

 **ONE IDENTITY™**

Syslog-ng 101, part 5: Sources

Peter Czanik

Source definition

- Sources contain one or more source drivers where syslog-ng receives log messages:

```
source <identifier> {  
    source-driver(parameters);  
    source-driver(parameters);  
    ...  
};
```

- A simple file source:

```
source s_file {  
    file("/path/to/the/file.log");  
};
```

Source definition

- Example source with multiple source drivers:

```
source s_local {  
    internal();  
    file("/path/to/the/first/file.log");  
    file("/path/to/the/next/file.log");  
    system();  
};
```

Source flags

- Source drivers can have flags:
 - no-parse: disables syslog message parsing, the whole incoming message is stored on the MESSAGE field
 - syslog-protocol: expects RFC5424 message format
- Further flags→ documentation

Source drivers

- `internal()`: internal messages of `syslog-ng`
- `unix-stream()`, `unix-dgram()`: unix domain sockets
- `systemd-journal()`: reads `systemd`'s journal files
- `file()`: opens one file and reads the messages
- `pipe()`: reads a named pipe
- `network()`: reads legacy sources
- `syslog()`: reads the RFC5424 syslog family standard
- `sun-stream()`: reads streams on Sun Solaris
- `program()`: runs a program and reads standard output
- `python()`: code your own source in Python

The system() source

- Collect system-specific log messages of the host
 - not required to discover all the possible local log sources of a system
 - Same configuration on multiple systems
 - A complete replacement of sytemd-journal, /dev/log /proc/kmsg, etc.
 - Parses messages automatically

- Usage:

```
@include "scl.conf"  
source s_all {  
    system();  
};
```

A Common mistake

- Duplicating sources can cause errors:
 - binding twice on the same IP and port
 - multiplying incoming messages
- Solution:
 - Define a source once and use it multiple times in different log paths

Checking the syslog-ng version

```
czanik@QDNDV8D3:/mnt/c/Users/PCzanik> syslog-ng -V
```

```
syslog-ng 4 (4.0.1)
```

```
Config version: 4.0
```

```
Installer-Version: 4.0.1
```

```
Revision:
```

```
Module-Directory: /usr/lib64/syslog-ng
```

```
Module-Path: /usr/lib64/syslog-ng
```

```
Include-Path: /usr/share/syslog-ng/include
```

```
Available-Modules: afstomp,syslogformat,cryptofuncs,http,add-contextual-data,affile,xml,csvparser,tfgetent,system-  
source,disk-buffer,map-value-pairs,appmodel,rate-limit-filter,kvformat,cef,tags-  
parser,examples,stardate,timestamp,hook-commands,basicfuncs,pseudofile,afprog,pacctformat,json-  
plugin,graphite,azure-auth-header,linux-kmsg-format,afuser,confgen,dbparser,secure-logging,regexp-  
parser,sdjournal,afsocket
```

```
Enable-Debug: off
```

```
Enable-GProf: off
```

```
Enable-Memtrace: off
```

```
Enable-IPv6: on
```

```
Enable-Spoof-Source: on
```

```
Enable-TCP-Wrapper: on
```

```
Enable-Linux-Caps: on
```

```
Enable-Systemd: on
```

 **ONE IDENTITY™**