Consola Forense para homogenizar el tratamiento y la visualización de todos estos eventos, asi se podrá observar en la misma pantalla y con un mismo formato los eventos de seguridad de un determinado momento, ya sean del Router, el Firewall, del

IDS, o del servidor Unix.

Al tener centralizados en la misma base de datos todo el evento de la red se obtendrá una gran "visibilidad" de lo que ocurre en ella, a partir de ese momento se podrá desarrollar procesos que permitan detectar patrones más complejos y distribuidos. (AlientVault, 2003)

3.2.2.4 Priorización

La prioridad de una alerta debe ser dependiente de la Topología y el Inventario de sistemas de la organización, las razones son bastante claras como muestran estos ejemplos:

a. Si una alerta que se refiere a un ataque al servicio IIS de Microsoft llega a una máquina con sistema operativo Unix y servidor Apache, la alerta debe ser despriorizada.
b. Si existe una conexión sospechosa de un usuario sobre un servidor, el sistema debe:
   - ✓ Darle máxima prioridad si el usuario es externo y ataca a la base de datos de clientes.
   - ✓ Darle prioridad baja si el usuario es interno y ataca a una impresora de red.
   - ✓ Descartarla pues es un usuario que normalmente hace pruebas contra un servidor de desarrollo.

Llamamos priorización al proceso de contextualización, es decir la evaluación de la importancia de una alerta respecto del escenario de nuestra organización. Este escenario está descrito en una base de conocimiento sobre la red del cliente, formada por:

- ✓ Inventario de Máquinas y Redes (identificadores, s. operativo, servicios, etc).
- ✓ Política de Accesos (desde donde a donde está permitido o prohibido).

Para realizar esta tarea (así como la valoración de riesgos explicada en el siguiente apartado) disponemos de un Framework donde se procede a configurar:

- ✓ Política de Seguridad. O valoración de parejas activo-amenazas según la Topología y flujo de los datos.

- ✓ Inventario.
- ✓ Valoración de activos.
- ✓ Valoración de amenazas (priorización de alertas).
- ✓ Valoración de Fiabilidad de cada alerta.
- ✓ Definición de Alarmas.

A través de la cualificación se realizará una de las partes más importante del filtrado de alertas recibidas por los detectores, la cual debe realizarse a través del proceso continuo de tunning y realimentación de la situación de nuestra organización. (AlientVault, 2003)

3.2.3 Valoración del Riesgo

La importancia que debemos dar a un evento debe ser dependiente de estos tres factores:

a. El valor del Activo al que el evento se refiere.
b. La amenaza que representa el evento.
c. La probabilidad de que este evento ocurra.

3.2.3.1 Riesgo Intrínseco

Con ellos construimos la definición clásica de riesgo: el valor del posible impacto de una amenaza sobre un activo ponderado con la probabilidad de que este ocurra.

La valoración de riesgos se ha referido clásicamente a riesgos intrínsecos, o riesgos latentes, es decir riesgos que soporta una organización derivados del hecho de "ser" (los activos que posee para desarrollar su negocio) y "estar" (las amenazas circunstanciales que existen sobre estos activos).

3.2.3.2 Riesgo Instantáneo

En este caso, debido a la capacidad de medir en tiempo real, se puede medir el riesgo asociado a la situación actual, en términos instantáneos.

En este caso el riesgo será medido como la medida ponderada del daño que produciría y la probabilidad de que esté ocurriendo en este momento la amenaza.

Esta probabilidad, derivada de la imperfección de nuestros sensores, no será más que el grado de fiabilidad de estos en la detección de la posible intrusión en curso.

Llamaremos Riesgo Instantáneo a la situación de riesgo producida por la recepción de una alerta, valorada de forma instantánea como la medida ponderada entre el daño que produciría el ataque y la fiabilidad del detector que lo reporta.

OSSIM calculará el Riesgo Instantáneo de cada evento recibido que será la medida objetiva que utilizaremos para valorar la importancia que un evento puede implicar en términos de seguridad, sólo a través de esta medida valoraremos la necesidad de actuar.

Incluiremos en nuestro sistema así mismo un Monitor de Riesgos descrito posteriormente que valorará el riesgo acumulado en el tiempo de redes y grupos de máquinas relacionados en un evento. (AlientVault, 2003)

3.2.4 Correlación

Definimos una función de correlación como un algoritmo que realiza una operación a través de unos datos de entrada y ofrece un dato de salida.

Pensemos en la información recogida por nuestros detectores y monitores como información específica pero parcial, dibujando pequeñas zonas del espectro de toda la información que nos interesaría tener.

Podemos pensar en la capacidad de correlación como la de aprovechar estos sistemas y a través de una nueva capa de proceso llenar otras zonas de ese espectro infinito de toda la información que podría existir de una red.

En contra de esta idea podía intentar instalarse un sistema único con un detector capaz de

localizar toda la información posible de la red, pero para ello necesitaríamos una visibilidad total desde un punto único y una capacidad de almacenamiento y de memoria casi ilimitada.

Los sistemas de correlación son por tanto artificios que suplen la falta de sensibilidad, fiabilidad y la visibilidad limitada de nuestros detectores. (AlientVault, 2003)

3.2.4.1 Entrada y Salida

En nuestra arquitectura de una forma simplificada podemos decir que tenemos dos elementos claramente diferenciados para ofrecer información a nuestras funciones de correlación:

- ✓ Los Monitores. Que nos ofrecerán normalmente indicadores.
- ✓ Los Detectores. Que nos ofrecerán normalmente alertas.

Como salida se obtendrán también uno de estos dos elementos: alertas o indicadores. Nuestras funciones se habrán convertido en nuevos detectores o monitores. (AlientVault, 2003)

3.2.4.2 Monitores. Chequean las siguientes anomalías:

- ✓ **Monitorización de riesgos**. Despliega información obtenida por el algoritmo CALM que mide los niveles de riesgos de compromisos y ataques.
- ✓ **Uso de sesión y control de políticas**. Provee información como número de bytes transmitidos al día, actividad de los usuarios, y monitoreo de sesiones en la red.
- ✓ **Monitor de Paths**. Monitoriza los paths usados en la red por diferentes máquinas. Identificando ataques de varias máquinas (DOS) o identificando mapeo de puertos o redes por medio de protocolos (TCP, ICMP, UDP). (AlientVault, 2003)

3.2.4.3 Consola de Análisis forense

Proporciona acceso a los datos generados y guardados por el colector de eventos. Esta consola es un buscador que opera en la base de datos, permitiendo al administrador analizar

posteriormente los eventos en relación a elementos críticos de la red de una manera centralizada. (AlientVault, 2003)

3.2.4.4 Panel de Control.

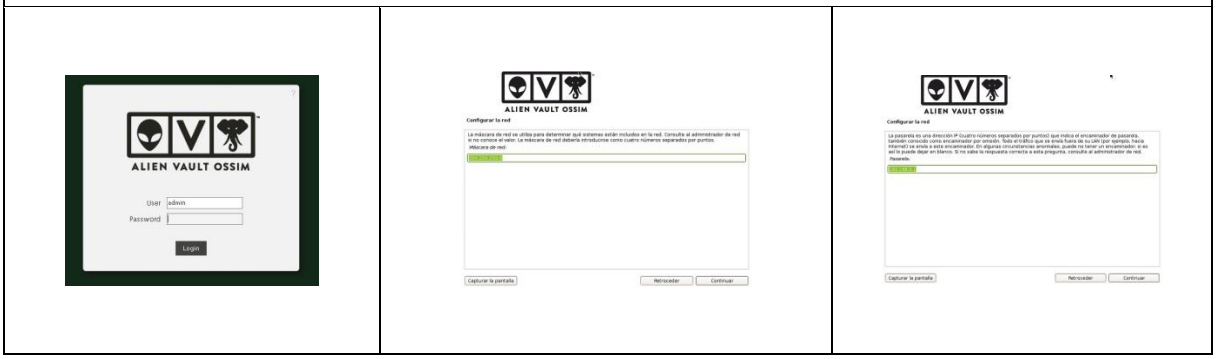
Permite visualizar una situación de seguridad de alto nivel, monitoriza una serie de indicaciones que manejan el estado de la organización en relación a la seguridad. (AlientVault, 2003)

3.2.5 Configuración

OSSIM está desarrollado para correr sobre plataformas Linux y virtuales; sin embargo, para el desarrollo de nuestra investigación se ha optado por la utilización de la imagen disponible en la página oficial de AlientVault, ya que en este sitio recomienda su uso.

Una vez instalado OSSIM, se debe configurarlo con el mayor nivel de detalle posible, ya que cuanta más información se le proporcione, aumentará tanto la fiabilidad como la sensibilidad de las alertas producidas. Para ello este sistema ofrece una interfaz web desde donde se podrá gestionar y visualizar el estado de la red.

Ilustración 12: Pantallas de instalación de OSSIM



3.2.5.1 Inventario de la Red

El inventario de activos y de la estructura de la red, es el primer paso que se debe realizar en la configuración de OSSIM, en donde se detallán todos los equipos conectados a nuestra red y subred.

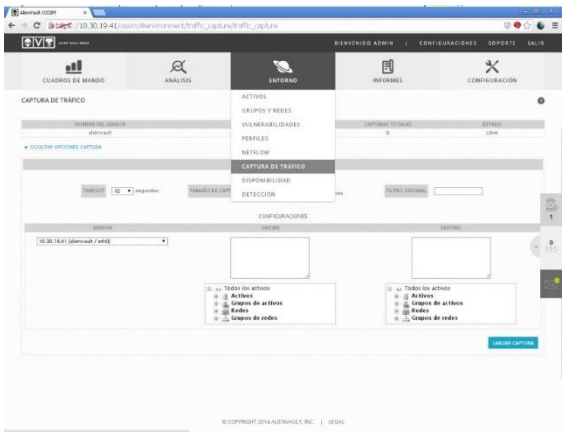
La aplicación NMAP, que viene integrada al sistema nos permitirá a encontrar fácilmente y de manera automatizada los equipos que se encuentren conectados a nuestra red y obtendrá el detalle de servicios y el sistema operativo que se está ejecutando en cada uno de ellos.

Para nuestro caso se ha configurado:

Ilustración 13: Configuración OSSIM

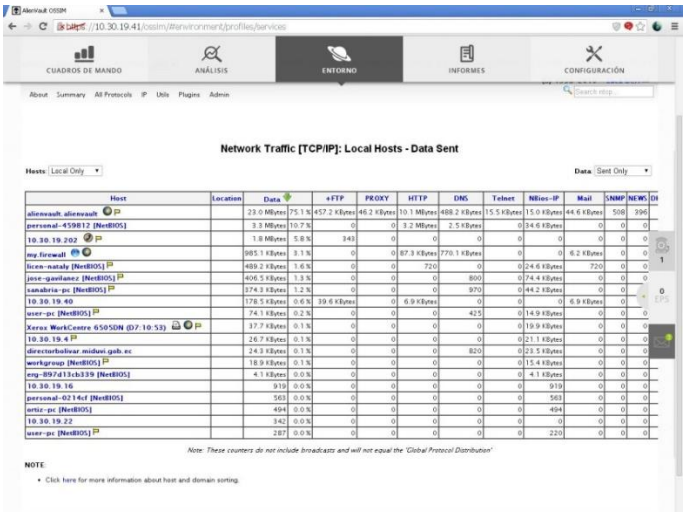
Una vez definidas las redes se debe buscar los activos conectados a cada una de ellas, para lo cual desde la sección herramientas, se utiliza la interfaz de NMAP que se encuentra integrado a OSSIM como ya lo mencionados anteriormente, este script buscará para la red definida los activos y servicios que en esta se ejecutan.

Ilustración 14: Nmap integrado OSSIM



A continuación, se puede visualizar los equipos como resultado de la búsqueda y personalizar la configuración de cada uno de ellos con más detalle, como detallar el umbral de compromiso y ataque permitido para cada dispositivo.

Ilustración 15: Equipos hallados por NMAP

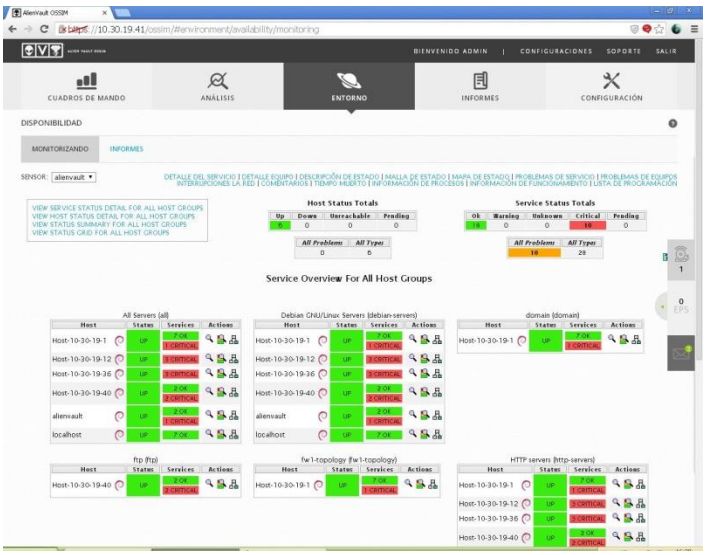


3.2.5.2 Sensores

OSSIM utiliza sensores para recopilar la información de los activos y servicios disponibles en la red, mismos que envían estos datos al servidor para realizar la respectiva colección, estos sensores se encuentran distribuidos por toda la red.

A continuación, se puede observar el detalle de los activos, el estado y los servicios que están levantados o bajados en los servidores.

Ilustración 16 : Sensores OSSIM



3.2.5.3 Puertos

Cuando realizamos el inventario de las máquinas, el sistema detecta los puertos activos en cada una de ellas y utiliza la nomenclatura RFC para describir cada uno de ellos; sin embargo, muchos de estos puertos no están definidos, por lo que realizar un inventario de los puertos utilizados en nuestra red, nos ayudará a tener una visión más rápida y eficaz a la hora de leer las alarmas y eventos.

Desde esta sección se puede visualizar todo los puertos o grupos de puertos inventariados y gestionar el inventario añadiendo, modificando o eliminando los mismos.

Ilustración 17: Puertos OSSIM

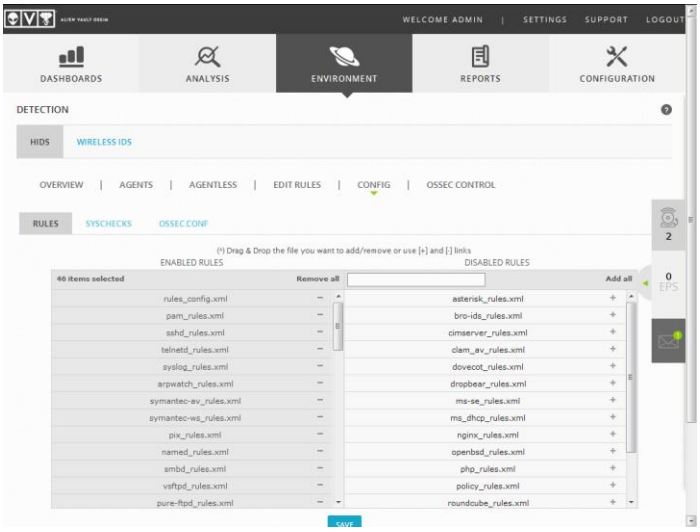
3.2.5.4 Definición de la Política.

Desde aquí se definen las reglas y parámetros que definirán el comportamiento del aplicativo, desde aquí se controla parte de la colección, correlación y priorización de eventos.

Similar a una política de cortafuegos se puede definir lo que se puede hacer y que no, en la red. La política es esencialmente un grupo de ajustes que manejan el comportamiento y seguridad de la red, desde aquí se puede definir qué hacer para ciertos eventos o alarmas con origen y destino conocido.

Esta sección permite ver la política definida y crear nuevas políticas cuando sea necesario.

Ilustración 18 : SIEM



3.2.5.5 Gestión

Una vez configurado OSSIM, la interfaz web de este sistema nos presenta una multitud de opciones para poder visualizar y gestionar el estado de la red. En este separado vamos a detallar cada una de las secciones que nos permitirán realizar una gestión diaria de nuestra red.

Panel de Control.

El cuadro de mandos monitoriza una serie de indicadores que miden el estado de la organización respecto de seguridad, mediante él se puede ofrecer una visión de alto nivel de la situación de nuestra red respecto a seguridad.

Permitirá definir una serie de parámetros u objetivos que se desea se cumplan, estos parámetros podrán ser determinados de forma absoluta o relativa como un grado de anomalía. Se puede asignar el envío de alarmas cuando se superen los parámetros previamente establecidos o la ejecución de cualquier procedimiento automático.

Es importante así mismo la forma de visualización de la información en este cuadro de mandos pues debe ser lo más concisa y simple posible. Para ello se necesita una configuración versátil que muestre únicamente la información relevante en ese momento.

El cuadro de mandos debe ser nuestro termómetro general de todo lo que ocurre en la red. A través de él cada una de las herramientas de monitorización se enlazarán para profundizar sobre cualquier problema localizado. (AlientVault, 2003)

Ilustración 19: Panel de control

Como ejemplo podríamos visualizar los siguientes datos:

- Monitorización permanente de los niveles de riesgo de las principales redes de la organización.
- Monitorización de las máquinas o subredes que superan el umbral de seguridad.
- Monitorización permanente de parámetros generales de red, sistema y niveles de servicio:
    - ✓ Throughput y Tráfico de principales redes.
    - ✓ Recursos de la base de datos principal.
    - ✓ Latencia de Servicios críticos.
    - ✓ Número de transacciones de servicios críticos.
- Monitorización de aquellos parámetros de red o niveles de servicio que superen el umbral establecido:

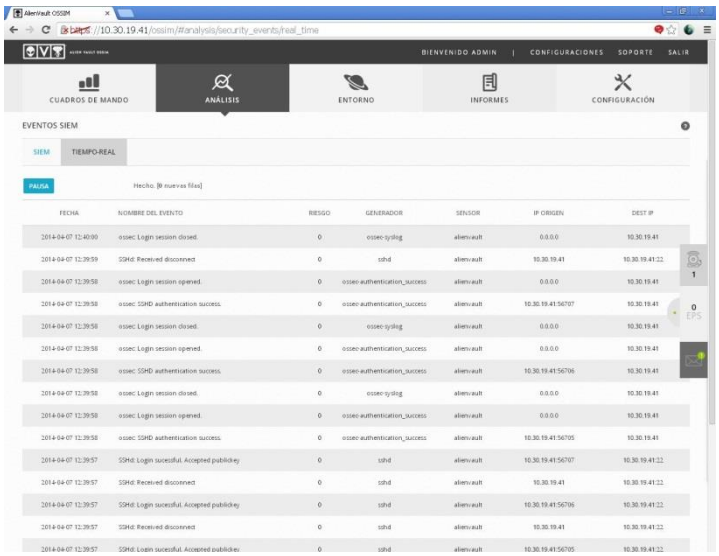
- ✓ Número de correos, virus, accesos externos.
- ✓ Latencia de servicios, uso de tráfico por servicios.

- Monitorización de perfiles que superen los umbrales por:
  - ✓ Uso de tráfico.
  - ✓ Uso de servicios críticos.
  - ✓ Uso de servicios anómalos.
  - ✓ Cambios en configuración.
  - ✓ Cualquier otra anomalía de comportamiento. (AlientVault, 2003)

Alarmas.

Esta opción permite observar a un nivel más detallado todas las alarmas generadas por el sistema, estas alarmas son generadas por los eventos que estén o no correlacionadas y que excedieron algún parámetro configurado como riesgo. Muestra información acerca de cualquier tipo de violación a la red.

Ilustración 20 : Alarmas

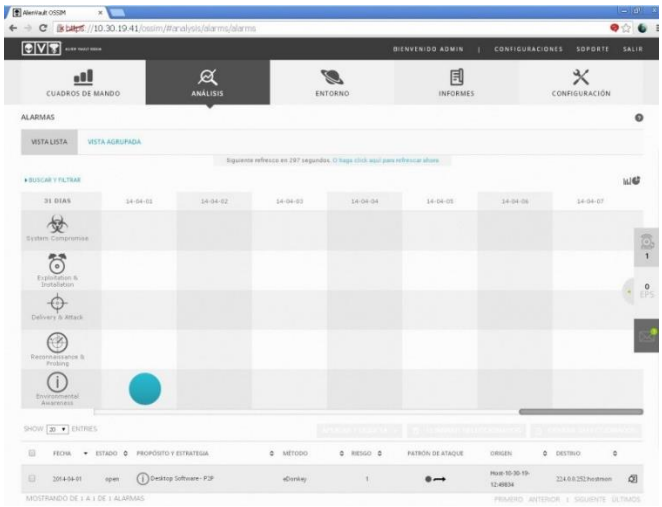


La grafica permite observar las diferentes incidencias presentadas en nuestra red y estas se pueden filtrar por fecha, dirección IP y estado, además visualizará el detalle del incidente y gestionarlo a través de la asignación de un ticket

Incidencias.

La sección de incidencias permite observar el detalle de los incidentes registrados por OSSIM automáticamente o de forma manual, desde aquí el administrador podrá gestionar su cierre, informar vía correo electrónico, o simplemente redactar un informe del procedimiento ejecutado con esta incidencia.

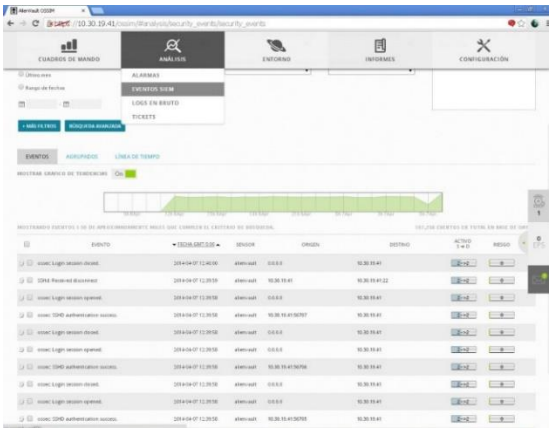
Ilustración 21: Incidencias



Eventos.

Los eventos generados por los diferentes agentes y recolectados por OSSIM son visualizados en esta sección del sistema, datos que servirán para realizar el análisis forense de todas las anomalías e incidentes presentados. Se puede realizar un filtro para solo obtener los eventos relacionados con una alarma, maquina, tipo, etc.

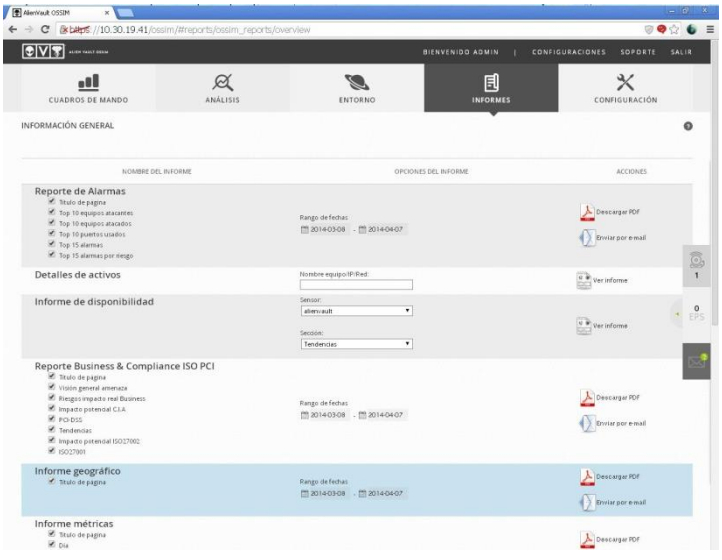
Ilustración 22 : Eventos



Informes.

Esta opción del sistema permite generar y descargar informes en formato PDF, mismo que contiene detalle de las incidencias, tickets generados, acciones emprendidas, etc., mismas que representan el estado en el que se encuentra el estado de la red de la organización.

Ilustración 23: Informes



Configuración.

La sección de configuración, permite realizar cualquier tipo de ajuste que se necesite ejecutar en el sistema como: perfiles de usuarios, actualizaciones, opciones de envió por correo, Backups, etc.

Ilustración 24: Configuración

3.3 Open NMS

OpenNMS (Network Management System) es un sistema que permite una supervisión y gestión de red el cual esta licenciado bajo Licencia Pública General GNU. Es la primera plataforma de grado empresarial en el mundo y galardonada como mejor Sistema de Gestión de Herramientas con varios premios por parte de la comunidad TIC (Tecnologías de la Información y de la Comunicación) debido a que es una alternativa a soluciones de pago como HP OpenView o IBM Tivoli.

Consta de una comunidad que soporta el proyecto como de una organización que se encarga de la parte comercial, es decir servicios, entrenamiento a los usuarios y soporte.

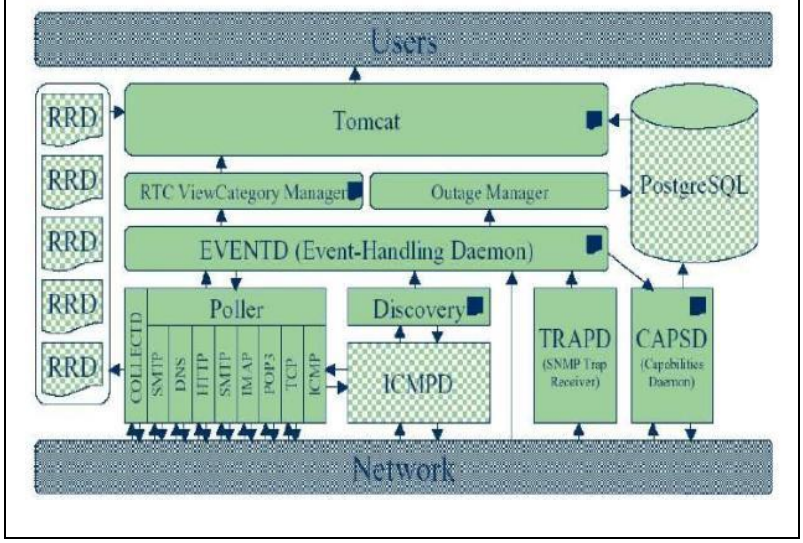
OpenNMS principalmente escrito en Java, se caracteriza por monitorizar servicios, host que corren en la red, proveer de informes y cuadros estadísticos que detallan anomalías producidas; pero su característica principal es correr en forma distribuida y escalonada en un número ilimitado

de dispositivos. Posee funcionalidades de autodescubrimiento de distintos dispositivos conectados a la red. (OpenNMS Group, 2016)

3.3.1 Arquitectura

Usando la Figura (Composición genérica de un NMS) como referencia, se puede analizar paralelamente la composición de referencia y la arquitectura de OpenNMS. La figura siguiente demuestra los componentes que forman OpenNMS.

Ilustración 25: Arquitectura (OpenNMS, 2016)



En el nivel de datos, OpenNMS utiliza PostgreSQL como su RDBMS. En el nivel exterior, utiliza JSP y la tecnología del servlet del Tomcat de Apache Jakarta para proporcionar una interfaz de usuario flexible y adaptable. Está también disponible una interfaz de usuario basada en Perl. Varias utilidades administrativas están escritas en Shell script de UNIX y Perl. OpenNMS utiliza un conjunto de tareas concurrentes de Java que corresponden a la supervisión, administración, monitoreo y al componente del control en la figura para proporcionar esta funcionalidad. (OpenNMS, 2016)

3.3.2 Funcionalidad

Entre las funcionalidades de OpenNMS se puede destacar que es una herramienta capaz de autodescrubrir los servicios en la red en la cual está funcionando, de forma que un proceso actúa automáticamente mediante una lista o rango de direcciones IP. Se puede utilizar la interfaz web de usuario o crear archivos personalizables de configuración en XML para dicha tarea. El aprovisionamiento de los procesos es asíncrono para la escalabilidad, y existen redes de suministro con más de 50.000 dispositivos conectados.

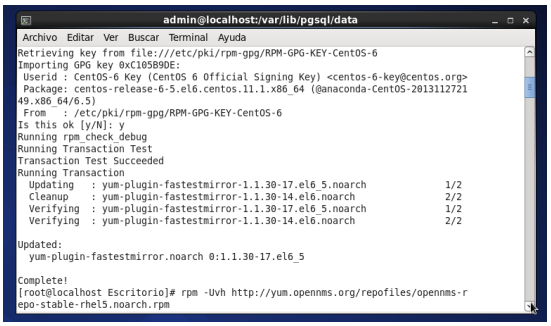
Puede generar eventos y notificaciones o incluso recibirlos de fuentes externas, como por ejemplo, SNMP, syslog o TL/1. Puede procesar 125.000 mensajes de syslog por minuto de forma continua y enviar dichas notificaciones mediante e-mail, XMPP, SMS o a una aplicación de tickets que disponga de comunicación bidireccional como pueden ser JIRA, OTRS, etc. También ofrece servicios para la gestión de los tiempos de respuesta (SLAs), como pueden ser solicitudes ICMP (ping), visitas a un puerto determinado TCP para comprobar la instancia, aplicaciones web mediante el protocolo HTTP o pruebas de comprobación de ida y vuelta de correo mediante el servicio API MTM (Mail Transport Monitor). Pudiendo generar informes detallados y representaciones gráficas sobre la disponibilidad de dichos servicios y configurar los tiempos de inactividad, a partir de los datos recogidos en la base de datos, lo cual ayuda a identificar los problemas dentro de la red. (OpenNMS, 2016)

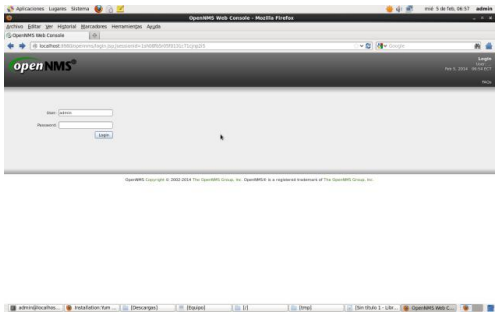
3.3.3 Configuración

La instalación de OpenNMS se la realizó sobre el sistema operativo Centos 6.0 y toda la configuración está almacenada en archivos XML que se encuentra dentro de un directorio dentro de la raíz, muchas de estas configuraciones también se las puede encontrar en la interface gráfica,

las mismas que incluyen los tiempos de barrido, mapeado de traps del tipo eventos/alarmas, gestión de MIBs, etc.

Ilustración 28: Instalación y Configuración





3.3.4 Descubrimiento de la Red

Dado un rango de direcciones, OpenNMS puede descubrir por sí mismo los elementos y servicios dentro de una red. Automáticamente asocia puertos con nodos. La nomenclatura por defecto de un nodo en la base de datos se rellenará con el nombre del dispositivo detectado por un escaneo SNMP del dispositivo.

El proceso responsable de la tarea de detectar los servicios es Capsd y es capaz de detectar los siguientes servicios:

Citrix	Microsoft Exchange
DHCP	MX4J
DNS	Notes HTTP
Domino IIOP	NSClient (Nagios Agent)
FTP	NRPE (Nagios Remote Plugin Executor)
General Purpose (script based)	NTP
HTTP	POP3
HTTPS	Radius
ICMP	SMB
IMAP	SMTP
JBOSS (JMX)	SNMP
JDBC	SSH
JDBC Stored Procedure	TCP
JSR160	Windows Services (SNMP-based)
K5	LDAP

Es posible importar la configuración de los servicios con un fichero tipo XML. Esta configuración deshabilitará los procesos de descubrimiento por medio de barridos ping. El proceso Capsd es el responsable de descubrir todos los servicios a monitorizar sobre un dispositivo. Recopila y almacena datos de diversas fuentes, incluyendo SNMP, JMX, HTTP y NSClient.

Si el dispositivo tiene implementado SMNP, entonces es capaz de manejar todos los servicios interrogando y registrando los tiempos de respuesta utilizando transacciones sintéticas. (Monteverde, 2013)

Ilustración 26: Descubrimiento de red

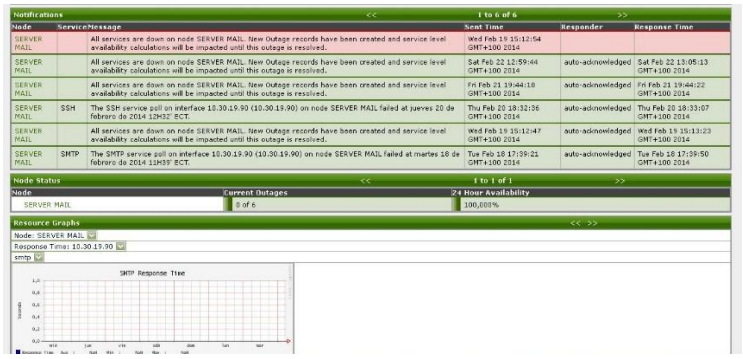
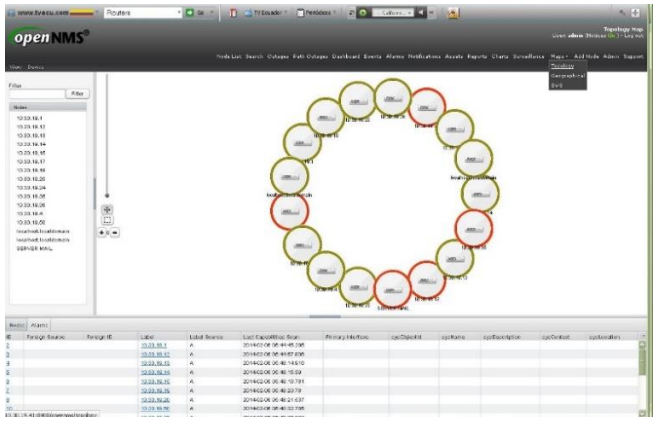


Ilustración 27: Descubrimiento de red



3.3.5 Configuración de Interfaces

También se pueden utilizar archivos XML conteniendo la configuración de las interfaces y así modificar el nombre y el inventario de la Red. Como ejemplo comentar que esta interfaz la utiliza Swisscom para sincronizar OpenNMS con su red WIFI Europea de Hotspots. (Monteverde, 2013)

Ilustración 28: Configuración de interfaces

3.3.6 Gestión

3.3.6.1 Recolección de Eventos

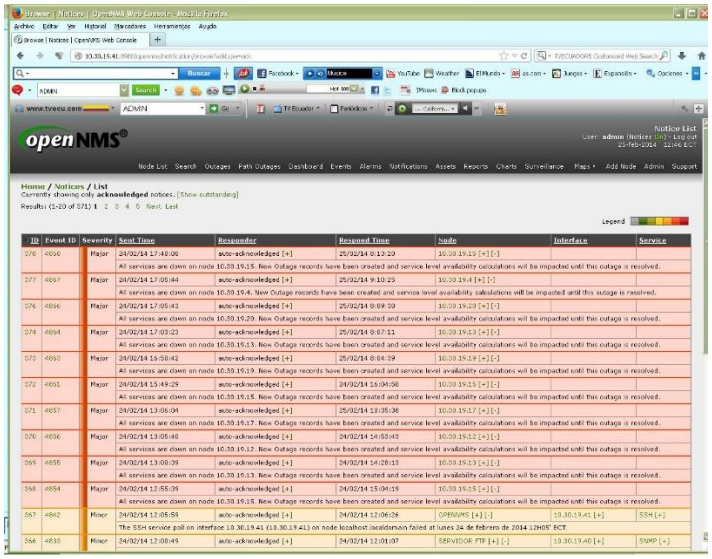
OpenNMS puede registrar todo tipo de eventos ocurridos: Trigers, evaluación de eventos, automatización de acciones en función del procesado de la tabla de alarmas.

Los Nodos Pasivos se utilizan para representar servicios o recursos gestionados por otro agente. Existen dos procesos llamados Event Translator y Pasive Status que permiten a los eventos mapearse a estos nodos. (Monteverde, 2013)

El proceso Actiond se utiliza para generar acciones Java basados en la recepción de eventos. También se pueden enviar los eventos que se deseen via XML-RPC a otro sistema de gestión remoto.

Los eventos se controlan con el proceso Eventd el cual recibe y graba toda la información. Este proceso escucha el puerto 5817 por el cual los demás procesos envían peticiones e incluso se pueden enviar desde sistemas externos a OpenNMS. (Monteverde, 2013)

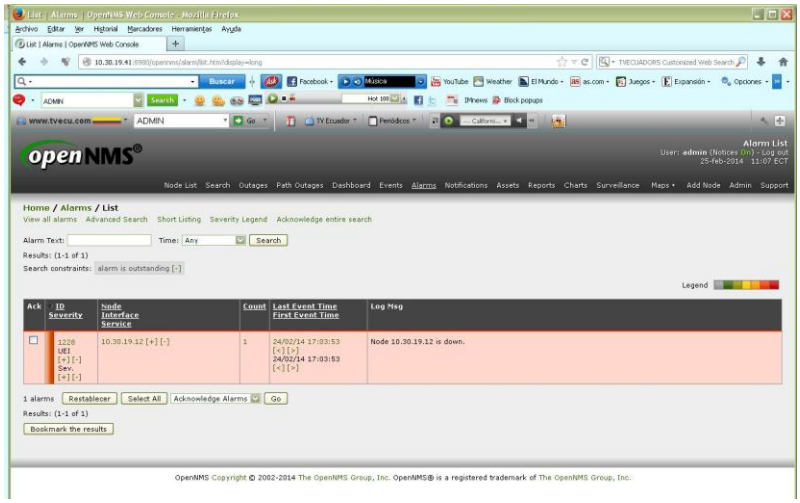
Ilustración 29: Recolección de eventos



3.3.6.2 Correlación de Alarmas

Se utiliza un mecanismo de Alarma para manejar traps de recolección de alarmas o traps de anulación de alarmas en un entorno de gestión de alarmas cíclico. Cuando se recibe por primera vez un trap o disparo se recoge una alarma. Si se reciben sucesivos traps, éstos se contarán en la misma alarma. Si se reconoce la alarma, se provocará un trap de limpieza de la alarma y ésta desaparecerá quedando el sistema preparado para recibir un nuevo evento. Este mecanismo de utilización es el más simple en un listado de alarmas. El usuario también puede configurar reglas más sofisticadas de tratamiento de eventos de alarmas incluso automatizándolo en función de un sofisticado análisis ya que posee un motor de reglas. (Monteverde, 2013)

Ilustración 30: Corrección de alarmas 1



3.3.6.3 Notificaciones de Usuario y Escalados Programados

Se utiliza un mecanismo de Alarma para manejar traps de recolección de alarmas o traps de anulación de alarmas en un entorno de gestión de alarmas cíclico. Cuando se recibe por primera vez un trap o disparo se recoge una alarma. Si se reciben sucesivos traps, éstos se contarán en la misma alarma. Si se reconoce la alarma, se provocará un trap de limpieza de la alarma y ésta desaparecerá quedando el sistema preparado para recibir un nuevo evento. Este mecanismo de utilización es el más simple en un listado de alarmas. El usuario también puede configurar reglas más sofisticadas de tratamiento de eventos de alarmas incluso automatizándolo en función de un sofisticado análisis ya que posee un motor de reglas.

Ilustración 31: Corrección de alarmas 1

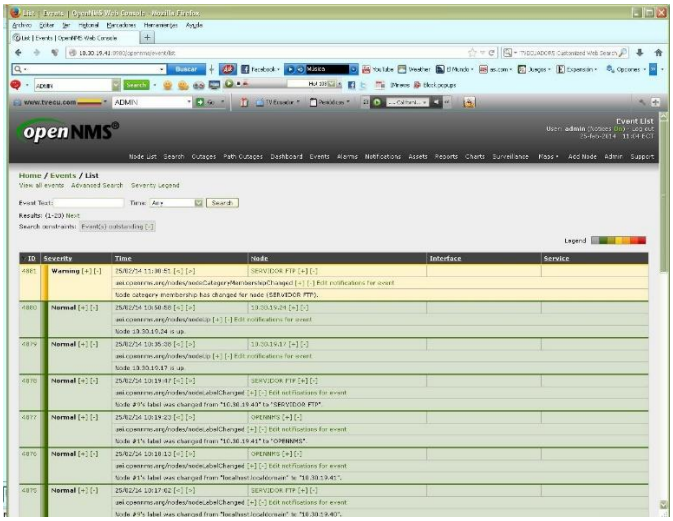
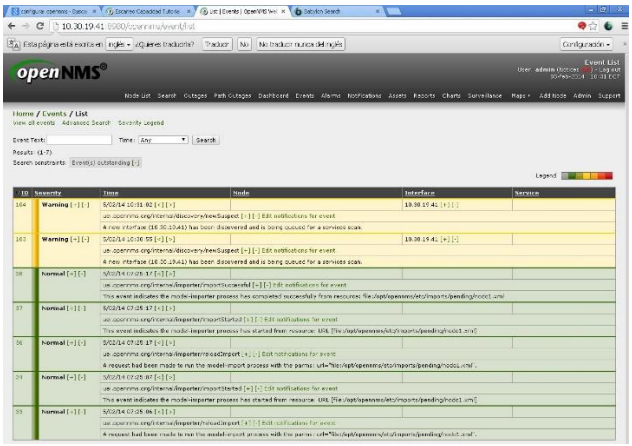


Ilustración 32 : Corrección de alarmas 2



OpenNMS soporta múltiples usuarios y proporciona un mecanismo de Escalado de Notificaciones entre los usuarios. Si se detecta un evento severo, como una alarma Mayor, este mecanismo generará una Notificación que se escalará en el tiempo a través de una lista de usuarios si la alarma no se reconoce en un periodo de tiempo definido por el usuario. El sistema también puede generar un sonido, un email o un mensaje instantáneo para llamar la atención sobre la notificación. También existen mecanismos de notificación tales:

- XMPP: Jabber, un protocolo de mensajería instantánea.

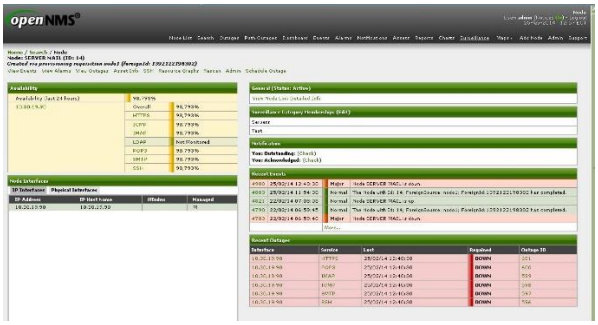
- Programas externos

- Traps SNMPs

- HTTP GET/POST hacia una web site.

Se pueden definir grupos de usuarios y roles a los cuales se les puede asociar cuentas email genéricas.

Ilustración 33: Notificaciones de Usuario y Escalados Programados



Integración de Trouble Tickets

Si el mecanismo de escalado básico no es suficiente, OpenNMS también dispone de una interface Trouble Ticket para integrarlo en el sistema con un número de incidencia. (Monteverde, 2013)

3.3.6.4 Rendimiento y Gestión de recolección de datos

Como en otras herramientas de gestión de redes tales como Nagios o Cricket, OpenNMS almacena datos en ficheros RRD. Se puede utilizar la herramienta RRD para hacer la recolección de datos, pero la librería preferida es JRobin la cual es una implementación Java de RRD.

OpenNMS ya lleva implementada una MIBS (base de datos SMNP) que soporta la gran mayoría de fabricantes de equipamiento, pero los usuarios pueden definir sus propias configuraciones. Las comunidades de usuarios suelen compartir estos trabajos y sus experiencias con los nuevos equipos.

Sin embargo, a diferencia de estas herramientas, toda la programación de la recolección de datos se controla totalmente por un proceso Java dentro de OpenNMS el cual hace que la solución sea muy escalable.

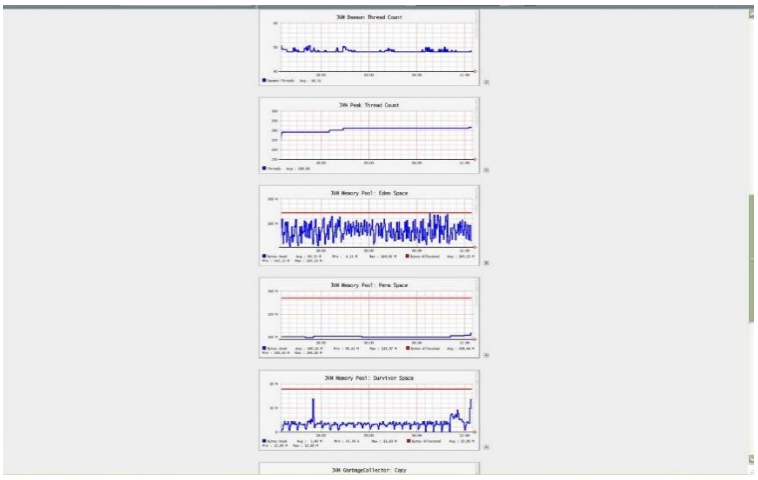
Los datos pueden recogerse desde varias fuentes distintas: sondeo SNMP, traps de gestión, mensajes ASCII tipo syslog, TL1, JMX. También existe una integración con Nagios que permite la utilización de plugins de Nagios. OpenNMS también se ha integrado con SNORT. (Monteverde, 2013)

3.3.6.5 Visualización de Datos

OpenNMS presenta los datos de rendimiento en forma de gráficos. Estos gráficos también se pueden exportar en forma de informes de rendimiento.

También se pueden definir umbrales que generan alarmas cuando hay cambios en los datos. OpenNMS puede realizar transacciones sintéticas para comprobar la disponibilidad de servicios en los nodos. Esto se puede realizar de una manera centralizada o con un conjunto de rollers distribuidos remotamente. (Monteverde, 2013)

Ilustración 34: Visualización de Datos



3.3.6.6 Gestión de SLAs (nivel de servicio esperado)

Se pueden definir umbrales en los SLAs, mimos que generarán una alarma en cuanto se rebasen y pueden escalarse en función de las reglas definidas. A cada punto de recolección de datos de rendimiento se le puede asignar dos umbrales superiores y otro inferior, para evitar los rebotes de alarmas. (Monteverde, 2013)

Ilustración 35: Gestión de SLAs

3.4 HP Open View

Es una familia de productos de software muy amplia, que intenta cubrir la mayoría de las problemáticas de administración de los departamentos de TI; es de uso y distribución comercial, de la familia de productos HP Open View, para efectos de este trabajo, se va a describir HP OpenView Network Node Manager, esta herramienta ofrece una poderosa solución para la administración de redes y sistemas de cómputo.

Es un administrador de información para el protocolo SNMP (Simple Network Management Protocol), posee funciones de monitorización de dispositivos, recolección, almacenamiento y procesamiento de información SNMP, también permite descubrir y configurar mapas de red a nivel de enrutamiento (nivel 3 del modelo OSI).

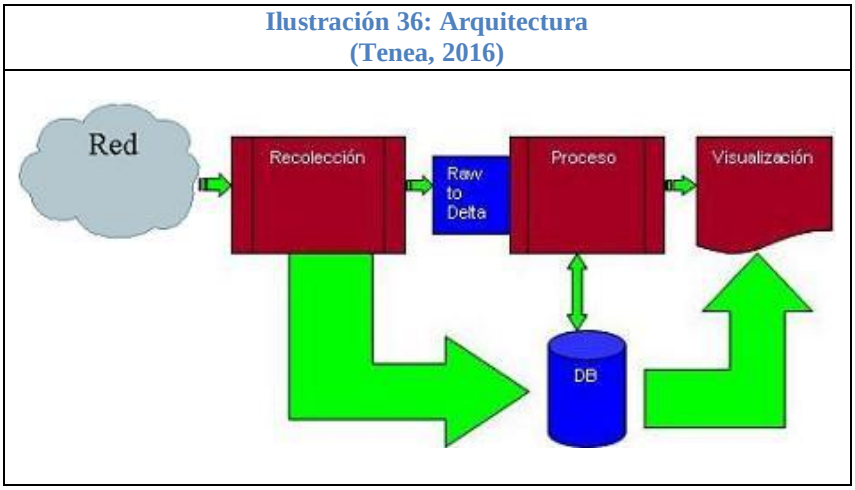
En las últimas versiones incluye funciones para visualizar información de nivel de 2 de la capa OSI, es una herramienta muy reconocida para la administración de redes y la más difundida en el mercado para esta problemática. (Hewllet Packard, 1999)

3.4.1 Arquitectura

La plataforma de gestión de rendimiento recolecta medidas SNMP, no SNMP realizando las siguientes funciones principales:

- ✓ Recolección de medidas: Consiste en el proceso de identificación de elementos de red y la obtención de medidas de métricas consultadas directamente por SNMP o mediante la recolección periódica de ficheros planos (bulk data) procedentes de sistema de gestión de elementos importados Recolección de medidas: Consiste en el proceso de identificación de elementos de red y la obtención periódicamente en la BD repositorio.
- ✓ Procesamiento de datos: Engloba el procesamiento de las medidas recogidas en bruto en datos sumariados en agregaciones horarias, diarias, semanales, mensuales y anuales. También permite realizar la exportación de los datos a aplicaciones externas.
- ✓ Visualización de informes: Engloba la publicación de los datos procesados en informes. (Tenea, 2016)

Ilustración 36: Arquitectura
(Tenea, 2016)



3.4.2 Funcionalidad

Hp Open View Network Node Manager comprende una extensa gama de herramientas que nos permiten controlar los elementos de una red LAN de manera individual, orientándonos a un mejor tiempo de respuesta garantizándonos de esta forma la disponibilidad de la red.

Entre las principales características:

- ✓ Consiste en soluciones dirigidas a diferentes aspectos del proceso.
- ✓ Diseñado para gestionar eficaz y eficientemente una red de equipos de cualquier marca que tengan agentes SNMP.
- ✓ Hp Open View Network Node Manager provee apertura para que aplicaciones específicas de gestión operen de una manera consistente.
- ✓ Nos muestra el estado actual de la red, que dispositivos están presentes y como están configurados, como están comportándose y si algo anda mal.
- ✓ Nos permite identificar tendencias por medio de lo cual se puede optimizar la red, cambiando la configuración o cambiando elementos en la red.
- ✓ Por medio del Hp Open View Network Node Manager se puede establecer umbrales en los dispositivos de red críticos para predecir que puede salir mal y evitar que ocurran problemas mayores (Boza Gaibor, López Potes, & Perugachi Benalcazar)

3.4.3 Configuración

La gestión de configuración está relacionada, por una parte, con la inicialización de la red y la desconexión ordenada de la misma o parte de ella, y por otro lado del mantenimiento, la adición de componentes y la actualización de las relaciones entre los componentes.

Esta función es responsable de encontrar y preparar los dispositivos de la red para poder controlar el comportamiento de ésta. El Hp Open View Network Node Manager nos ayuda a mantener un registro de la información de configuración permitiéndonos lo siguiente:

- ✓ Guardar información de configuraciones críticas tales como routers y switches.
- ✓ Llevar un inventario de los dispositivos de la red. (Boza Gaibor, López Potes, & Perugachi Benalcazar)

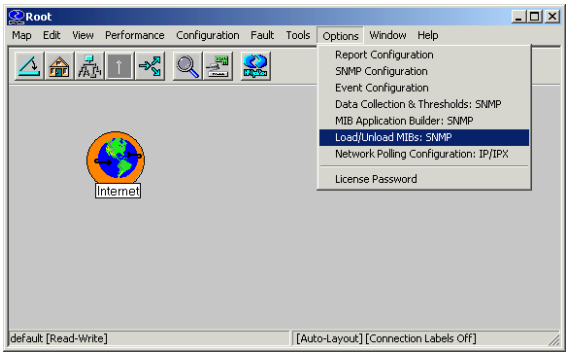
Las siguientes instrucciones se aplican a HP OpenView Network Node Manager versión 6.31, con pequeñas variaciones, las mismas instrucciones deben ser válidas para otras versiones del Gestor de la Red de nodos.

Cargue el archivo de texto SNMP MIB

Un archivo de texto SNMP MIB está incluido en el paquete y se instala como /var/opt/SUNWsymon/cfg/HALAdapterHPOpenview.mib en el servidor host. Copie este archivo desde el host del servidor en el host donde está instalado HP OpenView NNM.

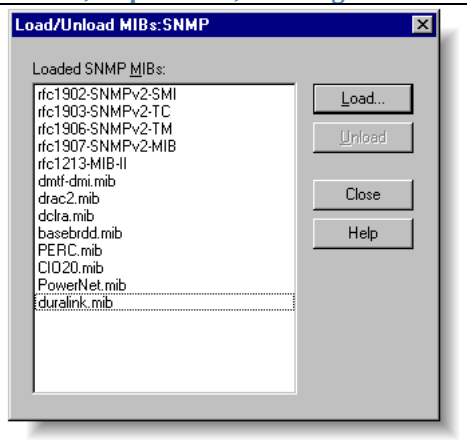
En la consola de NNM, seleccione "Cargar / Descargar MIB: SNMP" en el menú "Opciones".

Ilustración 37: Red Consola Node Manager (Boza Gaibor, López Potes, & Perugachi Benalcazar)



Haga clic en el botón "Cargar ..." en el "/ Carga en Descargar MIB: SNMP" de diálogo.

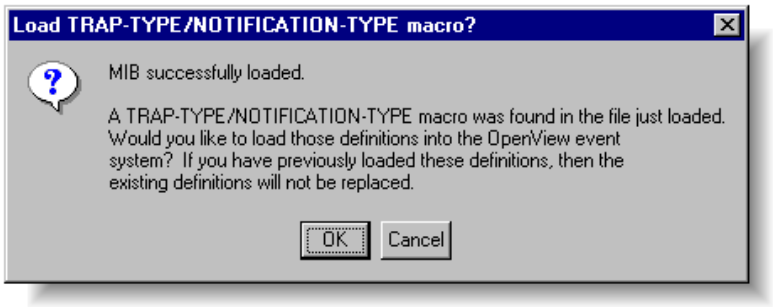
Ilustración 38: Cargar MIB
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



Añadir los tipos de notificación para el sistema de eventos

Cuando se carga el MIB, se le pedirá que añadir los tipos de notificación para el sistema de eventos. Haga clic en "Aceptar".

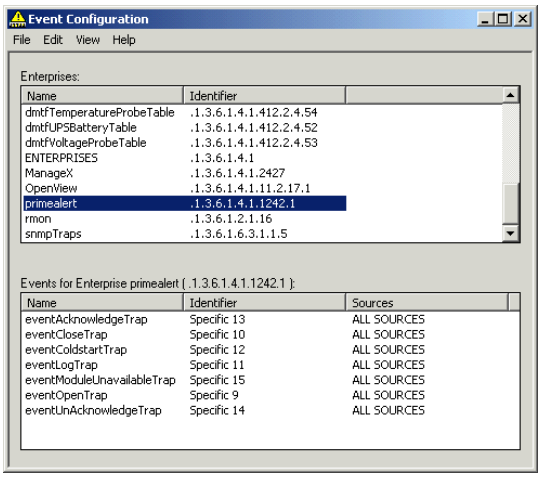
Ilustración 39: Cargar MIB
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



Configure las acciones

En la consola de NNM, seleccione "Configuración de eventos" en el menú "Opciones". Seleccione la empresa "primealert". Los diferentes tipos de trampas deben aparecer en la parte inferior.

Ilustración 40: Ventana de configuración de eventos (Boza Gaibor, López Potes, & Perugachi Benalcazar)

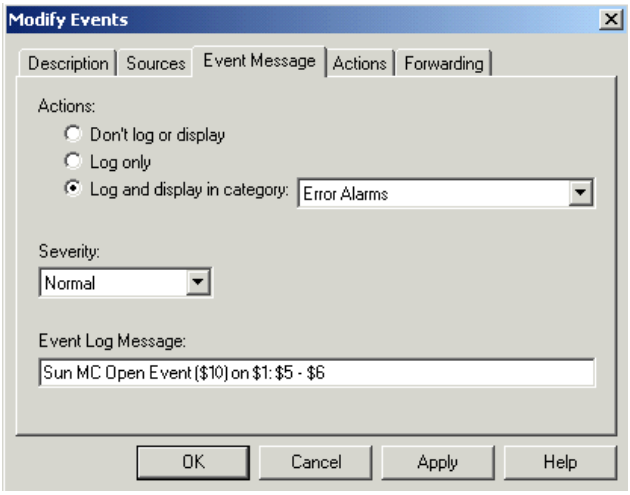


Las acciones ahora se pueden configurar para los tipos de eventos "eventOpenTrap", "eventCloseTrap", "eventLogTrap" y "eventAcknowledgeTrap". Los otros tipos de eventos no han sido reservados para un uso futuro. Este ejemplo muestra cómo conectarse cualquier "eventOpenTrap" para el registro de eventos de HP OpenView y mostrar el mensaje de evento en una ventana emergente.

Haga doble clic en "eventOpenTrap" para lanzar el "Modificar Eventos" de diálogo. En el Mensaje Ficha Evento, seleccione la opción "Registro y visualización en la categoría:" opción y seleccione la categoría "Alarmas de error (o eventos)". Elige la Gravedad "Normal".

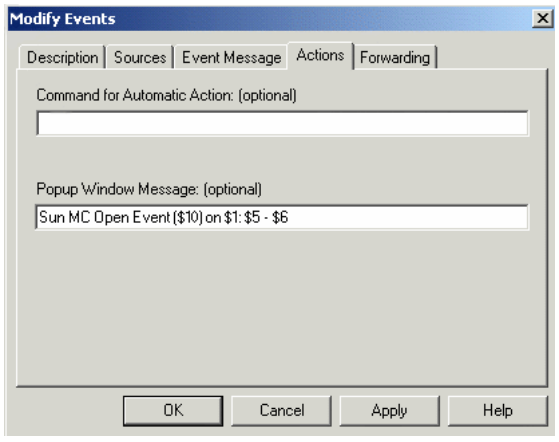
En "Mensaje de registro de sucesos:" escriba el texto: "Sun MC Abrir evento ($ 10) en $ 1: $ 5 - $ 6". Los parámetros de la trampa symonOpenEvent serán sustituidos. "$ 10" es el Sol MC Id Evento del evento fuente. "$ 1" es el nombre de host donde se originó el evento. "$ 5" es el estado de alarma del evento de origen (es decir, 'Crítica'). "$ 6" es el mensaje de estado del evento.

Ilustración 41: Ventana de configuración de eventos (Boza Gaibor, López Potes, & Perugachi Benalcazar)



Seleccione la pestaña "Acciones". Escriba la misma cadena "Sun MC Abrir evento ($ 10) en $ 1: $ 5 - $ 6" bajo "ventana de mensajes emergente". Esto hará que una ventana emergente que contiene los detalles del evento para que aparezca cuando se envía la trampa.

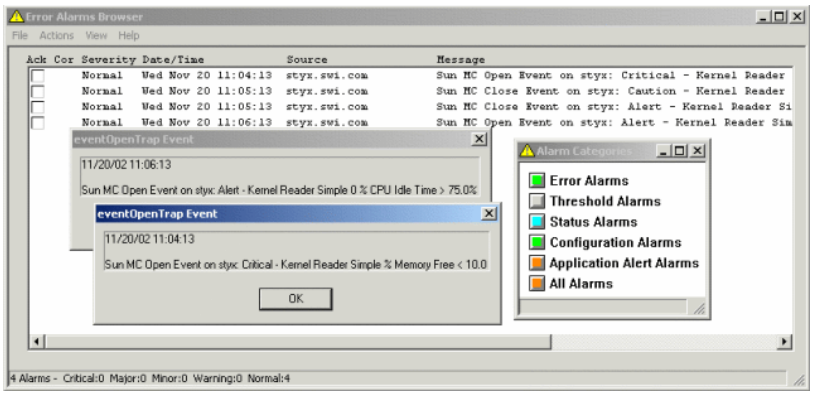
Ilustración 42: Modificar Mensaje Evento (Boza Gaibor, López Potes, & Perugachi Benalcazar)



Seleccione "Aceptar".

"Abiertos" Eventos deberían aparecer ahora tanto en el Visor de registro y en las ventanas emergentes.

Ilustración 43: Modificar Acciones de eventos
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



Puede probar forzando un evento, como por ejemplo mediante la desactivación de un módulo.

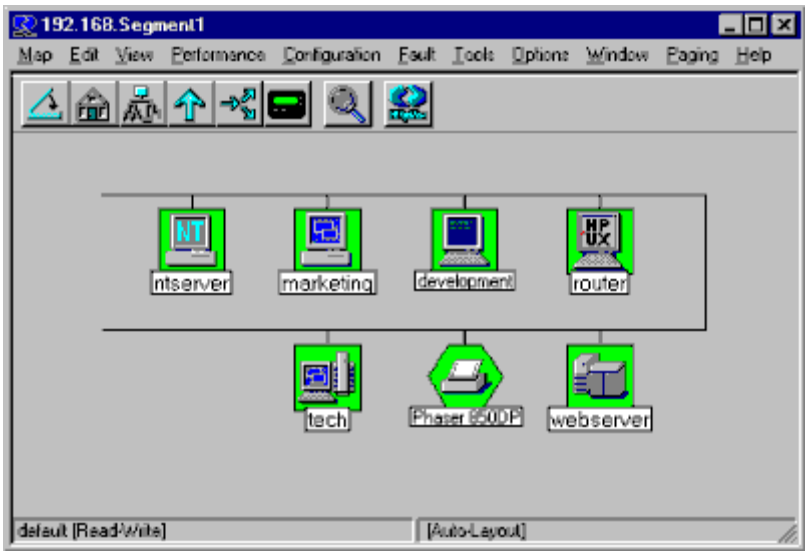
3.4.4 Gestión

3.4.4.1 Método para descubrir dispositivos.

El Servicio Netmon (proceso en background), usa una combinación de peticiones SNMP y de pings ICMP (Internet Control Message Protocol) transmitidos sobre UDP (User Datagram Protocol) e IPX (Internet Packet Exchange) para encontrar los nodos de la red.

Las informaciones sobre los nodos descubiertos se almacenan en la base de datos del Network Node Manager y este la usa para generar automáticamente el mapa de la red. Si Network Node Manager no encuentra el Nodo, se puede mandar un ping ICMP que fuerce su descubrimiento, o se lo puede adherir manualmente.

Ilustración 44: Activos de la Red
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



3.4.4.2 Bases de datos.

Hp OpenView Network Node Manager provee algunas bases de datos diseñadas para almacenar datos específicos y utilizarlos para varios propósitos, incluyendo una base de datos que almacena datos históricos de la red. (Boza Gaibor, López Potes, & Perugachi Benalcazar)

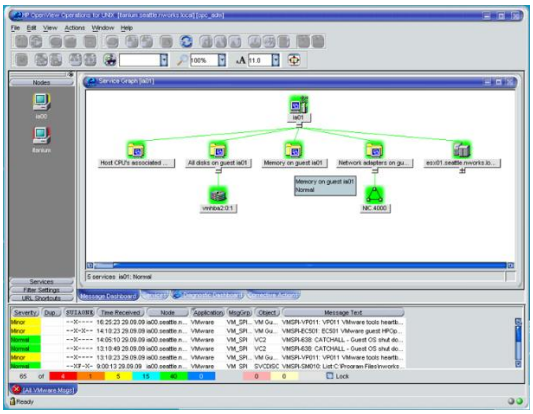
Las bases de datos operacionales son:

- ✓ Base de datos de objetos.
- ✓ Base de datos de mapas.
- ✓ Base de datos de topología.
- ✓ Base de datos de eventos.
- ✓ Base de datos de tendencias.

3.4.4.3 Visualización de mapas.

En el Network Node Manager cuando se ve una parte de la red, entonces se está viendo un submapa. La vista puede representar una visión amplia de la red o un submapa detallado de alguna porción de la red. (Boza Gaibor, López Potes, & Perugachi Benalcazar)

Ilustración 45: Mapa de la Red
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



3.4.4.4 Correlación de eventos.

Network Node Manager incluye el Servicio de Correlación de Eventos (ECS) por sus siglas en inglés, el cual nos ayudará a gestionar una eventual lluvia de eventos y definir relaciones entre los diferentes tipos de eventos. El servicio de correlación de eventos mejora la generación de alarmas suprimiendo las no deseadas y las redundantes, dando prioridad a las más significativas.

Esto produce menos alarmas, pero con mayor información, mostrándonos las relaciones y dependencias entre eventos de la red.

Lo que da como resultado la facilidad para identificar tendencias, aislar eventos importantes y reaccionar rápidamente a los problemas.

El servicio de correlación de eventos procesa eventos basándose en la relación entre eventos individuales, analizando eventos anteriores, actuales o subsecuentes, pudiendo inclusive crear nuevos eventos. (Boza Gaibor, López Potes, & Perugachi Benalcazar)

3.4.4.5 Sondeos y alarmas.

Existen muchos servicios dentro del Network Node Manager que recogen y generan información de eventos que se remiten a este. Estos eventos pueden ser emitidos desde agentes en nodos gestionados, de aplicaciones de gestión en diferentes estaciones de gestión, de algún nodo específico de la red o los eventos SNMP no solicitados llamados Traps.

Para gestionar esta alarma Network Node Manager ofrece un servicio, el visor de alarmas, por medio del cual se pude ver todos los Eventos y Traps que se generen, teniendo el control sobre todos ellos y de esta manera determinar cuáles se deben considerar lo suficientemente importantes como para definirlos como alarmas, facilitándonos la tarea de monitorización de las alarmas, para tomar decisiones apropiadas que nos garanticen el buen funcionamiento de la red.

Network Node Manager nos permite las siguientes operaciones relacionadas con las alarmas:

- ✓ Nos muestra la información útil de una alarma.
- ✓ Nos permite agrupar alarmas por categorías.
- ✓ Nos ayuda a reconocer que problema causó la alarma.
- ✓ Nos facilita obtener información particular mediante el filtrado de alarmas de distintas maneras.
- ✓ Nos permite ejecutar acciones adicionales una vez que se selecciona la alarma.

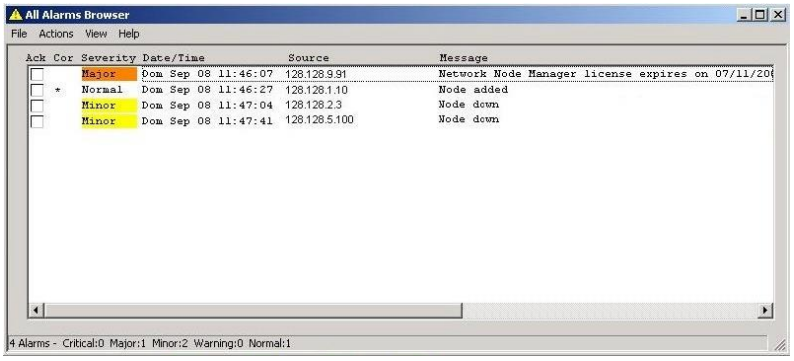
Para visualizar las alarmas existe el visor de alarmas el cual nos permite ver las alarmas por categorías, si deseamos ver las alarmas de cualquier símbolo en algún submapa, basta con

seleccionarlo y filtrar sus alarmar por categoría. (Boza Gaibor, López Potes, & Perugachi Benalcazar)

Ilustración 46: Sondeos y alarmas
(Boza Gaibor, López Potes, & Perugachi Benalcazar)

Al acceder a cualquiera de las categorías se mostrarán listadas en orden cronológico las alarmas pertenecientes a la categoría seleccionada, indicando la severidad, fecha, hora, que dispositivo la produjo y una breve descripción de la alarma.

Ilustración 47: Sondeos y alarmas
(Boza Gaibor, López Potes, & Perugachi Benalcazar)



3.5 Cuadro comparativo y Checklist

Después de conocer y detallar algunas de las herramientas de gestión más populares y reconocidas, se realizó una comparación específica entre todas las soluciones planteadas en base

a unos factores globales y competencias o especificaciones contenidas en dichos factores, los cuales se describen a continuación:

Funcionalidad:

- ✓ Monitorizar servicios, hardware y sistema operativo.
- ✓ Multiplataforma en cliente.
- ✓ Generar gráficas, informes y estadísticas.
- ✓ Enviar alarmas y notificaciones, etc.

Fácil uso:

- ✓ Interfaz o consola web con control total sobre la aplicación.
- ✓ Personalización de dicha interfaz.
- ✓ Extensión del sistema (plugins).
- ✓ Instalación, configuración y puesta en marcha, etc.

Arquitectura:

- ✓ Basada en varios procesos que realicen las funcionalidades de la aplicación.
- ✓ Consumo y requisitos previos aceptables (hardware, software, etc.)
- ✓ Sistema con agentes que trabajan en cada cliente o nodo.
- ✓ Posibilidad de monitorizar gran cantidad nº de nodos (varios miles).
- ✓ Estabilidad a cambios de configuración (reinicios del sistema), etc.

Calidad del Soporte Comunidad/Empresa:

- ✓ Desarrollo de nuevas mejoras y revisiones en la aplicación para la corrección de bugs.
- ✓ Actividad en el foro y wiki ante preguntas y resolución de problemas o peticiones de usuarios.

- ✓ Disponibilidad de una versión Enterprise de su herramienta, por si se requieren aspectos más específicos en el entorno de producción donde inicialmente se confió en una herramienta de software libre. En su defecto, un soporte profesional diferente al de la comunidad.
- ✓ Idiomas de la documentación disponible, etc.

A continuación, se expone un análisis criterioso de lo expuesto en los capítulos anteriores, a través de dos cuadros que reúnen y representarán de forma visual las características y consecución de objetivos de todo el software analizado, así:

COMPARATIVA GRÁFICA DE LAS PRINCIPALES CARACTERÍSTICAS DE LOS SISTEMAS DE MONITORIZACIÓN.

SISTEMA	SOFTWARE LIBRE	FUNCIONALIDAD	FÁCIL USO	ARQUITECTURA	SOPORTE	% Cumplimiento
OSSIM	✓	✓	✓	✓	✓	100%
OpenNMS	✓	✓	✗	✓	✓	80%
Hp OpenView	✗	✓	✓	✓	✓	80%

✓ La herramienta cumple. ✗ La herramienta no cumple.

CUADRO COMPARATIVO DE HERRAMIENTAS UTILIZADAS PARA LA GESTIÓN

SISTEMA / CARACTERISTICAS		OSSIM	OpenNMS	Hp OpenView
Recolección de Datos		SNMP, SSL, SSH, Packet Sniffing, RMON	SNMP, NSCLIENT, JMX	NETMON-SNMP
Alarmas	**Correo**	✓	✓	✓
	Sms	*	*	✓
Sistema Operativo		Linux Unix Windows	Linux Unix Windows	Microsoft Windows NT o Windows 2000 Workstation o Server versión 4.0
Tipo de Software		Libre	Libre	Comercial
Permisos a Usuarios		✓	✓	✓
Generación de Reportes		✓	✓	✓

* Se necesitan plugins adicionales.

En este proyecto de investigación se analizaron sólo una muestra del total de herramientas que existen actualmente en el mercado, debido a que sería imposible analizar todas las existentes a detalle, y no es el propósito de este trabajo.

En resumen, estas herramientas funcionan de manera similar cada una con sus propias características, algunas son más elaboradas que otras, unas de ellas cuentan con licencia comercial y otras tienen licencia de software libre, pero la mayoría contiene funciones equivalentes que nos ayudan a cuidar la integridad y disponibilidad de la red.

Hay que tener en cuenta que es decisión del administrador de red, escoger la herramienta que se acopla mejor a la infraestructura de la red con la que cuenta la institución o la empresa, es decir en base a un análisis criterioso de las necesidades que presenta la organización, para así aprovechar al máximo las características importantes como su funcionamiento, parámetros para

monitorización, protocolos usados, sensores y alarmas, esto con el fin de implementar un sistema de gestión que cumpla los objetivos planteados.

CAPÍTULO IV

4 CAPÍTULO 4: DISEÑO E IMPLEMENTACIÓN

4.1 Sistema a implementar

El sistema a implementar tiene que solucionar el principal problema de la red de la UEB, como es medir la utilización de sus recursos y poder administrarlos de una manera centralizada, para esto la herramienta debe contar con un sistema de alarmas que advierta de manera eficiente algún incidente o problema con la red o servidor, sin que sea necesario a cada momento que la interfaz del sistema tenga que estar siendo revisada. El sistema también deberá conservar una bitácora con los problemas presentados y su tiempo de respuesta de parte del departamento técnico, finalmente el sistema debe ser accesible desde una interfaz web y lo suficientemente flexible como para agregar nuevos módulos para necesidades futuras.

En conclusión y en base al análisis demostrado en los capítulos anteriores, la herramienta que se aproxima a los requerimientos planteados por su accesibilidad, flexibilidad y bajo costo en su implementación es el sistema Open Source SIM, mismo que será implementado en la Unidad de Redes y Telecomunicaciones de la Universidad Estatal de Bolívar, para esto se procedió a descargar la ISO de la página web oficial de AlienVault.

4.2 Requerimientos

Los requerimientos necesarios para la implementación son:

Requerimientos Técnicos

El requisito técnico más importante es el hardware para instalar OSSIM AlienVault, este dependerá en gran medida del número de eventos que tenga que procesar el servidor, de la cantidad de datos que pretendamos almacenar en la base de datos de OSSIM, y de la cantidad de hosts

disponibles en la red que pretendamos analizar, por lo que se optó por un equipo con las siguientes características:

ATRIBUTO	VALOR
capacidad disco duro interno	500 GB o superior
Chasis	Mini torre o Small Form Factor
interfaz de la unidad óptica	SATA
interfaz del disco duro	Serial ATA o superior
memoria cache	6 MB
memoria ram	4GB
Modelo	Modelo
Monitor	Mínimo 18.5" o de (20.1) LED,
número de núcleos	4 núcleos
Puertos	Minimo 2 USB 2.0 y 2 USB 3.0
soporte 64 bits	Si
soporte para virtualización	Si
tarjeta de red	10/100/1000
slots de memoria	4 slots
tipo de memoria	4 GB
tipo de procesador	i5-4590
velocidad con turbo	Si
velocidad de bus bidireccional (umi / dmi)	5 GT/s o equivalente según unidad de medida del fabricante
velocidad de reloj del procesador (sin turbo)	Ghz o superior

Requerimientos del personal

El perfil del servidor cuya misión sea el de administrar la red y el sistema, debe cumplir al menos con los siguientes requisitos:

- Seguridades informáticas.
- Sistemas operativos Linux, Windows y Windows Server.
- Interpretar los logs generados por los diferentes eventos en los sistemas operativos.
- Conocimientos básicos del modelo TCP/IP y redes LAN/WAN
- Debe saber interpretar gráficos estadísticos de reportes.

4.3 Implementación del Sistema Integrado de Gestión

Una vez escogido OSSIM como sistema de administración y monitorización para la red de la Universidad Estatal de Bolívar, se procedió con la fase de implementación en donde se tomaron en cuenta los siguientes factores:

Parámetros de configuración

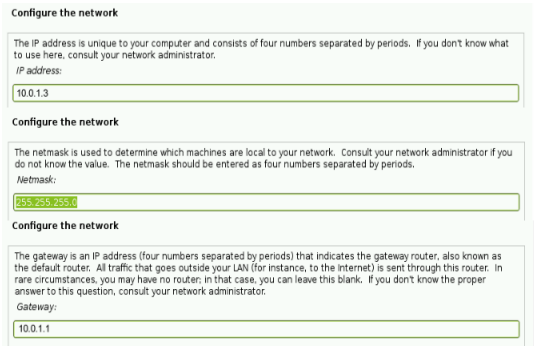
Los parámetros de configuración son los cimientos fundamentales para nuestro servidor OSSIM, por lo que se debe configurarlos de una manera correcta y adecuada para así poder recolectar los incidentes de una manera eficiente, las más importantes son:

4.3.1 Configuración de los parámetros de red.

En este paso, configuramos la red de OSSIM utilizando la tarjeta eth0 para la gestión y el resto de la red está conectado a la eth1, la configuración de la red para eth0 se muestra a continuación.

Ilustración 48: Tarjetas de red disponibles

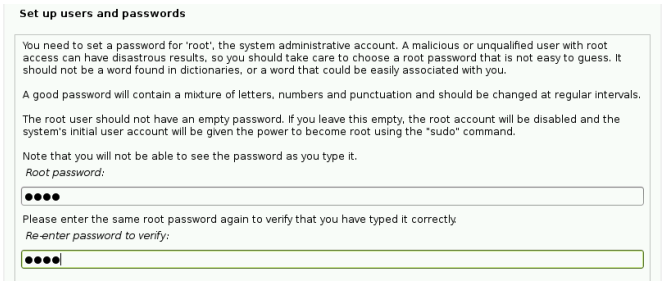
Ilustración 49: Configuración de direcciones IP



4.3.2 Configuración del usuario Root

Después de haber configurado lo parámetros de red, en las siguientes interfaces se ingresa la contraseña del usuario root para acceder a las configuraciones del servidor OSSIM.

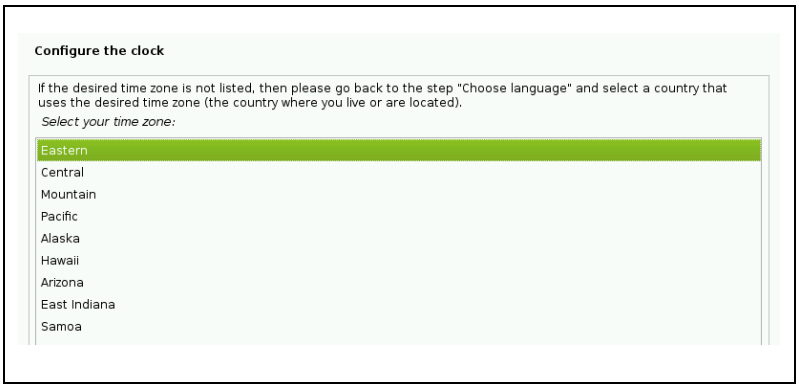
Ilustración 50: Configuración de contraseña



4.3.3 Zona Horaria y finalización de la instalación.

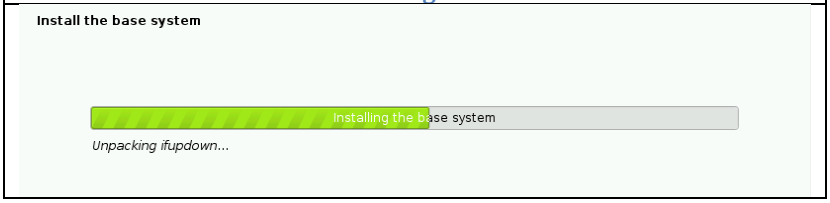
En este punto solo queda escoger nuestra zona horaria y el asistente automáticamente realizará la etapa de partición y empezará a instalar el sistema base como etapa final de la instalación.

Ilustración 52: Configuración de Idioma



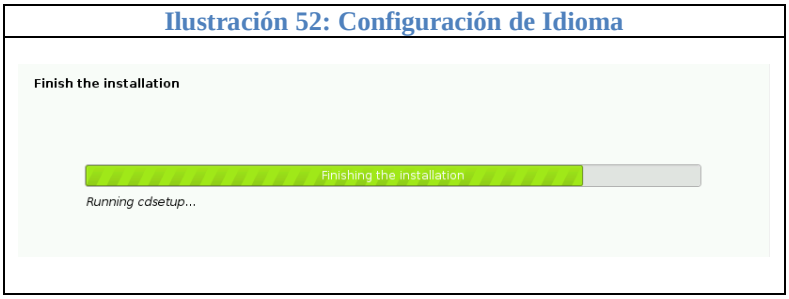
Después de configurar la zona horaria, el Asistente automáticamente realizar la etapa de partición y empezar a instalar el sistema base. Este paso se llevará a casi 15-20 minutos.

Ilustración 51: Configuración de Idioma



Etapa final de la instalación se muestra en la siguiente figura.

Ilustración 52: Configuración de Idioma



Iniciar sesión con el usuario root y la contraseña de la prueba en la CLI del servidor de OSSIM.

Ilustración 53: Inicio de sesión

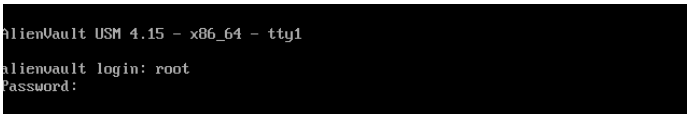
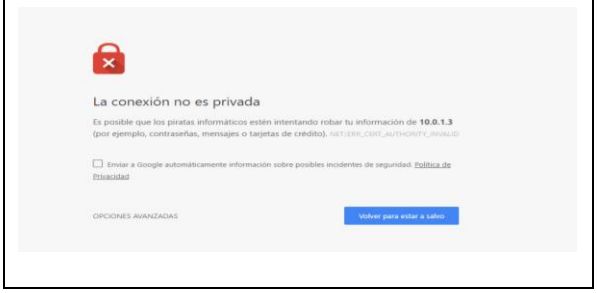


Ilustración 54: Consola de AlienVault

4.3.4 Panel de Administración vía Acceso Web

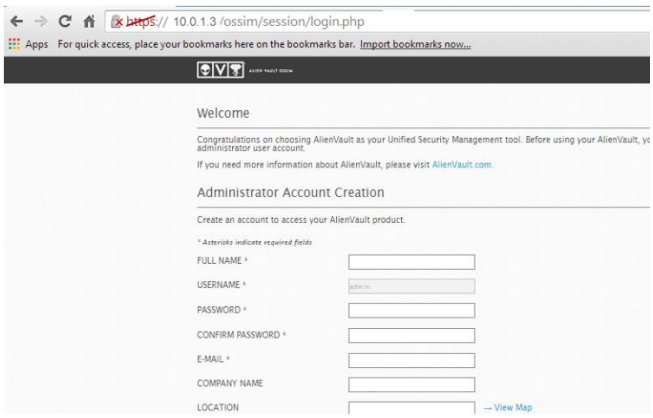
Parar terminar la configuración de OSSIM, se debe ingresar a la interfaz web utilizando el URL siguiente: 10.0.1.3.

Ilustración 55: Acceso vía web



Después de la aceptación de la excepción se debe ingresar la información necesaria para el perfil del administrador del servidor OSSIM. Complete los datos necesarios que se le plantean en la siguiente figura:

Ilustración 56: Información de registro



Una vez ingresada la información requerida en el formulario, se procede a ingresar el nombre de usuario es administrador y la contraseña anteriormente configurada.

Ilustración 57: Pantalla de login

Después de entrar con éxito en la interfaz web, el asistente aparecerá y se debe seguir los pasos para la configuración de servidor de OSSIM.

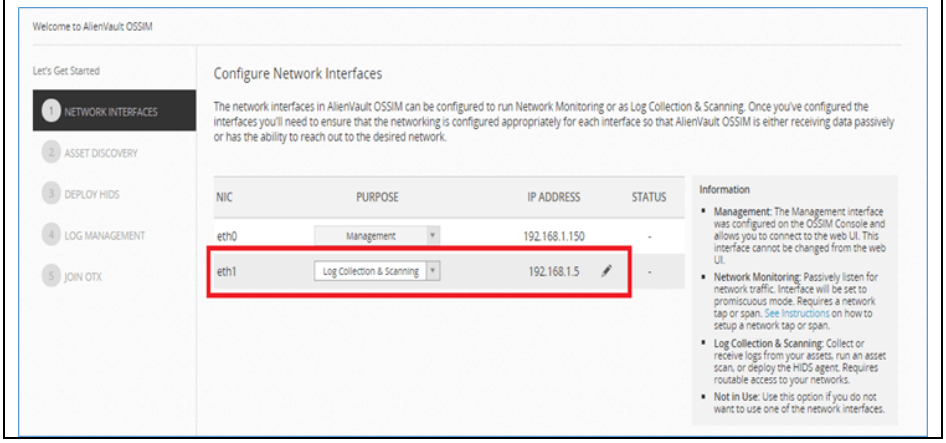
Ilustración 58: Configuración inicial

Aquí la interfaz gráfica nos muestra las siguientes tres opciones:

1. Monitor de red (Configurar la interface y monitor para el tráfico de la red).
2. Descubrimiento de activos (Detección automática de dispositivos de red en la organización).
3. Recolección de logs y seguimiento de nodos de la red.

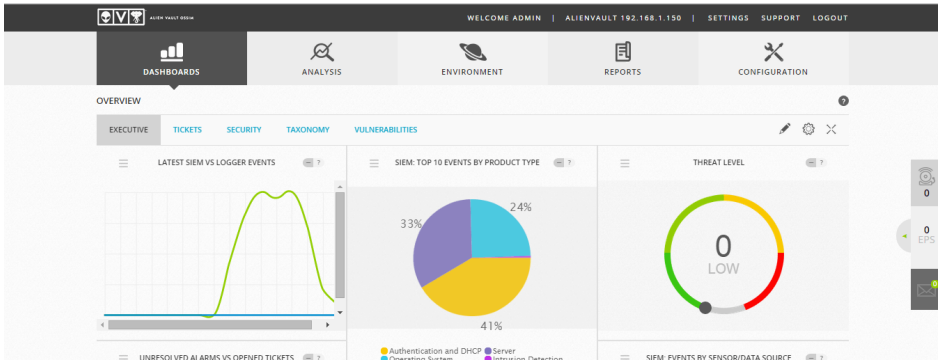
Se debe escoger el botón de inicio de la figura anterior para iniciar la configuración del servidor de OSSIM, acto seguido otras ventanas se generarán para introducir la configuración de la red que se muestra en la figura siguiente (se ha configurado eth1 para la interfaz de colector de registro y seguimiento del servidor de OSSIM).

Ilustración 59: Configuración de tarjeta monitor



Finalmente, la última opción del asistente de configuración es unirse a OTX (programa de intercambio de Amenaza de AlienVault). Para terminar la etapa de configuración damos clic en el botón “Finalizar”, a continuación, el tablero principal del servidor de OSSIM se desplegará así:

Ilustración 60: Menú principal

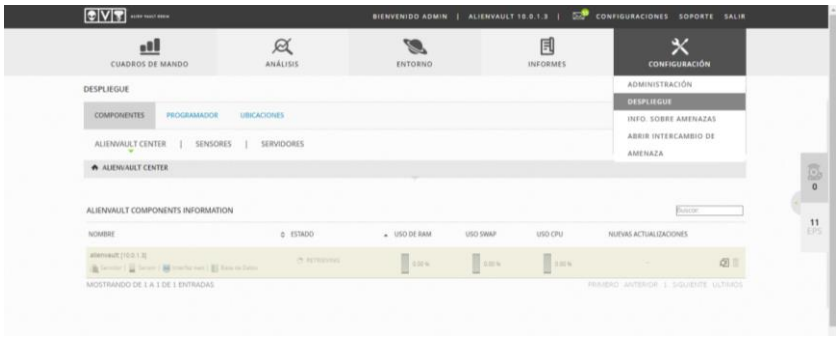


4.3.5 Configuración de mail server

Con el fin de que las políticas y acciones configuradas en nuestro servidor OSSIM puedan ser revisadas por el administrador de la red, se tiene que configurar un servidor de correo en el sistema, para este caso se utilizará una cuenta de Gmail configurándola de la siguiente forma:

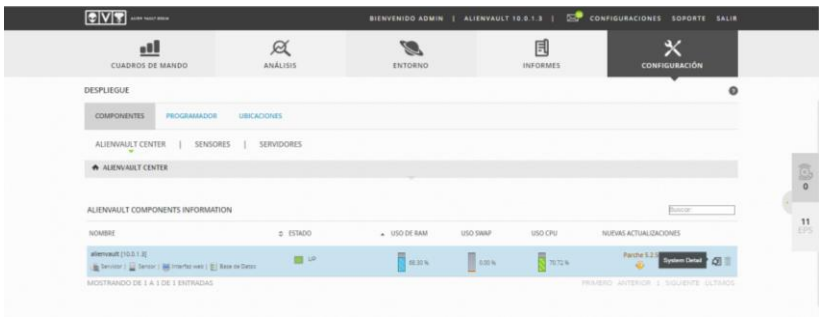
En la opción “configuración” del menú se debe escoger el item “Despliegue”:

Ilustración 61: Opción Despliegue



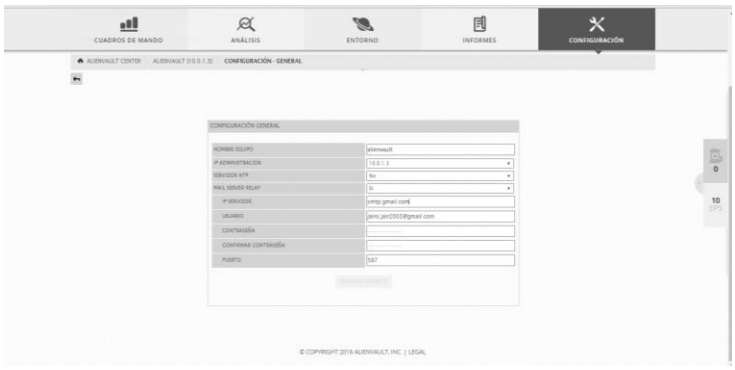
En esta opción la interfaz presentará el estado del servidor y para acceder a la opción de configuración general, se debe seleccionar “detalles del sistema”, misma que se encuentra en la parte derecha de la descripción.

Ilustración 62: Configuración General



Finalmente, en la sección de configuración general, se deben registrar los datos que solicita el formulario, cuyo contenido se detalla a continuación.

Ilustración 63: Configuración de parámetros



4.4 Características del sistema

4.4.1 Administración de Activos

La configuración de los activos de la red de la Universidad Estatal de Bolívar, se lo realizó mediante la opción “ASSETS & GROUPS” del menú principal “ENTORNO”, en esta opción el programa nos presenta el submenú añadir activos en donde se presentan varias opciones para añadirlos a nuestra red, para esto OSSIM utiliza Nmap:

Ilustración 64: Opción “Activos”

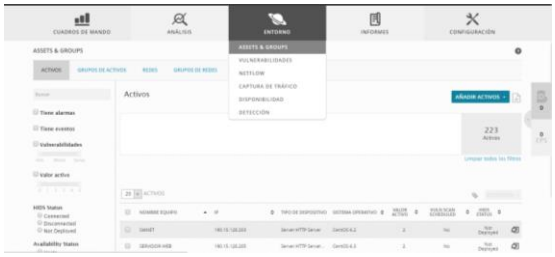
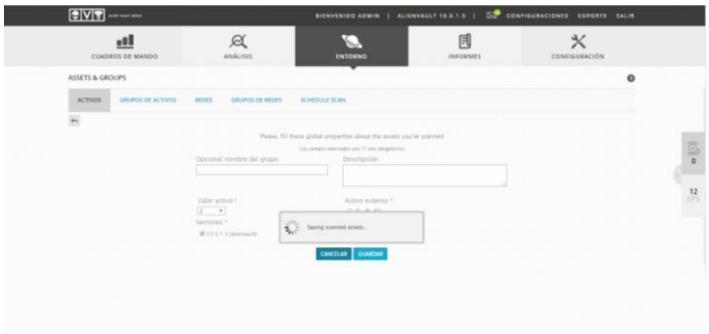


Ilustración 65: Despliegue de activos

Ilustración 66: Búsqueda de activos

Ilustración 67: Resultado de la búsqueda

Ilustración 68: Actualizando el inventario de activos



Lo recomendable en esta etapa es escanear la red a fin de encontrar todos los equipos conectados a la misma y así añadirlos automáticamente; sin embargo, también se pueden añadir los activos de forma manual:

Ilustración 69: Configuración de activos

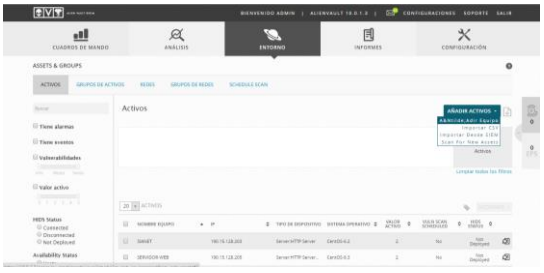
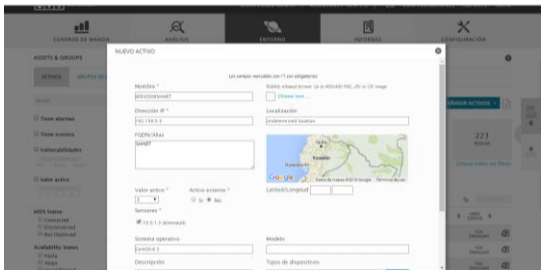


Ilustración 70: Parámetros de configuración

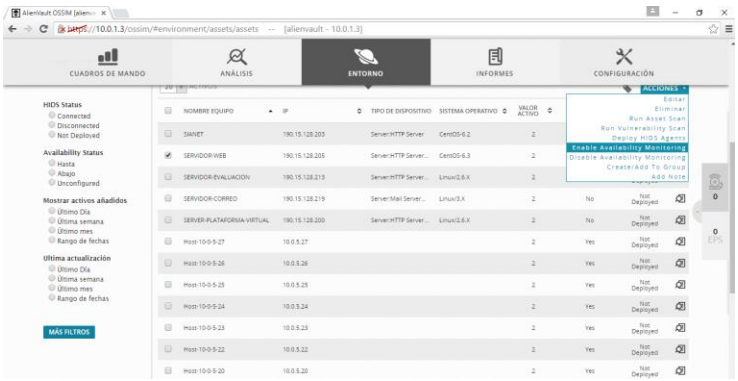


4.4.2 Monitorización de servicios

Una vez realizado el registro de los activos de la red, se debe habilitar la monitorización de los servicios que brindan los servidores de la organización, para esto en el menú inferior se

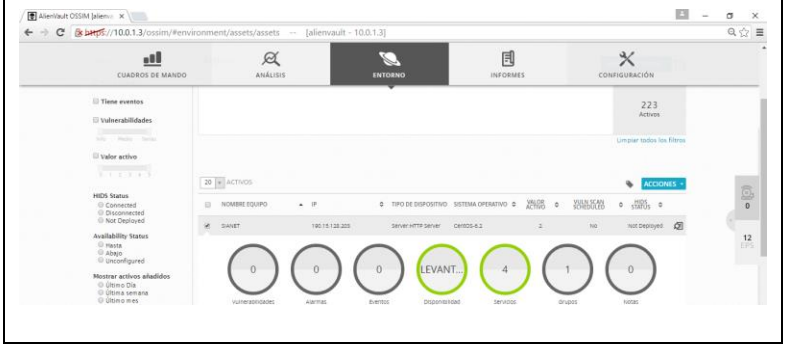
procederá a seleccionar las direcciones IPS de los equipos, opción “acciones” y “enable availability Monitoring”, para poder ejecutar este procedimiento OSSIM utiliza NAGIOS.

Ilustración 71: Monitorización de servicios



Los servicios que se ejecutan en nuestros servidores se mostraran de la siguiente manera:

Ilustración 71: Estado del activo



Estos servicios que pueden ser agregados, modificados y eliminados según nuestra necesidad a través de la opción EDIT SERVICES:

Ilustración 72: Servicios que corren en el activo

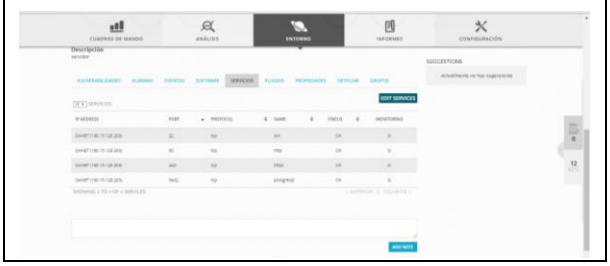
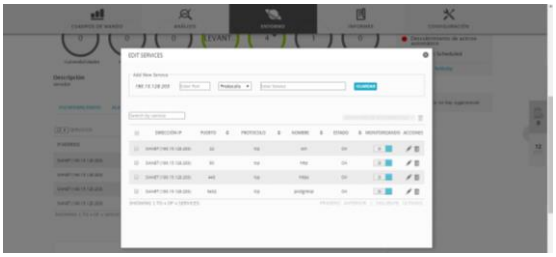


Ilustración 73: Configuración de los servicios a monitorear



4.4.3 Políticas de Seguridad

Esta característica de OSSIM nos permite definir reglas de seguridad para nuestros activos, estas definiciones permitirán disparar una alarma o una acción concreta ante un intento de acceso no autorizado. A continuación, se definen los parámetros de configuración de esta propiedad.

Ilustración 74: Definición de Políticas

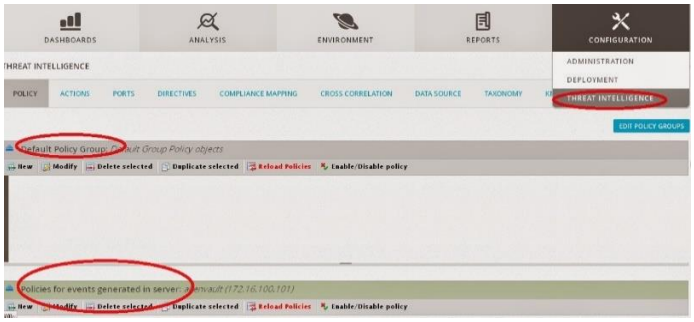
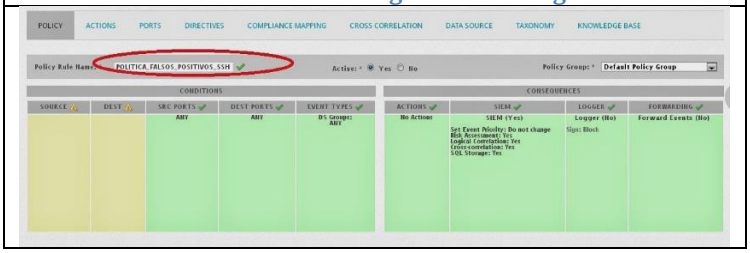


Ilustración 75: Configuración de reglas



En el submenú se despliega las distintas opciones seleccionado los bloques de color o en los menús laterales, configuramos las opciones relativas al origen, destino y puertos.

Ilustración 76: Definición del origen

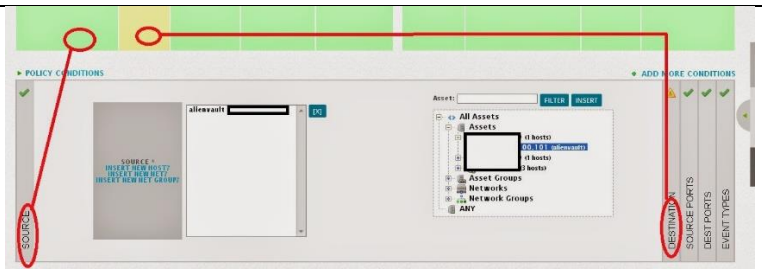
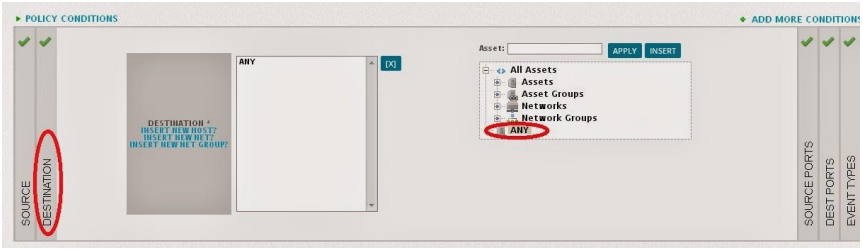


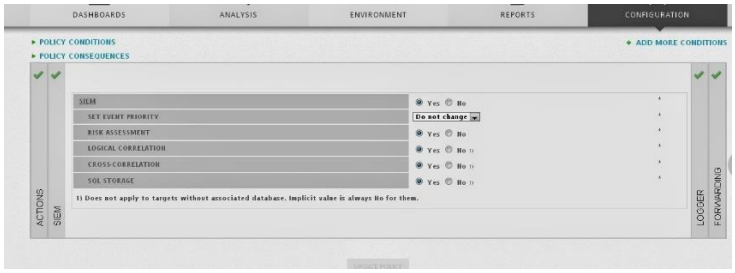
Ilustración 77: Definición del destino



Finalmente, para configurar los eventos se puede seleccionar por su taxonomía, categorización que tienen, o bien por fuentes de datos o DS (data sources).

Ilustración 78: Condición a monitorear

Ilustración 79: Política configurada



4.4.4 Visualización de Incidentes

Esta opción nos permite visualizar el tipo de amenazada detectada en nuestra red, así como los servicios que se encuentran vulnerables, estableciendo la hora y fecha de la detección y un ticket de seguimiento para el administrador, quién es la persona responsable de verificar la alerta y darle el procesamiento que amerite.

Ilustración 80: Monitor de incidentes

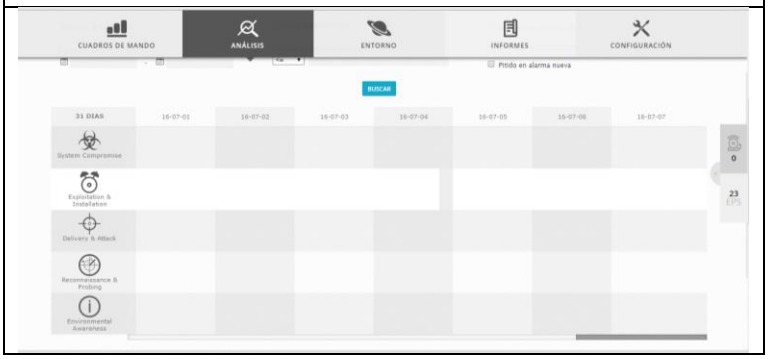
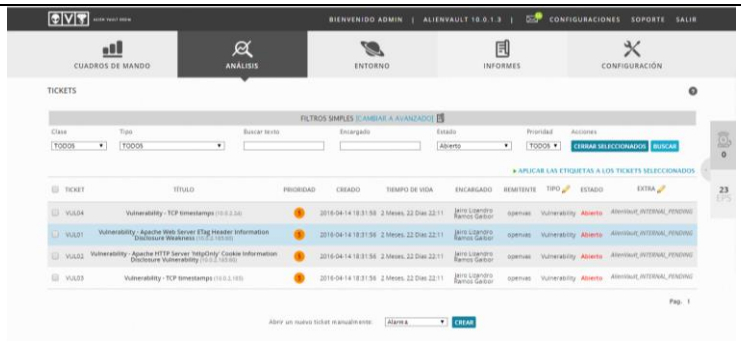
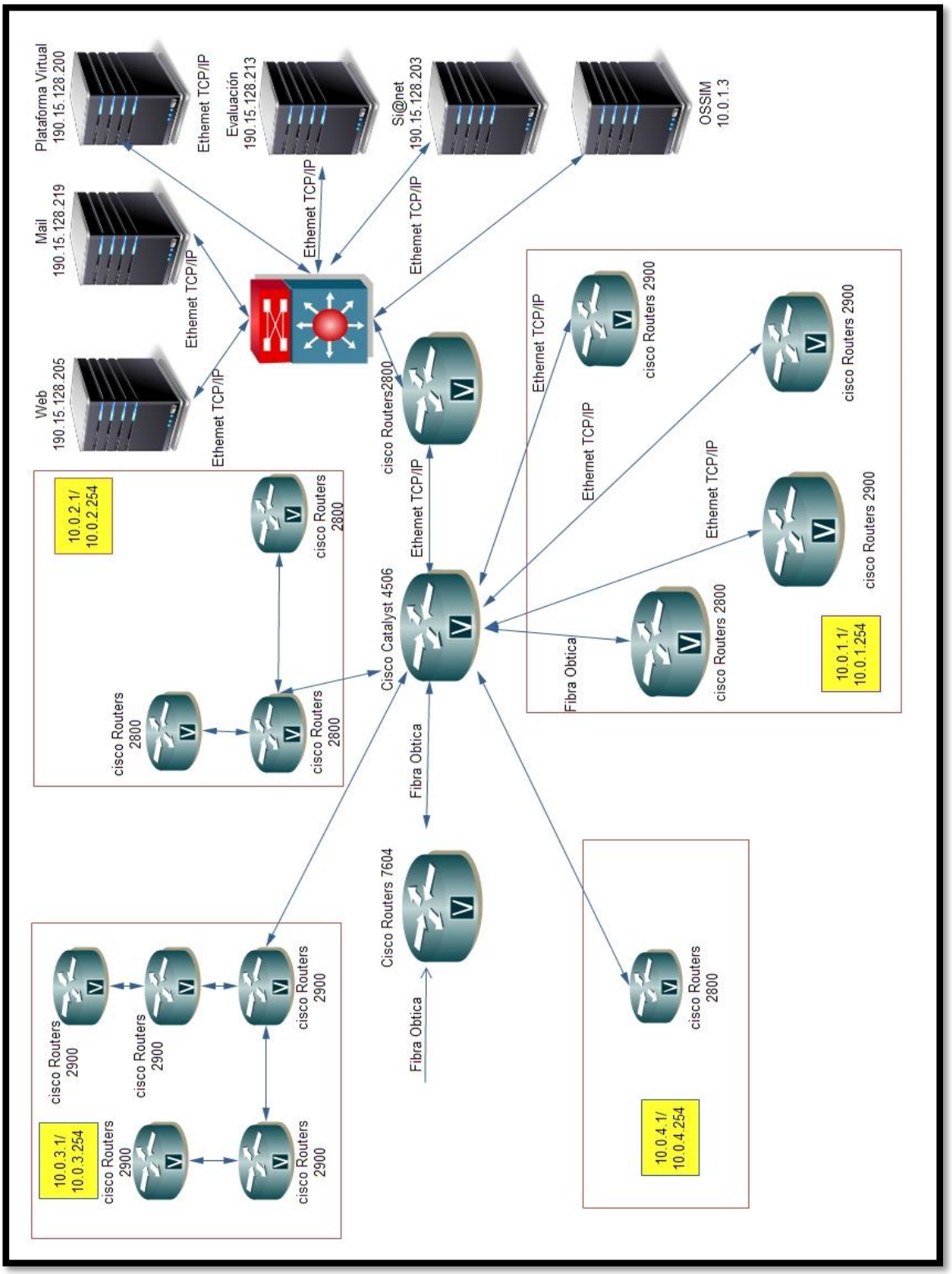


Ilustración 81: Detalle de incidentes registrados



4.5 Esquema de la red de la UEB



4.6 Backup del sistema

Esta característica nos permite respaldar y restaurar configuraciones del sistema, incluyendo el perfil, configuración de red, los datos de inventario, las políticas, los plugins, las directivas de correlación y otros ajustes básicos.

Las copias de seguridad se gestionan en la interfaz web y se ejecutan automáticamente cada día o según sea necesario. También se pueden restaurar las configuraciones de un archivo de copia de seguridad a través de la consola de AlienVault.

Cada archivo de configuración de copia de seguridad contiene lo siguiente:

- La configuración del sistema (redes, perfil del sistema, ajustes de configuración básica USM)
- Los datos de inventario
- políticas
- Plugins (tanto por defecto y personalizados)
- directivas de correlación
- configuraciones HIDS
- configuraciones de registro del sistema
- normas locales HIDS (v5.2.1)

Ilustración 82: Opción de respaldo

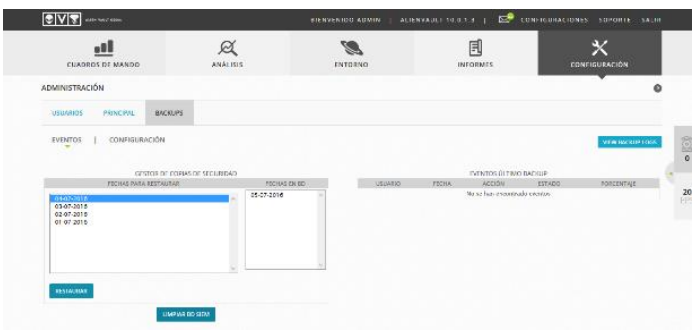
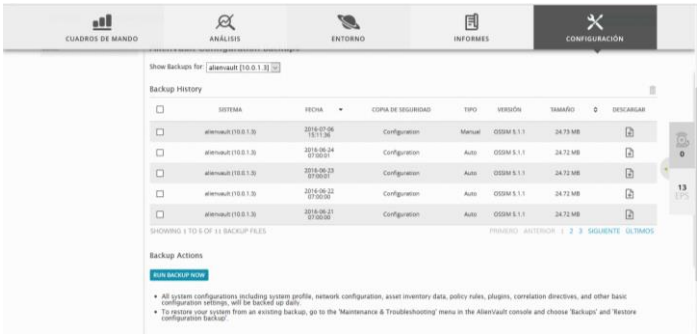


Ilustración 83: Detalle de respaldos disponibles



4.7 Interfaces

La interfaz web del servidor de OSSIM consta de las siguientes opciones en la interfaz de usuario principal:

- ✓ Cuadros de mando
- ✓ Análisis
- ✓ Entorno
- ✓ Informes
- ✓ Configuración

4.7.1 Cuadros de Mando

Se muestra una visión completa de todos los componentes del servidor de OSSIM como la gravedad de la amenaza, las vulnerabilidades, estado de implementación, los mapas de riesgo y las estadísticas OTX. En el sub menú del panel de control se muestra en la siguiente figura:

Ilustración 84: Cuadro de Mando

4.7.2 Análisis

Es un componente muy importante de OSSIM, servidor que analiza los hosts basados en sus registros. Este menú muestra las alarmas, SIEM (eventos de seguridad), entradas y registros en crudo, este menú de análisis se divide siguiente submenú:

Ilustración 85: Análisis

4.7.3 Entorno

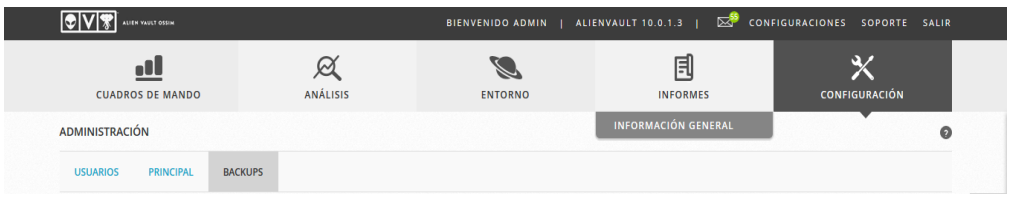
Este menú está relacionado con la configuración de los activos de la organización, se muestra el Activo, el Grupo y la Configuración de Red, Vulnerabilidades, Netflow y Detección. El submenú para todos estos parámetros se muestra a continuación.

Ilustración 86: Entorno

4.7.4 Informes

La notificación es un componente importante de cualquier servidor de registro, OSSIM servidor también genera informes que son muy útiles para la investigación detallada de cualquier host en específico.

Ilustración 87: Generación Informes



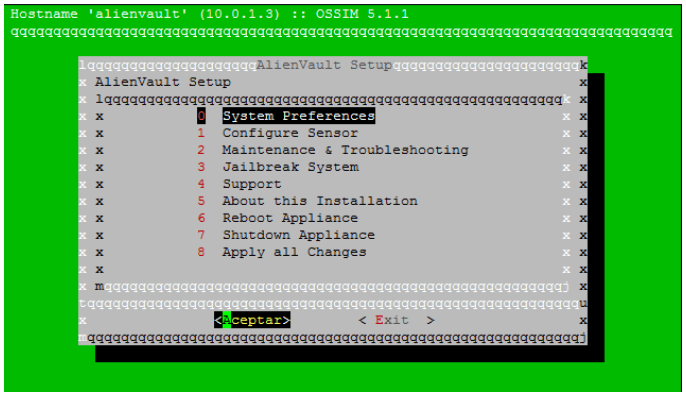
4.7.5 Configuración

Es el menú para configurar el servidor OSSIM, el usuario administrador puede cambiar la configuración del servidor de OSSIM tales como cambiar la dirección IP de la interfaz de administración, añadir más acogida para el seguimiento y registro y añadir / eliminar diferentes sensores / plugins. El sub menú para todos los servicios se muestra a continuación.

Ilustración 88: Configuración General

El sistema también se lo puede administrar desde la consola del servidor, en el cuál a través de comandos se puede modificar los archivos del servidor OSSIM, a continuación, se presenta el menú que muestra la citada consola:

Ilustración 89: Terminal de configuración



4.8 Utilización del sistema

La mayoría de electrónica de red (balanceadores, routers, conmuta- dores LAN, firewalls, sistemas de prevención de intrusos de red, etc), al igual que los sistemas operativos y las aplicaciones que corren en los mismos, generan información en forma de logs que es de gran utilidad para analizar una violación de la seguridad o cualquier problema.

Para facilitar el análisis de esta gran cantidad de información se ha implementado OSSIM, herramienta que se destaca por facilitar la integración de herramientas open source y herramientas propietarias, permitiendo contar con una amplia gama de recursos que se pueden utilizar, a fin de tener un mayor control en la monitorización y seguridad de la red, además permite tratar la información generada, almacenarla y priorizarla mediante técnicas de correlación, proporcionando una visión completa de la seguridad de la red desde una perspectiva de confidencialidad, integridad y disponibilidad.

CAPÍTULO V

5 CAPÍTULO 5: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Las conclusiones que encontramos al finalizar el presente proyecto de investigación son muchas, en especial el cumplimiento del objetivo a pesar de los obstáculos encontrados, a continuación, se detalla las más importantes.

- ✓ El presente trabajo de investigación ha plasmado un análisis criterioso de tres herramientas de gestión de red que se encuentran en el mercado, proporcionando a los diferentes departamentos responsables de la administración de las Tecnologías de la Información, un documento técnico que servirá para una mejor toma de decisiones a la hora de implementar un sistema de estas características.
- ✓ El sistema de gestión de red OSSIM, fue implementado en la Universidad Estatal de Bolívar no solo como una herramienta de monitoreo y de recolección de logs de diferentes dispositivos; sino también, como un SIEM (Security Information and Event Management), mismo que trae incorporado diversas características que buscan dar solución continua a cada uno de los inconvenientes que se generan en la ejecución de la confidencialidad, integridad y disponibilidad de la información.
- ✓ OSSIM otorga un gran aporte para la administración de la red de la UEB, ya que brinda al administrador información útil para la toma de decisiones en el campo de la seguridad y que enfocados en la visión principal, se ha logrado integrar varios dispositivos de red de diferentes marcas y diferentes servicios (Windows y Linux en la misma consola), logrando obtener un resultado confiable en la solución implementada.

- ✓ Existió dificultad al momento de la implementación de la herramienta, debido a que el área de redes de la UEB, no cuenta con inventario actualizado de los elementos activos de la red, así como tampoco cuenta con políticas, estándares y procedimientos de las actividades relacionadas con tecnología de información y comunicaciones que permitan asegurar la calidad e integridad de la información y de los servicios de red.
- ✓ OSSIM al tener la filosofía de código abierto y libre distribución, permite la implementación de una consola centralizada a un costo relativamente bajo, a más de poder desarrollar e incluir módulos según las necesidades de la Entidad.
- ✓ OSSIM es una herramienta muy poderosa al momento de visualizar la disponibilidad de los servidores y dispositivos de red, porque es eficiente y eficaz en el momento oportuno de detectar riesgos y amenazas generadas en la red interna por los diferentes hosts, al mismo tiempo presenta una gran cantidad de información que puede ser analizada detalladamente para la toma de decisiones.

5.2 RECOMENDACIONES

Con el desarrollo del presente proyecto de investigación, se logró detectar algunos puntos débiles en la administración la red de la UEB, por lo que a fin de explotar el 100% de las funcionalidades que nos brinda OSSIM, es necesario tomar en cuenta las siguientes sugerencias:

- ✓ Desarrollar e implementar políticas de seguridad basados en las normas ISO 27001, a fin de contar con una reacción metodológica y estandarizada ante la generación de algún evento o alarma.
- ✓ Con el propósito de no saturar el servidor OSSIM y a la vez recolectar la mayor cantidad de eventos y alarmas generados en la red interna, se sugiere instalar en el nodo de cada

facultad un ordenador con el sistema OSSIM cliente, el mismo que recolectara la información todos los eventos generados para enviarlos directamente al servidor.

- ✓ El administrador deberá profundizar sus conocimientos en el campo de seguridad informática y administración Linux, esto para aprovechar al máximo el funcionamiento de OSSIM y así ejecutar de una manera correcta sus configuraciones y actualizaciones, mismas que se presentan de manera muy recurrente.
- ✓ Desarrollar un módulo de notificación de alarmas y eventos vía SMS, a fin de que las notificaciones de los citados eventos y alarmas no solo sean reportadas por correo electrónico.
- ✓ Al no ser una red de gran magnitud se debe normar y fortalecer la utilización de OSSIM y no adquirir un sistema propietario para la gestión de red, esto a más del ahorro económico generado a la entidad, también cumplirá con el Decreto 1014 firmado por el Presidente de la Republica el 10 de abril de 2008, en el cual se exhorta a las instituciones públicas a usar software libre.

BIBLIOGRAFÍA

AlientVault. (21 de 10 de 2003). *AlientVault.* Obtenido de https://www.alienvault.com/docs/OSSIM-desc-es.pdf

ALIENVAULT. (20 de 02 de 2017). Obtenido de ALIENVAULT: https://www.alienvault.com/

Andrés, S. I. (6 de 02 de 2017). *Universidad Técnica de Ambato.* Obtenido de http://repositorio.uta.edu.ec/jspui/handle/123456789/8096

Árbol, M. R. (12 de 08 de 2010). *CincoDías*. Obtenido de http://www.cincodias.com/articulo/empresas/regala-producto-venceras/20100812cdscdiemp_22/

Asociación para el progreso de las comunicaciones. (07 de 02 de 2017). Obtenido de Asociación para el progreso de las comunicaciones: http://www.apc.org/es/glossary/term/241

Bowling, J. (1 de Mayo de 2010). *Linux Journal*. Obtenido de http://www.linuxjournal.com/magazine/alienvault-future-security-information-management?page=0,0

Boza Gaibor, F., López Potes, G., & Perugachi Benalcazar, C. (s.f.). Implementación de fucnciones de gestión de la red LAN de la compañia MAINT usando HP OPENVIEW Node Manager. *Tesis.* Escuela Superior Politécnica Litoral, Guayaquil.

Caballero, C. L. (2017). *Sistema de Monitorización.* Obtenido de Universidad de Sevilla: http://1984.lsi.us.es/pfe/trac/pfe-pandora/raw-attachment/wiki/WikiStart/3-Doc.Estado%20del%20Arte.pdf

Cabrer, M. R. (14 de Octubre de 2016). *Gestión y planificación de redes con sistemas inteligentes.* Obtenido de Gestión y planificación de redes con sistemas inteligentes: http://gssi.det.uvigo.es/users/mramos/public_html/gprsi/gprsi3.pdf

Caryuly, R. B. (11 de Julio de 2015). *Universidad Privada Dr. Rafael Belloso Chacín*. Obtenido de Protocolo SNMP: http://www.publicaciones.urbe.edu/index.php/telematique/article/viewArticle/782/1886

Casteleiro, A. G. (s.f.). Especificación del comportamiento de gestión de la red mediante ontologías. *Tesis Doctoral.* Universidad Politécnica de Madrid, Madrid.

CINCO DÍAS. (16 de 09 de 2013). Obtenido de CONCO DÍAS: http://cincodias.com/cincodias/2013/09/16/tecnologia/1379329588_005065.html

Cinvestav. (2016). *Cinvestav.* Obtenido de Cinvestav: http://www.tamps.cinvestav.mx/~vjsosa/clases/redes/MIB.pdf

Douglas R. Mauro y Kevin J. Schmidt. (2001). *Essential SNMP, First Edition.* Estados Unidos: O'Reilly.

Douglas R. Mauro y Kevin J. Schmidt. (2005). *Essential SNMP, Second Edition.* Estados Unidos: O'Reilly Media.

Ecured. (14 de 10 de 2016). Obtenido de Ecured: http://www.ecured.cu/index.php/Gesti%C3%B3n_de_Redes

ECURED. (20 de 02 de 2017). Obtenido de ECURED: https://www.ecured.cu/Ossim

ENISA. (2016). Obtenido de ENISA: http://www.enisa.es/documentos_web/documentos/Dossier%20de%20prensa%20Enisa%20201611.pdf

FUNIBER. (22 de 01 de 2017). *FUNIBER*. Obtenido de FUNIBER: https://www.funiber.org/gestion-de-redes/

García, A. (1 de Junio de 1999). *CCAPITALIA*. Obtenido de CCAPITALIA: http://www.ccapitalia.net/descarga/docs/1999-gestion-tmn-v1.pdf

Giménez, J. (2016). *JG Giménez.* Obtenido de JG Giménez: http://www.jggimenez.net/ucab/clases/redes2/clase15.pdf

Hewllet Packard. (Febrero de 1999). *IP Project Worj*. Obtenido de http://it-project-work.com/doc/HP-doc/openview/ITO%20open%20view%20operation%20administrators%20reference.pdf

ITU. (04 de Febrero de 2000). Obtenido de Unión Internacional de Telecomunicaciones: https://www.itu.int/rec/T-REC-M.3010-200002-I/es

Leskiw, A. (2016). *NetworkManagement Software*. Obtenido de NetworkManagement Software: http://www.networkmanagementsoftware.com/snmp-tutorial-part-2-rounding-out-the-basics/

Lorenzo, J. (2010). *Scadahacker*. Obtenido de https://scadahacker.com/library/Documents/Manuals/AlienVault_Installation_Guide.pdf

Luis, D. R., & Daniel, G. R. (22 de 01 de 2017). *UNAM*. Obtenido de UNAM: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/1027/Tesis.pdf?sequence=1

Martí, A. B. (1999). *Gestión de Red, Primera Edición.* Barcelona: Universidad Politécnica de Catalunia.

Mejía, L. M. (13 de 02 de 2001). *GNU*. Obtenido de GNU: https://www.gnu.org/philosophy/free-sw.es.html

Molero, L. (2010). *Planificación y Gestión de Red, 1ra. Edición.* Maracaibo.

Monteverde, J. (2013). *Ducumentos MX*. Obtenido de http://documents.mx/documents/sistema-de-monitorizacion-opennms.html

Nuñez, M. A. (2008). Propuesta de una Plataforma de Gestión de Información. *Telematica*, 18.

Omar, G. A., & Andrés, S. I. (22 de 01 de 2016). *UTA.* Obtenido de UTA: http://repositorio.uta.edu.ec/jspui/handle/123456789/8096

OpenNMS. (2016). *OpenNMS Group.* Obtenido de http://wiki.opennms.org/w/images/c/ca/ProvisioningUsersGuide.pdf

OpenNMS Group. (2016). *OpenNMS Group*. Obtenido de https://www.opennms.org/en

Ríos, M. E. (2016). *Universidad Nacional Autónoma de México* . Obtenido de http://redyseguridad.fi-p.unam.mx/pp/maru/labpracticas/Protocolos%20_Administracion%20_Red.pdf

Stallings, W. (1993). *SNMP, SNMPv2 and CMIP: The Practical Guide to Network-Management Standards.* Estados Unidos: Addison Wesley.

Suárez, D. I. (14 de 10 de 2016). *Angelfire.* Obtenido de Angelfire: http://www.angelfire.com/wy/licut/tareas/redes/gestion_osi.html

TechTarget. (2016). *TechTarget*. Obtenido de http://searchnetworking.techtarget.com/definition/NBAR-Network-Based-Application-Recognition

Tenea. (2016). *Tenea.* Obtenido de https://www.tenea.com/popups/servicios3_plataformas_pop8.html

Universidad de Mendoza. (2011). *Universidad de Mendoza*. Obtenido de Universidad de Mendoza: http://www.um.edu.ar/catedras/claroline/backends/download.php?url=L0RpYXBvcy9Nb25pdG9yZW8teS1HZXN0aW9uLWRlLVJlZGVzLnBkZg%3D%3D&cidReset=true&cidReq=2062

Universidad del Azuay. (2016). *Universidad del Azuay*. Obtenido de Universidad del Azuay: http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/snmp.htm

Varela, C. (1 de Junio de 2003). *Universidad El Bosque.* Obtenido de Universidad El Bosque: http://www.uelbosque.edu.co/sites/default/files/publicaciones/revistas/revista_tecnologia/volumen2_numero1/gestion_integrada_telecomunicaciones2-1.pdf

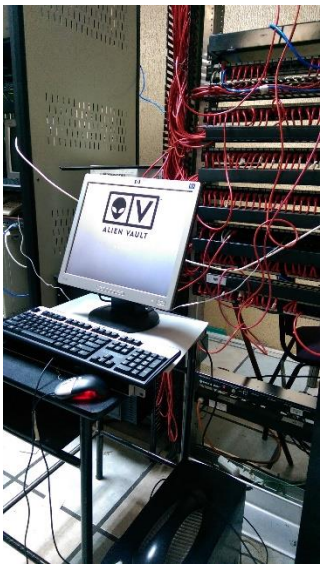
WIKIPEDIA. (10 de 12 de 2016). Obtenido de WIKIPEDIA: https://es.wikipedia.org/wiki/Open_Source_Security_Information_Management

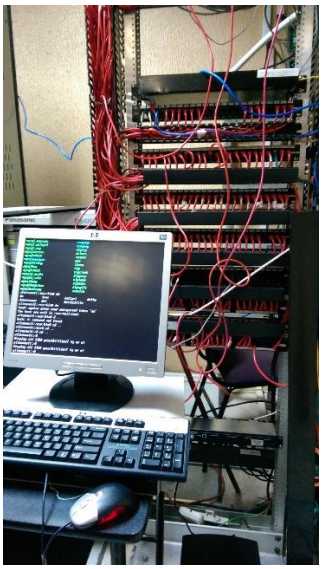
Zaizar, M. (2003). *Universidad de Colima.* Obtenido de Universidad de Colima: http://docente.ucol.mx/al986138/public_html/MARIO/adm_redes/Resumen%20Protocolos%20de%20Monitorizacion%20por%20Mz%20v1-0.pdf

ANEXOS

Anexo 1

Instalación y configuración del servidor OSSIM





Anexo 2

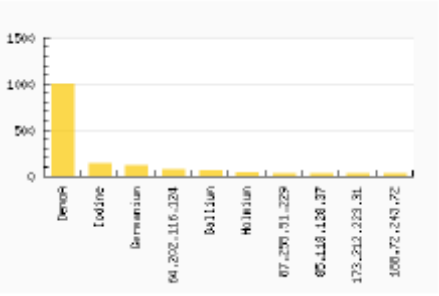
Reportes generados por el servidor OSSIM - Alarmas

ALIEN VAULT

Alarm Report_1

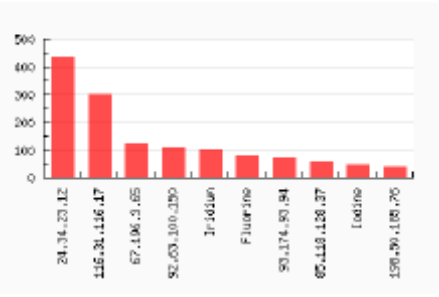
Alarms - Top 10 Attacked hosts from: 2016-08-01 to: 2016-08-30

Host	Occurrences
DemoA	1.006
Iodine	134
Germanium	108
64.202.116.124	75
Gallium	57
Holmium	39
87.255.51.229	31
85.118.128.37	29
173.212.223.31	27
188.72.243.72	24



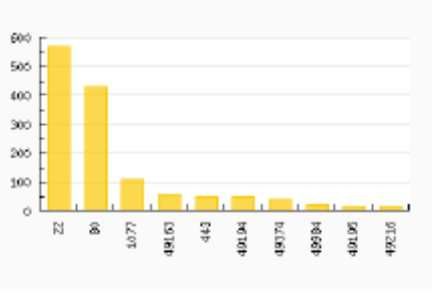
Alarms - Top 10 Attacker hosts from: 2016-08-01 to: 2016-08-30

Host	Occurrences
24.34.23.12	435
116.31.116.17	298
67.196.3.65	122
92.63.100.150	108
Iridium	99
Fluorine	81
93.174.93.94	71
85.118.128.37	57
Iodine	46
198.50.185.76	39



Alarms - Top 10 Destination Ports from: 2016-08-01 to: 2016-08-30

Port	Service	Occurrences
22	ssh	568
80	http	428
1077	unknown	108
49163	unknown	57
443	https	48
49194	unknown	48
49374	unknown	39
49984	unknown	22
49195	unknown	15
49216	unknown	15



User: guest / 2016-08-30 22:32:41 Page 2 / 4

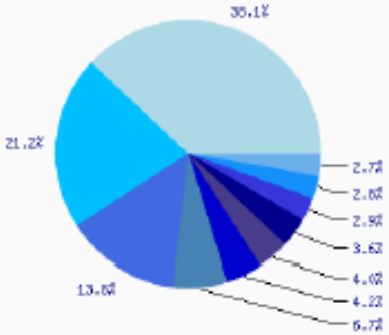
Top 10 de alarmas

ALIEN VAULT

Alarm Report_1

Alarms - Top 15 Alarms from: 2016-08-01 to: 2016-08-30

Alarm	Occurrences
Delivery & Attack — Bruteforce Authentication — SSH	512
Delivery & Attack — Bruteforce Authentication — Linux/Unix	285
Reconnaissance & Probing — Portscan — Nmap	186
Exploitation & Installation — Malicious website - Exploit Kit — Magnitude EK	90
Exploitation & Installation — Malicious website - Exploit Kit — GoonEK	57
System Compromise — Malware infection — Urausy	54
Exploitation & Installation — Malicious website - Exploit Kit — Java Rhino	48
Exploitation & Installation — Malicious website - Exploit Kit — Fiesta	39
Environmental Awareness — Vulnerable software — Java	37
Exploitation & Installation — Malicious website — Suspicious Java followed by an executable	36
Delivery & Attack — Malicious website - Exploit Kit — Magnitude EK	32
Exploitation & Installation — Malware infection — Exploit kit	30
Exploitation & Installation — Malicious website - Exploit Kit — Nuclear EK	27
System Compromise — C&C Communication — Sinkhole - Abuse.ch	27
Delivery & Attack — Malicious website - Exploit Kit — Neutrino EK	26



Alarms - Top 15 Alarms by Risk from: 2016-08-01 to: 2016-08-30

User: guest / 2016-08-30 22:32:41

Page 3 / 4

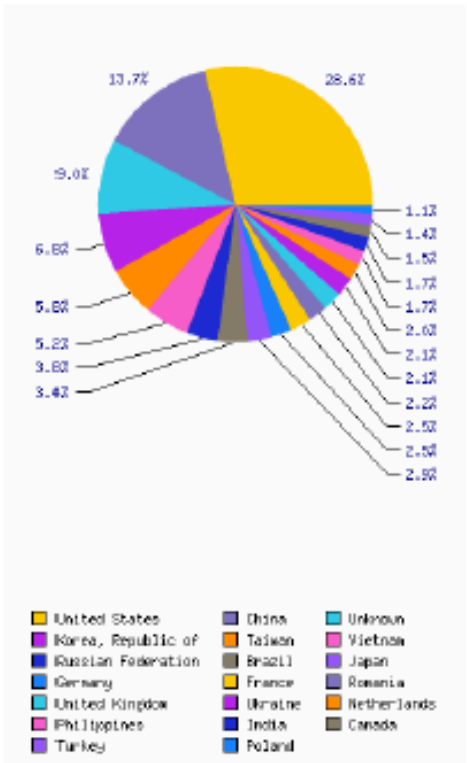
Reporte geográfico de alarmas

ALIEN VAULT

Geographic Report

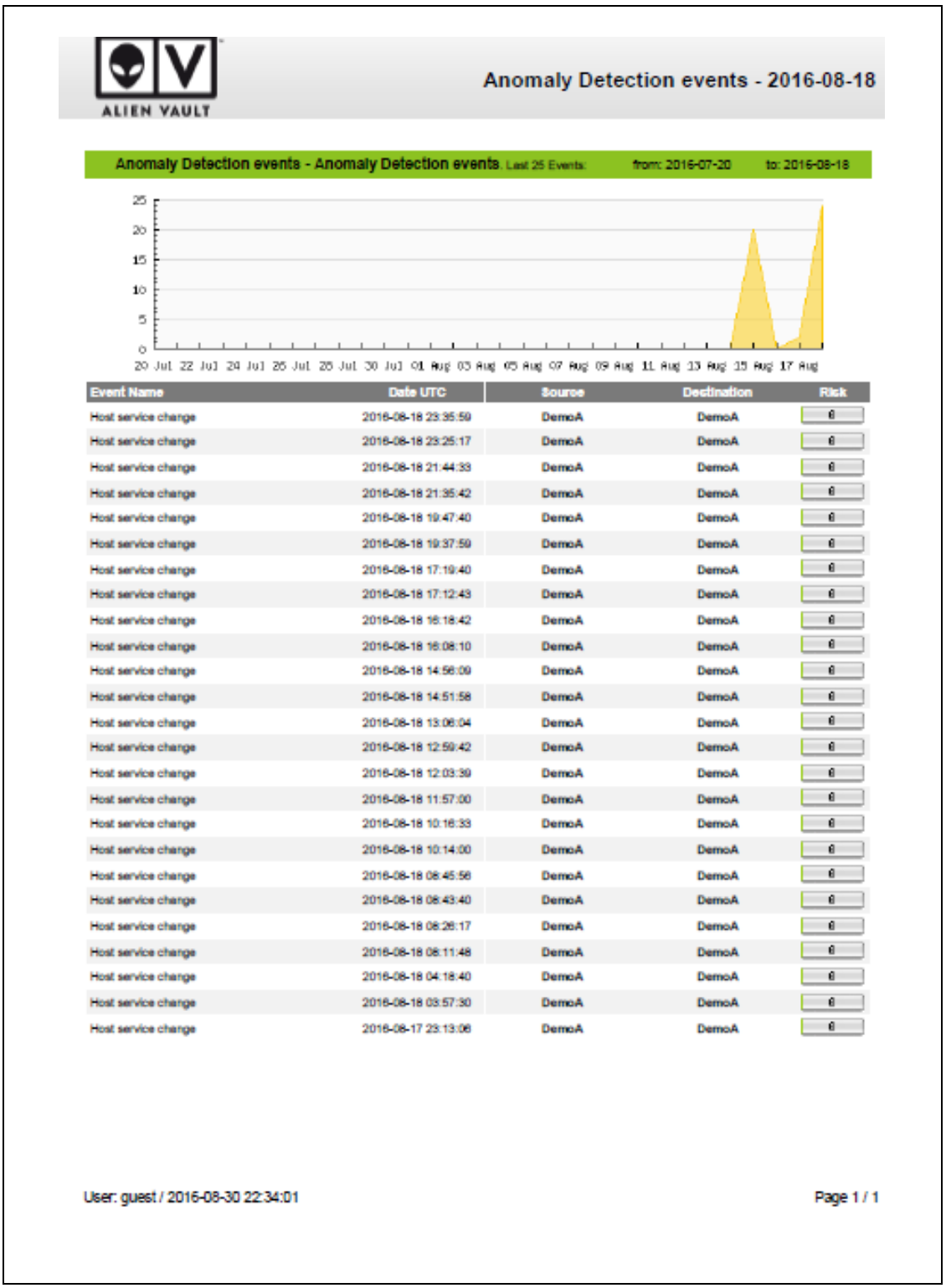
Geographic - Top 20 Attacker Countries from: 2016-08-01 to: 2016-08-30

Country	Attacks	%
United States	9125	28.6%
China	4364	13.7%
Unknown	2873	9%
Korea, Republic of	2177	6.8%
Taiwan	1859	5.8%
Vietnam	1675	5.2%
Russian Federation	1225	3.8%
Brazil	1090	3.4%
Japan	923	2.9%
Germany	811	2.5%
France	804	2.5%
Romania	710	2.2%
United Kingdom	681	2.1%
Ukraine	674	2.1%
Netherlands	633	2%
Philippines	544	1.7%
India	544	1.7%
Canada	465	1.5%
Turkey	436	1.4%
Poland	341	1.1%



User: guest / 2016-08-30 22:26:06 Page 3 / 4

Detección de eventos anómalos



ALIEN VAULT

Anomaly Detection events - 2016-08-18

Anomaly Detection events - Anomaly Detection events. Last 25 Events: from: 2016-07-20 to: 2016-08-18

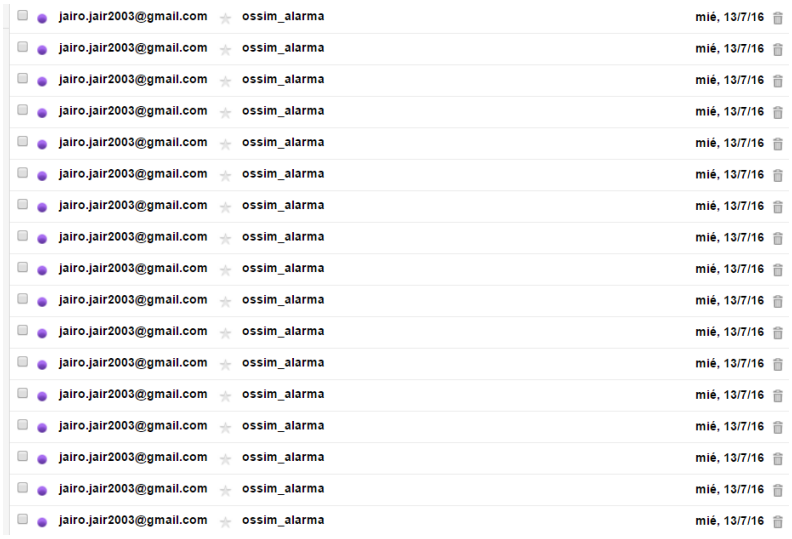
Event Name	Date UTC	Source	Destination	Risk
Host service change	2016-08-18 23:35:59	DemoA	DemoA	0
Host service change	2016-08-18 23:25:17	DemoA	DemoA	0
Host service change	2016-08-18 21:44:33	DemoA	DemoA	0
Host service change	2016-08-18 21:35:42	DemoA	DemoA	0
Host service change	2016-08-18 19:47:40	DemoA	DemoA	0
Host service change	2016-08-18 19:37:59	DemoA	DemoA	0
Host service change	2016-08-18 17:19:40	DemoA	DemoA	0
Host service change	2016-08-18 17:12:43	DemoA	DemoA	0
Host service change	2016-08-18 16:18:42	DemoA	DemoA	0
Host service change	2016-08-18 16:08:10	DemoA	DemoA	0
Host service change	2016-08-18 14:56:09	DemoA	DemoA	0
Host service change	2016-08-18 14:51:58	DemoA	DemoA	0
Host service change	2016-08-18 13:06:04	DemoA	DemoA	0
Host service change	2016-08-18 12:59:42	DemoA	DemoA	0
Host service change	2016-08-18 12:03:39	DemoA	DemoA	0
Host service change	2016-08-18 11:57:00	DemoA	DemoA	0
Host service change	2016-08-18 10:16:33	DemoA	DemoA	0
Host service change	2016-08-18 10:14:00	DemoA	DemoA	0
Host service change	2016-08-18 08:45:56	DemoA	DemoA	0
Host service change	2016-08-18 08:43:40	DemoA	DemoA	0
Host service change	2016-08-18 08:26:17	DemoA	DemoA	0
Host service change	2016-08-18 08:11:48	DemoA	DemoA	0
Host service change	2016-08-18 04:18:40	DemoA	DemoA	0
Host service change	2016-08-18 03:57:30	DemoA	DemoA	0
Host service change	2016-08-17 23:13:06	DemoA	DemoA	0

User: guest / 2016-08-30 22:34:01

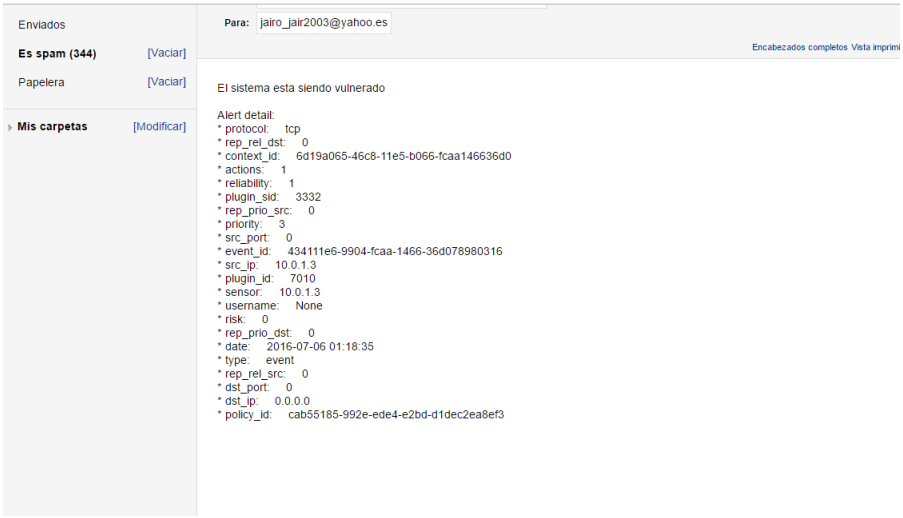
Page 1 / 1

Anexo 3

Eventos enviados por correo electrónico



Bandeja de entrada de la cuenta de correo del administrador.



Mensaje de alarma recibido.

Anexo 4

Data Sheet OSSIM

AlienVault Unified Security Management

AlienVault's Unified Security Management™ (USM™) platform accelerates and simplifies threat detection, incident response and compliance management for IT teams with limited resources, on day one. With essential security controls and integrated threat intelligence built-in, AlienVault USM puts complete security visibility of threats affecting your network and how to mitigate them within fast and easy reach.

Whether large or small, all organizations need complete visibility to:

- Detect emerging threats across your environment
- Respond quickly to incidents and conduct thorough investigations
- Measure, manage, and report on compliance (PCI, HIPAA, ISO, and more)
- Optimize your existing security investments and reduce risk

AlienVault's Unified Security Management solution delivers this complete security visibility by providing the five essential security capabilities in a unified platform, controlled by a single management console:

- **Asset Discovery** - active and passive network discovery
- **Vulnerability Assessment** – active network scanning, continuous vulnerability monitoring
- **Intrusion Detection** - network and host IDS, file integrity monitoring
- **Behavioral Monitoring** - netflow analysis, service availability monitoring
- **SIEM** - log management, event correlation, analysis, and reporting

Integrated Threat Intelligence

AlienVault Labs' Threat Intelligence service maximizes the effectiveness of any security monitoring program by providing regularly updated correlation directives, intrusion detection signatures, response guidance, and much more. These constant updates enable the USM platform to analyze the mountain of event data from all of your data sources, and tell you exactly what are the most important threats facing your network right now, and what to do about them. Our threat experts spend countless hours researching the latest exploits, malware strains, attack techniques, and malicious IPs, so you don't have to. They incorporate this expertise into the library of over 2,000 customizable correlation directives that ship with the USM platform, eliminating the need for you to conduct your own research and write your own correlation rules, giving you the ability to detect and respond to threats on day one.

The AlienVault Labs Threat Research Team also curates the Open Threat Exchange, the world's first truly open threat intelligence community that enables collaborative defense with open access to collaborative research on emerging threats. OTX integrates with AlienVault USM and enables everyone in the OTX community to actively collaborate, strengthening their own defenses while helping others do the same.

	USM ALL-IN-ONE					USM STANDARD			USM ENTERPRISE		
	AIO 25A	AIO 75A	AIO 150A	AIO UA[1]	Remote Sensor[2]	Server	Logger	Sensor	Server[3]	Logger	Sensor[4]
Device Performance											
Max Assets	25	75	150	--	--	--			--		
Max Events in Database (Millions)	200					200	--	--	200	--	--
Max Data Collection (EPS)	1,000			1,000	500	--	15,000	2,500	--	15,000	--
Max Data Correlation (EPS)	1,000			1,000	--	5,000	--	--	10,000	--	--
IDS Throughput (Mbps)	100			100	100	--	--	1,000	--	--	5,000
Hardware Specifications											
Form Factor	1U					1U			2 x 1U	1U	
Length x Width x Height (in)	26.6 x 17.2 x 1.7				11.3 x 17.2 x 1.7	26.6 x 17.2 x 1.7			26.6 x 17.2 x 1.7		
Weight (lb)	42				11	42			42		
Power Supply	2 x 700 / 750W				1 x 700/750W	2 x 700 / 750W			2 x 700 / 750W		
Network Interfaces	6 x 1GbE				2 x 1GbE	2 x 1GbE		6 x 1GbE 2 x 10GbE (option)	2 x 1GbE		6 x 1GbE 2 x 10GbE (option)
CPU	2 x Intel Xeon E5620 2.4GHz 8 Cores				1x Intel Xeon E3-1220, 3.1 MHz 4 Cores	2 x Intel Xeon E5620 2.4GHz 8 Cores	1 x Intel Xeon E5620 2.4 GHz 4 Cores		2 x Intel Xeon E5620 2.4GHz 8 Cores	1 x Intel Xeon E5420 2.4 GHz 4 Cores	
Storage Capacity (TB) Compressed[5] / Uncompressed	9.0 / 1.8				5.0 / 1.0	6.0 / 1.2	9.0 / 1.8	6.0 / 1.2	6.0 / 1.2	11.0 / 2.2	6.0 / 1.2
Disk Array Configuration	RAID 10				No	RAID 10			RAID 10		
Memory (GB)	24				8	24			24	48	24
Redundant Power Supply	Yes				No	Yes			Yes		
IPMI Interface	Yes					Yes			Yes		
Max Heat Dissipation (BTU/hr)	439.55				27.30	846.18	815.47	667.05 (6x1 option) 684.11 (2x10 option)	846.18	819.93	667.05 (6x1 option) 684.11 (2x10 option)
Max Power Consumption (kVA)	0.1288				0.1052	0.2480	0.2390	0.1955 (6x1 option) 0.2005 (2x10 option)	0.2480	0.2110	0.1955 (6x1 option) 0.2005 (2x10 option)

[1] If you disable the Sensor on the AIO UA appliance, you can still collect up to 2500 EPS from remote sensors.
[2] Remote Sensor device ships with feet for desktop deployment. Rack mount not required.
[3] Enterprise Server ships with 2 x 1U devices. One device is the Enterprise Server and one is the Enterprise DB
[4] Enterprise Sensor provides IDS capabilities only. It does not include data collection capabilities
[5] 5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

	USM ALL-IN-ONE						USM STANDARD		
	AIO 25A	AIO 75A	AIO 150A	AIO UA (Sensor Disabled)	AIO UA (Sensor Enabled)	Remote Sensor	Server	Logger	Sensor
Virtual Machine Requirements									
Virtual Cores	8					4	8		
RAM (GB)	16					8	24		
Storage Capacity[1] (TB) Compressed / Uncompressed	5.0 / 1.0						6.0 / 1.2	9.0 / 1.8	6.0 / 1.2
Vmware ESXi Support	ESXi 4.0+						ESXi 4.0+		

[1]5:1 compression ratio is the average experienced by our customers. Actual compression may be higher or lower depending on specific log data.

Try it today. Free for thirty days.

Ready to see how AlienVault's Unified Security Management can help you reduce risks, pass audits, and enhance your incident response program? Try one of our USM products in your environment today for free – for the first 30 days. Please visit this site to find out more information: **www.alienvault.com/free-trial**

About AlienVault

AlienVault has simplified the way organizations detect and respond to today's ever evolving threat landscape. Our unique and award-winning approach, trusted by thousands of customers, combines the essential security controls of our all-in-one platform, AlienVault Unified Security Management, with the power of AlienVault's Open Threat Exchange, the world's largest crowdsourced threat intelligence community, making effective and affordable threat detection attainable for resource-constrained IT teams. AlienVault is a privately held company headquartered in Silicon Valley and backed by Trident Capital, Kleiner Perkins Caufield & Byers, Institutional Venture Partners, GGV Capital, Intel Capital, Jackson Square Ventures, Adara Venture Partners, Top Tier Capital and Correlation Ventures. For more information visit **www.AlienVault.com** or follow us on **Twitter (@AlienVault)**.