KMIGRATE - a Kerberos Migration Utility

The **kmigrate** utility is a tool for migrating existing DCE and MVS users to a Kerberos registry managed by an OS/390 SecureWay Network Authentication and Privacy Service server. The intent is to ease the migration of users who are currently using Kerberos services, with or without DCE, to the IBM Kerberos server and to ease the initial population of a Kerberos registry from an existing RACF registry. This tool analyzes the existing RACF and DCE registries and provides a list of suggested RACF commands to prime the Kerberos registry with Kerberos principals. Where necessary, this tool will also suggest MVS userids for these principals.

This tool will provide suggested Kerberos principals to correspond to DCE principals andMVS userids. No changes will be made to the RACF registry until the customer has a chance to review these suggestions and make changes.

The kmigrate Command

Prime a Kerberos registry using information from RACF and DCE registries.

Format

kmigrate -r racf_db_file [-d dce_principal_file] [-k kerberos_prefix] [-n mvs]
[-o output_file] [-e error_file]

Parameters and Options

-r racf_db_file	Specifies the name of a file or dataset containing the output of RACF dababase unload (IRRDBU00). This file must contain records for users, DCE segments, and Kerberos segments, for the system whose registry is to be primed. Other records will be ignored. This file is required.
-d dce_principal_file	Specifies the name of a file or dataset containing a list of DCE principals. One way to generate such a list is to issue the command 'dcecp -c principal catalog -simplename' and pipe the results to a file. This file is optional. You may omit this file if you have no DCE cell, if you wish to handle defining new userids for DCE users at another time, or if all of the DCE principals you wish to define in the Kerberos registry are cross-linked to MVS userids.
-k kerberos_prefix	Specifies a prefix of 1 to 3 characters to be used in generating MVS userids to go with Kerberos principals. This prefix will be combined with a 4 to 6 digit number to create a 7-character userid. The default prefix is KRB.
-n mvs	(no MVS) Specifies that MVS userids without DCE segments are not to be included in the output file. This causes ADDUSER and ALTUSER commands to be generated for DCE users only. Commands will be generated for DCE principals whether or not they have been cross-linked to MVS userids.
-o output_file	Specifies the name of a file or dataset to contain the output. The default is stdout.
-e error_file	Specifies the name of a file or dataset to contain error data. This file will contain information about MVS userids that cannot easiy be assigned to Kerberos principals because the Kerberos principal already exists, and about DCE principals that cannot be easily resolved uniquely to either MVS userids or Kerberos principals because either the MVS userid already exist or a Kerberos principal already exists. The default is stderr.

Usage Notes

- The **kmigrate** command is run from the Unix System Services shell.
- The purpose of this command is to generate a suggested starter set for a Kerberos registry using the existing MVS userids on the target system, and also to assist in the migration of users from a DCE registry to a Kerberos registry. The DCE principals may or may not be cross-linked to MVS userids.
- This command will generate an input file to be used by a RACF administrator to define Kerberos principals for OS/390 Kerberos. The commands will be generated as follows:
  - For each MVS user, an ALTUSER command will be output to generate a Kerberos segment. If the user has a DCE segment, the Kerberos principal will be the same as the DCE principal. If the user does not have a DCE segment, the Kerberos principal will be the same as the MVS userid.
  - No output will be generated for MVS userids that already have Kerberos segments.
  - For each DCE user that is not an MVS user, an ADDUSER command will be output to generate an MVS user with a Kerberos segment. No other options will be used for ADDUSER. If these are used "as is" the system default group and password will be assigned. The MVS userid will be set to the prefix specified by the -k option (default KRB) followed by a 4-digit to 6-digit number to create a 7-character userid. The Kerberos principal will be set to the DCE principal. The following architected DCE principals will not be

included in the output: hosts/*, nobody, root, daemon, sys, bin, uucp, who, mail, tcb, dce-ptgt, dce-rgy.

  - For all existing DCE users: if the DCE principal name is too long to be used as a Kerberos principal (over 240 characters), the last 240 characters will be used to generate the Kerberos principal.

- Output will be placed in the file indicated by the -o option.
- MVS userids and Kerberos principals need to be unique. In the event that a duplicate Kerberos principal or a duplicate MVS userid would be generated, a message will be output to the file indicated by the -e option.

After the **kmigrate** command is run, the user should examine the output file and the error file. These can be edited as desired to add additional information to ADDUSER and ALTUSER commands and also to modify userids and principals. Conflicts indicated in the error file can be resolved by hand and additional ADDUSER and ALTUSER commands can be added. Records can also be deleted. When all editing is complete, the list can be run in TSO using the EXEC command.

Examples

To generate the ADDUSER and ALTUSER list, where the IRRDBU00 output is in irrdbu00.txt and the DCE principal list is in dcecp.txt, with output to user.txt:

```
kmigrate -r irrdbu00.txt -d dcecp.txt -o user.txt
```

To generate the ADDUSER and ALTUSER list, where the IRRDBU00 output is in dataset G085573.PRIVATE.SUSVT5.RACF and the DCE principal list is in dcecp.txt, with output to dataset G085573.PRIVATE.SUSVT5.KERB:

```
kmigrate -r "//'G085573.PRIVATE.SUSVT5.RACF'"  -d dcecp.txt -o \
"//'G085573.PRIVATE.SUSVT5.KERB'"
```

To generate the same list but using "KR" as a userid prefix and logging errors in error.txt:

```
kmigrate -r irrdbu00.txt -d dcecp.txt -o user.txt -e error.txt -k KR
```

Userids generated by the above command will have the format KRnnnnn (7 characters: 2-character prefix, 5 digits).

Sample Output

The following is an abbreviated sample of output from the **kmigrate** command. Input was taken from the RACF registry and the DCE registry. All other options were allowed to default. Note that users G9VWPF and SUDFS3 already have DCE principals.

```
ADDUSER KRB0001  KERB(KERBNAME('kadmin/changepw'))
ADDUSER KRB0002  KERB(KERBNAME('kadmin/admin'))
ADDUSER KRB0003  KERB(KERBNAME('krbtgt/dcesvt2.krbsvt52.ibm.com'))
ALTUSER XXX      KERB(KERBNAME('XXX'))
ALTUSER WEBSRV   KERB(KERBNAME('WEBSRV'))
ALTUSER WEBADM   KERB(KERBNAME('WEBADM'))
```

```
ALTUSER USER02   KERB(KERBNAME('USER02'))
ALTUSER USER01   KERB(KERBNAME('USER01'))
ALTUSER SUDFS3   KERB(KERBNAME('cell_admin'))
ALTUSER SUDFS2   KERB(KERBNAME('SUDFS2'))
ALTUSER SUDFS1   KERB(KERBNAME('SUDFS1'))
ALTUSER SKRBKDC  KERB(KERBNAME('SKRBKDC'))
ALTUSER SERVICE  KERB(KERBNAME('SERVICE'))
ALTUSER SERVER   KERB(KERBNAME('SERVER'))
ALTUSER SECADMIN KERB(KERBNAME('SECADMIN'))
ALTUSER OMVSKERN KERB(KERBNAME('OMVSKERN'))
ALTUSER ODEROOT  KERB(KERBNAME('ODEROOT'))
ALTUSER NFS      KERB(KERBNAME('NFS'))
ALTUSER MVSSTC   KERB(KERBNAME('MVSSTC'))
ALTUSER IBMUSER  KERB(KERBNAME('IBMUSER'))
ALTUSER G9VWPF   KERB(KERBNAME('g9vwpf'))
ALTUSER CDSD     KERB(KERBNAME('CDSD'))
ALTUSER CDSCLRK  KERB(KERBNAME('CDSCLRK'))
ALTUSER CDSADV   KERB(KERBNAME('CDSADV'))
ALTUSER CANCEL   KERB(KERBNAME('CANCEL'))
ALTUSER BPXROOT  KERB(KERBNAME('BPXROOT'))
```

Procedure for Migrating a DCE Registry to Kerberos

This procedure will prime an OS/390 Kerberos registry with principals taken from an existing DCE cell and also existing MVS userids.

1. Prepare the IBM Kerberos enviroment. To add Kerberos segments with principals, RACF must be able to determine the name of the local Kerberos realm. The IBM Kerberos server should be installed and configured according to the instructions in the Program Directory and in *OS/390 SecureWay Security Server Network Authentication and Privacy Service Administration* (SC24-5896).
2. Run the RACF Database Unload job (IRRDBU00) according to the instructions in the RACF System Administrator's Guide, and save the output. This should be run on the system where the Kerberos server will reside. If desired, run the resulting file through a sort program to extract records of type 0200 (User basic), 0290 (DCE user), and 02D0 (Kerberos user). This additional step is not required but it will reduce the size of the file that is input to the kmigrate program. Optionally, copy the resulting file to an HFS directory using the oput command.
3. Optional step for DCE customers: Run the dcecp command 'dcecp -c principal catalog -simplename' and pipe the output to a file. Copy the file to an HFS directory.
4. Optional step for DCE customers: Determine the userid prefix to be used for DCE principals who are not already cross-linked to MVS userids. This prefix will be used to generate a userid for each principal. It should be 1 to 3 characters. By default, userids will be of the format KRBnnnn where nnnn is a 4-digit number.
5. Run the **kmigrate** command.
6. Examine the resulting output file and make changes as desired. If the output is in an HFS file, use the TSO **oget** command to move it to a dataset.
7. Run the the output file as a CLIST, trapping output so you can check for errors. This will issue the RACF commands to create and alter MVS userids to add Kerberos segments with the specified principals. **Note:** RACF "special" authority is required in order to execute the ADDUSER and ALTUSER commands.
8. Examine the RACF log files for errors.

Each modified MVS userid will need to have its password changed, to generate a Kerberos key for the principal and enable participation in Kerberos authentication.

As automatically generated, each new MVS userid has a bare-bones definition. The password will start out

expired, and no Kerberos key will be generated for the user. To generate a valid password and Kerberos key, the user can logon through **rlogin** and change the password, or the administrator can change the password to a non-expired value. A Kerberos key will be generated for the principal when the password is changed.