



“Si te gustan *-Los Usuarios y Grupos-* Te gustará también *-OpenLDAP-*”

Objetivo:

→ **Conexión a un Servidor Central LDAP/Kerberos** → **server1.example.com**

↘ **Parámetros de conexión:**

- **LDAP Server:** **server1.example.com**
- **LDAP base DN:** **dc=example,dc=com**
- **Usar TLS:** **SI.**
- **RootCA:** **server1.example.com**
- **Kerberos REALM:** **EXAMPLE.COM**
- **Kerberos KDC:** **server1.example.com**
- **Kerberos admin server:** **server1.example.com**
- **Comprobar existencia de usuarios** → **ldapuser{1..3}**
- **Establecer una conexión ssh con el usuario** → **ldapuser1 ; password** → **password123**
- **Establecer una conexión ssh con el usuario** → **admin ; password** → **password123**, y crear un nuevo usuario → **ldapuser4 ; password** → **password123**

+++++
 (Tiempo máximo estimado → 15 minutos)...
 +++++

↘ **home**

[root@station1 ~]# yum install krb5-workstation authconfig pam_krb5 sssd

[root@station1 ~]# authconfig --help |grep home

--winbindtemplatehomedir=</home/%D/%U>

--enablemkhomedir crear el directorio principal de usuarios en su primer inicio de sesión

--disablemkhomedir no crear directorios principales de usuarios en el primer inicio de sesión

[root@station1 ~]# authconfig --enablemkhomedir --update

↘ **krb5**

[root@station1 ~]# authconfig --help |grep krb5

--enablekrb5 habilitar la autenticación con Kerberos por defecto

--disablekrb5 inhabilitar la autenticación con Kerberos por defecto

--krb5kdc=<servidor> KDC predeterminado de Kerberos

--krb5adminserver=<servidor>

--krb5realm=<entorno>

--enablekrb5kdcdns habilitar el uso de DNS para hallar los KDC de Kerberos

--disablekrb5kdcdns inhabilitar el uso del DNS para hallar los KDC de Kerberos

--enablekrb5realmdns habilitar el uso del DNS para hallar los entornos de Kerberos

--disablekrb5realmdns

--enablewinbindkrb5 Winbind usará Kerberos 5 para autenticación

--disablewinbindkrb5 Winbind usará el método de autenticación predeterminado

[root@station1 ~]# authconfig --enablekrb5 --krb5kdc=server1.example.com

--krb5adminserver=server1.example.com --krb5adminserver=EXAMPLE.COM --update

↘ pam

```
[root@station1 ~]# authconfig --help |grep pam
```

```
--enablepamaccess    chequear access.conf durante la autorización de cuenta  
--disablepamaccess  no chequear access.conf durante la autorización de cuenta  
the pam_faillock module options
```

```
[root@station1 ~]# authconfig --enablepamaccess --update
```

↘ ssd

```
[root@station1 ~]# authconfig --help |grep sssd
```

```
--enablesssd        habilitar por defecto SSSD para la información del usuario con el manejo  
manual de la configuración  
--disablesssd       inhabilitar por defecto SSSD para la información de usuario (todavía  
utilizado para configuraciones soportadas)  
--enablesssdauth    habilitar por defecto SSSD para la autenticación con el manejo manual de la  
configuración  
--disablesssdauth   inhabilita SSSD para la autenticación por defecto (todavía se usa para las  
configuraciones soportadas)
```

```
[root@station1 ~]# authconfig --enablesssd --enablesssdauth --update
```

↘ ldap

```
[root@station1 ~]# authconfig --help |grep ldap
```

```
--enableldap        habilitar por defecto LDAP para la información del usuario  
--disableldap       inhabilitar por defecto LDAP para la información del usuario  
--enableldapauth    habilitar por defecto LDAP para la autenticación  
--disableldapauth   inhabilitar por defecto LDAP para la autenticación  
--ldapserv=<servidor>  
--ldapbasedn=<dn>   DN de base LDAP por defecto  
--enableldaptls, --enableldapstarttls  
--disableldaptls, --disableldapstarttls  
--ldaploadcacert=<URL>
```

```
[root@station1 ~]# authconfig --enableldap --enableldapauth  
--ldapserv=server1.example.com --ldapbasedn="dc=example,dc=com" --enableldaptls  
--update
```

```
authconfig: Authentication module /usr/lib64/security/pam_ldap.so is missing. Authentication  
process might not work correctly.
```

```
[root@station1 ~]# yum provides */pam_ldap.so
```

...

```
nss-pam-ldapd-0.8.13-8.el7.i686 : An nsswitch module which uses directory servers
```

```
Repositorio      : base
```

```
Resultado obtenido desde:
```



Nombre del archivo : /usr/lib/security/pam_ldap.so

...

```
[root@station1 ~]# yum install nss-pam-ldapd
[root@station1 ~]# authconfig --enableldap --enableldapauth
--ldapserver=server1.example.com --ldapbasedn="dc=example,dc=com" --enableldaptls
--update
```

```
[root@station1 ~]# systemctl enable sssd
[root@station1 ~]# systemctl start sssd
[root@station1 ~]# systemctl status sssd
```

↘ Comprobación de usuarios y conexión ssh.

```
[root@station1 conf.d]# getent passwd ldapuser{1..3}
ldapuser1:*:789200001:789200001:ldapuser1 ldapuser1:/home/ldapuser1:/bin/bash
ldapuser2:*:789200003:789200003:ldapuser2 ldapuser2:/home/ldapuser2:/bin/bash
ldapuser3:*:789200004:789200004:ldapuser3 ldapuser3:/home/ldapuser3:/bin/bash
```

```
[root@station1 ~]# ssh ldapuser1@server1
```

Password:

Creating home directory for ldapuser1.

```
[ldapuser1@server1 ~]$ pwd
```

```
/home/ldapuser1
```

```
[root@station1 ~]# ssh admin@server1
```

Password:

```
[admin@server1 ~]$ ipa user-add ldapuser4 --first=ldapuser4 --last=ldapuser4 --password
```

Contraseña:

Ingrese Contraseña nuevamente para verificar:

```
-----
Ha sido agregado el usuario "ldapuser4"
-----
```

Ingreso de usuario: ldapuser4

Nombre: ldapuser4

Apellido: ldapuser4

Nombre y apellidos: ldapuser4 ldapuser4

Mostrar nombre: ldapuser4 ldapuser4

Iniciales: ll

Directorio principal: /home/ldapuser4

GECOS: ldapuser4 ldapuser4

Shell de ingreso: /bin/bash

Nombre principal: ldapuser4@EXAMPLE.COM

Principal alias: ldapuser4@EXAMPLE.COM

Dirección de correo electrónico: ldapuser4@example.com

UID: 789200005

GID: 789200005



Contraseña: True
Miembros de los grupos: ipausers
Claves Kerberos disponibles: True

[root@station1 ~]# getent passwd ldapuser{1..4}

```
ldapuser1*:789200001:789200001:ldapuser1 ldapuser1:/home/ldapuser1:/bin/bash
ldapuser2*:789200003:789200003:ldapuser2 ldapuser2:/home/ldapuser2:/bin/bash
ldapuser3*:789200004:789200004:ldapuser3 ldapuser3:/home/ldapuser3:/bin/bash
ldapuser4*:789200005:789200005:ldapuser4 ldapuser4:/home/ldapuser4:/bin/bash
```

Creative Commons

Reconocimiento-NoComercial-CompartirIgual 3.1 ESPAÑA

© 2018 by carlos briso. Usted es libre de copiar, distribuir y comunicar públicamente la obra y hacer obras derivadas bajo las condiciones siguientes:

a) Debe reconocer y citar al autor original.

b) No puede utilizar esta obra para fines comerciales (incluyendo su publicación, a través de cualquier medio, por entidades con fines de lucro).

c) Si altera o transforma esta obra o genera una obra derivada, sólo puede distribuir la obra generada bajo una licencia idéntica a ésta. Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso del titular de los derechos de autor. Los derechos derivados de usos legítimos u otras limitaciones no se ven afectados por lo anterior. Licencia completa en castellano.

→ La información contenida en este documento y los derivados de éste se proporcionan tal cual son y los autores no asumirán responsabilidad alguna si el usuario o lector hace mal uso de éstos.