**Searches & Use Cases**

Содержание

| № | Название | [CloudLogging](https://cloud.yandex.ru/docs/audit-trails/operations/export-cloud-logging) | [Elasticsearch](https://github.com/yandex-cloud/yc-solution-library-for-security/tree/master/auditlogs/export-auditlogs-to-ELK_main)GitHub - elastic/elasticsearch-php: Official PHP low-level client for  Elasticsearch.  Opensearch OpenSearch | [Yandex Query](https://cloud.yandex.ru/docs/query/concepts/)  (S3 or YDS) |
| --- | --- | --- | --- | --- |
| Searches | | | | |
| 1 | Найти, кто удалил фолдер (!!требует указания значений!!) | json\_payload.event\_type="yandex.cloud.audit.resourcemanager.DeleteFolder" and json\_payload.details.folder\_name="<название каталога>" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.resourcemanager.DeleteFolder and cloud.folder.name: <название каталога> | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.resourcemanager.DeleteFolder' and JSON\_VALUE(data, "$.details.folder\_name") = 'test' limit 100 |
| 2 | Найти, кто создал/остановил/перезапустил/удалил виртуальную машину  (!!требует указания значений!!) | json\_payload.details.instance\_id="<<идентификатор виртуальной машины>>" and (json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.UpdateInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.DeleteInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.StartInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.StopInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.RestartInstance") | event.dataset: yandexcloud.audittrail and event.action : yandex.cloud.audit.compute.\*Instance and cloud.instance.name: testdasdas | select \* from bindings.`binding`  where  (JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.DeleteInstance' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance') and JSON\_VALUE(data, "$.details.instance\_id") = 'fhmpgh36fo3vclan2e99' limit 100  ; |
| 3 | Какие действия совершал конкретный пользователь за период времени  (!!требует указания своих значений!!) | json\_payload.authentication.subject\_name="mirtov8@yandex-team.ru" and json\_payload.event\_time<"2022-03-01" and json\_payload.event\_time<"2022-04-01" | event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru and event\_time < 2022-07-15 | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.authentication.subject\_name") = 'mirtov8@yandex-team.ru' and cast(JSON\_VALUE(data, "$.event\_time")as Timestamp) > Date("2022-08-15") limit 10  ; |
| 4 | Поиск событий по объектам определенного фолдера (!!требует указания значений!!) | json\_payload.resource\_metadata.path[1].resource\_type="resource-manager.folder" and json\_payload.resource\_metadata.path[1].resource\_name="<имя каталога>") or (json\_payload.resource\_metadata.path[2].resource\_type="resource-manager.folder" and json\_payload.resource\_metadata.path[2].resource\_name="<имя каталога>" | event.dataset:yandexcloud.audittrail and cloud.folder.name:"mirtov-scale" | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.resource\_metadata.path[2].resource\_name") = 'mirtov-scale' limit 100  ; |
| 5 | NEWГруппировка событий по источнику события, типу и статусу |  |  | SELECT event\_source, event\_type, event\_status, count(\*) as count FROM (  SELECT  json\_value(data,"$.event\_type") as event\_type, json\_value(data,"$.event\_source") as event\_source, json\_value(data,"$.authentication.subject\_name") as subject\_name, json\_value(data,"$.event\_status") as event\_status, json\_value(data,"$.event\_id") as event\_id, DateTime::MakeDatetime($json\_datetime\_parse(json\_value(data,"$.event\_time"))) as event\_time, json\_value(data,"$.resource\_metadata.path[1].resource\_name") as cloud\_name, json\_value(data,"$.resource\_metadata.path[2].resource\_name") as folder\_name  FROM  bindings.`binding` ) as tbl  GROUP BY event\_source, event\_type, event\_status  LIMIT 100; |
| 6 | NEW *Отображение событий конкретного типа (в связке с запросом из пункта 5)* (!!требует указания значений!!) |  |  | SELECT \* FROM (  SELECT  --data, --выводит полную строку события  json\_value(data,"$.event\_type") as event\_type, json\_value(data,"$.event\_source") as event\_source, json\_value(data,"$.authentication.subject\_name") as subject\_name, json\_value(data,"$.event\_status") as event\_status, json\_value(data,"$.event\_id") as event\_id, json\_value(data,"$.event\_time") as event\_time, json\_value(data,"$.resource\_metadata.path[1].resource\_name") as cloud\_name, json\_value(data,"$.resource\_metadata.path[2].resource\_name") as folder\_name, json\_query(data,"$.authentication") as authentication, json\_value(data,"$.authorization.authorized") as authorized, json\_query(data,"$.details") as details  FROM  bindings.`binding`) as tbl  WHERE event\_type = "yandex.cloud.audit.storage.BucketDelete"  ORDER BY event\_time DESC  LIMIT 100; |
| 7 | NEW *Список событий, отфильтрованных по времени* |  |  | ﻿--Функции для работы со временем - https://yql.yandex-team.ru/docs/yt/udf/list/datetime  $datetime\_parse = DateTime::Parse("%Y-%m-%d %H:%M:%S");  $json\_datetime\_parse = DateTime::Parse("%Y-%m-%dT%H:%M:%SZ");  $format = DateTime::Format("%Y-%m-%d %H:%M:%S %Z");  SELECT \* FROM (  SELECT  json\_value(data,"$.event\_type") as event\_type, json\_value(data,"$.event\_source") as event\_source, json\_value(data,"$.authentication.subject\_name") as subject\_name, json\_value(data,"$.event\_status") as event\_status, json\_value(data,"$.event\_id") as event\_id, DateTime::MakeDatetime($json\_datetime\_parse(json\_value(data,"$.event\_time"))) as event\_time, json\_value(data,"$.resource\_metadata.path[1].resource\_name") as cloud\_name, json\_value(data,"$.resource\_metadata.path[2].resource\_name") as folder\_name  FROM  bindings.`binding` ) as tbl  --WHERE DateTime::MakeDatetime($datetime\_parse("2023-03-02 15:00:00")) <= event\_time and event\_time >= DateTime::MakeDatetime($datetime\_parse("2023-03-02 15:00:00"))  --WHERE event\_time >= CurrentUtcDatetime() - Interval("P1D") --использовать сдвиг по времени, формат строки сдвига - https://en.wikipedia.org/wiki/ISO\_8601#Durations  --ORDER BY event\_time DESC  LIMIT 100; |
| 8 | NEW *Отображение конкретного события (фильтрация по ID события) (!!требует указания значений!!)* |  |  | SELECT  --data, --выводит полную строку события  json\_value(data,"$.event\_type") as event\_type, json\_value(data,"$.event\_source") as event\_source, json\_value(data,"$.authentication.subject\_name") as subject\_name, json\_value(data,"$.event\_status") as event\_status, json\_value(data,"$.event\_id") as event\_id, json\_value(data,"$.event\_time") as event\_time, json\_value(data,"$.resource\_metadata.path[1].resource\_name") as cloud\_name, json\_value(data,"$.resource\_metadata.path[2].resource\_name") as folder\_name, json\_query(data,"$.authentication") as authentication, json\_value(data,"$.authorization.authorized") as authorized, json\_query(data,"$.details") as details  FROM  bindings.`binding`  WHERE json\_value(data,"$.event\_id") = "bpfrukrd6bbkdva3sbkh"  LIMIT 100; |
| 9 | NEW *Отображение всех событий с парсингом по полям (преобразует JSON в кологки)* |  |  | SELECT  json\_value(data,"$.event\_type") as event\_type, json\_value(data,"$.event\_source") as event\_source, json\_value(data,"$.authentication.subject\_name") as subject\_name, json\_value(data,"$.event\_status") as event\_status, json\_value(data,"$.event\_id") as event\_id, json\_value(data,"$.event\_time") as event\_time, json\_value(data,"$.resource\_metadata.path[1].resource\_name") as cloud\_name, json\_value(data,"$.resource\_metadata.path[2].resource\_name") as folder\_name, json\_query(data,"$.authentication") as authentication, json\_value(data,"$.authorization.authorized") as authorized, json\_query(data,"$.details") as details  FROM  bindings.`binding`  LIMIT 100; |
| Use cases | | | | |
| IAM | | | | |
| 1 | Срабатывание при создании credentials сервисных аккаунтов | json\_payload.event\_type="yandex.cloud.audit.iam.CreateAccessKey" or json\_payload.event\_type="yandex.cloud.audit.iam.CreateKey" or json\_payload.event\_type="yandex.cloud.audit.iam.CreateApiKey" | event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.iam.CreateAccessKey or yandex.cloud.audit.iam.CreateKey or andex.cloud.audit.iam.CreateApiKey) | select \* from bindings.`binding-yds`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.iam.CreateAccessKey' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.iam.CreateKey' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.iam.CreateApiKey' limit 1  ; |
| 2 | Срабатывание на любое действие под привелигированным account с ролью “resource-manager.clouds.owner” и “organization-manager.admin  ” (можно списком)  (!!требует указания значений!!) | json\_payload.authentication.subject\_name="mirtov8@yandex-team.ru" or json\_payload.authentication.subject\_name="kirill@yandex-team.ru" | event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru kirill8@yandex-team.ru | - |
| 3 | Аномальное кол-во попыток неуспешной авторизации (!!требует корреляции!!) | --- | event.dataset: yandexcloud.audittrail and error.message: Permission denied | - |
| 4 | Назначение прав admin (на ресурсы: folder, cloud) | json\_payload.details.access\_binding\_deltas.access\_binding.role\_i="admin" | event.dataset: yandexcloud.audittrail and details.access\_binding\_deltas.access\_binding.role\_id: admin | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.details.access\_binding\_deltas.access\_binding.role\_id") = 'admin' limit 1  ; |
| 5 | Назначение роли vpc.public.admin | json\_payload.details.access\_binding\_deltas.access\_binding.role\_id="vpc.publicAdmin" | event.dataset: yandexcloud.audittrail and details.access\_binding\_deltas.access\_binding.role\_id: vpc.publicAdmin | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.details.access\_binding\_deltas.access\_binding.role\_id") = 'vpc.publicAdmin' limit 1  ; |
| 6 | Обращение к API с помощью YC или terraform под подозрительным пользователем или ip | json\_payload.request\_metadata.user\_agent:"YC" or json\_payload.request\_metadata.user\_agent:"Terraform" | event.dataset: yandexcloud.audittrail and (user\_agent.original.keyword: \*YC/\* or user\_agent.original.keyword: \*Terraform\*) | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.details.request\_metadata.user\_agent") = 'YC' or JSON\_VALUE(data, "$.details.request\_metadata.user\_agent") = 'Terraform' limit 1  ; |
| 7 | new  В федерацию добавили новый сертификат | json\_payload.event\_type="yandex.cloud.audit.organizationmanager.saml.CreateCertificate" | --- | - |
| 8 | new  Изменили настройки федерации | json\_payload.event\_type="yandex.cloud.audit.organizationmanager.saml.UpdateFederation" | --- | - |
| 9 | Любое действие с помощью сервисного аккаунта облака из диапозона IP адресов вне облака | not json\_payload.request\_metadata.remote\_address:"51.250"…. | event.dataset: yandexcloud.audittrail and user.type: SERVICE\_ACCOUNT and not source.ip: ("51.250.0.0/17" or "31.44.8.0/21" or "62.84.112.0/20" or "84.201.128.0/18" or "84.252.128.0/20" or "130.193.32.0/19" or "178.154.192.0/18" or "178.170.222.0/24" or "185.206.164.0/22" or "193.32.216.0/22" or "217.28.224.0/20") and source.ip: \* | - |
|  | new Назначение права на управление членством в группах iam | (json\_payload.event\_type="yandex.cloud.audit.organizationmanager.UpdateOrganizationAccessBindings" and json\_payload.details.access\_binding\_deltas.access\_binding.role\_id="organization-manager.groups.memberAdmin") or (json\_payload.event\_type="yandex.cloud.audit.organizationmanager.UpdateGroupAccessBindings" and json\_payload.details.access\_binding\_deltas.access\_binding.role\_id="editor") |  |  |
|  |  |  |  |  |
| Compute | | | | |
| 10 | Срабатывание на событие с созданием ВМ с белым IP адресом | json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and json\_payload.details.network\_interfaces.primary\_v4\_address.one\_to\_one\_nat.address exists | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and details.network\_interfaces.primary\_v4\_address.one\_to\_one\_nat.address: \* | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON\_EXISTS(data, "$.details.network\_interfaces.primary\_v4\_address.one\_to\_one\_nat.address") limit 1  ; |
| 11 | Срабатывание на создания "двуногих" виртуальных машин | json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and json\_payload.details.network\_interfaces[1].index="1" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and details.network\_interfaces.index: 1 | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON\_VALUE(data, "$.details.network\_interfaces[1].index") = '1' limit 1  ; |
| 12 | Загрузка image в облако не из фиксированного S3 Bucket (!!требует указания значений!!) | json\_payload.event\_type="yandex.cloud.audit.compute.CreateImage" and not json\_payload.details.source\_uri:"https://storage.yandexcloud.net/action-log-123" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateImage and not cloud.image.source\_uri: "https://storage.yandexcloud.net/action-log-123" | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateImage' and JSON\_VALUE(data, "$.details.source\_uri") != 'https://storage.yandexcloud.net/action-log-123' limit 1  ; |
| 13 | Создание ВМ с image\_id из Marketplace | not json\_payload.details.product\_ids[0]=null | event.dataset: yandexcloud.audittrail and details.product\_ids: \* | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON\_VALUE(data, "$.details.product\_ids[0]") != 'null' limit 1  ; |
| 14 | Добавление публичного IP-адреса существующей виртуальной машине | json\_payload.event\_type="yandex.cloud.audit.compute.AddInstanceOneToOneNat" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.AddInstanceOneToOneNat | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.AddInstanceOneToOneNat' limit 1  ; |
| 15 | События создания/изменеения ВМ – включение серийного порта | json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and json\_payload.details.metadata\_serial\_port\_enable="1" | event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and details.metadata\_serial\_port\_enable: 1 | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON\_VALUE(data, "$.details.metadata\_serial\_port\_enable") = '1' limit 1  ; |
| 16 | Изменение ВМ - добавление доступа к серийной консоли | json\_payload.event\_type="yandex.cloud.audit.compute.UpdateInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and json\_payload.details.metadata\_serial\_port\_enable="1" | event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: (yandex.cloud.audit.compute.CreateInstance or yandex.cloud.audit.compute.UpdateInstance) and details.metadata\_serial\_port\_enable: 1 | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.UpdateInstance' and JSON\_VALUE(data, "$.details.metadata\_serial\_port\_enable") = '1' limit 1  ; |
| 17 | Значение пользовательской метадаты ВМ предполагаемо содержит чувствительные данные | (json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" or json\_payload.event\_type="yandex.cloud.audit.compute.UpdateInstance") and json\_payload.details.metadata\_keys[0]: secret… | event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.compute.UpdateInstance or yandex.cloud.audit.compute.CreateInstance) and details.metadata\_keys: secret key password pass token oauth aws\_access\_key\_id and event.outcome : success | - |
| 18 | Создание ВМ без SG | json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and not json\_payload.details.network\_interfaces.security\_group\_ids EXISTS | event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and not details.network\_interfaces.security\_group\_ids: \* | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.compute.CreateInstance' and JSON\_EXISTS(data, "$.details.network\_interfaces[0].security\_group\_ids") = False limit 4  ; |
|  | Создание compute instance с включенным получением токена через AWS IMDSv1 |  |  |  |
| VPC | | | | |
| 19 | Создание слишком широкого (небезопасного) ACL Security Group для ipv4, tcp | json\_payload.event\_type="yandex.cloud.audit.network.CreateSecurityGroup" or json\_payload.event\_type="yandex.cloud.audit.network.UpdateSecurityGroup" and json\_payload.details.rules[0].direction="INGRESS" and json\_payload.details.rules[0].cidr\_blocks.v4\_cidr\_blocks[0]="0.0.0.0/0" | event.dataset: yandexcloud.audittrail and (event.action: yandex.cloud.audit.network.CreateSecurityGroup or yandex.cloud.audit.network.UpdateSecurityGroup) and details.rules.direction: INGRESS and details.rules.cidr\_blocks.v4\_cidr\_blocks: \*0.0.0.0\* | select \* from bindings.`binding`  where  (JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.network.CreateSecurityGroup' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.network.UpdateSecurityGroup') and (JSON\_VALUE(data, "$.details.rules[0].direction") = 'INGRESS' and JSON\_VALUE(data, "$.details.rules[0].cidr\_blocks.v4\_cidr\_blocks[0]") = '0.0.0.0/0') limit 1  ; |
| 20 | Создание публичного адреса без галочки защиты от ддос | json\_payload.event\_type="yandex.cloud.audit.compute.CreateInstance" and not json\_payload.details.external\_ipv4\_address.requirements.ddos\_protection\_provider exists | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.CreateAddress and not details.external\_ipv4\_address.requirements.ddos\_protection\_provider: qrator | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.network.CreateAddress' and JSON\_EXISTS(data, "$.details.external\_ipv4\_address.requirements.ddos\_protection\_provider") = False limit 2  ; |
| 21 | Создание/применение security group аккаунтом не из списка разрешенных  (!!требует указания значений!!) | (json\_payload.event\_type="yandex.cloud.audit.network.CreateSecurityGroup" or json\_payload.event\_type="yandex.cloud.audit.network.UpdateSecurityGroup") and not json\_payload.authentication.subject\_name="mirtov8@yandex-team.ru" | event.dataset: yandexcloud.audittrail and (event.action: yandex.cloud.audit.network.CreateSecurityGroup or yandex.cloud.audit.network.UpdateSecurityGroup) and not user.name: mirtov8@yandex-team.ru kirill@yandex-team.ru | - |
| 22 | Любое действие с объектами Security Group | json\_payload.event\_type="yandex.cloud.audit.network.CreateSecurityGroup" or json\_payload.event\_type="yandex.cloud.audit.network.UpdateSecurityGroup" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.\*SecurityGroup | select \* from bindings.`binding`  where  (JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.network.CreateSecurityGroup' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.network.UpdateSecurityGroup') limit 5  ; |
| ObjectStorage(S3) | | | | |
| 23 | Подозрительные дейсвия с хранилищем логов AuditTrails (S3 Bucket) | json\_payload.event\_type="yandex.cloud.audit.storage.BucketAclUpdate" or json\_payload.event\_type="yandex.cloud.audit.storage.BucketPolicyUpdate" | event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.storage.BucketAclUpdate or yandex.cloud.audit.storage.BucketPolicyUpdate) | select \* from bindings.`binding`  where  (JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.storage.BucketAclUpdate' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.storage.BucketPolicyUpdate') limit 5  ; |
| 24 | Object storage bucket (S3) стал публичным при создании/изменении | json\_payload.event\_type="yandex.cloud.audit.storage.BucketUpdate" and (json\_payload.details.objects\_access: "true" or json\_payload.details.settings\_read\_access: "true" or json\_payload.details.list\_access: "true") | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.storage.BucketUpdate and (details.objects\_access: true or details.settings\_read\_access: true or details.list\_access: true) | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.storage.BucketUpdate' and (JSON\_VALUE(data, "$.details.objects\_access") = 'true' or JSON\_VALUE(data, "$.details.settings\_read\_access") = 'true' or JSON\_VALUE(data, "$.details.list\_access") = 'true') limit 5  ; |
| 25 | Object storage bucket (S3) стал публичным при создании/изменении через ACL | json\_payload.event\_type="yandex.cloud.audit.storage.BucketAclUpdate" and json\_payload.details.acl.grants.grant\_type: "ALL\_USERS" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.storage.BucketAclUpdate and details.acl.grants.grant\_type: "ALL\_USERS" | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.storage.BucketUpdate' and JSON\_VALUE(data, "$.details.acl.grants.grant\_type") = 'ALL\_USERS' limit 5  ; |
| Lockbox/KMS | | | | |
| 26 | Срабатывание на изменение прав доступа на симметричные ключи шифрования KMS | json\_payload.event\_type="yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings" or json\_payload.event\_type="yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit. kms. \*SymmetricKeyAccessBindings | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings' limit 5  ; |
| 27 | Удаление ключа KMS | json\_payload.event\_type="yandex.cloud.audit.kms.DeleteSymmetricKey" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.kms.DeleteSymmetricKey | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.kms.DeleteSymmetricKey' limit 5  ; |
| 28 | Назначение/Обновление прав на секрет LockBox | json\_payload.event\_type="yandex.cloud.audit.lockbox.UpdateSecretAccessBindings" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.UpdateSecretAccessBindings | - |
| 29 | Назначение имеющего доступ к локбокс  cекретам сервисного аккаунта на ВМ  (!!требует указания значений!!) | json\_payload.event\_type="yandex.cloud.audit.compute.UpdateInstance" and json\_payload.details.service\_account\_id: "ajeg2ar8m8o25u63dj9f" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.UpdateInstance and details.service\_account\_id: ajeg2ar8m8o25u63dj9f | - |
| 30 | Чтение секрета из Lockbox с IP адреса отличного от [диапозона адресов облака](https://cloud.yandex.ru/docs/vpc/concepts/ips)  (!!требует указания значений!!) | json\_payload.event\_type="yandex.cloud.audit.lockbox.GetPayload"  and not json\_payload.request\_metadata.remote\_address:"51.250"…. | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.GetPayload and not source.ip: ("51.250.0.0/17" or "31.44.8.0/21" or "62.84.112.0/20" or "84.201.128.0/18" or "84.252.128.0/20" or "130.193.32.0/19" or "178.154.192.0/18" or "178.170.222.0/24" or "185.206.164.0/22" or "193.32.216.0/22" or "217.28.224.0/20") | - |
| 31 | Чтение секрета из Lockbox с помощью учетной записи, которая отличается от целевой  (!!требует указания значений!!) | json\_payload.event\_type="yandex.cloud.audit.lockbox.GetPayload" and not json\_payload.authentication.subject\_id: "ajesnkfkc77lbh50isvg" and json\_payload.details.secret\_id="e6q7q5msguqg22ji78e0" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.GetPayload and not user.id: ajeg2ar8m8o25u63dj9f and details.secret\_name: secret1 | - |
| Managed Kubernetes (k8s) | | | | |
|  | new  Назначена SG на мастер |  |  |  |
|  | new  Кластер не имеет публичный адрес |  |  |  |
|  | new  Группы узлов не имеют публичный адрес |  |  |  |
|  | new  "Ensure Kubernetes cluster auto-upgrade is enabled." |  |  |  |
|  | new  "Ensure Kubernetes node group auto-upgrade is enabled." |  |  |  |
|  | new  "Ensure etcd database is encrypted with KMS key." |  |  |  |
|  | new  Включена network policy либо cilium |  |  |  |
| ALB | | | | |
|  | new  Создан балансировщик без группы безопасности | json\_payload.event\_type: "CreateLoadBalancer" and not json\_payload. request\_parameters.security\_group\_ids EXISTS |  |  |
|  | new  Создан балансировщик с обработчиком HTTP (а не HTTPS) | json\_payload.event\_type: "CreateLoadBalancer" and json\_payload.details.listeners[0].http EXISTS |  |  |
|  |  |  |  |  |
| MDB | | | | |
| 32 | Создание кластера MDB пользователем облака не из списка администраторов  (!!требует указания значений!!) | json\_payload.event\_type: "yandex.cloud.audit.mdb." and not json\_payload.authentication.subject\_name: "test" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.\*.CreateCluster and not user.name : mirtov8@yandex-team.ru kirill@yandex-team.ru | - |
| 33 | Создание/Изменение пользователя MDB | json\_payload.event\_type: "CreateUser" or json\_payload.event\_type: "UpdateUser" | event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.\*.UpdateUser or yandex.cloud.audit.mdb.\*.CreateUser) | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.mdb.postgresql.CreateUser' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.mdb.postgresql.UpdateUser' limit 5  ; |
| 34 | Удаление кластера MDB | json\_payload.event\_type: "DeleteCluster" | event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.\*.DeleteCluster | select \* from bindings.`binding`  where  JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.mdb.postgresql.DeleteCluster' or JSON\_VALUE(data, "$.event\_type") = 'yandex.cloud.audit.mdb.postgresql.UpdateUser' limit 5  ; |
| 35 | Административные действия с MDB с ip адресов, которые отличаются от доверенного диапозона  (!!требует указания значений!!) | (json\_payload.event\_type: "DeleteCluster" or json\_payload.event\_type: "CreateCluster") and not json\_payload.request\_metadata.remote\_address: "51.250" | event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.\*.UpdateUser or yandex.cloud.audit.mdb.\*.CreateUser or yandex.cloud.audit.mdb.\*.CreateCluster or yandex.cloud.audit.mdb.\*.UpdateCluster ) and source.ip : ("2a00:1fa0:474:9876:4cac:6c43:12aa:2bd2" or "2a00:1fa0:474:9876:4cac:6c43:12aa:2bd1" ) | - |
| 36 | new  Включение потенциально опасной настройки при создании или обновлении кластера:  -доступ из datalens  -публичный доступ  -доступ из консоли управления  -доступ из serverless | (json\_payload.event\_type: "CreateCluster" or json\_payload.event\_type: "UpdateCluster") and (json\_payload. request\_parameters.config\_spec.access.data\_lens: "true" or json\_payload. request\_parameters.config\_spec.access.serverless: "true" or json\_payload. request\_parameters.config\_spec.access.web\_sql: "true" or json\_payload.host\_specs[0].assign\_public\_ip: "true") | --- |  |
| 38 | new  Не включена «Защита от удаления» при создании | json\_payload.event\_type: "CreateCluster" and not json\_payload. request\_parameters.deletion\_protection EXISTS | --- |  |
| 39 | new  Отключение аудит логов mdb postgres | json\_payload.event\_type: "UpdateCluster" and json\_payload.request\_parameters.config\_spec.postgresql\_config\_14.log\_statement:"LOG\_STATEMENT\_NONE" | --- |  |
| 40 | new  Выдача привелигированных GRANT mdb\_admin пользователю | json\_payload.event\_type: "UpdateUser" and json\_payload.request\_parameters.grants[0]:"mdb\_admin" | --- |  |
| 41 | new  Создание кластера без установленной Security Group | json\_payload.event\_type: "CreateCluster" and not json\_payload. request\_parameters.security\_group\_ids EXISTS | --- |  |
| Следующие Use cases не являются частью Audit Trails, а являются нативными аудит логами k8s, также на текущий момент их невозможно анализировать в CloudLogging | | | | |
| Kubernetes (для событий k8s необходимо настроить [решение](https://github.com/yandex-cloud/yc-solution-library-for-security/tree/master/auditlogs/export-auditlogs-to-ELK_k8s)) | | | | |
| Общие | | | | |
| 1 | События отказа в доступе - unauthorized | ---­ | event.dataset : yandexcloud.k8s\_audit\_logs and responseStatus.reason : Forbidden and not user.name : (system\*node\* or \*gatekeeper\* or \*kyverno\* or \*proxy\* or \*scheduler\* or \*anonymous\* or \*csi\* or \*controller\*) |  |
| 2 | Назначение cluster-admin или admin роли (clusterrolebinding или rolebinding) | --- | event.dataset : yandexcloud.k8s\_audit\_logs and requestObject.roleRef.name.keyword:(cluster-admin or admin) and objectRef.resource.keyword: (clusterrolebindings or rolebindings) and verb : create and not responseObject.reason : AlreadyExists |  |
| 3 | Успешное подключение к кластеру с внешнего IP адреса | --- | event.dataset : yandexcloud.k8s\_audit\_logs and source.ip : \* and not responseStatus.status : Failure |  |
| 4 | NetworkPolicies: создание, удаление, изменение | --- | event.dataset : yandexcloud.k8s\_audit\_logs and requestObject.kind.keyword: (NetworkPolicy or CiliumNetworkPolicy or DeleteOptions) and verb : (create or update or delete) and objectRef.resource : networkpolicies |  |
| 5 | Exec внутрь контейнера (шелл внутрь контейнера) | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.subresource.keyword: exec |  |
| 6 | Создание pod с image НЕ из Yandex container registry (не актуально для Клиентов использующих собственный cr) | --- | event.dataset : yandexcloud.k8s\_audit\_logs and not requestObject.status.containerStatuses.image.keyword: \*cr.yandex/\* and requestObject.status.containerStatuses.containerID : \*docker\* and verb : patch and not requestObject.status.containerStatuses.image.keyword: (\*falco\* or \*openpolicyagent\* or \*kyverno\* or \*k8s.gcr.io\*) |  |
| 7 | Создание pod в kube-system namespace | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.namespace.keyword: kube-system and verb : create and objectRef.resource.keyword: pods and objectRef.name : \* and not objectRef.name : (\*calico\* or \*dns\* or \*npd\* or \*proxy\* or \*metrics\* or \*csi\* or \*masq\*) |  |
| 8 | Обращение к k8s-api под сервисным аккаунтом с внешнего ip адреса | --- | event.dataset : yandexcloud.k8s\_audit\_logs and user.name : system\\\:serviceaccount\\\:\* not source.ip: ("10.0.0.0/8  " or " 172.16.0.0/12" or " 192.168.0.0/16" |  |
| Falco | | | | |
| 9 | Любой Alert от Falco | --- | event.dataset : yandexcloud.k8s\_falco and not objectRef.namespace: falco |  |
| 10 | Falco удален | --- | event.dataset : yandexcloud.k8s\_audit\_logs and verb : delete and objectRef.namespace.keyword: falco and objectRef.resource.keyword : daemonsets |  |
| OPA Gatekeeper | | | | |
| 11 | Срабатывание OPA Gatekeeper – denied events (только в режиме enforce) | --- | event.dataset : yandexcloud.k8s\_audit\_logs and responseObject.status.keyword: Failure and responseObject.message :" admission webhook \\\"validation.gatekeeper.sh\\\" denied the request" and not objectRef.namespace : falco and not user.name : system\\\:serviceaccount\\\:kube-system\\\:daemon-set-controller |  |
| 12 | Удаление Gatekeeper из кластера k8s | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.name.keyword: gatekeeper-validating-webhook-configuration and verb : delete |  |
| 13 | Изменение/удаление объекта Constraint | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.apiGroup.keyword: constraints.gatekeeper.sh and (verb : delete or update) and not user.name : "system:serviceaccount:gatekeeper-system:gatekeeper-admin" |  |
| Kyverno | | | | |
| 14 | Срабатывание Kyverno – denied events (только в режиме enforce) | --- | event.dataset : yandexcloud.k8s\_audit\_logs and responseObject.status.keyword: Failure and responseObject.message :" admission webhook \\\"validate.kyverno.svc\\\" denied the request" and not objectRef.namespace : falco and not user.name : system\\\:serviceaccount\\\:kube-system\\\:daemon-set-controller |  |
| 15 | Удаление Kyverno из кластера k8s | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.name.keyword: kyverno-resource-validating-webhook-cfg and verb : delete |  |
| 16 | Изменение/удаление объекта Kyverno Policy | --- | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.apiGroup.keyword: kyverno.io and (verb : delete or update) and objectRef.resource.keyword: \*policies |  |
| Kyverno-report | | | | |
| 17 | Срабатывание Kyvenro: fail status of policy result (Yandexcloud:k8s:kyverno-reporter-detect) | --- | event.dataset : yandexcloud.k8s\_kyverno and Status : fail |  |
| External Secrets | | | | |
| 18 | Изменение /создание объекта external secrets учеткой отличной от ci/cd (данный объект ходит в lockbox и копирует оттуда секрет) |  | event.dataset : yandexcloud.k8s\_audit\_logs and not user.name: "ajesnkfkc77lbh50isvg" and not user.name: "system:serviceaccount:external-secrets:external-secrets" and objectRef.name: "external-secret" and verb: (patch or create) |  |
| 19 | Чтение секретов под учетной записью пользователя |  | event.dataset : yandexcloud.k8s\_audit\_logs and objectRef.resource: "secrets" and verb: "get" and not user.name: ("system:serviceaccount:external-secrets:external-secrets" or "system:serviceaccount:kube-system:hubble-generate-certs" or "system:serviceaccount:kyverno:kyverno") |  |
|  |  |  |  |  |