

Autoryzacja 1

written by archi | 16 października 2019



Uruchamiamy integrację systemu operacyjnego z LDAP. W tym celu musimy zainstalować kilka dodatków rozszerzających możliwości systemu operacyjnego:

- „libnss-ldap„

2. W trakcie instalacji system poprosi o podanie danych pozwalających na przyłączenie się do LDAP (**podaj wyłącznie w tej linii !!!!! : 127.0.0.1**):

Package configuration

Configuring ldap-auth-config

Please enter the URI of the LDAP server to use. This is a string in the form of ldap://<hostname or IP>:<port>. ldaps:// or ldapi:// can also be used. The port number is optional.

Note: It is usually a good idea to use an IP address because it reduces risks of failure in the event name service problems.

LDAP server Uniform Resource Identifier:

127.0.0.1

<Ok>

UWAGA! : zmieniona domena LDAP na: **dc=lab,dc=pl**

Package configuration

Configuring ldap-auth-config

Please enter the distinguished name of the LDAP search base. Many sites use the components of their domain names for this purpose. For example, the domain "example.net" would use "dc=example,dc=net" as the distinguished name of the search base.

Distinguished name of the search base:

dc=lab,dc=pl

<Ok>

LDAP version: 3

Package configuration

Configuring ldap-auth-config

Please enter which version of the LDAP protocol should be used by ldapns. It is usually a good idea to set this to the highest available version.

LDAP version to use:

3
2

<Ok>

Ustawiamy konto root jako admina LDAP

Package configuration

Configuring ldap-auth-config

This option will allow you to make password utilities that use pam to behave like you would be changing local passwords.

The password will be stored in a separate file which will be made readable to root only.

If you are using NFS mounted /etc or any other custom setup, you should disable this.

Make local root Database admin:

<Yes>

<No>

Włączamy wymaganie logowania do dostępu do bazy LDAP

Package configuration

Configuring ldap-auth-config

Choose this option if you are required to login to the database to retrieve entries.

Note: Under a normal setup, this is not needed.

Does the LDAP database require login?

<Yes>

<No>

LDAP account for root: cn=admin,dc=lab,dc=pl

Package configuration

Configuring ldap-auth-config

This account will be used when root changes a password.

Note: This account has to be a privileged account.

LDAP account for root:

<Ok>

Podać właściwe hasło dla użytkownika ADMIN (podane w poprzednim laboratorium)

Package configuration

Configuring ldap-auth-config

Please enter the password to use when ldap-auth-config tries to login to the LDAP directory using the LDAP account for root.

The password will be stored in a separate file /etc/ldap.secret which will be made readable to root only.

Entering an empty password will re-use the old password.

LDAP root account password:

<OK>

Wskazać jako użytkownika uprzywilejowanego na: cn=admin,dc=lab,dc=pl

Package configuration

Configuring ldap-auth-config

Please enter the name of the account that will be used to log in to the LDAP database.

Warning: DO NOT use privileged accounts for logging in, the configuration file has to be world readable.

Unprivileged database user:

`cn=admin,dc=lab,dc=pl`

<Ok>

Podać właściwe hasło (jak było wcześniej)

Package configuration

Configuring ldap-auth-config

Please enter the password that will be used to log in to the LDAP database.

Password for database login account:

<Ok>

3. Zmieniamy ustawienia w pliku „/etc/ldap.conf„

- Przesławiamy SCOPE na „SUB”

```
#uri ldaps://127.0.0.1/...
#uri ldapi://%2fvar%2frun%2fldapi_sock/
# Note: %2f encodes the '/' used as directory separator

# The LDAP version to use (defaults to 3
# if supported by client library)
ldap_version 3

# The distinguished name to bind to the server with.
# Optional: default is to bind anonymously.
binddn cn=admin,dc=lab,dc=pl

# The credentials to bind with..
# Optional: default is no credential.
bindpw user

# The distinguished name to bind to the server with
# if the effective user ID is root. Password is
# stored in /etc/ldap.secret (mode 600)
rootbinddn cn=admin,dc=lab,dc=pl

# The port.
# Optional: default is 389.
#port 389

# The search scope.
scope sub
#scope one
#scope base

# Search timelimit
#timelimit 30
```

- Włączamy obsługę przesyłania jawnych haseł

```

#nss_map_attribute shadowLastChange pwdLastSet
#nss_map_objectclass posixGroup group
#nss_map_attribute uniqueMember member
#pam_login_attribute sAMAccountName
#pam_filter objectclass=User
#pam_password ad

# configure --enable-authpassword is no longer supported
# AuthPassword mappings
#nss_map_attribute userPassword authPassword

# AIX SecureWay mappings
#nss_map_objectclass posixAccount aixAccount
#nss_base_passwd ou=aixaccount,?one
#nss_map_attribute uid userName
#nss_map_attribute gidNumber gid
#nss_map_attribute uidNumber uid
#nss_map_attribute userPassword passwordChar
#nss_map_objectclass posixGroup aixAccessGroup
#nss_base_group ou=aixgroup,?one
#nss_map_attribute cn groupName
#nss_map_attribute uniqueMember member
#pam_login_attribute userName
#pam_filter objectclass=aixAccount
pam_password clear

# Netscape SDK LDAPS
#ssl on

# Netscape SDK SSL options
#sslpath /etc/ssl/certs

```

- Zapisujemy modyfikacje w pliku...

4. Dopisujemy obsługę LDAP do „/etc/nsswitch.conf„

- Dopisujemy wykorzystanie bazy LDAP

```
mc [root@linux]:/etc
/etc/nsswitch.conf 530/530 100%
# /etc/nsswitch.conf
#
# Example configuration of GNU Name Service Switch functionality.
# If you have the `glibc-doc-reference' and `info' packages installed, try:
# `info libc "Name Service Switch"' for information about this file.

passwd:      files systemd ldap
group:       files systemd ldap
shadow:     files ldap
gshadow:    files ldap

hosts:      files dns
networks:   files

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

netgroup:   nis

1Help 2UnWrap 3Quit 4Hex 5Goto 6 7Search 8Raw 9Format 10Quit
```

- Zapisujemy modyfikacje...

5. Jeżeli wykonaliśmy wszystko poprawnie powinni być widoczni użytkownicy z bazy LDAP. Można to sprawdzić przy pomocy polecenia „id” ze wskazaniem nazwy użytkownika np.:

```
id user1
```

W wyniku otrzymamy informacje o użytkowniku user1 (jego UID i GID)

```
uid=10000(user1) gid=100(users) grupy=100(users)

root@linux:~# id user1
uid=10000(user1) gid=100(users) groups=100(users)
root@linux:~#
```