

















Searches & Use Cases





Содержание





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
Searches				
1	Найти, кто удалил фолдер (!!требуется указание значений!!)	<code>json_payload.event_type="yandex.cloud.audit.resourcemanager.DeleteFolder" and json_payload.details.folder_name="<название каталога>"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.resourcemanager.DeleteFolder and cloud.folder.name: <название каталога></code>	<code>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</code>
2	Найти, кто создал/остановил/перезапустил/удалил виртуальную машину (!!требуется указание значений!!)	<code>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")</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.*Instance and cloud.instance.name: testdasdas</code>	<code>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.StopInstance' or JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.compute.StartInstance' or JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.compute.UpdateInstance' or JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.compute.CreateInstance')</code>





№	Название	CloudLogging 	Elasticsearch   Opensearch	Yandex Query  (S3 or YDS)
		<code>udit.compute.StopInstance" or json_payload.event_type="yandex.cloud.audit.compute.RestartInstance")</code>		<code>ce' or JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit.compute.CreateInstance') and JSON_VALUE(data, "\$..details.instance_id") = 'fhmpgh36fo3vclan2e99' limit 100 ;</code>
3	Какие действия совершал конкретный пользователь за период времени (!!требуется указания своих значений!!)	<code>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"</code>	event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru and event_time < 2022-07-15	<code>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</code>



№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				;
4	Поиск событий по объектам определенного фолдера (!!требуется указание значений!!)	<code>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>"</code>	<code>event.dataset:yandexcloud.audittrail and cloud.folder.name:"mirtov-scale"</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$resource_metadata.path[2].resource_name") = 'mirtov-scale' limit 100 ;</code>
Use cases				
IAM				
1	Срабатывание при создании credentials сервисных аккаунтов	<code>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"</code>	<code>event.dataset:yandexcloud.audittrail and event.action: (yandex.cloud.audit.iam.CreateAccessKey or yandex.cloud.audit.iam.CreateKey or yandex.cloud.audit.iam.CreateApiKey)</code>	<code>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 iam.CreateKey' or</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				<code>JSON_VALUE(data, "\$\$.event_type") = 'yandex.cloud.audit. iam.CreateApiKey' limit 1 ;</code>
2	Срабатывание на любое действие под привелигированным account с ролью "resource-manager.clouds.owner" и "organization-manager.admin" (можно списком) (!!требуется указания значений!!)	<code>json_payload.authentication.subject_name="mirtov8@yandex-team.ru" or json_payload.authentication.subject_name="kirill@yandex-team.ru"</code>	<code>event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru kirill8@yandex-team.ru</code>	-
3	Аномальное кол-во попыток неуспешной авторизации	---	<code>event.dataset: yandexcloud.audittrail and error.message: Permission denied</code>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	(!!требует корреляции!!)			
4	Назначение прав admin (на ресурсы: folder, cloud)	<code>json_payload.details.access_binding_deltas.access_binding.role_id="admin"</code>	<code>event.dataset: yandexcloud.audittrail and details.access_binding_deltas.access_binding.role_id : admin</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$.details.access_binding_deltas.access_binding.role_id") = 'admin' limit 1 ;</code>
5	Назначение роли vpc.public.admin	<code>json_payload.details.access_binding_deltas.access_binding.role_id="vpc.publicAdmin"</code>	<code>event.dataset: yandexcloud.audittrail and details.access_binding_deltas.access_binding.role_id : vpc.publicAdmin</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$.details.access_binding_deltas.access_binding.role_id") = 'vpc.publicAdmin' limit 1 ;</code>
6	Обращение к API с помощью YC или terraform	<code>json_payload.request_metadata.user_agent:"YC" or json_payload.request_metadata.user_agent:"Terraform"</code>	<code>event.dataset: yandexcloud.audittrail and (user_agent.original.keyword: *YC/* or</code>	<code>select * from bindings.`binding` where</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	под подозрительны м пользователем или ip		user_agent.original.keyword: *Terraform*)	<pre>JSON_VALUE(data, "\$details.request_m etadata.user_agent") = 'YC' or JSON_VALUE(data, "\$details.request_m etadata.user_agent") = 'Terraform' limit 1 ;</pre>
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"	---	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
9	Любое действие с помощью сервисного аккаунта облака из диапазона IP адресов вне облака	<code>not json_payload.request_metadata.remote_address:"51.250"...</code>	<code>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: *</code>	-
10	new Назначение права на управление членством в группах iam	<code>(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")</code>		
Compute				




№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
11	Срабатывание на событие с созданием ВМ с белым IP адресом	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.network_interfaces.primary_v4_address.one_to_one_nat.address exists</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute .CreateInstance and details.network_interfaces .primary_v4_address.one_to _one_nat.address: *</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. compute.CreateInstance' and JSON_EXISTS(data, "\$..details.network_i nterfaces.primary_v4 _address.one_to_one_ nat.address") limit 1 ;</code>
12	Срабатывание на создания "двуногих" виртуальных машин	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.network_interfaces[1].index="1"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute .CreateInstance and details.network_interfaces .index: 1</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. compute.CreateInstance' and JSON_VALUE(data, "\$..details.network_i</code>



№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				<code>nterfaces[1].index") = '1' limit 1 ;</code>
13	Загрузка image в облако не из фиксированного S3 Bucket (!!требует указания значений!!)	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateImage" and not json_payload.details.source_uri:"https://storage.yandexcloud.net/action-log-123"</code>	<code>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"</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. compute.CreateImage' and JSON_VALUE(data, "\$..details.source_uri") != 'https://storage.yan dexcloud.net/action- log-123' limit 1 ;</code>
14	Создание VM с image_id из Marketplace	<code>not json_payload.details.product_ids[0]=null</code>	<code>event.dataset: yandexcloud.audittrail and details.product_ids: *</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. compute.CreateInstan</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				<pre>ce' and JSON_VALUE(data, "\$\$.details.product_i ds[0]") != 'null' limit 1 ;</pre>
15	Добавление публичного IP-адреса существующей виртуальной машине	<pre>json_payload.event_type="yandex.cloud.audit.compute.AddInstanceOneToOneNat"</pre>	<pre>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute .AddInstanceOneToOneNat</pre>	<pre>select * from bindings.`binding` where JSON_VALUE(data, "\$\$.event_type") = 'yandex.cloud.audit. compute.AddInstanceO neToOneNat' limit 1 ;</pre>
16	События создания/изменения ВМ – включение серийного порта	<pre>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.metadata_serial_port_enable="1"</pre>	<pre>event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute .CreateInstance and details.metadata_serial_po rt_enable: 1</pre>	<pre>select * from bindings.`binding` where JSON_VALUE(data, "\$\$.event_type") = 'yandex.cloud.audit. compute.CreateInstance' and JSON_VALUE(data, "\$\$.details.metadata_</pre>





№	Название	CloudLogging 	Elasticsearch   Opensearch	Yandex Query  (S3 or YDS)
				<pre>serial_port_enable") = '1' limit 1 ;</pre>
17	Изменение VM - добавление доступа к серийной консоли	<pre>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"</pre>	<pre>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</pre>	<pre>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 ;</pre>
18	Значение пользовательской метадаты VM предполагаемо содержит чувствительные данные	<pre>(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...</pre>	<pre>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</pre>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
19	Создание VM без SG	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not json_payload.details.network_interfaces.security_group_ids EXISTS</code>	<code>event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and not details.network_interfaces.security_group_ids: *</code>	<code>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 ;</code>
20	new Создание/ Изменение compute instance с включенным получением токена через AWS IMDSv1	<code>(json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance" or json_payload.event_type="yandex.cloud.audit.compute.CreateInstance") and json_payload.details.metadata_options.aws_v1_http_token="ENABLED"</code>		
VPC				





№	Название	CloudLogging 	Elasticsearch   Opensearch	Yandex Query  (S3 or YDS)
21	Создание слишком широкого (небезопасного) ACL Security Group для ipv4, tcp	<pre>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"</pre>	<pre>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*</pre>	<pre>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 ;</pre>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
22	Создание публичного адреса без галочки защиты от ддос	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not json_payload.details.external_ipv4_address.requirements.ddos_protection_provider exists</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.CreateAddress and not details.external_ipv4_address.requirements.ddos_protection_provider: qrator</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.network.CreateAddresses' and JSON_EXISTS(data, "\$.details.external_ipv4_address.requirements.ddos_protection_provider") = False limit 2 ;</code>
23	Создание/применение security group аккаунтом не из списка разрешенных (!!требуется указания значений!!)	<code>(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"</code>	<code>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</code>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
24	Любое действие с объектами Security Group	<code>json_payload.event_type="yandex.cloud.audit.network.CreateSecurityGroup" or json_payload.event_type="yandex.cloud.audit.network.UpdateSecurityGroup"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.*SecurityGroup</code>	<code>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;</code>
ObjectStorage(S3)				
25	Подозрительные действия с хранилищем логов AuditTrails (S3 Bucket)	<code>json_payload.event_type="yandex.cloud.audit.storage.BucketAclUpdate" or json_payload.event_type="yandex.cloud.audit.storage.BucketPolicyUpdate"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.storage.BucketAclUpdate or yandex.cloud.audit.storage.BucketPolicyUpdate)</code>	<code>select * from bindings.`binding` where (JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.storage.BucketAclUpdate' or</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				<pre>JSON_VALUE (data, "\$.event_type") = 'yandex.cloud.audit. storage.BucketPolicy Update') limit 5 ;</pre>
26	Object storage bucket (S3) стал публичным при создании/изменении	<pre>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")</pre>	<pre>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)</pre>	<pre>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</pre>




№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
27	Object storage bucket (S3) стал публичным при создании/изменении через ACL	<code>json_payload.event_type="yandex.cloud.audit.storage.BucketAclUpdate" and json_payload.details.acl.grants.grant_type: "ALL_USERS"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.storage.BucketAclUpdate and details.acl.grants.grant_type: "ALL_USERS"</code>	<code>; 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 ;</code>
Lockbox/KMS				
28	Срабатывание на изменение прав доступа на симметричные ключи шифрования KMS	<code>json_payload.event_type="yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings" or json_payload.event_type="yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.kms.*SymmetricKeyAccessBindings</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.kms.UpdateSymmetricKeyAccessBindings' or JSON_VALUE(data, "\$.event_type") =</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
				<code>'yandex.cloud.audit.kms.CreateSymmetricKeyAccessBindings'</code> <code>limit 5</code> <code>;</code>
29	Удаление ключа KMS	<code>json_payload.event_type="yandex.cloud.audit.kms.DeleteSymmetricKey"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.kms.DeleteSymmetricKey</code>	<code>select * from bindings.`binding` where JSON_VALUE(data, "\$.event_type") = 'yandex.cloud.audit.kms.DeleteSymmetricKey' limit 5 ;</code>
30	Назначение/Обновление прав на секрет LockBox	<code>json_payload.event_type="yandex.cloud.audit.lockbox.UpdateSecretAccessBindings"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox.UpdateSecretAccessBindings</code>	-
31	Назначение имеющего доступ к локбокс секретам сервисного аккаунта на ВМ	<code>json_payload.event_type="yandex.cloud.audit.compute.UpdateInstance" and json_payload.details.service_account_id : "ajeg2ar8m8o25u63dj9f"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.UpdateInstance and details.service_account_id : ajeg2ar8m8o25u63dj9f</code>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	(!!требуется указания значений!!)			
32	Чтение секрета из Lockbox с IP адреса отличного от <u>диапазона</u> <u>адресов облака</u> (!!требуется указания значений!!)	<code>json_payload.event_type="yandex.cloud.audit.lockbox.GetPayload" and not json_payload.request_metadata.remote_address:"51.250"...</code>	<code>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")</code>	-
33	Чтение секрета из Lockbox с помощью учетной записи, которая отличается от целевой (!!требуется указания значений!!)	<code>json_payload.event_type="yandex.cloud.audit.lockbox.GetPayload" and not json_payload.authentication.subject_id:"ajesnkfk77lbh50isvg" and json_payload.details.secret_id="e6q7q5m sguqg22ji78e0"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.lockbox .GetPayload and not user.id: ajeg2ar8m8o25u63dj9f and details.secret_name: secret1</code>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
Managed Kubernetes (k8s)				
	new Не назначена SG на мастер	<pre>json_payload.event_type: "yandex.cloud.audit.k8s.CreateCluster" and not json_payload.request_parameters.master_spec.security_group_ids EXISTS</pre>		
	new Кластер имеет публичный адрес	<pre>json_payload.event_type: "yandex.cloud.audit.k8s.CreateCluster" and json_payload.request_parameters.master_spec.zonal_master_spec.external_v4_address_spec.address EXISTS</pre>		
	new Группы узлов имеют публичный адрес	<pre>json_payload.event_type : "yandex.cloud.audit.k8s.CreateNodeGroup" and json_payload.request_parameters.node_template.v4_address_spec.one_to_one_nat_spec exists</pre>		
	new Не включено автоматическое обновление для Kubernetes master	<pre>json_payload.event_type: "yandex.cloud.audit.k8s.CreateCluster" and not json_payload.request_parameters.master_spec.maintenance_policy.auto_upgrade EXISTS</pre>		
	new Не включено автоматическое обновление Kubernetes node	<pre>json_payload.event_type : "yandex.cloud.audit.k8s.CreateNodeGroup" and not json_payload.request_parameters.maintenance_policy.auto_upgrade = "true"</pre>		





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	New Не включено шифрование на KMS ключе etcd базы	<code>json_payload.event_type : "yandex.cloud.audit.k8s.CreateCluster" and not json_payload.request_parameters.kms_provider.key_id exists</code>		
	new Не включена network policy либо cilium на уровне кластера	<code>json_payload.event_type : "yandex.cloud.audit.k8s.CreateCluster" and not json_payload.request_parameters.network_policy.provider exists</code>		
ALB				
	new Создан балансировщик без группы безопасности	<code>json_payload.event_type: "CreateLoadBalancer" and not json_payload.request_parameters.security_group_ids EXISTS</code>		
	new Создан балансировщик с обработчиком HTTP (а не HTTPS)	<code>json_payload.event_type: "CreateLoadBalancer" and json_payload.details.listeners[0].http EXISTS</code>		
MDB				
32	Создание кластера MDB	<code>json_payload.event_type: "yandex.cloud.audit.mdb." and not</code>	<code>event.dataset: yandexcloud.audittrail and</code>	-





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	пользователем облака не из списка администраторов (!!требуется указания значений!!)	<code>json_payload.authentication.subject_name: "test"</code>	<code>event.action: yandex.cloud.audit.mdb.*.createCluster and not user.name : mirtov8@yandex-team.ru kirill@yandex-team.ru</code>	
33	Создание/Изменение пользователя MDB	<code>json_payload.event_type: "CreateUser" or json_payload.event_type: "UpdateUser"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.*.UpdateUser or yandex.cloud.audit.mdb.*.createUser)</code>	<code>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 ;</code>
34	Удаление кластера MDB	<code>json_payload.event_type: "DeleteCluster"</code>	<code>event.dataset: yandexcloud.audittrail and event.action:</code>	<code>select * from bindings.`binding` where</code>





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
			yandex.cloud.audit.mdb.*.DeleteCluster	<pre>JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. mdb.postgresql.Delete Cluster' or JSON_VALUE(data, "\$..event_type") = 'yandex.cloud.audit. mdb.postgresql.Update User' limit 5 ;</pre>
35	Административные действия с MDB с ip адресов, которые отличаются от доверенного диапазона (!!требуется указания значений!!)	<pre>(json_payload.event_type: "DeleteCluster" or json_payload.event_type: "CreateCluster") and not json_payload.request_metadata.remote_address: "51.250"</pre>	<pre>event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.mdb.*. UpdateUser or yandex.cloud.audit.mdb.*.C reateUser or yandex.cloud.audit.mdb.*.C reateCluster or yandex.cloud.audit.mdb.*.U pdateCluster) and source.ip : ("2a00:1fa0:474:9876:4cac: 6c43:12aa:2bd2" or "2a00:1fa0:474:9876:4cac:6 c43:12aa:2bd1")</pre>	-
36	new	<pre>(json_payload.event_type: "CreateCluster" or</pre>	---	





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	Включение потенциально опасной настройки при создании или обновлении кластера: -доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	<code>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")</code>		
38	new Не включена «Защита от удаления» при создании	<code>json_payload.event_type: "CreateCluster" and not json_payload.request_parameters.deletion_protection EXISTS</code>	---	
39	new Отключение аудит логов mdb postgres	<code>json_payload.event_type: "UpdateCluster" and json_payload.request_parameters.config_spec.postgresql_config_14.log_statement: "LOG_STATEMENT_NONE"</code>	---	
40	new	<code>json_payload.event_type: "UpdateUser" and json_payload.request_parameters.grants[0]: "mdb_admin"</code>	---	





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	Выдача привелигированных GRANT mdb_admin пользователю			
41	new Создание кластера без установленной Security Group	<code>json_payload.event_type: "CreateCluster" and not json_payload.request_parameters.security_group_ids EXISTS</code>	---	
Container registry vulnarebility scanner				
42	new Обнаружены критические уязвимости при сканировании образа	<code>json_payload.event_type : "yandex.cloud.audit.containerregistry.ScannedImage" and json_payload.details.vulnerability_statuses.critical > 0</code>		
Managed service for gitlab				
43	new Создание инстанса Gitlab	<code>json_payload.event_type : "yandex.cloud.audit.gitlab.CreateInstance"</code>		
44	new Домен префикс содержит имя компании	<code>json_payload.event_type : "yandex.cloud.audit.gitlab.CreateInstance" and json_payload.request_parameters.domain_prefix = "teststastatsata"</code>		





№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
Следующие Use cases не являются частью Audit Trails, а являются нативными аудитлогами k8s, также на текущий момент их невозможно анализировать в CloudLogging				
Kubernetes (для событий k8s необходимо настроить решение)				
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,	---	event.dataset : yandexcloud.k8s_audit_logs and	

№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
	удаление, изменение		requestObject.kind.keyword: (NetworkPolicy or CiliumNetworkPolicy or DeleteOptions) and verb : (create or update or delete) and objectRef.resource : networkpolicies	
5	Ехес внутрь контейнера (шелл внутрь контейнера)	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.subresource.keyword: exec	
6	Создание pod с image HE 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	

№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
			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	

№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
			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 :	

№	Название	CloudLogging 	Elasticsearch  Opensearch 	Yandex Query  (S3 or YDS)
			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 Kyverno: 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		event.dataset : yandexcloud.k8s_audit_logs and not user.name: "ajesnkfk77l50isvg" and not user.name:	

№	Название	CloudLogging 	Elasticsearch   Opensearch	Yandex Query  (S3 or YDS)
	отличной от ci/cd (данный объект ходит в lockbox и копирует оттуда секрет)		"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")	