ods-ksmutil

This is a utility that allows several different actions to be performed (relatively) easily.

On this Page

- Global Options
- Command: --version
- Command: setup
- Command: start|stop|notify
- Command: update
- Command: zone add
- Command: zone delete
- Command: zone list
- Command: repository list
- Command: policy export
- Command: policy import
- Command: policy list
- Command: policy purge (experimental)
- Command: key list
- Command: key export
- Command: key import
- Command: key rollover
- Command: key purge
- Command: key generate
- Command: key ds-seen
- Command: key ksk-retire
- Command: key delete
- Command: backup done
- Command: backup prepare
- Command: backup commit
- Command: backup rollback
- Command: backup list
- Command: database backup
- Command: rollover list
- Command: zonelist export
- Command: zonelist import
- Allowed values

Global Options

```
--config <config>          aka -c
```

Change the conf.xml file that is used, from the default.

Command: --version

```
ods-ksmutil --version              aka -V
```

Report version information

Command: setup

```
ods-ksmutil setup
```

Delete current contents of database (including any keys) and then import repository list, kasp.xml and zonelist.xml into a database.

Command: start|stop|notify

```
ods-ksmutil start|stop|notify
```

Start, stop or SIGHUP the ods-enforcerd

Command: update

```
ods-ksmutil update kasp
ods-ksmutil update zonelist
ods-ksmutil update conf
ods-ksmutil update all
```

Update database by importing contents of kasp.xml, zonelist.xml or the repository list from conf.xml into a database (or all three). For zonelist and conf the update replaces the existing contents of the database (but note the keys are not updated by any of these commands). For kasp the update replaces or adds to the existing content, but does not delete any policies. The command 'ods-ksmutil' policy purge can be used to remove polices with no zones associated with them.

Note that 'update kasp' is equivalent to 'import policy' and 'update zonelist' is equivalent to 'import zonelist'.

Command: zone add

```
ods-ksmutil zone add
```

Add a zone to both zonelist.xml and the database (both locations read from conf.xml).

Options

```
--zone <zone>                    aka -z
[--policy <policy>]              aka -p
[--signerconf <signerconf.xml>]  aka -s
[--input <input>]                aka -i
[--in-type <input type>]         aka -j
[--output <output>]              aka -o
[--out-type <output type>]       aka -q
[--no-xml]                       aka -m
```

- The <input type> and <output type> fields specify what kind of adaptor should be configured for the zone. Valid values are '*File*' (default) and '*DNS*' for both input and output:
    - When using a '*File*' adaptor the <input> field specifies the location of the unsigned zone and the <output> field specifies the location of the signed zone
    - When using a '*DNS*' adaptor the <input> and <output> fields specify the location of the xml file that describes the adapter to be used e.g. *{prefix}/etc/opendnssec/addns.xml*
- Defaults are provided for all options but zone name:
    - --policy will use the '*default*' policy
    - --signerconf will default to use the *{prefix}/var/opendnssec/signerconf/<zone>.xml* file
    - --input will default to *{prefix}/var/opendnssec/unsigned/<zone>* for a '*File*' adaptor or (available from 1.4.3) *{prefix}/var/opendnssec /addns.xml* for a 'DNS' adaptor
    - --in-type will default to '*File*'
    - --output will default to *{prefix}/var/opendnssec/signed/<zone>* for a '*File*' adaptor or (available from 1.4.3) *{prefix}/var/opendnssec /addns.xml* for a 'DNS' adaptor
    - --out-type will default to '*File*'
- The "no-xml" flag is useful when adding a number of zones; it prevents zonelist.xml from being written to thus speeding up the process. If the "no-xml" flag is used then after all the zones have been added then the zonelist file will need to be updated via the command:

```
ods-ksmutil zonelist export
```

Command: zone delete

```
ods-ksmutil zone delete
```

Delete a zone to both zonelist.xml and the database (both locations read from conf.xml).

Options

```
--zone <zone> | --all            aka -z / -a
```

Command: zone list

```
ods-ksmutil zone list
```

List zones from the zonelist.xml

Command: repository list

```
ods-ksmutil repository list
```

List repositories from the database

Command: policy export

```
ods-ksmutil policy export
```

Export a policy from the database in kasp.xml format.

Options

```
--policy <policy> | --all        aka -p / -a
```

Command: policy import

```
ods-ksmutil policy import
```

Update the database with the contents of kasp.xml; identical to "update kasp". (Note this does not delete any policies. The command 'ods-ksmutil' policy purge can be used to remove polices with no zones associated with them.)

Command: policy list

```
ods-ksmutil policy list
```

List policies available.

Command: policy purge (experimental)

```
ods-ksmutil policy purge
```

Delete all policies and associated keys if there are no zones currently using the policy. This command should be used with caution and it is recommended to backup your database before using it.

Command: key list

```
ods-ksmutil key list
```

List information about keys in zone.

Options

```
Pre 1.4.4:
[--verbose]
--zone <zone> | --all            aka -z / -a

1.4.4 and later:
[--verbose]                            aka -v
[--zone <zone>]                        aka -z
[--keystate <state>| --all]            aka -e / -a
[--keytype <type>]                     aka -t
```

By default:

- keys for all zones are listed when using 'ods-ksmutil key list'
- the 'ods-ksmutil key list' command does not list keys in the GENERATE or DEAD state.

In 1.4.4 the command was extended to support filters on key state and key type.

- The --all option now results in a listing of keys in all key states, including GENERATE and DEAD

Command: key export

```
ods-ksmutil key export
```

Export key information in a suitable format for putting into a zonefile

Options

```
--zone <zone> | --all            aka -z
[--keystate <state>]             aka -e
[--keytype <type>]               aka -t
[--ds]                           aka -d
```

Command: key import

```
ods-ksmutil key import
```

Add a key which was created outside of the OpenDNSSEC code into the database

Options

```
--cka_id <CKA_ID>                aka -k
--repository <repository>        aka -r
--zone <zone>                    aka -z
--bits <size>                    aka -b
--algorithm <algorithm>          aka -g
--keystate <state>               aka -e
--keytype <type>                 aka -t
--time <time>                    aka -w
[--check-repository]             aka -C
[--retire <retire>]              aka -y
```

- (Available from 1.4.3) If the --check-repository flag is used then the import will fail if no key with the matching cka_id is available in the repository.

Command: key rollover

```
ods-ksmutil key rollover
```

Rollover active keys on a zone or policy

Options

```
--zone <zone> | --policy <policy>
--keytype <type> | --all
```

"keytype" specifies a single type of key to roll. After running, the enforcer will be woken up so that the signer can be sent the new information.

If the policy that the zone is on specifies that keys are shared then all zones on that policy will be rolled. A backup of the sqlite DB file is made (if appropriate).

From 1.4.1 either the keytype must be specified or the '–all' option is required for this command. This is to avoid the possibility of rolling more keys than intended by accidentally forgetting to specify a key type.

Command: key purge

```
ods-ksmutil key purge
```

Remove keys that are in the "Dead" state from the repository and from the enforcer DB

Options

```
--zone <zone> | --policy <policy>        aka -z | -p
```

Command: key generate

```
ods-ksmutil key generate
```

Create enough keys for the given policy to last for the period of time given by interval.

Options

```
--policy <policy>                   aka -p
--interval <interval>               aka -n

[--zonetotal <zone total>]          aka -Z
--auto-accept                       aka -A
```

- Intervals are specified in the format used in the configuration files, see Configuration.
- (Available in 1.4.2) Optionally specify a total number of zones to generate keys for (default is all the zones on the policy) with the --zonetotal parameter.
- The command predicts the number of keys that will be generated and then the user is requested to confirm the operation. If the --auto-accept parameter is specified the confirmation step is skipped.

Command: key ds-seen

```
ods-ksmutil key ds-seen
```

Indicate that a submitted DS record has appeared in the parent zone (this triggers the completion of a KSK rollover, or the provisioning of a standby KSK).

Options

```
--zone <zone>                           aka -z
--keytag <keytag> | --cka_id <CKA_ID>   aka -x / -k
[--no-notify|-l]                        aka -l
[--no-retire|-f]                        aka -f
```

- Specifiying a zone will speed up the search of keys by narrowing the field but is not mandatory
- cka_id can be used to resolve a keytag clash.
- By default the command will simultaneously move the current key into the retired state. If you wish to delay this step then add the *--no-retire flag* and use the *ksk-retire* command when needed.
- (Available in 1.4.3) By default the command will notify the enforcer there has been a change so that the changes take full effect. If you wish to delay this step then add the *--no-notify* flag and use the *ods-control enforcer notify*command after all the ds-seen commands have been issued.

Command: key ksk-retire

```
ods-ksmutil key ksk-retire
```

Move a key from active to retired (if a replacement key is already active).

Options

```
--zone <zone>                       aka -z
--keytag <keytag>                   aka -x
--cka_id <CKA_ID>                   aka -k
```

Specifiying a zone alone will retire the oldest key in the zone; if the cka_id or keytag are specified then that key will be retired. The specified key must be in the active state, and there must be 2 or more active keys on the zone for this command to work.

Command: key delete

```
ods-ksmutil key delete
```

Remove a key from the system.

Options

```
--cka_id <CKA_ID>                   aka -k
--no-hsm
```

Keys in the GENERATE or DEAD state can be removed from the system at any time as they are not actually being used. The no-hsm flag indicates that the key should be left on the HSM.

Command: backup done

```
ods-ksmutil backup done
```

DEPRECATED: This command is deprecated in OpenDNSSEC 1.4.0 and onwards; it will be removed in OpenDNSSEC 2.0.0 and beyond.

It can be replaced with the following command sequence:

```
ods-ksmutil backup prepare
ods-ksmutil backup commit
#OR# ods-ksmutil backup rollback
```

The improvement of switching to this is sequence is transactional security of the backup. Prior to this change, there were two ways of making uncertain backups:

- Running `ods-ksmutil backup done` after the actual backup: If the Enforcer was running and creating keys during the backup, the newest keys might not have been backed up, but they would still be marked as if they were by the backup done command.
- Running `ods-ksmutli backup done` before the actual backup: If the backup failed, then there would be no way to fix this. In the new situation, one can retry or execute `ods-ksmutil backup rollback`

This sequence creates time between a preparation phase and the actual commit of the backup. This time is meant for actually doing the backup.

Indicate that a backup of the given repository has been done, all non-backed up keys will now be marked as backed up.
This is especially important if the repository used has the **RequireBackup** flag set.

NOTE: Keys generated between a backup being made and the backup done command being run will be erroneously marked as having been backed up. To avoid this, either choose a backup schedule that doesn't run while the enforcer might be generating keys, or shutdown the enforcer while a backup is performed.

Options

```
--repository <repository>     aka -r
--force
```

- (If no options are given then all repositories are marked as backed up.) Include this call in a HSM backup process to avoid warnings or errors about using non-backed up keys.
- If the --force option is not used then a manual confirmation step is required to complete the backup.

Command: backup prepare

```
ods-ksmutil backup prepare
```

Mark all keys in preparation of an HSM key backup. Later invocation of `ods-ksmutil backup commit` or `ods-ksmutil backup rollback`, will only influence these marked keys.

This command is intended as part of the following key backup procedure:

- `ods-ksmutil backup prepare`
- Make the actual HSM key backup
- `ods-ksmutil backup commit` (or, in case of problems, `ods-ksmutil backup rollback`)

This is especially important if the repository used has the **RequireBackup** flag set.

Options

```
--repository <repository>     aka -r
```

(If no options are given then all keys in all repositories are marked for backed up.) Include this call in a HSM backup process to avoid warnings or errors about using non-backed up keys.

Command: backup commit

```
ods-ksmutil backup commit
```

Mark all keys that were previously marked with `ods-ksmutil backup prepare` as actually having been backed up. This means that the Enforcer can henceforth depend on these keys. A successful backup is a necessary precondition for the dependency on keys if the **RequireBackup** flag is set.

This command is intended as part of the following key backup procedure:

- `ods-ksmutil backup prepare`
- Make the actual HSM key backup
- `ods-ksmutil backup commit` (or, in case of problems, `ods-ksmutil backup rollback`)

Options

```
--repository <repository>     aka -r
```

(If no options are given then all keys in all repositories that were marked before are made available to the Enforcer.) Include this call in a HSM backup process to avoid warnings or errors about using non-backed up keys.

Command: backup rollback

```
ods-ksmutil backup rollback
```

Undo the previous marking of keys for backup with `ods-ksmutil backup prepare`. This means that the Enforcer cannot depend on these keys if the **RequireBackup** flag is set – their availability is not sufficiently guaranteed. A future backup can try again, starting once more from `ods-ksmutil backup prepare`.

This command is intended as part of the following key backup procedure:

- `ods-ksmutil backup prepare`
- Make the actual HSM key backup
- `ods-ksmutil backup commit` (or, in case of problems, `ods-ksmutil backup rollback`)

Note that OpenDNSSEC does not place restrictions on the repair of a failing HSM backup by attempting several times; the core idea is simply that `ods-ksmutil backup commit` is *only* executed when a backup has succeeded. The command `ods-ksmutil backup rollback` exists to handle persisting problems with backups, and to enable the backup procedure to start again with marking all the keys that are available for backup at *that* moment. It is probably good practice to round off a backup procedure with either `commit` or `rollback` on the same day (or other timeslot) as `prepare` was invoked.

Options

```
--repository <repository>     aka -r
```

(If no options are given then all keys in all repositories will have their backup-preparation marking udone.)

Command: backup list

```
ods-ksmutil backup list
```

List the backups that have been made on the given repository.

Options

```
--repository <repository>     aka -r
```

Command: database backup

```
ods-ksmutil database backup
```

Make a copy of the enforcer database (if using sqlite). It makes sure that the database is in a consistent state by taking a lock out first.

Options

```
[--output <output>]       aka -o
```

If --output is omitted then the usual enforcer.db.backup is used.

Command: rollover list

```
ods-ksmutil rollover list
```

List the expected dates and times of upcoming rollovers.

Options

```
[--zone <zone>]       aka -z
```

Command: zonelist export

```
ods-ksmutil zonelist export
```

Export the zone information held in the kasp database to zonelist.xml formatted text.

Command: zonelist import

```
ods-ksmutil zonelist import
```

Synchronise the database with the contents of zonelist.xml; identical to "update zonelist".

Allowed values

When specifying a keystate the following keywords are recognised:

```
GENERATED|PUBLISHED|READY|ACTIVE|RETIRED|REVOKED|DEAD
```

When specifying a keytype the following keywords are recognised:

```
KSK|ZSK
```

When specifying a time (for **key import**) the following formats can be used:

```
YYYYMMDD[HH[MM[SS]]]                  (all numeric)

    or  D-MMM-YYYY[:| ]HH[:MM[:SS]]     (alphabetic  month)
    or  DD-MMM-YYYY[:| ]HH[:MM[:SS]]    (alphabetic  month)
    or  YYYY-MMM-DD[:| ]HH[:MM[:SS]]    (alphabetic month)

    D-MM-YYYY[:| ]HH[:MM[:SS]]          (numeric month)
    DD-MM-YYYY[:| ]HH[:MM[:SS]]         (numeric month)
    or  YYYY-MM-DD[:| ]HH[:MM[:SS]]     (numeric month)
```

... and the distinction between them is given by the location of the hyphens.