Running OpenDNSSEC

This section describes how to start OpenDNSSEC and the operations used to manage and monitor the system.

The details of the command utilities shown below can be found here.

On this Page

All directories are prepared by the build script and are set to be owned by root, so all commands in the default configuration must also be run by root. To change this, alter the configuration or privileges on the files and directories.

Before starting OpenDNSSEC for the first time

Before you run the system for the first time you must import your policy and zone list into the database using the following command:

```
ods-ksmutil setup
```

After running this the first time, you will be ready to run OpenDNSSEC with an empty set of zones. On the other hand, if this command is run on an existing database, then will all meta-information about the zones be lost. The keys would then still exist in HSMs, so you should not forget to clean them up.

Starting / Stopping the system

OpenDNSSEC consist of two daemons, *ods-signerd* and *ods-enforcerd*. To start and stop them use the following commands:

```
ods-control start
```

A proper-looking response to this commands is:

```
Starting enforcer...
OpenDNSSEC ods-enforcerd started (version 1.2.0b1), pid 11424
Starting signer engine...
OpenDNSSEC signer engine version 1.2.0b1
```

At any time, you can stop OpenDNSSEC's daemons orderly with:

```
ods-control stop
```

After this, your logs should contain messages like:

```
Stopping enforcer...
Stopping signer engine..
Engine shut down.
```

Uploading a Trust Anchor (Publish of DS to the parent)

Your zone will be signed, once you have setup the system and started it. When you have verified that the zone is operational and working, it is time to upload the trust anchor to the parent zone. The Enforcer is waiting for zone to be connected to the trust chain before considering the KSK to be active.

```
ods-ksmutil key list --verbose

Keys:
Zone:                          Keytype:      State:    Date of next transition:
CKA_ID:                          Repository:                     Keytag:
example.com                    ZSK           active    2010-10-15 06:59:28
92abca348b96aaef42b5bb62c8daffb0  softHSM2                       28743
example.com                    KSK           ready     waiting for ds-seen
9621ca39306ce050e8dd94c5ab837001  softHSM1                       22499
```

1. Export the public key either as DNSKEY or DS, depending on what format your parent zone wants it in. See the section Export the public keys, on how to get the key information.

   This step can be automated or semi-automated by placing a command in the <DelegationSignerSubmitCommand> tag. This should point to a binary which will accept the required key(s) as DNSKEY RRs on STDIN.
2. Notify the Enforcer when you can see the DS RR in your parent zone. You usually give the keytag to the Enforcer, but if there are KSKs with the same keytag then use the CKA_ID.

   ```
   ods-ksmutil key ds-seen -z example.com -x 22499
   ```

   or

   ```
   ods-ksmutil key ds-seen -z example.com -k 9621ca39306ce050e8dd94c5ab837001
   ```

   ```
   Result:
   Found key with CKA_ID 9621ca39306ce050e8dd94c5ab837001
   Key 9621ca39306ce050e8dd94c5ab837001 made active
   ```

   And you will see that your KSK is now active:

   ```
   ods-ksmutil key list

   Keys:
   Zone:                          Keytype:      State:    Date of next transition:
   example.com                    ZSK           active    2010-10-15 07:20:53
   example.com                    KSK           active    2010-10-15 07:31:03
   ```

Key Management

The details of common key management activities are described on the Key Management page - these include:

- Configuring the system to only make keys active once they have been backed up.
- Exporting public keys.
- Performing manual key rollovers.

Zone Management

The details of common zone management activities are described on the Zone Management page - these include:

- Adding / Removing zones
- Updating an unsigned zone

Updating an unsigned zone

When you update the content of an unsigned zone you must manually tell the signer engine to re-read the unsigned zone file using the *ods-signer* command like this:

```
ods-signer sign example.com
```

Updating the xml config files (including the KASP policy)

When you make changes to conf.xml, kasp.xml or zonelist.xml you must run the

```
ods-ksmutil update all
```

command (or the appropriate command listed below) in order for the changes to be propagated to the system database.

conf.xml

If you make changes to the enforcer or auditor section of the conf.xml file then you must run

```
ods-ksmutil update conf
```

For most other changes to the conf.xml file it is advisable to stop and start OpenDNSSEC to ensure the changes are detected.

kasp.xml

When you make changes to a policy or add a new policy in kasp.xml you must update the changes to the database.

```
ods-ksmutil update kasp
```

When making changes to the KASP policy the following should also be considered:

- It is advised not to update policy details (in particular propagation times) while a rollover is in progress.
- Changing the algorithm used in a policy is not supported in 1.3 or 1.4.
- Certain policy changes e.g. changing 'Standby keys" from 'on' to 'off' may lead to orphaned keys.
- After updating signature timers in the policy it may be helpful to issue the command:

  ```
  $ ods-signer clear <zone>; ods-signer sign <zone>
  ```

  as it will speed up acclimatising timers for the signatures.

zonelist.xml

If you add zones directly into the zonelist (rather than using the ods-ksmutil zone add command) you must tell the enforcer to re-read the zone list by using the command:

```
ods-ksmutil update zonelist
```

Monitoring the system

- The pids used by the enforcer and signer processes are reported in syslog on startup.
- The command '*ods-signer running*' will report the status of the signer process, or restart it if it is not running.
- When the enforcer daemon has run and completed enforcing the zones is sends a message to the syslog containing the text "*Sleeping for*" rep orting how long it will be until it next runs
- The signer produces a log containing the text "*[STAT]"* whenever a zone is successfully signed
- A Nagios plugin is available to check signed zones: https://github.com/opendnssec/dnssec-monitor

Logging

Details of logs produced by the system can be found on the Logging page.