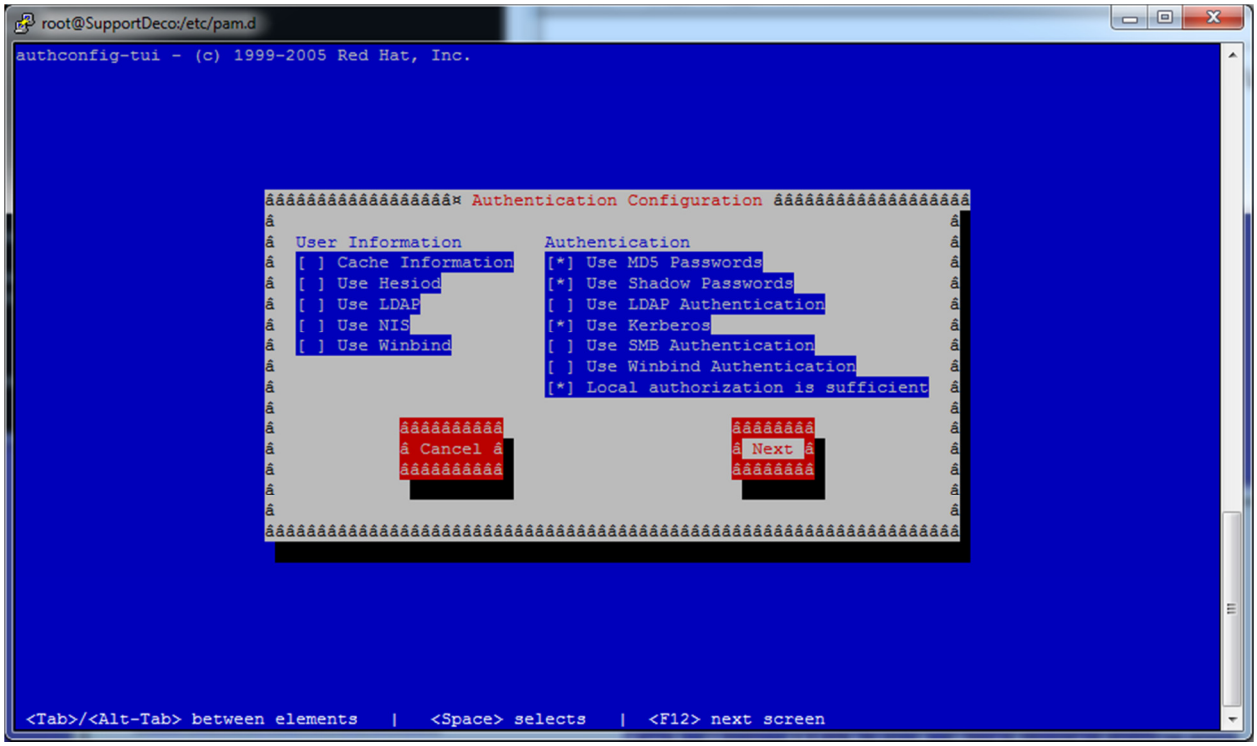
# Active Directory Authentication

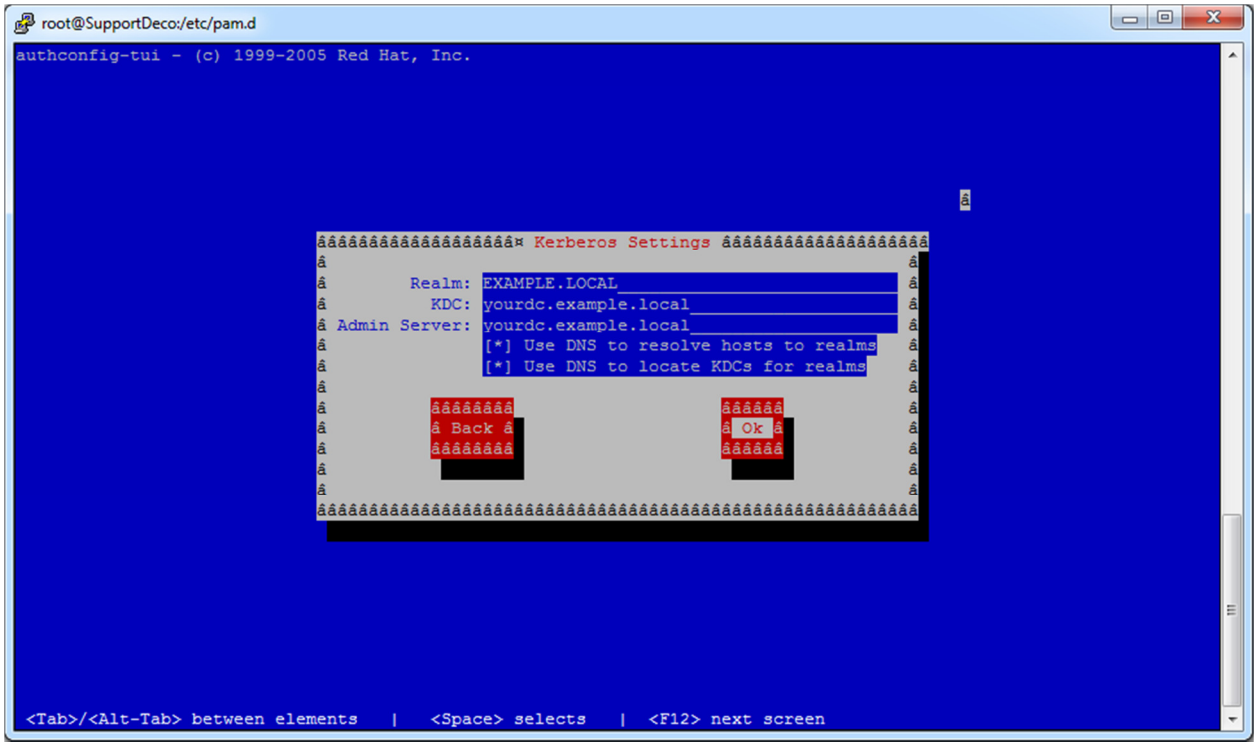
## Prerequisites:

1. Ensure that your appliance's clock is set correctly, preferably using NTP against the domain controller you will be authenticating to. Kerberos operation requires that client and server clocks be closely synced.
2. It is best practice to have DNS configured correctly on your appliance. Your DNS server should be a domain controller or other DNS server that has the Active Directory DNS records.

## Fedora 9-based Appliances

1. Log into your appliance via ssh as *root.*
2. Run *authconfig-tui* from the command line. Select "Use Kerberos" and "Local authorization is sufficient."
3. 

4. Choose *Next.*

5. Enter your Kerberos realm, which should be your Active Directory domain name in ALL CAPS (this must be done in all caps).
6. Set your KDC and Admin Server to your AD domain controller.
7. Check “Use DNS to resolve hosts to realms” and “Use DNS to locate KDCs for realms.”
8. 

9. Choose *Ok.*
10. You should now be back at a command line. Enter “kinit <YourADUserName>” to test Kerberos authentication. Enter your AD password when prompted. The command will produce no output if it is successful, but will generate an error if it fails.

**Things to check in the event of a failure: Is your *resolv.conf* file set up correctly for DNS? Is your appliance’s clock synced with your domain controller using NTP?**

11. Edit the NetWitness config file so that the appliance can authenticate against AD. You can do so in Administrator under Files, and “Netwitness” in the pull down menu.
12. Comment out all lines in the Netwitness file and add the following line at the end:
    “*auth required pam_krb5.so no_user_check*”

```
##
## This configuration file configures NetWitness to use PAM login modules
## for authentication when setting the External Auth Type option for Netwitness User
Accounts.
## For more information see the Linux-PAM System Administrators Guide
## http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/Linux-PAM_SAG.html
##
## Sample of standard UNIX authentication
##
#auth required pam_unix.so
#account required pam_deny.so
#password required pam_deny.so
#session required pam_deny.so
auth    required        pam_krb5.so no_user_check
```

13. You will now need to define the username via the NetWitness Admin User Management interface. Create a user and set the authentication source to External. Add the user to the proper group and save.
14. After the user has been created, try connecting via Investigator using that account. If you’re having trouble, look for error messages in */var/log/secure*.