

5 июня 2024 • Москва, LOFT HALL#2

БЕКОН'24

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Вы еще не читаете Audit Log?
Тогда мы идем к Вам!

Алиса Кириченко

Лаборатория Числитель



лаборатория
ЧИСЛИТЕЛЬ

О СЕБЕ



Алиса Кириченко

Ведущий аналитик платформы контейнерной оркестрации «Штурвал»

Лаборатория Числитель

СЦЕНАРИЙ ДОКЛАДА

10%



Зачем нужны
Kube-Audit логи?

10%



Откуда берутся
Kube-Audit логи?

20%



Куда разместить логи,
чтобы не выстрелить в ногу?

30%



Как создать
политику для
записи логов?

30%



Рекомендации, нюансы
и немного личного опыта
на сладкое

ЗАЧЕМ НУЖНЫ KUBE-AUDIT ЛОГИ?



ЗАЧЕМ НУЖНЫ KUBE-AUDIT ЛОГИ?



Права доступа



Сетевые политики



Запуск контейнеров



Конфигурации и другое

ЗАЧЕМ НУЖНЫ KUBE-AUDIT ЛОГИ?



Права доступа



Сетевые политики



Запуск контейнеров



Конфигурации и другое



Кто запросил?

Какой ресурс?

Какое действие?

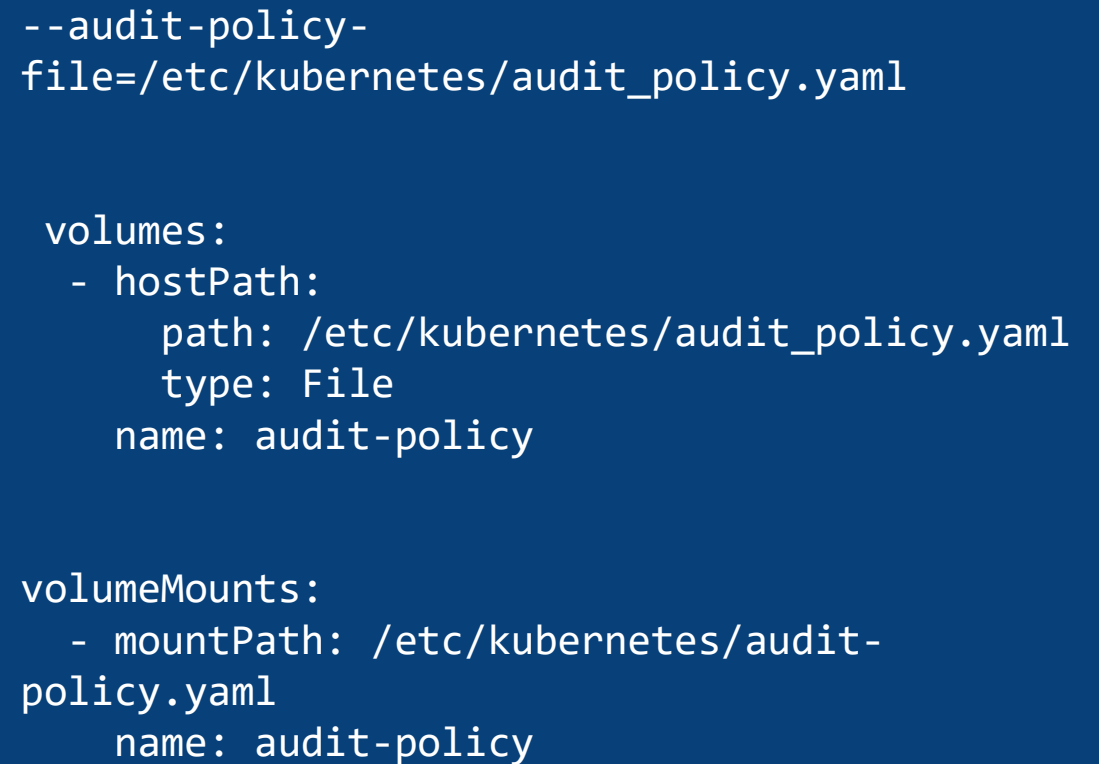
Когда запросил?

Где это произошло?

С каким результатом?

ОТКУДА БЕРУТСЯ KUBE-AUDIT ЛОГИ?





КАК СОЗДАТЬ ПОЛИТИКУ ДЛЯ ЗАПИСИ ЛОГОВ?



Когда и сколько записываем?

stage

level

verbs

Что, где и от кого записываем?

- Users
- Usergroups
- Namespaces
- Nonresourceurls (/metrics, /healthz*)
- Resources
- Resourcenames



**ПОДРОБНЕЕ О ТОМ,
КАК СОБРАТЬ ПОЛИТИКУ
ЕСТЬ НА ОФИЦИАЛЬНОМ
САЙТЕ KUBERNETES,
А ТАКЖЕ НА YOUTUBE**

СТАДИИ

RequestReceived

ResponseStarted

ResponseComplete

Panic

omitStages

```
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
  - "RequestReceived"
  - "ResponseStarted"
rules:
...
```

None

для исключений

```
- level: None
  userGroups:
  ["system:authenticated"]
  nonResourceURLs:
  - "/api*"
  - "/version"
```

None

для исключений

```
- level: None
  userGroups:
["system:authenticated"]
  nonResourceURLs:
  - "/api*"
  - "/version"
```

Metadata

факт запроса
или чувствительная
информация

```
- level: Metadata
  verbs: ["create",
"update", "delete", "get"]
  resources:
  - group: ""
resources: ["secrets",
"configmaps"]
```

```
{
  "apiVersion": "audit.k8s.io/v1",
  "kind": "Event",
  "stageTimestamp": "2024-05-31T08:24:03.050866Z",
  "level": "Metadata",
  "requestReceivedTimestamp": "2024-05-31T08:24:03.049386Z",
  "auditID": "908027cf-c1ad-428b-a70f-43914113f1f4",
  "verb": "get",
  "stage": "ResponseComplete",
  "objectRef": {
    "namespace": "myclustername-sec",
    "resource": "secrets",
    "name": "myclustername-sec-kubeconfig",
    "apiVersion": "v1"
  },
  "requestURI": "/api/v1/namespaces/myclustername-sec/secrets/myclustername-sec-kubeconfig",
  "userAgent": "sh-backend-api/v0.0.0 (linux/amd64) kubernetes/$Format",
  "sourceIPs": [
    "10.XX.XXX.214"
  ],
}
```

```
"responseStatus": {
  "metadata": {},
  "code": 200
},
"user": {
  "groups": [
    "system:authenticated"
  ],
  "username": "a.kirichenko"
}
...
```

None

для исключений

```
- level: None
  userGroups:
  ["system:authenticated"]
  nonResourceURLs:
  - "/api*"
  - "/version"
```

Metadata

факт запроса
или чувствительная
информация

```
- level: Metadata
  verbs: ["create",
"update", "delete", "get"]
  resources:
  - group: ""
resources: ["secrets",
"configmaps"]
```

Request

данные тела
запроса

```
- level: Request
  resources:
  - group: ""
    resources:
  ["pods/exec"]
```



```
{
  "kind": "Event",
  "apiVersion": "audit.k8s.io/v1",
  "level": "Request",
  "auditID": "b98bb1d4-bcf4-4b60-bf53-0564303b2c02",
  "stage": "ResponseComplete",
  "requestURI":
"/apis/cilium.io/v2/namespaces/bekon/ciliumnetworkpolicies?timeout=1m0s",
  "verb": "create",
  ...
  "objectRef": {
    "resource": "ciliumnetworkpolicies",
    "namespace": "default",
    "name": "bekon-test-policy",
    "apiGroup": "cilium.io",
    "apiVersion": "v2"
  },
  "responseStatus": {
    "metadata": {},
    "code": 201
  },
}
```



```
"requestObject": {
  "apiVersion": "cilium.io/v2",
  "kind": "CiliumNetworkPolicy",
  "metadata": {
    "creationTimestamp": "2024-05-31T20:33:51.400917Z",
    "name": "bekon-test-policy",
    "namespace": "bekon"
  },
  "spec": {
    "egress": [
      {
        "toEntities": [
          "cluster"
        ]
      }
    ],
    "endpointSelector": {},
    "ingress": [
      {
        "fromEntities": [
          "cluster"
        ]
      }
    ]
  }
}
```

None

для исключений

```
- level: None
  userGroups:
  ["system:authenticated"]
  nonResourceURLs:
  - "/api*"
  - "/version"
```

Metadata

факт запроса
или чувствительная
информация

```
- level: Metadata
  verbs: ["create",
"update", "delete", "get"]
  resources:
  - group: ""
resources: ["secrets",
"configmaps"]
```

Request

данные тела запроса

```
- level: Request
  resources:
  - group: ""
resources:
["pods/exec"]
```

RequestResponse

последствия
изменений

```
- level: RequestResponse
  verbs: ["create",
"patch", "update"]
  resources:
  - group: ""
resources: ["pods"]
```

REQUESTRESPONSE

```
...
"requestObject": {
  "kind": "Pod",
  "apiVersion": "v1",
  "metadata": {
    "name": "test-bekon",
    "namespace": "default",
    "creationTimestamp": null,
    "labels": {
      "app": "test-bekon"
    }
  },
  "spec": {
    "containers": [
      {
        "name": "containername",
        "image": "somedestination.tech/someimage",
        "resources": {},
        "terminationMessagePath": "/dev/termination-log",
        "terminationMessagePolicy": "File",
        "imagePullPolicy": "IfNotPresent"
      }
    ]
  }
}
...
```

```
"responseObject": {
  "kind": "Pod",
  "apiVersion": "v1",
  "metadata": {
    "name": "test-bekon",
    "namespace": "default",
    "uid": "b9c0fdb4-d3f3-417a-be06-9f1bc9add688",
    "resourceVersion": "12547816",
    "creationTimestamp": null,
    "labels": {
      "app": "test-bekon"
    }
  },
  "spec": {
    "containers": [
      {
        "name": "containername",
        "image": "sonedestination.tech/someimage",
        "resources": {},
        "terminationMessagePath": "/dev/termination-log",
        "terminationMessagePolicy": "File",
        "imagePullPolicy": "IfNotPresent"
      }
    ]
  }
}
...
```

ЗАКРЕПЛЕНИЕ РЕЦЕПТА



**Записывать вообще всё
не нужно. Совсем без правил
тоже нельзя.**



**Когда важна создаваемая/
изменяемая спецификация
– на уровне request**



**Ресурсы, содержащие
чувствительную информацию,
– на уровне metadata**



**Ресурсы, которые могут быть
изменены в процессе создания,
– на уровне requestresponse**

ЗАКРЕПЛЕНИЕ РЕЦЕПТА



Фильтры пишем по принципу от частного к общему

```
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
  - "RequestReceived"
rules:
  # Регистрировать события создания подов
  - level: Request
    resources:
      - group: ""
        resources: ["pods"]
        verbs: ["create"]
  # Не регистрировать события создания подов в
  # namespace test
  - level: None
    resources:
      - group: ""
        resources: ["pods"]
        namespaces: ["test"]
        verbs: ["create"]
```



```
apiVersion: audit.k8s.io/v1
kind: Policy
omitStages:
  - "RequestReceived"
rules:
  # Не регистрировать события создания подов в
  # namespace test
  - level: None
    resources:
      - group: ""
        resources: ["pods"]
        namespaces: ["test"]
        verbs: ["create"]
  # Регистрировать события создания подов во всех
  # остальных namespace
  - level: Request
    resources:
      - group: ""
        resources: ["pods"]
        verbs: ["create"]
```



**КУДА РАЗМЕСТИТЬ ЛОГИ,
ЧТОБЫ НЕ ВЫСТРЕЛИТЬ
В НОГУ?**





Log Backend



- + Не требует сторонних приложений
- + Простая настройка
- + Данные не теряются



- Использует локальное хранилище
- Поиск логов на узлах
- Медленная запись на диск

Webhook backend?



- + Быстрая запись по сети
- + Логи в одном месте



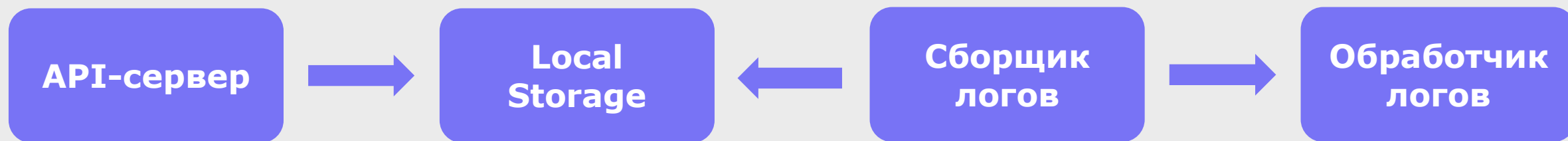
- Нужен webhook и HTTP-сервер
- Нагружает API-сервер
- Зависит от окружения

`apiserver_audit_event_total` -

общее количество экспортированных событий аудита

`apiserver_audit_error_total` -

общее количество событий, потерянных из-за ошибки во время экспорта



- 1 | Может быть использован в разных окружениях**
- 2 | Не занимает место на диске**
- 3 | Возможность просмотра логов в одном окне**
- 4 | Доступ к логам на узлах**
- 5 | Не требует отслеживания метрик для масштабирования**

СРАВНЕНИЕ ПОДХОДОВ

Характеристика	Log Backend	Webhook Backend	Log Backend +
Сложность настройки	Низкая	Средняя/Высокая	Средняя
Необходимость дополнительных сервисов	Нет	Да	Да
Удобство анализа логов	Среднее	Высокое	Высокое
Надежность	Высокая	В зависимости от доп. сервисов	Высокая
Масштабируемость	Низкая	Высокая	Высокая
Скорость работы	Средняя	В зависимости от доп. сервисов	Средняя

РЕЖИМЫ ЗАПИСИ/ОТПРАВКИ ДАННЫХ



BLOCKING

- последовательная обработка данных
- запись поочередно



BLOCKING-STRICT

- последовательная обработка данных
- блокирование запроса, если нет возможности аудировать



BATCH

- одновременная обработка данных
- запись данных пакетами



и еще

30+
параметров

**для конфигурации
API-сервера...**

РЕКОМЕНДАЦИИ, НЮАНСЫ И НЕМНОГО ЛИЧНОГО ОПЫТА НА СЛАДКОЕ



КОРОТКО О ГЛАВНОМ

API есть, а поработать с ним как с другими YAML ресурсами по RESTful нельзя

Изменения параметров политики и сбора логов требуют перезапуска API-сервера

На всех Master-узлах должна быть одинаковая политика

Ошибки в YAML приводят к падению API-сервера

На все правила только 1 политика

Не является Policy Engine инструментом



**КАК УПРАВЛЯТЬ ПОЛИТИКОЙ
НА ВСЕХ МАСТЕРАХ СРАЗУ
РАССКАЗЫВАЕМ НА YOUTUBE**



ANONYMOUS

```
{ "kind": "Event", "apiVersion": "audit.k8s.io/v1", "level": "Metadata", "auditID": "76ff5b20-95d8-4e11-a83e-245026c6d2a5", "stage": "ResponseComplete", "requestURI": "/readyz", "verb": "get", "user": { "username": "system:anonymous", "groups": [ "system:unauthenticated" ], "sourceIPs": [ "10.XX.XXX.41" ], "userAgent": "kube-probe/1.28", "responseStatus": { "metadata": {}, "code": 200 } }
```

USER

```
{ "_index": "myclustername-2024.05.20", "_id": "5E2E146A-BC30-1C5A-4572-922838957A9E", "_version": 1, "_score": 0, "_source": { "@timestamp": "2024-05-20T10:12:11.665Z", "impersonatedUser": { "groups": [ "shturval:namespace-admin", "system:authenticated" ], "username": "shturval:p.petrov" } }
```

SERVICEACCOUNT

```
{ "_index": "myclustername-ruzanov-dev-2024.05.20", "_id": "5259BDE3-163C-8046-7F48-A5761DC7F8F4", "_version": 1, "_score": 0, "_source": { "@timestamp": "2024-05-20T09:29:41.061Z", "requestReceivedTimestamp": "2024-05-20T09:29:41.058914Z", "user": { "groups": [ "system:serviceaccounts", "system:serviceaccounts:kyverno", "system:authenticated" ], "username": "system:serviceaccount:kyverno:shturval-policy-manager-admission-controller" }
```


РЕГИСТРИРУЕТ ВСЁ!...

```
_ "annotations": {
  "authorization.k8s.io/decision": "allow",
  "authorization.k8s.io/reason": "RBAC: allowed by
ClusterRoleBinding \"system:controller:replicaset-
controller\" of ClusterRole
\"system:controller:replicaset-controller\" to
ServiceAccount \"replicaset-controller/kube-system\"",

  "mutation.webhook.admission.k8s.io/round_0_index_1":
  "{ \"configuration\": \"kyverno-resource-mutating-
webhook-cfg\", \"webhook\": \"mutate.kyverno.svc-
ignore\", \"mutated\": false }",

  "mutation.webhook.admission.k8s.io/round_0_index_2":
  "{ \"configuration\": \"kyverno-resource-mutating-
webhook-cfg\", \"webhook\": \"mutate.kyverno.svc-
fail\", \"mutated\": true }",
```

```
"mutation.webhook.admission.k8s.io/round_1_index_1":
"{ \"configuration\": \"kyverno-resource-mutating-
webhook-cfg\", \"webhook\": \"mutate.kyverno.svc-
ignore\", \"mutated\": false }",

  "patch.webhook.admission.k8s.io/round_0_index_2":
  "{ \"configuration\": \"kyverno-resource-mutating-
webhook-cfg\", \"webhook\": \"mutate.kyverno.svc-
fail\", \"patch\": [{ \"op\": \"add\", \"path\": \"/metadata/
labels/alisa\", \"value\": \"iscool\" }, { \"op\": \"add\", \"
path\": \"/metadata/annotations\", \"value\": { \"policies.
kyverno.io/last-applied-patches\": \"add-labels.add-
labels.kyverno.io: added
/metadata/labels/alissa\\n\\\" } } ], \"patchType\": \"JSONPat
ch\" }",

  "pod-security.kubernetes.io/enforce-policy":
  "privileged:latest"
}
}
```

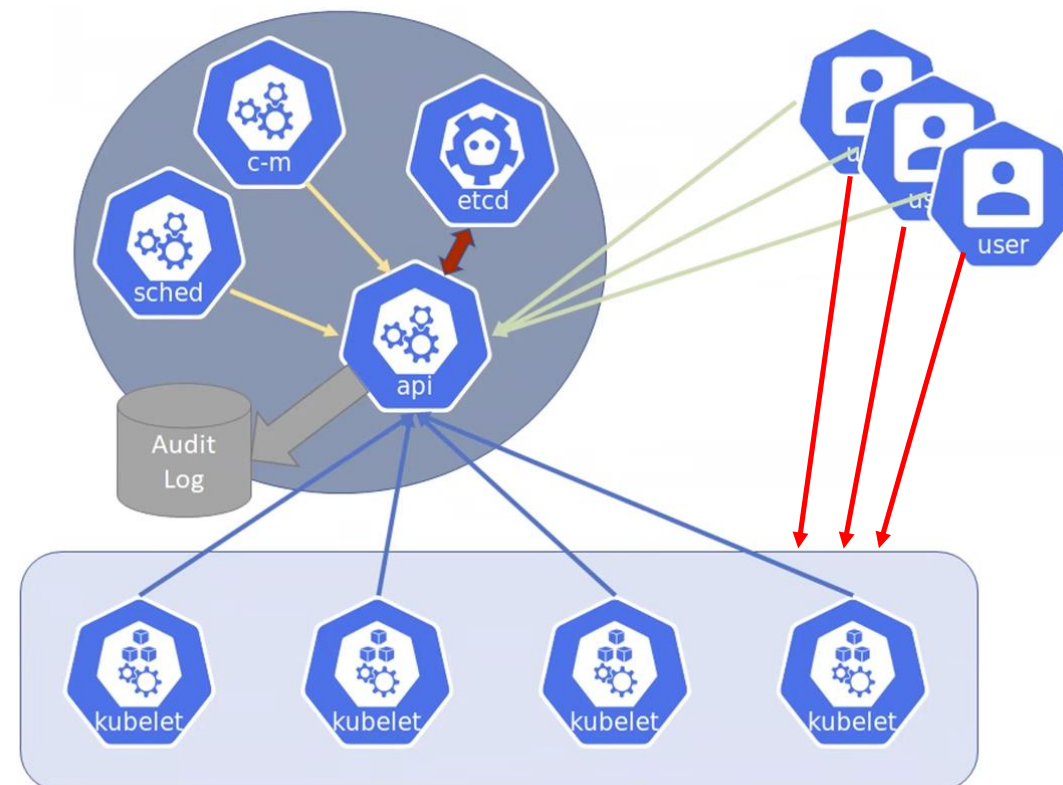
ИЛИ НЕ ВСЁ?



Не логирует
аутентификацию



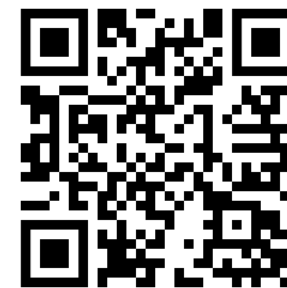
Не логирует
Node/proxy



События аудита можно подделать с помощью заголовков
X-Forwarded-For и **X-Real-IP**

```
curl -H 'Audit-ID: Lorem' -H 'X-Forwarded-For: 8.8.8.8'  
http://127.0.0.1:8001/api/v1/pods/
```

```
{"kind":"Event","apiVersion":"audit.k8s.io/v1","level":"Metadata","auditID":"Lorem","stage":"ResponseComplete","requestURI":"/api/v1/pods/","verb":"list","user":{"username":"kubernetes-admin","groups":["system:masters","system:authenticated"]},"sourceIPs":["8.8.8.8","127.0.0.1","172.18.0.1"],"userAgent":"curl/7.81.0","objectRef":{"resource":"pods","apiVersion":"v1"},"responseStatus":{"metadata":{},"code":200},"requestReceivedTimestamp":"2023-10-01T09:28:15.307641Z","stageTimestamp":"2023-10-01T09:28:15.313353Z","annotations":{"authorization.k8s.io/decision":"allow","authorization.k8s.io/reason":""}}
```



**ПОДРОБНЕЕ
О ЗАГОЛОВКАХ**

Kubernetes добавляет системные поля в managed fields, из-за которых не все записи могут быть доставлены во внешний сервис

```
"managedFields": [  
  {  
    "apiVersion": "permissions.shturval.tech/v1beta1",  
    "fieldsType": "FieldsV1",  
    "fieldsV1": {  
      "f:metadata": {  
        "f:annotations": {  
          ".": {  
            },  
          },  
        "f:kubect1.kubernetes.io/last-applied-configuration": {  
          },  
        },  
      },  
    },  
  ],  
]
```

```
apiVersion: fluentbit.fluent.io/v1alpha2
kind: ClusterFilter
metadata:
  name: kube-api-audit
labels:
  fluentbit.fluent.io/enabled: "true"
  fluentbit.fluent.io/component: logging
```

```
spec:
  match: kube-api-audit
  filters:
    - lua:
        script:
          key: kube-api-audit.lua
          name: fluent-bit-kube-api-audit-config
        call: drop_managed_fields
        timeAsTable: true
```

```
apiVersion: v1
kind: ConfigMap
metadata:
  name: fluent-bit-kube-api-audit-configdata:
  kube-api-audit.lua: |
    function drop_managed_fields(tag, timestamp, record)
      if (record.metadata and
record.metadata.managedFields) then
        record["metadata"]["managedFields"] = nil
      end
    end
```

```
if (record.requestObject and record.requestObject.metadata
and record.requestObject.metadata.managedFields) then

  record["requestObject"]["metadata"]["managedFields"] = nil
  end

  if (record.responseObject and
record.responseObject.metadata and
record.responseObject.metadata.managedFields) then

    record["responseObject"]["metadata"]["managedFields"] =
nil

    end

    return 2, timestamp, record
  end
```

```
- level: Metadata
  resources:
    - group: "" # core API group
      resources: [ "secrets", "configmaps", "serviceaccount" ]
- level: Request
  verbs: [ "create", "delete", "update", "patch" ]
  resources:
    - group: "ops.shturval.tech"
      resources: [ "shturvalserviceconfigs" ]
- level: Request
  verbs: [ "create", "delete", "update", "patch" ]
  resources:
    - group: "ops.shturval.tech"
      resources: [ "shturvalrepoconfigs" ]
- level: Request
  userGroups: [ "system:authenticated" ]
  verbs: [ "create", "delete", "update", "patch" ]
  resources:
    - group: rbac.authorization.k8s.io
      resources: [ "roles", "clusterroles", "clusterrolebindings",
"rolebindings" ]
- level: Request
  userGroups: [ "system:authenticated" ]
  verbs: [ "create", "delete", "update", "patch" ]
  resources:
    - group: permissions.shturval.tech
      resources: [ "grouproles", "userroles" ]
```

ПАРАМЕТРЫ API СЕРВЕРА

- --audit-log-maxage=30
- --audit-log-maxbackup=10
- --audit-log-maxsize=100
- --audit-log-mode=batch

1 кластер

Env: **PROD**

Master Nodes: **3**

Worker Nodes: **17**

Pods: **380**

Kube-Audit log index: **70 Мб/день**



Регистрирует вызовы с успешным и неуспешным результатом к объектам на нужном уровне детализации



Является встроенным функционалом Kubernetes. Конфигурируется с помощью YAML манифеста



Формат лога в JSON/строках позволяет анализировать в любых системах



Полезно для расследования функциональных сбоев и инцидентов ИБ

5 июня 2024 📍 Москва, LOFT HALL#2
Конференция по БЕзопасности
КОНтейнеров и контейнерных сред



Алиса Кириченко

Ведущий аналитик платформы контейнерной
оркестрации «Штурвал», Лаборатория Числитель



лаборатория
ЧИСЛИТЕЛЬ