|  |  |  |
| --- | --- | --- |
| **Поле ECS** | **Поле JSON** | **Пример** |
| event.kind | ”event” | - |
| event.action | event\_type | "event\_type" : yandex.cloud.audit.iam.CreateAccessKey, |
| [event.module](https://www.elastic.co/guide/en/ecs/current/ecs-event.html#field-event-module) | event\_source | "event\_source" : iam, |
| event.status (custom) | event\_status | "event\_status" : DONE, |
| event.id | event\_id | "event\_id" : ajehpht38uh1q0povo7j, |
| [event.category](https://www.elastic.co/guide/en/ecs/current/ecs-event.html#field-event-category) | configuration, iam | - |
| event.dataset | “yandexcloud.audittrail” | - |
| event.outcome | success ("if": "event.status == 'DONE'" -) | - |
| cloud.account.id | resource\_metadata.path.0.resource\_id | "resource\_id" : yc.organization-manager.yandex, |
| cloud.account.name | resource\_metadata.path.0.resource\_name | "resource\_name" : yc-organization-manager-yandex |
| cloud.cloud.name (custom) | resource\_metadata.path.0.resource\_name | "resource\_name" : arch |
| cloud.cloud.id (custom) | resource\_metadata.path.0.resource\_id | "resource\_id" : b1g3o4minpkuh10pd2rj, |
| cloud.folder.name (custom) | resource\_metadata.path.1.resource\_name | "resource\_id" : b1gci8pu7s2seup3mpor, |
| cloud.folder.id (custom) | resource\_metadata.path.1.resource\_id | "resource\_name" : mirtov-terraform-play |
| [cloud.instance.id](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-instance-id) | details.instance\_id | "details" : -{   * "instance\_id" : fhmkf7a1fdt7a1vead5o, |
| [cloud.instance.name](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-instance-name) | details.instance\_name | "details" : -{   * "instance\_name" : testvm-1, |
| cloud.instance.market\_image (custom) | details.product\_ids | "product\_ids" : -[   * f2efrqfcllr7ns1o7b1t |
| [cloud.availability\_zone](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-availability-zone) | details.instance\_zone\_id | * "zone\_id" : ru-central1-a, |
| [cloud.machine.type](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-machine-type) | details.platform\_id | * "platform\_id" : standard-v2, |
| [cloud.provider](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-provider) | “yandexcloud” | - |
| [cloud.service.name](https://www.elastic.co/guide/en/ecs/current/ecs-cloud.html#field-cloud-service-name) | “audittrail” | - |
| [source.address](https://www.elastic.co/guide/en/ecs/current/ecs-source.html#field-source-address) | request\_metadata.remote\_address | "request\_metadata" : -{   * "remote\_address" : 127.90.2.12 |
| [source.ip](https://www.elastic.co/guide/en/ecs/current/ecs-source.html#field-source-ip) | request\_metadata.remote\_address | "request\_metadata" : -{   * "remote\_address" : 127.90.2.12 |
| [user.id](https://www.elastic.co/guide/en/ecs/current/ecs-user.html#field-user-id) | authentication.subject\_id | "subject\_id" : ajesnkfkc77lbh50isvg, |
| [user.name](https://www.elastic.co/guide/en/ecs/current/ecs-user.html#field-user-name) | authentication.subject\_name | "subject\_name" : [mirtov8@yandex-team.ru](mailto:mirtov8@yandex-team.ru) |
| user.type (custom) | authentication.subject\_type | "subject\_type" : FEDERATED\_USER\_ACCOUNT, |
| user.authorization (custom) | authorization.authorized | "authorization" : -{   * "authorized" : true |
| user\_agent.original | request\_metadata.user\_agent | "user\_agent" : Yandex Cloud, |
| user.authenticated (custom) | authentication.authenticated | "authenticated" : true, |
| security\_group.id (custom) | details.security\_group\_id | * "security\_group\_id" : enp9b97fd6fjs8fj07s1, |
| cloud.image.name (custom) | details.image\_name | "image\_name" : strict-image |
| cloud.image.id (custom) | details.image\_id | "image\_id" : fd8at19knvi0ngnrm1g2, |
| cloud.image.source\_uri(custom) | details. source\_uri | "image\_id" : fd8at19knvi0ngnrm1g2, |
| object\_storage.id (custom) | details.bucket\_id | "bucket\_id" : imgae-buckets, |
| cloud.binding.role\_id (custom) | details. access\_binding\_deltas.access\_binding. role\_id | "access\_binding" : -{   * "role\_id" : admin, |
|  |  |  |