

NAME

krb5_admind.conf - configuration file for krb5_admind(8)

SYNOPSIS

krb5_admind.conf

DESCRIPTION

krb5_admind.conf is the configuration file for krb5_admind(8). The syntax is a Perl snippet which is evaluated and is expected to set the following variables:

\$allow_fetch is a boolean value which indicates whether krb5_admind(8) is willing to allow clients to directly fetch keys from the Kerberos database. Setting this to true may be necessary at some sites but is generally discouraged as it reduces certain security guarantees. Also see krb5_keytab(8)'s configuration variable *\$use_fetch*. This value defaults to false.

\$allow_fetch_old is a boolean value which indicates whether krb5_admind(8) is willing to allow clients to directly fetch old keys from the Kerberos database. Old keys are those whose version number is smaller than the highest key version number. This makes it possible to recover keys for outstanding tickets after creating a new key. Key recovery makes possible decryption of past traffic, and if possible should not be enabled. This value defaults to false.

\$enable_host_subdomain is a boolean variable that if true allows hosts to manage keys for services whose instance is a direct subdomain of the host. This supports multiple service namespaces on the same machine provided the subdomains all map to the same address (as with e.g. a wildcard *.hostname A record).

%xrealm_bootstrap is a hash which has keys that are Kerberos realms with values that are an array ref of Kerberos realms. If a host authenticates to krb5_admind(8) with a host principal in the key's realm then it will be authenticated to retrieve Kerberos host principals with a matching hostname in any of the realms listed in the value. E.g.

```
%xrealm_bootstrap = (
    'REALM1' => ['REALM2', 'REALM3'],
);
```

means that *host/foo@REALM1* can retrieve keys for *host/foo@REALM2* and *host/foo@REALM3*.

%win_xrealm_bootstrap is a hash that maps a Windows principal to a list of host principals which it may retrieve. The Windows principal's components must be lower case. This hash can be used when migrating from using Windows Active Directory to provide Kerberos for UNIX hosts to a strictly UNIX KDC framework.

%prestash_xrealm is a hash that maps a principal's realm to a list of realms on which the principal is allowed to be prestashed. E.g.

```
%prestash_xrealm = (  
    'REALM1' => ['REALM2', 'REALM3'],  
);
```

means that principals in REALM1 may be prestashed on hosts that are in REALM2 or REALM3.

Syntax errors will terminate parsing causing all subsequent configuration to be ignored and so it is critical that they not be present.

SEE ALSO

krb5_admin(8).

AUTHORS

krb5_admin.conf was written by Roland C. Dowdeswell.