CAPITULO III

3. PROPUESTA PARA LA REALIZACIÓN DE LA EVALUACION DEL DESEMPEÑO Y PLANIFICACION DE LA CAPACIDAD DEL SERVIDOR SOLARIS DE LA EMPRESA TEXTILERA LA AMERICANA DE LA CIUDAD DE QUITO

Presentación

En la actualidad la tecnología ha evolucionado de manera sorprendente en este sistema globalizado en el que se desempeña la sociedad, siendo la información uno de los recursos más importantes para toda empresa e institución pública o privada, con la aparición de herramientas tecnológicas que facilitan el tratamiento de la información es posible desarrollar aplicaciones que permitan agilizar y obtener mejoras significativas en cuanto al manejo y administración adecuado de los datos.

En nuestro país el sector del comercio se ha convertido en un punto muy importante ya que de aquí se está obteniendo el motor que genera el avance de la nación, por ello se ha visto la necesidad de prestar servicios de alta calidad de acuerdo a la tecnología. La mayoría de las empresas textiles tratan de automatizar todos sus procesos implementando software que contribuya en el desempeño de las actividades que se generen en este sector.

Las empresas textiles tienden a automatizar sus procesos mediante la adquisición de hardware y software, que facilite ofertar y suscribirse a sus servicios en cualquier parte del mundo, con el fin de mantener a sus empleados y clientes satisfechos con un servicio que justifique el adquirir sus productos y de parte de los empleados que les garantice que todas sus actividades estén siendo bien administradas y almacenadas.

Para este fin la empresa de textiles la americana ha creído conveniente invertir en la adquisición de un servidor de grandes prestaciones tecnologías las mismas que se hallan reflejadas en plataforma robusta de Solaris.

Todo bien es siempre una inversión y más aún cuando se trata del sector de la tecnología ya que es el motor que genera actividad a los empleados y que estos a su vez pueden brindar un servicio de calidad a los clientes quienes son los que permiten la existencia o no de las empresas. Cuando una empresa genera información es necesario adquirir equipos tecnológicos que estén en la capacidad de administrar y almacenar información bajo una atenta supervisión de las personas que conozcan de esta área.

Al mismo aseguramiento de la integridad y seguridad debería ser aplicado a los sistemas de computación y datos. La Internet ha facilitado el flujo de información, desde personal hasta financiera. Al mismo tiempo, también ha promovido muchos peligros. Los usuarios maliciosos y crackers buscan objetivos vulnerables tales como sistemas no actualizados, sistemas infectados con troyanos redes ejecutando servicios inseguros, servidores con puertos abiertos que pueden ser potenciales puertas de acceso a la información.

Las alarmas son necesarias para notificar a los administradores y a los miembros del equipo de seguridad que ha ocurrido una entrada ilegal para que los administradores de las redes y los servidores puedan responder en tiempo real a la amenaza. Se han diseñado Servidores de las más diversas plataformas con el fin de facilitar a los administradores su trabajo, y todos los servidores son capaces de brindar distintos servicios como compartir recursos y seguridades a todo nivel.

La empresa como generadora de recursos tanto económicos como profesionales en distintas áreas dentro del país ha buscado desarrollar una manera óptima de alternativa viable para precautelar la generación de la información que se obtiene de las distintas actividades que desarrollan sus directivos, empleados y clientes dentro de la textil.

Justificación

Los procesos automatizados, son factores de vital importancia en las empresas, es necesario que la información sea procesada y almacenada de una forma efectiva para agilizar los procesos de control y así lograr seguridad y efectividad en las actividades que se realizan dentro de la empresa. Con una evaluación de las seguridades y

comprobando o agilitando de mejor manera los recursos que puede brindar la plataforma tecnológica Solaris

A nivel de servidor el compromiso es disponer de una evaluación adecuada al servidor Solaris sparc 10 el mismo que hace las funciones de firewall para precautelar la información que se genera en empresa, y que a su vez administra la Base de datos haciendo las veces de servidor de aplicaciones y de proxy para el envió recepción del internet.

La evaluación se lo va a realizar mediante la aplicación de procesos que tienen que ver con estándares internacionales los mismos que norman las seguridades de la información y los procesos.

Objetivos

Objetivo general

Evaluar el desempeño y planificar la capacidad que puede brindar el servidor Solaris sparc 10 de la empresa textil la Americana de la ciudad de Quito

Objetivo Especifico

- Analizar el desempeño del servidor sparc tomado en cuenta los estándares internacionales de seguridad, eficiencia y eficacia.

- Diseñar una adecuada planificación para que el servidor sea explotado a su máximo nivel siempre precautelando la información que se genere en la empresa textil La americana.

- Obtener un manual del desempeño del servidor el mismo que sea un aporte para los administradores.

SISTEMA OPERATIVO SOLARIS

Solaris es un sistema operativo de tipo Unix desarrollado desde 1992 inicialmente por Sun Microsystems y actualmente por Oracle Corporation como sucesor de SunOS. Es un sistema certificado oficialmente como versión de Unix. Funciona en arquitecturas SPARC y x86 para servidores y estaciones de trabajo.

El primer sistema operativo de Sun nació en 1983 y se llamó inicialmente SunOS. Estaba basado en el sistema UNIX BSD, de la Universidad de Berkeley, del cual uno de los fundadores de la compañía fue programador en sus tiempos universitarios. Más adelante incorporó funcionalidades del System V, convirtiéndose prácticamente en un sistema operativo totalmente basado en System V.

Esta versión basada en System V fue publicada en 1992 y fue la primera en llamarse Solaris, más concretamente *Solaris 2*. Las anteriores fueron llamadas *Solaris 1* con efecto retroactivo. SunOS solo tendría sentido a partir de ese momento como núcleo de este nuevo entorno operativo Solaris. De esta forma Solaris 2 contenía SunOS 5.0. Desde ese momento se distingue entre el núcleo del sistema operativo (SunOS), y el entorno operativo en general (Solaris), añadiéndole otros paquetes como Apache o DTrace. Como ejemplo de esta función, Solaris 8 contiene SunOS 5.8.

Solaris usa una base de código común para las arquitecturas que soporta: SPARC y x86 (incluyendo AMD64/EM64T). También fue portado a la arquitectura PowerPC (en plataforma PReP) en la versión 2.5.1, pero el porte fue cancelado casi tan pronto como fue liberado. En un tiempo se planeó soporte para el Itanium pero nunca se llevó al mercado. Sun también tiene planes de implementar ABIs de Linux en Solaris 10, permitiendo la ejecución de código objeto Linux de forma nativa en la plataforma x86, lo cual sería facilitado por el hecho de que ambos sistemas operativos utilizan el formato ejecutable Executable and Linkable Format. Por el momento, Sun ha adoptado la tecnología Lxrun[2] y la ofrece como descarga gratuita, si bien no está incorporada a la distribución base. Solaris tiene una reputación de ser muy adecuado para el multiprocesamiento simétrico (SMP), soportando un gran número de CPUs. También ha incluido soporte para aplicaciones de 64

bits SPARC desde Solaris 7. Históricamente Solaris ha estado firmemente integrado con la plataforma hardware de Sun, SPARC, con la cual fue diseñado y promocionado como un paquete combinado. Esto proporcionaba frecuentemente unos sistemas más fiables pero con un coste más elevado que el del hardware de PC. De todas formas, también ha soportado sistemas x86 desde la versión Solaris 2.1 y la última versión, Solaris 10, ha sido diseñada con AMD64 en mente, permitiendo a Sun capitalizar en la disponibilidad de CPUs de 64 bits commodities basadas en la arquitectura AMD64. Sun ha promocionado intensamente Solaris con sus estaciones de trabajo de nivel de entrada basadas en AMD64, ha dejado de ofrecer estaciones de trabajo basadas en arquitectura SPARC, reemplazándolas por modelos basados en Intel Core 2 y AMD64.

3.1. Factibilidad

Para poder obtener las factibilidades tanto técnicas como tecnológicas y económicas debemos partir de los siguientes potenciales con que cuenta la plataforma tecnológica Solaris.

3.1.1. Factibilidad Técnica

PORTABILIDAD: El software conformado por una ABI aplicación de interfaces binaria (Application Binary Interface) ejecuta con un Shrink-wrapped (Contracción envuelta) el software en todos los sistemas vendidos con la misma arquitectura del microprocesador. Esto obliga a los desarrolladores de aplicaciones a reducir el costo del desarrollo del software y traer productos al mercado rápidamente, y obliga a los usuarios a actualizar el hardware mientras retienen sus aplicaciones de software y minimizan sus costos de conversión.

ESCALABILIDAD: Las aplicaciones se usan con más frecuencia en el sobre tiempo, y requiere sistemas más poderosos para soportarlos. Para operar en un ambiente creciente, el software debe ser capaz de ejecutar en un rango de ancho

poderoso y debe ser capaz de tomar ventajas del poder adicional que se está procesando.

INTEROPERATIBIDAD: La computación del ambiente heterogéneo es una realidad hoy. Los usuarios compran de muchos vendedores para implementar la solución que necesitan. La estandarización y una clara interface son criterios para un ambiente heterogéneo, permitiendo a los usuarios desarrollar estrategias para comunicarse por medio de su red. El sistema operativo de Solaris puede interoperar con unos sistemas muy populares hoy en el mercado, y aplicaciones que se ejecutan en UNIX se pueden comunicar fácilmente.

COMPATIBILIDAD: La tecnología de la computación continúa avanzando rápidamente, pero necesita permanecer en el ámbito competitivo para minimizar sus costos y maximizar sus ingresos

3.1.2. Factibilidad Económica

El comprar un equipo sun de la empresa Oracle siempre va a ser una inversión toda vez que ya vienen previamente instalados la plataforma tecnológica Solaris, está plataforma que en nuestro país todavía es insipiente su aprendizaje, resulta ser de las más poderosas a nivel mundial y los costos son muy inferiores a los que maneja la empresa Microsoft con sus productos Windows sea este 2003 server o el 2008 server que superan los precios en una proporción de un 500%, al igual que la empresa que distribuye las divisiones de Centos, Fedora y Red Hat que de acuerdo al mantenimiento y la división de hardware resulta mucho más conveniente.

3.1.3. Factibilidad Operacional

Dentro de las características de los usuarios tenemos: ESPACIO DE TRABAJO PARA EL ADMINISTRADOR (A workspace manager): cuenta con una ventana de manejo de servicios rápidos (open, close, more, etc.), así como herramientas el

cual le permite al usuario entallar su espacio de trabajo a sus necesidades personales. INTEGRACION DE SERVICIOS DESKTOP (Desktop Integration Services): incluyen ToolTalk, Drag and Drop (arrastrar y soltar), y cut and paste (cortar y pegar), proporcionando la base para que a las aplicaciones puedan integrarse unos con otros. BIBLIOTECAS GRAFICAS (Graphics Libraries): incluye XGL, Xlib, PEX, y XIL, proporcionando soporte para aplicaciones de 2D y 3D. Sistema Operativo I Solaris.

ADMINISTRADOR DE CALENDARIO (Calendar Manager): posee una aplicación de administrador de tiempo que despliega citas y todos los compromisos del día, semana, o un mes en una ojeada. También contiene un Multibrowse que hace un programa de reuniones entre un grupo de usuarios más fácil. Varios calendarios pueden ser cubiertos simultáneamente para determinar la conveniencia de la hora de una reunión en una ojeada. HERRAMIENTA DE IMAGEN (Image Tool): permite cargar, ver y salvar imágenes en 40 diferentes formatos incluyendo PICT, PostScript (TM), TIFF, GIF, JFIF, y muchas más. Otras herramientas incluyen una herramienta de impresión, audio, shell, reloj, y editor de texto.

El Sistema Solaris ofrece una variedad de herramientas nuevas para el administrador como lo son: Dispositivo de Información: los administradores pueden usar estos accesorios opcionales para obtener información sobre dispositivos instalados incluyendo nombres, atributos, y accesibilidad. Sistema de Administración de Archivo: estos accesorios permiten a los administradores crear, copiar, amontonar, depurar, reparar y desmontar sistemas de archivos, crear y remover cadenas de archivos y nombrar tuberías o pipes, y manejar volúmenes. Manejo del Proceso: este controla la agenda de control del sistema. Usando estos accesorios, administradores pueden generar reportes sobre el desempeño, entrada de identificación, ubicación del acceso a discos, y buscar la manera de afinar el desempeño del sistema. Usuarios y el manejo del grupo: con estos accesorios, un administrador puede crear y eliminar entradas en grupos y entradas de identificación del sistema, y asignar grupos e IDs de usuario. *Sistema Operativo I Solaris.*

Seguridad: El ASET (Automated Security Enhancement Tool) es un accesorio que incrementa la seguridad porque permite a los administradores de sistemas revisar archivos del sistema incluyendo permisos, pertenencia, y contenido del archivo. El ASET alerta a los usuarios acerca de problemas de seguridad potencial y donde es apropiado colocar el sistema de archivos automáticamente de acuerdo a los niveles de seguridad especificados. PAQUETES DE SOFTWARE Y CLUSTERS El software del sistema de Solaris es entregado en unidades conocidos como paquetes. Un paquete es una colección de archivos y directorios requeridos para el producto de un software. Un cluster (racimo) es una colección de paquetes. Hay 4 tipos de clusters: Núcleo del Soporte del Sistema (Core System Support): es el software de configuración mínima; contiene solo el software necesario para iniciar el funcionamiento del computador y ejecutar el ambiente operativo de Solaris. Sistema de Soporte para Usuarios Finales (End User System Support): contiene el Núcleo del Soporte del Sistema más el Sistema de soporte para usuarios finales, como lo es el Open Windows sistema de ventanas y aplicaciones de archivos DeskSet relacionados; este cluster incluye el software recomendado para un usuario final. Soporte de Sistemas Desarrollados (Developer System Support): contiene soporte de usuario final del sistema más librerías, incluye archivos y herramientas que se necesitan para desarrollar el software en el sistema de Solaris. Compiladores y depuradores no están incluidos en el sistema de Solaris 2.5. Distribución Entera (Entire Distribution): contiene todo el ambiente de Solaris

3.2. Distribución de equipos en una Red

3.2.1. Acceso Ilimitado a Internet

Hoy en día la gente se encuentra inundada de información y a menudo recibía más de la que podría manejar. El diluvio de información, con más revistas que leer, más publicaciones comerciales a mantener, más anuncios, más llamadas telefónicas y más reuniones, se convirtió en la corriente interminable de los bits de información.

Una de las ventajas es la navegación a altas velocidades sin restricción alguna, pero la seguridad en cambio se ve limitada y puede la empresa ser presa fácil de los piratas electrónicos que podrían incluso desde alterar información hasta perjudicar económicamente a una empresa.

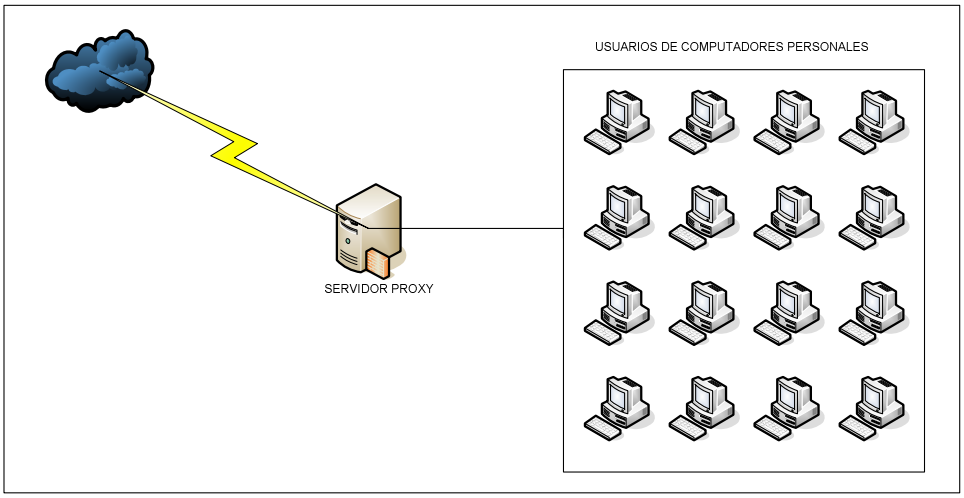

Figura 3.1: Representación Grafica del Acceso Ilimitado a Internet

Fuente: Grupo Investigador

3.2.2. Acceso Limitado a Internet

En este caso vamos a tomar en cuenta las configuraciones que se siguieron para poder configurar el servidor Proxy, el mismo que nos sirvió para distribuir de manera adecuada el ancho de banda como también nos permitió interactuar con un servidor firewall para restringir el acceso libre a nuestra red desde el exterior de la misma.

1. Empezamos cargando Solaris con la contraseña del administrador que para el caso del código abierto es el *root*, como podemos observar en el caso del Solaris 10 cuenta con un entorno parecido a todas las versiones de la empresa Sun.

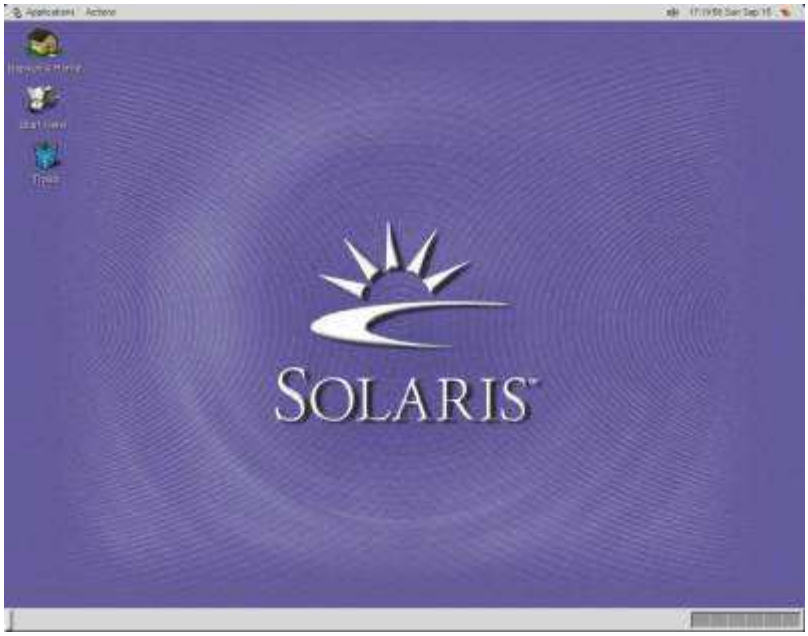

Figura 3.2: Representación Grafica del Acceso a Solaris

Fuente: Grupo Investigador

2. El entorno del sistema operativo es el siguiente en el cual, procedemos acudir al Terminal el mismo que nos ayudara para interactuar con el Solaris mediante una consola de comandos.

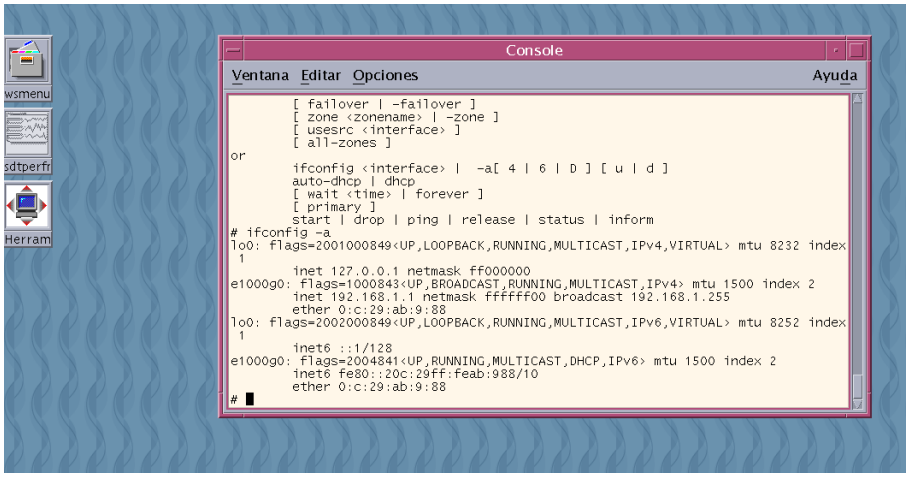

Figura 3.3: Escritorio de Solaris

Fuente: Grupo Investigador

Una parte de la configuración la misma que nos permite conocer cómo se encuentra trabajando el servidor de Solaris y cuál es el rendimiento efectivo de esta infraestructura tecnológica es un paquete parecido a lo que hace el mrtg en Linux o en Windows.

```
#Recommended minimum configuration:
acl all src 0.0.0.0/0.0.0.0
acl manager proto cache_object
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443 563
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443 563     # https, snews
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT
acl Red src 10.0.0.0/255.255.255.0
#Sitios denegados
acl negados url_regex "/etc/squid/sitios-denegados"
#Autentificacion de usuarios
#acl password proxy_auth REQUIRED
#  TAG: http_access
#     Allowing or Denying access based on defined access lists
#
#     Access to the HTTP port:
#     http_access allow|deny [!]aclname ...
#
#     NOTE on default values:
#
#     If there are no "access" lines present, the default is to deny
#     the request.
#
#     If none of the "access" lines cause a match, the default is the
#     opposite of the last line in the list.  If the last line was
#     deny, then the default is allow.  Conversely, if the last line
#     is allow, the default will be deny.  For these reasons, it is a
#     good idea to have an "deny all" or "allow all" entry at the end
```

```
#      of your access lists to avoid potential confusion.
#
#Default:
# http_access deny all
#
#Recommended minimum configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager
# Deny requests to unknown ports
http_access deny !Safe_ports
# Deny CONNECT to other than SSL ports
http_access deny CONNECT !SSL_ports
```

En estas líneas de código tenemos que se encuentra la información de todos los puertos que se encuentran abiertos en el servidor central teniendo en cuenta que siempre se va a tener abiertos los de navegación tanto los del servidor de http como los de https.

Todos los puertos se encuentran con las seguridades que posee el Solaris es decir encripta sus cuentas con Security Socket Layer o SSL como se lo abrevia todo esto sin necesidad de pagar la membrecía que se exige de parte de las empresas que comercializan este tipo de servicio.

3.3. Implementación de seguridades Lógicas mediante Firewall

3.3.1. Local (Interna)

Para garantizar la información interna de una empresa o institución hay que tomar en cuenta tres factores que son decisivos a la hora de implementar seguridades tanto a nivel de red como de servidores. Estos dos factores son:

- Administración del Acceso a Red
- Administración de los privilegios
- Administración de las Contraseñas

3.3.1.1. Administración del Acceso a Red

El acceso a la información y los procesos de negocio debe ser controlados sobre la base de los requerimientos la seguridad y de los negocios.

Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información. Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema.

3.3.1.2. Administración del servidor

Se debe limitar y controlar la asignación y uso de privilegios (cualquier característica o servicio de un sistema de información multi-usuario que permita que el usuario pase por alto los controles de sistemas o aplicaciones). El uso inadecuado de los privilegios del sistema resulta frecuentemente en el más importante factor que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multi-usuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Deben identificarse los privilegios asociados a cada producto del sistema por ej. Sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

b) Los privilegios deben asignarse a individuos sobre las bases de la necesidad de uso y evento por evento, por ej. El requerimiento mínimo para su rol funcional solo cuando sea necesario.

c) Se debe mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso de autorización.

d) Se debe promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

e) Los privilegios deben asignarse a una identidad de usuario diferente de aquellas utilizadas en las actividades comerciales normales.

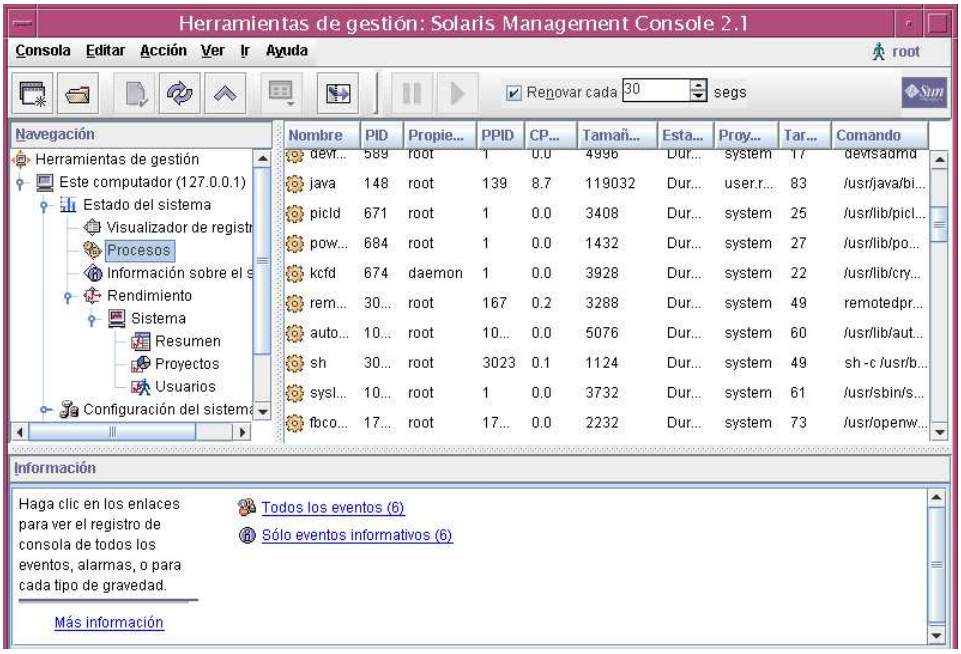

Figura 3.4: Herramienta de Administración de servicios del servidor Solaris 10

Fuente: Grupo Investigador

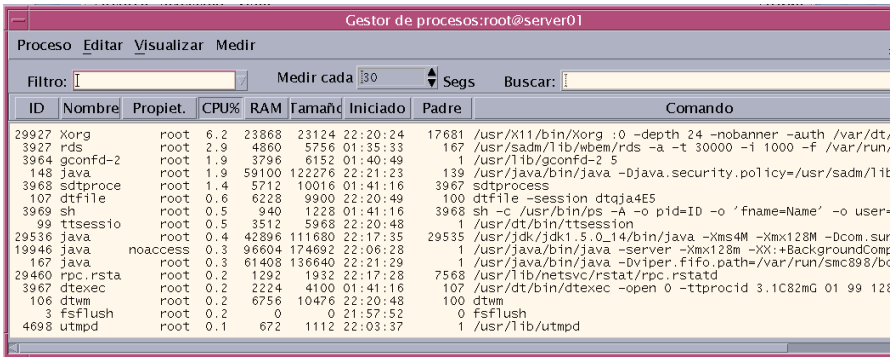

Figura 3.5: Administración de procesos en el servidor de Solaris 10

Fuente: Grupo Investigador

En horas pico cuando el servidor se encuentra ejecutando casi 200 procesos a la vez el sistema tiende a realizar una transacción casi a una velocidad de 1ms lo que es relativamente lento ya que no justificaría bajo ningún concepto la administración local ni remota de los usuarios.

3.3.1.3. Administración de Contraseñas

Las contraseñas constituyen un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información. La asignación de contraseñas debe controlarse a través de un proceso de administración formal, mediante el cual debe llevarse a cabo lo siguiente:

a) requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo (esto podría incluirse en los términos y condiciones de empleo.

b) Garantizar, cuando se requiera que los usuarios mantengan a sus propias contraseñas, que se provea inicialmente a los mismos de una contraseña provisoria segura, que deberán cambiar de inmediato. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, solo debe suministrarse una vez identificado el usuario.

c) Requerir contraseñas provisorias para otorgar a los usuarios de manera segura. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro). Los usuarios deben acusar recibo de la recepción de la clave (password). Las contraseñas nunca deben ser almacenadas en sistemas informativos sin protección. Se resulta pertinente, se debe considerar el uso de otras tecnologías de identificación y autenticación de usuarios, como la biométrica, por Ej... verificación de huellas dactilares, verificación de firma y uso de "tokens" de hardware, como las tarjetas de circuito integrado ("chip-cards").

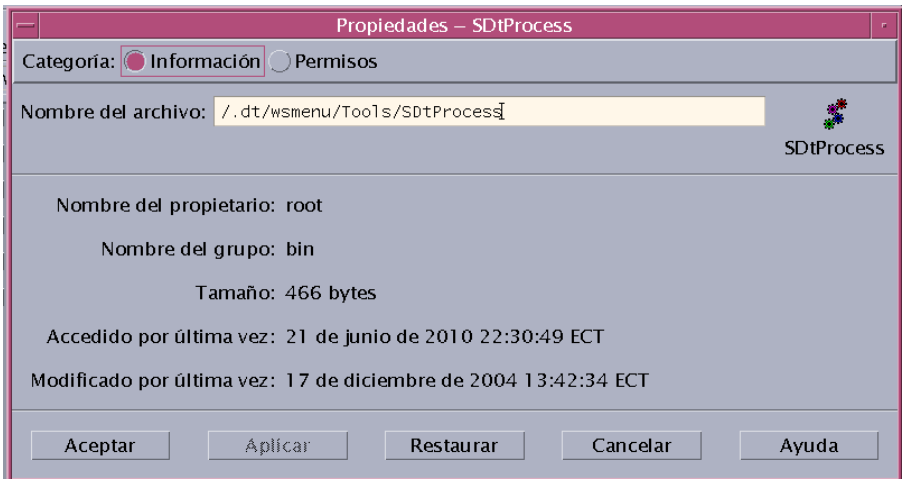

Figura 3.6: Administración de procesos

Fuente: Grupo Investigador

En esta grafica se puede observar las fuentes de los procesos que se tienen cuando se selecciona los servicios que se desea ejecutar y más aun todas las propiedades con las que cuentan los procesos los usuarios que pueden acceder, etc.

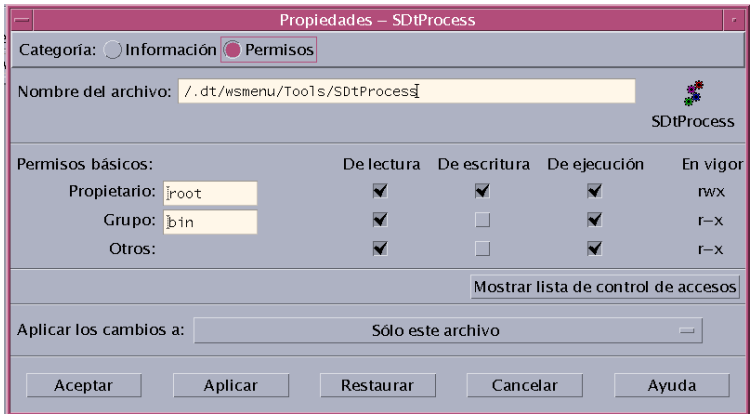

Figura 3.7: Perfiles de usuarios de acuerdo a los procesos

Fuente: Grupo Investigador

En esta pantalla podemos observar cómo se define los privilegios de los usuarios de acuerdo al nivel de responsabilidades, es necesario notar que este sistema operativo o plataforma tecnología si cuenta con súper usuarios es decir el root el cuenta con todos los privilegios en todos los procesos

3.3.2. Externa

Administrar la seguridad de la información dentro de la empresa. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

Deben establecerse adecuados foros de gestión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización, una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ej., comprometiendo la cooperación y colaboración de gerentes, usuarios, administradores, diseñadores de aplicaciones, auditores y personal de seguridad, y expertos en áreas como seguros y administración de riesgos.

Bajo estas premisas nosotras hemos planteado la opción de la implementación de un firewall mediante la utilización de los IPTABLE los mismos que su configuración se asemeja mucho la del squid salvo con algunas actividades que vamos a detallar a continuación:

IPTABLE.

iptables incluye un módulo que permite a los administradores inspeccionar y restringir conexiones a servicios disponibles en una red interna conocido como *seguimiento de conexiones*. El seguimiento de conexiones almacena las conexiones en una tabla, lo que permite a los administradores otorgar o negar acceso basado en los siguientes estados de conexiones:

- NEW. Un paquete solicitando una nueva conexión, tal como una petición HTTP.
- ESTABLISHED. Un paquete que es parte de una conexión existente.
- RELATED. Un paquete que está solicitando una nueva conexión pero que es parte de una conexión existente, tal como las conexiones FTP pasivas donde el puerto de conexión es 20, pero el puerto de transferencia puede ser cualquiera desocupado más allá del puerto 1024.
- INVALID. Un paquete que no forma parte de
- ninguna conexión en la tabla de seguimiento de conexiones.

Puede utilizar la funcionalidad de vigilancia continua de seguimiento de conexiones de iptables con un protocolo de red, aún si el protocolo mismo es sin supervisión (tal como UDP). La configuración del Firewall es la siguiente mediante la utilización de los IPTABLES:

```
# Política denegar y solo se permitirá pasar por el firewall aquello que se permita explícitamente.

# Carga del modulo NAT (esto carga también los otros).
modprobe iptable_nat

# Carga de módulos para solucionar problema de FTP en con IPTABLES
modprobe ip_conntrack_ftp
modprobe ip_nat_ftp

# Reseteo de las reglas ( flush )
iptables -F
iptables -t nat -F
```

```
# SNAT en POSTROUTONG de la interfase pública (eth0) para los paquetes
# provenientes de 10.0.0.0/23 (red administrativa)
# y 10.0.0.0/23 (red académica)
iptables -t nat -A POSTROUTING -s 10.0.0.0/23  -o eth0 -j SNAT --to-source
192.168.0.133
iptables -t nat -A POSTROUTING -s 10.0.0.0/23  -o eth0 -j SNAT --to-source
192.168.0.133
iptables -t nat -A POSTROUTING -s 192.168.0.153/255.255.255.0 -o eth0 -j
SNAT --to-source 192.168.0.133

#Filtrado de paquetes entre la RED LAN LOCAL y los DMZ.

#iptables -A FORWARD -d 192.168.0.155 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -i eth0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -o eth0 -p tcp --dport 80 -j ACCEPT
iptables -A FORWARD -s 10.2.0.0/23 -d 192.168.0.155/29 -p tcp --dport 80 -
j ACCEPT
iptables -A FORWARD -s 192.168.0.155/29 -d 10.2.0.0/23 -p tcp --dport 80 -
j ACCEPT

# negamos todo

iptables -A FORWARD -d 192.168.0.152/29 -j DROP


# Filtrado de paquetes entre las redes internas eth1 (administrativa)
# y eth2 (academic)

iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.2 -p tcp --dport 80 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.2 -p tcp --sport 80 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.2 -p tcp --dport 5101 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.2 -p tcp --sport 5101 -j
ACCEPT


# Regla que permite el paso de paquetes de la red administrativa al
Servidor de Internet red académica
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 80 -j
ACCEPT
```

```
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 80 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 3306 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 3306 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 22 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 22 -j
ACCEPT
iptables -A FORWARD -i eth1 -o eth2 -d 10.0.0.3 -p tcp --dport 23 -j
ACCEPT
iptables -A FORWARD -i eth2 -o eth1 -s 10.0.0.3 -p tcp --sport 23 -j
ACCEPT

#negamos todo
iptables -A FORWARD -i eth2 -o eth1 -j DROP
iptables -A FORWARD -i eth1 -o eth2 -j DROP


# Regla que envía los pedidos 192.188.58.157:5101 del firewall
# a 10.0.0.3:5101 en el servidor de la red interna
iptables -t nat -A PREROUTING -i eth0 -p tcp -d 192.168.0.133 --dport 5101
-j DNAT --to 10.0.0.3:5101

# Activa el reenvié de IP (IP forwarding)
echo 1 > /proc/sys/net/ipv4/ip_forward
```

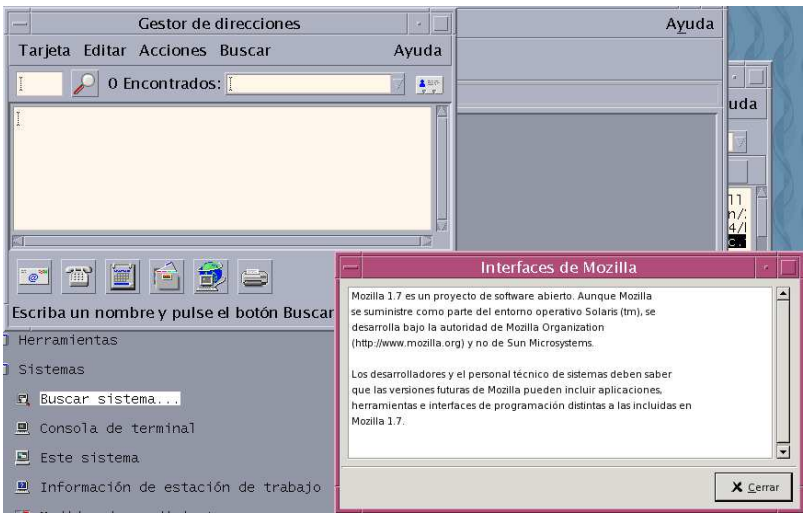

Figura 3.8: Administrador de direcciones web permitidas

Fuente: Grupo Investigador

3.4. Administración de los recursos del servidor a nivel local

Los puertos están dados de acuerdo al servicio que se desea brindar y cada unos de los procesos o servicios están dados de acuerdo a las necesidades que tenga la empresa a una hora determinada o para los servicios que se desean brindar en un determinado momento.

Figura 3.9: Medidor de rendimiento en horas pico

Fuente: Grupo Investigador

3.5. Asignación de IP´s de acuerdo a las necesidades

Para la configuración tanto del squid como del firewall el computador tiene que tener cuando menos 2 tarjetas de red la una que seria quien de la cara al exterior y la otra que va a ser la de configuración de la red interna de las empresas o las instituciones.

Cuando configuramos las tarjetas de red, el Linux por defecto configura todo el rango de direcciones IP, para que puedan acceder todos los usuarios que deseen, pero las reglas que se den en el firewall van a ser las que nos den el numero de maquinas y los privilegios de acceso.

La configuración quedaría de la siguiente manera luego de poner el comando *ifconfig*, que es el comando que detalla las configuraciones de las tarjetas de red.

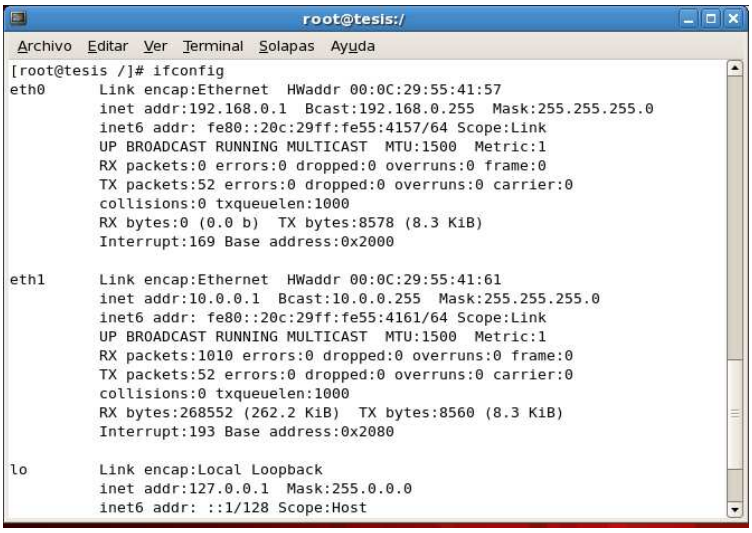

Figura 3.10: Configuración Tarjetas de Red

Fuente: Grupo Investigador

Por lo tanto, se desprende que en nuestro host contamos con 2 tarjetas de red las mismas que tienen las direcciones IP: 192.168.1.1 que es la que va a dar la cara al exterior y la otra tarjeta de red tiene la dirección IP: 10.0.0.1 que seria el servidor de la intranet, o para el Proxy de nuestra red

3.6. Asignación de flujo de trafico de acuerdo a perfiles

Están dadas de acuerdo a las reglas que se pusieron en el firewall, las mismas que fueron dadas para tiempo, impedir que se abran paginas que resten el ancho de banda así como también las paginas denominadas pornográficas o que por su contenido deben ser administradas por personas de criterio formado.

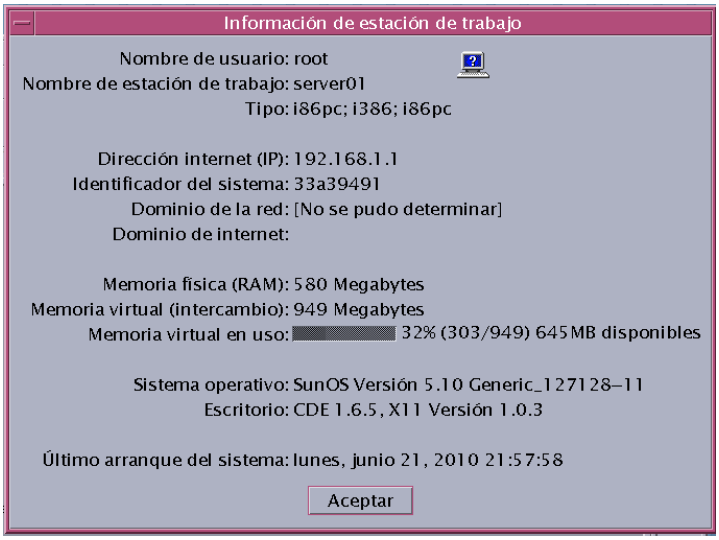

Figura 3.11: Escritorio de Solaris

Fuente: Grupo Investigador

Por último podemos observar las características del servidor que se encuentra trabajando en la actualidad en la empresa de textiles La Americana de la ciudad de Quito foto que fue tomada momentos antes de la impresión de la tesis final el día 21 de Junio del 2010 luego de terminada la jornada de trabajo de todos los señores empleados y una vez que se sacaron los respaldos en dispositivos magnéticos del día de labores

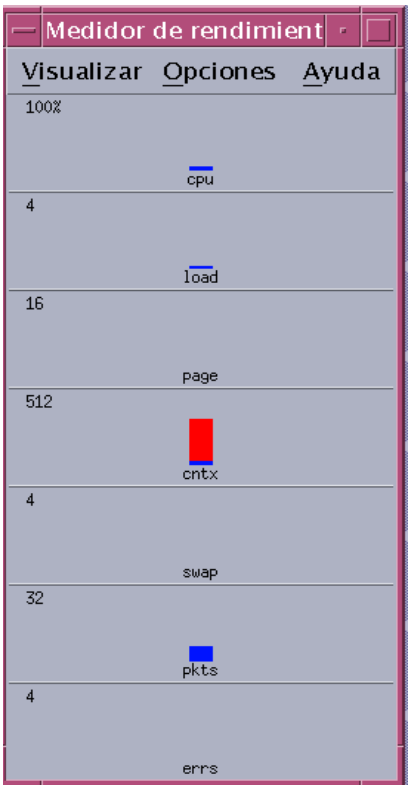

Figura 3.12: Grafica del rendimiento del servidor

Fuente: Grupo Investigador

Podemos notar que el servidor de Solaris en horas pico su rendimiento alcanza apenas el 50% de su potencial y cuando se inicia sus actividades o al medio día mientras se saca respaldados o algunas actividades que no implica mayor riesgo se obtiene apenas un 10%.