

AD Kerberos Troubleshooting

A short troubleshooting guide for Kerberos and Active Directory

📅 14 Aug 2014 - 09:24 | 📄 Version 3 | 👤 Daniel Lauk | 🏠 Domain

This topic briefly describes how to identify the cause of Kerberos problems with Active Directory and how to fix them.

Table of contents

[Check the computer clocks](#)

[Check DNS](#)

[Check network availability](#)

[Check general Kerberos configuration](#)

[Check the keytab file](#)

[Check that the principal name is unique on the KDC](#)

[Check the supported encryption types of the keys](#)

[Analyze the network traffic](#)

[Further documentation](#)

Check the computer clocks

Make sure that the clocks of all computers use the same time. Watch out for daylight saving time adjustments or time zone differences and be aware that the internal time of your computer and the time your graphical desktop display may be different. For use on PSI campus, **ideally** make sure all systems use PSI's time servers. (TODO: Add URLs of NTP servers)

The Kerberos protocol relies on timestamps to reduce the risk of attacks. The maximum time difference between two communicating systems (aka "clock skew") is 5 minutes.

Check DNS

Make sure, that **both, forward and reverse DNS resolution** work properly. You can find out easily by using the `nslookup` command.

The Kerberos protocol relies on checking the IP address and names via DNS to reduce the risk of attacks.

Example scenario

Let's assume you set up an SSH daemon on a computer named `myserver.psi.ch`. You got a Kerberos keytab for the principal `HOST/myserver.psi.ch@D.PSI.CH` in Active Directory and configured `sshd` correctly to use it. You are logged in locally on the server. You also have a TGT for the `D.PSI.CH` realm. To test, if your Kerberos SSO works, you try `ssh $USER@localhost`, but this fails. This is, because the host name `localhost` does not match the name in the service principal.

Next you try to do `ssh $USER@myserver.psi.ch`, but that still fails. This may be the case, if the `/etc/hosts` file maps `myserver.psi.ch` to `127.0.0.1` instead of the IP address registered in DNS (and your name resolution order uses the local file before querying DNS).

Check network availability

Make sure, that the Kerberos client can contact the KDC. Kerberos uses port 88 on both TCP and UDP. You can use `telnet d.psi.ch 88` to check for connectivity to that port. If that doesn't work, it may be a firewall or routing issue.

Check general Kerberos configuration

Make sure, that the Kerberos client can get "something" from the KDC. To do that, log on to the Kerberos client and obtain a fresh TGT from the KDC by using the `kinit` command. Verify, that it actually worked by using the `klist` command. You should see a ticket for `krbtgt/D.PSI.CH@D.PSI.CH` in the credentials cache.

If that didn't work, check the Kerberos configuration (e.g. `/etc/krb5.conf`).

Check the keytab file

Make sure, that the keytab file is OK.

The first and obvious thing to be checked -- as dull it may seem -- is: Make sure, that the service (and preferably only the service) has read access to the keytab file.

Next, check if the keytab actually contains the service principal, and the key version number ("kvno"). To do that, use the `klist` command (or `ktutil`, depending on your Kerberos implementation).

Third, check that the key version number ("kvno") in the keytab file matches the one on the KDC. To do that, use the `kvno` command.

Finally, check if the keytab works by requesting a TGT for the service principal. To do that, log on to the application server and use `kinit` with the keytab file and principal name of the application server. Verify, that it actually worked by using the `klist` command. You should see a ticket for `krbtgt/D.PSI.CH@D.PSI.CH` in the credentials cache and the credential cache must point out the name of the service principal.

Check that the principal name is unique on the KDC

If `kinit` fails with an error message like "Client not found in Kerberos database while getting initial credentials" (on the network this is protocol error `KRB5KDC_ERR_C_PRINCIPAL_UNKNOWN (6)`), this points at a problem with the setup of the principal names in Active Directory. In fact, this error will occur, if either the principal name is not set at all or if it is not unique (i.e. the same principal is set on multiple users).

Ask an Active Directory domain administrator to run `setspn -Q` for the service principal of the application server (e.g. `setspn -Q HTTP/myserver.psi.ch`). This must return **exactly one** entry!

The domain administrator can also run `setspn -F -X` to check the entire forest for duplicate SPNs. **Caution:** This command *may* take quite long (but at PSI it's usually finished within a few seconds).

In addition to the service principal name (SPN), the **user principal name** (UPN) is set, too, by Active Directory. It may be, that -- by accident -- the Kerberos principal got mapped into the UPN of the wrong account. To check for this error, run an LDAP search with a filter on the `userPrincipalName` attribute (e.g. in PowerShell run `Import-Module 'ActiveDirectory'; Get-ADUser -LDAPFilter '(userPrincipalName=HOST/myserver.psi.ch@D.PSI.CH)'`). This must return **exactly one** entry!

Check the supported encryption types of the keys

Active directory will issue tickets using the strongest encryption mechanism that both client and application server understand. Make sure that the strongest encryption types match.

Analyze the network traffic

Create a network trace to track down the problem. Ideally, you should record a network trace at the same time on both the client and the application server. You should purge the DNS and ticket caches before starting the network trace. (There are several products that can do this: Ethereal, Wireshark, Packetalyzer, Netmon... If in doubt, ask your friendly neighborhood network engineer for support.)

Further documentation

This is an unsorted list of various resources on the internet that deal with Kerberos and its peculiarities.

- <http://blogs.technet.com/askds/archive/2008/03/06/kerberos-for-the-busy-admin.aspx>
 - <http://blogs.technet.com/b/askds/archive/2008/05/14/troubleshooting-kerberos-authentication-problems-name-resolution-issues.aspx>
 - <http://neuntoeter.wordpress.com/2011/03/22/checkliste-fur-kerberos/>
-