nurit

BaroPAM solution installation summary

for multi-layer authentication to strengthen the security of information assets (OpenLDAP)

May, 2026

Ⅱ. Install BaroPAM OpenLDAP

1. Install OpenLDAP

1) Since openldap-servers does not exist in the default repository, add it to the repository

```
[root]# dnf config-manager --set-enabled plus
[root]# dnf repolist
저장소 ID                                    저장소 이름
appstream                                    Rocky Linux 9 - AppStream
baseos                                       Rocky Linux 9 - BaseOS
extras                                       Rocky Linux 9 - Extras
plus                                         Rocky Linux 9 - Plus
```

2) First, BaroPAM must be installed.
   Refer to the BaroPAM installation guide (Linux)

3) Install OpenLDAP and SASL related packages (written based on Redhat-based systems)

```
[root]# dnf -y install openldap-servers openldap-clients cyrus-sasl cyrus-sasl-plain
```

When trying to remove the installed OpenLDAP → dnf -y erase openldap-servers openldap-clients cyrus-sasl cyrus-sasl-plain

2. OpenLDAP settings

1) Create and run the OpenLDAP service (slapd) for automatic startup

```
[root]# systemctl enable --now slapd
Created symlink /etc/systemd/system/slapd.service → /usr/lib/systemd/system/slapd.service.
Created symlink /etc/systemd/system/multi-user.target.wants/slapd.service → /usr/lib/systemd/system/slapd.service.

[root]# systemctl start slapd
```

2) Configure the OpenLDAP(slapd) daemon to restart automatically when a problem occurs

```
[root]# vi /usr/lib/systemd/system/slapd.service
[Unit]
Description=OpenLDAP Server Daemon
After=syslog.target network-online.target
Documentation=man:slapd
Documentation=man:slapd-config
Documentation=man:slapd-mdb
Documentation=file:///usr/share/doc/openldap-servers/guide.html

[Service]
Type=forking
ExecStartPre=/usr/libexec/openldap/check-config.sh
ExecStart=/usr/sbin/slapd -u ldap -h "ldap:/// ldaps:/// ldapi:///"

Restart=on-failure
RestartSec=5s
StartLimitIntervalSec=600
StartLimitBurst=5

[Install]
WantedBy=multi-user.target
Alias=openldap.service
```

3) Restart slapd daemon

```
[root]# systemctl daemon-reload
[root]# systemctl restart slapd.service
```

4) OpenLDAP 데몬 실행

```
[root]# systemctl restart slapd →Service restart
[root]# systemctl start   slapd →Service start
[root]# systemctl stop    slapd →Service stop
[root]# systemctl status  slapd →Service status
```

5) Checking authentication logs from BaroPAM by integrating with OpenLDAP

```
[root]# tail -f /var/log/secure
```

참고) OpenLADP related log files: /var/log/radius/messages

3. Firewall settings

```
1) Install firewalld
[root]# dnf -y install firewalld

2) Enable firewalld
[root]# systemctl enable firewalld
[root]# systemctl start  firewalld

3) Allow port
[root]# firewall-cmd --permanent --add-service={ldap,ldaps}
success

4) Reload firewall
[root]# firewall-cmd --reload
success

5) Check if it works
[root]# systemctl status firewalld
* firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
   Active: active (running) since Tue 2024-01-09 20:35:10 KST; 14h ago
     Docs: man:firewalld(1)
 Main PID: 1009 (firewalld)
    Tasks: 2 (limit: 102061)
   Memory: 42.5M
   CGroup: /system.slice/firewalld.service
           `-1009 /usr/libexec/platform-python -s /usr/sbin/firewalld --nofork --nopid

Jan 09 20:35:09 vpntest systemd[1]: Starting firewalld - dynamic firewall daemon...
Jan 09 20:35:10 vpntest systemd[1]: Started firewalld - dynamic firewall daemon.
```

4. Set administrator password

Base Dn : cn=admin,dc=example,dc=com, Manageable using the administrator password

1) Create password

```
[root]# slappasswd
New password: baropam
Re-enter new password: baropam
{SSHA}052QoM5oM14WYbi3WkzcMPLQ27fFsxFt <-Copy needed
```

2) Create password DN

```
[root]# vi admin_pass.ldif
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}052QoM5oM14WYbi3WkzcMPLQ27fFsxFt <-Paste the copied password
```

3) Apply password DN

```
[root]# ldapadd -Y EXTERNAL -H ldapi:/// -f admin_pass.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}mdb,cn=config"
```

5. Set the default DN

1) Create base DN

```
[root]# vi base_structure.ldif
# base_structure.ldif
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcSuffix
olcSuffix: dc=example,dc=com

dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootDN
olcRootDN: cn=admin,dc=example,dc=com
```

2) Apply default DN

```
[root]# ldapadd -Y EXTERNAL -H ldapi:/// -f base_structure.ldif
SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
modifying entry "olcDatabase={2}mdb,cn=config"

modifying entry "olcDatabase={2}mdb,cn=config"
```

6. Load default schema

```
[root]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=cosine,cn=schema,cn=config"

[root]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=nis,cn=schema,cn=config"

[root]# ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/inetorgperson.ldif

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0
adding new entry "cn=inetorgperson,cn=schema,cn=config"
```

7. Default organization settings

1) Create Basic Organization DN

```
[root@baropam ~]# vi initial_org.ldif
# Definition of the organization's root DIT (Directory Information Tree) entry
# dc=example,dc=com must be changed to match the default domain set during installation.
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: My Company
description: My Company's main LDAP directory

# Definition of Organizational Units (OU) for users
dn: ou=users,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: users
description: All user accounts in My Company

# Definition of Organizational Units (OU) for groups
dn: ou=groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: groups
description: All user groups in My Company

# Definition of Organizational Units (OU) for departments
dn: ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: departments
description: Departments within My Company

# IT department OU definition (Located under department OU)
dn: ou=IT,ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: IT
description: Information Technology Department

# HR department OU definition (Located under department OU)
dn: ou=HR,ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: HR
description: Human Resources Department
```

2) Apply basic organization DN

```
[root]# ldapadd -x -W -D "cn=admin,dc=example,dc=com" -f initial_org.ldif
Enter LDAP Password: baropam
adding new entry "dc=example,dc=com"
adding new entry "ou=users,dc=example,dc=com"
adding new entry "ou=groups,dc=example,dc=com"
adding new entry "ou=departments,dc=example,dc=com"
adding new entry "ou=IT,ou=departments,dc=example,dc=com"
adding new entry "ou=HR,ou=departments,dc=example,dc=com"
```

8. Testing

```
1) baropam user DN creation
[root]# vi add_nurit.ldif
dn: uid=honggildong,ou=HR,ou=departments,dc=example,dc=com
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: nurit
sn: nuri
givenName: it
mail: nurit@example.com
uid: nurit
userPassword: {SSHA}052QoM5oM14WYbi3WkzcMPLQ27fFsxFt

2) Apply baropam user DN
[root]# ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f add_nurit.ldif
Enter LDAP Password: baropam
adding new entry "uid=honggildong,ou=HR,ou=departments,dc=example,dc=com"

3) Look up personnel belonging to the HR department
[root@baropam ~]# ldapsearch -x -b  "ou=HR,ou=departments,dc=example,dc=com" "(objectClass=person)" cn
.....
# honggildong, HR, departments, example.com
dn: uid=honggildong,ou=HR,ou=departments,dc=example,dc=com
cn: nurit

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

9. BaroPAM Environment Settings

```
1) PAM authentication: Set environment setting information in File
[root]# vi /etc/pam.d/ldap
auth     required  pam_env.so
auth     required  /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no
account  required  pam_unix.so

[root]# vi /etc/pam.d/saslauthd
auth     required  /usr/baropam/pam_baro_auth.so forward_pass secret=/usr/baropam/.baro_auth encrypt=no
auth     substack  password-auth
account  include   password-auth

2) PAM authentication: Set environment configuration information in MariaDB
[root]# vi /etc/pam.d/ldap
auth     required  pam_env.so
auth     required  /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql encrypt=no auth=openldap
account  required  pam_unix.so

[root]# vi /etc/pam.d/saslauthd
auth     required  /usr/baropam/pam_baro_sql.so forward_pass secret=/usr/baropam/.baro_sql encrypt=no auth=openldap
auth     substack  password-auth
account  include   password-auth

3) cURL authentication
[root]# vi /etc/pam.d/ldap
auth     required  pam_env.so
auth     required  /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no
account  required  pam_unix.so

[root]# vi /etc/pam.d/saslauthd
auth     required  /usr/baropam/pam_baro_curl.so forward_pass secret=/usr/baropam/.baro_curl encrypt=no
auth     substack  password-auth
account  include   password-auth
```

10. OpenLDAP Integration Environment Setup

1) saslauthd configuration (relay role)

Configure saslauthd to look at the Rocky Linux system's PAM instead of the internal DB.

```
[root]# vi /etc/sysconfig/saslauthd
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=

[root]# systemctl enable saslauthd
Created symlink /etc/systemd/system/multi-user.target.wants/saslauthd.service → /usr/lib/systemd/system/saslauthd.service.

[root]# vi /usr/lib/systemd/system/saslauthd.service
.........
Restart=on-failure
RestartSec=5s
StartLimitIntervalSec=600
StartLimitBurst=5

[Install]
WantedBy=multi-user.target

[root@baropam ~]# systemctl daemon-reload
[root@baropam ~]# systemctl restart saslauthd.service
```

2) OpenLDAP (slapd) Configuration (Bypass/Proxy)

Configure OpenLDAP to forward requests to SASL instead of handling them directly.

```
[root]# vi /etc/sasl2/slapd.conf
pwcheck_method: saslauthd
mech_list: plain login

[root]# systemctl restart slapd
```

11. Create user account

1) Create a Linux user account

```
[root]# useradd baropam
[root]# passwd baropam
Changing password for user raduser.
New password: baropam
Retype new password: baropam
passwd: all authentication tokens updated successfully.
```

2) Create OpenLDAP User Account

Create baropam user DN)

To ensure that OpenLDAP user passwords are authenticated by the system instead of being stored (delegating authentication to saslauthd), the userPassword property must use the format {SASL}username.

```
[root]# vi add_baropam.ldif
dn: uid=baropam,ou=HR,ou=departments,dc=example,dc=com
objectClass: top
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
sn: baropam
cn: baropam
uid: baropam
uidNumber: 1000
gidNumber: 1000
homeDirectory: /home/baropam
loginShell: /bin/bash
gecos: BaroPAM User
userPassword: {SASL}baropam
shadowLastChange: 0
shadowMax: 99999
shadowWarning: 7
```

11. Create user account

Apply baropam user DN)

```
[root]# ldapadd -x -D "cn=admin,dc=example,dc=com" -W -f add_baropam.ldif
Enter LDAP Password: baropam
adding new entry "uid=baropam,ou=HR,ou=departments,dc=example,dc=com"
```

Look up personnel belonging to the HR department)

```
[root]# ldapsearch -x -b  "ou=HR,ou=departments,dc=example,dc=com" "(objectClass=person)" cn
# extended LDIF
#
# LDAPv3
# base <ou=HR,ou=departments,dc=example,dc=com> with scope subtree
# filter: (objectClass=person)
# requesting: cn
#

# honggildong, HR, departments, example.com
dn: uid=honggildong,ou=HR,ou=departments,dc=example,dc=com
cn: nurit

# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

12. Integration test

1) Verify integration within the server (saslauthd <-> BaroPAM)

Before using the OpenLDAP client, verify it first with testsaslauthd. Since testsaslauthd assumes the service name is an imap by default and requests authentication from PAM, you must create a symbolic link.

```
[root]# ln -s /etc/pam.d/saslauthd /etc/pam.d/imap

[root]# testsaslauthd -u baropam -p baropam935018 <- baropam935018 = Password(baropam) + One-Time authentication key(935018)
0: OK "Success."
```

On success: 0: Prints OK "Success."
On failure: 0: Prints NO "authentication failed"

Note)

```
$  systemctl start   saslauthd ->Service start
$  systemctl stop    saslauthd ->Service stop
$  systemctl restart saslauthd ->Service restart
$  systemctl status  saslauthd ->Service status
```

2) Remote test from User (PC) (PC <-> OpenLDAP <-> saslauthd <-> BaroPAM)

Attempt SASL authentication on a PC using tools such as ldapwhoami.

```
[root]# ldapwhoami -h localhost -D "uid=baropam,ou=HR,ou=departments,dc=example,dc=com" -x -w "baropam566419"
dn:uid=baropam,ou=HR,ou=departments,dc=example,dc=com
```

On success: Prints dn: baropam,ou=HR,ou=departments,dc=example,dc=com
On failure: Invalid credentials (49) error occurred.

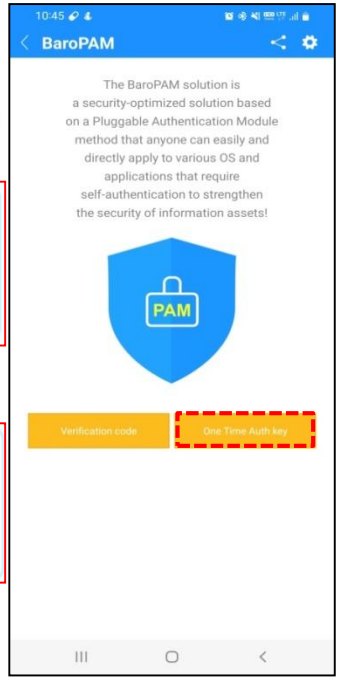
Note) If an error occurs, check the /var/log/messages and /var/log/secure logs to take action.

13. Install the BaroPAM app and set up information

BaroPAM App Download

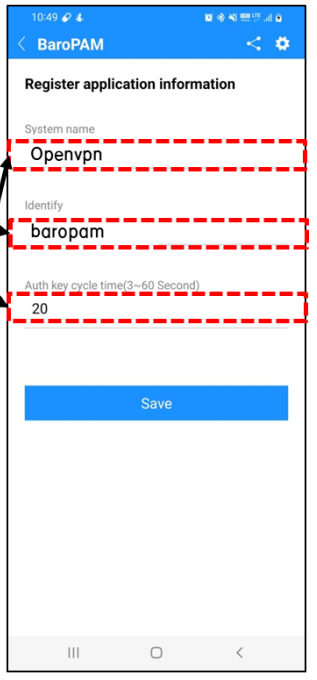
Google Play

App Store



Login-ID: baropam, phone number: 010-2771-4076

```
$ cat .baropam_auth
" AUTH_KEY
" RATE_LIMIT 3 30
" KEY_METHOD app512
" CYCLE_TIME 20
" SECURE_KEY 01027714076
" ACL_NAME /usr/baropam/.baro_acl
" ACL_TYPE deny
" HOSTNAME OpenVPN
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```



BaroPAM app can be used on Android 6.0 (Marshmalliw) API 23, iOS 13.0 or higher, and does not support landscape mode. After installing the **BaroPAM** app, After installing the **BaroPAM** app, run the **BaroPAM** app, click the "One Time Auth key" button on the menu selection screen, and enter the "Cycle time, ID, and system name" set in the RADIUS user information in the "Register application information" screen of the **BaroPAM** app. You must enter the same information. If you set the app code (kr: Korean, en: English, jp: Japanese, cn: Chinese) on the **BaroPAM** app settings -> change screen settings screen, the **BaroPAM** app changes accordingly.

Message: The "OTA key" is incorrect because the date and time of the Android phone or iPhone are different from the current time.
Cause: This is caused by not using the time provided by the network for the Android or iPhone's date and time.
Action: For Android phones, go to "Settings" -> "General management" -> "Date and time" -> "Automatic date and time" and "Automatic time zone" -> "Allow" For iPhone, go to "Settings" -> "Date & Time" -> "Set Automatically" -> "Allow"

Message: If you cannot log in because the OTA key does not match.
Cause: BaroPAM is a time synchronization method, so the time of the phone and Server must be the same.
Action: Check if the phone and Servers time are correct.

14. User connection

Enter the OpenLDAP user account(Username), the password is "baropam", and the password created in the BaroPAM app on your smartphone.
If the One-Time Authentication key is "613045", enter "baropam613045" in the "Password:" field and click the "OK" button to use BaroPAM.
If authentication is successful by requesting authentication from the module, the connection is established.

nurit

nurit

Password you don't need to remember!
BaroPAM will be with you.

Thank You!

www.nurit.co.kr
mc529@nurit.co.kr