

Introduction

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services that facilitate declarative configuration and automation. It has a large, rapidly growing ecosystem. Kubernetes services, support, and tools are widely available. This document covers the community release of the Kubernetes plug-in.

Scope

This community release covers Amazon Elastic Kubernetes Service (EKS), normalizing logs served from the CloudWatch log source, and Kubernetes installations on Linux, such as Ubuntu, normalizing logs served from the Linux (syslog) log source.

Package Contents

This release contains the following files:

- Kubernetes Alert Rules (4 alert rules)
 - Install via Settings > KB > Alert Rules > Import (KubernetesAlertRules.pak)
- Kubernetes Audit Compiled Normalizer
 - Install via Settings > Configuration > Universal Normalizer > Add > Browse (KubernetesAuditCompiledNormalizer.pak) > Upload Config
- Kubernetes Dashboard (8 dashboards)
 - Install via Settings > KB > Dashboards > Import (KubernetesDashboards.pak)
- Kubernetes Report Template (1 report)
 - Install via Reports > Report Templates > Import (KubernetesReportTemplate.pak)
- Kubernetes Search Template (1 report with 3 tabs)
 - Install via Settings > KB > Search Templates > Import (KubernetesSearchTemplate.pak)

I. LOGPOINT

Installation

Install each of the packages in turn, as detailed below:

Kubernetes Alert Rules (4 alert rules)

- Move to Settings > Knowledge Base > Alert Rules > Import
- Import the file KubernetesAlertRules.pak

The imported Alert Rules should look as below:

_							
•	BACK	All Alert Rules					
	TABULAR	VIEW 🔻 👩 ADD 🛕 ALL RULES 🔻	LIMPORT Select Log Source	4 ACTIVE RULES FILTER ACTIVE RULES		0 SELECTED MO	RE 🔻 search 🔕
E	S.N.	Name	Description	Log Source	Attack Category	Attack Tag	Actions
	1	K8s Resource Access Denied Active	This alert informs that the user tried to access some resource by was denied by the K8s Role Policy.	Kubernetes	Discovery	T1526 - Cloud Service Discovery T1580 - Cloud Infrastructure Discovery T1613 - Container and Resource Discovery T1619 - Cloud Storage Object Discovery	ঀৢৢৢ৾ঀৢড়ঀ৾৾ঀৣ৾ঀ৾ঀ৾৾ঀ৾৾ঀ৾৾ঀ৾৾৾ঀ৾৾
	2	K8s Exec into Container Active	This alert is triggered when ever a user tried to perform shell access into a container/pod in K8s Cluster.	kubernetes	Execution	T1609 - Container Administration Command	△◎♠♂徵會Q
0] 3	Possible Access or Tampering of Secrets by Unknown User Detected Active	This alert rule is triggered when it detects possible tampering of secrets across namespace. A Secret is an APP object used toos confidential data in key-value pairs which allows users to decouple environment specific Credentials from their contain images, so that their applications are easily portable. Adversaries can modify or delete Secrets in order to disrupt the execution of applications.	D D Pr	Reconnaissance Impact	T1565 - Data Manipulation T1589.001 - Credentials	മ ്പ ്പ് ലെ
] 4	K8s Suspicious Deletion of Kubernetes Events Resource Active	This alert rule is triggered when it detects deletion of Kubernetes "event" resources. These resources are never deleted by general users. Anomalous number of deleted events might indicate that adversaries are trying to cover their tracks.	Kubernetes	Defense Evasion	T1070.009 - Clear Persistence T1562 - Impair Defenses	▲⊘┑♂役ііQ

I LOGPOINT

Kubernetes Audit Compiled Normalizer

- Move to Settings > Configuration > Universal Normalizer > Add
- Specify the file KubernetesAuditCompiledNormalizer.pak in the dialogue that appears
- Choose Upload Config
- Make sure the screen looks the same as the screenshot below. If so, click **Save**.

ADD CUSTOM PA	CKAGE			0 0
UNIVERSAL NORM	IALIZER			
Config File:	KubernetesAuditCom	piledNormalizer.pak		Browse
				Upload Config
Application Name*	KubernetesAudit			
Norm IDN	kßsAuditNormalizer			
Norm ID-:	kosAdditivormalizer			
Log Identifier Rege	x*: audit.k8s.io/v1			
Device Category*:	ContainerOrchestrato	¢		
Log Type:	 JSON 	O CEF	\odot csv	
	○ XML	O LEEF	Key-Val	ue Pair
Parsing Depth:	5			Ŧ
		Parse Fields Further		
requestobject,	Successfully pulled image "<	im Successfully pulled image "ngir	Norm	5
requestobject,	Container image * <image_na< td=""><td>Container image *registry.k8s.ix</td><td>Norm</td><td>- 2 + -</td></image_na<>	Container image *registry.k8s.ix	Norm	- 2 + -
request_uri	<request_url:all>?command=</request_url:all>	/api/v1/namespaces/default/po</td <td>Norm</td> <td>- 6 + -</td>	Norm	- 6 + -
responsestatus	<forbidden_resource:words></forbidden_resource:words>	is pods is forbidden: User "system	Norm	- 6 + -
sourceips	[" <source_ip:ip>"]</source_ip:ip>	["10.45.20.141"]	Norm	- 6 + -
Field Taxonomy CS	V file: Select a CSV File to in	nport		Browse
				Upload Taxonomy
		Tes	t Sav	re Cancel

- Check the normalizer is installed by moving to Settings > Log Sources and clicking Add Log Source
- Choose either Linux or CloudWatch as the log source
- Move to the **Normalization** tab and type **Kubernetes** in the search bar on the left
- CustomKubernetesAuditCompiledNormalizer should be selected, as shown below

Log Sources / CloudWatch				
CloudWatch CloudWatchFetcher				Create Log Source
Details	Source Connector 🜖 Routing 🕦	Normalization Enrichment		
Template				Select Normalization Pol 🗸
Version: 3 - Last Updated: 2024/10/24 06:42:12	Normalizer			
Vendor Name AWS	0/733 items	Available	0/2 items	Available
Description Collects logs generated from AWS CloudWatch, including Amazon EC2 instances, Amazon EBS volumes,	kubernetes	Q		Q
Elastic Load Balancers, and Amazon RDS DB instances.	CustomKubernetesAuditCom	compiled	\equiv CloudWatchCompiledNormal	compiled
Documentation	CustomKubernete	esAuditCompiledNormalizer	⊟ LP_AWS CloudWatch	regex 🗍

I LOGPOINT

Kubernetes Dashboard (8 dashboards)

- Move to Settings > Knowledge Base > Dashboards > Import
- Import the file KubernetesDashboards.pak

The imported Dashboards should look as below (first dashboard only shown)

MY DASHBOARD 🔻 🔔 EXPORT 🛓 IMPORT		MORE *	0 SELECTED	search	0
S.N. Name	Widgets Info			Action	ns
1 Kubernetes - Roles and RoleBinding	widget_name: User Roles Created description: This widget shows us the information about the cluster user who has created new role in cluster. genery: "resource" of "roles" request_method=create [enname resource_name as roleName [chart count() by user, roleName, resource_namespace display_type: chart report: Trops for 1 LopPoints time_range: last 1 day public urit: https://3.250.41.15/s/epi/frame/widget/5/48859d4110f9Edb&e30a0			4 ⊘	i ← mî î 🕄
	wided/Luint: Thouse Loop and Link Terminan genery "resources" holds: Include a casted in last 24 Noun genery "resources" holds: Include-increased phant count) as Roles/Created display, type: chart pope: I report from LogPoints time_arrays: Last 1 day public with Terport, 2004, 117 Sept/Interne/widget/674855941109F3db8a30a2				
	widget_rame: RoleBinding Besource Created description: The direct hows the information about the rolebinding created by cluster user. gwary: "response, status_code" #201 "resource"="rolebindings" rename resource_name as RoleBindingCreated chart count() by user, RoleBindingCreated , source_jo display, byte: "chart count) by user, RoleBindingCreated , source_jo display, byte: "chart count of the source" and the source of the source of the source of the source of the source imm_arange_last 1 dy public uti: https://3.250.4.175/api/finame/widget/6748859d4110f93db830a4				
	widget_name: Number of RoleBindings Created description: The widget shows information about the RoleBinding created in a K8s Cluster. query: "response status.code" = 20" Insource "= rolebindings" chart count) as RoleBindingsCreated report: Inpos from 1 LopPoints time_range_List 1 dy public ut: https://s2.20.4.175/epi/frame/widget/6748859d41009Edb8e30e6				

To add a dashboard, move to **Dashboards** and click the orange + button on the right

• Move to **My Dashboards** and choose one of the dashboards shown below

ADD DASHBOARD						8	
New	×				Search	0	
My Dashboards		SN	Name	Widget Count			
Vendor Dashboards	•	1	Kubernetes - Roles and RoleBinding	4			
Used Dashboards	•	2	Kubernetes - Certificates Signing	5			
Shared Dashboards	•	3	KUBERNETES - CONFIGMAPS OVERVIEW	11			
		4	KUBERNETES - SECRETS OVERVIEW	12			
		5	Kubernetes - Deployment Overview	5			
		6	Kubernetes - Service Account	6			
			7	Kubernetes - Cluster Security Overview	20		
		8	Kubernetes - Pods Overview	7			
					Ok	Cancel	

An example dashboard is shown below

Dashboards					
All Dashboards					
AD: USER ACCOUNT MANAGEMENT LP_WINDOWS AUTHENTICATION SOC DARKT	RACE LP_WINDOWS OVERVIEW LP_DEFAULT NIVO	S ACCOUNT MANAGEMENT	ICHER KUBERNETES - CLUSTER SECURITY OVERVIEW	+	
🕼 ADD WIDGET 📄 REPORT 🅐 SHARE				CHANGE REPOS	AUTO ARRANGE
User Activities insides a K8s Cluster	K8s Nodes Information		Response Codes in K8s Cluster		~
0	Nodes 3		20 40 20 50 10 10 10 10 10 10 10 10 10 1	7к 8к	Hecision
Top 10 Source Address	 10.44 154 4 2.42 154 4 2.43 154 4 2.41 154 4 4.41 154 4	Top User Agents arrayet sex agent sex agent sex agent sex agent sex agent sex agent sex agen		kando 132	



Kubernetes Report Template (1 report)

- Move to **Reports > Report Templates > Import**
- Import the file KubernetesReportTemplate.pak

The imported report template should look as per the screenshot below.

MY REPORT TEMPLATES * 1 ADD 1 EXPORT			MORE V 0 SELECTED sean	ch
S.N. Name	Scheduled	User	Version	Actions
1 K8s_GDPR : K8s Secret Resource Audit	0	admin	-	42 to 🗎

Click on the **Run This Report** button () under **Actions** on the right to run the report

A sample from a report is shown below



I. LOGPOINT

Kubernetes Search Template (1 template with three tabs)

- Search Template (1 report with 3 tabs)
 - Install via Settings > KB > Search Templates > Import (KubernetesSearchTemplate.pak)
- Move to Settings > Knowledge Base > Search Templates > Import
- Import the file KubernetesSearchTemplate.pak

The imported search template should look as below

Search Templates		
MY SEARCH TEMPLATES 🔻 👩 ADD 🛓 IMPOR	RT 🔔 EXPORT	MORE * 0 SELECTED search
S.N. Name	Description	Actions
1 User Activity in K8s Cluster	This search Template shows the information about the User Activity in a specific K8s Cluster	🖘 Z L 🛍 🕄

To show the search template, move to **Search Templates** and click on the template name

- There are three tabs
 - User Activities containing 4 widgets
 - Resource Details containing 6 widgets
 - Investigation containing 5 widgets
- On each of the tabs, click on **Update** to see the populated widgets

Search templates are more efficient, update faster and use less memory than dashboards so it is recommended to use search templates over dashboards as much as possible.

An example search template is shown below

et created e created b created b created b created c created	SER ACTIVITIES RESOURCE DETAILS	INVESTIGATION	+				
e Created e created escurceCreated 5,406 e Deted						AUTO	O ARRANGE
e created escourceCreated 5,406							
<figure></figure>	esource Created		Resource Created				
esourceCreated 5,406 e Deleted							
<figure></figure>			user	resource	resource_namespace		
esourceCreated 5,403			_		maduation		
esourceCreated 5,406			system:serviceaccount:kube-sys		production		
s f f f f f f f f f f f f f f f f f f f	ResourceCreate	d	electro menero mader@electron	pods	development		
5,406 e Deleted	needen de choure	G	custer-resource-readerwerd.tocal		staging		
5,406 b c c c c c c c c c c c c c c c c c c c	E 40 (attackerepessiocal		testing		
e Deleted records of the second of the seco	5 406		am:aws:lam::022765405199:use	serviceaccounts	kube-system		
e Deleted	5,400		am:aws:lam::022765405199:us eks:cloud-controller-manager	deployments	calico-system		
e Deleted			am:aws:iam::022765405199:user am:aws:iam::022765405199:use	conngmaps	backend-app		
e Deleted			kube-admin@k8s.local	events	namespace2 namespace4 default		
e Deleted recorrece Deleted recorrece Deleted recorrece Deleted recorrece Deleted recorrece Deleted Resource Deleted Resource Deleted 3,3555			system:node:master-node		calico-apperver ingress-nginx event-geperator		
e Deleted resource_name parts resource_name parts resource_name parts resource_name parts resource_name parts resource_Deleted ResourceDeleted 3,3555 e Updated Resource Deleted ResourceDeleted again ResourceDeleted again ResourceDeleted again ResourceDeleted again ResourceDeleted again					samn-ns		
e Velee U resource Deleted resource Deleted resource Deleted Resource Deleted 3,3555 e Updated e Updated	ource Deleted			Posourco Dolotod			
<pre>result result resu</pre>	Source Deleted			Resource Deleted			
enderspiritzer bezahlen markespiritzer bezahl	r	resource	resource_namespace				
marker 1912 14.0 4 8 a marker 1912 14.0 19 7 a tam configer 1912 14.0 19 7 a tam configer 1912 14.0 19 7 a tam configer 1912 14.0 197 a tam configer 1912 14.0 1910 14.0 197 a tam configer 1912 14.0 197 a	system.node.ip-172-16-10-8.eu						
e Updated Protection Transmission Constraints of the Constraints of th	system:node.jp-172-16-10-9.eu						
e Updated Resource Updated		pods	staning	Resource	Deleted		
e Updated Resource Upda	systemmode.ip-172-16-10-7.eu		anging	Resource	Deleted		
tam::::27/246/3179:us verts verter::::::::::::::::::::::::::::::::::	mawsiam::022765405199:us						
e Updated Resource Updated	arn:aws:iam::022765405199:use	events	testing-ns		55		
e Updated Resource Updated			production-ns	5,5	55		
e Updated Resource Updated	am:aws:iam::022765405199:use	serviceacc	ounts testing				
e Updated Resource Updated	amawsiam:022765405199:use amawsiam:022765405199:us	rolebindin	gs production				
e Updated Resource Updated	arn:aws:iam::022765405199:user	deployme	nts				
e Updated Resource Updated	arn:aws.iam::022765405199:use	conigmap	a overopinant				
e Updated Resource Updated							
e updated Resource updated	0.1.5.1		P				
	source updated		Resource Updated				