

syslog-ng

Как отфильтровать логи конкретного systemd юнита:

```
filter nginx_service {
    "${.journald._SYSTEMD_UNIT}" eq "nginx.service";
};
```

Другие поля можно узнать посмотрев на лог:

```
journalctl --output json-pretty

{
    "_SYSTEMD_UNIT" : "init.scope",
    "_PID" : "1",
    "_MACHINE_ID" : "XXXXX",
    "INVOCATION_ID" : "ecad364ce7794e13ae6bc35a59ae4ac2",
    "CODE_LINE" : "574",
    "__MONOTONIC_TIMESTAMP" : "3003939058929",
    "_TRANSPORT" : "journal",
    "_UID" : "0",
    "PRIORITY" : "6",
    "_EXE" : "/usr/lib/systemd/systemd",
    "_CAP_EFFECTIVE" : "1fcfdcfcff",
    "_SYSTEMD_CGROUP" : "/init.scope",
    "SYSLOG_FACILITY" : "3",
    "_COMM" : "systemd",
    "MESSAGE" : "Starting The PHP 8.1 FastCGI Process Manager...",
    "CODE_FILE" : "src/core/job.c",
    "_SOURCE_REALTIME_TIMESTAMP" : "1694843970044480",
    "SYSLOG_IDENTIFIER" : "systemd",
    "_CMDLINE" : "/lib/systemd/systemd --system --deserialize 33",
    "_HOSTNAME" : "web",
    "JOB_ID" : "300568",
    "JOB_TYPE" : "start",
    "MESSAGE_ID" : "7d4958e842da4a758f6c1cdc7b36dcc5",
    "__REALTIME_TIMESTAMP" : "1694843970044562",
    "_GID" : "0",
```

```
"_BOOT_ID" : "04f27e01022c4fe5be6723ddae2991be",
"UNIT" : "php8.1-fpm.service",
"_SELINUX_CONTEXT" : "lxc-container-default-cgns (enforce)\n",
"_SYSTEMD_SLICE" : "-.slice",
"__CURSOR" :
"s=bf41ba4a89ec44e882c3d8729a337787;i=db8b;b=04f27e01022c4fe5be6723ddae2991be;m=2bb68b874f1;t=
605739cc8c292;x=fe2cf83fe8762ab3",
"CODE_FUNC" : "job_log_begin_status_message"
}
```

Revision #1

Created 2024-02-15 09:53:28 MSK by Ivan

Updated 2024-02-15 09:58:45 MSK by Ivan