









Searches & Use Cases



No	Name	CloudLogging 	Elasticsearch 	Comments
Searches				
1	Find who deleted a folder (requires values)	<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	Find who created/stopped/restarted/deleted a virtual machine (requires values)	<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	What actions did a particular user perform over a period of time (requires values)	<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>	<code>event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru and event_time < 2022-07-15</code>	



No	Name	CloudLogging 	Elasticsearch 	Comments
4	<i>Search for events by objects of a specific folder (requires values)</i>	<pre> 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>" </pre>	<pre> event.dataset:yandexcloud.audittrail and cloud.folder.name:"mirtov-scale" </pre>	
Use cases				
IAM				
1	<i>Triggered when creating service account credentials</i>	<pre> 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" </pre>	<pre> event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.iam.CreateAccessKey or yandex.cloud.audit.iam.CreateKey or yandex.cloud.audit.iam.CreateApiKey) </pre>	
2	Trigger on any action under a privileged account with the role "resource-manager.clouds.owner" and "organization-manager.admin" (can be a list) (requires values)	<pre> json_payload.authentication.subject_name="mirtov8@yandex-team.ru" or json_payload.authentication.subject_name="kirill@yandex-team.ru" </pre>	<pre> event.dataset: yandexcloud.audittrail and user.name : mirtov8@yandex-team.ru kirill8@yandex-team.ru </pre>	


No	Name	CloudLogging 	Elasticsearch 	Comments
	(requires values)			
3	Abnormal number of failed authorization attempts (requires values)	---	event.dataset: yandexcloud.audittrail and error.message: Permission denied	
4	Assignment of admin rights (for resources: 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	Assigning the vpc.public.admin role	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	Calling the API using YC or terraform under a suspicious user or ip	json_payload.request_metadata.user_agent:"YC" or json_payload.request_metadata.user_agent:"Terraform"	event.dataset: yandexcloud.audittrail and (user_agent.original.keyword: *YC/* or user_agent.original.keyword: *Terraform*)	
7	coming soon A new certificate has been added to the federation	---	---	
8	coming soon	---	---	



No	Name	CloudLogging 	Elasticsearch 	Comments
	Changed federation settings			
9	new <i>Any action using a cloud service account from a range of IP addresses outside the cloud</i>	not <code>json_payload.request_metadata.remote_address:"51.250"...</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: *	
Compute				
10	Triggering on an event with the creation of a VM with a white IP address	<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>	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and details.network_interfaces.primary_v4_address.one_to_one_nat.address: *	
11	Triggered to create "two-legged" virtual machines	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.network_interfaces[1].index="1"</code>	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.CreateInstance and	



No	Name	CloudLogging 	Elasticsearch 	Comments
			details.network_interfaces.index: 1	
12	Uploading an image to the cloud from a non-fixed S3 Bucket (requires values)	<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>	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"	
13	Create VM with image_id from Marketplace	<code>not json_payload.details.product_ids[0]=null</code>	event.dataset: yandexcloud.audittrail and details.product_ids: *	
14	Adding a public IP address to an existing virtual machine	<code>json_payload.event_type="yandex.cloud.audit.compute.AddInstanceOneToOneNat"</code>	event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.compute.AddInstanceOneToOneNat	
15	VM creation/modification events - enabling the serial port	<code>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and json_payload.details.metadata_serial_port_enable="1"</code>	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and details.metadata_serial_port_enable: 1	
16	new Modifying VM - Adding Access to Serial Console	<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>	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: (yandex.cloud.audit.compute.CreateInstance or	



No	Name	CloudLogging 	Elasticsearch 	Comments
			yandex.cloud.audit.compute.UpdateInstance) and details.metadata_serial_port_enable: 1	
17	new VM custom metadata value suspected to contain sensitive data	(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...	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	
	Creating a VM without SG	json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not json_payload.details.network_interfaces.security_group_ids EXISTS	event.dataset: yandexcloud.audittrail and event.outcome : success and event.action: yandex.cloud.audit.compute.CreateInstance and not details.network_interfaces.security_group_ids: *	
VPC				
18	Creating too wide (insecure) ACL Security Group for ipv4, tcp	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"	event.dataset: yandexcloud.audittrail and (event.action: yandex.cloud.audit.network.CreateSecurityGroup or yandex.cloud.audit.network.UpdateSecurityGroup) and details.rules.direction: INGRESS and	



№	Name	CloudLogging 	Elasticsearch 	Comments
			details.rules.cidr_blocks.v4_cidr_blocks: *0.0.0.0*	
19	Creating a public address without a DDoS protection checkbox	<pre>json_payload.event_type="yandex.cloud.audit.compute.CreateInstance" and not json_payload.details.external_ipv4_address.requirements.ddos_protection_provider exists</pre>	<pre>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.CreateAddress and not details.external_ipv4_address.requirements.ddos_protection_provider: qtrator</pre>	
20	new Creating / applying a security group by an account not from the list of allowed (requires values)	<pre>(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"</pre>	<pre>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</pre>	
21	Any action with Security Group objects	<pre>json_payload.event_type="yandex.cloud.audit.network.CreateSecurityGroup" or json_payload.event_type="yandex.cloud.audit.network.UpdateSecurityGroup"</pre>	<pre>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.network.*SecurityGroup</pre>	
ObjectStorage(S3)				
22	Подозрительные действия с хранилищем логов AuditTrails (S3 Bucket)	<pre>json_payload.event_type="yandex.cloud.audit.storage.BucketAclUpdate" or json_payload.event_type="yandex.cloud.audit.storage.BucketPolicyUpdate"</pre>	<pre>event.dataset: yandexcloud.audittrail and event.action: (yandex.cloud.audit.storage.BucketAclUpdate or yandex.cloud.audit.storage.BucketPolicyUpdate)</pre>	



No	Name	CloudLogging 	Elasticsearch 	Comments
23	new Suspicious activities with the AuditTrails log storage (S3 Bucket)	<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) became public when created/modified via 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>	
Lockbox/KMS				
25	Triggered by changing access rights to KMS symmetric encryption keys	<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	Removing a KMS key	<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>	



No	Name	CloudLogging 	Elasticsearch 	Comments
27	Assigning/Updating LockBox Secret Rights	<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 Assigning a person with access to a lockbox service account secrets on the VM (requires values)	<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 Reading a secret from Lockbox from an IP address different from the cloud address range (requires values)	<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>	



No	Name	CloudLogging 	Elasticsearch 	Comments
30	new Reading a secret from Lockbox using an account that is different from the target (requires values)	<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 Creating an MDB cluster by a cloud user not from the list of administrators (requires values)	<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 : mirtov8@yandex-team.ru kirill@yandex-team.ru</code>	
32	new Creating/Changing an MDB User	<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>	
33	new Deleting an MDB Cluster	<code>json_payload.event_type: "DeleteCluster"</code>	<code>event.dataset: yandexcloud.audittrail and event.action: yandex.cloud.audit.mdb.*.DeleteCluster</code>	
34	new	<code>(json_payload.event_type: "DeleteCluster" or</code>	<code>event.dataset: yandexcloud.audittrail and</code>	



No	Name	CloudLogging 	Elasticsearch 	Comments
	Administrative actions with MDB from ip addresses that are different from the trusted range (requires values)	<code>json_payload.event_type: "CreateCluster") and not json_payload.request_metadata.remote_address: "51.250"</code>	<code>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>	
35	coming soon Enabling a dangerous setting when creating a cluster	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
36	coming soon Enabling a dangerous setting when changing a cluster	-доступ из datalens -публичный доступ -доступ из консоли управления -доступ из serverless	---	
37	coming soon Not enabled / unchecked "Protection from deletion" when	--	---	



No	Name	CloudLogging 	Elasticsearch 	Comments
	creating/changing			
38	coming soon Changing settings affecting the collection of audit logs from MDB when creating / changing	-настройки log_statements and log_connections	---	
39	coming soon Issuing privileged GRANT mdb_admin to a user	---	---	
40	coming soon Creating/Modifying a Cluster without a Security Group Installed	---	---	
The following Use cases are not part of Audit Trails, but are native k8s audit logs, and currently they cannot be analyzed in CloudLogging				
Kubernetes (for k8s events, you need to set up a solution)				
General				

No	Name	CloudLogging 	Elasticsearch 	Comments
1	Access denied events - 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	Assigning a cluster-admin or admin role (clusterrolebinding or 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	Successful connection to the cluster from an external IP address	---	event.dataset : yandexcloud.k8s_audit_logs and source.ip : * and not responseStatus.status : Failure	
4	NetworkPolicies: create, delete, change	---	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	Exec inside the container (shell	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.subresource.keyword: exec	

No	Name	CloudLogging 	Elasticsearch 	Comments
	inside the container)			
6	Creating a pod with image NOT from Yandex container registry (not relevant for Clients using their own 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	Create pod in 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	Calling k8s-api under a service account from an external ip address	---	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				

No	Name	CloudLogging 	Elasticsearch 	Comments
9	Any Alert from Falco	---	event.dataset : yandexcloud.k8s_falco and not objectRef.namespace: falco	
10	Falco removed	---	event.dataset : yandexcloud.k8s_audit_logs and verb : delete and objectRef.namespace.keyword: falco and objectRef.resource.keyword : daemonsets	
OPA Gatekeeper				
11	OPA Gatekeeper triggered - denied events (only in enforce mode)	---	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 : system\\\\:serviceaccount\\\\:kube-system\\\\:daemon-set-controller	
12	Removing a gatekeeper from a k8s cluster	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword: gatekeeper-validating-webhook-configuration and verb : delete	
13	Modifying/deleting a Constraint object	---	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				

No	Name	CloudLogging 	Elasticsearch 	Comments
14	Kyverno triggered - denied events (only in enforce mode)	---	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 : system\\\\\\:serviceaccount\\\\\\:kube-system\\\\\\:daemon-set-controller	
15	Removing Kyverno from the k8s cluster	---	event.dataset : yandexcloud.k8s_audit_logs and objectRef.name.keyword: kyverno-resource-validating-webhook-cfg and verb : delete	
16	Changing/deleting a Kyverno Policy object	---	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	Kyverno triggered: fail status of policy result (Yandexcloud:k8s:kyverno-reporter-detect)	---	event.dataset : yandexcloud.k8s_kyverno and Status : fail	
External Secrets				

No	Name	CloudLogging 	Elasticsearch 	Comments
18	Changing / creating an external secrets object with an account other than ci / cd (this object goes to the lockbox and copies the secret from there)		event.dataset : yandexcloud.k8s_audit_logs and not user.name: "ajesnkfk77lbh50isvg" and not user.name: "system:serviceaccount:external-secrets:external-secrets" and objectRef.name: "external-secret" and verb: (patch or create)	
19	Read secrets under user account		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")	