2015년 정보보호학과 졸업 작품

리눅스 운영체제에서 SSO 인증 체제 구현

담당교수 : 양환석 교수님
팀 명 : Stellar
팀 장 : 안세진
팀 원 : 곽현민
이슬비
조성현

2015.06

중부대학교 정보보호학과

<목 차>

요 약

1인 평균 ID와 PW를 5개 이상 보유하고 있으며, 개인정보를 수정 할 때 가진 각각의 계정들을 수정하기 번거롭고 개인정보가 유출 될 때 언제 어디서 어떤 계정이 유출 됐는지 모르므로 관리하기 어렵다.
즉 SSO를 이용하게 되면
첫째, 다른 아이디와 암호 조합으로 인한 암호 피곤을 줄일 수 있다.
둘째, 같은 아이디마다 암호를 다시 입력하는 시간을 줄일 수 있다.
셋째, 암호를 답해줘야 하는 헬프데스크 비용을 줄일 수 있다.
이러한 장점들로 인해 리눅스 운영체제에서 SSO 인증 체제 구현을 하게 되었다. 리눅스 운영체제에서 SSO인증 체제 구현을 하기 위해서는 사용자, LDAP(디렉토리 서비스), Kerberos인증, Token 송/수신 수행을 이용해 구현하였다.

1. 서 론

일반적으로 서로 다른 시스템, 서로 다른 사이트에서는 각각의 사용자 정보를 관리하게 된다. 하지만 필요에 의해서 각각의 사용자 정보를 연동하여 사용해야 할 경우가 생긴다. 이때 하나의 사용자 정보를 기반으로 여러 시스템을 하나로 개발하기에는 어려움이 따름으로서 각각의 정보를 그대로 두고 통합인증을 사용하게 된다. 이때 각각의 시스템에 로그인할 때 통합인증 정보가 있는지 확인하고 통합인증정보가 있을 경우 타 시스템에서 자동으로 로그인 가능하도록 처리하고, 없을 때는 로그인 하면서 통합인증정보를 생성하여 다른 시스템에서 참조 가능하도록 한다.
최근 회사들이 그룹화 되거나 대형화가 되어 여러 사이트들을 통합 관리하는 경우 SSO를 사용하게 된다. 이때 통합인증 SSO를 사용하게 되면, 관리자는 하나의 아이디로 모든 고객을 통합관리 할 수있게 되기에 각각의 사이트 아이디를 관리할 필요가 없게되고 기존 사용자는 정보변경 없이 하나의 사이트에 되어 있다면, 다른 모든 사이트에 별도로 가입하지 않고 로그인 할 수 있게 된다.
회사가 그룹화 됨에 따라 조직이 점점 더 커질수록 SSO 시스템은 점점 더 필요하게 될 것이고 최근 SSO시스템을 도입하는 기업과 공공기관들이 점점 늘어나고 있다.
그러므로 운영체제의 한 종류인 리눅스에서 SSO 인증 체제를 구현하였다.

2. 관련 연구

2.1 SSO(Single Sign-On)

SSO란 Single Sign On 의 약자로 여러개의 사이트에서 한번의 로그인으로 여러가지 다른 사이트들을 자동적으로 접속, 사용하는 방법을 말한다.
일반적으로 서로 다른 시스템, 서로 다른 사이트에서는 각각의 사용자 정보를 관리하게 된다. 하지만 필요에 의해서 각각의 사용자 정보를 연동하여 사용해야 할 경우가 생긴다.

이때 하나의 사용자 정보를 기반으로 여러 시스템을 하나로 개발하기에는 많은 어려움이 따른다. 따라서 각각의 정보를 그대로 두고 통합인증을 사용하게 된다.
이때 각각의 시스템에 로그인할 때 통합 인증 정보가 있는지 확인하고 통합인증정보가 있을경우 타 시스템에서 자동으로 로그인 가능하도록 처리하고, 없을 때는 로그인하면서 통합인증정보를 생성하여 다른 시스템에서 참조 가능하도록 하는 것이다.

2.2 LDAP(Lightweight Directory Access Protocol)

LDAP(Lightweight Directory Access Protocol)은 TCP/IP 위에서 디렉터리 서비스를 조회하고 수정하는 응용 프로토콜이며 논리, 계급 방식 속에서 조직화된, 비슷한 특성을 가진 객체들의 모임이다.많은 서버들 사이에 분포될 수 있으며 각 서버는 전체 디렉터리의 사본을 가질 수 있고 그 내용이 주기적으로 동기화 된다.
X.500을 근거로 한 디렉터리 데이터베이스에 접속하기 위한 통신 규약. 미국 미시간 대학에서 개발되었으며 디렉터리 정보의 등록, 갱신, 삭제와 검색 등을 실행할 수 있다. 운영 체계(OS)나 그룹웨어 제품들이 지원해 주고 있다. RFC 2251에 규정된 버전 3이 최신판이며, 통신망을 이용한 이용자 메일 주소나 이용자의 정보를 검색하는 데 주로 사용된다. LDAP 서버에는 넷스케이프 디렉터리 서버와 같은 전용 서버 제품도 있다.

디렉토리 서비스
디렉토리는 데이타베이스와 유사하지만 더욱 설명적이고 속성에 기초한 정보를 갖고 있다. 디렉토리내의 정보는 일반적으로 쓰기보다는 읽기 작업에 더욱 빈번히 이용된다. 따라서, 디렉토리는 통상적으로 정규 데이타베이스들이 다량의 복잡한(high-volume complex) 갱신을 위해 사용하는 복잡한 처리(transaction) 또는 롤백 계획(프로그램에 따라 바로 전의 체크포인트로 돌아가기, roll-back)을 수행하지 않는다. 디렉토리는 일반적으로, 적어도 허용된다면, 전부 갱신되거나 아무 것도 변경되지 않는다.
디렉토리는 다량의 순람(lookup) 또는 검색 연산에 대해 빠르게 응답하기 위해 조정된다. 디렉토리는 응답 시간을 감소시키는 반면 가용성과 신뢰성을 증대시키기 위해 정보를 널리 복제할 수 있다. 디렉토리 정보가 복제될 때 복제된 정보들 사이의 일시적인 불일치는 결국 일치된다면 무방할 것이다. 디렉토리 서비스를 제공하는 많은 다른 방법이 있다. 각각의 방법들은 다양한 종류의 정보가 디렉토리에 저장되는 것을 허용하며, 그러한 정보가 어떻게 참조, 질의 및 갱신될 수 있는지 또는 허가받지 않은 엑세스로부터 어떻게 보호되는지 등에 대한 여러가지 요건을 둔다. 어떤 디렉토리 서비스는 제한된 상황(예를 들면 단독 머신에서 finger 서비스)에 대해서 서비스를 제공하는 지역적인 반면 다른 서비스는 더욱 넓은 상황에 대해서 서비스를 제공하는 전체적이다.
LDAP 디렉토리 서비스는 클라이언트-서버 모델에 기초하는데, 하나 또는 그 이상의 LDAP 서버들이 LDAP 디렉토리 트리 또는 백엔드(backend) 데이타베이스를 구성하는 자료를 갖고 있다. LDAP 클라이언트는 LDAP 서버에 연결해 질의하며, 서버는 답 또는 클라이언트가 더 많은 정보를 얻을 수 있는 포인터(일반적으로 다른 LDAP서버)를 갖고 응답한다. 클라이언트는 어떤 LDAP 서버에 연결하던지 간에 동일한 디렉토리 구조를 본다; 한 LDAP 서버에 보내지는 이름은 다른 LDAP에 있을 수 있는 동일한 엔트리를 참조하며 이것이 LDAP와 같은 전체적인 디렉토리 서비스의 중요한 특징이다.

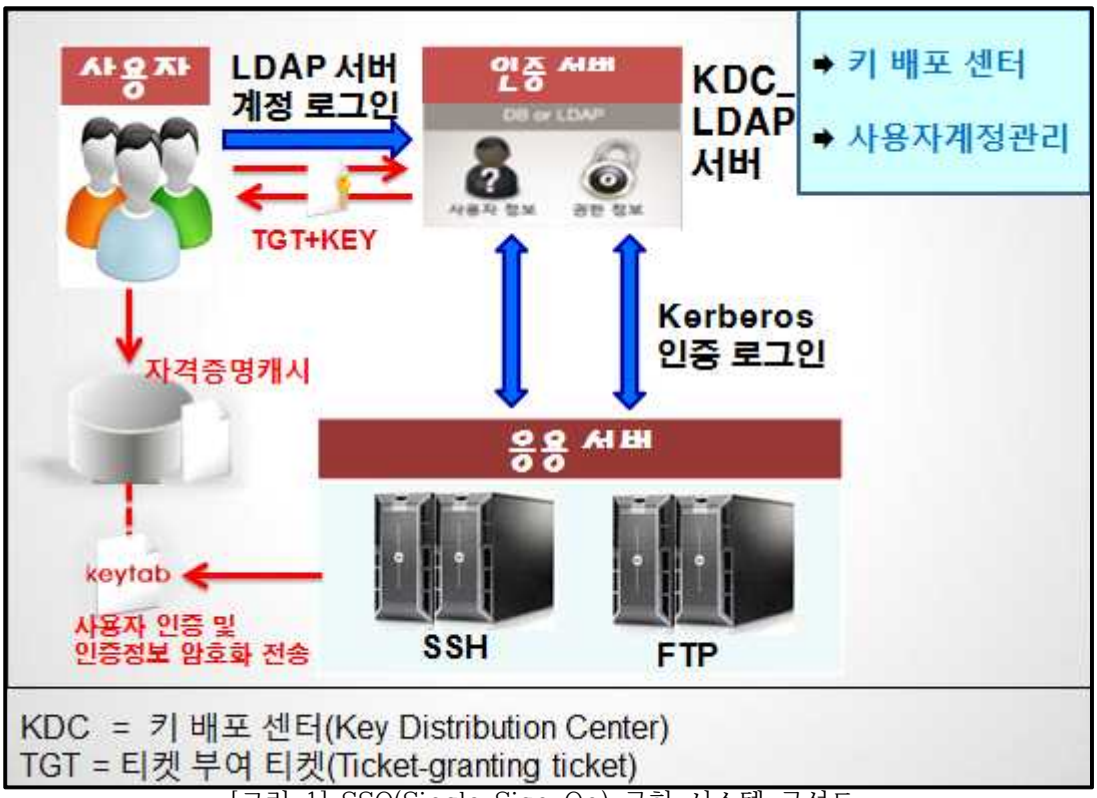
2.3 Kerbeors

Kerberos 서비스는 네트워크를 통해 보안 트랜잭션을 제공하는 클라이언트-서버 구조입니다. 이 서비스는 무결성 및 프라이버시를 비롯하여 강력한 사용자 인증을 제공한다. 인증은 네트워크 트랜잭션의 송신인과 수신자가 맞는지 보증한다. 이 서비스는 또한 앞뒤로 전달되는 데이터의 유효성을 확인(무결성)하고 전송 중 데이터를 암호화합니다(프라이버시). Kerberos 서비스를 사용할 경우 다른 시스템에 로그인, 명령 실행, 데이터 교환 및 안전한 파일 전송 등이 가능하다. 또한 이 서비스는 관리자가 서비스 및 시스템에 대한 액세스를 제한할 수 있도록 해주는 인증 서비스를 제공한다. 또한 Kerberos 사용자는 다른 사용자가 자신의 계정에 액세스하는 것을 규제할 수 있다.

Kerberos 서비스가 제공하는 보안 방식은 GSS-API(Generic Security Service Application Programming Interface)를 사용하는 응용 프로그램을 사용할 경우 인증, 무결성 및 프라이버시를 위해 Kerberos 사용을 허용한다. 이 서비스는 모듈 방식으로 GSS-API에 통합되었으므로 GSS-API를 사용하는 응용 프로그램이 필요에 가장 적합한 보안 방식을 사용할 수 있다.

3. 구축 내용

리눅스 상의 SSO(Single Sign On)구현 개념도

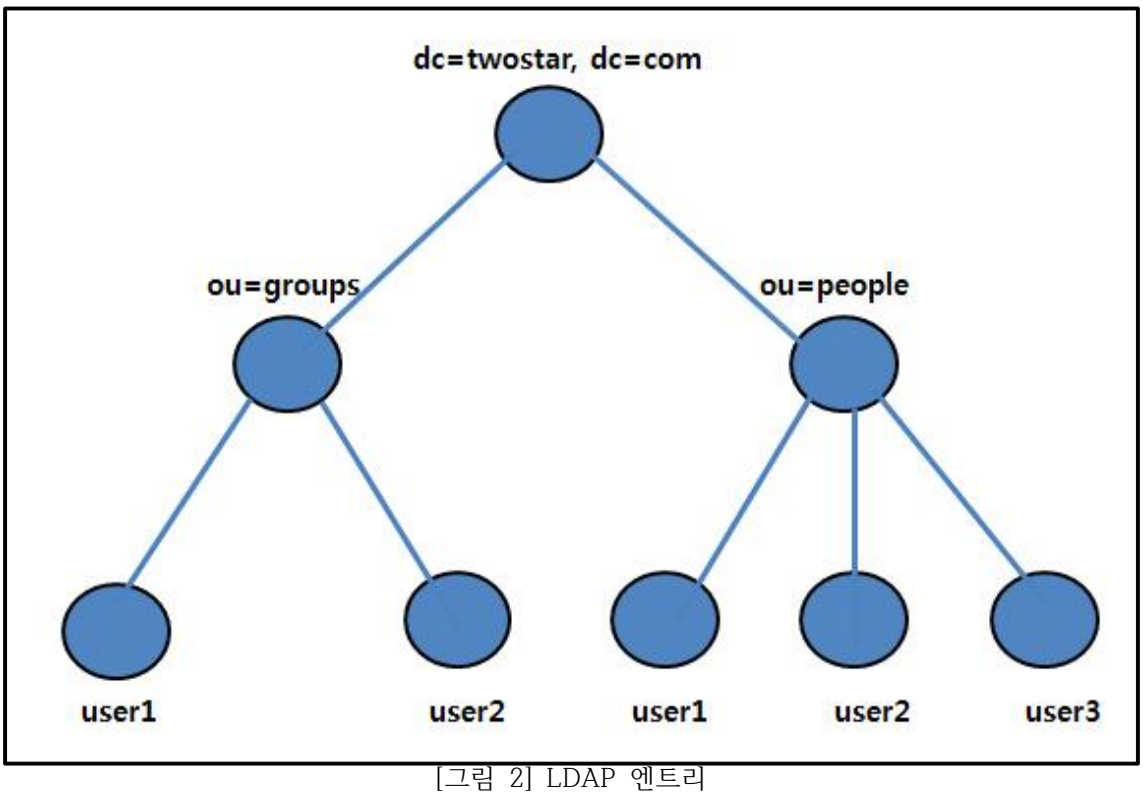


[그림 1] SSO(Single Sign On) 구현 시스템 구성도

1. phpLDAPadmin을 이용한 LDAP서버 구축
2. Kerberos 인증을 이용하기 위한 KDC 구축
3. LDAP 계정과 KDC 이용목적인 클라이언트 설정
4. SSH, FTP 서버간의 통합계정로그인

3.1 LDAP(Lightweight Directory Access Protocol) Server 설치 및 구축

이 시스템에서 쓰인 LDAP(Lightweight Directory Access Protocol) Server는 계정들을 관리하는 디렉토리 서버에 해당하는 역할을 해준다.



[그림 2] LDAP 엔트리

[그림 2]은 LDAP에서의 간단한 디렉토리의 구조의 예이다. 이러한 LDAP 디렉토리 트리 구조를 특별히 DIT(Directory Information Tree)라고 부른다. LDAP 트리(Tree) 구조에서 각 노드들을 엔트리(Entry)라고 부르고 엔트리는 LDAP에서 하나의 데이터를 나타낸다.
dc: 도메인 컨트롤러(domain controler), ou: 조직편성(organization unit)

LDAP server 설치

Source Install 방법과 yum을 이용한 설치 중 yum 을 이용한 설치방법을 설명을 하고자 한다.

yum을 이용한 설치

아래와 같은 yum 명령어를 이용해 ldap를 설치해준다.

```
yum install -y openldap openldap-servers openldap-client openldap-devel
```

```
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Updating   : cyrus-sasl-lib-2.1.23-15.el6_6.2.x86_64                    1/17
  Updating   : openldap-2.4.39-8.el6.x86_64                                2/17
  Updating   : cyrus-sasl-2.1.23-15.el6_6.2.x86_64                         3/17
  Installing : cyrus-sasl-devel-2.1.23-15.el6_6.2.x86_64                   4/17
  Installing : openldap-devel-2.4.39-8.el6.x86_64                          5/17
  Installing : openldap-servers-2.4.39-8.el6.x86_64                        6/17
  Updating   : openldap-clients-2.4.39-8.el6.x86_64                        7/17
  Updating   : cyrus-sasl-md5-2.1.23-15.el6_6.2.x86_64                     8/17
  Updating   : cyrus-sasl-gssapi-2.1.23-15.el6_6.2.x86_64                  9/17
  Updating   : cyrus-sasl-plain-2.1.23-15.el6_6.2.x86_64                  10/17
  Cleanup    : cyrus-sasl-2.1.23-13.el6_3.1.x86_64                         11/17
  Cleanup    : openldap-clients-2.4.23-32.el6_4.1.x86_64                   12/17
  Cleanup    : openldap-2.4.23-32.el6_4.1.x86_64                           13/17
  Cleanup    : cyrus-sasl-plain-2.1.23-13.el6_3.1.x86_64                   14/17
  Cleanup    : cyrus-sasl-gssapi-2.1.23-13.el6_3.1.x86_64                  15/17
  Cleanup    : cyrus-sasl-md5-2.1.23-13.el6_3.1.x86_64                     16/17
  Cleanup    : cyrus-sasl-lib-2.1.23-13.el6_3.1.x86_64                     17/17
  Verifying  : openldap-servers-2.4.39-8.el6.x86_64                        1/17
  Verifying  : cyrus-sasl-md5-2.1.23-15.el6_6.2.x86_64                     2/17
  Verifying  : openldap-clients-2.4.39-8.el6.x86_64                        3/17
  Verifying  : cyrus-sasl-devel-2.1.23-15.el6_6.2.x86_64                   4/17
  Verifying  : cyrus-sasl-gssapi-2.1.23-15.el6_6.2.x86_64                  5/17
  Verifying  : openldap-devel-2.4.39-8.el6.x86_64                          6/17
  Verifying  : cyrus-sasl-plain-2.1.23-15.el6_6.2.x86_64                   7/17
  Verifying  : openldap-2.4.39-8.el6.x86_64                                8/17
```

```
  Verifying  : cyrus-sasl-2.1.23-15.el6_6.2.x86_64                  9/17
  Verifying  : cyrus-sasl-lib-2.1.23-15.el6_6.2.x86_64              10/17
  Verifying  : openldap-2.4.23-32.el6_4.1.x86_64                    11/17
  Verifying  : cyrus-sasl-lib-2.1.23-13.el6_3.1.x86_64              12/17
  Verifying  : cyrus-sasl-2.1.23-13.el6_3.1.x86_64                  13/17
  Verifying  : cyrus-sasl-plain-2.1.23-13.el6_3.1.x86_64            14/17
  Verifying  : cyrus-sasl-md5-2.1.23-13.el6_3.1.x86_64              15/17
  Verifying  : cyrus-sasl-gssapi-2.1.23-13.el6_3.1.x86_64           16/17
  Verifying  : openldap-clients-2.4.23-32.el6_4.1.x86_64            17/17

Installed:
  openldap-devel.x86_64 0:2.4.39-8.el6   openldap-servers.x86_64 0:2.4.39-8.el6

Dependency Installed:
  cyrus-sasl-devel.x86_64 0:2.1.23-15.el6_6.2

Updated:
  openldap.x86_64 0:2.4.39-8.el6

Dependency Updated:
  cyrus-sasl.x86_64 0:2.1.23-15.el6_6.2
  cyrus-sasl-gssapi.x86_64 0:2.1.23-15.el6_6.2
  cyrus-sasl-lib.x86_64 0:2.1.23-15.el6_6.2
  cyrus-sasl-md5.x86_64 0:2.1.23-15.el6_6.2
  cyrus-sasl-plain.x86_64 0:2.1.23-15.el6_6.2
  openldap-clients.x86_64 0:2.4.39-8.el6

Complete!
[root@ldap ~]#
```

LDAP 서버 설정

/etc/openldap/slapd.d/cn=config/oldDatabase\=\{2\}bdb.ldif
의 내용을 아래와 같이 수정해준다.

```
root@ldap:/etc/openldap/slapd.d/cn=config
파일(F)  편집(E)  보기(V)  검색(S)  터미널(T)  도움말(H)
 1 dn: olcDatabase={2}bdb
 2 objectClass: olcDatabaseConfig
 3 objectClass: olcBdbConfig
 4 olcDatabase: {2}bdb
 5 olcSuffix: dc=twostar,dc=com
 6 olcAddContentAcl: FALSE
 7 olcLastMod: TRUE
 8 olcMaxDerefDepth: 15
 9 olcReadOnly: FALSE
10 olcRootDN: cn=Manager,dc=twostar,dc=com
11 olcSyncUseSubentry: FALSE
12 olcMonitoring: TRUE
13 olcDbDirectory: /var/lib/ldap
14 olcDbCacheSize: 1000
15 olcDbCheckpoint: 1024 15
16 olcDbNoSync: FALSE
17 olcDbDirtyRead: FALSE
18 olcDbIDLcacheSize: 0
19 olcDbIndex: objectClass pres,eq
20 olcDbIndex: cn pres,eq,sub
21 olcDbIndex: uid pres,eq,sub
22 olcDbIndex: uidNumber pres,eq
23 olcDbIndex: gidNumber pres,eq
24 olcDbIndex: mail pres,eq,sub
25 olcDbIndex: ou pres,eq,sub
26 olcDbIndex: sn pres,eq,sub
27 olcDbIndex: givenName pres,eq,sub
28 olcDbIndex: loginShell pres,eq
45 olcRootPW: {SSHA}XVWTeDHcO/bEp4i2zoKfpBybUau+qiIT
```

이어서

/etc/openldap/slapd.d/cn=config/oldDatabase\=\{1\}monitor.ldif

의 파일내용을 아래와 같이 수정해준다.

```
olcAccess: {0}to *  by dn.base="gidNumber=0+uidNumber=0,cn=peercred,cn=externa
 l,cn=auth" read  by dn.base="cn=Manager,dc=twostar,dc=com" read  by * none
```

수정한다음

```
[root@ldap ~]# updatedb
```

를 입력함으로써 db업데이트를 시켜준다.

이어서 /usr/share/openldap-servers/DB_CONFIG.example을 /var/lib/ldap/에 복사해 준다.

```
[root@ldap openldap-servers]# pwd
/usr/share/openldap-servers
[root@ldap openldap-servers]# ls
DB_CONFIG.example  slapd.conf.obsolete  slapd.ldif.example
[root@ldap openldap-servers]# cp DB_CONFIG.example /var/lib/ldap/DB_CONFIG
```

/var/lib/ldap/ 과 그 하위 풀더나 파일들에 소유권설정(사용자,그룹명)을 ldap으로 변경해준다.

```
[root@ldap ~]# chown -R ldap.ldap /var/lib/ldap
[root@ldap ~]# ls -ld /var/lib/ldap/
drwx------. 2 ldap ldap 4096 2015-05-27 00:23 /var/lib/ldap/
```

slaptest 명령으로 test가 성공적이라는 문구가 나타는 것을 확인 할 수 있다.

```
[root@ldap ~]# slaptest -u
config file testing succeeded
```

LDAP server를 start 해준다.

```
[root@ldap openldap-servers]# service slapd start
slapd (을)를 시작 중:                                     [  OK  ]
[root@ldap openldap-servers]# ps -ef | grep slapd
ldap      4882     1  4 12:36 ?        00:00:03 /usr/sbin/slapd -h  ldap:/// lda
pi:/// -u ldap
root      4890  4284  0 12:37 pts/0    00:00:00 grep slapd
[root@ldap openldap-servers]# netstat -nat | grep 389
tcp        0      0 0.0.0.0:389                 0.0.0.0:*                   LIST
EN
tcp        0      0 :::389                      :::*                        LIST
EN
```

ldapsearch 명령을 통해 확인한 상태다.

```
[root@ldap openldap-servers]# ldapsearch -x -b "dc=twostar,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=twostar,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 32 No such object

# numResponses: 1
```

migrationtools 설치

yum 명령을 통해 아래와 같이 설치해준다.

```
yum install -y migrationtools
```

```
Dependencies Resolved

================================================================================
 Package                Arch             Version              Repository     Size
================================================================================
Installing:
 migrationtools         noarch           47-7.el6             base           25 k

Transaction Summary
================================================================================
Install       1 Package(s)

Total download size: 25 k
Installed size: 104 k
Downloading Packages:
migrationtools-47-7.el6.noarch.rpm                          |  25 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing : migrationtools-47-7.el6.noarch                               1/1
  Verifying  : migrationtools-47-7.el6.noarch                               1/1

Installed:
  migrationtools.noarch 0:47-7.el6

Complete!
[root@ldap ~]#
```

migrate_ 설정 및 도구 사용

/usr/share/migrationtools/migrate_common.ph
다음 화면과 같이 파일내용을 수정해 준다.

```
70 # Default DNS domain
71 $DEFAULT_MAIL_DOMAIN = "twostar.com";
72
73 # Default base
74 $DEFAULT_BASE = "dc=twostar,dc=com";
75
76 # Turn this on for inetLocalMailReceipient
77 # sendmail support:  add the following to
78 # sendmail.mc (thanks to Petr@Kristof.CZ):
79 ##### CUT HERE #####
80 #define(`confLDAP_DEFAULT_SPEC',`-h "ldap.padl.com"')dnl
81 #LDAPROUTE_DOMAIN_FILE(`/etc/mail/ldapdomains')dnl
82 #FEATURE(ldap_routing)dnl
83 ##### CUT HERE #####
84 # where /etc/mail/ldapdomains contains names of ldap_routed
85 # domains (similiar to MASQUERADE_DOMAIN_FILE).
86 # $DEFAULT_MAIL_HOST = "mail.padl.com";
87
88 # turn this on to support more general object clases
89 # such as person.
90 $EXTENDED_SCHEMA = 1;
```

/usr/share/migrationtools/migrate_passwd_pl
의 파일 내용을 다음과 같이 수정해준다.

```
186 sub read_shadow_file
187 {
188         open(SHADOW, "/root/ldap/passwords") || return;
```

passwd, shadow, group의 계정 파일들을 /root/ldap/에 파일 생성 시킨다.

```
getent passwd | tail -n 5 > /root/ldap/users
getent shadow | tail -n 5 > /root/ldap/passwords
getent group | tail -n 5 > /root/ldap/groups
```

migration 도구 사용를 사용해 ldif 파일들을 생성

```
[root@ldap migrationtools]# ./migrate_base.pl > /root/ldap/base.ldif
```

ldapadd를 명령을 통해 base.ldif파일을 엔트리에 추가시킨다.

```
[root@ldap migrationtools]# ./migrate_passwd.pl /root/ldap/users > /root/ldap/users.ld
if
[root@ldap migrationtools]# ./migrate_group.pl /root/ldap/groups > /root/ldap/groups.l
dif
[root@ldap migrationtools]# ls /root/ldap
base.ldif  groups  groups.ldif  passwords  users  users.ldif
```

```
[root@ldap ldap]# ldapadd -x -W -D "cn=Manager,dc=twostar,dc=com" -f base.ldif
Enter LDAP Password:
adding new entry "dc=twostar,dc=com"

adding new entry "ou=Hosts,dc=twostar,dc=com"

adding new entry "ou=Rpc,dc=twostar,dc=com"

adding new entry "ou=Services,dc=twostar,dc=com"

adding new entry "nisMapName=netgroup.byuser,dc=twostar,dc=com"

adding new entry "ou=Mounts,dc=twostar,dc=com"

adding new entry "ou=Networks,dc=twostar,dc=com"

adding new entry "ou=People,dc=twostar,dc=com"

adding new entry "ou=Groups,dc=twostar,dc=com"

adding new entry "ou=Netgroup,dc=twostar,dc=com"

adding new entry "ou=Protocols,dc=twostar,dc=com"

adding new entry "ou=Aliases,dc=twostar,dc=com"

adding new entry "nisMapName=netgroup.byhost,dc=twostar,dc=com"
```

이어서 user.ldif, groups.ldif 파일을 엔트리에 추가시킨다.

```
[root@ldap ldap]# ldapadd -x -W -D "cn=Manager,dc=twostar,dc=com" -f users.ldif
Enter LDAP Password:
adding new entry "uid=user1,ou=People,dc=twostar,dc=com"

adding new entry "uid=user2,ou=People,dc=twostar,dc=com"

adding new entry "uid=user3,ou=People,dc=twostar,dc=com"

adding new entry "uid=user4,ou=People,dc=twostar,dc=com"

adding new entry "uid=user5,ou=People,dc=twostar,dc=com"
```

```
[root@ldap ldap]# ldapadd -x -W -D "cn=Manager,dc=twostar,dc=com" -f groups.ldif
Enter LDAP Password:
adding new entry "cn=user1,ou=Groups,dc=twostar,dc=com"

adding new entry "cn=user2,ou=Groups,dc=twostar,dc=com"

adding new entry "cn=user3,ou=Groups,dc=twostar,dc=com"

adding new entry "cn=user4,ou=Groups,dc=twostar,dc=com"

adding new entry "cn=user5,ou=Groups,dc=twostar,dc=com"
```

ldapsearch 명령 계정확인

ldapsearch명령을 통해 twostar.com을 검색한 화면이다.
base.ldif , users.ldif, groups.ldif 파일의 내용들이 검색 된 것을 확인할 수 있으며 중심적인 user1,user2,user3,user4,user5의 계정을 확인할 수 있다.

```
[root@ldap ~]# ldapsearch -x -b "dc=twostar,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=twostar,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# twostar.com
dn: dc=twostar,dc=com
dc: twostar
objectClass: top
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Hosts, twostar.com
dn: ou=Hosts,dc=twostar,dc=com
ou: Hosts
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Rpc, twostar.com
dn: ou=Rpc,dc=twostar,dc=com
```

ou: organization unit (조직 편성), cn : common name(기본 이름)
o: organization(조직), dc : domain controler

```
ou: Rpc
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Services, twostar.com
dn: ou=Services,dc=twostar,dc=com
ou: Services
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# netgroup.byuser, twostar.com
dn: nisMapName=netgroup.byuser,dc=twostar,dc=com
nisMapName: netgroup.byuser
objectClass: top
objectClass: nisMap
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Mounts, twostar.com
dn: ou=Mounts,dc=twostar,dc=com
ou: Mounts
objectClass: top
objectClass: organizationalUnit
```

조직들(Networks, People, Groups)의 정보를 볼 수 있다.

```
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Networks, twostar.com
dn: ou=Networks,dc=twostar,dc=com
ou: Networks
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# People, twostar.com
dn: ou=People,dc=twostar,dc=com
ou: People
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Groups, twostar.com
dn: ou=Groups,dc=twostar,dc=com
ou: Groups
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com
```

조직들(Netgroup, Protocols, Aliases, nisMapName)의 정보를 볼 수 있다.

```
# Netgroup, twostar.com
dn: ou=Netgroup,dc=twostar,dc=com
ou: Netgroup
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Protocols, twostar.com
dn: ou=Protocols,dc=twostar,dc=com
ou: Protocols
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Aliases, twostar.com
dn: ou=Aliases,dc=twostar,dc=com
ou: Aliases
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com

# netgroup.byhost, twostar.com
dn: nisMapName=netgroup.byhost,dc=twostar,dc=com
nisMapName: netgroup.byhost
```

People조직의 user1에 관한 엔트리

```
objectClass: top
objectClass: nisMap
objectClass: domainRelatedObject
associatedDomain: twostar.com

# user1, People, twostar.com
dn: uid=user1,ou=People,dc=twostar,dc=com
uid: user1
cn: user1
sn: user1
mail: user1@twostar.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JFVtaUZwRlJ3JFRRUTViUWlpb3UyemhMMzF1STZtV1FESkhaeFg
 xUWlsNlJtSjRvM0hsTThvdUYyWms5MnNvZGkucll0cDNNazRqdFFGNjdaNkplaFNJbEFQbXV1SU8x
shadowLastChange: 16558
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 501
gidNumber: 501
homeDirectory: /home/ldap/user1
```

People조직의 user2에 관한 엔트리

```
# user2, People, twostar.com
dn: uid=user2,ou=People,dc=twostar,dc=com
uid: user2
cn: user2
sn: user2
mail: user2@twostar.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JEkuYUNQcFhXJFA4bjV0US5yWjFKZ21IRnQxUE44N09oWVpQM0F
 NbXo4ZWFrbS55WUt2d3lWTy9BUzguMm5SdU9wc3RWRnRQaEJZNWFzV2sxUG0xUXI3QmdTTkdFdFAu
shadowLastChange: 16558
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 502
gidNumber: 502
homeDirectory: /home/ldap/user2

# user3, People, twostar.com
dn: uid=user3,ou=People,dc=twostar,dc=com
uid: user3
cn: user3
```

People조직의 user3에 관한 엔트리

```
sn: user3
mail: user3@twostar.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JFZpLkxsUFBqJE50VmhKcUtEWDUwRTBxY1B2NnlCejJyZEFSSFF
 VRnFXQmlKbTMuWExWYWY0ajk0OXJ1cTZMQTd2dmNEQnZrbXNvSHc0VTh5SHlTOEFSVFRGV3RhQ1Iu
shadowLastChange: 16558
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 503
gidNumber: 503
homeDirectory: /home/ldap/user3

# user4, People, twostar.com
dn: uid=user4,ou=People,dc=twostar,dc=com
uid: user4
cn: user4
sn: user4
mail: user4@twostar.com
objectClass: person
objectClass: organizationalPerson
```

People조직의 user4, user5에 관한 엔트리

```
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
userPassword:: e2NyeXB0fSQ2JEFtTzRwMHE4JEo5RWVWcWxFZ1JDNGMvdWFlL25DWXM3ME9JNHZ
 YY2pmOWJLWjhZVi90Z1NLdzAzWWtFZHhRbjVTSUFpTXlLbG9kVXJsM3JnQU91TXRQWXcxS1NkZEwx
shadowLastChange: 16558
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 504
gidNumber: 504
homeDirectory: /home/ldap/user4

# user5, People, twostar.com
dn: uid=user5,ou=People,dc=twostar,dc=com
uid: user5
cn: user5
sn: user5
mail: user5@twostar.com
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
```

Groups조직의 user1~ user3에 관한 엔트리

```
# user1, Groups, twostar.com
dn: cn=user1,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user1
userPassword:: e2NyeXB0fXg=
gidNumber: 501

# user2, Groups, twostar.com
dn: cn=user2,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user2
userPassword:: e2NyeXB0fXg=
gidNumber: 502

# user3, Groups, twostar.com
dn: cn=user3,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user3
userPassword:: e2NyeXB0fXg=
gidNumber: 503

# user4, Groups, twostar.com
dn: cn=user4,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
```

People조직의 user4, user5에 관한 엔트리

3.2 LDAP_Client 설치 및 설정

```
[root@client ldap]# yum install openldap-clients openldap openldap-devel -y
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: virror.hanoilug.org
 * centosplus: centos-hcm.viettelidc.com.vn
 * epel: mirror01.idc.hinet.net
 * extras: mirrors.vonline.vn
 * rpmforge: mirror.smartmedia.net.id
 * rpmforge-extras: mirror.smartmedia.net.id
 * updates: centosk3.centos.org
Setting up Install Process
Package openldap-clients-2.4.23-34.el6_5.1.i686 already installed and latest version
Package openldap-2.4.23-34.el6_5.1.i686 already installed and latest version
Package openldap-devel-2.4.23-34.el6_5.1.i686 already installed and latest version
Nothing to do
```

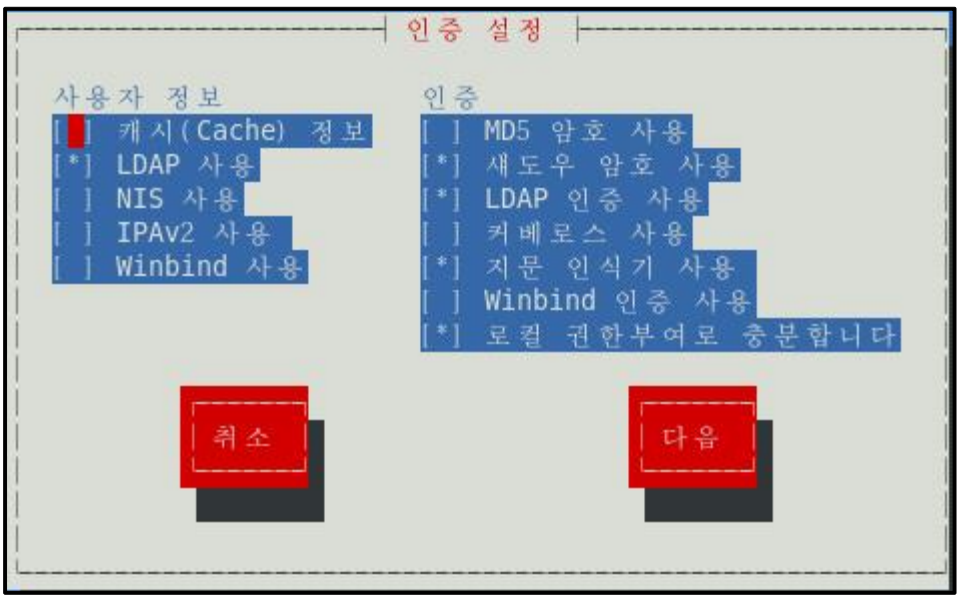
```
objectClass: top
cn: user4
userPassword:: e2NyeXB0fXg=
gidNumber: 504

# user5, Groups, twostar.com
dn: cn=user5,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user5
userPassword:: e2NyeXB0fXg=
gidNumber: 505

# search result
search: 2
result: 0 Success

# numResponses: 24
# numEntries: 23
```

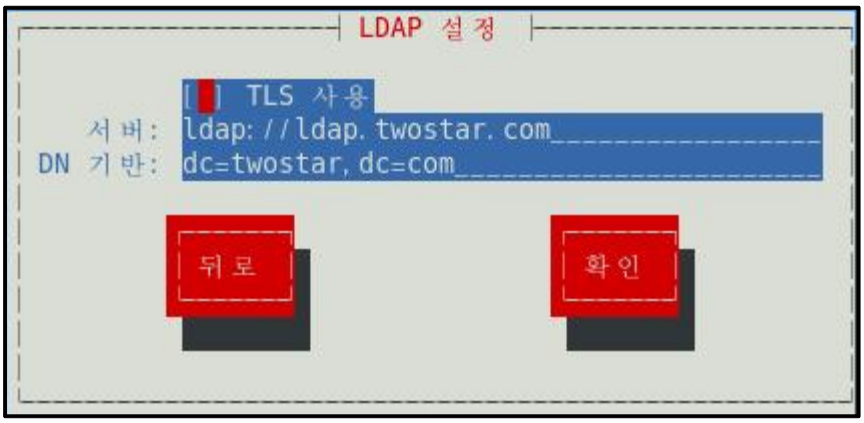
LDAP_Client 설정

authconfig-tui를 통해 ldap 설정을 해준다.

```
[root@client ~]# authconfig-tui
```

LDAP 사용을 체크 했으며 섀도우 암호 사용, LDAP 인증사용을 체크해 주었다.






```
[root@client ~]# authconfig-tui
sssd (을)를 시작 중:                                    [  OK  ]
```

이로서, Client 상에서 LDAP_server안의 계정을 검색 및 확인을 해보겠다.
user1~user5 계정을 확인해 볼 수 있다.

```
[root@client ~]# ldapsearch -x -b "dc=twostar,dc=com"
# extended LDIF
#
# LDAPv3
# base <dc=twostar,dc=com> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# twostar.com
dn: dc=twostar,dc=com
dc: twostar
objectClass: top
objectClass: domain
objectClass: domainRelatedObject
associatedDomain: twostar.com

# Hosts, twostar.com
dn: ou=Hosts,dc=twostar,dc=com
ou: Hosts
objectClass: top
objectClass: organizationalUnit
objectClass: domainRelatedObject
associatedDomain: twostar.com
```

중간생략..

```
# user1, Groups, twostar.com
dn: cn=user1,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user1
userPassword:: e2NyeXB0fXg=
gidNumber: 501

# user2, Groups, twostar.com
dn: cn=user2,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user2
userPassword:: e2NyeXB0fXg=
gidNumber: 502

# user3, Groups, twostar.com
dn: cn=user3,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user3
userPassword:: e2NyeXB0fXg=
gidNumber: 503

# user4, Groups, twostar.com
dn: cn=user4,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
```

```
objectClass: top
cn: user4
userPassword:: e2NyeXB0fXg=
gidNumber: 504

# user5, Groups, twostar.com
dn: cn=user5,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user5
userPassword:: e2NyeXB0fXg=
gidNumber: 505

# search result
search: 2
result: 0 Success

# numResponses: 24
# numEntries: 23
[root@client ~]#
```

로컬상 passwd 파일과 shadow 파일 안에 user1, user2 계정을 찾을 수 없는 것을 확인 할 수 있다.
getent passwd 명령을 통해 시스템에 등록된 사용자 목록(passwd 파일과 같이)을 보는 기능이 있으며, 다른 인증 수단에 등록된 정보도 같이 볼 수 있다.
그러므로 getent 명령으로 user1과 user2 계정을 확인 할 수 있다.

```
[root@client ~]# grep user1 /etc/passwd /etc/shadow
[root@client ~]# grep user2 /etc/passwd /etc/shadow
[root@client ~]# getent passwd user1
user1:*:501:501:user1:/home/ldap/user1:/bin/bash
[root@client ~]# getent passwd user2
user2:*:502:502:user2:/home/ldap/user2:/bin/bash
```

```
[root@client ~]# getent group user1
user1:*:501:
[root@client ~]# getent group user2
user2:*:502:
```

계정 변경인 su 명령어를 통해 user1 으로 로그인을 화면을 확인 할 수 있다.

```
[root@client ~]# su - user1
su: warning: cannot change directory to /home/ldap/user1: 그런 파일이나 디렉터리가 없습니다
-bash-4.1$ exit
logout
```

3,3 홈 디렉터리 자동 생성

홈디렉토리를 자동 생성 해주기 위해서

ldap_server 상에서

/etc/exports 내용안에 아래와 같이 작성을 해준다.

```
/home/ldap      192.168.123.0/255.255.255.0(rw,sync)
```

파일 공유 시스템을 시작해 주며 chkconifg nfs on의 명령을 씀으로서 자동 시작을 해준다.

```
[root@ldap ldap]# service nfs start
NFS 서비스를 시작하고 있습니다:                            [  OK  ]
NFS 쿼터를 시작하고 있습니다:                              [  OK  ]
NFS mountd를 시작중 입니다.                                [  OK  ]
NFS 데몬을 시작함:                                         [  OK  ]
RPC idmapd를 시작 중:                                      [  OK  ]
[root@ldap ldap]# chkconfig nfs on
```

showmount 명령을 통해 exports 파일 내용을 확인 할 수 있다.

```
[root@ldap ldap]# showmount -e ldap.twostar.com
Export list for ldap.twostar.com:
/home/ldap 192.168.123.0/255.255.255.0
```

Client에서

/etc/auto.master 내용 안에 추가 시켜준다.

```
/misc   /etc/auto.misc
/home/ldap      /etc/auto.ldap
```

/etc/auto.ldap 내용 안에 추가 시키며

```
*       -rw     ldap.twostar.com:/home/ldap/&
```

autofs을 실행시켜준다.

```
[root@client ~]# service autofs start
automount (을)를 시작 중: automount: program is already running.
                                                           [  OK  ]
[root@client ~]# service autofs restart
automount 를 정지 중:                                      [  OK  ]
automount (을)를 시작 중:                                  [  OK  ]
```

홈디렉토리 자동생성 전

```
[root@client ~]# ls /home
CSe  lost+found
```

홈디렉토리 자동생성 완료

```
[root@client ~]# su - user1
[user1@client ~]$ exit
logout
[root@client ~]# ls /home/ldap/
user1
```

ldap_server의 계정인 user2 ~ user5 까지 로그인 확인 할 수 있으며 홈 디렉토리가 자동적으로 생성 되는 것을 확인 할 수 있다.

```
[root@client ~]# su - user2
[user2@client ~]$ logout
[root@client ~]# su - user3
[user3@client ~]$ logout
[root@client ~]# su - user4
[user4@client ~]$ logout
[root@client ~]# su - user5
[user5@client ~]$ logout
[root@client ~]# ls /home/ldap
user1  user2  user3  user4  user5
```

3.4 phpLDAPadmin 설치 및 구동

yum을 이용해 아래와 같이 설치해준다.

```
yum install -y php php-cli php-common php-ldap
```

```
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: centos-hcm.viettelidc.com.vn
 * epel: buaya.klas.or.id
 * extras: centos-hcm.viettelidc.com.vn
 * rpmforge: mirror.smartmedia.net.id
 * updates: centos-hcm.viettelidc.com.vn
Setting up Install Process
Package php-cli-5.3.3-27.el6_5.i686 already installed and latest version
Package php-common-5.3.3-27.el6_5.i686 already installed and latest version
Package php-ldap-5.3.3-27.el6_5.i686 already installed and latest version
Nothing to do
```

wget 명령을 통해 아래와 같은 사이트 주소를 입력해 epel-realease-6-8.noarch.rpm파일을 다운로드 하였으며, yum 명령 설치방법이 아닌 rpm -Uvh 명령을 통해 설치를 해주었다.

```
[root@ldap tmp]# rpm -Uvh epel-release-6-8.noarch.rpm
경고: epel-release-6-8.noarch.rpm: Header V3 RSA/SHA256 Signature, key ID 0608b8
95: NOKEY
준비 중...                ########################################### [100%]
   1:epel-release           ########################################### [100%]
[root@ldap tmp]#
[root@ldap tmp]#
[root@ldap tmp]#
[root@ldap tmp]# yum --enablerepo=epel -y install phpldapadmin
```

```
[root@ldap tmp]# wget http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-release
-6-8.noarch.rpm
--2015-05-04 02:32:52--  http://dl.fedoraproject.org/pub/epel/6/x86_64/epel-rele
ase-6-8.noarch.rpm
Resolving dl.fedoraproject.org... 209.132.181.26, 209.132.181.27, 209.132.181.24
, ...
Connecting to dl.fedoraproject.org|209.132.181.26|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 14540 (14K) [application/x-rpm]
Saving to: `epel-release-6-8.noarch.rpm'

100%[======================================>] 14,540      --.-K/s   in 0.1s

2015-05-04 02:32:53 (108 KB/s) - `epel-release-6-8.noarch.rpm' saved [14540/1454
0]

[root@ldap tmp]#
[root@ldap tmp]#
[root@ldap tmp]# ls
epel-release-6-8.noarch.rpm  orbit-gdm            virtual-AnAn.PBzc2i
```

```
================================================================================
 Package             Arch          Version                 Repository      Size
================================================================================
Installing:
 phpldapadmin        noarch        1.2.3-1.el6             epel           806 k
Installing for dependencies:
 php                 x86_64        5.3.3-40.el6_6          updates        1.1 M

Transaction Summary
================================================================================
Install       2 Package(s)

Total download size: 1.9 M
Installed size: 5.9 M
Downloading Packages:
(1/2): php-5.3.3-40.el6_6.x86_64.rpm                     | 1.1 MB     00:00
(2/2): phpldapadmin-1.2.3-1.el6.noarch.rpm               | 806 kB     00:00
--------------------------------------------------------------------------------
Total                                           2.2 MB/s | 1.9 MB     00:00
warning: rpmts_HdrFromFdno: Header V3 RSA/SHA256 Signature, key ID 0608b895: NOK
EY
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-EPEL-6
Importing GPG key 0x0608B895:
 Userid : EPEL (6) <epel@fedoraproject.org>
 Package: epel-release-6-8.noarch (installed)
```

```
Installed:
  phpldapadmin.noarch 0:1.2.3-1.el6

Dependency Installed:
  php.x86_64 0:5.3.3-40.el6_6

Complete!
```

설치 후

/etc/phpldapadmin/config.php 안에 파일 내용을 아래와 같이 수정해 준다.

```
397 $servers->setValue('login','attr','dn');
398 //$servers->setValue('login','attr','uid');
```

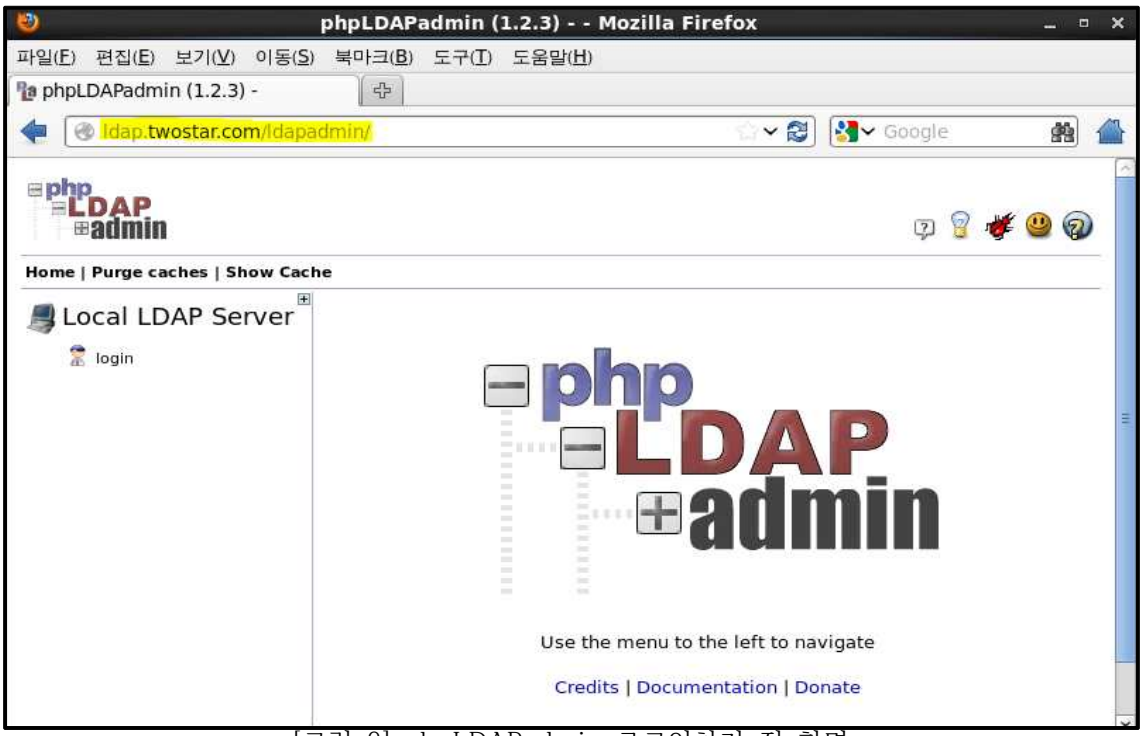
/etc/httpd/conf.d/phpldapadmin.conf 안에 파일 내용을 아래와 같이 192.168.123.0/24를 추가 시켜준다.

```
 1 #
 2 #  Web-based tool for managing LDAP servers
 3 #
 4
 5 Alias /phpldapadmin /usr/share/phpldapadmin/htdocs
 6 Alias /ldapadmin /usr/share/phpldapadmin/htdocs
 7
 8 <Directory /usr/share/phpldapadmin/htdocs>
 9   Order Deny,Allow
10   Deny from all
11   Allow from 127.0.0.1 192.168.123.0/24
12   Allow from ::1
13 </Directory>
14
```

설정후 httpd 재시작을 실행시킨다.

```
[root@ldap ~]# service httpd restart
httpd 를 정지 중:                                          [  OK  ]
httpd (을)를 시작 중:                                      [  OK  ]
```

주소창에 ldap.twostar.com/ldapadmin/ 이라고 친 상태이며 phpldapadmin 창이 나타나는 것을 확인 할 수 있다.

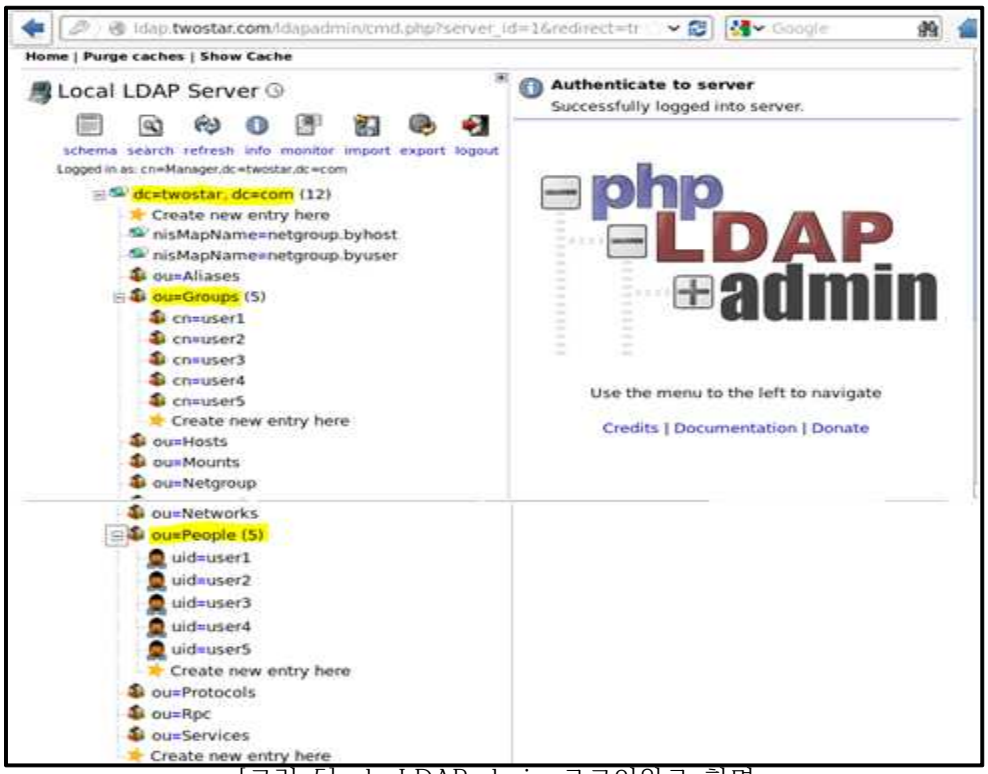


[그림 3] phpLDAPadmin 로그인하기 전 화면

[그림 3]을 봤을 때 로그인하려는 화면이며 계정과 패스워드를 적어준 화면이다.

[그림 4] phpLDAPadmin 로그인하는 화면

[그림 4]를 봤을 때, 계정 아이디 : cn=Manager,dc=twostar,dc=com (도메인 주소)
Password : ******** (처음 slappasswd 로 설정해준 패스워드이다)



[그림 5] phpLDAPadmin 로그인완료 화면

[그림 5]를 봤을 때 로그인을 하고 난 후 화면이며 Groups 와 People 안에 user1~user5의 계정이 있는 것을 확인 할 수 있다.

3.5 TLS보안향상

TLS(Transport Layer Security)란?

TLS는 클라이언트/서버 응용 프로그램이 네트워크로 통신을 하는 과정에서 도청, 간섭, 위조를 방지하기 위해서 설계되었다. 그리고 암호화를 해서 최종 단의 인증, 통신 기밀성을 유지시켜준다.
트랜스포트 레이어 보안 (TLS)과 보안 소켓 레이어 (SSL)는 암호 규약이다. 그리고 '트랜스포트 레이어 보안'이라는 이름은 '보안 소켓 레이어'가 표준화 되면서 바뀐 이름이다. 이 규약은 인터넷 같이 TCP/IP 네트워크를 사용하는 통신에 적용되며, 통신 과정에서 전송계층 종단간 보안과 데이터 무결성을 확보해준다.

자가 서명 인증서(Self-Signed Certificate) 생성

자가서명 인증서를 생성 해주면 twostarkey.pem와 twostar,pem 파일이 생성 된다.

```
[root@ldap certs]# openssl req -new -x509 -nodes -out /etc/pki/tls/certs/twostar
.pem -keyout /etc/pki/tls/certs/twostarkey.pem -days 365
Generating a 2048 bit RSA private key
.....................................................................+++
.....................................................................................
.....+++
writing new private key to '/etc/pki/tls/certs/twostarkey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:KR
State or Province Name (full name) []:Seoul
Locality Name (eg, city) [Default City]:Seoul
Organization Name (eg, company) [Default Company Ltd]:knowledgepia
Organizational Unit Name (eg, section) []:IT
Common Name (eg, your name or your server's hostname) []:ldap.twostar.com
Email Address []:star222039@gmail.com
[root@ldap certs]# ls
Makefile        ca-bundle.trust.crt  renew-dummy-cert  twostarkey.pem
ca-bundle.crt   make-dummy-cert      twostar.pem
```

두 개의 파일을 chown 명령을 써서 소유주와 소유그룹을 변경 시켜준다.

```
[root@ldap certs]# chown root.ldap twostar*
[root@ldap certs]#
[root@ldap certs]# ll twostar*
-rw-r--r--. 1 root ldap 1436 2015-05-05 23:06 twostar.pem
-rw-r--r--. 1 root ldap 1704 2015-05-05 23:06 twostarkey.pem
```

소유권을 변경후 twostar.pem 파일을 ftp폴더인 공용폴더 pub디렉터리에 복사를 해준다.

```
[root@ldap certs]# cp twostar.pem /var/ftp/pub/
```

Client에서 ncftp를 이용해 서버에서의 twostar.pem을 내려받기 한다.

```
NcFTP 3.2.4 (Apr 07, 2010) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 192.168.123.143...
(vsFTPd 2.2.2)
Logging in...
Login successful.
Logged in to ldap.
ncftp / > ls
pub/
ncftp / > ll
drwxr-xr-x    2 0        0            4096    5월  5 14:13   pub
ncftp / > cd /pub
Directory successfully changed.
ncftp /pub > ls
twostar.pem
ncftp /pub > get twostar.pem
```

서버로부터 내려 받아 진 것을 확인 할 수 있다.

```
[root@client cacerts]# ls
twostar.pem
```

twostar.pem 의 내용인 인증서 내용이다.

cat twostar.pem

```
MIID9zCCAt+gAwIBAgIJANV4FuPdH0+0MA0GCSqGSIb3DQEBBQUAMIGRMQswCQYD
VQQGEwJLUjEOMAwGA1UECAwFU2VvdWwxDjAMBgNVBAcMBVNlb3VsMRUwEwYDVQQK
DAxrbm93bGVkZ2VwaWExCzAJBgNVBAsMAklUMRkwFwYDVQQDDBBsZGFwLnR3b3N0
YXIuY29tMSMwIQYJKoZIhvcNAQkBFhRzdGFyMjIyMDM5QGdtYWlsLmNvbTAeFw0x
NTA1MDUxNDA2NDJaFw0xNjA1MDQxNDA2NDJaMIGRMQswCQYDVQQGEwJLUjEOMAwG
A1UECAwFU2VvdWwxDjAMBgNVBAcMBVNlb3VsMRUwEwYDVQQKDAxrbm93bGVkZ2Vw
aWExCzAJBgNVBAsMAklUMRkwFwYDVQQDDBBsZGFwLnR3b3N0YXIuY29tMSMwIQYJ
KoZIhvcNAQkBFhRzdGFyMjIyMDM5QGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANeG48PGja1jxaTecYk6xBufX+A5maPeypZgCvkXWrAF
LM4War4k3ohHPzjcpqDZdTMxxumH67vXEq7zeHJEFJQx3af2FVVqNSswqraDP7Ht
/sU9Oqa0WXCetm16Ehexe8aJVy+/MnZK12urbkkb5+ICEVUm/JmvWsJRzG0HVaFZ
owcmW/P//YJIFiB0dKLb0YjtbGyvNPYm1vROJ+G/g4hmHTj+OXD6GPfGtvRP4d7d
5jAAfJ/t8SvBd6U+0GjHfcTMqRwQ91jUFFxPRhfsiaSesSaMuNmC6vJfn+i9y35b
21NVJKJpxOQq4fLkQiWBj2ic8KfegSIiPS1DxJKUuzMCAwEAAaNQME4wHQYDVR0O
BBYEFKS2pSyQ0QOHdozQBNVEL3aPzyS6MB8GA1UdIwQYMBaAFKS2pSyQ0QOHdozQ
BNVEL3aPzyS6MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAM/lR4XU
2KUWvm8kBGamt2G12D80WmCgwi6fxpyH1PDTHqcQDt6a3MFT/EJXmk1Fw8iGJ7vT
ydHkHjLw1/ysMxK+D30rR4jUBTf+MDjOooM0Qoe3g/r1xN5qa6QuLlqA6545oW/8
ZZSIxaIaMBW/yXeYTXgbrkbmT32zYy+SlFU+COyCFqnaqHf2K0hpXzYhaMGhlBGC
SonqSDDrjIlGUNjUtxl+baJ6onDOD613U0wSErrMHC/DvNuiZltT4G4fVWSKsbqY
yhakZesQMCwJP5+dKqoIaLO95Kqz+Rz/9hG3m8g2Z4uH7cjwWKEssVe9HookgJJ0
VvhWJ6jAnTWSJvU=
-----END CERTIFICATE-----
```

/etc/openldap/ldap.conf

의 파일 내용안에 TLS_REQCERT allow 문장을 추가 시켜주었다.

```
TLS_CACERTDIR /etc/openldap/cacerts
TLS_REQCERT allow
URI ldaps://ldap.twostar.com
BASE dc=twostar,dc=com
```

3.6 LDAP_Kerberos Server 설치 및 구축

ldap서버 시스템에 kerberos 서버를 같이 구동

yum을 이용해 아래와 같이 명령을 줘서 설치를 한다.

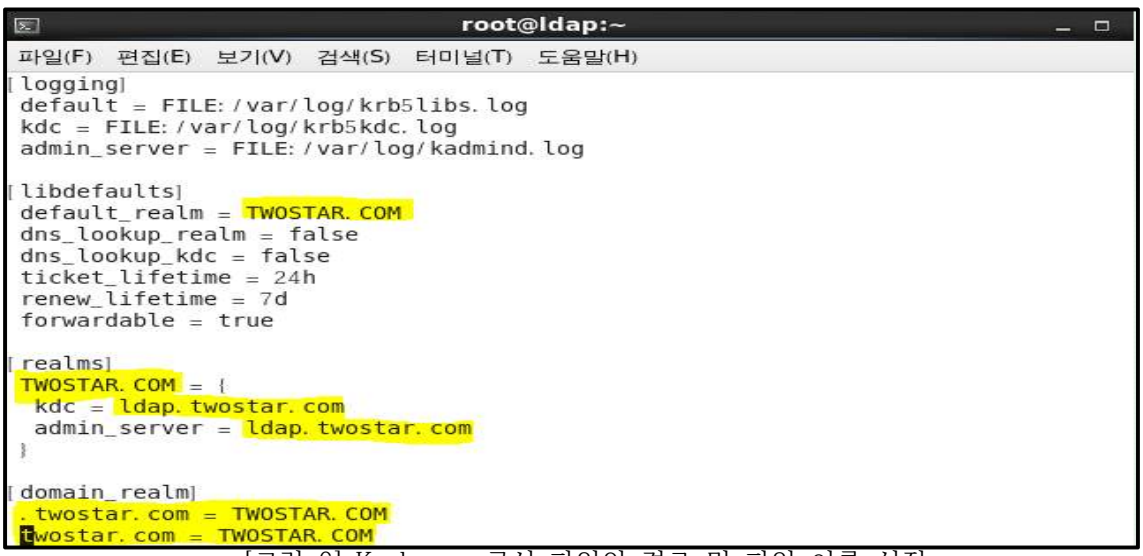
```
yum install -y krb5-server-ldap krb5-appl-servers krb5-server krb5-workstation
krb5-libs
```

설치 완료 후 rpm 명령으로 krb5*를 설치 완료 항목을 확인 할 수 있다.

```
[root@ldap ~]# rpm -qa krb5*
krb5-server-ldap-1.10.3-37.el6_6.x86_64
krb5-appl-servers-1.0.1-7.el6_2.1.x86_64
krb5-server-1.10.3-37.el6_6.x86_64
krb5-workstation-1.10.3-37.el6_6.x86_64
krb5-libs-1.10.3-37.el6_6.x86_64
```

LDAP_Kerberos Sever 설정

/etc/krb5.conf 내용 안에
아래와 같이 설정을 해준다. 아래와 같은 설정은 서버의 도메인 주소를 적어주면 되며 대문자 소문자 구별에 주의 해야 한다.



[그림 6] Kerberos 구성 파일의 경로 및 파일 이름 설정

/var/kerberos/krb5kdc/kadm5.acl 내용안에 admin 설정을 해준다.

```
*/admin@TWOSTAR.COM      *
```

/var/kerberos/krb5kdc/kdc.conf 내용 안에 도메인주소를 적어준다.

[그림 7] kdc.conf 내용 안에 도메인 주소 설정

설정을 다 한 후 krb5 서비스를 재시작 해준다.

```
[root@ldap krb5kdc]# /etc/init.d/krb5kdc restart
Kerberos 5 KDC 를 정지 중:                                  [실패]
Kerberos 5 KDC (을)를 시작 중:                              [  OK  ]
```

chkconfig krb5kdc on 명령을 줘서 자동 서비스 시작 되도록 설정한다.

Kerberos 사용자 추가

kadmin.local에 접속하여 listprincs 명령으로 principal(사용자) 리스트를 볼 수 있으며 addprinc명령으로 user1@TWOSTAR.COM을 추가 하는 것을 볼 수 있다.

```
[root@ldap krb5kdc]# kadmin.local
Authenticating as principal root/admin@TWOSTAR.COM with password.
kadmin.local:  listprincs
K/M@TWOSTAR.COM
kadmin/admin@TWOSTAR.COM
kadmin/changepw@TWOSTAR.COM
kadmin/ldap.twostar.com@TWOSTAR.COM
krbtgt/TWOSTAR.COM@TWOSTAR.COM
kadmin.local:  addprinc user1@TWOSTAR.COM
WARNING: no policy specified for user1@TWOSTAR.COM; defaulting to no policy
Enter password for principal "user1@TWOSTAR.COM":
Re-enter password for principal "user1@TWOSTAR.COM":
Principal "user1@TWOSTAR.COM" created.
kadmin.local:
kadmin.local:  quit
```

위와 마찬가지로 addprinc명령으로 root/admin@TWOSTAR.COM을 추가한 화면이다.

```
[root@ldap krb5kdc]# kadmin.local
Authenticating as principal root/admin@TWOSTAR.COM with password.
kadmin.local:
kadmin.local:   addprinc root/admin
WARNING: no policy specified for root/admin@TWOSTAR.COM; defaulting to no policy
Enter password for principal "root/admin@TWOSTAR.COM":
Re-enter password for principal "root/admin@TWOSTAR.COM":
Principal "root/admin@TWOSTAR.COM" created.
kadmin.local:
kadmin.local:
kadmin.local:   listprincs
K/M@TWOSTAR.COM
kadmin/admin@TWOSTAR.COM
kadmin/changepw@TWOSTAR.COM
kadmin/ldap.twostar.com@TWOSTAR.COM
krbtgt/TWOSTAR.COM@TWOSTAR.COM
root/admin@TWOSTAR.COM
user1@TWOSTAR.COM
kadmin.local:
```

ktadd 명령으로 Keytab kadmin/admin의 정보를 kadm5.keytab에 추가

```
kadmin.local:  ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/admin
Entry for principal kadmin/admin with kvno 3, encryption type aes256-cts-hmac-sh
a1-96 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type aes128-cts-hmac-sh
a1-96 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type des3-cbc-sha1 adde
d to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type arcfour-hmac added
 to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type des-hmac-sha1 adde
d to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/admin with kvno 3, encryption type des-cbc-md5 added
to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
kadmin.local:
```

ktadd 명령으로 kadmin/changepw의 정보를 kadm5.keytab에 추가

```
kadmin.local:  ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encryption type aes256-cts-hmac
-sha1-96 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type aes128-cts-hmac
-sha1-96 added to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type des3-cbc-sha1 a
dded to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type arcfour-hmac ad
ded to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type des-hmac-sha1 a
dded to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
Entry for principal kadmin/changepw with kvno 3, encryption type des-cbc-md5 add
ed to keytab WRFILE:/var/kerberos/krb5kdc/kadm5.keytab.
kadmin.local:
```

kerberos_ host/ldap.twostar.com 사용자 추가 화면이다

```
kadmin.local:  addprinc -randkey host/ldap.twostar.com
WARNING: no policy specified for host/ldap.twostar.com@TWOSTAR.COM; defaulting t
o no policy
Principal "host/ldap.twostar.com@TWOSTAR.COM" created.
kadmin.local:
```

ktadd 명령으로 host/ldap.twostar.com 의 사용자정보를 kadm5.keytab에 추가 화면이다.

```
kadmin.local:  ktadd -k /etc/krb5.keytab host/ldap.twostar.com
Entry for principal host/ldap.twostar.com with kvno 2, encryption type aes256-ct
s-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type aes128-ct
s-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des3-cbc-
sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type arcfour-h
mac added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des-hmac-
sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des-cbc-m
d5 added to keytab WRFILE:/etc/krb5.keytab.
kadmin.local:
```

krb5kdc과 kadmin를 재시작 하며 프로세스에서도 확인 할 수 있는 화면이다.

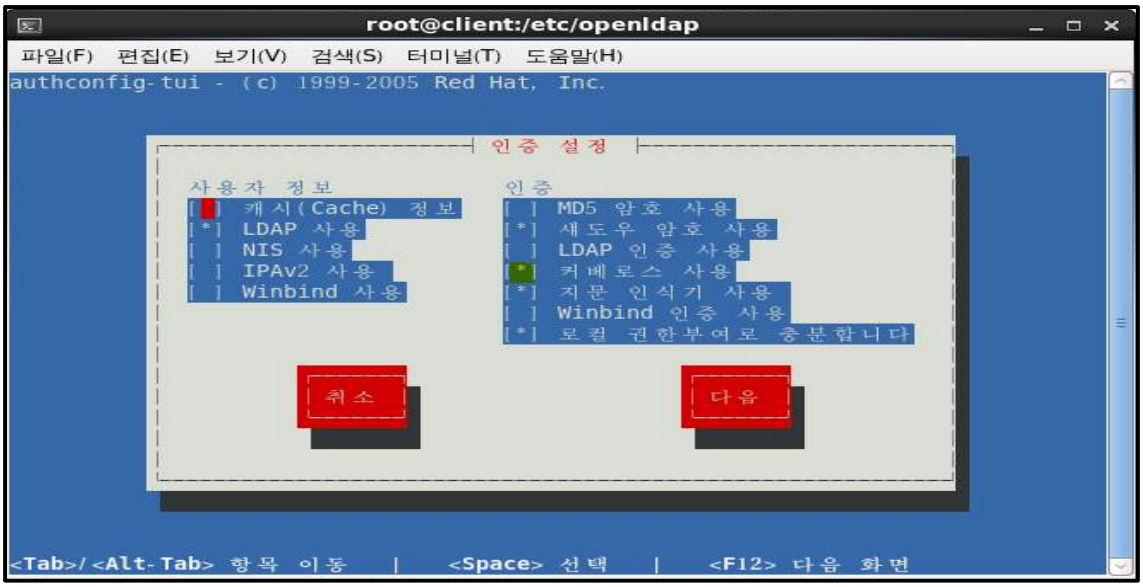
```
[root@ldap krb5kdc]# service krb5kdc restart
Kerberos 5 KDC 를 정지 중:                                 [  OK  ]
Kerberos 5 KDC (을)를 시작 중:                             [  OK  ]
[root@ldap krb5kdc]# service kadmin restart
Kerberos 5 Admin Server 를 정지 중:                        [실패]
Kerberos 5 Admin Server (을)를 시작 중:                    [  OK  ]
[root@ldap krb5kdc]# ps -ef |grep krb5
root     13542     1 21 05:17 ?        00:00:04 /usr/sbin/krb5kdc -P /var/run/kr
b5kdc.pid
root     13566 11483  4 05:17 pts/1    00:00:00 grep krb5
[root@ldap krb5kdc]# ps -ef |grep kadmin
root     13563     1  0 05:17 ?        00:00:00 /usr/sbin/kadmind -P /var/run/ka
dmind.pid
root     13568 11483  0 05:17 pts/1    00:00:00 grep kadmin
[root@ldap krb5kdc]# netstat -nat | grep 88
tcp        0      0 0.0.0.0:88                  0.0.0.0:*                   LIST
EN
tcp        0      0 :::88                       :::*                        LIST
EN
tcp        0      0 :::38884                    :::*                        LIST
EN
[root@ldap krb5kdc]# netstat -nat | grep 749
tcp        0      0 0.0.0.0:749                 0.0.0.0:*                   LIST
EN
tcp        0      0 :::749                      :::*                        LIST
EN
[root@ldap krb5kdc]#
```

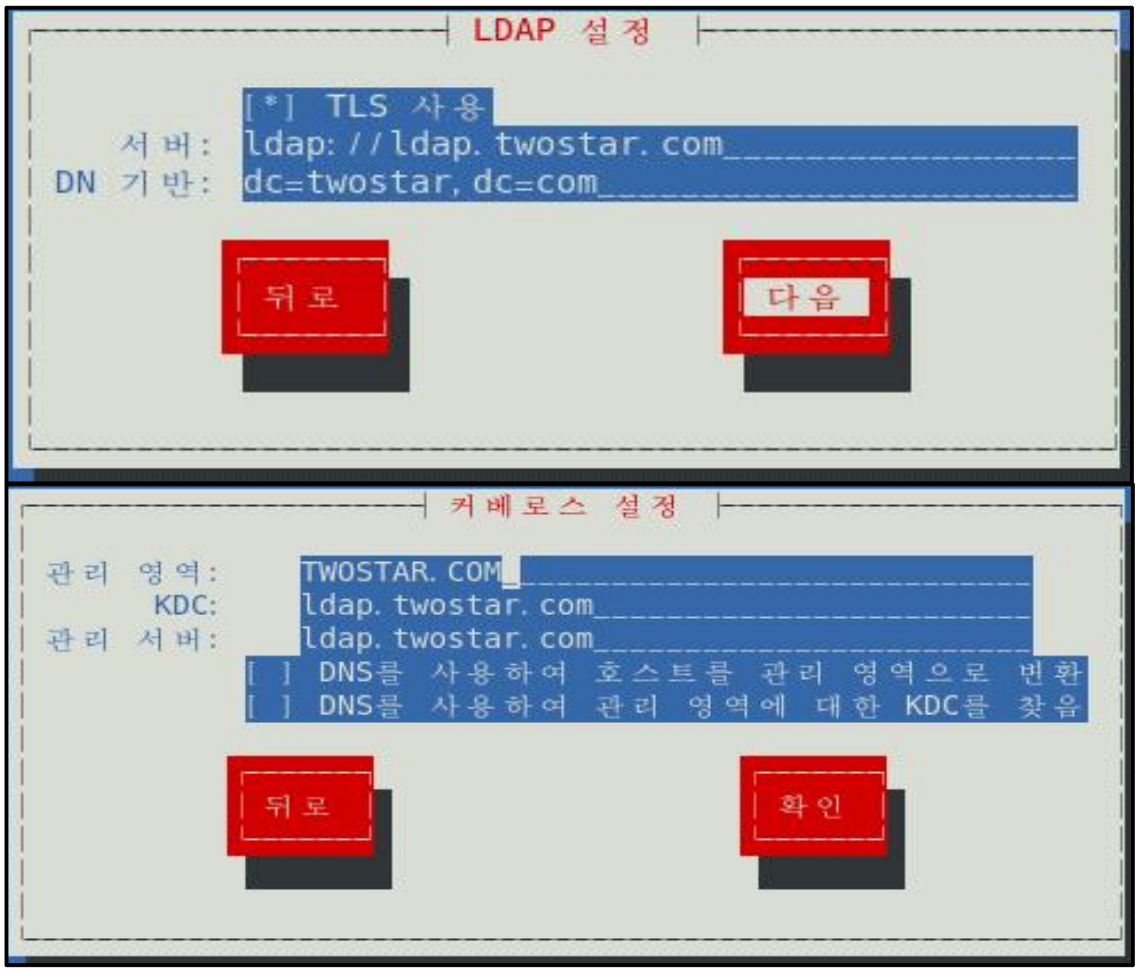
ktutil을 통해 principal 의 리스트를 확인 할 수 있다.

```
[root@ldap krb5kdc]# ktutil
ktutil:  rkt /var/kerberos/krb5kdc/kadm5.keytab
ktutil:  list
slot KVNO Principal
---- ---- ---------------------------------------------------------------------
   1    3                 kadmin/admin@TWOSTAR.COM
   2    3                 kadmin/admin@TWOSTAR.COM
   3    3                 kadmin/admin@TWOSTAR.COM
   4    3                 kadmin/admin@TWOSTAR.COM
   5    3                 kadmin/admin@TWOSTAR.COM
   6    3                 kadmin/admin@TWOSTAR.COM
   7    3              kadmin/changepw@TWOSTAR.COM
   8    3              kadmin/changepw@TWOSTAR.COM
   9    3              kadmin/changepw@TWOSTAR.COM
  10    3              kadmin/changepw@TWOSTAR.COM
  11    3              kadmin/changepw@TWOSTAR.COM
  12    3              kadmin/changepw@TWOSTAR.COM
ktutil:
```

3.7 LDAP_kerberos Client 설정 및 티켓 부여

LDAP_kerberos Client 설정 (authconfig-tui)





Kerberos Client 상에서

ldap서버에서의 krb5.conf 파일을 Client 로 옮기는 화면이다.

```
[root@client etc]# scp root@ldap:/etc/krb5.conf /etc/krb5.conf
The authenticity of host 'ldap (192.168.123.143)' can't be established.
RSA key fingerprint is 63:a9:2e:10:d5:65:9d:61:3e:5d:8f:2b:aa:7e:84:c7.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ldap,192.168.123.143' (RSA) to the list of known hos
ts.
root@ldap's password:
krb5.conf                                     100%  441     0.4KB/s   00:00
[root@client etc]# ls /etc/krb5.conf
/etc/krb5.conf
```

kadmin 명령을 통해 root/admin 에 접속을 해서 host/client.twostar.com 사용자를 추가 시키는 화면과 keytab의 항목에 추가 시키는 화면이다.

```
[root@client etc]# kadmin -p root/admin
Authenticating as principal root/admin with password.
Password for root/admin@TWOSTAR.COM:
kadmin:  addprinc -randkey host/client.twostar.com
WARNING: no policy specified for host/client.twostar.com@TWOSTAR.COM; defaulting
 to no policy
Principal "host/client.twostar.com@TWOSTAR.COM" created.
kadmin:
kadmin:  ktadd -k /etc/krb5.keytab host/client.twostar.com
Entry for principal host/client.twostar.com with kvno 2, encryption type aes256-
cts-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/client.twostar.com with kvno 2, encryption type aes128-
cts-hmac-sha1-96 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/client.twostar.com with kvno 2, encryption type des3-cb
c-sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/client.twostar.com with kvno 2, encryption type arcfour
-hmac added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/client.twostar.com with kvno 2, encryption type des-hma
c-sha1 added to keytab WRFILE:/etc/krb5.keytab.
Entry for principal host/client.twostar.com with kvno 2, encryption type des-cbc
-md5 added to keytab WRFILE:/etc/krb5.keytab.
kadmin:
```

전송 가능 티켓 부여 티켓(TGT)

kinit 명령을 사용함으로써 전송 가능 티켓 부여 티켓(TGT)를 얻게 된 화면이며 시작기간 및 시간(Valid starting)과 만료일(Expires) 서비스 사용자(Service principal)을 확인할 수 있다.

```
[root@ldap ~]# su - user1
[user1@ldap ~]$ klist
klist: No credentials cache found (ticket cache FILE:/tmp/krb5cc_501)
[user1@ldap ~]$
[user1@ldap ~]$
[user1@ldap ~]$ kinit
Password for user1@TWOSTAR.COM:
[user1@ldap ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_501
Default principal: user1@TWOSTAR.COM

Valid starting     Expires            Service principal
05/13/15 12:53:43  05/14/15 12:53:43  krbtgt/TWOSTAR.COM@TWOSTAR.COM
        renew until 05/13/15 12:53:43
[user1@ldap ~]$ ssh user1@client
The authenticity of host 'client (192.168.123.144)' can't be established.
RSA key fingerprint is 13:b4:6a:18:bf:6e:7c:e1:3e:f4:18:82:33:80:92:a2.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'client,192.168.123.144' (RSA) to the list of known h
osts.
Last login: Tue May 12 21:25:50 2015
[user1@client ~]$
```

3,8 LDAP_Kerberos 응용서버 설치 및 구축

Kerberos 응용서버인 SSH, FTP서버

Kerberos 응용 서버 설치

```
yum install -y krb-libs krb5-workstation krb5-devel krb5-appl-clients krb5-appl-servers krb5-server
```

```
[root@centos6 ~]# rpm -qa krb*
krb5-libs-1.10.3-37.el6_6.x86_64
krb5-workstation-1.10.3-37.el6_6.x86_64
krb5-devel-1.10.3-37.el6_6.x86_64
krb5-appl-clients-1.0.1-7.el6_2.1.x86_64
krb5-appl-servers-1.0.1-7.el6_2.1.x86_64
krb5-server-1.10.3-37.el6_6.x86_64
```

yum을 이용하여 설치 해준다.

```
yum install -y nss-pam-ldapd
```

```
[root@centos@twostar ~]# yum install -y nss-pam-ldapd
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base: ftp.kaist.ac.kr
 * extras: ftp.kaist.ac.kr
 * updates: ftp.kaist.ac.kr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package nss-pam-ldapd.x86_64 0:0.7.5-20.el6_6.3 will be installed
base/filelists_db                                        | 6.1 MB     00:02

Installed:
  nss-pam-ldapd.x86_64 0:0.7.5-20.el6_6.3

Dependency Installed:
  nscd.x86_64 0:2.12-1.149.el6_6.7          pam_ldap.x86_64 0:185-11.el6

Dependency Updated:
  glibc.i686 0:2.12-1.149.el6_6.7
  glibc.x86_64 0:2.12-1.149.el6_6.7
  glibc-common.x86_64 0:2.12-1.149.el6_6.7
  glibc-devel.x86_64 0:2.12-1.149.el6_6.7
  glibc-headers.x86_64 0:2.12-1.149.el6_6.7

Complete!
```

Kerberos 연동 서버 TLS 보안 향상 설정

```
[root@centos6 cacerts]# ncftp ldap
NcFTP 3.2.4 (Apr 07, 2010) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 192.168.123.143...
(vsFTPd 2.2.2)
Logging in...
Login successful.
Logged in to ldap.
ncftp / > ls
pub/
ncftp / > ll
drwxr-xr-x    2 0        0            4096    5월  5 14:13   pub
ncftp / > cd pub
Directory successfully changed.
ncftp /pub > ls
twostar.pem
ncftp /pub > get twostar.pem
twostar.pem:                                          1.40 kB   15.48 kB/s
ncftp /pub >
ncftp /pub >
Interrupted.
[root@centos6 cacerts]#
```

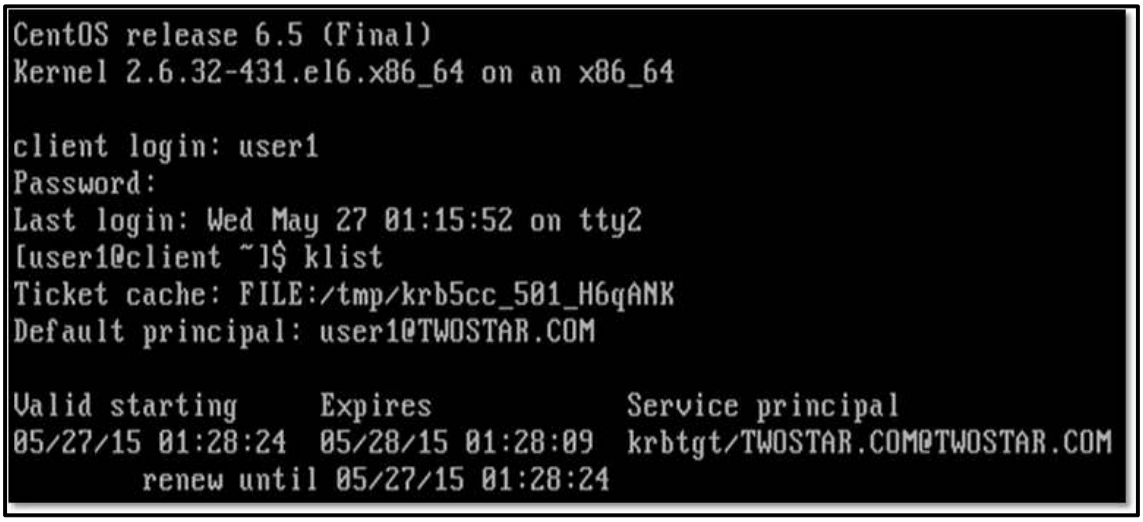
Client 설정할 때와 같이 TLS 보안 설정을 해준다.

Client에서 말했듯이 인증서 확인 부분이다.

```
[root@centos6 cacerts]# ls
582d8cf0.0  twostar.pem
[root@centos6 cacerts]# cat twostar.pem
-----BEGIN CERTIFICATE-----
MIID9zCCAt+gAwIBAgIJANV4FuPdH0+0MA0GCSqGSIb3DQEBBQUAMIGRMQswCQYD
VQQGEwJLUjEOMAwGA1UECAwFU2VvdWwxDjAMBgNVBAcMBVNlb3VsMRUwEwYDVQQK
DAxrbm93bGVkZ2VwaWExCzAJBgNVBAsMAklUMRkwFwYDVQQDDBBsZGFwLnR3b3N0
YXIuY29tMSMwIQYJKoZIhvcNAQkBFhRzdGFyMjIyMDM5QGdtYWlsLmNvbTAeFw0x
NTA1MDUxNDA2NDJaFw0xNjA1MDQxNDA2NDJaMIGRMQswCQYDVQQGEwJLUjEOMAwG
A1UECAwFU2VvdWwxDjAMBgNVBAcMBVNlb3VsMRUwEwYDVQQKDAxrbm93bGVkZ2Vw
aWExCzAJBgNVBAsMAklUMRkwFwYDVQQDDBBsZGFwLnR3b3N0YXIuY29tMSMwIQYJ
KoZIhvcNAQkBFhRzdGFyMjIyMDM5QGdtYWlsLmNvbTCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANeG48PGja1jxaTecYk6xBufX+A5maPeypZgCvkXWrAF
LM4War4k3ohHPzjcpqDZdTMxxumH67vXEq7zeHJEFJQx3af2FVVqNSswqraDP7Ht
/sU9Oqa0WXCetm16Ehexe8aJVy+/MnZK12urbkkb5+ICEVUm/JmvWsJRzG0HVaFZ
owcmW/P//YJIFiB0dKLb0YjtbGyvNPYm1vROJ+G/g4hmHTj+OXD6GPfGtvRP4d7d
5jAAfJ/t8SvBd6U+0GjHfcTMqRwQ91jUFFxPRhfsiaSesSaMuNmC6vJfn+i9y35b
21NVJKJpxOQq4fLkQiWBj2ic8KfegSIiPS1DxJKUuzMCAwEAAaNQME4wHQYDVR0O
BBYEFKS2pSyQ0QOHdozQBNVEL3aPzyS6MB8GA1UdIwQYMBaAFKS2pSyQ0QOHdozQ
BNVEL3aPzyS6MAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADggEBAM/lR4XU
2KUWvm8kBGamt2G12D80WmCgwi6fxpyH1PDTHqcQDt6a3MFT/EJXmk1Fw8iGJ7vT
ydHkHjLw1/ysMxK+D30rR4jUBTf+MDjOooM0Qoe3g/r1xN5qa6QuLlqA6545oW/8
ZZSIxaIaMBW/yXeYTXgbrkbmT32zYy+SlFU+COyCFqnaqHf2K0hpXzYhaMGhlBGC
SonqSDDrjIlGUNjUtxl+baJ6onDOD613U0wSErrMHC/DvNuiZltT4G4fVWSKsbqY
yhakZesQMCwJP5+dKqoIaLO95Kqz+Rz/9hG3m8g2Z4uH7cjwWKEssVe9HookgJJ0
VvhWJ6jAnTWSJvU=
-----END CERTIFICATE-----
```

3.9 통합 인증시스템 구현

Client LDAP 계정 로그인 화면



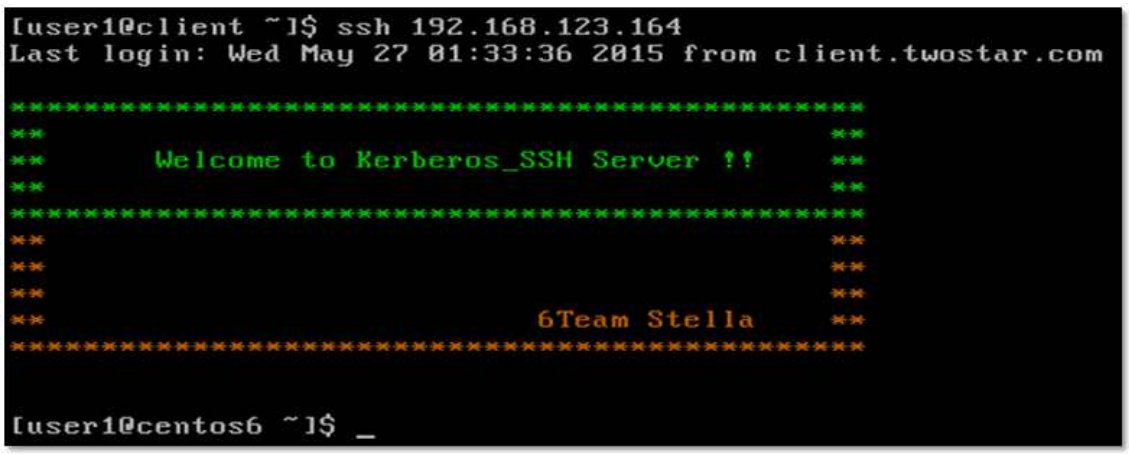
KDC_LDAP 티켓 서비스 화면

ldap서버의 계정 user1이 접속했다고 로그에 남아 있는 상태이다.

```
tail -f /var/log/krb5kdc.log
```

LDAP_Kerberos 연계 서버인_SSH서버 접속

Client 상에서 SSH서버 접속화면이다. 로그인 할 때 패스워드를 입력하지 않고 LDAP서버의 계정으로 접속하는 것을 확인 할 수 있다.



KDC_LDAP 티켓 서버스 화면이다.
user1@TWOSTAR.COM for host/centos6.twostar.com@TWOSTAR.COM 으로 user1으로 접속한 것을 확인 할 수 있는 것이다.

`tail -f /var/log/krb5kdc.log`

```
May 27 01:52:48 ldap.twostar.com krb5kdc[1717](info): TGS_REQ (4 etypes {18 17 16 23}) 192.168.123.144: ISSUE: authtime 1432659152, etypes {rep=18 tkt=18 ses=18}, user1@TWOSTAR.COM for host/centos6.twostar.com@TWOSTAR.COM
```

kerberos인 연동서버인 SSH서버 인증 화면이다. `tail -f /var/log/secure`
kerberos 인증이 됐다는 ok 사인이 나왔으며 ssh 로 인증접속했다는 메시지이다.

```
May 27 01:52:32 centos6 sshd[3527]: Authorized to user1, krb5 principal user1@TWOSTAR.COM (krb5_kuserok)
May 27 01:52:32 centos6 sshd[3527]: Accepted gssapi-with-mic for user1 from 192.168.123.144 port 48797 ssh2
May 27 01:52:32 centos6 sshd[3527]: pam_unix(sshd:session): session opened for user user1 by (uid=0)
```

LDAP_Kerberos 연계 서버인_FTP서버 접속

Client에서 FTP 서버인 192.168.123.164에 접속한 화면이며 인증이 성공적으로 된 것을 확인할 수 있으며

```
[user1@client ~]$ ftp 192.168.123.164
Connected to 192.168.123.164.
220 centos6.twostar.com FTP server (Version 5.60) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded
Name (192.168.123.164:user1): user1
232 GSSAPI user user1@TWOSTAR.COM is authorized as user1
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
```

ftp 서버에서 파일을 가져오는 상황을 볼 수 있는데 정상적으로 작동한다는 것을 확인할 수 있다.

```
ftp> cd /var/ftp/pub
250 CWD command successful.
ftp> ls
227 Entering Passive Mode (192,168,123,164,134,153)
150 Opening ASCII mode data connection for /bin/ls.
total 16
-rw-r--r--. 1 root 7 May 17 05:41 test1
-rw-r--r--. 1 root 6 May 17 05:41 test2
-rw-r--r--. 1 root 6 May 17 05:42 test3
-rw-r--r--. 1 root 6 May 17 05:43 test4
226 Transfer complete.
ftp> get test4
local: test4 remote: test4
227 Entering Passive Mode (192,168,123,164,173,145)
150 Opening BINARY mode data connection for test4 (6 bytes).
226 Transfer complete.
6 bytes received in 0.21 seconds (0.028 Kbytes/s)
ftp> quit
221 Goodbye.
[user1@client ~]$ ls
test4
[user1@client ~]$ _
```

KDC_LDAP 티켓 서비스 화면이다.
user1이 계정이 ftp 서버인 centos6.twostar.com(192.168.123.164)에 접속했다는 확인 메시지이다.

```
May 27 02:04:22 ldap.twostar.com krb5kdc[1717](info): TGS_REQ (4 etypes {18 17 16 23}) 192.168.123.144: ISSUE: authtime 1432659152, etypes {rep=18 tkt=18 ses=18}, user1@TWOSTAR.COM for ftp/centos6.twostar.com@TWOSTAR.COM
```

FTP 서버의 인증 메세지 화면이다. ftp 서버에 user1으로부터 접속했다는 것을 알 수 있는 메시지이다.

```
May 27 02:04:09 centos6 ftpd[3637]: pam_unix(gssftp:session): session opened for user user1 by (uid=0)
```

4. 결 론

정보 시스템 다양화에 따른 관리의 효율화필요와 중앙집중적 사용자 관리를 통한 보안강화 및 PKI 기술의 등장으로 SSO(Single Sign On)을 구현했다. 또한 1인 평균 ID와 PW를 5개 이상 보유하고 있고 개인정보를 수정 할 때 가진 각각의 계정들을 수정하기 번거롭고 개인정보가 유출 될 때 언제 어디서 어떤 계정이 유출 됬는지 모르므로 관리하기 어렵기 때문에 SSO(Single Sign On)을 구현 하였다.
다른 아이디와 암호 조합으로 인한 암호 피곤을 줄일 수 있고 같은 아이디마다 암호를 다시 입력하는 시간을 줄일 수 있으며, 암호를 답해줘야 하는 헬프데스크 비용을 줄일 수 있는 장점을 가지고 있다.
이러한 장점들로 인해 리눅스 운영체제에서 SSO 인증 체제 구현을 하게 되었다.
리눅스 운영체제에서 SSO인증 체제 구현을 하기 위해서는 사용자, LDAP(디렉토리 서비스), Kerberos인증, Token 송/수신 수행을 이용해 SSO 인증체제를 구현하였다.
리눅스 운영체제에서 중앙 집중적인 사용자 관리가 가능하고, 단일 ID와 Password만 사용함으로써 SSO의 유용성이 입증 됨으로써 보안관리가 용이하고 비용 절감 등 보안 관리 기능 향상을 기대하며 다양한 인터넷 환경에 대응하는 표준 보안 인프라 체계 구축 가능을 기대 해본다.

5. 참고문헌

[1] 서자룡의 실무 관리자를 위한 서버 구축 및 활용 CentOS 5.3
[2] KLDPWiki: LDAP-Tips , https://wiki.kldp.org/wiki.php/LDAP-Tips
[3] Open ldap을 이용한 통합 시스템 환경 구축 하기 ,http://blog.syszone.co.kr/2658
[4] Kerberos-Community Help Wiki , https://help.ubuntu.com/community/Kerberos
[5] DB_사랑넷 , http://database.sarang.net/
[6] Kerberos-CentOS , https://www.centos.org/docs/5/.../ch-kerberos.html
[7] LDAP/Kerberos - Debian Wiki . https://wiki.debian.org/LDAP/Kerberos

리눅스 운영체제에서 SSO 인증체제 구현

2015. 6. 9

지도 교수 : 양 환 석 교수님

6조 Stellar

1

목 차

- 조원 소개
- 주제 선정
- 추진 경과
- 시스템 구성도
- 통합인증시스템 구축
- 결 론

2

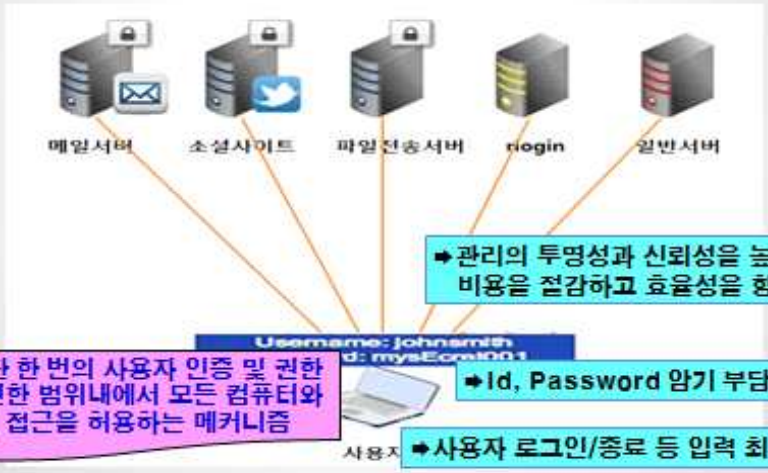
조원 소개

조 원	역할 분담
안세진	중앙인증서버관리, 전체 총괄
곽현민	연계시스템 구축
이슬비	계정통합관리
조성현	자료 조사

3

주제 선정

주제 : Single Sign-On(통합 인증) 구현



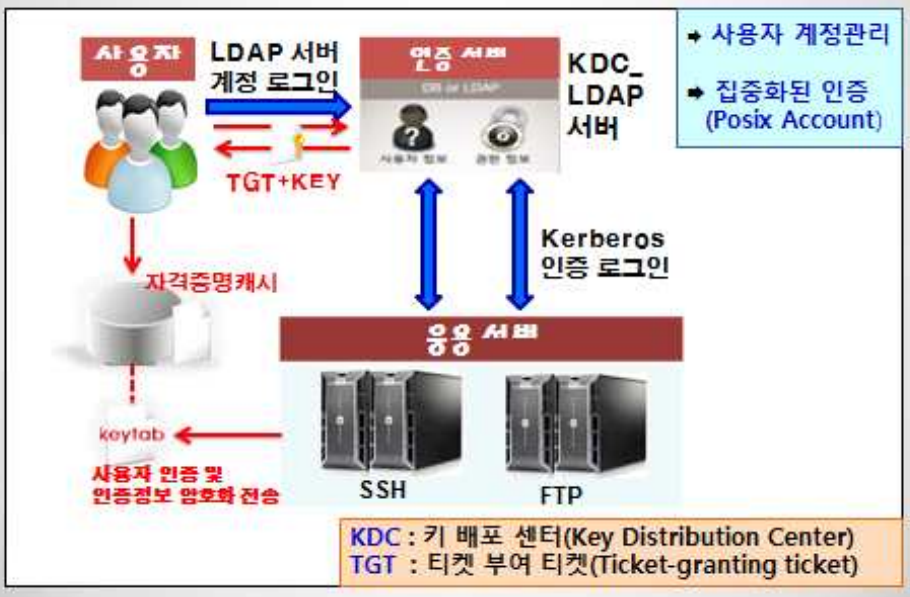
4

추진 경과

구 분	2014.9-12	2015.1	2015.2	2015.3	2015.4	2015.5
주제 선정, 자료 조사 및 시스템 구상	→					
LDAP 서버구축		→	→			
Kerberos 서버구축			→	→		
통합계정인증관리				→	→	→
TLS 보안향상 및 시스템 점검 보완						→

5

시스템 구성도



6

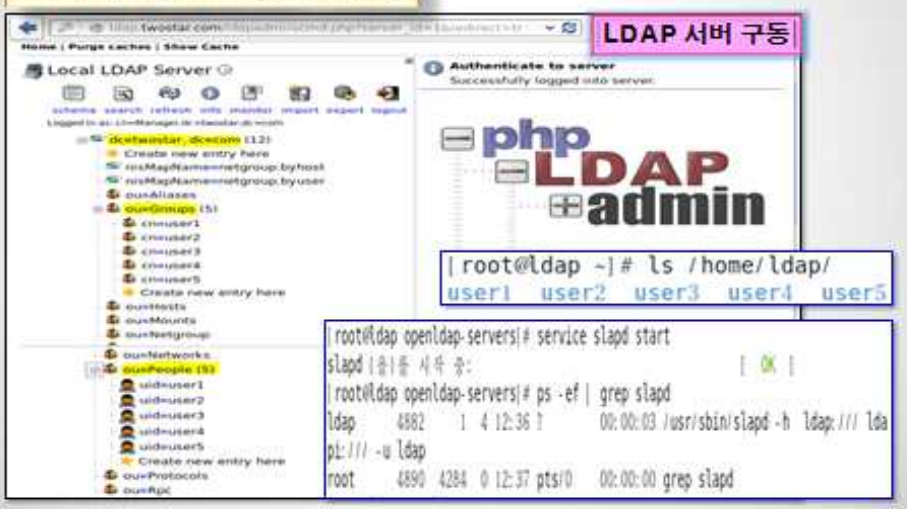
통합 인증시스템 구축

운영 환경

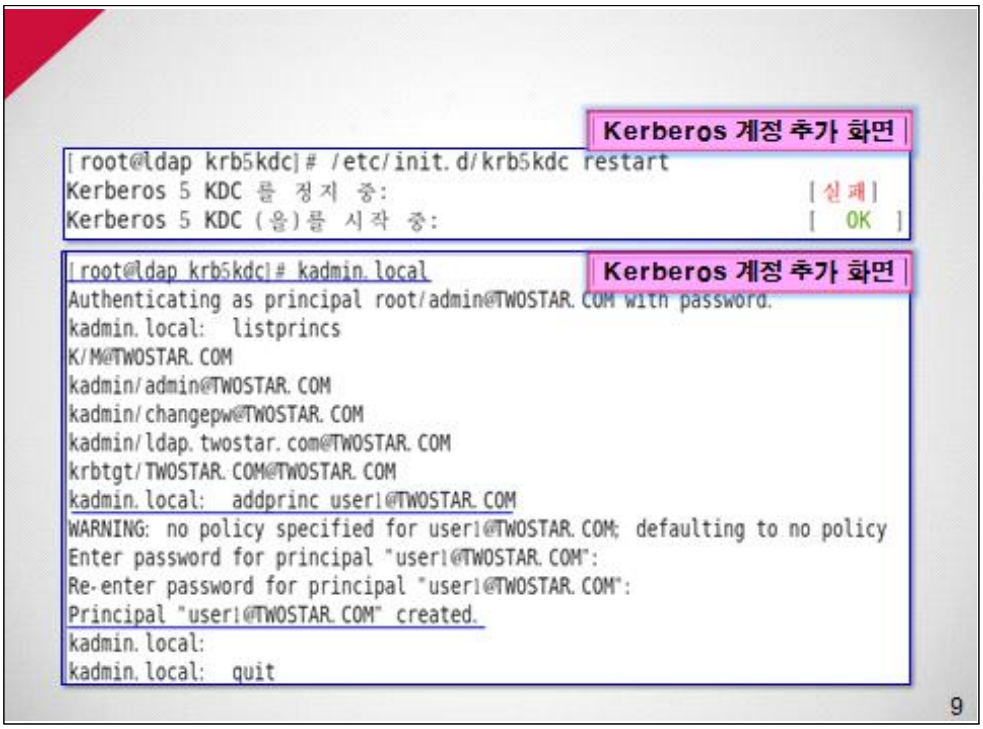
- 운영체제 : CentOS 6.5
- 인증관리서버 : LDAP, Kerberos서버
- 응용서버 : SSH, FTP 서버

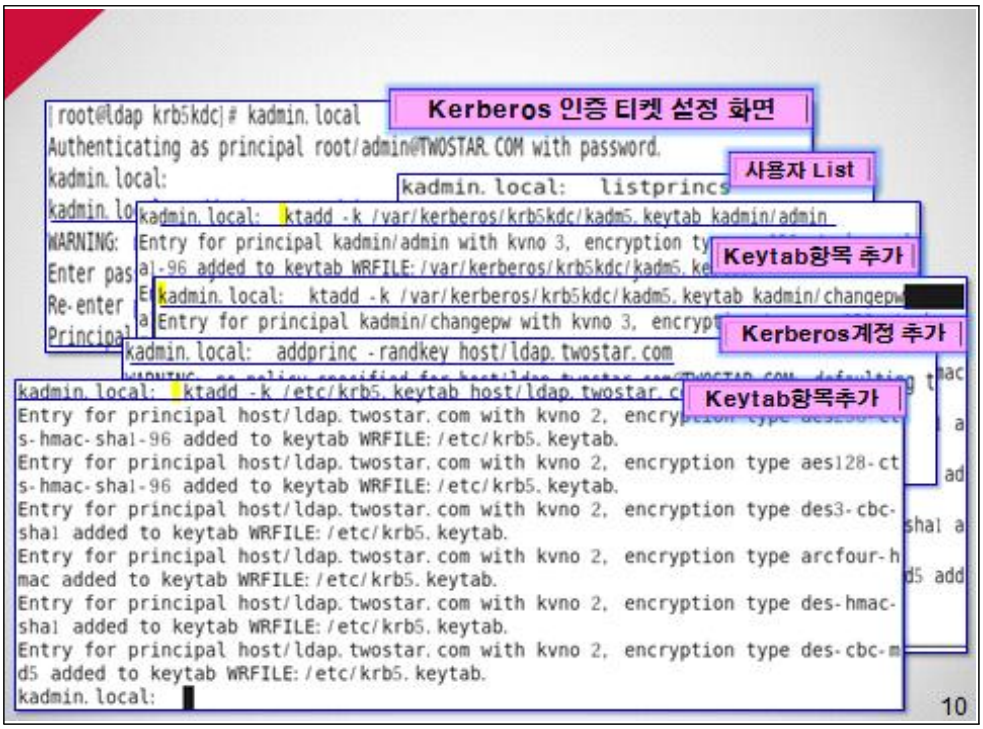
7

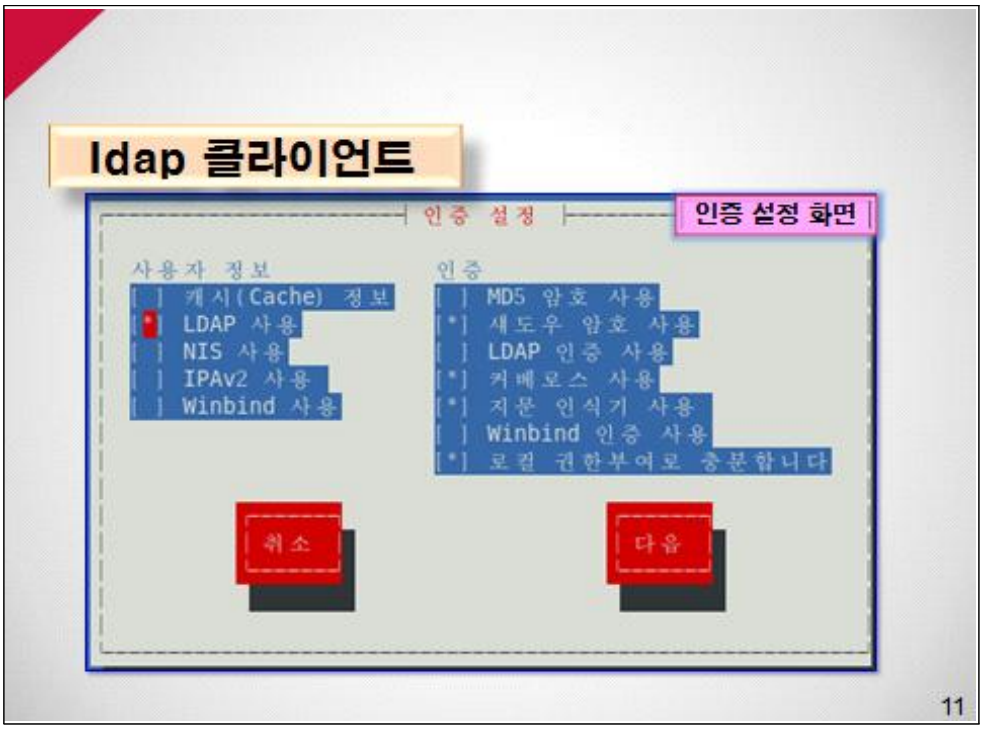
KDC_LDAP 서버

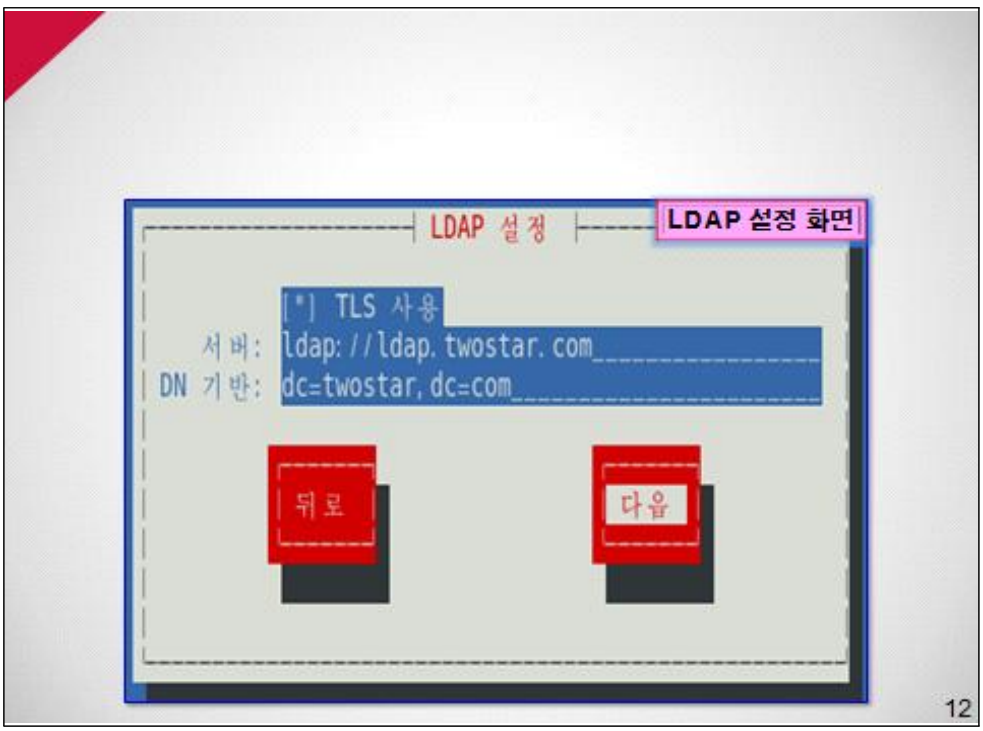


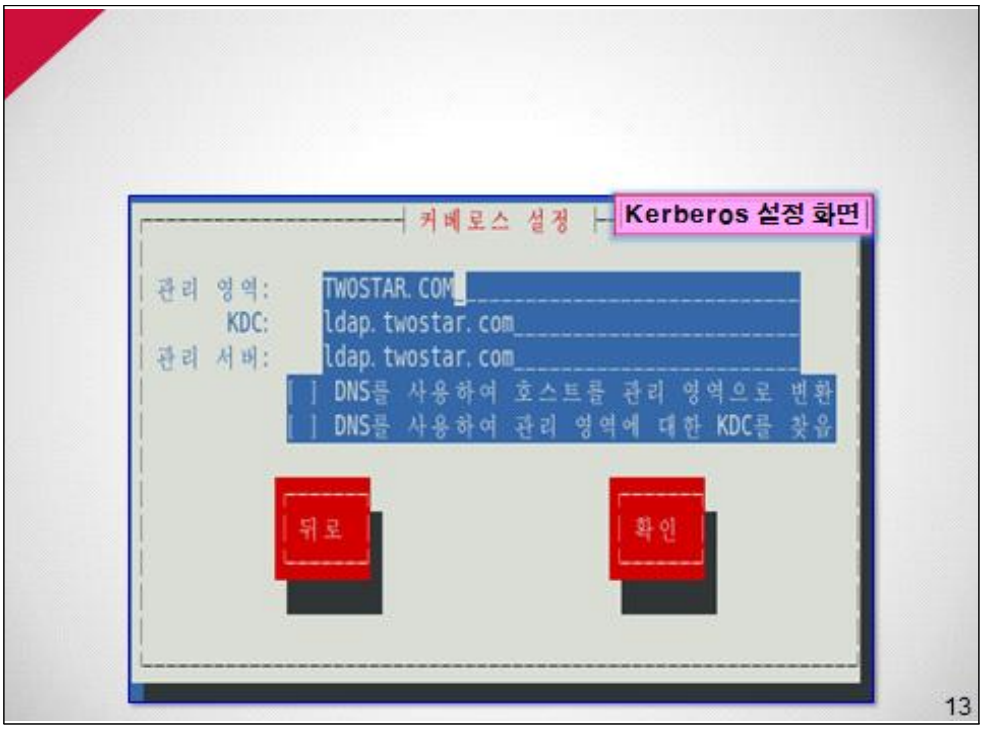
8

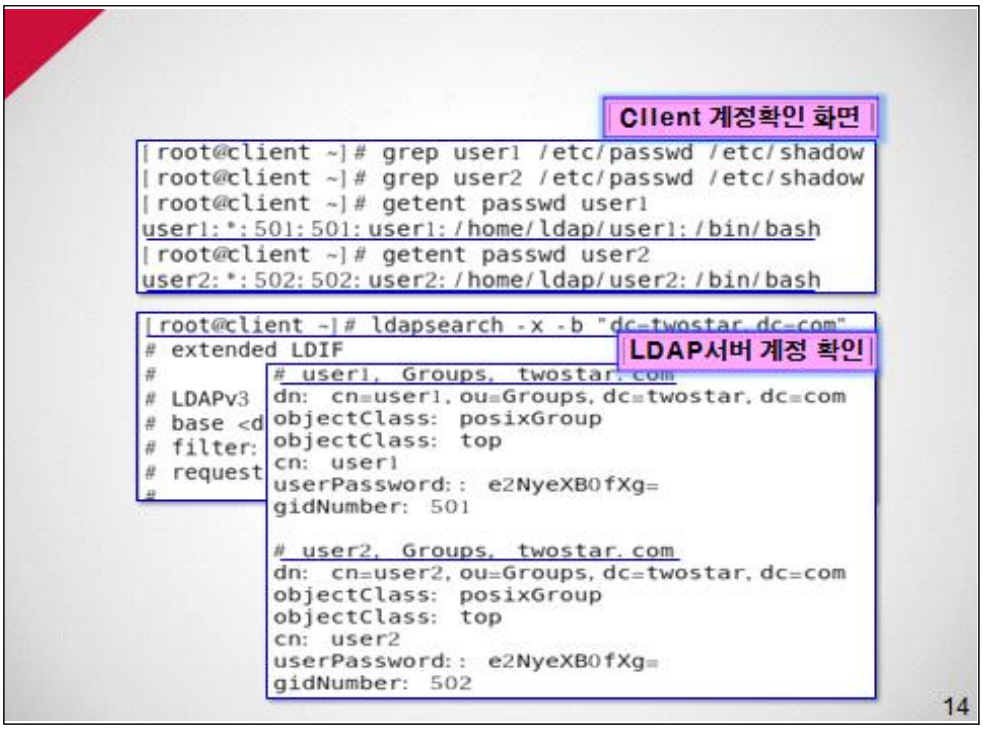

Kerberos 계정 추가 화면
[root@ldap krb5kdc]# /etc/init.d/krb5kdc restart
Kerberos 5 KDC 를 정지 중: [실패]
Kerberos 5 KDC (을)를 시작 중: [OK]
Kerberos 계정 추가 화면
[root@ldap krb5kdc]# kadmin.local
Authenticating as principal root/admin@TWOSTAR.COM with password.
kadmin.local: listprincs
K/M@TWOSTAR.COM
kadmin/admin@TWOSTAR.COM
kadmin/changepw@TWOSTAR.COM
kadmin/ldap.twostar.com@TWOSTAR.COM
krbtgt/TWOSTAR.COM@TWOSTAR.COM
kadmin.local: addprinc user1@TWOSTAR.COM
WARNING: no policy specified for user1@TWOSTAR.COM; defaulting to no policy
Enter password for principal "user1@TWOSTAR.COM":
Re-enter password for principal "user1@TWOSTAR.COM":
Principal "user1@TWOSTAR.COM" created.
kadmin.local:
kadmin.local: quit
9

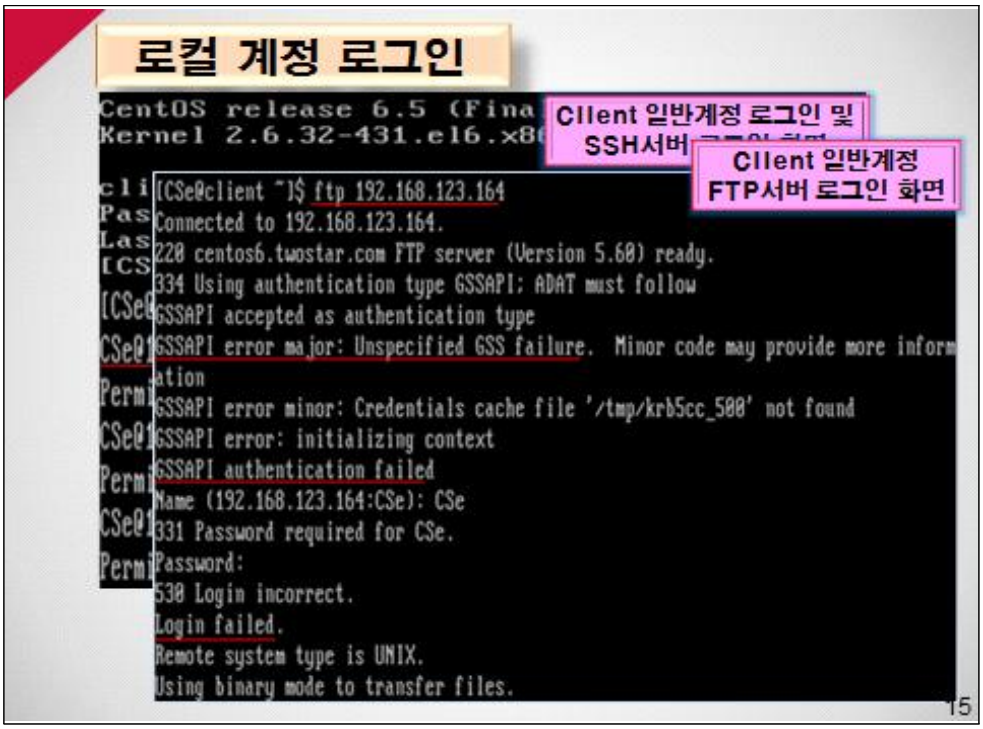

Kerberos 인증 티켓 설정 화면
[root@ldap krb5kdc]# kadmin.local
Authenticating as principal root/admin@TWOSTAR.COM with password.
kadmin.local:
사용자 List
kadmin.local: listprincs
kadmin.local: ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/admin
Entry for principal kadmin/admin with kvno 3, encryption ty
Keytab항목 추가
kadmin.local: ktadd -k /var/kerberos/krb5kdc/kadm5.keytab kadmin/changepw
Entry for principal kadmin/changepw with kvno 3, encrypt
Kerberos계정 추가
kadmin.local: addprinc -randkey host/ldap.twostar.com
kadmin.local: ktadd -k /etc/krb5.keytab host/ldap.twostar.c
Keytab항목추가
Entry for principal host/ldap.twostar.com with kvno 2, encry
s-hmac-sha1-96 added to keytab WRFILE: /etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type aes128-ct
s-hmac-sha1-96 added to keytab WRFILE: /etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des3-cbc-
sha1 added to keytab WRFILE: /etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type arcfour-h
mac added to keytab WRFILE: /etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des-hmac-
sha1 added to keytab WRFILE: /etc/krb5.keytab.
Entry for principal host/ldap.twostar.com with kvno 2, encryption type des-cbc-m
d5 added to keytab WRFILE: /etc/krb5.keytab.
kadmin.local:
10

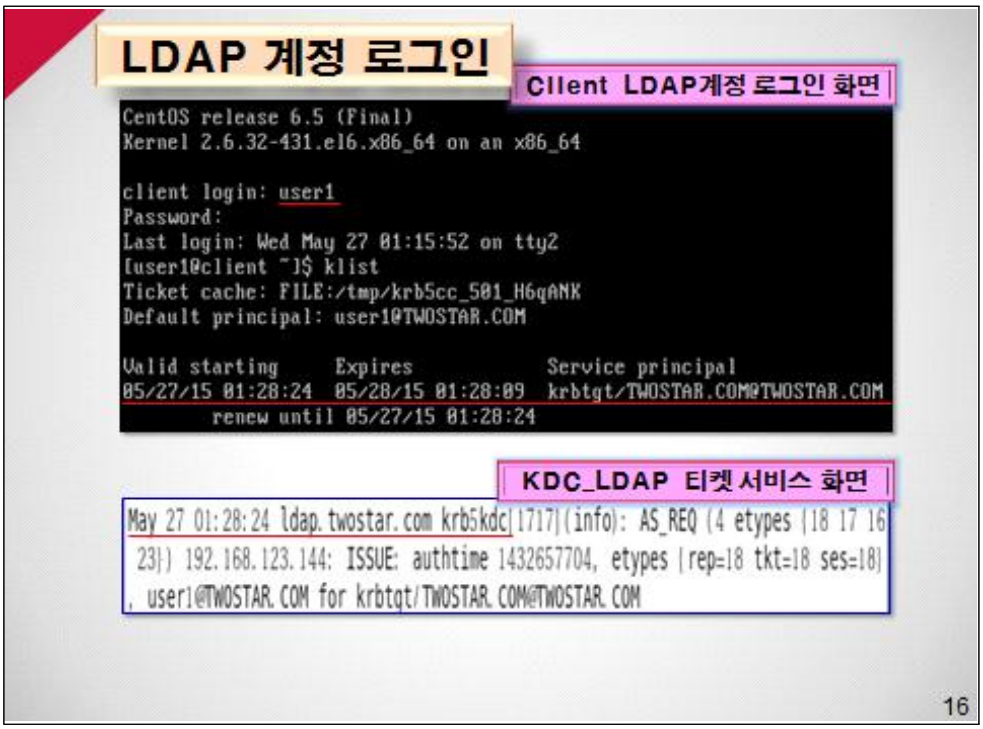

ldap 클라이언트
인증 설정
인증 설정 화면
사용자 정보
[ ] 캐시(Cache) 정보
[*] LDAP 사용
[ ] NIS 사용
[ ] IPAv2 사용
[ ] Winbind 사용
인증
[ ] MD5 암호 사용
[*] 새도우 암호 사용
[ ] LDAP 인증 사용
[*] 커베로스 사용
[*] 지문 인식기 사용
[ ] Winbind 인증 사용
[*] 로컬 권한부여로 충분합니다
취소
다음
11

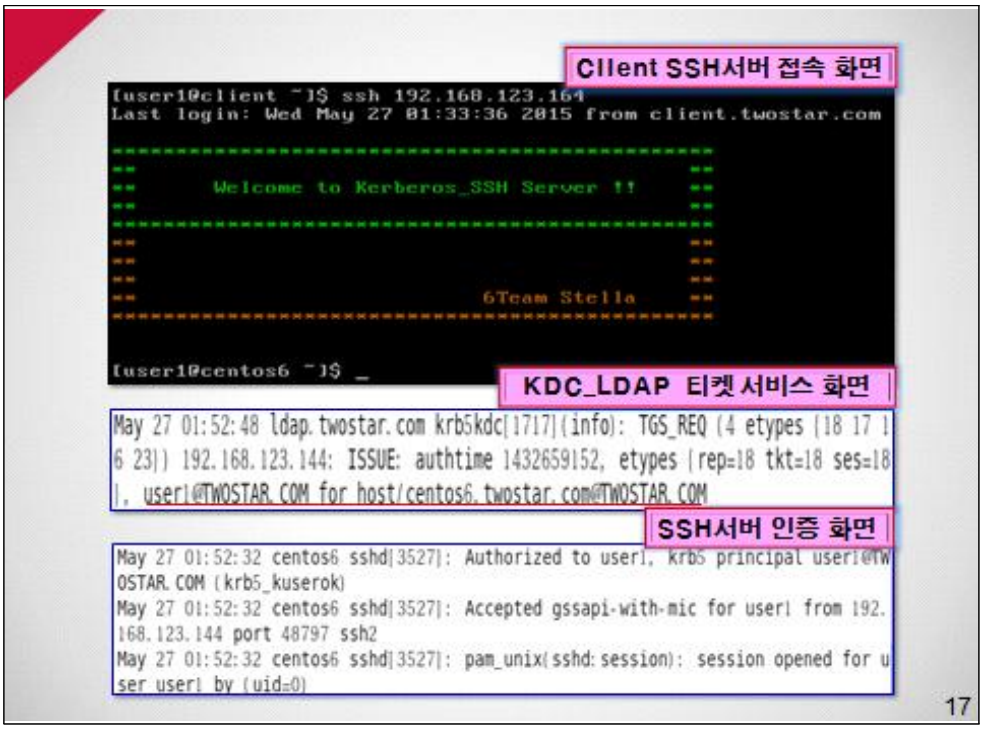

LDAP 설정
LDAP 설정 화면
[*] TLS 사용
서버: ldap://ldap.twostar.com
DN 기반: dc=twostar,dc=com
뒤로
다음
12


Kerberos 설정 화면
커베로스 설정
관리 영역: TWOSTAR.COM
KDC: ldap.twostar.com
관리 서버: ldap.twostar.com
[ ] DNS를 사용하여 호스트를 관리 영역으로 변환
[ ] DNS를 사용하여 관리 영역에 대한 KDC를 찾음
뒤로
확인
13

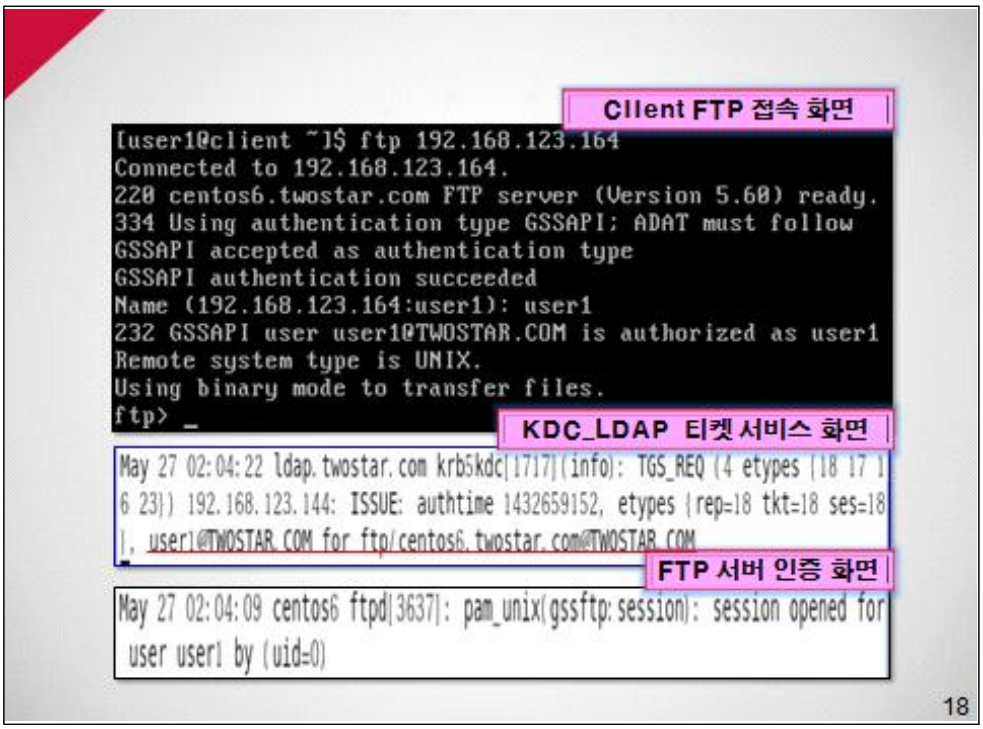

Client 계정확인 화면
[root@client ~]# grep user1 /etc/passwd /etc/shadow
[root@client ~]# grep user2 /etc/passwd /etc/shadow
[root@client ~]# getent passwd user1
user1:*:501:501:user1:/home/ldap/user1:/bin/bash
[root@client ~]# getent passwd user2
user2:*:502:502:user2:/home/ldap/user2:/bin/bash
[root@client ~]# ldapsearch -x -b "dc=twostar,dc=com"
extended LDIF
LDAP서버 계정 확인
user1, Groups, twostar.com
dn: cn=user1,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user1
userPassword:: e2NyeXB0fXg=
gidNumber: 501
user2, Groups, twostar.com
dn: cn=user2,ou=Groups,dc=twostar,dc=com
objectClass: posixGroup
objectClass: top
cn: user2
userPassword:: e2NyeXB0fXg=
gidNumber: 502
14


로컬 계정 로그인
CentOS release 6.5 (Fina
Kernel 2.6.32-431.el6.x8
Client 일반계정 로그인 및
SSH서버
Client 일반계정
FTP서버 로그인 화면
[CSe@client ~]$ ftp 192.168.123.164
Connected to 192.168.123.164.
220 centos6.twostar.com FTP server (Version 5.60) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI error major: Unspecified GSS failure. Minor code may provide more inform
ation
GSSAPI error minor: Credentials cache file '/tmp/krb5cc_500' not found
GSSAPI error: initializing context
GSSAPI authentication failed
Name (192.168.123.164:CSe): CSe
331 Password required for CSe.
Password:
530 Login incorrect.
Login failed.
Remote system type is UNIX.
Using binary mode to transfer files.
15


LDAP 계정 로그인
Client LDAP계정 로그인 화면
CentOS release 6.5 (Final)
Kernel 2.6.32-431.el6.x86_64 on an x86_64
client login: user1
Password:
Last login: Wed May 27 01:15:52 on tty2
[user1@client ~]$ klist
Ticket cache: FILE:/tmp/krb5cc_501_H6qANK
Default principal: user1@TWOSTAR.COM
Valid starting Expires Service principal
05/27/15 01:28:24 05/28/15 01:28:09 krbtgt/TWOSTAR.COM@TWOSTAR.COM
renew until 05/27/15 01:28:24
KDC_LDAP 티켓 서비스 화면
May 27 01:28:24 ldap.twostar.com krb5kdc[1717](info): AS_REQ (4 etypes {18 17 16
23}) 192.168.123.144: ISSUE: authtime 1432657704, etypes {rep=18 tkt=18 ses=18}
, user1@TWOSTAR.COM for krbtgt/TWOSTAR.COM@TWOSTAR.COM
16


Client SSH서버 접속 화면
[user1@client ~]$ ssh 192.168.123.164
Last login: Wed May 27 01:33:36 2015 from client.twostar.com
Welcome to Kerberos_SSH Server !!
6Team Stella
[user1@centos6 ~]$ _
KDC_LDAP 티켓 서비스 화면
May 27 01:52:48 ldap.twostar.com krb5kdc[1717](info): TGS_REQ (4 etypes {18 17 16 23}) 192.168.123.144: ISSUE: authtime 1432659152, etypes {rep=18 tkt=18 ses=18}, user1@TWOSTAR.COM for host/centos6.twostar.com@TWOSTAR.COM
SSH서버 인증 화면
May 27 01:52:32 centos6 sshd[3527]: Authorized to user1, krb5 principal user1@TWOSTAR.COM (krb5_kuserok)
May 27 01:52:32 centos6 sshd[3527]: Accepted gssapi-with-mic for user1 from 192.168.123.144 port 48797 ssh2
May 27 01:52:32 centos6 sshd[3527]: pam_unix(sshd:session): session opened for user user1 by (uid=0)

17


Client FTP 접속 화면
[user1@client ~]$ ftp 192.168.123.164
Connected to 192.168.123.164.
220 centos6.twostar.com FTP server (Version 5.60) ready.
334 Using authentication type GSSAPI; ADAT must follow
GSSAPI accepted as authentication type
GSSAPI authentication succeeded
Name (192.168.123.164:user1): user1
232 GSSAPI user user1@TWOSTAR.COM is authorized as user1
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> _
KDC_LDAP 티켓 서비스 화면
May 27 02:04:22 ldap.twostar.com krb5kdc[1717](info): TGS_REQ (4 etypes {18 17 16 23}) 192.168.123.144: ISSUE: authtime 1432659152, etypes {rep=18 tkt=18 ses=18}, user1@TWOSTAR.COM for ftp/centos6.twostar.com@TWOSTAR.COM
FTP 서버 인증 화면
May 27 02:04:09 centos6 ftpd[3637]: pam_unix(gssftp:session): session opened for user user1 by (uid=0)

18

FTP 파일전송 화면

```
ftp> cd /var/ftp/pub                    [user1@client ~]$ ls
250 CWD command successful.             [user1@client ~]$ _
ftp> ls
227 Entering Passive Mode (192,168,123,164,134,153)
150 Opening ASCII mode data connection for /bin/ls.
total 16
-rw-r--r--. 1 root 7 May 17 05:41 test1
-rw-r--r--. 1 root 6 May 17 05:41 test2
-rw-r--r--. 1 root 6 May 17 05:42 test3
-rw-r--r--. 1 root 6 May 17 05:43 test4
226 Transfer complete.
ftp> get test4
local: test4 remote: test4
227 Entering Passive Mode (192,168,123,164,173,145)
150 Opening BINARY mode data connection for test4 (6 bytes).
226 Transfer complete.
6 bytes received in 0.21 seconds (0.028 Kbytes/s)
ftp> quit
221 Goodbye.
[user1@client ~]$ ls
test4
[user1@client ~]$ _
```

19

결 론

◆ 리눅스 계열의 phpLDAPadmin을 활용

- LDAP 서버 계정으로 Kerberos 인증을 이용한 SSH, FTP 서버용 통합계정 로그인 체제를 구현

◆ 이를 통해

- 중앙 집중적인 사용자 관리가 가능하고, 단일 ID와 PW만 사용함으로써 SSO의 유용성이 입증
- 따라서 보안관리가 용이하고 비용 절감 등 보안관리 기능 향상이 기대

20


Q&A
Thank you
21