

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 🔻	La IMPORT Select Log Source	4 ACTIVE RULES FILTER ACTIVE RULES		0 SELECTED MOR	RE 🔻 search 🙁
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 - Claud Service Discovery T1580 - Claud Infrastructure Discovery T1613 - Container and Resource Discovery T1619 - Claud Storage Object Discovery	ঀৢৢ৶৻৵৻ড়ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻ড়৾৾৻
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	ঀৢ৹৸৻৽৻ঀ৾৾৾৽ঀ
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 API object used to store 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 modely or delete Secrets in order to disrupt the execution of applications.		Reconnaissance Impact	T1565 - Data Manipulation T1589.001 - Credentials	ঀৢৢ৶৻৵৻৻ঀৣ৾৾৻৻৻৾৾৾ঀ৾৾৾৻ঀ৾৾৾৾ঀ৾৾৾৾৾ঀ৾৾৾
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 PAG	CKAGE			0 0
UNIVERSAL NORM	ALIZER			
Config File:	KubernetesAuditComp	iledNormalizer.pak		Browse
				Upload Config
Application Name*:	KubernetesAudit			
Norm ID*:	k8sAuditNormalizer			
Log Identifier Regex	et: audit.k8s.io/v1			
Device Category*:	ContainerOrchestrator			
Log Type:	JSON	O CEF	⊖ csv	
	O XML	O LEEF	O Key-Val	ue Pair
Parsing Depth:	5			Ŧ
		Parse Fields Further		
requestobject,	Successfully pulled image * <in< td=""><td>Successfully pulled image "ngir</td><td>Norm</td><td>- 2 + -</td></in<>	Successfully pulled image "ngir	Norm	- 2 + -
requestobject,	Container image * <image_nar< td=""><td>Container image *registry.k8s.ix</td><td>Norm</td><td>- 6 + -</td></image_nar<>	Container image *registry.k8s.ix	Norm	- 6 + -
request_uri	<request_url:all>?command=<</request_url:all>	/api/v1/namespaces/default/po	Norm	- 2 + -
responsestatu:	<forbidden_resource:words> i</forbidden_resource:words>	pods is forbidden: User "system	Norm	2
sourceips	[" <source_ip:ip>"]</source_ip:ip>	["10.45.20.141"]	Norm	- 2 + -
Field Taxonomy CSV	/ file: Select a CSV File to im	sort		Browse
				Upload Taxonomy
		Tes	t Sar	ve 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 🗸
CloudWatch 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)

← BACK My Dashboards					
MY DASHBOARD * 🚖 EXPORT 🛓 IMPORT		MORE *	0 SELECTED	search	0
S.N. Name	Widgets Info			Actions	
1 Kubernetes - Roles and RoleBinding	widger_name: User Roles Created description: This widget shows us the information about the cluster user who has created new role in cluster. description: This widget shows us the information about the cluster user who has created new role in cluster. description: the shows a state of the shows a state report. In provide the shows a state of the shows a report. In provide the shows a state of the shows a report. In provide the shows a state of the shows a report. In provide the shows a state of the report. The shows a state of the shows a public util. https://220.4.1123.pg//fame/widget/0.48859641099Ddb8a30a/			£2⊘.	⊨ ≘ 3
	widget_name: Roles Created in Ists 24 Hours description: This widget shows us the number of neless created in Ists 24 Hours query: "resource" "roles " request_method=create[chart counti) as Roles/Created diplay, type: chart maps:: Ir topos from 1 LogPoints time_nange: Lest 1 dy public uti: https://d.230.4.175/api//frame/widget/674859/041109/8dole30a2				
	widget_umme: RoleBinding Resource Created description: The widget shows the information about the rolebinding created by cluster user. despr: "response", status, code "a": Discource "rolebindings" rename resource_mame as RoleBindingCreated chart count() by user, RoleBindingCreated , source_jp desponse; Typero from time_uropie.last 1 day public ut: https://a.250.4.175/spi/frame/widget/6748559d410093db8a3pa4				
	widger_name: Number of RoleBindings Created description: The widget show information about the RoleBinding created in a KBs Cluster. despr: "response status.code" = 20" incourse "rolebindings" Chart count) as RoleBindingsCreated expost: I repost from 1 LogPoints times.range1 and 1 dy public url: https://d.250.4.175/spi//frame/widget/67488594H109F8dble30e6				

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
		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 Car	ncel

An example dashboard is shown below

Dashboards									
All Dashboards									
	DARKTRACE LP_WINDOWS OVE	RVIEW LP_DEFAULT	NIYOS ACI	COUNT MANAGEMENT	LP_GATEWAT	CHER KUBERNETES - CLUSTER SECURITY OVER	new 🕂		
🕼 ADD WIDGET 📄 REPORT 🥐 SHARE								CHANGE REPOS	AUTO ARRANGE
User Activities insides a K8s Cluster	K8s Nodes Informa	ition				Response Codes in K8s Cluster			~
0		Node 3	es			200 201 201 201 201 201 201 201 201 201	δK	7к 8к	Hecision
Top 10 Source Address		■ 10.44,1 ■ 49242.5 ■ 47247.9 ■ 47247.9 ■ 112211 ■ 1920.22 ■ 1920.22 ■ 1920.22 ■ 100.50.6	16.44	Top User Agents see.agent udeentit 30.2 (deentities)				Lubert V1.32	



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 🔻 🚯 ADD 🔹 EXPORT 🛓 IMPORT			MORE • 0 SELECTED search	zh
S.N. Name	Scheduled	User	Version	Actions
1 K8s_GDPR : K8s Secret Resource Audit	٥	admin	-	la 🕈 🕒 🛱

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

USER ACTIVITIES RESOURCE DETAILS	INVESTIGATION	+				C
🛛 ADD WIDGET 📄 REPORT					AUTO ARRANGE	UPDATE PARAMETERS
						User:
Resource Created		Resource Created				*
						Resource:
		user	resource	resource_namespace		
		_		production		Namespace:
		system:serviceaccount:kube-sys				*
ResourceCreated	d	cluster-resource-reader@eks.local	pods	development		
Resource creates	u i			staging		Response Codes:
		attacker@eks.local		testing		•
5,406		am:aws:iam::022765405199:use	serviceaccounts	kube-system		Request Methods:
3,400		am:aws:lam::022765405199:us	deployments	calico-system		*
		etiscoloud-controllar-manager am:awstam:022765405199:user am:awstam:022765405199:use	configmaps	backend-app namespace) namespace for dyname call co-appression in protection in protection in protection in protection		
		kube-admin@k8s.local	events	namesbace2 namesbace4		Override widget time range
				catico-apperver		Last 10 minutes
		system:node:master-node		event-generator		REPOS
Resource Deleted			Resource Deleted			All
user	resource	resource_namespace				
system:node:ip-172-16-10-8.eu						
system.node.ip-172-16-10-9.eu						
system country of a revenue.	pods		Resource	Deleted		
system:node:ip-172-16-10-7.eu		staging	Resource	Deleted		
arnawsiam::022765405199:use arnawsiam::022765405199:us						
arr:awsiam::022765405199:use		testing-es	3,3			
am:aws:am::0.22765405199:use	events		3,3	55		
am:awsiam::022765405199:use	serviceacc	production-ns				
arn:awsiam::022765405199:use	roles	testing				
arn:awsiam::022765405199:us	rolebindin					
arn:awsiam::022765405199:user arn:awsiam::022765405199:use	deployme configmap					
antana am. 044 / 07/030						
Resource Updated		Resource Updated				
		1				Back Update St