



KSPM Playbook

- Detects **misconfigurations** in Kubernetes clusters.
- Aligns cluster misconfigurations with **CIS Kubernetes Benchmarks**.
- Visibility into **Kubernetes Identity and Entitlement Management** (KIEM).
 - Provides graph based view into into Kubernetes identities and RBAC best practices controls
 - Minimizes risks by identifying and managing overprivileged entities.

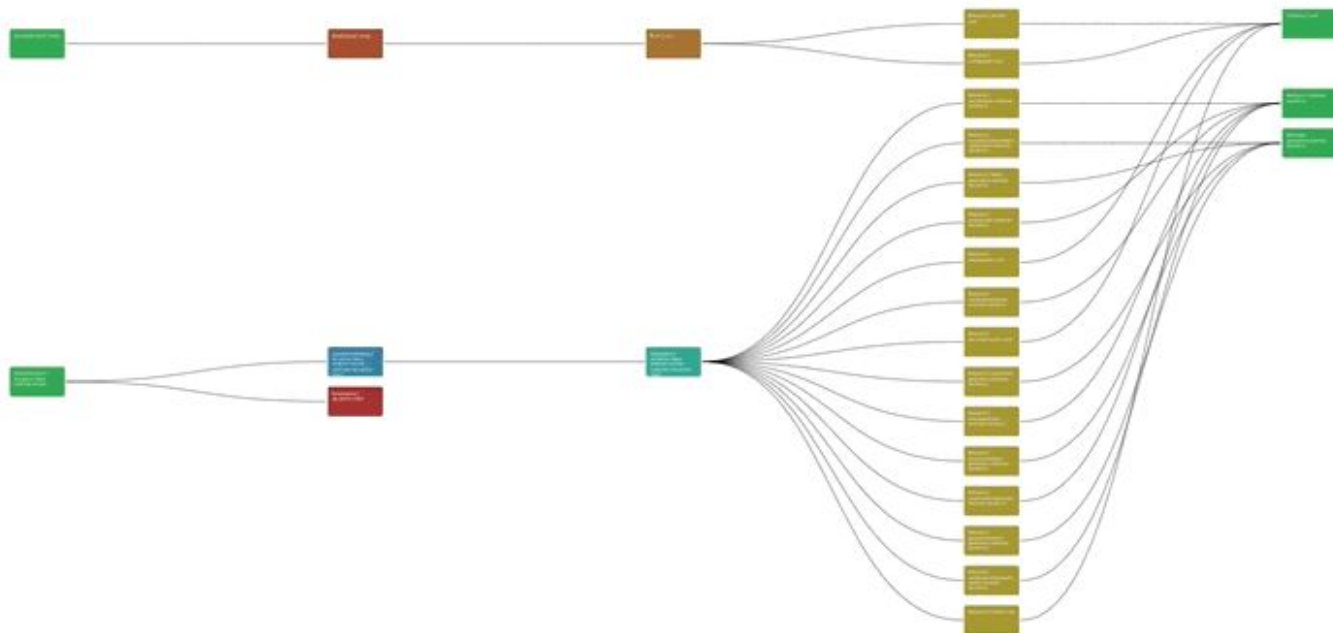


KIEM

General Filter

Save Current State

128 Principals with privileges on all resources



WhoCan

Key Queries

Entity Types

General Findings

Default

Service accounts with no workloads

Principals with high privileges

Anonymous/unauthenticated users/groups

Capabilities of default service account

Container service account mapping

Principals with privileges on all resources

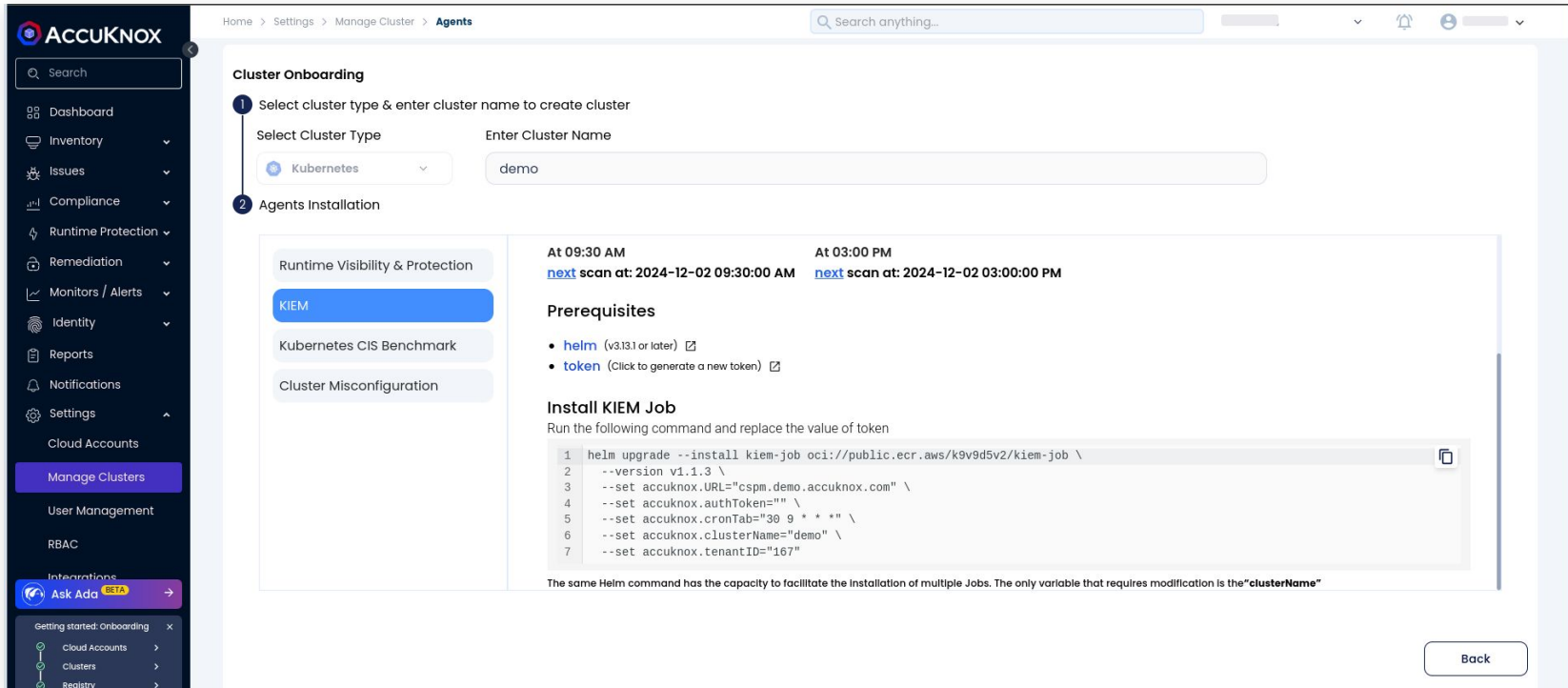
Principals with all privileges on a resource

105 Principals with high privileges



KIEM Installation (Agentless)

- Navigate to **Settings**, choose the onboarded cluster, and select **KIEM**.
- Install KIEM helm chart using the commands displayed on the screen.



The screenshot displays the AccuKnox web interface. On the left is a dark sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters (highlighted), User Management, RBAC, and Integrations. The main content area is titled 'Cluster Onboarding' and shows a progress bar with two steps: '1 Select cluster type & enter cluster name' and '2 Agents Installation'. Under step 1, there's a 'Select Cluster Type' dropdown set to 'Kubernetes' and an 'Enter Cluster Name' text box containing 'demo'. Under step 2, there's a list of options: 'Runtime Visibility & Protection', 'KIEM' (highlighted in blue), 'Kubernetes CIS Benchmark', and 'Cluster Misconfiguration'. To the right of this list, there are two timestamps: 'At 09:30 AM' and 'At 03:00 PM', each followed by a 'next scan at: 2024-12-02 09:30:00 AM' and 'next scan at: 2024-12-02 03:00:00 PM' respectively. Below this is a 'Prerequisites' section with two items: 'helm (v3.13.1 or later)' and 'token (Click to generate a new token)'. The 'Install KIEM Job' section instructs to 'Run the following command and replace the value of token' and provides a code block with a Helm upgrade command. A 'Back' button is located at the bottom right.

Home > Settings > Manage Cluster > Agents

Search anything...

Cluster Onboarding

- 1 Select cluster type & enter cluster name to create cluster
 - Select Cluster Type: Kubernetes
 - Enter Cluster Name: demo
- 2 Agents Installation

Runtime Visibility & Protection

KIEM

Kubernetes CIS Benchmark

Cluster Misconfiguration

At 09:30 AM
[next scan at: 2024-12-02 09:30:00 AM](#)

At 03:00 PM
[next scan at: 2024-12-02 03:00:00 PM](#)

Prerequisites

- [helm](#) (v3.13.1 or later)
- [token](#) (Click to generate a new token)

Install KIEM Job

Run the following command and replace the value of token

```
1 helm upgrade --install kiem-job oci://public.ecr.aws/k9v9d5v2/kiem-job \
2 --version v1.1.3 \
3 --set accuknox.URL="cspm.demo.accuknox.com" \
4 --set accuknox.authToken="" \
5 --set accuknox.cronTab="30 9 * * *" \
6 --set accuknox.clusterName="demo" \
7 --set accuknox.tenantID="167"
```

The same Helm command has the capacity to facilitate the installation of multiple Jobs. The only variable that requires modification is the "clusterName"

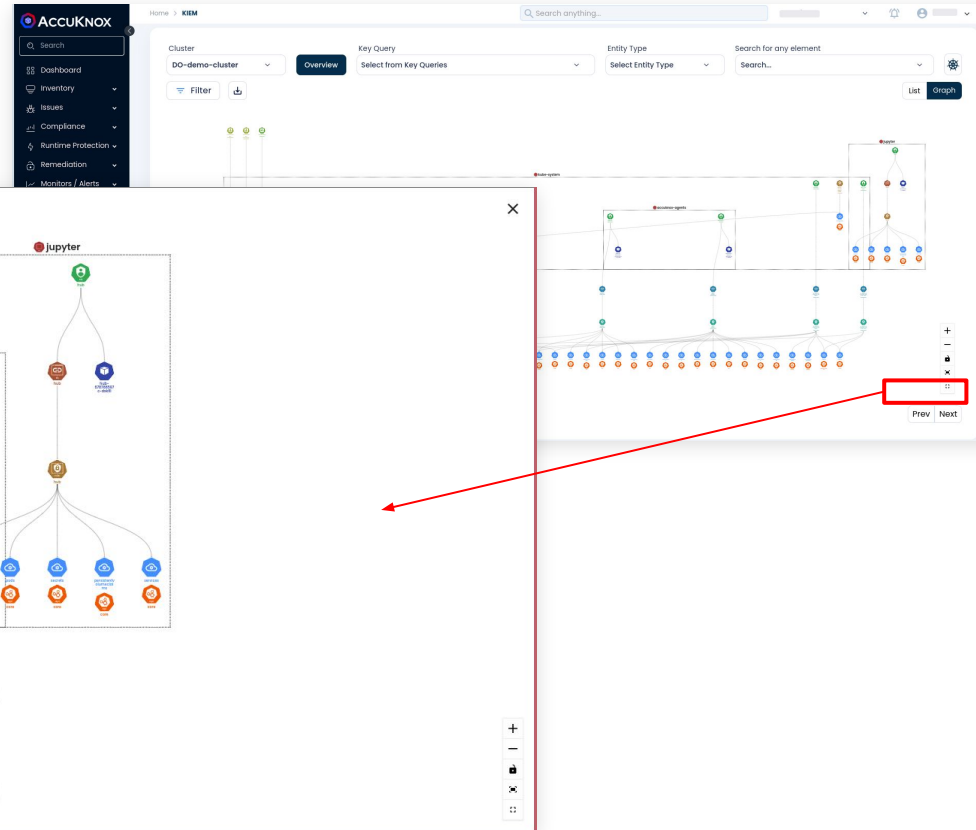
Back

confidential and proprietary - limited distribution under NDA

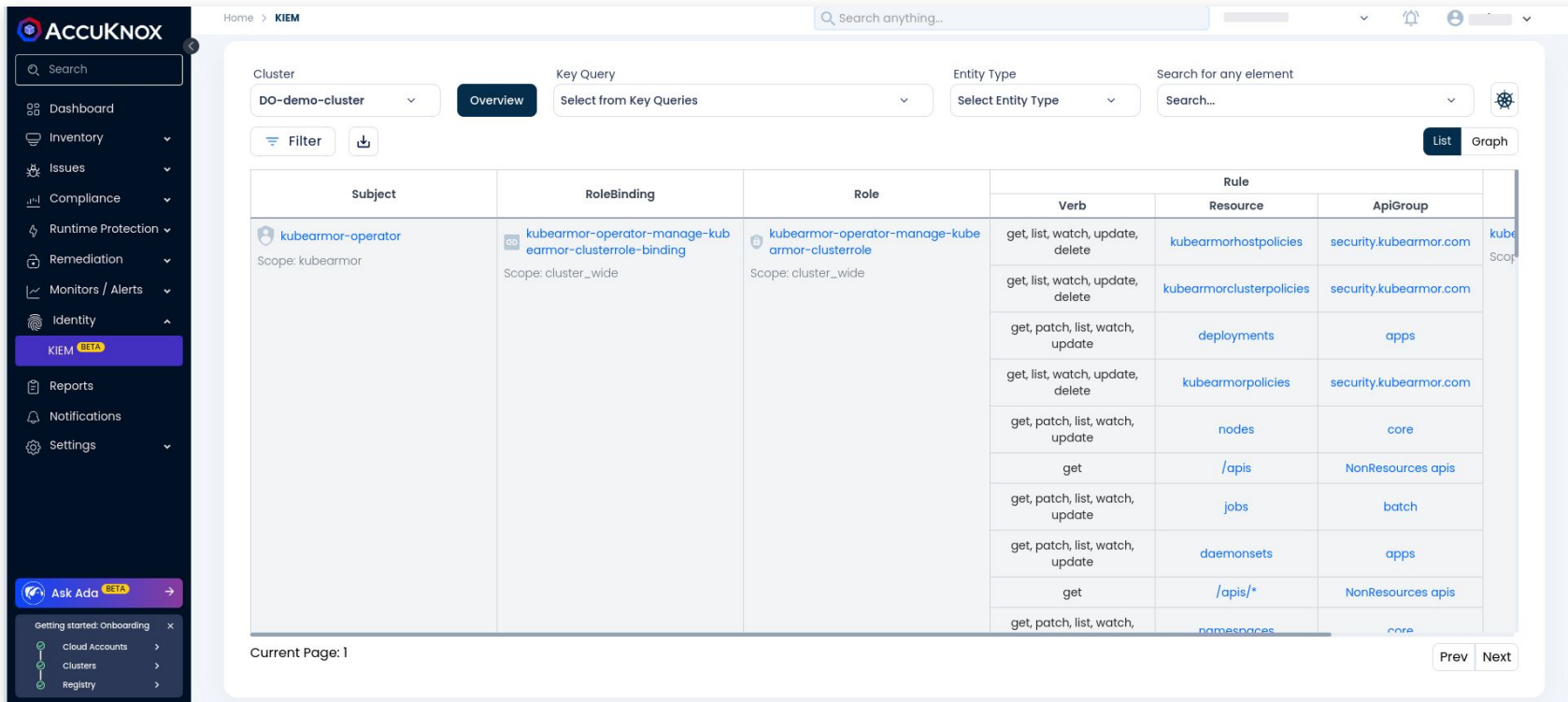
6

KIEM Graph View

- Navigate to **Identity** → **KIEM** to access the KIEM view.
- Click on **Fullscreen** for a detailed graph view.



KIEM data can be filtered by cluster, entity type, or queries such as excessive permissions and admin privileges.



Home > KIEM

Search anything...

Cluster: DO-demo-cluster

Key Query: Select from Key Queries

Entity Type: Select Entity Type

Search for any element: Search...

Filter

List Graph

Subject	RoleBinding	Role	Verb	Rule Resource	ApiGroup
kubearmor-operator Scope: kubearmor	kubearmor-operator-manage-kubearmor-clusterrole-binding Scope: cluster_wide	kubearmor-operator-manage-kubearmor-clusterrole Scope: cluster_wide	get, list, watch, update, delete	kubearmorhostpolicies	security.kubearmor.com
			get, list, watch, update, delete	kubearmorclusterpolicies	security.kubearmor.com
			get, patch, list, watch, update	deployments	apps
			get, list, watch, update, delete	kubearmorpolicies	security.kubearmor.com
			get, patch, list, watch, update	nodes	core
			get	/apis	NonResources apis
			get, patch, list, watch, update	jobs	batch
			get, patch, list, watch, update	daemonsets	apps
			get	/apis/*	NonResources apis
			get, patch, list, watch,	namespaces	core

Current Page: 1

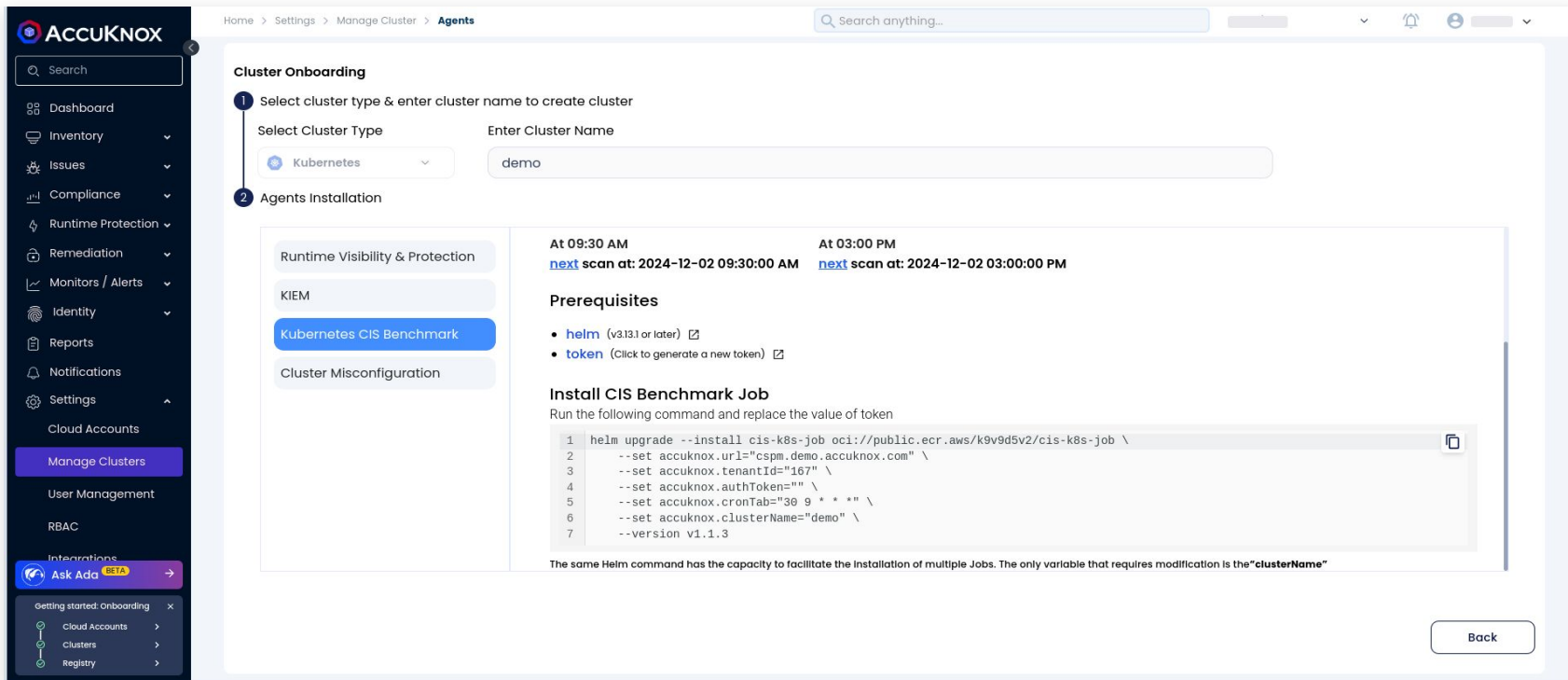
Prev Next



Kubernetes CIS Benchmark

Kubernetes CIS Benchmark (Agentless)

- Navigate to **Settings**, choose the onboarded cluster, and select **Kubernetes CIS Benchmark**.
- Install the helm chart using the commands displayed on the screen.



The screenshot displays the AccuKNOX web interface. On the left is a dark sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters (highlighted), User Management, RBAC, Integrations, and Ask Ada. The main content area is titled 'Cluster Onboarding' and shows a progress bar with two steps: '1 Select cluster type & enter cluster name to create cluster' and '2 Agents Installation'. Under step 1, 'Kubernetes' is selected as the cluster type, and 'demo' is entered as the cluster name. Under step 2, 'Kubernetes CIS Benchmark' is selected from a list of options. To the right, there are two scan status boxes: one for 'Runtime Visibility & Protection' (scanned at 2024-12-02 09:30:00 AM) and one for 'KIEM' (scanned at 2024-12-02 03:00:00 PM). Below these, the 'Prerequisites' section lists 'helm' (v3.13.1 or later) and 'token' (with a link to generate a new token). The 'Install CIS Benchmark Job' section provides a command to run, with a note that the 'clusterName' variable must be modified. A 'Back' button is located at the bottom right of the main content area.

Home > Settings > Manage Cluster > Agents

Search anything...

Cluster Onboarding

- 1 Select cluster type & enter cluster name to create cluster
 - Select Cluster Type: Kubernetes
 - Enter Cluster Name: demo
- 2 Agents Installation

Runtime Visibility & Protection

KIEM

Kubernetes CIS Benchmark

Cluster Misconfiguration

At 09:30 AM
[next scan at: 2024-12-02 09:30:00 AM](#)

At 03:00 PM
[next scan at: 2024-12-02 03:00:00 PM](#)

Prerequisites

- [helm](#) (v3.13.1 or later) [🔗](#)
- [token](#) (Click to generate a new token) [🔗](#)

Install CIS Benchmark Job

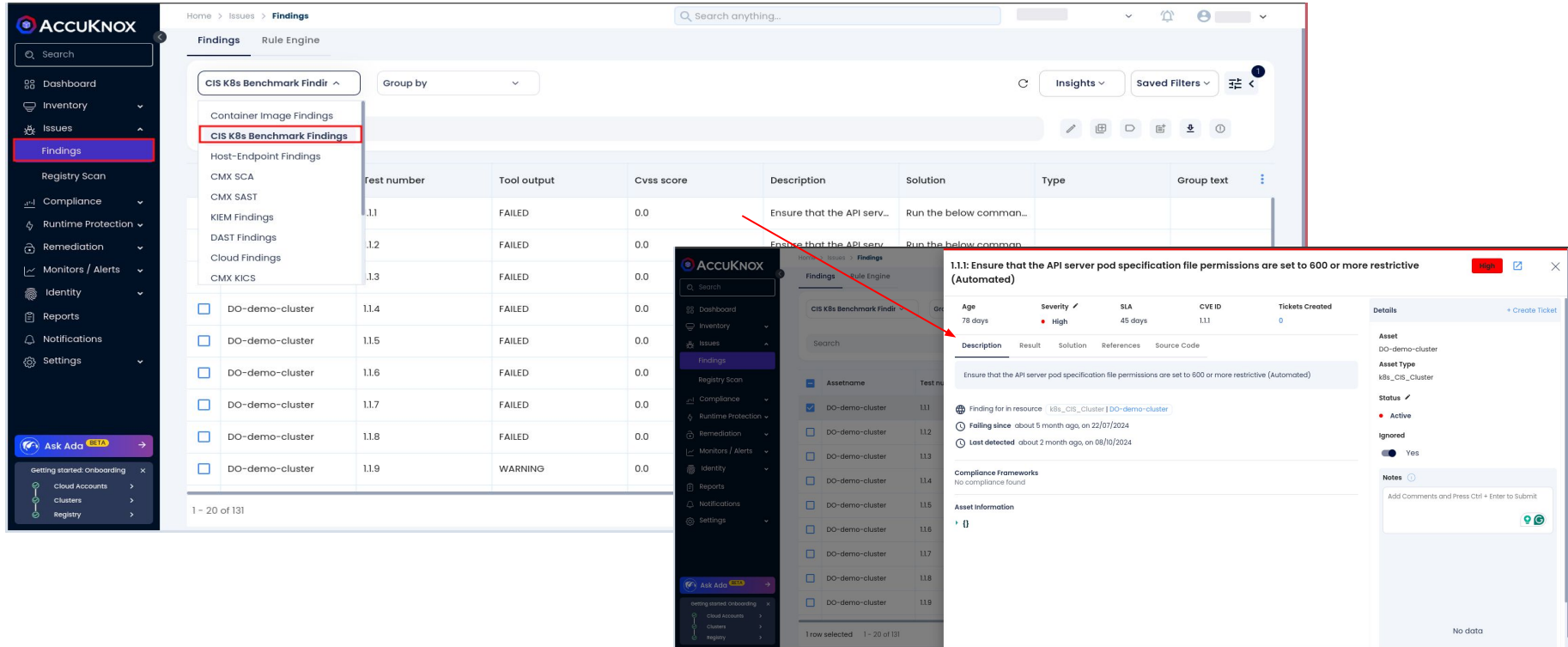
Run the following command and replace the value of token

```
1 helm upgrade --install cis-k8s-job oci://public.ecr.aws/k9v9d5v2/cis-k8s-job \
2 --set accuknox.url="cspm.demo.accuknox.com" \
3 --set accuknox.tenantId="167" \
4 --set accuknox.authToken="" \
5 --set accuknox.cronTab="30 9 * * *" \
6 --set accuknox.clusterName="demo" \
7 --version v1.1.3
```

The same Helm command has the capacity to facilitate the installation of multiple Jobs. The only variable that requires modification is the "clusterName"

Back

- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.



The screenshot displays the AccuKNOX Findings page. The left sidebar shows the navigation menu with 'Findings' highlighted. The main content area shows a list of findings under the 'CIS K8s Benchmark Findings' filter. A red box highlights the 'CIS K8s Benchmark Findings' filter in the sidebar. A red arrow points from the 'CIS K8s Benchmark Findings' filter to the detailed view of finding 1.1.1.

Test number	Tool output	Cvss score	Description	Solution	Type	Group text
1.1	FAILED	0.0	Ensure that the API serv...	Run the below comman...		
1.2	FAILED	0.0	Ensure that the API serv...	Run the below comman...		
1.3	FAILED	0.0				
1.4	FAILED	0.0				
1.5	FAILED	0.0				
1.6	FAILED	0.0				
1.7	FAILED	0.0				
1.8	FAILED	0.0				
1.9	WARNING	0.0				

1 - 20 of 131

1.1.1: Ensure that the API server pod specification file permissions are set to 600 or more restrictive (Automated)

Age: 78 days | Severity: High | SLA: 45 days | CVE ID: 1.1.1 | Tickets Created: 0

Description

Ensure that the API server pod specification file permissions are set to 600 or more restrictive (Automated)

Result

Finding for in resource: k8s_CIS_Cluster | DO-demo-cluster

Failing since: about 5 month ago, on 22/07/2024

Last detected: about 2 month ago, on 08/10/2024

Compliance Frameworks

No compliance found

Asset Information

Asset: DO-demo-cluster

Asset Type: k8s_CIS_Cluster

Status: Active

Ignored: Yes

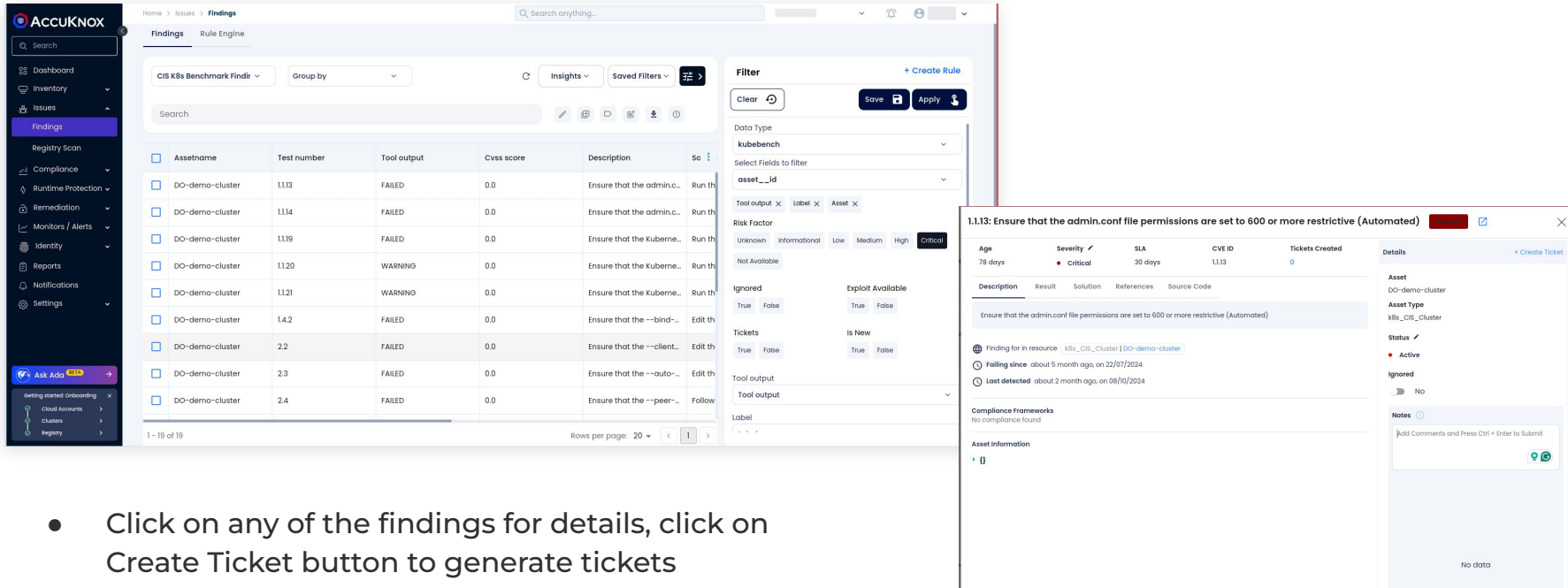
Notes

Add Comments and Press Ctrl + Enter to Submit

No data

Work on Critical Findings

- Select Group By as Findings
- In the Filters tab, select Critical under Risk Factor and click on Apply



The screenshot displays the AccuKnox Findings interface. On the left is a sidebar with navigation options: Dashboard, Inventory, Issues, Findings (selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main panel shows a table of findings under the 'Findings' tab. The table has columns for Assetname, Test number, Tool output, Cvss score, Description, and So. A filter panel on the right shows 'Risk Factor' set to 'Critical'. A detailed view of finding 1.1.13 is shown on the right, indicating it is 'Critical' and 'Automated'. The finding description is 'Ensure that the admin.conf file permissions are set to 600 or more restrictive (Automated)'. The finding is 'Active' and has been 'Failing since' about 5 months ago. A 'Create Ticket' button is visible in the top right of the detailed view.

Assetname	Test number	Tool output	Cvss score	Description	So
DO-demo-cluster	1.1.13	FAILED	0.0	Ensure that the admin.c...	Run th
DO-demo-cluster	1.1.14	FAILED	0.0	Ensure that the admin.c...	Run th
DO-demo-cluster	1.1.19	FAILED	0.0	Ensure that the Kuberne...	Run th
DO-demo-cluster	1.1.20	WARNING	0.0	Ensure that the Kuberne...	Run th
DO-demo-cluster	1.1.21	WARNING	0.0	Ensure that the Kuberne...	Run th
DO-demo-cluster	1.4.2	FAILED	0.0	Ensure that the --bind...	Edit th
DO-demo-cluster	2.2	FAILED	0.0	Ensure that the --client...	Edit th
DO-demo-cluster	2.3	FAILED	0.0	Ensure that the --auto...	Edit th
DO-demo-cluster	2.4	FAILED	0.0	Ensure that the --peer...	Follow

1.1.13: Ensure that the admin.conf file permissions are set to 600 or more restrictive (Automated)

Age: 78 days | Severity: Critical | SLA: 30 days | CVE ID: 1.1.13 | Tickets Created: 0

Description: Ensure that the admin.conf file permissions are set to 600 or more restrictive (Automated)

Asset: DO-demo-cluster | Asset Type: k8s_CIS_cluster | Status: Active

Finding for in resource: k8s_CIS_Cluster | DO-demo-cluster

Failing since: about 5 months ago, on 22/07/2024

Last detected: about 2 months ago, on 08/10/2024

Compliance Frameworks: No compliance found

Asset Information: No data

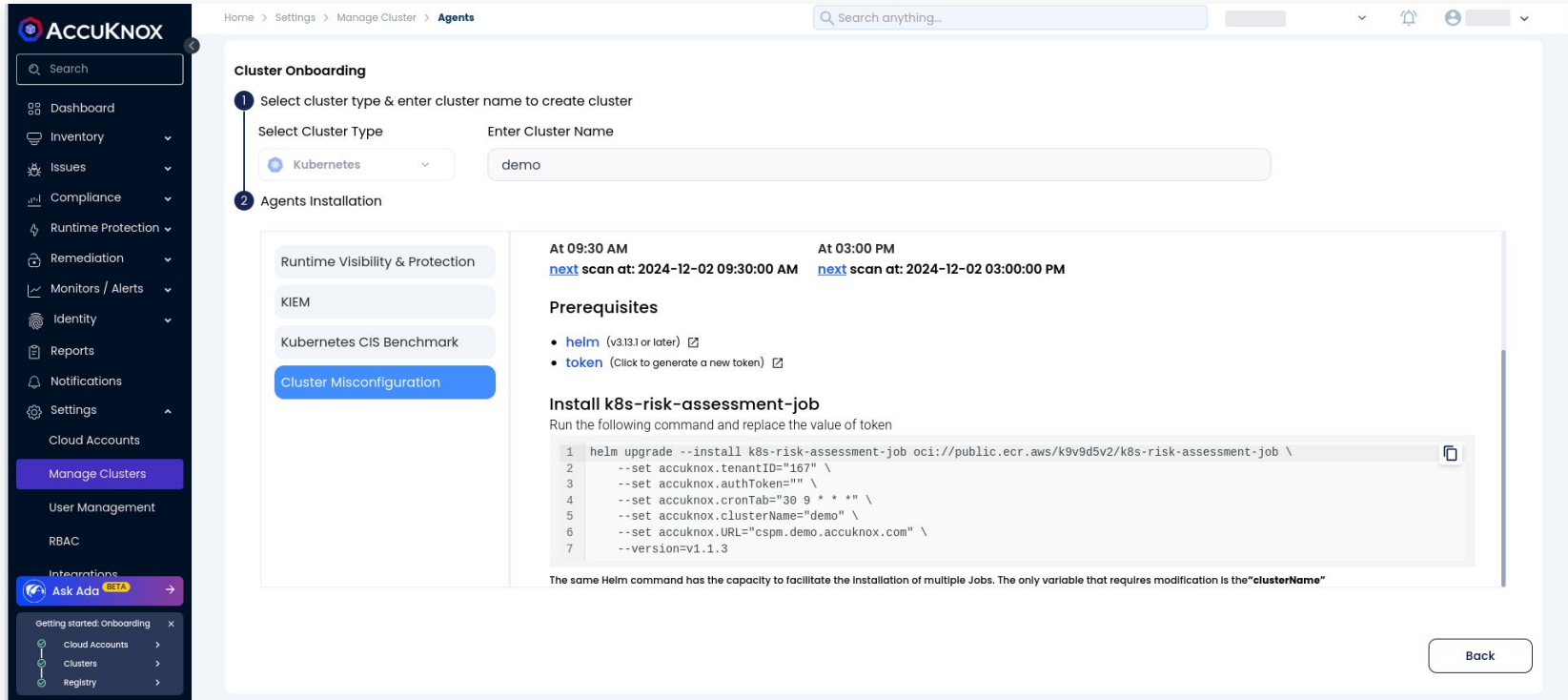
- Click on any of the findings for details, click on Create Ticket button to generate tickets



Cluster Misconfiguration

Cluster Misconfiguration (Agentless)

- Navigate to **Settings**, choose the onboarded cluster, and select **Cluster Misconfiguration**.
- Install the helm chart using the commands displayed on the screen.



The screenshot displays the AccuKNOX web interface. On the left is a dark sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters (highlighted), User Management, RBAC, and Integrations. The main content area is titled 'Cluster Onboarding' and shows two steps: 1. Select cluster type & enter cluster name to create cluster, and 2. Agents Installation. Under step 1, 'Kubernetes' is selected as the cluster type, and 'demo' is entered as the cluster name. Under step 2, 'Cluster Misconfiguration' is selected from a list of options. The page also shows scan times for 'next scan at: 2024-12-02 09:30:00 AM' and 'next scan at: 2024-12-02 03:00:00 PM'. A 'Prerequisites' section lists 'helm (v3.13.1 or later)' and 'token (Click to generate a new token)'. An 'Install k8s-risk-assessment-job' section provides a Helm command to run. A 'Back' button is located at the bottom right.

Home > Settings > Manage Cluster > Agents

Search anything...

Cluster Onboarding

- 1 Select cluster type & enter cluster name to create cluster
- 2 Agents Installation

Select Cluster Type: Kubernetes

Enter Cluster Name: demo

Runtime Visibility & Protection

KIEM

Kubernetes CIS Benchmark

Cluster Misconfiguration

At 09:30 AM
next scan at: 2024-12-02 09:30:00 AM

At 03:00 PM
next scan at: 2024-12-02 03:00:00 PM

Prerequisites

- [helm](#) (v3.13.1 or later) [🔗](#)
- [token](#) (Click to generate a new token) [🔗](#)

Install k8s-risk-assessment-job

Run the following command and replace the value of token

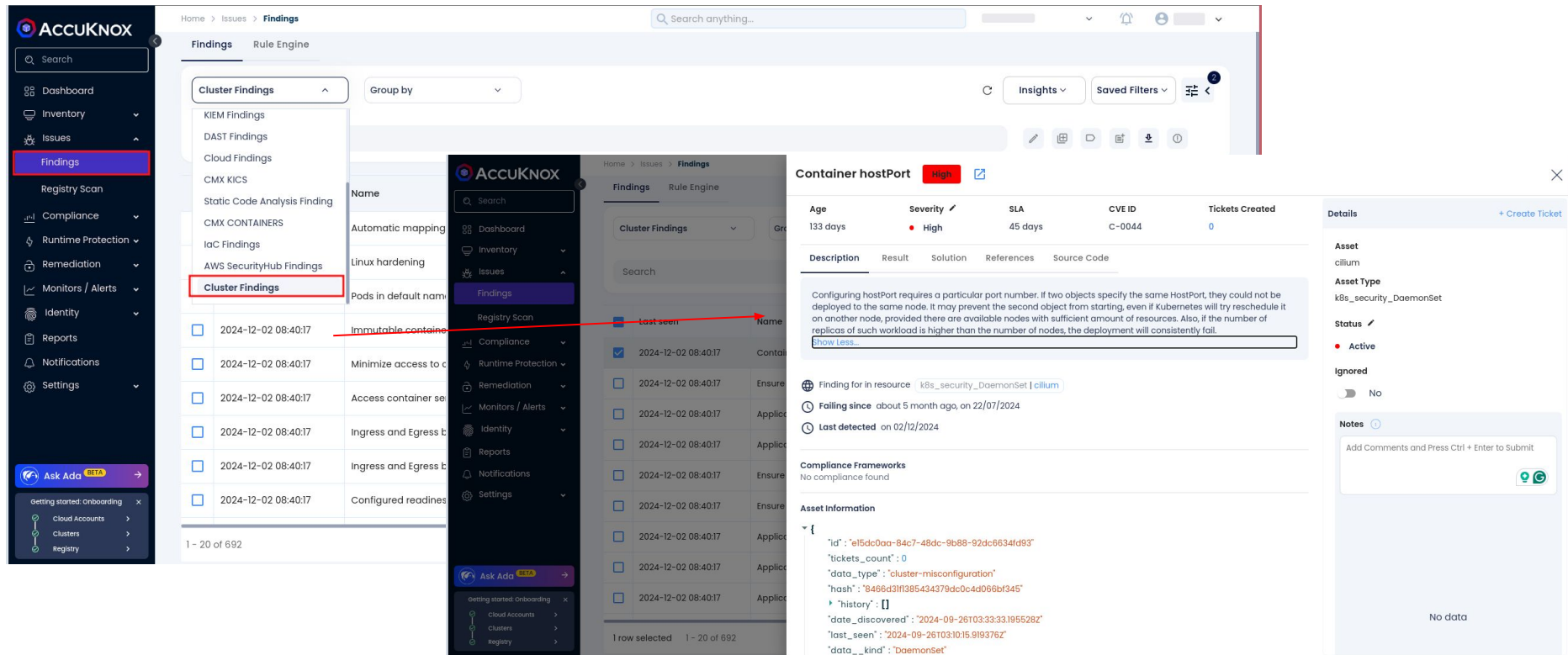
```
1 helm upgrade --install k8s-risk-assessment-job oci://public.ecr.aws/k9v9d5v2/k8s-risk-assessment-job \
2 --set accuknox.tenantID="167" \
3 --set accuknox.authToken="" \
4 --set accuknox.cronTab="30 9 * * *" \
5 --set accuknox.clusterName="demo" \
6 --set accuknox.URL="cspm.demo.accuknox.com" \
7 --version=v1.1.3
```

The same Helm command has the capacity to facilitate the installation of multiple Jobs. The only variable that requires modification is the "clusterName"

Back

View Findings

- View the findings on the **Findings** page. Select the **CIS k8s Benchmark Findings** to access the relevant details.



The screenshot displays the AccuKNOX interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below these is an 'Ask Ada' button and a 'Getting started: onboarding' section with links to Cloud Accounts, Clusters, and Registry.

The main content area is titled 'Findings' and includes a search bar and filters. A dropdown menu for 'Cluster Findings' is open, showing various finding categories. The 'Findings' list table has columns for Name, Age, Severity, SLA, CVE ID, Tickets Created, and Details. A finding titled 'Container hostPort' with a 'High' severity is selected. A red arrow points from the 'Cluster Findings' dropdown to this finding.

The detailed view for the 'Container hostPort' finding shows the following information:

- Age:** 133 days
- Severity:** High
- SLA:** 45 days
- CVE ID:** C-0044
- Tickets Created:** 0

Description: Configuring hostPort requires a particular port number. If two objects specify the same hostPort, they could not be deployed to the same node. It may prevent the second object from starting, even if Kubernetes will try reschedule it on another node, provided there are available nodes with sufficient amount of resources. Also, if the number of replicas of such workload is higher than the number of nodes, the deployment will consistently fail.

Compliance Frameworks: No compliance found

Asset Information:

```
{
  "id": "e15dc0aa-84c7-48dc-9b88-92dc6634fd93"
  "tickets_count": 0
  "data_type": "cluster-misconfiguration"
  "hash": "8466d31f385434379dc0c4d066bf345"
  "history": []
  "date_discovered": "2024-09-26T03:33:195528Z"
  "last_seen": "2024-09-26T03:10:15.919376Z"
  "data_kind": "DaemonSet"
}
```

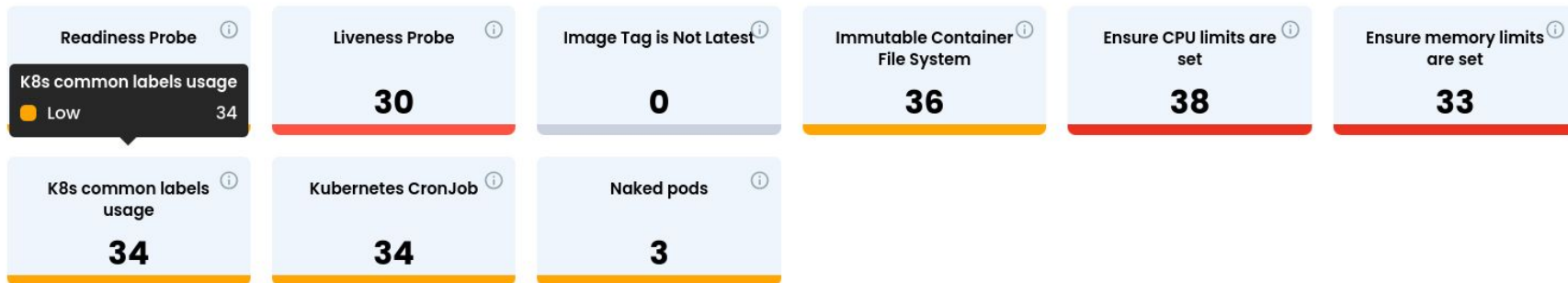
Details: Asset: cilium, Asset Type: k8s_security_DaemonSet, Status: Active, Ignored: No. Notes: Add Comments and Press Ctrl + Enter to Submit.



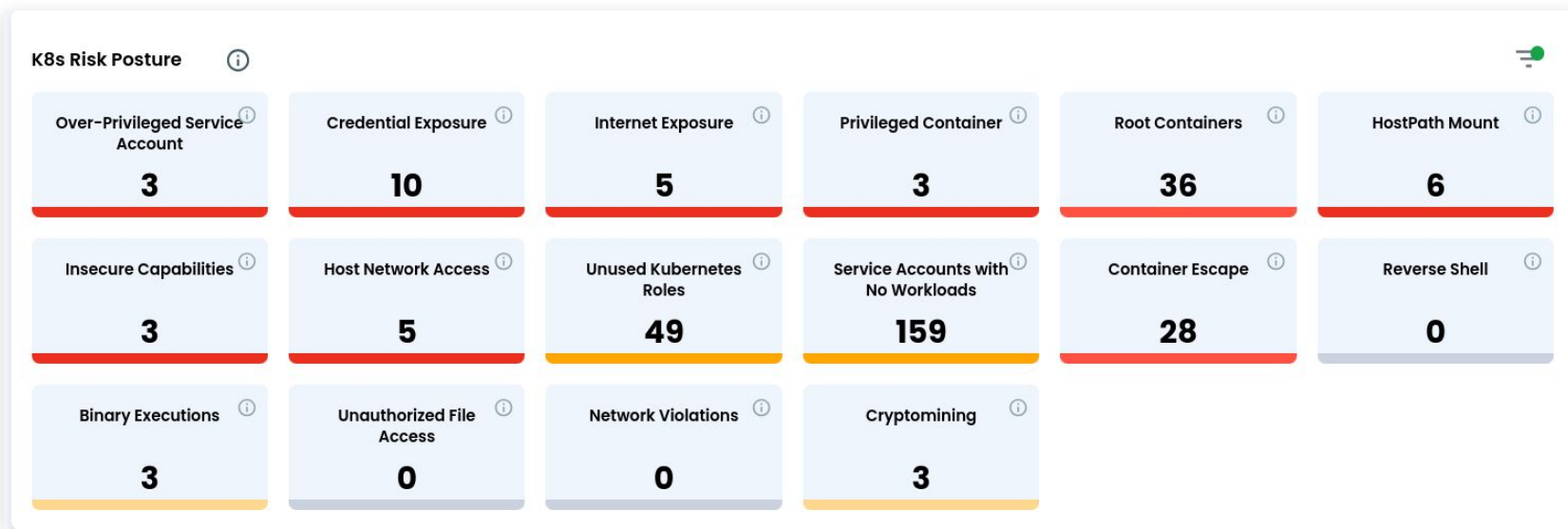
KSPM Customized Dashboard & Reporting Metrics

Resource Metrics Widgets [1]

K8s Resource Summary ⓘ

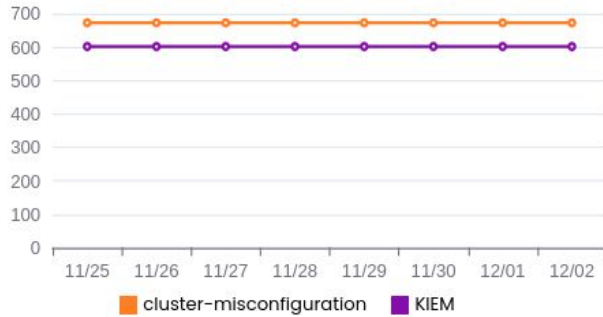


Security Risk Metrics Widgets [2]

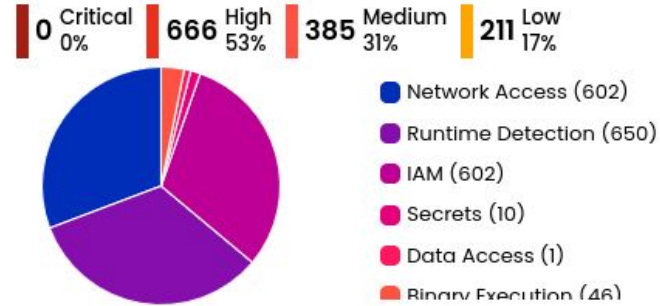


K8s Risk Overview - Widgets [3]

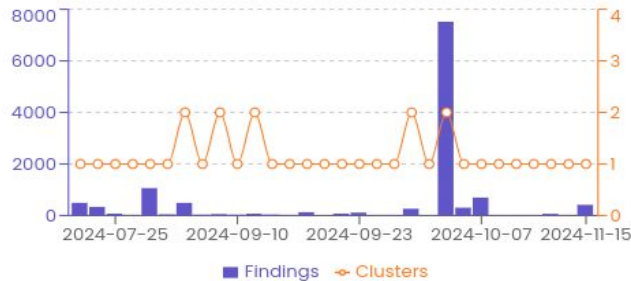
K8s Findings Trend



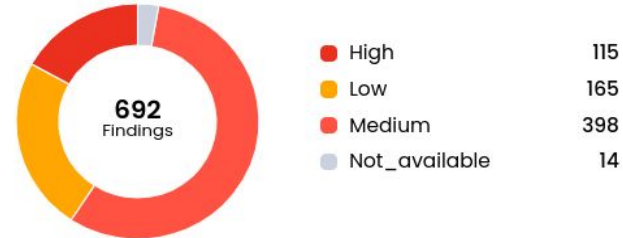
K8s Open Findings



New Cluster Findings Trend



Cluster Findings Summary by Severity



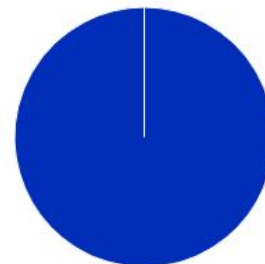
Cluster Wide Risk - Widgets [4]

Clusters with Public Exposure ⓘ



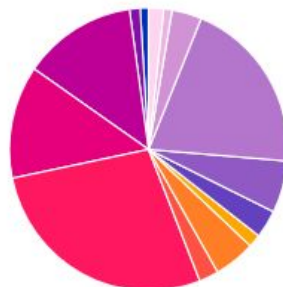
aws-stage-ka...	8.2K
aws-stage-ka...	16.4M
mongo-test-02	163.6K
DO-demo-clust...	1.7M

Privileged Containers by Clusters ⓘ



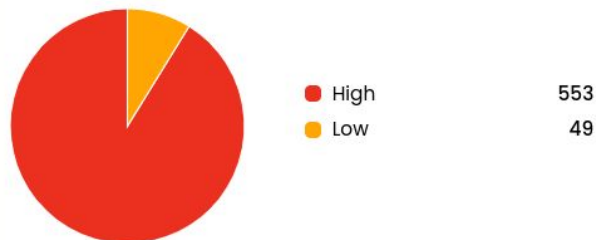
DO-demo-clust...	3
------------------	---

Cluster Findings by Asset Type ⓘ

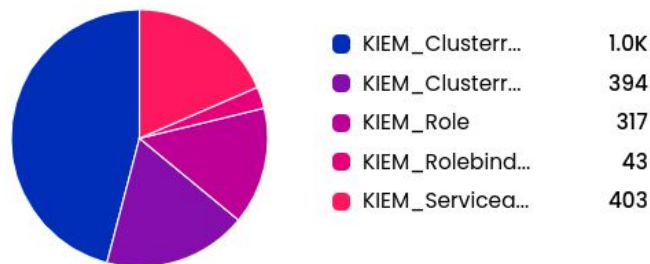


k8s_security_...	1
k8s_security_...	3
k8s_security_...	94
k8s_security_...	92
k8s_security_...	205
k8s_security_...	11

KIEM Risk Assessment



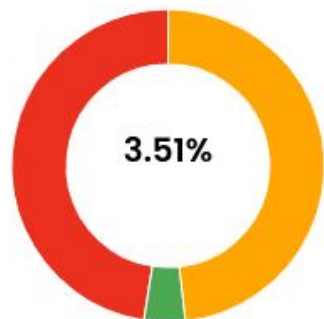
KIEM Findings by Asset Types



Top 5 Most Critical Findings

Permission to access different namespace	227
Service accounts with no workloads	159
Permission to Delete and Access ConfigMaps,PersistentVolumeClaims	71
Permission to modify workloads	32
Permission to read/list Secrets	27

K8s CIS Compliance Status



Total Count
570

- FAILED
- PASSED
- WARNING

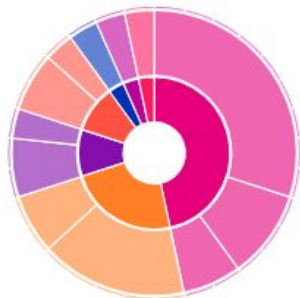
273
20
277

Top 5 K8s CIS Findings

Finding Name	Assets Impacted
● 2.5: Ensure that the --peer-client-cert-auth arg...	5
● 2.4: Ensure that the --peer-cert-file and --peer...	5
● 2.3: Ensure that the --auto-tls argument is not s...	5
● 2.2: Ensure that the --client-cert-auth argumen...	5
● 1.4.2: Ensure that the --bind-address argument ...	5

Container Specific Risk - Widgets [7]

Privileged Containers



- do-demo-cluster
- gke-k8s-misconfig
- insecure-scan
- insecure-cis-validation

[Go to All Findings >](#)

Top 5 K8s External Egress/Ingress Workloads

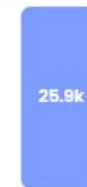


492066 Total External

Connections

Ingress 99.4 %

Egress 0.6 %



184.3k

103.6k

103.9k

71.4k

25.9k

deploye...

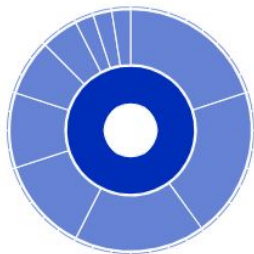
deploye...

deploye...

deploye...

deploye...

Workloads without Network Policies



- do-demo-cluster

[Go to Findings >](#)

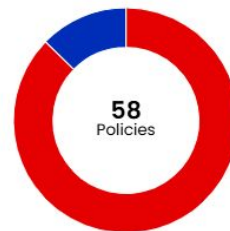
Privileged Containers



- do-demo-cluster

[Go to All Findings >](#)

Workloads Without Any Policy Applied



- Applied
- Not Applied

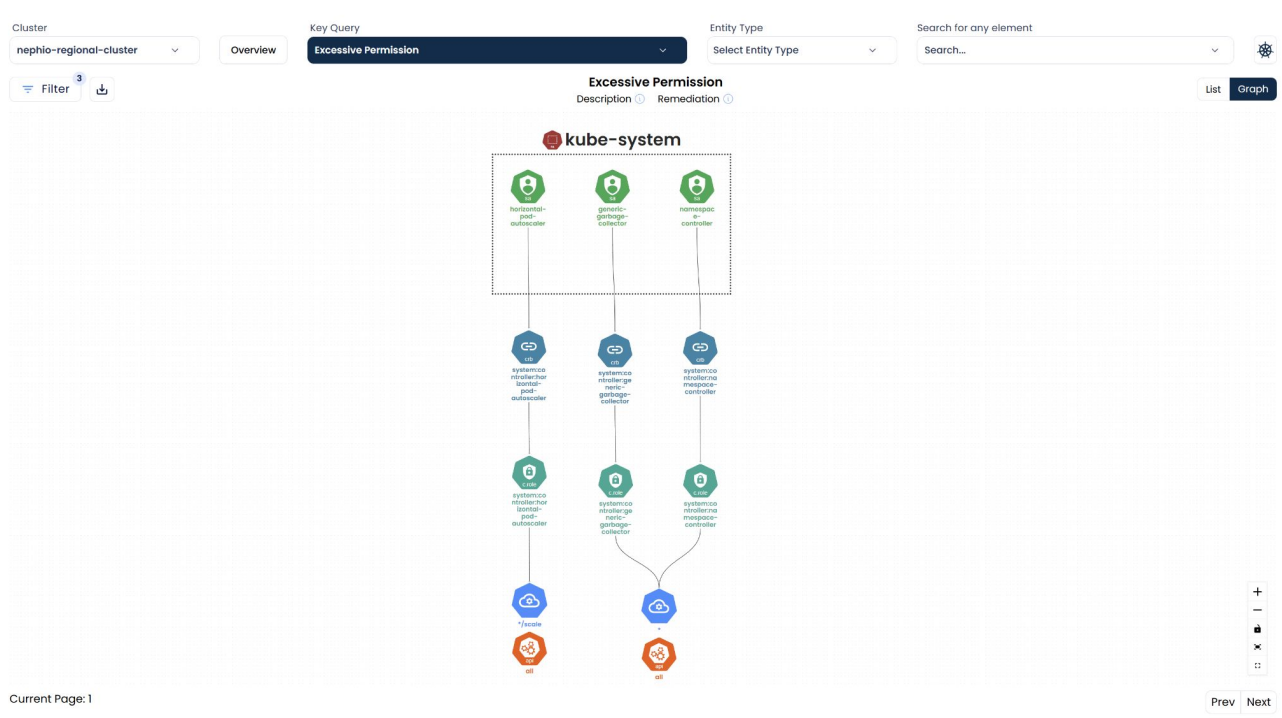
7

51



KSPM Use Cases

- A Kubernetes service account or role has excessive permissions, increasing the risk of privilege escalation.



- **AccuKnox recommends** minimizing permissions by enforcing least privilege, avoiding wildcards, restricting namespaces, and using RBAC with narrowly defined roles.

Cluster
DO-demo-cluster

Overview

Key Query
Excessive Permission

Entity Type
Select Entity Type










Search for any element
Search...

Filter 3

Download

Excessive Permission
Description Remediation

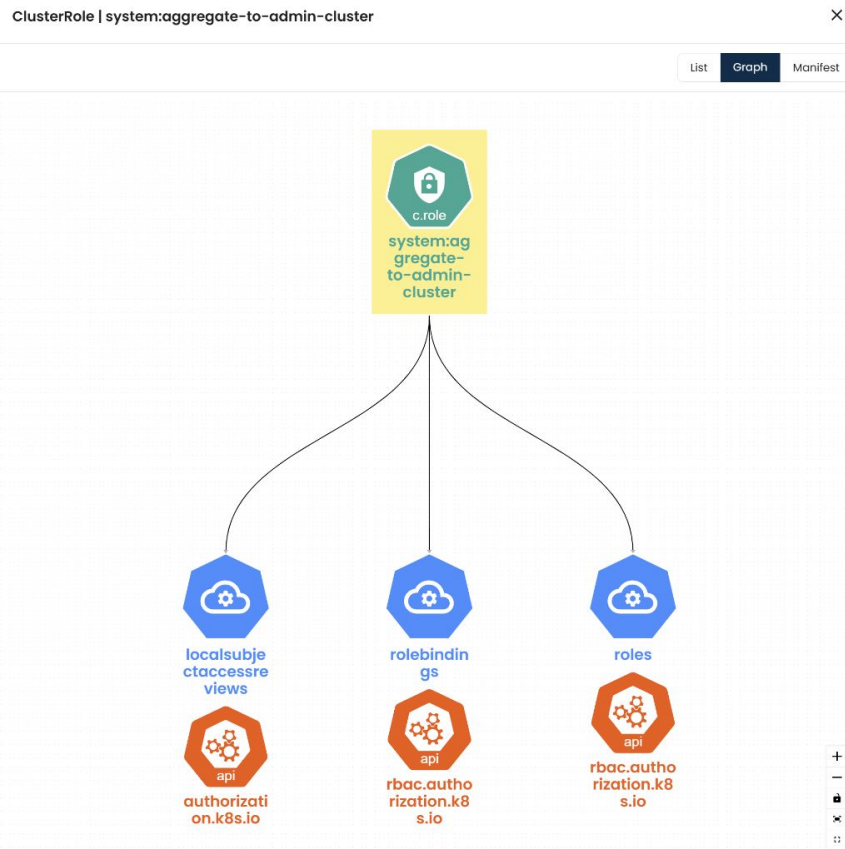
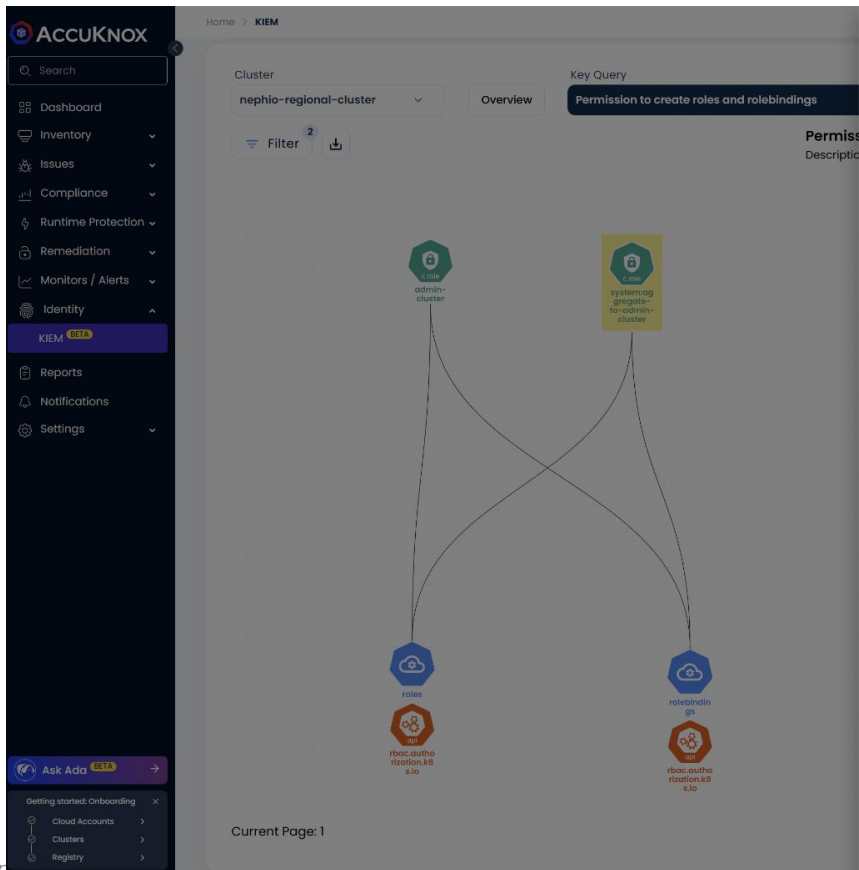
List Graph

Subject	RoleBinding	Role	Rule			Workload
			Verb	Resource	ApiGroup	
 namespace-controller Scope: kube-system	 system:controller:namespace-controller Scope: cluster_wide	 system:controller:namespace-controller Scope: cluster_wide	delete, deletecollection, get, list	*	all	-
 horizontal-pod-autoscaler Scope: kube-system	 system:controller:horizontal-pod-autoscaler Scope: cluster_wide	 system:controller:horizontal-pod-autoscaler Scope: cluster_wide	get, update	*/scale	all	-
 generic-garbage-collector Scope: kube-system	 system:controller:generic-garbage-collector Scope: cluster_wide	 system:controller:generic-garbage-collector Scope: cluster_wide	delete, get, list, patch, update, watch	*	all	-

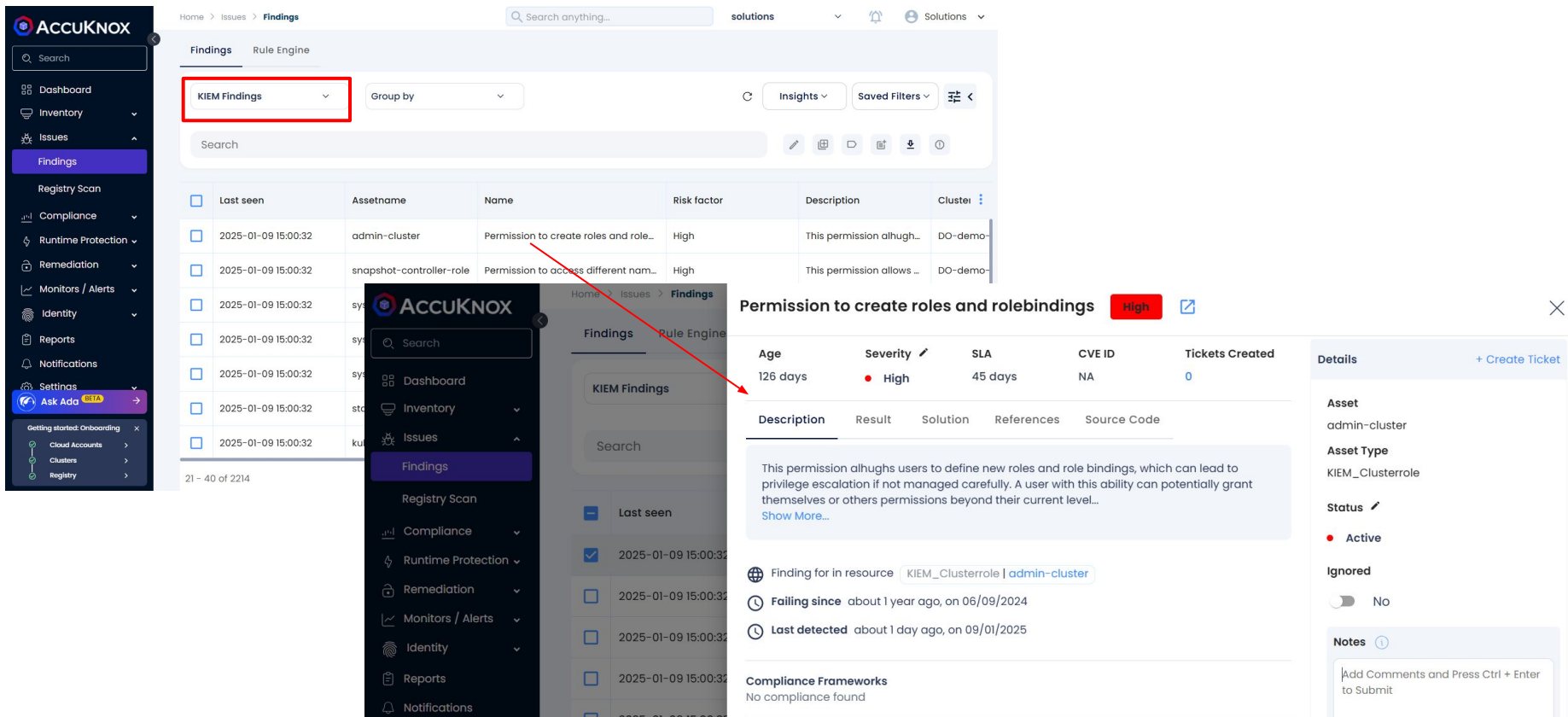
Current Page: 1

Prev Next

KIEM: Permission to create Roles & RoleBindings



KIEM: Track KIEM findings identified by filters



The screenshot displays the AccuKNOX interface with the 'Findings' tab selected. A red box highlights the 'KIEM Findings' filter in the top navigation bar. A red arrow points from this filter to a detailed view of a finding titled 'Permission to create roles and rolebindings'.

Findings Table:

Last seen	Assetname	Name	Risk factor	Description	Cluster
2025-01-09 15:00:32	admin-cluster	Permission to create roles and role...	High	This permission althugh...	DO-demo
2025-01-09 15:00:32	snapshot-controller-role	Permission to access different nam...	High	This permission allows ...	DO-demo

Permission to create roles and rolebindings High

Details:

- Age:** 126 days
- Severity:** High
- SLA:** 45 days
- CVE ID:** NA
- Tickets Created:** 0

Description: This permission althugh users to define new roles and role bindings, which can lead to privilege escalation if not managed carefully. A user with this ability can potentially grant themselves or others permissions beyond their current level...

Finding for in resource: KIEM_Clusterrole | admin-cluster

Failing since: about 1 year ago, on 06/09/2024

Last detected: about 1 day ago, on 09/01/2025

Compliance Frameworks: No compliance found

Asset: admin-cluster

Asset Type: KIEM_Clusterrole


Status: Active

Ignored: No

Notes: Add Comments and Press Ctrl + Enter to Submit

- Ensure etcd data directory permissions are set to 700 or more restrictive.
- AccuKnox identifies the vulnerability and proposes a solution.

1.1.11: Ensure that the etcd data directory permissions are set to 700 or more restrictive (Automated) High

Age	Severity 	SLA	CVE ID	Tickets Created
78 days	High	45 days	1.1.11	0

Description

Result

Solution

References

Source Code

On the etcd server node, get the etcd data directory, passed as an argument --data-dir, from the command 'ps -ef | grep etcd'.
Run the below command (based on the etcd data directory found above). For example, `chmod 700 /var/lib/etcd`


Details [+ Create Ticket](#)

Asset

DO-demo-cluster

Asset Type


k8s_CIS_Cluster

Status 



Active

Ignored

☐ No

Notes 

Add Comments and Press Ctrl + Enter to Submit

Cluster Misconfig Use Case: Anonymous Access Enabled



- Enabling anonymous access exposes the cluster to unauthorized access.
- **AccuKnox recommends:** Review and adjust your cluster's RBAC to ensure only authenticated, authorized users have the appropriate permissions.

Anonymous access enabled

High

Age

133 days

Severity

High

SLA

45 days

CVE ID

C-0262

Tickets Created

0

Description

Result

Solution

References

Source Code

Granting permissions to the system:unauthenticated or system:anonymous user is generally not recommended and can introduce security risks. Allowing unauthenticated access to your Kubernetes cluster can lead to unauthorized access, potential...

Show More...

Finding for in resource

k8s_security_ClusterRoleBinding | system:public-info-viewer

Failing since

about 5 month ago, on 22/07/2024

Last detected

on 02/12/2024

Compliance Frameworks

No compliance found

Asset Information

```
{
  "id": "a5786576-44b2-4005-ae70-525ded44d090"
  "tickets_count": 0
  "data_type": "cluster-misconfiguration"
  "hash": "8012037be364cd54735e347b65c888e8"
  "history": []
  "date_discovered": "2024-09-14T03:10:14.578184Z"
  "last_seen": "2024-09-26T03:10:15.919376Z"
  "data__kind": "ClusterRoleBinding"
  "data__roleRef": {
    "kind": "ClusterRole"
    "name": "system:public-info-viewer"
    "apiGroup": "rbac.authorization.k8s.io"
  }
}
```

Details

+ Create Ticket

Asset

system:public-info-viewer

Asset Type

k8s_security_ClusterRoleBinding

Status

Active

Ignored

No

Notes

No data