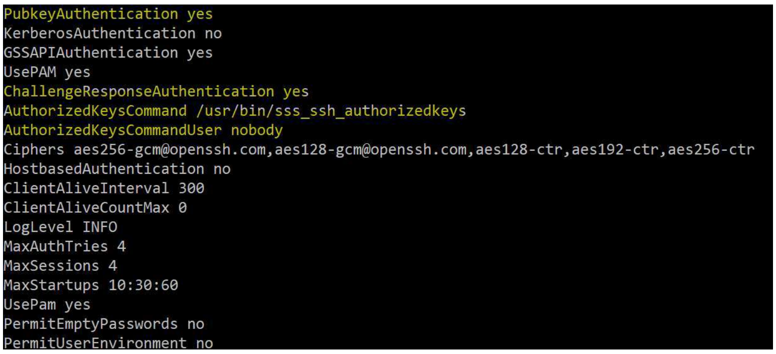
FreeIPA FAQ Troubleshooting and Tips

Q1: My IPA password does not work on the dex box(es), what should I do?
A1: This may be due to the SSSD cache out of sync with the IPA Master, you may login as a local account that has sudo right and run this command TWICE (**sudo sss_cache -E**) and then re-try your IPA login.

Q2: I have tried ‘sudo sss_cache -E’, it did not help, what else could I do?
A2: You may also try to restart sssd System Security Services Daemon (**sudo systemctl restart sssd**) and sshd SSH Server Daemon (**sudo systemctl restart sshd**) and then re-try your IPA login. You should also check SSH Server and Client config files ‘/etc/ssh/sshd_config’ and ‘/etc/ssh/ssh_config’ and append ‘-vvv’ to SSH client command line so as to troubleshoot. Further you may enable DEBUG syslog level in SSH Server daemon and check ‘/var/log/auth.log’ or ‘/var/log/syslog’.

Q3: My devbox SSH Server has been setup with both PublicKey (SSH Key) and ChallengeResponse (password) Authentication, the password login is working however SSH Key login is not, why?
A3: Make sure you have these config lines in ‘/etc/ssh/sshd_config’ and restart sshd. Sometimes due to some reasons the two (**AuthorizedKeyCommand** and **AuthorizedKeyCommandUser**) lines are missing. In the last resort, uninstall FreeIPA client and re-install.



```
PubkeyAuthentication yes
KerberosAuthentication no
GSSAPIAuthentication yes
UsePAM yes
ChallengeResponseAuthentication yes
AuthorizedKeysCommand /usr/bin/sss_ssh_authorizedkeys
AuthorizedKeysCommandUser nobody
Ciphers aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr
HostbasedAuthentication no
ClientAliveInterval 300
ClientAliveCountMax 0
LogLevel INFO
MaxAuthTries 4
MaxSessions 4
MaxStartups 10:30:60
UsePam yes
PermitEmptyPasswords no
PermitUserEnvironment no
```

Q4: How could I check my IPA account detatils?
A4: There are many ways, ‘**id -a**’, ‘**getent passwd my.ipaaccount**’, ‘**getent group my.ipagroup**’, ‘**kinit my.ipaaccount**’ followed by ‘**ipa user-show my.ipaaccount**’.

Q5: How could I check my IPA account password expiration, sudoers right (aka sudoRule in FreeIPA) and Host Based Access Control (HBAC) policy details?
A5: Get a Kerberos ticket (**kinit my.ipaacount**), run ‘**ipa user-show my.ipaaccount --all**’. It is better to run ‘**sudo -l**’ and HBAC test ‘**hbactest**’ just to confirm.

Q6: Can IPA account be granted local sudo right?
A6: Yes, either via ‘**wheel**’ (RHEL) or ‘**sudo**’ (ubuntu) local group or local ‘**/etc/sudoers.d/xxx**’ definition.

Q7: Can IPA account be setup as application/service account and not being able to perform interactive login?
A7: Yes, just like local account, define its login shell as ‘**/bin/false**’ or ‘**/usr/bin/nologin**’.

Q8: Can I use SSH key to do password-less login to IPA account?
A8: Yes, get a Kerberos ticket (**kinit my.ipaacount**), then run ‘**ipa user-mod my.ipaacount --sshpubkey=”$(cat id_rsa.pub)”**’.

Q9: How can I perform Host Based Access Control policy test?
A9: Get a Kerberos ticket (**kinit my.ipaacount**), run ‘**ipa hbactest --user my.ipaacount --host centos8.example.local --service sshd**’.

Q10: I run ‘**kinit my.ipaacount**’, it throws error message ‘**kinit: Unknown credential cache type while getting default ccache**’, what should I do?
A10: You have other search path example ~/anaconda3/bin that provides the kinit binary, simply **replace ‘kinit’ with ‘/usr/bin/kinit’**.

Q11: I have ‘**AllowUsers**’, ‘**DenyUsers**’, ‘**AllowGroups**’ and ‘**DenyGroups**’ directives with IPA users/groups definition in SSH Sever config ‘/etc/ssh/sshd_config’, will it work with IPA Host Based Access Control?
A11: No, this is specific to a particular host and not centralized control, please **re-design and use FreeIPA HBAC policy**.

=== End of doc ===