|  |  |
| --- | --- |
| Поле ECS | Поле JSON |
|  |  |
| sourceUserName | authentication\_subject\_name |
| sourceUserId | authentication\_subject\_id |
| sourceUserPrivileges | authentication\_subject\_type |
|  |  |
| deviceAction |  |
| requestClientApplication | request\_metadata\_user\_agent |
| sourceHostName | request\_metadata\_remote\_address |
| requestContext | request\_metadata\_request\_id |
| deviceCustomString1 | details |
| deviceCustomString1Label | \_\_stringConstant("details") |
| deviceCustomString2 | resource\_metadata |
| deviceCustomString2Label | \_\_stringConstant("resource\_metadata") |
| deviceCustomString3 | authentication\_authenticated |
| deviceCustomString3Label | \_\_stringConstant("authenticated") |
| deviceCustomString4 | authorization\_authorized |
| deviceCustomString4Label | \_\_stringConstant("authorized") |
| fileName | rm\_0\_resource\_name |
| filePath | rm\_0\_resource\_id |
| fileType | rm\_0\_resource\_type |
| oldFileName | rm\_1\_resource\_name |
| oldFilePath | rm\_1\_resource\_id |
| oldFileType | rm\_1\_resource\_type |
| endTime | event\_time |
| externalId |  |
| deviceVendor | \_\_stringConstant("Yandex Cloud") |
| deviceProduct | \_\_stringConstant("Yandex Cloud") |

|  |  |  |
| --- | --- | --- |
| 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 | "event\_status" : DONE, |
| event.id | event\_id | "event\_id" : ajehpht38uh1q0povo7j, |
|  |  |  |