

Recuperación UT4

Tejera Santana Adoney

Recuperación N.º 4 – 2ºA DAW

Curso 2024/2025

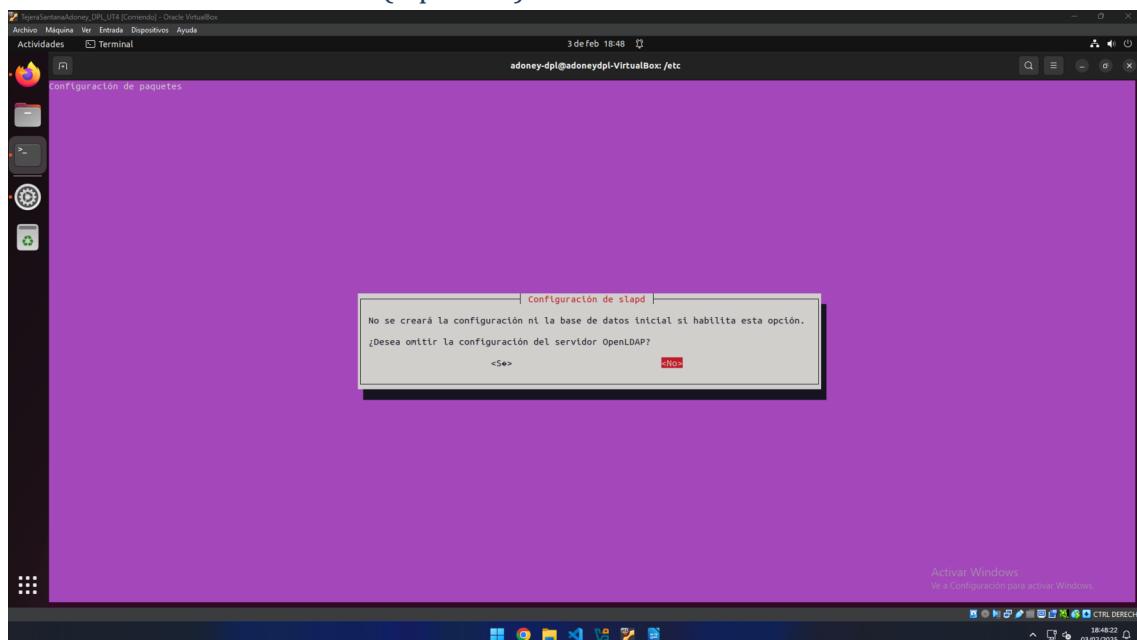
Índice

1 Descripción detallada de los trabajos realizados.....	4
1.1 Haciendo uso de la máquina empleada en clase para el servidor LDAP, hacer las configuraciones oportunas para que se integre en el dominio “examen-daw.ldap” así como modificar el archivo content.ldif para obtener la estructura LDAP que se muestra en la siguiente imagen. Se pide: (3,5 puntos).....	4
1.1.1 a) Configurar el Servidor LDAP para el nuevo dominio examen-daw.ldap y realizar el archivo content.ldif para obtener la estructura LDAP de la imagen. Realizar la carga en el directorio LDAP. Además quitar del archivo de hosts la referencia de dominio que hicimos de dpldaw.ldap. Ponerle una contraseña diferente a cada usuario, poner de contraseña el nombre del usuario. Aportar captura de pantalla de la nueva configuración del dominio del servidor LDAP obtenida con el comando desde terminal y captura con el contenido del archivo content.ldif, así como captura con la carga del archivo content.ldif al LDAP (2 puntos).....	4
1.1.2 b) Mostrar la estructura de directorios creada en LDAP con el phpLDAPAdmin, así como el contenido del /etc/hosts Aportar captura con la estructura LDAP mostrada en phpLDAPAdmin y captura del archivo hosts después de quitar o comentar la referencia a dpl-daw.ldap (1,5 puntos).....	7
1.2 Realizar los pasos correspondientes para crear un virtualhost llamado “villaaguimes.local” en una máquina cliente o en la misma del Servidor LDAP, que contenga dos carpetas con acceso limitadas (web y multiplataformas) con control de acceso por LDAP. Puedes hacer uso del archivo 000-default.conf Se pide: (3,5 puntos).....	8
1.2.1 a) Crear el sitio virtual con el dominio indicado, las carpetas web y multiplataformas, así como las configuraciones en Apache para que LDAP controle el acceso de los usuarios de acuerdo a su grupo a esas carpetas. A continuación se muestran los índices de referencia a incluir en esas carpetas.....	8
1.2.2 b) Realizar las pruebas correspondientes y habilitar el módulo correspondiente para la integración con LDAP si no es la máquina empleada en la actividad. Aportar captura de pantalla donde se muestre que pueden acceder los usuarios a sus áreas correspondientes e incluso que se vea que el navegador te solicita guardar la contraseña. Con que lo hagas para un usuario en cada área y uno que no tenga permisos para acceder a un área es suficiente (1,5 puntos).....	12

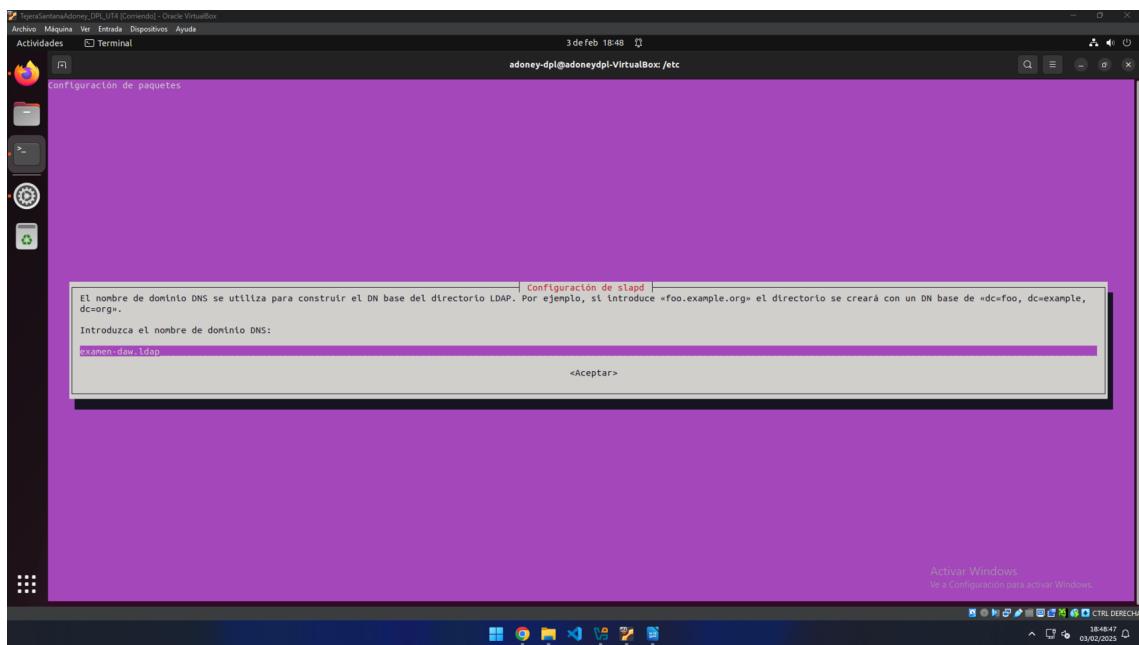
1.3 En la máquina del servidor DNS de clase asociar al dominio creado en la actividad nombrealumno.net, los siguientes subdominios:	
• ldap.nombre-alumno.net – IP del Servidor LDAP	
• villaaguimes.nombre-alumno.net – IP del Servidor WEB configurado en el apartado 2.....	14
2 Herramientas empleadas.....	17
3 Problemática encontrada y solución.....	17
4 Conclusiones.....	18

1 Descripción detallada de los trabajos realizados

- 1.1 Haciendo uso de la máquina empleada en clase para el servidor LDAP, hacer las configuraciones oportunas para que se integre en el dominio “examen-daw.ldap” así como modificar el archivo content.ldif para obtener la estructura LDAP que se muestra en la siguiente imagen. Se pide: (3,5 puntos).
- 1.1.1 a) Configurar el Servidor LDAP para el nuevo dominio examen-daw.ldap y realizar el archivo content.ldif para obtener la estructura LDAP de la imagen. Realizar la carga en el directorio LDAP. Además quitar del archivo de hosts la referencia de dominio que hicimos de dpldap.ldap. Ponerle una contraseña diferente a cada usuario, poner de contraseña el nombre del usuario. Aportar captura de pantalla de la nueva configuración del dominio del servidor LDAP obtenida con el comando desde terminal y captura con el contenido del archivo content.ldif, así como captura con la carga del archivo content.ldif al LDAP (2 puntos).



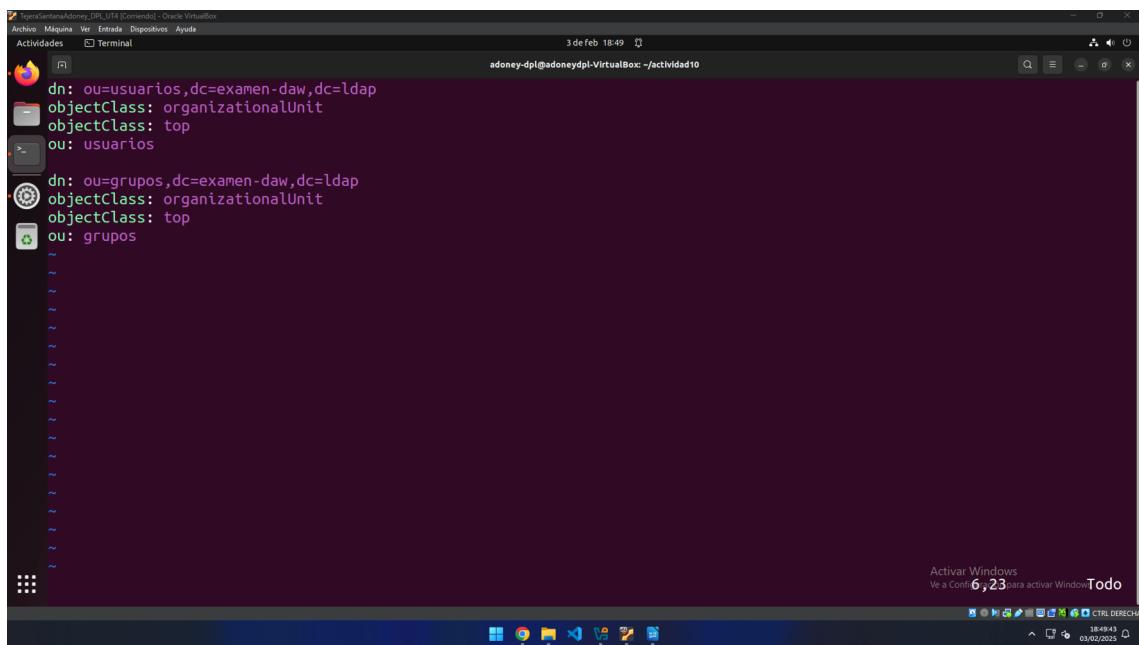
Empezamos reconfigurando el servicio.



Y se asigna el nuevo nombre.

```
adoney-dpl@adoneydpl-VirtualBox:~/actividad10$ sudo slacdap
dn: dc=examen,dw,dc=daw
objectclass: top
objectclass: containerObject
objectclass: organization
o: examen-daw-adoney
dc: examen-daw-adoney
structuralObjectClass: organization
entryUUID: 49b5258e-7eb-103f-84bd-8d8a50335e6a
creatorsName: cn=admin,dc=examen-daw,dc=daw
createTimestamp: 20250203184905Z#00000000#0000000000
modifiersName: cn=admin,dc=examen-daw,dc=daw
modifyTimestamp: 20250203184905Z#00000000#0000000000
```

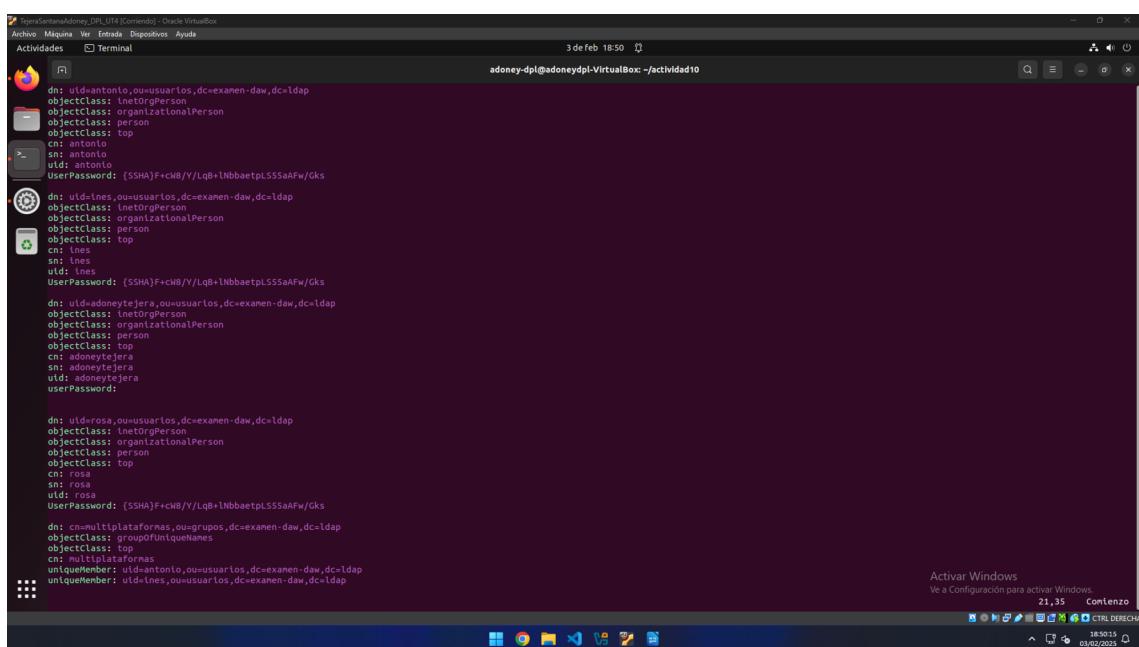
Se comprueba la configuración.



```
dn: ou=usuarios,dc=examen-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: usuarios

dn: ou=grupos,dc=examen-daw,dc=ldap
objectClass: organizationalUnit
objectClass: top
ou: grupos
```

Ahora construimos el fichero baso con los usuarios y grupos.



```
dn: uid=antonio,ou=usuarios,dc=examen-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: antonio
sn: antonio
uid: antonio
UserPassword: {SSHA}F+cW8/Y/Lqb+lnbbaetpl555aAFw/Gks

dn: uid=adoneytejera,ou=usuarios,dc=examen-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: adoneytejera
sn: adoneytejera
uid: adoneytejera
UserPassword: {SSHA}F+cW8/Y/Lqb+lnbbaetpl555aAFw/Gks

dn: uid=rosa,ou=usuarios,dc=examen-daw,dc=ldap
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
cn: rosa
sn: rosa
uid: rosa
UserPassword: {SSHA}F+cW8/Y/Lqb+lnbbaetpl555aAFw/Gks

dn: cn=multiplataformas,ou=grupos,dc=examen-daw,dc=ldap
objectClass: groupOfUniqueNames
objectClass: top
cn: multiplataformas
uniqueMember: uid=antonio,ou=usuarios,dc=examen-daw,dc=ldap
uniqueMember: uid=ines,ou=usuarios,dc=examen-daw,dc=ldap
```

Ahora el fichero content con todos los usuarios.

```

adoney-dpl@adoneydpl-VirtualBox: ~/actividad10$ sudo ldapadd -x -D cn=admin,dc=examen-daw,dc=ldap -W -f base.ldif
Enter LDAP Password:
adding new entry "ou=usuarios,dc=examen-daw,dc=ldap"
adding new entry "ou=grupos,dc=examen-daw,dc=ldap"
> adoney-dpl@adoneydpl-VirtualBox: ~/actividad10$ sudo ldapadd -x -D cn=admin,dc=examen-daw,dc=ldap -W -f content.ldif
Enter LDAP Password:
adding new entry "uid=unes,ou=usuarios,dc=examen-daw,dc=ldap"
adding new entry "uid=adoneytejera,ou=usuarios,dc=examen-daw,dc=ldap"
adding new entry "uid=rosa,ou=usuarios,dc=examen-daw,dc=ldap"
adding new entry "cn=multiplatformas,ou=grupos,dc=examen-daw,dc=ldap"
adding new entry "cn=web,ou=grupos,dc=examen-daw,dc=ldap"
adoney-dpl@adoneydpl-VirtualBox: ~/actividad10$ 

```

Ahora se inserta los datos a ldap.

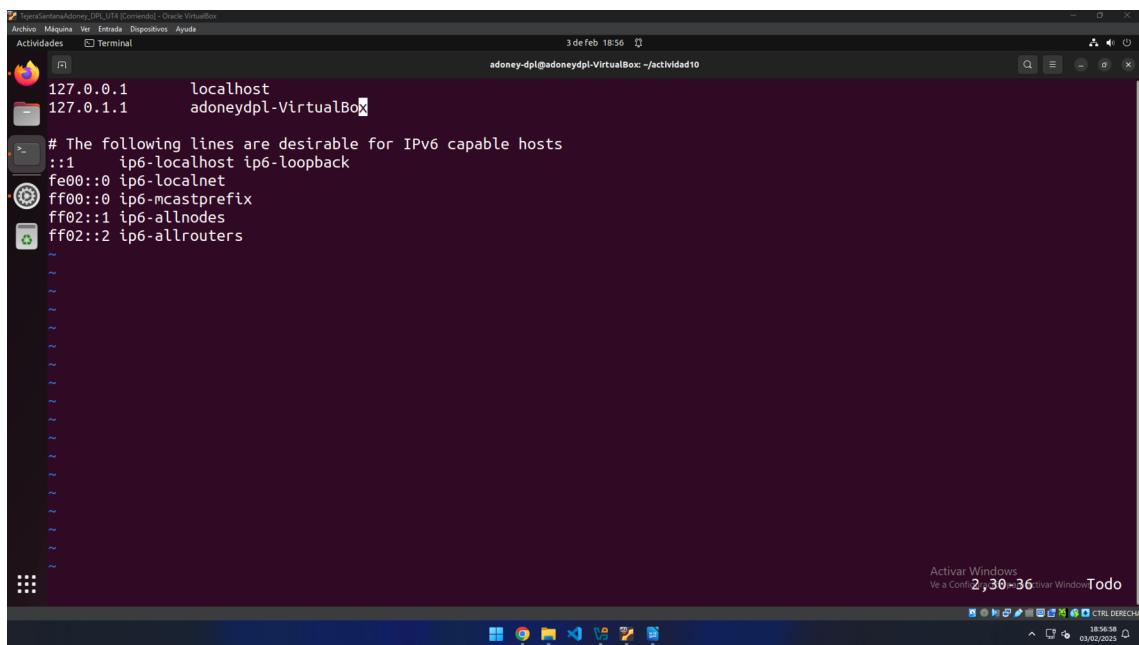
- 1.1.2 b) Mostrar la estructura de directorios creada en LDAP con el phpLDAPAdmin, así como el contenido del /etc/hosts Aportar captura con la estructura LDAP mostrada en phpLDAPAdmin y captura del archivo hosts después de quitar o comentar la referencia a dpl-daw.ldap (1,5 puntos).

The screenshot shows the phpLDAPAdmin interface running in a Firefox browser. The URL is `localhost/phpLDAPadmin/cmd.php?server_id=1&redirect=true`. The page title is "phpLDAPadmin". On the left, there's a sidebar with icons for search, refresh, info, import, export, and exit. It also shows the user is logged in as "cn=admin,dc=examen-daw,dc=ldap". The main content area shows a tree view of the LDAP structure under "My LDAP Server". The structure includes:

- dc=examen-daw,dc=ldap (2 children)
 - ou=grupos (2 children)
 - cn=multiplatformas
 - cn=web
 - * Crear nuevo objeto
- ou=usuarios (4 children)
 - uid=adoneytejera
 - uid=unes
 - uid=rosa
 - * Crear nuevo objeto
- * Crear nuevo objeto

 To the right of the tree view is a logo for "phpLDAPadmin" and a message: "Use el menú de la izquierda para navegar". At the bottom right, it says "1.2.6.3".

Se comprueba la estructura en ldapadmin.



The screenshot shows a terminal window titled "Terminal" with the command "adoney-dpl@adoneydpl-VirtualBox: ~/actividad10". The window displays the contents of an Apache configuration file, specifically the /etc/apache2/sites-available/000-default.conf. The configuration includes the following lines:

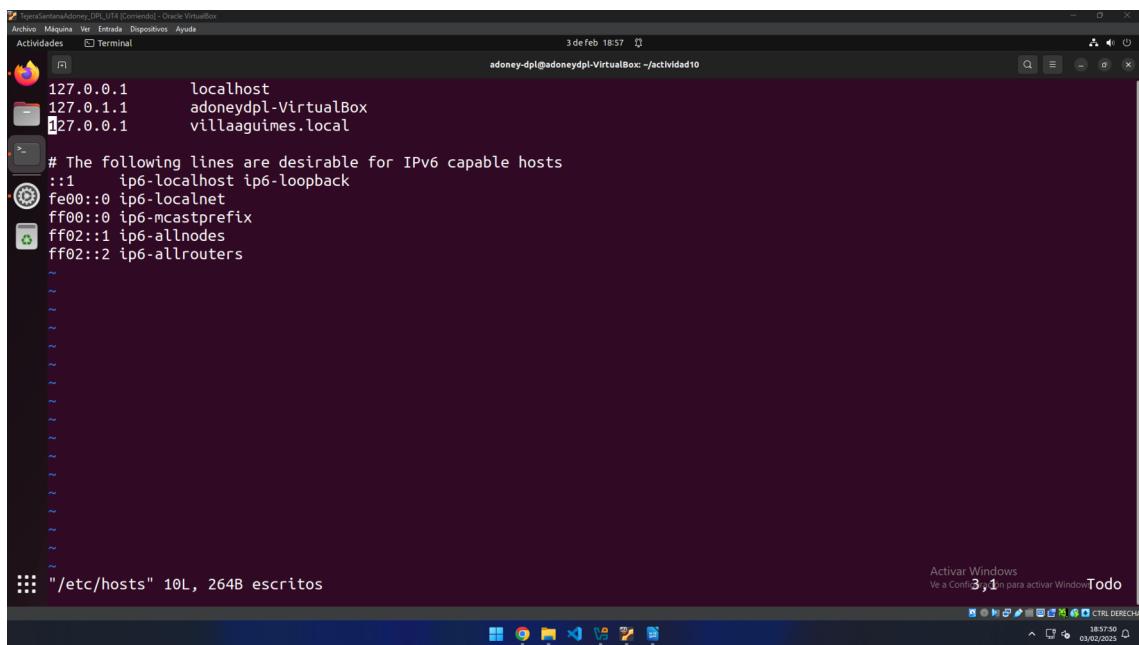
```
127.0.0.1      localhost
127.0.1.1      adoneydpl-VirtualBox

# The following lines are desirable for IPv6 capable hosts
::1    ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Y el del fichero htdocs.

1.2 Realizar los pasos correspondientes para crear un virtualhost llamado “villaaguimes.local” en una máquina cliente o en la misma del Servidor LDAP, que contenga dos carpetas con acceso limitadas (web y multiplataformas) con control de acceso por LDAP. Puedes hacer uso del archivo 000-default.conf Se pide: (3,5 puntos)

1.2.1 a) Crear el sitio virtual con el dominio indicado, las carpetas web y multiplataformas, así como las configuraciones en Apache para que LDAP controle el acceso de los usuarios de acuerdo a su grupo a esas carpetas. A continuación se muestran los índices de referencia a incluir en esas carpetas.

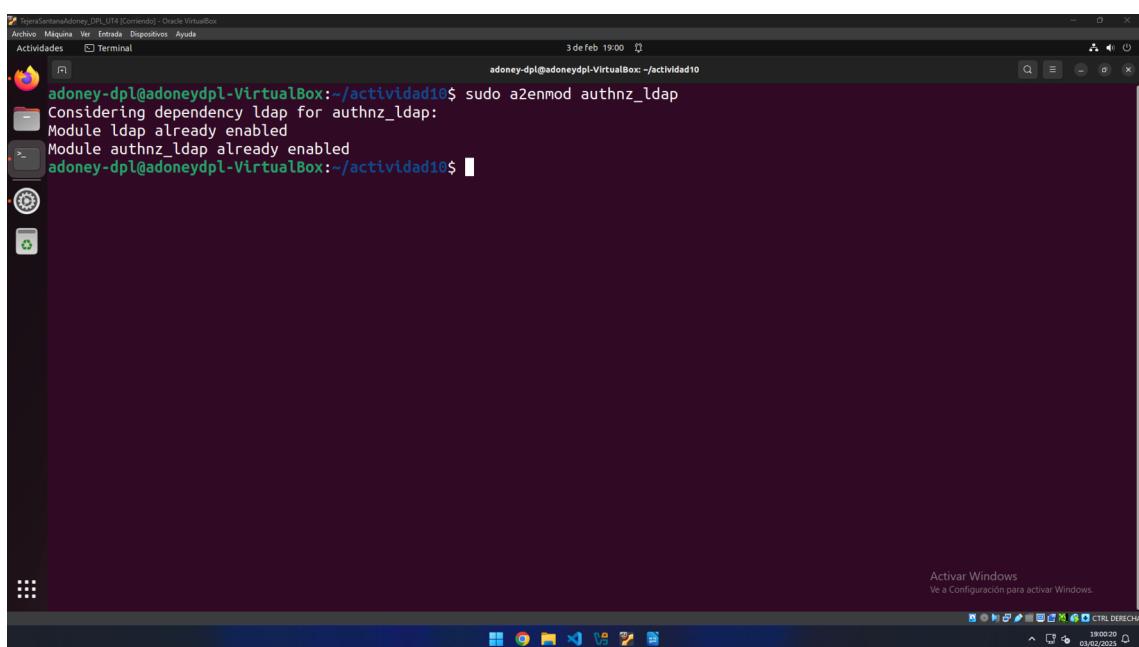


```
127.0.0.1      localhost
127.0.1.1      adoneydpl-VirtualBox
127.0.0.1      villaaguimes.local

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

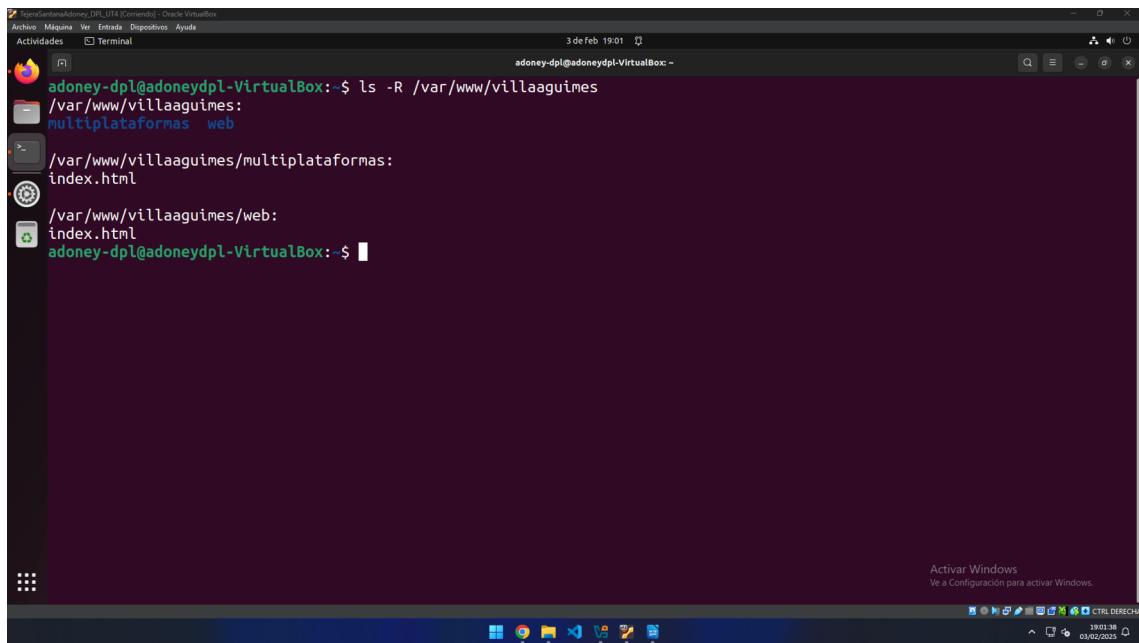
"/etc/hosts" 10L, 264B escritos
```

Lo primero será añadir la ruta localhost con nombre villaaguimes.local.



```
adoney-dpl@adoneydpl-VirtualBox:~/actividad10$ sudo a2enmod authnz_ldap
Considering dependency ldap for authnz_ldap:
Module ldap already enabled
Module authnz_ldap already enabled
adoney-dpl@adoneydpl-VirtualBox:~/actividad10$
```

Me aseguro de tener el módulo necesario instalado.

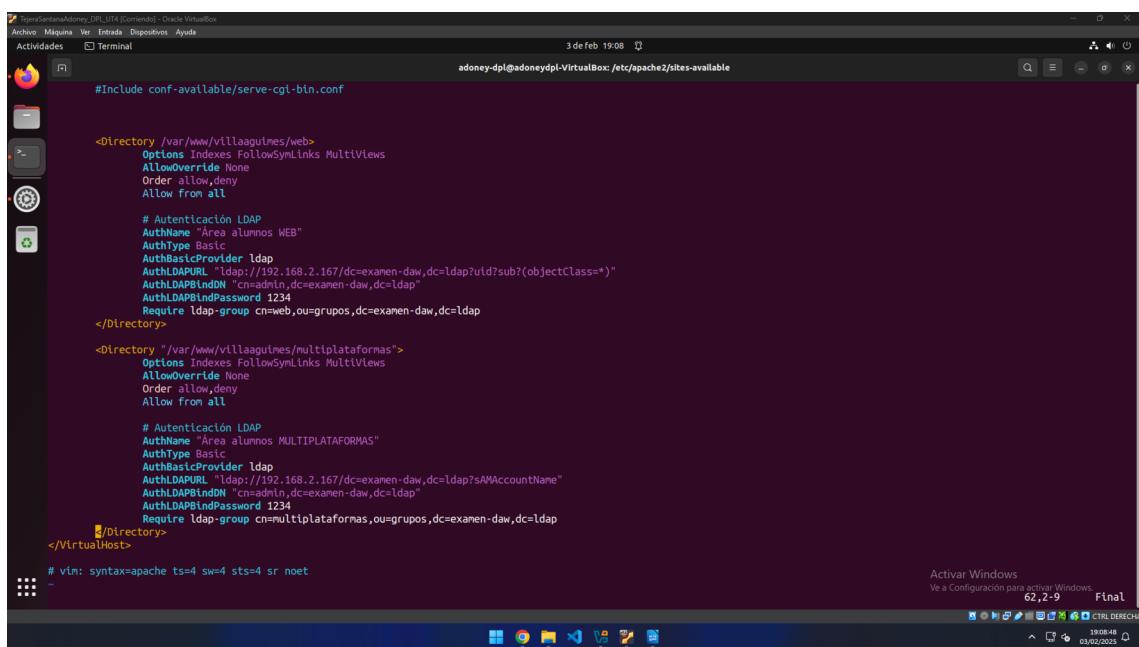


```
adoney-dpl@adoneydpl-VirtualBox: $ ls -R /var/www/villaaguimes
/var/www/villaaguimes:
multiplataformas web

/var/www/villaaguimes/multiplataformas:
index.html

/var/www/villaaguimes/web:
index.html
adoney-dpl@adoneydpl-VirtualBox: $
```

Creamos las carpetas y ficheros necesarios en var/www/villaaguimes.



```
#Include conf-available/serve-cgi-bin.conf

<Directory /var/www/villaaguimes/web>
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all

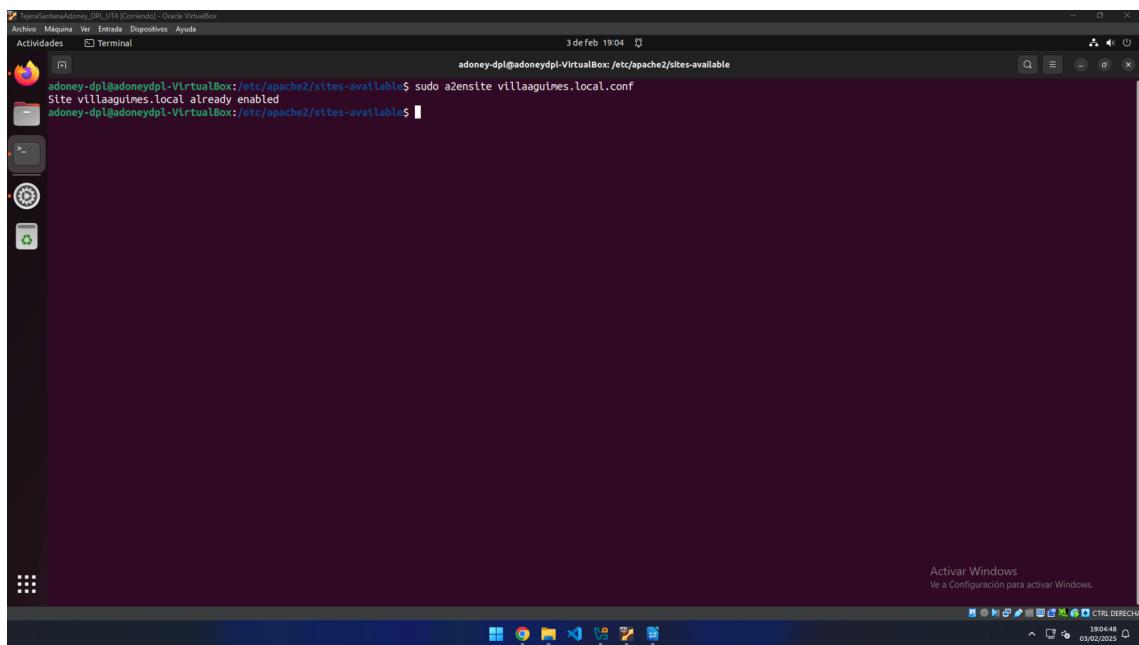
    # Autenticación LDAP
    AuthName "Área alumnos WEB"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://192.168.2.167/dc=examen-daw,dc=ldap?uid?sub?(objectClass=*)"
    AuthLDAPBindDN "cn=admin,dc=examen-daw,dc=ldap"
    AuthLDAPBindPassword 1234
    Require ldap-group cn=web,ou=grupos,dc=examen-daw,dc=ldap
</Directory>

<Directory "/var/www/villaaguimes/multiplataformas">
    Options Indexes FollowSymLinks MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all

    # Autenticación LDAP
    AuthName "Área alumnos MULTIPLATAFORMAS"
    AuthType Basic
    AuthBasicProvider ldap
    AuthLDAPURL "ldap://192.168.2.167/dc=examen-daw,dc=ldap?sAMAccountName"
    AuthLDAPBindDN "cn=admin,dc=examen-daw,dc=ldap"
    AuthLDAPBindPassword 1234
    Require ldap-group cn=multiplataformas,ou=grupos,dc=examen-daw,dc=ldap
</Directory>
</VirtualHost>

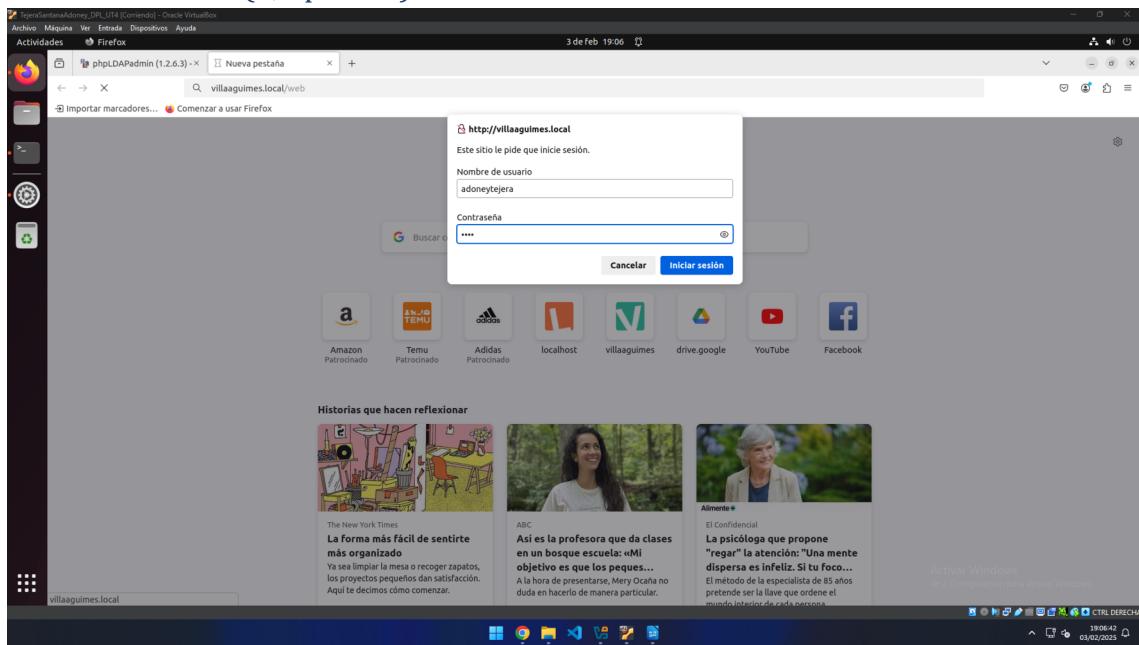
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet
```

Procedemos a crear y llenar un virtualhost villaaguimes.local.conf, el cual contendrá el directorio para el alumnado de Web y de Multiplataformas. En este caso ya contiene la configuración para la validación de usuarios.

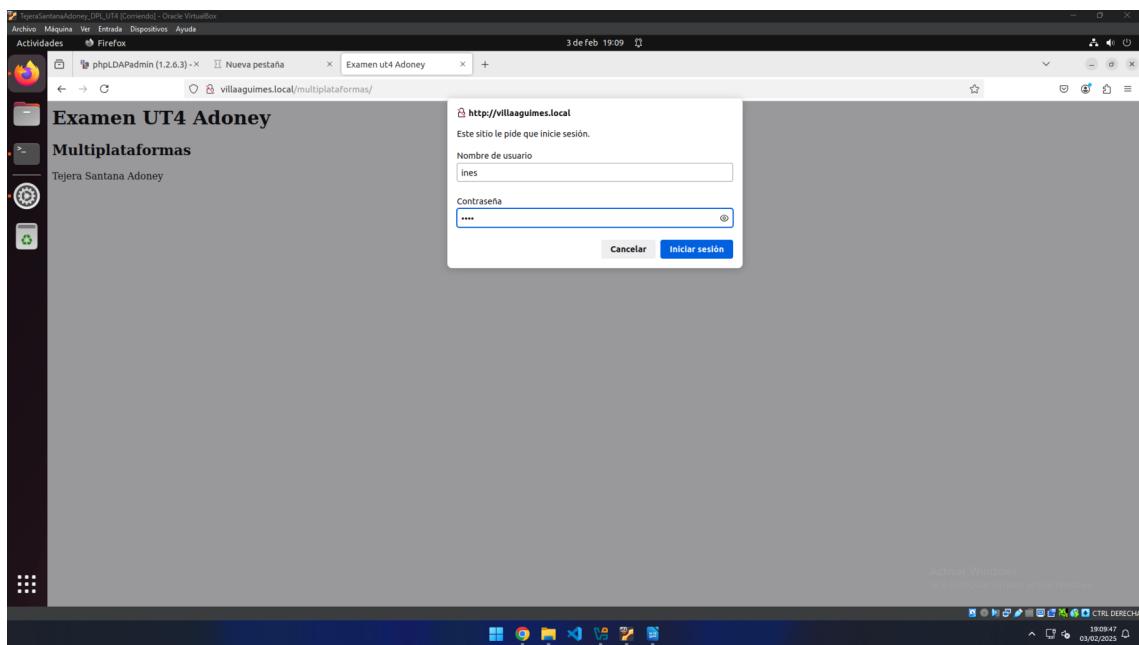


Habilitamos el virtualhost creado.

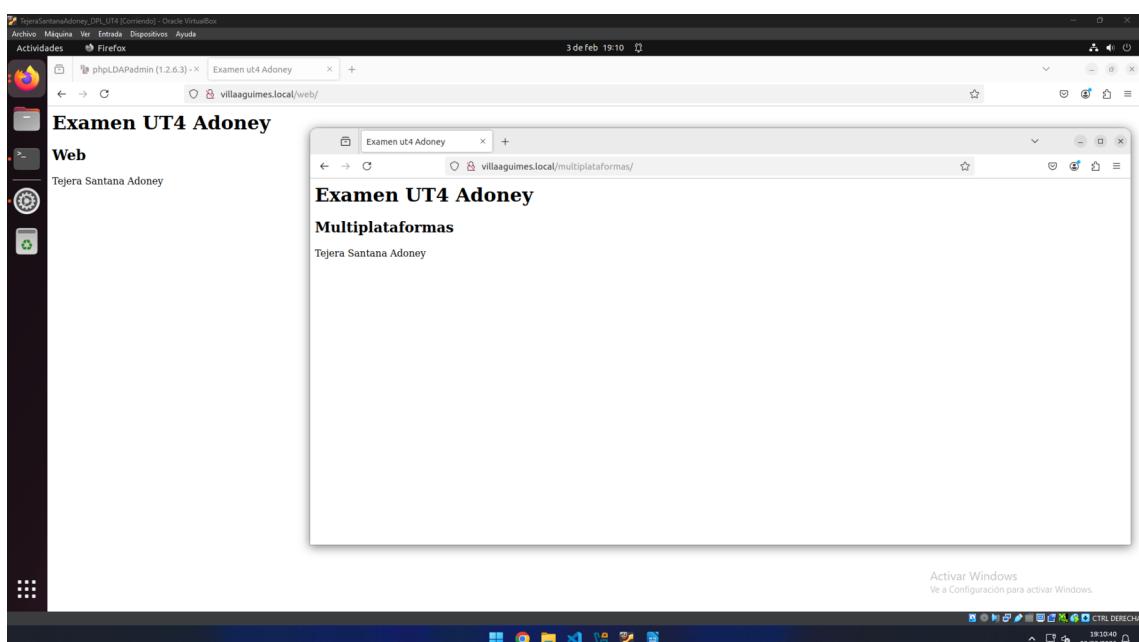
1.2.2 b) Realizar las pruebas correspondientes y habilitar el módulo correspondiente para la integración con LDAP si no es la máquina empleada en la actividad. Aportar captura de pantalla donde se muestre que pueden acceder los usuarios a sus áreas correspondientes e incluso que se vea que el navegador te solicita guardar la contraseña. Con que lo hagas para un usuario en cada área y uno que no tenga permisos para acceder a un área es suficiente (1,5 puntos).



Procedemos a comprobar la autenticación y se puede ver que nos pide usuario y contraseña en la ruta web.

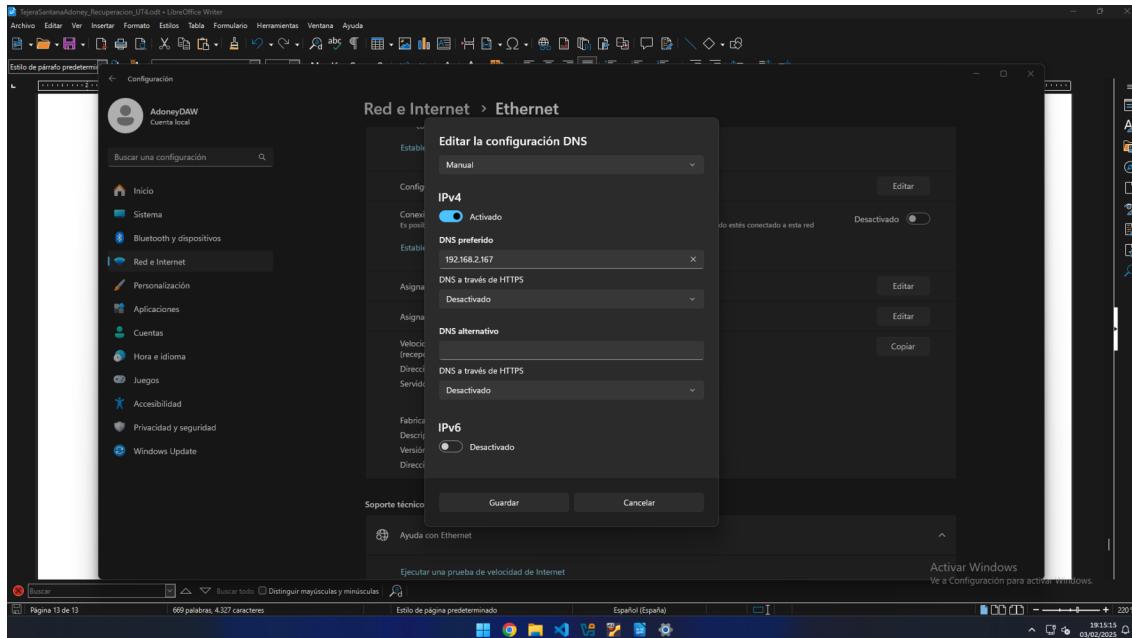


Y ahora con el de multiplataformas.

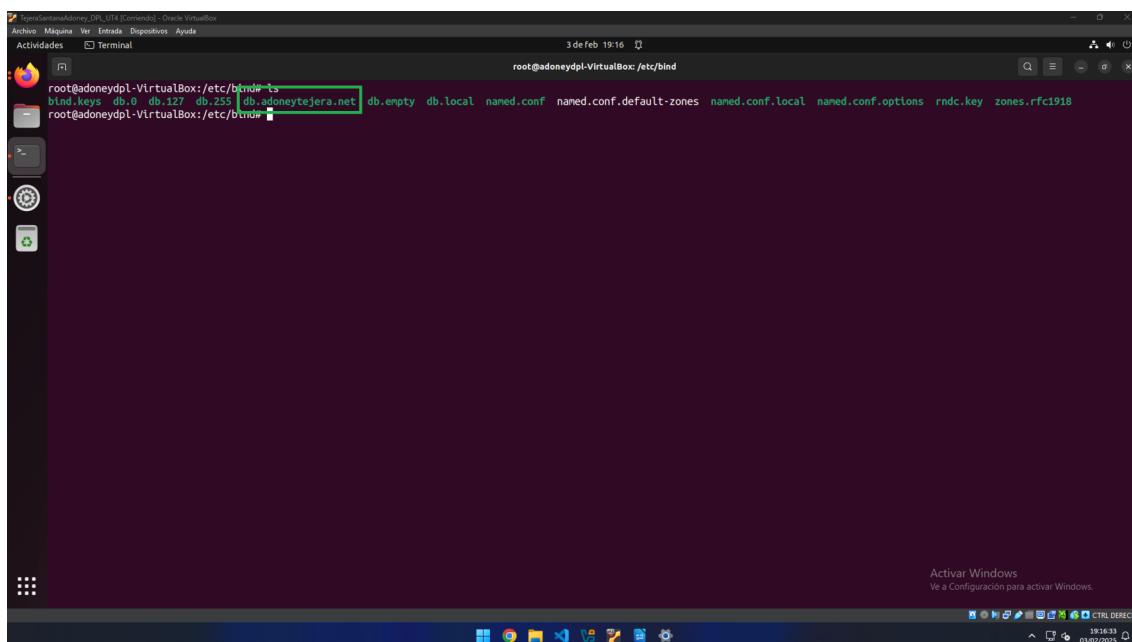


Y nos termina permitiendo acceder a las páginas configuradas.

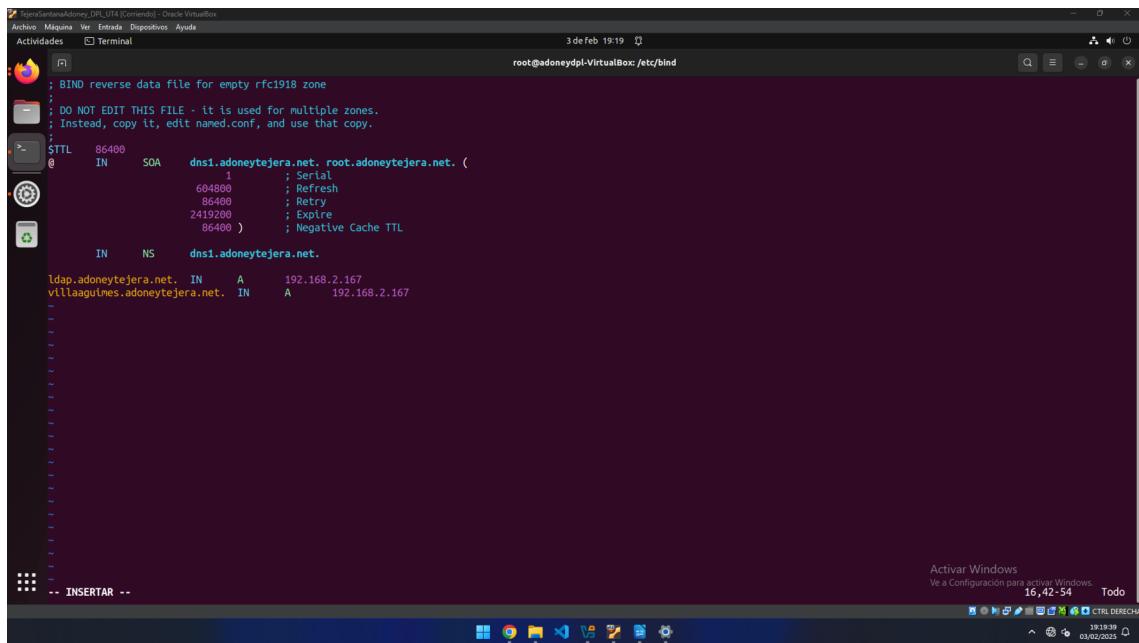
- 1.3 En la máquina del servidor DNS de clase asociar al dominio creado en la actividad nombrealumno.net, los siguientes subdominios:
- ldap.nombre-alumno.net – IP del Servidor LDAP
 - villaaguimes.nombre-alumno.net – IP del Servidor WEB configurado en el apartado 2.



Comenzamos asignando al servidor ubuntu como dns en nuestro sistema.



Posteriormente creamos un fichero db.adoneytejera.net para la configuración de los dominios.



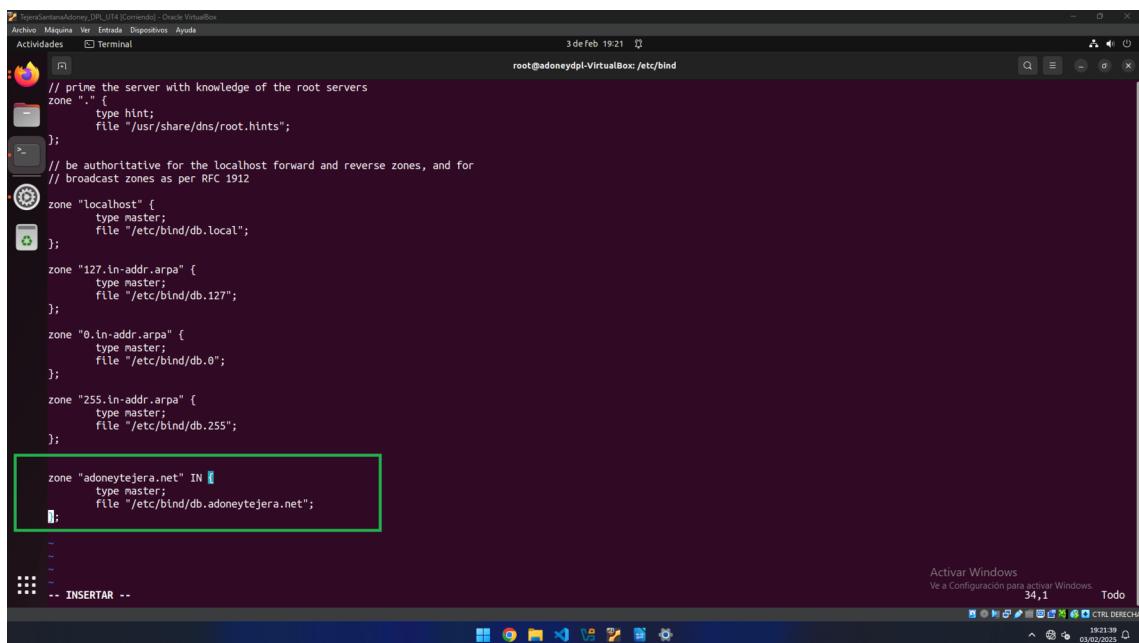
```
; BIND reverse data file for empty rfc1918 zone
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.

$TTL 86400
@ IN SOA dns1.adoneytejera.net. root.adoneytejera.net. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    6400 ) ; Negative Cache TTL

IN NS dns1.adoneytejera.net.

ldap.adoneytejera.net. IN A 192.168.2.167
villaaguimes.adoneytejera.net. IN A 192.168.2.167
```

Agregamos las rutas al fichero que acabamos de crear



```
// prime the server with knowledge of the root servers
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};

zone "adoneytejera.net" IN {
    type master;
    file "/etc/bind/db.adoneytejera.net";
};
```

Añadimos la zona a la configuración de por defecto de bind9.



Activar Windows
Ve a Configuración para activar Windows.



Se comprueba desde la máquina anfitrión que el dns funciona.

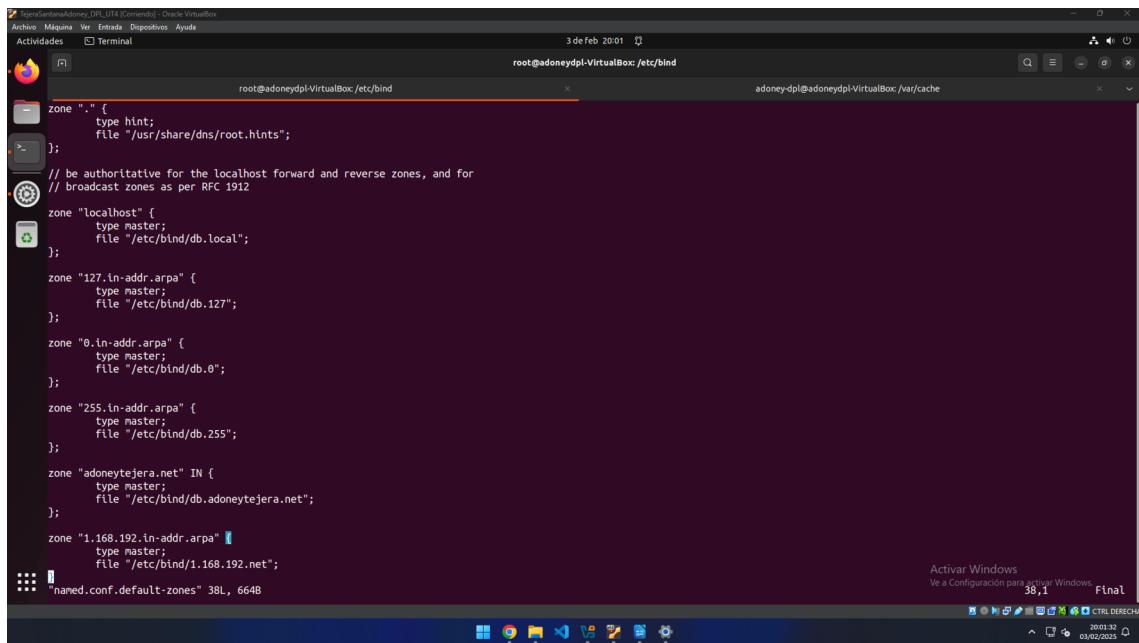
```
; BIND reverse data file for empty rfc1918 zone
; DO NOT EDIT THIS FILE - it is used for multiple zones.
; Instead, copy it, edit named.conf, and use that copy.

$TTL 86400
@ IN SOA ldap.adoneytejera.net. root.adoneytejera.net. (
    1 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    86400 ) ; Negative Cache TTL

;
IN NS ldap.adoneytejera.net.
167 IN PTR ldap.adoneytejera.net.

"db.1.168.192.net" 16L, 418B escritos
```

Y se configura al inverso.



```
root@adoneydpl-VirtualBox:/etc/bind
zone "." {
    type hint;
    file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912
zone "localhost" {
    type master;
    file "/etc/blnd/db.local";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/blnd/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/blnd/db.0";
};

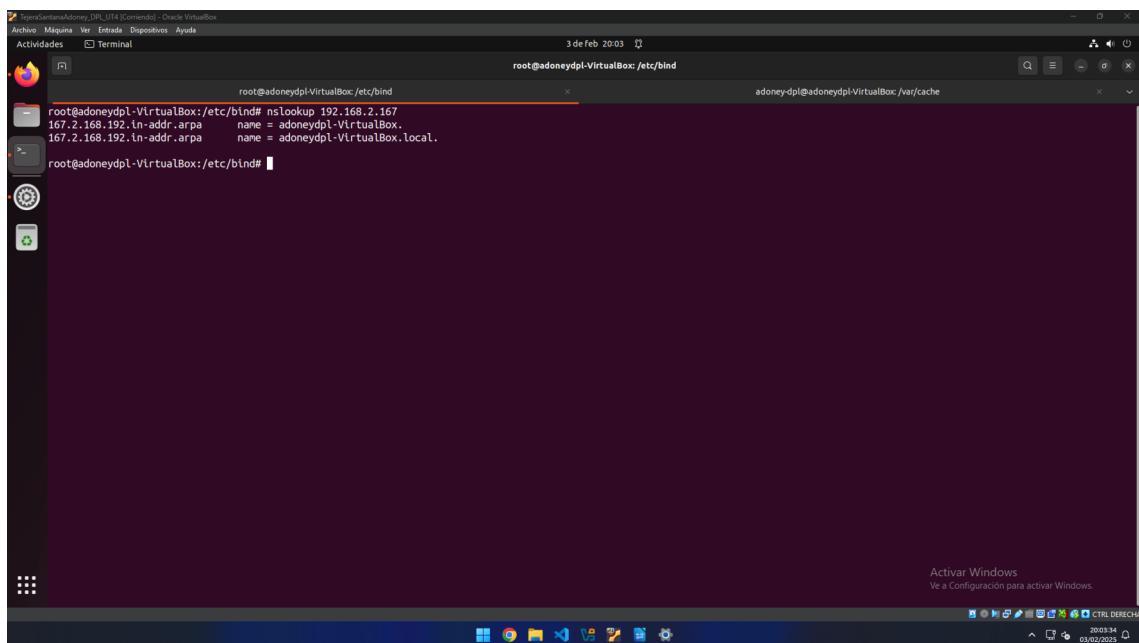
zone "255.in-addr.arpa" {
    type master;
    file "/etc/blnd/db.255";
};

zone "adoneytejera.net" IN {
    type master;
    file "/etc/blnd/db.adoneytejera.net";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    file "/etc/blnd/1.168.192.net";
};

named.conf.default-zones 38L, 664B
```

Se añade el fichero con el dns invertido.



```
root@adoneydpl-VirtualBox:/etc/bind
root@adoneydpl-VirtualBox:/etc/bind# nslookup 192.168.2.167
167.2.168.192.in-addr.arpa      name = adoneydpl-VirtualBox.
167.2.168.192.in-addr.arpa      name = adoneydpl-VirtualBox.local.
root@adoneydpl-VirtualBox:/etc/bind#
```

Y se comprueba el dns inverso.

2 Herramientas empleadas

Hechos hecho uso de bind9 para DNS, ldap para la autenticación y apache para el servidor.

3 Problemática encontrada y solución

No consigo hacer que en el dns, la ruta ldap.adoneytejera.net me lleve automáticamente a phpldapadmin

4 Conclusiones