

**UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA SEDE DE
CONCEPCIÓN - REY BALDUINO DE BÉLGICA**

**IMPLEMENTACIÓN DE LDAP-SAMBA PARA CONTROL DE ACCESO A
SERVIDOR ESXI**

Trabajo de Titulación para optar al Título de
Técnico Universitario en
TELECOMUNICACIONES Y REDES

Alumno:

Ian David Bustamante Chavez

Profesor Guía:

Ing. Israel Figueroa

Profesional correferente:

Ing. Milton Marín

RESUMEN

Sabiendo que se utiliza mucho el servidor para las asignaturas de la carrera con propósitos de aprendizaje y práctica, se propuso la idea de diseñar un sistema que permita gestionar las cuentas para los alumnos de la. En el marco teórico se dará una introducción a las máquinas virtuales, parte fundamental del proyecto ya que se trabajo mucho en ellas, siendo VMware el hypervisor donde se alojan las máquinas. Se abordará el cómo funcionan y de que manera se implementaran Samba y LDAP. Se explicará las configuraciones y ajustes que llevaran ahondando en algunas características mas importantes. Por ultimo se llevará a cabo una explicación para acoplar las implementaciones con VMware mostrando los resultados obtenidos.

ÍNDICE DE MATERIA

INTRODUCCIÓN	1
CAPITULO 1: PROBLEMÁTICA, CONTEXTO DE LA SITUACIÓN, MARCO TEÓRICO Y SOLUCIÓN PROPUESTA	2
1 PROBLEMÁTICA, CONTEXTO DE LA SITUACIÓN, MARCO TEÓRICO Y SOLUCIÓN PROPUESTA	3
1.1 CONTEXTO DE LA SITUACIÓN	3
1.2 DEFINICIÓN DE PROBLEMAS	3
1.3 OBJETIVOS DEL PROYECTO	4
1.4 INTRODUCCIÓN A LA VIRTUALIZACIÓN	5
1.4.1 VMware vSphere	6
1.4.2 VirtualBox	7
1.5 CONFIGURACIÓN DEL LABORATORIO	7
1.6 SERVIDOR DE DOMINIO	8
1.6.1 Protocolo LDAP	8
1.6.2 Active Directory	10
1.6.3 OpenLDAP	11
1.7 SAMBA	12
CAPITULO 2: CONFIGURACIÓN DE LDAP Y SAMBA	13
2 CONFIGURACIÓN DE OPENLDAP Y SAMBA	15
2.1 SOLUCIÓN PROPUESTA	15
2.2 INSTALACIÓN DE LDAP	16
2.2.1 Instalación del software LDAP	17
2.2.2 Instalación de software de apoyo	17
2.2.3 Configurar LDAP	17
2.2.3.1 Esquema LDAP	18
2.2.3.2 Algunos ajustes extra	19
2.3 INSTALACIÓN DE SAMA	20
2.3.1 Instalación del software Samba	20
2.3.2 Configuración de Samba	21
2.3.2.1 Smb.conf	21
2.3.2.2 Smbldap.conf	23
2.3.2.3 Smbldap_bin.conf	24
2.3.2.4 Últimos ajustes	24

<u>CAPITULO 3: PRUEBA DEL SISTEMA Y PROCEDIMIENTOS</u>	25
3 PRUEBA DEL SISTEMA Y PROCEDIMIENTOS	27
3.1 TAREAS REALIZADAS/TESTEO	27
3.1.1 Cuentas de usuario y grupos	27
3.2 PROCEDIMIENTO	28
3.2.1 Dominio LDAP-Samba en ESXi	28
Conclusión	35
Bibliografía	36
Anexos	37

ÍNDICE DE FIGURAS

Figura 1-1. Esquema de virtualización, hipervisor de tipo 1.	6
Figura 1-2. Esquema de administración de máquinas a través de vSphere.	6
Figura 1-3. Interfaz vSphere Client.	7
Figura 1-4. Esquema de virtualización, hypervisor de tipo 2.	7
Figura 1-5. Esquema jerárquico de LDAP. Estructura tipo árbol.	9
Figura 1-6. Ejemplo de un archivo de configuración.	10
Figura 1-7. Integración de Windows a través de Samba.	12
Figura 2-1. LDAP y SAMBA montados en máquinas virtuales.	15
Figura 2-2. Paquetes redirigidos desde “LDAP” a LDAP.	16
Figura 2-3. Pantalla de creación de contraseña.	17
Figura 2-4. Ejemplo de un archivo esquema o schema.	19
Figura 2-5. Los datos que van a 10.4.11.12 son redirigidos a 172.22.1.53.	22
Figura 3-1. Ventana de logueo VMware vSphere Client.	28
Figura 3-2. Menú de administración.	29
Figura 3-3. Menú de configuración.	29
Figura 3-4. Menú de configuración. Zoom izquierdo.	30
Figura 3-5. Ventana de configuración. Servicio de directorio.	30
Figura 3-6. Ventana de configuración. Unir dominio	31
Figura 3-7. Permisos de ESXi.	31
Figura 3-8. Ventana de asignación de permisos.	32
Figura 3-9. Ventana de selección de usuarios y grupos para asignar rol.	33
Figura 3-10. Ventana de asignación de permisos. Cambiando rol.	34

SIGLAS Y SIMBOLOGÍA

Siglas

IP	: Protocol Internet
S.O	: Sistema Operativo
Máquina virtual	: Hace referencia un sistema operativo alojado dentro de otro sistema operativo
AD	: Active Directory

Simbología

MB	: Megabytes
GB	: Gigabytes
TB	: Terabytes
GHz	: Gigahertz

INTRODUCCION

La idea surgió de la problemática en la gestión de cuentas ESXi para el servidor del laboratorio 209, el cual, cada vez que se requería registrar a una persona nueva, se le tenían que dar permisos específicos, si el usuario es estudiante, profesor u otros, y suministrarle un usuario y contraseña. VMware ESXi soporta que la autenticación se haga a través de un servidor de directorio, el cual almacena las cuentas de usuario y los privilegios de este.

El objetivo del proyecto será crear un control de acceso centralizado, con LDAP como servidor de directorio para autenticar las cuentas, de tal forma que con solo un usuario y contraseña registrado en la base de datos de LDAP, será posible ingresar al servidor del laboratorio.

Como funcionalidad adicional se intentará utilizar el control de acceso para autenticarse tanto en Windows como en Linux, tratando de abarcar todo el laboratorio.

CAPITULO 1: INTRODUCCIÓN A LA VIRTUALIZACIÓN Y SERVIDORES
DE DOMINIO

1 PROBLEMÁTICA, CONTEXTO DE LA SITUACIÓN, MARCO TEÓRICO Y SOLUCIÓN PROPUESTA

1.1 CONTEXTO DE LA SITUACIÓN

En la carrera de Técnico Universitario en Telecomunicación y Redes se trabaja mucho en entornos de red, por lo que se es necesario trabajar en un laboratorio con varios equipos para desarrollar un conocimiento y practica óptimos, para ello se dispuso del laboratorio 209 el cual equipado para realizar las diferentes actividades que demanda la carrera, ya que cuenta con computadores de altas prestaciones y servidores básicos con los que hacer pruebas de todo tipo, pero al pasar el tiempo apareció un problema, habían más alumnos cada año y ya no se podían hacer configuraciones o instalar sistemas operativos en los equipos ya que podrían afectar el avance o las configuraciones hechas por estudiantes de distintas asignaturas y semestre, es por esto que se decidió hacer uso de la virtualización, sistemas montados en máquinas virtuales, esto era posible gracias a software que permitían virtualizar de forma alojada. Pero también se vio poco eficiente y podría existir la posibilidad de que borrasen por error máquinas virtuales hechas en estos softwares, por lo que se compró un servidor exclusivo para la virtualización. Gracias a esto los alumnos pueden montar sus máquinas virtuales para instalar sistemas operativos, simular entornos de equipos físicos, instalar servicios como dhcp o dns, hacer pruebas de software de monitorización, en una red aislada o compartida sin temor a que sean borradas.

Este servidor tiene instalado un hypervisor que administra las máquinas virtuales, y un software cliente que nos permite visualizarlas. Para acceder a ellas se necesitan de credenciales, que son suministradas por el administrador de red del laboratorio.

1.2 DEFINICIÓN DE PROBLEMAS

Para hacer uso del servidor del laboratorio que tiene instalado el hypervisor ESXi, se tiene que acceder a través de un software de visualización o por interfaz web, que requiere de credenciales para poder ingresar. Aquí es donde surgen la problemática y la razón del proyecto.

- ¿Qué sucedería en el caso donde se quiere que un alumno nuevo de la carrera pueda hacer uso del servidor?

Solo se tendrían que crear credenciales para él. El problema surge al tener que configurar los permisos para cada nuevo usuario, ya sea un alumno o un profesor, y que

sumado a eso también tienen distintos grados de acceso. Configurar todo eso para cada usuario nuevo, es bastante tedioso y consume tiempo.

Otro problema que hay, aunque en menor medida es que, el usuario tendría que recordar sus credenciales del servidor aparte de las que ya tiene para las distintas plataformas que existen, siendo un poco molesto memorizar cada una de ellas.

1.3 **OBJETIVOS DEL PROYECTO**

- Objetivo General: Implementar un sistema de cuentas para el servidor de virtualización del laboratorio.
- Objetivos específicos:
 - Investigación sobre el método usado por el hypervisor para configurar cuentas de usuario.
 - Proponer una configuración que permita usar cuentas de usuario para el hypervisor, así como también otras necesidades del laboratorio.
 - Configurar un servidor de cuentas en el hypervisor disponible en el laboratorio.
 - Diseñar procedimiento para crear cuentas de usuario en el servidor de virtualización.

Como objetivo principal se tiene la implementación de un controlador de dominio para el servidor del laboratorio, creando un sistema de cuentas de usuarios más centralizado y no tener que hacerlas de forma local. Se desea que un estudiante o profesor, pueda ingresar al servidor con sus credenciales ya creadas y almacenadas en el controlador de dominio y que estas a su vez puedan servir para otros sistemas o plataformas. Para llevar a cabo esto, se usará el protocolo LDAP o más concretamente OpenLDAP. Samba se utiliza para emular un dominio Active Directory, conectandose a LDAP para acceder a las credenciales de los usuarios.

Si bien el hypervisor del servidor permite crear cuentas de usuarios y almacenarlas de forma local como cualquier sistema operativo, no permite la creación de grupos para asignar los permisos, por lo que todos los usuarios deben ser configurados de manera manual. Al verse en la necesidad de solucionar este problema, el hypervisor da la opción de conectar un host a un dominio para administrar usuarios, tal como un active directory proporcionado por Windows, pero en este caso se trabajará con OpenLDAP y Samba.

Samba será utilizado también para hacer las “traducciones” entre equipos Windows y Linux/UNIX. Si bien este proyecto estará enfocado en implementar un servidor de directorio para ESXi, el implementar LDAP servirá como base para futuras mejoras, tales como servicios de autenticación de WIFI o cuentas de sistema para servidores y PC de laboratorio.

Cabe mencionar que los servidores de LDAP y Samba estarán montados en máquinas virtuales diferentes, esto se decidió para que quedara una instalación limpia.

1.4 INTRODUCCIÓN A LA VIRTUALIZACIÓN

La virtualización hace uso del software para imitar las características del hardware, creando sistemas virtuales dentro de un equipo físico, pudiendo alojar varios sistemas virtuales a la vez, y de esta manera aprovechar mejor el potencial del hardware. Esto se hace a través de un hypervisor, una capa ligera de software que desvincula las máquinas virtuales del host y gestiona los recursos del hardware como lo son cpu, memoria, almacenamiento y conexiones de red, y los administra de forma dinámica según las necesidades de cada máquina.

Los aspectos que hacen interesante trabajar con máquinas virtuales y el por qué se decidió trabajar en éstas son:

- Creación de particiones: Se pueden instalar y ejecutar más de un sistema operativo en una sola maquina física. También se pueden administrar los recursos entre las máquinas virtuales.
- Aislamiento: Aísla la seguridad y los fallos a nivel de hardware.
- Encapsulación: Guardar el estado de una máquina, pudiendo respaldar o retroceder en caso de fallas, de forma sencilla y rápida. Otro aspecto que tiene es la versatilidad ya que se puede transferir, copiar, clonar y mover máquinas virtuales fácilmente.
- Independencia del hardware: Las máquinas pueden ser migradas de un equipo físico a otro.

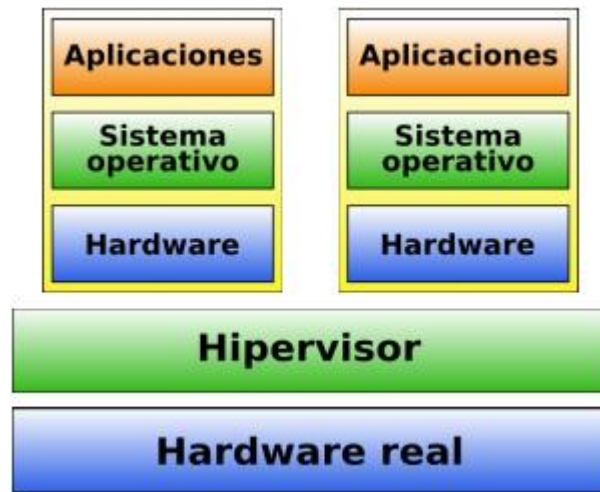


Figura 1-1. Esquema de virtualización, hipervisor de tipo 1

Alguno de los softwares que permiten virtualizar son Virtual Box, VMware vSphere, Microsoft Hyper-V Server, Proxmox, entre otros. En este caso se detallarán dos de ellos que fueron con los que se trabajó en el proyecto.

1.4.1 VMware vSphere

Partiendo por VMware Vsphere, este es un hipervisor de tipo 1, esto quiere decir que se instala directamente sobre el equipo, también llamado virtualización de forma nativa, haciendo la función tanto de sistema operativo como de virtualizador. Cabe mencionar que VMware vSphere es un conjunto de paquetes, donde cada uno cumple una función esencial en la virtualización, estos se componen de ESXi, vSphere Client y vCenter Server.

- VMware ESXi: Es el hipervisor instalado en el equipo, el sistema operativo que se encarga de la virtualización. Todas las máquinas virtuales o sistemas operativos invitados se instalan en el servidor ESXi.
- vSphere Client: El cliente vSphere es el que permite acceder al servidor, instalar y administrar las máquinas virtuales. Esto se hace desde cualquier equipo a través del software o desde el navegador.

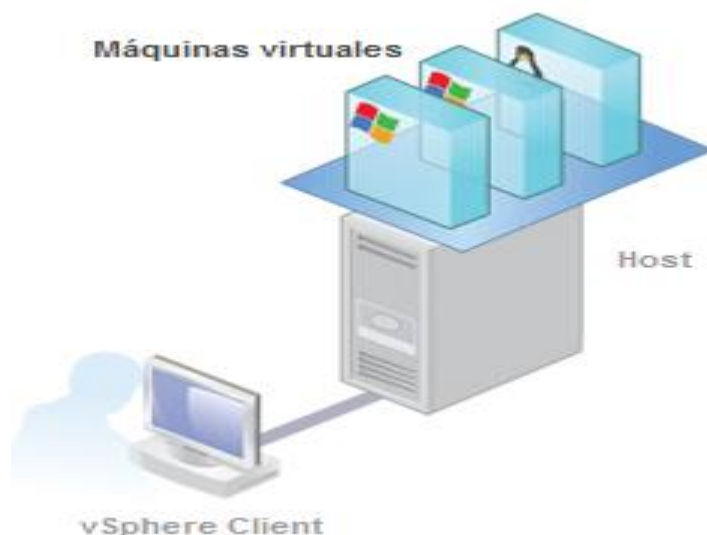


Figura 1-2. Esquema de administración de máquinas a través de vSphere

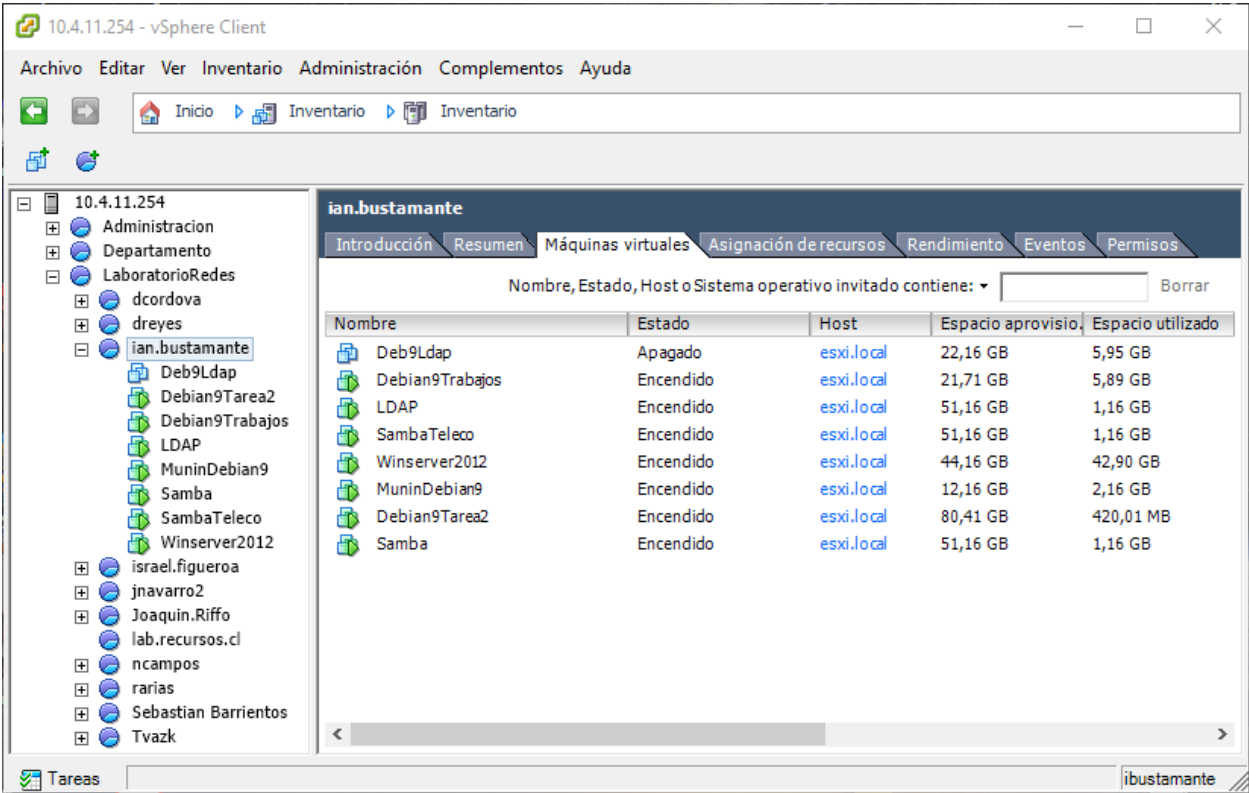


Figura 1-3. Interfaz vSphere Client

- vCenter Server: Este software sirve para administrar múltiples servidores vSphere ESXi de forma centralizada.

1.4.2 VirtualBox

El software VirtualBox a diferencia de VMware, es un hypervisor de tipo 2, lo que quiere decir que requiere de un sistema operativo anfitrión para ser instalado, teniendo como principal desventaja la eficiencia al momento de montar una máquina virtual, ya que la virtualización se hace a través de un software ya alojado en un anfitrión. Por lo general VirtualBox es utilizado para virtualizar máquinas más pequeñas, pensado para uso más domestico que empresarial.



Figura 1-4. Esquema de virtualización, hypervisor de tipo 2

1.5 **CONFIGURACIÓN DEL LABORATORIO**

El laboratorio cuenta con un servidor PowerEdge, que tiene instalado VMware ESXi, en este se virtualizaran las máquinas que alojaran Samba y el servidor de dominio las cuales son fundamentales en el proyecto. El equipo cuenta con las siguientes características:

- Fabricante: Dell Inc.
- Modelo: PowerEdge R540
- Núcleos de CPU: 28 CPU x 1,995 GHz
- Tipo de procesador: Intel® Xeon® Gold 5117 CPU @ 2.00GHz
- Memoria: 128 GB
- Almacenamiento: 3 TB
- Tarjetas de red: 2

Como detalle a recalcar, el servidor está configurado en RAID1+0 de manera que, en caso de alguna falla, quedara un respaldo de los datos. Como medida de seguridad, está provisto de una unidad de energía suplementaria en caso de algún corte de energía eléctrica, dándole soporte por 1 hora aproximadamente.

1.6 **CONTROLADOR DE DOMINIO**

Un servidor de dominio o un controlador de dominio es un término creado por Microsoft Windows para referirse a sistema centralizado de cuentas en donde los clientes cada vez que se intentan conectar a un servicio asociado al dominio, este le hace las consultas a una base de datos que contiene las credenciales de usuario y verifica su validación. Luego apareció una implementación que utilizaba el protocolo LDAP para hacer las consultas de credenciales, a la cual se le denominó como Active Directory. Como no se trabajará con Active Directory se tuvo que buscar una alternativa, LDAP+Samba que permite emular las características de un servidor de dominio Active Directory. Mientras que Samba será el controlador de dominio, como servidor de directorio tendremos a OpenLDAP que es la implementación libre del protocolo LDAP pero en sistemas Linux.

Como Active Directory y OpenLDAP son implementaciones basadas en el protocolo LDAP, se ahondará un poco en ambos para conocer sus ventajas, características principales, y diferencias entre estas dos.

1.6.1 Protocolo LDAP

¿Qué es LDAP? LDAP son las siglas de Lightweight Directory Access Protocol (en español Protocolo Ligero de Acceso a Directorios), un protocolo que accede a un servicio de directorio donde buscara la información o realizara consultas. Se podría considerar a LDAP como una base de datos pero que solo contiene cuentas de usuario, grupos u organizaciones. La manera en que organiza la información es de forma jerárquica, basada en el uso de directorios. Estos directorios pueden almacenar una variedad de información y se pueden incluso usar de forma similar al Servicio de Información de Red (NIS), permitiendo que cualquiera pueda acceder a su cuenta desde cualquier máquina de la red.

Los directorios de la base de datos tienen sistema de árbol, que se compone por un conjunto de entradas, las entradas a su vez se componen por conjunto de atributos, y estos por uno o mas valores. Las entradas tienen un nombre distinguido o DN (Distinguished Name) que vendría siendo su verificador único o nombre global, estas se componen de un nombre común o CN (Common Name) y de una componente de dominio o DC (Domain Componet). Un ejemplo de esto seria de la siguiente forma:

```
dc: cn=Ian Bustamante,dc=esxi,dc=cl
```

Para entender mejor esta estructura, ver figura 1-5 en la que se muestra la jerarquía de tipo árbol que tiene LDAP.

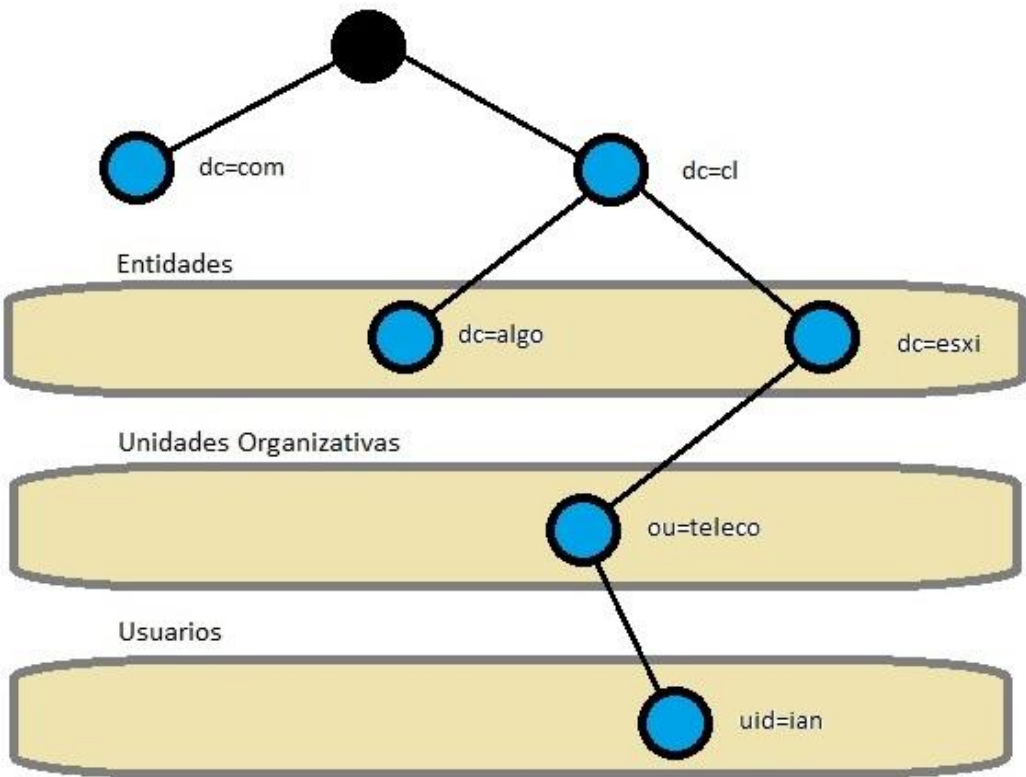


Figura 1-5. Esquema jerárquico de LDAP. Estructura tipo árbol

En una entrada el DN no es considerado un atributo, siendo los atributos datos de un usuario, y no necesariamente credenciales como usuario y contraseña. Estos atributos pueden ser *apellido*, *edad*, *grupo*, *AñoDeIngreso*, etc, y son determinados por esquemas de configuración. Por lo general las entradas se almacenan en archivos .ldif que es el formato con el que trabaja LDAP, y se estructuran de la siguiente manera:

```
dn: cn=Ian Bustamante,dc=esxi,dc=cl
cn: Ian Bustamante
givenName: Ian
sn: Bustamante
edad: 23
grupo: 3
AñoDeIngreso: 2017
Semestre: 5
mail: ian.bustamante@sansano.usm.cl
password: {MD5}3862dcc3e391855fd49302cb275140fb
objectClass: inetOrgPerson
objectClass: datos
objectClass: alumnos
objectClass: top
```

Figura 1-6. Ejemplo de un archivo de configuración

La línea que dice *objectClass* determina el tipo de objeto que es, y se refiere al conjunto de atributos que se le dará a la entrada, pudiendo tener más de un *objectClass* por entrada. Se puede tomar como ejemplo el *objectClass: alumnos* que asignó los atributos *grupo*, *AñoDeIngreso* y *Semestre*, mientras que *objectClass: datos*, asignó los atributos *edad* y *password*. No todos los atributos son obligatorios, esto quiere decir que hay campos opcionales los cuales si se quiere pueden no ser completados. Que un atributo sea obligatorio u opcional depende netamente del *objectClass*.

1.6.2 Active Directory/ Implementación de Windows

A la implementación de Windows basada en un servicio de directorio en un entorno de red de computadoras la nombraron Active Directory. No solo trabaja con el protocolo LDAP, sino que también con DHCP, DNS y Kerberos. Como está basado en el protocolo LDAP, este tiene todas características que se mencionaron antes, como la organización jerárquica. Active directory cumple la función de almacenamiento de cuentas y credenciales, permite el inicio de sesión de los usuarios de forma remota en

cualquier equipo que este dentro del dominio, organiza y administra a los usuarios en grupos y define permisos en función de la jerarquía.

Ventajas de Active Directory sobre OpenLDAP:

- Algo que destaca sobre OpenLDAP es que su configuración es más amigable y fácil de usar.
- Al ser una implementación de Microsoft, este se comporta mejor en un ambiente Windows.
- Es más fácil acoplar equipos con AD

1.6.3 OpenLDAP

Esta es una implementación libre, de código abierto, del protocolo LDAP, para sistemas Linux, BSD, AIX, HP-UX, Mac OS X, Solaris, Microsoft Windows (NT y derivados, incluyendo 2000, XP, Vista), y z/OS.

Características y ventajas de OpenLDAP sobre Active Directory:

- Una característica de esta implementación es la gran cantidad de plataformas soportadas, suponiendo una gran ventaja frente a AD.
- Utiliza menos recursos
- Es mas flexible a la hora de configurar, pudiendo cambiar, agregar o quitar características que en AD están más limitadas.
- Es un software libre (es totalmente gratuito)

1.7 SAMBA

Samba es una implementación libre del protocolo de archivos compartidos de Microsoft Windows (antiguamente llamado SMB, renombrado recientemente a CIFS) para sistemas de tipo UNIX. De esta forma, es posible que computadoras con GNU/Linux, Mac OS X o Unix en general se vean como servidores o actúen como clientes en redes de Windows. Samba también permite validar usuarios haciendo de Controlador Principal de Dominio (PDC), como miembro de dominio e incluso como un dominio Active Directory para redes basadas en Windows; aparte de ser capaz de servir colas de impresión, directorios compartidos y autenticar con su propio archivo de usuarios.

Para el propósito de este proyecto, Samba solo servirá de controlador de dominio para que los equipos con sistemas operativos Windows puedan acoplarse al dominio, es por esto que sus funciones de servidor de archivos compartidos no serán utilizadas. Para equipos Linux no es necesario pasar por Samba, sino que la comunicación se hace directamente con LDAP

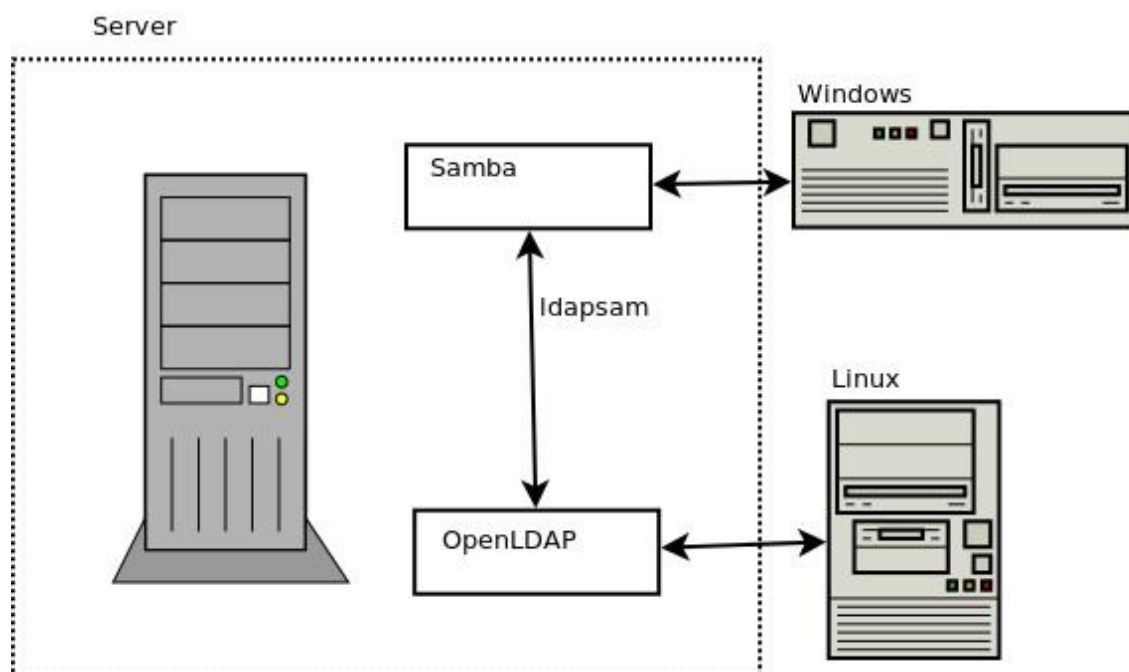


Figura 1-7. Integración de Windows a través de Samba

CAPITULO 2: INSTALACIÓN DE LDAP Y SAMBA

2 ASPECTOS GENERALES DE OPENLDAP Y SAMBA

2.1 SOLUCIÓN PROPUESTA

La solución propuesta se basa en una implementación de OpenLDAP y SAMBA, ambas instaladas en máquinas virtuales separadas, esto para hacer una instalación más limpia y a su vez más segura en caso de fallas. La máquina con OpenLDAP estará en una vlan distinta a la de SAMBA, una en Teleco-Servers mientras que la otra en USM-Redes.

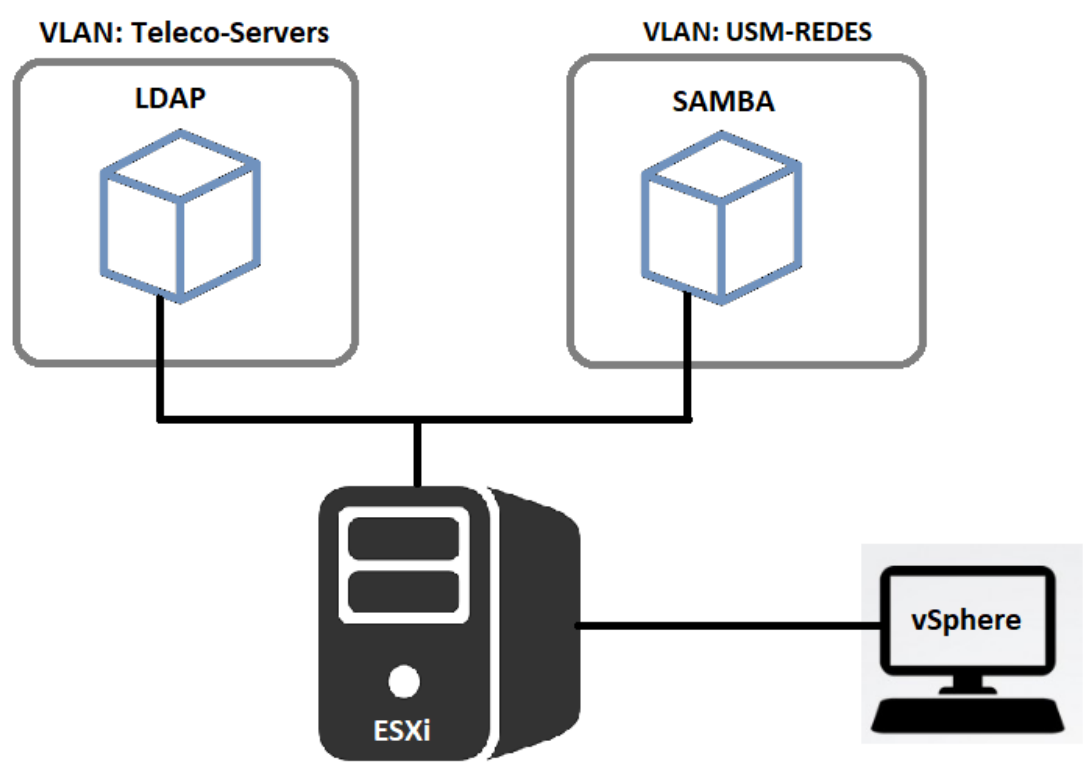


Figura 2-1. LDAP y SAMBA montados en máquinas virtuales.

Las cuentas de usuario se crearán en SAMBA, de manera que configurando unos parámetros se puede hacer que las cuentas y las consultas que se le hagan sean enviadas al servidor de LDAP. Ya que SAMBA tiene problemas para conectarse directamente con el servidor de LDAP, se tuvo que idear una forma de hacerlo, la cual consiste en fijar una IP de la misma red como falso LDAP, luego cambiando unas reglas de firewall, se redirigen todos los paquetes que vayan a la IP del supuesto LDAP a la verdadera IP de LDAP.

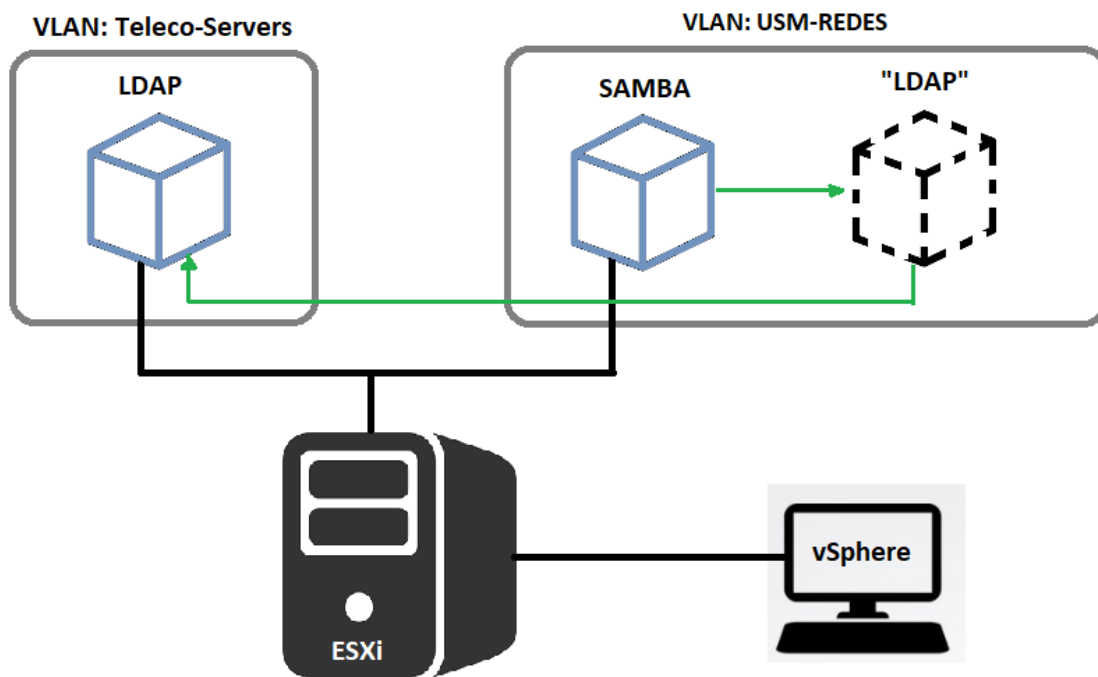


Figura 2-2. Paquetes redirigidos desde “LDAP” a LDAP.

2.2 INSTALACIÓN Y CONFIGURACIÓN DE LDAP

Antes de empezar con la instalación y configuración de OpenLDAP, hay que tener en cuenta algunos aspectos relevantes, como lo son las especificaciones que tendrá la máquina virtual o mas bien los recursos que se le asignaran y la configuración de la tarjeta de red. Para efectos de configuración, se hizo todo como usuario root.

- Especificaciones de la máquina virtual
 - S.O Debian 9
 - 50 GB de disco duro
 - 1 GB de memoria RAM
 - 1 procesador con 2 núcleos
- Configuración de la tarjeta de red

Para configurar la IP de la máquina, será necesario ingresar a un archivo llamado *interfaces* que se encuentra en */etc/network/* y editarlo. La configuración quedaría de la siguiente manera:

```
auto ens192
iface ens192 inet static
```

```
address 172.22.1.53
netmask 255.255.255.0
network 172.22.1.0
gateway 172.22.1.1
broadcast 172.22.1.255
```

Una vez hecho estos, ya se puede empezar la instalación de OpenLDAP y configurarlo.

2.2.1 Instalación de software OpenLDAP

Para instalar el software se usa el comando *apt-get install slapd*, luego aparecerá una pantalla de configuración que pedirá crear una contraseña para el administrador de LDAP. La contraseña creada es “Teleco2018!”.

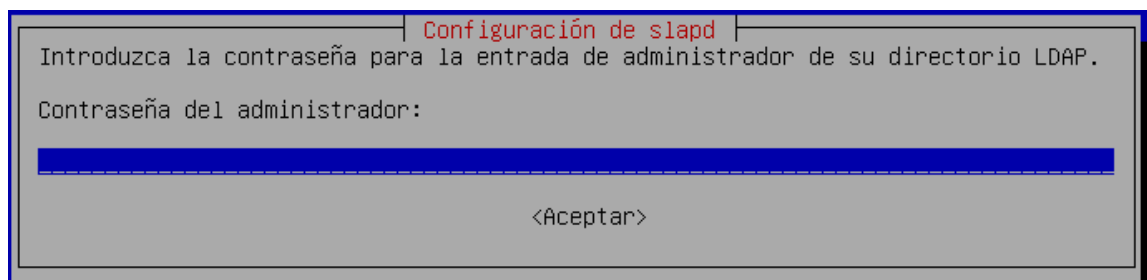


Figura 2-3. Pantalla de creación de contraseña

2.2.2 Instalación de software de apoyo

Como complemento se instala *ldap-utils* que son un conjunto de utilidades que nos servirán al momento de configurar *ldap*. Algunas de ellas permitirán buscar y mostrar entradas, agregarlas o eliminarlas. El comando que se debe ejecutar es *apt-get install ldap-utils*.

2.2.3 Configuración de LDAP

El servidor de LDAP, tal cual instalado y con su configuración por defecto no es suficiente y carece de algunas opciones. Es por ello por lo que se deben cambiar sus parámetros y adecuarlos al propósito del proyecto, haciéndolo de la siguiente manera. Para empezar, se moverán los archivos de configuración que están en el directorio */etc/ldap/slap.d*. En este caso se movió al directorio */root/* ya que allí no interferirá con la configuración de LDAP. Esto se hace para que la configuración de LDAP sea más fácil,

ya que solo es necesario crear un archivo de configuración en remplazo de los que se movieron.

El archivo creado será puesto en */etc/ldap/slapd.conf* y llevará ciertos parámetros que servirán para que funcione el servidor. La configuración estará anexa, acá solo se detallarán los parámetros más relevantes. [ver ANEXO 1]

- Suffix

“La línea *suffix* asigna el dominio para el que el servidor LDAP proporcionará información.” Por lo que el parametro *suffix* define el nombre del dominio que tendrá el servidor. El *dc* (domain component) o componente de dominio que se escogió para este proyecto es *esxi*.

Suffix “*dc=esxi*”

- Rootdn

“La entrada *rootdn* es el Nombre distinguido (DN) para un usuario que no está restringido por el control de acceso o los parámetros de límites administrativos fijados para operaciones en el directorio LDAP”. En este campo se debe completar con la información del dominio, el cual sería “*esxi*”, quedando de la siguiente manera.

Rootdn “*cn=admin,dc=esxi*”

2.2.3.1 Esquemas de LDAP

Los esquemas de LDAP son archivos de configuración que contiene un conjunto de *objectclass*, y este último a su vez es el que define los atributos que llevara la entrada, siendo este un archivo importante que la distribución de OpenLDAP ya trae consigo, pero que se pueden incluir más si se requiere. Los atributos que tiene cada *objectclass* no necesariamente son los que se quisieran, por lo que también es posible crear un archivo “.schema” con los *objectclass* y atributos personalizados.

Para los propósitos del proyecto se va a requerir copiar un esquema que viene de ejemplo en la distribución de samba, este esquema es necesario para crear las cuentas en samba y serán las credenciales que permitirán el acceso al servidor ESXi como también a las distintas plataformas. El único inconveniente de tratar de copiar el esquema es que la implementación de samba está instalada en otra máquina. por lo que se tuvo que buscar

alternativas para encontrar el contenido del archivo. Lo que se hizo fue buscar en algún foro el contenido del esquema, una vez encontrado, se creó un archivo llamado `samba.schema`, se copió el contenido, y por último se movió el archivo al directorio `/etc/ldap/schema/`.

Un ejemplo de un archivo schema seria de la siguiente forma:

```

attributetypes ( 2.25.128424792425578037463837247958458780603.1
    NAME 'MatriculaUSM'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )
attributetypes ( 2.25.128424792425578037463837247958458780603.2
    NAME 'Apellido'
    EQUALITY caseIgnoreMatch
    SUBSTR caseIgnoreSubstringsMatch
    SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 )

objectclass ( 2.25.128424792425578037463837247958458780603.14
    NAME 'alumno'
    DESC 'Datos de identificacion'
    AUXILIARY
    MAY (MatriculaUSM $ Apellido))

```

Figura 2-4. Ejemplo de un archivo esquema o schema

2.2.3.2 Algunos ajustes extras

Para finalizar con la instalación y configuración de OpenLDAP, debemos apagar el servicio `slapd` para poder otorgarle permisos especiales y luego restablecemos el servicio. Los pasos por seguir serían los siguientes:

- Para apagar el servicio utilizamos el comando
`systemctl stop slapd.service`
- Aplicamos el comando
`chown -R openldap:openldap /var/lib/ldap`
- Luego para iniciar de nuevo el servicio aplicamos

```
systemctl start slapd.service.
```

Con esto ya tenemos lista la maquina con OpenLDAP, de este punto en adelante es poco lo que se va a intervenir acá, por lo que se proseguirá a la instalación y configuración de Samba.

2.3 INSTALACIÓN DE SAMBA

Para este punto tendremos en cuenta los mismos aspectos que en la sección 2.2, que son las especificaciones de la máquina y la configuración de red. Cabe aclarar también que todas las configuraciones se harán como usuario root.

- Especificaciones de la maquina
 - S.O Debian 9
 - 50 GB de disco duro
 - 1 GB de memoria RAM
 - 1 procesador con 2 núcleos
- Configuración de la tarjeta de red

La máquina estará en la vlan USM-Redes y al igual que con la maquina con LDAP, deberemos editar el archivo de configuración de red:

```
nano /etc/network/interfaces
```

```
auto ens192
iface ens192 inet static
address 10.4.11.250
netmask 255.255.255.0
network 10.4.11.0
gateway 10.4.11.1
broadcast 10.4.11.255
```

2.3.1 Instalación del software Samba

Para instalar samba y poder autenticar contra LDAP, instalamos los paquetes *samba* y *smblldap-tool*. El comando que vamos a utilizar será el siguiente:

```
Apt-get install samba smblldap-tools
```

Con esto ya tendremos instalado samba, ahora es necesario configurarlo para que pueda almacenar las cuentas en LDAP y para que la autenticación se haga a través de esta.

2.3.2 Configuración de SAMBA

La configuración de Samba es un poco más extensa que la de LDAP ya que es desde acá donde se realizará la creación de las cuentas. Para empezar, paramos el servicio con *service smbd stop*. Lo que se necesita para configurar Samba con LDAP son tres archivos, *smb.conf*, *smblldap_bind.conf* y *smblldap.conf*. El único archivo que ya viene por defecto al realizar la instalación es *smb.conf*, mientras que los demás tienen que ser obtenidos desde otro directorio, por lo que debemos hacer lo siguiente:

```
cp      /usr/share/doc/smbldap-tools/examples/smbldap_bind.conf
/etc/smbldap-tools/smbldap_bind.conf

zcat    /usr/share/doc/smbldap-tools/examples/smbldap.conf.gz    >
/etc/smbldap-tools/smbldap.conf
```

Una vez obtenido todos los archivos, se empezará por *smb.conf*. que es el que tiene que ver con la configuración de Samba.

2.3.2.1 Smb.conf

La configuración de samba es un poco más extensa ya que es desde acá donde se realizará la creación de las cuentas. Para empezar, se busca el archivo *smb.conf* que es el que tiene que ver con la configuración de samba, por lo que ejecutamos el siguiente comando:

```
nano /etc/samba/smb.conf
```

Una vez dentro deberemos editar el contenido, y al igual que con LDAP, se dejará anexado el archivo de configuración y se detallaran los aspectos más importantes. [Ver anexo 2]

- Passdb backend

El passdb backend es el parámetro que permitirá que las cuentas de usuarios que se agreguen a SAMBA se almacenen en LDAP.

```
passdb backend = ldapsam:ldap://10.4.11.12/
```

El backend que se puso no es la del servidor LDAP, sino que se usó otra que estuviera en la misma VLAN que Samba, luego se cambiaron las reglas de firewall para que se redirigirán todos los paquetes que fueran enviados a 10.4.11.12 y sean enviados a la 172.22.1.53, solucionando el problema que existía con SAMBA al colocar como backend la IP de LDAP.

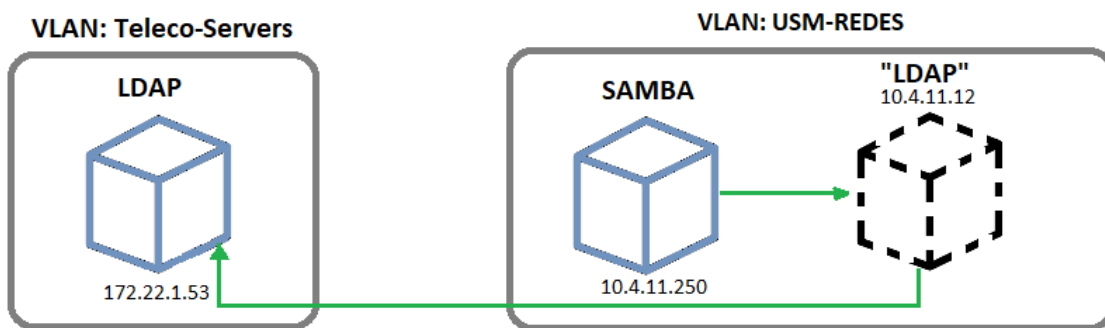


Figura 2-5. Los datos que van a 10.4.11.12 son redirigidos a 172.22.1.53

- *Ldap admin dn y Ldap suffix*

En una sección del archivo, está la configuración para LDAP en Samba. Lo que hay que tener en cuenta aquí es de colocar la componente de dominio del servidor de LDAP.

```
ldap admin dn = cn=admin,dc=esxi
ldap delete dn = Yes
ldap group suffix = ou=group
ldap idmap suffix = ou=idmap
ldap machine suffix = ou=computer
ldap suffix = dc=esxi
ldap ssl = no
ldap user suffix = ou=people
```

Luego de haber hecho las modificaciones, configuramos la contraseña de LDAP en Samba. Usamos el siguiente comando:

```
smbpasswd -w {password}
```

Entre las llaves va escrita la contraseña. En este caso usamos la siguiente: *smbpasswd -w {Teleco2019!}*.

2.3.2.2 Smbldap.conf

Proseguimos con el archivo smbldap.conf, el cual permite establecer parámetros globales que todos puedan leer, ejecutamos el siguiente comando para editarlo:

```
nano /etc/smbldap-tools/smbldap.conf
```

Los aspectos importantes que se describirán son parámetros que servirán para conectar con la maquina con LDAP.

- SID

Este valor lo obtendremos con el comando *net getlocalsid* el cual debera coincidir con el del archivo

```
SID="S-1-5-21-3384730673-3036888877-1999087345"
```

- SambaDomain

El dominio de samba será “esxi”.

```
sambaDomain="esxi"
```

- MasterLDAP y slaveLDAP

En masterLDAP y slaveLDAP se deberán colocar las IP del servidor de LDAP (en este caso la 10.4.11.12 ya que son redirigidos al verdadero servidor).

```
slaveLDAP="10,4,11,12"
```

```
slavePort="389"
```

```
masterLDAP="10.4.11.12"
```

```
masterPort="389"
```

- Suffix

El suffix debe ser *dc=esxi*

```
suffix="dc=esxi"
```

Esos son los pequeños cambios que hay que realizar respecto del archivo original. Una vez terminado, se guardan los cambios y se aplican los permisos necesarios de la siguiente manera:

```
chmod 0644 /etc/smbldap-tools/smbldap.conf
```

2.3.2.3 Smbldap_bind.conf

Este es un archivo que sirve para vincular dos cuentas para un servidor maestro y uno esclavo, pero ya que solo hay un solo servidor de LDAP, se usan los mismos datos para esclavo y maestro. Este archivo solo puede ser leído por el usuario root.

```
slaveDN="cn=admin,dc=esxi"
slavePw="Contraseña"
masterDN="cn=admin,dc=esxi"
masterPw="Contraseña"
```

Guardamos y aplicamos los permisos necesarios:

```
chmod 0600 /etc/smbldap-tools/smbldap_bind.conf
```

Ya teniendo bien configurado los tres archivos, se restablecen los servicios con el comando *service smbd start*.

2.3.2.4 Ultimos ajustes

Y para finalizar solo falta ejecutar el comando *samba-populate*, que sirve para poblar la base de datos de LDAP con las estructuras necesarias para Samba. Con esto ya esta terminada la parte de instalación y configuración.

CAPÍTULO 3: PRUEBA DEL SISTEMA Y PROCEDIMIENTOS

3 **PRUEBA DEL SISTEMA Y PROCEDIMIENTOS**

Este capítulo tendrá como enfoque la implementación del proyecto, pero estará dividido en dos secciones importantes, las tareas realizadas/testeadas y las por realizar. Esto se hizo por motivos de no haber alcanzado a realizar todas las pruebas necesarias de la implementación por la poca coordinación para ejecutar las pruebas en el servidor debido a que se tienen que realizar reinicios de la máquina, perjudicando el uso de este en clases y asignaturas.

3.1 **TAREAS REALIZADAS/TESTEO**

El procedimiento para crear usuarios y grupos se explicara a continuación.

3.1.1 **Cuentas de usuario y grupos**

Para la creación de cuentas de usuarios, se hará uso de Samba, ya que este añade los atributos automáticamente, y todas las cuentas serán almacenadas en LDAP. Mientras que los grupos serán creados con JXplorer, un software que permite administrar un servidor de LDAP de forma remota. Las cuentas se pueden crear con el siguiente comando:

```
smbldap-useradd -a -g "Alumnos" sujeto1
```

De esta manera se crea el usuario sujeto1 y a su vez se agrega al grupo Alumnos. A continuación, se deberá cambiar la contraseña.

```
smbldap-passwd sujeto1
```

Una manera de ver las cuentas que hay en LDAP es usando el comando *ldapsearch -x -LLL -b ou=people,dc=esxi*. Con el software JXplorer es más fácil ver los usuarios y grupos que existen.

3.2 **PROCEDIMIENTO**

A continuación, se describe el procedimiento para integrar el hipervisor con el servicio de autenticación.

3.2.1 **Dominio LDAP-Samba en ESXi**

Para unir el servidor ESXi al dominio de LDAP-Samba, se deberá ingresar al servidor a través de vSphere Client. La IP del servidor es 10.4.11.254

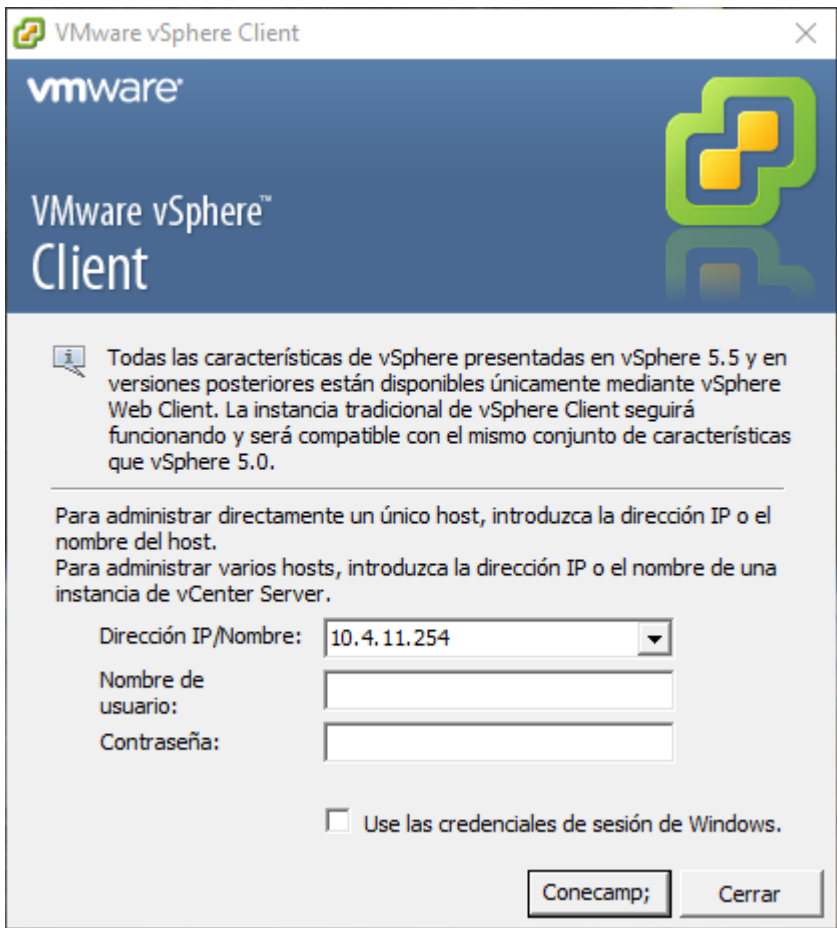


Figura 3-1. Ventana de logueo VMware vSphere Client

Nos autenticamos con una cuenta de administrador la que nos permitirá realizar cambios, asignar un dominio y cambiar el tipo de autenticación.



Figura 3-2. Menú de administración

Vamos a la casilla Configuration. Luego presionamos la opción que dice servidor de autenticación.

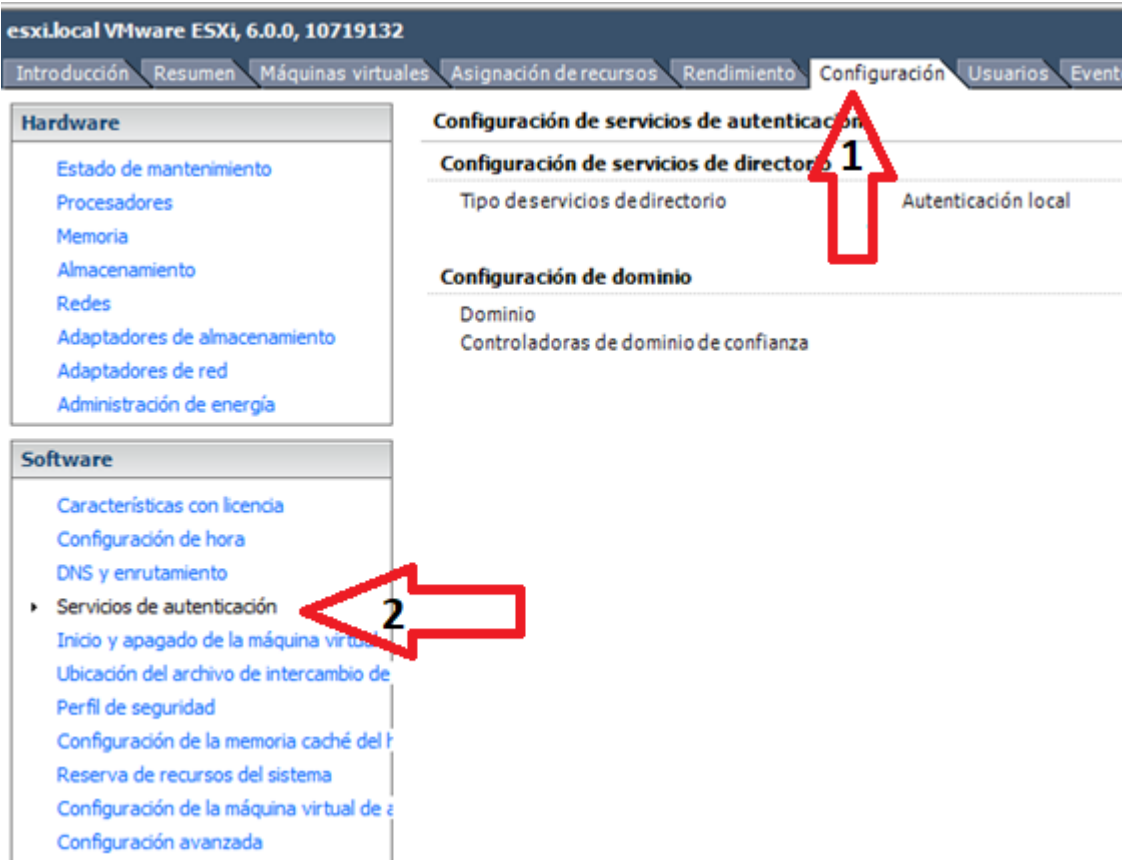


Figura 3-3. Menú de configuración

Vamos a propiedades.

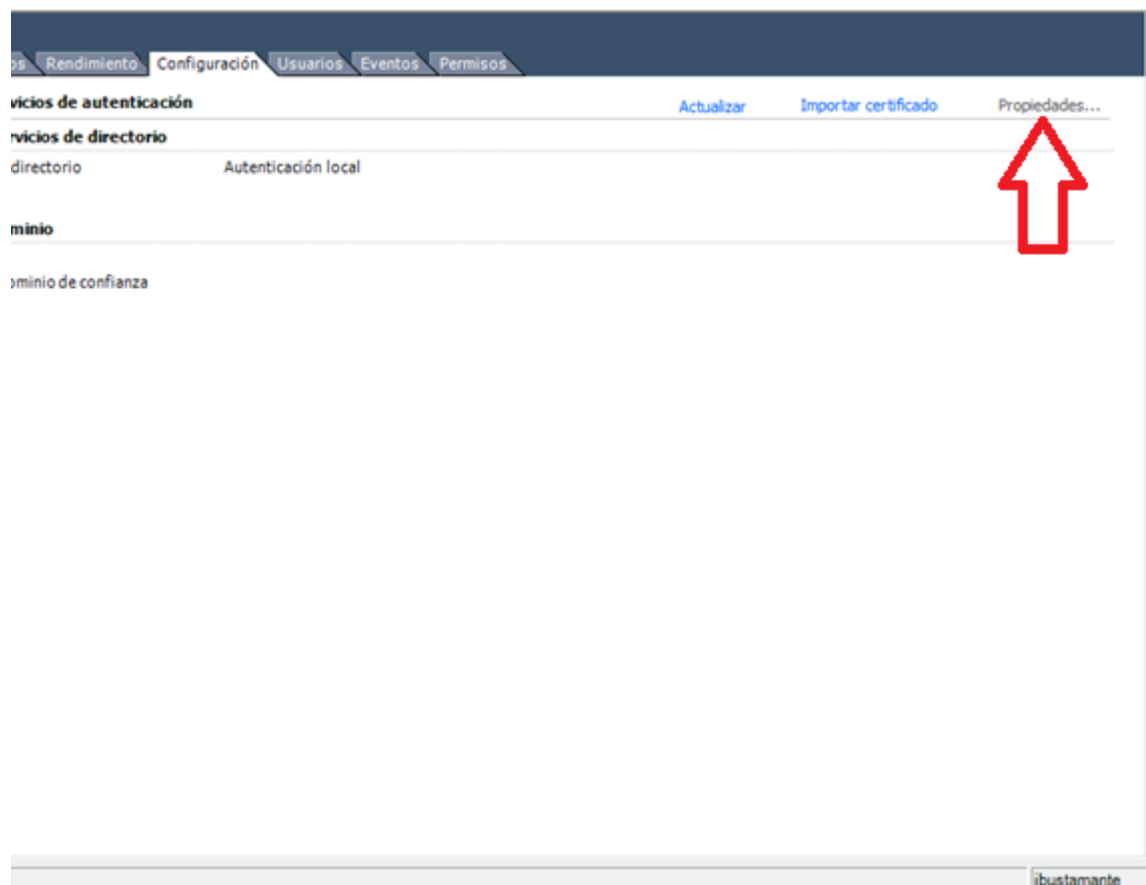


Figura 3-4. Menú de configuración. Zoom izquierdo.

Aparecerá una ventana, en la cual hay una opción para elegir el tipo de servidor de directorio, se desplegarán dos opciones, servidor local o active directory, seleccionamos este último. En la casilla Domain escribiremos el nombre del dominio de la maquina de LDAP el cual era *esxi*. Presionamos en Join Domain y debería aparecer una ventana que pedirá credenciales de administrador.

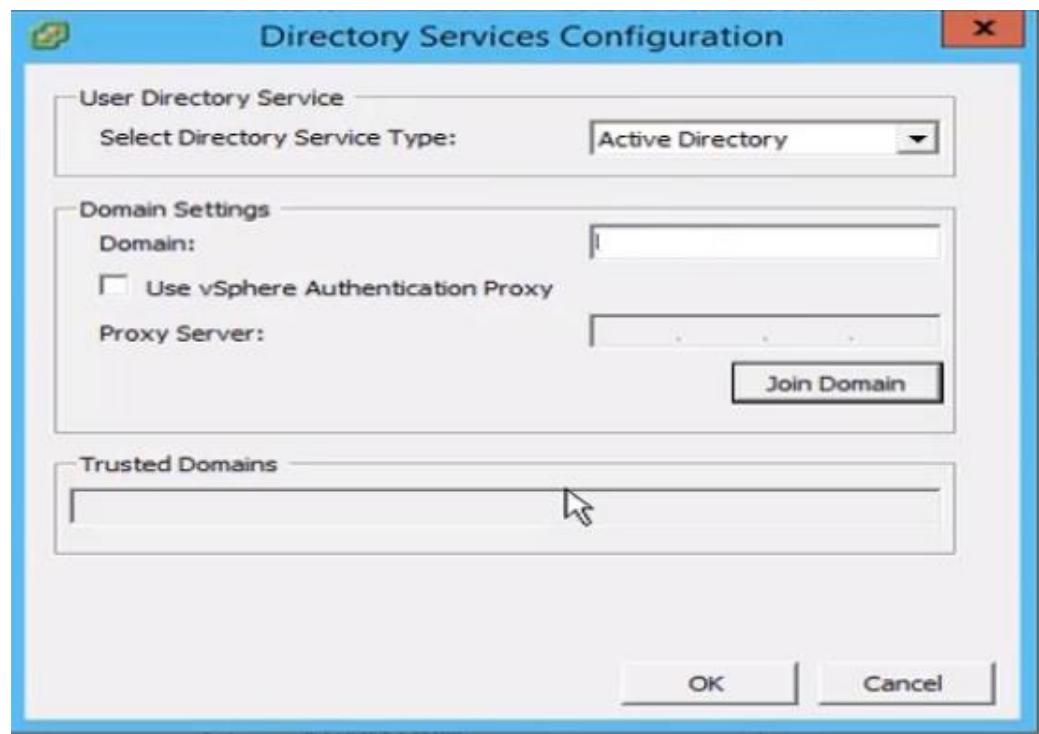


Figura 3-5. Ventana de configuracion. Servicio de directorio.

Utilizamos una cuenta con permisos para unir el servidor al dominio, por lo que usamos la de administrador.



Figura 3-6. Ventana de configuración. Unir dominio.

User Name: admin

Password: Teleco2018!

Finalmente le damos a Join Domain. Una vez integrado el host al servidor de LDAP, deberemos ir al home, una vez allí nos dirigiremos a la pestaña Permisos.

En esta pestaña deberemos asignar los roles que tendrán los usuarios o grupo de usuarios. La idea es asignar roles que tengan los permisos adecuados para cada tipo de usuario. Un profesor tendrá permisos distintos que un alumno, por lo que se deberá crear un rol para los alumnos y otro para los profesores.

Para agregar los permisos, hacemos click secundario en un espacio libre y presionaremos en agregar permisos y aparecerá una ventana de administración de permisos.

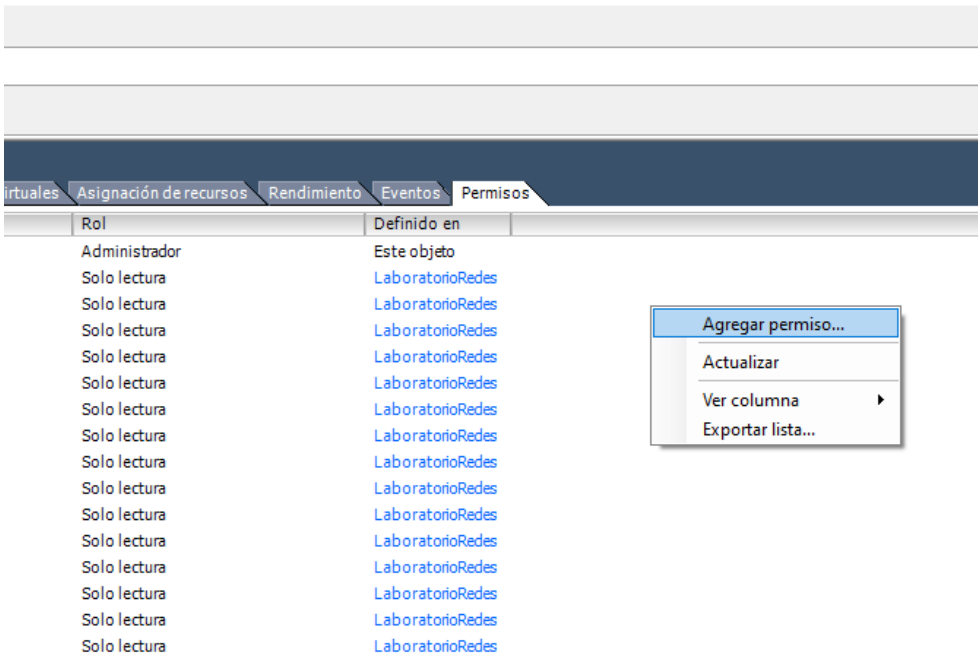


Figura 3-7. Permisos de ESXi

En esta ventana podremos ver los roles y permisos. Para agregar a un usuario o un grupo de usuarios y asignarle un rol deberemos ir a Agregar.

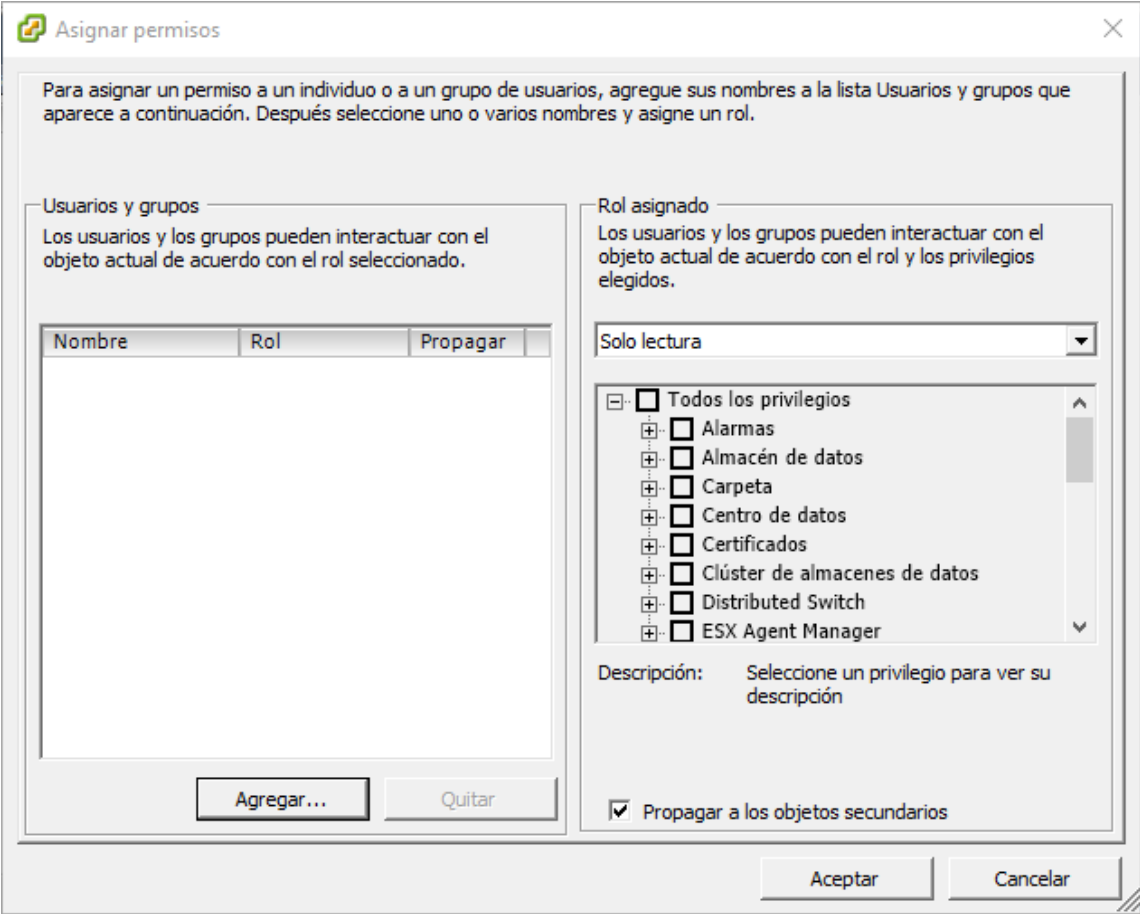


Figura 3-8. Ventana de asignación de permisos.

Aparecerá esta ventana, luego en la casilla desplegable donde dice dominio, seleccionamos el dominio de LDAP, en este caso esxi. Aparecerán todos los usuarios registrados en el servidor de LDAP, también aparecerán los grupos, todo dependerá de que es lo que queramos ver cambiándolo desde la casilla desplegable en usuarios y grupos. Una vez decidamos el usuario o grupo, lo agregaremos y le damos a aceptar.

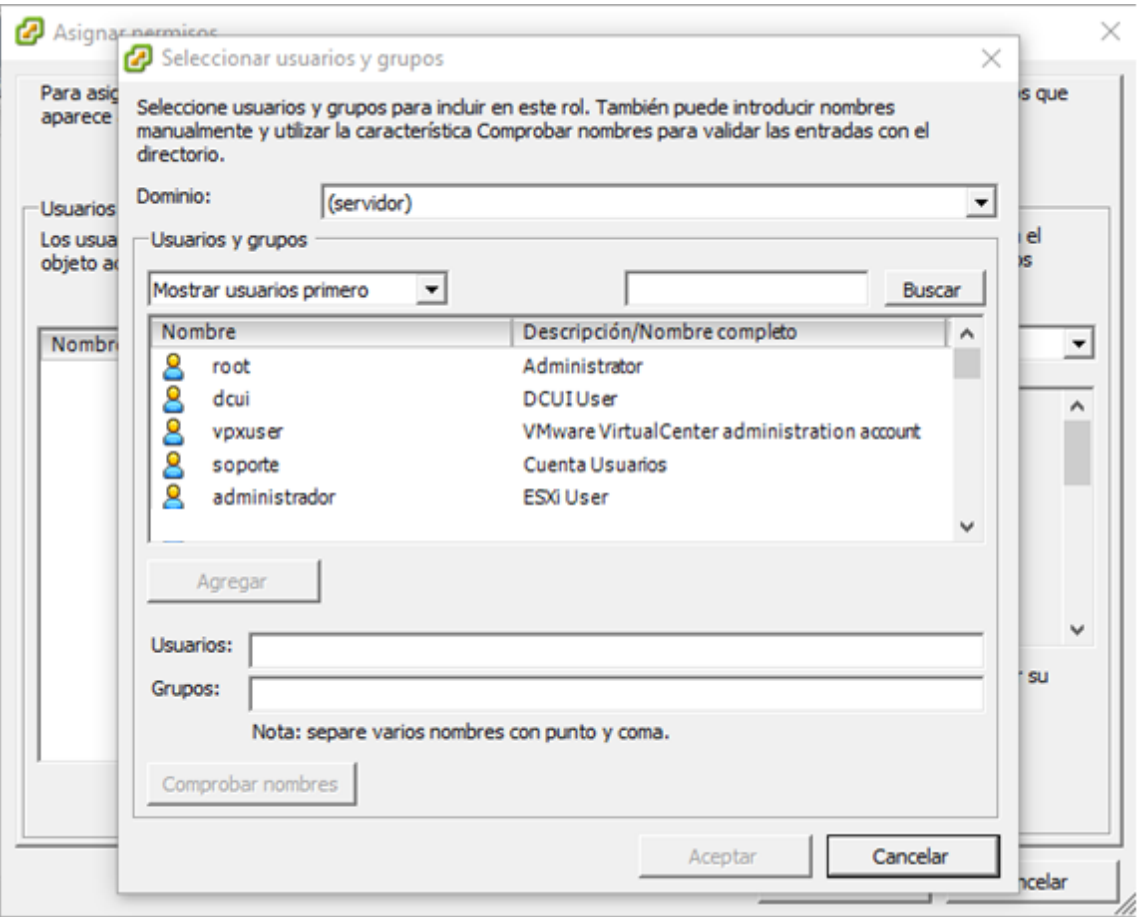


Figura 3-9. Ventana de selección de usuarios y grupos para asignar rol.

Una vez agregados los usuarios o grupos, podremos elegir el rol o los permisos que tendra. Por ultimo le damos a aceptar.

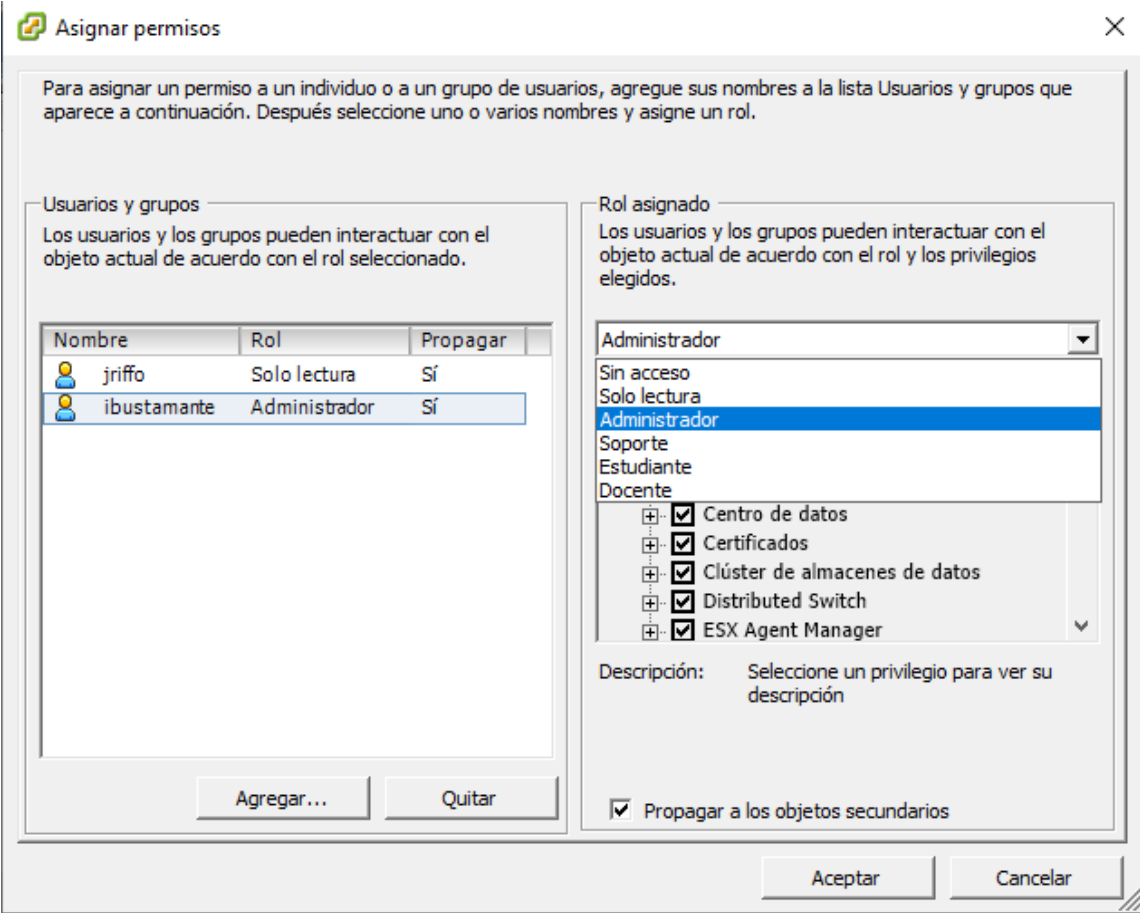


Figura 3-10. Ventana de asignación de permisos. Cambiando rol.

De esta manera los usuarios ya se podrían loguear en el servidor ESXi a través de la implementación de LDAP-Samba.

CONCLUSIONES

La virtualización a pesar de que no es una tecnología nueva, últimamente a tenido un gran realce y es que para un entorno donde quizás los recursos son limitados, tener que comprar equipos, hacerles mantención e incluso renovarlos, ya no es viable desde el punto de vista monetario, por lo que la virtualización vendría a solucionar este problema.

Cuando se piensa en una gran cantidad de usuarios, es difícil para un administrador tener que gestionar a cada uno de ellos, pero gracias a las herramientas que brindan los sistemas de autenticación esta tarea se simplifica, pudiendo controlar los recursos a los que tiene acceso cada usuario, un grupo o la totalidad de ellos. El tener que cambiar los permisos de cada usuario, uno por uno ya no es viable en entornos como una universidad, donde el flujo de personas es alto, siendo los sistemas de autenticación una necesidad casi una obligación.

Al trabajar en una memoria de título se entiende y se tiene mayor comprensión de lo visto en la carrera, hubo un proceso investigativo que dio cuenta del alcance que tienen las telecomunicaciones como lo fue trabajar en Linux que, aunque poco usado y desconocido para la mayoría de personas, es un sistema muy flexible (dependiendo de la distribución) y que se utiliza mucho en entornos de red, bases de datos, etc. Durante las investigaciones que se hicieron de Linux, concretamente la distribución Debian 9, un entorno distinto al que se está habituado como lo es Windows, da cuenta de lo importante que fue el trabajar con este durante la carrera.

BIBLIOGRAFÍA

- Bipin. Difference between vSphere, ESXi and vCenter.[en línea] 24 agosto 2012
<<http://www.mustbegeek.com/difference-between-vmware-esxi-and-vmware-vcenter/>>
- Gomez Periañez, Francisco. Tutorial de VirtualBox [en línea]. 8 septiembre 2016
<http://fpg.x10host.com/VirtualBox/tipos_de_hipervisores.html>
- Joaquin Vte, Servidor ldap-samba de un centro educativo [en línea]. 2 enero 2019
<<http://joaalsai.com/index.php/2019/01/02/servidor-ldap-samba-de-un-centro-educativo/>>
- Microsoft. Active Directory Domain Services Overview [en línea]. 30 mayo 2017
<<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>>
- Red Hat, Inc. Descripción general de la configuración de OpenLDAP. [en línea]. 2005
<<https://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-rg-es-4/s1-ldap-quickstart.html>>
- Shauns. Samba.schema. [en línea] 2014
<<https://gist.github.com/shauns/64b3dfa581fb74501c0d>>
- Techminded. Install Samba PDC + LDAP on Debian Squeeze. [en línea]. 2013
<<http://techminded.net/blog/install-samba-pdc--ldap-on-debian-squeeze.html>>
- VMware, Virtualización [en línea].
<<https://www.vmware.com/latam/solutions/virtualization.html>>

ANEXOS

ANEXO 1

Configuración del archivo slapd.conf (ubicación /etc/ldap/slapd.conf)

```
include /etc/ldap/schema/core.schema
include /etc/ldap/schema/collective.schema
include /etc/ldap/schema/corba.schema
include /etc/ldap/schema/cosine.schema
include /etc/ldap/schema/duaconf.schema
include /etc/ldap/schema/dyngroup.schema
include /etc/ldap/schema/inetorgperson.schema
include /etc/ldap/schema/java.schema
include /etc/ldap/schema/misc.schema
include /etc/ldap/schema/nis.schema
include /etc/ldap/schema/openldap.schema
include /etc/ldap/schema/ppolicy.schema
include /etc/ldap/schema/samba.schema
pidfile /var/run/slapd/slapd.pid
argsfile /var/run/slapd/slapd.args
loglevel none
modulepath /usr/lib/ldap
moduleload back_hdb
sizelimit 500
tool-threads 1
backend hdb
database hdb
suffix "dc=esxi"
rootdn "cn=admin,dc=esxi"
rootpw {MD5}X03M01qnZdYdgyfeuILPmQ==
directory "/var/lib/ldap"
dbconfig set_cachesize 0 2097152 0
dbconfig set_lk_max_objects 1500
dbconfig set_lk_max_locks 1500
dbconfig set_lk_max_lockers 1500
index objectClass eq,pres
index ou,cn,sn,mail,givenname eq,pres,sub
index uidNumber,gidNumber,memberUid eq,pres
index loginShell eq,pres
index uid pres,sub,eq
index displayName pres,sub,eq
index nisMapName,nisMapEntry eq,pres,sub
index sambaSID eq
index sambaPrimaryGroupSID eq
index sambaDomainName eq
index default sub
index uniqueMember eq
index sambaGroupType eq
index sambaSIDList eq
lastmod on
checkpoint 512 30
access to attrs=userPassword,sambaNTPassword,sambaLMPassword,sambaPwdMust
Change,sambaPwdLastSet
by self write
by anonymous auth
by * none
access to attrs=shadowLastChange,shadowMax
by self write
by * read
access to *
by * read
```

ANEXO 2

Configuracion del archivo *smb.conf*

```

dos charset = CP1251
unix charset = UTF8
display charset = UTF8
workgroup = LDAP
realm = OpenLDAP
server string = %h server
map to guest = Bad User
passdb backend = ldapsam:ldap://10.4.11.12/
pam password change = Yes
passwd program = /usr/sbin/smbldap-passwd -u %u
passwd chat = *New*password* %n\n *Retye*new*password* %n\n *all*authentication
*tokens*updated*
syslog = 0
time server = Yes
log file = /var/log/samba/log.%m
max log size = 1000
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
add user script = /usr/sbin/smbldap-useradd -m %u -d /domain/home/%u %u
delete user script = /usr/sbin/smbldap-userdel %u -r %u
add group script = /usr/sbin/smbldap-groupadd -p %g
delete group script = /usr/sbin/smbldap-groupdel %g
add user to group script = /usr/sbin/smbldap-groupmod -m %u %g
delete user from group script = /usr/sbin/smbldap-groupmod -x %u %g
set primary group script = /usr/sbin/smbldap-usermod -g %g %u
add machine script = /usr/sbin/smbldap-useradd -w %u
domain logons = Yes
os level = 10
preferred master = Yes
domain master = Yes
dns proxy = No
wins support = Yes
ldap admin dn = cn=admin,dc=esxi
ldap delete dn = Yes
ldap group suffix = ou=group
ldap idmap suffix = ou=idmap
ldap machine suffix = ou=computer
ldap suffix = dc=esxi
ldap ssl = no
ldap user suffix = ou=people
panic action = /usr/share/samba/panic-action %d
map acl inherit = Yes
case sensitive = No
hide unreadable = Yes
map hidden = Yes
map system = Yes

[homes]
comment = Home Directories
path = /domain/home/%u
valid users = %S
read only = No
create mask = 0600
directory mask = 0700
browseable = No

[netlogon]
path = /domain/netlogon
browseable = No

```

ANEXO 3

Configuración del archivo smbldap.conf

```
# Configuración general
SID="S-1-5-21-3384730673-3036888877-1999087345"
sambaDomain="esxi"
#####
# LDAP Configuración
#####
slaveLDAP="127.0.0.1"
slavePort="389"
masterLDAP="10.4.11.12"
masterPort="389"

ldapTLS="0"
ldapSSL="0"
verify="require"

cafile="/etc/smbldap-tools/ca.pem"
clientcert="/etc/smbldap-tools/smbldap-tools.pem"
clientkey="/etc/smbldap-tools/smbldap-tools.key"

suffix="dc=esxi"
usersdn="ou=people,${suffix}"
computersdn="ou=computer,${suffix}"
groupsdn="ou=group,${suffix}"
idmapdn="ou=idmap,${suffix}"

sambaUnixIdPool="sambaDomainName=${sambaDomain},${suffix}"
scope="sub"
hash_encrypt="MD5"
crypt_salt_format="%s"
#####
# Unix Accounts Configuration
#####
userLoginShell="/bin/bash"
userHome="/domain/home/%U"
userHomeDirectoryMode="700"
userGecos="System User"
defaultUserGid="513"
defaultComputerGid="515"
skeletonDir="/etc/skel"
defaultMaxPasswordAge="365"
#####
# SAMBA Configuration
#####
userSmbHome="//%L\%U"
userProfile=""
userHomeDrive="U:"
userScript=""
mailDomain="esxi"
#####
# SMLDAP-TOOLS Configuration
#####
with_smbpasswd="0"
smbpasswd="/usr/bin/smbpasswd"
with_slappasswd="0"

slappasswd="/usr/sbin/slappasswd"
```