

41132
60



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

**ESCUELA NACIONAL DE ESTUDIOS PROFESIONALES
CAMPUS ARAGÓN**

**“MIGRACIÓN DE PLATAFORMA Y
ADMINISTRACIÓN DEL SERVIDOR WEB ARGON DE
LA DGSCA A UN EQUIPO SUN ENTERPRISE 10000”**

T E S I S
QUE PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN

P R E S E N T A:

SANDRA SÁNCHEZ FERNÁNDEZ DE LARA

**ASESOR DE TESIS:
M. EN C. MARCELO PÉREZ MEDEL**



**TESIS CON
FALLA DE ORIGEN**

MÉXICO, 2003.

A



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

**TESIS
CON
FALLA DE
ORIGEN**

PAGINACION DISCONTINUA

AGRADECIMIENTOS

A mis padres,

Por haberme apoyado desde niña para cumplir mis metas sin escatimar esfuerzo alguno sacrificaron parte de su vida para forjarme y educarme. Y aunque mi padre no esté presente con nosotros, donde esté estará orgulloso de los logros que he alcanzado. Cada uno de ellos fueron gracias a que creyó en mí. A mi madre le agradezco infinitamente por brindarme la fortaleza de seguir siempre triunfante, por forjarme los valores que poseo, por el enorme sacrificio para brindarme una carrera Universitaria y por el amor que me brinda.

A Marco Antonio Mejía,

Por creer en mí y apoyarme en la culminación de este proyecto de Tesis. Gran parte de mi desarrollo profesional ha sido gracias a ti, agradezco cada una de tus enseñanzas. Y a pesar de los inconvenientes que tiene la vida has sido paciente, todo gracias a tu amor que valoro enormemente.

A mi Asesor de Tesis,

Mtro. Marcelo, le agradezco su paciencia y dedicación para dirigir este proyecto.

A mis profesores,

Por su enorme trabajo que hicieron cada uno al preocuparse por darme parte de su sabiduría de forma incondicional. En cada etapa de mi vida todos los profesores fueron importantes, pero los profesores de la Universidad fueron lo que enseñaron a valorar lo maravilloso que es aprender buscando el conocimiento.

A mis Abuelos y Tíos,

Por haberme brindado su amor y apoyo día con día.

A Mariene,

Por ser la amiga que siempre esperé, por esos días llenos de alegría y ternura desde la Universidad hasta la actualidad.

A mis amigos,

Por estar cuando lo he necesitado y por todos aquellos momentos llenos de compañerismo y de felicidad. Gracias Gabriel, Omar, Oscar, Rosario, Erika, Ivonne, Chayito, Daniel, Marco, Mario, Israel, Jesús y a todos aquellos que me han dado su apoyo.

TESIS CON
FALLA DE ORIGEN

B

ÍNDICE

Índice	I
Introducción	III
Capítulo 1. Antecedentes y Conceptos Básicos	1
1.1 Antecedentes históricos	1
1.1.1 Orígenes de Red UNAM	1
1.1.2 La Dirección de Telecomunicaciones Digitales (DTD)	5
1.1.3 Departamento de Administración de Servidores	6
1.2 Aspectos relevantes de administración de UNIX	9
1.2.1 Introducción UNIX	9
1.2.2 Control de Procesos y Utilerías UNIX	15
1.2.3 Administración de UNIX	23
Capítulo 2. Estudio de Factibilidad y Requerimientos para la migración	27
2.1 Definición del problema (del equipo origen)	27
2.1.1 Antecedentes.	27
2.1.2 Partes constitutivas	29
2.1.3 Rendimiento actual de la plataforma	32
2.2 Análisis de factibilidad	38
2.2.1 Expectativas y situación original de Argon	38
2.2.2 Beneficios para la DGSCA	40
2.3 Determinación y selección de los elementos requeridos a implementar	42
Capítulo 3. Metodología para la instalación, configuración y migración del sistema	46
3.1 Instalación y configuración del hardware y el software.	46
3.2 Migración de los datos	49
3.3 Documentación	60
3.4 Descripción de funcionamiento del sistema	68
Capítulo 4. Mantenimiento del sistema	70
4.1 Temas selectos de Administración de Solaris 8	70
4.1.1 Bitácoras del sistema y Archivos de Configuración	70
4.1.2 File System (Sistema de Archivos)	71
4.1.3 Niveles de inicialización	76
4.1.4 Scripts de inicialización	78

Índice

4.1.5 Respaldos	78
4.1.6 Administración de parches de Sistema Operativo	79
4.2 Area de Administración de rendimiento	81
4.3 Area de Administración de fallas	87
4.4 Area de Administración de la seguridad	92
Conclusiones	95
Apéndice A	98
Apéndice B	115
Apéndice C	132
Glosario	143
Bibliografía	144

INTRODUCCIÓN

INTRODUCCIÓN

Actualmente, el cómputo ha tenido un gran auge en todo lo referente a Internet. Principalmente, en los servicios de Web Hosting (hospedaje de páginas Web) y correo. El Web Hosting ha ido tomando un papel muy relevante en la UNAM, por el surgimiento de nuevos servicios de comercio electrónico, como son tiendas electrónicas y donaciones de exalumnos a Fundación UNAM. Siendo de trascendental importancia el Departamento de Administración de Servidores de la DGSCA por mantener los servidores centrales de Red UNAM.

En este proyecto se tratará sobre la migración del servidor de Web Hosting Argon¹, éste alojaba aproximadamente cien sitios, tanto de dependencias de la UNAM como externos. Además, brindaba a ciertos usuarios especiales el servicio de correo electrónico. Con respecto a los sitios Web, la mayor parte son de gran importancia, por la información que manipulan; otros sitios menores, por contener únicamente información sobre las actividades que realizan y otros con falta de vigencia o actualización. Cabe señalar que cada uno es igual para nosotros, ya que se busca mantener el buen servicio y mantener su información íntegra.

El servidor Argon ha ido presentando algunos síntomas de posible desaparición inesperada dentro de poco tiempo, debido a la arquitectura tan obsoleta y su larga actividad (9 años trabajando ininterrumpidamente). La arquitectura que maneja es una Sun SPARC Center 2000. También se considera un servidor inseguro; esto causado por la falta de espacio en disco para la actualización de herramientas de seguridad. Por ser un equipo obsoleto los discos ya no los fabrican.

Con base a lo anterior, surge la necesidad de realizar una migración de Sistema Operativo como de plataforma. Empleando Solaris y un dominio de la Sun Enterprise 10000, ubicada en Pitágoras, el cual es un site alteno donde están algunos servidores de UNAM.

El proyecto abarcará cuatro capítulos sobre el desarrollo de la migración de Argon y la administración de Einstein.

El CAPÍTULO 1, Antecedentes históricos y Conceptos básicos de UNIX, tratará sobre la historia de Red UNAM, la DTD, el Departamento de Administración de servidores e historia, conceptos básicos, procesos, utilerías sobre el sistema operativo UNIX.

¹ De ahora en adelante se referirá el servidor a través de su dominio (Argon), en lugar de su nombre de máquina (argon.servidores.unam.mx). Además, no se utilizarán acentos en los nombres de equipos de Internet.

INTRODUCCIÓN

El CAPÍTULO 2, Estudio de Factibilidad y Requerimientos para la migración, como su nombre lo indica se obtendrán todos los elementos importantes para llevar a cabo el proyecto y se justificará el por qué será llevado a cabo.

El CAPÍTULO 3, Metodología para la migración del sistema, tratará la mayor parte de los puntos técnicos para la puesta en marcha la migración y se establecerá la documentación que se requiera en un futuro para posibles modificaciones.

El CAPÍTULO 4, Administración y Mantenimiento del sistema se referirá a todos aquellos aspectos requeridos para mantener el servidor bien administrado y por consiguiente saber cuales pueden ser los puntos vulnerables y evitarlos.

Por medio de estos cuatro capítulos podrá llevarse a cabo los objetivos del proyecto de forma satisfactoria.

CAPÍTULO 1

Antecedentes y Conceptos Básicos

En este capítulo se tratará aquello referente sobre la historia de Red UNAM, a grandes rasgos como ha evolucionado y se hablará principalmente de la Dirección de Telecomunicaciones Digitales y específicamente al Departamento de Administración de Servidores, sus funciones principales y la importancia de los servicios que presta. También se detallará sobre la historia de UNIX, debido a que el proyecto se realizará empleando una versión de UNIX. Solaris, se definirá algunos comandos básicos y utilerías para familiarizarse con dicho sistema operativo.

1.1 Antecedentes históricos

1.1.1 Orígenes de Red UNAM²

Al final de los años 60's y a principio de los 70's se instalaron las primeras conexiones de teletipo a una computadora central; la red telefónica era de cobre y fue usada dentro y fuera de la UNAM.

En 1987, la UNAM se conecta a BITNET, desde Ciudad Universitaria al ITESM, de ahí a San Antonio Texas.

En 1989, la UNAM realiza un enlace a la red de NSF³ en EUA empleando un satélite mexicano, Morelos II, para conectar la red del Instituto de Astronomía con la Dirección General de Servicios de Cómputo Académico (DGSCA). Trayendo bastante equipo de cómputo para integrarlo a las redes locales. Se empezaron a establecer más enlaces de fibra óptica y satelitales a Cuernavaca, Morelos y a San Pedro Martir en Ensenada y además, el primer enlace de microondas.

A finales de 1989, se llevó a cabo un proyecto para renovar el sistema telefónico de la UNAM y con ello se creó la Dirección de Telecomunicaciones Digitales (DTD) para crear la Red Integral de Telecomunicaciones (RIT) de la UNAM, pero hasta 1992 es inaugurada.

² <http://www.nic.unam.mx/redunam/historia.html>

³ National Science Foundation

En 1990, con la creación del laboratorio de Red UNAM, la UNAM se convierte en la primera institución en Latinoamérica en incorporarse a la Red mundial de Internet enlazando millones de máquinas y decenas de millones de usuarios en todo el mundo, ofreciendo una gran cantidad de servicios a la comunidad universitaria, como correo electrónico, hospedaje de páginas Web, *ftp* anónimo, entre otros servicios. Un año después se brinda el servicio de *Gopher*.

En 1998, la UNAM forma parte de la RED TTVN⁴ y en el año 2000 la Universidad Autónoma de Nuevo León se integra a esta red.

Hoy en día la Red Integral de Telecomunicaciones tiene las principales características:

- Transmisión indistinta de datos y video mediante sistemas digitales basada en normas internacionales que rigen actualmente.
- Integración a la red de las principales instalaciones de la Universidad.

La columna vertebral⁵ de Red UNAM está conformada por 32 nodos de telefonía enlazados entre sí mediante fibra óptica, enlaces satelitales y de microondas. En la figura 1.1 se muestra un diagrama del backbone en el 2001, en donde se encuentran los equipos que controlan a RedUNAM

Se tiene instalados 13000 servicios telefónicos alimentados por 2400 troncales digitales conectados por fibra óptica con las centrales telefónicas públicas.

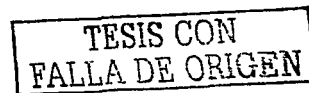
Red UNAM cuenta con una red complementaria con más de 1000 servicios basados en telefonía celular y 17 líneas telefónicas directas. Además, con más de 600 redes locales en ocho regiones del país enlazando aproximadamente más de 15000 computadoras de la UNAM entre sí y 30 millones en el resto del mundo.

Cabe señalar que la RIT es completamente privada y propiedad de la UNAM y es operada en su totalidad por personal de la DTD.

El backbone de Red UNAM tuvo algunas modificaciones en el 2002, la figura 1.2 muestra el diagrama.

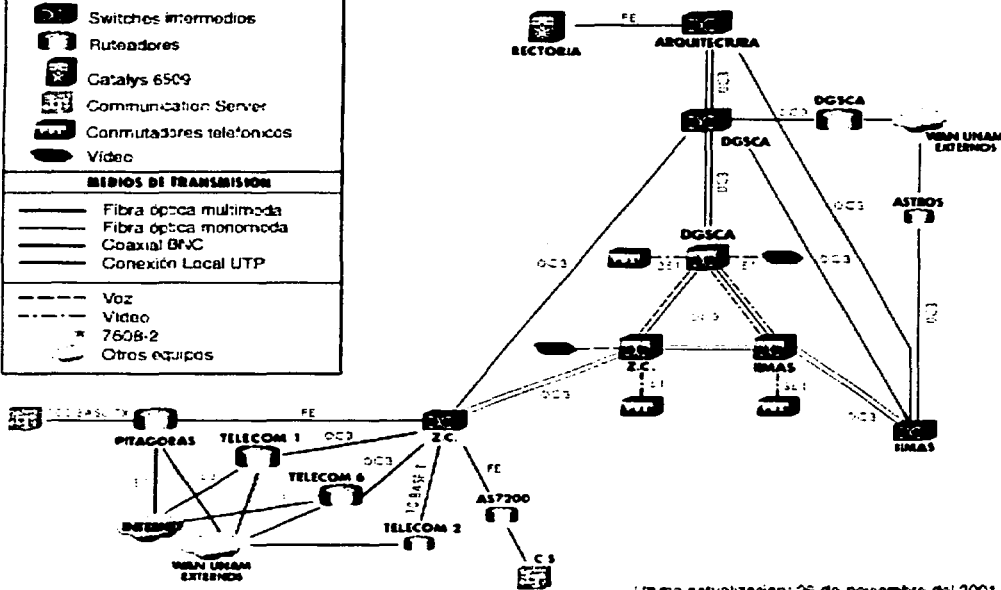
⁴ TransTexas Video Network

⁵ Se puede utilizar también el término de Backbone



Básicamente, el cambio realizado en RedUNAM fue porque se requería una mejor estabilidad en la red, es decir, antes se empleaba ATM y luego Ethernet, a través de los switches intermedios se redirigía el tráfico y eso hacía que la red fuera más lenta y poco eficiente. Con el nuevo cambio existe una mayor redundancia y mayor velocidad en el transporte de información por el empleo del protocolo de enrutamiento OCPF, dividiendo en áreas y poniendo como principal al área 0 (equipos de Core que están en las esquinas).

EQUIPOS DE COMUNICACION	
	Switches multimedia
	Switches intermedios
	Ruteadores
	Catalys 6509
	Communication Server
	Commutadores telefónicos
	Video
MEDIOS DE TRANSMISION	
	Fibra óptica multimoda
	Fibra óptica monomoda
	Coaxial BNC
	Conexión Local UTP
	Voz
	Video
	760B-2
	Otros equipos



Última actualización: 26 de noviembre del 2001

Figura 1.1 - Backbone ATM⁶

TESIS CON
FALLA DE ORIGEN

⁶ <http://www.dtd.unam.mx/REDUNAM/backbone.html>

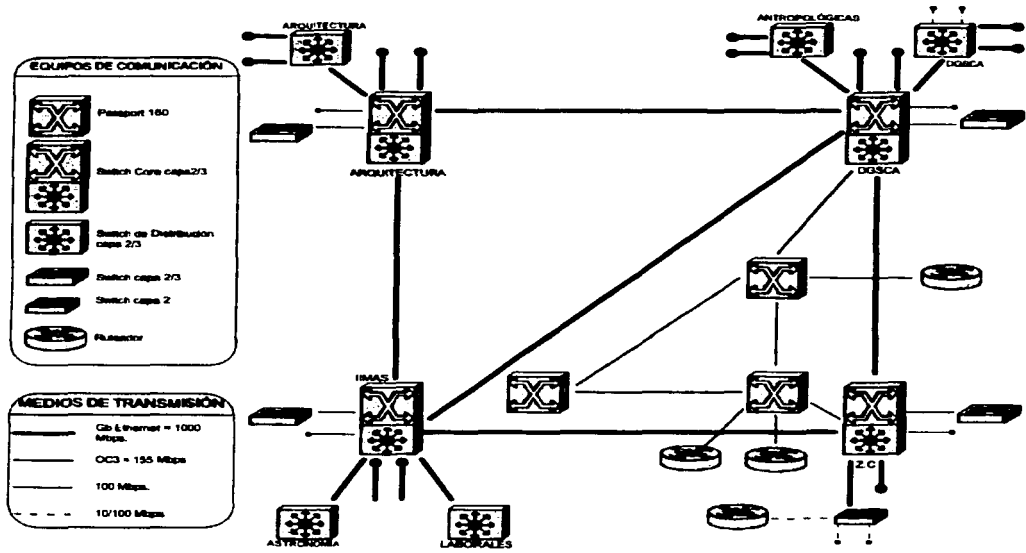


Figura 1.2 – Backbone actual (2003)

TESIS CON FALLA DE ORIGEN

1.1.2 La Dirección de Telecomunicaciones Digitales (DTD)

La DTD se originó en 1989 con el fin de crear la Red Integral de Telecomunicaciones de la UNAM. Las subdirecciones y coordinaciones de la DTD trabajan conjuntamente para dar una mejor optimización de los recursos y servicios que ofrece al público en general, así como a la comunidad universitaria. En la figura 1.3 se muestra el organigrama de la DTD.⁷

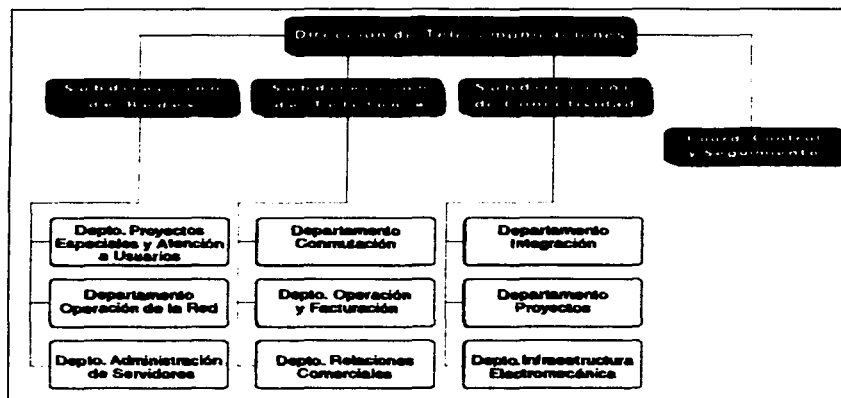


Figura 1.3 – Organigrama DTD⁸

Subdirección de redes

La Subdirección de redes opera, coordina y mantiene a la Red Universitaria de Datos (RedUNAM) a nivel técnico y Administrativo. Analiza y dirige los lineamientos a seguir en la evolución de la misma Red. Está integrada por los Departamentos de:

- Proyectos Especiales y Atención a Usuarios
- Operación de la Red
- Administración de Servidores

⁷ <http://www.dtd.unam.mx>

⁸ <http://www.dtd.unam.mx/organigrama.html>

TESIS CON
FALLA DE ORIGEN

1.1.3 Departamento de Administración de Servidores

El Departamento de Administración de Servidores⁹ se creó en 1997 como parte de la descentralización de la Coordinación de Servicios de Red (CSR). Perteneciendo desde esa fecha a la Subdirección de Redes. Para ese entonces, contaba con *Dragon*, *Servidor*, *Neon*, *Condor* y *Bachiller*¹⁰; los dos primeros estaban en dos equipos Sparc Center 2000, los dos últimos estaban en un equipo SUN "clasic". *Bachiller* era un servidor de correo para alumnos de bachillerato. Entre 1998 y 1999, se hicieron varias modificaciones en cuanto al equipo con la llegada de tres 3500. *Dragon* cambia de la Sparc Center 2000 a una 3000 (que fue prestada). *Servidor* también es migrado a una 3500. Otra 3500 es empleada para Tungsteno, equipo para la realización de respaldos de los servidores centrales.

Dragon tuvo un crecimiento acelerado, así que fue migrado a uno de los dominios de la primera Enterprise 10000. Surgiendo *Argon* con el fin de reestructurar parcialmente el servidor *Dragon*. Posteriormente llegan otras dos Enterprise 10000, una destinada para cursos y la otra enviada al site de Pitágoras. De esta manera el Departamento de Administración de Servidores se convirtió en el responsable de los servidores centrales de Red UNAM con el fin de brindar servicio a la comunidad universitaria.

En seguida se dará una descripción breve de los servidores y servicios más importantes a cargo del Departamento de Administración de Servidores.

CORREO ELECTRÓNICO

a) *servidor.unam.mx*

Servidor que brinda servicio de correo electrónico a la comunidad universitaria. Tiene actualmente 22000 usuarios registrados que intercambian un promedio de 65,000 mensajes diarios; estos datos son obtenidos de las estadísticas generadas dentro del sistema, el cual está a cargo del departamento de Administración de Servidores. Utiliza como agente de transporte de correo Sendmail. Los usuarios para ver sus correos pueden utilizar Eudora, Outlook, Pine (a través del puente pine.servidores.unam.mx) y la página web de www.correo.unam.mx.

⁹ <http://www.servidores.unam.mx>

¹⁰ Servidores que prestan diversos servicios a la comunidad universitaria, se denominarán con respecto al nombre del host. *Dragon*: dragon.dgsca.unam.mx, *Servidor*: servidor.unam.mx, *Neon*: neon.servidores.unam.mx, *condor*: condor.servidores.unam.mx y *Bachiller*: bachiller.dgsca.unam.mx

TESIS CON
FALLA DE ORIGEN

b) *www.correo.unam.mx*

Servidor que brinda servicio de correo electrónico a la comunidad universitaria y al público en general. Tiene actualmente 53000 usuarios registrados. Utiliza como agente de transporte Sendmail. Los usuarios para ver sus correos utilizan la página *www.correo.unam.mx*.

Este servicio se soporta en plataformas Sun Ultra Enterprise 3500 con 1 GB de memoria RAM, 261 GB en disco duro, y 4 procesadores Ultra Sparc II de 400 MHz.

HOSPEDAJE DE SITIOS WEB

Los sitios web residen en el servidor central *dragon.dgscs.unam.mx*, en *cobalto.servidores.unam.mx* y en *argon.servidores.unam.mx*. En conjunto tienen alrededor de 300 sitios hospedados y emplea Apache como servidor de web. El promedio de accesos diarios a los servidores de web alcanza casi los 2,000,000. Estos datos pueden consultarse en la página <http://www.servidores.unam.mx> en la sección de estadísticas.

a) *dragon.dgscs.unam.mx*

Servidor de web hosting para dependencias de la UNAM y externas. Hospeda entre sus sitios más importantes, la página principal de la UNAM y de la Jornada. Las herramientas instaladas son Sybase, Postgresql, Mysql, Perl, Php, entre otros.

b) *cobalto.servidores.unam.mx*

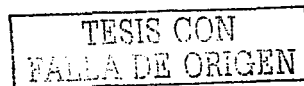
Servidor de web hosting para dependencias de la UNAM y externas. Las herramientas instaladas son: Sybase, Php, Perl y Sybperl. Los sitios más importantes pertenecen al Departamento de Publicaciones Digitales.

c) *argon.servidores.unam.mx*

Servidor de Web hosting para dependencias de la UNAM y externas. Las herramientas instaladas son: Sybase, Php, Perl, Sybperl y Websql.

FTP ANÓNIMO***euler.servidores.unam.mx***

Servidor que brinda el servicio de sitios "mirror" y el FTP Anónimo de la UNAM distribuye cientos de programas de dominio público a la comunidad en general. Este servicio cuenta con aplicaciones para plataformas UNIX y Windows y son actualizadas cada semana.



La página mirrors.unam.mx contiene diversos espejos de algunos de los sitios WEB y FTP más importantes sobre software; para facilitar y agilizar la descarga del mismo. Algunos de ellos son:

- sunfreeware.unam.mx. El primer sitio espejo oficial en México del popular sitio sunfreeware.com. En éste se encuentran aplicaciones y utilerías precompiladas para el sistemas operativo Solaris de Sun Microsystems, desde la versión 2.5.1 hasta la 9.
- apache.unam.mx. El primer sitio espejo del Proyecto Apache. Este proyecto tiene como misión desarrollar, entre otras aplicaciones importantes, el servidor web más confiable y utilizado en el WWW: Apache Web Server.
- www.gnu.unam.mx. El primer espejo en México es www.gnu.org. La organización GNU se encarga de desarrollar software de uso público para que sean revisados periódicamente, e incluso los usuarios se encargan de proponer y realizar mejoras al mismo para optimizar su funcionamiento.

SERVICIO DE AVISOS

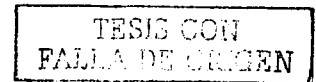
El Departamento de Administración de Servidores se encarga de difundir avisos o eventos de interés general a la comunidad universitaria a través del Servicio de Avisos.

Los viernes de cada semana a las 5:00 PM se envía un correo electrónico a todos los usuarios de servidor.unam.mx, en el cual se incluye un resumen de las actividades o eventos que se llevarán a cabo durante la(s) semana(s) posterior(es) a la difusión del mensaje. La recepción de avisos se cierra los viernes a las 3:00 PM. y deberán ser enviados por lo menos una semana de anticipación.

Los avisos son publicados en el sitio web www.avisos.unam.mx.

ESTADÍSTICAS

Cada uno de los servidores centrales de Web Hosting tiene el servicio de estadísticas para conocer los accesos a cada sitio. La actualizaciones se realizan de forma periódica cada semana a través del Webalizer¹¹.



¹¹ El Webalizer es un programa libre para analizar los archivos log de un servidor web

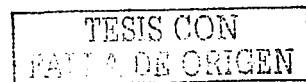
1.2 Aspectos relevantes de Administración de UNIX

Una computadora está compuesta por tres elementos hardware, sistema operativo y las aplicaciones. En donde el hardware incluye al CPU (unidad central de procesamiento), el teclado, disco duro, memoria, entre otros. Las aplicaciones son el por qué usamos la computadora para optimizar alguna tarea deseada en el sistema. El sistema operativo es el componente que por un lado maneja y controla el hardware y por otra las aplicaciones.

El sistema operativo ha utilizar en este proyecto es UNIX, el cual es muy rico y completo por ser empleado en equipos como supercomputadoras, mainframes, minicomputadoras, estaciones de trabajo o computadoras personales. A diferencia de otros sistemas operativos, UNIX posee diversas variantes o versiones para todas las arquitecturas, las divergencias radican en las múltiples utilidades, métodos de configuración o las interfaces de usuario. Aunque un aspecto muy importante que si se conoce una versión es relativamente sencillo manejar cualquier otra. En esta sección se tratará las características fundamentales del por qué se considera a UNIX un sistema operativo robusto, cuáles son los comandos de control de procesos, cuáles son las utilerías más importantes y fundamentos de administración de UNIX.

1.2.1 Introducción a UNIX

Historia de UNIX y sus versiones



A mediados de los años 60's American Telephone and Telegraph, Honeywell, General Electric y el Instituto Tecnológico de Massachussets llevaron a cabo un proyecto llamado MULTICS (Multiplexed Information and Computing Service). El sistema fue originalmente diseñado para operar una computadora GE-645 y tomando en cuenta la seguridad militar; sin embargo era muy grande, complejo y atrasado, por tanto los laboratorios BELL de AT&T abandonaron el proyecto en 1969.

Un grupo de investigadores de los laboratorios BELL, Ken Thompson, Dennis Ritchie, Peter Neumann y otros como Rudd Canaday, Doug Mxlroy y Joe Ossanna utilizaron una computadora PDP-7 para crear un nuevo sistema operativo que fuera suficientemente cómodo, rápido y que facilitara la investigación y desarrollo de programas, llamado UNIX. Un año después Thompson y Ritchie reescribieron UNIX (en un 90%) para que funcionara en una computadora PDP-11.

Thompson en 1973 reescribió nuevamente UNIX en lenguaje C, el cual fue inventado por Dennis Ritchie, permitiendo que los programas se pudieran trasladar de una computadora a otra, es decir

que fuera portátil, comprensible y además, los programas se ejecutaban casi tan rápido como si estuvieran escritos en lenguaje ensamblador.

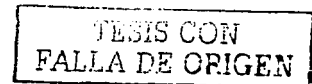
UNIX se hizo muy popular en las universidades, debido a que se utilizó con fines educativos. Bill Joy y Chuck Holley, estudiantes de la Universidad de California en Berkeley, no se limitaron a usar UNIX, realizaron varias modificaciones y anexaron una colección de programas denominándolo BSD (Berkeley Software Distribution), en 1978. Iniciando un conflicto entre AT&T y Berkeley debido a que éstos no consideraban a esta versión de UNIX un estándar. Además, la marca UNIX pertenecía a AT&T.

Para contrarrestar este nuevo UNIX mejorado, AT&T creó el USG (Unix Support Group). Este nuevo grupo de soporte a UNIX saca el AT&T System V, que no es otra cosa que una nueva versión de UNIX y lo declaró como el único "estándar", demeritando de esta manera al UNIX BSD.

Debido a las constantes fricciones entre Berkeley y AT&T, la versión 5.0 de BSD no pudo ser llamada de esta manera entonces fue llamada "versión 4.2". Aunque realmente los cambios eran importantes surgiendo así dos corrientes en los S.O. UNIX en la actualidad.

A mediados de los 80's, la mayor empresa comercial impulsora de BSD era Sun Microsystems que fue fundado por exalumnos de la universidad de California en Berkeley, ellos tenía su propio sistema operativo comercial UNIX, el SunOS, basado en BSD 4.1c. Pero no fue la única empresa en impulsar a BSD también DEC sacó su versión de UNIX llamada ULTRIX como es de suponerse basada en BSD 4.2. Cada nueva empresa que entraba a comercializar UNIX, debía basarse en una de estas dos corrientes (AT&T System V y BSD 4.2) tal es el caso de los fabricantes Data General, IBM, HP, Silicon Graphics, quienes adoptaron System V como estándar, sin embargo Sun Microsystems es el líder en el ramo.

Los usuarios comerciales y fabricantes les preocupaba la falta de un estándar por lo que algunas versiones de UNIX comenzaron a fusionarse, como fueron XENIX y System V de AT&T. En 1998, formaron UNIX System V/386 versión 3.12 para computadoras con procesador 80386. En ese mismo año AT&T y Sun Microsystems hicieron un gran avance en la estandarización de las corrientes de UNIX al fusionar System V y BSD formando así System V Release 4, (SVR4) compatible con programas escritos con cualquiera de estas corrientes, SUN Microsystems decide dejar de vender SunOS y saca su versión denominada SOLARIS basada en System V Release 4, actualmente es el líder en versiones de UNIX.



En 1988, sintiéndose amenazados por la alianza de Sun/AT&T fabricantes como, HP, IBM, Apollo Computer, Digital Equipment Corporation, entre otros crearon la OSF (Open Software Foundation). Esta fundación tenía como fin quitarle el control a AT&T sobre UNIX y dárselo a alguien sin fines de lucro para cuidar el desarrollo de UNIX y que estuviese bajo licencias iguales. La versión que propuso fue AIX, tendría varias bibliotecas UNIX y programas de HP, IBM y Digital. Pero, no fue exitosa su intención.

En 1993, AT&T vende UNIX System Laboratories (USL) a Novell, el cual transfirió la marca registrada UNIX a X/O Consortium. Posteriormente en 1995, Novell vende los programas fuente a SCO (Santa Cruz Operation).

La Figura 1.4 nos muestra la evolución de las versiones más importantes de UNIX.

TESIS CON
FALLA DE ORIGEN

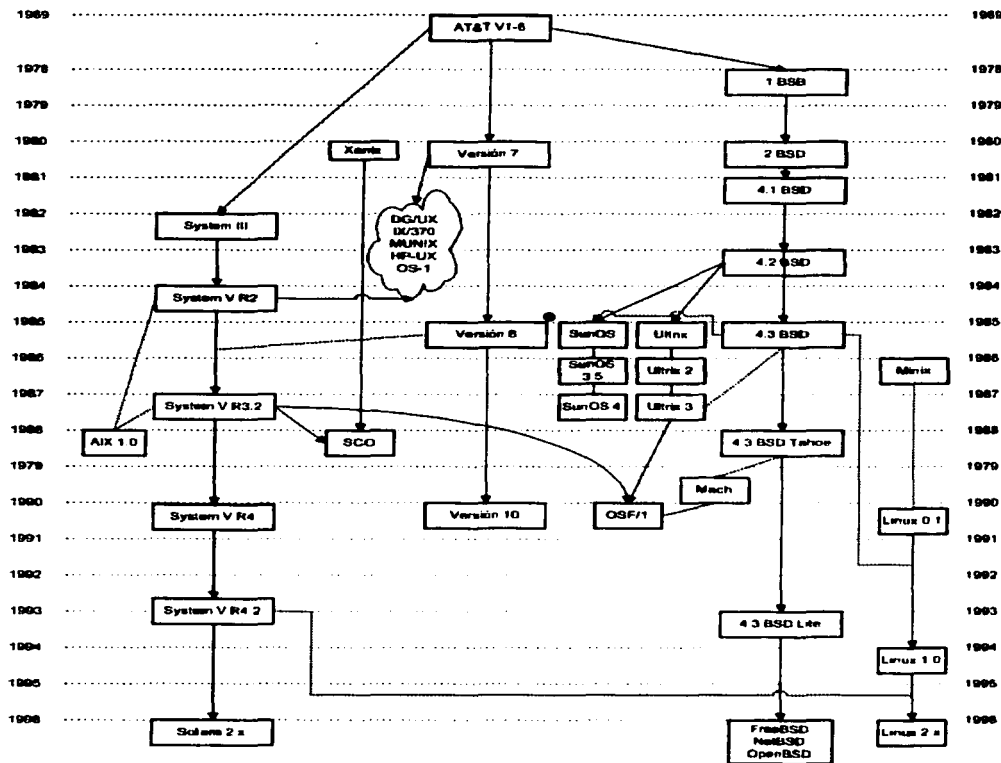


Figura 1.4 – Versiones de UNIX

Características de UNIX

- Sistema multiusuario y multitarea.
- Está escrito en un lenguaje de alto nivel, lenguaje C, característica que lo hace portátil.
- Tiene un enfoque de programación, para la gente que desea desarrollar aplicaciones.
- Utiliza redireccionamiento de entrada/salida, filtros e interconexiones.

TESIS CON FALLA DE ORIGEN

- Emplea sistema de archivos jerárquico, sencillo y eficiente, lo que permite proteger los archivos, cuentas y procesos.
- Ve todo como un archivo. Tanto la información como los dispositivos asociados a una terminal o disco.
- Realiza las instrucciones que le damos y las ejecuta al pie de la letra, asumiendo que sabemos qué se hace.
- Emplea manejo dinámico de memoria por intercambio o paginación.
- Tiene capacidad de interconexión de procesos y permite comunicación entre procesos.
- Tiene facilidad para redireccionamiento de Entrada/Salida.

Estructura

a) **Kernel:** es el núcleo del sistema operativo.

Funciones:

- Administrar dispositivos, memoria, procesos y demonios.
- Controlar las funciones entre los programas de sistema y el hardware.
- Calendarizar y ejecutar todo los comandos.

b) **Shell:** es la interfaz entre el usuario y el kernel. Funciona como un interprete de comandos, acepta los comandos luego los interpreta y envía el ejecutable al kernel.

Es importante señalar que el shell no es UNIX, sólo es una interfaz hacia él, ver Figura 1.5.

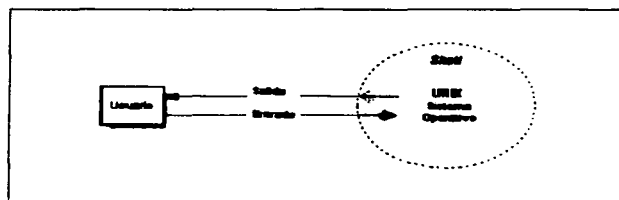


Figura 1.5 - Shell

TESIS CON
FALLA DE ORIGEN

Tipos:

- *Bourne shell - sh (\$)*: shell de default para Solaris, fue desarrollado por Steven Bourne (AT&T).
- *C shell - csh (%)*: similar a la programación del lenguaje C. Fue escrito por Bill Joy de la Universidad de California de Berkeley.
- *Korn shell - ksh (\$)*: fue inventado por David Korn(AT&T). Es una mejora de Bourne Shell porque agrega características de asignación de sinónimos (aliasing), history y edición en línea de comandos.
- *Bash shell - bash (Bourne-Again Shell)(\$)*: fue escrito por Brian Fox y Chet Ramey y es considerado software de dominio público, porque no hay que pagar por él.

c) Sistema de archivos: la estructura de archivos es una jerarquía de directorios, subdirectorios y archivos que se agrupan por un propósito en particular.

El *Directorio* es una localidad para otros archivos y directorios y el *Subdirectorio*, es cualquier directorio debajo de otro directorio.

La arquitectura de UNIX tomando en cuenta todos sus elementos, hardware, kernel, sistema operativo, shell, herramientas y aplicaciones se muestra en la Figura 1.6.

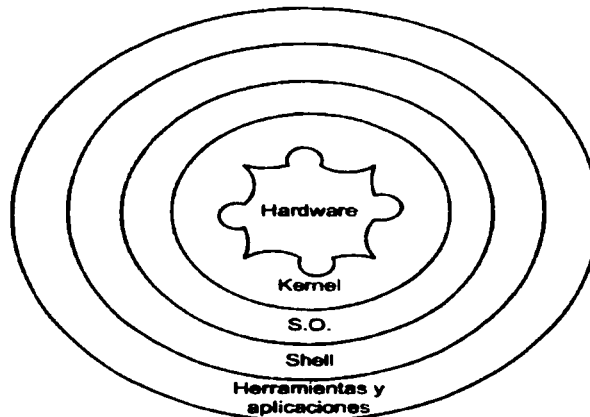


Figura 1.6 – Arquitectura UNIX

TESIS CON
FALLA DE ORIGEN

1.2.2 Control de Procesos y Utilerías UNIX

Control de Procesos

Una de las características importantes de UNIX es que es multiproceso, un ejemplo para entender con mayor claridad este concepto sería; supongamos que se está corriendo un comando que tomará mucho tiempo de procesamiento, en un sistema de una sola tarea como MS-DOS se introduciría el comando y se esperaría hasta que el sistema regrese el prompt, entonces no permite introducir otro comando. En cambio en UNIX un comando tecleado en "foreground" puede ser enviado a "background" y aparecería inmediatamente el prompt para introducir un comando sin dejar que se ejecute el comando anterior.

Proceso. Proceso es un programa ejecutable en forma binaria, junto con varias estructuras de datos que conservan el contexto del programa.

PID. Identificador de proceso, es un número entero y es único dentro del sistema.

Proceso en Segundo Plano (Background). Proceso hijo del shell que se le da un PID para que su padre no espere a que termine e inmediatamente muestra el prompt del shell para poder ejecutar otro comando. Para indicarle al shell se utiliza el terminador de comando `&`.

A continuación se muestra algunos comandos para el control de los procesos.

wait

Este comando permite hacer una espera en el sistema hasta que todos los procesos que estén corriendo en segundo plano terminen.

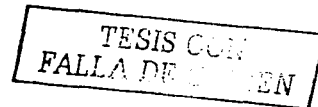
kill [-signo] pid1 [pid2 ... pidn]

Este comando permite eliminar procesos. Si omite signo éste tomará el valor de 15 que es la señal de terminación de un proceso: Sólo podrá eliminar sus propios procesos.

nohup bigjob argumentos &

Este comando permite inmunizar contra un kill, cuando se llama a nohup este genera un proceso con una prioridad baja. Una señal que garantiza la muerte de los procesos tanto ciclados como con nohup, tal es el siguiente caso:

```
$ kill -9 3421
```



ps *[opciones]*

El comando ps permite mantener un seguimiento sobre los procesos activos.

opciones

- Ninguna lista en formato corto (usuario)
- e lista todos los procesos (usuario)
- a lista todos los procesos que se estén corriendo sobre el servidor
- f suministra un listado completo (usuario)
- l suministra un listado largo (usuario)

nice *[-inc] comando [argumentos]*

El comando nice permite cambiar la prioridad de un proceso. Cada proceso tiene un número nice de 0 a 39 desde el cual el kernel calcula su prioridad. El valor de 0 representa la prioridad más alta y 39 la más baja. El número nice por default es 20, si deseamos bajar su prioridad, entonces se deberá aumentar su número nice de ahí el nombre de inc; el valor por default para inc es 10.

sleep *n*

El comando sleep duerme un proceso durante n segundos (no excede 65 535 segundos) si se agrega a un script shell se puede utilizar para atrasar una secuencia de exhibición.

Utilerías UNIX

Las utilerías UNIX son programas que nos auxilian en la obtención, procesamiento, control y presentación de la información.

Entrada y Salida estándar

Descriptor de archivos	Referencia	default
0	Entrada Estándar	Terminal
1	Salida Estándar	Terminal
2	Error	Terminal

TESIS CON
FALLA DE ORIGEN

Operaciones de entrada y salida:

1. **Redireccionamiento:** nos permite cambiar el dispositivo asociado (Salida o Entrada estándar).

Metacaracter	Sintaxis	Acción
>	Programa o comando > archivo	dirige salida hacia el archivo
>>	Programa o comando >> archivo	agrega salida hacia el archivo
<	Programa o comando < archivo	Extrae archivo hacia la entrada estandar

2. **Tuberías (pipes):** conectan la salida de un programa (a1) a la entrada (a2) de otro programa, nos sirve para no hacer archivos intermedios. Además, podemos hacer dos o más conexiones entre programas.

Metacaracter	Sintaxis
	a1 a2

3. Caracteres especiales:

a) **Comodines:** son caracteres que provocan que el shell realice una búsqueda en un rango de posibles valores.

? cualquier caracter

* cualquier número de caracteres (o nada)

[] un rango de caracteres comprendido dentro del valor entre los corchetes

b) Entrecorillado:

" delimita cadena de caracteres

' equivalente a las anteriores; escapa variables de ambiente

` refleja el resultado de un comando

TESIS CON
FALLA DE ORIGEN

c) **Metacaracteres:** El shell de UNIX posee un conjunto de operadores sobre caracteres que permite especificar más de un valor, son traducidos por el shell de forma que la orden no sabe si existe.

<, >, (), [], |, ?, /, \, \$, ", ' , ` , #, &, ^, espacio, tabulador, nueva línea.

d) Expresiones regulares:

- Se usan para definir o comparar una clase de cadena de caracteres.
- Se usan para seleccionar algún conjunto de registros o campos desde un conjunto de datos.
- Se construyen a través de caracteres planos y metacaracteres. Los caracteres planos se comparan entre ellos y los metacaracteres comparan diferentes grupos de caracteres o modifican la operación de otros caracteres.

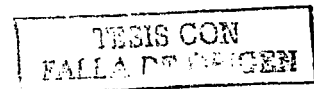
Operadores utilizados en expresiones regulares.

Operador	Significado
*	El elemento precedente debe de aparecer cero o mas veces
+	El elemento precedente debe de aparecer una o mas veces
.	Cualquier caracter menos salto de línea
?	Un solo caracter, el caracter precedente es opcional
	Uno u otro (OR)
^	Comienzo de línea
\$	Fin de línea
[]	Rango de caracteres (conjunto)
[^]	Caracteres no admitidos
-	Operador de rango
()	Agrupación
\	Escape de caracter

Utilerías de manejo de texto

A continuación se explica la forma de como procesa los datos la familia del grep.

1. Revisa la sintaxis para buscar la cadena.
2. Para cada línea de archivo realiza un barrido lineal.
 - a) Valida si la línea corresponde al criterio especificado.
 - b) Si es así realiza el procesamiento, exceptuando con la opción -v.
3. Al final del archivo termina la búsqueda.



Familia de grep**grep** [opciones] patron [archivo]

La utilidad grep (global regular expresión print), es el comando original de la familia de grep, el cual hace uso de las expresiones regulares básicas.

egrep [opciones] patron [archivo]

La utilidad egrep (extended global regular expresión print) hace uso de expresiones regulares extendidas.

fgrep [opciones] "cadena1 cadena2 ... cadenaN" [archivo]

El comando fgrep (fast global regular expresión print) no hace uso de expresiones regulares, únicamente usa un listado de cadenas de caracteres.

opciones

- i no importa si es minúscula o mayúscula
- v imprime aquellas que no contienen el patrón
- c muestra cuantas líneas contienen el patrón

Otras utilerías**head** -n [nom_arch]

El comando head muestra por defecto las primeras diez líneas.

- n Especifica el número de líneas a desplegar
- nom_arch - Se refiere al nombre del archivo

tail opciones [nom_arch]

El comando tail muestra por defecto las últimas diez líneas.

opciones

- n Especifica el número de las últimas líneas a desplegar
- +n Especifica desde que línea va a desplegar
- f Muestra las últimas líneas de un archivo que se van agregando en el mismo. No termina, espera a que se imprima algo

nom_arch - Se refiere al nombre del archivo



cut *-f lista [-d "separador"] [-s] archivo*

cut *-clista archivo*

Esta utilidad permite cortar columnas de un archivo

- f** especifica columnas, corta campos especificados en lista
- lista** número de columna(s) o carácter(es) a ser cortado(s). Es un número entero, con comas(,) se especifica columnas en particular y con guion(-) se especifica un rango
- d** especifica el separador o delimitador
- separador** caracter que delimita a las columnas
- c** indica el número de caracteres a cortar

sort *[opciones] [+pos1[-pos2] [archivo]*

La utilidad sort ordena las líneas de un archivo. Por defecto ordena primero los números, luego las mayúsculas y finalmente las minúsculas.

opciones

- f** deshabilita la sensibilidad por default, es decir toma por igual mayúsculas y minúsculas
- n** ordenamiento numérico
- r** ordenamiento descendente
- t"x"** x es el separador
- +pos1** ordenamiento comenzado en pos1
- pos2** terminado en pos2

paste *[opciones] archivo1 archivo2*

La utilidad paste pega en forma de columnas (horizontalmente)

opciones

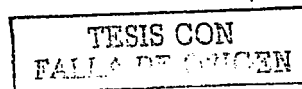
- d"x"** x el caracter que unirá a las líneas
- s** las líneas de un archivo las convierte en columnas (linealmente)

expr *argumentos*

La utilidad expr evalúa las expresiones aritméticas o de cadena.

argumentos

- +** Suma
- Resta
- *** Multiplicación
- /** División
- %** Módulo
- :** Actúa como un grep



uniq [opciones] [archivo1 [archivo2]]

La utilidad **uniq** obtiene o elimina líneas únicas de un archivo o identifica líneas repetidas dentro del mismo. Las líneas iguales deben de estar juntas, para ello se recomienda hacer antes un **sort**

opciones

- d extrae las líneas repetidas (copia)
- u extrae las líneas no repetidas (copia)
- c imprime antes de cada línea el número de veces que aparece

archivo1 es el archivo de entrada
archivo2 es el archivo de salida

diff [opciones] archivo1 archivo2

La utilidad **diff** informa que cambios hay que realizar en el **archivo1** para poder convertirlo en el **archivo2**. Para ello hace un despliegue lineal. En la salida muestra tres letras:

a append - agregar
d change - cambiar
d delete - borrar

NOTA: **archivo1** y **archivo2** pueden ser archivos largos.

tr [opciones] [cadena1[cadena2]]

La utilidad **tr** sustituye caracteres de la **cadena1** por caracteres de **cadena2**

opciones

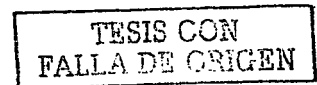
- d borra caracteres contenidos en **cadena1**
- s borra caracteres repetidos (que estén juntos)

tar opciones archivo.tar archivo

La utilidad **tar** nos permite agrupar y desagrupar archivos en uno solo. Además que nos permite realizar respaldos estándar entre versiones de UNIX.

opciones

- c crea agrupación de archivos y/o directorios
- r agrega archivos o directorios al archivo **archivo.tar**
- v verbose
- x desagrupa o extrae los archivos y/o directorios en **archivo.tar**
- f especifica el archivo
- t visualiza los archivos y/o directorios en **archivo .tar**



find ruta expresion

El comando **find** se encarga de encontrar archivos y directorios que utilizan los comodines más usuales (*, ? y []). Nos permite buscar archivos que cubren criterios más complejos, como tiempo del último acceso, propiedades, establecimientos de banderas de permisos y tipo de archivo.

expresion**Descripción**

-atime n	si el archivo se acceso por última vez exactamente hace n días.
-atime +n	si el archivo se acceso por última vez hace más de n días.
-atime -n	si el archivo se acceso por última vez hace menos de n días.
-ctime n	si el archivo se cambió por última vez hace exactamente n días.
-ctime +n	si el archivo se cambió por última vez hace más de n días.
-ctime -n	si el archivo se cambió por última vez hace menos de n días.
-exec comando {} \;	Ejecuta comando.
-mtime n	si el archivo se modificó por última vez hace exactamente n días.
-mtime +n	si el archivo se modificó por última vez hace mas de n días.
-mtime -n	si el archivo se modificó por última vez hace menos de n días.
-name archivo	si archivo aparea un nombre de archivo (los caracteres comodines se deben entrecorillar)
-ok comando {} \;	Ejecuta comando, pero pregunta
-perm modo_octal	Archivos o directorios con los permisos especificados
-size n	si el archivo es exactamente n bloques de largo (n x 512 bytes).
-size +n	si el archivo es mas largo que n bloques (n x 512 bytes).
-size -n	si el archivo es menos de n bloques de largo (n x 512 bytes).
-type t	tipo de archivo
-user unombre	Por nombre
-group gnombre	Por grupo

TESIS CON
FALLA DE ORIGEN

1.2.3 Administración de UNIX

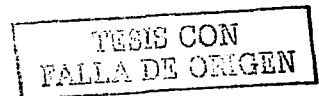
Requisitos y Tareas

Requisitos

- Tener conocimientos sobre utilerías UNIX, programación en shell, documentación del equipo, manuales en línea y sobre el hardware de la máquina.
- Ética. Debe respetar la información de tipo personal contenida en las cuentas de los usuarios.
- Actitud de servicio. Debe prestar ayuda a los usuarios buscando darles un buen servicio.

Tareas

- Controlar los recursos del equipo de acuerdo a las políticas de uso.
- Tener la responsabilidad de ofrecer acceso eficiente y efectivo al equipo, así como mantener su integridad.
- Conocer y utilizar el equipo que administra a nivel de usuario. Debe conocer sus características, componentes, configuración y posible crecimiento.
- Debe realizar documentación y procedimientos del equipo si no existe o bien mejorarla.
- Conocer los factores que bajan el rendimiento del equipo para ello debe de conocer, usar y monitorear el equipo diariamente.
- Debe planear las actividades que se realizarán en el equipo para avisarles a los usuarios con tiempo.
- Establecer políticas de uso y de administración e informar a los usuarios involucrados.
- Dar de alta y baja a usuarios, monitorear las actividades, asignar privilegios y determinar cuotas.
- Realizar respaldos de la información de los usuarios y del sistema operativo para restaurar los archivos que se requieran en un futuro. Estos respaldos deben de ser de forma periódica.
- Llevar un registro de los cambios realizados en el sistema a través de una bitácora.
- Conocer las aplicaciones que se instalen, poseer un manual de instalación del software a instalar.
- Actualizar las herramientas, parches y sistema operativo.



Cuentas de usuario

Las cuentas de usuario permiten tener acceso al sistema, son definidas en el archivo `/etc/passwd`, en donde se guarda las siguientes características:

- Nombre del usuario
- Grupo al que pertenecerá
- Tipo de shell a utilizar
- Directorio de trabajo

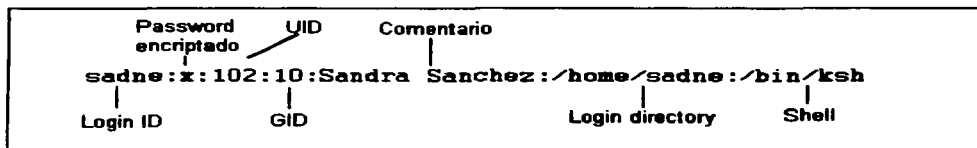


Figura 1.8 – Estructura de registro del `/etc/passwd`

Login ID: es el nombre del usuario, está limitado por 8 caracteres alfanuméricos, en minúsculas y debe ser único.

Password encriptado: mantiene este campo para la contraseña, la cual está contenida en el `/etc/shadow`. Este archivo contiene la contraseña encriptada. Sólo el administrador del sistema (`root`) puede leer este archivo.

UID: es el número del usuario para identificar al usuario dentro del sistema operativo. Los UID del 0 al 99 están reservados para cuentas del sistema (`root`, `daemon`, `bin`, `sys`, etc.), del 100 – 2147483647 para usuarios comunes, el 60001 está reservado para el usuario `nobody` y 60002 para `noaccess`.

GID: identifica el grupo primario al que pertenece el usuario.

Comentario: usualmente para poner los datos del usuario como el nombre completo.

Login directory: es el directorio base del usuario, comúnmente denominado "home", en el se guardan los archivos de los usuarios.

Shell: es el shell por defecto cuando el usuario entra al sistema.

Con el archivo `/etc/passwd` se maneja los usuarios, debido a que se almacena la información esencial de cada uno. Está dividido en 7 campos cada uno separado por dos puntos ":"

TESIS CON
FALLA DE ORIGEN

Comandos relevantes de administración**uptime**

Muestra la hora, tiempo que ha estado funcionando el servidor, los usuarios y el promedio del los procesos que están esperando ser atendidos por los procesadores.

uname

Con la opción `-a` despliega Sistema Operativo que está corriendo, el nombre de la máquina, la arquitectura, la versión del kernel y plataforma.

/usr/ucb/ps aux

Muestra todos los procesos ejecutándose en el sistema por uso de memoria y procesador.

sar 3 10

Despliega el porcentaje que está el Sistema Operativo sin actividad (idle), porcentaje de usuario, kernel y espera de operaciones de entrada y salida. En este caso el 3 es el número de segundos y el 10 el número de interacciones a desplegar.

df -k

Muestra el espacio libre y usado de los File Systems en KBytes.

swap -l

Muestra la memoria swap por areas, con este comando se puede ver la memoria swap adicional por archivo.

swap -s

Muestra la swap disponible y usada.

crontab -l [usuario]

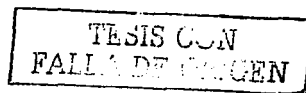
Muestra la definición de los crones que está ejecutando un usuario en particular.

last [usuario]

Muestra las últimas conexiones de los usuarios al sistema.

prtdiag

Muestra memoria RAM, procesador(es), tarjetas de entrada y salida del servidor.



format

Discos Duros disponibles para el servidor.

du . -k

Espacio en Kbytes de la ruta actual.

ifconfig -a

Muestra las tarjetas de red que se tienen, su dirección IP y direcciones MAC.

arch

Permite saber el tipo de arquitectura

netstat [opciones]

Muestra el estado de la red del servidor.

-r nos muestra las tablas de ruteo

-a muestra es estado de todos los sockets y todas las entradas de las tablas de ruteo, normalmente sockets usados por procesos del servidor no son mostrados y únicamente son mostrados la interface, host, red y default routers.

-n muestra las direcciones de red como números, despliega direcciones como símbolos.

En este Capítulo se trató sobre los fundamentos de UNIX y gran parte de su importancia, en el siguiente capítulo se abarcará todo lo referente al estudio previo a la realización del proyecto. Con lo que respecta a comandos más avanzados sobre UNIX se verá en el último Capítulo.

TESIS CON
FALLA DE ORIGEN

CAPÍTULO 2

Estudio de Factibilidad y Requerimientos para la migración

En el capítulo presente se describirá la situación del servidor Argon, su historia, rendimiento y problemática. Definiendo cuales son los puntos de estudio en cuanto a su arquitectura, herramientas y aplicaciones. Se propondrá el equipo y herramientas a instalar de acuerdo a una investigación previa sobre el servidor Argon. Finalmente se dará una descripción de la solución a la que se concluyó como la óptima medida para un mejoramiento en servicio de hospedaje de sitios web, empleando un dominio del equipo SUN Enterprise 10000.

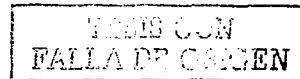
2.1 Definición del problema (del equipo origen)

2.1.1 Antecedentes.

El Departamento de Administración de Servidores tiene a su cargo los servidores centrales de Red de la UNAM, los cuales brindan principalmente los servicios de correo electrónico, FTP anónimo y hospedaje de páginas web dinámicas con bases de datos. Uno de los servidores que brindaba éste último servicio es el servidor llamado Argon con 117 sitios virtuales de web. Anteriormente brindaba servicio de correo electrónico a la comunidad universitaria con el nombre de Servidor, luego se reinstaló en el año de 1999 para reestructurar parcialmente el servidor de hospedaje de páginas web, denominado Dragon, debido a que presentaba problemas de mala organización en los directorios referentes a los sitios de web.

Argon por su crecimiento moderado en la demanda del servicio de hospedaje de páginas web, se le configuró un servidor de SYBASE para almacenar base de datos que pudieran ser accesadas desde un mismo sitio web. Ambos servidores Argon y Dragon se encuentran en el site de la DGSCA, Ciudad Universitaria.

Luego a principios del 2001, específicamente en febrero, surgió la necesidad de migrar el servidor Argon a un dominio de la Enterprise 10000, llamado Cobalto, este proyecto resultó en un fracaso por la falta de interés de los usuarios al no responder a las peticiones del administrador y por la dependencia presentada de algunas aplicaciones al sistema operativo (Solaris 2.5.1) que requerían algunos sitios para su correcto funcionamiento.



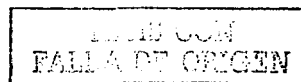
Posteriormente, en Mayo del 2001 por los movimientos normales de salida y entrada de personal a este departamento, se reasignó la tarea de administrar los servidores. Entonces, a mediados de noviembre del 2001 se me asignó el servidor Argon.

Al ir tomando las riendas de cómo administrar Argon encontré diversos problemas de optimización y administración del servidor por falta de documentación detallada y procedimientos, cabe señalar que sólo había unas bitácoras no actualizadas. Aunado a ésto la salida de los integrantes con mayor experiencia, el cambio de jefatura, la falta de herramientas de seguridad y el vencimiento de soporte técnico por parte del proveedor.

Como en todo lugar en donde se carece de metodologías, documentos, procedimientos y políticas van a surgir problemas debido a la falta del legado de conocimientos causado por la rotación del personal, no va existir en donde basarse para la realización de tareas cotidianas que ya han sido realizadas anteriormente sin problema alguno, va a existir falta de comunicación entre los antecesores y los nuevos integrantes. Esta fue la situación en el departamento de administración de servidores. Por ejemplo, nos dimos cuenta que los servidores eran administrados de una manera particular de los responsables, entonces fueron cumpliendo bien con su labor en mantenerlos funcionando, pero se llevaron los problemas más comunes, soluciones de los mismos, así como descripción detallada del servidor y recomendaciones para el mantenimiento del equipo.

Cuando los responsables administraban los equipos encontraban pequeños conflictos y los resolvían o quizá los acrecentaron. Realmente la capacidad de todos los integrantes no está puesta en duda, sin embargo cada quien tiene una manera de administrar equipos de cómputo, así como cada quien tiene una manera de administrar su casa, su negocio o su vida. Por eso una manera de solucionar los problemas sería organizando, estandarizando, administrando y documentando, tareas que actualmente se llevan a la práctica.

Actualmente, los servidores tienen un mejor rendimiento por modificaciones requeridas y realizadas, pero con la diferencia que existirán políticas dentro del Departamento de Administración de Servidores para que en un futuro las nuevas generaciones no detengan el proceso de aprendizaje en el área de administración de servidores y que cada vez sea mejor el servicio a la comunidad universitaria. Para que la UNAM siga siendo la pionera de diversas innovaciones en los servicios y tecnologías con respecto a otras instituciones educativas.



Todos los discos de la controladora 1 están bajo el dominio de DiskSuite, en el nivel de Raid 5 para tener una mejor disposición del espacio de disco de tal forma que tenga alguna falla, de lo contrario se tiene discos spare para los metadispositivos.

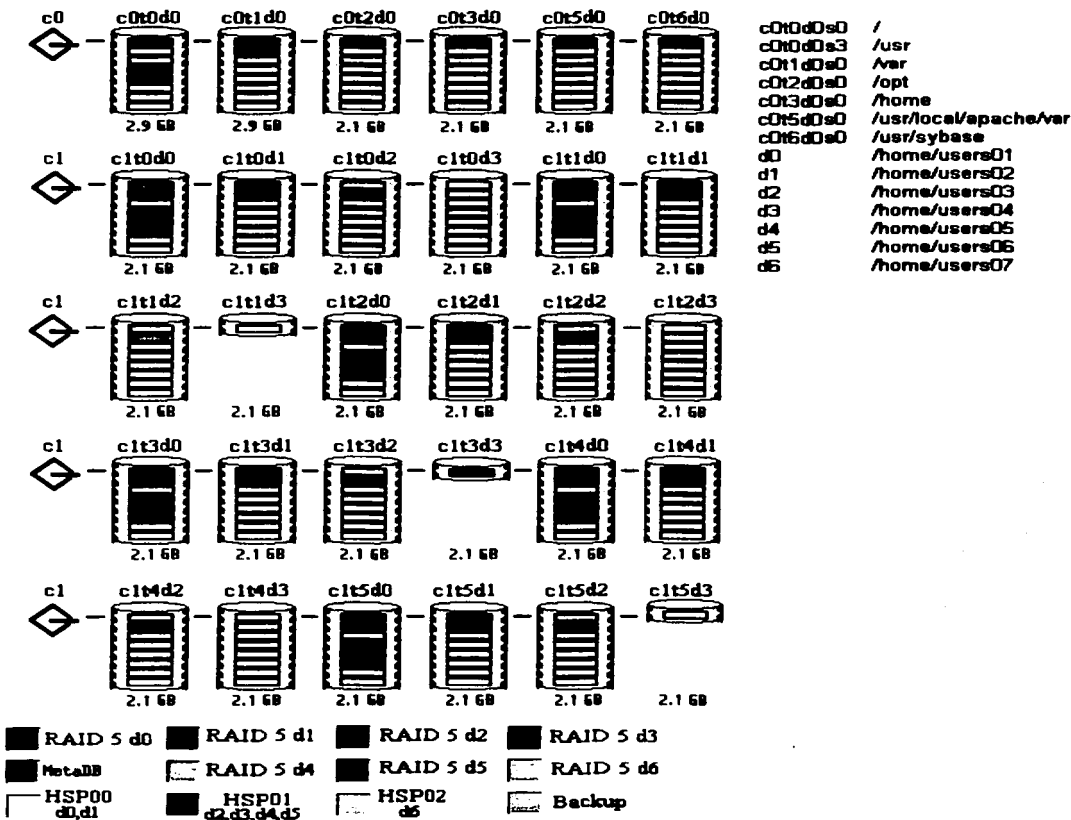


Figura 2.2 - Discos bajo DiskSuite

TESIS CON
FALLA DE ORIGEN

2.1.2 Partes constitutivas

El servidor Argon se encuentra alojado en un equipo Sun, específicamente en una SparcCenter 2000 (figura 2.1). Las características de cada uno de los elementos que la componen se detallan a continuación.

a) Descripción

Dominio: Argon

Nombre Máquina:

argon.servidores.unam.mx

Arquitectura: sun4d

Modelo: SPARCcenter-2000

Dirección IP: 132.248.10.6,
132.248.115.23

Host ID: 80742fc4

Ubicación equipo: Ciudad Universitaria

Cobertura de servicio técnico: sin servicio a estos equipos, SUN ya no lo brinda desde julio del 2001 por su antigüedad.

Memoria: 512 Megabytes

Procesadores: 8 procesadores sparc a
50 MHz

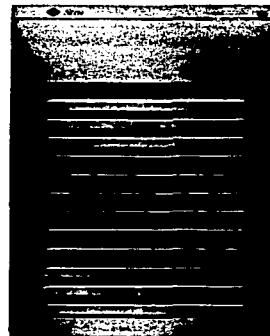


Figura 2.1 SparcCenter 2000

b) Discos

Los discos que se encuentran en la controladora 0 se relacionan con UNIX File Systems y los de la controladora 1 hacen referencia a metadispositivos (denominados con *dn*) de DiskSuite en RAID 5 (ver figura 2.2).

Argon tiene 30 discos duros, 2 de 2.9 GB y los restantes de 2.1 GB. Los pertenecientes a la controladora (c0) contiene S.O. y las aplicaciones. Los demás discos (en la controladora 1) pertenecen a un arreglo de discos para uso exclusivo de datos para los usuarios.

TESIS CON
FALLA DE ORIGEN

c) Sistema de Archivos (File Systems)

Un Sistema de archivos es un conjunto de archivos y directorios que está relacionado regularmente con un partición del disco, nos sirve para guardar datos y para controlar el espacio disponible. Los Sistemas de Archivos de Argon se pueden ver en la tabla 2.1. Ésta muestra el dispositivo lógico, tamaño y punto de montaje de los FS.

Sistema de Archivo	Tamaño (KBytes)	Punto de montaje
/dev/dsk/c0t0d0s0	95949	/
/dev/dsk/c0t0d0s3	866467	/usr
/dev/dsk/c0t1d0s0	2672342	/var
/dev/dsk/c0t3d0s0	1952573	/home
/dev/dsk/c0t2d0s0	1952573	/opt
/dev/dsk/c0t6d0s0	1952573	/usr/sybase
/dev/dsk/c0t5d0s0	1952573	/usr/local/apache/var
/dev/md/dsk/d0	5357784	/home/users01
/dev/md/dsk/d1	5357784	/home/users02
/dev/md/dsk/d2	4874601	/home/users03
/dev/md/dsk/d3	4881441	/home/users04
/dev/md/dsk/d4	4874601	/home/users05
/dev/md/dsk/d5	4881441	/home/users06
/dev/md/dsk/d6	4878401	/home/users07

Tabla 2.1 - Sistemas de archivos

```

/etc/vfstab
#device          device          mount          FS          fsck          mount          mount
#to mount       to fsck        point         type        pass         at boot      options
#
fd              /dev/fd fd          -          no          -          -
/proc          /proc proc        -          no          -          -
/dev/dsk/c0t0d0s1 /dev/rdsck/c0t0d0s0 -          swap
/dev/dsk/c0t0d0s0 /dev/rdsck/c0t0d0s0 /          ufs          1          no          -
/dev/dsk/c0t0d0s3 /dev/rdsck/c0t0d0s3 /usr         ufs          1          no          -
/dev/dsk/c0t1d0s0 /dev/rdsck/c0t1d0s0 /var         ufs          1          no          -
/dev/dsk/c0t3d0s0 /dev/rdsck/c0t3d0s0 /home        ufs          2          yes         -
/dev/dsk/c0t2d0s0 /dev/rdsck/c0t2d0s0 /opt         ufs          2          yes         -
/dev/dsk/c0t6d0s0 /dev/rdsck/c0t6d0s0 /usr/sybase  ufs          2          yes         -
/dev/dsk/c0t5d0s0 /dev/rdsck/c0t5d0s0 /usr/local/apache/var ufs          2          yes         -
/dev/md/dsk/d0 /dev/md/rdsck/d0 /home/users01 ufs          2          yes         -
/dev/md/dsk/d1 /dev/md/rdsck/d1 /home/users02 ufs          2          yes         -
/dev/md/dsk/d2 /dev/md/rdsck/d2 /home/users03 ufs          2          yes         -
/dev/md/dsk/d3 /dev/md/rdsck/d3 /home/users04 ufs          2          yes         -
/dev/md/dsk/d4 /dev/md/rdsck/d4 /home/users05 ufs          2          yes         -
/dev/md/dsk/d5 /dev/md/rdsck/d5 /home/users06 ufs          2          yes         -
/dev/md/dsk/d6 /dev/md/rdsck/d6 /home/users07 ufs          2          yes         -
swap          /tmp tmpfs        -          yes         -          -

```

Figura 2.3 - /etc/vfstab

TESIS CON
FALLA DE ORIGEN

En el proceso de alta del sistema existe una etapas de verificación de la integridad de los datos de los File Systems para posteriormente montarlos Sistemas de Archivos. El archivo donde se encuentran definidos es el vfstab dentro de /etc. En la figura 2.3 está el contenido de ese archivo. Las columnas se refieren al dispositivo lógico (donde están los datos), al dispositivo crudo (donde está la estructura del File System), al punto de montaje, el tipo de File System, cuantas veces revisará el File System cuando se corra la utilería fsck, si se monta al reiniciar el sistema, en la última columna puede habilitarse la opción de activación de cuotas.

d) Software instalado

En esta sección se lista las versiones de Sistema Operativo, aplicaciones y herramientas que se utilizaron en Argon, ver Tabla 2.2. La descripción de la mayor parte de los elementos se puede hallar en el Apéndice A.

Nombre	Versión
Solaris	5.5.1
Kernel	Generic_103640-29
Sendmail	8.9.3
BerkeleyDB	2.5.9
Gcc	2.8.1
Tcp-Wrappers	7.6
Perl	5.005_01
Gzip	1.2.4
OpenSSL	-
Zlib	-
Sybase	11.0.3
Apache	1.3.9
PHP	3 y 4
Groff	1.11
Libatdc++	2.8.1
Syperl	-
Pine	3.96
Pop	3
IMAP	4rev1 v11.241
Majordomo	1.94.4
Disk Suite	4.0
Front Page	Extensions 2000

*Fecha de última instalación de Parches: mayo de 1998

Tabla 2.2 - Software instalado

TESIS CON
FALLA DE ORIGEN

e) Cronos

Los crones nos permiten automatizar tareas que se realizan de forma periódica definidas en un archivo y ejecutados por un demonio denominado *crond*. En Argon no todos los usuarios pueden ejecutarlos sólo aquellos que estaban definidos en los archivos de control de acceso a este servicio (*/etc/cron.d*).

- Los usuarios autorizados: *cadmin, agn, arellano, latindex, servhem, isocmex, root, revista*
- La ubicación de los archivos ejecutados por el *crond*: */var/spool/cron/crontabs*

f) Scripts de inicio

Los scripts de inicio son tareas y servicios que se ejecutan de acuerdo al nivel que está corriendo el sistema operativo. Como los scripts de inicio no varían significativamente entre las versiones del sistema operativo, solamente se tomará en cuenta aquellos creados por el propio el administrador o los que están considerados como más relevantes para el funcionamiento del sistema.

Script adicional: /etc/rc3.d/S90brokers: este script levanta la herramienta de Harvest, la cual es un sistema para recopilar información, para poder hacer uso de ella a través de una interface de web, usando para este caso el servicio http. Esta herramienta la empleaba un usuario en especial del sistema, la cual no se considera trascendental para los demás usuarios.

TESIS CON
FALLA DE ORIGEN

2.1.3 Rendimiento actual de la plataforma

Siendo Argon una plataforma de hospedaje de páginas web, se dio la facilidad de que los usuarios desarrollaran aplicaciones en el mismo servidor, así como de emplear las herramientas que necesitaban y para ello podían instalarlas ellos mismos, pero realizando la aclaración que si es necesario el cambio o migración de versiones de software en el servidor, el administrador sólo estaba comprometido a hacer funcionar el software común para todos los usuarios. Al darles libertad de instalar las herramientas que necesitaran se fue perdiendo parte del control en cuanto a procesamiento y espacio en disco. Aunada que no se consideró el crecimiento a futuro que alcanzaría al instalar las herramientas que requerían los usuarios. La falta de espacio en disco trajo como consecuencia no actualizar software común y por consiguiente huecos de seguridad. No se agregaron más discos porque ya no los fabrican.

Como se mencionó anteriormente el equipo Argon es bastante obsoleto, siendo difícil de encontrar las herramientas si llegase a fallar algunos de sus componentes. Ésta fue una de las principales razones para la realización de la migración del sistema, debido que existe otro equipo SparcCenter 2000 que ya dejó de funcionar uno de sus componentes, afortunadamente no era un servidor en producción.

Para verificar el rendimiento de Argon se utilizó una herramienta de monitoreo, el MRTG (Multi Router Traffic Grapher).

El MRTG

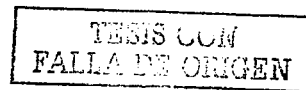
La principal característica de esta herramienta de tipo *GNU*, el MRTG¹², es que monitorea el ancho de banda, aunque no es lo único que puede monitorear, debido a que utiliza el protocolo *SNMP*¹³ para recoger datos del dispositivo que queremos vigilar.

Otra característica del MRTG es que no está limitado a monitorear el tráfico en la red sin embargo, es posible monitorear cualquier variable *SNMP* que se escoja o se puede usar un programa externo escrito en C, Perl o Shell, que obtenga los valores que deseamos graficar.

Debido a que está escrito en lenguaje C y en Perl hace que se moldee a nuestras necesidades.

¹² <http://people.ee.ethz.ch/~oetiker/webtools/mrtg/>

¹³ Protocolo de transferencia para las direcciones IP asignadas por el servidor.

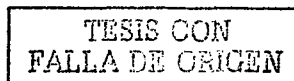


El MRTG genera páginas HTML con imágenes de formato *PNG*, que son de tipo GNU. Anteriormente generaba imágenes tipo *GIF*, pero se decidió cambiar para evitar problemas de derechos de autor. Trabaja bajo plataformas UNIX y Windows NT.

La página HTML generada contiene cuatro gráficos que nos representan los resultados durante el día, la semana, el mes y finalmente durante el año. El archivo de configuración genera una página de tipo HTML por cada etiqueta, ésta debe de tener un número consecutivo para crear la página índice que contenga todas nuestras gráficas. Una de las ventajas es que genera un *archivo .log*¹⁴ donde guarda los datos anteriores, sin crecer demasiado como otros archivos log, permitiéndonos monitorear diversos parámetros.

Para este proyecto se va a emplear scripts en shell para monitorear diversos aspectos de administración. Se utilizó ssh para la obtención de los resultados generados por los scripts que estaban ejecutándose en un cron dentro de Argon.

El servidor que tiene instalado MRTG es Titanio. El motivo que no se emplea SNMP es porque es muy vulnerable a ataques de desbordamiento de pila (buffer overflow). Además, el servidor no cuenta con éste servicio por la versión de Sistema Operativo y el personal del Departamento de Redes es el encargado de monitorear la red en los routers. En la figura 2.4 se muestra las gráficas generadas por día, las pueden consultar se en el sitio <http://www.servidores.unam.mx/sadne/mrtg>.



¹⁴ Archivos donde se guarda las bitácoras, o bien reportes de lo que hace la aplicación

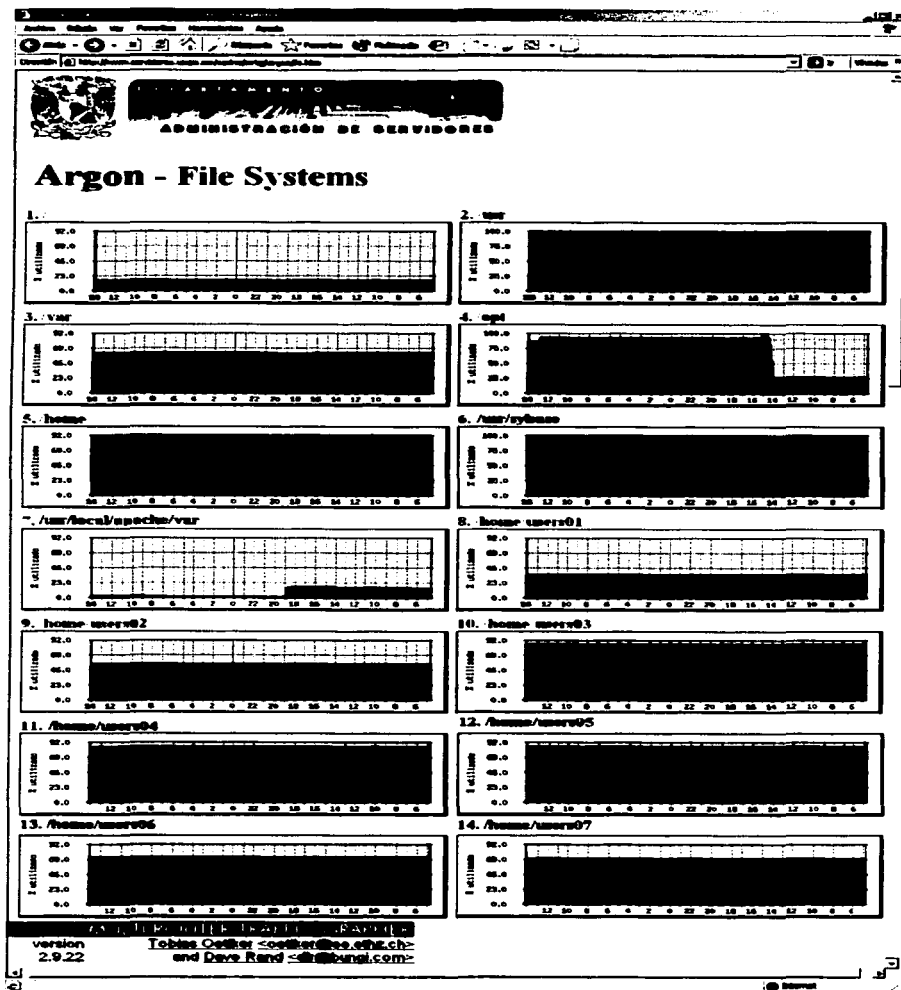


Figura 2.4 – Página índice de monitoreo MRTG - File Systems

TESIS CON
FALLA DE ORIGEN

Los diversos factores de Argon que se monitorean con el MRTG son los siguientes:

Sistemas de archivos (filesystem)

Los diferentes Sistemas de Archivos en Argon son monitoreados cada uno para verificar que no haya un comportamiento extraño en cuanto al crecimiento del espacio en disco. Las gráficas que los representan en la figura 2.4:

1. /
2. /usr
3. /var
4. /opt
5. /home
6. /usr/sybase
7. /usr/local/apache/var
8. /home/users01
9. /home/users02
10. /home/users03
11. /home/users04
12. /home/users05
13. /home/users06
14. /home/users07

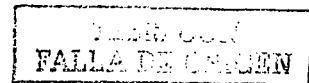
Los sistemas de archivos que no deben de variar demasiado en tamaño son:

/	normal 18%
/usr	normal 97%
/usr/sybase	normal 98%

Un sistema de archivos no debe de exceder del 90%, principalmente / y /var ya que puede volverse inestable el sistema, siendo el caso de Argon

Reporte de actividad del Servidor

Las gráficas 1 y 2 (Figura 2.5) nos muestran el porcentaje que el sistema está siendo utilizado por los usuarios, el sistema, operaciones de entrada y salida (wio) y la inactividad del servidor (Idle). La suma de las tres primeras no debe ser el 100%.



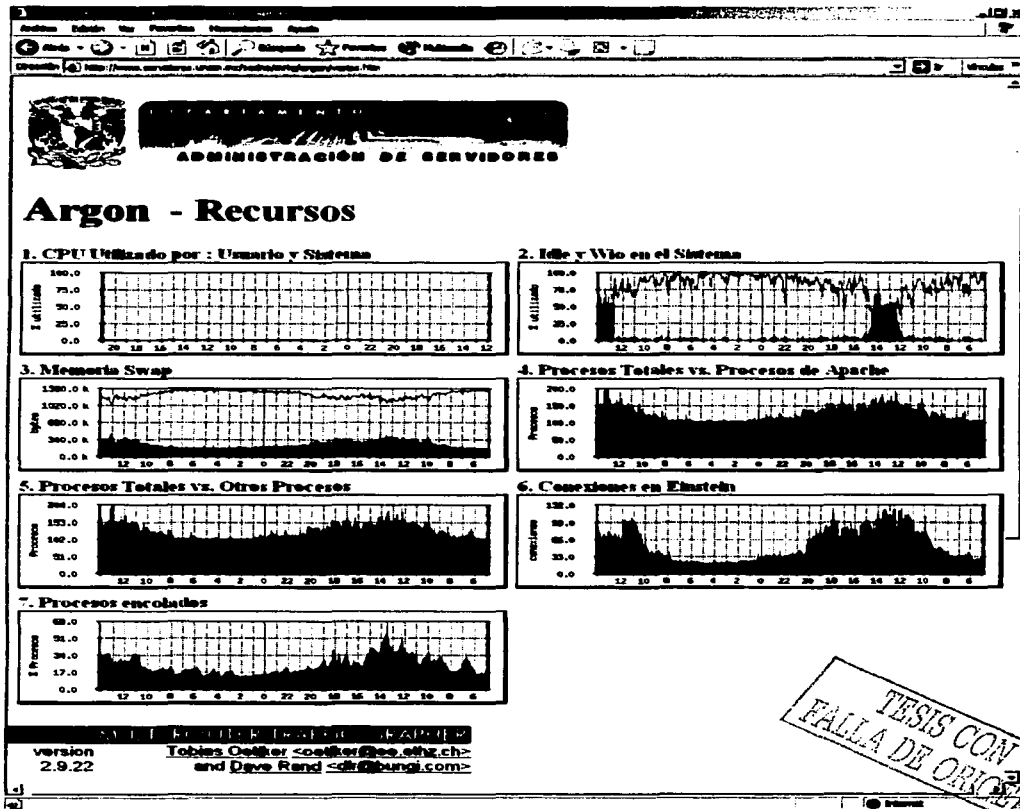


Figura 2.5 – Página índice de monitoreo MRTG - Actividad del servidor

Las gráficas que representan estos puntos son:

6. *Idle y Wio en el Sistema* En donde la parte sombreada se refiere al Wio y la línea azul representa el Idle.

10. *CPU Utilizado por: Usuario y Sistema* En donde la parte sombreada se refiere al porcentaje de CPU utilizado por el usuario y la línea azul representa el CPU utilizado por el kernel.

11. Las operaciones de entrada y salida se entiende como lectura y escritura de datos en el disco, se puede verificar el incremento cuando se hace algún respaldo del sistema.

El comando para ver los datos mencionados se pueden obtener con "sar".

Debemos verificar que la inactividad (idle) del sistema no sea muy pequeña, si llegase a suceder debemos identificar cual o cuales de los tres aspectos están afectando a nuestro servidor. Por ejemplo si existen muchas operaciones de lectura y escritura posiblemente algún cron esté generando bitácoras muy grandes o está recibiendo mucho correo electrónico nuestro servidor.

Memoria Swap

La parte sombreada corresponde a la memoria usada y la línea azul a la disponible. Para saber ésto se usa el comando `swap -s` (gráfica 3)

Procesos

Como es un servidor de Web principalmente se toma en cuenta los demonios de Apache que estén corriendo.

En la gráficas de "4. Procesos Totales vs. Procesos de Apache", la parte sombreada corresponde a los procesos totales la línea azul es el número de demonios de Apache.

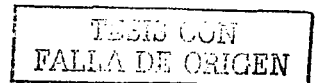
En la gráficas de "5. Procesos Totales vs. Otros Procesos", la parte sombreada son los procesos totales y la línea azul corresponde a otros procesos que no sean nobody (Apache) y de root.

Conexiones

En la gráfica 6 se visualiza el número de conexiones actuales que se hacen al servidor por los diferentes puertos abiertos (la parte sombreada) y las conexiones de los usuarios a través de una terminal dada (línea azul).

Procesos Encolados

Este aspecto se refiere al número de procesos que están esperando ser atendidos por los procesadores, estos datos son tomados cada 5 y 15 minutos de la salida del comando "uptime" (gráfica 7)



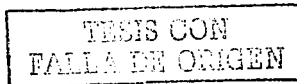
2.2 Análisis de factibilidad

A continuación se darán a conocer los diferentes aspectos que considero de suma importancia para llevar a cabo la migración de Argon a un equipo que brinde mayor rendimiento

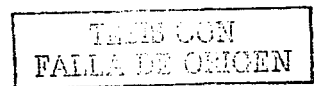
2.2.1 Expectativas y situación original de Argon

En esta sección se pretende explicar la situación actual de Argon y las acciones que se tomarían para mejorarla, entonces las letras en negritas son las expectativas y lo demás es la situación actual.

- **Disponer de un arreglo de discos con espacio suficiente para hospedar el sistema operativo, herramientas e información de los sitios con soporte técnico disponible por parte del proveedor.** Debido al crecimiento moderado que tiene Argon, ya no cuenta con espacio en disco para atender las demandas de crecimiento actuales, como actualización de sistema operativo y aplicaciones, así como dar hospedaje a más sitios web. Además, lo más importante, por ser un equipo antiguo no cuenta con soporte técnico por parte de SUN Microsystems, desde julio del 2000, ya que el proveedor lo considera obsoleto. Si llegase a fallar alguno de sus componentes no se tendría la asesoría, ni el repuesto para atender la falla y por consiguiente no se podría dar el servicio como se ha ido prestando.
- **Actualizar el sistema operativo y herramientas requeridas por los usuarios.** Otro factor importante es una nueva versión de sistema operativo que permita la utilización de herramientas actuales requeridas por los usuarios. Aunando otras bondades de las recientes versiones de Solaris. Argon está corriendo el sistema operativo Solaris 2.5.1, el cual es superado por Solaris 2.6, 2.7, 8 y 9.
- **Emplear un equipo de mayor capacidad de procesamiento.** Para que una computadora se considere de buen rendimiento debe considerarse uno de los elementos más importantes, el procesador, componente central del hardware de la computadora, es el encargado de hacer todos los cálculos para llevar a cabo una acción en específico, estas tareas se ejecutan a una velocidad dada, entre mayor sea la velocidad serán más rápidos los cálculos. El procesamiento de las computadoras se ha incrementado conforme van surgiendo nuevos modelos con tecnologías innovadoras. Por las características del equipo SparcCenter 2000 se puede describir como una computadora de bajo procesamiento, entonces para ello se debe de emplear un equipo más reciente.



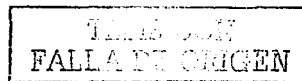
- **Disponer de una mayor capacidad de memoria RAM.** Como se mencionó anteriormente no sólo el procesamiento es el único elemento importante para considerar un equipo ofrezca un buen rendimiento, también lo es la memoria RAM, ya que no es útil un equipo con un procesador de alta velocidad de cálculo sin el dispositivo donde guarde las aplicaciones y los archivos mientras está trabajando con ellos. De igual manera el equipo SparcCenter 2000 no tiene la memoria suficiente para el buen funcionamiento de las aplicaciones y debe considerarse en la elección del nuevo equipo de cómputo a emplear en este proyecto.
- **Realizar "espejeo" del sistema operativo y de la información de los usuarios.** Con esta medida podremos estar, en cierto punto, tranquilos en tener la información de los usuarios replicada en otros discos con las mismas características a los originales. Sería de gran ayuda por si se llega a dañar un disco, podrá entrar el otro en su auxilio. Y nos evitaría la recuperación completa de la información almacenada en cintas, que es bastante lento y en algunas ocasiones incierto de recuperación total. El espejeo de sistema operativo e información no está disponible en Argon.
- **Depuración de sitios obsoletos.** Algunos de los sitios virtuales de web hospedados en Argon no son vigentes por diversas razones como: el motivo de su desarrollo fue para dar a conocer algún suceso temporal, el responsable administrativo del sitio no tiene los conocimientos suficientes para hacer los cambios pertinentes, o simplemente por olvido. La desventaja de tener información estática trae un desperdicio de cintas para hacer respaldos periódicos y la principal razón, Argon sufre por la falta de espacio. Entonces, los sitios candidatos para migrarse, tendrán que ser vigentes. Aquellos que no lo sean, podrán ser enviados a otro servidor exclusivo de sitios históricos, si así lo solicite el responsable, de lo contrario será eliminada la información en el servidor y se le brindará una copia de su sitio en cdrom, a través de una petición escrita.
- **Quitar el servicio de correo electrónico.** Argon además de servidor de hospedaje de páginas web, también cuenta con servicio de correo electrónico entrante y saliente. El servicio de correo entrante que no se debería brindar por el problema del *spam* y por las vulnerabilidades de Sendmail¹⁵. Solamente se deberá permitir enviar correo electrónico por parte de los usuarios, debido a que algunas secciones de los sitios lo requieren para su funcionamiento.



¹⁵ Es un MTA (Mail Transport Agent) el cual nos sirve para recibir y transportar correo entre computadoras.

- **Implementar, publicar y utilizar políticas para los usuarios y administradores.** Existen algunas políticas para los usuarios en cuanto al uso de Argon, que se saben por palabra, pero no existe ningún documento que avale por si llegase haber alguna falta por parte de los usuarios o administradores. Para la realización del proyecto se tendrá que contemplar este aspecto de suma importancia para ambas partes, usuario y administrador.
- **Automatizar tareas comunes para el administrador.** Algunas de las tareas que se realizan día con día deberán de ser de forma automática para no asignar espacios de tiempo grandes y disminuir los factores de error en su ejecución. Las tareas más comunes son respaldos periódicos, registro de estadísticas y monitoreo de bitácoras.
- **Replicar los sitios web en otro servidor por hardware o software.** Por hardware se requiere de otro equipo y por software se emplea el servidor Apache haciendo modificaciones en el httpd.conf. Por hardware se hace un gasto considerable y es empleado por empresas con recursos suficientes.
- **Implementar medidas de seguridad.** Existen dos aspectos importantes con respecto a la seguridad del equipo, una es la ubicación física y la otra la intrusión o ataques a nuestro sistema. La primera va relacionada con las políticas a establecer, así como el acondicionamiento de la sala de máquinas; con respecto a la seguridad del equipo SparcCenter 2000 está bien protegido con una red de cámaras de video y en un área controlada para permitir el acceso a personas autorizadas. La segunda no ha sido contemplada estrictamente, ya que no se cuenta con las herramientas de seguridad mínimas que requiere el sistema, calificando a Argon un servidor sumamente vulnerable, ya que está abierto el acceso a cualquier equipo. Para ello se debe contemplar instalar herramientas de seguridad y además bien configuradas.

2.2.2 Beneficios para la DGSCA



Como en todas las organizaciones ya sean gubernamentales, privadas o en su caso educativas la imagen del servicio que se presta es el punto más importante para ellas. En este caso el Departamento de Administración de Servidores presta un servicio a la comunidad universitaria y aquellas instituciones que lo requieran, el servicio de hospedaje de páginas web debe ser impecable para todos sus usuarios internos y externos.

- Disponibilidad de todos los sitios que estén bajo nuestra administración.
El usuario estará satisfecho si siempre que visite su página web, ésta se encuentre disponible.
- Alto rendimiento.
No sólo la disponibilidad es parte de esta confianza, también debemos tomar en cuenta que el acceso a la información sea el adecuado.

- Confiabilidad.

El hecho de saber el usuario que los datos transferidos al servidor es realmente lo que esperaba ver es parte de una buena imagen, no podemos permitir que su información se encuentre alterada de su original.

- Buena administración.

El contar con políticas y procedimientos hace las tareas de un administrador más sencillas, así como la transferencia de conocimientos es mucho más óptima al tener todo bien documentado. Si un proyecto cuenta con la documentación necesaria estamos alargando su vida útil.

- Contabilidad del sistema

Nos referimos para contabilidad del sistema a las estadísticas de uso y rendimiento de los servidores, ayudándonos a una buena planeación de las capacidades del sistema. Para que en un futuro se pueda prever con tiempo la obsolescencia del sistema.

TESIS CON
FALLA DE ORIGEN

2.3 Determinación y selección de los elementos a implementar

Entendiéndose como elementos a la plataforma, arreglo de discos, sistema operativo, herramientas y aplicaciones.

La DGSCA tiene a su cargo tres máquinas SUN Enterprise 10000, específicamente el Departamento de Administración de Servidores. Dos plataformas se encuentran físicamente en la DGSCA y la tercera en el site de Pitágoras. La única que no está en producción es la denominada "Musicos", en la DGSCA, porque sólo es empleada por el personal capacitado de SUN para impartir cursos sobre la misma. La otra Enterprise 10000 en la DGSCA, tiene 3 dominios, Dragon, Cobalto y Krypton. Actualmente, Dragon y Cobalto están en producción con el servicio de hospedaje de páginas Web, Krypton es un dominio que no está a nuestro cargo sino de la DGAE¹⁶. Científicos, la tercera Enterprise 10000, de igual forma tiene tres dominios, Einstein, Euler y Newton. Euler da el servicio de Ftp Anónimo y los otros dos están disponibles.

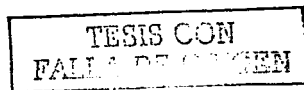
En marzo del 2001 arribó la Enterprise 10000 a Pitágoras como parte de un convenio por pronto pago de la primera que se adquirió, la Enterprise 10000 en producción. El proyecto que se propuso era para tener un espejo de toda la información contenida en la de producción. Aunque por motivos que desconozco no se pudo llevar a cabo.

Debido a las características de alto rendimiento de estos equipos se decidió por Einstein para que brinde hospedaje de páginas web, únicamente de sitios provenientes de Argon, sitios de la UNAM o sitios de suma importancia.

Servidor Sun Enterprise 10000

El servidor Sun Enterprise 10000 (también conocido como Starfire) se considera una plataforma muy escalable y posee características muy especiales, como el rendimiento de 3150 MIPS equivalentes de mainframe, 64 GB de memoria compartida y arriba de 12 GB/seg de ancho de banda en el sistema para una mayor transferencia de datos, soporta arreglos de discos de almacenamiento masivo (como sistema StorEdge T3 de Sun), soporta hot-swap para agregar o reemplazar componentes al vuelo sin reiniciar el sistema (aunque en la realidad no funciona como originalmente planteó SUN), entre otras características que han servido para ser calificada por empresas importantes como un servidor de alto rendimiento y rentable.

¹⁶ Dirección General de Asuntos Escolares



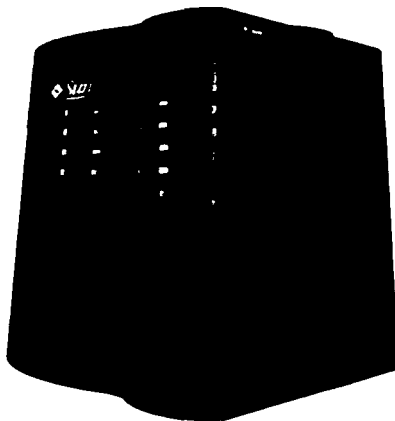


Figura 2.6 - Enterprise 10000

La Figura 2.6 muestra al equipo Enterprise 10000 vista de perfil, el lado derecho está la parte frontal de la misma.

Capacidad:

Software

Compatible con el sistema operativo Solaris 2.5.1, 2.6, 5.7, 5.8 y 5.9.

Procesadores:

No. De procesadores: de 4 a 64 a una velocidad de 400 MHz.

Arquitectura: Superscalar SPARC Versión 9, UltraSPARC.

System Boards

No. de System boards: máximo 16 system boards por Enterprise 10000, mínimo 1 system board cada una puede contener hasta 4 procesadores, 4 tarjetas Sbus, un módulo de memoria con 4 bancos de 8 SIMMS y un máximo de 4GB de memoria.

Memoria principal

2 GB a 64 GB de capacidad por plataforma.

TESIS CON
FALLA DE ORIGEN

Tarjetas estándar que soporta

Sbus bus de datos de 64 bits a 25 MHz.

PCI bus de datos de 64 bits a 33 o 66 MHz con charola especial.

Almacenamiento de datos

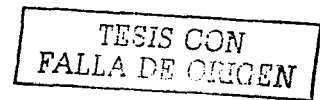
Arreglos de discos: Arreglo Sun StorEdge A7000 (UltraSCSI almacena 2,9 TB)
 Arreglo Sun StorEdge A5200
 (canal de fibra almacena 200 GB, 400 GB, 800 GB o 1.2 TB por arreglo)
 Arreglo Sun StorEdge A3500
 (UltraSCSI almacena hasta 6.4 TB por arreglo)
 Arreglo Sun StorEdge D1000 hasta 50 GB, 109 GB o 144 GB

Fuentes de poder

Máximo 8 fuentes de poder en redundancia.

Ventiladores

Máximo 16 fan tray (cada fan tray tiene 2 ventiladores).

**Características¹⁷:**

- System Domains: grupos de system boards que pueden correr copias independientes de Solaris, cada una está aislada de errores de hardware o software que puedan ocurrir en otro dominio¹⁸ (pero en la realidad si ocurre un error afecta a los demás componentes). Como máximo se puede tener 16 dominios y 16 copias de Solaris.
- Una máquina externa para controlar la plataforma, llamada SSP (System Service Processor), la cual permite una administración remota. Consiste en una estación de trabajo Ultra 5 o un servidor Enterprise 250 con Solaris 2.6 como mínimo. Las tareas que realiza son las siguientes:
 - 1) Crea, reconfigura e inicializa los dominios.
 - 2) Monitorea y muestra los niveles de temperatura y voltaje
 - 3) Monitorea y controla la potencia para los componentes dentro de la plataforma.
 - 4) Ejecuta programas de diagnóstico en un dominio como el POST
 - 5) Crea Inter Domain Network

¹⁷ Sun Enterprise 10000 Administration, Student Guide.

¹⁸ Un dominio consiste en una o más system boards agrupadas lógicamente dando la apariencia de un solo servidor, debido a que corre una versión de Solaris independiente. Un dominio puede estar compuesto por todas las systems boards disponibles.

- 6) Contiene los logs de interacción entre la SSP y los dominios
- 7) Desempeña Dynamic Reconfiguration
- Inter Domain Network (IDN) permite una velocidad de red muy alta entre los dominios para mayor velocidad de transferencia de datos, reducción de carga de la red externa y comunicación entre dominios, consolas de administración de plataforma (SSP) y Control Board.
 - Network virtual console (netcon), es una sesión de consola que se abre a través de la SSP para leer la salida y escribir a la consola del dominio. Se puede abrir varias consolas al mismo tiempo, pero sólo una tiene permisos de escritura.
 - Hostview graphical user interface (GUI), herramienta en la SSP que nos permite monitorear y controlar la Enterprise 10000 a través de una interfaz gráfica.
 - Alternate pathing, son rutas alternas duales al mismo dispositivo de E/S, dando redundancia a nivel de controladora y cableado.
 - Blacklist, es una lista de componentes que controla el hardware de un dominio que no está disponible.
 - Dynamic Reconfiguration (DR), el administrador puede agregar, quitar o reemplazar muchos componentes en línea del sistema sin alterar la producción que está siendo en uso. Se puede emplear DR para actualizar una system board, modificar la configuración del hardware de un dominio, reparar una system board que falla, crear un dominio de prueba, entre otros.
 - Mantenimiento concurrente, las fuentes de poder, ventiladores y unidades reemplazables FRUs pueden ser quitadas en "caliente", mientras el sistema esté activo.
 - Corrección de errores de interconexión, los buses de datos y direcciones son protegidos por una combinación de corrección de errores de códigos y paridad.

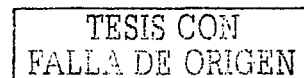
TESIS CON
FALLA DE ORIGEN

CAPÍTULO 3**Metodología para la migración del sistema**

Para la elaboración de este proyecto se realizó un estudio previo de los requerimientos de configuración, definiendo los aspectos más importantes a través de una lista de componentes a instalar y configurar. La determinación de qué herramientas y sus versiones a emplear está respaldada con una etapa previa de pruebas realizada en un servidor con características similares, permitiéndonos determinar y solucionar las posibles fallas. De igual manera para actualizaciones se recomienda no hacer caso omiso de la etapa de pruebas y detección de fallas. En ambos casos debe revisarse la documentación¹⁹ brindada junto con la herramienta.

El software se instaló en Einstein tomando las medidas recomendadas de la etapa de pruebas y revisando los manuales y documentos concernientes a la configuración de herramientas y aplicaciones necesarias para este proyecto de investigación. Cabe señalar que cualquier cambio en la configuración se documenta para posibles modificaciones a corto o largo plazo; la actualización de las herramientas se emplea de acuerdo a las innovaciones publicadas en los sitios oficiales y a las indagaciones de estabilidad.

La migración de Argon se realizó basándose en las etapas del área de Administración de la Configuración que a continuación se describe:

3.1 Instalación y configuración del hardware y el software.

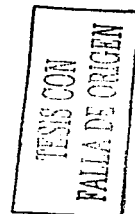
En esta etapa se realizó un estudio preliminar de compatibilidad y puesta en marcha en un servidor de pruebas con características similares para posteriormente elaborarse en el servidor destino. Además, se definió la fecha de ejecución²⁰ y se hizo un estimado sobre el tiempo de duración de la instalación de las diversas herramientas y aplicaciones. Las herramientas a instalar fueron en su mayoría las mismas a las instaladas en el servidor Argon, sin embargo con las versiones más recientes y estables, dichas herramientas se listan en la tabla 3.1

¹⁹ La documentación utilizada se refiere a manuales de sistema operativo y README

²⁰ La realización de la instalación de Sistema Operativo y las herramientas duró aproximadamente una semana, la configuración y finalización del software requerido por los usuarios fue durante un mes. Debido a que herramientas como Volume Manager y DiskSuite requiere tener precaución en la realización del espejeo de los datos.

Software de Sistema Operativo, Aplicaciones Web y Bases de Datos	Aplicaciones para correo electrónico
Gcc	Sendmail
Tcp-Wrappers	BerkerleyDB
Perl	Groff
Gzip	Pine
OpenSSL	Pop
Zlib	IMAP
Sybase	Majordomo
Apache	Front Page
PHP	
Syberpl	
Disk Suite	

Tabla 3.1 – Software instalado en Argon



Algunas herramientas no se instalaron, por el hecho de no ser indispensables para el funcionamiento óptimo de los sitios web o bien por algunas recomendaciones de seguridad, las herramientas se muestran en la tabla 3.1.

Sendmail no fue instalado porque no es recomendable tener servicios de Internet mezclados, por el simple hecho de si existiese una excesiva carga en la recepción de correo en el servidor, afectaría en la consulta de los sitios web por el aumento de procesos que están esperando ser atendidos por los procesadores. De esta manera, se podrá brindar mayor disponibilidad de un servicio a los usuarios. Esta medida se tomó porque en parte de la investigación del uso del servicio de correo electrónico era prácticamente nulo por parte de los usuarios, y la mayoría de ellos gozan del servicio brindado por Servidor y Correo UNAM. Las otras herramientas son necesarias para el uso de correo como son las restantes *BerkerleyDB*, *Groff*, *Pine*, *Pop*, *IMAP* y *Majordomo*²¹, exceptuando *Front Page*.

Con respecto a la última herramienta listada, *Front Page*, no se instaló debido a que los cambios o actualizaciones realizadas al sitio los transfieren al servidor a través del protocolo de FTP, el cual es uno de los servicios más inseguros por permitir que viajen en claro login y contraseña y si alguna persona con intenciones maliciosas “escucha” lo que pasa por la red puede hacer cambios nada agradables en esa cuenta.

La compatibilidad de las herramientas empleadas fue exitosa, sencillamente porque se manejó el mismo tipo de sistema operativo, sólo con una versión más vigente (Solaris 8). Aunando que la mayoría de las aplicaciones a emplear son los códigos fuente, mismos que son configurados,

²¹ Si se desea saber más de estas herramientas, se puede dirigir al Apéndice A para mayor información.

compilados y finalmente instalados, exceptuando por Sybase y Veritas Volume Manager que requiere licencia y son instaladas por medio de una aplicación.

La instalación del hardware es realizada por personal autorizado de SUN Microsystems para evitar la pérdida de la garantía, en este caso no se requirió ningún cambio físico de los componentes debido a que la configuración se realiza en el momento de instalar el software requerido.

Un aspecto muy importante a no olvidar al realizar cambios importantes a un servidor en producción, es que dichos cambios no son transparentes para el usuario, se debe notificar anticipadamente y generar un plan alterno por si llega haber alguna falla. En el caso de ésta instalación no se notificó, ya que no estaba dando servicio alguno.

Para no hacer tediosa esta sección la descripción de la instalación y configuración de las herramientas más importantes se puede consultar en el Apéndice A.

TESIS CON
FALLA DE ORIGEN

TESIS CON FALLA DE ORIGEN

3.2 Migración de los datos

En la parte de análisis de factibilidad se tocó el punto de la depuración de los sitios y de no migrar los datos por migrarlos, es por ello que en esta etapa los datos referentes a los sitios se hizo en base a una investigación de cómo estaba desarrollado un sitio y qué importancia tiene, entonces se contactó a los responsables administrativos y técnicos.

La etapa de investigación de qué herramientas utilizaba el desarrollador del sitio web en Argon, consistió en los siguientes pasos:

1. Se envió un correo electrónico a todos los usuarios de Argon para notificarles la migración del mismo, así como también se le anexó un cuestionario (figura 3.1) con el fin de obtener más datos de los sitios web y cuentas UNIX. Desde esta etapa pude constatar que no se hacía uso del servicio de correo brindado en Argon y por tanto no obtuve respuesta de todos los usuarios sólo aproximadamente de quince.
2. Indagación de quiénes eran los responsables técnicos o administrativos y en dónde localizarlos. Realmente se volvió una indagación ardua, por la falta de un documento, base de datos, o cualquier medio electrónico donde se pudiera obtener una relación de sitio y responsable. Entonces, se brindó una lista de los sitios en Argon al responsable de la Coordinación de Servicios de Red y al responsable del departamento de Publicaciones Digitales, los cuales son los que desarrollan la mayoría de los sitios para la UNAM. También se dio la lista de sitios al personal que estaba encargado de brindar el servicio de hospedaje de sitios web para instituciones u organismos no pertenecientes a la UNAM. Lamentablemente no se pudo obtener los suficientes responsables, debido a que varios sitios web pertenecían a usuarios que no requerían que se desarrollara su sitio por algún departamento en particular, es decir únicamente pidieran una cuenta y desarrollaban el sitio web.
3. Contactar a los responsables para notificarles sobre la migración. Primeramente, se hizo una llamada telefónica para que nos dieran un correo electrónico, enviarles el cuestionario y respondieran a *migracion@servidor.unam.mx*²². No todos contestaron el cuestionario, pero los que sí lo hicieron, se fue migrando su sitio. De aquellos que no se tenía contacto, busqué en su sitio alguna dirección de correo electrónico o nombre del responsable y le envié el cuestionario. Aun así faltaban contactos, aunque cabe señalar que contestaron el correo electrónico enviado.

²² Cuenta de correo electrónico que fue creada especialmente para tratar sobre la migración de Argon.

Por medio del presente se le informa que el servidor `argon.servidores.unam.mx` tendrá que ser migrado.

Argon será migrado a un equipo con más capacidad debido a que ha crecido drásticamente, ya no cuenta con espacio para atender las demandas de crecimiento actuales, y lo que es más importante, debido a su antigüedad, el equipo ya no cuenta a partir de julio del 2000 con soporte del proveedor por lo que si algún componente llegase a fallar, no obtendríamos la asesoría ni la parte de repuesto para atender la falla.

Otro de los motivos por lo cual es conveniente la migración es porque se le desea brindar un mejor servicio, los beneficios de dicha migración son importantes puesto que usted como administrador del sitio se vería beneficiado con:

- * Mayor capacidad de procesamiento.
- * Mayor rapidez en operaciones.
- * Mayor rapidez de acceso a los datos, entre otras cosas.

Por esta razón se le pide su total comprensión y participación para que este proyecto de migración pueda llevarse a cabo con éxito, proporcionándonos algunos datos sobre sus sitios que se encuentran alojados en este servidor, para hacer un análisis sobre que requerimientos se van a necesitar para dicha migración.

Si llegase a tener mas de un sitio a su cargo, favor de responder por cada sitio las siguientes preguntas:

RESPONSABLE:
DEPENDENCIA:
E-MAIL:
TELÉFONO:

- 1) ¿Cuál es su sitio(s) [URL]?
- 2) ¿Su sitio hace uso de GIS?
- 3) ¿Qué aplicación usa para hacer esos GIS y mencione si tienen dependencia de algún sistema operativo?
- 4) ¿Qué lenguaje de programación de páginas web utiliza y que módulos? (PHP, Perl)
- 5) ¿Su sitio ocupa Bases de Datos (Sybase)? ¿Cuáles son las Bases de Datos y su usuario?
- 6) ¿Por medio de qué servicio se conecta al servidor? (telnet, ftp, ssh, scp, etc).
- 7) ¿Desde qué dirección o direcciones IP se conecta al servidor o bien si es por módem que proveedor le proporciona el servicio?
- 8) Mencione que cuentas de usuario y/o de correo tiene en el servidor
- 9) Indique algunas sugerencias u observaciones en cuanto al servicio que se le brinda.

Cabe notar que entre más pronto sea brindada la información, se agilizará la migración de su(s) sitio(s). Siembre y cuando los requerimientos de su sitio vayan de acuerdo con las aplicaciones existentes en nuevo servidor.

El equipo donde se migrarán los sitios es Einstein, el cual cuenta con varias políticas para su uso, para informarse visite la página <http://einstein.servidores.unam.mx>

Sin más por el momento le agradezco su fina atención.

Jefe del Depto - Ing. Jesús Fernández Rauda

Departamento de Administración de Servidores
www.servidores.unam.mx
D.T.D. D.G.S.C.A. U.N.A.M.

Tel:56228568 56228249

Figura 3.1 – Correo electrónico enviado a los usuarios de Argon

TESIS CON
FALLA DE ORIGEN

4. Dar de baja temporal a sitios. Una vez migrado un sitio se fue comentando en el *archivo de configuración*²³ del Apache, indicando fecha y motivos. Al no tener contacto de los responsables decidí dar de baja temporalmente el sitio, aprobado por el director de la DTD; esperando que el usuario al verificar que su sitio no era visible nos contactara. Aun, al terminar la migración de los sitios con contacto del responsable, fueron pocos los que no se comunicaron para reactivar el funcionamiento de su sitio, por tanto era un indicio de no necesario.

Para la elaboración de la migración de los sitios se clasificó en dos categorías:

- Sitios desarrollados con HTML
- Sitios dinámicos con acceso a Bases de Datos Sybase

Esta clasificación se realizó debido que se considera más delicado migrar un sitio con interacción a una Base de Datos, por las transacciones que se realizan y por los datos que se manejan dentro de ellas. En cambio sitios desarrollados con código HTML o PHP se debe cuidar que no empleen rutas absolutas para correr algún programa o para PHP el empleo de una variable en específico. Este último caso no se dio, ya que al instalarlo se contempló dicho aspecto.

Los procedimientos a emplear fueron los siguientes:

PARA SITIOS DESARROLLADOS CON HTML

1. Obtención de datos de usuarios.

- login asociado al sitio web, para ello verificar en la tabla de usuarios (archivo passwd dentro de /etc)

```
root@argon # grep login /etc/passwd
```

- Cadena de contraseña relacionada con el login, guardada dentro del shadow en /etc

```
root@argon # grep login /etc/shadow
```

- Cuota asignada

```
root@argon # quota -v login
```

<p>TESIS CON FALLA DE ORIGEN</p>

²³ Este archivo se encuentra por lo regular en /usr/local/apache/conf y es denominado httpd.conf.

2. Crear Usuario.

- **Agregar el grupo²⁴.** En este caso se colocará el mismo ID al usuario y al grupo, así como el mismo nombre, para evitar modificaciones de archivos por mala asignación de permisos

```
root@einstein # groupadd <nom_grupo>
```
- **Verificar el UID²⁵ y el login, el UID debe ser consecutivo y el login no debe repetirse**

```
root@einstein # tail /etc/passw
```
- **Agregar el usuario**

```
root@einstein # useradd -u<UltimoIDuser+1> -g<GID> \  
-c"aquí se pone una descripción o comentario" \  
-d/home/users03/<usuario> -m -s </rutadel/shell> <usuario>
```
- **Agregar la contraseña encriptada en la columna correspondiente dentro del shadow**

```
root@einstein # vi shadow
```
- **Definirle una cuota al usuario, se debe de introducir en Kbytes, la primera es la suave y la segunda es la dura (ej. Suave: 150000, Dura: 153600; son 15MB)**

```
root@einstein # edquota <usuario>
```
- **Verificar la cuota, esté correctamente asignada al File System especificado en el archivo passwd.**

```
root@einstein # quota -v <usuario>  
Disk quotas for <usuario> (uid <UltimoIDuser+1>):  
Filesystem usage quota limit timeleft files quota limit timeleft  
/home/users?? 0 150000 153600 0 0 0
```

3. Copiar los archivos pertenecientes al usuario.

```
root@argon # cd ~login  
  
root@argon # scp -r * root@einstein:/home/users03/usuario
```

4. Cambiar dueño a los archivos.

```
root@einstein # chown -R login:grupo /home/users03/usuario
```

5. Copiar configuración del Apache (Einstein) referente al sitio virtual.

```
root@argon # vi httpd.conf  
root@einstein # vi httpd.conf
```

6. Revisar configuración del Apache y reiniciarlo.

```
root@einstein # apachectl configtest  
root@einstein # apachectl restart
```



²⁴ El GID (Identificador de Grupo) debe ser irrepitible. El nombre del grupo y el GID se encuentran dentro del archivo group en /etc.

²⁵ Como los primeros 100 UID están reservados para sistema (0 – 99) se tomó a partir del 100, aunque algunos administradores inician desde el 1000, de cualquier forma ambos son correctos.

7. Verificar que funcione correctamente el sitio.

Para ello hay que "engañar" a una máquina (en este caso plata), entonces se especificará en un archivo el dominio que apunta a la dirección IP definida. De esta forma los cambios realizados en Einstein no serán visibles para todos los demás, debido a que el protocolo HTTP busca directamente en el DNS si no está definido el dominio en el archivo hosts²⁶. Entonces, editamos el archivo.

```
root@plata# vi /etc/hosts
132.247.12.13 www.sitio.unam.mx
```

De esta forma los cambios realizados en el sitio www.sitio.unam.mx en Einstein sólo serán visibles para los que modificaron el archivo hosts. Asegurándonos que al solicitar el cambio en el DNS de la UNAM no haya falla en visualizar el sitio web migrado.

- 8. Solicitar a través de un reporte al personal del NIC el cambio de direccionamiento del DNS.**
- 9. Brindar un shell inválido a la cuenta del usuario en Argon.**

PARA SITIOS DINÁMICOS CON ACCESO A BASES DE DATOS SYBASE

- 1. Obtención de datos de usuarios.**
- 2. Crear Usuario.**
- 3. Copiar los archivos pertenecientes al usuario.**
- 4. Cambiar dueño a los archivos.**
- 5. Copiar configuración del apache (Einstein) referente al sitio virtual.**
- 6. Revisar configuración del Apache y reiniciarlo.**
- 7. Crear la Base de datos.**

- Entrar como usuario *sybase*

```
root@einstein # su - sybase
sybase % isql -Usa -w600
```

- Crear dispositivos

```
1> disk init name="nomDev>0", physname="/SWsybase/nomDev.dat", \
vdevno=<n>, size=<m>
2> go
```

<p>TESIS CON FALLA DE ORIGEN</p>

²⁶ El archivo hosts se denomina de igual forma en Windows como en UNIX, sólo que para el primero se encuentra dentro de la carpeta Windows y para el último en /etc.


```
1> disk init name="<nomDev>log0", \
physname="/SWsybase/<nomDev>.log", vdevno=<n>, size=<m>
2> go
```

- Creación de las bases de datos

```
1> create database <nom_BD> on <nomDev>0=<x> log on <nomDev>log0=<x>
2> go
```

- Creación del usuario de la base de datos

```
1> sp_addlogin <nom_login>,"<password>",<nomDB>
2> go
1> use <nomBD>
2> go
1> select db_name()
2> go
1> sp_changedbowner <nom_login>
2> go
1> use master
2> go
```

- Respalidar Base de Datos en Argon

```
root@argon # su - sybase
sybase % isql -Usa -w600
1> dump database <nomDB> on "/tmp/<nomDB>.dbf"
2> go
```

- Recuperar la base de datos

```
root@argon # scp "/tmp/<nomDB>.dbf" root@einstein:/tmp
root@einstein # su - sybase
sybase % isql -Usa -w600
1> restore database <nomDB> on "/tmp/<nomDB>.dbf"
2> go
1> online database <nomDB>
2> go
```

NOTA: verificar qué opciones tiene la base de datos y activarlos.

TESIS CON
FALLA DE ORIGEN

8. Verificar que funcione correctamente el sitio.

9. Solicitar a través de un reporte al personal del NIC el cambio de direccionamiento del DNS.

10. Brindar un shell inválido a la cuenta del usuario en Argon.

En el proceso de investigación de responsables y migración de sitios decidí clasificarlos de acuerdo a:

Baja definitiva, en la tabla 3.3 están aquellos sitios que no estarán activos por ordenes del responsable, para ello se solicita la baja en el DNS y obviamente en el servidor web (Apache).

Baja por migración, éstos son los sitios que se dieron de baja en Argon y de alta en Einstein, son aquellos que se consideran vigentes. Se cambia el direccionamiento del DNS para posteriormente dar de baja en el Apache de Argon (tabla 3.4).

Baja temporal, los sitios que no se encontró responsable, sólo se dieron de baja en el servidor de web de Argon (tabla 3.5).

Cuentas sin responsable, son aquellas que no han sido utilizadas o bien no se puede contactar al dueño (tabla 3.6).

Las tablas 3.2, 3.3 3.4 y 3.5 contienen un listado de los usuarios, sitios Web y Base de Datos en Argon.

La tabla 3.2 muestra los sitios que se eliminaron dentro del sistema, los motivos fueron por no ser vigentes, no eran funcionales o bien ya no se requerían.

La tabla 3.3 contiene los sitios que fueron eliminados por haber sido migrados a Einstein, clasificándolos por departamento o bien por otras dependencias.

La tabla 3.4 está la lista de los sitios que por falta de contacto se suspendió temporalmente el servicio. En un inicio era mayor la lista, pero conforme veía el usuario que el sitio Web no era accesible viendo una página temporal donde estaban nuestros datos, nos llamaba y le hacíamos el cuestionario para poder migrarlo.

La tabla 3.5 contiene los usuarios que no se relacionaba ningún sitio Web, aunque si tuvieran una Base de Datos.

TESIS CON
FALLA DE ORIGEN

BAJA DEFINITIVA		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
agn	www.agn.gob.mx	
amecider	www.amecider.org.mx	
amep	www.amep.org.mx	
ampil	www.ampil.org.mx	
apuntes	apuntes.aragon.unam.mx	
arq	arquitectura.posgrado.unam.mx	
avm	www.avm.org.mx	
bdigital	www.bibliodigital.unam.mx	
bosque	www.bosque-antiguo.org.mx	
busqadm	busqueda.unimex.edu.mx	
	busqueda.invdex.com.mx	
	busqueda.isocmex.org.mx	
	busqueda.cultural.unam.mx	
cadmin	busqueda.dgsca.unam.mx	
	www.contacto.unam.mx	
cae	contacto.unam.mx	
cae	cae.cpa.unam.mx	(12) cae - sa (15MB)
Ciees	www.ciees.edu.mx	
	busqueda.ciees.edu.mx	
Coloquio	www.coloquio-ccar.unam.mx	
comie	www.comie.org.mx	
compu200	www.computo2000.unam.mx	(26) computo2K - computo2K (70MB)
computo99	www.computo99.unam.mx	
coobco	www.coobco.com.mx	
dgdi	www.dgdi.unam.mx	
dialogo	www.dialogo.unam.mx	
educont	educont.dgsca.unam.mx	
em	www.ermexico.com	
farmacia	www.farmacia.unam.mx	
fca	contad.web.unam.mx	
fundpaz	www.fundacionpaz.org.mx	
furtado	www.redcelsofurtado.edu.mx	
hebraica	www.hebraica.edu.mx (BAJA)	
hilos	www.hilos.com.mx	
ict	Telecom.fi-b.unam.mx	
	www.ict-2000.unam.mx	
juridicas	www.juridicas.unam.mx	
	info.juridicas.unam.mx	
oye	www.oye.com.mx	
papilt	www.etica.com.mx	
plebunam	www.plebiscito.unam.mx	
pnueva	www.politicanueva.org.mx	
serunam	www.serunam.unam.mx	
unamhoy	www.unamhoy.unam.mx	
unimex	www.unimex.edu.mx	
wwwedm	Resultados.plebiscito.unam.mx	

TESIS CON
FALLA DE ORIGEN

Tabla 3.2 - Sitios-Baja definitiva

BAJA POR MIGRACIÓN		
Departamento Publicaciones Digitales		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
bibilweb	cae.cpa.unam.mx sac.servidores.unam.mx bibloweb.unam.mx	
cys	www.cys.unam.mx	
latindex	www.latindex.unam.mx	(16) latindex - latindex (530MB)
mmolina	www.nobel.unam.mx	
papiro	www.papiro.unam.mx	(25) papiro - papiro (150MB)
realia	www.realia.unam.mx	
revista	www.revista.unam.mx	(18) RDU - revista (8 MB)
Servhem	Serinfo.unam.mx	
Departamento Coordinación de Servicios de Red		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
bibliotk	www.bibliodgsca.unam.mx	
busqueda	www.busqueda.unam.mx	
dgsca	www.dgsca.unam.mx	
hmexico	www.h-mexico.unam.mx	(14) hmexico - hmexico (50MB)
invdes	www.invdes.com.mx	
Departamento Sistemas		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
compra	www.compra.unam.mx	(30) compra - dbcompra (30MB)
tdgsca	www.tienda.dgsca.unam.mx	(20) tienda_dgsca - dgsca (40MB)
Externos		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
diariomx	www.diariodemexico.com.mx	
isocmex	www.isocmex.org.mx	
Departamento Administración de Servidores		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
avisoa	www.avisos.unam.mx	
sac	sac.servidores.unam.mx	(7) sac-sacadm (100MB)
webmail	www.correo.unam.mx	(19) webmail - webmail (120 MB)
www	www.servidores.unam.mx	
Diversos		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
aerosol	Aerosoles.cca.unam.mx	
ateneo	www.ateneo.unam.mx	
biblio	biblioteca.dgsca.unam.mx	
catedrah	catedradh.unesco.unam.mx www.catedradh.unesco.unam.mx	
cbta	www.congresocbta.unam.mx	
cepe	www.cepe.unam.mx	
cusuti	www.cusautitan2.unam.mx	
chopo	www.chopo.unam.mx	
derecho	www.derecho.unam.mx	
dgee	www.evaluacion.unam.mx	(24) dgeeguila-dgeeguila
dirunam	www.directorio.unam.mx	(6)dirunam-dirunam (100MB)
ecolson	www.ecol-son.unam.mx	

TESIS CON
FALLA DE ORIGEN

ems	www.ems.unam.mx	
esteticas	www.esteticas.unam.mx	
fundunam	www.fundacion.unam.mx	
geologia	www.geologia-con.unam.mx	
hemerotk	www.hemerodigital.unam.mx	(17) hemeroteca - hemero (15MB)
l2unam	internet2.dgscs.unam.mx	
pumas	www.pumas.unam.mx	
registro	www.clavesredunam.unam.mx	(15) registro - regadm (12MB)
siae	www.dgae-siae.unam.mx	
simbio	www.simbiosis.unam.mx	
sistemas	sistemas.dgscs.unam.mx	
suc	www.suc.unam.mx	
tablada	www.tablada.unam.mx	
telemat	www.telematica.unam.mx	
visuales	www.artesvisuales.unam.mx	

Tabla 3.3 - Sitios Baja por Migración

BAJA TEMPORAL		
USUARIO	SITIO VIRTUAL	BASE DE DATOS
antroit	www.anroit.unam.mx	
arqedu	www.arqedu.unam.mx	
balletf	www.balletf.unam.mx	
conspa	www.padron.unam.mx	
cpa	www.cpa.unam.mx	(10) cpa - cpa (5MB)
digital	digital.dgscs.unam.mx	
dpida	www.dpida.unam.mx	
edusalud	www.edusalud.unam.mx	
evaluapc	evaluapc.dgscs.unam.mx	
fonsida	www.fonsida.unam.mx	(21) fonsida - fonsida (15MB)
gieh	www.gieh.unam.mx	
infotel	www.infotel.unam.mx	(22) infotel - infotel (97MG)
prucobi	www.prucobi.unam.mx	
redpuma	www.redpuma.unam.mx	
rim	www.rim.unam.mx	
sintesis	www.sintesis.unam.mx	
walc2000	www.walc2000.unam.mx	
webaries	aries.intercambio.unam.mx	
webdgia	www.intercambio.unam.mx	

Tabla 3.4 - Sitios Baja Temporal

TRIS CON
FALLA DE ORIGEN

<i>Cuentas sin responsables</i>		
USUARIO	CORREO VIRTUAL	BASE DE DATOS
alepez		
bhg		
bibliote		
buzonfe		
catalina		
cbta	cbta@congresocbta.unam.mx*	
cesar		
clasificado		(23) clasificado - clasificado (40MB)
coorfcpa		
ch		
dgesii		
diariom1	correo@diariodemexico.com.mx	
diariom2	admon@diariodemexico.com.mx	
docencia		
e10k		
erasto		
fomed		
foros		(24) foros - foros (15MB)
realia	correo@realia.unam.mx*	
revista	correo@revista.unam.mx*	(18) RDU - revista (8 MB)
susfcps		
tlaca		(9) tlacaele1 - tlaca (100MB)

Tabla 3.5 - Cuentas sin responsable

* Ya se cuenta con contacto del responsable

TESIS CON
FALLA DE ORIGEN

3.3 Documentación

Documentar cada tarea realizada durante el proceso de instalación y configuración tiene como fin obtener una descripción detallada y precisa de cómo se emplea cada recurso, así como el estado en que se liberó el proyecto. Las características de configuración del servidor Einstein, se describen a continuación, como referencia para cambios en la configuración, así como también auxilio en las tareas propias de administración.

a) Descripción:

Esta sección contiene los aspectos más importantes que se requieren para la instalación de herramientas, parches o bien para mantenimiento por parte del proveedor, son las características que a grandes rasgos nos pueden definir el rendimiento basándose en el Hardware.

Dominio: einstein

Plataforma: científicos

Systems Boards: 1

Nombre Máquina: einstein.servidores.unam.mx

Arquitectura: sun4u

Modelo: Ultra-Enterprise-10000

Número de serie: 7003A

Dirección IP: 132.247.12.13

Host ID: 80A69534

Ubicación equipo: Matias Romero # 1220, col. Del valle, México, D.F.

Cobertura de servicio: SunSpectrum Oro 7x24 / 2 hrs.

Memoria: 2048 Megabytes

	Memory	Units:	Size	
	0: MB	1: MB	2: MB	3: MB
	----	----	----	----
Board 1	1024	1024	0	0

Figura 3.2 - Memoria RAM

Las figuras 3.2, 3.3 y 3.4 muestran respectivamente memoria RAM, tarjetas de Entrada/Salida y Procesadores. Para el caso de la memoria, se observa que se tiene dos slots de memoria ocupados cada uno con 1 GB, en el caso de los procesadores se tiene 4 a 400 MHz.

TESIS CON
FALLA DE ORIGEN

I/O Cards:

Brd	Bus Type	Freq MHz	Slot	Name	Model
1	Sbus	25	0	SUNW,qfe	SUNW,sbus-qfe
1	Sbus	25	0	SUNW,qfe	SUNW,sbus-qfe
1	Sbus	25	0	SUNW,qfe	SUNW,sbus-qfe
1	Sbus	25	0	SUNW,qfe	SUNW,sbus-qfe
1	Sbus	25	0	QLGC,isp/sd (block)	QLGC,ISP1000
1	Sbus	25	1	SUNW,socal/sf (scsi-3)	501-5266
1	Sbus	25	1	QLGC,isp/sd (block)	QLGC,ISP1000

Figura 3.3 - Tarjetas de Entrada/Salida

Procesadores: 4x400MHz Ecache 8MB

Brd	CPU	Module	Run MHz	Ecache MB	CPU Impl.	CPU Mask
1	4	0	400	8.0	US-II	10.0
1	5	1	400	8.0	US-II	10.0
1	6	2	400	8.0	US-II	10.0
1	7	3	400	8.0	US-II	10.0

Figura 3.4 - Procesadores

TESIS CON
FALLA DE ORIGEN

b) Discos:

Recomendaciones de SUN. Los discos para datos no pertenecientes para sistema operativo deberán estar bajo el dominio de Veritas Volume Manager ²⁷ y los discos con el Sistema Operativo deberán estar espejeados con DiskSuite, debido a que es más fácil cambiar el disco activo con éste software. Por tanto se empleó esta recomendación.

La figura 3.5 muestra los metadispositivos que emplea DiskSuite, éstos describen los File System de sistema operativo, espejeados. El motivo de la realización del espejo es que si llega a dañarse el disco duro, puede ocuparse el espejo indicándole a *nivel 0*²⁸ cual es el dispositivo. Cabe aclarar como es un espejo cualquier cambio realizado en un disco se ve reflejado en el otro, o sea si se borra un archivo, no se puede recuperar al menos que haya un respaldo previo. Para el caso de d1 (/) se tomo la partición 0 de los discos que están en la controladora 0 y 1

²⁷ Veritas Volume Manager es una herramienta que permite tener un mejor desempeño y disponibilidad referente a los discos, manejando objetos físicos (discos duros) y virtuales (volúmenes).

²⁸ Véase Capítulo 4, niveles de inicialización.

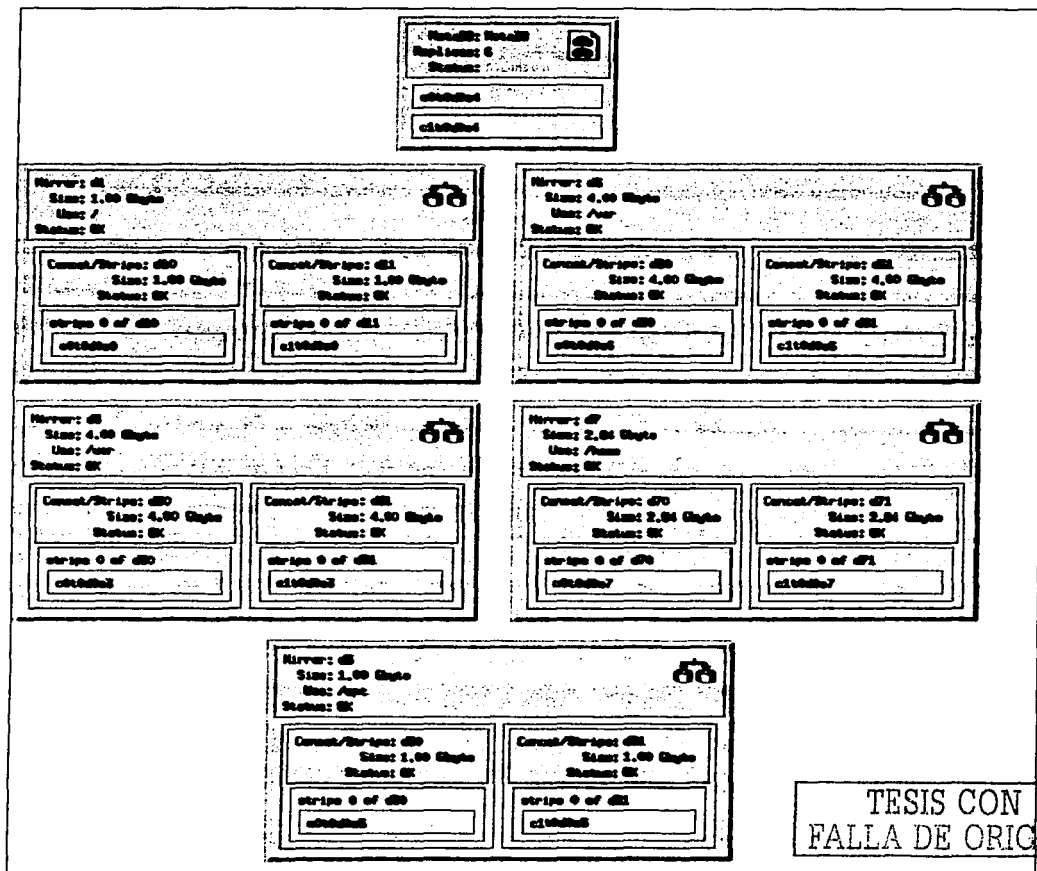


Figura 3.5 - Discos bajo DiskSuite

La Figura 3.6 representa los mismos metadispositivos, pero en este caso se muestran las particiones de los discos. Por ejemplo, para el metadispositivo d1 hace referencia a /, el cual se compone de otros dos (d10 y d11), cada uno se le asignó una partición en diferentes discos y controladoras, pero con el mismo tamaño.

Los únicos discos bajo DiskSuite son los que se encuentran en la controladora 0 y 1. Los otros 7 discos están bajo Volume Manager.

Se debe aclarar que se tiene 7 discos y no 14 discos como se aparenta al dar el comando format. Esto se debe a que el arreglo tiene 2 controladoras (c2 y c3), por si llega a fallar una.

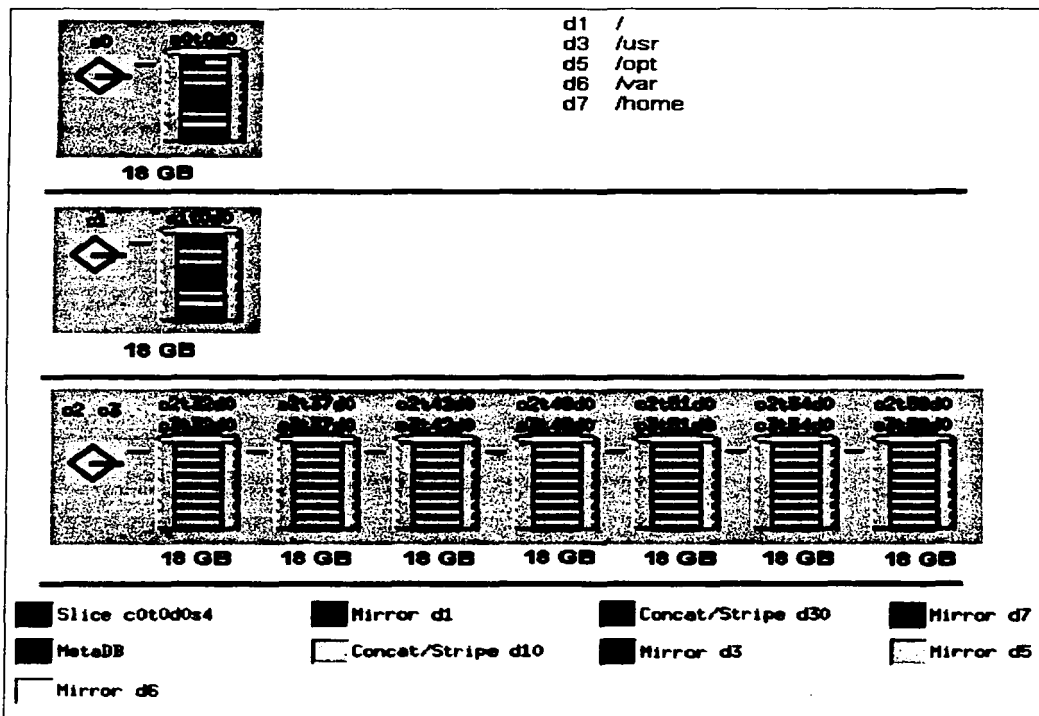


Figura 3.6 - Discos disponibles y discos bajo el dominio de DiskSuite

TESIS CON
FALLA DE ORIGEN

La Figura 3.7 representa los discos, File Systems y Volúmenes que están bajo el dominio de Volume Manager. De igual manera los volúmenes están espejados, éstos almacenan los datos de los usuarios.

Volume Manager Disks							
	Disk Name	Disk Group	Size	Unused	State	Spare	Reserved
	c0r0d0s2	-	0	-	Not Setup	-	-
	c1t0d0s2	-	0	-	Not Setup	-	-
	c2t32d0s2	disk01	16.9 G	0	Imported	No	No
	c2t37d0s2	disk02	16.9 G	0	Imported	No	No
	c2M2d0s2	disk03	16.9 G	16.9 G	Imported	No	No
	c2t40d0s2	disk04	16.9 G	16.9 G	Imported	No	No
	c2t51d0s2	disk05	16.9 G	0	Imported	No	No
	c2t54d0s2	disk06	16.9 G	0	Imported	No	No
	c2t50d0s2	disk07	16.9 G	16.9 G	Imported	Yes	No

Discos Volume Manager
 Discos - S.O. (Disk Suite)

Volume Manager File Systems							
	Mount Point	FS Type	Size	Used	Available	Capacity	
	/dev/vx/dsk/rootdg/vol01	/home/logs	ufs	7.9 G	40.7 M	7.1 G	1%
	/dev/vx/dsk/rootdg/vol02	/home/users01	ufs	4.0 G	9.0 K	3.8 G	1%
	/dev/vx/dsk/rootdg/vol03	/sybase	ufs	5.9 G	236.9 M	5.6 G	4%
	/dev/vx/dsk/rootdg/vol04	/SWsybase	ufs	3.9 G	606.6 M	3.3 G	16%
	/dev/vx/dsk/rootdg/vol05	/home/users03	ufs	6.8 G	1.7 G	5.0 G	26%
	/dev/vx/dsk/rootdg/vol06	/home/users02	ufs	3.9 G	9.0 K	3.6 G	1%

Volume Manager Volumes							
	Size	Disk Group	State	Mount Point	#Copies	Type	
	8.4 G	rootdg	Started	/home/logs	2	Concatenated	
	4.2 G	rootdg	Started	/home/users01	2	Concatenated	
	6.0 G	rootdg	Started	/sybase	2	Concatenated	
	4.0 G	rootdg	Started	/SWsybase	2	Concatenated	
	6.9 G	rootdg	Started	/home/users03	2	Concatenated	
	4.2 G	rootdg	Started	/home/users02	2	Concatenated	

Figura 3.7 Configuración de discos con Veritas Volume Manager

En la primera parte están los discos que tiene Einstein, los dos primeros no están bajo el dominio de Volume Manager. En la segunda parte están los File Systems que hacen regencia a un Volumen, el tipo de File System, tamaño y cuanto está siendo usado. La tercer parte muestra los 6 Volúmenes pertenecientes al mismo grupo "rootdg".

TESIS CON
FALLA DE ORIGEN

c) **Software instalado:**

Para mayor información sobre las características de cada software, así como su instalación consultar el Apéndice A.

<i>Nombre</i>	<i>Versión</i>	<i>Versión</i>
Sistema Operativo	SunOS 5.8	SunOS 5.5.1
Version Kernel	Generic_106541-20	Generic_103840-29
Patchcheck	1.1	No instalado
Veritas Volume Manager	3.0.4	No instalado
Gcc	2.95	2.8.1
Tcp-Wrappers	7.6	7.6
Perl	5.6.1	5.005_01
Gzip	1.3	1.2.4
OpenSSL	0.9.6b	Desconocida
Zlib	1.1.4	Desconocida
Open Secure Shell	3.0p1	No instalado
Sybase	11.1.1	11.0.3
Apache	1.3.24	1.3.9
PHP	4.1.2	3 y 4
Oracle cliente	8.1	No instalado
Portentry	1.1	No instalado
Disk Suite	4.2	4.0
Explorer	3.5.2	No instalado
Nullmailer	1.00RC5	No instalado

*Fecha de última instalación de Parches a Einstein: 10 de Enero del 2003

Tabla 3.6 - Software instalado

Si se compara la lista de Software instalado en Argon con la de Einstein se nota que se cambio significativamente en las versiones (Tabla 3.6)

TESIS CON
FALLA DE ORIGEN

d) Configuración de los Sistema de Archivos

Sistema de Archivos	Tamaño (Kb)	Punto de montaje
/dev/md/dsk/d1	1018191	/
/dev/md/dsk/d3	4131866	/usr
/dev/md/dsk/d6	4131866	/var
/dev/md/dsk/d7	1952573	/home
/dev/md/dsk/d5	1018191	/opt
/dev/vx/dsk/rootdg/vol03	6192654	/sybase
/dev/vx/dsk/rootdg/vol04	4128430	/SWsybase
/dev/vx/dsk/rootdg/vol05	7083105	/home/users03
/dev/vx/dsk/rootdg/vol02	4143839	/home/users01
/dev/vx/dsk/rootdg/vol06	4140255	/home/users02
/dev/vx/dsk/rootdg/vol01	8287950	/home/logs

Tabla 3.7 - Sistemas de Archivos

```

/etc/vfstab
#device      device      mount      FS      fsck      mount      mount
#to mount    to fsck     point      type     pass     at boot   options
#
#/dev/dsk/c1d0s2 /dev/rdsk/c1d0s2 /usr      ufs      1         yes      -
fd          -          /dev/fd fd      -        no        -
/proc       -          /proc proc      -        no        -
/dev/dsk/c0t0d0s1 -          -          swap     -        no        -
/dev/md/dsk/d1 /dev/md/rdsk/d1 /          ufs      1         no        -
/dev/md/dsk/d3 /dev/md/rdsk/d3 /usr      ufs      1         no        -
/dev/md/dsk/d5 /dev/md/rdsk/d5 /opt      ufs      2         yes       -
/dev/md/dsk/d6 /dev/md/rdsk/d6 /var      ufs      1         no        -
/dev/md/dsk/d7 /dev/md/rdsk/d7 /home     ufs      2         yes       -
#/dev/dsk/c0t0d0s3 /dev/rdsk/c0t0d0s3 /usr      ufs      1         no        -
#/dev/dsk/c0t0d0s6 /dev/rdsk/c0t0d0s6 /var      ufs      1         no        -
#/dev/dsk/c0t0d0s7 /dev/rdsk/c0t0d0s7 /home     ufs      2         yes       -
#/dev/dsk/c0t0d0s5 /dev/rdsk/c0t0d0s5 /opt      ufs      2         yes       -
swap        -          /tmp tmpfs     -        yes       -
/dev/vx/dsk/rootdg/vol03 /dev/vx/rdsk/rootdg/vol03 /sybase   ufs      3         yes       -
/dev/vx/dsk/rootdg/vol04 /dev/vx/rdsk/rootdg/vol04 /SWsybase ufs      3         yes       -
/dev/vx/dsk/rootdg/vol05 /dev/vx/rdsk/rootdg/vol05 /home/users03 ufs      3         yes       quotas
/dev/vx/dsk/rootdg/vol02 /dev/vx/rdsk/rootdg/vol02 /home/users01 ufs      3         yes       nosuid
/dev/vx/dsk/rootdg/vol06 /dev/vx/rdsk/rootdg/vol06 /home/users02 ufs      3         yes       nosuid
/dev/vx/dsk/rootdg/vol01 /dev/vx/rdsk/rootdg/vol01 /home/logs ufs      3         yes       nosuid,largefiles

```

Figura 3.8 - /etc/vfstab

En /home esta el home de los administradores

En /SWsybase está instalado el Sybase

En /SWsybase se encuentran las bases de datos (.log y .dat)

En /home/logs están las bitácoras del sistema

TESIS CON
FALLA DE ORIGEN

Los File Systems /home/users?? se utilizan para el home de los usuarios, lo cuales contienen su sitio web. Cada FS tiene activado las cuotas.

El File System /home/users03 contiene los primeros usuarios, se ha limitado el espacio a través de cuotas con un máximo de crecimiento del 85% real del espacio total. Así que al menos que se eliminen usuarios, se debe crear en el File System /home/users01.

e) Crones

Usuarios autorizados: adm, lp, root, sys, uucp, avisos y reunion

Los archivos para autorizar están en /etc/cron.d, denominados cron.allow y cron.deny.

- 1) Cron para la realización de los respaldos completos e incrementales, el cual se compone por los siguientes scripts:
 - 1.1) Script para respaldo de las bases de datos (Sybase)
 - 1.2) Script respaldo completo (mensual)
 - 1.3) Script respaldo incremental (semanal)
 - 1.4) Script para la realización de estadísticas de sitios web
 - 1.5) Script depuración de bitácoras de apache
- 2) Script depuración bitácoras de la salida del cron denominado "detocho" y de las base de datos

f) Scripts de Inicio

Los únicos scripts que se han agregado son los siguientes:

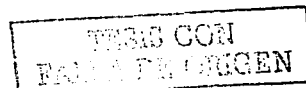
/etc/rc2.d/S88nullmailer	script que inicializa el nullmailer
/etc/rc3.d/S88apache	script que inicializa el servidor de web Apache

TESIS CON
FALLA DE ORIGEN

3.4 Descripción de funcionamiento del sistema

A continuación se dará una visión general de cómo está funcionando el servidor Einstein de acuerdo a las expectativas ya tratadas.

- Se tiene un arreglo de discos con la capacidad suficiente para alojar el sistema operativo, herramientas e información de los sitios; el arreglo de discos cuenta con soporte técnico disponible por parte del proveedor.
- Se actualizó el sistema operativo Solaris, así como las herramientas necesarias para los usuarios y los administradores del sistema.
- Como parte de una característica de la Enterprise 10000 habrá un mayor procesamiento de cálculo, mayor capacidad de memoria RAM (2 GB).
- Se realizó el espejeo de sistema operativo (con DiskSuite) y de sistemas de archivos de los usuarios (con Veritas Volume Manager).
- Se hizo una migración de los sitios, cuidando que los sitios funcionen correctamente y que sean actualizados regularmente por los responsables. Cabe señalar que se posee los contactos de los mismos. Para que en un futuro si llegase haber alguna aclaración sobre la información alojada, se resuelva lo más pronto posible para darles un mejor servicio.
- Como se ha mencionado anteriormente, Einstein no será un servidor de correo, así que sólo podrán enviar correo electrónico y no recibir.
- Antes de que se migrara cada uno de los sitios y bases de datos se elaboraron de forma escrita una serie de políticas para los usuarios, para que fueran autorizadas por el responsable de nuestra área y finalmente se publicaron. Las políticas de los administradores son realizadas por los miembros del Departamento de Administración de Servidores.
- Para realizar correctamente las tareas de administración del servidor Einstein se tiene diversos programas que se ejecutarán de forma periódica. Verificando que se haya llevado a cabo satisfactoriamente, de lo contrario revisar los errores para corregirlos y que no se repitan en un futuro.



- Como otra tarea de administración, que no se estuvo haciendo anteriormente en el servidor Argon, se documenta los cambios significativos, la configuración y procedimientos de las tareas comunes.
- Para la replicación o alta disponibilidad de los sitios se tiene que hacer varios estudios para que se pueda llevar a cabo, ésta será a través del software con Apache.

La realización de este proyecto no se limita únicamente en la implementación de los servicios y en la migración de los sitios web. Por consiguiente hay que mantener funcionando óptimamente el servidor a través una serie de especificaciones de cómo ir cuidando cada aspecto de administración para evitar en un futuro problemas acumulados a través del tiempo.

Se busca mejorar los servicios que se prestan a los usuarios, por ello cada aspecto mencionado en este capítulo y en el siguiente se considera de igual importancia debido que si se descuida cualquiera de ellos puede repercutir en el rendimiento.

Se recomienda tener siempre al alcance todo aquello que pueda describir el funcionamiento del servidor, entonces un aspecto útil sería en medio electrónico y escrito, como sería:

- Elementos de la Descripción de funcionamiento
- Documentación de Hardware (diagramas y especificaciones)
- Documentación de Software
- Documentación de qué hacer cuando exista una falla en la configuración y en los dispositivos.

Los documentos deben estar en un lugar donde los administradores puedan consultarlo, claro está en un lugar seguro y fuera del alcance de aquellas personas que no estén involucradas directamente con la administración del servidor.

El tema de seguridad en cómputo es bastante amplio y es acreedor a un proyecto bien planteado, por consiguiente se utilizará los métodos de seguridad básicos que requiere un sistema. Refiriéndome a método básico a la instalación de herramientas y medidas de seguridad recomendadas por los especialistas en éste ámbito.

TESIS CON
FALLA DE ORIGEN

CAPÍTULO 4**Mantenimiento del sistema**

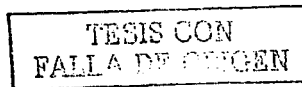
El mantenimiento del sistema una vez terminado la realización de cada una de las etapas de instalación y configuración es de igual forma un aspecto sumamente importante para conservar el buen funcionamiento, es decir continuar con el rendimiento esperado. Con el seguimiento del mantenimiento se pueden minimizar o evitar errores futuros facilitándonos la administración en cada una de las áreas contempladas en cuanto a servidores UNIX y siendo más específica empleando Solaris 8. Entonces, en este capítulo se abarcará los aspectos de administración a nivel técnico, administración del rendimiento, administración de fallas y administración de seguridad. Cada una está relacionada para poder obtener el rendimiento óptimo esperado. Así que hago hincapié que no sólo basta con tener un servidor funcionando sino tomar a conciencia las tareas y responsabilidades como administrador del servidor Einstein tomando en cuenta las diversas áreas.

4.1 Temas selectos de Administración de Solaris 8

La administración de un sistema UNIX consiste en darle mantenimiento al software y al hardware del sistema. Esto incluye la configuración del hardware, instalación del software, reconfiguración del kernel, red y cualquier aspecto que requiera hacer el sistema para trabajar y mantenerse funcionando de una manera satisfactoria. Para hacer estas tareas el administrador del sistema se refiere a un usuario especial, el super usuario o root, tiene privilegios de desempeñar muchas tareas que normalmente no son disponibles para cualquier usuario del sistema.

4.1.1 Bitácoras del sistema y Archivos de Configuración**Bitácoras del sistema**

Solaris como cualquier versión de UNIX contiene una serie de bitácoras donde se registra los cambios importantes durante la ejecución del Sistema Operativo y algunas aplicaciones. Se describirán las más importantes para saber qué registran comúnmente. Cabe señalar que se recomienda revisarlas periódicamente al menos 2 veces por día.



/var/log/syslog: archivo que contiene los mensajes de error o alertas de las opciones configuradas en `/etc/syslog.conf`. Si se tiene instalado Sendmail, aquí manda todos los mensajes sobre este programa.

/var/adm/sulog: archivo donde se registra el cambio entre usuarios a través del comando `su`. Indica el día y si fue satisfactorio o no (un + significa que fue exitoso y un - lo contrario).

/var/adm/messages: archivo donde manda los mensajes del sistema como booteo, falla de algún dispositivo, si un File System está lleno, etc.

/var/log/tcpdlog: archivo de registro de los usuarios que accesan o no al sistema a puertos específicos definidos en el `/etc/inetd.conf`. Este archivo es la bitácora de la herramienta de seguridad TcP-Wrappers.

Archivos de Configuración

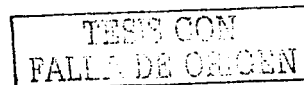
En estos archivos se especifica las características de funcionamiento de algunas herramientas o del tareas en particular para el Sistema Operativo.

/etc/hosts.allow y /etc/hosts.deny: archivos de configuración del TcP-wrappers. En el primero se define que equipos y servicios están disponibles en el servidor.

/etc/passwd, /etc/group y /etc/shadow: archivos de configuración para las cuentas de usuarios. El primero es donde se encuentran todos los logins y detalles de su cuenta, en el segundo están los grupos creados y el tercero contiene las contraseñas encriptadas de los usuarios.

4.1.2 File Systems (Sistema de Archivos)

Definición: Un File System es una colección de archivos y directorios que sirven para almacenar y organizar información. Siendo un conjunto de estructuras y bloques de datos que ocupan espacio definido por una partición²⁹.



²⁹ Sun educational services. "Fundamentals of Solaris 7 and System Admin"

Un File System nos permite manejar la información de forma sencilla, debido a que es jerárquico, es decir, no está en un solo nivel sino en varios, donde todos los directorios están bajo el directorio raíz (/-root).

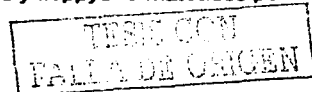
Los File Systems pueden ser creados como una parte de un disco o como un disco independiente. Para el último caso debe hacer referencia al disco; el usuario lo verá como un directorio más, siendo de esta manera para poder acceder a él.

Ventajas de los File Systems

- Protege los accesos a determinados archivos y directorios especificado dueño y/o grupo, es decir para la privacidad entre usuarios.
- Mayor control de espacio asignado para ciertas tareas dentro del sistema.
- Mayor organización referente al tipo de información contenida en el sistema, clasificando por aquella información de los usuarios, sistema operativo, aplicaciones y extras.
- Como es una estructura jerárquica, a nivel de hardware es de gran utilidad para aislar los posibles problemas en algún sector. Si existiese algún daño en una partición, sólo se vería afectado el File System relacionado y no toda la información contenida en el disco, ya que si estuviese en una sección importante de la estructura de árbol se perdería lo contenido en la parte inferior.
- Mayor control en la realización periódica de los respaldos, permitiéndonos respaldar la información crítica únicamente o bien ocupar menor número de cintas (en el caso que se envíen a este medio los respaldos).
- Si se requiere espejear la información contenida en los discos duros, es más sencillo espejear particiones pequeñas que una sola de gran tamaño.

Tipos de File System-Solaris

- ***ufs (UNIX File System)***: es el File System por defecto, el cual está basado en el BSD Fast File System. Optimiza el rendimiento del disco usando grupos de cilindros y bloques de datos continuos.
- ***hfs (High Sierra CD-ROM File System)***: es un File System para CD-ROM de sólo lectura, está basado en la High Sierra y en el ISO (International Standards Organization).
- ***pfs (Personal Computer File System)***: es un File System para computadora personal, el cual soporta lectura y escritura de archivos en discos y floppys formateados por DOS.



- **nfs (Network File System):** es usado para compartir File System en hosts remotos, principalmente en equipos UNIX.
- **File System basados en RAM:** es llamado algunas veces pseudo File System. Se caracteriza por no residir en disco duro, floppy o CD-ROM, reside en memoria física mientras el sistema operativo está corriendo.

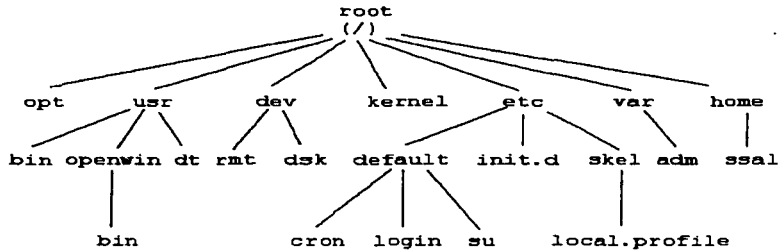


figura 4.2 – Estructura jerárquica de archivos

nota: El término de File System describe una jerarquía de archivos y directorios en una partición. El término estructura de archivo describe un árbol de archivos completo.

La estructura arborescente de File System consiste en el File System root (/) y otros File System montables, los cuales son asociados a un directorio del árbol de File System usando el comando mount. A continuación se describen los directorios más importantes de esta estructura.

File System /usr: contiene los subdirectorios:

bin – para comandos ejecutables y utilerías

lib - para bibliotecas del sistema

File System /home: contiene los directorios de los home de los usuarios, es decir, su directorio de trabajo.

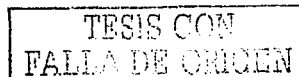
File System /var: contiene las bitácoras del sistema.

File System /opt: contiene algunas aplicaciones extras.

Directorio /dev: contiene los nombres de los dispositivos lógicos para los manejadores de los dispositivos físicos para acceder a los dispositivos de entrada/salida (discos, cintas, teclados, monitores, etc.).

Directorio /etc: contiene archivos de administración del sistema como el passwd o el hosts.

Directorio /kernel: contiene archivos de kernel para la arquitectura de la plataforma local. El kernel esta en el archivo genunix.



File System ufs – Solaris

Un ufs está compuesto por particiones "crudas" y de bloque

Partición cruda: define el comienzo y el tamaño del File System.

/dev/rdisk/c0t0d0s0

Partición de bloque: contiene el File System, donde se colocan los datos.

/dev/dsk/c0t0d0s0

Un UFS en UNIX se divide en las siguientes partes

1. La etiqueta del disco (VTOC): contiene la tabla de partición para el disco, la cual tiene la organización de directorios y archivos, la etiqueta del disco está en el primer sector del disco (512 - byte block).

2. El bloque de boot (bootblock): se encuentra en los siguientes 15 sectores del disco. Como su nombre lo indica está reservado para el programa de arranque boot. Solamente está activo en File System de root aunque el espacio esta reservado para cada File System.

3. Super bloque: está en los siguientes 16 sectores del bootblk, contiene las direcciones del disco, información esencial sobre las características del File System, como:

Tamaño de bloques de datos y fragmentados

Tamaño de la tabla de inodos

Nombre del File System

Nombre del punto de montaje

Fecha de última actualización

Lista de i-nodos libres

Lista de bitmaps libres

Lista de bloques libres

Estado del File System (clean, stable, active)

El super bloque es una área muy delicada porque cualquier cambio en la tabla de i-nodos o área de datos se ve reflejado en este bloque. La utilería fsck revisa las características mencionadas.

4. Super bloque de respaldo: es una replica del super bloque para proteger de una pérdida severa de datos.

5. Tabla de i-nodos: es una serie de bloques que contienen los i-nodos (i-nodes-indexnode). Cada i-nodo está numerado de tal forma que junto con el nombre del dispositivo identifican de forma única la localización de sus bloques de datos (archivos y/o directorios).

6. Área de datos: es aquella donde se guarda el contenido de los archivos y directorios.

TESIS CON
FALLA DE ORIGEN

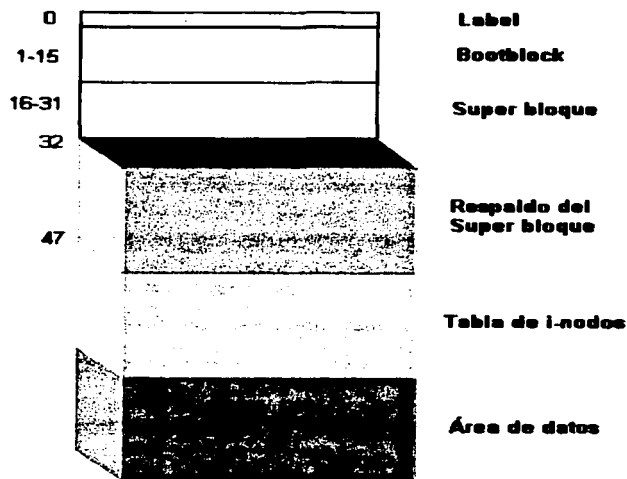


figura4.3 – Estructura de un ufs

Como crear un ufs

```
# newfs /dev/rdisk/c0t2d0s0
```

existen dos herramientas para crear un ufs, el *newfs* y el *mkfs*. La diferencia entre ambos es que el *newfs* es amigable (front end) y manda a llamar al *mkfs*.

Como verificar la integridad de un File System

La utilidad *fsck* (File System check) verifica el estado de cada File System, específicamente el superbloque, es decir revisa el contador de liga de cada i-nodo y que los bloques de datos sean llamados por un solo i-nodo.

La corrupción del superbloque puede ser causado por falta de sincronización (fallo de energía, fallo de hardware, o por no dar de baja bien el equipo).

Cada vez que se levanta el sistema operativo se ejecuta para reparar los File Systems automáticamente. Lo que hace es buscar archivos que no estén listados en un directorio y son

TESIS CON
FALLA DE ORIGEN

colocados en el directorio `/lost+found`. En seguida se mostrará algunos ejemplos más comunes de la utilización de esta herramienta.

```
# fsck /dev/rdisk/c0t2d0s0  Verifica un File System en específico
# fsck                    Verifica los File Systems en el /etc/vfstab
# fsck /opt                Verifica un File System en específico, que está asociado con el
                           punto de montaje /opt del /etc/vfstab
```

Como montar un File System

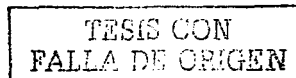
Montar es el proceso de separar los File Systems que son agregados a la jerarquía de los File Systems como punto de montaje, el cual es un directorio.

Montar y desmontar un File Systems ocurre cuando el sistema se inicia y se da de baja, basándose en el `(/etc/vfstab)` Virtual file system table). Toda la información de lo que se monta se guarda en el `(/etc/mnttab)`. En la siguiente lista se muestran algunos ejemplos de los comandos `mount` y `umount`.

```
# mount /dev/dsk/c0t3d0s7 /home  Monta un File System manualmente
# mount /home                    Monta un File System usando los contenidos del
                                 /etc/vfstab
# mountall -l                    Monta todos los File Systems locales
# mountall -r                    Monta todos los File Systems remotos
# umountall -l                   Desmonta todos los File Systems locales
# umountall -r                   Desmonta todos los File Systems remotos
# umount /dev/dsk/c0t3d0s7      Desmonta el File System, usando el dispositivo
# umount/home                    Desmonta el File System, usando el punto de montaje
```

4.1.4 Niveles de inicialización

Los niveles de inicialización representan el modo de funcionamiento del servidor, definiéndose por conjunto de servicios de red y de sistema que están disponibles en un servidor en cualquier instante de tiempo.



Nivel	Comando	Nombre	Función
0	init 0 shutdown ³⁰	OpenBoot PROM	<ul style="list-style-type: none"> - Aparece un promp de ok (OpenBoot PROM) - Servicios del sistema y todos los procesos que están corriendo son detenidos. - Todos los File System son desmontados. - Todos los sistemas Sun tienen un firmware que permite hacer las pruebas e inicializaciones de los elementos básicos de hardware, éstos son el chip boot PROM y la NVRAM (memoria de acceso aleatorio no volátil). - El boot PROM hace la prueba de energía POST(Power On Self Test) identificando procesador(es), memoria, buses; Para formar el árbol de dispositivos y los reconoce a través de los drivers "Device drivers". - La NVRAM tiene una dirección Ethernet permanente, un host ID y el reloj para fecha y hora, además la EEPROM en donde se almacenan los parámetros por default para arrancar el equipo.
1	init 1 init s init S shutdown -i 1	Monousuario (Single User)	<ul style="list-style-type: none"> - Sistema en modo single user. - Conectividad mínima de red. - Inicializa la máscara usando la local del archivo /etc/netmasks. - Obtiene la lista de interfaces de red. - Coloca o intenta colocar el router por default. - Verifica y monta / y /usr. Si esta en File System separado, monta a /var. - Emplea las tablas /etc/vfstab /etc/mnttab y hace ejecuta el comando fsck. - Todos los logins de usuario son deshabilitados y se desmontan todos los File System remotos.
2	init 2	Multiusuario	<ul style="list-style-type: none"> - Todos los File System son montados y todos los servicios de red son configurados exceptuando los File System compartidos (nfs).
3	init 3	Multiusuario completo	<ul style="list-style-type: none"> - Este nivel es que usa por defecto, tiene todos los servicios, todos los File Systems son montados hasta los compartidos.
4		No se usa	
5	init 5 shutdown -i 5 poweroff ³¹	Apagado (power off)	<ul style="list-style-type: none"> - Todos los procesos y servicios de sistema son detenidos y todos los File System son desmontados
6	init 6 reboot shutdown -i 6	Reinicio (Reboot)	<ul style="list-style-type: none"> - Detiene (halt) y reinicia (reboot) el sistema. Todos los servicios y procesos de sistema son detenidos y todos los File System son desmontados

Tabla 4.1 – Niveles de inicialización (Solaris).

³⁰ No recomendado a menos que estén cerradas todas las aplicaciones

³¹ Comando no recomendado

TESIS CON
FALLA DE ORIGEN

4.1.5 Scripts de inicialización

Los archivos de inicialización nos indican cuales son los servicios y acciones que se van a habilitar dependiendo del estado en el que se encuentra el sistema. Van a verificar la integridad de los sistemas de archivos en el sistema, montan los File Systems, despiertan los demonios, entre otras funciones.

/etc/inittab

En este archivo podemos encontrar las acciones o comandos que son habilitados al darse de alta el sistema. Es decir, los procesos y demonios que son creados por el init en cada nivel. Cada acción es definida para que se ejecute por el proceso `/usr/sbin/init`.

/etc/rc#

El comando `init` lee los scripts `rc` (run control) para cada uno de los 7 posibles niveles. Cada uno hace una liga al directorio `/sbin/rcn`³². Estos scripts son: `rcS`, `rc0`, `rc1`, `rc2`, `rc3`, `rc5` y `rc6`

4.1.6 Respaldos

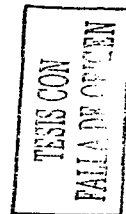
Respaldar es hacer copias de información como una medida de seguridad por si llega a perderse o dañarse el original, por lo regular se realiza en cintas

Razones para respaldar:

- Un usuario o el superusuario borró accidentalmente algunos archivos que son importantes y su pérdida puede traer consecuencias graves.
- Por falla de energía se corrompió un File System y la información se perdió.
- Algún disco falla en alguno de sus componentes.
- El equipo se dañó por algún accidente, por ejemplo un terremoto.

<i>Tipo</i>	<i>Capacidad</i>
Cinta de ½ de pulgada reel-to-reel	120 Mbytes
Cartucho QIC de ½ de pulgada	150 Mbytes a 6 Gbytes
Cartucho Exabyte de 8mm	Más de 40 Gbytes
Cartucho DAT de 4mm	Más de 24 Gbytes (usando compresión)
Cinta Digital Lineal (DLT)	Más de 70 Gbytes (usando compresión)

Tabla 4.2 - Tipos de cintas



³² Cada uno de los `/etc/rc#` leen el directorio `/etc/rc#.d`, donde '#' es el nivel.

Todas las cintas hacen referencia a un dispositivo lógico

`/dev/rmt/n1n`

`n` es el número de cinta

`1` es la densidad (h-high, m-media, l-low, c-compress, u-ultra)

`n` no se regrese cuando termine

Tipos de respaldo

- *Completo (nivel 0)*: respalda el File System completo.
- *Incremental (nivel 1-9)*: respalda archivos que cambiaron con respecto al último respaldo de menor nivel.

Las fechas son guardadas en el archivo `/etc/dumpdates`

4.1.7 Administración de Parches de Sistema Operativo

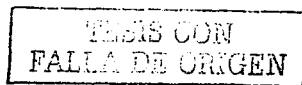
Parche

Una parche es una colección de archivos y directorios que reemplazan o actualizan archivos o directorios existentes para mejorar la ejecución del software.³³

Los parches corrigen bugs³⁴ de la aplicación o agregan mejoras al producto. Cada parche contiene un archivo README para detallar sobre las mejoras a realizar y especifica algunas instrucciones en particular para su instalación.

A los parches se le asigna un número, son puestos en un paquete dentro de un directorio nombrado con el número del paquete.

El lugar donde se pueden obtener los parches en <http://sunsolve.sun.com> o bien a través de un CD-ROM sobre parches. El sitio web se puede obtener el *cluster de parches*³⁵ recomendados o bien se pueden bajar de forma individual, verificando la versión de sistema operativo.



ESTA VEZ NO SALE
EL MANTENIMIENTO

³³ Sun educational services. "Fundamentals of Solaris 7 and System Admin"

³⁴ Término aplicado a los errores descubiertos al ejecutar un programa informático

³⁵ Son un conjunto de parches recomendados por SUN, es decir son las últimas mejoras para diversos archivos, programas más comunes.

Verificar parches instalados

```
# showrev -p                o bien
# patchadd -p
```

Instalación del cluster de parches recomendados

Descomprimir el archivo con el cluster de parches.

```
# unzip 8_Recommended.zip
```

Cambiarse de directorio y si leer la documentación

```
# cd 8_Recommended
# more CLUSTER_README
```

Ejecutar la herramienta

```
# ./install_cluster
```

Instalación de parches individuales

Leer la documentación, para verificar qué es lo que requiere.

```
# more 106760-01/README
```

Agregar parche

```
# patchadd 106760-01
```

La instalación del cluster de parches, o bien de cualquier parche donde tenga que hacerse cambio al kernel o servicio, debe realizarse en el nivel de monousuario, para evitar que se corrompa el binario o archivo de configuración, por eso la importancia de leer la documentación adjunta en los paquetes.

En esta sección se trató los aspectos más importantes de administración de Solaris desde un enfoque técnico, ahora en los siguientes apartados se desarrollará todo lo referente a las especificaciones y cuidados que hay que llevar a cabo durante la administración del equipo para obtener un óptimo funcionamiento, es decir, todos aquellas labores diarias o periódicas para mantener un control de los recursos del servidor.

TESIS CON
FALLA DE ORIGEN

4.2 Área de Administración del Rendimiento

El Área de Administración del Rendimiento nos permite mantener el nivel planeado con respecto al desempeño del servidor para la prevención de problemas futuros. Para ello se ha dividido en dos etapas:

- Monitoreo de los elementos referentes al comportamiento del servidor, los aspectos a observar y recolectar serían:
 - Uso del procesador
Por tipo: espera de entrada y salida (I/O), usuario, sistema (kernel)
Procesos en espera para ser atendidos por el (los) procesador(es)
Procesos totales y procesos del servicio
 - Uso de memoria swap
 - Espacio de disco utilizado por el Sistema de Archivos
 - Conexiones al servidor
 - Disponibilidad del servidor
- Análisis de los aspectos obtenidos en la etapa anterior, esta etapa nos permitirá interpretar el comportamiento del servidor para tomar las medidas pertinentes.

Para poder llevar un histórico del rendimiento del equipo se utilizó nuevamente la herramienta de monitoreo MRTG. Monitoreando los siguientes aspectos:

TESIS CON
FALLA DE ORIGEN

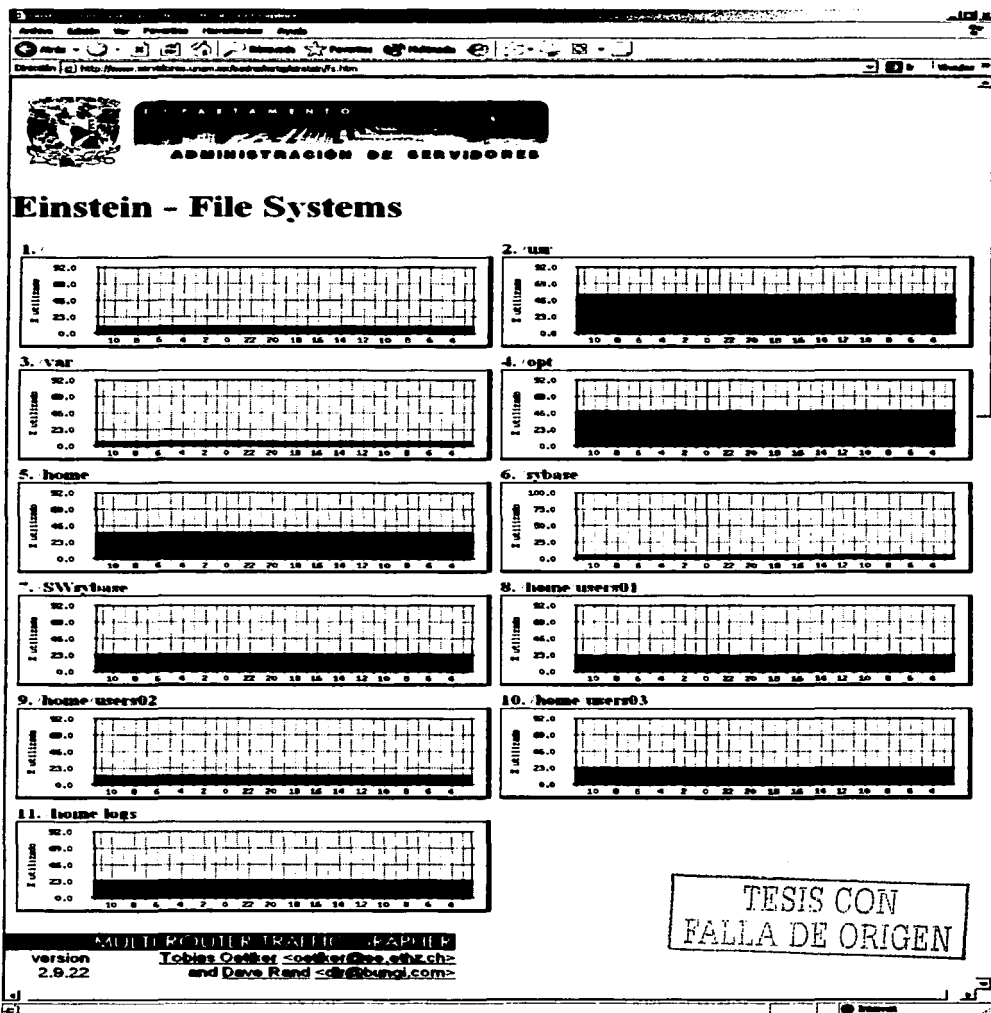


Figura 4.4 – Estadísticas de los File Systems en Einstein

Sistemas de archivos

Los diferentes Sistemas de Archivos en Einstein (figura 4.4) son monitoreados cada uno para verificar que no haya un comportamiento extraño en cuanto al crecimiento. Las gráficas que los representan son:

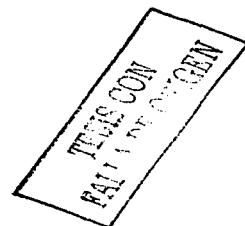
1. /
2. /usr
3. /var
4. /opt
5. /home
6. /sybase
7. /SVsybase
8. /home/users01
9. /home/users02
10. /home/users03
11. /home/logs

En la Tabla 4.3 se hace una comparación de los File Systems de Argon (Figura 2.4) y Einstein (Figura 4.4), como bien se sabe tanto /, /usr y el FS de Sybase (/sybase y /usr/sybase) no deben variar en el tamaño. Aunque para /usr puede hacerse una excepción para la actualización de software.

Para los File Systems de los usuarios se debe de igual forma monitorear que no exceda del 90%.

<i>File System</i>	<i>% de uso Argon</i>	<i>% de uso Einstein</i>
/	20	10
/usr	98	52
/var	65	5
/opt	75 (promedio)	47
/home	90	30
/sybase	98	5
/usr/sybase		

Tabla 4.3 - File Systems Argon - Einstein



Reporte de actividad del Servidor

Las gráficas 1 y 2 (Figura 4.5) nos muestran el porcentaje que el sistema está siendo utilizado por los usuarios, por el sistema, por operaciones de entrada y salida (wio) y la inactividad del servidor (Idle). La suma de las tres primeras no deben dar el 100%.

Las gráficas que representan estos puntos son:

- *Idle y Wio en el Sistema* En donde la parte sombreada se refiere al Wio y la línea azul representa el Idle.
- *CPU Utilizado por: Usuario y Sistema* En donde la parte sombreada se refiere al porcentaje de CPU utilizado por el usuario y la línea azul representa el CPU utilizado por el kernel.

Al comparar Figura 2.5 y Figura 4.5, para el caso de Argon se hace uso de procesador por operaciones de I/O y existe mayor inactividad (Idle), pero en Einstein se tiene alrededor del 99% y es constante. Ésto es normal porque Einstein tiene mejor capacidad de procesamiento, 4 procesadores a 400 MHz contra 8 procesadores a 50 MHz.

Memoria Swap

La parte sombreada corresponde a la memoria usada y la línea azul a la disponible. Para saber ésto se usa el comando *swap -s*. Figura 4.5, gráfica 3.

Para ambas gráficas (Figura 2.5 y 4.5) se tiene un comportamiento similar, sólo que en Einstein es más estable por no tener muchas variaciones.

Procesos

Como es un servidor de Web principalmente se toma en cuenta los demonios de Apache que estén corriendo. Figura 4.5, gráfica4.

En la gráfica de "4. Procesos Totales vs. Procesos de Apache" (figura 4.5), la parte sombreada corresponde a los procesos totales la línea azul es el número de demonios de Apache.

En la gráfica de "5. Procesos Totales vs. Otros Procesos" (figura 4.5), la parte sombreada son los procesos totales y la línea azul corresponde a otros procesos que no sean apache (Apache) y de root.

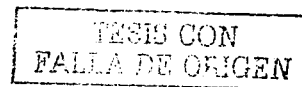
TESIS CON
FALLA DE ORIGEN

Para ambas gráficas (Figura 2.5 y 4.5) el comportamiento es similar, sólo que en Einstein es más estable por no tener muchas variaciones. Los picos que se llegan a presentar si se verifica la hora es cuando son más visitadas los sitios Web. Para la parte de otros procesos en Einstein se observa una línea casi recta esto probablemente porque no se cuenta con procesos como el Sendmail.

Conexiones

En esta gráfica se visualiza el número de conexiones actuales que se hacen al servidor por los diferentes puertos abiertos (la parte sombreada) y las conexiones de los usuarios a través de una terminal dada (línea azul). Figura 4.5

Procesos Encolados



Este aspecto se refiere al número de procesos que están esperando ser atendidos por los procesadores, estos datos son tomados cada 5 y 15 minutos de la salida del comando "uptime". Figura 4.5, gráfica 7.

Esta sección es muy importante para una administrador, ya que comúnmente se llama la carga del sistema. En teoría no debe de haber un número promedio mayor al total de los procesos disponibles en el servidor. Es decir, para Argon no debe ser mayor a 8 y para Einstein no mayor a 4.

En Argon (Figura 2.5) se observa varios picos pero no se excede en el número acordado, tiene de 17% a 68%, es decir 1.7 a 6.8

En Einstein (figura 4.5) casi no hay carga, ya que tiene un uso de 2% a 4%, es decir .02 a .04 Debo aclarar que MRTG no grafica números decimales así que el valor obtenido los multiplique por 10 o por 100. Para Argon fue por 10 y para Einstein por 100.

Si comparamos los resultados obtenidos del servidor Argon y de Einstein claramente se puede verificar el cambio en cuanto el rendimiento.

- El tamaño de los diferentes File Systems es bastante bajo, entonces lo que debe cuidarse es que no aumenten excesivamente y si aumenta debe verificarse el por qué.
- El porcentaje de procesador (CPU), operaciones de entrada/salida y de usuario son bajos, se puede verificar debido a que el idle es casi un 99%, lo cual es óptimo para un servidor.

- El uso de memoria swap es poco por lo mismo que no se tiene muchos procesos en el sistema. El número de procesos totales en promedio es de 150, realmente son pocos y por consiguiente no existen muchos encolados para ser atendidos por cualquiera de los cuatro procesadores.

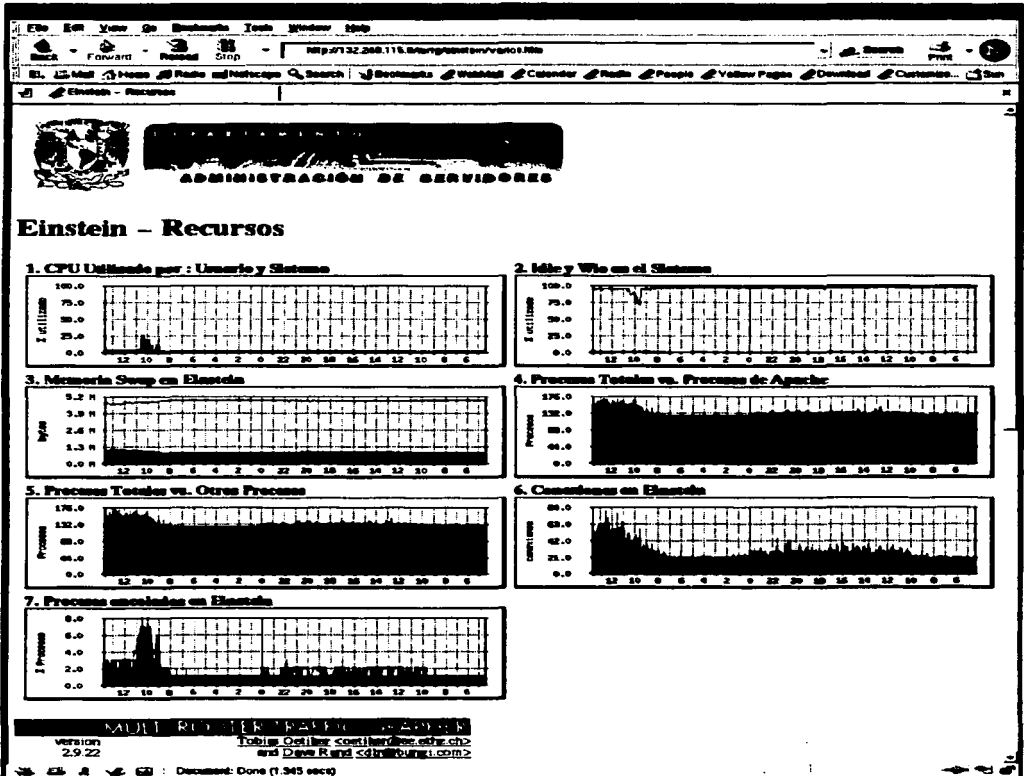


Figura 4.5 – Estadísticas de los recursos en Einstein

TESIS CON FALLA DE ORIGEN

4.3 Área de Administración de Fallas

El Área de Administración de Fallas tiene como objetivo principal reducir el impacto de una falla en los servicios, permitiéndonos mantener su confiabilidad.

Etapas:

1. Detectar los problemas a través de herramientas de monitoreo, como el MRTG o el RDTOOL, así como el top y a través de revisión de bitácoras o bien por medio de una notificación del usuario. Cada problema se clasifica de acuerdo a:

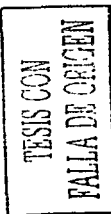
Severidad de la alarma

- Crítico. Cambio brusco en el curso de la realización de una tarea o función programada dentro del sistema por lo que no puede continuar su realización y puede llegar a traer consecuencias importantes en la prestación del servicio(s). Requiere de atención inmediata.
- Mayor. Cuando un servicio, tarea o dispositivo ha sido afectado y requiere inmediato restablecimiento. No es tan severo como el crítico, ya que el servicio se sigue ofreciendo aunque su calidad no sea la óptima.
- Menor. Indica la existencia de una condición que no afecta el servicio pero que debe tomarse las acciones pertinentes para prevenir una situación mayor.
- Indefinida. Cuando el nivel de severidad no ha sido determinado por alguna razón.

Tipo de alarma - Subsistema (hardware o rendimiento)

- Plataforma: referente al Sistema operativo, Hardware o bien elementos importantes para el rendimiento óptimo.
 - Herramientas y aplicaciones: aquellas que son trascendentales para brindar algún servicio, apache, Sybase, PHP, principalmente
2. Hacer pruebas de diagnóstico para determinar el origen. Se puede auxiliar de herramientas de monitoreo o bien a través de las bitácoras y comandos básicos y de administración.
 3. Corregir la falla lo mejor posible. Debe de considerarse brindar de forma inmediata el servicio, si se ve interrumpido.
 4. Registrar y dar seguimiento a los reportes generados por el usuario o administrador, los cuales nos ayudarán a conocer el estado actual de la falla. Además, facilitará la realización o mejora del procedimiento correspondiente.

Las diversas alarmas que pueden presentarse en el servidor Einstein se describen en la tabla 4.4:



PROBLEMA	ALARMA	DESCRIPCIÓN	NIVEL CRÍTICO	SUBSISTEMA
Sitio no visible	HTTP down	Demonio de Apache detenido	2	Apache
Sitio inseguro	Demonio del Apache (httpd) sin la opción -DSSL	Demonio de Apache activo sin opción de SSL	3	Apache
Sitio no visible	Forbidden You don't have permission to access on this server.	Falta de página índice en \$HOME/htdocs	4	Apache
Falta restricción en directorio del sitio	Acceso directorio URL sitio sin restricción de usuario y contraseña	Ausencia o error en configuración del archivo .htaccess o en httpd.conf	4	Apache
Conexión a base de datos fallida	Dataserver is not running	Manejador de base de dato Sybase abajo	2	Sybase
Conexión a base de datos fallida	There are not enough 'user connections' available to start a new process.	Se terminaron las conexiones permitidas	3	Sybase
No permite hacer cambio en la base de datos	Log transaction full	Archivo de transacciones lleno (.log)	3	Sybase
No respaldo base de datos	Backupserver is not running	El sybackup está abajo	4	Sybase
No reconoce base de datos	Don't find log\data device	Falta dispositivos físicos o lógicos (.log o .dat)	2	Sybase
PHP no funciona	Vista código fuente de PHP, no interpreta	Configuración del PHP no es correcta o extensiones asignadas inválidas	2	PHP
Saturación de File System	unix: NOTICE: reallocg: file system full	Exceso de archivos ".tar", ".zip", ".gz" o exceso de operaciones temporales de lectura y escritura. Aplicable a todos los File systems exceptuando /, /usr, /var; estos son para otro caso	3	Plataforma
No acceso via red	qfe0:cable problem	Falla en la configuración de red o en algún dispositivo	1	Plataforma
El rendimiento del equipo se ve degradado	unix: NOTICE: reallocg: file system full (/, /var, /usr)	File System(s) críticos lleno(s) /, /var o /usr. Causa inestabilidad al sistema	2	Plataforma
Memoria	unix: WARNING: [AFT1] Uncorrectable Memory Error on CPU5 Data access at TL=0, errID 0x000a8440.1a883633	Falla de un módulo de memoria	2	Plataforma
Permisos	Permission denied passwd(SYSTEM): They don't match.	Error al cambiar el password, requiere ser root o no se tecleo bien la contraseña	4	Plataforma
Permisos	su: 'su <usuarios>' failed for <user> on /dev/pts/n	Error al cambiar de usuario	4	Plataforma

TESIS CON
 FALLA DE ORIGEN

Disco interno	Scsi: [ID 102784 kern.warning] WARNING: /sbus@4c.0/QLGC.jsp@0.1000 0/st@5.0 (st26): error for command write Error level: Fatal	Falla en un disco	1	Plataforma
Disco interno	Scsi: [ID 102784 kern.warning] WARNING: /sbus@4c.0/QLGC.jsp@0.1000 0/st@5.0 (st26): error for command read Error level: Fatal	Error en la lectura del disco	1	Plataforma
Disco externo	Socal: [ID 348264 kern.warning] ID[SUNWvssa.socal@1,0/sf@0, 0/ssd@w2100002037c3e3d2,0 (ssd76): error for command read	Falla en un disco	1	Plataforma
Disco externo	vxio: [ID 834083 kern.notice] NOTICE: vxvmvxio: read error on object Afb-01 of mirror redo 01 in volume redo (start 0 length 34562048) corrected	Error en la lectura del disco	1	Plataforma
Disco externo	Socal: [ID 403145 kern.info] ID[SUNWvssa.socal.link.5010] socal2: port 0: Fibre Channel is OFFLINE	Error en el enlace de fibra óptica	1	Plataforma
Boot	syslogd: going down on signal 15 unix: syncing file systems... unix: done	Reinicio del equipo	2	Plataforma
Consoles	FanFailure: Fan 1 from tray slot 6 has FAILED	Falla de ventilador	2	Plataforma
Consoles	PowerOffact: Detected System board 15 has been powered OFF	Apagado de System Board	1	Plataforma
Consoles	PowerOffact: Detected System board 15 has been powered ON	Encendido de System Board	1	Plataforma
Consoles	Netcon_server: (einstein): INIT: New run level:0 Netcon_server: (einstein) The system is coming down. Please wait	Baja de dominio nivel 0	1	Plataforma

TESIS CON
 FALLA DE ORIGEN

Consoles	Netcon_server: (einstein) panic failed to stop cpu4 Netcon_server: (einstein): panic(cpu4)/thread=406fbc65: Kernel panic at trap level 2	Caída del sistema (panic)	1	Plataforma
Consoles	Postdump-(einstein): hpost -e -d "Edd-Record-Stop-Dump"-D3ff00,/var/opt/SUNWssp/adm/einstein/Edd-Record-Stop-Dump-10.24.03:33 for domain einstein and boards 3, being written to /var/opt/SUNWssp/adm/einstein/Edd-Record-Stop-Dump-10.24.03:33	Record stop en einstein	1	Plataforma
Servicio de acceso denegado	ssh ftp telnet: Unable to connect to remote host: Connection refused	Usuario no puede hacer conexión a través de ssh, FTP o telnet	4	Plataforma
Denegación de acceso	ssh ftp telnet: refused connect from <dirIP>	Dirección IP no autorizada para acceder al servidor	4	Plataforma
No levanta demonio de Apache	Apachectl start: httpd could not be started	Verificar definición de la variable \$LD_LIBRARY_PATH	2	Plataforma
/tmp lleno	unix: NOTICE: reallocg: file system /tmp full	Muchos procesos, posible baja del sistema "calda"	1	Plataforma
Promedio de procesos elevada	load average: 10.50, 10.20, 10.05	Número de procesos enclavados para ser atendido por uno de los procesadores elevada (4 a 8)	3	Plataforma
No funciona crones	crontab: you are not authorized to use cron. Sorry.	Usuario no autorizado para ejecutar crones	4	Plataforma
No funciona crones	cron may not be running - call your system administrator	Demonio de crond no activo	3	Plataforma
Falla respaldo incremental o completo del sistema	/dev/rmt/0n: No such file or directory /dev/rmt/1n: No such file or directory /dev/rmt/0n: no tape loaded or drive offline	Dispositivo incorrecto	4	Plataforma
Falla respaldo incremental o completo del sistema	no answer from maquina.servidores.unam.mx	Servidor de respaldo "abajo"	2	Plataforma
Falla respaldo incremental o completo del sistema	no answer from maquina.servidores.unam.mx	Falla conexión en la red	1	Plataforma

TEMS CON FALLA DE ORIGEN

Falla respaldo incremental o completo del sistema	/dev/rmt/0n: no tape loaded or drive offline	Cinta fuera de línea	3	Plataforma
Usuario no puede agregar o quitar archivos en su home	unix: NOTICE: quota_ufs: over hard disk limit (pid 5014, uid 11440, inum 664400, File System /home/users01	Usuario a excedido cuota asignada	4	Plataforma

Tabla 4.4 – Alarmas principales en el sistema

TESIS CON
FALLA DE ORIGEN

4.4 Área de Administración de la Seguridad

La seguridad en cómputo respecto a un sistema es cuando se puede confiar en que se comportará como se espera que lo haga. Para ello debe saberse qué se le permitirá acceso y cuáles son los aspectos más importantes a cuidar de acuerdo a nuestras necesidades, asignando una prioridad³⁶; como pueden ser:

Confidencialidad, proteger la información por personas autorizadas de no poder leerla o copiarla, es decir mantenerla en secreto.

Integridad de los datos, no exista modificación o eliminación alguna de la información por ningún factor como un error de software, hardware, humano o por alguien mal intencionado sin autorización.

Autenticación, consiste en comprobar una identificación, ésto se hace a través de la asignación de una contraseña para comprobar que es quien dice ser.

Disponibilidad, acceder en el momento y con la velocidad requeridas a la información requerida.

Control, regular quién tiene acceso al sistema, es decir que no entren personas no autorizadas como los *crackers*.

Auditoría, mantener registros que ayuden a averiguar quién hizo qué.

Referente a la seguridad de UNIX, puede decirse que es lo suficientemente seguro por su diseño, aunque la mayor problemática se debe a una mala configuración o un mal uso del sistema, así como la mayor parte de las utilerías extras que se emplean (como puede ser sendmail).

En esta sección se tratará todo lo referente a qué medidas tomar para evitar violaciones de seguridad, así como las acciones a tomar si llegase a ocurrir.

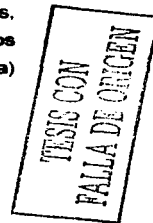
1. Análisis de riesgos

Prevención de ataques, cuidando los aspectos de seguridad física del equipo, seguridad de acceso, y seguridad lógica para ello debe existir políticas de administración y manejo de cuentas, por ejemplo. Identificando recursos (equipo, privacidad de los usuarios, contraseñas de los usuarios, imagen pública, etc.), amenazas (ambientales, estructura del edificio, acceso al sistema) y cálculo de riesgos.

Detección de intrusos. Puede ser a través de varias maneras:

- Descubriendo al intruso en el acto.

³⁶ La descripción de los diferentes aspectos de seguridad a cuidar se tratarán de mayor a menor prioridad de acuerdo a este proyecto.



- Deduciendo que alguien ha irrumpido en el sistema a través de cambios producidos en él, como incremento en la carga del sistema, reducción en el espacio en disco, modificación o eliminación de bitácoras, modificación en los binarios, etc.
- Recibiendo un mensaje del administrador de otro sistema indicando actividad extraña recibida desde nuestro sitio de trabajo.
- Actividades extrañas en el sistema, como caídas del sistema, gran actividad de disco, desaparición o incremento de las cuentas del sistema, o algún programa que revele información sensible sobre los usuarios del sistema, como la ejecución de "crack".

Procedimientos para respuesta a incidentes

Las medidas a tomar en el manejo de incidentes, se basa en tres aspectos principales.

- Mantener la calma y concentrarse para actuar de lo mejor posible. Para ello, primero hay que estar seguro de que haya sido un incidente, ya que puede ser un error humano o una falla de un programa. Si existió, entonces hay que verificar si realmente hubo un daño en el sistema, es decir, el intruso haya cambiado información privilegiada.
- Si se encontró evidencia de la violación en la seguridad, debe considerarse si es importante obtener y proteger la evidencia por si puede utilizarse en investigaciones futuras. También debe considerarse si el sistema continuará operando normalmente lo antes posible.
- Documentar toda la investigación del incidente, indicando fecha y hora, así como descripción del incidente. Puede emplearse el comando "script" para guardar todo lo que se investiga en un archivo mandando la salida de lo que se escribe y se muestra en la terminal.
- Hacerse la pregunta de ¿Puede suceder otra vez?. Se debe de tener tareas planeada si existe una violación y hacer simulacros de intrusión.

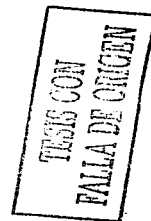
Paso 1: Identificar y entender el problema.

Paso 2: Contener o detener el problema.

Paso 3: Confirmar el diagnóstico y determine el daño.

Paso 4: Restaurar el sistema a través de respaldos en cinta o bien al reiniciar el sistema

Paso 5: Atacar el problema. Se refiere a detectar alguna debilidad de seguridad o de la operación del sistema y hacer los cambios de forma adecuada y repararlos lo antes posible de que el sistema opere de forma normal.



2. Seguimiento de políticas de seguridad

Las políticas de definen como un *conjunto de reglas y prácticas que regulan la manera como se maneja, protege y distribuye información sensible a través de la organización*. Para la elaboración de las políticas de seguridad se debe contemplar dos aspectos:

sujeto es algo activo en el sistema; usuarios, procesos y programas.

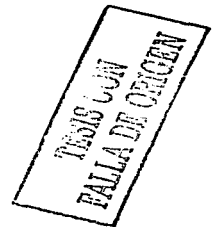
objeto es algo que está sujeto a la acción de un objeto; archivos, directorios, dispositivos, etc.

Una política de seguridad detalla las actividades que están o no permitidas, los pasos a seguir para obtener la protección adecuada así como los pasos a seguir en caso de presentarse un incidente de seguridad. Además, establece responsabilidades y derechos y explica las sanciones que se impondrán a los que falten a una regla. Siendo muy importante que cada usuario del sistema esté enterado de dicha política, para ello se debe entregarles una copia de las mismas al recibir su cuenta en el sistema, debe asegurarse que la lea y entienda, firmar el documento y guardar una copia. Y si es posible o factible publicarla.

Las políticas para los administradores y los usuarios se pueden encontrar en el Apéndice B, las cuales fueron realizadas en conjunto por los miembros del Departamento de Administración de Servidores.

3. Empleo de herramientas de seguridad

Existe una gran variedad de comandos que se pueden usar para descubrir a un usuario, además de excelentes paquetes de seguridad como Tiger, Tripwire o Cops que se deben monitorear periódicamente.



CONCLUSIONES

CONCLUSIONES

El estudio preliminar de la presente tesis fue un proyecto requerido y sugerido por el Departamento de Administración de Servidores en la DGSCA por lo cual estoy convencida de lo que realicé cumple con las expectativas y requerimientos originalmente planteados de acuerdo a los recursos disponibles y buscando siempre brindar un mejor servicio a los usuarios. La verificación del correcto funcionamiento de este proyecto fue llevada a cabo por el actual Jefe de departamento de Administración de servidores y por los usuarios existentes en Einstein quienes colaboraron en el término del proyecto.

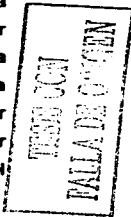
Como primera acción se realizó la migración inmediata de Hardware a una plataforma más reciente y con soporte técnico por si llega haber alguna falla en los componentes

Con el dominio de la Enterprise 10000 se obtuvo principalmente un mayor rendimiento (performance) y además mayor capacidad de almacenamiento. El rendimiento es comprobable debido a que se cuenta con mayor memoria RAM y procesamiento; estos aspectos se pueden ver claramente en las gráficas obtenidas con la herramienta de monitoreo MRTG.

Se tiene un menor número de procesos por la inexistencia de Sendmail y por mayor velocidad de procesamiento en el dominio. En Einstein existe regularmente entre 0.2 a 0.5 número de procesos que esperan ser atendidos por cualquiera de los 4 procesadores, en cambio en Argon era de 4 a 8 procesos. Realmente es un cambio significativo.

Existe mayor capacidad de almacenamiento en disco duro de 49 GB que tenía Argon a 162 GB disponibles en Einstein, suficiente para Sistema Operativo, aplicaciones, herramientas y datos de los usuarios. Cabe aclarar que no se utiliza todo el espacio disponible, ya que cuenta con discos espejo tanto para sistema operativo como para datos de los usuarios y discos spare.

Para controlar el espacio en disco se emplea cuotas por File System a través de una política para la asignación de cuota a todo usuario común en el sistema. Con esta medida el administrador puede controlar el espacio utilizado por los usuarios, es decir si un usuario no tiene cuota tiene la posibilidad de ocupar más espacio y cuando otro usuario intente escribir algo quizá no pueda porque ya no haya espacio donde escribir. Con esta medida el usuario administrará de la mejor manera su espacio y si requiere de más tendrá que notificar a través de una justificación por escrito. Ahora se tiene a todos los usuarios controlados por File System y se tiene contabilizado el espacio asignado sin sobrepasar el límite real.



CONCLUSIONES

Para el control de los discos duros se empleó en Einstein dos herramientas DiskSuite y Veritas Volume Manager. En Einstein se espejeó el Sistema Operativo y los datos de los usuarios. Para el Sistema Operativo se empleó DiskSuite y para los datos una herramienta muy robusta Veritas Volume Manager. El motivo por el cual no todos los servidores emplean Veritas Volume Manager es por el costo, ya que se necesita pagar una licencia; aunque para Einstein la licencia estaba incluida con la compra de un arreglo de discos A5200.

Con el espejeo de discos se podrá realizar más de dos respaldos idénticos del equipo, utilizando el disco espejo; el beneficio de tener más de un respaldo es tener una de las cintas en un lugar seguro y confiable por si la cinta que está al alcance sufre un daño o pérdida.

Se actualizaron satisfactoriamente el Sistema Operativo, algunas herramientas y aplicaciones para que fueran empleadas por los usuarios, eliminando vulnerabilidades publicadas por organismos especializados como CERT.

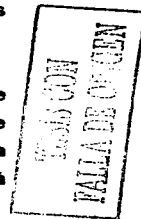
Se realizó la depuración de sitios no vigentes. Se había hecho la propuesta de migrar los sitios estáticos o un servidor de sitios históricos, pero de todos los que se pidió baja definitiva no se solicitó esta opción. Aunque si solicitaron un respaldo en cdrom.

Uno de los servicios que causaba conflictos en el rendimiento y almacenamiento era el correo, el cual sufrió unas modificaciones, los usuarios solo pueden enviar correo electrónico y no recibir, con esta medida se evita el problema de spam.

Se crearon y se publicaron políticas para los usuarios y administradores con el objetivo de controlar las tareas comunes para ambos. La clasificación de las políticas se realizó en base a las diferentes áreas, que fueran de contenido claro y descriptivo con el fin de no tener confusiones.

Se automatizaron las tareas comunes de administración, las cuales son respaldos periódicos, registro de estadísticas vía web, monitoreo de los recursos del servidor y depuración de bitácoras de log.

Se contempló la replica de sitios web en otro servidor por hardware o por software. Ambos no se realizaron, ya que implica hacer un estudio detallado de cómo realizarse o bien un costo extra que no disponía la Dirección de Telecomunicaciones. Con respecto al empleo de Apache para la alta disponibilidad de sitios web, puede considerarse como un proyecto bastante útil, que se realizará en un futuro en los servidores de Web.



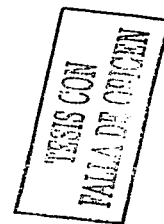
CONCLUSIONES

En el servidor Einstein se tomaron varias medidas de seguridad a un nivel intermedio. Se consideró la seguridad física, debido a que se encuentra en un site con las características de temperatura y control de acceso adecuado. Pero factores del medio ambiente como el polvo no se puede evitar debido a que está cerca de un puerta que permite el flujo de las corrientes de viento. La seguridad a nivel de software abarca la parte de políticas, procedimientos y herramientas de seguridad. Faltó instalar y configurar herramientas de seguridad críticas como Tripwire, Saint y Cops.

Se realizó una relación de los responsables de los sitios, donde contactarlos vía telefónica y correo electrónico. Además, se encuentra en desarrollo un sistema para guardar los contactos en una Base de Datos realizado por un miembro del Departamento.

La migración del servidor Einstein se hizo tomando diversos aspectos de forma cautelosa para culminar con éxito la depuración y con entero conocimiento de lo que tiene ahora el nuevo servidor Einstein, dejando claro en la documentación la descripción detallada sobre el estado actual y modificaciones en la configuración. Como administrador de Einstein puedo decir que conozco el servidor y en el caso que existiese alguna falla será con mayor rapidez la solución de la misma y principalmente cualquier otro administrador del departamento puede dar solución óptima al problema con ayuda de la documentación existente.

Finalmente, la metodología de migración no es para un caso en particular, puede aplicarse a servidores con necesidades similares. El punto clave es conocer el funcionamiento y los recursos de un servidor a través de documentación compuesta de diagramas, tablas, procedimientos, políticas, respuesta a alarmas, monitoreo y principalmente hacer las tareas en el momento que debe ser y de la mejor manera. El tener control y conocimiento de los recursos facilitará innovaciones en los servicios para permitimos alcanzar el punto máximo de administración el "Tuning".



APÉNDICE A**Software Instalado**

En este apéndice se describirá el diferente software instalado tanto en el servidor Argon y Einstein, sólo que para aquél software instalado en Einstein se describirá la bitácora de instalación. Algunas de las herramientas instaladas son comunes para ambos, las primeras que se describen son aquellas que no se instalaron en Einstein, la segunda sección es aquel software instalado en Einstein aunque de una forma general por si se requiere actualizar las versiones de las herramientas instaladas. Debe recordarse que para actualizar una herramienta primeramente se debe investigar cuánto cambia la nueva versión y hacer pruebas en otro servidor. Para facilitar la búsqueda del software se organizó de forma alfabética.

a) Software no instalado en Einstein, pero sí en Argon.**DB-BERKELEY**

Conjunto de bibliotecas que permiten la configuración y soporte para las aplicaciones que necesiten ser rápidas, de misión crítica y redituables. Es muy utilizada para la configuración e instalación de sendmail. El software se puede obtener del sitio oficial <http://www.sleepycat.com>

FRONT PAGE

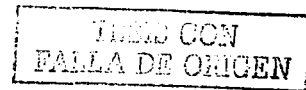
Frontpage es un software para la edición de sitios web que utiliza extensiones y herramientas para realizar ciertas tareas. Estas herramientas facilitan la creación de sitios web tanto para desarrolladores profesionales o no.

Las extensiones de FrontPage son un conjunto de archivos y programas CGI que se instalan para facilitar el uso de las características y complementos que este editor de páginas web ofrece.

GROFF

Groff (GNU Troff), es un procesador de texto que lee un texto plano con comandos de formato para dar una salida. Este software es muy útil para aplicaciones como sendmail.

El software se puede obtener del sitio oficial <http://www.gnu.org>, la UNAM cuenta ya con un site mirror de este sitio en <http://gnu.unam.mx>



IMAP / POP

(Internet Message Access Protocol) Protocolo de Internet para el acceso de mensajes, es un método para acceder al correo electrónico por medio de un cliente de correo, tal como Outlook, Eudora. POP (Post Office Protocol), protocolo de cliente servidor que sirve para manejar buzones electrónicos de usuarios. El software se puede obtener en: <ftp://ftp.cac.washington.edu/imap>.

BIBLIOTECAS PARA C++ (libstdc++)

Las bibliotecas libstdc++ son necesarias para poder utilizar algunas de las funciones que tiene el compilador GCC. Estas bibliotecas están disponibles en: <http://gcc.gnu.org/libstdc++>.

MAJORDOMO

Majordomo es un programa que automatiza la administración de listas de correo en Internet. Los comandos son enviados por e-mail para manipular y administrar todos los aspectos del programa, es decir no se requiere una sesión del postmaster para la administración del mismo.

Majordomo esta escrito en Perl. Trabaja con Perl 4.036 o 5.002 o superior, pero no trabaja con Perl 5.001. esto es un problema de Perl y no de Majordomo, para mayor información <http://www.perl.com/perl>.

La versión actual de Majordomo se puede obtener la distribución en el sitio <ftp://ftp.greatcircle.com/pub/majormo> o en <http://www.greatcircle.com/majordomo>.

Majordomo fue desarrollado principalmente para sistemas basados en UNIX, pero probablemente también trabaje en otros, si se consigue una versión de Perl que pueda compilar limpiamente en su sistema no UNIX y si utiliza un programa externo como Sendmail para enviar e-mail.

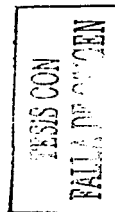
PINE

El nombre PINE es el acrónimo de Program for Internet News & Email, se trata de una aplicación desarrollada por la Universidad de Washington para el tratamiento y manejo de mensajes electrónicos el mismo se propone como alternativa al ELM (Electronic Mailer) pues su otro acrónimo es Pine Is Not Elm.

SENDMAIL

Sendmail es un Agente de Transporte de Mensajes, que se encarga de rutear y administrar los mensajes electrónicos (e-mail) de los usuarios.

El software se puede encontrar en el sitio oficial: <http://www.sendmail.org>.



b) Software instalado en Einstein.**APACHE**

Servidor web que permite el hospedaje de páginas web en una máquina específica. Esta herramienta tiene varias funciones tales como: permitir a los usuarios tener sus propias páginas web, restricción a determinados sitios web, conexiones seguras a través de ssl y configuración de módulos de programación.

El software se puede obtener del sitio oficial <http://www.apache.org>, la UNAM cuenta ya con un site mirror de este sitio en <http://apache.unam.mx>.

Requerimientos

- Aproximadamente 12 MB durante la instalación y 3MB para la instalación.
- Compilador ANSI-C, es recomendable GCC se obtiene de <http://www.gnu.org/>
- Modulo de criptografía para Apache a través de SSL y TLS, modssl, obtenerlo en <http://www.modssl.org>
- OSSP mm, la cual es una biblioteca para simplificar el uso de la memoria compartida entre los procesos creados. Se puede obtener en <http://www.oss.org/pkg/lib/mm/>
- Open-ssl. Obtenerlo de <http://www.openssl.org/>.

Instalación con ssl

1.- Descomprimir y desempaquetar el software.

```
$ gzip -d < apache-version.tar.gz | tar xvf -
$ gzip -d < mod_ssl--version.tar.gz | tar xvf -
$ gzip -d < mm-version.tar.gz | tar xvf -
```

2.- Cambiar al directorio.

```
$ cd mod_ssl-version
```

3.- Configuración del sistema; ejecutar el archivo configure.

```
$ ../configure \
--with-apache=../apache_version \
--with-ssl=/usr/local/ssl \
--with-mm=../mm-version \
--prefix=/usr/local/apache \
--enable-rule=EAPI \
--enable-shared=max
```



4.- Cambiarse de directorio del fuente de apache.

```
$ cd ../apache-version
```

5.- Realizar la compilación y creación de archivos de instalación.

```
$ make
```

6.- Instalar los archivos

```
$ su -
# cd ~/usuario/apache-version
# make certificate
# make install
```

7.- Editar los archivos de configuración de Apache, en este caso es la estructura de Red-Hat.

```
# vi /usr/local/apache/conf/httpd.conf
```

En este archivo en la línea de **ServerName** debe cambiarla al nombre de la máquina.

```
ServerName einstein.servidores.unam.mx
```

Para más información sobre apache <http://www.apache.org/docs/>

Iniciar el servicio

Para verificar que se instaló correctamente debemos de inicializar el demonio httpd

```
# /usr/local/apache/bin/apachectl startssl
```

Iniciar un navegador web y poner el nombre de máquina, o la dirección IP.

Para dar de baja el demonio:

```
# /usr/local/apache/bin/apachectl stop
```

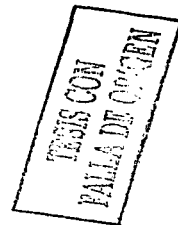
DISKSUITE

Solstice DiskSuite es una solución de gestión de almacenamiento y disco, como componente del entorno operativo Solaris, el software Solstice DiskSuite satisface la necesidad de alta disponibilidad de los datos, rendimiento mejorado de E/S del sistema y administración simplificada de grandes sistemas con varios dispositivos de almacenamiento.

Instalación:

1. Introducir el cdrom "Solaris Software", disco 2 y cambiarse al directorio donde se encuentran los paquetes.

```
# cd /cdrom/sol_8_401_sparc_2/Solaris_8/EA/products/Disksuite_4.2.1/sparc/Packages
```



2. Instalar los paquetes con la siguiente instrucción.

```
# pkgadd -d .
```

NOTA: el orden de instalación de los paquetes es 10, 9, 8, 4, 6, 7. También se instaló el parche 108693.

3. Sacar el cdrom y reiniciar el equipo.

```
# eject cdrom
# shutdown -y -i6 -g0
```

GCC

GCC (GNU C Compiler) compilador de lenguaje C desarrollado como parte del proyecto GNU, este compilador tiene la capacidad de compilar programas fuentes realizados en C, C++, Java, Fortran; con las bibliotecas correspondientes. El software se puede obtener del sitio oficial <http://www.gnu.org>, la UNAM cuenta ya con un site mirror de este sitio en <http://gnu.unam.mx>.

Requerimientos

- Aproximadamente 15 MB durante la instalación, y 3 MB para la instalación.
- Make de GNU, obtenerlo de <http://www.gnu.org>.

Instalación

1.- Convertirse en superusuario.

```
$ su - root
```

2.Descomprimir el paquete.

```
# gunzip gcc-solaris-sparc-local.gz
```

3.- Instalar el paquete.

```
# pkgadd -d gcc-solaris-sparc-local
```

GZIP

El paquete Gzip contiene programas para comprimir y descomprimir archivos usando el codificador Lempel-Ziv (LZ77).

Gzip instala los siguientes programas: gunzip (enlace a gzip), gzexe, gzip, uncompress (enlace a gunzip), zcat (enlace a gzip), zcmp, zdiff, zforce, zgrep, zmore y znew



Instalación

1.- Convertirse en superusuario.

```
$ su - root
```

2. Descomprimir el paquete

```
# gunzip gcc-solaris-sparc-local.gz
```

3. Instalar el paquete

```
# pkgadd -d gzip-solaris-sparc-local
```

NULLMAILER

Nullmailer es un MTA (Agente de Transporte de Correo) de reemplazo para los hosts que retransmiten a un sistema fijo de relay simple. Está diseñado para ser simple de configurar y especialmente útil en las máquinas esclavo.

El software se puede obtener en: <http://em.ca/~bruceg/nullmailer/>.

Instalación

```
$ sh ./configure
```

```
$ make
```

```
# make install
```

OPENSSSH

Es una herramienta de seguridad que permite la conexión de computadoras por medio de un canal cifrado, esta herramienta es muy útil para los usuarios que realizan conexiones a través del servicio telnet, ftp. El software se puede obtener de la siguiente dirección: <http://www.openssh.org>.

Requerimientos

- GCC (Compilador C de GNU)
- Open-ssl. Obtenorio de <http://www.openssl.org>.
- Bibliotecas Zlib. Obtenieras de: [http:// www.freesoftware.com](http://www.freesoftware.com).
- Tcprappers

Instalación

1.- Descomprimir y desempaquetar el software.

```
$ gunzip < openssh-version.tar.gz | tar xvf -
```



2.- Copiar los archivos del TCP-Wrappers "tcpd.h" y "libwrap.a".

```
# cp directorio/Tcp-wrappers/tcpd.h /usr/local/include
# cp directorio/Tcp-wrappers/tcpd.h /usr/include
# cp directorio/Tcp-wrappers/libwrap.a /usr/local/lib
# cp directorio/Tcp-wrappers/libwrap.a /usr/lib
```

3.- Cambiarse a el directorio de OpenSSH.

```
$ cd openssl-version
```

4.- Realizar la configuración de sistema.

```
$/configure --with-tcp-wrappers --with-ssl-dir=/usr/local/ssl
```

Debemos tomar en cuenta que todos los componentes requeridos en estas opciones, deben estar instalados y configurados antes de configurar el openssl.

5.- Crear los archivos.

```
$ make
```

6.- Editamos el archivo /etc/inetd.conf, agregando la siguiente línea para que tcp-wrappers reconozca las conexiones de ssh y /etc/services para definir el puerto.

```
# vi /etc/inetd.conf
ssh stream tcp nowait root /usr/etc/tcpd /usr/local/sbin/sshd -i

# vi /etc/services
ssh 22/tcp
ssh 22/udp
```

6.- Empezar la instalación. Para versiones 3.3, 3.4 y 3.5 requiere crear el usuario sshd con las siguientes características.

```
# groupadd ssh
# useradd -g 115 -u115 -c "Usuario para Openssh" \
-d/var/empty -s/bin/false sshd
# make install
```

7. Reiniciar el demonio de inetd.

```
#ps -fea |grep inetd
#kill -HUP PID-INETD
```



OPENSSL

El protocolo SSL es utilizado para proporcionar una conexión segura entre un cliente y un servidor para protocolos de alto nivel como el HTTP.

Las zlib son bibliotecas de compresión de datos para compilar todos los archivos y ejecutar el programa de verificación. Se puede obtener zlib en <http://www.gzip.org/zlib/> y Openssl en <http://www.openssl.org>

Instalación

1. Descomprimir y desempaquetar el software de zlib.

```
$ gunzip -d < zlib-version.tar.gz | tar xvf -
```

2. Cambiarse al directorio de zlib.

```
$ cd zlib-1.1.4
```

3. Configurar las zlib para ser compiladas.

```
$ ./configure
```

4. Compilar las bibliotecas e instalarlas

```
$ make  
# make install
```

5. Descomprimir y desempaquetar el openssl "open secure socket layer".

```
$ gunzip < openssl-version.tar.gz | tar xvf -
```

6. Cambiarse al directorio.

```
$ cd openssl-version
```

7. Configurar el openssl.

```
$ ./config
```

9. Compilamos los fuentes y luego se instalan

```
$ make  
# make install
```



PATCHECK

Patch Check determina los niveles de parches en un sistema, comparándolos con la lista de Parches recomendados y de seguridad que Sun publica. La forma en que muestra la información es en formato HTML.

Requerimientos:

- PERL 5.0 o superior
- pkginfo, showrev y uname

Instalación

1. Bajar el Patch Check en <http://sunsolve.sun.com>.

2. Descomprimir y desagrupar el archivi patchcheck_1.1.tar.Z.

```
$ zcat pchk_1.1.tar.Z | tar xvf -
```

3. Bajar el archivo de referencia "patchdiag.xref" en <http://sunsolve.sun.com>.

4. Almacenar el archivo de referencia en donde se encuentra el archivo "patchk.pl" se debe bajar este archivo cada vez que se quiera hacer uso de esta utilidad.

5. Correr el siguiente script.

```
$ perl patchk.pl -b -l
```

6. Ver el archivo generado con extensión .html en un navegador. Abrir el navegador para mostrar los parches instalados y cuales hacen falta. En esta página se selecciona los que deseamos bajar (Patchsuite). Los agrupa en un archivo .tar

PERL

Lenguaje de programación, derivado de C, ampliamente utilizado para la generación de scripts y CGI.

Instalación

1. Descomprimir y desempaquetar el software de perl.

```
$ gunzip -d < perl-version.tar.gz | tar xvf -
```



2. Cambiarse al directorio de perl.

```
$ cd perl-version
```

3. Configurar perl para ser compiladas.

```
$ ./configure
```

4. Compilar los fuentes e instalarlos los binarios.

```
$ make
```

```
# make install
```

PHP

PHP es un lenguaje de programación que permite la realización de páginas web interactivas, conexiones con bases de datos. Obtener la distribución de <http://www.php.net/>.

Requerimientos

- Espacio en disco duro 4 MB durante la instalación, después de instalar 1.5 MB.
- Servidor Apache instalado

Instalación**1.- Descomprimir y desempaquetar el software.**

```
$ gzip -d < php-version.tar.gz | tar xvf -
```

2.- Cambiar al directorio php-version.

```
$ cd php-version/
```

3.- Configuración del sistema con soporte para sybase y oracle.

```
$ ./configure \
--enable-libgcc \
--with-apxs=/usr/local/httpd/bin/apxs \
--enable-versioning \
--with-sybase=/sybase \
--with-imap=/usr/local \
--with-config-file-path=/usr/local/httpd/conf \
--with-oracle=/usr/local/extra/oracle8 \
--with-oci8=/usr/local/extra/oracle8 \
--with-mysql=no
```



4.- Creación de archivos de instalación y empezar la instalación.

```
$ make
# make install
```

6.- Editar archivo /etc/httpd/conf/httpd.conf para la configuración.

```
# vi /usr/local/httpd/conf/httpd.conf.
```

Agregar las líneas:

```
LoadModule php4_module      libexec/libphp4.so
AddModule mod_php4.c
AddType application/x-httpd-php .php .html .php3
AddType application/x-httpd-php-source .phps
```

6. Copiar la biblioteca necesaria para PHP.

```
# cp php.ini-dist /usr/local/lib/php.ini
```

7.- Reiniciar el demonio de Apache.

```
# /usr/local/httpd/bin/apachectl restart
```

8.- Probar instalación.

```
$ cd ~usuario/htdocs
$ cat > indice.php
<?php phpinfo() ?>
[ctrl-d]
```

Dirigir el navegador a <http://mihost/~usuario/indice.php>

SOLARIS

Sistema operativo basado en UNIX de Sun Microsystems³⁹.

Instalación:

1. Se debe tener los siguientes datos:

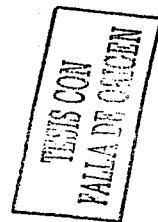
hostname: einstein

IP: 132.247.12.13

Domain: servidores.unam.mx

DNS: 132.248.204.1, 132.248.10.2

Máscara/subred: 255.255.255.0



³⁹ El documento completo de instalación de Solaris se puede consultar en el sitio <http://docs.sun.com>

2. Introducir el cdrom del software de Instalación de Solaris (disco 1 de 2). Ahora reiniciar el equipo desde cdrom o red, para el segundo caso se debe configurar la imagen de booteo.

```
OK boot cdrom o bien,  
OK boot net
```

3. Posteriormente aparecerá el ambiente de instalación de Solaris en modo texto, sólo basta seguir la secuencia de pantallas e ir introduciendo los datos como se requieran. Antes de indicar que particiones, aparecerá una pantalla donde se pregunta qué tipo de instalación se quiere, se lista a continuación, la primera es la más completa, así como la última es la más austera.

- Entire Solaris Software Group Plus OEM
- Entire Solaris Software Group
- Developer Solaris Software Group
- End User Solaris Software Group
- Core Solaris Software Group

Se recomienda utilizar para un servidor en producción la primera o segunda opción, eso dependerá del criterio del administrador y del espacio disponible en disco.

4. Configurar tarjeta de red

```
# ifconfig qfe0 inet 132.247.12.13 netmask 255.255.255.0 up
```

5. Configurar router. Se debe editar el archivo defaultrouter y agregando la dirección IP del router.

```
# vi /etc/defaultrouter  
132.247.12.253
```

6. Reiniciar el equipo.

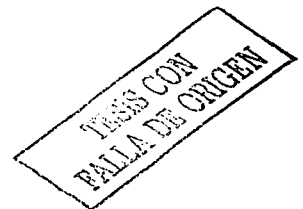
7. Hacer pruebas en otro equipo para verificar que esta correctamente configurada

```
plata $ ping 132.247.12.13
```

8. Bajar e instalar el cluster de parches del sitio <http://sunsolve.sun.com>

```
# cd /opt  
# unzip 8_Recommended.zip  
# cd 8_Recommended  
# ./install_cluster
```

9. Instalar las herramientas y aplicaciones que requiera brindar el servidor



SYBASE

Sybase es un Sistema Manejador de Bases de Datos (DBMS) relacionbal, soporta las instrucciones de SQL, maneja múltiples bases de datos, y usuarios

Instalación

Desde la unidad de cdrom compartida de Plata en Einstein.

1. Se monta el cdrom en /mnt en Einstein.

```
# mount -F nfs plata.servidores.unam.mx:/cdrom/sybase /mnt
```

2. Se debe crear el usuario sybase y que pertenezca al grupo other.

```
# useradd -g1 -u101 -c"Administrador de Sybase" -d/sybase -m sybase
```

3. Cambiarse a usuario sybase.

```
# su - sybase
```

4. Ejecuta el programa de instalación. Una vez ejecutado se deberá indicar en que directorio se instalara sybase, en este caso /sybase.

```
$ /mnt/syblog -D
SYBLOAD - Product Distribution Program
Sybase (c) 1996
Current directory is "/sybase".
Is this the correct directory for installation?
If so, please enter 'y' or 'Y': y
```

5. Indicar si la instalación es local o remota.

Is this a Local or Remote installation, as defined in your Installation Guide?

Please enter L for Local or R for Remote.

```
> l
```

6. Empezar instalación, dar numero de serie y el producto a instalar.

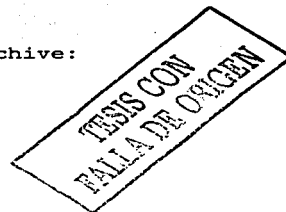
Please enter the full name of the disk file of the global archive:

```
> /mnt/sybimage
```

You specified /mnt/sybimage for the media device. Is this correct?

please enter 'y' or 'Y' to continue: **y**

Please enter your Customer Authorization String, letters only:



> AYHYBF HASYBK BYJKM BKBYBY BYHVB YIQE⁴⁰

Sybase Products available for installation:

Product No. 1: Adaptive Server Enterprise, Sun4_SVR4, 11.9.2

Product No. 2: Monitor Server for 11.9.2 ASE, Sun4_SVR4, 11.9.2

...

Product No. 12: Language Modules for Spanish, Sun4_SVR4, 11.9

Please enter the Product Numbers that you wish to install, one per line.

Terminate your entries with a blank line.

> 1

The following products were chosen for installation:

Choice No. 1: Adaptive Server Enterprise, Sun4_SVR4, 11.9.2

If this list is correct as shown,
please enter 'y' or 'Y' to continue,

'q' or 'Q' to quit,

or any other character to make another set of choices: y

SYBPERL

Syperl es un paquete de las extensiones de Perl que agregan básicamente las db_library API de Sybase para llamar a Perl; la combinación es una herramienta de gran alcance para los DBA de Sybase y los programadores.

Perl se ha convertido en el lenguaje a escoger para muchos gurús de WWW, debido a que Syperl se ha convertido en la herramienta para integrar las bases de datos de Sybase con la web y ahora hay algunas herramientas escritas en Syperl que hacen lo más simple uniforme.

Se puede obtener en: <http://www.perl.com/CPAN/authors/id/MEWP>

Instalación

```
# perl -CPAN -e shell;
cpan> i /sybase/
cpan> install Sybase::Syperl
```

TCP-WRAPPERS

TCP-Wrapper es una herramienta de seguridad que trabaja a través del demonio inetd, permitiendo el acceso a una máquina dada a través de los servicios que se definen en los archivos hosts.allow.

Se puede bajar de un lugar confiable:

⁴⁰ El número de serie que se muestra en este proyecto referente a Sybase es ficticio como medida de seguridad.



ftp://coast.cs.purdue.edu/pub/tools/unix/netutils/tcp_wrappers.

Requerimientos

Tener instalado GCC - Compilador C de GNU

Instalación

1. Descomprimir y desempaquetar el software.

```
$ gzip -d < tcp_wrappers_version.tar.gz | tar xvf -
```

2. Cambiar al directorio de tcp-wrappers.

```
$ cd tcp_wrappers_version
```

3. Editar el archivo Makefile para ajustar parámetros de compilación para solaris 2.x.

```
$ vi Makefile
```

En la línea 47, quitar #

```
o # REAL_DAEMON_DIR=/usr/sbin
n REAL_DAEMON_DIR=/usr/sbin
```

En la línea 409, quitar #

```
o #LIBS = -lsocket -lnsl # SysV.4 Solaris 2.x
n LIBS = -lsocket -lnsl # SysV.4 Solaris 2.x
```

En la línea 457, poner un # y quitar un # en la 459

```
o BUGS = -DGETPEERNAME_BUG -DBROKEN_FGETS -DLIBC_CALLS_STRTOK
n #BUGS = -DGETPEERNAME_BUG -DBROKEN_FGETS -DLIBC_CALLS_STRTOK
```

En la línea 517, cambiar LOG_MAIL a LOG_LOCAL0

```
o FACILITY= LOG_MAIL # LOG_MAIL is what most sendmail daemons use
n FACILITY= LOG_LOCAL0 # LOG_MAIL is what most sendmail daemons use
```

En la línea 554, Quitar #

```
o #AUTH = -DALWAYS_RFC931
n AUTH = -DALWAYS_RFC931
```

4. Editar el archivo /etc/syslog.conf agregar en la última línea:

```
# vi /etc/syslog.conf
local0.info /var/adm/tcpsdlog
```

NOTA:

- Los espacios entre ".info" y "/var" en la línea sean tabuladores y no espacios
- La ruta y el nombre del archivo son establecidos de acuerdo al criterio del administrador. En



este archivo se guardan los accesos al equipo a través de los servicios protegidos por tcp wrappers

5. Crear la ruta y el archivo especificados en /etc/syslog.conf

```
# touch /var/adm/tcpdlog
```

6. Crear ruta donde estará los binarios de tcpwrappers

```
# mkdir /usr/etc
```

7. Regresar a usuario normal y ejecutar el comando make.

```
$ make sunos5 CC=gcc
```

8. Convertirse en root.

```
$ su - Password:
```

9. Cambiarse al directorio de tcp wrappers y copiar los archivos indicados al directorio determinado por el administrador.

```
# cd ~user/tcp_wrappers_version
# cp tcpd tcpdmatch tcpdchk try-from safe_finger /usr/etc
```

10. Editar el archivo inetd.conf.

```
# vi /etc/inetd.conf
```

Cambiar las líneas que no concuerden con su archivo local.

```
#ftp      stream  tcp    nowait  root    /usr/sbin/in.ftpd      in.ftpd
ftp       stream  tcp    nowait  root    /usr/etc/tcpd          in.ftpd
#telnet   stream  tcp    nowait  root    /usr/sbin/in.telnetd   in.telnetd
Telnet    stream  tcp    nowait  root    /usr/etc/tcpd          in.telnetd
Ssh       stream  tcp    nowait  root    /usr/etc/tcpd          /usr/lib/ssh/sshd -i
```

11. Crear archivos de acceso.

```
# vi /etc/hosts.allow
```

```
ALL: LOCAL .dominio.com , ip.que.entra.aqui
```

12. Crear archivos de negación.

```
# vi /etc/hosts.deny
```

```
ALL : ALL
```

TESIS CON
FALLA DE ORIGEN

13. Levantar demonio de inetd.

```
# pgrep inetd
139
# kill -HUP 139
```

14.- Levantar demonio de syslog.

```
# pgrep syslogd
3757
# kill -HUP 3757
```

VERITAS VOLUME MANAGER

Veritas Volume Manager es una herramienta de administración de volúmenes en línea para entornos corporativos de fácil utilización. A diferencia de otras opciones tales como hardware RAID y Solstice DiskSuite, no escalan adecuadamente o son difíciles de administrar, Veritas Volume Manager asegura alta disponibilidad de datos, rendimiento superior y escalabilidad para la corporación - todo en línea.

Mediante la creación de dispositivos de almacenamiento virtual a partir de discos físicos y arrays de discos, Veritas Volume Manager remueve las limitaciones físicas de almacenamiento en disco de manera tal que se pueda configurar, compartir, y manejar el almacenamiento para su óptimo resultado. Los volúmenes lógicos sobrepasan las restricciones físicas impuestas por los dispositivos de hardware de discos.

Instalación**1. Insertar el CD de instalación****2. Cambiarse al directorio donde se encuentran los paquetes**

```
cd /cdrom/volume_managerversion/pkgs
```

3. Instalar los paquetes

```
# pkgadd -d . VRTSvlic VRTSvxvm VRTSvmdoc VRTSvmman VRTSob VRTSobgui \
VRTSvmpro VRTSfspro VRTSvxfs VRTSfsdoc
```

4. Reiniciar el equipo

```
# sync
# init 6
```

TESIS CON FALLA DE ORIGEN

APÉNDICE B**Políticas y Procedimientos****A) POLÍTICAS****POLÍTICAS PARA LOS ADMINISTRADORES****Políticas sobre uso de las cuentas**

- Es responsabilidad de los administradores cambiar password del superusuario (root) y de las cuentas de los administradores cada mes, dos meses o antes si se considera necesario. Si alguno de los administradores dejara de laborar en el Departamento de Administración de Servidores, modificar inmediatamente el password y notificar a los demás administradores.
- Las cuentas de los administradores en un servidor de producción, serán bloqueados inmediatamente a la salida del miembro. Y su cuenta será eliminada definitivamente, después de tres meses.
- El administrador deberá entrar siempre como usuario común y no como superusuario, al menos que se requiera entrar bajo circunstancias especiales, como no tener cuenta dentro de staff o bien cuando ocurre alguna emergencia que requiere entrar directamente como root.
- Las cuentas de usuario común de los administradores tendrán un nombre de grupo igual al del login, deberán cumplir con las características de cuentas únicas y letras minúsculas. En cuanto a su uso es personal e intransferible, por lo cual no se permite compartir su cuenta ni su contraseña con persona alguna, aún si ésta acredita la confianza del usuario.
- Todos los passwords, tanto root como usuarios comunes deberán cumplir con las siguientes características:
 - Tener dígitos y/o caracteres de puntuación.
 - Incluir algunos caracteres de control y/o espacios.
 - Tener tanto mayúsculas como minúsculas.
 - Contener palabras fáciles de recordar, de este modo no se necesita escribirlos en papel.
 - No deben ser palabras que estén dentro de un diccionario, secuencias conocidas de caracteres, datos personales ni acrónimos.
 - No enviar password a través de e-mail
 - Contener de 6 a 8 caracteres.

TESIS CON
FALLA DE ORIGEN

- Los administradores deberán seguir las siguientes precauciones con las contraseñas de root y usuario de administración. Si llegase a cometer un descuido cambiarla y notificar a los demás administradores:
 - No incluir el nombre de la cuenta y dominio.
 - No dejar la contraseña en lugares que sean fáciles de obtener (papel, cuaderno, pegada a la terminal, teclado o cualquier otra parte del sistema).
 - Al escribir la contraseña no hacerlo de manera explícita combinar la contraseña con otras letras o palabras incluso de la misma contraseña.
 - No grabar la contraseña electrónicamente (archivo, base de datos, correo electrónico) a menos que la contraseña se encuentre cifrada.
 - No usar la contraseña de la cuenta como contraseña para otras aplicaciones como juegos en línea, por ejemplo.

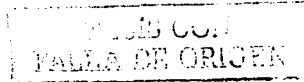
Políticas sobre conexión al sistema o de control de acceso

- El administrador deberá conectarse a los servidores a través de programas seguros (ssh, scp o sftp).
- El administrador deberá acceder a los servidores de producción a través de una dirección IP definida, preferentemente pertenecientes a las asignadas al departamento. Si se requiere acceder por modem deberá ser a través de una "equipo puente", el cual es un equipo que tiene abierto lo servicios para proveedores de Internet como modems de la UNAM y prodigy así como aquellas computadoras dentro de Red UNAM.

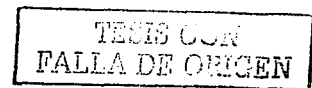
Políticas sobre tareas para los administradores

- El administrador podrá hacer uso de programas que rastrean o explotan vulnerabilidades en los sistemas propios y no en los ajenos, con el fin verificar el nivel de seguridad, se realizará un reporte detallado y si se hará los cambios necesarios.

El uso de herramientas para tener conocimiento de las características del servidor (como detección de puertos abiertos, vulnerabilidades o intento de ataque) en cualquiera de nuestro servidores deberá notificarse anticipadamente una semana y por escrito. Si no se notifica por escrito de forma clara lo que se desea realizar, estamos en nuestro derecho de sancionar al responsable. Un mal empleo de herramientas en un servidor de producción puede causar inestabilidad en el servidor por ser usado en horas críticas. Esto aplica a los administradores y a usuarios externos.



- No se permitirá bajo ninguna circunstancia el uso de cualquiera de las computadoras con propósitos de ocio o lucro.
 - El administrador deberá emplear regularmente herramientas de seguridad para verificar la integridad de los archivos del sistema, tales como: Satan, Cops, John the ripper, Tripwire, entre otras.
 - Revisar que no existan archivos de root con permisos de escritura para todo el mundo
 - Revisar que no existan archivos .rhosts con permisos de escritura para todo el mundo
 - Revisar que los directorios del sistema (como /, /bin, /usr, /usr/bin, etc.) pertenezcan a root y a los grupo sys y other, según sea el caso.
 - Revisar que no haya archivos cuyo dueño no aparezca en /etc/passwd.
 - Revisar que los archivos de dispositivos y configuración tengan los permisos correctos.
 - Revisar los usuarios con UID 0, investigar el por qué y cómo lo utilizan, posteriormente modificarlas.
 - Revisar detalladamente los archivos ocultos, con espacio, con nombres como: crack, irc, sniff, scan, .forward, shadow, passwd, hack y bitch.
 - El administrador deberá verificar que cada cuenta de los usuarios tenga contraseña y sea segura. Para ello hay que revisar periódicamente los archivos /etc/passwd y /etc/shadow con ejecutar periódicamente el programa de John the ripper.
 - El administrador deberá monitorear los recursos del servidor, memoria swap, tipo y número de procesos, espacio en disco, conexiones, entre otras.
 - Cada administrador deberá realizar una bitácora de las actividades realizadas por cada servidor a su cargo (control de cambios). Entendiéndose por actividades como: cambio en la configuración, actualizaciones, alta y baja de usuarios; en general, todo aquello que se considere importante. Se indicará la fecha y tipo de acción por servidor. Las bitácoras deberán estar en un lugar seguro, por tanto no estarán almacenadas en el mismo sistema. Deberá estar de forma escrita como en un medio electrónico.
 - Los scripts y bitácoras de las herramientas y aplicaciones referentes a la administración (estarán en cualquier de las siguientes rutas: /home/log, /home/logs o /home/root) ubicadas dentro de un File System propio o específico.
 - Cada uno de los servidores en producción deberá tener mínimamente documentado:
 - Configuración de Hardware y Software
 - Procedimientos
 - Bitácoras
 - Alamas (clasificación y descripción)
- La documentación deberá ser detallada y actual.
- Los File Systems con cuota para usuarios de los servicios se denominarán: /home/users?? o



alguno en especial, en ambos casos especificarlos en la documentación.

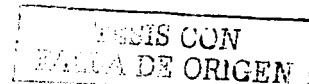
- Todos los usuarios que no sean del sistema (por ejemplo root o demonios) deberá asignarse una cuota después de ser creada la cuenta, sino se especifica será de 5MB.

Políticas de respaldos

- El administrador del sistema será el responsable de realizar respaldos de la información periódicamente. Cada treinta días deberá efectuarse un respaldo completo del sistema y cada semana deberán ser respaldados todos los archivos que fueron modificados o creados.
- La información respaldada deberá ser almacenada en un lugar seguro, es decir aquel lugar donde se almacenen las cintas, bajo llave y en condiciones que no dañen la integridad del dispositivo.
- Deberá mantenerse siempre una versión reciente impresa de los archivos más importantes del sistema, como son vfstab, inetd.conf, services, httpd.conf, bases de datos (logs y datos), hosts.allow.
- En el momento en que la información respaldada deje de ser útil a la organización, dicha información deberá ser borrada antes de deshacerse del medio.
- El administrador etiquetará las cintas empleadas para los respaldos, indicando fecha, servidor, tipo de respaldo y número de cinta. Además, llevar un registro de cada cinta en medio electrónico preferentemente.
- El administrador revisará que los respaldos sean recuperables, realizando pruebas para verificar que la información efectivamente se puede restaurar.
- Una vez realizado el respaldo, el administrador deberá retirar la cinta del dispositivo, guardarla y tratarla con cuidado, aislándola de factores como el electromagnetismo, la temperatura, el polvo, la humedad y los golpes.

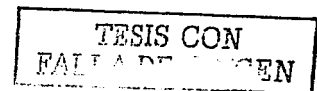
Políticas sobre uso de Hardware

- El acceso al site será únicamente para los administradores o bien por personas autorizadas previamente por el jefe del departamento y acompañadas por al menos un administrador.
- El site deberá permanecer cerrado bajo llave por el administrador.
- El administrador cuidará que los conectores, cables y dispositivos periféricos no estén dispersos, mal acomodados o cualquier factor que pueda provocar algún daño o mal funcionamiento.
- El administrador se asegurará de mantener limpio el site periódicamente, aclarando que se realizará por todos los administradores del departamento.



POLÍTICAS SOBRE EL SERVICIO DE WEB-HOSTING

- Para dar de alta un sitio web, deberá notificar el usuario a través de un documento los siguientes datos:
 - Responsable técnico y administrativo (correo electrónico, número telefónico)
 - Dependencia
 - Nombre del sitio y descripción
 - Programas y herramientas que empleará
 - Direcciones IP o dominios de los equipos donde se conectarán al servidor
 - Nombre del usuario - login (opcional)
 - Cuota (opcional)
- Los usuarios sólo podrán hacer uso de las herramientas instaladas por el administrador del servidor, las herramientas instaladas por el propio usuario serán eliminadas. Si se requiere de ella se hará un estudio sobre factibilidad, concediéndonos el derecho de no instalarlas si no cumplen los lineamientos de la etapa de pruebas de software instalado.
- Todos los usuarios deberán tener una cuota fija que se deberá especificar en el momento de darse de alta la cuenta. Si no es especificada se dará un mínimo de 5 MB
- Todos los sitios web dispondrán de estadísticas para verificar los hits de cada uno. Las estadísticas serán realizadas por una herramienta denominada Webalizer y se encuentran ubicadas en <http://einstein.servidores.unam.mx/estadisticas>.
- El contenido de los sitios deberán cumplir con los fines que persigue la UNAM, ciencia, cultura, investigación o docencia; por tanto no deberá perseguir fines de lucro ni ocio particulares.
- La baja definitiva de un sitio deberá realizarse primeramente en el servidor de Web, luego en el DNS (si se solicita), después de una semana o un respaldo completo borrar la cuenta dentro del sistema. Si el Responsable administrativo solicita un respaldo del sitio, se almacenará en un periférico de almacenamientos secundario (CD-ROM o diskette).
- El administrador dará de baja temporal un sitio cuando no se pueda localizar al responsable Técnico o Administrativo para aclarar el funcionamiento anormal de su sitio, el periodo será de 4 meses y posteriormente se dará de baja definitiva.



POLÍTICAS PARA LOS USUARIOS**Políticas de conexión**

- Los usuarios sólo deberán conectarse a los servidores a través de servicios seguros, como ssh (secure shell), scp (secure copy), sftp (secure file transfer protocol).
- El usuario deberá proporcionar la dirección IP o dominio al que pertenece el equipo por medio del cual se conectará.

Políticas de uso de cuentas

- Para cada usuario se creará un grupo con el mismo login, de esta forma se evitará modificaciones de información por parte de otros usuarios de este equipo (einstein.servidores.unam.mx). Si llegase haber modificaciones por una mala asignación de permisos, el departamento de Administración de Servidores no se hace responsable.
- El usuario recibirá una notificación de la creación de su cuenta, a partir de ese momento se hace responsable del uso que le dará. Cabe hacer notar que la cuenta es **personal, confidencial e intransferible**, por tanto cualquier anomalía que se suscite será responsabilidad del usuario y se hará acreedor a la(s) sancion(es) correspondiente(s) de acuerdo a la falta que incurra. (véase **sanciones**)
- El password correspondiente a la cuenta brindada deberá ser modificado por el usuario en el primer acceso a la misma. El nuevo password deberá componerse al menos de una secuencia de caracteres tales como letras, números, signos de puntuación, caracteres especiales (\$ % & @) y deberá tener un mínimo de 6 y máximo de 8 caracteres.
- El espacio disponible en disco para las cuentas de los usuarios, será asignado de acuerdo a la capacidad de almacenamiento con que disponga el servidor
- Se hará una revisión trimestral de la vigencia de las cuentas y sitios, así como una revisión diaria del uso adecuado de los recursos y servicios.

Políticas sobre aplicación, programas, herramientas o desarrollos

- Cualquier aplicación programa, herramienta o desarrollo que cause problemas de desempeño, ya sea de uso de memoria y/o procesador en el servidor, será bloqueado temporalmente hasta que sea arreglado por el usuario o bien borrado si no lo resuelve.
- El servidor `einstein.servidores.unam.mx` cuenta con el software que a continuación se lista.
 - Apache
 - Php
 - Sybase
 - Openssh
 - Perl

TESIS CON
FALLA DE ORIGEN

- Para evitar el uso inadecuado de los recursos disponibles se deberá justificar el uso de herramientas o aplicaciones de software (módulos extras de perl, php u otro software).

Sanciones

- 1a. Recurrencia. Se le avisará al usuario que incurrió en una falta y cuál fue dicha falta.
- 2a. Recurrencia. Será dado de baja temporalmente el usuario que este haciendo mal uso de su cuenta.
- 3a. Recurrencia. Se cancelará el servicio.

TESIS CON
FALLA DE ORIGEN

B) PROCEDIMIENTOS**Administración****a) Dar de alta usuario**

La creación de cuentas UNIX para el servidor Einstein se llevará a cabo de acuerdo a las políticas antes citadas, estarán en los File Systems para usuarios, /home/users??, donde ?? corresponden a un rango 00 hasta 03; se debe aclarar que existe espacio para crear más File Systems en el servidor.

1. Agregar el grupo.

```
# grouppadd <nom_grupo>
```

2. Verificar el UID y el login, el UID debe ser consecutivo y el login no debe repetirse.

```
# tail /etc/passw
```

3. Agregar el usuario.

```
# useradd -u<UltimoIDuser+1> -g<GID> -c"aqui se pone una descripcion o comentario" -d/home/usuario -m -s </rutadel/shell> <usuario>
```

4. Introducir una contraseña

```
# passwd <usuario>
```

5. Definirle una cuota al usuario, se debe de introducir en Kbytes, la primera es la suave y la segunda es la dura (ej. Suave: 150000, Dura: 153600; son 15MB).

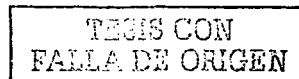
```
# edquota <usuario>
```

6. Verificar la cuota.

```
# quota -v <usuario>
```

```
Disk quotas for <usuario> (uid <UltimoIDuser+1>):
Filesystem usage quota limit timeleft files quota limit timeleft
/home/users?? 0 150000 153600 0 0 0
```

7. Probar la cuenta que funcione correctamente. Para ello se debe de entrar por primera vez a la cuenta como lo haría el usuario a través de ssh.



b) Asignar cuota a un File System (FS)

Los File Systems creados en Einstein para los usuarios tienen activada las cuotas, aunque se contempla que probablemente se requiera mayor espacio y se active cuota al nuevo File System.

1. Crear un archivo vacío llamado cuotas dentro del directorio que hace referencia al FS.

```
# touch /home/users03/cuotas
```

2. Cambiarle los permisos.

```
# chmod 600 cuotas
```

3. Habilitar el FS para que tenga cuotas.

```
# quotaon /dev/vx/dsk/rootdg/vol??
```

4. Probar que haya quedado bien, entonces le ponemos cuota a un usuario.

```
# edquota <usuario>
```

```
# quotacheck -va
```

c) Borrar usuarios

Se debe considerar diversos aspectos para dar de baja un usuario. Primeramente antes de borrarlo debe bloquearse temporalmente la cuota, de la siguiente forma:

```
# passwd -l <usuario>
```

La cuenta debe estar bloqueada hasta que se haga el siguiente respaldo completo, el motivo es como una medida de protección, ya que aunque para eliminar una cuenta debe ser bajo la autorización del usuario, existe la posibilidad que no tenga respaldo de su información y en un futuro la requiera.

1. Desactivar la cuota, poniéndola en ceros.

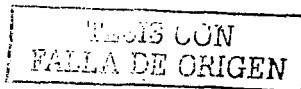
```
# edquota <usuario>
```

2. Eliminar el archivo donde se especifica los crones del usuario (si llegase a tener).

```
# rm /var/spool/cron/crontabs/<usuario>
```

3. Quitarlo del archivo /etc/cront.d/cron.allow, editando el archivo (si llegase a definirse el usuario).

```
# vi /etc/cron.d/cron.allow
```



4. Eliminar cuenta. Con el siguiente comando se eliminará en la tabla de passwd y su directorio HOME.

```
# userdel -r <usuario>
```

d) Respaldos

Los respaldo se realizan de forma periódica. Existen dos tipos incremental y completo, el primero se realiza semanalmente y el segundo mensualmente, los días viernes. El script es `/home/logs/root/scripts/DeTocho`

Existe un cron que realiza los respaldos a cintas DLT, contempla tanto respaldos incrementales y completos. En algunas ocasiones no se puede hacer los respaldos en cintas DLT, por la razón que no se cuentan con dichas cintas, así que se emplea cintas de 4mm, mientras se vuelve a disponer de cintas DLT. El procedimiento para respaldo en cintas de 4mm es:

Respaldo incremental.

1. Colocar la cinta de 4mm en la unidad de tungsteno.
2. Ejecutar el siguiente script.

```
# /home/logs/root/scripts/respSEMANAL/respIncTungsteno.4m.sh &
```

Respaldo completo.

1. Colocar la cinta de 4mm en la unidad de tungsteno.
2. Ejecutar el siguiente script.

```
# /home/logs/root/scripts/respCOMPLETO/respComTungsteno.4m.sh
```

NOTA: Requerirá más de una cinta. Cuando aparezca el mensaje quitar la cinta y colocar la nueva cinta, finalmente teclear "yes".

TESIS CON
FALLA DE ORIGEN

Apache**a) Crear Sitio**

Nota: Antes de crear un sitio ver el procedimiento de crear un usuario

1. Cambiarse al usuario.

```
# su - login
```

2. Crear el directorio htdocs, para que el usuario pueda colocar sus páginas, además poner el *indice.html* de prueba. Los archivos pueden ser: *index.html home.html index.htm indice.html index.php*.

```
usuario@einstein $ mkdir htdocs
usuario@einstein $ cd htdocs
usuario@einstein $ vi indice.html
<HTML>
<BODY>
    <CENTER> <H2> PAGINA EN CONSTRUCCION </H2> </CENTER>
</BODY>
</HTML>
```

3. Ubicarse en el directorio conf del apache y editar el archivo httpd.conf

```
# cd /usr/local/httpd/conf
# vi httpd.conf
```

4. Agregar las siguientes líneas después del último sitio.

```
#***** PONER DESCRIPCION DEL SITIO (DEPENDENCIA) www.sitio.unam.mx
CREACION/MIGRACION:
<VirtualHost 132.247.12.13>
ServerAdmin usuario@direccion.decorreo.com
DocumentRoot /home/users?/?/login/htdocs
ServerName www.sitio.unam.mx
ErrorLog /home/logs/apache/error_login.log
TransferLog /home/logs/apache/access_libiis.log
ScriptAlias /cgi-bin/ /home/users?/?/login/cgi-bin/
</VirtualHost>
<Directory /home/users?/?/login/htdocs
Options FollowSymLinks ExecCGI
</Directory>
```

TESIS CON
FALLA DE ORIGEN


```
<Directory /home/users??/login/cgi-bin/  
Options FollowSymLinks ExecCGI  
</Directory>
```

5. Revisar la configuración del apache (sintaxis).

```
# /usr/local/httpd/bin/apachectl configtest  
Debe marcar Ok
```

6. Detener e iniciar el apache o bien se puede reiniciar

```
# /usr/local/httpd/bin/apachectl stop  
# /usr/local/httpd/bin/apachectl startssl  
o  
# /usr/local/httpd/bin/apachectl restart
```

NOTA: La diferencia entre stop-startssl y restart, es que la primera opción requiere que se introduzcan los certificados y la segunda opción no lo requiere. Si no se introducen correctamente los certificados no se puede iniciar el Apache.

7. Verificar que funcione correctamente el sitio, para ello hay que "engañar" a una máquina (en este caso plata), esto se refiere a que busque primero el sitio en la máquina que tenga disponible un navegador. La engañamos porque si hay algún error y no verificamos que todo funcione correctamente, cuando se cambie el DNS, el error o errores los verá todo el mundo.

Entonces, editamos el siguiente archivo:

```
root@plata# vi /etc/hosts  
132.247.12.13          www.sitio.unam.mx
```

8. Luego abrimos un navegador.

9. Revisar si realmente funciona.

10. Notificar a los del NIC para que den de alta el sitio o cambien el direccionamiento del DNS, enviando un correo a nic@unam.mx.

TESIS CON
FALLA DE ORIGEN

b) Restringir acceso a un directorio**Restringido por el Administrador**

Directorio a restringir: http://www.sitio.unam.mx/ruta_directorio

1. Editar el archivo de configuración del Apache (httpd.conf)

```
# vi /usr/local/apache/conf/httpd.conf
## Poner fecha de modificación
<Directory /home/users??/usuario/htdocs/directorio_a_restringir>
    Options FollowSymLinks ExecCGI
    AuthType Basic
    AuthName "Modulo de modificacion"
    AuthUserFile /ruta/donde/esta/archivo_del_password
    <Limit GET POST>
        require valid-user
    </Limit>
</Directory>
```

2. Agregar usuario al archivo especificado (/ruta/donde/esta/archivo_del_password).

```
# /usr/local/apache/bin/htpasswd [-c] \
/ruta/donde/esta/archivo_del_password login
New password:
Re-type new password:
Adding password for user login
```

3. Verificar que esta funcionando correctamente en un navegador.

```
http://www.sitio.unam.mx/ruta_directorio
usuario: login
password:
```

Restringido por el Usuario**1. Crear el directorio a restringir**

```
$ mkdir /home/usuario/htdocs/directorio_a_restringir/
```

2. Cambiarse al directorio que será restringido

```
$ cd /home/usuario/htdocs/directorio_a_restringir/
```

3. Editar el archivo .htaccess con las siguientes líneas

```
$ vi .htaccess
AuthUserFile /home/usuario/.htpasswd
```



```
AuthName "Solo Administradores"
AuthType Basic
<Limit GET POST>
require valid-user
</Limit>
```

4. Agregar usuario al archivo especificado (/home/usuario/.htpasswd).

```
$ /usr/local/apache/bin/htpasswd -c \
/home/usuario/.htpasswd login
```

NOTA: la opción -c crea el archivo donde estarán los usuarios y contraseñas, si ya existe no es necesario ponerla.

5. Verificar que está funcionando correctamente en un navegador.

```
http://www.sitio.unam.mx/ruta_directorio
usuario: login
password:
```

c) Dar de baja un sitio

1. Ubicarse en el directorio conf del apache y editar el archivo httpd.conf. Para ello se debe comentar las líneas pertenecientes al sitio (usando # al inicio de cada línea).

```
# cd /usr/local/httpd/conf
# vi httpd.conf
```

2. Revisar la configuración del apache (sintaxis).

```
# /usr/local/httpd/bin/apachectl configtest
```

Debe marcar Ok

3. Reiniciar el Apache.

```
# /usr/local/httpd/bin/apachectl restart
```

4. Notificar a los del NIC para que den de baja el alias o cambien el direccionamiento del DNS, enviando un correo a nic@unam.mx.

TESIS CON
FALLA DE ORIGEN

d) Crear un Alias

1. Ubicarse en el directorio conf del apache y editar el archivo httpd.conf. Para ello se debe hacerse los cambios en la sección del sitio que contendrá el Alias, agregando la directiva de Alias, especificando el nombre del alias y la ubicación.

```
# cd /usr/local/httpd/conf
# vi httpd
<VirtualHost 132.247.12.13>
ServerAdmin usuario@direccion.decorreo.com
DocumentRoot /home/users??/login/htdocs
ServerName www.sitio.unam.mx
ErrorLog /home/logs/apache/error_login.log
TransferLog /home/logs/apache/access_libiis.log
ScriptAlias /cgi-bin/ /home/users??/login/cgi-bin/
Alias /nom_alias "/home/users??/login/ruta/alias"
</VirtualHost>.conf
```

2. Revisar la configuración del apache (sintaxis).

```
# /usr/local/httpd/bin/apachectl configtest
```

Debe marcar Ok

3. Reiniciar el Apache.

```
# /usr/local/httpd/bin/apachectl restart
```

4. Verificar que esta funcionando correctamente en un navegador.

```
http://www.sitio.unam.mx/ruta_directorio
```

TESIS CON
FALLA DE ORIGEN

Sybase**a) Crear una Base de datos****1. Entrar como usuario sybase.**

```
# su - sybase
sybase % isql -Usa -w600
```

2. Crear dispositivos.

```
1> disk init name = "<nomDev>0", \
    physname="/SWsybase/<nomDev>.dat", vdevno=<n>, size=<m>
1> disk init name = "<nomDev>log0", \
    physname="/SWsybase/<nomDev>.log", vdevno=<n>, size=<m>
```

nombre = el nombre del dispositivo, por lo regular esta relacionado con el de la base de datos
n = id del dispositivo, verificar el numero del ultimo dispositivo creado y poner el que le sigue. Para verificar utilizar el procedimiento almacenado `sp_helpdevice`.
m = es el tamaño, el cual equivale al tamaño en MB por 512

3. Creación de las bases de datos.

```
1> create database <nom_BD> on <nomDev>0=<x> log on <nomDev>log0=<x>
2> go
```

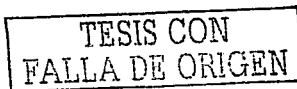
nom_BD = nombre de la base de datos a crear

x = tamaño del dispositivo en MB

4. Creación del usuario de la base de datos.

```
1> sp_addlogin <nom_login>,"<password>",<nomDB>
2> go
1> use <nomBD>
2> go
1> select db_name()
2> go
1> sp_changedbowner <nom_login>
2> go
1> use master
2> go
```

nom_login = el nombre del usuario para la base de datos



b) Crear un Usuario no dbo

1. Agregar un login.

```
1> sp_addlogin <usuario>,"<password>", <nomDB>
```

2. Cambiarse de Base de Datos.

```
1> use <nomDB>
```

3. Verificar cuantos usuarios hay en la Base de Datos.

```
1> sp_helpuser
```

```
Users_name ID_in_db Group_name Login_name
```

```
-----
```

```
dbo 1 public sistemas
```

```
(return status = 0)
```

4. Agregar el usuario a la base de datos.

```
1> sp_adduser dsis, dsis
```

5. Verificar que haya sido agregado a la Base de Datos.

```
1> sp_helpuser
```

```
Users_name ID_in_db Group_name Login_name
```

```
-----
```

```
dbo 1 public sistemas
```

```
dsis 3 public dsis
```

```
(return status = 0)
```

c) Borrar bases de Datos

```
1> drop database <nom_bd>
```

d) Respaldos

Los respaldos de las bases de datos se realizan semanalmente a través de un cron los días viernes. El script es /home/logs/root/scripts/DeTocho



APÉNDICE C

Niveles de RAID

Cada año desde hace 20 años la capacidad procesamiento ha aumentado un 40 % y los discos han doblado su capacidad, mientras que su costo se ha reducido a la mitad. Desgraciadamente, el aumento del rendimiento de los discos duros ha sido menos importante en comparación con el rendimiento del sistema, ya que tan sólo ha mejorado un 50 % durante la última década. Por tanto los discos duros son menos eficaces que el redimiendo general del sistema, provocando una descompensación entre el tratamiento de la información del sistema (muy rápido) y la lectura y escritura de datos en el disco duro(muy lenta). Para ello se inventó un sistema para guardar información en varios discos duros a la vez por lo que acceso se hacia más rápido, ya que la carga se distribuía entre los diferentes discos duros, a ésto se le llamó cadenas redundantes de discos de bajo costo (RAID). Pero a la hora de saber como optimizar el RAID existen algunos problemas, como puede ser encontrar la perfecta relación calidad-precio. Una de las ideas originales de los discos RAID, era la reducción del costo. Inicialmente se pensó que si se cambiaban los discos de gran capacidad por un conjunto de discos de menor capacidad y menor precio se reduciría el costo del mantenimiento. Desgraciadamente no es así, ya que, un disco RAID es más caro que un disco duro convencional de la misma capacidad.

Definición de RAID: RAID (Redundant Array of Independent Disks) es un conjunto de dos o más discos que funcionan de forma conjunta, para poder aumentar el rendimiento y el nivel de protección de los datos.

No obstante, los discos RAID proporcionan una serie de ventajas respecto a los discos duros convencionales, ya que pueden ser más útiles para nuestros sistemas.

Ventajas de los discos RAID:

- El rendimiento general del sistema aumenta, ya que pueden funcionar de forma paralela con los diferentes discos del conjunto.
- Dependiendo del nivel de RAID que escojamos, si uno de los discos del conjunto falla, la unidad continúa funcionando, sin pérdida de tiempo ni de datos. La reconstrucción de los datos del disco que ha fallado se hace de forma automática.
- La capacidad global del disco aumentará, ya que se suman las capacidades de los diferentes discos que componen el conjunto.

TESIS CON
FALLA DE ORIGEN

Los diferentes Niveles Raid.

La primera definición de RAID, fue en 1987, pueden definirse inicialmente 5 niveles RAID, aunque posteriormente se están haciendo 2 más. Los niveles RAID ofrecen grandes diferencias entre rendimiento e integridad de los datos, dependiendo de las especificaciones de cada nivel. No hay un nivel RAID perfecto para todos los usuarios, ya que cada uno de ellos cumplen distintos propósitos.

RAID 0: Data Striping Without Parity (DSA)

Striping es útil si se necesita cantidades grandes de datos que escribir o leer de un disco físico rápidamente, usando múltiples transferencias de datos en paralelo hacia muchos discos, es decir nos permite balancear carga de E/S.

Aplicaciones: Edición y producción de imágenes, video y prensa.

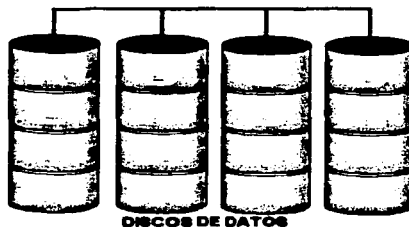


Figura C.1 - RAID 0

Ventajas RAID 0

- Proporciona un alto rendimiento.
- No tiene costo adicional.
- Toda la capacidad del disco se emplea.

Inconvenientes RAID 0

- No es verdaderamente un disco RAID, ya que es el único nivel que no tiene integridad de datos.
- Un error en uno de los discos implica la pérdida total de los datos.

TESIS CON
FALLA DE ORIGEN

RAID 1: Mirrored Disk Array (MDA)*Conjunto de discos en espejo*

El nivel RAID 1 es más conocido como mirroring ("espejeo"), ya que los datos son escritos al mismo tiempo en dos discos diferentes. Tienen dos copias exactas del total de la información. El RAID 1 es una solución cara, ya que desaprovecha la mitad de la capacidad total del conjunto de discos. Si falla un disco duro se convierte en inaccesible, pero el sistema continua funcionando usando el espejo no afectado.

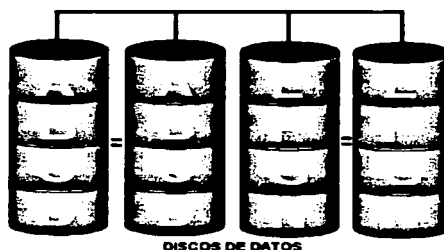


Figura C.2 - RAID 1

Ventajas RAID 1

- Mayor rendimiento en las lecturas de datos respecto a un disco convencional.
- Podemos recuperar todos los datos, en caso de error en uno de los discos.

Inconvenientes RAID 1

- Bastante caro, ya que necesitamos el doble de espacio del necesario.
- Moderada lentitud en la escritura de datos, ya que los hemos de escribir en dos localizaciones distintas

RAID 2: Hamming Code for Error Correction

TESIS CON
FALLA DE ORIGEN

RAID 2 es el primer nivel que usa código de correcciones de error utilizando la "generación Hamming" de códigos de error.

El nivel RAID 2 emplea múltiples discos, como en el nivel RAID 0, pero algunos de estos discos son empleados para códigos de error, los cuales los emplean para referencia de los datos en caso

de que falle uno de los discos. Este nivel tiene un costo bastante elevado, debido a que se necesita mucho disco para mantener los códigos de error.

Gracias a como están distribuidos los datos en los discos se consigue mejorar la velocidad de transferencia principalmente en la lectura, ya que podemos emplear todos los discos en paralelo.

Estos discos, aunque proporcionen un buen rendimiento, no son muy empleados, ya que los niveles 1,3 y 5 proporcionen una mayor relación costo/rendimiento.

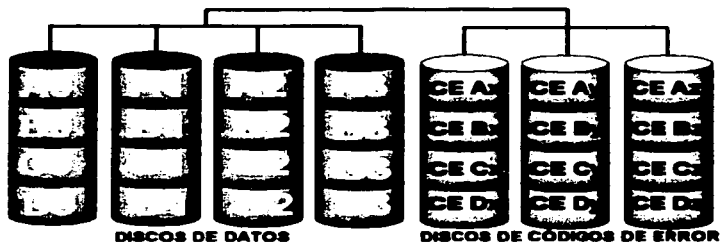


Figura C.3 - RAID 2

Ventajas RAID 2

- Se emplea para mejorar la velocidad de demanda y también la velocidad de transferencia.
- Podemos recuperar datos gracias a los discos de códigos de error.

Inconvenientes RAID 2

- Solución cara, ya que requeriremos mucho disco para guardar los códigos de error.
- Tiempo de escritura de datos bastante lento, incluso aunque los datos se separen en los diferentes discos.

RAID 3: Parallel Disk Array (PDA)

Sistema de discos en paralelo con disco de paridad para la corrección de errores.

RAID 3 emplea múltiples discos para hacer el striping, como en el nivel RAID 2, pero sólo hace falta un disco nada más para mantener la paridad por lo que se reduce el costo en discos.

Este nivel RAID es una buena alternativa para aplicaciones de velocidad de transferencia alta, ya que gracias a la distribución de datos podemos emplear todos los discos en paralelo.

TESIS CON
FALLA DE ORIGEN

Aplicaciones: Producción y distribución de video en streaming, Aplicaciones de imagen, video y prensa. Servidores de Base de Datos Mono-usuario.

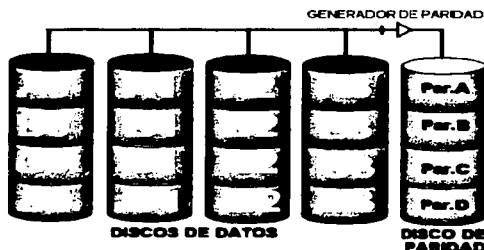


Figura C.4 - RAID 3

Ventajas RAID 3

- Alto rendimiento para aplicaciones de velocidad de transferencia alta, ya que ofrece una alta velocidad de transferencia para gráficos, imágenes y aplicaciones en general en las que necesitamos gran transferencia de datos.
- Gracias al disco de paridad, podemos recuperar datos.

Inconvenientes RAID 3

- Si perdemos el disco de paridad, perdemos toda la información redundante que teníamos.
- Tiempo de escritura de datos bastante lento.

RAID 4: Independent Disk Array (IDA)

Sistema de discos independientes con disco de control de errores

El nivel RAID 4 es más parecido al RAID 3. Los bloques de datos que distribuimos en los diferentes discos son más grandes por lo que se consigue un rendimiento superior en las escrituras.

Ventajas RAID 4

- Buen rendimiento en escritura de datos.
- Tiene integridad de datos.

Inconvenientes RAID 4

- Si perdemos el disco de paridad, perdemos toda la información redundante que teníamos.
- Menor rendimiento en las lecturas de datos.

TESIS CON
FALLA DE ORIGEN

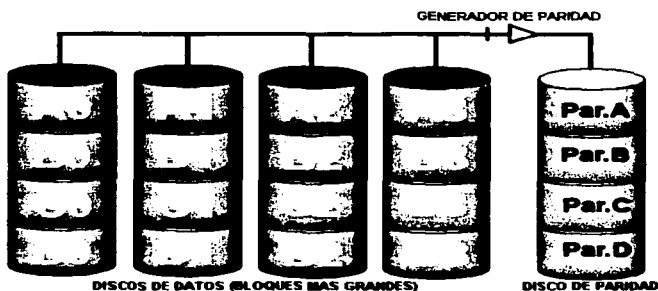


Figura C.5 - RAID 4

RAID 5: Independent Disk Array (IDA)

Sistema de discos independiente con integración de códigos de error mediante una paridad.

En RAID 5 los datos y la paridad son guardados en los mismos discos, por lo que se consigue aumentar la velocidad de demanda, ya que cada disco puede satisfacer una demanda independientemente de los demás. Con diferencia con el RAID 3, el RAID 5 guarda la paridad del dato dentro de los discos y no hace falta un disco para guardar dichas paridades. La paridad se genera haciendo un XOR de los datos A0,B0,C0,D0 creando la zona de paridad PAR0, como se ve la paridad nunca se guarda en los disco que contienen los datos que han generado dicha paridad, ya que en el caso que uno de ellos se estropeará como por ejemplo el dato A0 bastaría con regenerar las banda B0,C0,D0,PAR0 para que el dato volviera a establecerse.

Aplicaciones: Servidores de archivos y aplicaciones, Servidores de Base de Datos, Servidores www, correo, noticias, Servidores de Intranet.

Ventajas RAID 5

- Alto rendimiento en aplicaciones de velocidad de demanda interactivas. Ofrece una alta velocidad de demandas, tanto en escrituras como en lecturas
- Costo efectivo. No desaprovecha un disco exclusivamente para paridad.
- Se pueden recuperar datos.

Inconvenientes RAID 5

- El rendimiento en las escrituras de datos es bajo.
- No aumenta el rendimiento en las aplicaciones, aunque la velocidad de transferencia de datos es alta.

TESIS CON
FALLA DE ORIGEN

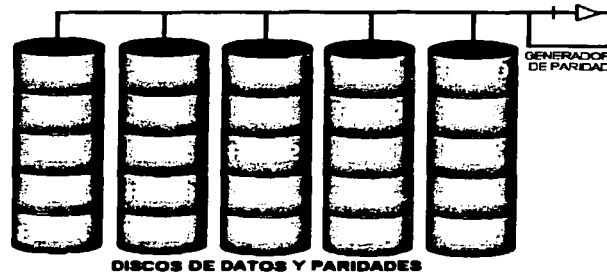


Figura C.6 - RAID 5

RAID 6: Independent Disk Array (IDA)

Sistema independiente de disco con integración de códigos de error mediante una doble paridad. RAID 6 es esencialmente una extensión del nivel RAID 5, para ello guarda una segunda paridad. Este nivel proporciona muy buena integridad de los datos y repara diversos errores en los discos.

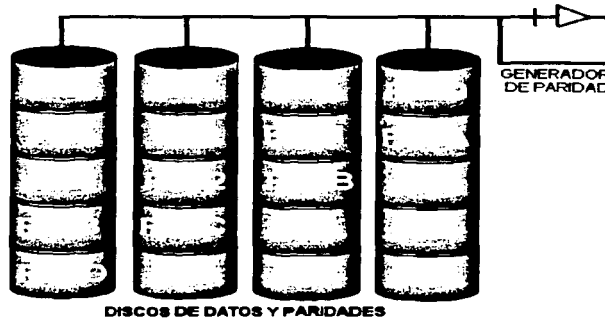


Figura C.7 - RAID 6

Ventajas RAID 6

- Podemos recuperar diversos errores simultáneamente.
- Nivel de integridad muy elevado. Solución perfecta para aplicaciones críticas.

Inconvenientes RAID 6

- El rendimiento en escrituras de datos es bastante lento.
- No se dispone de muchas implementaciones comerciales del nivel RAID 6.

TESIS CON
FALLA DE ORIGEN

RAID 7

El RAID 7, este tipo incluye un sistema operativo incrustado de tiempo real como controlador, haciendo las operaciones de caché a través de un bus de alta velocidad y otras características de un ordenador sencillo. Todas las transferencias son asíncronas. Y las E/S están centralizadas por la caché. Se necesita un disco de paridad exclusivo. El agente SNMP permite su administración remota. Un vendedor ofrece este sistema.

Aplicaciones: Sistemas de Tiempo Real (Industriales).

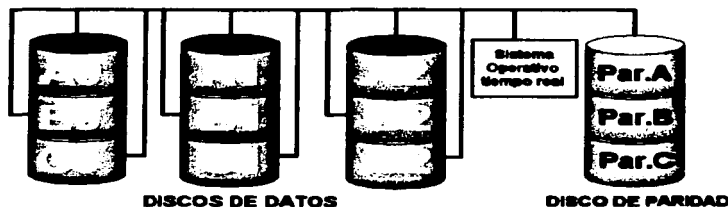


Figura C.8 - RAID 7

RAID 1 + RAID 0: Mirroring + Striping

La combinación de espejeo más striping ofrece los beneficios de distribuir los datos a través de múltiples discos (striping) mientras provee redundancia (mirroring) de los datos.

Si un disco llega a fallar se pierde redundancia entera, cuando se reemplaza el disco se debe actualizar completamente tomando una cantidad de tiempo sustancial.

Aplicaciones: Servidores de Bases de Datos con alto rendimiento y tolerancia a fallos.

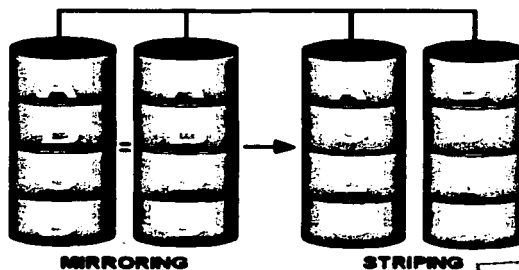


Figura C.9 - RAID 1 + RAID 0

TESIS CON FALLA DE ORIGEN

RAID 0 + RAID 1: Striping + Mirroring

Consiste en la duplicación de los datos en diferentes conjuntos de discos, para un posterior striping dentro de cada uno de dichos conjuntos. Este nivel está indicado para aplicaciones que necesiten altas prestaciones y un alto nivel de seguridad. Para Aplicaciones de Imagen y Servidores de archivos generales

Si algún disco llega a fallar solo una parte pierde redundancia y cuando el disco es reemplazado solo una parte necesita recuperarse.

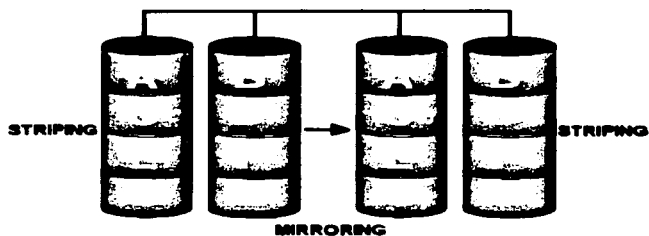


Figura C.10 - RAID 0 + RAID 1

TESIS CON
FALLA DE ORIGEN

GLOSARIO

GLOSARIO

Base de datos: nombre con el que se conoce aun conjunto de datos informáticos relacionados entre sí, que están almacenados de forma que son recuperables fácilmente, con la posibilidad de relacionarlos, ordenarlos, según criterios, etc.

Boot: acción de arrancar la computadora

Cracker: palabra inglesa que significa "intruso". Se trata de un individuo que intenta penetrar en una computadora o sistema informático ilegalmente con intenciones perversas (robar información, borrarla, etc.).

Demonio: proceso que administra tareas particulares del sistema y que corre en background.

Disco spare: véase Hot spare.

TESIS CON
FALLA DE ORIGEN

DNS (Domain Name server): se trata de una base de datos distribuida que gestiona todo lo referente a la conversión de nombres de dominio en formato alfanumérico al sistema real de direcciones de Internet, direcciones IP.

Eudora: se trata del nombre de uno de los programas mas reconocidos y usados para la gestión de correo electrónico, su autor es la empresa Qual Comm.

FTP (File Transfer protocol): protocolo de comunicación mediante el cual es posible enviar y recibir archivos de una computadora a otra a través de la red.

FTP Anónimo: servidor FTP que permite ser accedido por cualquier usuario sin necesidad de logins y passwords secretos, es accesible, libre y gratuito.

GNU: nombre con el que se conoce a toda aplicación compatible con UNIX que es totalmente gratuita. Proyecto iniciado por Richard Stallman en 1983 en el Instituto de Tecnología en Massachusets.

Gopher: consiste en un sistema de búsqueda de documentos y archivos localizados en Internet mediante menús jerárquicos. El usuarios necesita un programa de tipo "gopher" que accede a la información de cualquier gopher accesible y la suministra de forma unificada. este servicio esta actualmente en desuso.

TESIS CON
FALLA DE ORIGEN

GLOSARIO

HTML (Hypertext Markup Languaje): "lenguaje de programación" utilizado en WWW para crear paginas web con información en formato hipertexto.

HTTP (Hypertext Transport Protocol): protocolo usado para transferir archivos o documentos en la WWW.

Hacker: nombre con el que se conoce a los grandes expertos en informática, redes, programación e Internet en particular. Es un personaje benigno que intenta acceder a lugares prohibidos por simple diversión.

Hot swap: Son discos que se reemplazan en caliente. Esto quiere decir que si alguno de los discos RAID se estropeará físicamente bastaría con quitarlo y poner otro sin tener que apagar el sistema.

Hot spare: Disco sobrante. Es un disco que permanece siempre en el sistema esperando a que uno se estropee y él entre directamente en funcionamiento.

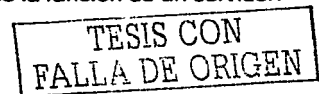
Integridad de los datos: es la capacidad que tiene un disco de aguantar un error de grabación, de corrupción o pérdida de datos. Para tal efecto se tiene que seleccionar un disco RAID o una alternativa. El nivel de integridad es uno de los primeros criterios que se han de investigar.

Internet: nombre con el que se conoce a una agrupación de redes informáticas interconectadas de todo el mundo que permiten la comunicación entre millones de usuarios de todo el planeta. La intención original de su creación fue la de conectar las universidades y centros de investigación de todo el mundo, aunque se ha convertido en el principal medio de comunicación de usuarios, empresas y todo tipo de organizaciones.

Memoria cache: memoria donde se puede almacenar datos de manera temporal, para evitar el acceso al disco duro (el cual es algo lento).

Memoria swap: parte reservada del disco que el kernel usa durante el procesamiento de forma temporal.

Mirror site (sitio mirror): computadora que contiene una replica exacta o "espejo" del contenido almacenado en las unidades de disco de otra computadora que hace la función de un servidor.



GLOSARIO

Navegador de Internet: programa para visualizar la información contenida de forma de paginas web en los campos de todo el mundo conectados a Internet.

Paridad: es una información redundante que es guardada para regenerar datos perdidos por un error en el disco. La paridad se genera haciendo un XOR sobre los datos de los discos y guardandolo en otro disco o en un disco dedicado a este efecto, esto dependerá del nivel RAID que usemos.

Plataforma: término de carácter genérico que designa normalmente una arquitectura de hardware, aunque también se usa a veces para sistemas operativos o para el conjunto de ambos.

Reconstrucción o regeneración: Cuando un disco falla la información redundante en los discos y los datos en los discos buenos son usados para regenerar la información del disco averiado.

Redundat Power Supplies: Fuente de alimentación redundante. El sistema consta de dos fuentes de alimentación. Si una se estropea, se pone en marcha la otra, pudiendose cambiar la estropeada en caliente.

Servidor: Genéricamente, dispositivo de un sistema que resuelve las peticiones de otros elementos del sistema, denominados clientes. Computadora que suministra servicios a los usuarios de la red, el servidor recibe solicitudes para los diferentes servicios y administra las solicitudes para que sean atendidas de una forma ordenada y en secuencia.

Servidor

Spam: palabra inglesa que se usa para indicar el hecho de recibir gran cantidad de mensajes propagandísticos vía correo electrónico.

Striping: es el acto de unir dos o más discos físicos en un solo disco lógico con el fin de dividir los datos entre los diferentes discos para ofrecer una significativa mejora en el rendimiento del conjunto de los discos.

Telnet: protocolo de comunicaciones estándar que permite conectar una computadora con Internet convirtiéndolo en una terminal del sistema.

WWW (Wold Wide Web): nombre del sistema de documentos de la Internet que junto con el correo electrónico es uno de los servicios mas usados de la red Internet.

TESIS CON
FALLA DE ORIGEN

BIBLIOGRAFÍA

BIBLIOGRAFÍA

- ◆ **Garfinkel Simson**, *Seguridad Práctica en UNIX e Internet*, O'Reilly, México, 1999.
- ◆ **Garfinkel Simson**, **Spafford Gene**. *Web Security, Privacy & Commerce*, 2nd Edition.
- ◆ **Icove David**, **Seger Karl**, **VonStorch William** **Computer Crime**, *A Crimefighter's Handbook*.
- ◆ **Zwicky Elizabeth D.**, **Cooper Simon**, **Chapman D. Brent**, *Building Internet Firewalls*, 2nd Edition.
- ◆ **Frish Eleen**, *Essential System Administration*, O'Reilly, USA 1995
- ◆ **McClure Stuart**, **Scambray Joel**, **Kurtz George**, *Hacking Exposed: Network Security Secrets & Solutions*, Third Edition.
- ◆ **Tim Parker**, *Linux System Administrator's Survival Guide*, Grupo SAMS, 1995.
- ◆ **Peek Jerry**, **O'Reilly Tim**, **Loukides Mike** *UNIX Power Tools*, O'Reilly. 2nd Edition.
- ◆ **By Daniel Gilly & the Staff of O'Reilly & Associates**. *UNIX in a Nutshell: System V Edition*. O'Reilly. Second Edition, June 1992
- ◆ **By Jerry Peek, Grace Todino & John Strang**. *Learning the UNIX Operating System*. O'Reilly. Fourth Edition, January 1998.
- ◆ **Stan Kelly-Bootle**, *Cómo usar UNIX Sistema V versión 4.0*, Limusa, México, 1993.
- ◆ Sun educational services. *Fundamentals of Solaris 7 and System Admin.*
- ◆ Sun educational services. *SUN StorEdge Volume Manager Administration*.
- ◆ *Solaris 8 (SPARC Platform Edition). Installation Guide*
- ◆ *Solstice DiskSuite 4.2 Reference Guide*
- ◆ *Solstice DiskSuite 4.2 User's Guide*
- ◆ *System Administration Guide, Volume 1,2,3*
- ◆ http://enete.us.es/docu_enete/nt4/tiposderaid.asp
- ◆ <http://sindominio.net/~apm/raid>
- ◆ http://sageweb.sage.org/resources/publications/code_of_ethics.html
- ◆ <http://www.acm.org/constitution/code.html>
- ◆ <http://docs.sun.com>
- ◆ <http://sunsolve.sun.com>

TESIS CON
FALLA DE ORIGEN