



# 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.

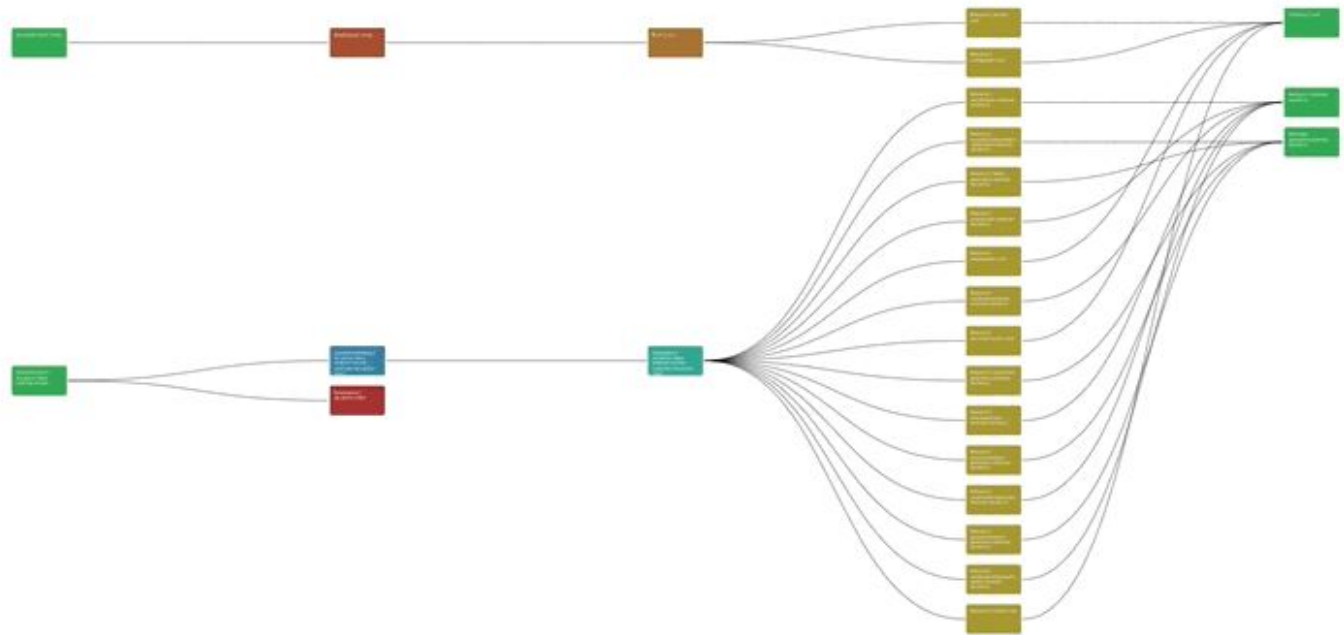


**KIEM**

General Filter ☰

Save Current State

128 Principals with privileges on all resources



WhoCan

Key Queries

Entity Types

General Fi

Default

Service accounts with no workloads

Principals with high privileges

Anonymous/unauthenticated users/groups

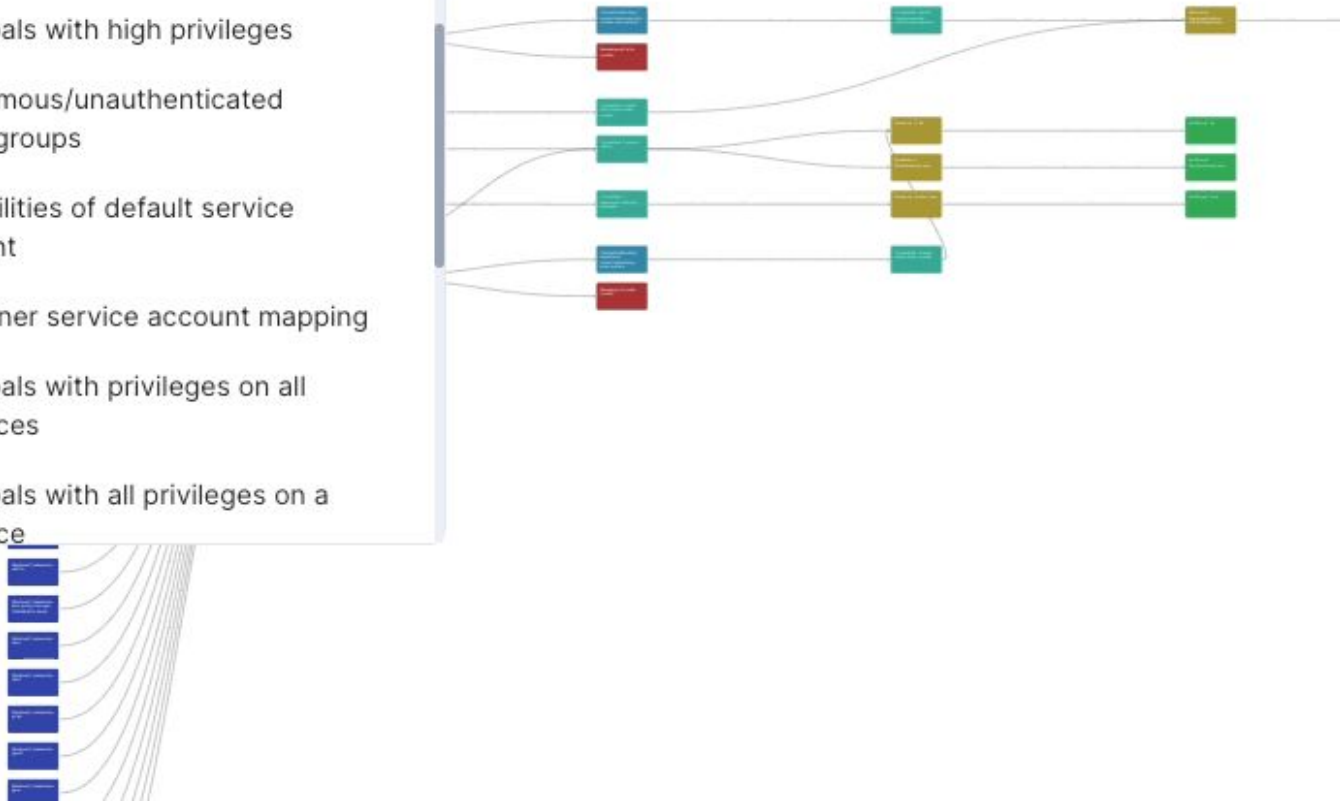
Capabilities of default service account

Container service account mapping

Principals with privileges on all resources

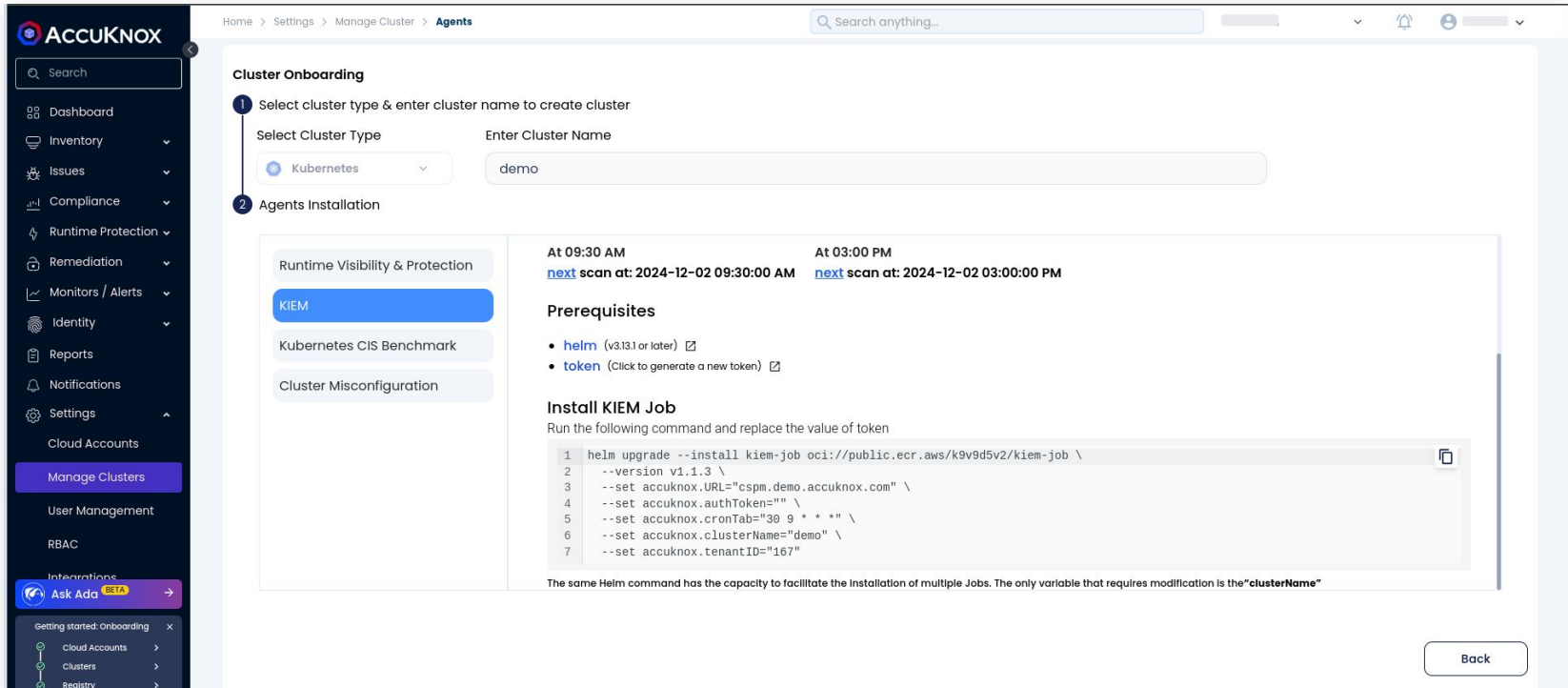
Principals with all privileges on a resource

105 Principals with high privileges





- 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 for cluster onboarding. The left sidebar contains navigation options: 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 indicator 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, "KIEM" is selected as the agent type. The interface also shows a scan history table with columns for time and scan status. Below this, there are sections for "Prerequisites" (helm and token) and "Install KIEM Job" with a code block containing the following command:

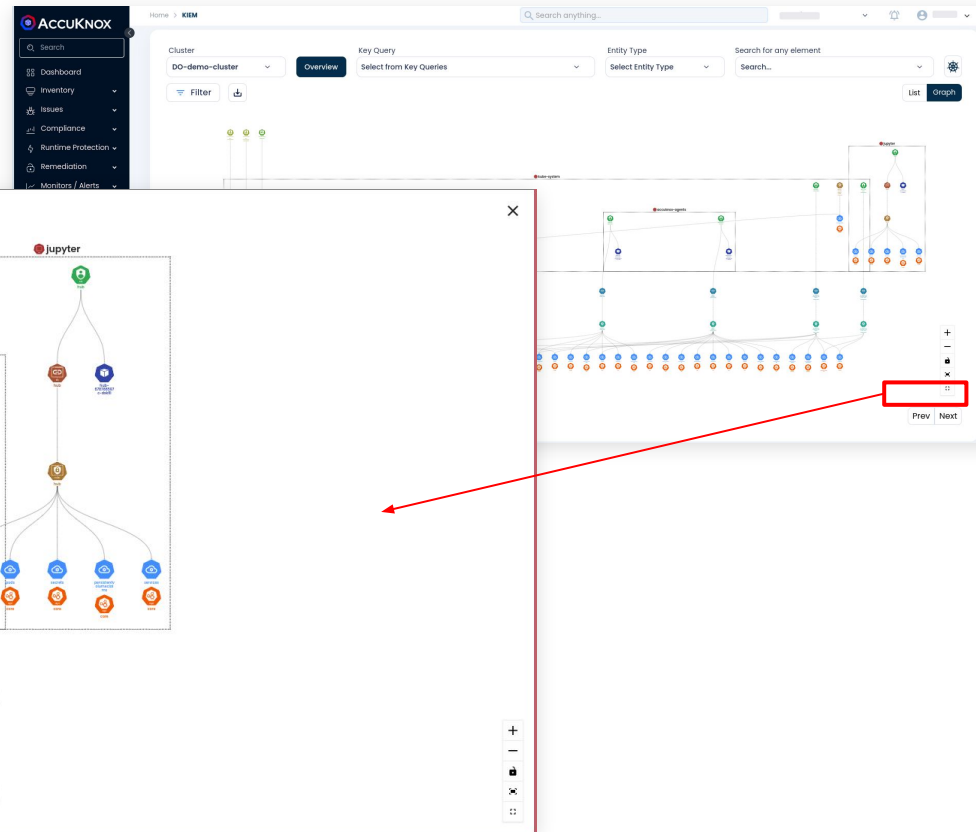
```
1 helm upgrade --install kiem-job oci://public.ecr.aws/k9v9d5v2/kiem-job \
2 --version v1.1.3 \
3 --set accuknox.URL="cspm.demo.accuknox.com" \
4 --set accuknox.authToken="" \
5 --set accuknox.cronTab="30 9 * * *" \
6 --set accuknox.clusterName="demo" \
7 --set accuknox.tenantID="167"
```

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

A "Back" button is located at the bottom right of the main content area.

# 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.

The screenshot displays the ACCUKNOX interface for the KIEM List View. The left sidebar contains navigation options: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, KIEM (highlighted in blue), Reports, Notifications, and Settings. The main content area shows a table of RoleBinding entries for the cluster 'DO-demo-cluster'. The table has columns for Subject, RoleBinding, Role, Verb, Rule Resource, and Rule ApiGroup. The first entry is for the 'kubearmor-operator' with a scope of 'kubearmor'. It lists various verbs and resources such as 'kubearmorhostpolicies', 'kubearmorclusterpolicies', 'deployments', 'kubearmorpolicies', 'nodes', '/apis', 'jobs', 'daemonsets', and 'namespaces'. The interface includes filters for Cluster, Key Query, and Entity Type, along with a search bar and pagination controls.

Subject	RoleBinding	Role	Rule		
			Verb	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

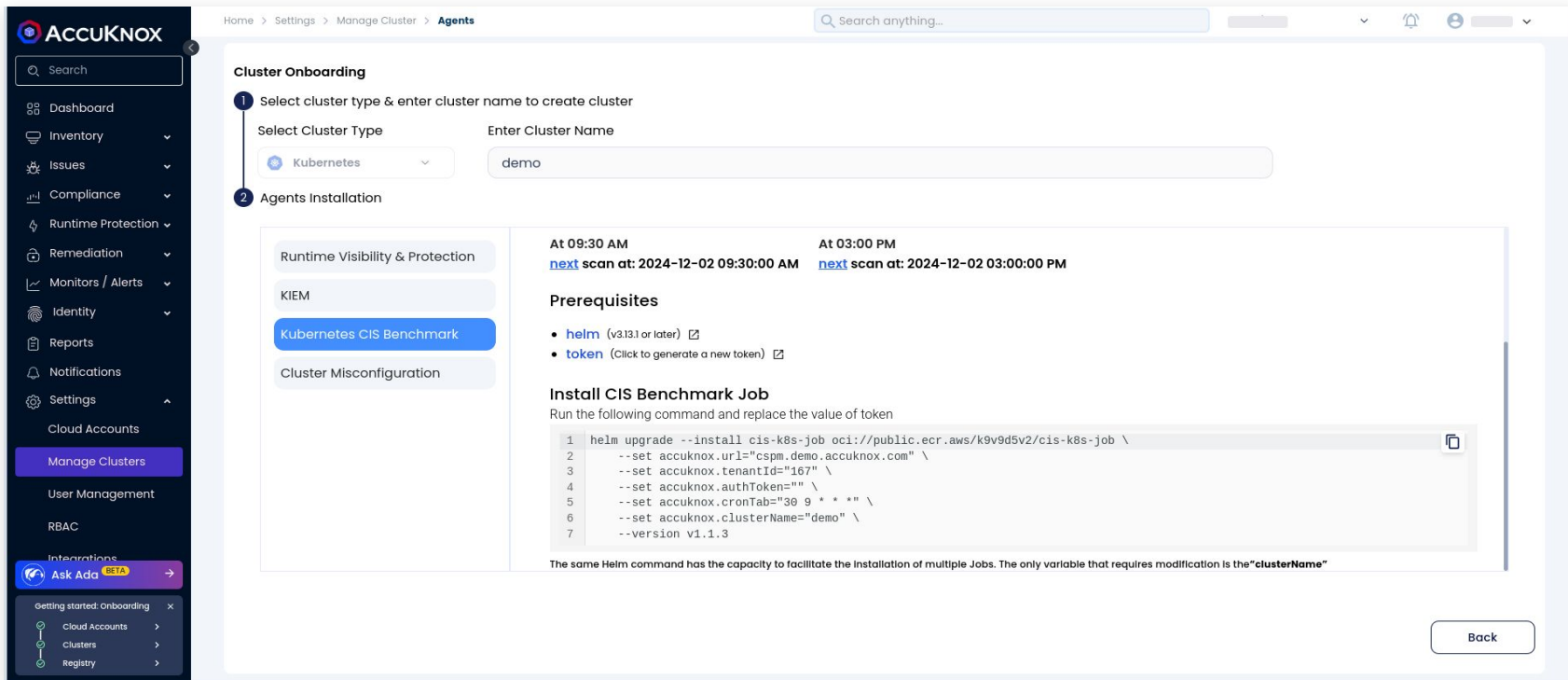




# Kubernetes CIS Benchmark

# 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 for configuring and installing the Kubernetes CIS Benchmark. The interface is divided into a left sidebar and a main content area.

**Left Sidebar:** Contains navigation options such as Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters (highlighted), User Management, RBAC, and Integrations (including Ask Ada BETA).

**Main Content Area:**

- Cluster Onboarding:** Shows a progress indicator with two steps: 1. Select cluster type & enter cluster name to create cluster, and 2. Agents Installation.
- Select Cluster Type:** A dropdown menu is set to "Kubernetes".
- Enter Cluster Name:** A text input field contains the value "demo".
- Configuration Options:** A list of options includes Runtime Visibility & Protection, KIEM, **Kubernetes CIS Benchmark** (highlighted in blue), and Cluster Misconfiguration.
- Timeline:** Shows two scan events: "At 09:30 AM" and "At 03:00 PM", both with a "next scan at: 2024-12-02 09:30:00 AM" and "2024-12-02 03:00:00 PM" respectively.
- Prerequisites:** Lists requirements for helm (v3.13.1 or later) and token (with a link to generate a new token).
- Install CIS Benchmark Job:** Instructs to run a command and replace the value of token. A code block shows the following command:

```
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
```
- Additional Info:** A note states: "The same Helm command has the capacity to facilitate the installation of multiple Jobs. The only variable that requires modification is the 'clusterName'".
- Buttons:** A "Back" button is located at the bottom right of the main content area.

- 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 table lists findings with columns for Test number, Tool output, Cvs score, Description, Solution, Type, and Group text. Finding 1.1.1 is highlighted, and a detailed view is shown on the right. The detailed view includes fields for Age (78 days), Severity (High), SLA (45 days), CVE ID (1.1.1), and Tickets Created (0). The description states: 'Ensure that the API server pod specification file permissions are set to 600 or more restrictive (Automated)'. The status is 'Active' and it was last detected on 08/10/2024.

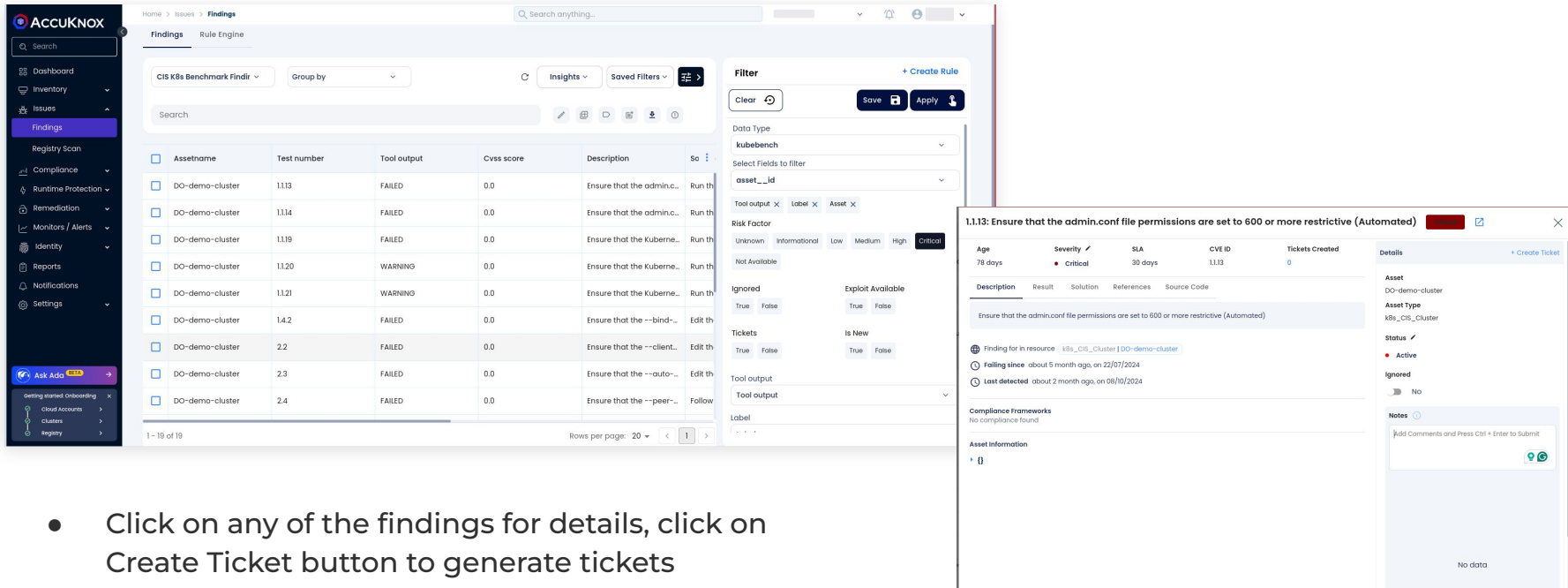
Test number	Tool output	Cvs score	Description	Solution	Type	Group text
1.1	FAILED	0.0	Ensure that the API serv...	Run the below comman...		
1.2	FAILED	0.0	Ensure that the API serv...	Run the below comman...		
1.3	FAILED	0.0				
1.4	FAILED	0.0				
1.5	FAILED	0.0				
1.6	FAILED	0.0				
1.7	FAILED	0.0	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

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

Description	Result	Solution	References	Source Code
Ensure that the API server pod specification file permissions are set to 600 or more restrictive (Automated)				

# 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. The main view shows a table of findings with columns for Assetname, Test number, Tool output, Cvs score, and Description. A filter panel on the right is open, showing the Risk Factor set to Critical. A modal window is open for finding 1.1.13, showing details such as Age (78 days), Severity (critical), SLA (30 days), CVE ID (1.1.13), and Tickets Created (0). The modal also includes a 'Create Ticket' button and a 'Details' section with asset information and notes.

Assetname	Test number	Tool output	Cvs score	Description	So
DO-demo-cluster	1113	FAILED	0.0	Ensure that the admin...	Run th
DO-demo-cluster	1114	FAILED	0.0	Ensure that the admin...	Run th
DO-demo-cluster	1119	FAILED	0.0	Ensure that the Kuber...	Run th
DO-demo-cluster	1120	WARNING	0.0	Ensure that the Kuber...	Run th
DO-demo-cluster	1121	WARNING	0.0	Ensure that the Kuber...	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	Severity	SLA	CVE ID	Tickets Created
78 days	critical	30 days	1.1.13	0

**Description** Result Solution References Source Code

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

⚙ Finding for in resource k8s\_cis\_cluster | DO-demo-cluster

- 🕒 **Falling since** about 5 month ago, on 22/07/2024
- 🕒 **Last detected** about 2 month ago, on 08/10/2024

**Tool output**

Tool output

**Compliance Frameworks**

No compliance found

**Asset Information**

1

**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

No data

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

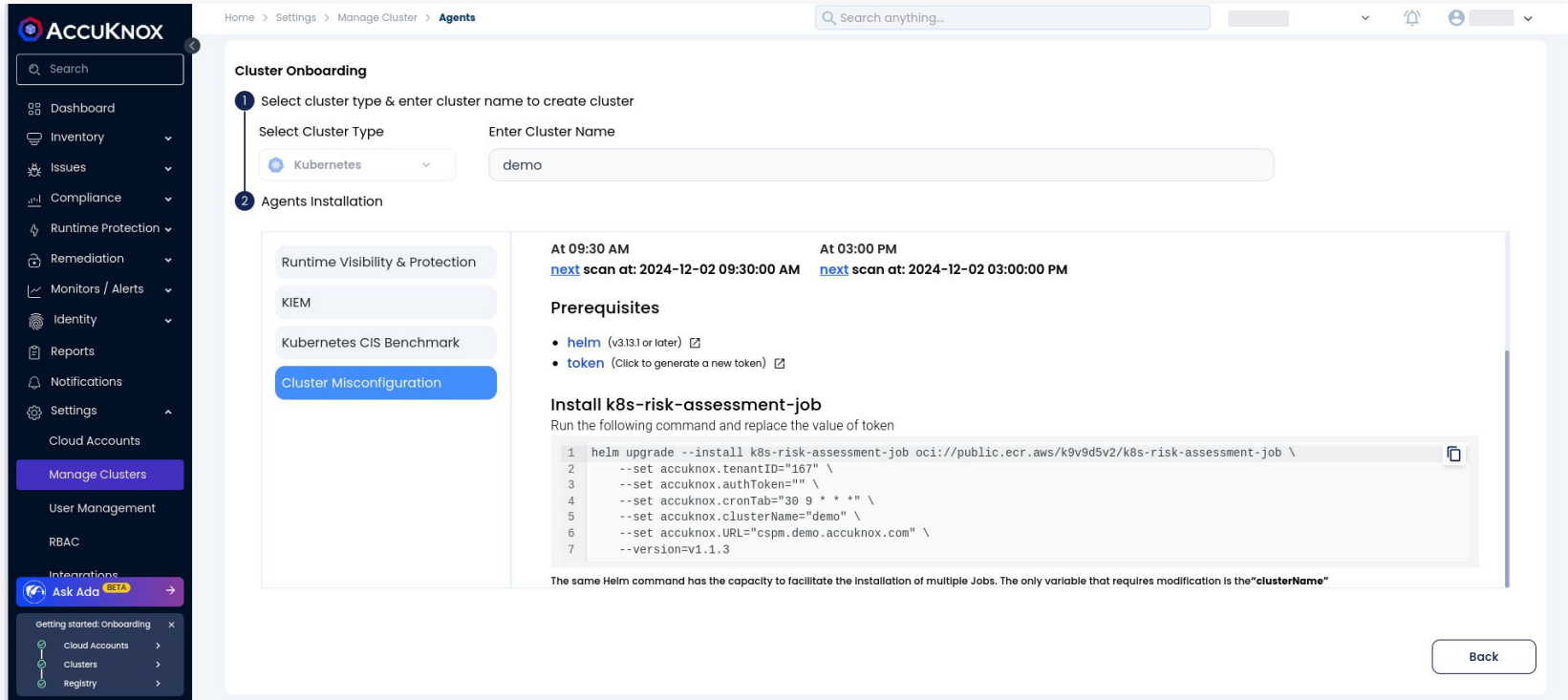




# Cluster Misconfiguration

# 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 shows the AccuKnox web interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters, User Management, RBAC, and Integrations. The main content area is titled 'Cluster Onboarding' and shows a progress indicator 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, 'Cluster Misconfiguration' is selected in a list of options. To the right, there are scan times: 'At 09:30 AM next scan at: 2024-12-02 09:30:00 AM' and 'At 03:00 PM next scan at: 2024-12-02 03:00:00 PM'. 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 k8s-risk-assessment-job' section provides a terminal command to run. 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 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 shows the AccuKnox interface. On the left is a navigation sidebar with 'Findings' highlighted. The main area is titled 'Findings' and shows a list of findings under 'Cluster Findings'. A red box highlights 'Cluster Findings' in the dropdown menu. A red arrow points from this menu item to a specific finding in the table: 'Container hostPort' with a severity of 'High'. The detailed view of this finding is shown on the right, including its description, compliance frameworks, and asset information.

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

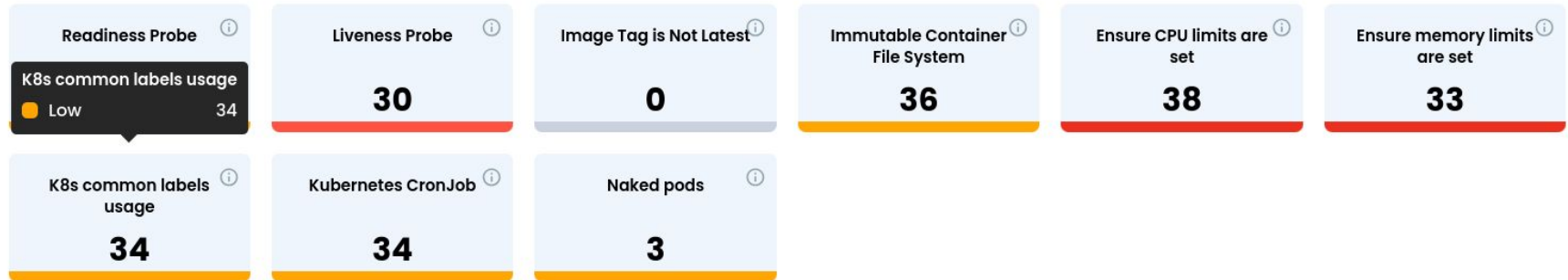
**Asset Information**

```
{
  "id": "e15dc0aa-84c7-48dc-9b88-92dc6634fd93"
  "tickets_count": 0
  "data_type": "cluster-misconfiguration"
  "hash": "8466d3f1f385434379dc0c4d066bf345"
  "history": []
  "date_discovered": "2024-09-26103:33.33.1955282"
  "last_seen": "2024-09-26103:10.15.919376Z"
  "data_kind": "DaemonSet"
}
```

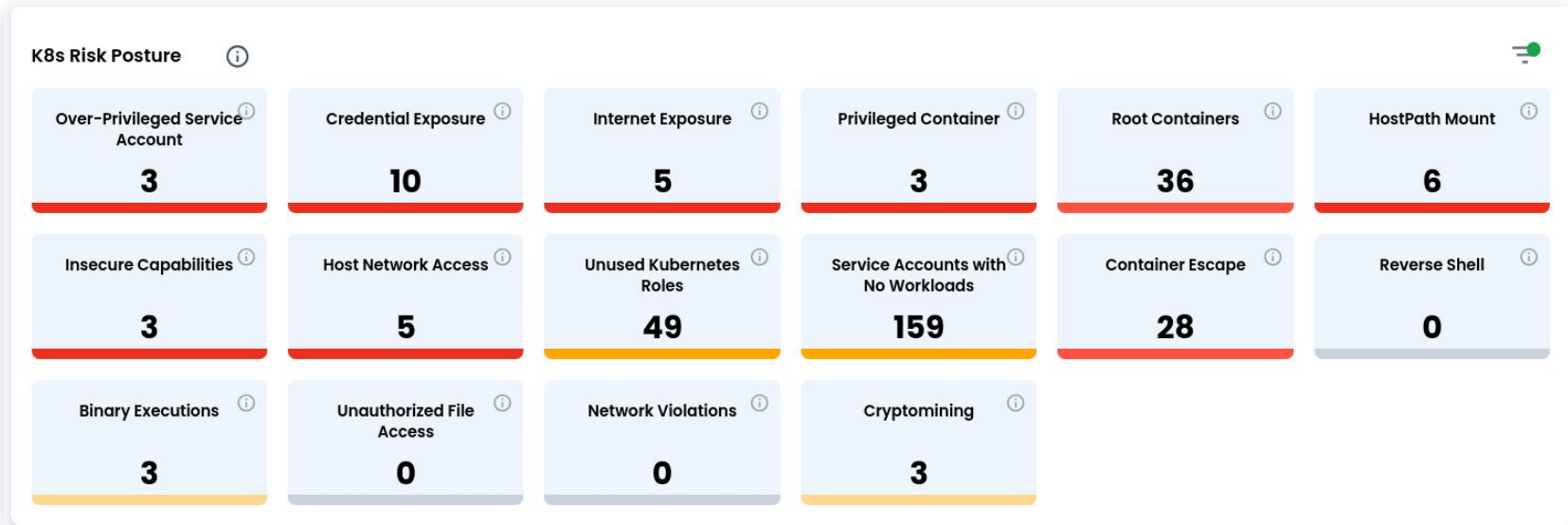


# KSPM Customized Dashboard & Reporting Metrics

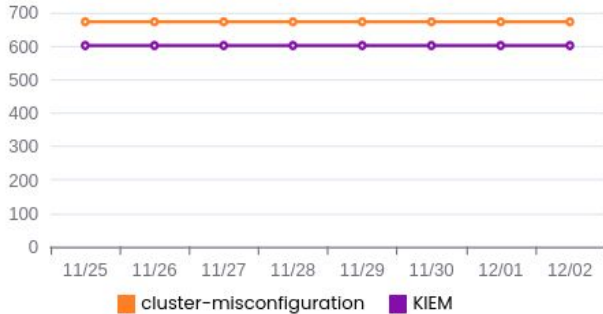
## K8s Resource Summary (i)



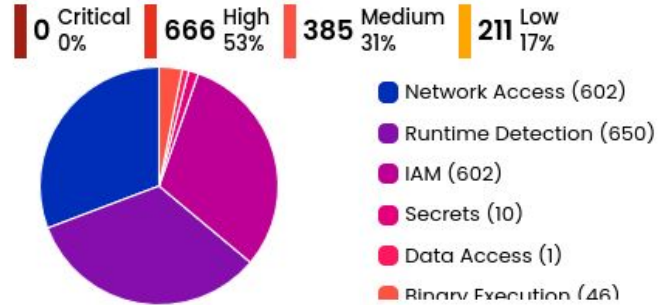
# Security Risk Metrics Widgets [2]



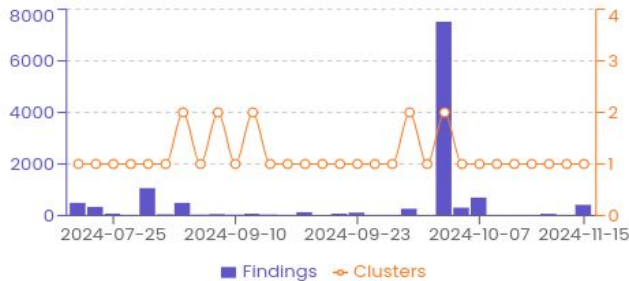
### K8s Findings Trend



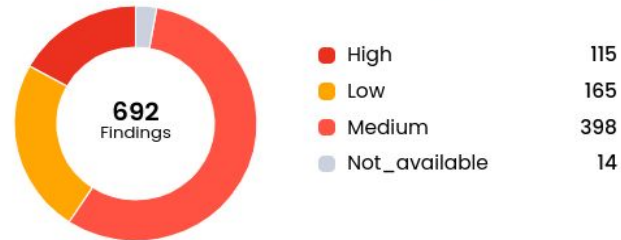
### K8s Open Findings



### New Cluster Findings Trend



### Cluster Findings Summary by Severity

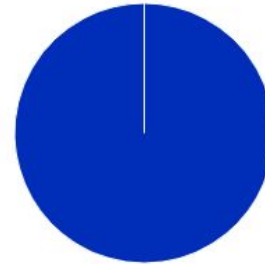


### Clusters with Public Exposure



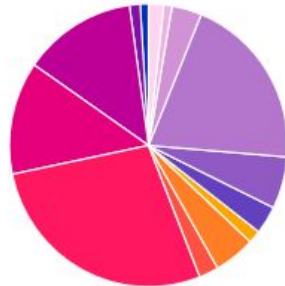
aws-stage-ka...	8.2K
aws-stage-ka...	16.4M
mongo-test-02	163.6K
DO-demo-clust...	1.7M

### Privileged Containers by Clusters



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

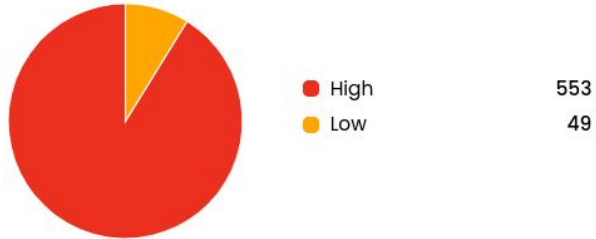
### Cluster Findings by Asset Type



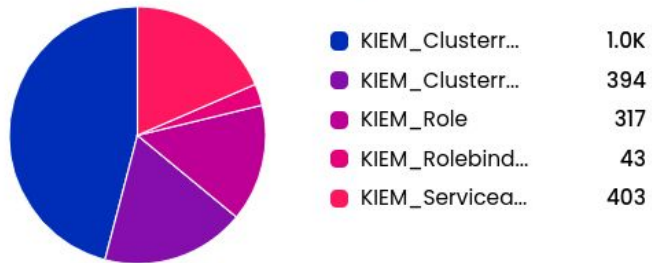
k8s_security_...	1
k8s_security_...	3
k8s_security_...	94
k8s_security_...	92
k8s_security_...	205
k8s_security_...	11



## KIEM Risk Assessment ⓘ



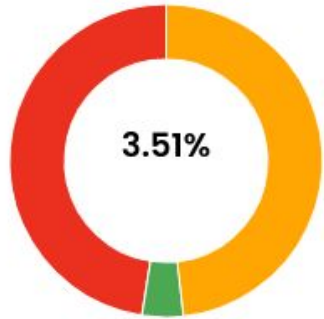
## KIEM Findings by Asset Types ⓘ



## 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

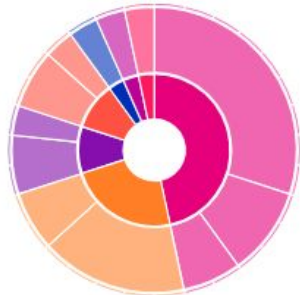
273  
20  
277

## Top 5 K8s CIS Findings ⓘ

Finding Name	Assets Impacted
<span style="color: red;">●</span> 2.5: Ensure that the --peer-client-cert-auth arg...	5
<span style="color: red;">●</span> 2.4: Ensure that the --peer-cert-file and --peer...	5
<span style="color: red;">●</span> 2.3: Ensure that the --auto-tls argument is not s...	5
<span style="color: red;">●</span> 2.2: Ensure that the --client-cert-auth argumen...	5
<span style="color: red;">●</span> 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 >](#)

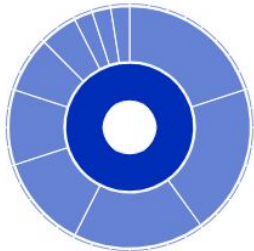
## Top 5 K8s External Egress/Ingress Workloads

492066 Total External Connections

Ingress 99.4% Egress 0.6%



## Workloads without Network Policies



- do-demo-cluster

[Go to Findings >](#)

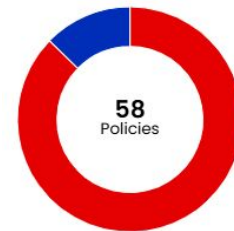
## Privileged Containers



- do-demo-cluster

[Go to All Findings >](#)

## Workloads Without Any Policy Applied

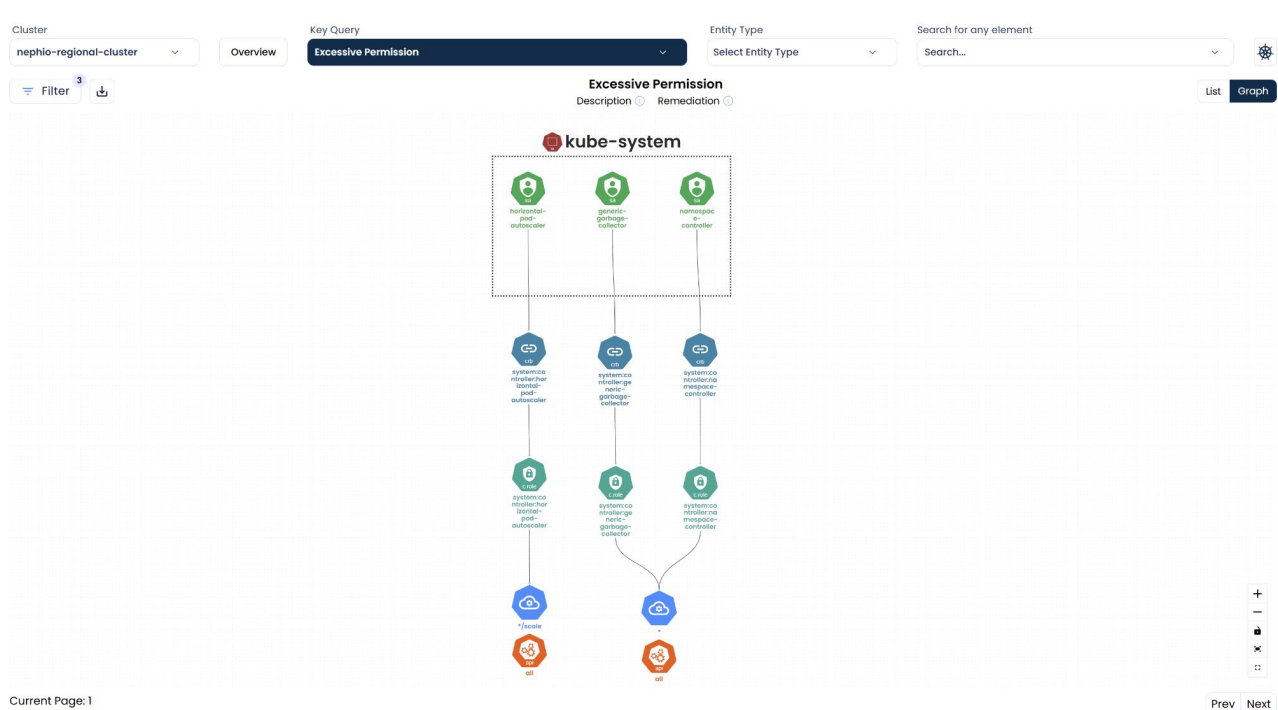


- Applied: 7
- Not Applied: 51



# KSPM Use Cases

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



Current Page: 1

Prev Next



- **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 | Excessive Permission | 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

The screenshot shows the ACCUKNOX KIEM interface. The top navigation bar includes 'Home > KIEM'. The main content area displays a permission graph for the cluster 'nephio-regional-cluster'. The graph shows a central node 'admin-cluster' (c.role) connected to two nodes: 'roles' and 'rolebindings'. Both 'roles' and 'rolebindings' are connected to two nodes: 'rbac.authorization.k8s.io' and 'api'. A 'Filter' button with a '2' indicates two filters are applied. The 'Key Query' section shows 'Permission to create roles and rolebindings'. The bottom left sidebar contains navigation options like 'Dashboard', 'Inventory', 'Issues', 'Compliance', 'Runtime Protection', 'Remediation', 'Monitors / Alerts', 'Identity', 'KIEM (ETA)', 'Reports', 'Notifications', and 'Settings'. The bottom right corner shows 'Current Page: 1'.

The detailed view shows the ClusterRole 'system:aggregate-to-admin-cluster'. The title bar reads 'ClusterRole | system:aggregate-to-admin-cluster'. The interface includes 'List', 'Graph', and 'Manifest' tabs. The 'Graph' tab is active, displaying a tree structure of permissions. The root node is 'system:aggregate-to-admin-cluster' (c.role). It branches into three nodes: 'localsubjectaccessreviews', 'rolebindings', and 'roles'. Each of these nodes is connected to an 'api' node, which is further connected to 'rbac.authorization.k8s.io'.

# KIEM: Track KIEM findings identified by filters

The screenshot displays the ACCUKNOX interface for tracking findings. The left sidebar contains navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, and Ask Ada. The main content area shows the 'Findings' page with a search bar and a filter dropdown set to 'KIEM Findings'. A table lists findings with columns for 'Last seen', 'Assetname', 'Name', 'Risk factor', 'Description', and 'Cluster'. A red box highlights the 'KIEM Findings' filter, and a red arrow points from it to a detailed view of a finding.

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

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

**Description** Result Solution References Source Code

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... [Show More...](#)

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

**Details** [+ Create Ticket](#)

**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	<span>High</span>	45 days	1.1.11	0

Description	Result	Solution	References	Source Code
<p>On the etcd server node, get the etcd data directory, passed as an argument <code>--data-dir</code>, from the command <code>ps -ef   grep etcd</code>. Run the below command (based on the etcd data directory found above). For example, <code>chmod 700 /var/lib/etcd</code></p>				


#### 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

- 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	Severity	SLA	CVE ID	Tickets Created
133 days	<span>High</span>	45 days	C-0262	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 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** [🔗](#)

Add Comments and Press Ctrl + Enter to Submit

No data