

openobserve

default

1 Ouerv Editor:

Showing 1 to 50 out of 351 events in 127 ms.(Delta Scan Size: 0.00 MB)

50

1 2 3 4 5

时间 (Asia/Taipei) source

> 2025-11-13 22:17:01.544	{"_audit_loginuid":0,"_audit_session":30998,"_boot_id":7a6fb77c5f9347d3a15bfa69e88488e,"_cap_effective":1,"_cap_inherited":0,"_cap_permitted":1,"_cap_bprm":0,"_cap_dac":0,"_cap_fowner":0,"_cap_fproc":0,"_cap_fsock":0,"_cap_ipc_lock":0,"_cap_ipc_owner":0,"_cap_kill":0,"_cap_linux_immutable":0,"_cap_mknod":0,"_cap_net_admin":0,"_cap_net_raw":0,"_cap_setgid":0,"_cap_setuid":0,"_cap_sys_admin":0,"_cap_sys_module":0,"_cap_sys_ptrace":0,"_cap_tcb":0,"_cap_wall":0,"_cap_xattr":0,"_cap_xfrm":0,"_cap_zo":0,"_cap_zo_admin":0,"_cap_zo_admin_v2":0,"_cap_zo_admin_v3":0,"_cap_zo_admin_v4":0,"_cap_zo_admin_v5":0,"_cap_zo_admin_v6":0,"_cap_zo_admin_v7":0,"_cap_zo_admin_v8":0,"_cap_zo_admin_v9":0,"_cap_zo_admin_v10":0,"_cap_zo_admin_v11":0,"_cap_zo_admin_v12":0,"_cap_zo_admin_v13":0,"_cap_zo_admin_v14":0,"_cap_zo_admin_v15":0,"_cap_zo_admin_v16":0,"_cap_zo_admin_v17":0,"_cap_zo_admin_v18":0,"_cap_zo_admin_v19":0,"_cap_zo_admin_v20":0,"_cap_zo_admin_v21":0,"_cap_zo_admin_v22":0,"_cap_zo_admin_v23":0,"_cap_zo_admin_v24":0,"_cap_zo_admin_v25":0,"_cap_zo_admin_v26":0,"_cap_zo_admin_v27":0,"_cap_zo_admin_v28":0,"_cap_zo_admin_v29":0,"_cap_zo_admin_v30":0,"_cap_zo_admin_v31":0,"_cap_zo_admin_v32":0,"_cap_zo_admin_v33":0,"_cap_zo_admin_v34":0,"_cap_zo_admin_v35":0,"_cap_zo_admin_v36":0,"_cap_zo_admin_v37":0,"_cap_zo_admin_v38":0,"_cap_zo_admin_v39":0,"_cap_zo_admin_v40":0,"_cap_zo_admin_v41":0,"_cap_zo_admin_v42":0,"_cap_zo_admin_v43":0,"_cap_zo_admin_v44":0,"_cap_zo_admin_v45":0,"_cap_zo_admin_v46":0,"_cap_zo_admin_v47":0,"_cap_zo_admin_v48":0,"_cap_zo_admin_v49":0,"_cap_zo_admin_v50":0,"_cap_zo_admin_v51":0,"_cap_zo_admin_v52":0,"_cap_zo_admin_v53":0,"_cap_zo_admin_v54":0,"_cap_zo_admin_v55":0,"_cap_zo_admin_v56":0,"_cap_zo_admin_v57":0,"_cap_zo_admin_v58":0,"_cap_zo_admin_v59":0,"_cap_zo_admin_v60":0,"_cap_zo_admin_v61":0,"_cap_zo_admin_v62":0,"_cap_zo_admin_v63":0,"_cap_zo_admin_v64":0,"_cap_zo_admin_v65":0,"_cap_zo_admin_v66":0,"_cap_zo_admin_v67":0,"_cap_zo_admin_v68":0,"_cap_zo_admin_v69":0,"_cap_zo_admin_v70":0,"_cap_zo_admin_v71":0,"_cap_zo_admin_v72":0,"_cap_zo_admin_v73":0,"_cap_zo_admin_v74":0,"_cap_zo_admin_v75":0,"_cap_zo_admin_v76":0,"_cap_zo_admin_v77":0,"_cap_zo_admin_v78":0,"_cap_zo_admin_v79":0,"_cap_zo_admin_v80":0,"_cap_zo_admin_v81":0,"_cap_zo_admin_v82":0,"_cap_zo_admin_v83":0,"_cap_zo_admin_v84":0,"_cap_zo_admin_v85":0,"_cap_zo_admin_v86":0,"_cap_zo_admin_v87":0,"_cap_zo_admin_v88":0,"_cap_zo_admin_v89":0,"_cap_zo_admin_v90":0,"_cap_zo_admin_v91":0,"_cap_zo_admin_v92":0,"_cap_zo_admin_v93":0,"_cap_zo_admin_v94":0,"_cap_zo_admin_v95":0,"_cap_zo_admin_v96":0,"_cap_zo_admin_v97":0,"_cap_zo_admin_v98":0,"_cap_zo_admin_v99":0,"_cap_zo_admin_v100":0,"_cap_zo_admin_v101":0,"_cap_zo_admin_v102":0,"_cap_zo_admin_v103":0,"_cap_zo_admin_v104":0,"_cap_zo_admin_v105":0,"_cap_zo_admin_v106":0,"_cap_zo_admin_v107":0,"_cap_zo_admin_v108":0,"_cap_zo_admin_v109":0,"_cap_zo_admin_v110":0,"_cap_zo_admin_v111":0,"_cap_zo_admin_v112":0,"_cap_zo_admin_v113":0,"_cap_zo_admin_v114":0,"_cap_zo_admin_v115":0,"_cap_zo_admin_v116":0,"_cap_zo_admin_v117":0,"_cap_zo_admin_v118":0,"_cap_zo_admin_v119":0,"_cap_zo_admin_v120":0,"_cap_zo_admin_v121":0,"_cap_zo_admin_v122":0,"_cap_zo_admin_v123":0,"_cap_zo_admin_v124":0,"_cap_zo_admin_v125":0,"_cap_zo_admin_v126":0,"_cap_zo_admin_v127":0,"_cap_zo_admin_v128":0,"_cap_zo_admin_v129":0,"_cap_zo_admin_v130":0,"_cap_zo_admin_v131":0,"_cap_zo_admin_v132":0,"_cap_zo_admin_v133":0,"_cap_zo_admin_v134":0,"_cap_zo_admin_v135":0,"_cap_zo_admin_v136":0,"_cap_zo_admin_v137":0,"_cap_zo_admin_v138":0,"_cap_zo_admin_v139":0,"_cap_zo_admin_v140":0,"_cap_zo_admin_v141":0,"_cap_zo_admin_v142":0,"_cap_zo_admin_v143":0,"_cap_zo_admin_v144":0,"_cap_zo_admin_v145":0,"_cap_zo_admin_v146":0,"_cap_zo_admin_v147":0,"_cap_zo_admin_v148":0,"_cap_zo_admin_v149":0,"_cap_zo_admin_v150":0,"_cap_zo_admin_v151":0,"_cap_zo_admin_v152":0,"_cap_zo_admin_v153":0,"_cap_zo_admin_v154":0,"_cap_zo_admin_v155":0,"_cap_zo_admin_v156":0,"_cap_zo_admin_v157":0,"_cap_zo_admin_v158":0,"_cap_zo_admin_v159":0,"_cap_zo_admin_v160":0,"_cap_zo_admin_v161":0,"_cap_zo_admin_v162":0,"_cap_zo_admin_v163":0,"_cap_zo_admin_v164":0,"_cap_zo_admin_v165":0,"_cap_zo_admin_v166":0,"_cap_zo_admin_v167":0,"_cap_zo_admin_v168":0,"_cap_zo_admin_v169":0,"_cap_zo_admin_v170":0,"_cap_zo_admin_v171":0,"_cap_zo_admin_v172":0,"_cap_zo_admin_v173":0,"_cap_zo_admin_v174":0,"_cap_zo_admin_v175":0,"_cap_zo_admin_v176":0,"_cap_zo_admin_v177":0,"_cap_zo_admin_v178":0,"_cap_zo_admin_v179":0,"_cap_zo_admin_v180":0,"_cap_zo_admin_v181":0,"_cap_zo_admin_v182":0,"_cap_zo_admin_v183":0,"_cap_zo_admin_v184":0,"_cap_zo_admin_v185":0,"_cap_zo_admin_v186":0,"_cap_zo_admin_v187":0,"_cap_zo_admin_v188":0,"_cap_zo_admin_v189":0,"_cap_zo_admin_v190":0,"_cap_zo_admin_v191":0,"_cap_zo_admin_v192":0,"_cap_zo_admin_v193":0,"_cap_zo_admin_v194":0,"_cap_zo_admin_v195":0,"_cap_zo_admin_v196":0,"_cap_zo_admin_v197":0,"_cap_zo_admin_v198":0,"_cap_zo_admin_v199":0,"_cap_zo_admin_v200":0,"_cap_zo_admin_v201":0,"_cap_zo_admin_v202":0,"_cap_zo_admin_v203":0,"_cap_zo_admin_v204":0,"_cap_zo_admin_v205":0,"_cap_zo_admin_v206":0,"_cap_zo_admin_v207":0,"_cap_zo_admin_v208":0,"_cap_zo_admin_v209":0,"_cap_zo_admin_v210":0,"_cap_zo_admin_v211":0,"_cap_zo_admin_v212":0,"_cap_zo_admin_v213":0,"_cap_zo_admin_v214":0,"_cap_zo_admin_v215":0,"_cap_zo_admin_v216":0,"_cap_zo_admin_v217":0,"_cap_zo_admin_v218":0,"_cap_zo_admin_v219":0,"_cap_zo_admin_v220":0,"_cap_zo_admin_v221":0,"_cap_zo_admin_v222":0,"_cap_zo_admin_v223":0,"_cap_zo_admin_v224":0,"_cap_zo_admin_v225":0,"_cap_zo_admin_v226":0,"_cap_zo_admin_v227":0,"_cap_zo_admin_v228":0,"_cap_zo_admin_v229":0,"_cap_zo_admin_v230":0,"_cap_zo_admin_v231":0,"_cap_zo_admin_v232":0,"_cap_zo_admin_v233":0,"_cap_zo_admin_v234":0,"_cap_zo_admin_v235":0,"_cap_zo_admin_v236":0,"_cap_zo_admin_v237":0,"_cap_zo_admin_v238":0,"_cap_zo_admin_v239":0,"_cap_zo_admin_v240":0,"_cap_zo_admin_v241":0,"_cap_zo_admin_v242":0,"_cap_zo_admin_v243":0,"_cap_zo_admin_v244":0,"_cap_zo_admin_v245":0,"_cap_zo_admin_v246":0,"_cap_zo_admin_v247":0,"_cap_zo_admin_v248":0,"_cap_zo_admin_v249":0,"_cap_zo_admin_v250":0,"_cap_zo_admin_v251":0,"_cap_zo_admin_v252":0,"_cap_zo_admin_v253":0,"_cap_zo_admin_v254":0,"_cap_zo_admin_v255":0,"_cap_zo_admin_v256":0,"_cap_zo_admin_v257":0,"_cap_zo_admin_v258":0,"_cap_zo_admin_v259":0,"_cap_zo_admin_v260":0,"_cap_zo_admin_v261":0,"_cap_zo_admin_v262":0,"_cap_zo_admin_v263":0,"_cap_zo_admin_v264":0,"_cap_zo_admin_v265":0,"_cap_zo_admin_v266":0,"_cap_zo_admin_v267":0,"_cap_zo_admin_v268":0,"_cap_zo_admin_v269":0,"_cap_zo_admin_v270":0,"_cap_zo_admin_v271":0,"_cap_zo_admin_v272":0,"_cap_zo_admin_v273":0,"_cap_zo_admin_v274":0,"_cap_zo_admin_v275":0,"_cap_zo_admin_v276":0,"_cap_zo_admin_v277":0,"_cap_zo_admin_v278":0,"_cap_zo_admin_v279":0,"_cap_zo_admin_v280":0,"_cap_zo_admin_v281":0,"_cap_zo_admin_v282":0,"_cap_zo_admin_v283":0,"_cap_zo_admin_v284":0,"_cap_zo_admin_v285":0,"_cap_zo_admin_v286":0,"_cap_zo_admin_v287":0,"_cap_zo_admin_v288":0,"_cap_zo_admin_v289":0,"_cap_zo_admin_v290":0,"_cap_zo_admin_v291":0,"_cap_zo_admin_v292":0,"_cap_zo_admin_v293":0,"_cap_zo_admin_v294":0,"_cap_zo_admin_v295":0,"_cap_zo_admin_v296":0,"_cap_zo_admin_v297":0,"_cap_zo_admin_v298":0,"_cap_zo_admin_v299":0,"_cap_zo_admin_v300":0,"_cap_zo_admin_v301":0,"_cap_zo_admin_v302":0,"_cap_zo_admin_v303":0,"_cap_zo_admin_v304":0,"_cap_zo_admin_v305":0,"_cap_zo_admin_v306":0,"_cap_zo_admin_v307":0,"_cap_zo_admin_v308":0,"_cap_zo_admin_v309":0,"_cap_zo_admin_v310":0,"_cap_zo_admin_v311":0,"_cap_zo_admin_v312":0,"_cap_zo_admin_v313":0,"_cap_zo_admin_v314":0,"_cap_zo_admin_v315":0,"_cap_zo_admin_v316":0,"_cap_zo_admin_v317":0,"_cap_zo_admin_v318":0,"_cap_zo_admin_v
---------------------------	--

 TB

Portainer

□□□□□ /var/lib/docker/volumes/openobserve □ □ **Portainer** □□□□□

```
services:
  openobserve:
    image: public.ecr.aws/zinclabs/openobserve:latest
    container_name: openobserve
    restart: always
    ports:
```


Distribution	sources.list component
Debian 12 (x86-64)	debian-bookworm
Debian 11 (x86-64)	debian-bullseye
Debian Unstable (x86-64)	debian-sid
Debian Testing (x86-64)	debian-testing
Ubuntu 25.04 (x86-64)	ubuntu-plucky
Ubuntu 24.10 (x86-64)	ubuntu-oracular
Ubuntu 24.04 (x86-64)	ubuntu-noble
Ubuntu 23.10 (x86-64)	ubuntu-mantic
Ubuntu 23.04 (x86-64)	ubuntu-lunar
Ubuntu 22.04 (x86-64)	ubuntu-jammy
Ubuntu 20.04 (x86-64)	ubuntu-focal

```
wget -q0 - https://pkg.axoflow.io/axoflow-code-signing-pub.asc | gpg --dearmor > /usr/share/keyrings/axoflow-code-signing-pub.gpg
```

```
echo "deb [signed-by=/usr/share/keyrings/axoflow-code-signing-pub.gpg] https://pkg.axoflow.io/apt stable debian-bookworm" | tee --append /etc/apt/sources.list.d/axoflow.list
```

```
apt update
```

```
apt install axosyslog
```

openobserve

default

重置 Token

数据源

推荐自定义Web ServersDatabasesSecurityDevOpsNetworkingMessage QueuesLanguages/FrameworksOther

日志

指标

追踪

Curl

Filebeat

FluentBit

Fluentd

Vector

OTEL Collector

Logstash

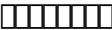
Syslog-Ng

```
destination d_openobserve_http {
  openobserve-log(
    url("http://192.168.0.245:9002")
    organization("default")
    stream("syslog-ng")
    user("root@example.com")
    password("9aoK6vydrDCjzAtw")
  );
};

log {
  source(s_src);
  destination(d_openobserve_http);
  flags(flow-control);
};

Check further documentation at https://axoflow.com/docs/axosyslog-core/chapter-destinations/openobserve/
```

systemctl restart syslog-ng.service



openobserve

default

查询

1 Query Editor:

syslog-ng

搜索字段

_timestamp

facility

host

isodate

message

pid

priority

program

Showing 1 to 29 out of 29 events in 61 ms.(Scan Size: 0.00 MB)

50

1

时间 (Asia/Taipei)	source
> 2025-11-19 10:57:04.000	("_timestamp":"1763521024000000","facility":syslog,"host":lab-pve,"isodate":2025-11-19T10:57:04+08:00,"message":--- MARK --,"priorit
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":daemon,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":Started session-462
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":auth,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":New session 46280 of
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":daemon,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":Started session-462
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":authpriv,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":pam_unix(sshd:ses
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":auth,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":New session 46280 of
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":authpriv,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":pam_unix(sshd:ses
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":auth,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":Accepted password for
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":authpriv,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":pam_env(sshd:ses
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":auth,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":Accepted password for
> 2025-11-19 10:56:00.000	("_timestamp":"1763520960000000","facility":authpriv,"host":lab-pve,"isodate":2025-11-19T10:56:00+08:00,"message":pam_env(sshd:ses
> 2025-11-19 10:54:09.000	("_timestamp":"1763520849000000","facility":syslog,"host":home-pve,"isodate":2025-11-19T10:54:09+08:00,"message":--- MARK --,"priori
> 2025-11-19 10:53:44.000	("_timestamp":"1763520824000000","facility":daemon,"host":OpenWrt,"isodate":2025-11-19T10:53:44+08:00,"message":possible DNS-rebind

Revision #2
Created 13 November 2025 14:55:39 by Jason
Updated 19 November 2025 03:02:58 by Jason