LISENET

← *Setting up LDAP and Kerberos Client Authentication on RHEL 7 (using nslcd)*

Getting Started with KVM on Debian Jessie →

Setting up LDAP and Kerberos Client Authentication on RHEL 7 (using sssd)

Posted on 07/05/2016 by Tomas

We are going to configure a RHEL 7 system to authenticate against FreeIPA using LDAP/Kerberos.

Prerequisites

To get Kerberos running, NTP synchronisation and DNS resolution must be working.

We are going to use the FreeIPA server which we set up previously. Check this post for how to setup a FreeIPA server on RHEL 7.

SSSD

The System Security Services Daemon (SSSD) provides access to different identity and authentication providers.

What SSSD does is allow a local service to check with a local cache in SSSD, but that cache may be taken from any variety of remote identity providers — an LDAP directory, an Identity Management domain, even a Kerberos realm.

Configure LDAP Authetication

We use a RHEL 7.0 server (instructions were also tested on a RHEL 7.2) with SELinux set to enforcing mode.

DNS is configured to point to the FreeIPA server:

```
# cat /etc/resolv.conf
search rhce.local
nameserver 10.8.8.70
```

```
# host 10.8.8.70
70.8.8.10.in-addr.arpa domain name pointer ipa.rhce.local.
```

Installation

```
# yum install -y sssd nss-pam-ldapd wget
```

Download the CA certificate from the IPA server to our local server:

```
# mkdir /etc/openldap/cacerts
# wget -P /etc/openldap/cacerts/ ftp://ipa.rhce.local/pub/cacert.p1
```

Configuration

Open the file `/etc/sysconfig/authconfig` and ensure the following are set:

```
USESSSDAUTH=yes
FORCELEGACY=no
USESSSD=yes
```

Once done, run the authconfig utility.

```
# authconfig-tui
```

In User Information, select **Use LDAP**, and under Authentication, select **Use LDAP Authentication**. In the LDAP Settings screen, select **Use TLS** and specify the following:

```
Server: ipa.rhce.local
Base DN: dc=rhce,dc=local
```

Open the file `/etc/sssd/sssd.conf` and add the following line:

```
ldap_tls_reqcert = never
```

Check man sssd-ldap for more options that are available.

Make sure nslcd is disabled, and sssd enabled:

```
# systemctl stop nslcd; systemctl disable nslcd
# systemctl enable sssd; systemctl restart sssd
```

Verify by logging in with an LDAP user:

```
# su - alice
su: warning: cannot change directory to /home/alice: No such file c
$ id
uid=1219400005(alice) gid=1219400005(alice) groups=1219400005(alice
```

Configure Kerberos Authentication

Installation

```
# yum install -y pam_krb5 krb5-workstation
```

Configuration

I found erasing the file's `/etc/krb5.conf` content helpful when configuring Kerberos authentication from scratch:

```
# > /etc/krb5.conf
```

Run the authconfig in a text mode:

```
# authconfig-tui
```

On the authentication Configuration screen, under Authentication, select **Use Kerberos** to enable Kerberos authorisation. In the LDAP Settings screen, do not change anything. In the Kerberos settings screen, specify the following:

```
Realm: RHCE.LOCAL
KDC: ipa.rhce.local
Admin Server: ipa.rhce.local
```

Obtain a Kerberos ticket for the Kerberos alice user:

```
# kinit alice
```

Verify the ticket:

```
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: alice@RHCE.LOCAL

Valid starting     Expires            Service principal
07/05/16 11:21:27  08/05/16 11:21:25  krbtgt/RHCE.LOCAL@RHCE.LOCAL
```

These are for references.

```
# cat /etc/krb5.conf
[libdefaults]
 default_realm = RHCE.LOCAL
 dns_lookup_realm = false
 dns_lookup_kdc = false
[realms]
 RHCE.LOCAL = {
  kdc = ipa.rhce.local
  admin_server = ipa.rhce.local
 }

[domain_realm]
 rhce.local = RHCE.LOCAL
 .rhce.local = RHCE.LOCAL
```

```
# cat /etc/sssd/sssd.conf
[domain/default]

autofs_provider = ldap
cache_credentials = True
krb5_realm = RHCE.LOCAL
ldap_search_base = dc=rhce,dc=local
id_provider = ldap
auth_provider = krb5
```

```
chpass_provider = krb5
ldap_uri = ldap://ipa.rhce.local/
ldap_id_use_start_tls = True
ldap_tls_cacertdir = /etc/openldap/cacerts
ldap_tls_reqcert = never
krb5_server = ipa.rhce.local
krb5_store_password_if_offline = True
krb5_kpasswd = ipa.rhce.local
[sssd]
services = nss, pam, autofs
config_file_version = 2

domains = default
[...]
```

Test Kerberos Configuration

```
# su - alice
su: warning: cannot change directory to /home/alice: No such file c
```

```
$ hostname
srv2.rhce.local
```

```
$ kinit
Password for alice@RHCE.LOCAL:
```

```
$ klist
Ticket cache: FILE:/tmp/krb5cc_1219400005
Default principal: alice@RHCE.LOCAL

Valid starting     Expires            Service principal
07/05/16 12:04:44  87/05/16 12:04:42  krbtgt/RHCE.LOCAL@RHCE.LOCAL
```

We should be able to reconnect without giving any password:

```
$ ssh ipa.rhce.local
Could not create directory '/home/alice/.ssh'.
[...]
Could not chdir to home directory /home/alice: No such file or dire
```

```
$ hostname
ipa.rhce.local
```

This entry was posted in LDAP/Kerberos, Linux and tagged EX300, Kerberos, LDAP, RHCE, RHEL, sssd. Bookmark the permalink. If you notice any errors, please contact us.

← Setting up LDAP and Kerberos Client Authentication on RHEL 7 (using nslcd)

Getting Started with KVM on Debian Jessie →

48 thoughts on “Setting up LDAP and Kerberos Client Authentication on RHEL 7 (using sssd)”

Saul Bertuccio says:
16/08/2016 at 8:28 am

Hi,
i have noticed the use of
tls_reqcert never in /etc/nslcd.conf for nslcd
and
ldap_tls_reqcert = never in /etc/sssd/sssd.conf for sssd.

If I'm not wrong, this disable the use of tsl certificate. You can check this deleting the certification authority certificate (ca.crt) in /etc/openldap/cacerts.
This because the authconfig-tui does not properly create hash link for the ca.crt.
Instead authconfig-gtk properly create the hash link.
Then I think is better to configure ldap authentication using authconfig-gtk.
If you want to configure ldap/kerberos authentication using authconfig-tui, without disabling tls, you need to:

Configure authentication ldap/kerberos using authconfig-tui. At end authconfig-tui warn you to copy the CA certificate in /etc/openldap/cacerts.

cd /etc/openldap/cacerts

IPA server CA certificate is /etc/ipa/ca.crt you can copy it in the pub ftp directory:
– cp /etc/ipa.crt /var/ftp/pub/
Then dowload it using wget:
– wget -O ca.crt ftp://labipa.example.com/pub/ca.crt
The we need to get the certificate hash:
– /etc/pki/tls/misc/c_hash ca.crt
example : 45e037a3.0 => ca.crt
Now we need to properly create the hash link:
– ln -s ca.crt 45e037a3.0

then restart sssd

Reply

Tomas says:
16/08/2016 at 9:59 am

I'm afraid you misunderstood. It does not disable the TLS certificate.

Setting **ldap_tls_reqcer**t to "never" means that the client does not "request" a server certificate. Now whether the server sends its certificate or not is not under the client's

control, but setting it to “never” just tells the client to do no checking of the server certificate, if any, that is received.

Balucio says:
07/09/2016 at 5:15 am

Hi,
yes but if I set tls_reqcert never or ldap_tls_reqcert never in nslcd or sssd I don’t need to dowload the CA certificate.

Tomas says:
07/09/2016 at 9:36 am

Interesting, thanks.

JustinSoul says:
02/02/2017 at 4:20 am

CentOS 7.3 creates symlink to /etc/openldap/cacerts/ca.crt (taken from FreeIPA host /etc/ipa/ca.crt) automatically after enabling TLS support using authconfig-tui.

Note: LDAPS will not work with `cacert.p12` file. You need to copy CA certificate in `.crt` or `.pem` format.
The easiest way is:

1.
[root@srv1 ~]# mkdir /etc/openldap/cacerts
[root@srv1 ~]# scp ipa.rhce.local:/etc/ipa/ca.crt /etc/openldap/ca.crt

2. Then enable TLS for LDAP using `authconfig-tui` utility.

In this case you don’t need to use `ldap_tls_reqcert = never` on srv1.rhce.local.

Tomas says:
02/02/2017 at 10:26 am

Thanks, that’s interesting.

Art says:
01/11/2016 at 8:16 pm

Is there a reason I can’t use ipa-client-install after I “yum -y install ipa-client” instead of going through all that?

Reply

Tomas says:
01/11/2016 at 9:04 pm

You can use **ipa-client-install** if you know the Kerberos admin credentials (exam wise).

Santosh Lohar says:
11/01/2017 at 9:41 pm

HI Tomas,

DO I need to do all the tasks mentioned in “Setting up LDAP and Kerberos Client Authentication on RHEL 7 (using sssd) ” this page for RHCE exam . Please let me know . I am preparing now for the exam . Just I want to know clear idea about the task.
Thanks in advance.

Reply

Tomas says:
11/01/2017 at 11:16 pm

I cannot tell how many tasks mentioned here you need to do, but you surely need to know how to configure LDAP/Kerberos authentication. And be advised that you don’t have to stick with **authconfig-tui** if you don’t want to, it’s not the only option available for the job.

hunter86_bg says:
17/04/2017 at 6:14 am

@Tomas, please update the section for download of the ipa certificate. According to the following errata it should be replaced with “/etc/ipa.ca.crt”

Reply

Tomas says:
17/04/2017 at 6:18 pm

That looks like a random link on the Internet that anyone can post and not a valid Errata per se. Do you happen to have a weblink to the Red Hat source?

Michael says:

12/05/2017 at 4:17 pm

kerberos authentication for ssh doesn't appear to work using the instructions given here. Is there anything that needs to be changed to allow ssh to use kerberos? I am using Redhat 7.3.

Reply

Tomas says:
19/05/2017 at 1:39 pm

Not sure to be honest, I didn't use RHEL 7.3.

Alex says:
13/08/2017 at 8:13 am

Hi Tomas, thanks for this guide.

I've got few questions, why you use here sssd instead of nslcd? Is it ok to use nslcd?

Configuring sssd in this way, did not create sssd.conf automatically. Maybe I've missed something? As installing different packages previously I don't have to configure it, it was created automatically, but not I cannot make it work.

ps. works properly on RHEL 7.3 except sssd.conf

Reply

Tomas says:
13/08/2017 at 11:36 am

Hi Alex, you can use whichever you like, there is a guide for setting an LDAP client up with nslcd too.

I haven't tried the instructions on RHEL 7.3, therefore cannot really tell much, but on RHEL 7.0 and RHEL 7.2 it should work as per blog post.

Muhammad Asif says:
13/10/2017 at 6:43 am

Thanks for this great article.

This is bit confusing for me .
Exam Objective is : Configure a system to authenticate using Kerberos

Q1:
Why would we need to Configure LDAP Authetication first and then Configure Kerberos Authentication

Q2: ipa-client package will join the IPA server without any difficulties. If we use ipa-client only , will it work smoothly ???

If you provide a short tutorial about IPA Server with ipa-client , I think will help us more.

Reply

Tomas says:
13/10/2017 at 9:42 am

Hi, these are excellent questions!

In short, Kerberos is used for authentication to manage credentials securely while LDAP is used for holding authoritative information about user accounts, such as the user's full name and uid, or what they're allowed to access (authorisation).

While LDAP can be used for both authentication and authorisation, it is best, in my opinion, to avoid using LDAP for authentication and go with Kerberos.

Having said that, you do not need to configure LDAP in order to use Kerberos. For the exam you need to know how to configure Kerberos authentication.

The ipa-client should work without issues, there is an example provided on the following page:
https://www.lisenet.com/2016/kerberised-nfs-server-on-rhel-7/

lars says:
20/10/2017 at 12:59 pm

Great stuff, much better than use of ipa-client.

Reply

Stef says:
10/11/2017 at 6:37 am

Hi,
I followed these instructions exactly and I found that nslcd is started as well as sssd. Is this expected? I would expect only sssd to be

started/enabled, correct?
I'm following Sander van Vugts course (and his VMs, rhel 7.2) and got the same result. After some googling I found your site (very helpful!) and tried your guide ending up in the same situation where nslcd is started/used as well as sssd. nslcd is started only after configuring kerberos.
Any idea what's going wrong?

Thanks,
Stef

Reply

Tomas says:
10/11/2017 at 9:07 am

I think I had to disable nslcd. It should be mentioned in the blog post.

Stef says:
10/11/2017 at 10:21 am

Hi Tomas,
Thanks for your reply. I did that and found nslcd was already disabled /not running.
So to be clear, nslcd should not be running at all right?

Thanks

Reply

Tomas says:
10/11/2017 at 7:25 pm

Yes, you should be using either sssd or nslcd.

pilcher says:
25/03/2018 at 9:14 am

Hi Tomas,

I followed your tutorial about configuring kerberos authentication with sssd on my centos 7.0 and when i'm running "kinit lisa" i'm getting the following error : " kinit: Generic preauthentication failure while getting initial credentials "
but if i'm doing " kinit admin " it's working , what could be the problem ?

Regards,
Pilcher

Reply

pilcher says:
25/03/2018 at 9:16 am

I forgot to mention that i've got the ipa server from sander and i didn't do any modifications , just followed your setup.

Tomas says:
25/03/2018 at 11:36 am

In this case you might be better off asking Sander, or you can always use my FreeIPA configuration:

https://www.lisenet.com/2016/freeipa-server-on-rhel-7-centos-7/

Tomas says:
25/03/2018 at 11:35 am

Could me many things, hard to say without knowing your setup.

Pilcher says:
26/03/2018 at 11:08 am

Thanks Tomas,

I'm going to write a message to Sander.

Regards,
Pilcher

Reply

omipenguin says:
29/08/2018 at 12:49 pm

Hello Tomas,

Thanks for providing the guide and greate tutorials. I'm trying to apply above tutorial. IPA is working fine I created the user ALICE on IPA server. Now while configuring Kerberos on Serv2 followed line by line. when i tried to login to do "su – alice" on serv2 it slapped me with message "su: user alice does not exist" . Also even though i

install the package for /etc/sssd/sssd.conf still sssd.conf file was not created , so i had to copy the file from “/usr/share/doc/sssd-common-1.11.2/sssd-example.conf” and save it as a /etc/sssd/sssd.conf.

And uncommented last two lines and changed the realm
krb5_server = ipa.rhce.local
krb5_realm = RHCE.LOCAL

Now when i try to start the service “systemctl start sssd” it gives another message.
“Aug 29 14:41:27 serv2.rhce.local sssd[3245]: SSSD couldn’t load the configuration database [2]: No such file or directory.
Aug 29 14:41:27 serv2.rhce.local systemd[1]: sssd.service: control process exited, code=exited status=4
Aug 29 14:41:27 serv2.rhce.local systemd[1]: Failed to start System Security Services Daemon.
”

Note: IPA server is Centos 7.2 and Serv2 is Centos 7.0

Any idea what im missing

Reply

Tomas says:
29/08/2018 at 7:47 pm

You cannot log in because LDAP authentication is not working. Did you use authconfig-tui?

omipenguin says:
30/08/2018 at 7:53 am

Do i also have to enable LDAP. yes i used authconfig-tui and authconfig-gtk

Tomas says:
01/09/2018 at 10:16 am

Yes, give it a go.

rezance says:
18/10/2018 at 1:30 pm

Hi all,
I had same issue, firstly I tried same as you copying sssd.con from another location. But that i got “No such file or directory” error same as you..

Then I try another approach.
1. run authconfig-tui again UNCHECK “Use LDAP” and “Use Ldap configuration”, click Next.
2. Then verify if you don’t forgot to configure setting in /etc/sysconfig/authconfig (this was maybe reason why sssd.conf was not generated at least in my case.
3. run authconfig-tui again CHECK “Use LDAP” and “Use Ldap configuration”, click Next. Continue as you would according this tutorial.

Tomas says:
23/10/2018 at 12:23 pm

Thanks.

Gerardo says:
06/09/2018 at 11:20 pm

Is the ldap configuration still a part of the RHCE? I dont see that as an objective only the configuration for kerberos using a keytab file.

Reply

Tomas says:
07/09/2018 at 12:28 pm

I think RHCE objectives require you to know Kerberos only. LDAP is part of RHCSA objectives.

Mykhailo Kravchuk says:
14/09/2018 at 9:53 pm

Hi,

I would like to ask about sssd. I made configuration on RH 7.2 with sssd and got a problem, that secondary groups (configured on IPA server) aren’t available. Only I have such problem when sssd is enabled? With nslcd everything is working.
Basically it isn’t the big problem until will be needed setup with group collaboration.
Found this discussion: https://www.redhat.com/archives/freeipa-users/2016-July/msg00284.html

Reply

Tomas says:
15/09/2018 at 10:45 am

Thanks for your feedback. If nslcd works for you then it makes sense to use nslcd.

Ovitus says:
27/11/2018 at 5:12 pm

Do we know what version of RHEL the exam is based on? Also any hint as to whether the admin credentials for the FreeIPA server are given or not? I would like to use ipa-client-install, as I still haven't gotten this process working in getting Kerberos setup correctly.

Reply

Tomas says:
27/11/2018 at 5:26 pm

The exam is based on RHEL 7.

You need to know how to configure Kerberos client without admin credentials.

Ovitus says:
28/11/2018 at 3:23 pm

Is the keytab file provided? I've read that you can use that with 'ipa-client-install -k keytabfile' to avoid having to enter admin credentials, it would save allot of time on the exam if that's the case.

I've read some saying it was 7.0 and others stating it was a later release like 7.1+. My concern is with NFS with Kerberos and the difference in setup. I think on later releases certain things like nfs-secure-server and nfs-secure don't need to be started?

Tomas says:
28/11/2018 at 4:54 pm

You need to know how to use the keytab file.

If you practise Kerberos configuration on different RHEL releases, then it won't matter which version the exam is on. You can always contact Red Hat to clarify the OS version.

atpal says:

30/01/2019 at 3:06 am

Hi, Great material!
Quick question, I had setup kerberos auth from authconfig-tui -> Checked(use ldap, use shadow password, use ldap auth,use kerberos), and the put the kdc info etc.. It starts the nslcd service. however if i just use ldap auth without kerberos sssd works. I want sssd to be working with kerberos as well..Am i missing something?

Reply

martin says:
01/02/2019 at 11:28 pm

You can not use both at same time, choose nslcd or sssd. if you want to use sssd you need to install it, and then do not forget to enable it USESSSD=yes in /etc/sysconfig/authconfig before start of authconfig-tui utility.

If you start authconfig-tui before you usually get a problem because /etc/sssd/sssd.conf is not generated, so it need to be troubleshooted.

atpal says:
08/05/2019 at 4:49 am

Hi,
I have an issue with kerberos sssd, i am able to su to the ldap user but unable to ssh to the client machine with ldap user, and also logs show its looking for nslcd. I want it to default to sssd. wondering what I could be doing wrong?
[root@ipaclient cacerts]# egrep -i 'sssd|leg' /etc/sysconfig/authconfig
FORCELEGACY=no
USESSSD=yes
USESSSDAUTH=yes

May 7 23:45:15 ipaclient sshd[1801]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.10.0.1 user=alice
May 7 23:45:15 ipaclient sshd[1801]: pam_krb5[1801]: authentication fails for 'alice' (alice@RHCE.LOCAL): Authentication failure (Preauthentication failed)
May 7 23:45:15 ipaclient sshd[1801]: pam_ldap(sshd:auth): error opening connection to nslcd: No such file or directory
May 7 23:45:17 ipaclient sshd[1801]: Failed password for alice from 192.168.4.29 port 38104 ssh2

May 7 23:45:15 ipaclient sshd[1801]:
pam_unix(sshd:auth): authentication failure; logname=
uid=0 euid=0 tty=ssh ruser= rhost=192.168.4.29
user=alice
May 7 23:45:15 ipaclient sshd[1801]: pam_krb5[1801]:
authentication fails for ‘alice’ (alice@RHCE.LOCAL):
Authentication failure (Preauthentication failed)
May 7 23:45:15 ipaclient sshd[1801]:
pam_ldap(sshd:auth): error opening connection to nslcd:
No such file or directory
May 7 23:45:17 ipaclient sshd[1801]: Failed password for
alice from 192.168.4.29 port 38104 ssh2

Ivan says:
05/05/2019 at 6:52 am

I’m puzzled as to what I am doing wrong. I follow all the steps, every thing looks like it’s going well, then when I try to su – alice from either srv1 or srv2 it says:

[root@srv1 openldap]# su – alice
su: user alice does not exist

If I try it with kerberos, it does the same thing. However if I do the kinit alice it will ask for the password for that user, and accept it. I can then ssh to the IPA server and it works, I just can’t do a su – alice from either srv1 or srv2.

Any thoughts as to what I might be missing here?

Reply

Ivan says:
05/05/2019 at 3:07 pm

I found out what needed to be changed. I’m using a RHEL 7.0 Server (as the exam still is based on RHEL 7.0, however very soon it will be RHEL 8).

Anyway, I had to make the following changes:

yum groupinstall “Directory Client”
wget -P /etc/openldap/cacerts/
ftp://prometheus.home.therootuser.com/pub/ca.crt
This was instead of the cacert.p12 file that you said to copy over.
rm /etc/openldap/cacerts/cacert.p12
systemctl enable sssd; systemctl restart sssd

systemctl status sssd
su – alice

At that point, it worked.

Cheers,

Ivan Windon

*Mike_* says:
08/10/2019 at 2:02 am

Hello,
I have a question regarding Kerberos and ssh.

I noticed that after setting up Kerberos on a client and server a test for a user was able to successfully log on as that user using a Kerberos ticket, but only once. E.g. If I exit the logon, up arror to re-logon it fails. This is not intuitive to me; I would think that as long as my ticket is still valid, it should work. If I remove or comment "GSSAPIDelegateCredentials yes" from ssh_config, I can logon numerous times with the same ticket. If I try a second time to the server, it too fails. It's as if the ticket is no longer any good. How should it work? I assumed if I logged out of my test user completely, then the ticket would no longer be valid, but I am still the test user, just logged out of the ssh session.

I am using Centos 7.0.1406 with zero updates from outside sources. There are some bugs in some of these releases, but I am trying to stay as close to the baseline as possible for testing purposes.

Reply

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Post Comment

LOOKUP

Search …

ARCHIVES

Archives

Select Month

CATEGORIES

- AWS (14)
- Database (8)
- DNS (5)
- Exchange Server (6)
- FTP (3)
- High Availability (23)
- LDAP/Kerberos (9)
- Linux (207)
- Mac OS X (2)
- Mail/SMTP (6)
- Monitoring (29)
- Networking (11)
- Notes (9)
- OpenVPN (3)
- Proxy (3)
- Python (4)
- Raspberry Pi (4)
- Samba/NFS (7)
- Security (17)

SSH (2)

Virtualisation (8)

VoIP (4)

Webserver (7)

Windows (24)

RECENT COMMENTS

Tomas on Passed EX436 High Availability Clustering

Tomas on Katello: Import CentOS Errata into Pulp

Tomas on Passed EX280 OpenShift Administration

Tomas on Anthy Keyboard to Write in Hiragana and not Katakana

Binu on Anthy Keyboard to Write in Hiragana and not Katakana