v1.18_WIDS

-
-
-
  -
  -
  - eltex-wids-service
  - /etc/eltex-wids-service/config.hocon
-
  -
    -
    -
    - MongoDB
    -

WIPS/WIDS - () .

, , , , .

(1.18.0) :

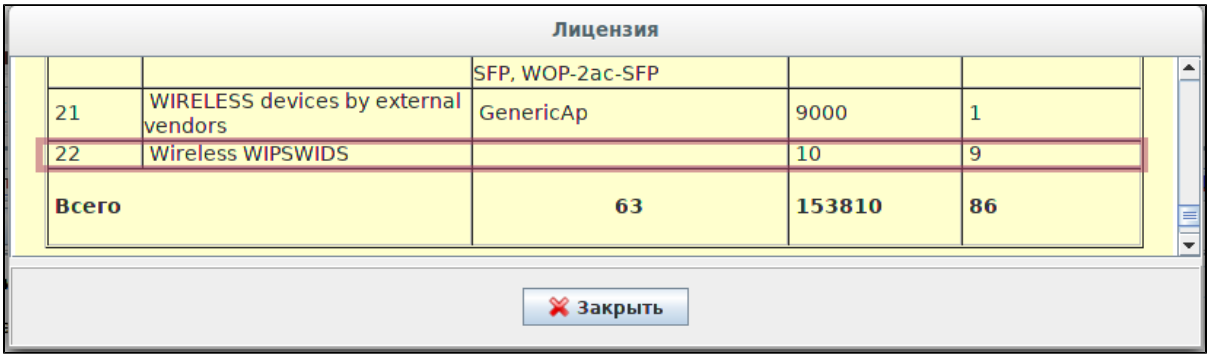
1. DDoS ;
2. ;
3. ;
4. , SSID;
5. , MAC;
6. ;
7. .

eltex-wids-service - , / "" WIPS/WIDS.

WIPS/WIDS .

- EMS (-) 2- .

GUI EMS :



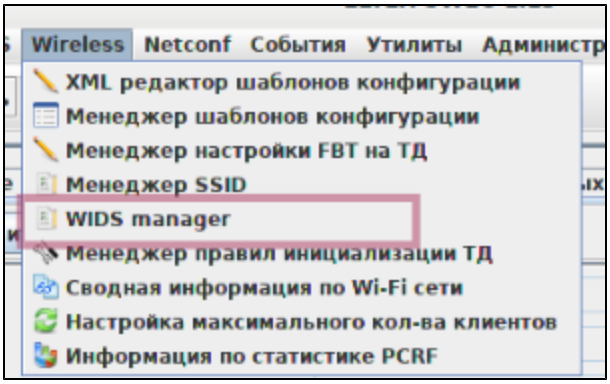
/usr/lib/eltex-ems/conf/licence

/licence.xml:

/usr/lib/eltex-ems/conf/licence/licence-dist.xml

```
        <group>
            <title>Wireless WIPSWIDS</title>
            <count>10</count>
            <typeList>
                <type>WiFi</type>
            </typeList>
        </group>
```

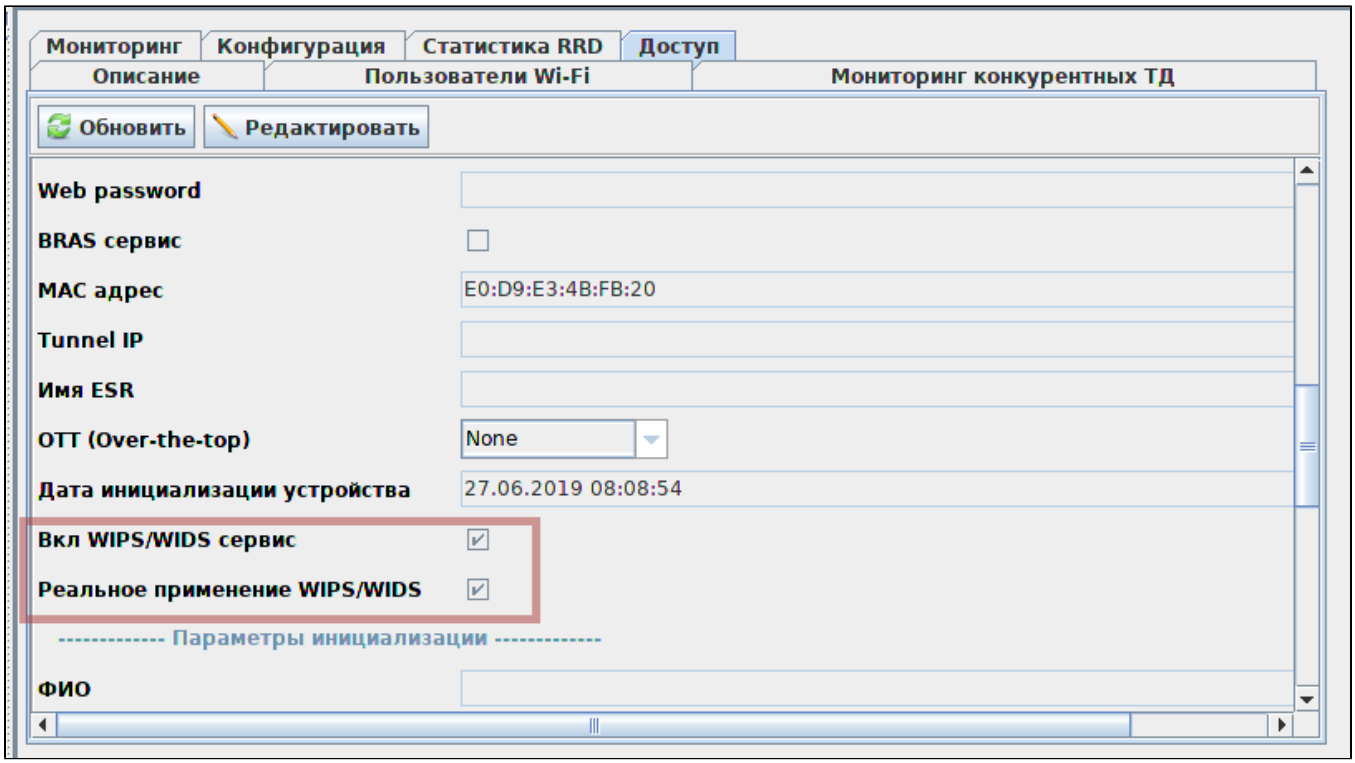
WIPS/WIDS , GUI EMS "*Wireless*" "*WIDS manager*":



"" .

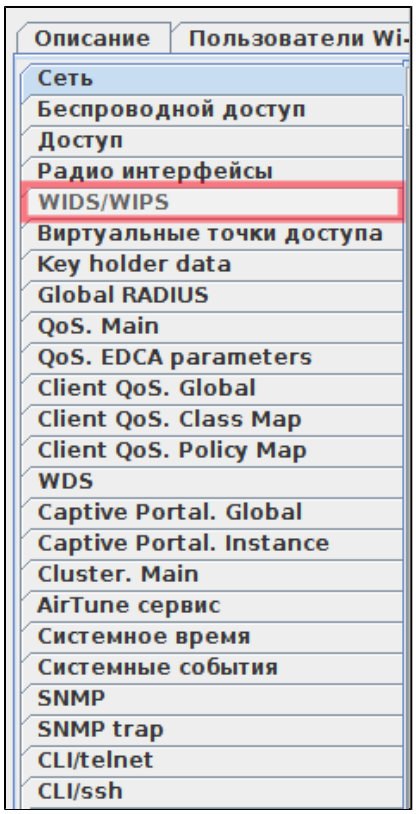
GUI EMS . :

- " WIDS/WIPS " - , . , , WIDS/WIPS, 1. - - WIPS/WIDS .
- " WIDS/WIPS" - , . , " WIDS/WIPS " , , , .



, , :

- "" :
  1. " WIDS/WIPS ";
  2. " WIDS/WIPS".
- "" - "*WIDS/WIPS*"



:

1. " " - , , ;
2. "" - , ;
3. "" - , - , MAC- SSID .

" " , Beacon , WIDS, .

, *Shared key* .

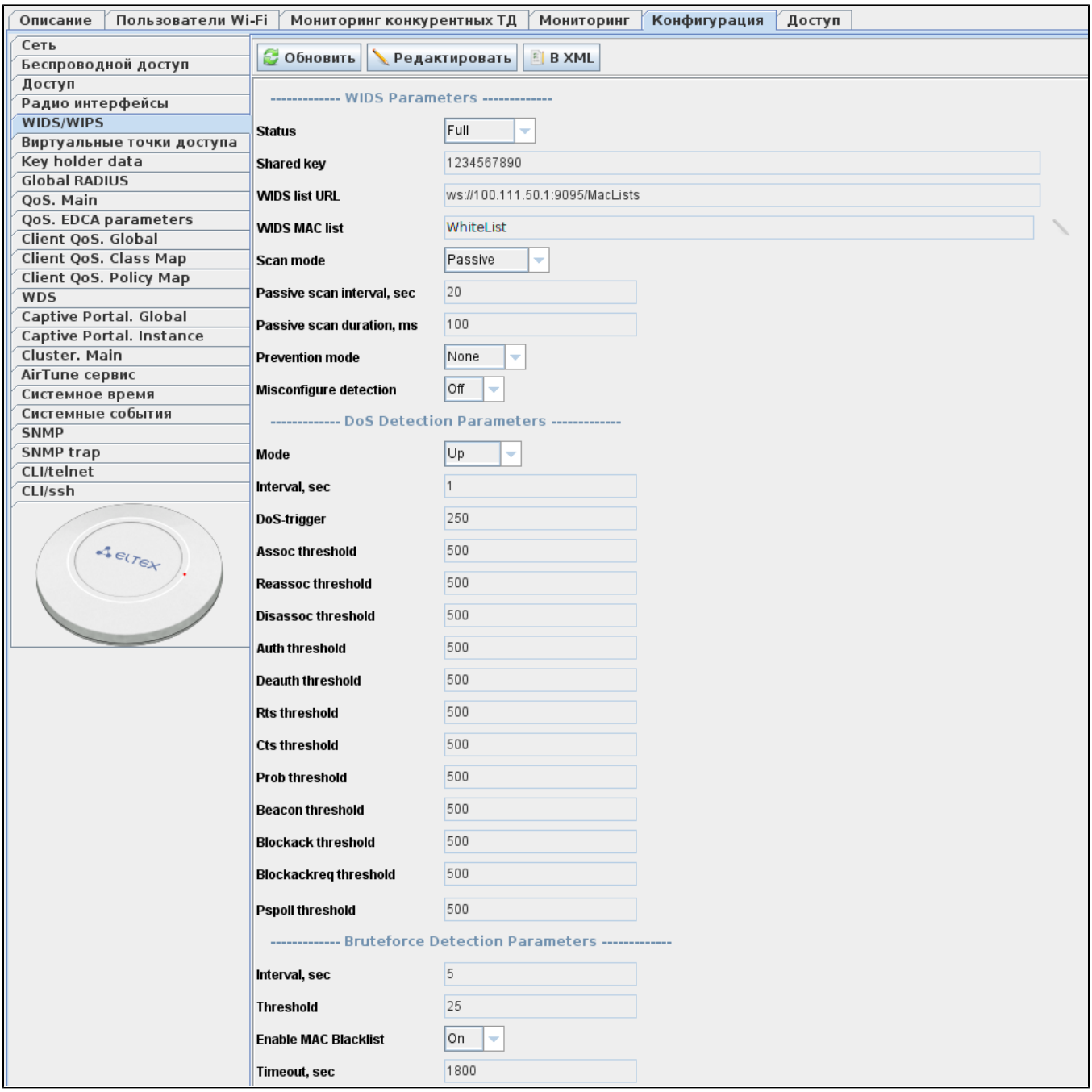
, , , , " ". ""

" " MAC- SSID, , "", , .

```
              : 2019-05-13 15:31:04
         : WEP-12ac_13
                :      : E0:D9:E3:4F:9D:F0, ssid Eltex-Local,  1!
                : CRITICAL
OID                       : 1.3.6.1.4.1.35265.1.60.1.8.3.0.2
```

, , "" . *eltex-wids-service.*

"*WIDS/WIPS*" "*:*



WIDS Parameters		
Status	Full/Down/Key-only	Full - . **Down** - . -. Key-only - , . Key-only Beacon , "", . *Shared key.*
Shared key	ASCII 10 32	, . - , .

WIDS list URL	ws://<ip>:<port>/MacLists	eltex-wids-service. .
WIDS MAC list		MAC-, *"Wireless - WIDS Manager"* .
Scan mode	Passive/Sentry/Home-only	. **Passive** - (*Passive scan interval*) (*Passive scan duration*) ( ) , . , , . -. Sentry - - . . Home-only - , . Passive , .
Passive scan interval, sec	5..3600	. -: *20* .
Passive scan duration, ms	10..2000	. -: *100* .
Home-only scan interval, sec	5..3600	Home-only. -: *20* .
Home-only scan duration, ms	10..2000	Home-only. -: *100* .
Prevention mode	None/Rogue/All	. **None** - . -. Rogue - MAC- , "" , DeAuth "" "" . All - DeAuth , "" , , " " .
Misconfigure detection	Off/On	, , . -: *off* - v1.17_ : 01.07.2019 02:13:09 : wep12 : . system: ; wids-service: ; : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.6
DoS Detection Parameters		
Mode	Up/Down	DoS-. -: *down.* DoS . , destination mac mac- . (Beacon)
Interval, sec	1..86400	, . , SNMP- . : 08.07.2019 17:30:20 : WEP-12ac_13 : " " wlan1(5GHz): Beacon (159 99). 40 : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.8.3.0.1 -: *1* .
DoS-trigger	1..1000000000	, , DoS-. -: *250.*
... treshlold	1..10000	(Assoc, ReAssoc, DiAssoc, Auth, DeAuth, RTS, CTS, Prob, Beacon, BlockAck, BlockAckReq, Pspoll) -: *500.*
Bruteforce Detection Parameters		

Interval, sec	0..86400	. SSID (Personal Enterprise) . Threshold , " ". : 12.07.2019 14:37:02 : WEP-12ac_13 : " " wlan0vap2(2.4GHz)(_ES_24_test_timers_enter), -: 0c:9d:92:6e:d9:20 : CRITICAL OID : 1.3.6.1.4.1.35265.1.60.1.1.1.14 *-: 5 .* Interval = 0, " " .
Threshold	1..10000	. *-: 25.*
Enable MAC Blacklist	On/Off	MAC- , " ", Timeout. "MAC Blacklist" Timeout, , . *-: off*
Timeout, sec	1..86400	MAC- . *-: 1800*

1.18.0 . (*ap-security*) - :

180 3 (login/password) telnet/ssh/web/consol, ip- , , 5 , .

```
: 19.09.2019 13:26:02
: WEP-12ac_13
: tel c 100.111.50.151.
: MAJOR
OID : 1.3.6.1.4.1.35265.1.60.1.7.1.1
```

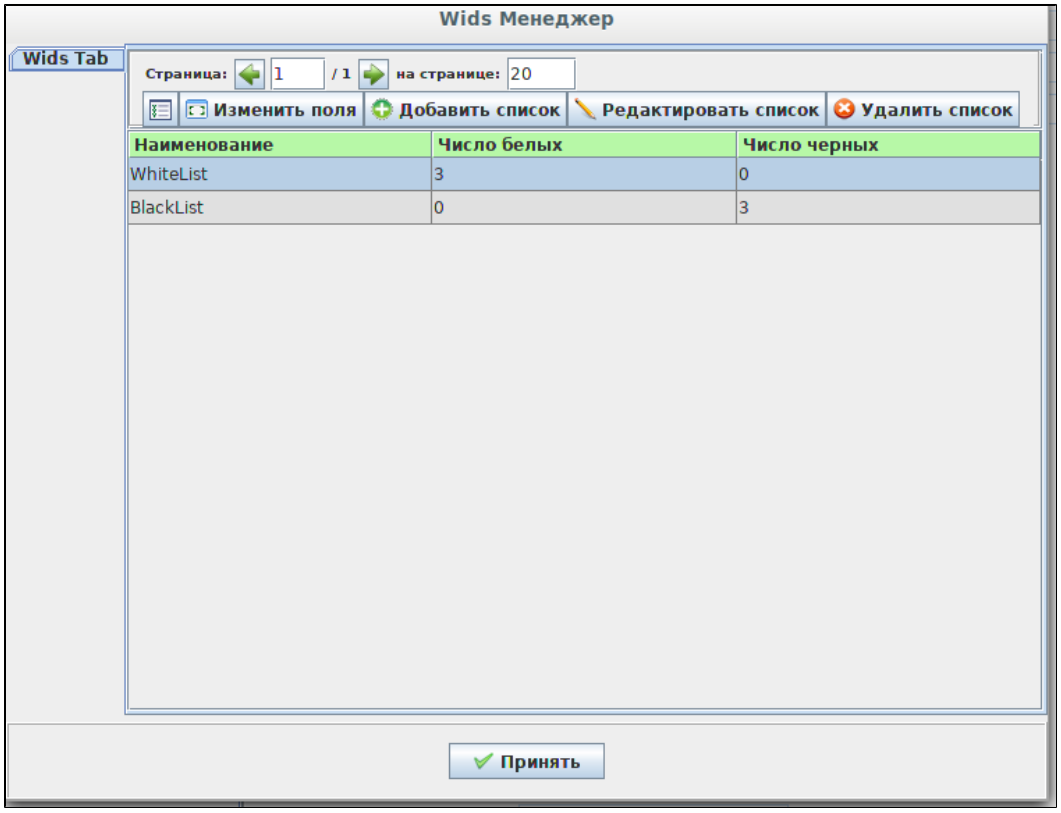
logon-snmp-retries	0..127	, logon-snmp-interval, ip- " ". *: 3*
logon-snmp-interva, sec	1..86400	, . *: 180*
logon-snmp-freeze-interval, sec	0..600	, ip- , , . *: 300*

, / , CLI .

```
    : get ap-security
  :
Property                    Value
--------------------------------
logon-snmp-retries          3
logon-snmp-interval         180
logon-snmp-freeze-interval  300

    : set ap-security <_> <>
: set ap-security logon-snmp-interval 86400

    : set ap-security logon-snmp-retries 0

     : save-running
```

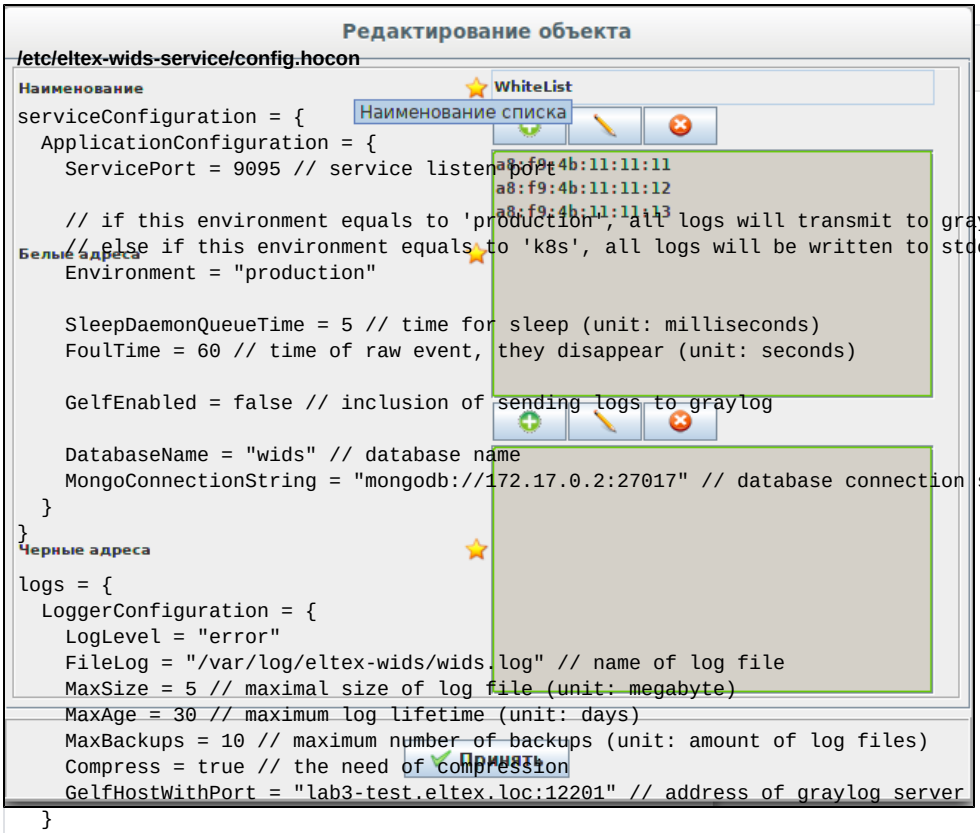
eltex-wids-service

"" "" GUI EMS (*"Wireless WIDS Manager"*) "*WIDS MAC list*" "*WIDS/WIPS*" "".



/etc/eltex-wids-service/config.hocon

.




```
serviceConfiguration = {
  ApplicationConfiguration = {
    ServicePort = 9095 // service listen port

    // if this environment equals to 'production', all logs will transmit to graylog
    // else if this environment equals to 'k8s', all logs will be written to stdout
    Environment = "production"

    SleepDaemonQueueTime = 5 // time for sleep (unit: milliseconds)
    FoulTime = 60 // time of raw event, they disappear (unit: seconds)

    GelfEnabled = false // inclusion of sending logs to graylog

    DatabaseName = "wids" // database name
    MongoConnectionString = "mongodb://172.17.0.2:27017" // database connection string
  }
}
logs = {
  LoggerConfiguration = {
    LogLevel = "error"
    FileLog = "/var/log/eltex-wids/wids.log" // name of log file
    MaxSize = 5 // maximal size of log file (unit: megabyte)
    MaxAge = 30 // maximum log lifetime (unit: days)
    MaxBackups = 10 // maximum number of backups (unit: amount of log files)
    Compress = true // the need of compression
    GelfHostWithPort = "lab3-test.eltex.loc:12201" // address of graylog server
  }
}
```

- , :

```
ServicePort = 9095
```

- . 2 : "production" - Graylog, "k8s" - stdout.

```
Environment = "production"
```

- Graylog:

```
GelfEnabled = false
```

- , :

```
DatabaseName = "wids"
```

- :

```
MongoConnectionString = "mongodb://172.17.0.2:27017"
```

- :

```
LogLevel = "error"
```

- :

```
FileLog = "/var/log/eltex-wids/wids.log"
```

- :

```
MaxSize = 5
```

- :

```
MaxAge = 30
```

- :

```
MaxBackups = 10
```

- :

```
Compress = true
```

- Graylog:

```
GelfHostWithPort = "lab3-test.eltex.loc:12201"
```

---

docker-. .env docker-compose.yml

docker-compose.yml

```
version: "3"

services:
  wids:
    image: hub.eltex-co.ru/softwlc/eltex-wids:1.18-467
    ports:
      - 9095:9095
    volumes:
      - "/var/log/eltex-wids:/var/log/eltex-wids"
      - "/etc/eltex-wids-service/config.hocon:/etc/eltex-wids-service/config.hocon"
    environment:
      - LogLevel=${WIDS_LOG_LEVEL}
      - MongoUrl=${WIDS_MONGO_URL}
      - DBName=${WIDS_DB_NAME}
      - SleepDaemonQueueTime=${WIDS_SLEEP_DAEMON_QUEUE_TIME}
      - FoulTime=${WIDS_FOUL_TIME}
```

.env

```
WIDS_LOG_LEVEL=error
WIDS_MONGO_URL=mongodb://<IP-address>:27017
WIDS_DB_NAME=wids
WIDS_SLEEP_DAEMON_QUEUE_TIME=5
WIDS_FOUL_TIME=60
```

- **ServicePort** - , .

- **SleepDaemonQueueTime** - ;
- **FoulTime** - .

MongoDB

- **DBName** -
- **MongoUrl** - MongoDB-.

- **LogLevel** - (ERROR, INFO, DEBUG);
- **FileLog** - ;
- **MaxSizeFileLog** - - ;
- **MaxAgeFileLog** - - ;
- **MaxBackupsFileLog** - ;
- **CompressLogs** - -;
- **GelfHostWithPort** - GrayLog;
- **LogEnvironment** - ; , (file/stdout);
- **GelfEnabled** - GrayLog.