

Chapter 18: Additional UNIX Sysadmin

Information for Off-Site Installations

In this chapter, we discuss some miscellaneous issues that sysadmins of off-site Kerberos installations should be aware of. Also see Chapter 6: *Logging In from Off-Site*.

18.1 root access to /usr

The binaries for the **kerberos** product go into `/usr/krb5`, so you don't need access to `/usr/local`. As long as you have *root* access to `/usr`, you can install the product.

18.2 Obtaining the krb5.conf File

We recommend that you use the most recent **UPS** tar file for `krb5.conf` from `ftp://ftp.fnal.gov/products/krb5conf/` (as of this writing, December 4, this would be `ftp://ftp.fnal.gov/products/krb5conf/v1_5/NULL/krb5conf_v1_5_NULL.tar`). The `krb5.conf` template is updated from time to time. These updates are announced on the *kerberos-announce* mailing list.

If you're not running **UPS**, untar it and look at the top of the `installAsRoot` script for instructions on how to install it without **UPS**. If you're not running AFS, check to be sure that the `installAsRoot` script changes the line in `/etc/krb5.conf` to:

```
krb5_run_aklog = false
```

The `krb5.conf.template` file from the `krb5conf` product now has lines containing `xMYREALMx` and `xMYNODEx` which have to be edited if doing a manual installation. To join the FNAL.GOV production realm, change `xMYREALMx` to `FNAL.GOV` and `xMYNODEx` to the fully-qualified name of host.

18.3 When your Node is in a Different Domain

If your machine is part of a different domain than `.fnal.gov`, you need to inform applications (e.g., **rsh**, **rlogin**, **telnet**, **FTP**) that it is part of the `FNAL.GOV` strengthened realm. There are two ways to do this:

The First Way:

In the `[domain_realm]` section of the `/etc/krb5.conf` file on the systems from which you'll be logging on, add lines of the form:

```
<domain> = FNAL.GOV
```

with and without the leading dot, e.g.,

```
.myuniv.edu = FNAL.GOV
```

```
myuniv.edu = FNAL.GOV
```

(You only need to add the domain without the leading dot if the undotted form is the name of some host, which is sometimes the case.) This tells applications that any node in this domain should be assumed to be in the `FNAL.GOV` realm. Otherwise the host's realm is taken to be the hostname's domain portion converted to upper case.

Since the **krb5conf** product can be updated independently of each new release of the Fermi **kerberos** product, you can send mail to *nightwatch@fnal.gov* to request that your domain be added to the template.

The Second Way:

Whenever you run one of the network connection applications (except **FTP**), just add **-k FNAL.GOV** to the command line, e.g.,:

```
% telnet -x -k FNAL.GOV mynode.myuniv.edu
```

18.4 Connecting from One Off-Site Domain to Another

This concerns connections between two Kerberized machines in the `FNAL.GOV` strengthened realm where neither is in the `fnal.gov` domain and they are in different domains from each other, e.g., *mynode.myuniv.edu* and *yournode.youruniv.edu*. In order for one of these Kerberized machines to connect directly to the other via **telnet** or **FTP**, the `/etc/krb5.conf` file

on each must contain the `[domain_realm]` mapping for both off-site domains. This does not concern portal mode where the client machine is unstrengthened.

