nurit

정보자산의 보안강화를 위하여 다계층 인증을 위한

BaroPAM 솔루션 설치 요약서 (OpenLDAP)

2026. 5.

1. OpenLDAP 설치

1) 기본 레파지토리에는 openldap-servers가 존재하지 않으므로 레피지토리에 추가

```
[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) 먼저, BaroPAM 설치 설치되어 있어야 함.
   BaroPAM 설치 가이드(Linux) 참조

3) OpenLDAP와 SASL 관련 패키지를 설치(Redhat 계열을 기준으로 작성됨)

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

설치된 OpenLDAP를 제거 할려고 할 때 → dnf -y erase openldap-servers openldap-clients cyrus-sasl cyrus-sasl-plain

2. OpenLDAP 설정

1) 자동 시작을 위한 OpenLDAP 서비스(slapd)를 생성 및 실행

```
[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) OpenLDAP(slapd) 데몬에 문제가 생겼을 때 자동으로 재시작하도록 설정

```
[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) slapd 데몬 재시작

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

4) OpenLDAP 데몬 실행

```
[root]# systemctl restart slapd → 데몬 재실행
[root]# systemctl start   slapd → 데몬 실행
[root]# systemctl stop    slapd → 데몬 종료
[root]# systemctl status  slapd → 데몬 상태
```

5) OpenLDAP을 연동하여 BaroPAM에서 인증한 로그 확인

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

참고) OpenLADP 관련 로그 파일: /var/log/radius/messages

3. 방화벽 설정

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

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

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

4) 방화벽 재로드
[root]# firewall-cmd --reload
success

5) 작동여부 확인
[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. 관리자 비밀번호 설정

Base Dn : cn=admin,dc=example,dc=com, 관리자 비밀번호를 사용하여 관리 가능

1) 비밀번호 생성

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

2) 비밀번호 DN 생성

```
[root]# vi admin_pass.ldif
dn: olcDatabase={2}mdb,cn=config
changetype: modify
replace: olcRootPW
olcRootPW: {SSHA}052QoM5oM14WYbi3WkzcMPLQ27fFsxFt <-복사한 비밀번호 붙여 넣기
```

3) 비밀번호 DN 적용

```
[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. 기본 DN을 설정

1) 기본 DN 생성

```
[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) 기본 DN 적용

```
[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. 기본 스키마 로드

```
[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. 기본 조직 설정

1) 기본 조직 DN 생성

```
[root@baropam ~]# vi initial_org.ldif
# 조직의 루트 DIT(Directory Information Tree) 항목 정의
# dc=example,dc=com은 설치 시 설정한 기본 도메인에 맞춰 변경해야 합니다.
dn: dc=example,dc=com
objectClass: top
objectClass: dcObject
objectClass: organization
o: My Company
description: My Company's main LDAP directory

# 사용자들을 위한 조직 구성 단위(OU) 정의
dn: ou=users,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: users
description: All user accounts in My Company

# 그룹들을 위한 조직 구성 단위(OU) 정의
dn: ou=groups,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: groups
description: All user groups in My Company

# 부서들을 위한 조직 구성 단위(OU) 정의
dn: ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: departments
description: Departments within My Company

# IT 부서 OU 정의 (부서 OU 아래에 위치)
dn: ou=IT,ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: IT
description: Information Technology Department

# HR 부서 OU 정의 (부서 OU 아래에 위치)
dn: ou=HR,ou=departments,dc=example,dc=com
objectClass: top
objectClass: organizationalUnit
ou: HR
description: Human Resources Department
```

2) 기본 조직 DN 적용

```
[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. 테스트

1) baropam 사용자 DN 생성

```
[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) baropam 사용자 DN 적용

```
[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) HR부서에 속한 인원을 조회

```
[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 환경 설정

```
1) PAM 인증: 환경 설정 정보를 File에 설정
[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 인증: 환경 설정 정보를 MariaDB에 설정
[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 인증
[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 연동 환경 설정

1) saslauthd 설정 (중계역할)

saslauthd가 내부 DB가 아닌 Rocky Linux 시스템의 PAM을 바라보게 설정.

```
[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) 설정 (Bypass/Proxy)

OpenLDAP이 요청을 받으면 직접 처리하지 않고 SASL로 던지도록 설정.

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

[root]# systemctl restart slapd
```

11. 사용자 계정 생성

1) Linux 사용자 계정 생성

```
[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) OpenLDAP 사용자 계정 생성

baropam 사용자 DN 생성)

OpenLDAP 사용자의 비밀번호가 저장되는 대신 시스템 인증을 타도록(인증을 saslauthd에게 위임) userPassword 속성에 {SASL}username 형식을 사용해야 함.

```
[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. 사용자 계정 생성

```
baropam 사용자 DN 적용)

[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"

HR부서에 속한 인원을 조회)

[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. 연동 테스트

1) 서버 내부에서 연동 확인 (saslauthd <-> BaroPAM)

OpenLDAP 클라이언트를 쓰기 전에 testsaslauthd로 먼저 검증한다. testsaslauthd는 기본적으로 서비스 이름을 imap으로 가정하고 PAM에 인증을 요청하기 때문에 반드시 심볼릭 링크을 생성해야 한다.

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

[root]# testsaslauthd -u baropam -p baropam935018 <- baropam935018 = 비밀번호(baropam) + 일회용 인증키(935018)
0: OK "Success."
```

성공 시: 0: OK "Success." 출력.
실패 시: 0: NO "authentication failed" 출력.

참고)

```
$  systemctl start   saslauthd ->서비스 시작
$  systemctl stop    saslauthd ->서비스 종료
$  systemctl restart saslauthd ->서비스 재시작
$  systemctl status  saslauthd ->서비스 상태
```

2) User(PC)에서 원격 테스트 (PC <-> OpenLDAP <-> saslauthd <-> BaroPAM)

PC에서 ldapwhoami 등의 도구를 사용하여 SASL 인증을 시도한다.

```
[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
```

성공 시: dn: baropam,ou=HR,ou=departments,dc=example,dc=com 출력.
실패 시: Invalid credentials (49) 에러 발생.

참고) 오류 발생 시 /var/log/messages, /var/log/secure 로그를 확인하여 조치를 해야 한다.

13. BaroPAM 앱 설치 및 정보 설정

BaroPAM 앱 다운로드

Google Play

App Store

로그인-ID: nurit, 폰번호: 010-2771-4076인 경우

```
$ cat .nurit_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 BaroPAM
" DISALLOW_REUSE
33458936
19035576
15364353
54649370
84342192
```

BaroPAM 앱은 Android 6.0 (Marshmalliw) API 23, iOS 13.0 이상에서 사용 가능하며, 가로보기 모드를 지원하지 않는다.
BaroPAM 앱을 설치한 후 BaroPAM 앱을 실행하여 메뉴 선택화면에서 "일회용 인증키" 버튼을 클릭하여 RADIUS 사용자 정보에 설정한 "**인증주기, 아이디, 시스템명**"을 BaroPAM 앱의 "**애플리케이션 정보 등록**" 화면에서 동일하게 입력해야 한다.
BaroPAM 앱의 설정 -> 화면설정 변경 화면에서 앱코드(kr: 한국어, en: 영어, jp: 일본어, cn: 중국어)를 설정하면 BaroPAM 앱이 그에 맞게 변경된다.

현상 : 안드로이폰 또는 아이폰의 날짜와 시간이 현재 시간과 차이가 발생하여 "일회용 인증키"가 맞지 않은 경우
원인 : 안드로이폰 또는 아이폰의 날짜와 시간을 네트워크에서 제공하는 시간을 사용하지 않아서 발생.
조치 : 안드로이폰인 경우는 폰의 "설정" -> "일반" -> "날짜 및 시간" -> "날짜 및 자동 설정"과 "시간대 자동 설정" -> "허용"
아이폰인 경우는 폰의 "설정" -> "날짜 및 시간" -> "자동으로 설정" -> "허용"

nurit

8. 사용자 접속

OpenLDAP의 사용자 계정(Username)을 입력하고, 암호가 " baropam " 이고, 스마트 폰의 BaroPAM 앱에서 생성한 일회용 인증키가 " 613045 " 이라면 " 암호: " 란에 " baropam613045 " 를 입력한 후 "확인" 버튼을 클릭하면 BaroPAM 모듈에 인증을 요청하여 검증이 성공하면 접속된다.

nurit

기억할 필요가 없는 비밀번호!
BaroPAM이 함께 합니다.

감사합니다!

www.nurit.co.kr

서울시 강서구 마곡중앙2로 15, 913호(마곡동, 마곡테크노타워2)
주식회사 누리아이티 대표전화 : 02-2665-0119