

Tracing Extended DHCP Operations

Both the extended DHCP local server and the extended DHCP relay agent support tracing operations. DHCP tracing operations track extended DHCP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

- Important events are logged in a file called `jdhcpd` located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located.
- When the file `jdhcpd` reaches 128 kilobytes (KB), it is renamed `jdhcpd.0`, then `jdhcpd.1`, and so on, until there are three trace files. Then the oldest trace file (`jdhcpd.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000. (For more information about how log files are created, see the *JUNOS System Log Messages Reference*.)

- Log files can be accessed only by the user who configures the tracing operation.

To configure DHCP local server and DHCP relay agent tracing operations:

1. Specify that you want to configure tracing options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit traceoptions
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.

See “Configuring the Extended DHCP Log Filename” on page 2.

3. (Optional) Configure the number and size of the log files.

See “Configuring the Number and Size of Extended DHCP Log Files” on page 2.

4. (Optional) Configure access to the log file.

See “Configuring Access to the Extended DHCP Log File” on page 3.

5. (Optional) Configure a regular expression to filter logging events.

See “Configuring a Regular Expression for Extended DHCP Lines to Be Logged” on page 3.

6. (Optional) Configure flags to filter the operations to be logged.

See “Configuring the Extended DHCP Tracing Flags” on page 4.

The extended DHCP traceoptions operations are described in the following sections:

- Configuring the Extended DHCP Log Filename on page 2
- Configuring the Number and Size of Extended DHCP Log Files on page 2
- Configuring Access to the Extended DHCP Log File on page 3
- Configuring a Regular Expression for Extended DHCP Lines to Be Logged on page 3
- Configuring the Extended DHCP Tracing Flags on page 4

Configuring the Extended DHCP Log Filename

By default, the name of the file that records trace output is `jdhcpd`. You can specify a different name by including the `file` option:

To configure the filename for DHCP local server and DHCP relay agent tracing operations:

- Specify the name of the file used for the trace output. (DHCP local server and DHCP relay agent both support the `file` option for the `traceoptions` statement.)

```
[edit system services dhcp-local-server traceoptions]  
user@host# set file dhcp_logfile_1
```

Configuring the Number and Size of Extended DHCP Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed `filename.0`, then `filename.1`, and so on, until there are three trace files. Then the oldest trace file (`filename.2`) is overwritten.

You can optionally configure the maximum file size to be from 10 KB through 1 gigabyte (GB). You can also specify the number of trace files to be from 2 through 1000.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation (`filename`) reaches 2 MB, `filename` is renamed `filename.0`, and a new file called `filename` is created. When the new `filename` reaches 2 MB, `filename.0` is renamed `filename.1` and `filename` is renamed `filename.0`. This process repeats until there are 20 trace files. Then the oldest file (`filename.19`) is overwritten by the newest file (`filename.0`).

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (DHCP local server and DHCP relay agent both support the **files** and **size** options for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 files 20 size 2097152
```

Configuring Access to the Extended DHCP Log File

By default, log files can be accessed only by the user who configures the tracing operation. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

To specify that all users can read the log file:

- Configure the log file to be world-readable. (DHCP local server and DHCP relay agent both support the **world-readable** option for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 world-readable
```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable. (DHCP local server and DHCP relay agent both support the **no-world-readable** option for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 no-world-readable
```

Configuring a Regular Expression for Extended DHCP Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events. You can refine the output by including regular expressions that will be matched.

To configure regular expressions to be matched:

- Configure the regular expression. (DHCP local server and DHCP relay agent both support the **match** option for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]
user@host# set file dhcp_logfile_1 match regex
```

Configuring the Extended DHCP Tracing Flags

By default, only important events are logged. You can specify which trace operations are logged by including specific tracing flags. The following table describes the flags that you can include.

| Flag | Description |
|---------------|--|
| all | Trace all events |
| auth | Trace authentication events |
| database | Trace database events |
| fwd | Trace firewall process events |
| general | Trace miscellaneous events |
| ha | Trace high availability-related events |
| interface | Trace interface operations |
| io | Trace I/O operations |
| packet | Trace packet decoding operations |
| packet-option | Trace DHCP option decoding operations |
| rpd | Trace routing protocol process events |
| rtstock | Trace routing socket operations |
| session-db | Trace session database events |
| state | Trace changes in state |
| ui | Trace user interface operations |

To configure the flags for the events to be logged:

- Configure the flags. (DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement.)

```
[edit system services dhcp-local-server traceoptions]  
user@host# set flag packet-option
```