

# Re: Kerberos authenticatino and ldap authorization

---

*Source:* <http://unix.derkeiler.com/Mailing-Lists/FreeBSD/questions/2007-03/msg00578.html>

---

- *From:* Tillman Hodgson <[tillman@xxxxxxxxxxxxxxxxxxx](mailto:tillman@xxxxxxxxxxxxxxxxxxx)>
  - *Date:* Wed, 7 Mar 2007 19:31:19 -0600
- 

On Wed, Mar 07, 2007 at 02:43:15AM -0700, RJ45 wrote:

there are many difficulties and YES there is the documentation on FreeBSD handbook but it does not helped me so much I Still ahve difficulties.

I isntalled MIT krb5 also and I Am using kadmin from MIT to manage krb5 server.

So no possibility of \$PATH problems?

First problem

```
kadmin: ktadd -k /etc/krb5.keytab host/host.domain
kadmin: Unsupported key table format version number while adding key to
keytab
```

I can't undertand this message i touched /etc/krb5.keytab but via kadmin it is unable to export the krb5 key I added before with

Touching it ahead of time shouldn't be necessary. Your syntax might be off, I'm not sure because it looks like you've made it "generic" for purposes of posting it to the list. Here's a cut'n'paste of "live" data of me doing it (the host has been decommissioned recently, and I haven't yet deleted the host key from the KDC, which I'll do shortly):

```
[root@surya ~]# ls -l /etc/test.keytab
ls: /etc/test.keytab: No such file or directory
```

```
[root@surya ~]# kadmin.local
Authenticating as principal toor/admin@xxxxxxxxxxxxxxxx with password.
kadmin.local: getprinc -terse host/blues.seekingfire.prv@xxxxxxxxxxxxxxxx
"host/blues.seekingfire.prv@xxxxxxxxxxxxxxxx" 0 1037304860 0 2419200 "toor/admin@xxxxxxxxxxxxxxxx"
1037300
kadmin.local: ktadd -k /etc/test.keytab
```

## Re: Kerberos authenticatino and ldap authorization

```
host/blues.seekingfire.prv@xxxxxxxxxxxxxxxxx
Entry for principal host/blues.seekingfire.prv@xxxxxxxxxxxxxxxxx with kvno 6, encryption type Triple DES
cbc mode with HMAC/sha1
Entry for principal host/blues.seekingfire.prv@xxxxxxxxxxxxxxxxx with kvno 6, encryption type DES cbc
mode with CRC-32 added to keytab
kadmin.local: exit
```

```
[root@surya ~]# ls -l /etc/test.keytab
-rw----- 1 root wheel 164 Mar 7 19:15 /etc/test.keytab
```

```
[root@surya ~]# ktutil
ktutil: read_kt /etc/test.keytab
ktutil: list
slot KVNO Principal
-----
```

---

```
1 6 host/blues.seekingfire.prv@xxxxxxxxxxxxxxxxx
2 6 host/blues.seekingfire.prv@xxxxxxxxxxxxxxxxx
ktutil: exit
```

So it does indeed work.

```
addprinc -randkey host/host.domain
```

```
i also chmod 777 krb5.keytab nothing to do
```

chmod 777 on a keytab is a very very bad thing to do :-)

If someone can read your keytab, it opens the door to impersonating that principal.

at the end I exported it from the kdc and copied it by hand in /etc/krb5.keytab on my client FreeBSD box, but I do not know if in this way it will work.

I'm never tried it -- it definitely doesn't sound like it'd be fun to type in, however :-)

I tend to extract my keytabs right on the KDC and then scp them to the appropriate host. I don't use kadmin for remote admin -- if I need to admin the KDC, I log in via the serial console and use kadmin.local to keep everything off the network.

anyway now I have another problem.  
I am not able to configure ssh to login via kerberos.

## Re: Kerberos authenticatino and ldap authorization

I tryed everything

```
KerberosAuthentication yes
KerberosOrLocalPasswd yes
KerberosTicketCleanup yes
```

Kerberos\* is, counterintuitively, not what you want. Google for "sshd\_config GSSAPI".

At the end anyway the scenario needs to be krb5 for authentication and LDAP for authorization

I use Kerberos for authentication and NIS-over-IPsec (transport mode), which is very similar. I have a cross-realm trust to another Realm that uses Kerberos and flat files, also on BSD. It's definitely doable.

For now I am not able to authenticate via krb5  
any hints ?

Get some basic troubleshooting information in place by trying the following tests and posting the results to the list:

- \* Have a running KDC computer, a workstation computer, and a server computer that can run a Kerberos service (let's say it's the kerberos telnetd for this example). Ensure that all their clocks are in sync. Ensure that all computers have full naem resolution correctly working.
- \* Confirm the KDC is running and that you ave at least one valid user principal and one valid host principal created. The user principal should also exist in /etc/passwd and the other flat files on both the workstation and the server computer.
- \* Confirm that your /etc/krb5.conf on the KDC sets your default realm and gives the hostname of the KDC
- \* From the KDC, confirm that you can kinit and obtain a TGT (test with klist)
- \* From a workstation with the krb5.conf installed, confirm that you can kinit and obtain a TGT (test with klist)
- \* From a workstation with the krb5.conf, attempt to use a kerberos service on the host that has the valid host principal. Confirm with klist that you're able to obtain the host service ticket.
- \* On the KDC, extract (ktadd) the server principal to a keytab file. Securely copy it (scp is fine) to the server host and ensure it's named /etc/krb5.keytab. Permissions should be 600 and owned by root.
- \* Attempt to use the kerberos telnet client to connect to the kerberos host with the valid host principal (i.e., `telnet -x server\_host`). You should be able to connect and login passwordless.

Re: Kerberos authenticatino and ldap authorization

If any of those steps don't work, please post back to the list with details on what worked, what didn't work, and what the resulting error messages were.

-T

--

"What is Zen?"

"Not always so."

- Shunryu Suzuki

---

freebsd-questions@xxxxxxxxxxx mailing list

<http://lists.freebsd.org/mailman/listinfo/freebsd-questions>

To unsubscribe, send any mail to "freebsd-questions-unsubscribe@xxxxxxxxxxx"