GNU/Linux Administration - Support #167

Backing Up and Restoring Kerberos Database

08/12/2013 10:19 AM - Daniel Curtis

Status:	Closed	**Start date:**	08/12/2013
Priority:	Normal	**Due date:**	
Assignee:	Daniel Curtis	**% Done:**	100%
Category:	Domain Controller	**Estimated time:**	0.50 hour
Target version:		**Spent time:**	0.50 hour

Description

Back U Kerberos Database

- Become superuser on the master KDC.
- Back up the Kerberos database by using the dump command of the kdb5_util command.

```
/usr/sbin/kdb5_util dump [-verbose] [-d dbname] [filename [principals...]]
```

- -verbose: Prints the name of each principal and policy that is being backed up.
- dbname: Defines the name of the database to back up. Note that ".db" is appended to whatever database name is specified, and you can specify an absolute path for the file. If the -d option is not specified, the default database name is /var/krb5/principal, which actually becomes /var/krb5/principal.db.
- filename: Defines the file that is used to back up the database. You can specify an absolute path for the file. If you don't specify a file, the database is dumped to standard output.
- principal: Defines a list of one or more principals (separated by a space) to back up. You must use fully-qualified principal names. If you don't specify any principals, the entire database is backed up.

Example—Backing Up the Kerberos Database

- In the following example, the Kerberos database is backed up to a file called dumpfile. Because the -verbose option is specified, each principal is printed as it is backed up.

```
kdb5_util dump -verbose dumpfile
```

  - *Example output*

```
kadmin/kdc1.eng.example.com@ENG.EXAMPLE.COM
krbtgt/eng.example.com@ENG.EXAMPLE.COM
kadmin/history@ENG.EXAMPLE.COM
pak/admin@ENG.EXAMPLE.COM
pak@ENG.EXAMPLE.COM
changepw/kdc1.eng.example.com@ENG.EXAMPLE.COM
```

Restore a Kerberos Database from a Dumpfile

- To restore a Kerberos database dump from a file, use the kdb5_util load command on one of the KDCs. The syntax is:

```
kdb5_util load [-old] [-b6] [-b7] [-ov] [-verbose] [-update] [-hash] dumpfilename dbname [admi
n_dbname]
```

The kdb5_util load command takes the following options:

- -old: requires the dump to be in the Kerberos 5 Beta 5 and earlier dump format ("kdb5_edit load_dump version 2.0").
- -b6: requires the dump to be in the Kerberos 5 Beta 6 format ("kdb5_edit load_dump version 3.0").
- -b7: requires the dump to be in the Kerberos 5 Beta 7 format ("kdb5_edit load_dump version 4").
- -ov: requires the dump to be in ovsec_adm_export format.

- -verbose: causes the name of each principal and policy to be printed as it is loaded.
- -update: causes records from the dump file to be updated in or added to the existing database. This is useful in conjunction with an ovsec_adm_export format dump if you want to preserve per-principal policy information, since the current default format does not contain this data.
- -hash: causes the database to be stored as a hash rather than a binary tree.

Example—Restoring the Kerberos Database

- Restore the Kerberos Database

```
kdb5_util load dumpfile principal
kdb5_util load –update dumpfile principal
```

If the database file exists, and the -update flag was not given, kdb5_util will overwrite the existing database.

Adding a script to rsnapshot

1. Create backup script to dump Kerberos principals database

```
sudo vi /usr/local/bin/backup_kdb5.sh
```

   - And add the following:

```
#!/bin/bash
#Script to dump Kerberos principals database
kdb5_util dump backupfile
```

2. Make the script executable

```
sudo chmod +x /usr/local/bin/backup_kdb5.sh
```

3. Edit the rsnapshot config file

```
sudo vi /etc/rsnapshot.conf
```

   - And add the script to the end of the rsnapshot configuration file

```
backup_script /usr/local/bin/backup_kdb5.sh  localhost/kdb5dump/
```

Related issues:

Related to GNU/Linux Administration - Feature #163: Installing Kerberos 5 on ...	**Closed**	**08/08/2013**

History

#1 - 02/16/2015 02:30 PM - Daniel Curtis

- Project changed from 22 to GNU/Linux Administration

- Description updated

- Category set to Domain Controller