NAME

k5login − Kerberos V5 acl file for host access

DESCRIPTION

The .k5login file, which resides in a user's home directory, contains a list of the Kerberos principals. Anyone with valid tickets for a principal in the file is allowed host access with the UID of the user in whose home directory the file resides. One common use is to place a .k5login file in root's home directory, thereby granting system administrators remote root access to the host via Kerberos.

EXAMPLES

Suppose the user **alice** had a .k5login file in her home directory containing just the following line:

```
bob@FOOBAR.ORG
```

This would allow **bob** to use Kerberos network applications, such as ssh(1), to access **alice**'s account, using **bob**'s Kerberos tickets. In a default configuration (with **k5login_authoritative** set to true in *krb5.conf*), this .k5login file would not let **alice** use those network applications to access her account, since she is not listed! With no .k5login file, or with **k5login_authoritative** set to false, a default rule would permit the principal **alice** in the machine's default realm to access the **alice** account.

Let us further suppose that **alice** is a system administrator. Alice and the other system administrators would have their principals in root's .k5login file on each host:

```
alice@BLEEP.COM

joeadmin/root@BLEEP.COM
```

This would allow either system administrator to log in to these hosts using their Kerberos tickets instead of having to type the root password. Note that because**bob** retains the K erberos tickets for his own principal, **bob@FOOBAR.ORG**, he would not have any of the privileges that require **alice**'s tickets, such as root access to any of the site's hosts, or the ability to change **alice**'s password.

SEE ALSO

kerberos(1)

AUTHOR

MIT

COPYRIGHT