

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](#))

Installation

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

Kubernetes Alert Rules (4 alert rules)

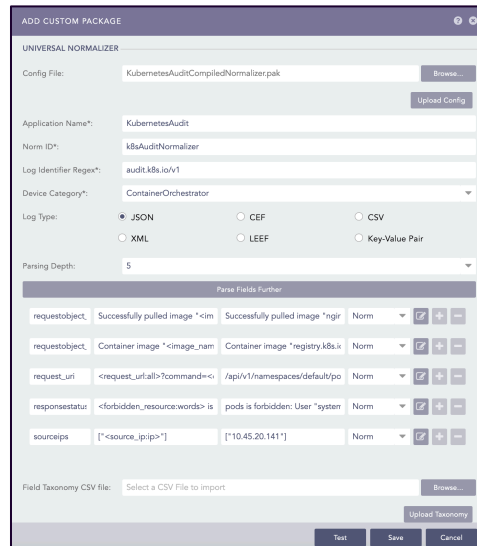
- Move to **Settings > Knowledge Base > Alert Rules > Import**
- Import the file [KubernetesAlertRules.pak](#)

The imported Alert Rules should look as below:

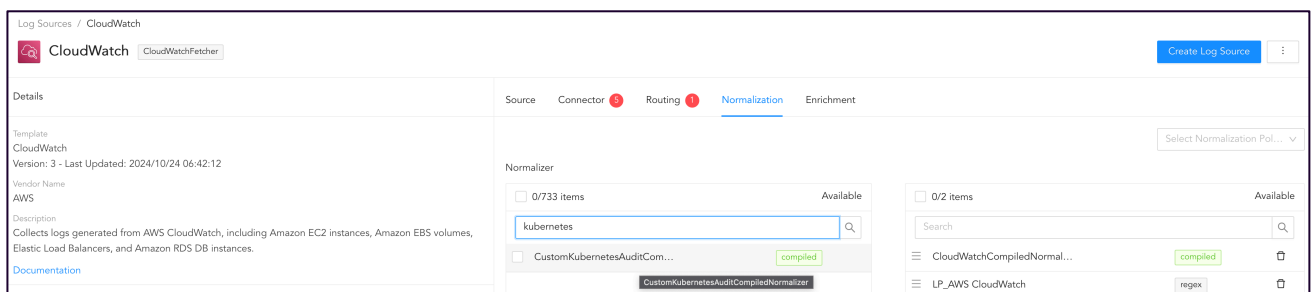
<div> BACK All Alert Rules </div> <div> <div>TABULAR VIEW</div> <div> <div>ADD</div> <div>ALL RULES</div> <div>IMPORT</div> <div>Select Log Source</div> <div>4 ACTIVE RULES</div> <div>FILTER ACTIVE RULES</div> </div> <div>0 SELECTED</div> <div>MORE</div> <div>search</div> </div>							
S.N.	Name	Description	Log Source	Attack Category	Attack Tag	Actions	
1	K8s Resource Access Denied <small>Active</small>	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		
2	K8s Exec into Container <small>Active</small>	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		
3	Possible Access or Tampering of Secrets by Unknown User Detected <small>Active</small>	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 container images, so that their applications are easily portable. Adversaries can modify or delete Secrets in order to disrupt the execution of applications.		Reconnaissance Impact	T1565 - Data Manipulation T1589.001 - Credentials		
4	K8s Suspicious Deletion of Kubernetes Events Resource <small>Active</small>	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		

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**.



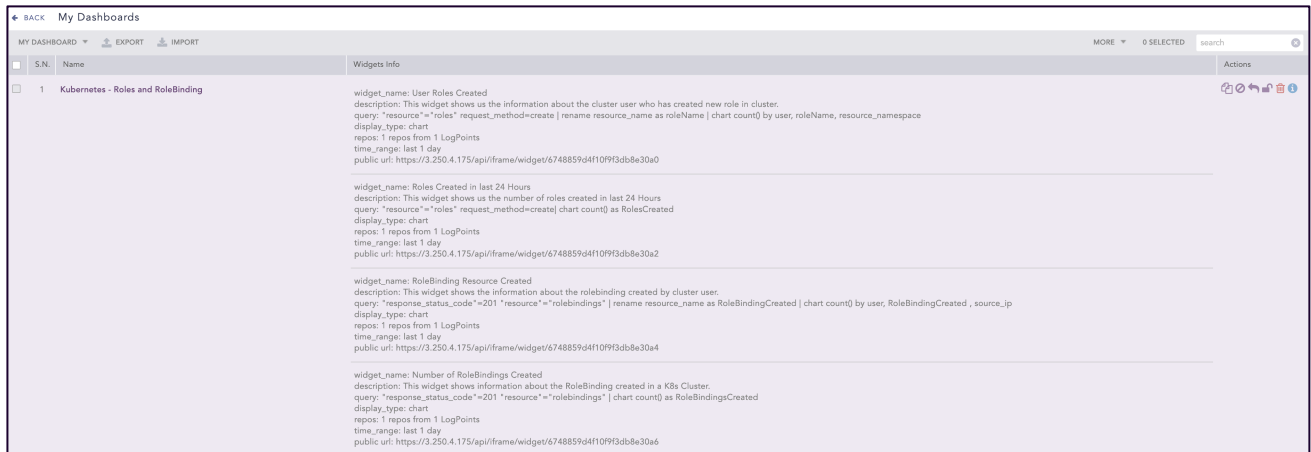
- Check the normalizer is installed by moving to **Settings > Log Sources** and clicking **Add Log Source**
- Choose either **Linux** or **CloudWatch** as the log source
- Move to the **Normalization** tab and type **Kubernetes** in the search bar on the left
- **CustomKubernetesAuditCompiledNormalizer**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



Kubernetes Dashboard (8 dashboards)

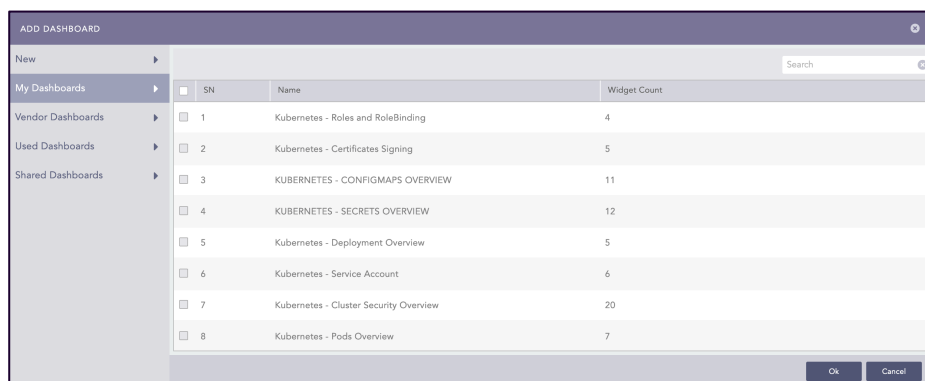
- Move to **Settings > Knowledge Base > Dashboards > Import**
- Import the file **KubernetesDashboards.pak**

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

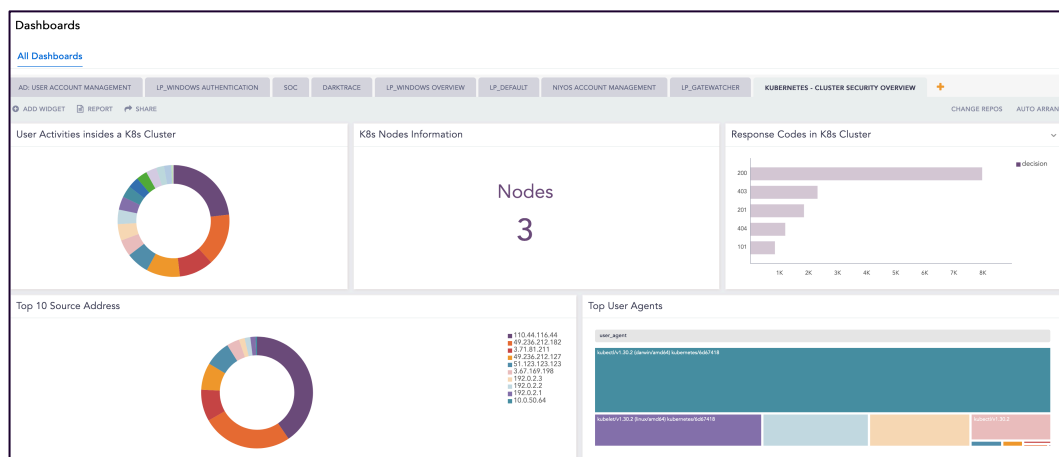


To add a dashboard, move to **Dashboards** and click the orange + button on the right

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



An example dashboard is shown below



Kubernetes Report Template (1 report)

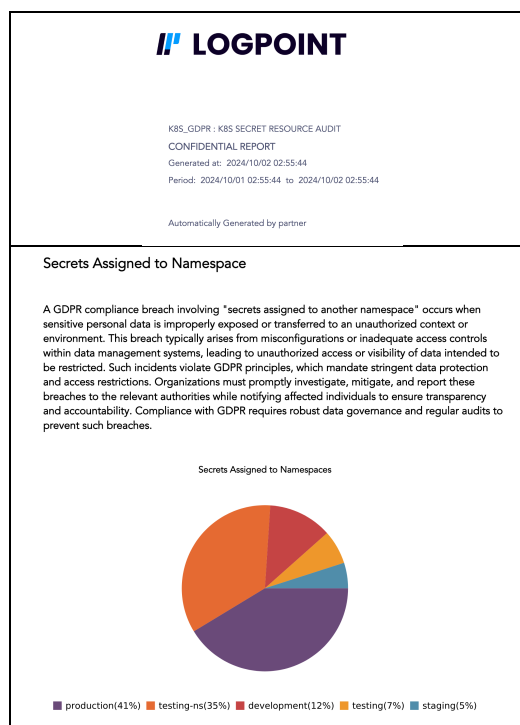
- Move to **Reports > Report Templates > Import**
- Import the file [KubernetesReportTemplate.pak](#)

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

MY REPORT TEMPLATES				MORE		0 SELECTED	search
	S.N.	Name	Scheduled	User	Version	Actions	
<input type="checkbox"/>	1	K8s_GDPR : K8s Secret Resource Audit		admin	-		

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

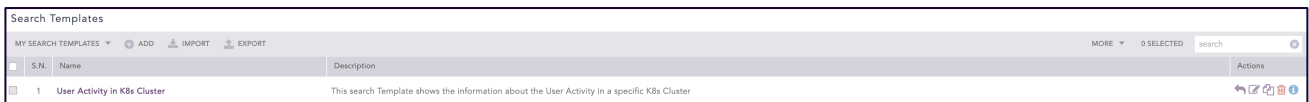
A sample from a report is shown below



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



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

