NAME

kerberos – introduction to the Kerberos system

DESCRIPTION

The Kerberos system authenticates individual users in a network environment. After authenticating yourself to Kerberos, you can use the **kerberos** authentication option of network services such as NFS. In addition, in some environments you can use network utilities such as **rlogin**(1), **rcp**(1), and **rsh**(1) without having to present passwords to remote hosts and without having to bother with **.rhosts** files. See your system administrator for more information about Kerberos support at your site.

Before you can use Kerberos, you must be registered as a user in the Kerberos database. You can use the **kinit**(1) command to find out your status. This command tries to log you into the Kerberos system. **kinit** will prompt you for a username and password. Enter your username and password. If the utility lets you login without giving you a message, you have already been registered.

If you enter your username and **kinit** responds with this message:

Principal unknown (kerberos)

you haven't been registered as a Kerberos user. See your system administrator.

A Kerberos name contains three parts. The first is the *principal name*, which is usually a user's or service's name. The second is the *instance*, which in the case of a user is usually NULL. Some users may have privileged instances, however, such as **root** or **admin**. In the case of a service, the instance is the name of the machine on which it runs; that is, there can be an NFS service running on the machine ABC, which is different from the NFS service running on the machine XYZ. The third part of a Kerberos name is the *realm*. The realm corresponds to the Kerberos service providing authentication for the principal. For example, at MIT there is a Kerberos running at the Laboratory for Computer Science and one running at Project Athena.

When writing a Kerberos name, the principal name is separated from the instance (if not NULL) by a period, and the realm (if not the local realm) follows, preceded by an ''@'' sign. The following are examples of valid Kerberos names:

billb
jis.admin
srz@lcs.mit.edu
treese.root@athena.mit.edu

When you authenticate yourself with Kerberos, typically through the **kinit** command, Kerberos gives you an initial Kerberos *ticket*. (A Kerberos ticket is an encrypted protocol message that provides authentication.) Kerberos uses this ticket for network utilities such as NFS, **rlogin** and **rcp**. The ticket transactions are done transparently, so you do not have to worry about their management.

Note, however, that tickets expire. Privileged tickets, such as root instance tickets, expire in a few minutes, while tickets that carry more ordinary privileges may be good for several hours or a day, depending on the installation's policy. If your login session extends beyond the time limit, you will have to re-authenticate yourself to Kerberos to get new tickets. Use the **kinit** command to re-authenticate yourself.

If you use the **kinit** command to get your tickets, you can use the **kdestroy**(1) command to destroy your tickets before you end your login session. For more information about the **kinit** and **kdestroy** commands, see the **kinit**(1) and **kdestroy**(1) manual pages.

Currently, Kerberos supports NFS and other RPC network services using the **AUTH_KERB** authentication type. In some environments, the following network services are also supported: **rlogin**, **rsh**, and **rcp**. Other services are being worked on, such as the **pop** mail system, but are not yet available.

SEE ALSO

kdestroy(1), **kinit**(1), **klist**(1), **kerbd**(1M), **kerberos**(3N), **krb.conf**(4)

BUGS

Kerberos will not do authentication forwarding. In other words, if you use **rlogin** to login to a remote host, you cannot use Kerberos services from that host until you authenticate yourself explicitly on that host. Although you may need to authenticate yourself on the remote host, be aware that when you do so, **rlogin** sends your password across the network in clear text.

AUTHORS

Steve Miller, MIT Project Athena/Digital Equipment Corporation
Clifford Neuman, MIT Project Athena

The following people helped out on various aspects of the system:

Jeff Schiller designed and wrote the administration server and its user interface, **kadmin**. He also wrote the **dbm** version of the database management system.

Mark Colan developed the Kerberos versions of **rlogin**, **rsh**, and **rcp**, as well as contributing work on the servers.

John Ostlund developed the Kerberos versions of **passwd** and **userreg**.

Stan Zanarotti pioneered Kerberos in a foreign realm (LCS), and made many contributions based on that experience.

Many people contributed code and/or useful ideas. These include, Jim Aspnes, Bob Baldwin, John Barba, Richard Basch, Jim Bloom, Bill Bryant, Rob French, Dan Geer, David Jedlinsky, John Kohl, John Kubiatowicz, Bob McKie, Brian Murphy, Ken Raeburn, Chris Reed, Jon Rochlis, Mike Shanzer, Bill Sommerfeld, Jennifer Steiner, Ted Ts'o, and Win Treese.

RESTRICTIONS