

Using Kerberos to Authenticate to ASURITE

\$Date: 2004/06/22 17:45:38 \$ \$Revision: 1.4 \$

1 Introduction

This document describes how to configure Red Hat Linux to use Kerberos to authenticate to the ASURITE domain. Under this configuration, each user must be specifically authorized to have access to a machine. If you would like to configure the machine to allow access to any user with an ASURITE account, without manual per-user configuration, see the document “Using Kerberos, LDAP, and AFS with ASURITE.”

2 Prerequisites

Before you begin you must have the following packages installed. These packages are all available as part of the Red Hat distribution.

```
krb5-libs
krb5-workstation
krbafs
pam_krb5
```

To simplify configuration you can use GUI tools provided by Red Hat. These tools are provided by

```
authconfig
authconfig-gtk
```

3 Configuring Kerberos

The first step is to configure Kerberos to authenticate to the ASURITE domain. Edit the file `/etc/krb5.conf` to include the following:

```
[libdefaults]
    default_realm = ASU.EDU
    default_tkt_enctypes = des3-hmac-sh1 des-cbc-crc
    default_tgs_enctypes = des3-hmac-sh1 des-cbc-crc

[realms]
ASU.EDU = {
    kdc = krb1.asu.edu:88
    kdc = krb2.asu.edu:88
    kdc = krb3.asu.edu:88
    admin_server = krb1.asu.edu:749
    default_domain = asu.edu
}

[domain_realm]
    .asu.edu = ASU.EDU
    asu.edu = ASU.EDU
```

You will also need to edit the files `/etc/krb.conf` and `/etc/krb.realms` for compatibility with Kerberos v4. The file `krb.conf` should contain the following:

```
ASU.EDU
ASU.EDU authen1.asu.edu
ASU.EDU authen2.asu.edu
ASU.EDU author2.inre.asu.edu admin server
```

and `krb.realms` should contain:

```
.asu.edu asu.edu
.inre.asu.edu asu.edu
```

The next step is to configure the operating system to use Kerberos to authenticate users.

4 Configuring PAM

Red Hat uses PAM (Pluggable Authentication Modules) for authentication. Since most Linux applications that perform authentication use PAM, changing the system-wide PAM configuration can change the way the system uses authentication without making changes to each application.

4.1 Automatic Configuration Tools

If you have the `authconfig` and `authconfig-gtk` packages installed, you can run `redhat-config-authentication` to configure PAM to use Kerberos. Choose the tab labeled “Authentication” and select the checkbox “Enable Kerberos Support”. You do not have to click “Configure Kerberos” because the appropriate settings have already been added to `krb5.conf`. Choose “OK” to apply the changes.

If you have the `authconfig` package installed but not `authconfig-gtk`, you can run a console-based program to make the same changes. Run `authconfig` as root. From the first page of settings, choose “Next”. On the second page choose “Use Kerberos 5”. The Kerberos settings in the right-hand column should show the settings added to `krb5.conf`. Choose “OK” to apply the changes.

4.1.1 Important Addition

The version of PAM included with all recent versions of Red Hat (including Red Hat 9 and Red Hat Enterprise 3) has a bug that makes it impossible for local users (including root) to log in if the machine loses network connectivity. As a workaround, it is necessary to edit the PAM configuration file by hand, even if you use the automatic configuration tools described above.

Edit the file `/etc/pam.d/system-auth` and add the following line to the account section:

```
account      sufficient    /lib/security/$ISA/pam_localuser.so
```

In the account options line (beginning with `account [default=bad ...]`) add the following directive:

```
authinfo_unavail=ignore
```

4.2 Manual Configuration

If you don't have `authconfig`, you can manually edit the PAM configuration file. The file `/etc/pam.d/system-auth` should contain the following:

```
auth      required    /lib/security/$ISA/pam_env.so
auth      sufficient  /lib/security/$ISA/pam_unix.so likeauth nullok
auth      sufficient  /lib/security/$ISA/pam_krb5.so use_first_pass
auth      required    /lib/security/$ISA/pam_deny.so

account   required    /lib/security/$ISA/pam_unix.so
account   sufficient  /lib/security/$ISA/pam_localuser.so
account   [default=bad success=ok user_unkown=ignore service_err=ignore
```

```

system_err=ignore authinfo_unvail=ignore] /lib/security/$ISA/pam_krb5.so

password    required    /lib/security/$ISA/pam_cracklib.so  retry=3 type=
password    sufficient  /lib/security/$ISA/pam_unix.so  nullok use_authtok md5
shadow
password    sufficient  /lib/security/$ISA/pam_krb5.so  use_authtok
password    required    /lib/security/$ISA/pam_deny.so

session     required    /lib/security/$ISA/pam_limits.so
session     required    /lib/security/$ISA/pam_unix.so
session     optional   /lib/security/$ISA/pam_krb5.so

```

Note that the account options line (`account [default=bad ...] ... pam_krb5.so`) should be entered as one long line, not wrapped as shown here.

5 Finishing Up

After Kerberos and PAM have been configured, the system should be ready to authenticate to ASURITE. The final step is to create local accounts for users who should have access to the machine. This is done with the `useradd` command. You do not have to set a password for the user (this will be handled by Kerberos) but you should take care to set the numeric UID to match the user's ASURITE UID. This is required to gain access to the NetApp's NFS shares. To add a user with a certain UID, run the command `useradd -u uid username`.

Note that any kernel version prior to 2.4 cannot handle the large UIDs used by ASU. To determine the version of the kernel on a machine, you can run `uname -r`. If it is not 2.4.x, you must upgrade the kernel to finish the installation.

If you would like to configure the machine for AFS access, see the document "Accessing ASU Shared File Space." Some notes about this configuration:

- The configuration changes take effect immediately. There is no need to reboot the machine.
- Under this configuration, a user can authenticate successfully using either a local password (if a local account exists) or a Kerberos password.
- No special changes are needed to allow for graphical logins using `xdm` or `gdm`.