Odne Rindheim

Assignment 5

Assignment was done with 2 Virtual Machines running AlmaLinux 9 with brigaded network settings, the setup would be identical using 2 lab computers, but I did not have access to 2 computers on the lab for this redo.

Task 1: Logging

A) Configure systemd journal at the lab to save the logs persistent in the file system.

Created a directory for journal logs:

Sudo mkdir -p /var/log/journal

Assigned the correct permissions:

Sudo systemd-tmpfiles –create –prefix /var/log/journal

Modified the sysemd-journald configuration to ensure the following line is present:

Sudo nano /etc/systemd/journald.conf

Storage=persistent

Restart the systemd-journald service:

Sudo systemctl restart systemd-journald

B) Enable the Seal feature and create a sealing key

Edit the file /etc/sysemd/journald.conf/ and enable sealing:

Sudo nano /etc/systemd/journald.conf

Seal=Yes

Restart systemd-journald:

Sudo systemctl restart systemd-journald

Creating seal key:

Sudo journalctl –setup-key
Generating seed...

Generating key pair...

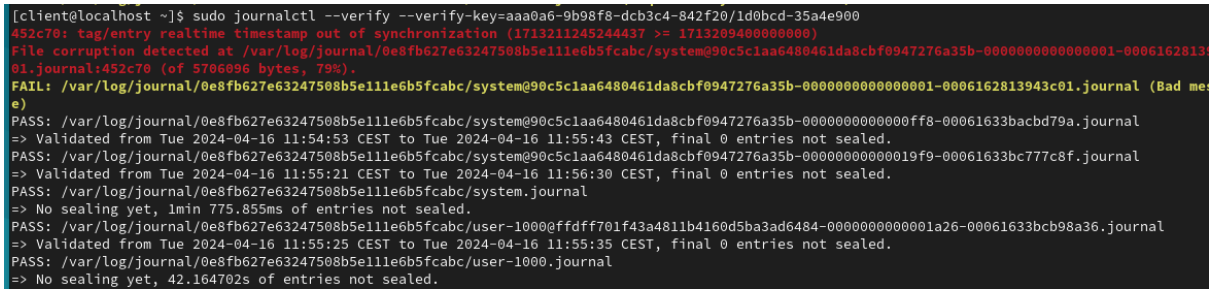
Generating sealing key...

Verify:

Sudo journalctl –verify

Odne Rindheim

this was the output:



Configure rsyslog for local5

Create config file local5.conf in /etc/rsyslog.d/:

Sudo nano /etc/rsyslog.d/local5.conf

Local5.=crit -/var/log/local5

Local5.=info -/var/log/local5

Restart the rsyslog:

Sudo systemctl restart rsyslog

Test:

Logger -p local5.info “Test info”

Logger -p local5.info “Test crit”

Check log:

Sudo cat /var/log/local5

Apr 15 20:54:14 localhost client[3568]: Test info

Apr 15 20:54:17 localhost client[3573]: Test crit

Odne Rindheim

Task 2: LDAP

Install required packages

Sudo dnf install opneldap openldap-clients openldap-servers -y

Enable and start ldap service

Sudo systemctl enable –now slapd

Check the base DN suffix:

Sudo ldapsearch -LLL -Q -Y EXTERNAL -H ldapi:/// -o ldif-wrap=no -b “oldDatabase={2}mdb,cn=config” olcSuffix

Configure base DN and Administrator DN

Made a directory for all my ldap-configs

Mkdir ~/ldap-configs

Created a basedn.ldif:

dn: olcDatabase={2}mdb,cn=config

changetype: modify

replace: olcSuffix

olcSuffix: dc=h128,dc=dat151

-

replace: olcRootDN

olcRootDN: cn=Manager,dc=h128,dc=dat151

apply changes:

sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ~/ldap-configs/basedn-ldif

Set administrator password

Slappasswd

Created a maanger.ldif

dn: olcDatabase={2}mdb,cn=config

changetype: modify

add: olcRootPW

olcRootPW: <slappaswd output>

-

add: olcAccess

*olcAccess: to * by dn="cn=Manager,dc=h128,dc=dat151" write by self write by * read*

Odne Rindheim

apply changes:

sudo ldapmodify -Y EXTERNAL -H ldapi:/// -f ~/ldap-configs/manager.ldif

Install cosine and nis schemas

Sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/cosine.ldif

Sudo ldapadd -Y EXTERNAL -H ldapi:/// -f /etc/openldap/schema/nis.ldif

Create the user database

Creating file top.ldif

dn: dc=h128,dc=dat151

dc: h128

objectClass: top

objectClass: domain

sudo ldapadd -D “cn=Manager,dc=h128,dc=dat151” -x -W -f ~/ldap-configs/top.ldif

```
No such object (32)
[server@localhost ~]$ sudo ldapadd -D "cn=Manager,dc=h214,dc=dat151" -x -W -f ~/ldap-configs/top.ldif
Enter LDAP Password:
adding new entry "dc=h214,dc=dat151"

[server@localhost ~]$ ldapsearch -LLL -b "dc=h214,dc=dat151" -x dn
dn: dc=h214,dc=dat151
```

Created ou.ldif:

dn: ou=People,dc=h128,dc=dat151

objectClass: organizationalUnit

ou: People

dn: ou=Group,dc=h128,dc=dat151

objectClass: organizationalUnit

ou: Group

```
[server@localhost ~]$ sudo ldapadd -D "cn=Manager,dc=h214,dc=dat151" -W -f ~/ldap-configs/ous.ldif
Enter LDAP Password:
adding new entry "ou=People,dc=h214,dc=dat151"

adding new entry "ou=Group,dc=h214,dc=dat151"
```

Adding user and group

Created users.ldif and groups.ldif

dn: uid=odne,ou=People,dc=h128,dc=dat151

uid: odne

cn: odne

Odne Rindheim

objectClass: account

objectClass: posixAccount

objectClass: top

objectClass: shadowAccount

shadowMin: 0

shadowMax: 99999

shadowWarning: 7

loginShell: /bin/bash

uidNumber: 6969

gidNumber: 69696

homeDirectory: /share/home/done

dn: cn=e82,ou=Group,dc=h128,dc=dat151

objectClass: posixGroup

objectClass: top

cn: e82

gidNumber: 69696

sudo ldapadd -D “cn=Manager,dc=h128,dc=dat151” -W -f ~/ldap-configs/users.ldif

sudo ldapadd -D “cn=Manager,dc=h128,dc=dat151” -W -f ~/ldap-configs/groups.ldif

```
[server@localhost ~]$ sudo ldapadd -D "cn=Manager,dc=h214,dc=dat151" -W -f ~/ldap-configs/users.ldif
Enter LDAP Password:
adding new entry "uid=odne,ou=People,dc=h214,dc=dat151"

[server@localhost ~]$ sudo ldapadd -D "cn=Manager,dc=h214,dc=dat151" -W -f -W -f ~/ldap-configs/groups.ldif
ldapadd: -f previously specified
[server@localhost ~]$ sudo ldapadd -D "cn=Manager,dc=h214,dc=dat151" -W -f ~/ldap-configs/groups.ldif
Enter LDAP Password:
adding new entry "cn=e82,ou=Group,dc=h214,dc=dat151"
```

Checking with ldapsearch:

Ldapsearch -LLL -b “dc=h128,dc=dat151” -x dn

```
[server@localhost ~]$ ldapsearch -LLL -b "dc=h214,dc=dat151" -x dn
dn: dc=h214,dc=dat151

dn: ou=People,dc=h214,dc=dat151

dn: ou=Group,dc=h214,dc=dat151

dn: uid=odne,ou=People,dc=h214,dc=dat151

dn: cn=e82,ou=Group,dc=h214,dc=dat151
```

Task 3: SSSD

I had to create two new virtual machines. The perryDC (192.168.230.128) is set up exactly the same as the previously used domain controller server. The new client machine, perryCL(192.168.230.129) is set up like this:

Setup:

Hostnames:

perryDC

Sudo hostnamectl set-hostname ldapserver

perryCL

Sudo hostnamectl set-hostname ldapclient

Both

Sudo nano /etc/hosts

192.168.230.128 ldapserver

192.168.230.129 ldapclient

Set firewall to allow service ldap

sudo firewall-cmd -permanent –add-service=ldap

sudo firewall-cmd --reload

Setting up ldapclient:

Installed openldap openldap-client openldap-servers

Verified i could access the LDAPserver from the client:

```
[perrycl@ldapclient ~]$ ping ldapserver
PING ldapserver (192.168.230.128) 56(84) bytes of data.
64 bytes from ldapserver (192.168.230.128): icmp_seq=1 ttl=64 time=0.234 ms
64 bytes from ldapserver (192.168.230.128): icmp_seq=2 ttl=64 time=0.724 ms
```

```
[perrycl@ldapclient ~]$ ldapsearch -x -H ldap://ldapserver -b "dc=h128,dc=dat151"
# extended LDIF
#
# LDAPv3
# base <dc=h128,dc=dat151> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# h128.dat151
dn: dc=h128,dc=dat151
dc: h128
objectClass: top
objectClass: domain

# Groups, h128.dat151
dn: ou=Groups,dc=h128,dc=dat151
objectClass: organizationalUnit
ou: Groups

# People, h128.dat151
dn: ou=People,dc=h128,dc=dat151
objectClass: organizationalUnit
ou: People

# e82, Groups, h128.dat151
dn: cn=e82,ou=Groups,dc=h128,dc=dat151
objectClass: posixGroup
objectClass: top
cn: e82
gidNumber: 69696

# odne, People, h128.dat151
dn: uid=odne,ou=People,dc=h128,dc=dat151
uid: odne
cn: odne
objectClass: account
objectClass: posixAccount
objectClass: top
objectClass: shadowAccount
shadowMin: 0
shadowMax: 99999
shadowWarning: 7
loginShell: /bin/bash
uidNumber: 6969
gidNumber: 69696
homeDirectory: /share/home/odne
userPassword:: e1NTSEF9dmk4NkwwdjhJcVk4T0h5SzNOQnJNSU9BUFU2YU1ibk4=

# search result
search: 2
result: 0 Success

# numResponses: 6
# numEntries: 5
```

Without CA:

Configuring SSSD:

Created configuration file for SSSD:

Sudo nano /etc/sssd/sssd.conf

Odne Rindheim

```
  GNU nano 5.6.1
[sssd]
config_file_version = 2
services = nss, pam
domains = LDAP

[domain/LDAP]
id_provider=ldap
auth_provider=ldap
ldap_uri = ldap://ldapserver
ldap_search_base = dc=h128,dc=dat151
ldap_schema = rfc2307bis
ldap_user_object_class = posixAccount
ldap_group_object_class = posixGroup
ldap_create_homedir = true
ldap_auth_disable_tls_never_use_in_production = true
```

Started and enabled SSSD service:

sudo systemctl start sssd

sudo systemctl enable sssd

Su - odne

```
[perrycl@ldapclient ~]$ su - odne
Password:
Last login: Wed Apr 24 16:06:27 CEST 2024 on pts/0
```

Setting up CA:

perryDC (ldap server)

Requested a cert.

Openssl req -new -newkey rsa:2048 -nodes -keyout private.key -our request.csr

Got the cert signed and put it inside /etc/certs/ along with private.key

Updated the ldap server config to use the signed certificate
olcTLSCertificateFile: /etc/openldap/certs/600870.cert.pem

olcTLSCertificateKeyFile: /etc/openldap/certs/private.key

set the appropriate permission on the certificate and private key files to the ldap:ldap

Restarted ldap service (slapd)

Set firewall-cmd –add-service=ldaps and reloaded firewall

perryCL (ldap client)

Downloaded the CA certificate (dat151.ldapcacert.pem) provided by lecturer.

Updated the sssd configuration file (/etc/sssd/sssd.conf) on perryCL to specify the path to the ca certificate:

Set firewall-cmd –add-service=ldaps and reloaded firewall

Odne Rindheim

ldap_tls_cacert = /etc/openldap/certs/dat151.ldapcacert.pem

removed ldap_auth_disable_tls_never_use_in_production = true

Restarted the SSSD Service

Tested by signing into user done again.

```
[perrycl@ldapclient ~]$ su - odne
Password:
Last login: Tue Apr 30 18:12:48 CEST 2024 on pts/0
[odne@ldapclient ~]$ exit
```

Odne Rindheim

Task 4: Kerbros

Kserver (192.168.0.48)

Sudo hostnamectl set-hostname kserver.driftslab

Edit etc/hosts:

192.168.0.239 kclient.driftlsab

192.168.0.48 kserver.driftslab

Check with hostname -f:

[kserver@kserver ~]$ hostname -f

kserver.driftslab

sudo yum install krb5-server

edit krb5.conf, kdc.conf and kadm5.acl

krb5.conf

```
[libdefaults]
    dns_lookup_realm = false
    dns_lookup_kdc = false
    ticket_lifetime = 24h
    renew_lifetime = 7d
    forwardable = true
    rdns = false
    pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
    spake_preauth_groups = edwards25519
    dns_canonicalize_hostname = fallback
    qualify_shortname = ""
    default_realm = DRIFTSLAB.HVL.NO
    default_ccache_name = KEYRING:persistent:%{uid}


[realms]
 DRIFTSLAB.HVL.NO = {
     kdc = kserver.driftslab
     admin_server = kserver.driftslab
 }


[domain_realm]
 .driftslab = DRIFTSLAB.HVL.NO
```

Odne Rindheim

```
 driftslab = DRIFTSLAB.HVL.NO


# kdc.conf
[kdcdefaults]
    kdc_ports = 88
    kdc_tcp_ports = 88
    spake_preauth_kdc_challenge = edwards25519


[realms]
DRIFTSLAB.HVL.NO = {
     master_key_type = aes256-cts-hmac-sha384-192
     acl_file = /var/kerberos/krb5kdc/kadm5.acl
     dict_file = /usr/share/dict/words
     default_principal_flags = +preauth
     admin_keytab = /var/kerberos/krb5kdc/kadm5.keytab
    supported_enctypes = aes256-cts-hmac-sha384-192:normal aes128-cts-hmac-sha256-128:normal aes256-cts-hmac-sha1-
96:normal aes128-cts-hmac-sha1-96:normal c>
    # Supported encryption types for FIPS mode:
    #supported_enctypes = aes256-cts-hmac-sha384-192:normal aes128-cts-hmac-sha256-128:normal
}
# kadm5.acl
/admin@DRIFTSLAB.HVL.NO        *
```

[kserver@kserver ~]$ sudo kdb5_util create -r DRIFTSLAB.HVL.NO -s

Initializing database '/var/kerberos/krb5kdc/principal' for realm 'DRIFTSLAB.HVL.NO',

master key name 'K/M@DRIFTSLAB.HVL.NO'

You will be prompted for the database Master Password.

It is important that you NOT FORGET this password.

Enter KDC database master key:

Re-enter KDC database master key to verify:

[kserver@kserver ~]$ sudo systemctl start krb5kdc

sudo systemctl start kadmin

sudo systemctl enable krb5kdc

sudo systemctl enable kadmin

Odne Rindheim

[kserver@kserver ~]$ sudo kadmin.local -q "addprinc root/admin"

[kserver@kserver ~]$ sudo firewall-cmd --permanent --add-service=kerberos

success

[kserver@kserver ~]$ sudo firewall-cmd --reload

Success

[kserver@kserver ~]$ sudo kadmin.local -q "addprinc student@DRIFTSLAB.HVL.NO"

Authenticating as principal root/admin@DRIFTSLAB.HVL.NO with password.

No policy specified for student@DRIFTSLAB.HVL.NO; defaulting to no policy

Enter password for principal "student@DRIFTSLAB.HVL.NO":

Re-enter password for principal "student@DRIFTSLAB.HVL.NO":

add_principal: Password mismatch while reading password for "student@DRIFTSLAB.HVL.NO".

[kserver@kserver ~]$ sudo kadmin.local -q "addprinc student@DRIFTSLAB.HVL.NO"

Authenticating as principal root/admin@DRIFTSLAB.HVL.NO with password.

No policy specified for student@DRIFTSLAB.HVL.NO; defaulting to no policy

Enter password for principal "student@DRIFTSLAB.HVL.NO":

Re-enter password for principal "student@DRIFTSLAB.HVL.NO":

Principal "student@DRIFTSLAB.HVL.NO" created.

[kserver@kserver ~]$ sudo kadmin.local -q "addprinc -randkey host/kclient.driftslab@DRIFTSLAB.HVL.NO"

Authenticating as principal root/admin@DRIFTSLAB.HVL.NO with password.

No policy specified for host/kclient.driftslab@DRIFTSLAB.HVL.NO; defaulting to no policy

Principal "host/kclient.driftslab@DRIFTSLAB.HVL.NO" created.

kadmin.local -q "addprinc -randkey host/kserver.driftslab@DRIFTSLAB.HVL.NO"

kadmin.local -q "ktadd -k /etc/krb5.keytab host/kserver.driftslab@DRIFTSLAB.HVL.NO"

Edited the sshd_config to allow gassapi stuff

GSSAPI options

GSSAPIAuthentication yes

GSSAPICleanupCredentials yes

#GSSAPIStrictAcceptorCheck yes

#GSSAPIKeyExchange no

Odne Rindheim

#GSSAPIEnablek5users no

Also created a file /etc/ssh/sshd_config.d/60-kerberos.conf that includes the following code:
Match Address 192.168.0.239 AuthenticationMethods gssapi-with-mic

Kclient (192.168.0.239)

Set hostname and updated /etc/hosts

sudo hostnamectl set-hostname kclient.driftslab

192.168.0.239 kclient.driftslab

192.168.0.48 kserver.driftslab

[kclient@kclient ~]$ hostname

kclient.driftslab

installed krb5-workstation

changed the krb5.conf to match the kserver:

```
[libdefaults]
   dns_lookup_realm = false
   dns_lookup_kdc = false
   ticket_lifetime = 24h
   renew_lifetime = 7d
   forwardable = true
   rdns = false
   pkinit_anchors = FILE:/etc/pki/tls/certs/ca-bundle.crt
   spake_preauth_groups = edwards25519
   dns_canonicalize_hostname = fallback
   qualify_shortname = ""
   default_realm = DRIFTSLAB.HVL.NO
   default_ccache_name = KEYRING:persistent:%{uid}

[realms]
 DRIFTSLAB.HVL.NO = {
    kdc = kserver.driftslab
    admin_server = kserver.driftslab
 }

[domain_realm]
```

Odne Rindheim

.driftslab = DRIFTSLAB.HVL.NO

driftslab = DRIFTSLAB.HVL.NO

obtain ticket for student and check list:

[kclient@kclient ~]$ kinit student

Password for student@DRIFTSLAB.HVL.NO:

[kclient@kclient ~]$ klist

Ticket cache: KCM:1000

Default principal: student@DRIFTSLAB.HVL.NO

Valid starting Expires Service principal

05/01/2024 12:42:59 05/02/2024 12:42:57 krbtgt/DRIFTSLAB.HVL.NO@DRIFTSLAB.HVL.NO

renew until 05/01/2024 12:42:59

Create the user student

Sudo useradd -m student

Attempt ssh from kclient:

[kclient@kclient ~]$ ssh student@kserver.driftslab

[student@kserver.driftslab ~]$