Jose Bermejo Porcuna
David Ferrero Carmona
Administració de Sistemes Informàtics en Xarxa
2021-2022

Licencia

Datos del proyecto y resumen

Datos del proyecto	
Título:	NextLDAP
Autores	David Ferrero Carmona, Jose Bermejo Porcuna
Profesores:	Óscar Torrente, Fernando Porrino
Breve descripción:	Este proyecto se basa en desarrollar una infraestructura para poder facilitar la tarea a los usuarios, para que puedan usar cualquier ordenador del centro como si siempre fuera el mismo, es decir cuando el usuario deja de usar la maquina esta sube los cambios a la nube y cuando inicia sesión en cualquier ordenador los datos del usuario se bajan y puede seguir usando sus archivos. Las funcionalidades principales serán la siguientes: - Subir y bajar archivos automáticamente. - Autogenerar usuarios en LDAP -> Nextcloud - Conexión SSO LDAP -> Nextcloud - Acceder a la nube “Nextcloud” desde casa. - Sistema de alta disponibilidad

Introducción

Este documento presenta el proceso de creación y desarrollo de una infraestructura mediante la cual cualquier usuario podrá disponer de sus ficheros en el escritorio personal, los cuales estarán almacenados remotamente en la red, independientemente del ordenador en el cual inicia sesión.

Para realizar este proyecto se usará principalmente LDAP para la autenticación de usuarios complementado con el uso de un servidor Nextcloud para almacenar los archivos personales de cada usuario(alumno/profesores/secretaria).

El sistema operativo utilizado en el servidor y en el cliente será Ubuntu, dado que es software libre y de código abierto.
Los diferentes servidores que se usarán estarán alojados en la nube de Amazon, AWS.

PARTE I. Gestión del proyecto

Objetivos

Los objetivos planteados por el equipo de desarrollo para este proyecto serían los siguientes:

- Instalar y configurar una “nube privada” Nextcloud para almacenar los ficheros de los usuarios.

- Instalar y configurar un servidor LDAP para que puedan iniciar sesión con su usuario desde cualquier máquina del centro.

- Carga y descarga de los ficheros de la máquina local al Nextcloud y viceversa mediante un script.

- Configurar un cliente LDAP para las máquinas del centro.

- Hacer que se sincronice el servidor LDAP con el Nextcloud para crear los usuarios automáticamente en este y que se puedan manejar los ficheros mediante su nombre de usuario.

- Tener un sistema de backups del Nextcloud y LDAP. Y junto a eso un sistema de alta disponibilidad.

- Realizar un script para que cuando se bajen los ficheros del Nextcloud se coloquen de manera automática en sus carpetas correspondientes.

- Realizar un script para que cuando se cierre la sesión los ficheros del usuario, se suban a su cuenta de Nextcloud y se borren de la máquina física.

- Automatizar la creación de usuarios al servidor LDAP.

- Hacer que el sistema LDAP + Nextcloud tenga un nivel de seguridad alto.

Entorno del proyecto

Contexto

El contexto de este proyecto surge a partir de ver lo común que es que a una persona que está trabajando en un sitio (por ejemplo, el instituto) y tiene que continuar este trabajo en otro lugar (por ejemplo el domicilio de esa persona), se le olvida subir o guardarse el fichero para continuar trabajando en él.

Justificación

Se ha optado por crear una infraestructura para que los ordenadores de un centro educativo no dependan de su almacenamiento local para almacenar los datos de los usuarios(Alumnos/profesores/secretaría) y estos puedan tenerlos en una nube propia donde la privacidad de sus datos está garantizada, de esta forma pueden tener acceso ellos desde sus casas o desde cualquier ordenador del centro.

Una de las justificaciones por la que usamos LDAP para hacer una cuenta para cada alumno es para que tengan mas privacidad en sus archivos ya que cada cuenta esta aisladas de las demás y lo otros alumnos no pueden acceder(no pueden conectar un disco duro por ejemplo).

Soluciones existentes

No se han encontrado soluciones existentes sobre la temática de este proyecto. Lo más similar que se ha encontrado sería Google Drive, pero no es del todo igual ya que este proyecto está dirigido más a trabajar de forma local y no en la nube.
En Google Drive se encuentran los archivos y con los diferentes programas que ofrece Google se puede trabajar en estos archivos en la propia nube, mientras que en este proyecto, los archivos se encuentran en la nube pero se descargan y se trabaja sobre ellos de forma local.

Alcance

Situación actual

La situación actual del proyecto es planificar qué tareas va a realizar cada integrante del equipo, plantear cómo se va a implementar los servidores LDAP, Nextcloud, que software complementará a estos dos para añadirle más seguridad, persistencia y disponibilidad al producto final. Puesto que este proyecto parte de cero se tiene que investigar cómo funcionan estas tecnologías y de qué formas se pueden integrar unas con las otras.

Los servidores LDAP que se plantearon usar fueron OpenLDAP y 389 DS:
389 DS:

389 DS	
PROS	CONTRAS
Gran número de documentación disponible de antemano	Inexperiencia del equipo de desarrollo en el uso de este
Notable capacidad de adaptabilidad	Escasa documentación y comunidad en la red
Gran tolerancia a errores	

OpenLDAP	
PROS	CONTRAS
Gran número de documentación y comunidad en internet	Inexperiencia del equipo de desarrollo en el uso de este
Gran capacidad de escalabilidad	Menor rendimiento en comparación con otros servidores LDAP.
	Gran cantidad de experiencia requerida para operar con él debido al hecho de que funciona por línea de comandos en su gran mayoría.

El servidor LDAP que se ha planteado usar el equipo de desarrollo en un primer momento, es el 389 DS, puesto que se cuenta con documentación ofrecida por profesores y según la primera investigación se ha llegado a la conclusión de que este servidor suele tener mayores capacidades de adaptabilidad, suele ser más tolerante ante configuraciones que puedan tener algún error. La otra principal tecnología que se quiere usar es Nextcloud. Se ha elegido Nextcloud, en contraparte a otras tecnologías como ownCloud, puesto que el equipo de desarrollo ya había trabajado con ella en proyectos personales. Este ofrece al proyecto una gran cantidad de extensiones para añadirle funcionalidades, conectores para que se puedan integrar con una gran cantidad de tecnologías

como por ejemplo(LDAP, Google Drive,etc...). Esta “nube privada” tiene la también la posibilidad de poder añadir, si fuese necesario, hasta editores de texto colaborativos, conversores de video, editores de fotografías, etc...

El equipo de desarrollo ha decidido alojar los servidores que se usen en este proyecto en AWS, aprovechando que se contaba con dos cuentas en este sitio con un saldo de 100$ cada una. Se ha escogido esta opción por el hecho de que no hay que preocuparse de mantener la máquina donde está el servidor. También permite acceder rápidamente a la máquina del servidor desde cualquier sitio.
No hay que hacer una inversión monetaria(comprar el equipo, etc) antes de montar la máquina ya que se paga por el uso que se haga de la máquina.

El sistema de backups se realizará mediante mysqldump, puesto que, después de una investigación sobre realizar backups de NextCloud, se ha determinado que es la única manera de poder realizar un backup del Nextcloud.

Se planteó la idea de realizar backups incrementales, pero Nextcloud no guarda los ficheros en la propia base de datos, los guarda en una carpeta que después se hace referencia en la base de datos, esto imposibilita realizar backups incrementales, esta es otra de las razones por lo que solo se puede realizar el backup con mysqldump.

Adicionalmente a mysqldump, por el hecho que se ha mencionado en el párrafo anterior, se debe hacer un backup también de la carpeta donde se encuentren los ficheros que guarda Nextcloud.

Alcance y posibles obstáculos

El objetivo del proyecto es realizar un sistema mediante el cual un usuario no tenga sus ficheros en un ordenador en local, que los tenga en la “nube” privada del centro, de esta forma tendrá una copia de seguridad y podrá cambiar de sitio, es decir podrá cambiar de ordenador sin perder ningún fichero. El funcionamiento que se espera conseguir será el siguiente: el usuario iniciará sesión y se bajarán sus archivos al ordenador donde se encuentre en ese momento, estos se montarán en sus respectivas carpetas y cuando el usuario cierre sesión estos se comprimirán y se almacenarán en su carpeta personal dentro de Nextcloud con la fecha y el dia para que sirva en caso de pierda algún fichero de backup. Gracias a esto el usuario podrá trabajar de manera local sin preocuparse de almacenar su trabajo en cualquier sitio(pendrive,almacenamiento en la nube externo al centro, etc..).

Posibles dificultades:

- Problemas de integración entre los diferentes componentes que conforman el proyecto.

- Inexperiencia del equipo de desarrollo a la hora de trabajar con las diferentes tecnologías que se usarán en la realización del proyecto.

- Falta de documentación relacionada con las diferentes tecnologías por el hecho de que no se han podido encontrar soluciones existentes o meramente similares.

Metodología, validación y herramientas de seguimiento

Este proyecto principalmente seguirá la metodología Scrum con la finalidad de gestionar las prioridades del proyecto, ver las tareas. Esta forma de trabajar permite al equipo trabajar de forma colaborativa, utilizando principalmente un tablero compuesto por distintas columnas para hacer el seguimiento de qué tareas quedan por realizar, que está en progreso y que se ha finalizado, así de esta forma se puede realizar un seguimiento de la evolución del proyecto y poder ver el estado de las tareas.
La siguiente lista de tareas es la que el equipo de desarrollo estableció para este proyecto. En esta lista se pueden observar las tareas iniciales que se establecieron en las primeras fases del proyecto, por lo tanto está sujeta a cambios por los posibles contratiempos que se puedan presentar en un futuro.
A la hora de repartir las tareas, el equipo de desarrollo se basó en intereses personales de los miembros del equipo (cada miembro del equipo eligió qué tareas quería hacer). Este método de asignación de tareas fue el escogido puesto que así cada miembro del equipo trabaja en el campo que más le apasiona, y por lo tanto puede afectar positivamente a la realización del proyecto.

Amarillo: Jose Bermejo.
Rojo: David Ferrero.

Presupuesto

Elementos de la estimación inicial

Tras un primer estudio realizado por el equipo, se ha llegado a dos tipos de presupuestos posibles: uno en el que la potencia de computación se encuentra en la nube (AWS) y otro presupuesto en el que se hace todo en local, es decir con servidores físicos.

Presupuesto (Máquinas en la nube)	Marzo	Abril	Mayo	Total
Sueldo medio Administrador de sistemas (David Ferrero)	2300	2300	2300	6900
Sueldo medio Administrador de sistemas (Jose Bermejo)	2300	2300	2300	6900
Instancias AWS*	230	230	230	690
Licencias Software	0	0	0	0
	4830	4830	4830	14490

Presupuesto (Máquinas Locales)	Marzo	Abril	Mayo	Total
Sueldo medio Administrador de sistemas (David Ferrero)	2300	2300	2300	6900
Sueldo medio Administrador de sistemas (Jose Bermejo)	2300	2300	2300	6900
Licencias Software	0	0	0	0
Servidor principal	1228	0	0	1228
Servidor Secundario	620	0	0	620
	6448	4600	4600	15648

Instancias AWS* -> se refiere a que este precio puede ser variable en función de si hay incidencias con la instancia principal y se requiere de una segunda instancia, el precio máximo ascendería a unos 460€ aproximadamente al mes

Justificación de los costos estimados

Para calcular los presupuestos expuestos anteriormente el equipo de desarrollo a tenido en cuenta los siguientes puntos:

- Inicialmente se le asignará 1Gb a todos los usuarios del Nextcloud, por lo tanto la máquina como mínimo necesitará 1TB de espacio, para este presupuesto se le ha asignado 1,250TB, como se requiere de una alta velocidad de acceso se han seleccionado SSD lo que aumenta el coste de las maquina.

- Los sueldos se han calculado en base al sueldo medio de un administrador de sistemas.

- Puesto que todo el software utilizado en el desarrollo es OpenSource, no se requiere de un desembolso monetario adicional.

- En el presupuesto de servidores en local se han seleccionado los servidores tanto el principal como el secundario en base a los requisitos básicos establecidos por los desarrolladores oficiales de las tecnologías escogidas, estos requisitos son los siguientes:

    - El sistema operativo de la máquina tiene que tener como mínimo para instalar las tecnologías 1GB de almacenamiento disponible.

    - 4Gb de memoria RAM

    - Un procesador de 32/64 bits de 2 Ghz o más.

- En el presupuesto con los servidores en la nube lo que encarece el presupuesto es el hecho de requerir más almacenamiento, el precio de una instancia al mes sería de unos 230€ aproximadamente, con la posibilidad de tener que ampliar a un instancia más en caso de incidencia con la instancia principal.

Planificación temporal

Fases del proyecto

Este proyecto tiene 3 bloques:

1. El primer bloque, nombrado servidor, trata sobre todo aquello relacionado con la creación de la infraestructura que se plantea en este proyecto.
   Dentro de este bloque se pueden encontrar 3 apartados:
    - Análisis: en este apartado es donde se definirán diferentes aspectos sobre el proyecto (objetivos que se quieren conseguir en el proyecto, la tecnología que se usará y los diferentes requisitos que el proyecto deberá cumplir).
    - Diseño: en este apartado es donde se planificarán y diseñarán diferentes aspectos del proyecto (la arquitectura que tendrá, los diferentes métodos para añadir seguridad al proyecto y cómo será la persistencia de los datos que se manejarán en el proyecto).
    - Desarrollo: en este apartado es donde se llevará a cabo el proyecto, donde el diseño se llevará a la realidad.
    - Pruebas: en este apartado es donde se realizarán diferentes pruebas para encontrar errores y mejorar el funcionamiento del proyecto.
2. El segundo bloque, nombrado memoria, trata sobre la redacción de la memoria y su revisión final.
3. El tercer bloque es donde se preparará la defensa del proyecto.

Planificación inicial

NextLDAP	Horas Planificadas
Proyecto	198
Servidor	**179**
Analisis	**13**
Objetivos	3
Requisitos	6
Tecnologia	4
Diseño	**12**
Arquitectura	4
Seguridad	4
Persistencia	4
Desarrollo	**152**
Estrategia de desarrollo	2
Instalación y configuración de Nextcloud	30
Instalación y configuración de LDAP	30
Integración Nextcloud+LDAP	35
Configurar cliente Ubuntu	30
Añadir capas de seguridad	25
Pruebas	**2**
Rendimiento	2
Memoria	12
Redacción	10
Revisión	2
Presentación	7
Presentación oral	2
Matereiales(PowerPoint,etc..)	5

Soluciones a eventuales desviaciones

Se han contemplado posibles desviaciones en la planificación respecto a la configuración del servidor LDAP, puesto que esta tecnología es bastante nueva para el equipo de desarrollo, tiene poca o nula experiencia con esta tecnología.
La manera que se ha planteado para solucionar estas posibles desviaciones en este ámbito es dedicar, en caso de que fuera necesario, horas de otros apartados.

Justificación de la finalización a tiempo

Punto de control

Cambios respecto a la planificación inicial

Respecto a la planificación inicial, se ha acortado el tiempo en el apartado de instalación y configuración de Nextcloud, puesto que el equipo de desarrollo no encontró ningún contratiempo. Este recorte de tiempo también se debe a que esta tarea fue más fácil de lo que se esperaba.
A pesar de esta disminución de tiempo en el apartado anterior, ha habido un incremento en la duración de la configuración de LDAP, esto debido a que el equipo de desarrollo encontró un contratiempo a la hora de configurar el servidor LDAP y un cliente Ubuntu para que se pudiera hacer login a este mediante el servidor LDAP. Este contratiempo se trató de que para que el cliente LDAP pueda verificar al usuario tiene que hacer una consulta al servidor en modo anónimo por lo que el equipo tuvo que implementar una ACL para modificar los permisos de las conexiones anónimas.
En el apartado de configuración del cliente se ha utilizado un poco más del tiempo del estipulado debido al desconocimiento de ciertas tecnologías implicadas en este apartado.
Concretamente en cómo subir ficheros a Nextcloud, puesto que este no acepta subir ficheros zip por terminal por defecto y al equipo de desarrollo le costó encontrar una solución a esto.
El equipo de desarrollo se percató durante la realización de los scripts relacionados con las carpetas de los usuarios (ver anexo 7 para ver los scripts que se realizaron en ese momento) que está opción requeriría de mucho tiempo de desarrollo y por lo tanto se decidió usar las opciones nativas que ofrece Ubuntu y Nextcloud. Finalmente para montar la carpeta remota que cada usuario tiene en Nextcloud se ha utilizado una funcionalidad que el propio Ubuntu ya tiene de serie que es las cuentas en línea, esta funcionalidad ofrece la integración nativa de un usuario de Nextcloud en el Nautilus como si se estuviera trabajando en local.

Consecuencias de los cambios respecto a los objetivos y desarrollo del proyecto

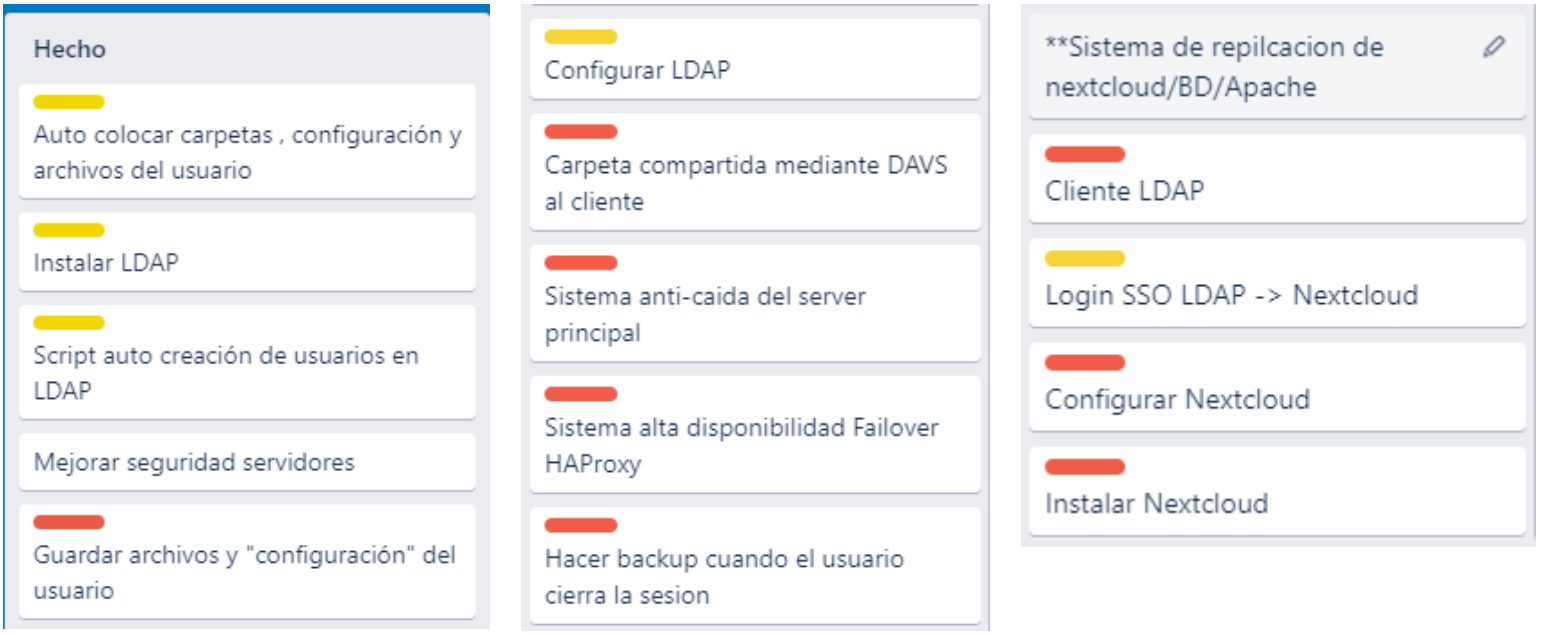
Los cambios realizados cambian los objetivos iniciales del proyecto puesto que se 2 objetivos se sustituyen por uno nuevo. Como se ha mencionado anteriormente el equipo de desarrollo se percató que realizar los scripts relacionados con las carpetas de los usuarios(subir y bajar las carpetas de Nextcloud y colocarlas en el escritorio) iba a consumir mucho tiempo de desarrollo por lo que se decidió buscar soluciones nativas y se encontró que Ubuntu y Nextcloud ofrecen soluciones nativas para que el usuario pueda interactuar con sus carpetas (perfiles móviles).
El resto de cambios en la planificación són menos relevantes puesto que no suponen un giro en el desarrollo del proyecto, son solo recortes de tiempo o incrementos de tiempo que al final acaban siendo neutros.

Situación del proyecto en el punto de control

Como se ha mencionado en el punto de cambios respecto a la planificación inicial se ha instalado y configurado el servidor LDAP y el Nextcloud. En cuanto a la integración de LDAP con la nube Nextcloud, se realizó más o menos en la planificación que se había estipulado inicialmente, el equipo no entró grandes contratiempos más allá de la inexperiencia al usar la tecnología LDAP y Nextcloud.
Respecto a la fase de configuración del cliente Ubuntu(que será la configuración que deberán tener las máquinas del centro) está también realizada según la planificación inicial.
En esta fase, a pesar de estar acabada, se buscará la manera de perfeccionarla si es posible para así favorecer el funcionamiento global del sistema que está realizando.
La última adición que se ha realizado al proyecto ha sido la capacidad de que al usuario se le descarguen y se le suban los ficheros automáticamente al Nextcloud.
El proyecto se encuentra en la nueva fase de implementar las soluciones nativas que se mencionan anteriormente.
Actualmente también se está acabando de implementar un sistema de replicación del Nextcloud, para así asegurar que no se pierden datos y en casos de caída, tener un servidor funcional instantáneamente para sustituir al servidor caído.

Planificación final

Dados los diferentes factores que se han encontrado a lo largo de la realización del proyecto, la lista de tareas, como ya se anticipó desde un principio, ha sufrido cambios. La lista de tareas definitiva es la siguiente.



**Esta tarea está marcada de esta manera puesto que era una tarea que se tenía pensada como secundaria.
La planificación inicial del proyecto se ha respetado en el conjunto final de horas, pero como se puede apreciar se ha recortado tiempo de ciertas fases y a la vez se han restrasado ciertas fases.

NextLDAP	Horas Planificadas	Horas reales	Estado
Proyecto	198	198	0
Servidor	**179**	**179**	0
Analisis	**13**	**13**	0
Objetivos	3	3	0
Requisitos	6	6	0
Tecnologia	4	4	0
Diseño	**12**	**12**	0
Arquitectura	4	4	0
Seguridad	4	4	0

Persistencia	4	4	0
Desarrollo	**152**	**152**	0
Estrategia de desarrollo	2	2	0
Instalación y configuración de NextCloud	30	27	3
Instalación y configuración de LDAP	45	48	-3
Integración NextCloud+LDAP	35	32	3
Configurar cliente ubuntu	30	33	-3
Añadir capas de seguridad	10	10	0
Pruebas	**2**	**2**	0
Rendimiento	2	2	0
Memoria	12	14	-2
Redacción	10	12	-2
Revisión	2	2	0
Presentación	7	5	2
Presentación oral	2	2	0
Matereiales(PowerPoint,etc..)	5	3	2

Leyes y normativa

Este proyecto se ha desarrollado siguiendo las directrices de la Ley Orgánica de protección de datos personales y garantía de los derechos digitales (LOPD-*GDD). Se ha utilizado esta ley puesto que el proyecto trata con datos personales de usuarios. La LOPD-*GDD entró en vigor a partir del 2019, la finalidad de la ley es proteger la intimidad, privacidad e integridad del usuario.
Se considera datos personales aquella información en texto, imagen o audio que permita la identificación de una persona. Existen datos que se consideran de poco riesgo, como el nombre o el correo electrónico, mientras que otros son considerados de riesgo más elevado, por ejemplo datos sensibles relacionados con la religión o la salud personal.
El objetivo de esta ley es que las empresas y organizaciones tengan un compromiso mayor con el tratamiento de datos y archivos personales.

PARTE II. Ejecución del proyecto

Análisis

Especificación de requisitos

Funcionales

Login de usuarios
El usuario (ya sea alumno o profesor) tendrá una cuenta en el servidor LDAP, con la cual podrá hacer login desde cualquier ordenador del centro.

Almacenaje de los documentos del usuario
Se almacenarán los ficheros de los usuarios en la nube de Nextcloud. Estos podrán acceder a ellos desde cualquier sitio mediante el navegador web, aparte de lo que menciona a continuación.

Disponibilidad de los documentos en cualquier máquina
El usuario una vez haga login en la máquina que sea del centro tendrá disponible los documentos que ha tenido en otras máquinas.

No funcionales

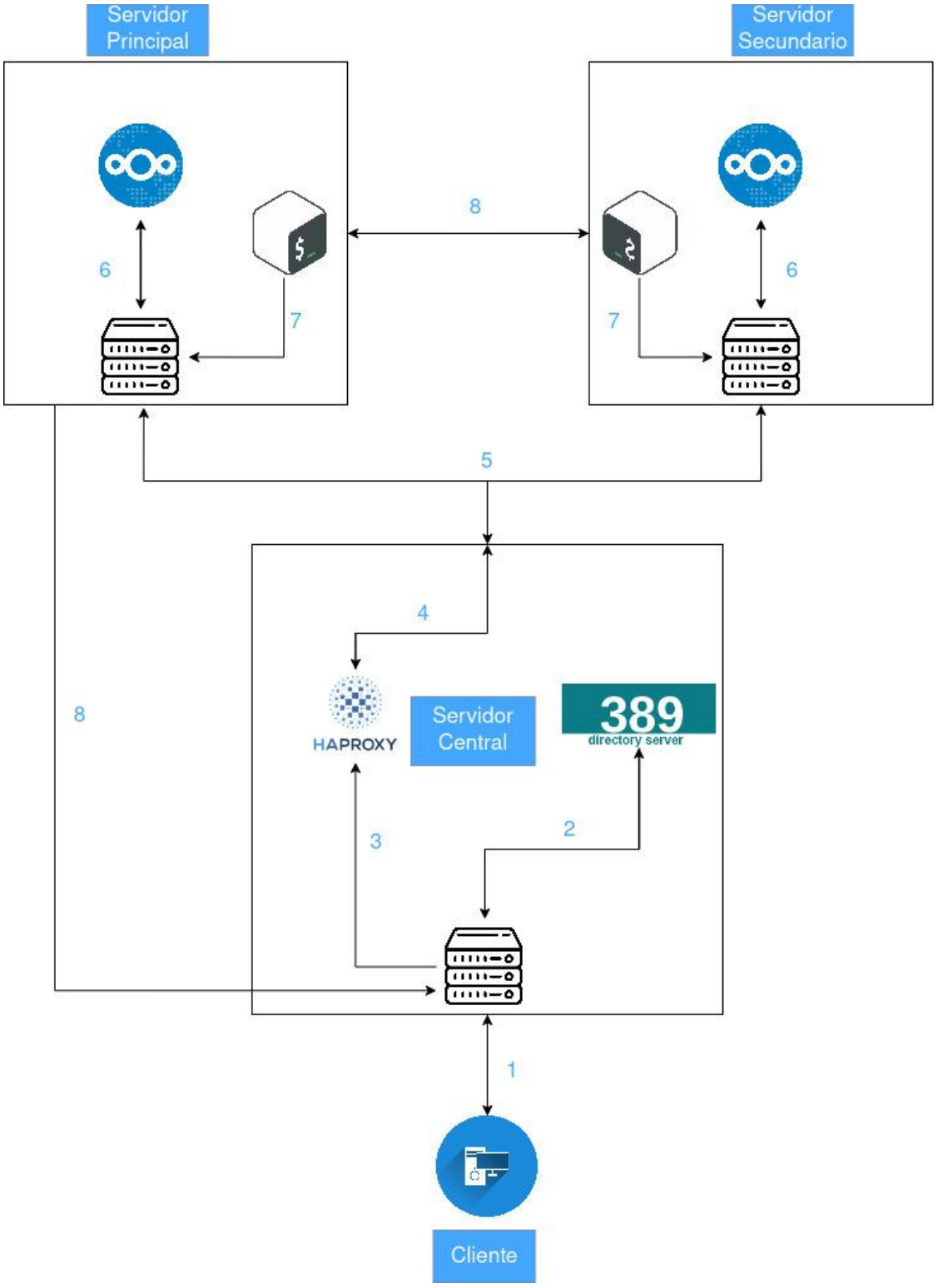
Servidor secundario
Se dispondrá de un servidor secundario con la información del principal (esta se irá replicando diariamente), para que en caso de que fallé el servidor principal, haya otro disponible para cubrirlo (alta disponibilidad).

Encriptación de los documentos de los usuarios
Los documentos que se encuentren en el Nextcloud se encriptan para así asegurar que ante un ataque se dificulte la obtención del contenido de estos documentos.

Diseño

Funcionamiento General del proyecto

En el siguiente esquema se presenta el funcionamiento general del proyecto



A continuación se expondrá en detalle el funcionamiento de todas las partes del sistema implementado en este proyecto:

1: Cuando el usuario quiere iniciar sesión en un equipo del centro (ver instalación de los clientes en anexo 6), cuando haga login en el gdm de linux, le envía la petición al servidor central, que es el encargado de tener el servidor LDAP, el cual contiene los usuarios de todas las personas del centro.

2: Una vez el servidor LDAP recibe la petición para iniciar sesión el programa instalado en los clientes hace una verificación para poder autenticar al usuario en el sistema, cuando el servidor lo ha verificado devuelve una respuesta al cliente, que es el encargado de permitir o denegar el acceso a la cuenta del usuario.

3 y 4: Si el resultado de la verificación en el servidor LDAP ha sido positiva, entonces es cuando el cliente necesita montar su carpeta que se encuentra disponible mediante el protocolo WebDAV en el servidor principal o secundario a través del software Nextcloud (ver anexo 3 para ver la configuración de los servidores Nextcloud y la implementación de este con el servidor LDAP), para acceder a esta carpeta se tiene que pasar por el HAProxy (ver anexo 4 para ver su configuración) que es el encargado de proporcionar un sistema por el cual solo hay un certificado de servidor, es decir los dos servidores usan para el HTTPS el certificado del servidor central. El HAProxy también es el encargado de administrar el sistema de alta disponibilidad, por lo general siempre ofrecerá a los usuarios el servidor principal y en caso de que este falle redirige todo el tráfico al servidor secundario de mientras el principal se encuentra en reparación, una vez que el principal vuelva a estar operativo el HAProxy volvería a dar como respuesta el servidor principal volviendo a pasar a un segundo plano al secundario.

En resumen el HAProxy se encarga de dirigir la petición de los usuarios a los servidores principal y secundario en función de su disponibilidad.

5: Como se ha expuesto en el punto anterior, es aquí donde se redirige las peticiones hacia un servidor u otro dependiendo de si están activos o no.

6: Cuando el Nextcloud recibe la petición se encarga de preparar y enviar la carpeta remota del usuario que la ha solicitado o se encarga de ofrecer sus funcionalidades a través de un navegador web, la respuesta se la devuelve al HAProxy del servidor central, que a su vez este último es el responsable de responder al cliente.

7: En este punto entra en escena el bash script, que junto con el demonio cron son los encargados de administrar la replicación de tanto la base de datos como

de los ficheros de los usuarios almacenados en el Nextcloud (ver anexo 2 para ver como se ha realizado la replicación), esta tarea se produce una vez al día y preferiblemente se desarrolla por la noche puesto que es el momento en el que menos usuarios se encuentran activos, si no fuera posible porque en el momento de hacer los cambios alguno de los servidores se encuentre en mantenimiento, apagado o fuera de servicio, se podría realizar a mano.

Por ejemplo, si el servidor principal cae, el servidor secundario tendría los datos del último backup realizado (del día anterior). Cuando el principal volviera a estar operativo habría que ejecutar los scripts disponibles en la máquina secundaria para pasar todos los cambios nuevos realizados a la máquina principal, no habría grandes problemas con las versiones que están en un servidor y en el otro, puesto que Nextcloud implementa un sistema de versiones de ficheros por lo que estaría el fichero de antes de que el server principal cayera y los cambios que se hubieran realizado en el servidor secundario.

8: Este punto es el encargado de transportar las copias de seguridad de un servidor a otro mediante el software RSync a través de SSH, mediante las tareas programadas anteriormente mencionadas. Como seguridad extra el servidor central también es receptor de los backups que va realizando el servidor principal así se aumenta la probabilidad de que los datos no se pierdan en caso de que los dos servidores cayeran o corrompieran.

Seguridad

En cuanto a este apartado el equipo de desarrollo, principalmente ha buscado que el usuario esté protegido tanto en la comunicación como cuando deposita sus ficheros e información en el Nextcloud. Para hacer cumplir estas directrices de seguridad el equipo ha empleado plugins de seguridad disponibles en la tienda de Nextcloud como pueden ser:

- **Antivirus for files**: Este plugin se encarga de buscar virus o cualquier tipo de software malicioso que intente hacer cualquier tipo de acción maliciosa en el Nextcloud, este funciona junto con el antivirus de linux ClamAV.

- **Ransomware protection**: Con este plugin se intenta que el Nextcloud tenga un poco más de protección frente a este tipo de ataques, ya que el plugin lo que hace es escanear los finales de cada ficheros con el fin de poder detectarlos.

Dentro de la propia configuración de Nextcloud también se ha hecho uso de varias herramientas que trae ya integradas de serie como pueden ser:

- **Brute-force protection**: Esta funcionalidad nos permite configurar cuantos intentos fallidos se considera como un ataque de fuerza bruta, en el caso de que salte la alerta de que se está intentando este tipo de ataque desde una IP, lo que hace es bloquear todas las peticiones que provengan de esta, la información de las IPs que va bloqueando se guardan dentro de una tabla propia de Nextcloud en su base de datos mysql.

- **Encriptación en el servidor**: Gracias a esta funcionalidad se consigue que todos los datos que el servidor carga en memoria principal, transacciones y comunicaciones están cifradas con un sistema de clave asimétrica

Ahora en cuanto a la seguridad de los servidores, se ha hecho uso de softwares para aumentar la seguridad de estos, las herramientas designadas para la protección de los servidores han sido:

- **ClamAV**: Este software se trata de un antivirus para linux que permite escanear todos los archivos del sistema con tal de encontrar ficheros maliciosos.

- **Fail2ban**: Con esta herramienta se pretende reducir la posibilidad de que el servidor sucumba ante un ataque de fuerza bruta, puesto que lo que hace es que en caso de que se falle la contraseña en los intentos que se le ha configurado, primero prohíbe el acceso a esa IP por un minuto, después de volver a fallar por tres minutos y así hasta que los atacantes desistan en su intento de penetrar el sistema.

- **Let's Encrypt:** Esta herramienta nos permite generar certificados emitidos por una CA, para que los navegadores, cuando lean el certificado, lo detecten como seguro y así le de al usuario más seguridad a la hora de navegar por el sitio web de Nextcloud. Este certificado ha sido creado de forma que se encuentra en el servidor central donde está el software HAProxy para que cifre las conexiones.

Persistencia

Para la persistencia de los datos en el proyecto, el equipo de desarrollo ha hecho uso de bases de datos puesto que el Nextcloud así lo requería y el grueso de los datos corre a cuenta de los diferentes dispositivos de almacenamiento de estado sólido proporcionados por las instancias de AWS.
Los datos están almacenados principalmente en el servidor principal, pero cada noche estos serán replicados al disco duro de la máquina secundaria y central, para que en caso de fallo, la supervivencia de estos sea la más alta posible.

Esta replicación estará compuesta de dos fases: la primera estará compuesta por el envío de la carpeta donde se almacena la configuración, ficheros de los usuarios e información necesaria para el funcionamiento de Nextcloud, una vez estos datos están en la otra máquina, entrará una segunda fase en la que se tendrá que replicar la información almacenada en el motor de base de datos MySQL, puesto que si la información no coincide con la que tiene la carpeta de Nextcloud, este no será capaz de arrancar.
(Para más información sobre la replicación realizada, ver anexo 2, donde se encuentra la realización de esta).
Respecto a la política que se seguirá, hablando de los backups, será mantener los backups durante una semana y después borrarlos, para así no sobrecargar el almacenamiento de la máquina central.

Tecnología

Nextcloud es una serie de programas cliente-servidor de código abierto que permiten la creación de servicios de alojamiento de archivos: **Esto se usará para almacenar los diferentes archivos de los usuarios**

El 389 Directory Server es un servidor de protocolo ligero de acceso a directorios (LDAP) desarrollado por Red Hat como parte del Proyecto Fedora: **Este será el servidor LDAP que se implementará.**

Oracle VM VirtualBox es un software de virtualización para arquitecturas x86/amd64, desarrollado por Oracle Corporation como parte de su familia de productos de virtualización. **Esto se usará para implementar el servidor y el cliente Ubuntu.**

Apache es un servidor web HTTP de código abierto, para plataformas Unix, Microsoft Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1 desarrollado por Apache Software Foundation: **Este será el encargado de albergar la página del Nextcloud.**

MySQL es un sistema de gestión de bases de datos relacional desarrollado bajo licencia dual: Licencia pública general/Licencia comercial por Oracle Corporation y está considerada como la base de datos de código abierto más popular del mundo:
Este SGBD es el encargado de administrar los datos internos del Nextcloud.

HAProxy es un software gratuito y de código abierto que proporciona un equilibrador de carga de alta disponibilidad y un proxy inverso para aplicaciones basadas en TCP y HTTP que distribuye solicitudes entre varios servidores.
HAProxy será el que se encargará de ofrecer un sistema de failover.

AWS es una colección de servicios de computación en la nube pública que en conjunto forman una plataforma de computación en la nube, ofrecidas a través de Internet por Amazon.com.
Aquí será donde estarán alojadas todas las máquinas involucradas en el proyecto. (Ver anexo 1 para ver el proceso para alojar las máquinas).

Bash es un intérprete de órdenes que generalmente se ejecuta en una ventana de texto donde el usuario escribe órdenes en modo texto. Bash también puede leer y ejecutar órdenes desde un archivo, llamado script.
Gracias a bash se podrán realizar scripts e interpretarlos para realizar la replicación del Nextcloud y la creación automática de usuarios del servidor LDAP (ver anexo 5 para ver este script).

Problemas encontrados en el desarrollo del proyecto

Durante el desarrollo del proyecto el equipo ha tenido que ir sorteando una serie de dificultades e inconvenientes, algunos debidos a la poca experiencia en las tecnologías involucradas en el proyecto y otros a situaciones inusuales, a continuación se expondrán una serie de errores ocurridos durante el desarrollo:

All vs Anyone

Este error viene dado porque cuando los usuarios querían hacer login a través de la GUI del cliente Ubuntu, este iniciaba el proceso de login pero saltaba otra vez a la lista de usuarios, tras una investigación de cómo funcionaba el software cliente, el equipo de desarrollo llegó a la conclusión de que por cómo está hecho el software necesita acceder para según qué procedimientos como anónimo, por lo tanto se requiere de crear un regla para que los anónimos puedan acceder a solo una serie de información no sensible para poder hacer las verificaciones pertinentes. Para solucionar este error primero se probó a implementar una ACL en el LDAP con el ALL pero esta regla tampoco servía puesto que solo hace efecto a todos los usuarios, pero solo si se han autenticado previamente, por lo tanto, el problema finalmente se solucionó poniendo en la regla ACL anyone, para hacer que los anónimos tengan permiso para poder acceder a cierta información del servidor LDAP.

Permisos de lectura plugin Nextcloud-LDAP

A la hora de poner el plugin que implementa la interconectividad entre el servidor LDAP y el software Nextcloud, el equipo de desarrollo se encontró con que a la hora de que el plugin encontrará los usuarios y grupos añadidos previamente, no encontraba nada, mediante una búsqueda de información sobre los permisos base del servidor LDAP, el equipo dedujo que el problema venía de que el usuario que utiliza Nextcloud para acceder a esta información no estaba teniendo todo el acceso a la información que necesitaba por lo tanto, la solución implementada fue una serie de reglas ACL dentro del servidor LDAP que permiten al usuario con el que se conecta Nextcloud, leer la información que necesita.

Redirecciones HTTPS a HTTP

Este contratiempo le surgió al equipo de desarrollo de manera inesperada puesto que el sistema por el que funciona la conexión del usuario con los servidores Nextcloud, es dirigido mediante el software HAProxy, el cual hasta la fecha en la que empezó a ocurrir no había expresado ningún problema. El problema se trataba de que cuando el usuario hacia login en la página del Nextcloud está en HTTPS pero a la hora de seleccionar el botón de iniciar sesión este dirigía al usuario a una página HTTP la cual no existía, pero si el usuario volvía hacia la página de login anterior haciendo uso de las flechas del navegador, se cargaba el escritorio del Nextcloud con normalidad a través de HTTPS. El equipo de desarrollo mediante el seguimiento de los paquetes, los cuales se enviaban entre el cliente y el servidor HAProxy encontró que en la configuración de este último se estaba confundiendo a la hora de recibir y enviar las peticiones, puesto que las recibia en HTTPS y las devolvía en HTTP, la solución desarrollada por el equipo se trata de una configuración en el HAProxy que obliga a que todo el tráfico sea HTTPS y en la configuración del Nextcloud en el fichero de configuración también se le obliga a que toda comunicación que tenga sea por el puerto HTTPS y que cada vez que sobre escriba una URL la cambie HTTP por el protocolo cifrado con SSL/TLS.

Tarea programada en el servidor principal no se ejecuta

Este error consistía en que la tarea programada(con el demonio cron) que ejecutaba el script backup2.sh (ver anexos 2.1 para ver este script), no se realizaba. El equipo de desarrollo fue investigando las posibles causas de este problema. Cabe recalcar algo muy importante en este apartado y es que este script, ejecutado en un terminal normal, funcionaba correctamente, pero como tarea programada no se ejecutaba.
Durante esta investigación se identificaron diferentes aspectos que podrían ser los causantes de la no ejecución de esta tarea programada.

El primer aspecto que se identificó fue el no uso de rutas absolutas en el script, debido a que un script que se quiera ejecutar desde el demonio cron debe tener todo con rutas absolutas, puesto que no se ejecuta desde, por ejemplo el home de un usuario. Arregladas las líneas del script que no usaban rutas absolutas se probó de nuevo la ejecución de la tarea programada, sin éxito.
El segundo aspecto que se identificó fue el posible uso de variables de entorno en algún aspecto de script (esto es debido a que una tarea programada en el demonio cron no usa las variables de entorno a nos ser que se especifiquen en el fichero de configuración de las tareas programadas), lo cual se daba en el agente ssh que gestiona el anillo de claves, que en su momento utilizaba una variable de entorno (ver anexos 2.2.1, concretamente la línea que está en rojo, que es donde se usaba esta variable de entorno, fue sustituida por su valor debido a que siempre era el mismo). Arreglado este problema, se volvió a probar la ejecución de la tarea programada, una vez más, sin éxito.
El tercer aspecto que el equipo de desarrollo identificó fue, después de supuestamente ejecutar sin éxito la tarea programada múltiples veces, el puerto 22 de el servidor secundario, el que utiliza SSH, se había bloqueado, pero solo si se intentaba acceder desde el servidor principal. Esto fue debido al programa que se instaló anteriormente para añadir seguridad al servidor, fail2ban, que como se ha mencionado anteriormente, bloquea el acceso a la máquina en la cual está instalado desde ips que hayan hecho cierto número de logins fallidos.
Este hecho dio que pensar al equipo de desarrollo, ya que si había bloqueado las conexiones, es porque alguna autenticación que hacía el script sobre la máquina secundaria, de alguna manera, estaba fallando. Investigando este suceso se descubrió que, en ciertas ocasiones, las claves generadas para que la conexión ssh no pida contraseña, se corrompen al ejecutarse un comando que las utiliza desde el cron. Para solucionar esto, solo hubo que generar de nuevo las claves y finalmente, la tarea programada del script backup2.sh se ejecutó.

No visualiza correctamente los ficheros de los usuarios después de la replicación del Nextcloud

Cuando se hacía la replicación/backup del servidor principal al servidor secundario, los ficheros de cada usuario se replicaban correctamente, pero, a la hora de abrirlos, daba un error y no se mostraba el contenido del fichero.
Después de una ardua investigación, se encontró el detonante de este error. Este error era debido a que estaba activada una opción en la configuración de los 2 servidores Nextcloud que lo que realizaba era encriptar los ficheros directamente en el disco. El problema que presentaba esta opción de configuración es que, para encriptar los ficheros utilizaba un par de claves(pública y privada) únicas de cada servidor, por lo tanto, al replicar los ficheros del servidor principal al secundario, este último no tenía el par de claves correcto para desbloquearlo. Cabe mencionar que este par de claves es único para cada servidor y no se puede cambiar, puesto que, si se cambia por otro par de claves, el servidor no funciona.

La solución que se encontró fue no encriptar los datos en el disco directamente, si no, encriptar los datos en la memoria principal de un ordenador, la RAM.

Conclusiones

Conclusiones generales del proyecto

Las conclusiones que ha sacado el equipo de desarrollo de este proyecto ha sido que Nextcloud ofrece una gran cantidad de posibilidades, ya que dispone de una ingente cantidad de plugins desarrollados por la comunidad y por Nextcloud GmbH, desarrolladora de Nextcloud.

Este software tiene herramientas de todo tipo, desde extensiones que permiten a usuarios colaborar a la hora de editar ficheros, integración con moodle, algo que sería interesante para este proyecto puesto que el centro trabaja con esta herramienta, hasta una aplicación para dispositivos móviles que permite al usuario acceder a todos sus ficheros y funcionalidades sin la necesidad de acceder desde un navegador web o un equipo de sobremesa.

Y en cuanto a las conclusiones personales que ha podido sacar el equipo de desarrollo de este proyecto, es que ha sido positivo puesto que ha nutrido altamente su conocimientos en la utilización de las diferentes tecnologías, técnicas para depurar errores, búsqueda de información y resolución de incidencias.

Consecución de los objetivos

En cuanto a la consecución de los objetivos propuestos para el proyecto el equipo de desarrollo a conseguido cumplir todos los puntos:

Objetivos cumplidos	Objetivos no cumplidos
• Servidor LDAP • Nextcloud • Carpetas compartida con los clientes por DAVS • Sistema de failover (HAProxy) • Backups en el cierre de sesión del usuario • Mejora de la seguridad de los servidores • Sistema de replicación entre el servidor principal y secundario • Cliente LDAP • Integración LDAP -> Nextcloud • Script crear usuarios LDAP de un CSV	

Valoración de la metodología y planificación

La metodología y planificación planteada para este proyecto ha sido, en su gran mayoría, seguida de manera idónea. Este hecho se puede observar en la planificación final del proyecto, que muestra que no ha habido ninguna gran desviación de tiempo en ninguna de las fases. Por esto último el equipo de desarrollo confirma que la planificación y metodología planteadas fueron las correctas.

Visión a futuro

Como visión a futuro el equipo ha fijado una serie de "objetivos" posibles para la mejora de la infraestructura desarrollada en el proyecto, a continuación se expondrán un serie de posibles mejoras:

- Puesto que el centro funciona con moodle se podría implementar la integración de este con el software Nextcloud para su mejor funcionamiento, tambien se podria implementar una serie de plugins para que los usuarios puedan editar simultáneamente un fichero, para que se puedan tratar ficheros ZIP, con la finalidad de poder ofrecer la mismas funcionalidades que google drive.

- Llegar a conseguir el funcionamiento correcto de la "doble encriptación" que proporciona Nextcloud, concretamente el funcionamiento de la encriptación en disco, puesto que está, al realizar la replicación daba ciertos errores que impedían el buen funcionamiento del servicio.

- Conseguir un mayor grado de automatización en la replicación del Nextcloud, puesto que actualmente está automatizado el funcionamiento de esta desde el servidor principal al secundario (debido a que el equipo de desarrollo estimó que el servidor principal no se caería a menudo). Por lo tanto lo que se debería hacer es automatizar el proceso pero a la inversa, es decir, del secundario al principal, para que, cuando caiga el principal y se use el servidor secundario, una vez el principal vuelva a funcionar, se repliquen los datos del secundario al principal de manera automática..

- Como el sistema de los clientes funciona con libnss-ldap, una herramienta que cumple con su cometido pero hay sistemas más nuevos que implementan más privacidad, como por ejemplo: que solo se ve el usuario sssd y no los usuarios ldap, por lo tanto si algún usuario inspecciona el

fichero “passwd” con la herramienta SSSD estos usuarios no se verían reflejados.

- Puesto que el equipo de desarrollo llegó a la conclusión de que esta infraestructura estaba en fase de planificación y desarrollo no adquirió instancias de AWS muy potentes y sin mucho espacio por lo que para llevar este proyecto a un entorno real se requerirían máquinas con una gran capacidad de almacenamiento y una capacidad de computación razonable para por albergar a muchos usuarios simultáneamente.

- En cuanto a las carpetas compartidas que los clientes tienen en sus máquina podría haber una mejora en cuanto a los backups puesto que si el fichero que se crea es un poco pesado puede tardar un rato, por lo que si en el transcurso de tiempo se fuera la conexión o fallara alguna parte de la infraestructura, habría el peligro de que el usuario perdiera información por lo que se podría hacer que la carpeta home del usuario realmente fuera la de la nube, de esta manera solo se trabajaría en la nube y no se tendría que estar traspasando ficheros.

- Otro objetivo a futuro sería llegar a conseguir extraer la contraseña del primer inicio de sesión sin la necesidad de tener que preguntarla una segunda vez, que es como funciona actualmente.

- Crear un playbook de ansible para así automatizar la creación de los clientes con la configuración necesaria para que funcionen con la infraestructura de este proyecto. Esto lo que permitiría sería poder configurar todas las máquinas del centro de manera rápida y eficaz, sin necesidad de ir una a una.

- Adaptar el tema de la página web de Nextcloud a la imagen del centro,

Bibliografía

Organización del proyecto:

https://trello.com/

Servidor LDAP:

https://www.javieranto.com/kb/GNU-Linux/pr%C3%A1cticas/Administraci%C3%B3n%20b%C3%A1sica%20389DS/

Curso de LDAP en GNU/Linux — Plone site (xeill.net)

Documentación ofrecida por el profesor Don Óscar Torrente Artero.

Cliente LDAP:

https://www.youtube.com/watch?v=dQKCvkbgUwg&t=1097s

Backups Nextcloud:

https://docs.nextcloud.com/server/latest/admin_manual/maintenance/backup.html

https://kenfavors.com/code/how-to-restore-a-nextcloud-backup/

HAProxy:

The Four Essential Sections of an HAProxy Configuration - HAProxy Technologies

HAProxy Configuration Basics: Load Balance Your Servers - HAProxy Technologies

https://www.youtube.com/watch?v=twCmZfSSWwc

https://www.youtube.com/watch?v=7ljiOD6MbLA

https://help.clouding.io/hc/es/articles/360010289000-Balancear-servicio-web-con-HAProxy-con-certificado-SSL-en-Ubuntu-18-04

https://www.haproxy.com/blog/failover-and-worst-case-management-with-haproxy/

Instalar NextCloud:

Installation on Linux — Nextcloud latest Administration Manual latest documentation

https://www.youtube.com/watch?v=uc_eKXeqqvI

https://www.youtube.com/watch?v=3GXhnHDPOsE

Configuración Nextcloud:

Nextcloud configuration — Nextcloud latest Administration Manual latest documentation

Reverse proxy — Nextcloud latest Administration Manual latest documentation

Carpeta compartida Nextcloud -> cliente ubuntu:

Nextcloud configuration — Nextcloud latest Administration Manual latest documentation

command line - gio mount - how to use Gnome keyring for password? - Ask Ubuntu

Subida de ficheros a Nextcloud:

https://help.nextcloud.com/t/how-to-upload-a-file-via-cli-to-nextcloud-bash/71837

https://docs.nextcloud.com/server/latest/user_manual/es/files/access_webdav.html

AntiVirus Nextcloud:

Easy Nextcloud Server Snap Setup for Cloud Storage, Chat, Documents, and More (hannahtech.co)

Interconexión Nextcloud -> Servidor LDAP:

User authentication with LDAP — Nextcloud latest Administration Manual latest documentation

Encriptación Nextcloud:

https://www.techrepublic.com/article/how-to-enable-server-side-encryption-in-nextcloud/

Archivos Nextcloud:

Archivos y sincronización — documentación de Nextcloud latest User Manual - latest

MySQLDump:

mysqldump - Una guía práctica (linuxtotal.com.mx)

ACLs server LDAP:

https://breest.io/_/389-directory-server-aci-reference/

Demonio CRON:

Manual básico de como usar Cron (linuxtotal.com.mx)

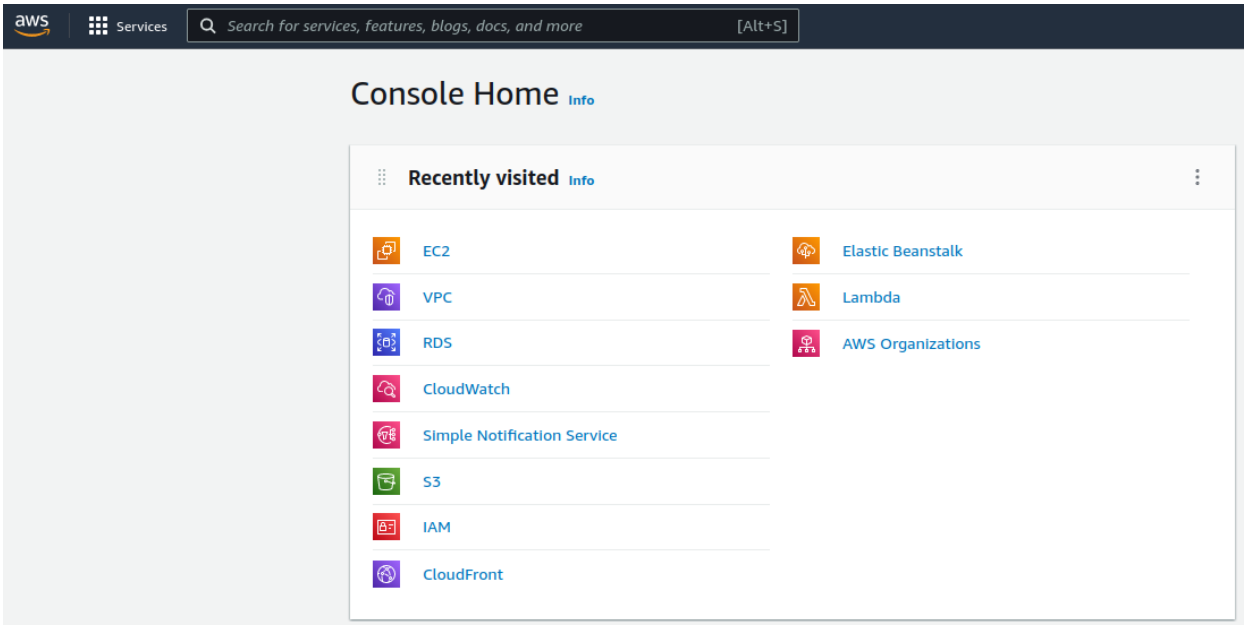
Textos cliente linux:

Zenity, diálogos para GNOME , Cinnamon, MATE... - Atareao

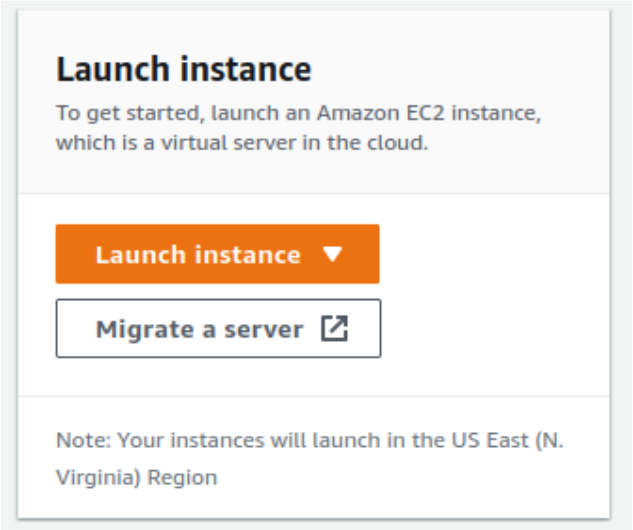
Anexos

1. Amazon Web Service (AWS)

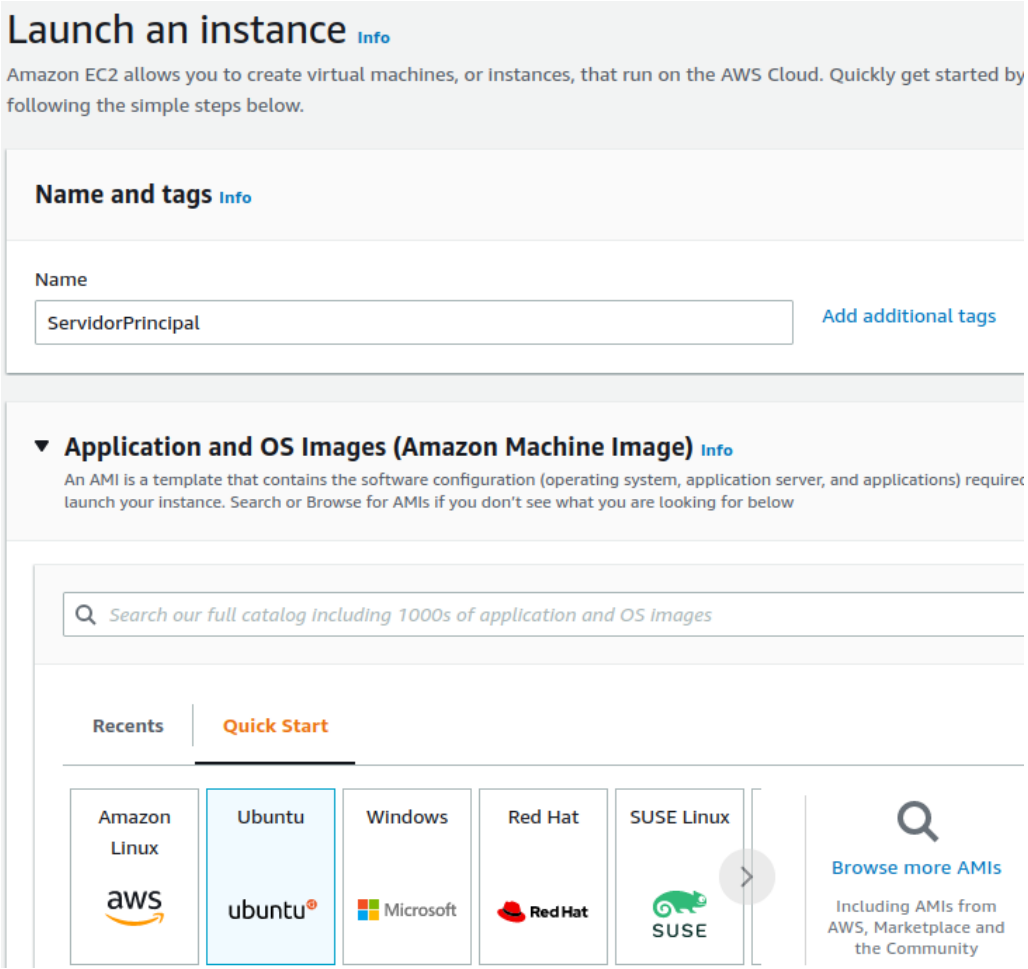
Una vez iniciada sesión hay que ir al apartado de EC2, que es donde se encuentra la funcionalidad para hacer las máquina virtuales dentro de AWS:



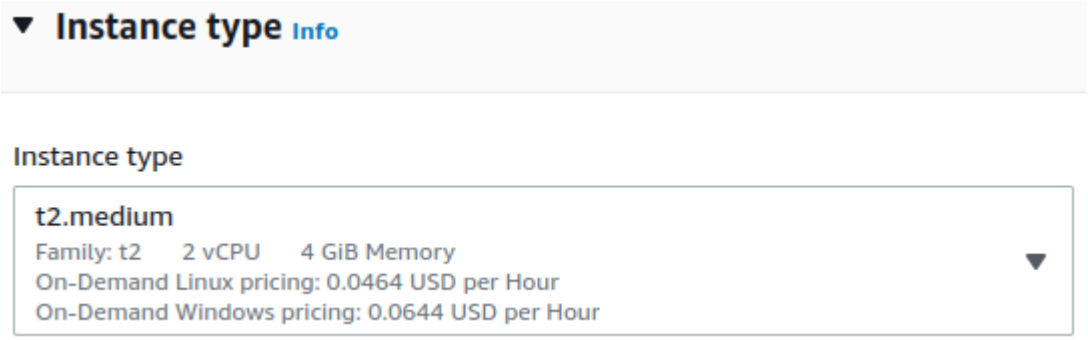
Dentro del apartado de EC2 tenemos primero que lanzar una instancia:



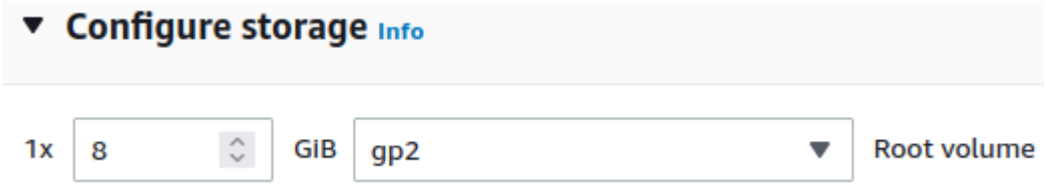
En el menú para lanzar la instancia, tenemos que indicarle el nombre, que sistema operativo queremos que tenga, etc...:



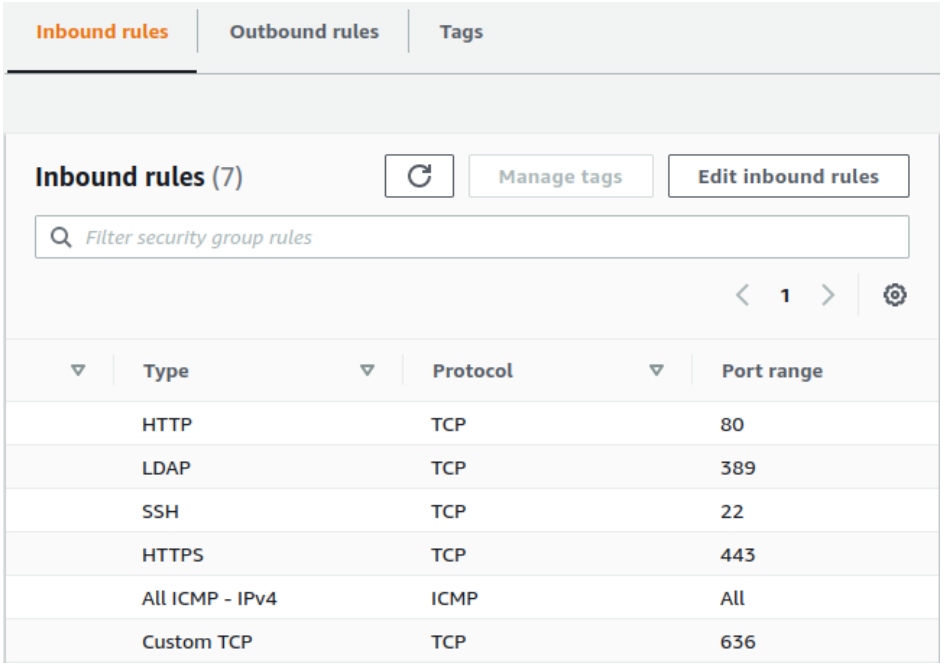
Y le indicamos el tipo de instancia que queremos usar, las instancias se diferencian por el tipo que es cada una en función de los núcleos y ram que necesitemos nos aumentará el coste monetario por hora de uso:



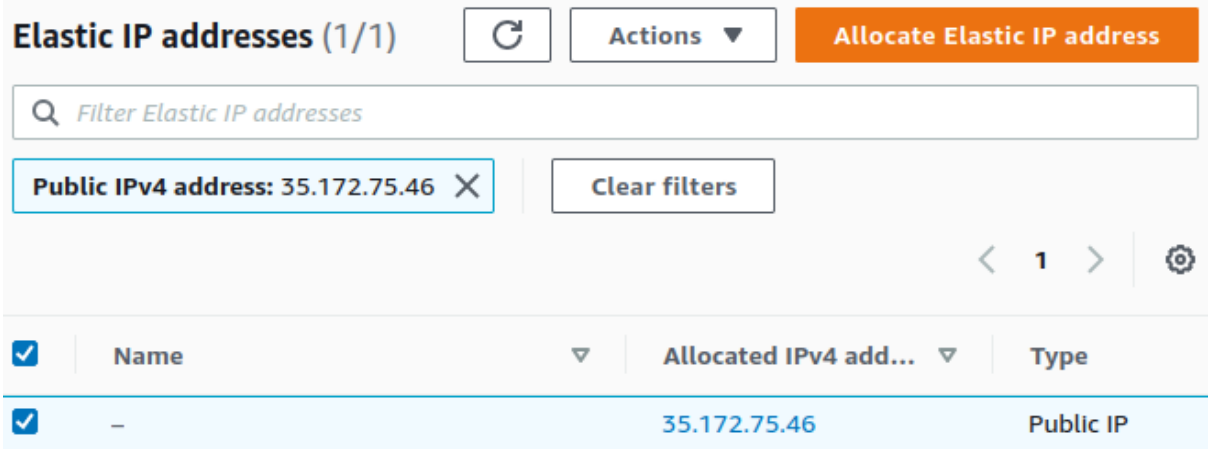
Por último tendremos que indicarle el espacio que tendrá la máquina, AWS cobra por cantidad de datos almacenados en las máquinas:



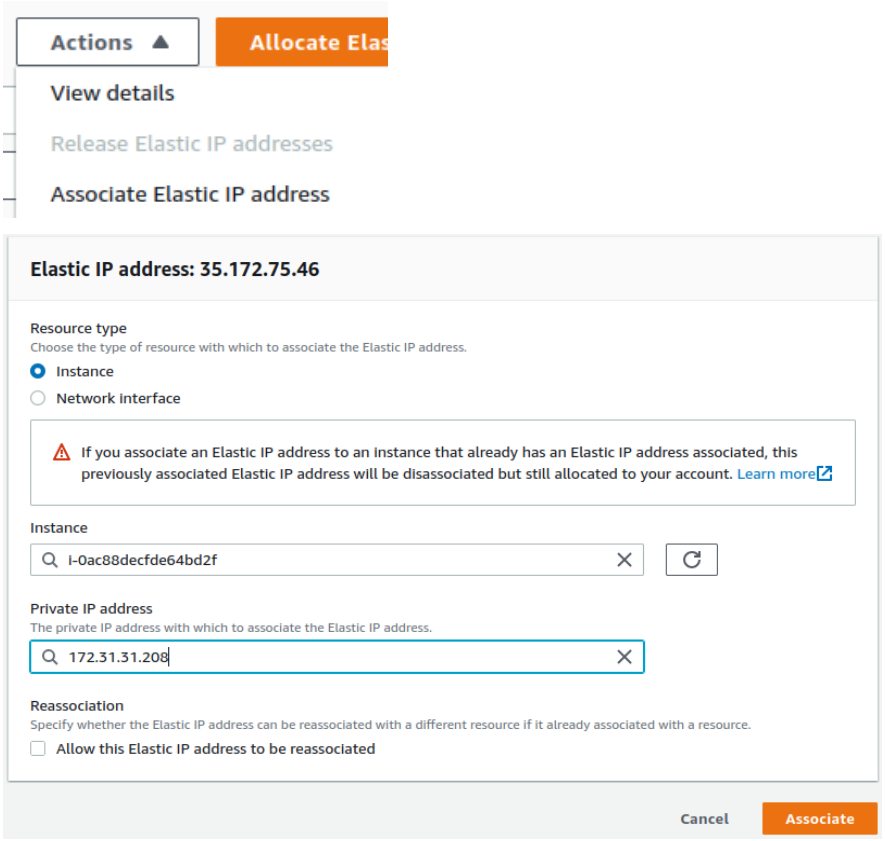
Una vez la máquina está funcionando tenemos que abrir los puertos para que se pueda acceder desde fuera a la máquina:



Después de abrir los puertos para que pueda recibir peticiones, es recomendable asignarle una IP elastica, es decir que siempre será la misma, para solicitarla solo tenemos que seleccionar el botón de 'Allocate Elastic IP address':



Cuando AWS nos asigna la IP pública permanente le damos a Actions y se la asignamos a la instancia (“máquina virtual”) creada anteriormente:



Cuando ya está configurada y con la ip fija asociada, para acceder a la instancia (“máquina virtual”), le indicamos el fichero de ssh que contiene la ip pública y se accede sin contraseña:

```
asix2-2021@ada-107:~$ ssh -i /home/asix2-2021/Baixades/labsuser.pem ubuntu@3.223.238.58
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.13.0-1025-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed May 25 19:37:22 CEST 2022

  System load:  0.0               Processes:             130
  Usage of /:   15.9% of 29.02GB  Users logged in:       1
  Memory usage: 17%               IPv4 address for eth0: 172.31.95.139
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

6 updates can be applied immediately.
To see these additional updates run: apt list --upgradable


Last login: Wed May 25 19:18:12 2022 from 188.26.210.148
ubuntu@ip-172-31-95-139:~$
```

2. Replicación de Nextcloud

2.1. Scripts replicar datos

Hacer un acl para que con la comanda rsync se pueda escribir en esa carpeta ya que el propietario es www-data que no tiene contraseña y no es recomendable tocar ese usuario.
Importante que estas dos acl se ejecuten en ambos servidores, si no no se podrá enviar la información por falta de permisos.
Esta acl se encuentra en el script llamado backup1.sh que se ejecutará en el servidor principal y para el servidor secundario se podrá ver más adelante que esta acl es una tarea programada con el demonio cron.
Scripts y orden de ejecución servidor principal

1. backup1.sh

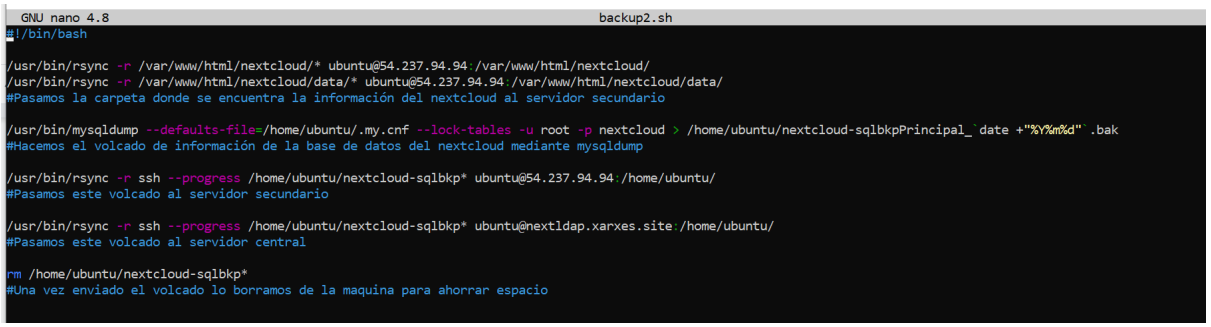
```
#!/bin/bash
setfacl -R -m u:ubuntu:rwx /var/www/html
#Con la linea anterior se permite al usuario poder leer, escribir y ejecutar ficheros de esa carpeta y su contenido.
```

2. backup2.sh

```
#!/bin/bash
/usr/bin/rsync -r /var/www/html/nextcloud/*
ubuntu@54.237.94.94:/var/www/html/nextcloud/
/usr/bin/rsync -r /var/www/html/nextcloud/data/*
ubuntu@54.237.94.94:/var/www/html/nextcloud/data/
#Pasamos la carpeta donde se encuentra la información del Nextcloud al servidor secundario
/usr/bin/mysqldump --defaults-file=/home/ubuntu/.my.cnf --lock-tables -u root -p nextcloud > /home/ubuntu/nextcloud-sqlbkpPrincipal_`date +"%Y%m%d"`.bak
#Hacemos el volcado de información de la base de datos del Nextcloud mediante mysqldump
/usr/bin/rsync -r ssh --progress /home/ubuntu/nextcloud-sqlbkp*
ubuntu@54.237.94.94:/home/ubuntu/
#Pasamos este volcado al servidor secundario
/usr/bin/rsync -r ssh --progress /home/ubuntu/nextcloud-sqlbkp*
ubuntu@nextldap.xarxes.site:/home/ubuntu/
#Pasamos este volcado al servidor central
rm /home/ubuntu/nextcloud-sqlbkp*
```

```
#Una vez enviado el volcado lo borramos de la maquina para ahorrar espacio
```

Aquí se puede ver una mejor representación de este script:



3. Volver a ejecutar el script backup1.sh, debido a que al enviar la carpeta, el acl se pierde.

Scripts y orden de ejecución servidor secundario

1. database.sh

```
#!/bin/bash
#Para realizar el volcado de la base de datos, se borrará la base de datos existente en este servidor y se creará de nuevo, volcando los datos recibidos del servidor principal.
#Las siguientes 3 lineas realizan estas tareas.
mysql --defaults-file=~/.my.cnf -u root -p -e "DROP DATABASE nextcloud"
mysql --defaults-file=~/.my.cnf -u root -p -e "CREATE DATABASE nextcloud"
mysql -u root -p nextcloud < /home/ubuntu/nextcloud-sqlbkp*
```

2. databaseOwner.sh

```
#!/bin/bash
#Se le da la propiedad al usuario www-data, de la carpeta que se ha pasado del principal al secundario
chown -R www-data:www-data /var/www/html/nextcloud
```

3. database3.sh

```
#!/bin/bash
setfacl -R -m u:ubuntu:rwx /var/www/html/nextcloud/
#Con la linea anterior se permite al usuario poder leer, escribir y ejecutar ficheros de esa carpeta y su contenido.
systemctl restart apache2
#Se reinicia el servicio apache para que se apliquen los cambios realizados
rm /home/ubuntu/nextcloud-sqlbkp*
#Una vez enviado el volcado lo borramos de la maquina para ahorrar espacio
```

2.2. Tareas programadas

2.2.1. Anillo de llaves

Para realizar las tareas programadas, las comandas rsync no deberían de pedir contraseña. Para evitar esto se ha decido utilizar un anillo de claves.

Ha habido que encender el canal dbus del usuario puesto que al ser un servidor, es decir una sesión de texto, este no viene encendido.
Se ha realizado de la siguiente manera:
Se han añadido las dos últimas líneas al fichero del servicio dbus del usuario(el fichero en este caso es ~/.config/systemd/user/dbus.service) , puesto que sin estas no dejaba habilitar el servicio, para que así se encienda al encender el sistema:

```
[Unit]
Description=D-Bus User Message Bus
Documentation=man:dbus-daemon(1)
Requires=dbus.socket
[Service]
ExecStart=/usr/bin/dbus-daemon --session --address=systemd: --nofork
--nopidfile --systemd-activation --syslog-only
ExecReload=/usr/bin/dbus-send --print-reply --session --type=method_call
--dest=org.freedesktop.DBus / org.freedesktop.DBus.ReloadConfig
[Install]
WantedBy=multi-user.target
```

Habilitamos el servicio dbus del usuario

```
systemctl --user enable dbus
```

Después de habilitar el canal dbus del usuario habrá que crear el agente ssh para que gestione el anillo de claves. Para ello:

Crear el fichero ~/.config/systemd/user/ssh-agent.service y poner en su contenido lo siguiente:

```
[Unit]
Description=SSH key agent's systemd user service
[Service]
Type=simple
ExecStart=/usr/bin/ssh-agent -D -a /run/user/1000/ssh-agent.socket
[Install]
```

```
WantedBy=default.target
```

Habilitar este servicio

```
systemctl --user enable ssh-agent && systemctl --user start ssh-agent
```

2.2.2. Comandos mysql y mysqldump

Para evitar que las comandas mencionadas no pida contraseña al ejecutarse la tarea programada se ha propuesto la siguiente solución.

Creación del fichero ~/.my.cnf, este fichero permitirá que los comandos mysql y mysqldump realizar sin que pida contraseña, puesto que las leerá de este fichero por defecto. Darle permisos 600, para que así solo el usuario que le pertenezca el fichero pueda leerlo y escribirlo, así nos aseguramos de que ningún otro usuario pueda leer las contraseñas.
No se ponen las contraseñas por razones de seguridad.

```
[mysqldump]
password=..............
[mysql]
password=..............
```

En las imágenes siguientes se puede observar una prueba de que funciona, no pide contraseña en ningún momento.

```
ubuntu@ip-172-31-95-139:~$ mysql -u root -p
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 155
Server version: 8.0.29-0ubuntu0.20.04.3 (Ubuntu)

Copyright (c) 2000, 2022, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

```
ubuntu@ip-172-31-95-139:~$ mysqldump --lock-tables -u root -p nextcloud > /home/ubuntu/nextcloud-sqlbkp_`date +"%Y%m%d"`
.bak
ubuntu@ip-172-31-95-139:~$ ls
backup.sh  nextcloud-sqlbkp_20220523.bak
```

2.2.3. Automatización de los scripts

Para que estos scripts se ejecuten de manera automática para realizar el backup se ha usado el demonio cron. En el servidor principal se han establecido las siguientes tareas programadas en el archivo de /etc/crontab:

```
18 *    * * *   root    /home/ubuntu/backup1.sh
19 *    * * *   ubuntu  /home/ubuntu/backup2.sh
20 *    * * *   root    /home/ubuntu/backup1.sh
```

Y en el servidor secundario se han establecido las siguientes:

```
20 *  * * *  root   /usr/bin/bash setfacl -R -m u:ubuntu:rwx /var/www/html/
21 *  * * *  ubuntu  /usr/bin/bash /home/ubuntu/database.sh
22 *  * * *  root   /usr/bin/bash /home/ubuntu/databaseOwner.sh
23 *  * * *  root   /usr/bin/bash /home/ubuntu/database3.sh
```

Después de escribir las tareas programadas en el fichero /etc/crontab, habrá que decirle al demonio cron qué fichero y que usuario debe usar para ejecutar las tareas, esto se hace con la comanda:

```
sudo crontab -u root /etc/crontab
```

Para que se apliquen los cambios reiniciamos el demonio cron con la siguiente comanda:

```
sudo systemctl restart cron
```

3. Configuración Nextcloud

A continuación se muestran diferentes aspectos a tener en cuenta sobre la configuración de Nextcloud.

3.1. Habilitar replicación

Para permitir que se pueda hacer la replicación antes mencionada hay que ejecutar el siguiente comando.

```
root@miservidor:/var/www/html/nextcloud# sudo -u www-data php occ app:enable files_external
files_external 1.15.0 enabled
```

3.2. Permitir ficheros ZIP

Un dato curioso sobre la instalación por defecto de Nextcloud es que no admite archivos comprimidos(.zip). Para habilitar la subida de archivos .zip se deberá editar el siguiente fichero:

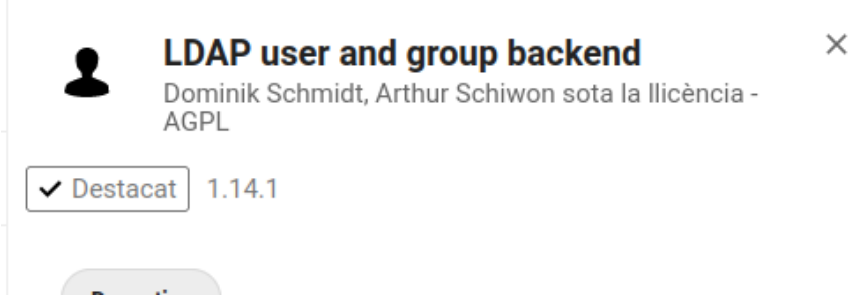
```
root@miservidor:/var/www/html/nextcloud# nano .htaccess
```

Y añadir en la línea FIlesMatch el parámetro zip:

```
# Add cache control for static resources
<FilesMatch "\.(css|js|svg|gif|png|jpg|ico|wasm|tflite|zip)$">
  Header set Cache-Control "max-age=15778463"
</FilesMatch>
```

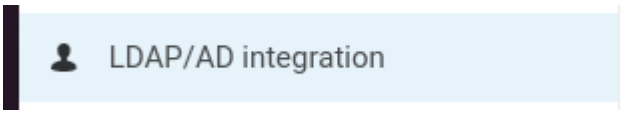
3.3. Plugin LDAP user and group backend

En este apartado se mostrará la configuración del plugin LDAP user and group backend.

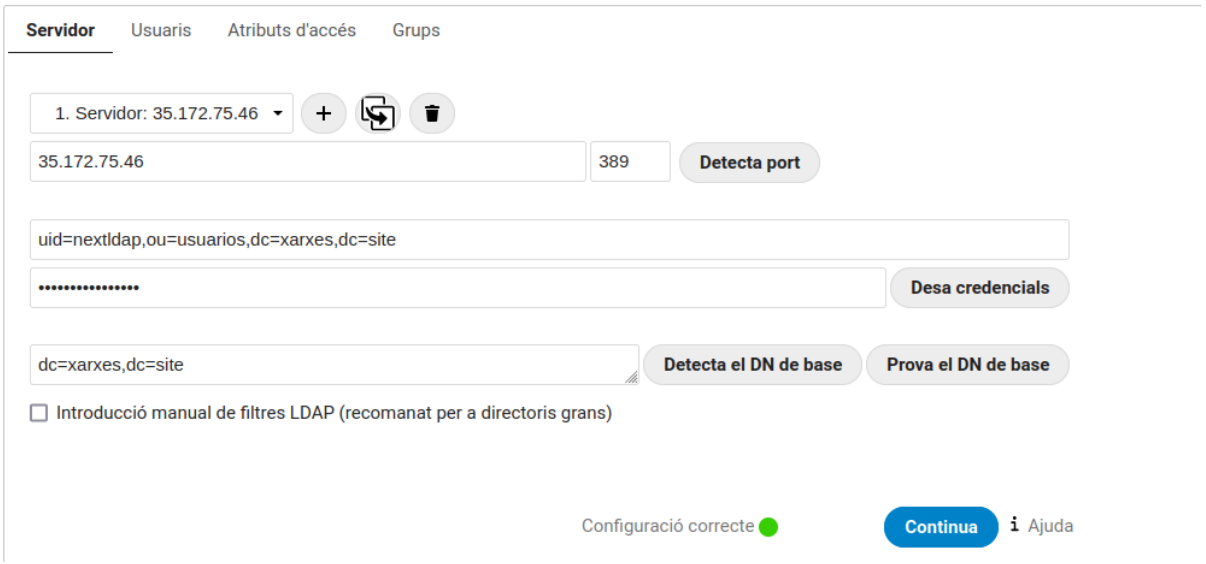


Este plugin permite conectar el servidor LDAP con el servidor Nextcloud, y así utilizar los usuarios del servidor LDAP en este último.

Para configurar este plugin y por lo tanto, se usen los usuarios del servidor LDAP en Nextcloud, habrá que dirigirse, desde el usuario administrador, a parámetros, después en el apartado de administrador, entrar en el siguiente apartado:

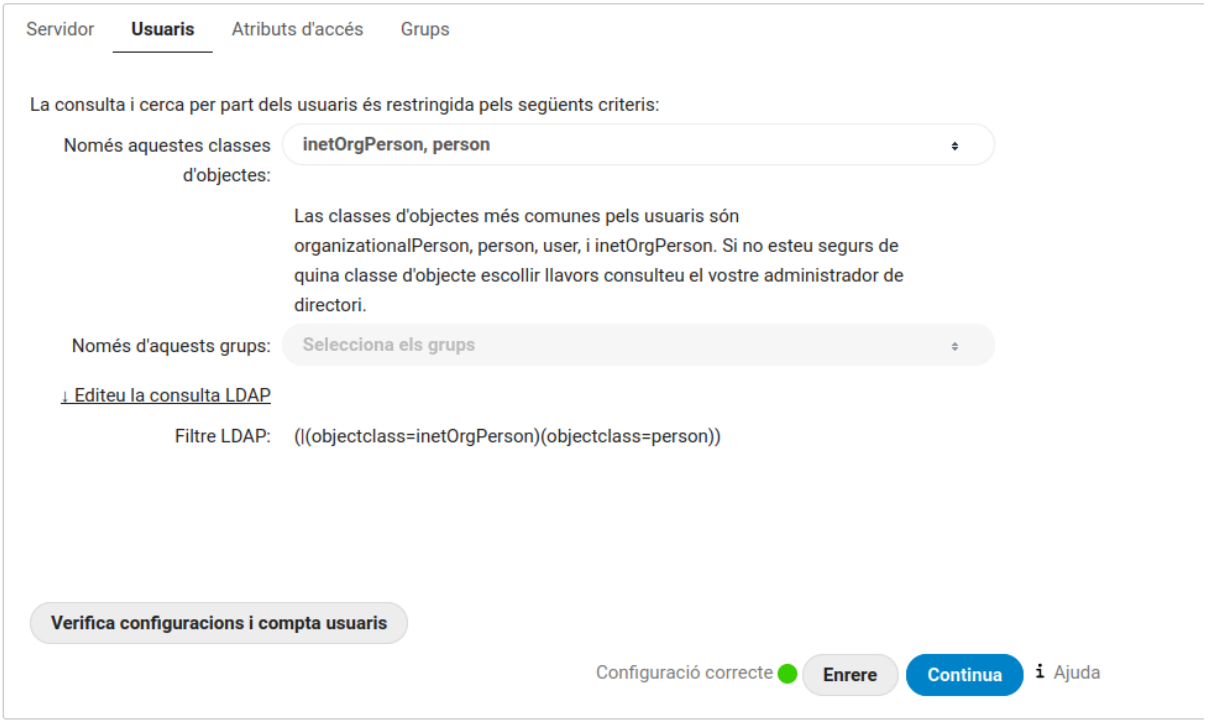


En la primera pantalla que sale, en el caso de este proyecto, la configuración que habrá que aplicar es la siguiente:



En este apartado habrá que indicar la ip del servidor LDAP, el puerto por el que escucha, el usuario administrador del servidor LDAP, su contraseña y la ruta raíz del árbol del servidor LDAP donde se encuentran los usuarios.

A continuación, habrá que entrar en el apartado de “Usuaris” e introducir la siguiente configuración:



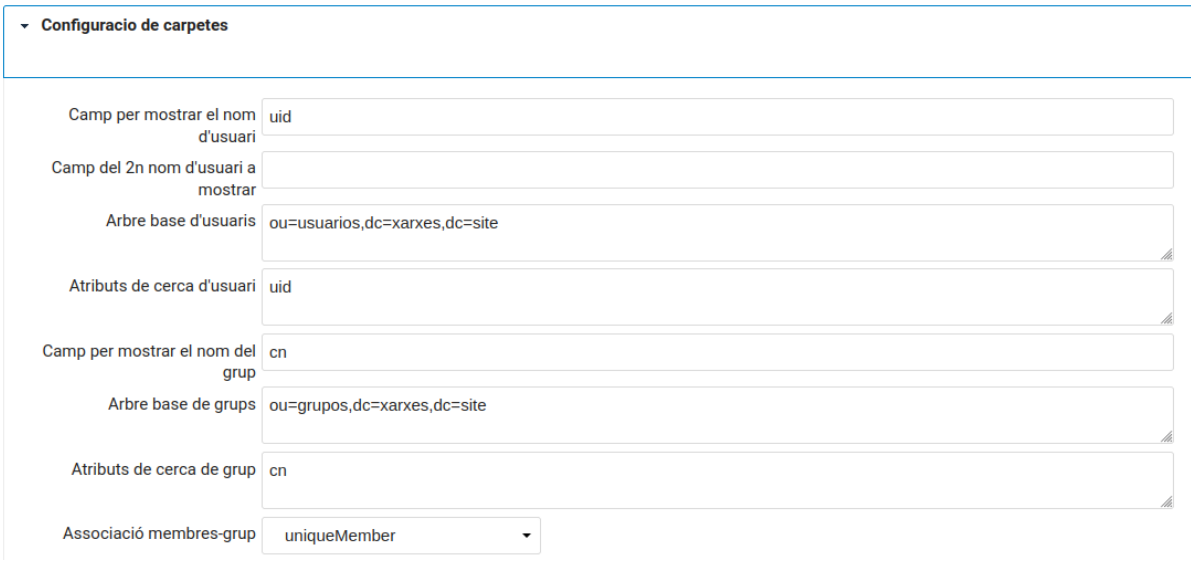
Habrá que indicar que tipo de objetos del servidor LDAP tienen permitido realizar búsquedas sobre este mismo desde el Nextcloud.

Después habrá que acceder al apartado de “Atributs d'accés”

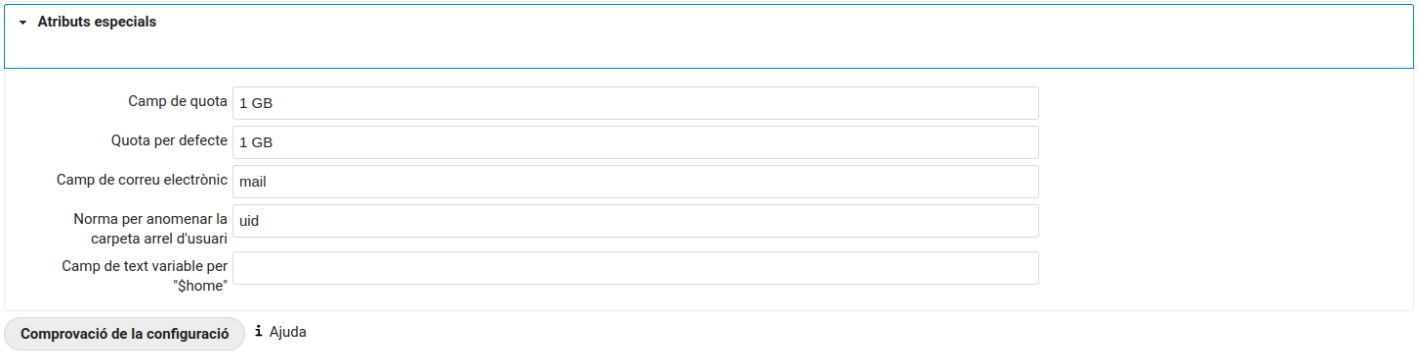
En este apartado habrá que indicar cómo deberá buscar el Nextcloud en el servidor LDAP, es decir el criterio que usará.
A continuación ir al apartado de “Grups” y introducir la siguiente configuración:

En este apartado se deberá indicar qué tipo de objetos del servidor LDAP estarán disponibles para visualizar desde Nextcloud.

En la siguiente imagen se muestra la configuración avanzada del plugin que sirve para poder indicarle a la extensión donde se encuentran los usuarios, los grupos y que campo queremos que seleccione para visualizarlos, es decir le decimos que el nombre de usuario será el UID o que busque a los grupos por el campo CN o que tipo de asociación tienen los miembros de cada grupo(pueden estar asociados como miembro único, por gid, por memberOf,etc...).



En el siguiente apartado se establecerá el espacio disponible que tendrá cada uno de los usuarios, y también el nombre que tendrá su carpeta personal, que será el mismo nombre del usuario.



Por último habrá que realizar las siguientes configuraciones en el servidor LDAP para permitir la lectura de usuarios:

Regla ACL creada para que el plugin del Nextcloud que ofrece la integración con LDAP pueda buscar y leer los usuarios:

```
dn:ou=usuarios,dc=midominio,dc=net
changetype: modify
add:aci
aci:
(target="ldap:///ou=usuarios,dc=midominio,dc=net")(targetattr="*")(version
3.0; acl "xxx"; allow(read,search)(userdn="ldap:///all");)
```

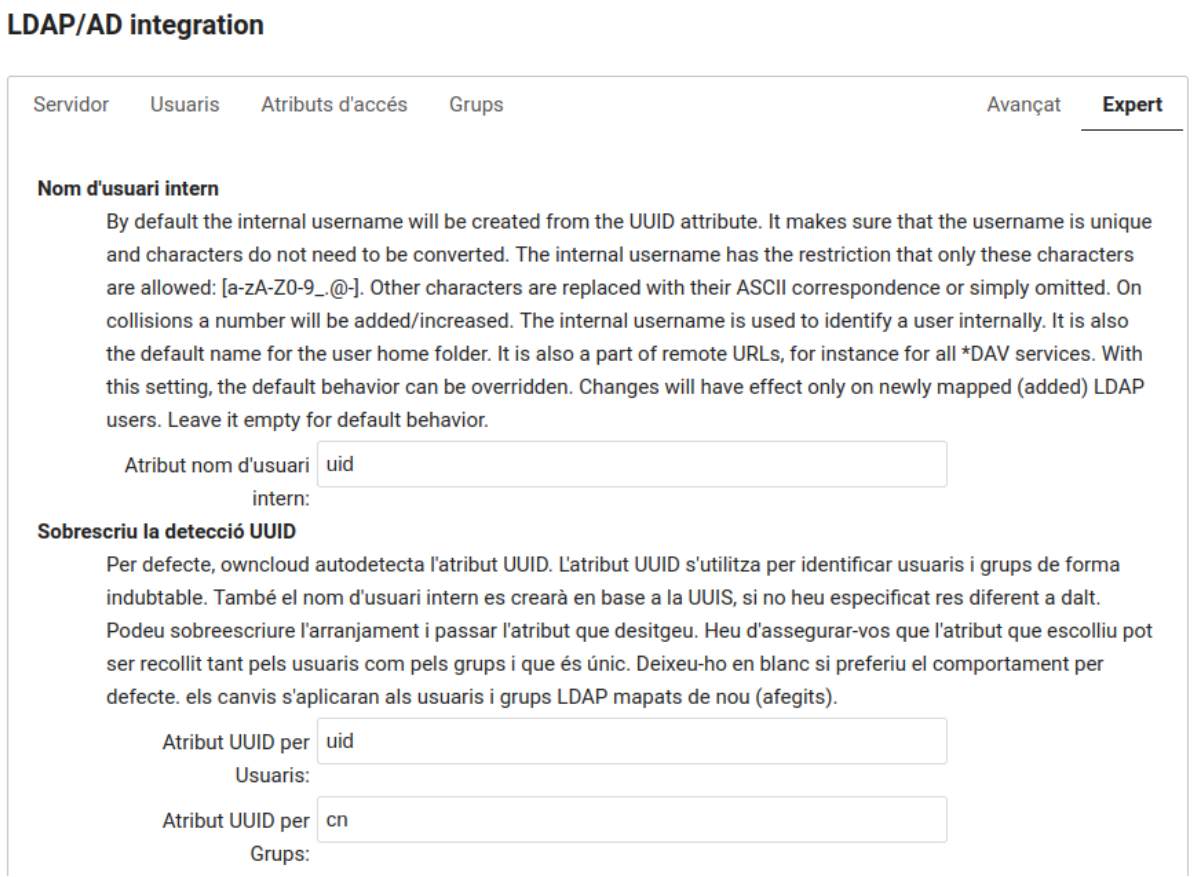
Regla ACL creada para que el plugin del Nextcloud que ofrece la integración con LDAP pueda buscar y leer los grupos :

```
dn:ou=grupos,dc=midominio,dc=net
changetype: modify
add:aci
aci:
(target="ldap:///ou=grupos,dc=midominio,dc=net")(targetattr="*")(version
3.0; acl "xxx"; allow(read,search)(userdn="ldap:///all");)
```

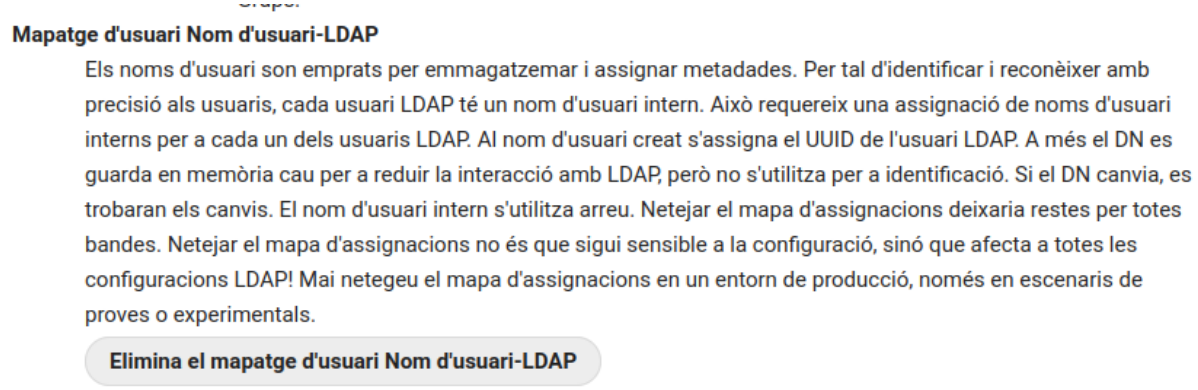
Comando para añadir las ACLs al servidor LDAP, dentro del fichero 'cambiosACLs' se tiene que separar cada regla por un salto de línea:

```
ldapmodify -D cn=admin -W -f cambiosACLs.ldif
```

Cuando el plugin recibe la información del servidor LDAP, por defecto le pone un una serie de caracteres alfanuméricos aleatorios, para que el nombre que le ponga internamente sea el se quiere es decir el del campo UID del servidor LDAP, también tenemos que indicarle que seleccione el uid para que se lo ponga como UUID interno del Nextcloud y el campo CN para identificar a los grupos.

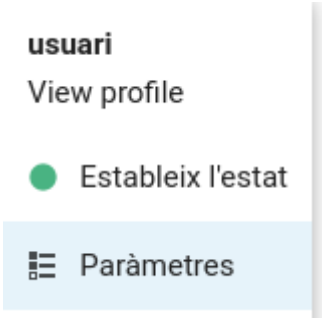


En caso de que ya tuviéramos creados con anterioridad algún usuario con esos caracteres alfanumericos que no se sabe cual es cual podemos decirle al plugin que realice un re-mapeado de los usuarios, para que les vuelva a asignar un nombre:

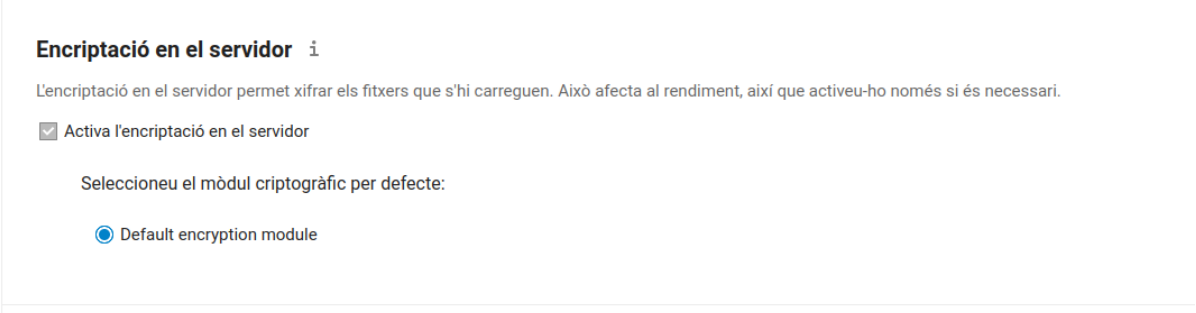


3.4. Encriptación

Para habilitar la encriptación de los ficheros que se encuentran en el servidor, habrá que ir, desde el usuario admin al apartado de parámetros:



Seguidamente al de administración, entrar en seguridad y finalmente habilitar la opción de activar la encriptación del servidor.



4. HAProxy

Para comenzar con la configuración del HAProxy tenemos que hacer primero un frontend que será lo que verá el usuario, es decir en este caso verá que se conectan a través de https:

```
frontend nextldapf
   bind *:443 ssl crt /etc/ssl/nextldap.xarxes.site/nextldap.xarxes.site.pem
   redirect scheme https code 301 if !{ ssl_fc }
   mode http
   default_backend nextldapb
   option forwardfor
        option http-server-close
        option http-pretend-keepalive

        #Only allow some services to be available internally
        acl network_allowed src 192.168.2.0/24
        acl restricted_page path_beg /internal
        block if restricted_page !network_allowed

        # App definitions
        acl is_nc path_beg /nc
```

Pero realmente en la parte del backend le indicamos los servidores que darán servicio, en este caso hay un servidor principal y otro secundario, para decir que es el secundario se lo indicamos con el parámetro backup:

```
backend nextldapb
   mode http
   server serverprincipal 3.223.238.58:80 check
   server serversecundario 54.237.94.94:80 check backup
```

Y para comprobar que se encuentra activo podemos utilizar el comando 'systemctl status haproxy':

```
● haproxy.service - HAProxy Load Balancer
     Loaded: loaded (/lib/systemd/system/haproxy.service; enabled; vendor preset
     Active: active (running) since Fri 2022-05-27 00:45:11 CEST; 9min ago
       Docs: man:haproxy(1)
             file:/usr/share/doc/haproxy/configuration.txt.gz
   Main PID: 600 (haproxy)
      Tasks: 3 (limit: 4691)
     Memory: 9.4M
     CGroup: /system.slice/haproxy.service
             ├─600 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/hap
             └─604 /usr/sbin/haproxy -Ws -f /etc/haproxy/haproxy.cfg -p /run/hap

May 27 00:45:11 nextldap.xarxes.site haproxy[600]: [WARNING] 146/004511 (600) :
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: [WARNING] 146/004511 (600) :
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: [WARNING] 146/004511 (600) :
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: [WARNING] 146/004511 (600) :
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: Proxy nextldapf started.
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: Proxy nextldapf started.
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: Proxy nextldapb started.
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: Proxy nextldapb started.
May 27 00:45:11 nextldap.xarxes.site haproxy[600]: [NOTICE] 146/004511 (600) : N
May 27 00:45:11 nextldap.xarxes.site systemd[1]: Started HAProxy Load Balancer.
```

5. Script creación automática de usuarios LDAP

```
#!/bin/bash

while IFS="," read -r usuario nombre apellidos password uidn gid cpostal
do

cat <<EOF >> alumnos.ldif
dn: uid=$usuario,ou=usuarios,dc=xarxes,dc=site
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
uid: $usuario
cn: ${nombre} ${apellidos}
uidNumber: $uidn
gidNumber: $gid
userPassword: $password
gecos: $usuario
loginShell: /bin/bash
homeDirectory: /home/$usuario
shadowExpire: -1
shadowFlag: 0
```

```
shadowWarning: 7
shadowMin: 8
shadowMax: 999999
shadowLastChange: 10877
displayName: ${nombre} ${apellidos}
sn: $apellidos
mail: ${usuario}@elpuig.xeill.net
postalCode: $cpostal

EOF
done < $1

ldapadd -w admin1234 -D cn=admin -f alumnos.ldif

rm alumnos.ldif
```

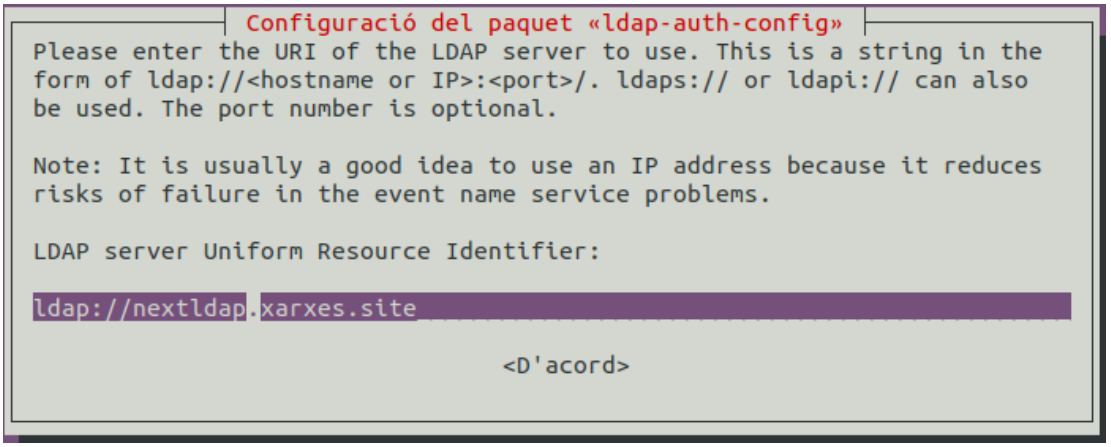
6. Instalación cliente LDAP

1: para instalar el cliente los primeros pasos a realizar serían los de instalar el software necesario y las librerías:

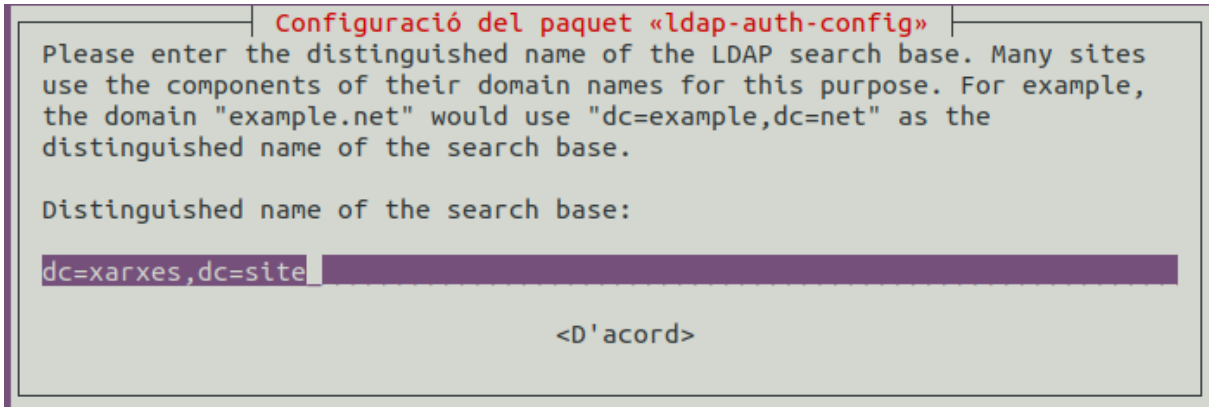
```
sudo apt install libnss-ldap libpam-ldap
```

2: Durante el proceso de instalación van apareciendo una serie de pantallas en las que tenemos que ir rellenando la información necesaria para hacer que se conecte con el servidor LDAP:

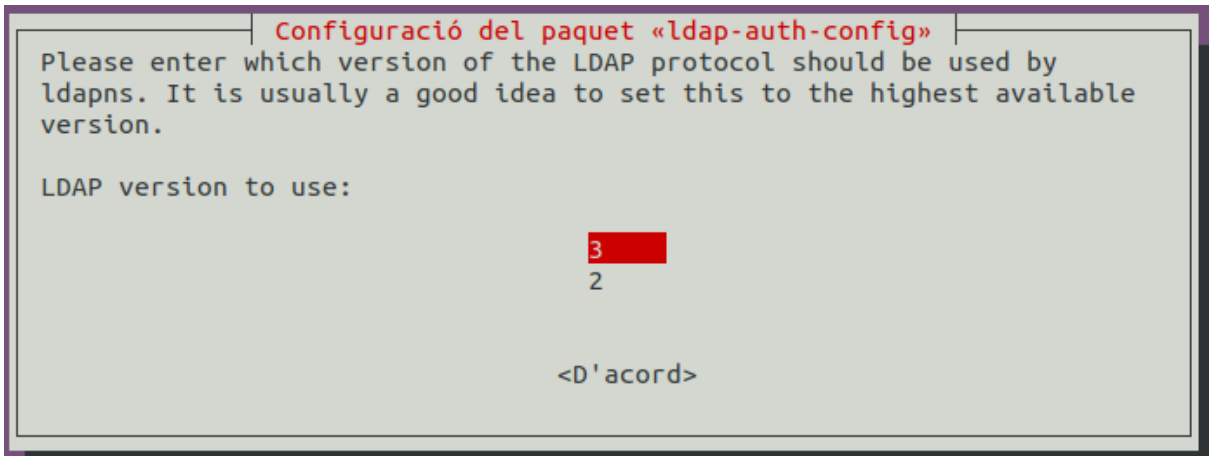
En esta primera pantalla tenemos que indicarle la URL para que se conecte y en función del puerto por el que queremos conectar pondremos ldap(389) o ldaps(636):



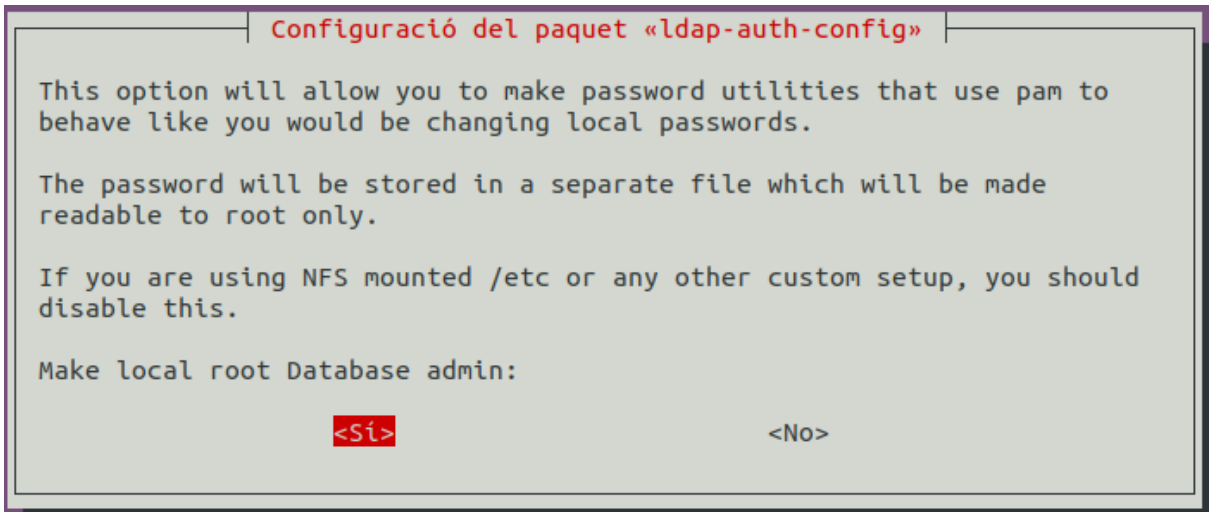
En la siguiente le indicamos cuál será la base de búsqueda en el dominio:

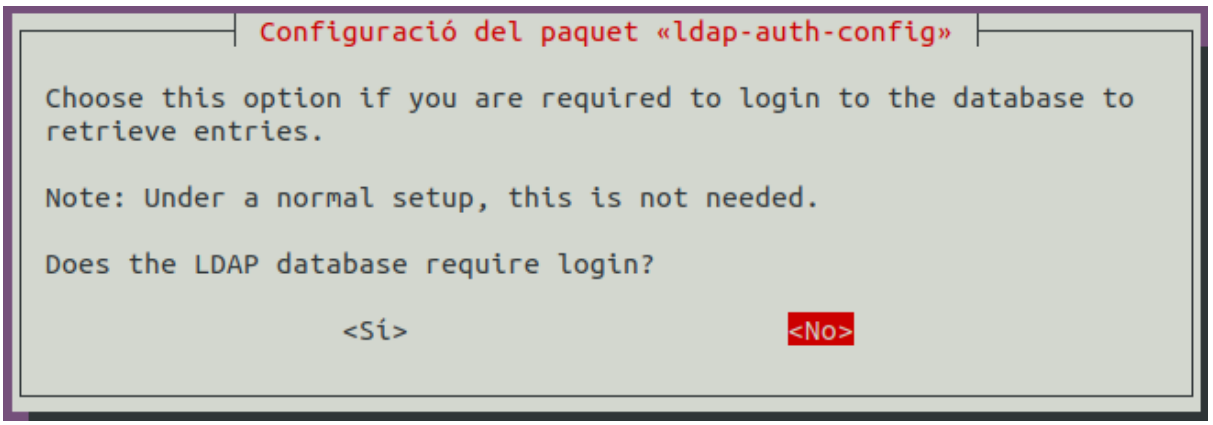


Seleccionamos la versión del protocolo LDAP:

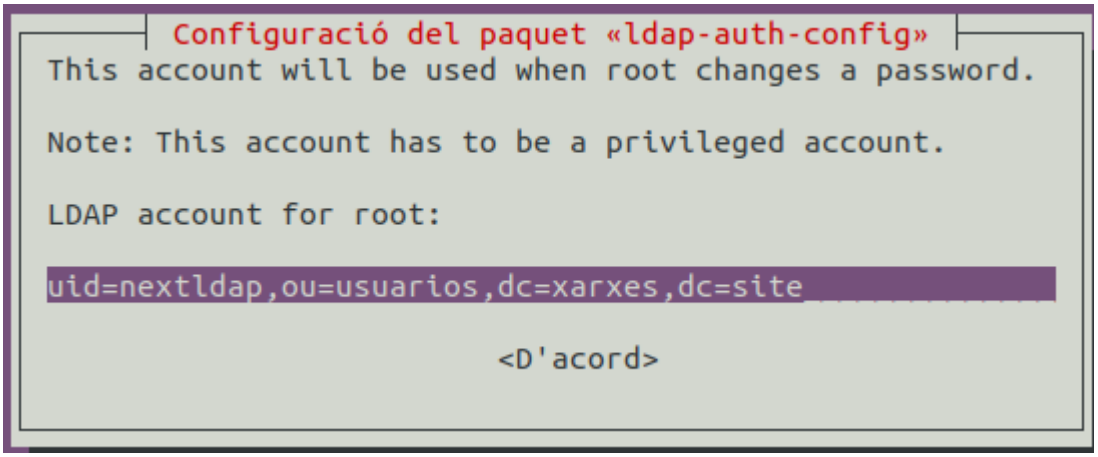


Y las siguientes opciones las dejamos por defecto:

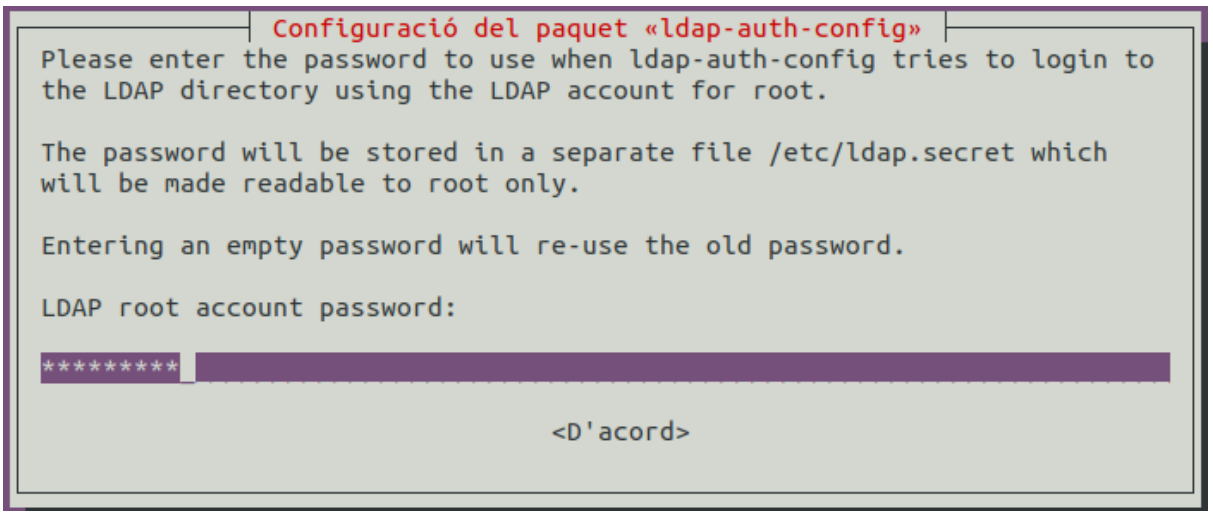




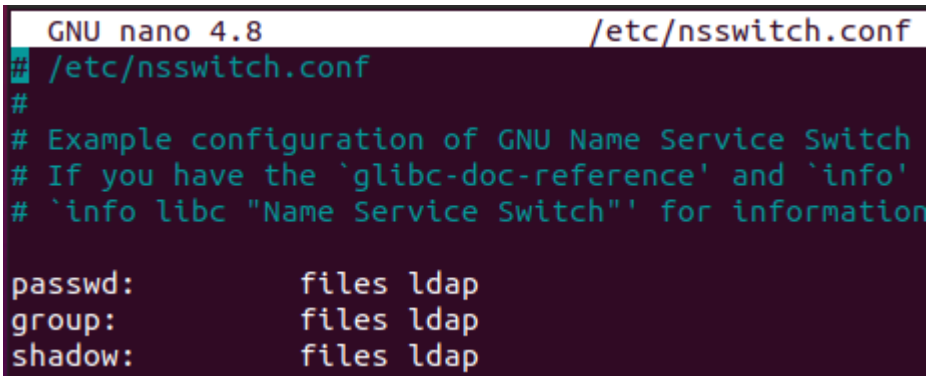
Por último tenemos que poner el usuario que hará de conector entre el servidor y el cliente:



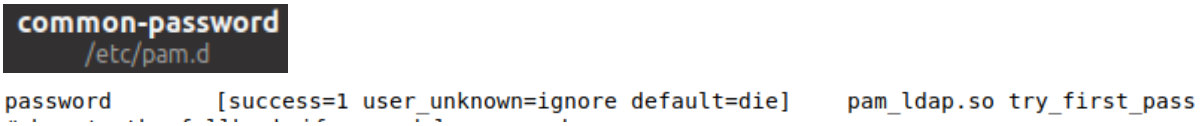
Y le indicamos la contraseña:



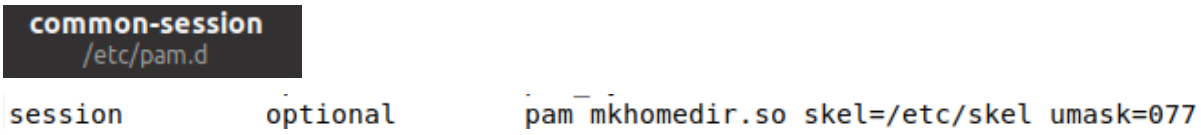
3: Ahora tenemos que modificar el fichero nsswitch para que el sistema coga la nueva información que le llega desde el servidor LDAP:



4: Accedemos al fichero /etc/pam.d/common-password y modificamos la siguiente línea para que quede tal que así:



5: A continuación accedemos al fichero /etc/pam.d/common-session y añadimos la siguiente línea al final de este:



6: Y por ultimo instalamos el paquete que permite a los usuarios hacer login en la interfaz gráfica de Ubuntu:

```
sudo apt install nslcd
```

7: y en la carpeta /etc/skel, añadimos las siguientes líneas al fichero .profile:

```
./inicioSesion.sh &
rm -rf /opt/login/*
touch /opt/login/$LOGNAME
```

Script inicio sesión:

```
#!/bin/bash

keyring get dav2 $USERNAME > /dev/null
status=$?

if [ $status -eq '0' ]
then

 keyring get dav2 $USERNAME > .secret

 gio mount "davs://$USERNAME@nextldap.xarxes.site/remote.php/webdav/" <
.secret

else

 pass1=$(zenity --password --title="Carpeta remota" --width=250
--ok-label="Aceptar" --cancel-label="Cancelar" --text="Vuelve a  introducir la
contraseña porfavor:")

 echo $pass1 > .secret

 gio mount "davs://$USERNAME@nextldap.xarxes.site/remote.php/webdav/" <
.secret

 status1=$?

 if [ $status1 -eq '0' ]

 then

  keyring set dav2 $USERNAME < .secret

  exit

 else

 echo 'la contraseña no es correcta vuelve a ejecutar el script con el comando
./iniciarSesion.sh' > .mensaje.txt

 zenity --text-info --title="Contraseña incorrecta" --filename=.mensaje.txt
--width=500 --height=200
```

```
 fi

fi
```

Este script es el utilizado para que cuando el usuario cierra sesión o apaga la máquina se hace un backup de su home y se sube a su carpeta personal del Nextcloud:

```
#!/bin/sh

usuario=$(ls -A /opt/login/)

su -c 'zip -r $HOME/backup.zip $HOME/*' $usuario

su -c 'while read -r line; do curl -u $LOGNAME:$line -T $HOME/backup.zip
https://nextldap.xarxes.site/remote.php/dav/files/$LOGNAME/; done <
$HOME/.secret' $usuario

su -c 'rm $HOME/backup.zip' $usuario

su -c 'touch $HOME/$usuario' $usuario

rm -rf /opt/login/*

exit 0
```

7. Primera versión de los scripts

A continuación se muestra el primer prototipo de script para cuando los usuarios hacen login que se les bajara la carpeta del home almacenada en la nube a la máquina local:

```
#!/bin/bash

pass=$(zenity --password --title="Desencriptar ficheros" --width=250
--ok-label="Aceptar" --cancel-label="Modo offline" --text="Introduce la
contraseña:")
echo $pass > /tmp/cont.txt
(
echo "10" ; sleep 1
echo "# Desencriptando Home" ;

curl -X GET -u $LOGNAME:$pass
http://miservidor.midominio.net/nextcloud/remote.php/dav/files/$LOGNAME
/dir.zip --output dir.zip

echo "20" ;
unzip dir.zip

echo "# Descomprimiendo zip" ;

sleep 1
echo "50" ; sleep 1
echo "nada" ; sleep 1
echo "75" ; sleep 1
echo "# Restableciendo fichero y config" ; sleep 1
mv dir/* /home/$LOGNAME/
echo "100" ; sleep 1
) |
zenity --progress \
  --title="Desencriptando Home" \
  --text="Espera un momento porfavor..." \
  --percentage=0

if [ "$?" = -1 ] ; then
        zenity --error \
        --text="Fallo al desencriptar"
fi
```

A continuación se muestra el primer prototipo de script para cuando los usuarios cierran sesión que se comprima su home y se suba a su carpeta de Nextcloud, una vez subida se borra la carpeta de la máquina local:

```
#!/bin/bash

while IFS= read -r line
do

zenity --title="Encriptar ficheros" --width=250 --ok-label="Aceptar"

(
echo "10" ; sleep 1
echo "# Comprimiendo Home" ; sleep 1

cd /home/$LOGNAME
zip /home/$LOGNAME/dir.zip *

echo "20" ; sleep 1
echo "# Subiendo Home a la nube" ; sleep 1
echo "50" ; sleep 1

curl -u $LOGNAME:$line -T dir.zip
http://miservidor.midominio.net/nextcloud/remote.php/dav/files/$LOGNAME

echo "nada" ; sleep 1
echo "75" ; sleep 1
echo "# Borrando usuario de la maquina" ; sleep 1
echo "100" ; sleep 1
rm -rf /home/$LOGNAME/*
) |
zenity --progress \
  --title="Encriptando Home" \
  --text="Espera un momento porfavor..." \
  --percentage=0

if [ "$?" = -1 ] ; then
        zenity --error \
        --text="Fallo al desencriptar"
fi

done < /tmp/cont.txt
```