NAME

krb5_verify_init_creds_opt_init, **krb5_verify_init_creds_opt_set_ap_req_nofail**, **krb5_verify_init_creds** - verifies a credential cache is correct by using a local keytab

LIBRARY

Kerberos 5 Library (libkrb5, -lkrb5)

SYNOPSIS

#include <krb5.h>

struct krb5_verify_init_creds_opt;
void
krb5_verify_init_creds_opt_init(*krb5_verify_init_creds_opt *options*);

void
krb5_verify_init_creds_opt_set_ap_req_nofail(*krb5_verify_init_creds_opt *options*, *int ap_req_nofail*);

krb5_error_code
krb5_verify_init_creds(*krb5_context context*, *krb5_creds *creds*, *krb5_principal ap_req_server*,
*krb5_ccache *ccache*, *krb5_verify_init_creds_opt *options*);

DESCRIPTION

The **krb5_verify_init_creds** function verifies the initial tickets with the local keytab to make sure the response of the KDC was spoof-ed.

krb5_verify_init_creds will use principal *ap_req_server* from the local keytab, if NULL is passed in, the code will guess the local hostname and use that to form host/hostname/GUESSED-REALM-FOR-HOSTNAME. *creds* is the credential that **krb5_verify_init_creds** should verify. If *ccache* is given **krb5_verify_init_creds**() stores all credentials it fetched from the KDC there, otherwise it will use a memory credential cache that is destroyed when done.

krb5_verify_init_creds_opt_init() cleans the the structure, must be used before trying to pass it in to **krb5_verify_init_creds**().

krb5_verify_init_creds_opt_set_ap_req_nofail() controls controls the behavior if *ap_req_server* doesn't exists in the local keytab or in the KDC's database, if it's true, the error will be ignored. Note that this use is possible insecure.

SEE ALSO

krb5(3), krb5_get_init_creds(3), krb5_verify_user(3), krb5.conf(5)