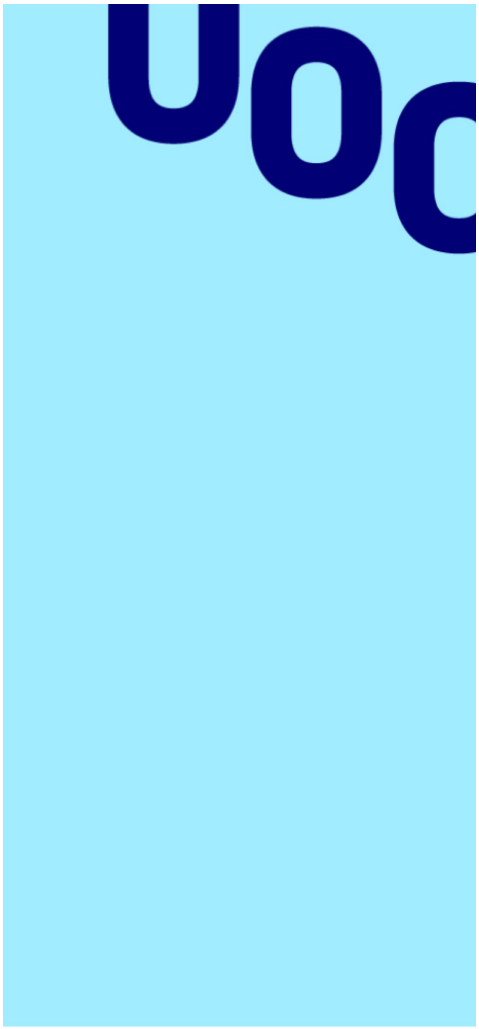
Integración de un sistema LDAP para la autenticación de usuarios en un Centro Educativo



Universitat Oberta de Catalunya

Teodoro Andrés Laírla Morlans

Seguridad Empresarial

Máster Universitario en Ciberseguridad y Privacidad

Nombre del tutor/a de TF:
Àngel Linares Zapater

Nombre del/de la PRA:
Victor Garcia Font

11 de junio de 2024

Quiero dedicar este trabajo al Departamento de Informática y al Equipo Directivo del Sierra de Guara, en especial a David, Adrián y Manuel.

También al Equipo Vitalinux: Nacho y Arturo.

Ficha Del Trabajo Final

Título del trabajo:	Integración de un sistema LDAP para la autenticación de usuarios en un Centro Educativo
Nombre del autor/a:	Teodoro Andrés Laírla Morlans
Nombre del tutor/a de TF:	Àngel Linares Zapater
Nombre del/de la PRA:	Victor Garcia Font
Fecha de entrega:	11 de junio de 2024
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del trabajo final:	Seguridad Empresarial
Idioma del trabajo:	Castellano
Palabras clave:	LDAP, centro educativo, instituto, ies, google, autenticación, linux, sssd, radius, freeradius, red inalámbrica, wifi, wpa-empresarial

Resumen del trabajo

Este proyecto tiene como objetivo principal mejorar la privacidad y la seguridad en los centros educativos que utilicen el entorno de trabajo de Google para educación (Google Workspace for Education) usando las cuentas proporcionadas por Google para la autenticación, tanto en las máquinas Linux del centro educativo como en la red inalámbrica aprovechando el servicio LDAP que proporciona el panel de administración del entorno Google.
Para ello se creará una configuración en pruebas que cuyos objetivos serán: crear una configuración válida para la autenticación con las cuentas de Google para el inicio de sesión en las máquinas Vitalinux del centro, integrando la configuración de permisos y grupos existente; y conseguir implementar en pruebas la autenticación LDAP en la configuración de la red inalámbrica del centro mediante un servidor Radius y la configuración del ecosistema de puntos de acceso ubiquiti ya instalados.
La configuración del inicio de sesión permite dejar en desuso las cuentas genéricas de los equipos del centro, evitando cruces de sesiones de navegador entre los usuarios de las máquinas, mientras que la implantación de la red inalámbrica permitirá granularizar el acceso a la red inalámbrica, aumentando así la privacidad y la seguridad en general en el centro educativo.
Dado que la configuración es similar en todos los centros educativos de Aragón y que la configuración del sistema Vitalinux y de las redes inalámbricas está centralizada desde el Centro Aragonés de Tecnologías para la Educación (CATEDU); y el el Servicio Provincial de Educación de Huesca, este proyecto podría ser fácilmente implantable en muchos centros educativos.

Abstract

This project aims to improve privacy and security in educational centers that use Google Workspace for Education, utilizing Google-provided accounts for authentication, both on Linux machines within the educational center and on the wireless network by leveraging the LDAP service provided by the Google administration panel.
To achieve this, a configuration for IES Sierra de Guara in Huesca will be created with the following objectives: to create a valid configuration for authentication using Google accounts for logging into the Vitalinux machines at the center, integrating the existing permissions and groups configuration; and to implement LDAP authentication in the wireless network configuration at the center in a test environment using a Radius server and the already installed Ubiquiti access point ecosystem.
The login configuration will allow the discontinuation of generic accounts on the center's machines, preventing browser session crossovers between machine users, while the implementation of the wireless network will enable granular access control, thus increasing overall privacy and security within the educational center.
Since the configuration is similar in all educational centers in Aragón and the configuration of the Vitalinux system and wireless networks is centralized by the Aragonese Centre of Technologies for Education (CATEDU) and the Provincial Education Service of Huesca, this project could be easily implemented in many educational centers.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

En España, las administraciones educativas dependientes de las Comunidades Autónomas, han adoptado algunas estrategias comunes en cuanto a digitalización. En primer lugar, suelen proporcionar cuentas de correo electrónico a alumnado y profesorado, bien a nivel de comunidad autónoma, bien a nivel de centro educativo. En la ciudad de Huesca, todos los centros educativos de Secundaria y Formación Profesional, además de la Escuela Oficial de Idiomas hacen uso de cuentas de Google para profesorado y alumnado. Este trabajo se implementará en uno de esos centros.

En segundo lugar, muchas comunidades autónomas han creado una distribución Linux personalizada que se usa e instala en los diferentes centros educativos: Linkat en Cataluña, Max en la Comunidad de Madrid, Lluirex en Valencia y Vitalinux en Aragón[1].

En tercer lugar, la mayoría de institutos y colegios, poseen una red inalámbrica de tipo Wifi-5 o Wifi-6, con puntos de acceso Ubiquiti y gestión centralizada mediante un gestor de puntos de acceso, aunque estos puntos de acceso permiten configuración Radius empresarial, la configuración más habitual es tener una clave WPA2 compartida (PSK: Pre-Shared Key). Esto presenta una dificultad añadida, ya que al autenticar todos los ordenadores con la misma clave, es muy sencillo que esa clave acabe siendo pública, con lo que se permite el acceso a la red de la organización por parte de todos los usuarios en posesión de la clave y esta situación plantea muchos riesgos de seguridad.

Este proyecto plantea aprovechar estos tres elementos comunes (cuentas de Google, Sistemas Linux y red inalámbrica gestionable y centralizada) para buscar una solución de autenticación común a la red inalámbrica y los sistemas Linux contra el servidor LDAP proporcionado por el entorno de Google para Educación (*Google Workspace for Education*).

1.1. Contexto y justificación del trabajo

El trabajo se contextualiza en un centro educativo en el que conviven las tecnologías para las cuales se han desarrollado los objetivos: Google Workspace para educación, red inalámbrica y ordenadores de usuario con un sistema operativo GNU/Linux.

1.1.1. Centro de referencia: IES Sierra de Guara

El IES Sierra de Guara, en Huesca, es un centro educativo de Educación Secundaria, Bachillerato y todas las etapas de Formación Profesional. En él comenzaron el curso 23/24 un total de 1.163 estudiantes y 126 docentes. Todos y todas necesitan usar la infraestructura tecnológica del centro y, para ello, al principio de curso se les otorga una cuenta de Google Workspace para educación (antes llamado GSuite).

Además, el centro participa en el programa Vitalinux de la DGA[2]. El sistema Vitalinux EDU, proporcionado por el Gobierno de Aragón, se encuentra instalado en más de 120 portátiles, en todos los ordenadores de profesorado de las aulas de la ESO y parte de las de Bachillerato; y en la mayoría de aulas de ordenadores del centro.

Con este proyecto, se pretende implementar una configuración para el IES Sierra de Guara de modo que 1) los ordenadores que utilizan el sistema operativo Vitalinux EDU, puedan iniciar sesión con los usuarios de la organización de Google Workspace por medio de un servicio LDAP vinculando los permisos con los grupos del sistema de Google y 2) se pueda implantar una configuración inalámbrica con un sistema Radius para autenticar contra el servicio LDAP.

Para realizar este proyecto, se estudiará un caso en concreto, en el IES Sierra de Guara de Huesca, en el que se pretende implantar el uso de un sistema de LDAP para homogeneizar el inicio de sesión, en Vitalinux y en la red inalámbrica.

1.1.2. Sistemas Operativos en el IES Sierra de Guara

En los centros educativos de secundaria en España es casi ubicuo el uso del ecosistema de Google para educación.

En Aragón, el gobierno lanzó una distribución Linux llamada VitaLinux, cuya versión educativa VitaLinux EDU (DGA) está implantada en 149 centros de la comunidad autónoma de primaria, secundaria y formación profesional. Esa distribución utiliza un sistema de gestión automatizada basado en Migasfree con el que, mediante un sencillo sistema de etiquetas, se consigue realizar despliegues de software automáticos y configuraciones masivas para cada etiqueta [2]. En el IES Sierra de Guara, más de 300 equipos utilizan este sistema operativo.

Hasta ahora, los usuarios dentro de Vitalinux son genéricos (estudiante y docente) y habitualmente los perfiles se eliminan en cada reinicio. Esto conlleva algunos problemas, por ejemplo, se da el caso de que un estudiante deja la sesión iniciada en un equipo, lo que puede propiciar que la siguiente persona que acceda a ese ordenador, se encuentre con una sesión abierta de cualquier servicio dentro del navegador. El borrado de los datos de sesión se da sólo en el reinicio, si un usuario o usuaria cierra la sesión de escritorio genérica, en lugar de apagar el equipo, también podría dejarse la sesión abierta en los navegadores.

El primero de los objetivos de este proyecto va encaminado al inicio de sesión personalizado en los equipos Linux del centro usando el servidor LDAP configurado en Google Workspace, tanto para profesores como para alumnos o personal administrativo y servicios y la configuración correcta de los perfiles de profesorado y alumnado según la estructura de unidades organizativas del Google Workspace adecuando los perfiles de seguridad a lo ya existente en la configuración del sistema Vitalinux.

1.1.3. Configuración inalámbrica en el IES Sierra de Guara

En los centros educativos de la provincia de Huesca, el equipo informático del Servicio Provincial de Educación, establece una configuración estándar para todos los centros, que se basa en la instalación de puntos de acceso Ubiquiti gestionados por Ubiquiti UniFi Controller. Este sistema permite, desde el mismo portal, desplegar una configuración común para todos los puntos de acceso del mismo centro de manera automática.

La seguridad de la red inalámbrica, está establecida usando una contraseña WPA2/PSK. Por ello, el segundo de los objetivos tiene que estar encaminado a eliminar esa contraseña compartida de la configuración inalámbrica. Para ello se pretende establecer un servicio Radius conectado al LDAP configurado de Google Workspace, para usar esas mismas credenciales de acceso, para la autenticación y acceso dentro de la red inalámbrica.

1.1.4. Problemas identificados

Una vez identificada la configuración en el IES en el punto anterior, se detallan los problemas identificados.

Problemas derivados de los usuarios genéricos

El uso de usuarios genéricos en ordenadores compartidos, puede conllevar problemas de suplantación de identidad. En este sentido, en el IES Sierra de Guara, se han producido muchas veces situaciones de utilización de sesiones ajenas para el envío de mensajes, suplantando así las cuentas de correo electrónico u otros servicios de Internet entre estudiantes.

Para solventar, o al menos, paliar estos problemas, los datos de las cuentas de usuario se borran tras reiniciar la máquina, como una configuración general de todos los equipos Linux. Esta solución no es óptima, ya que puede darse el caso de que un usuario olvide apagar la máquina o que cierre sesión en lugar de apagar, lo que no conlleva el borrado de los datos de usuarios.

Además, este borrado de datos, no permite el uso de historiales de comandos, aplicaciones, archivos o visitas del navegador, con lo que todas las bondades de tener un usuario propio para iniciar sesión, se ven limitadas al uso de la sesión particular y no se extienden a lo largo de los días, como cabría esperar.

Problemas derivados del uso de una clave compartida

Debido a la gran cantidad de dispositivos que usan esta red inalámbrica, afrontar un cambio en la contraseña inalámbrica supone la configuración de muchísimos dispositivos. Además, el equipo técnico del instituto ha detectado equipos personales del alumnado conectados a la red inalámbrica, con lo que se pone de manifiesto la filtración de esa contraseña, ya que en un principio, sólo debiera estar disponible para profesorado y personal administrativo y no para el alumnado.

Este hecho supone una potencial brecha de seguridad por la cual un equipo ajeno a la organización se conecta directamente a ella y, si bien es cierto que existe una subred específica para los dispositivos inalámbricos y que dicha subred se encuentra aislada de los dispositivos

críticos y cableados de la organización mediante un firewall, la conexión a la red del centro debería ser controlada en todo momento.

1.2. Objetivos del trabajo

Los objetivos que se pretenden alcanzar en este TFM son los siguientes:

Objetivo 1 Configuración del servicio LDAP de Google Workspace.

- **1.1** Investigación sobre LDAP.
- **1.2** Investigación sobre LDAP de Google Workspace.
- **1.3** Configuración del servidor LDAP Google Workspace.

Objetivo 2 Configuración de inicio de sesión en VitaLinux.

- **2.1** Investigación de la integración Linux-LDAP.
- **2.2** Configuración del inicio de sesión.

Objetivo 3 Configuración de permisos

- **3.1** Investigación de Permisos LDAP Unidades Organizativas.
- **3.2** Configuración del rol "estudiante".
- **3.3** Configuración del rol "docente".
- **3.4** Configuración del rol "administrador".

Objetivo 4 Autenticación Radius para redes inalámbricas aprovechando LDAP de Google Workspace

- **4.1** Investigación Radius.
- **4.2** Configurar servidor.
- **4.3** Conexión Radius - LDAP.
- **4.4** Configuración de un punto de acceso genérico.
- **4.5** Configuración del ecosistema Ubiquiti /UniFi Controller.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

El compromiso de la Universidad Oberta de Catalunya con los Objetivos de Desarrollo Sostenible (ODS) de la Organización de las Naciones Unidas (ONU), se hace patente en esta sección, en la que se establecen los posibles impactos positivos que este TFM puede tener sobre los ODS.

1.3.1. Impacto ético

Este proyecto tiene un impacto en la gestión de la privacidad de los datos. Al establecer un sistema de sesiones vinculado a un servicio personalizado como lo es el Google Workspace, se evita que datos personales sean recopilados en cuentas de usuario genéricas, accesibles por todo el mundo.

Además, el hecho de usar sistemas de identificación, podría llevar en futuras etapas de este proyecto, a un monitoreo y respuesta ante incidentes más personalizado, cuyo aspecto ético se enfoca en la rendición de cuentas del usuario.

Esta configuración, supone preparar a las máquinas cliente para iniciar sesión contra un servicio de autenticación abierto como lo es LDAP, aunque en esta fase se usará un LDAP proporcionado por Google, la configuración abre la puerta a el uso de otras implementaciones del servicio LDAP, que puedan ser libres y abandonar paulatinamente la dependencia de las instituciones educativas a las tecnologías de Google o Microsoft.

Así este proyecto contribuye al ODS 9: «Industria, Innovación e Infraestructura», fomentando la innovación en la gestión de datos y sistemas de autenticación abiertos, impulsando la infraestructura tecnológica sostenible, además la rendición de cuentas y la protección de los datos personales contribuye al ODS 16: «Paz, Justicia e Instituciones Solidarias».

1.3.2. Impacto social

El uso de tecnologías Vitalinux, democratiza el acceso a las nuevas tecnologías por parte de usuarios cuya situación económica no les permita acceder a licencias propietarias. La integración de los estándares abiertos en los sistemas educativos sobre distribuciones de código abierto, permite visibilizar el movimiento *Open Software*, cuyo impacto real en la sociedad es desconocido por no ser el sistema de escritorio mayoritario.

Además, la integración y utilización de sistemas de virtualización de escritorios permite a los usuarios el acceso a hardware y software con una potencia mucho mayor que el encontrado habitualmente en los hogares, mediante el acceso a máquinas.

Al democratizar el acceso a la tecnología en el entorno educativo, este proyecto contribuye al ODS 4: «Educación en Calidad» y al ODS 10: «Reducción de las desigualdades».

1.3.3. Impacto ambiental

El uso de sistemas ligeros en entornos educativos, por ejemplo Vitalinux, permite alargar la vida útil del hardware informático, esto conlleva, necesariamente, una reducción de residuos tecnológicos además de un ahorro energético.

El uso de microordenadores como Raspberry Pi, para servicios ligeros, como se pretende establecer en este proyecto para el servidor Radius, permite tener un ahorro inicial por su bajo importe de compra y energético debido a su bajo consumo energético.

El uso de servidores virtualizados y entornos VDI mejora la eficiencia energética[3].

Este impacto ambiental, contribuye a los ODS 12: «Producción y Consumo Responsables» y ODS 13: «Acción por el Clima».

1.4. Metodología

Para este proyecto se intentará seguir una metodología basada en etapas y ciclos. Una vez se hayan definidos los objetivos, se irá trabajando en ellos uno a uno hasta su resolución, afrontando todos los objetivos de la misma manera, siguiendo un ciclo de objetivos. Tras haber afrontado todos los objetivos, se efectuarán las etapas finales.

- Planificación General
  - Justificación Motivación.
  - Investigación preliminar.
  - Definición de los objetivos concretos.
  - Planificación de los ciclos de los objetivos.
  - Estudio de los recursos disponibles y costes.
  - Análisis de Riesgos.
- Ciclos de objetivos (uno por cada objetivo del proyecto)
  - Investigación del objetivo y de las tecnologías implicadas.
  - Diseño del objetivo.
  - Implementación del objetivo.
  - Pruebas y validación del objetivo.
  - Documentación y generación de instrucciones.
- Conclusión
  - Estudio de consecución de los objetivos.
  - Redacción de conclusiones.
  - Líneas y objetivos futuros.
- Redacción final, presentación final y defensa.

Esta metodología se considera la idónea debido a que los trabajos se pueden separar por objetivos, a mi experiencia en la planificación de desarrollo de proyectos siguiendo la misma metodología; y a que se puede hacer una correspondencia directa de los ciclos con las diferentes entregas de la evaluación continua del proyecto.

1.5. Planificación

Para la planificación, se seguirá el método propuesto por la asignatura del TFM basado en evaluación continua. Se planifican las tareas temporalmente englobadas en 4 grupos, correspondientes a las 4 Pruebas de Evaluación Continua (PEC1, PEC2, PEC3 y PEC4) pautadas en la asignatura. Las entregas serán consideradas hitos del proyecto con una fecha fija de finalización.

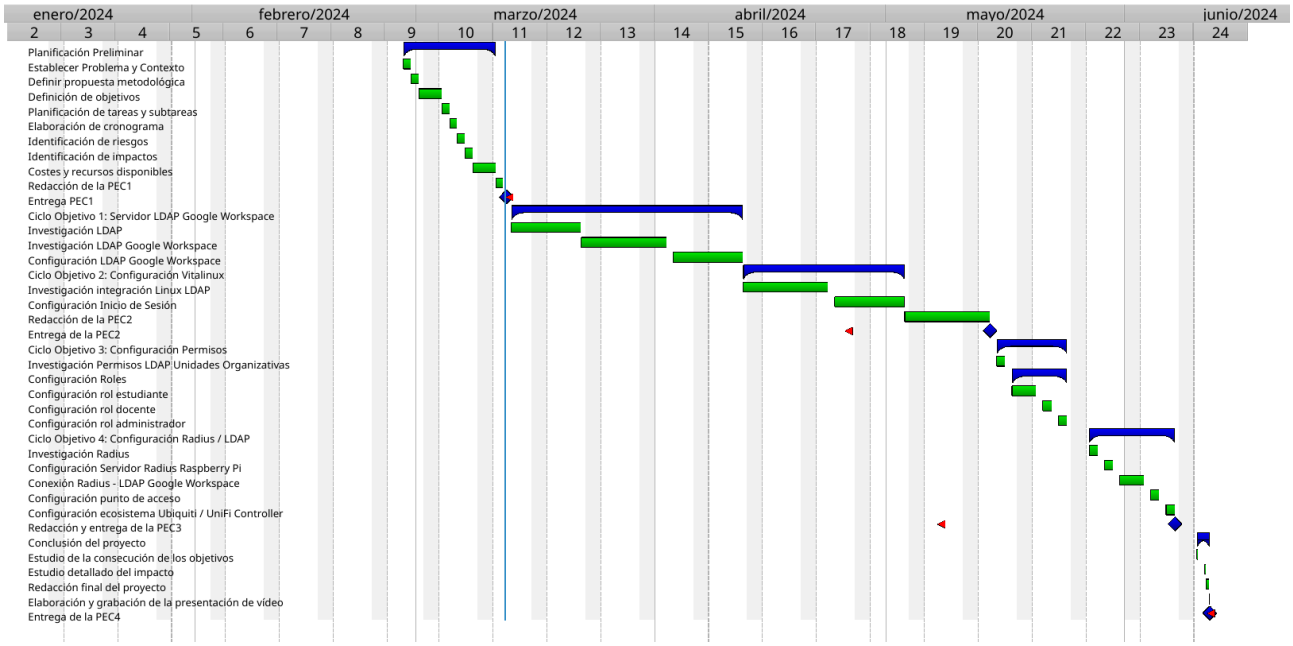


Figura 1.1: Diagrama de Gantt con las tareas propuestas en la tabla 1.1

En la tabla 1.1 se relacionan las tareas con su planificación temporal. Nótese que las filas sombreadas son tareas que se desglosan debajo y que su fecha de inicio y finalización así como su duración es un compendio de todas las tareas que engloban. Además, las filas en negrita corresponden a los diferentes hitos del proyecto en forma de Pruebas de Evaluación Continua (PECs). Todas las fechas corresponden al año 2024.

1.6. Diagrama de Gantt

Con la temporalización propuesta en la tabla 1.1 se realiza un diagrama de Gantt para la visualización de las tareas del proyecto en una línea temporal.

1.7. Sumario de productos obtenidos

Tras la finalización del TFM, se enumeran aquí los resultados obtenidos que están relacionados con los 4 objetivos:

1. Manual de configuración del servicio LDAP de Google, tanto para el cliente SSSD como para el cliente FreeRadius.

2. Manual de configuración del demonio SSSD en Linux (basado en ubuntu).

3. Manual de configuración del módulo PAM `pam_group` para adquirir la pertenencia a grupos de la máquina basándose en grupos del dominio.

4. Manual de configuración e implantación del servidor FreeRadius para la conexión con LDAP de Google.

Cód.	Tarea	Inicio	Fin	Duración
1	Planificación Preliminar	28 feb.	12 mar.	50
1.1	Establecer problema y contexto	28 feb.	29 feb.	4
1.2	Definir propuesta metodológica	29 feb.	1 mar.	4
1.3	Definición de objetivos	1 mar.	4 mar.	4
1.4	Planificación de tareas y subtareas	4 mar.	5 mar.	4
1.5	Elaboración de cronograma (Gantt)	5 mar.	6 mar.	4
1.6	Identificación de riesgos	6 mar.	7 mar.	4
1.7	Identificación de impactos	7 mar.	8 mar.	4
1.8	Costes y recursos disponibles	8 mar.	11 mar.	4
2	Hito: Redacción y entrega de la PEC1	28 feb.	12 mar.	10
3	Ciclo Obj. 1: Servidor LDAP Google Workspace	13 mar.	10 abr.	45
3.1	Investigación sobre LDAP	13 mar.	21 mar.	15
3.2	Investigación sobre LDAP de Google Workspace	21 mar.	28 mar.	15
3.3	Configuración de los servicios LDAP	28 mar.	10 abr.	15
4	Ciclo Obj. 2: Configuración Vitalinux	10 abr.	25 abr.	30
4.1	Investigación integración Linux LDAP	10 abr.	17 abr.	15
4.2	Configuración de inicio de sesión	17 abr.	25 abr.	15
5	Hito: Redacción y entrega de la PEC2	13 mar.	25 abr.	30
6	Ciclo de Obj. 3: Configuración de permisos	26 abr.	1 may.	45
6.1	Investigación Permisos LDAP y Ud. Organizativas	26 abr.	27 abr.	8
6.2	Investigación adquisición de permisos en el inicio	28 abr.	29 abr.	8
6.3	Investigación grupos de usuarios	30 abr.	1 may.	8
6.4	Configuración de roles	1 may.	2 may.	8
7	Ciclo de Obj. 4:	2 may.	7 may.	45
7.1	Investigación Radius	2 may.	3 may.	8
7.2	Configuración Servidor - LDAP Google Workspace Pi	3 abr.	4 may.	5
7.3	Conexión Radius - LDAP Google Workspace	10 abr.	17 abr.	5
7.4	Configuración entorno local de pruebas	10 abr.	17 abr.	5
7.5	Implantación en el centro educativo	10 abr.	17 abr.	7
8	Hito: Redacción y entrega de PEC3: Objetivos 3 y 4.	26 abr.	7 may.	10
9	Conclusión del proyecto	8 may.	9 jun.	60
9.1	Estudio de la consecución de los objetivos.	8 may.	12 may.	15
9.2	Estudio detallado del impacto.	12 may.	16 may.	15
9.3	Redacción final del proyecto.	16 may.	20 may.	15
9.4	Elaboración y grabación de la presentación de vídeo.	20 may.	24 may	15
10	Hito: Redacción y entrega de PEC4	8 may	9 jun.	
	Defensa del proyecto			
	Total	28 feb.	20 jun.	275

Tabla 1.1: Planificación temporal de las tareas.

5. Manual de configuración e implantación de una red inalámbrica con seguridad WPA2-Empresarial basada en Radius en un ecosistema Ubiquiti.

1.8. Descripción de la memoria

La memoria estará compuesta por diferentes capítulos además de esta Introdución, aquí se detalla brevemente en qué consiste cada uno:

- Estado del arte (cap. 2): Se analizan las opciones disponibles para la consecución de los objetivos.
- Materiales (cap. 3): Descripción de las herramientas de trabajo para llevar a cabo los objetivos.
- Solución Tecnológica (cap. 4): Descripción detallada de la configuración de todos los sistemas para lograr los objetivos.
- Resultados (cap. 5): Análisis de los resultados obtenidos correlacionándolos con los objetivos.
- Conclusiones y trabajos futuros (cap. 6): Se elaboran unas conclusiones y se enumeran una serie de trabajos que pueden seguir a este TFM.
- Finalmente, una bibliografía (cap. 7) y un glosario de términos.

Capítulo 2

Estado del arte

Para la realización de este proyecto, se consideran opciones de Software Libre en la medida de lo posible, de acuerdo con la política del Plan Digital de Centro de estudio donde se implantará la solución.

2.1. Servicios de Identificación y Autenticación (LDAP)

El sistema de directorio LDAP (Lightweight Directory Access Protocol) es un método de autenticación e identificación ampliamente utilizado. Existen varias implementaciones del mismo entre las que destacan OpenLDAP y Active Directory de Microsoft. Sin embargo, para este proyecto se ha decidido utilizar el servicio proporcionado por Google para el Entorno de trabajo educativo debido a los siguientes motivos:

1. A priori, la configuración es sencilla desde el panel de administración de Google, y el servicio se inicia y configura en cuestión de minutos.

2. Todas las cuentas de usuario y grupos ya están creados de antemano en el entorno educativo. Es un trabajo que hay que hacer a principio de curso para todos los usuarios del centro.

3. El servicio de Google sólo se puede utilizar con seguridad mediante certificados.

4. Se pueden iniciar diferentes servicios con diferentes finalidades y seleccionar qué parte de la organización estará disponible en cada servicio mediante Unidades Organizativas o Grupos de usuarios.

5. El servicio es de sólo lectura, sólo se pueden cambiar los datos del servicio LDAP desde el panel de administración de Google, esto añade una capa de seguridad extra ya que operaciones diferentes a las de consulta o autenticación no se pueden realizar, al no estar disponibles en el servicio.

6. Aunque existe en el centro un Active Directory de Microsoft, sólo es utilizado por parte de los alumnos de Formación Profesional para el inicio de sesión en Windows, por lo que si se quisiera uitilizar estos servicios para la autenticación, habría que importar el resto del alumnado del centro.

7. Se ha descarta el uso de OpenLDAP como servicio LDAP para la autenticación ya que se debería hacer una importación de todos los usuarios.

8. Aunque el servidor de Google es privativo, todo lo relacionado con la comunicación LDAP y el estándar RFC2307bis[4] que utiliza es libre.

2.2. Cliente de autenticación LDAP en Linux

Para seleccionar un programa cliente para gestionar el inicio de sesión contra un servidor de identidad y autenticación, se puede optar por 3 opciones de Software Libre:

2.2.1. LDAPD

El demonio ldapd proporciona un mecanismo que permite la autenticación contra un servicio LDAP usando NSS y PAM, además el servicio también puede ser utilizado para la configuración de Active Directory. Sin embargo, carece de autenticación multidominio.

2.2.2. Winbind

Es un demonio que forma parte del ecosistema de aplicaciones del protocolo SAMBA, se utiliza para permitir que sistemas Linux autentiquen usuarios basándose en dominios de Active Directory, como ya se ha decidido usar un servicio LDAP y no un Active Directory, este cliente de autenticación queda descartado para este trabajo.

2.2.3. SSSD

El cliente de autenticación SSSD proporciona acceso a identidades remotas y mecanismos de autenticación. Se utiliza para autenticar el acceso a los sistemas basados en Linux utilizando varias fuentes, incluido LDAP y Active Directory. Además es multidominio, lo que quiere decir que una máquina puede ser configurada para autenticarse de manera local con los usuarios del sistema de archivos, y contra varios servicios de autenticación remotos. Se gana flexibilidad al poder configurar, además de el servicio LDAP objeto de este proyecto, el inicio de sesión con autenticación remota mediante otros sistemas presentes en el centro como el servidor Active Directory para los alumnos de FP que hacen uso de él.

2.3. Servidor Radius

2.3.1. FreeRadius

FreeRadius es un servidor RADIUS de código abierto que proporciona autenticación centralizada para dispositivos y servicios, como redes WiFi. Se integra con varios sistemas de backend, incluidos LDAP y bases de datos SQL. Se considera la mejor alternativa de Software Libre y es, por ejemplo, el proveedor del servicio recomendado por la plataforma Eduroam.

2.3.2. Radiator

Hay alternativas no libres como por ejemplo Radiator, un servidor RADIUS comercial que ofrece amplia configurabilidad y soporte para múltiples métodos de autenticación, pero que conlleva un coste. También, se puede configurar Microsoft NPS (Network Policy Server) como parte de los servicios de Active Directory que permite la autenticación y autorización RADIUS en entornos Windows, pero es una opción que se ha descartado ya para evitar tener duplicidad de usuarios en el Entorno de Trabajo de Google y el Active Directory Local.

Capítulo 3

Materiales

Se enumeran a continuación los materiales de los que se disponen para realizar este TFM:

- Google Workspace para centros educativos: IES Sierra de Guara. Cuenta de administrador.
- Acceso a campus virtual VDI Isard VDI con la cuenta del IES Sierra de Guara.
- Raspberries Pi 3B+ para configuración de servidores de prueba.
- Punto de acceso de pruebas con OpenWRT.
- 2 Servidores Windows Server 2016 para la instalación de máquinas virtuales.
- Conexión a internet del centro educativo: Fibra óptica simétrica de 600 Mbps.
- Conexión a internet en el hogar. Fibra óptica.
- Conexión VPN con el centro educativo.
- Entorno de trabajo multipantalla.
- Cuenta de Google Educativa de la UOC.
- Ordenador personal con las siguientes características:
  - Procesador hexacore Intel® Core™ i7-8750H CPU @ 2.20GHz.
  - 20 GiB RAM SODIMM DDR4 Synchronous 2400 MHz
  - 2 TB de espacio.
  - Sistema Operativo: Debian GNU/Linux 12 (bookworm).
  - Sistema Operativo: Windows 10.

Capítulo 4

Solución Tecnológica

Vistas las alternativas, el siguiente apartado se describirán las características del entorno y se detallará la solución tecnológica aplicada tras el desarrollo de los ciclos de objetivos. Se han implementado configuraciones en 3 ámbitos principales:

1. El servicio LDAP de Google Workspace para educación mediante el panel de administración:
    a) Servicio LDAP para el inicio de Sesión de Vitalinux.
    b) Servicio LDAP para el servidor Radius.
2. Las máquinas de trabajo de Vitalinux:
    a) Configuración del demonio SSSD: /etc/sssd/sssd.conf
    b) Configuración de los sistemas NSS: /etc/nsswitch.conf
    c) Configuración del sistema PAM: /etc/pam
        i. Creación del perfil para pam-auth-update en /usr/lib/pam/pam-configs
        ii. Mapeo de grupos /etc/security/group.conf para la configuración de permisos
3. Configuración Inalámbrica
    a) Servidor Radius: FreeRadius
    b) Configuración de la red inalámbrica en el controlador Unify

En la figura 4.1 se representa el esquema general de la configuración.

4.1. Características del entorno

4.1.1. Ecosistema de Google para educación

El ecosistema de Google para educación es una versión de su conjunto de herramientas empresarial. En él, se pueden crear cuentas de usuario organizadas en Unidades Organizativas. El sistema de Unidades Organizativas es jerárquico y tiene herencia, una Unidad Organizativa

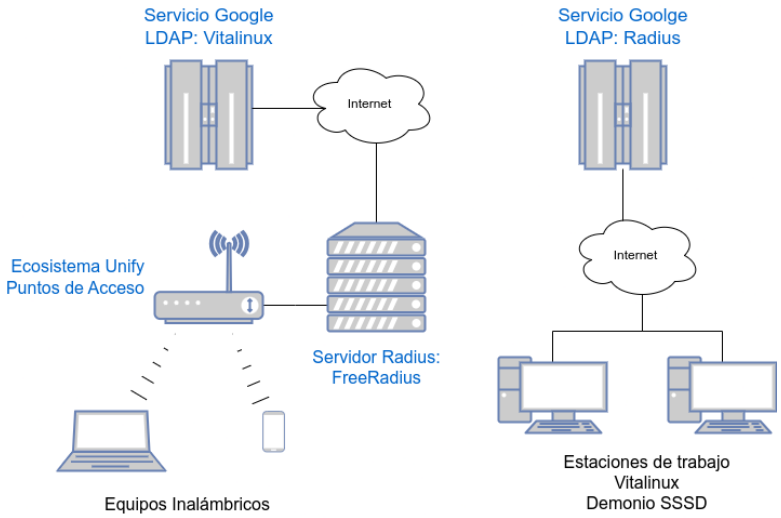


Figura 4.1: Esquema general de la configuración

puede tener Unidades Organizativas internas. Todos los usuarios deben pertenecer a una Unidad Organizativa y sólo a una. Se pueden configurar herramientas para toda una Unidad Organizativa. La configuración específica de una Unidad Organizativa es heredada por los usuarios que pertenezcan a ella o a las Unidades Organizativas dependientes de ella.

Además, el sistema prevé la utilización de grupos de usuarios, diferentes de las unidades organizativas, que tienen menos restricciones. Por ejemplo, un usuario puede pertenecer a varios grupos, y se pueden crear grupos de grupos.

Tanto las Unidades Organizativas como los Grupos son objeto acceso por el servicio LDAP.

4.1.2. Sistema Operativo Vitalinux

Vitalinux es una distribución Linux basada en la versión más reciente de Ubuntu LTS, que tiene las siguientes características:

- Entorno de trabajo personalizado con fines educativos
- Entorno de escritorio e interfaz ligeros.
- Sistema de Etiquetas Migasfree para la configuración remota.

Esta distribución está implantada en 149 centros educativos de los cuales 130 lo utilizan activamente [5]. La herramienta principal para la gestión de Vitalinux es Migasfree: «un software libre que gestiona despliegues de software, manteniendo y asegurando la integridad de los sistemas informáticos», según su sitio web [6]. Esta herramienta permite dotar a un equipo un perfil de configuración basado en etiquetas. El sistema cliente revisará al inicio de cada sesión si hay algún cambio que aplicar en alguna de las etiquetas que tiene asignado y, si es así, aplicará los cambios. Así, la configuración propuesta en este proyecto podría ser implantada de manera masiva en aquellos centros de Aragón que utilizan este sistema y que utilizan Google Workspace para educación, lo que aumenta de manera drástica el potencial impacto de la solución.

4.1.3. Red inalámbrica: Ecosistema Unify de Ubiquiti

En el IES Sierra de Guara la red inalámbrica está gestionada por el Servicio Provincial de Educación de Huesca y consta de 16 puntos de acceso repartidos por los 4 edificios del centro.

La configuración está centralizada por un controlador Unify y permite despliegues de red inalámbrica automáticos en los puntos de acceso seleccionados o en todos a la vez a través de una interfaz web.

4.2. Servicio LDAP. Configuración completa.

Como ya se ha avanzado en la introducción, la configuración de todo el sistema de autenticación se basará en los servicios de LDAP proporcionados por el entorno de trabajo de Google para educación, aunque es un sistema privativo, el hecho de que todas las cuentas estén incluidas en el sistema lo hace idóneo para un despliege inmediato y plenamente funcional, además de que no conlleva un coste económico para el centro y de que la interfaz del panel de administración ya es conocida por los usuarios con privilegios administrativos del dominio.

El servicio LDAP se encuentra dentro de las «Aplicaciones» del entorno y permite iniciar varios servicios diferentes que se autenticarán mediante certificados criptográficos. En este trabajo se crearán 2 servicios diferenciados, uno para el inicio de sesión en máquinas Vitalinux y otro para la configuración autenticación de la red inalámbrica del servidor Radius. Además, se permite crear un usuario administrador del servicio que será necesario para el servidor FreeRadius, pero no lo es para el demonio SSSD.

Los pasos para crear estos servicios, que en la interfaz web se denominan «Cliente», son los siguientes:

1. Crear el servicio LDAP en el panel de administración del Google Workspace
    - Ir a https://admin.google.com.
    - Ir a Aplicaciones → LDAP.
    - Hacer clic en «AÑADIR CLIENTE».
    - En el paso 1, establecer un nombre y una descripción al cliente y hacer clic en «SIGUIENTE».
    - En el paso 2:
        - Seleccionar quién podrá autenticarse, por ejemplo «Todo el dominio». En este punto se pueden seleccionar grupos o unidades organizativas.
        - Seleccionar qué usuarios podrán leer la información de otros usuarios. Otra vez, se puede dejar «Todo el dominio» o granularizar.
        - Activar la opción «Leer información de grupos para para poder hacer configuraciones relativas a permisos».
        - Hacer clic en «AÑADIR CLIENTE LDAP»
    - Ir a «Estado del Servicio» y marcar «Activado para todos».
    - Finalmente, descargar el certificado, que en realidad es un fichero comprimido con el certificado `.crt` y el fichero de clave `.key`.

- En el caso del FreeRadius, hace falta crear unas «credenciales de acceso», además de un certificado.

Cada uno de estos servicios se puede configurar para que dé acceso a un subconjunto de usuarios, bien sea por unidades organizativas o por grupos de usuarios. Así, se configura el servicio LDAP para el inicio de sesión en Vitalinux disponible para todos los usuarios del dominio y el servicio de FreeRadius para que esté disponible para el profesorado.

4.3. Configuración de las máquinas

La configuración en las máquinas de trabajo Vitalinux para la autenticación de los usuarios del sistema a través de LDAP implica varias herramientas. Por un lado, la pantalla de autenticación LightDM, por otro el demonio de resolución de nombres NSS y los módulos de autenticación de PAM; y, finalmente, el demonio de autenticación e identificación SSSD contra el servicio LDAP.

4.3.1. Configuración LightDM

El gestor de inicio de sesión instalado en Vitalinux es el Lightdm-gtk. En este caso, el sistema se integra con sssd de manera nativa. Como se quiere priorizar el inicio de sesión mediante los usuarios LDAP, se ocultará la lista de usuarios locales para que el usuario tenga que introducir a mano sus credenciales. En el fichero `/etc/lightdm/lightdm.conf` se establecerá la siguiente directiva.

```
1 greeter-hide-users = true
```

Configuración 4.1: Añadido al fichero de configuración `/etc/lightdm/lightdm.conf`.

4.3.2. Cliente multidominio para autenticación: Demonio SSSD

Nota: Tanto el servidor LDAP como el cliente SSSD pueden ser referenciados como servicios, uno como un servicio en la nube y otro como un servicio local de la máquina Linux, para evitar confusiones, en el texto se reservará el término servicio para el servidor LDAP (aunque en el panel de administración incluya el nombre «Clientes») y se utilizará el término demonio para el servicio local SSSD que representará al cliente en la autenticación.

Para el demonio de autenticación, se ha optado por la opción de SSSD, este servicio se ha elegido por permitir la autenticación en varias tecnologías diferentes (Active Directory, FreeIPA, LDAP...). Además, uno de los puntos fuertes de este demonio, es que permite la autenticación contra diferentes sistemas de identidad en diferentes dominios, así se podría tener en una misma máquina usuarios autenticados por el servidor LDAP y otros por alguno de los servidores Active Directory ya presente en el centro. En este TFM, sólo se hará la configuración para el dominio LDAP del Google Workspace.

Otra de las ventajas del demonio SSSD es que la autenticación está integrada con PAM (Pluggable Authentication Modules) que es el sistema que utilizan la mayoría de distribuciones

Linux modernas, y la resolución de los números de identificación de usuario y grupo (uid y gid) está integrada con el demonio NSS del ecosistema Unix.

La discriminación de qué dominio se utiliza para autenticar a un usuario se hace por orden de aparición en el fichero de configuración de los diferentes servicios de identificación o bien discriminando por el dominio de la cuenta en caso de proporcionar un nombre de usuario completo del tipo «usuario@dominio».

Instalación del demonio

Para la instalación del demonio SSSD en el sistema se necesitan los siguientes paquetes y sus dependencias, todos están disponibles en los repositorios por defecto de la distribución Vitalinux que está basada en Ubuntu 22.04.3 LTS (Jammy Jellyfish):

- `sssd`: Paquete principal del demonio.
- `sssd-ldap`: Paquete que incluye la integración con servicios LDAP para el demonio SSSD.
- `sssd-tools`: Paquete con herramientas que permiten, por ejemplo, el borrado de la caché de nombres, el borrado de logs, la comprobación del fichero de configuración, etc. Aunque no es un paquete estrictamente necesario para el funcionamiento del demonio, las herramientas que proporciona son muy útiles para la configuración y el proceso de pruebas.

```
1 sudo apt install sssd sssd-ldap sssd-tools
```

Configuración 4.2: Instalación del demonio SSSD

Configuración del demonio SSSD

El demonio SSSD se puede configurar en un único fichero de tipo INI, cuya ubicación en las distribuciones Debian y Ubuntu se encuentran en `/etc/sssd/sssd.conf`. Sin embargo, también se permite la utilización de ficheros separados en el directorio `/etc/sssd/conf.d/`, que se irán leyendo por orden alfabético, y cuya configuración se cargará al inicio del servicio siempre y cuando el nombre de archivo no comience por el carácter punto y sí tenga la extensión `.conf`.

En este caso se van a configurar dos ficheros separados, uno con la configuración general del demonio y otro con la configuración específica del servicio LDAP para el dominio `iessierradeguara.com`. Esto se hace con la finalidad de tener una configuración más organizada y, en un futuro, tener la capacidad de añadir más dominios de autenticación en sus respectivos ficheros.

En el fichero `/etc/sssd/sssd.conf` se especifican las opciones generales del demonio y se deja la configuración específica del dominio para el fichero `01-iessierradeguara.com.conf` en el directorio `/etc/sssd/conf.d/`.

Tras un estudio detallado de las páginas del manual de linux de `sssd`, `sssd.conf`, `sssd-ldap` y `sssd-ldap-attributes` mediante el comando `man` se termina definiendo el siguiente fichero, las opciones más importantes están explicadas en los comentarios:

Primero se modifica el fichero `/etc/sssd/sssd.conf` con la configuraición general, hay que asegurarse de que el propietario del fichero sea `root` y de que los permisos sean `0600`:

```
# Fichero /etc/sssd/sssd.conf (Configuración general)

[sssd]
config_file_version = 2

services = nss, pam
domains = iessierradeguara.com
reconnection_retries = 3

#Configuración del respondedor NSS.
#Se filtran los usuarios y grupos locales.

[nss]
filter_groups = root, dga, estudiante, docente, cau, admin
filter_users = root, estudiante, dga, docente, cau, lightdm, admin

#Configuración del respondedor de autenticación.
[pam]
# Las credenciales no expiran.
# Esto permite el login offline de usuaros cacheados.
offline_credentials_expiration = 0
offline_failed_login_attempts = 100
offline_failed_login_delay = 5

```

Configuración 4.3: Fichero `/etc/sssd/sssd.conf`.

Tras haber configurado el fichero general, se crea la configuración particular del dominio LDAP `@iessierradeguara.com` en el fichero `/etc/sssd/conf.d/01-iessierradeguara.com.conf`, teniendo en cuenta que el propietario y grupo del mismo sean `root` de que los permisos sean de nuevo `0600`:

```
# Configuración específica del dominio iessierradeguara.com
# Hay más configuración general en /etc/sssd/sssd.conf

[domain/iessierradeguara.com]

id_provider = ldap
auth_provider = ldap
access_provider = ldap
ldap_search_base = dc=iessierradeguara,dc=com
ldap_user_search_base = ou=Users,dc=iessierradeguara,dc=com
```

```
11 ldap_group_search_base = ou=Groups,dc=iessierradeguara,dc=com
12 ldap_access_order = filter
13 ldap_access_filter = objectClass=posixAccount
14 ldap_id_use_start_tls = true
15 ldap_uri = ldaps://ldap.google.com
16 ldap_tls_cert = /var/certificados/google-ldap.crt
17 ldap_tls_key = /var/certificados/google-ldap.key
18 ldap_schema = rfc2307bis
19 ldap_user_uuid = entryUUID
20
21 # Parámetro ldap_group_nesting_level
22 # (cuantos grupos anidados se evaluarán para cada usuario)
23 ldap_group_nesting_level = 1
24 cache_credentials = true
25
26 # Creación automática del grupo principal
27 # del usuario en base a los atributos LDAP.
28
29 auto_private_groups = true
30 # ruta para el home %u=usuario %d=dominio.
31 # Por ejemplo /home/test_ldap1@iessierradeguara.com/
32 override_homedir = /home/%u@%d
```

Configuración 4.4: Fichero `/etc/sssd/conf.d/01-iessierradeguara.com.conf`.

Los ficheros `google-ldap.crt` y `google-ldap.key` que aparecen en las líneas 16 y 17 del fichero 4.4, son los obtenidos en la configuración LDAP en el Google Workspace 4.2, sólo tienen permiso de lectura para el propietario `root`, y se han colocado en el directorio `/var/certificados` que se ha configurado con permisos de lectura y ejecución sólo para el propietario `root`.

```
1 root@vitalinux:/var/certificados# ls -la
2 total 16
3 dr-x------  2 root root 4096 may  8 04:27 .
4 drwxr-xr-x 15 root root 4096 may 22 16:42 ..
5 -r--------  1 root root 1274 may  8 02:50 google-ldap.crt
6 -r--------  1 root root 1700 may  8 02:50 google-ldap.key
```

Configuración 4.5: Muestra de los permisos en el directorio de los certificados.

4.3.3. Configuración NSS

Name Service Switch o servicio de resolución de nombres permite identificar un nombre de usuario con su id en el sistema y también a un nombre de grupo con su gid en el sistema de identidad. Su configuración en los sistemas Ubuntu y Debian se encuentra en `/etc/nsswitch.conf`.

Este fichero se modifica al instalar `sssd`, sin embargo, hay que asegurarse de que `sss` está después de `files` en las líneas en las que aparece.

Esto llevará a comprobar primero los usuarios locales del sistema, lo que es una buena política debido a la latencia de LDAP en remoto, cuando se quiere iniciar sesión con los usuarios locales, así se reduce sensiblemente la latencia en caso de querer iniciar sesión con un usuario local.

```
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:         files systemd sss
group:          files sss systemd
shadow:         files sss
gshadow:        files sss

hosts:          files mdns4_minimal [NOTFOUND=return] dns
networks:       files

protocols:      db files
services:       db files sss
ethers:         db files
rpc:            db files

netgroup:       nis
automount:      sss
```

Configuración 4.6: Fichero `/etc/nsswitch.conf`.

4.3.4. Configuración PAM. Directorio personal.

El servicio PAM está perfectamente integrado con SSSD, y al instalar el servicio SSSD se añade el módulo necesario dentro de los ficheros de configuración `/etc/pam.d/`. Lo primero que hay que especificar es activar la opción de creación del directorio de home en caso de ser un usuario nuevo para la máquina. Ya hay un módulo de PAM preparado para tal efecto que se denomina `pam_mkhomedir.so`. Con el objetivo de garantizar la privacidad de los archivos de cada usuario, se establecerá una política de permisos al directorio personal del tipo `0700`, esto es, permisos de lectura, escritura y ejecución para el propietario del directorio y ningún permiso para el resto de usuarios del sistema.

Para ello, el manual de `pam_mkhomedir.so` establece que la creación de directorio atenderá a lo establecido en el fichero `/etc/login.defs` para configurar los permisos. En concreto a los valores de `HOME_DIR` primero, y si este no estuviera establecido, al valor de `UMASK` (entendiendo el primero como el valor octal de permisos y el segundo como el valor de la máscara, es decir, lo contrario).

Así, estableciendo el valor `HOME_DIR` con el valor `0700` Y el valor de `UMASK` a `0077` dentro de ese fichero, debería bastar para la creación del directorio con los permisos requeridos, sin embargo, un bug bien documentado[7][8] nos indica que en la distribución Ubuntu el módulo no atiende a esos valores. Para solucionar esta problemática se debe forzar al módulo PAM la máscara de permisos.

Para ello, se edita el fichero `/usr/share/pam-configs/mkhomedir` añadiéndole el parámetro `umask=0077` después del módulo `pam_mkhomedir.so` quedando el contenido del mismo así:

```
1
2  Name: Create home directory on login
3  Default: no
4  Priority: 0
5  Session-Type: Additional
6  Session-Interactive-Only: yes
7  Session:
8          optional                        pam_mkhomedir.so umask=0077
9
```

Configuración 4.7: Fichero `/usr/share/pam-configs/mkhomedir`.

4.3.5. Configuración PAM. Asignación de grupos.

Por una parte, aunque LDAP sí permite la utilización de atributos para la elevación de privilegios en máquinas concretas, el servicio proporcionado por Google carece de esa opción, no pudiendo editar ni añadir atributos a los ficheros LDIFF desplegados por el servicio.

Por otra parte, la elevación de privilegios en Vitalinux se lleva a cabo mediante el comando sudo, cuya configuración reside en el fichero `sudoers`.

Hay establecidos varios perfiles de privilegios, el menor es el del estudiante (grupo `estudiantes` y, por retrocompatibilidad con otras versiones de Vitalinux, también el grupo `alumno`).

El siguiente nivel de privilegios es para el grupo `docentes` que tienen algunos permisos, como la gestión de las impresoras y otros dispositivos.

Por último, y con totales privelgios, el grupo `sudo`. Cabe recordar que la configuración de usuarios y grupos es homogénea en todas las máquinas con el sistema Vitalinux instalado.

Aprovechando el módulo de PAM `pam_group` que permite la asignación automática de grupos durante la autenticación, se realizará una correspondencia entre los grupos del dominio y estos grupos privilegiados de la máquina local.

¡Importante!: Se ha de tener en cuenta, tal y como aparece en el manual del módulo `pam_group`, que el uso del mismo requiere de que todos los sistemas de archivos accesibles en modo escritura por los usuarios sean montados con el parámetro `nosuid`[9].

Si esto no se hace, un usuario malicioso podría utilizar el bit `setgid` para recuperar la membresía de un grupo al que no pertenece pero al que una vez perteneció. Para garantizar que esto no pasa, se ha de montar el directorio `/home` desde una partición separada y añadiendo la opción `nosuid` en el fichero `/etc/fstab`.

Una vez hecha esta aclaración, para implementar la correspondencia o mapeo entre los grupos del dominio y los grupos locales de la máquina se han tenido que modificar varios ficheros.

Primero se ha modificado el fichero `/etc/security/groups.conf` que permite llevar a cabo la asignación automática de grupos locales a usuarios locales o remotos en el momento de la autenticación. Así, se ha configurado que:

- Todos los usuarios se incorporarán en el momento de la autenticación a los grupos `audio`, `cdrom`, `dialout`, `floppy`, `plugdev`, `sambashare` y `dip`.
- Si un usuario pertenece al grupo LDAP remoto vitalinuxsudo@iessierradeguara.com, al autenticarse se le añada al grupo `sudo`.
- A los usuarios que pertenencen al grupo remoto claustro@iessierradeguara.com, que se corresponde a todos los profesores, se los integra en los grupos locales correspondientes al usuario local docente, que son: docentes,adm,profesor y lpadmin

Para ello se han añadido las siguientes líneas al fichero `/etc/security/group.conf`.

```
# Configuración usuarios LDAP
*;*;*;Al0000-2400;audio,cdrom,dialout,floppy,plugdev,sambashare,dip
*;*;%vitalinuxsudo;Al0000-2400;sudo
*;*;%claustro;Al0000-2400;docentes,adm,profesor,lpadmin
...
```

Configuración 4.8: Fichero `/etc/security/group.conf`. Todos los usuarios, administradores y docentes.

Además, para los estudiantes, se han establecido reglas referidas a los grupos que los integran, todas ellas hacen que cualquier estudiante del centro educativo se integre en los grupos locales `estudiantes` y `alumno` que son los grupos que están asignados al usuario local estudiante. Sólo se pondrán aquí dos reglas, como ejemplo, para evitar que el documento se extienda demasiado:

```
...
*;*;%alumnado.1eso;Al0000-2400;estudiantes,alumno
*;*;%alumnado.2eso;Al0000-2400;estudiantes,alumno
...
```

Configuración 4.9: Fichero `/etc/security/group.conf`. Grupos de alumnos, recortado.

Para que el mapeo se haga efectivo, tiene que utilizarse el módulo `pam_group` durante el proceso de autenticación PAM. Para ello, en lugar de modificar los ficheros contenidos en `/etc/pam.d/`, Ubuntu proporciona un sistema de perfiles, concretamente en el directorio `/usr/share/pam-configs/`, que permite al comando `pam-auth-update` integrar las configuraciones dentro de los archivos automáticamente.

Así, se crea el fichero `/usr/share/pam-configs/vitalinux-ldap-groups-mapping` con el siguiente contenido:

```
Name: Activating /etc/security/groups.conf
Default: yes
```

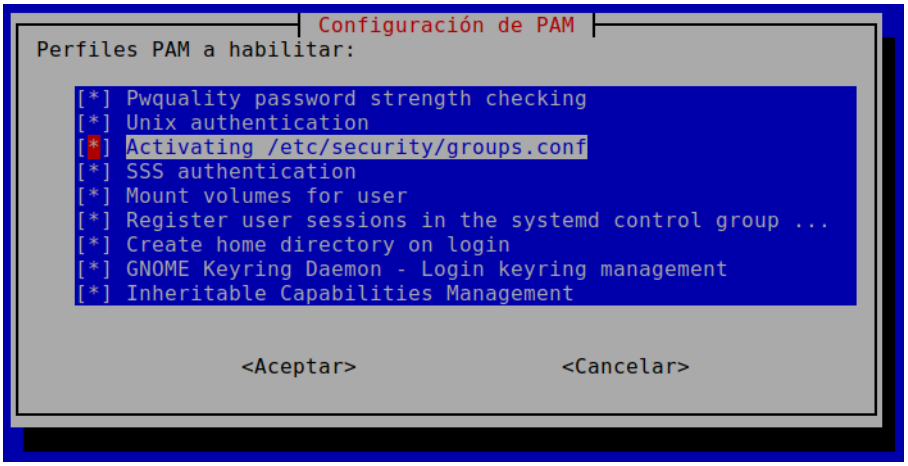


Figura 4.2: Configuración de PAM.

```
3 Priority: 129
4 Auth-Type: Primary
5 Auth:
6         required                pam_group.so
```

Configuración 4.10: Fichero `/usr/share/pam-configs/vitalinux-ldap-groups-mapping`.

Tras crear el archivo, el comando `pam-auth-update` nos muestra nuestro fichero de configuración como una de las opciones de configuración disponibles 4.2. Este proceso es equivalente a la ejecución del comando:

```
1 root@vitalinux:~# pam-auth-update --enable  vitalinux-ldap-groups-mapping
```

Configuración 4.11: Activación del perfil de PAM para la asignación de grupos mediante comando.

El uso de la activación de perfiles PAM tiene como resultado la modificaición segura de los ficheros que realmente tienen la configuración final que va a utilizar PAM y que se encuentran en `/etc/pam/pam.d`, en concreto, el perfil creado modifica el fichero `common-auth` dejándolo como aparece en la figura 4.3.

4.4. Configuración RADIUS

El servidor Radius permite una configuración de seguridad inalámbrica empresarial, en la que en lugar de tener una clave compartida para el acceso a la red inalámbrica, cada usuario se identifica con su usuario y contraseña ante el servidor Radius. Como objetivo de este proyecto está configurar un servidor radius interno que haga de pasarela de autenticación entre la wifi y el servidor LDAP de Google. Así el servidor Radius recibiría las peticiones de los dispositivos inalámbricos (usuario y contraseña) y las traspasaría al cliente LDAP confi1gurado en el panel de administración de Google Workspace que se encargaría de devolver una respuesta de acceso

```
dga@vitalinux:~$ cat /etc/pam.d/common-auth
#
# /etc/pam.d/common-auth - authentication settings common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.).  The default is to use the
# traditional Unix authentication mechanisms.
#
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules.  See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
auth    [success=3 default=ignore]      pam_unix.so nullok
auth    required                        pam_group.so
auth    [success=1 default=ignore]      pam_sss.so use_first_pass
# here's the fallback if no module succeeds
auth    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
auth    required                        pam_permit.so
# and here are more per-package modules (the "Additional" block)
auth    optional        pam_mount.so
auth    optional                        pam_cap.so
# end of pam-auth-update config
dga@vitalinux:~$
```

Figura 4.3: Fichero `/etc/pam/pam.d/common-auth` tras la aplicación del prefil creado para la asignación de grupos.

concedido. Entre las limitaciones de este servicio se encuentra la de 2.400 consultas SLDAP por minuto[10], lo que en el centro que nos atañe no debería de suponer ningún problema ya que el número total de usuarios es de unos 1.200 y existen turnos de asistencia para el profesorado y el alumnado. Además, en el momento de la implantación, se activará sólo para el profesorado.

4.4.1. Configuración del Servidor FreeRadius

La configuración del servidor Radius se ejecuta en varios planos, primero la máquina en la que se va a instalar, después la instalación y por último la configuración. En la configuración hay que tener en cuenta los módulos (modules o mods), los sitios (sites), los clientes (clients) y la parte de la autoridad certificadora.

El servidor

Para configurar el Radius, el departamento de informática del IES Sierra de Guara ha instalado una máquina virtualizada a través de Hyper-V dentro de un servidor Windows Server 2016 que proporciona servicio de Active Directory a los departamentos de Admnistrativo e Informática del centro educativo. A este servidor se ha podido acceder mediante una VPN también configurada por ellos. El servidor virtualizado, llamado `radius-google-ldap` tiene las siguientes características:

- Sistema Operativo: Ubuntu 24.04 LTS x86_64

- Host: Virtual Machine 7.0
- Kernel: 6.8.0-31-generic
- CPU: Intel Xeon E3-1220 v6 (1) @ 2.999GHz
- Memoria: 131MiB / 459MiB
- Dirección IP fija: 192.168.4.20

El servidor ha sido minimizado, es decir, se han eliminado los paquetes que no se utilizarán para hacer una máquina lo más ligera posible. La única finalidad de este servidor será la de actuar de pasarela de autenticación Radius hacia el servicio de LDAP. Tiene un usuario `sudo` y es accesible mediante un servicio SSH.

Instalación de los paquetes necesarios

La instalación de FreeRADIUS es trivial, basta con instalar el paquete `freeradius-ldap`, cuyas dependencias incluyen el paquete principal `freeradius` y todas sus dependencias.

```
1 sudo apt install freeradius-ldap
```

Configuración 4.12: Instalación del software FreeRadius.

Configuración de los Clientes de FreeRadius

La configuración de freeradius conlleva la creación de clientes y la instalación y configuración de módulos del programa. Los clientes se corresponden con las redes desde que se va a conectar un cliente wifi, en este caso, se configuran 2 clientes, uno genérico que gestionará todos los usuarios que se conecten a la red inalámbrica del centro y otro específico que gestionará los usuarios que se conecten desde la red inalámbrica del departamento de informática, ya que está separada y «nateada», por lo que todas las peticiones llegarán desde el lado WAN del router que la separa. Estas redes son:

- Red general: 192.168.4.0/22
- Router del departamento de informática: IP del router por el lado WAN siendo 192.168.4.120

Esta configuración se especifica en el fichero `/etc/freeradius/3.0/clients.conf` que, una vez eliminados todos los comentarios explicativos que vienen por defecto tiene el contenido siguiente:

```
1 client localhost {
2         ipaddr = 127.0.0.1
3         proto = *
4         secret = -#######-
5         require_message_authenticator = no
```

```
        nas_type         = other        # localhost isn't usually a NAS...
        limit {
                max_connections = 16
                lifetime = 0
                idle_timeout = 30
        }
}

client principales {
        ipaddr        = 192.168.4.0/22
        secret        = -#######-
}

client dpto-inf {
        ipaddr        = 192.168.4.120
        secret        = -#######-
}
```

Configuración 4.13: Fichero `/etc/freeradius/3.0/clients.conf` con la configuración de los clientes.

Nota: Se han sustituido por `-#######-` *todos los secretos. Esto será una constante en los ficheros de configuración que contengan información sensible.*

Configuración de FreeRadius. Certificados de Google.

Para este servicio de FreeRadius se ha configurado un servicio diferente de Google LDAP para poder gestionar desde el panel de administración de Google el acceso de los usuarios al servicio mediante las herramientas de acceso de grupos y unidades organizativas proporcionadas en el panel. Por lo que se generan otros certificados y se crea un usuario como administrador del servicio para configurarlo dentro de FreeRadius. Este usuario, se utilizará en el fichero de configuración del módulo de FreeRADIUS `ldap_google`.

El certificado se renombra a `certificate.crt` y el fichero de clave privada a `key.key` y ambos se descargan en el directorio `/etc/freeradius/3.0/certs/google`. Si no se renombraran, habría que cambiar las líneas que hacen referencia a ellos en el fichero de cónfiguración del módulo. Después, hay que dar propiedad y permisos al usuario `freerad` y el grupo `freerad` para los archivos creados, y eliminar los permisos del resto de usuarios:

```
chown freerad:freerad -R /etc/freeradius/3.0/certs/google
chmod -R 640 /etc/freeradius/3.0/certs/google
```

Configuración 4.14: Modificación de permisos para el certificado y el fichero de clave de Google.

Configuración de FreeRadius. Módulos.

La configuración de los módulos y de freeradius se establece mediante la creación de enlaces simbólicos desde el directorio `mods_avaliable` al directorio `mods_enabled` al estilo del servidor web Apache. Así se crean los enlaces simbólicos para activar los módulos `ldap_google` y `cache_auth`.

```
sudo ln -s /etc/freeradius/3.0/mods_available/ldap_google /etc/freeradius/3.0/mods_enabled
sudo ln -s /etc/freeradius/3.0/mods_available/cache_auth /etc/freeradius/3.0/mods_enabled
```

Configuración 4.15: Ejemplo de activación de módulos en FreeRadius.

Módulo LDAP La configuración del módulo ldap_google de FreeRADIUS se establece editando el fichero `/etc/freeradius/mods_enabled/ldap_google` para que quede como sigue, modificando el proporcionado por el FreeRADIUS:

```
ldap ldap_google {
        server = 'ldaps://ldap.google.com:636/'
        identity = '-#######-'
        password = '-#######-'
        base_dn = 'dc=iessierradeguara,dc=com'

        update {
                control:                  += 'radiusControlAttribute'
                request:                  += 'radiusRequestAttribute'
                reply:                   += 'radiusReplyAttribute'
        }

        user_dn = "LDAP-UserDn"
        user {
                base_dn = "ou=Users,${..base_dn}"
                filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})"
                scope = 'sub'
        }

        group {
                base_dn = "ou=Groups,${..base_dn}"
                filter = '(objectClass=posixGroup)'
                scope = 'sub'
                name_attribute = cn
                membership_attribute = 'memberOf'
        }

        options {
```

```
29                  chase_referrals = no
30                  res_timeout = 10
31                  srv_timelimit = 3
32                  net_timeout = 3
33                  idle = 60
34                  probes = 3
35                  interval = 3
36                  ldap_debug = 0x0000
37          }
38
39          tls {
40                  certificate_file = ${certdir}/google/certificate.crt
41                  private_key_file = ${certdir}/google/key.key
42                  require_cert        = 'allow'
43          }
44
45          pool {
46                  start = ${thread[pool].start_servers}
47                  min = ${thread[pool].min_spare_servers}
48                  max = ${thread[pool].max_servers}
49                  spare = ${thread[pool].max_spare_servers}
50                  uses = 0
51                  retry_delay = 30
52                  lifetime = 0
53                  idle_timeout = 60
54          }
55  }
```

Configuración 4.16: Fichero `/etc/freeradius/mods_enabled/ldap_google` con la configuración específica del LDAP de Google.

Nótese en las líneas 3 y 4 del fichero de configuración que esos valores entre comilla simple son los valores del usuario creado en el servicio LDAP desde el panel de Administración de Google especificados en 4.2 como «credenciales de acceso», y cuyos valores se omiten por razones de seguridad.

Módulo EAP El módulo EAP viene habilitado por defecto, pero hay que modificar ligeramente su configuración. En concreto hay que establecer la configuración por defecto a ttls, dentro de la configuración ttls hay que establecer el protocolo PAP y especificar google-ldap en la opción virtual_server. Por último, hay que habilitar la caché mediante el parámetro enable = yes dentro de su sección. Así el fichero del módulo /etc/freeradius/3.0/mods-enabled/eap queda de la siguiente manera:

```
1   eap {
2           default_eap_type = ttls
```

```
        timer_expire = 60
        ignore_unknown_eap_types = no
        cisco_accounting_username_bug = no
        max_sessions = ${max_requests}
        md5 { }
        gtc { auth_type = PAP }
        tls-config tls-common {
                private_key_password = -#######-
                private_key_file = ${certdir}/server.pem
                certificate_file = ${certdir}/server.pem
                ca_file = ${certdir}/ca.pem
                ca_path = ${cadir}
                cipher_list = "DEFAULT"
                cipher_server_preference = no
                tls_min_version = "1.2"
                tls_max_version = "1.2"
                ecdh_curve = ""
                cache {
                        enable = yes
                        lifetime = 24 # hours
                        store {         Tunnel-Private-Group-Id }
                }
                verify { }

                ocsp {
                        enable = no
                        override_cert_url = yes
                        url = "http://127.0.0.1/ocsp/"
                }
        }
        tls { tls = tls-common }
        ttls {
                tls = tls-common
                default_eap_type = pap
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                virtual_server = "google-ldap"
        }
        peap {
                tls = tls-common
                default_eap_type = mschapv2
                copy_request_to_tunnel = no
                use_tunneled_reply = no
                virtual_server = "inner-tunnel"
        }
```

```
48          mschapv2 {          }
49  }
```

Configuración 4.17: Fichero `/etc/freeradius/mods_enabled/eap` con la configuración específica del módulo EAP.

Configuración de FreeRadius. Sitios.

Además de los módulos, hay que configurar los "sitios" (sites) que son la primera línea del servicio ante las peticiones de los usuarios. En este caso, se debe activar el sitio inner_tunnel y google_ldap_auth mediante un método análogo al de los módulos creando enlaces simbólicos entre sites_available y sites_enabled.

El sitio google_ldap_auth contendrá la configuración específica para afrontar la autenticación contra Google y el sitio inner_tunnel tendrá la configuración del túnel seguro entre los clientes Radius y el servidor FreeRADIUS. La configuración del túnel seguro es primordial para garantizar la confidencialidad de la contraseña que tiene que viajar en claro hasta el servidor FreeRADIUS para que éste pueda autenticar contra el servicio LDAP de Google en nombre del usuario.

```
1  ln -s /etc/freeradius/3.0/sites_available/google_ldap_auth \
2                  /etc/freeradius/3.0/sites_enabled
3  ln -s /etc/freeradius/3.0/sites_available/inner_tunnel \
4                  /etc/freeradius/3.0/sites_enabled
```

Configuración 4.18: Ejemplo de activación de sitios en FreeRadius.

Sitio inner-tunnel La configuración de este túnel viene por defecto configurada para ldap, pero hay que especificar que se usará el módulo `ldap_google` sustituyendo las palabra ldap por ldap_google allí donde haga referencia la módulo (cuando aparece en minúsculas).

Además hay un cambio de sintaxis en la línea del primer `if`, en el que hay que cambiar`control.Auth_Type` que viene por defecto por `control:Auth_Type` (con el carácter dos puntos «:»).

```
1  server inner-tunnel {
2
3  listen {
4         ipaddr = 127.0.0.1
5         port = 18120
6         type = auth
7  }
8  authorize {
9          filter_username
10         chap
```

```
        mschap
        suffix
        update control { &Proxy-To-Realm := LOCAL
        eap { ok = return }
        files
        -sql
        -ldap_google
        expiration
        logintime
        pap
        if (!&control:Auth-Type && &User-Password) {
                update control { &Auth-Type := LDAP }
        }
}
authenticate {
        Auth-Type PAP { pap         }
        Auth-Type CHAP { chap }
        Auth-Type MS-CHAP {         mschap }
        mschap
        Auth-Type LDAP { ldap_google        }
        eap
}
session { radutmp }
post-auth {
        -sql
        if (0) {
                update reply {
                        User-Name !* ANY
                        Message-Authenticator !* ANY
                        EAP-Message !* ANY
                        Proxy-State !* ANY
                        MS-MPPE-Encryption-Types !* ANY
                        MS-MPPE-Encryption-Policy !* ANY
                        MS-MPPE-Send-Key !* ANY
                        MS-MPPE-Recv-Key !* ANY
                }
                update { &outer.session-state: += &reply: }
        }
        Post-Auth-Type REJECT {
                -sql
                attr_filter.access_reject
                update outer.session-state {
                        &Module-Failure-Message := &request:Module-Failure-Message
                }
        }
```

```
56 }
57 pre-proxy { }
58 post-proxy { eap }
59 } # inner-tunnel server block
```

Configuración 4.19: Configuración del sitio `inner-tunnel`.

Configuración de FreeRadius. Certificados y seguridad

FreeRadius garantiza la seguridad en la conexión por medio de certificados. La opción más habitual y más segura, es usar la Autoridad de Certificación incluida en el software de FreeRADIUS para crear nuevos certificados. Por defecto, FreeRADIUS se configura con unos certificados de test, para realizar las primeras pruebas, pero el manual recomienda para la puesta en producción regenerar todos los certificados. Para ello, en el directorio /etc/freeradius/3.0/certs existe un fichero Makefile que permite, mediante el comando make, reconfigurar los certificados y regenerarlos. Para regenerar los certificados de la autoridad certificadora y del servidor se utilizan los siguientes comandos:

```
1 cd /etc/freeradius/3.0/certs
2 make ca.pem
3 make ca.der
4 make server.pem
5 make server.csr
```

Configuración 4.20: Regeneración de los certificados de FreeRadius.

Durante este proceso, nos pedirá contraseñas para cifrar las diferentes claves privadas de los certificados, estas contraseñas serán las que haya que usar en los ficheros del módulo eap para el túnel cifrado en el parámetro `private_key_password` de la línea 10 de la Configuración 4.17.

Estos certificados, serán los que se utilicen en los dispositivos finales y los que permitirán cifrar la conexión punto a punto entre el servidor FreeRadius y el dispositivo Final de cara a la autenticación. Hay que tener en cuenta que el servidor FreeRadius recibe la contraseña en claro a través del túnel cifrado y es entonces cuando ejecuta la autenticación en nombre del usuario LDAP para garantizar el acceso a la red inalámbrica.

4.4.2. Configuración del ecosistema de puntos de acceso Ubiquiti

La configuración del ecosistema de puntos de acceso Ubiquiti está centralizada en un panel de administración disponible en línea, cuya administración se hace conjuntamente entre el equipo informático del Servicio Provincial de Educación de la Provincia de Huesca y el Departamento de Informática del IES Sierra de Guara. Para poder configurarlo, se proporcionaron unas credenciales de acceso a la interfaz web y, para evitar conflictos y minimizar riesgos, la configuración se hizo remotamente durante una videollamada y bajo la supervisión de varios miembros del departamento, entre ellos, el responsable de medios tecnológicos del centro en un el horario entre el turno de mañanas y el turno de tardes donde no hay apenas alumnado ni

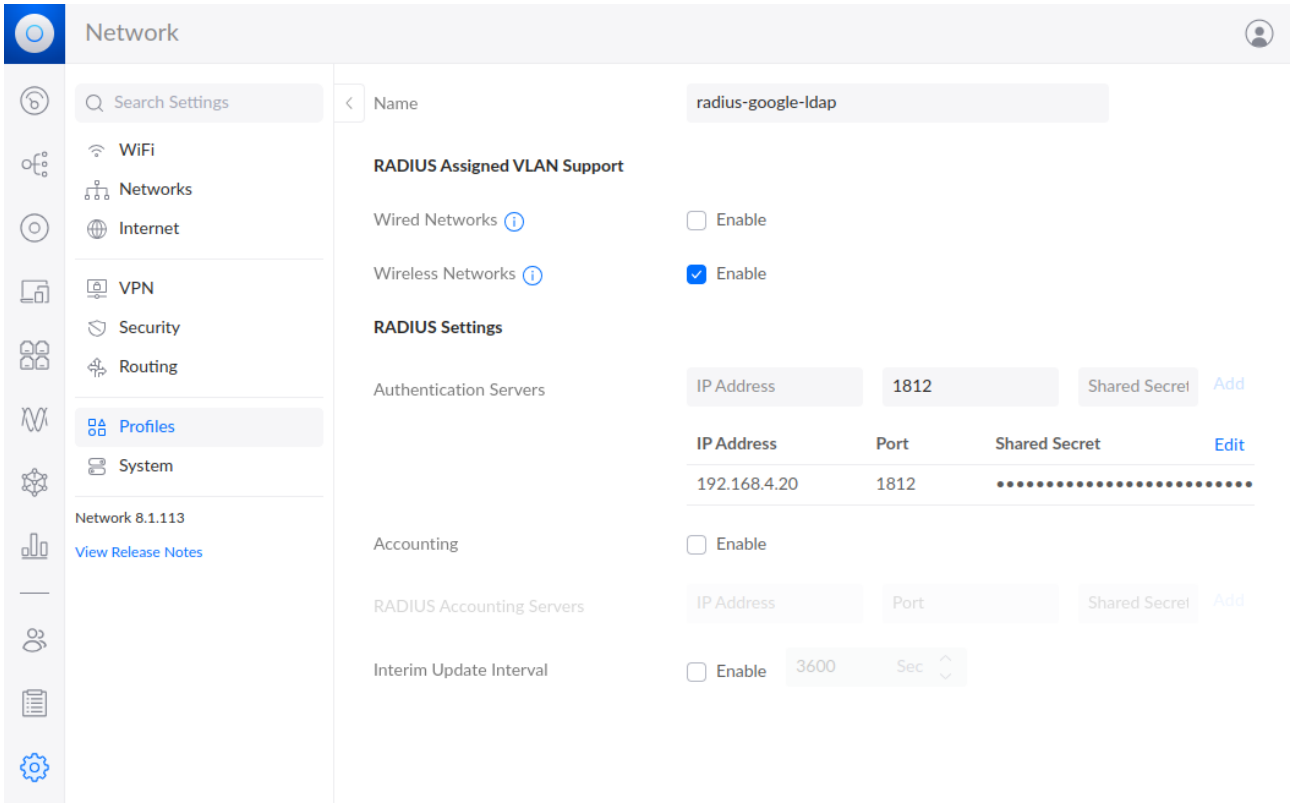


Figura 4.4: Captura de pantalla con la configuración del perfil Radius.

usuarios en el centro. Esto se hizo para tener posibilidad de actuar en el improbable caso de un fallo en la configuración que provocara una incidencia en el servicio de red inalámbrica.

Configuración del perfil de Radius

Una vez en el panel de administración del entorno de Ubiquti, hay que crear un perfil empresarial Radius que poder usar en una red inalámbrica. Para ello hay que navegar hasta `Settings > Profiles > Radius`.

Después se añade un nuevo perfil RADIUS, al que se le llama `radius-google-ldap`. Hay que entrar en el perfil, marcar la casilla `Wireless Networks` para que el perfil esté disponible para las redes inalámbricas, y añadir un nuevo servidor de autenticación con los siguientes valores, tal como aparece en la captura de pantalla 4.4.

- IP: `192.168.4.20`, que es la IP del servidor Radius.
- Port: `1812`, que es el puerto por defecto.
- Shared Secret: `-#######-`, que es la frase secreta que se estableció en la línea 4 del fichero de configuración 4.13.

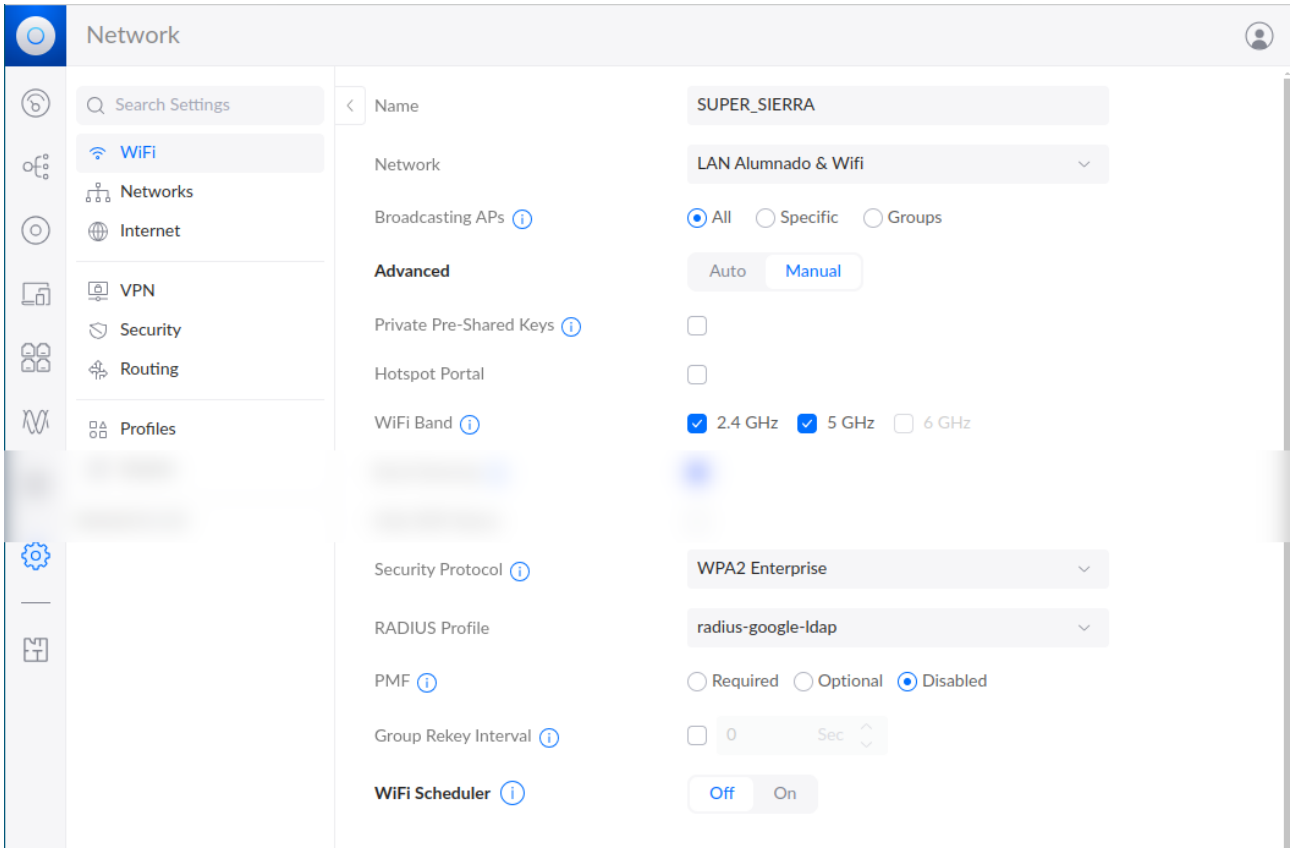


Figura 4.5: Captura de pantalla con las opciones configuradas para usar la autenticación Radius. Nótese que la captura ha sido recortada por el centro y en la parte difuminada habría muchas opciones que se han dejado por defecto.

Configuración de la nueva red inalámbrica

Finalmente, hay que configurar una nueva red inalámbrica que tendrá como método de seguridad WPA2 Empresarial, con el perfil Radius recién creado. Para ello, desde el panel web de administración hay que navegar hasta `Radios > Create New` y especificar los siguientes valores, dejando todo lo demás por defecto. Ver figura 4.5

- Name: SUPER_SIERRA, que será el nombre de la red inalámbrica (ESSID).
- Advanced: Manual.
- Security Protocol: WPA2 Enterprise.
- Radius Profile: radius-google-ldap, que es le perfil creado en el paso anterior 4.4.2.

4.4.3. Configuración de dispositivos

La configuración en los diferentes dispositivos **no es objeto de este TFM** debido a que al configurarse remotamente no es posible realizar las pruebas necesarias.

En las pruebas que se hicieron en local se pudo configurar en un proceso muy parecido un punto de acceso con el firmware OpenWRT contra un Servidor FreeRadius instalado en una Máquina Virtual Debian con el mismo procedimiento, autenticando contra los servidores LDAP de Google.

En cuanto a los dispositivos, se consiguió conectar con un equipo Windows 10, un móvil Android y un equipo Linux Debian usando los certificados de la autoridad certificadora creados en el punto análogo 4.20 para validar el servidor cuando la interfaz de configuración lo requería.

Sin embargo, tras la configuración de la red inalámbrica en el IES Sierra de Guara, en el Departamento de Informática han podido comprobar que funciona la configuración en dispositivos Android, Vitalinux, Windows 10, Windows 11 y apple ibook.

No han conseguido configurarlo en dispositivos iphone, ya que, al ser un sistema de seguridad empresarial según sus investigaciones, se necesita un perfil de configuración creado y firmado por una cuenta apple empresarial.

En los equipos de escritorio de apple sí que deja conectar tras mútliples advertencias de seguridad, al no estar firmado el archivo con una cuenta apple empresarial, pero no así en los dispositivos iphone. Para conseguir que funcione en todos los dispositivos, el equipo de informática del Centro debería contactar con Apple para conseguir una cuenta administrativa de apple y poder firmar los ficheros de configuración para dispositivos iphone, ipad y ibook.

Capítulo 5

Resultados

En este capítulo se analizan los resultados obtenidos y el posible impacto que puedan tener.

5.1. Autenticación LDAP en Vitalinux

La autenticación LDAP en Vitalinux ha sido un éxito, se consigue no solo iniciar sesión con la cuenta de usuario de Google, sino adquirir los permisos preestablecidos en el sistema Vitalinux en los roles *estudiante*, *docente* y *administrador*, para una integración ligera y una adaptación rápida de los usuarios ya acostumbrados a estos perfiles.

Así pues, la nueva configuración permitiría la personalización de los entornos en cada una de las máquinas (escritorio, idiomas, etc.) y la preservación de archivos propios y privados en la cuenta de usuario, aumentando su privacidad. Hay que recordar que los archivos y la personalización serán locales a la máquina y que no se tratan de «perfiles móviles».

5.2. Autenticación de Radius en red inalámbrica

La autenticación en radius se ha conseguido configurar satisfactoriamente así como la red inalámbrica asociada.

Capítulo 6

Conclusiones y trabajos futuros

6.1. Conclusiones

6.1.1. Conclusiones respecto al uso del servicio LDAP de Google

Problemas de latencia

En las diferentes pruebas realizadas para el inicio de sesión, se ha encontrado que la latencia del servidor para la autenticación es más de lo que el demonio SSSD espera. No en vano, hay que subir la opción de latencia LDAP dentro de la configuración del demonio para obtener una autenticación satisfactoria, si no el demonio agota el tiempo de espera por defecto y retorna error de autenticación.

Además, se ha visto que, en rarísimas ocasiones, la asignación de grupos en el inicio de sesión no se ha completado, debido a que no se han podido determinar los grupos del usuario de LDAP durante la autenticación lo que da lugar a problemas de permisos.

Esto puede ser debido también a los problemas de latencia, ya que la obtención de los grupos de usuarios se hace en peticiones LDAP posteriores a la comprobación del usuario para su autenticación.

No se puede concluir que el servicio de Google LDAP sea óptimo, aunque funciona la mayor parte de las veces.

Problemas de dependencia

El ecosistema de Google es cada vez más versátil y potente, incluyendo herramientas para la administración de sistemas como el servicio LDAP utilizado en este TFM. Sin embargo, esto crea una dependencia de los usuarios al uso de sus herramientas, lo que no favorece la compentencia. Además, siendo una empresa privada, pudiera llegar el día en que cambiaran su política con respecto a las cuentas educativas y comenzaran a cobrar por sus servicios.

LDAP de sólo lectura

El servicio de LDAP de Google es de solo lectura, por lo que aunque los sistemas operativos permiten realizar cambios de contraseña mediante el comando passwd, esas peticiones son

rechazadas por el servicio. Es obligatorio pues, para cambiar cualquier campo de los usuarios, hacerlo a través del panel de administración de Google.

Sin posibilidad de sudo dentro de LDAP

Aunque el estándar sí admite la posibilidad de incluir configuraciones de sudo en las respuestas LDAP para usuarios y grupos, y el demonio SSSD sí implementa esa solución, el ecositema de Google no permite hacer ningún cambio en las respuestas LDAP ni incluir campos al respecto, por lo que se pierde parte de la configuración que sería interesante en un entorno con mútiples máquinas.

6.1.2. Conclusiones respecto al demonio SSSD

El demonio SSSD funciona bien para autenticar usuarios con el servicio de Google LDAP. Es un sistema flexible que permite la configuración de varios dominios e implementa opciones para mejorar el rendimiento, como la profundidad de anidamiento de grupos, que evita llamadas recursivas en dominios grandes.

Además, las herramientas auxiliares del software, permiten borrar la caché y los registros de una manera sencilla.

6.1.3. Conclusiones respecto al proceso de adquisición de privilegios

El módulo `pam_group` es una manera sencilla y efectiva de coordinar los grupos del dominio con los grupos previamente configurados en la máquina.

Más que una solución, es una estrategia para evitar la falta de configuración de los parámetros sudo dentro del LDAP proporcionado por Google que funciona bien debido a la homogeneidad de las máquinas Vitalinux.

Riesgo de escalada de privilegios

Aunque LDAP sí permite configurar permisos de sudo para grupos y usuarios a través de los ficheros `.ldif`, el servicio proporcionado por Google no permite modificar ningún tipo de parámetro a este respecto. Así, se ha utilizado el módulo `pam_group` del servicio PAM, que concede a los usuarios autenticados la pertenencia a un grupo. Esto puede ocasionar una brecha de seguridad según aparece en el manual módulo, si un usuario con pertenencia a un grupo, crea un binario con el permiso setgid activado. Este usuario, podría, una vez fuera de ese grupo, recuperar la pertenencia al mismo a través de ese binario [9].

Así, habría que garantizar que los directorios con permiso de escritura de los usuarios que pertenezcan a grupos otorgados por el módulo `pam_group`, estén montados con la opción nosuid para evitar este hecho.

En nuestra solución, se crea una separación de la partición de la carpeta home y se ha montado con la opción nosuid para evitar este hecho. Además, se ha comunicado al equipo Vitalinux y se propone que se implemente una separación de la carpeta home en una partición diferente montada con la opcion nosuid en la instalación del sistema.

6.1.4. Conclusiones respecto al sistema Radius para red inalámbrica

El sistema Radius brinda seguridad, privacidad y comodidad a los usuarios que no tienen que aprender más contraseñas en su día a día. La configuración del ecosistema Ubiquiti es muy sencilla y la interfaz web es muy clara. La configuración del servidor FreeRadius, en combinación con el servicio LDAP de Google, ha sido una de las partes más costosas de implementar, debido a la cantidad de conceptos criptográficos y restricciones impuestas por el servicio de Google.

6.1.5. Éxito del Proyecto Vitalinux

Una de las partes fundamentales de la configuración de equipos de los centros educativos en Aragón es el proyecto Vitalinux, que gestiona remotamente miles de máquinas.

Una de las conclusiones de este TFM es que el proyecto y sus responsables están haciendo un gran trabajo, mostrando una gran disposición a la colaboración y adaptándose rápido a las necesidades reales de los centros educativos.

Tanto es así, que en el momento de escribir estas líneas, el equipo Vitalinux ya ha implementado un paquete con el despliegue de la solución de inicio de sesión y se está pilotando en algunos ordenadores del IES Sierra de Guara.

6.1.6. Seguimiento de la planificación

Para la elaboración de este trabajo se ha seguido una planificación elaborada en la introducción 1.5. Si bien el orden de las tareas ha sido el establecido y se ha seguido rigurosamente, es cierto que el tiempo planificado a priori para ello no fue calculado con precisión.

Algunas tareas como la configuración de los Servicios en la plataforma de Google y la configuración del ecosistema Ubiquiti fueron planificadas con demasiada holgura y en otras el tiempo establecido no fue suficiente, por ejemplo en la redacción final o en la configuración de Radius y del Demonio LDAP, que llevaron bastante más tiempo de lo esperado.

En general, la documentación del demonio SSSD y los ejemplos en la web no están muy extendidos, y el sistema LDAP que proporciona Google es muy estricto con la configuración de seguridad, por lo que hay que establecer correctamente todos y cada uno de los parámetros de los clientes.

6.1.7. Problemas detectados en la solución propuesta

Configuración en equipos portátiles, junto con la red Radius

SSSD cachea los usuarios y la autenticación, esto hace que cuando no hay conexión con el servidor LDAP, un usuario pueda iniciar sesión siempre y cuando hubiera iniciado sesión alguna vez con éxito en la máquina. Esto es una característica muy útil para entornos con conexión inalámbrica y máquinas portátiles ya que en caso de no disponer de alcance de red inalámbrica puedes seguir trabajando con normalidad. Sin embargo, un usuario LDAP que no haya iniciado sesión nunca en una máquina, no podrá iniciar sesión si el servidor LDAP no está disponible, por ejemplo, si no hay alcance de la red inalámbrica en un portátil.

Un problema se plantea si se unen las dos soluciones propuestas en este TFM, el inicio de sesión mediante LDAP y la conexión inalámbrica mediante un servidor Radius. En una máquina

Vitalinux, la pantalla de login no deja acceder a la configuración inalámbrica, por lo que un eventual inicio de sesión de un usuario nuevo en una máquina que tuviera al alcance sólo una red con seguridad WPA-Empresarial como la implementada en 4.4.2 no sería posible, ya que para iniciar sesión haría falta conexión de red y para configurar la red inalámbrica haría falta iniciar sesión. Este problema se puede superar con varias alternativas:

1. Conectar un cable de red la primera vez que se inicie sesión.
2. Iniciar sesión con una cuenta local, conectar a la red inalámbrica con las credenciales del usuario LDAP y cambiar de usuario. Nótese que:
   a) Esto sólo habría que hacerlo una vez, para iniciar sesión con nuestro usuario nuevo, después se puede iniciar sesión sin estar conectado a la red usando la autenticación cacheada.
   b) Habría que asegurarse de que no se guarda el perfil de red en el usuario local y, si se ha guardado, borrarlo.
   c) Una vez que se ha iniciado sesión ya se puede volver a conectar a la red mediante radius con el usuario LDAP.
3. Tener configurada una red con el acceso restringido a todo menos a la conexión con el LDAP de google y configurarla mediante /etc/network/interfaces, para asegurar que hay conexión antes del inicio de sesión.

Ninguna de estas alternativas puede considerarse una solución permanente sino estrategias para solucionar el problema puntualmente. En las líneas futuras 6.2 se plantean soluciones más adecuadas, como por ejemplo, usar el servidor Radius como método de autenticación o crear un script que, en caso de no haber conexión a internet, se ejecute entre la introducción de credenciales y la autenticación PAM para crear lo conexión mediante RADIUS.

6.2. Trabajos futuros y líneas de investigación

6.2.1. LDAP en local

El tiempo de latencia de LDAP es muy alto, y errático, tanto que se ha de modificar la configuración del demonio SSSD aumentando el valor de timeout en el fichero de configuración. Así, se propone como trabajo futuro implementar el sistema en el orden contrario, ya que según la documentación de Google, se puede conectar un servidor LDAP al dominio de Google y cargar todos los datos de las cuentas de LDAP dentro del Google Workspace.

Esta sería, pues, una configuración ideal, que permitiría mantener los datos en un LDAP local y que fuera Google el que actualizara los datos del dominio remoto, evitando así los problemas de latencia y mejorando el rendimiento general del sistema.

Además, blindaría al centro en caso de no poder utilizar el servicio de Google porque cambiaran sus terminos, y le otorgaría la flexibilidad necesaria de poder cambiar de servicio de correo manteniendo la información de las cuentas en el servidor LDAP.

6.2.2. Radius como autenticador de todo

Según lo estudiado, se podría establecer mediante el mismo demonio de sssd un método de autenticación utilizando el servidor Radius en funcionamiento. Esto permitiría que los certificados de Google no se tuvieran que propagar en cada máquina y que la configuración en las máquinas no estuviera sujeta a los cambios en el servicio de Google.

El servicio de autenticación Radius no se puede evitar, ya que es el responsable de la autenticación en el inicio de sesión en la red inalámbrica, pero sí se podría aprovechar también para el inicio de sesión en las máquinas Vitalinux.

6.2.3. Cuotas de usuario en el inicio de sesión

Una de las líneas de trabajo futuro sería el establecer límites de cuota de disco para las máquinas Vitalinux. Los perfiles no son móviles, sino que toda la información se guarda en la máquina en la que se inicie sesión en el carpeta personal del usuario, con lo que el espacio disponible podría reducirse a lo largo del tiempo, según fueran iniciando sesión más y más usuarios.

En este trabajo no se ha planteado como objetivo, ya que la configuración en sistema Vitalinux se hace de manera centralizada y es común a todos los institutos, sin embargo, se ha puesto en conocimiento al Equipo Vitalinux de esta situación, para que estudien la activación de un sistema de cuotas.

6.2.4. Resolución del problema de los portátiles y la red Radius en el primer inicio de sesión

Para solucionar el problema apuntado en 6.1.7 se proponen varias soluciones que pueden ser objeto de trabajos posteriores:

- Configurar una red inalámbrica con clave WPA-PSK, con acceso filtrado exclusivamente al LDAP que esté configurada en el inicio de sesión en el fichero `/etc/network/interfaces` o en un perfil de network-manager con prioridad mínima, pero con acceso a todos los usuarios para que se conecte antes del inicio de sesión. Esta red no permitiría otras conexiones diferentes a las de LDAP, pero sí permitiría la autenticación y por tanto el inicio de sesión.

- Crear un script de configuración que se interponga entre el inicio de sesión y la autenticación, que cree el perfil de conexión y conecte la red inalámbrica antes del proceso de autenticación.

- Explorar la autenticación mediante Radius también para el inicio de sesión.

6.2.5. Conexión de otras aplicaciones Web

Aprovechando los conocimientos generados en este TFM, se propone la conexión de otras aplicaciones Web al servicio LDAP de Google, como por ejemplo NextCloud para compartición de archivos o una aplicación Moodle de gestión educativa.

Capítulo 7

Bibliografía

Referencias

[1] J. J. de Haro Ollé. «Guía de Software Libre en Educación, Linux y educación», Instituto Nacional de Tecnologías Educativas y Formación del Profesorado. (), [En línea]. Disponible en: https://descargas.intef.es/cedec/proyectoedia/guias/contenidos/guiasoftwarelibre/linux_y_educacin.html (visitado 01-04-2024).

[2] A. Blázquez. «Programación General Anual Curso 2023/2024», IES Sierra de Guara. (2023), [En línea]. Disponible en: https://iessierradeguara.com/wordpress/wp-content/uploads/PGA-2023-24.pdf (visitado 02-06-2024).

[3] A. A. Z. A. Ibrahim, D. Kliazovich, P. Bouvry y A. Oleksiak, «Using Virtual Desktop Infrastructure to Improve Power Efficiency in Grinfy System», en *2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 2016, pp. 85-89. DOI: 10.1109/CloudCom.2016.0028. [En línea]. Disponible en: https://ieeexplore.ieee.org/document/7830669.

[4] A. Boring. «LDAP Schemas: RFC2307 vs RFC2307bis». (jul. de 2019), [En línea]. Disponible en: https://unofficialaciguide.com/2019/07/31/ldap-schemas-for-aci-administrators-rfc2307-vs-rfc2307bis/ (visitado 29-03-2024).

[5] A. Romero y N. Sancho. «Información del proyecto Vitalinux». (2024), [En línea]. Disponible en: https://docs.vitalinux.educa.aragon.es/info/ (visitado 12-04-2024).

[6] «Web de Migasfree», Migasfree. (2024), [En línea]. Disponible en: https://migasfree.org (visitado 03-04-2024).

[7] A. Murray. «Private home directories for Ubuntu 21.04 onwards». (nov. de 2020), [En línea]. Disponible en: https://discourse.ubuntu.com/t/private-home-directories-for-ubuntu-21-04-onwards/19533 (visitado 09-05-2024).

[8] A. Murray. «pam-mkhomedir does not honor private home directories». (ene. de 2022), [En línea]. Disponible en: https://bugs.launchpad.net/ubuntu/+source/pam/+bug/1957024 (visitado 09-05-2024).

[9] A. G. Morgan et al. «pam_group (8) Linux man page». (2023), [En línea]. Disponible en: https://linux.die.net/man/8/pam_group (visitado 12-04-2024).

[10] «Google Admin SDK, Límites y cuotas de la API», Google Workspace. (mar. de 2024), [En línea]. Disponible en: https://developers.google.com/admin-sdk/directory/v1/limits (visitado 20-05-2024).

[14] J. Sermersheim. «Lightweight Directory Access Protocol (LDAP): The Protocol». (jun. de 2006), [En línea]. Disponible en: https://www.rfc-editor.org/info/rfc4511.

Bibliografía adicional

[11] S. G. Archambault, «Student privacy in the digital age», *BYU Educ. & LJ*, 2021.

[12] Google Workspace Admin Help. «Secure LDAP: Connect LDAP-based apps and services», Google inc. (2019), [En línea]. Disponible en: https://support.google.com/a/topic/9048334 (visitado 12-04-2024).

[13] Debian Wiki Team. «LDAP Utilities». (2021), [En línea]. Disponible en: https://wiki.debian.org/LDAP/LDAPUtils (visitado 30-04-2024).

[15] Canonical Ubuntu Team. «How to set up SSSD with LDAP», Canonical Ubuntu. (abr. de 2024), [En línea]. Disponible en: https://ubuntu.com/server/docs/how-to-set-up-sssd-with-ldap (visitado 05-04-2024).

[16] «LDAP for Rocket Scientists», Zydax Inc. (ene. de 2022), [En línea]. Disponible en: https://www.zytrax.com/books/ldap/ (visitado 02-03-2024).

Glosario

apt *Advanced Package Tool*, herramienta de gestión de paquetes utilizada en sistemas basados en Debian.

EAP *Extensible Authentication Protocol*, protocolo de autenticación extensible utilizado en redes de computadoras.

LDAP *Lightweight Directory Access Protocol*, protocolo ligero de acceso a directorio [14]

LDIF *LDAP Data Interchange Format*, formato estándar para la representación de datos de directorio LDAP.

LightDM Gestor de sesiones ligero para entornos gráficos en sistemas Unix.

Makefile Archivo de configuración utilizado por el comando `make` para automatizar la compilación de programas u otros procesos.

Migasfree Herramienta de gestión y despliegue de software en entornos GNU/Linux, especialmente diseñada para administraciones públicas y centros educativos.

MS-CHAP *Microsoft Challenge-Handshake Authentication Protocol*, protocolo de autenticación basado en el protocolo CHAP de Microsoft.

NSS *Name Service Switch*, servicio de resolución de nombres. Permite resolver identificadores de usuario y grupos en base a sus nombres y viceversa usando diferentes fuentes de datos como archivos locales, directorios u otras bases de datos

PAM *Pluggable Authentication Modules*, marco flexible para la autenticación de usuarios en sistemas Unix.

PEAP *Protected Extensible Authentication Protocol*, protocolo de autenticación que encapsula EAP dentro de una conexión TLS.

PSK *PreShared Key*, clave previamente compartida. Se refiere a una clave de cifrado que es conocida por ambas partes de la comunicación.

RADIUS *Remote Authentication Dial-In User Service*, servicio de autenticación y autorización centralizado para redes.

SSSD *System Security Services Daemon*, demonio que proporciona acceso a diferentes servicios de autenticación y base de datos.

TLS *Transport Layer Security*, protocolo criptográfico diseñado para proporcionar comunicaciones seguras a través de una red.

TTLS *Tunneled Transport Layer Security*, extensión del protocolo TLS que proporciona una capa adicional de seguridad en túneles de autenticación.

Ubuntu Distribución de Linux basada en Debian, conocida por su facilidad de uso.

WPA *Wi-Fi Protected Access*, Acceso protegido a Wi-Fi es un estándar de seguridad para redes inalámbricas que fue creado para proteger las conexiones inalámbricas de manera segura.

WPA-Enterprise *Wi-Fi Protected Access Enterprise*, variante del estándar WPA que utiliza un servidor de autenticación para mejorar la seguridad.

XFCE Entorno de escritorio ligero para sistemas Unix, conocido por su velocidad y bajo consumo de recursos.