Troubleshooting

There are a number of common issues that are straightforward to diagnose and fix... If OpenDNSSEC is not behaving as expected then the first place to look is in the logs. Where these will be depends on your system and your configuration.

The following are log messages which you may see, and what to do about them (if anything).

On this Page

Enforcer

ods-enforcerd: ERROR: Trying to make non-backed up ZSK active when RequireBackup flag is set
This is not an error as such. It means that in conf.xml you have indicated that keys should not be used unless they are backed up. However, the enforcer has determined that if it continues then a non backed up key will be made active.
The solution Take a backup of your keys (how this is done will depend on your key storage).
Once this has been done then run **ods-ksmutil backup done** to mark all keys as having been backed up.

ods-enforcerd: WARNING: Making non-backed up KSK active, PLEASE make sure that you know the potential problems of using keys which are not recoverable
This is the same as above, but without **RequireBackup** being set in conf.xml

ods-enforcerd: WARNING: key rollover not completed as there are no keys in the ready state: ods-enforcerd will try again when it runs next
This is seen when a rollover is happening but there is no replacement key ready (because one has not been published for long enough). It indicates that the rollover will be delayed until the replacement key is ready, the time that this will happen depends on the policy.

ods-enforcerd: Could not call signer engine
If the enforcer makes a change to a zones signer configuration (say it adds a new key) it calls the signer to get it to resign that zone. This message indicates that the signer is not running, although it has been seen on a system where everything is working fine. (See KNOWN_ISSUES.)

ods-enforcerd: Not enough keys to satisfy zsk policy for zone
or **ods-enforcerd: Not enough keys to satisfy ksk policy for zone**

One of these messages will be seen if the enforcer does not have enough unallocated keys to provide for the zone specified. If the **ManualKeyGeneration** tag is set in conf.xml then you will need to create new keys using **ods-ksmutil key generate**, otherwise new keys will be created when the enforcer runs next. (Don't forget to backup any new keys.)

ods-enforcerd: Rollover of KSK expected at <DATE TIME> for <ZONE>
This is not an error, but a notification of an upcoming (scheduled) rollover. This will appear in your logs at a time prior to the rollover as configured in conf.xml (the**Enforcer/RolloverNotification** tag).

ods-enforcerd: WARNING: KSK Retirement reached; please submit the new DS for <ZONE> and use ods-ksmutil key ksk-roll to roll the key.
Rolling a KSK requires the DS record of the replacement key to be published in the parent of the zone. This message indicates that your KSK has reached the end of its life (as specified by your policy), and that it is time to submit the DS record to the parent.

ods-enforcerd: Error: database in config file <path_to_conf.xml> does not match libksm
This indicates that either you have libksm built for sqlite, but have specified a MySQL database in conf.xml, or *vice versa*.
The solution is to either rebuild libksm or to change conf.xml

ods-enforcerd: Error reading config
This usually means that conf.xml is either absent, not readable by the user, or badly formed. There should be a line above this one which gives a more specific error message.

ods-enforcerd: Error getting db lock
When using sqlite any process using the database tries to get an exclusive write lock on a file in the same directory as the kasp.db. If this directory is not writeable by the user then this message will be seen, again a more specific error message should have been issued.

ods-enforcerd: Repository <NAME> is full, cannot create more <KSKs|ZSKs> for policy <POLICY>
In conf.xml a capacity can be specified for a repository. When this is reached then no more keys will be generated in that repository.
The solution is to either run **ods-ksmutil key purge** to remove dead keys, or to raise this capacity and run **ods-ksmutil update conf** to push this change into the database. If the repository is really at capacity, and purge does not free up any space, then a new repository will be needed.

ods-enforcerd: Repository <NAME> is nearly full, will create X <KSKs|ZSKs> for policy <POLICY> (reduced from Y)
Y keys were needed to satisfy the policy, but the repository only has room for X more. This warning might precede the error detailed above, and the solution is the same.

ods-enforcerd: NOTE: keys generated in repository <NAME> will not become active until they have been backed up
This is not an error, but a reminder that a backup needs to be done (as new keys have just been generated).

ods-enforcerd: Signconf not written for <ZONE>
Some error has happened and the enforcer will not overwrite the existing signconf file, so the old one will be left in place. There should be a more specific message indicating the root cause just prior to this line. (*E.g.* attempting to use a non backed up key.)

ods-enforcerd: There are no <KSKs|ZSKs> in the generate state; please use "ods-ksmutil key generate" to make some
ManualKeyGeneration has been set (in conf.xml) and the system has run out of keys.
The solution is to run the **ods-ksmutil key generate** command, back up the keys, and the system will recover when it runs next.

Signer

These messages might show up in the logs if there is a parse or semantic error in one of the configuration files.
ods-signerd: error: unable to read cfgfile <file>
ods-signerd: error: unable to parse cfgfile <file>
ods-signerd: error: unable to read conf rng file <file>
ods-signerd: error: unable to create XML RelaxNGs parser context
ods-signerd: error: unable to parse a schema definition resource
ods-signerd: error: unable to create RelaxNGs validation context
ods-signerd: error: configuration file validation failed
ods-signerd: error: unable to create new XPath context for cfgile <file>
ods-signerd: error: unable to evaluate required element <element> in cfgfile <file>
ods-signerd: error: cfgfile <file> has errors
ods-signerd: error: unable to evaluate xpath expression <expr>
ods-signerd: error: unable to open zone list file <file>
ods-signerd: error: unable to extract zone name from zonelist
ods-signerd: error: unable to read zone <dname>; skipping
ods-signerd: error: unable to add zone <zone> to zone list
ods-signerd: error: error parsing zone list file <file>
ods-signerd: error: invalid salt <salt>
ods-signerd: error: unable to parse signconf file <file>
ods-signerd: error: unable to read signconf file <file>
ods-signerd: error: signconf-check: no signature resign interval found
ods-signerd: error: signconf-check: no signature resign interval found
ods-signerd: error: signconf-check: no signature default validity found
ods-signerd: error: signconf-check: no signature denial validity found
ods-signerd: error: signconf-check: no signature jitter found
ods-signerd: error: signconf-check: no signature inception offset found
ods-signerd: error: signconf-check: no nsec3 algorithm found
ods-signerd: error: signconf-check: wrong nsec type <rrtype>
ods-signerd: error: signconf-check: no keys found
ods-signerd: error: signconf-check: no dnskey ttl found
ods-signerd: error: signconf-check: no soa ttl found
ods-signerd: error: signconf-check: no soa minimum found
ods-signerd: error: signconf-check: wrong soa serial type <string>

These messages might show up in the logs if the signer engine daemon was unable to start up. All of them are provided with a specific message indicating the cause.
ods-signerd: error: unable to create command handler, <reason>
ods-signerd: error: cannot connect to command handler: <reason>
ods-signerd: error: setup failed: chdir to <directory> failed: <reason>
ods-signerd: error: setup failed: unable to drop privileges
ods-signerd: error: setup failed: unable to fork daemon: <reason>
ods-signerd: error: setup failed: unable to setsid daemon: <reason>
ods-signerd: error: setup failed: unable to write pid file
ods-signerd: error: setup failed: unable to start command handler
ods-signerd: error: setup failed: unable to start command handler
ods-signerd: error: setup failed: error initializing libhsm (errno <no>)
ods-signerd: error: signer setup failed
ods-signerd: error: failed to fork zone fetcher: <reason>
ods-signerd: error: failed to setsid zone fetcher: <reason>
ods-signerd: error: cannot stop zone fetcher: <reason>
ods-signerd: error: cannot start zone fetcher

These messages might show up in the logs if the signer was unable to sign the zone
ods-signerd: error: task [read zone <dname>] failed
File not found or readable, parse error, ...
ods-signerd: error: task [add dnskeys to zone <dname>] failed
HSM re-initialized, no privileges for accessing HSM, ...
ods-signerd: error: task [update zone <dname>] failed
DNS related errors in zone, for example other RRs next to a CNAME
ods-signerd: error: task [nsecify zone <dname>] failed
ods-signerd: error: task [sign zone <dname>] failed
No privileges for accessing HSM, ...
ods-signerd: error: task [write zone <dname>] failed
Output directory not writable

These messages might show up in the logs if a zone update failed
ods-signerd: error: cannot keep SOA SERIAL from input zone (<serial>): output SOA SERIAL is <serial>
<SOA><Serial> is set to keep in kasp policy file, but SOA SERIAL in unsigned zone file was not increased
ods-signerd: error: occluded (non-glue non-DS) data at <dname> NS
Found unallowed RRs at the delegation
ods-signerd: error: occluded data at <dname> (below <dname> DNAME)
Found RRs below DNAME
ods-signerd: error: occluded (non-glue) data at <dname> (below <dname> NS
Found non-glue RRs below delegation
ods-signerd: error: other data next to <dname> CNAME
Found unallowed RRs next to CNAME
ods-signerd: error: multiple records for singleton type at <dname> <rrtype>
Found multiple RRs of a singleton RRtype (CNAME or DNAME) at the same owner name
ods-signerd: error: update zone <dname> failed: zone data contains errors

These messages might show up in the logs if one of the backup files was corrupted
ods-signerd: error: error creating DNSKEY for key <locator>
ods-signerd: error: error adding DNSKEY[<keytag>] for key <locator>
ods-signerd: error: error creating NSEC3 parameters for zone <dname>
ods-signerd: error: error adding NSEC3PARAMS record to zone <dname>
ods-signerd: error: error adding DNSKEYs to zone <dname>
ods-signerd: error: error adding NSEC3PARAMS RR to zone <dname>
ods-signerd: error: cannot backup zone: cannot open file <file> for writing
ods-signerd: error: error adding key from backup file <file> to key list
ods-signerd: error: error recovering DNSKEY[<keytag>] rr
ods-signerd: error: error recovering nsec3 parameters from file <file>
ods-signerd: error: error recovering NSEC3PARAMS rr
ods-signerd: error: error reading key credentials from backup
ods-signerd: error: error reading RRSIG from backup
ods-signerd: error: expecting RRtype RRSIG from backup
ods-signerd: error: error reading domain from backup file
ods-signerd: error: error adding domain from backup file
ods-signerd: error: error reading NSEC(3) RR from backup file
ods-signerd: error: error adding NSEC(3) RR from backup file
ods-signerd: error: unable to recover zone state from file <file>: <reason>
ods-signerd: error: unable to recover denial of existence from file <file>: <reason>
ods-signerd: error: unable to recover unsorted zone from file <file>: <reason>
ods-signerd: error: unable to recover dnskeys from file <file>: <reason>
ods-signerd: error: unable to recover rrsigs from file <file>: <reason>
ods-signerd: error: domain part in backup file is corrupted
ods-signerd: error: unable to recover RR to domain: failed to add RRset
ods-signerd: error: ods-signerd: error: unable to recover RRSIG to domain: no NSEC RRset
ods-signerd: error: unable to recover RRSIG to domain: no NSEC3 RRset
ods-signerd: error: unable to recover RRSIG to domain: no such RRset
ods-signerd: error: nsec3params part in backup file is corrupted
ods-signerd: error: key part in backup file is corrupted
ods-signerd: error: unable to recover signconf backup file <file>: corrupt

HSM login / PIN daemon

hsm_prompt_pin(): Could not access the named semaphore / shared memory: ...

These errors might indicate that shared memory is not configured or configured incorrectly for the system or the OpenDNSSEC user, please see your systems manual for shared memory and ipc/ipcs commands.

hsm_prompt_pin(): Bad memory size, ...

This error should most likely be a result of an upgrade where the data structures stored in memory have changed size. There should be information about this in the migration documentation between versions. If you did not make an upgrade something else might have changed the memory outside of OpenDNSSEC.

You can try and clear the shared memory, see section below.

hsm_prompt_pin(): Bad permissions on the shared memory, ...

This error indicated that the shared memory exist but has the wrong permissions, either it was created by another user or something else changed the permissions.

If you are using user/group privileges see to it that you use the same user/group when you login the PIN:

```
$ sudo -u <user> -g <group> ods-hsmutil login
```

You can view the shared memory to see if the permissions is correct using ipcs, the user/group should be what you configured in conf.xml and permissions should be read+write for user and read+write for group.

Note that output will vary between systems.

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x0d50d5ec 983040     opendnssec 660        25600      0

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x0d50d5ec 425985     opendnssec 660        1
```

Clearing the PIN daemon shared memory

You can clear the PIN daemon memory by destroying the shared memory, first shutdown OpenDNSSEC.

```
$ ods-control stop
```

Then find the shared memory and the semaphore by using ipcs.

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status
0x0d50d5ec 983040     opendnssec 660        25600      0

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
0x0d50d5ec 425985     opendnssec 660        1
```

Now we remove the shared memory and the semaphore by logging out.

```
$ ods-hsmutil logout
```

And then run ipcs again so we see that the shared memory and the semaphore are gone.

```
$ ipcs
------ Shared Memory Segments --------
key        shmid      owner      perms      bytes      nattch     status

------ Semaphore Arrays --------
key        semid      owner      perms      nsems
```