

Universidad Tecnológica de El Salvador



Análisis e interpretación de información de servidores seleccionados en la empresa Negocios Asociados S. A. para el estudio sobre la posibilidad de migración a un ambiente virtual utilizando tecnología Vmware en los nuevos servidores que serán adquiridos por la empresa con el fin de virtualizar.

Integrantes

William Adonis Díaz Valdez

Carlos Ernesto Hernández Granados

Cesar Augusto Viana

Carné

25-5700-2008

25-1242-2008

25-4407-2007

Índice de contenido

Introducción	1
1. Descripción del proyecto de investigación	2
1.1. Objetivos	2
1.1.1. Objetivo General	2
1.1.2. Objetivos Específicos	2
1.2. Alcances y limitantes	4
1.2.1. Alcances	4
1.2.2. Limitantes	4
1.3. Situación Problemática	5
1.4. Justificación	5
1.5. Cronograma de actividades	7
2. Marco teórico	8
2.1. Descripción de la Empresa	8
2.2. Descripción de las tecnologías, metodologías a utilizar en el proyecto . .	10
2.2.1. Metodología a emplear	10
2.2.2. Síntesis de las tecnologías a utilizar	10
2.2.3. Cuadros comparativos	23

Introducción

Como aporte para la empresa Negocios Asociados S. A se ha desarrollado el presente trabajo con la finalidad de colaborar con el correcto desempeño de las labores cotidianas de los empleados que hacen uso de los sistemas de información y brindar apoyo que permita conocer las condiciones de funcionalidad de los servidores que brindan sus diferentes servicios para que los empleados puedan realizar sus labores cotidianas.

La empresa se dedica a comercializar productos eléctricos de baja, media y alta tensión, es una empresa regional que cuenta con muchas sucursales en la región Centroamericana, debido a esto tiene diseminado por la región muchos servidores con mucha información valiosa, pero nuestro trabajo se enfocara en una de las sucursales que se llama “Electrobodegas”, donde se encuentra centralizada mucha información y la mayoría del personal administrativo con que cuenta la empresa.

En la empresa se encuentran funcionando muchos servidores y algunos de ellos presentan algún tipo de dificultad y que expondremos a los miembros del equipo de IT de la empresa para que tomen en consideración nuestro estudio sobre los recursos con los que actualmente cuenta la empresa y que se tienen pensado llevarse a un ambiente virtual.

Capítulo 1 - Descripción del proyecto de investigación

1.1 Objetivos

1.1.1 Objetivo General

Aportar a la empresa Negocios Asociados S. A. un análisis de los servidores que se podrían virtualizar, propuestos por la empresa, en el cual se estudiarán las características y especificaciones técnicas de cada uno y que arrojará los resultados para saber si estos pueden ser llevados a un ambiente virtual.

1.1.2 Objetivos Específicos

- Implementar herramientas de diagnóstico en los servidores escogidos que brinden la información necesaria para el análisis que arrojará los resultados necesarios para saber qué clase de equipos Negocios Asociados S. A. podría adquirir.
- Diagnosticar y hacer observaciones sobre cualquier mal funcionamiento o irregularidad que se encuentre durante el estudio de los equipos para posteriormente hacer recomendaciones sobre estos para así evitar futuras fallas que comprometan el funcionamiento de los servidores.
- Presentar propuestas sobre la optimización de los recursos de los servidores que se van a convertir a máquinas virtuales para así aprovechar mejor los equipos

tecnológicos que la empresa va adquirir.

1.2 Alcances y limitantes

1.2.1 Alcances

- Recolectar la información necesaria sobre uso de recursos de entrada y salida de periféricos principales como memoria RAM, disco duros y procesador, así como uso de la red de los servidores que se podrían virtualizar.
- Analizar el funcionamiento actual de los servidores y verificar posibles fallas que estos pudiesen tener como falta de recursos, aplicaciones ligadas a cierto software que el servidor utiliza o si hay un gran tráfico de red.
- Crear una propuesta de hardware de los servidores que serán virtualizados para estos no sufran de falta de recursos o desperdicio de estos y que tecnología de virtualización les beneficiaría.

1.2.2 Limitantes

- Debe ser utilizada solo una herramientas de diagnostico para evitar que las herramientas de monitoreo gasten recursos en los servidores que se monitorearan.
- Se enfoca en aquellas aplicaciones o servicios que tienen más importancia en los servidores.
- Los recursos que serán recomendados serán aquellos que tienen mayor relevancia para la creación de una máquina virtual (memoria RAM, procesador, discos duros, tarjetas de red) en los servidores seleccionados por la empresa Negocios Asociados S.A.

1.3 Situación Problemática

La situación en la empresa es la siguiente:

Como empresa han tomado la decisión de migrar algunos servidores a un ambiente virtualizado.

Algunas de las razones por la que se desean implementar virtualización son:

- Uno de los servidores ya no cuenta con fuente redundante
- Problemas de espacio en almacenamiento
- No tiene soporte en discos duros, esto por que ya no se encuentran discos para este modelo de servidor.
- La información que se encuentra en el servidor es de vital importancia, ahí están las bases de datos de la empresa.
- Uno de los servidor tiene problemas similares, en este funcionan el Active Directory, Servidor DHCP y servidor de aplicaciones.

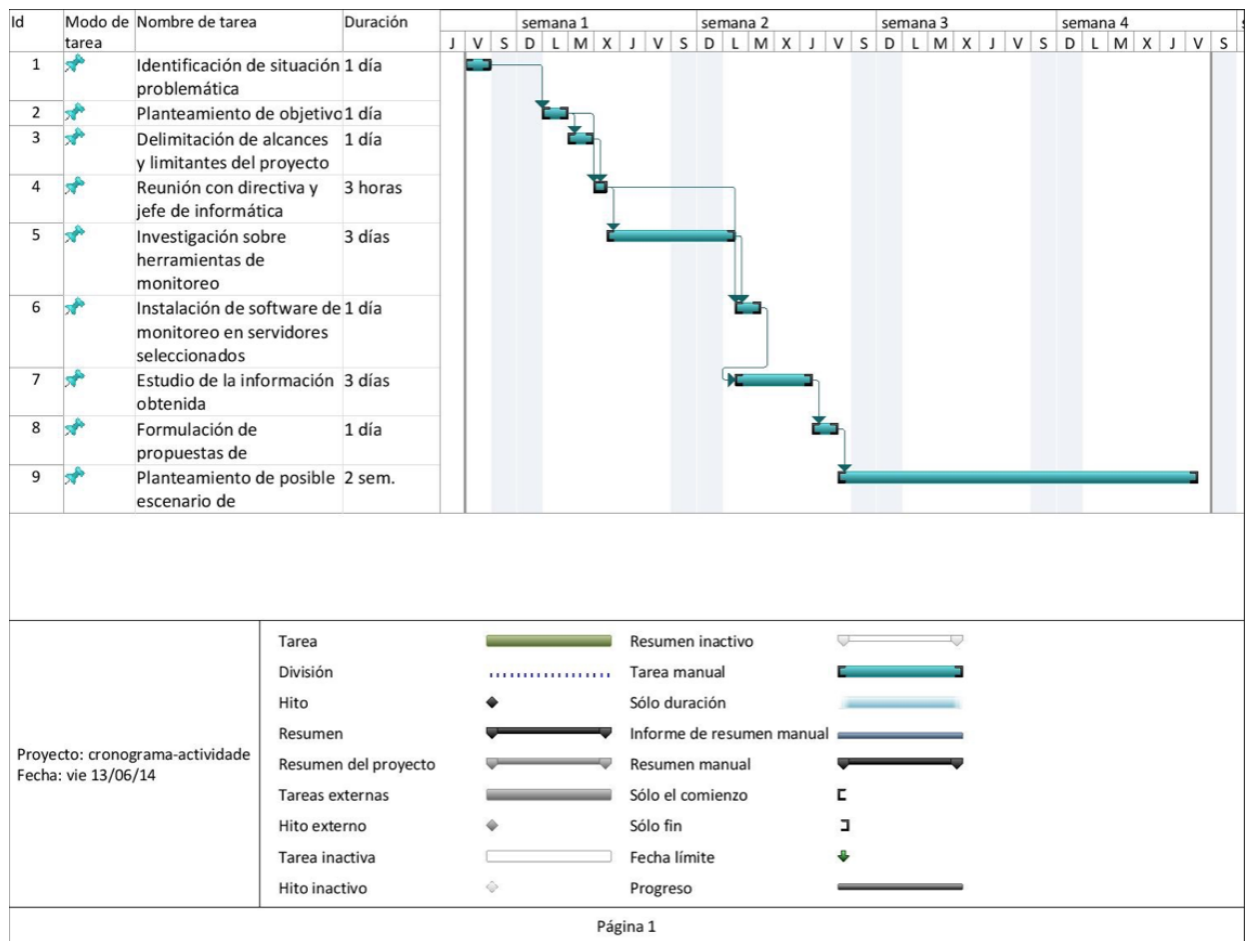
1.4 Justificación

Muchas serian las ventajas que obtendría la empresa Negocios Asociados S. A. del proyecto que realizaremos.

- Conocimiento del rendimiento de sus servidores para la toma de decisiones.
- Redimensionar el disco duro del servidor al momento de una posible migración a un ambiente virtual.
- Optimizar el tamaño de la memoria ram para un mejor desempeño.

- La empresa Negocios Asociados S.A obtendrá nuevo hardware para llevar acabo el proceso de migración.

1.5 Cronograma de actividades



Capítulo 2 - Marco teórico

2.1 Descripción de la Empresa

Grupo ElectroBodegas pertenece a un grupo de empresas hermanas, que se dedican a comercializar productos eléctricos de baja, mediana y alta tensión. Cuenta con un gran número de clientes entre ellos personas, empresas, alcaldías, ONG's, Gobierno Central, además compete en licitaciones para adjudicarse proyectos estatales de presupuesto mediano y grande.

Sitio web de Electro Bodegas: <http://www.electrobodegas.com/>



Figura 2.1: Logo de Electro Bodegas

Ubicación:

La empresa se encuentra en una ubicación accesible desde varios puntos de la capital, en la 27 av. Sur y 6° 10° calle poniente, al sur del parque Cuscatlan.

Empresas hermanas:



Figura 2.2: Mapa de ubicación de Electro Bodegas (Vista satélite Google maps)



Surtielectric

Ubicación: Av. España y
Alameda Juan Pablo II los Próceres.



Csh Ingeniería

Ubicación: Av. España y Alameda
Juan Pablo II los Próceres.



Tecnelec

Ubicación: San Miguel.



Pelsa Panama

2.2 Descripción de las tecnologías, metodologías a utilizar en el proyecto

2.2.1 Metodología a emplear

Para realizar el monitoreo de los servidores se han tomado como referencia dos programas de monitoreo de servidores las cuales fueron Nagios y Zenoss.

Nagios y Zenoss poseen características parecidas, al final del estudio se decidió utilizar Zenoss como herramienta de monitoreo debido a experiencia previa con este. A continuación listamos algunas

diferencias.

2.2.2 Síntesis de las tecnologías a utilizar

Una de las preguntas más comunes de los usuarios de software abierto es la diferencia entre Zenoss y Nagios. Aunque Nagios tiene una de las mayores bases instaladas de cualquier solución de monitoreo está es una pregunta lógica pero Zenoss tiene una serie de características que lo diferencian de Nagios. Nagios es básicamente un planificador que ejecuta comprobaciones de mantenimiento y pruebas contra los dispositivos de red y los reportes regresan los resultados. Nagios también tienen una lista completa de extensiones o plugins que son similar a los plugins de Zenoss. Así que es posible utilizar los plugins de Nagios en Zenoss, ya que proporciona la capacidad de ejecutarlos.

- **Descubrimiento automático** - Zenoss puede descubrir automáticamente hosts y iniciar a monitorizar de forma automática. Nagios requiere que se introduzca de

forma manual en un archivo de configuración.

- **Monitoreo de Rendimiento** - Zenoss puede generar gráficos de series de tiempo del rendimiento. Nagios no puede sin plugins adicionales o software. A menudo los usuarios utilizan el motor gráfico popular llamado Cacti, que aprovecha RRDTool para recopilar datos de series de tiempo.
- **Gestión de Eventos** - Zenoss puede normalizar los datos dentro de eventos, más allá de la colección desde otra fuente y deduplicación los eventos almacenan las ocurrencias en un contador el cual permite a los usuarios configurar alertas basadas en la frecuencias de una alerta.
- **Monitoreo de Logs del sistema** - Zenoss puede monitorear los registros del sistema Unix, Linux, Windows y más. En adición Zenoss puede ser utilizado para traducir los datos dentro de los evento y normalizarlos junto con la disponibilidad y rendimiento recopilados a través de otros métodos como SNMP y SSH.
- **Alertas sofisticadas** - Las alertas de Nagios se pueden enviar a una dirección de correo electrónico o a un localizado basado en ciertas condiciones. Sin embargo, Zenoss tiene un sistema de alerta más robusto, donde las alertas pueden enviarse a una sola persona o a un grupo de individuos. El escalamiento de reglas puede hacerse cumplir de manera que cuando una alertas van sin reconocimiento, puedan ser promovidas a otro operador de red.

NAGIOS

Nagios es un sistema de monitorización de redes ampliamente utilizado, de código abierto, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado. Entre sus carac-

terísticas principales figuran la monitorización de servicios de red (SMTP, POP3, HTTP, SNMP...), la monitorización de los recursos de sistemas hardware (carga del procesador, uso de los discos, memoria, estado de los puertos...), independencia de sistemas operativos, posibilidad de monitorización remota mediante túneles SSL cifrados o SSH, y la posibilidad de programar plugins específicos para nuevos sistemas.

Se trata de un software que proporciona una gran versatilidad para consultar prácticamente cualquier parámetro de interés de un sistema, y genera alertas, que pueden ser recibidas por los responsables correspondientes mediante (entre otros medios) correo electrónico y mensajes SMS, cuando estos parámetros exceden de los márgenes definidos por el administrador de red.

Llamado originalmente Netsaint, nombre que se debió cambiar por coincidencia con otra marca comercial, fue creado y es actualmente mantenido por Ethan Galstad, junto con un grupo de desarrolladores de software que mantienen también varios complementos.

Nagios fue originalmente diseñado para ser ejecutado en GNU/Linux, pero también se ejecuta bien en variantes de Unix.

Nagios está licenciado bajo la GNU General Public License Version 2 publicada por la Free Software Foundation.

CARACTERÍSTICAS

- Monitorización de servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP).
- Monitorización de los recursos de equipos hardware (carga del procesador, uso de los discos, logs del sistema) en varios sistemas operativos, incluso Microsoft Windows con los plugins NRPE_NT o NSClient++.

- Monitorización remota, a través de túneles SSL cifrados o SSH.
- Diseño simple de plugins, que permiten a los usuarios desarrollar sus propios chequeos de servicios dependiendo de sus necesidades, usando sus herramientas preferidas (Bash, C++, Perl, Ruby, Python, PHP, C#. . .).
- Chequeo de servicios paralizados.
- Posibilidad de definir la jerarquía de la red, permitiendo distinguir entre host caídos y host inaccesibles.
- Notificaciones a los contactos cuando ocurren problemas en servicios o hosts, así como cuando son resueltos (a través del correo electrónico, busca personas, Jabber, SMS, o cualquier método definido por el usuario junto con su correspondiente complemento).
- Posibilidad de definir manejadores de eventos que ejecuten al ocurrir un evento de un servicio o host para resoluciones de problemas proactivas.
- Rotación automática del archivo de registro.
- Soporte para implementar hosts de monitores redundantes.
- Visualización del estado de la red en tiempo real a través de interfaz web, con la posibilidad de generar informes y gráficas de comportamiento de los sistemas monitorizados, y visualización del listado de notificaciones enviadas, historial de problemas, archivos de registros. . .

ZENOSS CORE

Zenoss Core es un software abierto, una plataforma de monitoreo de red y sistema que es patrocinado por Zenoss, Inc. la cual desarrolla dos versiones de Zenoss: Core y Enterprise. Core pertenece a la comunidad y es desarrollada por la comunidad.

Enterprise añade algunas características de valor sobre la versión Core, tal vez como una librería extendida de reportes, transacciones web sintéticas, monitores certificados (ZenPacks), y un panel de administración para múltiples instalaciones de Zenoss. Las características adicionales permiten a Zenoss Inc. vender la versión Enterprise como un producto de software comercial con soporte.

Zenoss Core es una solución de monitoreo que puede ser tan complementaria como nosotros lo deseemos. Y mientras que casi cualquier persona puede instalarlo, correrlo, y monitorear “algo,” Zenoss Core está repleto de características en una interfaz complicada. La interfaz ha mejorado drásticamente en la versión 2, pero no es el tipo de software que se puede utilizar de forma intuitiva, un poco de orientación es necesaria.

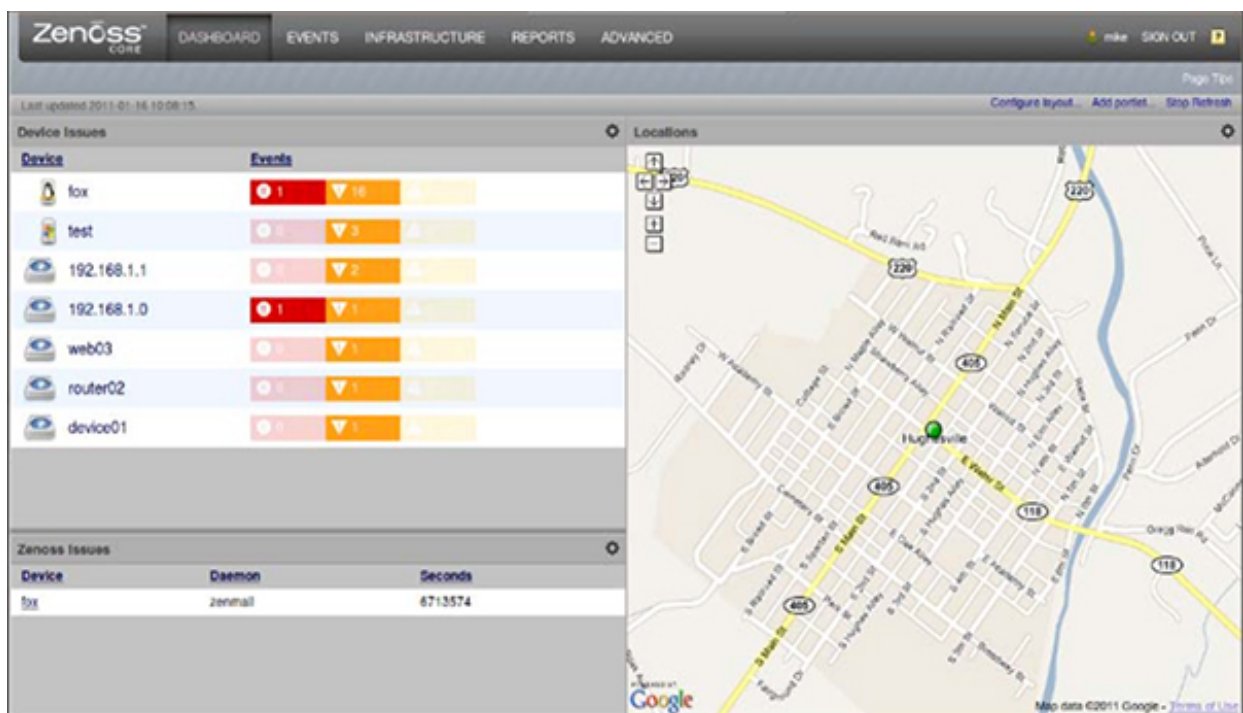
Zenoss Core provee una solución de monitoreo que incorpora los siguientes:

- Gestión de dispositivos
- Monitoreo de disponibilidad
- Gráficos de rendimiento
- Gestión de usuarios y alertas
- Arquitectura de plugins
- Informes de seguimiento

Para monitorear activos de Tecnología de información (Servidores, routers, switches,

sitios web, y cualquier cosa conectada a la red), se debe instalar Zenoss Core en un servidor. A pesar que Zenoss Core está diseñado para ser instalado en un servidor Linux, aplicaciones virtuales están disponibles para permitir a los usuarios de Machintosh y Windows instalar Zenoss core utilizando VMware.

Después de la instalación, usted puede manejar su instalación de Zenoss Core y su configuración de monitorización de una interfaz web. La siguiente imagen muestra la vista del panel:



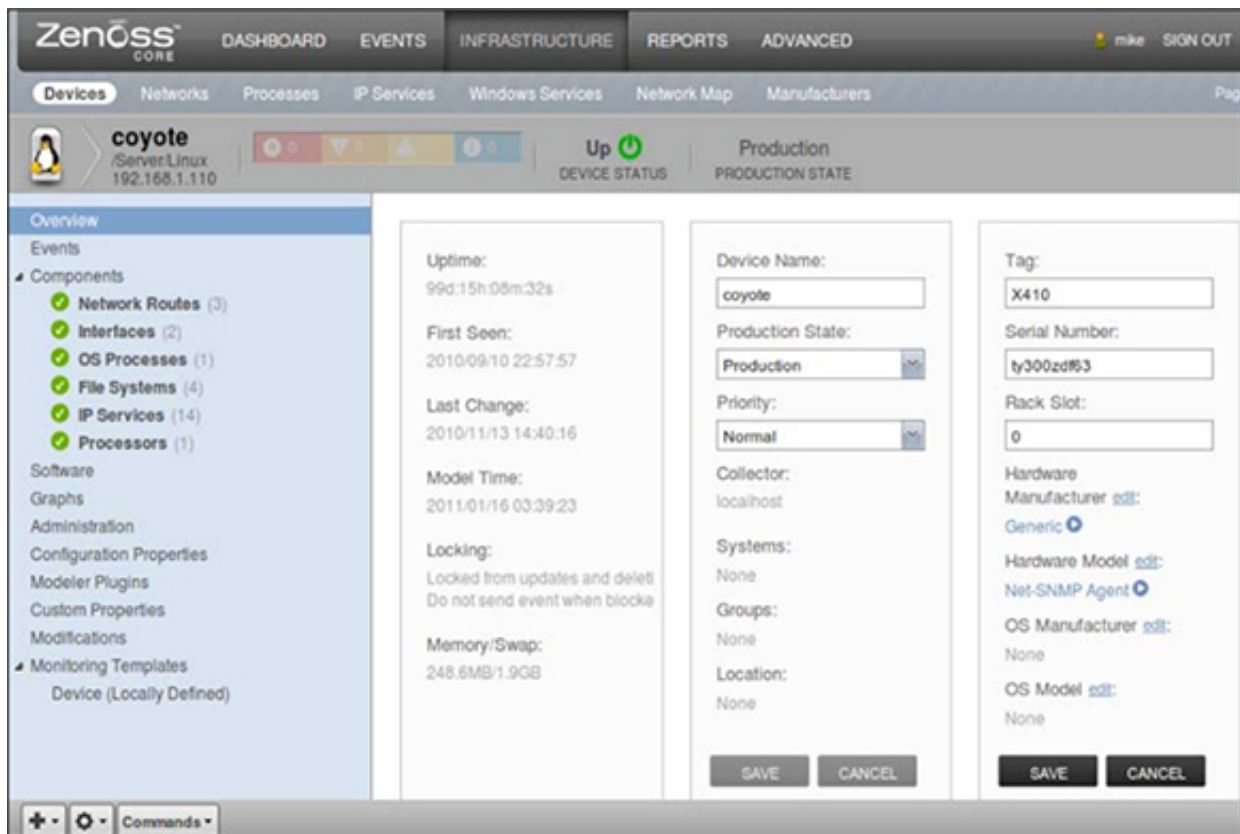
El portal web es la cara del sistema de Zenoss Core y es el lugar donde pasamos la mayor parte de nuestro tiempo. Este provee un único acceso para el sistema de monitoreo y no requiere saber acerca del sistema operativo. La interfaz web ofrecer arrastrar y soltar, portlets que muestra una vista personalizada de la red en cualquier punto.

GESTIÓN DE DISPOSITIVOS

En el corazón de la gestión de dispositivos, Zenoss Core utiliza una Base de Datos de la Gestión de Configuración (CMDB), el cual almacena un modelo del entorno de TI a la CMDB de una en una o por auto-descubrimiento de dispositivos activos al recorrer la tabla de enrutamiento. Los dispositivos son gestionados a través de protocolo simple de administración de red (SNMP), SSH (o Telnet), o escaneos de puertos.

Zenoss Core permite organizar dispositivos por ubicaciones definidas por el usuario, grupos y sistemas. Uno de los más poderosos conceptos organizativos de Zenoss Core es clases, el cual permite definir las características de monitoreo basadas en una clasificación jerárquica de los dispositivos, lo que permite a un dispositivo a heredar las propiedades de seguimiento de su clase padre.

La siguiente captura de pantalla ofrece un vistazo a una página de estado del dispositivo:



MONITORES DE DISPONIBILIDAD Y RENDIMIENTO

Mediante el uso de la motorización ICMP y SNMP, Zenoss Core informa sobre la disponibilidad de los siguiente:

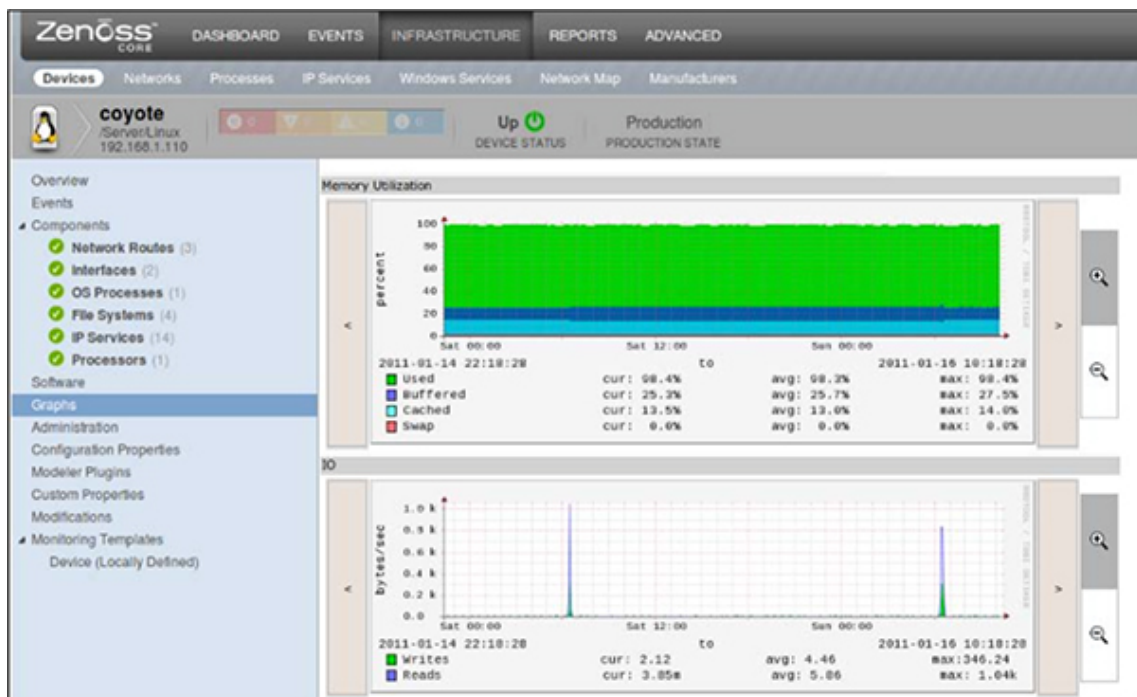
- Dispositivos de red
- Servicios y puerto TCP/IP
- Disponibilidad de URL
- Servicios y procesos de Windows
- Procesos de Linux\UNIX

Zenoss Core está en el nivel 3 de la topología de red, lo cual reduce la cantidad de alertas mediante la creación de un evento solamente sobre el dispositivo problemático y no sobre los dispositivos que dependen de él.

Monitores de rendimiento recopilan datos de series de tiempo y son proporcionados con un análisis gráfico de los siguientes componentes:

- Estadísticas del sistema de ficheros.
- Uso de CPU y memoria.
- Monitoreo de JMX para servidores J2EE (disponible a través de un ZenPack).
- Soporte para plugins Nagios y Cacti.

La siguiente captura de pantalla muestra un gráfico basado en la actividad de monitoreo de Zenoss Core:



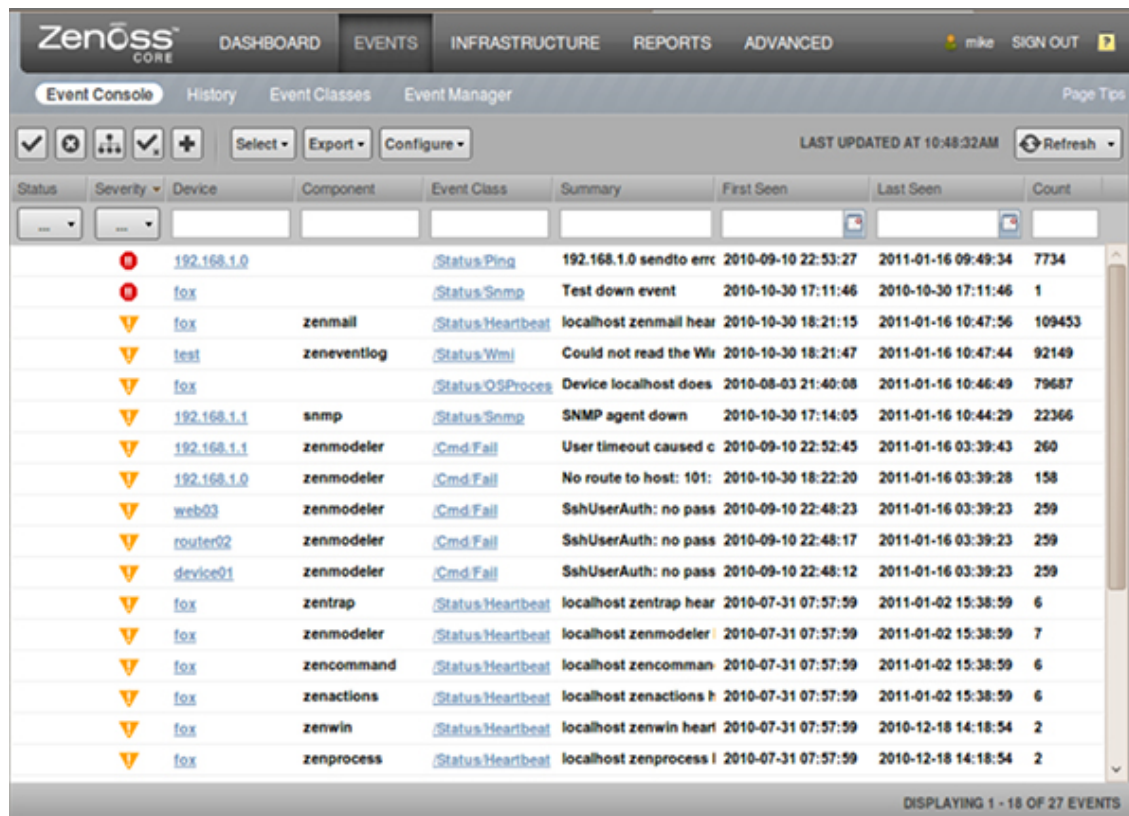
Utilizando el sistema de gestión de eventos incorporado, se puede configurar Zenoss Core para generar un evento si un dispositivo supervisado cruza un umbral definido.

GESTIÓN DE EVENTOS

Zenoss Core monitorea una variedad de recursos en busca de problemas, incluyendo logs del sistema, disponibilidad y monitoreo de rendimiento, trampas SNMP, registros de eventos de Windows y scripts personalizados. Las características principales del sistema de gestión de eventos incluyen:

- Eventos personalizados
- Priorización automática de eventos
- Duplicación de eventos
- Correlación de eventos Arriba\Abajo

La siguiente captura de pantalla muestra la **Consola de Eventos**:



The screenshot shows the Zenoss Core Event Console interface. At the top, there are tabs for DASHBOARD, EVENTS (selected), INFRASTRUCTURE, REPORTS, and ADVANCED. Below the tabs, there's a navigation bar with 'Event Console', 'History', 'Event Classes', and 'Event Manager'. A 'Page Tips' button is on the right. Below the navigation bar, there are buttons for 'Select', 'Export', and 'Configure'. A status bar indicates 'LAST UPDATED AT 10:48:32AM' and a 'Refresh' button. The main area is a table of events with columns: Status, Severity, Device, Component, Event Class, Summary, First Seen, Last Seen, and Count. The table lists various events, including status checks, command failures, and heartbeat events. The bottom of the interface shows 'DISPLAYING 1 - 18 OF 27 EVENTS'.

Status	Severity	Device	Component	Event Class	Summary	First Seen	Last Seen	Count
●	●	192.168.1.0		/Status/Ping	192.168.1.0 sendto emc	2010-09-10 22:53:27	2011-01-16 09:49:34	7734
●	●	fox		/Status/Snmp	Test down event	2010-10-30 17:11:46	2010-10-30 17:11:46	1
▼	▼	fox	zenmail	/Status/Heartbeat	localhost zenmail hear	2010-10-30 18:21:15	2011-01-16 10:47:56	109453
▼	▼	test	zeneventlog	/Status/Wmi	Could not read the Wmi	2010-10-30 18:21:47	2011-01-16 10:47:44	92149
▼	▼	fox		/Status/OSProcess	Device localhost does	2010-08-03 21:40:08	2011-01-16 10:46:49	79687
▼	▼	192.168.1.1	snmp	/Status/Snmp	SNMP agent down	2010-10-30 17:14:05	2011-01-16 10:44:29	22366
▼	▼	192.168.1.1	zenmodeler	/Cmd/Fail	User timeout caused c	2010-09-10 22:52:45	2011-01-16 03:39:43	260
▼	▼	192.168.1.0	zenmodeler	/Cmd/Fail	No route to host: 101:	2010-10-30 18:22:20	2011-01-16 03:39:28	158
▼	▼	web03	zenmodeler	/Cmd/Fail	SshUserAuth: no pass	2010-09-10 22:48:23	2011-01-16 03:39:23	259
▼	▼	router02	zenmodeler	/Cmd/Fail	SshUserAuth: no pass	2010-09-10 22:48:17	2011-01-16 03:39:23	259
▼	▼	device01	zenmodeler	/Cmd/Fail	SshUserAuth: no pass	2010-09-10 22:48:12	2011-01-16 03:39:23	259
▼	▼	fox	zentrap	/Status/Heartbeat	localhost zentrap hear	2010-07-31 07:57:59	2011-01-02 15:38:59	6
▼	▼	fox	zenmodeler	/Status/Heartbeat	localhost zenmodeler	2010-07-31 07:57:59	2011-01-02 15:38:59	7
▼	▼	fox	zencommand	/Status/Heartbeat	localhost zencomman	2010-07-31 07:57:59	2011-01-02 15:38:59	6
▼	▼	fox	zenactions	/Status/Heartbeat	localhost zenactions h	2010-07-31 07:57:59	2011-01-02 15:38:59	6
▼	▼	fox	zenwin	/Status/Heartbeat	localhost zenwin hear	2010-07-31 07:57:59	2010-12-18 14:18:54	2
▼	▼	fox	zenprocess	/Status/Heartbeat	localhost zenprocess i	2010-07-31 07:57:59	2010-12-18 14:18:54	2

El sistema de ventos mitiga eventos duplicados y borra automáticamente eventos cuando el estado de los eventos cambia de inactivo a activo. Zenoss Core también recopilar eventos de secuencias de comandos personalizadas y aplicaciones externas. En respuesta a los acontecimientos, Zenoss Core puede enviar correo electrónico o paginas de alertas, correr un script o no hacer nada. Zenoss Core puede ser configurado para responder a un evento mediante la definición de reglas de alerta. Las reglas de alertas son definidas en base aun usuario o grupo de usuarios.

ARQUITECTURA DE PLUGINS

Zenoss Core ofrece varias maneras para extender la funcionalidad base:

- ZenPacks: Zenoss Core complemento de módulos
- Plugins de Nagios
- Plugins de Cacti

La arquitectura ZenPack permite empaquetar plugins y configuraciones para su distribución a otros usuario y la comunidad en general.

REPORTES DEL SISTEMA

Zenoss Core contiene un conjunto de reportes estándar que permiten ver que está sucediendo en este momento, así como lo que ha sucedido en el pasado. Los informes se integran con la gestión de dispositivos, monitores de rendimiento, eventos y funcionalidades de usuario.

La siguiente captura de pantalla muestra el reporte de Todos los componentes monitoreados:

Device	Component	Type	Description	Status
10.10.10.1	/	Filesystem	/	OK
10.10.10.1	/boot	Filesystem	/boot	OK
10.10.10.1	/home	Filesystem	/home	OK
10.10.10.1	/proc/bus/usb	Filesystem	/proc/bus/usb	OK
10.10.10.1	0	CPU	0	OK
10.10.10.1	Eventlog	WinService	'Event Log' StartName: StartName: LocalSystem	OK
10.10.10.1	apache2	OSProcess	apache2	OK
10.10.10.1	eth0	IpInterface	eth0	OK
10.10.10.1	lo	IpInterface	lo	OK
10.10.10.1	tcp-80	IpService	tcp-80 ip:0.0.0.0	OK
10.10.10.1	user/sbin/apache2 4 start	OSProcess	/usr/sbin/apache2 4 start	OK

INFORMES PERSONALIZADOS DE DISPOSITIVOS

Zenoss Core permite a los usuarios escribir informes personalizados de dispositivos en la interfaz web, como se ven en la siguiente captura de pantalla:

The screenshot displays the Zenoss Core web interface. The top navigation bar includes links for DASHBOARD, EVENTS, INFRASTRUCTURE, REPORTS, and ADVANCED (with a user profile 'mike' and a 'SIGN OUT' button). The breadcrumb trail indicates the current location: Reports > Custom Device Reports > Comments. The page title is 'RRD Graph state at time: 2011/01/16 11:02:45'. The left sidebar contains two links: 'View Report' and 'Edit Report'. The main content area is a form for configuring a custom report. The fields are as follows:

Field	Value
Name	Comments
Title	
Path	/HTTP
Query	here.comments != ""
Sort Column	Name
Sort Sense	asc
Columns	getId comments
Column Names	Name Comment

2.2.3 Cuadros comparativos

Nombre	Nagios	Zenoss
Gráficas	Si	Si
Informes SLA	Si	No
Grupos Lógicos	Si	Si
Estadísticas	Si	Si
Predicción de estadísticas	Si	Si
Autodescubrimiento	Si	Si
Agentes	Si	SNMP, WMI, IMX, etc.
SSMP	A través de plugin	Si
Syslog	Si	Si
Scripts externos	Si	Si
Complementos (plugins)	Si	Si
Creación de complementos	Media	Fácil
Alertas	Si	Si
Aplicación web	Solo virtualización	Control total
Monitorización distribuida	Si	Si
Método de almacenaje de datos	SQL	RRDtool y MySQL
Licencia	GPL	GPL