ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DISEÑO E IMPLEMENTACIÓN DE UNA SOLUCIÓN DE INTEGRACIÓN DE AUTENTICACIÓN ENTRE PLATAFORMAS WINDOWS Y LINUX, UTILIZANDO EL DIRECTORIO ACTIVO DE WINDOWS COMO CONTROLADOR DE DOMINIO"

INFORME DE PROYECTO INTEGRADOR

Previa a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

JAZMÍN DEL ROCÍO AVILÉS CARPIO

MILDRED YANINA PERALTA ORRALA

GUAYAQUIL – ECUADOR

AÑO: 2015

AGRADECIMIENTOS

Agradezco a mis padres por sus valiosos consejos y apoyo incondicional, a mi hermana y sobrina porque siempre me dieron ánimos para continuar, también agradezco a mis amigos ya que con sus palabras de aliento me impulsaron a seguir de frente ante cualquier adversidad y a mis profesores por otorgarme sus conocimientos y experiencias para forjarme como profesional. ¡Mildred, lo logramos!

Jazmín del Rocío Avilés Carpio

Agradezco en primer lugar a Papito Dios por darme la oportunidad de estudiar en la ESPOL y llenarme de bendiciones en esta prestigiosa universidad, a mi hermosa madre Glenda Orrala por darme fuerzas para salir adelante y apoyarme en todo momento, a mi compañera de proyecto Jazmín Avilés por tenerme paciencia y por permitirme compartir este merito junto a ella, a mis profesores: el Ing. Roberto Patiño, el Ing. Rayner Durango, el Ing. Jorge Magallanes y a la Ing. María Angélica Santacruz, porque todos demostraron tenernos paciencia, por dedicarnos su tiempo y brindarnos sus conocimientos, además quiero agradecer a mis amigos, los Ingenieros Fernando Ortiz y Ángel Bravo porque jamás nos negaron su ayuda en momentos de inquietud.

Mildred Yanina Peralta Orrala

DEDICATORIA

Dedico este trabajo a mi familia, pilar fundamental en mi vida, en especial a mi madre cuyo apoyo y guía ha permitido culminar esta meta y forjar nuevas, a mis profesores por depositar sus conocimientos en mí y confiar en mi éxito como profesional.

Jazmín del Rocío Avilés Carpio

Quiero dedicar mi proyecto de graduación a papito Dios, ya que siempre le oré para que me motivara y me diera fuerzas para seguir investigando, quiero dedicársela a mi madre porque ella siempre me lo ha dado absolutamente todo, a mi familia entera para que se sientan orgullosos de tener una profesional más en el hogar, a mi novio y mejor amigo Luigi Rubio, porque desde lejos sé que está esperando verme graduada y ser toda una profesional, a mi profesor el Ing. Jorge Magallanes porque él nos motivó a realizar este proyecto, y a mis compañeros de carrera, para demostrarles que todo es posible en esta vida, en especial para aquellos que aún no obtienen su título y están egresados.

Mildred Yanina Peralta Orrala

TRIBUNAL DE EVALUACIÓN

Ing. José Roberto Patiño Sánchez	**Ing. María Angélica Santacruz Maridueña**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

"La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual"

Jazmín del Rocío Avilés Carpio

Mildred Yanina Peralta Orrala

RESUMEN

El presente proyecto solventa la problemática de las empresas con una compleja administración, en el servicio de autenticación de los usuarios por la presencia de ambientes híbridos, para lo cual se planteó dos alternativas que permiten la integración del servicio de autenticación entre las plataformas Linux y Windows, utilizando el sistema operativo Windows como controlador de dominio y directorio principal, por lo que se emplearon servidores y estaciones de trabajo virtuales de ambas plataformas para la ejecución de las pruebas pertinentes, siendo utilizado en el ambiente Windows la estación de trabajo Windows 8 y como servidor Windows Server 2012 R2 y en el ambiente Linux la estación de trabajo Ubuntu 14.04 y como servidor CentOS 7.0.

Los métodos de integración que se utilizaron en este proyecto fueron System Security Services Daemon (SSSD) y Winbind, los cuales involucran a los protocolos Lightweight Directory Access Protocol (LDAP) y Kerberos. Ambos métodos permiten que los clientes Linux se autentiquen con el controlador de dominio Windows, obteniendo la administración centralizada de los usuarios.

Sin embargo cabe mencionar que SSSD es una alternativa relativamente nueva cuya complejidad es menor pero de igual adaptabilidad que Winbind, lastimosamente se encuentra limitado por el uso únicamente del protocolo LDAP, lo cual es contrario a la alternativa de Winbind, por lo que se concluye que dependiendo del ambiente de la empresa se debe escoger la solución que mejor se adapte, es decir se sugiere la utilización de Winbind en ambientes que usen el protocolo NT LAN Manager (NTLM) y la utilización de SSSD en ambientes que usen el protocolo LDAP, por lo que en este proyecto se detallan los conceptos básicos y específicos que describen la integración de las plataformas, además de las respectivas configuraciones y los diseños para cada solución.

ÍNDICE GENERAL

CAPÍTULO 1

1. PROBLEMÁTICA

En la actualidad, es frecuente la existencia de plataformas híbridas en las organizaciones, ya sea por motivos económicos, requerimientos específicos o inclusive preferencia por un determinado sistema.

Por ello el presente proyecto se lleva a cabo con las plataformas más utilizadas en el mercado empresarial, Linux y Windows, ya que por ejemplo Windows maneja una interfaz intuitiva para el usuario, convirtiéndolo en un sistema de configuración elemental y de mayor uso en el mercado, con lo cual se le atribuye un número considerable de aplicaciones compatibles, a su vez Linux es reconocido por su confiabilidad y robustez, además que es un sistema de código abierto, con lo cual la empresa no invierte en licenciamiento.

Pero independientemente de la infraestructura tecnológica a manejar dentro de una red corporativa, sea ésta Linux o Windows, el personal de tecnología de información (TI) tiene como prioridad asegurar un servicio de alta disponibilidad, calidad y productividad para la compañía.

Sin embargo, siempre han existido inconvenientes relacionados en la administración de las cuentas de los usuarios, como por ejemplo: la información de la cuenta de un usuario está almacenada en la base de datos del sistema operativo donde fue creado, en este caso un servidor Windows, el usuario puede acceder al sistema libremente y sin inconvenientes, no obstante al necesitar acceso a los servidores o estaciones de trabajo Linux, este requerimiento no podrá llevarse cabo ya que el servidor Linux no posee información sobre la cuenta del usuario, es por ello que el administrador de la red se verá obligado a crear una nueva cuenta de usuario, usada únicamente para realizar esta función, cabe recalcar que esta tarea puede llevarse a cabo con múltiples usuarios más, lo que involucra un considerable esfuerzo administrativo.

1.1. Identificación del Problema

Con el pasar del tiempo es habitual que las empresas presenten dificultades a nivel tecnológico, ya sea por no existir una proyección de crecimiento del número de usuarios a mediano, largo plazo o por una organización ineficiente.

El problema puede extenderse provocando deficiencia en la seguridad de la información por la duplicación de datos de las cuentas de usuarios, porque cada sistema operativo Linux o Windows maneja una base de datos independiente, lo que dificulta el control de los registros de los usuarios al sistema y dificulta una administración centralizada de los usuarios en la red.

1.2. Justificación

Mediante el diseño de una solución de autenticación entre diferentes plataformas, las empresas en el Ecuador con arquitecturas híbridas, podrán obtener una administración centralizada de las cuentas de los usuarios.

Ya que la implementación permitirá una reducción de la duplicación de datos de los usuarios y un control sobre los registros de acceso de los usuarios a los servicios o equipos, mejorará la seguridad informática en la empresa.

1.3. Objetivos

1.3.1. Objetivo General

Analizar, diseñar e implementar una solución de autenticación para la integración de plataformas Linux y Windows con la finalidad de centralizar la gestión de los usuarios en un ambiente empresarial, integrado por el Directorio Activo de Windows.

1.3.2. Objetivos Específicos

- Analizar el servicio de autenticación de los sistemas operativos Linux y Windows.
- Analizar el presupuesto de la solución.
- Diseñar e implementar una solución de autenticación para la unificación de plataformas híbridas.
- Ofrecer una solución asequible y de corto tiempo para facilitar a las empresas una adecuada administración de sus usuarios.

1.4. Solución propuesta

La solución incluye únicamente la manipulación de archivos de configuración, evitando la adquisición de equipos y por ende gastos adicionales, por lo que este proyecto está orientado a empresas con plataformas heterogéneas, en la cual se escogió al Directorio Activo de Windows como controlador de dominio y directorio principal, y se estableció que los otros sistemas operativos que posee la empresa deban acceder al directorio principal para la autenticación de los usuarios, obteniendo de esta manera una administración centralizada.

1.5. Metodología

En el proyecto se utilizó la metodología cascada, esta técnica es un proceso secuencial de actividades, las cuales fueron desarrolladas de la siguiente manera:

1. Investigar la solución de la problemática: En este pasó se realizó una investigación sobre los métodos de autenticación de los usuarios dentro de un ambiente de dominio entre las plataformas Linux y Windows, así también como los protocolos involucrados.
2. Analizar los requerimientos de la implementación: Se selecciona el software virtualizador y los sistemas operativos Linux y Windows a utilizar.

3. Crear el diseño de la implementación: Se lleva cabo el diseño lógico de la solución propuesta y la investigación de las configuraciones pertinentes.
4. Implementar la solución: Se ejecutan las alternativas de solución de acuerdo a las configuraciones específicas para las distintas plataformas.
5. Realizar pruebas: En este último paso se elaboran diversas pruebas para evaluar la implementación realizada, así también se establecen las ventajas, desventajas y limitaciones de acuerdo a los resultado obtenidos para la elaboración de las conclusiones.

En la Figura 1.1 se puede visualizar de manera gráfica la metodología utilizada en el proyecto.

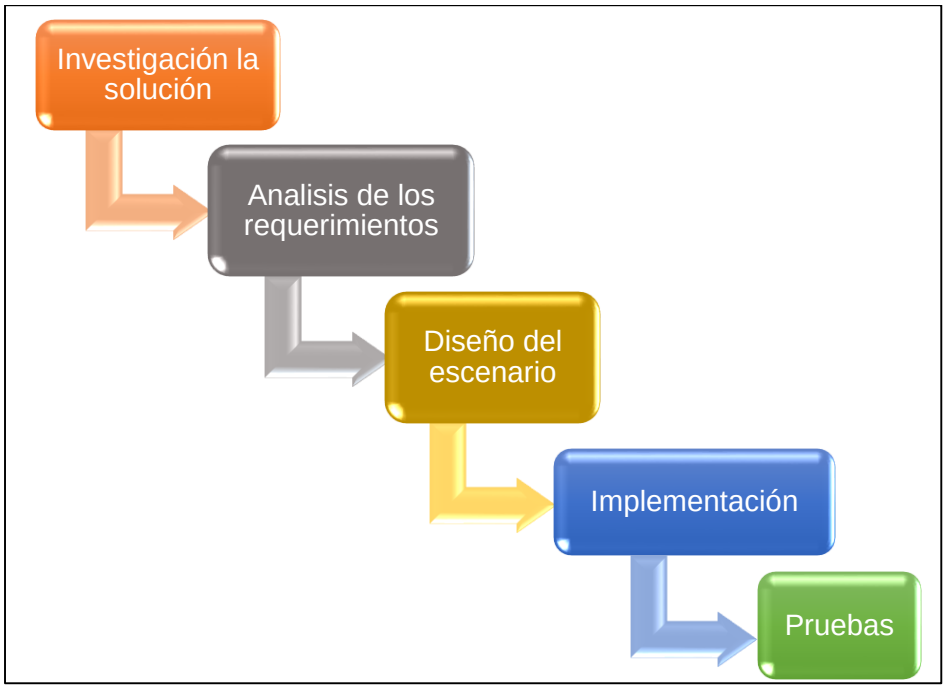


Figura 1.1. Metodología Cascada

1.6. Integración de plataformas en el Ecuador

En el Ecuador, las organizaciones con plataformas heterogéneas han ido en aumento por la emisión del decreto 1014, que establece en las empresas de Administración Pública la utilización de software libre en sus sistemas y equipamientos informáticos [1], por ello las compañías han llevado a cabo la incorporación y migración a software no licenciado, sin embargo el arraigado conocimiento de los sistemas Windows y la poca noción de la plataforma Linux, ha producido conflictos sobre la autenticación para los administradores o jefes del departamento de informática e inclusive a los propios trabajadores de la empresa.

Es por ello que para la resolución de dicha problemática, se propone una integración entre plataformas con el fin armar un escenario unificado en la empresa a nivel de autenticación, en otras palabras se desea que cualquier usuario de la compañía pueda acceder al equipo de trabajo o servidor siempre y cuando su nombre de usuario y contraseña esté almacenado en un directorio principal y tenga los permisos requeridos.

1.7. Servicio de directorio

El servicio de directorio es una o varias aplicaciones que almacenan de forma organizada la información de los usuarios en una red corporativa, existen numerosas implementaciones de servicios de directorio, entre las más conocidas están; Directorio Activo de Microsoft, Directorio Abierto de Apple, OpenLDAP en Linux, entre otros [2].

Directorio Activo de Windows:

Hoy en día, es considerada la herramienta de directorio predominante en las infraestructuras empresariales [3] ya que permite un “todo en uno”, porque además de proveer un directorio para el almacenamiento de las cuentas de usuarios, proporciona permisos por grupo, usuario o unidad organizativa, así también permite compartir archivos e impresoras, sin embargo su costo es

elevado al igual que su mantenimiento y existe poco soporte para la comunicación con equipos Linux y Mac [4].

En la actualidad el protocolo más utilizado que permite el acceso a los servicios de directorio es LDAP, el cual puede almacenar de manera central toda la información de una organización, ya que facilita la reserva de datos en el directorio de manera jerárquica y sencilla [5]. Por lo cual, uno de los motivos principales para implementar LDAP es la creación de una red unificada para los usuarios, ya que otorga una única identidad indiferentemente del sistema operativo que utilicen. Ya que LDAP es un protocolo independiente de la plataforma puede ser implementado en servidores y estaciones de trabajo Windows y Linux [3].

1.8. Servicio de autenticación

La autenticación es un proceso en el cual se identifica a un usuario o servicio de acuerdo a ciertos criterios [6], por lo que un mecanismo de autenticación es un servicio del sistema que facilita la identificación de algo o alguien, mediante el conocimiento de cierta información o posesión de un objeto que permita verificar su identidad. Al igual que los servicios de directorios los servicios de autenticación manejan sus propios protocolos, como es el caso del protocolo Kerberos que será utilizado en la implementación del proyecto por ser compatible con ambas plataformas.

Kerberos es un protocolo de elección para entornos de red multi-plataforma, utiliza criptografía de claves simétricas brindando seguridad al momento de validar los usuarios con los servicios de la red esto se lo realiza con el fin de evitar enviar las contraseñas a través de la red. [7]

Para la autenticación del servidor principal en Windows server con los clientes Windows se utiliza la autenticación kerberos versión 5, el cual emite tickets para tener acceso a la red, estos tickets contienen información cifrada para confirmar la identidad del usuario.

Al momento de realizar la instalación del Directorio Activo de Windows, viene por defecto el servicio de KDC que se ejecuta en kerberos 5, la cual almacena usuario y contraseña del cliente. [8]

La diferencia de utilizar Kerberos en Linux, radica en que se tiene que fusionar con otros mecanismos, por ejemplo para el caso de la autenticación serían el módulo PAM y otros archivos de configuración, al contrario de Windows que funciona de manera transparente [9][10].

1.9. Tipos de Integración

Se entiende a la integración en informática como un proceso cuyo objetivo es unir los datos contenidos en diferentes subsistemas para convertirlo en uno sistema más extenso, permitiendo un método rápido y sencillo para compartir datos cada vez que fuera necesario [11].

No obstante el concepto es enfocado al servicio de autenticación de las plataformas, con lo cual se unifica la autenticación de los usuarios mediante el nombre de usuario y contraseña alojados en un directorio principal.

La integración se puede realizar de dos maneras:

- Directa
- Indirecta

La integración directa como se puede observar en la Figura 1.2, facilita que los sistemas Linux interactúen directamente con el Directorio Activo de Windows sin ningún tipo de equipo intermediario [12].

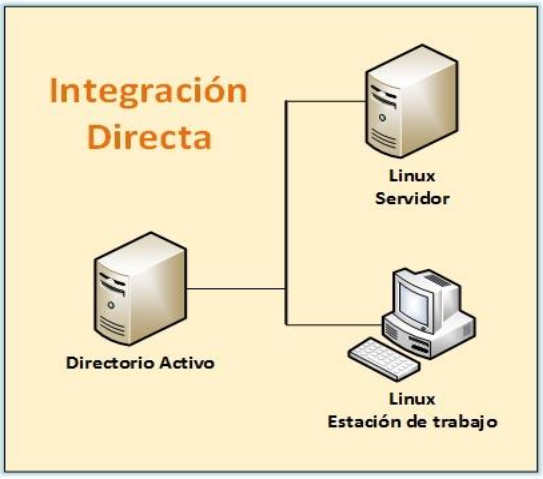


Figura 1.2. Integración Directa, reproducción basada en [12]

A su vez, mediante la integración indirecta como se visualiza en la Figura 1.3, los sistemas Linux deben de interactuar con un equipo intermediario que trabaja de identificador central y éste a su vez se comunica con el Directorio Activo de Windows. [12]

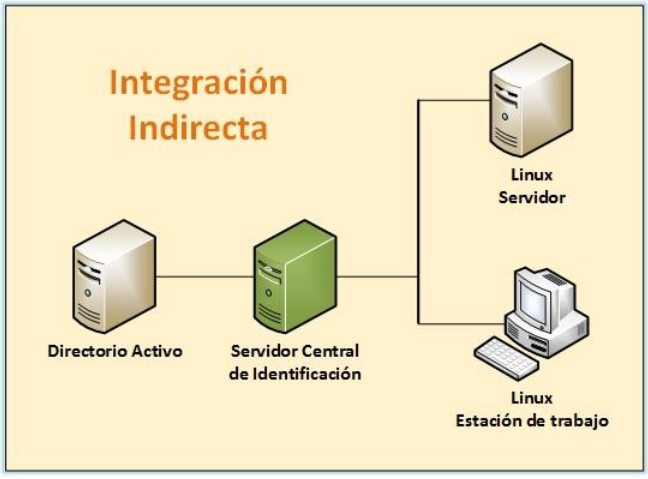


Figura 1.3. Integración Indirecta, reproducción basada en [12]

¿Cuándo utilizar integración directa o indirecta? Esto se puede resolver de acuerdo a los siguientes aspectos; tamaño de la implementación, costos, permisos u otros. Por lo general la integración directa se utiliza cuando el tamaño de la implementación, es decir la cantidad de equipos a los cuales se

desea integrar es relativamente pequeña, en cambio se utiliza la integración indirecta cuando se tiene demasiados sistemas y es necesarios centralizarlos antes de integrarlos para una mejor gestión, otro factor que se considera relevante son los costos, ya que al implementar una integración indirecta se utilizaría sistemas de terceros lo cual podría elevar el costo de la implementación, sin embargo existen soluciones que se sujetan a licencias libres pero su soporte implica un gasto adicional. [12]

Cabe mencionar que el proyecto se sujeta a la integración directa por ahorro de costos y escenarios de implementación relativamente pequeños, además de la ventaja de independencia de algún otro sistema o equipo, por lo que la comunicación entre el controlador de dominio con los clientes es inmediata, evitando problemas de conexión en caso de que el sistema falle.

1.10. Métodos de autenticación de multiplataforma

La unificación de las plataformas en un ambiente empresarial ha ido en crecimiento, ya sea por las restricciones a datos e información privilegiada o por el control de cuentas de usuarios, pero debido a la incompatibilidad de las principales plataformas, se han desarrollado diversas alternativas para cumplir con dicha función, las cuales dependen del tipo de integración a realizar, alcance u otros. Ya que se decidió utilizar la integración directa se escogió dos mecanismos para realizar dicha autenticación, los cuales son: Winbind y SSSD.

SSSD

System Security Services Daemon es un conjunto de demonios que permiten la administración de directorios y mecanismos de autenticación, proporcionando una interfaz NSS y PAM. [13].

Winbind

Es un componente de la suite samba que permite inicio sesión unificado, extrayendo información de identidad de un usuario, como el nombre usuario y su respectiva contraseña del Directorio Activo de Windows logrando que actúe como un miembro del dominio. [14]

CAPÍTULO 2

2. ANÁLISIS Y DISEÑO DE LAS POSIBLES SOLUCIONES A IMPLEMENTAR.

En este capítulo se analizan y diseñan dos alternativas para la solución de autenticación, las cuales serán implementadas posteriormente en un ambiente de prueba, lo que permitirá cumplir con el objetivo de centralizar las cuentas de usuarios.

2.1. Análisis de posibles soluciones

En el presente proyecto se explican dos alternativas para solventar la problemática de inicio de sesión multiplataforma, que son los demonios Winbind y SSSD ya que ambos involucran a los protocolos LDAP y kerberos y debido a su compatibilidad con ambas plataformas permitirán una comunicación Linux-Windows. Como información adicional se denomina demonio en Linux al proceso ejecutado en segundo plano, es decir ejecutado sin intervención del usuario.

El mecanismo de autenticación kerberos que será utilizada en ambas alternativas proporciona un boleto que demuestra la identidad del usuario y una clave de sesión compatible, esta clave contiene información relacionada al usuario y del servicio al cual va acceder. Cuando un usuario inicia sesión por primera vez, el KDC crea un boleto y una clave de inicio sesión, esto constituye como un credencial para el usuario, el KDC accede a una base de datos para autenticar la identidad del usuario y le devuelve un boleto que le permite el acceso al otro equipo permitiendo demostrar la identidad mutua entre dos equipos de red de manera segura. Cabe mencionar que por cada servicio que se ejecute en un servidor determinado, el usuario debe tener una nueva credencial, este proceso de creación de credenciales es transparente [15] [16].

Solución utilizando SSSD

Es un intermediario entre los clientes locales y el servidor principal, que realiza la gestión de controlar el dominio, es decir proporciona el acceso a varios proveedores de identidad y autenticación. Utiliza interfaces estándar PAM y NSS para proveer la interfaz al sistema y además de permitir la comunicación de diferentes cuentas. [17]

SSSD, es independiente de las aplicaciones, ya que trabaja con un robusto almacenamiento de caché local que pertenece a la identidad de un grupo o de un usuario. La ventaja de esta solución es que almacena las credenciales en el equipo local, en otras palabras permite trabajar desconectado de la red [18] [19], sin embargo no es compatible con el protocolo NTLM.

En la Figura 2.1 se muestra de manera sencilla el esquema de funcionamiento de SSSD y la presencia de los protocolos LDAP y kerberos.

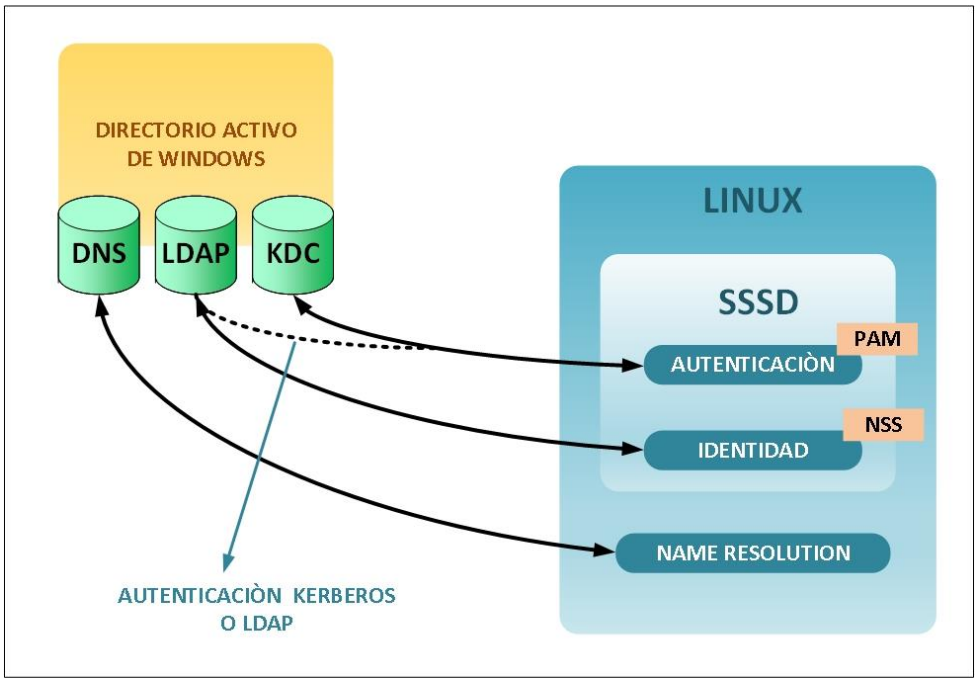


Figura 2.1. Esquema SSSD, reproducción basada en [44]

Solución utilizando Winbind

Winbind trabaja con el módulo PAM y el servicio de nombres NSS, lo que le permite realizar tres funciones separadas: autenticar las credenciales de usuarios, nombre de usuario y contraseña a través PAM, facilitar la resolución de identidad mediante NSS, es decir que permite adquirir información del nombre del host o del usuario, y también mantener una base de datos llamada winbind_idmap.tdb, en donde se registran las identificaciones entre ambas plataformas. [14]

Cabe aclarar que Winbind resuelve el problema de sincronizar contraseñas entre distintos sistemas, ya que toda la información relacionada a las contraseñas se guardó en un solo punto, en el controlador de dominio Windows. [14]

En la Figura 2.2 se observa el funcionamiento del esquema de Winbind trabajando como intermediario y relacionándose con LDAP y kerberos.

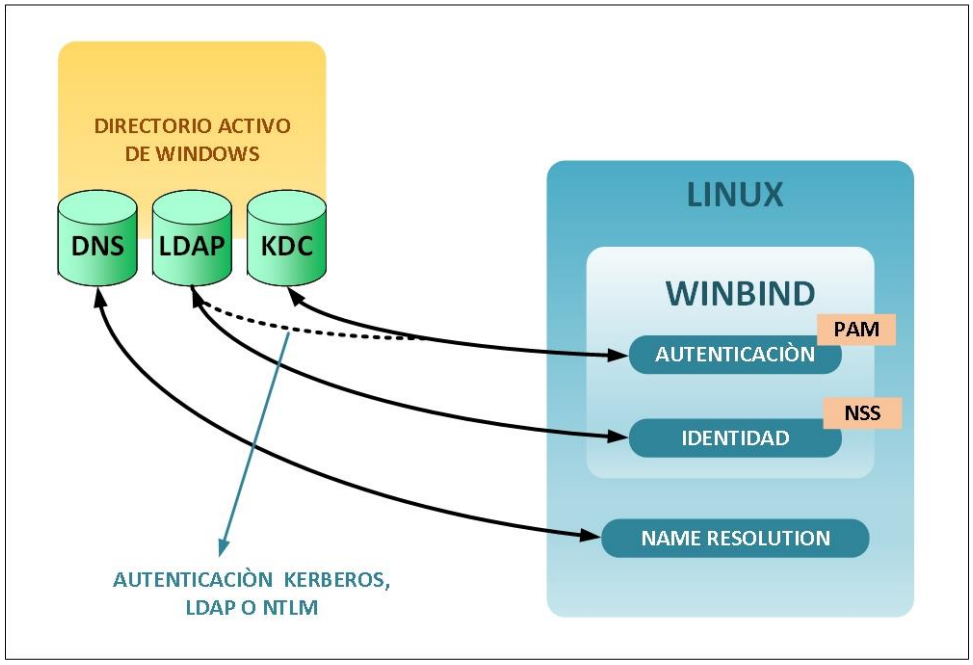


Figura 2.2. Esquema de Winbind, reproducción basada en [44]

2.2. Diseño del esquema lógico de la red

Una vez comprendido el esquema de funcionamiento de Winbind y SSSD, se procede a la creación del diseño lógico de la red que se usará para la elaboración de la implementación de los escenarios y posterior ejecución de pruebas.

En la Figura 2.3 se muestra el diseño propuesto para la resolución de la problemática, en el cual “Proyecto.com” es el nombre de dominio de la empresa, las estaciones de trabajo Windows y los servidores y estaciones de trabajo Linux se autentican con el Directorio Activo de Windows, el cual es el contenedor de las cuentas de los usuarios de la organización.

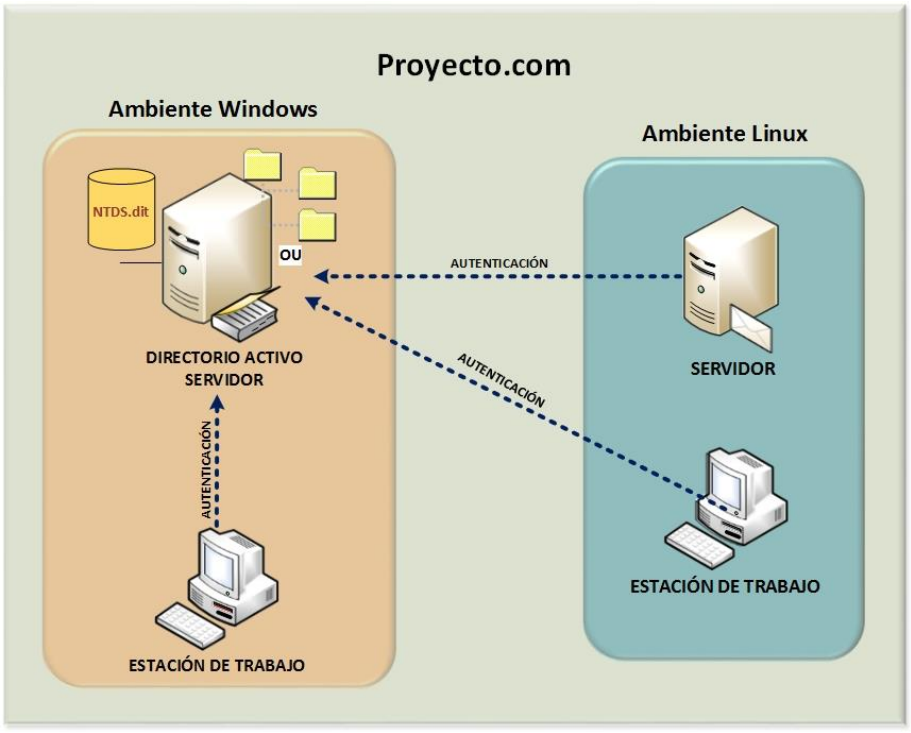


Figura 2.3. Esquema lógico de la red

2.3. Diseño de los escenarios de las alternativas solución

En este apartado se definen los escenarios para la implementación de las alternativas de solución, así también como la topología de red de cada ambiente.

Solución SSSD

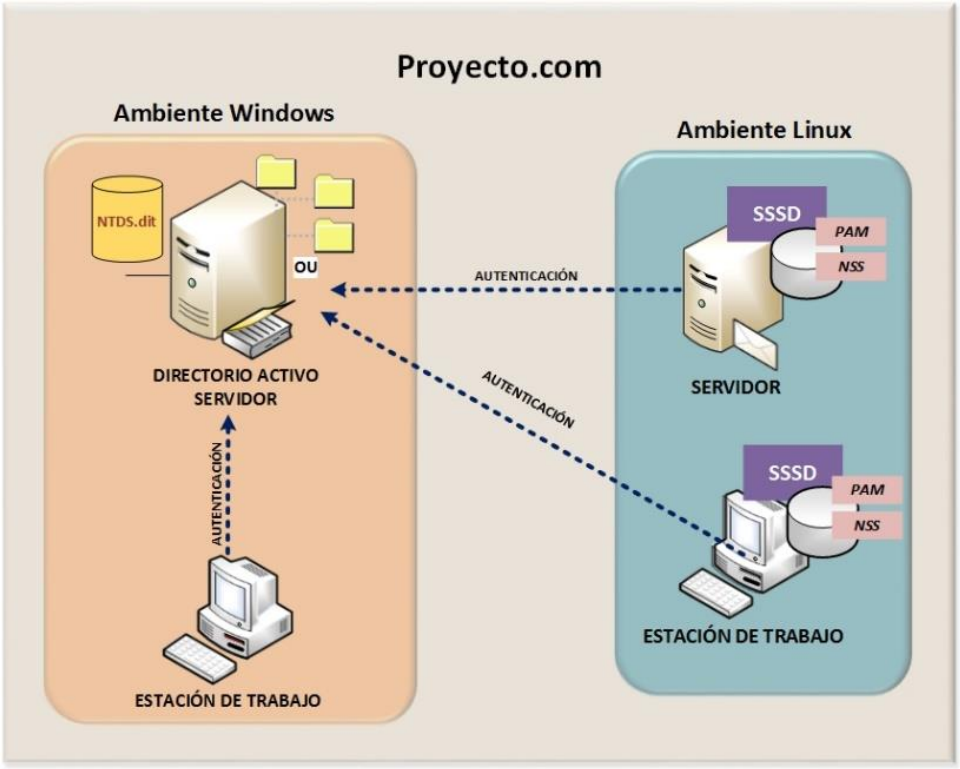


Figura 2.4. Solución SSSD

El diseño de solución de la Figura 2.4 se basa en la utilización de un controlador de dominio principal en Windows y el acceso de los clientes de la empresa al Directorio Activo, en las estaciones de trabajo clientes Linux se modificará los archivo de configuración relacionados con la solución SSSD, la cual cambia de manera transparente la información relacionada con PAM y NSS permitiendo la integración de dicho servidor con el servidor principal.

Solución utilizando Winbind

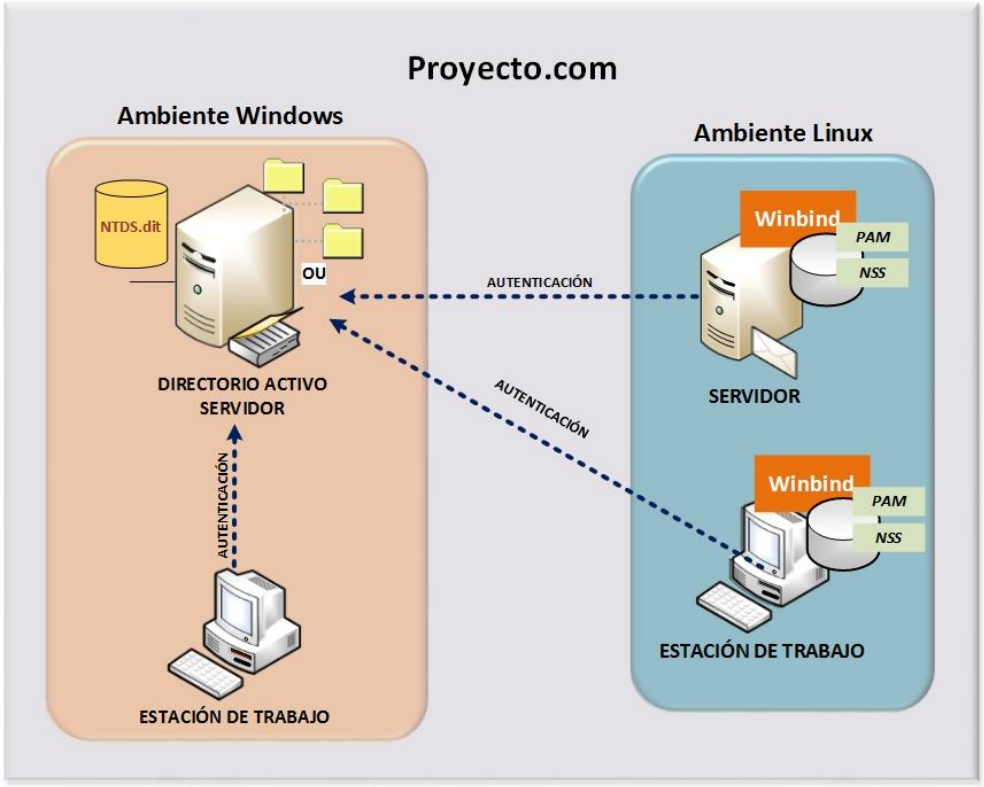


Figura 2.5. Solución Winbind

La Figura 2.5 establece como servidor principal al directorio activo de Windows con sus clientes; estaciones de trabajo Windows, servidores y estaciones de trabajo Linux, en este escenario la integración de la autenticación se produce por la presencia de Winbind que afecta a la configuración NSS y PAM.

Para la implementación de ambos escenarios se establece un direccionamiento IP el cual es detallado en las tabla 1, tabla 2 y tabla 3.

	Windows server 2012 R2	**Windows 8**
Dirección IP:	192.168.1.10	192.168.1.20
Máscara de Red:	255.255.255.0	
Puerta de Enlace:	192.168.1.10	
DNS primario:	192.168.1.10	

Tabla 1. Configuración de red en equipos Windows en ambos escenarios

	CentOS 7.0	**Ubuntu 14.04**
Dirección IP:	192.168.1.50	192.168.1.21
Máscara de Red:	255.255.255.0	
Puerta de Enlace:	192.168.1.10	
DNS primario:	192.168.1.10	

Tabla 2. Configuración de red de escenario SSSD

	CentOS 7.0	**Ubuntu 14.04**
Dirección IP:	192.168.1.150	192.168.1.101
Máscara de Red:	255.255.255.0	
Puerta de Enlace:	192.168.1.10	
DNS primario:	192.168.1.10	

Tabla 3. Configuración de red de escenario Winbind

En la tabla 4, se visualiza los nombres de las máquinas virtuales de cada escenario.

Nombre del dominio:	proyecto.com
Directorio Activo:	Serverad
Windows 8:	windows-cliente
Escenario SSSD	
Servidor CentOS:	centos-sssd
Estación de trabajo Ubuntu:	ubuntu-sssdd
Escenario Winbind	
Servidor CentOS:	centos-winb
Estación de trabajo Ubuntu:	Ubuntu-winbb

Tabla 4. Nombre de las máquinas

2.4. Análisis del software y equipos a utilizar

En esta sección se dará a conocer el equipo de cómputo y el programa virtualizador que se utilizó para la implementación del proyecto.

Cabe recalcar ciertos conceptos que se utilizan dentro de la virtualización, tales como:

- Sistema operativo anfitrión: Sistema operativo del computador, aquel donde está instalado el virtualizador.
- Sistema operativo invitado: Sistema operativo ejecutado dentro de una máquina virtual, creado mediante el virtualizador.
- Máquina virtual: es un entorno o ambiente de un sistema operativo invitado creado en el sistema operativo anfitrión a través del virtualizador.

Para la elección del virtualizador se compara a los dos software más utilizados para la virtualización en escritorios: VMware Workstation y Oracle VirtualBox.

Oracle VirtualBox:

VirtualBox es un software que permite la virtualización multiplataforma, en otras palabras puede crear máquinas virtuales o ejecutar múltiples sistemas operativos dentro de la máquina donde se encuentra instalado el virtualizador, su mayor ventaja es la licencia GLP Licencia Pública General, que es un licencia de código abierto y puede ser distribuida y modificada libremente sin costo alguno, además de ser un sistema portable, permite la virtualización de sistemas de 32 y 64 bits y es el más utilizado en ambientes de escritorio. [20]

VMware Workstation:

VMware al igual que VirtualBox es un software virtualizador multiplataforma, pero con costo de licenciamiento, permite la función “fácil instalación” en la cual reconoce el sistema a instalar y de manera automática realiza las configuraciones pertinentes para la ejecución de la máquina virtual.

VMware ofrece seguridad a nivel de hardware y al igual que VirtualBox permite detener o guardar el estado de una máquina virtual en ejecución, generalmente es usado a nivel empresarial y para la virtualización en servidores. [20] [21].

Se concluye utilizar el software Oracle VirtualBox debido al libre licenciamiento, portabilidad de los discos y preferencia de software por los conocimientos adquiridos con proyecto anteriores, dicho programa será utilizado para virtualizar a los sistemas operativos de las plataformas Linux y Windows.

Debido a que la virtualización consume los recursos del sistema y disminuye su rendimiento, la implementación de los escenarios con las alternativas de solución se llevó a cabo en un equipo de cómputo robusto pero económicamente accesible, por ello se utilizó una computadora del Laboratorio de Computación de la Facultad de Ingeniería en Electricidad y Computación.

Dicho virtualizador fue ejecutado en una estación de trabajo marca HP compaq Pro 6300, como se muestra en la Figura 2.6, con procesador Intel(R) Core (TM) i7-3770 CPU, memoria RAM de 8.00 GB y sistema operativo Windows 7 Professional

Figura 2.6 Equipo Intel Core i7 usado para los escenarios de prueba

2.5. Análisis de los sistemas operativos

Ambiente Windows

Para la implementación del proyecto, se decidió utilizar como controlador de dominio Windows Server 2012 R2 y como estación de trabajo Windows 8.

Windows Server 2012 R2: el motivo para la elección de este sistema operativo es porque es flexible y ágil, tiene como ventaja ofrecer servicios en la nube de escala global, esto quiere decir la consolidación de los servidores virtuales en un solo equipo físico. Proporciona una plataforma común para la integración, con el objetivo de automatizar tareas comunes a través de diversas herramientas como por ejemplo Windows PowerShell, además

permite la protección de la información al administrar una única identidad para cada cliente, en varias aplicaciones, tanto locales o basadas en la nube. [22]

Windows Server 2012 R2, define la información de acceso de todos los usuarios al sistema, por ejemplo, desde qué dispositivo y a qué información se accede, aplicando autenticación multifactor, además de proporcionar acceso remoto seguro a los trabajadores móviles por medio de Virtual Private Network (VPN) [22].

Este sistema operativo se define como una plataforma de categoría empresarial, ya que ofrece cinco veces más procesadores lógicos en relación a la memoria física que ofrece 4 veces más, y para las máquinas virtuales ofrece 16 veces más memoria para cada una.[22]

Windows 8: Ya que Windows es el sistema operativo más utilizado como estación de trabajo en las empresas por la compatibilidad que existe con las aplicaciones más utilizadas[23], se optó por implementar un cliente Windows 8 en cada escenario, cuyo principal motivo se debe a los convenios que tiene con muchas empresas multinacionales de varios sectores, como el caso de Hewlett-Packard Development Company, que vende computadoras con el sistemas operativo Windows preinstalado, el cual generalmente ofrece la última versión estable de la familia Windows [24], lo que proporciona facilidades a los clientes de obtener un equipo completamente funcional, así también como herramientas de mantenimiento, solución de problemas en línea mediante foros y centros de ayuda Microsoft [25].

Cabe mencionar que, debido al convenio existente de Microsoft con la Escuela Superior Politécnica del Litoral, a través de Dreamspark, se facilitó económicamente la adquisición de las imágenes ISO de los sistemas operativos Windows a utilizar.

Ambiente Linux

CentOS 7.0: Para la elección del servidor principal en Linux, se optó por los sistemas operativos de la compañía Red Hat, la cual es una empresa privada responsable de la creación de Red Hat Enterprise Linux (RHEL), Fedora y CentOS, esta empresa es conocida a nivel mundial en el desarrollo de software y soporte de varios sistemas operativos Linux, sin embargo el mayor inconveniente de implementar Red Hat en el proyecto, es que no permite la descarga directa de paquetes, servicios o ficheros, por lo tanto se tomó la decisión de utilizar la última versión gratuita y estable de RHEL, la cual es CentOS 7.0. [26] [27].

Reh Hat Enterprise Linux está considerada como una de las mejores distribuciones empresariales, ya fue creada para los centros de datos modernos, proporcionando flexibilidad, adaptabilidad y estabilidad, además de su fantástica evolución ya que primero empezó con un escenario de cliente-servidor y se ha transformado en un escenario móvil-nube. [26][27]

CentOS, es una distribución compilada a partir de las fuentes de RHEL, pero de código abierto, es decir es una distribución que permite la descarga de paquetes de manera directa, sin la necesidad de pagar por estos servicios, tiene como objetivo trabajar como un software de tipo empresarial sin costo alguno, ahorrando tiempo, energía y presupuesto. Además de ser un sistema operativo estable, robusto, fácil de utilizar e instalar [28] [29].

Ubuntu 14.04: Para la elección del sistema operativo en Linux como estación de trabajo se eligió Ubuntu 14.04, ya que provee una interfaz amigable, recomendado para los usuarios que van a dar los primeros pasos utilizando software libre, de manera que no se dificulte la interacción entre los usuarios y la máquina Linux [30], además de que el consumo de recursos disminuye mientras que la velocidad de procesamiento aumenta, esto convierte a este software en un sistema estable.

Como dato adicional estos sistemas operan adecuadamente sin el uso de un antivirus, debido a las constantes actualizaciones del sistema, que permiten las correcciones adecuadas en donde pueda ejecutarse un posible software

malicioso, además que el sistema es 100% configurable, es decir permite la modificación de escritorios, aplicaciones, fondos de pantallas, etc. [31]

Los sistemas operativos así como las características de las máquinas virtuales que se utilizaron para la implementación de proyecto se detallan en la Tabla 5:

Windows			
Cantidad	**Sistema Operativo**	**Tipo**	**Características**
1	Windows server 2012 R2	Servidor	1 GB memoria RAM 25GB de disco duro
1	Windows 8	Estación de trabajo	1 GB memoria RAM 25GB de disco duro
Linux			
Cantidad	**Sistema Operativo**	**Tipo**	**Características**
2	CentOS 7.0	Servidor	1 GB memoria RAM 25GB de disco duro
2	Ubuntu 14.04	Estación de trabajo	1 GB memoria RAM 25GB de disco duro

Tabla 5. Características de las máquinas virtuales

El proceso de las configuraciones básicas como configuración de red, y adicionales de los equipos Windows y Linux se detallan en el anexo A.

CAPÍTULO 3

3. IMPLEMENTACIÓN Y RESULTADOS

Una vez elaborados y definidos los diseños de los escenarios, se procede a la ejecución de la implementación, por lo que a lo largo de este capítulo se detallan las configuraciones adecuadas, las pruebas pertinentes y se elabora un análisis de costos.

3.1. Configuración de los sistemas operativos Windows y Linux

En esta sección se explicarán brevemente las configuraciones generales para cada servidor y estación de trabajo a utilizar, así también como las configuraciones adecuadas para cada escenario.

Configuraciones básicas

Son las configuraciones que se deberán realizar en cada servidor y estación de trabajo Linux y Windows. Comenzando con la configuración de las direcciones IP de acuerdo a las tablas 1, 2 y 3, estas configuraciones se detallan en el anexo A, para luego realizar la prueba de conectividad la cual se describe a continuación:

Prueba de conectividad

Prueba ejecutada entre los servidores y estaciones de trabajo Linux y Windows con Directorio Activo de Windows, de la siguiente manera:

ping 192.168.1.10 # colocar la dirección IP del Directorio Activo

El cual debe ser exitoso, luego se procede a la segunda prueba, en la cual se indicará si el equipo Linux logra resolver el nombre del Directorio Activo:

ping serverad.proyecto.com # colocar el nombre del Directorio Activo.

Si han existido inconvenientes en la prueba de conectividad, revisar la configuración de las direcciones IP del anexo A y el cable de acceso a la red, caso contrario realizar lo siguiente de acuerdo a cada plataforma:

Equipos Windows

Se debe cambiar el nombre del servidor del Directorio Activo para una mejor administración, posterior a ello se crean las cuentas de los usuarios en el dominio indicando nombre de usuario y contraseña, se recomienda que se asocien por grupos de acuerdo a departamentos, para mayor información sobre la configuración revisar el anexo A sección: configuraciones adicionales Windows.

Equipos Linux

Se debe instalar y configurar los equipos como clientes kerberos cuando se implemente la solución Winbind, modificando el archivo de configuración krb5.conf indicando la información pertinente del Directorio Activo, como se describe en el anexo A sección: configuraciones adicionales Linux.

Una vez realizada correctamente las configuraciones básicas, se procede a la ejecución de las implementaciones en cada escenario.

Escenario SSSD

Primero se procede a la instalación de los paquetes SSSD adecuados, así también como el demonio realm que será usado como un componente adicional para minimizar la cantidad de configuraciones.

Se utiliza realm para el descubrimiento del dominio del Directorio Activo.

Se realiza la solicitud de un boleto al servidor Kerberos mediante el comando kinit, para luego unir del equipo al dominio Windows, esta configuración se realiza a través de realm.

Se edita el archivo de configuración de SSSD, luego se reinicia el servicio y se realiza una comprobación del funcionamiento.

Esta configuración se detalla en el anexo B.

Escenario Winbind

Se ejecuta la instalación de los paquetes de samba adecuados, e inmediatamente se edita al archivo de configuración principal smb.conf, en el cual se indica el nombre del dominio, nombre de la máquina que alberga al Directorio Activo, nombre del grupo de trabajo, entre otros, no olvidar reiniciar el servicio.

Se edita el archivo nsswitch.conf, que determina el orden de búsqueda de las bases de datos del sistema [32] en el cual se debe indicar la utilización de los archivos de winbind.

Se solicita un boleto al servidor Kerberos mediante el comando kinit, y se finaliza con la unión del equipo al dominio Windows y comprobar su funcionamiento.

Esta configuración se detalla en el anexo C.

3.2. Prueba de funcionalidad

Para verificar el funcionamiento de la implementación en ambos escenarios, se realizaron cuatro pruebas:

1. Inicio de sesión por primera vez.
2. Inicio de sesión posterior al cambio de contraseña.
3. Inicio de sesión de acuerdo a permisos restringidos.
4. Permisos de administrador

Es decir tanto en el escenario de SSSD así como en el escenario de Winbind, se creó varios usuarios en el Directorio Activo de Windows separados en tres grupos de pruebas distribuidos equitativamente, simulando los departamentos de una empresa, la cantidad de usuarios se obtuvo del cálculo

mínimo de observaciones descrito en la siguiente sección “Análisis estadísticos de resultados”, dichos usuarios se autenticaron en la estación de trabajo Windows 8, en el servidor de CentOS y en la estación de trabajo de Ubuntu de cada escenario.

En ambos escenarios los equipos Linux fueron configurados para que creen de manera automática un directorio de usuario la primera vez que éste se autentica, dicha función viene habilitada de manera predeterminada en la estación de trabajo Windows.

Posterior a la autenticación, en el Directorio Activo de Windows se cambió la contraseña de los usuarios y se procedió a realizar una nueva autenticación en todos los equipos y en ambos escenarios, la cual se efectuó sin ningún inconveniente.

Como tercera prueba se realizó un procedimiento en la que el Directorio Activo de Windows restringió el acceso de los usuarios del domino a los equipos Windows a través de grupos acorde a departamentos o funciones, y como prueba final se le otorgó privilegios de Administrador a ciertos grupos, cabe mencionar que en ambas pruebas los equipos Linux fueron configurados de manera diferente e independiente para que realicen la misma función, definiendo un único o varios grupos de usuario que pueden acceder a ciertos equipos y otorgando privilegios a ciertos usuarios para que puedan cambiar la configuración de cada uno de los dispositivos Linux, y al igual que las otras pruebas anteriores ambas se ejecutaron adecuadamente, dando por resultado una implementación exitosa.

La configuración de la primera prueba de inicio de sesión se detalla en el anexo B y C, la segunda prueba se especifica en el anexo A en la sección “Configuraciones adicionales de Windows”, la tercera prueba y cuarta prueba se describen en el anexo A “Configuraciones adicionales Linux”.

3.3. Análisis estadístico de resultados

Se procedió a la realización de un análisis estadístico de los resultados una vez que la implementación haya sido exitosa, para lo cual se calcula el número mínimo de observaciones necesarias para considerar al proyecto óptimo, dicho análisis se realizará a partir de los resultados obtenidos mediante la ecuación 3.1.

$$n = \frac{(W - W^2)\,[Z_\beta + 1.4\,(Z_\alpha)]^2}{W^2} \tag{3.1}$$

Siendo n el número de observaciones mínimas, Z_β poder estadístico y Z_α nivel de confianza establecido y W el mínimo rendimiento esperado. [33]

Nivel de confianza:

Se decide tomar 99% de confiabilidad, y de acuerdo a la siguiente tabla obtener un valor de: 2.576

NIVEL DE CONFIANZA (1-α)		
A	**%**	**Z_α**
0,050	95,0	1,960
0,025	97,5	2,240
0,010	99,0	2,576

Tabla 6. Valores de Zα para diferentes niveles de confianza

Nivel de poder estadístico:

Se decide tomar 85% de poder estadístico, y de acuerdo a la siguiente tabla obtener un valor de: 1.036

PODER ESTADISTICO (1-β)		
B	**%**	**Z_β**
0,20	80,0	0,842
0,15	85,0	1,036
0,10	90,0	1,282

Tabla 7. Valores de Zβ para diferentes niveles de poder estadístico

Por lo que para calcular el mínimo número de observaciones se reemplaza en la fórmula 4.1 los siguientes valores:

$\mathbf{Z_{\alpha}}$ = 2,576

$\mathbf{Z_{\beta}}$ = 1.036

W = 0,80

$$n = \frac{(0{,}80 - 0{,}80^2)\,[1.036 + 1.4\,(2{,}576)]^2}{0{,}80^2} = 5{,}38 = 6$$

El mínimo número de observaciones para cada escenario deberá ser de 6.

Por lo tanto se procede a la realización de las pruebas de funcionalidad como se describe en el subcapítulo 3.2, con lo cual se obtiene un resultado exitoso o fallido en la autenticación de los usuarios, que son detallados en la tabla 8.

Pruebas	**Escenarios**		
	Windows	**SSSD**	**Winbind**
Primer inicio de sesión	Éxito	Éxito	Éxito
Cambio de contraseña	Éxito	Éxito	Éxito
Acceso restringido	Éxito	Éxito	Éxito
Permiso de administrador	Éxito	Éxito	Éxito

Tabla 8. Resultado de pruebas exitosas o fallidas

Luego de obtener el número mínimo de observaciones se procede a la aplicación de la estadística descriptiva, tomando los resultados exitosos para la aprobación del proyecto.

Media	6
Desviación estándar	0
Varianza de la muestra	0
Mínimo	6
Máximo	6

Tabla 9. Resultados de estadística descriptiva

Podemos concluir que los resultados fueron exitosos ya que la media mostró un dato favorable, sin embargo cabe recalcar que debido a que es un escenario de prueba los resultados obtenidos son ideales, los cuales varía en un ambiente real.

3.4. Análisis de las pruebas e implementaciones

Se determinan las principales características de las soluciones SSSD y Winbind basándose en las pruebas ejecutadas de las implementaciones, así también como la recopilación de información detalla de cada una de ellas en el capítulo 3.

La principal característica de SSSD es la incompatibilidad con el protocolo NTLM en caso de utilizar un Directorio Activo que maneje dicho protocolo, al contrario de Winbind que es compatible tanto con NTLM y LDAP.

Samba/Winbind proporciona servicios de acceso de inicio de sesión y compartición de archivos, a diferencia de SSSD que solo permite el acceso de inicio de sesión.

SSSD facilita el acceso a diferentes identidades tales como Directorio Activo de Windows, IdM de Red Hat, LDAP nativo u otros, cabe mencionar que SSSD y Winbind puede trabajar en conjunto, siendo la configuración SSSD es de menor complejidad y una solución actualizada.

Ya que las pruebas fueron exitosas en ambos escenarios se demuestra que ambos mecanismos son viables para resolver la integración del servicio de autenticación de las plataformas, sin embargo hay que tener presente que pueden existir inconvenientes posteriores al ejecutarse en un ambiente real.

3.5. Inconvenientes presentados en las configuraciones

Se presentaron varios inconvenientes en el inicio de sesión de la estación de trabajo Ubuntu, que involucran la creación de directorios de manera automática la primera vez que se inicia sesión, y la presencia de la cuenta

invitado en la interfaz gráfica que prohíbe el inicio de sesión de un usuario que no haya sido creado en el computador, así también existió un inconveniente en los servidores CentOS, debido a que la interfaz de red no iniciaba de manera automática por lo que no permitía el inicio de sesión de los usuarios.

El primer problema pudo ser resuelto al agregar el módulo PAM llamado pam_mkhomedir en el archivo /etc/pam.d/common-session, y el segundo percance se solucionó al crear el archivo lightdm.conf en el cual se debe deshabilitar la cuenta invitado y permitir inicio de sesión de manera manual, el inconveniente presentado en los servidores CentOS se resolvió con la edición del archivo de configuración de la interfaz de red, de manera que se inicie cada vez que se enciende el servidor, estas configuraciones se detallan en el anexo D.

3.6. Análisis de Costos

El costo del proyecto se basa únicamente en el servicio de configuración necesaria para la implementación, el cual es proporcional al número de servidores involucrados en el proyecto, número de usuarios de la empresa y el precio medio utilizado por los competidores directos en el mercado. Para obtener dicho valor se llevó a cabo una serie de cotizaciones a empresas que ofertan servicios similares como se visualiza en la tabla N°10.

Empresa	**Valor del servicio**
Servicom	$300.00+iva
Serconnet	$900.00+iva
Pc Ecuador	$750,00 +iva
Jsgm Easy – Tec	$585,00+iva
64bits	$500.00+iva
Sync	$600.00+iva
Palosanto	$750.00+iva
Dinamoconsulting	$820.00+iva

It Soluciones Ecuador	$400.00+iva
Its Ecuador	$600.00+iva
E-open Solutions Ltda.	$540.00+iva
Ecualinux NodoVIP	$580.00+iva
Innova services	$720.00+iva
Troncal net	$790.00+iva

Tabla 10. Cotización a empresas

Se cotizó en base a los escenarios de las implementaciones, compuesto por dos servidores principales, un servidor Windows y otro servidor Linux y un aproximado de 75 usuarios, cuyo requerimiento principal es la integración de estas plataformas.

Se elabora una tabla de barras visible en la figura 3.1 cuyo valor promedio se considera como un valor ideal para ofertar en la solución de la problemática, el cual es obtenido realizando la sumatoria de todos los valores que ofrecen las distintas empresas, dividido para el número de empresas que se contactó para el análisis de la cotización, siendo aproximadamente $570+IVA el costo del servicio, incluyendo transporte de los técnicos y otros.

Sin embargo este valor puede varía por la cantidad de servidores o estaciones de trabajo a configurar y el tiempo requerido para dicho proyecto, para lo cual se elabora un plan de trabajo básico que detalla las actividades esenciales del proyecto, el cual puede ser visualizado en el anexo E.

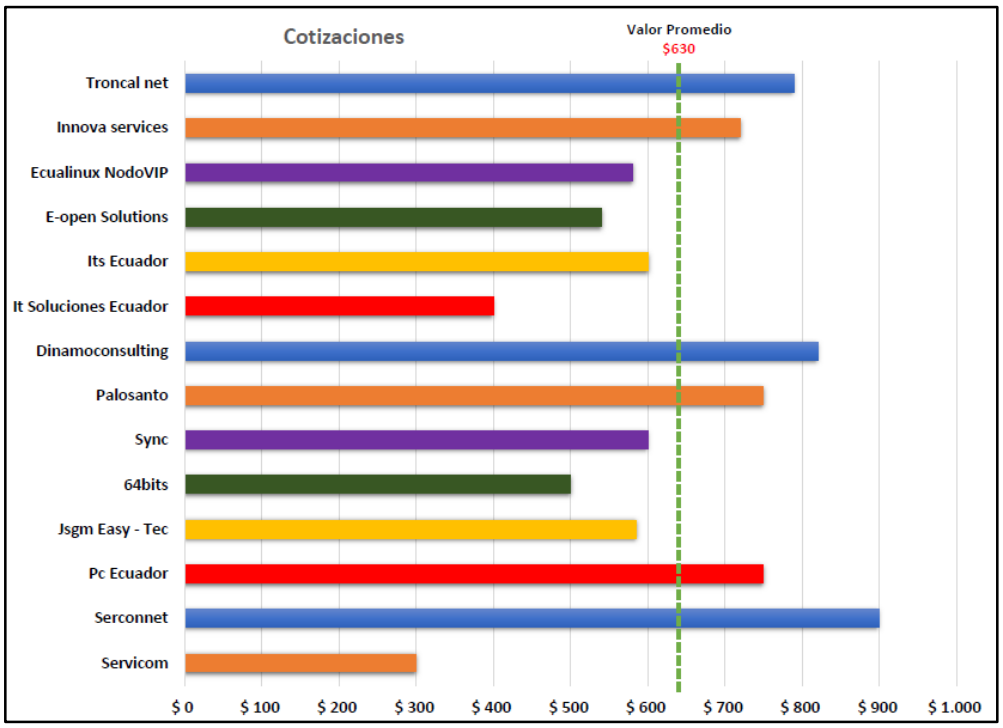


Figura 3.1. Valor del proyecto por empresa

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. La mayoría de fallas en la seguridad informática a menudo están relacionadas con el acceso de los usuarios al sistema, por lo que la solución propuesta beneficia al control de la autenticación de los clientes.
2. Se logra minimizar la cantidad de errores por medio de la ejecución del demonio realmd, que facilita la configuración de las alternativas SSSD o Winbind.
3. La implementación de la solución SSSD a pesar de ser relativamente nueva permite tener una menor cantidad de archivos de configuración y un menor tiempo de ejecución, además de poseer mayor flexibilidad en comparación con Winbind.

Recomendaciones

1. La solución por medio de la integración directa es ideal en ambientes pequeños o medianos.
2. Si se ha implementado la autenticación mediante Winbind se recomienda mantener la configuración, ya que la migración a la autenticación SSSD significa un considerable gasto económico y de esfuerzo.
3. Se puede integrar el servicio de autenticación SSSD y el servicio para compartir archivos de la suite samba, siempre y cuando SSSD haya sido configurado previamente.
4. Se podría integrar en otra fase de implementación servicios de autenticación en otros equipos como impresoras e inclusive servicios de correo, base de datos u otros.

BIBLIOGRAFÍA

[1] Correa Delgado Rafael. (2008, Abril) Uso de estándares abiertos y software libre [Online]. Disponible en: http://www.administracionpublica.gob.ec/wp-content/uploads/downloads/2014/06/DecretoEjecutivo1014.pdf

[2] Wikipedia. (2015, Agosto 19) Servicio de directorio. [Online]. Disponible en: https://es.wikipedia.org/wiki/Servicio_de_directorio

[3] RedHat. (2014, Mayo) Discover an open source world, [Online]. Disponible en: http://opensource.com/business/14/5/top-4-open-source-LDAP-implementations

[4] JumpClud,(2015, Enero) LDAP vs Active Directory vs JumpCloud, [Online]. Disponible en: https://jumpcloud.com/blog/LDAP-vs-active-directory/

[5] Heslin Mark, Integrating Red Hat Enterprise Linux 6 with Active Directory, versión 1.5, marzo 2014.

[6] Oracle (2011, Mayo) Servicios de autenticación. [Online]. Disponible en: http://docs.oracle.com/cd/E24842_01/html/E23286/secov-5.html

[7] Ghudson (2015, Julio). Kerberos: The Network Authentication Protocol. [Online]. Disponible en: http://web.mit.edu/kerberos/

[8] Microsoft, (2010, Enero) .Autenticación Kerberos V5, [Online]. Disponible en: https://msdn.microsoft.com/es-es/library/cc783708(v=ws.10).aspx

[9] Red Hat Enterprise Linux 4: Manual de referencia, Capítulo 19. Kerberos, edición 6, 2010.

[10] Rouse Margaret, (2015, Junio). Integration Definition, [Online]. Disponible en: http://searchcrm.techtarget.com/definition/integration

[11] Pal Dmitri, (2015, Enero). Aspect of Integration, [Online].Disponible en: http://rhelblog.redhat.com/2015/01/28/aspects-of-integration/

[12] Pal Dmitri, (2015, Mayo) Direct, or Indirect, that is the question. [Online]. Disponible en: http://rhelblog.redhat.com/2015/05/27/direct-or-indirect-that-is-the-question/

[13] Linuxman page, (2013, Mayo).SSSD, [Online]. Disponible en: http://linux.die.net/man/8/sssd

[14] Potter Tim, (2011, Junio). Manual de referencia, capítulo 21. Winbind: Uso de cuentas de Dominio, [Online]. Disponible en: http://www.bdat.net/documentos/samba/html/winbind.html

[15] Oracle (2011, Mayo). Cómo funciona el servicio Kerberos [Online]. Disponible en: http://docs.oracle.com/cd/E24842_01/html/E23286/intro-25.html

[16] Oracle (2011, Mayo). Cómo funciona el sistema de autenticación Kerberos [Online]. Disponible en: Http://docs.oracle.com/cd/E24842_01/html/E23286/refer-14.html

[17] Fedoram (2010, Mayo) Features/SSSD [Online]. Disponible en: https://fedoraproject.org/wiki/Features/SSSD

[18] Desde Linux (2013, Agosto). Red SWL (IV): Ubuntu Precise y clearos, Autenticación SSSD contra LDAP nativo, [Online]. Disponible en: http://blog.desdelinux.net/red-swl-iv-ubuntu-precise-y-clearos-autenticacion-sssd-contra-ldap-nativo/

[19] RedHat, Guía de Planificación de Migración - SSSD, edición 6, 2010.

[20] Storagecraf recovery zone,(2013, Julio) Battle of Free Virtualization Tools: VMware vs. VirtualBox, [Online]. Disponible en: http://www.storagecraft.com/blog/battle-of-free-virtualization-tools-vmware-vs-virtualbox/

[21] vmWare (2015, Mayo) Virtualización, [Online]. Disponible en: https://www.vmware.com/latam/virtualization/how-it-works

[22] Microsoft (2015, Mayo) Windows Server 2012 R2 - Características, [Online]. Disponible en: http://www.microsoft.com/es-xl/server-cloud/products/windows-server-2012-r2/Features.aspx

[23] Contreras Manu, (2015, Abril), Windows XP aún sigue siendo más usado que Windows 8.1, [Online]. Disponible en: https://www.fayerwayer.com/2015/04/windows-xp-aun-sigue-siendo-mas-usado-que-windows-8-1/

[24] Noel, (2014, Abril) ¿Windows es el sistema operativo más usado? ¿Tiene rivales? [Online]. Disponible en: http://lignux.com/windows-es-el-sistema-operativo-mas-usado-tiene-rivales/, fecha de publicación abril 2014

[25] Kupper Victor (2011, Noviembre). Porque Windows es el Sistema más usado, [Online]. Disponible en: http://ec.globedia.com/windows-sistema-usado

[26] Bhartiya Swapnil (2015, Febrero). The top 11 best Linux distros for 2015, [Online]. Disponible en: http://www.linux.com/news/software/applications/810295-the-top-11-best-linux-distros-for-2015

[27] Singh Karanbir (2014, Enero). CentOS Project joins forces with Red Hat, [Online]. Disponible en: http://lists.centos.org/pipermail/centos-announce/2014-January/020100.html

[28] CentOS (2015, Enero). CentOS Linux, [Online]. Disponible en: http://www.centos.org/about/

[29] Red Hat (2013, Mayo). Una plataforma de próxima generación, creada para los centros de datos modernos, [Online]. Disponible en: http://www.redhat.com/es/technologies/linux-platforms/enterprise-linux,

[30] DesdeLinux,(2015, Agosto). UBUNTU14.04: Breve reseña sobre su rendimiento, consumo, apariencia y usabilidad, [Online]. Disponible en: http://blog.desdelinux.net/ubuntu-14-04-breve-resena/

[31] Setfree Luis,(2014, Enero). Ventajas de Ubuntu, [Online]. Disponible en: http://tech.batanga.com/13080/ventajas-de-ubuntu

[32] Oracle, (2010, Mayo). Archivo nsswitch.conf, [Online]. Disponible en: https://docs.oracle.com/cd/E19957-01/820-2981/6nei0r174/index.html

[33] Lumbreras Vicente, “Determinación del número mínimo de observaciones en investigación, obviando las estimaciones de la varianza de datos” en Revista Didáctica Ambiental, pp. 64 -51, fecha de publicación diciembre 2011.

[34] Prieto José Manuel, (2014, Diciembre). LINUX AND WINDOWS INTEGRATION. [Online]. Disponible en: http://blog.qosit.eu/linux-windows-integration/

[35] TechNet, (2013, Agosto). Guía paso a paso para configurar el controlador de dominio de Windows Server 2012 (es-ES), [Online]. Disponible en: http://social.technet.microsoft.com/wiki/contents/articles/19495.guia-paso-a-paso-para-configurar-el-controlador-de-dominio-de-windows-server-2012-es-es.aspx.

[36] Server World, (2014, Diciembre) Join in Windows Active Directory, [Online]. Disponible en: http://www.server-world.info/en/note?os=CentOS_7&p=realmd

[37] El tipo de informática, (2010, Febrero). Instalación de Samba en Centos y Conexión con Active Directory (Parte 2), [Online]. Disponible en: http://www.eltipodeinformatica.com/2010/02/instalacion-de-samba-en-centos-y.html

[38] Unixmen, (2015, Junio). How to Join an Ubuntu Desktop into an Active Directory Domain, [Online]. Disponible en: http://www.unixmen.com/how-to-join-an-ubuntu-desktop-into-an-active-directory-domain/

[39] Petersen Richard, Red Hat Enterprise Linux 6: Desktop and Administration, 1º edición, 2011.

[40] Wiley Jhon, Red Hat Enterprise Linux 6 Administration, 1º edition, Real World Skills for Red Hat Administrators, 2013.

[41] Negus Christopher, Linux Bible, 9º edición, fecha de publicación abril 2015.

[42] Panek William, MCSA Windows Server 2012 R2 Administration Study Guide, 1º edición, marzo 2015

Petersen Richard, Red Hat Enterprise Linux 6: Desktop Administration, 4º edición, febrero 2011.

[43] Sysadmin, (2012, Febrero). CentOS 6 network: sin red después de instalar, [Online]. Disponible en: http://www.aradaen.com/sysadmin/centos-6-network-sin-red-despues-de-instalar/

[44] Dmitri Pal, (2015, Febrero) Overview of Direct Integration Options [Online]. Disponible en: http://rhelblog.redhat.com/2015/02/04/overview-of-direct-integration-options/

[45] Der Flounder, (2014, Diciembre) Adding AD domain groups to /etc/sudoers, [Online]. Disponible en: https://derflounder.wordpress.com/2012/12/14/adding-ad-domain-groups-to-etcsudoers/

[46] Ubuntu Documentation, (2015, Agosto) SSSD and Active Directory, [Online]. Disponible en: https://help.ubuntu.com/lts/serverguide/sssd-ad.html

[47] HumanOS, (2010, Noviembre). [¿Cómo se hace?] Restringir acceso de usuarios a tu PC en GNU/Linux, [Online]. Disponible en: https://humanos.uci.cu/2010/11/%C2%BFcomo-se-hace-restringir-acceso-de-usuarios-a-tu-pc-en-gnulinux/

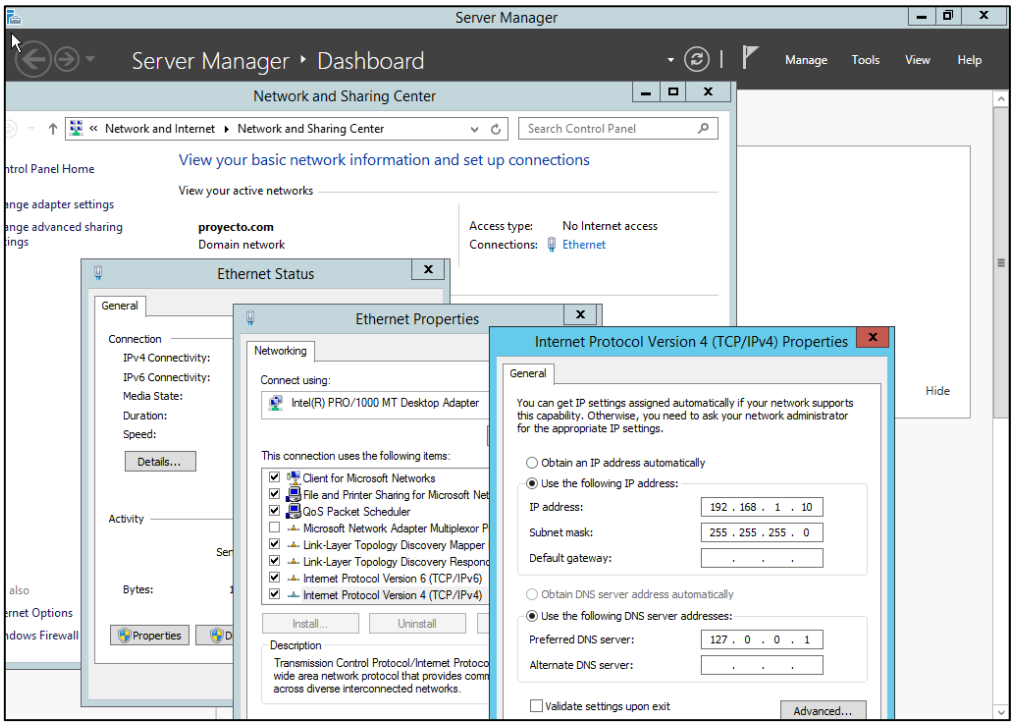
ANEXOS

A: Configuración básicas

Configuraciones de red

- **Windows server 2012 R2**

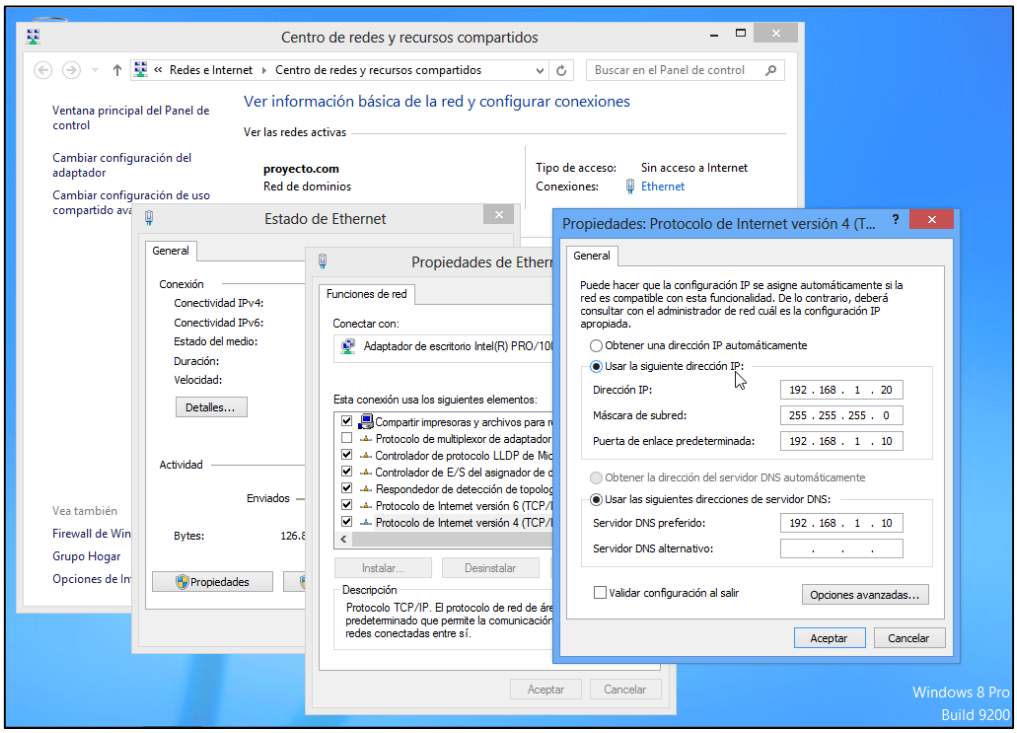
  Para realizar la configuración de red en el servidor principal, se lo realiza con la siguiente ruta: configuración/panel de control/redes e internet/centro de redes y recursos compartidos/conexión de área local o Ethernet/propiedades/protocolo de internet versión 4 (TCP/IPV4)/propiedades/general/utilizar dirección IP estática, se puede visualizar en la siguiente imagen:



- **Windows 8**

  La configuración de red de la máquina de escritorio en Windows 8.0 se lo realiza con la siguiente ruta: configuración/panel de control/redes e internet/centro de redes y recursos compartidos/conexión de área

local/propiedades/ protocolo de internet versión 4 (TCP/IPV4)/propiedades/general/utilizar dirección IP estática, se puede visualizar en la siguiente imagen:



- **CentOS 7.0**

La configuración de red en los servidores de CentOS 7.0 se lo realizó utilizando los siguientes comandos:

nano /etc/sysconfig/network-scripts/ifcfg-enp0s3

BOOTPROTO="static"

IPADDR="192.168.1.50"

NETMASK="255.255.255.0"

DNS= 192.168.1.10

GATEWAY=192.168.1.10

Reiniciar el servicio

#services network restart

- **Ubuntu 14.04**

  La configuración de red en la máquina se la realizó utilizando los siguientes comandos:

  Archivo de configuración de la interfaz

  $ sudo nano /etc/network/interfaces

  ```
  iface eth1 inet static
  address 192.168.1.101
  netmask 255.255.255.0
  gateway 192.168.1.10
  ```

  Agregar el DNS

  $ sudo nano /etc/resolv.conf

  ```
  Nameserver 192.168.1.10
  ```

  Reiniciar el servicio

  $ sudo /etc/init.d/networking restart

Configuraciones adicionales Windows

- **Windows server 2012 R2**

  Para llevar a cabo la integración de las plataformas se debe realizar las siguientes configuraciones que incluye la instalación del Directorio Activo, la creación de las cuentas de usuarios y su cambio de contraseña, además la elaboración de políticas básicas para una adecuada gestión.

  Configuración del Directorio Activo [42]

  1. Cambiar el nombre de la máquina, este paso es opcional, pero es aconsejable modificarlo para una mejor administración.
  2. Agregar el rol del directorio activo de Windows, en el “Server Manager”, en el icono “Manage”, escoger la opción “Add Roles and Features Wizard”
  3. Escoger el tipo de instalación “Role-based or features-based installation” lo cual indica que es una instalación basada en roles o en funciones

4. Seleccionar el servidor, de manera predeterminada se selecciona el servidor creado, esto se lo hace marcado la opción de “Select a server from ther server pool”, que indica seleccionar un servidor desde el pool de servidores
5. Marcar en la opción de “Server Roles” “Active Directory Domain Services”, El Directorio Activo instala de manera predeterminada DNS y kerberos, sin embargo esta configuración puede ser modificada.
6. Para finalizar se confirma los roles que se decidió instalar, se da clic en la opción de “Restart the destination server automatically if requiered” y para culminar la instalación clic en instalar

Se puede verificar el funcionamiento como controlador de dominio al realizar la autenticación después de reiniciado el sistema. [35]

Creación de cuentas de usuario [50]

Para la creación de cuentas de usuario en el controlador de dominio Windows se realiza lo siguiente:

1. Acceder a la herramienta “Active Directory Users and Computers” en la ruta Server Manager/Tools
2. En la unidad organizativa “Cuentas” crear los usuarios que necesarios para la implementación, dando clic derecho “New User”. Se recomienda la creación de la unidad organizativa para una mejor administración.
3. Detallar información del usuario como nombres, apellidos y el nombre de inicio de sesión del usuario, dar clic en siguiente, agregar la contraseña para el usuario u dar clic en finalizar. Dicho usuario deberá ser agregado a un grupo para una correcta gestión de las políticas.

Para distinguir el inicio de sesión de ambas implementaciones, se configuró para que los equipos Linux que usan SSSD permitan el inicio de sesión únicamente por el nombre de la cuenta de usuario, quedando de la siguiente manera:

Escenario SSSD: javiles #nombre de la cuenta de usuario

Escenario Winbind: proyecto\javiles #nombre de la cuenta de usuario.

Cambio de contraseña de las cuentas de usuario

Una vez creada y autenticada por primera vez la cuenta de usuario, se realiza la segunda prueba de funcionamiento relacionada al cambio de contraseña que se lleva a cabo de la siguiente manera:

1. Acceder a la herramienta “Active Directory Users and Computers” en la ruta Server Manager/Tools
2. Dar clic en la unidad organizativa “Cuentas”, que muestra las cuentas y grupos creadas del dominio.
3. Dar clic derecho sobre la cuenta del usuario y seleccionar Reset Password
4. Colocar la nueva contraseña y quitar el visto de la opción “User must change password at next logon” en caso de querer que la contraseña se habilite instantáneamente, clic en OK. Se puede colocar una contraseña nueva y dejar habilitada la opción “User must change password at next logon” para cuando el usuario desee acceder a su equipo pueda realizar el cambio de contraseña.

Las siguientes configuraciones forman parte de la tercera prueba de funcionamiento de un escenario exclusivamente Windows, puesta en marcha mediante la creación de políticas en la consola “Group Policy Management” que permitirá otorgar permisos privilegiados a usuarios del dominio y restringir el acceso de inicio de sesión de los usuarios a los equipos Windows.

Restringir acceso a usuarios del dominio

Se desea restringir el inicio de sesión a los usuarios que no pertenezcan al departamento permitiendo la autenticación solo a los usuarios del departamento y del equipo de soporte técnico, por ende la opción óptima sería permitir únicamente el acceso de ciertos usuarios ya que los demás usuarios están implícitamente bloqueados.

1. Acceder a la consola” Group Policy Management” en el Directorio Activo de Windows.

2. Crear una nueva política seleccionando la unidad organizativa a la cual se la va a aplicar.
3. Clic derecho sobre la política seleccionando “Edit”.
4. Esta política se aplica a nivel de computador, accediendo en la sección “User Rights Management”, en la opción “Allow log on locally”, mediante la ruta: Computer Configuration/Windows Settings/Security Settings/Local Policies/
5. Doble clic en la opción “Allow log on locally”, en ella se coloca a los usuarios y grupos que pueden acceder a los equipos, cli en ok.
6. Se puede comprobar su funcionamiento mediante el inicio de sesión.

Conceder privilegios a usuarios del dominio

Se permitirá a ciertos usuarios del dominio tener privilegios de administrador en cada equipo Windows de la empresa, lo cual será configurado de manera global en el Directorio Activo, evitando la configuración manual.

1. Acceder a la consola” Group Policy Management” en el Directorio Activo de Windows.
2. Debido a que solo el grupo “Tecnicos” tendrá privilegios para modificar las configuraciones en todos los equipos Windows, imaginando que la empresa es local y sin sucursal alguna, se procede a crear una nueva “GPO” o política al nivel del dominio, cuyo nombre será “Permisos-tecnicos”. Esta política funcionará en todos los equipos Windows indistintamente de la unidad organizativa que en la que esté ubicada.
3. Clic derecho sobre la política, seleccionando la opción “Edit”
4. Esta política se aplica a nivel de computador, en la sección “Restricted Groups” accediendo a la ruta: Computer Configuration/Windows Settings/Security Settings/Restricted Groups
5. Clic derecho Add Group, clic en Browse
6. Escribir el nombre de grupo “Tecnicos”, clic en chrck names, clic ok

7. Se abre una nueva ventana, seleccionar Add en la sección “This group is a member of” y escribir el nombre del grupo “Administrators”, clic en ok, clic en ok.
8. Para forzar la actualización de la política escribir en la consola del Windows server: gpupdate /force.
9. Se puede comprobar su funcionamiento en los clientes ejecutando la consola de Windows como Administrador, la cual no deberá de requerir ninguna contraseña adicional.

- **Windows 8**

  Unión de equipo al dominio

  Se debe realizar este procedimiento en cada uno de los equipos Windows, cuyos pasos son similares indiferentemente de la versión:

  1. Cambiar el nombre a la máquina, para tener una mejor administración del equipo
  2. Acceder a la configuración de equipo, Panel de control/ Todos los elementos de Panel de control/ Sistema/ Cambiar de configuración/ Propiedades del Sistema/
  3. Clic en la opción cambiar y en la opción de miembro del y se debe escoger la opción de Dominio.
  4. Al reiniciar la máquina se debe autenticar con usuario y contraseña de los clientes del directorio activo.

Configuraciones adicionales Linux

- **Instalación y configuración del cliente Kerberos [46]:**

  Este procedimiento se debe realizar previo a la configuración del escenario Winbind, debido a que en el escenario SSSD, realmd configura el archivo de manera automática.

1. Instalar el paquete de cliente kerberos como se muestra a continuación:

   Centos: yum -y install krb5-workstation

   Ubuntu: sudo apt-get install krb5-user

2. Modificar archivo de configuración de kerberos /etc/krb5.conf para que se muestre de la siguiente manera:

```
[libdefaults]
        default_realm = PROYECTO.COM
        ticket_lifetime = 24h
        renew_lifetime = 7d
[realms]
        PROYECTO.COM= {
        kdc = serverad.proyecto.com
        }
[domain_realm]
        .proyecto.com = PROYECTO.COM
        proyecto.com = PROYECTO.COM
```

Las siguientes configuraciones forman parte de la tercera prueba de funcionamiento, realizadas después de la integración mediante SSSD o Winbind descritas en el anexo C y D respectivamente, en la que se otorga permisos privilegiados a usuarios del dominio y se restringe el acceso de inicio de sesión a los equipos.

Conceder privilegios a usuarios de dominio [45]:

Esta configuración permitirá que ciertos usuarios del dominio tengan privilegios para modificar la configuración de los equipos Linux teniendo la misma libertad que un usuario “root”.

Acceder como usuario “root” y modificar el archivo sudoers de la siguiente manera:

```
#visudo
%PROYECTO\\Tecnicos          ALL= (ALL)     ALL
```

Tecnicos es un grupo de usuarios creados en el dominio que debe tener acceso para modificar la configuración de los equipos Linux y Windows.

Restringir acceso a usuarios del dominio: [47]

Para restringir el acceso a los usuarios del dominio en los equipos Linux se llevó a cabo la siguiente configuración que es similar en la mayoría de las distribuciones pero con ciertas variaciones.

1. Editar el archivo /etc/system/access
   + : root (Tecnicos): ALL
   - : ALL : ALL
2. Colocar “account required pam_access.so” en los siguientes archivos:
   CentOS:
   /etc/pam.d/system-auth al final de la sección “account”
   /etc/pam.d/gdm-password al final de la seccion account
   Ubuntu:
   /etc/pam.d/common-session al inicio del archivo

B: Configuración SSSD

En este anexo se detallan las configuraciones de la solución SSSD tanto en el servidor como estación de trabajo Linux [36] [39]:

Servidor CentOS y estación de trabajo de Ubuntu:

1. Instalación de paquetes SSSD pertinentes:

   Centos: yum -y install realmd sssd oddjob-mkhomedir samba-common adcli
   Ubuntu: sudo apt-get install realmd sssd sssd-tools samba-common samba-libs adcli

2. Descubrir el dominio del Directorio Activo mediante realm, el configurará al equipo como cliente SSSD de manera automática.

   realm discover serverad.proyecto.com

3. Solicitar el boleto al servidor kerberos:

   #kinit Administrator@proyecto.com

4. Unirse al dominio del Directorio Activo

   realm join proyecto.com

5. Editar archivo de configuración sssd.conf, para que permita el ingreso por el nombre de usuario, este paso es opcional:

   use_fully_qualified_names = False

6. Reiniciar el servicio sssd.

   CentOS: systemctl restart sssd
   Ubuntu: sudo service sssd restart

7. Comprobar el funcionamiento

   id mperalta #usuario del dominio

C: Configuración Winbind

En este anexo se detallan las configuraciones de la solución Winbind tanto en el servidor como estación de trabajo Linux [37] [40]:

Servidor CentOS y estación de trabajo Ubuntu:

1. Como primer paso, instalar todos los paquetes relacionados con Winbind:

   Centos: yum -y samba-common samba-winbind samba-winbind-clients
   Ubuntu: sudo apt-get install winbind samba libpam-winbind libnss-winbind

2. Editar el archivo de configuración smb.conf en la ruta /etc/samba, en este archivo se indican el grupo de trabajo que en este caso es el nombre del dominio, así también como el nombre de la máquina que contiene el Directorio Activo e indicar el tipo de seguridad a usar, que debe ser ads que es la seguridad del Directorio Activo, quedando de la siguiente manera:

   ```
   [global]
     workgroup = PROYECTO
     password server = serverad.proyecto.com
     realm = PROYECTO.COM
     security = ads
     template shell = /bin/bash
     winbind use default domain = false
     winbind offline login = false
   ```

3. Se Inicia los servicios de samba y winbind, ejecutando:

   # smbd restart
   # nmbd restart
   # winbindd restart

4. Agregar y modificar archivo de configuración /etc/nsswitch.conf, quedando de la siguiente manera:

#nano /etc/nsswitch.conf

passwd: files winbind

shadow: files winbind

group: files winbind

5. Se debe solicitar boleto al servidor Kerberos, proporcionando las credenciales de usuario administrador del controlador de dominio:

   #kinit Administrator@proyecto.com

6. Para confirmar que la obtención del ticket es exitoso se escribe:

   #klist

7. Se agrega la máquina al dominio ejecutando los comandos:

   #net ads join proyecto.com -U administrator
   Enter administrator's password:
   Using short domain name -- PROYECTO
   Joined 'Centos-Winbind' to realm 'proyecto.com'

D: Solución de inconvenientes presentados

Estaciones de trabajo Ubuntu [38] [41]**:**

- Crear de manera automática los directorios para los nuevos usuarios del dominio: Agregar la siguiente línea en el archivo de configuración ubicado en /etc/pam.d/common_session:

  session required pam_mkhomedir.so skel=/etc/skel/ umask=0077

- Permitir el acceso de los usuarios por medio de la interfaz gráfica: Crear un archivo lightdm.conf en la ruta /etc/lightdm, el cual permitirá que los usuarios del dominio puedan iniciar sesión, ya que se prohíbe el acceso por usuario invitado, quedando el archivo de la siguiente manera:

  [SeatDefaults]
  allow-guest=false
  greeter-show-manual-login=true

Servidores CentOS [42] [43]:

- Habilitar el inicio automático de la interfaz de red: Editar el parámetro ONBOOT de configuración de la interfaz de red, que puede ser visualizado mediante el comando ifconfig, y está ubicado en la ruta /etc/sysconfig/network-scripts/ quedando de la siguiente manera:

  ONBOOT="yes"

E: Plan de trabajo

En el plan de trabajo se indican las actividades a realizar en el proyecto, así como el tiempo ideal para su ejecución.

Id	Nombre de la tarea	Duración	Comienzo	Fin
1	**Análisis de la empresa**	**2 días**	**Lun 12/10/15**	**Mar 13/10/15**
2	Análisis de los servicios y estaciones de trabajo	2 días	Lun 12/10/15	Mar 13/10/15
3	**Inicio propuesta de servicio**	**3 días**	**Mie 14/10/15**	**Vie 16/10/15**
4	Reunión con los gerentes y técnicos de la empresa para acordar costos, fechas y métodos para la solución	2 días	Mie 14/10/15	Jue 15/10/15
5	Pago del 70% de cotización para inicio del proyecto	1 día	Vie 16/10/15	Vie 16/10/15
6	**Implementación y Configuración**	**9 días**	**Lun 19/10/15**	**Jue 29/10/15**
7	Implementación de solución en el servidor DC (Controlador de Dominio)	2 días	Lun 19/10/15	Mar 20/10/15
8	Implementación de solución en los servidores Linux	3 días	Mie 21/10/15	Vie 24/10/15
9	Implementación de solución en las estaciones de trabajo Windows	3 días	Lun 26/10/15	Mie 28/10/15
10	Análisis de pruebas de la implementación	1 día	Jue 29/10/15	Jue 29/10/15
11	**Finalización Propuesta de servicio**	**1 día**	**Vie 30/10/15**	**Vie 30/10/15**
12	Pago del 30% restante	1 días	Vie 30/10/15	Vie 30/10/15

Diagrama de Grantt del plan de trabajo