Logging using Men & Mice Suite and BIND

Symptom:

Men & Mice Suite lets you manage the logging settings for each log channel used by your BIND name server. When the DNS Server Controller is installed, it creates two new channels. Within each channel, you can select what categories to log, and what severity level to log at. All messages in the selected categories that have the selected severity or higher will be logged.

Problem:

Every message logged by the BIND name server has a category and a severity. Below, you will find a list of BIND logging categories, along with a description of what types of messages are logged in that category. Each category has a name used in the configuration file and an English label used in the Management Console's server options window.

Categories differ between BIND 8 and BIND 9. Some categories are the same, some have the same name but different meanings, and the rest are entirely different between versions.

Solution

Common Logging Categories

- **queries**: A short log message is generated for every query the server receives. In BIND 9, using this category will enable query logging.
- **lame-servers**: Lame servers. These are misconfiguration in remote servers, discovered by the BIND name server when trying to query those servers during the process of recursion.
- **update**: Messages about dynamic updates.
- **xfer-in**: Zone transfers the server is receiving.
- **xfer-out**: Zone transfers the server is sending.
- **notify**: Messages relating to the DNS NOTIFY protocol.
- **security**: Approval and denial of requests.

Logging Categories Specific to BIND 8

- **default**: The catch-all. Many things aren't classified into categories, and they all end up here. Not the same as the `default` category in BIND 9.
- **config**: High-level configuration file processing. Low-level processing messages belong to category `parser`. Not the same as the `config` category in BIND 9.
- **eventlib**: Debugging info from the event system. Only one channel may be specified for this category, and it must be a file channel.
- **packet**: Dumps of packets received and sent. Only one channel may be specified for this category, and it must be a file channel.
- **panic**: If the server has to shut itself down due to an internal problem, it will log the problem in this category as well as in the problem's native category.
- **parser**: Low-level configuration file processing. High-level processing messages belong to category `config`.
- **statistics**: Statistics.
- **ncache**: Messages about negative caching.
- **db**: All database operations.
- **cname**: Messages like "... points to a CNAME".
- **os**: Operating system problems.
- **insist**: Internal consistency check failures.
- **maintenance**: Periodic maintenance events such as cache cleaning.
- **load**: Zone loading messages.
- **response-checks**: Messages arising from response checking, such as "malformed response", "wrong ans. name", "unrelated additional info", "invalid RR type", and "bad referral".

Logging Categories Specific to BIND 9

- **default**: The default category defines the logging options for those categories where no specific configuration has been defined - this doesn't usually come up with Men & Mice Suite, since the installer for Men & Mice DNS Server Controller normally specifies logging for each category (even those categories not logged to any channel). Not the same as the `default` category in BIND 8.
- **config**: Configuration file parsing and processing. For BIND 9, there's only one category for this operation, as opposed to BIND 8's `config` and p `arser` categories.
- **client**: Processing of client requests.
- **database**: Messages relating to the databases used internally by the name server to store zone and cache data.
- **dispatch**: Dispatching of incoming packets to the server modules where they are to be processed.
- **dnssec**: DNSSEC and TSIG protocol processing.
- **general**: The catch-all. Many things aren't classified into categories, and they all end up here. Similar to the `default` category in BIND 8.
- **network**: Network operations.
- **resolver**: DNS resolution, such as the recursive lookups performed on behalf of clients by a caching name server.
- **unmatched**: Messages that named was unable to determine the class of or for which there was no matching view. A one line summary is also logged to the client category. This category is best sent to a file.
- **update-security**: Approval and denial of update requests.
- **query-errors**: Information about queries that resulted in some failure.

- **delegation-only**: Logs queries that have been forced to NXDOMAIN as the result of a delegation-only zone or a delegation-only in a hint or stub zone declaration.
- **edns-disabled**: Log queries that have been forced to use plain DNS due to timeouts. This is often due to the remote servers not being RFC 1034 compliant (not always returning FORMERR or similar to EDNS queries and other extensions to the DNS when they are not understood). In other words, this is targeted at servers that fail to respond to DNS queries that they don't understand.
  Note: the log message can also be due to packet loss. Before reporting servers for non-RFC 1034 compliance they should be re-tested to determine the nature of the non-compliance. This testing should prevent or reduce the number of false-positive reports.
  Note: eventually named will have to stop treating such timeouts as due to RFC 1034 non compliance and start treating it as plain packet loss. Falsely classifying packet loss as due to RFC 1034 non compliance impacts on DNSSEC validation which requires EDNS for the DNSSEC records to be returned.
- **query-errors**: specifically intended for debugging purposes: To identify why and how specific queries result in responses which indicate an error. Messages of this category are therefore only logged with debug levels.