AccuKnox

User Manual – Getting Started Guide

July 25, 2023

Table of Contents

Getting Started Guide

CSPM Prerequisites

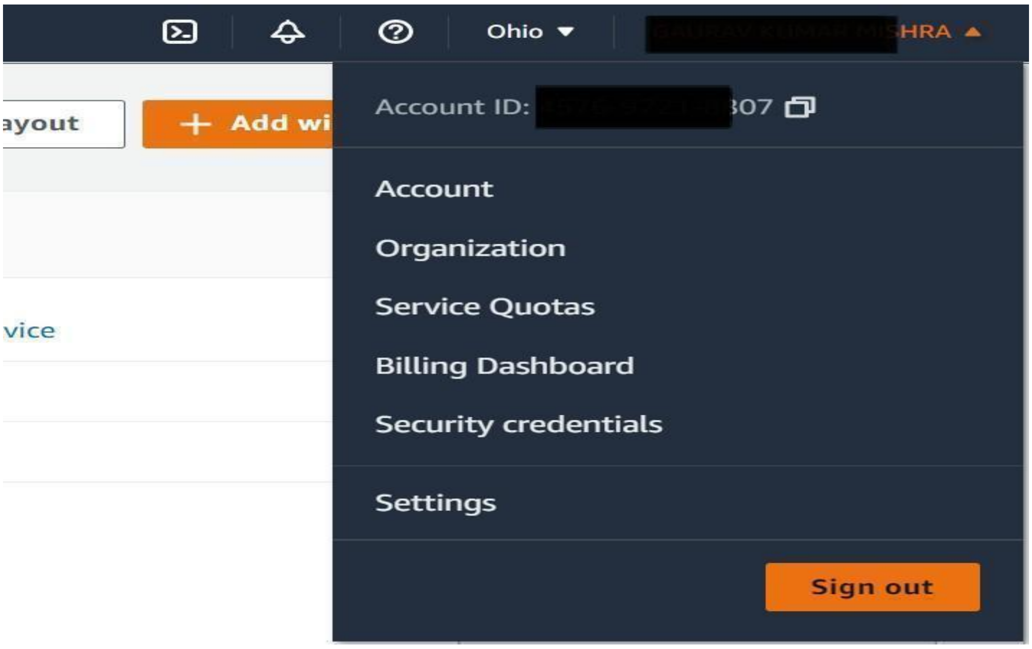
Cloud Account Onboarding

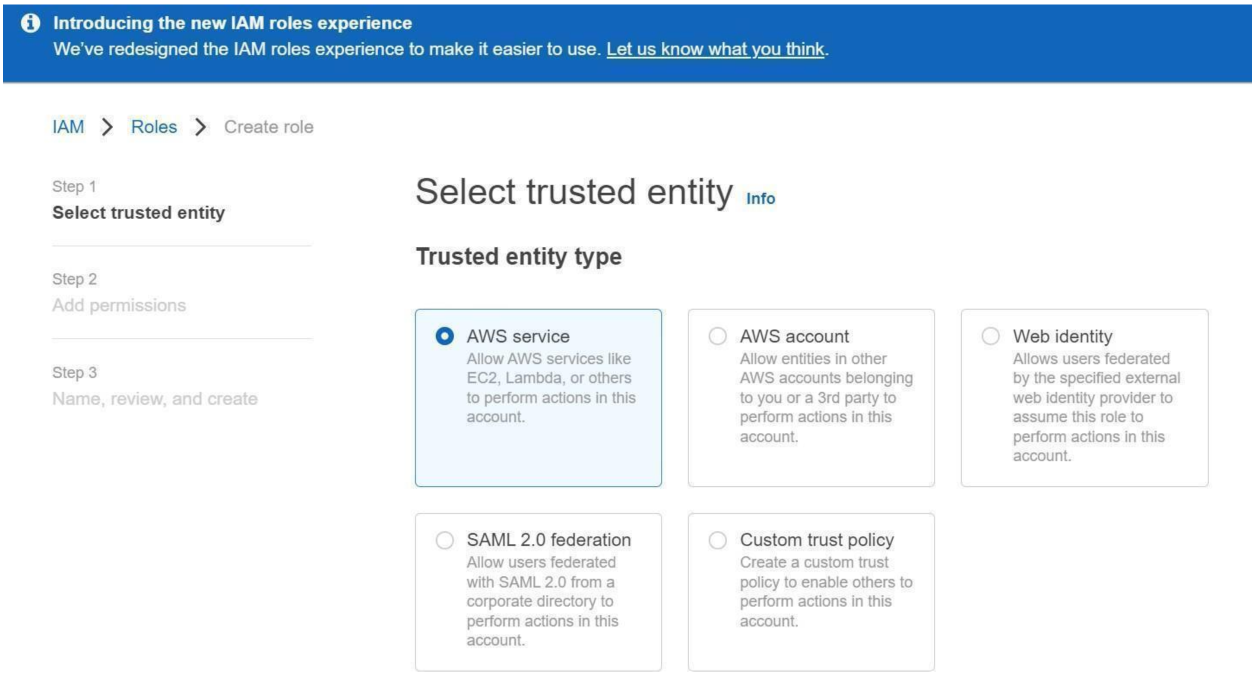
AWS

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”





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.

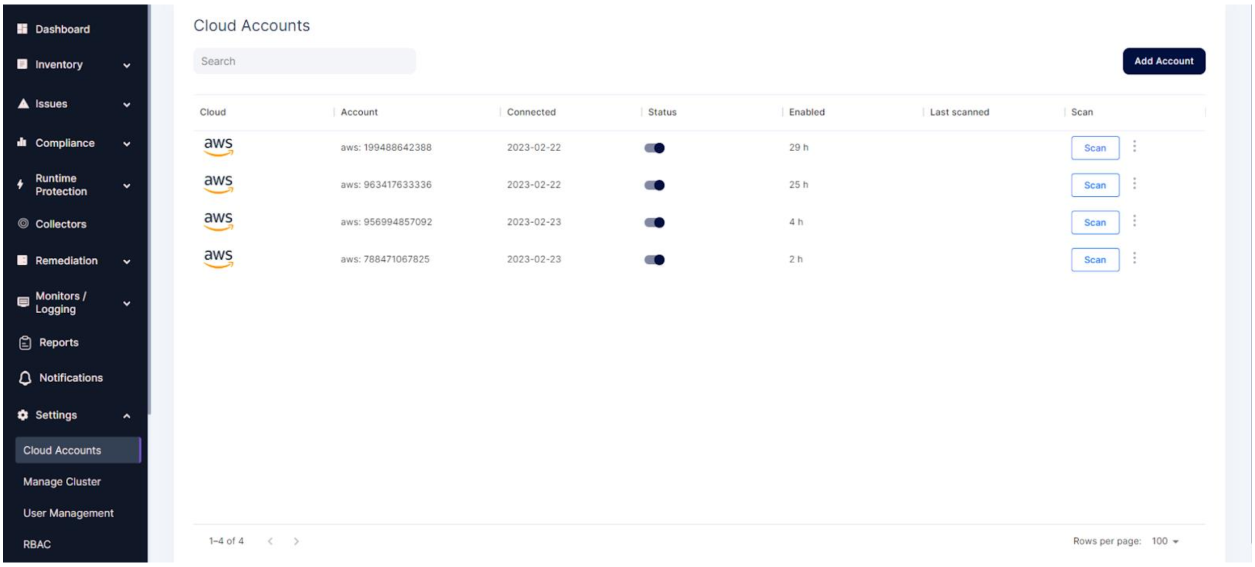
○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ 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 Key Method)

- Click settings -> Cloud Accounts
- Click Add account



Cloud Accounts

Search

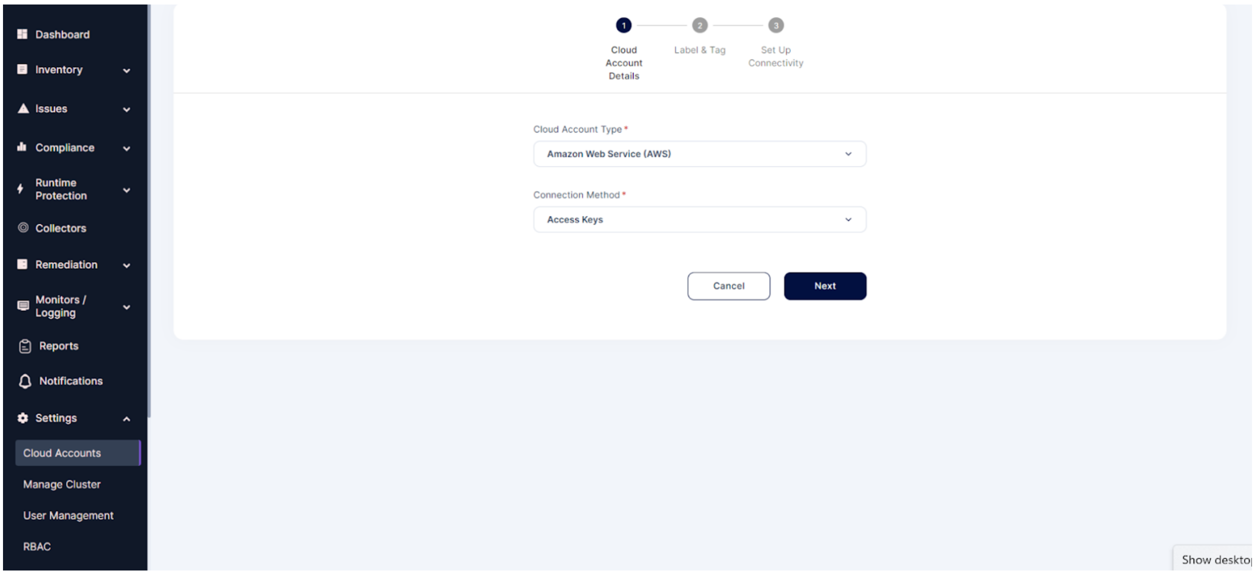
Add Account

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

1–4 of 4

Rows per page: 100

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

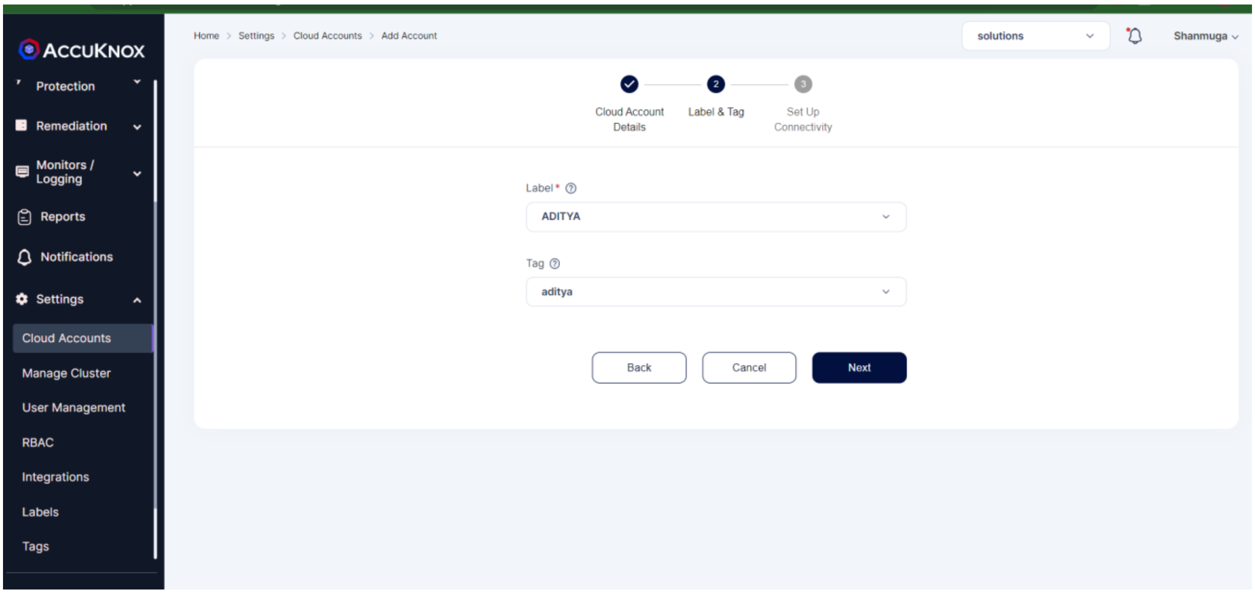


Cloud Account Type *: Amazon Web Service (AWS)

Connection Method *: Access Keys

- Select the Labels and Tags

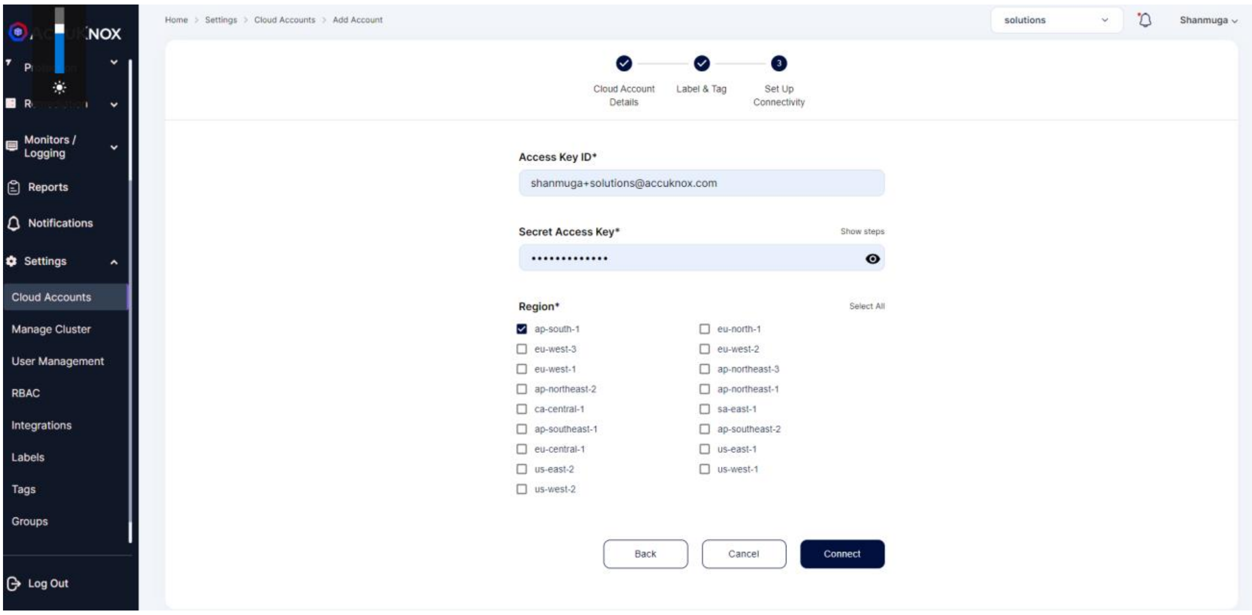
Note: If there are no labels and tags create new labels and tags via the settings



Label *: ADITYA

Tag: aditya

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



Access Key ID*
shanmuga+solutions@accuknox.com

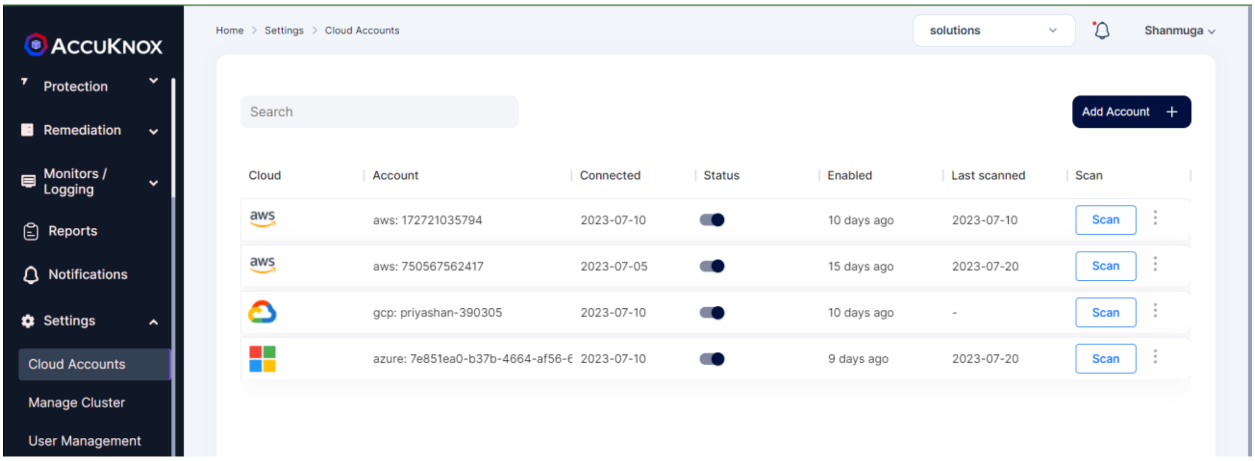
Secret Access Key* (Show steps)
•••••••••••••

Region* (Select All)

☑ ap-south-1
☐ eu-west-3
☐ eu-west-1
☐ ap-northeast-2
☐ ca-central-1
☐ ap-southeast-1
☐ eu-central-1
☐ us-east-2
☐ us-west-2
☐ eu-north-1
☐ eu-west-2
☐ ap-northeast-3
☐ ap-northeast-1
☐ sa-east-1
☐ ap-southeast-2
☐ us-east-1
☐ us-west-1

- 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.

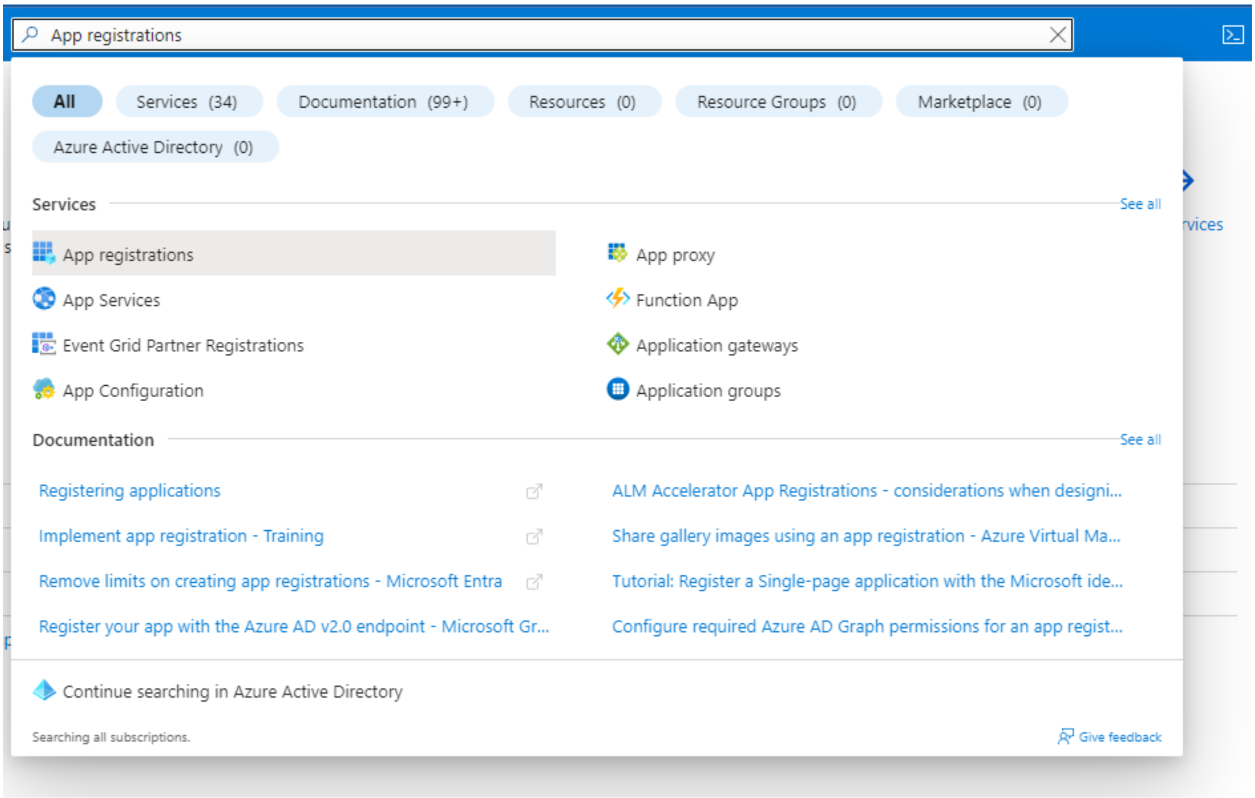


Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	●	10 days ago	2023-07-10	Scan
aws	aws: 750567562417	2023-07-05	●	15 days ago	2023-07-20	Scan
	gcp: priyashan-390305	2023-07-10	●	10 days ago	-	Scan
	azure: 7e851ea0-b37b-4664-af56-€	2023-07-10	●	9 days ago	2023-07-20	Scan

AZURE

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

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



App registrations

All | Services (34) | Documentation (99+) | Resources (0) | Resource Groups (0) | Marketplace (0) | Azure Active Directory (0)

Services — See all

- App registrations
- App Services
- Event Grid Partner Registrations
- App Configuration
- App proxy
- Function App
- Application gateways
- Application groups

Documentation — See all

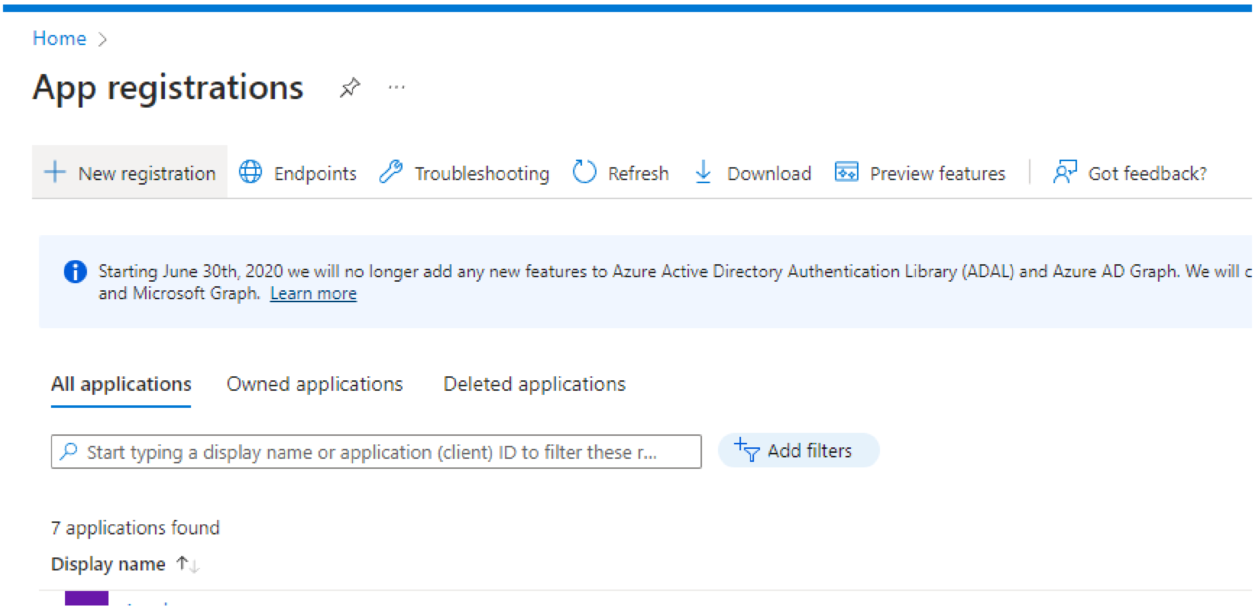
- Registering applications
- Implement app registration - Training
- Remove limits on creating app registrations - Microsoft Entra
- Register your app with the Azure AD v2.0 endpoint - Microsoft Gr...
- ALM Accelerator App Registrations - considerations when designi...
- Share gallery images using an app registration - Azure Virtual Ma...
- Tutorial: Register a Single-page application with the Microsoft ide...
- Configure required Azure AD Graph permissions for an app regist...

Continue searching in Azure Active Directory

Searching all subscriptions.

Give feedback

- 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 c
and Microsoft Graph. Learn more

All applications | Owned applications | Deleted applications

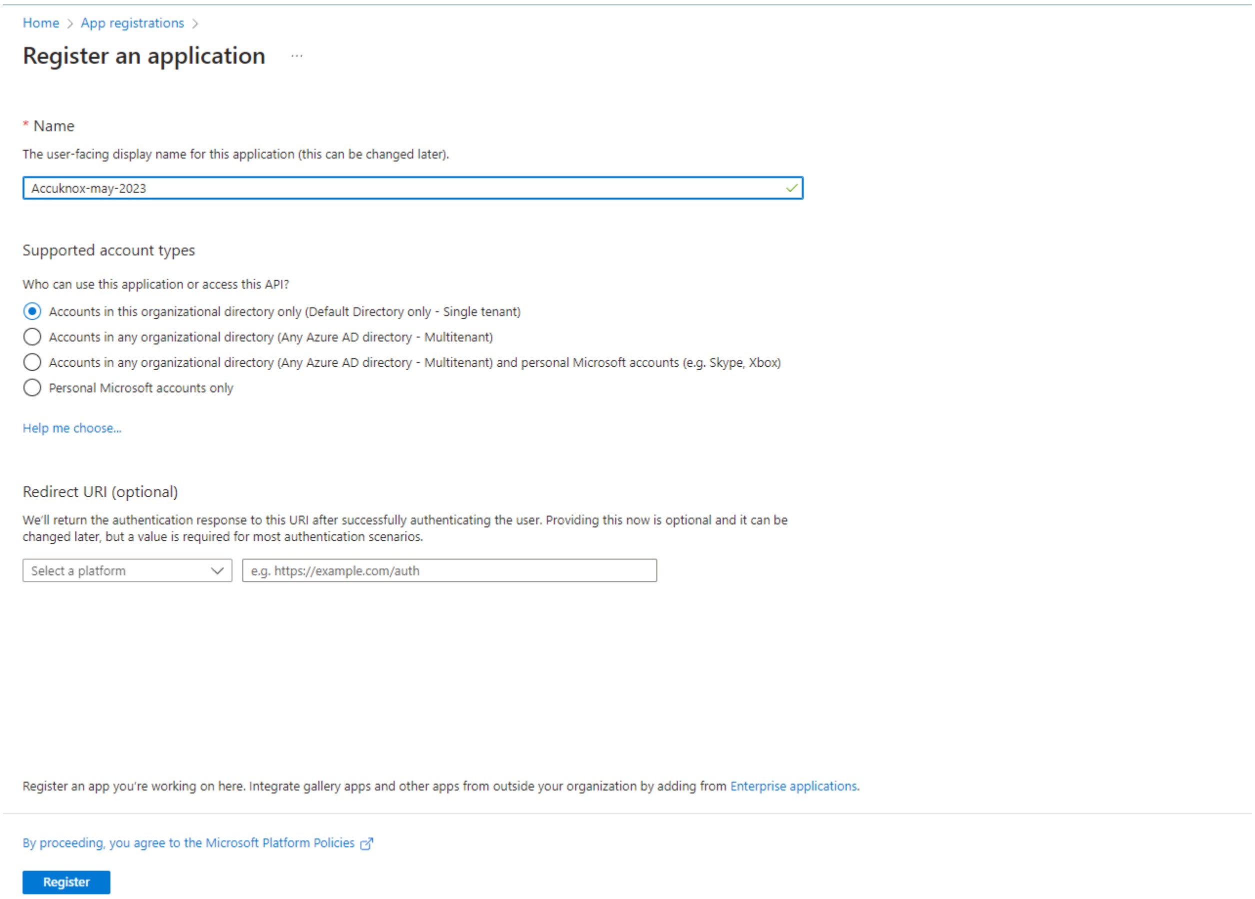
Start typing a display name or application (client) ID to filter these r...

Add filters

7 applications found

Display name ↑↓

- Name your application, 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).

Accuknox-may-2023

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...

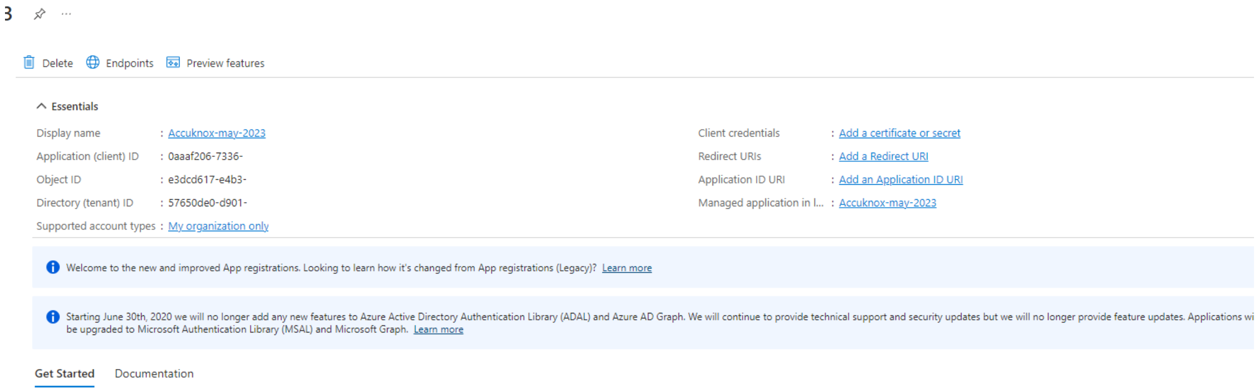
Redirect URI (optional)

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

- 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’

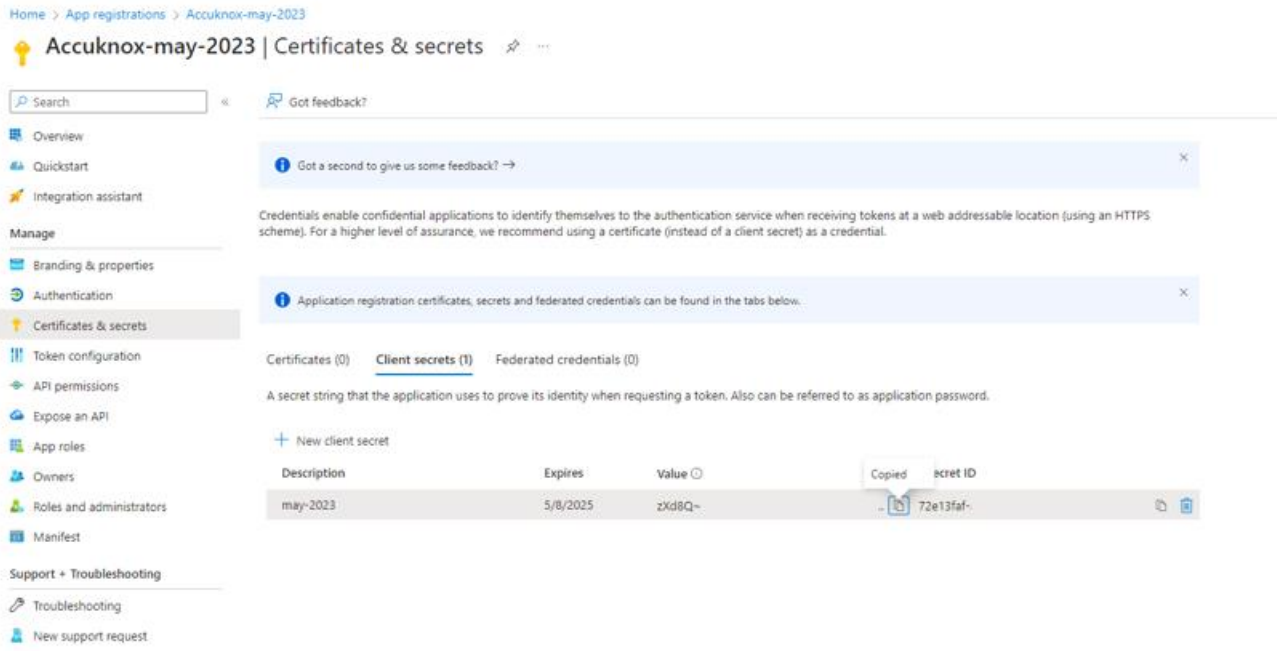


Display name	: Accuknox-may-2023	Client credentials	: Add a certificate or secret
Application (client) ID	: 0aaaf206-7336-	Redirect URIs	: Add a Redirect URI
Object ID	: e3dcd617-e4b3-	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 57650de0-d901-	Managed application in l...	: Accuknox-may-2023
Supported account types	: My organization only		

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 wi be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

- 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.



Home > App registrations > Accuknox-may-2023

Accuknox-may-2023 | Certificates & secrets

Got feedback?

Got a second to give us some feedback? →

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

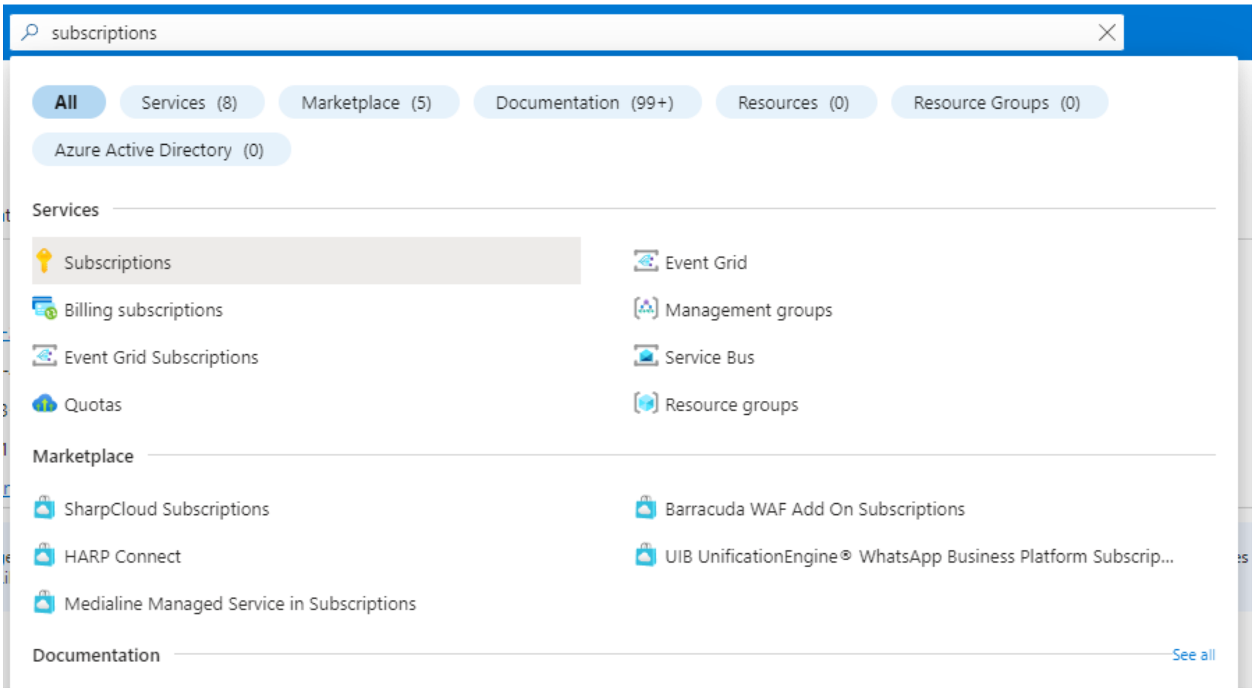
Certificates (0) | Client secrets (1) | Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

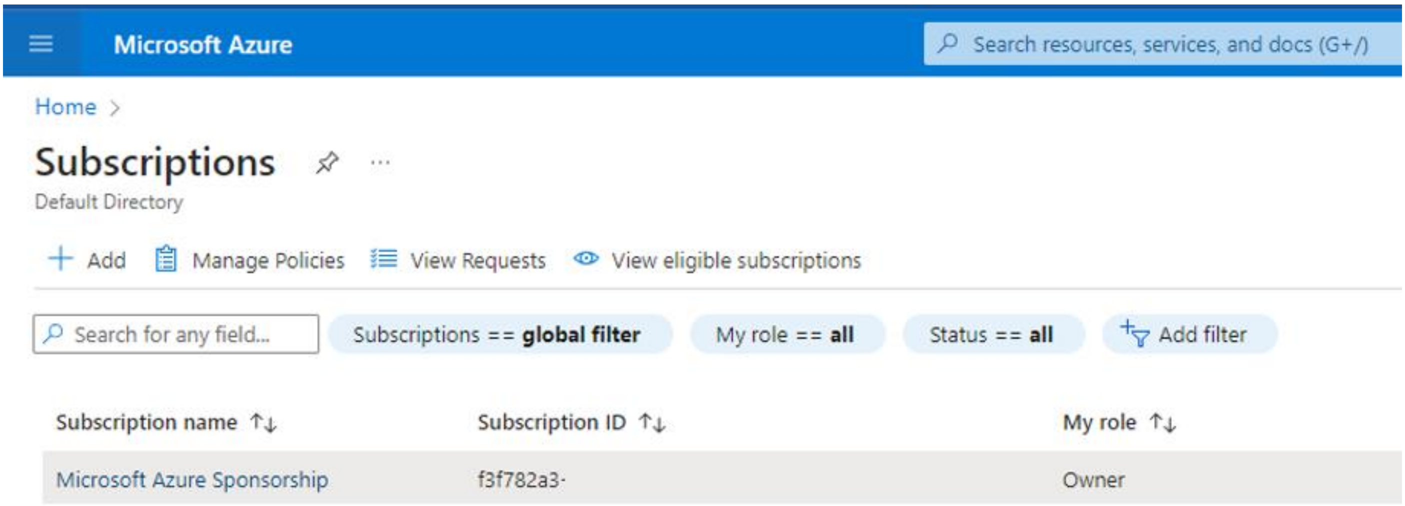
Description	Expires	Value	Secret ID
may-2023	5/8/2025	zXd8Q~	72e13faf-

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



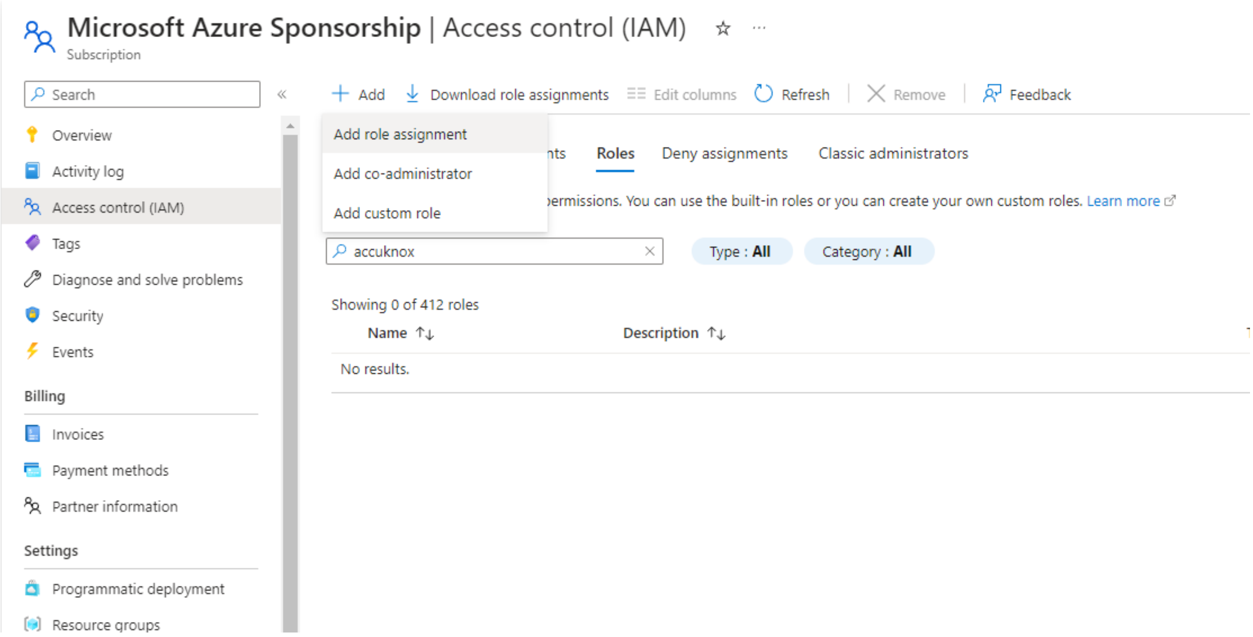
subscriptions

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



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

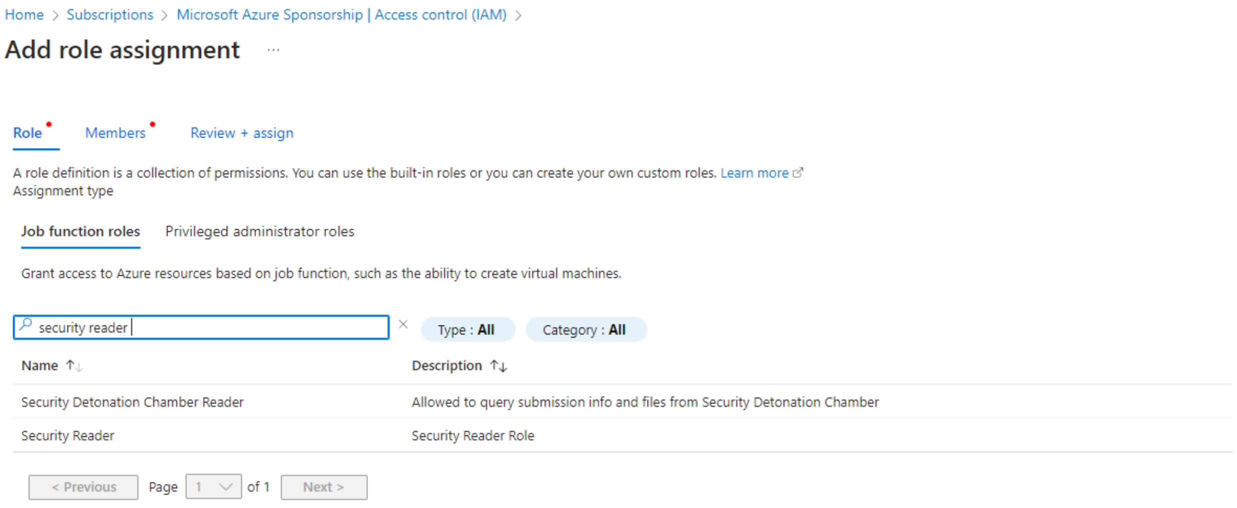


ermissions. You can use the built-in roles or you can create your own custom roles. Learn more

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 ...

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

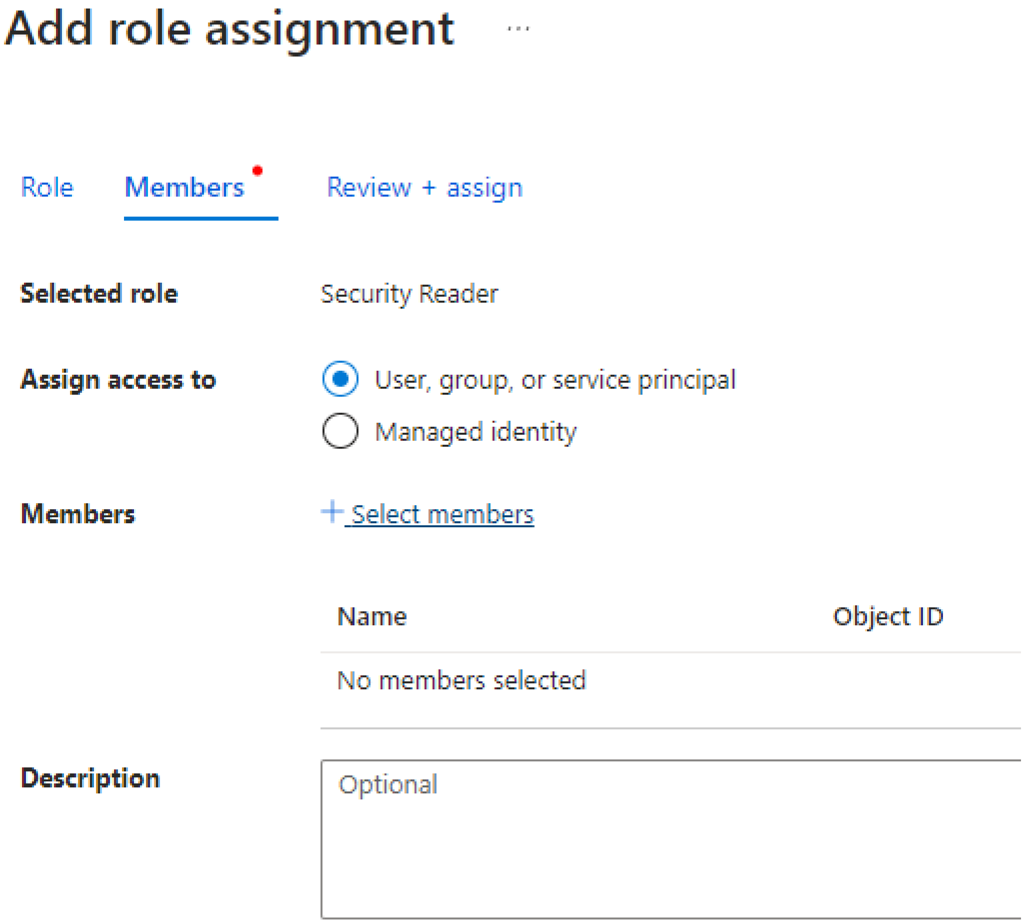
Grant access to Azure resources based on job function, such as the ability to create virtual machines.

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

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



Add role assignment ...

Selected role: Security Reader

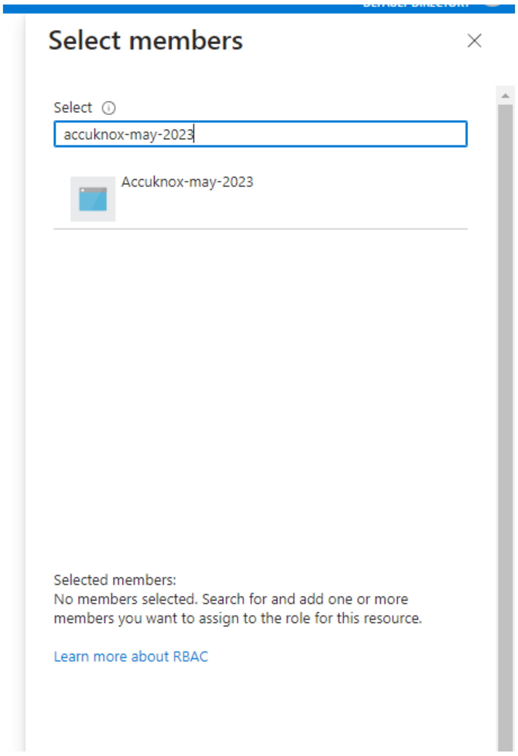
Assign access to: ● User, group, or service principal ○ Managed identity

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.



Select members

Select ⓘ

accuknox-may-2023

Accuknox-may-2023

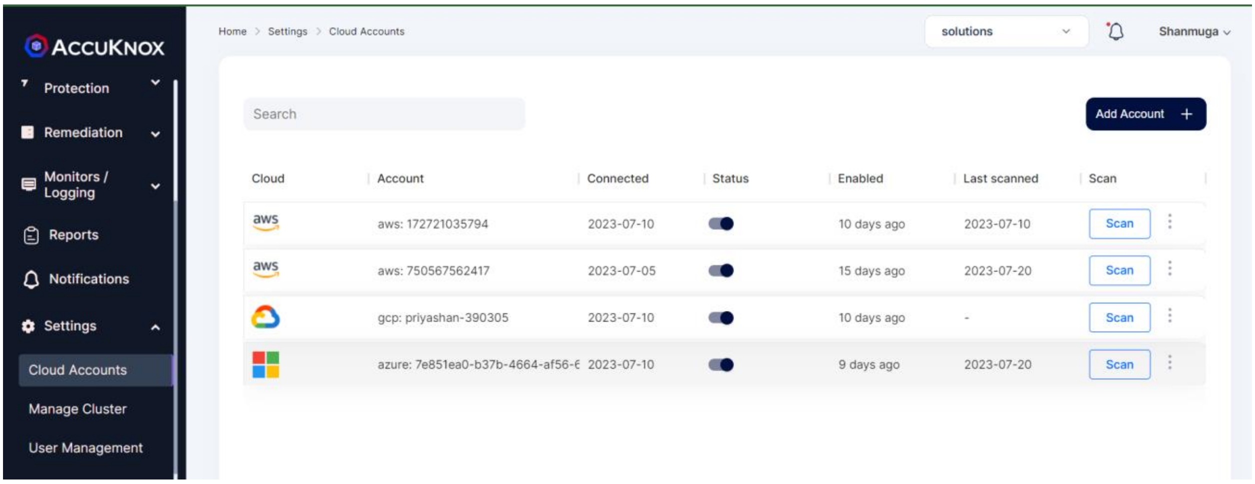
Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

From AccuKnox SaaS UI

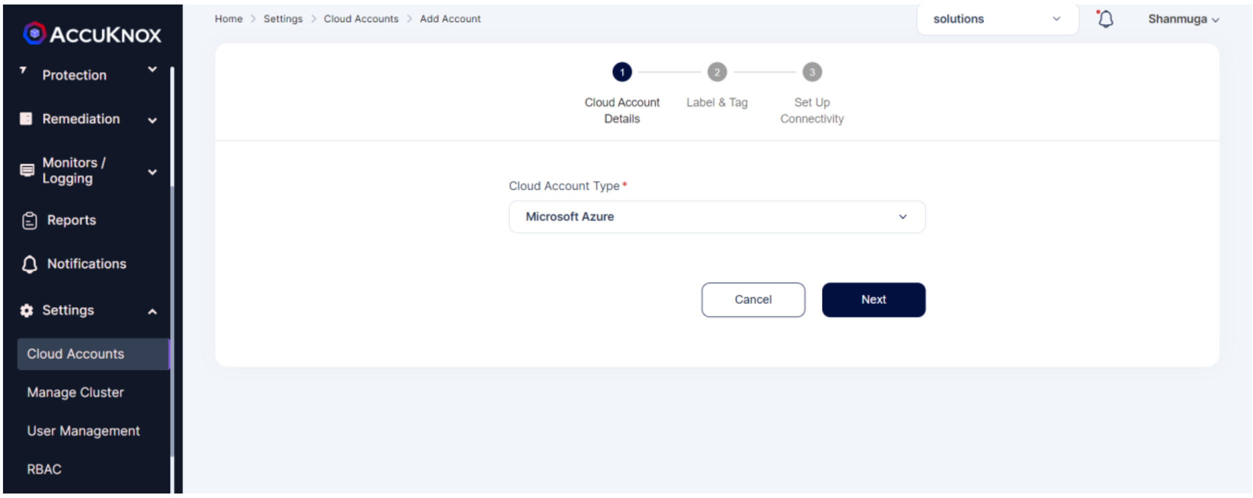
Configuring your Azure cloud account is complete, now we need to onboard the cloud account onto Accuknox Saas Platform.

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



Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	●	10 days ago	2023-07-10	Scan
aws	aws: 750567562417	2023-07-05	●	15 days ago	2023-07-20	Scan
	gcp: priyashan-390305	2023-07-10	●	10 days ago	-	Scan
	azure: 7e851ea0-b37b-4664-af56-€	2023-07-10	●	9 days ago	2023-07-20	Scan

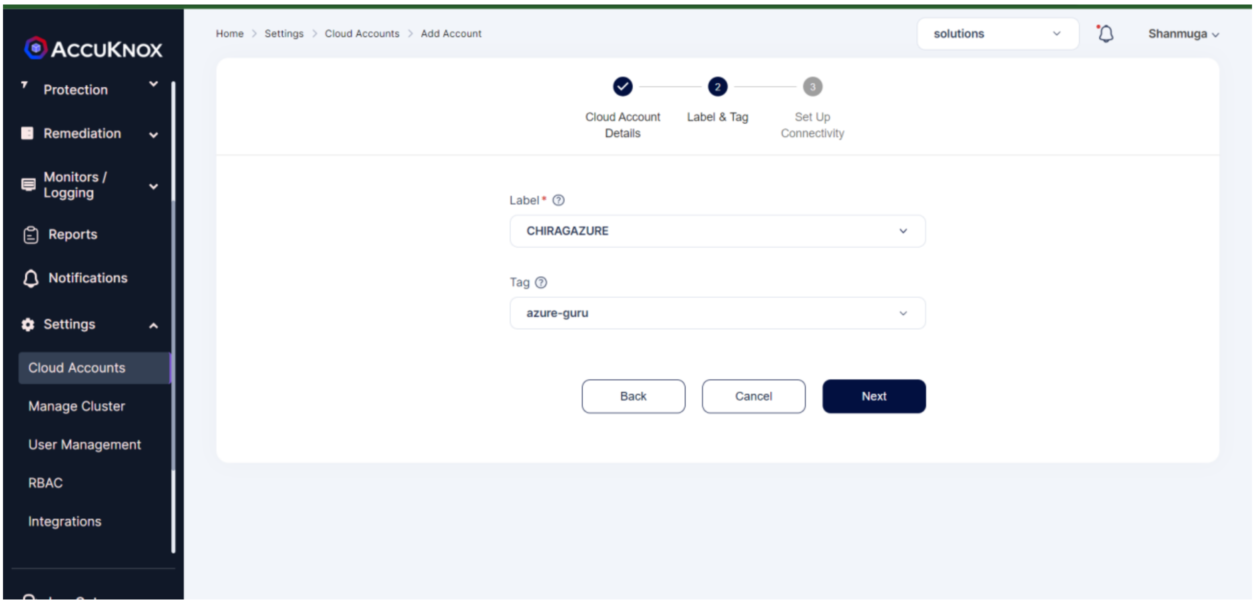
- Select Microsoft Azure as Cloud Account Type and click on next



Cloud Account Type *

Microsoft Azure

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



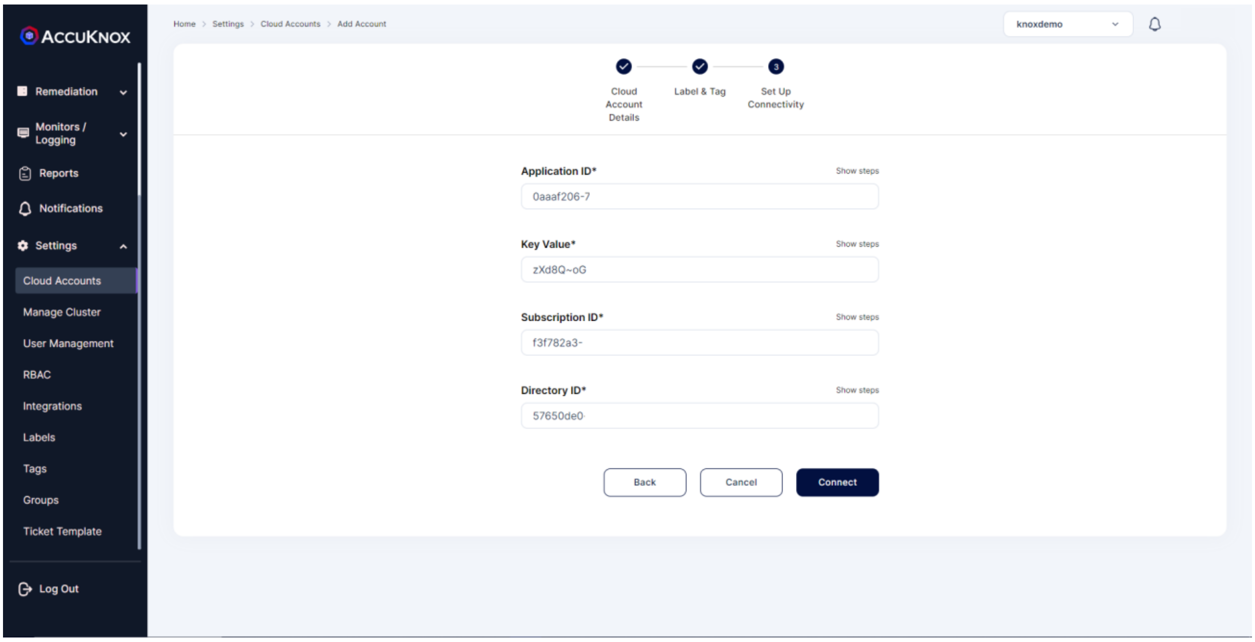
Label *

CHIRAGAZURE

Tag

azure-guru

- 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



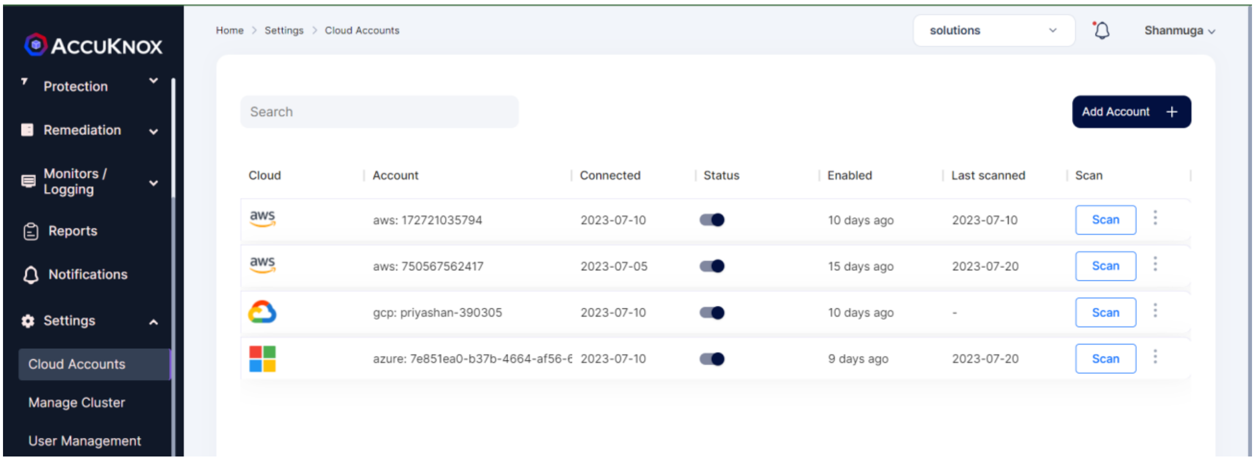
Application ID*: 0aaaf206-7

Key Value*: zXd8Q~oG

Subscription ID*: f3f782a3-

Directory ID*: 57650de0

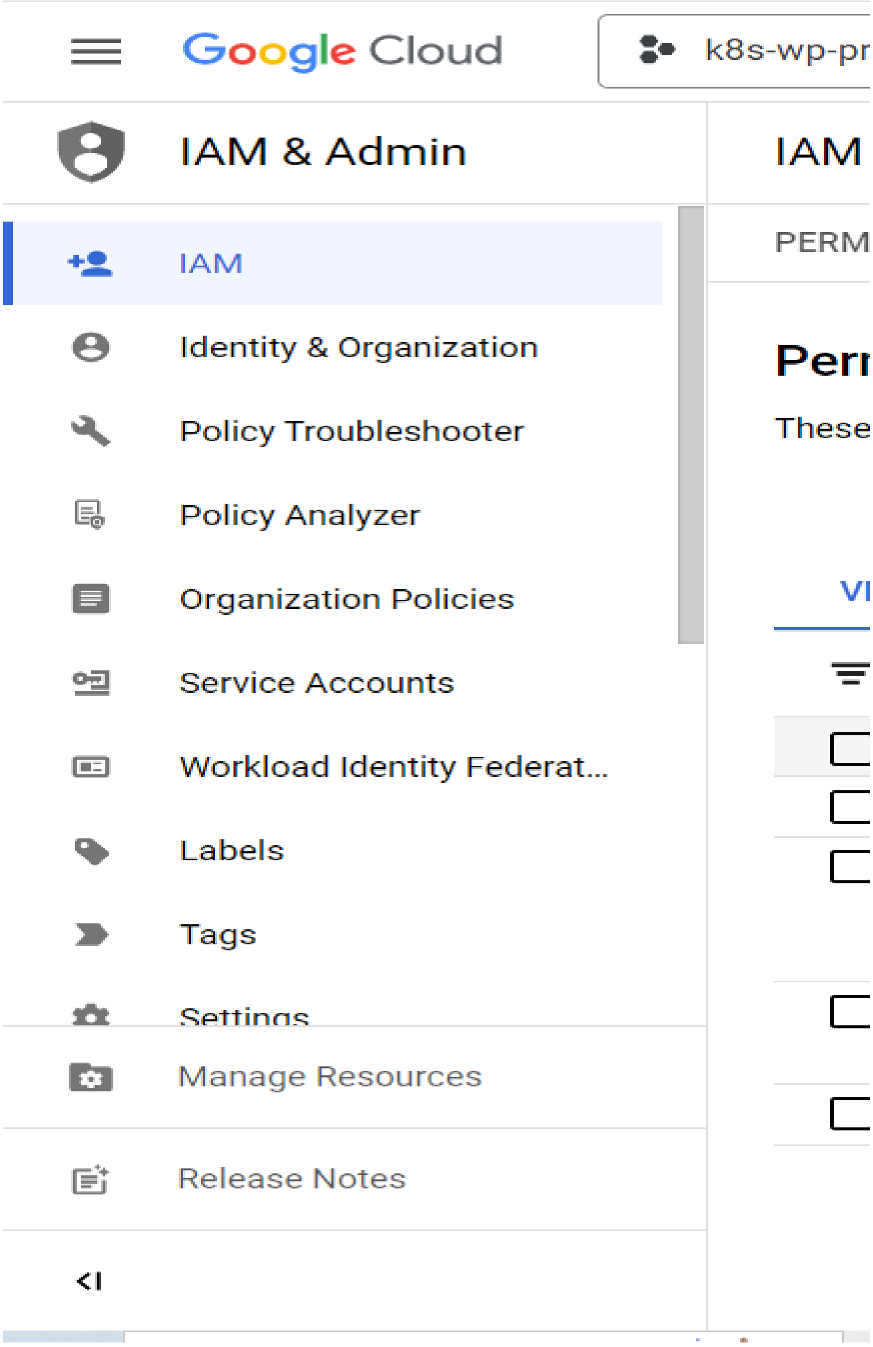
- After successfully connecting your cloud account will show up in the list



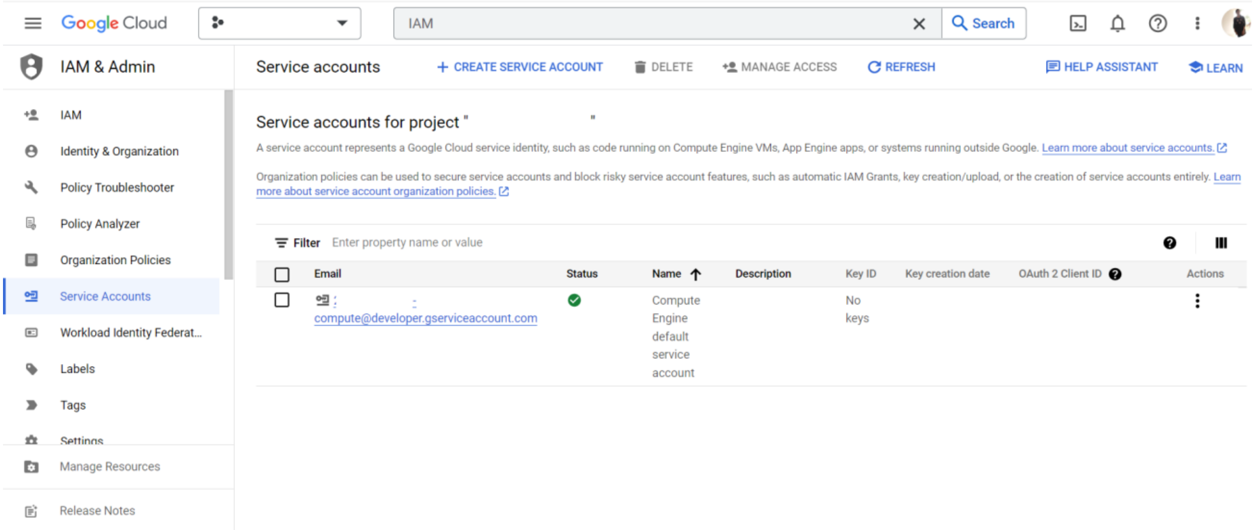
Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	●	10 days ago	2023-07-10	Scan
aws	aws: 750567562417	2023-07-05	●	15 days ago	2023-07-20	Scan
	gcp: priyashan-390305	2023-07-10	●	10 days ago	-	Scan
	azure: 7e851ea0-b37b-4664-af56-6	2023-07-10	●	9 days ago	2023-07-20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

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



- Click on "Create Service Account".



Service accounts for project " "

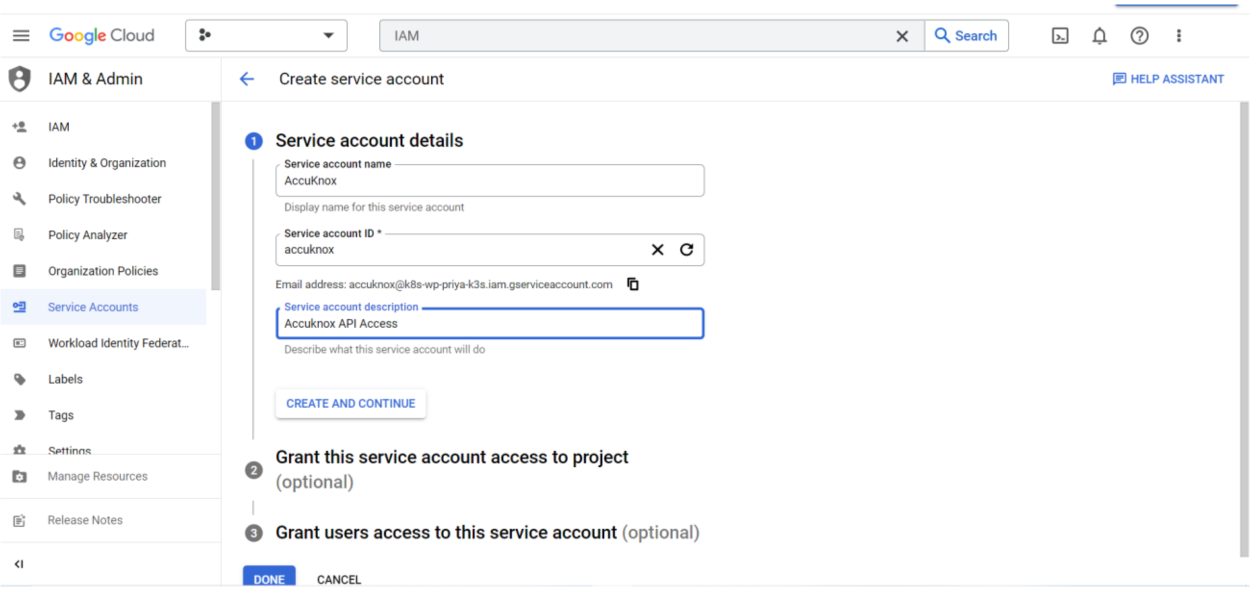
A service account represents a Google Cloud service identity, such as code running on Compute Engine VMs, App Engine apps, or systems running outside Google. Learn more about service accounts.

Organization policies can be used to secure service accounts and block risky service account features, such as automatic IAM Grants, key creation/upload, or the creation of service accounts entirely. Learn more about service account organization policies.

Filter Enter property name or value

□	Email	Status	Name ↑	Description	Key ID	Key creation date	OAuth 2 Client ID	Actions
□	compute@developer.gserviceaccount.com	✓	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.



Create service account

1 Service account details

Service account name: AccuKnox

Display name for this service account

Service account ID *: accuknox

Email address: accuknox@k8s-wp-priya-k3s.iam.gserviceaccount.com

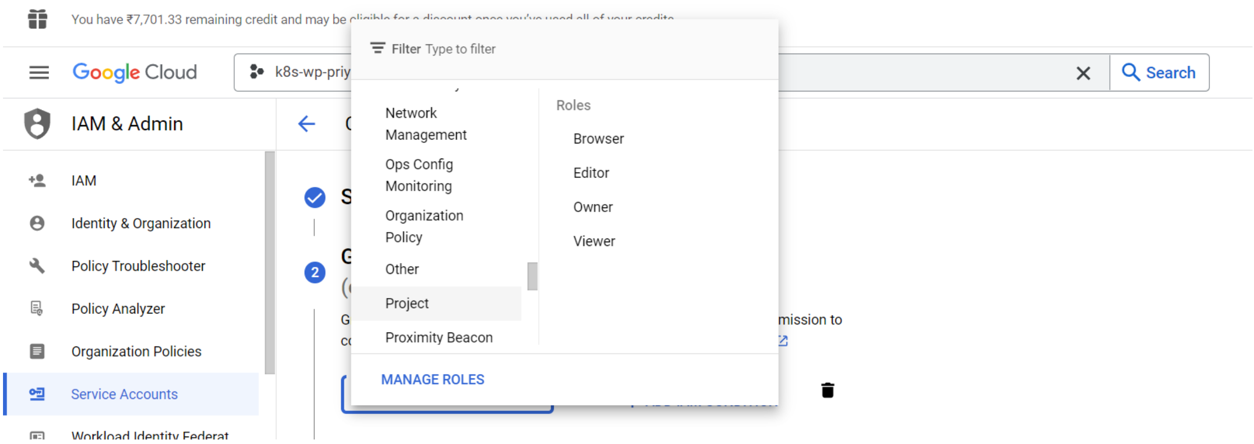
Service account description: Accuknox API Access

Describe what this service account will do

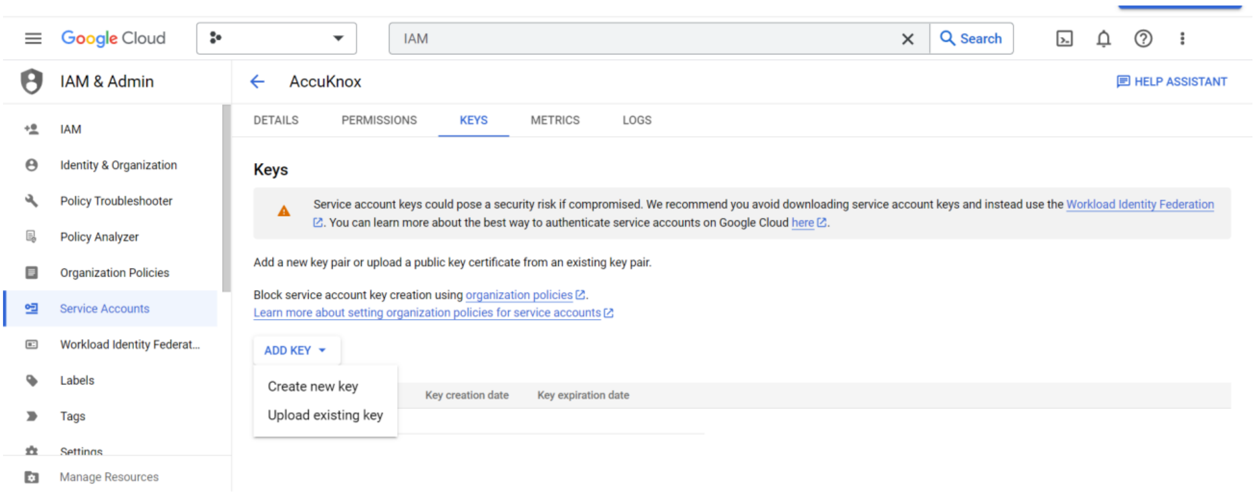
2 Grant this service account access to project (optional)

3 Grant users access to this service account (optional)

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



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



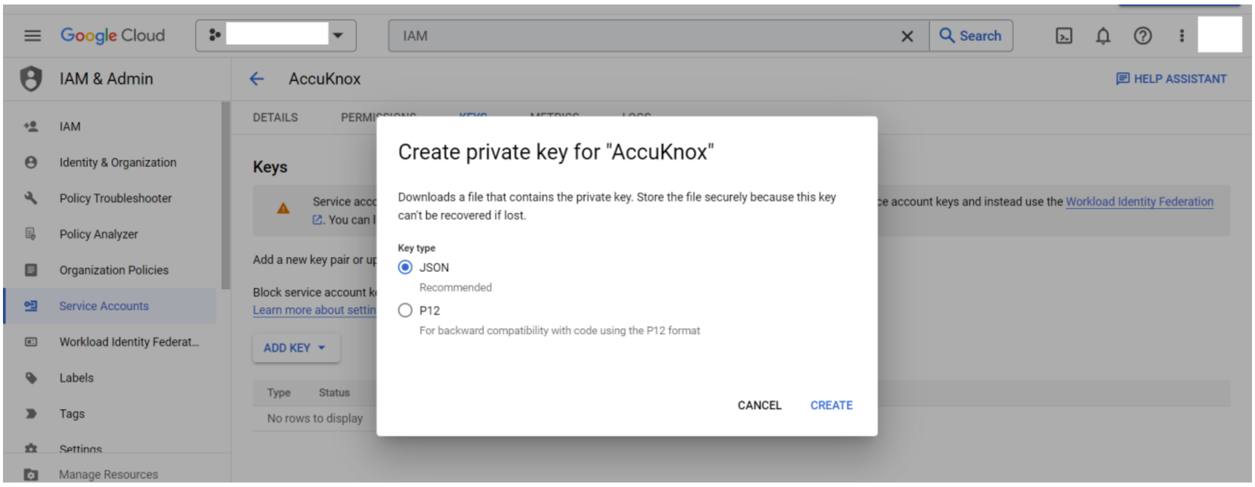
Service account keys could pose a security risk if compromised. We recommend you avoid downloading service account keys and instead use the Workload Identity Federation. You can learn more about the best way to authenticate service accounts on Google Cloud here.

Add a new key pair or upload a public key certificate from an existing key pair.

Block service account key creation using organization policies.
Learn more about setting organization policies for service accounts

- 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.



Service acc… …ce account keys and instead use the Workload Identity Federation
. You can l…

Add a new key pair or up…

Block service account k…
Learn more about settin…

No rows to display

Create private key for "AccuKnox"

Downloads a file that contains the private key. Store the file securely because this key can't be recovered if lost.

Key type

● JSON
Recommended

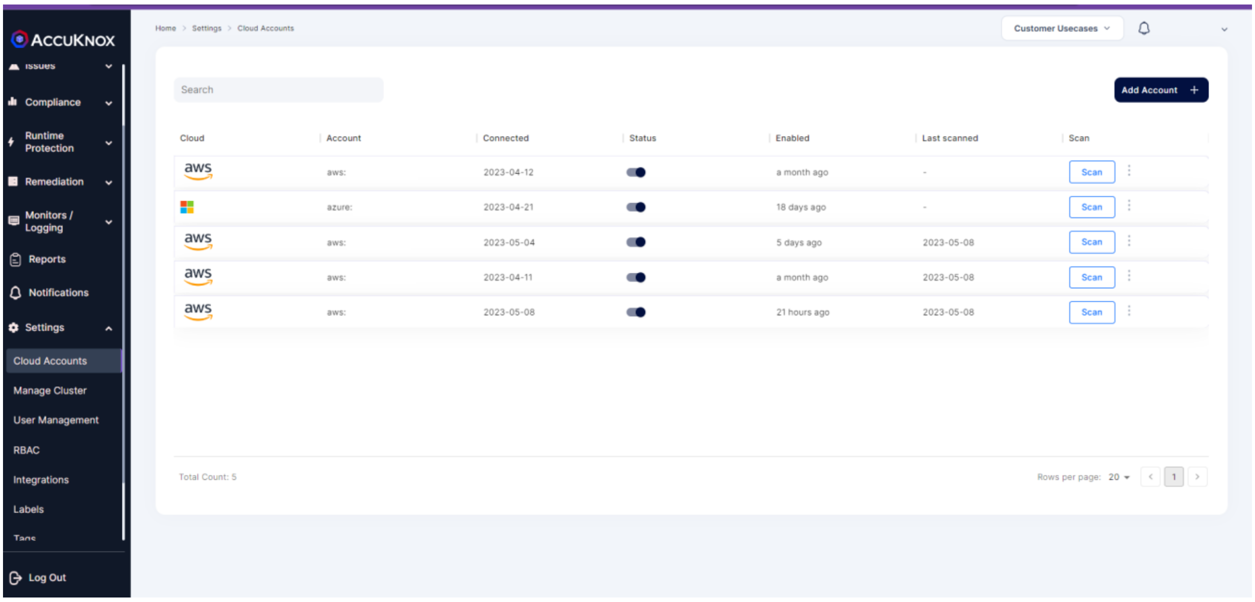
○ P12
For backward compatibility with code using the P12 format

CANCEL CREATE

2. From AccuKnox SaaS UI

- Click settings -> Cloud Accounts

Click Add account

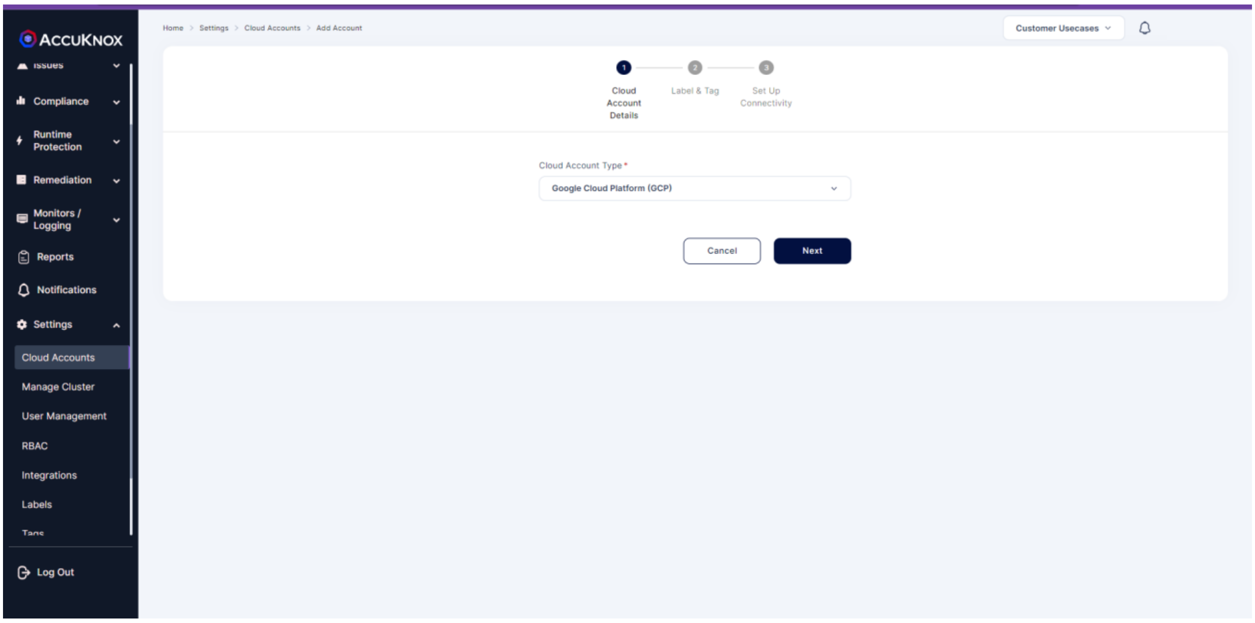


Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws:	2023-04-12	●	a month ago	-	Scan
	azure:	2023-04-21	●	18 days ago	-	Scan
aws	aws:	2023-05-04	●	5 days ago	2023-05-08	Scan
aws	aws:	2023-04-11	●	a month ago	2023-05-08	Scan
aws	aws:	2023-05-08	●	21 hours ago	2023-05-08	Scan

Total Count: 5

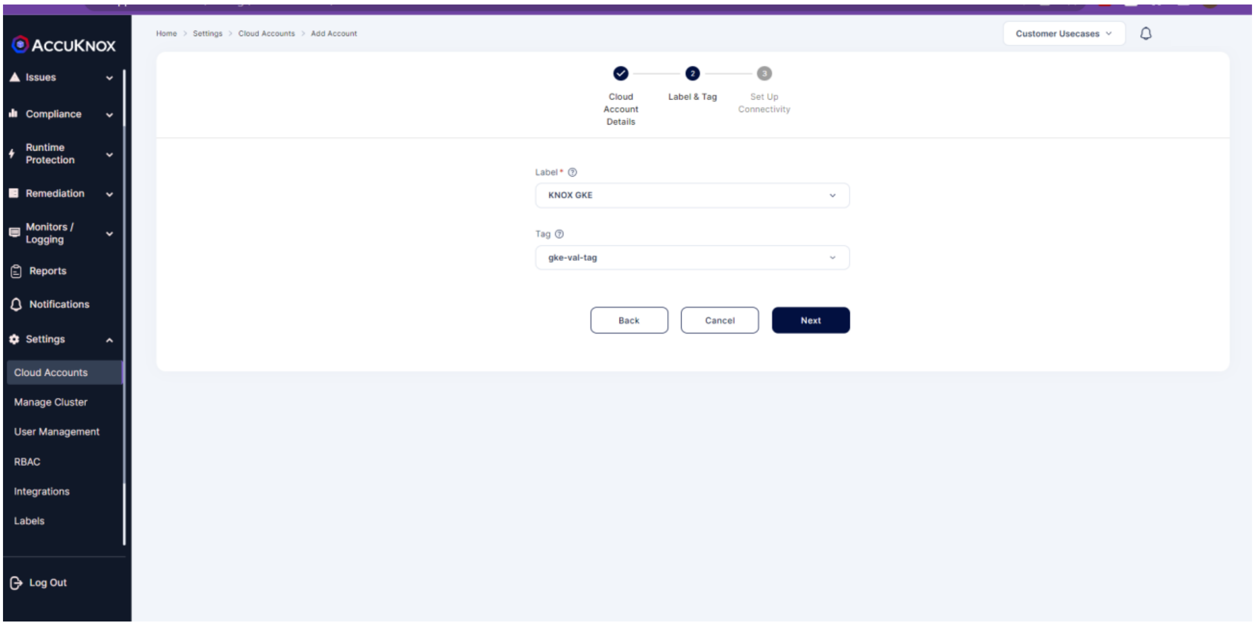
Rows per page: 20 1

- Select the Cloud Account type to GCP and Click Next



Cloud Account Type *
Google Cloud Platform (GCP)

- Select the Labels and Tags and click Next

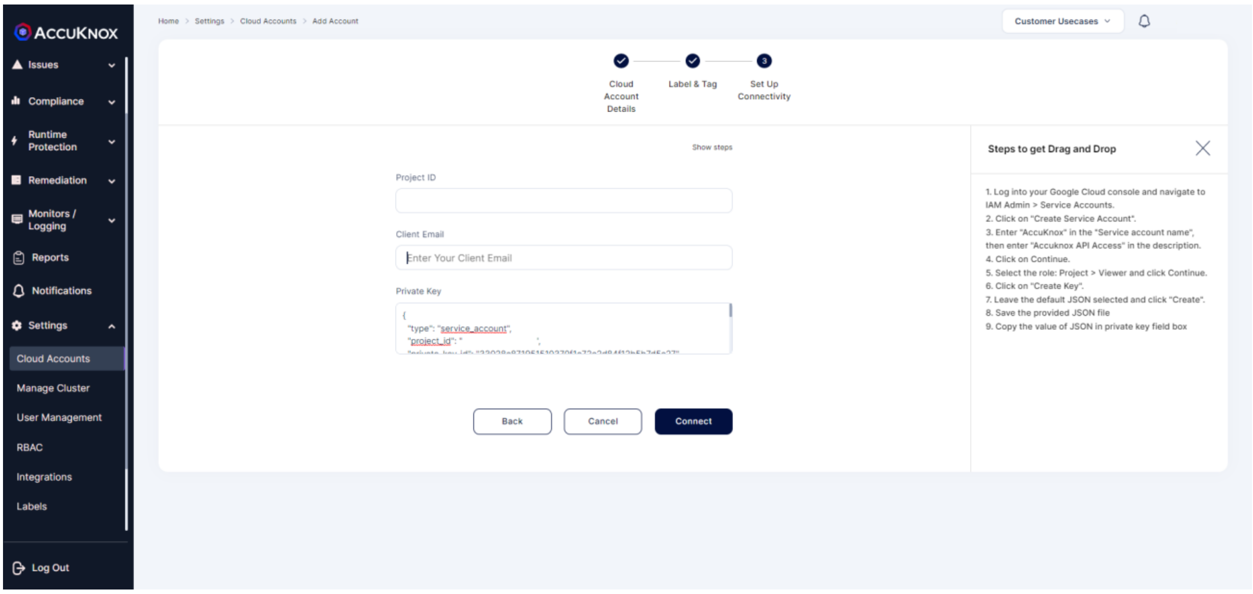


Label *
KNOX GKE

Tag
gke-val-tag

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

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



Project ID

Client Email: Enter Your Client Email

Private Key

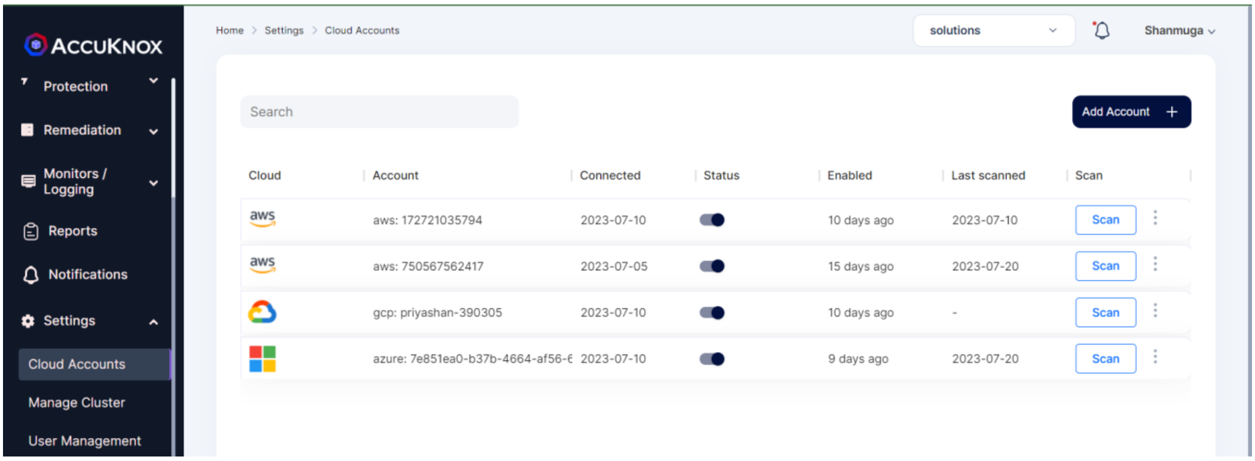
```
{
  "type": "service_account",
  "project_id": "                     ",
```

Steps to get Drag and Drop

1. Log into your Google Cloud console and navigate to IAM Admin > Service Accounts.
2. Click on "Create Service Account".
3. Enter "AccuKnox" in the "Service account name", then enter "Accuknox API Access" in the description.
4. Click on Continue.
5. Select the role: Project > Viewer and click Continue.
6. Click on "Create Key".
7. Leave the default JSON selected and click "Create".
8. Save the provided JSON file
9. Copy the value of JSON in private key field box

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.



Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 172721035794	2023-07-10	●	10 days ago	2023-07-10	Scan
aws	aws: 750567562417	2023-07-05	●	15 days ago	2023-07-20	Scan
	gcp: priyashan-390305	2023-07-10	●	10 days ago	-	Scan
	azure: 7e851ea0-b37b-4664-af56-€	2023-07-10	●	9 days ago	2023-07-20	Scan

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	-	-

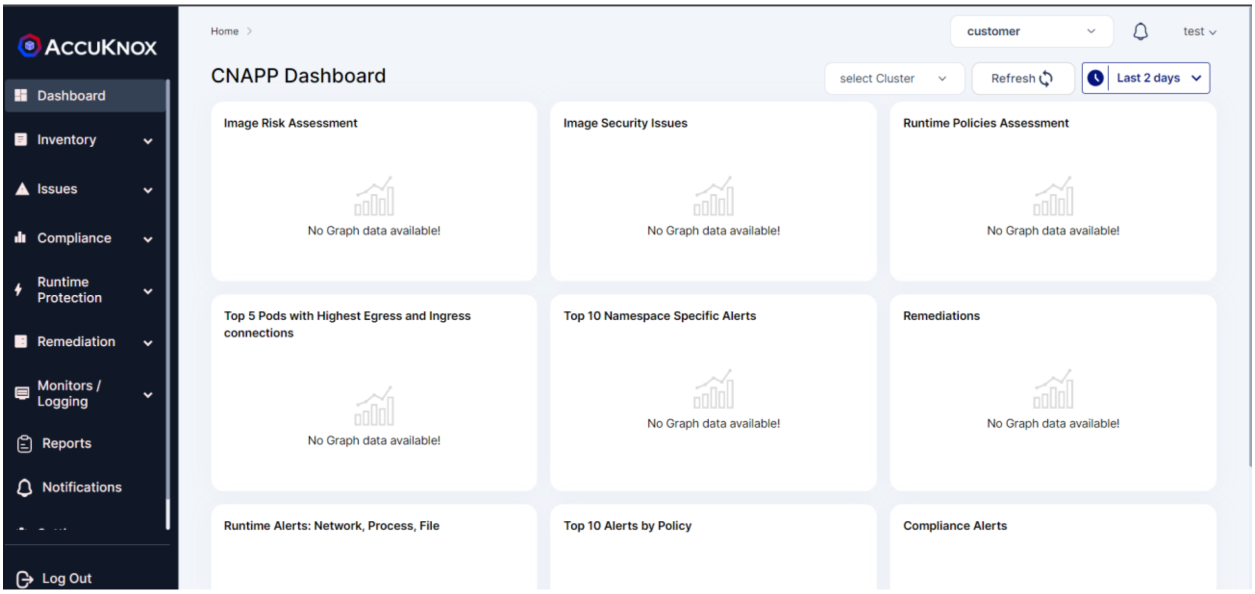
Deployments	Resource usage	Port	Connection Type
Shared Informer Agent	CPU: 20 m, Memory: 50 Mi	3000	Inbound/Outbound
Feeder Service	CPU: 50 m, Memory: 100 Mi	3000	Inbound/Outbound
Policy Enforcement	CPU: 10 m, Memory: 20 Mi	443	Inbound/Outbound

- These ports need to be allowed through the firewall.

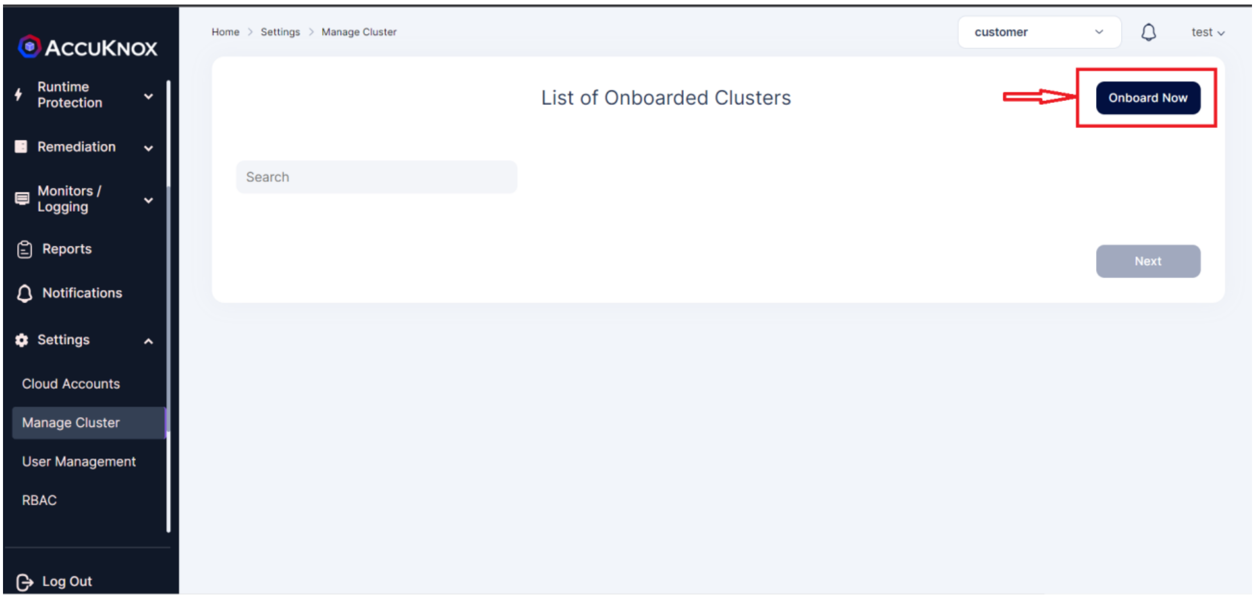
Cluster Onboarding

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

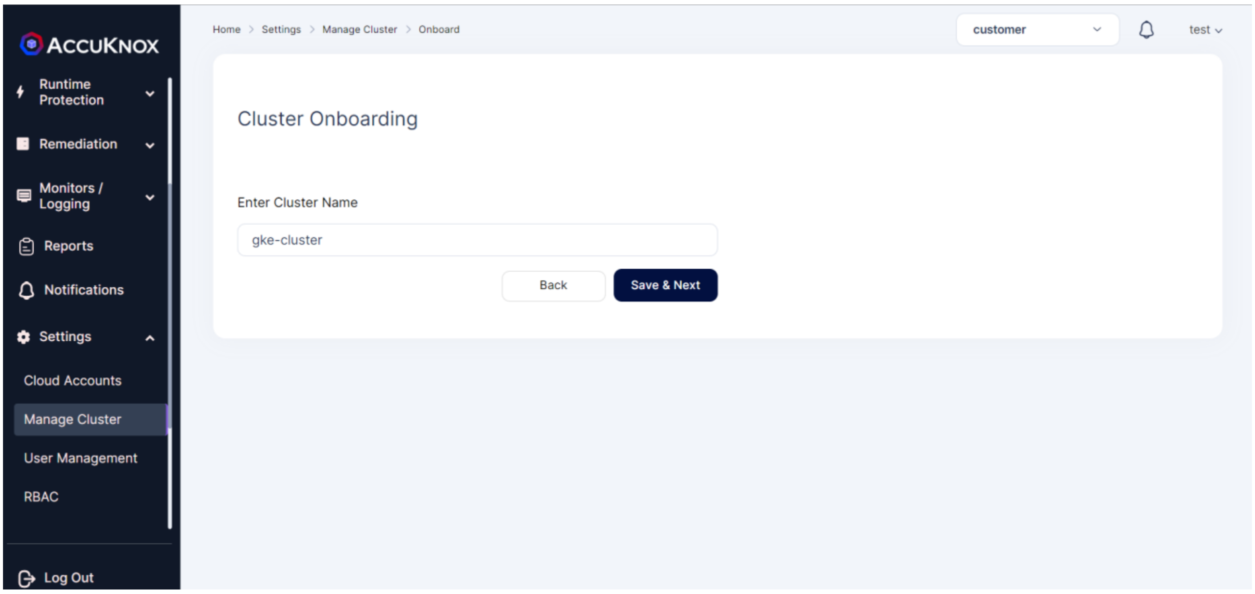
Step 1: After signing up, the user will be taken to the CNAPP dashboard. Since there is no cluster or cloud account onboarded, widgets will not have any data.



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-premises environment or virtual machines. To onboard cluster select onboard now option.



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



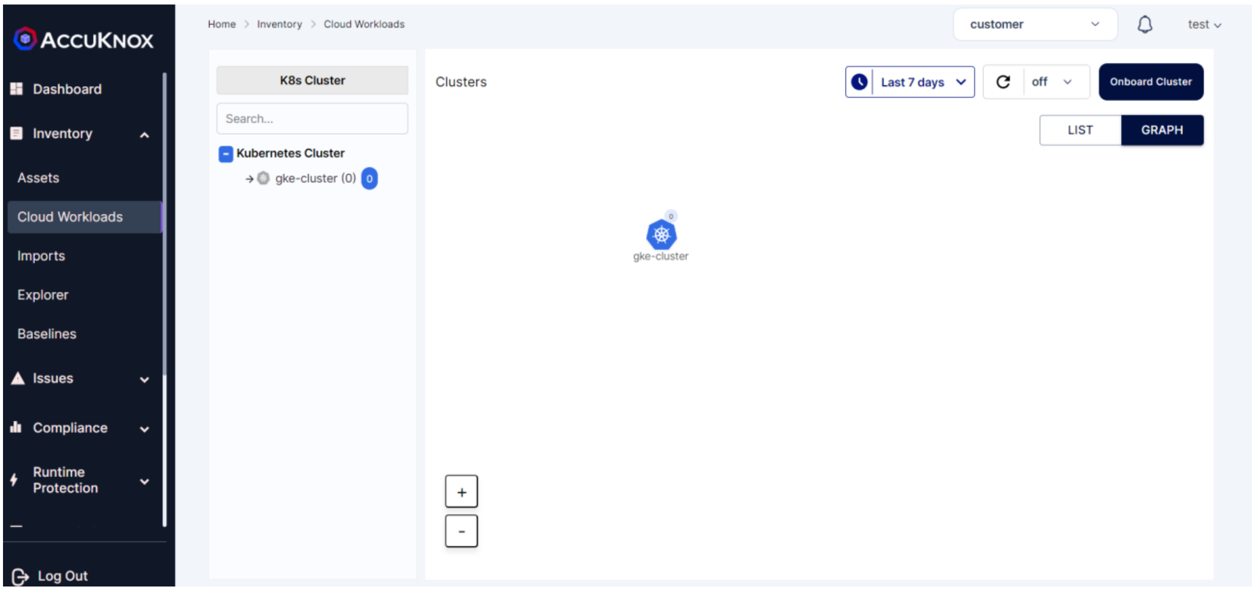
Cluster Onboarding

Enter Cluster Name

gke-cluster

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.

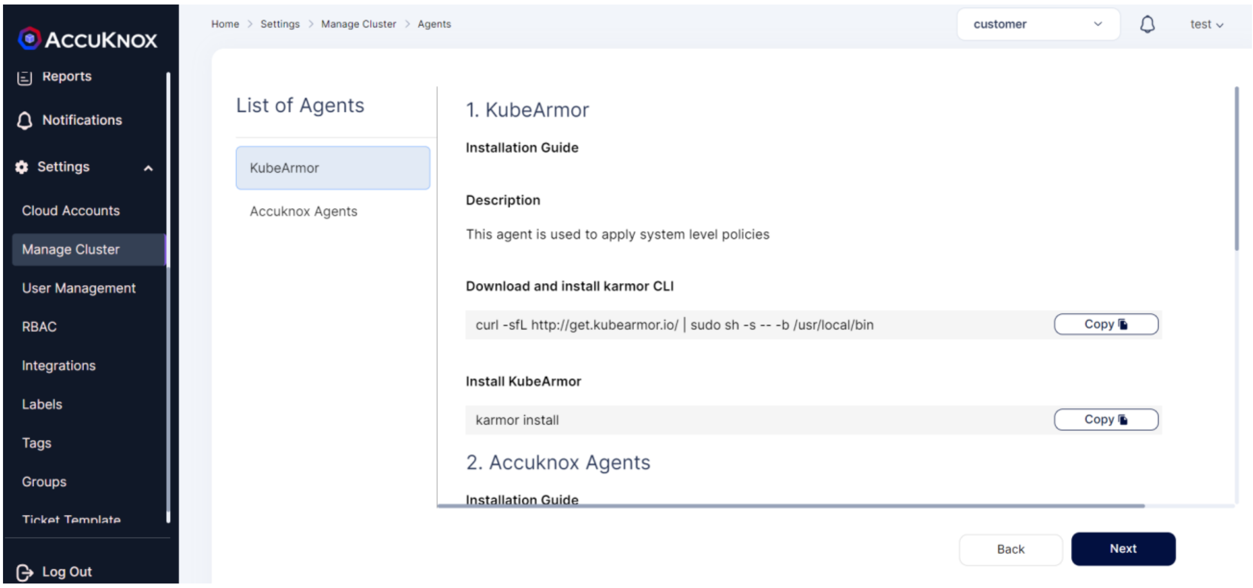
Step 5.1: KubeArmor Installation:

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.



List of Agents

KubeArmor

Accuknox Agents

1. KubeArmor

Installation Guide

Description

This agent is used to apply system level policies

Download and install karmor CLI

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

Install KubeArmor

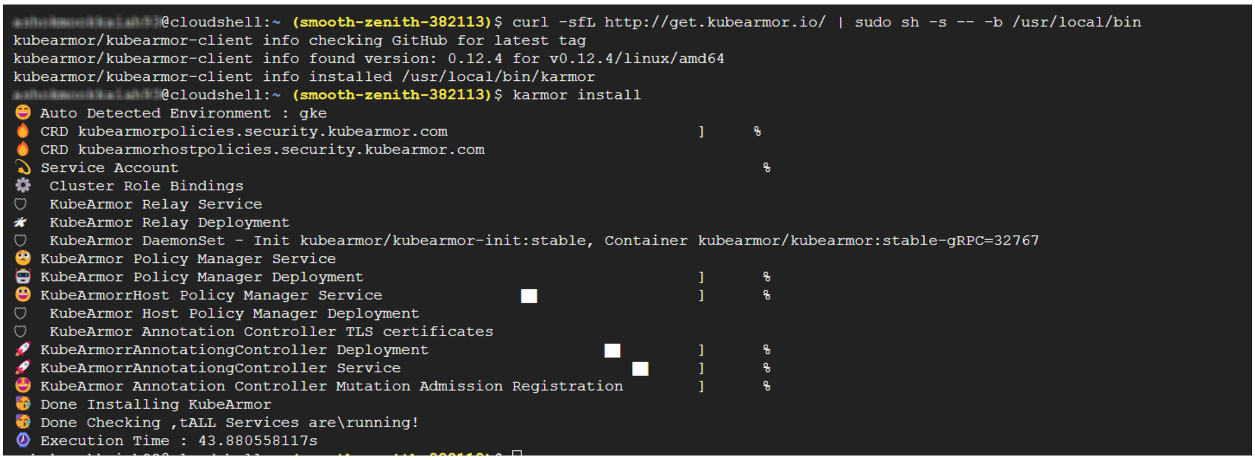
```
karmor install
```

2. Accuknox Agents

Installation Guide

KubeArmor is installed using the following commands:

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



```
[redacted]@cloudshell:~ (smooth-zenith-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
[redacted]@cloudshell:~ (smooth-zenith-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            □                  ]      %
🛡  KubeArmor Host Policy Manager Deployment
🛡  KubeArmor Annotation Controller TLS certificates
🚀 KubeArmorrAnnotationgController Deployment                □         ]      %
🚀 KubeArmorrAnnotationgController 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.

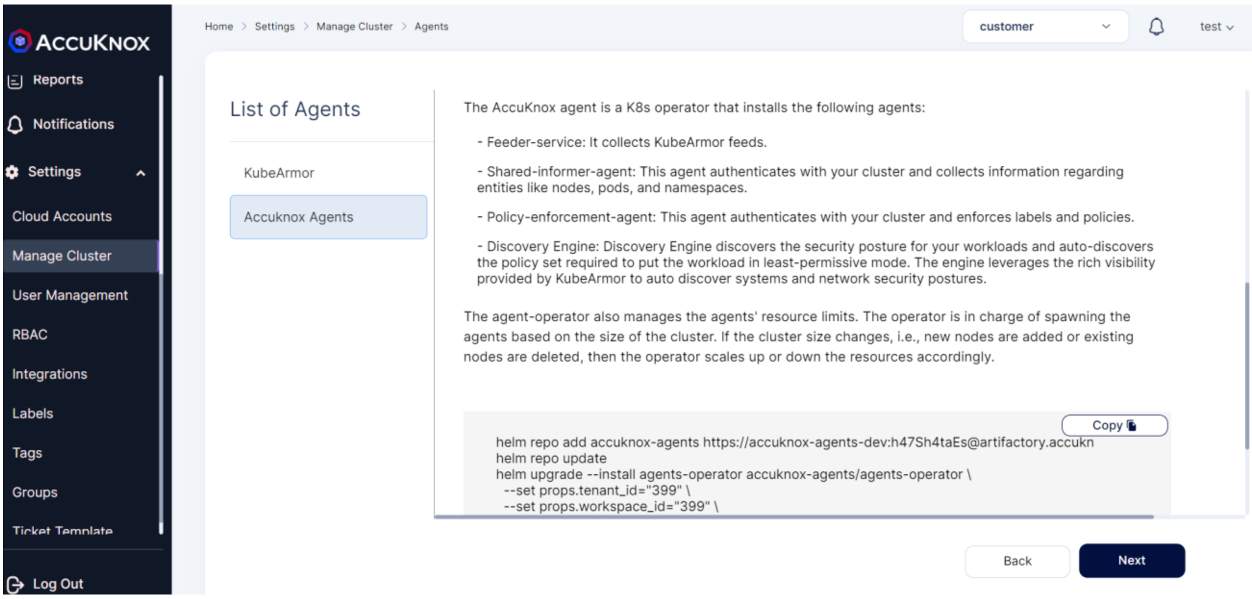
AccuKnox Agents:

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:

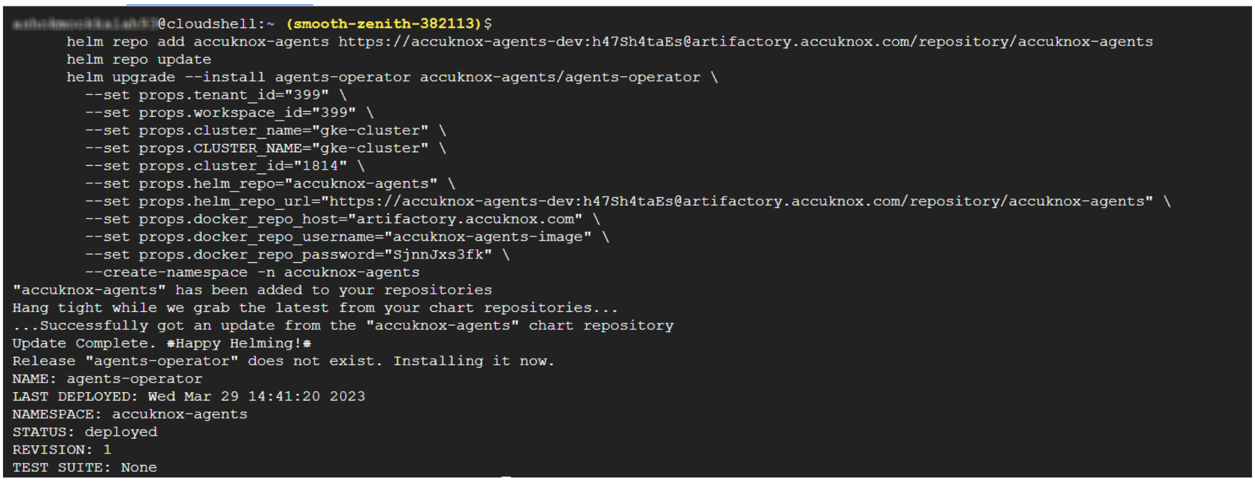
- Feeder-service: It collects KubeArmor feeds.
- Shared-informer-agent: This agent authenticates with your cluster and collects information regarding entities like nodes, pods, and namespaces.
- Policy-enforcement-agent: This agent authenticates with your cluster and enforces labels and policies.
- Discovery 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.accukn
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:

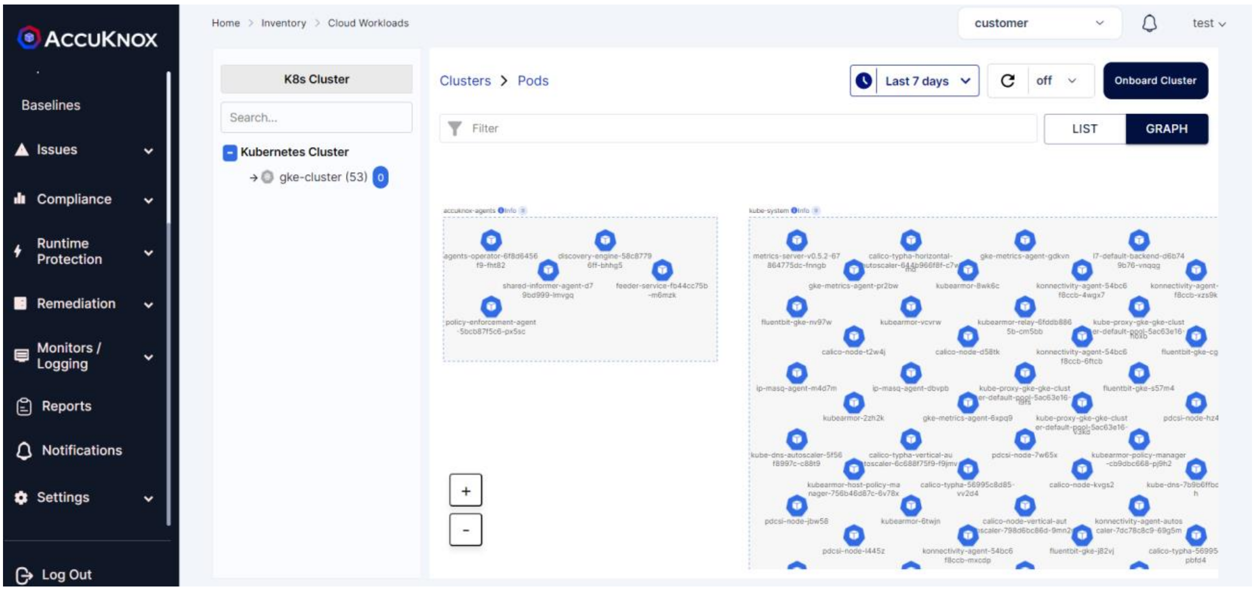
```
    helm repo add accuknox-agents https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/repository/accuknox-agents
      helm repo update
      helm upgrade --install agents-operator accuknox-agents/agents-operator \
        --set props.tenant_id="399" \
        --set props.workspace_id="399"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



```
[redacted]@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 Helming!*
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 is specific to this example, and it will vary based on the cluster

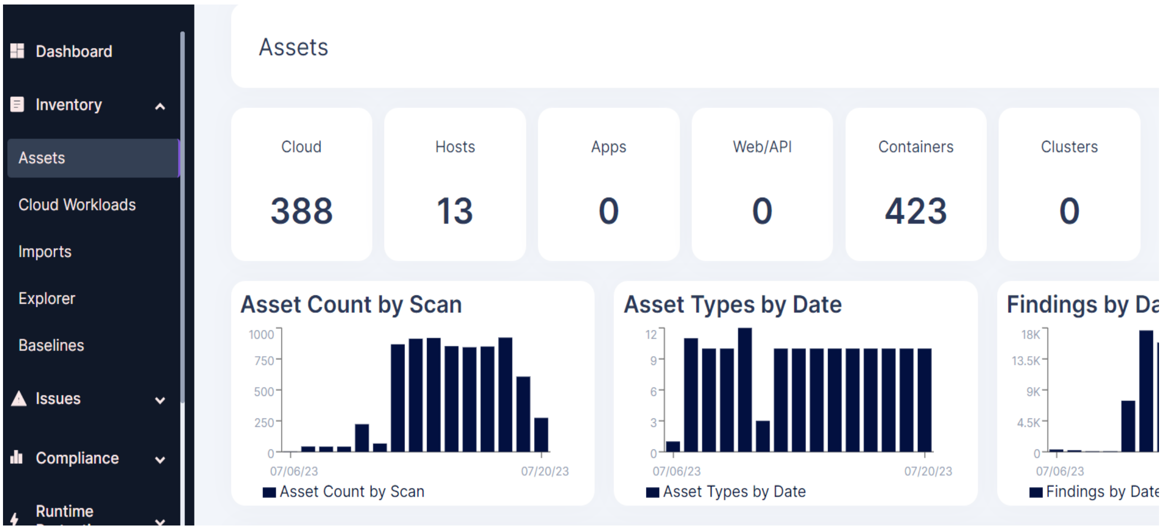
Step 6: After installing all the AccuKnox agents the cluster is onboarded successfully into the SaaS application. We can see the workload details of the onboarded cluster by Navigating to Inventory->cloud Workloads option



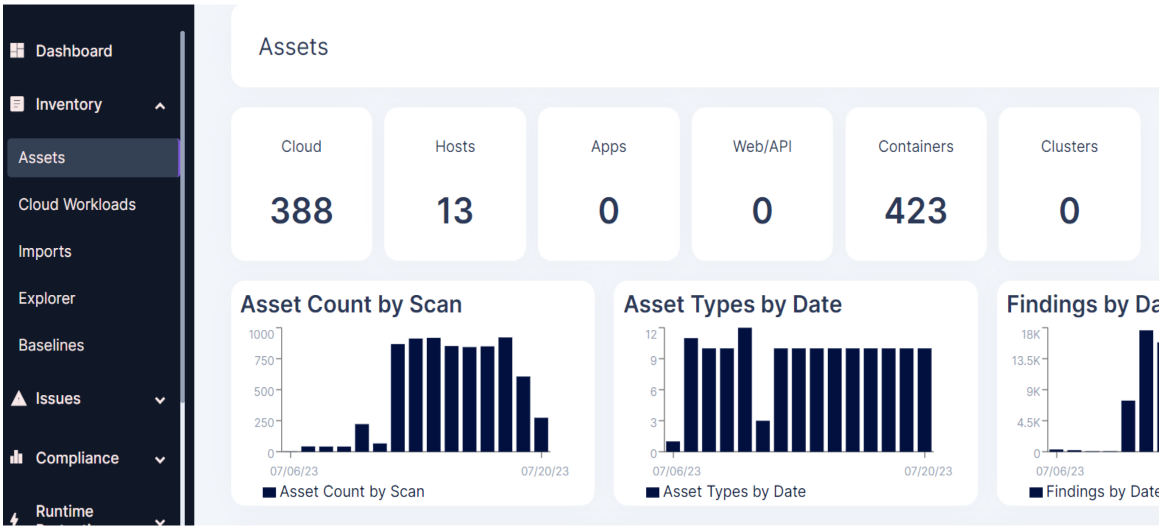
Asset Inventory

Cloud Assets

- How to find a particular asset
  - First navigate to the Assets screen under Inventory:



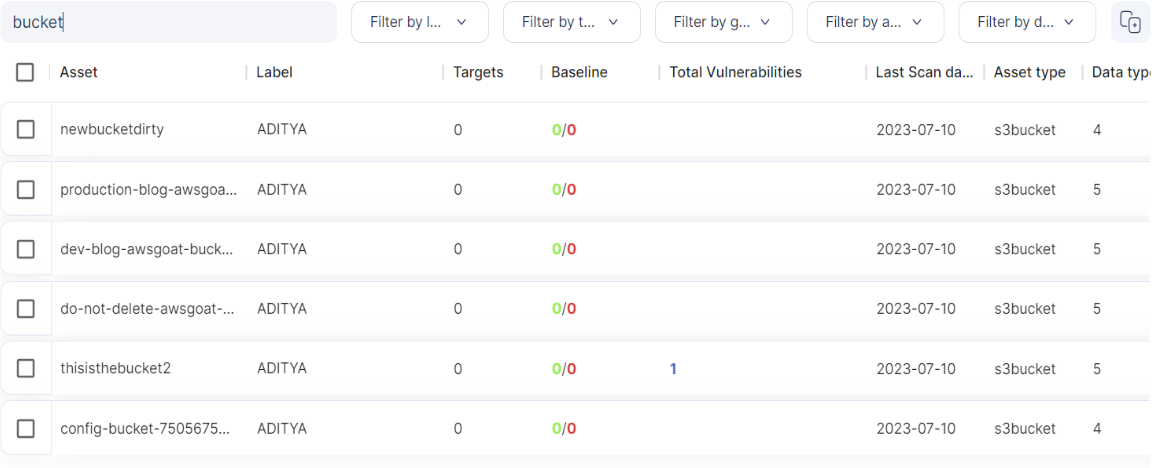
- First navigate to the Assets screen under Inventory:



Assets

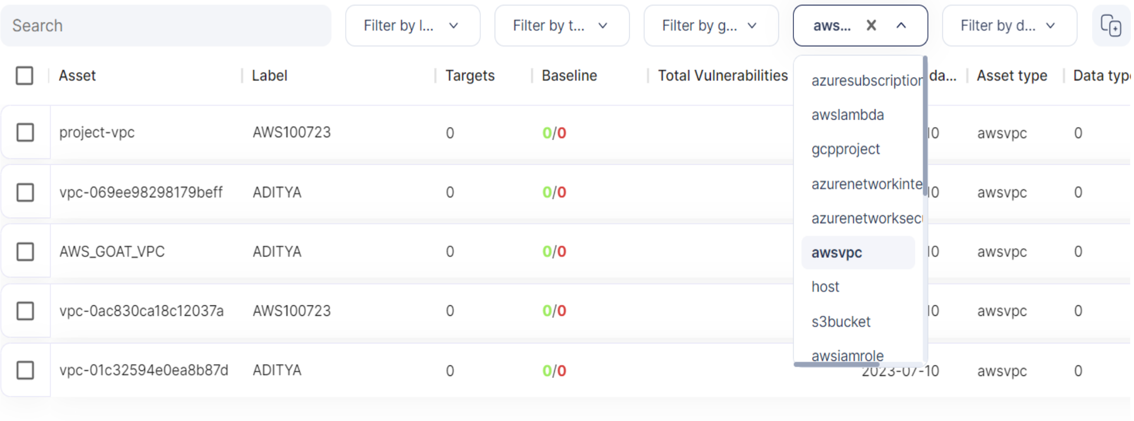
Cloud	Hosts	Apps	Web/API	Containers	Clusters
388	13	0	0	423	0

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



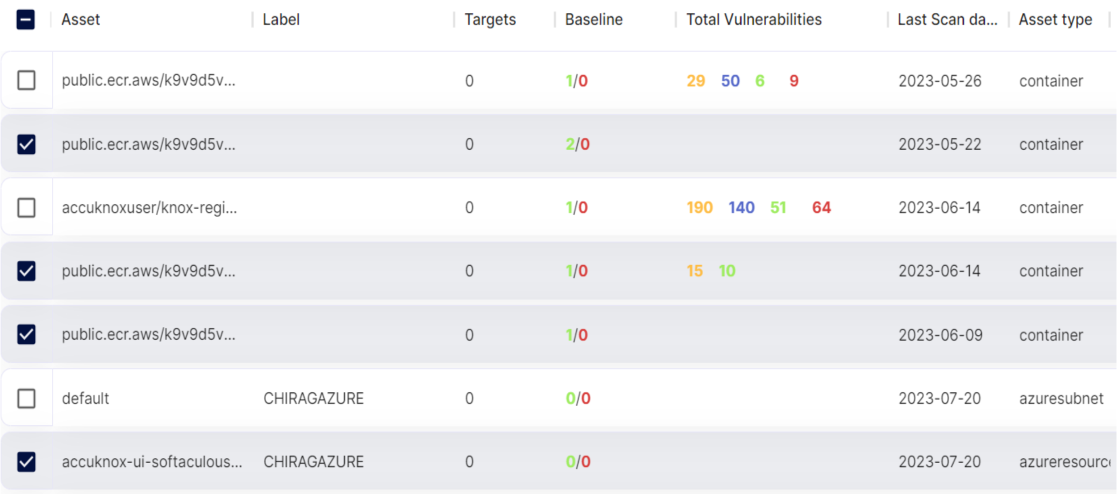
☐	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ
☐	newbucketdirty	ADITYA	0	0/0		2023-07-10	s3bucket	4
☐	production-blog-awsgoa...	ADITYA	0	0/0		2023-07-10	s3bucket	5
☐	dev-blog-awsgoat-buck...	ADITYA	0	0/0		2023-07-10	s3bucket	5
☐	do-not-delete-awsgoat-...	ADITYA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

- 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:



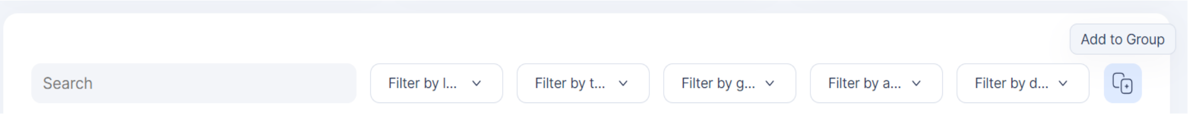
☐	Asset	Label	Targets	Baseline	Total Vulnerabilities	da...	Asset type	Data typ
☐	project-vpc	AWS100723	0	0/0		l0	awsvpc	0
☐	vpc-069ee98298179beff	ADITYA	0	0/0		l0	awsvpc	0
☐	AWS_GOAT_VPC	ADITYA	0	0/0		l0	awsvpc	0
☐	vpc-0ac830ca18c12037a	AWS100723	0	0/0		l0	awsvpc	0
☐	vpc-01c32594e0ea8b87d	ADITYA	0	0/0		2023-07-10	awsvpc	0

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

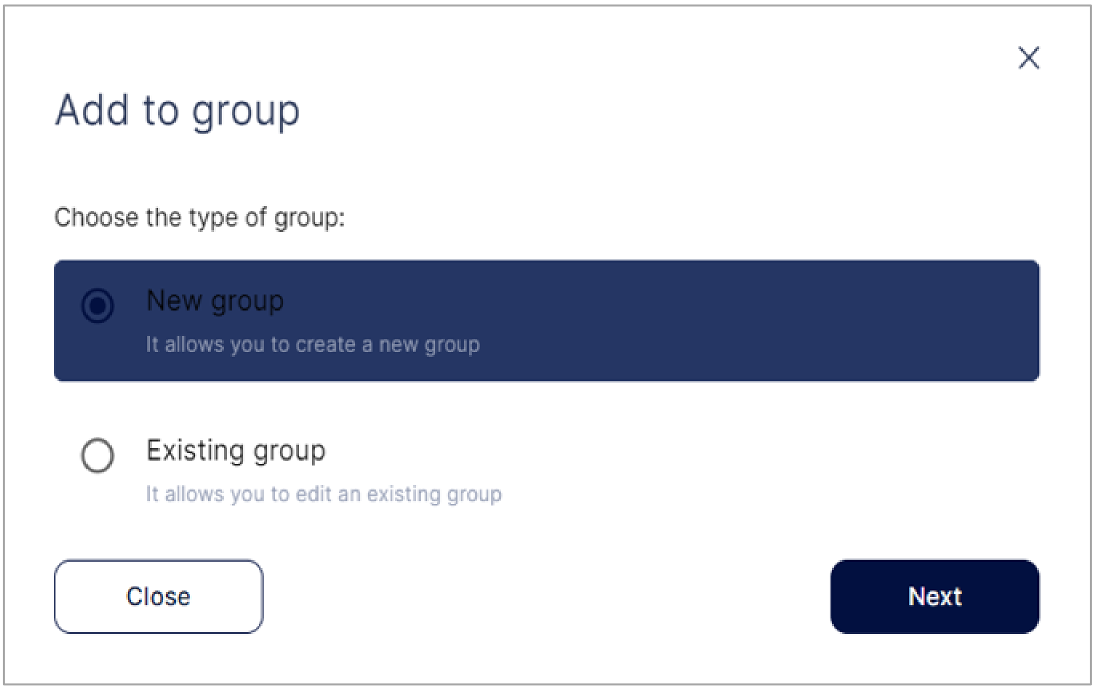


⊟	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type
□	public.ecr.aws/k9v9d5v...		0	1/0	29 50 6 9	2023-05-26	container
☑	public.ecr.aws/k9v9d5v...		0	2/0		2023-05-22	container
□	accuknoxuser/knox-regi...		0	1/0	190 140 51 64	2023-06-14	container
☑	public.ecr.aws/k9v9d5v...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

- 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:



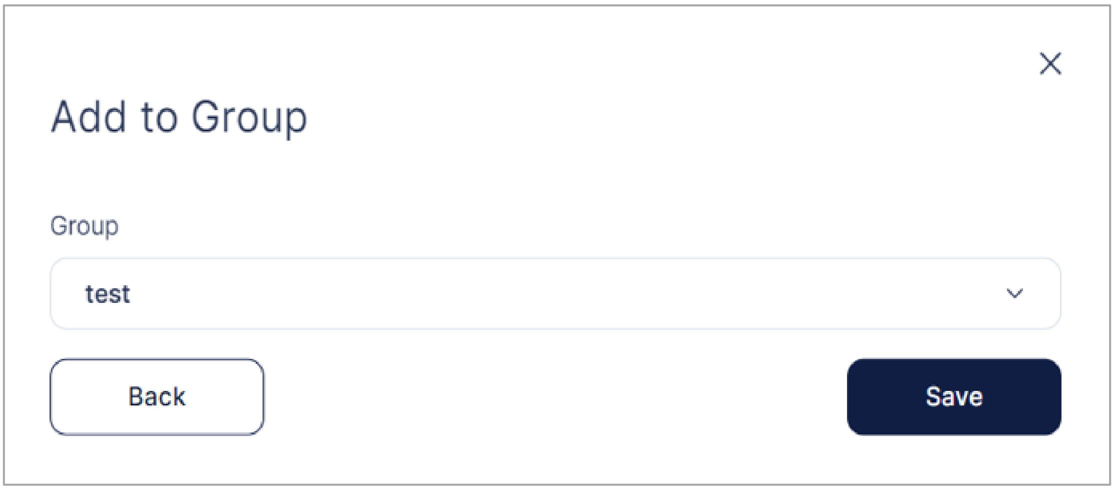
Add to group

Choose the type of group:

● New group
It allows you to create a new group

○ Existing group
It allows you to edit 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:

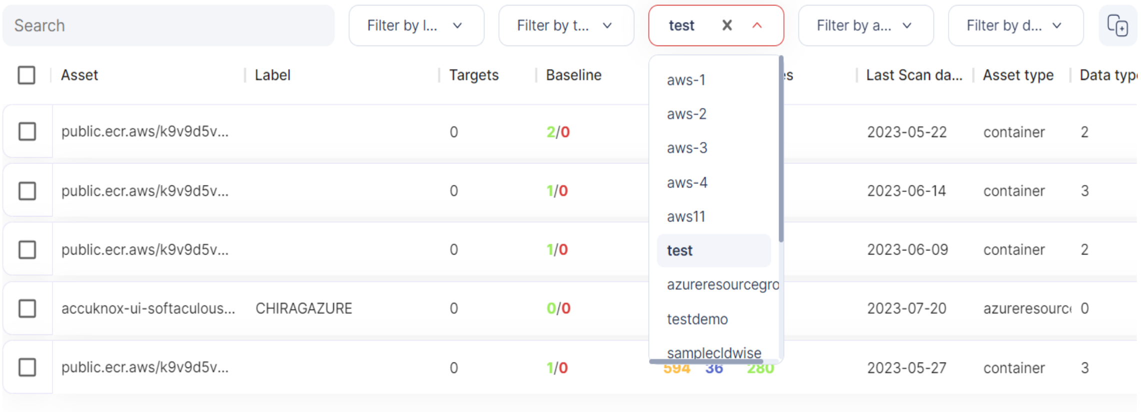


Add to Group

Group

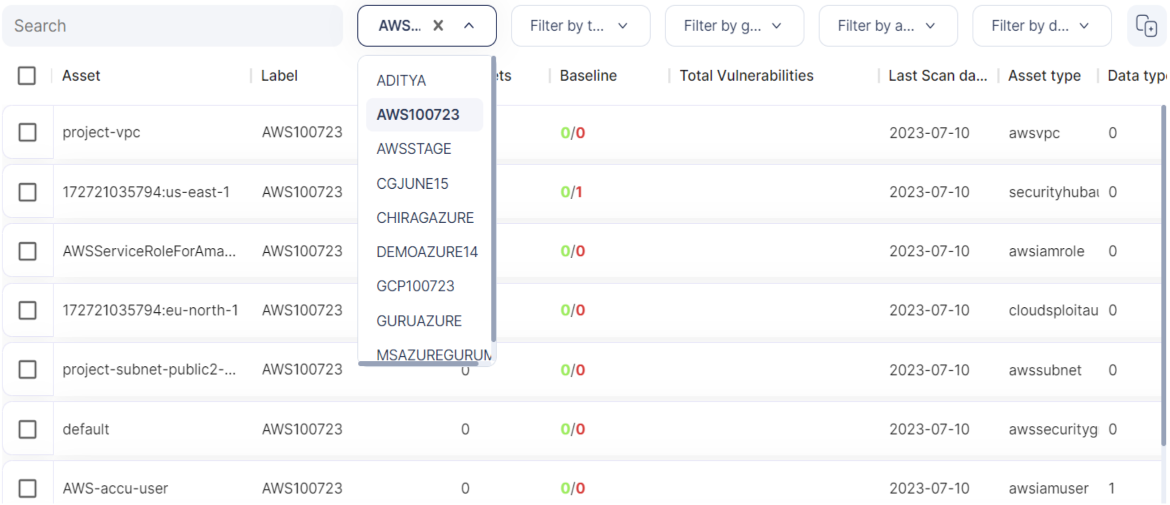
test

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



☐	Asset	Label	Targets	Baseline	...s	Last Scan da...	Asset type	Data typ
☐	public.ecr.aws/k9v9d5v...		0	2/0		2023-05-22	container	2
☐	public.ecr.aws/k9v9d5v...		0	1/0		2023-06-14	container	3
☐	public.ecr.aws/k9v9d5v...		0	1/0		2023-06-09	container	2
☐	accuknox-ui-softaculous...	CHIRAGAZURE	0	0/0		2023-07-20	azureresourc	0
☐	public.ecr.aws/k9v9d5v...		0	1/0	594 36 280	2023-05-27	container	3

- 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:

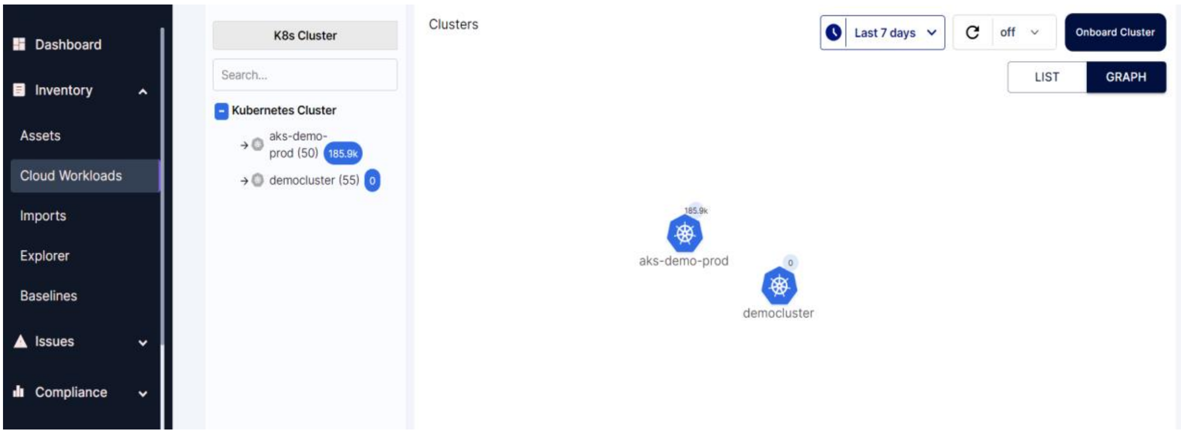


□	Asset	Label	ts	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ
□	project-vpc	AWS100723		0/0		2023-07-10	awsvpc	0
□	172721035794:us-east-1	AWS100723		0/1		2023-07-10	securityhubaı	0
□	AWSServiceRoleForAma...	AWS100723		0/0		2023-07-10	awsiamrole	0
□	172721035794:eu-north-1	AWS100723		0/0		2023-07-10	cloudsploitau	0
□	project-subnet-public2-...	AWS100723	0	0/0		2023-07-10	awssubnet	0
□	default	AWS100723	0	0/0		2023-07-10	awssecurityg	0
□	AWS-accu-user	AWS100723	0	0/0		2023-07-10	awsiamuser	1

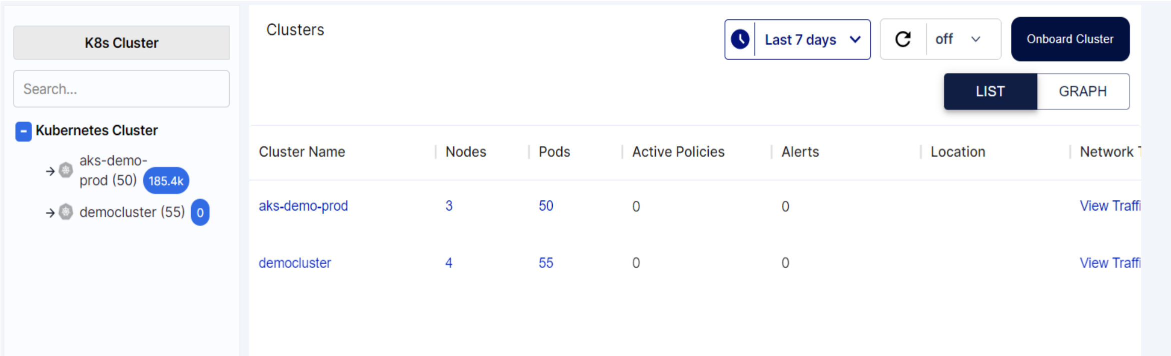
- To further refine the results, we can use the search bar or add additional filters such as Assets

Cloud Workload

- How to find graph view of clusters
  - Navigate to Cloud Workloads screen under Inventory to view the clusters that have been onboarded:

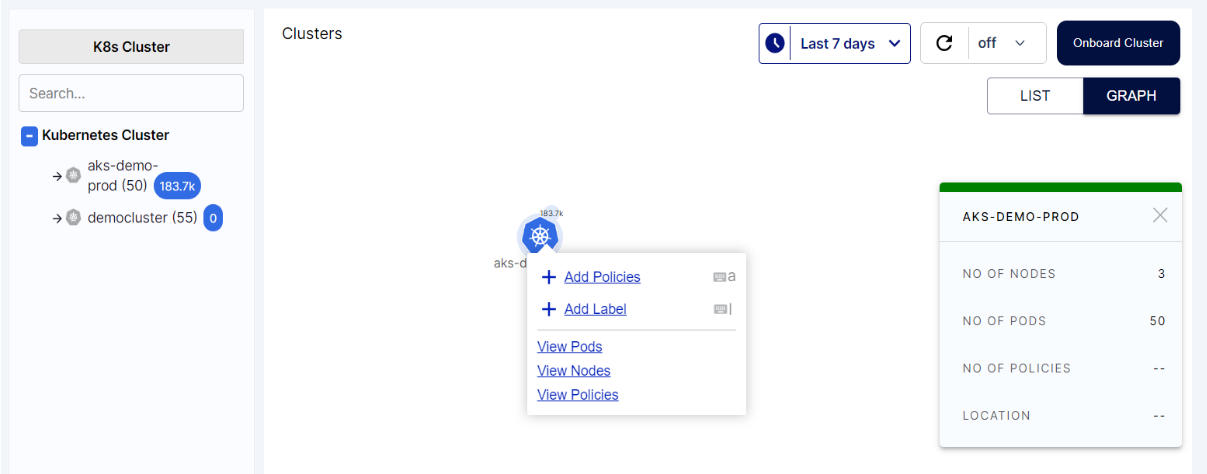


- How to find list view of clusters
    - Click on the LIST option in the top right of the Cloud Workloads screen to get a list view of all the clusters

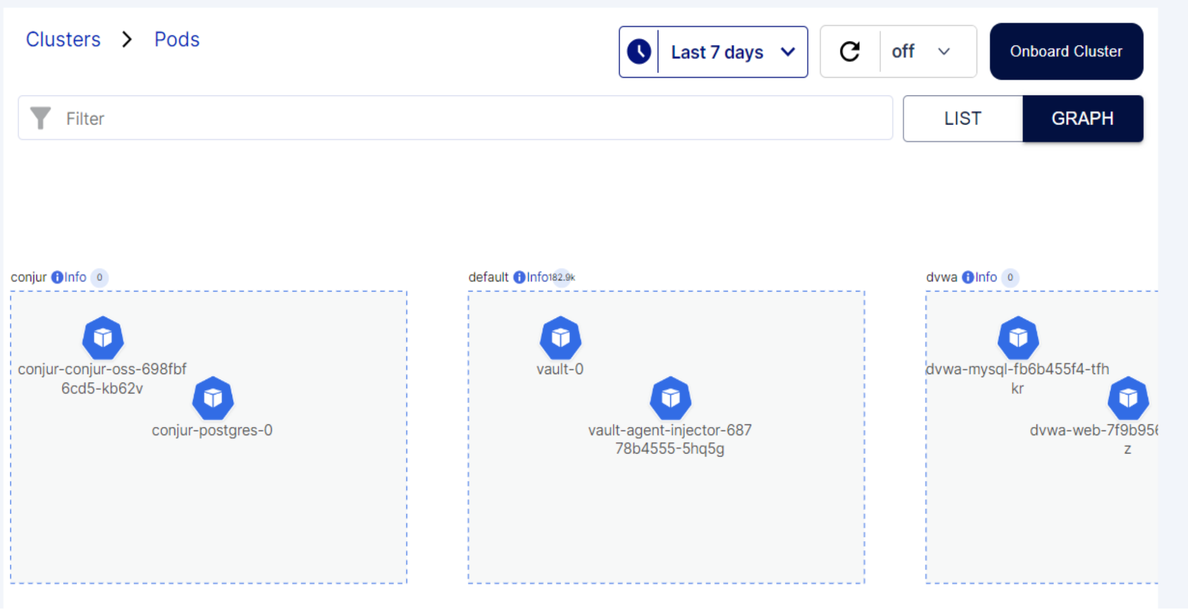


Cluster Name	Nodes	Pods	Active Policies	Alerts	Location	Network T
aks-demo-prod	3	50	0	0		View Traffi
democluster	4	55	0	0		View Traffi

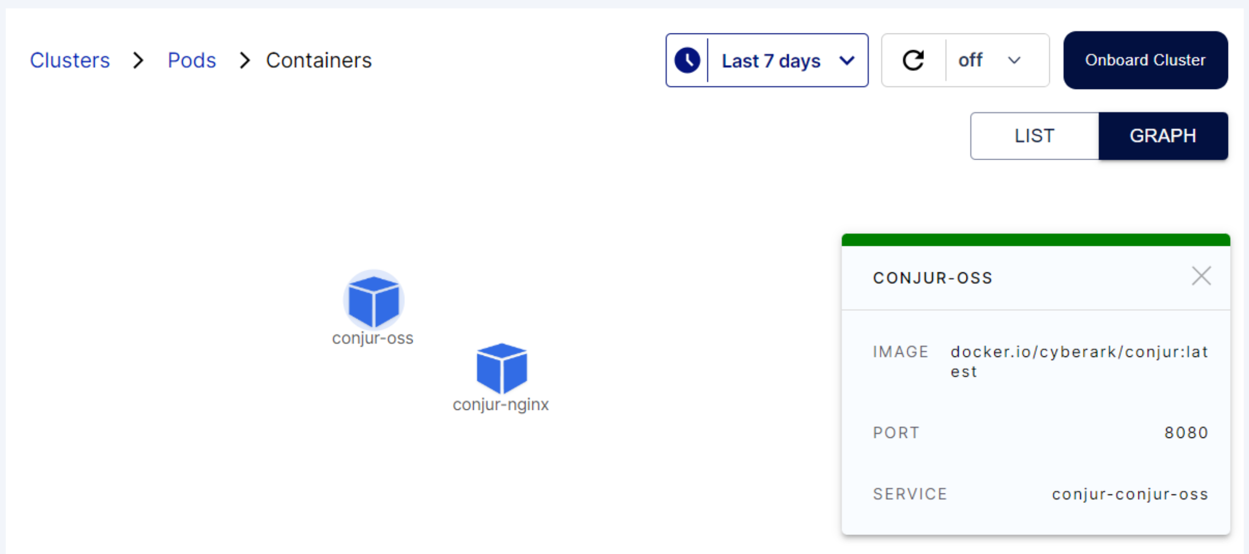
- The view can be freely switched between LIST and GRAPH as required
- How to find details on cluster
    - Clicking on any of the clusters in the Cloud Workloads screen gives more information about the cluster:



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



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

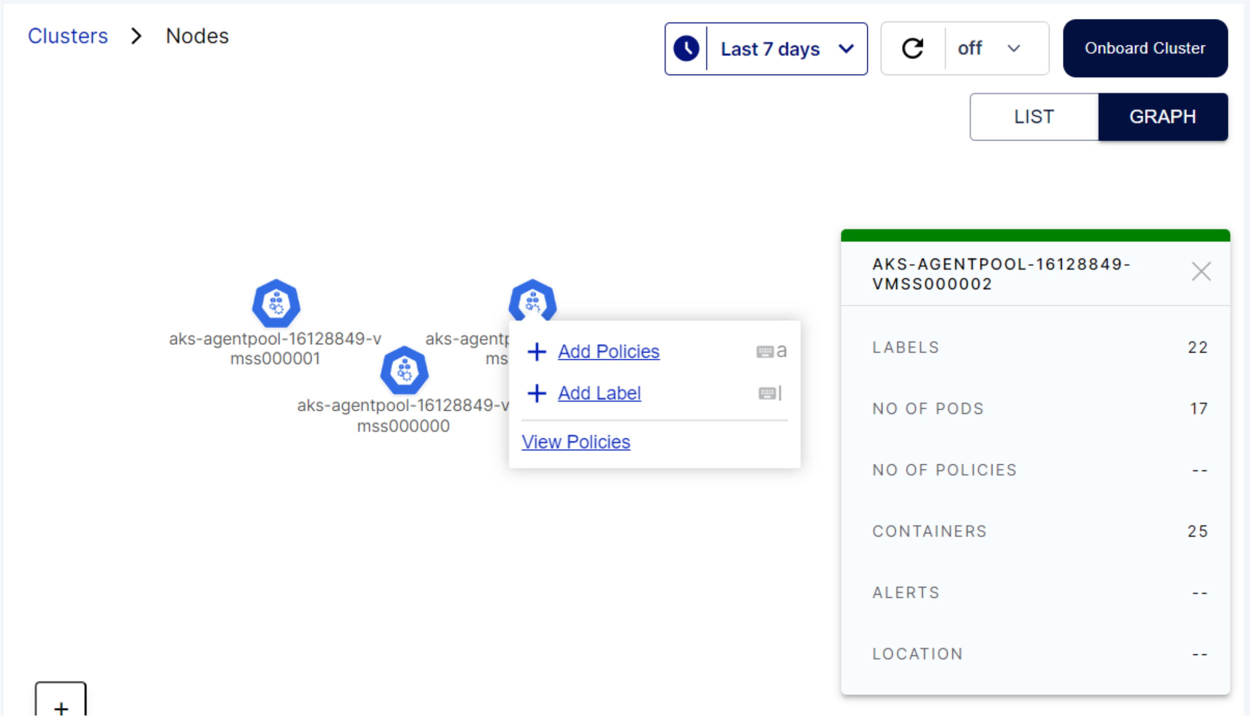


CONJUR-OSS

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.

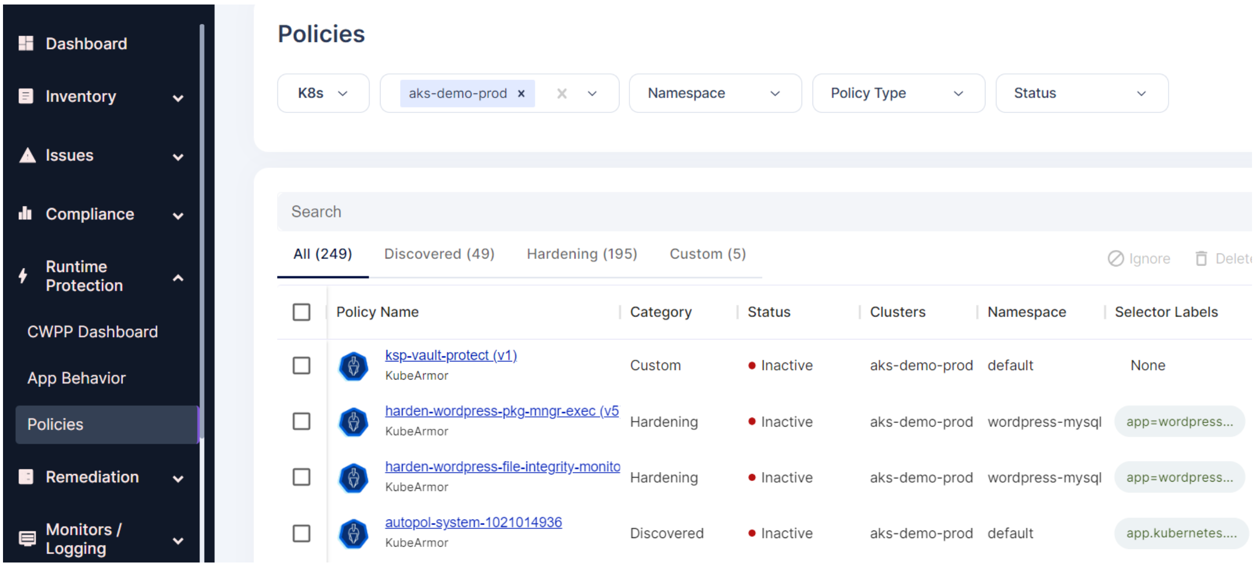
Navigate back to the Clusters screen and select a cluster and then click on View Nodes. In the nodes screen, we can view the nodes used by the cluster. Selecting a node gives more information about it:



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:



Policies

K8s | aks-demo-prod × | Namespace | Policy Type | Status

Search

All (249) | Discovered (49) | Hardening (195) | Custom (5) | Ignore | Delet

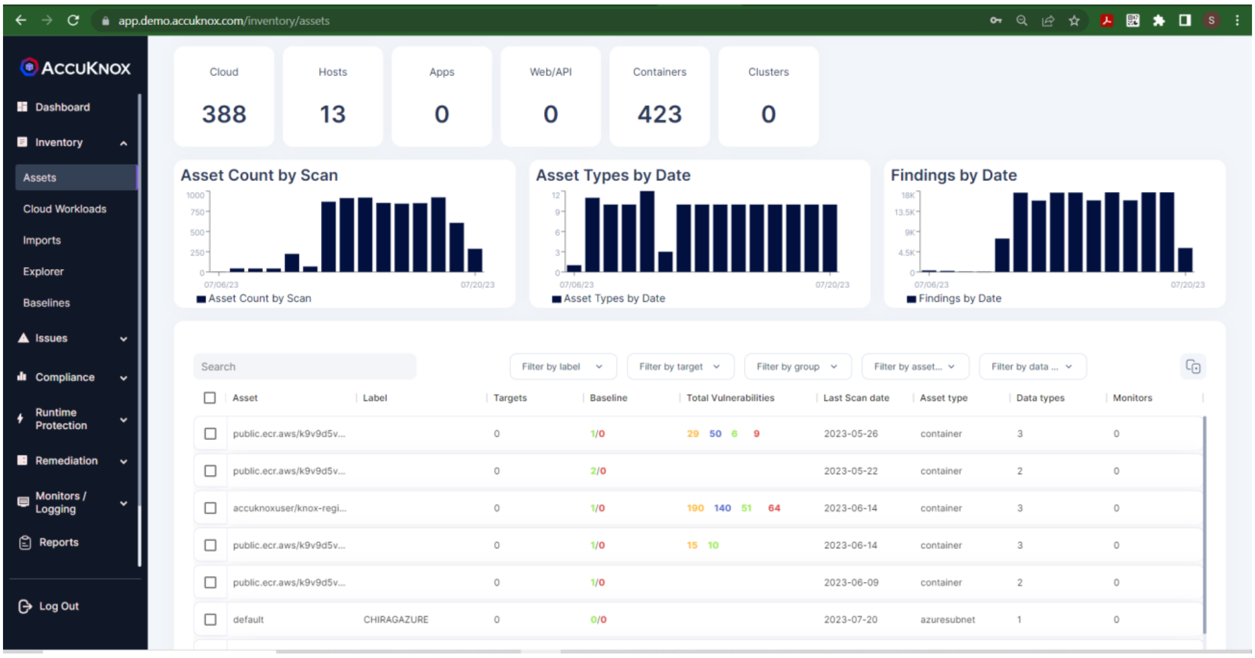
□	Policy Name	Category	Status	Clusters	Namespace	Selector Labels
□	ksp-vault-protect (v1) KubeArmor	Custom	● Inactive	aks-demo-prod	default	None
□	harden-wordpress-pkg-mngr-exec (v5 KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...
□	harden-wordpress-file-integrity-monito KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...
□	autopol-system-1021014936 KubeArmor	Discovered	● Inactive	aks-demo-prod	default	app.kubernetes....

Misconfigurations

Where to find misconfigurations

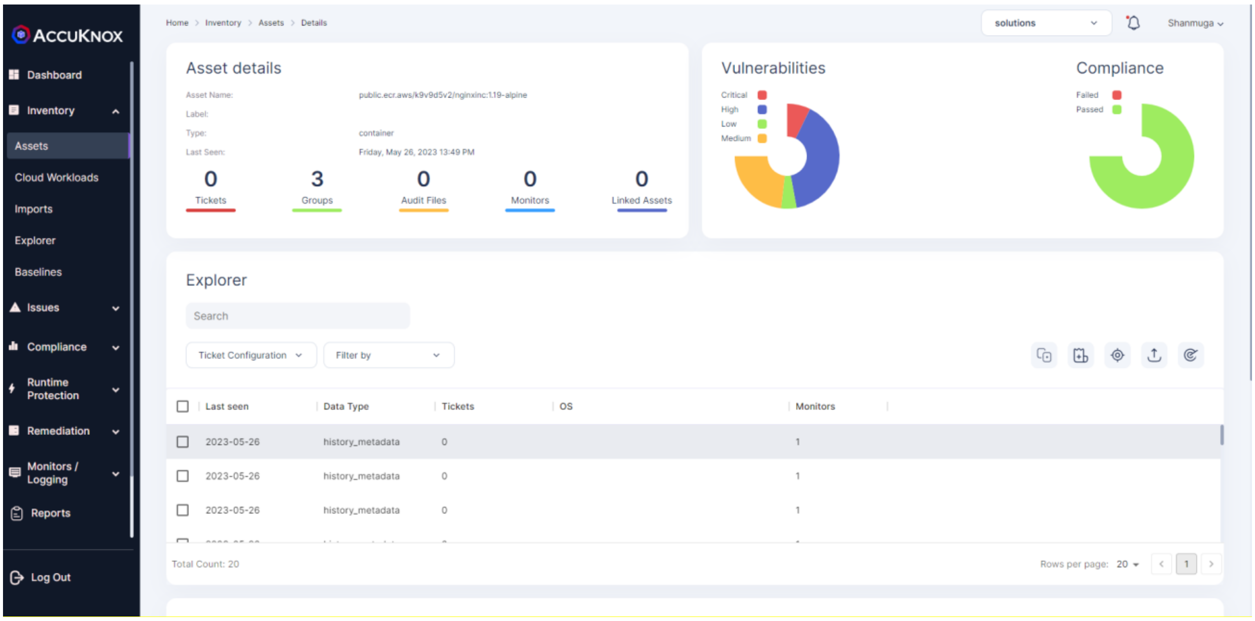
Asset Detail Page

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:1.19-alpine

Label:

Type: container

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

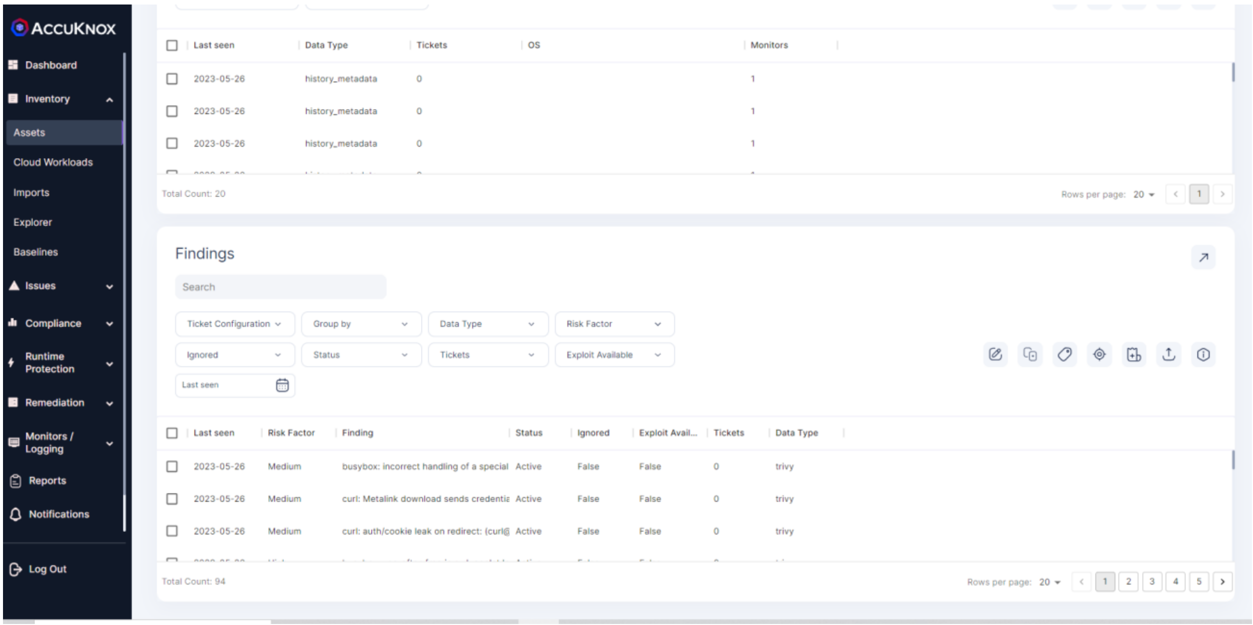
0	3	0	0	0
Tickets	Groups	Audit Files	Monitors	Linked Assets

□	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 < 1 >

Scroll down for the Findings



□	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

Findings

Search

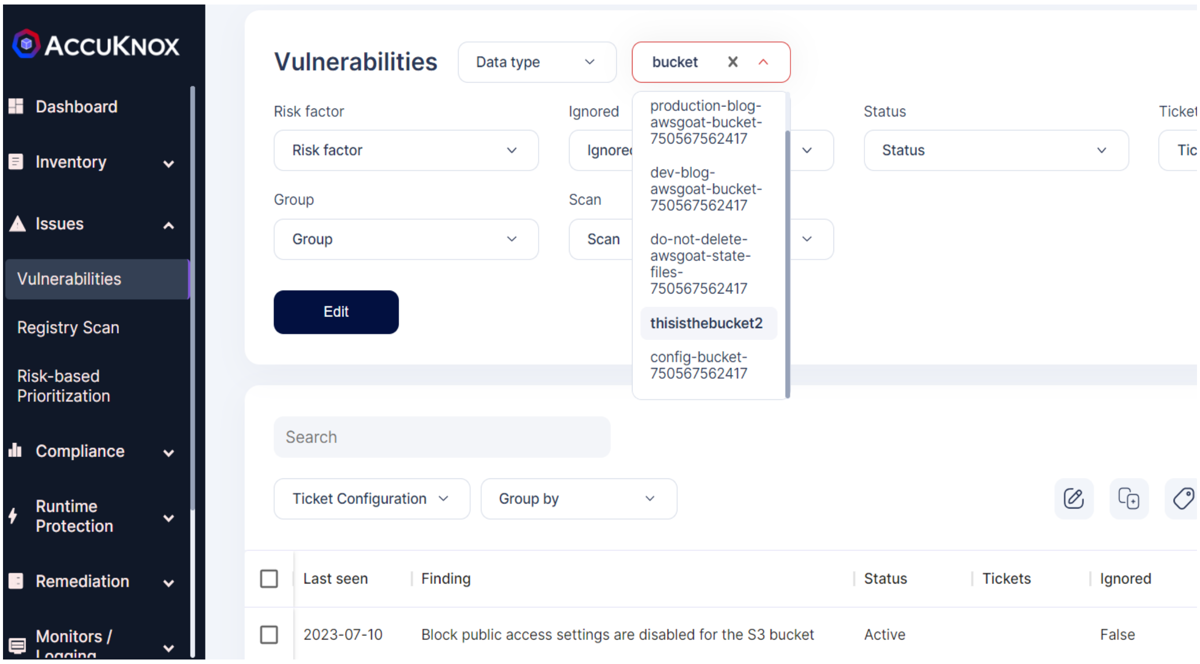
Ticket Configuration · Group by · Data Type · Risk Factor · Ignored · Status · Tickets · Exploit Available · Last seen

□	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
□	2023-05-26	Medium	busybox: incorrect handling of a special	Active	False	False	0	trivy
□	2023-05-26	Medium	curl: Metalink download sends credentia	Active	False	False	0	trivy
□	2023-05-26	Medium	curl: auth/cookie leak on redirect: (curl@	Active	False	False	0	trivy

Total Count: 94 Rows per page: 20

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

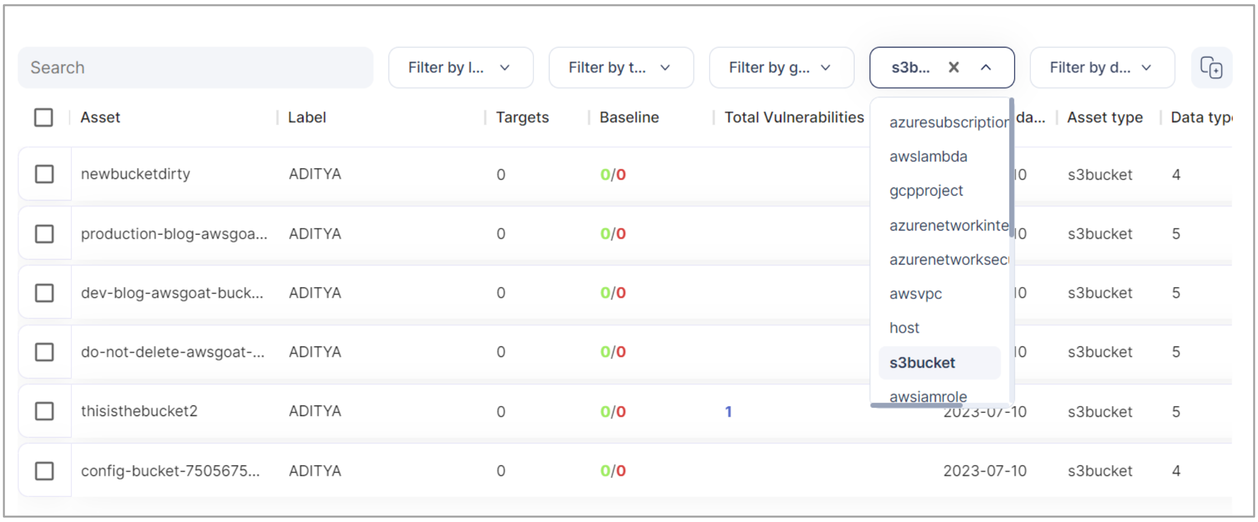
- Issue Page
  - Navigate to Vulnerabilities screen under Issues and select an Asset from the drop down at the top to view all misconfigurations associated with the Asset:



□	Last seen	Finding	Status	Tickets	Ignored
□	2023-07-10	Block public access settings are disabled for the S3 bucket	Active		False

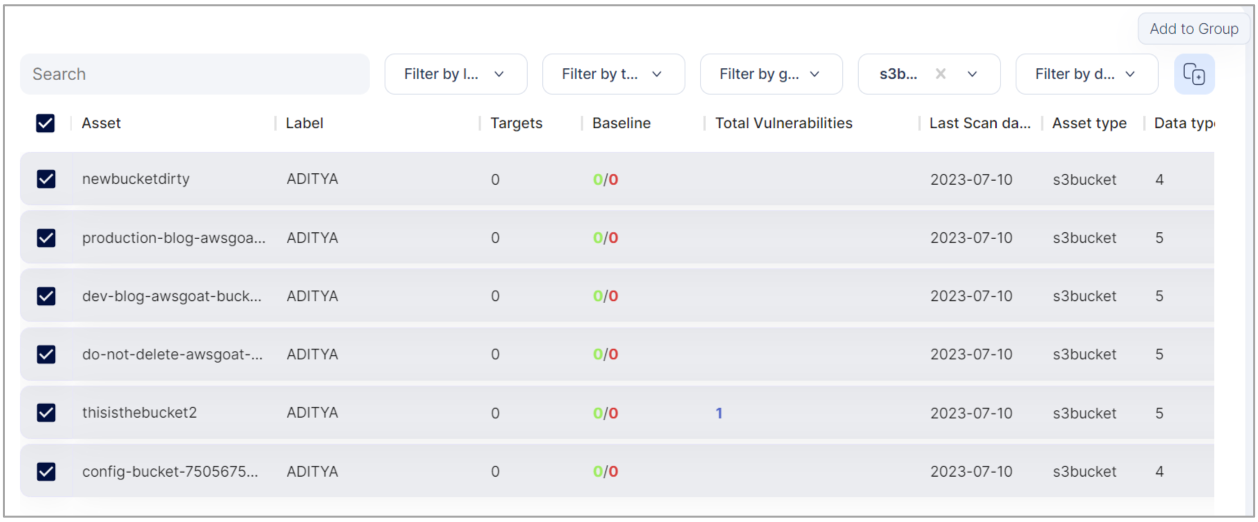
- You can also type in the Assets drop down to search for a particular Asset
  - How to group by Asset, say s3 and find misconfiguration

Step 1 : In the Assets screen under Inventory, filter by Assets to view only the S3 buckets:



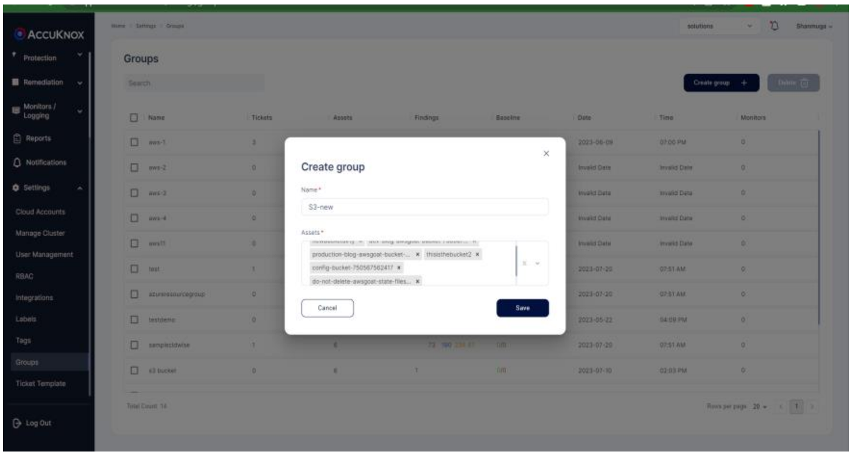
☐	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type	Data typ
☐	newbucketdirty	ADITYA	0	0/0			s3bucket	4
☐	production-blog-awsgoa...	ADITYA	0	0/0			s3bucket	5
☐	dev-blog-awsgoat-buck...	ADITYA	0	0/0			s3bucket	5
☐	do-not-delete-awsgoat-...	ADITYA	0	0/0			s3bucket	5
☐	thisisthebucket2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

Step 2 : 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-awsgoa...	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

Step 3: Click on Save



Create group

Name*: S3-new

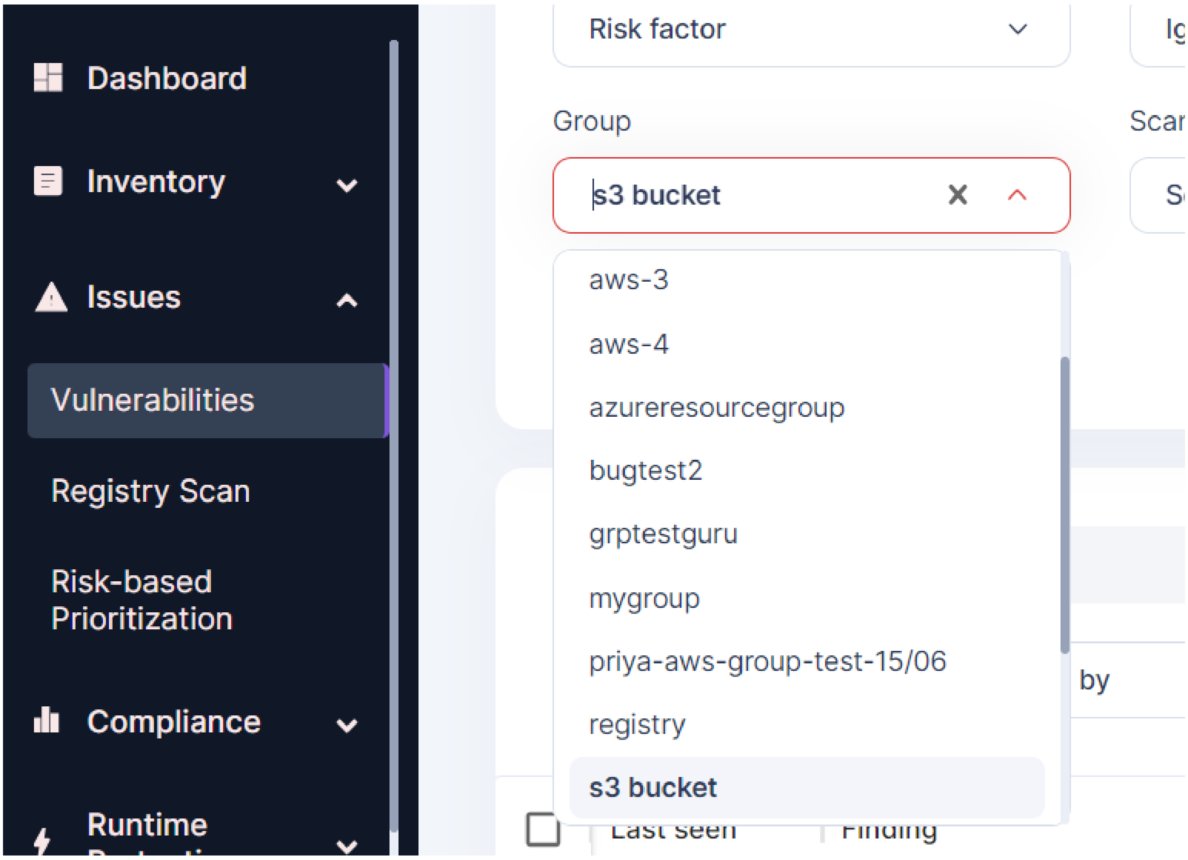
Assets*: production-blog-awsgoat-bucket-... × thisisthebucket2 × config-bucket-750567562417 × do-not-delete-awsgoat-state-files... ×

Cancel | Save

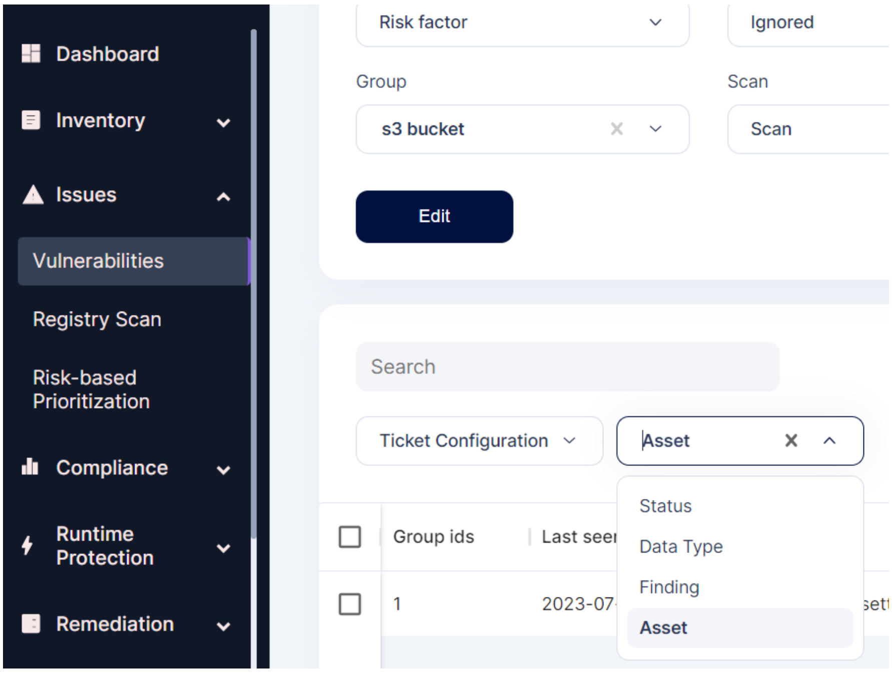
☐	Name	Tickets	Assets	Findings	Baseline	Date	Time	Monitors
☐	aws-1	3				2023-06-09	07:00 PM	0
☐	aws-2	0				Invalid Date	Invalid Date	0
☐	aws-3	0				Invalid Date	Invalid Date	0
☐	aws-4	0				Invalid Date	Invalid Date	0
☐	aws11	0				Invalid Date	Invalid Date	0
☐	test	1				2023-07-20	07:51 AM	0
☐	azureresourcegroup	0				2023-07-20	07:51 AM	0
☐	testdemo	0				2023-05-22	04:09 PM	0
☐	samplecldwise	1	6	73 190 234 67	0/0	2023-07-20	07:51 AM	0
☐	s3 bucket	0	6	1	0/0	2023-07-10	02:03 PM	0

Total Count: 14 — Rows per page 20 — 1

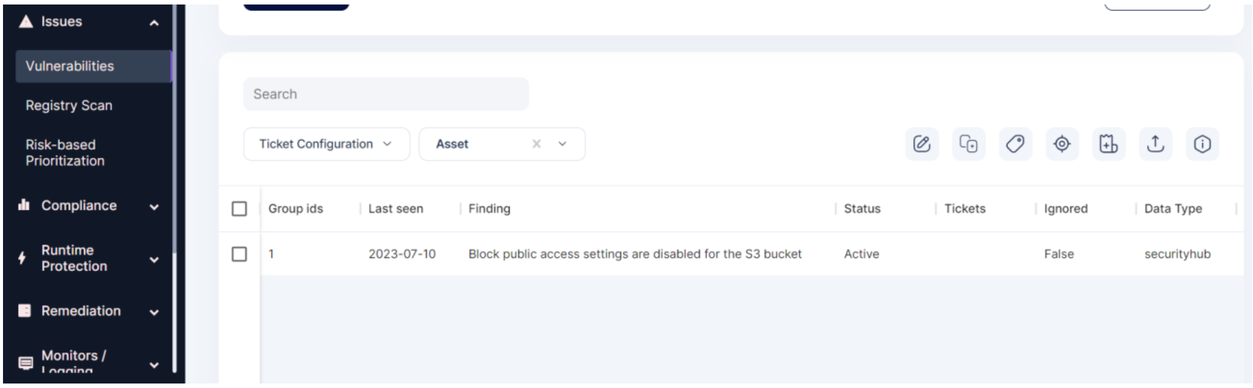
Step 4 : Click non Issues -> Vulnerabilities and select the group that was created from the drop down:



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

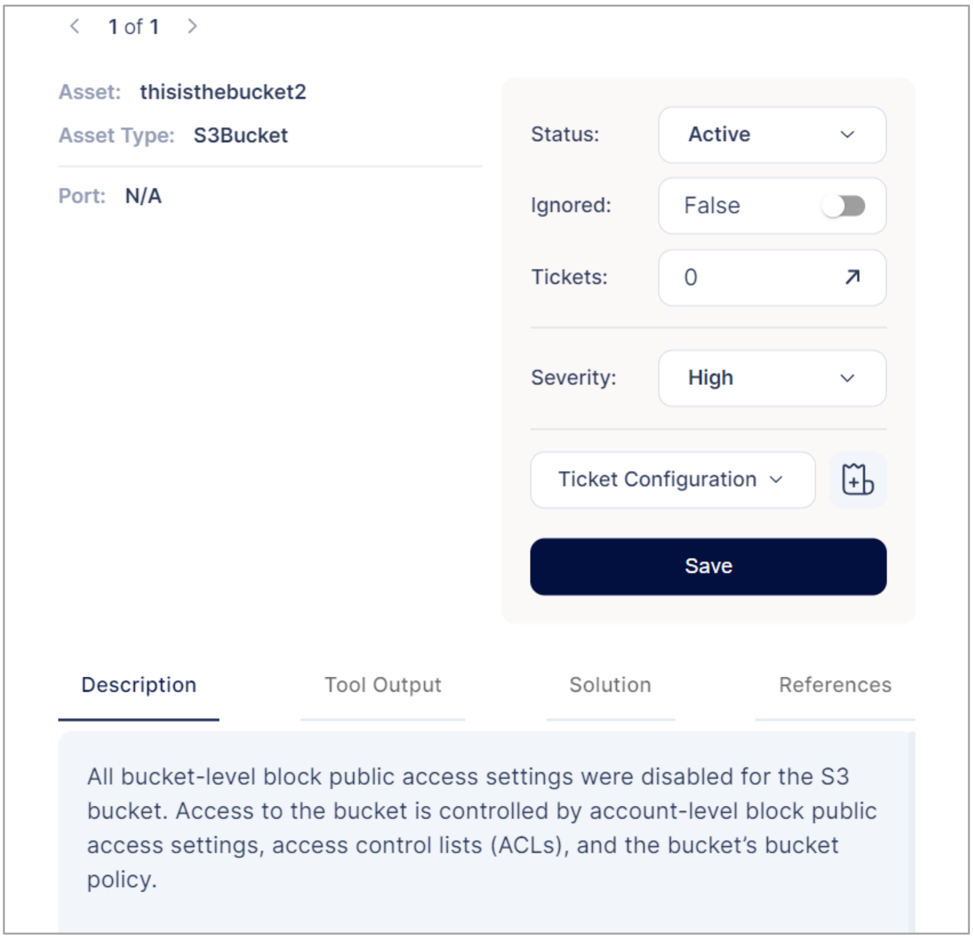


Step 6: Now, the list of s3 buckets with any misconfigurations associated with them can be seen



	Group ids	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



Asset: thisisthebucket2

Asset Type: S3Bucket

Port: N/A

Status: Active

Ignored: False

Tickets: 0

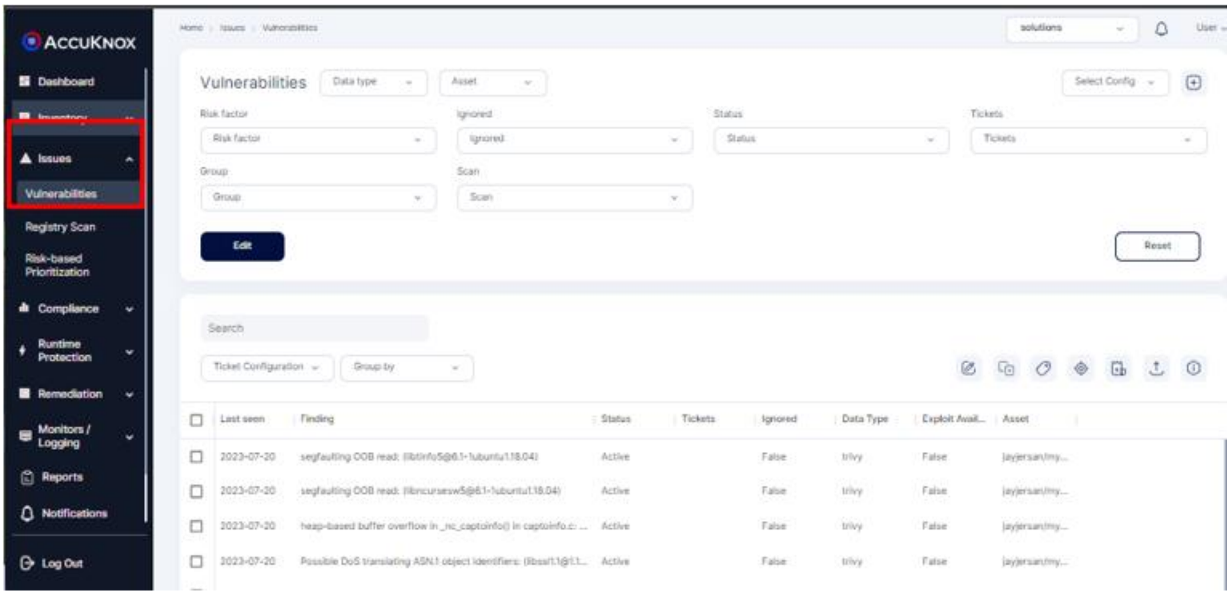
Severity: High

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.

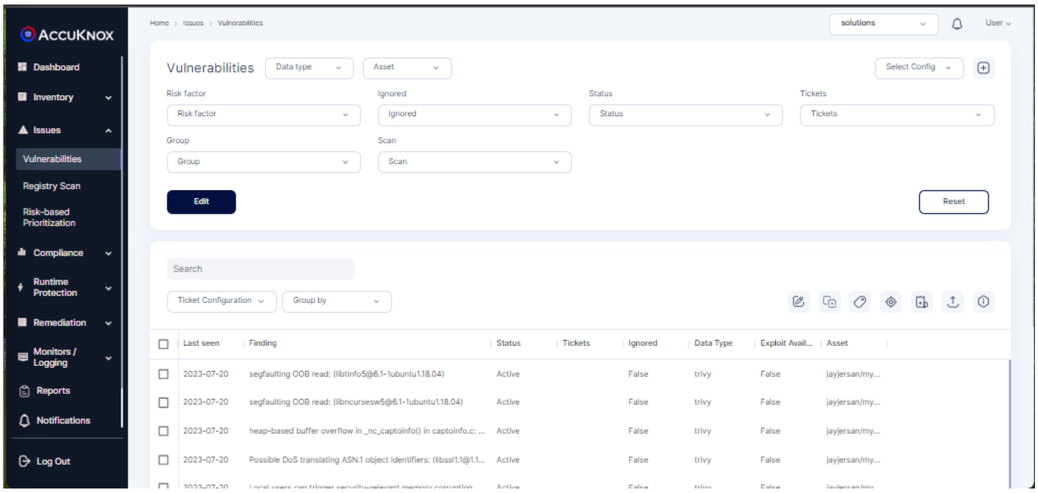
How to group by findings

1. Goto Issues tab, click on Vulnerabilities section



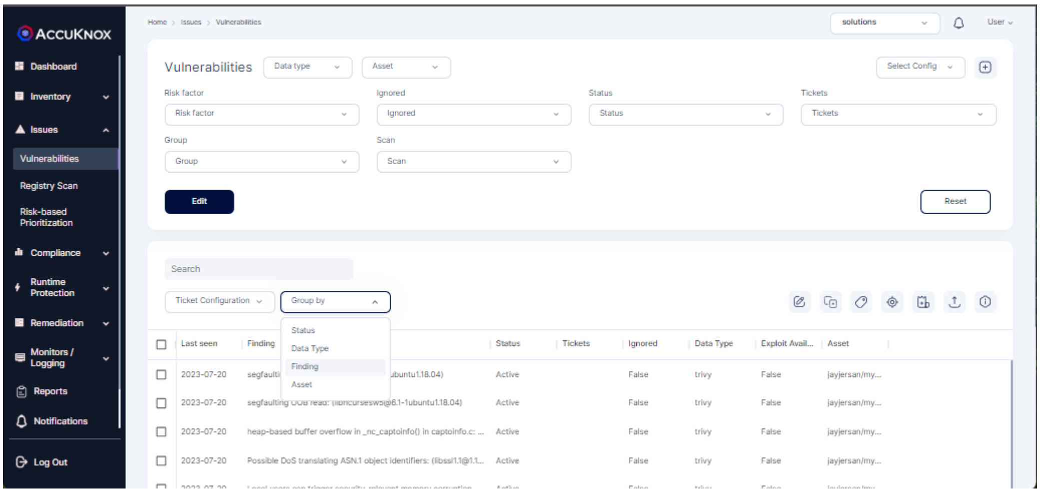
☐	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
☐	2023-07-20	segfaulting OOB read: (libtinfo5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	segfaulting OOB read: (libncursesw5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: ...	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	Possible DoS translating ASN.1 object identifiers: (libssl1.1@1.1...	Active		False	trivy	False	jayjersan/my...

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



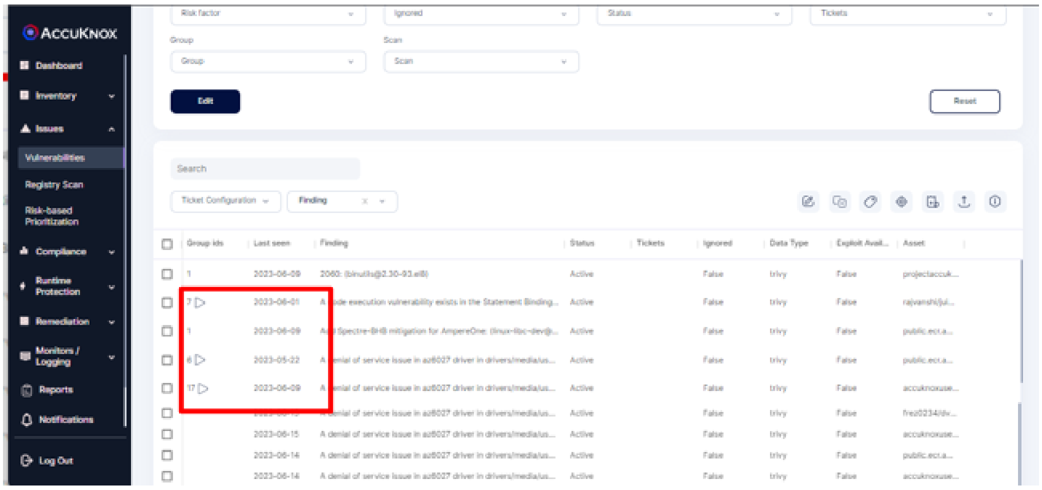
☐	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
☐	2023-07-20	segfaulting OOB read: (libtinfo5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	segfaulting OOB read: (libncursesw5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: ...	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	Possible DoS translating ASN.1 object identifiers: (libssl1.1@1.1...	Active		False	trivy	False	jayjersan/my...

Click on it and choose ***Findings***



☐	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
☐	2023-07-20	segfaulti... ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	segfaulting OOB read: (libncursesw5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: ...	Active		False	trivy	False	jayjersan/my...
☐	2023-07-20	Possible DoS translating ASN.1 object identifiers: (libssl1.1@1.1...	Active		False	trivy	False	jayjersan/my...

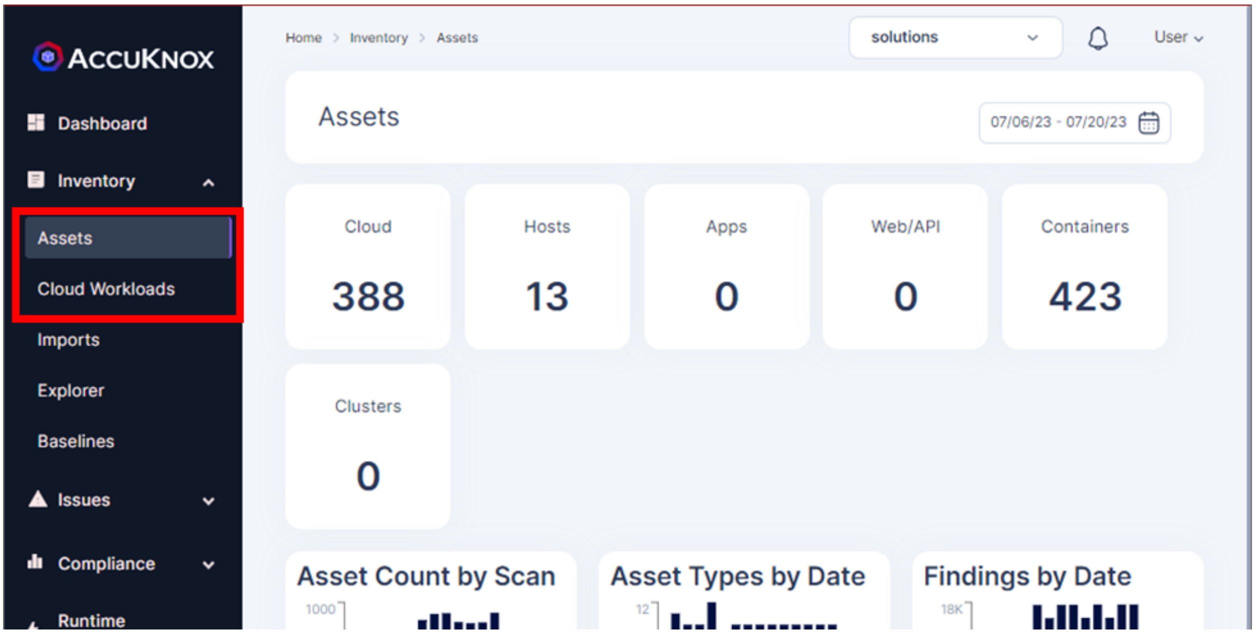
Now, you can see that similar findings are grouped. On clicking the arrow button in the findings list, you will be able to view all the assets it is found in



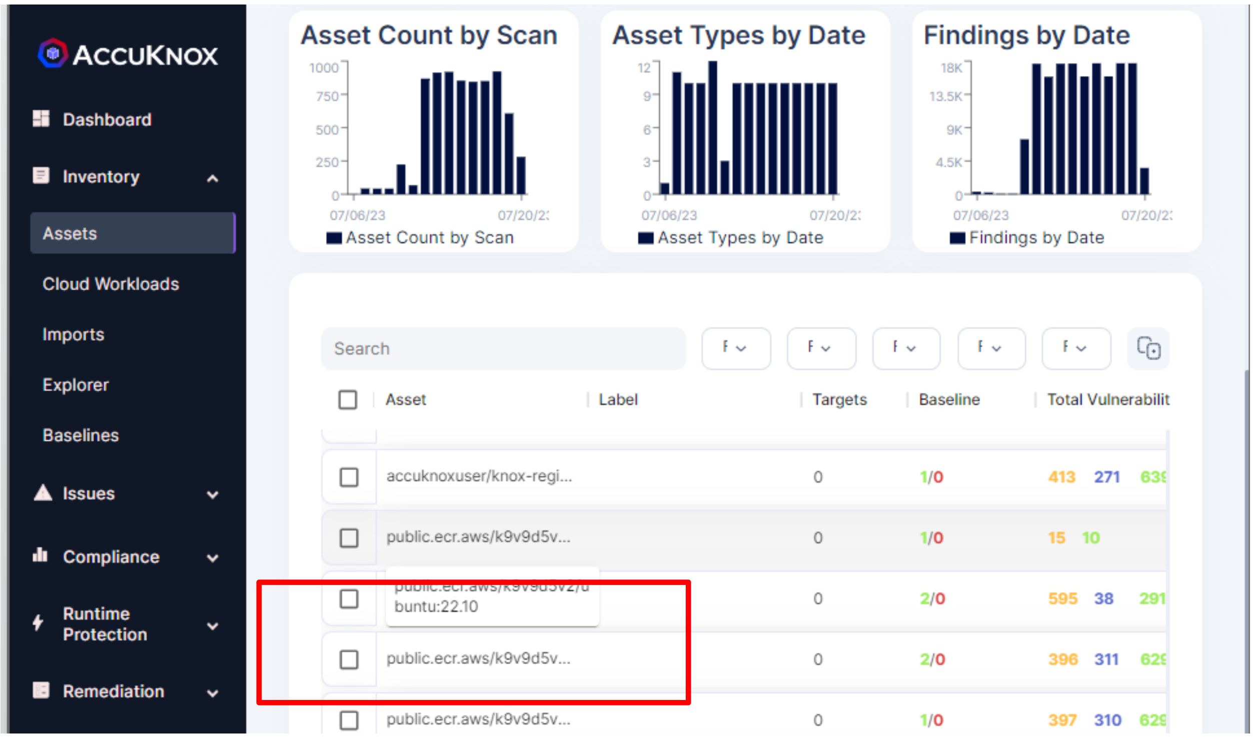
☐	Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
☐	1	2023-06-09	2060: (binutils@2.30-93.el8)	Active		False	trivy	False	projectaccuk...
☐	7 ▷	2023-06-01	A [illegible]ode execution vulnerability exists in the Statement Binding...	Active		False	trivy	False	rajvanshi/jul...
☐	1	2023-06-09	A[illegible] Spectre-BHB mitigation for AmpereOne: (linux-libc-dev@...	Active		False	trivy	False	public.ecr.a...
☐	6 ▷	2023-05-22	A [illegible]enial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	public.ecr.a...
☐	17 ▷	2023-06-09	A [illegible]enial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	accuknoxuse...
☐		[illegible]	[illegible]enial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	frez0234/dv...
☐		2023-06-15	A denial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	accuknoxuse...
☐		2023-06-14	A denial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	public.ecr.a...
☐		2023-06-14	A denial of service issue in az6007 driver in drivers/media/us...	Active		False	trivy	False	accuknoxuse...

How to group by criticality and Status

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

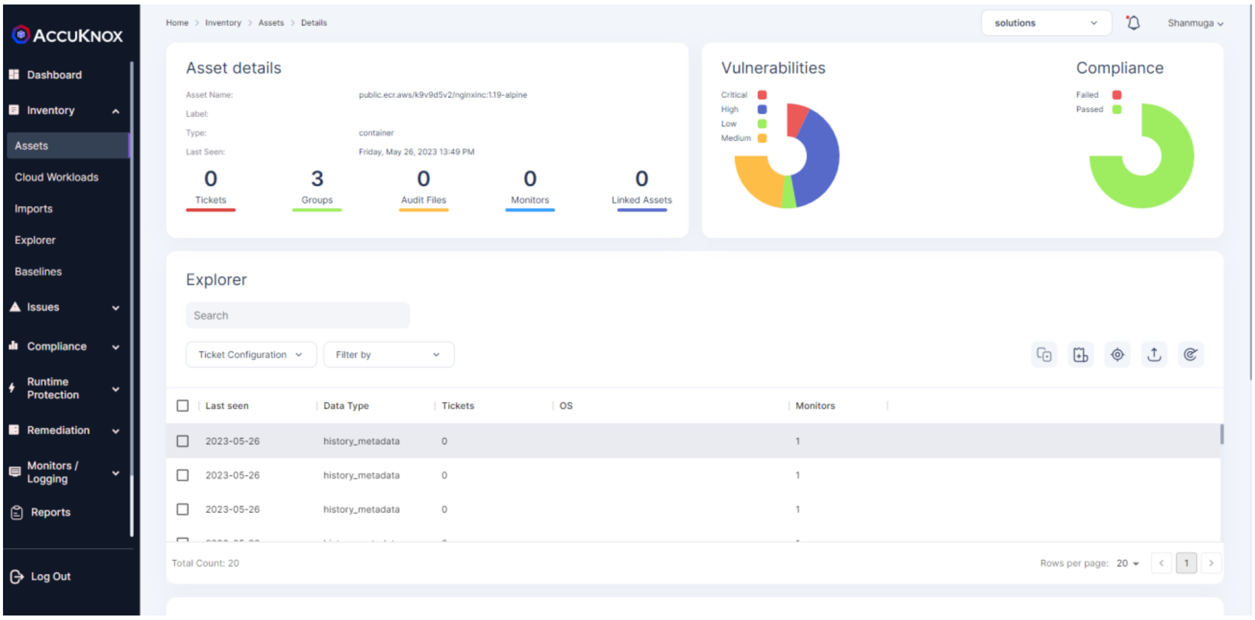


2. Scroll down and click on the particular asset for which misconfiguration need to be viewed



□	Asset	Label	Targets	Baseline	Total Vulnerabilit
□	accuknoxuser/knox-regi...		0	1/0	413 271 639
□	public.ecr.aws/k9v9d5v...		0	1/0	15 10
□	public.ecr.aws/k9v9d5v2/ubuntu:22.10		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

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



Asset details

Asset Name: public.ecr.aws/k9v9d5v2/nginxinc:1.19-alpine

Label:

Type: container

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

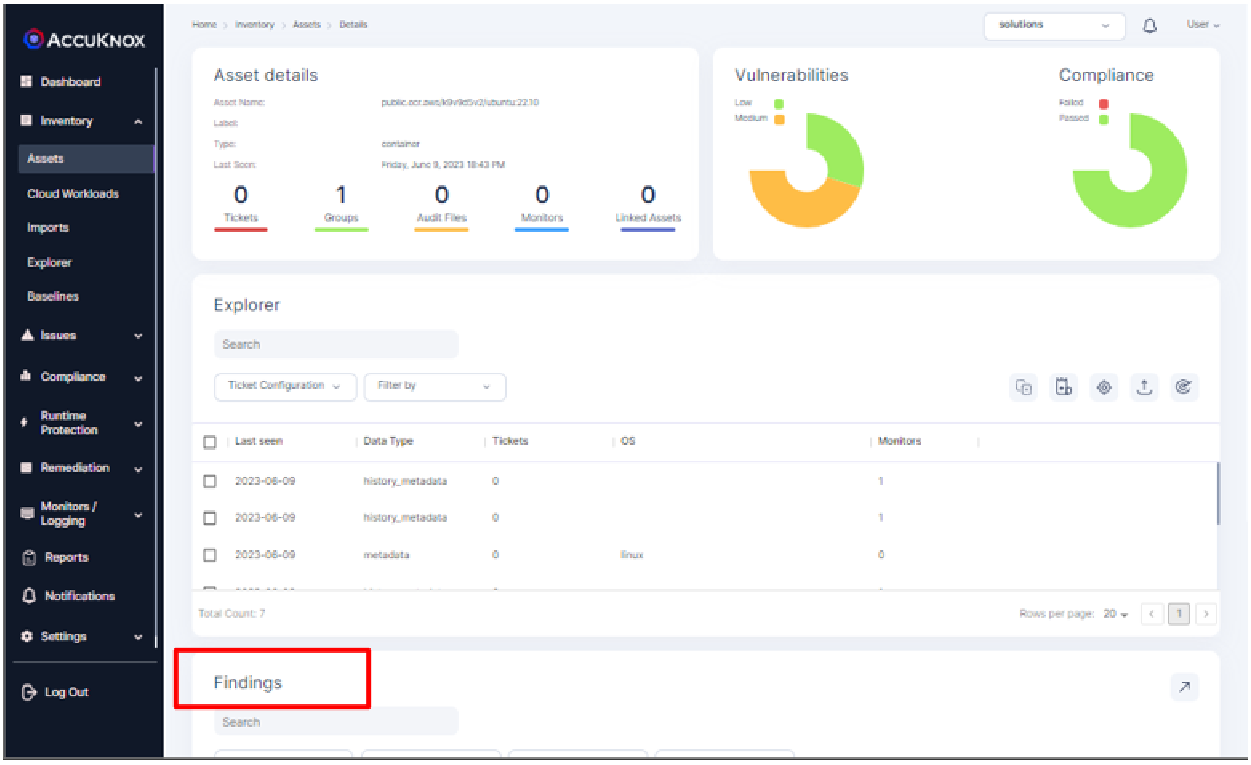
0 Tickets | 3 Groups | 0 Audit Files | 0 Monitors | 0 Linked Assets

Explorer

□	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



Asset details

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

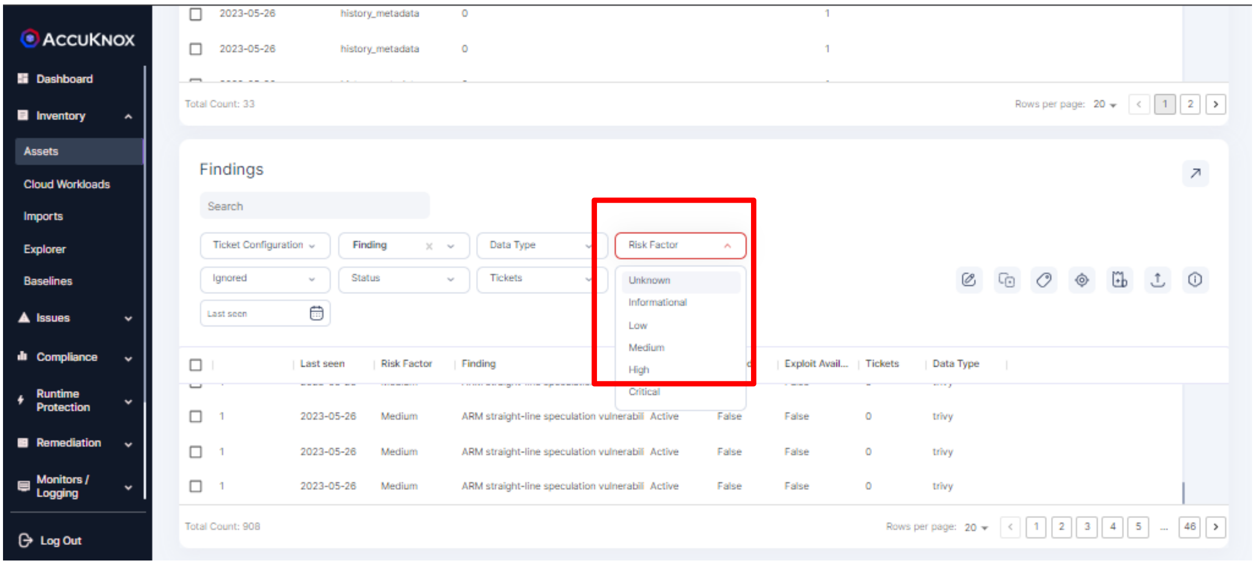
0	1	0	0	0
Tickets	Groups	Audit Files	Monitors	Linked Assets

Explorer

□	Last seen	Data Type	Tickets	OS	Monitors
□	2023-06-09	history_metadata	0		1
□	2023-06-09	history_metadata	0		1
□	2023-06-09	metadata	0	linux	0

Total Count: 7 Rows per page: 20

Navigate to the Risk Factor filter and choose the severity level.



□	2023-05-26	history_metadata	0	1
□	2023-05-26	history_metadata	0	1

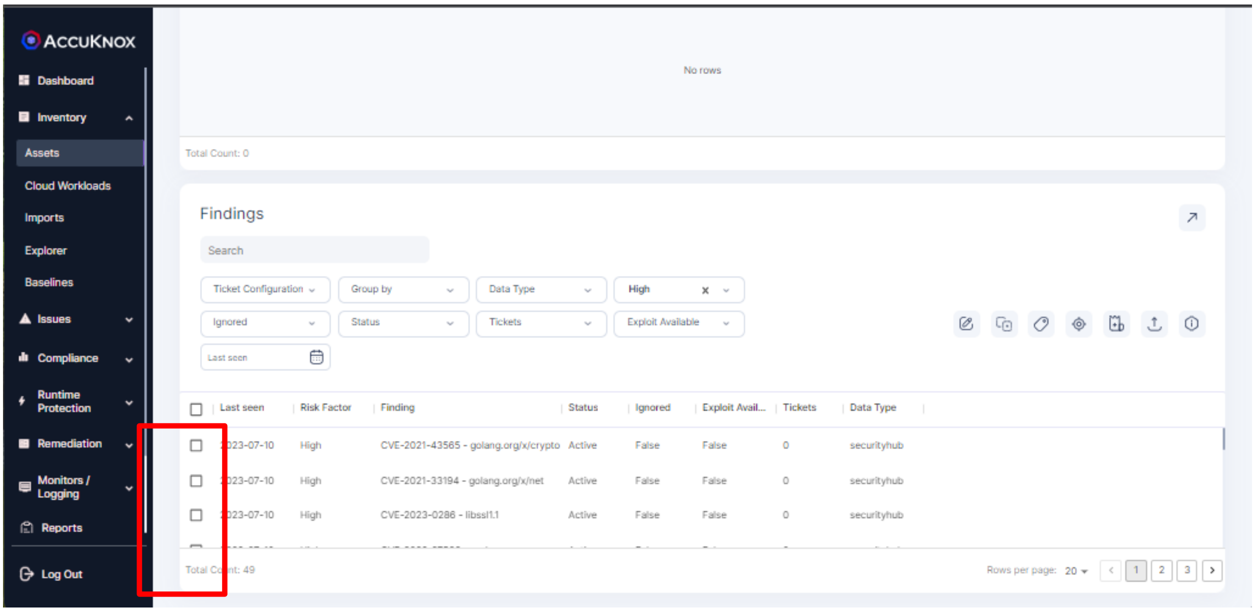
Total Count: 33 Rows per page: 20 1 2

Findings

□		Last seen	Risk Factor	Finding			Exploit Avail...	Tickets	Data Type
□	1	2023-05-26	Medium	ARM straight-line speculation vulnerabil	Active	False	False	0	trivy
□	1	2023-05-26	Medium	ARM straight-line speculation vulnerabil	Active	False	False	0	trivy
□	1	2023-05-26	Medium	ARM straight-line speculation vulnerabil	Active	False	False	0	trivy

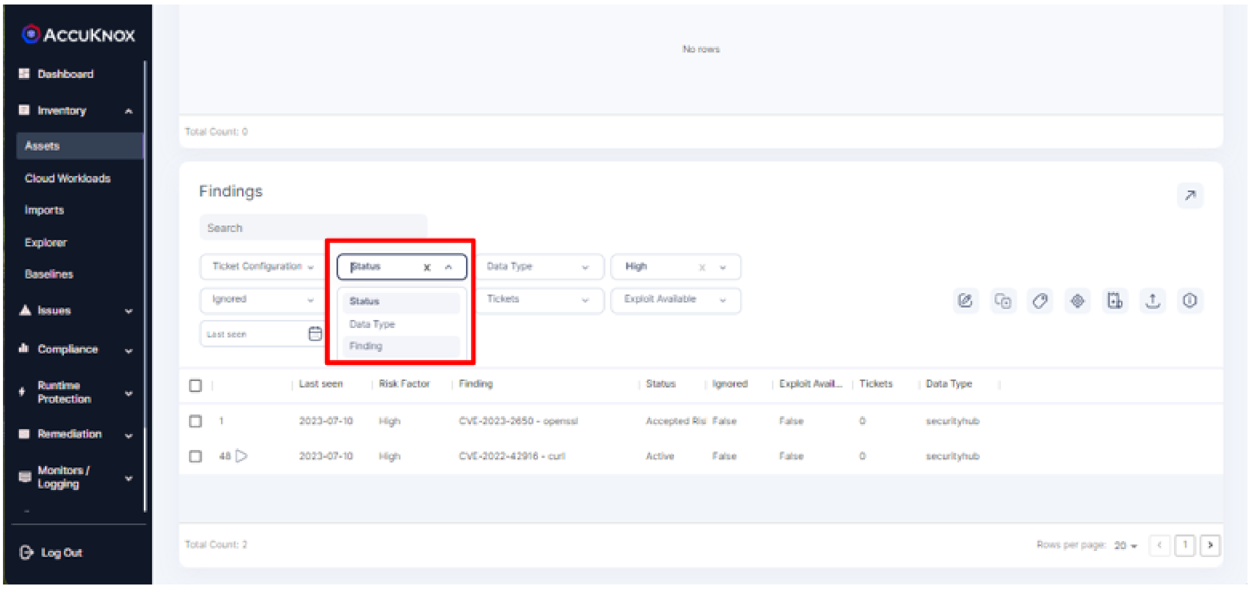
Total Count: 908 Rows per page: 20 1 2 3 4 5 ... 46

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



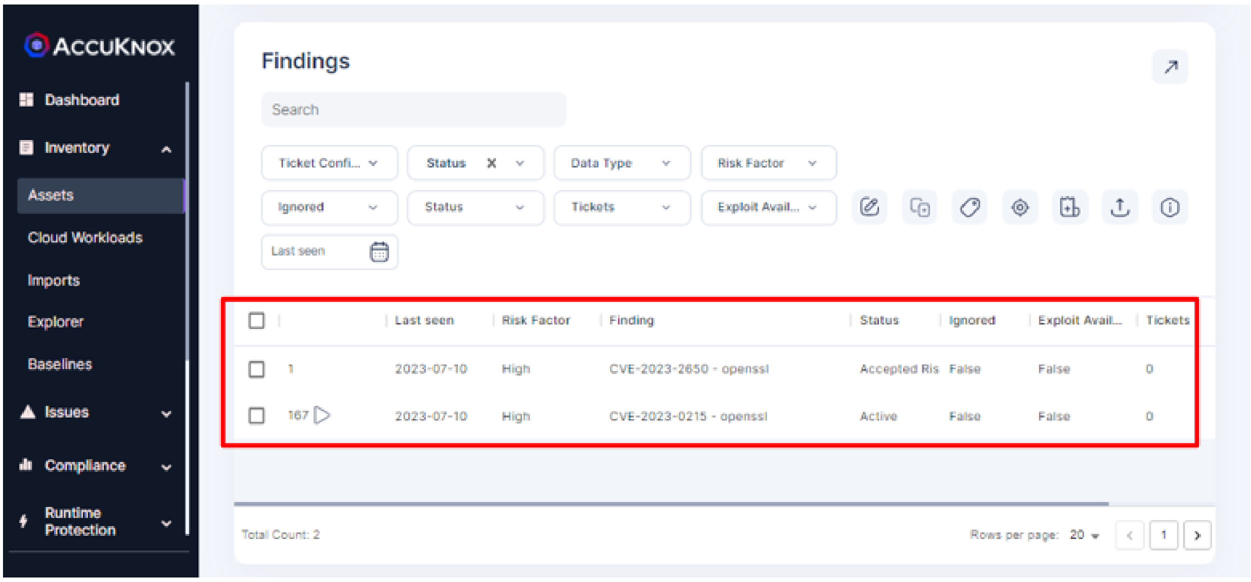
□	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
□	2023-07-10	High	CVE-2021-43565 - golang.org/x/crypto	Active	False	False	0	securityhub
□	2023-07-10	High	CVE-2021-33194 - golang.org/x/net	Active	False	False	0	securityhub
□	2023-07-10	High	CVE-2023-0286 - libssl1.1	Active	False	False	0	securityhub

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



□		Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
□	1	2023-07-10	High	CVE-2023-2650 - openssl	Accepted Ris	False	False	0	securityhub
□	48 ▷	2023-07-10	High	CVE-2022-42916 - curl	Active	False	False	0	securityhub

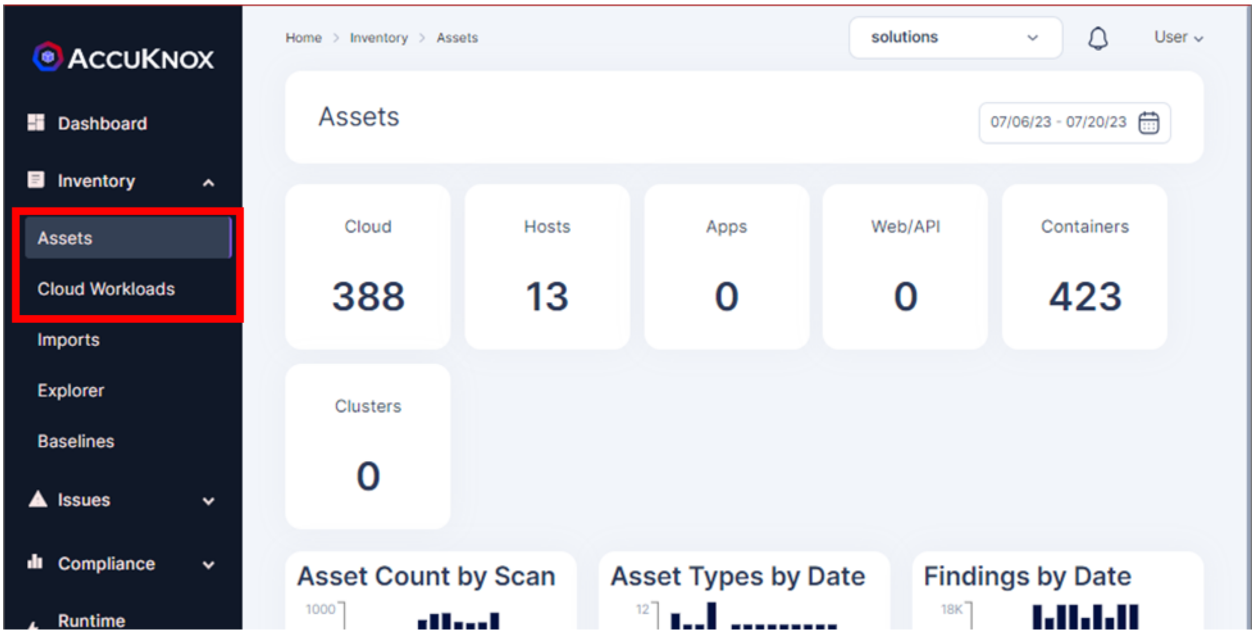
Now, you can view the findings grouped by the status, such as active and accepted risk



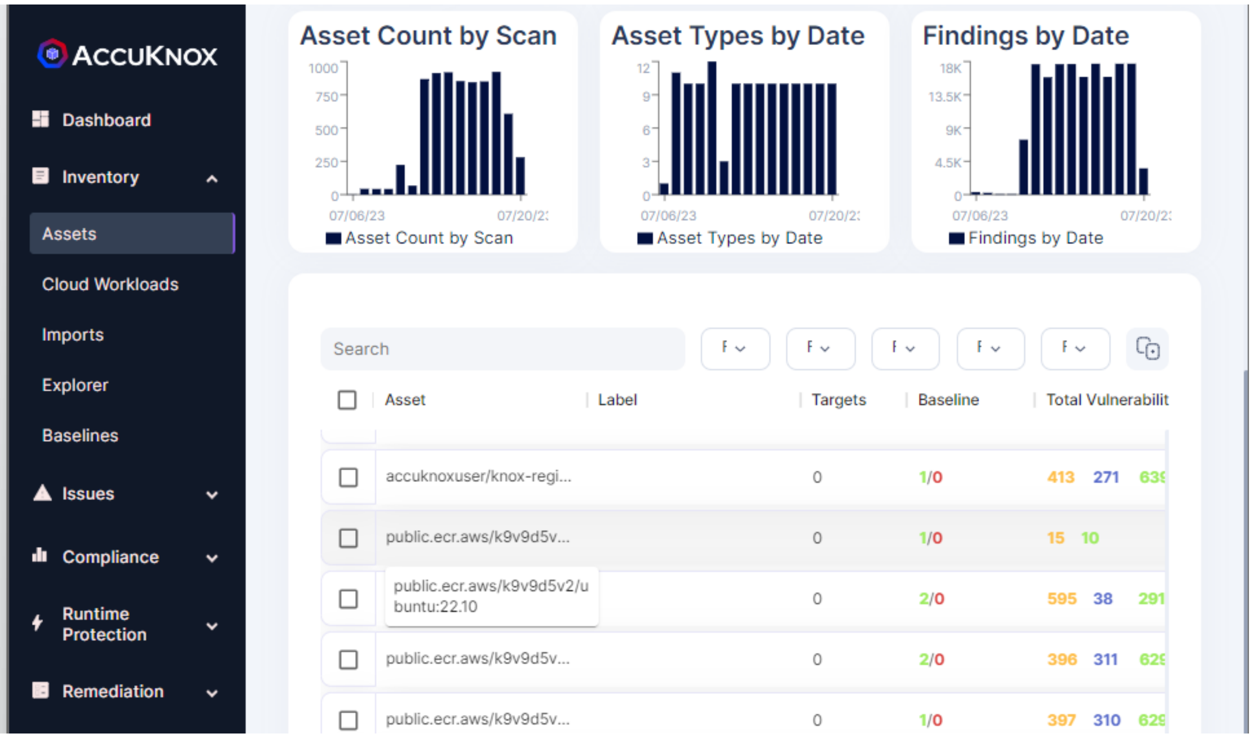
		Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets
□	1	2023-07-10	High	CVE-2023-2650 - openssl	Accepted Ris	False	False	0
□	167 ▷	2023-07-10	High	CVE-2023-0215 - openssl	Active	False	False	0

How to create a ticket

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

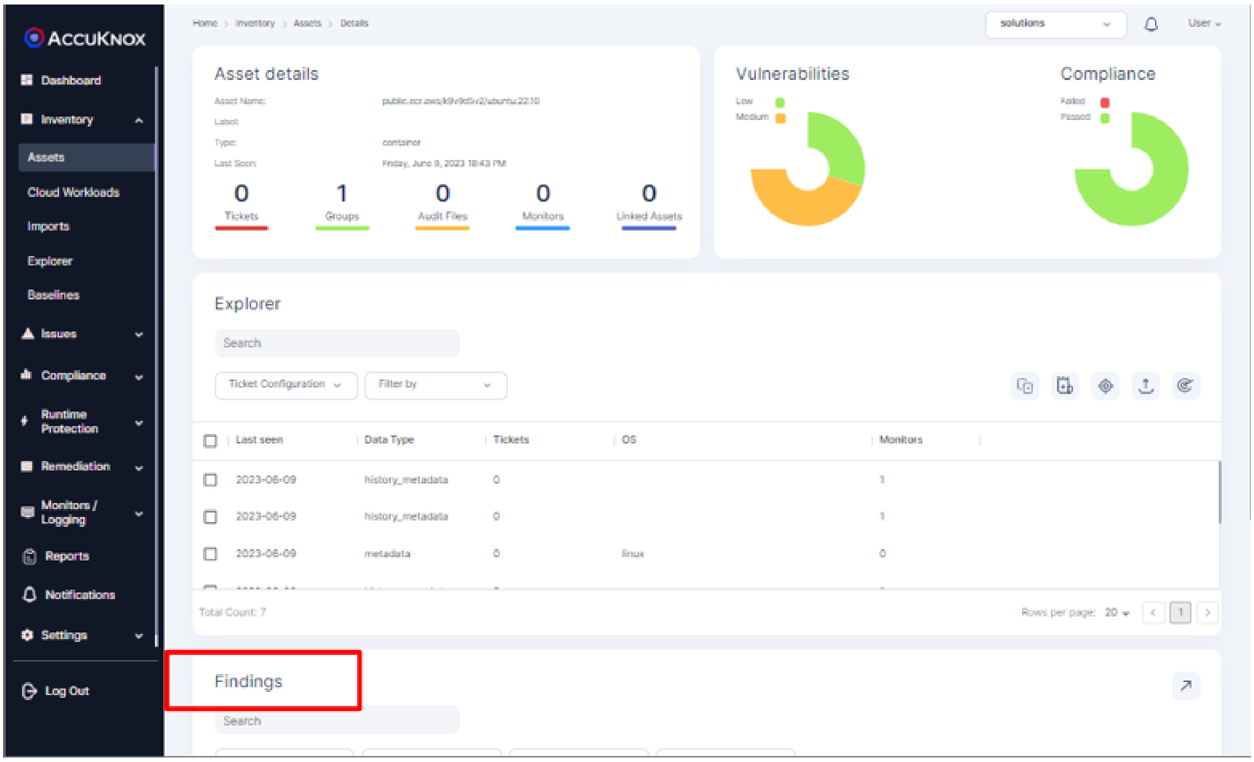


a. Scroll down and click on the particular asset for which misconfiguration need to be viewed



☐	Asset	Label	Targets	Baseline	Total Vulnerabilit
☐	accuknoxuser/knox-regi...		0	1/0	413 271 639
☐	public.ecr.aws/k9v9d5v...		0	1/0	15 10
☐	public.ecr.aws/k9v9d5v2/ubuntu:22.10		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

b. 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

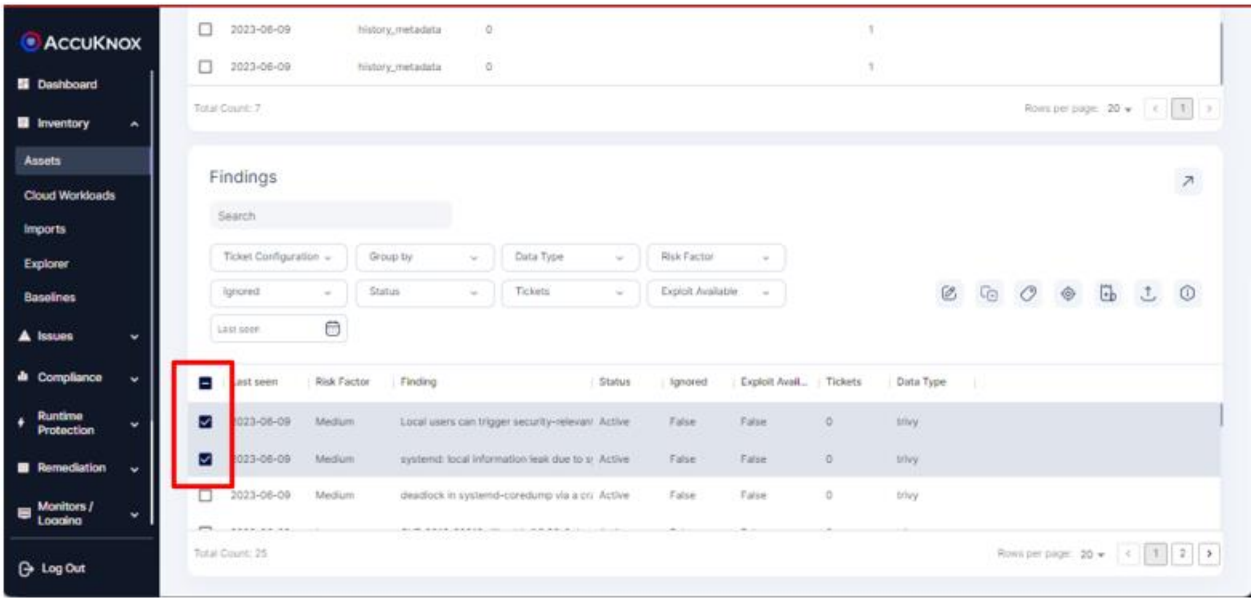
0 Tickets | 1 Groups | 0 Audit Files | 0 Monitors | 0 Linked Assets

Explorer

☐	Last seen	Data Type	Tickets	OS	Monitors
☐	2023-06-09	history_metadata	0		1
☐	2023-06-09	history_metadata	0		1
☐	2023-06-09	metadata	0	linux	0

Total Count: 7 Rows per page: 20

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

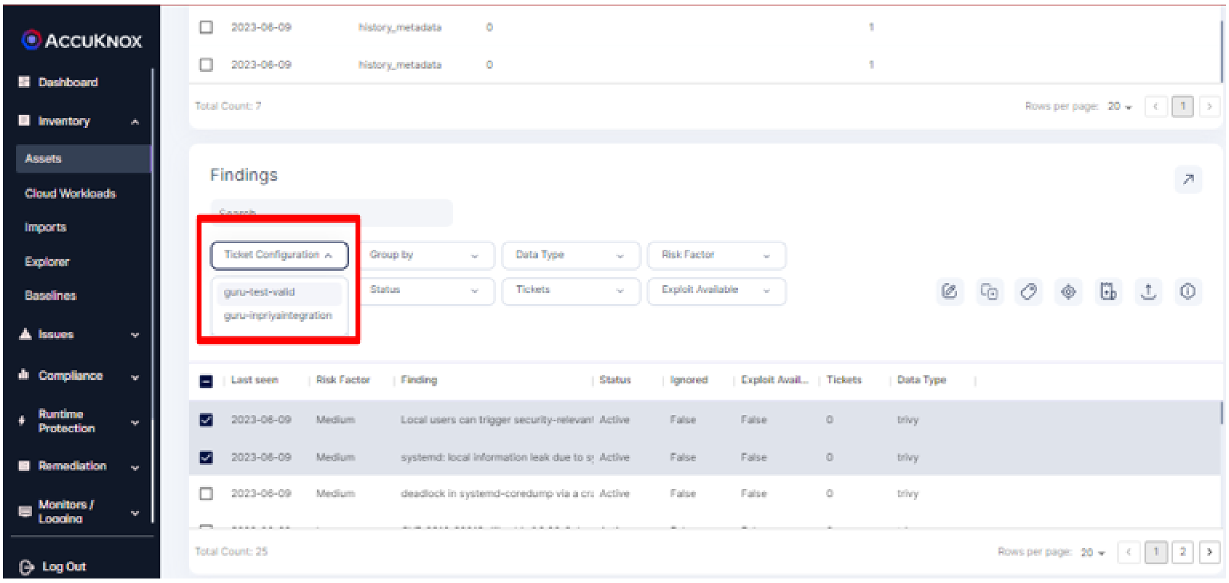


□	2023-06-09	history_metadata	0		1
□	2023-06-09	history_metadata	0		1

Total Count: 7

☑	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
☑	2023-06-09	Medium	Local users can trigger security-relevan	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

Total Count: 25



□	2023-06-09	history_metadata	0		1
□	2023-06-09	history_metadata	0		1

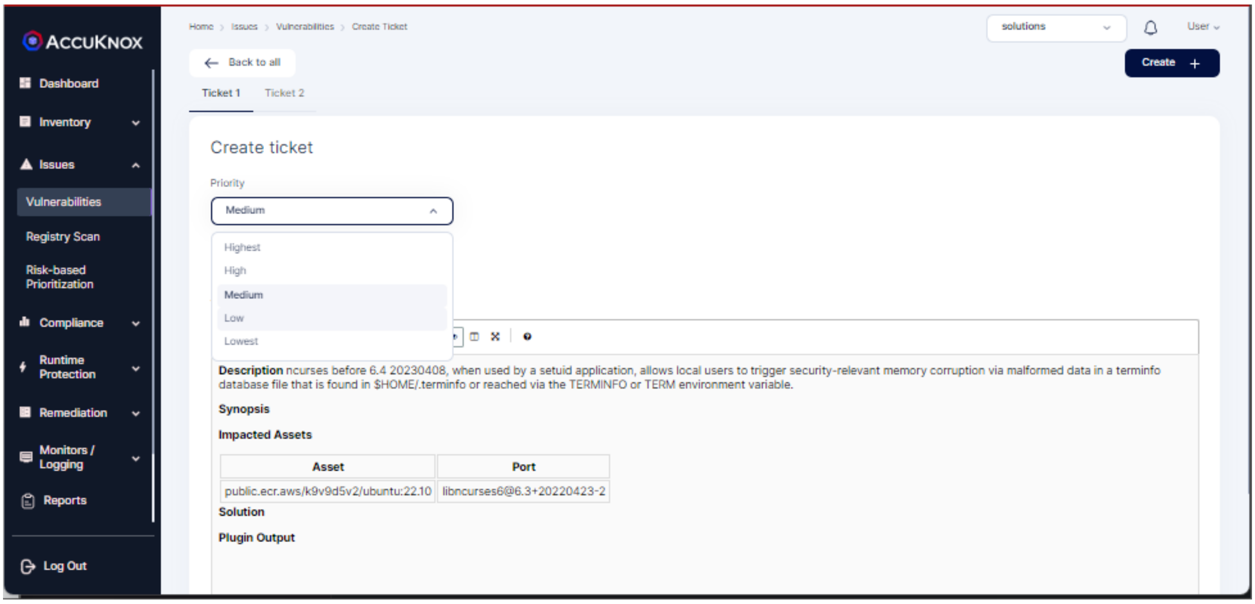
Total Count: 7

☑	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
☑	2023-06-09	Medium	Local users can trigger security-relevan	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

Total Count: 25

Select the desired ticket configuration by which ticket will be created (Create a ticket configuration if it does not exist already)

d. Choose the ***Priority*** from the dropdown.



Description ncurses before 6.4 20230408, when used by a setuid application, allows local users to trigger security-relevant memory corruption via malformed data in a terminfo database file that is found in $HOME/.terminfo or reached via the TERMINFO or TERM environment variable.

Synopsis

Impacted Assets

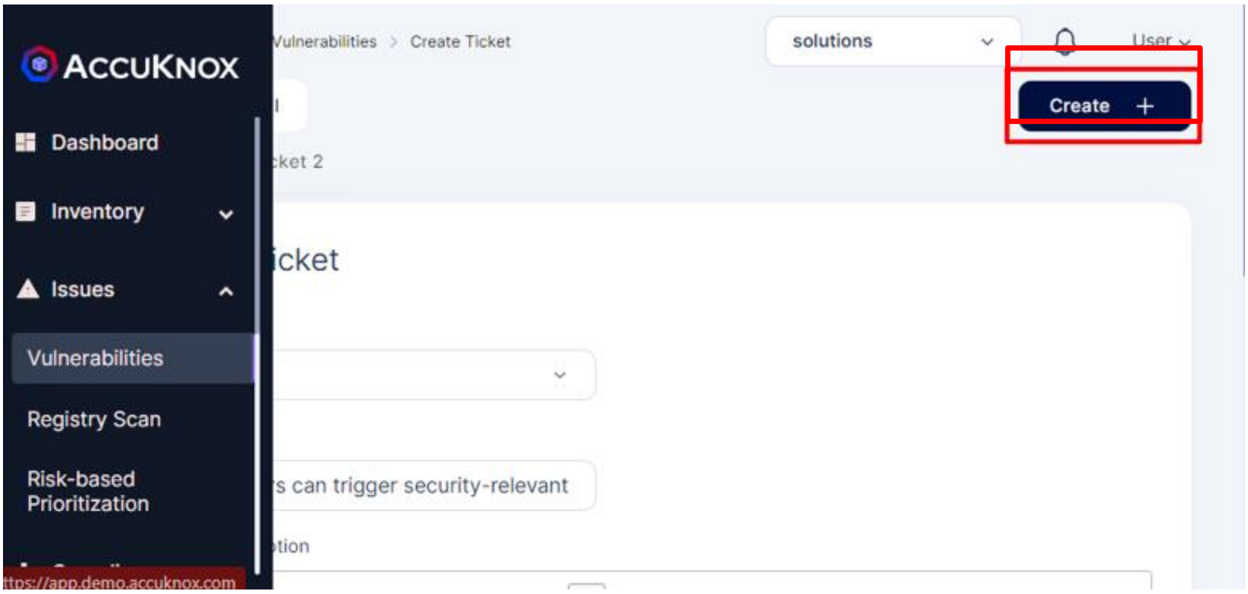
Asset	Port
public.ecr.aws/k9v9d5v2/ubuntu:22.10	libncurses6@6.3+20220423-2

Solution

Plugin Output

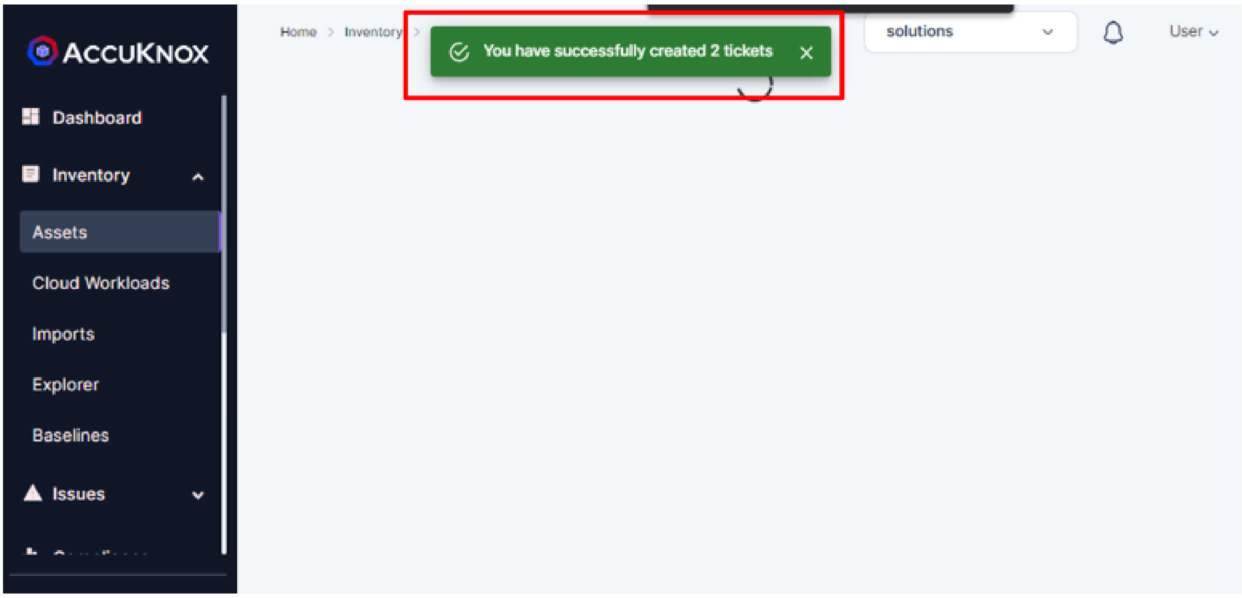
1. Edit the Ticket Title and Ticket Description, as required.

2. Click on the Create button at the top right corner.



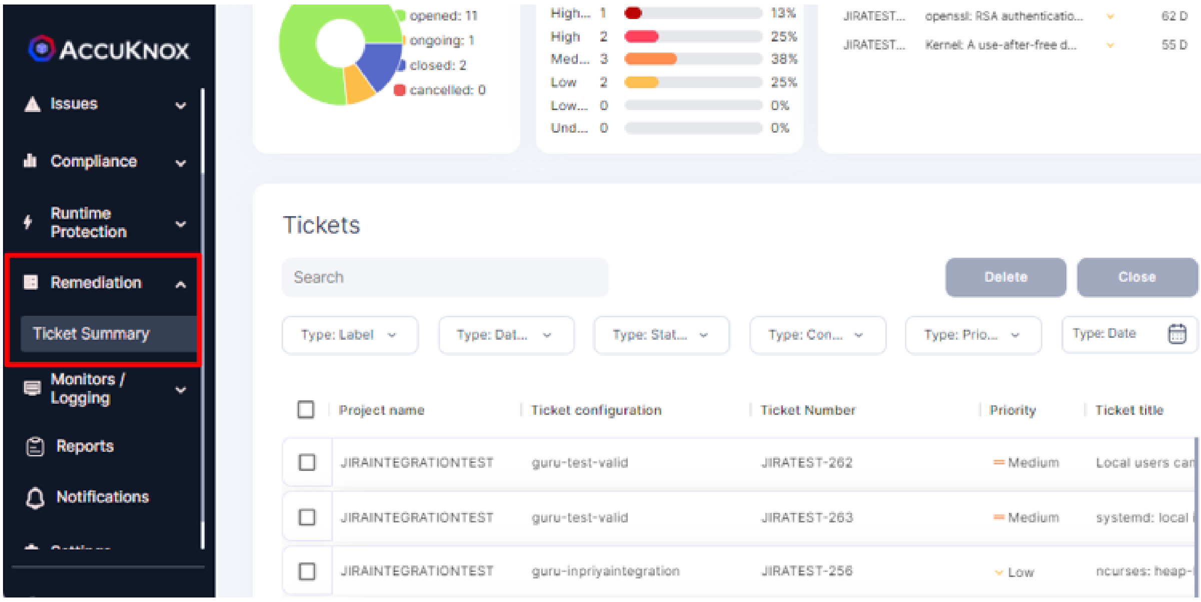
ACCUKNOX
Dashboard
Inventory
Issues
Vulnerabilities
Registry Scan
Risk-based Prioritization
Vulnerabilities > Create Ticket
solutions
User
Create +
ket 2
icket
s can trigger security-relevant
tion
ttps://app.demo.accuknox.com

You can see the tickets were created successfully.



You have successfully created 2 tickets

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



Tickets

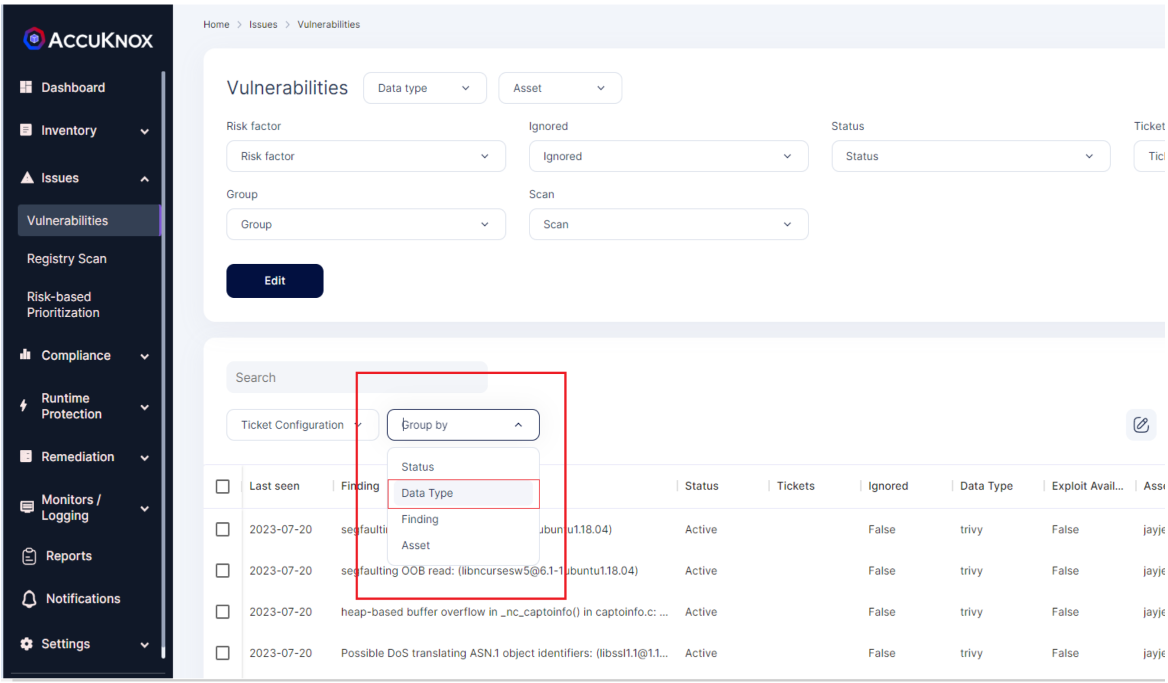
☐	Project name	Ticket configuration	Ticket Number	Priority	Ticket title
☐	JIRAINTEGRATIONTEST	guru-test-valid	JIRATEST-262	Medium	Local users can
☐	JIRAINTEGRATIONTEST	guru-test-valid	JIRATEST-263	Medium	systemd: local
☐	JIRAINTEGRATIONTEST	guru-inpriyaintegration	JIRATEST-256	Low	ncurses: heap-

Issues/Vulnerabilities

Group findings by source and severity

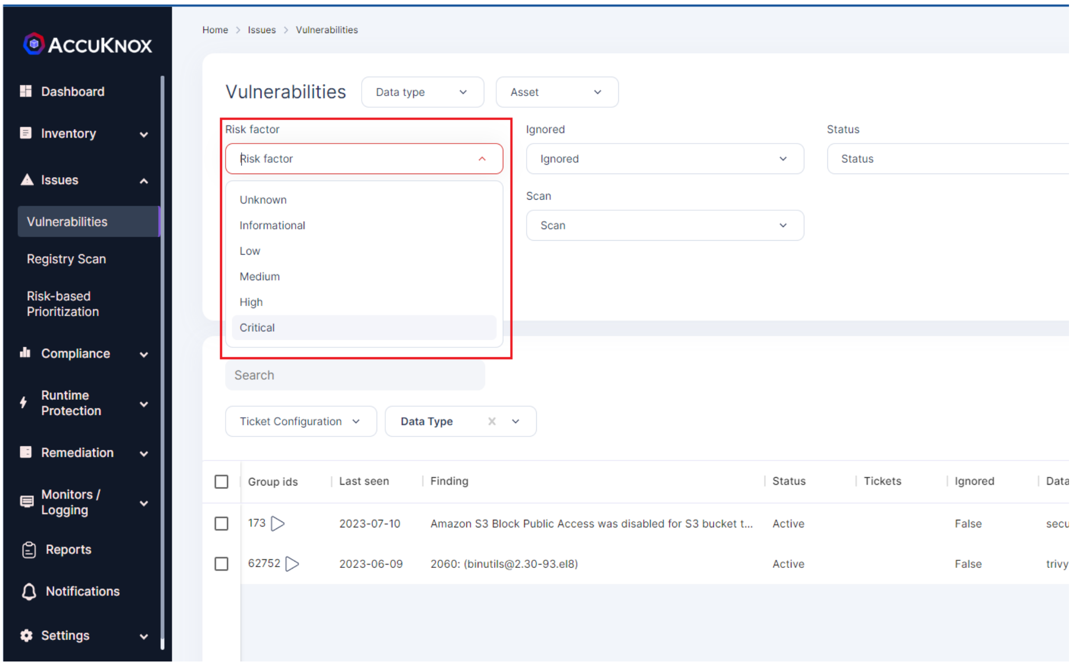
AccuKnox automatically scans assets with the help of various open-source tools. It uses tools like Clair, Trivy, CLOC, Fortify, Snyk, SonarQube, Cloudsploit, Kube Bench, and various other open-source tools for Scanning.

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.



Last seen	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Ass
2023-07-20	segfaulti... ubuntu1.18.04)	Active		False	trivy	False	jayje
2023-07-20	segfaulting OOB read: (libncursesw5@6.1-1ubuntu1.18.04)	Active		False	trivy	False	jayje
2023-07-20	heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: ...	Active		False	trivy	False	jayje
2023-07-20	Possible DoS translating ASN.1 object identifiers: (libssl1.1@1.1...	Active		False	trivy	False	jayje

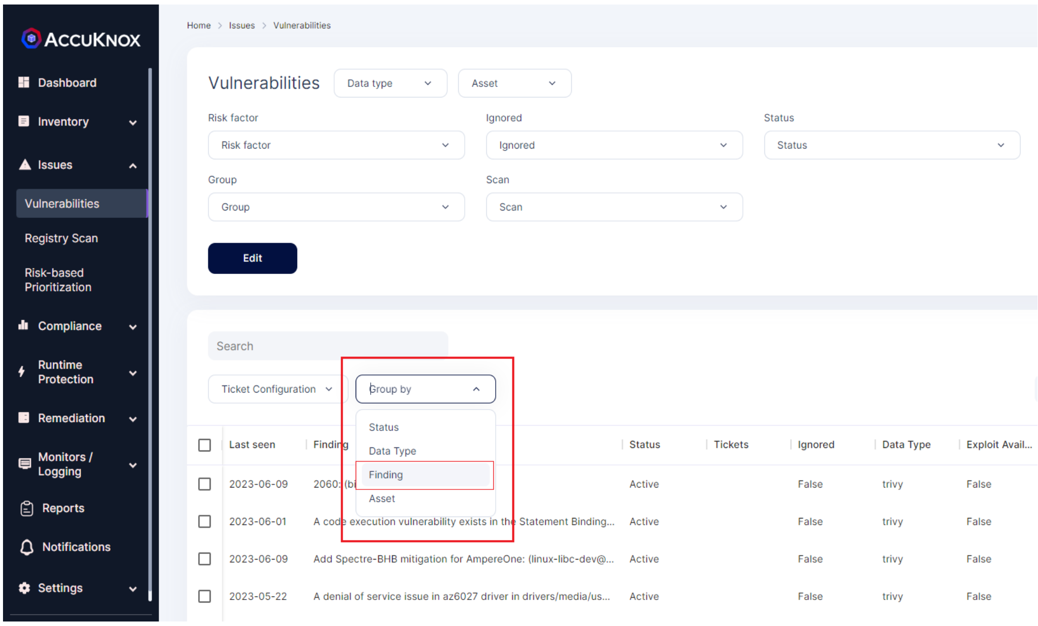
Users can further filter the findings with respect to their Risk factor so that they can have a view of the most critical findings from each tool being used.



Group ids	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

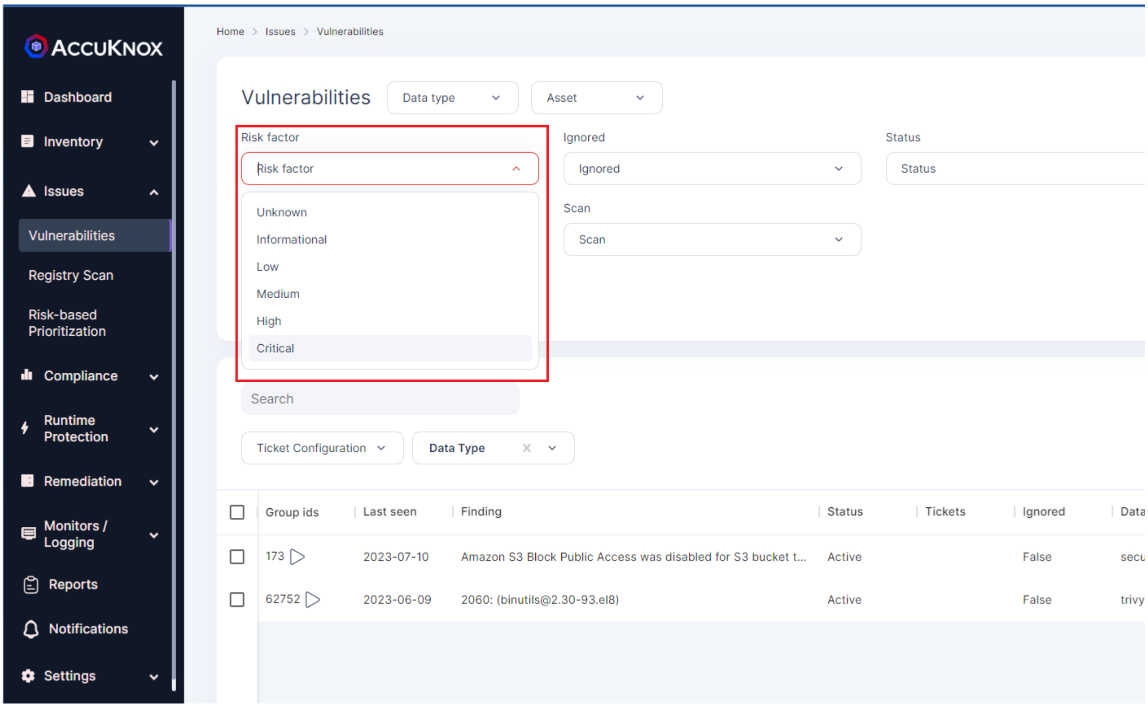
How to group by Findings and severity

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.



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

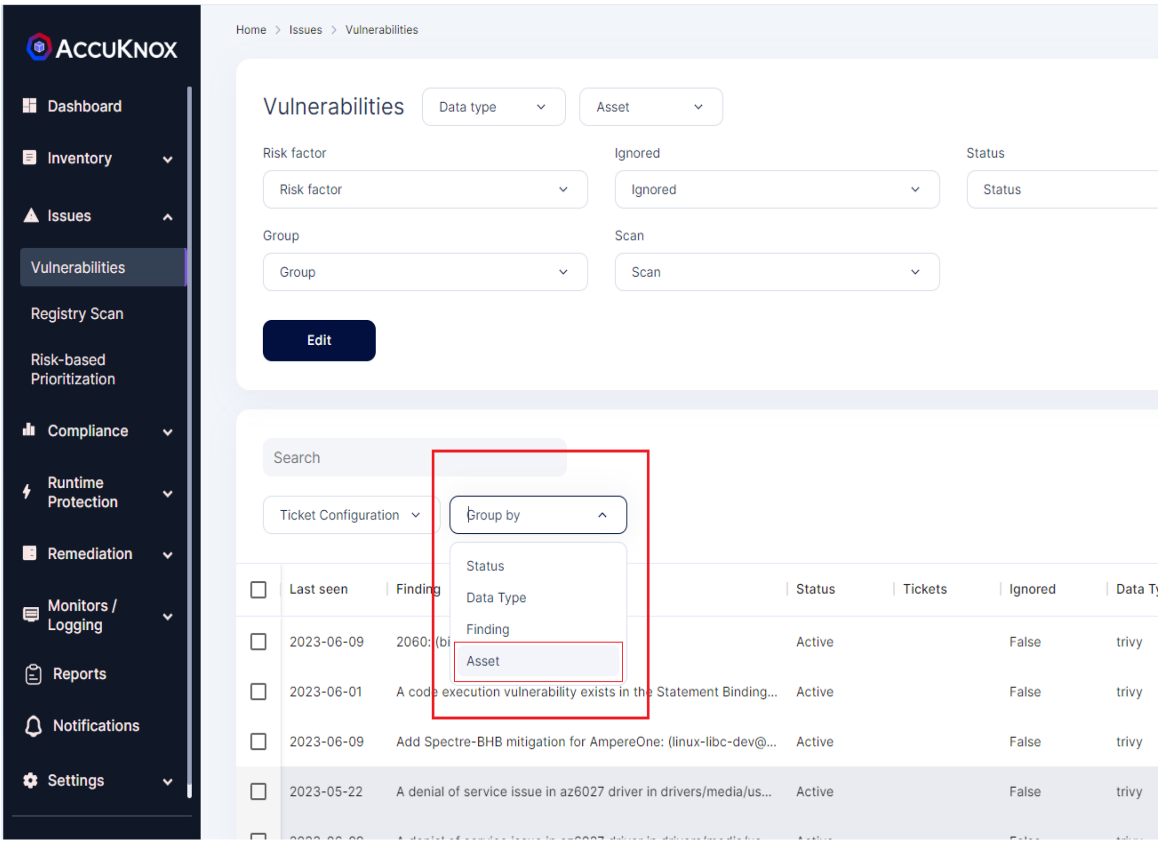
Further users can select the Risk Factor to filter the findings based on their severity. This again narrows the findings that need to be remediated.



□	Group ids	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

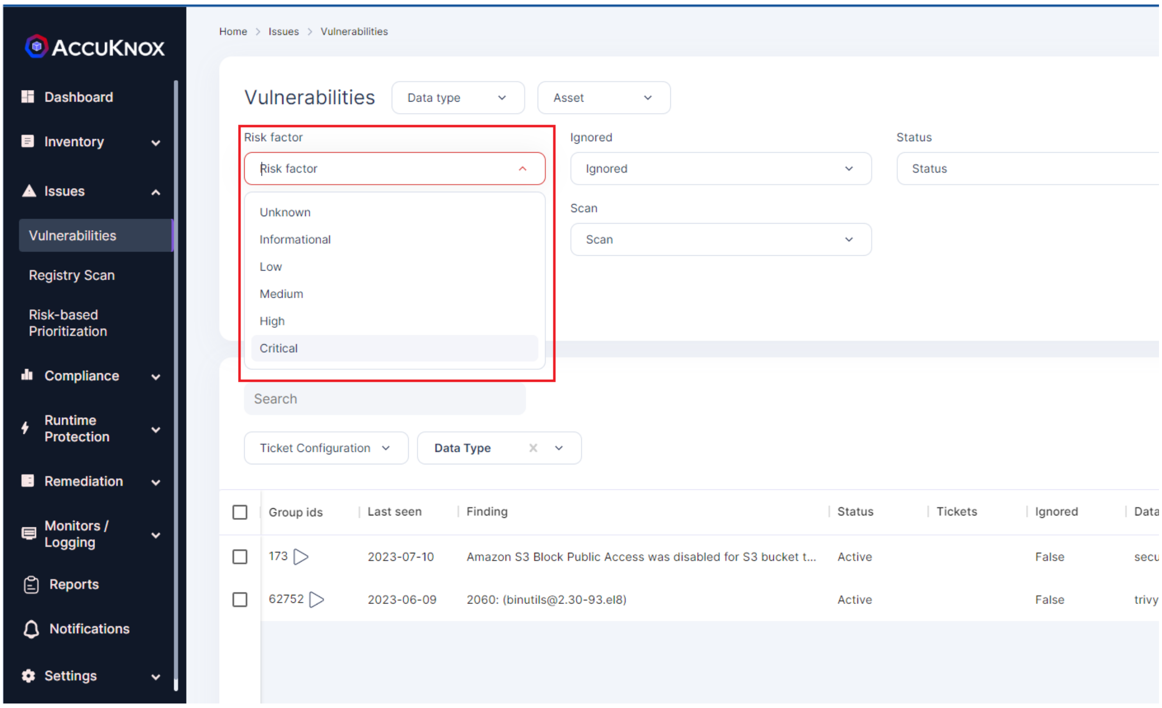
How to group by Asset and severity

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



☐	Last seen	Finding	Status	Tickets	Ignored	Data Ty
☐	2023-06-09	2060: (bi	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

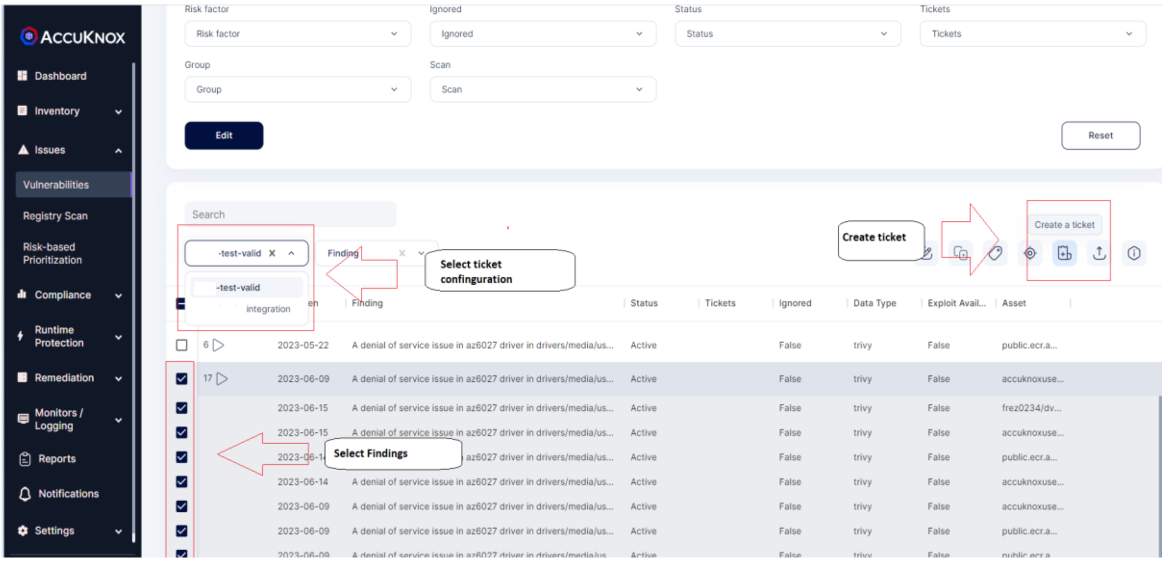
If coupled with the Risk factor filter, users can have a view of the most critical assets i.e., the assets that have the most no. of critical findings.



☐	Group ids	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 create automated tickets in Findings and Asset grouping

AccuKnox enables customers to manage 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.



		en	Finding	Status	Tickets	Ignored	Data Type	Exploit Avail...	Asset
☐	6 ▷	2023-05-22	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy	False	public.ecr.a...
☑	17 ▷	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	frez0234/dv...
☑		2023-06-15	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy	False	accuknoxuse...
☑		2023-06-1	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...
☑		2023-06-09	A denial of service issue in az6027 driver in drivers/media/us...	Active		False	trivy	False	accuknoxuse...
☑		2023-06-09	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	public.ecr.a

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 does registry scan happen?

AccuKnox CSPM tool provides 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.

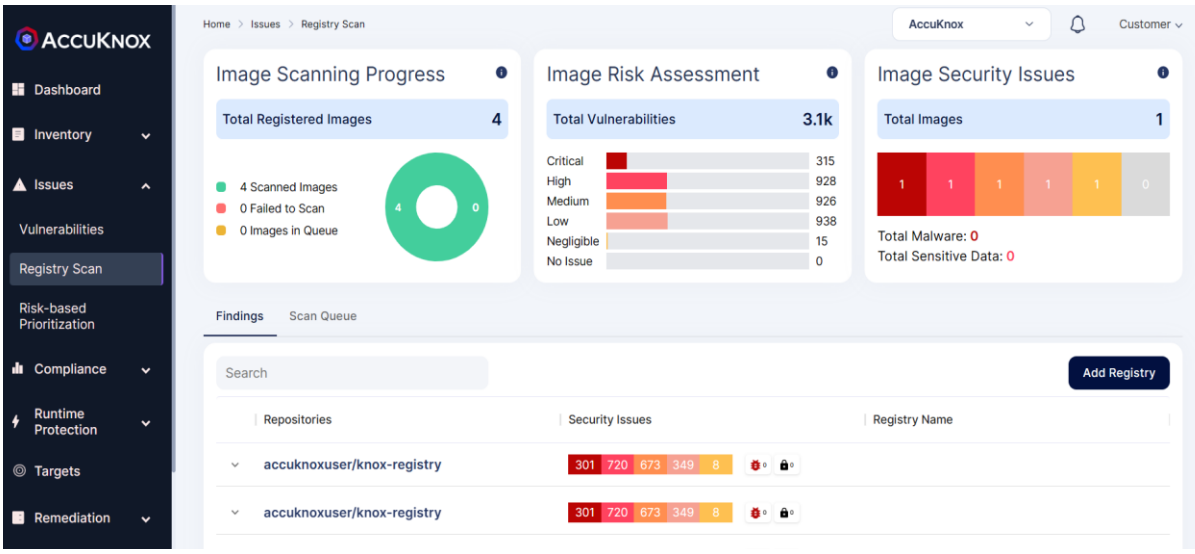


Image Scanning Progress

Total Registered Images 4

- 4 Scanned Images
- 0 Failed to Scan
- 0 Images in Queue

Image Risk Assessment

Total Vulnerabilities 3.1k

Critical	315
High	928
Medium	926
Low	938
Negligible	15
No Issue	0

Image Security Issues

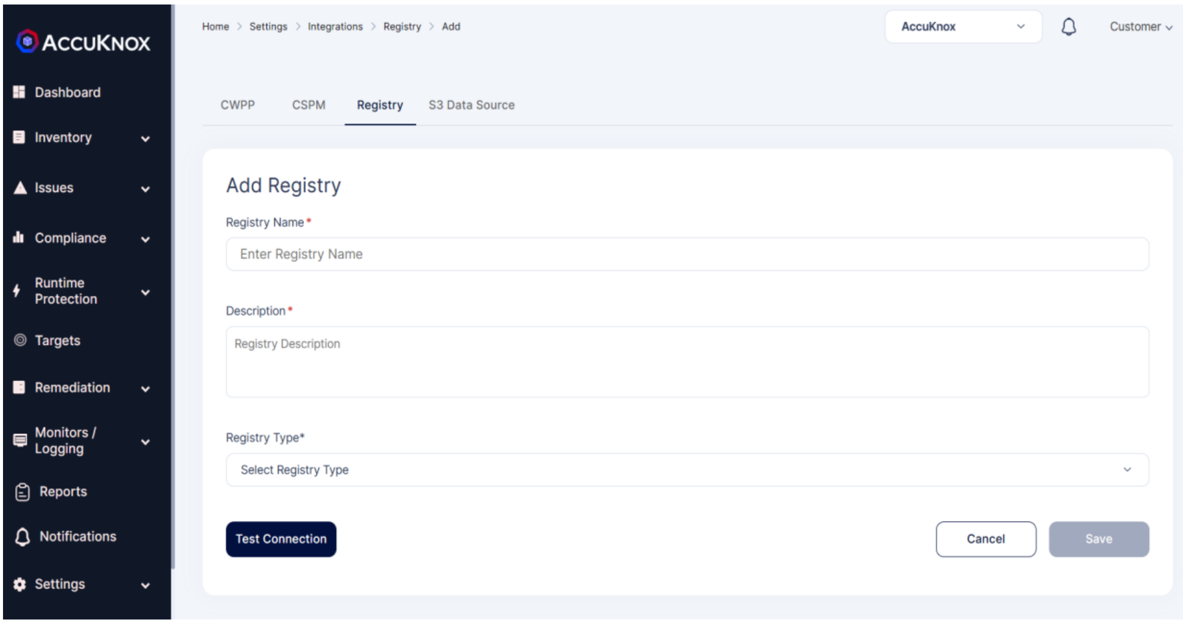
Total Images 1

Total Malware: 0

Total Sensitive Data: 0

Repositories	Security Issues	Registry Name
accuknoxuser/knox-registry	301 720 673 349 8	
accuknoxuser/knox-registry	301 720 673 349 8	

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.



Add Registry

Registry Name*

Enter Registry Name

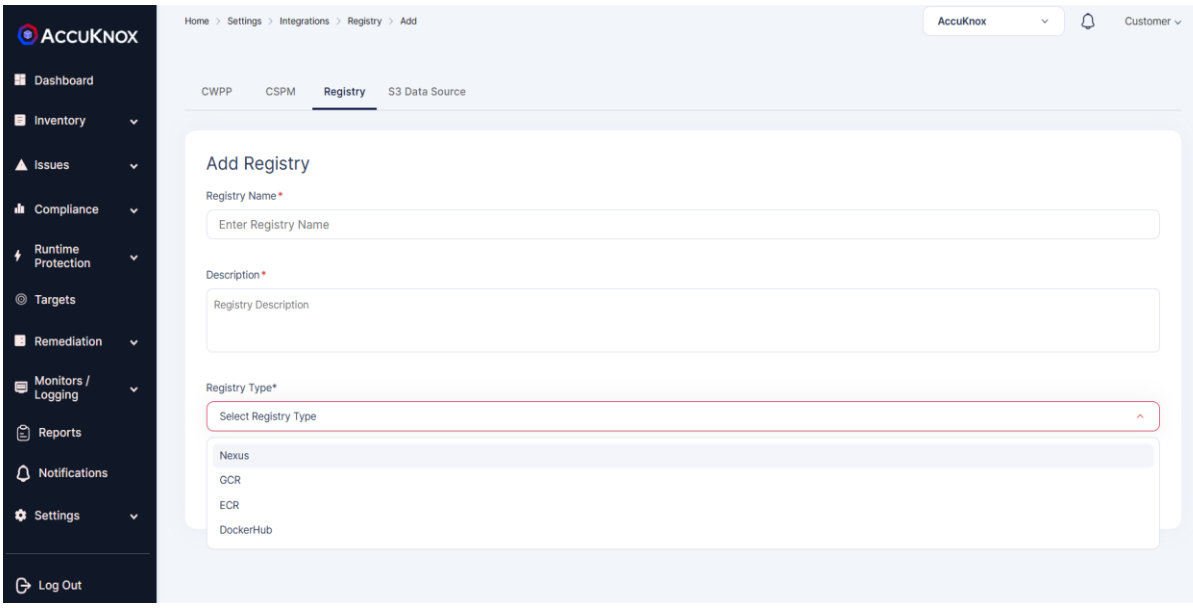
Description*

Registry Description

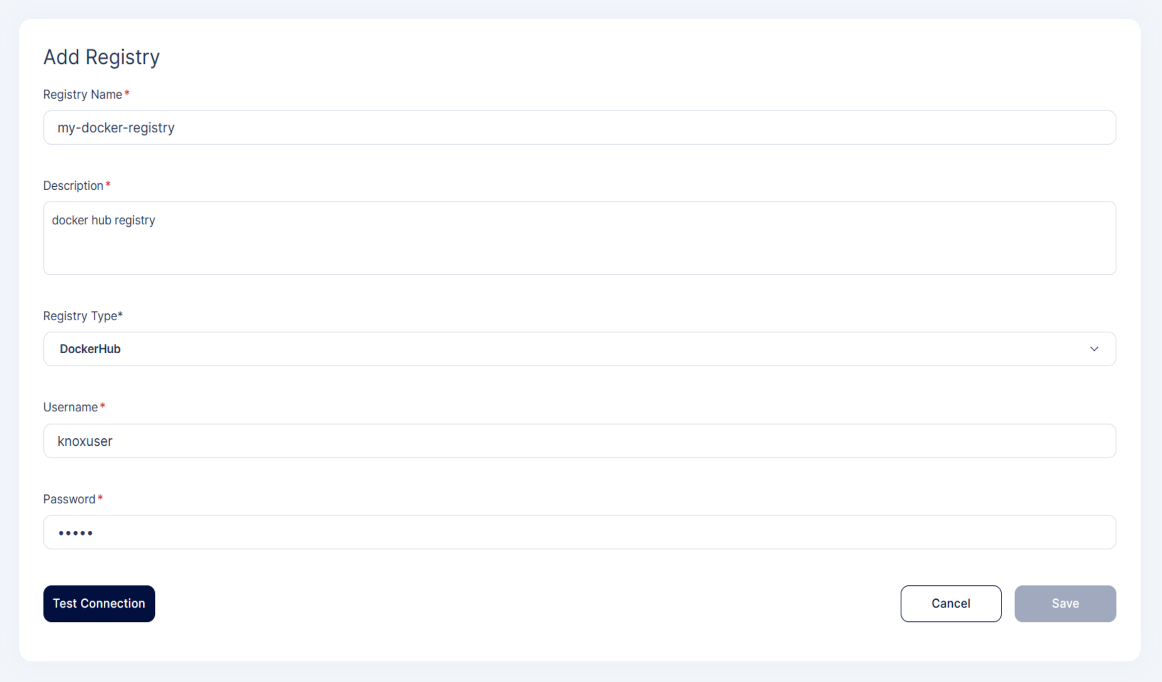
Registry Type*

Select Registry Type

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



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



Registry Name *: my-docker-registry

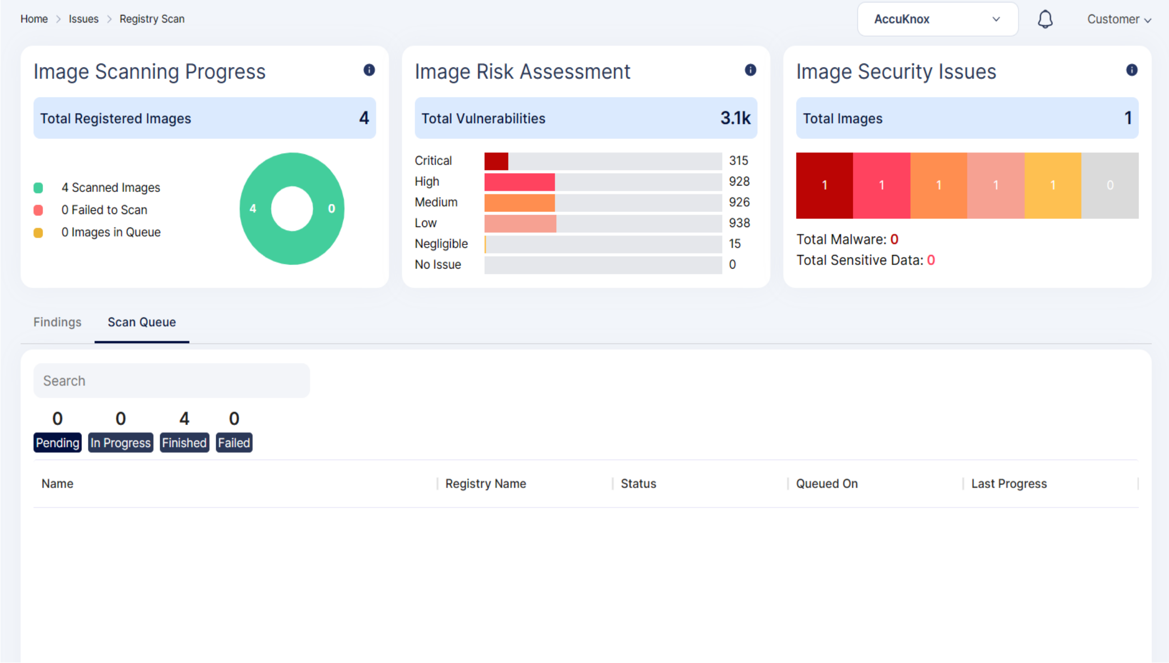
Description *: docker hub registry

Registry Type*: DockerHub

Username *: knoxuser

Password *: •••••

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.



Home > Issues > Registry Scan   AccuKnox   Customer

Image Scanning Progress

Total Registered Images	4

- 4 Scanned Images
- 0 Failed to Scan
- 0 Images in Queue

Image Risk Assessment

Total Vulnerabilities	3.1k
Critical	315
High	928
Medium	926
Low	938
Negligible	15
No Issue	0

Image Security Issues

Total Images	1

Total Malware: 0
Total Sensitive Data: 0

Findings | Scan Queue

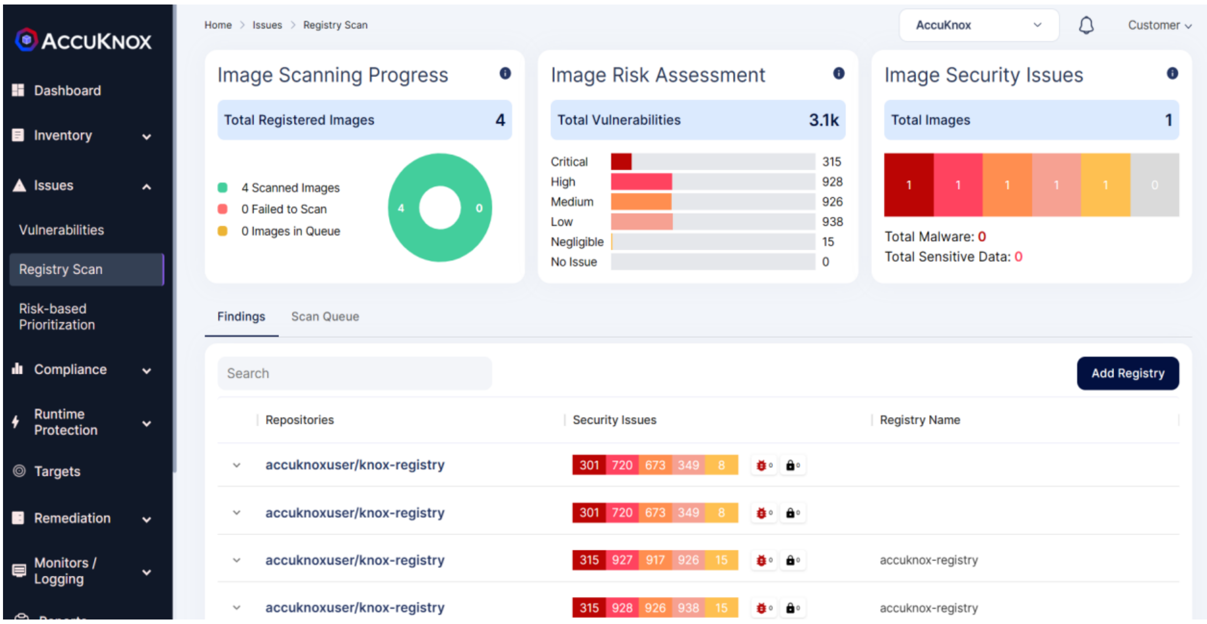
Search

0	0	4	0
Pending	In Progress	Finished	Failed

Name	Registry Name	Status	Queued On	Last Progress

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.



Home > Issues > Registry Scan   AccuKnox   Customer

Image Scanning Progress

Total Registered Images	4

- 4 Scanned Images
- 0 Failed to Scan
- 0 Images in Queue

Image Risk Assessment

Total Vulnerabilities	3.1k
Critical	315
High	928
Medium	926
Low	938
Negligible	15
No Issue	0

Image Security Issues

Total Images	1

Total Malware: 0
Total Sensitive Data: 0

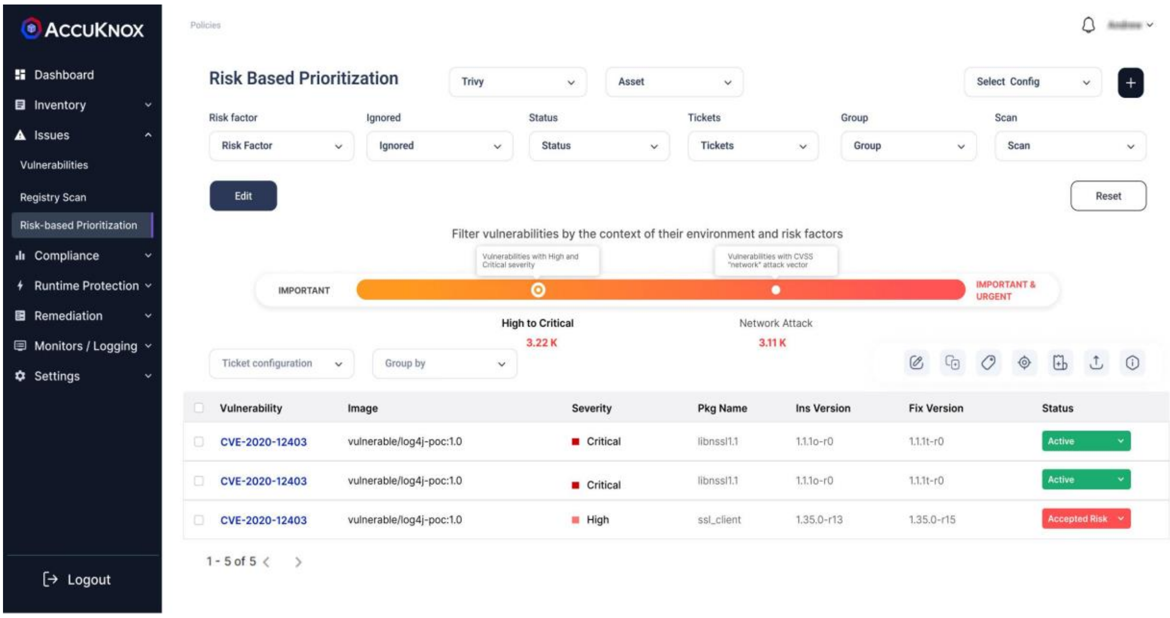
Findings | Scan Queue

Search   Add Registry

Repositories	Security Issues	Registry Name
accuknoxuser/knox-registry	301 720 673 349 8	
accuknoxuser/knox-registry	301 720 673 349 8	
accuknoxuser/knox-registry	315 927 917 926 15	accuknox-registry
accuknoxuser/knox-registry	315 928 926 938 15	accuknox-registry

What is Risk Based Prioritization?

In this section, users will be given a comprehensive risk analysis that is found in their onboard 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.



Risk Based Prioritization

Trivy | Asset | Select Config

Risk factor: Risk Factor
Ignored: Ignored
Status: Status
Tickets: Tickets
Group: Group
Scan: Scan

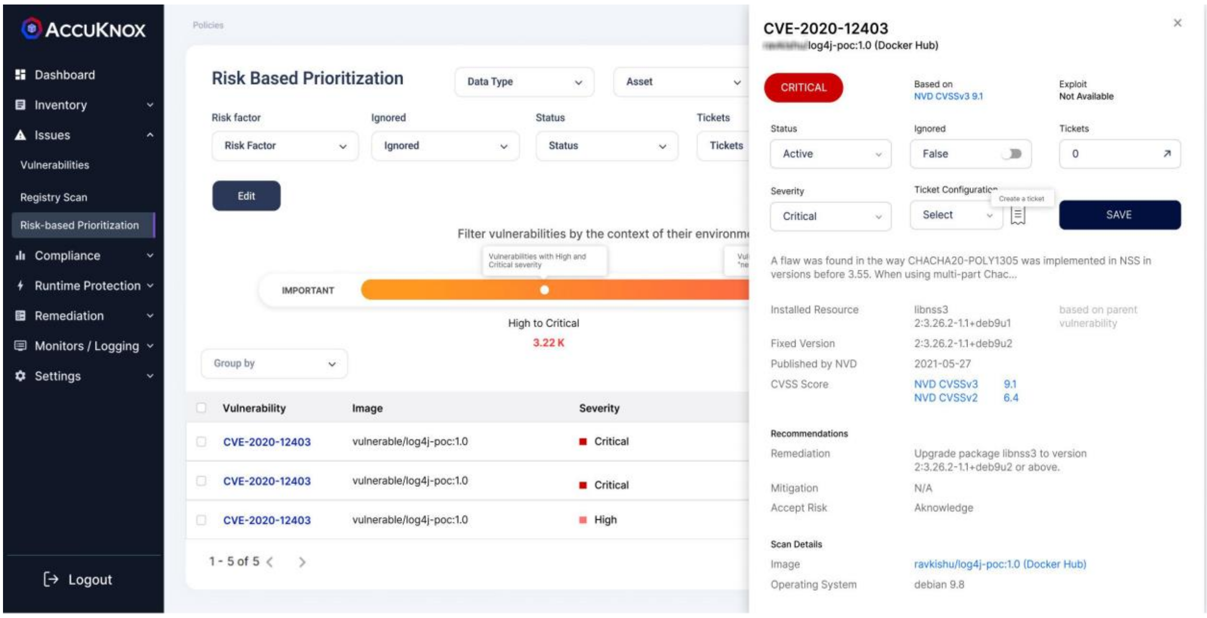
Filter vulnerabilities by the context of their environment and risk factors

High to Critical 3.22 K
Network Attack 3.11 K

Vulnerability	Image	Severity	Pkg Name	Ins Version	Fix Version	Status
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical	libnssl1.1	1.1.1o-r0	1.1.1t-r0	Active
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical	libnssl1.1	1.1.1o-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

1 - 5 of 5

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.



Risk Based Prioritization

Data Type | Asset

Risk factor: Risk Factor
Ignored: Ignored
Status: Status
Tickets: Tickets

Filter vulnerabilities by the context of their environm

High to Critical 3.22 K

Vulnerability	Image	Severity
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical
CVE-2020-12403	vulnerable/log4j-poc:1.0	Critical
CVE-2020-12403	vulnerable/log4j-poc:1.0	High

1 - 5 of 5

CVE-2020-12403
[redacted]log4j-poc:1.0 (Docker Hub)

CRITICAL
Based on: NVD CVSSv3 9.1
Exploit: Not Available

Status: Active
Ignored: False
Tickets: 0
Severity: Critical
Ticket Configuration: Select

A flaw was found in the way CHACHA20-POLY1305 was implemented in NSS in versions before 3.55. When using multi-part Chac...

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: Aknowledge

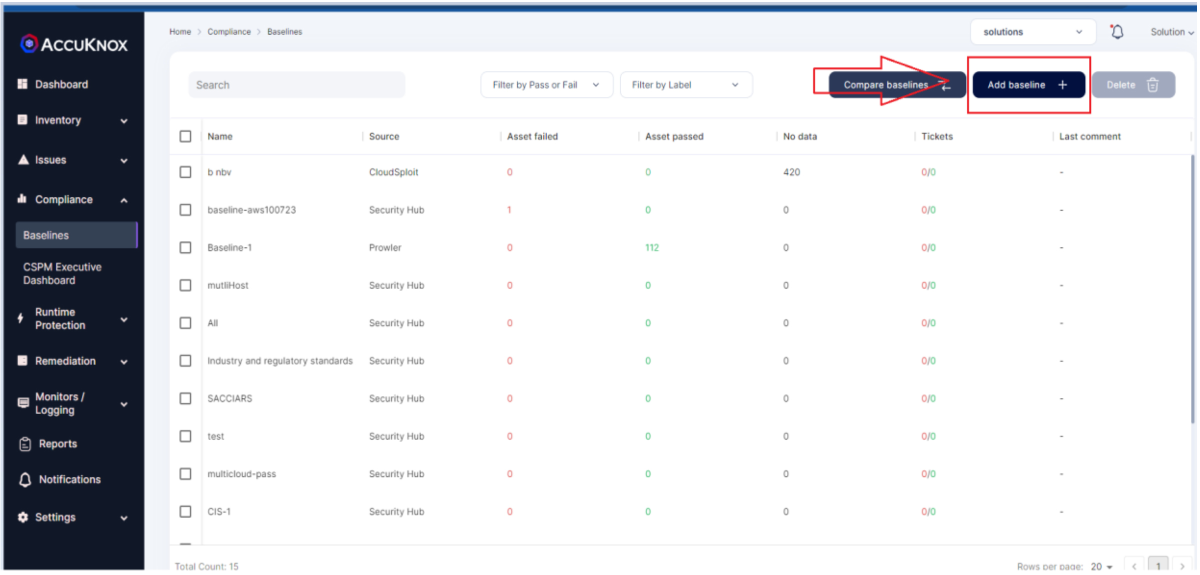
Scan Details
Image: ravkishu/log4j-poc:1.0 (Docker Hub)
Operating System: debian 9.8

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 baseline, follow these steps:
Step 1: Head to the Baselines page and click on add baseline

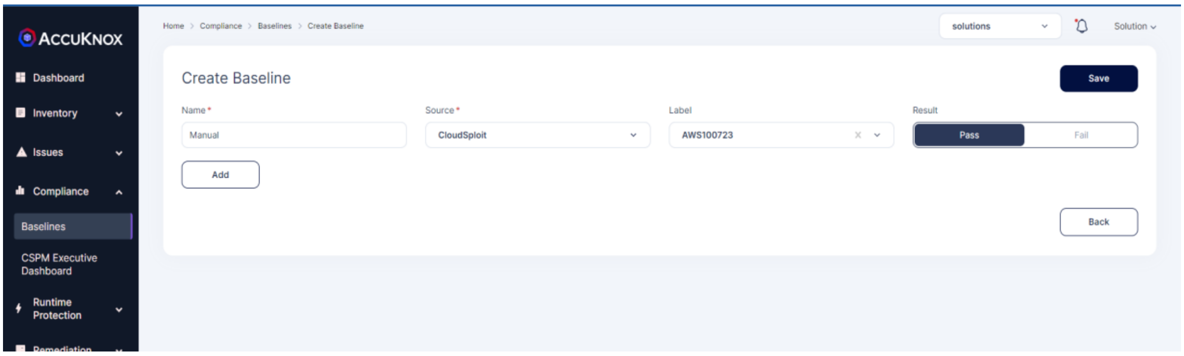


☐	Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
☐	b nbv	CloudSploit	0	0	420	0/0	-
☐	baseline-aws100723	Security Hub	1	0	0	0/0	-
☐	Baseline-1	Prowler	0	112	0	0/0	-
☐	mutliHost	Security Hub	0	0	0	0/0	-
☐	All	Security Hub	0	0	0	0/0	-
☐	Industry and regulatory standards	Security Hub	0	0	0	0/0	-
☐	SACCIARS	Security Hub	0	0	0	0/0	-
☐	test	Security Hub	0	0	0	0/0	-
☐	multicloud-pass	Security Hub	0	0	0	0/0	-
☐	CIS-1	Security Hub	0	0	0	0/0	-

Total Count: 15

Rows per page: 20

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



Create Baseline

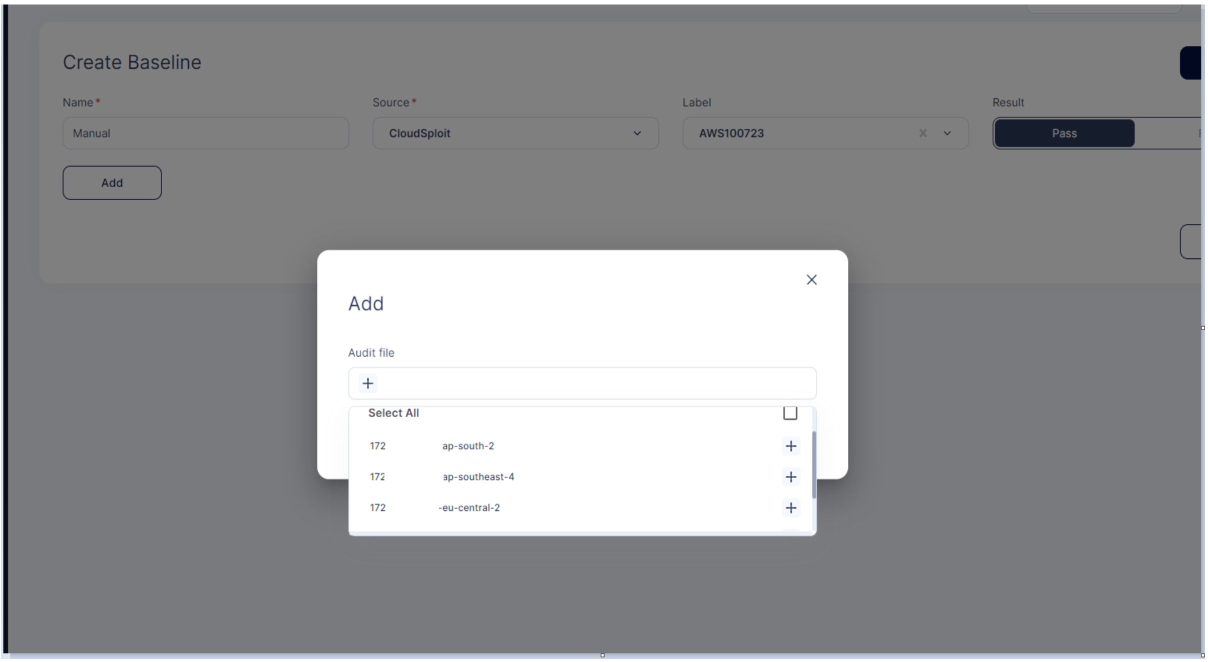
Name *: Manual

Source *: CloudSploit

Label: AWS100723

Result: Pass | Fail

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



Create Baseline

Name * Manual

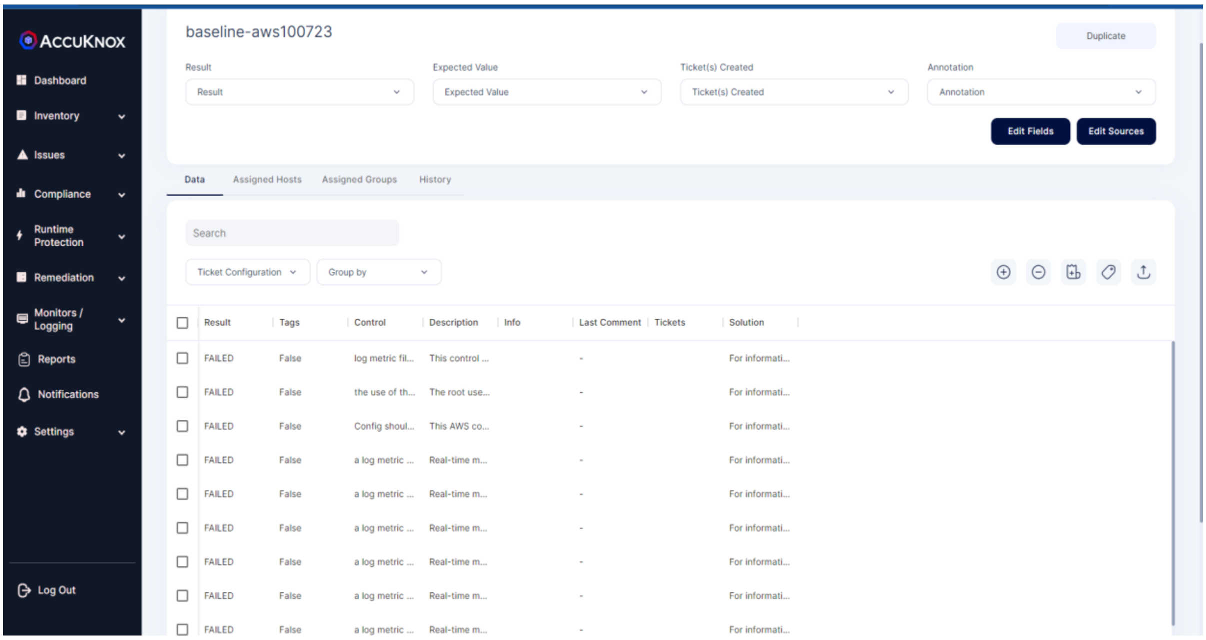
Source * CloudSploit

Label AWS100723

Result Pass

Add

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



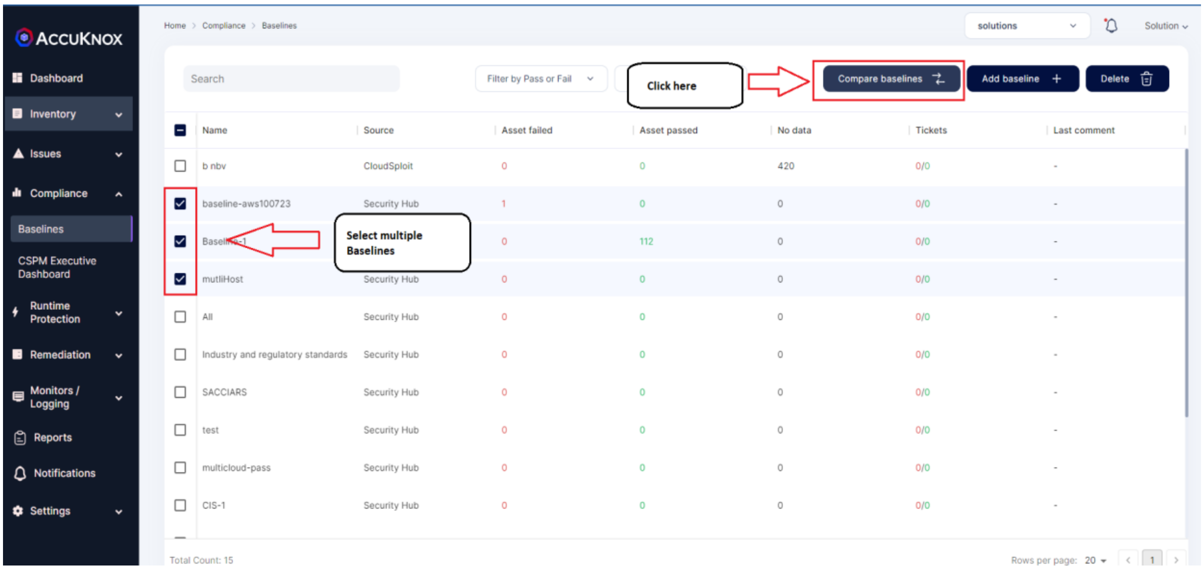
baseline-aws100723

□	Result	Tags	Control	Description	Info	Last Comment	Tickets	Solution
□	FAILED	False	log metric fil...	This control ...		-		For informati...
□	FAILED	False	the use of th...	The root use...		-		For informati...
□	FAILED	False	Config shoul...	This AWS co...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...
□	FAILED	False	a log metric ...	Real-time m...		-		For informati...

How to compare two 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.



Click here

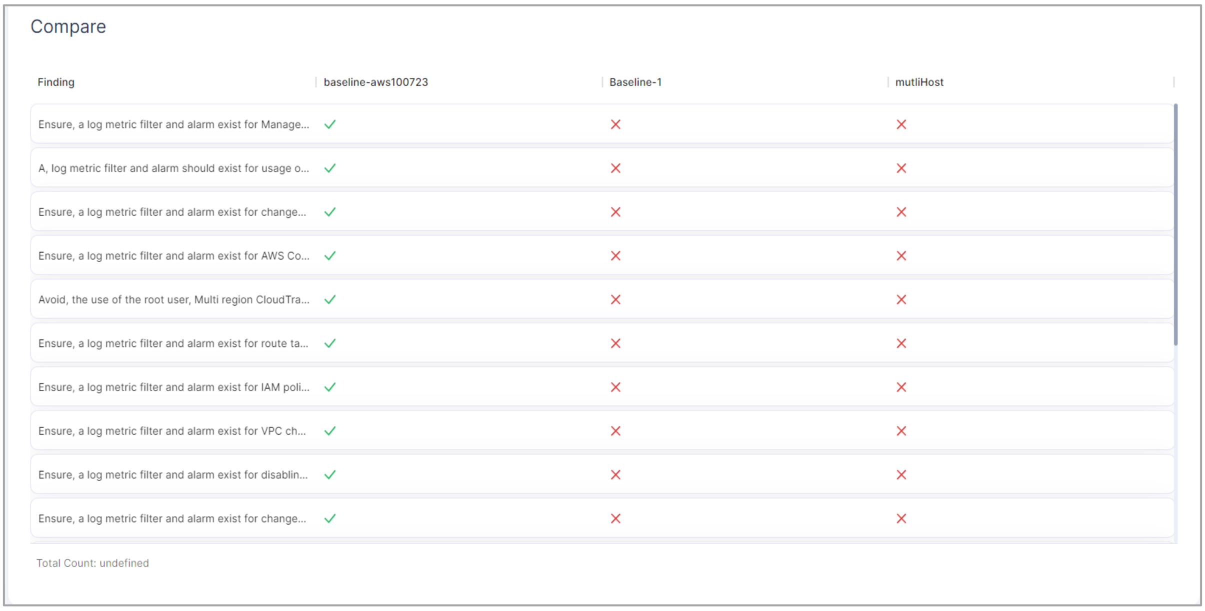
Select multiple Baselines

	Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
☐	b nbv	CloudSploit	0	0	420	0/0	-
☑	baseline-aws100723	Security Hub	1	0	0	0/0	-
☑	Baseline-1		0	112	0	0/0	-
☑	mutliHost	Security Hub	0	0	0	0/0	-
☐	All	Security Hub	0	0	0	0/0	-
☐	Industry and regulatory standards	Security Hub	0	0	0	0/0	-
☐	SACCIARS	Security Hub	0	0	0	0/0	-
☐	test	Security Hub	0	0	0	0/0	-
☐	multicloud-pass	Security Hub	0	0	0	0/0	-
☐	CIS-1	Security Hub	0	0	0	0/0	-

Total Count: 15

Rows per page: 20 < 1 >

The comparison will look like following



Compare

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...	✓	✗	✗

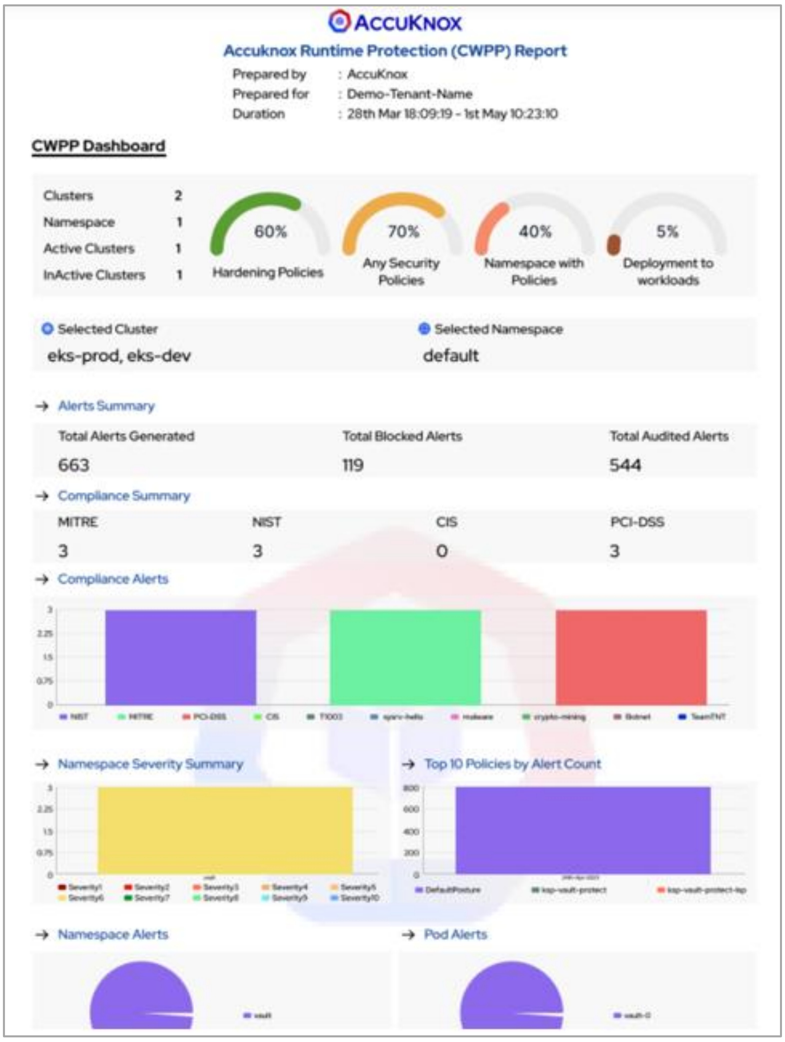
Total Count: undefined

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
Namespace	1
Active Clusters	1
InActive Clusters	1

Selected Cluster	Selected Namespace
eks-prod, eks-dev	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

→ Namespace Severity Summary

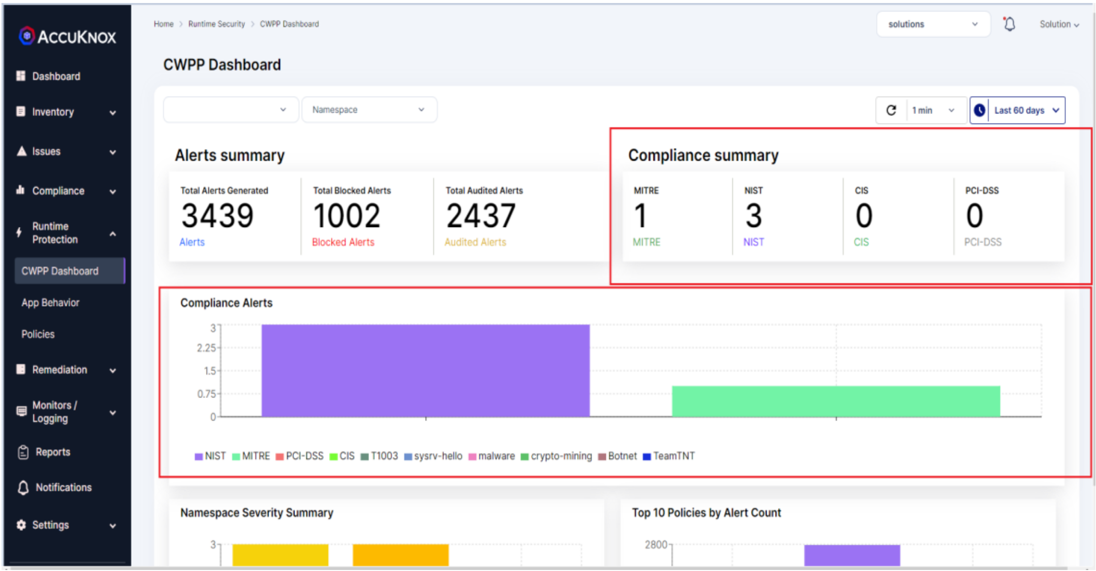
→ Top 10 Policies by Alert Count

→ Namespace Alerts

→ Pod Alerts

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.



CWPP Dashboard

Alerts summary

Total Alerts Generated 3439 Alerts

Total Blocked Alerts 1002 Blocked Alerts

Total Audited Alerts 2437 Audited Alerts

Compliance summary

MITRE 1 MITRE

NIST 3 NIST

CIS 0 CIS

PCI-DSS 0 PCI-DSS

Compliance Alerts

Namespace Severity Summary

Top 10 Policies by Alert Count

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 information is collected at the pod level granularity. So that the users can get information about each pod that is running in each namespace. 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

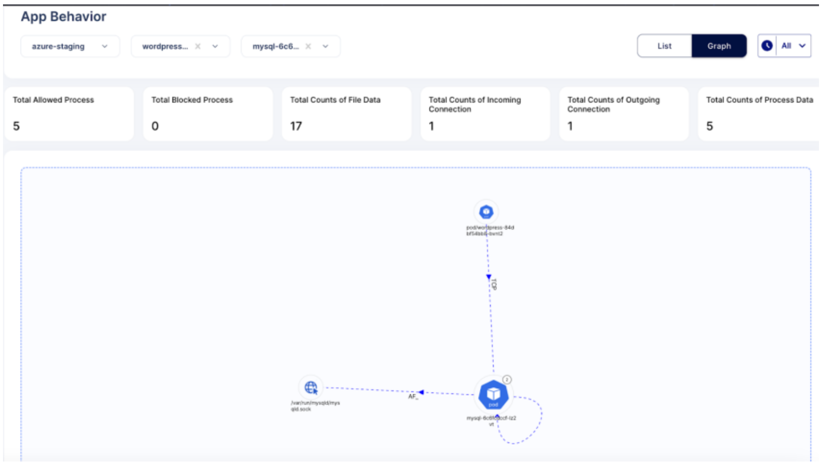
Let us understand this by following use-case example - **Auditing Application Behavior of MySQL application**

1. **Install workload**:

```
sh kubectl apply -f
https://raw.githubusercontent.com/kubearmor/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.



App Behavior

Total Allowed Process 5

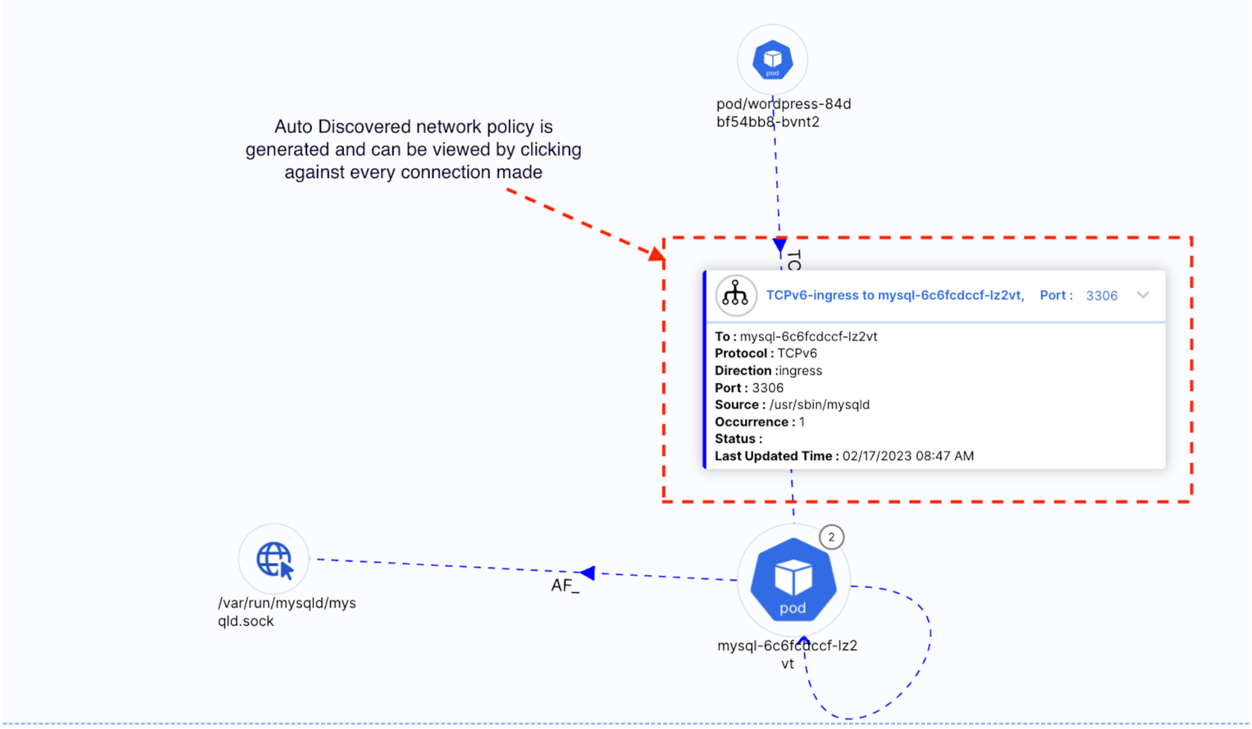
Total Blocked Process 0

Total Counts of File Data 17

Total Counts of Incoming Connection 1

Total Counts of Outgoing Connection 1

Total Counts of Process Data 5

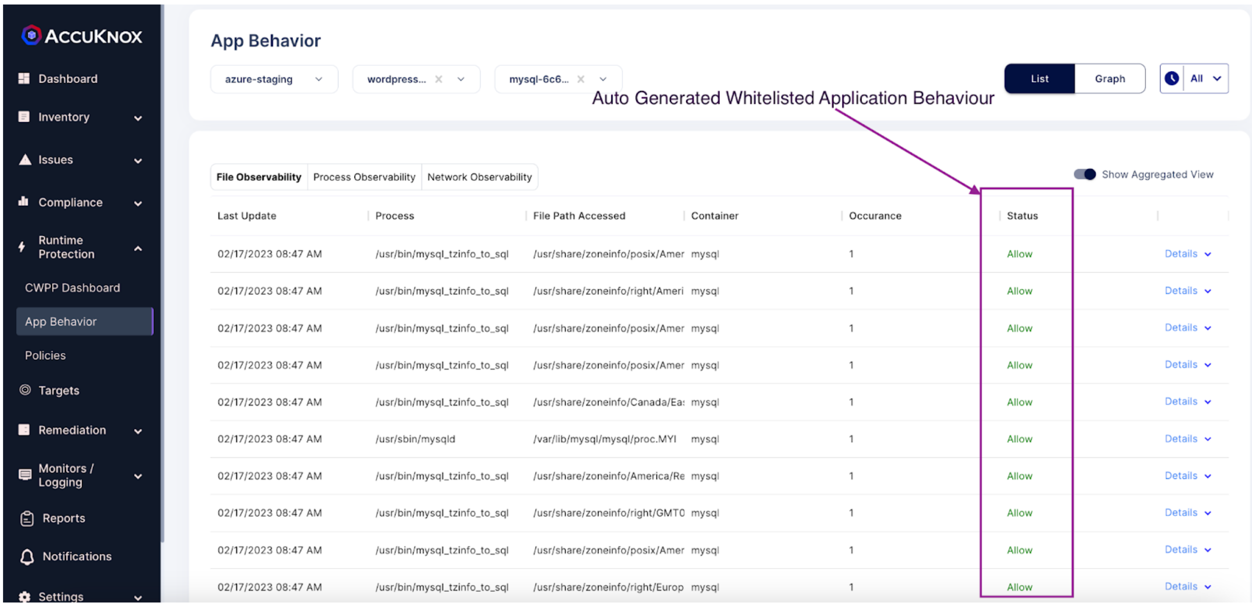


Auto Discovered network policy is generated and can be viewed by clicking against every connection made

TCPv6-ingress to mysql-6c6fcdccf-lz2vt, Port : 3306

To : mysql-6c6fcdccf-lz2vt
Protocol : TCPv6
Direction :ingress
Port : 3306
Source : /usr/sbin/mysqld
Occurrence : 1
Status :
Last Updated Time : 02/17/2023 08:47 AM

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



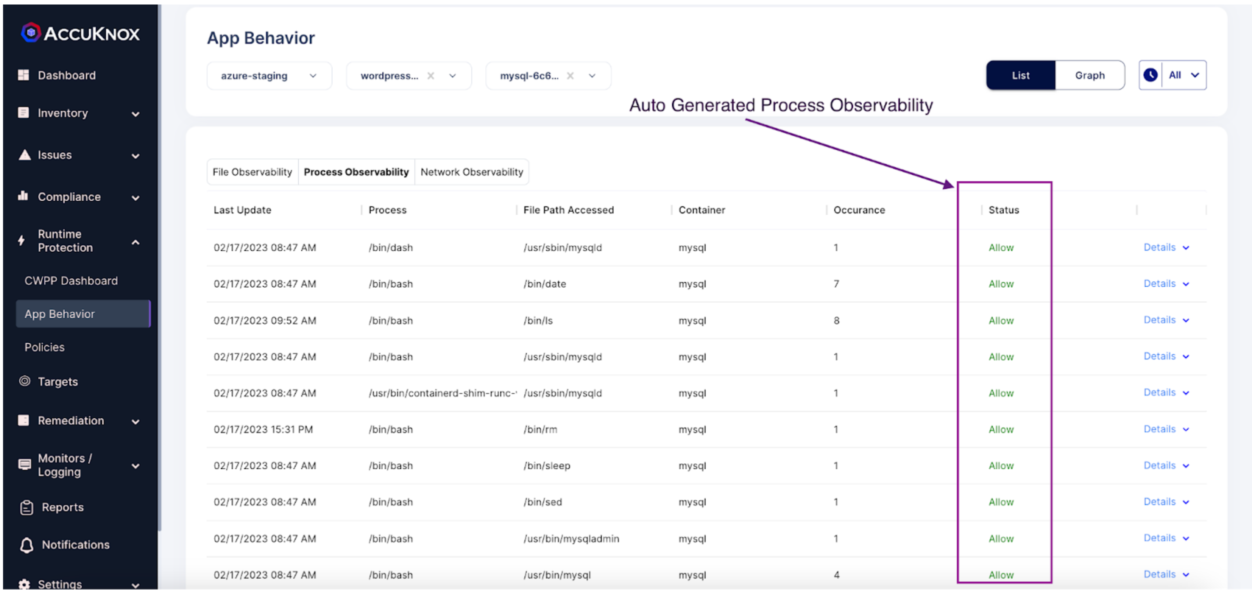
App Behavior

Auto Generated Whitelisted Application Behaviour

File Observability | Process Observability | Network Observability

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

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

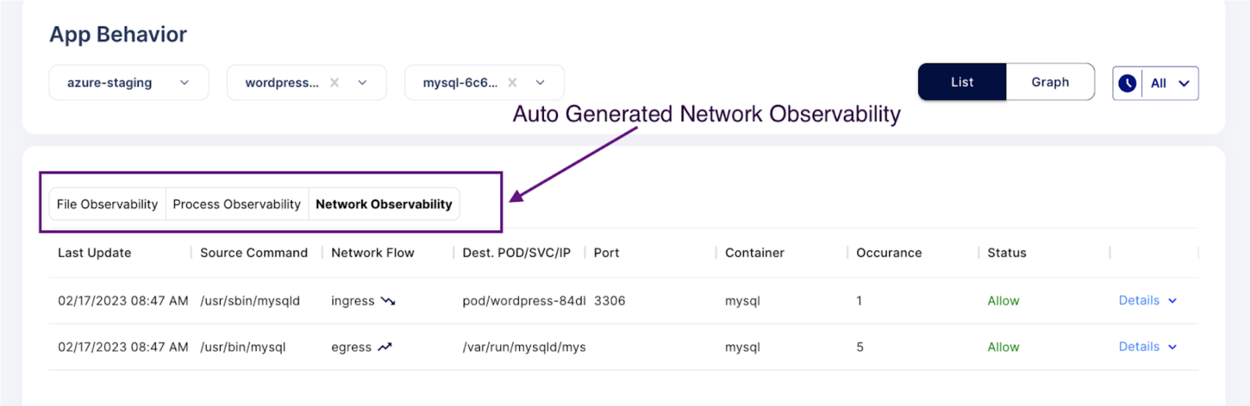


Auto Generated Process Observability

File Observability | **Process Observability** | Network Observability

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

- 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.



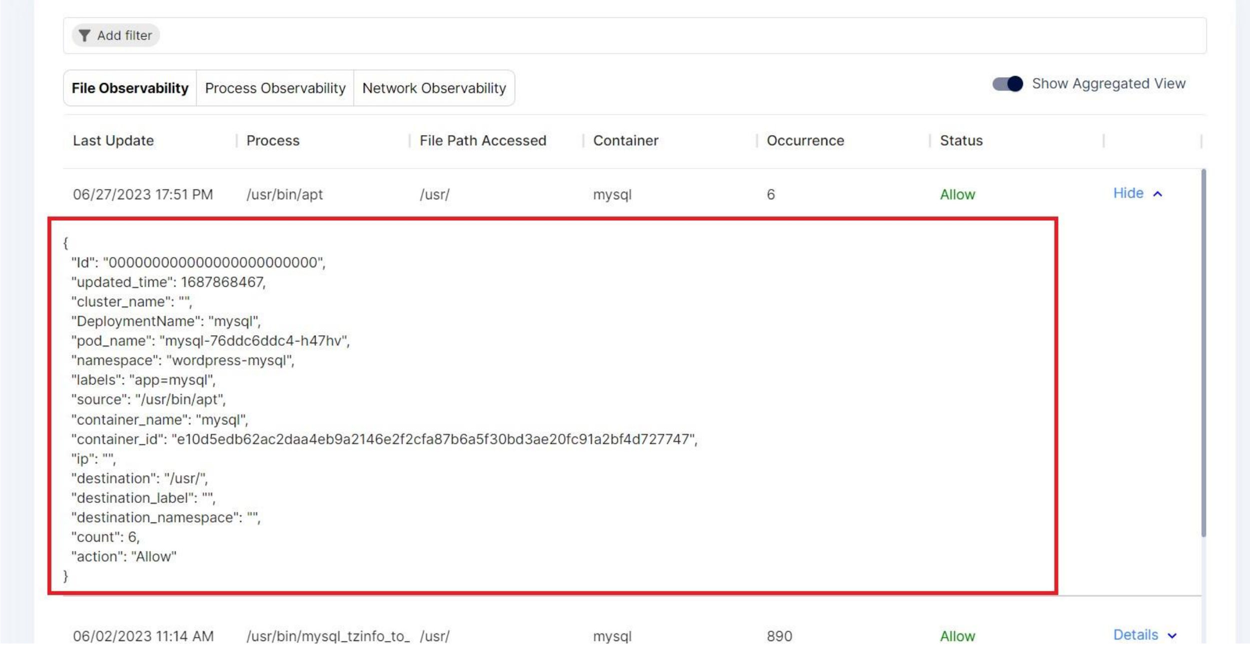
Auto Generated Network Observability

File Observability | Process Observability | **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-84dl	3306	mysql	1	Allow	Details
02/17/2023 08:47 AM	/usr/bin/mysql	egress	/var/run/mysqld/mys		mysql	5	Allow	Details

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

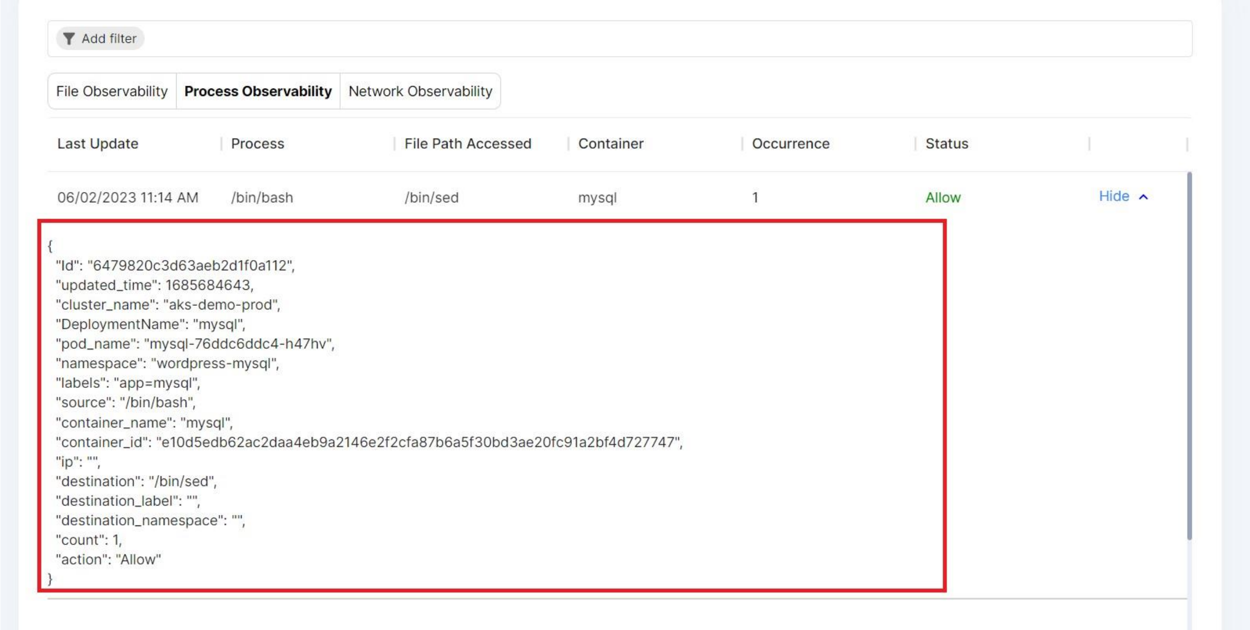


Last Update	Process	File Path Accessed	Container	Occurrence	Status	
06/27/2023 17:51 PM	/usr/bin/apt	/usr/	mysql	6	Allow	Hide ^

```
{
  "Id": "000000000000000000000000",
  "updated_time": 1687868467,
  "cluster_name": "",
  "DeploymentName": "mysql",
  "pod_name": "mysql-76ddc6ddc4-h47hv",
  "namespace": "wordpress-mysql",
  "labels": "app=mysql",
  "source": "/usr/bin/apt",
  "container_name": "mysql",
  "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747",
  "ip": "",
  "destination": "/usr/",
  "destination_label": "",
  "destination_namespace": "",
  "count": 6,
  "action": "Allow"
}
```

06/02/2023 11:14 AM	/usr/bin/mysql_tzinfo_to_	/usr/	mysql	890	Allow	Details ⌄

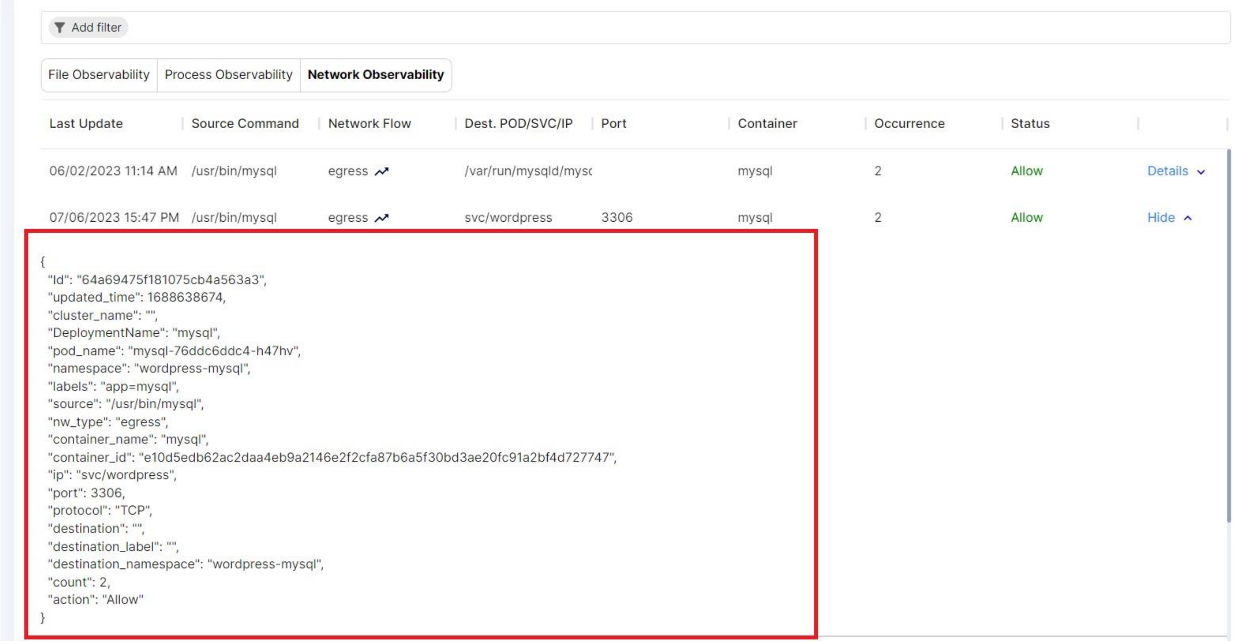
- **Process Observability Telemetry:** To see the process observability related telemetry user needs to click the list view and select process observability part and click on any of the process events to see the Telemetry



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

```
{
 "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



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

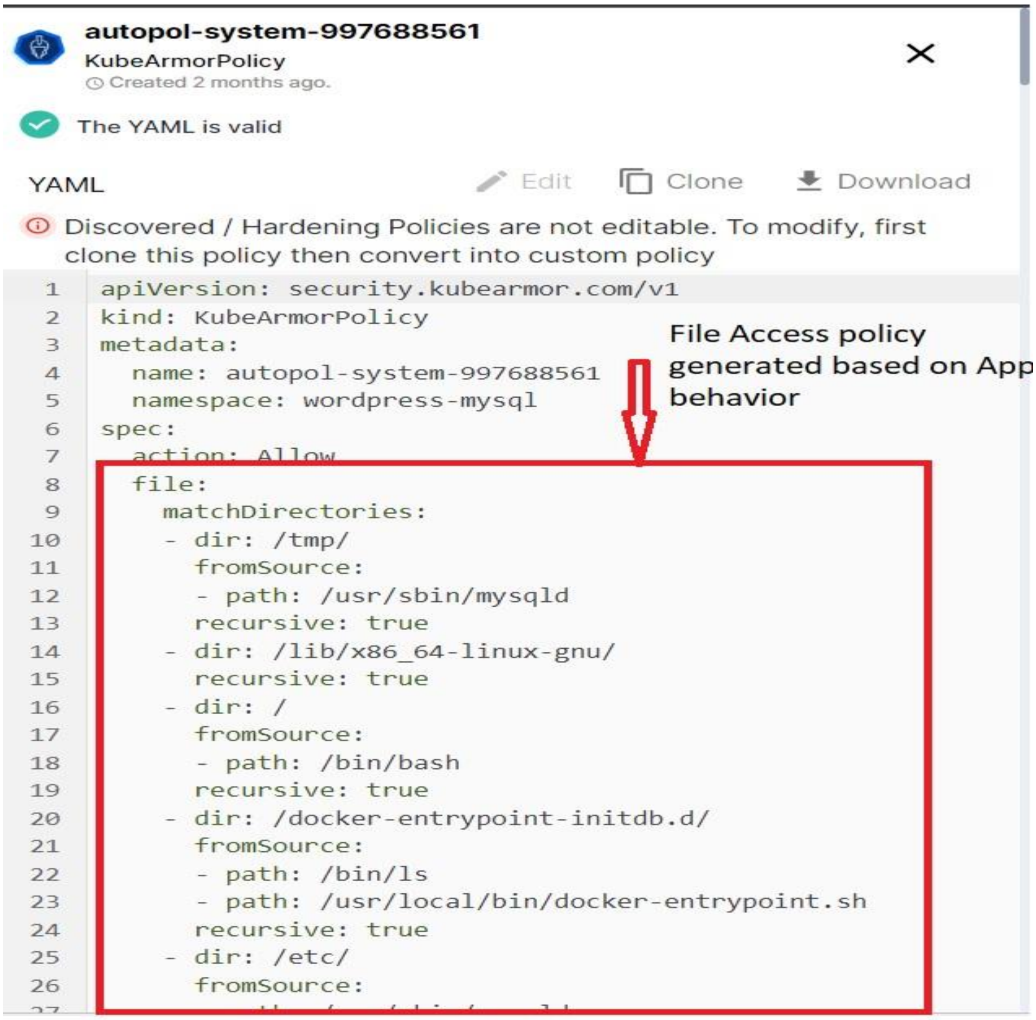
```
{
 "Id": "64a69475f181075cb4a563a3",
 "updated_time": 1688638674,
 "cluster_name": "",
 "DeploymentName": "mysql",
 "pod_name": "mysql-76ddc6ddc4-h47hv",
 "namespace": "wordpress-mysql",
 "labels": "app=mysql",
 "source": "/usr/bin/mysql",
 "nw_type": "egress",
 "container_name": "mysql",
 "container_id": "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 produces 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.

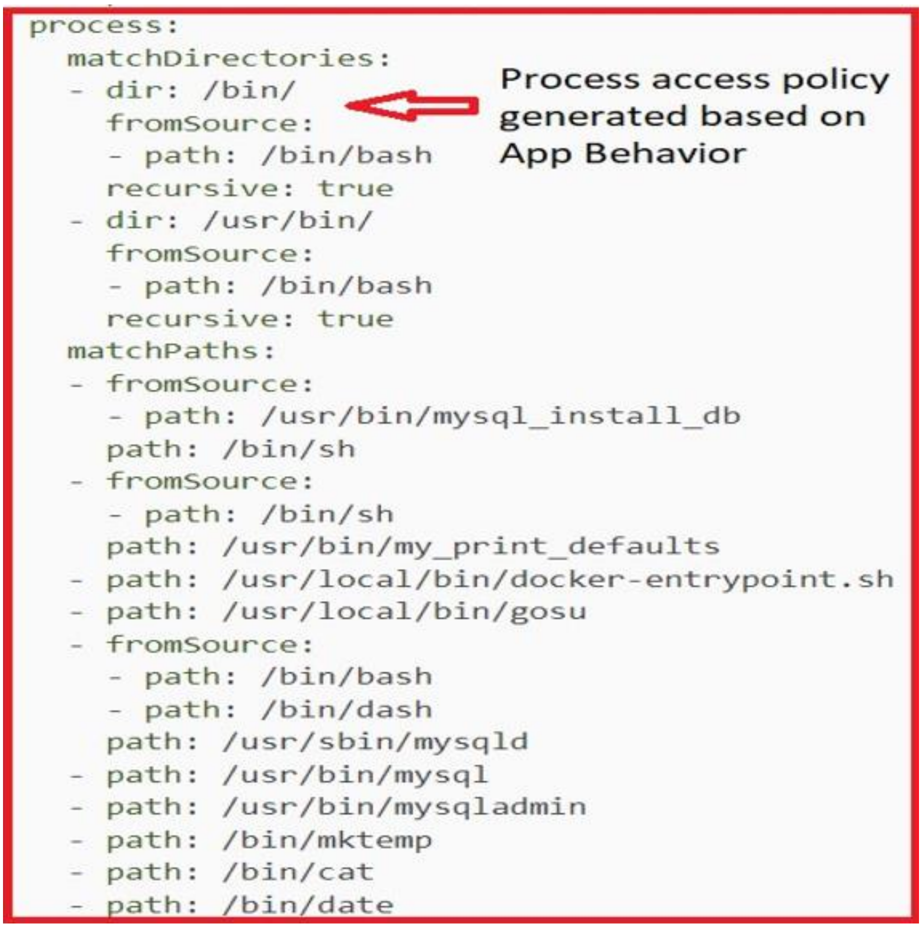


Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: autopol-system-997688561
  namespace: wordpress-mysql
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /tmp/
      fromSource:
      - path: /usr/sbin/mysqld
      recursive: true
    - dir: /lib/x86_64-linux-gnu/
      recursive: true
    - dir: /
      fromSource:
      - path: /bin/bash
      recursive: true
    - dir: /docker-entrypoint-initdb.d/
      fromSource:
      - path: /bin/ls
      - path: /usr/local/bin/docker-entrypoint.sh
      recursive: true
    - dir: /etc/
      fromSource:
```

File Access policy generated based on App behavior

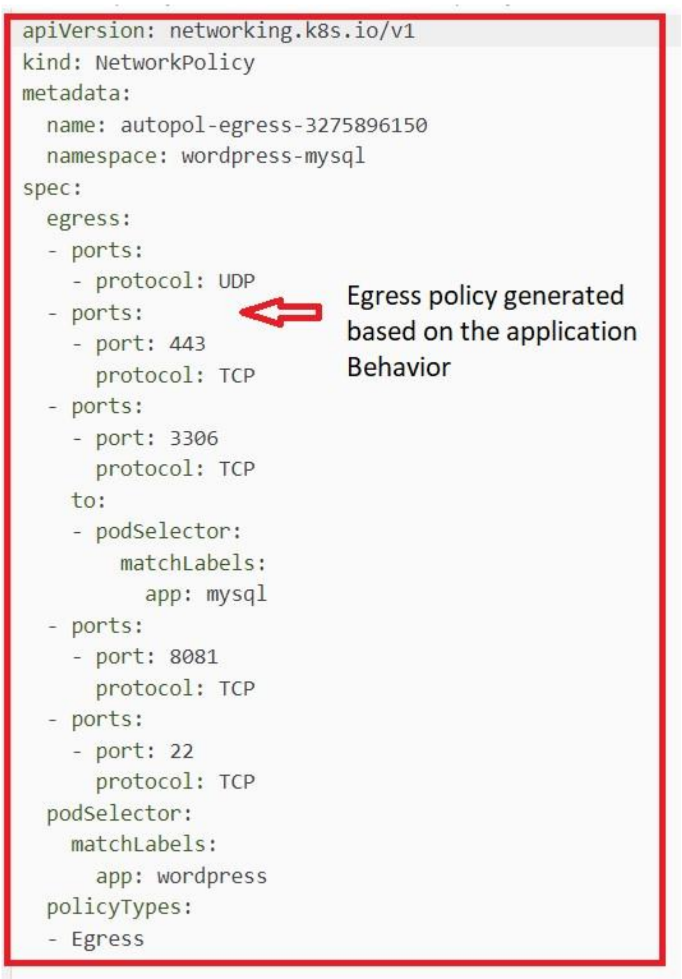
- **Process access behavior-based policies:** Based on the process that are running in pod, the Auto discovered system policies are generated. To view that policy user must navigate to *Runtime Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered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

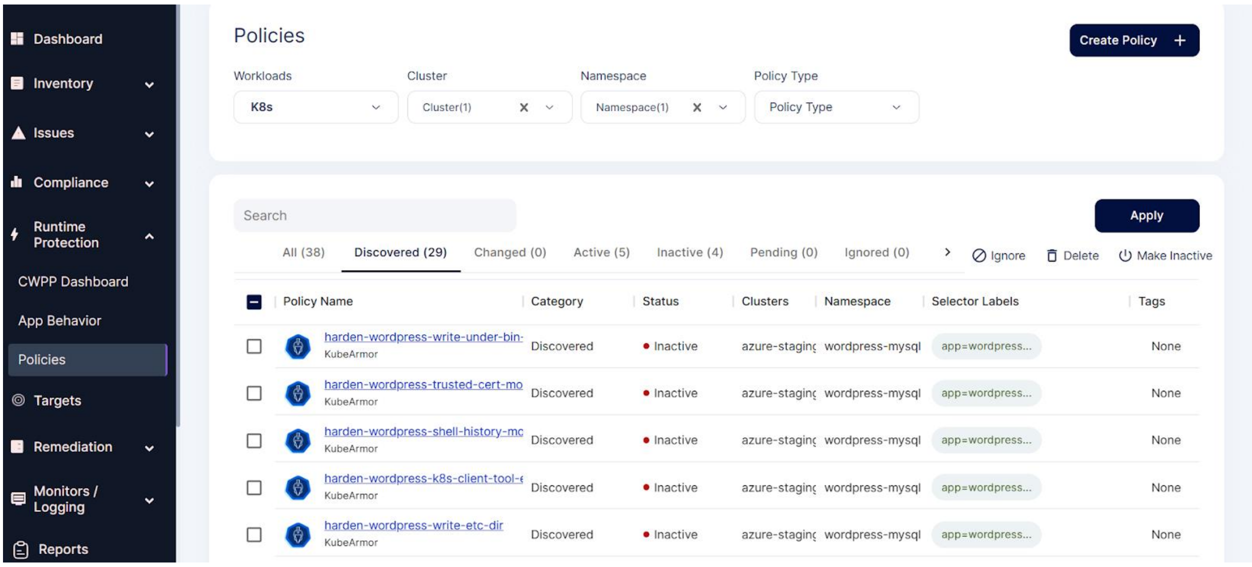
Egress policy generated based on the application Behavior

How to understand Hardening policies

One of the methods to achieve 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 are 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.

- Let us understand by taking a 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 a list of hardening policies for the selected Namespace.



Policies

Workloads: K8s

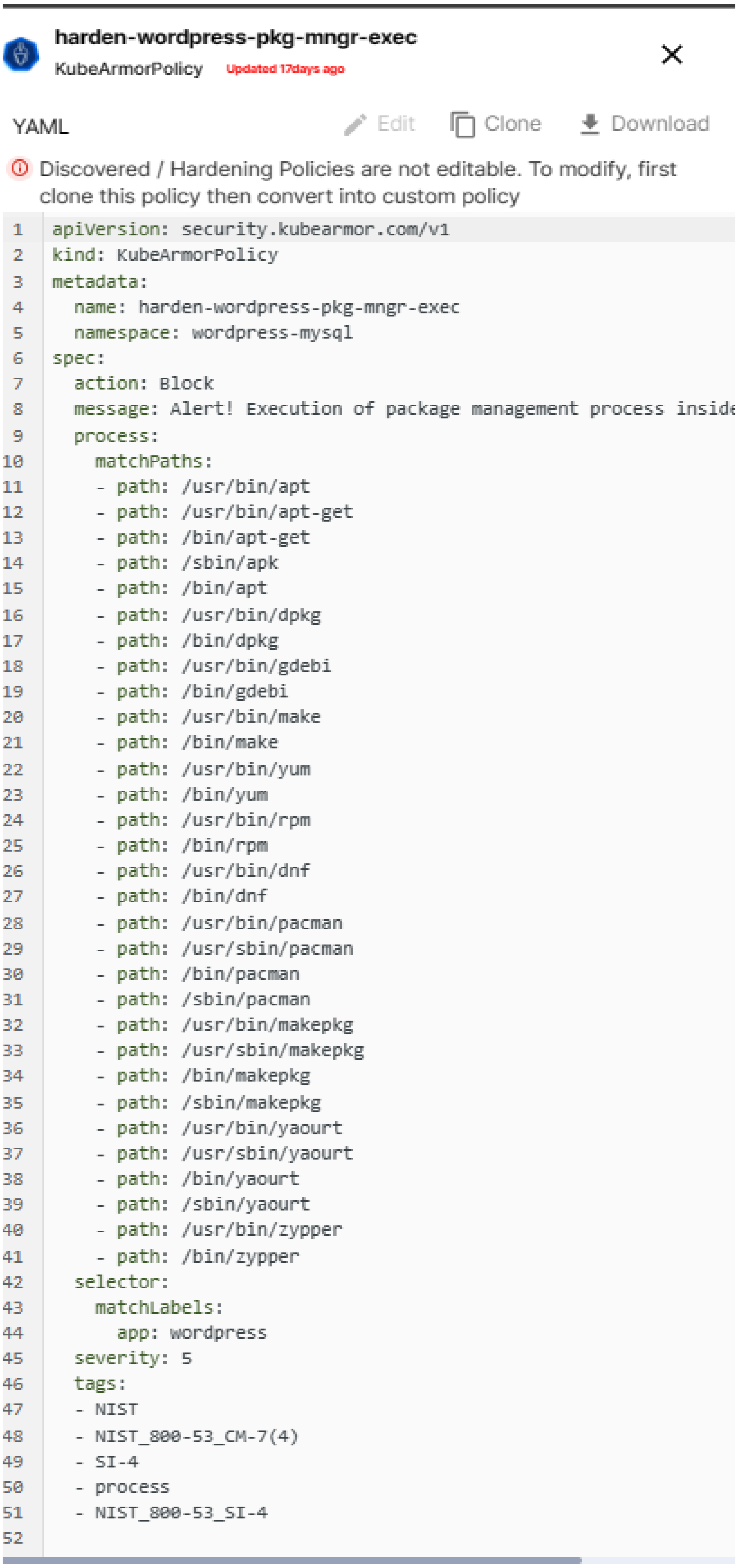
Cluster: Cluster(1)

Namespace: Namespace(1)

Policy Type: Policy Type

Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
harden-wordpress-write-under-bin- KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None
harden-wordpress-trusted-cert-mo KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None
harden-wordpress-shell-history-mc KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None
harden-wordpress-k8s-client-tool- KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None
harden-wordpress-write-etc-dir KubeArmor	Discovered	● Inactive	azure-staging	wordpress-mysql	app=wordpress...	None

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



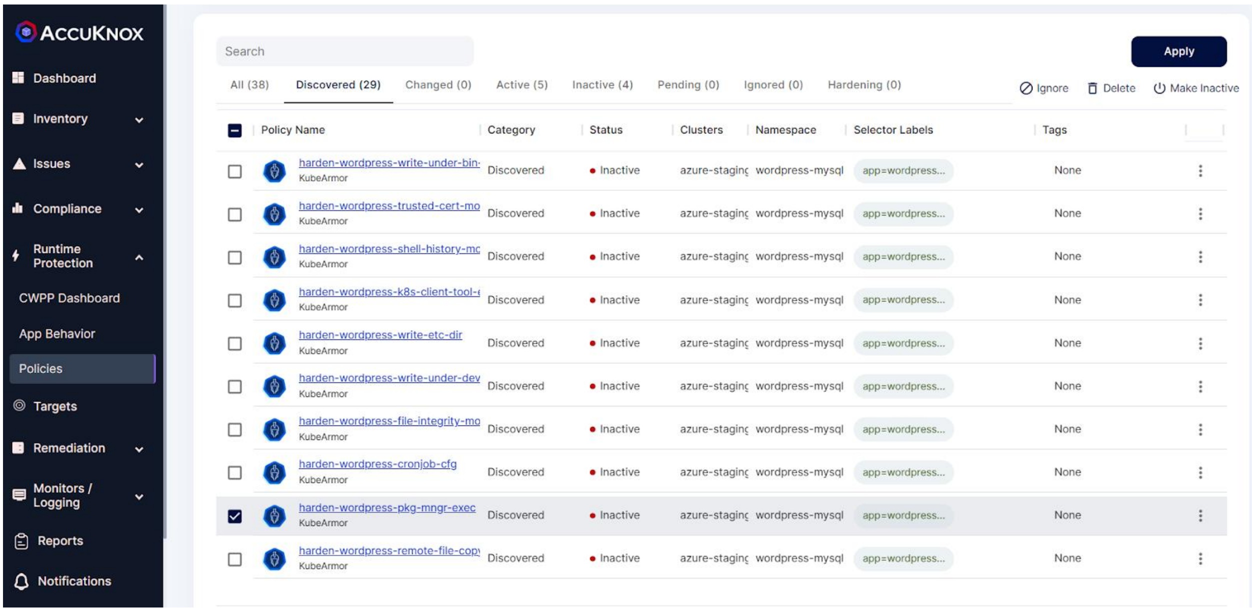
harden-wordpress-pkg-mngr-exec

KubeArmorPolicy Updated 17days ago

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

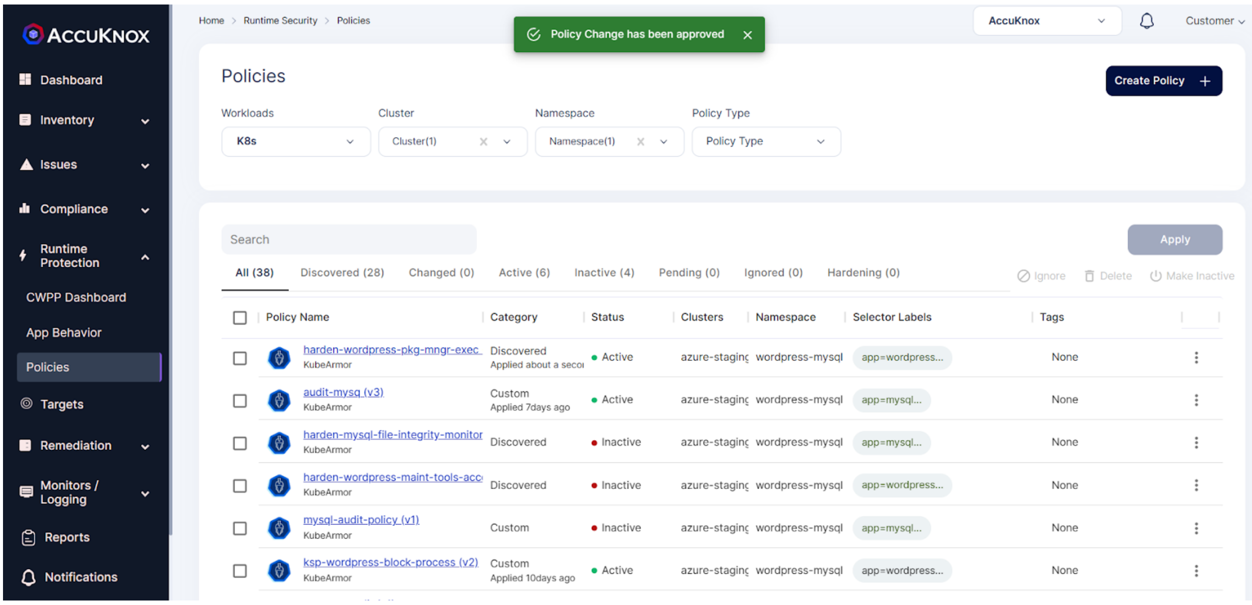
```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: harden-wordpress-pkg-mngr-exec
  namespace: wordpress-mysql
spec:
  action: Block
  message: Alert! Execution of package management process inside
  process:
    matchPaths:
    - path: /usr/bin/apt
    - path: /usr/bin/apt-get
    - path: /bin/apt-get
    - path: /sbin/apk
    - path: /bin/apt
    - path: /usr/bin/dpkg
    - path: /bin/dpkg
    - path: /usr/bin/gdebi
    - path: /bin/gdebi
    - path: /usr/bin/make
    - path: /bin/make
    - path: /usr/bin/yum
    - path: /bin/yum
    - path: /usr/bin/rpm
    - path: /bin/rpm
    - path: /usr/bin/dnf
    - path: /bin/dnf
    - path: /usr/bin/pacman
    - path: /usr/sbin/pacman
    - path: /bin/pacman
    - path: /sbin/pacman
    - path: /usr/bin/makepkg
    - path: /usr/sbin/makepkg
    - path: /bin/makepkg
    - path: /sbin/makepkg
    - path: /usr/bin/yaourt
    - path: /usr/sbin/yaourt
    - path: /bin/yaourt
    - path: /sbin/yaourt
    - path: /usr/bin/zypper
    - path: /bin/zypper
  selector:
    matchLabels:
      app: wordpress
  severity: 5
  tags:
  - NIST
  - NIST_800-53_CM-7(4)
  - SI-4
  - process
  - NIST_800-53_SI-4

```

3. Select this policy and click on the apply option



	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	harden-wordpress-write-under-bin- KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-trusted-cert-mo KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-shell-history-mc KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-k8s-client-tool-ε KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-write-etc-dir KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-write-under-dev KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-file-integrity-mo KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-cronjob-cfg KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☑	harden-wordpress-pkg-mngr-exec KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	harden-wordpress-remote-file-copy KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None

4. After applying policy goes into active state.



Policy Change has been approved

Policies

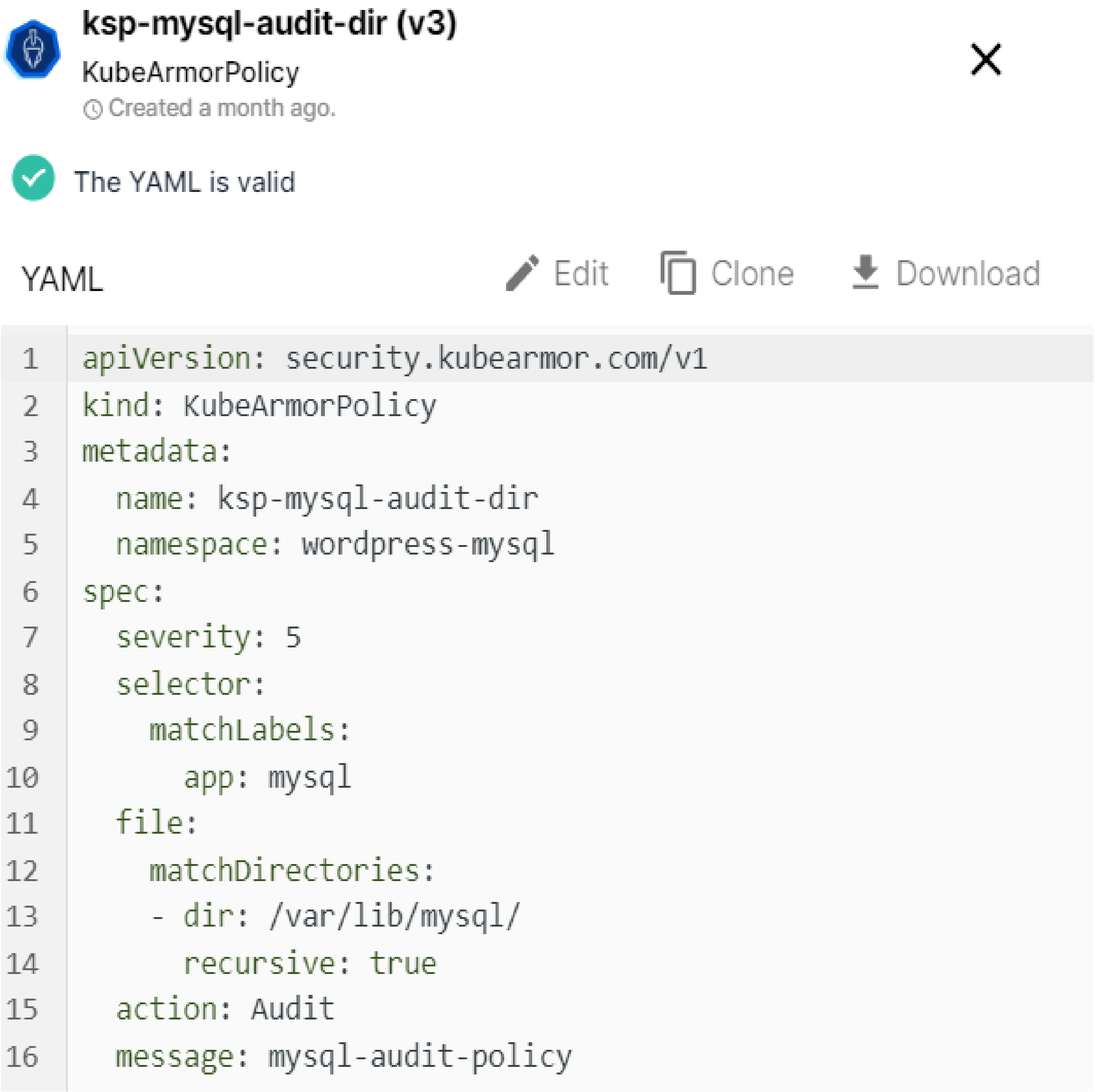
Workloads: K8s
Cluster: Cluster(1)
Namespace: Namespace(1)
Policy Type: Policy Type

	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	harden-wordpress-pkg-mngr-exec KubeArmor	Discovered Applied about a secoi	● Active	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	audit-mysq (v3) KubeArmor	Custom Applied 7days ago	● Active	azure-staginc	wordpress-mysql	app=mysql...	None
☐	harden-mysql-file-integrity-monitor KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=mysql...	None
☐	harden-wordpress-maint-tools-acc KubeArmor	Discovered	● Inactive	azure-staginc	wordpress-mysql	app=wordpress...	None
☐	mysql-audit-policy (v1) KubeArmor	Custom	● Inactive	azure-staginc	wordpress-mysql	app=mysql...	None
☐	ksp-wordpress-block-process (v2) KubeArmor	Custom Applied 10days ago	● Active	azure-staginc	wordpress-mysql	app=wordpress...	None

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

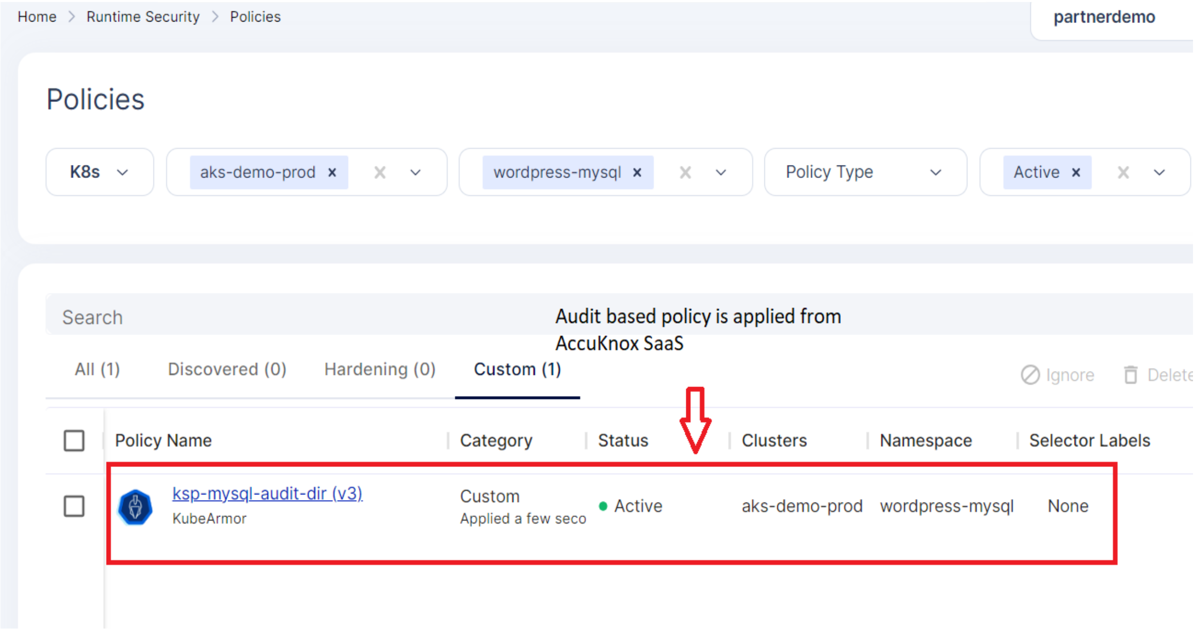
How to Audit application and get alerts for that

- AccuKnox Runtime Security Engine KubeArmor can be used for auditing the application with the help of audit-based security policies. Let us consider the following policy



```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: ksp-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
```

- 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

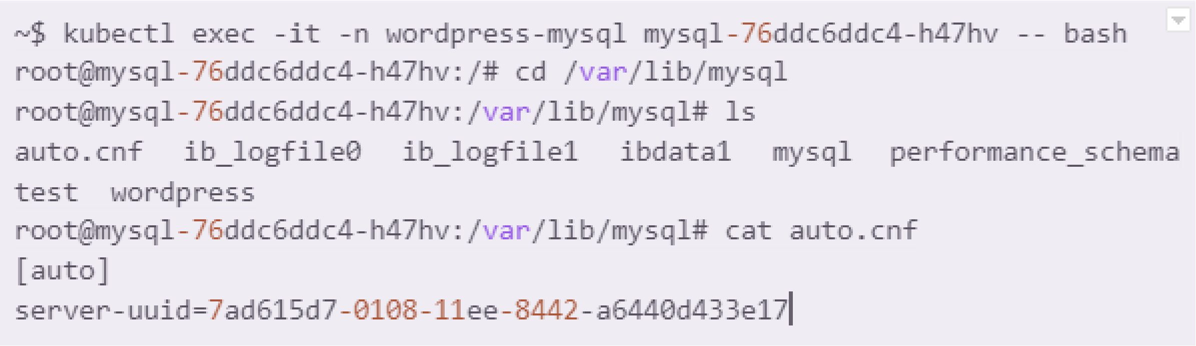


Policies

Audit based policy is applied from AccuKnox SaaS

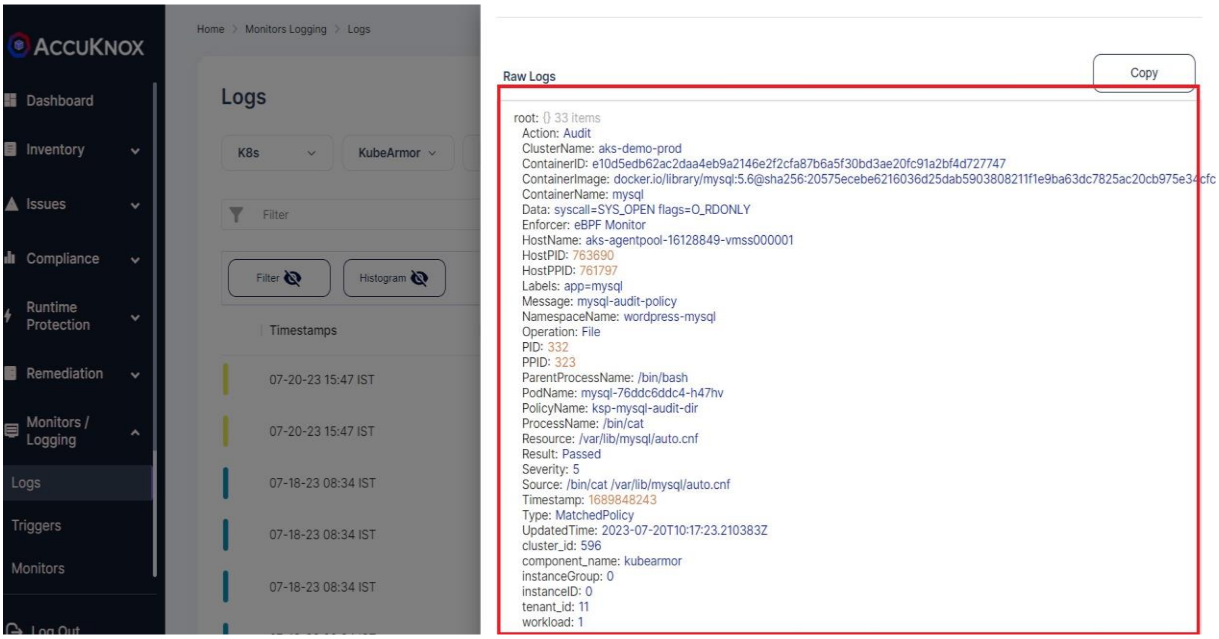
□	Policy Name	Category	Status	Clusters	Namespace	Selector Labels
□	ksp-mysql-audit-dir (v3) KubeArmor	Custom Applied a few seco	● Active	aks-demo-prod	wordpress-mysql	None

- 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
```

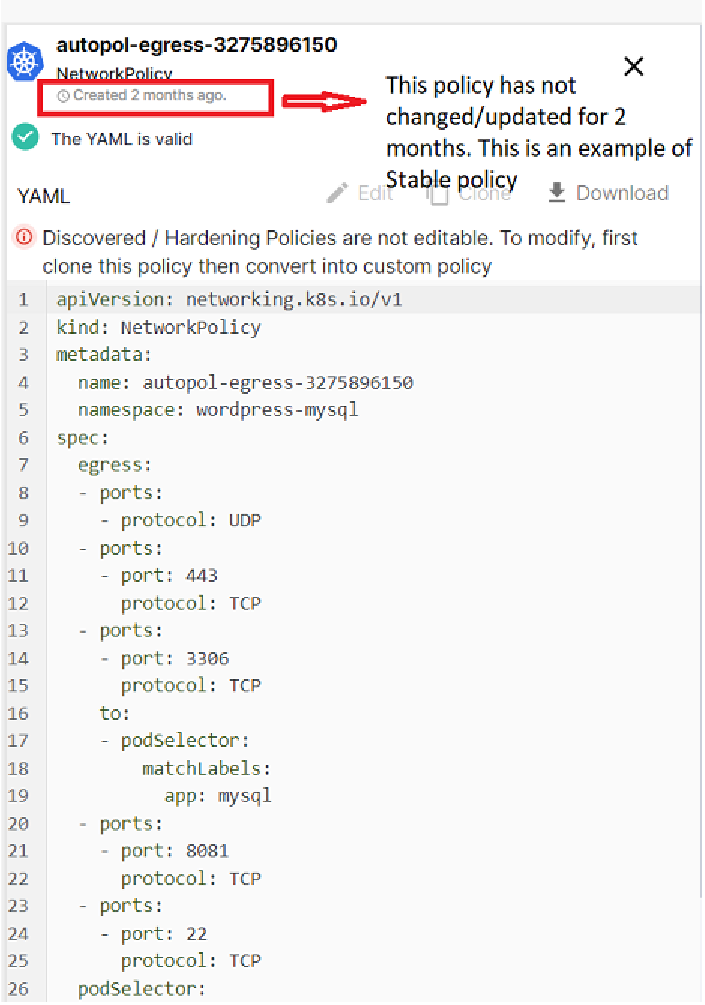
- We can see the Audit based alert in the Monitoring/Logging Section from AccuKnox SaaS as below



```
root: {} 33 items
  Action: Audit
  ClusterName: aks-demo-prod
  ContainerID: e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747
  ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab5903808211f1e9ba63dc7825ac20cb975e34cfc
  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: 323
  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
  instanceGroup: 0
  instanceID: 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 does not change for some days then we can say that the policy which was discovered is stable. For example, consider the following policy



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

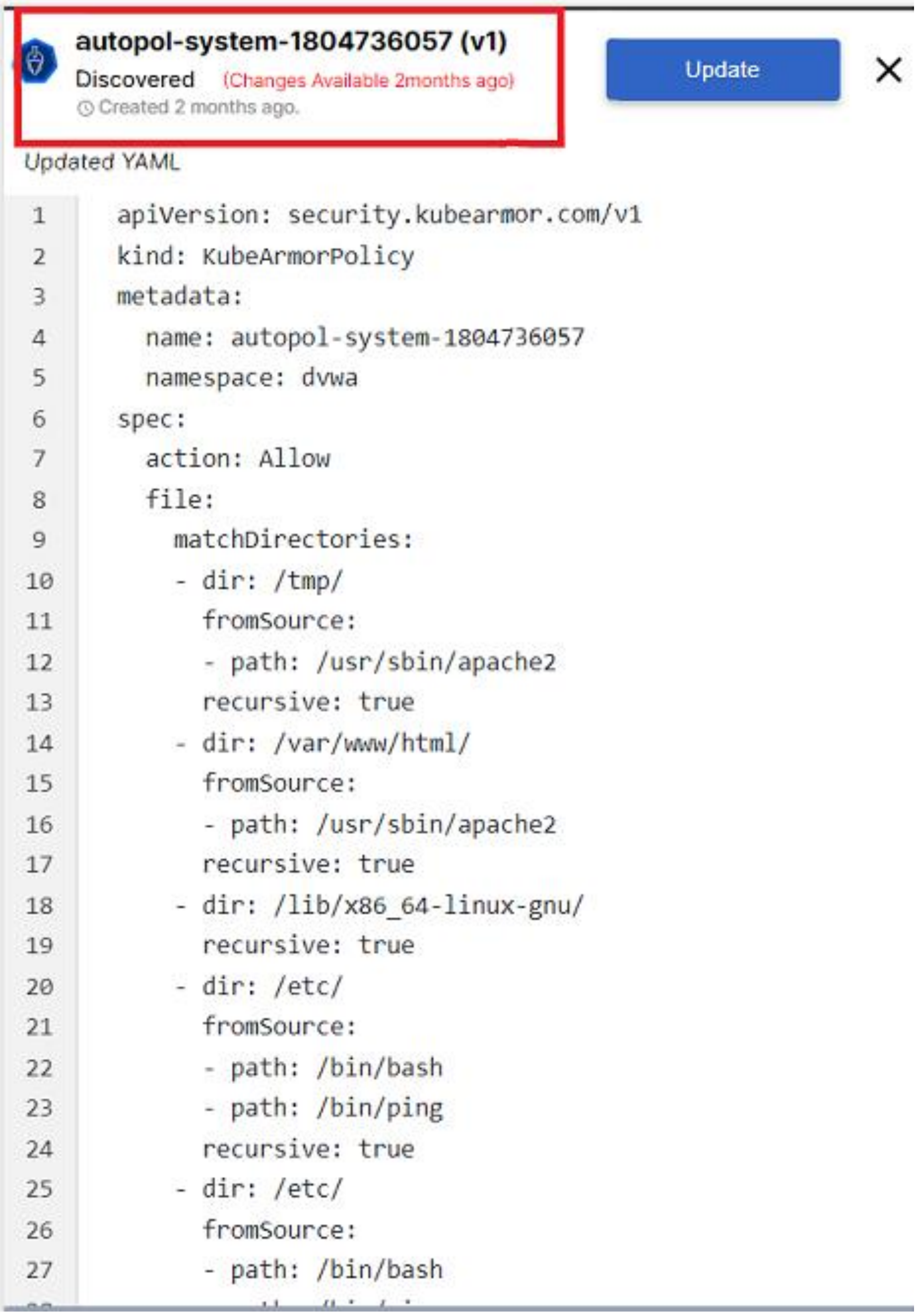
Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```
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:
```

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

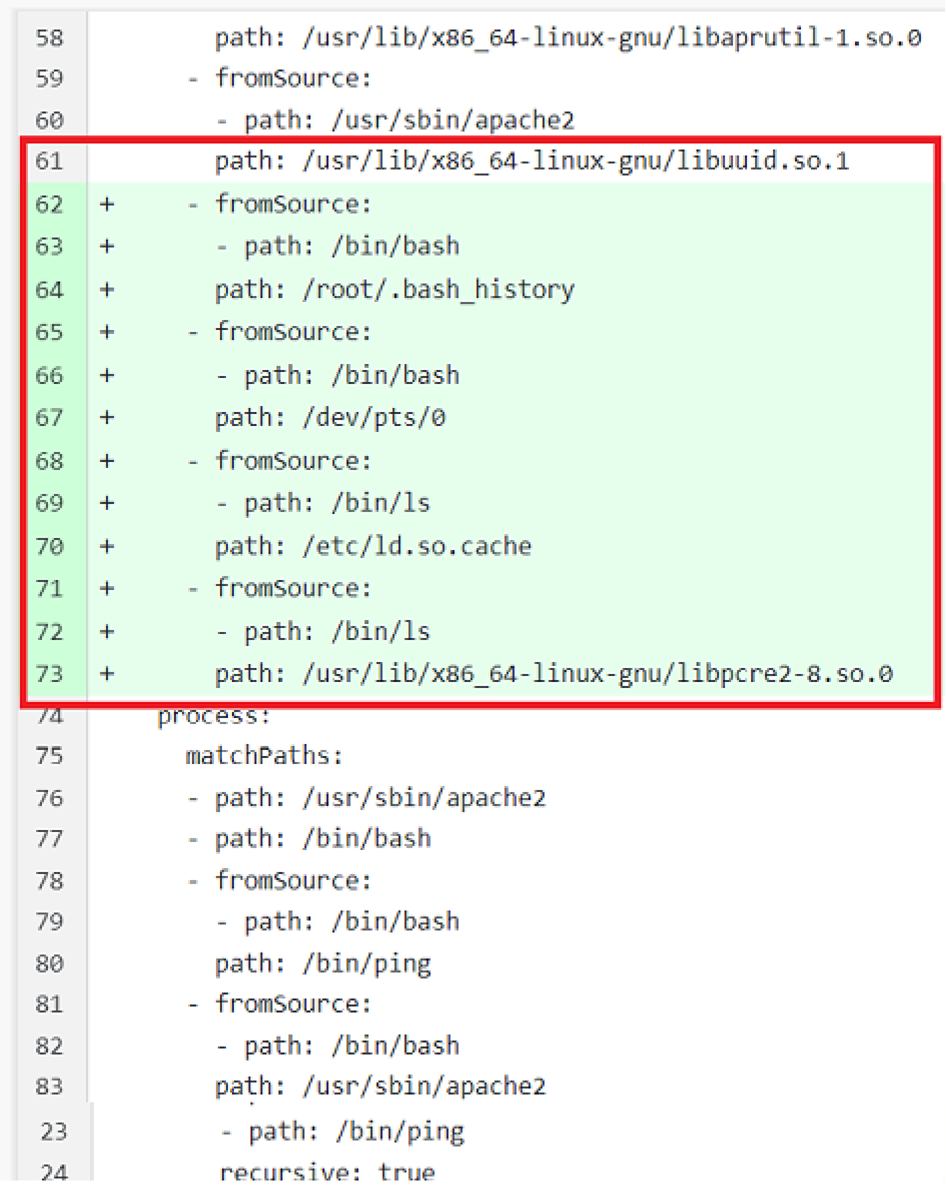
What if something changes in Application??

- 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
Updated YAML

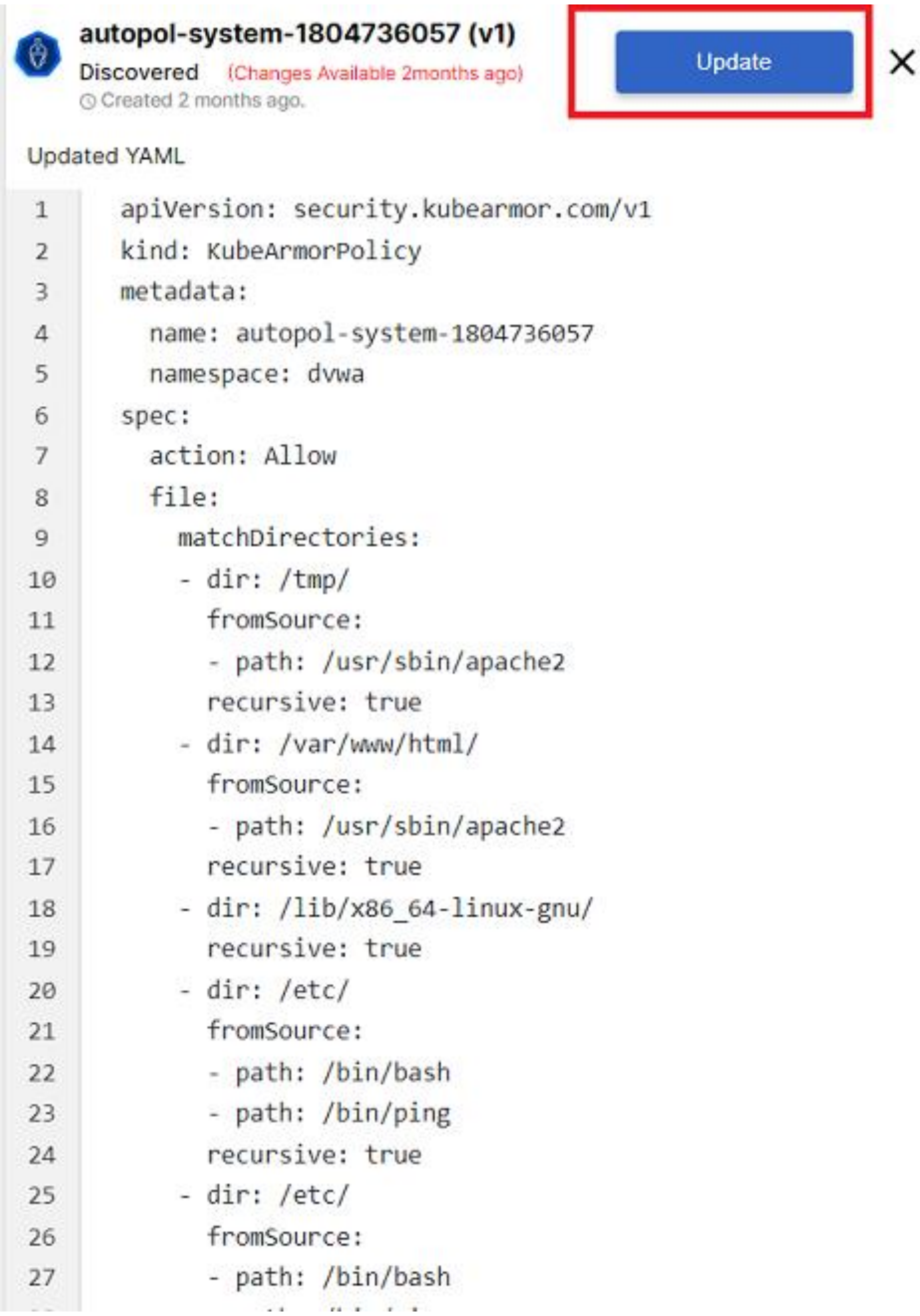
```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: autopol-system-1804736057
  namespace: dvwa
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /tmp/
      fromSource:
      - path: /usr/sbin/apache2
      recursive: true
    - dir: /var/www/html/
      fromSource:
      - path: /usr/sbin/apache2
      recursive: true
    - dir: /lib/x86_64-linux-gnu/
      recursive: true
    - dir: /etc/
      fromSource:
      - path: /bin/bash
      - path: /bin/ping
      recursive: true
    - dir: /etc/
      fromSource:
      - 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.



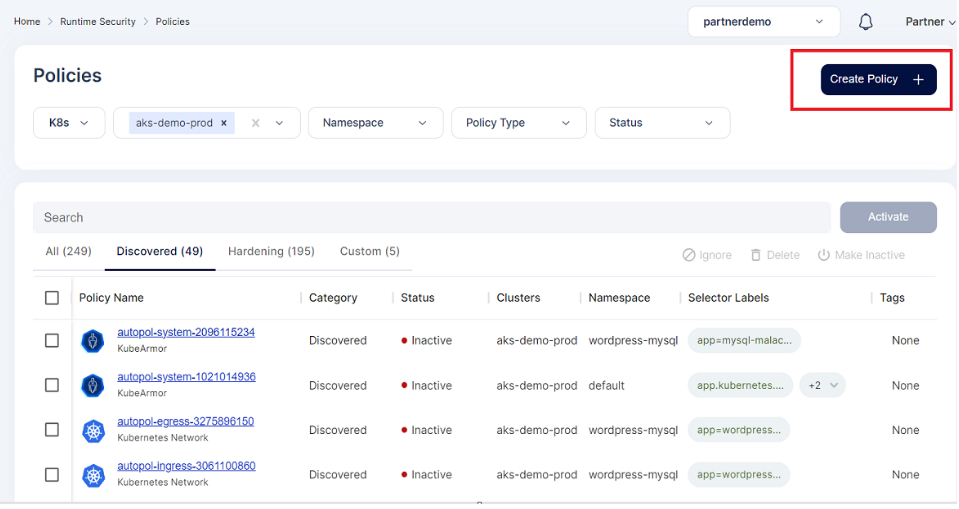
```
            path: /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0
          - fromSource:
            - path: /usr/sbin/apache2
            path: /usr/lib/x86_64-linux-gnu/libuuid.so.1
+         - fromSource:
+           - path: /bin/bash
+           path: /root/.bash_history
+         - fromSource:
+           - path: /bin/bash
+           path: /dev/pts/0
+         - fromSource:
+           - path: /bin/ls
+           path: /etc/ld.so.cache
+         - fromSource:
+           - path: /bin/ls
+           path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0
      process:
        matchPaths:
          - path: /usr/sbin/apache2
          - path: /bin/bash
          - fromSource:
            - path: /bin/bash
            path: /bin/ping
          - fromSource:
            - path: /bin/bash
            path: /usr/sbin/apache2
            - path: /bin/ping
            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

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: autopol-system-1804736057
  namespace: dvwa
spec:
  action: Allow
  file:
    matchDirectories:
    - dir: /tmp/
      fromSource:
      - path: /usr/sbin/apache2
      recursive: true
    - dir: /var/www/html/
      fromSource:
      - path: /usr/sbin/apache2
      recursive: true
    - dir: /lib/x86_64-linux-gnu/
      recursive: true
    - dir: /etc/
      fromSource:
      - path: /bin/bash
      - path: /bin/ping
      recursive: true
    - dir: /etc/
      fromSource:
      - 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

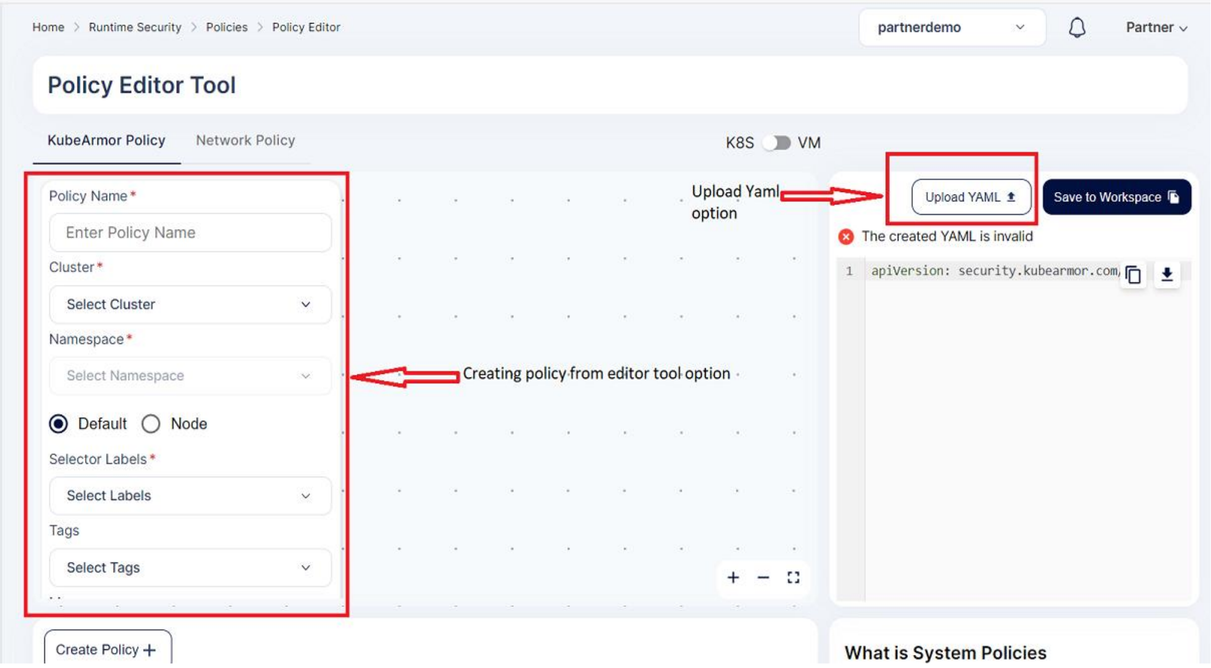


Policies

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

□	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
□	autopol-system-2096115234 KubeArmor	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=mysql-malac...	None
□	autopol-system-1021014936 KubeArmor	Discovered	● Inactive	aks-demo-prod	default	app.kubernetes.... +2	None
□	autopol-egress-3275896150 Kubernetes Network	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	None
□	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



Policy Editor Tool

Policy Name *: Enter Policy Name

Cluster *: Select Cluster

Namespace *: Select Namespace

● Default ○ Node

Selector Labels *: Select Labels

Tags: Select Tags

Upload Yaml option

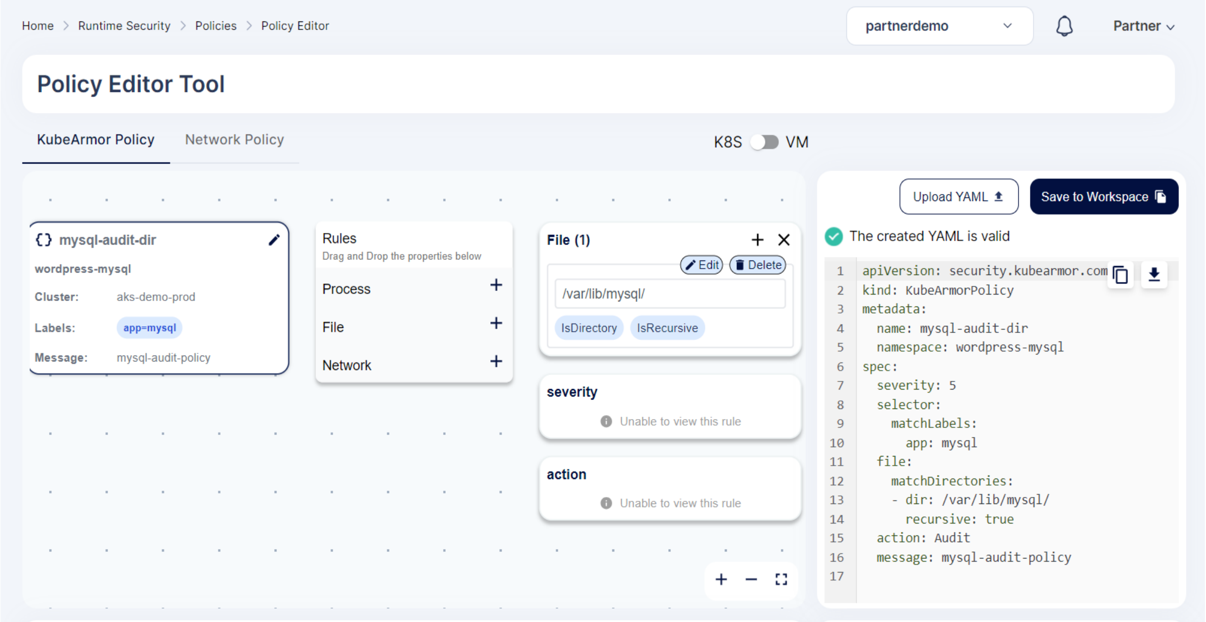
Creating policy from editor tool option

The created YAML is invalid

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

What is System Policies

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



Policy Editor Tool

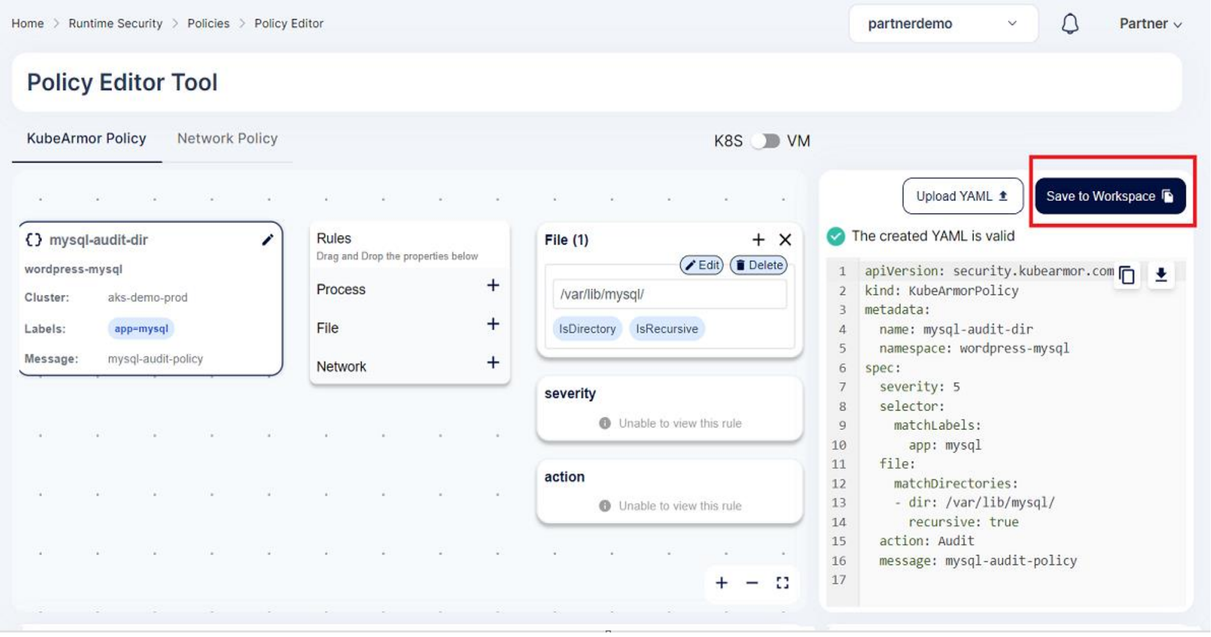
mysql-audit-dir
wordpress-mysql
Cluster: aks-demo-prod
Labels: app=mysql
Message: mysql-audit-policy

/var/lib/mysql/

The created YAML is valid

```
apiVersion: security.kubearmor.com
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



Policy Editor Tool

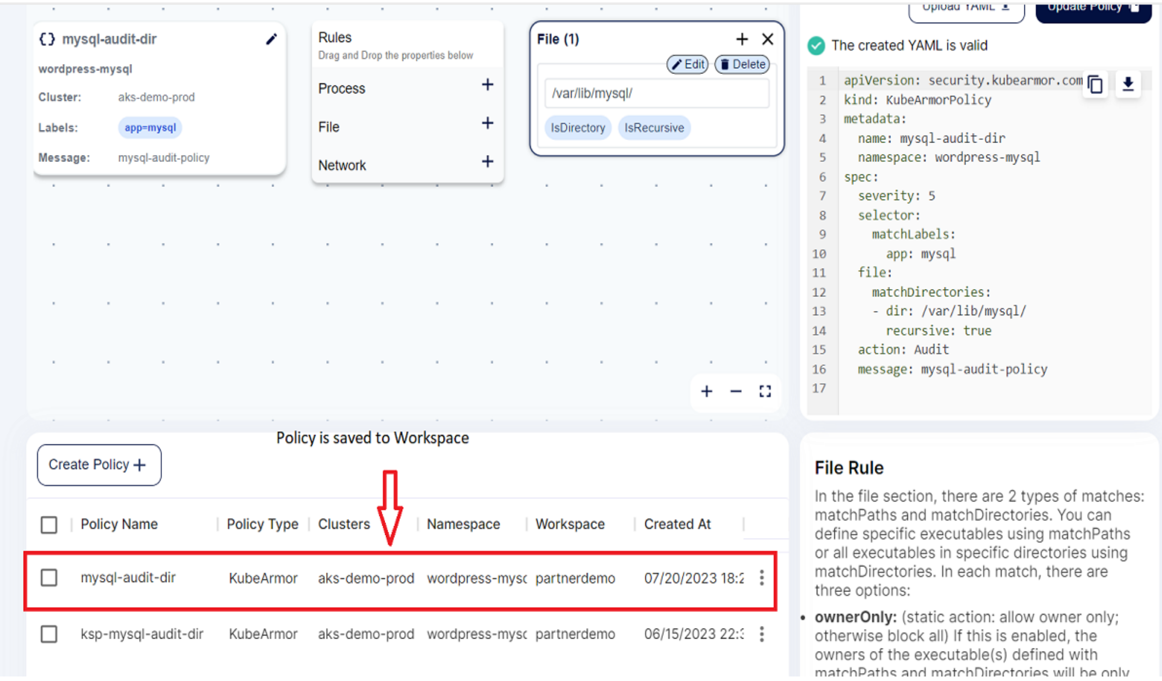
mysql-audit-dir
wordpress-mysql
Cluster: aks-demo-prod
Labels: app=mysql
Message: mysql-audit-policy

/var/lib/mysql/

The created YAML is valid

```
apiVersion: security.kubearmor.com
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 created YAML is valid

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

Policy is saved to Workspace

Create Policy +

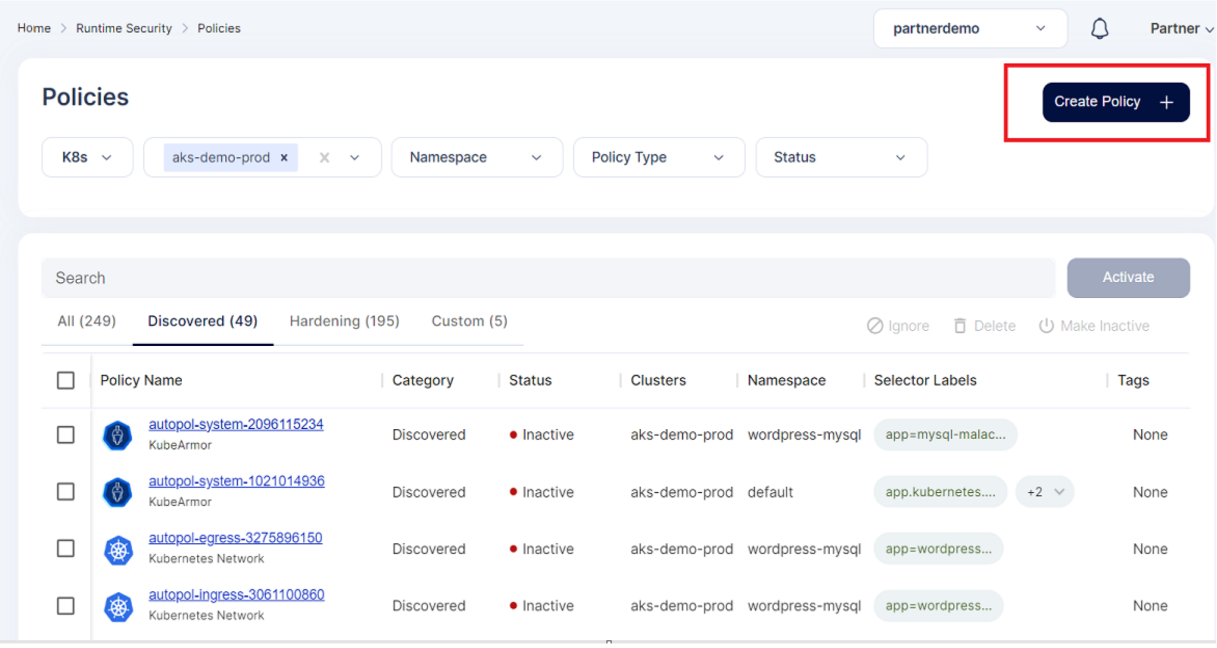
□	Policy Name	Policy Type	Clusters	Namespace	Workspace	Created At
□	mysql-audit-dir	KubeArmor	aks-demo-prod	wordpress-mysc	partnerdemo	07/20/2023 18:2
□	ksp-mysql-audit-dir	KubeArmor	aks-demo-prod	wordpress-mysc	partnerdemo	06/15/2023 22::

File Rule

In the file section, there are 2 types of matches: matchPaths and matchDirectories. You can define specific executables using matchPaths or all executables in specific directories using matchDirectories. In each match, there are three options:

- **ownerOnly:** (static action: allow owner only; otherwise block all) If this is enabled, the owners of the executable(s) defined with matchPaths and matchDirectories will be only

- 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

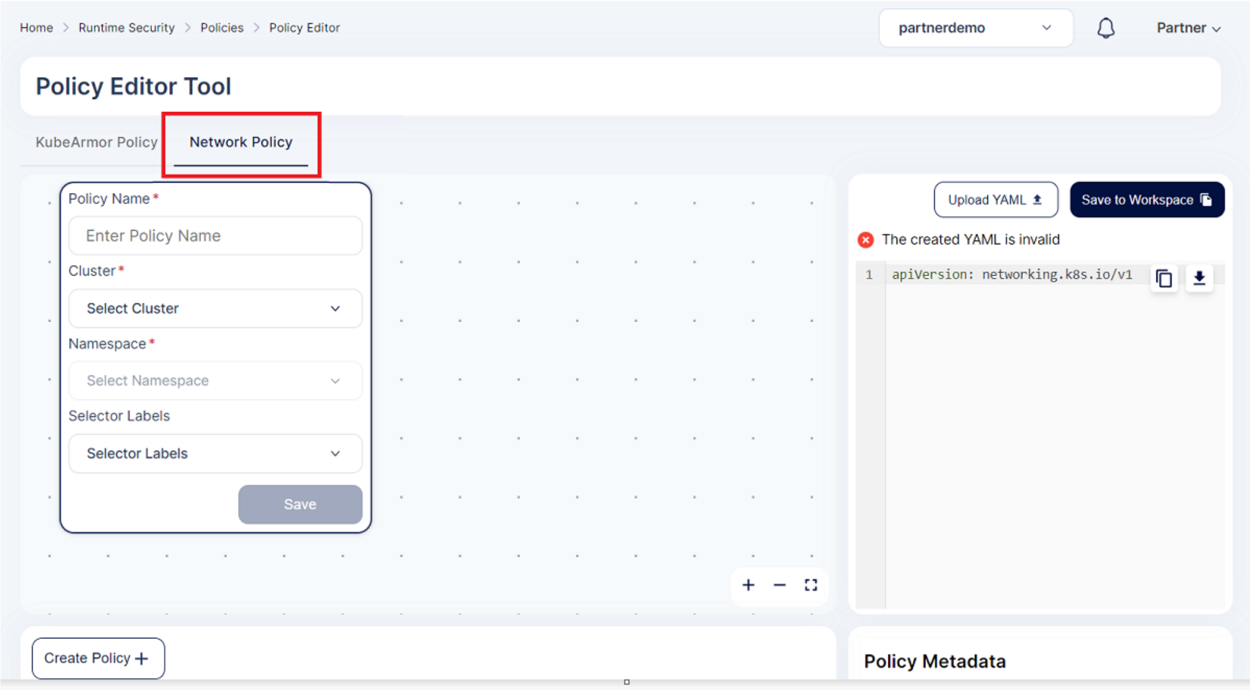


Policies

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

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

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



Home > Runtime Security > Policies > Policy Editor

Policy Editor Tool

Policy Name *: Enter Policy Name

Cluster *: Select Cluster

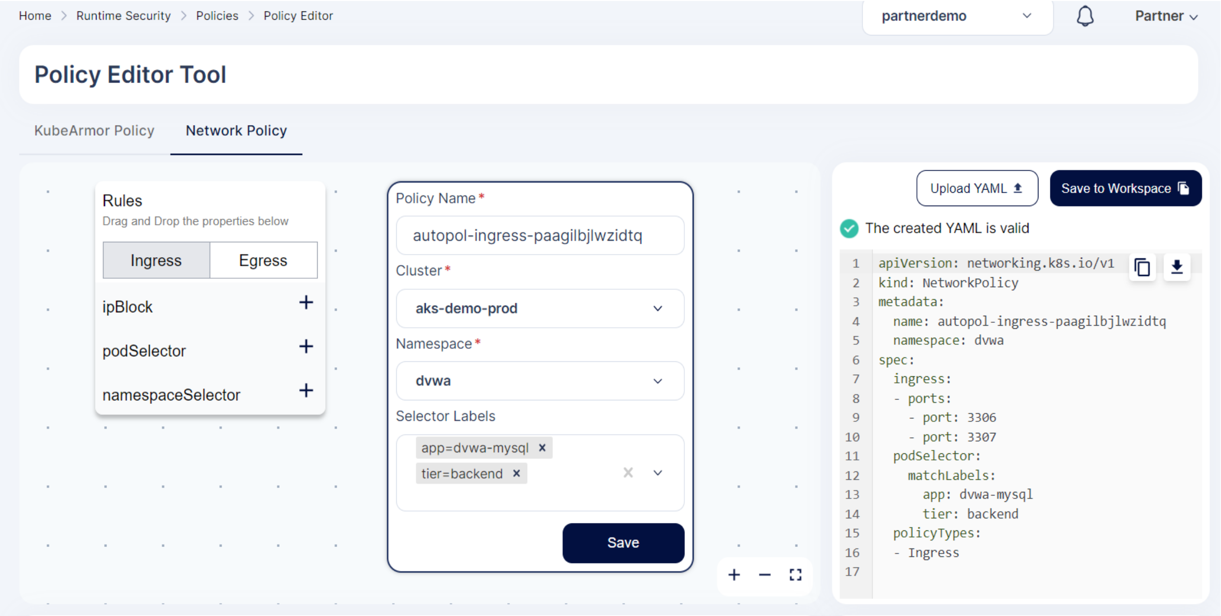
Namespace *: Select Namespace

Selector Labels: Selector Labels

The created YAML is invalid

```
apiVersion: networking.k8s.io/v1
```

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



Home > Runtime Security > Policies > Policy Editor

Policy Editor Tool

Policy Name *: autopol-ingress-paagilbjlwzidtq

Cluster *: aks-demo-prod

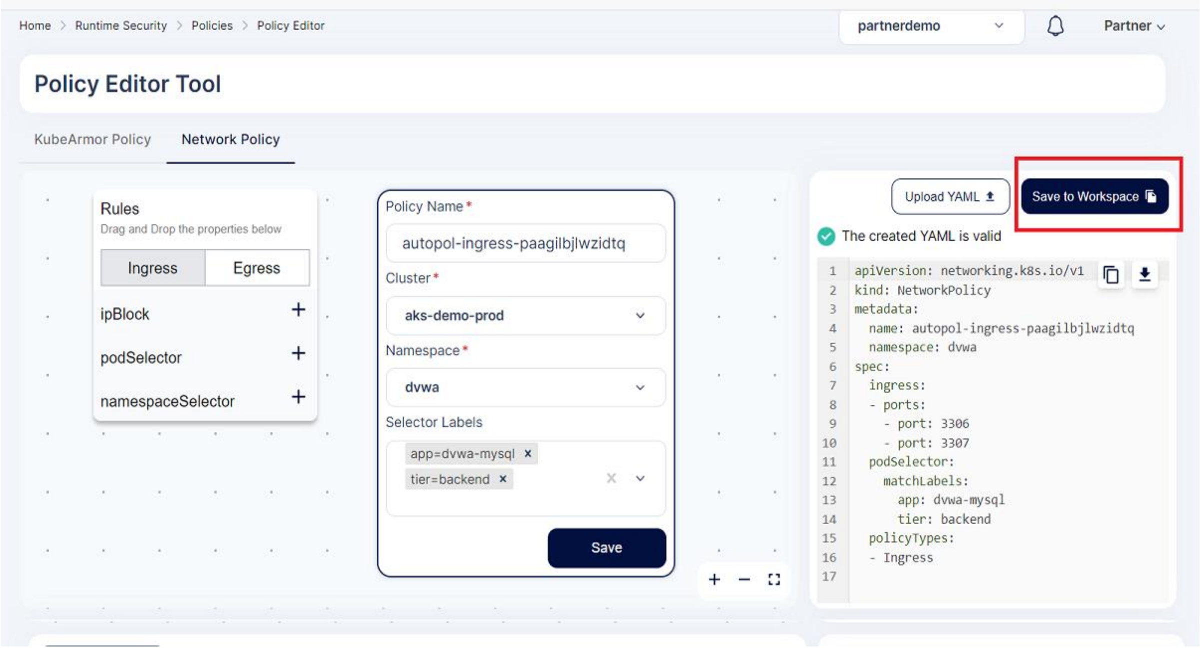
Namespace *: dvwa

Selector Labels: app=dvwa-mysql × tier=backend ×

The created YAML is valid

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: autopol-ingress-paagilbjlwzidtq
  namespace: dvwa
spec:
  ingress:
  - ports:
    - port: 3306
    - port: 3307
  podSelector:
    matchLabels:
      app: dvwa-mysql
      tier: backend
  policyTypes:
  - Ingress
```

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



Policy Editor Tool

Policy Name*: autopol-ingress-paagilbjlwzidtq

Cluster*: aks-demo-prod

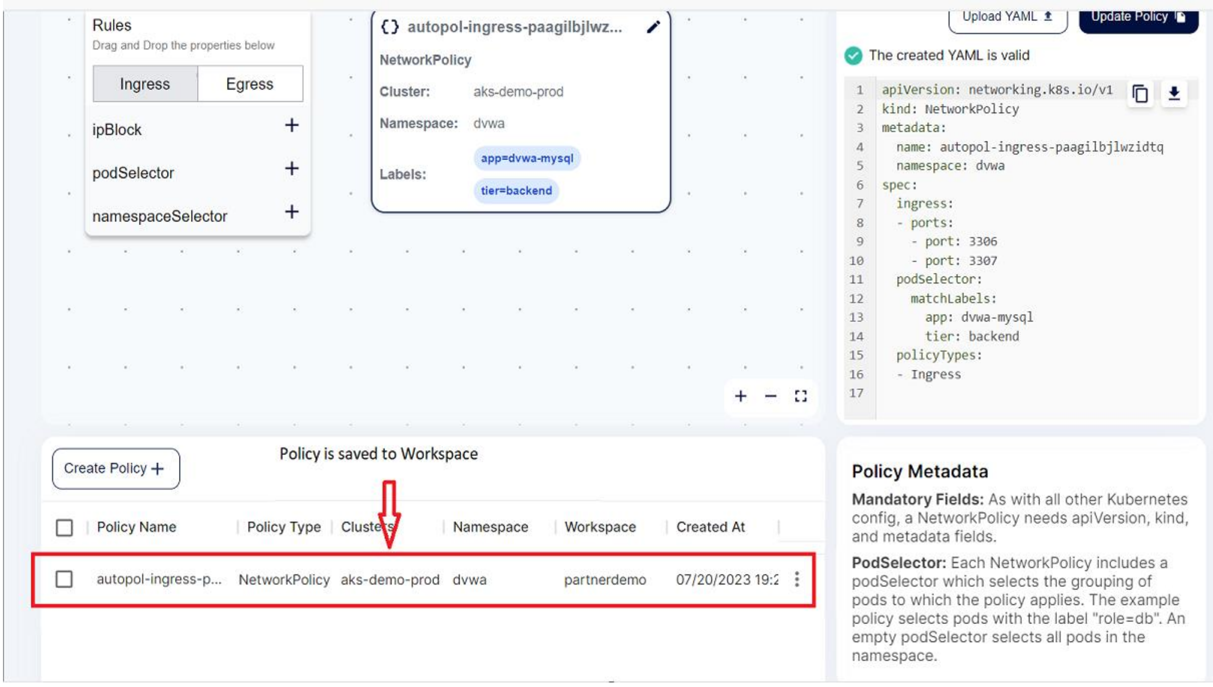
Namespace*: dvwa

Selector Labels: app=dvwa-mysql × tier=backend ×

The created YAML is valid

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: autopol-ingress-paagilbjlwzidtq
  namespace: dvwa
spec:
  ingress:
  - ports:
    - port: 3306
    - port: 3307
  podSelector:
    matchLabels:
      app: dvwa-mysql
      tier: backend
  policyTypes:
  - Ingress
```

- After that policy will be saved to the workspace.



{} autopol-ingress-paagilbjlwz...

NetworkPolicy

Cluster: aks-demo-prod

Namespace: dvwa

Labels: app=dvwa-mysql tier=backend

The created YAML is valid

```
apiVersion: networking.k8s.io/v1
kind: NetworkPolicy
metadata:
  name: autopol-ingress-paagilbjlwzidtq
  namespace: dvwa
spec:
  ingress:
  - ports:
    - port: 3306
    - port: 3307
  podSelector:
    matchLabels:
      app: dvwa-mysql
      tier: backend
  policyTypes:
  - Ingress
```

Policy is saved to Workspace

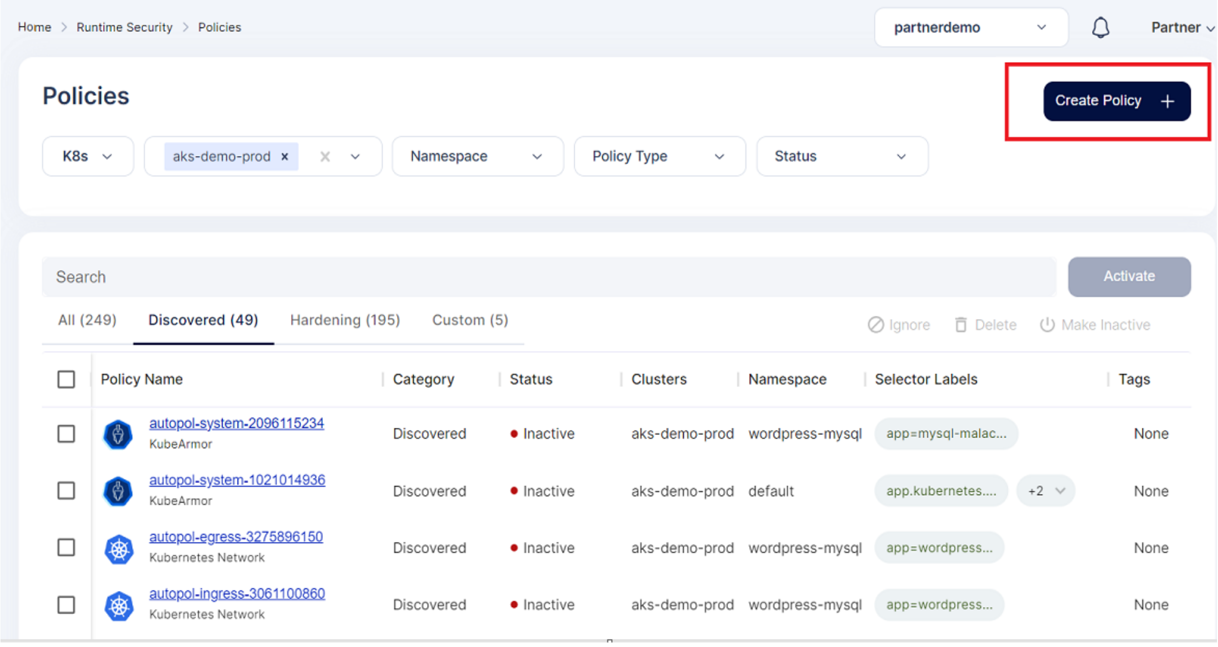
☐	Policy Name	Policy Type	Clusters	Namespace	Workspace	Created At
☐	autopol-ingress-p...	NetworkPolicy	aks-demo-prod	dvwa	partnerdemo	07/20/2023 19:2

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



Home > Runtime Security > Policies

partnerdemo | Partner

Policies

Create Policy +

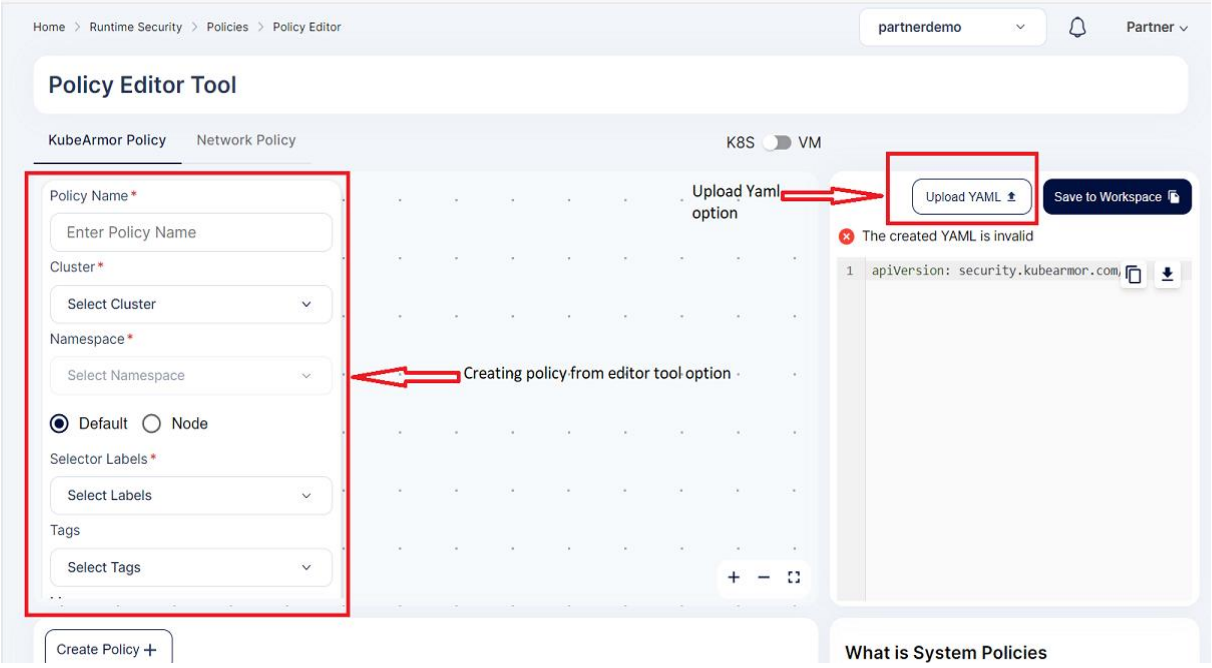
K8s | aks-demo-prod × | Namespace | Policy Type | Status

Search | Activate

All (249) | Discovered (49) | Hardening (195) | Custom (5) | Ignore | Delete | Make Inactive

☐	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	autopol-system-2096115234 KubeArmor	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=mysql-malac...	None
☐	autopol-system-1021014936 KubeArmor	Discovered	● Inactive	aks-demo-prod	default	app.kubernetes.... +2	None
☐	autopol-egress-3275896150 Kubernetes Network	Discovered	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	None
☐	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

partnerdemo | Partner

Policy Editor Tool

KubeArmor Policy | Network Policy | K8S | VM

Policy Name*: Enter Policy Name

Cluster*: Select Cluster

Namespace*: Select Namespace

● Default ○ Node

Selector Labels*: Select Labels

Tags: Select Tags

Upload Yaml option

Upload YAML | Save to Workspace

The created YAML is invalid

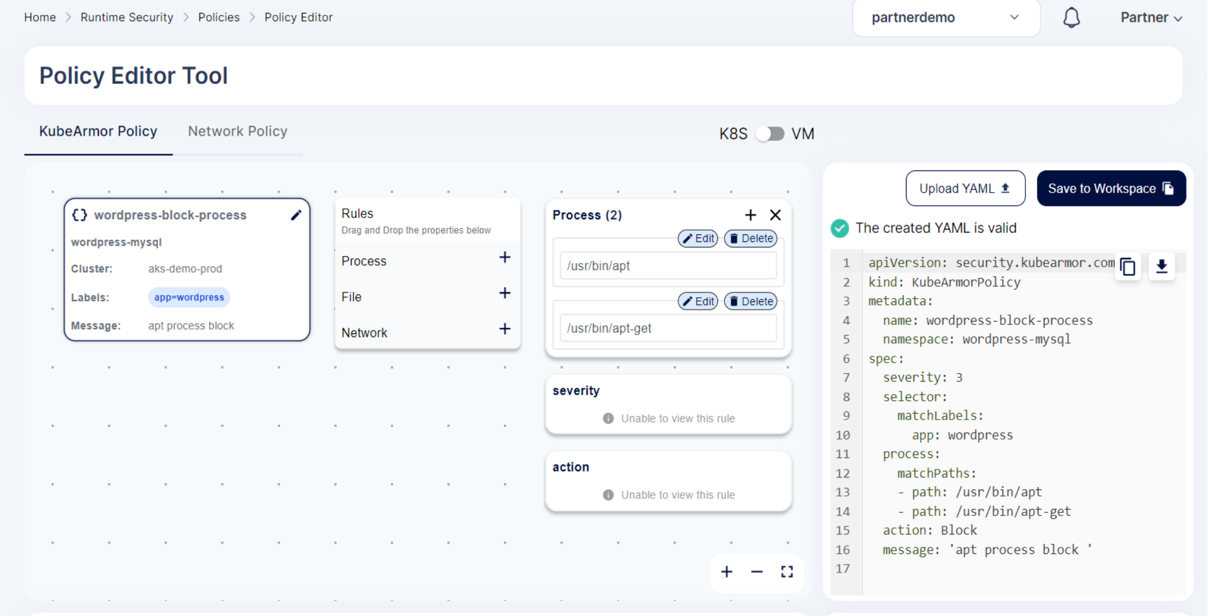
```
apiVersion: security.kubearmor.com,
```

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 uploaded some the columns on the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to apply and click save.



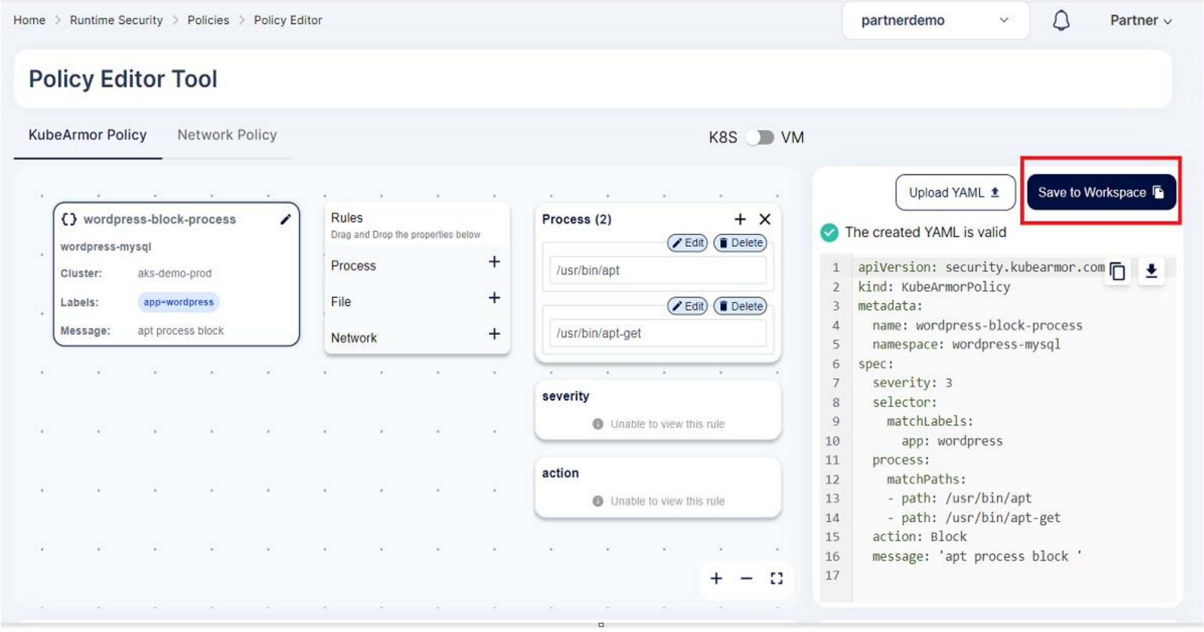
wordpress-block-process
wordpress-mysql
Cluster: aks-demo-prod
Labels: app=wordpress
Message: apt process block

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

The created YAML is valid

```
apiVersion: security.kubearmor.com
kind: KubeArmorPolicy
metadata:
  name: wordpress-block-process
  namespace: wordpress-mysql
spec:
  severity: 3
  selector:
    matchLabels:
      app: wordpress
  process:
    matchPaths:
    - path: /usr/bin/apt
    - path: /usr/bin/apt-get
  action: Block
  message: 'apt process block '
```

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



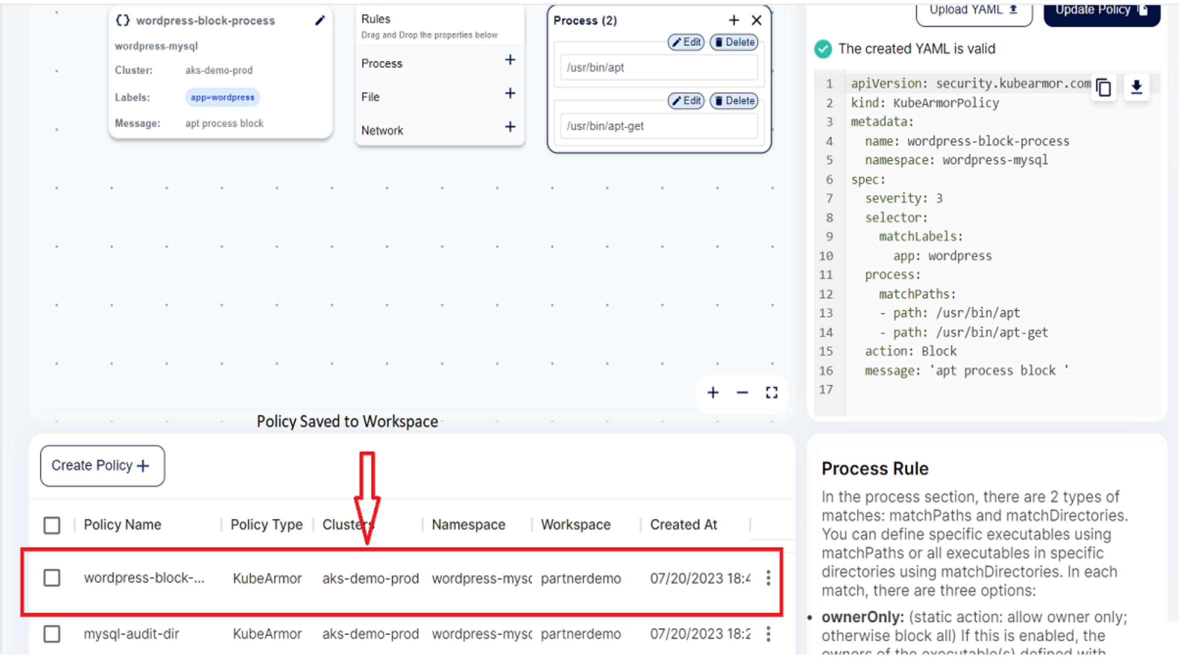
wordpress-block-process
wordpress-mysql
Cluster: aks-demo-prod
Labels: app=wordpress
Message: apt process block

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

The created YAML is valid

```
apiVersion: security.kubearmor.com
kind: KubeArmorPolicy
metadata:
  name: wordpress-block-process
  namespace: wordpress-mysql
spec:
  severity: 3
  selector:
    matchLabels:
      app: wordpress
  process:
    matchPaths:
    - path: /usr/bin/apt
    - path: /usr/bin/apt-get
  action: Block
  message: 'apt process block '
```

- After that policy will be saved to the workspace.



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

/usr/bin/apt

/usr/bin/apt-get

The created YAML is valid

```
apiVersion: security.kubearmor.com
kind: KubeArmorPolicy
metadata:
  name: wordpress-block-process
  namespace: wordpress-mysql
spec:
  severity: 3
  selector:
    matchLabels:
      app: wordpress
  process:
    matchPaths:
    - path: /usr/bin/apt
    - path: /usr/bin/apt-get
  action: Block
  message: 'apt process block '
```

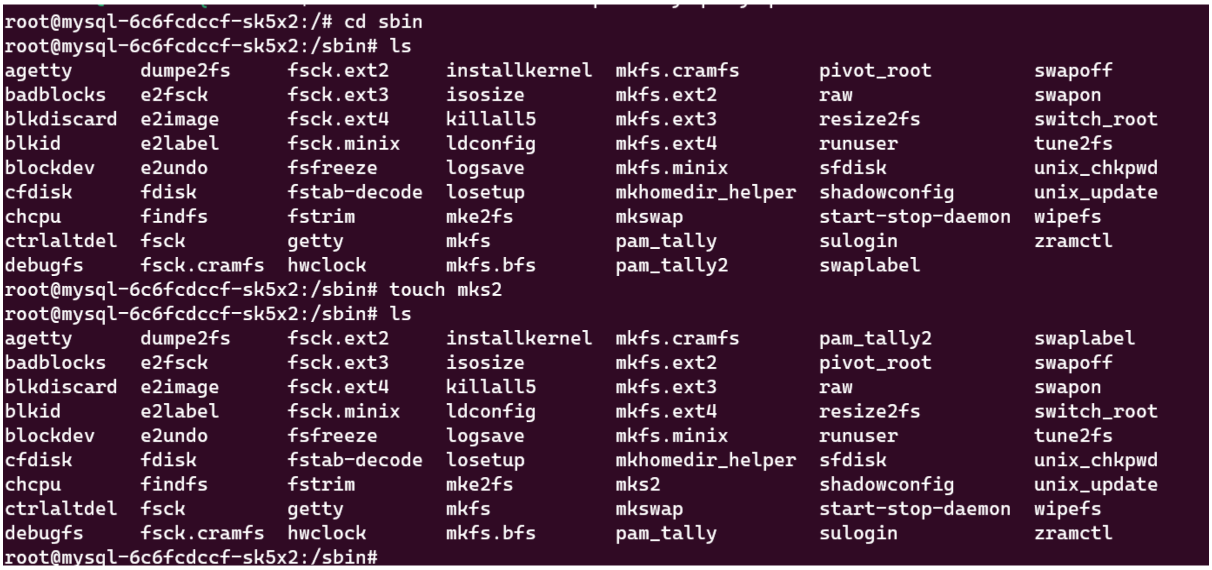
☐	Policy Name	Policy Type	Clusters	Namespace	Workspace	Created At	
☐	wordpress-block-...	KubeArmor	aks-demo-prod	wordpress-mysc	partnerdemo	07/20/2023 18:4	⋮
☐	mysql-audit-dir	KubeArmor	aks-demo-prod	wordpress-mysc	partnerdemo	07/20/2023 18:2	⋮

Process Rule

In the process section, there are 2 types of matches: matchPaths and matchDirectories. You can define specific executables using matchPaths or all executables in specific directories using matchDirectories. In each match, there are three options:

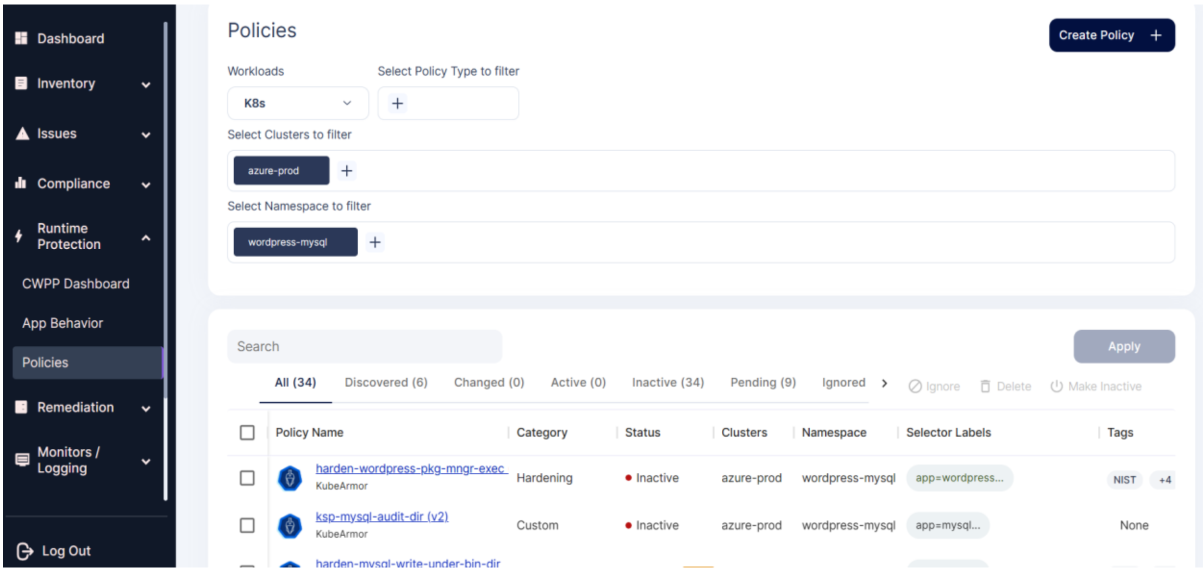
- **ownerOnly:** (static action: allow owner only; otherwise block all) If this is enabled, the owners of the executable(s) defined with

- 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-6c6fcdccf-sk5x2:/# cd sbin
root@mysql-6c6fcdccf-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       unix_update
chcpu       findfs       fstrim        mke2fs         mkswap            start-stop-daemon  wipefs
ctrlaltdel  fsck         getty         mkfs           pam_tally         sulogin            zramctl
debugfs     fsck.cramfs  hwclock       mkfs.bfs       pam_tally2        swaplabel
root@mysql-6c6fcdccf-sk5x2:/sbin# touch mks2
root@mysql-6c6fcdccf-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       mkfs.bfs       pam_tally         sulogin            zramctl
root@mysql-6c6fcdccf-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.



Policies

Workloads: K8s

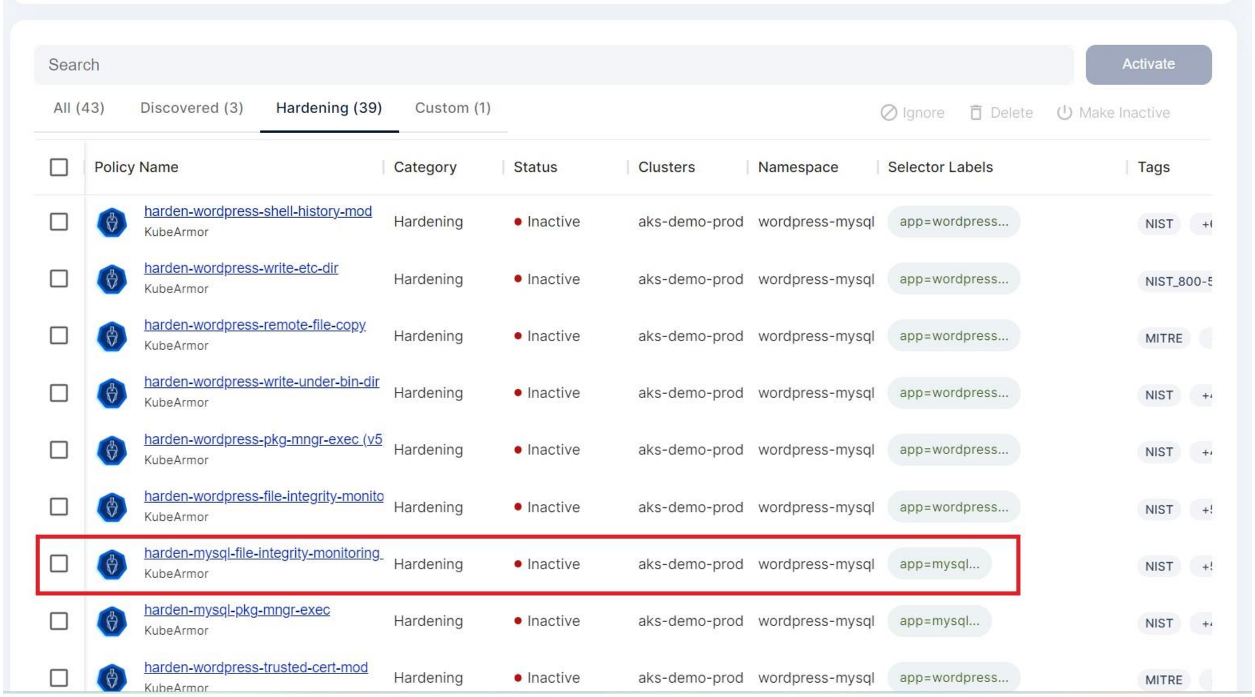
Select Policy Type to filter: +

Select Clusters to filter: azure-prod +

Select Namespace to filter: wordpress-mysql +

☐	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	harden-wordpress-pkg-mngr-exec KubeArmor	Hardening	● Inactive	azure-prod	wordpress-mysql	app=wordpress...	NIST +4
☐	ksp-mysql-audit-dir (v2) KubeArmor	Custom	● Inactive	azure-prod	wordpress-mysql	app=mysql...	None
☐	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

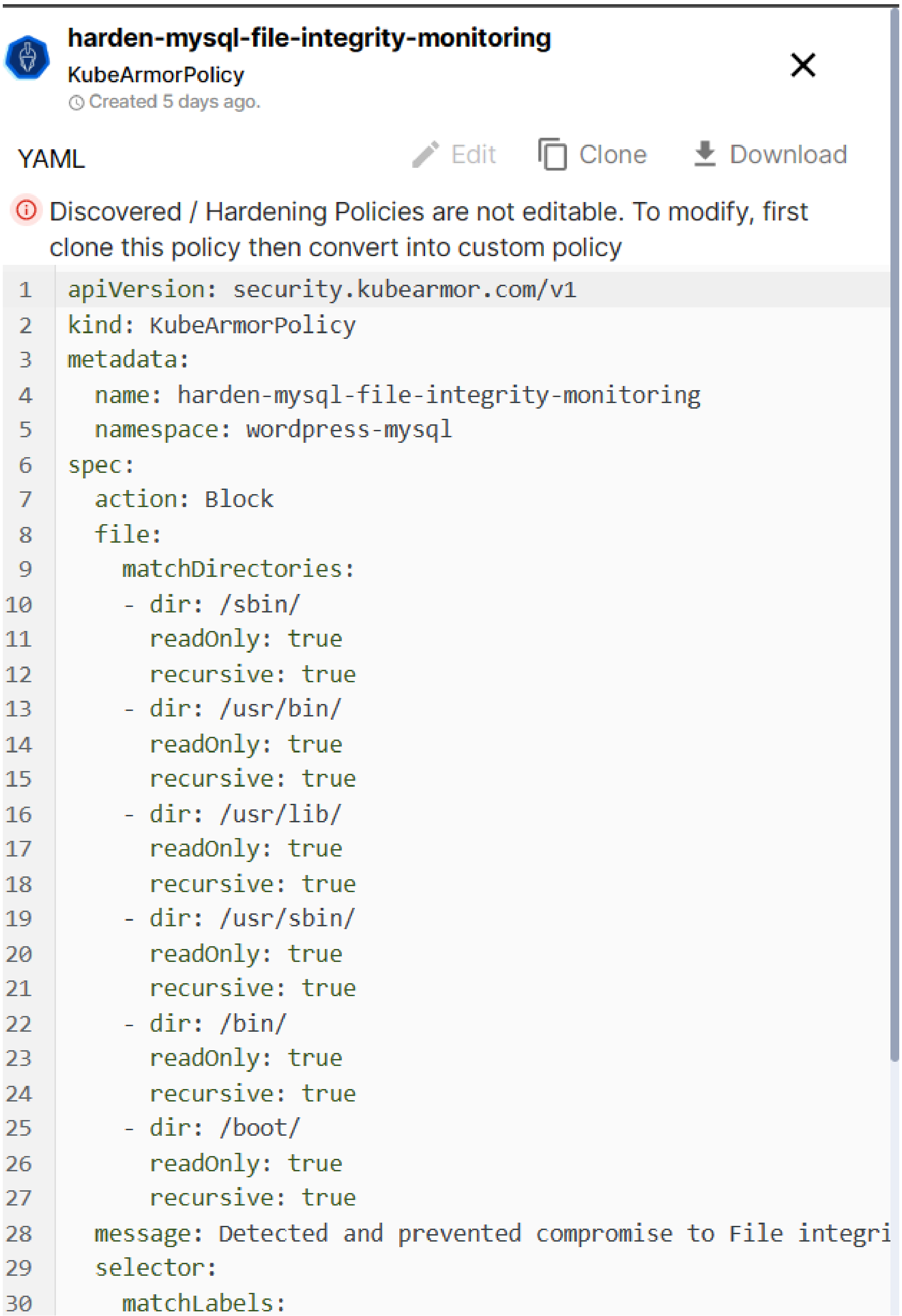
Activate

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

Ignore | Delete | Make Inactive

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

KubeArmorPolicy

Created 5 days ago.

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

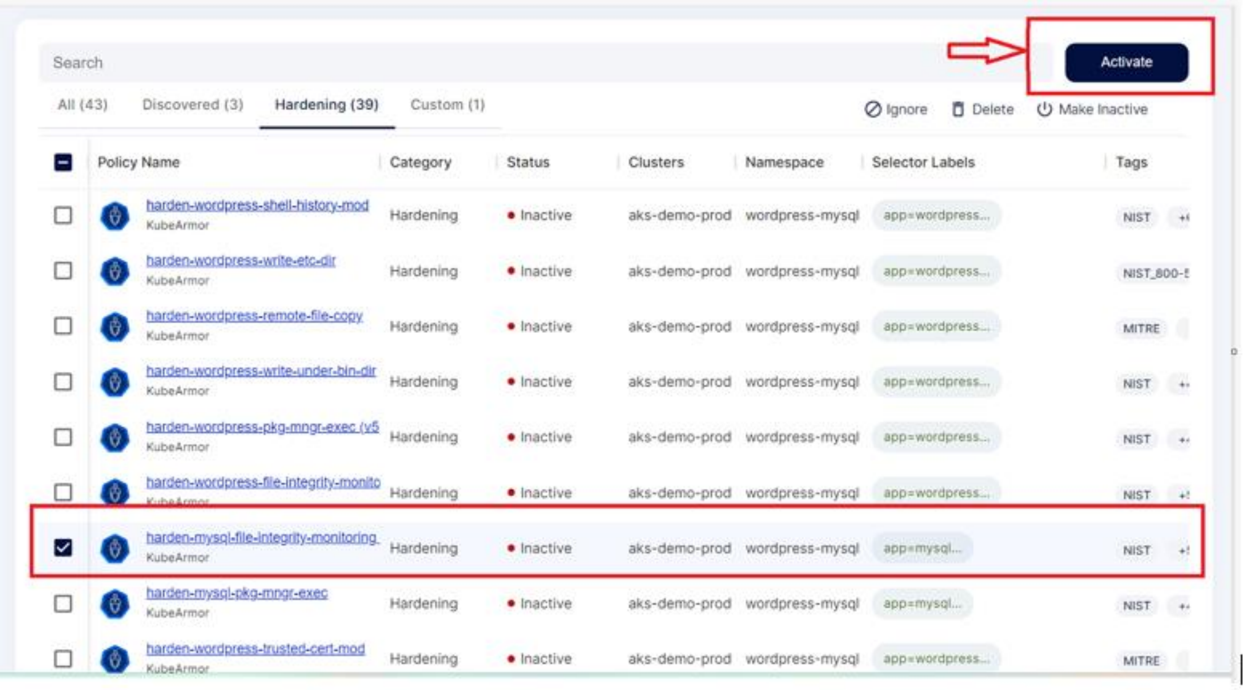
```yaml
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: harden-mysql-file-integrity-monitoring
  namespace: wordpress-mysql
spec:
  action: Block
  file:
    matchDirectories:
    - dir: /sbin/
      readOnly: true
      recursive: true
    - dir: /usr/bin/
      readOnly: 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 integri
  selector:
    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
```

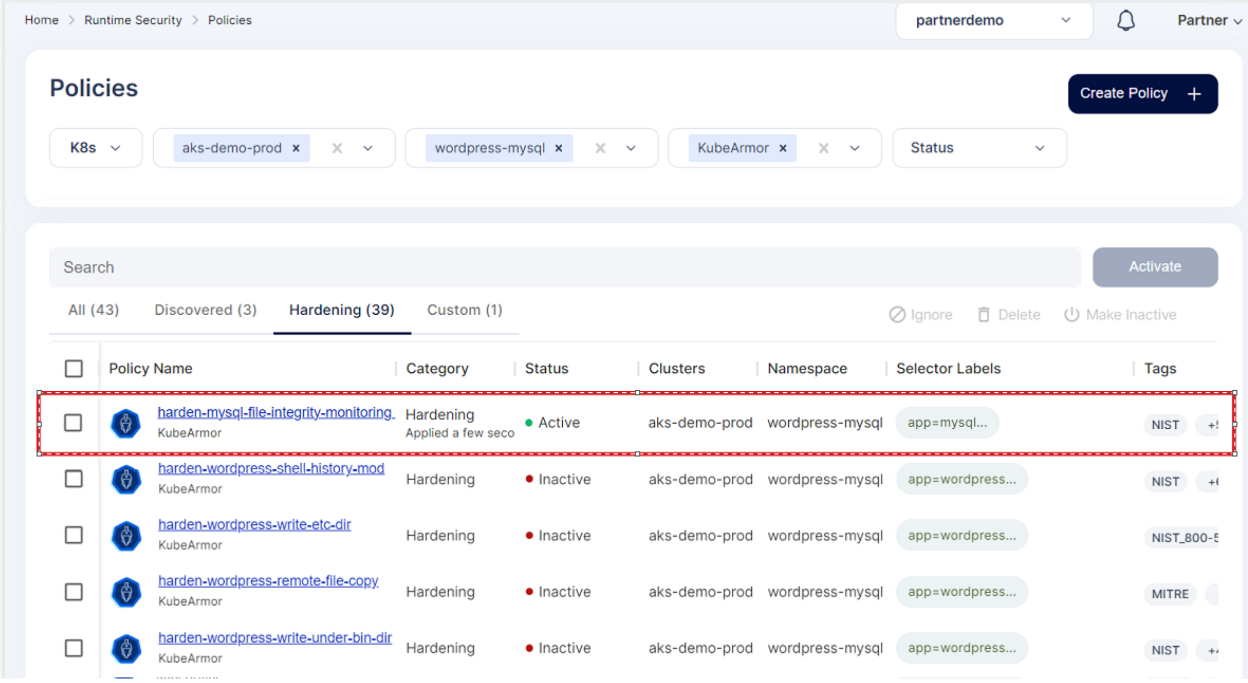
```
metadata:
name: harden-mysql-file-integrity-monitoring
namespace: wordpress-mysql
spec:
action: Block
file:
matchDirectories:
- dir: /sbin/
readOnly: true
recursive: true
- dir: /usr/bin/
readOnly: true
recursive: true
- dir: /usr/lib/
readOnly: true
recursive: true
- dir: /usr/sbin/
readOnly: true
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



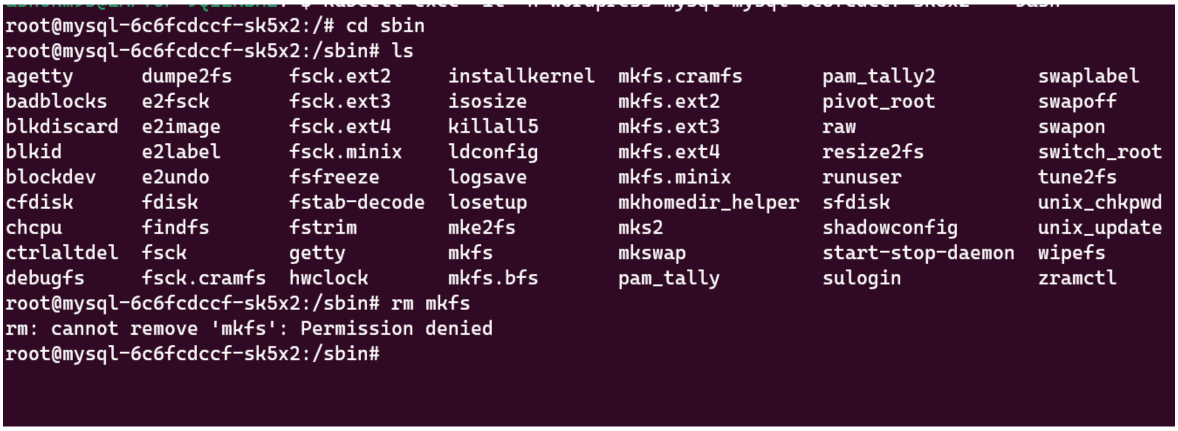
	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	harden-wordpress-shell-history-mod KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +(
☐	harden-wordpress-write-etc-dir KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...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

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



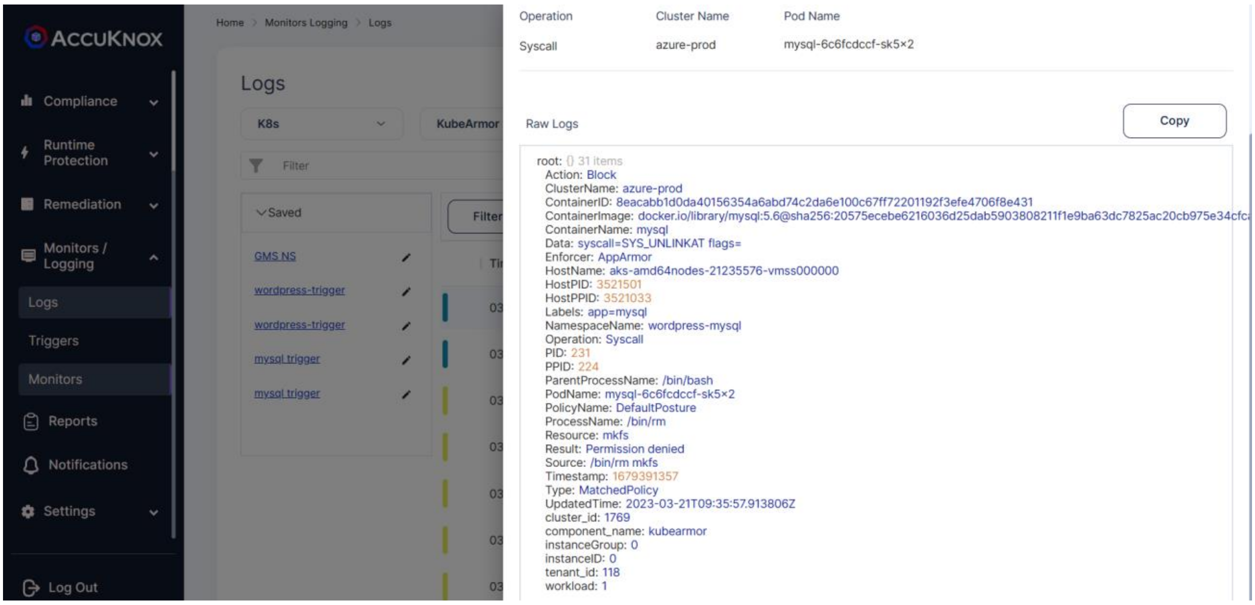
	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
☐	harden-mysql-file-integrity-monitoring KubeArmor	Hardening Applied a few seco	● Active	aks-demo-prod	wordpress-mysql	app=mysql...	NIST +!
☐	harden-wordpress-shell-history-mod KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql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



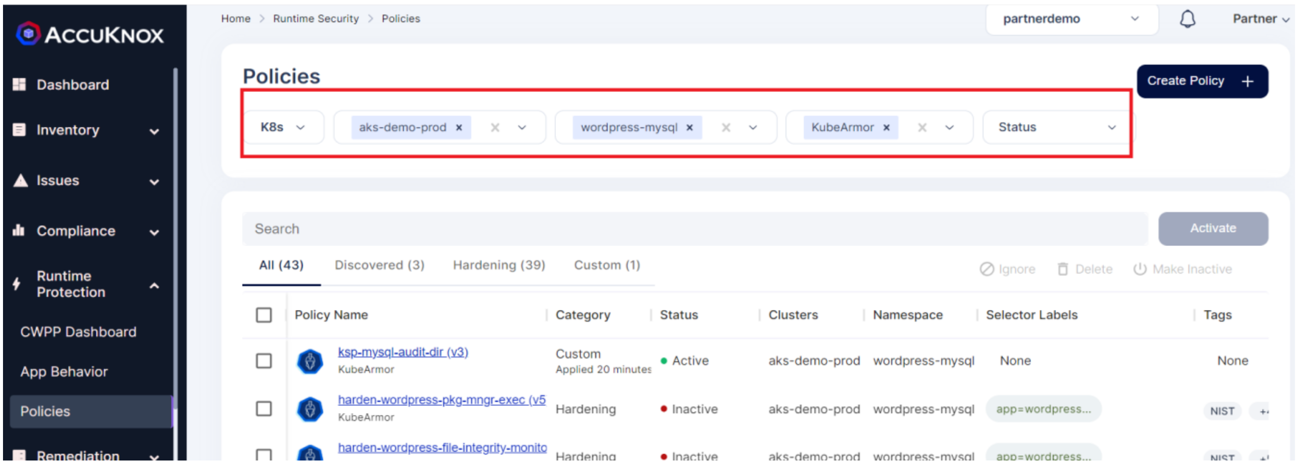
Operation	Cluster Name	Pod Name
Syscall	azure-prod	mysql-6c6fcdccf-sk5×2

Raw Logs

```
root: {} 31 items
  Action: Block
  ClusterName: azure-prod
  ContainerID: 8eacabb1d0da40156354a6abd74c2da6e100c67ff72201192f3efe4706f8e431
  ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab5903808211f1e9ba63dc7825ac20cb975e34cfc
  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-sk5×2
  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: 1
```

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



Policies

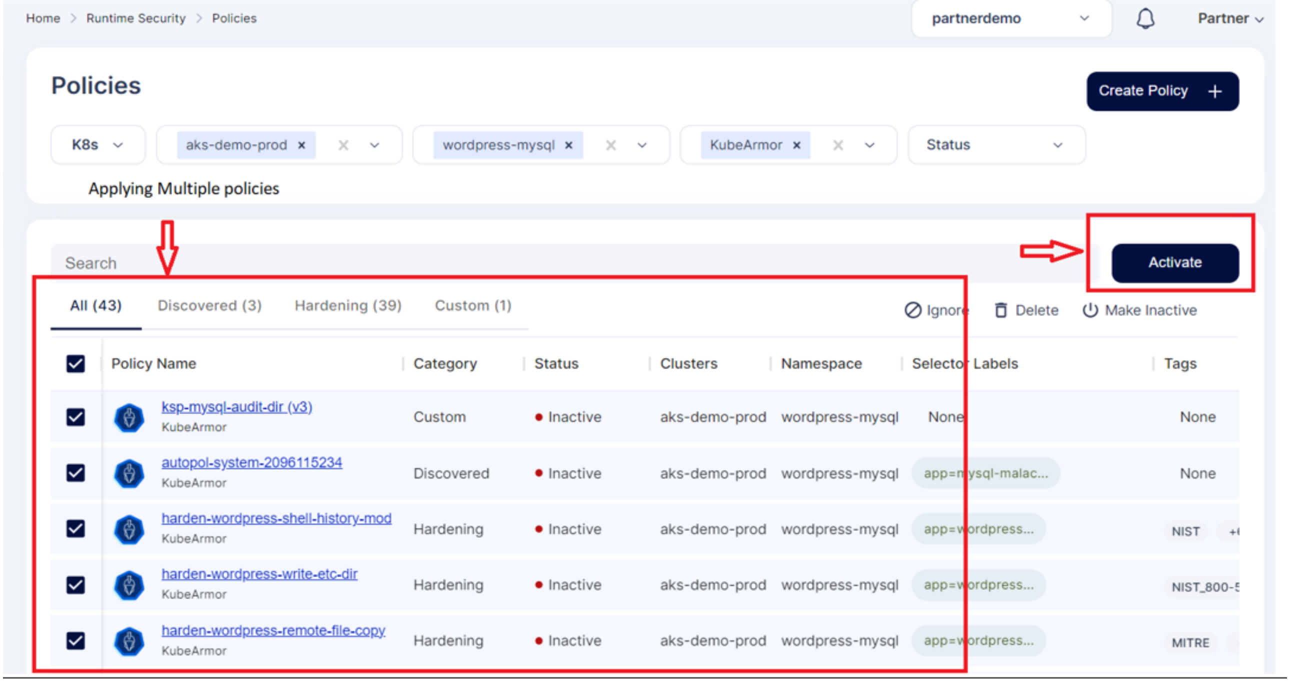
K8s | aks-demo-prod × | wordpress-mysql × | KubeArmor × | Status

Search

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

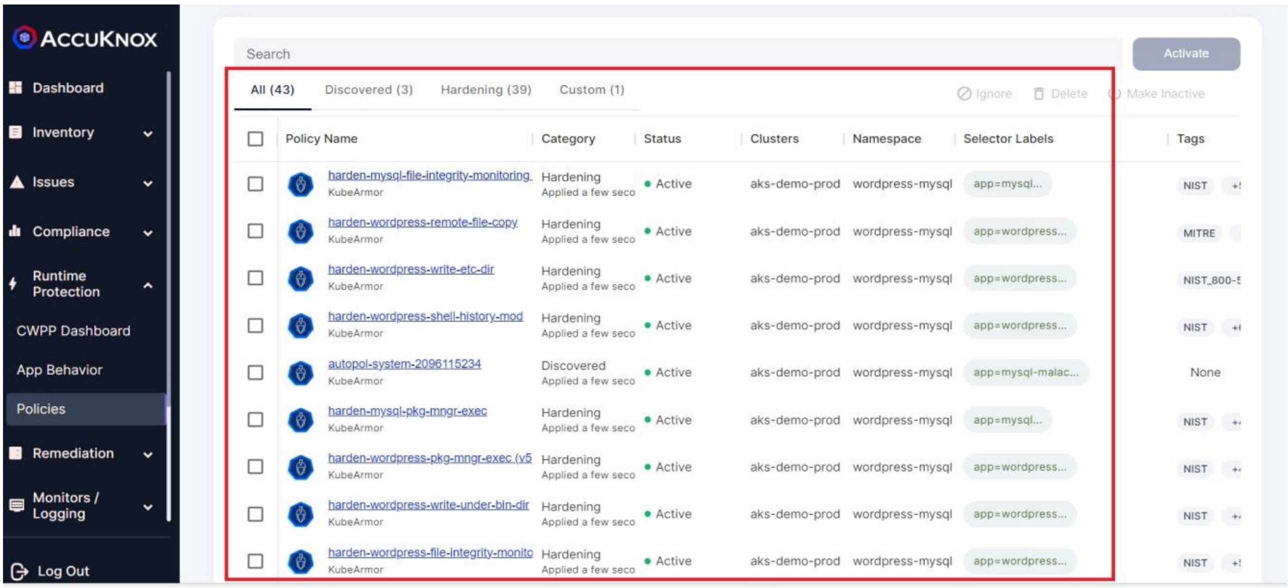
□	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
□	ksp-mysql-audit-dir (v3) KubeArmor	Custom Applied 20 minutes	● Active	aks-demo-prod	wordpress-mysql	None	None
□	harden-wordpress-pkg-mngr-exec (v5 KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +·
□	harden-wordpress-file-integrity-monito	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST +·

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



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

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



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

Integrations

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 Depolyed and HEC URL generated first for Splunk Integration.

Integration of Splunk:

a. Prerequisites:

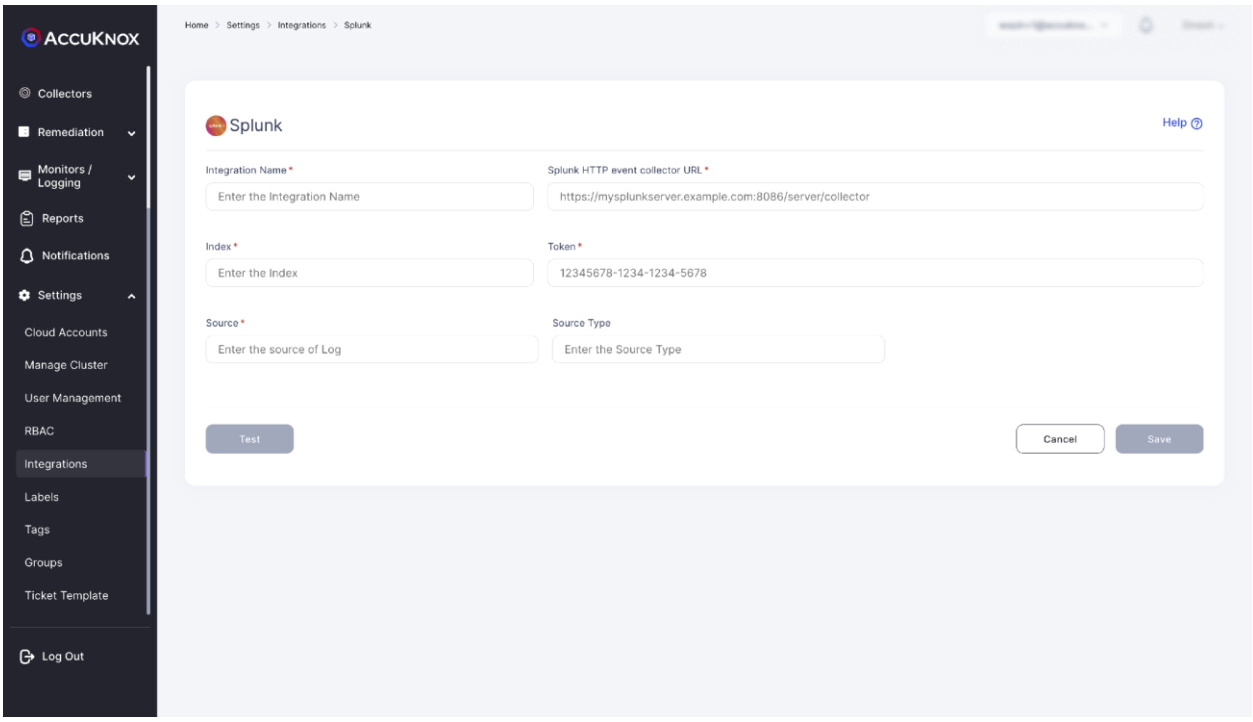
Set up Splunk HTTP Event Collector (HEC) to view alert notifications from AccuKnox in Splunk. Splunk HEC lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols.

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.



Splunk

Integration Name * : Enter the Integration Name

Splunk HTTP event collector URL * : https://mysplunkserver.example.com:8086/server/collector

Index * : Enter the Index

Token * : 12345678-1234-1234-5678

Source * : Enter the source of Log

Source Type : Enter the Source Type

- 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 = xxxxxx-deployment-xxxxxx-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.

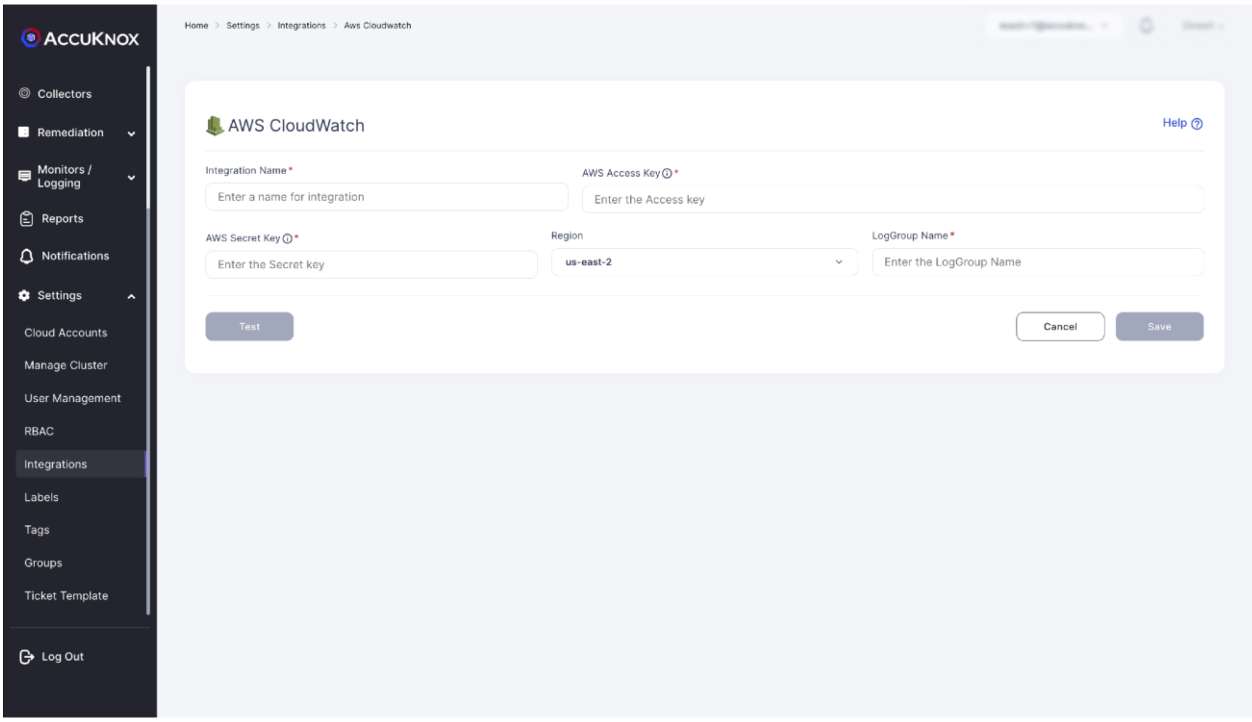
Integration of Amazon CloudWatch:

a. ***Prerequisites***

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

b. ***Steps to Integrate:***

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



Integration Name * : Enter a name for integration
AWS Access Key * : Enter the Access key
AWS Secret Key * : Enter the Secret key
Region: us-east-2
LogGroup Name * : Enter the LogGroup Name

- Here you will 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 evaluate 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:

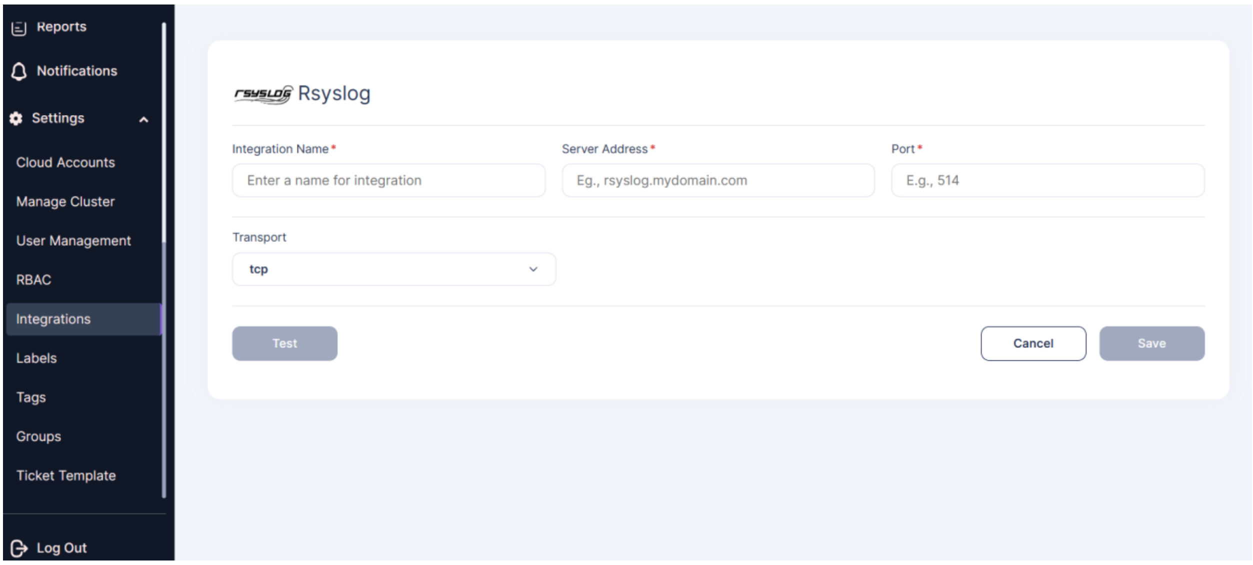
a. ***Prerequisites:***

- 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

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:

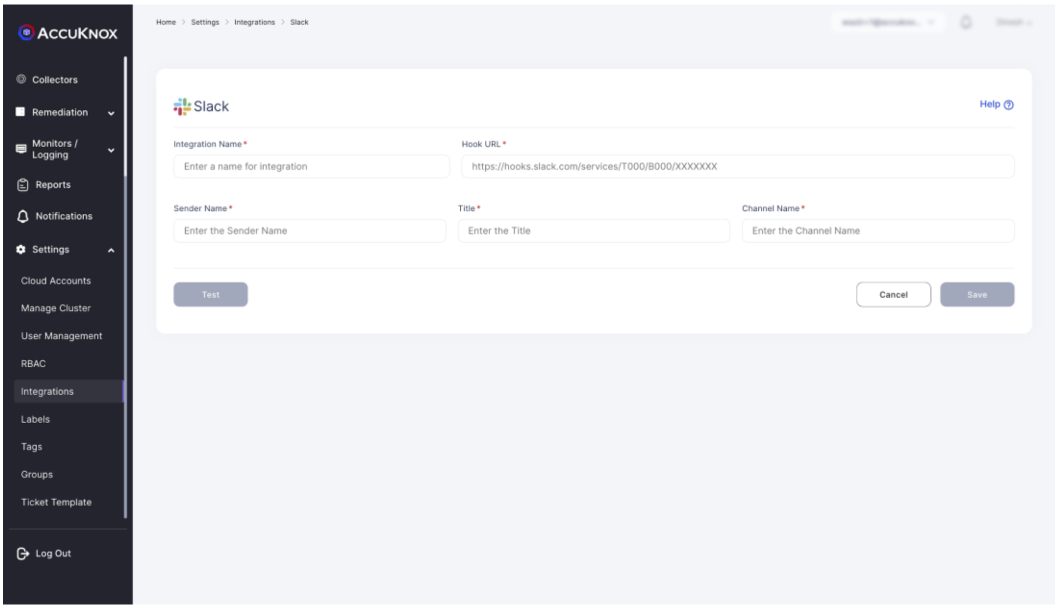
a. Prerequisites:

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.



Slack

Integration Name * Enter a name for integration

Hook URL * https://hooks.slack.com/services/T000/B000/XXXXXXX

Sender Name * Enter the Sender Name

Title * Enter the Title

Channel Name * Enter the Channel Name

- 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/XXXXXXX

- Sender Name: Enter the sender's 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.

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:

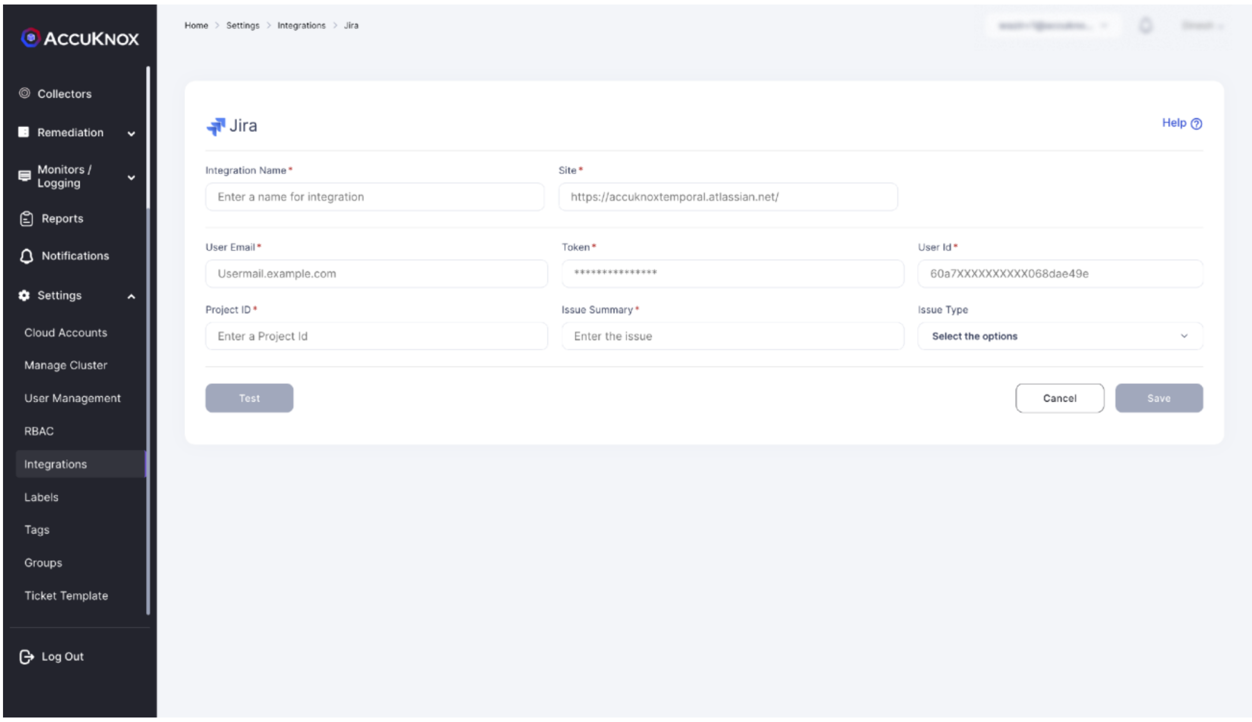
a. Prerequisites

- 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



Jira

Integration Name *: Enter a name for integration

Site *: https://accuknoxtemporal.atlassian.net/

User Email *: Usermail.example.com

Token *: ***************

User Id *: 60a7XXXXXXXXXX068dae49e

Project ID *: Enter a Project Id

Issue Summary *: Enter the issue

Issue Type: Select the options

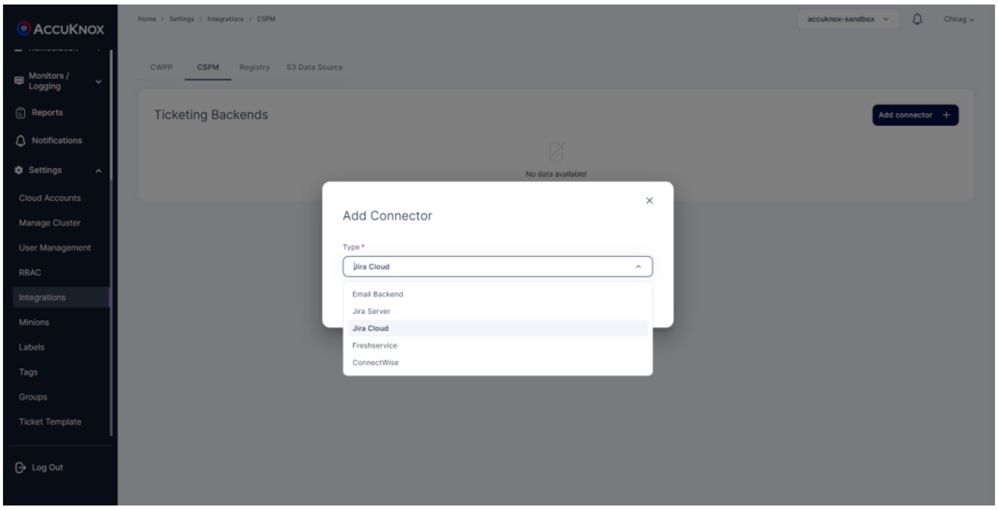
- Enter the following details to configure JIRA.
- **Integration Name**: Enter the name for the integration. You can set any name. e.g., Test JIRA
- **Site**: Enter the site name of your organization. e.g., https://jiratest.atlassian.net/
- **User Email**: Enter your Jira account email address here. e.g., jira@organisation.com
- **Token**: Enter the generated Token here from https://id.atlassian.com/manage-profile/security/api-tokens. .e.g., kRVxxxxxxxxxxxxx39
- **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., 5bbxxxxxxxxxx0103780

- **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, 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

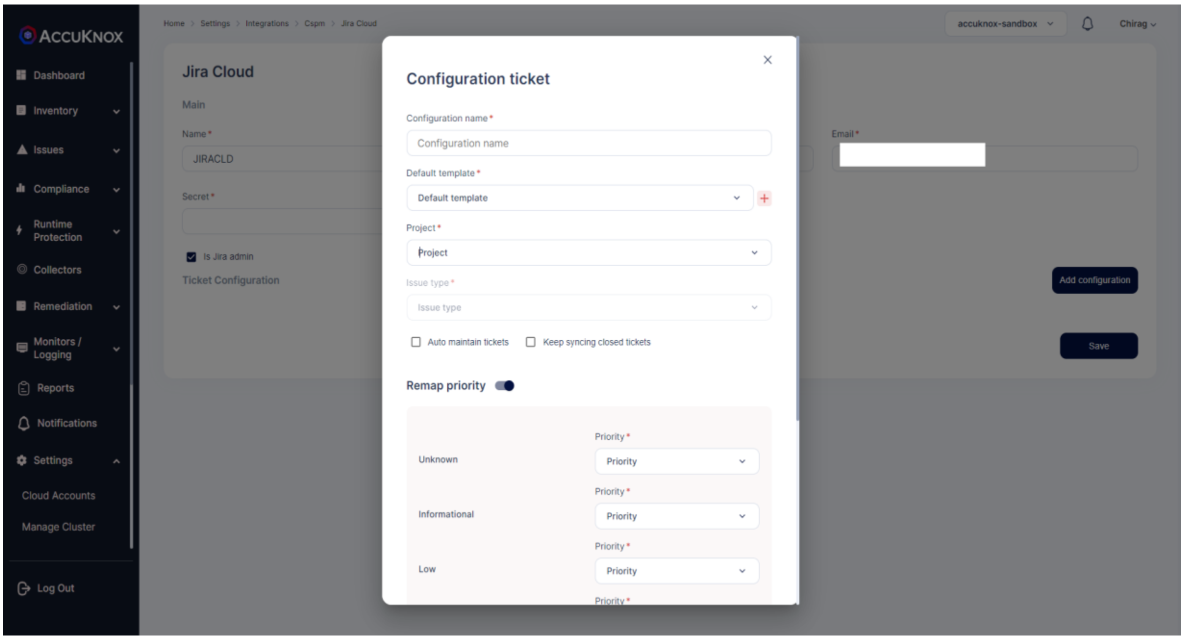


Add Connector

Type *: 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., kRVxxxxxxxxxxxxx39



Jira Cloud

Main

Name * JIRACLD

Secret *

☑ Is Jira admin

Ticket Configuration

Email *

Configuration ticket

Configuration name * Configuration name

Default template * Default template

Project * Project

Issue type * Issue type

□ Auto maintain tickets □ Keep syncing closed tickets

Remap priority

Unknown Priority * Priority

Informational Priority * Priority

Low Priority * Priority

Priority *

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

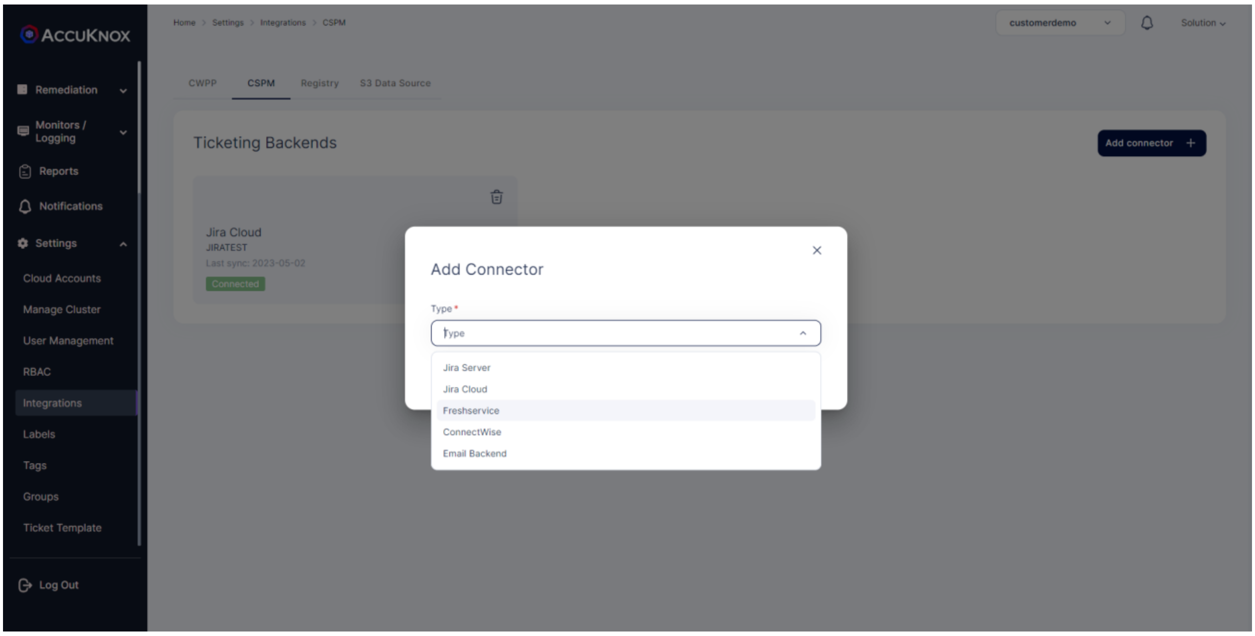
- You need a Company domain, Email & API key (secret) for this integration.

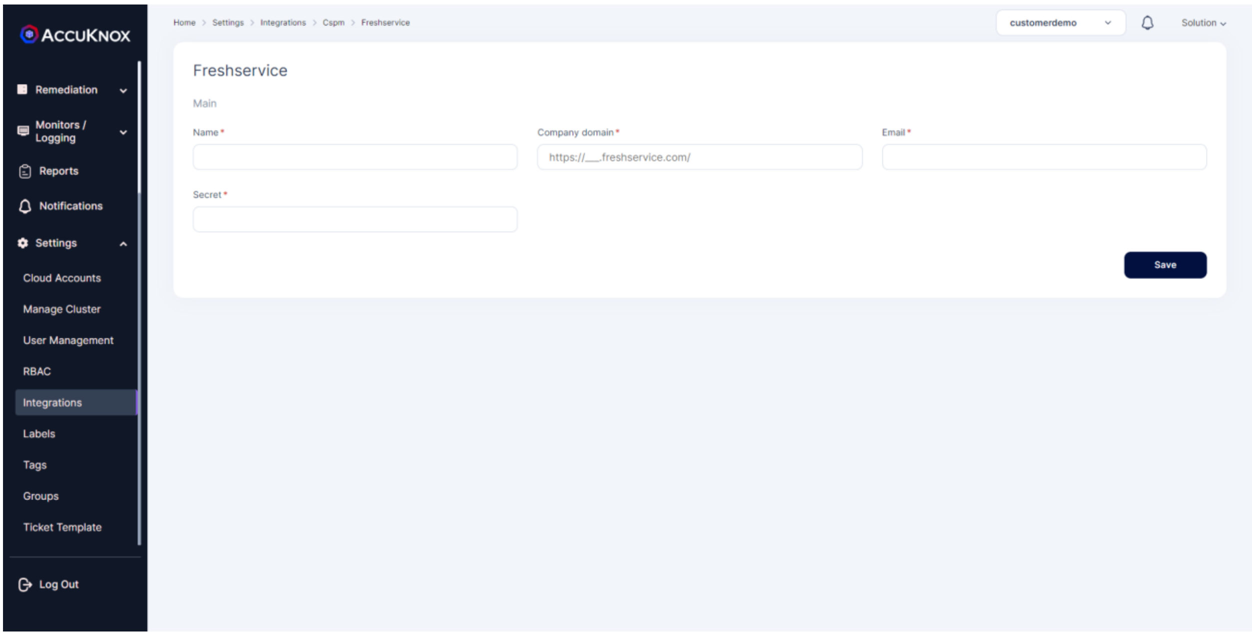
- You can find your API key in profile settings in the right-side column.

b. ***Steps to Integrate:***

- Go to Channel Integration -> CSPM.

- Click on Add the connector and select Freshservice

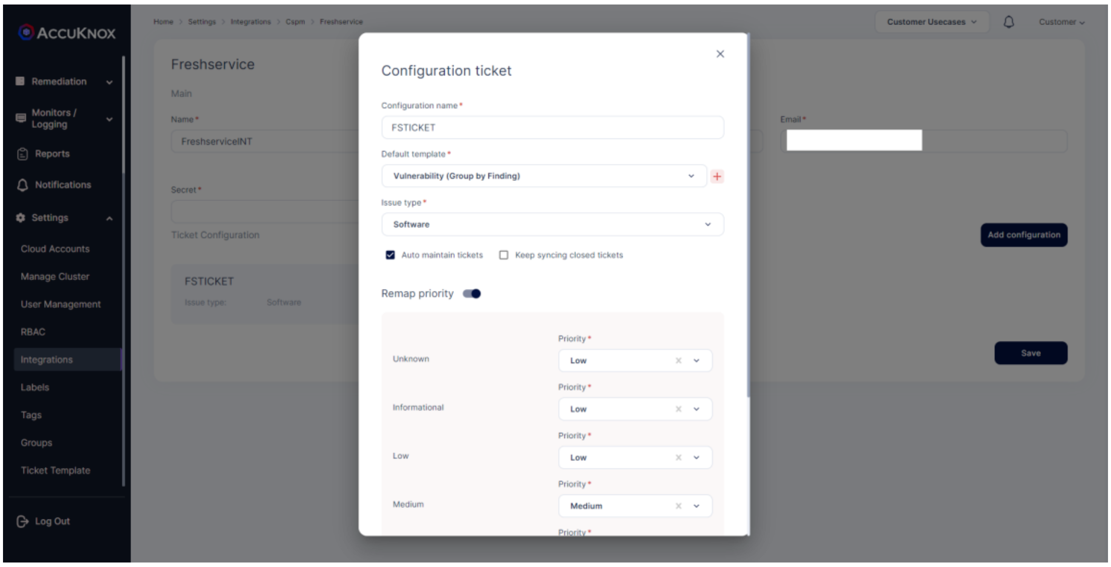




Enter the following details to configure Fresh Service.

- 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.



Freshservice

Main

Name*: FreshserviceINT

Email*

Secret*

Ticket Configuration

FSTICKET
Issue type: Software

Configuration ticket

Configuration name*: FSTICKET

Default template*: Vulnerability (Group by Finding)

Issue type*: Software

☑ Auto maintain tickets ☐ Keep syncing closed tickets

Remap priority

	Priority*
Unknown	Low
Informational	Low
Low	Low
Medium	Medium

Click on the Freshservice ticketing backend to add configuration.

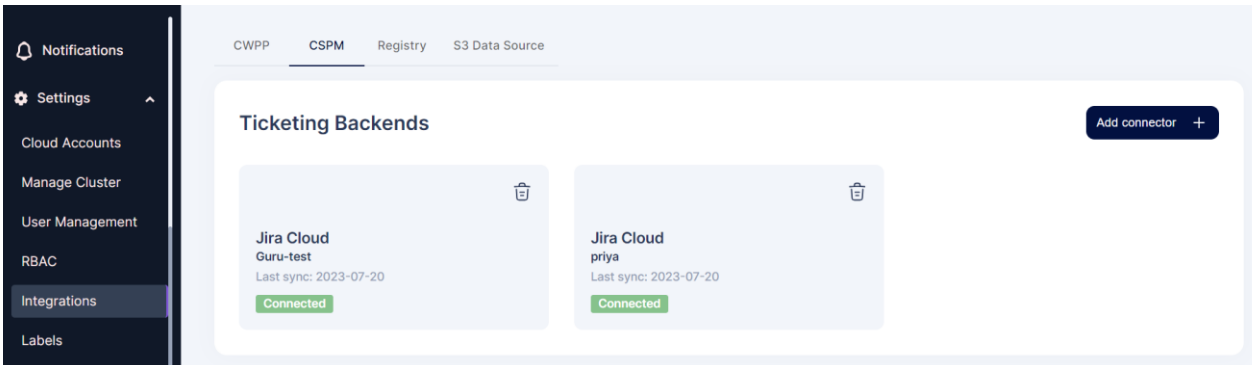
Here Enter the following details:

- 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:

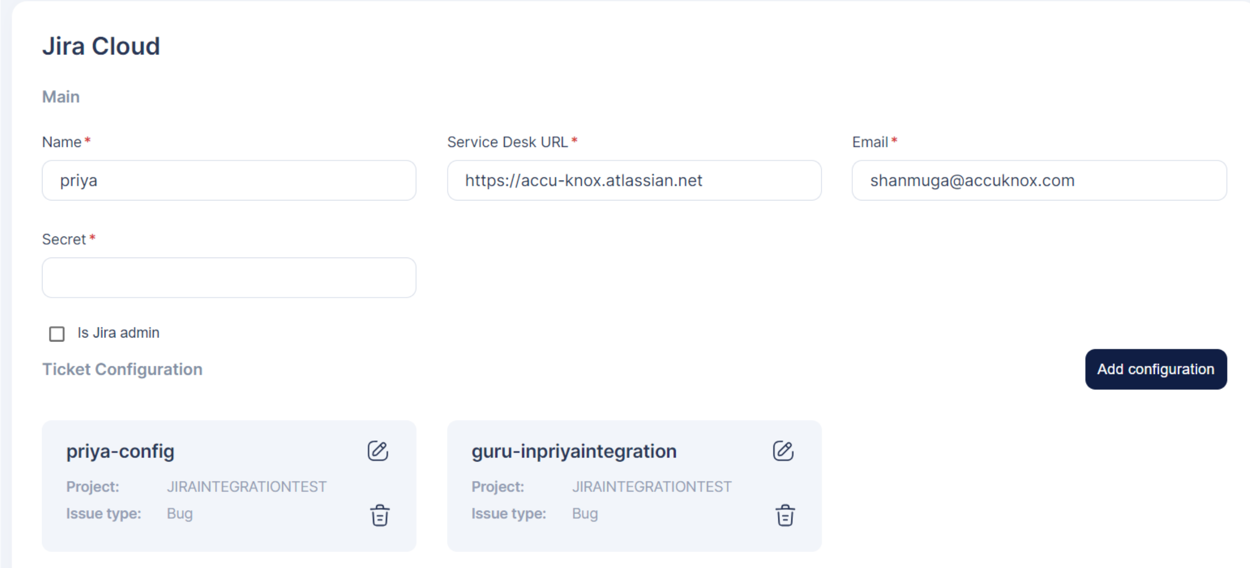


Ticketing Backends

Jira Cloud
Guru-test
Last sync: 2023-07-20
Connected

Jira Cloud
priya
Last sync: 2023-07-20
Connected

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



Jira Cloud

Main

Name * : priya

Service Desk URL * : https://accu-knox.atlassian.net

Email * : shanmuga@accuknox.com

Secret * :

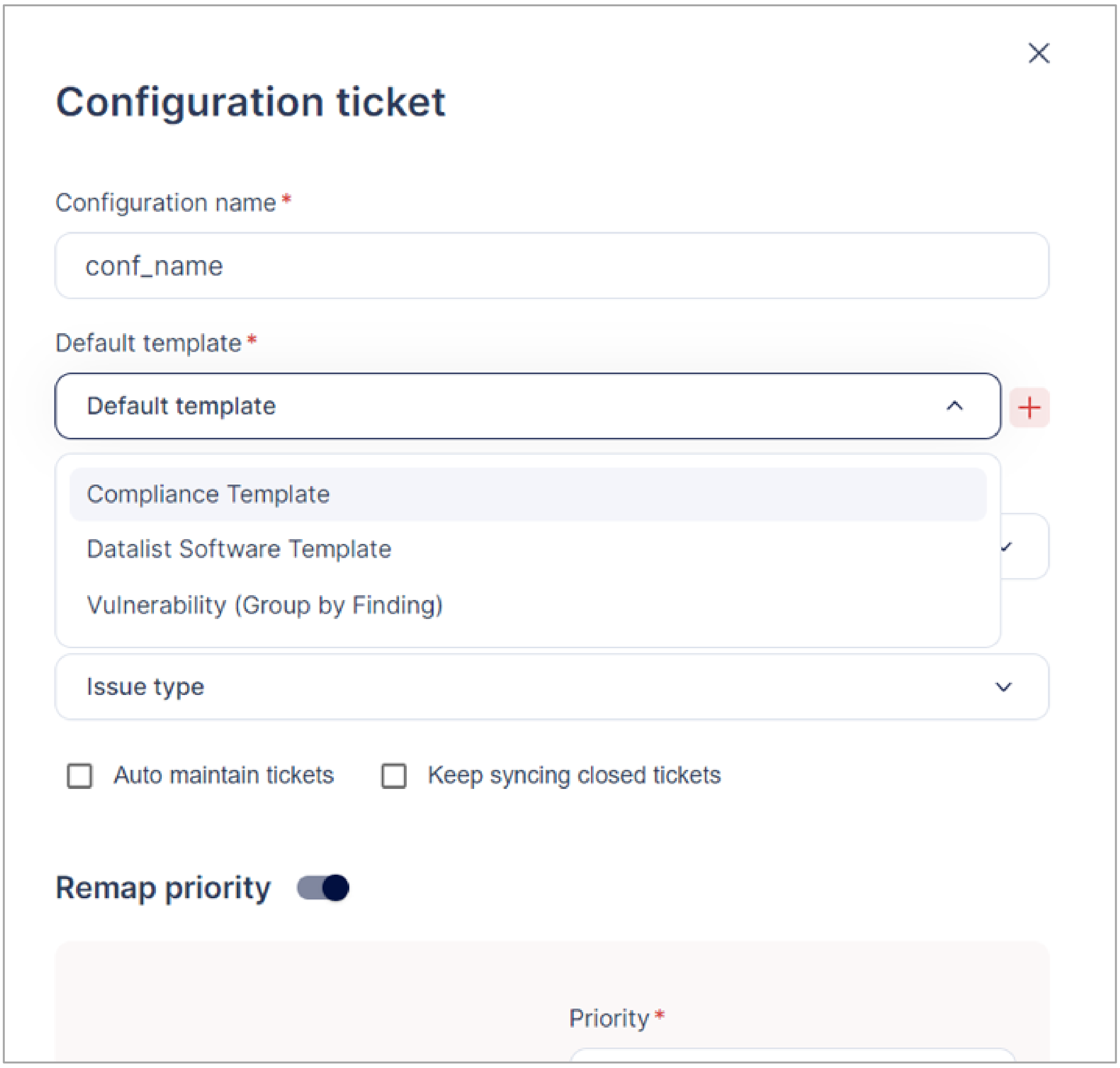
☐ Is Jira admin

Ticket Configuration

priya-config
Project: JIRAINTEGRATIONTEST
Issue type: Bug

guru-inpriyaintegration
Project: JIRAINTEGRATIONTEST
Issue type: Bug

- Enter a name for the configuration and select a 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 *

conf_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 *

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

Integrate Registries

Registry

- AccuKnox CSPM tool provides 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]

a. *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.

b. *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.

c. *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.

d. *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.

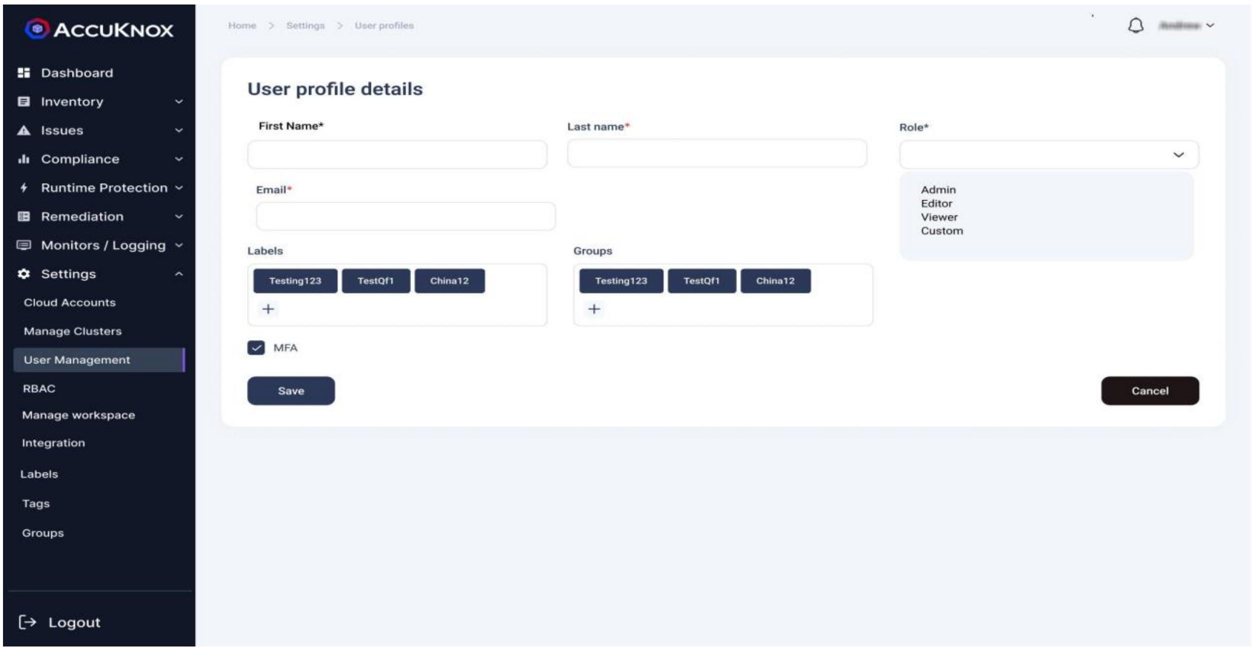
Permission is given to users by assigning roles while creating a user profile. These roles are created in the RBAC section. Deactivated users can be viewed under the Deactivated Users subsection.

Creating a user sends an invite to their email id, invites that are not yet accepted are present inside the Pending Invites subsection.

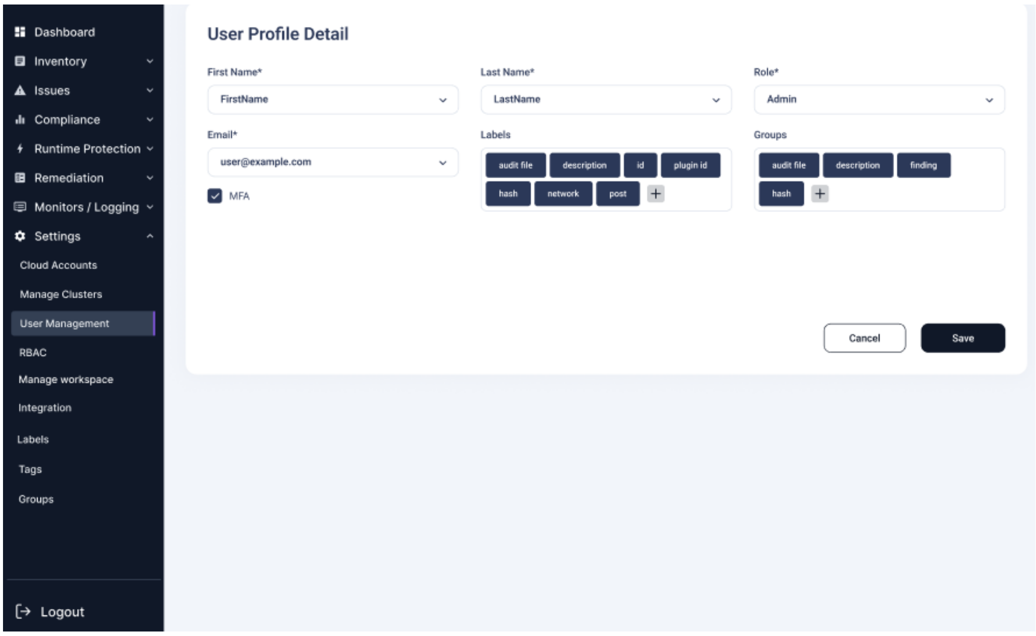
Invite folks to the workspace

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.



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



User Profile Detail

First Name*: FirstName

Last Name*: LastName

Role*: Admin

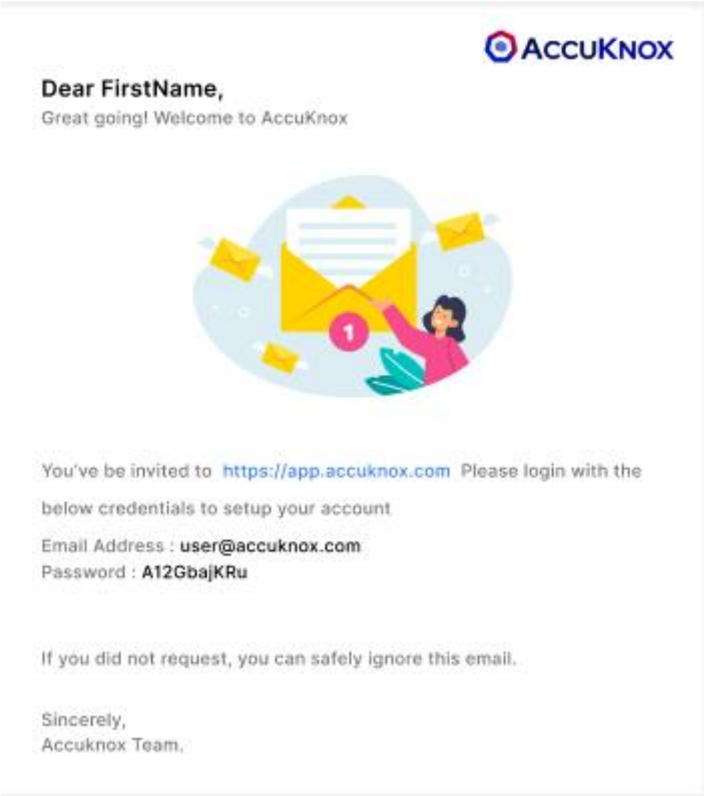
Email*: user@example.com

☑ MFA

Labels: audit file, description, id, plugin id, hash, network, post +

Groups: audit file, description, finding, hash +

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



Dear FirstName,

Great going! Welcome to AccuKnox

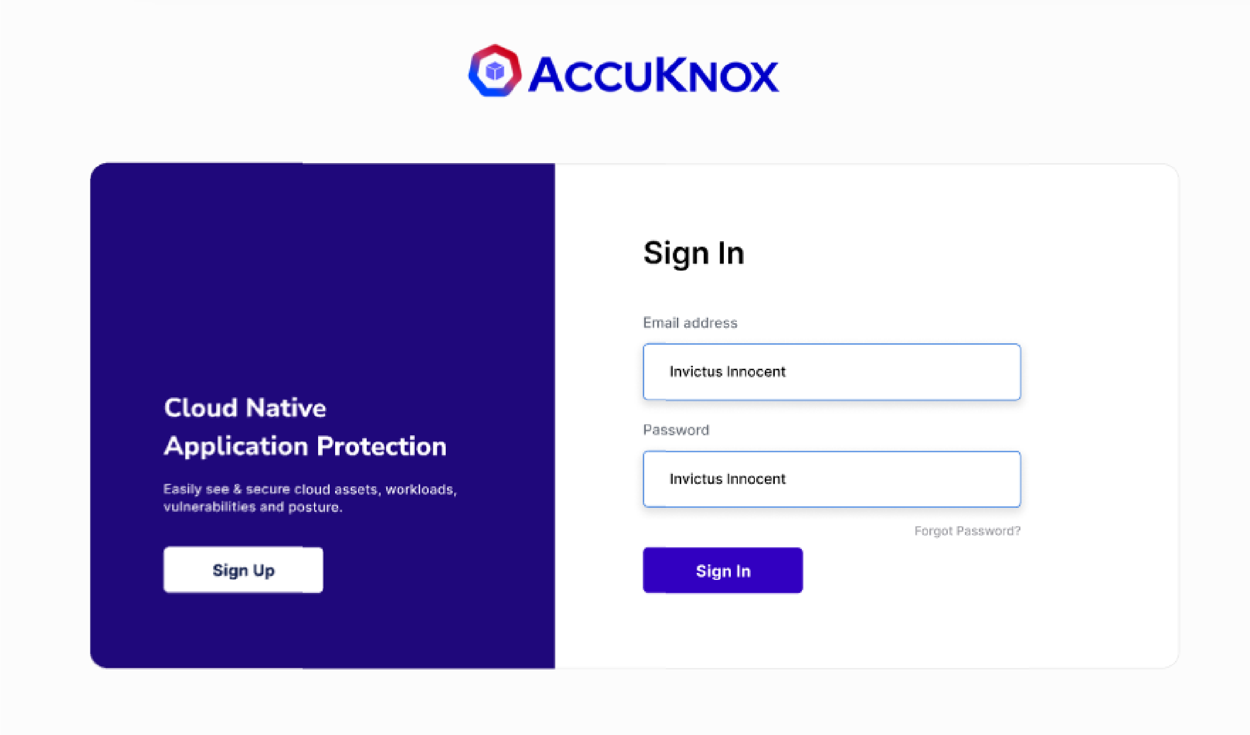
You've be invited to https://app.accuknox.com Please login with the below credentials to setup your account

Email Address : user@accuknox.com
Password : A12GbajKRu

If you did not request, you can safely ignore this email.

Sincerely,
Accuknox Team.

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



ACCUKNOX

Cloud Native
Application Protection

Easily see & secure cloud assets, workloads, vulnerabilities and posture.

Sign Up

Sign In

Email address

Invictus Innocent

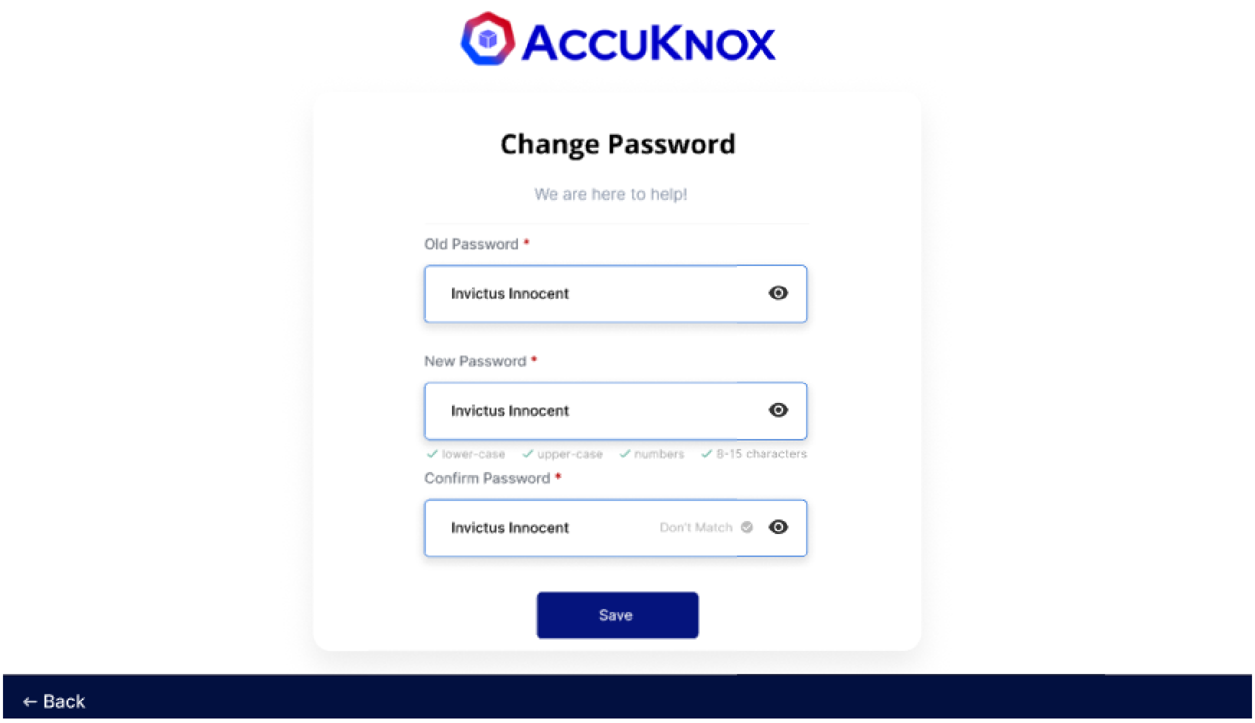
Password

Invictus Innocent

Forgot Password?

Sign In

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



ACCUKNOX

Change Password

We are here to help!

Old Password *

Invictus Innocent

New Password *

Invictus Innocent

✓ lower-case ✓ upper-case ✓ numbers ✓ 8-15 characters

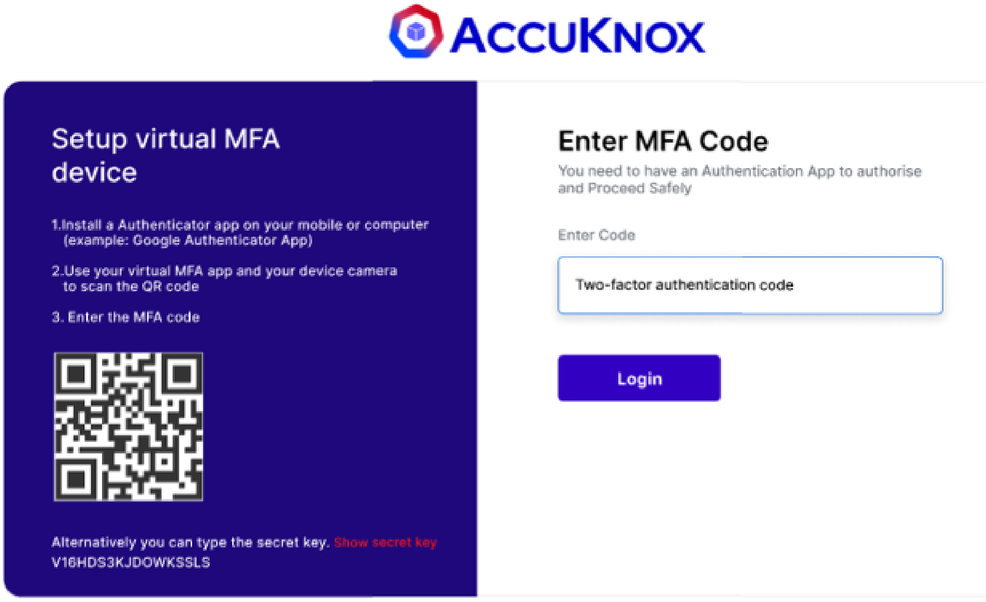
Confirm Password *

Invictus Innocent Don't Match

Save

← Back

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



Setup virtual MFA device

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

3. Enter the MFA code

Alternatively you can type the secret key. Show secret key
V16HDS3KJDOWKSSLS

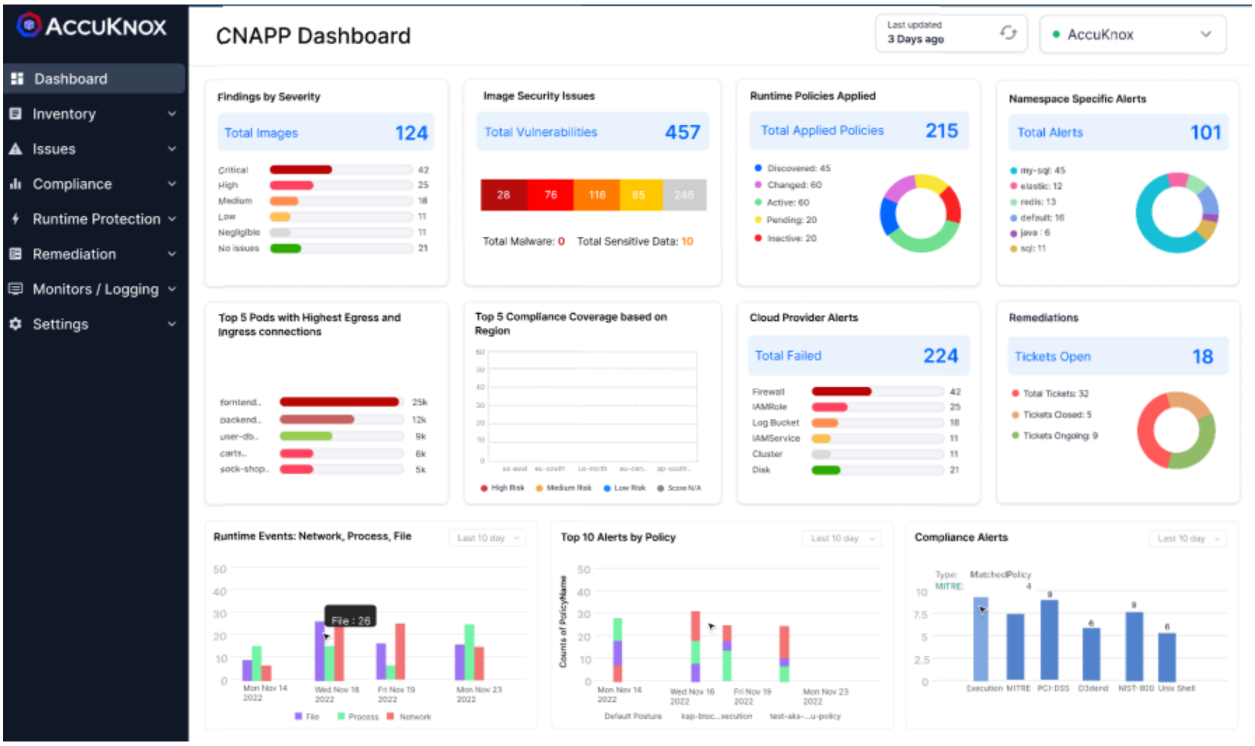
Enter MFA Code

You need to have an Authentication App to authorise and Proceed Safely

Enter Code

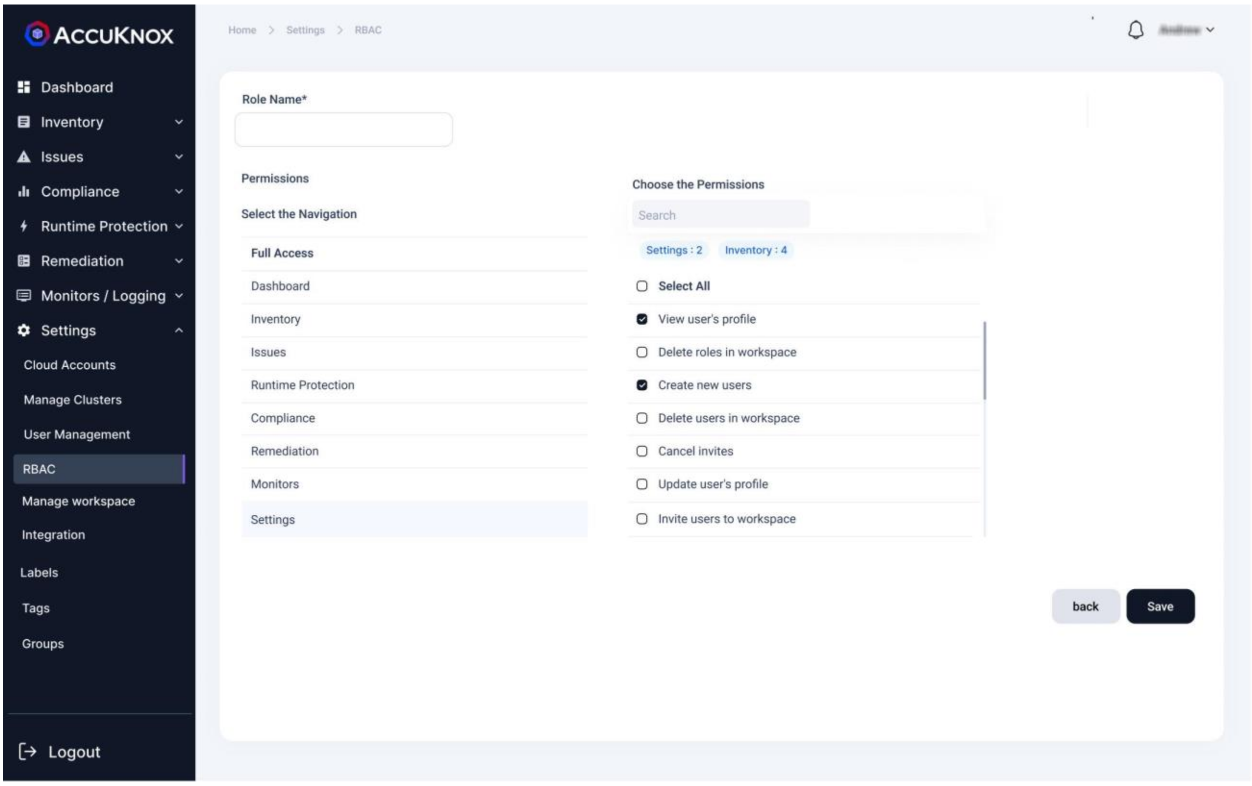
Two-factor authentication code

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

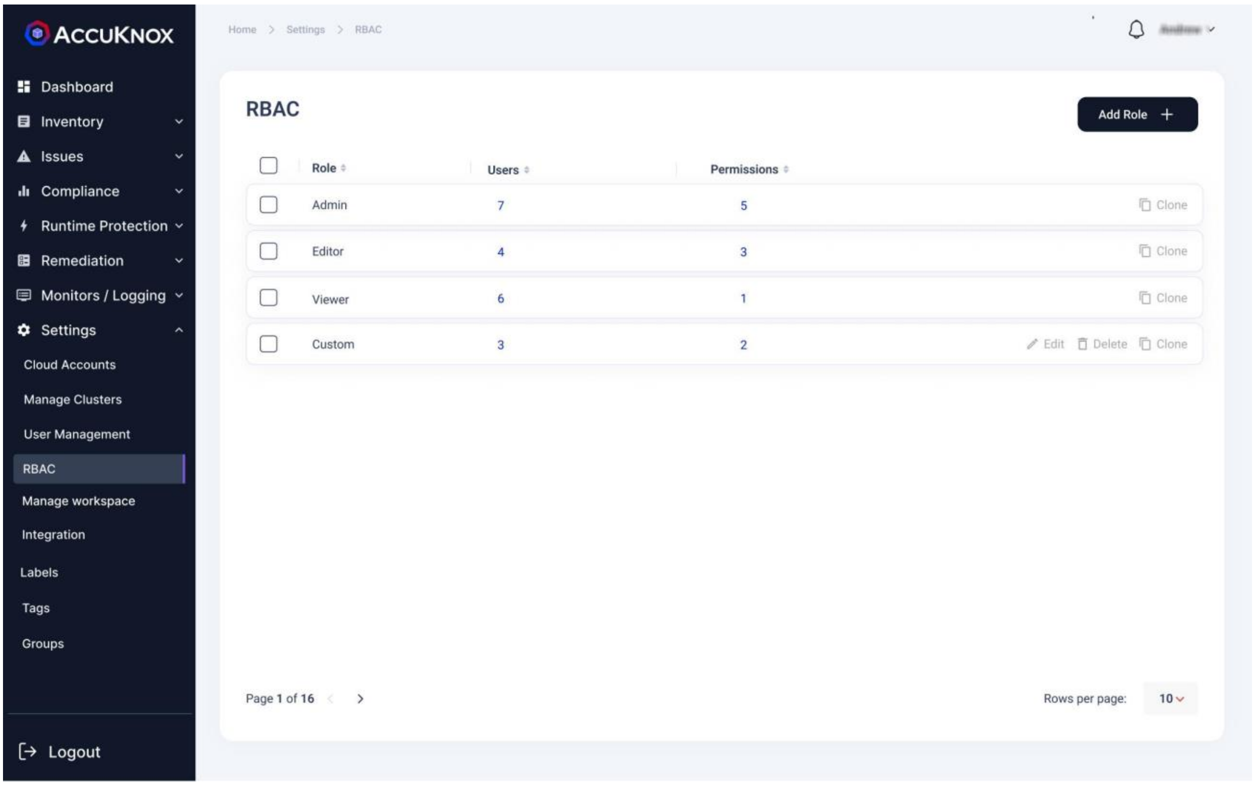
Full Access
Dashboard
Inventory
Issues
Runtime Protection
Compliance
Remediation
Monitors
Settings

Choose the Permissions

Search

Settings : 2 Inventory : 4

□ Select All
☑ View user's profile
□ Delete roles in workspace
☑ Create new users
□ Delete users in workspace
□ Cancel invites
□ Update user's profile
□ Invite users to workspace



RBAC

□	Role	Users	Permissions	
□	Admin	7	5	Clone
□	Editor	4	3	Clone
□	Viewer	6	1	Clone
□	Custom	3	2	Edit Delete Clone

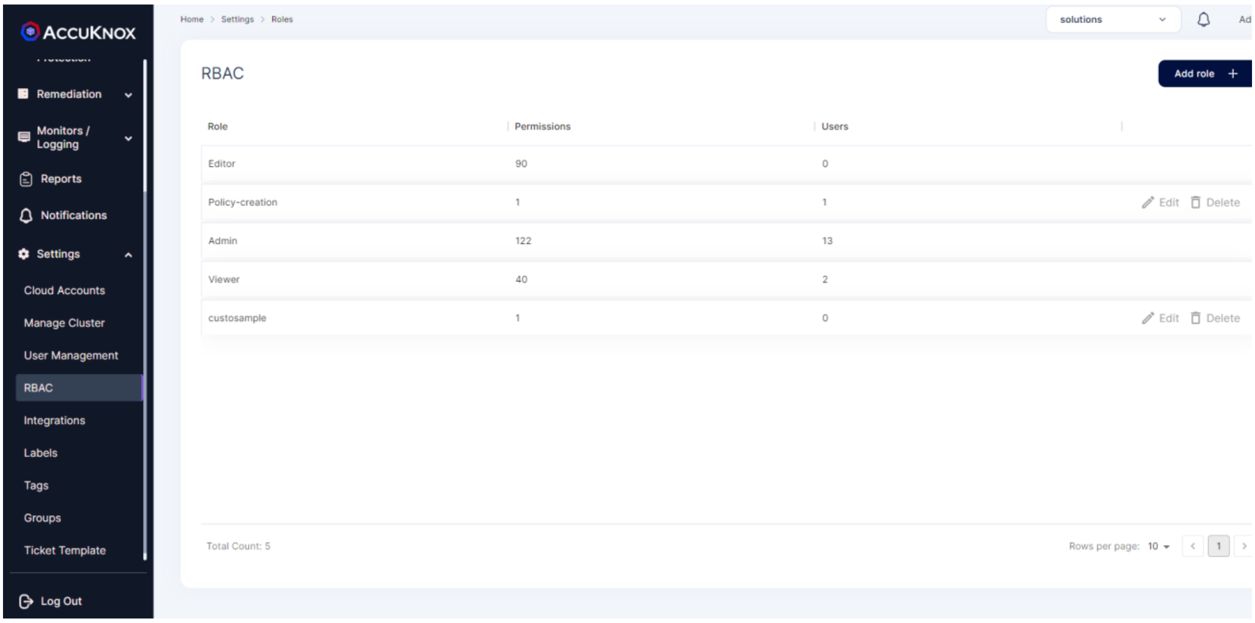
Page 1 of 16

Rows per page: 10

Create Roles and Assign Users

Steps:

- Click on Add Role



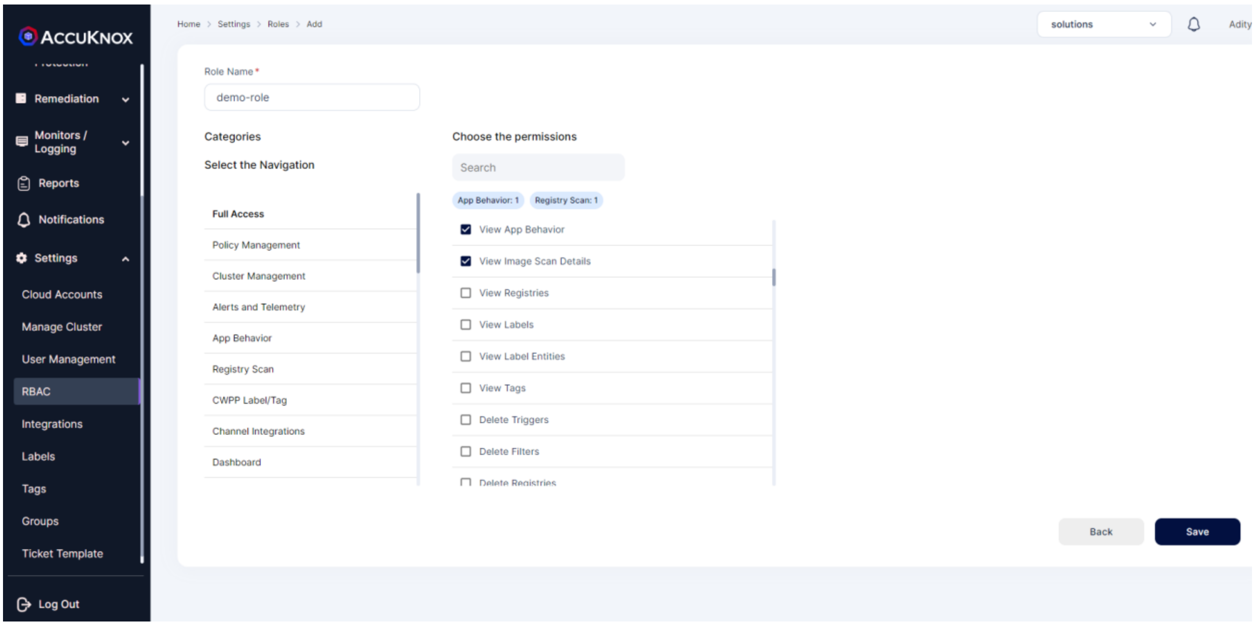
RBAC

Role	Permissions	Users	
Editor	90	0	
Policy-creation	1	1	Edit Delete
Admin	122	13	
Viewer	40	2	
custosample	1	0	Edit Delete

Total Count: 5

Rows per page: 10

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



Role Name *
demo-role

Categories

Select the Navigation

- Full Access
- Policy Management
- Cluster Management
- Alerts and Telemetry
- App Behavior
- Registry Scan
- CWPP Label/Tag
- Channel Integrations
- Dashboard

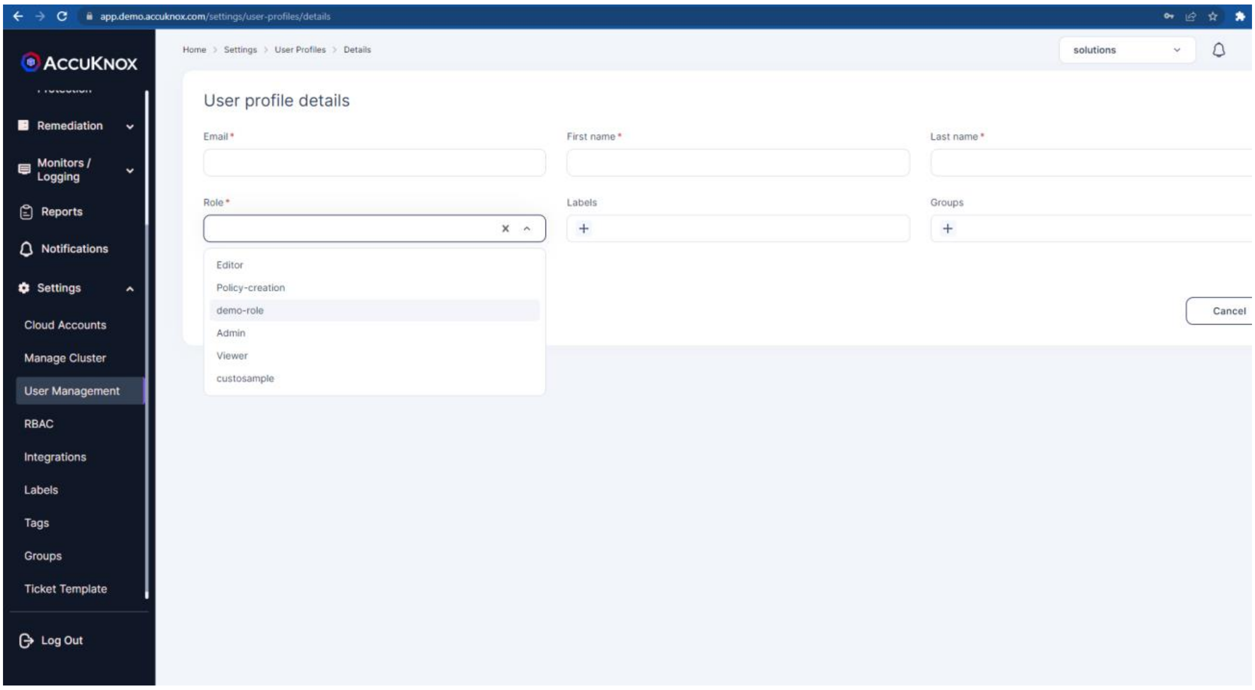
Choose the permissions

Search

App Behavior: 1 Registry Scan: 1

☑ View App Behavior
☑ View Image Scan Details
☐ View Registries
☐ View Labels
☐ View Label Entities
☐ View Tags
☐ Delete Triggers
☐ Delete Filters
☐ Delete Registries

- 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



User profile details

Email *

First name *

Last name *

Role *

- Editor
- Policy-creation
- demo-role
- Admin
- Viewer
- custosample

Labels

Groups