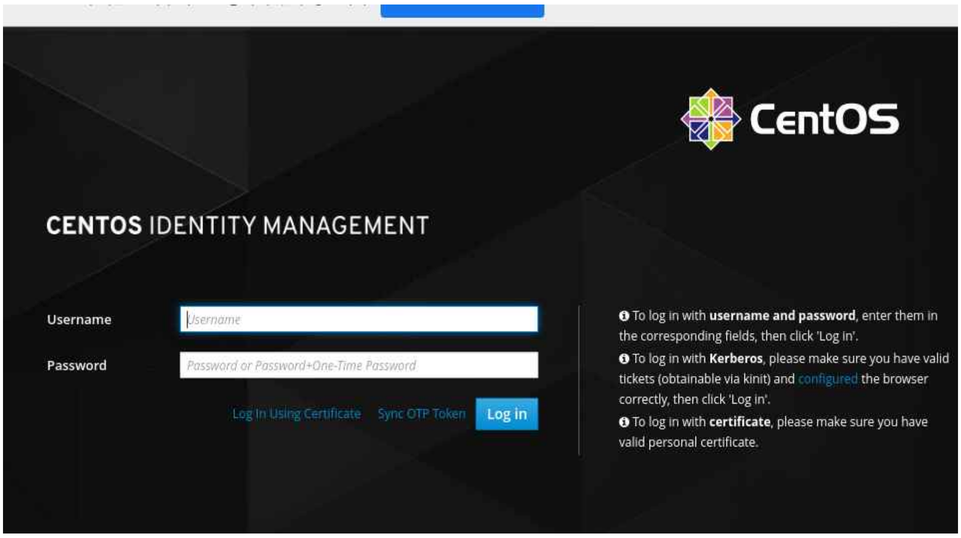
IPA + NFS + AUTOMOUNT 실습



CENTOS IDENTITY MANAGEMENT

Username: Username

Password: Password or Password+One-Time Password

- To log in with **username and password**, enter them in the corresponding fields, then click 'Log in'.
- To log in with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and configured the browser correctly, then click 'Log in'.
- To log in with **certificate**, please make sure you have valid personal certificate.

계획)

---MainSserver---		---client---
IpaServer	--사용자 정보 제공 -->	사용자 로그인
NFS Server	-- 공유 자원 제공 -->	자원을 가지고 있지 않지만 사용
AutoFs		

실제 게임 서버에서 제공하는 시스템을 이해하기 위해서

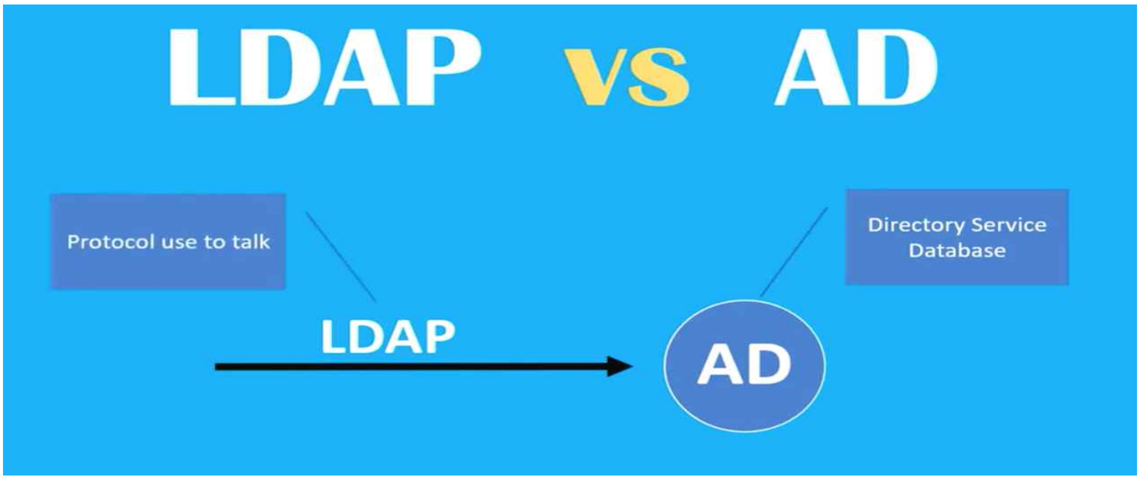
1) ipaserver
2) nfs server
3) autofs

를 사용하여 실습을 해보자

DAP(Directory Access Protocol)

디렉터리에 저장된 데이터에 접근하기위한 프로토콜(X.500, LDAP 등)

디렉터리 형태로 데이터가 저장된 서버와 그것에 접근는 클라이언트 간의 통신 규약


LDAP vs AD

Protocol use to talk

Directory Service Database

LDAP

AD

X.500

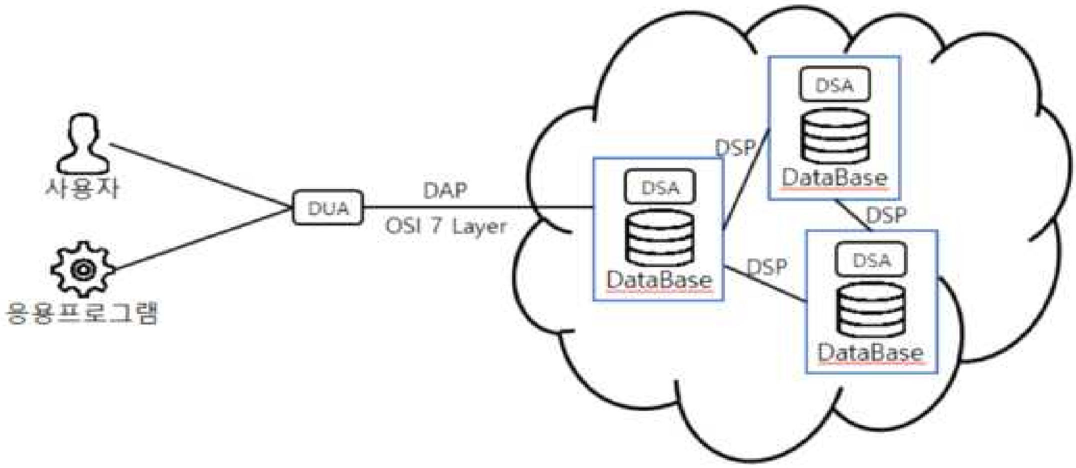
OSI 7 Layer 의 응용계층에 속한 프로토콜,

클라이언트		서버
DUA(Directory User Agent)	-	DSA(Directory System Agent)
사용자와 디렉토리 간의 인터페이스 역할 수행		디렉토리 내 사용자의 요구 수행 프로세스

DAP(Directory Access Protocol)

DSA(Directory System Protocol)

Directory Service의 구성



1) 사용자,응용프로그램에서 DUA를 통해 서비스 요청

2) DAP를 통해 DSA로 요청이 보내지고 DSA는 요청 서비스 해석

3) DataBase를 통해 서비스 수행 후 결과를 DUA를 통해 전송

※ 분산 디렉토리 서비스라면 요청 처리시 DSP를 통해 DSA간 분산처리 실행

1) LDAP(Lightweight Directory Access Protocol)

X.500의 단점 보안(DAP가 방대하고 복잡하여 구현하기 어려움)

--> X.500을 기본 모델로 하여 인터넷 환경에서 필수적인 내용 구성

경량화된 DAP

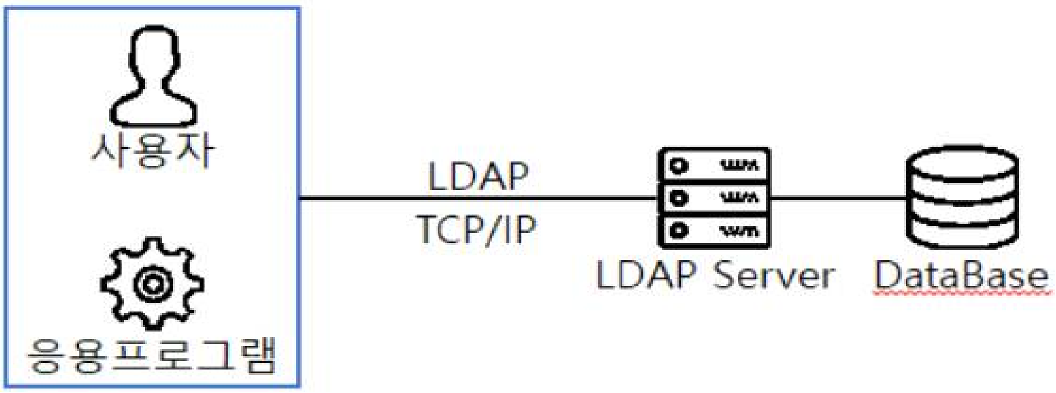
네트워크 상에서 **정보 등을 찾아보는 것**을 가능하게 만든 **소프트웨어 프로토콜**

트리 구조로 저장하여 조회하거나 관리

특정 데이터를 **중앙에서 일관 관리**하는 일반적인 경우에 사용

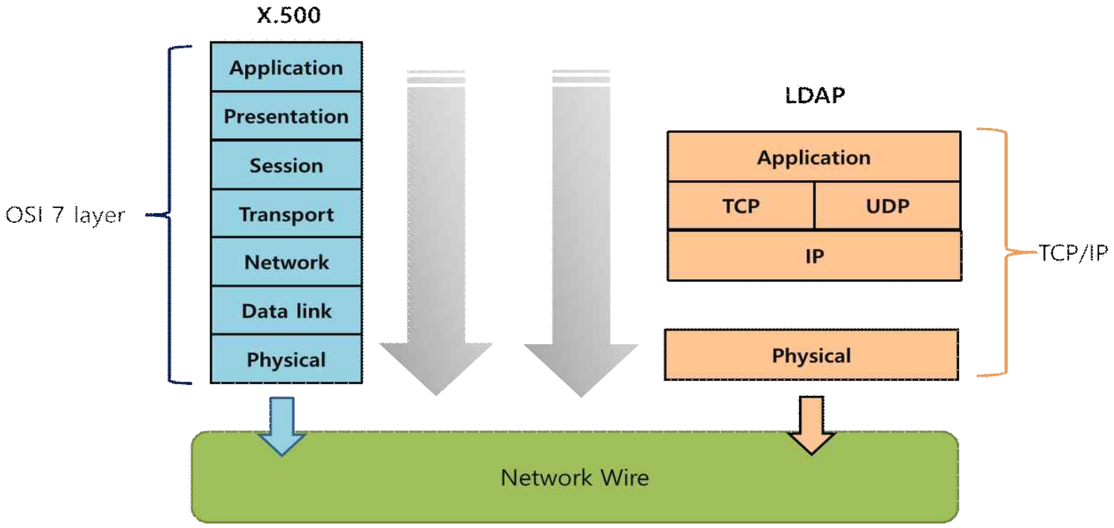
TCP/IP 네트워크 기반으로 구성 --> 경량화된 구성 가능

LDAP의 구성



1) 사용자,응용프로그램에서 LDAP을 통해 LDAP 서버에 요청 전달

2) 서버는 요청 처리 후 다시 LDAP을 통해 요청자에게 결과 전송



2) Kerberos(커버로스)

티켓 기반의 컴퓨터 네트워크 인증 **암호화 프로토콜**

티켓을 가진 유저만 서버에 접속할 수 있도록 제어 가능

티켓

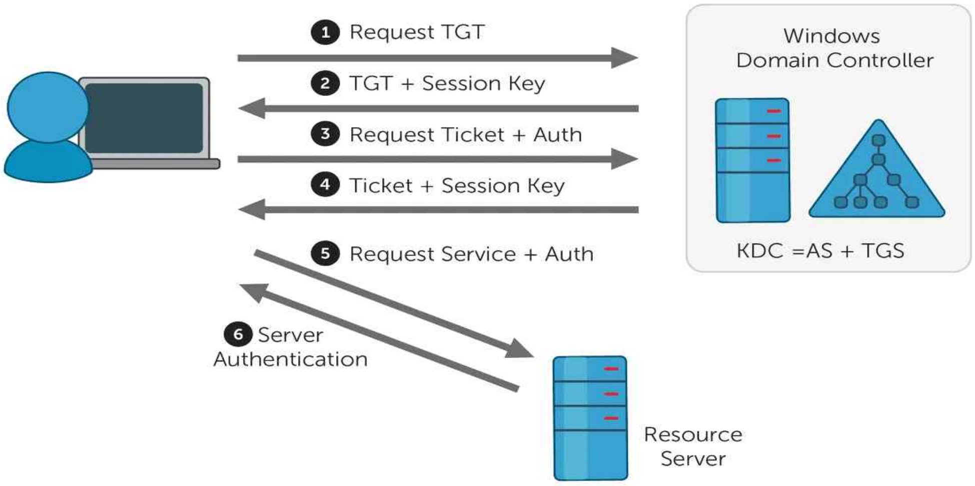
(유저 아이디, 유저 호스트 ip주소, timestamp, 티켓 수명, 세션키) 등을 안전하게 전달하는데 사용되는 정보 패킷

- 유저 아이디
- 유저 호스트 IP주소
- timestamp
- 티켓 수명
- 세션키

동작과정

커버로스는 **대칭키 암호화 방식**(암호하 복호화 키가 같다)

AS	=	인증서버
TGS	=	티켓 발급 서버
SS	=	서비스 서버(유저가 통신하고자 하는 서버)



1. 사용자가 로그인 시도, [클라이언트 -- 유저아이디 --> AS(인증서버)] 전송

2. AS(인증서버)는 사용자 아이디로 데이터베이스를 조회하고 일치 시 TGS와 TGT 생성해서 유저에게 보냄

- **TGS 세션키**는 데이터베이스 안에 있는 유저의 패스워드를 키로해서 암호화
- **TGT(Tiket Granting Tiket)** : 티켓을 받기 위한 티켓

※ TGT = (Client ID + network ip + expired time + TGS session key)

3. 유저는 받은 정보로 Authenticator를 만들어 TGT와 함께 티켓인증서버(TGS)에 보냄

4. 티켓인증서버(TGS)는 받은 TGT와 Authenticator을 복호화하여 일치 확인 후 **Ticket + SS Session Key 발급**

5. SS(서비스서버)와 유저는 TGS로 부터 받은 SS세션키를 복호화하여 또다른 Authenticator를 만들고 티켓과 함께 SS에 보냄

- 유저는 TGS Session Key가 있으므로 **SS세션키를 복호화가능**
- Authenticator - [유저 아이디와 타임스탬프] **SS 세션키로 암호화**한 데이터다.

6. SS는 유저로 부터 받은 Autehenticator와 티켓을 복호화하여 유저 아이디가 일치하는지 확인한 후, 일치한다면 Authenticator에 들어있던 타임스탬프를 SS 세션키로 암호화하여 유저에게 보낸다.

7. 유저는 받은 데이터를 SS 세션키로 복호화하여 SS에게 보낸 타임스탬프와 일치하는 지 여부를 확인한다.

커버로스가 적용된 시스템에 로그인 할 때 사용하는 명령어

$ kinit

FreeIPA

IPA(Identity Policy Authentication)

Red Hat에서 Identity Management을 위해 만들어진 소프트웨어

다음과 같은 구성요소에 대한 설치 및 관리도구 제공

LDAP 서버	- 389 프로젝트 기반
KDC	- MIT Kerberos 구현 기반
Dogtag	- 프로젝트 기반 PKI

Active Directory 통합을 위한 Samba 라이브러리

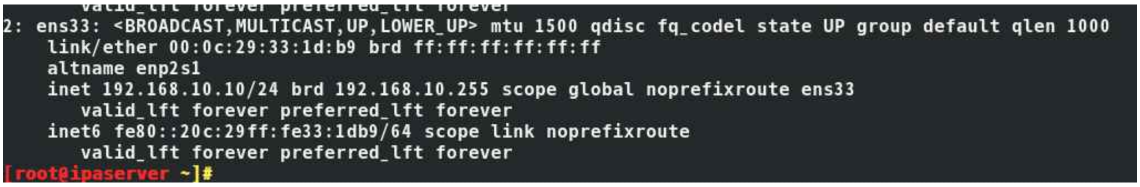
BIND 및 Bind-DynDB-LDAP 플러그인 기반 DNS 서버 .

	클라이언트	**서버**
패키지:	FreeIPA Client	FreeIPA Server

ipa 서버 구축

1. 네트워크 설정

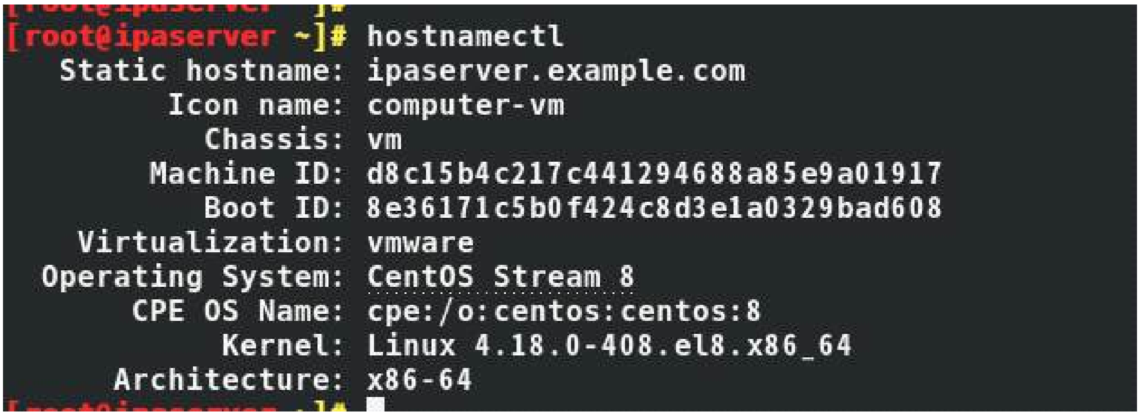
   # nmtui



```
       valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:33:1d:b9 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    inet 192.168.10.10/24 brd 192.168.10.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe33:1db9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@ipaserver ~]#
```

2. 호스트네임 설정

   # hostnamectl set-hostname "ipaserver.example.com"



```
[root@ipaserver ~]#
[root@ipaserver ~]# hostnamectl
   Static hostname: ipaserver.example.com
         Icon name: computer-vm
           Chassis: vm
        Machine ID: d8c15b4c217c441294688a85e9a01917
           Boot ID: 8e36171c5b0f424c8d3e1a0329bad608
    Virtualization: vmware
  Operating System: CentOS Stream 8
       CPE OS Name: cpe:/o:centos:centos:8
            Kernel: Linux 4.18.0-408.el8.x86_64
      Architecture: x86-64
[root@ipaserver ~]#
```

3. ipa 서버 설치

   # yum list ipa-server

      ipa-server.x86_64

   # yum list ipa-server-dns

      ipa-server-dns.noarch

   # yum list bind-dyndb-ldap

      bind-dyndb-ldap.x86_64

# yum install ipa-server.x86_64 ipa-server-dns.noarch bind-dyndb-ldap.x86_64

```
# ipa-server-install --setup-dns  /* DNS 포함 설정 */ 직접세팅 기존dns x
# ipa-server-install              /* 외부 DNS 설정 */
# ipa-server-install --uninstall
```

ipa-server-install 실행
(주의)
이 설정에서는 내부에서만 돌도록 resolv.conf 파일을 건들였다.
외부로 돌리고 싶을 경우 example.com 처럼 이미 있는 도메인을 사용 시 오류가 뜸

```
# echo "nameserver 192.168.10.10" > /etc/resolv.conf
# ipa-server-install
```

```
The log file for this installation can be found in
/var/log/ipaserver-install.log
==============================================================================
This program will set up the IPA Server.

This includes:
  * Configure a stand-alone CA (dogtag) for certificate management
  * Configure the Network Time Daemon (ntpd)
  * Create and configure an instance of Directory Server
  * Create and configure a Kerberos Key Distribution Center (KDC)
  * Configure Apache (httpd)
  * Configure DNS (bind)
  * Configure the KDC to enable PKINIT

To accept the default shown in brackets, press the Enter key.

WARNING: conflicting time&date synchronization service 'chronyd' will be
disabled in favor of ntpd

Enter the fully qualified domain name of the computer
on which you're setting up server software. Using the form
<hostname>.<domainname>
Example: master.example.com.


Server host name [ipaserver.example.com]: <ENTER>

Warning: skipping DNS resolution of host ipaserver.example.com
The domain name has been determined based on the host name.

Please confirm the domain name [example.com]: <ENTER>

The kerberos protocol requires a Realm name to be defined.
This is typically the domain name converted to uppercase.

Please provide a realm name [EXAMPLE.COM]: <ENTER>
Certain directory server operations require an administrative user.
This user is referred to as the Directory Manager and has full access
to the Directory for system management tasks and will be added to the
instance of directory server created for IPA.
The password must be at least 8 characters long.

Directory Manager password: (soldesk1.)
Password (confirm): (soldesk1.)

The IPA server requires an administrative user, named 'admin'.
This user is a regular system account used for IPA server administration.

IPA admin password: (soldesk1.)
Password (confirm): (soldesk1.)

Checking DNS domain example.com., please wait ...
Do you want to configure DNS forwarders? [yes]: no
No DNS forwarders configured
```

```
Do you want to search for missing reverse zones? [yes]: no

The IPA Master Server will be configured with:
Hostname:      ipaserver.example.com
IP address(es): 192.168.10.10
Domain name:    example.com
Realm name:     EXAMPLE.COM

BIND DNS server will be configured to serve IPA domain with:
Forwarders:       No forwarders
Forward policy:   only
Reverse zone(s):  No reverse zone

Continue to configure the system with these values? [no]: yes

The following operations may take some minutes to complete.
Please wait until the prompt is returned.

Configuring NTP daemon (ntpd)
  [1/4]: stopping ntpd
  [2/4]: writing configuration
  [3/4]: configuring ntpd to start on boot
  [4/4]: starting ntpd
Done configuring NTP daemon (ntpd).
Configuring directory server (dirsrv). Estimated time: 30 seconds
  [1/44]: creating directory server instance
  [2/44]: enabling ldapi
  [3/44]: configure autobind for root
  [4/44]: stopping directory server
  [5/44]: updating configuration in dse.ldif
  [6/44]: starting directory server
  [7/44]: adding default schema
  [8/44]: enabling memberof plugin
  [9/44]: enabling winsync plugin
  [10/44]: configuring replication version plugin
  [11/44]: enabling IPA enrollment plugin
  [12/44]: configuring uniqueness plugin
  [13/44]: configuring uuid plugin
  [14/44]: configuring modrdn plugin
  [15/44]: configuring DNS plugin
  [16/44]: enabling entryUSN plugin
  [17/44]: configuring lockout plugin
  [18/44]: configuring topology plugin
  [19/44]: creating indices
  [20/44]: enabling referential integrity plugin
  [21/44]: configuring certmap.conf
  [22/44]: configure new location for managed entries
  [23/44]: configure dirsrv ccache
  [24/44]: enabling SASL mapping fallback
  [25/44]: restarting directory server
  [26/44]: adding sasl mappings to the directory
  [27/44]: adding default layout
  [28/44]: adding delegation layout
  [29/44]: creating container for managed entries
  [30/44]: configuring user private groups
  [31/44]: configuring netgroups from hostgroups
  [32/44]: creating default Sudo bind user
  [33/44]: creating default Auto Member layout
  [34/44]: adding range check plugin
  [35/44]: creating default HBAC rule allow_all
  [36/44]: adding entries for topology management
  [37/44]: initializing group membership
  [38/44]: adding master entry
  [39/44]: initializing domain level
  [40/44]: configuring Posix uid/gid generation
  [41/44]: adding replication acis
  [42/44]: activating sidgen plugin
  [43/44]: activating extdom plugin
  [44/44]: configuring directory to start on boot
Done configuring directory server (dirsrv).
Configuring Kerberos KDC (krb5kdc)
  [1/10]: adding kerberos container to the directory
  [2/10]: configuring KDC
  [3/10]: initialize kerberos container
  [4/10]: adding default ACIs
  [5/10]: creating a keytab for the directory
  [6/10]: creating a keytab for the machine
  [7/10]: adding the password extension to the directory
  [8/10]: creating anonymous principal
  [9/10]: starting the KDC
  [10/10]: configuring KDC to start on boot
Done configuring Kerberos KDC (krb5kdc).
Configuring kadmin
  [1/2]: starting kadmin
  [2/2]: configuring kadmin to start on boot
Done configuring kadmin.
Configuring ipa-custodia
  [1/5]: Making sure custodia container exists
  [2/5]: Generating ipa-custodia config file
  [3/5]: Generating ipa-custodia keys
  [4/5]: starting ipa-custodia
  [5/5]: configuring ipa-custodia to start on boot
Done configuring ipa-custodia.
Configuring certificate server (pki-tomcatd). Estimated time: 3 minutes
  [1/29]: configuring certificate server instance
  [2/29]: reindex attributes
  [3/29]: exporting Dogtag certificate store pin
  [4/29]: stopping certificate server instance to update CS.cfg
  [5/29]: backing up CS.cfg
  [6/29]: disabling nonces
  [7/29]: set up CRL publishing
  [8/29]: enable PKIX certificate path discovery and validation
  [9/29]: starting certificate server instance
  [10/29]: configure certmonger for renewals
  [11/29]: requesting RA certificate from CA
  [12/29]: setting audit signing renewal to 2 years
  [13/29]: restarting certificate server
  [14/29]: publishing the CA certificate
  [15/29]: adding RA agent as a trusted user
  [16/29]: authorizing RA to modify profiles
  [17/29]: authorizing RA to manage lightweight CAs
  [18/29]: Ensure lightweight CAs container exists
  [19/29]: configure certificate renewals
  [20/29]: configure Server-Cert certificate renewal
  [21/29]: Configure HTTP to proxy connections
  [22/29]: restarting certificate server
  [23/29]: updating IPA configuration
  [24/29]: enabling CA instance
  [25/29]: migrating certificate profiles to LDAP
  [26/29]: importing IPA certificate profiles
  [27/29]: adding default CA ACL
  [28/29]: adding 'ipa' CA entry
  [29/29]: configuring certmonger renewal for lightweight CAs
Done configuring certificate server (pki-tomcatd).
Configuring directory server (dirsrv)
  [1/3]: configuring TLS for DS instance
  [2/3]: adding CA certificate entry
  [3/3]: restarting directory server
Done configuring directory server (dirsrv).
Configuring ipa-otpd
```

```
  [1/2]: starting ipa-otpd
  [2/2]: configuring ipa-otpd to start on boot
Done configuring ipa-otpd.
Configuring the web interface (httpd)
  [1/22]: stopping httpd
  [2/22]: setting mod_nss port to 443
  [3/22]: setting mod_nss cipher suite
  [4/22]: setting mod_nss protocol list to TLSv1.0 - TLSv1.2
  [5/22]: setting mod_nss password file
  [6/22]: enabling mod_nss renegotiate
  [7/22]: disabling mod_nss OCSP
  [8/22]: adding URL rewriting rules
  [9/22]: configuring httpd
  [10/22]: setting up httpd keytab
  [11/22]: configuring Gssproxy
  [12/22]: setting up ssl
  [13/22]: configure certmonger for renewals
  [14/22]: importing CA certificates from LDAP
  [15/22]: publish CA cert
  [16/22]: clean up any existing httpd ccaches
  [17/22]: configuring SELinux for httpd
  [18/22]: create KDC proxy config
  [19/22]: enable KDC proxy
  [20/22]: starting httpd
  [21/22]: configuring httpd to start on boot
  [22/22]: enabling oddjobd
Done configuring the web interface (httpd).
Configuring Kerberos KDC (krb5kdc)
  [1/1]: installing X509 Certificate for PKINIT
Done configuring Kerberos KDC (krb5kdc).
Applying LDAP updates
Upgrading IPA:. Estimated time: 1 minute 30 seconds
  [1/10]: stopping directory server
  [2/10]: saving configuration
  [3/10]: disabling listeners
  [4/10]: enabling DS global lock
  [5/10]: disabling Schema Compat
  [6/10]: starting directory server
  [7/10]: upgrading server
  [8/10]: stopping directory server
  [9/10]: restoring configuration
  [10/10]: starting directory server
Done.
Restarting the KDC
Configuring DNS (named)
  [1/11]: generating rndc key file
  [2/11]: adding DNS container
  [3/11]: setting up our zone
  [4/11]: setting up our own record
  [5/11]: setting up records for other masters
  [6/11]: adding NS record to the zones
  [7/11]: setting up kerberos principal
  [8/11]: setting up named.conf
  [9/11]: setting up server configuration
  [10/11]: configuring named to start on boot
  [11/11]: changing resolv.conf to point to ourselves
Done configuring DNS (named).
Restarting the web server to pick up resolv.conf changes
Configuring DNS key synchronization service (ipa-dnskeysyncd)
  [1/7]: checking status
  [2/7]: setting up bind-dyndb-ldap working directory
  [3/7]: setting up kerberos principal
  [4/7]: setting up SoftHSM
  [5/7]: adding DNSSEC containers
  [6/7]: creating replica keys
  [7/7]: configuring ipa-dnskeysyncd to start on boot
Done configuring DNS key synchronization service (ipa-dnskeysyncd).
Restarting ipa-dnskeysyncd
Restarting named
Updating DNS system records
Configuring client side components
Using existing certificate '/etc/ipa/ca.crt'.
Client hostname: ipaserver.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com

Skipping synchronizing time with NTP server.
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
trying https://ipaserver.example.com/ipa/json
[try 1]: Forwarding 'schema' to json server
'https://ipaserver.example.com/ipa/json'
trying https://ipaserver.example.com/ipa/session/json
[try 1]: Forwarding 'ping' to json server
'https://ipaserver.example.com/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server
'https://ipaserver.example.com/ipa/session/json'
Systemwide CA database updated.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server
'https://ipaserver.example.com/ipa/session/json'
SSSD enabled
Configured /etc/openldap/ldap.conf
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring example.com as NIS domain.
Client configuration complete.
The ipa-client-install command was successful

==============================================================================
Setup complete

Next steps:
    1. You must make sure these network ports are open:
        TCP Ports:
          * 80, 443: HTTP/HTTPS
          * 389, 636: LDAP/LDAPS
          * 88, 464: kerberos
          * 53: bind
        UDP Ports:
          * 88, 464: kerberos
          * 53: bind
          * 123: ntp

    2. You can now obtain a kerberos ticket using the command: 'kinit admin'
       This ticket will allow you to use the IPA tools (e.g., ipa user-add)
       and the web user interface.

Be sure to back up the CA certificates stored in /root/cacert.p12
These files are required to create replicas. The password for these
files is the Directory Manager password
```

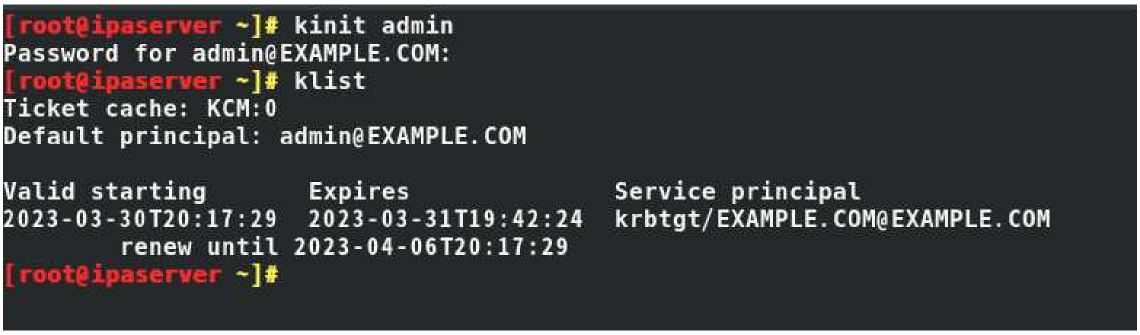
티켓 발급 및 확인)

(주의)

아래 사진은 티켓 기간만료를 설정해서 더 길게 추가 된거고 기본적으로 실행할시 renw util 은 안뜰거임

kinit admin

klist



```
[root@ipaserver ~]# kinit admin
Password for admin@EXAMPLE.COM:
[root@ipaserver ~]# klist
Ticket cache: KCM:0
Default principal: admin@EXAMPLE.COM

Valid starting       Expires              Service principal
2023-03-30T20:17:29  2023-03-31T19:42:24  krbtgt/EXAMPLE.COM@EXAMPLE.COM
        renew until 2023-04-06T20:17:29
[root@ipaserver ~]#
```

admin 유저 확인)

#ipa user-find admin

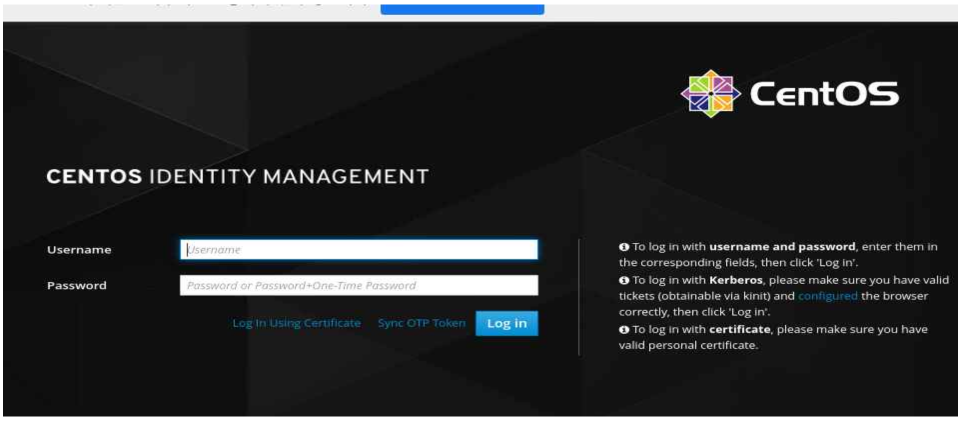
```
--------------
1 user matched
--------------
  User login: admin
  Last name: Administrator
  Home directory: /home/admin
  Login shell: /bin/bash
  Principal alias: admin@EXAMPLE.COM
  UID: 1155000000
  GID: 1155000000
  Account disabled: False
----------------------------
Number of entries returned 1
----------------------------
```

ipa-server ui 확인)

(주의)

firefox로 실행시 인증등의 오류가 떠서 그냥 chrome으로 실행

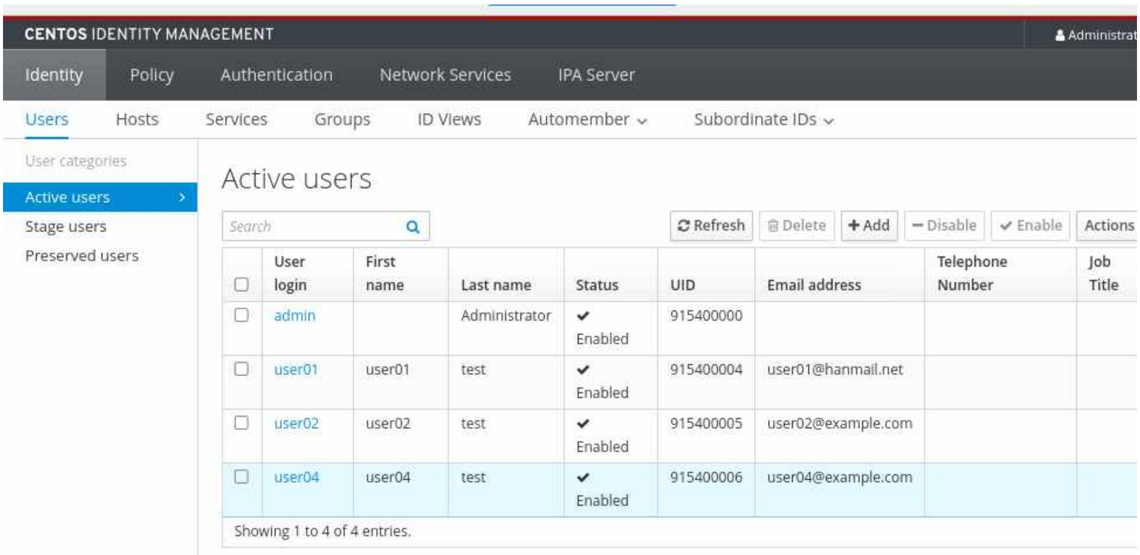
# google-chrome --no-sandbox https://ipaserver.example.com &



To log in with **username and password**, enter them in the corresponding fields, then click 'Log in'.

To log in with **Kerberos**, please make sure you have valid tickets (obtainable via kinit) and configured the browser correctly, then click 'Log in'.

To log in with **certificate**, please make sure you have valid personal certificate.



Active users

☐	User login	First name	Last name	Status	UID	Email address	Telephone Number	Job Title
☐	admin		Administrator	✓ Enabled	915400000			
☐	user01	user01	test	✓ Enabled	915400004	user01@hanmail.net		
☐	user02	user02	test	✓ Enabled	915400005	user02@example.com		
☐	user04	user04	test	✓ Enabled	915400006	user04@example.com		

Showing 1 to 4 of 4 entries.

사용자 추가 및 확인)

```
# ipa user-add user01 \
--first=user01 --last=test --email=user01@hanmail.net \
--shell=/bin/bash --password
```

```
Password: (soldesk1.)
Enter Password again to verify: (soldesk1.)
-------------------
Added user "user01"
-------------------
  User login: user01
  First name: SeoungChan
  Last name: Baik
  Full name: SeoungChan Baik
  Display name: SeoungChan Baik
  Initials: SB
  Home directory: /home/user01
  GECOS: SeoungChan Baik
  Login shell: /bin/bash
  Principal name: user01@EXAMPLE.COM
  Principal alias: user01@EXAMPLE.COM
  User password expiration: 20200325035001Z
  Email address: jang4sc@hanmail.net
  UID: 1155000001
  GID: 1155000001
  Password: True
  Member of groups: ipausers
  Kerberos keys available: True
```

```
# ipa user-find user01
```

클라이언트의 dns record 추가 및 확인

```
# ipa dnsrecord-add example.com client --a-rec 192.168.10.20
# ipa dnsrecord-show example.com client
```

```
  Record name: client
  A record: 192.168.10.20
```

클라이언트 설정

1) 네트워크 설정

```
# nmtui
```

2) hostname 설정

```
# hostnamectl set-hostaname ipaclient.example.com
```

3) resolv.conf 설정

```
# vi /etc/resolv.conf
nameserver 192.168.10.10
```

4) hosts파일 설정

```
# vi /etc/hosts
192.168.10.10  ipaserver.example.com  ipaserver
192.168.10.20  ipaclient.example.com  ipaclient
```

5) ipa-client 설치

```
# yum list ipa-client
    ipa-client.x86_64
# yum install ipa-client.x86_64
# ipa-client-install --mkhomedir --force-ntpd
```

- `--mkhomedir       create home directories for users on their first login`
- `--force-ntpd      Stop and disable any time&date synchronization`

```
Discovery was successful!
Client hostname: ipaclient.example.com
Realm: EXAMPLE.COM
DNS Domain: example.com
IPA Server: ipaserver.example.com
BaseDN: dc=example,dc=com

Continue to configure the system with these values? [no]: yes
Synchronizing time with KDC...
Attempting to sync time using ntpd.  Will timeout after 15 seconds
Attempting to sync time using ntpd.  Will timeout after 15 seconds
Unable to sync time with NTP server, assuming the time is in sync. Please
check that 123 UDP port is opened.
User authorized to enroll computers: admin
Password for admin@EXAMPLE.COM: (soldesk1.)
Successfully retrieved CA cert
    Subject:     CN=Certificate Authority,O=EXAMPLE.COM
    Issuer:      CN=Certificate Authority,O=EXAMPLE.COM
    Valid From:  2020-03-25 03:17:56
    Valid Until: 2040-03-25 03:17:56

Enrolled in IPA realm EXAMPLE.COM
Created /etc/ipa/default.conf
New SSSD config will be created
Configured sudoers in /etc/nsswitch.conf
Configured /etc/sssd/sssd.conf
Configured /etc/krb5.conf for IPA realm EXAMPLE.COM
trying https://ipaserver.example.com/ipa/json
[try 1]: Forwarding 'schema' to json server
'https://ipaserver.example.com/ipa/json'
trying https://ipaserver.example.com/ipa/session/json
[try 1]: Forwarding 'ping' to json server
'https://ipaserver.example.com/ipa/session/json'
[try 1]: Forwarding 'ca_is_enabled' to json server
'https://ipaserver.example.com/ipa/session/json'
Systemwide CA database updated.
Hostname (ipaclient.example.com) does not have A/AAAA record.
Missing reverse record(s) for address(es): 192.168.10.20.
Adding SSH public key from /etc/ssh/ssh_host_rsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ecdsa_key.pub
Adding SSH public key from /etc/ssh/ssh_host_ed25519_key.pub
[try 1]: Forwarding 'host_mod' to json server
'https://ipaserver.example.com/ipa/session/json'
SSSD enabled
```

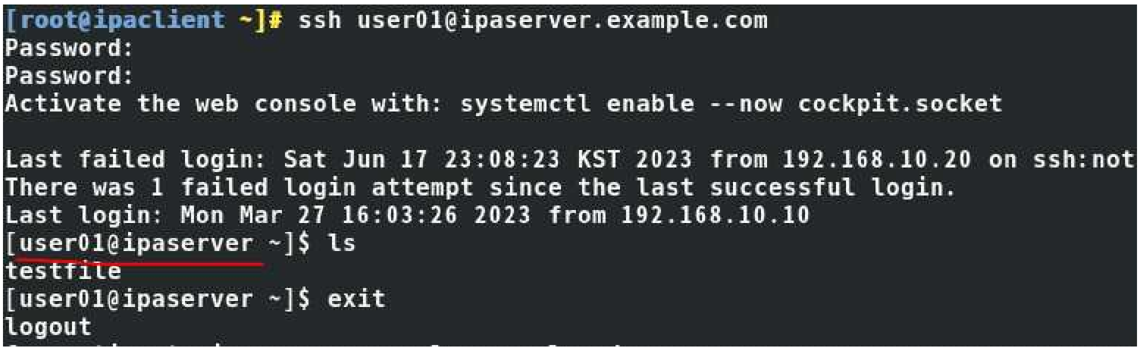
```
Configured /etc/openldap/ldap.conf
NTP enabled
Configured /etc/ssh/ssh_config
Configured /etc/ssh/sshd_config
Configuring example.com as NIS domain.
Client configuration complete.
The ipa-client-install command was successful
```

server에서 클라이언트 호스트 확인)

```
    # ipa host-show ipaclient.example.com
```

server와 클라이언트에서 접속이 되나 확인)

```
    (client)
    ssh user01@ipaserver.example.com
    (server)
    ssh user01@ipaclient.example.com
```



```
[root@ipaclient ~]# ssh user01@ipaserver.example.com
Password:
Password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Jun 17 23:08:23 KST 2023 from 192.168.10.20 on ssh:not
There was 1 failed login attempt since the last successful login.
Last login: Mon Mar 27 16:03:26 2023 from 192.168.10.10
[user01@ipaserver ~]$ ls
testfile
[user01@ipaserver ~]$ exit
logout
```

autofs + NFS Server

automount

```
--- NFS Server ---          --- NFS Client ----
공유(/share)          # mount -o OPTIONS NFSServer:/share /mnt/server
              automountd
              * MAP File(s)
```

MAP File(s)

어떤 디렉토리에 어떻게 마운트하는지 설정을 하는 설정파일

AutoFS 모듈이 동작하는데 필요한 정보가 저장된 설정 파일

1.(마스터 맵) Master Map(/etc/auto.master, /etc/auto.master.d/*.autofs)

AutoFS파일 시스템에서 가장 기준이 되는 맵, 가장 기본으로 만드는 설정 파일

```
    /mnt     /etc/auto.server
    -        /etc/auto.server2
```

2, (직접 맵) Direct Map(/etc/auto.server2)

맵 내부의 마운트 포인터로 절대경로 지정

```
    /mnt/server   -soft    NFS'sIP:/share
```

3. (간접 맵) Indirect Map(/etc/auto.server)

맵 내부의 마운트 포인터로 상대경로 지정

```
    server    -soft     NFS'sIP:/share
```

서버에서 공유된 /home/user01 .... 엄청많이 마운트해야하니까

(디렉토리)auto.master.d

automount할때 이 폴더를 기본적으로 참조,

이 안에 *.autofs 라는 파일을 만든다

*.autofs 파일에 절대경로를 쓰는방식

*.autofs 파일에 /etc에 파일을 만들어서 상대경로를 쓰는방식

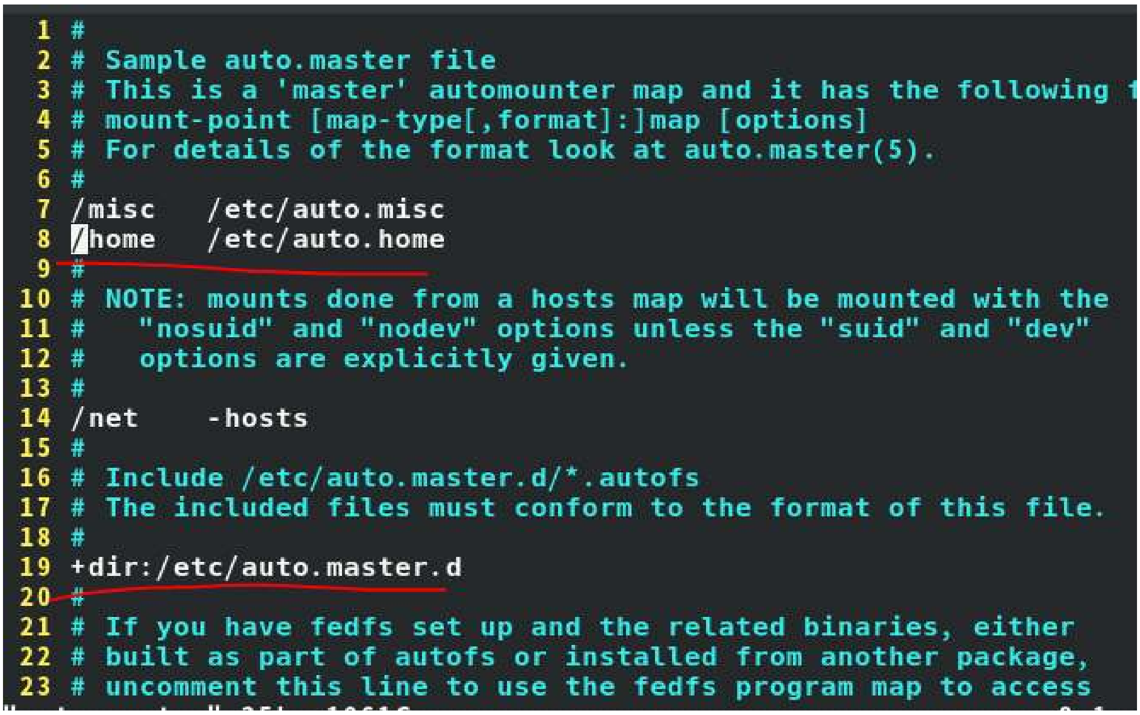
auto.master 제일 중요-메인이되는

==> master.d랑 에서 dir 저거 참고하라고 해주니 거기로 경로가 간거임

자동으로 마운트 될 디렉토리와 대상 설정 파일이 들어있음

+dir:/etc/auto.master.d

/misc /etc/auto.misc



```
#
# Sample auto.master file
# This is a 'master' automounter map and it has the following f
# mount-point [map-type[,format]:]map [options]
# For details of the format look at auto.master(5).
#
/misc   /etc/auto.misc
/home   /etc/auto.home
#
# NOTE: mounts done from a hosts map will be mounted with the
#   "nosuid" and "nodev" options unless the "suid" and "dev"
#   options are explicitly given.
#
/net    -hosts
#
# Include /etc/auto.master.d/*.autofs
# The included files must conform to the format of this file.
#
+dir:/etc/auto.master.d
#
# If you have fedfs set up and the related binaries, either
# built as part of autofs or installed from another package,
# uncomment this line to use the fedfs program map to access
```

auto.misc

==> 잡다한것 이거있으니까 참고

#boot -fstype=ext2 :/dev/hda1

auto.nfs

==> 여러개의 포인트를 만들어놓고 실행하면 자동 마운트

/maintest -rw,sync 192.16/8.10.20:/test

/* * *

.....

autofs.conf

==>automount 설정파일 (ex, nfs.conf / httpd/conf 처럼)

지속되지 않으면 끊어버리겠다

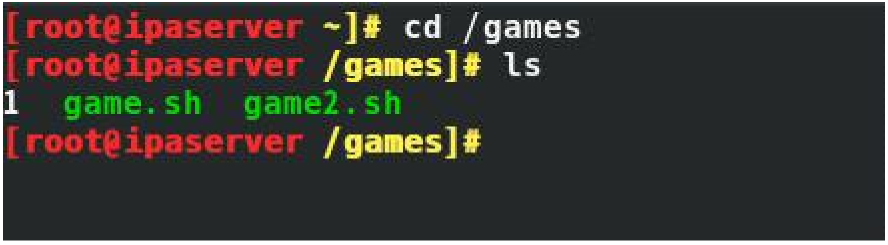
서버측에서 실행

공유 자원 생성)

ipaserver가 설치된 곳에 설치해야함.

```
# mkdir -p /games
# touch /games/game.sh
```

공유하고자하는 자원(게임 파일) 생성



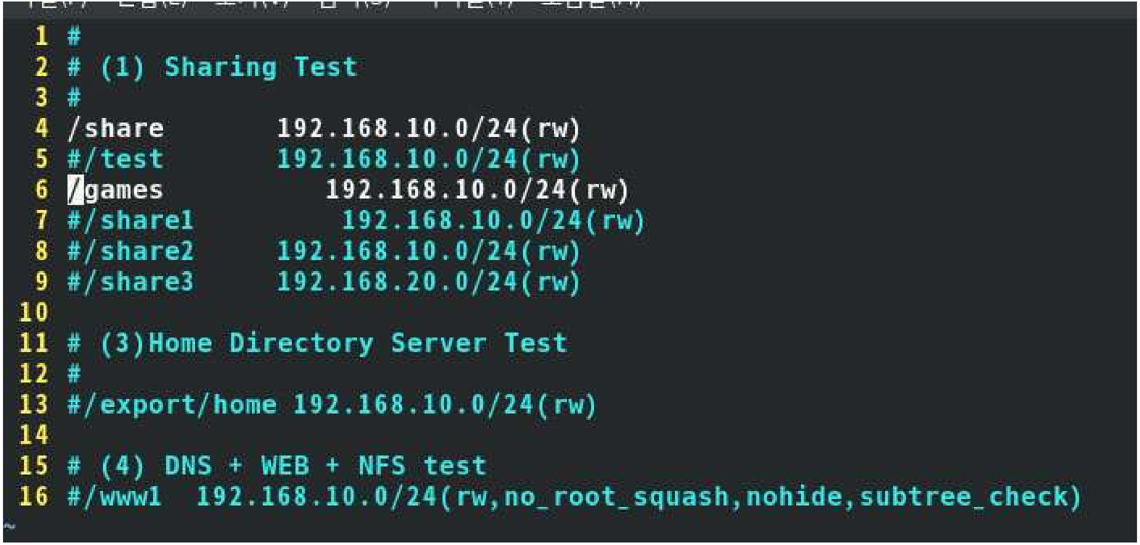
```
[root@ipaserver ~]# cd /games
[root@ipaserver /games]# ls
1   game.sh   game2.sh
[root@ipaserver /games]#
```

nfs-server 설치)

```
# yum list nfs-utils
# yum install nfs-utils.x86_64
```

nfs 공유자원 설정)

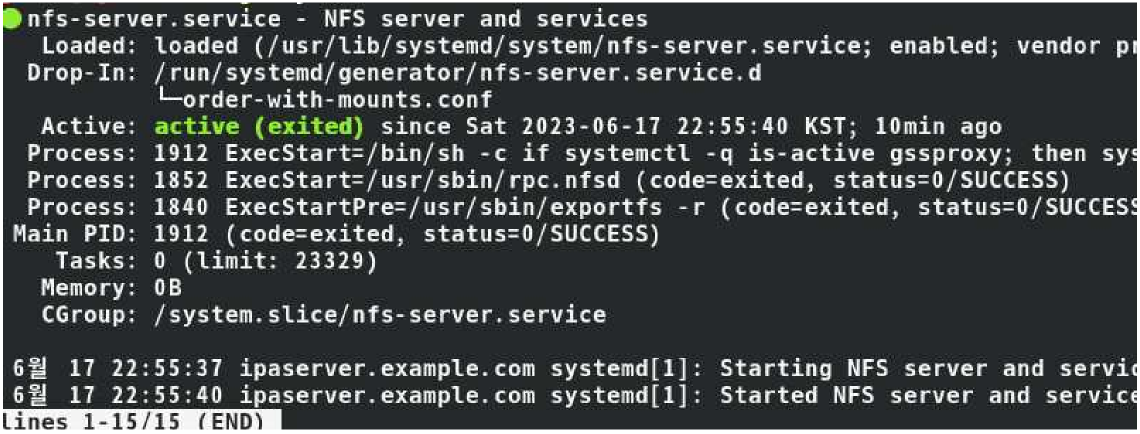
```
# vi /etc/exports
/games     *(rw)
# systemctl restart nfs-server
```



```
#
# (1) Sharing Test
#
/share        192.168.10.0/24(rw)
#/test        192.168.10.0/24(rw)
/games           192.168.10.0/24(rw)
#/share1          192.168.10.0/24(rw)
#/share2      192.168.10.0/24(rw)
#/share3      192.168.20.0/24(rw)

# (3)Home Directory Server Test
#
#/export/home 192.168.10.0/24(rw)

# (4) DNS + WEB + NFS test
#/www1  192.168.10.0/24(rw,no_root_squash,nohide,subtree_check)
~
```



```
● nfs-server.service - NFS server and services
   Loaded: loaded (/usr/lib/systemd/system/nfs-server.service; enabled; vendor pr
  Drop-In: /run/systemd/generator/nfs-server.service.d
           └─order-with-mounts.conf
   Active: active (exited) since Sat 2023-06-17 22:55:40 KST; 10min ago
  Process: 1912 ExecStart=/bin/sh -c if systemctl -q is-active gssproxy; then sys
  Process: 1852 ExecStart=/usr/sbin/rpc.nfsd (code=exited, status=0/SUCCESS)
  Process: 1840 ExecStartPre=/usr/sbin/exportfs -r (code=exited, status=0/SUCCESS
 Main PID: 1912 (code=exited, status=0/SUCCESS)
    Tasks: 0 (limit: 23329)
   Memory: 0B
   CGroup: /system.slice/nfs-server.service

 6월 17 22:55:37 ipaserver.example.com systemd[1]: Starting NFS server and servic
 6월 17 22:55:40 ipaserver.example.com systemd[1]: Started NFS server and service
lines 1-15/15 (END)
```

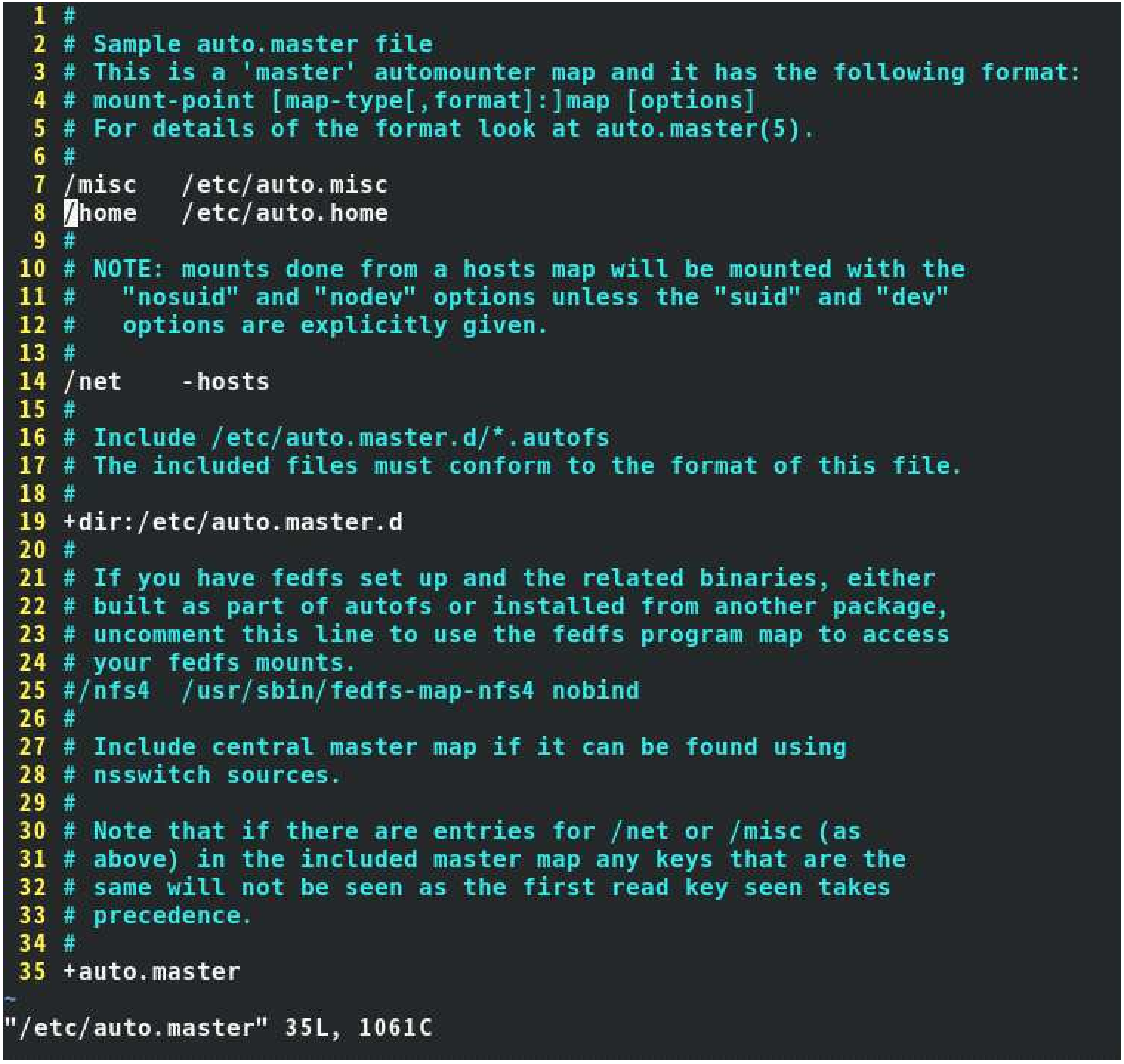
automount 설치)

```
# yum list autofs
# yum install autofs.x86_64
```

autofs 설정)

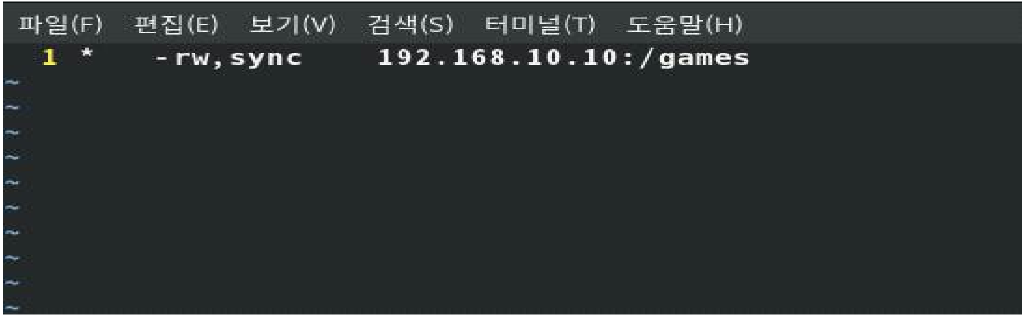
Automount(192.168.10.10:/games /home/user01)

```
# vi /etc/auto.master
/home       /etc/auto.home
```



```
#
# Sample auto.master file
# This is a 'master' automounter map and it has the following format:
# mount-point [map-type[,format]:]map [options]
# For details of the format look at auto.master(5).
#
/misc   /etc/auto.misc
/home   /etc/auto.home
#
# NOTE: mounts done from a hosts map will be mounted with the
#   "nosuid" and "nodev" options unless the "suid" and "dev"
#   options are explicitly given.
#
/net    -hosts
#
# Include /etc/auto.master.d/*.autofs
# The included files must conform to the format of this file.
#
+dir:/etc/auto.master.d
#
# If you have fedfs set up and the related binaries, either
# built as part of autofs or installed from another package,
# uncomment this line to use the fedfs program map to access
# your fedfs mounts.
#/nfs4  /usr/sbin/fedfs-map-nfs4 nobind
#
# Include central master map if it can be found using
# nsswitch sources.
#
# Note that if there are entries for /net or /misc (as
# above) in the included master map any keys that are the
# same will not be seen as the first read key seen takes
# precedence.
#
+auto.master
~
"/etc/auto.master" 35L, 1061C
```

```
# vi /etc/auto.home
*     -rw,sync     192.168.10.10:/games
```

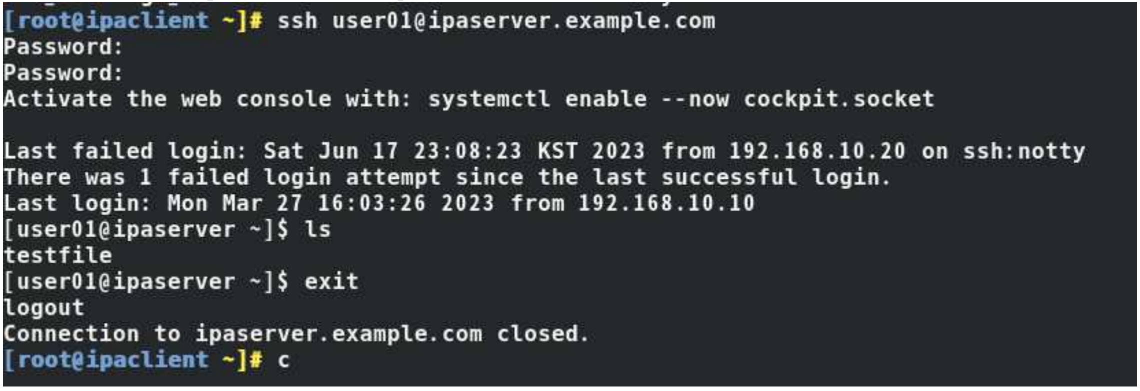


```
*     -rw,sync     192.168.10.10:/games
~
~
~
~
~
~
~
~
~
~
```

```
# systemctl restart autofs
```

클라이언트측에서 실행

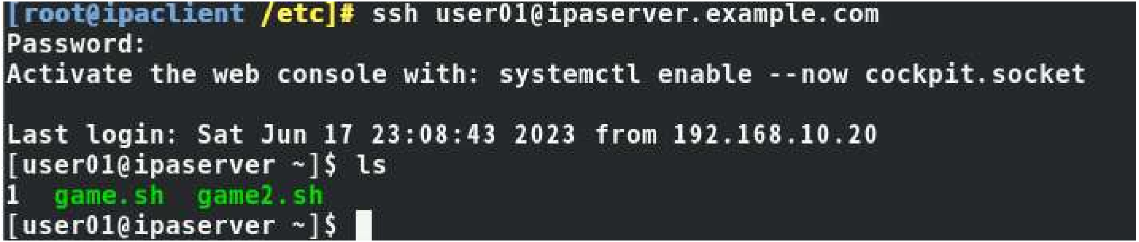
서버측에서 autofs 시작 전)
# ssh user01@ipaserver.example.com



```
[root@ipaclient ~]# ssh user01@ipaserver.example.com
Password:
Password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Sat Jun 17 23:08:23 KST 2023 from 192.168.10.20 on ssh:notty
There was 1 failed login attempt since the last successful login.
Last login: Mon Mar 27 16:03:26 2023 from 192.168.10.10
[user01@ipaserver ~]$ ls
testfile
[user01@ipaserver ~]$ exit
logout
Connection to ipaserver.example.com closed.
[root@ipaclient ~]# c
```

공유된 자원 확인)
# ssh user01@ipaserver.example.com



```
[root@ipaclient /etc]# ssh user01@ipaserver.example.com
Password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sat Jun 17 23:08:43 2023 from 192.168.10.20
[user01@ipaserver ~]$ ls
1  game.sh  game2.sh
[user01@ipaserver ~]$
```

autofs를 끈 후 시간이 지난후 공유된 자원이 사라졌나 확인
--> 남아있음
(기본 설정에 파일이 남아있는 기간이 설정되어있기 때문)

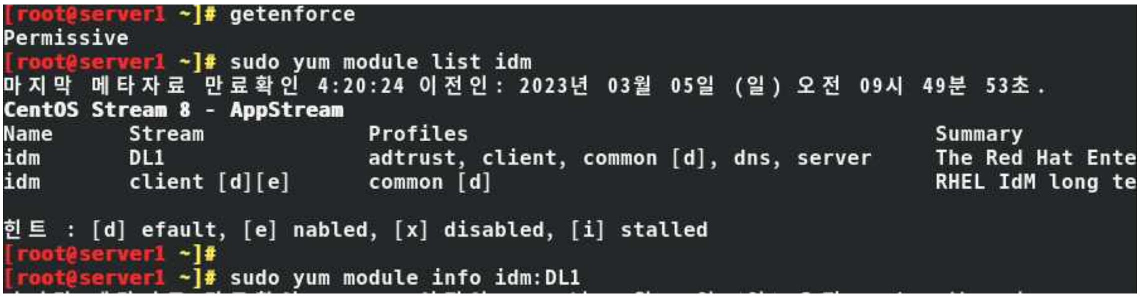
<IPA - 설치 실패 시>

yum install ipa-server 명령으로 받았더니 실패

idm이라는 꾸러미에 Profiles에 해당하는 파일이 들어있음

서버 설정이니 idm에 해당하는 DL1이라는 패키지를 받아야함

왜 ipa-server 패키지를 받는게 아닌 idm이라는걸 통해서 받나

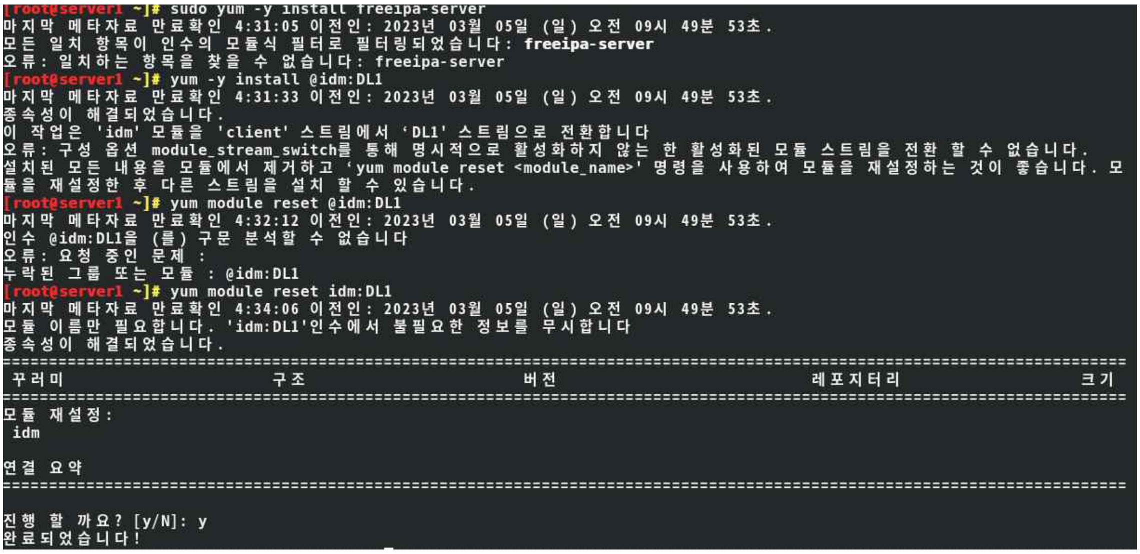


```
[root@server1 ~]# getenforce
Permissive
[root@server1 ~]# sudo yum module list idm
마지막 메타자료 만료확인 4:20:24 이전인: 2023년 03월 05일 (일) 오전 09시 49분 53초.
CentOS Stream 8 - AppStream
Name      Stream              Profiles                                    Summary
idm       DL1                 adtrust, client, common [d], dns, server    The Red Hat Ente
idm       client [d][e]       common [d]                                  RHEL IdM long te

힌트 : [d] efault, [e] nabled, [x] disabled, [i] stalled
[root@server1 ~]#
[root@server1 ~]# sudo yum module info idm:DL1
```

module reset idm:DL1 ==> 우분투 계열의 모듈을 받는 방식으로 받은 것

redhat계열의 패키지는 ~~머머하면서 있었던 걸 확인 가능

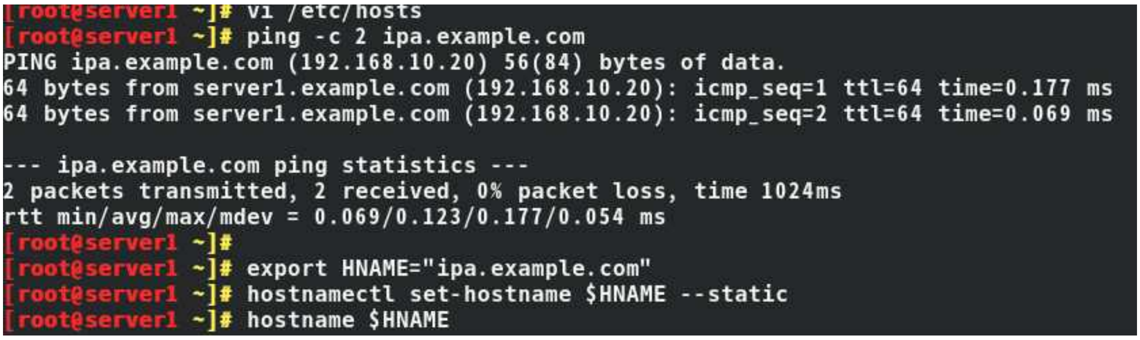


```
[root@server1 ~]# sudo yum -y install freeipa-server
마지막 메타자료 만료확인 4:31:05 이전인: 2023년 03월 05일 (일) 오전 09시 49분 53초.
모든 일치 항목이 인수의 모듈식 필터로 필터링되었습니다: freeipa-server
오류: 일치하는 항목을 찾을 수 없습니다: freeipa-server
[root@server1 ~]# yum -y install @idm:DL1
마지막 메타자료 만료확인 4:31:33 이전인: 2023년 03월 05일 (일) 오전 09시 49분 53초.
종속성이 해결되었습니다.
이 작업은 'idm' 모듈을 'client' 스트림에서 'DL1' 스트림으로 전환합니다
오류: 구성 옵션 module_stream_switch를 통해 명시적으로 활성화하지 않는 한 활성화된 모듈 스트림을 전환 할 수 없습니다.
설치된 모든 내용을 모듈에서 제거하고 'yum module reset <module_name>' 명령을 사용하여 모듈을 재설정하는 것이 좋습니다. 모
듈을 재설정한 후 다른 스트림을 설치 할 수 있습니다.
[root@server1 ~]# yum module reset @idm:DL1
마지막 메타자료 만료확인 4:32:12 이전인: 2023년 03월 05일 (일) 오전 09시 49분 53초.
인수 @idm:DL1을 (를) 구문 분석할 수 없습니다
오류: 요청 중인 문제 :
누락된 그룹 또는 모듈 : @idm:DL1
[root@server1 ~]# yum module reset idm:DL1
마지막 메타자료 만료확인 4:34:06 이전인: 2023년 03월 05일 (일) 오전 09시 49분 53초.
모듈 이름만 필요합니다. 'idm:DL1'인수에서 불필요한 정보를 무시합니다
종속성이 해결되었습니다.
================================================================================================================
 꾸러미                        구조                          버전                               레포지터리           크기
================================================================================================================
모듈 재설정:
 idm

연결 요약
================================================================================================================

진행 할 까요? [y/N]: y
완료되었습니다!
```

<hostname ipa.example.com으로 바꿔주는 과정>

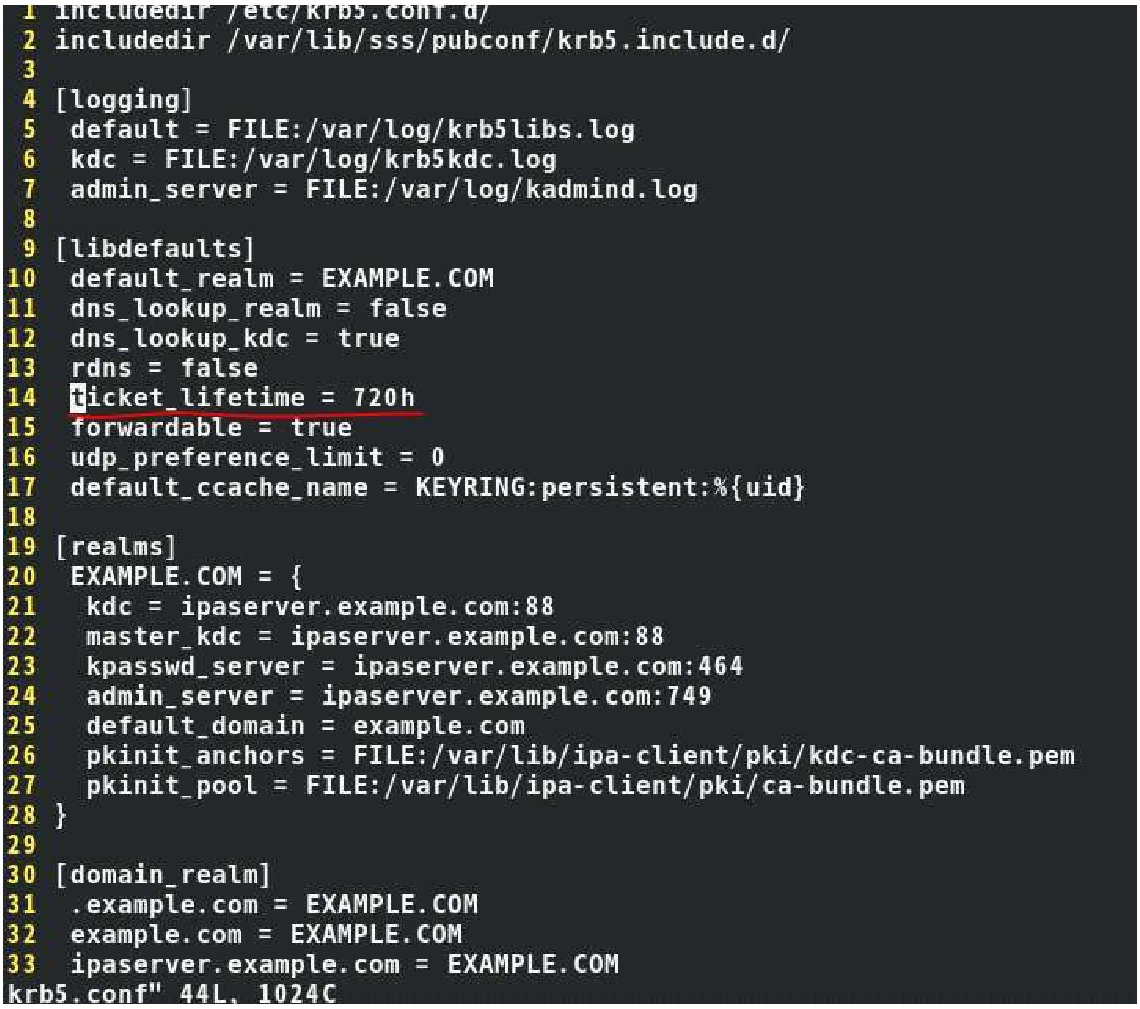


```
[root@server1 ~]# vi /etc/hosts
[root@server1 ~]# ping -c 2 ipa.example.com
PING ipa.example.com (192.168.10.20) 56(84) bytes of data.
64 bytes from server1.example.com (192.168.10.20): icmp_seq=1 ttl=64 time=0.177 ms
64 bytes from server1.example.com (192.168.10.20): icmp_seq=2 ttl=64 time=0.069 ms

--- ipa.example.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1024ms
rtt min/avg/max/mdev = 0.069/0.123/0.177/0.054 ms
[root@server1 ~]#
[root@server1 ~]# export HNAME="ipa.example.com"
[root@server1 ~]# hostnamectl set-hostname $HNAME --static
[root@server1 ~]# hostname $HNAME
```

<kerberos ticket만료기간 늘리고 싶은 경우 >

```
# vi krb5.conf
```



```
includedir /etc/krb5.conf.d/
includedir /var/lib/sss/pubconf/krb5.include.d/

[logging]
 default = FILE:/var/log/krb5libs.log
 kdc = FILE:/var/log/krb5kdc.log
 admin_server = FILE:/var/log/kadmind.log

[libdefaults]
 default_realm = EXAMPLE.COM
 dns_lookup_realm = false
 dns_lookup_kdc = true
 rdns = false
 ticket_lifetime = 720h
 forwardable = true
 udp_preference_limit = 0
 default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 EXAMPLE.COM = {
  kdc = ipaserver.example.com:88
  master_kdc = ipaserver.example.com:88
  kpasswd_server = ipaserver.example.com:464
  admin_server = ipaserver.example.com:749
  default_domain = example.com
  pkinit_anchors = FILE:/var/lib/ipa-client/pki/kdc-ca-bundle.pem
  pkinit_pool = FILE:/var/lib/ipa-client/pki/ca-bundle.pem
 }

[domain_realm]
 .example.com = EXAMPLE.COM
 example.com = EXAMPLE.COM
 ipaserver.example.com = EXAMPLE.COM
krb5.conf" 44L, 1024C
```

참고

[X.500 과 LDAP 개념]
https://m.blog.naver.com/PostView.naver?isHttpsRedirect=true&blogId=mhyoo1228&logNo=221681448674

[redhat에서 제공하는 ipaserver 구성]
https://access.redhat.com/documentation/ko-kr/red_hat_enterprise_linux/8/html-single/configuring_and_managing_identity_management/index