

Getting Started Guide	4
● CSPM Prerequisites	4
● Cloud Account Onboarding	4
○ AWS	4
○ AZURE	8
○ GCP	17
CWPP Prerequisites	23
● Cluster Onboarding	24
● Asset Inventory	30
○ Cloud Assets	30
■ How to find a particular asset	30
■ How to group assets	32
■ How to search asset by label	35
● Cloud Workload	35
● How to find graph view of clusters	35
● How to find list view of clusters	36
● How to find details on cluster	36
● Misconfigurations	39
○ Where to find misconfigurations	39
■ Asset Detail Page	39
● Issue Page	40
● How to group by Asset, say s3 and find misconfiguration	41
○ How to group by findings	45
● How to group by criticality and Status	47
○ How to create a ticket	50
Issues/Vulnerabilities	55
● Group findings by source and severity	55
● How to group by Findings and severity	56
● How to group by Asset and severity	57
● How to create automated tickets in Findings and Asset grouping	59
● How registry scan happens?	60
● How to interpret Registry scan results	63
● What is Risk Based Prioritization?	63
Baseline	65
● How to create a Baseline out of a data source	65
● How to compare 2 baselines	67
Compliance	68
● How to get Compliance for Cloud Assets	68
● How to get Compliance for Cloud Workload	70

App Behavior	71
● How to interpret network graph	71
● How to see App Behavior Telemetry	74
Runtime Protection w/ Policy Management	76
● How to understand discover policies	76
● How to understand Hardening policies	79
● How to Audit application and get alerts for that	82
● When do we say policies are stable?	84
● What if something changes in Application??	85
● How to create a custom Policy	89
● How to enforce Policies and see anomalies	96
How to perform bulk operation on applying policies	103
Integrations	105
1. Integrate SIEM tools	105
Splunk	105
Splunk Integration:	105
Integration of Splunk:	105
a. Prerequisites:	105
b. Steps to Integrate:	106
AWS Cloudwatch	107
AWS CloudWatch Integration	107
Integration of Amazon CloudWatch:	107
a. Prerequisites	107
b. Steps to Integrate:	107
c. Configuration of Alert Triggers:	108
d. Logs Forwarding:	109
Rsyslog	109
RSyslog Integration	109
Integration of Rsyslog:	109
a. Prerequisites:	109
b. Steps to Integrate:	109
2. Integrate Notifications Tools	111
Slack	111
Slack Integration:	111
Integration of Slack:	111
a. Prerequisites:	111
b. Steps to Integrate:	111
3. Integrate Ticketing Tools	112
Jira Integration	112
Integration of JIRA:	113
Prerequisites	113

JIRA integration for CWPP:	113
JIRA integration for CSPM:	114
Freshservice	116
Freshservice Integration:	116
Integration of Freshservice:	116
a. Prerequisites	116
b. Steps to Integrate:	116
Creating Ticket Configuration	119
4. Integrate Registries	120
Registry	120
Amazon Elastic Container Registry:	121
Google Container Registry:	121
Nexus Registry:	121
DockerHub Registry:	121
User Management	122
Invite folks to the workspace	122
Assign RBAC	126
Create Roles and Assign Users	127

==AccuKnox Manual==

Getting Started Guide

- CSPM Prerequisites

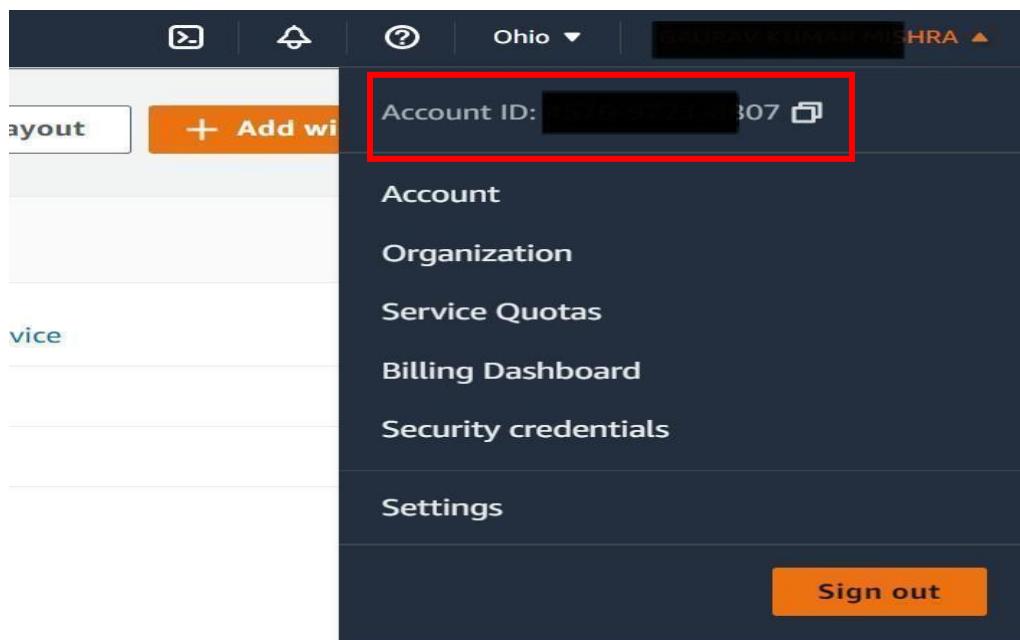
Cloud Account Onboarding

- AWS

1. Manual Setup

For AWS there is a requirement for ARN number related to AWS Account Login to AWS Account & click top right name icon to get Account ID

Create a new IAM role & select “trusted entity type” as “AWS service”



i Introducing the new IAM roles experience
We've redesigned the IAM roles experience to make it easier to use. [Let us know what you think.](#)

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

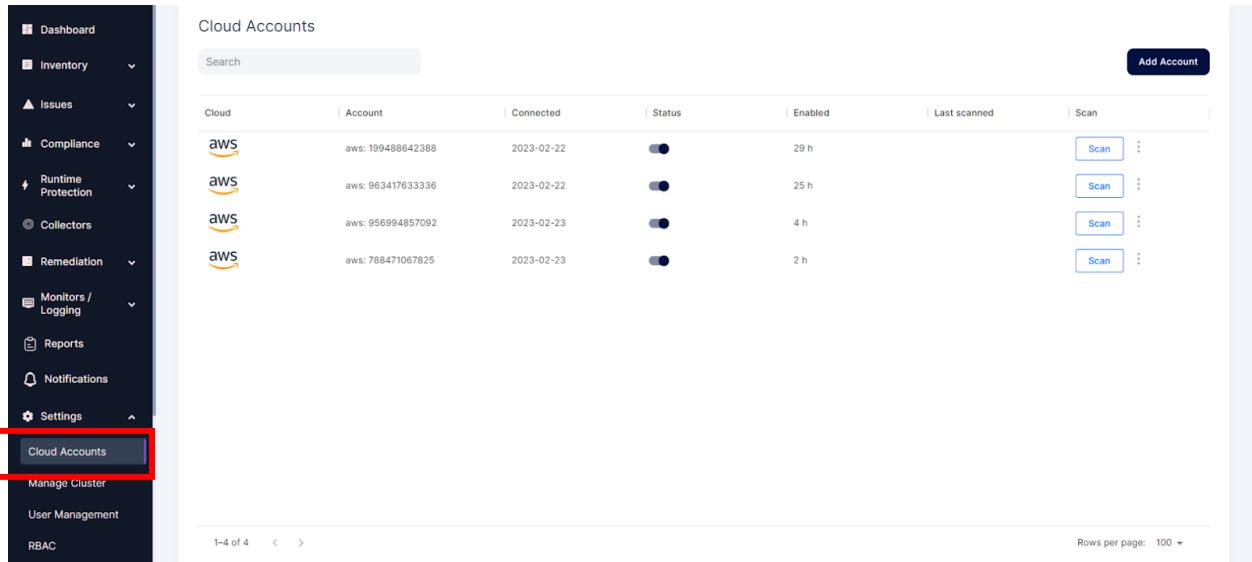
Select trusted entity Info

Trusted entity type

- AWS service Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity Allows users federated by the specified external web identity provider to assume this role and perform actions in this account.
- SAML 2.0 federation Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy Create a custom trust policy to enable others to perform actions in this account.

2. From AccuKnox SaaS UI (Access Ley Metod)

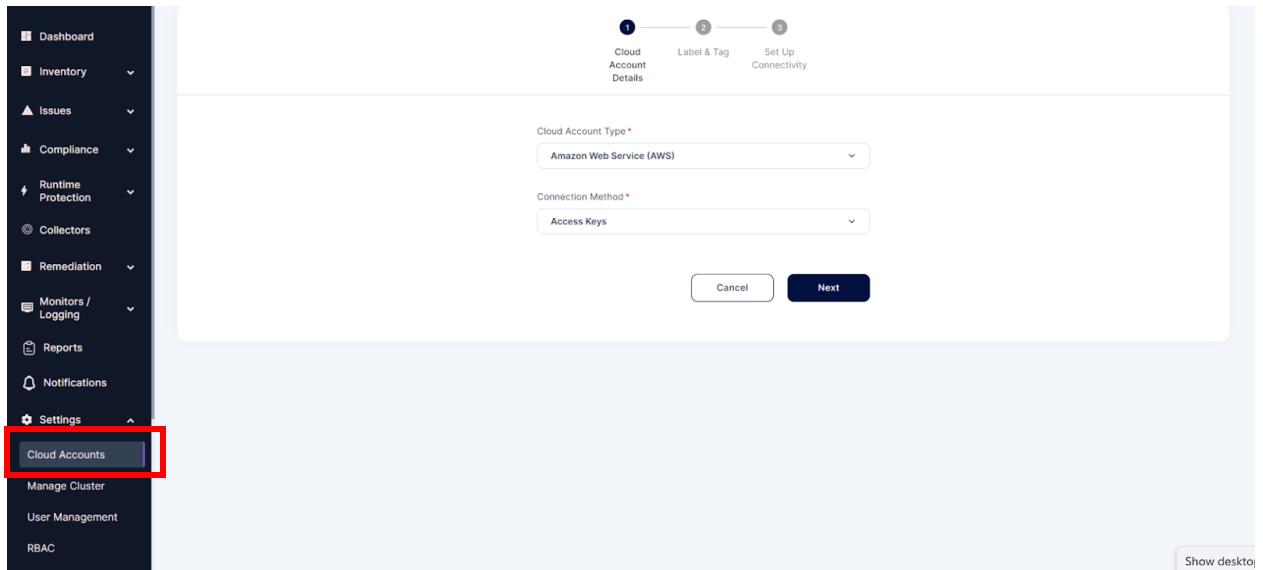
- Click settings -> Cloud Accounts
- Click Add account



The screenshot shows the AccuKnox SaaS UI interface. On the left, there is a dark sidebar with various navigation options: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Collectors, Remediation, Monitors / Logging, Reports, Notifications, Settings, Cloud Accounts (which is highlighted with a red box), Manage Cluster, User Management, and RBAC. The main content area is titled "Cloud Accounts" and contains a table with four rows of data. The columns are: Cloud, Account, Connected, Status, Enabled, Last scanned, and Scan. Each row has an "aws" logo icon under "Cloud", an account ID under "Account", a date under "Connected", a status indicator under "Status" (green circle with a dot), a time under "Enabled" (e.g., 29 h), and a date under "Last scanned". To the right of each row is a "Scan" button and a more options menu (three dots). At the top right of the main area, there is a "Add Account" button.

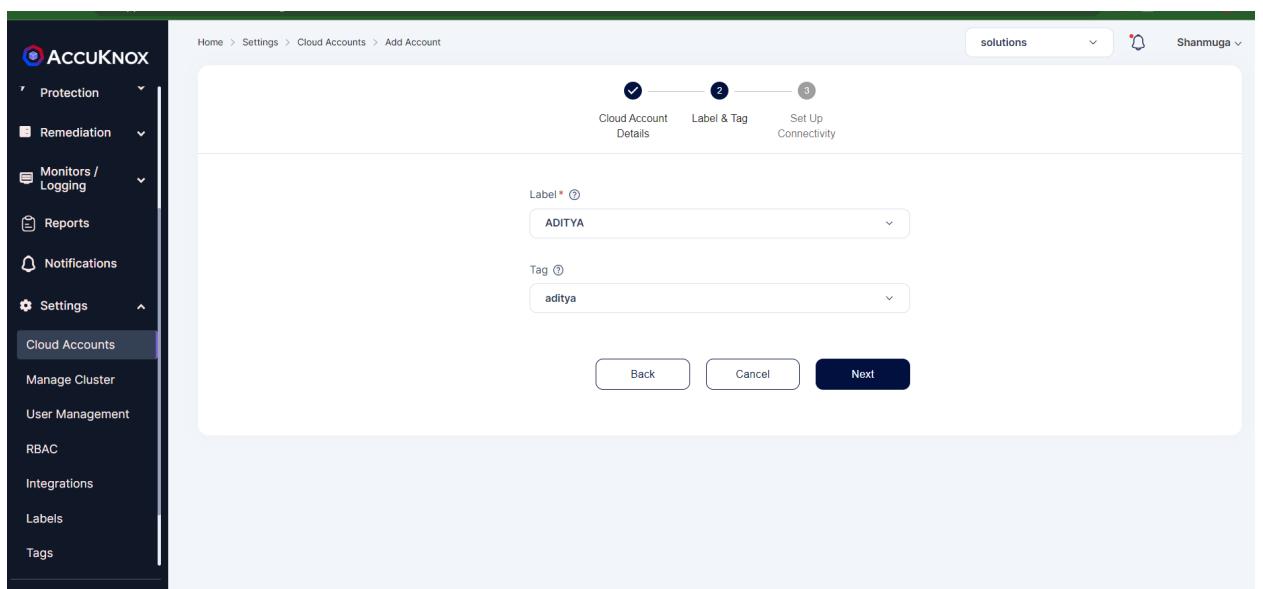
Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 199488642388	2023-02-22	●	29 h		<button>Scan</button> ...
aws	aws: 963417633336	2023-02-22	●	25 h		<button>Scan</button> ...
aws	aws: 956994857092	2023-02-23	●	4 h		<button>Scan</button> ...
aws	aws: 788471067825	2023-02-23	●	2 h		<button>Scan</button> ...

- Select the Cloud Account type to AWS
- Select the Connection method to Access key

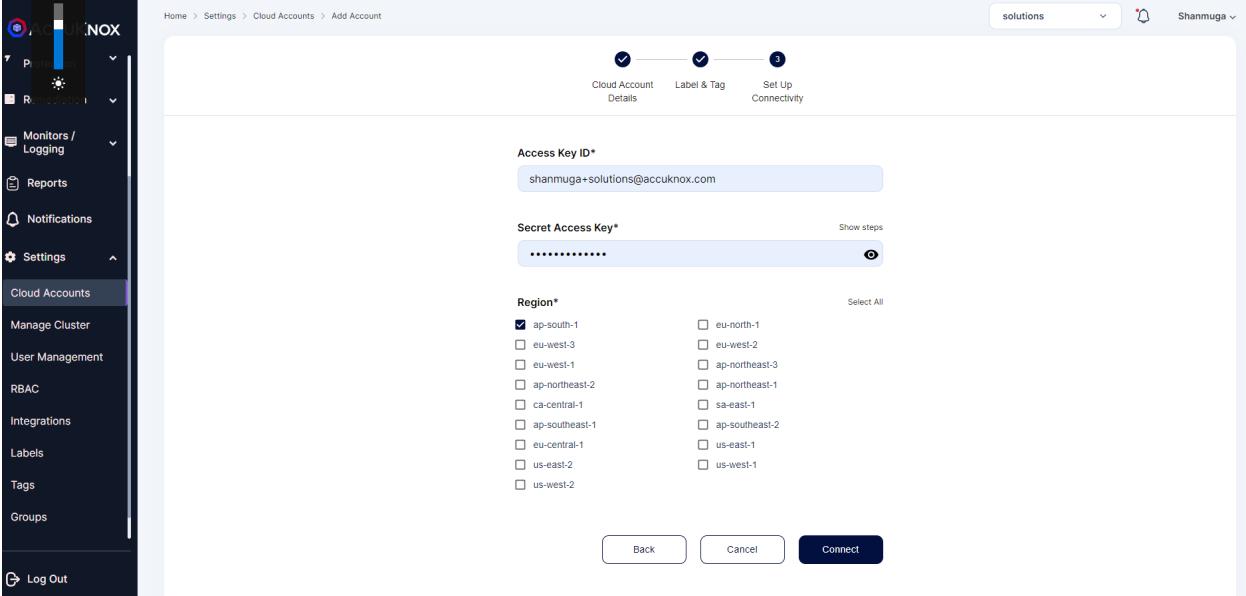


- Select the Labels and Tags

Note: If there are no labels and tags create new labels and tags via the settings



- Fill the fields with Access key and Secret access key of the AWS account



Cloud Account Details

Label & Tag

Set Up Connectivity

Access Key ID*

shanmuga+solution@accuknox.com

Secret Access Key*

Show steps

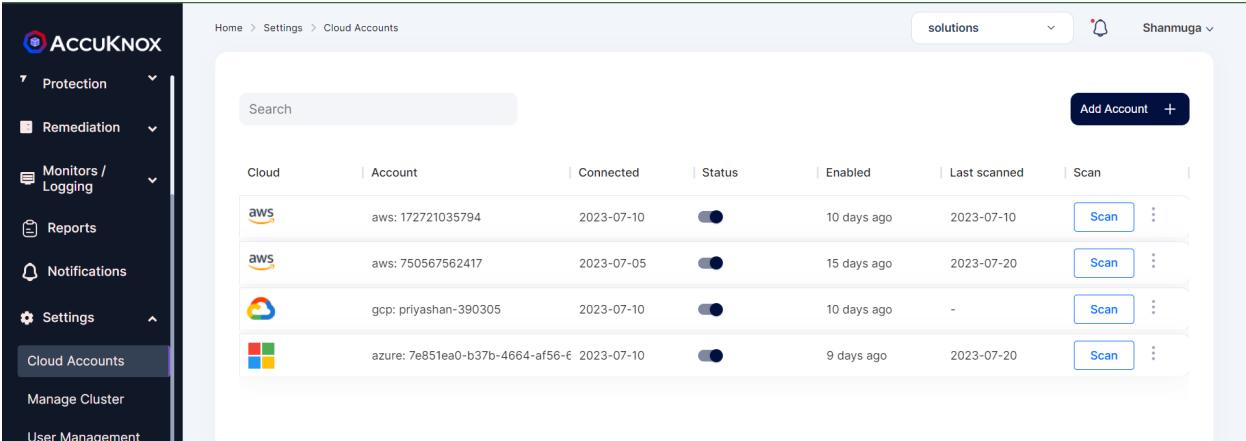
Region*

Select All

<input checked="" type="checkbox"/> ap-south-1	<input type="checkbox"/> eu-north-1
<input type="checkbox"/> eu-west-3	<input type="checkbox"/> eu-west-2
<input type="checkbox"/> eu-west-1	<input type="checkbox"/> ap-northeast-3
<input type="checkbox"/> ap-northeast-2	<input type="checkbox"/> ap-northeast-1
<input type="checkbox"/> ca-central-1	<input type="checkbox"/> sa-east-1
<input type="checkbox"/> ap-southeast-1	<input type="checkbox"/> ap-southeast-2
<input type="checkbox"/> eu-central-1	<input type="checkbox"/> us-east-1
<input type="checkbox"/> us-east-2	<input type="checkbox"/> us-west-1

Back Cancel Connect

- Select the regions and click connect
Note: Only the regions that have been specified will have resources scanned.
- Check Settings → Cloud Accounts. You will see your cloud account is added successfully.

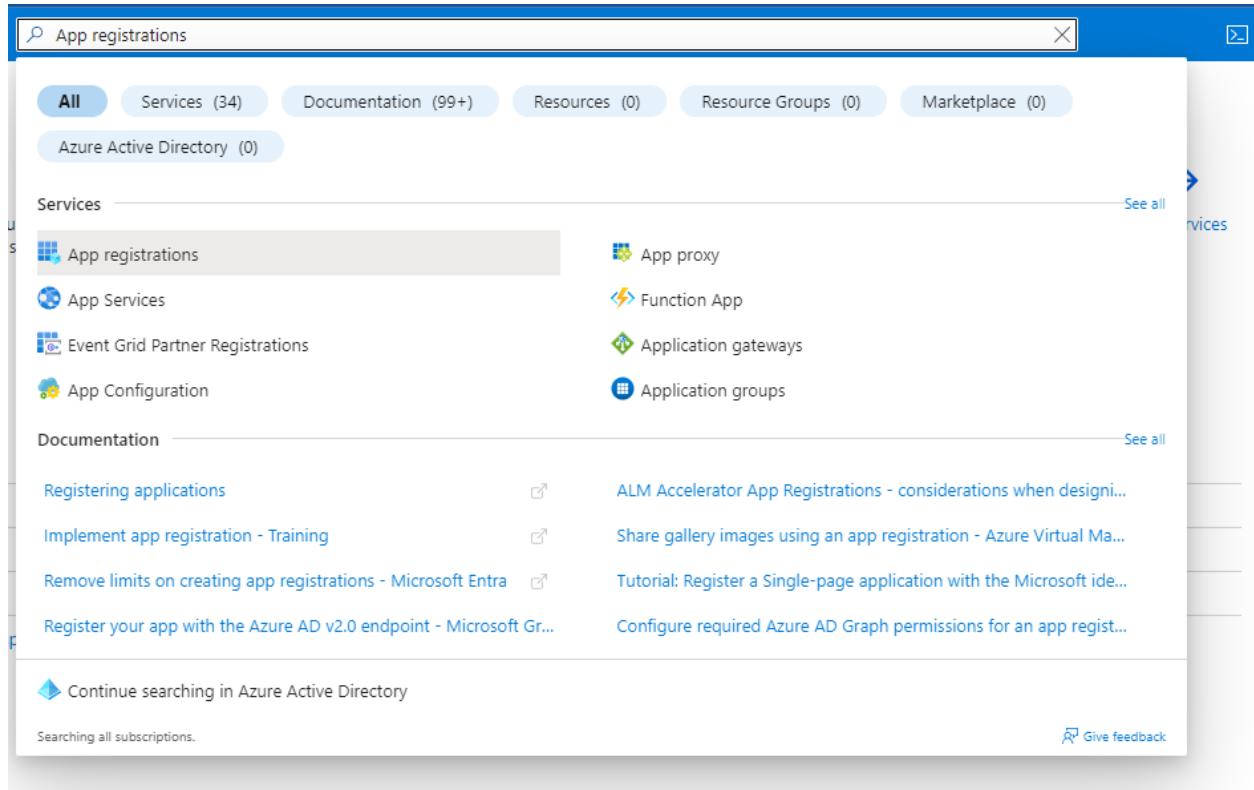


Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	<input checked="" type="button"/>	10 days ago	2023-07-10	<button>Scan</button> ...
aws	aws: 750567562417	2023-07-05	<input checked="" type="button"/>	15 days ago	2023-07-20	<button>Scan</button> ...
gcp	gcp: priyashan-390305	2023-07-10	<input checked="" type="button"/>	10 days ago	-	<button>Scan</button> ...
azure	azure: 7e851ea0-b37b-4664-af56-6	2023-07-10	<input checked="" type="button"/>	9 days ago	2023-07-20	<button>Scan</button> ...

- AZURE

For Azure Onboarding it is required to register an App and giving Security read access to that App from the Azure portal.

- Go to your Azure Portal and search for App registrations and open it



The screenshot shows the Azure portal interface. At the top, there is a search bar with the text "App registrations". Below the search bar, there are several navigation tabs: "All", "Services (34)", "Documentation (99+)", "Resources (0)", "Resource Groups (0)", and "Marketplace (0)". Under the "Services" tab, there is a sub-section titled "Azure Active Directory (0)". The main content area is titled "Services" and contains a list of services. "App registrations" is highlighted with a blue background and has a small icon of a blue square with a white gear. Other services listed include "App proxy", "Function App", "Application gateways", and "Application groups". Below the services, there is a section titled "Documentation" with several links: "Registering applications", "Implement app registration - Training", "Remove limits on creating app registrations - Microsoft Entra", "Register your app with the Azure AD v2.0 endpoint - Microsoft Gr...", "ALM Accelerator App Registrations - considerations when designi...", "Share gallery images using an app registration - Azure Virtual Ma...", "Tutorial: Register a Single-page application with the Microsoft ide...", and "Configure required Azure AD Graph permissions for an app regist...". At the bottom of the page, there is a link "Continue searching in Azure Active Directory" and a "Give feedback" button.

- Here click on New registration

Home >

App registrations

[New registration](#) [Endpoints](#) [Troubleshooting](#) [Refresh](#) [Download](#) [Preview features](#) | [Got feedback?](#)

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to support the existing features. [Learn more](#)

All applications Owned applications Deleted applications

Start typing a display name or application (client) ID to filter these results... [Add filters](#)

7 applications found

Display name	Action
Accuknox-may-2023	...

- Give your application a name, remember this name as it will be used again later,
For the rest keep the default settings

Home > App registrations >
Register an application ...

* Name
The user-facing display name for this application (this can be changed later).

Supported account types
Who can use this application or access this API?
 Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only
[Help me choose...](#)

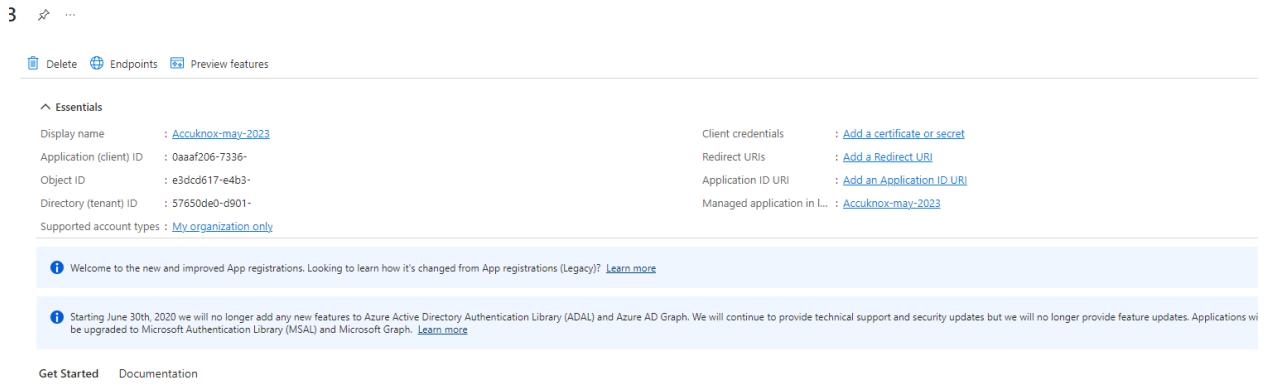
Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

By proceeding, you agree to the Microsoft Platform Policies [View](#)

[Register](#)

- Now your application is created, save Application ID and Directory ID as they will be needed to for onboarding on Accuknox Saas and then click on 'Add a certificate or secret'



Essentials

Display name : [Accuknox-may-2023](#)

Application (client) ID : 0aaaf206-7336-

Object ID : e3ddcd617-e4b3-

Directory (tenant) ID : 57650de0-6901-

Supported account types : [My organization only](#)

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

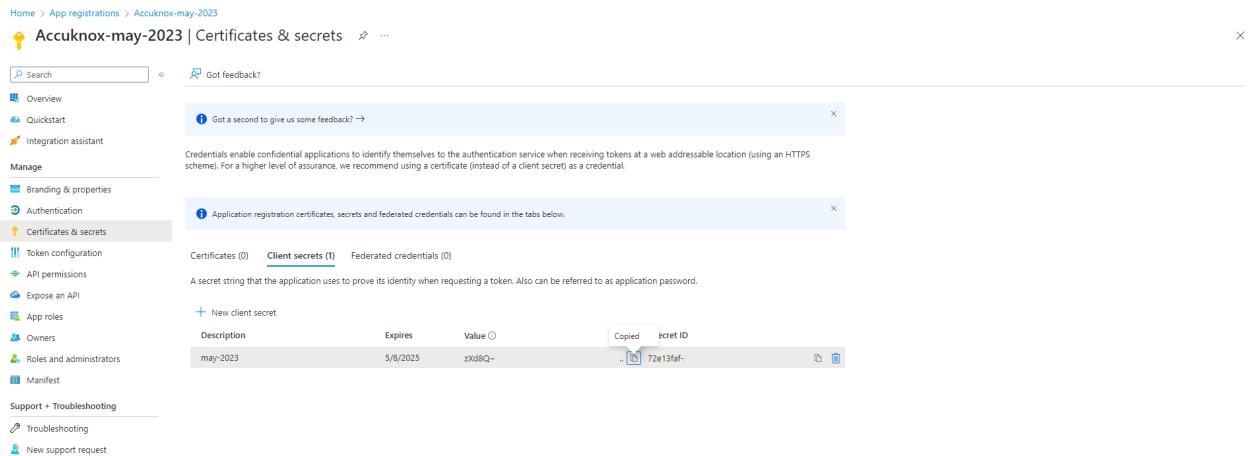
Managed application in ... : [Accuknox-may-2023](#)

Notes:

- Welcome to the new and improved App registrations. Looking to learn how it's changed from App registrations (Legacy)? [Learn more](#)
- Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure AD Graph. We will continue to provide technical support and security updates but we will no longer provide feature updates. Applications will be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. [Learn more](#)

[Get Started](#) [Documentation](#)

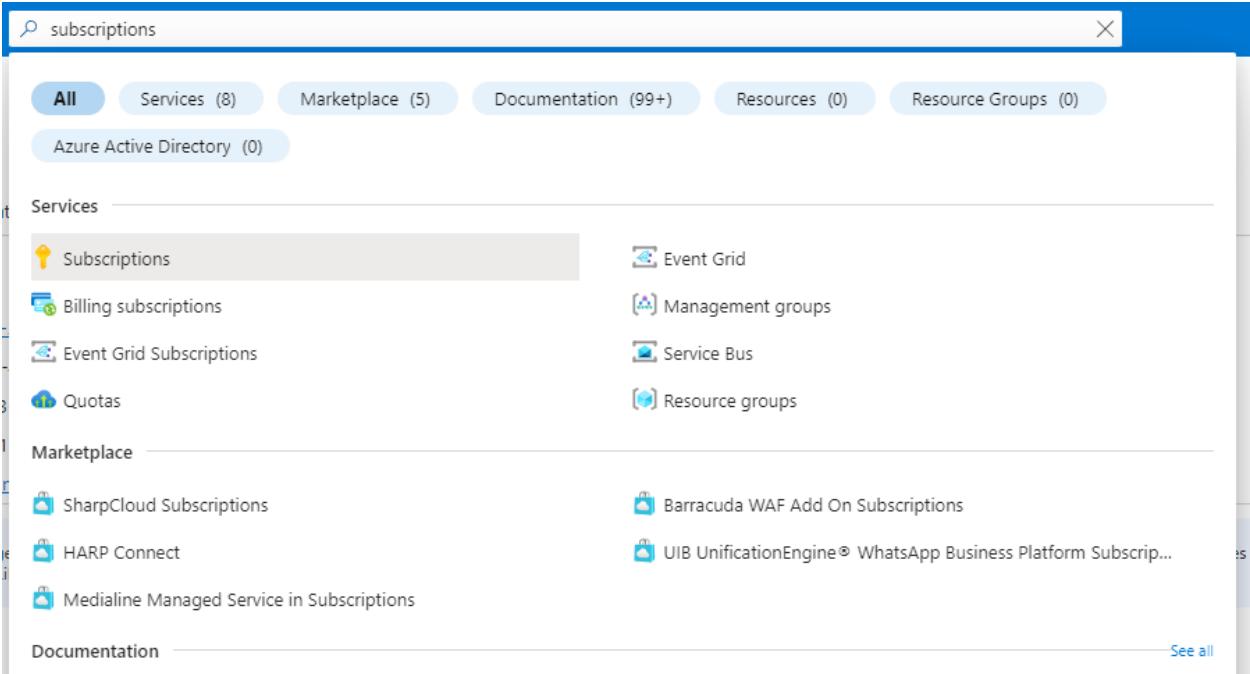
- Click on new client secret and enter the name and expiration date to get secret id and secret value, save this secret value as this will also be needed for onboarding.



Certificates & secrets

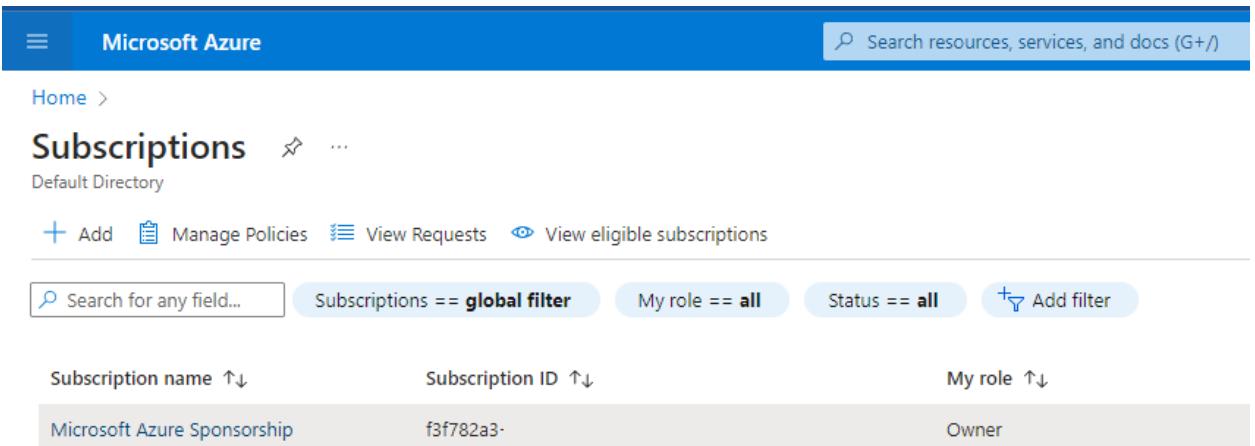
Description	Expires	Value	Copied	Ret ID
may-2023	5/8/2025	zXd8Q-		72e13faf-

- Now we need to give Security read permissions to this registered Application , to do that go to subscriptions



The screenshot shows a search interface with a search bar containing 'subscriptions'. Below the search bar, there are several tabs: All (selected), Services (8), Marketplace (5), Documentation (99+), Resources (0), Resource Groups (0), and Azure Active Directory (0). The main content area is titled 'Services' and contains a list of items under three categories: Subscriptions, Billing subscriptions, Event Grid Subscriptions, Quotas, Management groups, Service Bus, Resource groups, SharpCloud Subscriptions, Barracuda WAF Add On Subscriptions, HARP Connect, UIB UnificationEngine® WhatsApp Business Platform Subscript..., and Medialine Managed Service in Subscriptions. A 'See all' link is at the bottom right.

- First save the subscription ID and click on the subscription name , here it is “Microsoft Azure Sponsorship”



The screenshot shows the Microsoft Azure portal's 'Subscriptions' page. At the top, there is a search bar and a 'Home >' breadcrumb. The main heading is 'Subscriptions' with a 'Default Directory' link. Below the heading are buttons for 'Add', 'Manage Policies', 'View Requests', and 'View eligible subscriptions'. There are also filters for 'Search for any field...', 'Subscriptions == global filter', 'My role == all', 'Status == all', and 'Add filter'. The table below lists one subscription: 'Microsoft Azure Sponsorship' with 'Subscription ID' f3f782a3-... and 'My role' set to 'Owner'.

Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓
Microsoft Azure Sponsorship	f3f782a3-	Owner

- Navigate to Access control(IAM) and go to Roles , here select Add and Add role assignment

Microsoft Azure Sponsorship | Access control (IAM)

Subscription

Search

Add Download role assignments Edit columns Refresh Remove Feedback

- Overview
- Activity log
- Access control (IAM)**
- Tags
- Diagnose and solve problems
- Security
- Events
- Billing
- Invoices
- Payment methods
- Partner information
- Settings
- Programmatic deployment
- Resource groups

Add role assignment Roles Deny assignments Classic administrators

Add co-administrator

Add custom role

Search: accuknox Type: All Category: All

Showing 0 of 412 roles

Name ↑↓	Description ↑↓
No results.	

- Search for “Security Reader” Job function Role, select it and press next

Home > Subscriptions > Microsoft Azure Sponsorship | Access control (IAM) >

Add role assignment ...

Role * **Members *** **Review + assign**

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. [Learn more](#)

Assignment type

Job function roles Privileged administrator roles

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

security reader

Type: All

Category: All

Name ↑↓

Description ↑↓

Security Detonation Chamber Reader

Allowed to query submission info and files from Security Detonation Chamber

Security Reader

Security Reader Role

< Previous

Page

1 / 1

of 1 Next >

- In the member section click on Select members it will open a dropdown menu on the right hand side

Add role assignment ...

Role **Members** • Review + assign

Selected role Security Reader

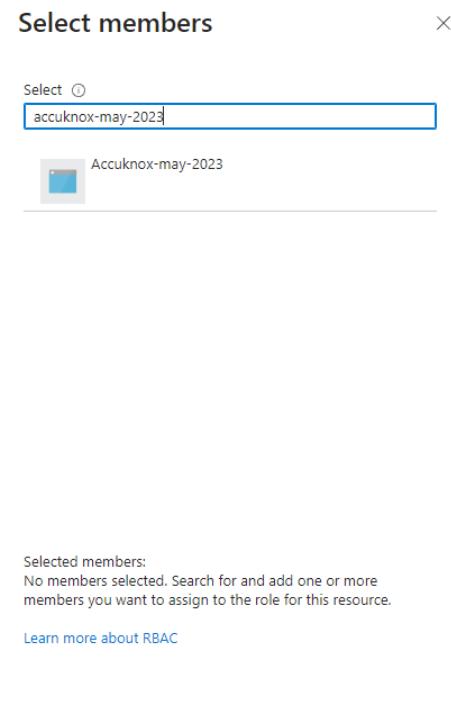
Assign access to User, group, or service principal
 Managed identity

Members [+ Select members](#)

Name	Object ID
No members selected	

Description Optional

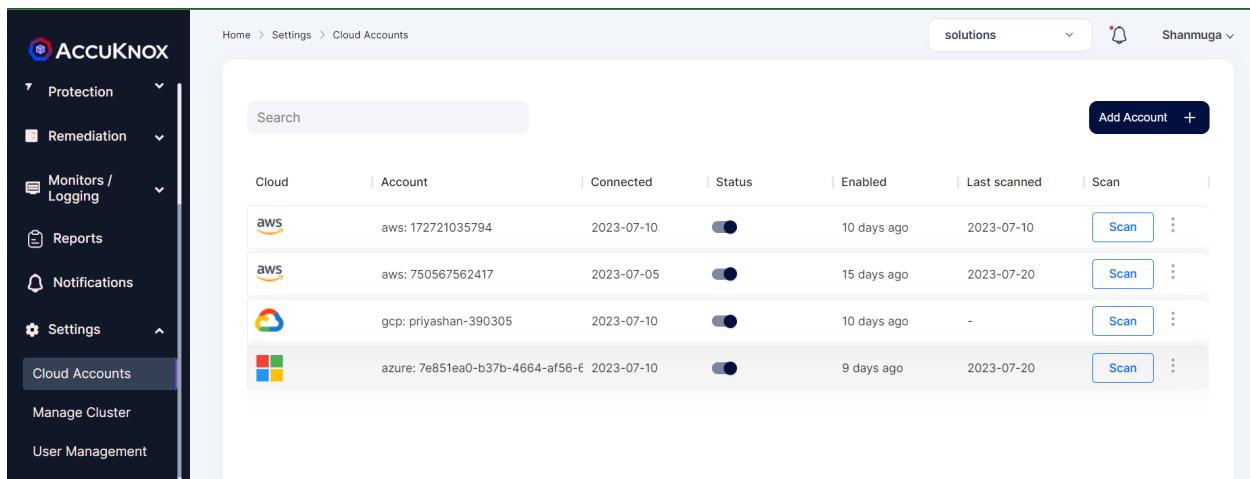
- Here search for the Application that you registered in the beginning , select the application and click on review and assign.



From AccuKnox SaaS UI

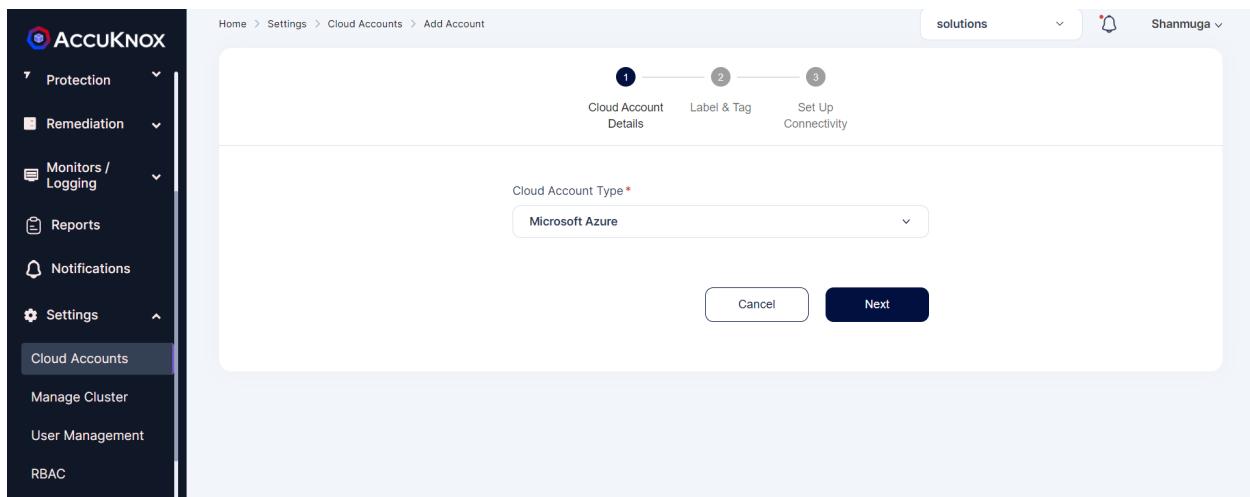
Configuring your Azure cloud account is complete, now we need to onboard the cloud account onto AccuKnox SaaS Platform.

- Go to settings-> Cloud Account and click on Add Account

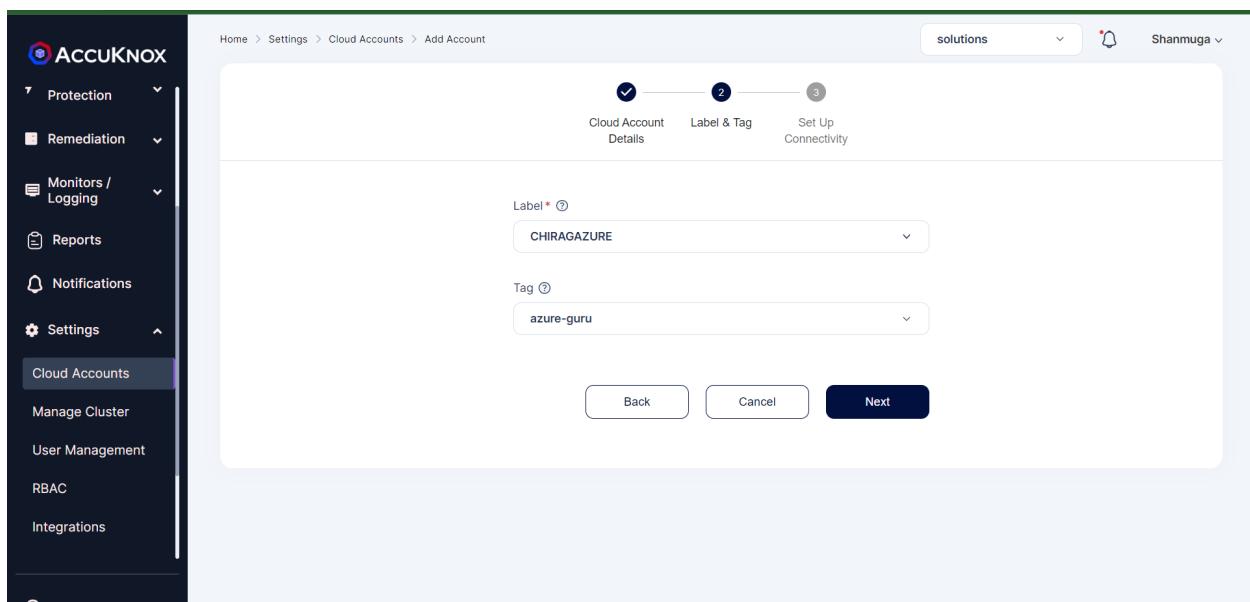


Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	ON	10 days ago	2023-07-10	<button>Scan</button> <button>⋮</button>
aws	aws: 750567562417	2023-07-05	ON	15 days ago	2023-07-20	<button>Scan</button> <button>⋮</button>
gcp	gcp: priyashan-390305	2023-07-10	ON	10 days ago	-	<button>Scan</button> <button>⋮</button>
azure	azure: 7e851ea0-b37b-4664-af56-6	2023-07-10	ON	9 days ago	2023-07-20	<button>Scan</button> <button>⋮</button>

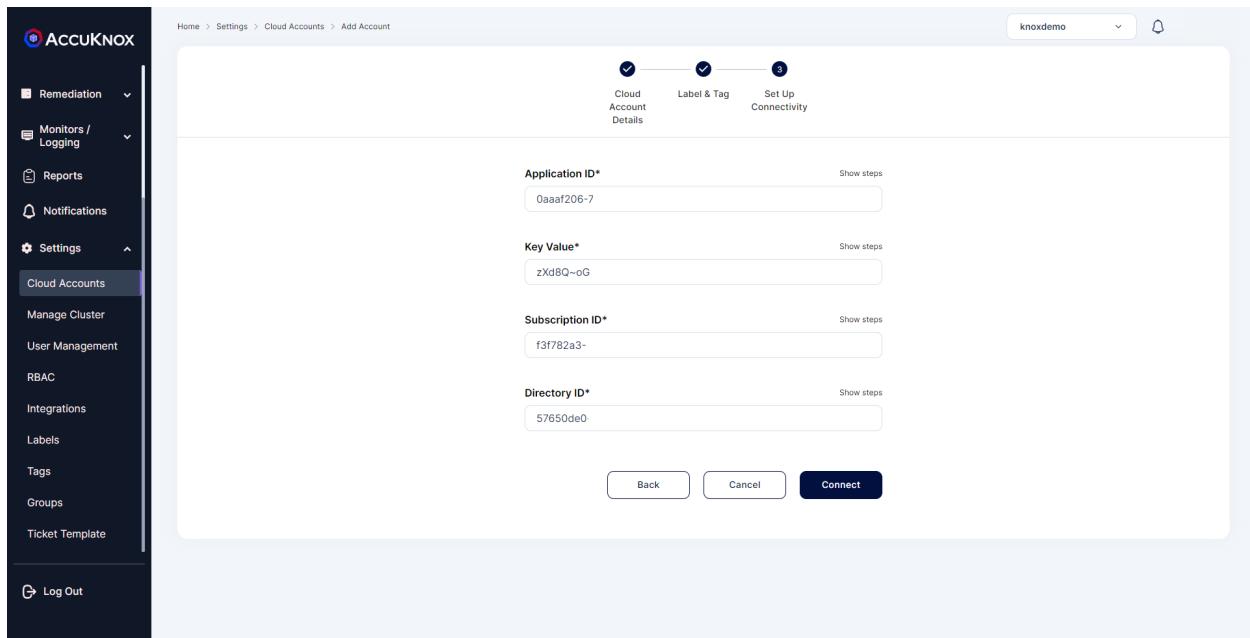
- Select Microsoft Azure as Cloud Account Type and click on next



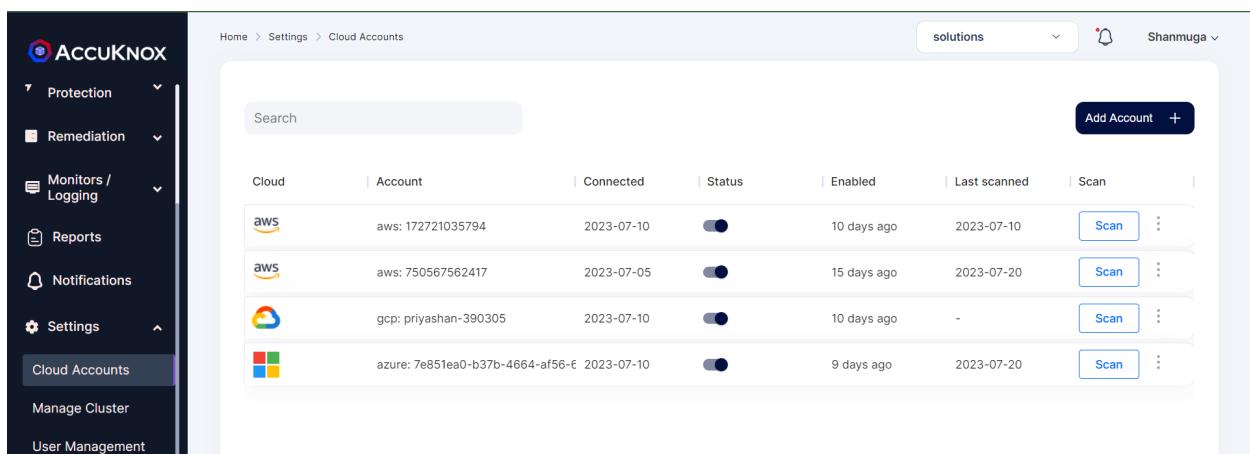
- Select or create label and Tags that will be associated with this Cloud Account



- Enter the details that we saved earlier during the steps for app registration and subscription id from subscriptions in azure portal and click on connect

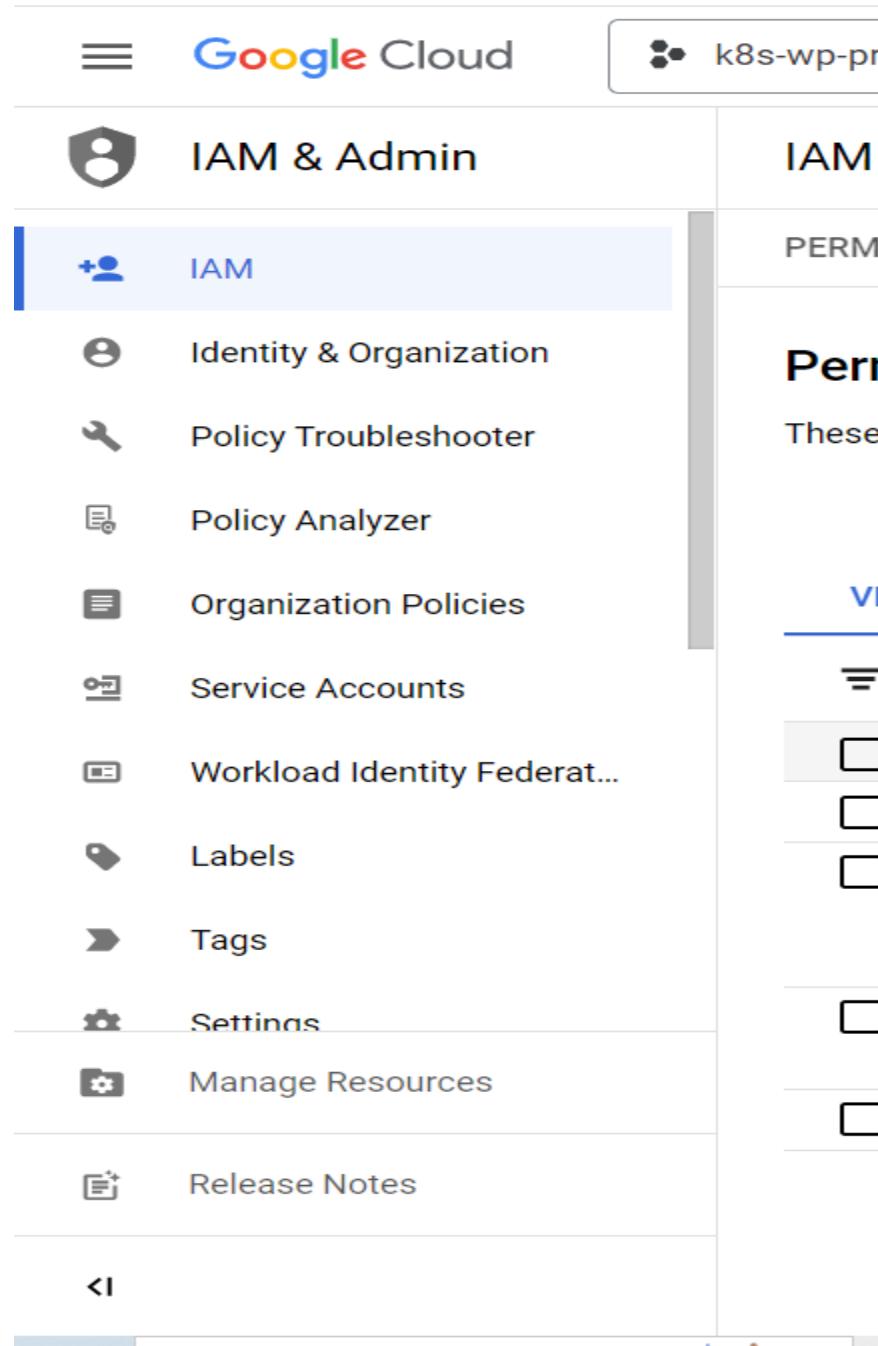


- After successfully connecting your cloud account will show up in the list



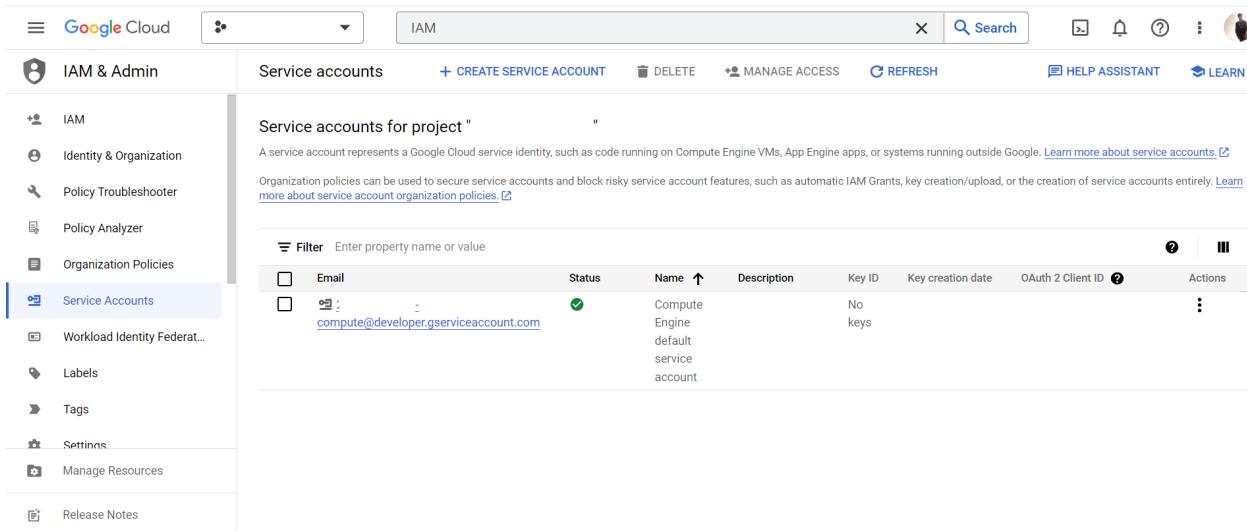
- o GCP

For GCP there is a requirement for IAM Service Account Access. + Log into your Google Cloud console and navigate to IAM Admin > Service Accounts



The screenshot shows the Google Cloud IAM & Admin interface. The top navigation bar includes the Google Cloud logo and a project selector for 'k8s-wp-pr'. Below the navigation is a sidebar with several options: 'IAM' (selected), 'Identity & Organization', 'Policy Troubleshooter', 'Policy Analyzer', 'Organization Policies', 'Service Accounts', 'Workload Identity Federat...', 'Labels', 'Tags', 'Settings', 'Manage Resources', and 'Release Notes'. To the right of the sidebar, the word 'PERM' is displayed above a list of permissions, with 'Service Accounts' having three checkboxes checked. A vertical scroll bar is visible on the right side of the main content area.

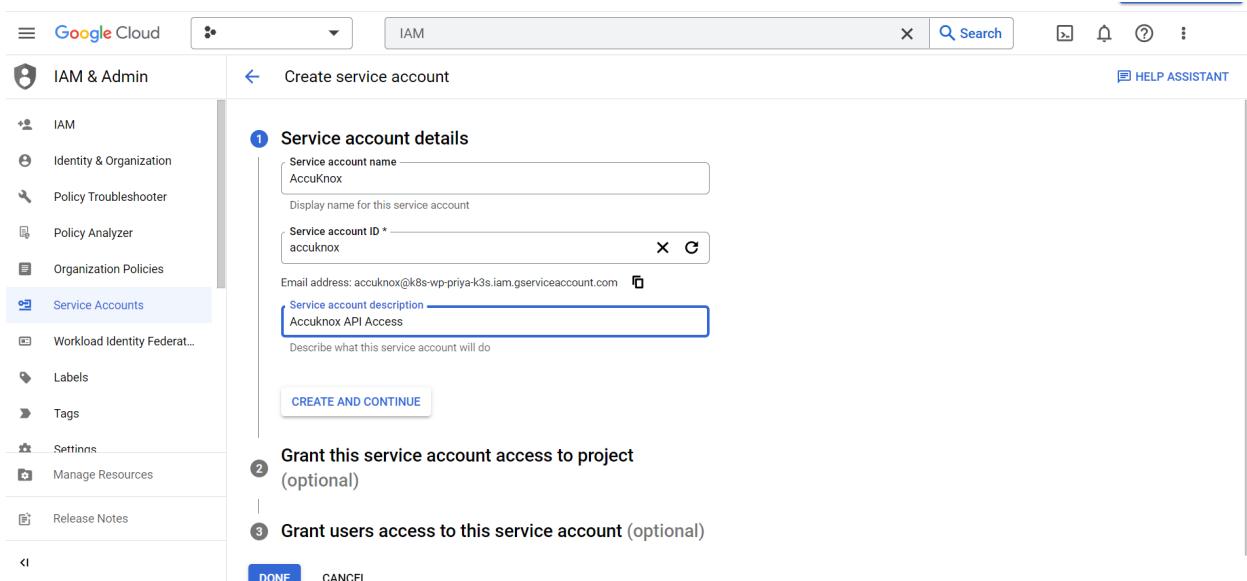
- Click on "Create Service Account".



The screenshot shows the Google Cloud IAM & Admin Service Accounts page. On the left sidebar, 'Service Accounts' is selected. The main area displays a table of service accounts. One account is listed:

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
compute@developer.gserviceaccount.com	Green checkmark	Compute Engine default service account	No keys				⋮

- Enter "AccuKnox" in the "Service account name", then enter "Accuknox API Access" in the description.
- Click on Continue.



The screenshot shows the 'Create service account' dialog. The 'Service account details' step is active. The form fields are filled as follows:

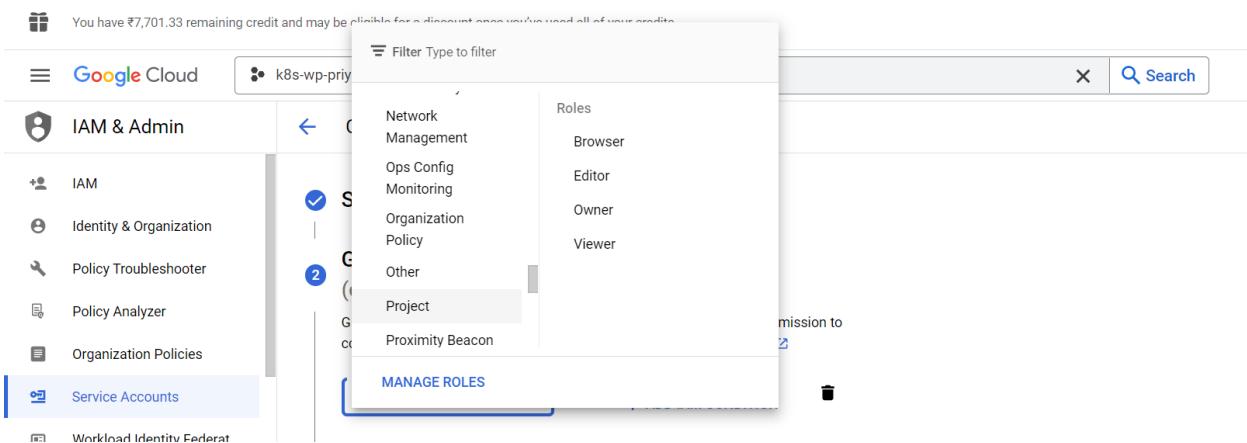
- Service account name: AccuKnox
- Display name for this service account: (empty)
- Service account ID: accuknox
- Email address: accuknox@k8s-wp-priya-k3s.iam.gserviceaccount.com
- Service account description: Accuknox API Access

Below the form, there are two optional steps:

- Grant this service account access to project (optional)
- Grant users access to this service account (optional)

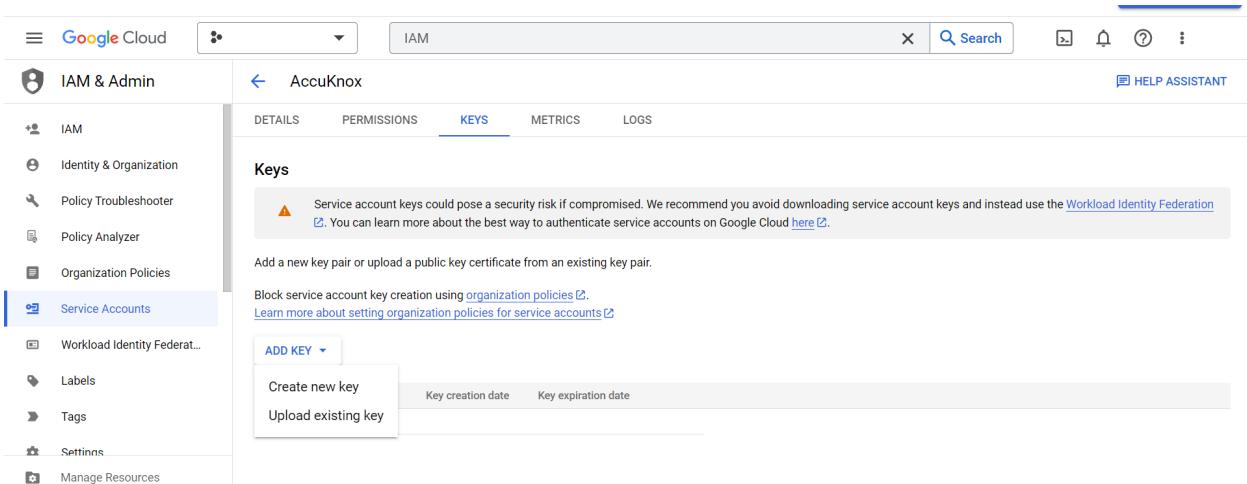
At the bottom are 'DONE' and 'CANCEL' buttons.

- Select the role: Project > Viewer and click Continue.



The screenshot shows the Google Cloud IAM & Admin interface. On the left sidebar, under 'Service Accounts', a context menu is open over a service account named 'k8s-wp-prv'. The menu is titled 'Filter Type to filter' and lists several role categories: Network Management, Ops Config, Monitoring, Organization Policy, Other, Project, and Proximity Beacon. The 'Project' category is highlighted with a blue border. At the bottom of the menu, there is a 'MANAGE ROLES' button. To the right of the menu, a list of roles is shown, with 'Viewer' selected and highlighted in blue. Other roles listed include Browser, Editor, and Owner.

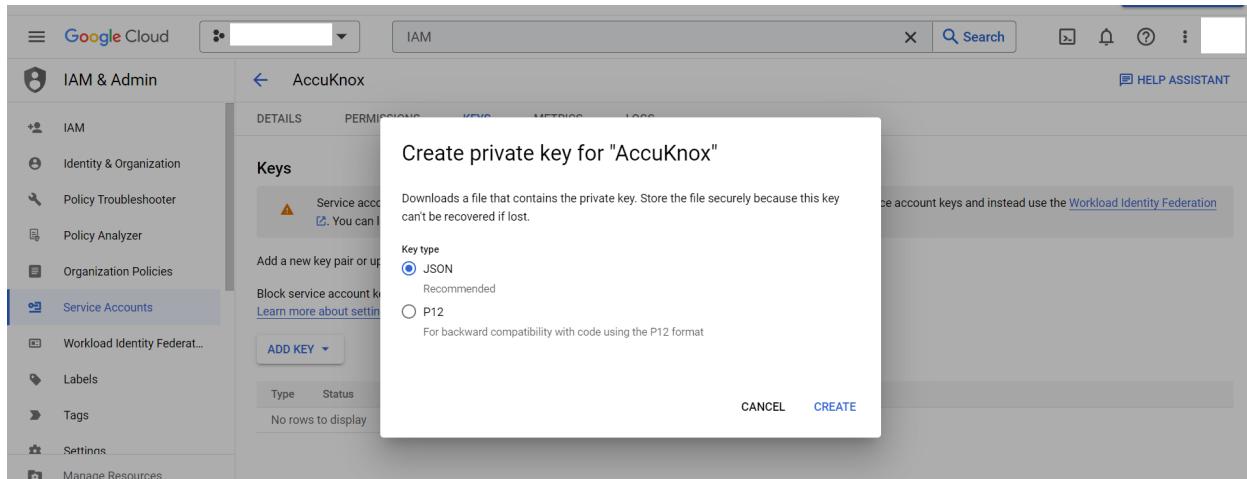
- Click on “Done”
- To create a “Key” click the created service account



The screenshot shows the Google Cloud Service Accounts interface. On the left sidebar, under 'Service Accounts', a context menu is open over a service account named 'AccuKnox'. The menu is titled 'AccuKnox' and includes options for DETAILS, PERMISSIONS, KEYS, METRICS, and LOGS. The 'KEYS' tab is currently selected. Below the tabs, there is a section titled 'Keys' with a warning message: 'Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation'. It also says 'You can learn more about the best way to authenticate service accounts on Google Cloud [here](#)'. Below this, there is a note: 'Add a new key pair or upload a public key certificate from an existing key pair.' and 'Block service account key creation using organization policies'. There is a link to 'Learn more about setting organization policies for service accounts'. At the bottom of the 'KEYS' section, there is a 'CREATE NEW KEY' button and a 'UPLOAD EXISTING KEY' button. A tooltip for the 'CREATE NEW KEY' button says 'ADD KEY ▾'.

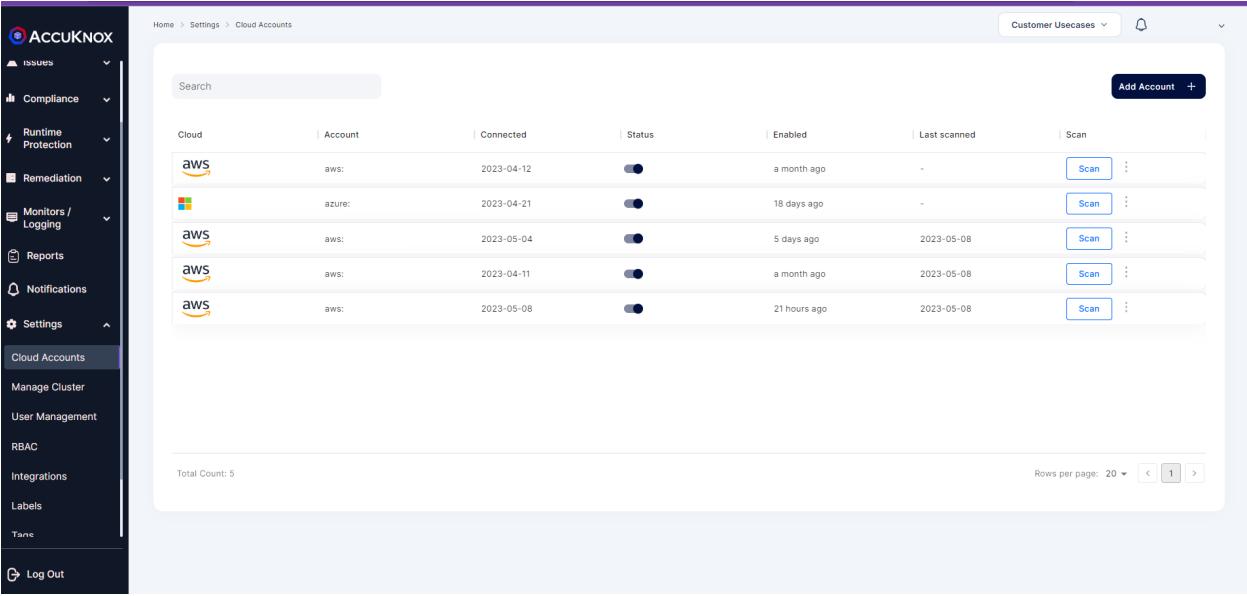
- Click Add Key and Create new key
- Check the JSON file and create.

Note: The created JSON private key file will be downloaded to your local machine by default.



2. From AccuKnox SaaS UI

- Click settings -> Cloud Accounts
- Click Add account

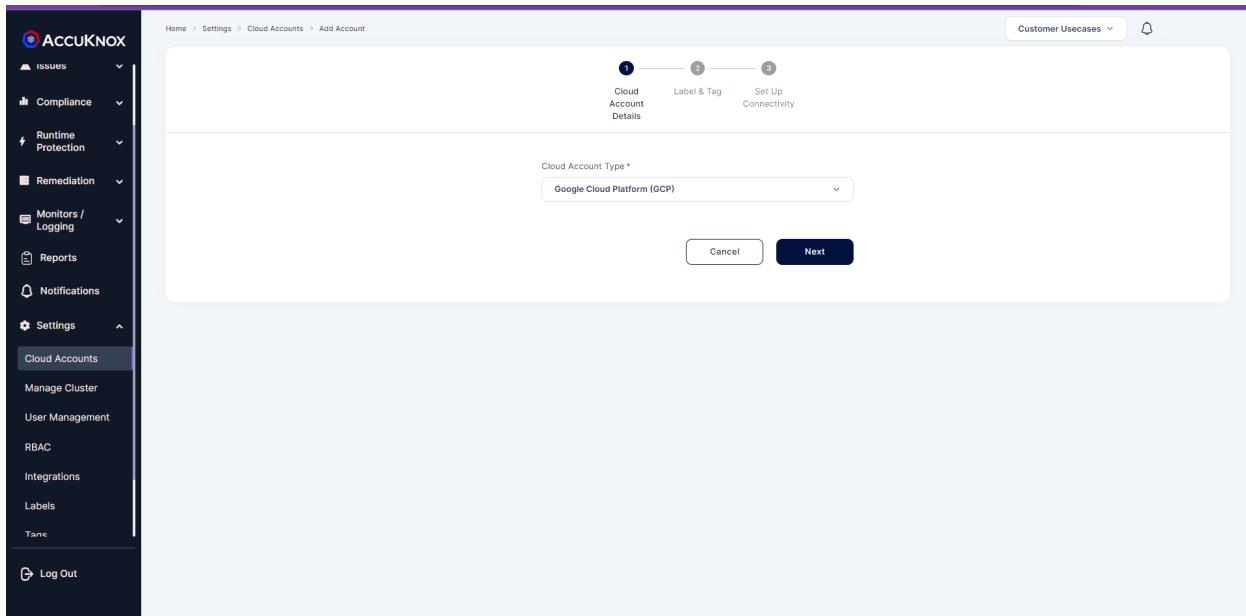


The screenshot shows the AccuKnox SaaS UI. The left sidebar has a 'Cloud Accounts' section selected. The main area displays a table of connected cloud accounts:

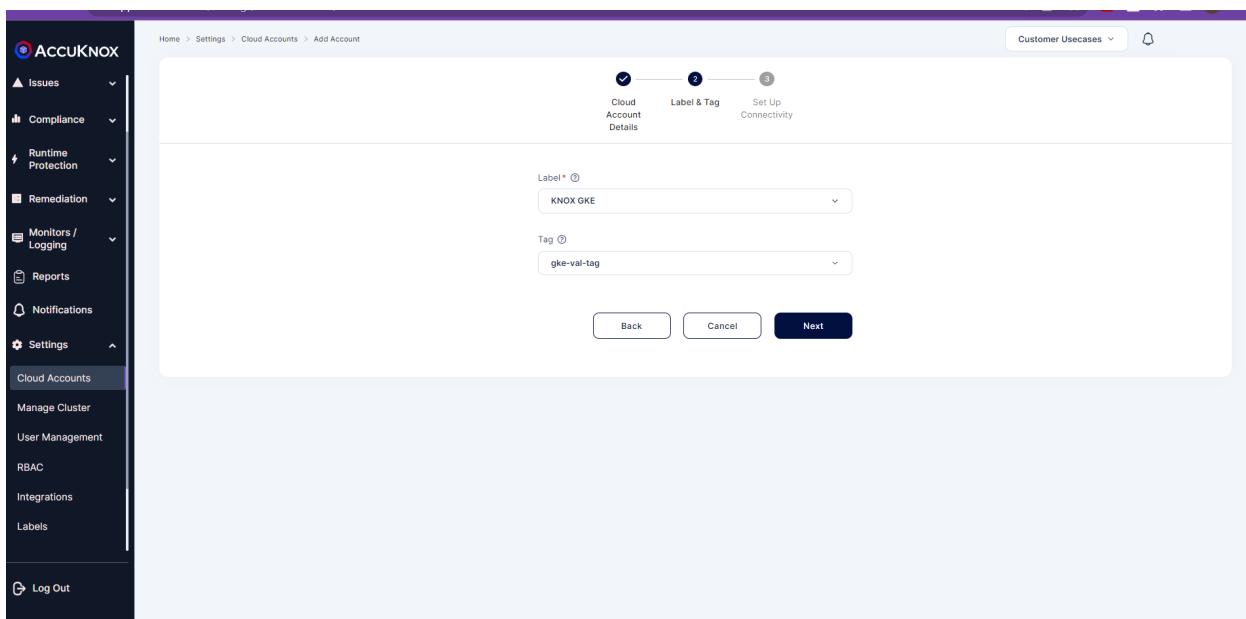
Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws:	2023-04-12	●	a month ago	-	<button>Scan</button> ⋮
azure	azure:	2023-04-21	●	18 days ago	-	<button>Scan</button> ⋮
aws	aws:	2023-05-04	●	5 days ago	2023-05-08	<button>Scan</button> ⋮
aws	aws:	2023-04-11	●	a month ago	2023-05-08	<button>Scan</button> ⋮
aws	aws:	2023-05-08	●	21 hours ago	2023-05-08	<button>Scan</button> ⋮

At the bottom, it says 'Total Count: 5' and 'Rows per page: 20' with navigation buttons.

- Select the Cloud Account type to GCP and Click Next

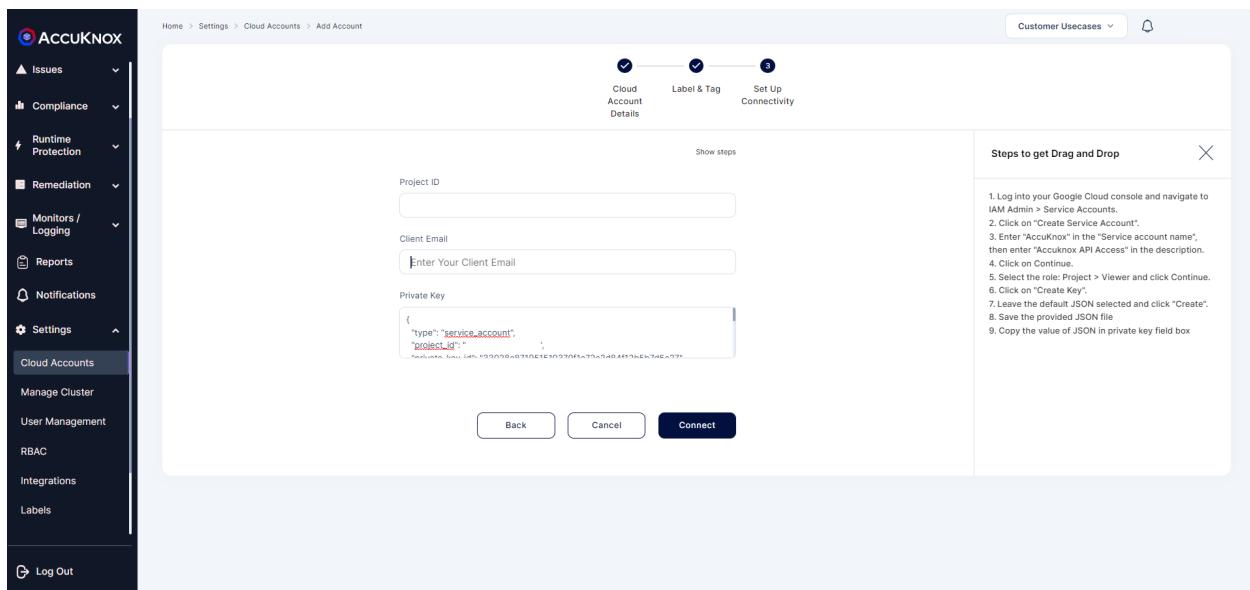


- Select the Labels and Tags and click Next



Note: If there are no labels and tags create new labels and tags via the settings

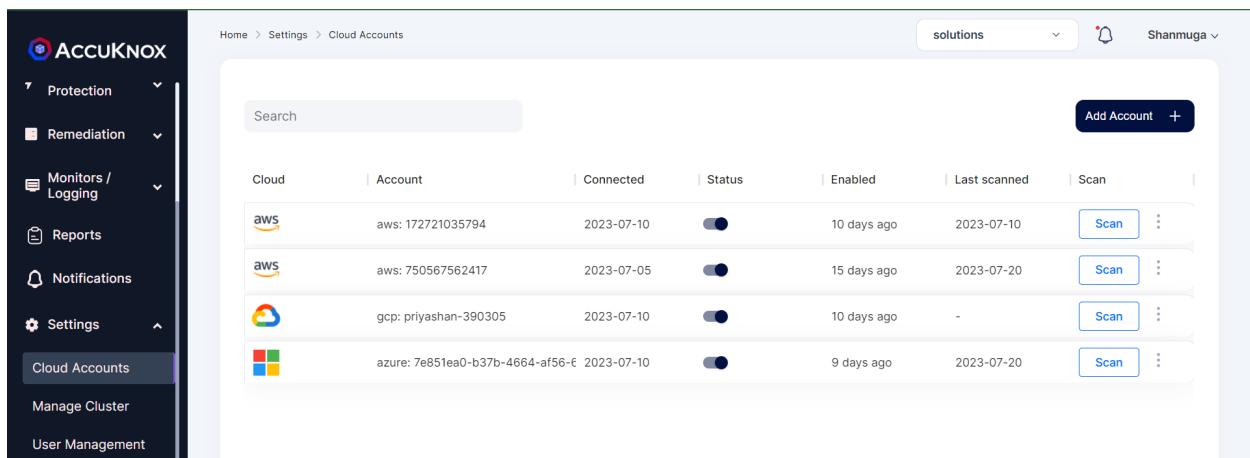
- Fill the Project ID, Client Email and Private Key then click Connect.



The screenshot shows the 'Cloud Account Details' step of the 'Add Account' wizard. The left sidebar has 'Cloud Accounts' selected. The main form has three tabs at the top: 'Cloud Account Details' (selected), 'Label & Tag', and 'Set Up Connectivity'. Below the tabs are fields for 'Project ID' (a dropdown menu), 'Client Email' (a text input with placeholder 'Enter Your Client Email'), and 'Private Key' (a code editor containing JSON). A 'Show steps' link is above the private key field. To the right is a panel titled 'Steps to get Drag and Drop' with a close button, containing numbered instructions from 1 to 9.

Note: For Client Email Id copy the mail id from the Service Account > Details section

- Check Settings → Cloud Accounts. You will see your cloud account is added successfully.



The screenshot shows the 'Cloud Accounts' dashboard. The left sidebar has 'Cloud Accounts' selected. The main area displays a table of connected accounts:

Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	<input checked="" type="checkbox"/>	10 days ago	2023-07-10	<button>Scan</button>
aws	aws: 750567562417	2023-07-05	<input checked="" type="checkbox"/>	15 days ago	2023-07-20	<button>Scan</button>
gcp	gcp: priyashan-390305	2023-07-10	<input checked="" type="checkbox"/>	10 days ago	-	<button>Scan</button>
azure	azure: 7e851ea0-b37b-4664-af56-e	2023-07-10	<input checked="" type="checkbox"/>	9 days ago	2023-07-20	<button>Scan</button>

CWPP Prerequisites

Minimum Resource required

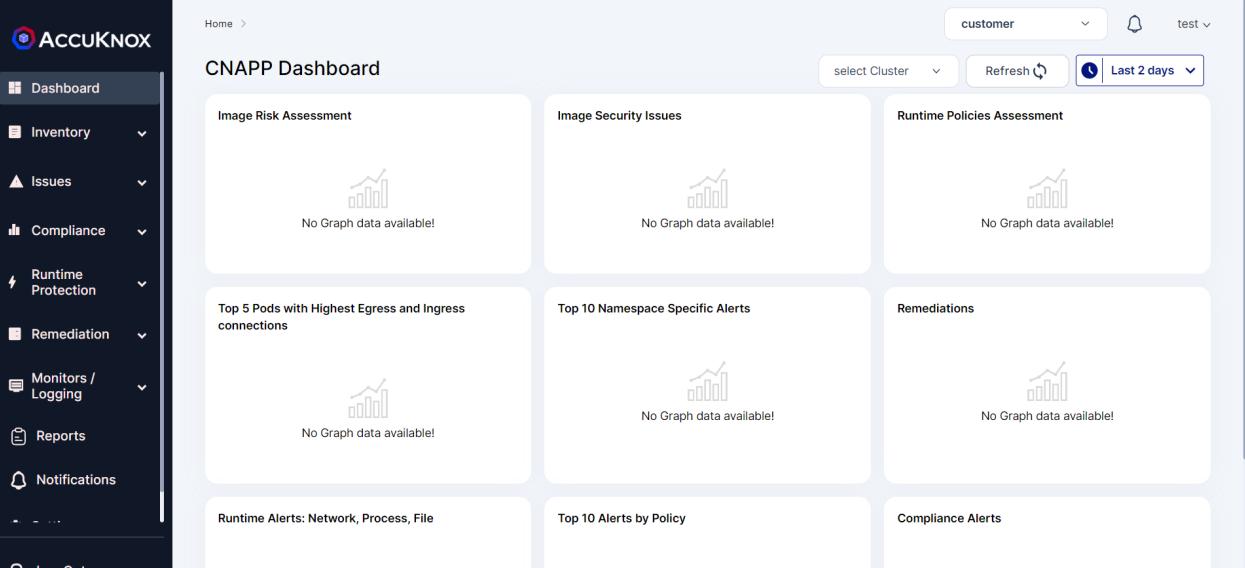
Deployments	Resource usage	Port	Connection Type
KubeArmor	CPU: 200 m, Memory: 200 Mi	-	-
Agents Operator	CPU: 50 m, Memory: 50 Mi	8081	Inbound/Outbound
Discovery Engine	CPU: 100 m, Memory: 100 Mi	-	-
Shared Informer Agent	CPU: 20 m, Memory: 50 Mi	3000	Inbound/Outbound
Feeder Service	CPU: 50 m, Memory: 100 Mi	3000	Inbound/Outbound
Policy Enforcement	CPU: 10 m, Memory: 20 Mi	443	Inbound/Outbound

- These ports need to be allowed through the firewall.

● Cluster Onboarding

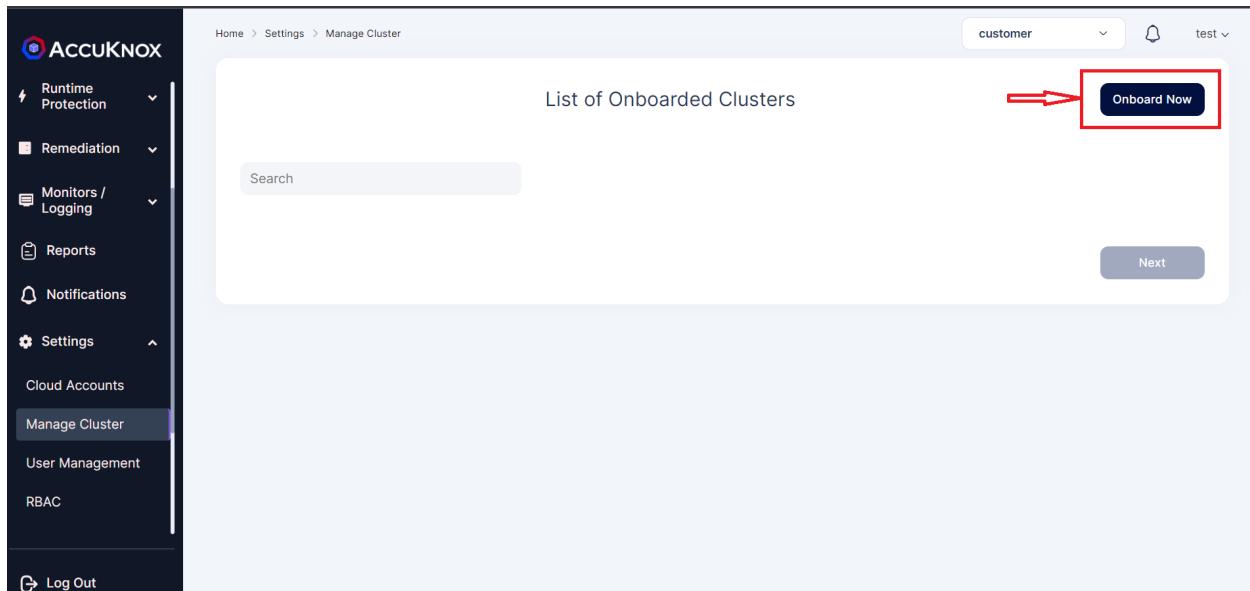
The cluster onboarding steps are the same for both managed and unmanaged clusters as follows:

Step 1: After signing up, the user will be taken to the CNAPP dashboard. Since there is no cluster or cloud account onboarded widgets will not have any data.



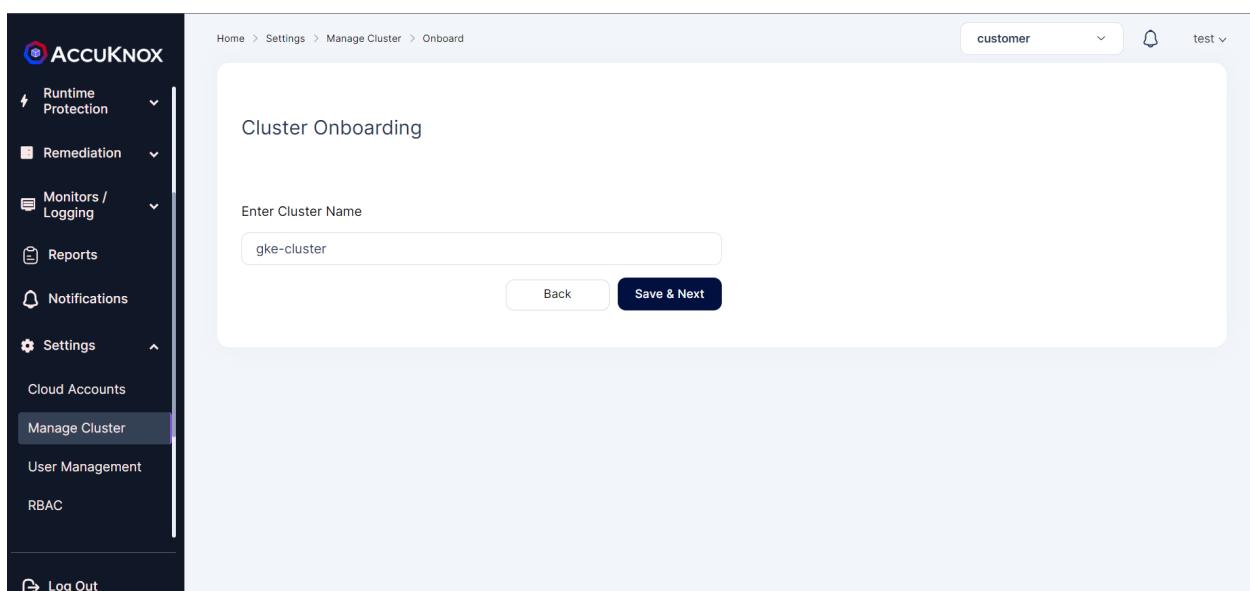
The screenshot shows the AccuKnox CNAPP Dashboard. The left sidebar contains navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Reports, Notifications, and Log Out. The main dashboard area has several sections: 'Image Risk Assessment', 'Image Security Issues', 'Runtime Policies Assessment', 'Top 5 Pods with Highest Egress and Ingress connections', 'Top 10 Namespace Specific Alerts', 'Remediations', 'Runtime Alerts: Network, Process, File', 'Top 10 Alerts by Policy', and 'Compliance Alerts'. Each section includes a small bar chart icon and the message 'No Graph data available!'

Step 2: Navigate to *Manage Cluster from Settings Tab*. From this page we can onboard the clusters running in various cloud platforms like GCP,AWS and Azure. We can also onboard unmanaged clusters set up locally in the on-premise environment or virtual machines. To onboard cluster select onboard now option



The screenshot shows the ACCUKNOX web interface. The left sidebar has a dark theme with white text. The 'Manage Cluster' option is selected and highlighted in purple. The main content area is titled 'List of Onboarded Clusters'. It features a search bar at the top and a large central area for listing clusters. In the top right corner, there is a 'customer' dropdown, a bell icon, and a 'test' dropdown. Below the dropdowns is a red rectangular box containing a black button labeled 'Onboard Now'. A red arrow points from the left towards this button.

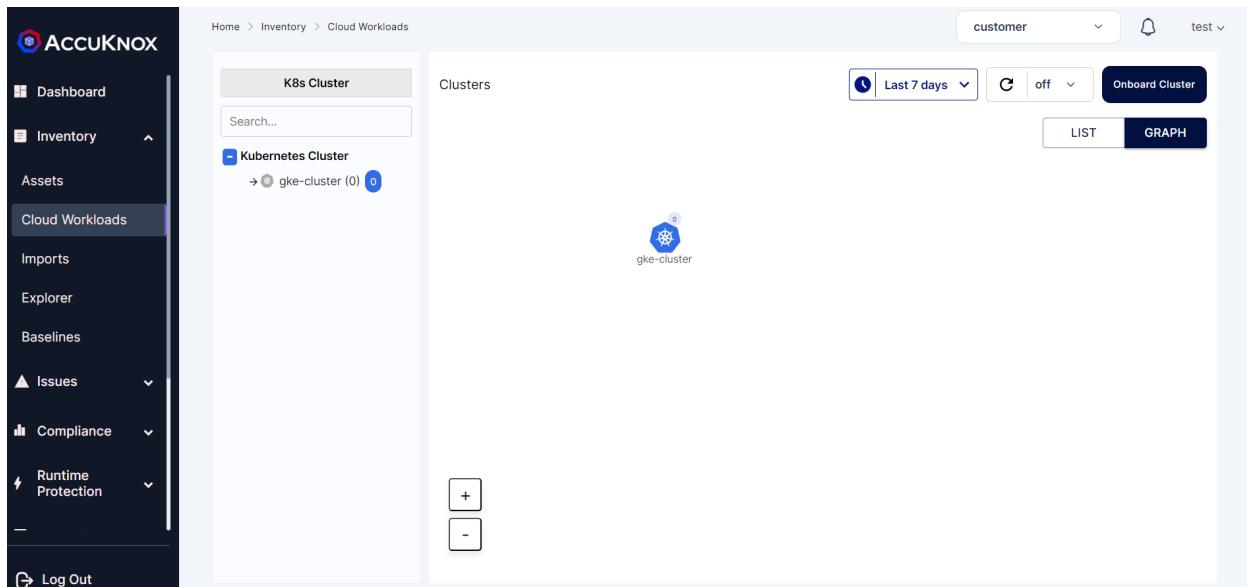
Step 3: In this screen, give any name to the cluster that you are going to onboard now.



The screenshot shows the 'Cluster Onboarding' step of the process. The left sidebar is identical to the previous screenshot. The main content area is titled 'Cluster Onboarding'. It has a form with a text input field labeled 'Enter Cluster Name' containing the value 'gke-cluster'. Below the input field are two buttons: 'Back' and a dark blue 'Save & Next' button. A red rectangular box surrounds the 'Save & Next' button, and a red arrow points from the left towards it.

Step 4: Onboarded Cluster without AccuKnox agents:

The onboarded cluster's workload details will not be visible as we have not installed AccuKnox agents. So next we will be installing AccuKnox agents.



Step 5: Installing KubeArmor and AccuKnox agents:

We are going to install KubeArmor and AccuKnox-agents to connect to the AccuKnox SaaS application.

Step 5.1: KubeArmor Installation:

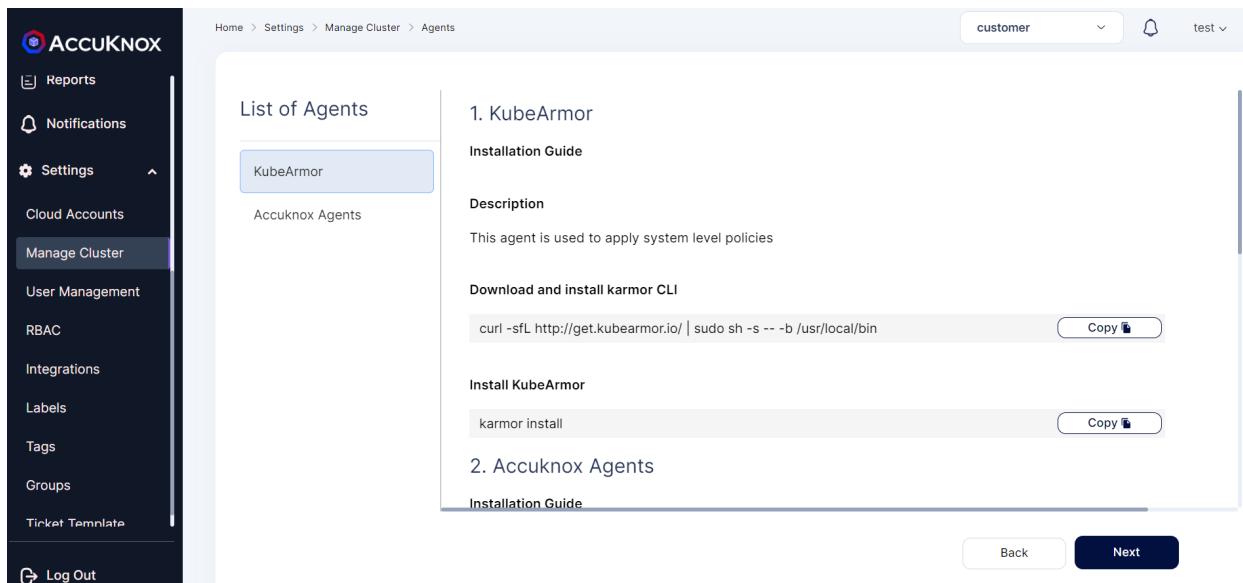
KubeArmor:

KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operation) of containers and nodes at the system level. With KubeArmor, a user can:

- Restrict file system access for certain processes
- Restrict what processes can be spawned within the pod
- Restrict the capabilities that can be used by the processes within the pod

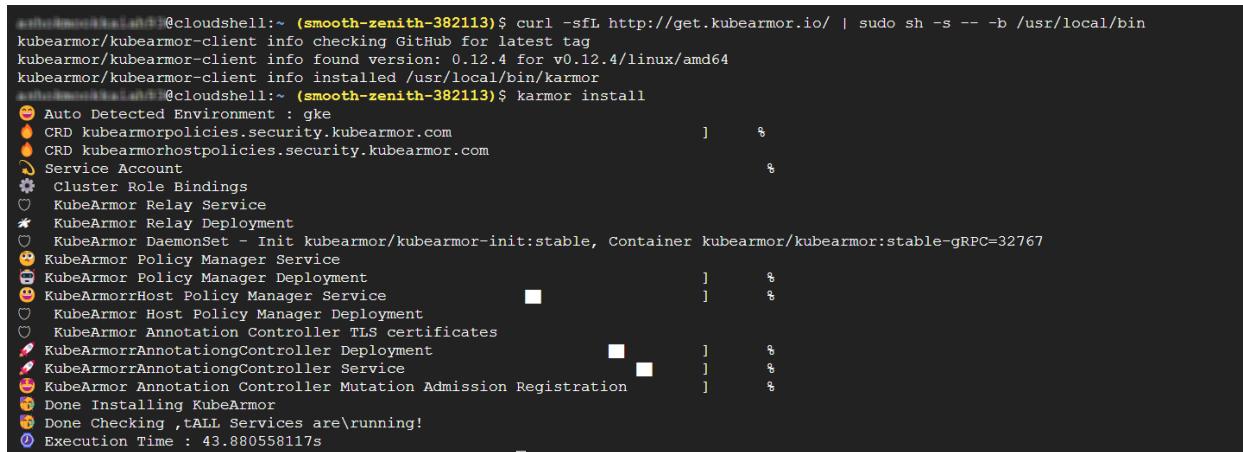
KubeArmor differs from seccomp-based profiles, wherein KubeArmor allows to dynamically set the restrictions on the pod. With seccomp, the restrictions must be

placed during the pod startup and cannot be changed later. KubeArmor leverages Linux Security Modules (LSMs) to enforce policies at runtime.



KubeArmor is installed using the following commands:

```
>> curl -sfL http://get.kubearmor.io/ | sudo sh -s -- -b /usr/local/bin
>> karmor install
```



```
@cloudshell:~ (smooth-zephyr-382113)$ curl -sfL http://get.kubearmor.io/ | sudo sh -s -- -b /usr/local/bin
kubearmor/kubearmor-client info checking GitHub for latest tag
kubearmor/kubearmor-client info found version: 0.12.4 for v0.12.4/linux/amd64
kubearmor/kubearmor-client info installed /usr/local/bin/karmor
@cloudshell:~ (smooth-zephyr-382113)$ karmor install
⌚ Auto Detected Environment : gke
🔥 CRD kubearmorpolicies.security.kubearmor.com
🔥 CRD kubearmorhostpolicies.security.kubearmor.com
⌚ Service Account
⚙️ Cluster Role Bindings
⌚ KubeArmor Relay Service
✳️ KubeArmor Relay Deployment
⌚ KubeArmor DaemonSet Init kubearmor/kubearmor-init:stable, Container kubearmor/kubearmor:stable-gRPC=32767
⌚ KubeArmor Policy Manager Service
⌚ KubeArmor Policy Manager Deployment
⌚ KubeArmorrHost Policy Manager Service
⌚ KubeArmorrHost Policy Manager Deployment
⌚ KubeArmor Host Policy Manager Deployment
⌚ KubeArmor Annotation Controller TLS certificates
🚀 KubeArmorrAnnotationController Deployment
🚀 KubeArmorrAnnotationController Service
⌚ KubeArmor Annotation Controller Mutation Admission Registration
⌚ Done Installing KubeArmor
⌚ Done Checking ,tALL Services are\running!
⌚ Execution Time : 43.880558117s
```

Step 5.2: AccuKnox-Agents installation:

After installing KubeArmor we are going to install AccuKnox Agents in the cluster.

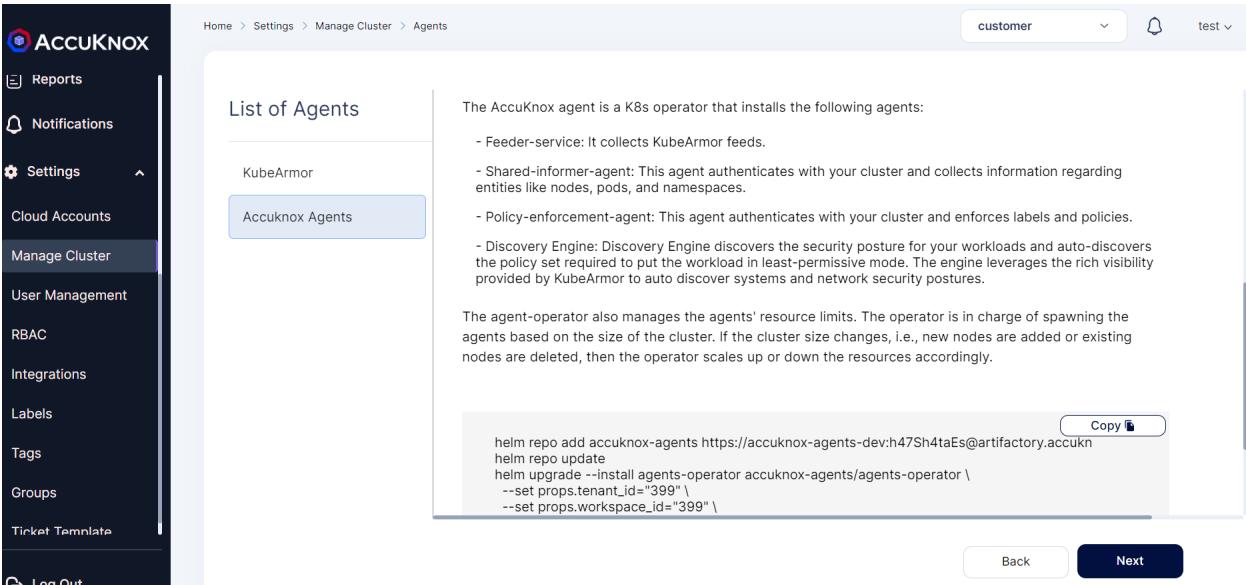
AccuKnox Agents:

1.KubeArmor: KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operation) of containers and nodes at the system level. KubeArmor dynamically set the restrictions on the pod. KubeArmor leverages Linux Security Modules (LSMs) to enforce policies at runtime.

2.Feeder Service: It collects the feeds from kubeArmor and relays to the app.

3.Shared Informer Agent: It collects information about the cluster like pods, nodes, namespaces etc.,

4.Policy Discovery Engine: It discovers the policies using the workload and cluster information that is relayed by a shared informer Agent.



The AccuKnox agent is a K8s operator that installs the following agents:

- Feeder-service: It collects KubeArmor feeds.
- Shared-informer-agent: This agent authenticates with your cluster and collects information regarding entities like nodes, pods, and namespaces.
- Policy-enforcement-agent: This agent authenticates with your cluster and enforces labels and policies.
- Discovery Engine: Discovery Engine discovers the security posture for your workloads and auto-discovers the policy set required to put the workload in least-permissive mode. The engine leverages the rich visibility provided by KubeArmor to auto discover systems and network security postures.

The agent-operator also manages the agents' resource limits. The operator is in charge of spawning the agents based on the size of the cluster. If the cluster size changes, i.e., new nodes are added or existing nodes are deleted, then the operator scales up or down the resources accordingly.

```
helm repo add accuknox-agents https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents
helm repo update
helm upgrade --install agents-operator accuknox-agents/agents-operator \
--set props.tenant_id="399" \
--set props.workspace_id="399" \
```

AccuKnox Agents can be installed using the following command:

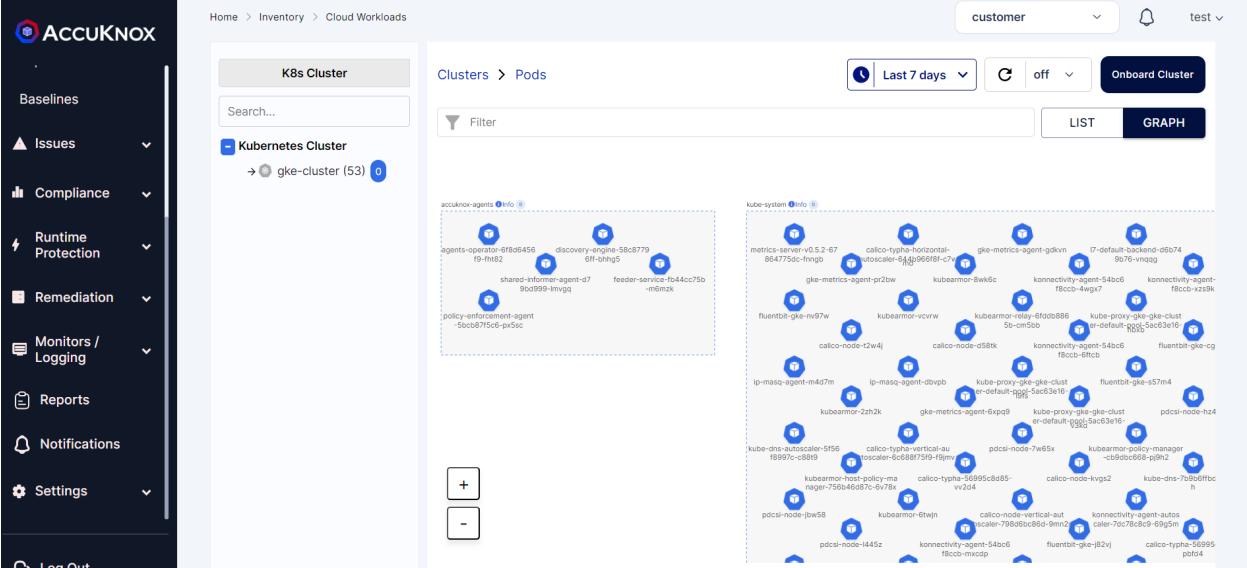
```
helm repo add accuknox-agents https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents
helm repo update
helm upgrade --install agents-operator accuknox-agents/agents-operator \
```

```
--set props.tenant_id="399" \
--set props.workspace_id="399" \
--set props.cluster_name="gke-cluster" \
--set props.CLUSTER_NAME="gke-cluster" \
--set props.cluster_id="1814" \
--set props.helm_repo="accuknox-agents" \
                                         --set
props.helm_repo_url="https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents" \
--set props.docker_repo_host="artifactory.accuknox.com" \
--set props.docker_repo_username="accuknox-agents-image" \
--set props.docker_repo_password="SjnnJxs3fk" \
--create-namespace -n accuknox-agents
```

```
@cloudshell:~ (smooth-zenith-382113)$
helm repo add accuknox-agents https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents
helm repo update
helm upgrade --install agents-operator accuknox-agents/agents-operator \
--set props.tenant_id="399" \
--set props.workspace_id="399" \
--set props.cluster_name="gke-cluster" \
--set props.CLUSTER_NAME="gke-cluster" \
--set props.cluster_id="1814" \
--set props.helm_repo="accuknox-agents" \
--set props.helm_repo_url="https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents" \
--set props.docker_repo_host="artifactory.accuknox.com" \
--set props.docker_repo_username="accuknox-agents-image" \
--set props.docker_repo_password="SjnnJxs3fk" \
--create-namespace -n accuknox-agents
"accuknox-agents" has been added to your repositories
Hang tight while we grab the latest from your chart repositories...
...Successfully got an update from the "accuknox-agents" chart repository
Update Complete. *Happy Helm-ing!*
Release "agents-operator" does not exist. Installing it now.
NAME: agents-operator
LAST DEPLOYED: Wed Mar 29 14:41:20 2023
NAMESPACE: accuknox-agents
STATUS: deployed
REVISION: 1
TEST SUITE: None
```

Note: In the above command workspace_id,cluster_name,tenant_id are specific to this example and it will vary based on the cluster

Step 6: After installing all the AccuKnox agents the cluster is onboarded successfully into the SaaS application. We can see the workload details of the onboarded cluster by Navigating to Inventory->cloud Workloads option



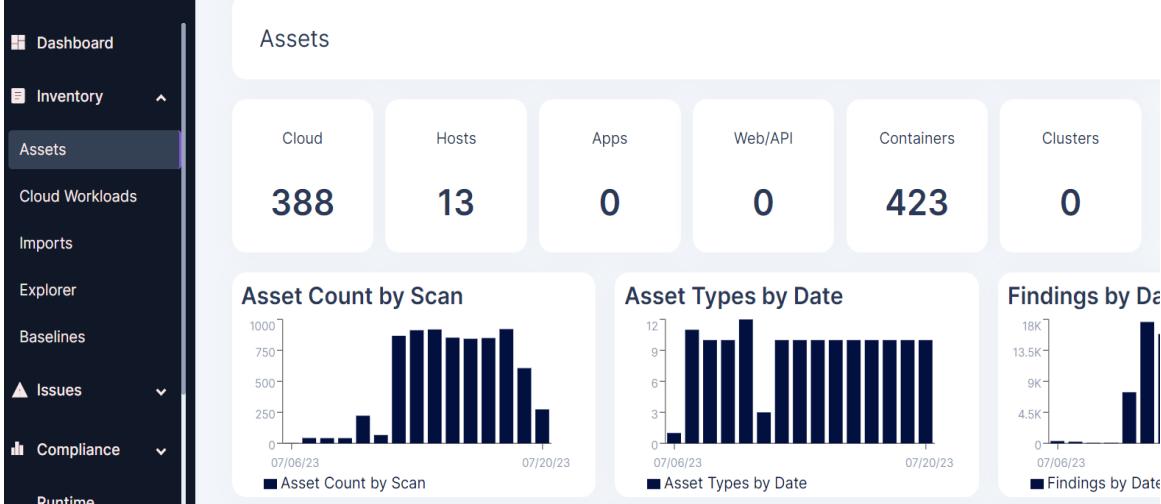
The screenshot shows the ACCUKNOKX platform's Cloud Workloads section. On the left, a sidebar navigation includes Baselines, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Reports, Notifications, Settings, and Log Out. The main area displays a "Clusters > Pods" view for a "Kubernetes Cluster" named "gke-cluster (53)". A search bar at the top allows filtering by "customer" and "test". Below the search bar are buttons for "Last 7 days", "C off", and "Onboard Cluster". The pod list is presented in two sections: "accuknox-agents" and "kube-system". Each pod entry includes a blue circular icon with a white symbol, the pod name, and its status.

● Asset Inventory

○ Cloud Assets

■ How to find a particular asset

- First navigate to the Assets screen under Inventory:



The screenshot shows the ACCUKNOKX platform's Assets screen under the Inventory section. The left sidebar includes Dashboard, Inventory (Assets selected), Cloud Workloads, Imports, Explorer, Baselines, Issues, Compliance, and Runtime. The main area displays a summary of asset counts across six categories: Cloud (388), Hosts (13), Apps (0), Web/API (0), Containers (423), and Clusters (0). Below this are three data visualizations: "Asset Count by Scan" (a bar chart showing asset counts per scan date from July 6 to July 20, 2023), "Asset Types by Date" (a bar chart showing the number of asset types per date), and "Findings by Date" (a bar chart showing findings per date).

- Now, if the name of the Asset is known, we can use the search bar to search for the Asset:

Search: bucket

	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ...
<input type="checkbox"/>	newbucketdirty	ADITYA	0	0/0		2023-07-10	s3bucket	4
<input type="checkbox"/>	production-blog-awsgoa...	ADITYA	0	0/0		2023-07-10	s3bucket	5
<input type="checkbox"/>	dev-blog-awsgoat-buck...	ADITYA	0	0/0		2023-07-10	s3bucket	5
<input type="checkbox"/>	do-not-delete-awsgoat-...	ADITYA	0	0/0		2023-07-10	s3bucket	5
<input type="checkbox"/>	thisisthebucket2	ADITYA	0	0/0	1	2023-07-10	s3bucket	5
<input type="checkbox"/>	config-bucket-7505675...	ADITYA	0	0/0		2023-07-10	s3bucket	4

- Or if the name is not known but the Asset type is known, the Filter by Asset drop down can be used to filter the assets list. The search functionality can also be used on the filtered result:

Search: aws...

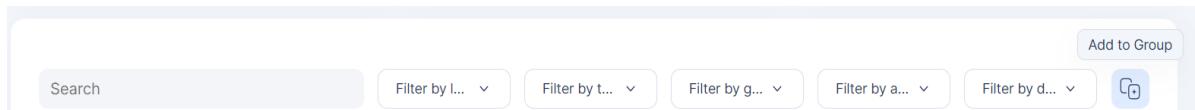
	Asset	Label	Targets	Baseline	Total Vulnerabilities	Asset type	Data typ...
<input type="checkbox"/>	project-vpc	AWS100723	0	0/0		aws...	da...
<input type="checkbox"/>	vpc-069ee98298179beff	ADITYA	0	0/0		aws...	da...
<input type="checkbox"/>	AWS_GOAT_VPC	ADITYA	0	0/0		aws...	da...
<input type="checkbox"/>	vpc-0ac830ca18c12037a	AWS100723	0	0/0		aws...	da...
<input type="checkbox"/>	vpc-01c32594e0ea8b87d	ADITYA	0	0/0		aws...	da...

■ How to group assets

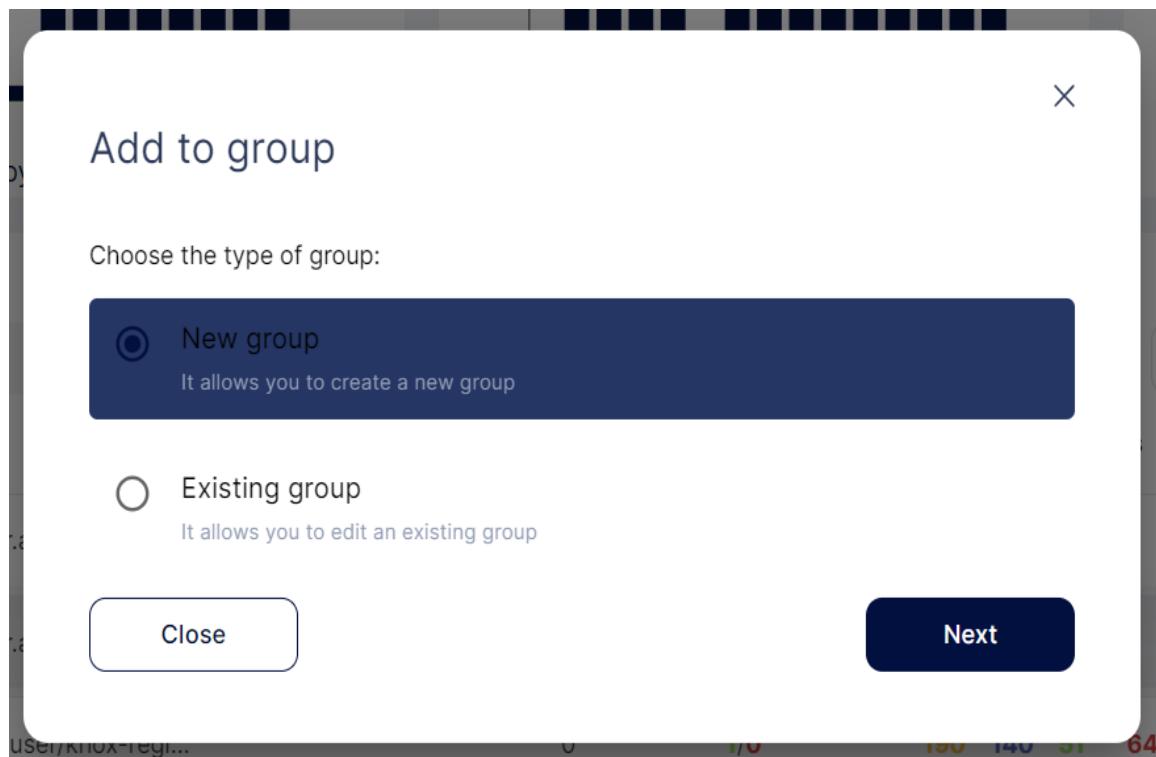
- Select the assets to be grouped in the Assets screen:

	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type
<input type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0	29 50 6 9	2023-05-26	container
<input checked="" type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	2/0		2023-05-22	container
<input type="checkbox"/>	accuknoxuser/knox-regi...		0	1/0	190 140 51 64	2023-06-14	container
<input checked="" type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0	15 10	2023-06-14	container
<input checked="" type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0		2023-06-09	container
<input type="checkbox"/>	default	CHIRAGAZURE	0	0/0		2023-07-20	azuresubnet
<input checked="" type="checkbox"/>	accuknox-ui-softaculous...	CHIRAGAZURE	0	0/0		2023-07-20	azureresource

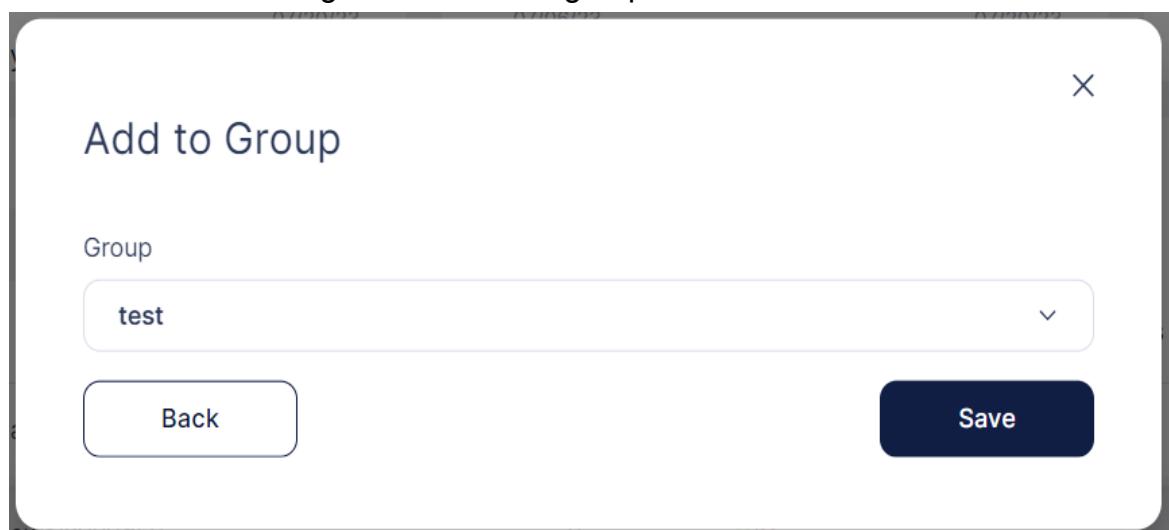
- Click on the Add to group button on the top right:



- In the pop-up that follows, create a new group or add to an existing group:



- After entering a name for the group or selecting an existing group, click on Save to finish adding the assets to a group:



- Now, filtering by group allows us to see only the assets that were added to the group:

Search Filter by l... Filter by t... test X Filter by a... Filter by d...

	Asset	Label	Targets	Baseline	Last Scan da...	Asset type	Data typ...
<input type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	2/0			
<input type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0			
<input type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0			
<input type="checkbox"/>	accuknox-ui-softaculous...	CHIRAGAZURE	0	0/0			
<input type="checkbox"/>	public.ecr.aws/k9v9d5v...		0	1/0			

Assets	Last Scan date	Asset type	Data type
aws-1	2023-05-22	container	2
aws-2	2023-06-14	container	3
aws-3			
aws-4	2023-06-09	container	2
aws11			
test	2023-07-20	azureresourcegroup	0
azureresourcegroup			
testdemo			
samplecldwis...	2023-05-27	container	3
samplecldwis...	594	36	280

■ How to search asset by label

- To find all the assets that have a particular label, select the label from the Filter by Label drop down in the Assets screen:

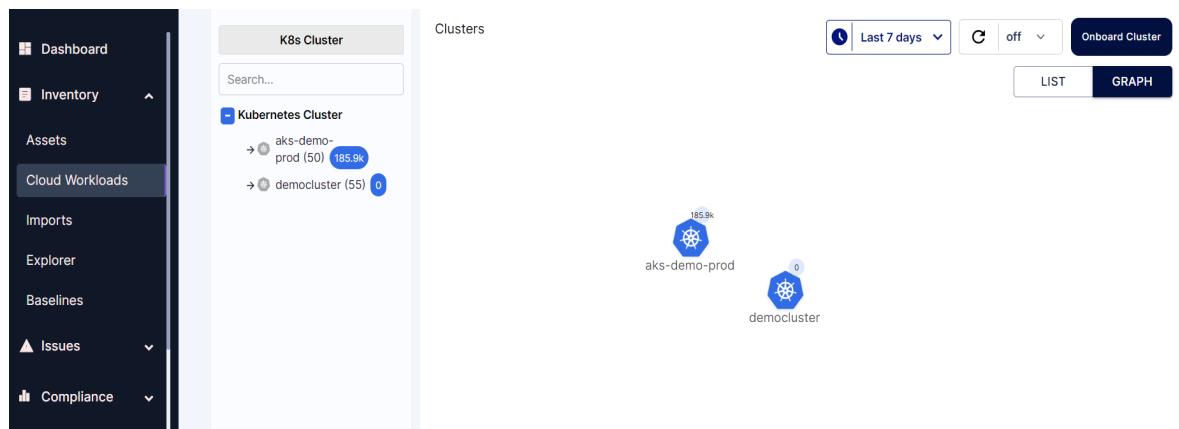
Asset	Label	Assets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ...
project-vpc	AWS100723	AWS100723	0/0	0	2023-07-10	aws vpc	0
172721035794:us-east-1	AWS100723	CGJUNE15	0/1	0	2023-07-10	security hub	0
AWSServiceRoleForAma...	AWS100723	CHIRAGAZURE	0/0	0	2023-07-10	aws iam role	0
172721035794:eu-north-1	AWS100723	DEMOAZURE14	0/0	0	2023-07-10	cloudsploit aut...	0
project-subnet-public2-...	AWS100723	GCP100723	0/0	0	2023-07-10	aws s3 bucket	0
default	AWS100723	GURUAZURE	0/0	0	2023-07-10	cloudsploit autom...	0
AWS-accu-user	AWS100723	MSAZUREGURU...	0/0	0	2023-07-10	aws subnet	0
			0/0	0	2023-07-10	aws security group	0
			0/0	0	2023-07-10	aws iam user	1

- To further refine the results, we can use the search bar or add additional filters such as Assets

● Cloud Workload

● How to find graph view of clusters

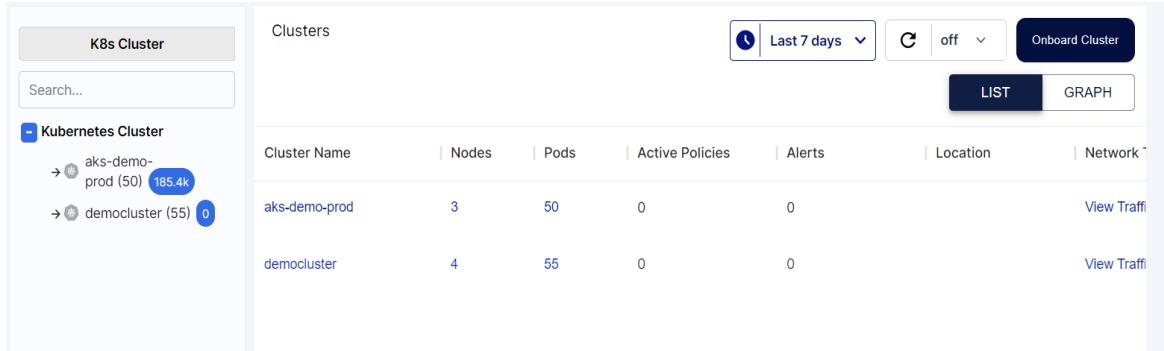
- o Navigate to Cloud Workloads screen under Inventory to view the clusters that have been onboarded:



The screenshot shows the ACCUKNOX interface with the following details:

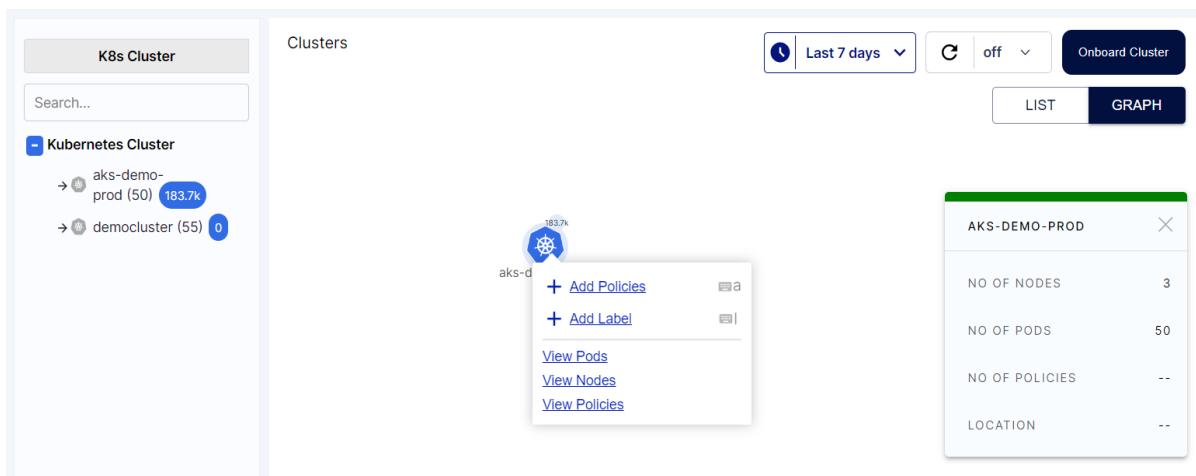
- Left Sidebar:** Includes sections for Dashboard, Inventory (selected), Assets, Cloud Workloads (selected), Imports, Explorer, Baselines, Issues, and Compliance.
- Middle Section - K8s Cluster:** A search bar with placeholder "Search...". Below it, a list of Kubernetes Clusters:
 - Kubernetes Cluster:** Contains two items:
 - aks-demo-prod (50) 185.9k
 - democluster (55) 0
- Right Section - Clusters:** A summary of onboarded clusters:
 - aks-demo-prod: 185.9k
 - democluster: 0
- Top Right Controls:** Filter by "Last 7 days", status "off", "Onboard Cluster" button, and "GRAPH" tab (which is selected).

- How to find list view of clusters
 - Click on the LIST option in the top right of the Cloud Workloads screen to get a list view of all the clusters



The screenshot shows the 'Clusters' section of the Cloud Workloads interface. On the left, there's a sidebar with a search bar and a 'Kubernetes Cluster' section containing two items: 'aks-demo-prod (50)' with 185.4k members and 'democluster (55)' with 0 members. The main area is titled 'Clusters' and contains a table with columns: Cluster Name, Nodes, Pods, Active Policies, Alerts, Location, and Network. Two rows are listed: 'aks-demo-prod' (3 nodes, 50 pods, 0 policies, 0 alerts) and 'democluster' (4 nodes, 55 pods, 0 policies, 0 alerts). Each row has a 'View Traffic' button on the right.

- The view can be freely switched between LIST and GRAPH as required
- How to find details on cluster
- Clicking on any of the clusters in the Cloud Workloads screen gives more information about the cluster:

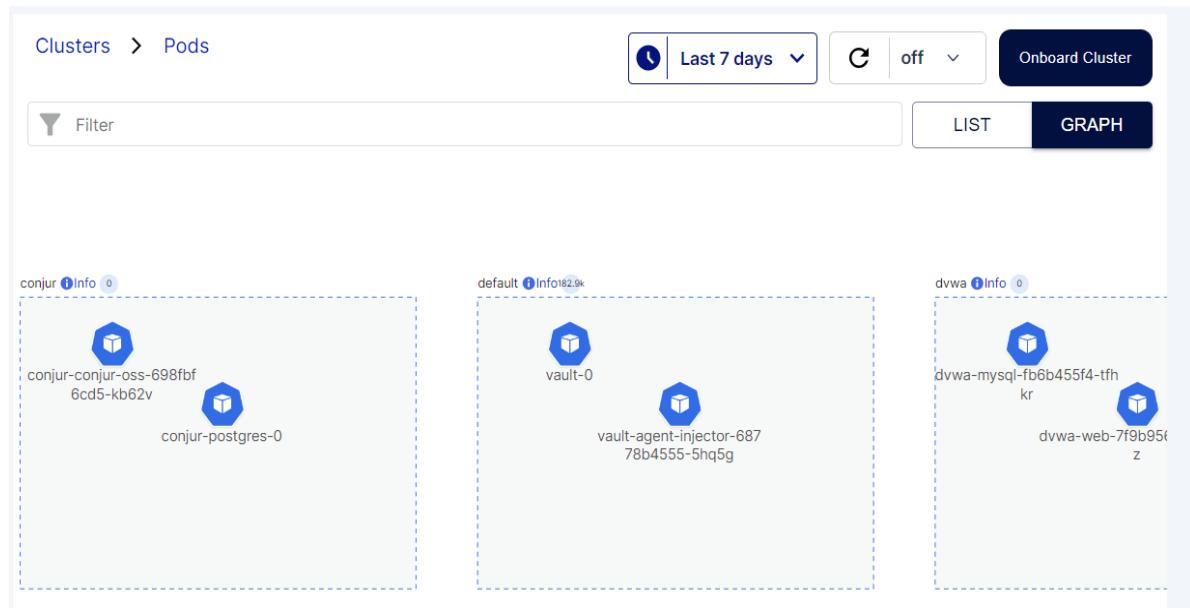


The screenshot shows the same interface as above, but with a modal window open over the 'aks-demo-prod' cluster row. The modal is titled 'AKS-DEMO-PROD' and contains the following details:

NO OF NODES	3
NO OF PODS	50
NO OF POLICIES	--
LOCATION	--

Below the modal, there are buttons for '+ Add Policies', '+ Add Label', 'View Pods', 'View Nodes', and 'View Policies'. The cluster table row for 'aks-demo-prod' now has a blue background and a small gear icon above it, indicating it is selected.

- Click on View Pods to view the Pods present in the cluster classified according to the namespaces they are present in:



The screenshot shows the AccuKnox interface for managing clusters. At the top, there's a navigation bar with 'Clusters > Pods'. Below it are several filter and search options: a clock icon for time range ('Last 7 days'), a gear icon for status ('off'), and a button to 'Onboard Cluster'. There are also 'Filter' and 'LIST/GRAFH' buttons. The main area displays three distinct pods, each with a dashed border:

- conjur** (Info 0): Contains two containers: 'conjur-conjur-oss-698fbf' (6cd5-kb62v) and 'conjur-postgres-0'.
- default** (Info 182.9k): Contains two containers: 'vault-0' and 'vault-agent-injector-687' (78b4555-5hq5g).
- dvwa** (Info 0): Contains two containers: 'dvwa-mysql-fb6b455f4-tfh' (kr) and 'dvwa-web-7f9b95c' (z).

- Double click on the pods to view the containers present in them. Select any container to view more details:



The screenshot shows the AccuKnox interface for managing clusters, specifically navigating to the 'Containers' page for the 'conjur-oss' pod. The top navigation bar shows 'Clusters > Pods > Containers'. The main area lists two containers: 'conjur-oss' and 'conjur-nginx'. On the right, a detailed view of the 'conjur-oss' container is displayed in a modal window:

CONJUR-OSS	
IMAGE	docker.io/cyberark/conjur:latest
PORT	8080
SERVICE	conjur-conjur-oss

- Notice the Hierarchical structure above: Clusters > Pods > Containers. Clicking on any of them allows navigation through the different screens.
- Navigate back to the Clusters screen and select a cluster and then click on View Nodes. In the nodes screen, we can view the nodes used by the cluster. Selecting a node gives more information about it:

Clusters > Nodes

Last 7 days
Onboard Cluster

LIST
GRAPH

+
aks-agentpool-16128849-v
mss000001
aks-agentpool-16128849-v
mss000000
aks-agentpool-16128849-v
mss000002

+ Add Policies
+ Add Label
[View Policies](#)

AKS-AGENTPOOL-16128849-VMSS000002

LABELS	22
NO OF PODS	17
NO OF POLICIES	--
CONTAINERS	25
ALERTS	--
LOCATION	--

- We can also double click on the node to view the Pods running in them
- View Policies can be clicked to jump to the Policies screen to show the policies for the selected cluster or pod:

- Dashboard
- Inventory
- Issues
- Compliance
- Runtime Protection
- CWPP Dashboard
- App Behavior
- Policies
- Remediation
- Monitors / Logging

Policies

K8s
aks-demo-prod
Namespace
Policy Type
Status

Search

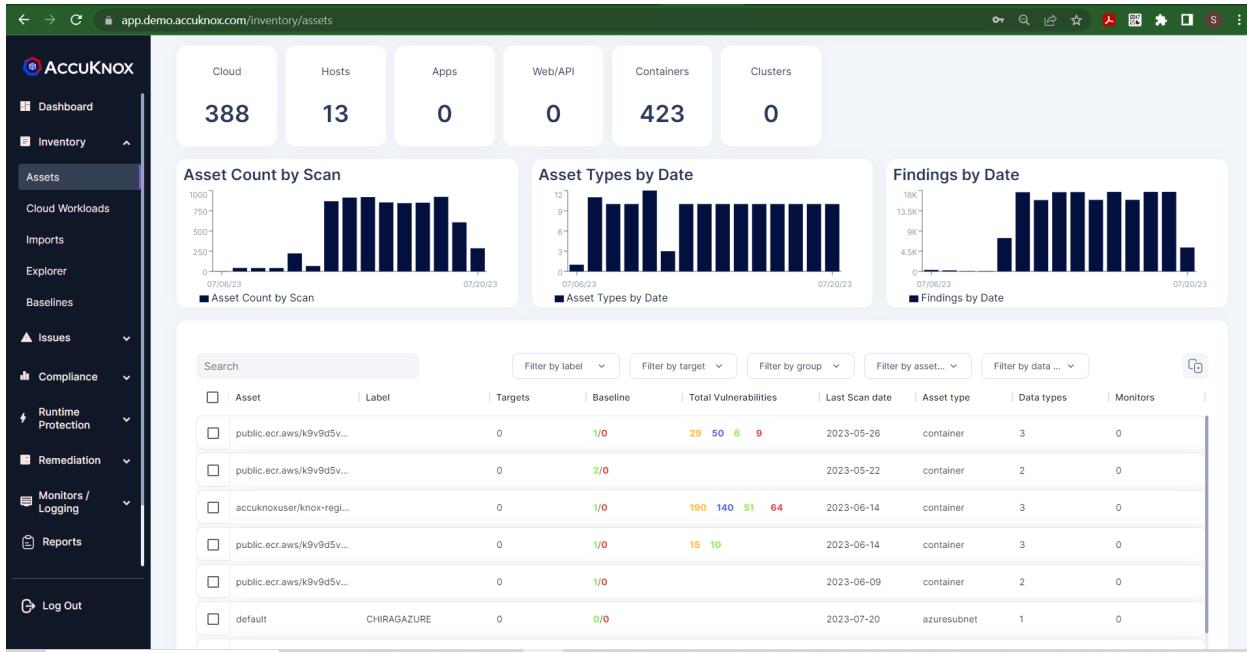
All (249)	Discovered (49)	Hardening (195)	Custom (5)	Ignore	Delete
<input type="checkbox"/> ksp-vault-protect (v1)					
<input type="checkbox"/> harden-wordpress-pkg-mngr-exec (v5)					
<input type="checkbox"/> harden-wordpress-file-integrity-monito					
<input type="checkbox"/> autopol-system-1021014936					

● Misconfigurations

- Where to find misconfigurations

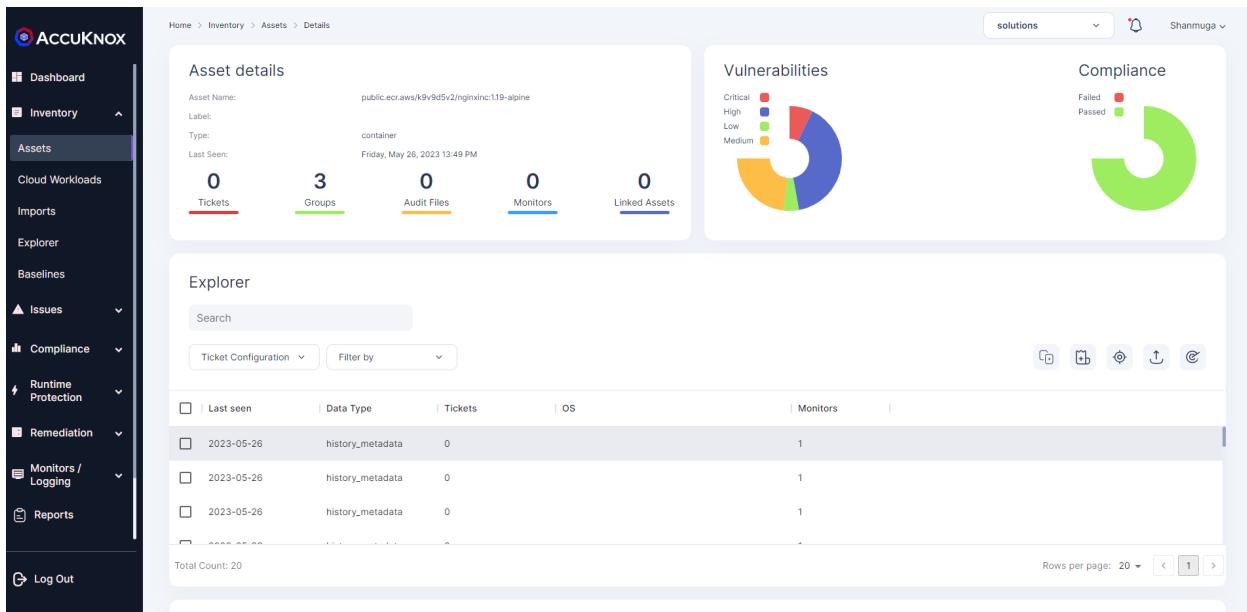
- Asset Detail Page

Once we have onboard the Cloud Account, we can navigate to the Inventory → Asset page where we can see the List of Assets with vulnerabilities.



Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan Date	Asset Type	Data Types	Monitors
public.ecr.aws/k9v9d5v...		0	1/0	29 50 6 9	2023-05-26	container	3	0
public.ecr.aws/k9v9d5v...		0	2/0		2023-05-22	container	2	0
accuknoxuser/knox-regi...		0	1/0	190 140 51 64	2023-06-14	container	3	0
public.ecr.aws/k9v9d5v...		0	1/0	15 10	2023-06-14	container	3	0
public.ecr.aws/k9v9d5v...		0	1/0		2023-06-09	container	2	0
default	CHIRAGAZURE	0	0/0		2023-07-20	azuresubnet	1	0

From the Asset listing click any Asset for the Asset Details.



Asset details

Asset Name: public.ecr.aws/k9v9d5v2/nginxinc:119-alpine

Type: container

Last Seen: Friday, May 26, 2023 13:49 PM

0 Tickets	3 Groups	0 Audit Files	0 Monitors	0 Linked Assets
-----------	----------	---------------	------------	-----------------

Vulnerabilities



Compliance



Explorer

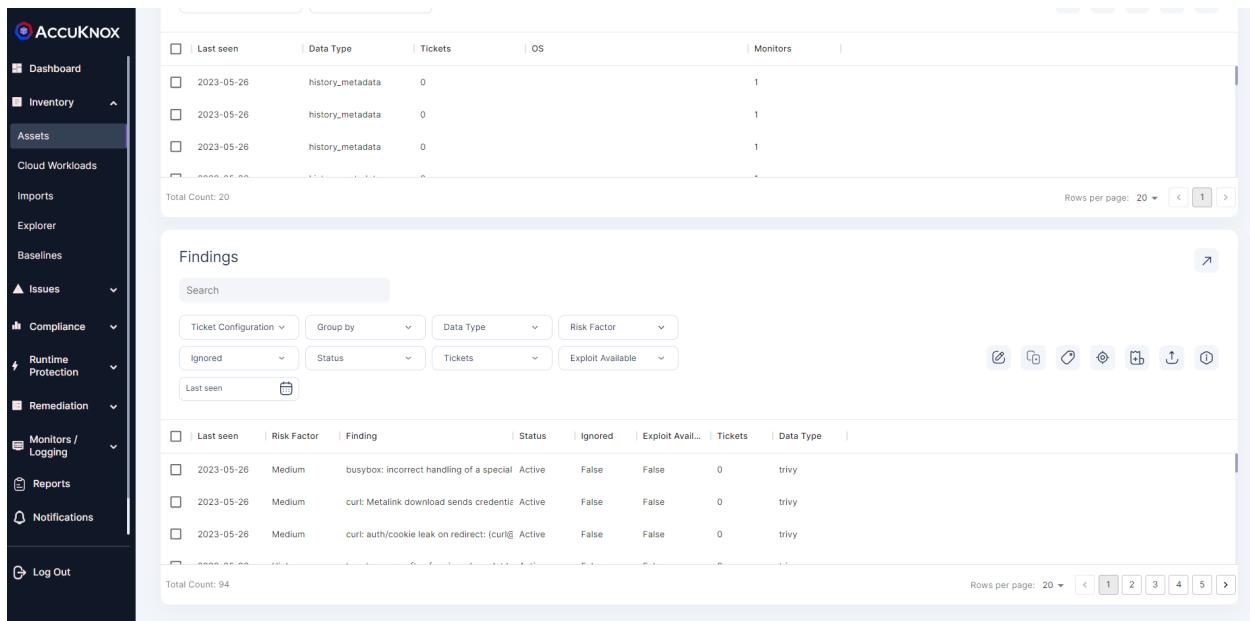
Search:

Ticket Configuration:

Last seen	Data Type	Tickets	OS	Monitors
2023-05-26	history_metadata	0		1
2023-05-26	history_metadata	0		1
2023-05-26	history_metadata	0		1

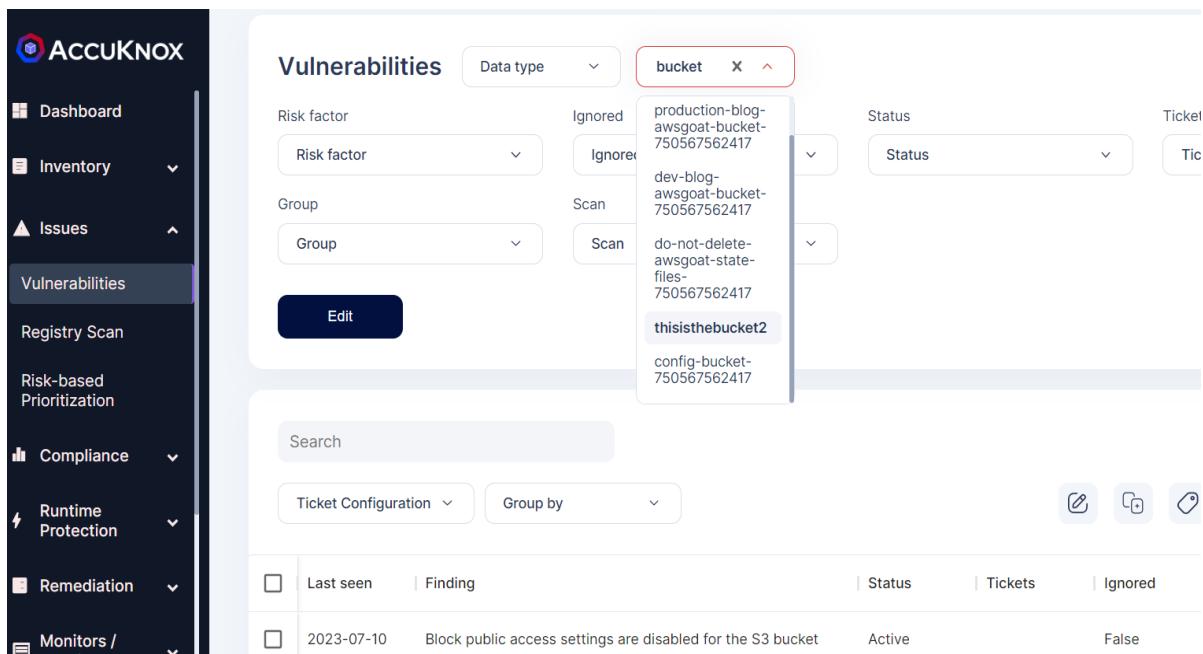
Total Count: 20 Rows per page: 20

Scroll down for the Findings



Where you can see the Risk Factor for the particular Findings.

- Issue Page
 - Navigate to Vulnerabilities screen under Issues and select an Asset from the drop down at the top to view all misconfigurations associated with the Asset:



- You can also type in the Assets drop down to search for a particular Asset

- How to group by Asset, say s3 and find misconfiguration

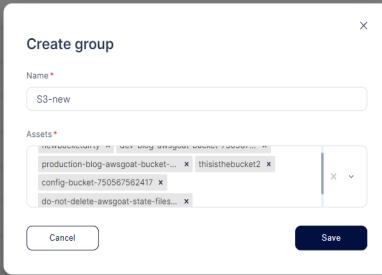
Step1 : In the Assets screen under Inventory, filter by Assets to view only the S3 buckets:

Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ...
newbucketdirty	ADITYA	0	0/0			awsiamrole	2023-07-10
production-blog-awsgoat...	ADITYA	0	0/0			s3bucket	2023-07-10
dev-blog-awsgoat-buck...	ADITYA	0	0/0			s3bucket	2023-07-10
do-not-delete-awsgoat-...	ADITYA	0	0/0			s3bucket	2023-07-10
thisisthebucket2	ADITYA	0	0/0	1		s3bucket	2023-07-10
config-bucket-7505675...	ADITYA	0	0/0			s3bucket	2023-07-10

Step2 : Select all and Add to a group by clicking the Add to group button:

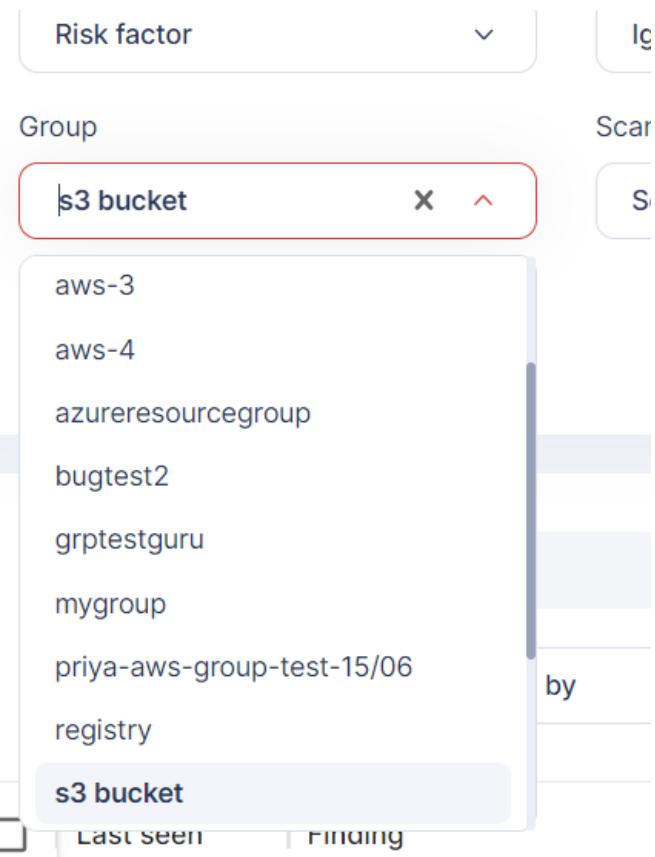
Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ...
newbucketdirty	ADITYA	0	0/0		2023-07-10	s3bucket	4
production-blog-awsgoat...	ADITYA	0	0/0		2023-07-10	s3bucket	5
dev-blog-awsgoat-buck...	ADITYA	0	0/0		2023-07-10	s3bucket	5
do-not-delete-awsgoat-...	ADITYA	0	0/0		2023-07-10	s3bucket	5
thisisthebucket2	ADITYA	0	0/0	1	2023-07-10	s3bucket	5
config-bucket-7505675...	ADITYA	0	0/0		2023-07-10	s3bucket	4

Step3: Click on Save



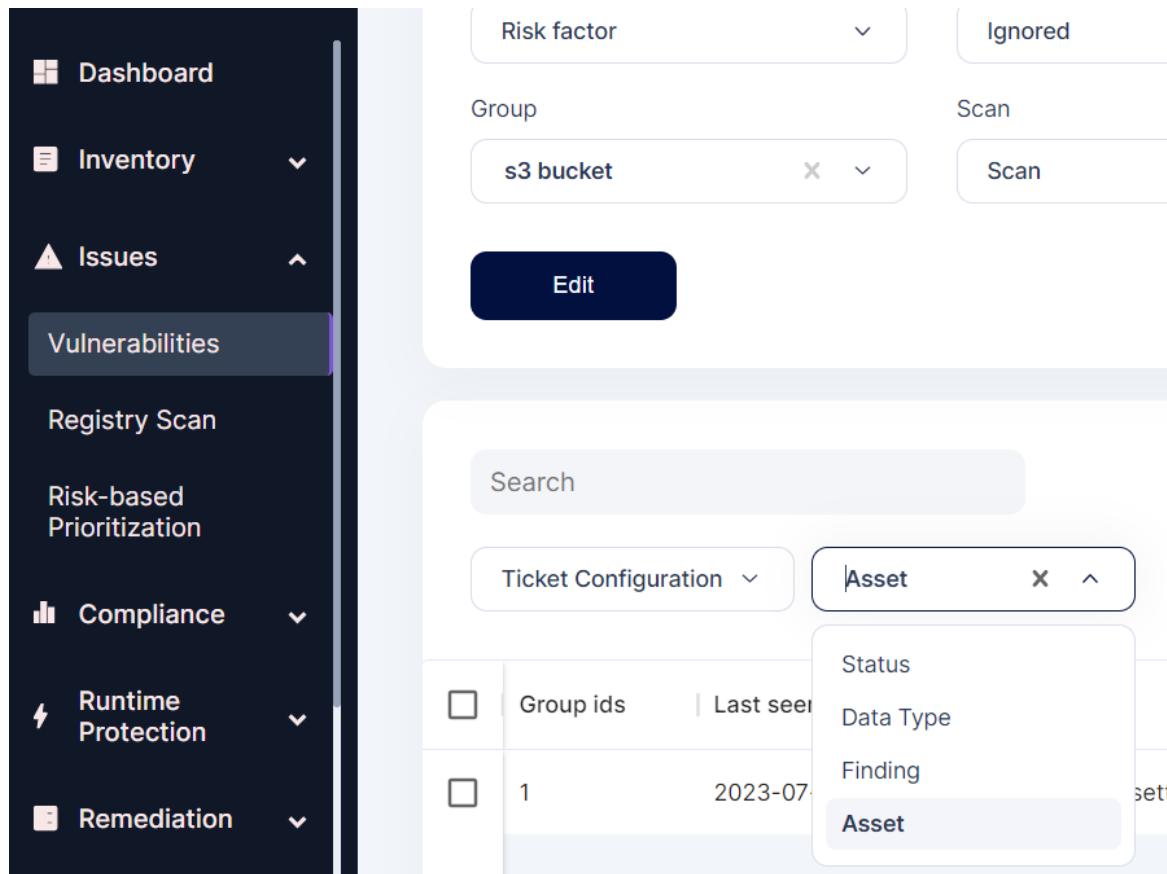
The screenshot shows the ACCUKNOX web interface. On the left, a sidebar menu includes 'Protection', 'Remediation', 'Monitors / Logging', 'Reports', 'Notifications', 'Settings', 'Cloud Accounts', 'Manage Cluster', 'User Management', 'RBAC', 'Integrations', 'Labels', 'Tags', 'Groups' (which is selected), and 'Ticket Template'. Below the sidebar, there's a 'Log Out' link. The main area is titled 'Groups' and shows a table with columns: Name, Tickets, Assets, Findings, Baseline, Date, Time, and Monitors. The table lists groups like 'aws-1' through 'aws-4', 'aws11', 'test', 'azureresourcegroup', 'testdemo', 'sampleoldwise', and 's3 bucket'. A search bar at the top of the table says 'Search'. At the top right, there are buttons for 'Create group' and 'Delete'. The bottom right of the main area has a 'Rows per page' dropdown set to 20.

Step 4 : Click on Issues -> Vulnerabilities and select the group that was created from the drop down:



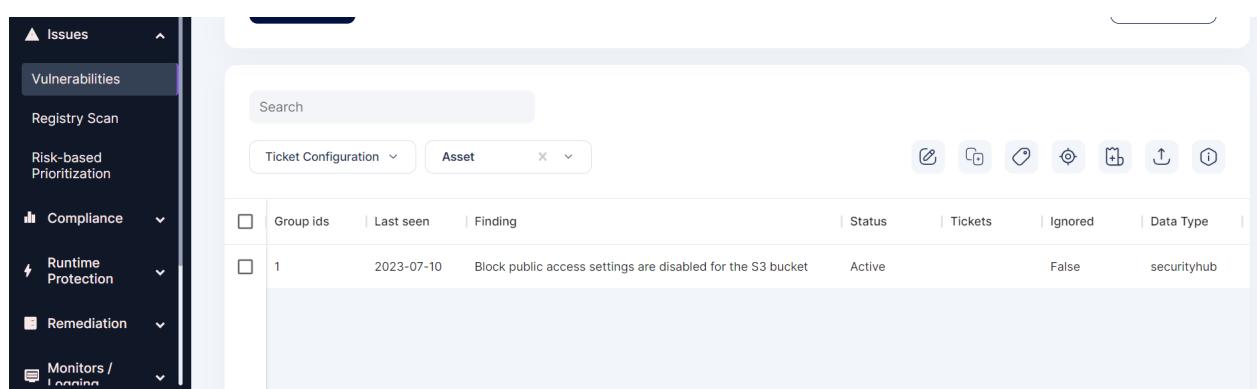
The screenshot shows the ACCUKNOX 'Issues' section. On the left, a sidebar menu includes 'Dashboard', 'Inventory', 'Issues' (which is selected), 'Vulnerabilities' (highlighted in blue), 'Registry Scan', 'Risk-based Prioritization', 'Compliance', and 'Runtime'. The main area displays a list of vulnerabilities under the 'Vulnerabilities' tab. A dropdown menu for 'Group' is open, showing a list of available groups: aws-3, aws-4, azureresourcegroup, bugtest2, grpptestguru, mygroup, priya-aws-group-test-15/06, registry, and s3 bucket. The 's3 bucket' option is highlighted with a red border. The bottom of the screen shows a navigation bar with icons for 'Last seen' and 'Finding'.

Step 5: To view the Grouped S3 bucket details, click on the group by option and select Asset:



Group id	Last seen	Finding
1	2023-07-10	Block public access settings are disabled for the S3 bucket

Step 6: Now, the list of s3 buckets with any misconfigurations associated with them can be seen



Group id	Last seen	Finding	Status	Tickets	Ignored	Data Type
1	2023-07-10	Block public access settings are disabled for the S3 bucket	Active	False		securityhub

Step 7: Click on any of them to get more details

< 1 of 1 >

Asset: thisisthebucket2

Asset Type: S3Bucket

Port: N/A

Status: Active 

Ignored: False 

Tickets: 0 

Severity: High 

Ticket Configuration 



Save

Description

Tool Output

Solution

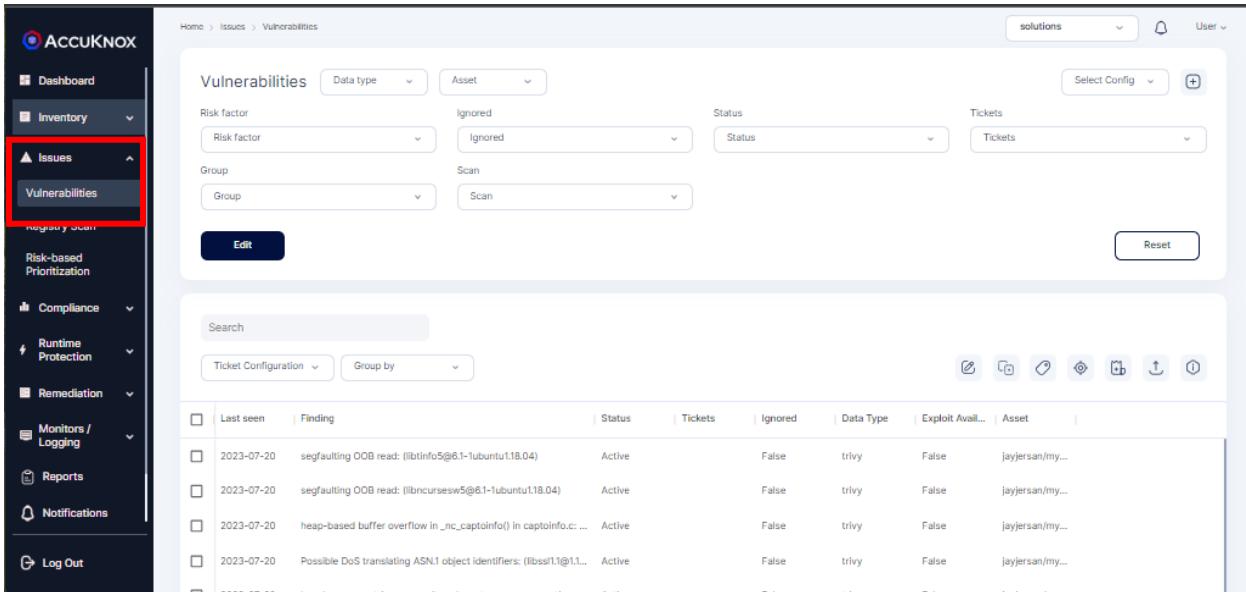
References

All bucket-level block public access settings were disabled for the S3 bucket. Access to the bucket is controlled by account-level block public access settings, access control lists (ACLs), and the bucket's bucket policy.

Similarly, we can use only the group by option to view all the misconfigurations grouped together for each Asset.

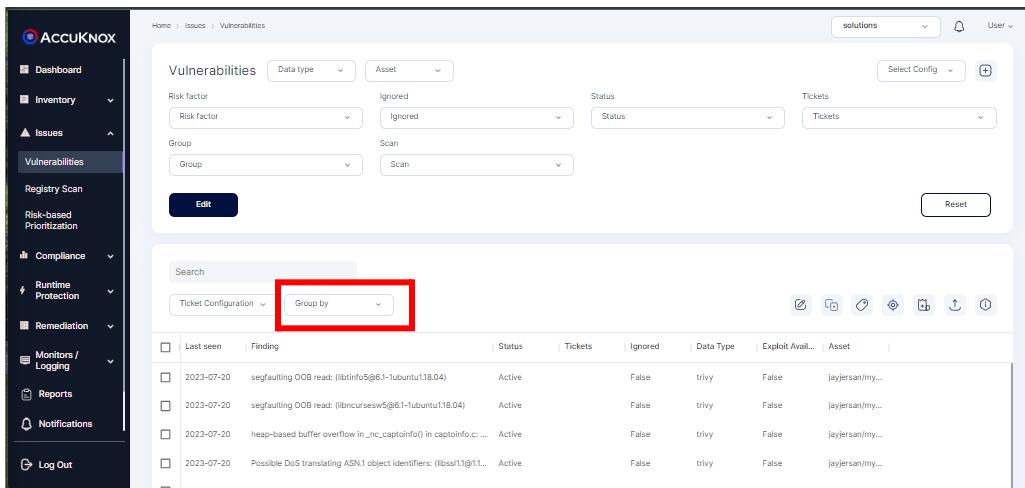
- How to group by findings

1. Goto **Issues** tab, click on **Vulnerabilities** section



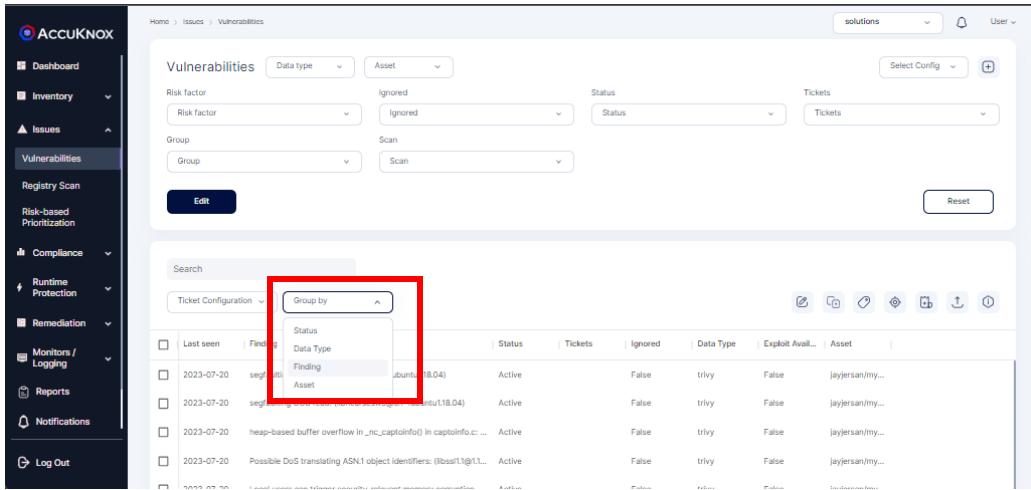
The screenshot shows the ACCUKNOX interface. The left sidebar has a tree view with 'Issues' expanded, and 'Vulnerabilities' is selected. The main content area is titled 'Vulnerabilities' and contains several filter dropdowns: 'Risk factor' (set to 'Ignored'), 'Status' (set to 'Status'), and 'Tickets' (set to 'Tickets'). Below these are 'Group' dropdowns set to 'Scan'. There is an 'Edit' button and a 'Reset' button. The main table lists four vulnerabilities, each with a checkbox, last seen date, finding description, status, ticket count, ignore status, data type, exploit availability, and asset information. A red box highlights the 'Group by' dropdown in the search bar.

2. Navigate to **Group by** filter.



This screenshot is identical to the one above, showing the 'Vulnerabilities' section of the ACCUKNOX interface. The 'Group by' dropdown in the search bar is highlighted with a red box. The rest of the interface, including the sidebar and the table of vulnerabilities, remains the same.

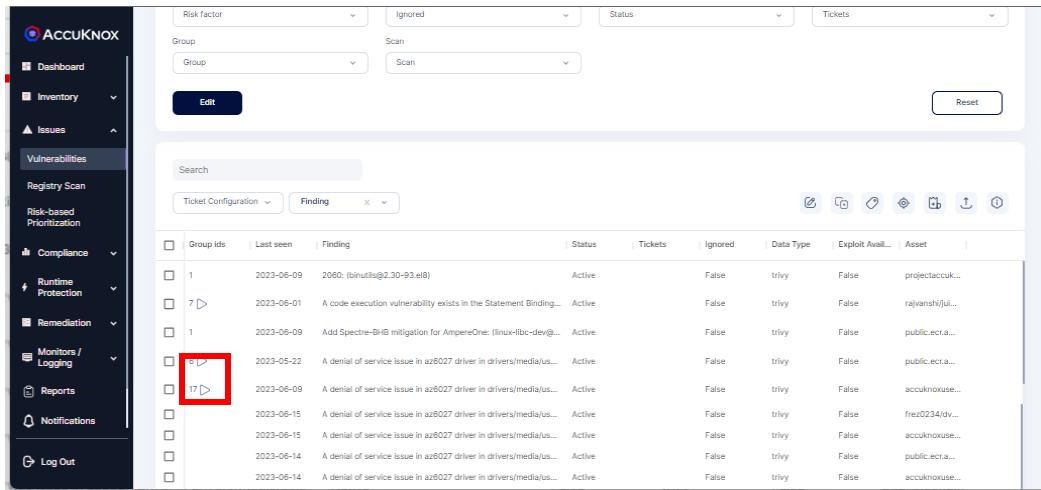
3. Click on it and choose **Findings**



The screenshot shows the AccuKnox interface with the 'Vulnerabilities' tab selected. In the search bar, 'Ticket Configuration' is set to 'Finding'. A dropdown menu is open under 'Group by' with options: Status, Data Type, Finding, and Asset. The 'Asset' option is highlighted with a red box. The main table lists several findings, each with a checkbox, Last seen date, Finding description, Status, Tickets, Ignored, Data Type, Exploit Available, and Asset name.

Group Ids	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Available	Asset
1	2023-06-09	2060: (binutils@2.30-93.el8)	Active	False	trivy	False	projectaccuk...	
7	2023-06-01	A code execution vulnerability exists in the Statement Binding...	Active	False	trivy	False	rajvanshi/jul...	
1	2023-06-09	Add Spectre-B1B mitigation for AmpereOne: (linux-libc-dev@...	Active	False	trivy	False	public.ecr.a...	
17	2023-05-22	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	False	public.ecr.a...	
	2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	False	accuknoxuse...	
	2023-06-15	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	False	accuknoxuse...	
	2023-06-14	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	False	public.ecr.a...	
	2023-06-14	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	False	accuknoxuse...	

Now, you can view that similar findings are grouped. On clicking the arrow button in the findings list, you will able to view all the assets it is found in

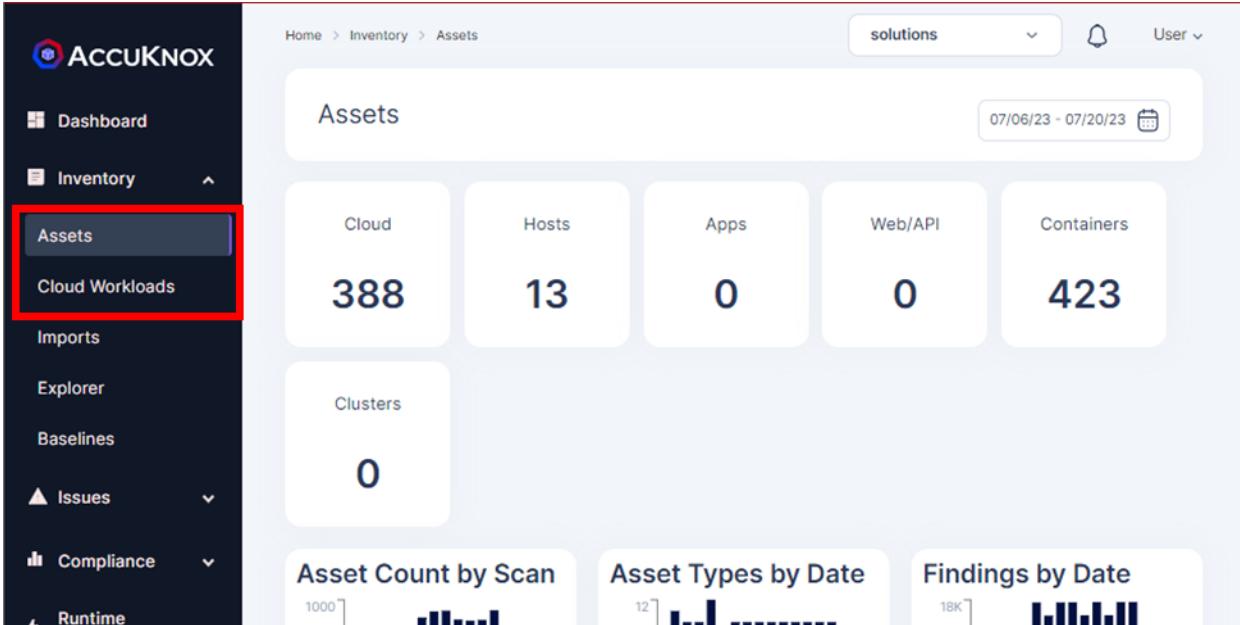


This screenshot shows the same AccuKnox interface after expanding the asset groups. The 'Group by' dropdown now shows 'Asset'. The main table now displays asset details for each finding group. The first two rows from the previous screenshot are shown here, with the asset details expanded:

Group Ids	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Available	Asset
1	2023-06-09	2060: (binutils@2.30-93.el8)	Active	False	trivy	False	projectaccuk...	projectaccuk...
7	2023-06-01	A code execution vulnerability exists in the Statement Binding...	Active	False	trivy	False	rajvanshi/jul...	rajanvanshi/jul...

- How to group by criticality and Status

1. Goto **Inventory** tab, click on **Assets** section



Assets

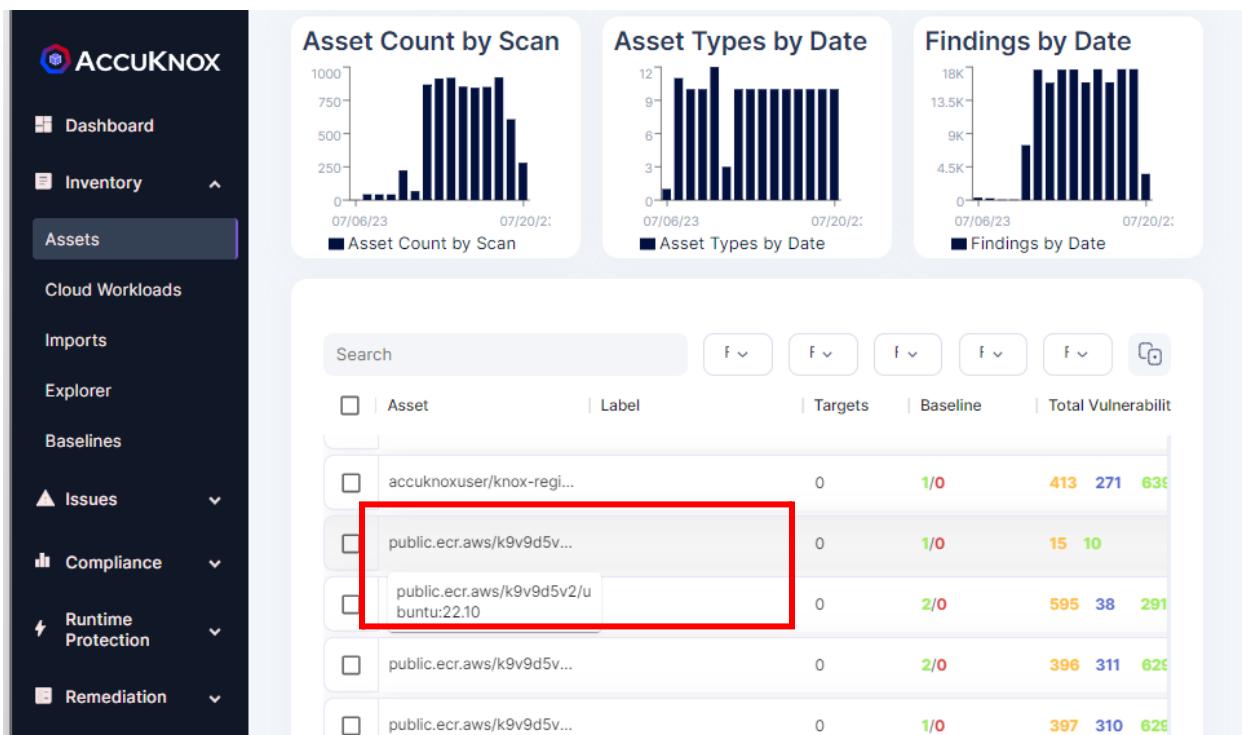
Cloud Hosts Apps Web/API Containers

388 13 0 0 423

Clusters: 0

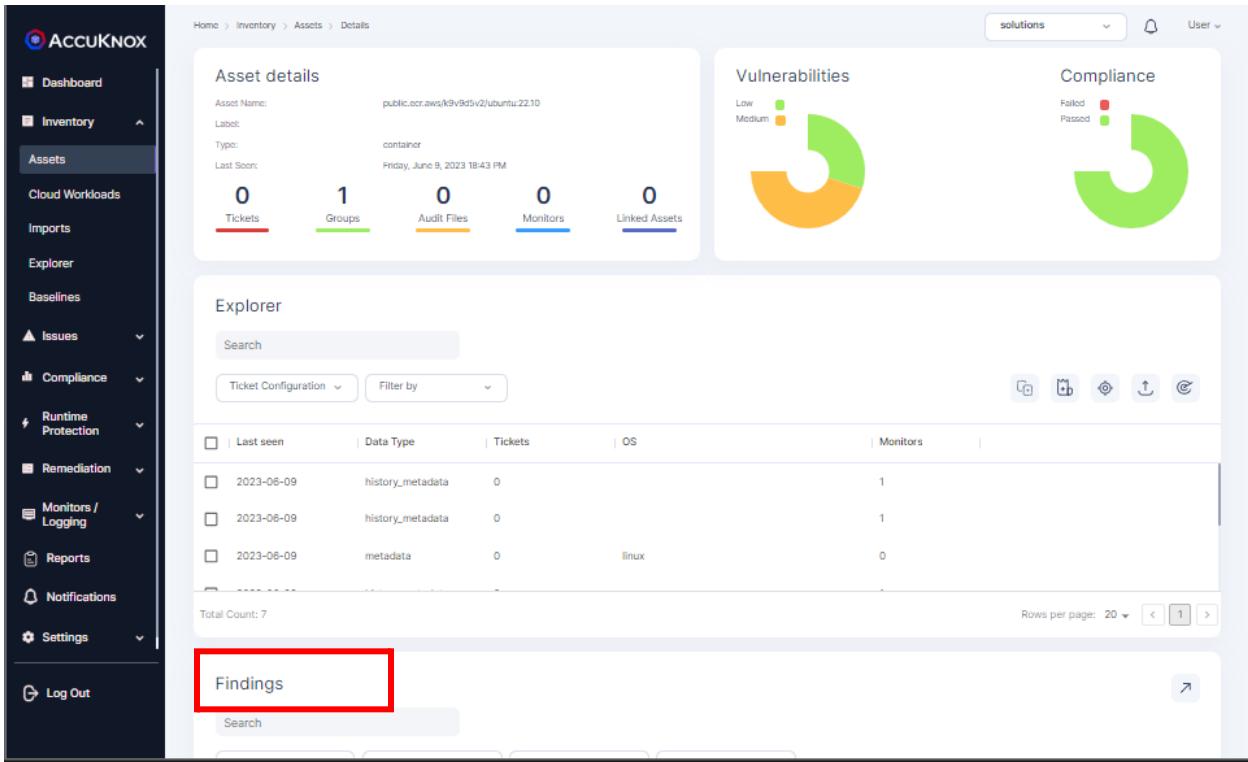
Asset Count by Scan Asset Types by Date Findings by Date

2. Scroll down and click on the particular asset for which misconfiguration need to be viewed



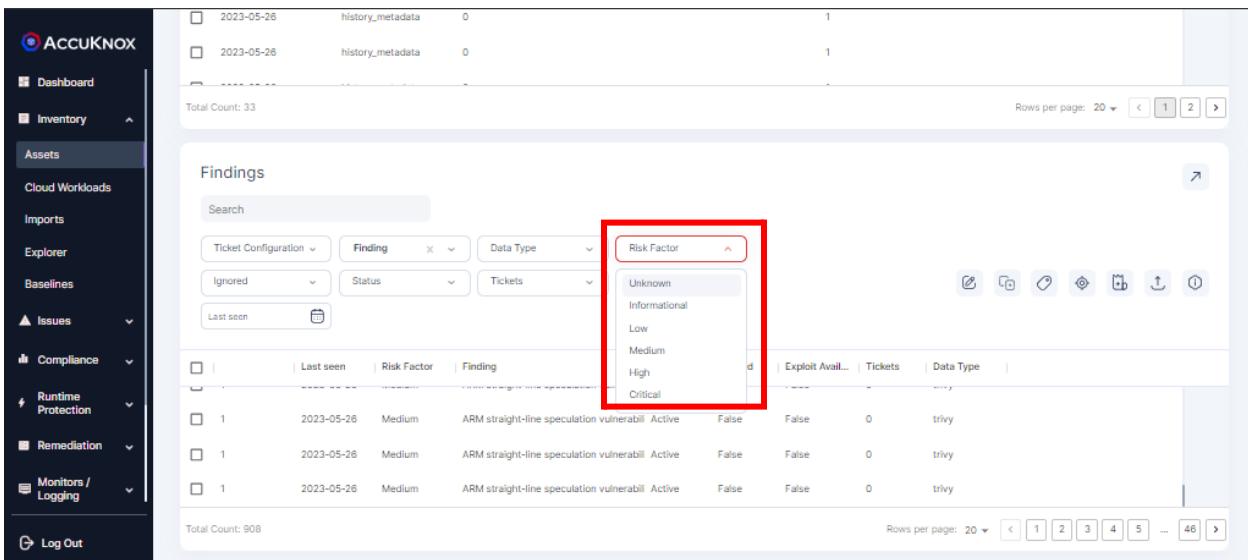
Asset	Label	Targets	Baseline	Total Vulnerability
accuknoxuser/knox-regi...		0	1/0	413 271 639
public.ecr.aws/k9v9d5v...		0	1/0	15 10
public.ecr.aws/k9v9d5v2/u...		0	2/0	595 38 291
public.ecr.aws/k9v9d5v...		0	2/0	396 311 629
public.ecr.aws/k9v9d5v...		0	1/0	397 310 629

3. You will land on the page as shown below. Scroll down and navigate to **Findings** sections.



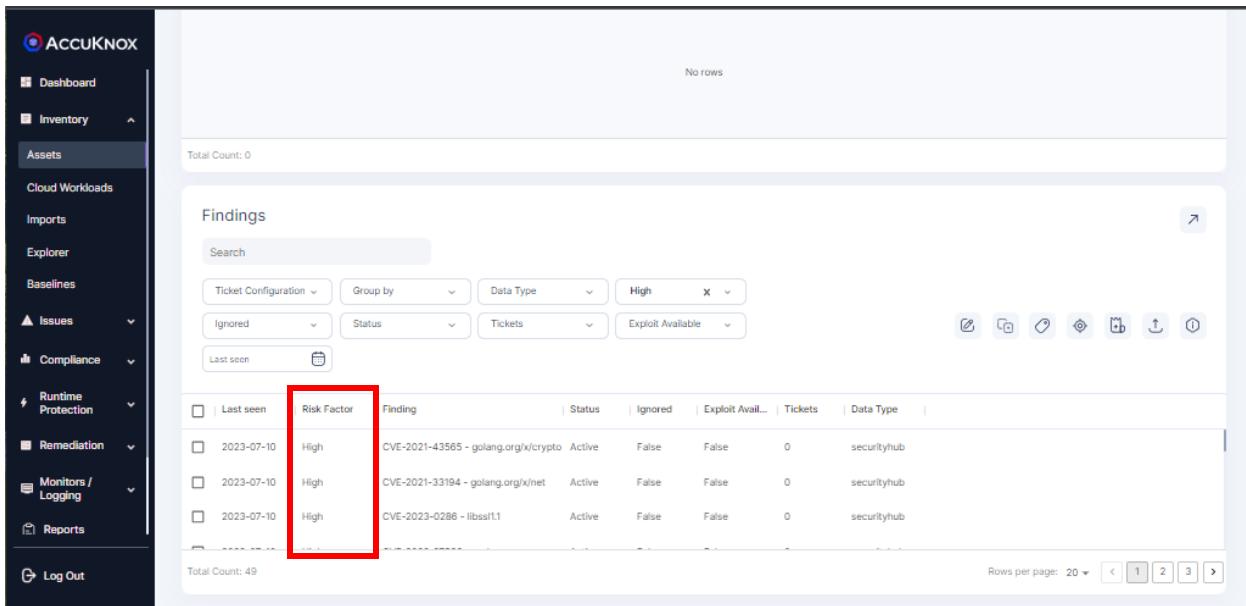
The screenshot shows the ACCUKNOKX Asset Details dashboard. The left sidebar is titled 'Inventory' and includes sections for Assets, Cloud Workloads, Imports, Explorer, Baselines, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Reports, Notifications, Settings, and Log Out. The main content area has tabs for 'Asset details', 'Vulnerabilities', and 'Compliance'. Under 'Asset details', asset information is listed: Asset Name: public.ecr.aws/k9v9d5v2/ubuntu:22.10, Label: container, Type: container, Last Seen: Friday, June 9, 2023 18:43 PM. Below this are counts for Tickets (0), Groups (1), Audit Files (0), Monitors (0), and Linked Assets (0). To the right are two donut charts: 'Vulnerabilities' showing Low (green) and Medium (orange) levels, and 'Compliance' showing Failed (red) and Passed (green) status. The 'Explorer' section contains a table of historical metadata entries. A red box highlights the 'Findings' section below, which includes a search bar and a table of findings.

4. Navigate to the **Risk Factor** filter, and choose the severity level.



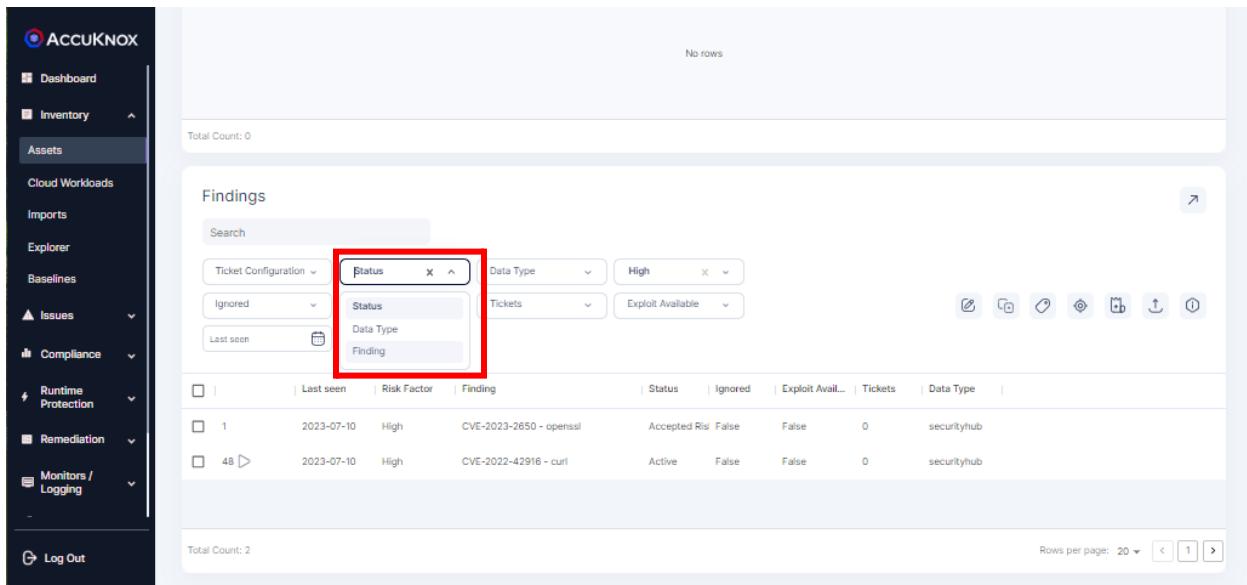
The screenshot shows the 'Findings' section of the ACCUKNOKX interface. The left sidebar is identical to the previous dashboard. The 'Findings' section has a search bar and filters for Ticket Configuration, Finding, Status, Data Type, and Last seen. A red box highlights the 'Risk Factor' dropdown menu, which lists categories: Unknown, Informational, Low, Medium, High, and Critical. Below the dropdown is a table of findings with columns for Last seen, Risk Factor, Finding, Exploit Available, Status, Tickets, and Data Type. The table shows three entries, all categorized as Medium risk. The bottom of the screen shows a navigation bar with a dark blue gradient.

Now, you can find the findings as per the criticality level as shown below



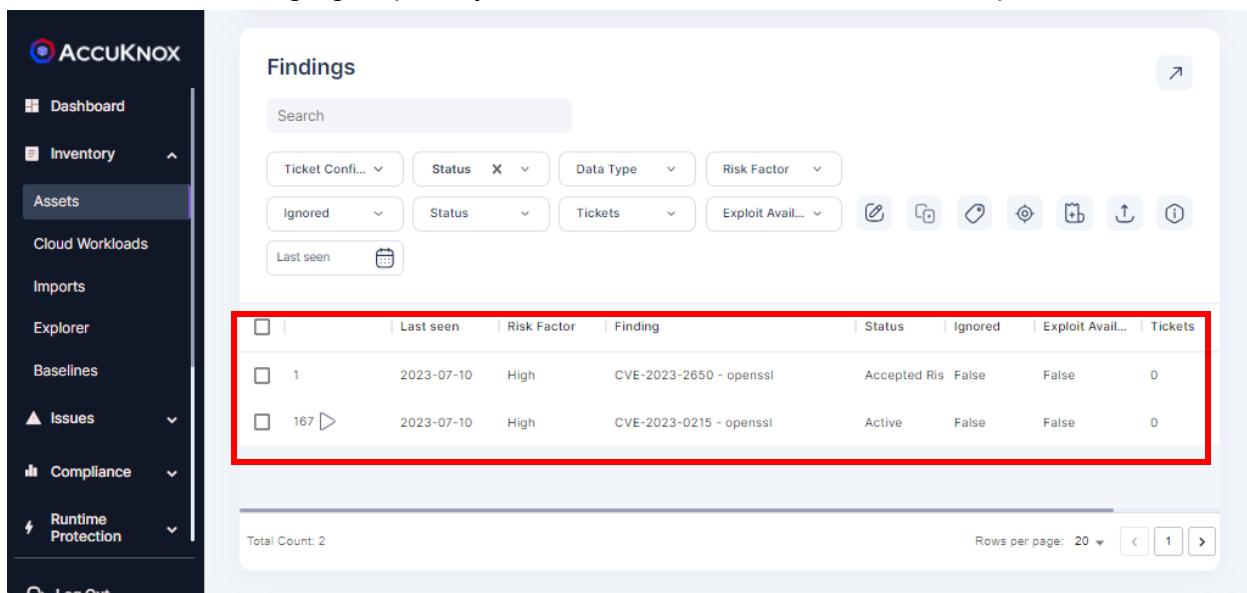
The screenshot shows the ACCUKNOX interface under the 'Assets' section. On the left sidebar, 'Issues' is expanded, and 'Findings' is selected. In the main area, a search bar and several filters are present: 'Ticket Configuration' (dropdown), 'Group by' (dropdown), 'Data Type' (dropdown set to 'High'), 'Ignored' (dropdown), 'Status' (dropdown), 'Tickets' (dropdown), and 'Exploit Available' (dropdown). Below these filters is a 'Last seen' button. A red box highlights the 'Risk Factor' column header in the table. The table has columns: Last seen, Risk Factor, Finding, Status, Ignored, Exploit Avail..., Tickets, Data Type, and a checkbox column. The data shows three findings from July 10, 2023, all categorized as 'High' risk. The first finding is CVE-2021-43565 - golang.org/x/crypto, the second is CVE-2021-33194 - golang.org/x/net, and the third is CVE-2023-0286 - libss1.1. All findings are marked as 'Active'. The status bar at the bottom indicates a total count of 49 findings.

5. Navigate to the **Group by** filter, and choose **Status**.



This screenshot shows the same ACCUKNOX interface after applying the 'Status' filter. The 'Status' dropdown in the filter bar is highlighted with a red box. The table now groups findings by their status: 'Accepted Risk' and 'Active'. The 'Accepted Risk' group contains one finding (CVE-2023-2650 - openssl) and the 'Active' group contains 48 findings (CVE-2022-42916 - curl). The rest of the interface remains consistent with the previous screenshot.

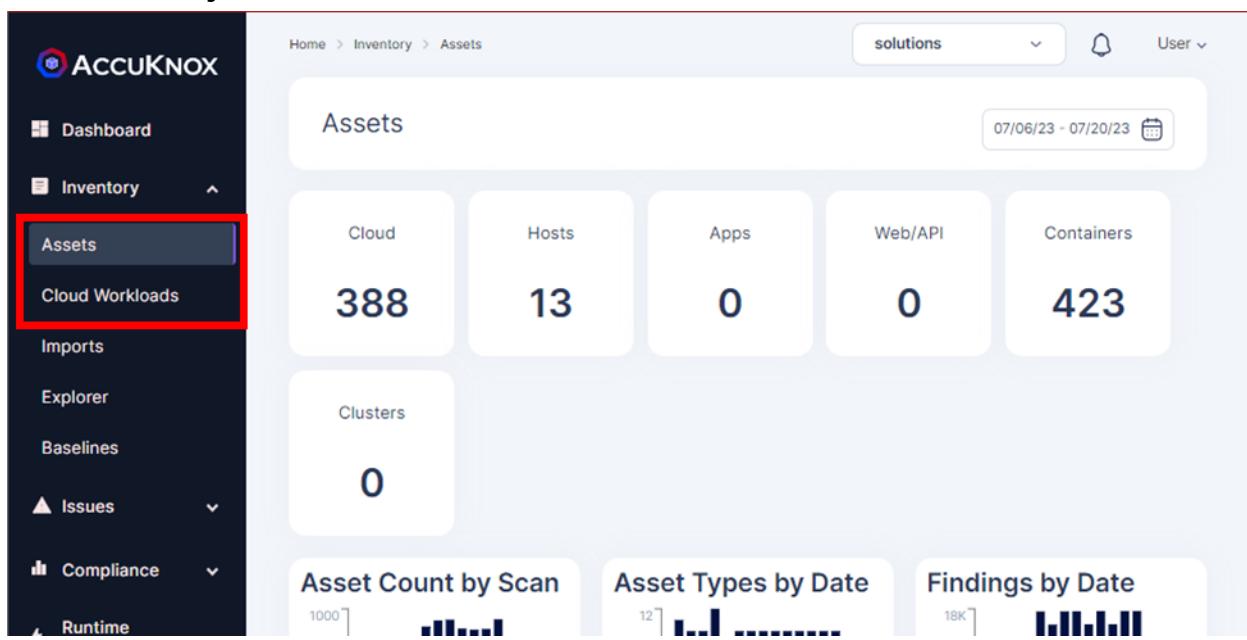
Now, you can view the findings grouped by the status, such as active and accepted risk



	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets
1	2023-07-10	High	CVE-2023-2650 - openssl	Accepted Risk	False	False	0
167	2023-07-10	High	CVE-2023-0215 - openssl	Active	False	False	0

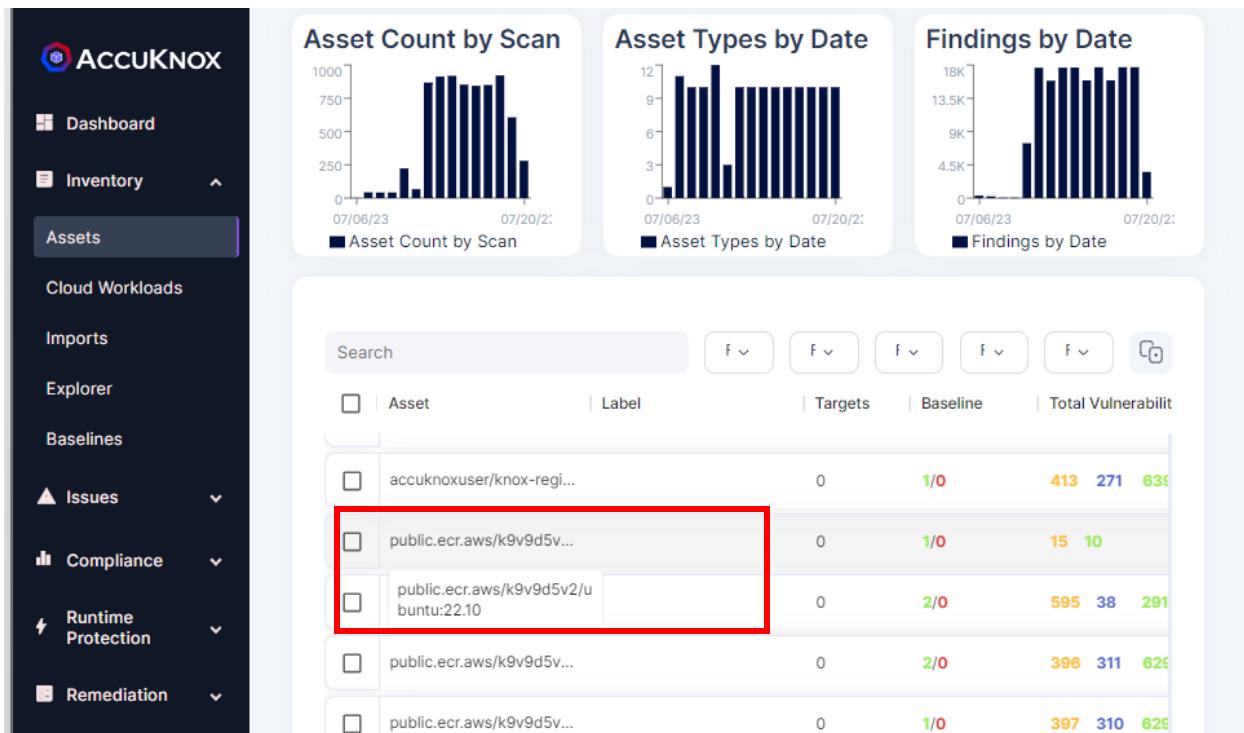
- How to create a ticket

1. Goto **Inventory** tab, click on **Assets** section



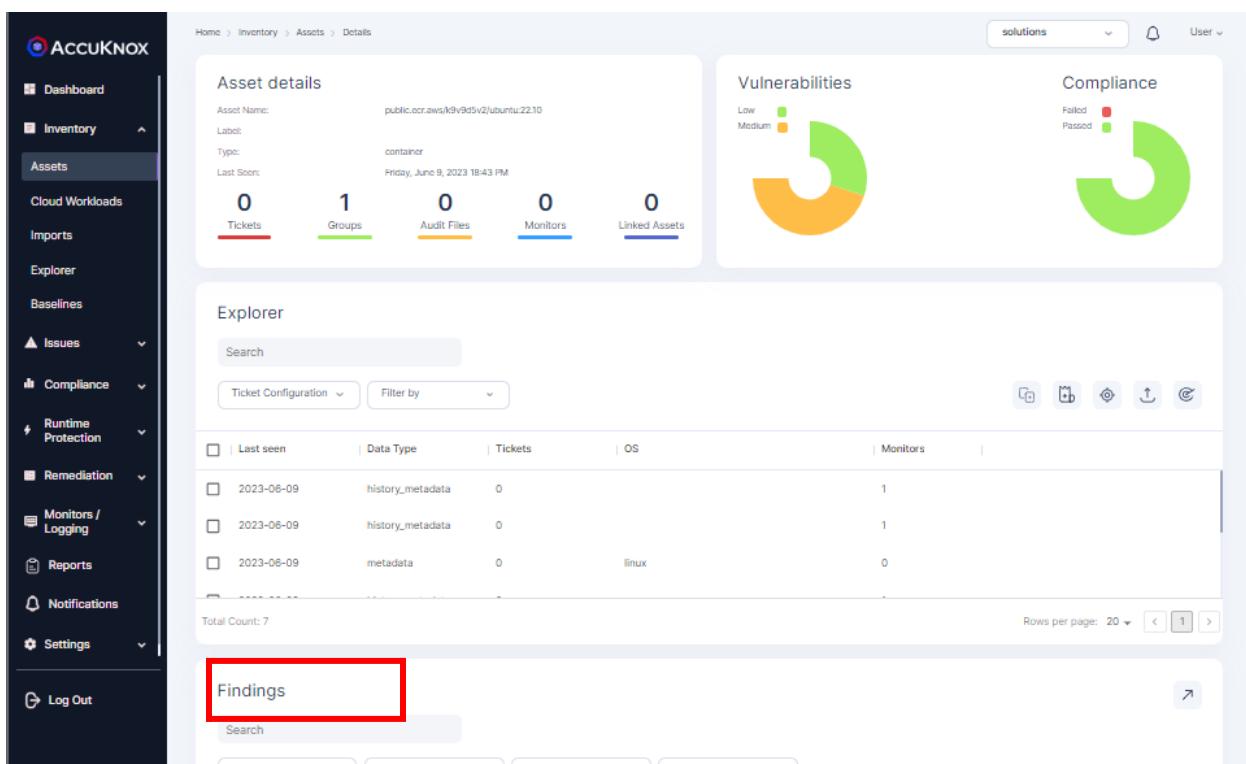
Category	Count
Cloud	388
Hosts	13
Apps	0
Web/API	0
Containers	423

- a. Scroll down and click on the particular asset for which misconfiguration need to be viewed



Asset Name	Targets	Baseline	Total Vulnerabilities
accuknoxuser/knox-regi...	0	1/0	413 271 639
public.ecr.aws/k9v9d5v...	0	1/0	15 10
public.ecr.aws/k9v9d5v2/u...	0	2/0	595 38 291
public.ecr.aws/k9v9d5v...	0	2/0	396 311 629
public.ecr.aws/k9v9d5v...	0	1/0	397 310 629

2. You will land on the page as shown below. Scroll down and navigate to **Findings** sections.



Asset details

- Asset Name: public.ecr.aws/k9v9d5v2/ubuntu:22.10
- Label:
- Type: container
- Last Seen: Friday, June 9, 2023 18:43 PM

Tickets	Groups	Audit Files	Monitors	Linked Assets
0	1	0	0	0

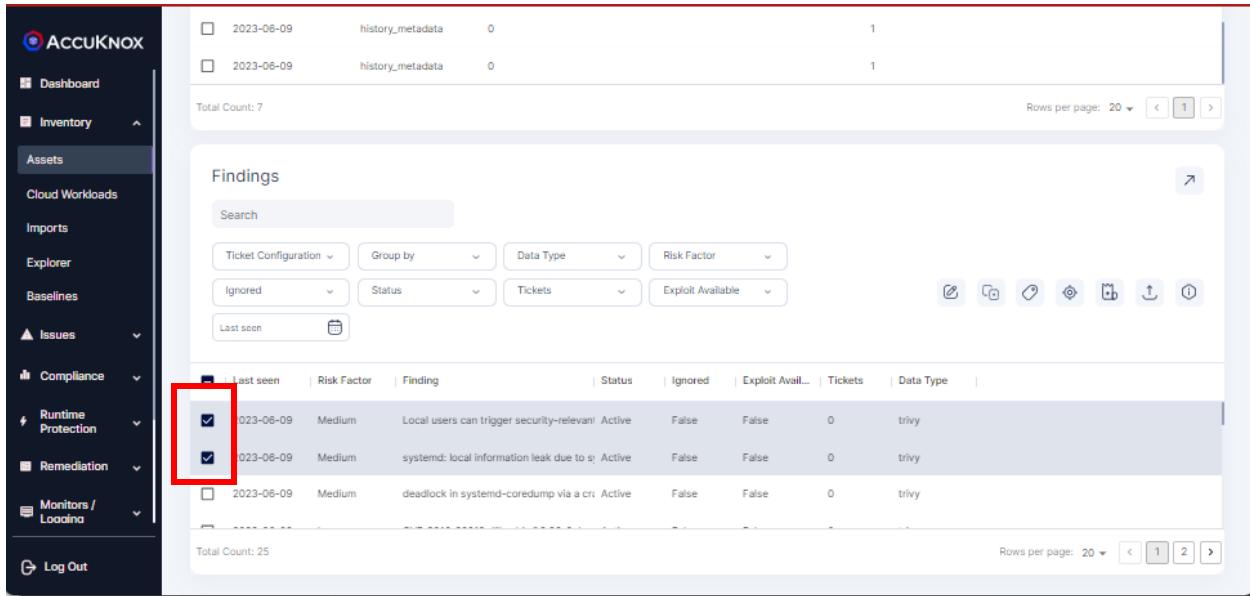
Vulnerabilities

Compliance

Explorer

Findings

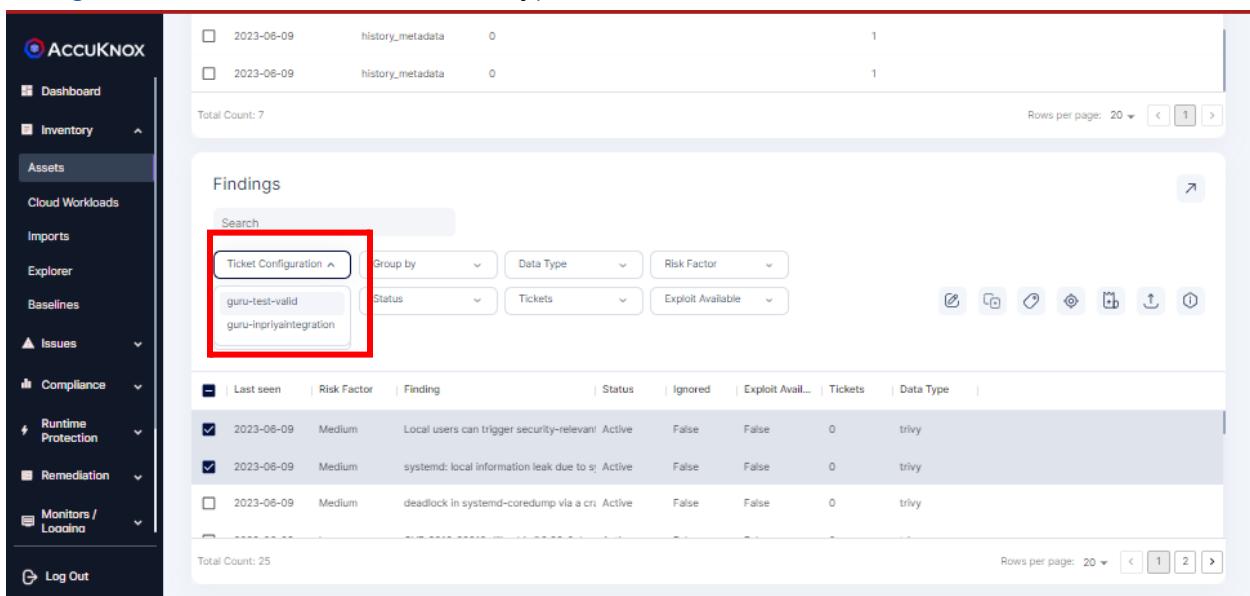
3. Select the check mark behind the ***Findings*** for which ticket needs to be created.



The screenshot shows the ACCUKNOX interface with the 'Findings' section selected. Two findings are highlighted with checkboxes checked, indicating they are selected for ticket creation. The findings listed are:

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2023-06-09	Medium	Local users can trigger security-relevant	Active	False	False	0	trivy
2023-06-09	Medium	systemd: local information leak due to s	Active	False	False	0	trivy
2023-06-09	Medium	deadlock in systemd-coredump via a cr	Active	False	False	0	trivy

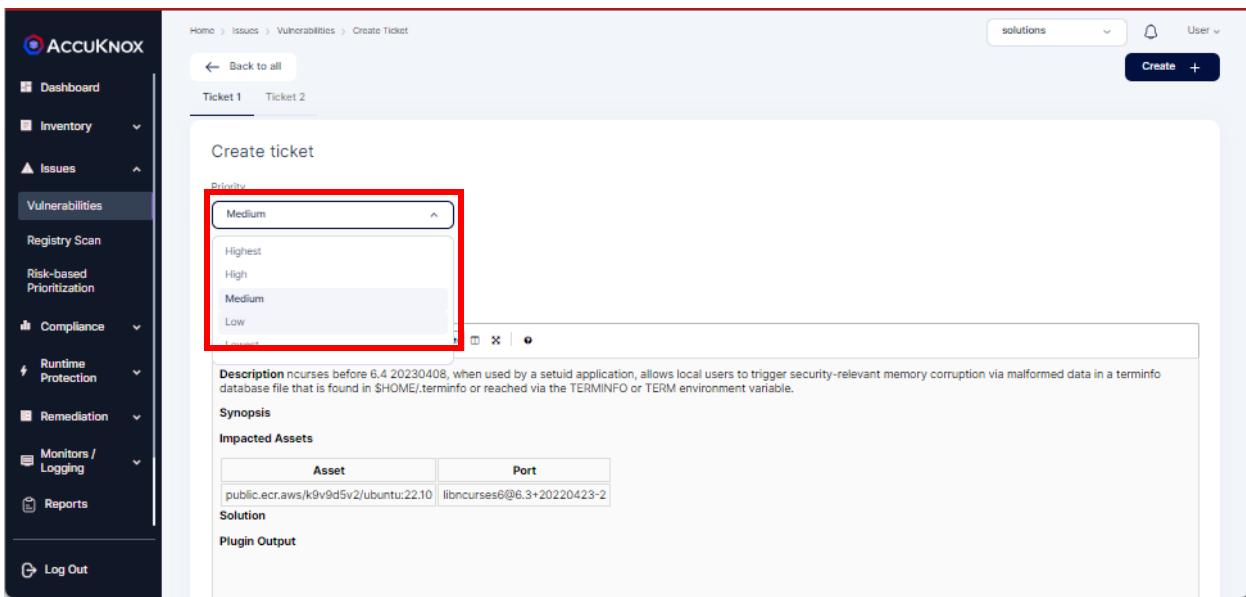
4. Select the desired ticket configuration by which ticket will be created ([Create a ticket configuration](#) if it doesn't exist already)



The screenshot shows the ACCUKNOX interface with the 'Findings' section selected. The 'Ticket Configuration' dropdown is open, displaying two options: 'guru-test-valid' and 'guru-inpriyaintegration'. The findings listed are:

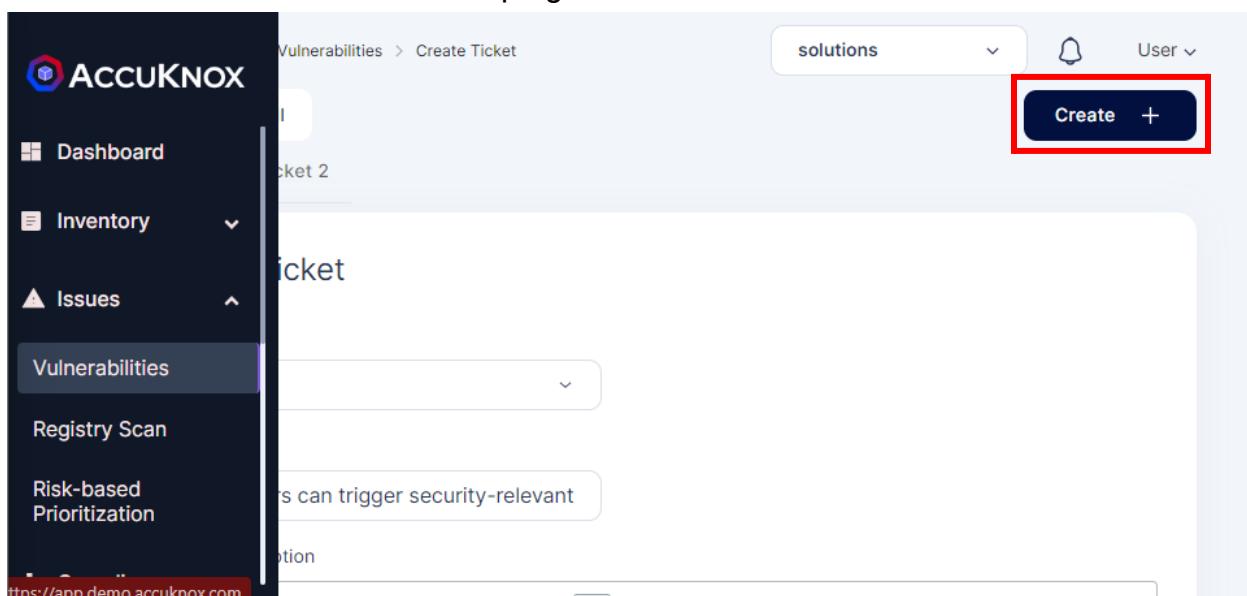
Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2023-06-09	Medium	Local users can trigger security-relevant	Active	False	False	0	trivy
2023-06-09	Medium	systemd: local information leak due to s	Active	False	False	0	trivy
2023-06-09	Medium	deadlock in systemd-coredump via a cr	Active	False	False	0	trivy

5. Choose the **Priority** from the dropdown.



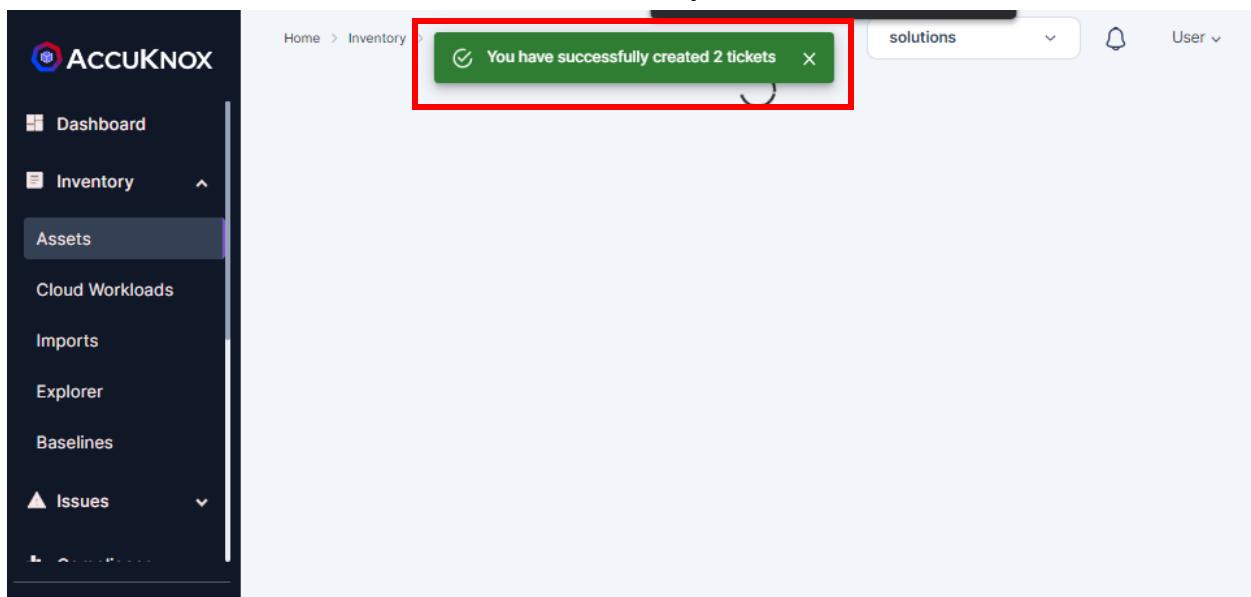
The screenshot shows the 'Create ticket' interface in the AccuKnox web application. On the left is a sidebar with navigation links like Dashboard, Inventory, Issues, Vulnerabilities, Registry Scan, Risk-based Prioritization, Compliance, Runtime Protection, Remediation, Monitors / Logging, and Reports. The main area has tabs for 'Ticket 1' and 'Ticket 2'. A 'Create ticket' section contains a 'Priority' dropdown menu with options: Medium (selected), Highest, High, Medium, Low, and Lowest. Below the dropdown is a 'Description' field containing technical details about a vulnerability. There are sections for 'Synopsis', 'Impacted Assets' (with a table showing Asset and Port), 'Solution', and 'Plugin Output'. At the top right is a 'Create +' button.

6. Edit the **Ticket Title** and **Ticket Description**, as required.
 7. Click on the **Create** button at the top right corner.

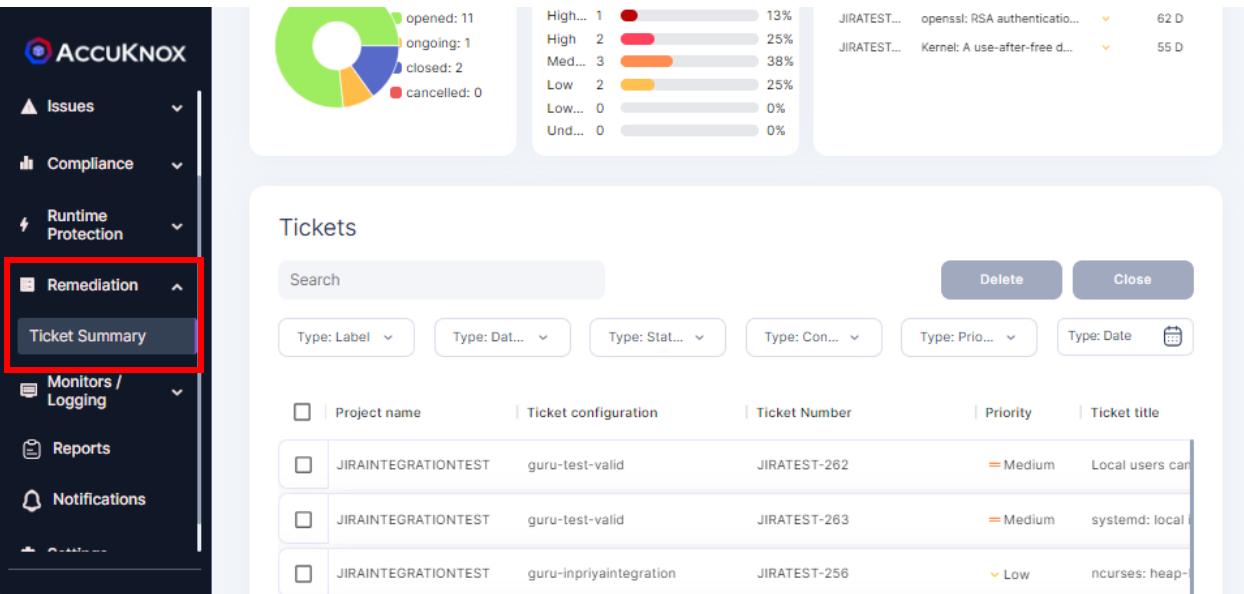


This screenshot shows the same 'Create ticket' interface as above, but with a red box highlighting the 'Create +' button at the top right. The sidebar and form fields are identical to the previous screenshot.

You can see the tickets were created successfully.



You can manage the created tickets in the **Ticket Summary** section, under the **Remediation** tab.



The screenshot shows the ACCUKNOKX interface with the Remediation tab selected in the sidebar (highlighted with a red box). The main area displays a "Tickets" summary card. It includes a pie chart showing ticket status distribution (opened: 11, ongoing: 1, closed: 2, cancelled: 0) and a horizontal bar chart showing ticket priority distribution (High: 1, High: 2, Med: 3, Low: 2, Low: 0, Und: 0). Below this is a table of created tickets:

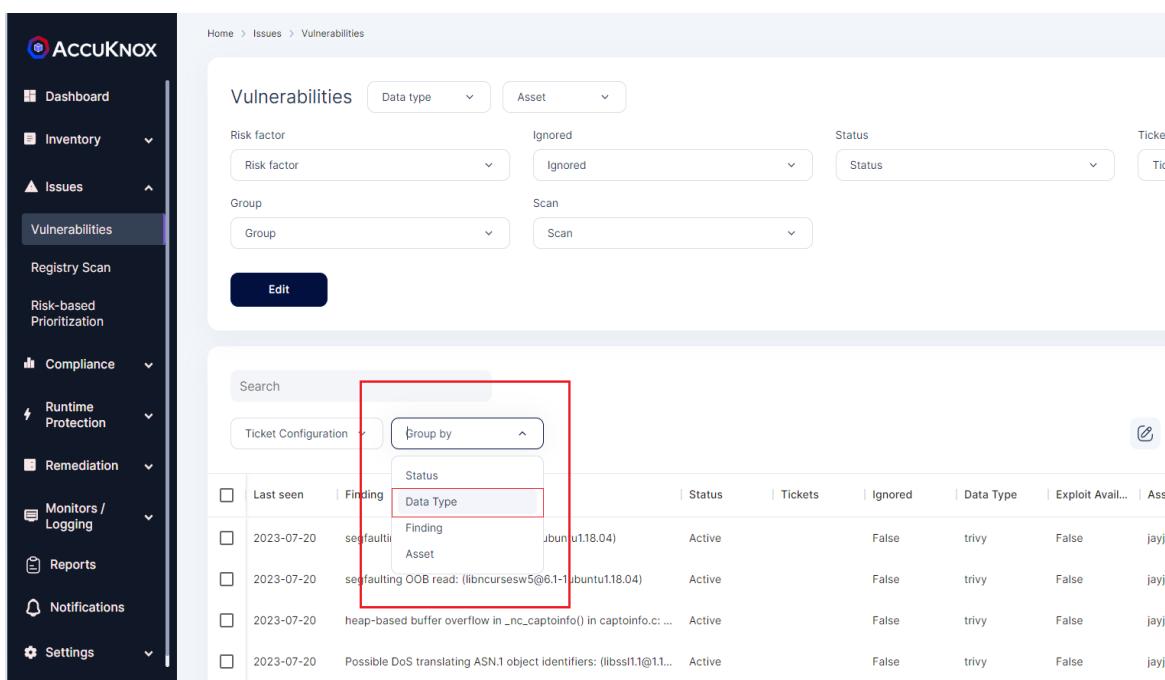
<input type="checkbox"/>	Project name	Ticket configuration	Ticket Number	Priority	Ticket title
<input type="checkbox"/>	JIRAINTEGRATIONTEST	guru-test-valid	JIRATEST-262	= Medium	Local users can...
<input type="checkbox"/>	JIRAINTEGRATIONTEST	guru-test-valid	JIRATEST-263	= Medium	systemd: local...
<input type="checkbox"/>	JIRAINTEGRATIONTEST	guru-inpriyaintegration	JIRATEST-256	< Low	ncurses: heap-...

Issues/Vulnerabilities

- Group findings by source and severity

AccuKnox automatically scans assets with the help of various open-source tools. It uses tools like Clair, Trivy, CLOC, Fortify, Snyk, SonarQube, Cloudsploit, Kube Bench, and various other open-source tools for Scanning.

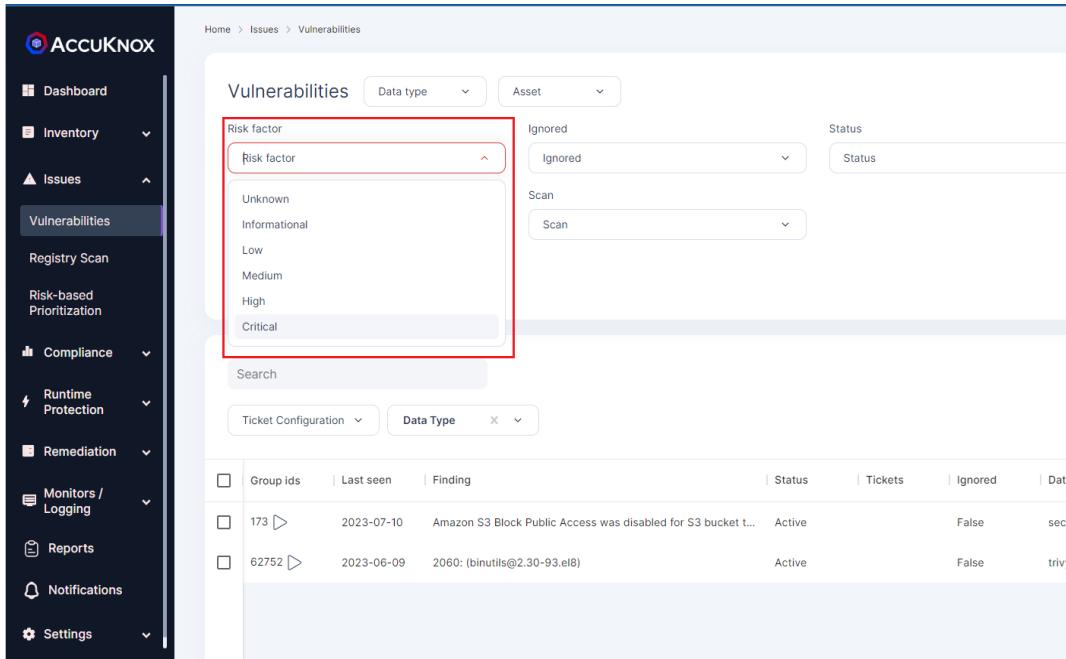
Findings can be grouped according to the tools that were used to do the scan by selecting the “Data Type” option from the “Group By” drop down in the Vulnerabilities screen.



The screenshot shows the AccuKnox interface with the 'Vulnerabilities' section selected in the sidebar. On the right, the 'Vulnerabilities' page is displayed with several filter options at the top. A red box highlights the 'Group by' dropdown menu, which is currently set to 'Data Type'. Below this, a table lists several findings, each with columns for Last seen, Finding, Status, Tickets, Ignored, Data Type, Exploit Available, and Asset. The findings listed are:

Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Available	Asset
2023-07-20	segfault in /libnssw5@6.1-1ubuntu1.18.04	Active		False	trivy	False	jayje
2023-07-20	segfaulting OOB read: (/libnssw5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayje
2023-07-20	heap-based buffer overflow in _nc_captainfo() in captainfo.c: ...	Active		False	trivy	False	jayje
2023-07-20	Possible DoS translating ASN.1 object identifiers: (/libssl1.1@1.1.1)	Active		False	trivy	False	jayje

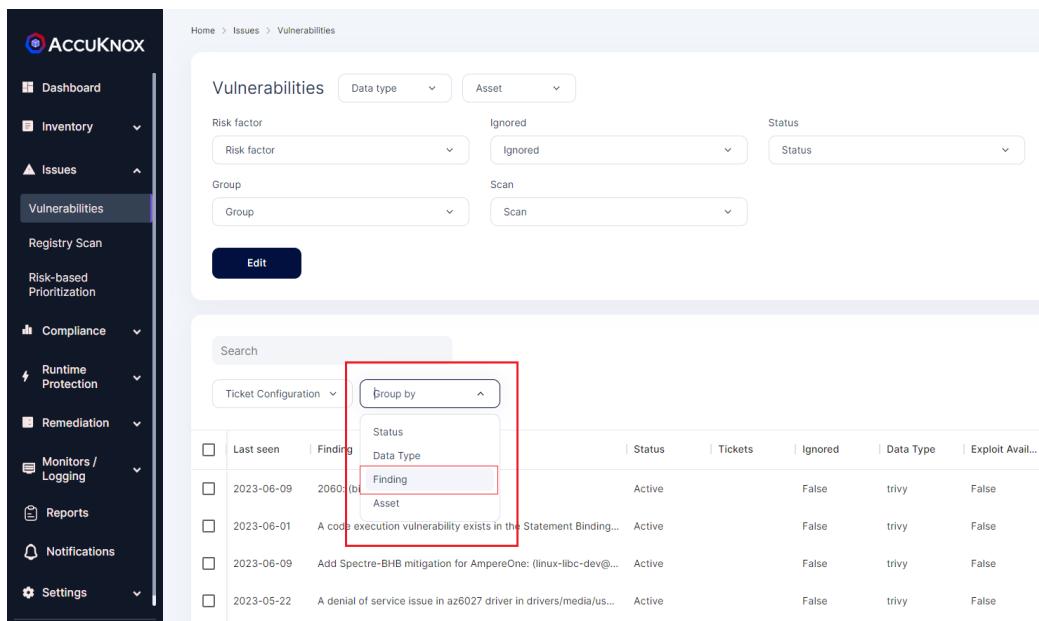
Users can further filter the findings with respect to their Risk factor so that they can have a view of most critical findings from each tool being used.



The screenshot shows the ACCUKNOX interface with the 'Vulnerabilities' section selected. At the top, there are filters for 'Data type' and 'Asset'. Below these are dropdown menus for 'Risk factor' (set to 'Ignored') and 'Status' (set to 'Scan'). A search bar and ticket configuration buttons are also present. The main table lists vulnerabilities with columns for Group ID, Last seen, Finding, Status, Tickets, Ignored, and Data Type. Two entries are shown: one for Amazon S3 Block Public Access disabled and another for binutils@2.30-93.el8.

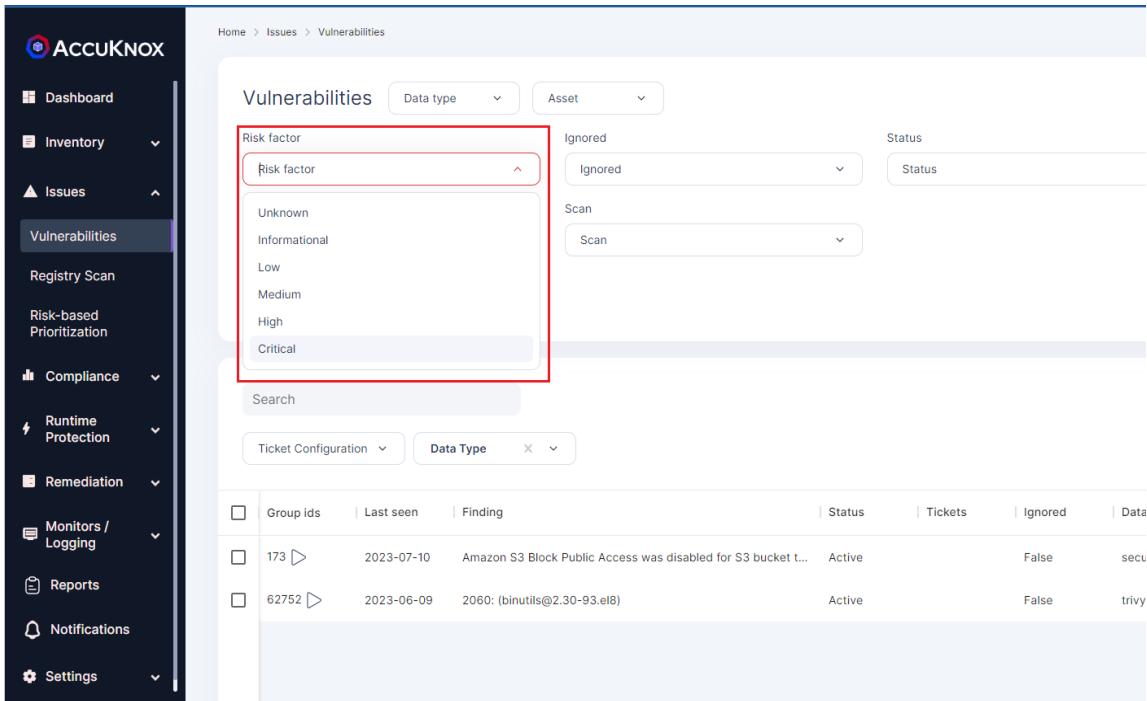
- How to group by Findings and severity

When resolving and patching vulnerabilities it is important to tackle the findings that are most abundant and most severe first. Users can use the Group by Findings feature to look for the vulnerabilities or misconfiguration that exist in large no. of assets and prioritize them accordingly.



This screenshot shows the same ACCUKNOX interface as above, but with the 'Edit' button highlighted. The 'Group by' dropdown in the search bar is also highlighted with a red box, showing options like Status, Data Type, Finding, and Asset. The main table displays the same two vulnerability entries as the previous screenshot.

Further users can select the Risk Factor to filter the findings based on their severity. This again narrows the findings that need to be remediated.

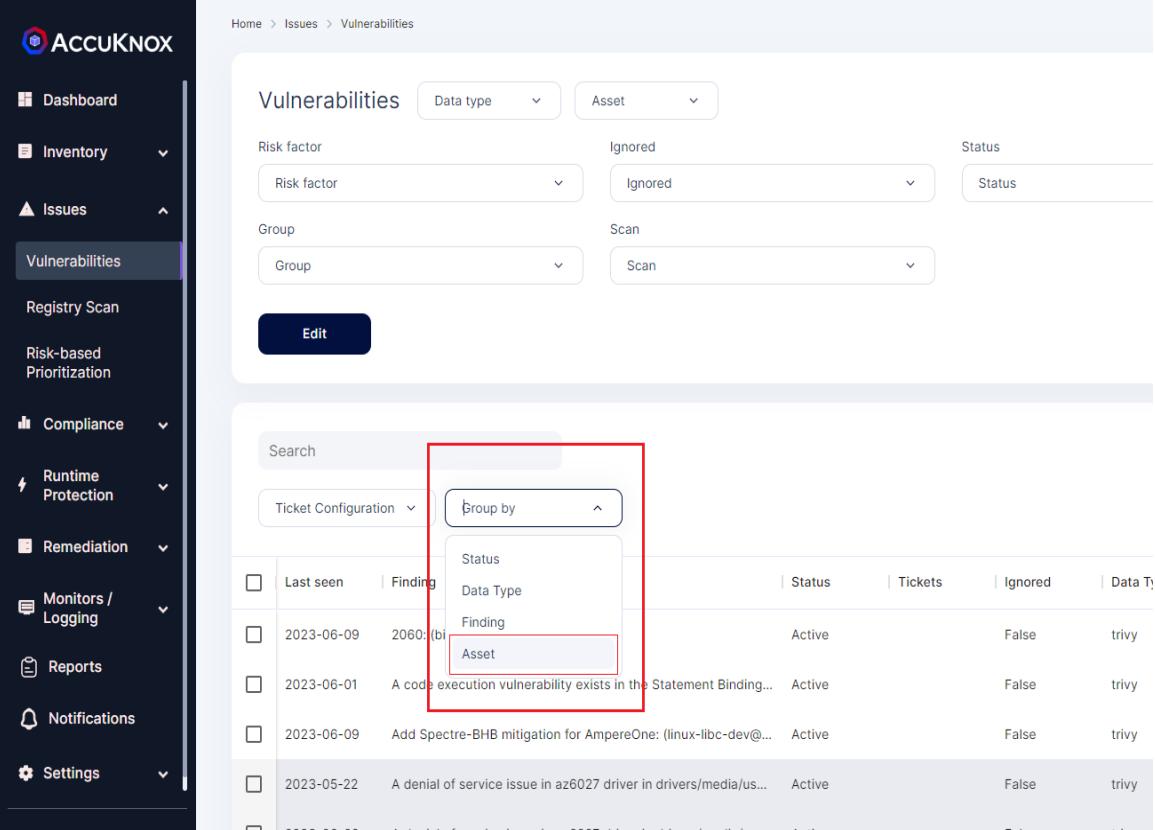


The screenshot shows the ACCUKNOX interface with the 'Vulnerabilities' tab selected in the sidebar. The main view displays a table of findings with columns for Group ID, Last Seen, Finding, Status, Tickets, Ignored, and Data. Above the table, there are several filters: 'Risk factor' dropdown (with options Unknown, Informational, Low, Medium, High, Critical), 'Ignored' dropdown (set to Ignored), 'Status' dropdown (set to Scan), and 'Ticket Configuration' and 'Data Type' dropdowns. A red box highlights the 'Risk factor' dropdown menu, which lists the severity levels from Unknown to Critical.

Group ID	Last seen	Finding	Status	Tickets	Ignored	Data
173	2023-07-10	Amazon S3 Block Public Access was disabled for S3 bucket t...	Active		False	secu
62752	2023-06-09	2060: (binutils@2.30-93.el8)	Active		False	trivy

- How to group by Asset and severity

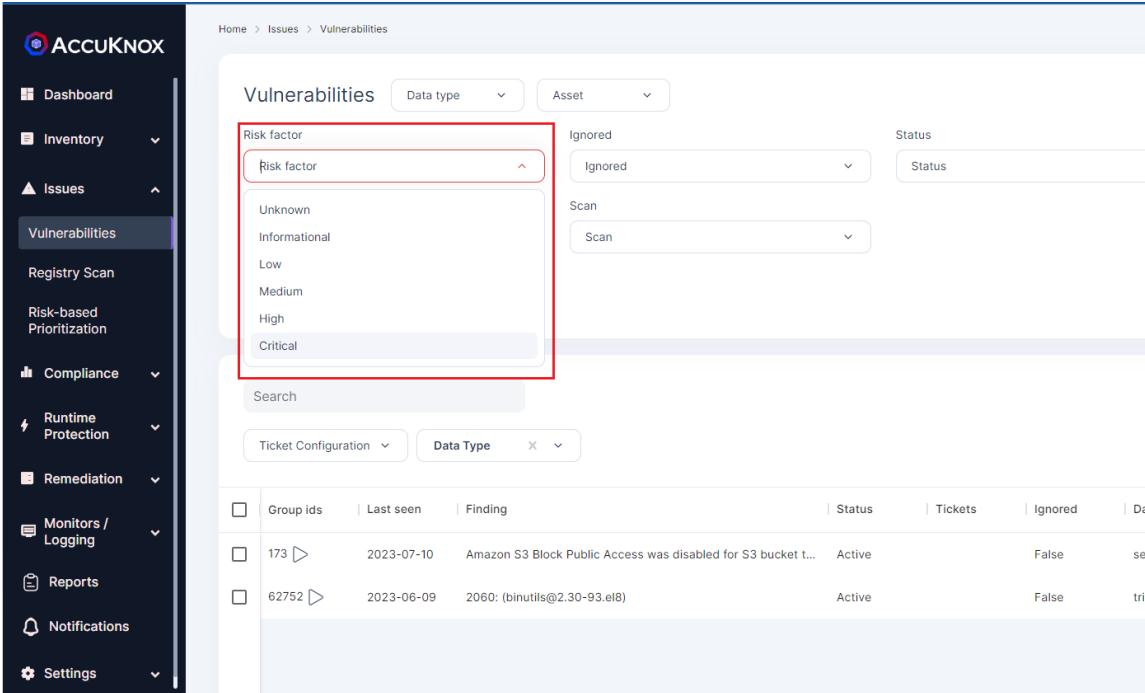
Users can have an Asset wise view of the findings. Grouping by assets, groups the vulnerabilities or misconfigurations together with respect to the asset that they are associated with.



The screenshot shows the ACCUKNOK web interface. On the left is a dark sidebar with various navigation options. The 'Issues' section is expanded, and 'Vulnerabilities' is selected. The main content area is titled 'Vulnerabilities' and includes several filter dropdowns: 'Risk factor' (set to 'Ignored'), 'Data type' (dropdown), 'Asset' (dropdown), 'Status' (dropdown), 'Group' (dropdown), and 'Scan' (dropdown). A large red box highlights the 'Group by' dropdown in the search bar above the table. Below the table, there is a note: 'If coupled with the Risk factor filter, users can have a view of the most critical assets ie the assets that has the most no. of critical findings.' The table lists vulnerabilities with columns for Last seen, Finding, Status, Tickets, Ignored, and Data Type.

Last seen	Finding	Status	Tickets	Ignored	Data Type
2023-06-09	2060: (b) Asset	Active	False	trivy	
2023-06-01	A code execution vulnerability exists in the Statement Binding...	Active	False	trivy	
2023-06-09	Add Spectre-BHB mitigation for AmpereOne: (linux-libc-dev@...	Active	False	trivy	
2023-05-22	A denial of service issue in az6027 driver in drivers/media/us...	Active	False	trivy	

If coupled with the Risk factor filter, users can have a view of the most critical assets ie the assets that has the most no. of critical findings.

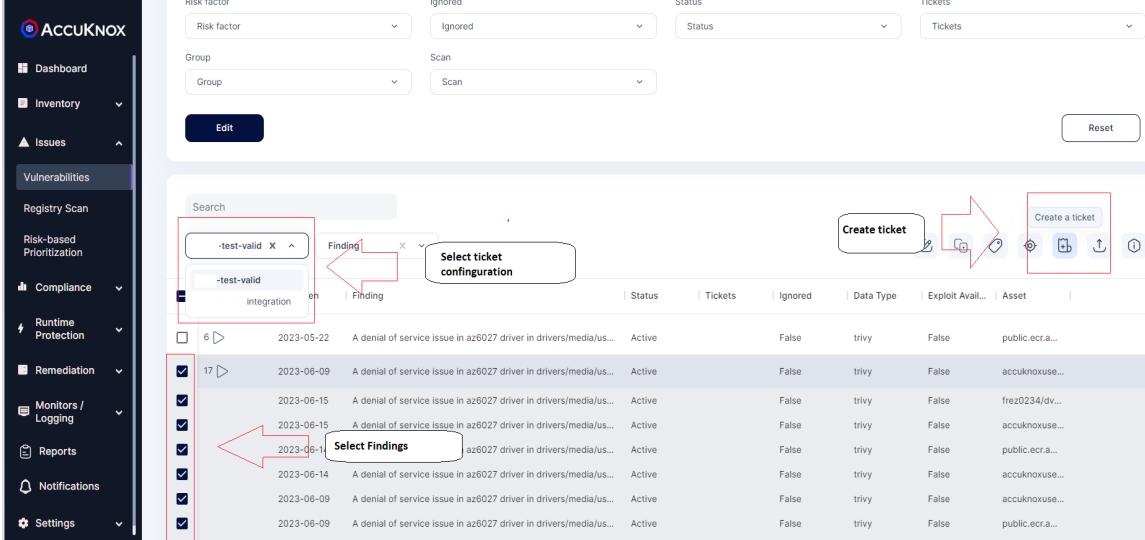


The screenshot shows the AccuKnox interface with the 'Vulnerabilities' section selected in the sidebar. The main area displays a table of findings. The 'Risk factor' dropdown in the top right is highlighted with a red box, showing options like Unknown, Informational, Low, Medium, High, and Critical.

	Group Ids	Last seen	Finding	Status	Tickets	Ignored	Data
<input type="checkbox"/>	173	2023-07-10	Amazon S3 Block Public Access was disabled for S3 bucket t...	Active		False	secu...
<input type="checkbox"/>	62752	2023-06-09	2060: (binutils@2.30-93.el8)	Active		False	trivy...

- How to create automated tickets in Findings and Asset grouping

AccuKnox enables customers to handle the vulnerabilities/findings through auto-creation of tickets on bulk of security findings of similar kind. To create tickets select a set of findings, select the ticketing configuration and click create ticket.



The screenshot shows the 'Edit' screen for creating tickets. It features a search bar with filters for 'Risk factor' (Unknown), 'Status' (Ignored), and 'Tickets'. Below the search bar, there's a 'Group' section with a 'Scan' dropdown. The main area shows a table of findings with checkboxes on the left. A red box highlights the 'Select ticket configuration' button. Another red box highlights the 'Select Findings' button, which is used to filter the list of findings shown below. A third red box highlights the 'Create ticket' button at the top right.

	Group Ids	Last seen	Finding	Status	Tickets	Ignored	Data
<input checked="" type="checkbox"/>	6	2023-05-22	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>	17	2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-15	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-15	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-15	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-14	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...
<input checked="" type="checkbox"/>		2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy...

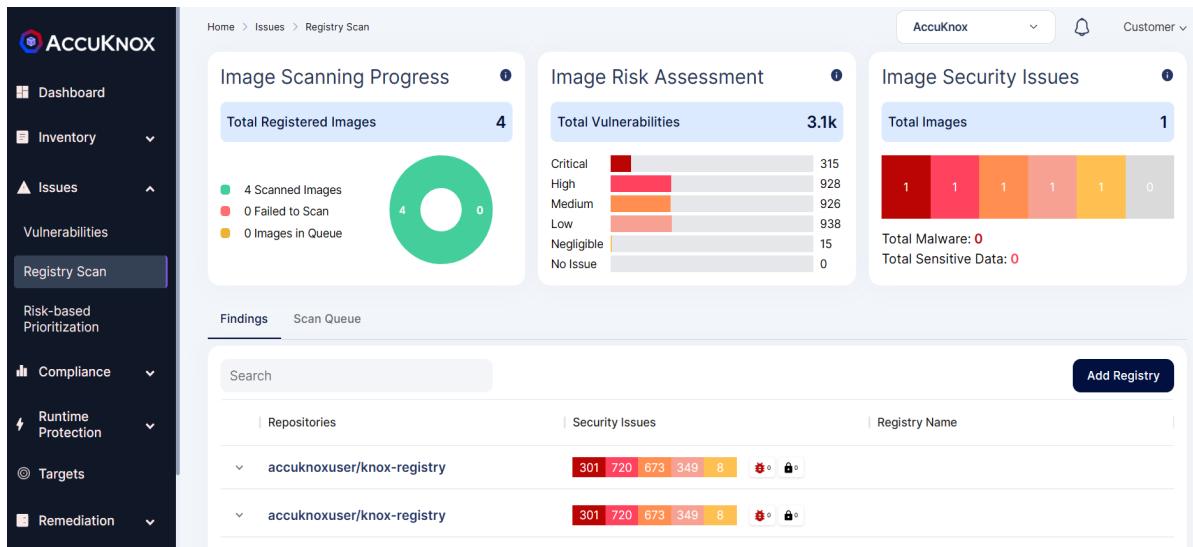
Similarly, the same steps can be followed for creating tickets in asset groupings, click on the desired asset and scroll down to the vulnerabilities section and do the steps.

- How registry scan happens?

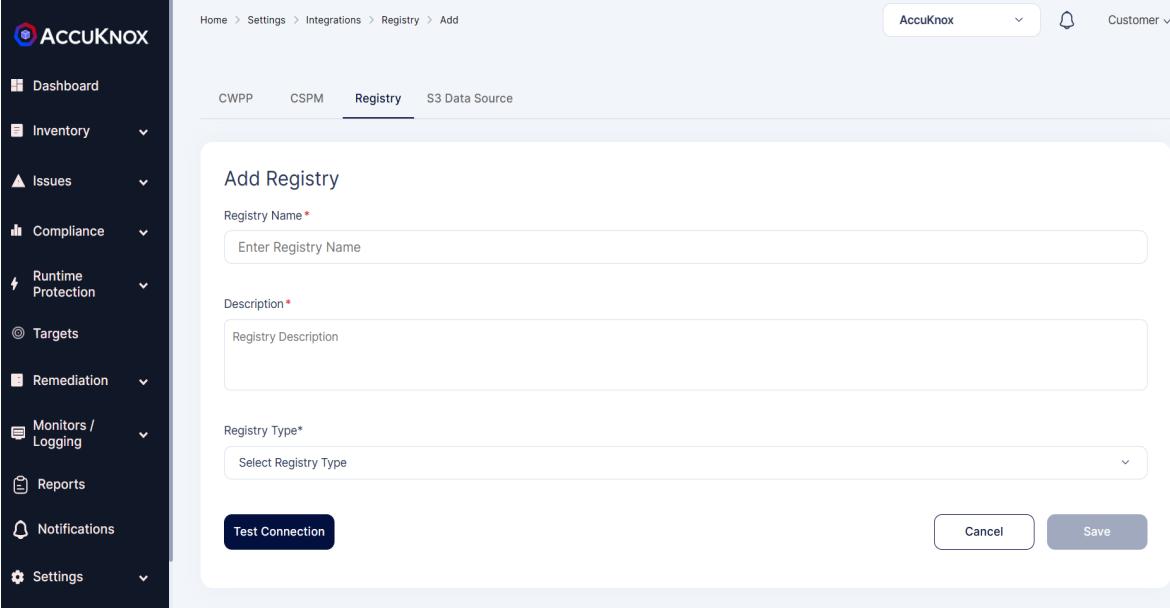
AccuKnox CSPM tool provides with registry scan where the user can onboard their Docker Hub, Nexus, GCR, and ECR registries. Once the registry is onboarded, the scanning of the registry starts automatically in the background. After the scanning is completed, the findings will be populated in the registry scan dashboard.

Registry Onboarding:

Step 1: To onboard a registry user needs to navigate to Issues->Registry Scan.

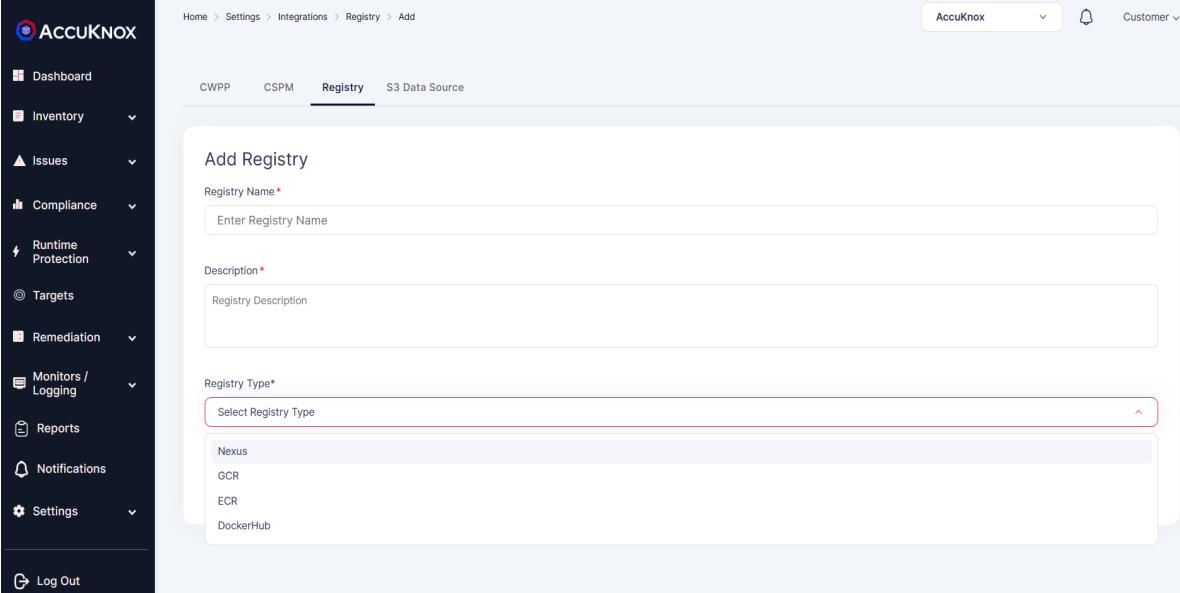


Step 2: The user needs to select Add Registry option from the above screen. When a user clicks Add Registry, they will be directed to a new screen to add registry details.



The screenshot shows the AccuKnox web application's left sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Targets, Remediation, Monitors / Logging, Reports, Notifications, and Settings. The main content area is titled 'Add Registry' under the 'Integrations > Registry' section. It includes fields for 'Registry Name*', 'Description*', 'Registry Type*', and a 'Test Connection' button. At the bottom right are 'Cancel' and 'Save' buttons.

Step 3: User can onboard Nexus, GCR, ECR, DockerHub Registry by giving necessary details.



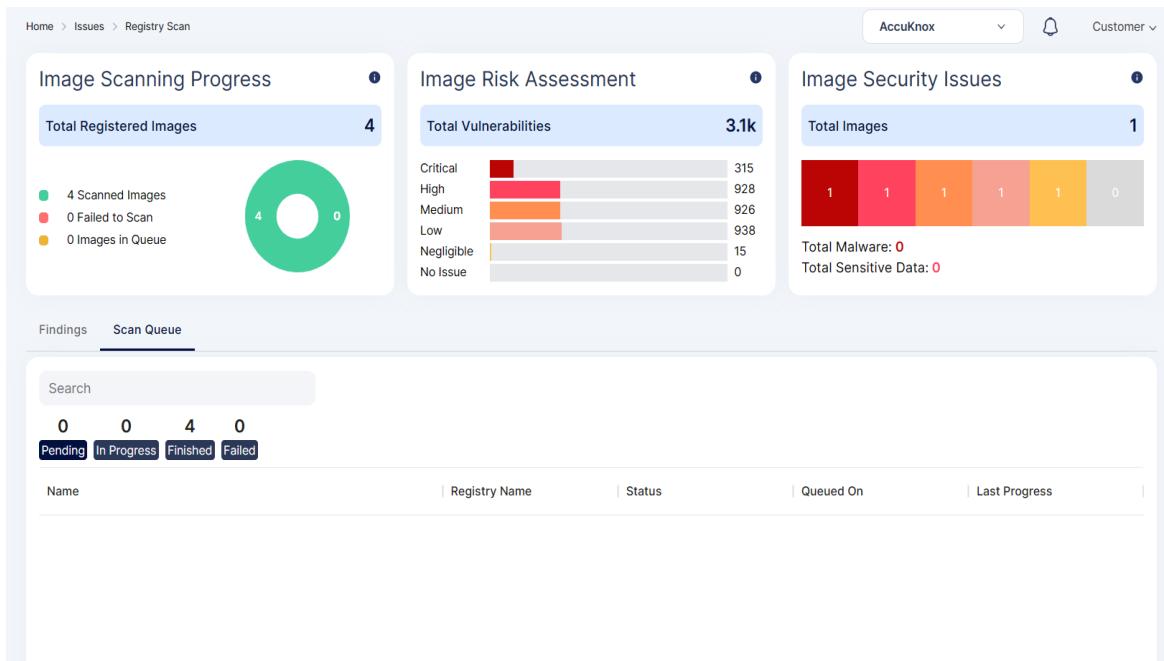
This screenshot is similar to the previous one but shows a dropdown menu for 'Select Registry Type' expanded. The visible options are Nexus, GCR, ECR, and DockerHub. The rest of the interface remains the same, including the sidebar and the 'Add Registry' form.

Step 4: After giving necessary details, the user needs to test connection and save the registry



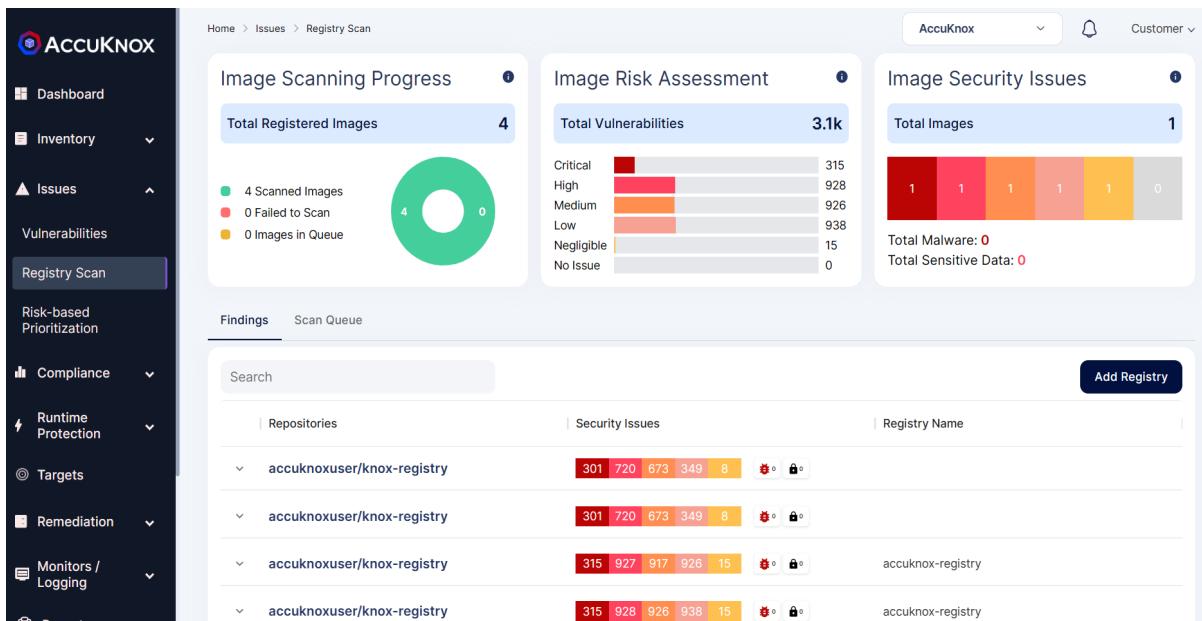
The screenshot shows the 'Add Registry' form. It includes fields for Registry Name (my-docker-registry), Description (docker hub registry), Registry Type (DockerHub), Username (knoxuser), and Password (*****). At the bottom are 'Test Connection', 'Cancel', and 'Save' buttons.

Step 5: Once the user clicks the save option registry will be added and scanning will be done in the background. After the scan is complete the findings data will be populated.



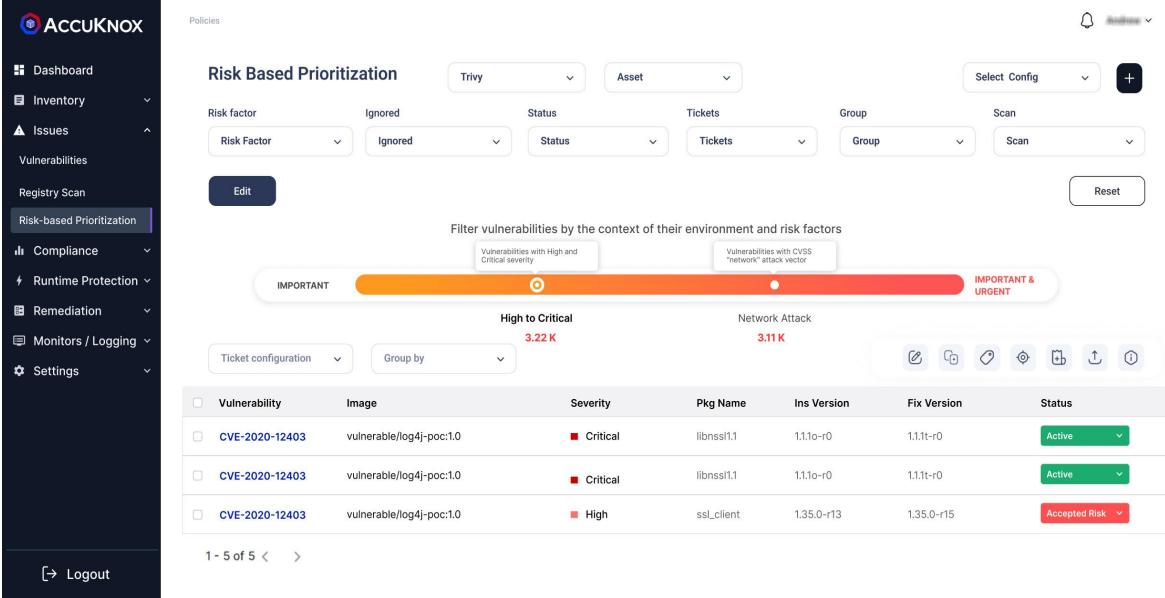
- How to interpret Registry scan results

After the scan is complete, the scan data and findings will be populated into the screen. In this screen the user will be getting information like no. of images scanned and risk associated with the images. Risks are classified as Critical, High, Medium, Low.



- What is Risk Based Prioritization?

In this section, users will be given a comprehensive risk analysis that is found in their onboarded environment. The risks that are identified are classified as High to critical based on the severity of those risks. Users will get details about the risks associated with images, and their CVSS scores identified based on which source and severity of the risk.



The screenshot shows the AccuKnox web interface under the 'Risk-based Prioritization' section. On the left is a dark sidebar with navigation links like Dashboard, Inventory, Issues, Vulnerabilities, Registry Scan, Risk-based Prioritization (which is selected), Compliance, Runtime Protection, Remediation, Monitors / Logging, and Settings. At the bottom of the sidebar is a 'Logout' button.

The main area has a header with dropdowns for 'Policies' (set to Trivy), 'Asset' (set to Ignored), and 'Select Config'. Below this are several filter dropdowns: 'Risk factor' (set to Ignored), 'Status' (set to Ignored), 'Tickets' (set to Status), 'Group' (set to Group), and 'Scan' (set to Scan). There's also an 'Edit' button and a 'Reset' button.

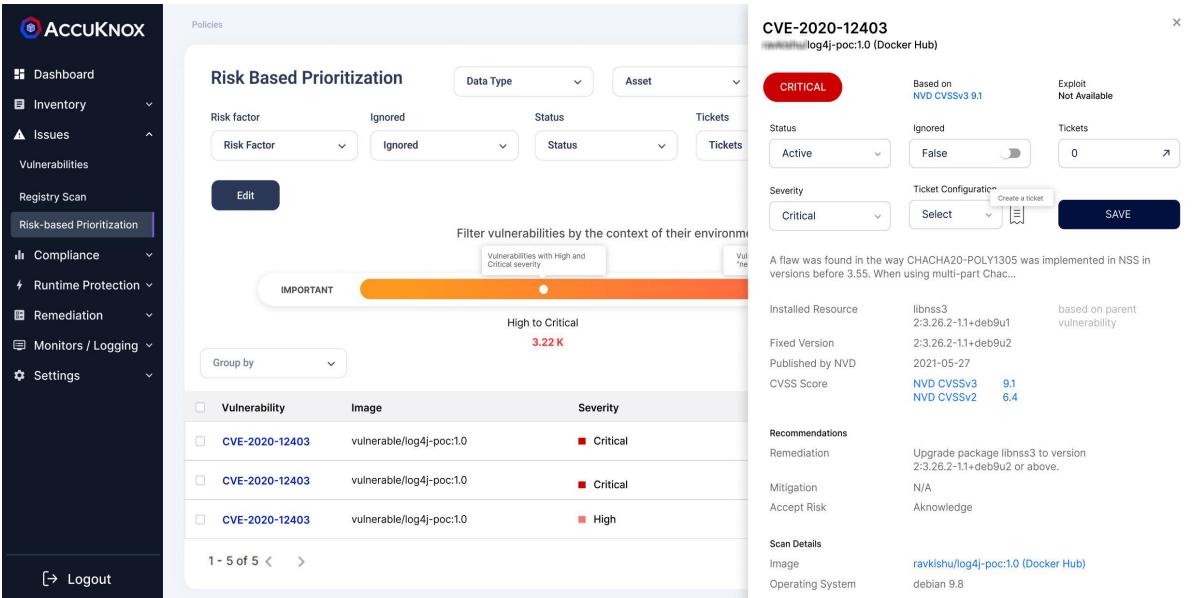
A horizontal bar at the top indicates the context of environment and risk factors, with segments for 'Vulnerabilities with High and Critical severity' and 'Vulnerabilities with CVSS "network" attack vector'. Below this is a progress bar labeled 'IMPORTANT' on the left and 'IMPORTANT & URGENT' on the right.

The central part of the screen displays two counts: 'High to Critical' (3.22 K) and 'Network Attack' (3.11 K). Below these are buttons for 'Ticket configuration' and 'Group by'. A table follows, showing three rows of vulnerability details:

Vulnerability	Image	Severity	Pkg Name	Ins Version	Fix Version	Status
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical	libnss1.1	1.1.0-r0	1.1.1t-r0	Active
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical	libnss1.1	1.1.0-r0	1.1.1t-r0	Active
CVE-2020-12403	vulnerable/log4j-poc:1.0	High	ssl_client	1.35.0-r13	1.35.0-r15	Accepted Risk

At the bottom of the table are navigation buttons for '1 - 5 of 5' and '< >'.

When a user clicks on the risk from the list, they will be getting more details related to the risks like the package associated with the risk. It also gives details related to the risks, the CVSS score of the risk, and the associated image where the risk is present.



This screenshot shows the same AccuKnox interface as the previous one, but with a modal window open on the right side. The modal is titled 'CVE-2020-12403' and describes a flaw found in libnss3. It includes tabs for 'CRITICAL' (selected), 'Based on NVD CVSSv3 9.1', and 'Exploit Not Available'. The 'Status' dropdown is set to 'Active', 'Ignored' is set to 'False', and 'Tickets' is set to '0'. The 'Severity' dropdown is set to 'Critical'. Below these are buttons for 'Ticket Configuration' (with a 'Create a ticket' link) and 'SAVE'.

The modal also contains a large amount of detailed information about the vulnerability, including:

- Installed Resource:** libnss3 2:3.26.2-1.1+deb9u1 based on parent vulnerability
- Fixed Version:** 2:3.26.2-1.1+deb9u2
- Published by NVD:** 2021-05-27
- CVSS Score:** NVD CVSSv3 9.1, NVD CVSSv2 6.4
- Recommendations:** Remediation: Upgrade package libnss3 to version 2:3.26.2-1.1+deb9u2 or above. Mitigation: N/A. Accept Risk: Acknowledge.
- Scan Details:** Image: ravkishu/log4j-poc:1.0 (Docker Hub), Operating System: debian 9.8

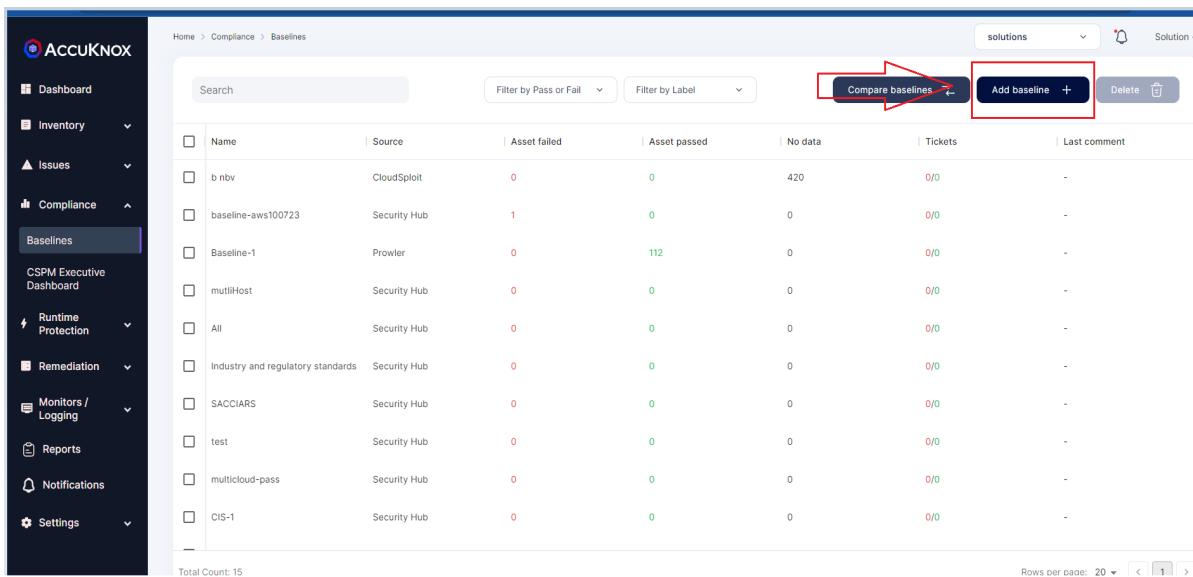
Baseline

- How to create a Baseline out of a data source

AccuKnox's Baseline is an approach to detect drift in configuration from the conformance suite from multiple 'data sources' that AccuKnox and that can be associated to a specific 'asset' or 'group' of assets. It is a golden benchmark that is used to detect any change in compliance behavior proactively.

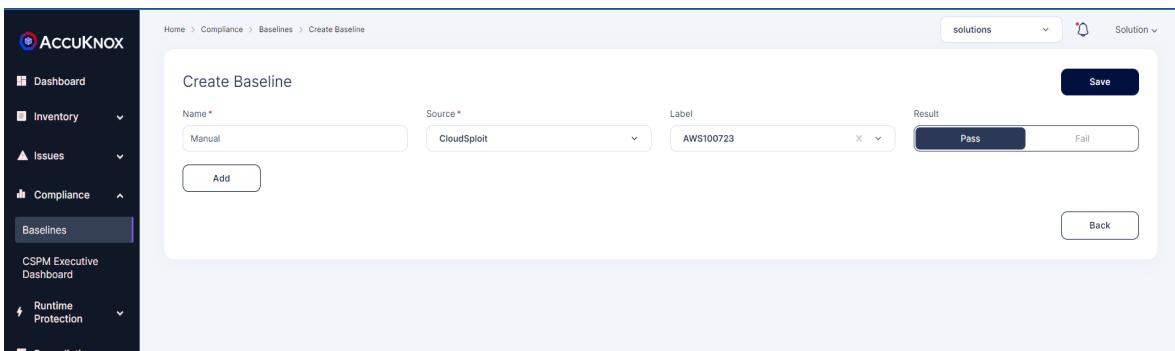
To create a baselines follow these steps:

Step 1: Head to the Baselines page and click on add baseline



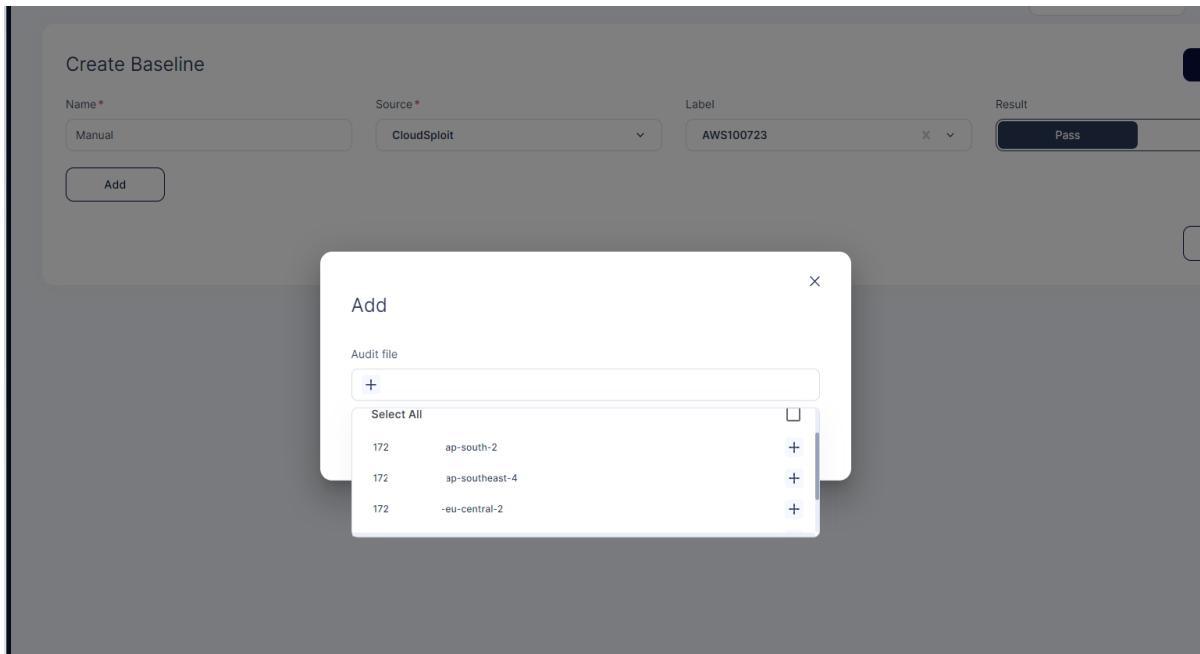
The screenshot shows the AccuKnox Compliance Baselines page. On the left is a dark sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance (Baselines selected), Runtime Protection, Remediation, Monitors / Logging, Reports, Notifications, and Settings. The main area has a header with 'Home > Compliance > Baselines'. Below the header is a search bar and two filter dropdowns ('Filter by Pass or Fail' and 'Filter by Label'). To the right of these are three buttons: 'Compare baselines' (with a red box and arrow), 'Add baseline' (highlighted with a red box and plus sign), and 'Delete'. The main content area is a table with columns: Name, Source, Asset failed, Asset passed, No data, Tickets, and Last comment. The table lists several baselines: 'b nbv' (CloudSploit), 'baseline-aws100723' (Security Hub), 'Baseline-1' (Prowler), 'multiHost' (Security Hub), 'All' (Security Hub), 'Industry and regulatory standards' (Security Hub), 'SACCIARS' (Security Hub), 'test' (Security Hub), 'multicloud-pass' (Security Hub), and 'CIS-1' (Security Hub). At the bottom of the table, it says 'Total Count: 15' and 'Rows per page: 20'. There are also navigation arrows at the bottom right.

Step 2: Provide a name , select the source and select the bias for your baseline and add a label for your baseline

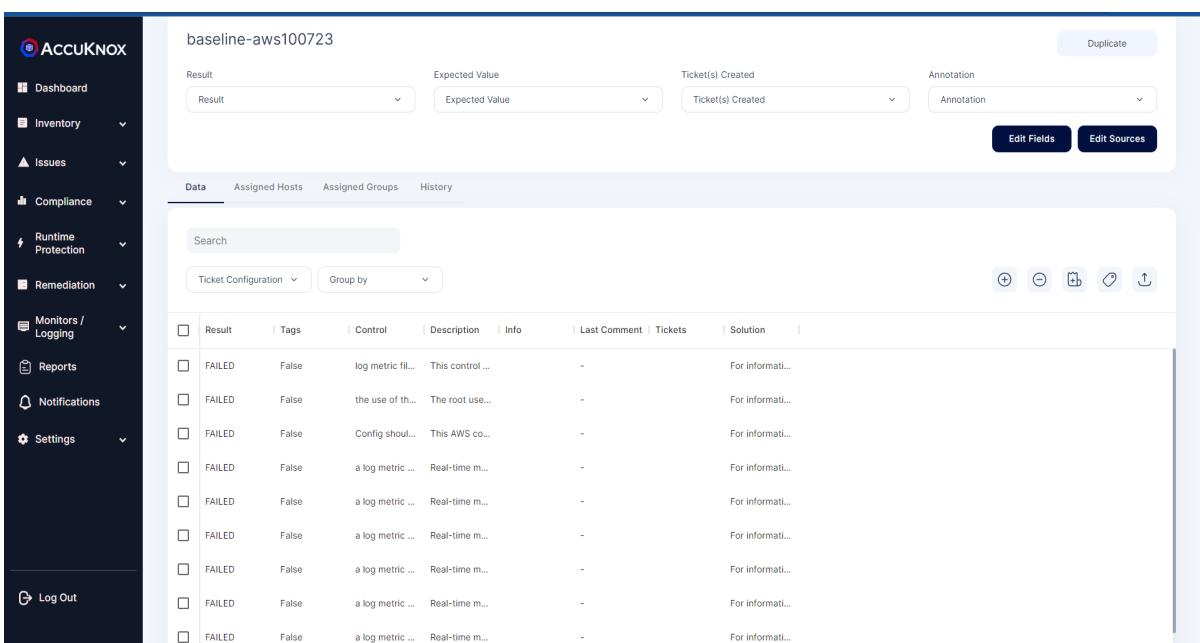


The screenshot shows the 'Create Baseline' form. The left sidebar is identical to the previous screenshot. The main form has a title 'Create Baseline'. It contains fields for 'Name' (set to 'Manual'), 'Source' (set to 'CloudSploit'), 'Label' (set to 'AWS100723'), and 'Result' (set to 'Pass'). Below these fields is a large text area labeled 'Add' which is currently empty. At the bottom right of the form are 'Save' and 'Back' buttons.

Step 3: Finally add the audit files by clicking on add, these files contain the compliance analysis from different cloud accounts.



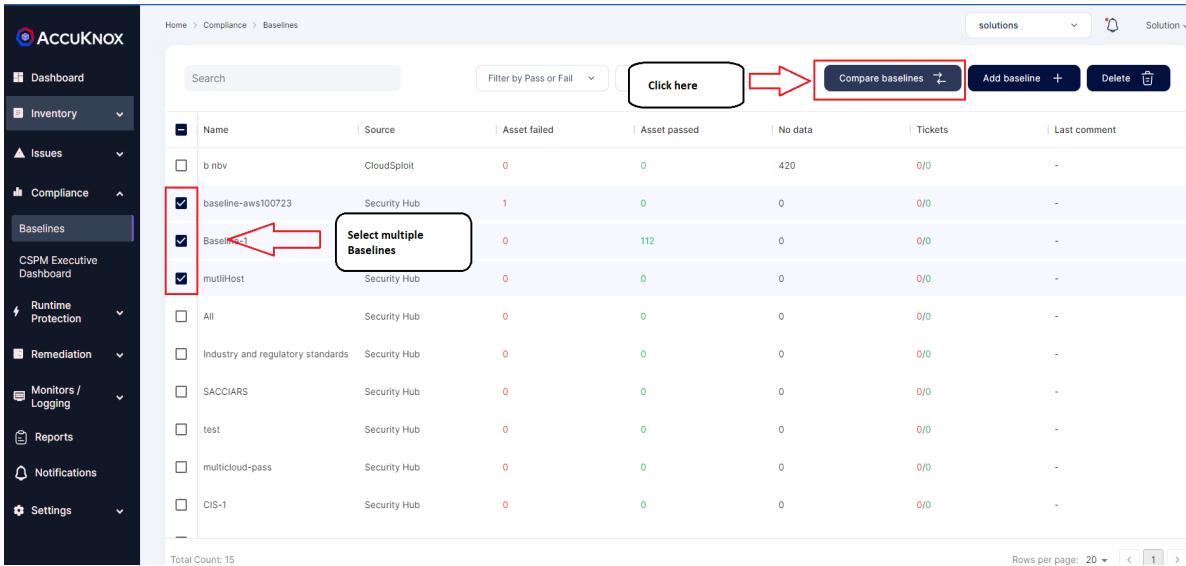
Now you can see the compliance analysis by clicking on the baseline that you created



- How to compare 2 baselines

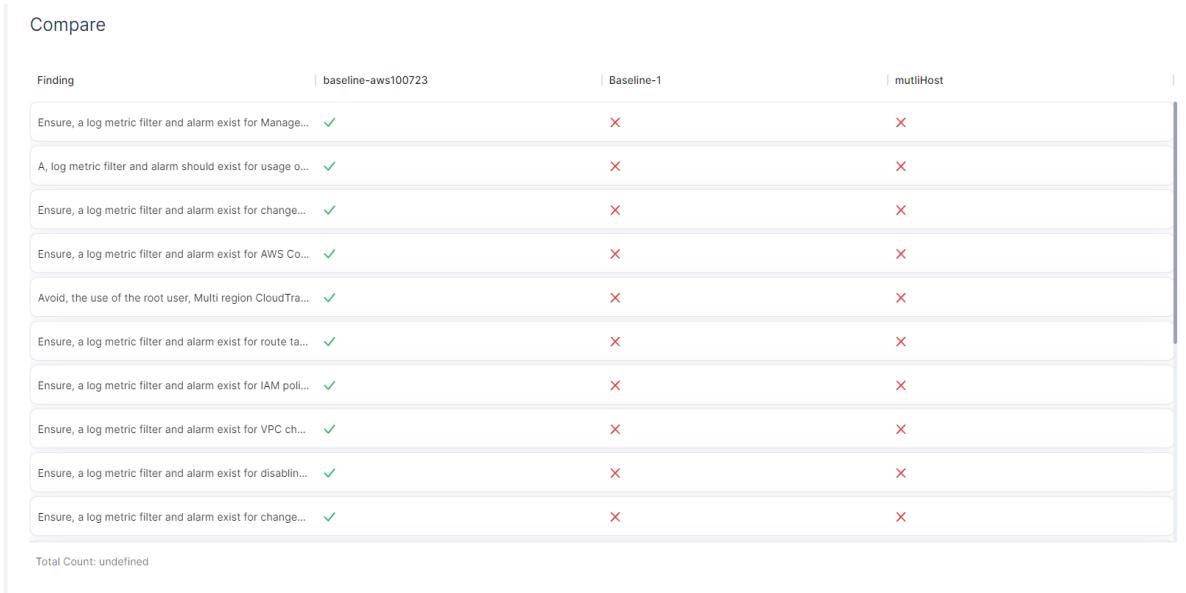
Once you have created a baseline for your cloud infrastructure, to ensure continuous compliance you can create another baseline and compare them to see if there is any drift in the configuration between your past baseline and your current baseline.

To compare your baselines , select multiple baseline baselines and click on compare baselines to see the comparison.



The screenshot shows the AccuKnox Compliance Baselines page. On the left, a sidebar menu includes 'Baselines' under the 'Compliance' section. In the main area, a table lists various baselines. Two specific baselines are selected: 'baseline-aws100723' and 'Baseline-1'. A red arrow points from the text 'Select multiple Baselines' to the selected rows. Another red arrow points from the 'Compare baselines' button to the right. The table columns include Name, Source, Asset failed, Asset passed, No data, Tickets, and Last comment. The total count at the bottom is 15.

The comparison will look like following



The screenshot shows a 'Compare' results table. It has four columns: Finding, baseline-aws100723, Baseline-1, and mutliHost. The table lists 14 findings, each with a green checkmark or a red 'X'. The findings are:

Finding	baseline-aws100723	Baseline-1	mutliHost
Ensure, a log metric filter and alarm exist for Manage...	✓	✗	✗
A, log metric filter and alarm should exist for usage o...	✓	✗	✗
Ensure, a log metric filter and alarm exist for change...	✓	✗	✗
Ensure, a log metric filter and alarm exist for AWS Co...	✓	✗	✗
Avoid, the use of the root user, Multi region CloudTra...	✓	✗	✗
Ensure, a log metric filter and alarm exist for route ta...	✓	✗	✗
Ensure, a log metric filter and alarm exist for IAM poli...	✓	✗	✗
Ensure, a log metric filter and alarm exist for VPC ch...	✓	✗	✗
Ensure, a log metric filter and alarm exist for disablin...	✓	✗	✗
Ensure, a log metric filter and alarm exist for change...	✓	✗	✗

Total Count: undefined

Compliance

AccuKnox helps you to review your cloud infrastructure health and compliance posture. AccuKnox also helps you to generate reports that contain summary and detailed assessment of vulnerability/findings and compliance risks in your cloud infrastructure or in applications.

- **How to get Compliance for Cloud Assets**
 - Each baseline is a set of compliance checks for configuration of your cloud infrastructure against various benchmarks and frameworks.
 - Source selection while creating baselines lets you control the framework or benchmark you want analysis against, e.g. CloudSploit provides PCI DSS, HIPPA and CIS compliance analysis.
 - CSPM Dashboard displays the compliance score for different frameworks for each cloud account onboarded.

AccuKnox

AccuKnox Runtime Protection (CWPP) Report

Prepared by : AccuKnox
 Prepared for : Demo-Tenant-Name
 Duration : 28th Mar 18:09:19 - 1st May 10:23:10

CWPP Dashboard

Clusters	2	 60%	 70%
Namespace	1	 40%	 5%
Active Clusters	1		
InActive Clusters	1		

Selected Cluster
eks-prod, eks-dev

Selected Namespace
default

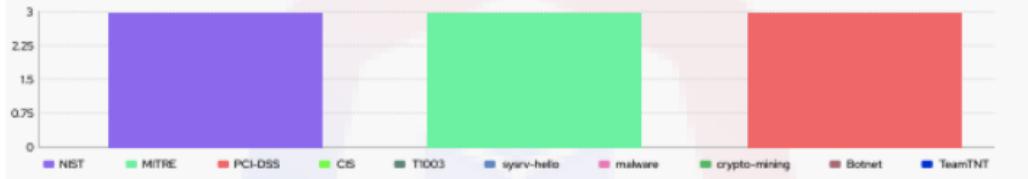
→ [Alerts Summary](#)

Total Alerts Generated	Total Blocked Alerts	Total Audited Alerts
663	119	544

→ [Compliance Summary](#)

MITRE	NIST	CIS	PCI-DSS
3	3	0	3

→ [Compliance Alerts](#)



A bar chart showing the count of alerts for various compliance frameworks. The y-axis ranges from 0 to 3. The x-axis categories are NIST (purple), MITRE (green), PCI-DSS (red), CIS (light green), T1003 (blue), svyrv-hello (pink), malware (yellow), crypto-mining (orange), Botnet (dark red), and TeamTNT (dark blue). The chart shows 3 for NIST, 3 for MITRE, 0 for CIS, and 3 for PCI-DSS.

→ [Namespace Severity Summary](#)



A bar chart showing the count of alerts by namespace severity level. The y-axis ranges from 0 to 3. The x-axis categories are Severity1 through Severity10. The chart shows a single bar at 3 for Severity6.

→ [Top 10 Policies by Alert Count](#)



A bar chart showing the top 10 policies by alert count. The y-axis ranges from 0 to 800. The x-axis categories are DefaultPosture, ksp-vault-protect, and ksp-vault-protect-lsp. The chart shows a single bar at approximately 750 for DefaultPosture.

→ [Namespace Alerts](#)



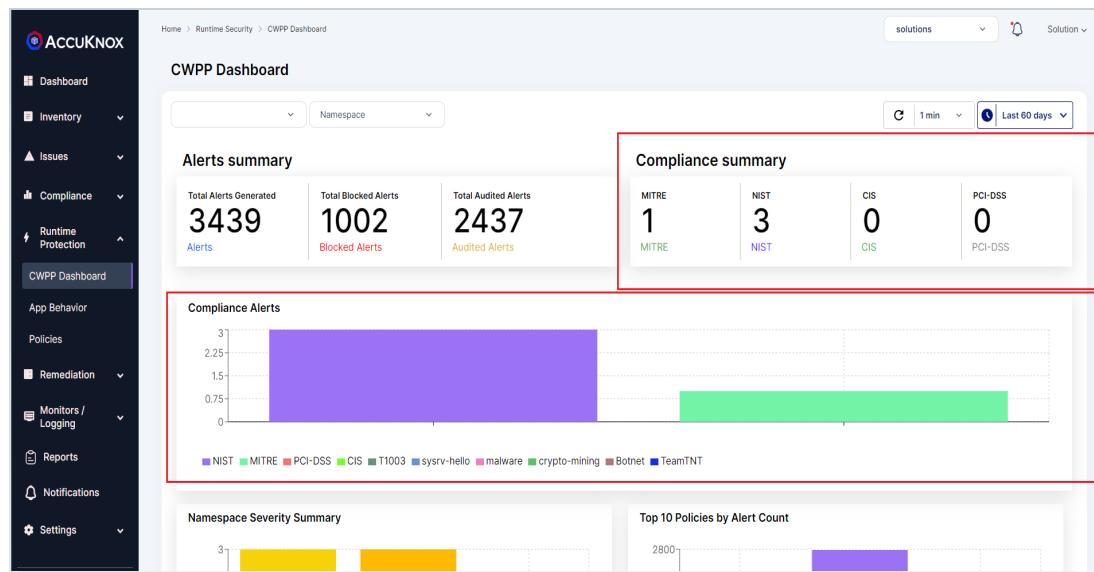
A donut chart showing the distribution of namespace alerts. The chart is mostly purple, with a small sliver of another color visible.

→ [Pod Alerts](#)



A donut chart showing the distribution of pod alerts. The chart is mostly purple, with a small sliver of another color visible.

- How to get Compliance for Cloud Workload
 - AccuKnox leverage KubeArmor to harden your workload by enforcing hardening policies
 - These hardening policies are based on different compliance frameworks like NIST, CIS, MITRE etc.
 - When these policies get enforced and we get the logs based on these policies, then the compliance analysis can be seen from CWPP Dashboard.



App Behavior

Application Behavior of the cluster workloads that are onboarded to the AccuKnox SaaS are collected with help of KubeArmor and the AccuKnox Agents that are installed as Daemon sets in the cluster. The informations are collected at the pod level granularity. So that the users can get the information about each pods that are running in each namespaces. Application behavior of the cluster workloads are given in two ways, one is the list view and other is the Graphical view.

- How to interpret network graph

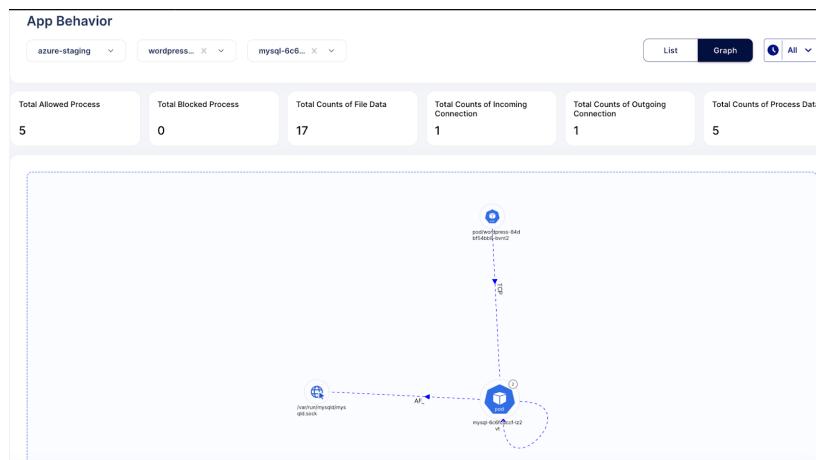
Lets understand this by following use-case example - **Auditing Application Behavior of MySQL application**

1. Install workload:

```
sh           kubectl          apply      -f
https://raw.githubusercontent.com/kubearmory/KubeArmor/main/examples
/wordpress-mysql/wordpress-mysql-deployment.yaml
```

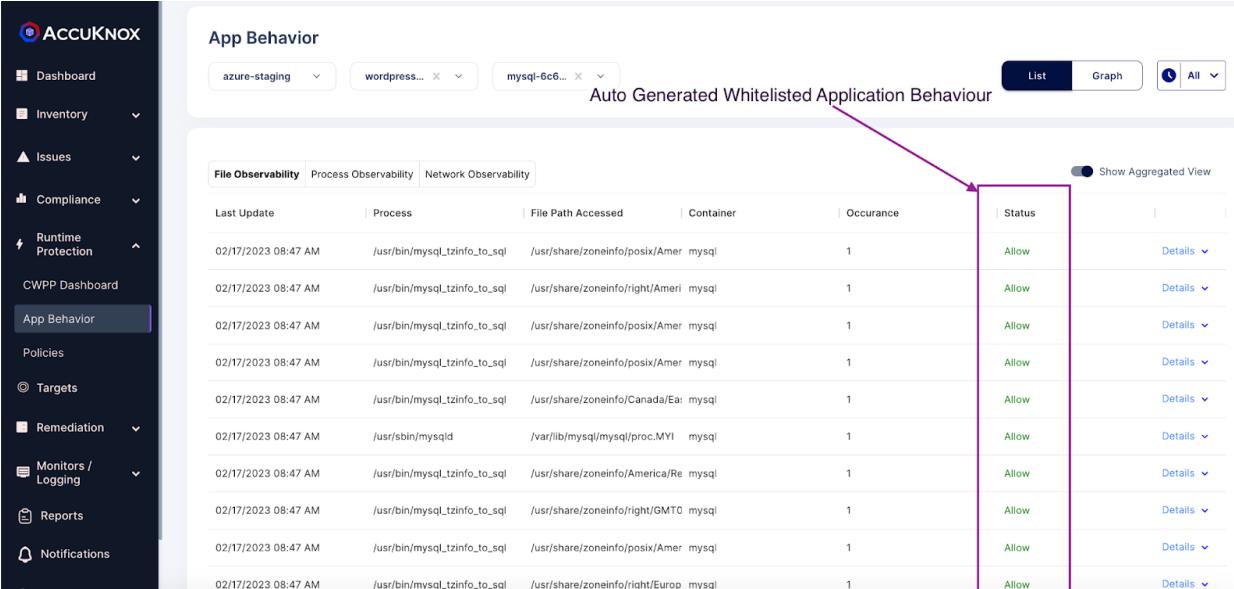
2. Showing App behavior screen in the context of the wordpress-mysql application. To see the Application Behavior user must Navigate to the *Runtime Protection->App Behavior* section. Then click on the Cluster and Namespace and pod from the filters to see the Application Behavior.

- Network Graph: This view gives the graphical representation of Ingress and Egress traffic that are occurring in the Pod. When we click on the connections we can get a clear view of the traffic type and port details.





- File Observability: This view gives details about the files that are getting accessed in the pod.

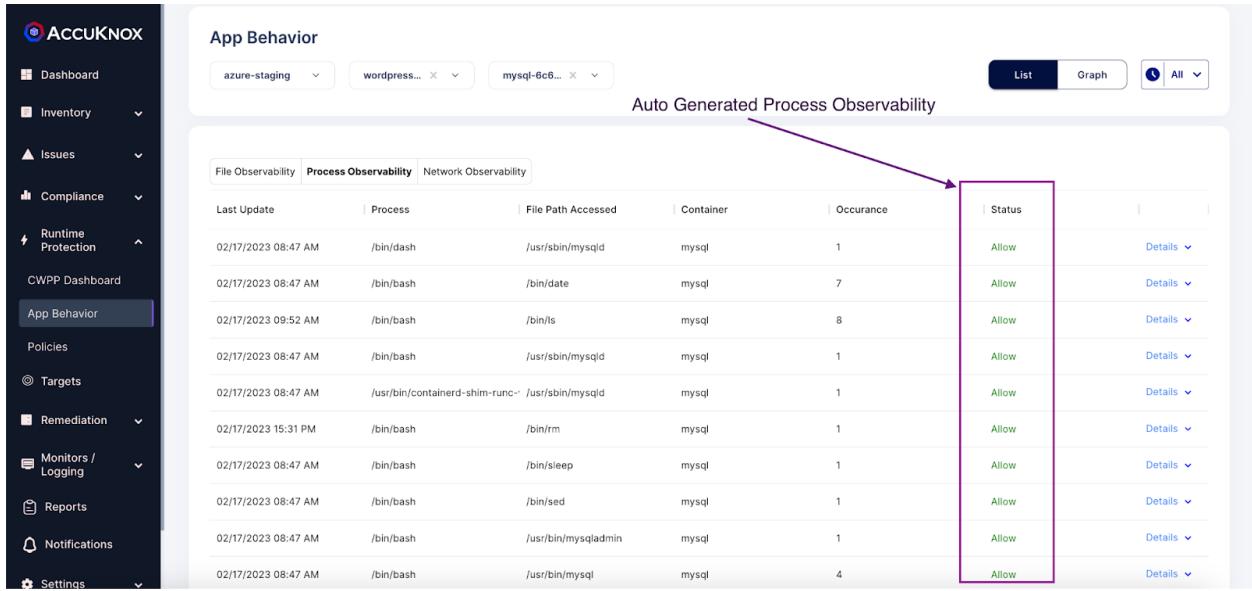


App Behavior

Auto Generated Whitelisted Application Behaviour

Last Update	Process	File Path Accessed	Container	Occurance	Status	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/America/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/America/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/America/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/America/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/Canada/Eastern/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/sbin/mysqld	/var/lib/mysql/mysql/proc.MYI		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/America/Reykjavik/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/GMT0/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/America/mysql		1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/Europe/mysql		1	Allow	Details

- Process Observability: This view gives the details of Processes that are currently running in the Pod.

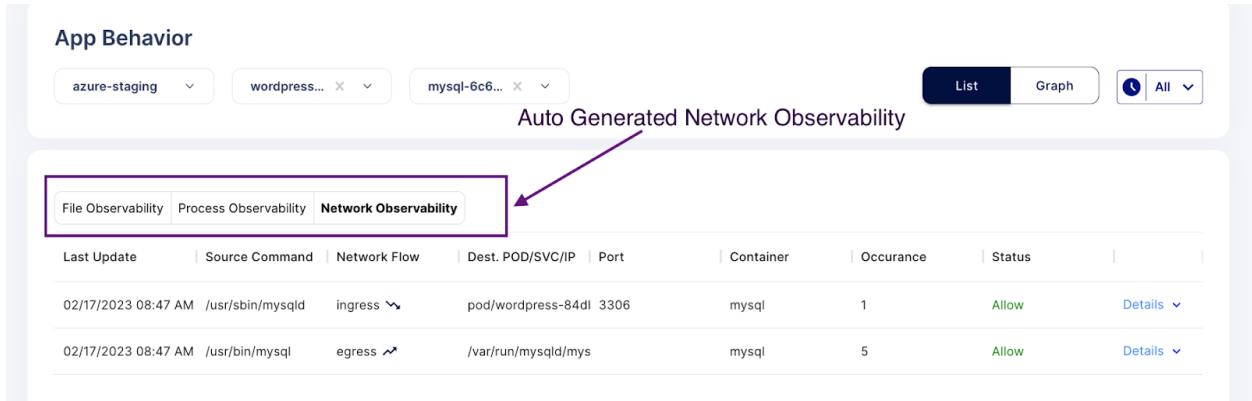


App Behavior

Auto Generated Process Observability

Last Update	Process	File Path Accessed	Container	Occurance	Status
02/17/2023 08:47 AM	/bin/dash	/usr/sbin/mysqld	mysql	1	Allow
02/17/2023 08:47 AM	/bin/bash	/bin/date	mysql	7	Allow
02/17/2023 09:52 AM	/bin/bash	/bin/ls	mysql	8	Allow
02/17/2023 08:47 AM	/bin/bash	/usr/sbin/mysqld	mysql	1	Allow
02/17/2023 08:47 AM	/usr/bin/containerd-shim-runc-	/usr/sbin/mysqld	mysql	1	Allow
02/17/2023 15:31 PM	/bin/bash	/bin/rm	mysql	1	Allow
02/17/2023 08:47 AM	/bin/bash	/bin/sleep	mysql	1	Allow
02/17/2023 08:47 AM	/bin/bash	/bin/sed	mysql	1	Allow
02/17/2023 08:47 AM	/bin/bash	/usr/bin/mysqladmin	mysql	1	Allow
02/17/2023 08:47 AM	/bin/bash	/usr/bin/mysql	mysql	4	Allow

- Network Observability: The network observability can also be seen in the list here you can see the details of ingress and egress traffic in the list view.



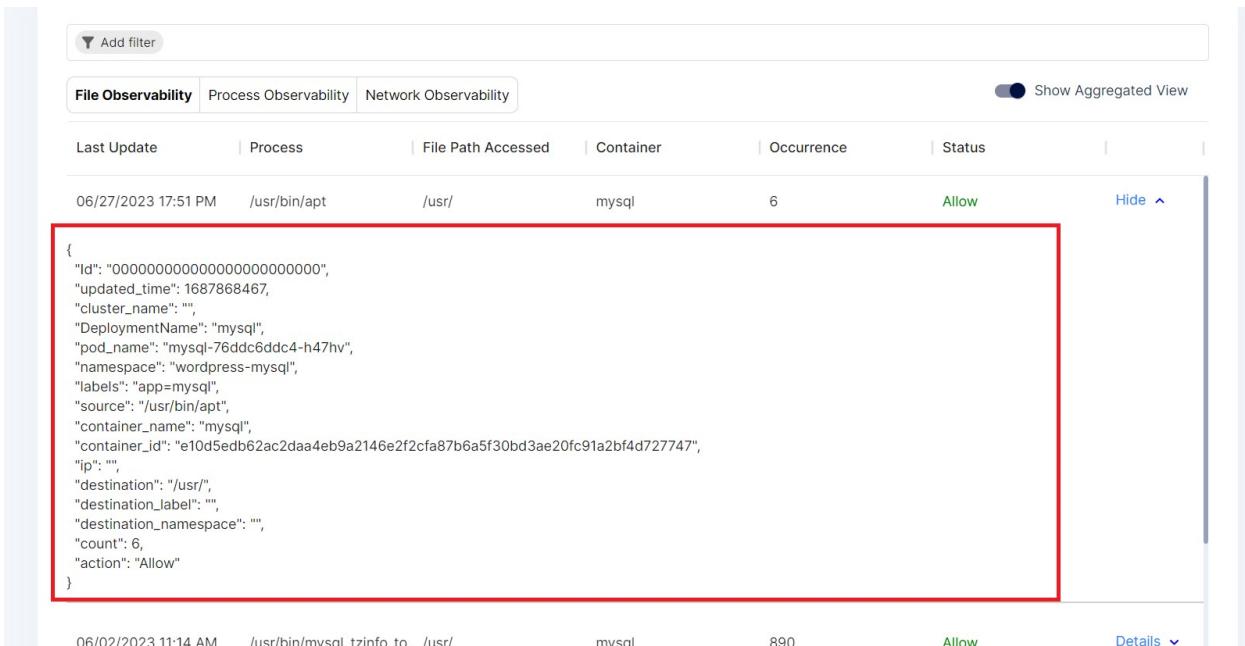
App Behavior

Auto Generated Network Observability

Last Update	Source Command	Network Flow	Dest. POD/SVC/IP	Port	Container	Occurance	Status
02/17/2023 08:47 AM	/usr/sbin/mysqld	ingress ↗	pod/wordpress-84d1	3306	mysql	1	Allow
02/17/2023 08:47 AM	/usr/bin/mysql	egress ↘	/var/run/mysqld/mys		mysql	5	Allow

- How to see App Behavior Telemetry

- To see the contextual information about the File and Network and Process observability user needs to navigate to the *Runtime Protection->App Behavior* Section.
- **File Observability Telemetry:** To see the file observability related telemetry user needs to click the list view and select file observability part and click on any of the file events to see the Telemetry

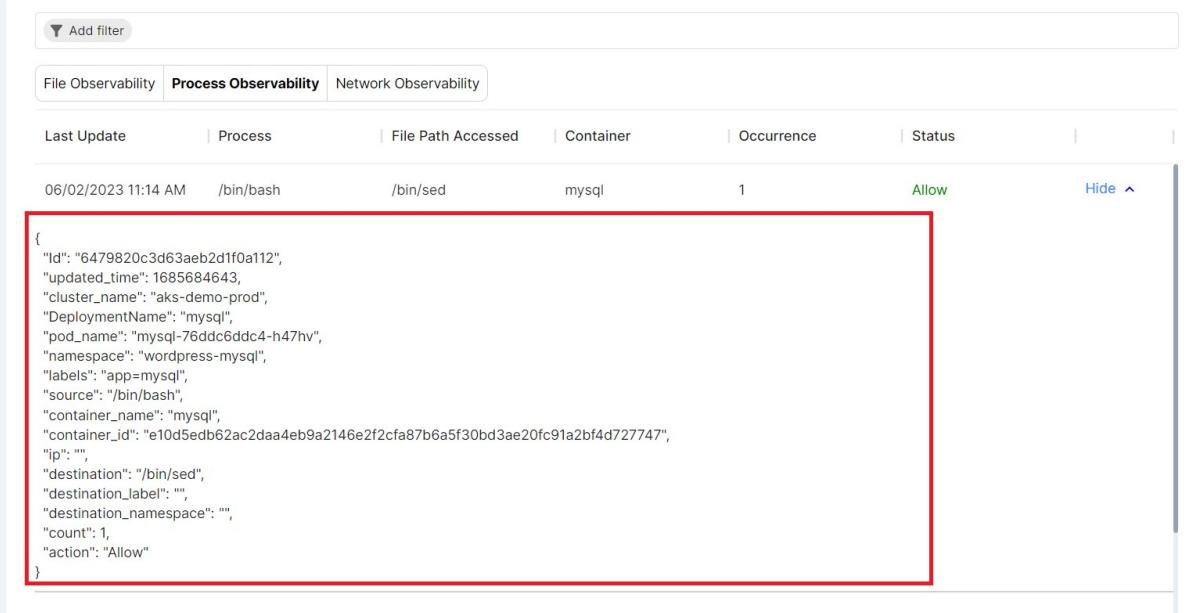


The screenshot shows a web-based interface for monitoring application behavior. At the top, there are tabs for "File Observability", "Process Observability", and "Network Observability". A "Show Aggregated View" button is also present. Below the tabs is a table header with columns: Last Update, Process, File Path Accessed, Container, Occurrence, Status, and a "Details" column with a dropdown arrow. The first row of data is highlighted with a red border. The "Status" column for this row shows "Allow". The "Details" column contains a "Hide" link. The "File Path Accessed" column displays the JSON data for the event:

```
{
  "Id": "00000000000000000000000000000000",
  "updated_time": 1687968467,
  "cluster_name": "",
  "DeploymentName": "mysql",
  "pod_name": "mysql-76ddc6ddc4-h47hv",
  "namespace": "wordpress-mysql",
  "labels": "app=mysql",
  "source": "/usr/bin/apt",
  "container_name": "mysql",
  "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfab7b6a5f30bd3ae20fc91a2bf4d727747",
  "ip": "",
  "destination": "/usr/",
  "destination_label": "",
  "destination_namespace": "",
  "count": 6,
  "action": "Allow"
}
```

Below this row, another row of data is partially visible, showing a timestamp of "06/02/2023 11:14 AM", a process name of "/usr/bin/mysql_tzinfo_to_ /usr/", a container name of "mysql", an occurrence count of "890", and a status of "Allow". The "Details" column for this row has a "Details" link with a dropdown arrow.

- **Process Observability Telemetry:** To see the process observability related telemetry user needs to click the list view and select process observability part and click on any of the process events to see the Telemetry



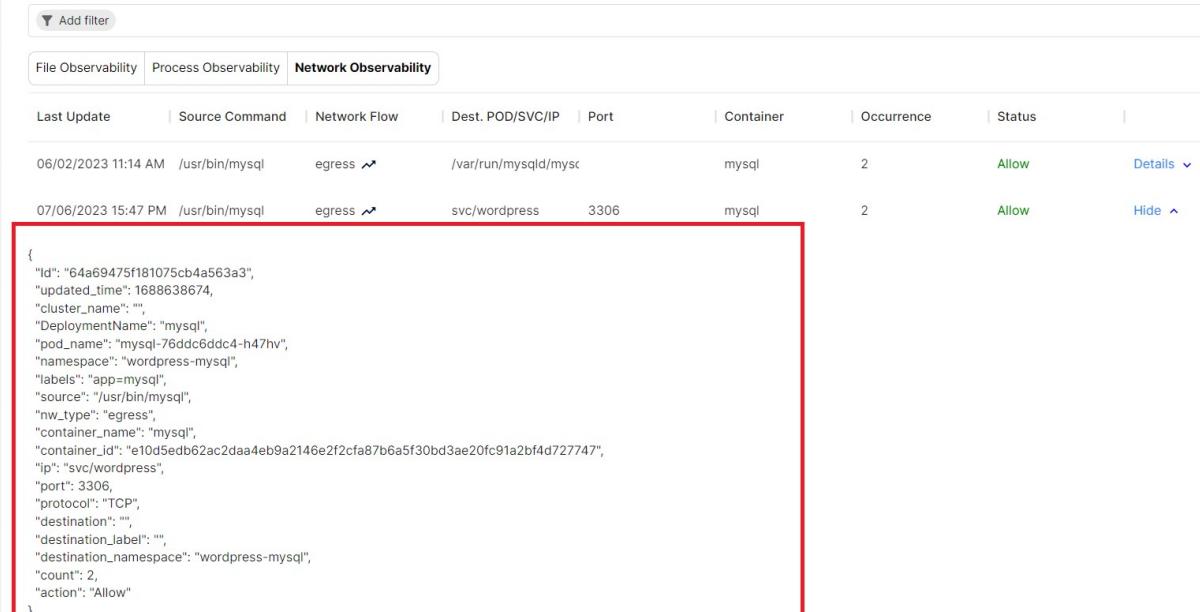
The screenshot shows a table with the following columns: Last Update, Process, File Path Accessed, Container, Occurrence, Status, and a Hide button. There is one row visible:

Last Update	Process	File Path Accessed	Container	Occurrence	Status	Hide
06/02/2023 11:14 AM	/bin/bash	/bin/sed	mysql	1	Allow	Hide

A red box highlights the JSON data for the first event:

```
{
  "Id": "6479820c3d63aeb2d1f0a112",
  "updated_time": 1685684643,
  "cluster_name": "aks-demo-prod",
  "DeploymentName": "mysql",
  "pod_name": "mysql-76ddc6ddc4-h47hv",
  "namespace": "wordpress-mysql",
  "labels": "app=mysql",
  "source": "/bin/bash",
  "container_name": "mysql",
  "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747",
  "ip": "",
  "destination": "/bin/sed",
  "destination_label": "",
  "destination_namespace": "",
  "count": 1,
  "action": "Allow"
}
```

- **Network observability:** To see the Network observability related telemetry user needs to click the list view and select Network observability part and click on any of the Network events to see the Telemetry



The screenshot shows a table with the following columns: Last Update, Source Command, Network Flow, Dest. POD/SVC/IP, Port, Container, Occurrence, Status, and a Details button. There are two rows visible:

Last Update	Source Command	Network Flow	Dest. POD/SVC/IP	Port	Container	Occurrence	Status	Details
06/02/2023 11:14 AM	/usr/bin/mysql	egress ↗	/var/run/mysqld/mysq		mysql	2	Allow	Details
07/06/2023 15:47 PM	/usr/bin/mysql	egress ↗	svc/wordpress	3306	mysql	2	Allow	Hide

A red box highlights the JSON data for the first event:

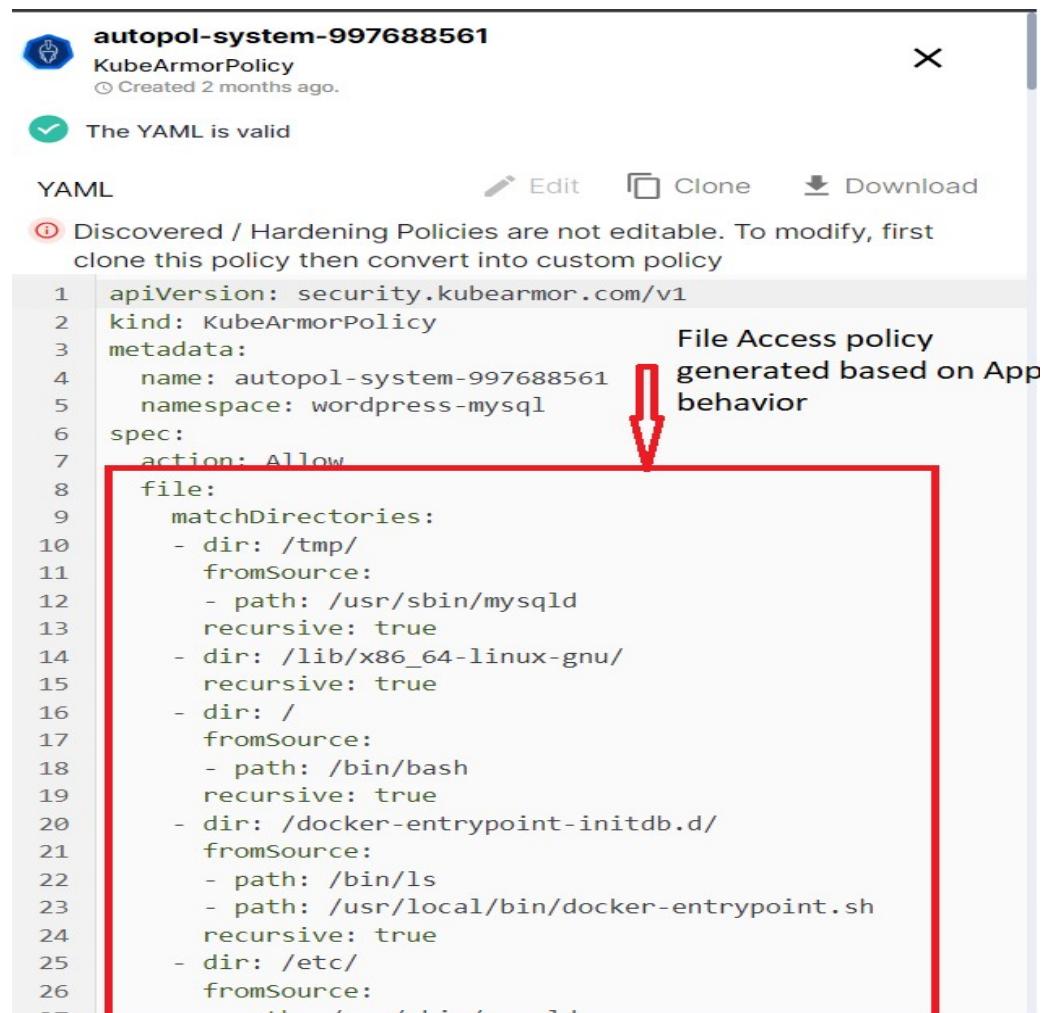
```
{
  "Id": "64a69475f181075cb4a563a3",
  "updated_time": 1688638674,
  "cluster_name": "",
  "DeploymentName": "mysql",
  "pod_name": "mysql-76ddc6ddc4-h47hv",
  "namespace": "wordpress-mysql",
  "labels": "app=mysql",
  "source": "/usr/bin/mysql",
  "nw_type": "egress",
  "container_name": "mysql",
  "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747",
  "ip": "svc/wordpress",
  "port": 3306,
  "protocol": "TCP",
  "destination": "",
  "destination_label": "",
  "destination_namespace": "wordpress-mysql",
  "count": 2,
  "action": "Allow"
}
```

Runtime Protection w/ Policy Management

- **How to understand discover policies**

Auto Discovered Policies are generated based on the Application Behavior. AccuKnox Runtime Security Engine KubeArmor when deployed as agent will model the default application behavior of the workload and comes up with the Auto discovered policies.

- **File access behavior based policies:** Based on the files that are accessed in pod, the Auto discovered system policies are generated. To view that policy user must navigate to *Runtime Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered policies.



autopol-system-997688561 ×

KubeArmorPolicy
Created 2 months ago.

The YAML is valid

YAML Edit Clone Download

Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```

1  apiVersion: security.kubearmory.com/v1
2  kind: KubeArmorPolicy
3  metadata:
4    name: autopol-system-997688561
5    namespace: wordpress-mysql
6  spec:
7    action: Allow
8    file:
9      matchDirectories:
10     - dir: /tmp/
11       fromSource:
12         - path: /usr/sbin/mysql
13         recursive: true
14     - dir: /lib/x86_64-linux-gnu/
15         recursive: true
16     - dir: /
17       fromSource:
18         - path: /bin/bash
19         recursive: true
20     - dir: /docker-entrypoint-initdb.d/
21       fromSource:
22         - path: /bin/ls
23         - path: /usr/local/bin/docker-entrypoint.sh
24         recursive: true
25     - dir: /etc/
26       fromSource:
27

```

File Access policy generated based on App behavior

- **Process access behavior based policies:** Based on the process that are running in pod, the Auto discovered system policies are generated. To view that policy user must navigate to *Runtime Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered policies.

```
process:  
  matchDirectories:  
    - dir: /bin/  
      fromSource:  
        - path: /bin/bash  
        recursive: true  
    - dir: /usr/bin/  
      fromSource:  
        - path: /bin/bash  
        recursive: true  
  matchPaths:  
    - fromSource:  
      - path: /usr/bin/mysql_install_db  
      path: /bin/sh  
    - fromSource:  
      - path: /bin/sh  
      path: /usr/bin/my_print_defaults  
    - path: /usr/local/bin/docker-entrypoint.sh  
    - path: /usr/local/bin/gosu  
    - fromSource:  
      - path: /bin/bash  
      - path: /bin/dash  
      path: /usr/sbin/mysqld  
    - path: /usr/bin/mysql  
    - path: /usr/bin/mysqladmin  
    - path: /bin/mktemp  
    - path: /bin/cat  
    - path: /bin/date
```

Process access policy generated based on App Behavior



- **Network access behavior based Policies:** Based on the Network connections that are Ingress and egress connections that are present in pod, the auto discovered system policies are generated. To view that policy user must navigate to the Runtime *Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered policies.

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: autopol-egress-3275896150
  namespace: wordpress-mysql
spec:
  egress:
  - ports:
    - protocol: UDP
    - ports:
      - port: 443
        protocol: TCP
    - ports:
      - port: 3306
        protocol: TCP
    to:
    - podSelector:
        matchLabels:
          app: mysql
  - ports:
    - port: 8081
      protocol: TCP
  - ports:
    - port: 22
      protocol: TCP
  podSelector:
    matchLabels:
      app: wordpress
  policyTypes:
  - Egress
```

Egress policy generated
based on the application
Behavior

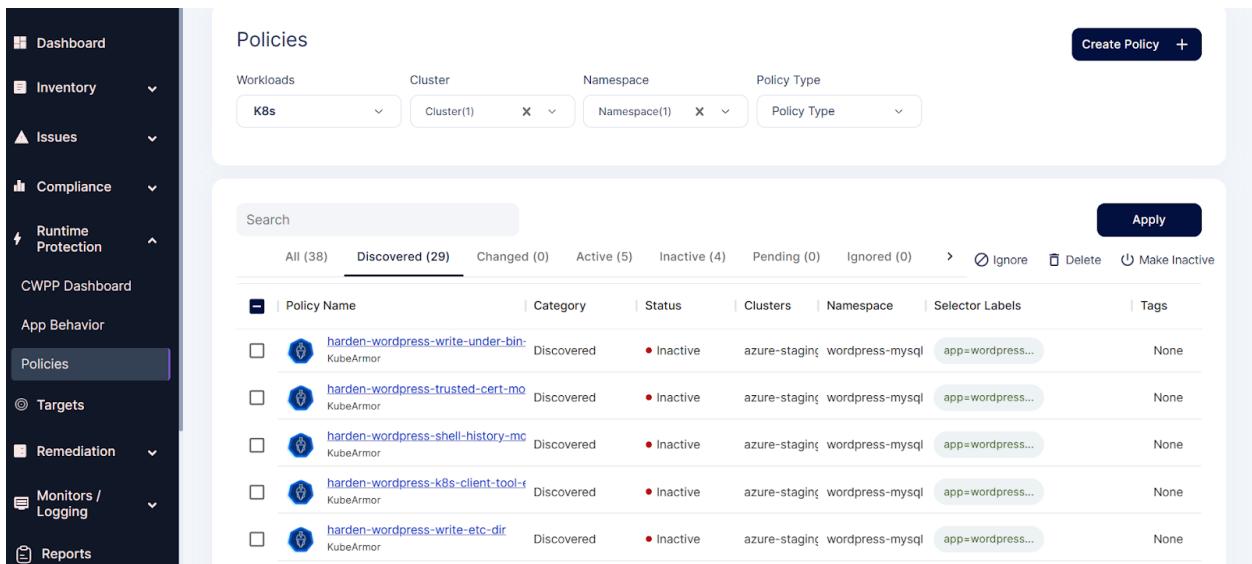


- How to understand Hardening policies

One of the methods to achieve for a zero-trust environment is Application Hardening. KubeArmor is a security solution for the Kubernetes and cloud native platforms that helps protect your workloads from attacks and threats. It does this by providing a set of hardening policies which is a block based policies. It is based on industry-leading technical conformance to standard compliance and attack frameworks such as CIS, MITRE, NIST-800-53, and STIGs. These policies are designed to help you secure your workloads in a way that is compliant with these frameworks and recommended best practices.

- Lets understand by taking an use-case example - **Disallowing any binaries execution to prevent from RCE Vulnerability**

1. Select your cluster and namespace from this Policies screen. We will be getting list of hardening policies for the selected Namespace.



The screenshot shows the KubeArmor UI under the 'Policies' section. The left sidebar includes options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, CWPP Dashboard, App Behavior, Policies (which is selected), Targets, Remediation, Monitors / Logging, and Reports. The main 'Policies' page has a header with 'Create Policy +'. Below it, there are filters for Workloads (K8s), Cluster (Cluster(1)), Namespace (Namespace(1)), and Policy Type. A search bar at the top allows filtering by 'All (38)', 'Discovered (29)', 'Changed (0)', 'Active (5)', 'Inactive (4)', 'Pending (0)', and 'Ignored (0)'. An 'Apply' button is also present. The main table lists six discovered policies, each with a checkbox, icon, name, category, status (Inactive), clusters (azure-staging), namespaces (wordpress-mysql), selector labels (app=wordpress...), and tags (None). The policies listed are: 'harden-wordpress-write-under-bin-' (KubeArmor), 'harden-wordpress-trusted-cert-mo' (KubeArmor), 'harden-wordpress-shell-history-mc' (KubeArmor), 'harden-wordpress-k8s-client-tool-f' (KubeArmor), and 'harden-wordpress-write-etc-dir' (KubeArmor).

2. Selecting the below hardening policy to apply. This policy disallows execution of any of the Package management tools inside the pod. This policy is generated based on the Compliance Frameworks like NIST, NIST 800

harden-wordpress-pkg-mngr-exec

KubeArmorPolicy Updated 17days ago

[YAML](#) [Edit](#) [Clone](#) [Download](#)

① Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```
1  apiVersion: security.kubearmor.com/v1
2  kind: KubeArmorPolicy
3  metadata:
4    name: harden-wordpress-pkg-mngr-exec
5    namespace: wordpress-mysql
6  spec:
7    action: Block
8    message: Alert! Execution of package management process inside
9    process:
10      matchPaths:
11        - path: /usr/bin/apt
12        - path: /usr/bin/apt-get
13        - path: /bin/apt-get
14        - path: /sbin/apk
15        - path: /bin/apt
16        - path: /usr/bin/dpkg
17        - path: /bin/dpkg
18        - path: /usr/bin/gdebi
19        - path: /bin/gdebi
20        - path: /usr/bin/make
21        - path: /bin/make
22        - path: /usr/bin/yum
23        - path: /bin/yum
24        - path: /usr/bin/rpm
25        - path: /bin/rpm
26        - path: /usr/bin/dnf
27        - path: /bin/dnf
28        - path: /usr/bin/pacman
29        - path: /usr/sbin/pacman
30        - path: /bin/pacman
31        - path: /sbin/pacman
32        - path: /usr/bin/makepkg
33        - path: /usr/sbin/makepkg
34        - path: /bin/makepkg
35        - path: /sbin/makepkg
36        - path: /usr/bin/yaourt
37        - path: /usr/sbin/yaourt
38        - path: /bin/yaourt
39        - path: /sbin/yaourt
40        - path: /usr/bin/zypper
41        - path: /bin/zypper
42    selector:
43      matchLabels:
44        app: wordpress
45      severity: 5
46    tags:
47      - NIST
48      - NIST_800-53_CM-7(4)
49      - SI-4
50      - process
51      - NIST_800-53_SI-4
52
```

3. Select this policy and click on the apply option

Search									Apply		
	All (38)	Discovered (29)	Changed (0)	Active (5)	Inactive (4)	Pending (0)	Ignored (0)	Hardening (0)	Ignore	Delete	Make Inactive
	Policy Name		Category	Status	Clusters	Namespace	Selector Labels	Tags			
	<input type="checkbox"/>	harden-wordpress-write-under-bin	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-trusted-cert-mo	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-shell-history-mo	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-k8s-client-tool-i	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-write-etc-dir	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-write-under-dev	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-file-integrity-mo	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-cronjob-cfg	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input checked="" type="checkbox"/>	harden-wordpress-pkg-mngr-exec	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		
	<input type="checkbox"/>	harden-wordpress-remote-file-copy	KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None		

4. After applying policy goes into active state.

The screenshot shows the AccuKnox interface for Runtime Security Policies. The left sidebar includes links for Dashboard, Inventory, Issues, Compliance, Runtime Protection (selected), CWPP Dashboard, App Behavior, Policies (selected), Targets, Remediation, Monitors / Logging, Reports, and Notifications. The main header shows 'Home > Runtime Security > Policies'. A green banner at the top right says 'Policy Change has been approved'. The 'Policies' section has tabs for Workloads (K8s selected), Cluster (Cluster(1)), Namespace (Namespace(1)), and Policy Type. A search bar and an 'Apply' button are above the table. The table lists 38 policies, with columns for Policy Name, Category, Status, Clusters, Namespace, Selector Labels, and Tags. Policies listed include 'harden-wordpress-pkg-mngr-exec', 'audit-mysq(v3)', 'harden-mysql-file-integrity-monitor', 'harden-wordpress-maint-tools-acc', 'mysql-audit-policy.(v1)', and 'ksp-wordpress-block-process.(v2)'. Most policies are active or discovered.

All (38)	Discovered (28)	Changed (0)	Active (6)	Inactive (4)	Pending (0)	Ignored (0)	Hardening (0)	Ignore	Delete	Make Inactive
<input type="checkbox"/> Policy Name										
<input type="checkbox"/> harden-wordpress-pkg-mngr-exec KubeArmor	Discovered	Applied about a sec	● Active		azure-staging	wordpress-mysql	app=wordpress...			None
<input type="checkbox"/> audit-mysq(v3) KubeArmor	Custom	Applied 7days ago	● Active		azure-staging	wordpress-mysql	app=mysql...			None
<input type="checkbox"/> harden-mysql-file-integrity-monitor KubeArmor	Discovered		● Inactive		azure-staging	wordpress-mysql	app=mysql...			None
<input type="checkbox"/> harden-wordpress-maint-tools-acc KubeArmor	Discovered		● Inactive		azure-staging	wordpress-mysql	app=wordpress...			None
<input type="checkbox"/> mysql-audit-policy.(v1) KubeArmor	Custom		● Inactive		azure-staging	wordpress-mysql	app=mysql...			None
<input type="checkbox"/> ksp-wordpress-block-process.(v2) KubeArmor	Custom	Applied 10days ago	● Active		azure-staging	wordpress-mysql	app=wordpress...			None

5. After applying this policy the attacker might not able to install any of the packages for performing Remote code execution attack.

- How to Audit application and get alerts for that
 - AccuKnox Runtime Security Engine kubeArmor can be used for auditing the application with help of audit based security policies. Let us consider the following policy

 **ksp-mysql-audit-dir (v3)** 

KubeArmorPolicy
Created a month ago.

 The YAML is valid

[YAML](#)  [Edit](#)  [Clone](#)  [Download](#)

```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: ksp-mysql-audit-dir
5   namespace: wordpress-mysql
6 spec:
7   severity: 5
8   selector:
9     matchLabels:
10    app: mysql
11   file:
12     matchDirectories:
13       - dir: /var/lib/mysql/
14         recursive: true
15   action: Audit
16   message: mysql-audit-policy
```

- This policy helps to audit the access to /var/lib/mysql/ folder. If any modification or any contents of this folder is read user will be intimated with alerts.
- Applying the Audit base policy from SaaS

Home > Runtime Security > Policies partnerdemo

Policies

K8s ▾ aks-demo-prod × X ▾ wordpress-mysql × X ▾ Policy Type Active × X ▾

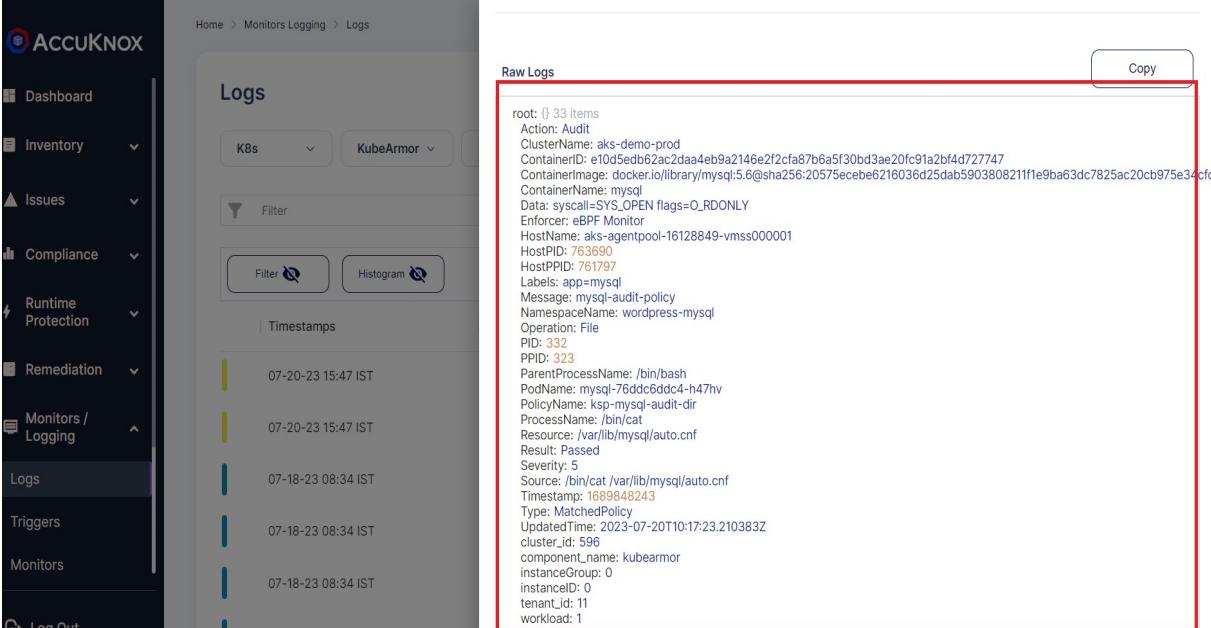
Search Audit based policy is applied from AccuKnox SaaS

All (1)	Discovered (0)	Hardening (0)	Custom (1)	Ignore	Delete
Policy Name	Category	Status	Clusters	Namespace	Selector Labels
ksp-mysql-audit-dir (v3) KubeArmor	Custom	Applied a few secos • Active	aks-demo-prod	wordpress-mysql	None

- Now if we try to read the contents of this /var/lib/mysql folder running in a mysql pod by exec into the pod.

```
~$ kubectl exec -it -n wordpress-mysql mysql-76ddc6ddc4-h47hv -- bash
root@mysql-76ddc6ddc4-h47hv:/# cd /var/lib/mysql
root@mysql-76ddc6ddc4-h47hv:/var/lib/mysql# ls
auto.cnf  ib_logfile0  ib_logfile1  ibdata1  mysql  performance_schema
test  wordpress
root@mysql-76ddc6ddc4-h47hv:/var/lib/mysql# cat auto.cnf
[auto]
server-uuid=7ad615d7-0108-11ee-8442-a6440d433e17|
```

- We can see the Audit based alert in the Monitoring/Logging Section from AccuKnox SaaS as below



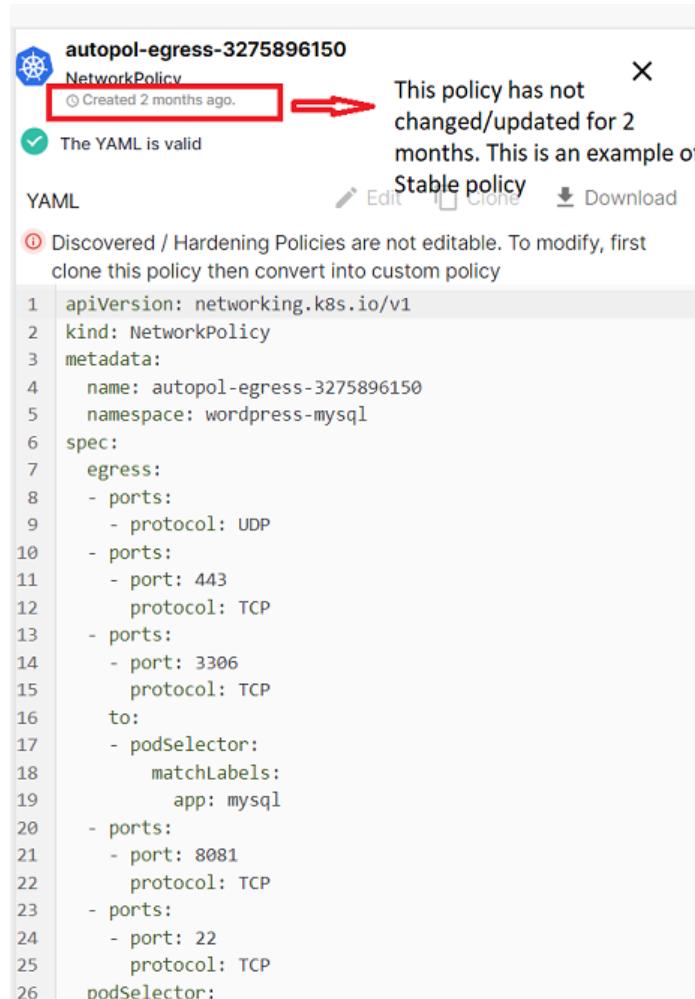
The screenshot shows the AccuKnox SaaS dashboard with the 'Logs' section selected. The 'Raw Logs' panel displays an audit log entry with the following details:

```

root: 33 items
Action: Audit
ClusterName: aks-demo-prod
ContainerID: e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747
ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab590380821ff1e9ba63dc7825ac20cb975e3...cfc
ContainerName: mysql
Data: syscall=SYS_OPEN flags=O_RDONLY
Enforcer: eBPF Monitor
HostName: aks-agentpool-16128849-vmss000001
HostPID: 763690
HostPPID: 761797
Labels: app=mysql
Message: mysql-audit-policy
NamespaceName: wordpress-mysql
Operation: File
PID: 332
PPID: 333
ParentProcessName: /bin/bash
PodName: mysql-76ddc6ddc4-h47hv
PolicyName: ksp-mysql-audit-dir
ProcessName: /bin/cat
Resource: /var/lib/mysql/auto.cnf
Result: Passed
Severity: 5
Source: /bin/cat /var/lib/mysql/auto.cnf
Timestamp: 1689848243
Type: MatchedPolicy
UpdatedTime: 2023-07-20T10:17:23.210383Z
cluster_id: 596
component_name: kubearmor
instance_group: 0
instance_id: 0
tenant_id: 11
workload: 1

```

- When do we say policies are stable?
 - AccuKnox Runtime Security Engine KubeArmor will discover the policies based on the Application Behavior. If the Application behavior changes the Policies generated will also be updated.
 - When the policy created date or updated date doesn't change for some days then we can say that the policy which was discovered is stable. For example consider the following policy



autopol-egress-3275896150
NetworkPolicy
Created 2 months ago.
The YAML is valid

This policy has not changed/updated for 2 months. This is an example of Stable policy

YAML Edit Clone Download

```

1 apiVersion: networking.k8s.io/v1
2 kind: NetworkPolicy
3 metadata:
4   name: autopol-egress-3275896150
5   namespace: wordpress-mysql
6 spec:
7   egress:
8     - ports:
9       - protocol: UDP
10      - ports:
11        - port: 443
12          protocol: TCP
13        - ports:
14          - port: 3306
15            protocol: TCP
16          to:
17            - podSelector:
18              matchLabels:
19                app: mysql
20            - ports:
21              - port: 8081
22                protocol: TCP
23            - ports:
24              - port: 22
25                protocol: TCP
26    podSelector:

```

- The above auto discovered policy has not changed for more than a month. This policy can be called a stable policy as it didn't get any updates or changes.

- What if something changes in Application??
- AccuKnox Runtime Security Engine KubeArmor will discover the policies based on the Application Behavior. If the Application behavior changes the Policies generated will also be updated.
- For example consider the following auto discovered policy

autopol-system-1804736057 (v1)

Discovered (Changes Available 2months ago)
Created 2 months ago.

Update X

Updated YAML

```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: autopol-system-1804736057
5   namespace: dvwa
6 spec:
7   action: Allow
8   file:
9     matchDirectories:
10    - dir: /tmp/
11      fromSource:
12        - path: /usr/sbin/apache2
13        recursive: true
14    - dir: /var/www/html/
15      fromSource:
16        - path: /usr/sbin/apache2
17        recursive: true
18    - dir: /lib/x86_64-linux-gnu/
19      recursive: true
20    - dir: /etc/
21      fromSource:
22        - path: /bin/bash
23        - path: /bin/ping
24        recursive: true
25    - dir: /etc/
26      fromSource:
27        - path: /bin/bash
.. .. ..
```

- In the above policy there are some changes that are detected after the initial policy discovery due to changes in application behavior. Those changes are highlighted.

```
58     path: /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0
59   - fromSource:
60     - path: /usr/sbin/apache2
61     path: /usr/lib/x86_64-linux-gnu/libuuid.so.1
62 +   - fromSource:
63 +     - path: /bin/bash
64 +     path: /root/.bash_history
65 +   - fromSource:
66 +     - path: /bin/bash
67 +     path: /dev/pts/0
68 +   - fromSource:
69 +     - path: /bin/ls
70 +     path: /etc/ld.so.cache
71 +   - fromSource:
72 +     - path: /bin/ls
73 +     path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0
74 process:
75   matchPaths:
76     - path: /usr/sbin/apache2
77     - path: /bin/bash
78     - fromSource:
79       - path: /bin/bash
80       path: /bin/ping
81     - fromSource:
82       - path: /bin/bash
83       path: /usr/sbin/apache2
84     - path: /bin/ping
85   recursive: true
```

- If the user is satisfied with the changes they can accept the change by clicking on the update button

 **autopol-system-1804736057 (v1)**

Discovered (Changes Available 2months ago)
Created 2 months ago.

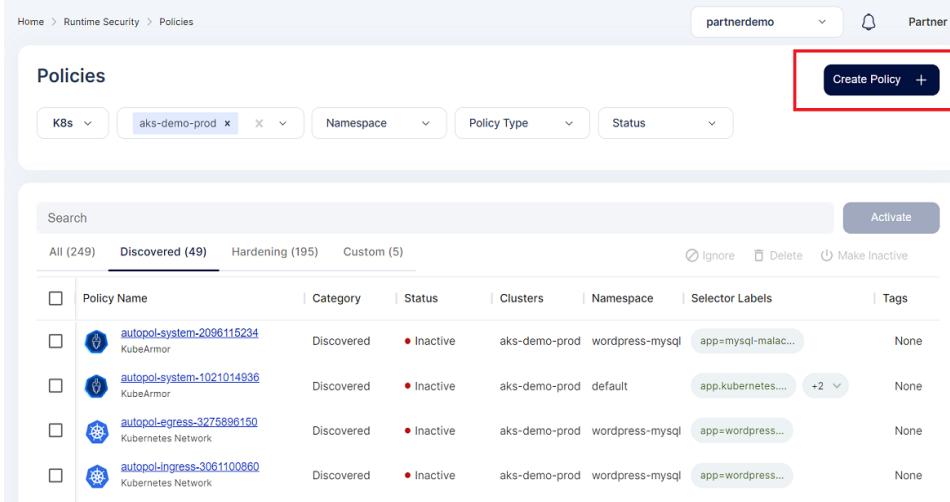
Update 

Updated YAML

```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: autopol-system-1804736057
5   namespace: dwva
6 spec:
7   action: Allow
8   file:
9     matchDirectories:
10    - dir: /tmp/
11      fromSource:
12        - path: /usr/sbin/apache2
13      recursive: true
14    - dir: /var/www/html/
15      fromSource:
16        - path: /usr/sbin/apache2
17      recursive: true
18    - dir: /lib/x86_64-linux-gnu/
19      recursive: true
20    - dir: /etc/
21      fromSource:
22        - path: /bin/bash
23        - path: /bin/ping
24      recursive: true
25    - dir: /etc/
26      fromSource:
27        - path: /bin/bash
... . . .
```

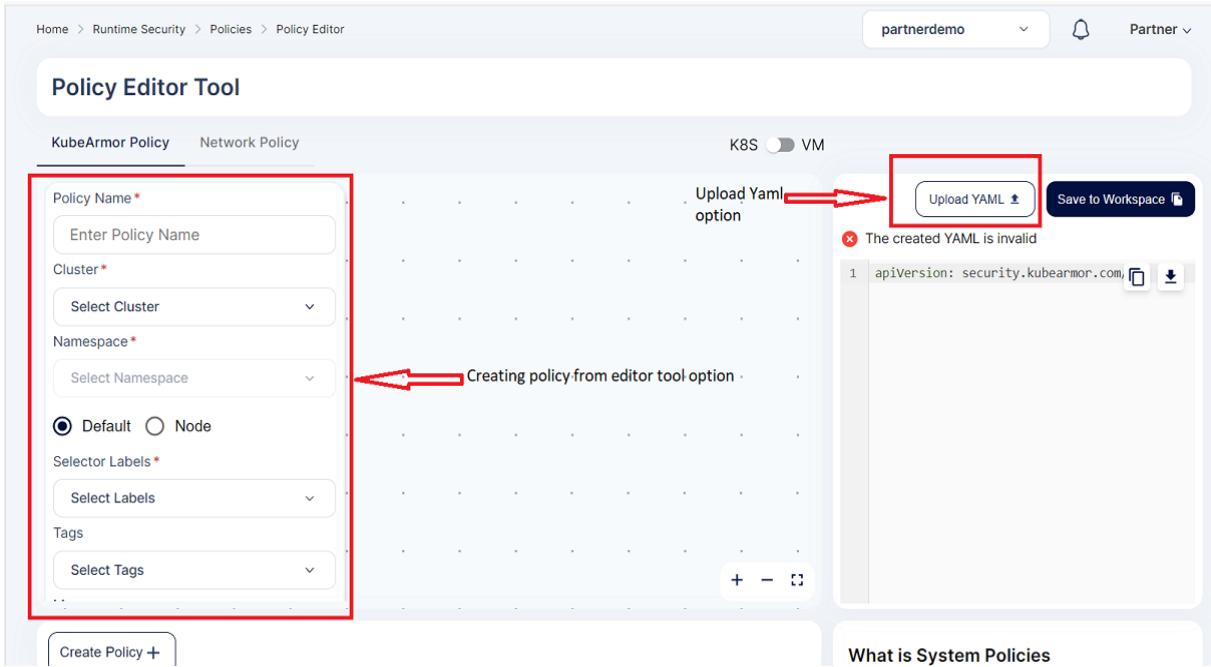
- After the user clicks the update the policy will be updated.

- How to create a custom Policy
 - File restriction Policy
 - To create a file restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
 - To create the policy user needs to click on the create policy option



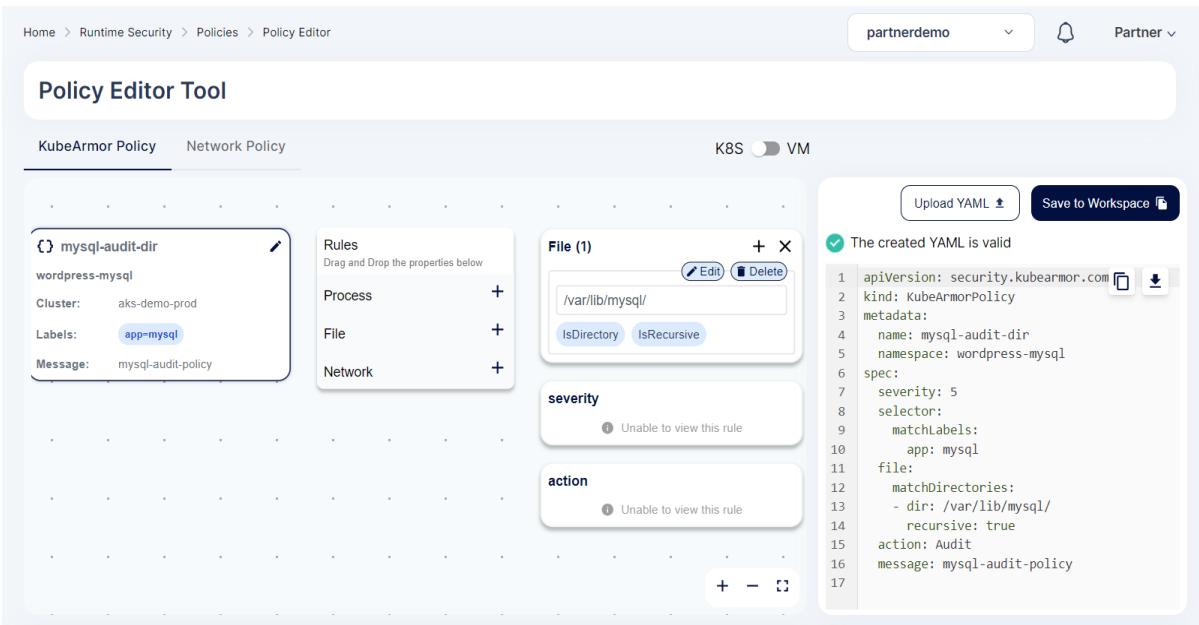
The screenshot shows the 'Policies' section of the AccuKnox interface. At the top right, there is a 'Create Policy' button with a plus sign, which is highlighted with a red box. Below the header, there are several filter options: 'K8s' dropdown, 'aks-demo-prod' selected in a 'Cluster' dropdown, 'Namespace' dropdown, 'Policy Type' dropdown, and 'Status' dropdown. A search bar and an 'Activate' button are also present. The main table lists policies under the 'Discovered' tab, showing columns for Policy Name, Category, Status, Clusters, Namespace, Selector Labels, and Tags. Four policies are listed as 'Discovered' and 'Inactive': 'autopol-system-2096115234' (KubeArmor), 'autopol-system-1021014936' (KubeArmor), 'autopol-egress-3275896150' (Kubernetes Network), and 'autopol-ingress-3061100860' (Kubernetes Network).

- Now user has two options either to upload the yaml file or to create the policy from policy editor tool



The screenshot shows the 'Policy Editor Tool' section of the AccuKnox interface. On the left, there is a form for creating a 'KubeArmor Policy' with fields for 'Policy Name*', 'Cluster*', 'Namespace*', 'Selector Labels*', and 'Tags'. Below the form is a 'Create Policy +' button. On the right, there is a 'VM' tab, an 'Upload YAML' button with a red box around it, and a message stating 'The created YAML is invalid'. A code editor window shows a single line of YAML: 'apiVersion: security.kubearmory.com'. At the bottom, there is a 'Save to Workspace' button and a 'What is System Policies' link.

- Now upload the file access policy yaml from your system. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.

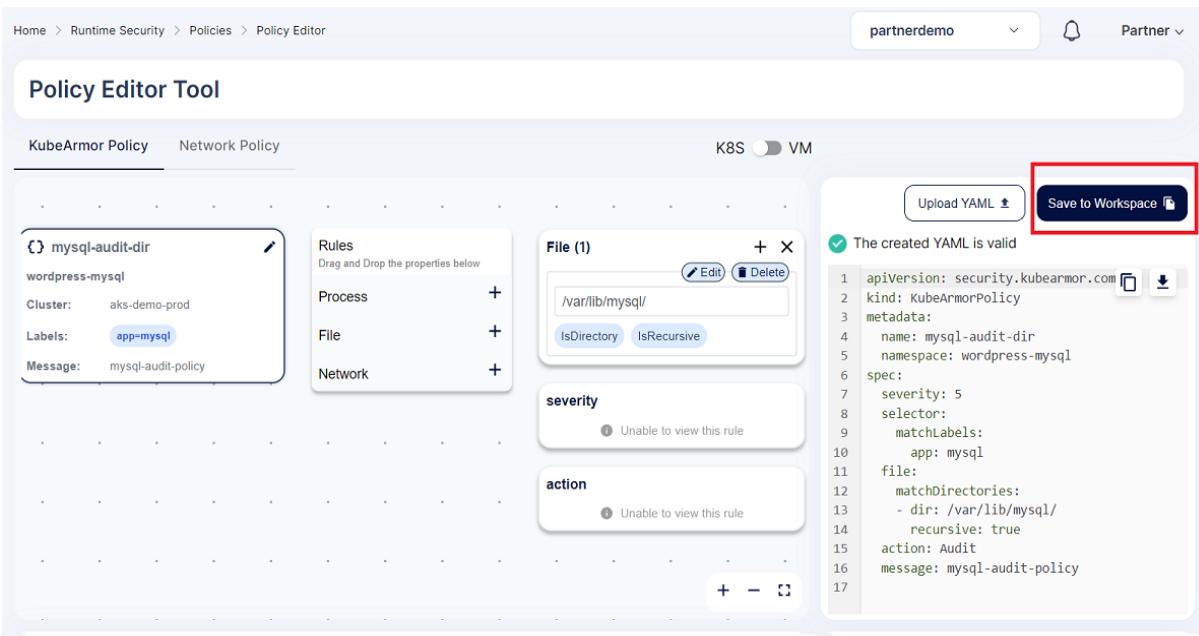


```

apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: mysql-audit-dir
  namespace: wordpress-mysql
spec:
  severity: 5
  selector:
    matchLabels:
      app: mysql
  file:
    matchDirectories:
      - dir: /var/lib/mysql/
        recursive: true
  action: Audit
  message: mysql-audit-policy

```

- Now to save the policy user needs to click the **save to workspace** option

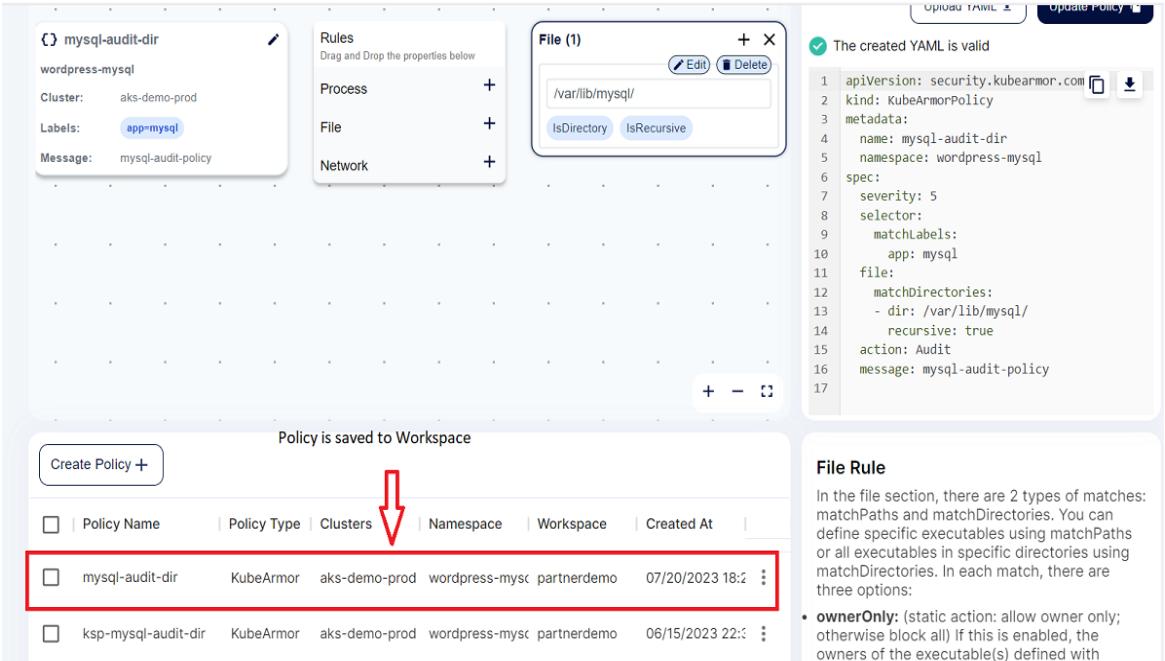


```

apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: mysql-audit-dir
  namespace: wordpress-mysql
spec:
  severity: 5
  selector:
    matchLabels:
      app: mysql
  file:
    matchDirectories:
      - dir: /var/lib/mysql/
        recursive: true
  action: Audit
  message: mysql-audit-policy

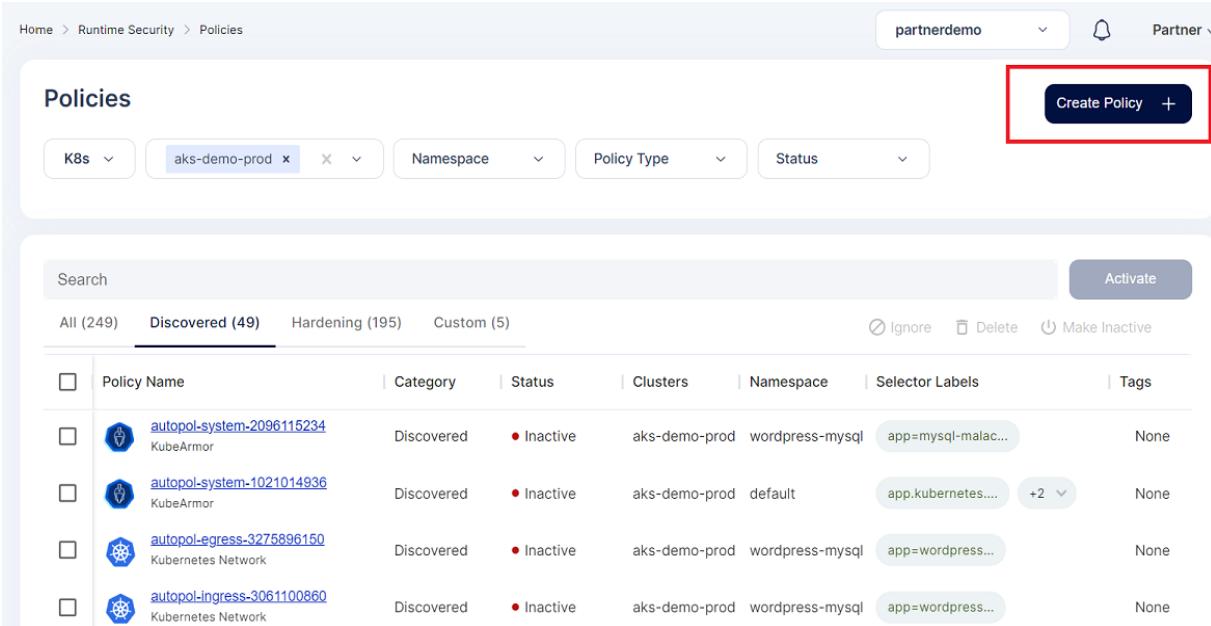
```

- After that policy will be saved to the workspace.



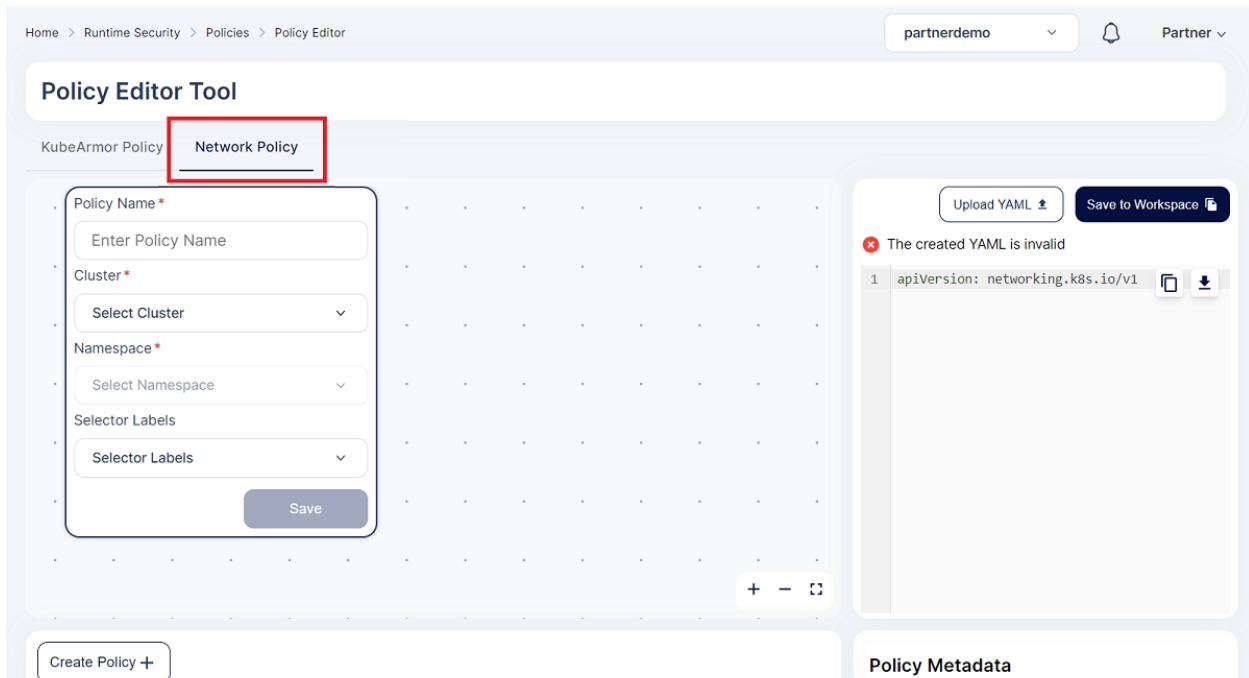
The screenshot shows the ACCUKNOKX platform's policy creation interface. On the left, a policy named "mysql-audit-dir" is being configured for the "wordpress-mysql" namespace in the "aks-demo-prod" cluster. It has a single rule under "File" that matches the directory "/var/lib/mysql/" and is recursive. The YAML code for this policy is displayed on the right, showing a KubeArmorPolicy with a file rule. A success message indicates the policy is valid. Below the editor, a confirmation message says "Policy is saved to Workspace". The workspace list at the bottom shows two policies: "mysql-audit-dir" (created 07/20/2023) and "ksp-mysql-audit-dir" (created 06/15/2023). A red arrow points from the "Clusters" header in the workspace list towards the policy creation area.

- Network access Policy
 - To create a Network access policy restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
 - To create the policy user needs to click on the create policy option



The screenshot shows the ACCUKNOKX Policies page. At the top, there are filters for "K8s" (set to "aks-demo-prod"), "Namespace" (set to "default"), "Policy Type" (dropdown), and "Status" (dropdown). A prominent red box highlights the "Create Policy +" button. Below the filters, there is a search bar and an "Activate" button. The main table lists 49 discovered policies. The columns include "Policy Name", "Category", "Status", "Clusters", "Namespace", "Selector Labels", and "Tags". Some policies listed are "autopol-system-2096115234", "autopol-system-1021014936", "autopol-egress-3275896150", and "autopol-ingress-3061100860". The status for most policies is "Inactive".

- In this screen for Network Policy creation user needs to select the Network policy editor tool

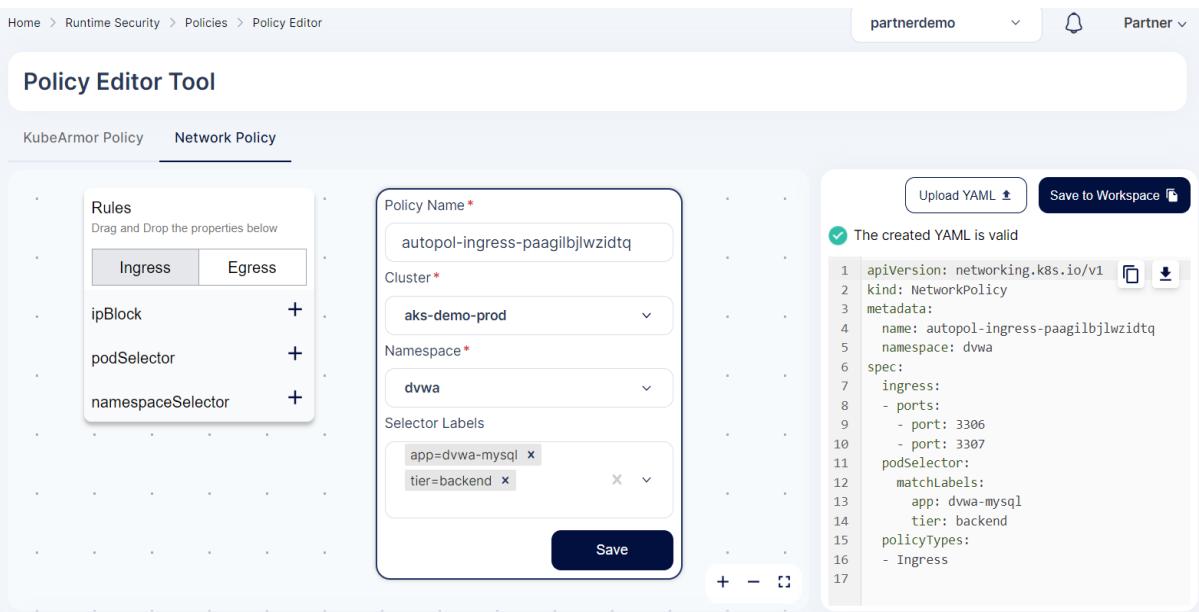


The screenshot shows the 'Policy Editor Tool' interface. At the top, there are tabs for 'KubeArmor Policy' and 'Network Policy', with 'Network Policy' being the active tab and highlighted with a red box. Below the tabs, there is a form for creating a new policy:

- Policy Name ***: Enter Policy Name
- Cluster ***: Select Cluster
- Namespace ***: Select Namespace
- Selector Labels**: Selector Labels

At the bottom of the form is a 'Save' button. To the right of the form, there is a large grid area for viewing or managing policies. On the far right, there are buttons for 'Upload YAML' and 'Save to Workspace'. A message box indicates that the created YAML is invalid.

- Now upload the Network policy yaml from your system by clicking the *upload yaml* option. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.



The screenshot shows the 'Policy Editor Tool' interface with the 'Network Policy' tab selected. On the left, there is a 'Rules' section with 'Ingress' and 'Egress' buttons, and a list of items: 'ipBlock', 'podSelector', and 'namespaceSelector'. In the center, there is a form for creating a policy:

- Policy Name ***: autopol-ingress-paagilbjlwzidtq
- Cluster ***: aks-demo-prod
- Namespace ***: dwva
- Selector Labels**: app=dvwa-mysql tier=backend

At the bottom of the form is a 'Save' button. To the right, there is a code editor showing the uploaded YAML, which is now valid. The message box indicates that the created YAML is valid.

- Now to save the policy user needs to click the *save to workspace* option

Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy

Rules
Drag and Drop the properties below

Ingress Egress

ipBlock +
podSelector +
namespaceSelector +

Policy Name*: autopol-ingress-paagilbjlwzidtq
Cluster*: aks-demo-prod
Namespace*: dvwa
Selector Labels: app=dvwa-mysql tier=backend

Save

Upload YAML **Save to Workspace**

The created YAML is valid

```

1 apiVersion: networking.k8s.io/v1
2 kind: NetworkPolicy
3 metadata:
4   name: autopol-ingress-paagilbjlwzidtq
5   namespace: dvwa
6 spec:
7   ingress:
8     - ports:
9       - port: 3306
10      - port: 3307
11   podSelector:
12     matchLabels:
13       app: dvwa-mysql
14       tier: backend
15   policyTypes:
16     - Ingress
17

```

After that policy will be saved to the workspace.

Rules
Drag and Drop the properties below

Ingress Egress

ipBlock +
podSelector +
namespaceSelector +

autopol-ingress-paagilbjlwzidtq

NetworkPolicy

Cluster: aks-demo-prod
Namespace: dvwa
Labels: app=dvwa-mysql tier=backend

Upload YAML **Update Policy**

The created YAML is valid

```

1 apiVersion: networking.k8s.io/v1
2 kind: NetworkPolicy
3 metadata:
4   name: autopol-ingress-paagilbjlwzidtq
5   namespace: dvwa
6 spec:
7   ingress:
8     - ports:
9       - port: 3306
10      - port: 3307
11   podSelector:
12     matchLabels:
13       app: dvwa-mysql
14       tier: backend
15   policyTypes:
16     - Ingress
17

```

Policy is saved to Workspace

Create Policy +

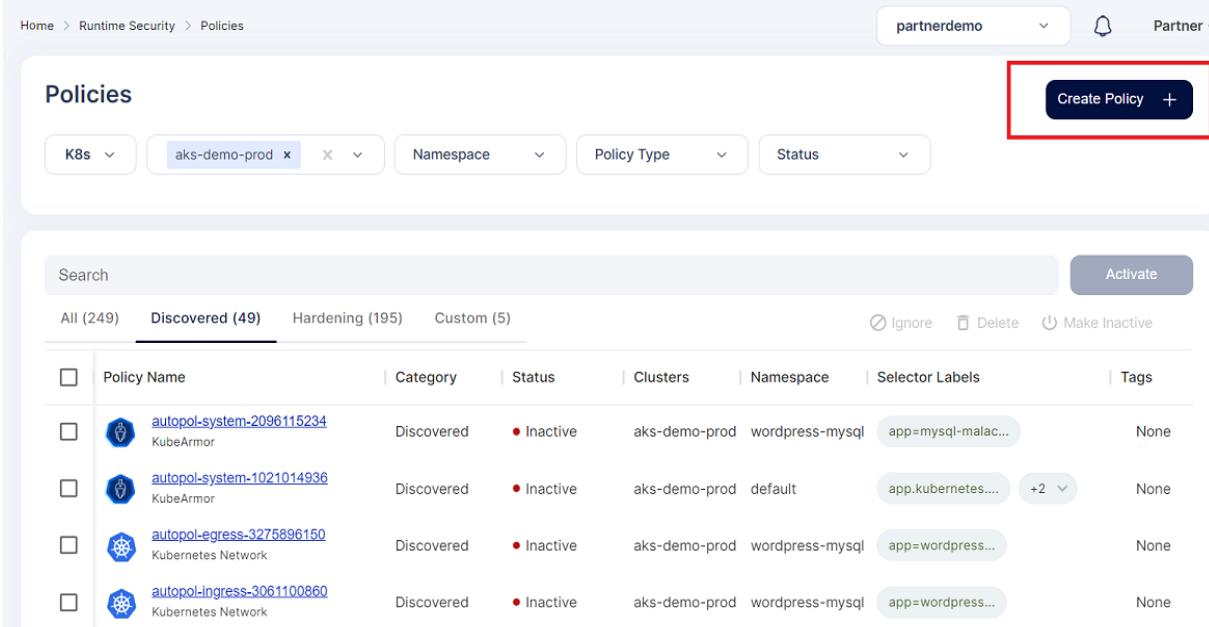
<input type="checkbox"/> Policy Name	Policy Type	Clusters	Namespace	Workspace	Created At
<input type="checkbox"/> autopol-ingress-p...	NetworkPolicy	aks-demo-prod	dvwa	partnerdemo	07/20/2023 19:2

Policy Metadata

Mandatory Fields: As with all other Kubernetes config, a NetworkPolicy needs apiVersion, kind, and metadata fields.

PodSelector: Each NetworkPolicy includes a podSelector which selects the grouping of pods to which the policy applies. The example policy selects pods with the label "role=db". An empty podSelector selects all pods in the namespace.

- Process block restriction Policy
 - To create a Process access restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
 - To create the policy user needs to click on the create policy option



Policies

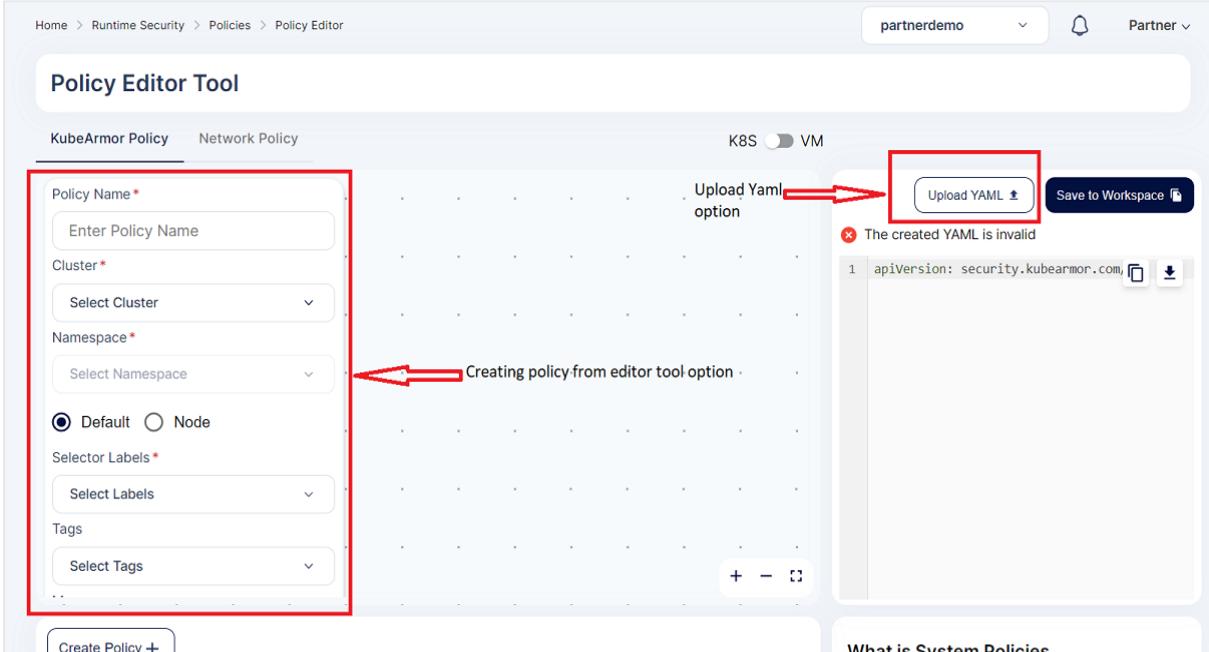
K8s Namespace Status

Search

All (249) **Discovered (49)** Hardening (195) Custom (5)

<input type="checkbox"/>	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
<input type="checkbox"/>	autopol-system-2096115234 KubeArmor	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=mysql-malac...	None
<input type="checkbox"/>	autopol-system-1021014936 KubeArmor	Discovered	● Inactive	aks-demo-prod	default	app.kubernetes....	+2
<input type="checkbox"/>	autopol-egress-3275896150 Kubernetes Network	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	None
<input type="checkbox"/>	autopol-ingress-3061100860 Kubernetes Network	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	None

- Now user has two options either to upload the yaml file or to create the policy from policy editor tool



Home > Runtime Security > Policies > Policy Editor

Policy Editor Tool

KubeArmor Policy Network Policy K8S VM

Enter Policy Name
 Cluster
 Namespace
 Default Node
 Selector Labels
 Tags

Upload YAML option Save to Workspace

The created YAML is invalid

```
apiVersion: security.kubearmor.com
```

Creating policy from editor tool option

Create Policy + What is System Policies

- Now upload the process block policy yaml from your system. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.

Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy K8S VM

wordpress-block-process
 wordpress-mysql
 Cluster: aks-demo-prod
 Labels: app=wordpress
 Message: apt process block

Rules
 Drag and Drop the properties below

Process (2)

- + /usr/bin/apt
- + /usr/bin/apt-get

severity
Unable to view this rule

action
Unable to view this rule

Upload YAML
Save to Workspace

The created YAML is valid

```

1 apiVersion: security.kubearmor.com
2 kind: KubeArmorPolicy
3 metadata:
4   name: wordpress-block-process
5   namespace: wordpress-mysql
6 spec:
7   severity: 3
8   selector:
9     matchLabels:
10       app: wordpress
11   process:
12     matchPaths:
13       - path: /usr/bin/apt
14       - path: /usr/bin/apt-get
15     action: Block
16     message: 'apt process block '
17

```

■ Now to save the policy user needs to click the save to workspace option

Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy K8S VM

wordpress-block-process
 wordpress-mysql
 Cluster: aks-demo-prod
 Labels: app=wordpress
 Message: apt process block

Rules
 Drag and Drop the properties below

Process (2)

- + /usr/bin/apt
- + /usr/bin/apt-get

severity
Unable to view this rule

action
Unable to view this rule

Upload YAML
Save to Workspace

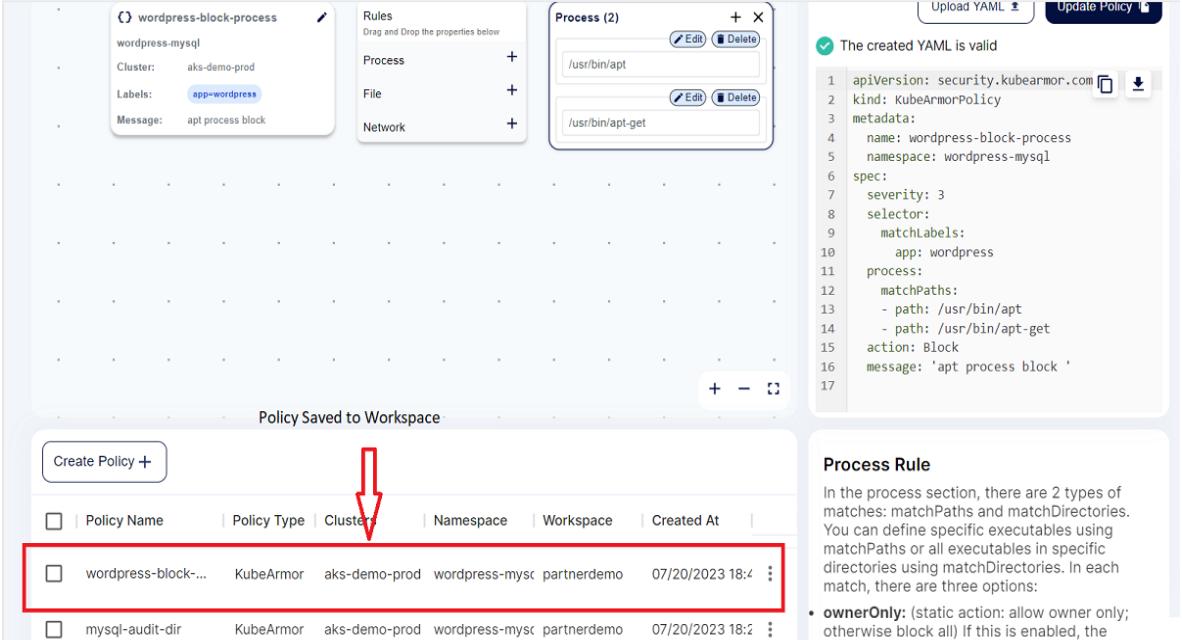
The created YAML is valid

```

1 apiVersion: security.kubearmor.com
2 kind: KubeArmorPolicy
3 metadata:
4   name: wordpress-block-process
5   namespace: wordpress-mysql
6 spec:
7   severity: 3
8   selector:
9     matchLabels:
10       app: wordpress
11   process:
12     matchPaths:
13       - path: /usr/bin/apt
14       - path: /usr/bin/apt-get
15     action: Block
16     message: 'apt process block '
17

```

■ After that policy will be saved to the workspace.



The screenshot shows the AccuKnox interface for creating and managing security policies. At the top, a policy named "wordpress-block-process" is being edited. It includes a "Cluster" (aks-demo-prod), "Labels" (app=wordpress), and a "Message" (apt process block). The "Rules" section allows dragging and dropping properties, with a "Process" rule currently defined. This rule has two entries: "/usr/bin/apt" and "/usr/bin/apt-get", both set to "Edit" mode. To the right, the "YAML" view shows the generated configuration file:

```

1 apiVersion: security.kubearmor.com
2 kind: KubeArmorPolicy
3 metadata:
4   name: wordpress-block-process
5   namespace: wordpress-mysql
6 spec:
7   severity: 3
8   selector:
9     matchLabels:
10    app: wordpress
11   process:
12     matchPaths:
13       - path: /usr/bin/apt
14       - path: /usr/bin/apt-get
15   action: Block
16   message: 'apt process block'
17

```

A green checkmark indicates the YAML is valid. Below this, a message says "Policy Saved to Workspace". In the bottom left, a table lists existing policies: "wordpress-block..." (selected, highlighted with a red box and a red arrow pointing to it) and "mysql-audit-dir". The table columns include Policy Name, Policy Type, Cluster, Namespace, Workspace, and Created At.

- How to enforce Policies and see anomalies

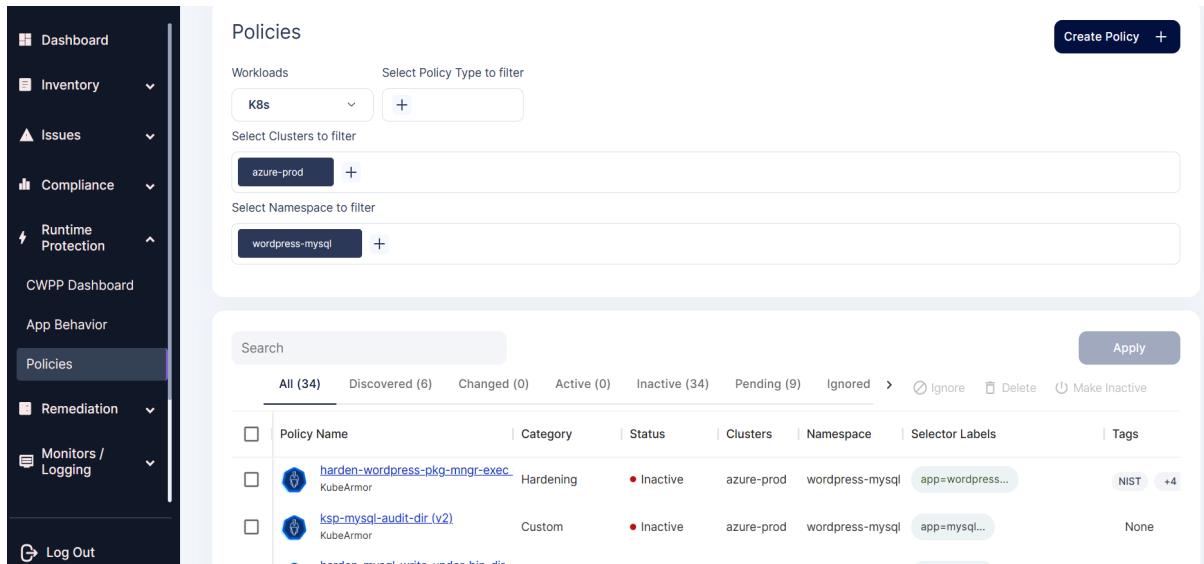
- We can apply any of the Auto Discovered, Hardening or custom policies and see the anomalies getting detected using the Monitoring and Logging section.
- Let us consider the WordPress- MySQL application. In the MySQL application, certain folders will be having certain critical data which can be allowed to access but not modified. So using our AccuKnox hardening policy we are going to prevent the modification of contents inside these critical folders.
- **Before applying the policy:** Currently, any attacker who gets access to the bash or shell of the MySQL pod can modify the contents of the sbin folder by creating a new file and editing the old files.

```

root@mysql-6c6fdcccf-sk5x2:/# cd sbin
root@mysql-6c6fdcccf-sk5x2:/sbin# ls
agetty      dumpe2fs    fsck.ext2    installkernel  mkfs.cramfs      pivot_root      swapoff
badblocks   e2fsck     fsck.ext3    isosize       mkfs.ext2       raw           swapon
blkdiscard  e2image    fsck.ext4    killall5     mkfs.ext3       resize2fs     switch_root
blkid       e2label    fsck.minix  ldconfig     mkfs.ext4       runuser      tune2fs
blockdev    e2undo    fsfreeze    logsave     mkfs.minix     sfdisk       unix_chkpwd
cfdisk      fdisk     fstab-decode losetup     mkhomedir_helper shadowconfig start-stop-daemon wipefs
chcpu       findfs    fstrim     mke2fs      mkswap        pam_tally    slogin
ctrlaltdel  fsck     getty      mkfs       pam_tally2    swaplabel
debugfs     fsck.cramfs hwclock   mks2       pam_tally2
root@mysql-6c6fdcccf-sk5x2:/sbin# touch mks2
root@mysql-6c6fdcccf-sk5x2:/sbin# ls
agetty      dumpe2fs    fsck.ext2    installkernel  mkfs.cramfs      pam_tally2    swaplabel
badblocks   e2fsck     fsck.ext3    isosize       mkfs.ext2       pivot_root  swapoff
blkdiscard  e2image    fsck.ext4    killall5     mkfs.ext3       raw          swapon
blkid       e2label    fsck.minix  ldconfig     mkfs.ext4       resize2fs   switch_root
blockdev    e2undo    fsfreeze    logsave     mkfs.minix     runuser      tune2fs
cfdisk      fdisk     fstab-decode losetup     mkhomedir_helper sfdisk       unix_chkpwd
chcpu       findfs    fstrim     mke2fs      mks2         shadowconfig unix_update
ctrlaltdel  fsck     getty      mkfs       mkswap        start-stop-daemon wipefs
debugfs     fsck.cramfs hwclock   mks2       pam_tally2    slogin
root@mysql-6c6fdcccf-sk5x2:/sbin#

```

- Now we are going to prevent this using AccuKnox CWPP Solution.
- Step 1:** Navigate to the Runtime Protection-> Policies and select the cluster and namespace where the WordPress-MySQL application is deployed.



All (34)	Discovered (6)	Changed (0)	Active (0)	Inactive (34)	Pending (9)	Ignored	Ignore	Delete	Make Inactive
<input type="checkbox"/> harden-wordpress-pkg-mngr-exec	KubeArmor	Hardening	● Inactive	azure-prod	wordpress-mysql	app=wordpress...	NIST	+4	
<input type="checkbox"/> ksp-mysql-audit-dir (v2)	KubeArmor	Custom	● Inactive	azure-prod	wordpress-mysql	app=mysql...			None
<input type="checkbox"/> harden-mysql-write-under-bin-dir									

- **Step 2:** In the screen select the hardening policies in the policy filter section to view the hardening policies related to the WordPress-MySQL application.

Search Activate

All (43)	Discovered (3)	Hardening (39)	Custom (1)	<input type="button" value="Ignore"/>	<input type="button" value="Delete"/>	<input type="button" value="Make Inactive"/>		
		Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
<input type="checkbox"/>	 harden-wordpress-shell-history-mod	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	NIST 
<input type="checkbox"/>	 harden-wordpress-write-etc-dir	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	NIST_800-53 
<input type="checkbox"/>	 harden-wordpress-remote-file-copy	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	MITRE 
<input type="checkbox"/>	 harden-wordpress-write-under-bin-dir	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	NIST 
<input type="checkbox"/>	 harden-wordpress-pkg-mngr-exec (v5)	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	NIST 
<input type="checkbox"/>	 harden-wordpress-file-integrity-monito	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	NIST 
<input type="checkbox"/>	 harden-mysql-file-integrity-monitoring	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=mysql...</code>	NIST 
<input type="checkbox"/>	 harden-mysql-pkg-mngr-exec	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=mysql...</code>	NIST 
<input type="checkbox"/>	 harden-wordpress-trusted-cert-mod	KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	<code>app=wordpress...</code>	MITRE 

- **Step 3:** Click on the MySQL file integrity hardening policy from the list of policies to see the policy

 **harden-mysql-file-integrity-monitoring** X

KubeArmorPolicy
Created 5 days ago.

[YAML](#) [!\[\]\(3c8b6b75891fac713b16780e99ebae58_img.jpg\) Edit](#) [!\[\]\(0e61ef0f65bebe25b92287cebf61df98_img.jpg\) Clone](#) [!\[\]\(6fe491ad38beb7b637a29209c8fffbee_img.jpg\) Download](#)

ⓘ Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

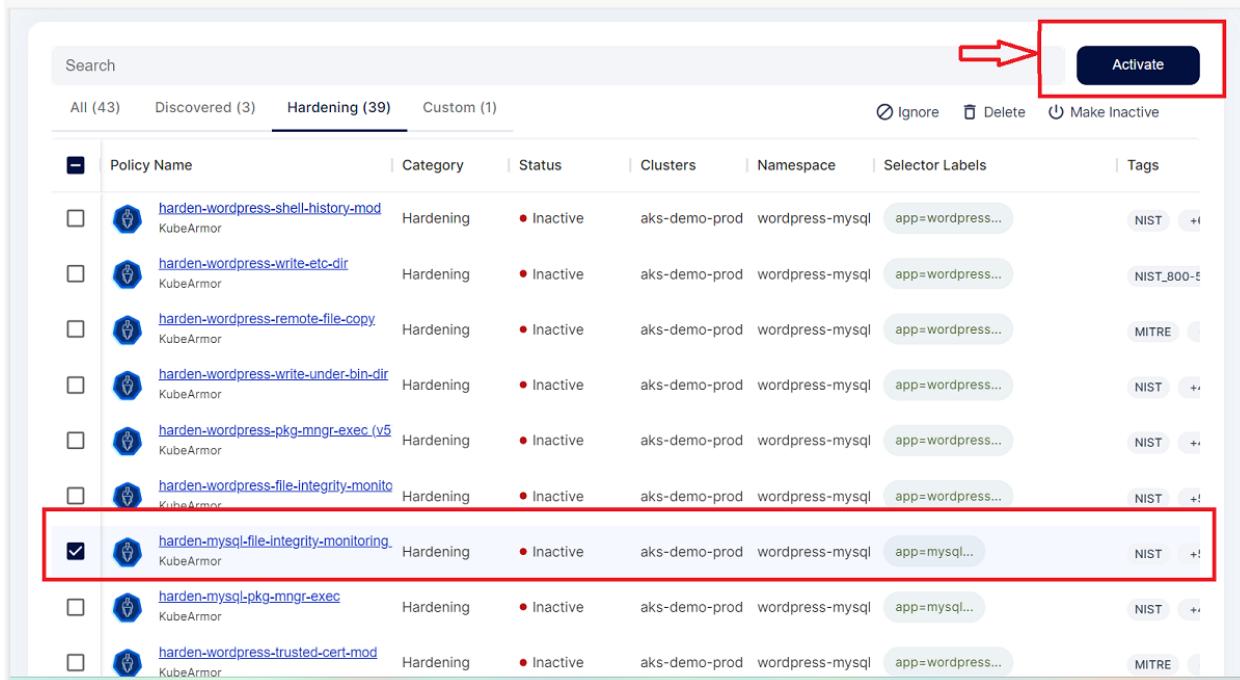
```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: harden-mysql-file-integrity-monitoring
5   namespace: wordpress-mysql
6 spec:
7   action: Block
8   file:
9     matchDirectories:
10    - dir: /sbin/
11      readOnly: true
12      recursive: true
13    - dir: /usr/bin/
14      readOnly: true
15      recursive: true
16    - dir: /usr/lib/
17      readOnly: true
18      recursive: true
19    - dir: /usr/sbin/
20      readOnly: true
21      recursive: true
22    - dir: /bin/
23      readOnly: true
24      recursive: true
25    - dir: /boot/
26      readOnly: true
27      recursive: true
28   message: Detected and prevented compromise to File integrity
29   selector:
30     matchLabels:
```

- The policy is allowing users to access the critical folders but it is blocking the write or modify access by whitelisting only read access.

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
```

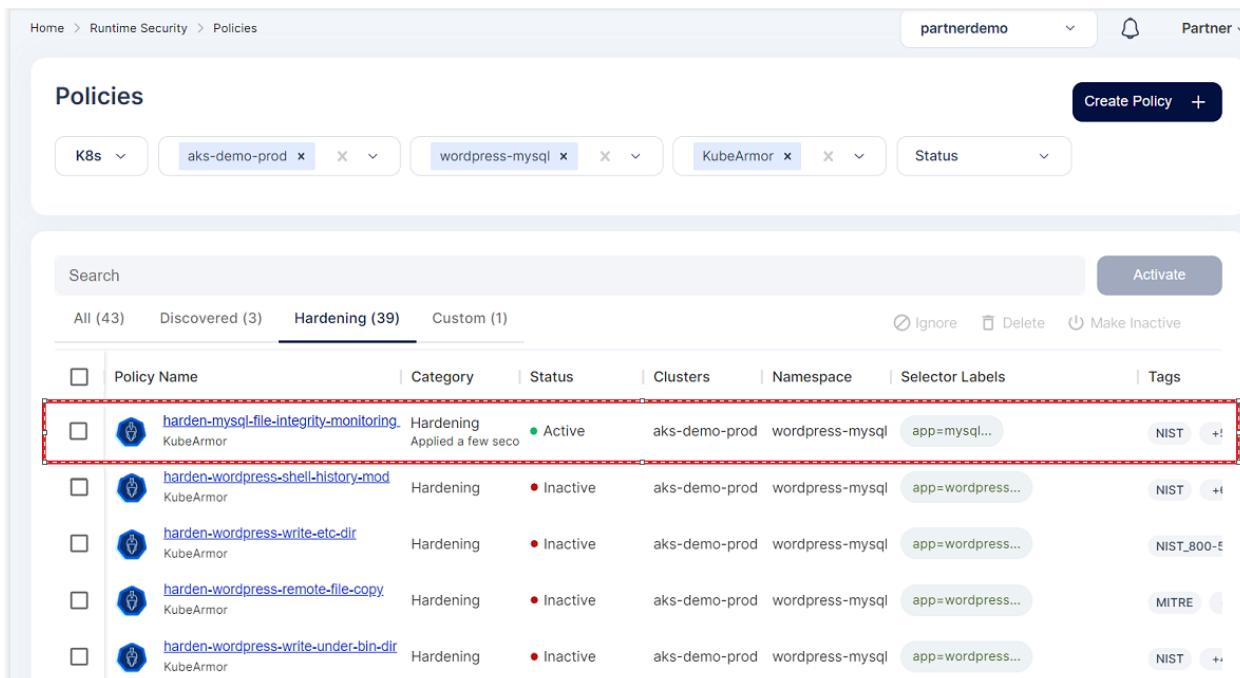
```
metadata:
name:
harden-mysql-file-integrity-monitoring
namespace: wordpress-mysql
spec:
action: Block
file:
matchDirectories:
- dir: /sbin/
readOnly: true
recursive: true
- dir: /usr/bin/
readOnly: true
recursive: true
- dir: /usr/lib/
readOnly: true
recursive: true
- dir: /usr/sbin/
readOnly: true
recursive: true
- dir: /bin/
readOnly: true
recursive: true
- dir: /boot/
readOnly: true
recursive: true
message: Detected and prevented
compromise to File integrity
selector:
matchLabels:
app: mysql
severity: 1
tags:
- NIST
- NIST_800-53_AU-2
- NIST_800-53_SI-4
- MITRE
- MITRE_T1036_masquerading
- MITRE_T1565_data_manipulation
```

- **Step 4:** To apply this policy, select the policy checkbox and click Activate option



Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
harden-wordpress-shell-history-mod	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-write-etc-dir	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST_800-5
harden-wordpress-remote-file-copy	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE
harden-wordpress-write-under-bin-dir	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-pkg-mngr-exec (v5)	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-file-integrity-monito	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-mysql-file-integrity-monitoring	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
harden-mysql-pkg-mngr-exec	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
harden-wordpress-trusted-cert-mod	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE

- **Step 5:** Now the policy is active and applied on the cluster

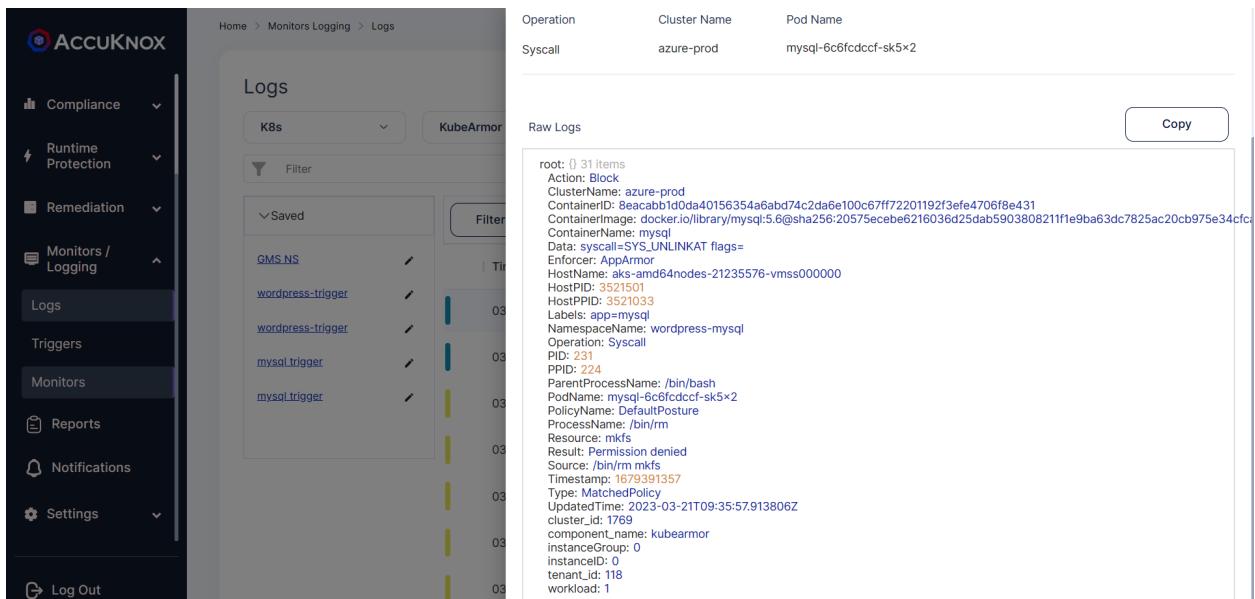


Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
harden-mysql-file-integrity-monitoring	Hardening	Active Applied a few sec	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
harden-wordpress-shell-history-mod	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-write-etc-dir	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST_800-5
harden-wordpress-remote-file-copy	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE
harden-wordpress-write-under-bin-dir	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!

- **Step 6:** If any attacker now tries to modify the content of the critical folders it will be blocked.

```
root@mysql-6c6fcdccf-sk5x2:/# cd sbin
root@mysql-6c6fcdccf-sk5x2:/sbin# ls
agetty      dump2fs    fsck.ext2    installkernel  mkfs.cramfs      pam_tally2      swaplabel
badblocks   e2fsck     fsck.ext3    isosize        mkfs.ext2       pivot_root     swapoff
blkdiscard  e2image    fsck.ext4    killall5      mkfs.ext3       raw           swapon
blkid       e2label    fsck.minix  ldconfig      mkfs.ext4       resize2fs     switch_root
blockdev    e2undo    fsfreeze     logsave      mkfs.minix     runuser      tune2fs
cfdisk      fdisk     fstab-decode losetup      mkhomedir_helper  sdfdisk     unix_chkpwd
chcpu       findfs    fstrim      mke2fs       mks2          shadowconfig  unix_update
ctrlaltdel  fsck     getty      mkfs         mkswap        start-stop-daemon  wipefs
debugfs    fsck.cramfs hwclock    mkfs.bfs    pam_tally     sulogin      zramctl
root@mysql-6c6fcdccf-sk5x2:/sbin# rm mkfs
rm: cannot remove 'mkfs': Permission denied
root@mysql-6c6fcdccf-sk5x2:/sbin#
```

- **Step 7:** To see the logs Navigate to the Monitoring/logging->logs



Logs

K8s

Raw Logs

root: [31 items]

Action: Block

ClusterName: azure-prod

ContainerID: 8eacab10da40156354a6abd74c2da6e100c67ff72201192f3efe4706f8e431

ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab5903808211f1e9ba63dc7825ac20cb975e34cfca

ContainerName: mysql

Data: syscall=SYS_UNLINKAT flags=

Enforcer: AppArmor

HostName: aks-amd64nodes-21235576-vmss000000

HostPID: 3521501

HostPPID: 3521033

Labels: app=mysql

NamespaceName: wordpress-mysql

Operation: Syscall

PID: 231

PPID: 224

ParentProcessName: /bin/bash

PodName: mysql-6c6fcdccf-sk5x2

PolicyName: DefaultPosture

ProcessName: /bin/rm

Resource: mkfs

Result: Permission denied

Source: /bin/rm mkfs

Timestamp: 1679391357

Type: MatchedPolicy

UpdatedTime: 2023-03-21T09:35:57.913806Z

cluster_id: 1769

component_name: kubearmor

instanceGroup: 0

instanceID: 0

tenant_id: 118

workload_id: 118

How to perform bulk operation on applying policies

- AccuKnox SaaS supports applying multiple policies at one time. To perform this user must navigate to the *Runtime Protection->Policies* Section.
- From the Filters shown in the Screen user must select the Cluster and Namespace for which they are going to apply multiple policies

Home > Runtime Security > Policies

partnerdemo Partner ▾

Policies

K8s aks-demo-prod wordpress-mysql KubeArmor Status Create Policy +

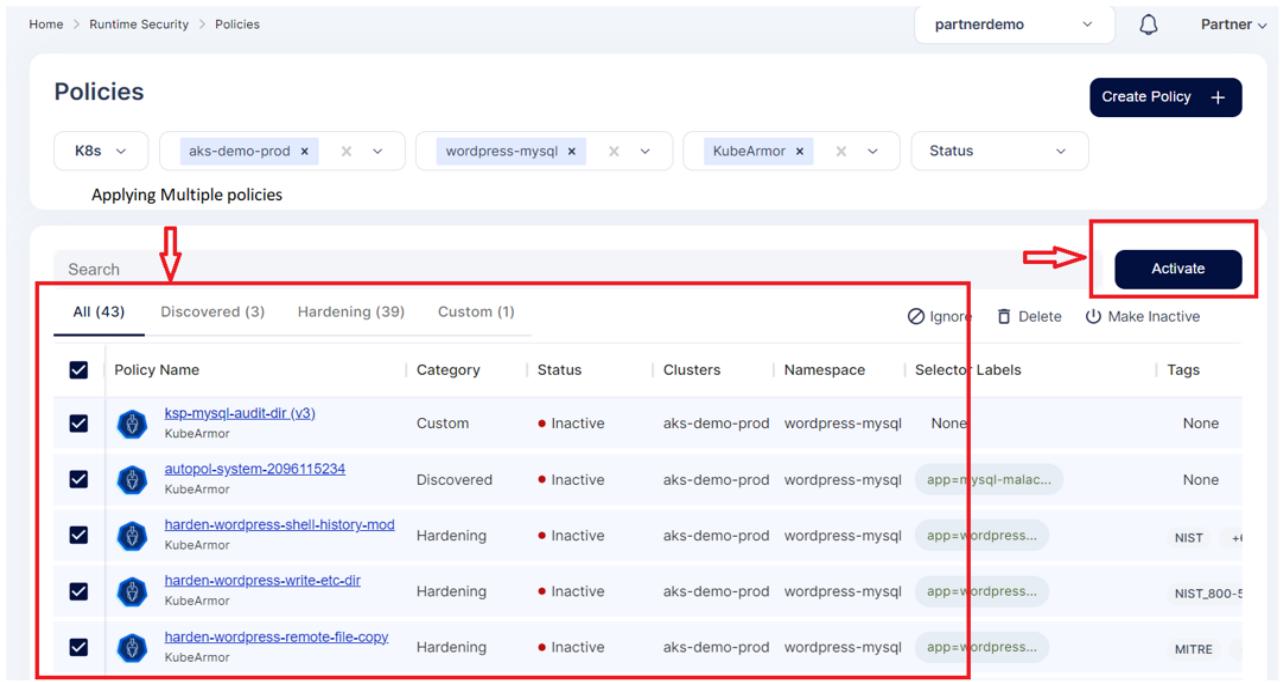
Search

All (43) Discovered (3) Hardening (39) Custom (1)

Ignore Delete Make Inactive

<input type="checkbox"/>	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
<input type="checkbox"/>	ksp-mysql-audit-dir (v3) KubeArmor	Custom Applied 20 minutes	● Active	aks-demo-prod	wordpress-mysql	None	None
<input type="checkbox"/>	harden-wordpress-pkg-mngr-exec (v5) KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +
<input type="checkbox"/>	harden-wordpress-file-integrity-monitor KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +

- To apply multiple policies in single go select the all policies from the screen and click Activate button

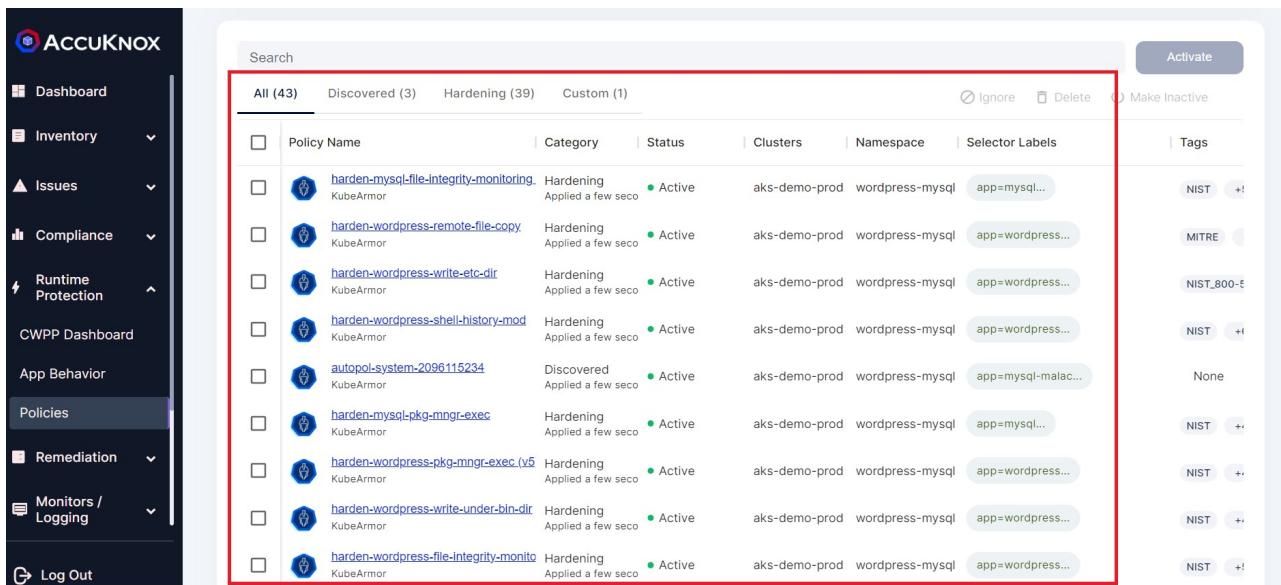


The screenshot shows the ACCUKNOX Policies page. At the top, there are several filter dropdowns: K8s, aks-demo-prod, wordpress-mysql, KubeArmor, and Status. A red arrow points down to the search bar. Another red box highlights the list of policies under the heading "All (43)". The policies listed include:

Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
ksp-mysql-audit-dir (v3)	Custom	Inactive	aks-demo-prod	wordpress-mysql	None	None
autopol-system-2096115234	Discovered	Inactive	aks-demo-prod	wordpress-mysql	app=mysql-malac...	None
harden-wordpress-shell-history-mod	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-write-etc-dir	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST_800-5
harden-wordpress-remote-file-copy	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE

On the right side, there are buttons for Ignore, Delete, Make Inactive, and a prominent red-bordered "Activate" button.

- Now after activating all the policies they will be made active and applied in the cluster.



The screenshot shows the ACCUKNOX Policies page after activation. The list of policies is identical to the previous screenshot, but now every policy entry has a checked checkbox in the first column. The "Status" column now shows "Active" for all policies. The "Activate" button at the top right is no longer highlighted.

Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
harden-mysql-file-integrity-monitoring	Hardening	Active	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
harden-wordpress-remote-file-copy	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE
harden-wordpress-write-etc-dir	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST_800-5
harden-wordpress-shell-history-mod	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
autopol-system-2096115234	Discovered	Active	aks-demo-prod	wordpress-mysql	app=mysql-malac...	None
harden-mysql-pkg-mngr-exec	Hardening	Active	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
harden-wordpress-pkg-mngr-exec (v5)	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-write-under-bin-dir	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!
harden-wordpress-file-integrity-monito	Hardening	Active	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +!

Integrations

1. Integrate SIEM tools

- SPLUNK
- AWS Cloud Watch
- Rsyslog

Splunk

Splunk Integration:

Splunk is a software platform to search, analyze, and visualize machine-generated data gathered from websites, applications, sensors, and devices.

AccuKnox integrates with Splunk and monitors your assets and sends alerts for resource misconfigurations, compliance violations, network security risks, and anomalous user activities to Splunk. To forward the events from your workspace you must have Splunk Deployed and HEC URL generated first for Splunk Integration.

Integration of Splunk:

a. Prerequisites:

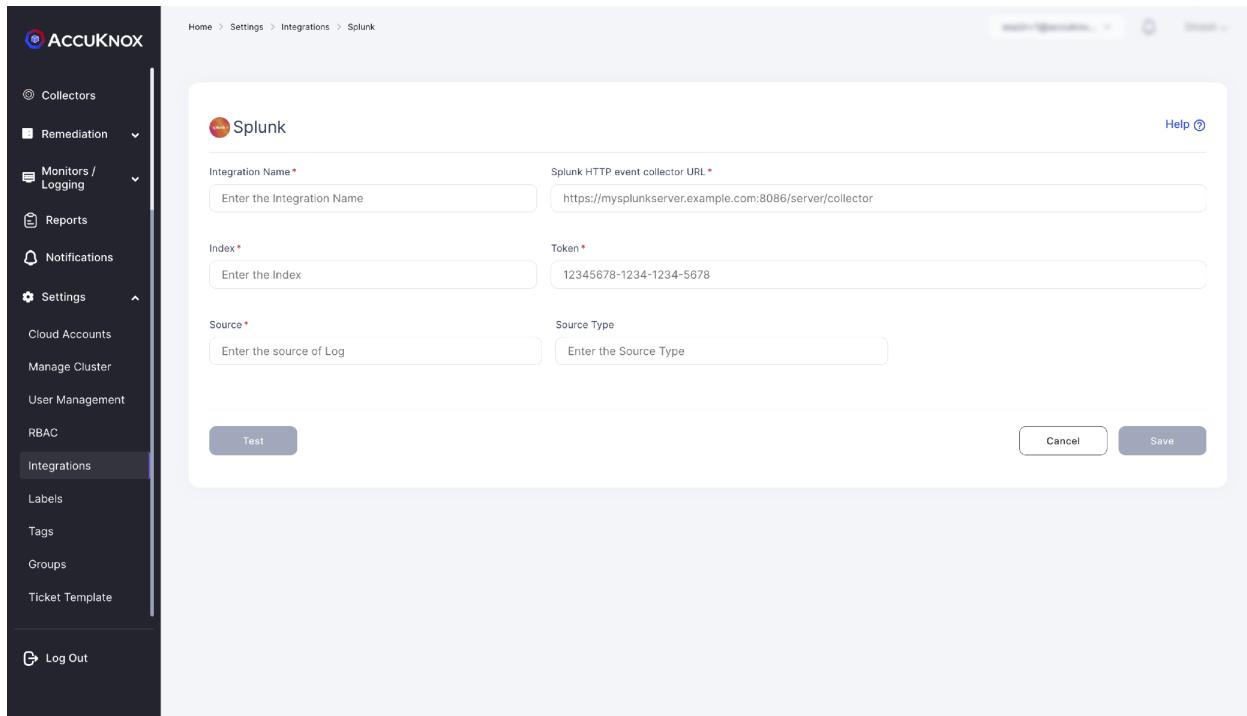
Set up Splunk HTTP Event Collector (HEC) to view alert notifications from AccuKnox in Splunk. Splunk HEC lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols.

To set up HEC, use instructions in [Splunk documentation](#). For source type,_json is the default; if you specify a custom string on AccuKnox, that value will overwrite anything you set here.

Select Settings > Data inputs > HTTP Event Collector and make sure you see HEC added in the list and that the status shows that it is Enabled.

b. Steps to Integrate:

- Go to Settings->Integration.
- Click Integrate now on Splunk.



- Enter the following details to configure Splunk.
- Select the Splunk App: From the dropdown, Select Splunk Enterprise.
 - Integration Name: Enter the name for the integration. You can set any name. e.g., sh Test Splunk
 - Splunk HTTP event collector URL: Enter your Splunk HEC URL generated earlier.e.g., sh https://splunk-xxxxxxxxxx.com/services/collector
 - Index: Enter your Splunk Index, once created while creating HEC. e.g., sh main
 - Token: Enter your Splunk Token, generated while creating HEC URL. e.g., sh x000x0x0x-0xxx-0xxx-xxxx-xxxxx00000
 - Source: Enter the source as http: sh Kafka
 - Source Type: Enter your Source Type here, this can be anything and the same will be attached to the event type forwarded to Splunk. e.g., sh _json

- Click Test to check the new functionality, You will receive the test message on the configured slack channel. e.g.,sh Test Message host = xxxxxxxx-deployment-xxxxxxxx-xxx00 source = http:kafka sourcetype = trials
- Click Save to save the Integration. You can now configure Alert Triggers for Slack Notifications.

AWS Cloudwatch

AWS CloudWatch Integration

Navigate to Settings->Integrations. Choose "AWS CloudWatch" services and click the Integrate Now button.

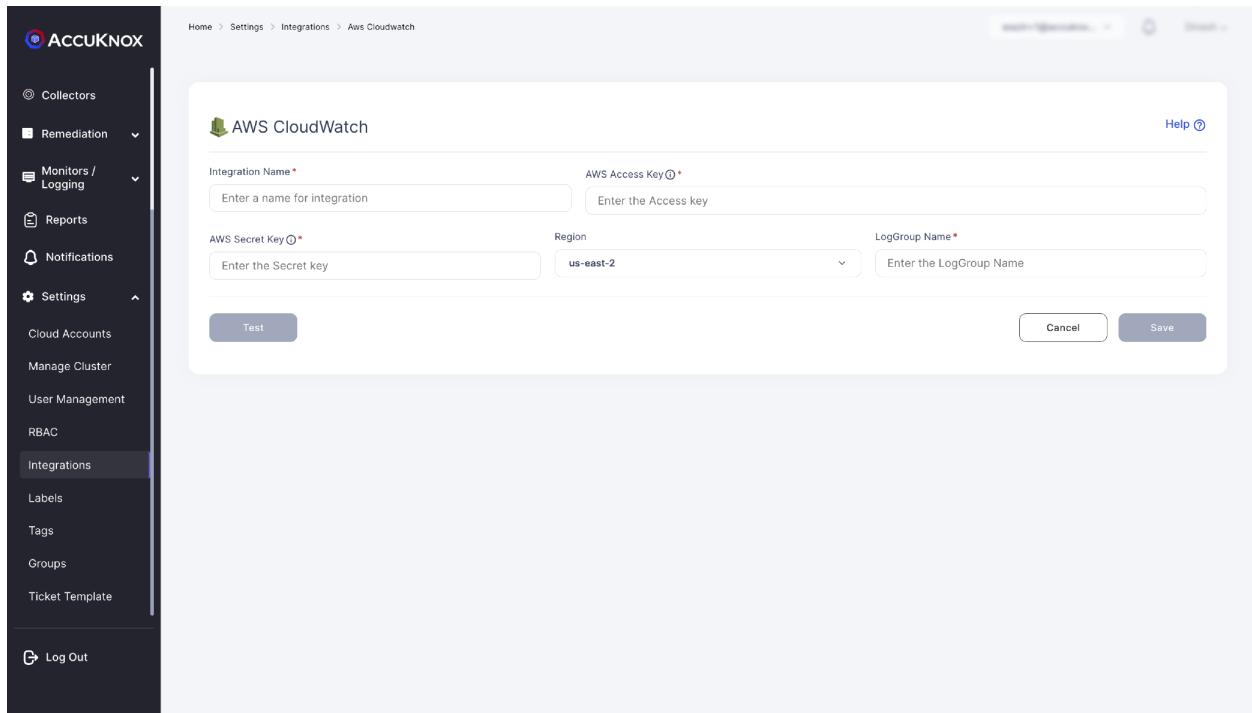
Integration of Amazon CloudWatch:

a. Prerequisites

- AWS Access Key / AWS Secret Key is required for this Integration.
- [Note]: Please refer to this link to create an access keys [link](#)

b. Steps to Integrate:

- Go to Channel Integration URL
- Click the Integrate Now button -> AWS CloudWatch



- Here you'll be able to see these entries:
 - Integration Name: Enter the name for the integration. You can set any name.
 - AWS Access Key: Enter your AWS Access Key here.
 - AWS Secret Key: Enter your AWS Secret Key here.
 - Region Name: Enter your AWS Region Name here.
- Once you fill in every field and then click the button this will test whether your integration is working or not.
- Click the Save button.

c. Configuration of Alert Triggers:

- On the Logs page, after choosing a specific log filter click on the 'Create Trigger' button.
- The below fields need to be entered with appropriate data:
 - Name: Enter the name of the trigger. You can set any name without special characters.
 - When to Initiate: The frequency of the trigger as Real Time /.
 - Status: Enter the severity of the trigger.
 - Search Filter Data: The filter log chosen is automatically populated here. This is optional.
 - Predefined queries: The list of predefined queries for this workspace is shown as default.

- Notification Channel: Select the integration channel that needs to receive logs. This should be AWS CloudWatch. (Note: Channel Integration is done on the previous step)
- Save: Click on Save for the trigger to get stored in the database.

d. Logs Forwarding:

- For each Enabled Trigger, please check the AWS platform to view the logs.
- Based on Frequency (Real Time / Once in a Day / Week)
- The Rule Engine matches the real-time logs against the triggers created.

Rsyslog

RSyslog Integration

To forward the events to RSyslog you must first set up the RSyslog Integration.

Integration of RSyslog:

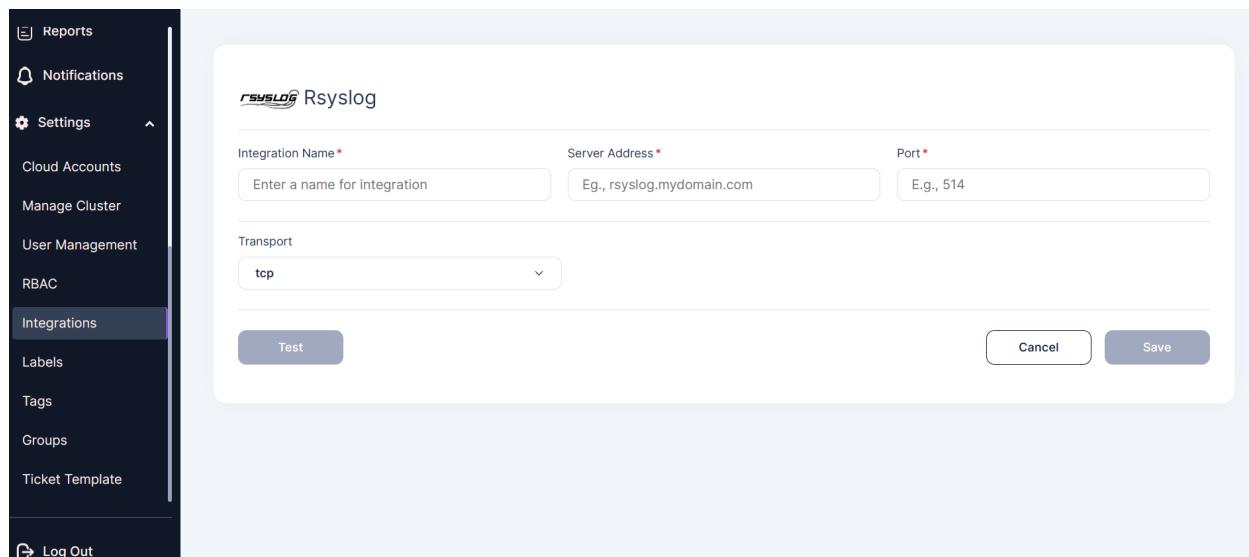
a. Prerequisites:

- A running RSyslog server.
- Host name/IP, Port number, Transport type(TCP or UDP)

Note: To deploy the RSyslog server, follow [RSyslog Documentation](#).

b. Steps to Integrate:

- Go to Settings → Integrations → CWPP(Tab).
- Click integrate now on RSyslog.



- Fill up the following fields:

- Integration Name: Enter the name for the integration. You can set any name of your choice. e.g., Container Security Alerts
- Server Address: Enter your RSyslog Server address here, IP address or fully qualified domain name (FQDN) of the RSyslog server e.g.,rsyslog.mydomain.com or 35.xx.xx.xx
- Port: The port number to use when sending RSyslog messages (default is UDP on port 514); you must use the same port number. e.g., 514
- Transport: Select UDP, or TCP as the method of communication with the RSyslog server
- Click Test to check the new functionality, You will receive the test message on configured RSyslog Server. -Test message Please ignore !!
- Click Save to save the Integration. You can now configure Alert Triggers for RSyslog Events

2. Integrate Notifications Tools

- Slack

Slack

Slack Integration:

To send an alert notification via Slack you must first set up the Slack notification Channel.

Integration of Slack:

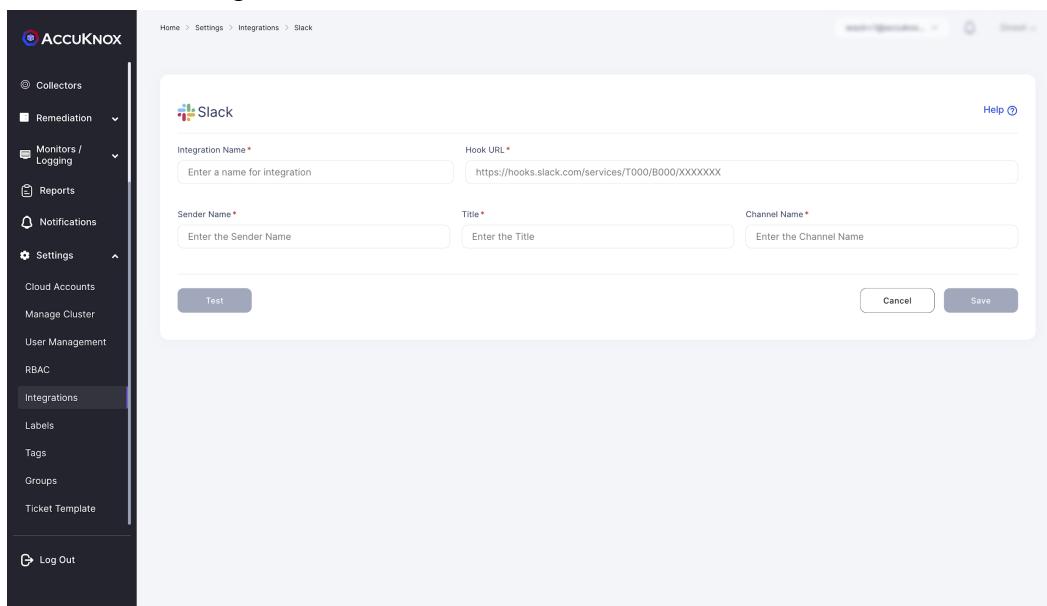
a. Prerequisites:

You need a valid and active account in Slack. After logging into your Slack channel, you must generate a Hook URL.

Note: To generate a Hook URL follow the steps, [Webhooks-for-Slack](#).

b. Steps to Integrate:

- Go to Channel Integration.
- Click Integrate now on Slack.



- Fill up the following fields:

- Integration Name: Enter the name for the integration. You can set any name. e.g., Container Security Alerts
- Hook URL: Enter your generated slack hook URL here. e.g., <https://hooks.slack.com/services/T000/B000/XXXXXX>
- Sender Name: Enter the sender name here. e.g., AccuKnox User
- Channel Name: Enter your slack channel name here. e.g., livealertsforcontainer
- Click Test to check the new functionality, You will receive the test message on configured slack channel. Test message Please ignore !!
- Click Save to save the Integration. You can now configure Alert Triggers for Slack Notifications.

3. Integrate Ticketing Tools

- Jira cloud
- fresh service

Jira Integration

Integrate AccuKnox with Jira and receive AccuKnox alert notifications in your Jira accounts. With this integration, you can automate the process of generating Jira tickets with your existing security workflow.

To set up this integration, you need to coordinate with your Jira administrator and gather the inputs needed to enable communication between AccuKnox and Jira.

Integration of JIRA:

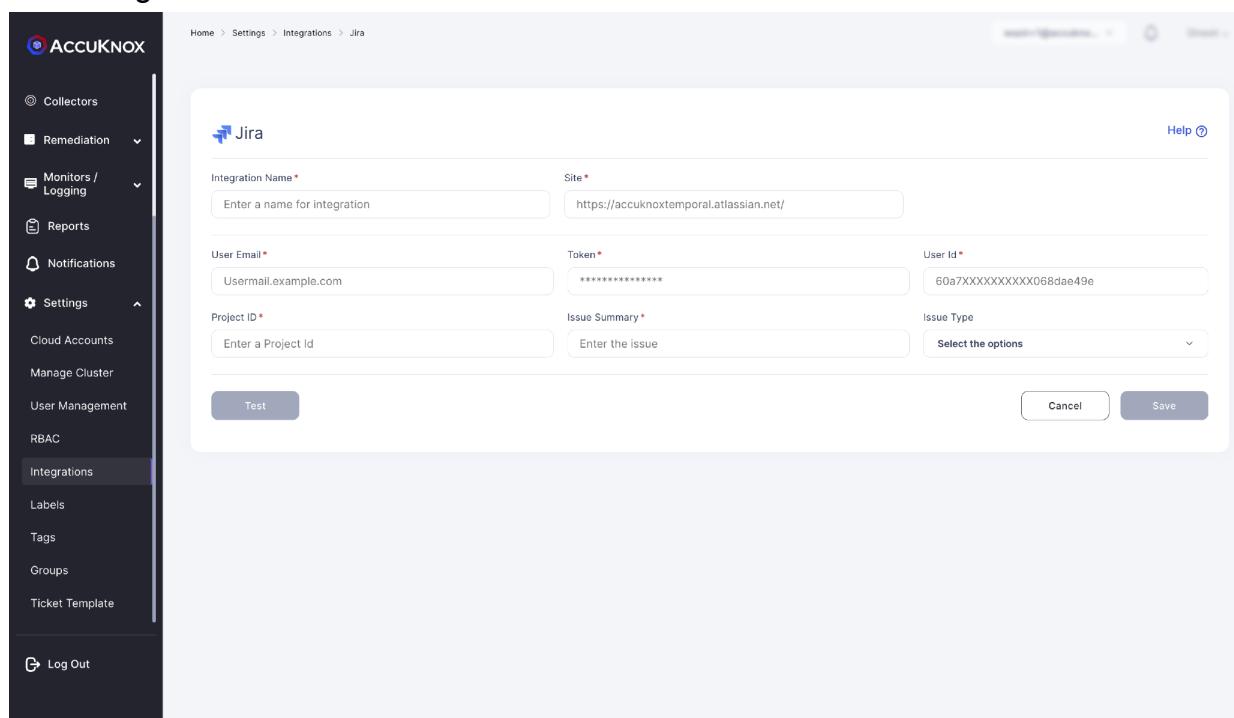
Prerequisites

- You need a Jira Site URL, Email, UserID & API token, and Project key for this integration.
- To create a JIRA token go to <https://id.atlassian.com/manage-profile/security/api-tokens>, and click on create an API token.

JIRA integration for CWPP:

Steps to Integrate:

- Go to Channel Integration.
- Click integrate now on JIRA



The screenshot shows the AccuKnox interface for setting up a Jira integration. On the left, a sidebar menu is open with 'Integrations' selected under 'Settings'. The main content area is titled 'Jira' and contains the following form fields:

- Integration Name ***: Test
- Site ***: https://accuknoxtemporal.atlassian.net/
- User Email ***: Usermail.example.com
- Token ***: (Redacted)
- User Id ***: 60a7XXXXXXXXXX068dae49e
- Project ID ***: Enter a Project Id
- Issue Summary ***: Enter the issue
- Issue Type**: Select the options

At the bottom of the form are three buttons: 'Test', 'Cancel', and 'Save'.

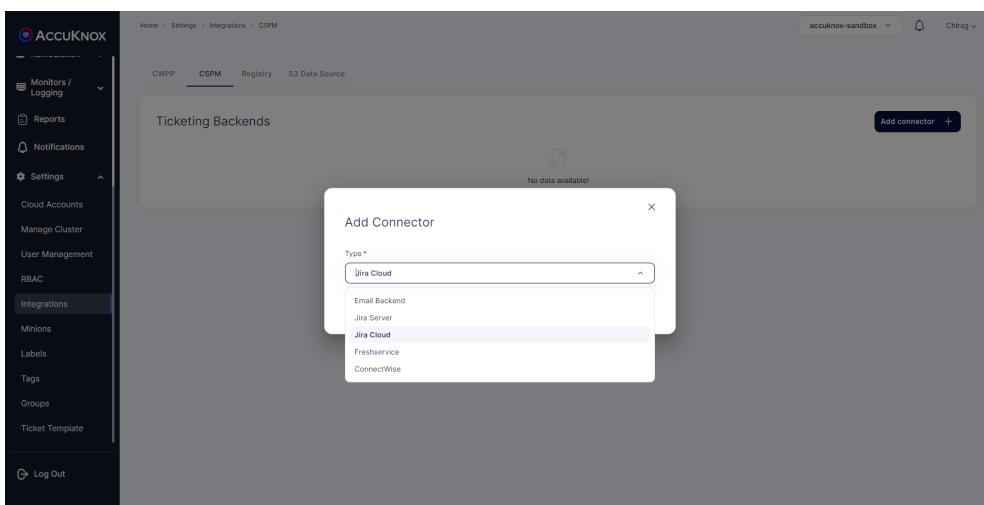
- Enter the following details to configure JIRA.
- **Integration Name:** Enter the name for the integration. You can set any name. e.g., Test JIRA
- **Site:** Enter the site name of your organization. e.g., <https://jiratest.atlassian.net/>

- User Email: Enter your Jira account email address here.e.g., jira@organisation.com
- Token: Enter the generated Token here from <https://id.atlassian.com/manage-profile/security/api-tokens>. e.g., kRVxxxxxxxxxxxxxx39
- User ID: Enter your Jira user ID here. You can visit the people section and search your name to see the User ID. For more details check here. e.g., 5bbxxxxxxxxx0103780
- Project ID: Enter your Project key here, each project in an organization starts with some key value and is case-sensitive. Breakdown of a Jira ticket to identify Project ID: [https://\[JIRA-SITE\]/browse/\[PROJECT ID\]-1414](https://[JIRA-SITE]/browse/[PROJECT ID]-1414), e.g., DEVSECOPS
- Issue Summary: Enter the summary for the JIRA tickets to be viewed in each JIRA ticket created. e.g., Issues generated from High Severity Incidents on the onboarded cluster.
- Issue Type: You can choose from the dropdown. i.e., Story and Bug
- Click Test to check if the entered details are being validated, If you receive Test Successful, you have entered valid JIRA credentials.
- Click Save to save the Integration.

JIRA integration for CSPM:

Steps to Integrate:

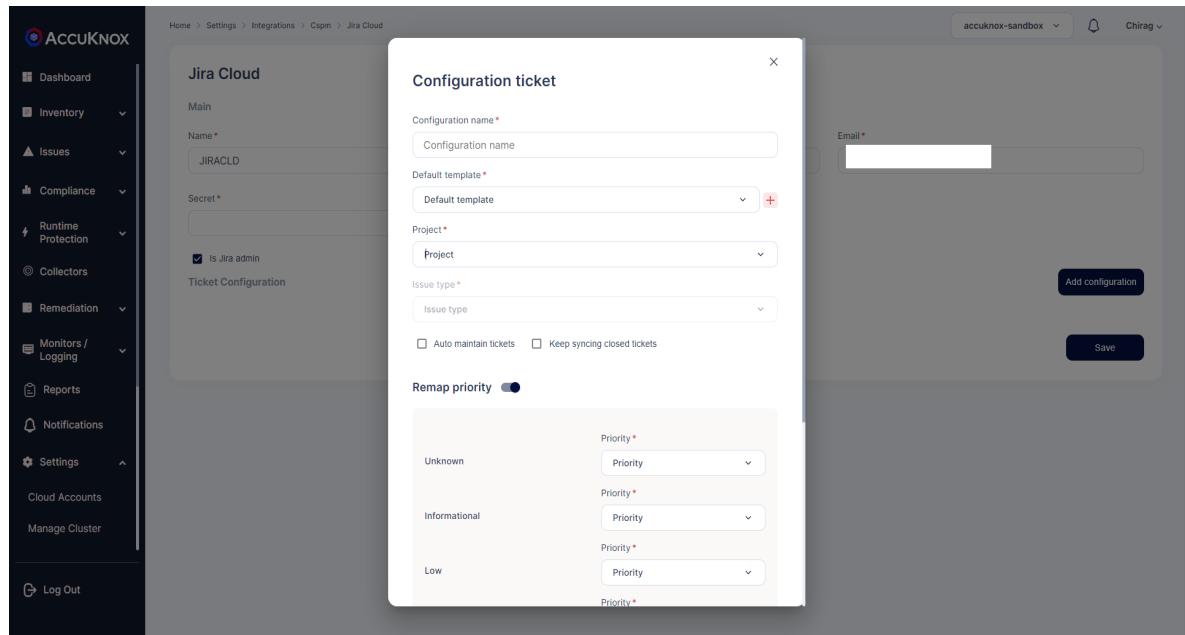
- Go to Channel Integration -> CSPM.
- Click on add the Connector and select JIRA Cloud



Enter the following details to configure JIRA.

- Integration Name: Enter the name for the integration. You can set any name. e.g., Test JIRA

- Site: Enter the site name of your organization. e.g., <https://jiratest.atlassian.net/>
- User Email: Enter your Jira account email address here.e.g., jira@organisation.com
- Token: Enter the generated Token here from <https://id.atlassian.com/manage-profile/security/api-tokens>. .e.g., [kRVxxxxxxxxxxxxxx39](#)



Click on the Jira ticketing backend to add config. Here Enter the following details:

- Configuration name: this name will be displayed under ticket configuration while creating tickets.
- Default template: to specify the data that this configuration will be used for making tickets.
- Project name: From the list of projects select the project where you want your tickets to be created.
- Issue Type: You can choose from the dropdown.
- Fill in the priority mapping according to your choice and press save.

You can now configure Alert Triggers for JIRA.

Freshservice

Freshservice Integration:

Integrate AccuKnox with Freshservice and receive AccuKnox alert notifications in your Freshservice accounts. With this integration, you can automate the process of generating Freshservice “Problem alerts” with your existing security workflow.

To set up this integration, you need to coordinate with your Freshservice administrator and gather the inputs needed to enable communication between AccuKnox and Freshservice.

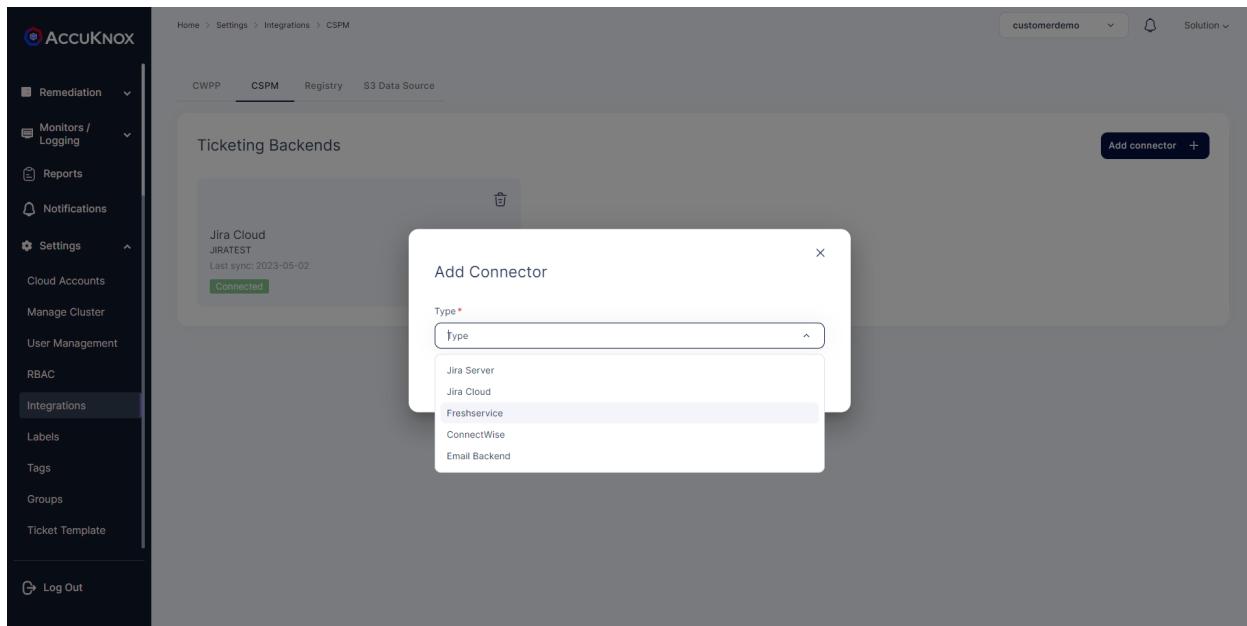
Integration of Freshservice:

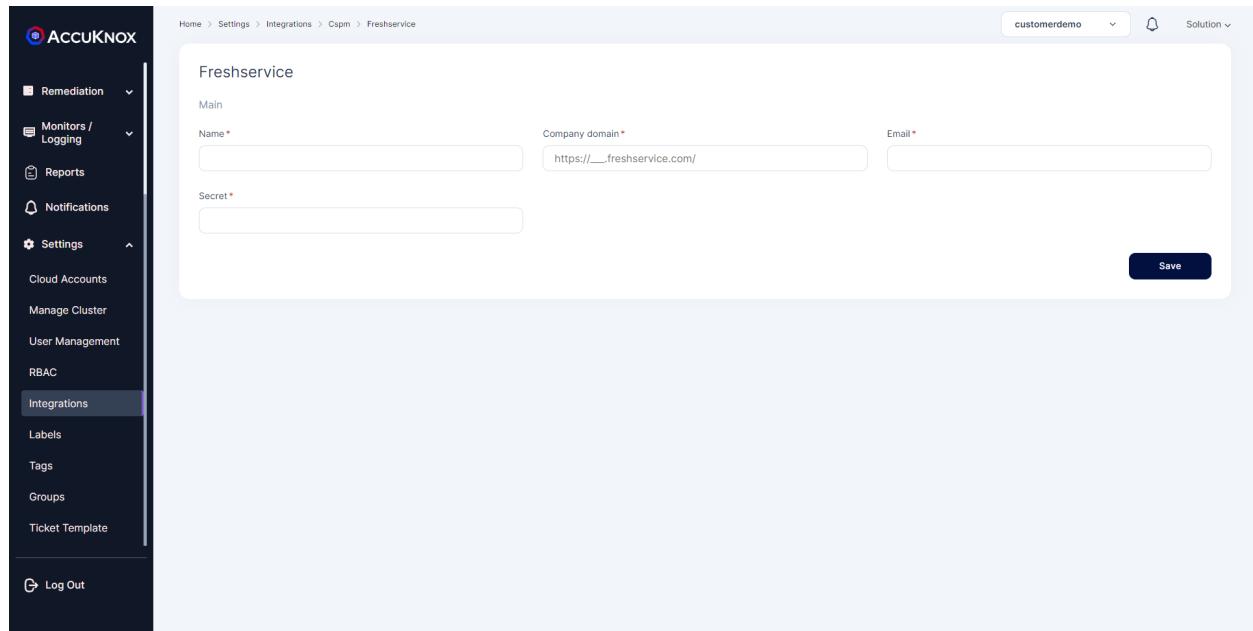
a. Prerequisites

- You need a Company domain, Email & API key (secret) for this integration.
- You can find your API key in profile settings in the right side column.

b. Steps to Integrate:

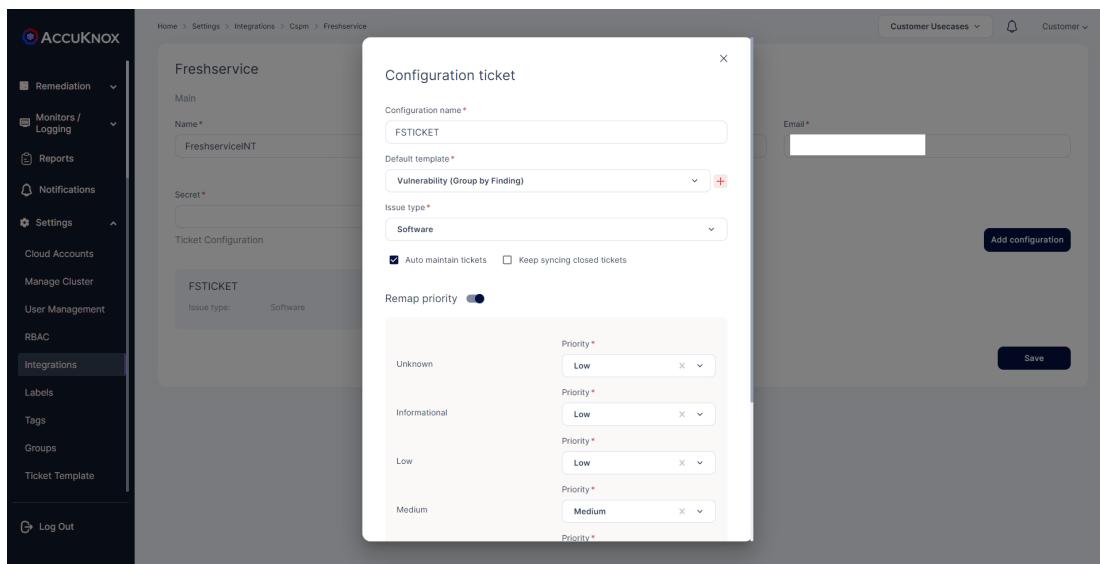
- Go to Channel Integration -> CSPM.
- Click on Add the connector and select Freshservice





Enter the following details to configure Fresh Service.

- **Integration Name:** Enter the name for the integration. You can set any name. e.g., TestFreshservice
- **Domain Name:** Enter the site name of your organization as shown in your URL. e.g., for https://accuknoxexample.freshservice.com/ enter the domain name as accuknoxexample.
- **User Email:** Enter your Freshservice account email address here. e.g., freshservice@organisation.com
- **Secret:** Enter the API key Here. This can be found in profile settings.
- **Click Save to save the Integration.**



Click on the Freshservice ticketing backend to add configuration.

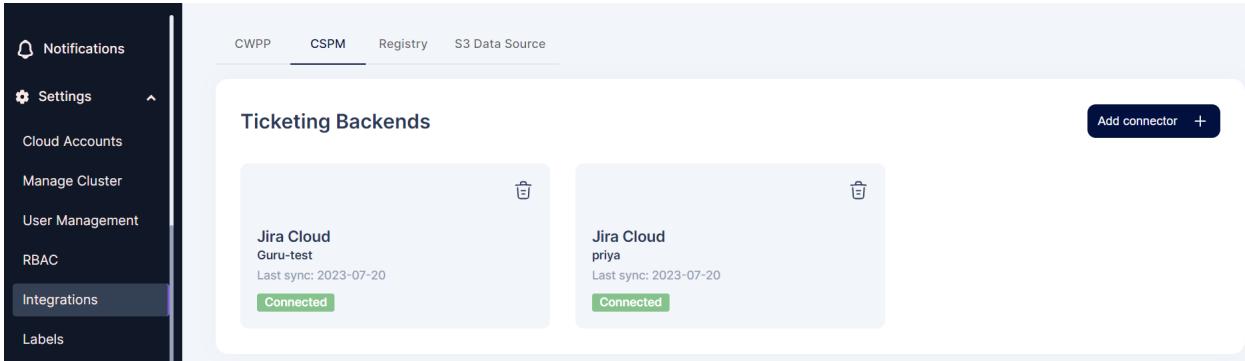
Here Enter the following details:

- Configuration name: this name will be displayed under ticket configuration while creating tickets.
- Default template: to specify the data that this configuration will be used for making tickets.
- Issue Type: You can choose from the dropdown.
- Fill in the priority mapping according to your choice and press save.

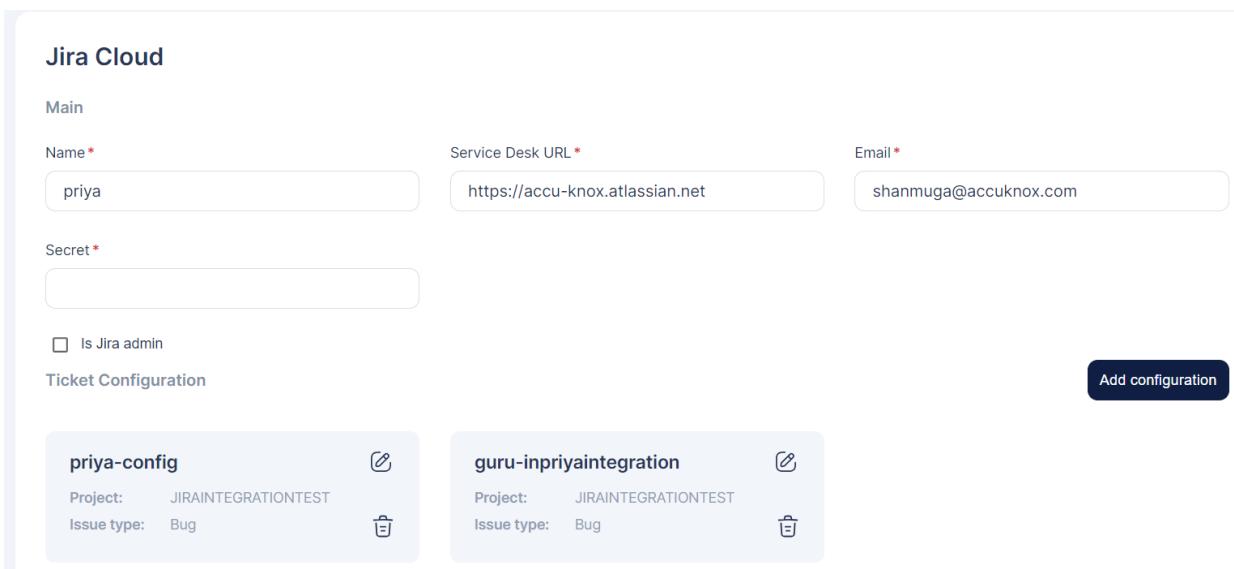
You can now configure Alert Triggers for Freshservice.

Creating Ticket Configuration

- To create a ticket configuration, navigate to Integrations under Settings and click on the CSPM tab. This will show all the ticketing backends that have been integrated:



- Click on one of the integrated Ticketing backends and click on Add Configuration button in the subsequent screen:



- Enter a name for the configuration and select template for the ticket. The selected template will make it available in the respective screen as a ticket configuration. Eg. Selecting Vulnerability will make it available as a ticket configuration to select under Issues -> Vulnerabilities for creating tickets.

Configuration ticket

Configuration name *

Default template *

Default template

+  

Compliance Template
Datalist Software Template
Vulnerability (Group by Finding)

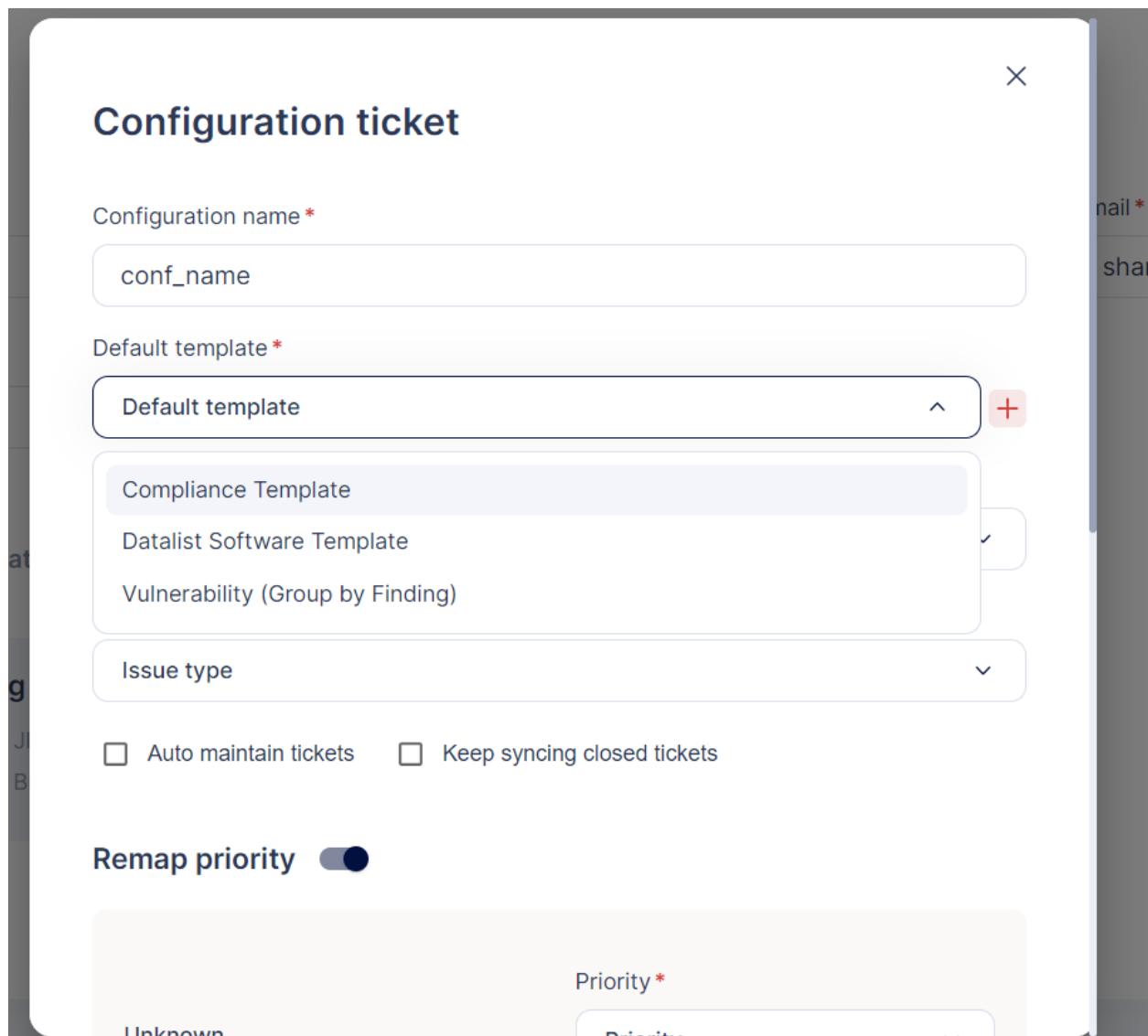
Issue type 

Auto maintain tickets Keep syncing closed tickets

Remap priority 

Priority * 

Unknown 



- Enter the relevant data in the remaining fields and click on Save. The ticket configuration is created successfully

4. Integrate Registries

Registry

- AccuKnox CSPM tool provides with registry scan where the user can onboard their Docker Hub, Nexus, GCR, and ECR registries. Once the registry is onboarded, the scanning of the registry starts automatically in the background. After the scanning is completed, the findings will be populated in the registry scan dashboard.

- To Onboard Registry [click here](#)

Amazon Elastic Container Registry:

- Accuknox CSPM security tool scans images that are present in the onboarded [Amazon Elastic Container Registry](#) and identifies any known vulnerabilities and risks associated with those images. These are then categorized based on their severity. Users will be getting a comprehensive view of these risks and vulnerabilities in the dashboard which can be remediated.

Google Container Registry:

- [Google Container Registry](#) with images Once onboarded into the AccuKnox SaaS platform, the images are scanned. The risks and vulnerabilities associated with these images are identified and shown in the scan results. The vulnerabilities are classified based on the CVSS Scores.

Nexus Registry:

- AccuKnox CSPM Security leverages various open-source scanning tools to scan the images present in the onboarded Nexus Repository. It identifies the common vulnerabilities and exploits associated with those images and risks. These Vulnerabilities and risks are classified based on their severity.

DockerHub Registry:

- [DockerHub](#) Repositories can be integrated with AccuKnox SaaS. Once these registries are onboarded, the images are scanned for vulnerabilities and risks. These findings are populated in the dashboard with Critical, High, and low vulnerabilities.

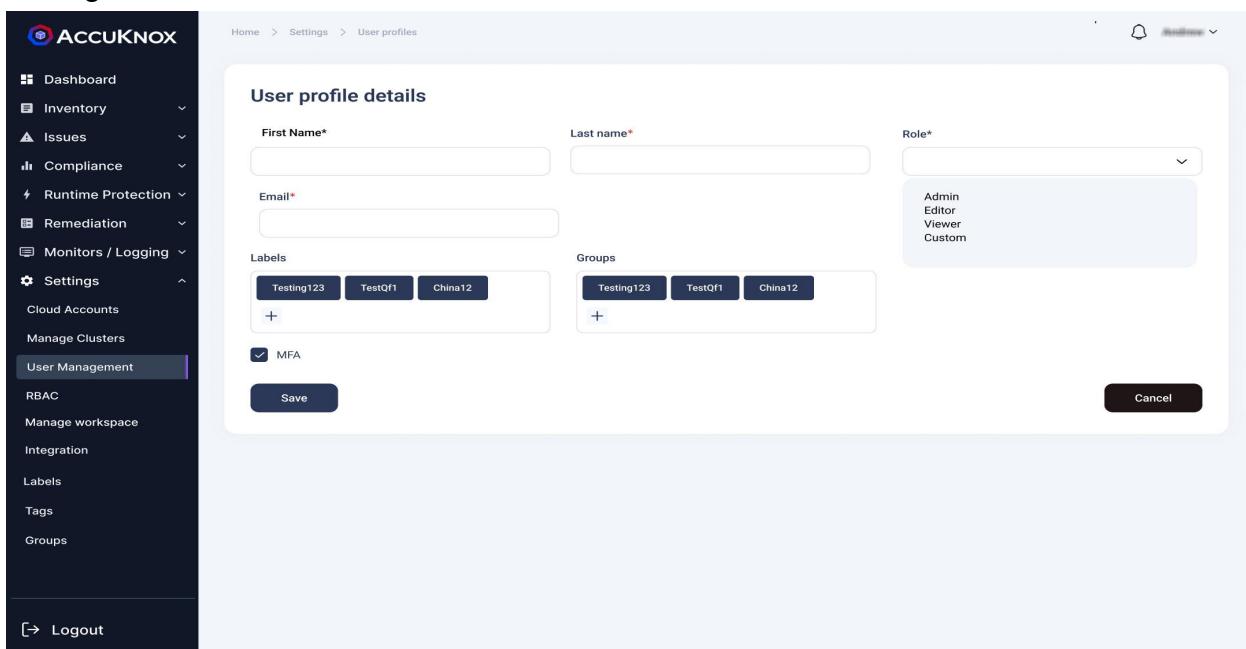
User Management

AccuKnox SaaS provides the ability to authenticate and authorize multiple users to access and utilize the SaaS platform. Inside the user management section user can create profiles for other users and these profiles are displayed in the form of a list. From the list, users can View Permissions, Edit, Deactivate, and delete user profiles. Permission is given to users by assigning roles while creating a user profile. These roles are created in the RBAC section. Deactivated users can be viewed under the Deactivated Users subsection. Creating a user sends an invite to their email id, invites that are not yet accepted are present inside the Pending Invites subsection.

Invite folks to the workspace

Inviting new users:

Step 1: we can invite a new user to the tenant by clicking on the Add user option provided on the screen. In the below screen, new user details need to be given for inviting him to this tenant id.



The screenshot shows the AccuKnox SaaS platform's User Management section. The left sidebar has a dark theme with various navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Settings, Cloud Accounts, Manage Clusters, and User Management (which is currently selected). Below these are RBAC, Manage workspace, Integration, Labels, Tags, and Groups. At the bottom is a Logout button. The main content area is titled "User profile details". It contains fields for First Name*, Last name*, Email*, and Role*. The Role* dropdown is open, showing options: Admin, Editor, Viewer, and Custom. There are also sections for Labels (with buttons for Testing123, TestQf1, China12) and Groups (with buttons for Testing123, TestQf1, China12). A checkbox for MFA is checked. At the bottom are Save and Cancel buttons.

Step 2: Fill in the necessary details for the user invite

Dashboard

Inventory

Issues

Compliance

Runtime Protection

Remediation

Monitors / Logging

User Management

RBAC

Manage workspace

Integration

Labels

Tags

Groups

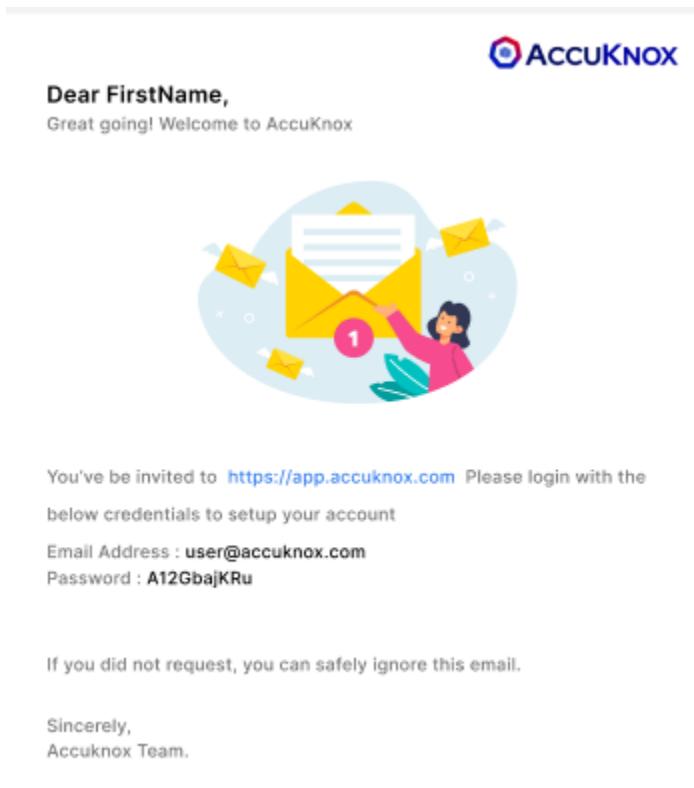
[Logout](#)

User Profile Detail

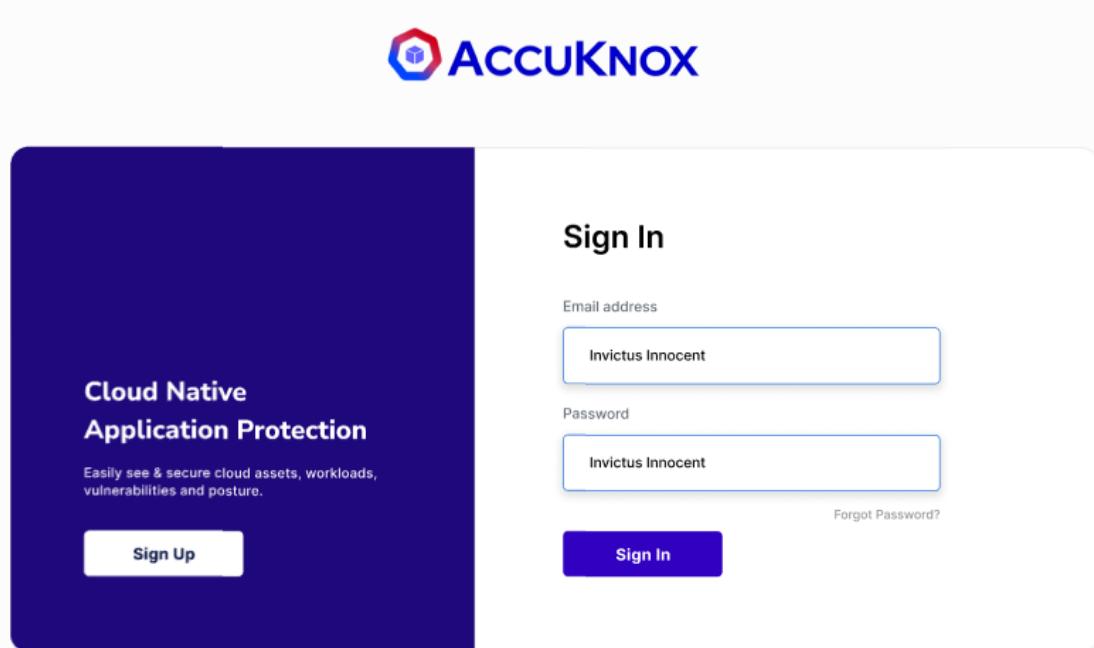
First Name*	Last Name*	Role*
<input type="text" value="FirstName"/>	<input type="text" value="LastName"/>	<input type="text" value="Admin"/>
Email*	Labels	Groups
<input type="text" value="user@example.com"/>	<input type="text" value="audit file"/> <input type="text" value="description"/> <input type="text" value="id"/> <input type="text" value="plugin id"/> <input type="text" value="hash"/> <input type="text" value="network"/> <input type="text" value="post"/> <input type="button" value="+"/>	<input type="text" value="audit file"/> <input type="text" value="description"/> <input type="text" value="finding"/> <input type="text" value="hash"/> <input type="button" value="+"/>
<input checked="" type="checkbox"/> MFA		
<input type="button" value="Cancel"/> <input type="button" value="Save"/>		

Step 3:

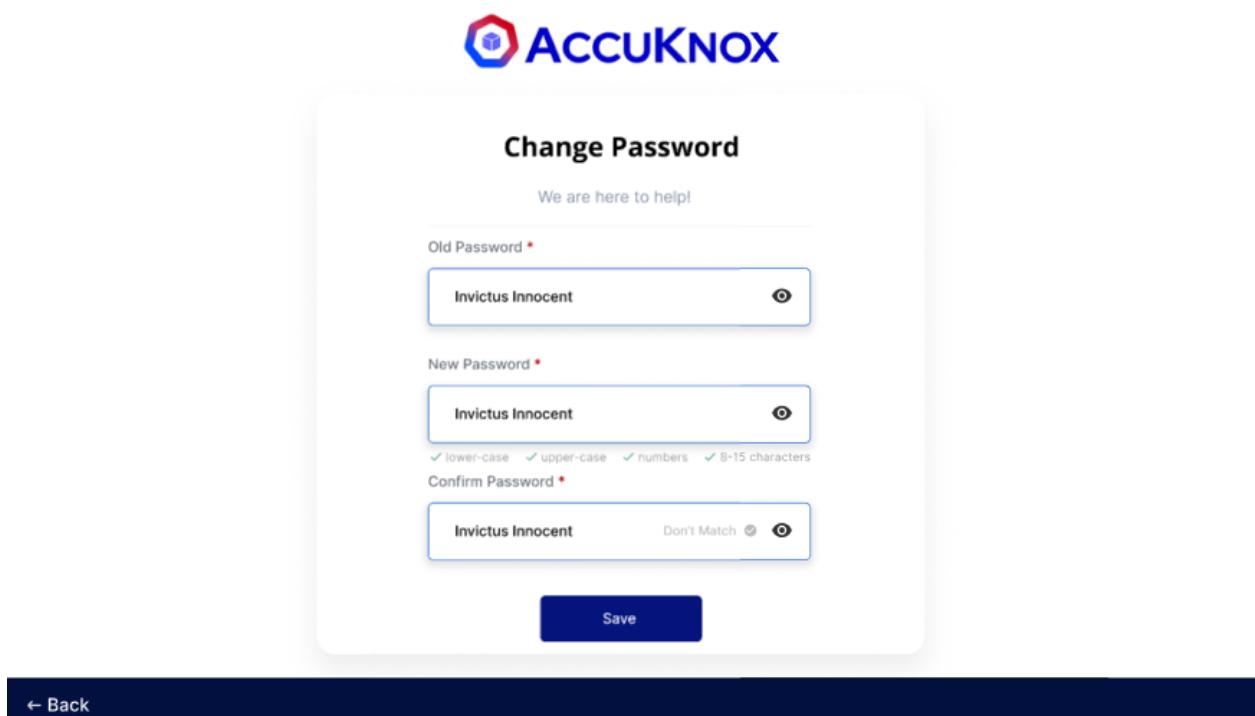
After we click save, the new user will be getting a user invite email with username, password, and sign in link to the mentioned email id



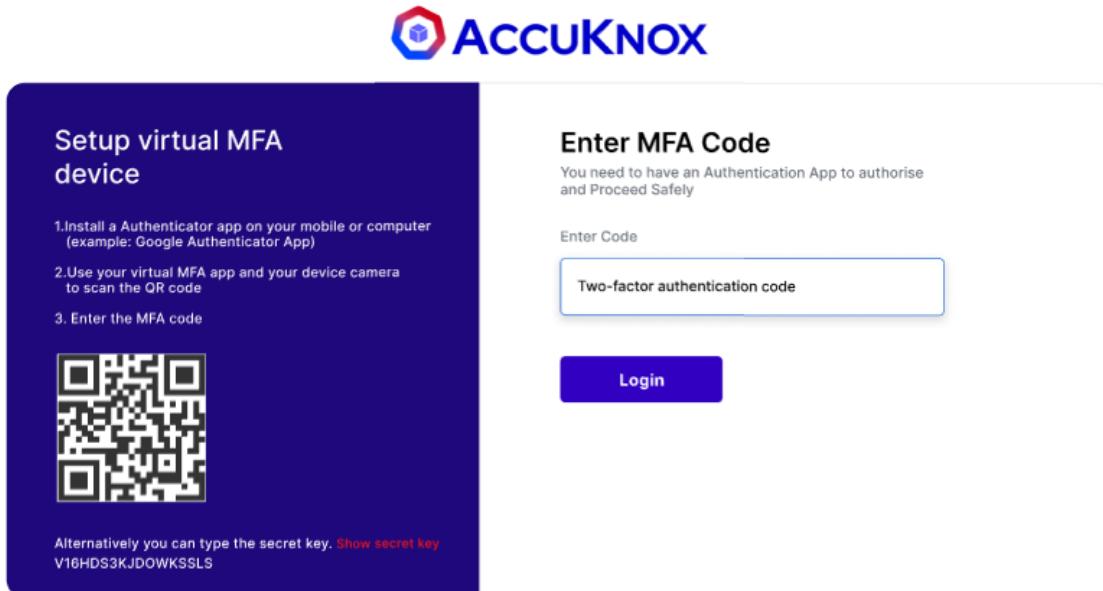
Step 4: The user needs to sign in with the credentials provided in the email.



Step 5: After signing in user will be prompted to change the password.

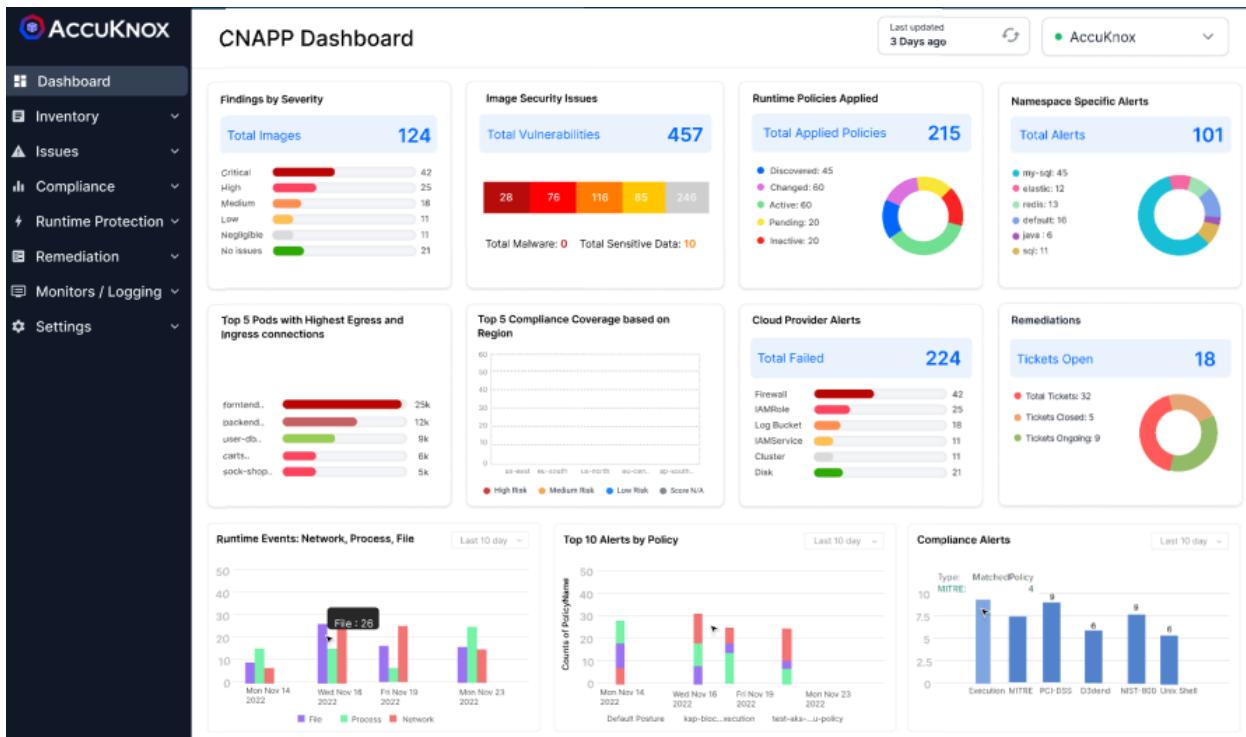


Step 6: Once the password is changed, the user will need to set MFA for his account using any Authenticator Application.



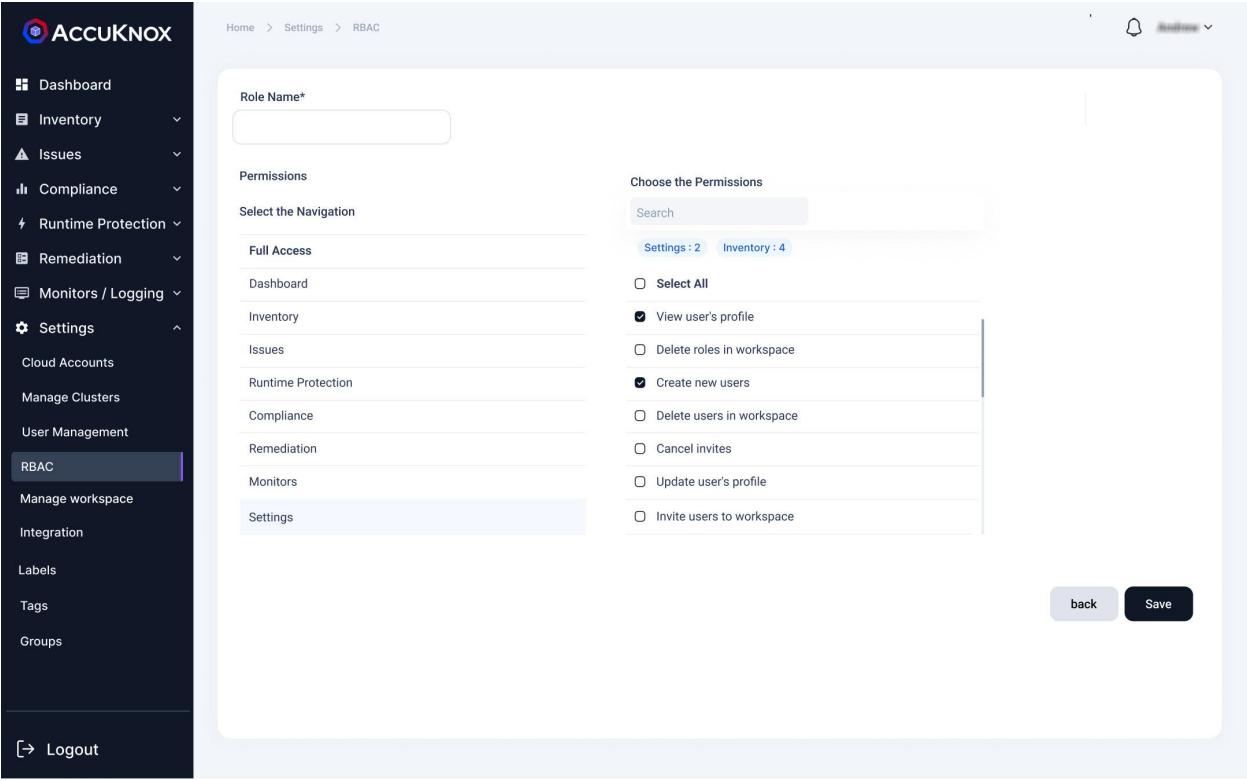
The screenshot shows the MFA setup process. On the left, under 'Setup virtual MFA device', there are three steps: 1. Install a Authenticator app on your mobile or computer (example: Google Authenticator App), 2. Use your virtual MFA app and your device camera to scan the QR code, and 3. Enter the MFA code. A large QR code is displayed. An alternative secret key is provided: V16HDS3KJDOWKSSL. On the right, under 'Enter MFA Code', it says 'You need to have an Authentication App to authorise and Proceed Safely'. There is a 'Enter Code' input field labeled 'Two-factor authentication code', a 'Login' button, and a note 'Last updated 3 Days ago'.

Step 7: After successful login, the user will be directed to the Dashboard screen.



Assign RBAC

The role-Based Access Control option gives the option of creating users with different roles. we can create and manage roles that will be assigned to user profiles for their authorization. Users can select a set of permissions for each role like access to the Dashboard, Inventory, Issues, Runtime Protection, Compliance, Remediation, Monitors, and Settings. Roles can be created by clicking add roles or by cloning the existing roles. Roles are of two types, default roles come prebuilt and cannot be edited or deleted, and all other roles are custom roles.



Role Name*

Permissions

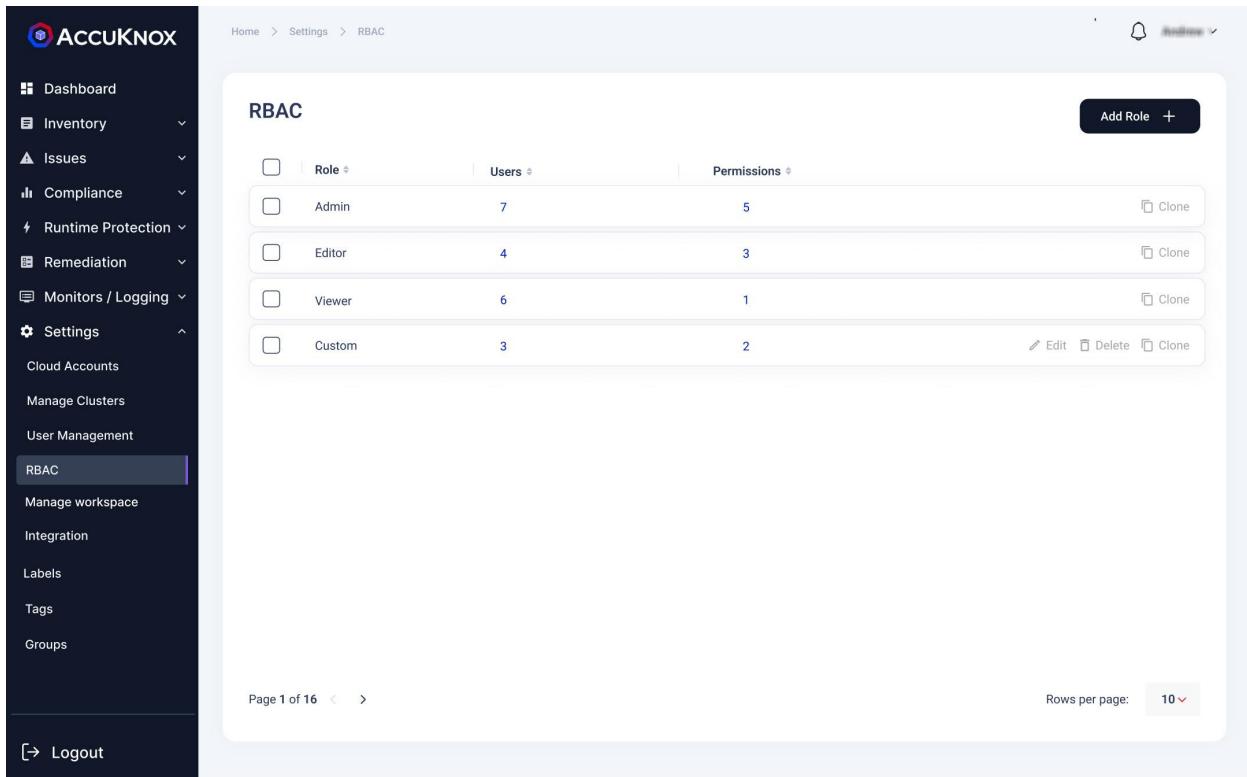
Select the Navigation

Full Access	Choose the Permissions
Dashboard	<input type="checkbox"/> Select All
Inventory	<input checked="" type="checkbox"/> View user's profile
Issues	<input type="checkbox"/> Delete roles in workspace
Runtime Protection	<input checked="" type="checkbox"/> Create new users
Compliance	<input type="checkbox"/> Delete users in workspace
Remediation	<input type="checkbox"/> Cancel invites
Monitors	<input type="checkbox"/> Update user's profile
Settings	<input type="checkbox"/> Invite users to workspace

Search

Settings : 2 Inventory : 4

back Save



The screenshot shows the ACCUKNOX interface with the RBAC module selected. The left sidebar includes categories like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Logging, Settings (selected), Cloud Accounts, Manage Clusters, User Management, RBAC (selected), Manage workspace, Integration, Labels, Tags, and Groups. At the bottom of the sidebar is a Logout button. The main content area is titled 'RBAC' and displays a table of roles:

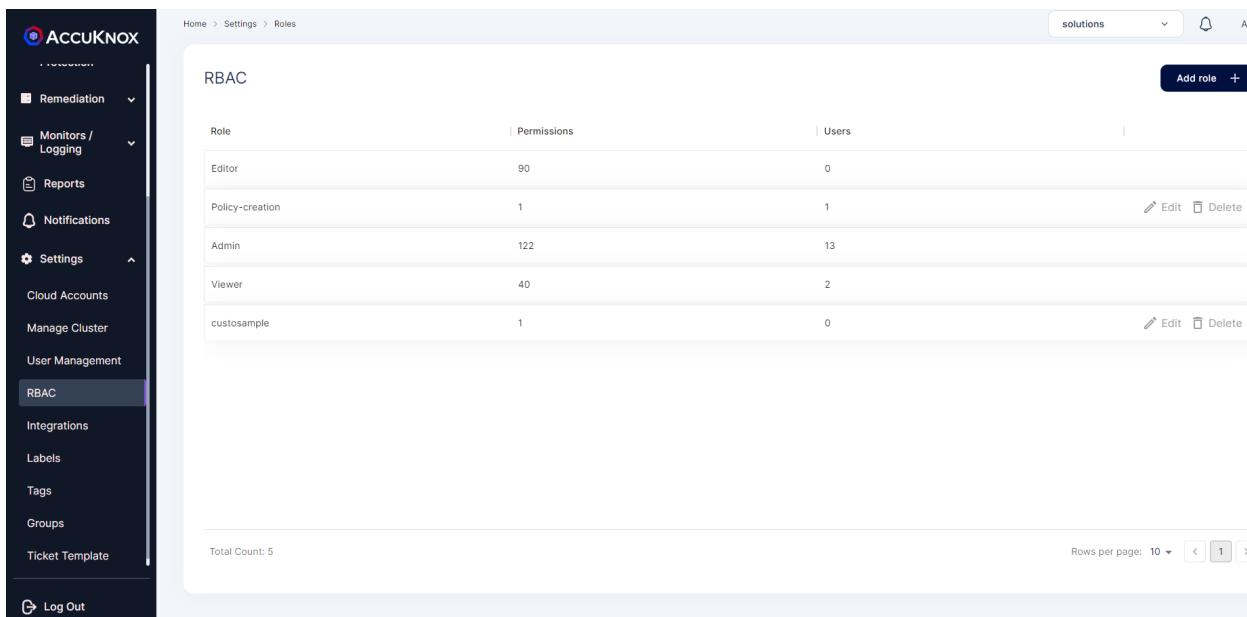
Role	Users	Permissions	Actions
Admin	7	5	<input type="checkbox"/> Clone
Editor	4	3	<input type="checkbox"/> Clone
Viewer	6	1	<input type="checkbox"/> Clone
Custom	3	2	<input type="checkbox"/> Edit <input type="checkbox"/> Delete <input type="checkbox"/> Clone

At the bottom of the page, there are navigation links for 'Page 1 of 16' and 'Rows per page: 10'.

Create Roles and Assign Users

Steps:

- Click on Add Role

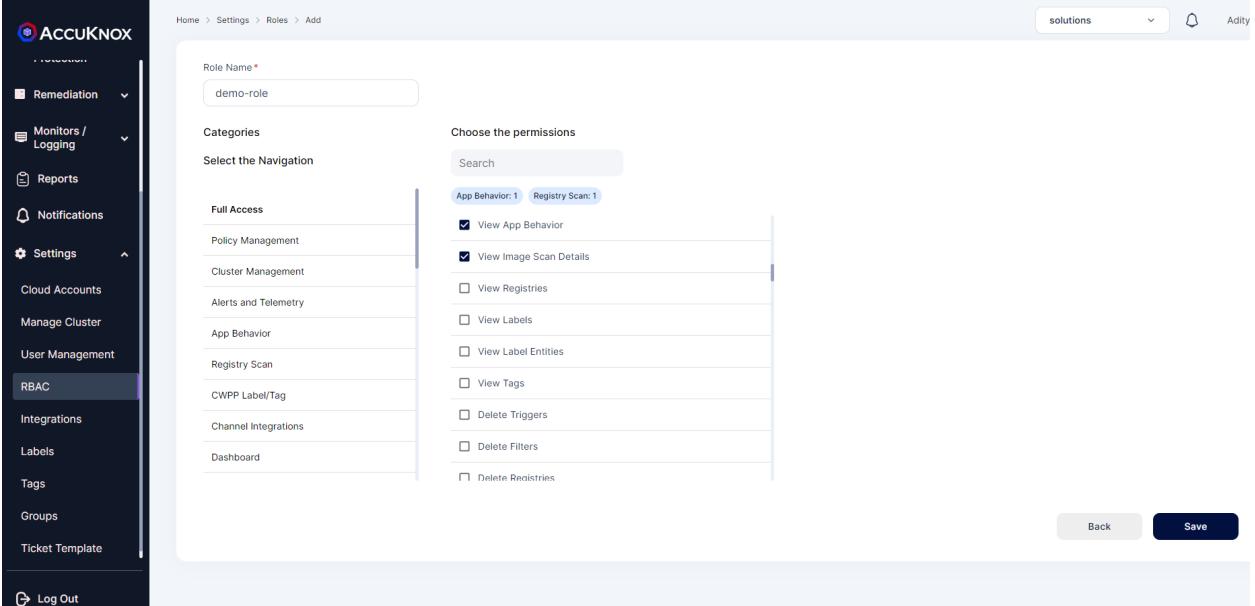


The screenshot shows the ACCUKNOX interface with the RBAC module selected. The left sidebar includes categories like Remediation, Monitors / Logging, Reports, Notifications, Settings (selected), Cloud Accounts, Manage Cluster, User Management, RBAC (selected), Integrations, Labels, Tags, Groups, and Ticket Template. At the bottom of the sidebar is a Log Out button. The main content area is titled 'RBAC' and displays a table of roles:

Role	Permissions	Users	Actions
Editor	90	0	<input type="checkbox"/> Edit <input type="checkbox"/> Delete
Policy-creation	1	1	<input type="checkbox"/> Edit <input type="checkbox"/> Delete
Admin	122	13	<input type="checkbox"/> Edit <input type="checkbox"/> Delete
Viewer	40	2	<input type="checkbox"/> Edit <input type="checkbox"/> Delete
custosample	1	0	<input type="checkbox"/> Edit <input type="checkbox"/> Delete

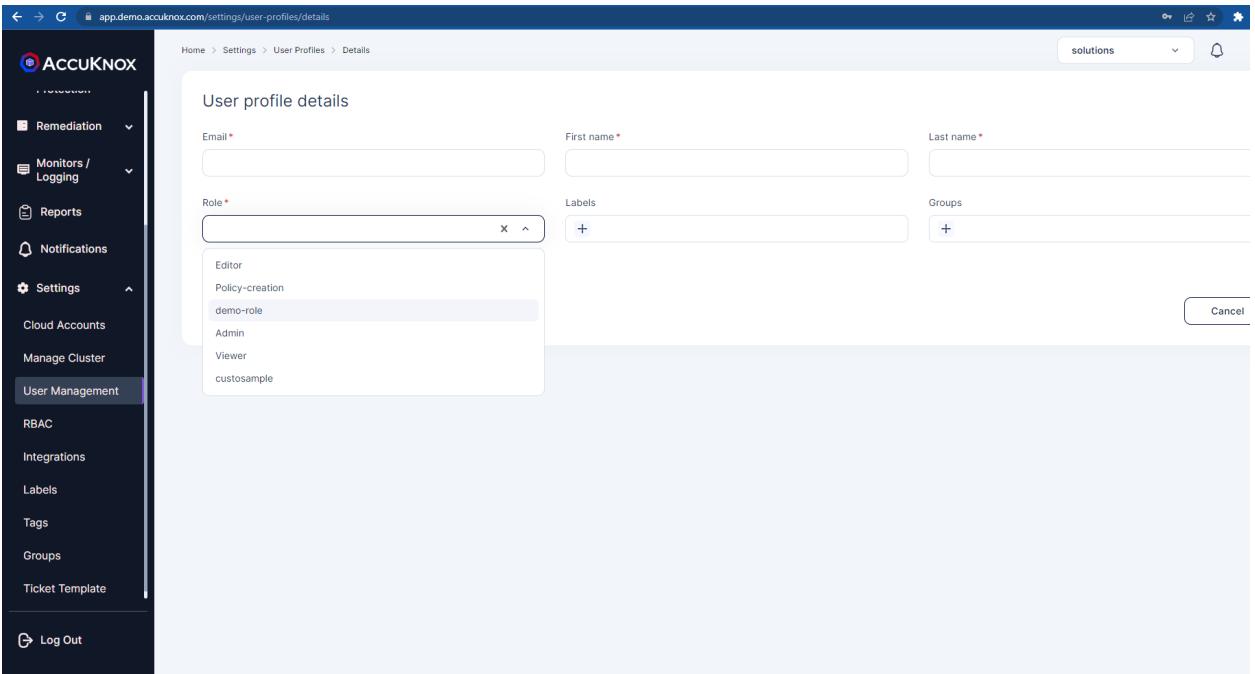
At the bottom of the page, there is a 'Total Count: 5' message and a 'Rows per page: 10' dropdown.

- Enter the name for Role along with it specify the role permission



The screenshot shows the 'Add' role creation page in the ACCUKNOX interface. The left sidebar is the navigation menu with 'RBAC' selected. The main form has a 'Role Name' field containing 'demo-role'. Under 'Categories', 'Full Access' is selected. In the 'Choose the permissions' section, several checkboxes are checked under 'App Behavior' and 'Registry Scan'. At the bottom right are 'Back' and 'Save' buttons.

- Click on Save
- Navigate to User Management > Add User > Choose the role created
- Send the send to the new user with custom role and permission



The screenshot shows the 'User profile details' page for a new user. The left sidebar is the navigation menu with 'User Management' selected. The main form includes fields for 'Email', 'First name', 'Last name', 'Role' (with 'demo-role' selected), 'Labels', and 'Groups'. A 'Cancel' button is at the bottom right. The browser address bar shows the URL: app.demo.accurknox.com/settings/user-profiles/details.