Поле ECS	Поле JSON	Пример
event.kind	"event"	-
event.action	event type	"event type" : yandex.cloud.audit.ia
	<u>-</u> -7F-	m.CreateAccessKey,
		, , , , , , , , , , , , , , , , , , , ,
event.module	event source	"event_source" : iam,
C V GIIIIIII G GGIC		, iam,
event.status	event status	"event status" : DONE,
(custom)	ovent_status	ovent_status . Dorve,
event.id	event id	"event id": ajehpht38uh1q0povo7j,
		overs_is value out que varig
event.category	configuration, iam	_
event.dataset	"yandexcloud.audittrail"	-
event.outcome	success ("if": "event.status ==	_
	'DONE'" -)	
cloud.cloud.name	resource_metadata.path.0.resourc	"resource name" : arch
(custom)	e_name	
cloud.cloud.id	resource_metadata.path.0.resourc	"resource_id": b1g3o4minpkuh10pd
(custom)	e_id	2rj,
cloud.folder.name	resource_metadata.path.1.resourc	"resource_id": b1gci8pu7s2seup3m
(custom)	e_name	por,
cloud.folder.id	resource_metadata.path.1.resourc	"resource_name" : mirtov-terraform-
(custom)	e_id	play
cloud.instance.id	details.instance_id	"details" : -{
Cloud.mstance.id	details.ilistance_id	• "instance id": fhmkf7a1fdt7
		alvead5o,
		arveauso,
cloud.instance.name	details.instance_name	"details" : -{
croad:mstance:name	details.iiistariee_name	• "instance name": testvm-1,
		instance_name : testvin 1,
cloud.instance.mark	details.product_ids	"product ids":-[
et image (custom)	details.product_ids	• f2efrqfcllr7ns1o7b1t
cloud.availability_z	details.instance_zone_id	• "zone id" : ru-central1-a,
one	details.iiistanee_zone_id	Zone_id . id-contrait-a,
cloud.machine.type	details.platform_id	• "platform id" : standard-v2,
cioud.macmine.type	details.pidtioiii_id	prationin_id . Standard v2,
cloud.provider	"yandexcloud"	_
cloud.service.name	"audittrail"	_
source.address	request_metadata.remote_addres	"request metadata" : -{
source.address	s	• "remote address" : 127.90.2.
	Ĭ	12 12
		12
source.ip	request_metadata.remote_addres	"request metadata":-{
Source.ip	s	• "remote_address" : 127.90.2.
		12 12
user.id	authentication.subject_id	"subject_id" : ajesnkfkc77lbh50isvg,
usci.iu	addientication.subject_id	subject_id . ajeslikike//lulibulsvg,
licon norma	authoritisation subject, name	"auhiaat nama" mintavo @vianda
user.name	authentication.subject_name	"subject_name" : mirtov8@yandex-
	<u> </u>	team.ru

user.type (custom)	authentication.subject_type	"subject type": FEDERATED US
user.type (eustoni)		2 _ 2 1
		ER_ACCOUNT,
user.authorization	authorization.authorized	"authorization" : -{
(custom)		• "authorized" : true
user_agent.original	request_metadata.user_agent	"user_agent" : Yandex Cloud,
user.authenticated	authentication.authenticated	"authenticated": true,
(custom)		·
security group.id	details.security_group_id	• "security group id": enp9b9
(custom)		7fd6fjs8fj07s1,
cloud.image.name	details.image_name	"image name" : strict-image
(custom)		
cloud.image.id	details.image_id	"image id": fd8at19knvi0ngnrm1g2
(custom)		,
cloud.image.source	details. source_uri	"image id": fd8at19knvi0ngnrm1g2
uri(custom)	_	,
object storage.id	details.bucket_id	"bucket id": imgae-buckets,
(custom)	_	
cloud.binding.role i	details. access_binding_deltas.acc	"access binding":-{
d (custom)	ess_binding. role_id	• "role id" : admin,