









Searches & Use Cases



Содержание


№	Название	CloudLogging 	Elasticsearch 	Примечания
Searches				
1	Найти, кто удалил фолдер (!!требует указания 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>	
2	Найти, кто создал/остановил/перезапустил/удалил виртуальную машину (!!требует указания 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" or json_payload.event_type="yandex.cloud.audit.compute.RestartInstance")</code>	<code>event.dataset: yandexcloud.audittrail and event.action : yandex.cloud.audit.compute.*Instance and cloud.instance.name: testdasdas</code>	
3	Какие действия совершал конкретный	<code>json_payload.authentication.subject_name="mirtov8@yandex-team.ru" and json_payload.event_time"<"2022-03-01"</code>	<code>event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	пользователь за период времени (!!требует указания своих значений!!)	<code>and json_payload.event_time<"2022-04-01"</code>	<code>team.ru and event_time < 2022-07-15</code>	
4	Поиск событий по объектам определенного фолдера (!!требует указания 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>	
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>	
2	Срабатывание на любое действие под привелигированным account c	<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>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	ролью “resource- manager.clouds. owner” и “organization- manager.admin ” (можно списком) (!!требуется указания значений!!)			
3	Аномальное кол-во попыток неуспешной авторизации (!!требуется 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_id="admin"	event.dataset: yandexcloud.audittrail and details.access_binding_deltas .access_binding.role_id: admin	
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	
6	Обращение к API с помощью	json_payload.request_metadata.user_agent:"YC" or	event.dataset: yandexcloud.audittrail and	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	YC или terraform под подозрительным пользователем или ip	<code>json_payload.request_metadata.user_agent:"Terraform"</code>	<code>(user_agent.original.keyword:*YC/* or user_agent.original.keyword:*Terraform*)</code>	
7	Coming soon В федерацию добавили новый сертификат	---	---	
8	Coming soon Изменили настройки федерации	---	---	
9	new 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>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
Compute				
10	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>	
11	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>	
12	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>	
13	Создание ВМ 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>	
14	Добавление публичного IP-адреса существующей	<code>json_payload.event_type="yandex.cloud.audit.compute.AddInstanceOneToOneNat"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.AddInstanceOneToOneNat</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	виртуальной машине			
15	События создания/изменения ВМ – включение серийного порта	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.metadata_serial_port_enable="1"</code>	<code>event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and details.metadata_serial_port_enable: 1</code>	
16	new Изменение ВМ - добавление доступа к серийной консоли	<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_serial_port_enable="1"</code>	<code>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</code>	
17	new Значение пользовательской метадаты ВМ предположительно содержит чувствительные данные	<code>(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...</code>	<code>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</code>	
	Создание ВМ без SG	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not</code>	<code>event.dataset: yandexcloud.audittrail and event.outcome : success and</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
		<code>json_payload.details.network_interfaces.security_group_ids EXISTS</code>	<code>event.action: yandex.cloud.audit.compute.CreateInstance and not details.network_interfaces.security_group_ids: *</code>	
VPC				
18	Создание слишком широкого (небезопасного) ACL Security Group для ipv4, tcp	<code>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"</code>	<code>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*</code>	
19	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: grator</code>	
20	new Создание/применение security group аккаунтом не из списка разрешенных	<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 	Примечания
	(!!требуется указание значений!!)			
21	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>	
ObjectStorage(S3)				
22	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>	
23	new Object storage bucket (S3) стал публичным при создании/изменении	<code>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")</code>	<code>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)</code>	
24	new 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>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
Lockbox/KMS				
25	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>	
26	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>	
27	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>	
28	new Назначение имеющего доступ к локбокс секретам сервисного аккаунта на ВМ (!!требуется указание значений!!)	<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>	
29	new	<code>json_payload.event_type="yandex.cloud.audit.lockbox.GetPayload"</code>	<code>event.dataset: yandexcloud.audittrail and</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	Чтение секрета из Lockbox с IP адреса отличного от <u>диапозона адресов облака</u> (!!требуется указания значений!!)	<code>and not json_payload.request_metadata.remote_address:"51.250"...</code>	<code>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>	
30	new 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>	
MDB				
31	new Создание кластера MDB пользователем облака не из	<code>json_payload.event_type: "yandex.cloud.audit.mdb." and not json_payload.authentication.subject_name: "test"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.*.CreateCluster and not user.name :</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
	списка администраторов (!!требуется указания значений!!)		mirtov8@yandex-team.ru kirill@yandex-team.ru	
32	new Создание/Изменение пользователя MDB	<code>json_payload.event_type: "CreateUser"</code> or <code>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>	
33	new Удаление кластера MDB	<code>json_payload.event_type: "DeleteCluster"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.*.DeleteCluster</code>	
34	new Административные действия с MDB с ip адресов, которые отличаются от доверенного диапазона (!!требуется указания значений!!)	<code>(json_payload.event_type: "DeleteCluster" or json_payload.event_type: "CreateCluster") and not json_payload.request_metadata.remote_address: "51.250"</code>	<code>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")</code>	



№	Название	CloudLogging 	Elasticsearch 	Примечания
35	coming soon Включение опасной настройки при создании кластера	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
36	coming soon Включение опасной настройки при изменении кластера	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
37	coming soon Не включена /снятие галочки «Защита от удаления» при создании/измен ении	--	---	
38	coming soon Изменение настроек влияющих на сбор аудит логов из MDB при создании/измен ении	-настройки log_statements and log_connections	---	

№	Название	CloudLogging 	Elasticsearch 	Примечания
39	coming soon Выдача привелегированных GRANT mdb_admin пользователю	---	---	
40	coming soon Создание/Изменение кластера без установленной Security Group	---	---	
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	

№	Название	CloudLogging 	Elasticsearch 	Примечания
			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	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 responseObject.status.containerStatuses.image.keyword: *cr.yandex/* and responseObject.status.containerStatuses.containerID : *docker* and verb : patch and not responseObject.status.containerStatuses.image.keyword: (*falco* or *openpolicyagent* or *kyverno* or *k8s.gcr.io*)	

№	Название	CloudLogging 	Elasticsearch 	Примечания
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-аpi 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 :	

№	Название	CloudLogging 	Elasticsearch 	Примечания
			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 : "\"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	

№	Название	CloudLogging 	Elasticsearch 	Примечания
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	