ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO

FACULTAD DE INFORMÁTICA Y ELECTRÓNICA

ESCUELA DE INGENIERÍA ELECTRÓNICA EN TELECOMUNICACIONES Y REDES

"ANÁLISIS COMPARATIVO DE SERVIDORES DE AUTENTIFICACIÓN RADIUS Y LDAP CON EL USO DE CERTIFICADOS DIGITALES PARA MEJORAR LA SEGURIDAD EN EL CONTROL DE ACCESO A REDES WIFI"

TESIS DE GRADO

Previa a la obtención del título de

INGENIERO EN ELECTRÓNICA TELECOMUNICACIONES Y REDES

Presentado por:

GLADIS SOFÍA ASADOVAY LEMA

LILIANA MERCEDES CAIZA ORTIZ

RIOBAMBA – ECUADOR
2013

AGRADECIMIENTO

En primer lugar quiero agradecer a Dios, por guiar mi camino y permitirme culminar con éxito mi carrera profesional.

A mis padres, por haberme apoyado incondicionalmente y por la motivación constante que me ha permitido cumplir con mis metas.

A mis amigos Liliana, Mónica y Cristian, con los cuales he compartido los mejores y peores momentos de mi vida y por hacer de la vida estudiantil una tarea más llevadera y alegre.

A los docentes de la Escuela de Ingeniería Electrónica por haber depositado en mí todos sus conocimientos. En especial al Ing. Danilo Pástor por su apoyo incondicional y desinteresado en el desarrollo de esta tesis, sin su ayuda no hubiese sido posible la culminación de la misma.

Sofía

Agradezco a DIOS, por haberme dado el regalo de la vida y permitirme culminar mis estudios.

A mis padres y hermanos, por brindarme su amor y apoyo incondicional día a día y por enseñarme a plantearme nuevos objetivos y luchar por alcanzarlos, también por la felicidad que le han dado siempre a mi vida.

A todos mis amigos, en especial a Sofía, Mónica y Cristian por su apoyo y cariño durante todo este tiempo, por compartir sus conocimientos conmigo y por permitirme formar parte de sus vidas.

Al Ing. Danilo Pastor por su contribución y consejos que permitieron que este trabajo se realice.

Liliana

DEDICATORIA

Esta tesis va dedicada a Dios, por acompañarme y cuidarme en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.

A mi Padre Enrique por ser el pilar fundamental en todo lo que soy, en toda mi educación, tanto académica, como de la vida, por su incondicional apoyo ya que siempre ha estado presente brindándome su constante apoyo y confianza, gracias al gran esfuerzo que ha realizado para darme la educación que hoy me ha permitido llegar hasta aquí y culminar con éxito mis estudios.

Sofía

A Dios.

Por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.

A mi madre Carmen.

Por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor, porque desde el cielo sigue guiando mi camino y cuidando de mí.

A mi padre Feliciano.

Por los ejemplos de perseverancia y constancia que lo caracterizan y que me ha infundado siempre, por el valor mostrado para salir adelante y por su amor, a él le debo lo que soy.

Liliana

FIRMAS RESPONSABLES Y NOTA

NOMBRE	**FIRMA**	**FECHA**
Ing. Iván Menes **DECANO FACULTAD** **INFORMÁTICA Y ELECTRÓNICA**	……	…..……
Ing. Wilson Baldeón **DIR. ESC. ING. ELECTRÓNICA EN** **TELECOMUNICACIONES Y REDES**	……	…..……
Ing. Danilo Pástor **DIRECTOR DE TESIS**	……	…..……
Ing. Wilson Baldeón **MIEMBRO DEL TRIBUNAL**	……	…..……
Tlgo. Carlos Rodríguez **DIRECTOR CENTRO DE** **DOCUMENTACIÓN**	……	…..……

NOTA DE LA TESIS: ……

RESPONSABILIDAD DEL AUTOR

"Nosotras, Gladis Sofía Asadovay Lema y Liliana Mercedes Caiza Ortiz, somos las responsables de las ideas, doctrinas y resultados expuestos en esta Tesis, y el patrimonio intelectual de la misma pertenecen a la ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO".

---------- ----------

Gladis Sofía Asadovay Lema Liliana Mercedes Caiza Ortiz

ÍNDICE DE ABREVIATURAS

ANSI	American National Standards Institute, Instituto Nacional Estadounidense deEstándares
AP	Access Point, Punto de Acceso
AES	Advanced Encryption Standard
AAA	Autentificación, Autorización y Contabilidad
ATA	Advanced Technology Attachment, Tecnología Avanzada de Contacto
BD	Base de Datos
BSD	Berkeley Software Distribution, Distribución de Software Berkeley
CPU	Central Processing Unit, Unidad Central de Procesos
CA	Certificate Authority, Autoridad Certificadora
CN	Common Name, Nombre Común
CRC	Algoritmo de Chequeo de Integridad
CHAP	Challenge Handshake Authentication Protocol, Protocolo de Autentificación por Desafío Mutuo
CRL	Lista de Certificados Revocados
DES	Data Encryption Standard, Cifrado Estadarizado de Datos
DSL	Digital Subscriber Line, Línea de Abonado Digital
DNS	Domain Name Service, Servicio de Nombres de Dominio
DHCP	Dinamic Host Configuration Protocol
DN	Domain Name, Nombre de Dominio
ESPOCH	Escuela Superior Politécnica de Chimborazo
EAP	Protocolo de autentificación extensible
EAP-TLS	EAP Transport Level Security
EAPOL	EAP OverLan
E/S	Entrada/Salida
Eduroam	EDUcation ROAMing
GPL	General Public License, Licencia Pública General

HTTP	Hipertext Transfer Protocol, Protocolo de Transferencia de Hipertexto
Hi	Hipótesis de Investigación
IEEE	Institute of Electricaland Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos
IDEA	International Data Encription Algorithm
ITU-T	International Telecommunications Union, Unión internacional de telecomunicaciones
IETF	Fuerza de Trabajo de la Ingeniería del Internet
IP	Protocolo de Internet
ISP	Internet Service Provider, Proveedor de servicios de Internet
IMAP	Internet Message Access Protocol, Protocolos de internet para la recepción de mails
IAS	Servicio de autentificación de Internet
LDAP	Lightweight Directory Access Protocol, Protocolo Ligero de Acceso a Directorios
LAN	Local Area Network, Red de Área Local
LDIF	LDAP Data Interchange Format, Formato de Intercambio de Datos de LDAP
L2TP	Layer 2 Tunneling Protocol, El Protocolo de túnel de capa 2
MySQL	My Structured Query Language, Mi Lenguaje de Consulta Estructurada.
MD5	Message-Digest Algorithm 5
MAC	Control Access Media, Control de Acceso al Medio
MB	Mega Bytes
NAS	Network Access Server, Servidor de Acceso a la Red
NNTP	Network News Transfer Protocol, Protocolo de Transferimiento de noticias de red
NPS	Servidor de directivas de red
OSI	Open Systems Interconnection, Interconexión de Sistemas Abiertos
PGP	Pretty Good Privacy
PPP	Pointo to Point Protocol
POP3	Post Office Protocol, Protocolo de Oficina de Correos

PAP	Password Authentication Protocol, Protocolo de Autentificación por Password
PAM	Pluggable Authentication Service
PEAP	Protocolo de autentificación Extensible Protegido
RADIUS	Remote Authentication Dial-In User Service
RC5	Rivest Cypher 5
RSA	Rivest Shamir Adleman
RFI	Request For Information
RFC	Request for Comment
RAM	Random Access Memory, Memoria de Acceso Aleatorio
SO	Sistema Operativo
SW	Software
SSL	Secure Socket Layer, Nivel de Zócalo Seguro
SHA	Secure Hash Algorithm
SSID	Service Set IDentifier
SMTP	Simple Mail Transfer Protocol, Protocolo Simple de Transmisión de Correo
SSH	Secure Shell, Intérprete de Órdenes Segura
TLS	Transport Layer Security, Seguridad para Nivel de Transporte
TKIP	Protocolo de integridad de clave temporal
TACACS	Protocolo de Autentificación Remota propietario de CISCO
TCP	Transmission Control Protocol, Protocolo de Control de Transmisión
UID	Identificador de Usuario
UDP	Protocolo de Datagramas de Usuario
VPN	Virtual Private Network
VLAN	Virtual Local Area Network, Red de área Local Virtual
Wifi	Wireless Fidelity, Fidelidad Inalámbrica
WEP	Wired Equivalent Privacy, Privacidad Equivalente a Cableado
WPA	Wi-Fi Protected Access, Acceso Protegido Wi-Fi
WLAN	Wireless Local Areanetwork, Red de Área Local Inalámbrica

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo de investigación de tesis previo a la obtención del título de Ingeniería en Electrónica, Telecomunicaciones y Redes, trata de el "ANÁLISIS COMPARATIVO DE SERVIDORES DE AUTENTIFICACIÓN RADIUS Y LDAP CON EL USO DE CERTIFICADOS DIGITALES PARA MEJORAR LA SEGURIDAD EN EL CONTROL DE ACCESO A REDES WIFI"

Es un estudio comparativo de las principales características que presentan los servidores de autentificación RADIUS y LDAP para obtener como resultado el servidor más eficiente y que mejor se adapte a una red inalámbrica en general aportando un mayor grado de seguridad a los usuarios.

Anteriormente al implementar un servidor de autentificación, la gran mayoría de administradores de red no tomaban en cuenta las ventajas y desventajas que este ofrecía, además de su desempeño y rendimiento. Ya que solo les importaba un sistema que sea fácil e intuitivo de administrar, lo cual generalmente se lograba con aplicaciones de software comercial como los que proporciona Windows.

En la actualidad, antes de implementar un sistema de este tipo, se realiza un análisis profundo de los requerimientos que tiene la red, tomando en cuenta la tendencia de utilizar software libre que se ha venido desarrollando en los últimos años y un parámetro indispensable con el que todo sistema debe cumplir antes de ser implementado es ofrecer un buen nivel de seguridad, motivo por el cual se añade a este estudio la creación y administración de certificados digitales en el proceso de autentificación.

El presente trabajo contiene los siguientes capítulos:

En el capítulo I se presenta el planteamiento de la investigación, antecedentes, objetivos, hipótesis, el cual constituye el marco referencial para el desarrollo de la tesis.

En al capítulo II se describe los conceptos teóricos y demás terminología necesarios para la comprensión y desarrollo del objetivo de estudio.

En el capítulo III se realiza el análisis comparativo de los servidores de autentificación en estudio, que son RADIUS y LDAP para determinar cuál es el más eficiente para ser implementado en una red inalámbrica. Además de haber determinado los indicadores e índices adecuados, los mismos que servirán para la comparación de los servidores y como resultado de esto se hace la comprobación o negación de la hipótesis.

En el Capítulo IV se muestra detalladamente la implementación del prototipo de servidor de autentificación que pueda ser adaptable a la mayoría de redes, lo que implica configuración del servidor, creación de la CA, creación de la red inalámbrica, instalación del certificado digital en el cliente, configuración del AP y finalmente la realización de una prueba de funcionamiento del servidor.

Para el proceso de autentificación se ingresara el nombre de usuario y clave compartida, que se asignó cuando fueron creados los certificados digitales para cada usuario.

CAPÍTULO I

MARCO REFERENCIAL

En este primer capítulo se describen los objetivos planteados en la tesis, además de una breve descripción los problemas que se presentan en la actualidad con las redes inalámbricas y las razones por las cuales se sustenta la investigación.

1.1. ANTECEDENTES

Durante los últimos años la evolución de las tecnologías de acceso inalámbrico, la facilidad de implementación y el bajo costo en relación a las redes cableadas ha impulsado el incremento en la demanda de redes inalámbricas por parte de los usuarios que requieren movilidad.

La seguridad siempre ha sido uno de los factores más delicados a tomar en cuenta al momento de diseñar un sistema de comunicaciones y más aún cuando se transmite información confidencial a través de él. Las redes Wifi son un caso muy particular porque

los datos viajan a través de un medio totalmente inseguro, lo que da origen a la necesidad de crear un sistema de seguridad específico para este tipo de tecnología.

En la actualidad la mayoría de redes Wifi no cuentan con un sistema de autentificación seguro que garantice que la información no pueda ser accedida ni mucho menos modificada por usuarios no autorizados, ya que cada vez aparecen herramientas de ataque mas sofisticadas es importante contar con un sistema de Seguridad capaz de minimizar amenazas a los recursos de la red por usuarios no autorizados.

Existe una variedad de sistemas de autentificación, basados tanto en software libre como privativo, entonces para la empresa la elección de un único método de autentificación se torna difícil, pues se debe optar por un protocolo y un método de acceso que cumpla con las políticas y necesidades definidas por dicha institución.

El mayor inconveniente para que las pequeñas y medianas empresas no puedan acceder a un sistema de autentificación seguro, es que se requiere de una inversión bastante alta que gran parte de usuarios o administradores no están dispuestos a asumir, pues no consideran indispensable contar con un sistema de este tipo.

Otro punto que las instituciones deben considerar muchas veces es como, además de proveer seguridad e integridad de la información, garantizar que el acceso al recurso inalámbrico sea controlado, es decir, que se pueda controlar quienes pueden hacer uso de un determinado recurso.

1.2. JUSTIFICACIÓN

Debido a las vulnerabilidades que se presentan en las Redes Inalámbricas y aparición de sofisticadas herramientas de ataque es importante contar con un sistema de Seguridad capaz de minimizar amenazas a los recursos de la red por usuarios no autorizados.

Con el planteamiento del proyecto se pretende elevar en mayor grado el nivel de seguridad de la red Wifi con el uso de encriptación en el intercambio de información a través de Certificados Digitales. Con esta alternativa tratamos de permitir el acceso únicamente a los usuarios que cuenten con un certificado digital previamente autorizado y registrado en el servidor de autentificación. El uso del protocolo WEP no es seguro debido a que facilita descifrar las claves, el uso de Certificados Digitales resuelve este problema proporcionando un sistema más robusto y seguro.

Aprovechando las potentes herramientas que nos ofrece el software libre, construiremos un sistema de autentificación lo suficientemente bueno y seguro como para que pueda ser adaptado a todo tipo de pequeña o mediana empresa y al no tener que pagar licencias por el software, se reduce sustancialmente la inversión convirtiéndose en una alternativa muy atractiva al momento de implementarla.

Con la implementación del Servidor de autentificación en la red inalámbrica de la Escuela de Ingeniería Electrónica en Telecomunicaciones y Redes se pretende incrementar los niveles de seguridad en el ingreso, al mismo tiempo que se quiere mantener un control más directo sobre los usuarios que se conecten a dicha red.

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Realizar un análisis comparativo entre los servidores de autentificación RADIUS y LDAP complementado con el uso de certificados digitales para mejorar la seguridad en el acceso a redes Wifi.

1.3.2. OBJETIVOS ESPECÍFICOS

- Estudiar conceptos relacionados con los Servidores de autentificación en redes Wifi para determinar las alternativas más apropiadas que soporten certificados digitales.
- Determinar los parámetros que permitan realizar el estudio comparativo entre RADIUS y LDAP.
- Realizar un escenario de pruebas que nos permita determinar cuantitativamente la mejor opción de servidor de autentificación.
- Seleccionar el servidor de autentificación más óptimo de acuerdo a los parámetros definidos, para implementar un prototipo que se adecue a cualquier tipo de red wifi.

1.4. HIPÓTESIS

La implementación de un servidor LDAP proporciona una mayor eficiencia en la autentificación de usuarios en una red inalámbrica frente a un Servidor Radius.

CAPITULO II

MARCO TEÓRICO

2.1. Introducción

En este capítulo, se realiza una revisión del proceso de Autentificación, Protocolos y Métodos utilizados en dicho proceso, conceptos relacionados con Criptografía e Intercambio de Llaves, se detalla también el uso de Certificados Digitales y Autoridad Certificadora.

2.2. Autentificación

El proceso de Autentificación en un sistema cualquiera tiene como objetivo probar la identidad de un proceso o usuario mediante la presentación de credenciales, puede realizarse de manera simple desde la presentación de datos como Usuario/Password hasta sistemas más robustos como la utilización de Firmas o Certificados Digitales.

Existen dos maneras de identificar a un individuo y dependen de si la información que se utiliza es intrínseca o extrínseca. La información **intrínseca** se basa en identificadores físicos del individuo: huellas digitales, patrones de la voz, patrones de la retina, etc.

Mientras que la información **extrínseca** se refiere a algo que el individuo conoce o es capaz de hacer: contraseñas, el número de la tarjeta de crédito, etc.

En una red inalámbrica 802.11, el proceso de autentificación facilita la tarea de control de acceso a los recursos de la red. Es necesario poder verificar de forma fiable la autenticidad de los distintos elementos que interactúan: la información que se intercambia, los usuarios que acceden y los dispositivos que intervienen, todo esto para garantizar la confidencialidad e integridad en la red.

La criptografía ofrece la posibilidad de realizar este proceso con garantías de seguridad, utilizando diferentes métodos y protocolos de intercambio de información protegida.

2.3. Criptografía

Consiste en cifrar o descifrar información digital utilizando técnicas matemáticas. Como se observa en la figura II.1. Se pretende ocultar la información contenida en un mensaje. Este proceso es totalmente transparente para el usuario, no incrementa el tamaño de los paquetes y solo puede ser desencriptado por quien tenga la clave para hacerlo.

Figura II.1 Cifrado y Descifrado de datos
Fuente: https://zonatic.usatudni.es/images/criptografia/criptografia_2.png

Los métodos de encriptación pueden dividirse en dos grandes grupos:

2.3.1. Criptografía de Clave Simétrica (Clave Secreta)

Tanto emisor como receptor utilizan una misma clave para la encriptación y desencriptación de la información transmitida a través del canal inseguro. Esta clave se debe intercambiar entre los equipos por medio de un canal seguro.

Para que un algoritmo de este tipo sea considerado fiable debe cumplir algunos requisitos básicos:

- Conocido el criptograma (texto cifrado) no se pueden obtener de él ni el texto en claro ni la clave.
- Conocidos el texto en claro y el texto cifrado debe resultar más caro en tiempo o dinero descifrar la clave que el valor posible de la información obtenida por terceros.

La seguridad en clave simétrica reside en la propia clave secreta, y por tanto el principal problema es la distribución de esta clave a los distintos usuarios para cifrar y descifrar la información. La misión del emisor y receptor es mantener la clave en secreto. La principal ventaja de los algoritmos simétricos es la velocidad de los algoritmos, y son muy usados para el cifrado de grandes cantidades de datos.

2.3.1.1. Algoritmos Simétricos

Todos los sistemas criptográficos clásicos se pueden considerar simétricos, y los principales algoritmos simétricos actuales son DES, IDEA y RC5.

- **DES**

Se basa en un sistema mono alfabético, con un algoritmo de cifrado consistente en la aplicación sucesiva de varias permutaciones y sustituciones.

Inicialmente el texto a cifrar se somete a una permutación, con bloque de entrada de 64 bits (o múltiplo de 64), para posteriormente ser sometido a la acción de dos funciones principales, una función de permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits, en un proceso que consta de 16 etapas de cifrado.

En general, DES utiliza una clave simétrica de 64 bits, de los cuales 56 son usados para la encriptación, mientras que los 8 restantes son de paridad, y se usan para la detección de errores en el proceso.

Ventajas:

- Es uno de los sistemas más empleados y extendidos, por tanto es de los más probados.
- Implementación sencilla y rápida.

Desventajas:

- No se permite una clave de longitud variable, es decir, no se puede aumentar para tener una mayor seguridad.
- Es vulnerable al criptoanálisis diferencial (2^{47} posibilidades) siempre que se conozco un número suficiente de textos en claro y cifrados.
- La longitud de clave de 56 bits es demasiado corta, y por tanto vulnerable. Actualmente DES ya no es un estándar, debido a que en 1999 fue roto por un ordenador.

Actualmente se utiliza el Triple DES **3DES** con una clave de 128 bits y que es compatible con el DES visto anteriormente. Este nuevo algoritmo toma una clave de 128 bits y la divide en dos de 64 bits cada una, de la siguiente forma:

- Al documento a cifrar se le aplica un primer cifrado mediante la primera clave, C1.

- Al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2.
- Y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave, C1.

- **RC5**

Se aplican operaciones XOR sobre los datos, pudiendo ser de 32, 64 o 128 bits. Permite diferentes longitudes de clave, y un número variable de iteraciones (la seguridad del cifrado aumenta exponencialmente cuanto mayor número de iteraciones), también funciona como un generador de número aleatorios, sumándoles a los bloques de texto rotados mediante la XOR.

- **IDEA (International Data Encriptión Algorithm)**

Trabaja con bloques de texto de 64 bits, operando siempre con números de 16 bits usando operaciones como XOR y suma y multiplicación de enteros. El algoritmo de desencriptación es muy parecido al de encriptación, por lo que resulta muy fácil y rápido de programar, y hasta ahora no ha sido roto nunca, aportando su longitud de clave una seguridad fuerte ante los ataques por fuerza bruta (prueba y ensayo o diccionarios).

Este algoritmo es de libre difusión y no está sometido a ningún tipo de restricciones o permisos nacionales, por lo que se ha difundido ampliamente, utilizándose en sistemas como UNIX y en programas de cifrado de correo como PGP.

- **AES (Advanced Encryption Standard)**

Este cifrado puede implementar tanto en sistemas hardware como en software. El sistema criptográfico AES opera con bloques y claves de longitudes variable, hay AES de 128 bits, de 192 bits y de 256 bits. El resultado intermedio del cifrado constituye una matriz de bytes de cuatro filas por cuatro columnas. A esta matriz se le vuelve a aplicar una serie de

bucles de cifrado basado en operaciones matemáticas (sustituciones no lineales de bytes, desplazamiento de filas de la matriz, combinaciones de las columnas mediante multiplicaciones lógicas y sumas XOR en base a claves intermedias).

Otra preocupación es la estructura de AES. A diferencia de la mayoría de cifradores de bloques, AES tiene una descripción matemática muy ordenada, es usado en los cifrados wireless de los routers de los hogares como método de cifrado (no clave) ya que en los routers podemos usar una clave estática o una dinámica mediante un servidor Radius.

2.3.2. Criptografía de clave asimétrica

La criptografía de clave asimétrica también es conocida como cable pública, emplea dos llaves diferentes en cada uno de los extremos de la comunicación. Cada usuario tendrá una clave pública y otra privada. La clave privada tendrá que ser protegida y guardada por el propio usuario, será secreta y no la deberá conocer nadie. La clave pública será accesible a todos los usuarios del sistema de comunicación.

Los algoritmos asimétricos están basados en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas realizarlo en sentido inverso a menos que se conozca la llave.

Las claves públicas y privadas se generan simultáneamente y están ligadas la una a la otra. Esta relación debe ser muy compleja para que resulte muy difícil que obtengamos una a partir de la otra. Si se tiene una pareja de claves para cifrar un mensaje con la llave privada, ese mensaje sólo podrá ser descifrado con la llave pública asociada. Y si se cifra con la pública, se descifra con la privada. Si ciframos un mensaje con la clave privada, no podremos descifrarlo con la propia llave privada, deberemos usar la pública.

La criptografía asimétrica proporciona autenticidad, integridad y no repudio. La ventaja del cifrado asimétrico sobre el simétrico radica en que la clave pública puede ser conocida por todo el mundo (no así la privada), sin embargo en el cifrado simétrico deben conocer la misma clave los dos usuarios (y la clave debe hacerse llegar a cada uno de los distintos usuarios por el canal de comunicación).

2.3.2.1. Algoritmos Asimétricos

Los principales algoritmos de cifrado de clave asimétrica son:

- **Diffie-Hellman**

No es un algoritmo simétrico propiamente dicho, se usa para generar una clave privada simétrica a ambos extremos de un canal de comunicación inseguro. Se emplea para obtener la clave secreta con la que posteriormente cifrar la información, junto con un algoritmo de cifrado simétrico. Es muy usado en los diferentes sistemas seguros implementados en Internet, por ejemplo: SSL y VPN.

Su seguridad radica en la dificultad de calcular el logaritmo discreto de números grandes. El problema de este algoritmo es que no proporciona autentificación, no puede validar la identidad de los usuarios, por tanto si un tercer usuario se pone en medio de la "conversación" también se le facilitaría las claves y por tanto podría establecer comunicaciones con el emisor y el receptor suplantando las identidades.

- **RSA**

La seguridad de este algoritmo radica en el problema de la factorización de números enteros.

Ventajas:

- Resuelve el problema de la distribución de las llaves simétricas (cifrado simétrico).
- Se puede emplear para ser utilizado en firmas digitales.

Desventajas:

- La seguridad depende de la eficiencia de los ordenadores.
- Es más lento que los algoritmos de clave simétrica.
- La clave privada debe ser cifrada por algún algoritmo simétrico.

2.4. Algoritmos de Autentificación HASH

Una función hash es método para generar claves o llaves que representen de manera casi unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original. El contenido es ilegible. Es posible que existan huellas digitales iguales para objetos diferentes, porque una función hash, en el caso del SHA-1 tiene 160bits, y los posibles objetos a resumir no tienen un tamaño límite.

A partir de un hash o huella digital, no se puede recuperar el conjunto de datos originales. Los más conocidos son el MD5 y el SHA-1. Cifrar una huella digital se conoce como firma digital.

- **MD5**

Es una función hash de 128 bits. Como todas las funciones hash, toma unos determinados tamaños a la entrada, y salen con una longitud fija (128 bits). El algoritmo MD5 no sirve para cifrar un mensaje. La información original no se puede recuperar ya que hay pérdida de datos.

- **SHA-1**

Es parecido a MD5, pero tiene un bloque de 160 bits en lugar de los 128 bits del MD5. La función de compresión es más compleja que la función de MD5. SHA-1 es más lento que MD5 porque el número de pasos son de 80 (64 en MD5) y porque tiene mayor longitud que MD5 (160 bits contra 128 bits). Lo que convierte a SHA-1 más robusto y seguro, totalmente apto para VPN's por ejemplo.

- **SHA-2**

Las principales diferencias con SHA-1 radica en el diseño y que los rangos de salida han sido incrementados y podemos encontrar: SHA-224, SHA-256, SHA-384, y SHA-512. Como ocurre con todos los cifrados y hash, cuanto más seguro, más lento su procesamiento y uso, debemos encontrar un equilibrio entre seguridad y velocidad.

Como ocurre con todos los cifrados y hash, cuanto más seguro, más lento su procesamiento y uso, se debe encontrar un equilibrio entre seguridad y velocidad.

2.5. Autentificación y no repudio: Certificados Digitales

Una firma digital es creada después de pasar el texto de un mensaje a través de un algoritmo de "hashing". Esto genera un mensaje comprimido. Este mensaje comprimido es luego encriptado empleando la Clave Privada del individuo que está generando el mensaje, transformándolo en una firma digital. La firma digital sólo puede ser desencriptada empleando la Clave Pública del mismo usuario.

El receptor del mensaje desencripta la firma digital y recalcula el mensaje comprimido. El valor calculado de este nuevo mensaje comprimido se compara con el valor del mensaje comprimido hallado en la firma. Si los dos cálculos son iguales, significa que el mensaje no ha sido alterado. Desde el momento en que la Clave Pública del emisor fue usada para verificar la firma, el texto tiene que haber sido firmado con la Clave Privada, conocida

exclusivamente por el emisor. Este proceso de autentificación es implementado en toda aplicación que requiere seguridad en las comunicaciones.

2.5.1. Certificado Digital

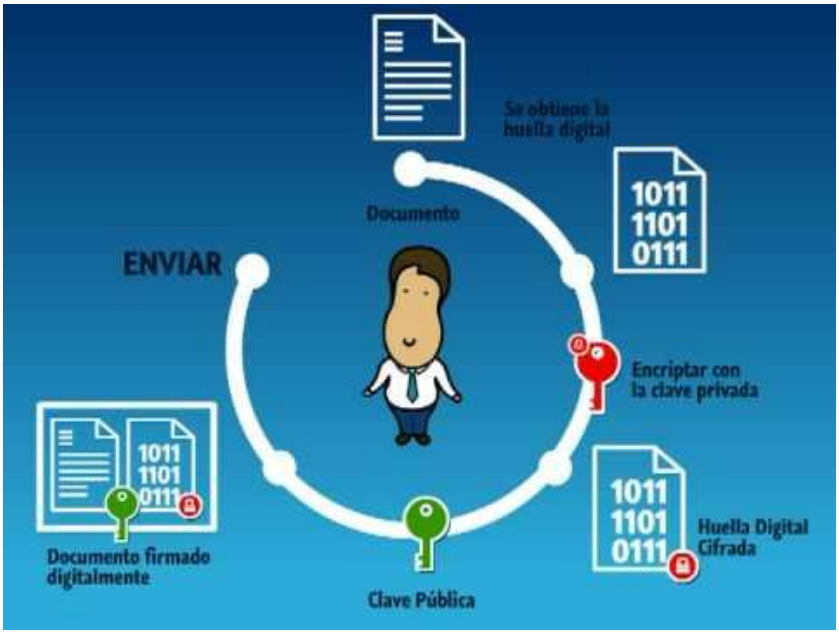


Figura II.2 Encriptación y Desencriptación con Certificado Digital
Fuente: http://2.bp.blogspot.com/-Cy1ITa1Cc4A/TsPMucdf8XI/s1600/Firma_Digital.png

Un certificado es un conjunto de credenciales de autentificación cifradas. Los certificados se autentican mediante una clave pública que comprueba la firma digital incluida. Los certificados pueden residir en el almacén de certificados del equipo o en una tarjeta inteligente. Una de las principales utilidades de los certificados consiste en proporcionar a los servidores una capa criptográfica para evitar la circulación de información en claro por la red, particularmente cuando se intercambian datos importantes

Las tres partes más importantes de un certificado digital son:

- Una clave pública
- La identidad del implicado: nombre y datos generales

- La firma privada de una tercera entidad llamada autoridad certificadora que todos reconocen como tal y que válida la asociación de la clave pública en cuestión con el tipo que dice ser.

En la actualidad casi todas las aplicaciones de comercio electrónico y transacciones seguras requieren un certificado digital, se ha propagado tanto su uso que se tiene ya un formato estándar de certificado digital, este es conocido como X509 v. 3. Un certificado digital entonces se reduce a un archivo de uno o dos k de tamaño, que autentica a un usuario de la red.

2.5.2. Formato de Certificado Digital

Existen diversos formatos de certificados, pero el más extendido es el X.509, definido por la norma del ITU-T X.509 (versión 3).

Un certificado X.509 normalmente es un fichero pequeño que contiene la siguiente información:

- **Nombre Distintivo del propietario**

  Se puede proporcionar la siguiente información:

  Nombre Común (CN), el nombre a ser certificado.

  Organización o Compañía (O), el nombre asociado con la organización

  Ciudad/Localidad (L) Ciudad donde está localizado el CN.

  Estado/Provincia (SP) Provincia donde está localizado el CN.

  País (C), el país donde está localizado CN.

- Nombre Distintivo de la Autoridad Certificadora. Identificación y firma de la Autoridad Certificadora (CA) que firmó el certificado.
- El período de tiempo de vigencia del certificado
- Información adicional sobre la CA, números de serie o versión.

2.5.3. Extensiones de certificados

Los certificados digitales se pueden almacenar en distintos formatos a cada uno de los cuales se le suele asignar una extensión al nombre del fichero. Algunos ficheros pueden incluir simultáneamente las llaves pública y privada y también podemos mantenerlas en ficheros separados.

- **Llave privada**

Se puede almacenar en un fichero independiente y la extensión suele ser .key o .pem. La llave privada debe mantenerse segura, mejor, protegida por contraseña. La posesión de la llave privada implica la posesión de la identidad, además partiendo de la llave privada se pueden generar la llaves públicas asociadas, más adelante se describe cómo.

- **Solicitud de certificado**

Una solicitud de certificado es, básicamente, una llave pública asociada a una llave privada que contiene una identidad. Una solicitud de certificado, una vez firmada se convierte en un certificado. Las extensiones que se utilizan para los ficheros de solicitud de certificados son .req o .pem.

- **Certificados**

Es la llave pública firmada por una autoridad. Puede tener distintos formatos, por ejemplo, los ficheros pueden ser binarios para los ficheros DER (.der), o en formato texto como los

PEM (.pem). Los ficheros de texto pueden incluir una serie de textos informativos. El formato PKCS12 es binario, contiene las llaves pública y privada.

2.6. Autoridad Certificadora CA

Una Autoridad Certificadora (CA, Certificate Authority) es la autoridad encargada de firmar los certificados y posteriormente confirmar que el dueño de un certificado es realmente quien dice ser.

Para la firma de certificados, una Autoridad Certificadora puede establecer una política que especifique qué campos del Nombres *Distintivo* es necesario incluir y cuáles son opcionales, o qué valores de los campos son o no admisibles.

Una Autoridad Certificadora puede certificar las identidades de otras Autoridades Certificadoras y así sucesivamente. Este proceso se detiene en el momento en que una Autoridad no tenga quién la certifique, en este caso, el certificado lo tiene que firmar ella misma (``self-signed'') y se trata del Certificado de raíz.

2.6.1. Confianza en un certificado

Una vez que la autoridad certificadora firma el certificado como se observa en la Figura II.3, le otorga su confianza. Se puede tener certificados digitales auto creados y auto firmados sin tener que pagar a una empresa por el servicio, pero en este caso, cada vez que se utilice el certificado el sistema no reconoce a la autoridad certificadora, sin embargo el certificado debe ser instalado y la comunicación sigue siendo segura debido a que existe cifrado de la información.

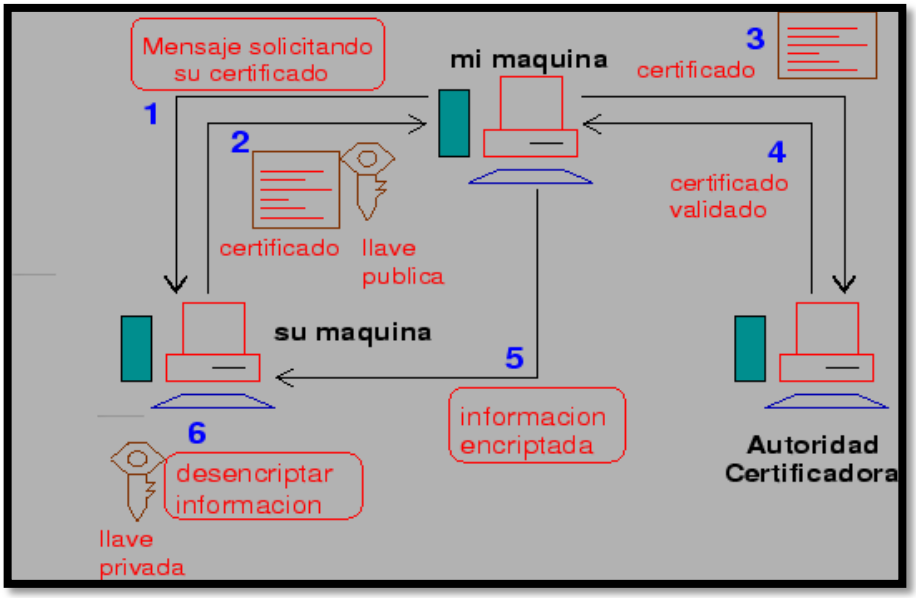


Figura II.3 Firma del Certificado Digital
Fuente: http://2.bp.blogspot.com/s1600/certificados+electronicos.jpg

Si el certificado se va a utilizar en un servidor lo mejor es no ponerle contraseña de acceso para evitar tener que introducirla cada vez que iniciemos el servidor. Si el certificado es para un usuario sí debemos protegerlo y crearlo cifrado con contraseña.

Las Autoridades Certificadoras no solamente ofrecen certificados, sino también los administran, determinan cuánto tiempo van a ser válidos y mantienen listas de certificados que ya no son válidos (Listas de Revocación de Certificados o CRLs).

2.6.2. Renovación de Certificados

Este proceso conlleva una actualización de los datos del usuario que posee el certificado, se realiza cuando las claves han expirado o su seguridad ha sido comprometida.

2.6.3. Revocación de Certificados

Un certificado deja de ser confiable si su clave privada se ve comprometida o el usuario que lo posee pierde derechos sobre el mismo. La AC debe notificar a todas las entidades

que confían en un determinado certificado cuando este se encuentra suspendido o revocado. Esta acción se la realiza mediante la publicación de las CRLs. Los usuarios pueden descargar estas listas de la AC o son enviadas sin previa petición periódicamente.

2.7. Jerarquías de Certificación

Los Certificados Digitales brindan una amplia gama de usos, que abarcan desde el correo electrónico dentro de una empresa hasta importantes transferencias electrónicas. A fin de poder utilizar los Certificados Digitales, debe necesariamente existir un alto grado de confianza asociado con la vinculación de un Certificado Digital a un usuario u organización en particular.

Esta confianza se logra construyendo jerarquías de Certificados Digitales, en la que todos sus miembros adhieren a las mismas políticas y principios. Los Certificados Digitales sólo pueden ser emitidos a individuos u organizaciones, como miembros potenciales de esa jerarquía, una vez que su identidad haya sido establecida. Diferentes jerarquías pueden tener diferentes políticas acerca de cómo se establece la identidad y de qué forma los Certificados Digitales son emitidos.

La herramienta que se va a utilizar para generar y administrar los Certificados Digitales y la Autoridad Certificadora es **OpenSSL,** una implementación libre, de código abierto, de los protocolos SSL (Secure Sockets Layer o Nivel de Zócalo Seguro) y TLS (Transport Layer Security, o Seguridad para Nivel de Transporte).

2.8. Mecanismos de Seguridad en redes Wireless

- **WEP**

(Wired Equivalent Privacy) Protocolo que permite cifrar la información que se transmite. Utiliza el algoritmo de cifrado RC4, y utiliza claves de 64 bits o de 128 bits. Se basa en dos

componentes para cifrar las tramas que circulan por la red: el algoritmo de cifrado RC4 y el algoritmo de chequeo de integridad CRC.

RC4 es un algoritmo de cifrado de flujo que genera una secuencia de números pseudoaleatorios de mayor tamaño. Esta secuencia de números pseudoaleatorios se unifica con el mensaje mediante una operación XOR para obtener un mensaje cifrado.

Posee varias características que lo convierten en un sistema vulnerable, a pesar de esto es muy usado debido a la facilidad de implementación y compatibilidad con todos los dispositivos que soportan 802.11.

- **WPA/WPA2**

WPA (Wi-Fi Protected Access, Acceso Protegido Wi-Fi), utiliza la encriptación de clave dinámica, lo que significa que la clave cambia constantemente. WPA fue diseñado para utilizarse con un servidor de autentificación que distribuye claves diferentes a cada usuario.

La información es cifrada utilizando el algoritmo con una clave de 128 bits y un vector de inicialización de 48 bits. WPA incluye dos versiones que utilizan diferentes procesos para la autentificación:

1. **TKIP:** El Protocolo de integridad de clave temporal es un tipo de mecanismo utilizado para crear encriptación de clave dinámica y autentificación mutua.
2. **EAP:** El Protocolo de autentificación extensible se utiliza para intercambiar mensajes durante el proceso de autentificación, este protocolo emplea la tecnología de servidor 802.1x para autentificar a los usuarios a través de un servidor Radius, este proceso proporciona un nivel de seguridad industrial para la red aunque se requiere WPA2. Aunque puede ser utilizado en redes cableadas es más usado en redes inalámbricas.

La principal diferencia entre WPA y WPA2 es que WPA2 requiere el estándar de encriptación avanzado para encriptar los datos, en tanto WPA utiliza TKIP.

- **WPA empresarial**

En redes corporativas se requiere mecanismos de control de acceso más flexibles y fáciles de mantener que permitan autentificar a los usuarios con nombre/contraseña o Certificado Digital. Los clientes WPA tienen que estar configurados para utilizar un sistema concreto de validación que es completamente independiente del punto de acceso. Los sistemas de validación WPA pueden ser, entre otros, EAP-TLS, PEAP-TTLS

- **EAP-TLS** (EAP-Transport Level Security)

Se utiliza en entornos de seguridad basados en certificados. El intercambio de mensajes EAP-TLS permite la autentificación y negociación mutua del método de cifrado y el intercambio seguro de claves cifradas entre el cliente de acceso remoto y el autenticador.

- **Filtrado de direcciones MAC**

Este mecanismo consiste en configurar en el Punto de Acceso las direcciones MAC de los usuarios autorizados para tener acceso. De esta manera el dispositivo al recibir tramas de direcciones diferentes no permite la conexión. Este método no se recomienda debido a la vulnerabilidad y a que no facilita la escalabilidad en entornos empresariales.

- **Estándar 802.1x**

(Port-based Network Access Control) Protocolo creado por la IEEE para Control de Admisión de Red basada en puertos, se basa en la arquitectura Cliente-Servidor. Este sistema hace uso de certificados digitales para proporcionar a los usuarios tanto servicios de autentificación como de autorización, gestionando confiabilidad en la comunicación.

802.1X plantea un escenario con tres entidades básicas como son el **cliente**, el elemento que proporciona la conectividad a la red (**punto de acceso**) y **el servidor de autentificación** encargado de averiguar si un determinado cliente ha sido autorizado a hacer uso de dicha red.

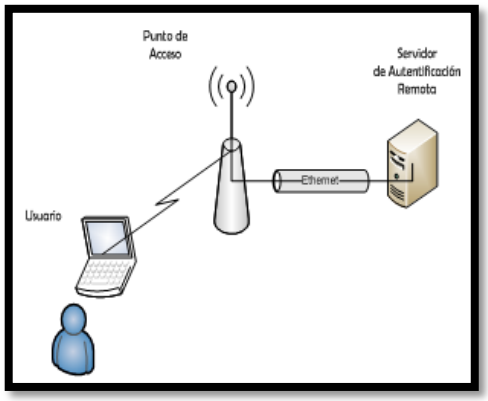


Figura II.4 Entidades 802.1x
Fuente: Creación del Autor

Este protocolo fue desarrollado para permitir a cualquier elemento de la red (switches, AP, etc.) pedir un proceso de autentificación para una conexión que se acaba de producir utiliza EAPOL (EAP OverLan) para realizar una encapsulación del protocolo EAP sobre la red privada para llegar al Servidor de Autentificación. El proceso de Autentificación se realiza de la siguiente manera.

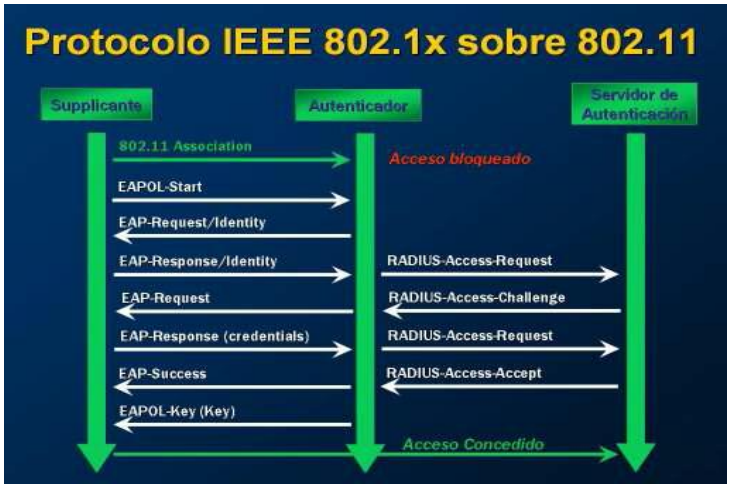


Figura II.5 Proceso de Autentificación de 802.1X
Fuente: http://t1.gstatic.com/images?q=tbn:AN

- El usuario se asocia al AP utilizando el protocolo 802.11
- El Suplicante inicia el proceso de autentificación 802.1X porque el AP no le concede acceso a la red y se elige el EAP-Method.
- El Autenticador requiere la Identidad al Suplicante.
- El Suplicante le entrega la Identidad al Autenticador que retransmitirá al Servidor de Autentificación. Las credenciales pueden ser desde el par usuario/contraseña hasta el uso de certificados de seguridad X.509.
- Servidor RADIUS valida las credenciales y acepta la conexión y entrega la EAPOL-Key que no es más que una secuencia de bits que utilizaremos como Clave Maestra en el proceso de cifrado del algoritmo de cifrado elegido (TKIP o AES). Así, cada vez que tenemos un proceso de autentificación o re-autentificación se genera una nueva Clave Maestra.

Para llevar a cabo la autentificación, son necesarios al menos 3 certificados digitales distintos. En primer lugar, es necesario disponer de una autoridad de certificación que actúe como raíz de confianza y que emita el resto de los certificados. En segundo lugar, el servidor RADIUS debe tener asociado su propio certificado para demostrar a los clientes que están solicitando el acceso a la red a través de un servidor de autentificación confiable. Por último, cada cliente debe disponer de su propio certificado digital, el cual presentará al servidor RADIUS para demostrar su derecho de acceso.

Llevar a cabo este proceso permite reducir la inseguridad de las redes inalámbricas porque:

1. **Proporciona acceso controlado:** Toda usuario (humano o máquina) que quiera acceder al recurso debe identificarse.
2. **Permite autorizar el uso:** A parte de saber quién intenta acceder a un recurso, se puede hacer un control de qué acciones puede ejecutar un usuario.

3. **Permite el registro de actividades:** Permite llevar logs o registros sobre cuál es el comportamiento de los usuarios en la red, y tener datos estadísticos que orienten la toma de decisiones para desempeñar una mejor gestión de la red.

Estos tres aspectos corresponden a tres palabras claves: Autentificación, Autorización y Contabilidad, conocidos también como servicios AAA, por su nombre en inglés: Authentication, Authorization and Accounting.

2.9. Protocolos AAA

Los protocolos AAA fueron una de las soluciones propuestas a los problemas de control de acceso presentados desde el nacimiento de internet para prestar los servicios AAA anteriormente presentados. Entre los protocolos más conocidos se encuentra TACACS, TACACS+, RADIUS y DIAMETER. El primero corresponde al protocolo pionero que suplió la carencia de servicios AAA. Actualmente ha caído en desuso y, su creador, CISCO, le retiró el soporte. Sin embargo, un protocolo nuevo entró a reemplazarlo. Éste se llamó TACACS+ y aunque hoy en día todavía se usa, sólo es implementado en una pequeña porción del mercado, debido al poco dinamismo de las soluciones comerciales.

Adicionalmente, los anuncios de la llegada de un nuevo protocolo que venía desarrollándose por parte de Livingston Enterprises, fortaleció la decisión de observar detenidamente la nueva propuesta, que además prometía nueva funcionalidades.

Con las incipientes implementaciones del nuevo protocolo, llamado RADIUS, se logró vislumbrar el potencial que tenía, convirtiéndose luego en un estándar de la IETF. Desde entonces se ha mantenido vigente a través de muchas aplicaciones que implementan el protocolo y siguen siendo actualizadas y mejoradas.

Actualmente se está desarrollando, DIAMETER, otro protocolo AAA, que pretende mejorar la especificación de RADIUS y proveer nuevas funcionalidades. Sin embargo, su calidad de

“estándar en construcción” o “borrador”, no ha facilitado el desarrollo de aplicaciones que lo implementen, ocasionando que su incursión en ambientes de producción sea mínima.

2.9.1. RADIUS

RADIUS (acrónimo en inglés de Remote Authentication Dial-In User Server). Es un protocolo de autentificación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza los puertos 1812 y 1813 UDP para establecer sus conexiones (para autentificar/autorizar y contabilizar, respectivamente).

Cuando se realiza la conexión con un ISP mediante un módem, DSL, cable módem, Ethernet o Wi-Fi, se envía una información que generalmente es un nombre de usuario y una contraseña. Esta información se transfiere a un dispositivo NAS (Network Access Server o Servidor de Acceso a la Red) sobre el protocolo PPP, quien redirige la petición a un servidor RADIUS sobre el protocolo RADIUS.

El servidor RADIUS comprueba que la información es correcta utilizando esquemas de autentificación como PAP, CHAP o EAP. Si es aceptado, el servidor autorizará el acceso al sistema del ISP y le asigna los recursos de red como una dirección IP, y otros parámetros como L2TP, etc.

RADIUS consta de tres componentes: un protocolo con un formato de trama que utiliza el protocolo de datagramas de usuario (UDP), un servidor y un cliente.

Los paquetes que se envían a través de la red manejan un formato propio del protocolo RADIUS, los mismos que contienen un campo denominado código que indica el tipo de paquete, como se muestra en la siguiente figura:

Valor	Nombre del Campo	Descripción
1	*Access-Request*	Cliente: Petición de acceso
2	*Access-Accept*	Servidor: Petición aceptada
3	*Access-Reject*	Servidor: Petición rechazada
4	*Accounting-Request*	Cliente: Petición de Registro
5	*Accounting-Response*	Servidor: Respuesta de Registro
11	*Access-Challenge*	Servidor: Desafío para autenticación
12	*Status-Server*	Reservado (experimental)
13	*Status-Client*	Reservado (experimental)
255	*Reserved*	Reservado

Figura II.6 Valores de código de la trama RADIUS
http://cybertesis.usmp.edu.pe/usmp/2009/coronado_ja/xml/ressources/fig041.jpg

Principales características:

- Funciona bajo el modelo cliente-servidor.
- Ofrece nivel limitado de seguridad en la red ya que aunque las comunicaciones entre el cliente y el servidor son validadas mediante un secreto compartido que no se envía por la red, solo se encripta la clave del usuario en los paquetes de solicitudes de acceso desde el cliente al servidor, utilizando el método de encriptación MD5. El resto del paquete no está encriptado pudiendo ser objeto de captura el nombre de usuario, servicios autorizados y la contabilización de estos.
- Los servidores RADIUS soportan varios esquemas de autentificación de usuario como: EAP, PAP y CHAP y soportan varios orígenes de información como: una base de datos del sistema (/etc/passwd), o una base de datos interna (del propio servidor RADIUS), mecanismos PAM y otros como Active Directory, LDAP y Kerberos.
- Capacidad para el manejo de sesiones, notificando inicio/cierre de conexión, lo que permite que al usuario se le pueda determinar su consumo y facturar en consecuencia; esta constituye una de las características fundamentales de este protocolo.

Aplicaciones e implementaciones del servidor RADIUS:

- **FreeRADIUS**

FreeRADIUS es un paquete de software de código abierto y libre distribución que implementa diversos elementos relacionados con RADIUS, tales como una biblioteca BSD para clientes, módulos para soporte en apache y un servidor de RADIUS.

- El servidor de FreeRADIUS es modular, para facilitar su extensión, y es muy escalable. Soporta prácticamente toda clase de clientes Radius (por ejemplo, ChilliSpot, JRadius, etc.)
- Se puede ejecutar en múltiples sistemas operativos: Linux (Debian, Ubuntu, Suse, Mandriva, FedoraCore, etc.), FreeBSD, MacOS, OpenBSD, Solaris, e incluso MS Windows por medio de cygwin.
- Soporta el uso de proxies y la replicación de servidores.

- **El proyecto EDUROAM**

Eduroam (EDUcation ROAMing) es un proyecto internacional creado para facilitar el acceso a Internet a los miembros de las instituciones científico-académicas asociadas, desde cualquiera de estas instituciones. Infraestructura de roaming basada en RADIUS**.** La conexión a Internet se hace habitualmente mediante un punto de acceso inalámbrico (cuyo identificador SSID es “eduroam”) que conecta al usuario directamente a una red IEEE 802.11 local. El proceso de autentificación se hace mediante el protocolo EAP, esta autentificación la hace siempre el centro al que pertenece el usuario (y no el centro al que se quiere conectar), y para llevar a cabo este proceso de manera segura y escalable se emplea el protocolo RADIUS.

2.9.2. LDAP

LDAP (Lightweight Directory Access Protocol) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP también es considerado una base de datos (aunque su sistema de almacenamiento puede ser diferente) al que pueden realizarse consultas. Habitualmente, almacena la información de login o acceso a un sistema (usuario y contraseña) y es utilizado para autentificarse aunque es posible almacenar otra información (datos de contacto del usuario, ubicación de diversos recursos de la red, permisos, certificados, etc).

En conclusión, LDAP es un protocolo de acceso unificado a un conjunto de información sobre una red. Existen diversas implementaciones y aplicaciones reales del protocolo LDAP:

- **Active Directory**

Active Directory es el nombre utilizado por Microsoft (desde Windows 2000) como almacén centralizado de información de uno de sus dominios de administración.

Bajo este nombre se encuentra realmente un esquema (definición de los campos que pueden ser consultados).

- **Novell Directory Services**

También conocido como eDirectory es la implementación de Novell utilizada para manejar el acceso a recursos en diferentes servidores y computadoras de una red. Básicamente está compuesto por una base de datos jerárquica y orientada a objetos, que representa cada servidor, computadora, impresora, servicio, personas, etc. entre los cuales se crean permisos para el control de acceso, por medio de herencia. La ventaja de esta

implementación es que corre en diversas plataformas, por lo que puede adaptarse fácilmente a entornos que utilicen más de un sistema operativo.

- **OpenLDAP**

Se trata de una implementación libre del protocolo que soporta múltiples esquemas por lo que puede utilizarse para conectarse a cualquier otro LDAP.

Tiene su propia licencia, la OpenLDAP Public License. Al ser un protocolo independiente de la plataforma, varias distribuciones Linux y BSD lo incluyen, al igual que AIX, HP-UX, Mac OS X, Solaris, Windows (2000/XP) y z/OS.

OpenLDAP tiene cuatro componentes principales:

- Slapd Demonio LDAP autónomo.
- Slurpd Demonio de replicación de actualizaciones LDAP autónomo.
- Rutinas de biblioteca de soporte del protocolo LDAP.
- Utilidades, herramientas y clientes.

- **Red Hat Directory Server**

Directory Server es un servidor basado en LDAP que centraliza configuración de aplicaciones, perfiles de usuarios, información de grupos, políticas así como información de control de acceso dentro de un sistema operativo independiente de la plataforma.

Forma un repositorio central para la infraestructura de manejo de identidad, Red Hat Directory Server simplifica el manejo de usuarios, eliminando la redundancia de datos y automatizando su mantenimiento.

CAPITULO III

Determinación de los Servidores de Autentificación

Los servidores de autentificación tienen como fin la administración del acceso a recursos sea de forma directa o remota. Entre lo que más cabe resaltar es que brindan un servicio de alta fiabilidad y dependiente de los recursos con que se cuentan para su perfecto funcionamiento. Estos protocolos son el resultado de una constante evolución de ofertas de seguridad con el fin de dar un servicio de completa confianza y mayor seguridad.

A continuación se presentan una lista de los servidores de autentificación más populares:

- ✓ RADIUS
- ✓ LDAP
- ✓ Internet Authentication Service IAS
- ✓ NPS
- ✓ KERBEROS
- ✓ TACACS Y TACACS+

- **RADIUS**

Servidor encargado de autentificar las conexiones remotas de forma segura. Puede utilizar un protocolo como PAP, CHAP o EAP para comprobar la identidad del usuario. Además, utiliza el protocolo UDP para el intercambio de información con los otros equipos.

- **LDAP**

(Lightweight Directory Access Protocol, o Protocolo Ligero de Acceso a Directorios) es un protocolo a nivel de aplicación que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

- **Servicio de autentificación de Internet IAS**

Implementación de Microsoft, ejecuta autentificación, autorización y seguimiento centralizado de la conexión para varios tipos de acceso a la red, como pueden ser accesos inalámbricos y conexiones por Red Privada Virtual (VPN). Como proxy propaga los mensajes de autentificación y seguimiento a otros servidores.

- **Servidor de directivas de red (NPS)**

Es la implementación de Microsoft de un proxy y un servidor de autentificación remota. Puede usar Active Directory de Windows como su base de datos de cuentas de usuario y forma parte de una solución de inicio de sesión único.

- **Kerberos**

Es un protocolo de autentificación que usa una criptografía de claves simétricas para validar usuarios con los servicios de red, evitando así tener que enviar contraseñas a través de la red. Al validar los usuarios para los servicios de la red por medio de Kerberos,

se frustran los intentos de usuarios no autorizados que intentan interceptar contraseñas en la red.

- **TACACS**

Es un protocolo de autentificación remota propietario de CISCO, que se usa para gestionar el acceso a servidores y dispositivos de comunicaciones, proporciona servicios separados de autentificación, autorización y registro. TACACS+ está basado en TACACS, pero, a pesar de su nombre, es un protocolo completamente nuevo e incompatible con las versiones anteriores de TACACS.

Para la realización de este análisis comparativo se han seleccionado los siguientes servidores de autentificación RADIUS y LDAP por las siguientes razones:

- Poseen buena documentación en línea y comunidad de usuarios.
- Pueden ser desarrollados en software libre.
- Soportan múltiples plataformas y base de datos.
- Añaden mayor seguridad a la red mediante el soporte de certificados digitales.
- Facilidad de uso y transparencia en los procesos para el usuario.

3.1. Descripción de los Servidores de Autentificación a Comparar

3.1.1. RADIUS

3.1.1.1. Historia

El origen del protocolo RADIUS se remonta al año 1991cuando Merit Network, organización de la Universidad de Michigan, mediante una RFI (Request For Information) especificó los requisitos para remplazar sus servidores «dial-In» propietarios por otros estandarizados, a la que respondió Livingston Enterprises con la descripción de un

Servidor RADIUS. En 1997 se convirtió en estándar mediante la publicación por parte del IETF de las RFC's 2058 y 2059. A partir del 2000 se lo especificó en los RFC´s 2865 y 2866.

En sus inicios debido a las soluciones tecnológicas del momento, se concibió para controlar de forma centralizada el acceso remoto de usuarios cuya conexión se realizaba mediante módems. A medida que se ha ido produciendo el desarrollo tecnológico, el protocolo RADIUS se ha implementado con éxito en escenarios de redes inalámbricas, ofreciéndoles la robustez y control necesarios en lo que a seguridad se refiere.

3.1.1.2. Instancias que intervienen

Se presenta una arquitectura Cliente-Servidor, como se indica en la Figura XX, los elementos que intervienen en el proceso de Autentificación con un servidor RADIUS, son:

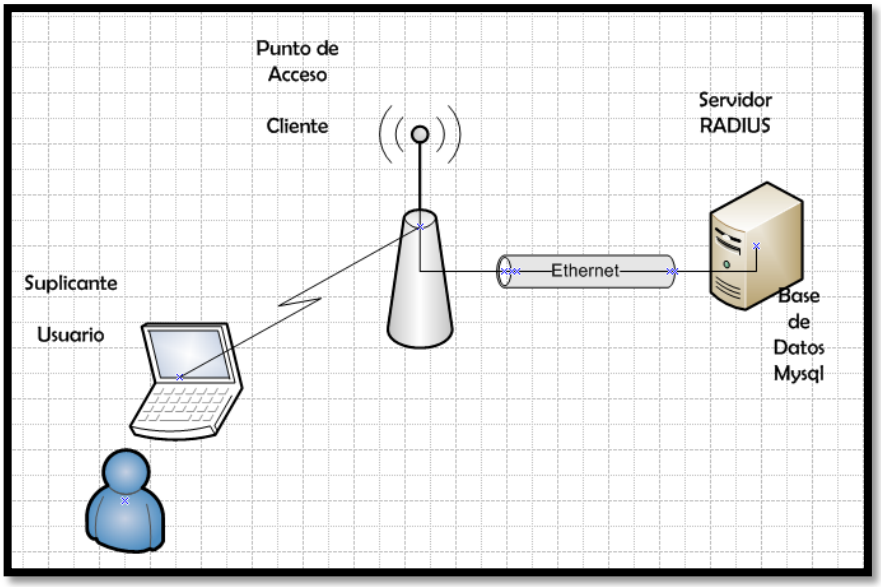


Figura III. 7 Arquitectura 802.1x con RADIUS

1. **Servidor RADIUS** Sistema que autoriza o no las peticiones de conexión en base a la información de usuarios que contiene en una base de datos.

2. **Network Access Server (NAS) o Cliente** Es un sistema que proporciona acceso a la red. Cuando un cliente quiere hacer uso de uno de estos servicios se conecta a

NAS, quien a su vez se conecta al servidor RADIUS preguntando si los credenciales proporcionados por el cliente son válidos. Basándose en su respuesta, además le permitirá acceder o no al recurso protegido.

3. **Usuarios o Suplicantes** Envían peticiones de conexión al Cliente de RADIUS con su respectivo nombre de usuario y contraseña.

3.1.1.3. Fases de Autentificación

- El usuario que desea tener acceso a la red, envía al Cliente Radius tanto su nombre de usuario como su clave de acceso empleando un protocolo de autentificación a nivel de enlace PPP (Point to Point Protocol).
- Una vez que el Cliente Radius ha obtenido los datos del usuario final, envía las credenciales de usuario, información de parámetros de conexión y la identificación del cliente Radius por la que está recibiendo la petición de acceso.
- Cuando esta petición llega al Servidor Radius, éste verifica la información recibida y puede:
  - Rechazar la petición, ya sea porque el usuario no sea válido o el servicio que solicita no le sea permitido.
  - Aceptar la conexión, facilitando información extra como por ejemplo una dirección IP asignada, para el establecimiento de la sesión.

3.1.1.4. Características

- Una de las características más importantes del protocolo RADIUS es su capacidad de manejar sesiones, notificando cuando comienza y termina una conexión, así que al usuario se le podrá determinar su consumo y facturar en consecuencia; los datos se pueden utilizar con propósitos estadísticos.
- Modelo cliente-servidor.

- El protocolo RADIUS ofrece una base de datos central donde almacenar toda la información del usuario de marcado. Todos los servidores de acceso a redes compatibles con RADIUS pueden utilizar esta base de datos.
- Un servidor RADIUS puede actuar como cliente Proxy a otros servidores RADIUS u a otro tipo de servidores de autentificación.
- Radius soporta dos lenguajes, uno construido internamente tipo C llamado Rewrite u otro llamado Schema que requiere Guile versión 1.4 o mayor. Este le permite al administrador escribir sus propios métodos de autentificación y contabilidad
- Opera en la capa 2 del modelo OSI con el uso del protocolo 802.1x. Ya que la autentificación de la Capa 2 opera en el nivel local, la red física, se evita que los intrusos utilicen la red física sin autentificarse.
- Algunos servidores usan el puerto UDP 1645 para mensajes de autentificación y, el puerto 1646, para mensajes de cuentas. Esto último debido a que son los puertos que se usaron inicialmente para este tipo de servicio.

3.1.1.5. Ventajas

Este estándar trae las siguientes ventajas:

- Alto nivel de seguridad porque puede usar nombres de usuarios y contraseñas o certificados de usuario.
- Cifrado más seguro.
- Autentificación y cohesión a la WLAN transparentes.
- Autentificación por separado de usuarios y de equipos.
- Bajo costo de hardware de red.
- Alto rendimiento porque el cifrado se lleva a cabo en el hardware de la WLAN y no en el procesador del equipo cliente.

- Sus clientes tan sólo tienen que implementar el protocolo de comunicación con RADIUS, y no todas las posibilidades de AAA existentes (PAP, CHAP, LDAP, Kerberos, mySQL, etc.).
- En su comunicación con el Cliente Radius, nunca transmite las contraseñas directamente por la red, ni siquiera al usar PAP, sino que usa algoritmos para ocultar las contraseñas como MD5.

3.1.1.6. Soporte de Plataformas

Un servidor RADIUS puede ser implementado en las plataformas más populares: Linux, Microsoft Windows y SUN/SOLARIS. El software utilizado FreeRADIUS ha sido compilado y probado en:

- Linux (todas las versiones)
- FreeBSD
- NetBSD
- Solaris

Plataformas en las que es soportado pero no ha sido completamente probado:

- HP/UX
- AIX
- MINGW32 (Unix-style environment under Windows NT)
- SFU (Interix, for Windows XP)

3.1.1.7. Almacenamiento de Datos

RADIUS al recibir los datos proporcionados por un usuario, para realizar la Autentificación, puede verificarlos desde:

- **Sistema de Base de Datos** Usuario y contraseña se almacenan en /etc/passwd en el servidor, es decir, son usuarios "normales" de UNIX en el sistema.
- **Internal Database** ID del usuario, contraseña, etc. se almacenan en la base de datos interna de RADIUS.
- **Autentificación de SQL** La información del usuario es almacenada en una base de datos SQL.
- **Autentificación PAM** El usuario está autenticado mediante PAM (Pluggable Authentication Service) que utiliza un conjunto de librerías compartidas que permiten a las aplicaciones solicitar que un usuario se autentifique.
- Además tiene la factibilidad de usar software de Base de Datos como OpenLDAP, PostgreSQL, Oracle.

3.1.1.8. Seguimiento y Monitoreo

Para monitorear el Servidor, existen las opciones:

- **Gestión SNMP** Radius permite la gestión SNMP de sus actividades. Su árbol de la MIB contiene propuestas por RFC 2619 y 2621, así como sus extensiones privadas.

- Se genera un archivo logfile ubicado en /var/log/freeradius/radius.log donde se puede observar lo que ocurre con cada módulo y archivo de RADIUS al realizar la autentificación.

- En /var/log/auth.log se encuentra información sobre todo tipo de autentificación: Usuarios de Linux o de RADIUS.

- **freeradius –X** es el archivo ejecutable de RADIUS que con la opción **–X** permite iniciar el servicio en modo debug y muestra en pantalla detalles del proceso de autentificación y notifica posibles errores en cada módulo.

3.1.1.9. Seguridad y Cifrado

Para fortalecer la seguridad e incrementar la integridad de los datos, RADIUS usa el concepto de secretos compartidos (Shared Secrets), valores aleatorios conocidos únicamente por el cliente y el servidor.

Son usados con todas las operaciones que requieran ocultar los datos, como contraseñas. Alternativamente, cuando se usa el protocolo CHAP se puede usar una clave en texto plano, pero esta opción no es recomendable por razones de seguridad.

La contraseña del usuario se almacena en forma encriptada utilizando la función hash MD5 o algoritmo DES, según sea el caso. Debido a la vulnerabilidad de este algoritmo RADIUS usa el protocolo de cifrado **TLS**, que encapsula los paquetes para reducir el riesgo de ataques a MD5.

Además, para cifrar la contraseña, RADIUS soporta la función hash **sha,** como se observa en la siguiente figura

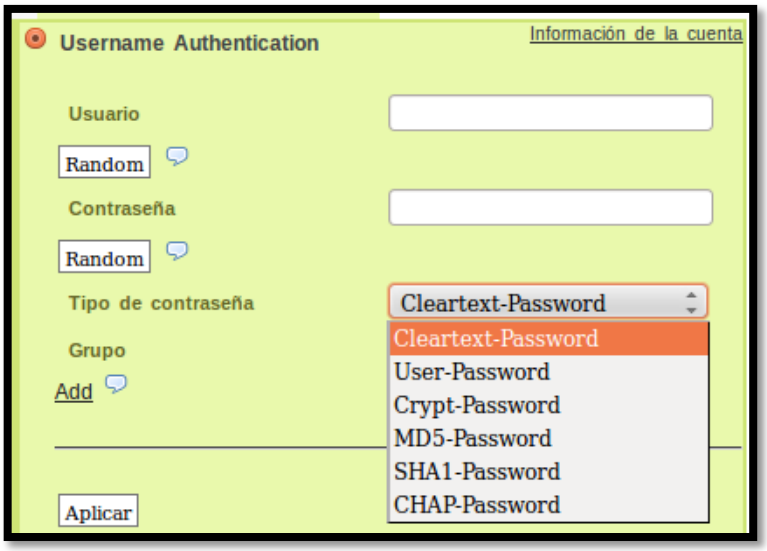


Figura III. 8 Algoritmos de Cifrado que soporta daloRADIUS

3.1.2. LDAP

3.1.2.1. Historia

LDAP aparece con el estándar de los directorios de servicios. La versión original fue desarrollada por la Universidad de Michigan. La primera versión no se usó y fue en 1995 cuando se publicaron los RFC (Request For Comments) de la versión LDAPv2. Los RFC para la versión LDAPv3 fueron publicados en 1997. La versión 3 incluía características como las listas de acceso (control Access Lists) y replicación de directorios.

El proyecto OpenLDAP se inició en 1998 por Kurt Zeilenga, comenzó como un clon de la implementación LDAP de la Universidad de Michigan, entidad donde se desarrolló originalmente el protocolo LDAP y que también actualmente trabaja en la evolución del mismo.

En abril de 2006, el proyecto OpenLDAP incorpora tres miembros principales: Howard Chu (Arquitecto jefe), Pierangelo Masarati, y Kurt Zeilenga. Hay otros importantes y activos contribuyentes incluyendo Luke Howard, Hallvard Furuseth, Quanah Gibson-Mount, y Gavin Henry.

Históricamente la arquitectura del servidor OpenLDAP (slapd, Standalone fue dividida entre una sección frontal que maneja las conexiones de redes y el procesamiento del protocolo, y un base de datos dorsal o de segundo plano (backend) que trata únicamente con el almacenamiento de datos. La arquitectura es modular y una variedad de backends está disponible para interactuar con otras tecnologías, no sólo bases de datos tradicionales.

3.1.2.2. Numero de instancias que intervienen

A continuación se detallan los elementos utilizados en el proceso de autentificación de los usuarios en un servidor LDAP.

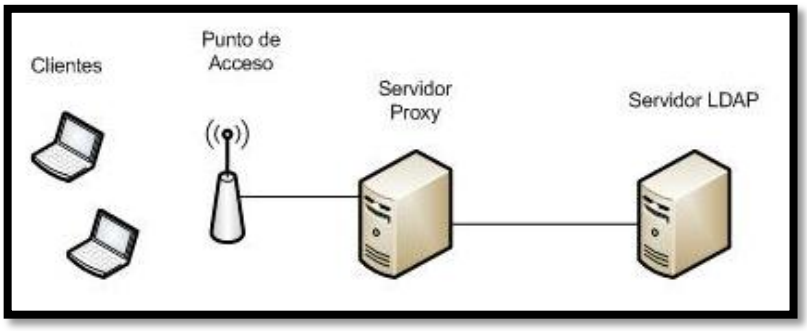


Figura III. 9 Elementos que Intervienen en la Autentificación de LDAP

- **Servidor LDAP:** protocolo de tipo cliente-servidor para acceder a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.
- **Servidor Proxy:** intercepta las conexiones de red que un cliente hace a un servidor de destino, por varios motivos como seguridad, rendimiento, etc. Esta función puede ser realizada por un programa o dispositivo. Este servidor es el encargado de permitir o no que determinado usuario tenga acceso a los recursos de la red.
- **Punto de Acceso:** dispositivo que recepta las conexiones de los clientes, y el que asigna una dirección ip a cada usuario.
- **Clientes:** dispositivos que envían peticiones a los servidores para acceder a la red.

3.1.2.3. Fases de Autentificación

- El servicio LDAP se basa en un modelo de cliente servidor lo cual quiere decir que uno o más servidores LDAP contienen los datos que forman el árbol LDAP o base de datos troncal.

- El cliente LDAP se conecta al AP para autentificarse.
- Como intermediario tenemos a un servidor proxy el cual debe estar configurado en el cliente.
- Al momento que el cliente abre una página de internet se le pide autentificarse con nombre de usuario y contraseña.
- El Proxy se conecta al servidor LDAP para verificar si el nombre de usuario y contraseña proporcionado por el cliente es correcto.
- Si es correcto la autentificación es satisfactoria y el usuario tendrá acceso a los recursos de la red.
- Caso contrario no podrá acceder a ningún tipo de servicio.

3.1.2.4. Características

- **Operaciones de lectura muy rápidas.** Debido a la naturaleza de los datos almacenados en los directorios las lecturas son más comunes que las escrituras.
- **Datos relativamente estáticos.** Los datos almacenados en los directorios no suelen actualizarse con mucha frecuencia.
- **Entorno distribuido**, fácil replicación
- **Estructura jerárquica.** Los directorios almacenan la información de forma jerárquica de forma nativa.
- **Orientadas a objetos.** El directorio representa a elementos y a objetos. Los objetos son creados como entradas, que representan a una colección de atributos.
- **Esquema estándar.** Los directorios utilizan un sistema estándar que pueden usar fácilmente diversas aplicaciones.

3.1.2.5. Ventajas

- LDAP es muy utilizada porque puedes almacenar información que desees leer desde muchas localizaciones. Aunque esta facilidad sirve siempre y cuando esta no se actualice frecuentemente.
- Dispone de un modelo de nombres globales que asegura que todas las entradas son únicas.
- Permite múltiples directorios independientes.
- Funciona sobre TCP/IP y SSL.
- Pueden tener capacidad de replicar información de forma amplia, con el fin de aumentar la disponibilidad y fiabilidad, y a la vez reducir tiempo de respuesta.
- Hay muchas formas de proporcionar un servicio de directorio. Los diferentes métodos permiten almacenar en el directorio diferentes tipos de información, establecer requisitos diferentes para hacer referencias a la información, consultarla y actualizarla, la forma en que protege al directorio de accesos no autorizados.
- Un servidor LDAP es usado para procesar peticiones (queries) a un directorio LDAP. Pero LDAP procesa las órdenes de borrado y actualización de un modo muy lento. "LDAP es un tipo de base de datos, pero no es una base de datos relacional"
- Muchas aplicaciones de todo tipo tienen interfaces de conexión a LDAP y se pueden integrar fácilmente.
- La mayoría de aplicaciones disponen de soporte para LDAP.
- La mayoría de servidores LDAP son fáciles de instalar, mantener y optimizar.
- Buena Documentación.

3.1.2.6. Cantidad de Datos Utilizados

LDAP puede almacenar 3 tipos de datos que se detallan a continuación:

- **Caracteres ASCII** que habitualmente almacena información de los usuarios que conforman una red, como el nombre de usuario, contraseña, directorio hogar, etc. Es posible almacenar otro tipo de información tal como, bebida preferida, número de teléfono celular, fecha de cumpleaños, etc.
- **Certificados Digitales** los cuales servirán para una autentificación segura de todos los usuarios de la red.
- **Imágenes** si un atributo contiene valores no ASCII, como las imágenes en formato JPEG, se codifica en formato Base64, para su posterior almacenamiento en el servidor.

3.1.2.7. Numero de Plataformas Soportadas

- Linux
- BSD
- AIX
- HP-UX
- Mac OS X
- Solaris
- z/OS
- Microsoft Windows

3.1.2.8. Cantidad de Almacén de datos Soportados

- Base de datos propia del servidor
- Usuarios del sistema
- Mysql

3.1.2.9. SEGURIDAD

El servidor LDAP es compatible con el cifrado de datos mediante el protocolo SSL (Capa de sockets seguros, el cual cifrarán todos los datos, incluidos el nombre de usuario y la contraseña. El servidor LDAP se debe configurar para que sea compatible con SSL, incluida la configuración de un certificado que establezca su identidad. Además, la interfaz de red del dispositivo se debe configurar con un certificado de una autoridad emisora de certificados para que valide el servidor LDAP. Normalmente, es el puerto 389 para un enlace **Sencillo** o el puerto 636 para un enlace **Simple por SSL**.

La autentificación SASL es la opción por defecto. Tiene como ventaja que transmite cifradas las password y como desventaja que se deben guarda en claro en el directorio.

Soporta variedad de esquemas de almacenamiento de la password, pero no son estándar.

Funciones Hash

- SSHA
- SHA
- SMD5
- MD5
- CRYPT
- CLEARTEXT

3.2. Determinación de los Parámetros de Comparación

Para la comparación de los Servidores de Autentificación en lo que se refiere a su eficiencia se debe considerar varios aspectos, importantes para determinar el Servidor más eficiente. Se han considerado 6 indicadores con sus respectivos índices para

determinar por separado sus potencialidades y debilidades. Se describe a continuación los parámetros de Comparación

- **Gestión de Usuarios**
  - Ingreso
  - Modificación
  - Eliminación

- **Autentificación**
  - Tiempo de Conexión
  - Cantidad de Paquetes Entrada/Salida
  - Número de Instancias que intervienen

- **Gestión de Datos**
  - Nivel de Acceso de Usuarios
  - Cantidad de Datos Utilizados

- **Rendimiento**
  - Cantidad de Memoria Usada
  - Nivel de Carga del CPU
  - Cantidad de Procesos

- **Funcionalidad**
  - Facilidad Instalación
  - Número de Plataformas soportadas
  - Cantidad de Almacén de Datos soportados
  - Facilidad de Seguimiento y Monitoreo

- **Seguridad**
  - Soporte de Cifrado
  - Cantidad de Protocolos soportados
  - Soporte de Funciones HASH

3.2.1. Indicador 1: Gestión de Usuarios

Describe el grado de facilidad que va a tener el administrador del sistema, al realizar las tareas más básicas y comunes como son el ingreso, modificación y eliminación de usuarios.

TABLA III. I DESCRIPCIÓN INDICADOR 1: GESTIÓN DE USUARIOS

Indicador	**Gestión de Usuarios**	Se refiere a la creación y mantenimiento de cuentas de usuarios y proporciona pautas sobre el grado de facilidad con la que se realizan estas tareas.
Índice 1	**Ingreso**	Describe el proceso mediante el cual se da de alta a un usuario en el sistema.
Índice 2	**Modificación**	Describe la modificación de datos de un usuario existente y los campos involucrados.
Índice 3	**Eliminación**	Describe el proceso mediante el cual se da de baja a un usuario.

3.2.2. Indicador 2: Autentificación

Describe la cantidad de elementos que intervienen en el proceso de autentificación, además del tiempo que tarda el servidor en autentificar a un usuario.

TABLA III. II DESCRIPCIÓN INDICADOR 2: AUTENTIFICACIÓN

Indicador	**Autentificación**	Se refiere al proceso y tiempo necesarios para comprobar la identidad de las instancias que intervienen en la comunicación.
Índice 1	**Número de Instancias que intervienen**	Número de Instancias necesarias para establecer la comunicación y realizar el proceso de Autentificación.
Índice 2	**Cantidad de Paquetes Entrada/Salida**	Número de paquetes que se intercambian entre las diferentes instancias para realizar la autentificación.
Índice 3	**Tiempo de Conexión**	Velocidad con la que se realiza el intercambio de paquetes de autentificación.

3.2.3. Indicador 3: Gestión de Datos

En este indicador se describe la cantidad de tipo de datos que el servidor puede alojar, además del nivel de acceso que tienen los usuarios sobre estos.

TABLA III. III DESCRIPCIÓN INDICADOR 3: GESTIÓN DE DATOS

Indicador	**Gestión de Datos**	Se refiere al tipo de Información que se puede guardar en el servidor y la manera de acceder a ellos.
Índice 1	**Nivel de Acceso de**	Permisos para acceder y/o modificar la información

	Usuarios	de los usuarios.
Índice 2	**Cantidad de Datos Utilizados**	Número y Tipos de Datos de Usuario que se almacenan en el servidor.

3.2.4. Indicador 4: Rendimiento

En este indicador se describe la cantidad de memoria que ocupa el servidor en funcionamiento, es decir la cantidad de recursos que consume.

TABLA III. IV DESCRIPCIÓN INDICADOR 4: RENDIMIENTO

Indicador	**Rendimiento**	Proporciona la información necesaria acerca de la cantidad de recursos que está consumiendo el servidor.
Índice 1	**Cantidad de Memoria Usada**	Describe el porcentaje de memoria RAM y SWAP utilizada.
Índice 2	**Nivel de carga del CPU**	Describe la cantidad de CPU que consume el protocolo de autentificación.
Índice 3	**Cantidad de Procesos**	Describe el número de procesos que genera el servidor en funcionamiento.

3.2.5. Indicador 5: Funcionalidad

En la sección de Funcionalidad se describe el grado de facilidad de instalación y monitoreo que presenta el servidor, además de las principales características técnicas.

TABLA III. V DESCRIPCIÓN INDICADOR 5: FUNCIONALIDAD

Indicador	**Funcionalidad**	Proporciona la información necesaria acerca delas principales características técnicas de cada servidor de autentificación.
Índice 1	**Facilidad de Instalación**	Describe el nivel de facilidad o complejidad en el proceso de instalación de los servidores.
Índice 2	**Numero de Plataformas Soportadas**	Determina la cantidad de sistemas operativos en los cuales se puede implementar.
Índice 3	**Cantidad de Almacén de datos Soportados**	Describe los tipos de bases de datos con los que son compatibles los servidores de autentificación.
Índice 4	**Facilidad de Seguimiento y Monitoreo**	Mide el grado de simplicidad en el registro y control de las actividades que se ejecutan.

3.2.6. Indicador 6: Seguridad

El indicador de Seguridad describe las alternativas y mecanismos que presenta cada servidor de autentificación, para elevar el grado de seguridad que ofrecen a los usuarios.

TABLA III. VI DESCRIPCIÓN INDICADOR 6: SEGURIDAD

Indicador	**Seguridad**	Describe si cumple con los parámetros necesarios para ofrecer una autentificación segura
Índice 1	**Soporte de Cifrado**	Determina si provee la codificación necesaria

		para un intercambio seguro de información.
Índice 2	**Cantidad de protocolos soportados**	Describe el número de protocolos de cifrado que soportan los servidores.
Índice 3	**Soporte de funciones HASH**	Determina si soporta o no funciones hash para añadir mayor grado de seguridad al intercambio de datos.

3.3. Descripción de los Módulos de Prueba

Los módulos de prueba son escenarios que nos permiten obtener los datos necesarios para determinar que servidor de autentificación es el más eficiente ante determinado escenario.

Los módulos serán implementados en los dos servidores de autentificación seleccionados previamente.

Se desarrollarán tres módulos de pruebas para los dos Servidores, estos son:

- Módulo de Transacciones de Alta y Baja
- Módulo de Rendimiento
- Módulo de Procesos de Autentificación
- Módulo de Implementación

A continuación se detallara en que consiste cada uno de los módulos de prueba antes de su implementación.

3.3.1. Módulo de Transacciones de Alta y Baja

Este módulo se refiere a la manera en que los Usuarios interactúan con el sistema, el tipo de datos que pueden ser almacenados y la forma en que se puede manipular la información almacenada en la base de datos de cada servidor. Permite determinar el nivel de acceso que poseen los usuarios a los datos y el grado de facilidad para realizar las transacciones de ingreso, modificación y eliminación de usuarios.

Es decir que con este módulo se lograra determinar que servidor proporciona mayor facilidad en las tareas de administración de usuarios.

3.3.2. Módulo de Rendimiento

Con este módulo se prueba el rendimiento y la capacidad de carga que posee el servidor en funcionamiento. Se comprobara que servidor consume mayor cantidad de recursos en las mismas condiciones.

3.3.3. Módulo de Procesos de Autentificación

Describe la manera en la que se realiza el proceso de Autentificación, el número de elementos necesarios que deben participar para poner en funcionamiento el servidor, la cantidad de paquetes que se intercambian durante este proceso y el tiempo que toma desde que un usuario intenta conectarse al AP hasta que ya forma parte de la red.

3.3.4. Módulo de Implementación

Describe el proceso de Instalación de los servidores, las características técnicas más determinantes de cada servidor.

3.4. Desarrollo de los Módulos de Pruebas

Cada servidor de autentificación que será desarrollado, deberá ser implementado en las mismas condiciones o idénticas, para de esta manera realizar una comparación equitativa.

3.4.1. Servidor RADIUS

3.4.1.1. Módulo de Transacciones de Alta y Baja

Para realizar cualquier tarea sobre los datos de usuarios y equipos almacenados en la base de datos de RADIUS, se requiere ser administrador e ingresar la clave asignada para tener los permisos para manipular la información y gestionar el sistema.

Al estar en red, cualquier usuario puede cargar la página principal de DaloRADIUS con la dirección IP del Servidor, pero solamente el administrador puede entrar al sistema con su Password. No hay la posibilidad de crear un usuario con permisos diferentes, por ejemplo lectura de la base de datos, que tenga acceso al sistema.

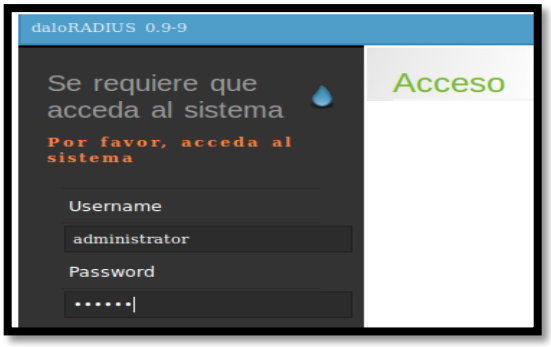


Figura III. 10 Interfáz de Autentificación de daloRADIUS

Una vez que se ha ingresado al sistema, las transacciones sobre los usuarios y su información se pueden realizar por medio de la interfaz gráfica o por línea de comando mediante el acceso a la Base de Datos MySQL.

a) Interfaz Gráfica

- **Ingreso de Usuario Nuevo**

Primero se ingresa a la interfaz gráfica de RADIUS (DaloRADIUS) como administrador del sistema, seleccionamos la opción NUEVO USUARIO, aparecerá un formulario para ingresar:

· Los datos de la cuenta: Nombre, Contraseña, Grupo, MAC, etc. Además se elige el tipo de encriptación de la contraseña o puede aparecer en texto plano.

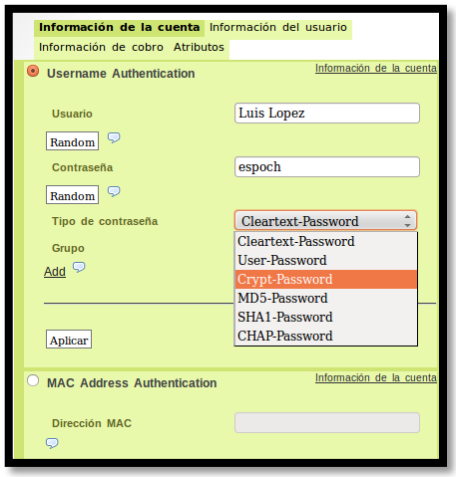


Figura III. 11 Interfaz de Ingreso de Nuevo Usuario

· Datos personales: Nombre Completo, Correo Electrónico, Notas, etc.

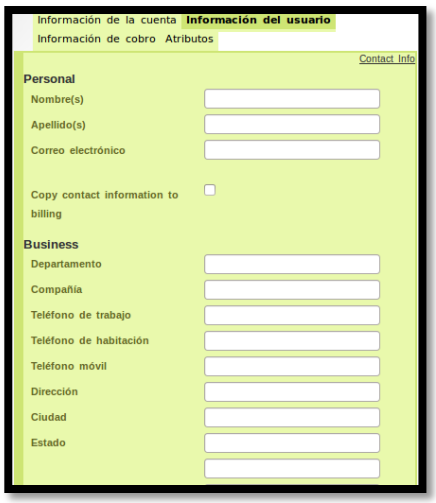


Figura III. 12 Formulario de Datos de Usuario

Una vez llenado el formulario, se selecciona APLICAR para escribir los datos en la Base de Datos. Cabe destacar que RADIUS solo admite almacenar información de tipo texto.

- **Modificación de Usuario**

Primero se ingresa el nombre del usuario, y se selecciona la opción **Editar Usuario** y a continuación aparecen los datos para ser modificados:

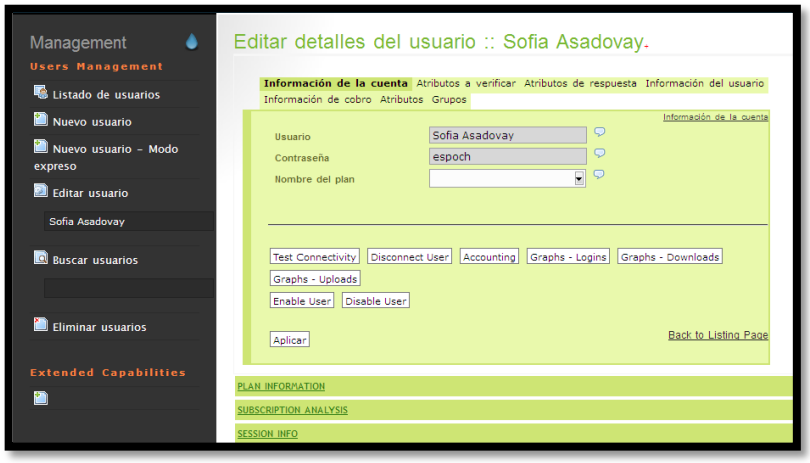


Figura III. 13 Formulario para Editar Usuario

Una vez modificados los campos requeridos, se selecciona aplicar para guardar los cambios.

- **Eliminar Usuario**

Se elige la opción **Eliminar Usuarios,** y aparece un formulario donde se ingresa el nombre del usuario a eliminar y si se desea o no borrar todos los registros que corresponden a dicho usuario.

Figura III. 14 Interfaz para eliminar Usuario

Al aplicar, se habrán borrado los datos de la base de Datos.

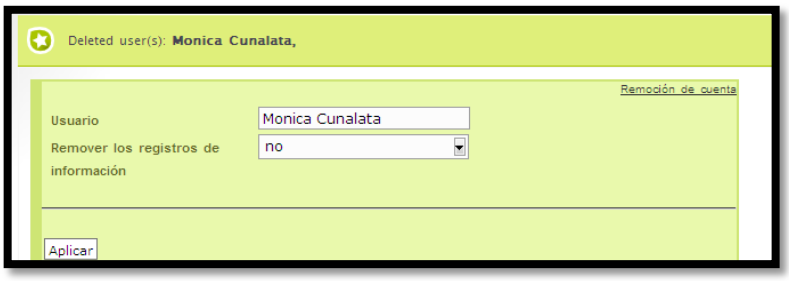


Figura III. 15 Notificación de Borrado de un Usuario

b) Línea de Comandos

- **Ingreso de Usuario Nuevo**

En el terminal, se accede a la base de Datos denominada Radius.

```
root@ubuntu:~# mysql -u root -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 46
Server version: 5.5.24-0ubuntu0.12.04.1 (Ubuntu)
```

Figura III. 16 Ingreso a MySQL

Se crea un nuevo usuario indicando la tabla correspondiente y los valores a ingresar.

```
mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('sofia', 'Clear
text-Password', 'sofilu');
Query OK, 1 row affected (0.05 sec)
```

Figura III. 17 Comando para crear nuevo usuario

- **Modificación de Usuario**

Para editar los datos de un usuario existente se utiliza el siguiente comando:

```
mysql> UPDATE radcheck SET value='cisco' WHERE id=1;
Query OK, 1 row affected (0.07 sec)
Rows matched: 1  Changed: 1  Warnings: 0
```

Figura III. 18 Comando para Editar Usuario

Donde, radcheck es el nombre de la tabla, value el campo que contiene la contraseña e id el campo que identifica al usuario, también se puede usar el nombre.

- **Eliminar Usuario**

Se ingresa el comando, con el nombre de la tabla y el campo que identifique al usuario que va a ser dado de baja del sistema.

```
mysql> DELETE from radcheck WHERE username='Luis Lopez';
Query OK, 1 row affected (0.02 sec)
```

Figura III. 19 Comando para eliminar Usuario

La ventaja de realizar estas tareas por línea de comando es que se obtiene el tiempo que toma cada proceso, así: Crear Usuario tarda 0.05 s, Modificar Usuario tarda 0.07 s y eliminar Usuario tarda 0.02 s. De esta manera se concluye que el servidor tarda más en modificar la información, además le toma menos tiempo borrar los registros de un usuario que en crearlos.

3.4.1.2. Módulo de Rendimiento

En la interfaz gráfica DaloRADIUS se muestra el estado del Servidor:

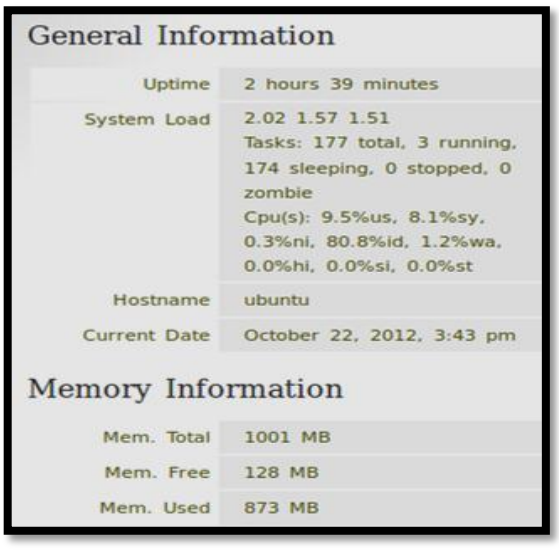


Figura III. 20 Información del Estado de Memoria en daloRADIUS

Como se observa en la figura el Servidor en funcionamiento ocupa 873 MB de memoria de los 1001 MB disponibles.

La carga promedio del CPU se refiere al número promedio de procesos ejecutables en el sistema. La carga promedio es a menudo listada como tres conjuntos de números, lo que representa la carga promedio para los últimos 1, 5 y 15 minutos, indicando que el sistema en este ejemplo no estaba muy ocupado.

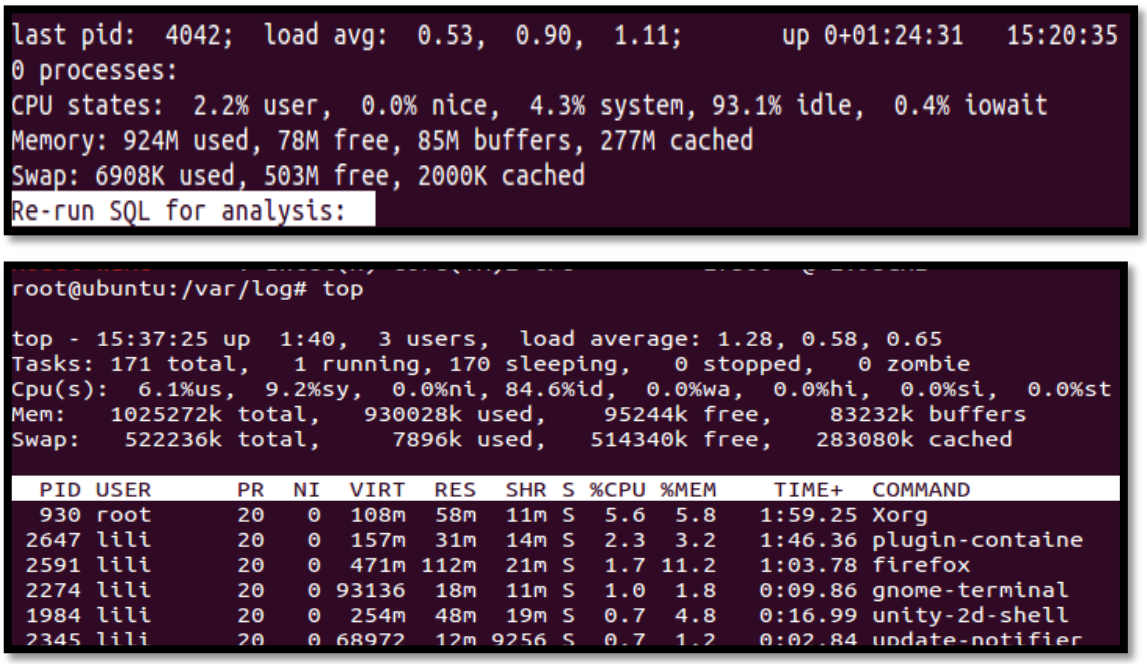
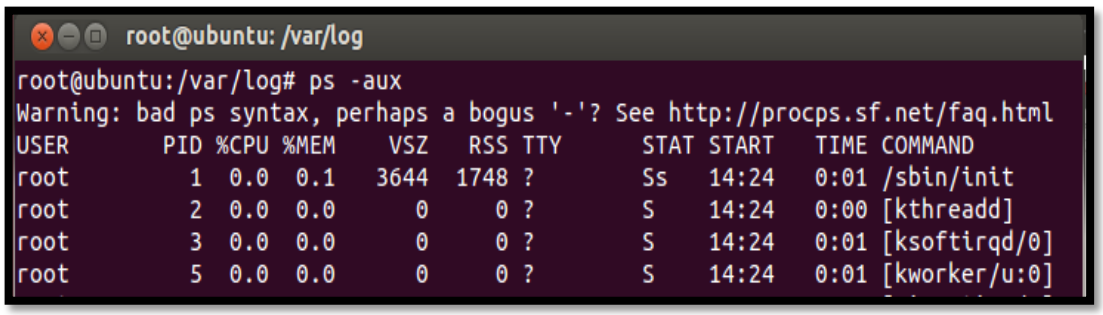


Figura III. 21 Resultado del comando top

Se observa en la figura que el Servidor genera una cantidad de 4066 procesos, el proceso **freeradius** con ID 4030 ocupa un 0.2 de CPU y 0.5 de memoria.



```
www-data   3258  0.0  0.4  37944  4808 ?        S    14:49   0:00 /usr/sbin/apach
www-data   3261  0.0  0.7  38988  7660 ?        S    14:49   0:00 /usr/sbin/apach
www-data   3262  0.0  0.7  39344  8176 ?        S    14:49   0:00 /usr/sbin/apach
www-data   3263  0.0  0.8  39136  8224 ?        S    14:49   0:00 /usr/sbin/apach
root       3779  0.0  0.0      0     0 ?        S    16:04   0:00 [kworker/0:0]
root       3822  0.0  0.0      0     0 ?        S    16:09   0:00 [kworker/0:1]
root       3848  0.0  0.0      0     0 ?        S    16:14   0:00 [kworker/0:3]
root       3880  0.0  0.0      0     0 ?        S    16:19   0:00 [kworker/0:2]
lili       3921  0.1  0.3   7224  3560 pts/1    Ss   16:22   0:00 bash
root       3975  0.0  0.1   5780  1732 pts/1    S    16:22   0:00 sudo -s
root       3976  0.1  0.3   7220  3644 pts/1    S    16:22   0:00 /bin/bash
freerad    4030  0.2  0.5  20696  5752 pts/1    S+   16:22   0:00 freeradius -X
lili       4055  3.0  3.1 152576 32156 ?        Sl   16:24   0:00 /usr/bin/unity-
root       4066  0.0  0.1   4928  1172 pts/0    R+   16:24   0:00 ps -aux
root@ubuntu:/var/log#
```

Figura III. 22 Procesos ejecutándose en el Servidor RADIUS

3.4.1.3. Módulo de Procesos de Autentificación

- **Paquetes Entrada/Salida**

El protocolo 802.1x permite a cualquier elemento de la red pedir un proceso de autentificación para establecer una conexión. Utiliza EAPOL (EAP Over LAN) porque lo que va a realizar es una encapsulación del protocolo EAP sobre la red privada para llegar al Servidor RADIUS. Se tiene el siguiente esquema:

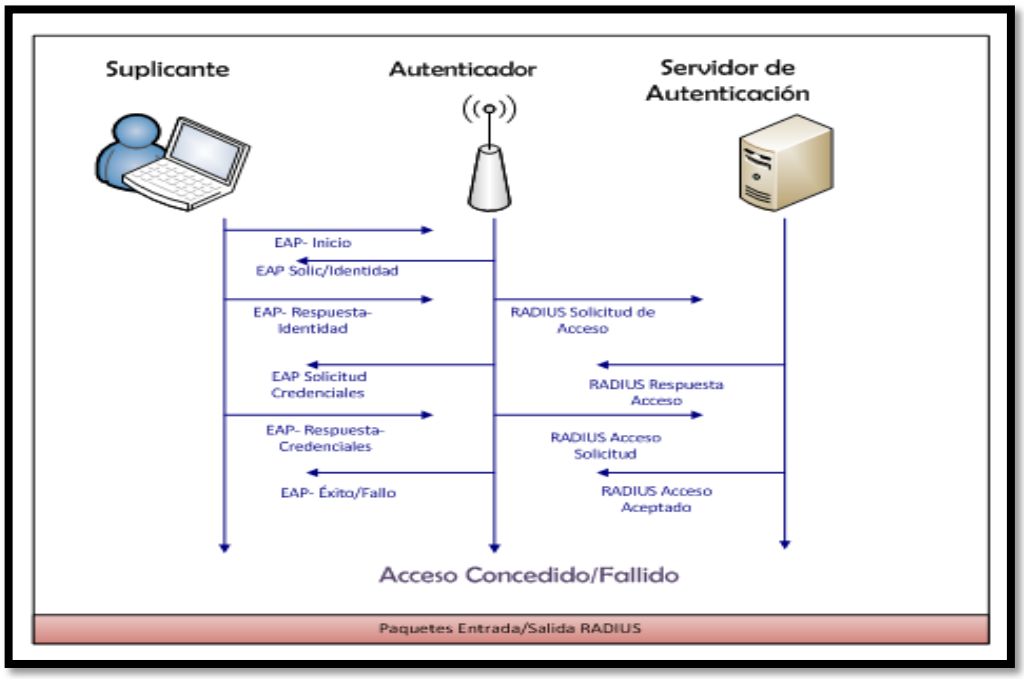


Figura III. 23 Paquetes Intercambiados en la Autentificación de RADIUS

1. El suplicante envía un mensaje de inicio de EAP para proceso de autentificación.
2. El NAS a la red responde con una solicitud de autentificación EAP.
3. El usuario envía un mensaje EAP con los datos de autentificación.
4. El NAS envía un Access-Request al Servidor, paquete que contiene el nombre de usuario, el atributo de la dirección IP NAS o el atributo de identificador NAS, la contraseña de usuario encriptada, la dirección del puerto NAS y opcionalmente otros atributos.
5. El Servidor de autentificación verifica los datos suministrados por el cliente mediante algoritmos, y envía un paquete de Access-Accept o Access-Reject para aceptar o rechazar la conexión.
6. El punto de acceso suministra un mensaje EAP de aceptación o rechazo, dejando que el cliente se conecte o rechazándolo.
7. Una vez autentificado, el servidor envía los paquetes necesarios para efectuar la Autorización y Contabilidad correspondientes a cada Usuario.

En la figura se muestra la captura de los paquetes que se transfieren durante el proceso de Autentificación utilizando el Sniffer Wireshark, solo se capturo los mensajes relacionados con el protocolo.

Figura III. 24 Paquetes del Protocolo RADIUS

- **Tiempo de Conexión**

Por medio de Wireshark, se capturan los paquetes, en este caso se observa con detalle el paquete Access-Accept y en la parte inferior se indica el tiempo de autentificación que es de 0.174366 segundos, como se muestra en la figura:

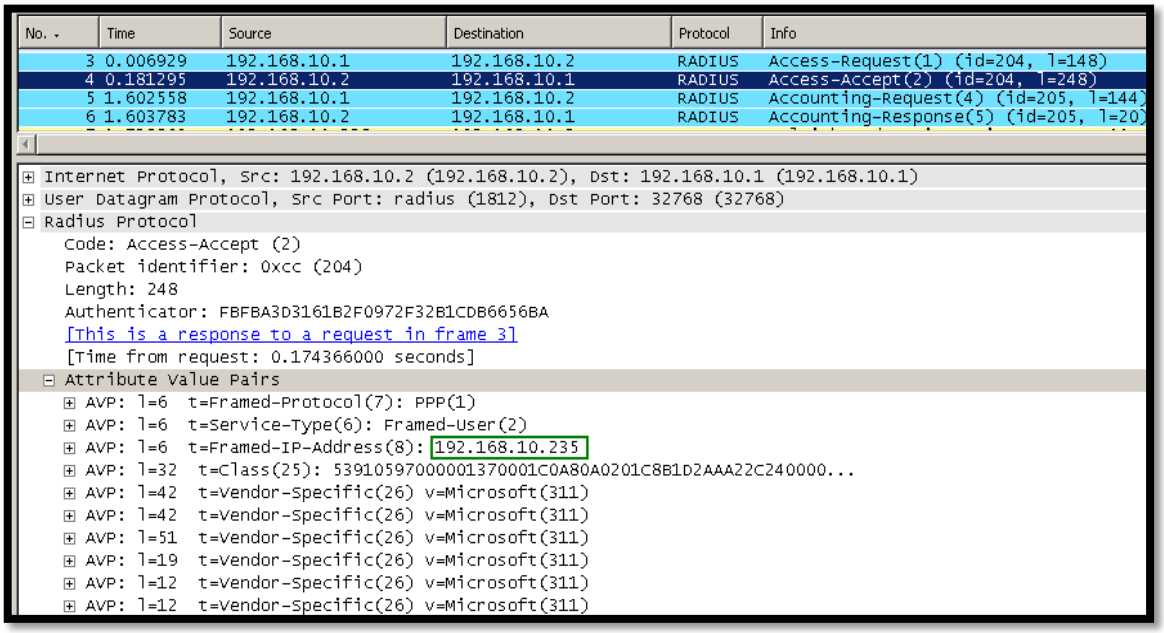


Figura III. 25 Tiempo de Autentificación de RADIUS usando Wireshark

3.4.1.4. Módulo de Implementación

Implementación

Para implementar el Servidor RADIUS, son necesarios varios paquetes y configuraciones de archivos, proceso que se detalla a continuación.

1. Lo primero es instalar **MySQL y Freeradius**, para ello se instalaran los paquetes necesarios: mySQL, freeradius, freeradius-mysql y DaloRADIUS.

2. El archivo **radiusd.conf** es editado para que RADIUS utilice la base de datos **MySQL** para almacenar la información de los usuarios.

3. Se ingresa **MySQL** y se crea la base de datos **radius,** además se crea el usuario **radius,** que contará con todos los permisos sobre la misma. Se exporta el formato de las tablas hacia la nueva base de datos desde RADIUS.

4. Se edita el fichero **sql.conf** para poder autentificar a los usuarios remotos.

5. Se reinician los servicios para guardar los cambios.

3.4.2. LDAP

3.4.2.1. Módulo de Transacciones Alta y Baja

- **INGRESO**

Creamos un archivo .ldif de un usuario, en el cual agregamos la información

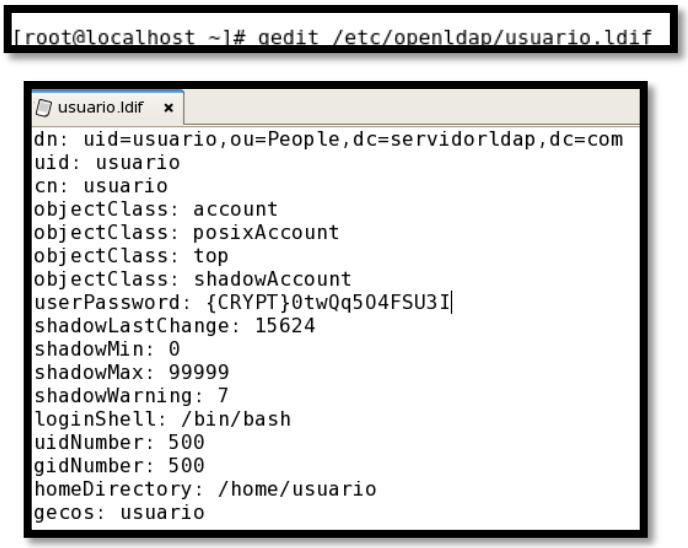


Figura III. 26 Contenido del Archivo LDIF de OpenLDAP

El campo userPassword lo obtenemos de la siguiente manera

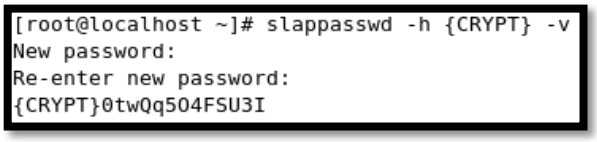


Figura III. 27 Comando para cambiar de Clave al Administrador de LDAP

Mediante línea de comandos añadir el usuario anterior al sistema:

ldapmodify -axvWD "cn=manager,dc=servidorldap,dc=com" -f /etc/openldap/usuario.ldif

Dónde:

-a: añadir al árbol ldap

-x: autentificación simple (sin SSL, etc.)

-v: verbose

-W: pedir el password del DN con que me autentifique

-f fichero: fichero donde se va a escribir las modificaciones

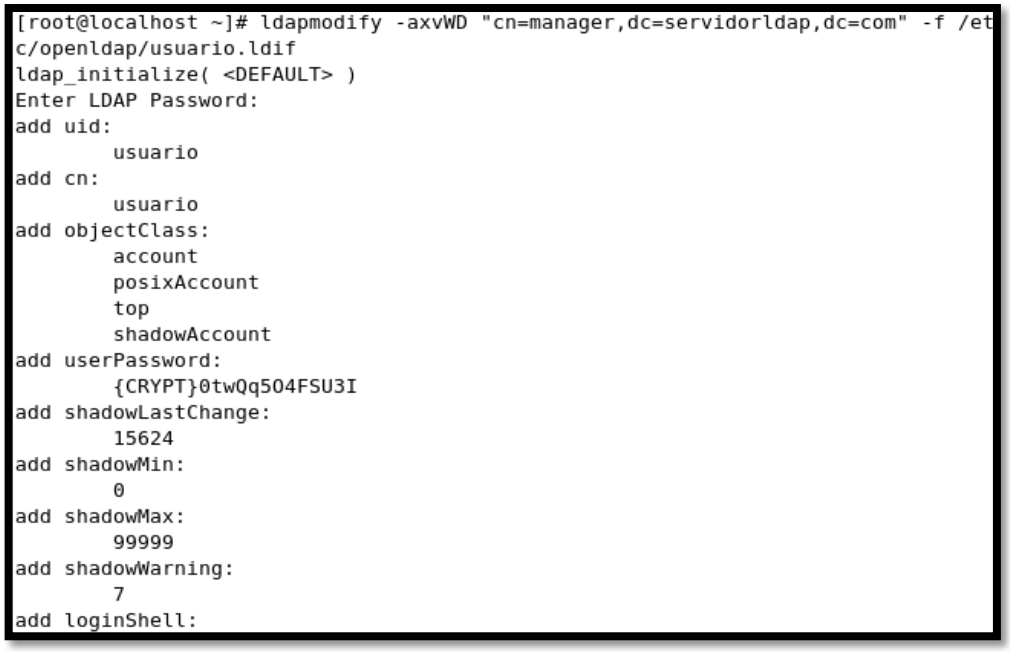


Figura III. 28 Comando de Ingreso de nuevo Usuario en LDAP

- **MODIFICACIÓN**

Por ejemplo se va a añadir el número telefónico a los datos del usuario anterior, para eso se tiene que modificar su archivo usuario.ldif

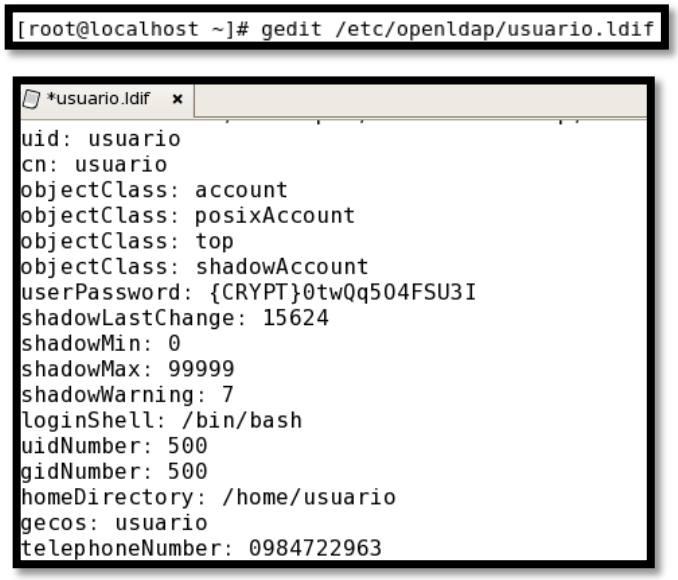


Figura III. 29 Modificación de in Archivo LDIF para añadir nuevos Datos

Se usa el siguiente comando para que el sistema actualice los campos añadidos o modificados de ese usuario.

```
replace loginShell:
        /bin/bash
replace uidNumber:
        500
replace gidNumber:
        500
replace homeDirectory:
        /home/usuario
replace gecos:
        usuario
replace telephoneNumber:
        0984722963
modifying entry "uid=usuario,ou=People,dc=servidorldap,dc=com"
modify complete
```

Figura III. 30 Comando de Actualización de Datos en LDAP

- **ELIMINACIÓN**

Para eliminar un usuario del árbol del directorio se debe crear un archivo del tipo ldif como se muestra a continuación:

*borrar.ldif ×

```
dn: uid=usuario,ou=People,dc=servidorldap,dc=com
changetype: delete
```

Figura III. 31 Contenido del Archivo LDIF para Eliminar Usuarios

Se ejecuta el siguiente comando para eliminar un usuario del árbol LDAP

```
[root@localhost ~]# ldapmodify -x -D "cn=manager,dc=servidorldap,dc=com" -W -f /
etc/openldap/borrar.ldif
Enter LDAP Password:
deleting entry "uid=usuario,ou=People,dc=servidorldap,dc=com"
```

Figura III. 32 Ejecución del Comando para Eliminar Usuarios

- **Nivel de Acceso de Usuarios**

Como usuario normal se puede ver todos los usuarios

```
[monica@localhost ~]$ ldapsearch -x -b "dc=servidorldap,dc=com" '(objectclass=*)
```

```
# cristian, People, servidorldap.com
dn: uid=cristian,ou=People,dc=servidorldap,dc=com
uid: cristian
cn: cristian
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQxJDJYcEI5RWlGJGlSYm9NNmxlSnVReTc5WUxvbTIwcS4=
shadowLastChange: 15624
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 506
gidNumber: 506
homeDirectory: /home/cristian

# paulina, People, servidorldap.com
dn: uid=paulina,ou=People,dc=servidorldap,dc=com
uid: paulina
cn: paulina
objectClass: account
objectClass: posixAccount
```

Figura III. 33 Comando para Búsqueda de Datos como Usuario Normal

No se puede detener el sistema

```
[monica@localhost ~]$ service ldap restart
bash: service: command not found
```

Figura III. 34 Comando para Reiniciar el Servicio LDAP

Creando el usuario prueba

```
dn: uid=prueba,ou=people,dc=servidorldap,dc=com
uid: prueba
cn: usuario prueba
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:
shadowLastChange: 14001
shadowMax: 99999
shadowWarming: 7
loginshel:/bin/bash
uidNumber: 1001
gidNumber: 1001
homeDirectory: /home/prueba
gecos: usuario prueba
```

Figura III. 35 Contenido del Archivo LDIF para crear un Nuevo Usuario

Como se muestra en el paso anterior, no se puede crear un nuevo usuario.

```
[monica@localhost ~]$ vi prueba.ldif
[monica@localhost ~]$ gedit prueba.ldif
[monica@localhost ~]$ ldapadd -x -W -D "cn=people,dc=servidorldap,dc=com" -f pr
eba.ldif
Enter LDAP Password:
ldap_bind: Server is unwilling to perform (53)
        additional info: unauthenticated bind (DN with no password) disallowed
[monica@localhost ~]$ slappasswd
bash: slappasswd: command not found
```

Figura III. 36 Resultado de la Ejecución del Comando para Añadir Usuario

Para eliminar un usuario.

```
eliminar.ldif ×
dn: uid=paulina,ou=peole,dc=servidorldap,dc=com"
changetype: delete
```

Figura III. 37 Contenido del Archivo LDIF para Eliminar Usuario

No se puede:

```
[monica@localhost ~]$ ldapmodify -x -D "cn=people,dc=servdidorldap,dc=com" -W -
 eliminar.ldif
Enter LDAP Password:
ldap_bind: Invalid credentials (49)
```

Figura III. 38 Resultado del Comando ldapmodify como usuario Normal

3.4.2.2. Módulo de Rendimiento

- **Cantidad de Memoria Usada**

```
[root@localhost ~]# cat /proc/meminfo
MemTotal:       1034708 kB
MemFree:         436076 kB
Buffers:          87740 kB
Cached:          369012 kB
SwapCached:           0 kB
Active:          259892 kB
Inactive:        307540 kB
HighTotal:       131008 kB
HighFree:           256 kB
LowTotal:        903700 kB
LowFree:         435820 kB
SwapTotal:      3068372 kB
SwapFree:       3068372 kB
Dirty:               24 kB
Writeback:            0 kB
AnonPages:       110692 kB
Mapped:           51312 kB
Slab:             18456 kB
PageTables:        3504 kB
NFS_Unstable:         0 kB
Bounce:               0 kB
CommitLimit:    3585724 kB
```

```
Committed_AS:    557984 kB
VmallocTotal:    114680 kB
VmallocUsed:       6216 kB
VmallocChunk:    108276 kB
HugePages_Total:      0
HugePages_Free:       0
HugePages_Rsvd:       0
Hugepagesize:      4096 kB
```

Figura III. 39 Resultado del Comando meminfo del Servidor LDAP

La cantidad de memoria utilizada por el servidor en funcionamiento es de 598, 632 MB.

- **Nivel de Carga del CPU**

Este archivo ofrece una vista de la carga promedio del procesador con respecto al sobretiempo de CPU y de E/S, así como también datos adicionales utilizados por uptime y otros comandos. Las primeras tres columnas muestran la utilización de CPU y de E/S en los últimos periodos de 1, 5 y 10 minutos. La cuarta columna le muestra el número de procesos actualmente en ejecución y el número total de los mismos. La última columna visualiza el último ID de proceso usado.

```
[root@localhost proc]# cat loadavg
0.36 0.31 0.23 1/157 4328
```

Figura III. 40 Resultado del Comando loadavg del Servidor LDAP

- **Cantidad de Procesos**

```
[root@localhost proc]# ps -aux
Warning: bad syntax, perhaps a bogus '-'? See /usr/share/doc/procps-3.2.7/FAQ
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.1  0.0   2160   644 ?        Ss   16:59   0:01 init [5]
root         2  0.0  0.0      0     0 ?        S<   16:59   0:00 [migration/0]
root         3  0.0  0.0      0     0 ?        SN   16:59   0:00 [ksoftirqd/0]
root         4  0.0  0.0      0     0 ?        S<   16:59   0:00 [events/0]
root         5  0.0  0.0      0     0 ?        S<   16:59   0:00 [khelper]
root         6  0.0  0.0      0     0 ?        S<   16:59   0:00 [kthread]
root         9  0.0  0.0      0     0 ?        S<   16:59   0:00 [kblockd/0]
root        10  0.0  0.0      0     0 ?        S<   16:59   0:00 [kacpid]
root       174  0.0  0.0      0     0 ?        S<   16:59   0:00 [cqueue/0]
root       177  0.0  0.0      0     0 ?        S<   16:59   0:00 [khubd]
root       179  0.0  0.0      0     0 ?        S<   16:59   0:00 [kseriod]
root       243  0.0  0.0      0     0 ?        S    16:59   0:00 [khungtaskd]
root       244  0.0  0.0      0     0 ?        S    16:59   0:00 [pdflush]
root       245  0.0  0.0      0     0 ?        S    16:59   0:00 [pdflush]
root       246  0.0  0.0      0     0 ?        S<   16:59   0:00 [kswapd0]
root       247  0.0  0.0      0     0 ?        S<   16:59   0:00 [aio/0]
root       465  0.0  0.0      0     0 ?        S<   16:59   0:00 [kpsmoused]
root       495  0.0  0.0      0     0 ?        S<   16:59   0:00 [mpt_poll_0]
```

```
root       3612  0.0  0.5  45556  5512 ?        Ss   17:02   0:00 gnome-power-man
root       3613  0.0  0.0   1960   636 ?        S    17:02   0:00 /sbin/pam_times
root       3621  0.0  0.2  18352  2436 ?        Sl   17:02   0:00 ./escd --key_In
root       3625  0.0  0.2   6504  3096 ?        S    17:02   0:00 /usr/sbin/nm-sy
root       3627  0.0  0.7  76484  7816 ?        S    17:02   0:00 /usr/libexec/tr
root       3629  0.0  1.0  47336 10932 ?        S    17:02   0:00 /usr/libexec/wn
root       3653  0.0  0.0   2572   884 ?        S    17:02   0:00 /usr/libexec/ma
root       3695  0.0  0.6  23364  6608 ?        S    17:02   0:00 /usr/libexec/no
root       3697  0.0  1.0  29424 10404 ?        S    17:02   0:00 /usr/libexec/cl
root       3699  0.0  1.1  59140 11760 ?        Sl   17:02   0:00 /usr/libexec/mi
root       3704  0.1  1.3  40996 13788 ?        Sl   17:02   0:01 gnome-terminal
root       3706  0.0  0.0   2576   716 ?        S    17:02   0:00 gnome-pty-helpe
root       3707  0.0  0.1   4632  1444 pts/1    Ss   17:02   0:00 bash
root       3722  0.0  0.8  39984  8904 ?        S    17:02   0:00 /usr/libexec/no
root       3726  0.0  0.2  16900  2124 ?        Ss   17:02   0:00 gnome-screensav
ldap       4146  0.0  0.3  42160  3484 ?        Ssl  17:08   0:00 /usr/sbin/slapd
root       4247  0.0  0.1   4576  1108 ?        S    17:11   0:00 /bin/sh /usr/li
root       4279  3.3  4.2 225176 43752 ?        Sl   17:11   0:09 /usr/lib/firefo
root       4336  0.0  0.0   4352   960 pts/1    R+   17:16   0:00 ps -aux
```

Figura III. 41 Resultado del Comando ps -aux del Servidor LDAP

3.4.2.3. Módulo de Autentificación

- **Tiempo de Conexión**

Para medir el tiempo que tarda un usuario en autentificarse y obtener los privilegios por formar parte de la red, utilizamos el sniffer wireshark mediante el cual capturamos todos los paquetes que atraviesan la red. Se realizó 2 pruebas, la primera es con un usuario y/o contraseña errónea cuyo tiempo es aproximadamente de 1 mili segundo y con los datos correctos tardo 2 mili segundos aproximadamente, es decir casi el doble del tiempo anterior.

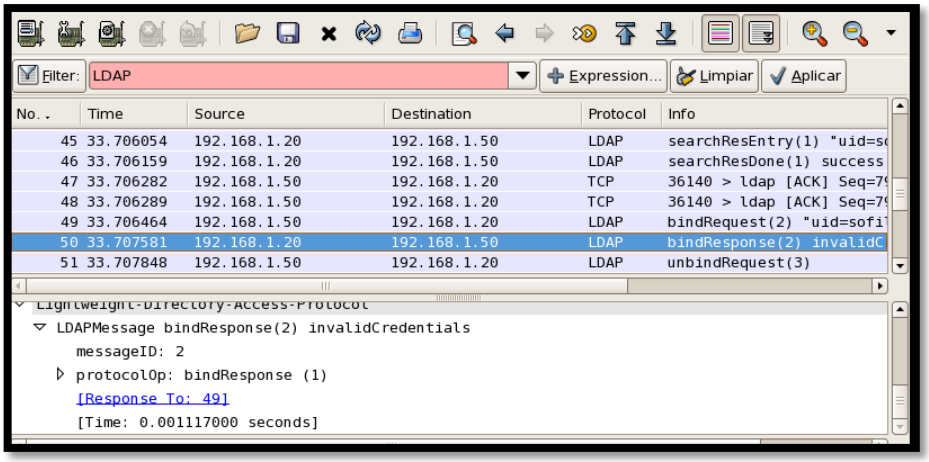


Figura III. 42Tiempo de autentificación de un usuario con Credenciales Inválidas en LDAP

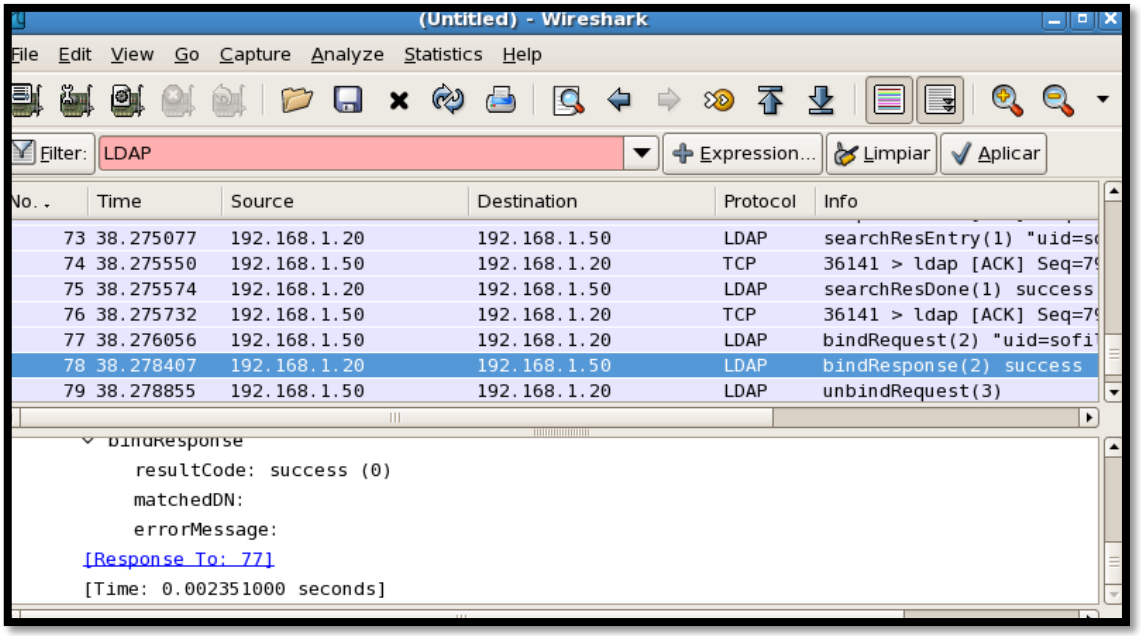


Figura III. 43 Tiempo de autentificación de un usuario con Credenciales Válidas en LDAP

Cantidad de Paquetes Entrada/Salida

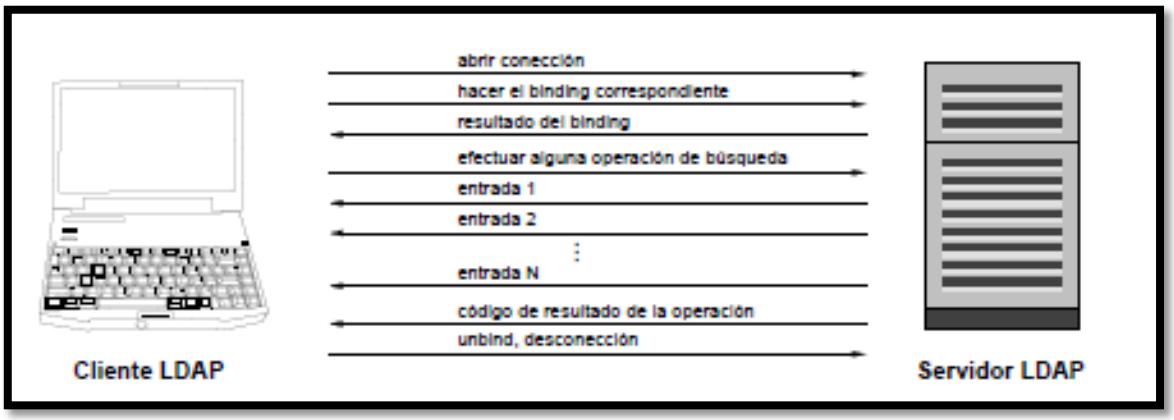


Figura III. 44 Paquetes Intercambiados durante el proceso de Autentificación LDAP

LDAP es un protocolo cliente - servidor de tal manera que un cliente construye un mensaje de requerimiento de cierta acción y lo envía a través de la red. El intercambio de paquetes entre un cliente y servidor LDAP se describe a continuación:

1. Conseguir nombre de usuario (uid) y password del usuario, habitualmente a través de un formulario web o en este caso utilizando un servidor proxy. El establecimiento de una sesión implica que el cliente LDAP debe especificar la

dirección IP o nombre del servidor, además del puerto TCP sobre el cual el servicio LDAP está disponible.

2. Enlazar o hacer un binding del servidor LDAP con la cuenta de usuario y clave que se encuentra alojada en el servidor. Luego en el binding al directorio, el cliente debe proveer un username y una clave para la autentificación y así acceder a los permisos y accesos apropiados para la ejecución de las tareas del siguiente punto.
3. Buscar en el directorio el DN asociado al alias del usuario. El cliente efectúa una o más operaciones de búsqueda (lectura) o de actualización en el directorio. Estas operaciones son las vistas en la sección del Modelo
4. Si devuelve una entrada y solo una, este es el DN del usuario buscado. Si hay cero o más de una entrada se devolverá usuario no encontrado.
5. Re-bind al LDAP con el DN devuelto en el paso 4 y la password del paso 1.
6. Si el servidor LDAP permite el BIND el login ha tenido éxito, si no devuelve "password no válida".

A continuación se adjunta la captura de los paquetes intercambiados entre cliente y servidor mediante el Sniffer wireshark.

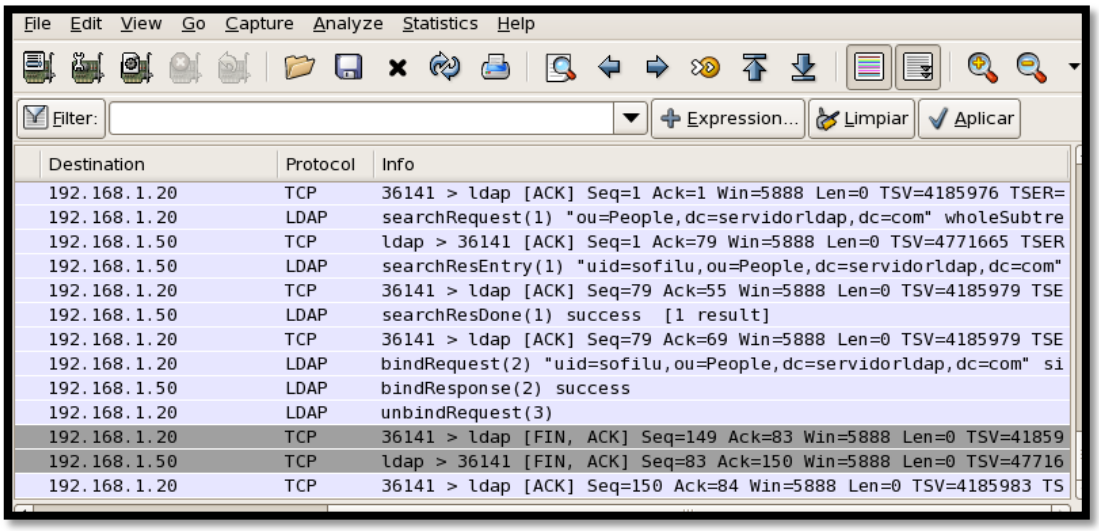


Figura III. 45 Paquetes Intercambiados con LDAP capturados con Wireshark

3.4.2.4. Módulo de Implementación y Funcionalidad

- **Facilidad de Instalación**

· Para montar el servidor LDAP es necesario instalar un conjunto de paquetes que son: openldap, openldap-servers, openldap-clients, openldap-devel.

· Generamos el password del administrador del servidor utilizando las función hash SSHA que es la más segura.

Figura III. 46 Resultado del Comando slappasswd

Se configura el archivo localizado en /etc/openldap/slapd.conf en él se copia la contraseña generada anteriormente y se modifica los parámetros de nombre del servidor.

Figura III. 47 Configuración del Archivo /etc/openldap/slapd.conf

· Editar el archivo /etc/openldap/ldap.conf, se ingresa la dirección IP del servidor y el nombre de dominio que se está usando.

Figura III. 48 Configuración del Archivo /etc/openldap/ldap.conf

- Editar el archivo /usr/share/openldap/migration/migrate_common.ph en el cual hay que especificar el dominio de la red.

```
# Default DNS domain
$DEFAULT_MAIL_DOMAIN = "servidorldap.com";

# Default base
$DEFAULT_BASE = "dc=servidorldap,dc=com";

# Turn this on for inetLocalMailReceipient
# sendmail support; add the following to
# sendmail.mc (thanks to Petr@Kristof.CZ):
##### CUT HERE #####
#define(`confLDAP_DEFAULT_SPEC',`-h "ldap.padl.com"')dnl
#LDAPROUTE_DOMAIN_FILE(`/etc/mail/ldapdomains')dnl
```

Figura III. 49 Configuración Archivo /usr/share/openldap/migration/migrate_common.ph

- Transformar las entradas del directorio en formato binario a formato LDIF que es el estándar para representar entradas en formato texto.

```
[root@localhost ~]# /usr/share/openldap/migration/migrate_base.pl > /etc/openlda
p/servidorldap.ldif
```

Figura III. 50 Comando para transformar un directorio binario a Formato LDIF

- **Facilidad de Seguimiento y Monitoreo**

- El servidor LDAP utiliza el recurso syslog para generar registros de su actividad. Pero este archivo no se crea automáticamente al instalar el servidor, sino que debe ser creado por el administrador. Y se localiza en /var/log/ldap.log.

```
[root@localhost log]# cat /var/log/ldap.log
Oct 24 23:49:25 localhost slapd[2823]: conn=5 fd=11 ACCEPT from IP=192.168.1.50:
46314 (IP=0.0.0.0:389)
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=0 SRCH base="ou=People,dc=servi
dorldap,dc=com" scope=2 deref=0 filter="(uid=sofilu)"
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=0 SRCH attr=1.1
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=0 SEARCH RESULT tag=101 err=0 n
entries=1 text=
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=1 BIND dn="uid=sofilu,ou=People
,dc=servidorldap,dc=com" method=128
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=1 BIND dn="uid=sofilu,ou=People
,dc=servidorldap,dc=com" mech=SIMPLE ssf=0
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=1 RESULT tag=97 err=0 text=
Oct 24 23:49:25 localhost slapd[2823]: conn=5 op=2 UNBIND
Oct 24 23:49:25 localhost slapd[2823]: conn=5 fd=11 closed
```

Figura III. 51 Resultado del Comando /var/log/ldap.log

- Al tener su propio archivo de logs ya creado, no se almacena ningún registro en el archivo general de logs del sistema que está localizado en /var/log/messages. Ahí solo se registra la actividad del resto de servicios.
- LDAP soporta monitoreo SNMP dando la posibilidad de configurar traps o notificaciones cada vez que un usuario se autentique en el servidor, o si existe alguna falla en el sistema.
- Existen varios software como Applications Manager que ofrece el monitoreo exhaustivo de la disponibilidad y el rendimiento del servidor LDAP. Con este podrá monitorear cuánto tiempo le tomó a un usuario iniciar sesión en el dominio y gracias al monitoreo del tiempo para iniciar sesión, el tiempo de respuesta y la disponibilidad, podrá constatar si el servidor LDAP funciona correctamente. Cuando se cruce algún umbral, recibirá una notificación vía email o SMS, lo que facilitará la localización y resolución rápida de problemas.

3.5. ANÁLISIS COMPARATIVO

Se presentan los resultados de los indicadores con sus respectivos índices y sus valoraciones después de haber realizado los escenarios de prueba.

3.5.1. Gestión de Usuarios

3.5.1.1. Determinación del Indicador

La sección de Gestión de Usuarios posee 3 índices, cada uno de los cuales fueron sometidos a diferentes pruebas. Los resultados obtenidos sirven para determinar el grado de facilidad con que se realizan las tareas de Gestión de Usuarios, de esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

TABLA III. VII VALORIZACIÓN PARA EL INDICADOR 1: GESTIÓN DE USUARIOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

Los Índices Ingreso, Modificación y Eliminación se valorizarán de acuerdo al número de pasos necesarios para realizar cada transacción.

TABLA III. VIII VALORIZACIÓN DE LOS ÍNDICES 1.1-3

Nº de Pasos	Valor Cualitativo
0-1	Alto
2-3	Medio
Mayor de 4	Bajo

3.5.1.2. Valoraciones

TABLA III. IX RESULTADOS DEL INDICADOR 1: GESTIÓN DE USUARIOS

Gestión de Usuarios		
Índice	**RADIUS**	**LDAP**
Ingreso	1	3
Modificación	1	2
Eliminación	1	2

3.5.1.3. Calificación

Se basa en la calificación de la TABLA III. VIII VALORIZACIÓN DE LOS ÍNDICES 1.1-3.

TABLA III. X CALIFICACIÓN DEL INDICADOR 1: GESTIÓN DE USUARIOS

Gestión de Usuarios		
Índice	**RADIUS**	**LDAP**
Ingreso	3	2
Modificación	3	2
Eliminación	3	2

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Ingreso de RADIUS

C2(X)= Valor de Índice Modificación de RADIUS

C3(X)= Valor de Índice Eliminación de RADIUS

C1(Y)= Valor de Índice Ingreso de LDAP

C2(Y)= Valor de Índice Modificación de LDAP

C3(Y)= Valor de Índice Eliminación de LDAP

Pa(X)= Valor Acumulativo de RADIUS

Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= ∑ C1(X) + C2(X) +C3(X)

Pa(Y)= ∑ C1(Y) + C2(Y) +C3(Y)

PpT(X)= Porcentaje parcial Total de RADIUS

PpT(Y)= Porcentaje parcial Total de LDAP

Vm= Valor máximo de Índices es 9

PpT(X)=(Cn(X)/Vm)*100%

PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. XI VALORES Y PORCENTAJES FINALES DEL INDICADOR 1: GESTIÓN DE USUARIOS, CON SUS RESPECTIVOS ÍNDICES

	GESTIÓN DE USUARIOS			
	RADIUS		**LDAP**	
	Valor(X)	**% PpT**	**Valor(Y)**	**% PpT**
Ingreso: C1	3	33,33	2	22,22
Modificación: C2	3	33,33	2	22,22
Eliminación: C3	3	33,33	2	22,22

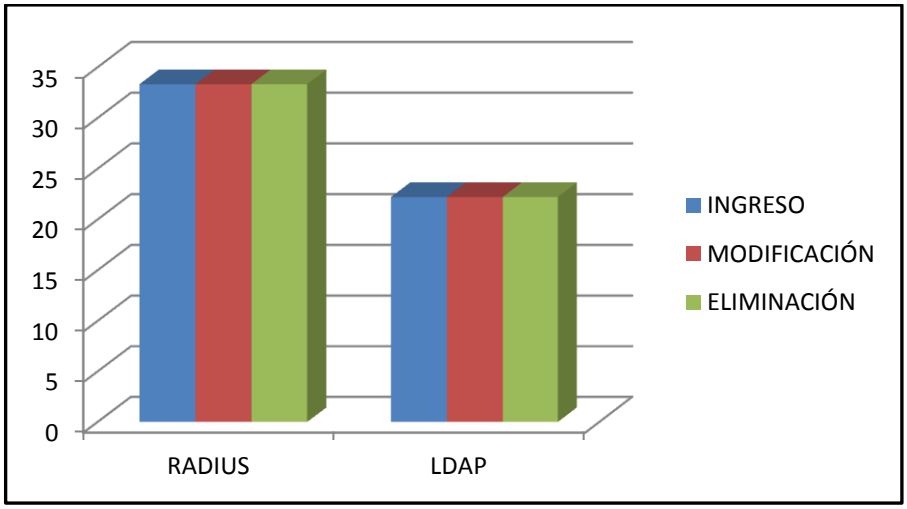


Figura III. 52 Resultado por índice del Indicador 1: Gestión de Usuarios

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (9/9)*100%

PT(X)=100%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (6/9)*100%

PT(Y)= 66,66%

TABLA III. XII VALORES Y PORCENTAJES FINALES DEL INDICADOR 1: GESTIÓN DE USUARIOS

	Gestión de Usuarios	
	Valor (Pa)	**% (PT)**
RADIUS: (X)	9	100
LDAP: (Y)	6	66,66

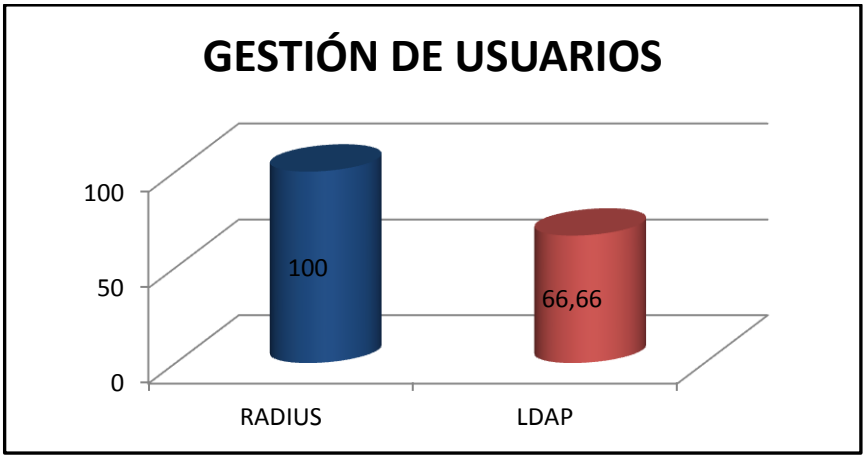


Figura III. 53 Resultado Final del Indicador 1: Gestión de Usuarios

3.5.1.4. Interpretación

TABLA III. XIII REPRESENTACIÓN DEL INDICADOR 1: GESTIÓN DE USUARIOS

Gestión de Usuarios		
Índice	**RADIUS**	**LDAP**
Ingreso	◊◊◊	◊◊
Modificación	◊◊◊	◊◊
Eliminación	◊◊◊	◊◊

3.5.1.5. Descripción de Resultados

Según los resultados expuestos en la tabla III. XIII "Representación del indicador 1: Gestión de usuarios" se explicaran por índices.

Ingreso: Las pruebas realizadas indican que RADIUS presenta mayor grado de facilidad al ingresar nuevos usuarios al sistema, ya que utiliza una interfaz gráfica que es bastante amigable e intuitiva para el administrador, y solo consiste en hacer clic sobre esta opción y llenar los datos requeridos para añadir una nueva entrada.

Cosa que no sucede con LDAP ya que requiere mayor conocimiento acerca de Linux, pues todo se realiza mediante líneas de comando, cada usuario requiere un archivo, en este se debe almacenar los datos que se crean necesarios pero respetando la sintaxis para no

generar errores el momento de añadir este archivo al servidor, mediante una línea de comando.

Modificación: en este índice también obtuvo mejor puntuación RADIUS, ya que para realizar algún cambio en los datos de usuarios almacenados, se ingresa al usuario y se cambia los datos que se requieran, para luego proceder a aplicarlos, mientras que en LDAP es mucho más complejo, ya que requiere la creación de un nuevo archivo indicando el nombre del comando que se va a ejecutar, que en este caso es modificar.

Además de indicar el atributo que se va a modificar y el valor por el cual se le va a remplazar, para luego mediante línea de comandos ejecutar el archivo que se creó anteriormente. Como se nota es necesario conocer claramente la sintaxis y comandos propios de LDAP. Aun así esta tarea se hace bastante tediosa.

Eliminación: para realizar esta tarea RADIUS únicamente requiere ingresar al usuario y elegir la opción eliminar usuarios y registros del servidor, para posteriormente proceder a aplicar los cambios realizados, en cambio en LDAP se requiere crear un nuevo script, en el cual se indica el uid del usuario a eliminar y el nombre del comando que se va a ejecutar, luego mediante comandos se ejecuta esta tarea.

Como se ha notado en los índices del indicador de gestión de usuarios, el servidor RADIUS, le lleva una gran ventaja a LDAP, facilitando de esta manera al administrador del sistema realizar la Gestión de Usuarios. Esto es muy importante ya que al tener una gran número de usuarios en el sistema y siendo estas tareas tan comunes, es necesario que sean lo mas fáciles posibles para su correcta administración.

3.5.2. Autentificación

Determinación del Indicador

La sección de Autentificación posee tres índices que fueron sometidos a prueba en el Módulo de Autentificación. Cada índice se valorizará por separado debido a sus distintas características.

3.5.2.1. Índice 2.1 Número de Instancias que Intervienen

En este indice se va a determinar el nivel de facilidad de implementación del Servidor de Autentificación con respecto al número de elementos que intervienen durante este proceso. De esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

III. XIV VALORIZACIÓN PARA EL ÍNDICE 2.1: NÚMERO DE INSTANCIAS QUE INTERVIENEN

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 2.1 se valorizará de acuerdo al número de instancias o elementos que intervienen en el proceso de Autentificación.

TABLA III. XV VALORIZACIÓN DEL ÍNDICE 2.1

Nº de Instancias	Valor Cualitativo
1-3	Alto
4-5	Medio
Mayor de 6	Bajo

- **Valoración**

TABLA III. XVI RESULTADOS DEL ÍNDICE 2.1

Autentificación		
Índice	**RADIUS**	**LDAP**
Número de Instancias que intervienen	3	4

- **Calificación**

TABLA III. XVII CALIFICACIÓN DEL ÍNDICE 2.1

Autentificación		
Índice	**RADIUS**	**LDAP**
Número de Instancias que intervienen	3	2

3.5.2.2. Índice 2.2 Cantidad de Paquetes Entrada/Salida

Este índice permite determinar el número de paquetes que se intercambian en la autentificación, de esta manera se establece una escala de valoración Alto, Medio y Bajo.

TABLA III. XVIII VALORIZACIÓN PARA EL ÍNDICE 2.2: CANTIDAD DE PAQUETES E/S

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊
Medio	2	◊◊
Bajo	3	◊◊◊

El Índice 2.2 se valorizará de acuerdo al número de paquetes propios del Protocolo que se intercambian el cliente y el servidor en el proceso de Autentificación.

TABLA III. XIX VALORIZACIÓN DEL ÍNDICE 2.2

Nº Paquetes E/S	Valor Cualitativo
1-3	Bajo
3-6	Medio
Mayor de 6	Alto

- **Valoración**

TABLA III. XX RESULTADOS DEL ÍNDICE 2.2

Autentificación		
Índice	**RADIUS**	**LDAP**
Cantidad de Paquetes Entrada/Salida	7	6

- **Calificación**

TABLA III. XXI CALIFICACIÓN DEL ÍNDICE 2.2

Autentificación		
Índice	**RADIUS**	**LDAP**
Cantidad de Paquetes Entrada/Salida	1	2

3.5.2.3. Tiempo de Autentificación

Los resultados permiten determinar el grado de rapidez con que se realiza el proceso de autentificación, de esta manera se establece una escala de valorización rápido, Medio y lento.

TABLA III. XXII VALORIZACIÓN PARA EL ÍNDICE 2.3: TIEMPO DE AUTENTIFICACIÓN

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Lento	1	◊
Medio	2	◊◊
Rápido	3	◊◊◊

El Índice 2.3 se valorizará de acuerdo al tiempo en mili segundos (ms) que toma el proceso de Autentificación.

TABLA III. XXIII VALORIZACIÓN DEL ÍNDICE 2.3

Tiempo en milisegundos	Valor Cualitativo
0-5	Rápido
05-10	Medio
Mayor de 10	Lento

- **Valoración**

TABLA III. XXIV RESULTADOS DEL ÍNDICE 2.3

Autentificación		
Índice	**RADIUS**	**LDAP**
Tiempo de Autentificación	17.43	2.35

- **Calificación**

TABLA III. XXV CALIFICACIÓN DEL ÍNDICE 2.3

Autentificación		
Índice	**RADIUS**	**LDAP**
Tiempo de Autentificación	1	3

TABLA III. XXVI CALIFICACIÓN DEL INDICADOR 2: AUTENTIFICACIÓN

Autentificación		
Índice	**RADIUS**	**LDAP**
Numero de Instancias que intervienen	3	2
Cantidad de Paquetes E/S	1	2
Tiempo de Conexión	1	3

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Número de Instancias que intervienen de RADIUS
C2(X)= Valor de Índice Cantidad de Paquetes Entrada/Salida de RADIUS
C3(X)= Valor de Índice Tiempo de Conexión de RADIUS

C1(Y)= Valor de Índice Número de Instancias que intervienen de LDAP
C2(Y)= Valor de Índice Cantidad de Paquetes Entrada/Salida de LDAP
C3(Y)= Valor de Índice Tiempo de Conexión de LDAP

Pa(X)= Valor Acumulativo de RADIUS
Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= ∑ C1(X) + C2(X) +C3(X)
Pa(Y)= ∑ C1(Y) + C2(Y) +C3(Y)

PpT(X)= Porcentaje parcial Total de RADIUS
PpT(Y)= Porcentaje parcial Total de LDAP
Vm= Valor máximo de Índices es 9

PpT(X)=(Cn(X)/Vm)*100%
PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. XXVII VALORES Y PORCENTAJES FINALES DEL INDICADOR 2: AUTENTIFICACIÓN CON SUS RESPECTIVOS ÍNDICES

	AUTENTIFICACIÓN			
	RADIUS		**LDAP**	
	Valor(X)	**% PpT**	**Valor(Y)**	**% PpT**
Nº Instancias: C1	3	33,33	2	22,22
Cant. Paquetes E/S: C2	1	11,11	2	22,22
Tiempo de Conexión: C3	1	11,11	3	33,33

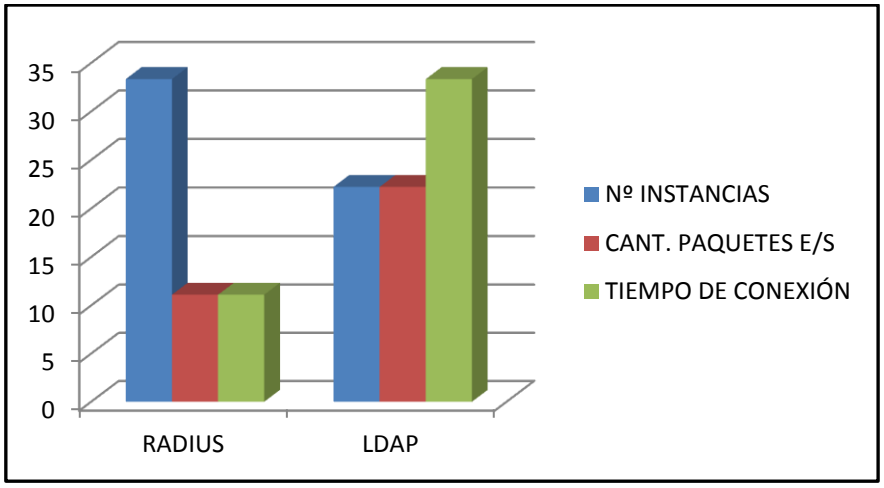


Figura III. 54 Resultado por índice del Indicador 2: Autentificación

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (5/9)*100%

PT(X)=55,56%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (7/9)*100%

PT(Y)= 77,78%

TABLA III. XXVIII VALORES Y PORCENTAJES FINALES DEL INDICADOR 2: AUTENTIFICACIÓN

	Autentificación	
	Valor (Pa)	**% (PT)**
RADIUS: (X)	5	55,56
LDAP: (Y)	7	77,78

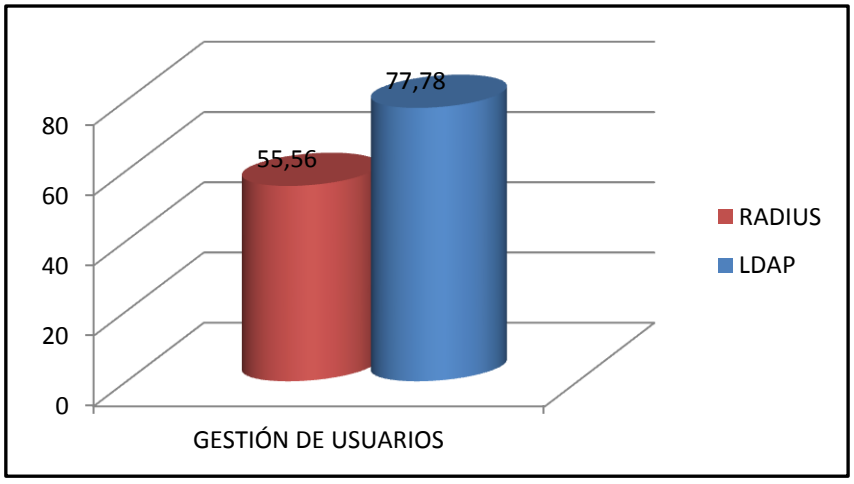


Figura III. 55 Resultado Final del Indicador 2: Autentificación

3.5.2.4. Interpretación

TABLA III. XXIX REPRESENTACIÓN DEL INDICADOR 2: AUTENTIFICACIÓN

Autentificación		
Índice	**RADIUS**	**LDAP**
Número de Instancias que Intervienen	◊◊◊	◊◊
Cantidad de Paquetes Entrada/Salida	◊	◊◊
Tiempo de Autentificación	◊	◊◊◊

3.5.2.5. Descripción de Resultados

De acuerdo con los resultados descritos en la tabla III. XXIX "Representación del indicador 2: Autentificación" se explicaran por índices.

Número de Instancias que Intervienen: RADIUS obtuvo mayor puntaje debido a que no requiere un servidor adicional para que sus usuarios puedan autentificarse en el servidor, cosa que no sucede con LDAP que necesita un Servidor Proxy adicional para realizar este proceso, ya que Windows por defecto no soporta autentificación LDAP y es necesario configurar un servidor intermediario que haga la conexión del servidor LDAP con el Access Point al que accede un usuario que desea autentificarse.

Cantidad de Paquetes Entrada/Salida: con respecto a este índice se destacó LDAP, ya que el número de paquetes que se intercambian entre el cliente y el servidor durante el

proceso de autentificación, es menor que en RADIUS. Desde el punto de vista del administrador es mejor que se transmitan menos paquetes, ya que esto generara una reducción del consumo de ancho de banda. Aunque la diferencia entre ambos servidores no es muy marcada, pues solo existe la diferencia de un paquete, pero al autentificar varios usuarios a la vez, esta diferencia será mucho más notable y determinante en la rapidez del proceso de autentificación para cada usuario. Para este análisis se tomó en cuenta únicamente los paquetes propios de cada servidor de autentificación.

Tiempo de Autentificación: en este índice LDAP tuvo una marcada diferencia con respecto a RADIUS. Ya que según las pruebas se determinó que en promedio LDAP es aproximadamente seis veces más rápido en autentificar a un usuario con respecto a RADIUS. Siendo esta la mejor ventaja que presenta este servidor, pero el gran inconveniente que presenta LDAP, es que al no ser una base de datos relacional, no está apta para realizar varios cambios de información simultáneos. Es por este motivo que LDAP se utiliza especialmente en empresas en donde la información que se almacena no sufrirá mayores cambios y permanecerá casi estática. En cambio RADIUS es más rápido en actualizar los cambios que se realizan en los datos del usuario.

3.5.3. Gestión de Datos

Determinación del Indicador

La sección de Gestión de Datos posee dos índices, los mismos que fueron sometidos a prueba en el Módulo de Transacciones de Alta y Baja. Cada índice se valorizará por separado de acuerdo a sus diferentes características.

3.5.3.1. Índice 3.1 Nivel de Acceso de Usuarios

Los resultados obtenidos del módulo de prueba realizado sirven para determinar el nivel de acceso que poseen los usuarios a la información almacenada en el Servidor. De esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

TABLA III. XXX VALORIZACIÓN PARA EL ÍNDICE 3.1: NIVEL DE ACCESO DE USUARIOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊◊◊
Medio	2	◊◊
Bajo	3	◊

El Índice 3.1 se valorizará de acuerdo a los permisos que poseen los Usuarios y el administrador para realizar la lectura, escritura y ejecución de la información de usuarios almacenada en los servidores.

TABLA III. XXXI VALORIZACIÓN DEL ÍNDICE 3.1

Tipo de Permiso	Valor Cualitativo
Usuario tiene permisos de Lectura y Escritura.	Alto
Usuario tiene permisos de Lectura.	Medio
Administrador tiene permisos de Lectura y Escritura.	Bajo

- **Valoración**

TABLA III. XXXI RESULTADOS DEL ÍNDICE 3.1: NIVEL DE ACCESO DE USUARIOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Nivel de Acceso de Usuarios	Bajo	Medio

- **Calificación**

TABLA III. XXXII CALIFICACIÓN DEL ÍNDICE 3.1: NIVEL DE ACCESO A USUARIOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Nivel de Acceso de Usuarios	3	2

3.5.3.2. Índice 3.2 Cantidad de Datos Utilizados

Estos resultados sirven para calificar al Servidor de acuerdo al número de datos que puede alojar el Servidor. De esta manera se realiza una escala de valorización Muy Bueno, Bueno y Regular.

TABLA VALORIZACIÓN III. XXXIII PARA EL ÍNDICE 3.2: CANTIDAD DE DATOS UTILIZADOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Muy Bueno	3	◊◊◊
Bueno	2	◊◊
Regular	1	◊

El Índice 3.2 se valorizará de acuerdo a la cantidad de tipo de datos que se pueden almacenar en el servidor de autentificación.

TABLA III. XXXIV VALORIZACIÓN DEL ÍNDICE 3.2

Tipo de Datos	Valor Cualitativo
Texto, Imágenes y Certificados Digitales	Muy Bueno
Texto y Certificados Digitales	Bueno
Texto e Imágenes	Regular

- **Valoración**

TABLA III. XXXV RESULTADOS DEL ÍNDICE 3.2: CANTIDAD DE DATOS UTILIZADOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Cantidad de Datos Utilizados	Bueno	Muy Bueno

- **Calificación**

TABLA III. XXXVI CALIFICACIÓN DEL ÍNDICE 3.2: CANTIDAD DE DATOS UTILIZADOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Cantidad de Datos Utilizados	2	3

TABLA III. XXXVII CALIFICACIÓN DEL INDICADOR 3: GESTIÓN DE DATOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Nivel de Acceso de Usuarios	3	2
Cantidad de Datos Utilizados	2	3

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Nivel de Acceso de Usuarios de RADIUS

C2(X)= Valor de Índice Cantidad de Datos Utilizados de RADIUS

C1(Y)= Valor de Índice Nivel de Acceso de Usuarios de LDAP

C2(Y)= Valor de Índice Cantidad de Datos Utilizados de LDAP

Pa(X)= Valor Acumulativo de RADIUS

Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= $\sum$ C1(X) + C2(X)

Pa(Y)= $\sum$ C1(Y) + C2(Y)

PpT(X)= Porcentaje parcial Total de RADIUS

PpT(Y)= Porcentaje parcial Total de LDAP

Vm= Valor máximo de Índices es 6

PpT(X)=(Cn(X)/Vm)*100%

PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. XXXVIII VALORES Y PORCENTAJES FINALES DEL INDICADOR 3: GESTIÓN DE DATOS CON SUS RESPECTIVOS ÍNDICES

	GESTIÓN DE DATOS			
	RADIUS		LDAP	
	Valor(X)	% PpT	Valor(Y)	% PpT
Nivel de Acceso de Usuarios: C1	3	50	2	33,33
Cantidad de Datos Utilizados: C2	2	33,33	3	50

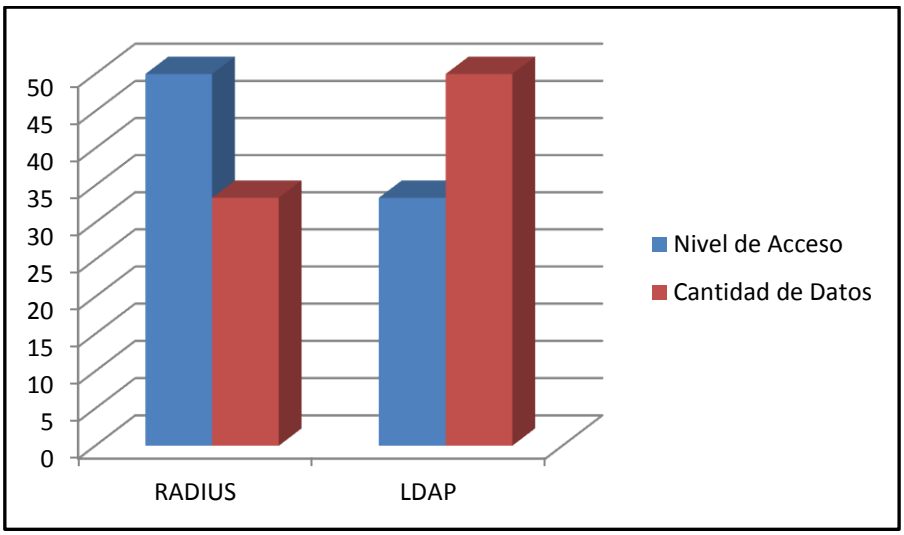


Figura III. 56 Resultado por índice del Indicador 3: Gestión de Datos

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (5/6)*100%

PT(X)=83,33%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (5/6)*100%

PT(Y)= 83,33%

TABLA III. XXXIX VALORES Y PORCENTAJES FINALES DEL INDICADOR 3: GESTIÓN DE DATOS

	Gestión de Datos	
	Valor (Pa)	% (PT)
RADIUS: (X)	5	83,33
LDAP: (Y)	5	83,33

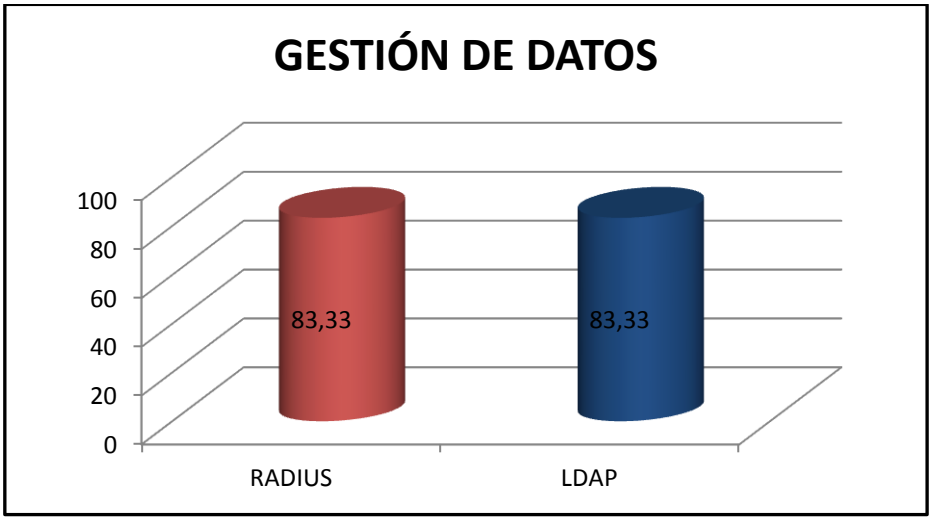


Figura III. 57 Resultado Final del Indicador 3: Gestión de Datos

3.5.3.3. Interpretación

TABLA III. XL REPRESENTACIÓN DEL INDICADOR 3: GESTIÓN DE DATOS

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Nivel de Acceso de Usuarios	◊◊◊	◊◊
Cantidad de Datos Utilizados	◊◊	◊◊◊

3.5.3.4. Descripción de Resultados

De acuerdo con los resultados mostrados en la tabla XL "Representación del indicador 3: Gestión de Datos" se explicaran por índices.

Nivel de Acceso de Usuarios: RADIUS posee mayor calificación debido a que solamente el administrador puede manipular los Datos de Usuario, es decir que está en la capacidad de leer y modificar todos los datos que están alojados en el servidor, mientras que en LDAP además de las tares descritas anteriormente que podrá hacer el administrador, un usuario

normal puede leer toda la información de los usuarios registrados en el sistema, aunque las claves se muestran encriptadas, este aspecto hace que LDAP tenga un gran problema en cuanto a seguridad, haciéndolo poco atractivo para su implementación por parte de los administradores de red.

Cantidad de Datos Utilizados: LDAP, además de almacenar Usuario y Password, puede alojar imágenes y Certificados Digitales. Haciéndolo más versátil ya que no está limitado al tipo de Datos que el servidor permite guardar. RADIUS también permite almacenar texto y certificados digitales pero no imágenes. Siendo no tan relevante ese tipo de datos, ya que algo fundamental es que puedan alojar en su sistema los certificados digitales, los cuales si son de gran importancia ya que ofrecerán mayor grado de seguridad en el proceso de autentificación. Aun así las imágenes servirían para personalizar la información de cada usuario.

3.5.4. Rendimiento

Determinación del Indicador

El indicador de Rendimiento posee tres índices, los mismos que fueron sometidos a prueba en el Módulo de Rendimiento. Cada índice se valorizará por separado de acuerdo a sus diferentes características.

3.5.4.1. Índice 4.1 Cantidad de Memoria Usada

Los resultados obtenidos del módulo sirven para determinar la cantidad de memoria que utiliza el servidor en funcionamiento. De esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

TABLA III. XLI VALORIZACIÓN PARA EL ÍNDICE 4.1: CANTIDAD DE MEMORIA USADA

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊
Medio	2	◊◊
Bajo	3	◊◊◊

El Índice 4.1 se valorizará de acuerdo al porcentaje de memoria total que utiliza el servidor cuando ya tiene autenticado usuarios en el sistema.

TABLA III. XLII VALORIZACIÓN DEL ÍNDICE 3.1

Porcentaje de Memoria Total Usada	Valor Cualitativo
0 – 30%	Bajo
31 – 60%	Medio
Mayor que 60%	Alto

- **Valoración**

TABLA III. XLIII RESULTADOS DEL ÍNDICE 4.1: CANTIDAD DE MEMORIA USADA

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Memoria Usada	85,21%	57,85%

- **Calificación**

TABLA III. XLIV CALIFICACIÓN DEL ÍNDICE 4.1: CANTIDAD DE MEMORIA USADA

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Memoria Usada	1	2

3.5.4.2. Índice 4.2 Nivel de Carga del CPU

Los resultados sirven para determinar el nivel de carga que tiene el CPU, en determinado intervalo de tiempo. De esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

TABLA III. XLV VALORIZACIÓN PARA EL ÍNDICE 4.2: NIVEL DE CARGA DEL CPU

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊
Medio	2	◊◊
Bajo	3	◊◊◊

El Índice 4.2 se valorizará de acuerdo a la carga promedio del procesador con respecto al sobretiempo de CPU y de E/S en los últimos periodos de 1, 5 y 10 minutos.

TABLA III. XLVI VALORIZACIÓN DEL ÍNDICE 4.2

Carga Promedio del CPU	Valor Cualitativo
0 – 30%	Bajo
31 – 60%	Medio
Mayor que 60%	Alto

- **Valoración**

TABLA III. XLVII RESULTADOS DEL ÍNDICE 4.2: NIVEL DE CARGA DEL CPU

Rendimiento		
Índice	**RADIUS**	**LDAP**
Nivel de Carga del CPU	71%	30%

- **Calificación**

TABLA III. XLVIII CALIFICACIÓN DEL ÍNDICE 4.2: NIVEL DE CARGA DEL CPU

Gestión de Datos		
Índice	**RADIUS**	**LDAP**
Cantidad de Datos Utilizados	1	3

3.5.4.3. Índice 4.3 Cantidad de Procesos

Los resultados permiten determinar el número de procesos del Servidor. Se establece una escala de valoración con los Niveles Alto, Medio y Bajo.

TABLA III. XLIX VALORIZACIÓN PARA EL ÍNDICE 4.3: CANTIDAD DE PROCESOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊
Medio	2	◊◊
Bajo	3	◊◊◊

El Índice 4.3 se valorizará de acuerdo al número de procesos generados por el Servidor en funcionamiento.

TABLA III. L VALORIZACIÓN DEL ÍNDICE 4.3

Nº de Procesos	Valor Cualitativo
1-3000	Bajo
3001-6000	Medio
Mayor que 6000	Alto

- **Valoración**

TABLA III. LI RESULTADOS DEL ÍNDICE 4.3

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Procesos	4066	4336

- **Calificación**

TABLA III. LII CALIFICACIÓN DEL ÍNDICE 4.3

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Procesos	2	2

TABLA III. LIII CALIFICACIÓN DEL INDICADOR 4: RENDIMIENTO

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Memoria Usada	1	2
Nivel de Carga del CPU	1	3
Cantidad de Procesos	2	2

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Cantidad de Memoria Usada de RADIUS

C2(X)= Valor de Índice Nivel de Carga del CPU de RADIUS

C3(X)= Valor de Índice Cantidad de Procesos de RADIUS

C1(Y)= Valor de Índice Cantidad de Memoria Usada de LDAP

C2(Y)= Valor de Índice Nivel de Carga del CPU de LDAP

C3(Y)= Valor de Índice Cantidad de Procesos de LDAP

Pa(X)= Valor Acumulativo de RADIUS

Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= $\sum$ C1(X) + C2(X) +C3(X)

Pa(Y)= $\sum$ C1(Y) + C2(Y) +C3(Y)

PpT(X)= Porcentaje parcial Total de RADIUS

PpT(Y)= Porcentaje parcial Total de LDAP

Vm= Valor máximo de Índices es 9

PpT(X)=(Cn(X)/Vm)*100%

PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. LIV VALORES Y PORCENTAJES FINALES DEL INDICADOR 4: RENDIMIENTO CON SUS RESPECTIVOS ÍNDICES

	RENDIMIENTO			
	RADIUS		**LDAP**	
	Valor(X)	**% PpT**	**Valor(Y)**	**% PpT**
Cantidad de Memoria Usada: C1	1	11,11	2	22,22
Nivel de Carga del CPU: C2	1	11,11	3	33,33
Cantidad de Procesos: C3	2	22,22	2	22,22

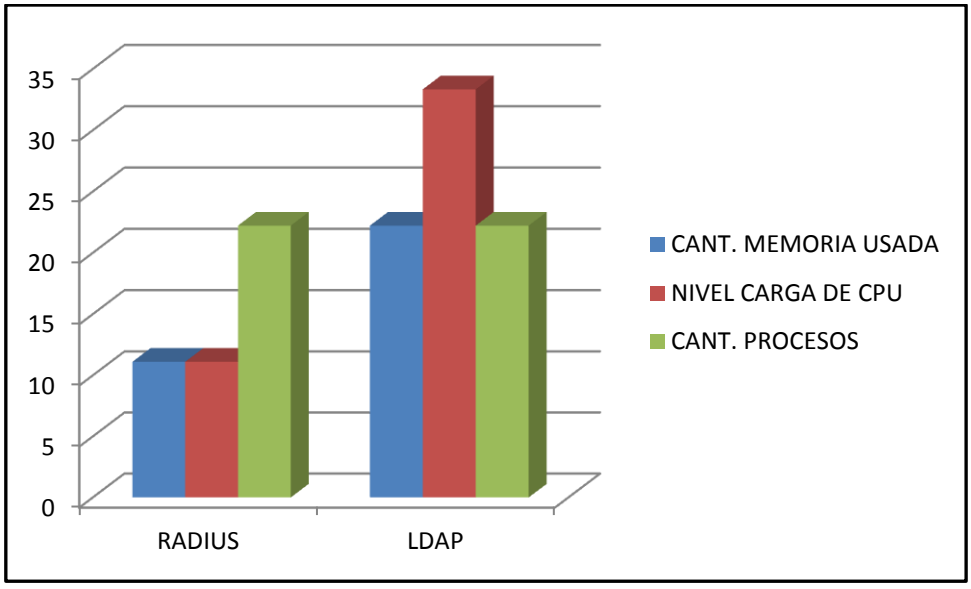


Figura III. 58 Resultado por índice del Indicador 4: Rendimiento

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (4/9)*100%

PT(X)=44,44%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (7/9)*100%

PT(Y)= 77,78%

TABLA III. LV VALORES Y PORCENTAJES FINALES DEL INDICADOR 4: RENDIMIENTO

	Rendimiento	
	Valor (Pa)	**% (PT)**
RADIUS: (X)	4	44,44
LDAP: (Y)	7	77,78

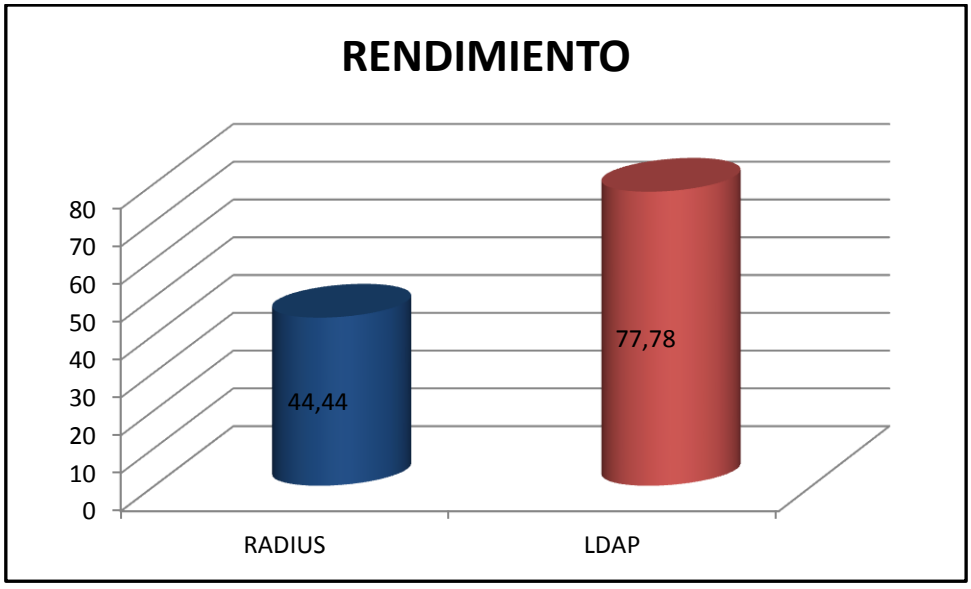


Figura III: 59 Resultado Final del Indicador 4: Rendimiento

3.5.4.4. Interpretación

TABLA III. LVI REPRESENTACIÓN DEL INDICADOR 4: RENDIMIENTO

Rendimiento		
Índice	**RADIUS**	**LDAP**
Cantidad de Memoria	◊	◊◊
Nivel Carga CPU	◊	◊◊◊
Cantidad de Procesos	◊◊	◊◊

3.5.4.5. Descripción de Resultados

Según los resultados detallados en la tabla III. LVI "Representación del indicador 4: Rendimiento" se explicaran por índices.

Cantidad de Memoria Usada: Este parámetro es muy importante debido a que se analiza la velocidad de funcionamiento que tendrá el servidor, RADIUS ocupa aproximadamente un 30% más memoria que LDAP. Esto es debido a que RADIUS intercambia mayor cantidad de paquetes durante el proceso de autentificación y en las distintas tareas que se pueden ejecutar en el servidor, consumiendo de esta forma mayor cantidad de memoria para atender a cada transacción que se realice.

Nivel de Carga de CPU: En este índice se impuso notablemente el servidor LDAP debido a que el nivel de carga que genera es aproximadamente un 40% menos de lo que genera RADIUS, esto se debe a que la cantidad de memoria utilizada va de la mano con el nivel de carga que presenta cada servidor, pues mientras más cantidad de tareas ejecuta un servidor más carga tendrá. Obviamente para un administrador lo óptimo es que estos dos valores tengan un valor mínimo, para garantizar la disponibilidad del servidor, y que no falle debido a una sobrecarga de usuarios conectados al sistema.

Cantidad de Procesos: LDAP produce aproximadamente un 10% más cantidad de procesos que RADIUS, sin embargo como se observó anteriormente, RADIUS presenta mayor carga, la explicación a esto es que los procesos que genera LDAP consumen menor cantidad de memoria y para su ejecución consumen poco tiempo de CPU, cosa que no sucede con RADIUS. En conjunto se puede notar que en cuanto al rendimiento LDAP es bastante superior pues es muy rápido en la ejecución de las tareas.

3.5.5. Funcionalidad

Determinación del Indicador

La sección de Funcionalidad posee cuatro índices, los mismos que fueron sometidos a prueba en el Módulo de Implementación y Funcionalidad. Cada índice se valorizará por separado debido a sus características.

3.5.5.1. Índice 5.1 Facilidad de Instalación

Los resultados permiten determinar el Grado de Facilidad que existe en el proceso de Instalación de cada servidor. De esta manera se establece una escala de Valorización con los niveles Alto, Medio y Bajo.

TABLA III. LVII VALORIZACIÓN PARA EL ÍNDICE 5.1: FACILIDAD DE INSTALACIÓN

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	1	◊
Medio	2	◊◊
Bajo	3	◊◊◊

El Índice 5.1 se valorizará de acuerdo al número de pasos necesarios para completar la instalación y configuración del Servidor para su funcionamiento.

TABLA III. LVIII VALORIZACIÓN DEL ÍNDICE 5.1

Nº de Pasos de Instalación	Valor Cualitativo
2-3	Bajo
4-5	Medio
Mayor que 6	Alto

- **Valoración**

TABLA III. LIX RESULTADOS DEL ÍNDICE 5.1: FACILIDAD DE INSTALACIÓN

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Instalación	4	6

- **Calificación**

TABLA III. LX CALIFICACIÓN DEL ÍNDICE 5.1: FACILIDAD DE INSTALACIÓN

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Instalación	2	1

3.5.5.2. Índice 5.2 Numero de Plataformas Soportadas

Determina el número de Plataformas en las que el Servidor puede ser implementado y permite determinar el nivel de Soporte de Plataformas por medio de la escala Alto, Medio y Bajo.

TABLA III. LXI VALORIZACIÓN PARA EL ÍNDICE 5.2: NÚMERO DE PLATAFORMAS SOPORTADAS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 5.2 se valorizará de acuerdo al soporte de los tres sistemas Operativos más populares: Linux, Microsoft y Sun/Solaris y sus respectivas versiones, de esta manera el nivel Alto corresponde al soporte de las 3 Plataformas principales.

TABLA III. LXII VALORIZACIÓN DEL ÍNDICE 5.2

Nº de Plataformas	Valor Cualitativo
3	Alto
2	Medio
1	Bajo

- **Valoración**

TABLA III. LXIII RESULTADOS DEL ÍNDICE 5.2: NÚMERO DE PLATAFORMAS SOPORTADAS

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Numero de Plataformas Soportadas	3	3

- **Calificación**

TABLA III. LXIV CALIFICACIÓN DEL ÍNDICE 5.2: NÚMERO DE PLATAFORMAS SOPORTADAS

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Numero de Plataformas Soportadas	3	3

3.5.5.3. Índice 5.3 Cantidad de Almacén de datos Soportados

Los resultados permiten determinar el número de Bases de Datos que soporta el Servidor. De estamanera se establece una escala con los valores Alto, Medio y Bajo.

TABLA III. LXV VALORIZACIÓN PARA EL ÍNDICE 5.3: CANTIDAD DE ALMACÉN DE DATOS SOPORTADOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 5.3 se valorizará de acuerdo al número de bases de Datos en las que el Servidor almacena la información de los Usuarios y Equipos y donde realiza las consultas durante el proceso de Autentificación.

TABLA III. LXVI VALORIZACIÓN DEL ÍNDICE 5.3

Nº de Almacén de datos Soportados	Valor Cualitativo
Mayor que 4	Alto
3-4	Medio
1-2	Bajo

- **Valoración**

TABLA III. LXVII RESULTADOS DEL ÍNDICE 5.: CANTIDAD DE ALMACÉN DE DATOS SOPORTADOS

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Cantidad de Almacén de datos Soportados	5	3

- **Calificación**

TABLA III. LXVIII CALIFICACIÓN DEL ÍNDICE 5.3

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Cantidad de Almacén de datos Soportados	3	2

3.5.5.4. Facilidad de Seguimiento y Monitoreo

Los resultados permiten determinar la facilidad que ofrece el Servidor para ser monitoreado durante su funcionamiento con una escala de valoración de Alto, Medio y Bajo.

TABLA III. LXIX VALORIZACIÓN PARA EL ÍNDICE 5.4: FACILIDAD DE SEGUIMIENTO Y MONITOREO

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 5.4 se valorizará de acuerdo al número de herramientas de monitoreo y seguimiento (cantidad) que ofrece el servidor.

TABLA III. LXX VALORIZACIÓN DEL ÍNDICE 5.4

Nº de Herramientas de Monitoreo	Valor Cualitativo
Mayor que 4	Alto
3-4	Medio
1-2	Bajo

- **Valoración**

TABLA III. LXXI RESULTADOS DEL ÍNDICE 5.4: FACILIDAD DE SEGUIMIENTO Y MONITOREO

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Seguimiento y Monitoreo	4	4

- **Calificación**

TABLA III. LXXII CALIFICACIÓN DEL ÍNDICE 5.4: FACILIDAD DE SEGUIMIENTO Y MONITOREO

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Seguimiento y Monitoreo	2	2

TABLA III. LXXIII CALIFICACIÓN DEL INDICADOR 5: FUNCIONALIDAD

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Instalación	2	1
Número de Plataformas Soportadas	3	3
Cantidad almacén de Datos	3	2
Facilidad de Seguimiento y Monitoreo	2	2

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Facilidad de Instalación de RADIUS

C2(X)= Valor de Índice Número de Plataformas Soportadas de RADIUS

C3(X)= Valor de Índice Cantidad almacén de Datos de RADIUS

C4(X)= Valor de Índice Facilidad de Seguimiento y Monitoreo de RADIUS

C1(Y)= Valor de Índice Facilidad de Instalación de LDAP

C2(Y)= Valor de Índice Número de Plataformas Soportadas de LDAP

C3(Y)= Valor de Índice Cantidad almacén de Datos de LDAP

C4(Y)= Valor de Índice Facilidad de Seguimiento y Monitoreo de RADIUS

Pa(X)= Valor Acumulativo de RADIUS

Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= $\sum$ C1(X) + C2(X) +C3(X) +C4(X)

Pa(Y)= $\sum$ C1(Y) + C2(Y) +C3(Y) +C4(Y)

PpT(X)= Porcentaje parcial Total de RADIUS

PpT(Y)= Porcentaje parcial Total de LDAP

Vm= Valor máximo de Índices es 12

PpT(X)=(Cn(X)/Vm)*100%

PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. LXXIV VALORES Y PORCENTAJES FINALES DEL INDICADOR 5: FUNCIONALIDAD CON SUS RESPECTIVOS ÍNDICES

	FUNCIONALIDAD			
	RADIUS		LDAP	
	Valor(X)	% PpT	Valor(Y)	% PpT
Facilidad de Instalación: C1	2	16,67	1	8,33
Num. Plataformas: C2	3	25	3	25
Cant. Almacén Datos: C3	3	25	2	16,67
Facilidad Monitoreo: C4	2	16,67	2	16,67

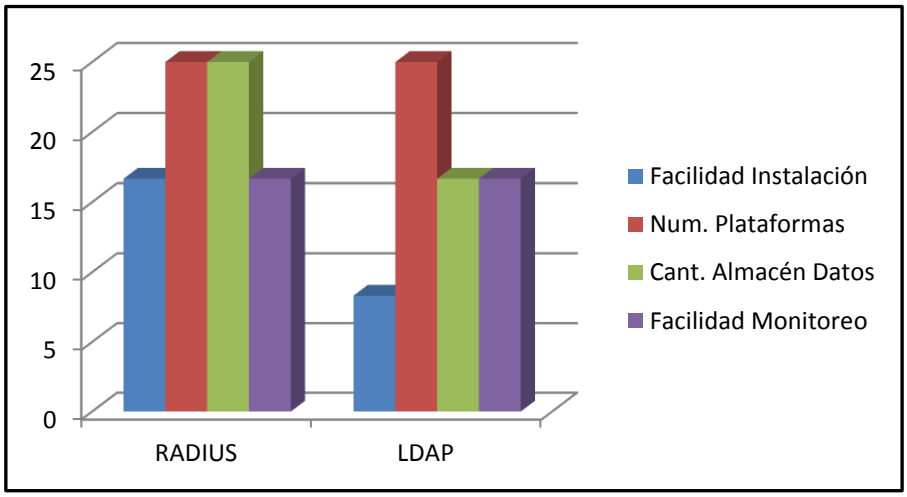


Figura III. 60 Resultado por índice del Indicador 5: Funcionalidad

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (10/12)*100%

PT(X)=83,33%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (8/12)*100%

PT(Y)= 66,67%

TABLA III. LXXV VALORES Y PORCENTAJES FINALES DEL INDICADOR 5: FUNCIONALIDAD

	Funcionalidad	
	Valor (Pa)	% (PT)
RADIUS: (X)	10	83,33
LDAP: (Y)	8	66,67

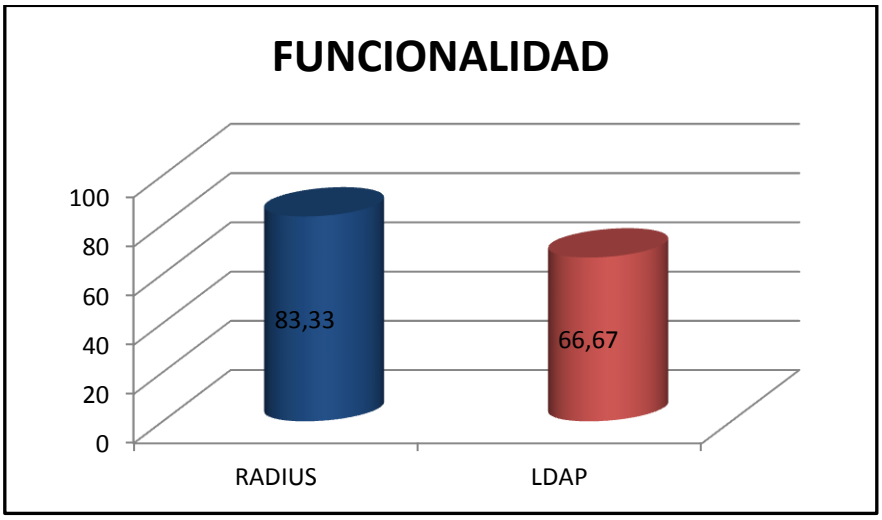


Figura III. 61 Resultado Final del Indicador 5: Funcionalidad

3.5.5.5. Interpretación

TABLA III. LXXVI REPRESENTACIÓN DEL INDICADOR 5: FUNCIONALIDAD

Funcionalidad		
Índice	**RADIUS**	**LDAP**
Facilidad de Instalación	◊◊	◊
Numero de Plataformas Soportadas	◊◊◊	◊◊◊
Cantidad de Almacén de datos Soportados	◊◊◊	◊◊
Facilidad de Seguimiento y Monitoreo	◊◊	◊◊

3.5.5.6. Descripción de Resultados

Según los resultados mostrados en la tabla III. LXXVI "Representación del indicador 5: Funcionalidad" se explicaran por índices.

Facilidad de Instalación: El servidor RADIUS obtuvo mayor puntaje debido a que presenta un mayor grado de facilidad, al requerir un menor número de pasos durante el proceso de instalación y una interfaz gráfica amigable con el usuario, sin embargo requiere un conocimiento medio de Linux, en cambio LDAP requiere tener un buen conocimiento de sistemas Linux, para editar y adecuar los archivos de configuración propios del servidor, además LDAP para poder funcionar en una red inalámbrica necesita de un servidor Proxy adicional, que trabajara como intermediario entre el usuario que se conecta al Access Point hacia el servidor. Como administradores de red es mejor que el proceso de instalación sea relativamente rápido y fácil.

Número de Plataformas Soportadas: Esta característica es importante ya que determina la versatilidad que presenta cada servidor, al ser adaptable en cualquier tipo de Plataforma. En este caso los dos servidores de autentificación presentan versiones compatibles con las tres plataformas principales que se manejan.

Cantidad de Almacén de datos Soportados: RADIUS presenta la posibilidad de elegir el tipo de almacén de datos queremos utilizar, dependiendo del tipo de información y a que empresa está destinada, soporta base de datos de tipo relacional como mysql, la cual soporta varias transacciones simultáneas, en cambio LDAP no proporciona un almacén de datos de este tipo, en cambio permite transformar los usuarios del sistema a usuarios de LDAP. Debido a la variedad de almacén de datos con la que RADIUS es compatible obtuvo mayor calificación frente a LDAP.

Facilidad de Seguimiento y Monitoreo: Los dos servidores obtuvieron la misma calificación, ya que soportan varias herramientas de monitoreo, especialmente SNMP que proporciona la posibilidad de generar avisos o interrupciones cuando el servidor falle, además generan sus propios archivos de log que informan todo lo que sucede durante cada transacción.

3.5.6. Seguridad

Determinación del Indicador

La sección de Seguridad posee cuatro índices, los mismos que fueron sometidos a prueba en el Módulo de Implementación y Funcionalidad. Cada índice se valorizará por separado de acuerdo a sus características.

3.5.6.1. Índice 6.1 Soporte de Cifrado

Los resultados obtenidos del módulo sirven para determinar si el servidor soporta cifrado o no. De esta manera se realiza una escala de valorización con la respuesta si o no.

TABLA III. LXXVII VALORIZACIÓN PARA EL ÍNDICE 6.1: SOPORTE DE CIFRADO

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Si	1	◊
No	0	

- **Valoración**

TABLA III. LXXVIII RESULTADOS DEL ÍNDICE 6.1: SOPORTE DE CIFRADO

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Cifrado	Si	Si

- **Calificación**

TABLA III. LXXIX CALIFICACIÓN DEL ÍNDICE 6.1: SOPORTE DE CIFRADO

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Cifrado	1	1

3.5.6.2. Índice 6.2 Cantidad de Protocolos Soportados

Los resultados sirven para determinar los protocolos criptograficos que soporta el servidor. De esta manera se realiza una escala de valorización con los niveles alto, medio y bajo.

TABLA III. LXXX VALORIZACIÓN PARA EL ÍNDICE 6.2: CANTIDAD DE PROTOCOLOS SOPORTADOS

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 6.2 se valorizará de acuerdo al número de protocolos de cifrado que soporta el servidor de autentificación.

TABLA III. LXXXI VALORIZACIÓN DEL ÍNDICE 6.2

Nº de Protocolos	Valor Cualitativo
0 - 2	Bajo
3-4	Medio
Mayor que 4	Alto

- **Valoración**

TABLA III. LXXXII RESULTADOS DEL ÍNDICE 6.2: CANTIDAD DE PROTOCOLOS SOPORTADOS

Seguridad		
Índice	**RADIUS**	**LDAP**
Cantidad de Protocolos Soportados	1	2

- **Calificación**

TABLA III. LXXXIII CALIFICACIÓN DEL ÍNDICE 6.2

Seguridad		
Índice	**RADIUS**	**LDAP**
Cantidad de Protocolos Soportados	1	1

3.5.6.3. Índice 6.3 Soporte de Funciones Hash

Los resultados permiten determinar las funciones hash que puede utilizar el servidor para cifrar los datos en el proceso de autentificación. Se establece una escala de valoración con los Niveles Alto, Medio y Bajo.

TABLA III. LXXXIV VALORIZACIÓN PARA EL ÍNDICE 6.3: SOPORTE DE FUNCIONES HASH

Valor Cualitativo	Valor Cuantitativo	Valor Representativo
Alto	3	◊◊◊
Medio	2	◊◊
Bajo	1	◊

El Índice 6.3 se valorizará de acuerdo al número de funciones hash que soporta el servidor.

TABLA III. LXXXV VALORIZACIÓN DEL ÍNDICE 6.3

Nº de Funciones Hash	Valor Cualitativo
1 – 3	Bajo
4 – 6	Medio
Mayor que 6	Alto

- **Valoración**

TABLA III. LXXXVI RESULTADOS DEL ÍNDICE 6.3: SOPORTE DE FUNCIONES HASH

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Funciones Hash	4	6

- **Calificación**

TABLA III. LXXXVII CALIFICACIÓN DEL ÍNDICE 6.3: SOPORTE DE FUNCIONES HASH

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Funciones Hash	2	2

TABLA III. LXXXVIII CALIFICACIÓN DEL INDICADOR 6: SEGURIDAD

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Cifrado	1	1
Cantidad de Protocolos soportados	1	1
Soporte de Funciones Hash	2	2

Para sacar los porcentajes se utilizarán las siguientes fórmulas:

X= Servidor RADIUS

Y= Servidor LDAP

C1(X)= Valor de Índice Soporte de Cifrado de RADIUS

C2(X)= Valor de Índice Cantidad de Protocolos soportados de RADIUS

C3(X)= Valor de Índice Soporte de Funciones Hash de RADIUS

C1(Y)= Valor de Índice Soporte de Cifrado de LDAP

C2(Y)= Valor de Índice Cantidad de Protocolos soportados de LDAP

C3(Y)= Valor de Índice Soporte de Funciones Hash de LDAP

Pa(X)= Valor Acumulativo de RADIUS

Pa(Y)= Valor Acumulativo de LDAP

Pa(X)= ∑ C1(X) + C2(X) +C3(X)

Pa(Y)= ∑ C1(Y) + C2(Y) +C3(Y)

PpT(X)= Porcentaje parcial Total de RADIUS

PpT(Y)= Porcentaje parcial Total de LDAP

Vm= Valor máximo de Índices es 7

PpT(X)=(Cn(X)/Vm)*100%

PpT(Y)=(Cn(Y)/Vm)*100%

TABLA III. LXXXIX VALORES Y PORCENTAJES FINALES DEL INDICADOR 6: SEGURIDAD CON SUS RESPECTIVOS ÍNDICES

	SEGURIDAD			
	RADIUS		LDAP	
	Valor(X)	% PpT	Valor(Y)	% PpT
Soporte Cifrado: C1	1	14,29	1	14,29
Cantidad de Protocolos Soportados: C2	1	14,29	1	14,29
Soporte Funciones Hash: C3	2	28,57	2	28,57

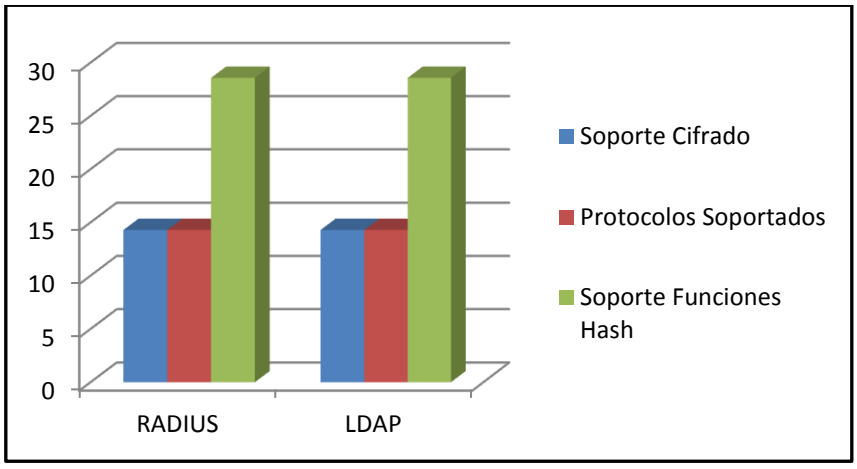


Figura III. 62 Resultado por índice del Indicador 6: Seguridad

Para sacar los porcentajes de cada índice se utilizara las siguientes formulas, donde:

PT(X)= Porcentaje Total de RADIUS

PT(Y)= Porcentaje Total de LDAP

PT(X)=(Pa(X)/Vm)*100%

PT(X)= (4/7)*100%

PT(X)= 57,14%

PT(Y)= (Pa(Y)/Vm)*100%

PT(Y)= (4/7)*100%

PT(Y)= 57,14%

TABLA III. XC VALORES Y PORCENTAJES FINALES DEL INDICADOR 6: SEGURIDAD

	Seguridad	
	Valor (Pa)	% (PT)
RADIUS: (X)	4	57,14
LDAP: (Y)	4	57,14

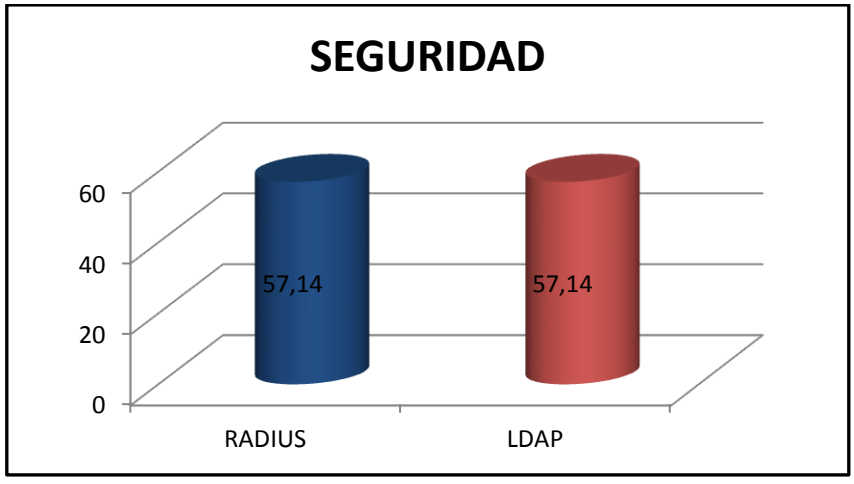


Figura III. 63 Resultado Final del Indicador 6: Seguridad

3.5.6.4. Interpretación

TABLA III. XCI REPRESENTACIÓN DEL INDICADOR 6: SEGURIDAD

Seguridad		
Índice	**RADIUS**	**LDAP**
Soporte de Cifrado	◊	◊
Cantidad de Protocolos Soportados	◊	◊
Soporte de Funciones Hash	◊◊	◊◊

3.5.6.5. Descripción de Resultados

Tanto el servidor LDAP como RADIUS ofrecen varios mecanismos de seguridad para proteger la información que se transmite durante el proceso de autentificación, ya que esta es muy sensible al tratarse de nombre de usuario y contraseña; y por esta misma razón debe estar muy protegida para evitar que personas mal intencionadas capturen este tipo de datos y traten de alterar el funcionamiento del servidor.

Para proporcionar este nivel de seguridad ambos servidores tienen la posibilidad de utilizar protocolos, algoritmos y funciones hash, necesarias para realizar un cifrado de los datos del usuario principalmente en el proceso de autentificación. Ambos servidores están a la par únicamente que LDAP soporta un mayor número de funciones hash.

Además un aspecto muy importante que ambos servidores tienen, es la posibilidad de utilizar certificados digitales en lugar de pedir usuario y contraseña en el proceso de autentificación, obviamente esto le añade mayor nivel de seguridad pues los certificados digitales proporcionan un mayor grado de seguridad. Por las razones mencionadas, los dos servidores obtuvieron la misma puntuación.

3.6. Puntuación obtenida

Se presenta una tabla de resumen sobre la calificación obtenida por RADIUS y LDAP en cada uno de los índices.

TABLA III. XCII RESUMEN DE LOS PUNTAJES OBTENIDOS POR CADA SERVIDOR DETALLADOS POR INDICADORES

INDICADOR	ÍNDICES	SERVIDOR	
		RADIUS	LDAP
Gestión de Usuarios	Ingreso	3	2
	Modificación	3	2
	Eliminación	3	2
Autentificación	Número de Instancias que Intervienen	3	2
	Cantidad de Paquetes Entrada/Salida	1	2
	Tiempo de Conexión	1	3
Gestión de Datos	Nivel de Acceso de Usuarios	3	2
	Cantidad de Datos Utilizados	2	3
Rendimiento	Cantidad de Memoria Usada	1	3
	Nivel de Carga del CPU	1	2
	Cantidad de Procesos	2	2
Funcionalidad	Facilidad de Instalación	2	1
	Número de Plataformas soportadas	3	3
	Cantidad de Almacén de Datos soportados	3	2
	Facilidad de Seguimiento y Monitoreo	2	2
Seguridad	Soporte de Cifrado	1	1
	Cantidad de Protocolos soportados	1	1
	Soporte de Funciones HASH	2	2
TOTAL		37	37

Se presenta una Tabla con los valores totales de cada Indicador y el valor máximo.

TABLA III. XCIII PUNTAJE TOTAL

Indicador	Valor Máximo	RADIUS		LDAP	
		Calificación	Porcentaje (%)	Calificación	Porcentaje (%)
Gestión de Usuarios	9	9	100	6	66.66
Autentificación	9	5	55,55	7	77,77
Gestión de Datos	6	5	83,33	5	83,33
Rendimiento	9	4	44,44	7	77,77
Funcionalidad	12	10	83,33	8	66,66
Seguridad	7	4	57,14	4	57,14
TOTAL	52	37	71,15	37	71,15

Para determinar el Servidor más eficiente se asigna un peso a cada Indicador de acuerdo a la importancia que tiene desde el punto de vista del Administrador del Sistema.

TABLA III. XCIV ASIGNACIÓN DE PESOS A CADA INDICADOR SEGÚN SU IMPORTANCIA

Indicador	Ponderación (%)
Gestión de Usuarios	20
Autentificación	15
Gestión de Datos	15
Rendimiento	10
Funcionalidad	25
Seguridad	15
TOTAL	100%

Como se observa en la Tabla III. XCIV, el Indicador de mayor importancia es **Funcionalidad,** debido a que comprende la facilidad de instalación del Servidor, la configuración y puesta en marcha del mismo, las plataformas y Bases de Datos que soporta, así como la capacidad de monitorear el Sistema para controlar el funcionamiento.

En lo que se refiere a **Gestión de Usuarios,** este proceso debe ser fácil e intuitivo, para que de esta manera el ingreso o modificación de varios Usuarios no se vuelva una tarea compleja o sobrecargue la capacidad del servidor, por este motivo este indicador adquiere gran importancia, el servidor elegido debe adaptarse tanto en empresas pequeñas como grandes.

La **Seguridad** es algo fundamental en un ambiente de red, pero en este caso no se ha asignado un peso muy alto, debido a que ambos servidores ofrecen casi los mismos mecanismos de seguridad, no existe una diferencia notable en este parámetro.

El **Rendimiento** determinara la velocidad con las que se realizan las tareas de gestión de datos de los usuarios del sistema, y es de mucha importancia para el usuario, pero le asignamos el peso más bajo puesto esto estará directamente relacionado con las características físicas que tenga el servidor, además como se mencionó anteriormente el servidor RADIUS presenta mayor carga, sin embargo LDAP necesita un servidor adicional para su funcionamiento, lo que hará que también en este indicador ambos servidores se encuentren a la par.

3.7. Calificación del Servidor

Se califica cada indicador tanto de RADIUS como LDAP de acuerdo al peso asignado a cada indicador.

TABLA III. XCV CALIFICACIÓN DE LOS INDICADORES DE CADA SERVIDOR SEGÚN LOS PESOS ASIGNADOS

Indicador	Peso	RADIUS	LDAP
Gestión de Usuarios	20	20	13,33
Autentificación	15	8,33	11,67
Gestión de Datos	15	12,5	12,5
Rendimiento	10	4,44	7,78

Funcionalidad	25	20,83	16,67
Seguridad	15	8,57	8,57
TOTAL		74,67	70,52

3.8. Interpretación

Los resultados obtenidos en los módulos de prueba realizados muestran las fortalezas y debilidades que posee cada servidor de autentificación, los cuales están detallados en el desarrollo del análisis comparativo.

En el indicador Gestión de Usuarios, los servidores presentan una gran diferencia RADIUS con 100% frente a LDAP con 66.66%, y prácticamente es el parámetro que ha determinado que servidor es el más eficiente para ser posteriormente implementado, pues en el resto de indicadores la calificación de los servidores no tiene mucha diferencia. En este indicador se destacó notablemente RADIUS, ya que las tres tareas principales que un administrador ejecuta con mayor frecuencia como son el ingreso, modificación y eliminación de usuarios, son mucho más fáciles de realizar que en LDAP, ya que posee una interfaz gráfica muy intuitiva que hace estas tareas presenten menor complejidad.

Con los resultados del módulo de Implementación y analizando las características propias de cada servidor, se observa que destaca RADIUS, debido a que es un 20% más fácil de instalar que LDAP y no requiere un conocimiento avanzado de sistemas Linux, es compatible con la mayoría de plataformas y soporta un gran conjunto de almacén de datos, haciendo que este servidor sea más versátil al momento de su implementación.

RADIUS fue desarrollado para soportar un gran número de usuarios y varias transacciones simultáneas debido a la facilidad con la que se pueden realizar estas tareas. Por esta razón es

usado por ISPs para controlar el acceso de sus Usuarios y facturar los servicios, lo que no ocurre con LDAP ya que al no ser una base de datos relacional los cambios en la información almacenada resultan más complejos, además está orientado a empresas donde la información no está en modificación constante.

En cuanto a la seguridad ambos servidores, se encuentran en similar condición, debido a que soportan cifrado y una variedad de funciones hash que permiten un proceso de autentificación bastante seguro.

En el indicador de Rendimiento se evaluó la utilización de los recursos Hardware durante la realización de todas las tareas de las pruebas efectuadas y destaca LDAP, debido a que presenta aproximadamente un 42% menos de carga que RADIUS, sin embargo al necesitar de un servidor adicional para su funcionamiento obviamente va a consumir muchos más recursos, incluso para su implementación se hace mucho más complicado, ya que se debe realizar una conexión entre el servidor LDAP y el Proxy que actúa como un intermediario.

En el indicador Autentificación, LDAP se impone sobre RADIUS con un porcentaje aproximado del 28%, esto se debe a que tarda menos en autentificar a un cliente a pesar de que intercambia mayor número de paquetes y necesita de un elemento adicional como es el proxy.

Al final, con las pruebas realizadas, la puntuación de los dos servidores es similar, RADIUS obtuvo la mayor puntuación debido al conjunto de características óptimas que reúne, para ser fácilmente adaptable a todo tipo de empresa.

3.9. Análisis de Resultados

Después de la interpretación de resultados realizado anteriormente, destaca el servidor RADIUS como el idóneo para desarrollar la implementación del prototipo de servidor de

autentificación, para una red inalámbrica, que va de acuerdo a los objetivos planteados al inicio de la tesis, debido a que RADIUS presenta un conjunto de características que facilitan la gestión de usuarios, soporta una variedad de almacén de datos, es compatible con la mayoría de plataformas, puede alojar certificados digitales para aumentar el nivel de seguridad durante el proceso de autentificación, permite realizar cambios constantes y de varios usuarios simultáneamente en la información almacenada debido a que soporta base de datos de tipo relacional y cuenta con varios mecanismos de seguimiento y monitoreo del sistema.

En conclusión por contar con un gran conjunto de ventajas frente al servidor LDAP y con la experiencia de haber montado los escenarios de prueba, se concluye que el servidor RADIUS es el más eficaz para implementar un prototipo adaptable a todo tipo de red inalámbrica.

3.10. Comprobación de Hipótesis

La hipótesis planteada es:

Hi: La implementación de un servidor LDAP proporciona una mayor eficiencia en la autentificación de usuarios en una red inalámbrica frente a un Servidor RADIUS.

La hipótesis descrita anteriormente es de tipo descriptiva, por tal motivo no posee variables dependientes e independientes.

Según la Tabla III. XCV Calificación de los Indicadores de cada servidor según los pesos asignados se establece que:

TABLA III. XCVI EFICIENCIA DEL SERVIDOR

Indicador	RADIUS	LDAP
Gestión de Usuarios	20	13,33
Autentificación	8,33	11,67

Gestión de Datos	12,5	12,5
Rendimiento	4,44	7,78
Funcionalidad	20,83	16,67
Seguridad	8,57	8,57
EFICIENCIA	74,67%	70,52%

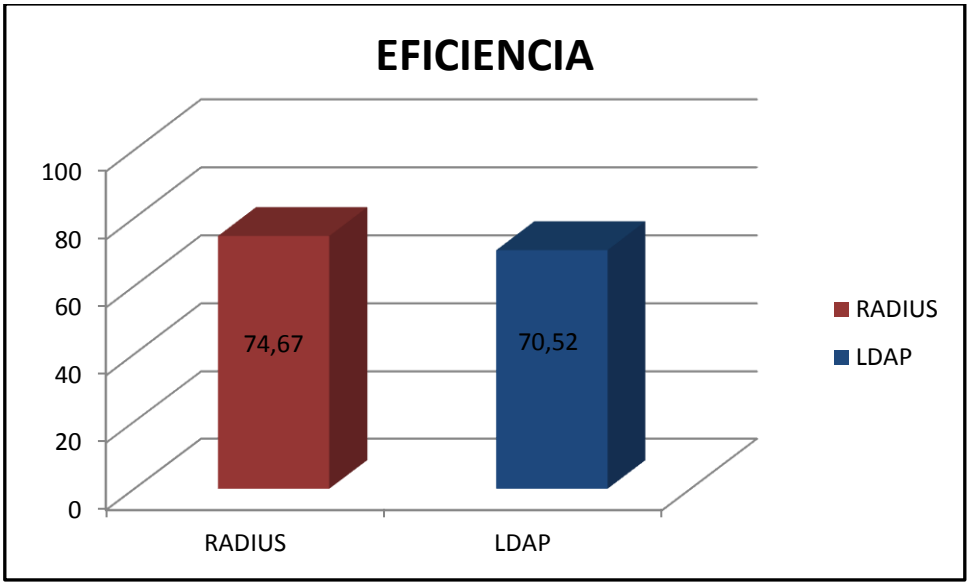


Figura III. 64 Resultado final del análisis

Conclusión: Haciendo referencia a la tabla III. XCVI y por observación directa, se concluye que el servidor RADIUS posee el valor más alto 74,67% frente a LDAP con el 70,52%, superándolo de esta manera en aproximadamente un 6%. De esta manera se concluye que la Hipótesis Hi es nula, debido al conjunto de ventajas que posee el servidor RADIUS en relación a LDAP, las cuales han sido determinadas después del análisis de los respectivos indicadores, estos indican a RADIUS como el servidor más eficiente al momento de autentificar usuarios en una red inalámbrica.

CAPITULO IV

MARCO PROPOSITIVO

4.1. IMPLEMENTACIÓN DEL PROTOTIPO DE SERVIDOR DE AUTENTIFICACIÓN

Una vez seleccionado RADIUS como servidor de autentificación, además de haber adquirido el suficiente conocimiento acerca de su configuración y funcionamiento se procede con la implementación del prototipo. En este capítulo serán descritos todos los elementos y requerimientos necesarios para el correcto funcionamiento del servidor.

4.2. HARDWARE

Para la implementación se utilizó un AP LYNKSYS GIGABIT WIRELESS-N modelo WRT310N de propiedad de la Academia CISCO de la Escuela Superior Politécnica de Chimborazo.

4.2.1. Access Point LYNKSYS WRT310N

Figura IV. 65 AP LYNKSYS WRT310N

Este Router Wireless permite conexiones estables y de suficiente ancho de banda para navegar por Internet, descargar archivos MP3, hacer llamadas telefónicas de Internet VOIP, compartir archivos, jugar juegos de red, y el flujo de alta definición videos. Alto rendimiento inalámbrico para múltiples usuarios y multimedia streaming, especialmente para los grandes hogares y pequeñas y medianas oficinas. Muy rápido y potente de 300 Mbps.

4.2.1.1. Características

- Funciona como Router, Switch y como Access Point, todo en uno.
- Todos los puertos soportan velocidad GIGABIT Y Auto-Crossover (MDI/MDI-X).
- Access point de velocidad y alcance mejorados integrado.
- Estándares IEEE 802.11n, IEEE 802.3, IEEE 802, IEEE 802.11g, IEEE 802.11b
- Cuenta con los siguientes puertos: 4 Ethernet GIGABIT, 1 internet, 1 corriente.
- Acceso wifi protegido a través de WPA2.
- Filtrado de direcciones MAC inalámbrico.

- Poderoso Firewall SPI y Seguridad con clave de 128 Bits.
- Soporta dispositivos con normas 802.11 b, g y n.

4.2.1.2. Características Técnica

- Increíble cobertura y rendimiento para su hogar conectado
- Router para compartición de Internet y switch (conmutador) Gigabit de 4 puertos con un punto de acceso inalámbrico integrado de mayor velocidad y alcance
- La tecnología MIMO utiliza múltiples radios por banda para crear potentes señales para máximo alcance y velocidad, con menos puntos muertos
- Mucho más rápida que la tecnología inalámbrica g, pero también funciona bien con dispositivos inalámbricos b y g.
- Señales inalámbricas protegidas por codificación tipo industrial y su red queda protegida de los ataques de Internet mediante un potente cortafuegos (firewall).
- Alimentación Externa, 12 V CC, 0,5 A
- Certificación FCC, UL, CE, Wi-Fi (802.11b, 802.11g, 802.11n), WPA2, WMM
- Temperatura de funcionamiento 0 °C a 40 °C (32 °F a 104 °F)
- Temperatura de almacenamiento -20 °C a 60 °C (-4 °F a 140 °F)
- Humedad de funcionamiento 10% a 85% sin condensación
- Humedad de almacenamiento 5% a 90% sin condensación

4.2.1.3. Requisitos mínimos

- Internet Explorer 6.0 o Firefox 1.0 o superior para la configuración basada en Web
- Unidad de CD-ROM
- Windows XP, Vista or Vista 64-bit edition

4.3. HERRAMIENTAS Y SOFTWARE

Para la implementación del servidor de autentificación RADIUS se va a utilizar la siguiente herramienta:

4.3.1. Zeroshell

Zeroshell es una potente herramienta que permite disponer rápidamente de un servidor Radius sin tener que montar toda la infraestructura software que ello requiere y evitando la complejidad que supone, además de una fácil e intuitiva forma de administración de certificados digitales. Es una distribución OpenSource para servidores y dispositivos embebidos cuyo objetivo es ofrecer los principales servicios que una red LAN o WLAN requiere, como por ejemplo:

- DHCP
- DNS.
- Firewall.
- VLAN.
- VPN.
- RADIUS.
- LDAP.
- Portal Cautivo

4.3.1.1. Ventajas

- La posibilidad de configurar ZeroShell desde un terminal o vía ssh, para usuarios avanzados. No obstante, también puede ser administrado de forma remota desde un navegador gracias a que dispone de una interfaz web.

- Pero la principal ventaja es que no requiere ser instalado en disco duro, ya que funciona directamente en modo live desde un CD o incluso en un dispositivo USB, lo que permite tener un servidor altamente disponible.
- Los datos y ajustes se almacenan en una base de datos que puede ser almacenada en discos ATA, SATA, SCSI y USB. Cuando se configura, se crea un perfil. Ese perfil se puede copiar a otro equipo y, en caso de avería de la máquina, tener funcionando de nuevo el servidor en pocos minutos. Además, si tenemos guardado un perfil en el equipo, al arrancar ZeroShell lo detectará y directamente lo cargará.
- La base de datos se puede almacenar en un equipo que ya tenga un sistema operativo instalado sin destruir nada. El sistema de ficheros donde se almacena puede ser ext2, ext3, reiserfs o fat32.
- Otra opción para tener un servidor altamente disponible es montarlo en una máquina virtual y, en lugar de guardar tan sólo la BD de ZeroShell, guardar la máquina virtual completa.

4.4. IMPLEMENTACIÓN DEL PROTOTIPO

4.4.1. Instalación de la Imagen de Zeroshell

- La imagen de Zeroshell se encuentra disponible en: http://www.zeroshell.net/eng/, desde ahí se descarga para proceder con su instalación.
- Se va a configurar a Zeroshell en una máquina virtual utilizando VMware y no como un live CD.
- Para crear una nueva máquina virtual abrir VMware, elegir la opción file, new y escoger la opción virtual machine.

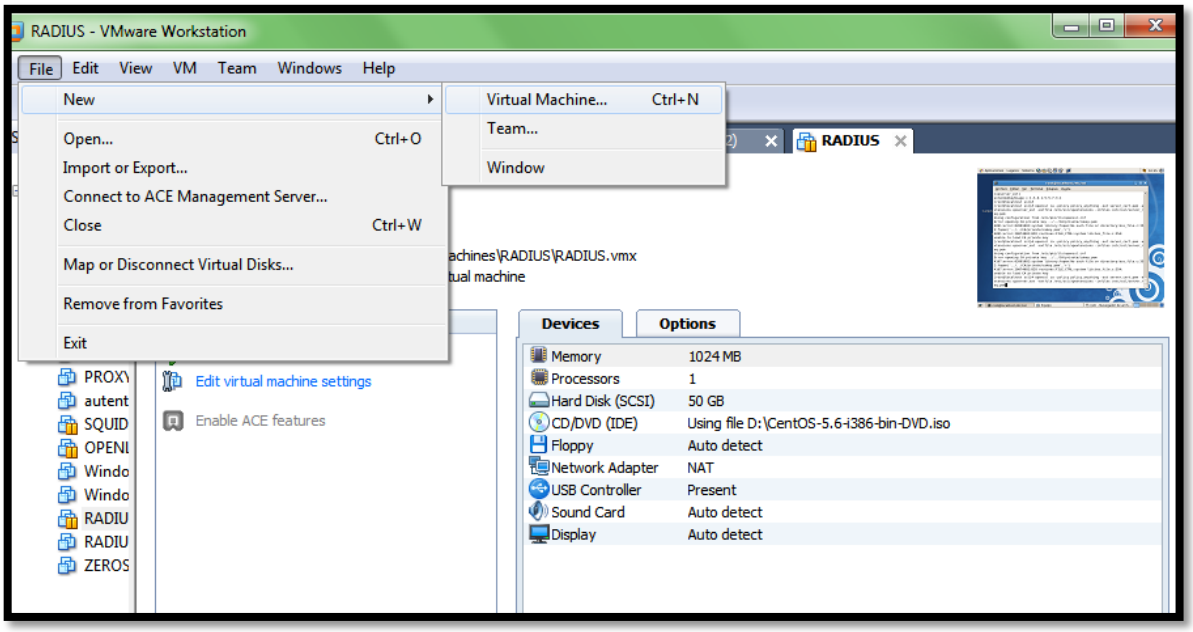


Figura IV. 66 Creación de Máquina Virtual

- Se puede elegir entre una instalación típica o avanzada, es este caso para mayor facilidad se utiliza la típica.

Figura IV. 67 Modo de Instalación

- Cargar la imagen de zeroshell, desde la ubicación en la que se haya almacenado al descargar.

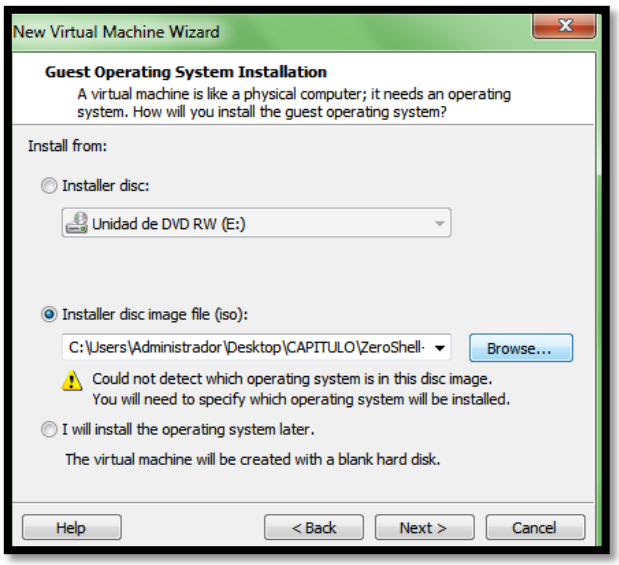


Figura IV. 68 Elección de Imagen de Máquina Virtual

- Escoger el tipo de sistema operativo, que se está instalando, que en este caso es Linux y pulsar siguiente.

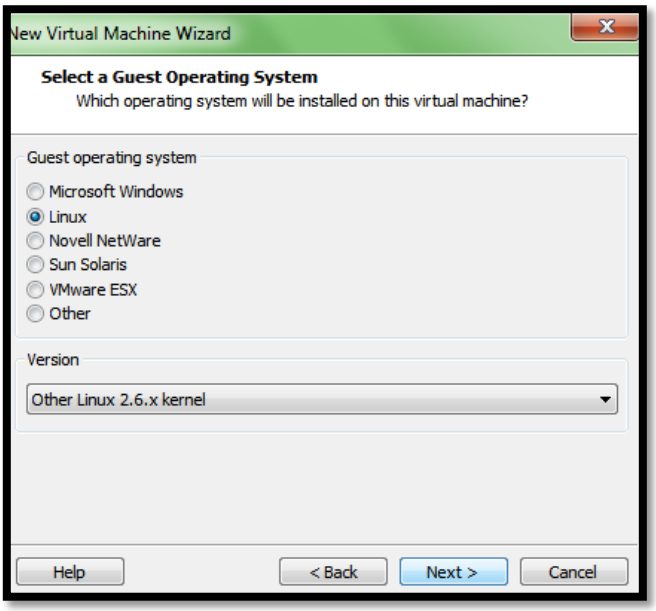


Figura IV. 69 Tipo de Sistema Operativo

- Asignar un nombre a la máquina virtual y pulsar siguiente.

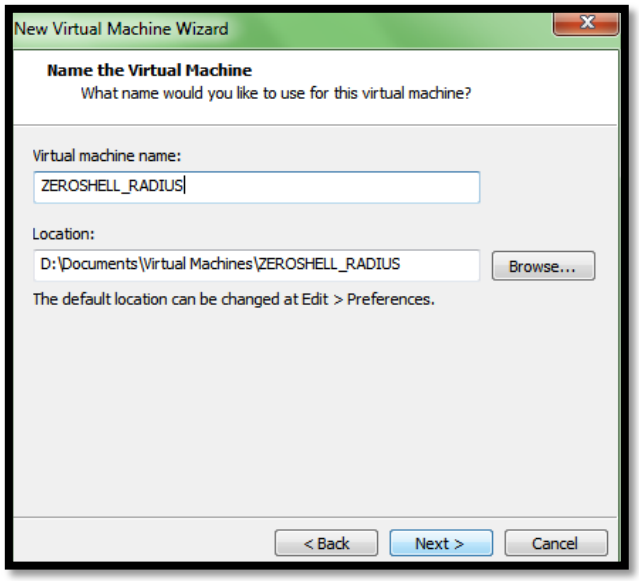


Figura IV. 70 Asignación de nombre

- Asignar el tamaño de disco que tendrá la máquina virtual en GB y continuar con la instalación. Tener en cuenta que el tamaño dependerá de la cantidad de usuarios que vaya a autentificar el servidor, previo a un riguroso análisis del escenario en el que se vaya a implementar.

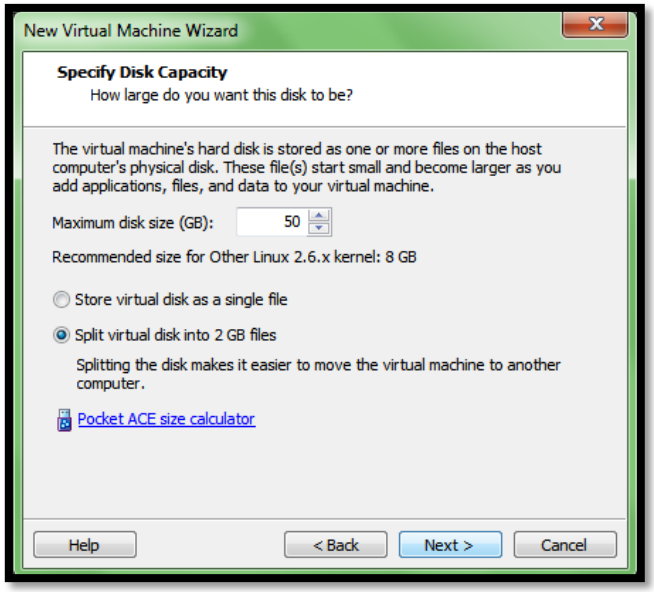


Figura IV. 71 Asignación de espacio en disco

- Finalmente se muestra un resumen de la máquina virtual que se está creando, para revisar si todo esta correcto y pulsar finalizar.

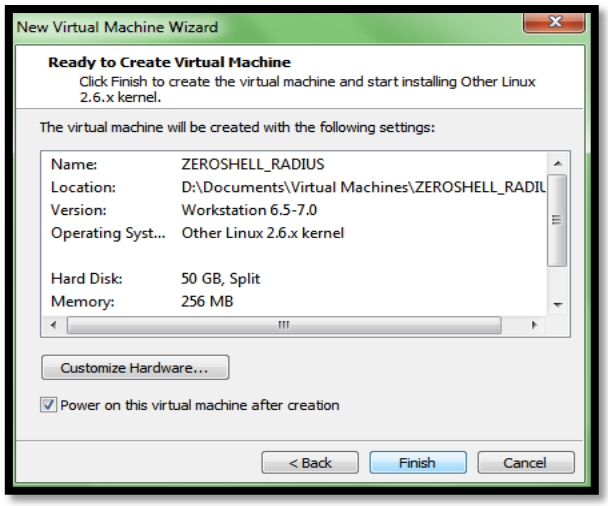


Figura IV. 72 Características de la Máquina Virtual

- Al comenzar la instalación se muestra un menú y para continuar pulsar el número 1, que significa un normal inicio del sistema.

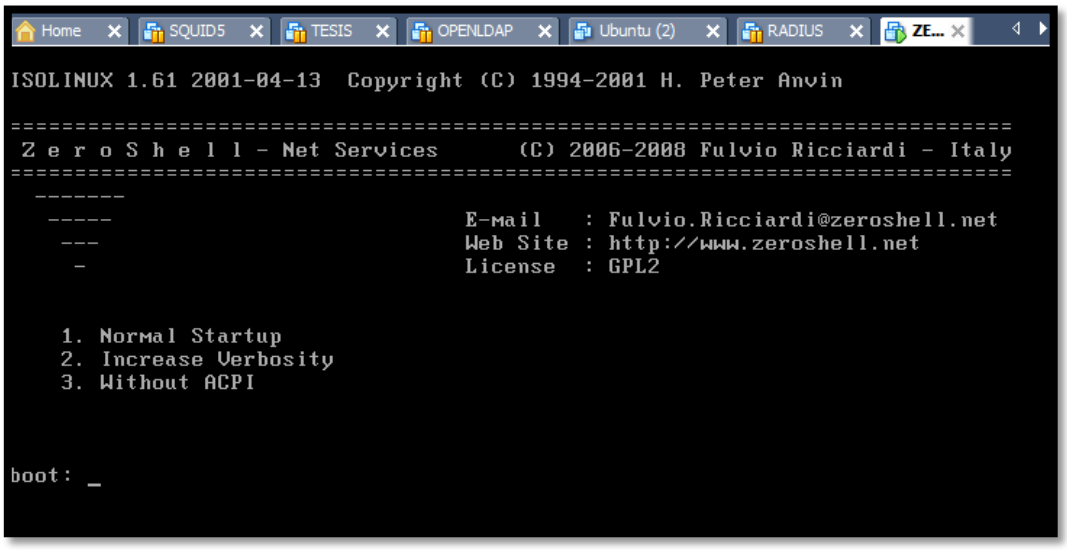


Figura IV. 73 Menú de Zeroshell

- Se muestra cómo se van cargando los componentes de Zeroshell.

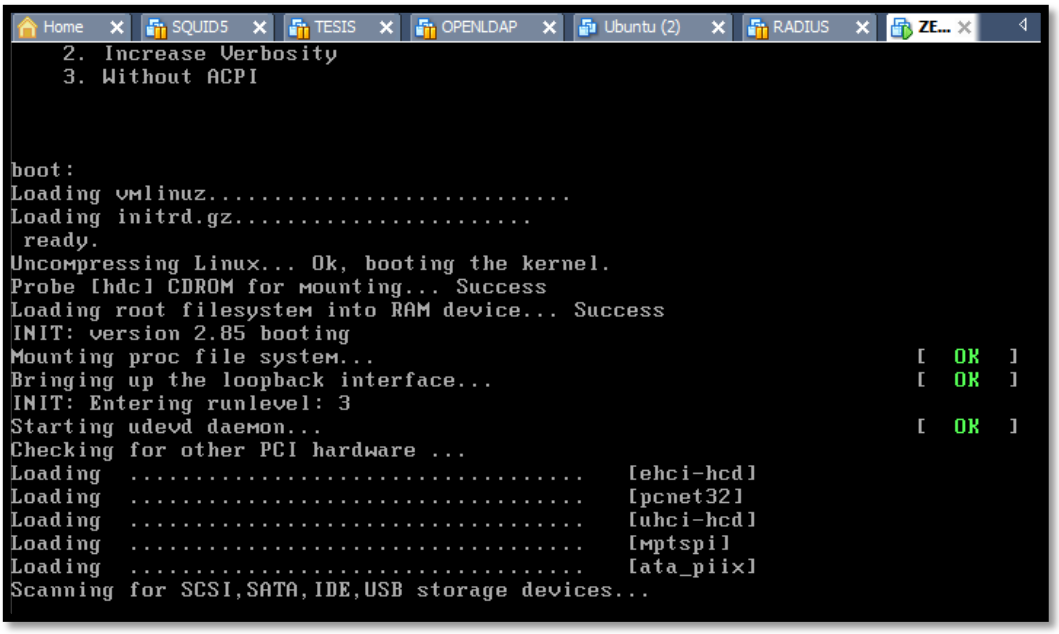


Figura IV. 74 Inicio del Sistema

- En la pantalla de inicio de Zeroshell se muestra las opciones básicas y necesarias para la configuración del servidor. Lo más relevante para este caso es la clave del administrador, dirección IP, mascara de subred y default Gateway de la interfaz de red.

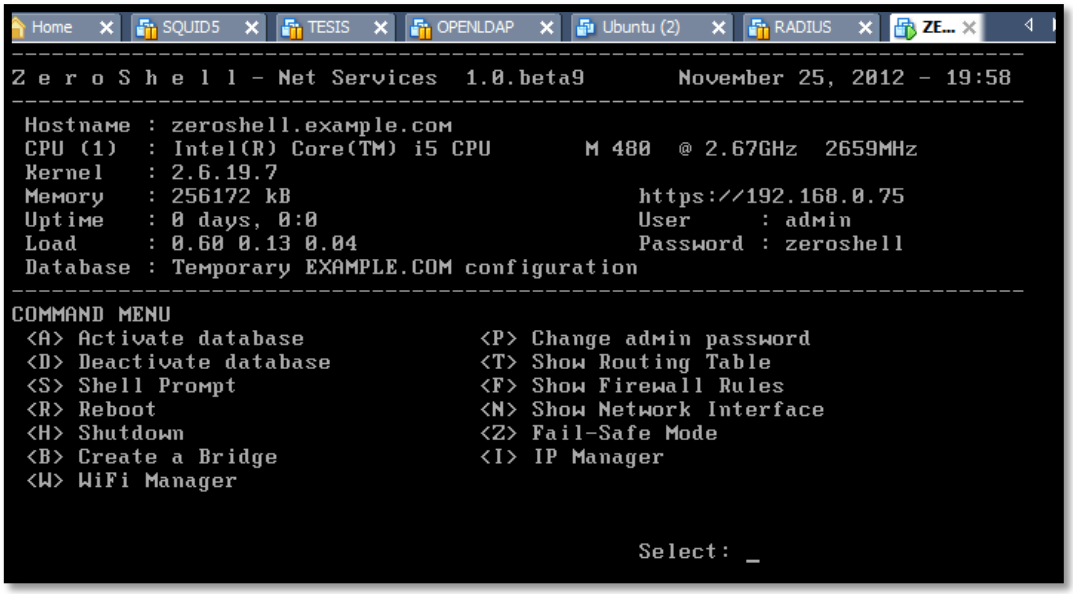


Figura IV. 75 Opciones de Configuración de Zeroshell

- Lo primero que se debe hacer es cambiar la dirección IP del servidor, para poder ingresar a su configuración mediante un navegador web, entonces pulsar la tecla I para que se muestre las opciones de configuración de la tarjeta de red del servidor. Por defecto se instala con la dirección IP 192.168.0.75/24.

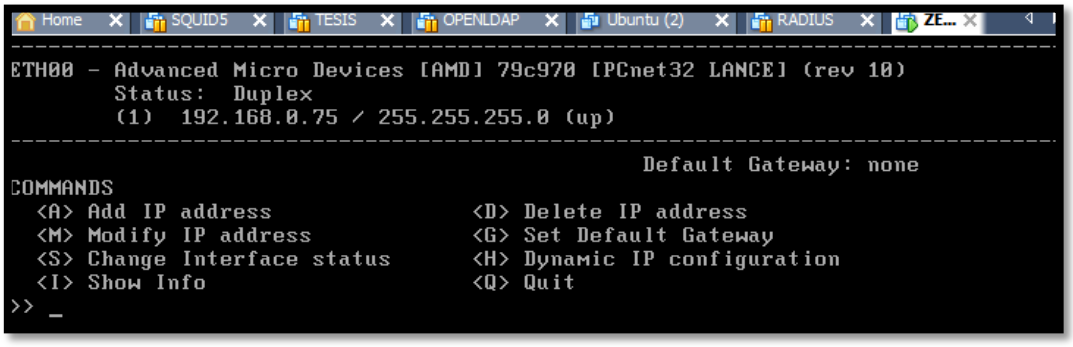


Figura IV. 76 Configuración de Red

- Pulsar M para modificar la dirección IP que está configurada por defecto, para este caso se puso la dirección IP 192.168.1.5 con mascara de subred de 255.255.255.0.

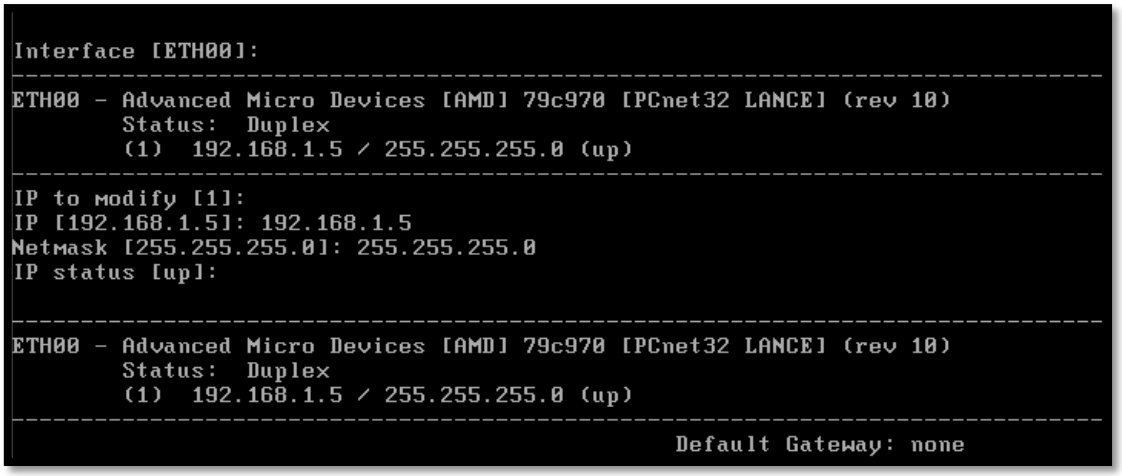


Figura IV. 77 Cambio de Dirección IP

- También es importante asignarle un default Gateway al servidor, para que pueda establecer comunicación con el resto de host que forman parte de la red. Para esto se ingresa la letra G. El default Gateway será la dirección del Access Point, en este caso es 192.168.1.1.

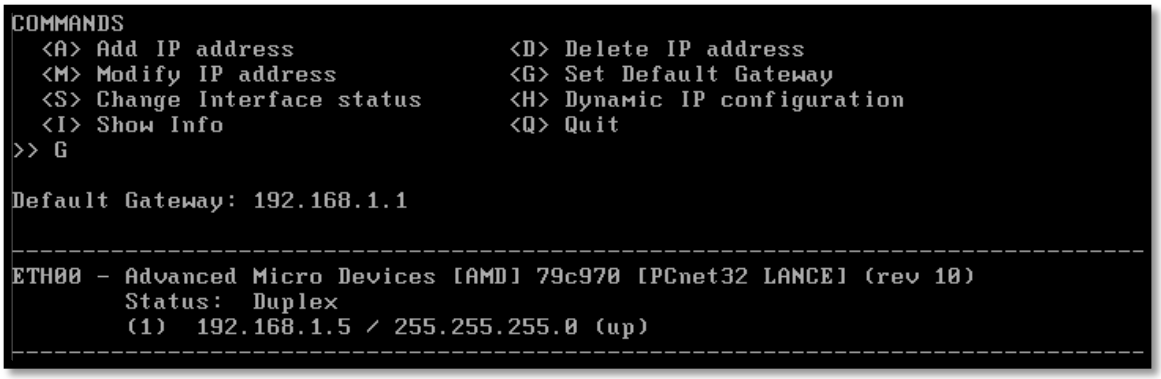


Figura IV. 78 Configuración de Gateway

- Es necesario cambiar la clave de ingreso para la configuración vía web que ofrece zeroshell, por defecto el login es admin y la clave es zeroshell. Para configurar una clave se pulsa la letra P, se pedirá el ingreso de una nueva clave y su respectiva confirmación.

Figura IV. 79 Password del administrador

- Ya configurados los parámetros de red, se puede ingresar a la interfaz web para continuar con la configuración. Para lo cual es necesario abrir un navegador web e ingresar la dirección IP del servidor configurada anteriormente.

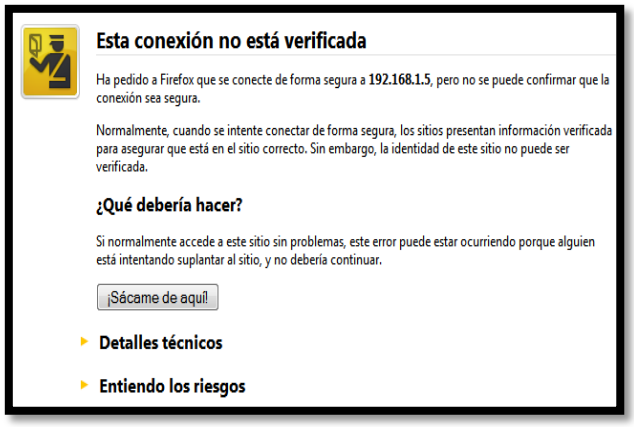


Figura IV. 80 Ingreso al sistema mediante Interfaz WEB

- Al cargar la página, se muestra un mensaje indicando que el servidor posee un certificado de seguridad no válido, porque aún no se lo ha configurado. Así que, hacer clic sobre la opción añadir una excepción y aparecerá una ventana donde se puede confirmar la excepción de seguridad. Se tiene que confirmar la excepción de seguridad porque el servidor aún no tiene creados sus certificados.

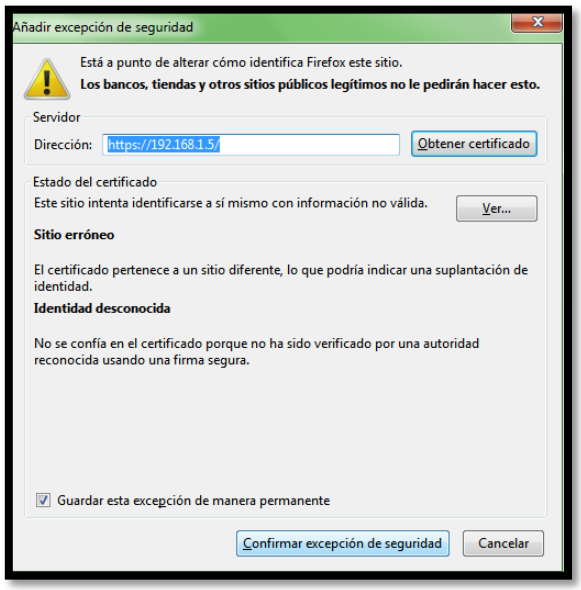


Figura IV. 81 Generación de Certificados del Servidor

- Realizado esto, se muestra la pantalla de acceso a Zeroshell, en el cual se ingresa el username que es admin y la contraseña configurada anteriormente.

Figura IV. 82 Ingreso al Sistema

- Después de haberse autenticado, se muestra la interfaz gráfica que posee este software, además de todas las opciones que presenta.

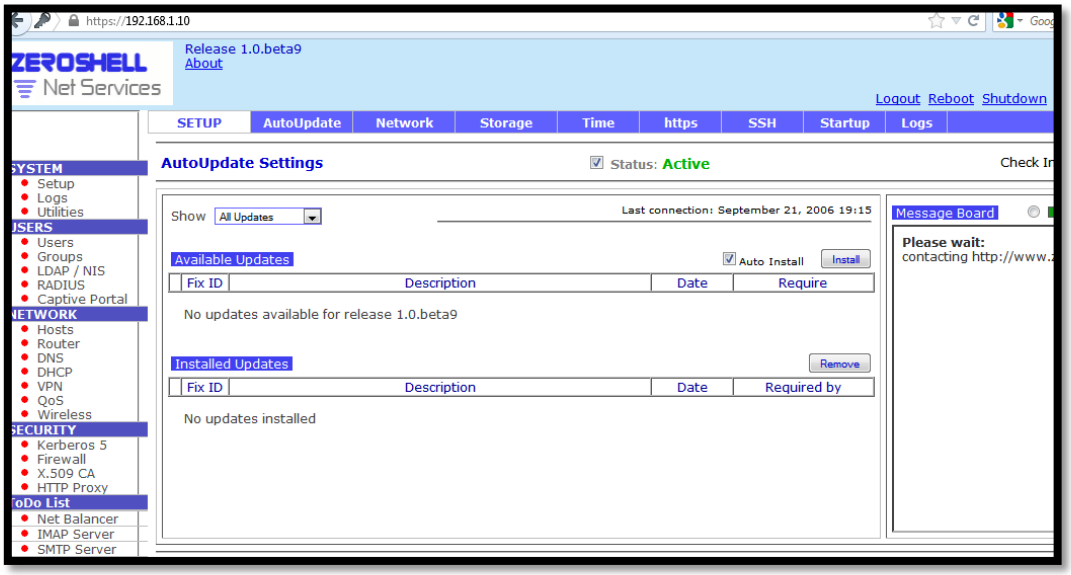


Figura IV. 83 Interfaz gráfica de Zeroshell

- Es necesario crear una partición en el disco duro virtual mediante un perfil para guardar los ajustes. Un perfil es la base de datos donde se van a guardar los ajustes. Mientras no se cree un perfil, cada vez que arranque Zeroshell se iniciará con la configuración por defecto. Para ello, hacer clic en Storage y seleccionar el disco duro en el que se va a guardar el perfil.

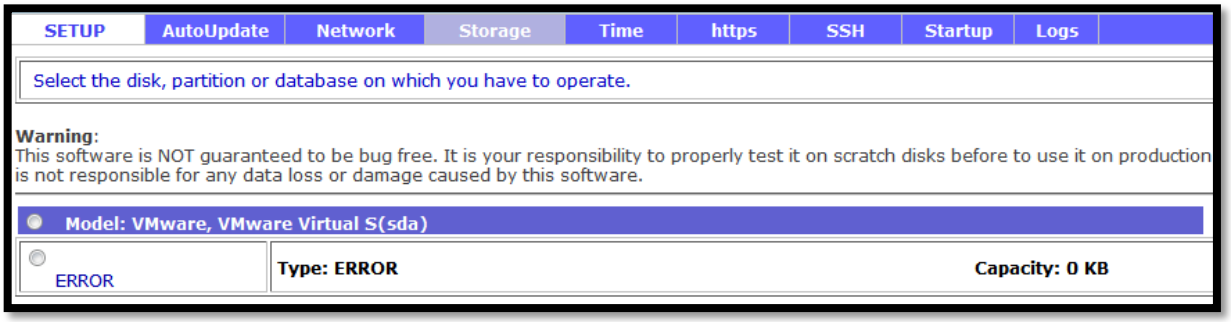


Figura IV. 84 Interfaz gráfica de Zeroshell Creación de Perfil

- Como se está trabajando en máquina virtual en la que no se ha creado ninguna partición aparece un mensaje de error. Así que hay que crear una partición. Para ello, seleccionar la opción Model: VMware y hacer clic en el botón “New partition”.

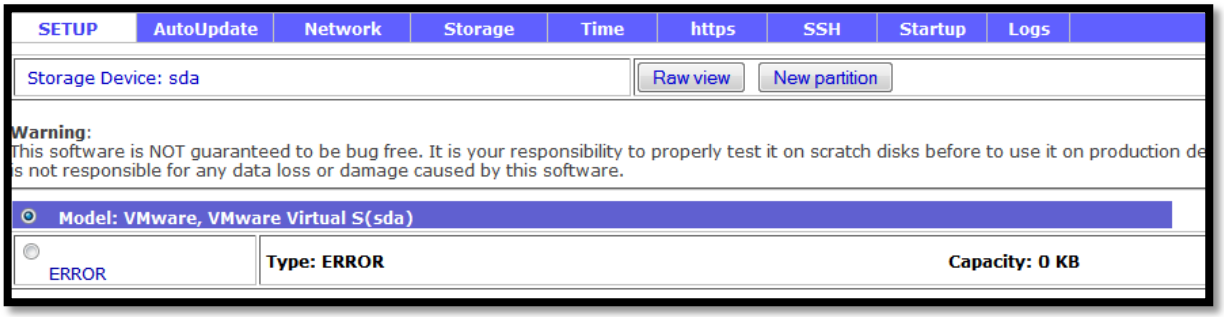


Figura IV. 85 Creación de nueva partición

- Se muestra una pantalla, en la que se debe ingresar un nombre para el disco virtual en Label y hacer clic en “CreatePartition”. Una vez creada la partición, aparecerá una ventana en la que se seleccionara el disco hda1, para guardar ahí el perfil.

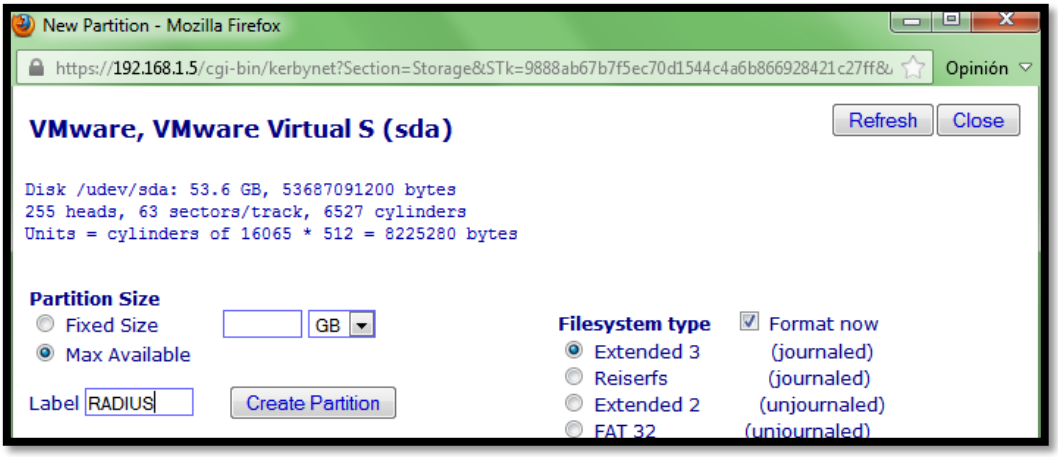


Figura IV. 86 Tipo de partición

- Se indica que la creación de la partición, puede tardar varios minutos.

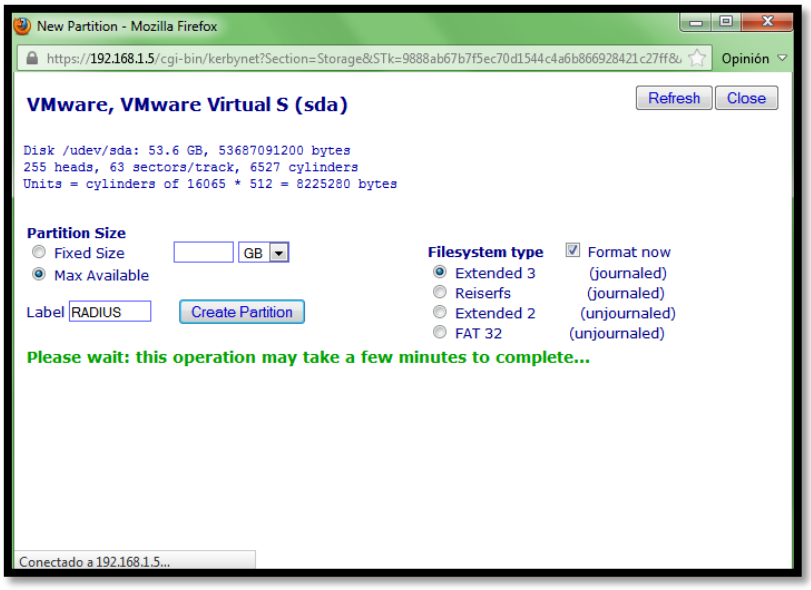


Figura IV. 87 Proceso de creación de partición

- Se debe crear un perfil, para esto seleccionar la partición creada anteriormente, y elegir la opción créate DB.

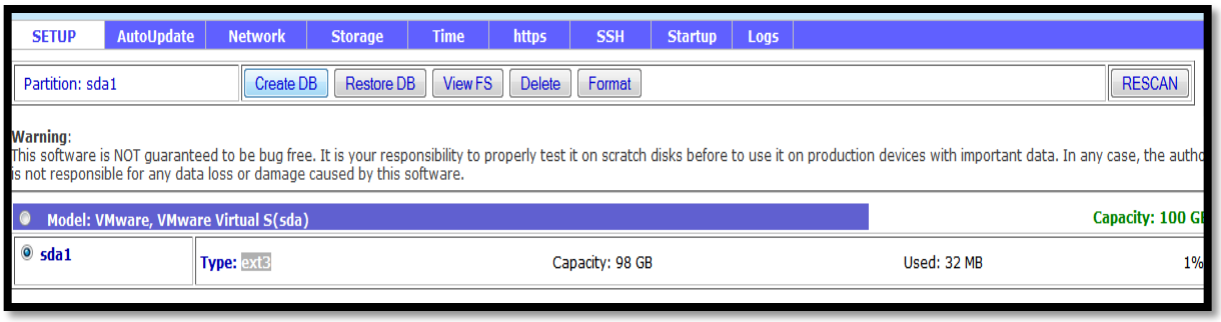


Figura IV. 88 Selección de partición creada para perfil

- Debe aparecer una ventana en la que hay que ingresar la descripción, Hostname, Realm, LDAP Base, la contraseña de administrador y la IP del gateway por defecto. Una vez especificados estos datos, pulsar el botón Create y se creará un perfil.

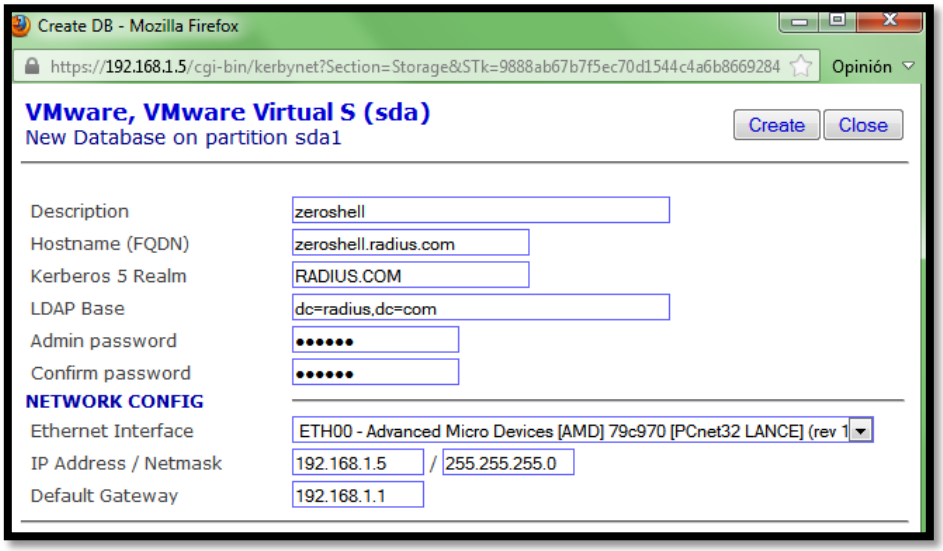


Figura IV. 89 Formulario para creación de perfil

- Luego se muestra la base de datos creada anteriormente

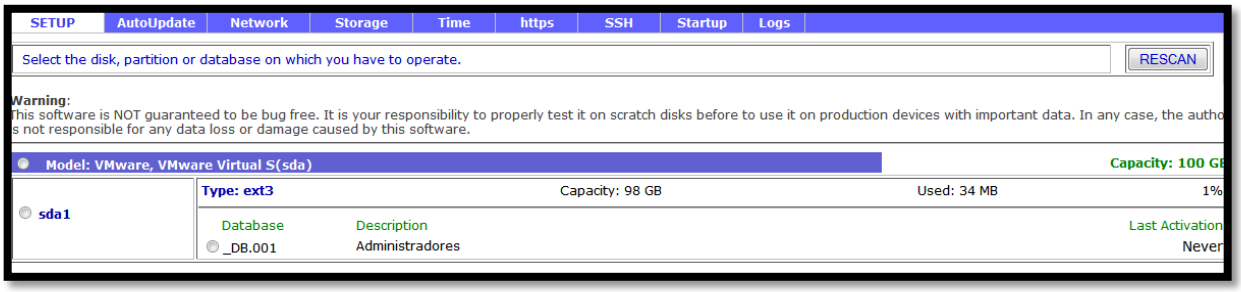


Figura IV. 90 Información sobre perfil creado

- Para activar este perfil solo se selecciona

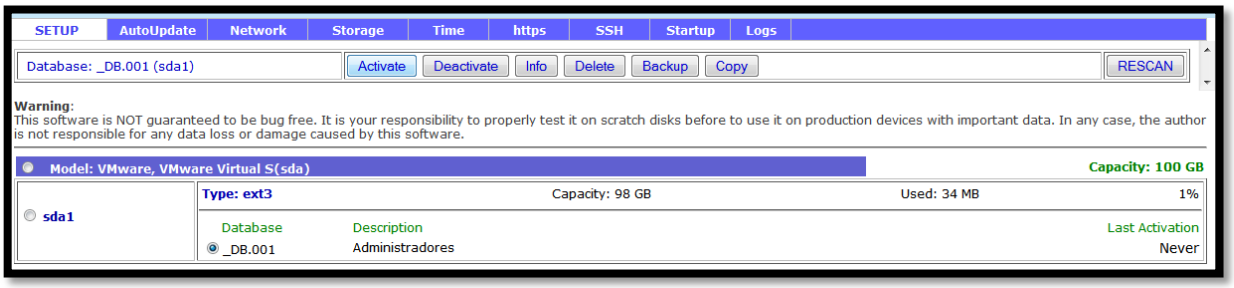


Figura IV. 91 Selección de perfil creado

- Luego de pulsar aparece un resumen del perfil creado, en el cual aparece un mensaje de que no está activado.

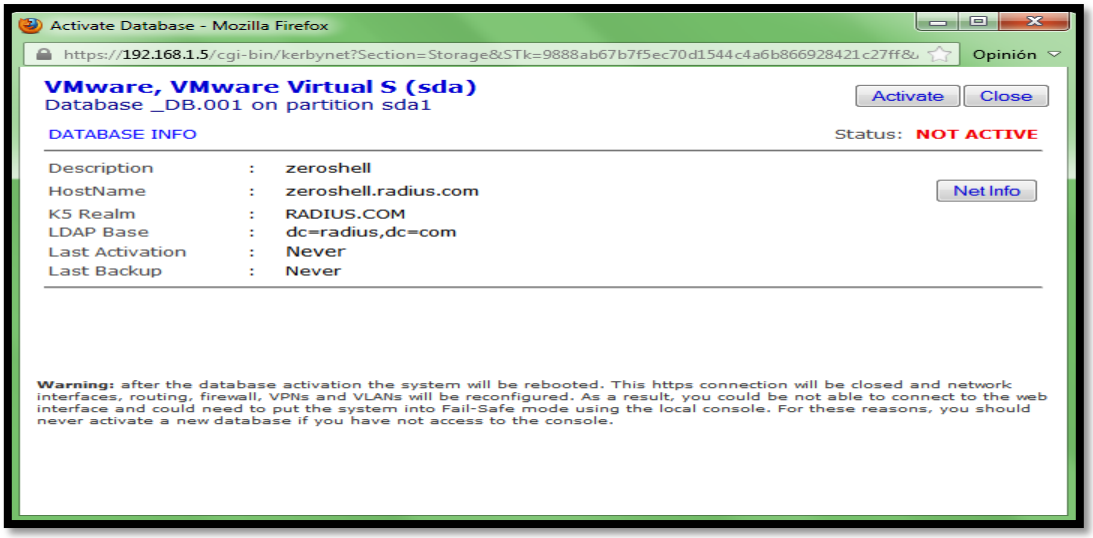


Figura IV. 92 Información sobre no activación de perfil

- Pulsar nuevamente el botón activar, aparece un mensaje indicando si está seguro de activar la base de datos,

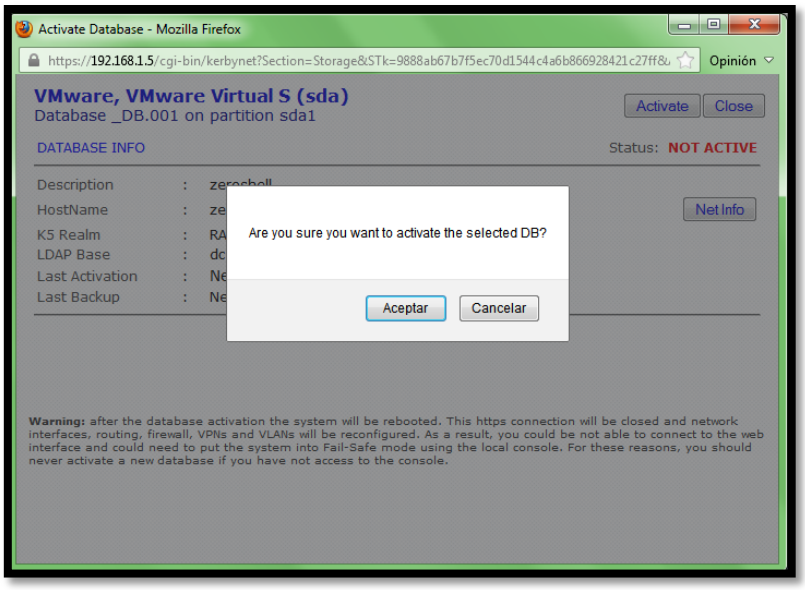


Figura IV. 93 Activación de perfil creado

- Para aplicar los cambios realizados anteriormente el sistema se reiniciara, y hay que autentificarse nuevamente en el servidor, para que no se genere errores al querer ingresar por el navegador, hay que eliminar el cache ya que todavía no es válido el certificado que está configurado.

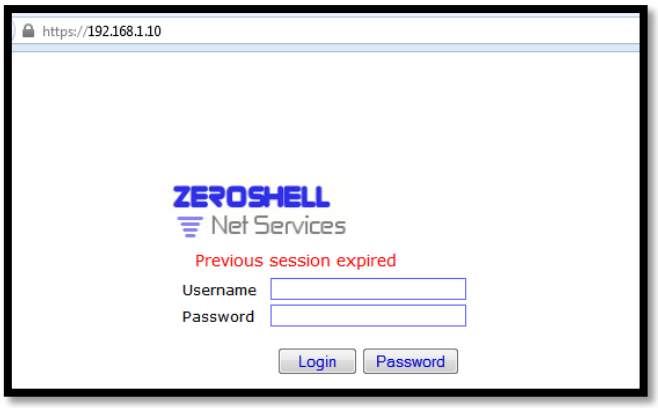


Figura IV. 94 Ingreso al sistema reiniciado

4.4.2. CREACIÓN DE LA AUTORIDAD CERTIFICADORA

- Seleccionar el botón CA X509 en el lado izquierdo de la interfaz web.

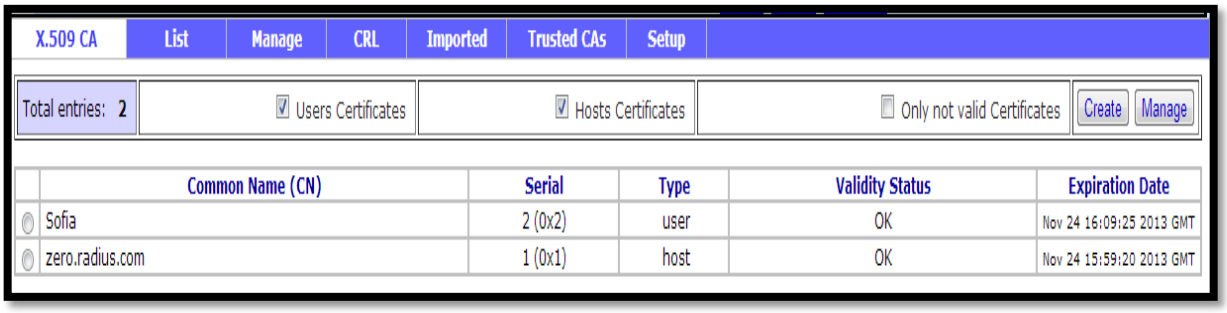


Figura IV. 95 Creación de la CA

- Hacer clic en la opción setup, se muestra una pantalla en la que se debe agregar información como: nombre de la autoridad certificadora, tamaño en bits que tendrá la clave pública, número de días en los que el certificado digital es válido, país, provincia, organización, dirección de correo electrónico.

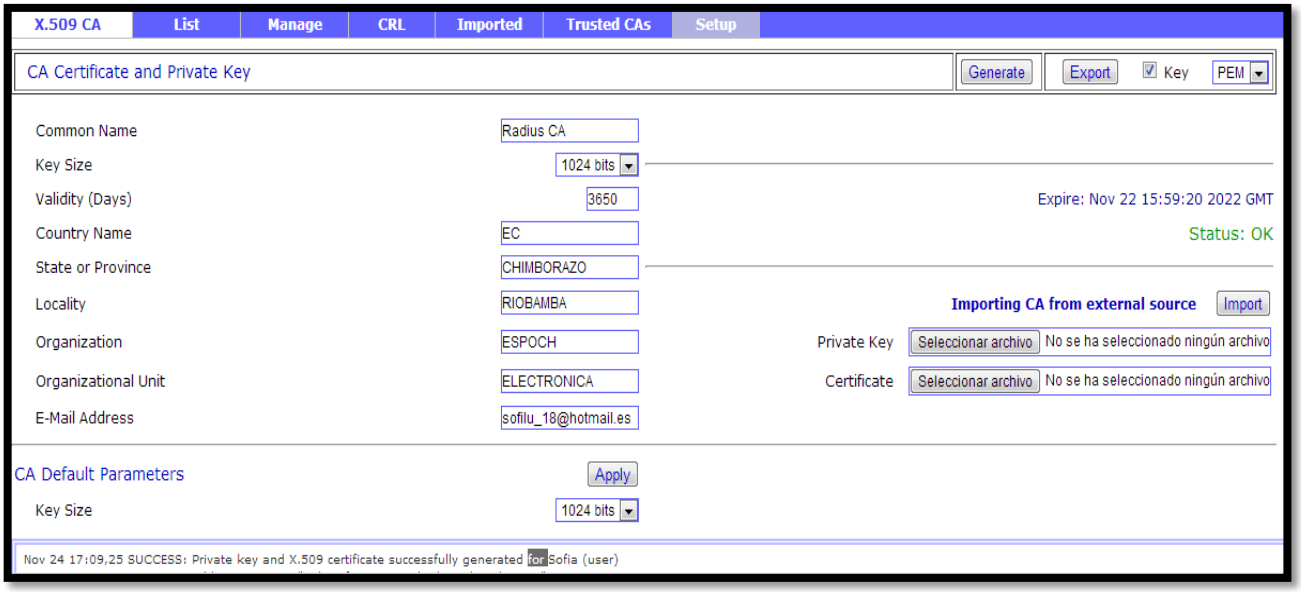


Figura IV. 96 Formulario de creación de CA

- Llenada la información requerida pulsar "Generate", y luego "Ok" en el mensaje que se muestra, indicando si está seguro o no de crear el certificado.

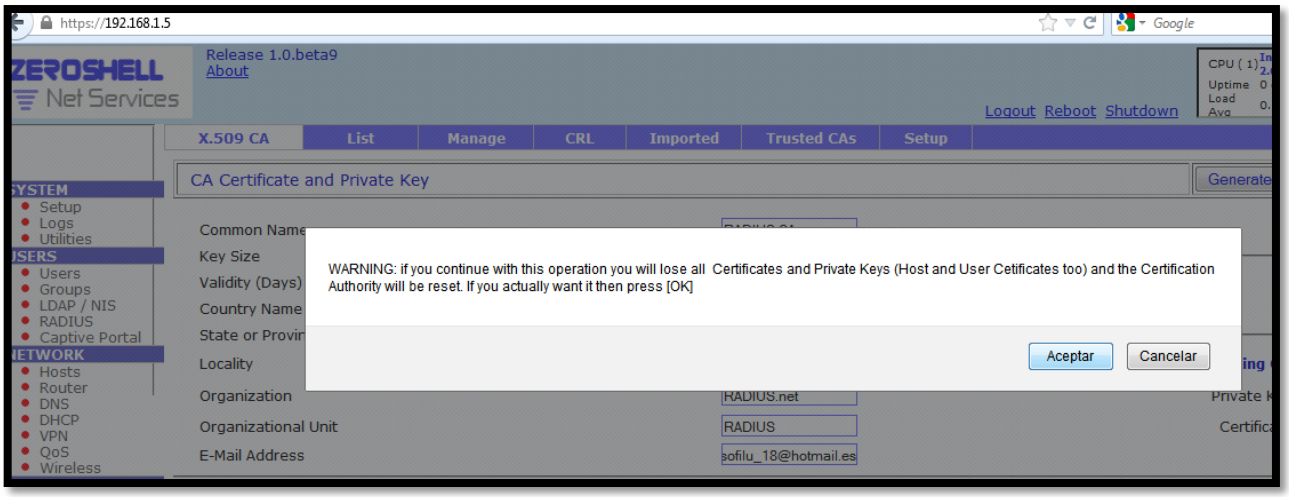


Figura IV. 97 Creación de Certificado de la CA

- Por último se acepta y la autoridad certificadora está correctamente configurada. Cuando se actualiza asegurarse de que todos los campos estén correctos.

4.4.3. CREAR USUARIOS

- A continuación hay que crear los usuarios de RADIUS, para esto hacer clic en el menú USERS y luego en la opción RADIUS. Y se despliega la lista de usuarios creados en el sistema, por el momento únicamente existe el usuario administrador.

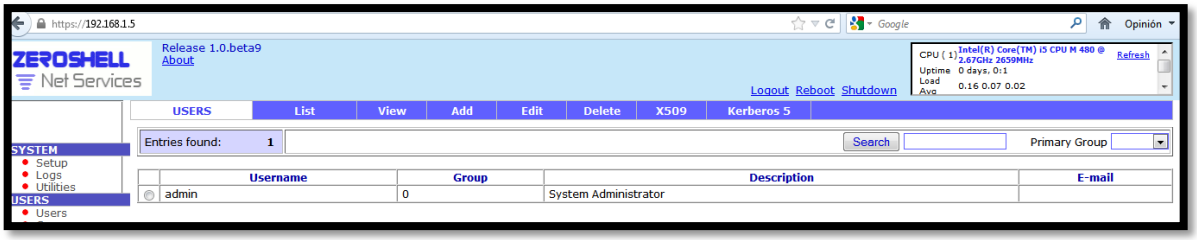


Figura IV. 98 Lista de usuarios

- Para añadir nuevos usuarios, hacer clic en la pestaña Add.

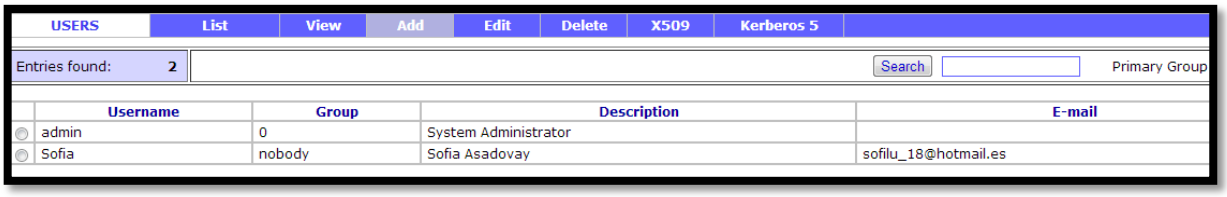


Figura IV. 99 Opción añadir usuario

- Llenar los datos requeridos como: nombre de usuario, home directory, nombre y apellido del usuario, descripción, correo electrónico y la contraseña.

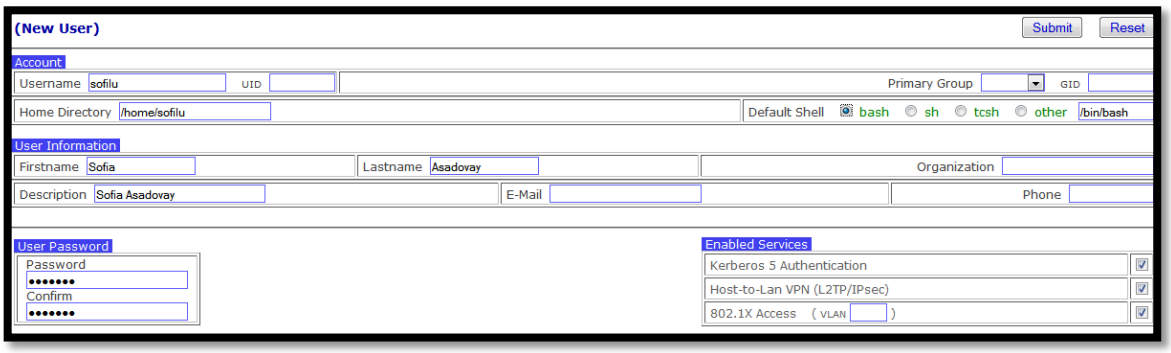


Figura IV. 100 Formulario nuevo usuario

- Pulsar submit y a continuación se muestra una pantalla con los detalles del certificado generado.

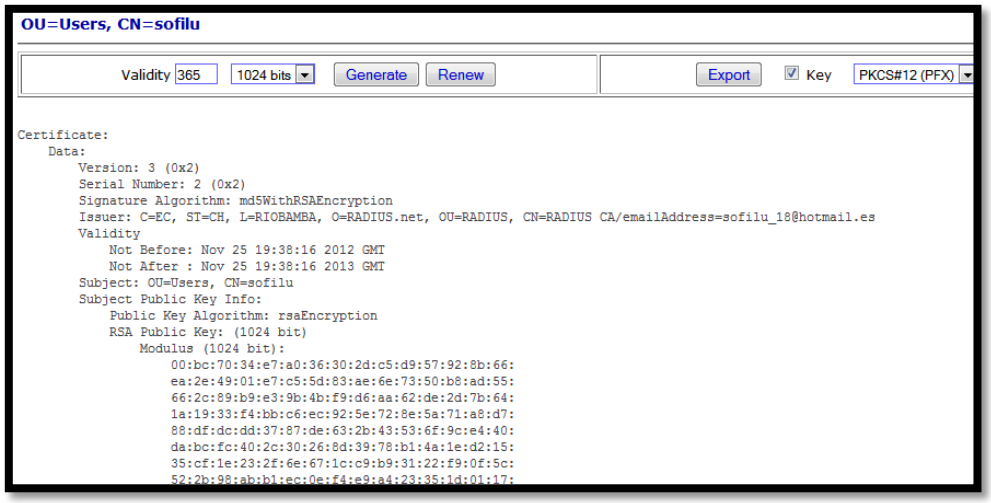


Figura IV. 101 Detalles del certificado

- Se debe seguir el mismo procedimiento para seguir añadiendo los usuarios que se necesiten.

4.4.4. CONFIGURACIÓN DEL SERVIDOR RADIUS

- Primero se tiene que activar la opción de RADIUS, para esto hacer clic en la opción "RADIUS" del menú "USERS" que se encuentra a la izquierda de la pantalla y marcar el casillero que indica enabled.

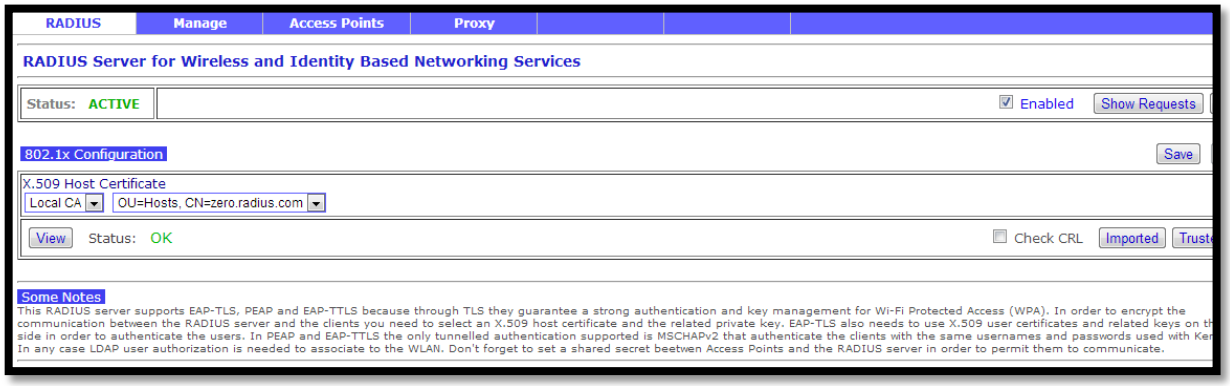


Figura IV. 102 Activación de RADIUS

- Se debe registrar los puntos de acceso que van a tener acceso al servidor RADIUS, para configurar esto hacer clic en la pestaña "Access Point" en la barra de navegación de la parte superior.

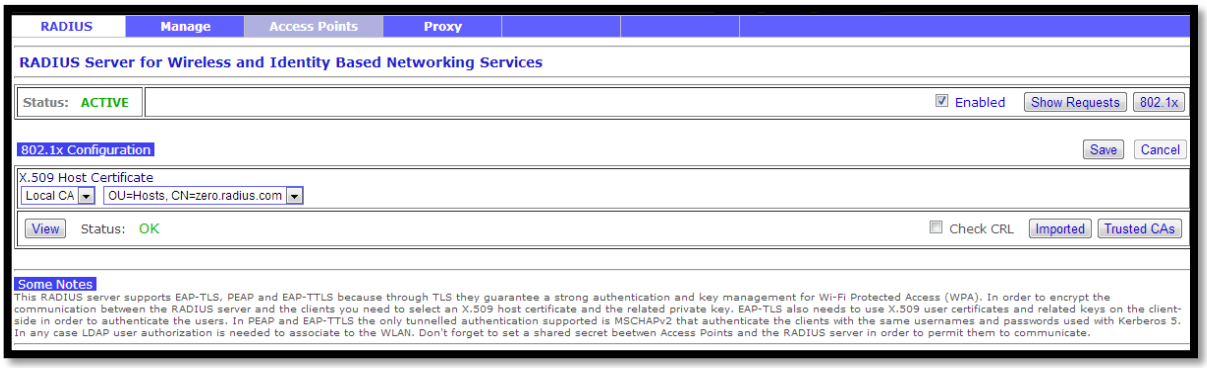


Figura IV. 103 Registro de AP

- Para añadir un punto de acceso se debe ingresar un nombre para poder distinguirlo, la dirección IP y mascara de subred en este caso es 192.168.1.1/24, y la clave secreta que compartirá el servidor y el Access Point. Para que los usuarios que se conectan a la red inalámbrica puedan autentificarse. Deben tener en cuenta que la clave secreta no puede tener más de 32 caracteres.

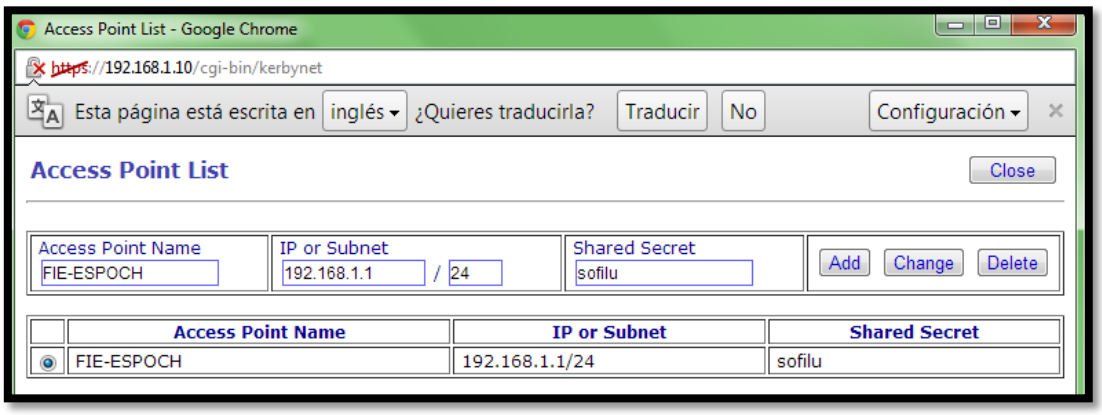


Figura IV. 104 Formulario de registro de AP

- Una vez introducidos los datos de cada punto de acceso pulsar el botón “Add” y se añadirá a la lista. Cuando termine de añadir puntos de acceso pulsar el botón “Close”.

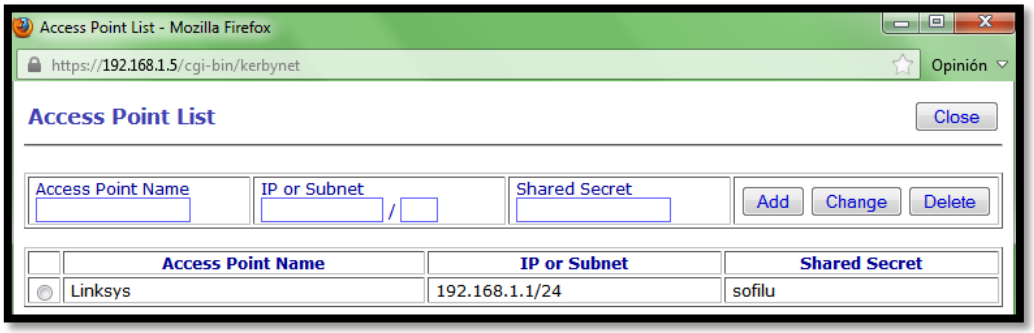


Figura IV. 105 AP registrado

- Para que los cambios realizados tengan efecto reiniciar Zeroshell con la pestaña que se encuentra en la parte superior de la página web. Y el servidor RADIUS está listo para entrar en funcionamiento.

4.4.5. CONFIGURACIÓN DEL ACCESS POINT

- Para la implementación de un sistema con RADIUS, se debe utilizar un AP que soporte este protocolo, en este caso se muestra la configuración de un LYNKSYS GIGABIT WIRELESS-N modelo WRT310N.
- Se configura mediante un navegador web, colocando la dirección IP 192.168.1.1, es bastante sencillo ya que únicamente hay que ingresar en la opción wireless, en la pestaña wireless security, se tiene que escoger el modo de seguridad, algoritmo WPA que se va a utilizar, dirección IP del servidor RADIUS, número de puerto que utiliza este protocolo y la clave compartida que se configuro anteriormente en el servidor RADIUS.

Figura IV. 106 Configuración del AP

4.4.6. CONFIGURACIÓN DE UN CLIENTE WINDOWS

4.4.6.1. Importación de la Clave Pública

- Primero se tiene que exportar la clave pública del servidor, para instalarlo en los clientes.
- Hacer clic en la opción x.509 CA que se encuentra dentro de SECURITY y escoger la pestaña TrustedCAs.

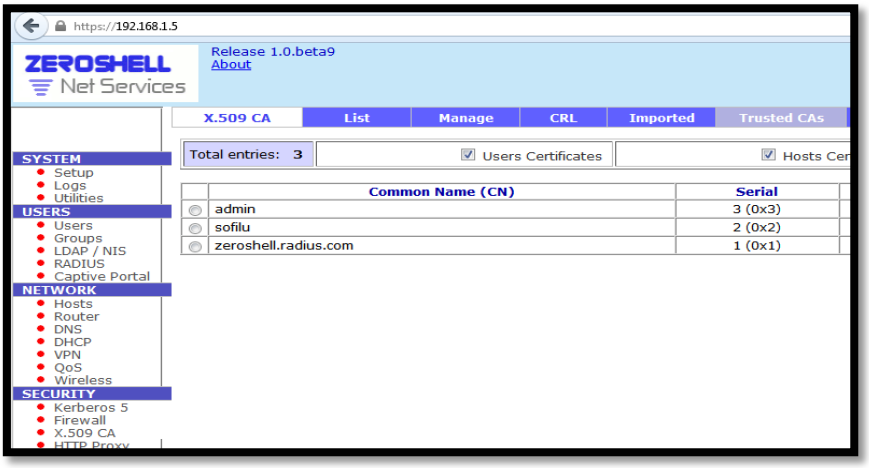


Figura IV. 107 Importación de clave

- Seleccionar la autoridad certificadora y pulsar en el botón exportar. Se descarga un archivo llamado TrustedCA.pem.

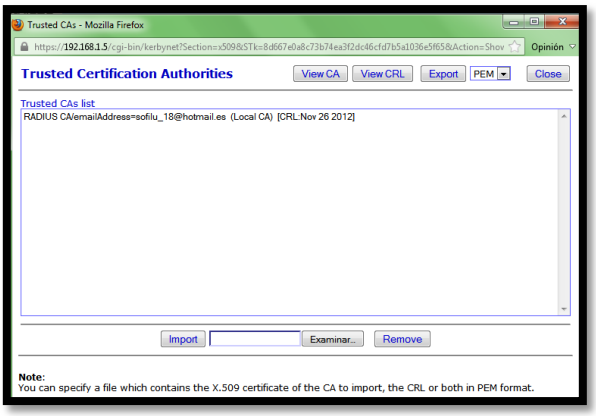


Figura IV. 108 Selección de la clave

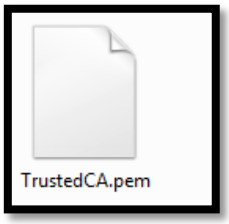


Figura IV. 109 Clave Pública

4.4.6.2. Importación de la clave Privada

- Hacer clic en el menú USERS, la opción Users y se desplegara la lista de los usuario registrados en el sistema.

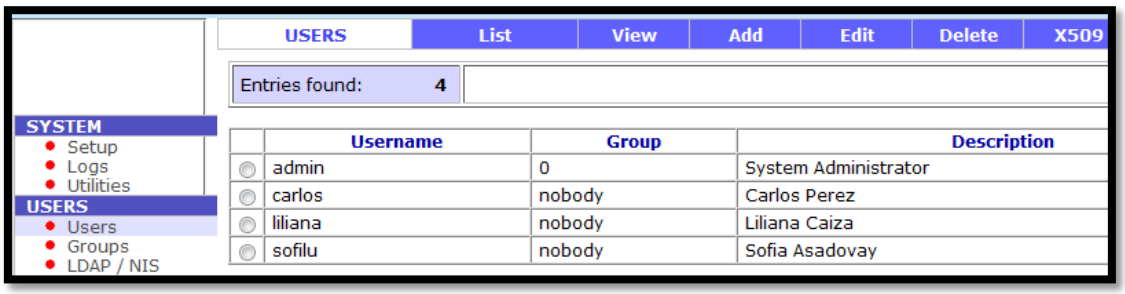


Figura IV. 110 Lista de Usuarios del Sistema

- Seleccionar el usuario del cual se quiere exportar la clave privada y hacer clic en la pestaña de X509, que se encuentra en la parte superior de la lista de usuarios.

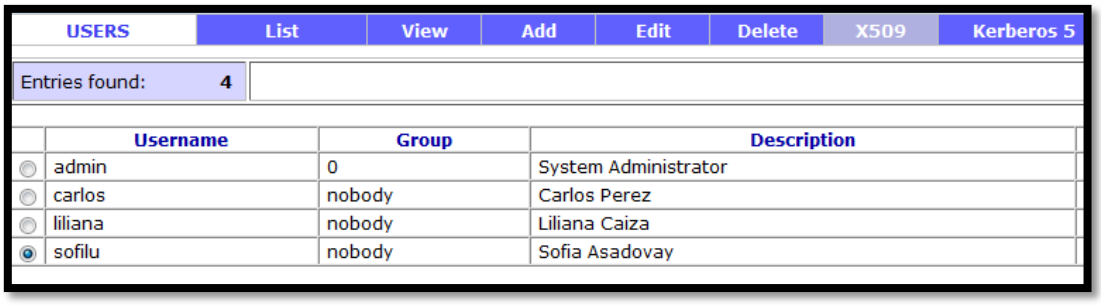


Figura IV. 111 Selección de clave de usuario

- Se muestra una nueva ventana con todos los detalles de la clave privada del usuario en mención.

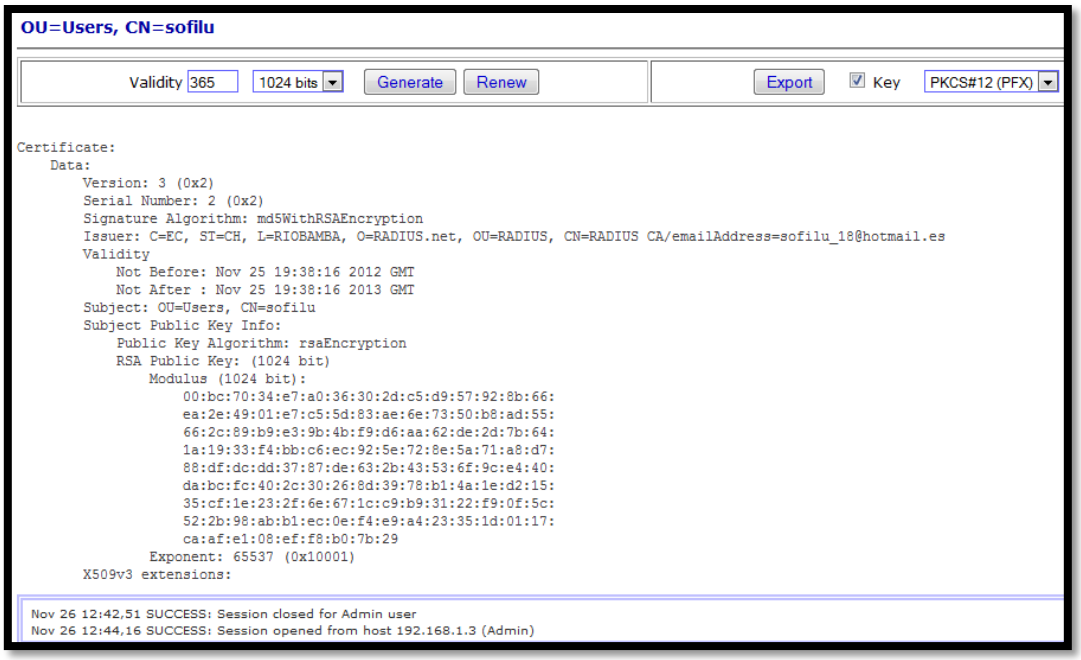


Figura IV. 112 Detalles de la clave

- En la parte superior de la ventana mostrada en el paso anterior, hacer clic en el botón Export, teniendo en cuenta que el formato en que se debe exportar para un cliente de Windows es PKCS#12(PFX). Se indica el lugar en el que se va a guardar el archivo.

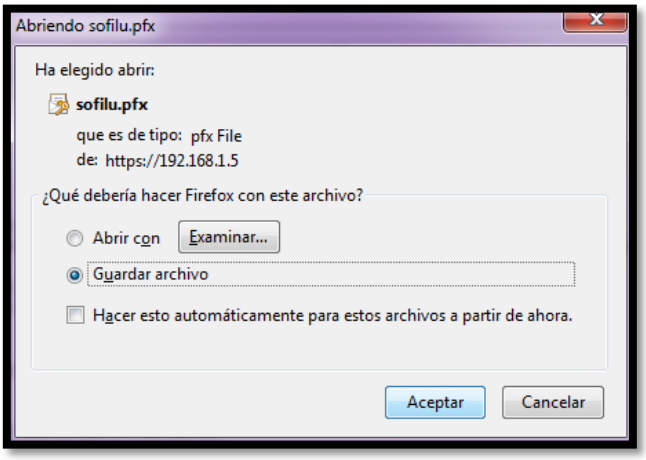


Figura IV. 113 Exportación de la clave del usuario

- Finalmente aceptar y verificar que se haya guardado en el lugar que se indicó.

Figura IV. 114 Clave Privada

4.4.6.3. Instalación de la Clave Pública

- Para instalar el certificado digital en el cliente pulsar ctrl + tecla de Windows, y escribir MMC.

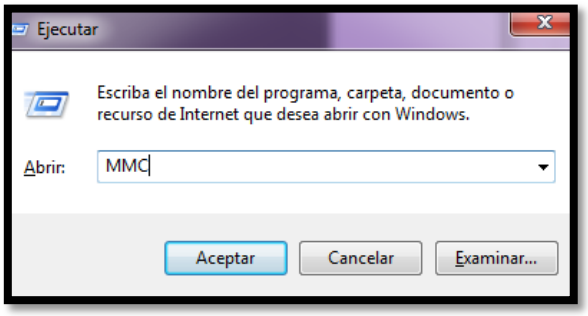


Figura IV. 115 Instalación del certificado

- Hacer clic en aceptar y se muestra la siguiente consola

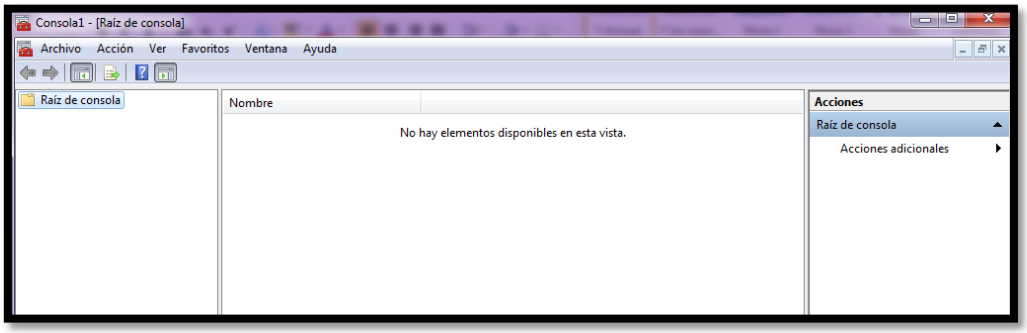


Figura IV. 116 Consola para instalar certificado

- Escoger la opción archivo, agregar o quitar complemento del menú archivo.

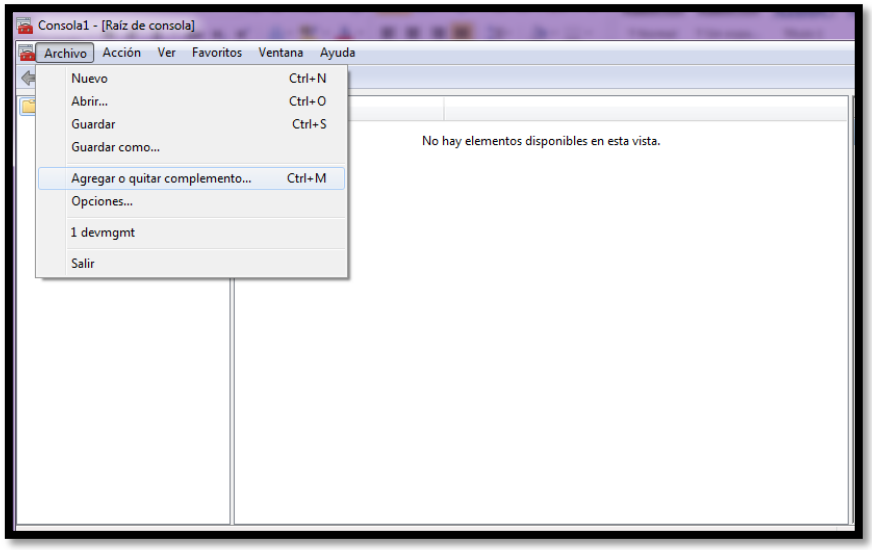


Figura IV. 117 Agregar complemento

- En el menú que se muestra escoger la opción certificados y hacer clic en agregar.

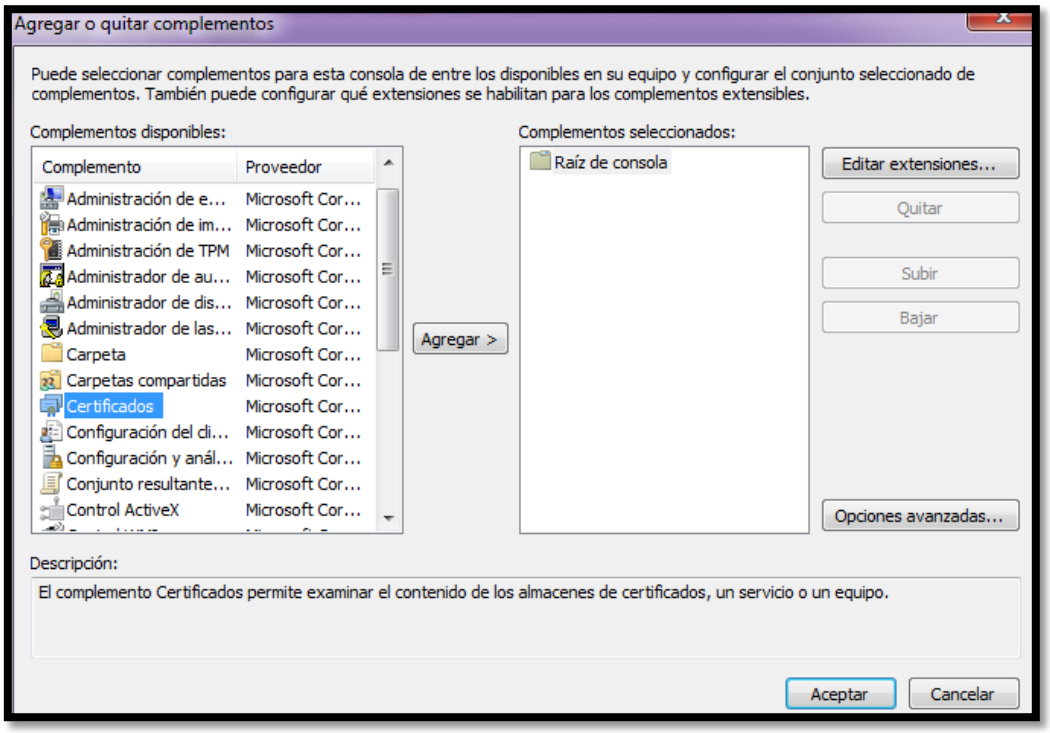


Figura IV. 118 Agregar certificado

- Seleccionar la opción para que el complemento administre los certificados de Mi cuenta de Usuario y finalizar.

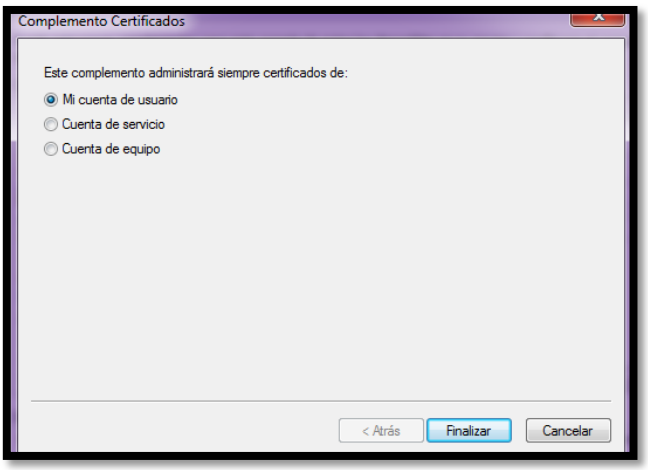


Figura IV. 119 Selección de cuenta

- Al aceptar se muestra los Certificados del usuario actual, desplegar su contenido y escoger la carpeta entidades de certificación raíz de confianza y dentro de esta se encuentra certificados. Al costado derecho de esta ventana hacer clic en la opción Acciones adicionales, todas las tareas y finalmente en importar.

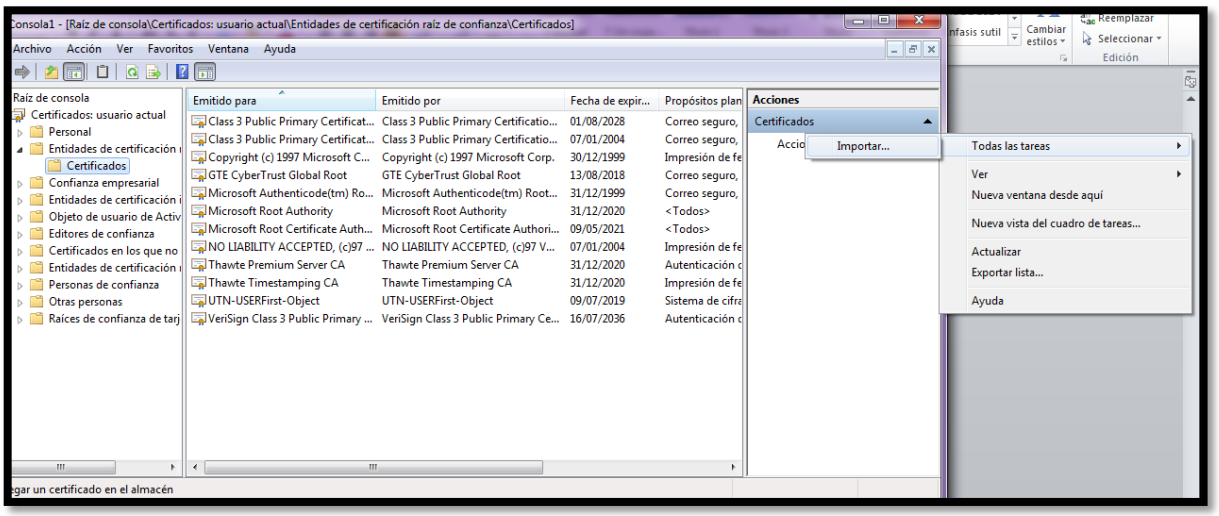


Figura IV. 120 Importación de Certificado

- Aparece el asistente para importación de certificados y pulsar siguiente.

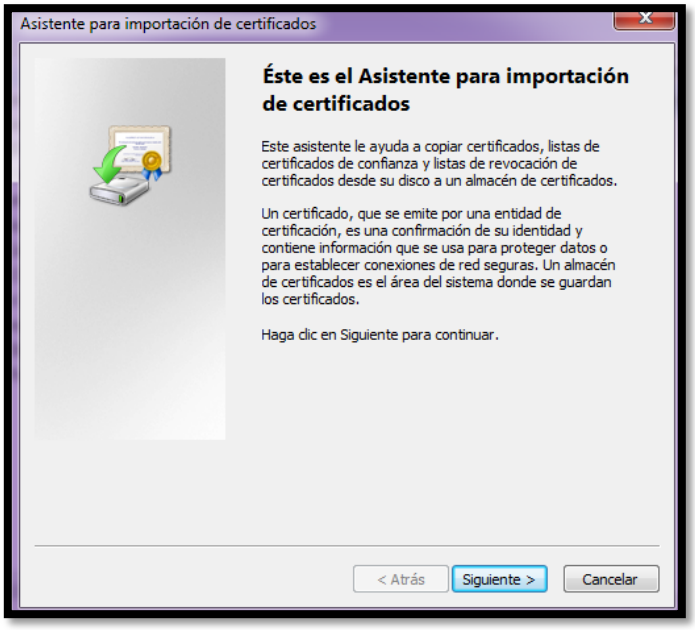


Figura IV. 121 Asistente de importación de certificado

- En la opción examinar, indicar la ubicación de certificado descargado anteriormente, el cual se va a importar y hacer clic en siguiente.

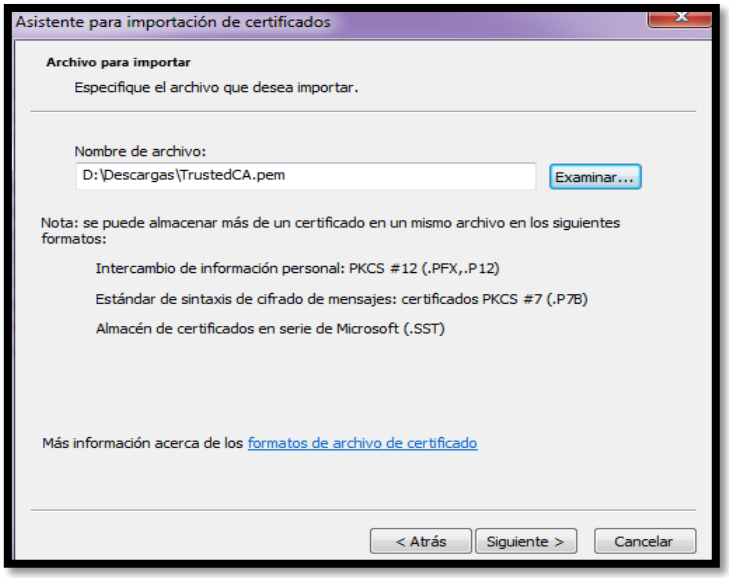


Figura IV. 122 Ubicación del Certificado

- Escoger como almacén de los certificados a Entidades de certificación raíz de confianza y siguiente.

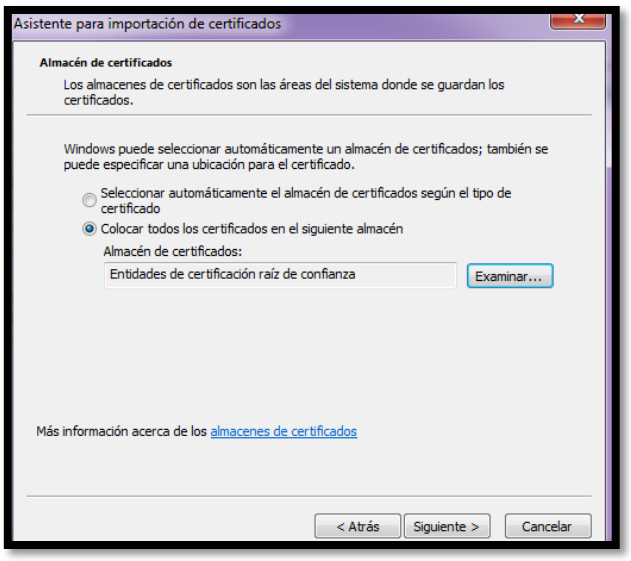


Figura IV. 123 Almacén del certificado

- Se muestra un resumen de los detalles ingresados durante el proceso de instalación del certificado, para poder verificar si todo es correcto o realizar alguna corrección si es necesario.

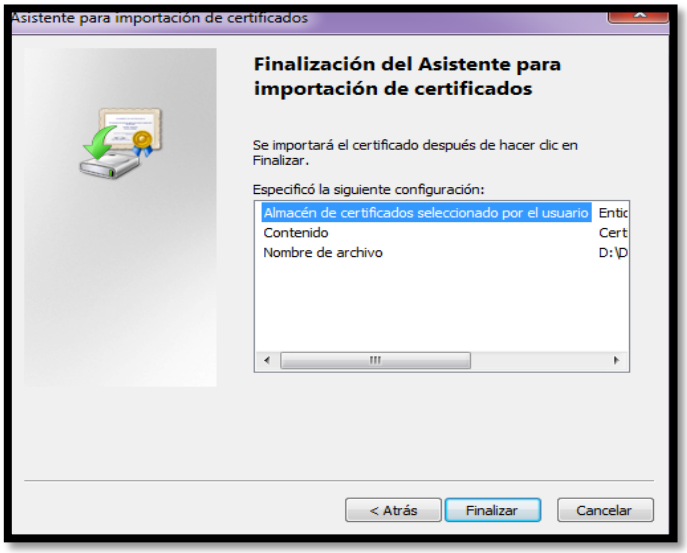


Figura IV. 124 Detalles de la instalación

- Pulsar finalizar y aparece un mensaje de advertencia indicando si está seguro o no de instalar el certificado en el sistema, aceptar.

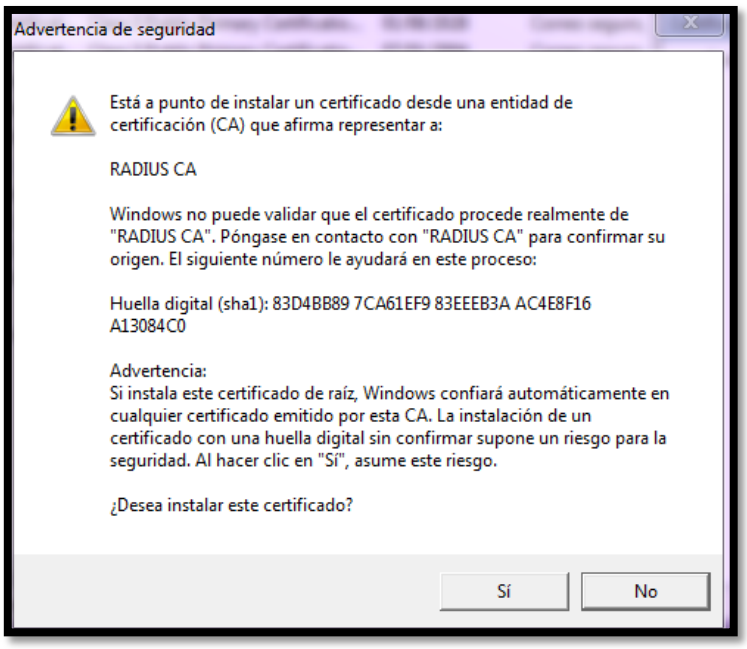


Figura IV. 125 Confirmación de instalación

- Se muestra un mensaje que comunica que la importación se ha realizado correctamente.

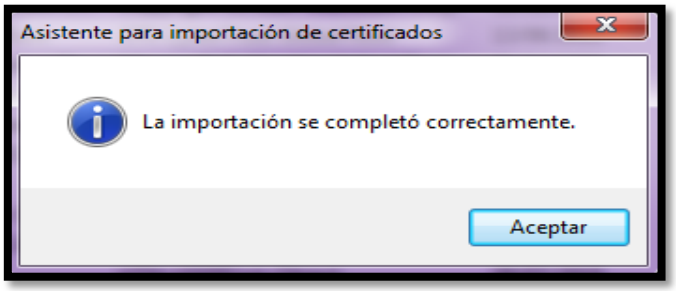


Figura IV. 126 Importación finalizada

- Se observa que a la lista de autoridad certificadora anterior se ha añadido, la CA creada en el servidor RADIUS y llamada RADIUS CA.

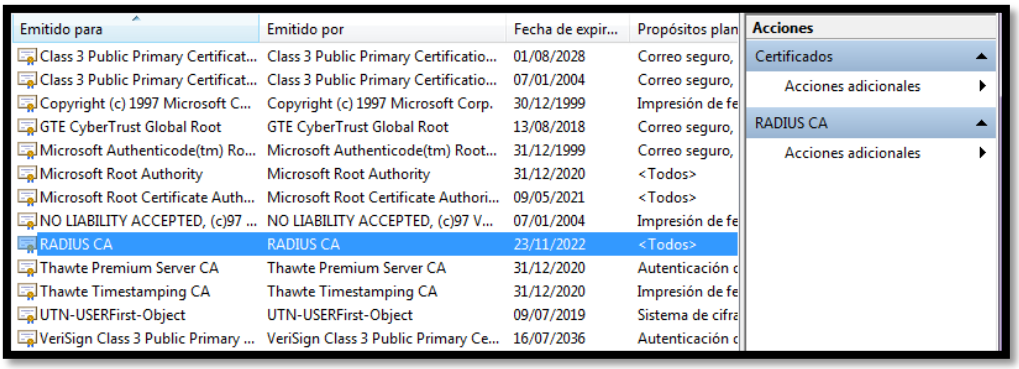


Figura IV. 127 Lista de CA

- Al hacer doble clic sobre la CA se muestran todos los detalles de esta.

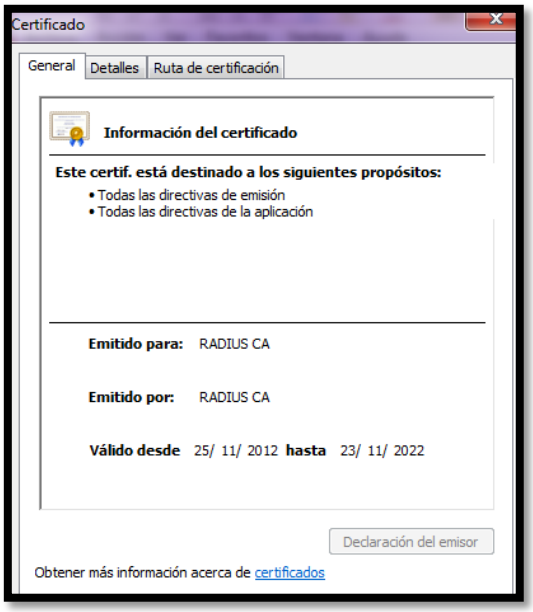


Figura IV. 128 Detalles de la CA

4.4.6.4. Instalación de la Clave Privada

- Hacer doble clic sobre el certificado que se exporto, se muestra el asistente para importación de certificados y pulsar siguiente.

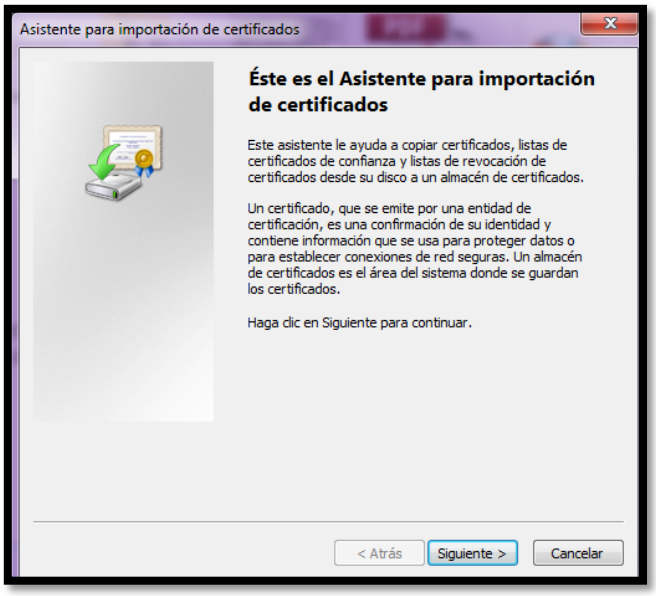


Figura IV. 129 Instalación de clave privada

- Se muestra el lugar donde se encuentra almacenado el certificado, verificar si es correcto y hacer clic en siguiente.

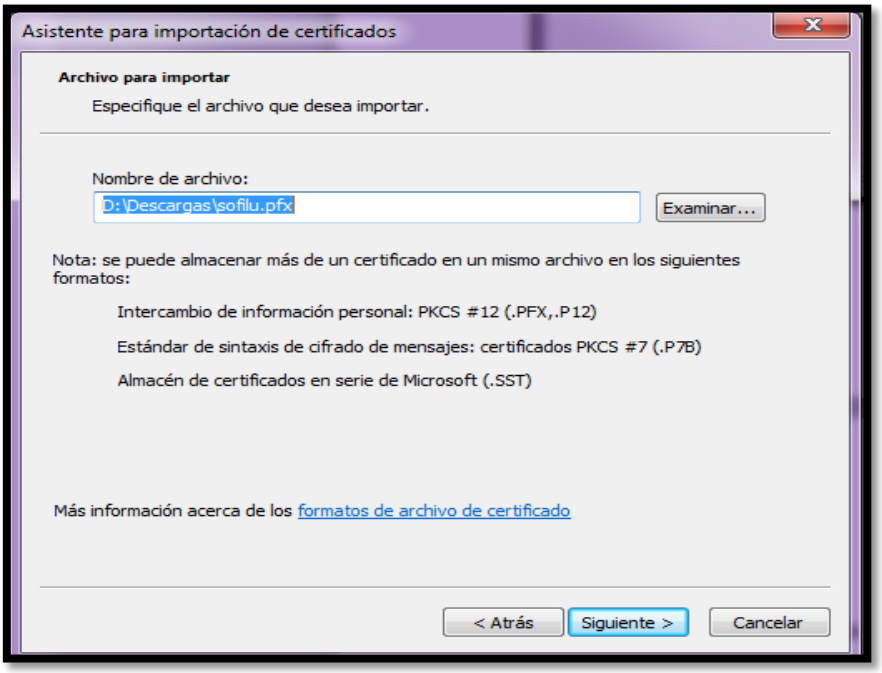


Figura IV. 130 Ubicación de certificado

- Para mayor seguridad en la instalación, se pide ingresar la contraseña de la clave privada que se configuro al crearse el certificado, marcar el casillero para que se incluyan las propiedades extendidas y hacer clic en siguiente.

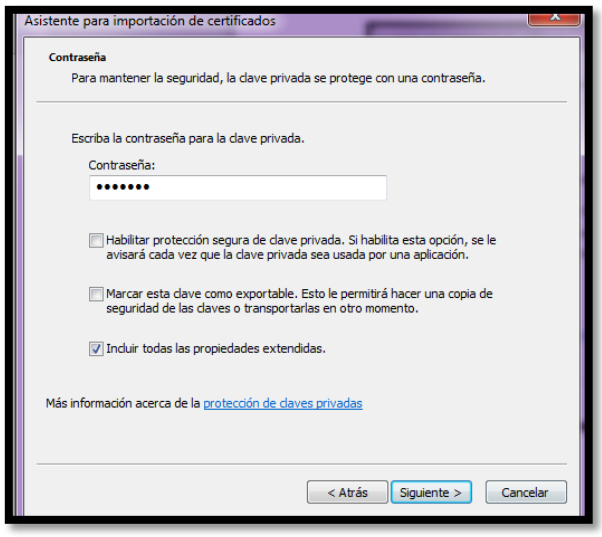


Figura IV. 131 Ingreso de contraseña de clave privada

- A continuación hay que elegir el almacén del certificado

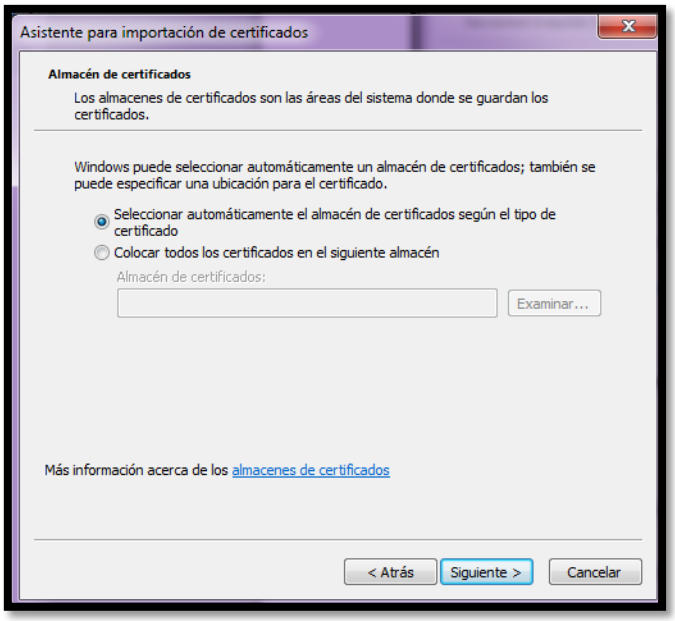


Figura IV. 132 Selección de almacén

- Marcar en la opción Colocar todos los certificados en el siguiente almacén y hacer clic en el botón examinar y se mostrara las opciones de almacén con las que cuenta.

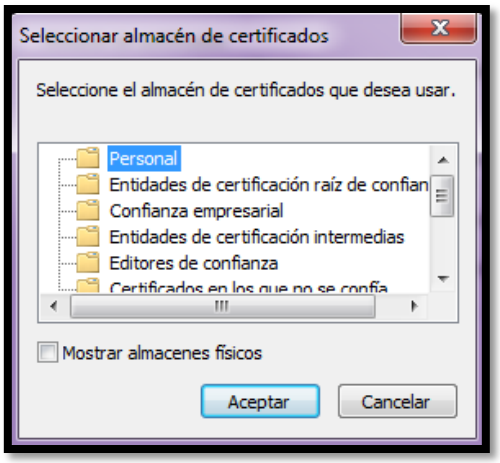


Figura IV. 133 Lista de almacenes de certificados

- Como es la clave privada hay que elegir como almacén de certificado a Personal y no a Entidades de certificación de confianza como fue el caso de la clave pública y aceptar.

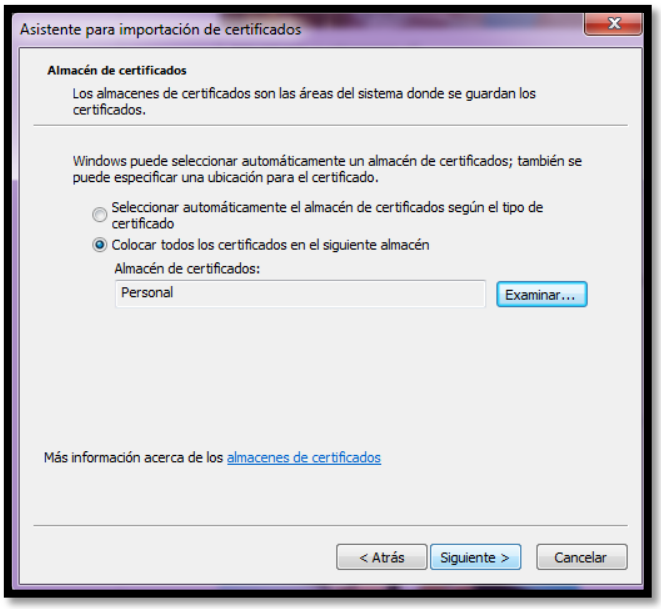


Figura IV. 134 Selección de almacén personal

- Al hacer clic en siguiente se muestran los detalles del certificado que se quiere instalar, se debe revisar con mucha atención para verificar si existe algún error y regresar a corregirlo, caso contario hacer clic en finalizar.

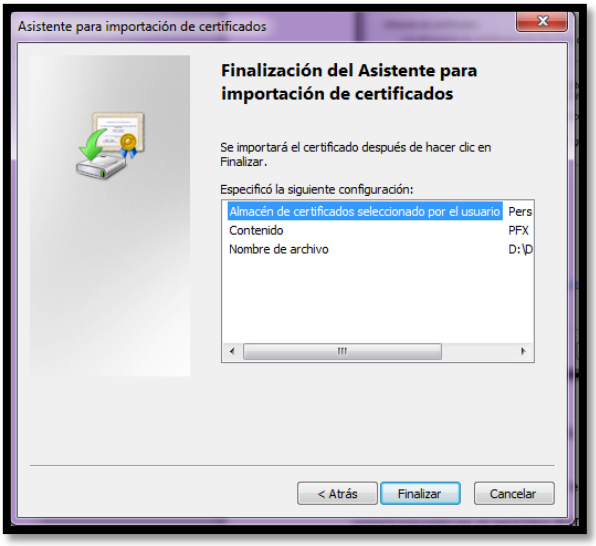


Figura IV. 135 Detalles del certificado

- Por último se muestra un mensaje indicando que la importación se realizó correctamente

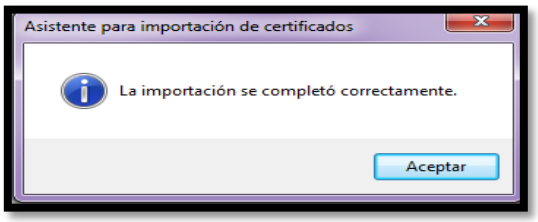


Figura IV. 136 Importación finalizada

4.4.7. CREAR LA RED INALÁMBRICA

Es necesario crear un perfil de red inalámbrica que se ajuste a los parámetros configurados anteriormente en el servidor RADIUS y en el AP.

- Ingresar al panel de control, escoger la opción Redes e Internet, Centro de redes y recursos compartidos y en Administrar redes Inalámbricas.

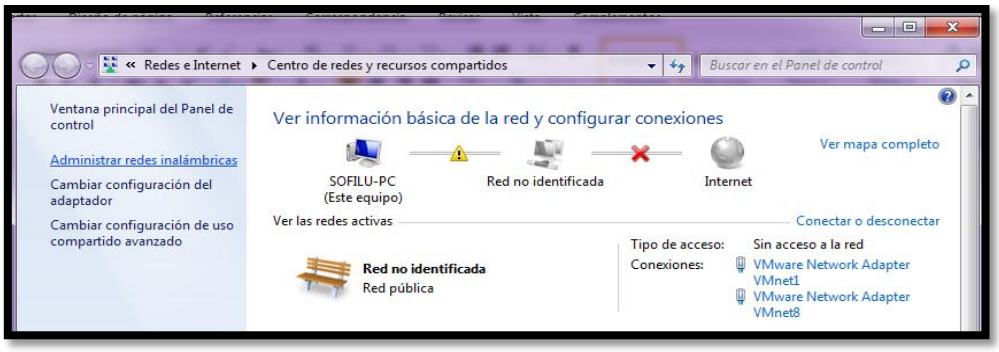


Figura IV. 137 Administración de redes inalámbricas

- Hacer clic en la pestaña agregar.

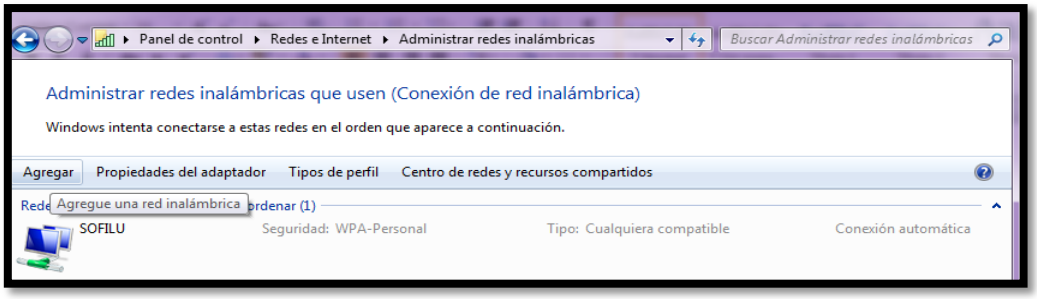


Figura IV. 138 Agregar red inalámbrica

- Escoger la opción crear un perfil de red manualmente.

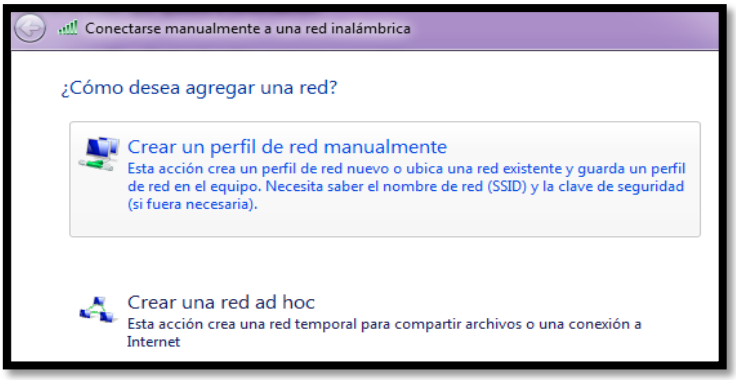


Figura IV. 139 Creación manual de perfil

- Ingresar el nombre de la red, el tipo de seguridad y cifrado que tendrá la red, estos parámetros deben coincidir con los configurados en el Access Point.

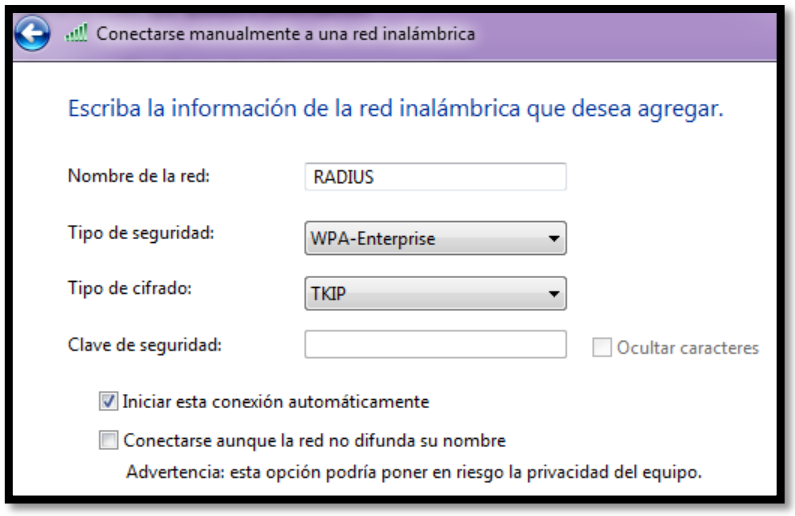


Figura IV. 140 Parámetros de red

- Al aceptar se genera un mensaje indicando que la red ha sido agregada correctamente, para adecuar la red a los requerimientos de RADIUS, hacer clic en la opción cambiar la configuración de conexión.

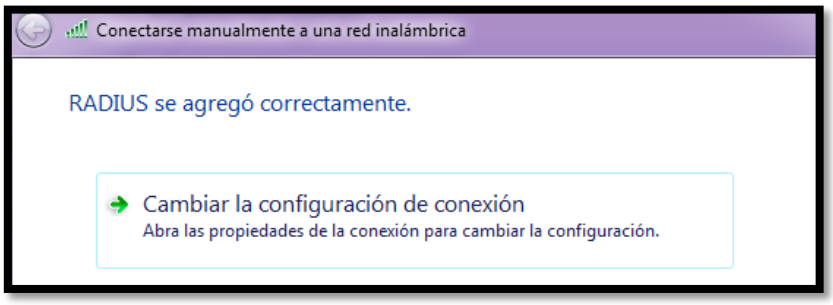


Figura IV. 141 Configuración de conexión

- En la ventana que se abre, hacer clic en la pestaña seguridad y escoger como método de autentificación de red a Microsoft EAP protegido (PEAP) y hacer clic en el botón configuración.

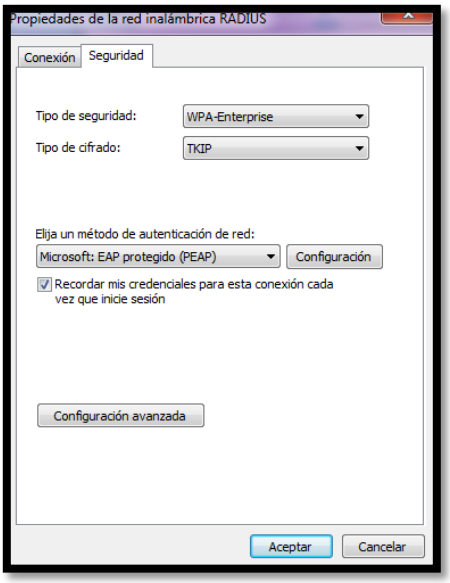


Figura IV. 142 Método de Autenticación

- Desmarcar el casillero de Validar un certificado de servidor, en método de autentificación elegir Contraseña segura (EAP-MSCHAP v2) y hacer clic en el botón configurar.

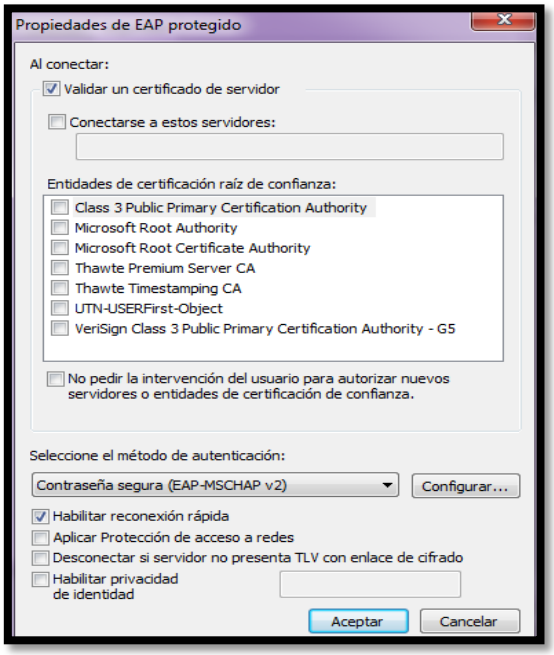


Figura IV. 143 Validación de certificado

- Se debe desmarcar la casilla que indica el uso automático del nombre de inicio de sesión y contraseña de Windows.

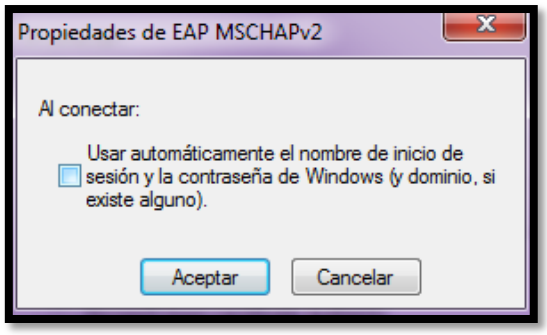


Figura IV. 144 Selección de modo de inicio de sesión

- Aceptar para que se guarden los cambios realizados, volver a la pantalla principal de las propiedades de la red inalámbrica que se está configurando y hacer clic en opciones avanzadas.

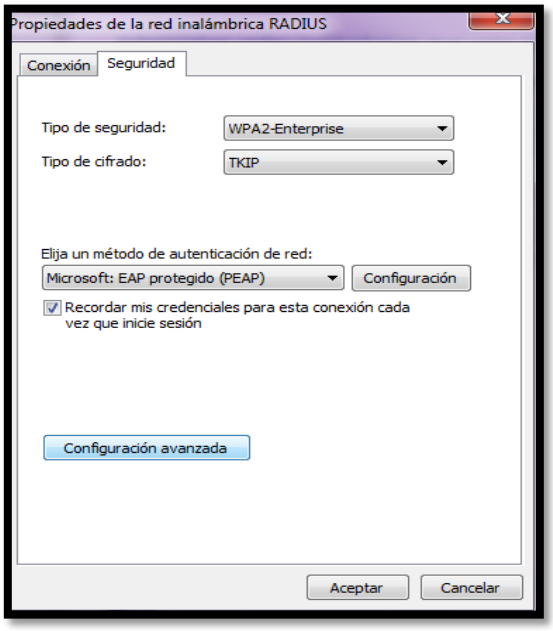


Figura IV. 145 Selección de configuración avanzada

- En esta ventana se debe elegir el modo de autentificación que se va a utilizar, para esto hay que marcar la casilla de Especificar modo de autentificación y escoger únicamente la opción autentificación de usuarios.

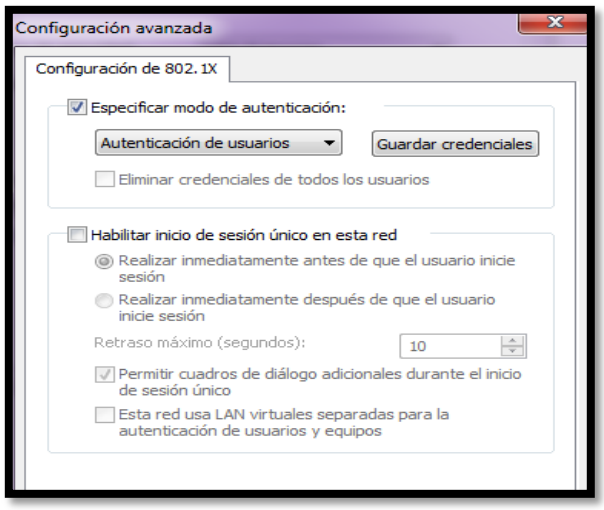


Figura IV. 146 Selección de modo de autentificación

- Finalmente pulsar en aceptar para que se guarde la configuración realizada, la red inalámbrica esta lista para ser usada.

4.4.8. REALIZACIÓN DE UNA PRUEBA

- Para probar el correcto funcionamiento del servidor, simplemente conectar el computador a la red inalámbrica configurada anteriormente y se va a mostrar un cuadro en el cual hay que ingresar el nombre de usuario y contraseña que se registró en el servidor RADIUS, recordando que únicamente se podrá autentificar con las credenciales asignadas al usuario del cual se instaló el certificado digital.

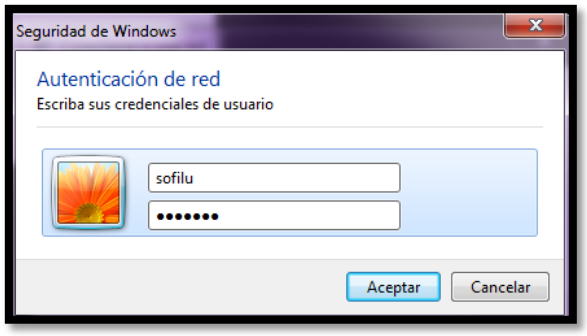


Figura IV. 147 Ingreso de credenciales para conexión a la red

- Si el nombre de usuario y contraseña son correctos, el usuario será exitosamente autenticado a la red y podrá gozar de los recursos que esta posea.

4.4.9. CONFIGURACIÓN DE UN CLIENTE UBUNTU

4.4.9.1. Instalación de WICD

- WICD es un gestor de redes inalámbricas bastante completo que detecta distintos tipos de cifrado como WEP, WPA, WPA2, etc.
- Instalar wicd, desde los repositorios propios de Ubuntu, mediante línea de comando.

```
sofilu@ubuntu:~$ sudo apt-get install wicd
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  wicd
0 upgraded, 1 newly installed, 0 to remove and 481 not upgraded.
Need to get 0 B/4,434 B of archives.
After this operation, 47.1 kB of additional disk space will be used.
WARNING: The following packages cannot be authenticated!
  wicd
Install these packages without verification [y/N]? y
Selecting previously unselected package wicd.
(Reading database ... 140605 files and directories currently installed.)
Unpacking wicd (from .../wicd_1.7.2.3-1ubuntu0.1_all.deb) ...
Setting up wicd (1.7.2.3-1ubuntu0.1) ...
sofilu@ubuntu:~$
```

Figura IV. 148 Comando para Instalar WICD

- Para ejecutar el programa, basta con ingresar el comando sudo wicd, pero al querer iniciarlo se produce un error.

```
sofilu@ubuntu:~$ sudo wicd
It seems like the daemon is already running.
If it is not, please remove /var/run/wicd/wicd.pid and try again.
```

Figura IV. 149 Inicio fallido de WICD

- Como indico el mensaje, se debe eliminar el archivo /var/run/wicd/wicd.pid, para que se pueda iniciar el programa.

```
sofilu@ubuntu:~$ sudo rm /var/run/wicd/wicd.pid
```

Figura IV. 150 Eliminación del archivo wicd.pid

- Volver a ejecutar el comando: sudo wicd, esta vez ya no se debe mostrar ningún mensaje de error, esto indicara que se inició exitosamente.

```
sofilu@ubuntu:~$ sudo wicd
sofilu@ubuntu:~$
```

Figura IV. 151 Inicio del Gestor WICD

4.4.9.2. Creación del Perfil de Red Inalámbrica

- Para crear la red inalámbrica, es necesario ingresar al modo gráfico del gestor wicd, para esto en buscar ingresamos wicd y se mostrara el icono de este programa.

Figura IV. 152 Icono de WICD

- Al hacer doble clic en el icono de wicd, se abre una ventana en la cual, se debe hacer clic en Add para ingresar el nombre del perfil de red que se vaya a crear.

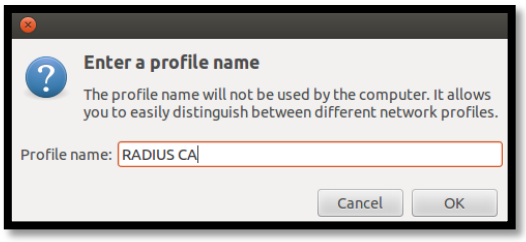


Figura IV. 153 Ingreso del Nombre del Perfil de Red

- Ya registrado el nombre, hacer clic en properties para ingresar los parámetros de configuración necesarios, para que pueda ser autenticado en el servidor RADIUS.

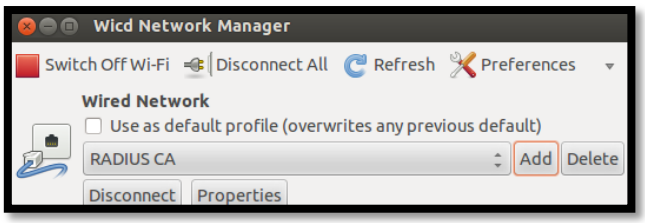


Figura IV. 154 Interfáz Gráfica de WICD

- Marcar el casillero Use Encryption y escoger como método de autentificación a 802.1x, en identity colocar el nombre de usuario y en Password el secreto compartido que se configuró anteriormente en el servidor RADIUS.

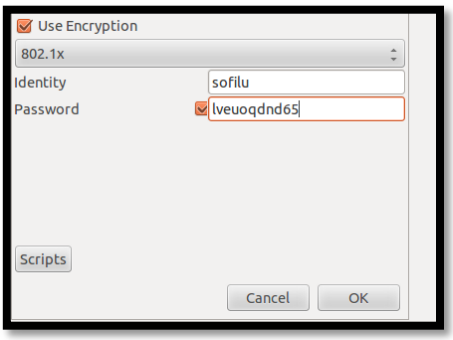


Figura IV. 155 Configuración de los Parámetro de red

- Hacer clic en aceptar para que se guarde la configuración realizada anteriormente.

4.4.9.3. Copia de los Certificados Digitales

- A diferencia de Windows, para las distribuciones de Linux en general, no hace falta instalar los certificados digitales, solo se los debe copiar en los directorios adecuados.
- La clave privada se debe copiar dentro del directorio /etc/ssl/private

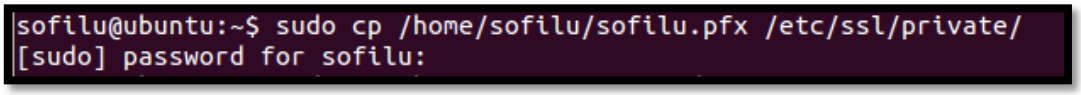


Figura IV. 156 Directorio para almacenar la Clave Privada

- La clave pública se coloca dentro del mismo directorio principal /etc/ssl/certs

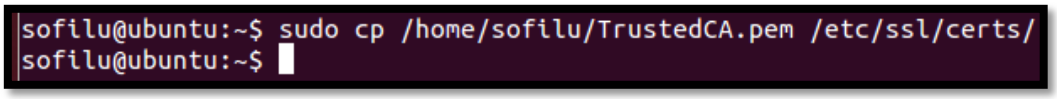


Figura IV. 157 Directorio para almacenar la Clave Pública

- Para autenticarse en el servidor RADIUS, al igual que con un cliente Windows simplemente hay que conectarse a la red inalámbrica, con el nombre de usuario y secreto compartido que se configuro para ese usuario.

CONCLUSIONES

1. Mediante un adecuado conocimiento de los dos servidores de autentificación en estudio, se logra tener un mejor panorama a la hora del diseño e implementación de una red inalámbrica, con los parámetros adecuados de rendimiento y seguridad.

2. El análisis comparativo nos permitió determinar el servidor de autentificación más eficiente y que mejor se adapte a la mayoría de redes inalámbricas desarrolladas en la actualidad, proporcionando un mayor grado de seguridad.

3. Los resultados obtenidos en los módulos de prueba realizados muestran las fortalezas y debilidades que posee cada servidor de autentificación, como es el caso de la utilización eficiente de los recursos Hardware y Software para realizar el proceso de autentificación de uno o varios usuarios, parámetros que fueron de mucha utilidad para la demostración de la hipótesis.

4. El indicador en el cual se notó más la diferencia es en Gestión de Usuarios pues RADIUS obtuvo un 100% de grado de facilidad en la ejecución de las tres tareas principales que un administrador realiza con mayor frecuencia, como son el ingreso, modificación y eliminación de usuarios. Frente a un 66,66% de LDAP, ya que al no contar con una interfaz gráfica, estas tareas se vuelven más complejas de realizar.

5. En cuanto a la seguridad ambos servidores, se encuentran en similar condición, ya que soportan cifrado y una variedad de funciones hash que permiten un proceso de autentificación bastante seguro, por lo tanto obtuvieron el mismo porcentaje de 57,14%.

6. RADIUS fue desarrollado para soportar un gran número de usuarios y varias transacciones simultáneas debido a la facilidad con la que se pueden realizar estas tareas. Por esta razón es usado por ISPs para controlar el acceso de sus Usuarios y facturar los servicios, lo que no ocurre con LDAP ya que al no ser una base de datos relacional los cambios en la información almacenada resultan más complejos, debido a esto está orientado a Empresas donde la información no está en modificación constante.

7. La implementación de certificados digitales en lugar del nombre de usuario y contraseña que se utiliza para la autentificación en la mayoría de sistemas convencionales, le añade cierto nivel de seguridad, pues al autenticarse permite la creación de un túnel que encriptara todos los datos que se transmitan mientras dure la sesión, también es cierto que esto generara un aumento en el uso del ancho de banda.

8. En cuanto al rendimiento se destaca LDAP con 7,78 frente a un 4,44 de RADIUS, sin embargo necesita de un servidor adicional para su funcionamiento, esto conlleva el consumo de más recursos, incluso su implementación se hace mucho más compleja, ya

que se debe realizar una conexión entre el servidor LDAP y el Proxy que actúa como un intermediario.

9. Al final del análisis comparativo, RADIUS posee el valor más alto en eficiencia, con un 74,67% frente a LDAP con el 70,52%, superándolo de esta manera en aproximadamente un 6%, convirtiéndolo en el servidor más idóneo para su implementación en cualquier empresa o institución que requiera tener un control sobre el acceso de los usuarios a los recursos de la red y al mismo tiempo brindar un mayor grado de seguridad. Los dos protocolos RADIUS y LDAP establecen un canal de comunicación seguro, es decir, la información está protegida no solo en el momento de autentificarse, sino durante el tiempo que dura la conexión.

RECOMENDACIONES

1. Al momento de seleccionar un servidor para el control de acceso, se debe considerar el grado de facilidad en cuanto a instalación y administrador que posee el servidor, para que el trabajo del administrador del sistema no se torne compleja.

2. Para configurar una red inalámbrica con autentificación mediante RADIUS, se debe constatar que el AP soporte el protocolo 802.1X.

3. Se debe realizar una análisis previo del número promedio de usuarios simultáneos que se van a conectar al AP, para verificar si es necesario añadir más AP a la red, además de si el servidor RADIUS soporta ese número de usuarios o si de igual manera es necesario adicionar más servidores.

4. Se recomienda que los certificados en el cliente sean instalados únicamente por el administrador del servidor, pues sería una tarea muy tediosa y con cierto grado de dificultad para un usuario normal, ya que no poseen el conocimiento necesario.

5. Tener mucho cuidado en los algoritmos de cifrado y mecanismos de control de acceso que se configuren, recordando que deben ser los mismos que se configuran tanto en el AP como en el perfil de red inalámbrica que se crea en el cliente, si esto no sucede no existirá conexión entre el cliente y el servidor.

6. Es recomendable que el secreto compartido entre el servidor RADIUS y el AP sea lo suficientemente complejo, es decir combinando números, letras mayúsculas y minúsculas, para que evitar que sufra ataques de diccionario.

7. Recordar que el usuario se autentifica en el servidor, mediante la clave de la llave privada que se creó en el servidor RADIUS, mediante esta se encripta o desencripta la información.

8. Tomar en cuenta que al crear un certificado, este tiene un tiempo de validez, pasado dicho tiempo el certificado se vuelve obsoleto y la CA lo añade a la lista de certificados revocados, razón por la cual debe ser renovado para tener acceso a los recursos de la red nuevamente.

9. Se recomienda la implementación de RADIUS en empresas que tienen que soportar un gran número de usuarios y varias transacciones simultáneas debido a la facilidad con la que se pueden realizar estas tareas. Por esta razón es usado por ISPs para controlar el acceso de sus Usuarios y facturar los servicios, lo que no ocurre con LDAP ya que al no ser una base de datos relacional los cambios en la información almacenada resultan más complejos, además está orientado a empresas donde la información no está en modificación constante.

RESUMEN

Análisis comparativo de servidores de autentificación RADIUS y LDAP complementado con el uso de certificados digitales para mejorar la seguridad en el acceso a redes Wifi y su aplicación como prototipo de un sistema de autentificación para una red inalámbrica en general.

Utilizando el método científico experimental, se desarrolló ambientes de prueba de los servidores en estudio para establecer las diferencias que existen entre estos, mediante las herramientas de software daloRADIUS, MySQL, OpenLDAP 2.2.5, ZeroShell 2.0 y Squid-2.5. Además de la observación que permitió determinar cuál es el servidor más eficiente y para qué tipo de red son más adaptables, utilizando técnicas de revisión bibliográfica para la instalación, configuración, administración y monitoreo de los servidores.

Se compararon los siguientes indicadores: Gestión de usuarios, Autentificación, Gestión de Datos, Rendimiento, Funcionalidad y seguridad, dando como resultado que LDAP tiene el 70,52% de eficiencia y RADIUS un 74,67%, estableciéndose una diferencia de aproximadamente un 6% entre los dos servidores de autentificación

Se concluye que el servidor de autentificación más eficiente para ser implementado en una red inalámbrica es RADIUS, debido a la facilidad de administración que presenta y la rapidez con la que se realizan las actualizaciones de datos.

Se recomienda la utilización de certificados digitales como credenciales para poder conectarse a la red, en lugar del usuario y contraseña tradicional que se utiliza en la autentificación convencional, para añadirle mayor seguridad en el proceso de autentificación.

SUMMARY

This investigation was carried out to make a Comparative analysis authentication servants Remote Authentication Dial-In User Server (RADIUS) and Lightweight Directory Access Protocol (LDAP) supplemented with use digital certificates to improve the security in access to nets wifi and their application like prototype of an authentication system for a wireless net in general.

The experimental scientific method was used to develop atmosphere set of test the servants in study in order to establish the differences that exists among these, by means of tools software daloRADIUS, MySQL, OpenLDAP 2.2.5, ZeroShell 2.0 and Squid-2.5. Besides the observation allowed determining the most efficient servant is what reason net type for, they are more adaptive, using technical of bibliographical revision for the installation, configuration, administration and monitored servants.

Then, the following indicators were compared: Usernames' management, Authentication, Data Management, Performance, Functionality and Safety, resulting in LDAP has 79,52% of efficiency and RADIUS 74,67%, settling down a difference of approximately 6% among two authentication servants.

It conclude that the most efficient authentication to be implanted in a wireless network is RADIUS, due to administration easiness that presents and speed, which are carried out the upgrades data.

It recommended the use of digital certificates as credentials to connect the network instead of the traditional username and password authentication is used in conventional, to add greater security authentication process.

BIBLIOGRAFÍA

1. **LIZA, L.,** Diseño de una red local inalámbrica utilizando un sistema de seguridad basado en los protocolos wpa y 802.1x para un complejo hotelero., Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería, Ingeniería Electrónica ., Lima – Perú., **TESIS**., 2007., Pp. 53 – 73.

2. **MATANZO, A.,** Implementación del Protocolo CHAP en un Sistema de Seguridad para Redes WLAN., Universidad de las Américas Puebla, Facultad de Ingeniería y Ciencias, Ingeniería en Sistemas Computacionales., Puebla – México., **TESIS**., 2006., Pp. 35 – 49.

3. **ORTÍZ, S.,** Diseño e implementación de una infraestructura de claves públicas jerárquicas con certificados digitales X.509 y su aplicación en redes 802.11 con el estándar 802.1X., Escuela Politécnica Nacional, Facultad de Ingeniería Eléctrica y Electrónica, Ingeniería Electrónica y Redes de Información., Quito – Ecuador., **TESIS**., 2006., Pp. 125 – 146.

4. **RAMOS, F.,** Estudio de un sistema de Configuración para Redes Inalámbricas con Seguridad de Servidor., Universidad Técnica de Ambato, Facultad de Ingeniería en Sistemas, Electrónica e Industrial, Ingeniería en Sistemas Informáticos y., Ambato – Ecuador., **TESIS**., 2009., Pp. 12 – 42.

5. SERVIDOR LDAP LINUX

http://www.linuxparatodos.net/portal/staticpages/index.php?page=servidor-ldap
2012/07/12

6. INSTALACIÓN Y CONFIGURACIÓN DE LDAP

http://www.codigofantasma.com/blog/instalar-y-configurar-servidor-ldap-en-ubuntu-linux/
http://www.docmirror.net/es/linux/howto/misc/LDAP-Linux-Como/LDAP-Linux-Como-2.html
2012/07/15

7. INTEGRACIÓN DE SQUID CON LDAP

http://www.alcancelibre.org/staticpages/index.php/19-1-como-squid-autenticacion
http://gnunick.blogspot.com/2011/06/integrando-squid-con-ldap.html
2012/07/28

8. INSTALACIÓN Y CONFIGURACIÓN DE DALORADIUS

http://blog.e2h.net/2011/07/01/servidor-radius-con-gestion-web-freeradius-daloradius/
http://www.soportejm.com.sv/kb/index.php/article/daloradius
2012/08/05

9. CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA

http://www.kzgunea.net/docs/cursos/Izenpe/castellano/capitulo2-2.htm
2012/08/12

10. SOLUCIONES DE SEGURIDAD INALÁMBRICA

http://www.cisco.com/web/LA/soluciones/comercial/proteccion_wireless.html
2012/08/25

11. INSTALACIÓN Y CONFIGURACION DE ZEROSHELL

http://www.zeroshell.net/listing/zeroshell-manual-spanish.pdf
http://www.nomatch.es/media/2246/cursozeroshell.pdf
2012/09/14

12. CONFIGURACIÓN DEL CLIENTE WINDOWS PARA AUTENTICAR EN RADIUS

http://www.masqueteclas.com/2012/03/autenticar-conwindows-xp7-en.html
2012/10/12

13. CONFIGURACIÓN DEL ACCESS POINT

http://personales.alumno.upv.es/~hecmargi/manuales/linux/freeradius/
2012/11/14

ANEXOS

ANEXO 1

INSTALACIÓN DE FREERADIUS CON MYSQL

REQUERIMIENTOS

- Ubuntu 10.10
- Freeradius

Instalación de paquetes necesarios (Instalación LAMP)

Para comenzar la instalación del servidor Freeradius, debemos instalar el paquete LAMP, que incluye Apache, PHP y Mysql.

En el terminal, con permisos de root, se ejecutan los siguientes comandos:

- **Instalación de Apache**

apt-get install apache

Para comprobar que todo se instaló correctamente, se escribe en la barra de direcciones del navegador lo siguiente:

http://localhost

- **Instalación de PHP y MySQL**

  # apt-get install php5 libapache2-mod-php5 php5-cli php5-mysql
  # apt-get install mysql-server
  #apt-get install mysql-client mysql-admin mysql-query-browser libmysqlclient15-dev
  #mysql –u root -p
  #apt-get install phpmyadmin

- **Instalación de Librerías necesarias**

  #apt-get install debhelper libltdl3-dev libpam0g-dev libmysqlclient15-dev build-essential
  libgdbm-dev libldap2-dev libsasl2-dev libiodbc2-dev libkrb5-dev snmp autotools-dev dpatch libperl-dev libtool dpkg-dev libpq-dev libsnmp-dev libssl-dev

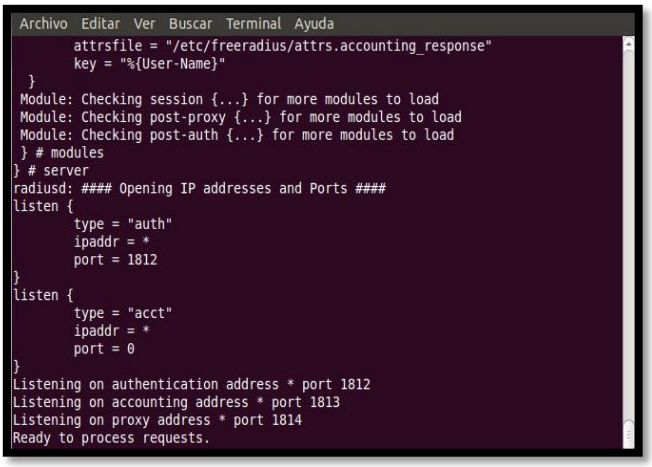
Instalación Freeradius y soporte MySQL

apt-get install freeradius freeradius-mysql

Se inicia el servidor RADIUS en modo debug, así:

freeradius stop
#freeradius -f -X

De esta manera se puede observar un log de todas las acciones que se realizan con el servidor.



Para probar la conexión con el servidor:

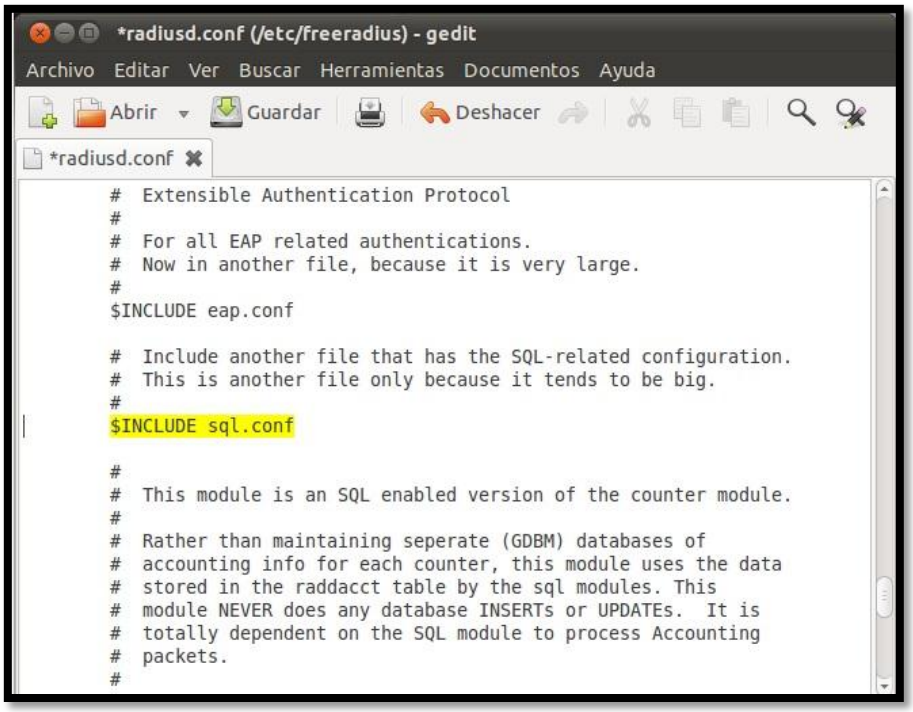
#radtest steve testing 127.0.0.1 1812 testing123

Y se recibe una repuesta del servidor, ya sea aceptando o rechazando la autenticación del usuario:

- **CONFIGURACIÓN DE MYSQL**

Editar el archivo, que se encuentra localizado en el path:

/etc/freeradius/radiusd.conf y descomentamos la linea "$INCLUDE sql.conf"



Para acceder a la administración de MySQL por consola, se ingresa el siguiente comando:

#mysql -u root -p

Se crea la base de datos:

> CREATE DATABASE radius;

Se asigna Usuario y Contraseña para la base de datos creada:

> GRANT all ON radius.* TO radius@localhost IDENTIFIED BY 'radius';

Utilizando el usuario radius asignado, se inserta en la base de datos con los esquemas incluidos con Freeradius:

#mysql -uradius -pradius radius < /etc/raddb/sql/mysql/cui.sql
#mysql -uradius -pradius radius < /etc/raddb/sql/mysql/ippool.sql
#mysql -uradius - pradius radius < /etc/raddb/sql/mysql/nas.sql

#mysql -uradius - pradius radius < /etc/raddb/sql/mysql/schema.sql

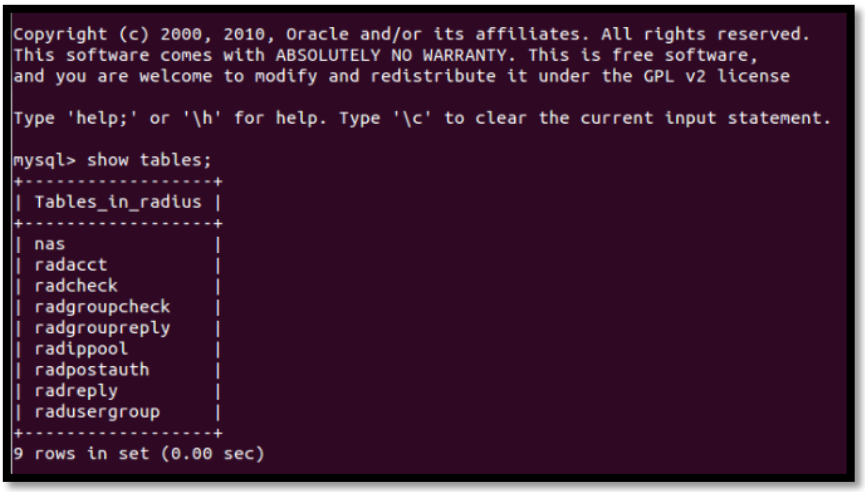
#mysql -uradius - pradius radius < /etc/raddb/sql/mysql/wimax.sql

Para ver las tablas creadas:

#mysql -u root -p

>use radius;

>show tables;



Se edita el archivo /etc/freeradius/sql.conf

#nano /etc/freeradius/sql.conf

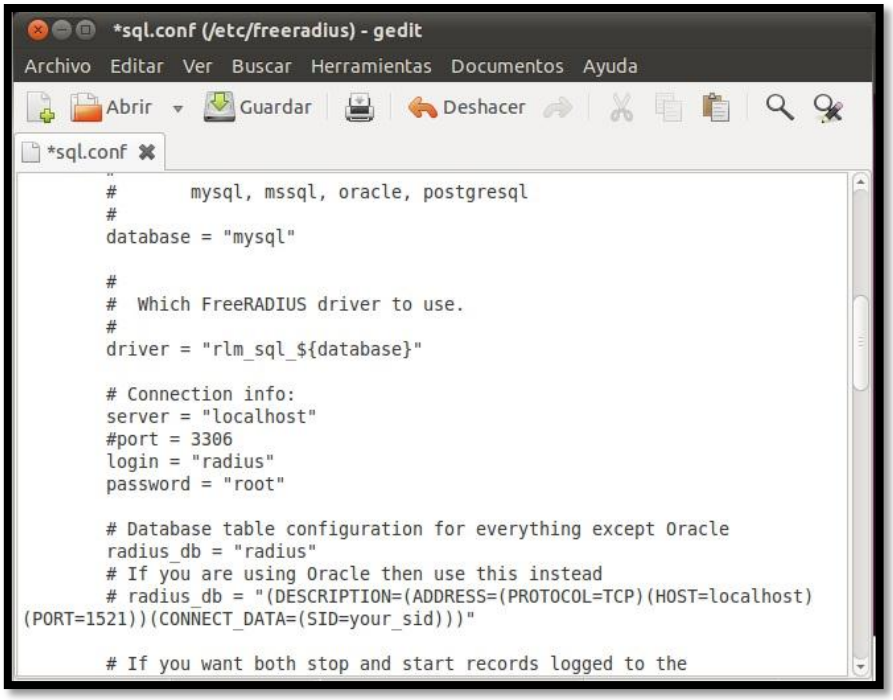
Se realiza la siguiente configuración para la conexión con el servidor MySQL:

Es necesario editar el archivo /etc/freeradius/radiusd.conf y descomentar la linea $INCLUDE sql.conf

```
#  Include another file that has the SQL-related configuration.
#  This is another file only because it tends to be big.
#
$INCLUDE sql.conf

#
#  This module is an SQL enabled version of the counter module.
#
#  Rather than maintaining seperate (GDBM) databases of
#  accounting info for each counter, this module uses the data
#  stored in the raddacct table by the sql modules. This
#  module NEVER does any database INSERTs or UPDATEs.  It is
#  totally dependent on the SQL module to process Accounting
#  packets.
#
$INCLUDE sql/mysql/counter.conf

#
#  IP addresses managed in an SQL table.
#
$INCLUDE sqlippool.conf
```

Connection info:

server = "localhost"
login = "radius"
password = "radius"

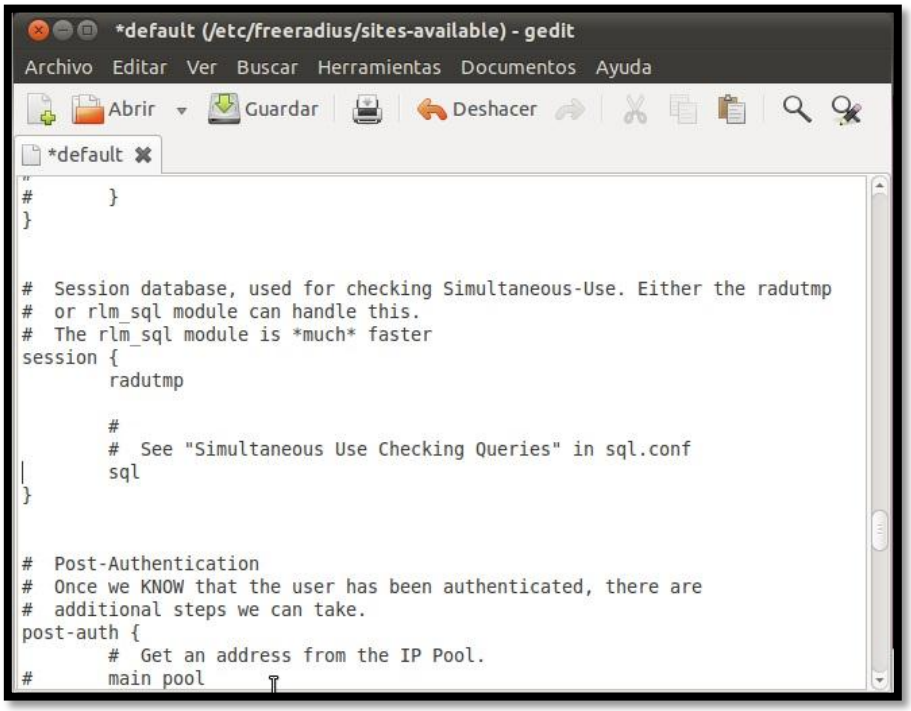


Y se descomenta la variable: readclients = yes

```
        # Set to 'yes' to read radius clients from the database ('nas' table)
        # Clients will ONLY be read on server startup.  For performance
        # and security reasons, finding clients via SQL queries CANNOT
        # be done "live" while the server is running.
        #
        readclients = yes

        # Table to keep radius client info
        nas_table = "nas"
```

Se edita el archivo **/etc/freeradius/sites-available/default** y se agrega la variable "sql" en las secciones de: authorize{}, accounting{}, session{}, postauth{} esto permite traer los datos desde las tablas en la base de datos "radius".

#nano /etc/freeradius/sites-available/default



Para comprobar las configuraciones, se crea un usuario en la base de datos, con el siguiente comando:

> INSERT INTO radcheck (username, attribute, value) VALUES ('usuario1', 'Password', 'root');

```
mysql> use radius;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> insert into radcheck(username, attribute, value) values('usuario1', 'pass
word', 'root');
Query OK, 1 row affected (0.00 sec)

mysql>
```

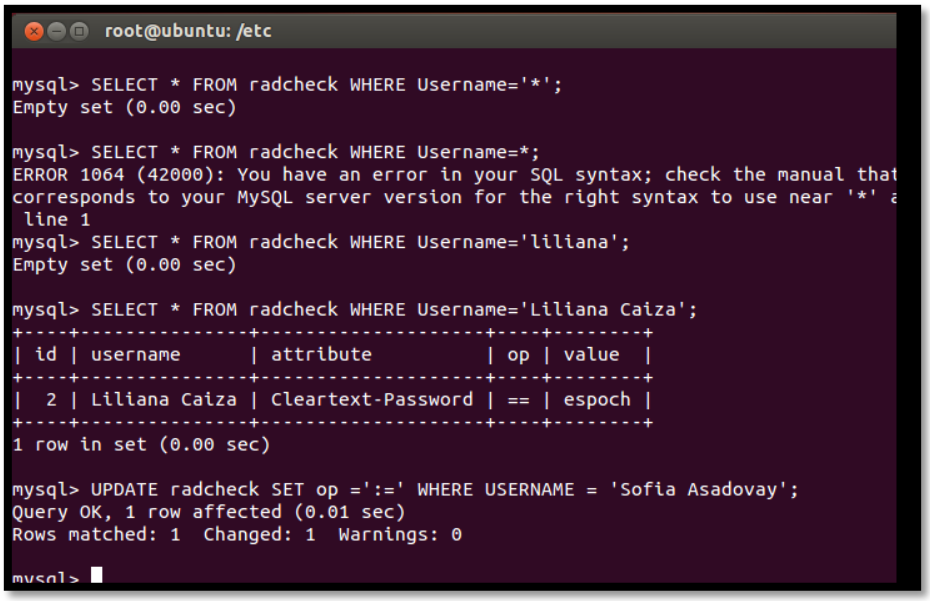
```
root@ubuntu: /etc

mysql> INSERT INTO radcheck (UserName, Attribute, Value) VALUES ('sofia', 'Clea
text-Password', 'sofilu');
Query OK, 1 row affected (0.05 sec)

mysql> select .* from radius;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near '* fr
m radius' at line 1
mysql> select * from radius;
ERROR 1146 (42S02): Table 'radius.radius' doesn't exist
mysql> select * from radius limit 11,10;
ERROR 1146 (42S02): Table 'radius.radius' doesn't exist
mysql> select * from radius limit 5;
ERROR 1146 (42S02): Table 'radius.radius' doesn't exist
mysql> SELECT * FROM radcheck WHERE Username='sofia';
+----+----------+--------------------+----+---------+
| id | username | attribute          | op | value   |
+----+----------+--------------------+----+---------+
|  1 | sofia    | Cleartext-Password | == | sofilu |
+----+----------+--------------------+----+---------+
1 row in set (0.03 sec)

mysql>
```

Lo anterior equivale a añadir usuario1 Cleartext-Password := "root" en el fichero /etc/raddb/users.

Verifique que el usuario se dio de alta correctamente:

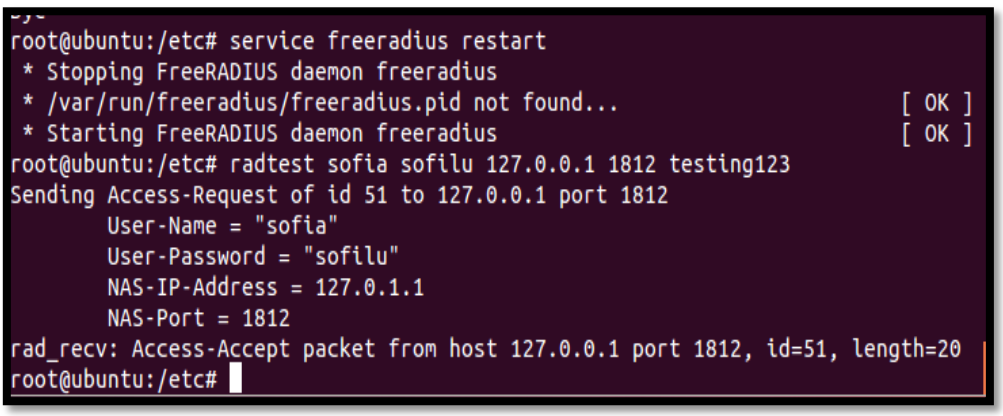
>select * from radcheck where username='usuario1';

```
mysql> select * from radcheck where username='usuario1';
+----+----------+-----------+----+-------+
| id | username | attribute | op | value |
+----+----------+-----------+----+-------+
|  1 | usuario1 | password  | == | root  |
+----+----------+-----------+----+-------+
1 row in set (0.00 sec)
```



Con el usuario creado en la base de datos MySQL, se prueba la autentificación en el Servidor RADIUS:

#radtest usuario1 root localhost 1812 testing123



En este punto, el servidor RADIUS sólo es capaz de autenticar usuarios de manera local local. Para que pueda hacerlo con **clientes remotos** (el punto de acceso será uno de ellos) se ha de modificar la tabla SQL. Para ello se utiliza la siguiente sentencia:

mysql > INSERT INTO nas (nasname, shortname, type, secret) VALUES ('192.168.1.1', 'tplink', 'other', 'admin');

El significado de cada uno de los parámetros es el siguiente:

- **nasname =** Dirección IP privada del cliente radius (en este caso la IP del punto de acceso)
- **shortname =** Nombre identificativo del cliente radius (puede ser cualquier valor)
- **type =** Tipo del dispositivo (cisco, etc.) se recomienda poner el valor other
- **secret =** Clave del usuario radius creado al principio, en nuestro caso radius.

Cada uno de los clientes radius que existan, se añadirá como nueva entrada en la tabla nas.

Para caso de pruebas, se ingresa la dirección del Servidor RADIUS en la tabla **nas.**

Servidor RADIUS con gestión Web: FreeRADIUS + daloRADIUS

Las tareas de Gestión de usuarios en la base de datos MySQl, se pueden realizar de una manera más fácil mediante una interfaz Web para el servidor RADIUS, denominada Daloradius.

Primero se instalan los paquetes necesarios y se descarga el paquete Daloradius de la siguiente dirección:

apt-get install php5-gd php-pear php-db

wget http://downloads.sourceforge.net/project/daloradius/daloradius/daloradius0.9-9/daloradius-0.9-9.tar.gz?r=http%3A%2F%2Fsourceforge.net%2Fprojects%2Fdaloradius%2Ffiles%2F&ts=1345296201&use_mirror=nchc

Se descomprime:

tar xvfz daloradius-0.9-9.tar.gz

mv daloradius-0.9-9 daloradius

Se mueve el archive a /var/www, el diredctorio del servidor Web.

mv daloradius-0.9-9 daloradius

mv daloradius /var/www

Es necesario configurar el sistema para que al ingresar usuarios mediante Daloradius, no se utilice una base diferente de MySQL:

cd /var/www/daloradius/contrib/db

mysql -u root -p radius < mysql-daloradius.sql

Se realiza la configuración del archivo de Daloradius:

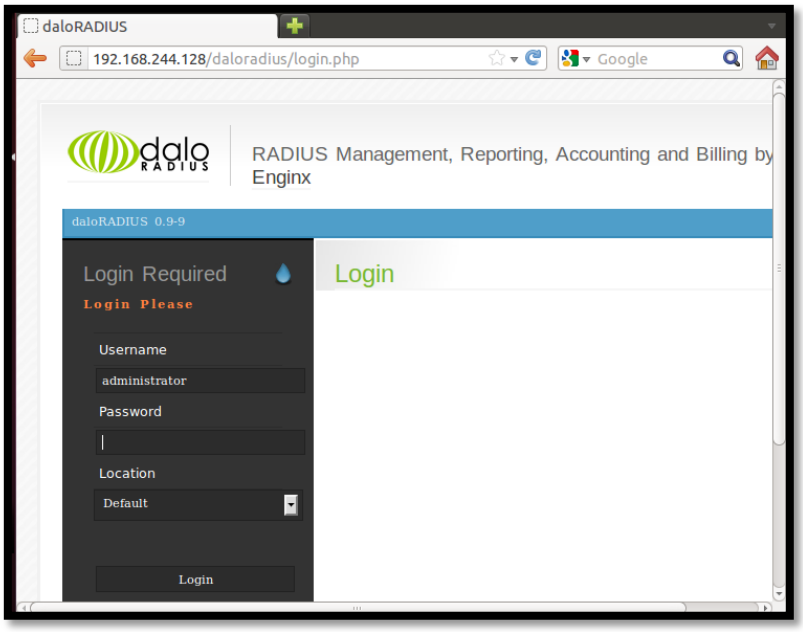
#vim /var/www/daloradius/library/daloradius.conf.php

Se cambia la contraseña de acceso al sistema:

$configValues['CONFIG_DB_PASS'] = 'radius';

Para accede al sistema, se coloca en el navegador la dirección IP del servidor Radius:

http://192.168.1.5./daloradius



Username: Administrator y Password: radius

Este sistema nos permite Gestionar a los Usuarios de manera más rápida e intuitiva, así como monitorear el rendimiento del Servidor, llevar un registro del acceso de cada usuario. De igual manera, los datos ingresados mediante línea de comandos se reflejan en la interfaz gráfica.

ANEXO 2

Instalación del Servidor OpenLDAP

Instalar los paquetes necesarios

```
[root@localhost ~]# yum -y install openldap*
```

```
Finished Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : openldap-servers                                [1/8]
  Installing     : cyrus-sasl-devel                                [2/8]
  Installing     : unixODBC                                        [3/8]
  Installing     : openldap-devel                                  [4/8]
  Installing     : openldap-servers-overlays                       [5/8]
  Installing     : openldap-clients                                [6/8]
  Installing     : compat-openldap                                 [7/8]
  Installing     : openldap-servers-sql                            [8/8]

Installed: compat-openldap.i386 0:2.3.43_2.2.29-3.el5 openldap-clients.i386 0:2.
3.43-3.el5 openldap-devel.i386 0:2.3.43-3.el5 openldap-servers.i386 0:2.3.43-3.e
l5 openldap-servers-overlays.i386 0:2.3.43-3.el5 openldap-servers-sql.i386 0:2.3
.43-3.el5
Dependency Installed: cyrus-sasl-devel.i386 0:2.1.22-4 unixODBC.i386 0:2.2.11-7.
1
Complete!
```

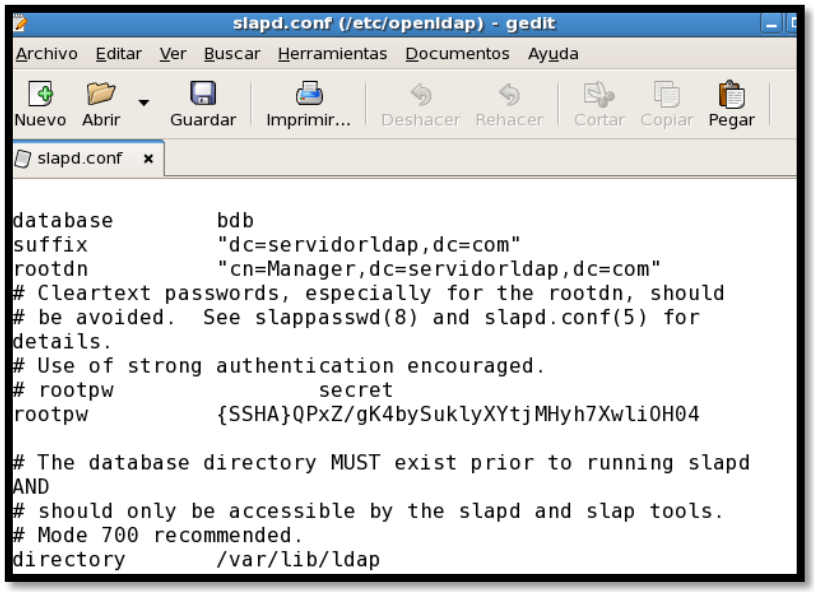
Generar una nueva clave que permita la configuración de los parámetros del servidor LDAP, para esto se usa el comando slappasswd, para luego ingresar la clave y que genera una clave encriptada.

```
[root@localhost ~]# slappasswd
New password:
Re-enter new password:
{SSHA}zhwROoJb0j/nX3KGx82HA5kAZ/CwolNq
[root@localhost ~]#
```

Configurar el archivo slapd.conf, q está localizado en /etc/openldap/slapd.conf

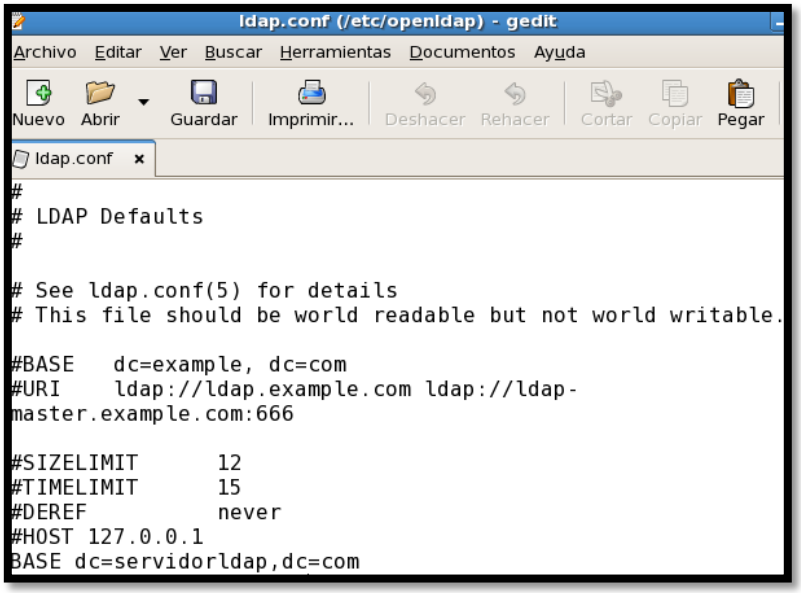
```
[root@localhost ~]# gedit /etc/openldap/slapd.conf
```

Copiar la contraseña generada anteriormente en el campo rootpw y modificar los parámetros de acuerdo a los valores que tendrá el servidor, como es el dominio al que pertenece.



Configurar el archivo ldap.conf que se encuentra en /etc/openldap/ldap.conf

Al final de este archivo añadir la direccion IP del localhost y el dominio al que pertenece el servidor.



Crear un propio archivo de base de datos, para ello es necesario copiar el ejemplo que viene en el paquete de openldap.

```
[root@localhost ~]# cp /etc/openldap/DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

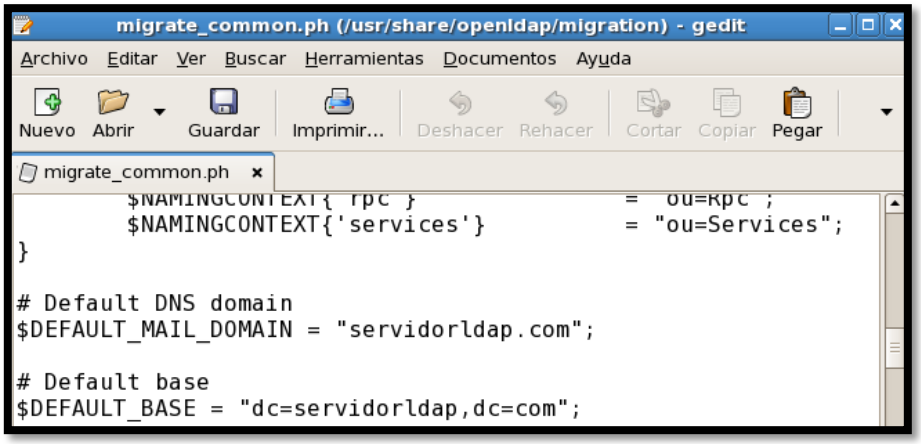
Iniciar el servicio de ldap, para verificar que no existe ningún error en la configuración de alguno de los archivos.

```
[root@localhost ~]# service ldap start
Iniciando slapd:                                           [  OK  ]
```

Migrar los datos de usuario de servidor con la herramienta que proporciona openldap

```
[root@localhost ~]# gedit /usr/share/openldap/migration/migrate_common.ph
```

En este archivo modificar el dominio al que pertenece el servidor ldap, en este caso el dominio que se está configurando es servidorldap.com



Crear un archivo ldif para agregarlo a la base de datos y poder migrar.

```
[root@localhost ~]# /usr/share/openldap/migration/migrate_base.pl > /etc/openlda
p/servidorldap.ldif
```

Después de haber configurado el servidor LDAP, se procede a la creación de usuarios para la realización de las posteriores pruebas.

- **INGRESO**

Creamos un archivo .ldif de un usuario, en el cual agregamos la información

```
[root@localhost ~]# gedit /etc/openldap/usuario.ldif
```

usuario.ldif

```
dn: uid=usuario,ou=People,dc=servidorldap,dc=com
uid: usuario
cn: usuario
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword: {CRYPT}0twQq5O4FSU3I
shadowLastChange: 15624
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 500
gidNumber: 500
homeDirectory: /home/usuario
gecos: usuario
```

El campo userPassword lo obtenemos de la siguiente manera

```
[root@localhost ~]# slappasswd -h {CRYPT} -v
New password:
Re-enter new password:
{CRYPT}0twQq5O4FSU3I
```

Mediante línea de comandos añadir el usuario anterior al sistema:

ldapmodify -axvWD "cn=manager,dc=servidorldap,dc=com" -f /etc/openldap/usuario.ldif

Dónde:

-a: añadir al árbol ldap

-x: autentificación simple (sin SSL, etc.)

-v: verbose

-W: pedir el password del DN con que me autentifique

-f fichero: fichero donde se va a escribir las modificaciones

```
[root@localhost ~]# ldapmodify -axvWD "cn=manager,dc=servidorldap,dc=com" -f /et
c/openldap/usuario.ldif
ldap_initialize( <DEFAULT> )
Enter LDAP Password:
add uid:
        usuario
add cn:
        usuario
add objectClass:
        account
        posixAccount
        top
        shadowAccount
add userPassword:
        {CRYPT}0twQq5O4FSU3I
add shadowLastChange:
        15624
add shadowMin:
        0
add shadowMax:
        99999
add shadowWarning:
        7
add loginShell:
```

```
        /bin/bash
add uidNumber:
        500
add gidNumber:
        500
add homeDirectory:
        /home/usuario
add gecos:
        usuario
adding new entry "uid=usuario,ou=People,dc=servidorldap,dc=com"
modify complete
```

Configuración del Servidor Proxy

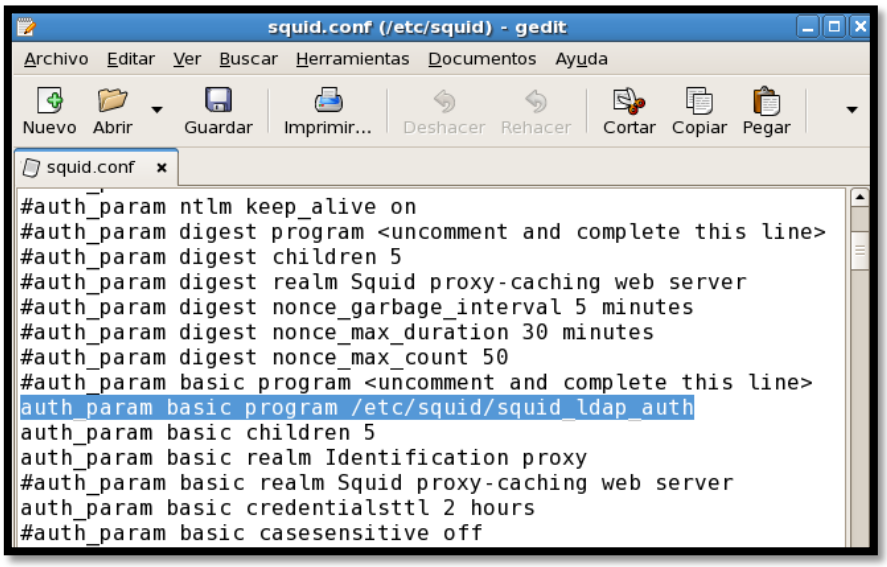
Primero se tiene que instalar el paquete squid, en cualquiera de sus versiones.

Crear el script que permita la autenticación con el servidor ldap, configurado anteriormente.

```
[root@localhost ~]# gedit /etc/squid/squid_ldap_auth
```

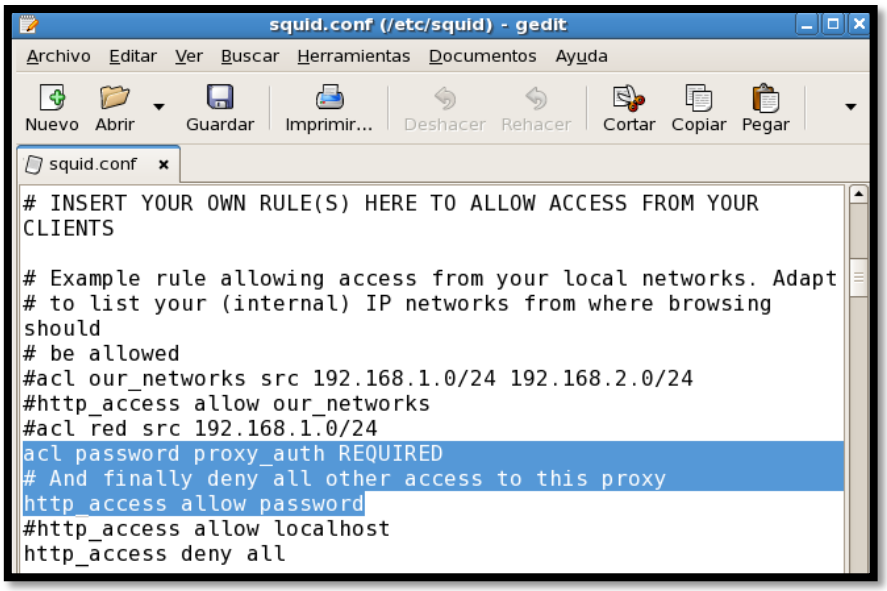
El mismo que contendrá la localización del archivo de autenticación que posee squid para ldap, este archivo se genera al instalar el servidor proxy. Además se debe indicar el dominio al que pertenece el servidor ldap y la dirección IP que se configuro en LDAP.

Configurar el archivo del servidor proxy localizado en /etc/squid/squid.conf, en el cual hay que indicar la dirección donde se encuentra el script de configuración creado en el paso anterior.

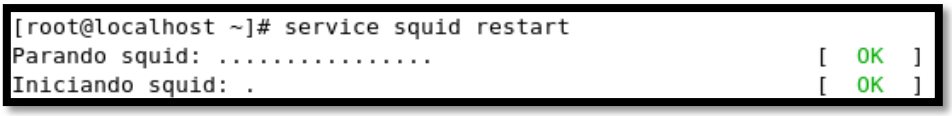


Definir la lista de control de acceso llamad password, en la cual se indica que se requiere autenticación. Para que la configuración se complemente añadir una regla permitiendo que

los host que cumplan con la acl definida puedan autenticarse y finalmente otra regla que niegue el acceso al todo lo demás.



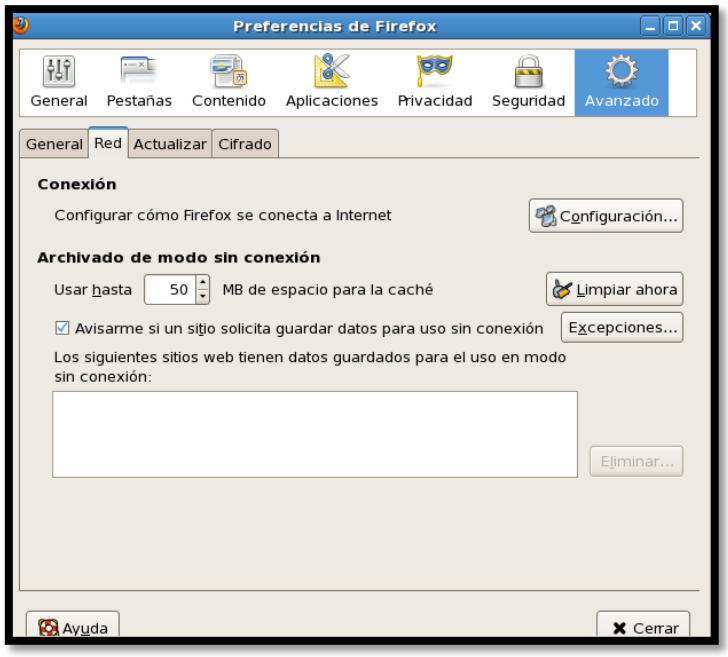
Reiniciar el servicio



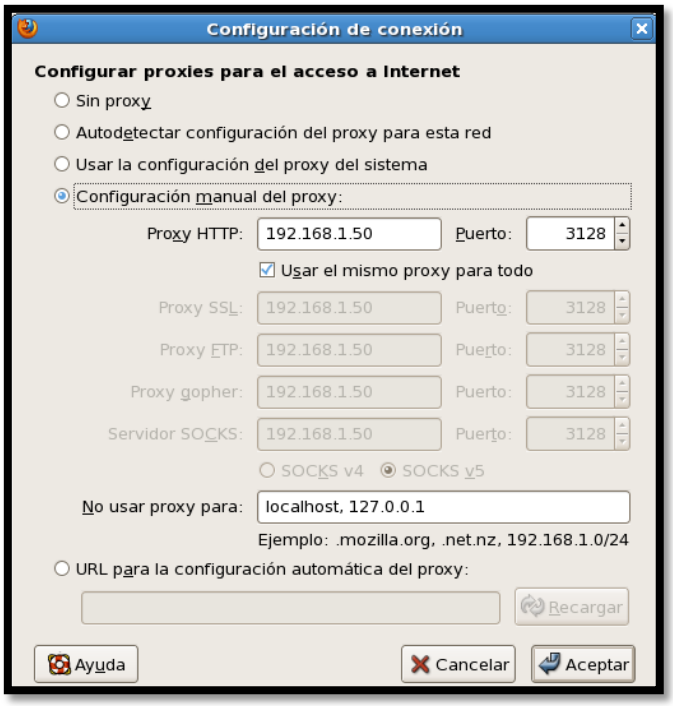
Configuración del navegador web para que salga utilizando el servidor proxy configurado anteriormente.

En este caso, será configurado el navegador web Moxila Firefox, para lo cual hacer clic en la pestaña editar, opción preferencias.

En la ventana que se abre a continuación, hacer clic en la pestaña avanzado, escoger la opción red y por ultimo hacer clic en configuración.



A continuación, seleccionar la opción configuración manual del proxy, ingresando la dirección Ip del servidor proxy que es 192.168.1.50 y el puerto por defecto que utiliza squid para su funcionamiento que es el puerto número 3128.



Luego de realizar los pasos anteriores, la configuración está lista y solo falta efectuar una prueba, para esto solo basta con abrir el navegador web y al colocar cualquier dirección web a la que queramos ingresar, se abrirá una nueva ventana en la cual nos pide ingresar el nombre de usuario y contraseña que se configuro en el servidor LDAP.