-=AccuKnox Manual=-

Getting Started Guide

- CSPM Prerequisites

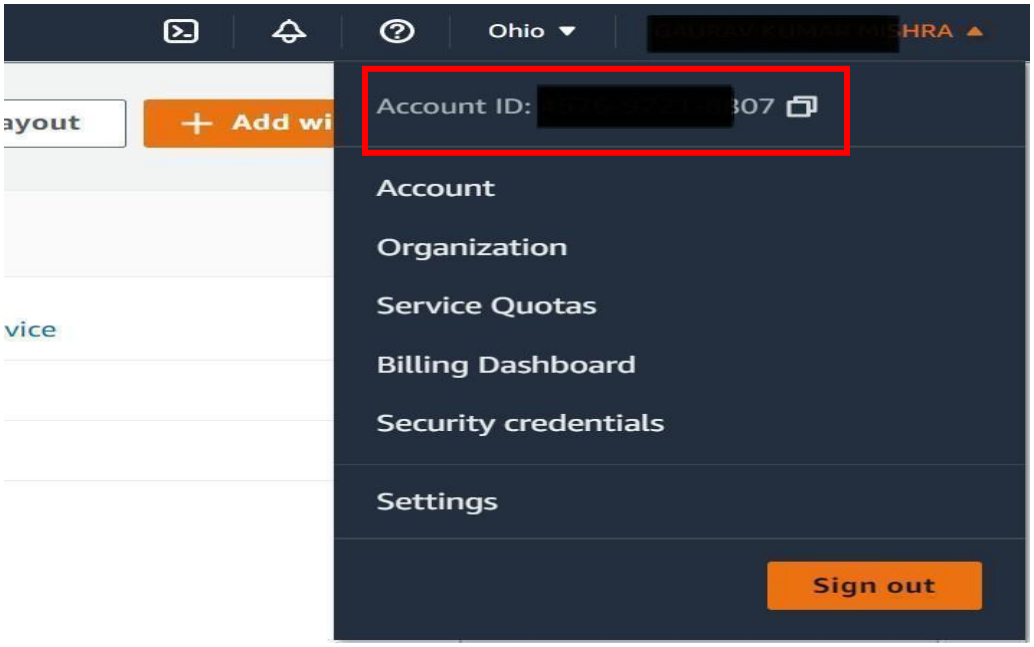
Cloud Account Onboarding

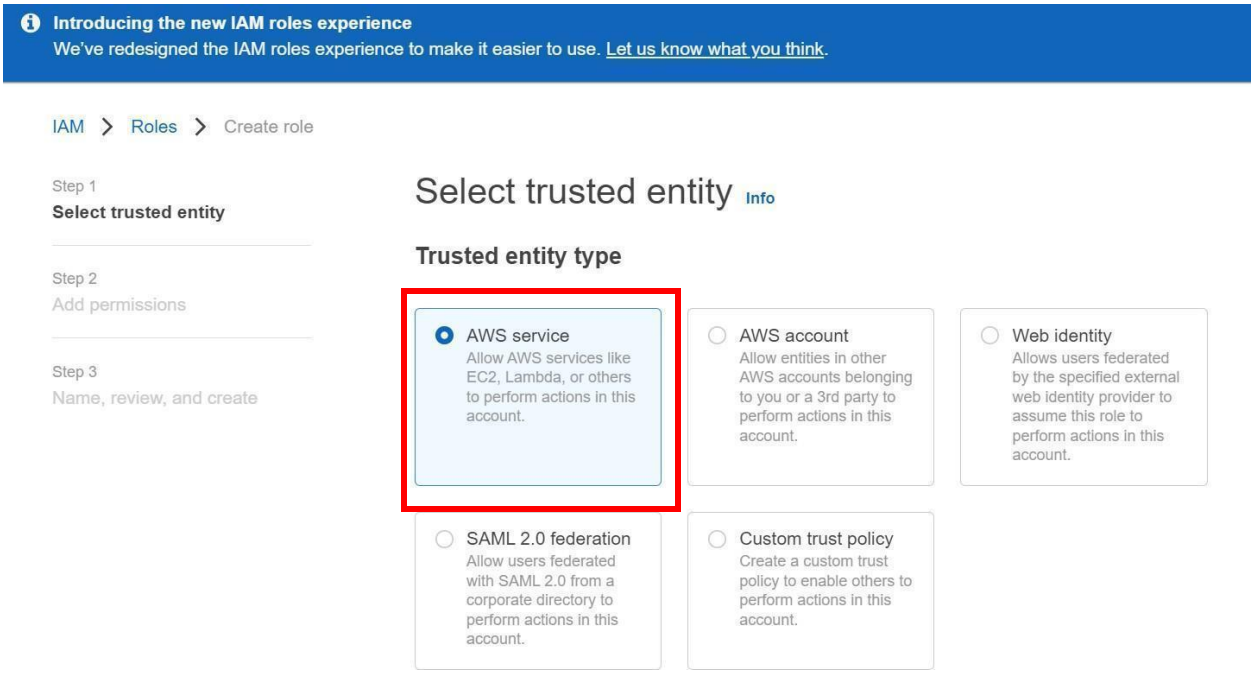
- AWS

1. <u>Manual Setup</u>

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

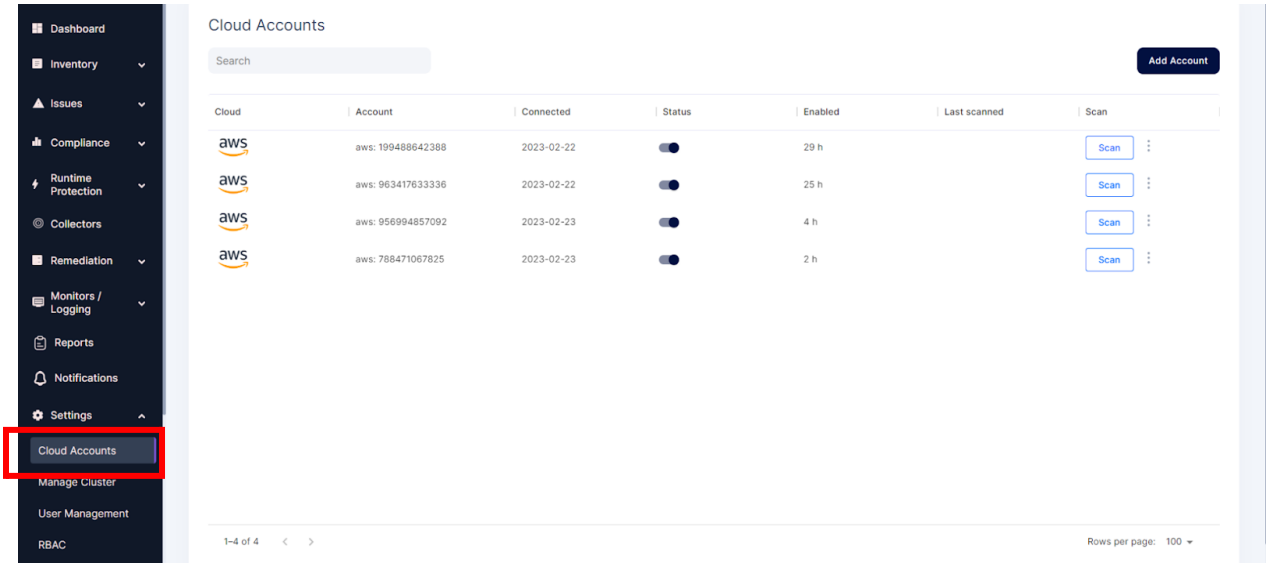
Create a new IAM role & select “trusted entity type” as “AWS service”



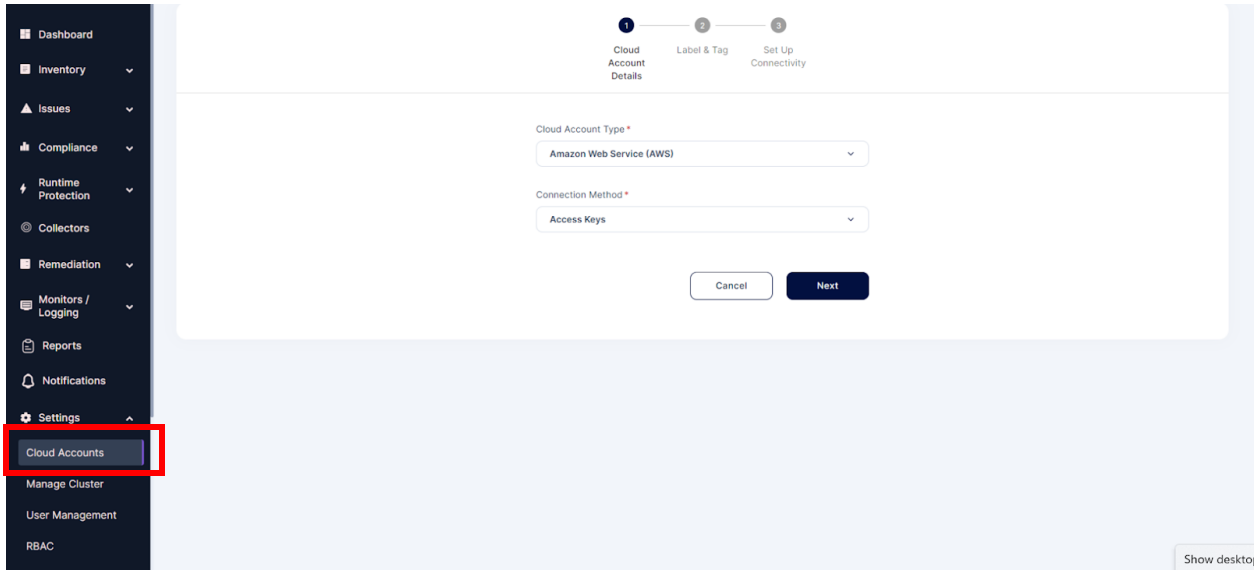


2. From AccuKnox SaaS UI (Access Ley Metod)

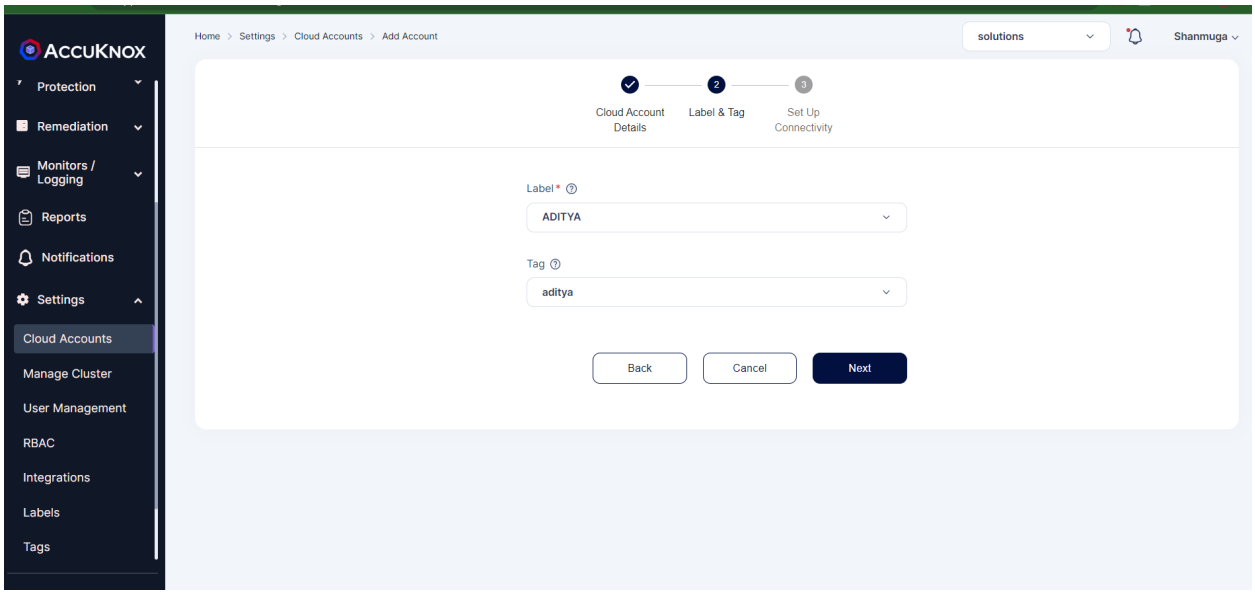
- Click settings -> Cloud Accounts
- Click Add account



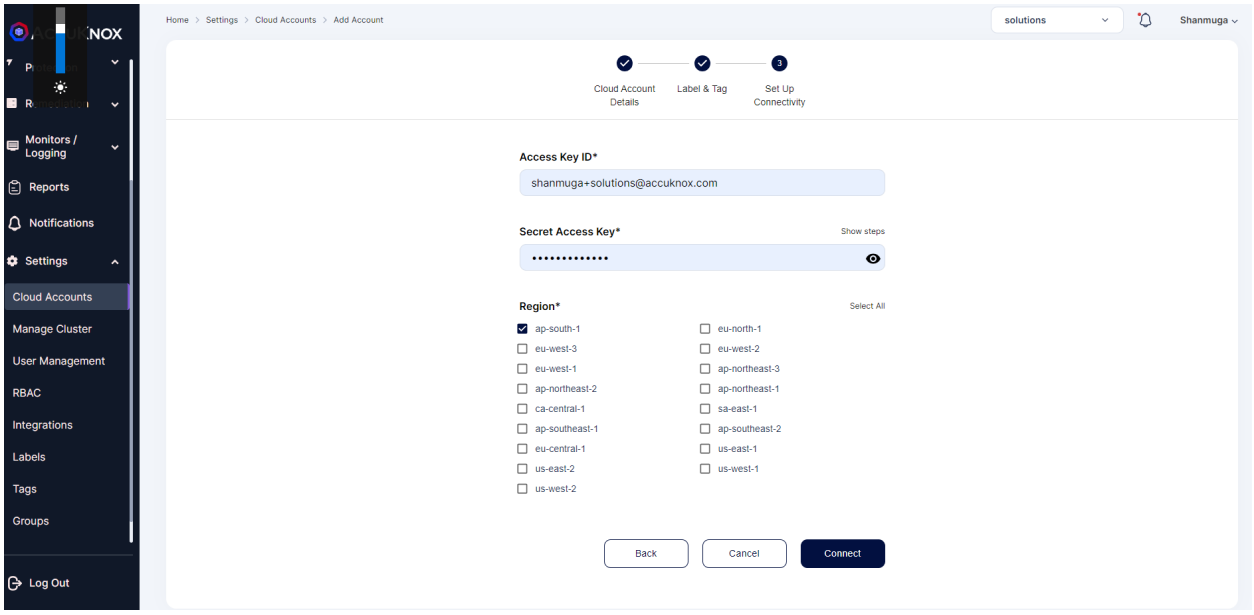
- Select the Cloud Account type to AWS
- Select the Connection method to Access key



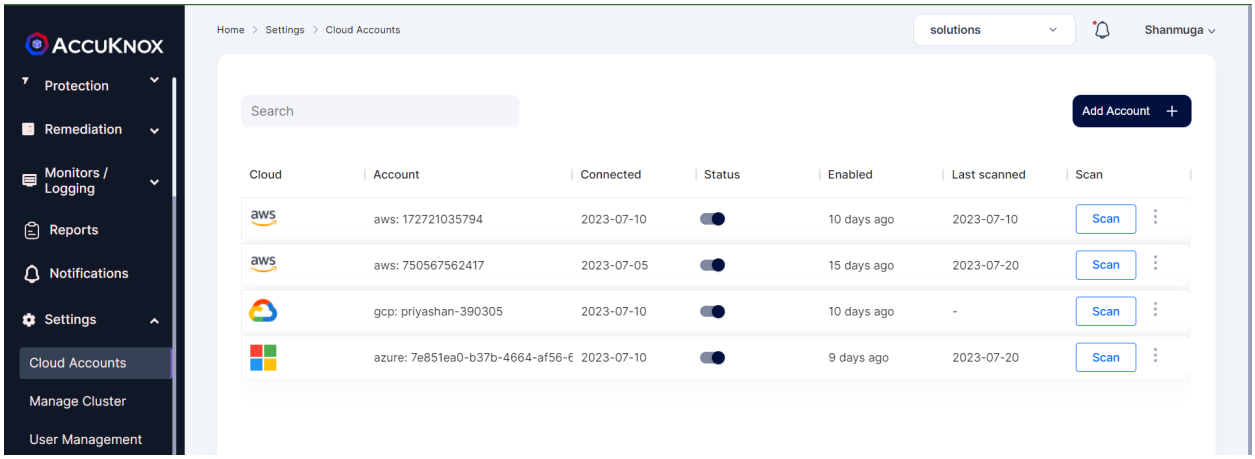
- Select the Labels and Tags
  Note: If there are no labels and tags create new labels and tags via the settings



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



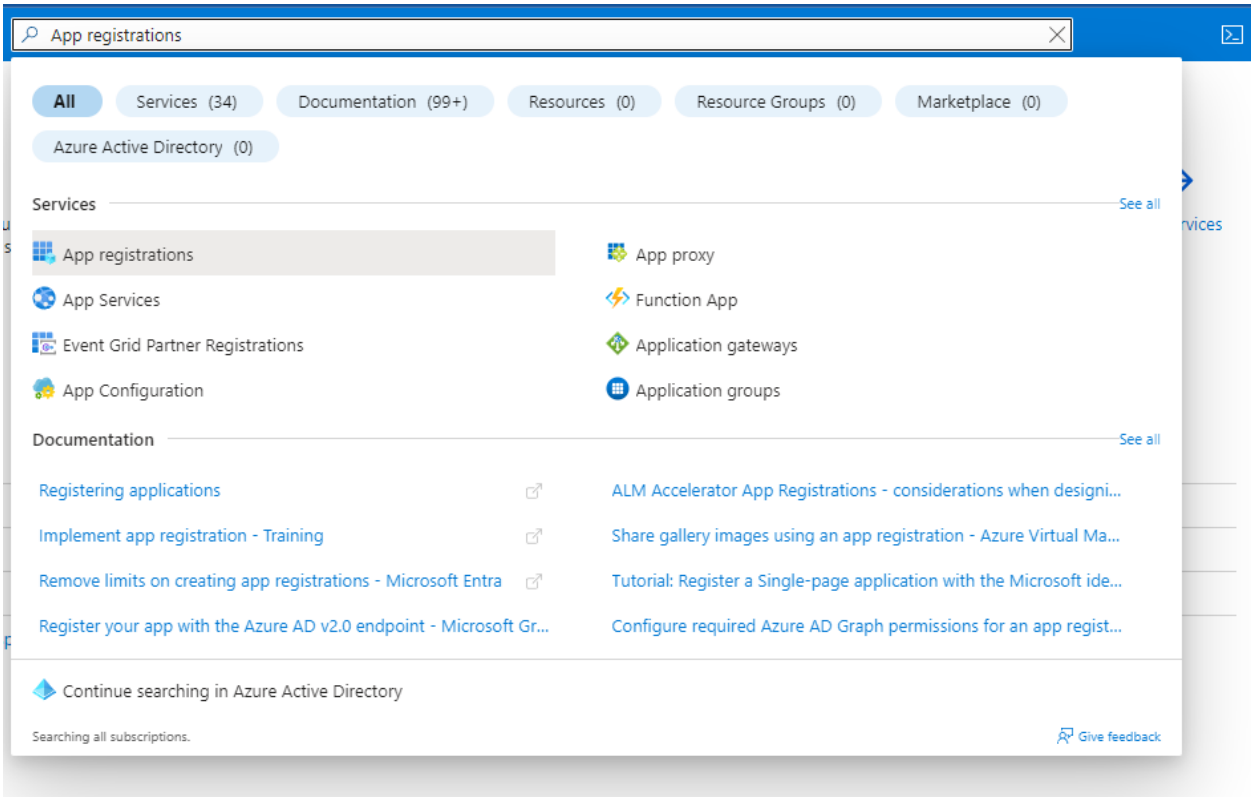
- Select the regions and click connect
  Note: Only the regions that have been specified will have resources scanned.
- Check Settings → Cloud Accounts. You will see your cloud account is added successfully.



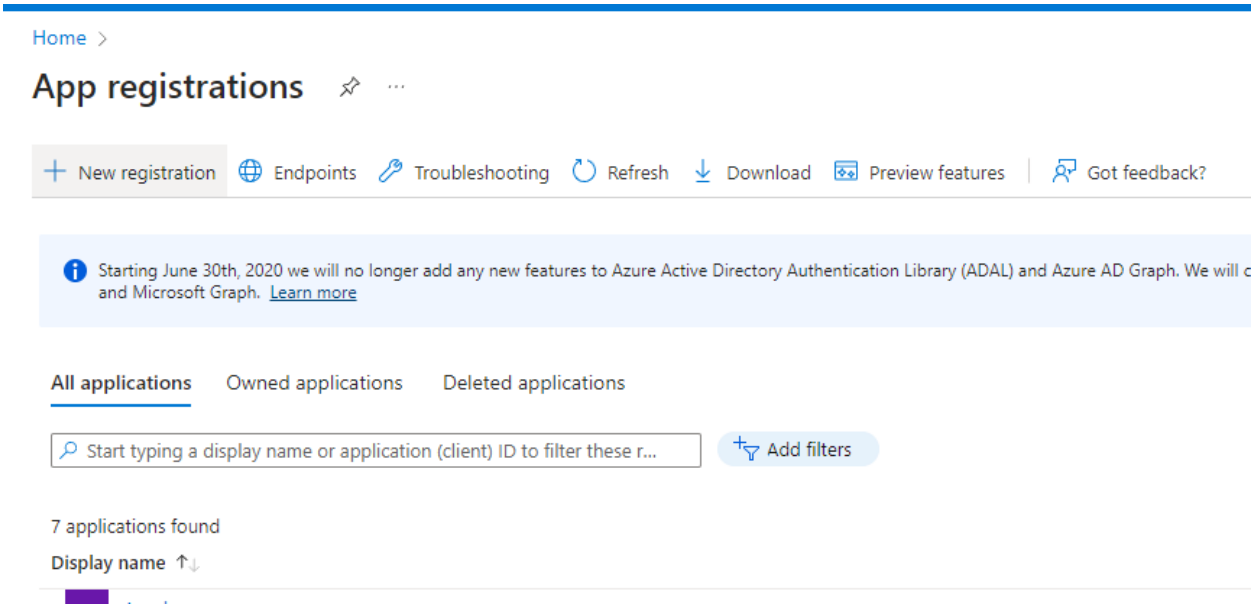
- AZURE

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

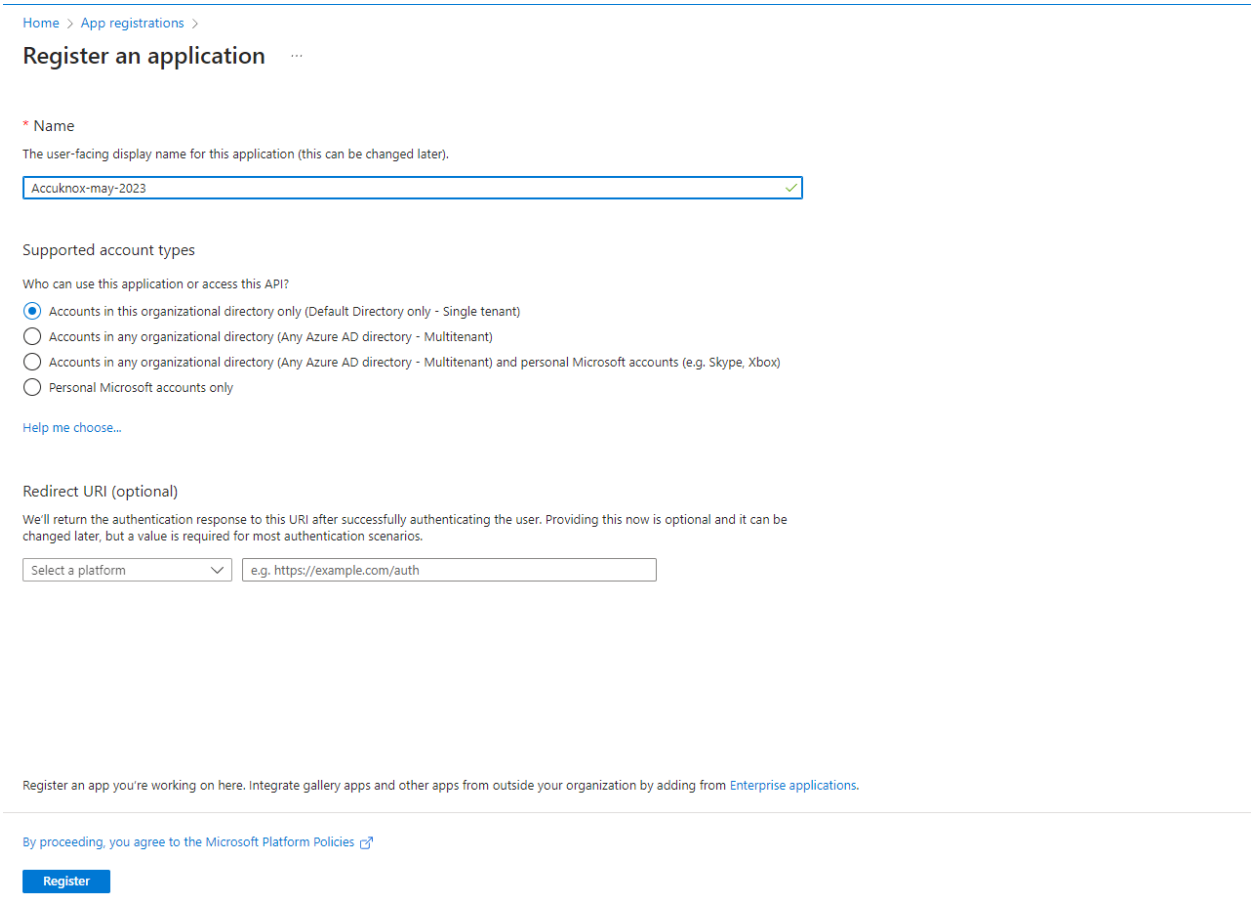
- Go to your Azure Portal and search for App registrations and open it



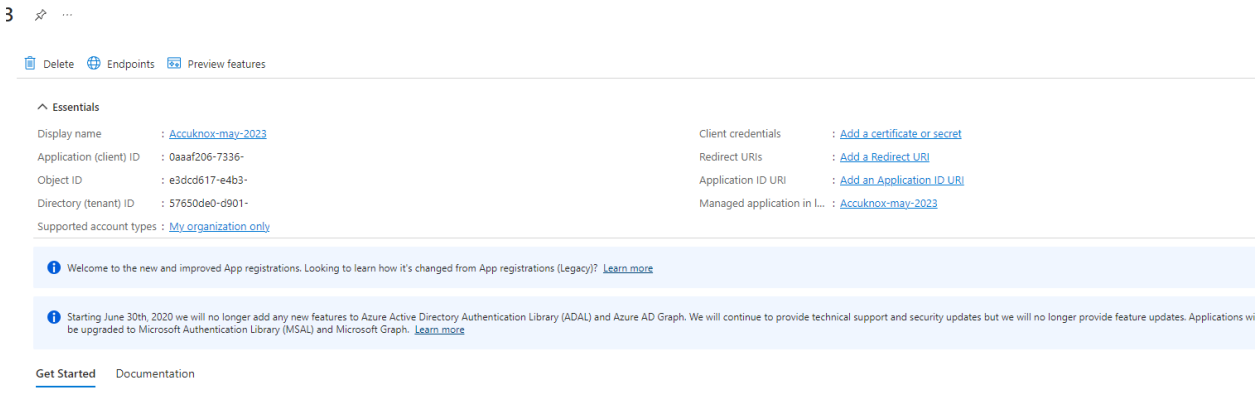
- Here click on New registration



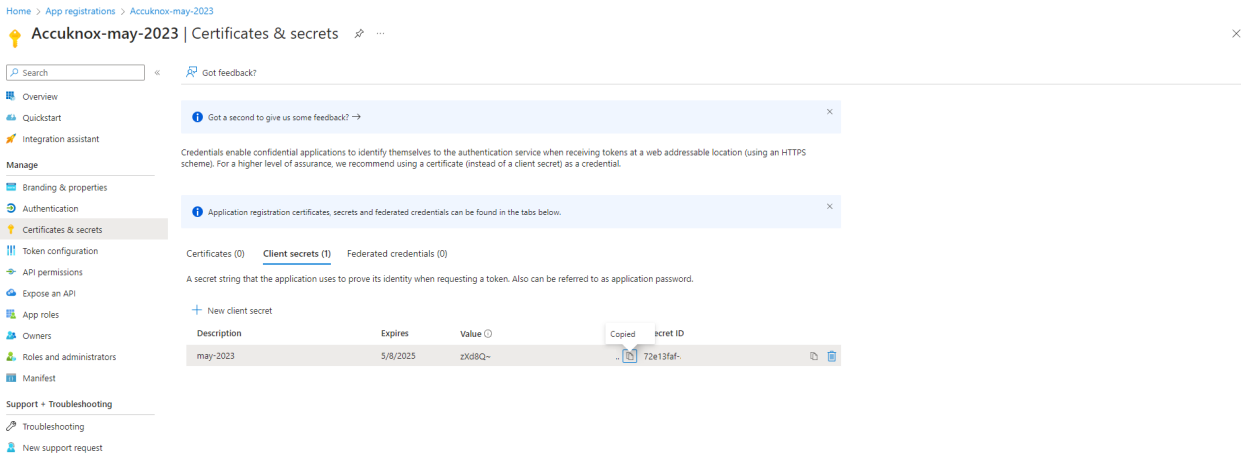
- Give your application a name, remember this name as it will be used again later, For the rest keep the default settings



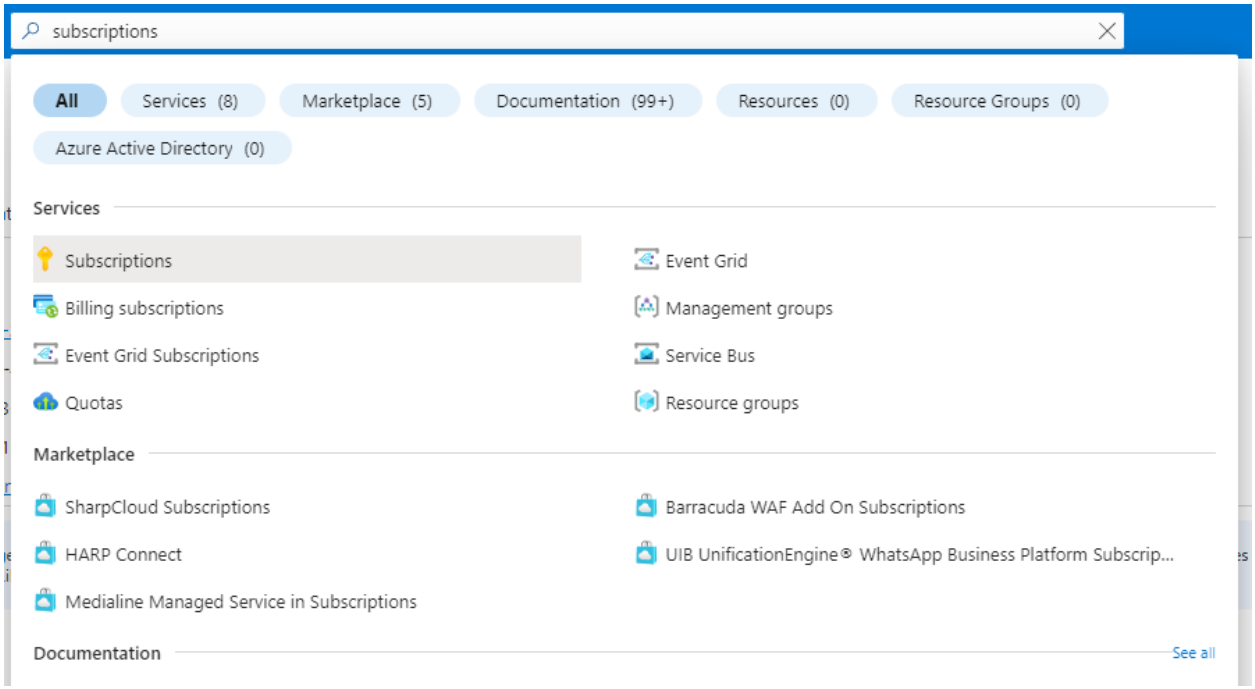
- Now your application is created, save Application ID and Directory ID as they will be needed to for onboarding on Accuknox Saas and then click on ‘Add a certificate or secret’



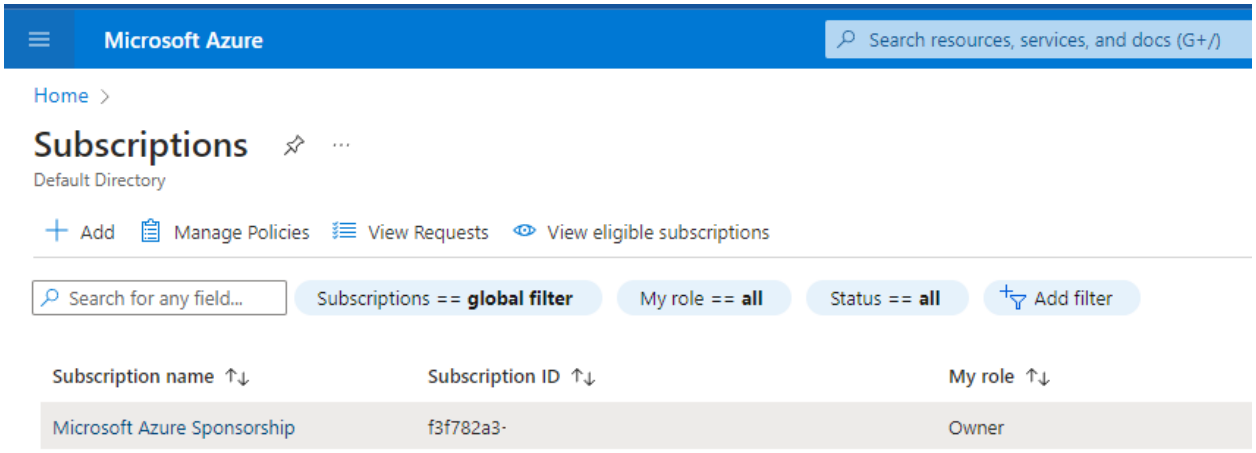
- Click on new client secret and enter the name and expiration date to get secret id and secret value, save this secret value as this will also be needed for onboarding.



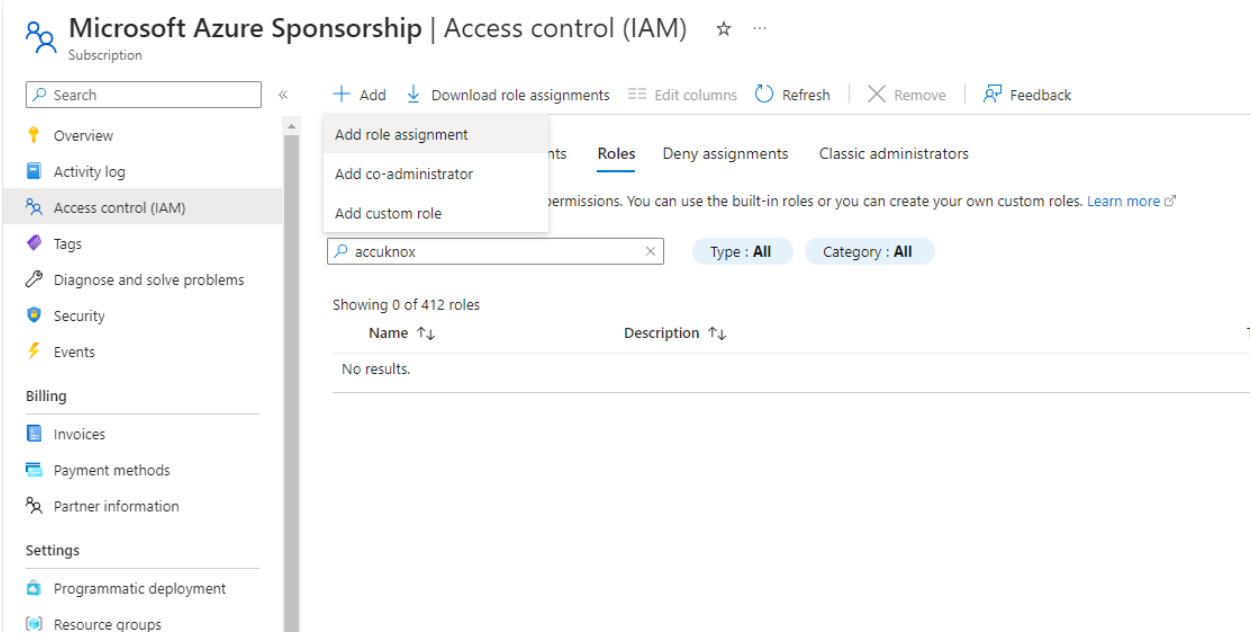
- Now we need to give Security read permissions to this registered Application , to do that go to subscriptions



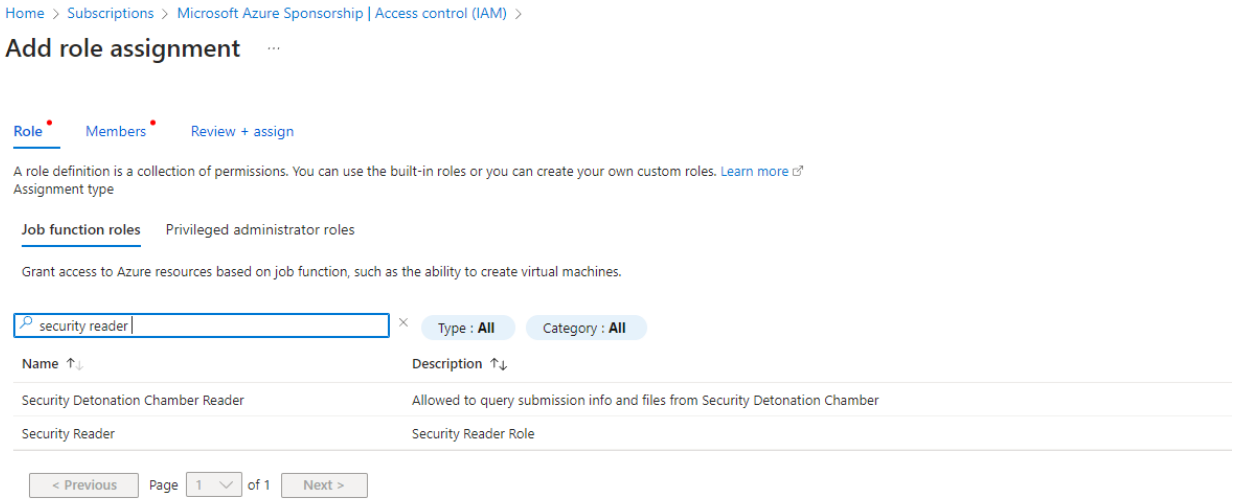
- First save the subscription ID and click on the subscription name , here it is “Microsoft Azure Sponsorship“



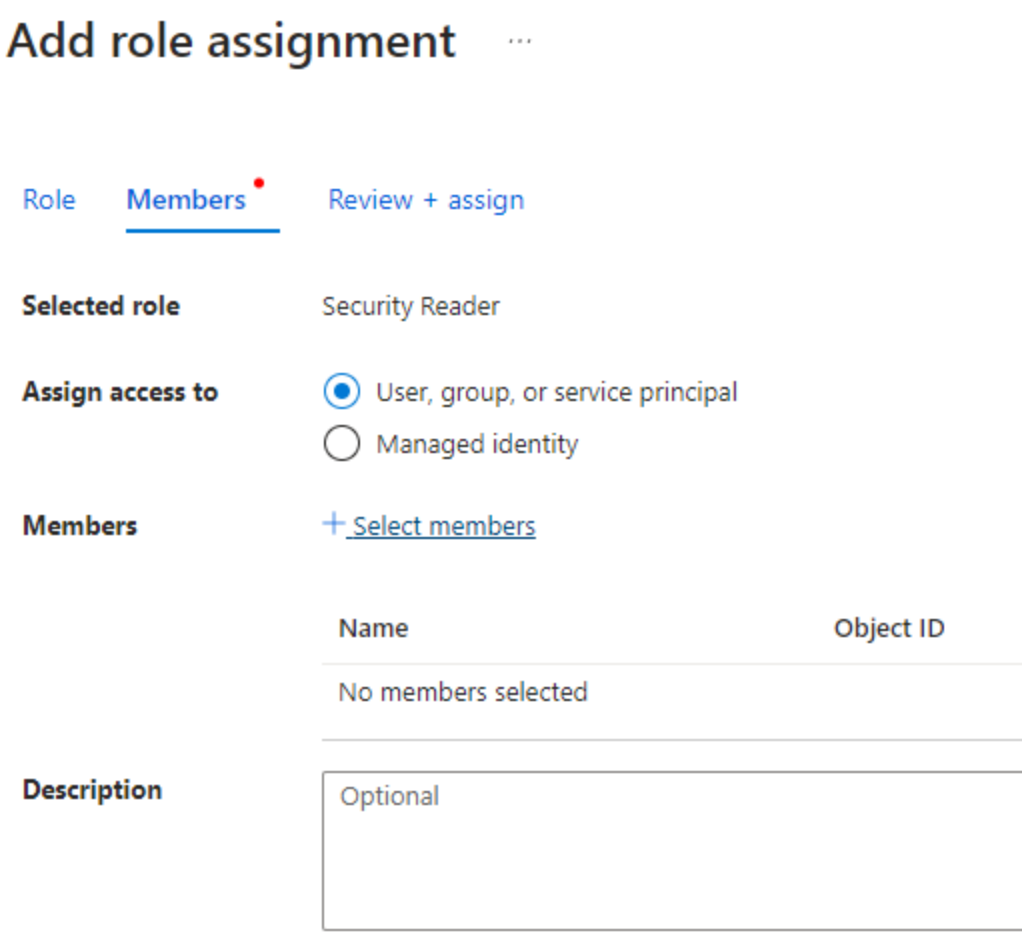
- Navigate to Access control(IAM) and go to Roles , here select Add and Add role assignment



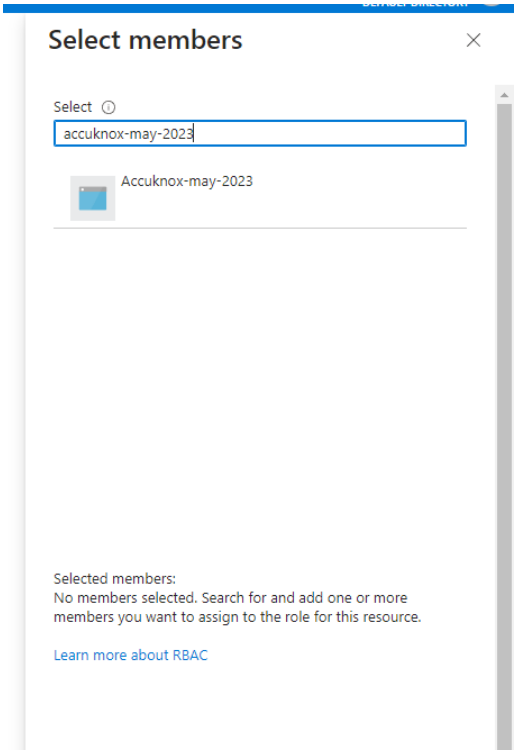
- Search for “Security Reader” Job function Role, select it and press next



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



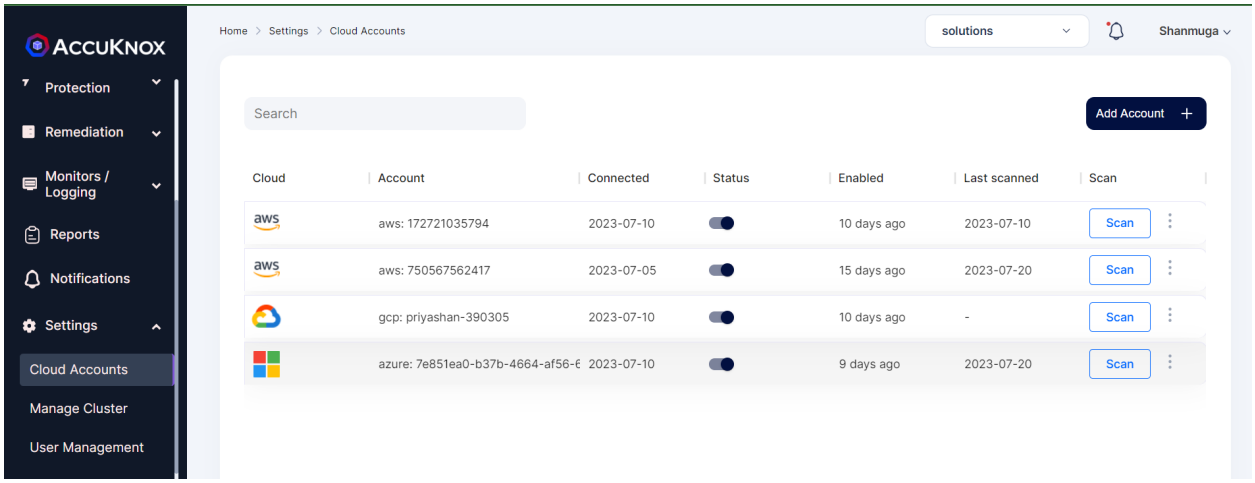
- Here search for the Application that you registered in the beginning , select the application and click on review and assign.



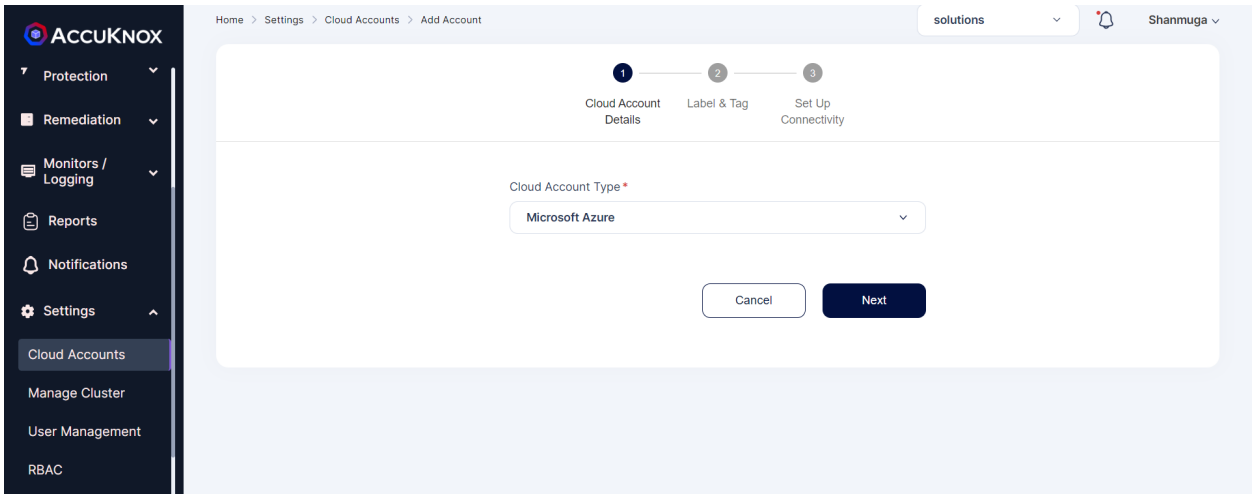
From AccuKnox SaaS UI

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

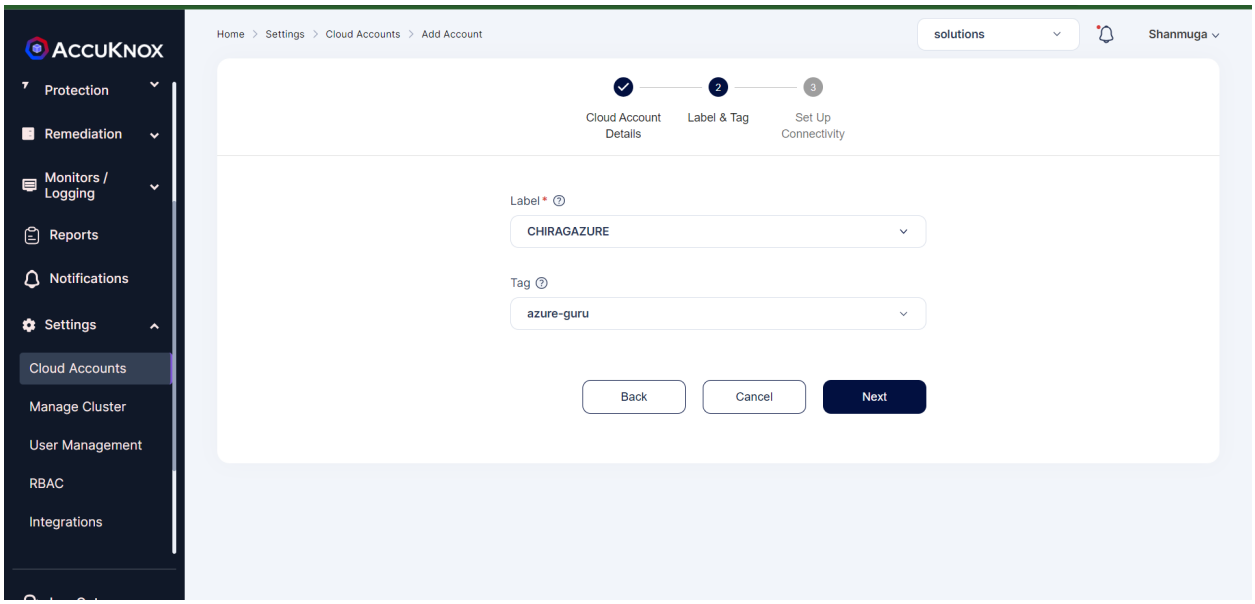
- Go to settings-> Cloud Account and click on Add Account



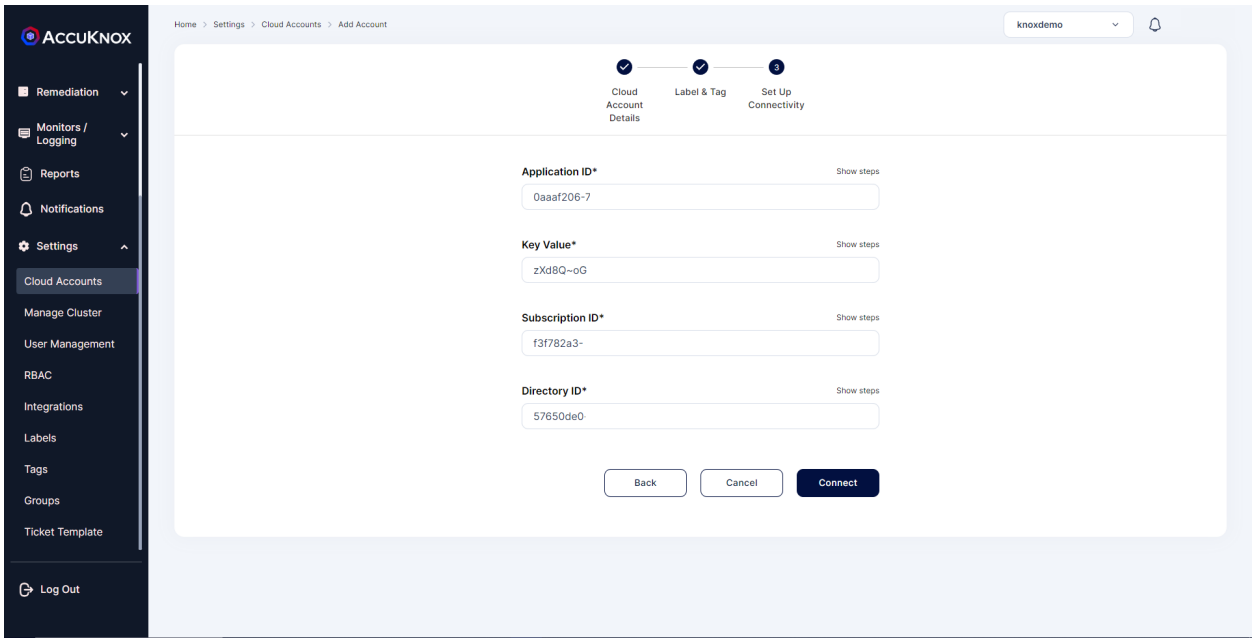
- Select Microsoft Azure as Cloud Account Type and click on next



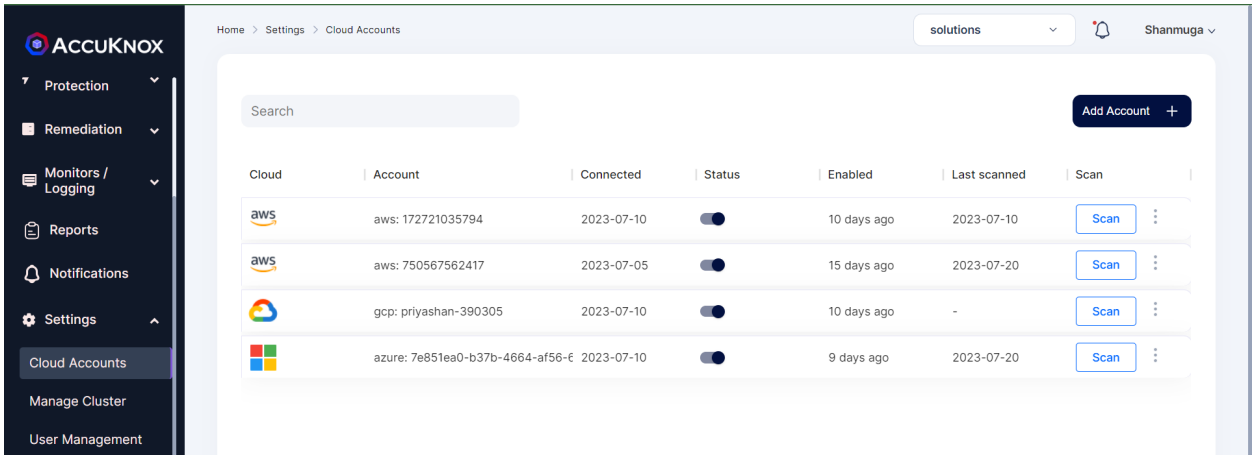
- Select or create label and Tags that will be associated with this Cloud Account



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

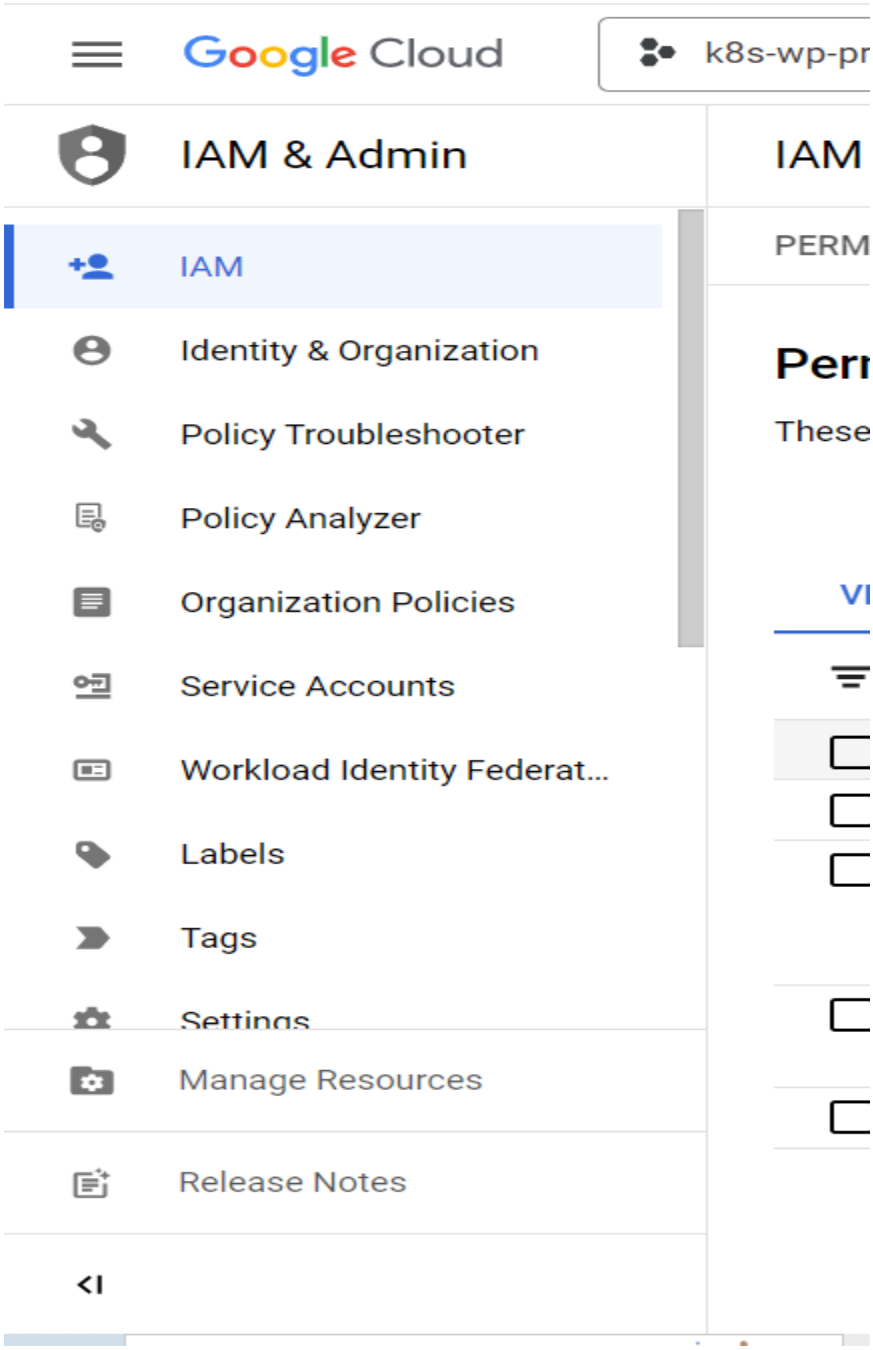


- After successfully connecting your cloud account will show up in the list

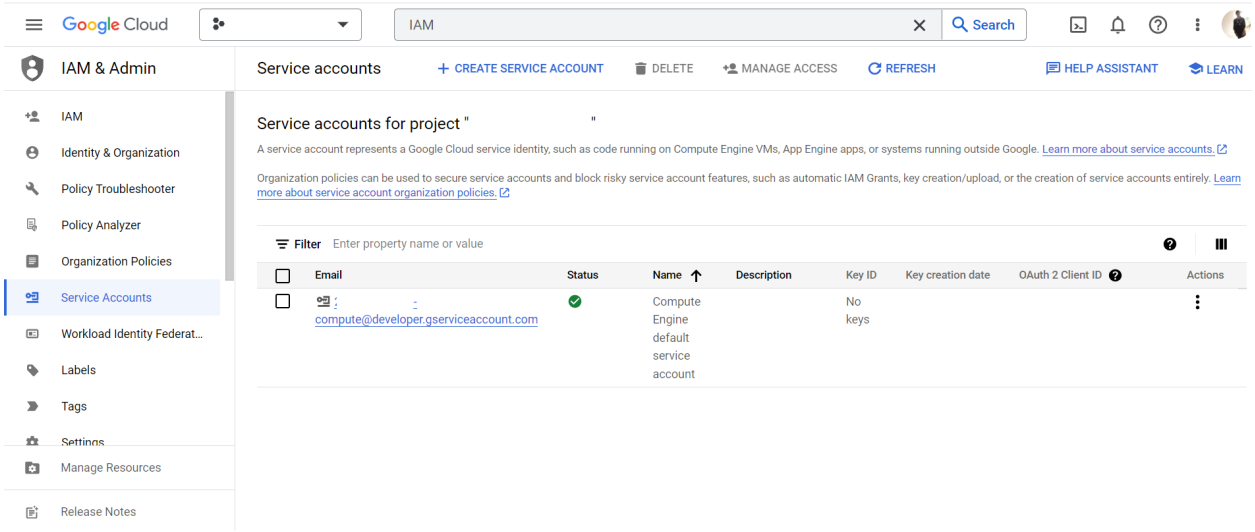


- GCP

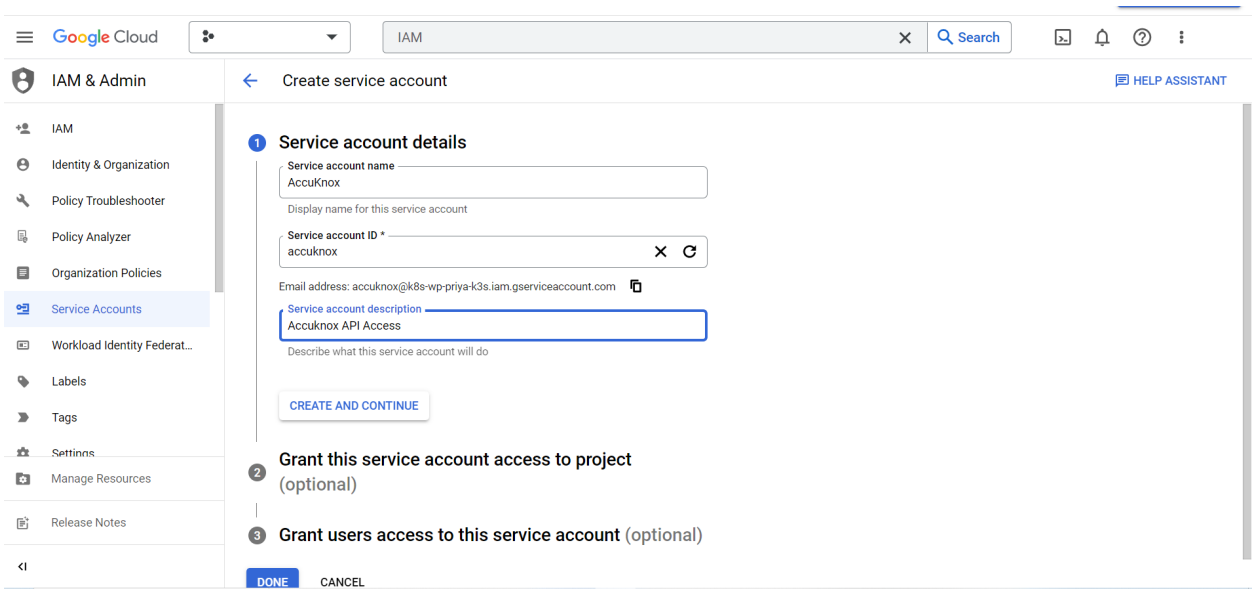
For GCP there is a requirement for IAM Service Account Access. + Log into your Google Cloud console and navigate to IAM Admin > Service Accounts



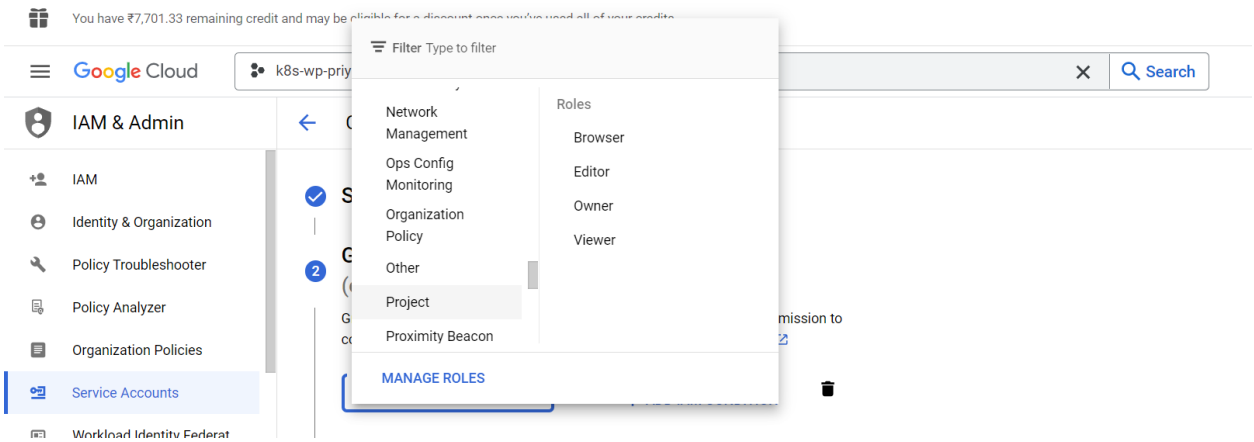
- Click on "Create Service Account".



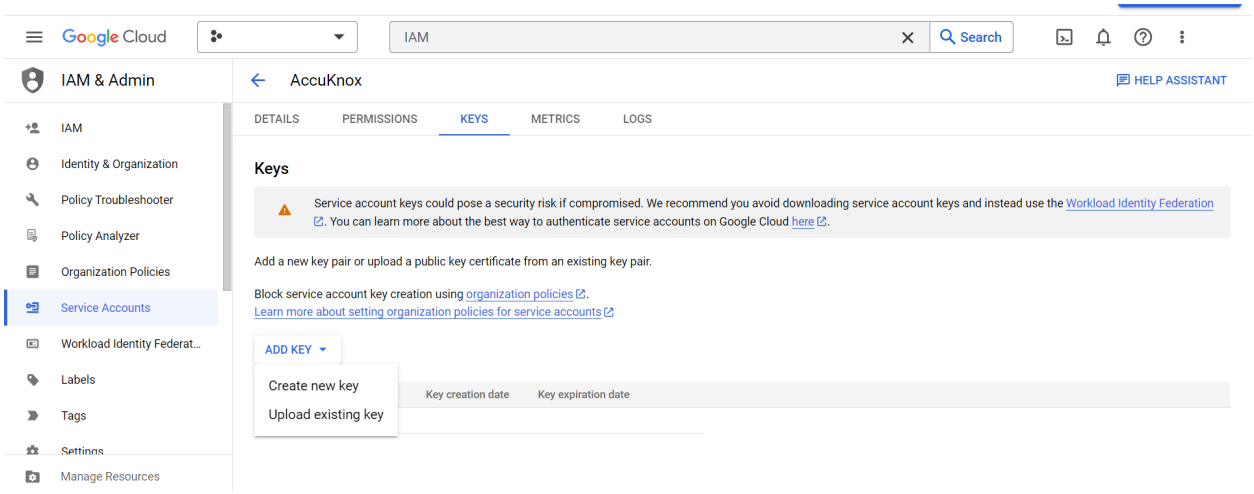
- Enter "AccuKnox" in the "Service account name", then enter "Accuknox API Access" in the description.
- Click on Continue.



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

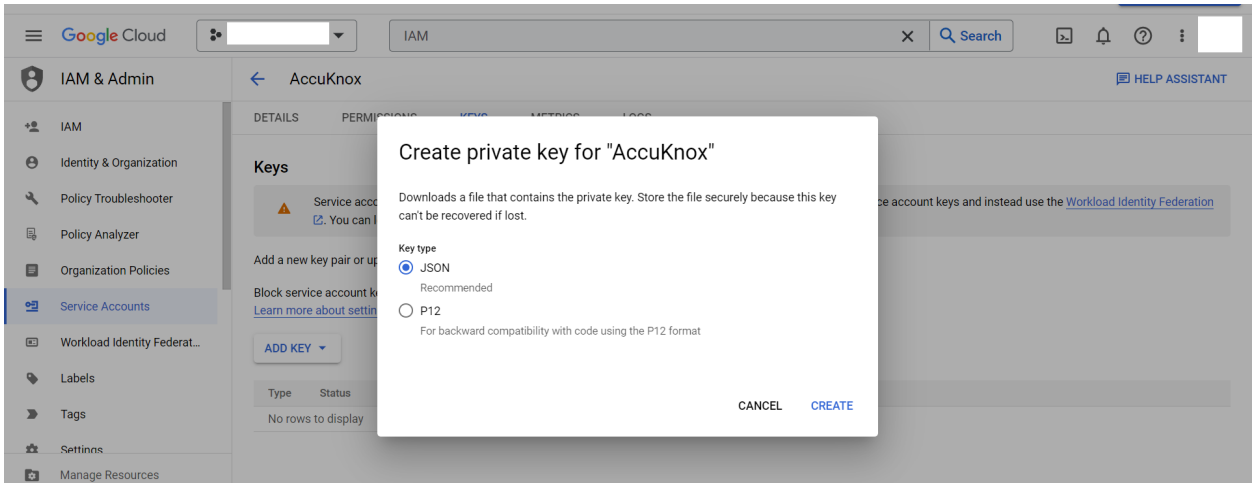


- Click on “Done”
- To create a “Key” click the created service account



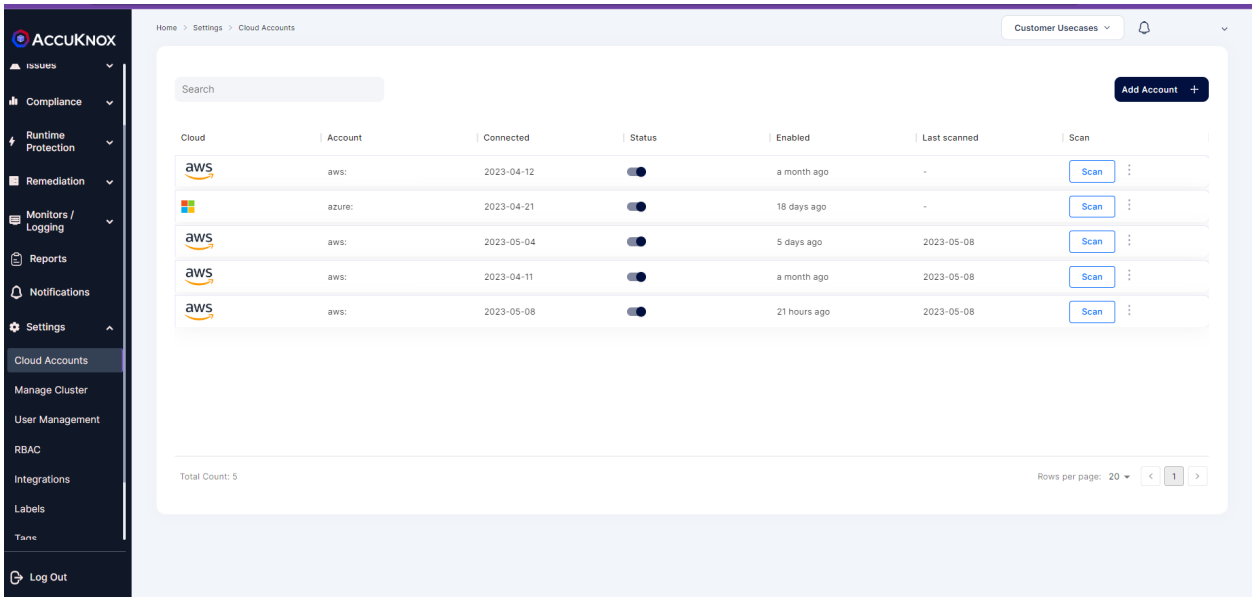
- Click Add Key and Create new key
- Check the JSON file and create.

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

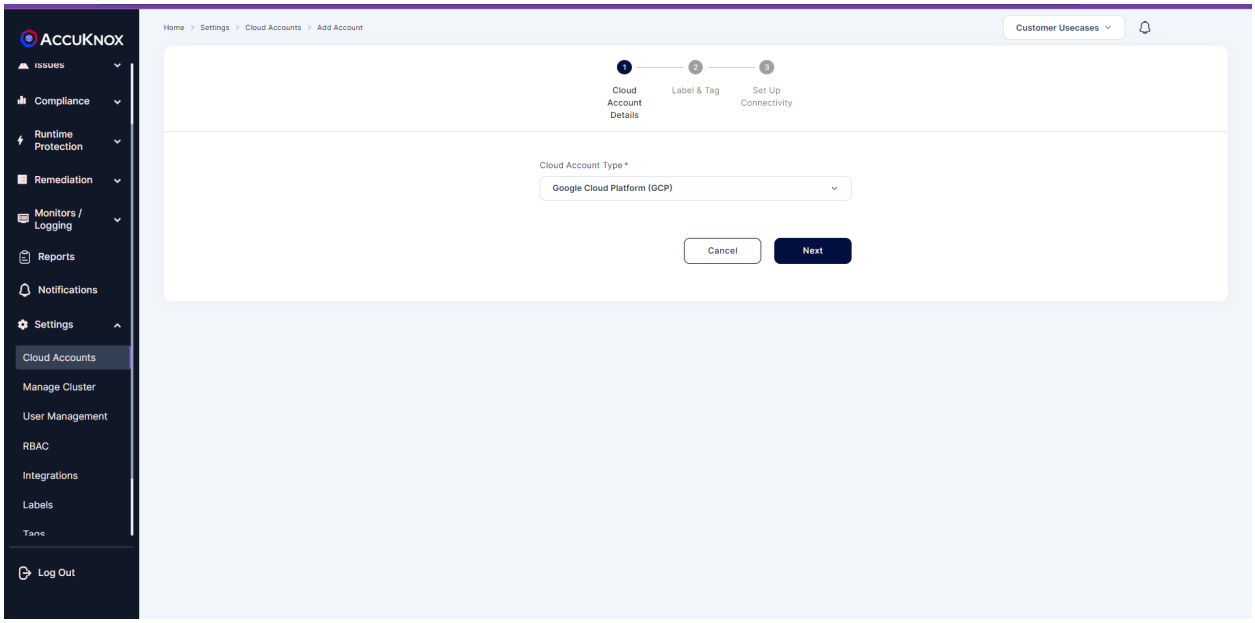


2. From AccuKnox SaaS UI

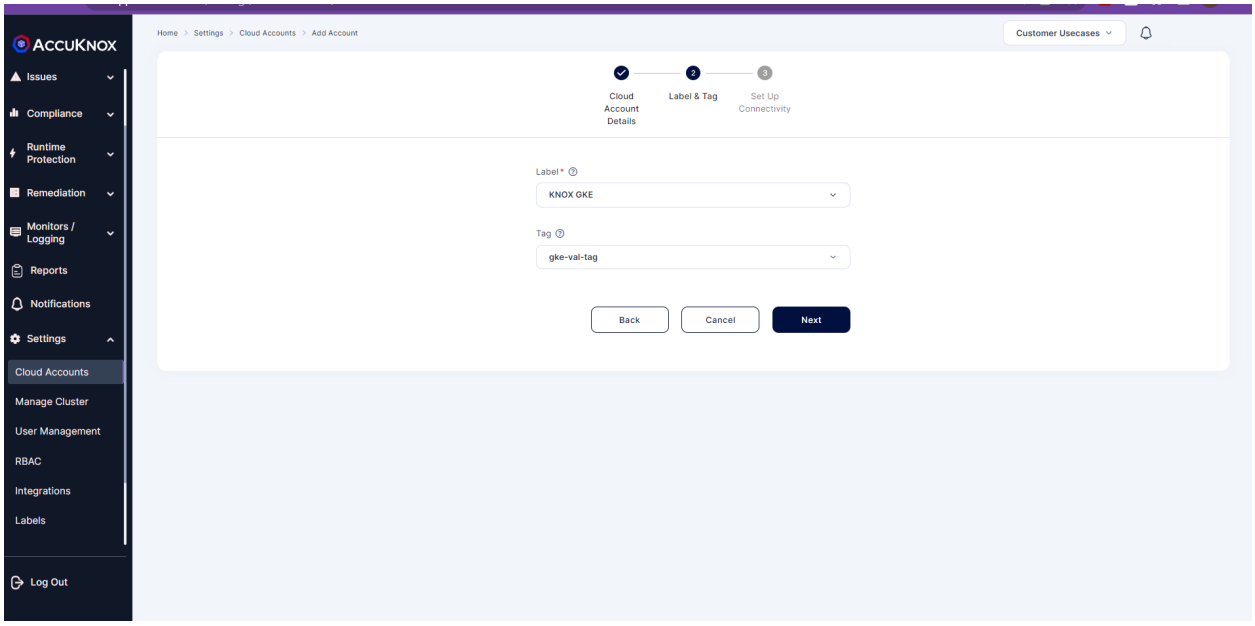
- Click settings -> Cloud Accounts
- Click Add account



- Select the Cloud Account type to GCP and Click Next

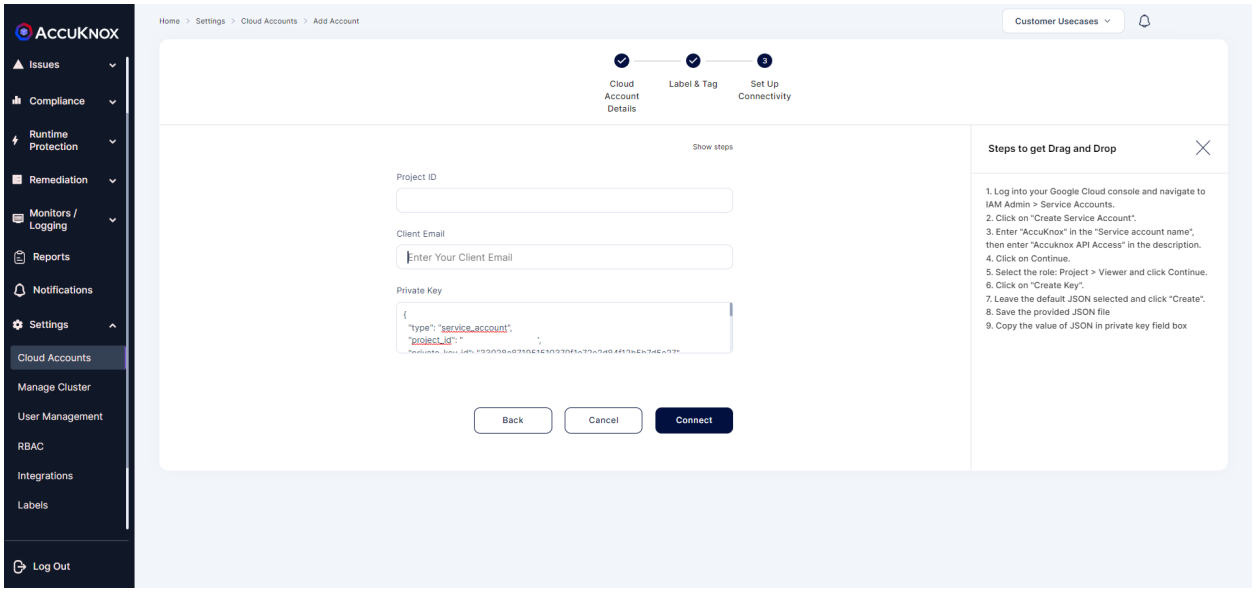


- Select the Labels and Tags and click Next



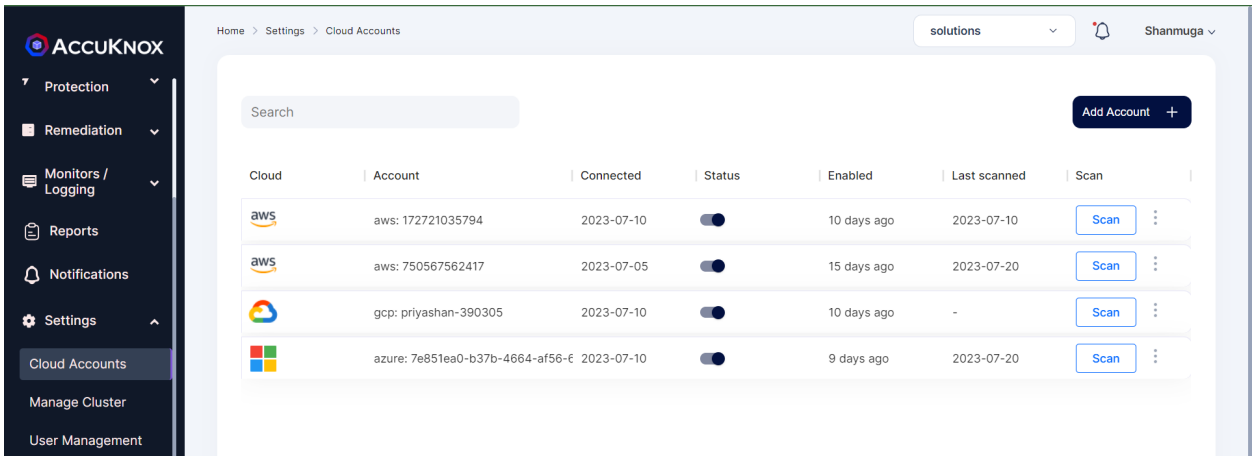
Note: If there are no labels and tags create new labels and tags via the settings

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



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.



CWPP Prerequisites

Minimum Resource required

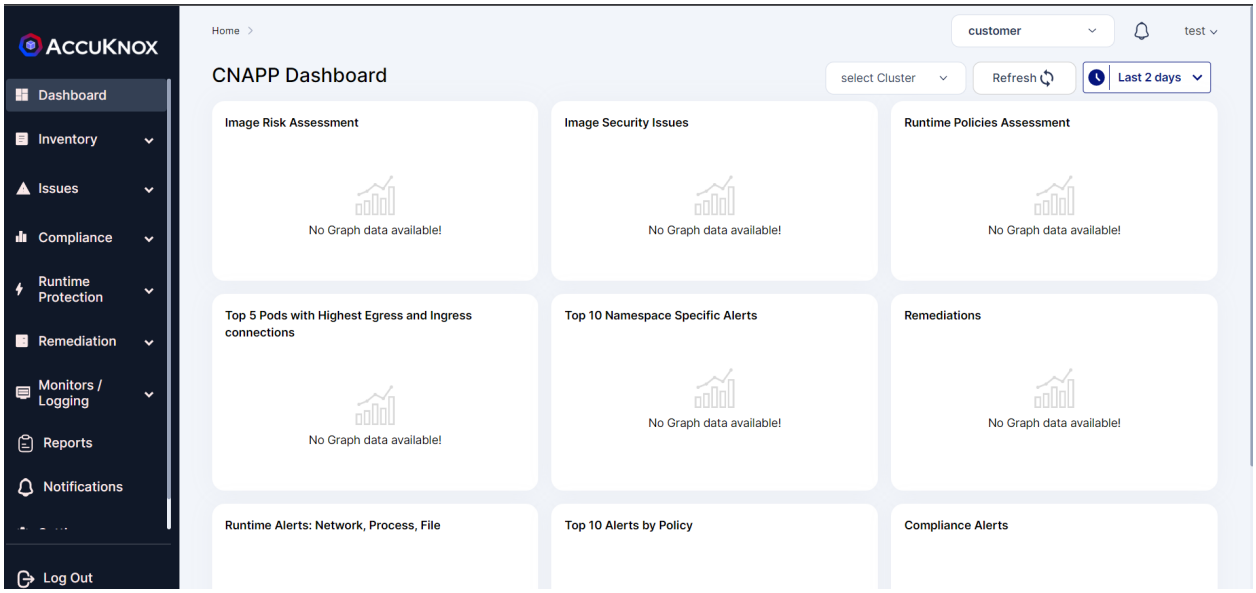
Deployments	Resource usage	Port	Connection Type
KubeArmor	CPU: 200 m, Memory: 200 Mi	-	-
Agents Operator	CPU: 50 m, Memory: 50 Mi	8081	Inbound/Outbound
Discovery Engine	CPU: 100 m, Memory: 100 Mi	-	-
Shared Informer Agent	CPU: 20 m, Memory: 50 Mi	3000	Inbound/Outbound
Feeder Service	CPU: 50 m, Memory: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

- These ports need to be allowed through the firewall.

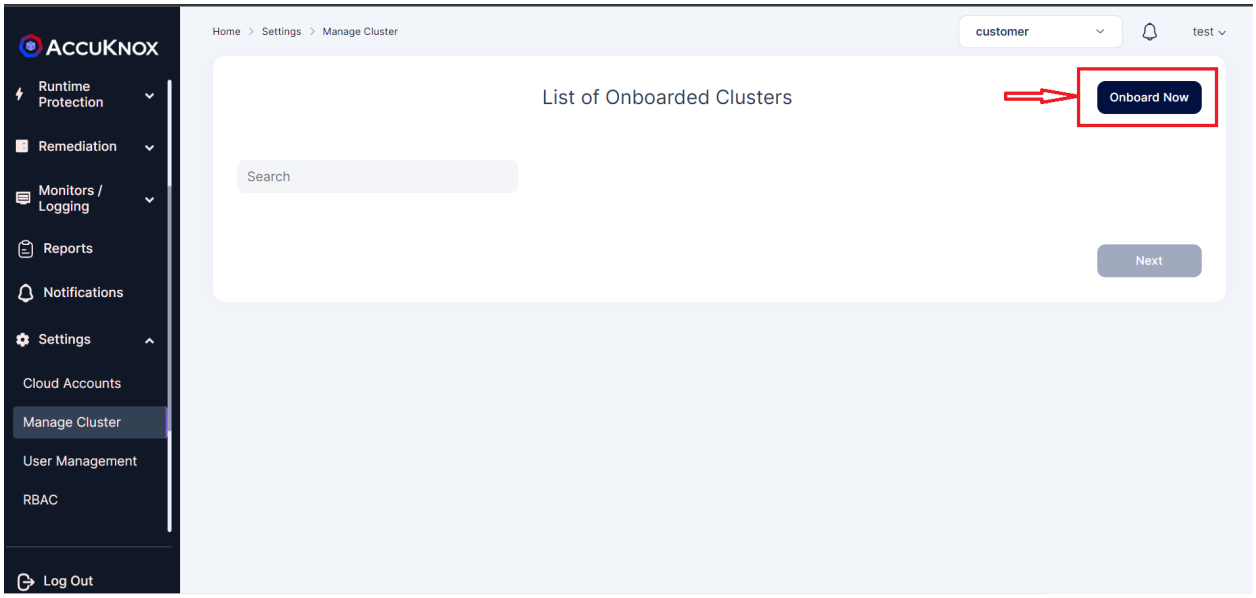
- Cluster Onboarding

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

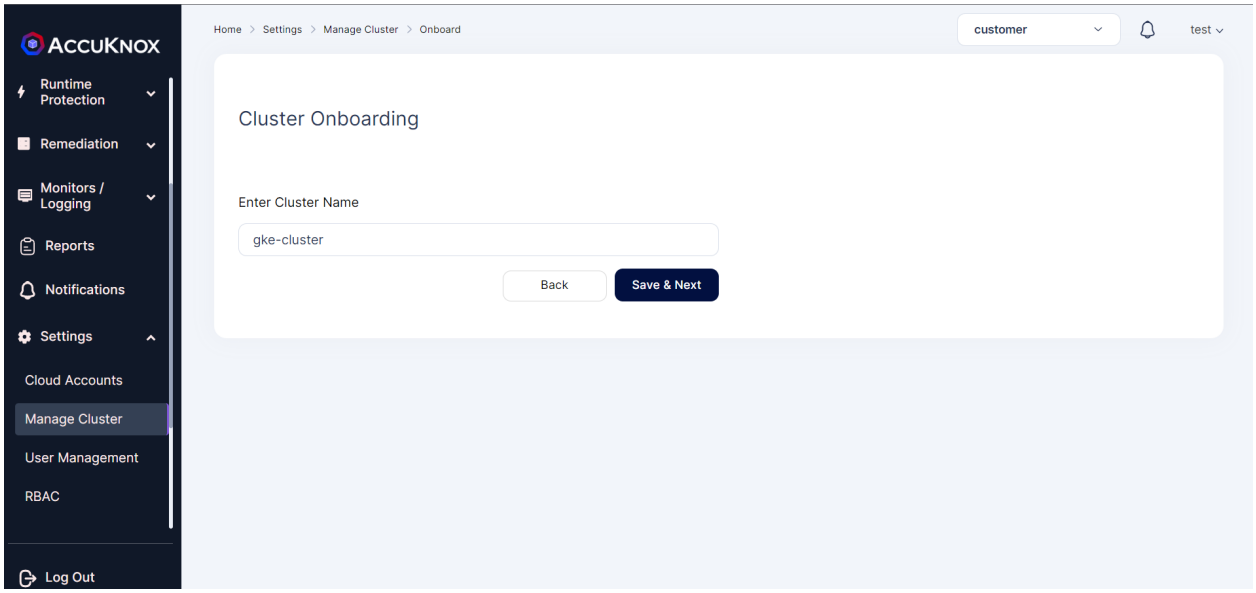
Step 1: After signing up, the user will be taken to the CNAPP dashboard. Since there is no cluster or cloud account onboarded widgets will not have any data.



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

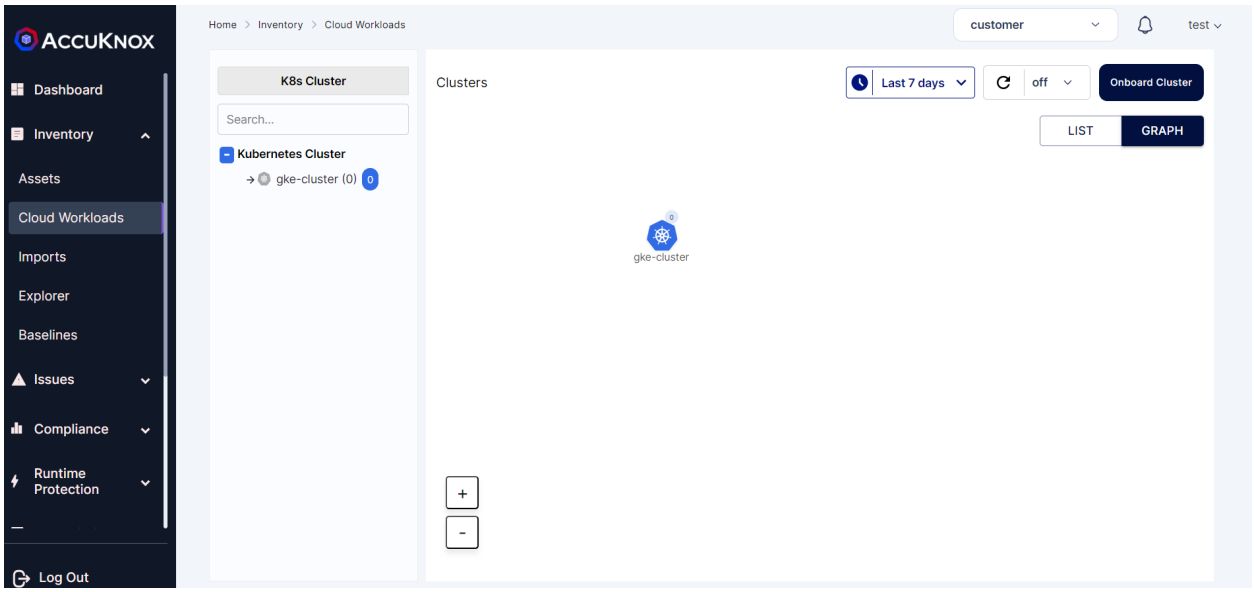


Step 3: In this screen, give any name to the cluster that you are going to onboard now.



Step 4: Onboarded Cluster without AccuKnox agents:

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



Step 5: Installing KubeArmor and AccuKnox agents:

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

Step 5.1: KubeArmor Installation:

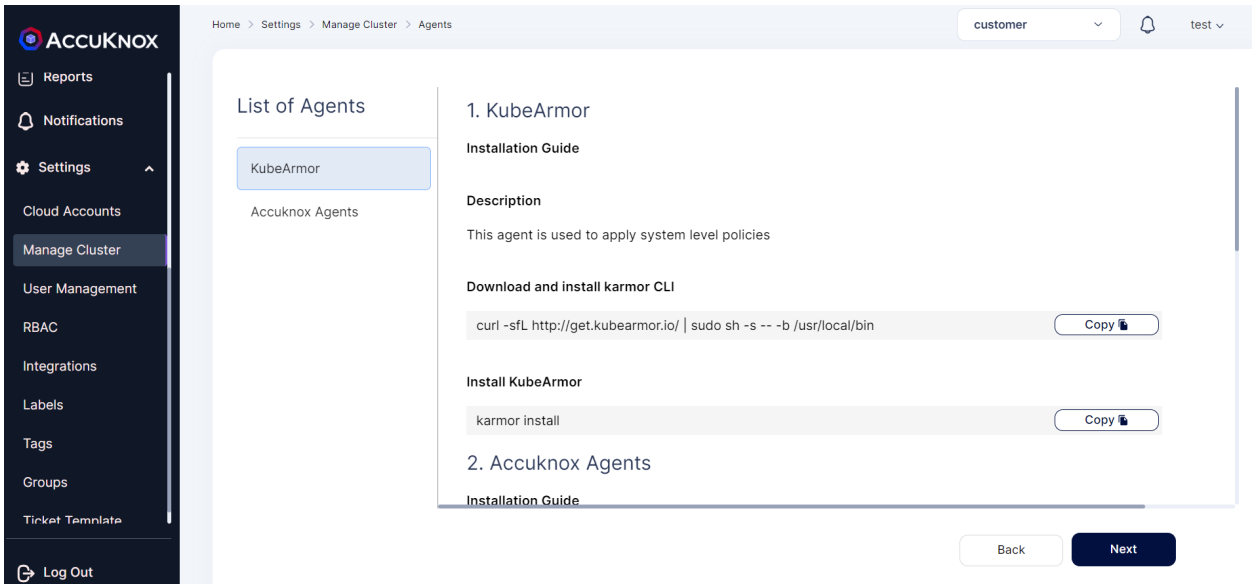
KubeArmor:

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

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

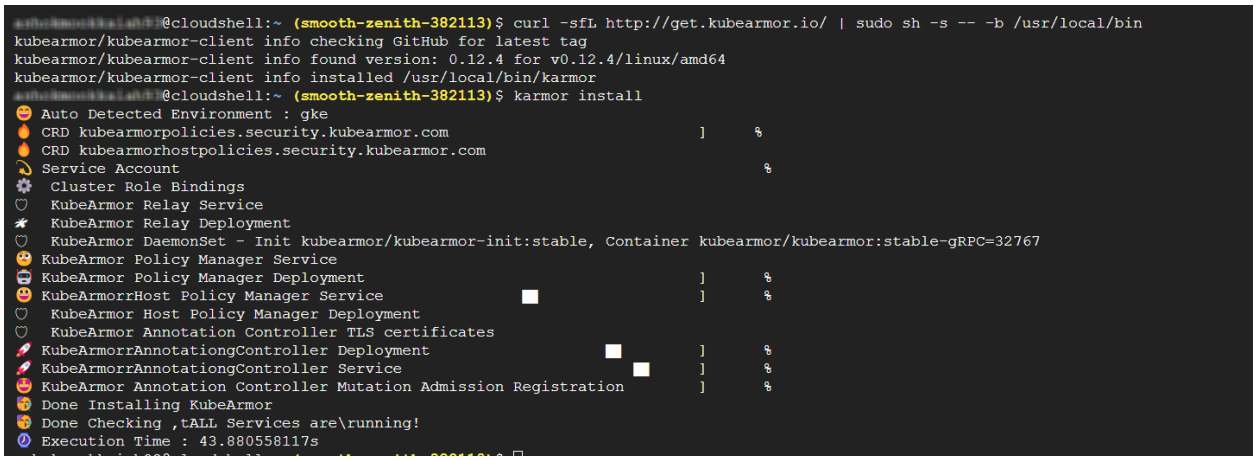
KubeArmor differs from seccomp-based profiles, wherein KubeArmor allows to dynamically set the restrictions on the pod. With seccomp, the restrictions must be

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



KubeArmor is installed using the following commands:

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



Step 5.2: AccuKnox-Agents installation:

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

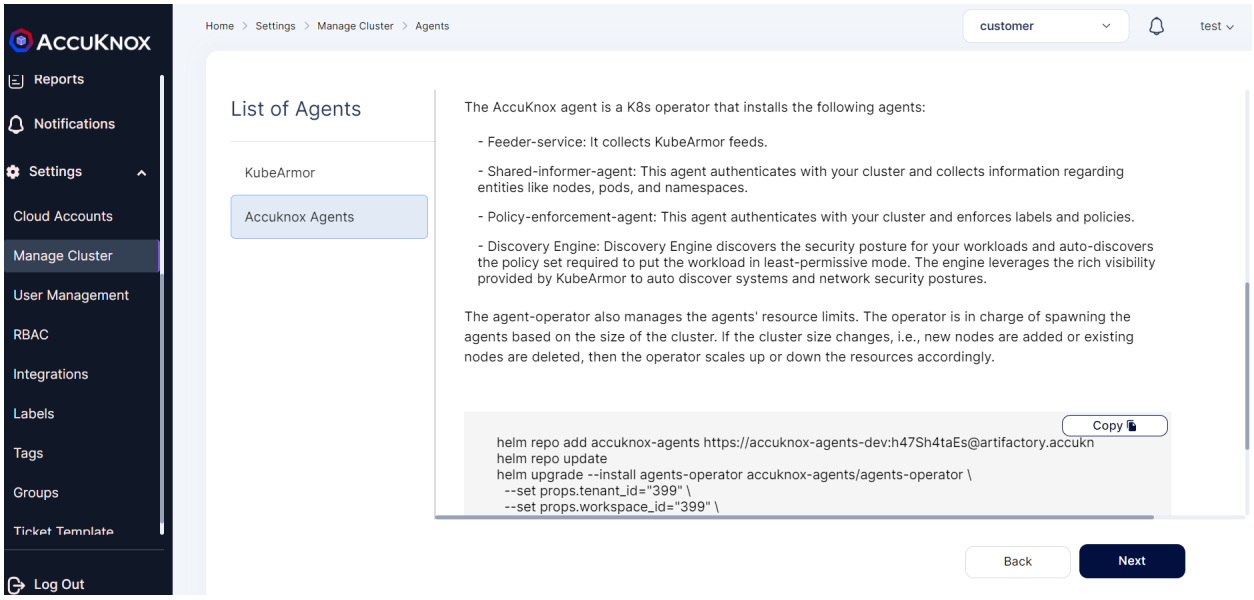
AccuKnox Agents:

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.,

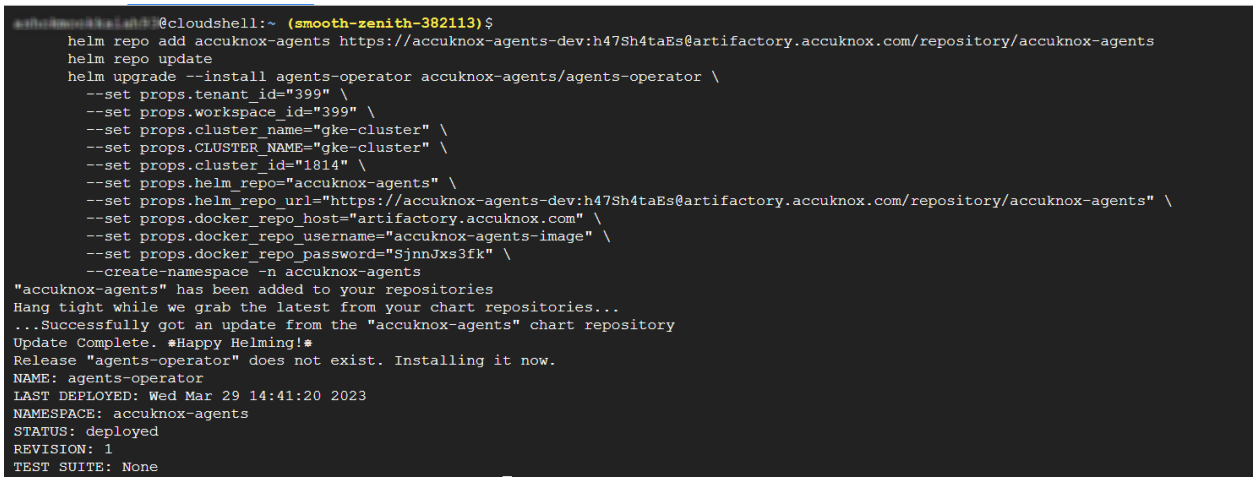
4.Policy Discovery Engine: It discovers the policies using the workload and cluster information that is relayed by a shared informer Agent.



AccuKnox Agents can be installed using the following command:

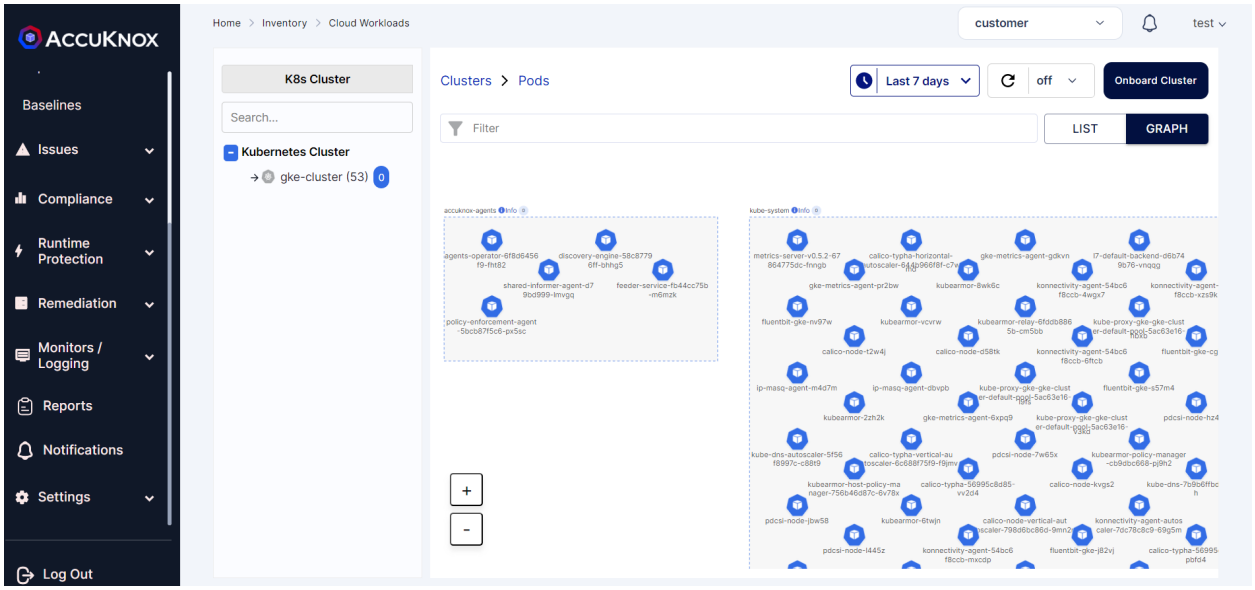
```
                    helm repo add accuknox-agents
https://accuknox-agents-dev:h47Sh4taEs@artifactory.accuknox.com/rep
ository/accuknox-agents
      helm repo update
                    helm upgrade --install agents-operator
accuknox-agents/agents-operator \
```

```
        --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@artifac
tory.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
```

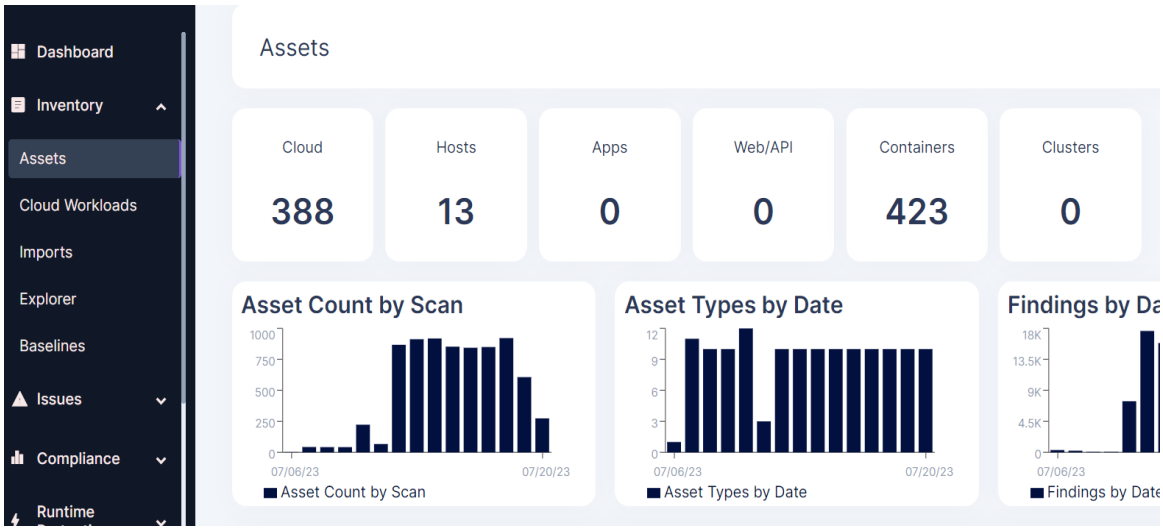


Note: In the above command workspace_id,cluster_name,tenant_id are specific to this example and it will vary based on the cluster

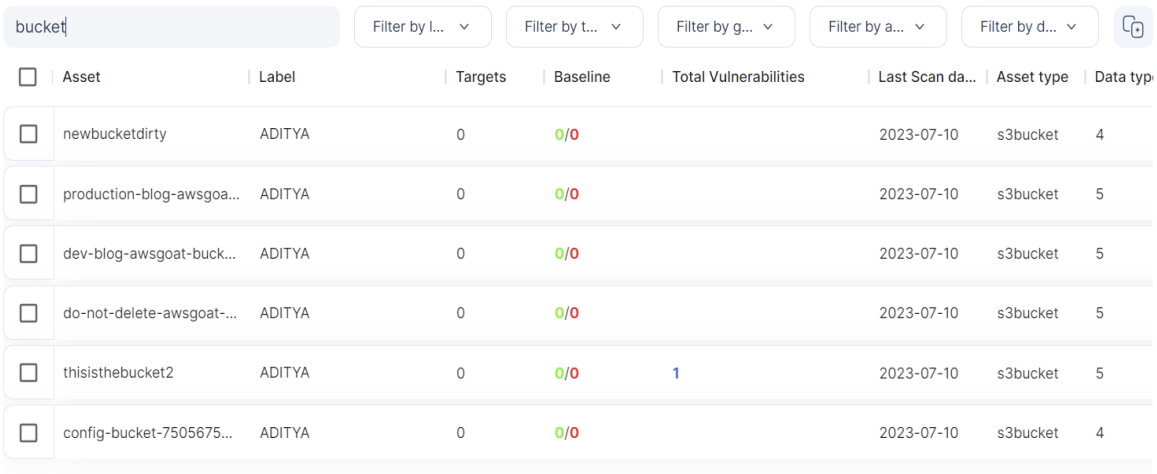
Step 6: After installing all the AccuKnox agents the cluster is onboarded successfully into the SaaS application. We can see the workload details of the onboarded cluster by Navigating to Inventory->cloud Workloads option



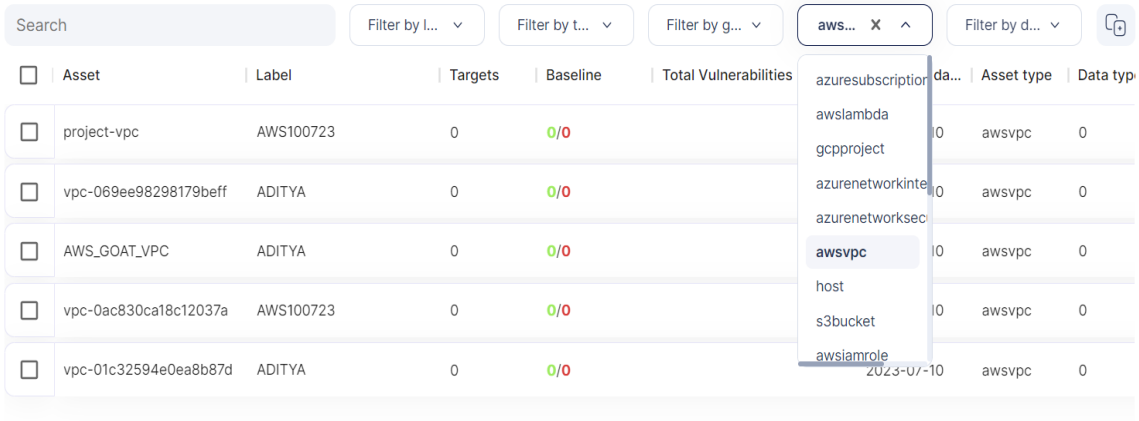
- Asset Inventory
  - Cloud Assets
    - How to find a particular asset
      - First navigate to the Assets screen under Inventory:



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

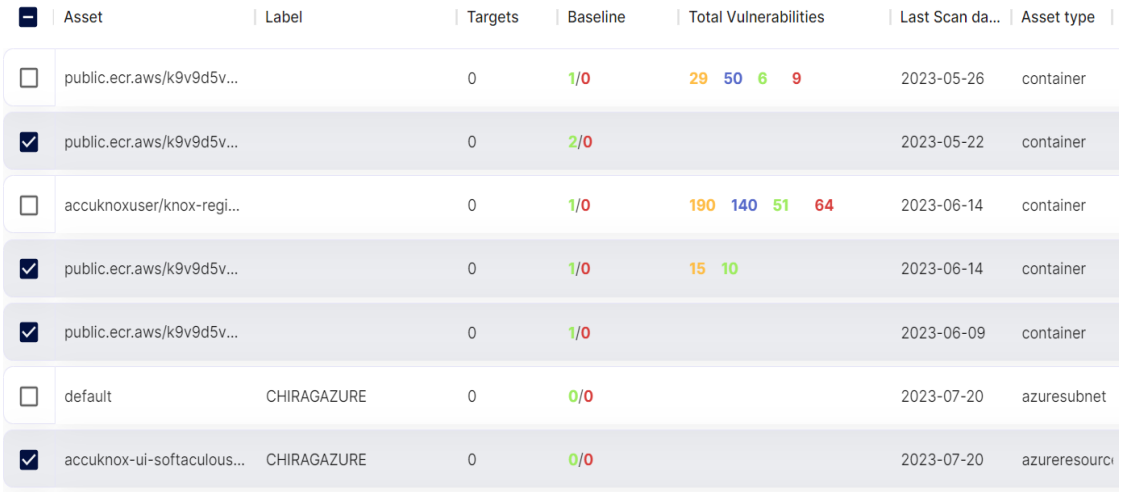


- Or if the name is not known but the Asset type is known, the Filter by Asset drop down can be used to filter the assets list. The search functionality can also be used on the filtered result:



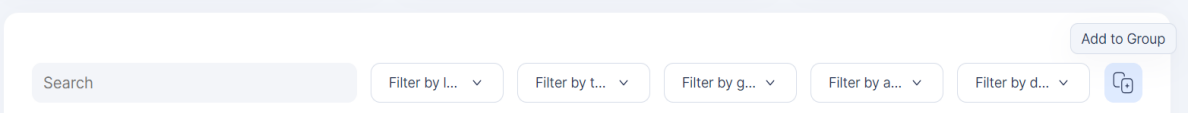
How to group assets

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

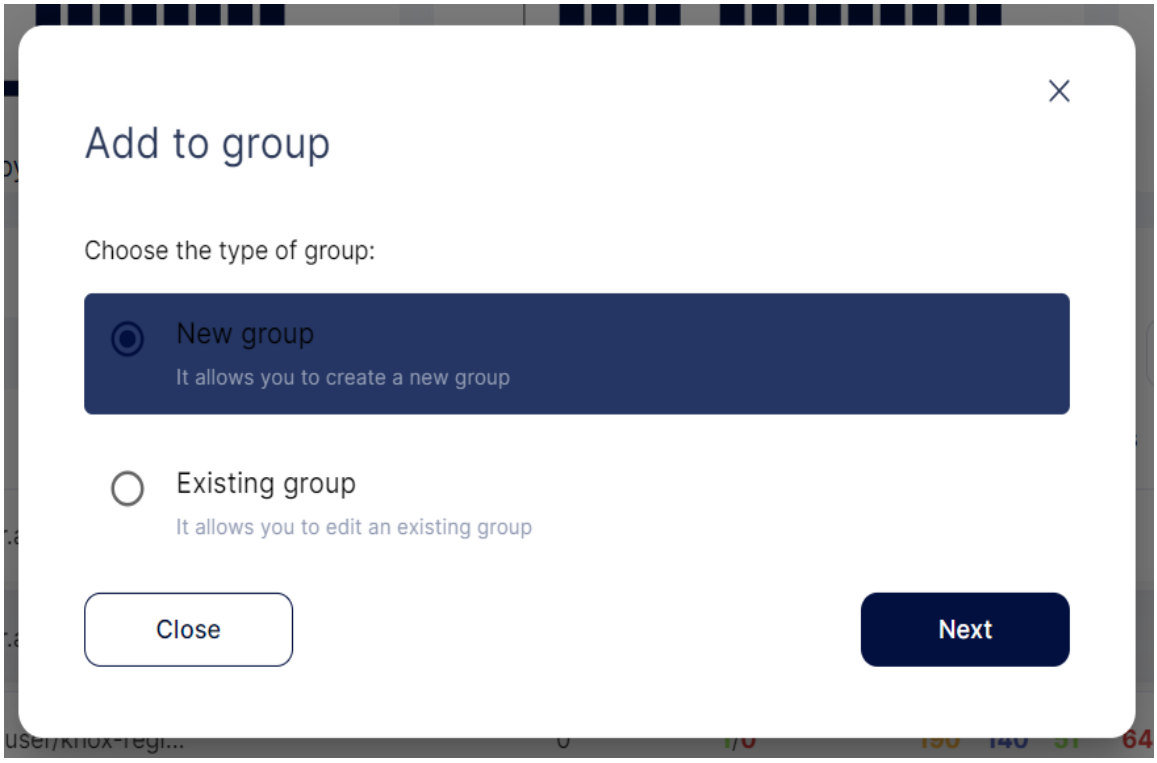


Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da...	Asset type
public.ecr.aws/k9v9d5v...		0	1/0	29 50 6 9	2023-05-26	container
public.ecr.aws/k9v9d5v...		0	2/0		2023-05-22	container
accuknoxuser/knox-regi...		0	1/0	190 140 51 64	2023-06-14	container
public.ecr.aws/k9v9d5v...		0	1/0	15 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:

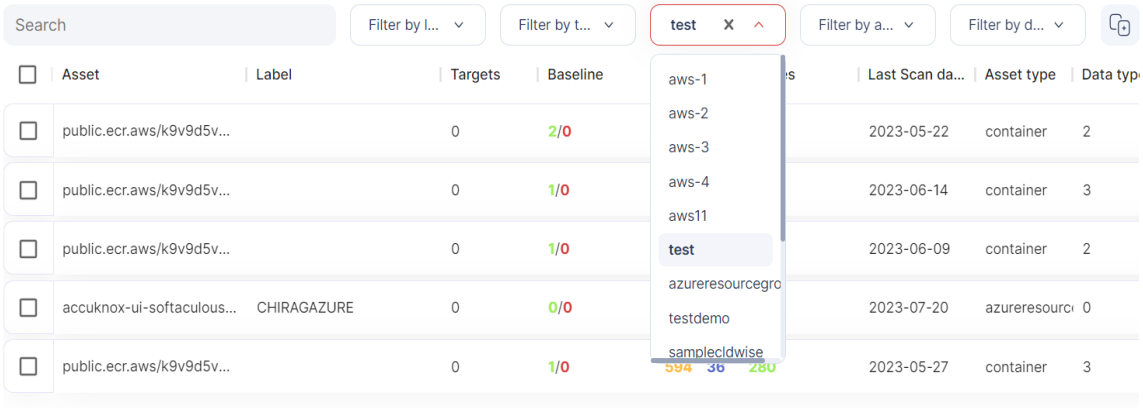


  - In the pop-up that follows, create a new group or add to an existing group:

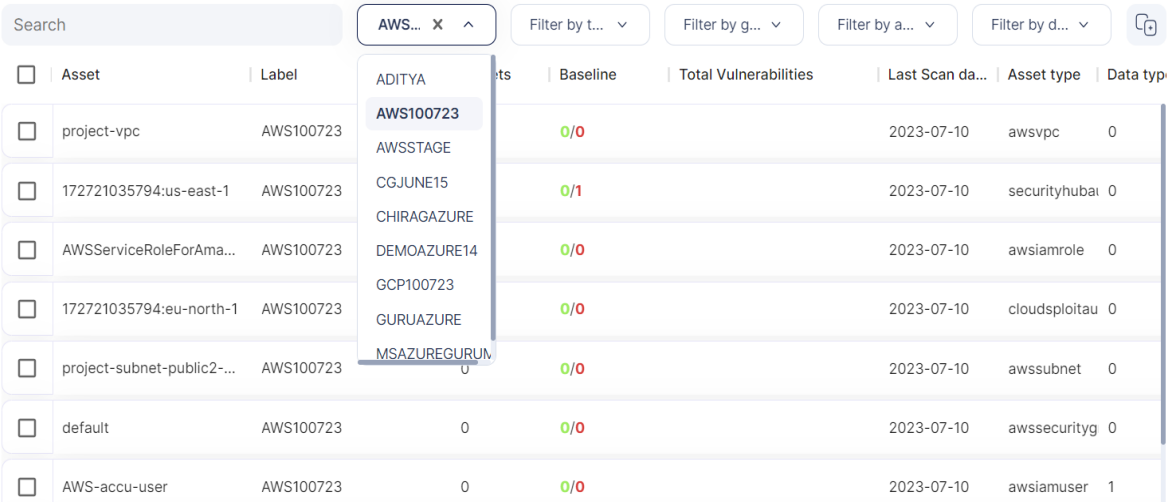


- After entering a name for the group or selecting an existing group, click on Save to finish adding the assets to a group:

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

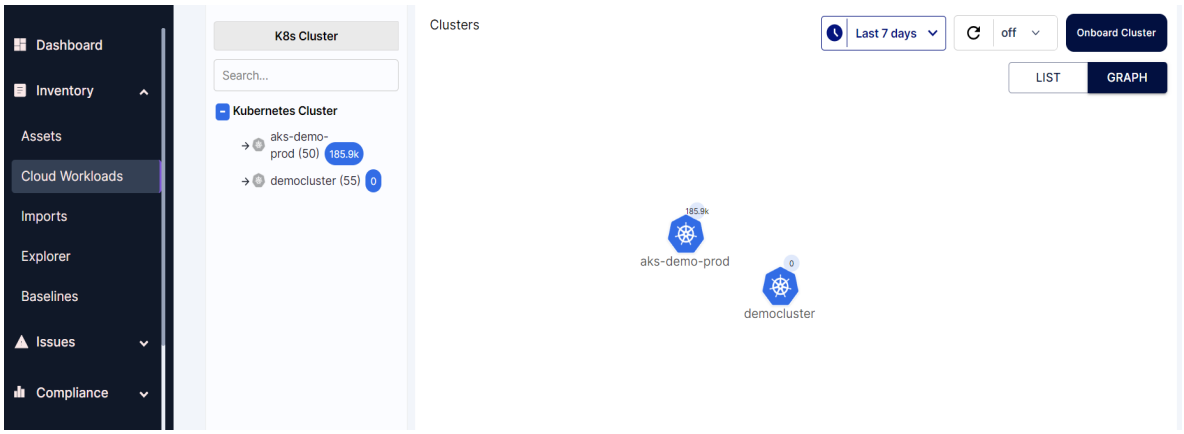

Search
Filter by l...
Filter by t...
test
Filter by a...
Filter by d...
Asset
Label
Targets
Baseline
Last Scan da...
Asset type
Data typ
public.ecr.aws/k9v9d5v...
0
2/0
2023-05-22
container
2
public.ecr.aws/k9v9d5v...
0
1/0
2023-06-14
container
3
public.ecr.aws/k9v9d5v...
0
1/0
2023-06-09
container
2
accuknox-ui-softaculous...
CHIRAGAZURE
0
0/0
2023-07-20
azureresourc
0
public.ecr.aws/k9v9d5v...
0
1/0
2023-05-27
container
3
aws-1
aws-2
aws-3
aws-4
aws11
test
azureresourcegro
testdemo
samplecldwise

- 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:

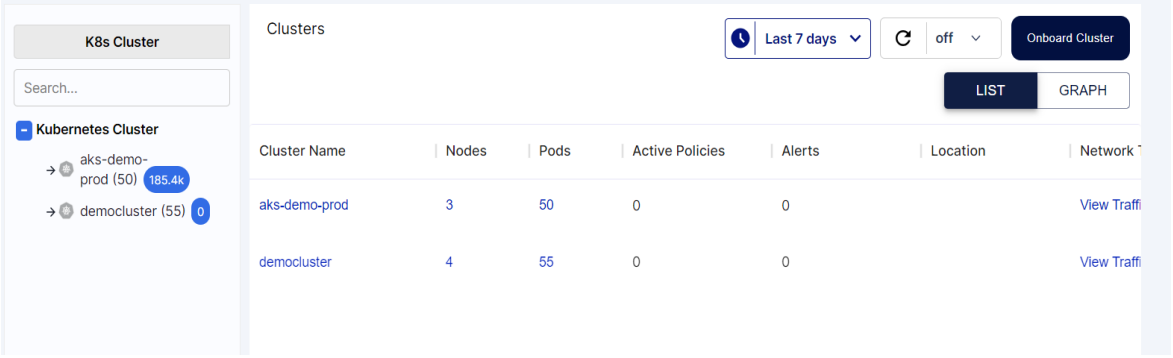


  - To further refine the results, we can use the search bar or add additional filters such as Assets

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

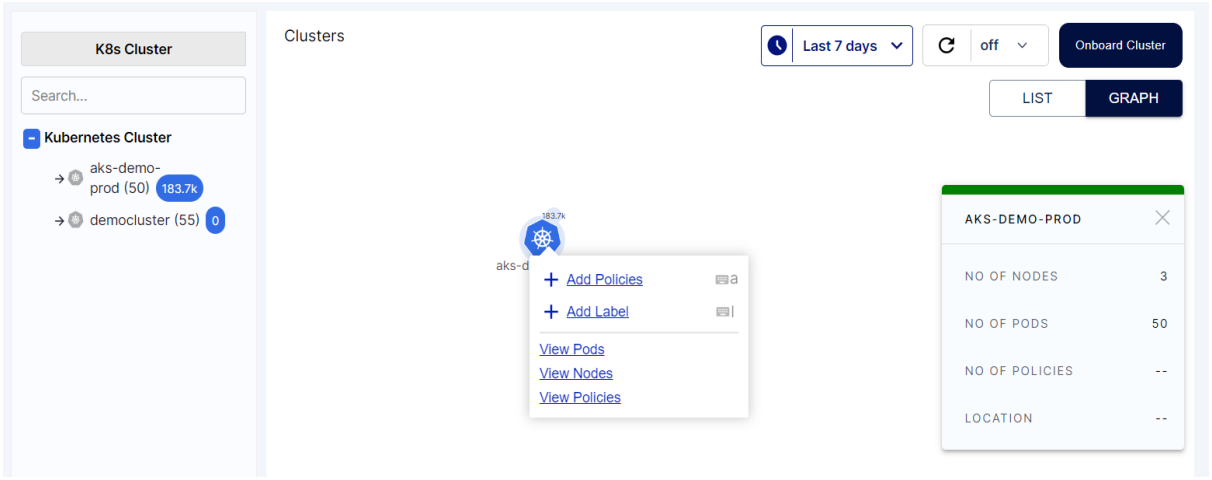


- How to find list view of clusters
    - Click on the LIST option in the top right of the Cloud Workloads screen to get a list view of all the clusters

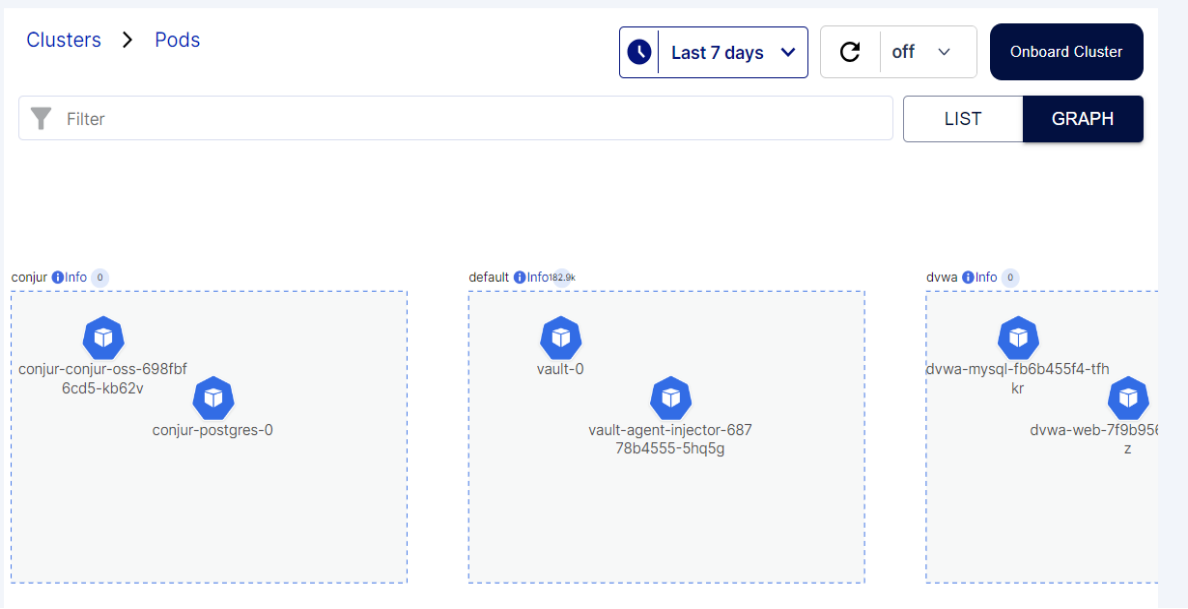


- The view can be freely switched between LIST and GRAPH as required

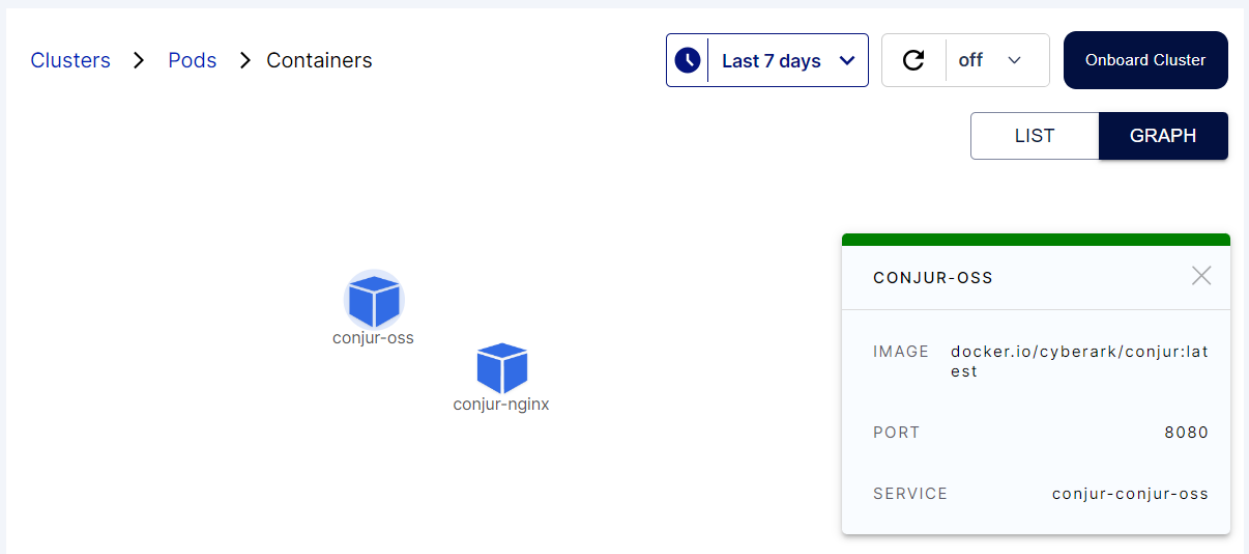
- How to find details on cluster
- Clicking on any of the clusters in the Cloud Workloads screen gives more information about the cluster:



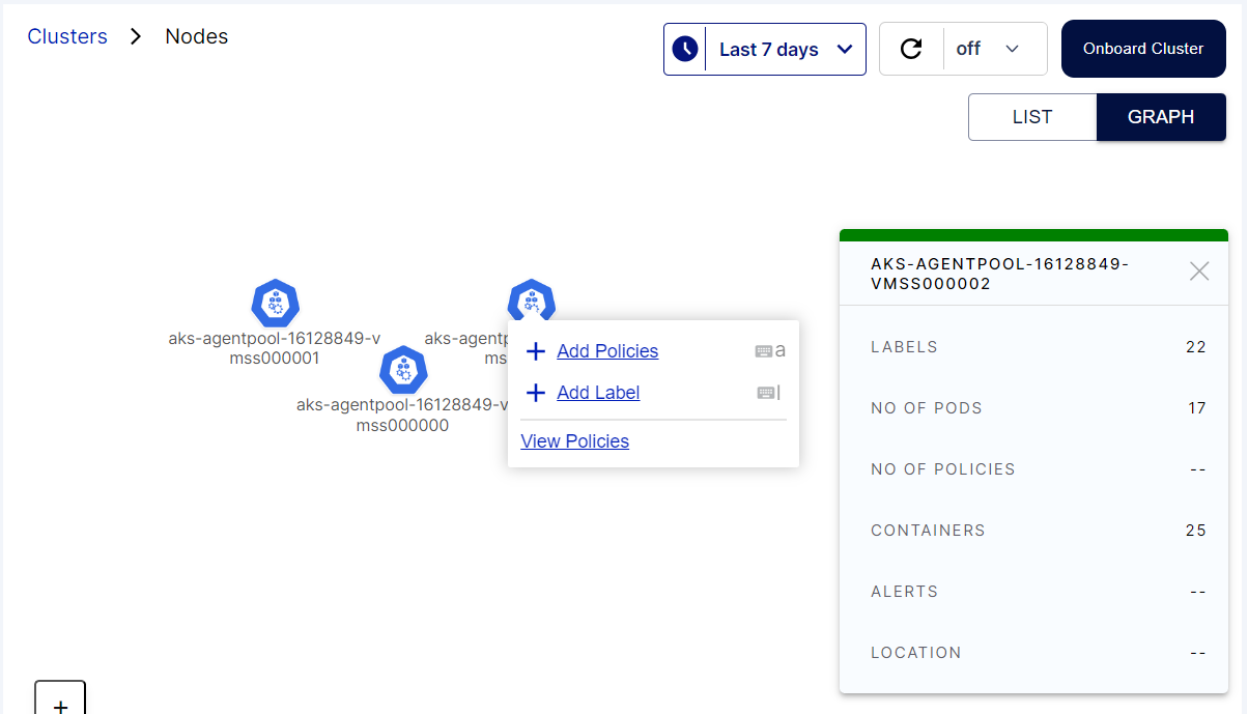
- Click on View Pods to view the Pods present in the cluster classified according to the namespaces they are present in:



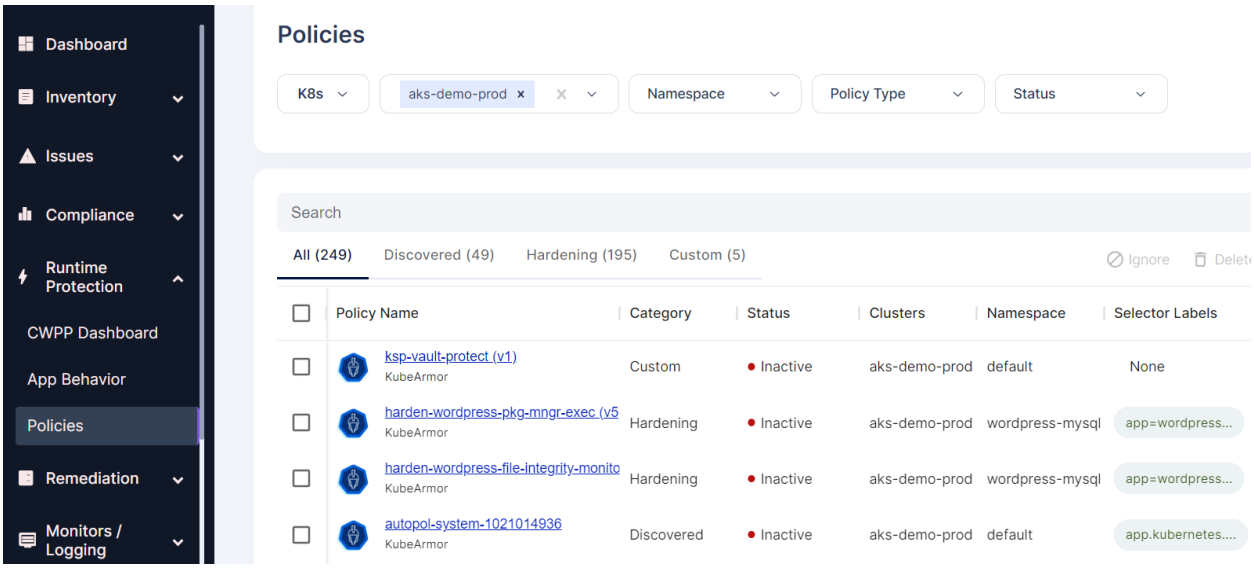
- Double click on the pods to view the containers present in them. Select any container to view more details:



- 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:

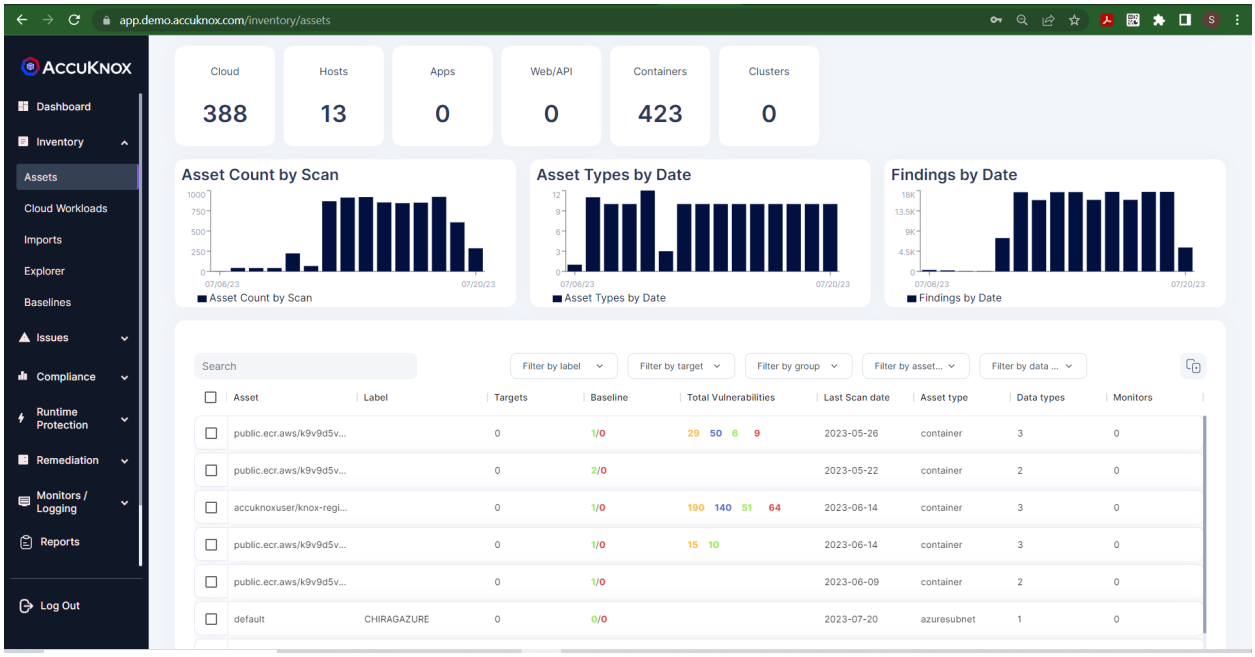


- We can also double click on the node to view the Pods running in them
- View Policies can be clicked to jump to the Policies screen to show the policies for the selected cluster or pod:

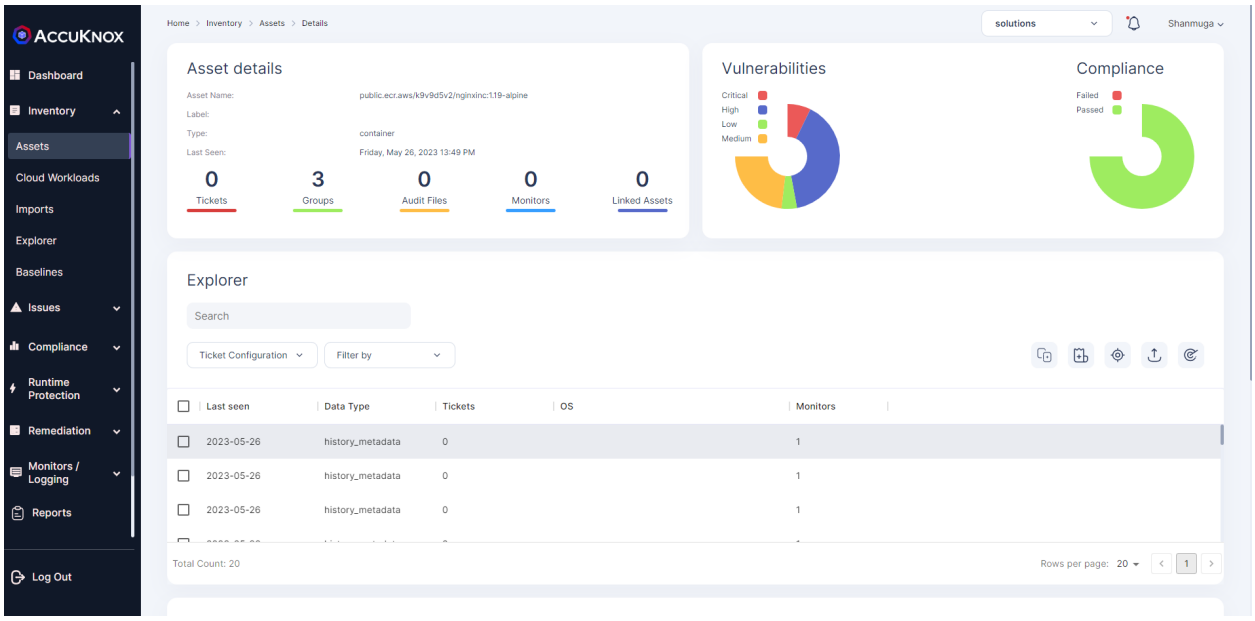


- Misconfigurations
  - Where to find misconfigurations
    - Asset Detail Page

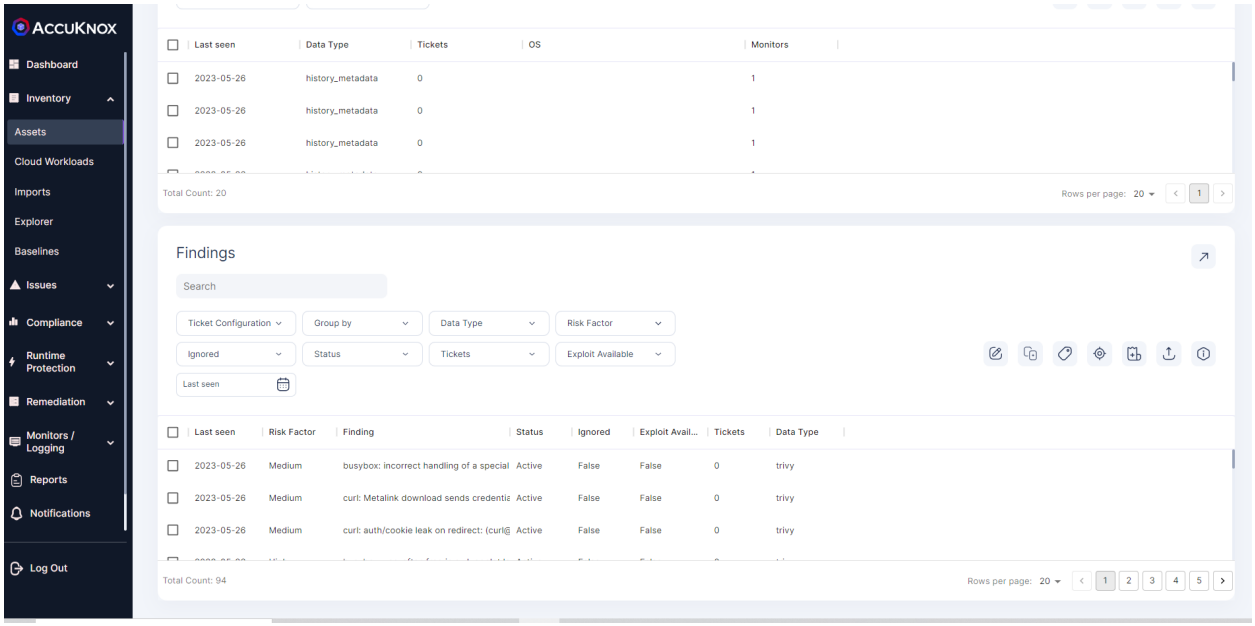
Once we have onboard the Cloud Account, we can navigate to the Inventory → Asset page where we can see the List of Assets with vulnerabilities.



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

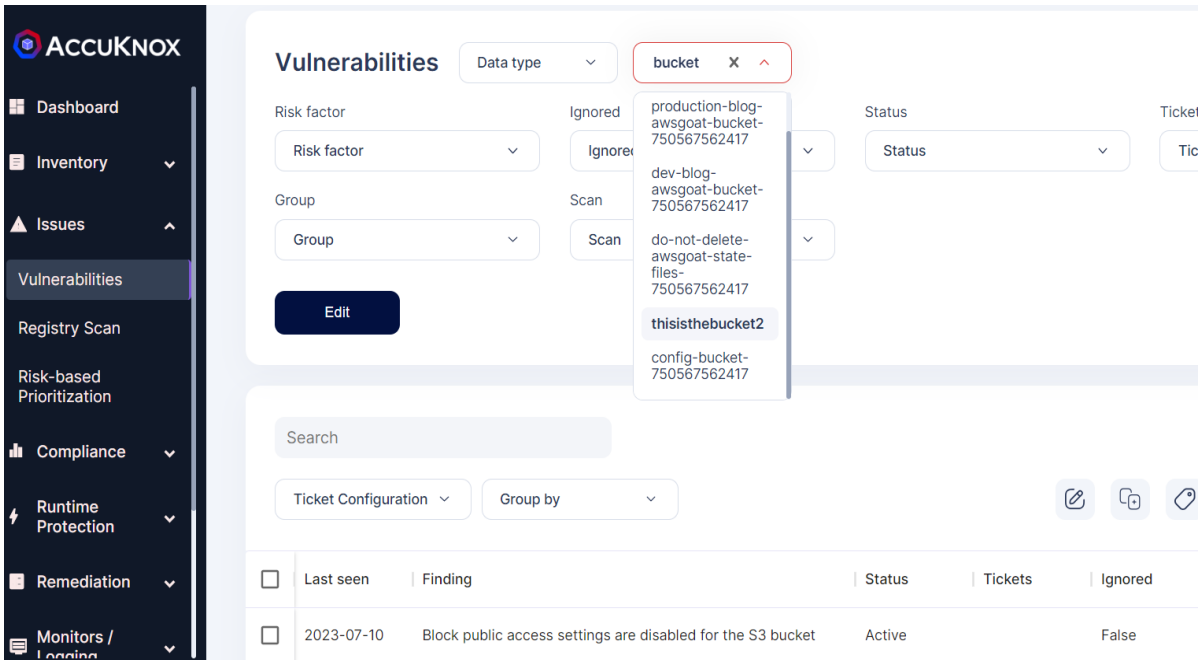


Scroll down for the Findings



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

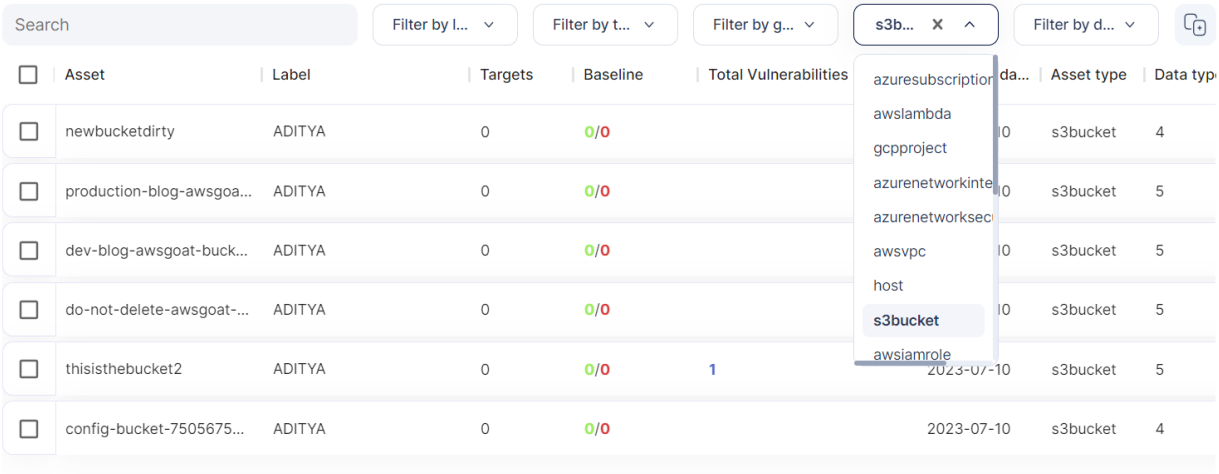
- Issue Page
  - Navigate to Vulnerabilities screen under Issues and select an Asset from the drop down at the top to view all misconfigurations associated with the Asset:



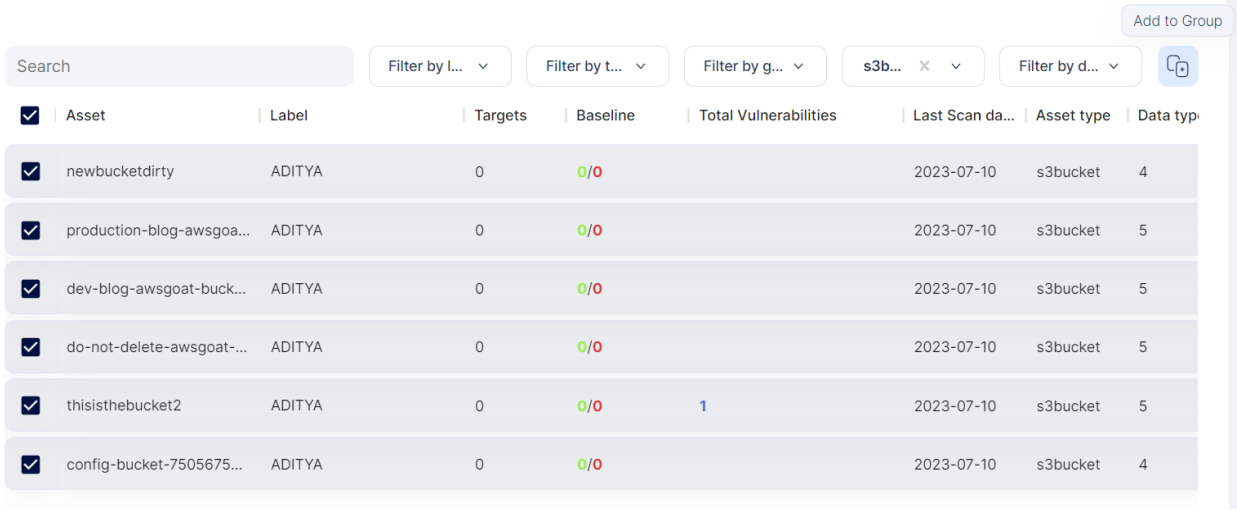
- You can also type in the Assets drop down to search for a particular Asset

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

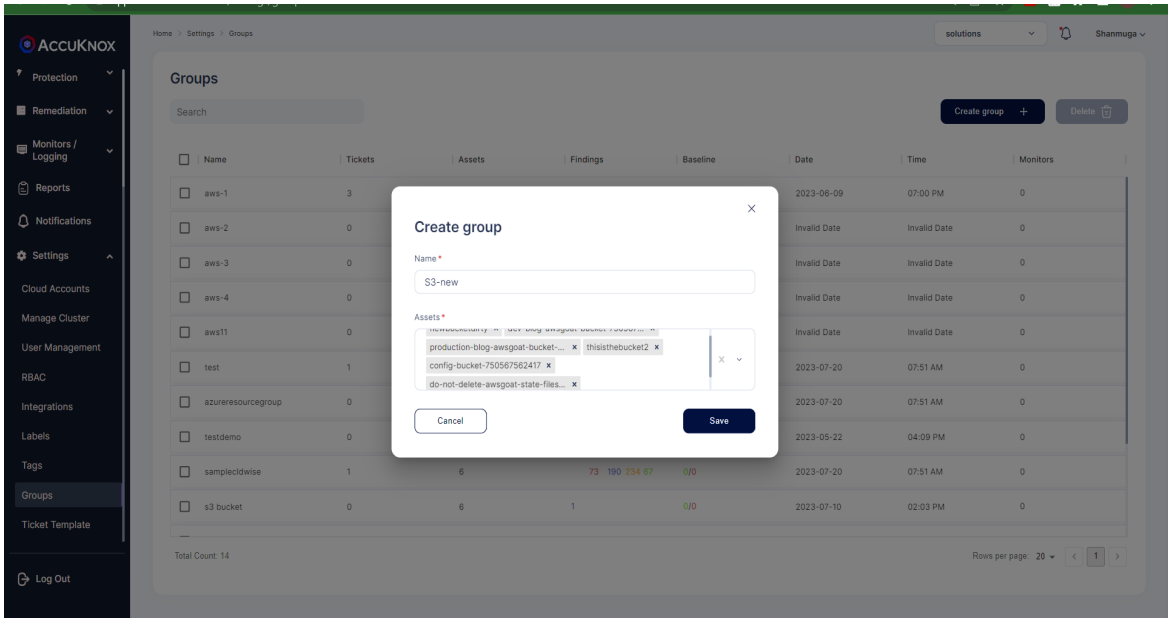
Step1 : In the Assets screen under Inventory, filter by Assets to view only the S3 buckets:



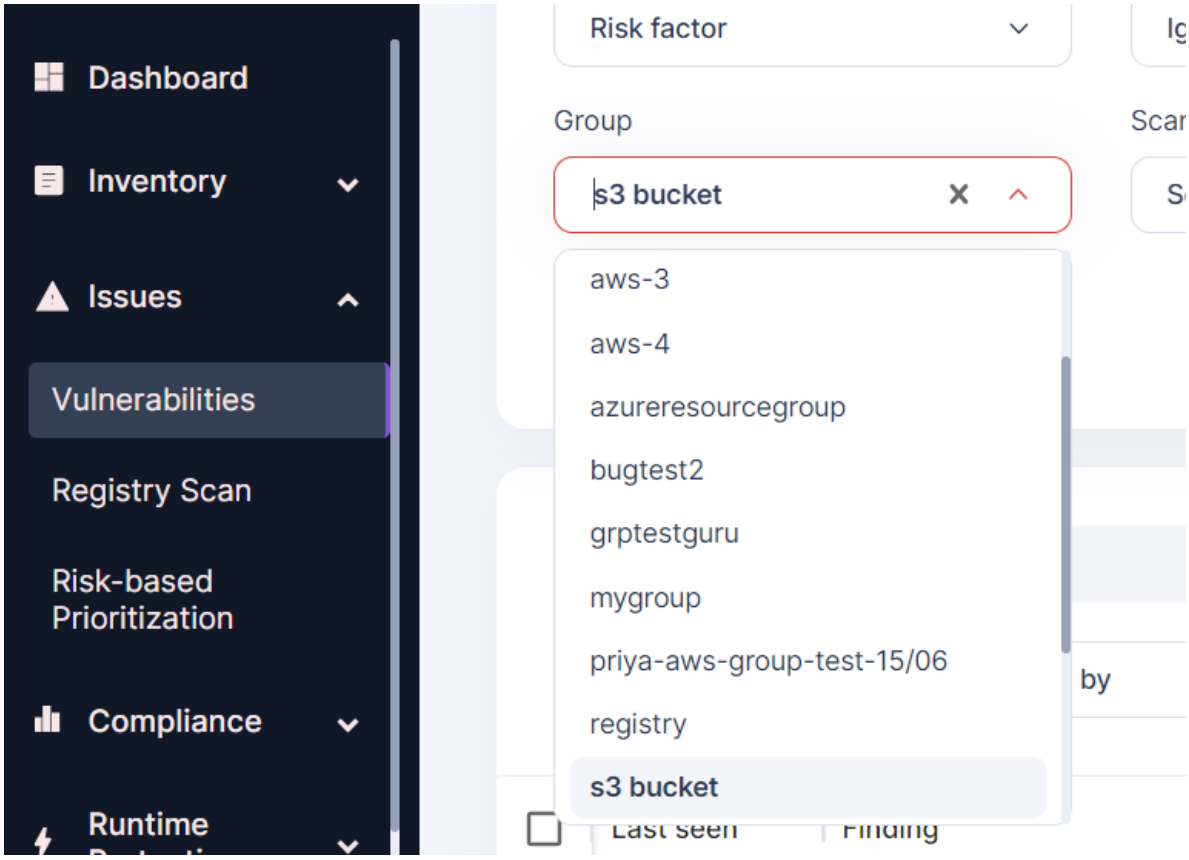
Step2 : Select all and Add to a group by clicking the Add to group button:



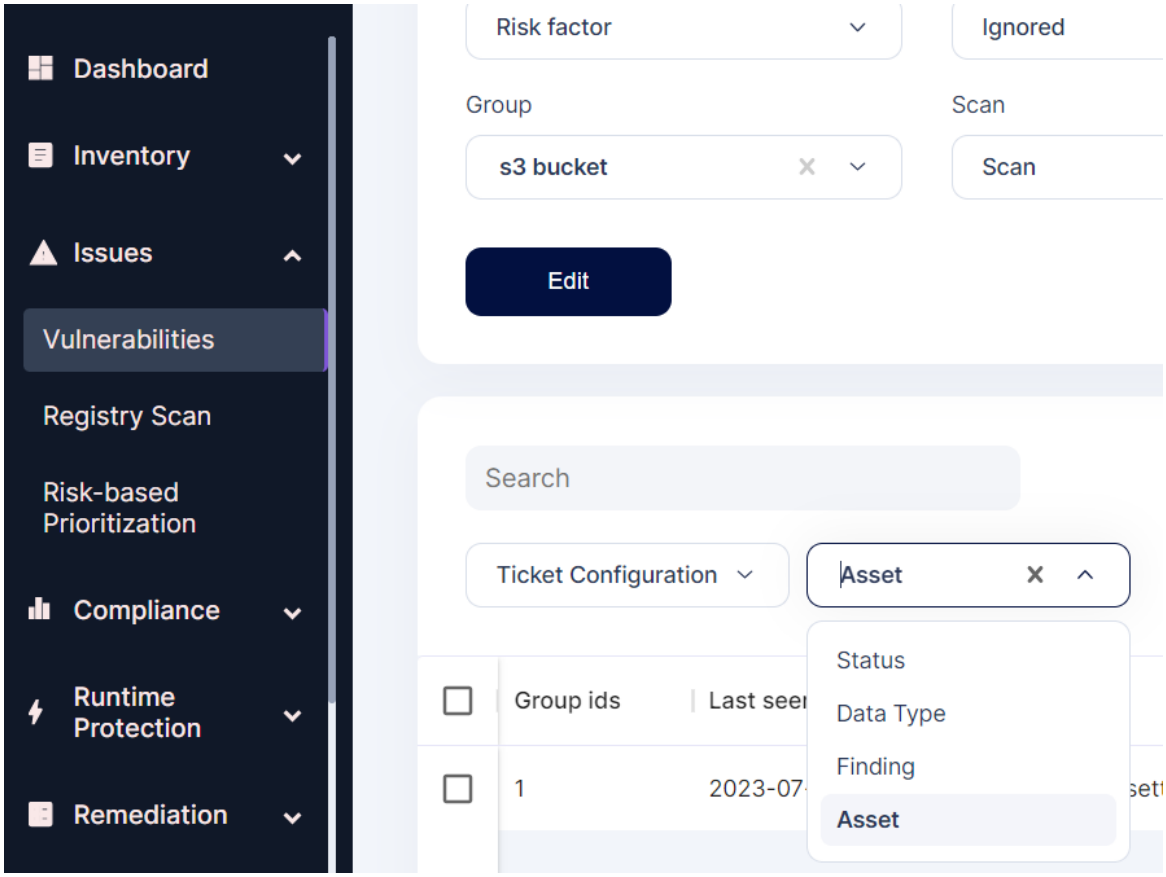
Step3: Click on Save



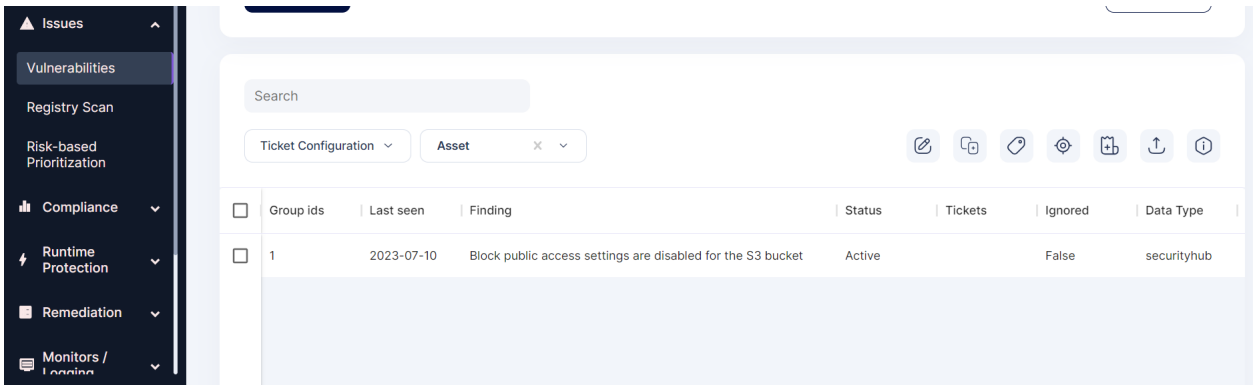
Step 4 : Click on Issues -> Vulnerabilities and select the group that was created from the drop down:



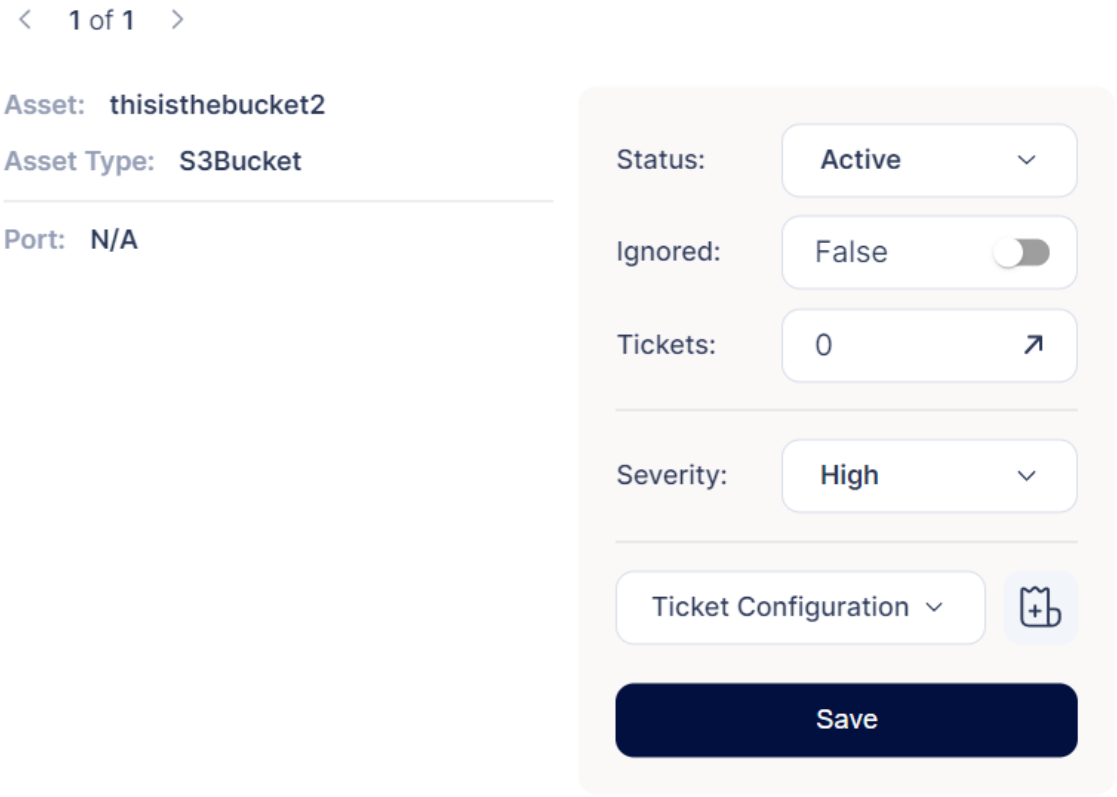
Step 5: To view the Grouped S3 bucket details, click on the group by option and select Asset:



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



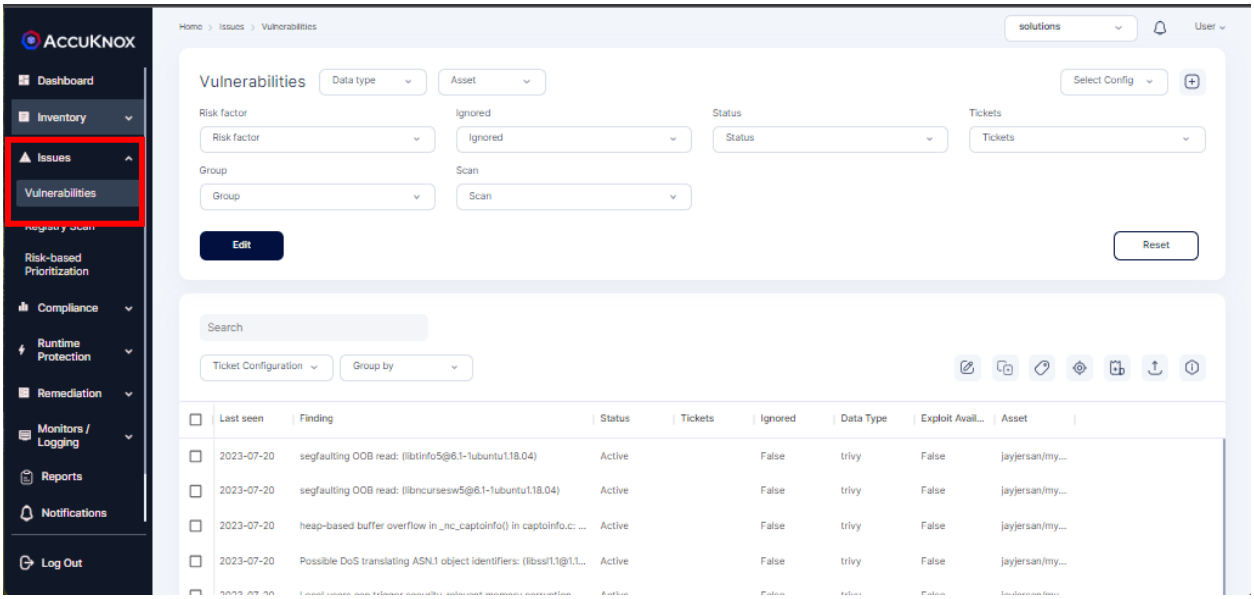
Step 7: Click on any of them to get more details



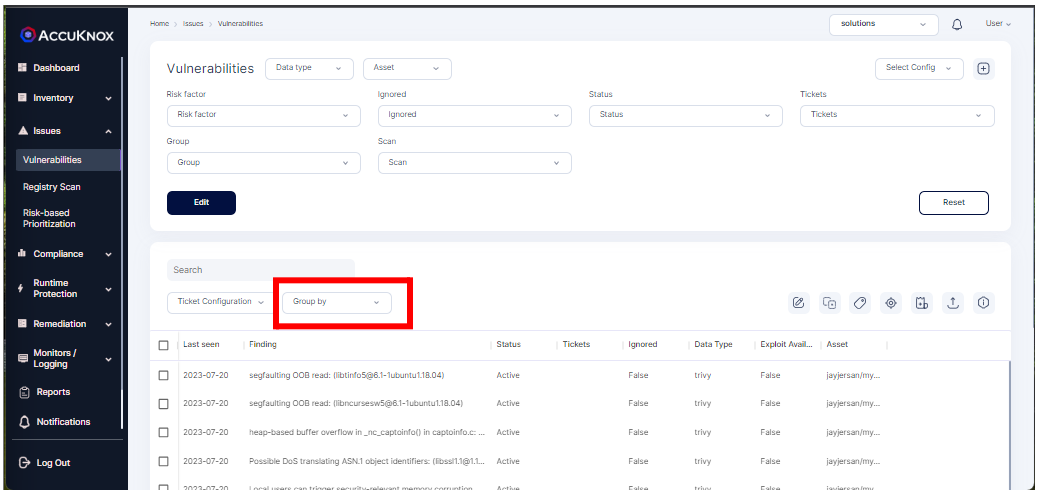
Similarly, we can use only the group by option to view all the misconfigurations grouped together for each Asset.

- How to group by findings

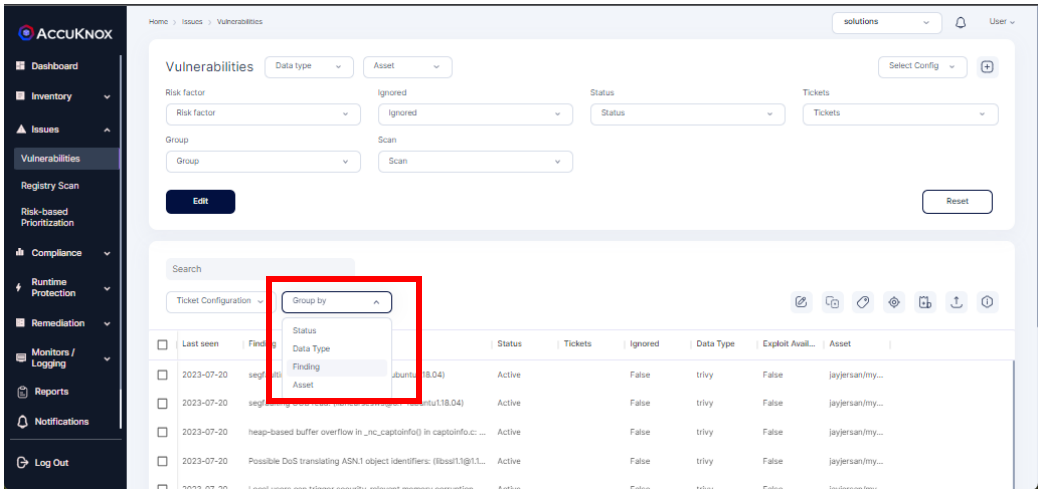
1. Goto ***Issues*** tab, click on ***Vulnerabilities*** section



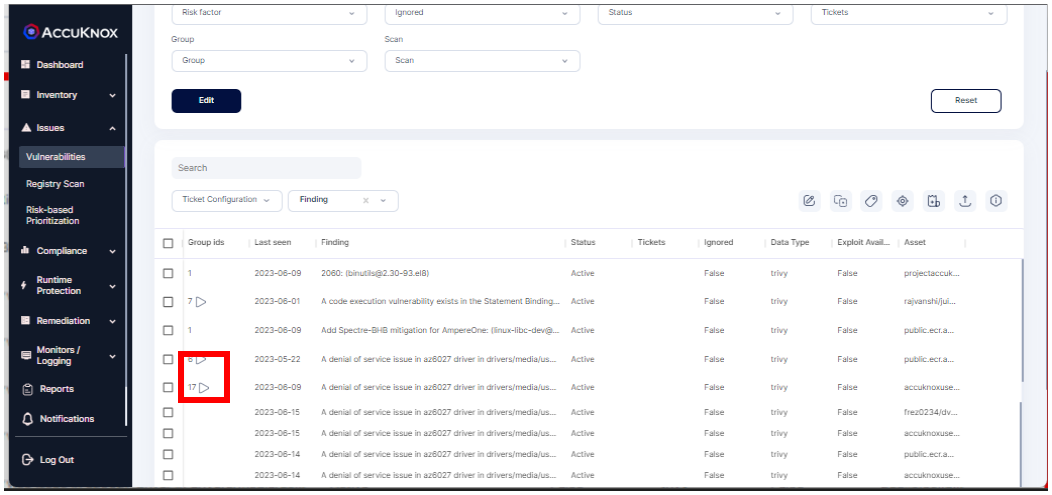
2. Navigate to ***Group by*** filter.



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

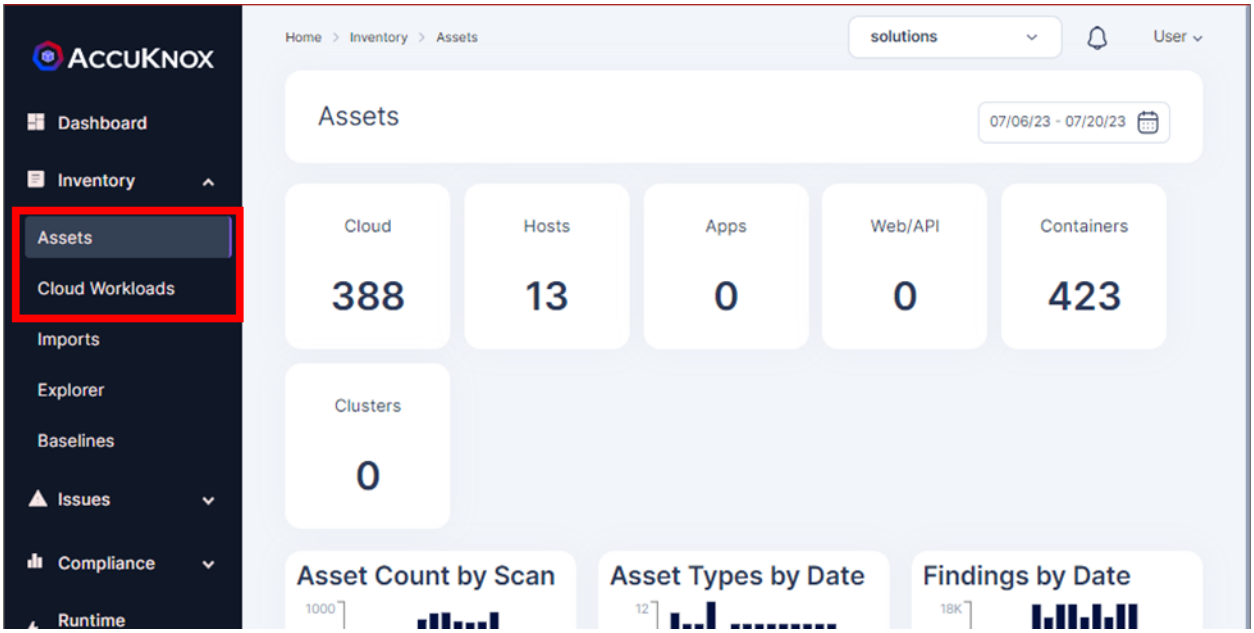


Now, you can view that similar findings are grouped. On clicking the arrow button in the findings list, you will able to view all the assets it is found in

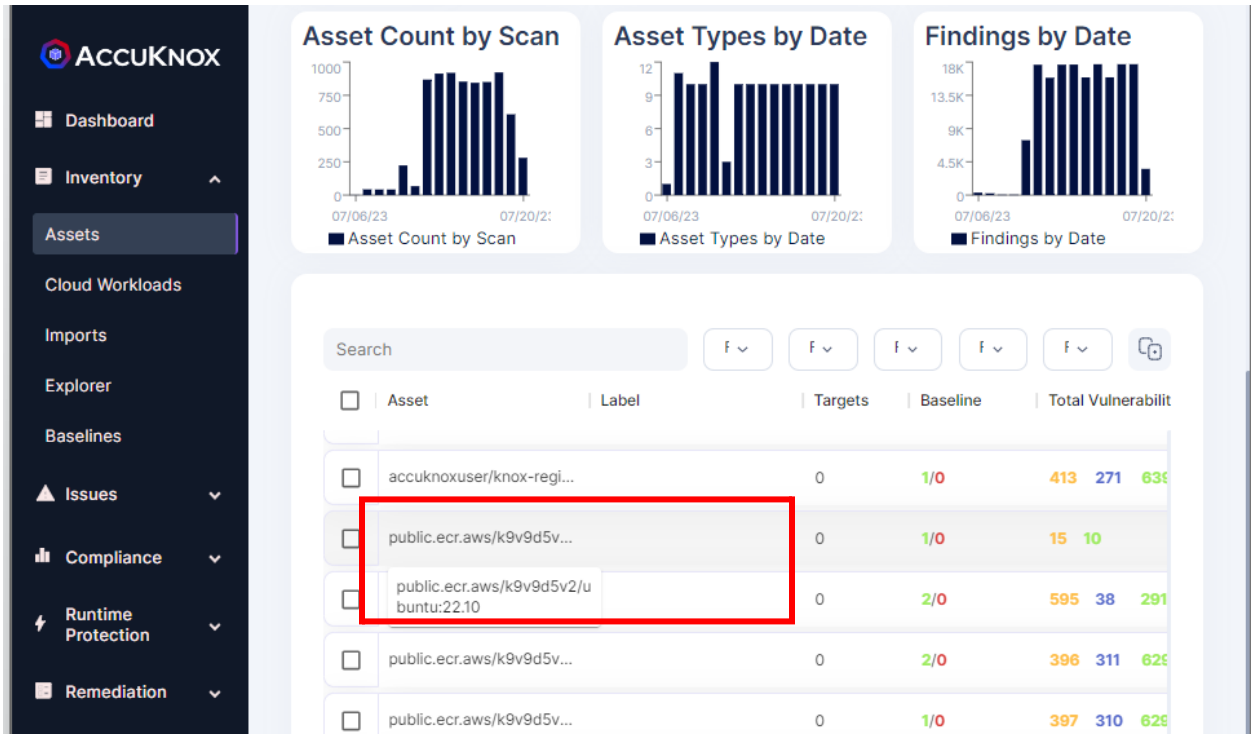


- How to group by criticality and Status

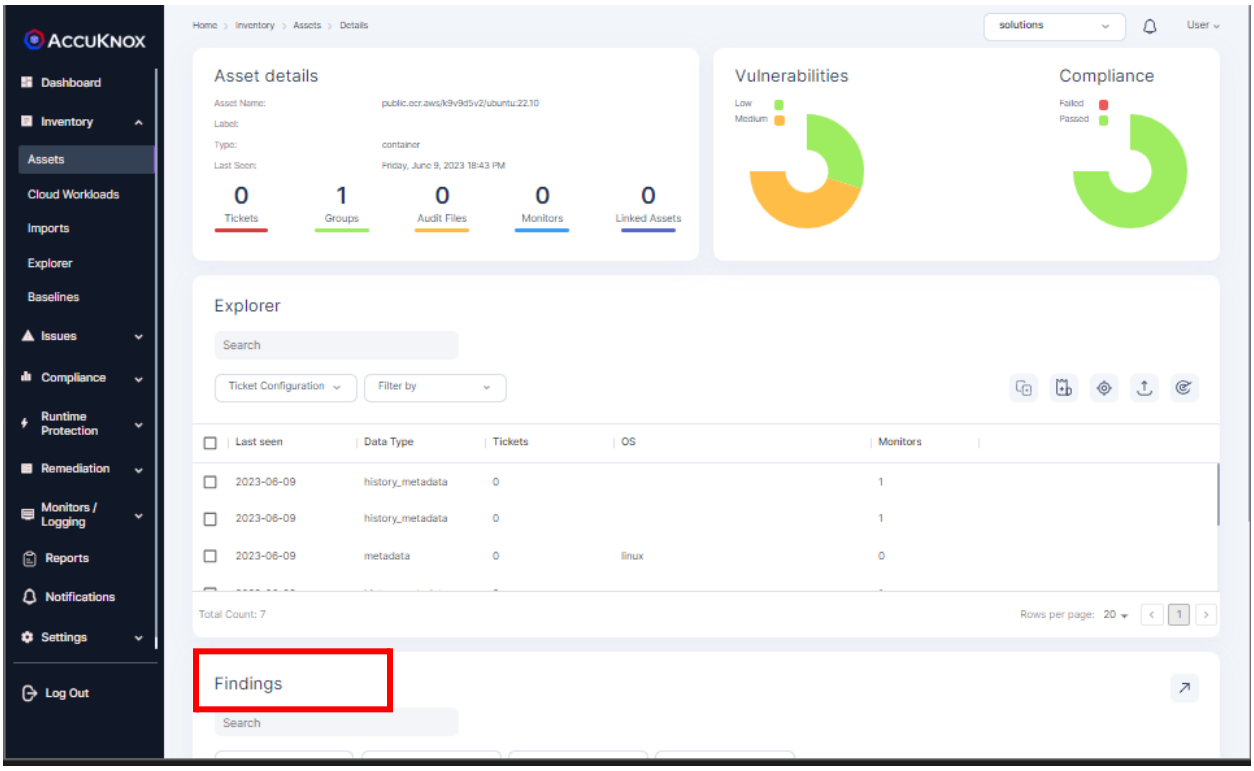
1. Goto ***Inventory*** tab, click on ***Assets*** section



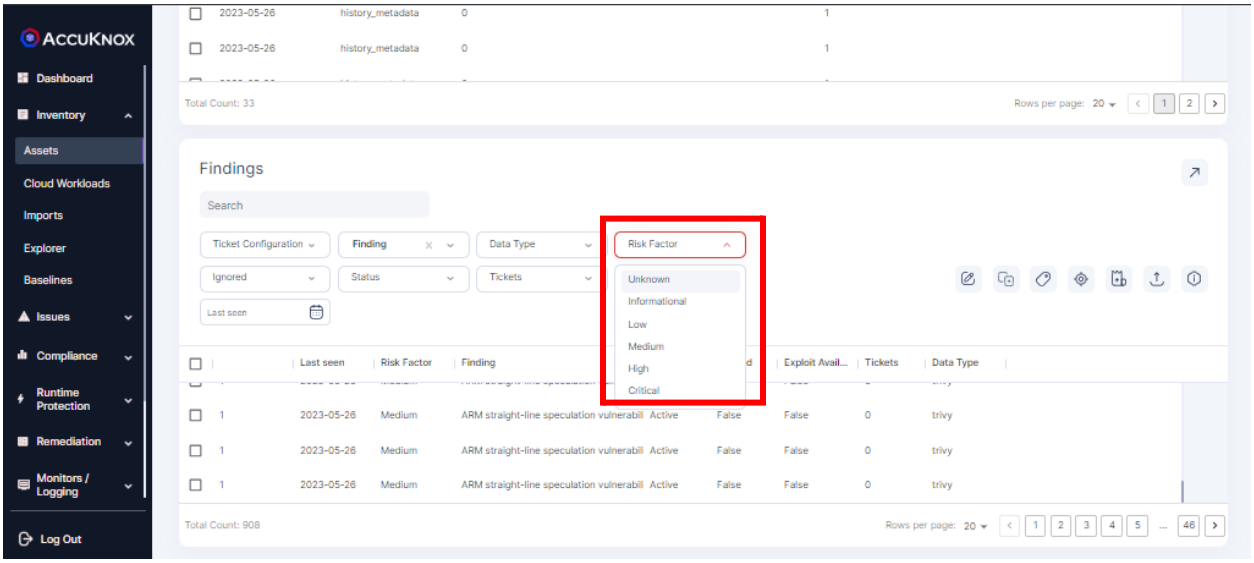
2. Scroll down and click on the particular asset for which misconfiguration need to be viewed



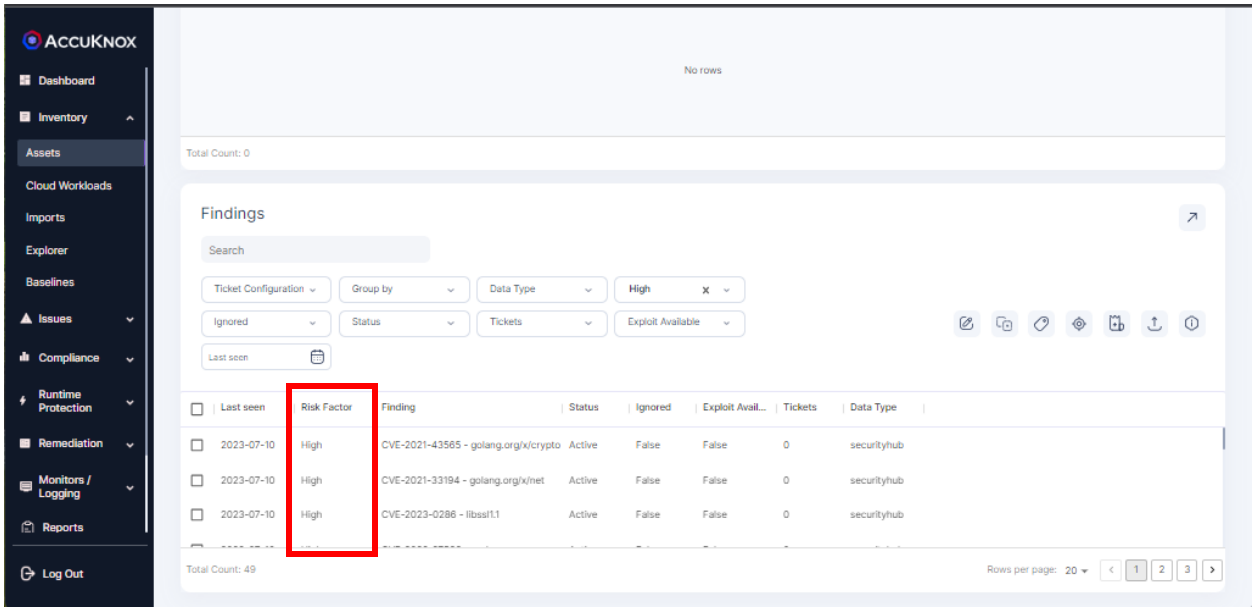
3. You will land on the page as shown below. Scroll down and navigate to ***Findings*** sections.



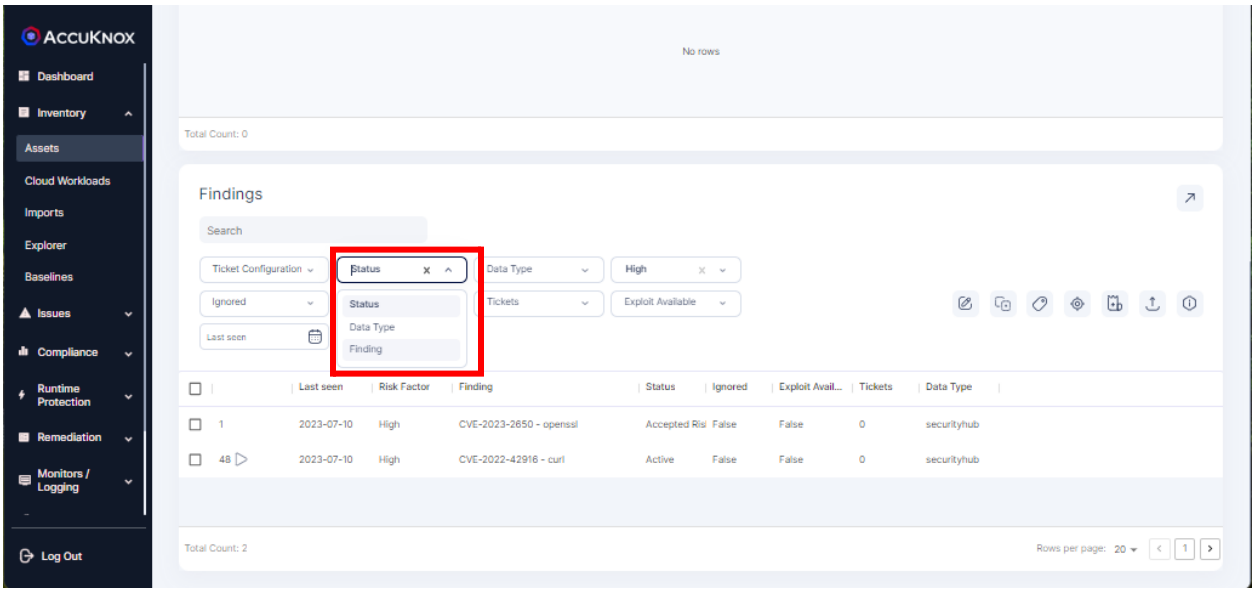
4. Navigate to the ***Risk Factor*** filter, and choose the severity level.



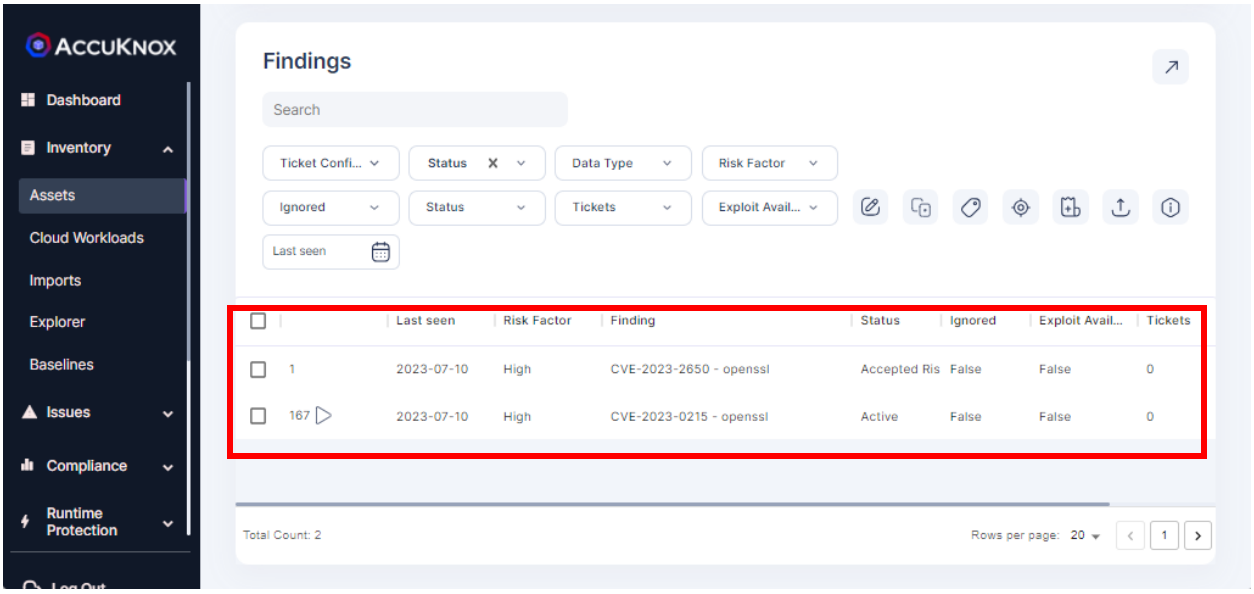
Now, you can find the findings as per the criticality level as shown below



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

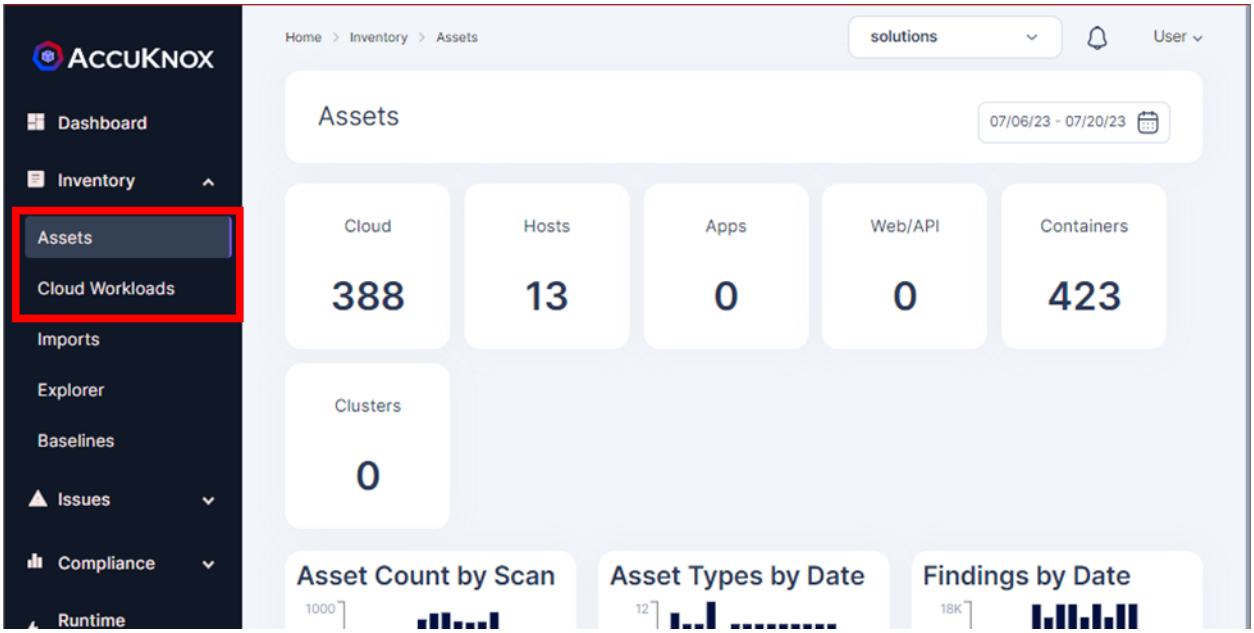


Now, you can view the findings grouped by the status, such as active and accepted risk

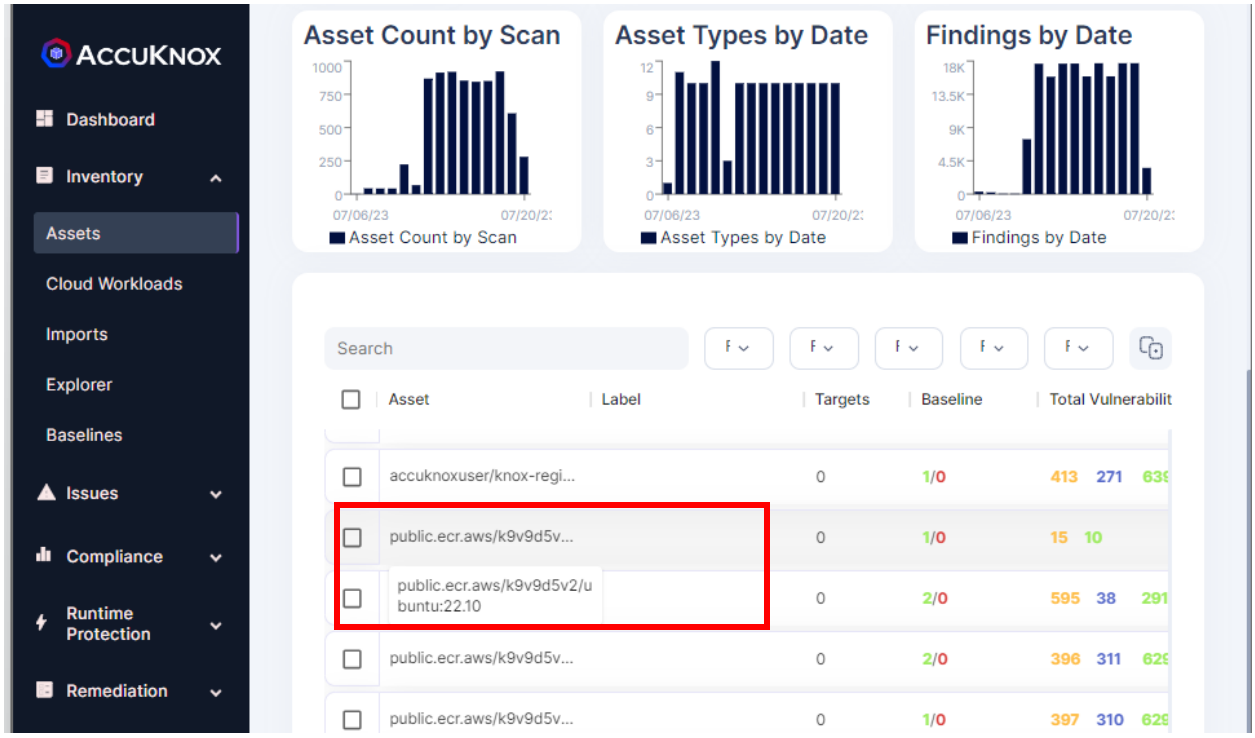


- How to create a ticket

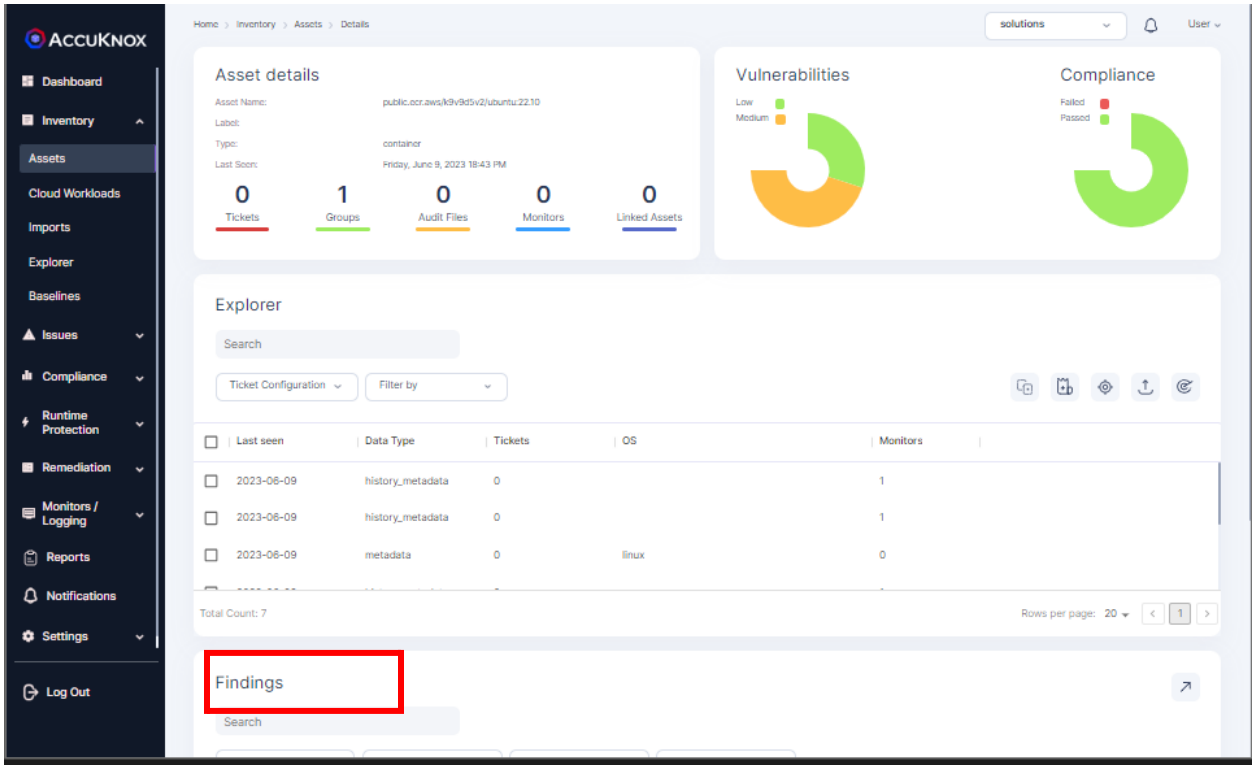
1. Goto ***Inventory*** tab, click on ***Assets*** section



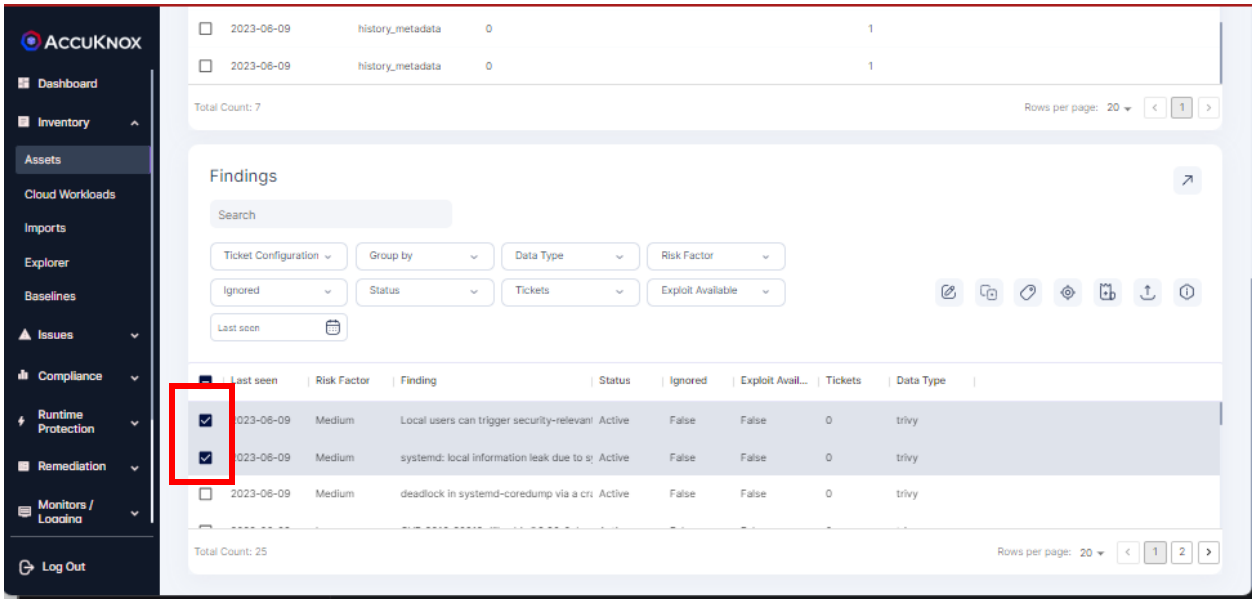
a. Scroll down and click on the particular asset for which misconfiguration need to be viewed



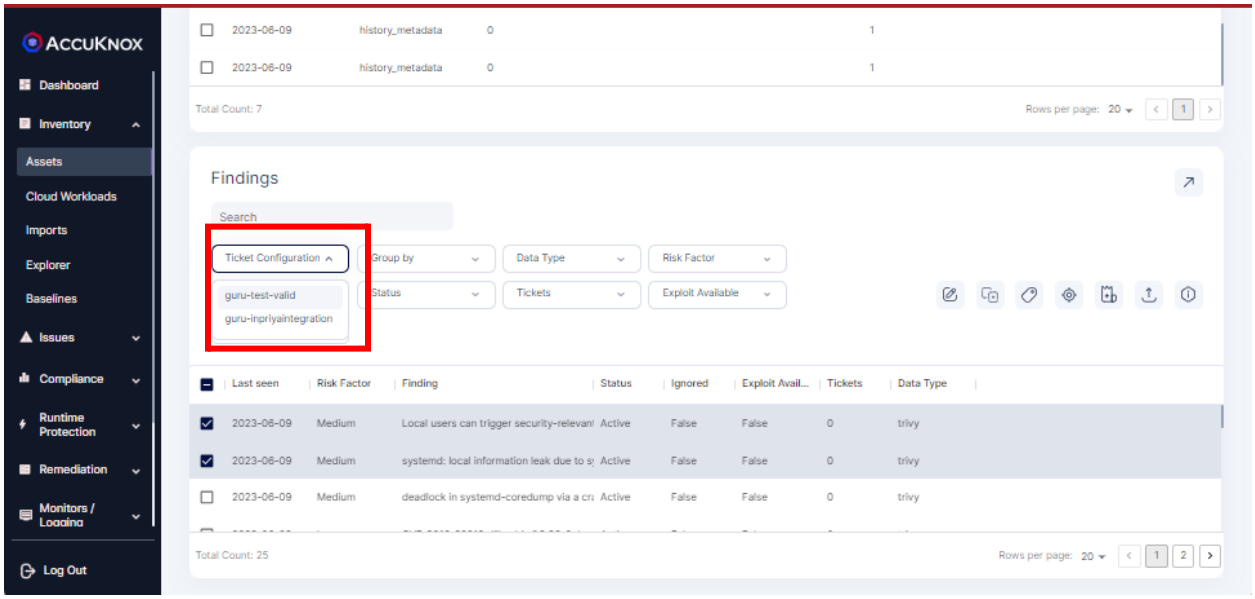
2. You will land on the page as shown below. Scroll down and navigate to ***Findings*** sections.



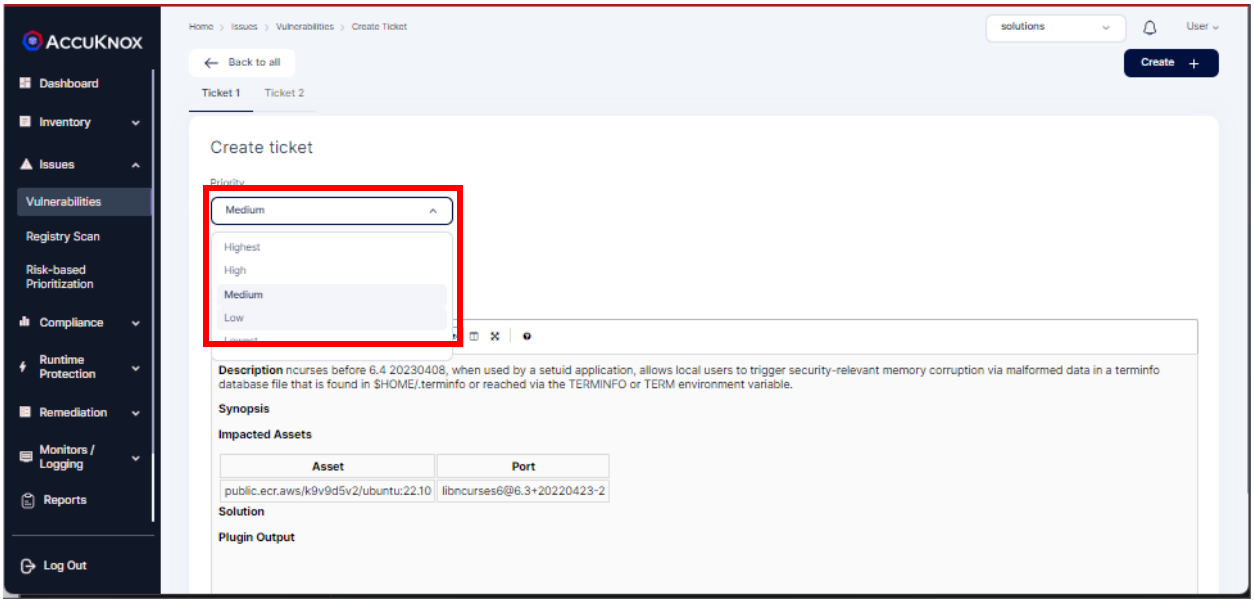
3. Select the check mark behind the ***Findings*** for which ticket needs to be created.



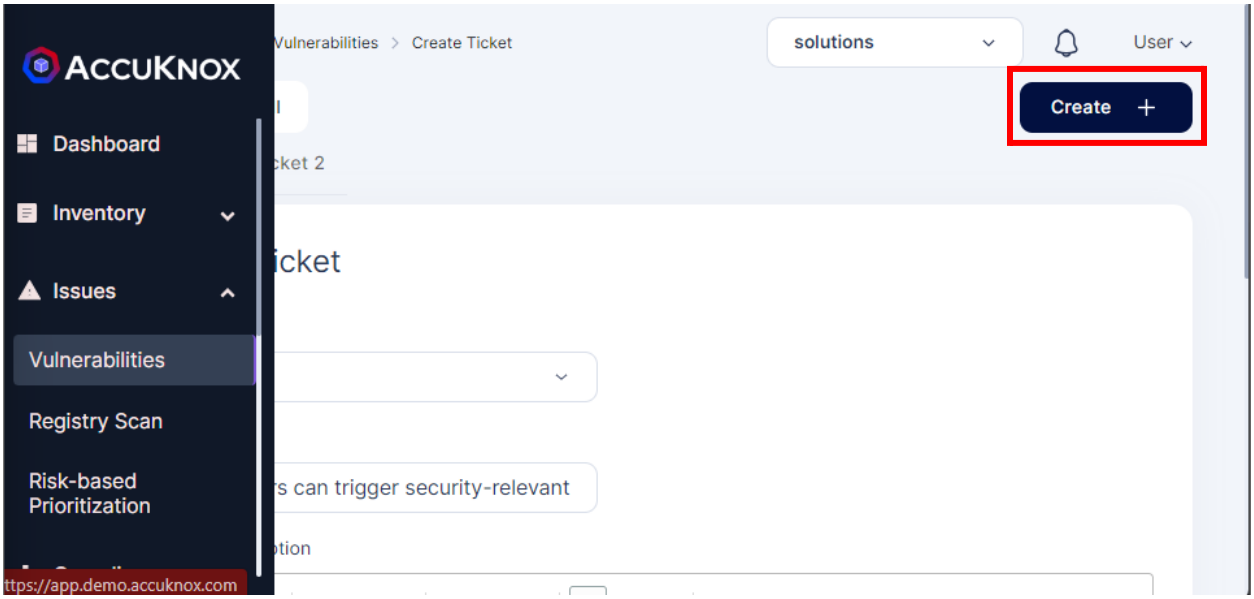
4. Select the desired ticket configuration by which ticket will be created (Create a ticket configuration if it doesn't exist already)



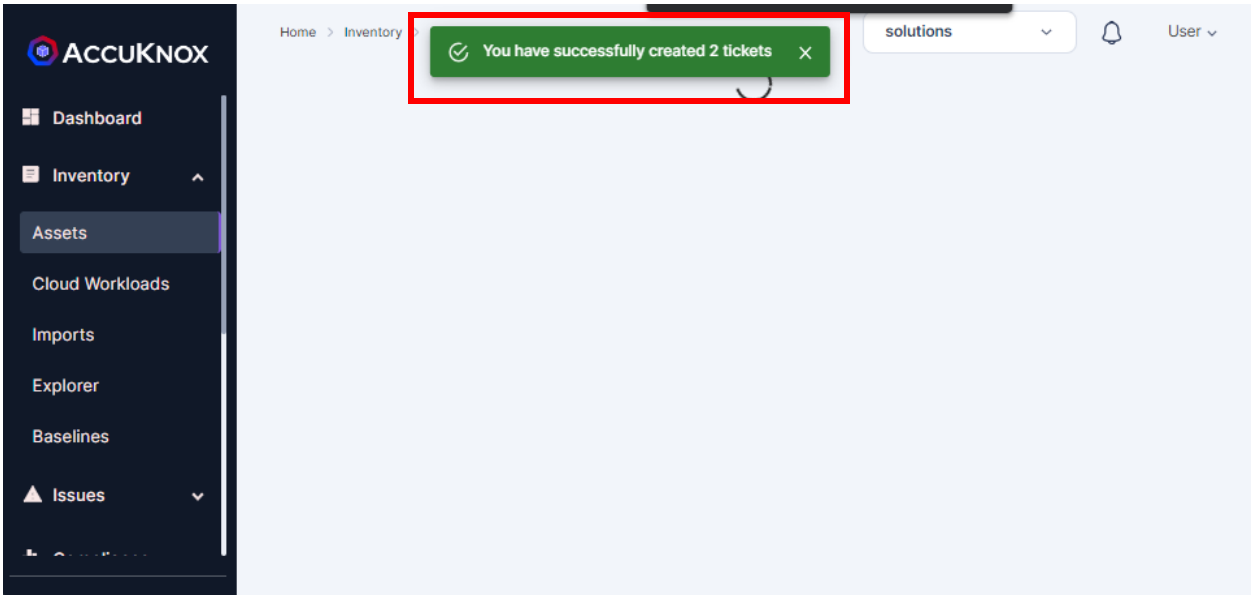
5. Choose the ***Priority*** from the dropdown.



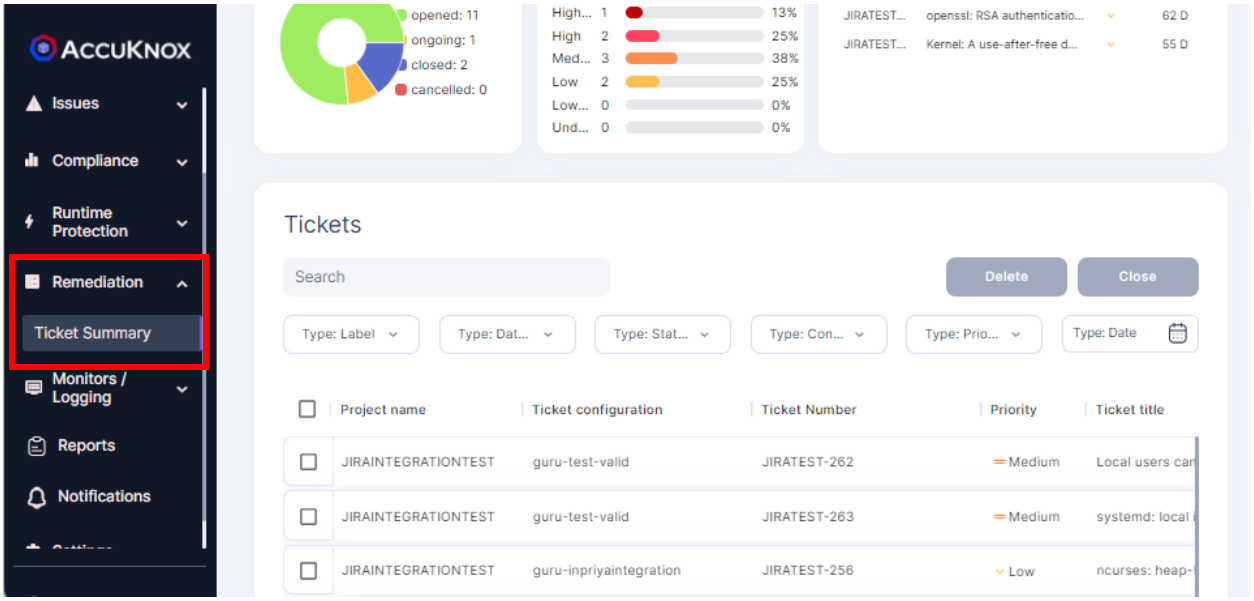
6. Edit the ***Ticket Title*** and ***Ticket Description***, as required.
7. Click on the ***Create*** button at the top right corner.



You can see the tickets were created successfully.



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

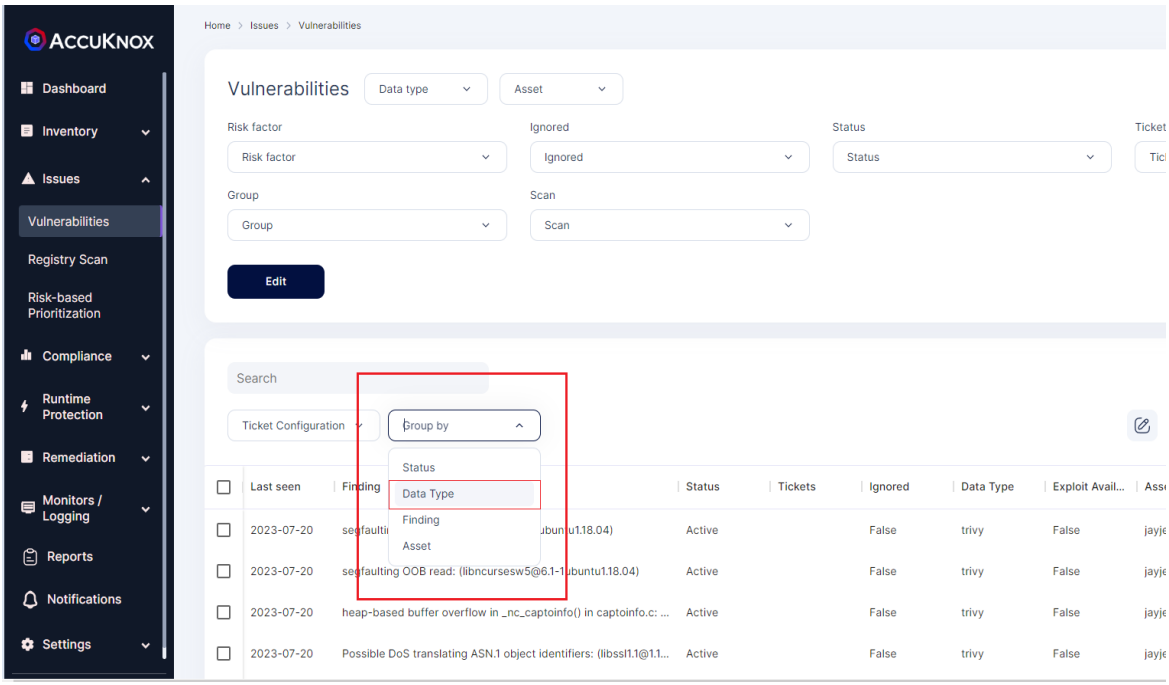


Issues/Vulnerabilities

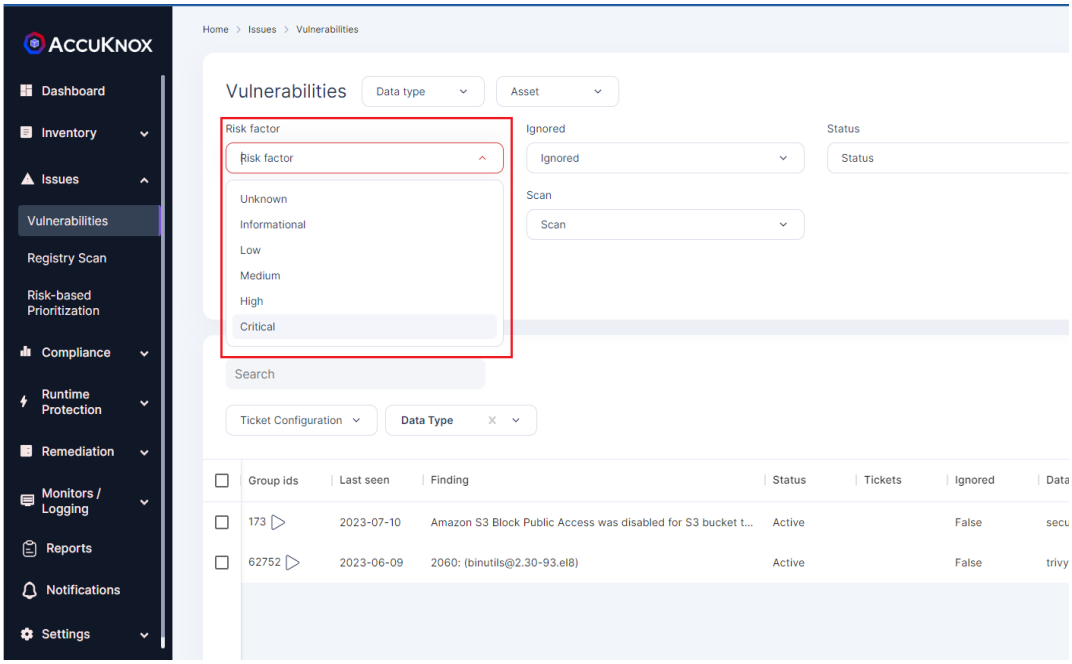
- Group findings by source and severity

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.

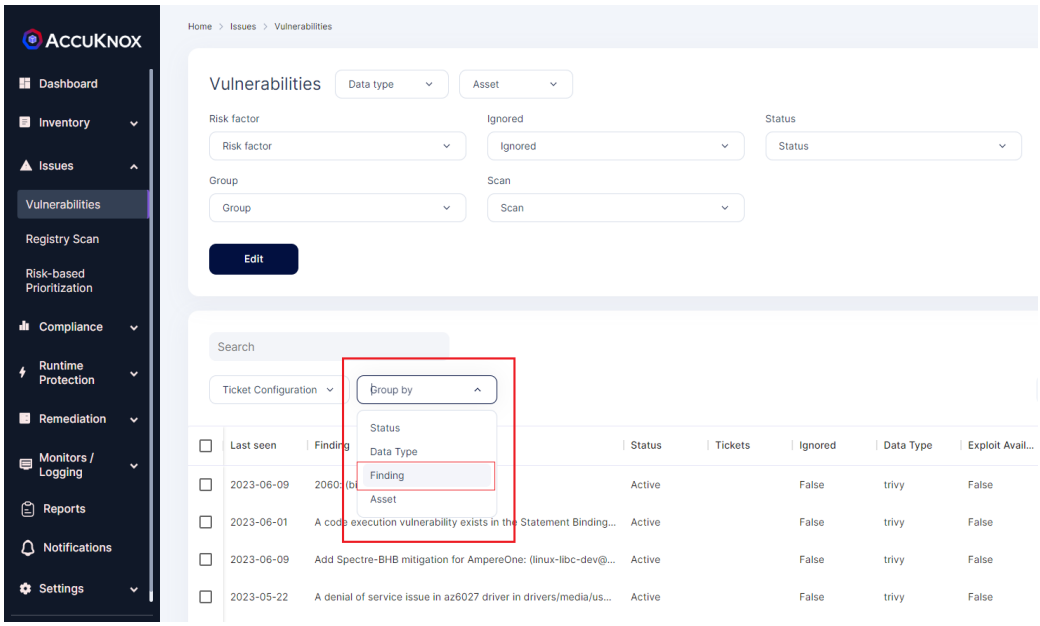


Users can further filter the findings with respect to their Risk factor so that they can have a view of most critical findings from each tool being used.

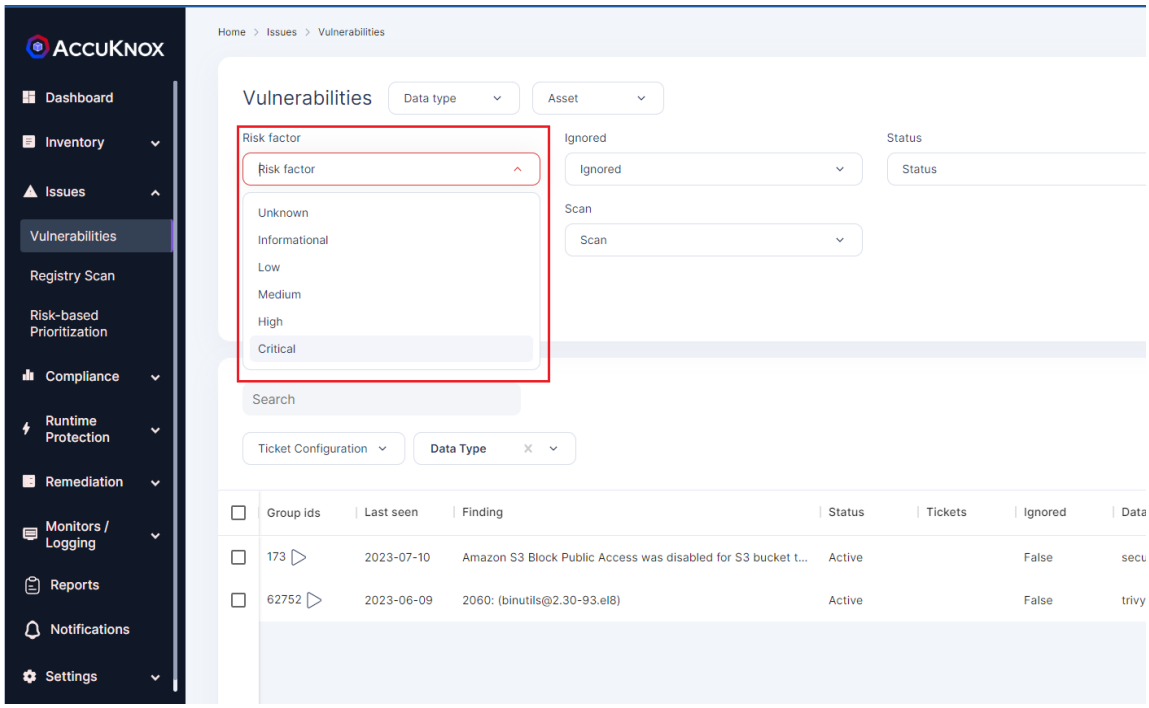


- How to group by Findings and severity

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.

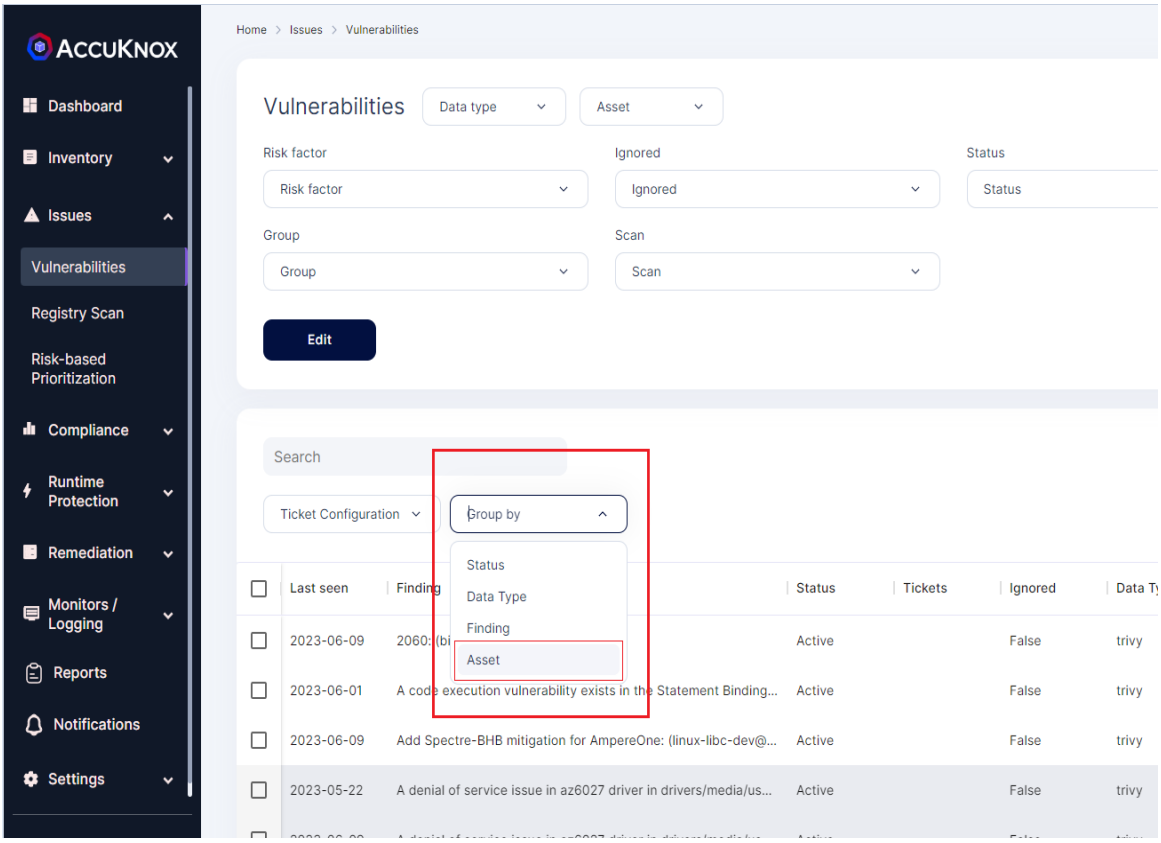


Further users can select the Risk Factor to filter the findings based on their severity. This again narrows the findings that need to be remediated.

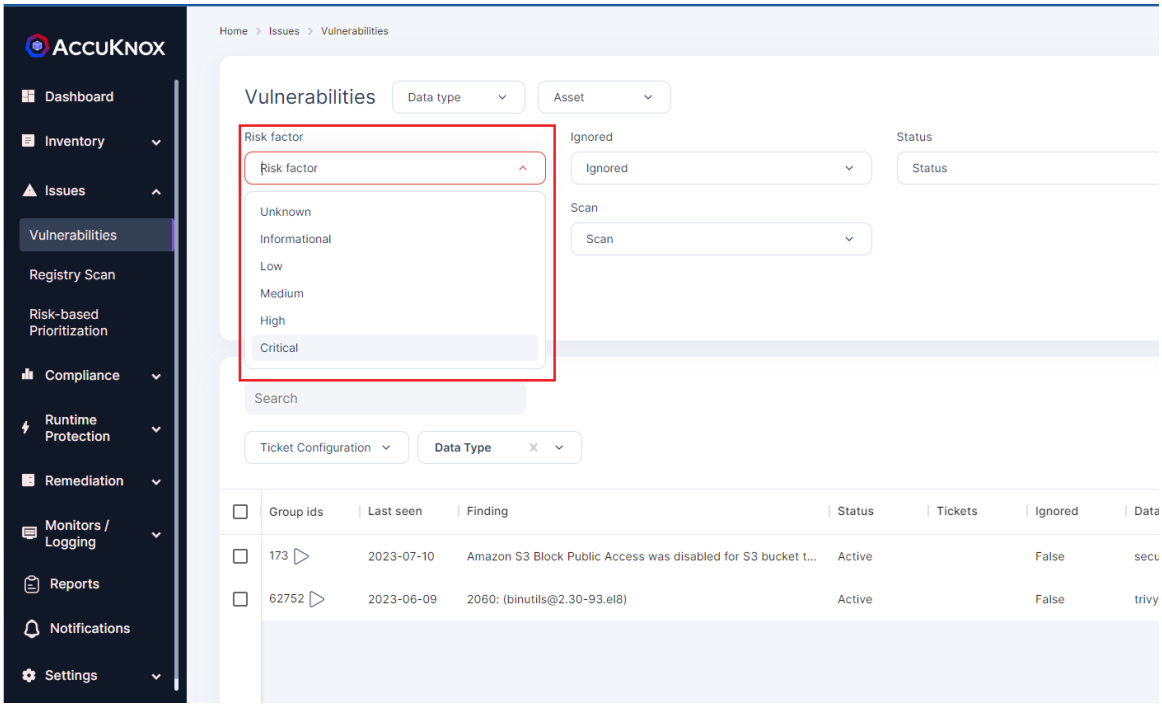


- How to group by Asset and severity

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

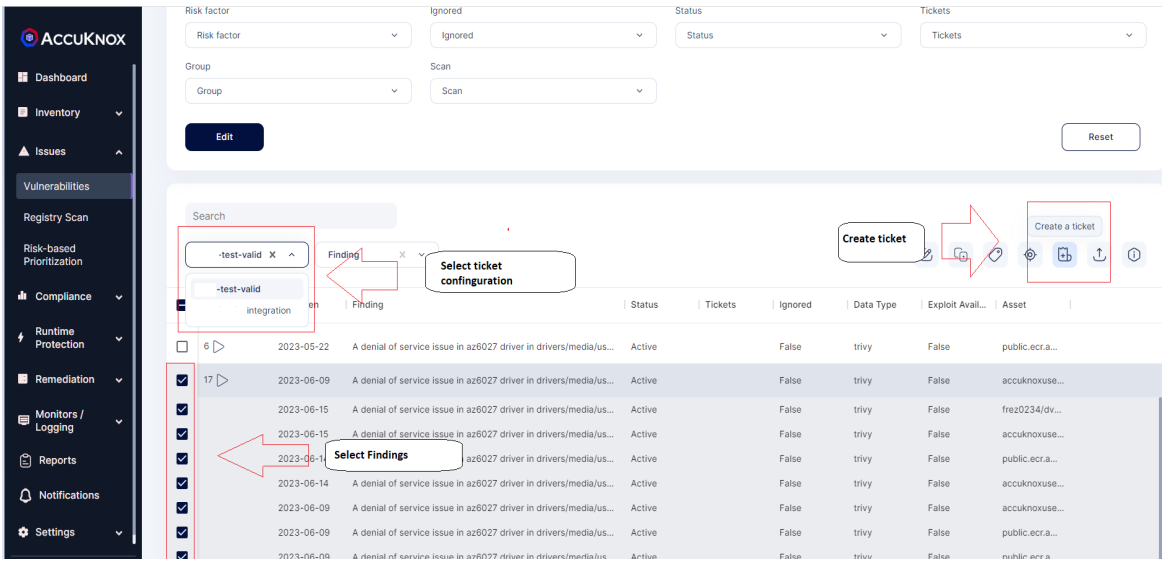


If coupled with the Risk factor filter, users can have a view of the most critical assets ie the assets that has the most no. of critical findings.



- How to create automated tickets in Findings and Asset grouping

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



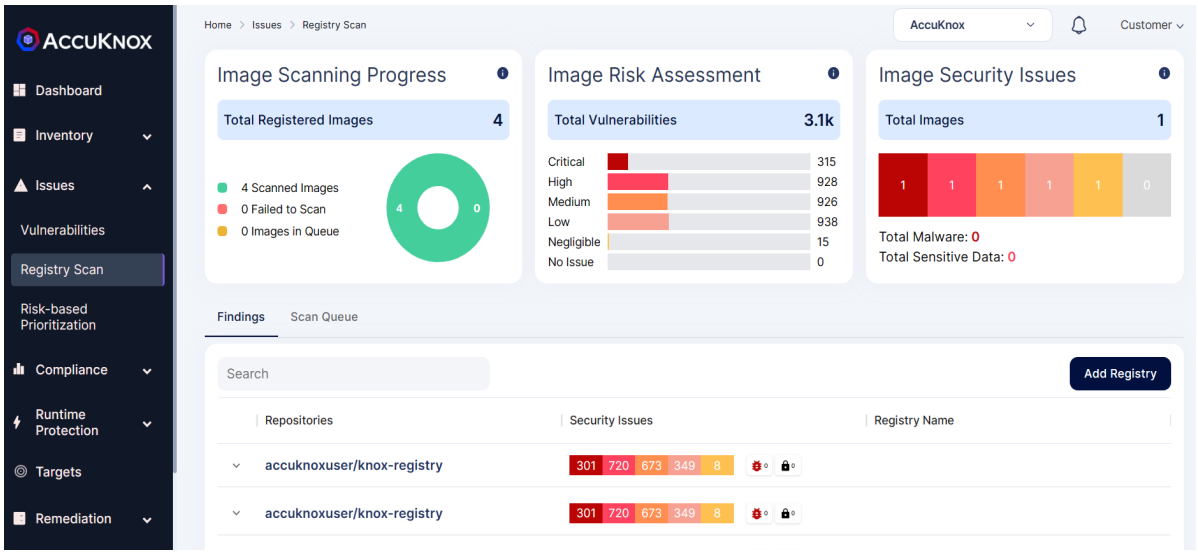
Similarly, the same steps can be followed for creating tickets in asset groupings, click on the desired asset and scroll down to the vulnerabilities section and do the steps.

- How registry scan happens?

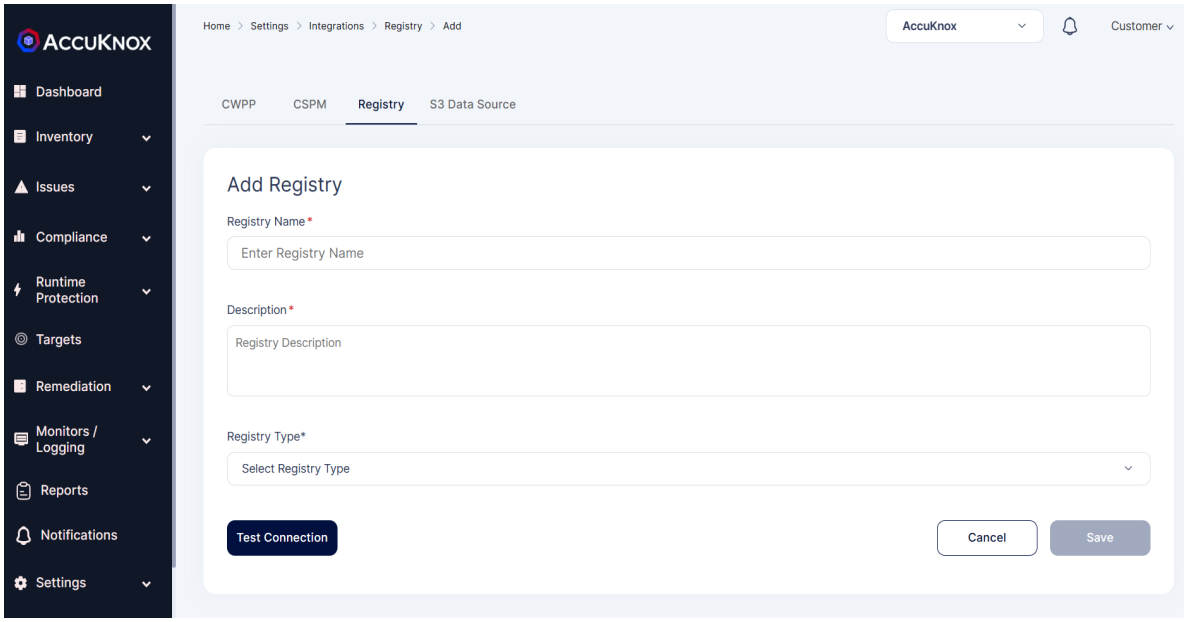
AccuKnox CSPM tool provides with registry scan where the user can onboard their Docker Hub, Nexus, GCR, and ECR registries. Once the registry is onboarded, the scanning of the registry starts automatically in the background. After the scanning is completed, the findings will be populated in the registry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

Registry Onboarding:

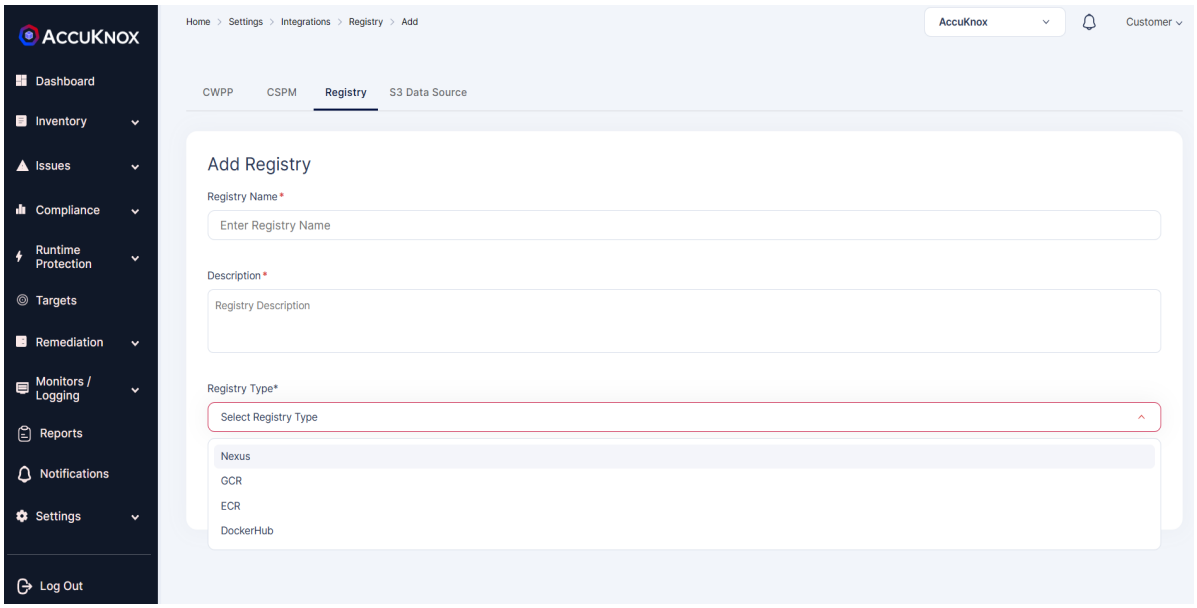
Step 1: To onboard a registry user needs to navigate to Issues->Registry Scan.



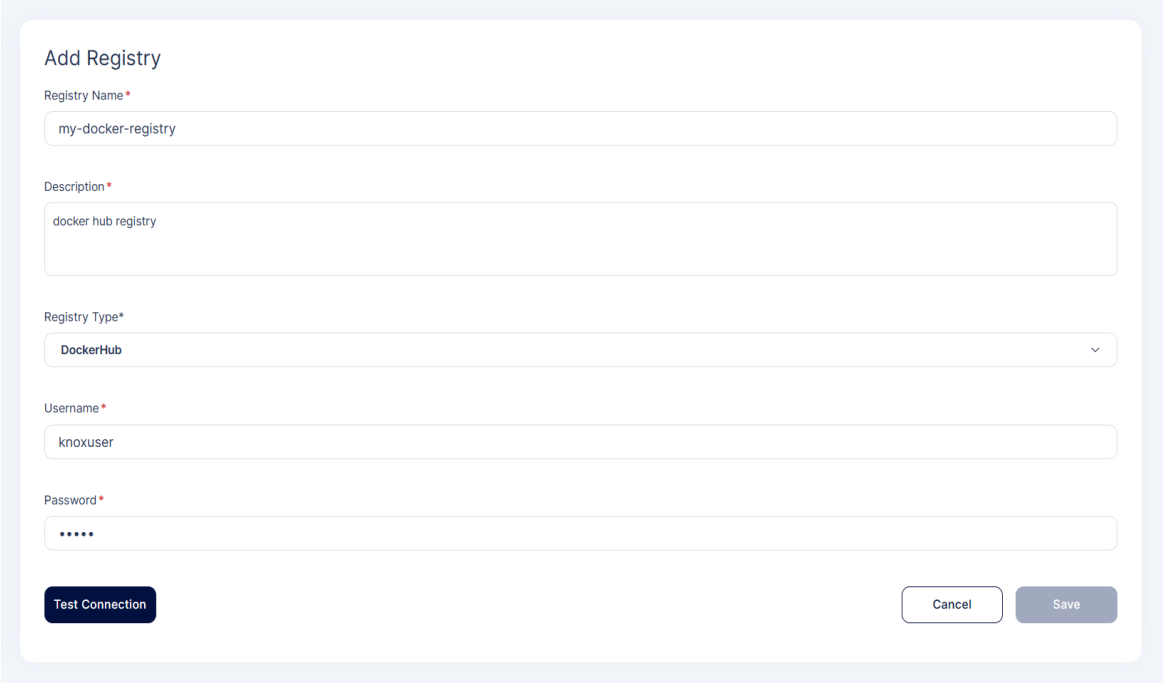
Step 2: The user needs to select Add Registry option from the above screen. When a user clicks Add Registry, they will be directed to a new screen to add registry details.



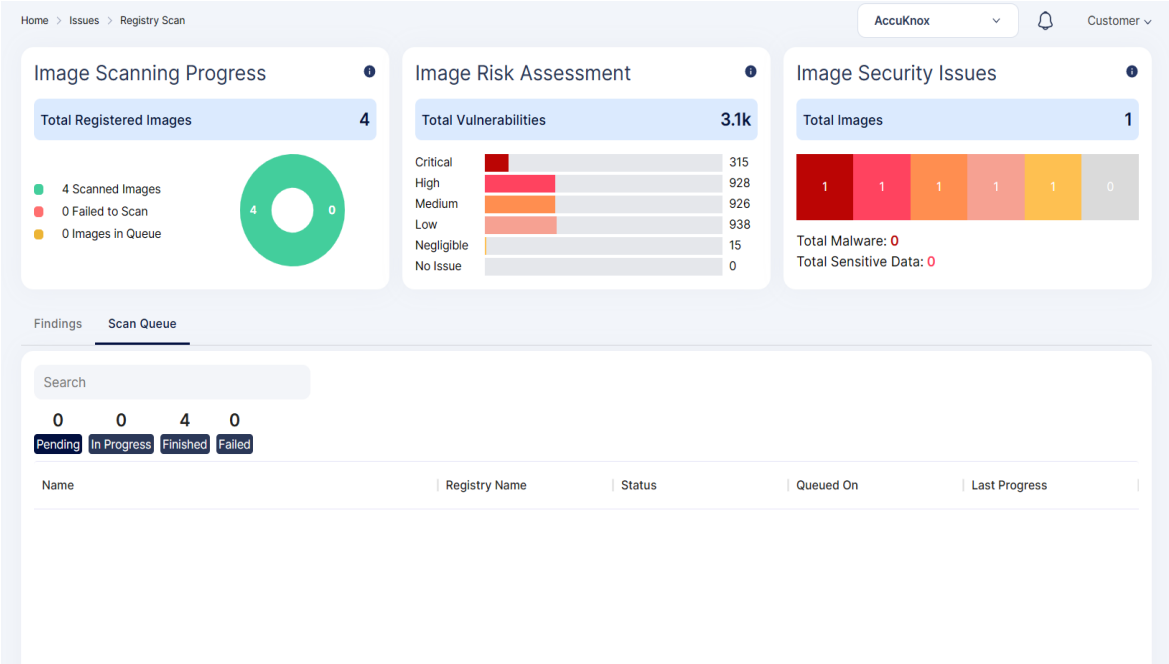
Step 3: User can onboard Nexus, GCR,ECR, DockerHub Registry by giving necessary details.



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

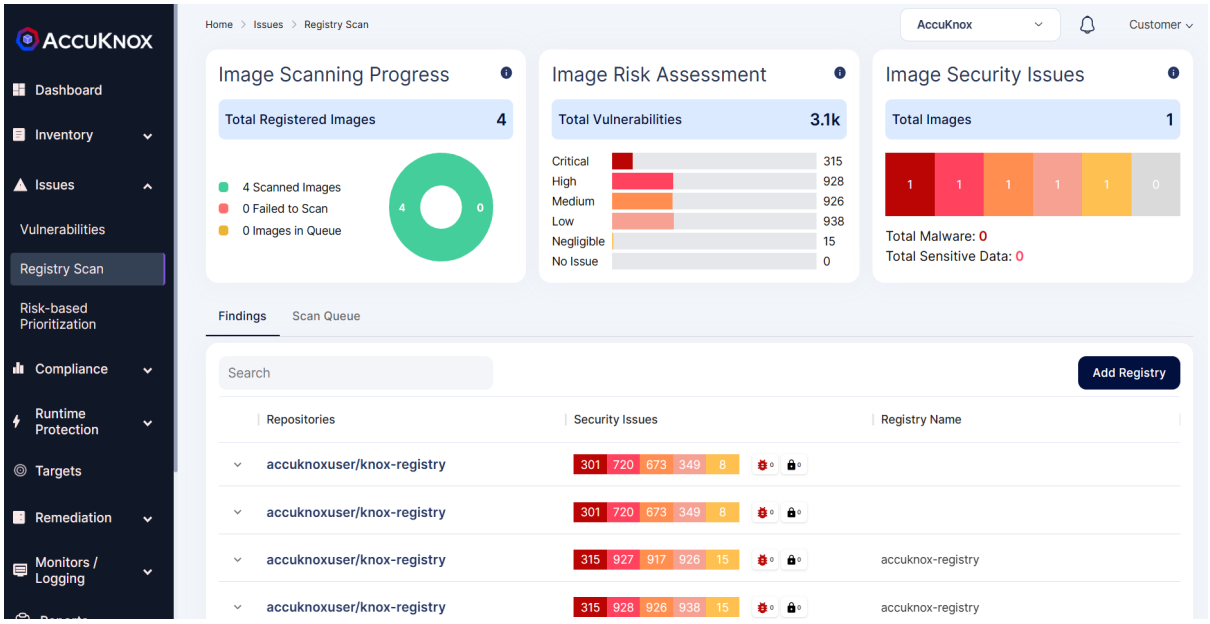


Step 5: Once the user clicks the save option registry will be added and scanning will be done in the background. After the scan is complete the findings data will be populated.



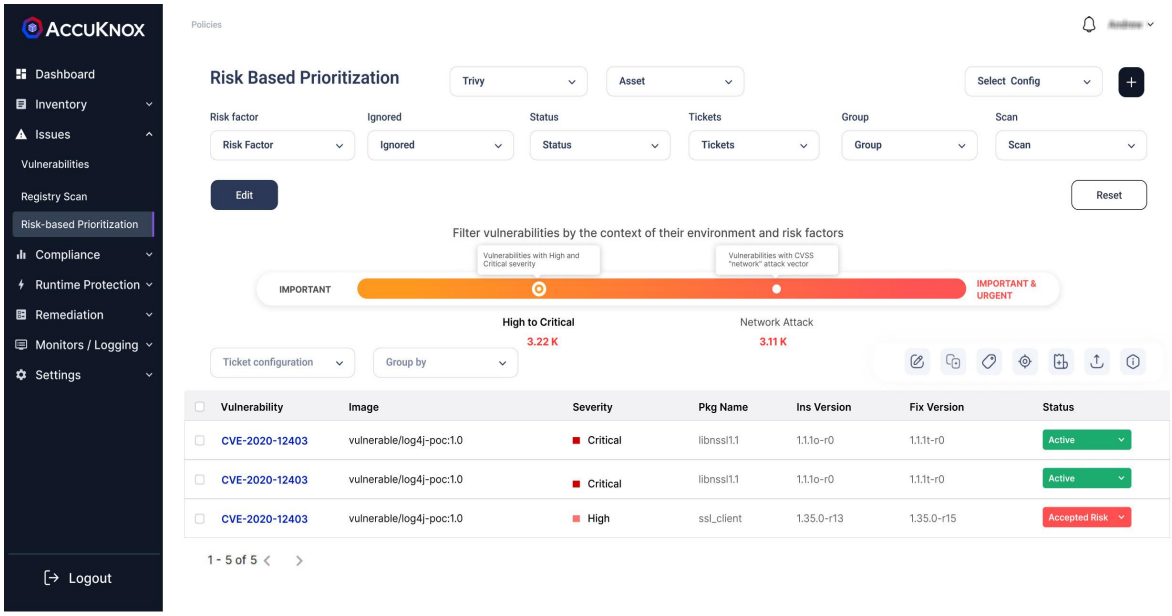
- How to interpret Registry scan results

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

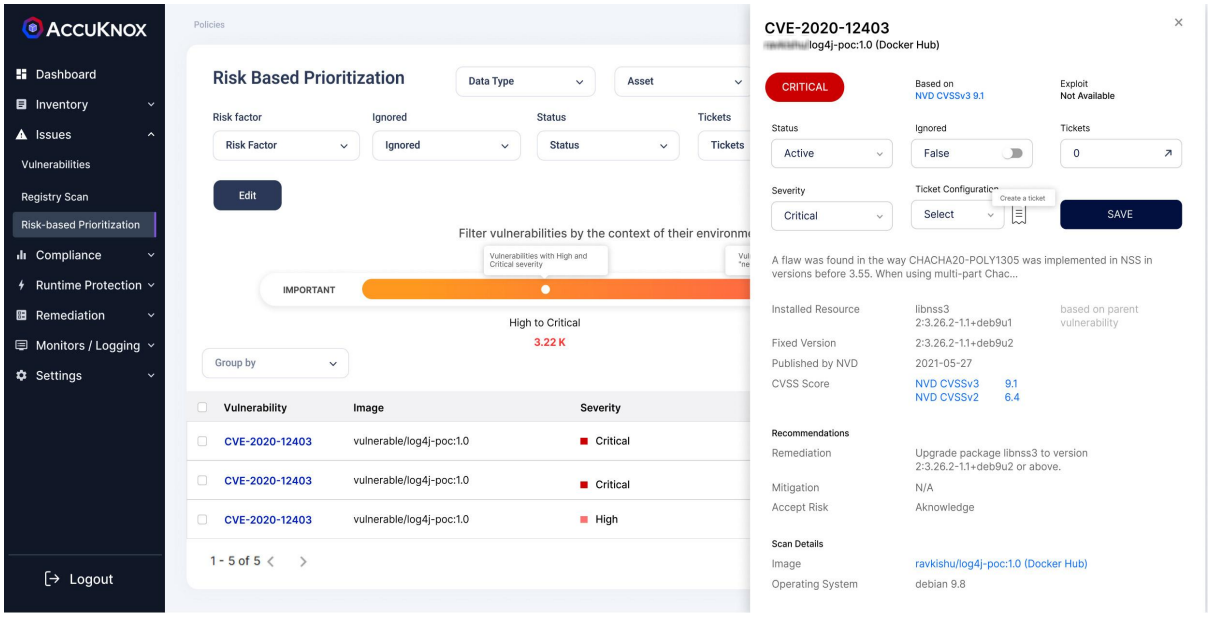


- What is Risk Based Prioritization?

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



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.

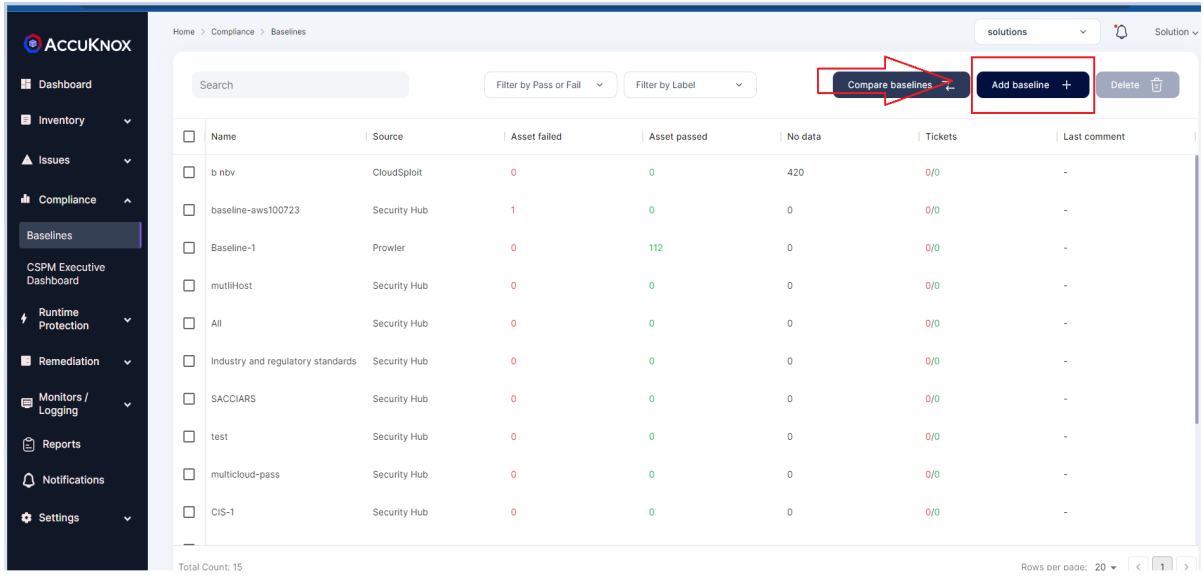


Baseline

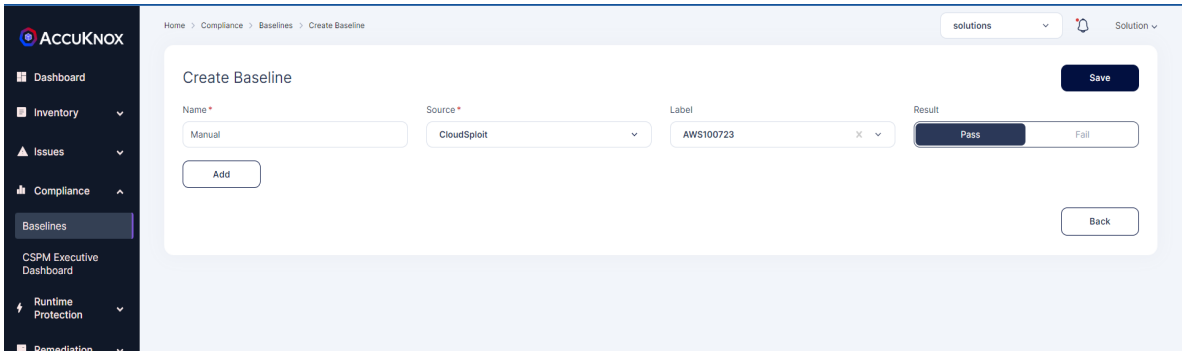
- How to create a Baseline out of a data source

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

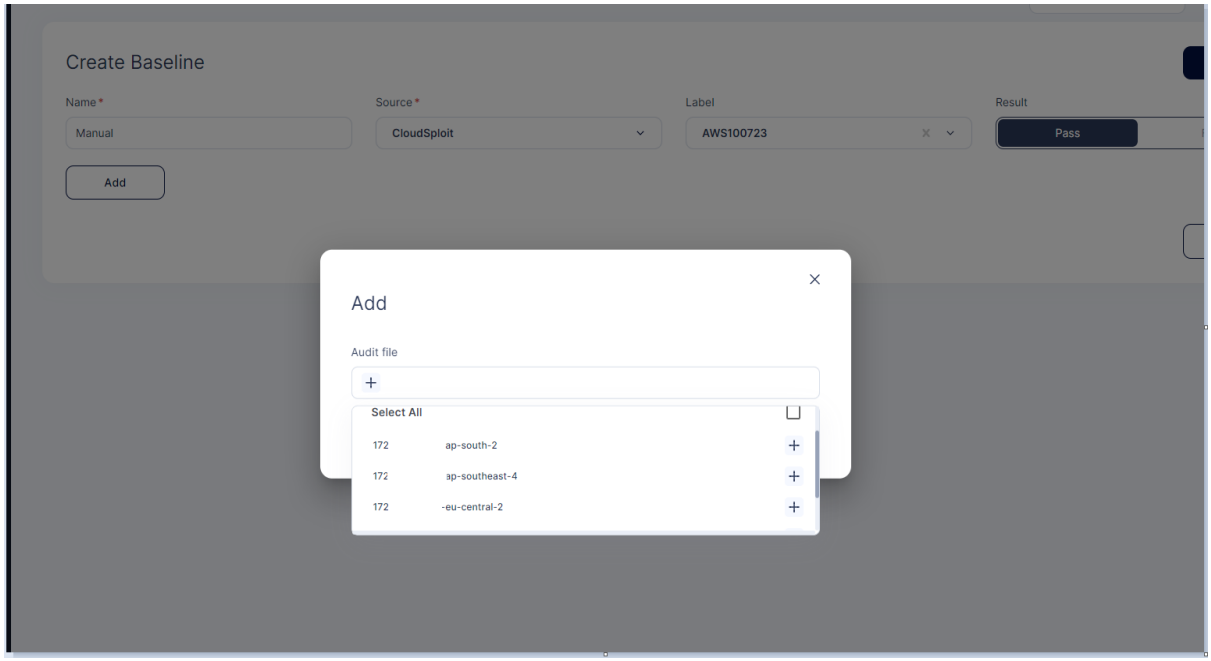
To create a baselines follow these steps:
Step 1: Head to the Baselines page and click on add baseline



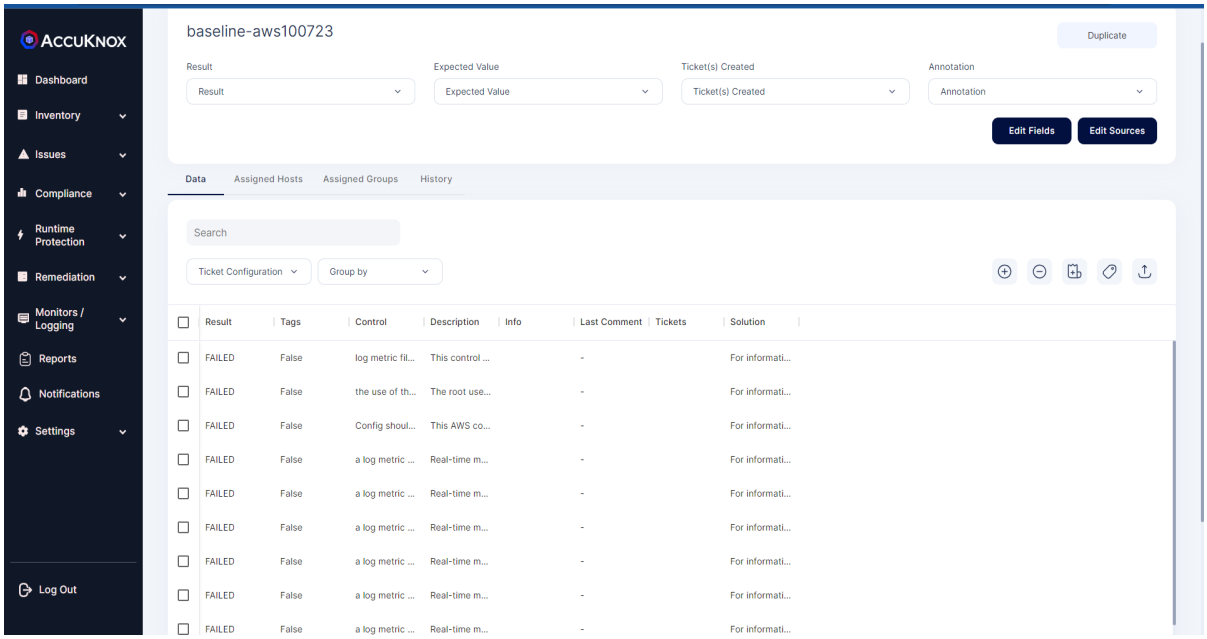
Step 2: Provide a name , select the source and select the bias for your baseline and add a label for your baseline



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



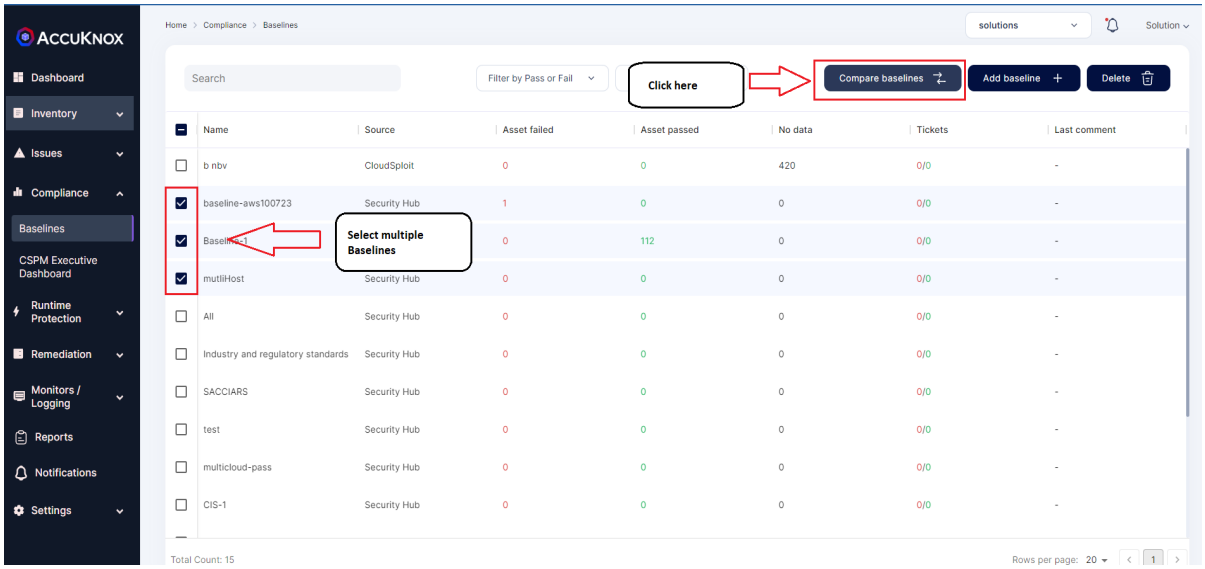
Now you can see the compliance analysis by clicking on the baseline that you created



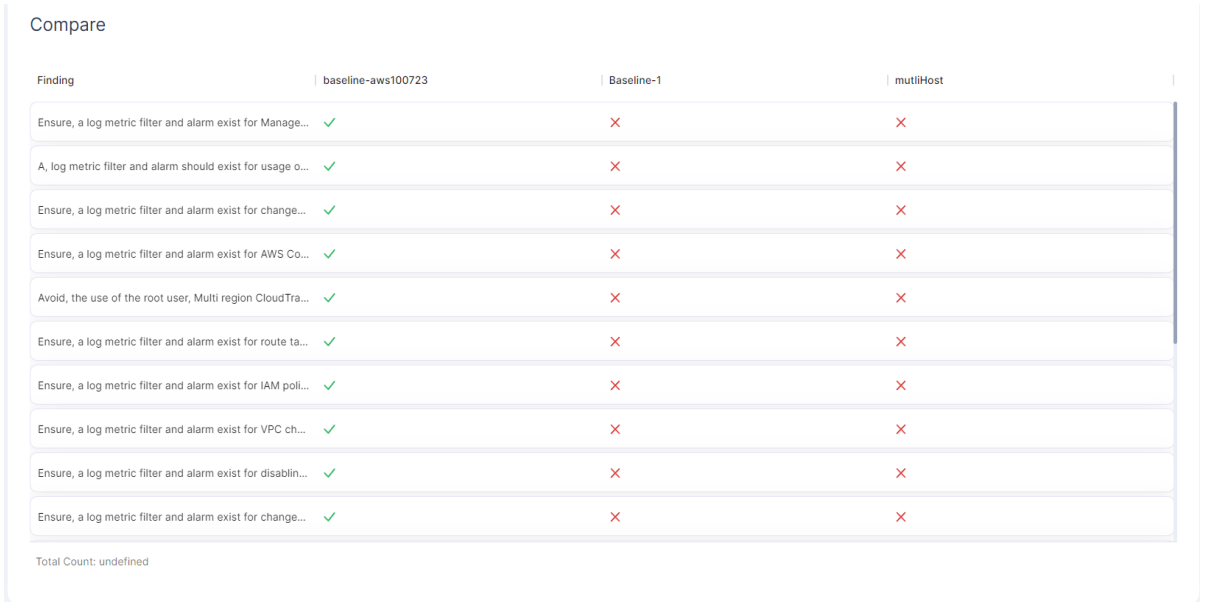
- How to compare 2 baselines

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

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



The comparison will look like following



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

60% Hardening Policies
70% Any Security Policies
40% Namespace with Policies
5% Deployment to workloads

Selected Cluster: eks-prod, eks-dev
Selected Namespace: default

→ Alerts Summary

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

→ Compliance Summary

MITRE	NIST	CIS	PCI-DSS
3	3	0	3

→ Compliance Alerts

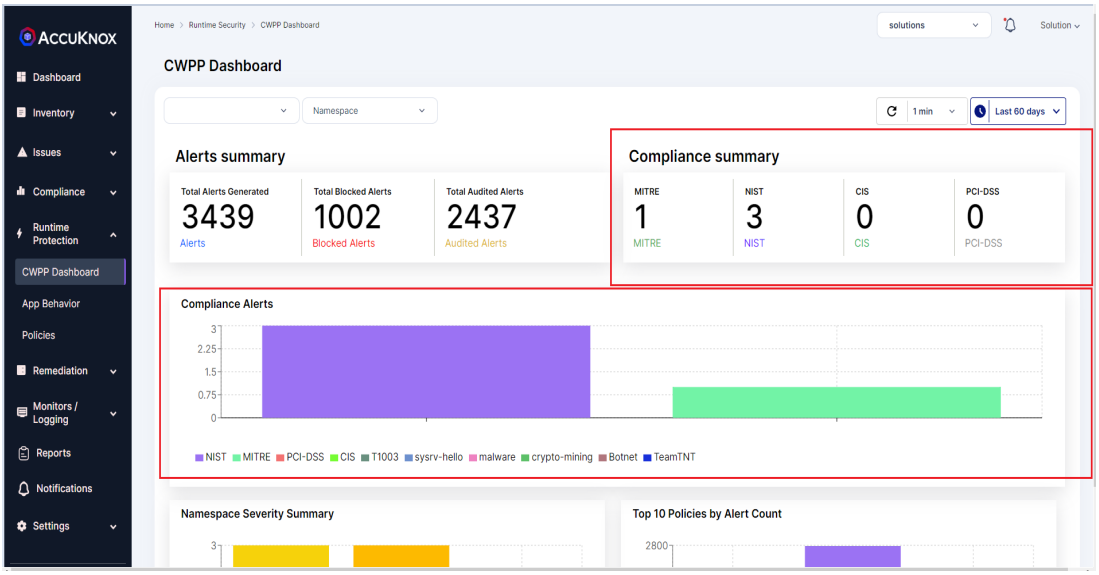
→ Namespace Severity Summary

→ 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.



App Behavior

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

- How to interpret network graph

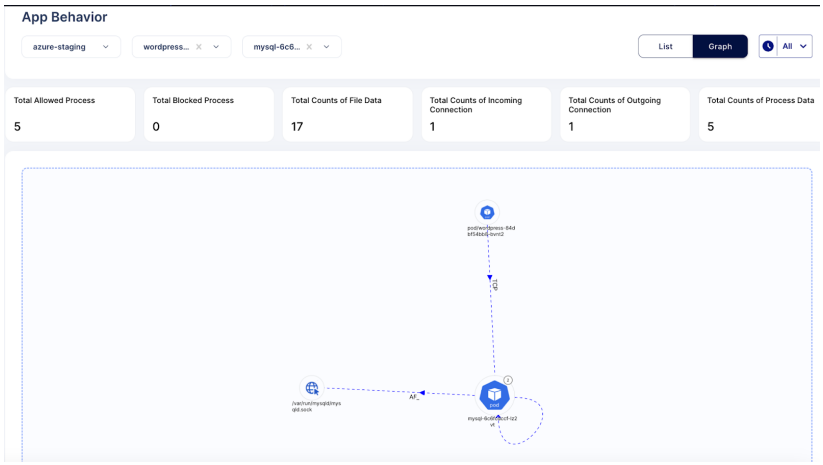
Lets understand this by following use-case example - **Auditing Application Behavior of MySQL application**

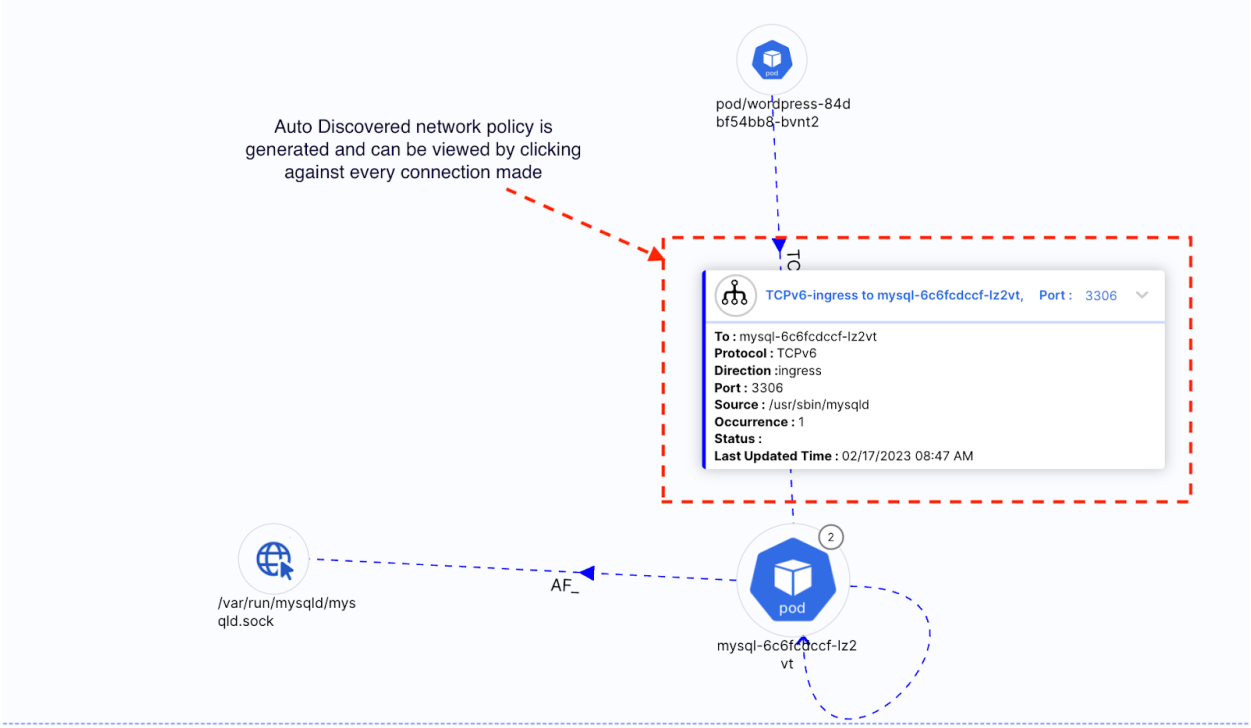
1.Install workload:

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

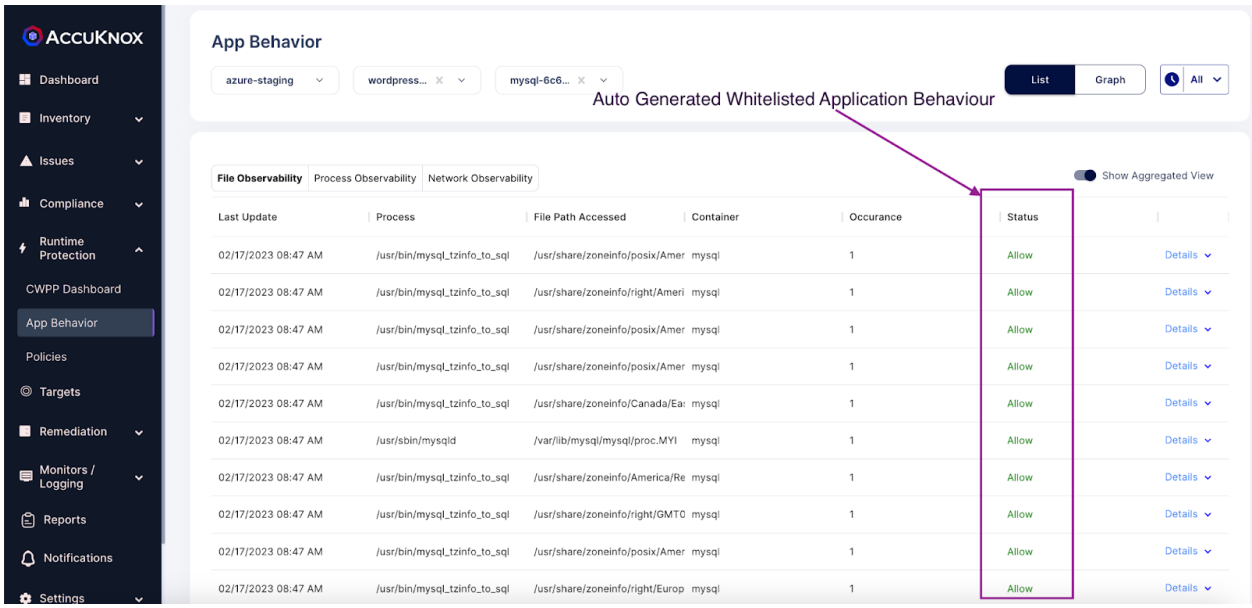
2.Showing App behavior screen in the context of the wordpress-mysql application. To see the Application Behavior user must Navigate to the *Runtime Protection->App Behavior* section. Then click on the Cluster and Namespace and pod from the filters to see the Application Behavior.

- 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.

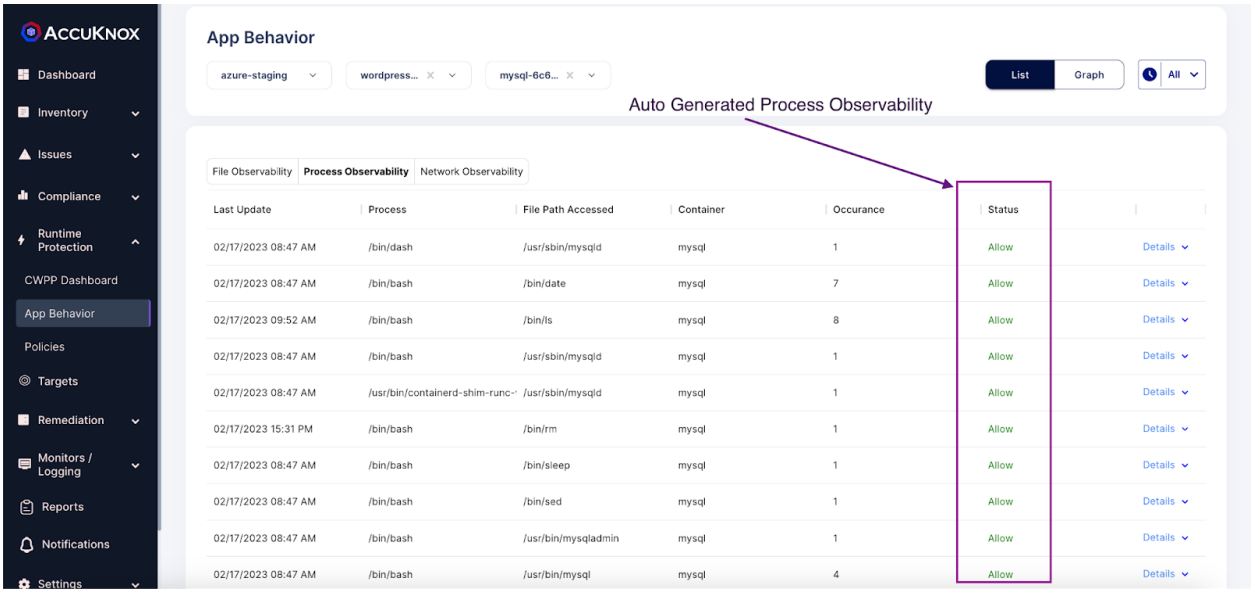




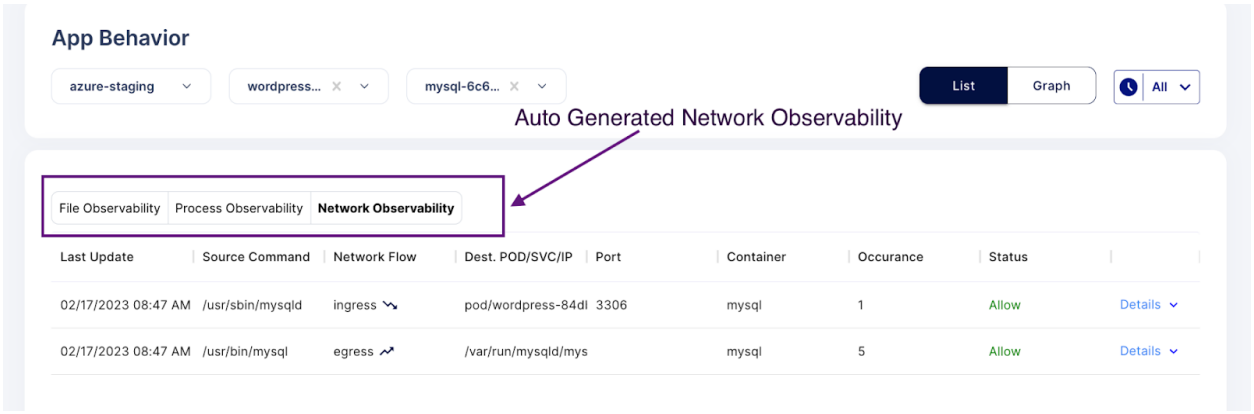
- File Observability: This view gives details about the files that are getting accessed in the pod.



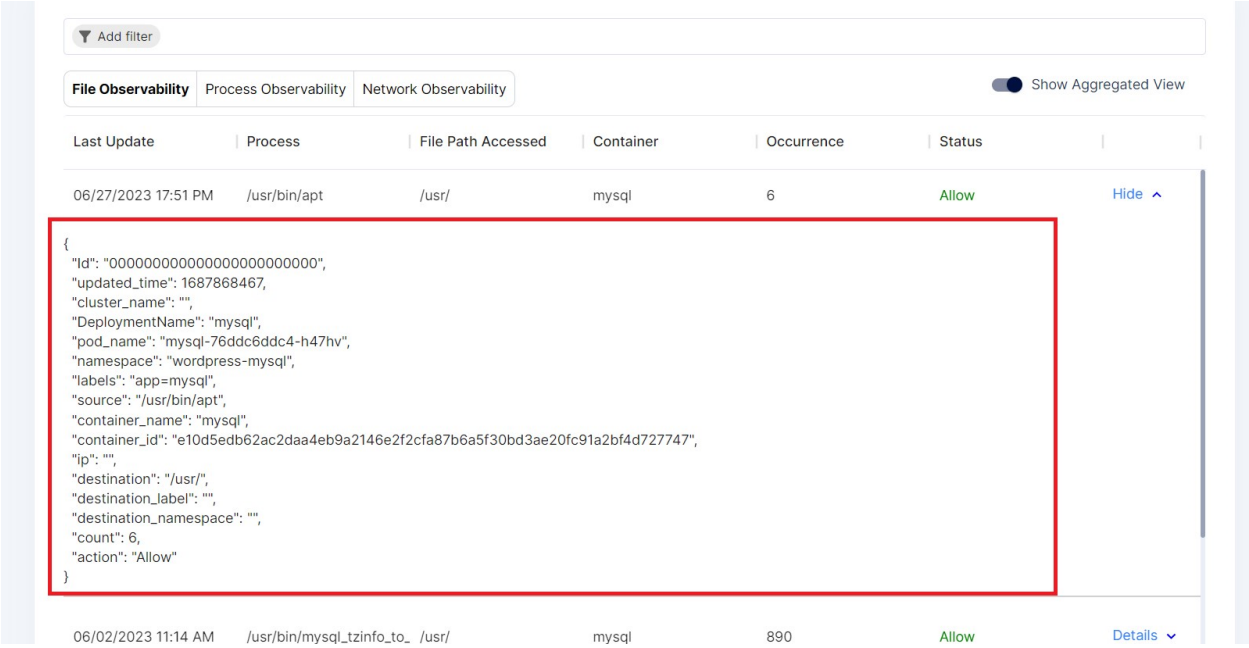
- Process Observability: This view gives the details of Processes that are currently running in the Pod.



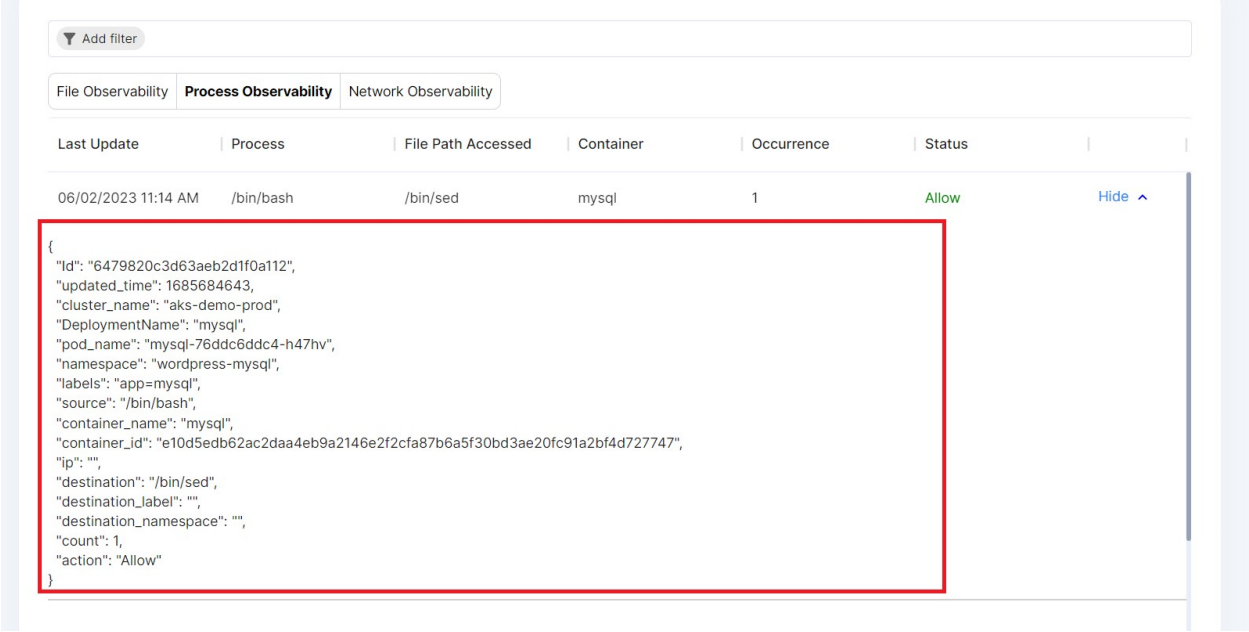
- Network Observability: The network observability can also be seen in the list here you can see the details of ingress and egress traffic in the list view.



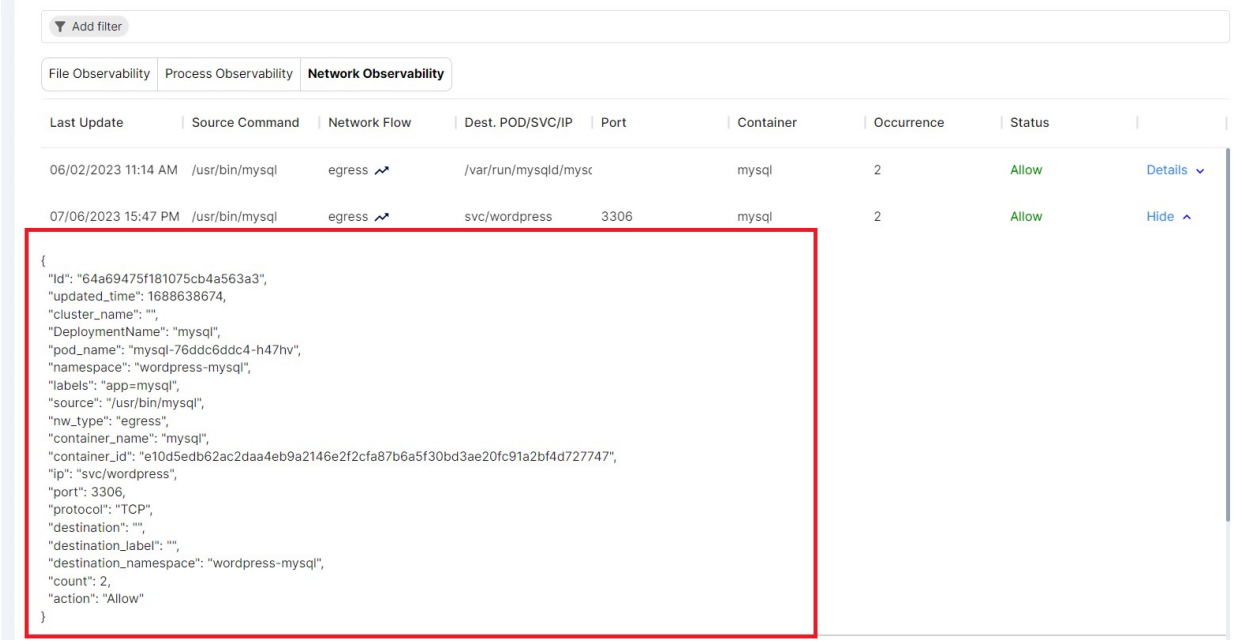
- How to see App Behavior Telemetry
  - To see the contextual information about the File and Network and Process observability user needs to navigate to the *Runtime Protection->App Behavior* Section.
  - **File Observability Telemetry:** To see the file observability related telemetry user needs to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



- **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



- **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

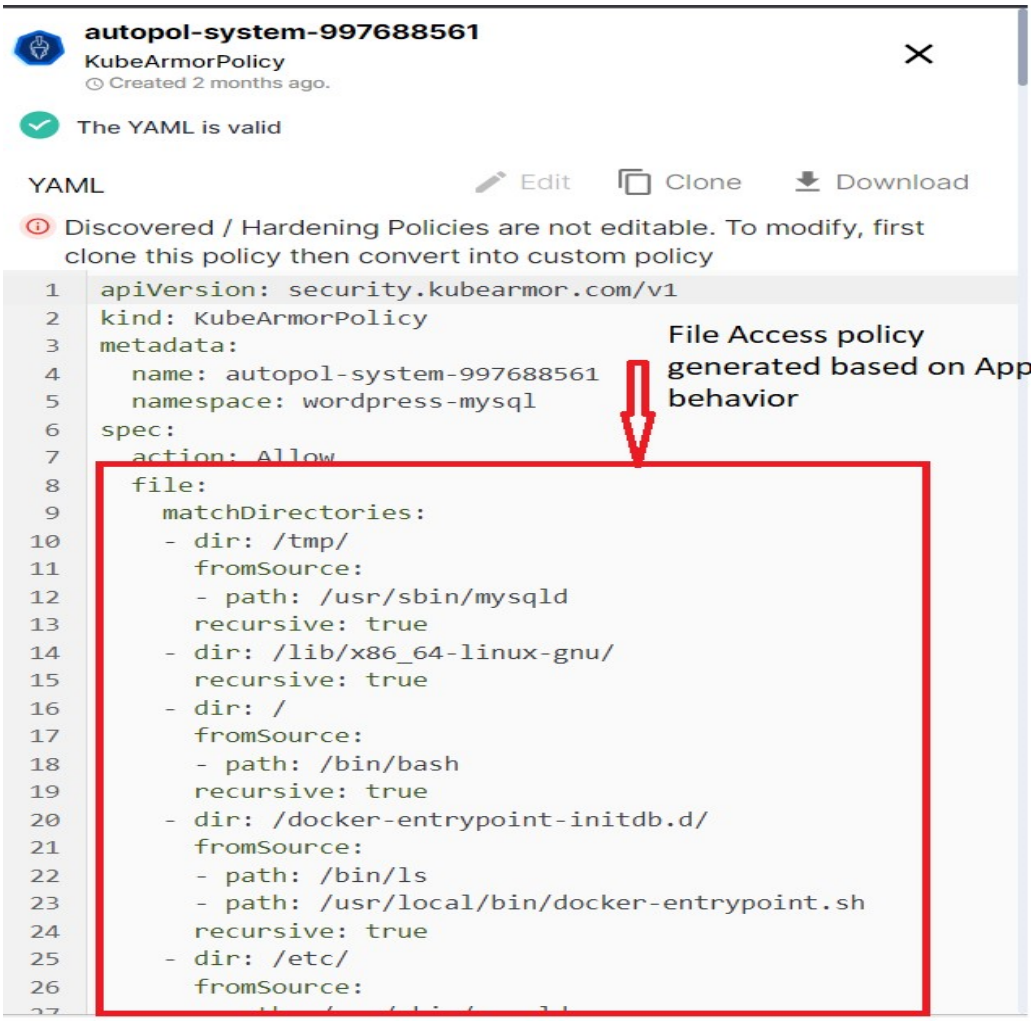


Runtime Protection w/ Policy Management

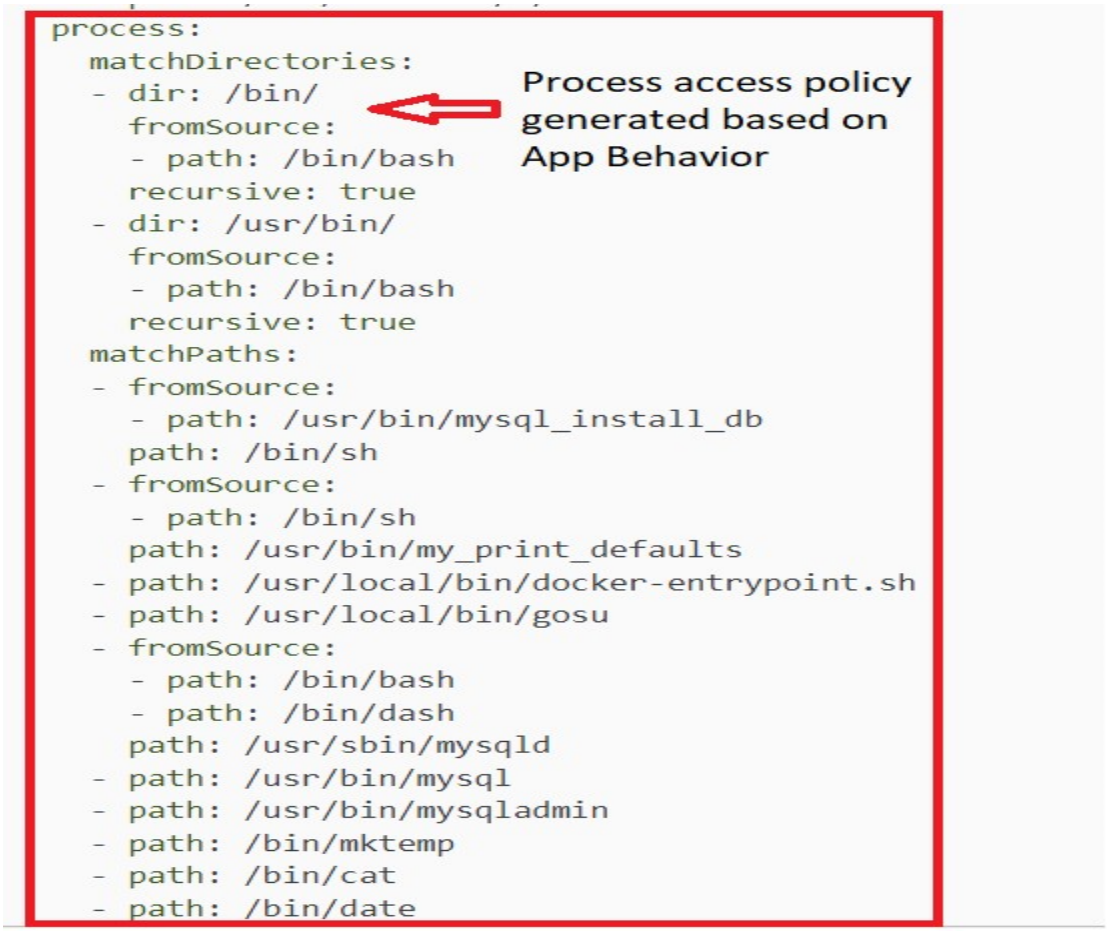
- **How to understand discover policies**

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

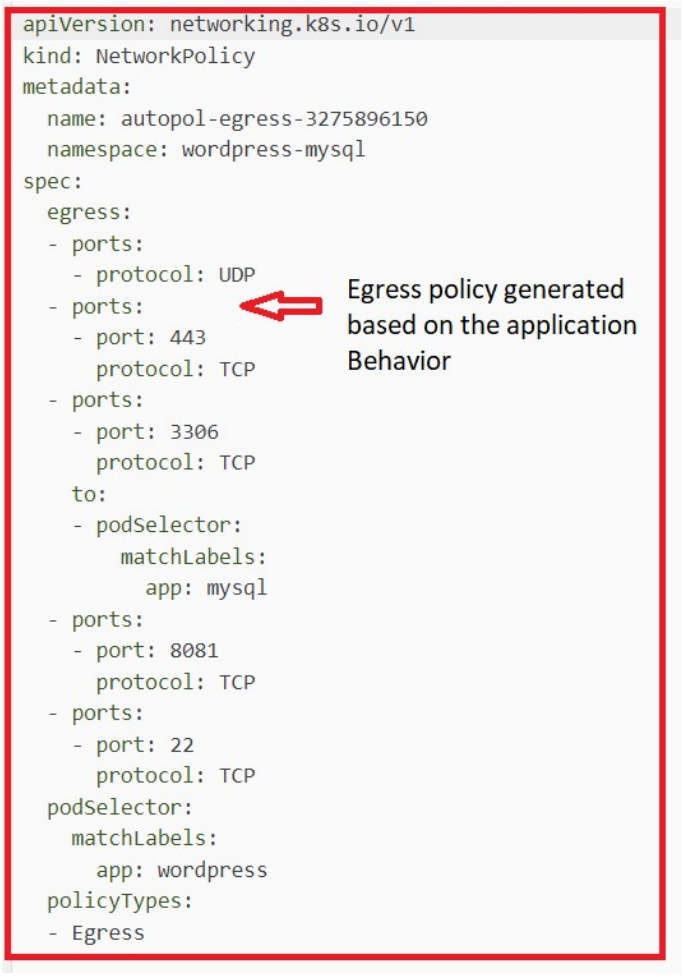
  - **File access behavior based policies:** Based on the files that are accessed in pod, the Auto discovered system policies are generated. To view that policy user must navigate to *Runtime Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered policies.



- **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.



- **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.

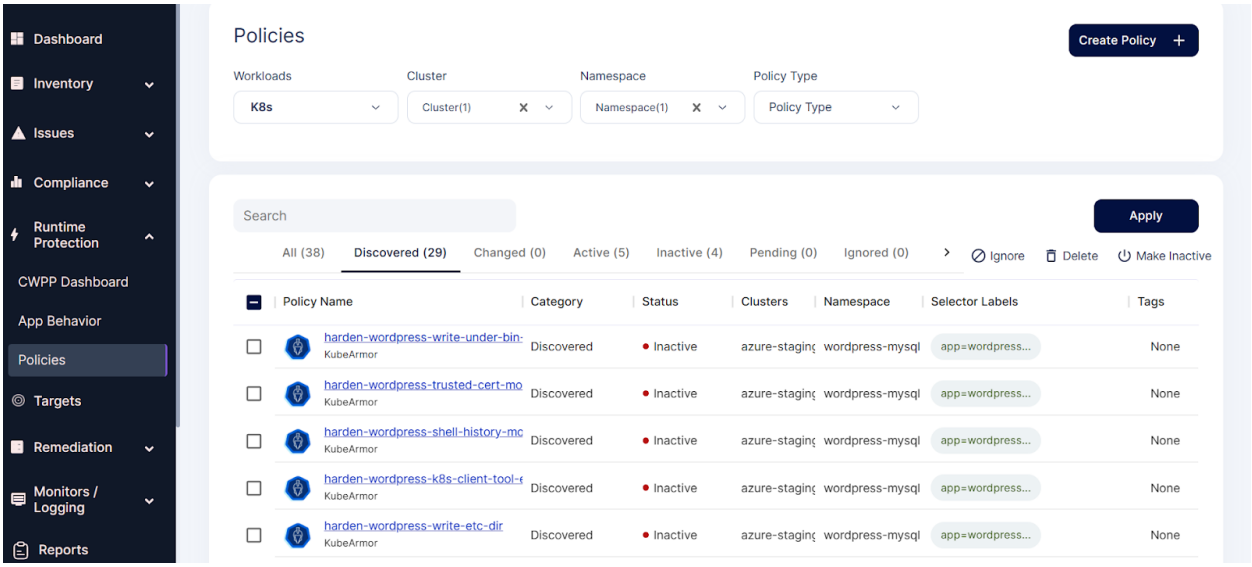


- How to understand Hardening policies

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

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

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



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

harden-wordpress-pkg-mngr-exec

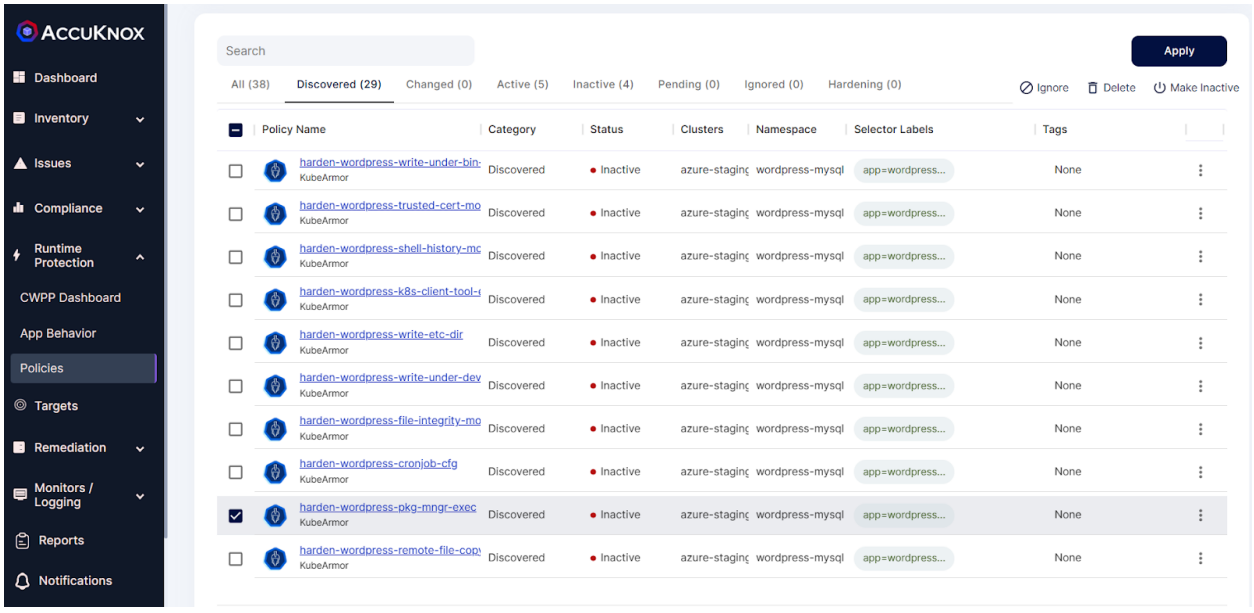
KubeArmorPolicy Updated 17days ago

YAML Edit Clone Download

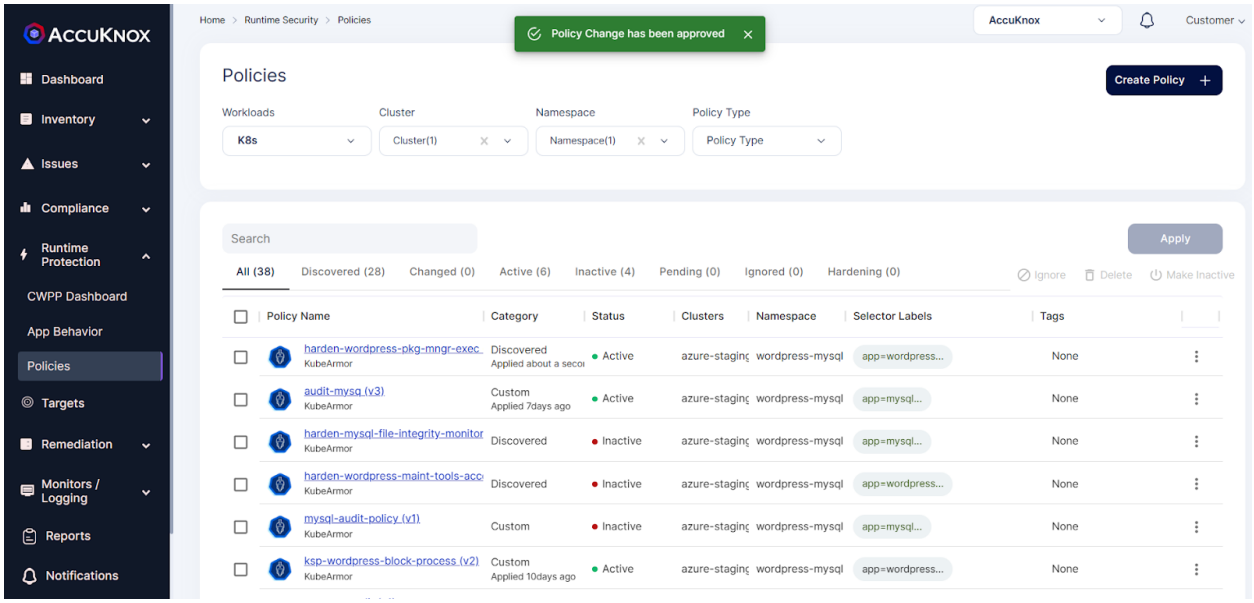
Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```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

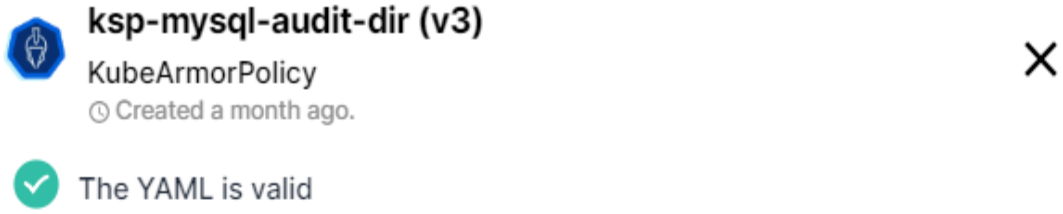


4. After applying policy goes into active state.



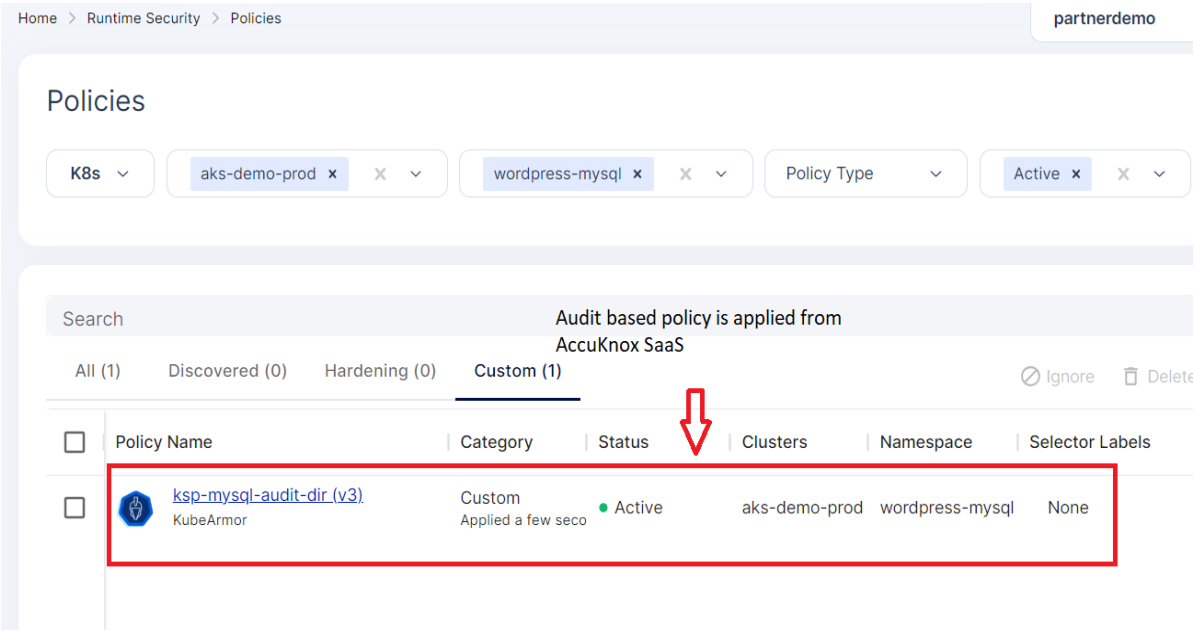
5. After applying this policy the attacker might not able to install any of the packages for performing Remote code execution attack.

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




```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
```

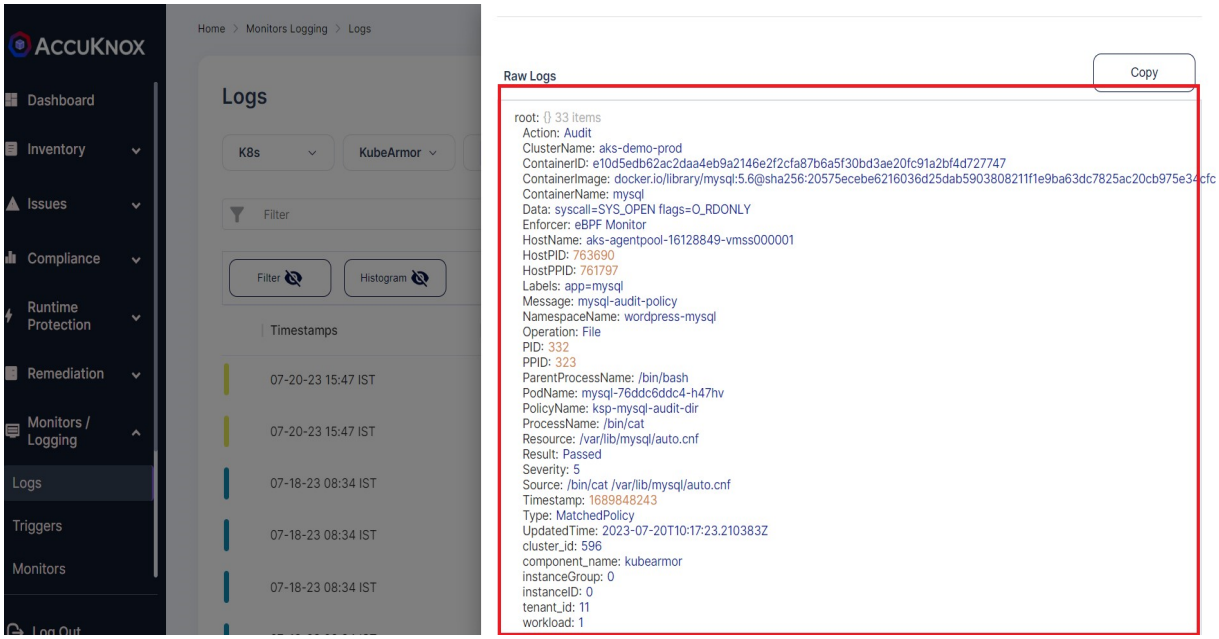
- This policy helps to audit the access to /var/lib/mysql/ folder. If any modification or any contents of this folder is read user will be intimated with alerts.
- Applying the Audit base policy from SaaS



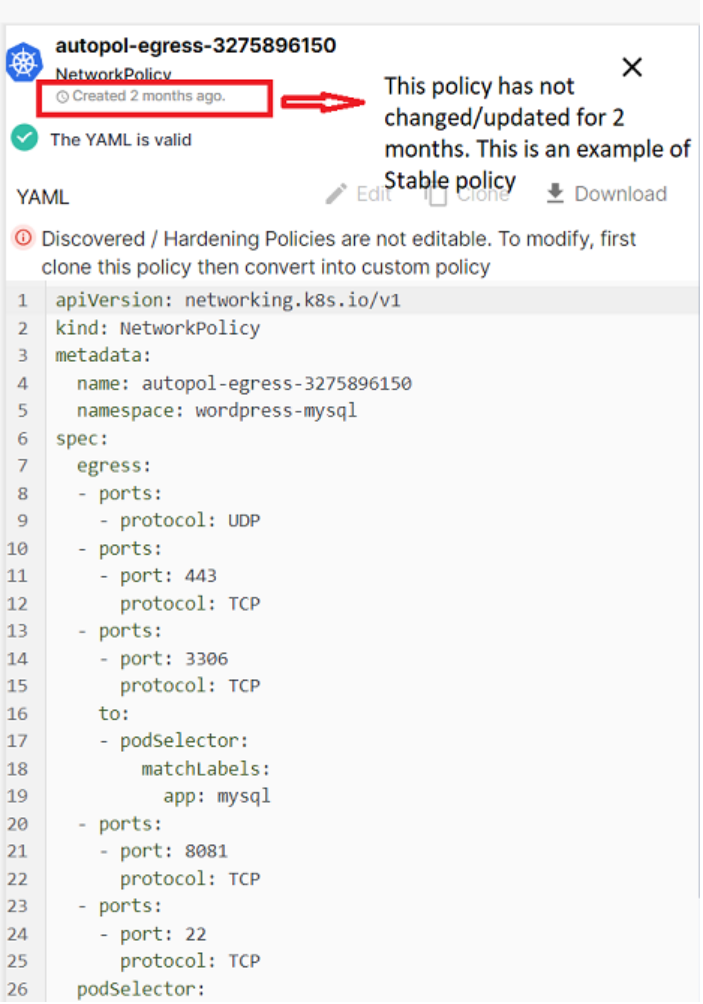
- Now if we try to read the contents of this /var/lib/mysql folder running in a mysql pod by exec into the pod.

```
~$ 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

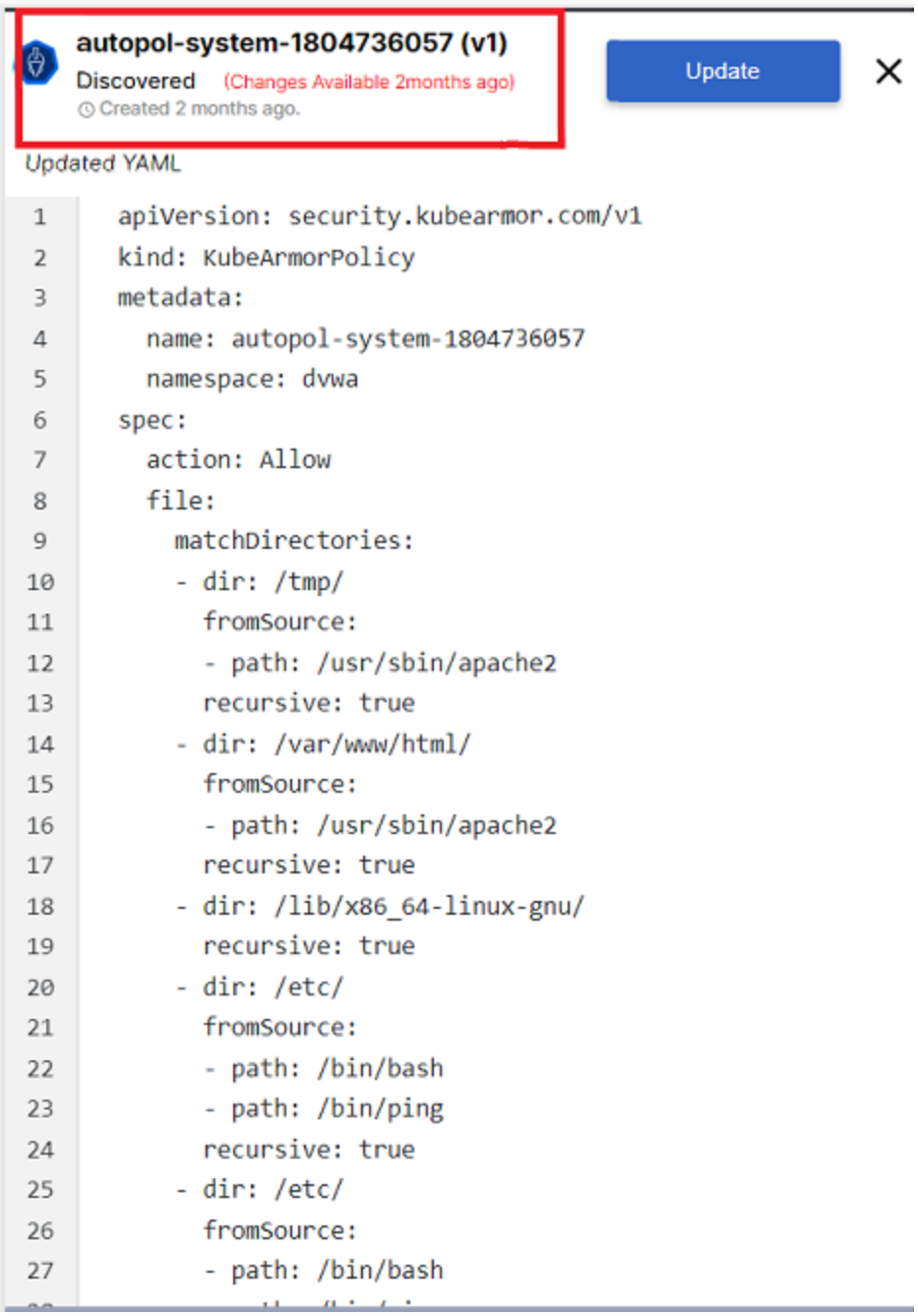


- When do we say policies are stable?
  - AccuKnox Runtime Security Engine KubeArmor will discover the policies based on the Application Behavior. If the Application behavior changes the Policies generated will also be updated.
  - When the policy created date or updated date doesn't change for some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

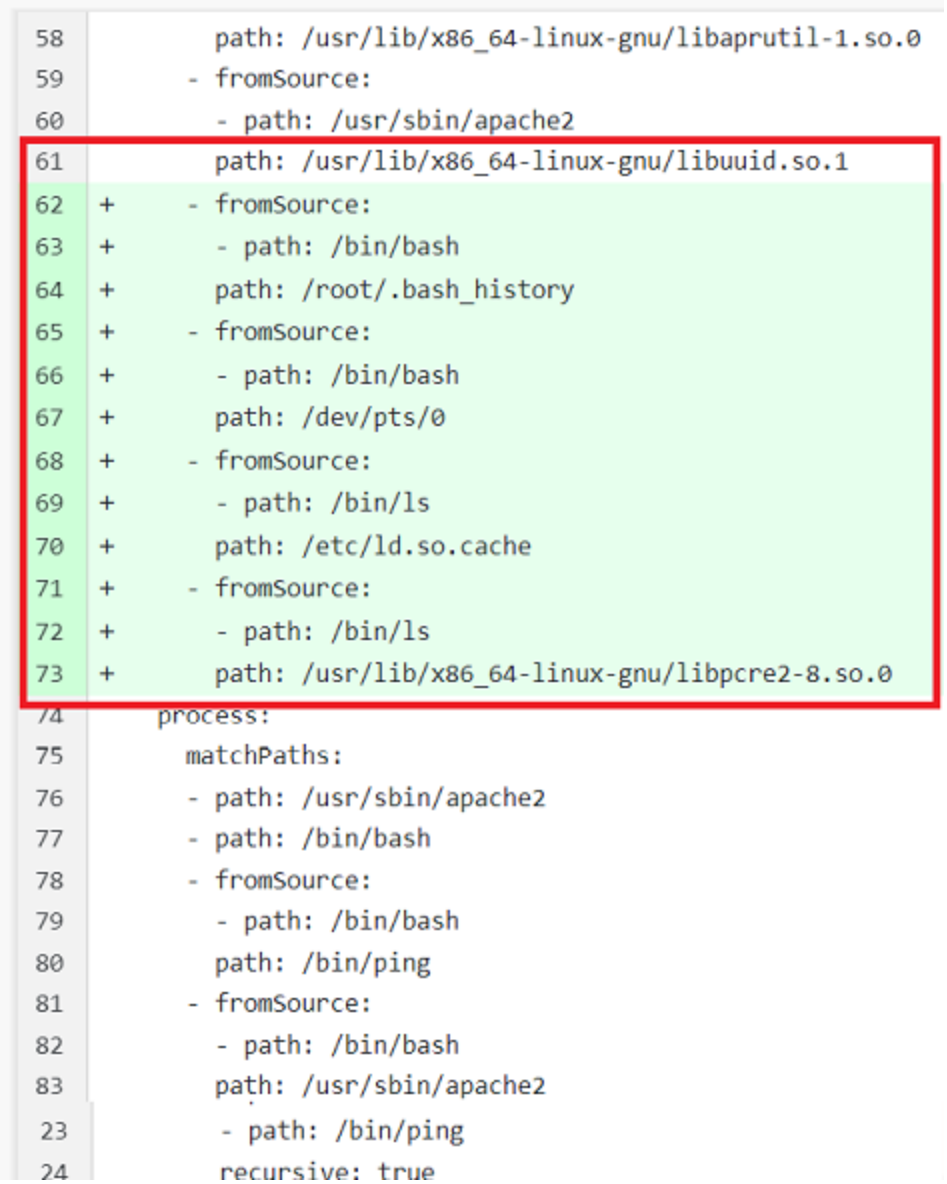


- The above auto discovered policy has not changed for more than a month. This policy can be called a stable policy as it didn't get any updates or changes.

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

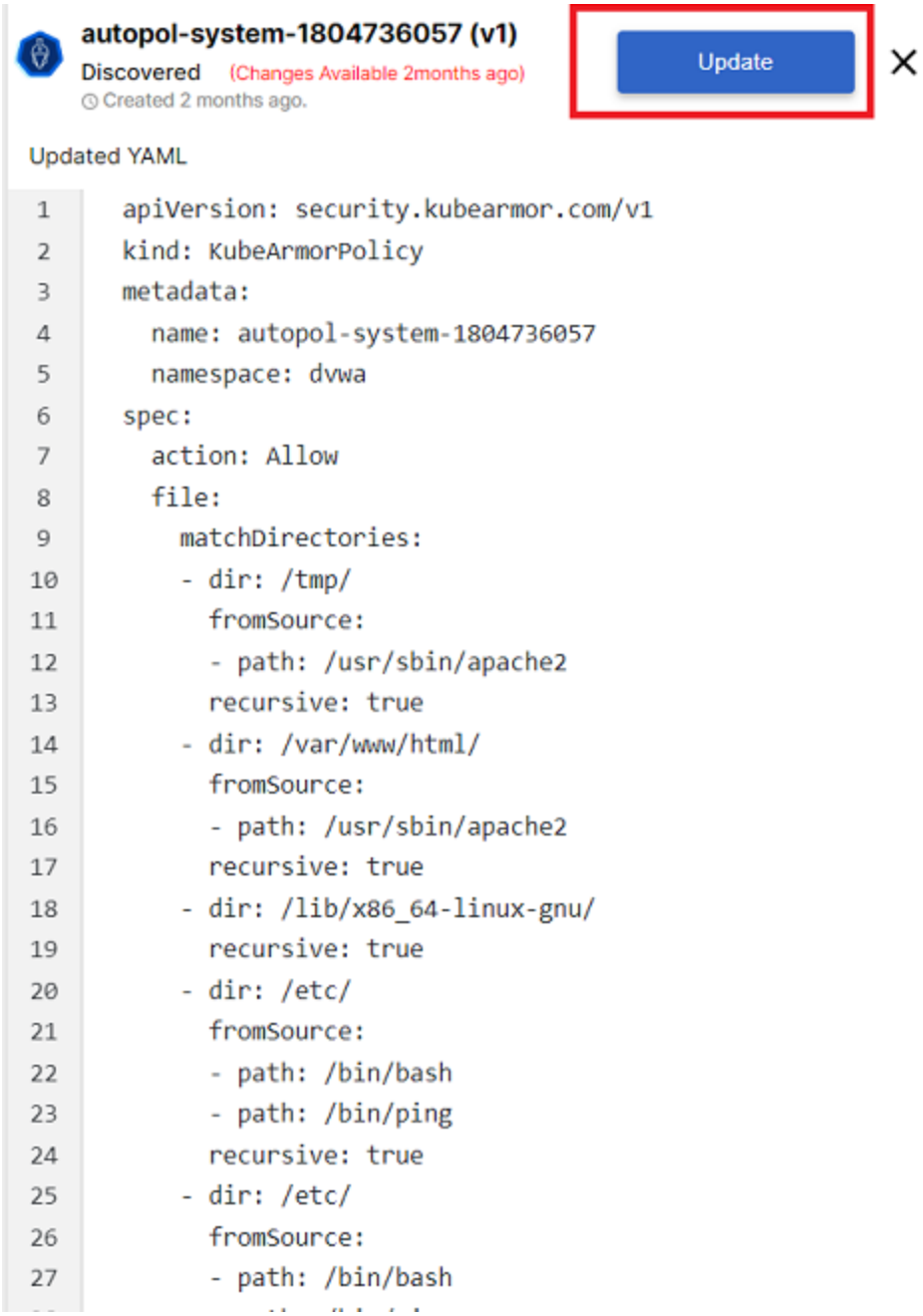


- In the above policy there are some changes that are detected after the initial policy discovery due to changes in application behavior. Those changes are highlighted.



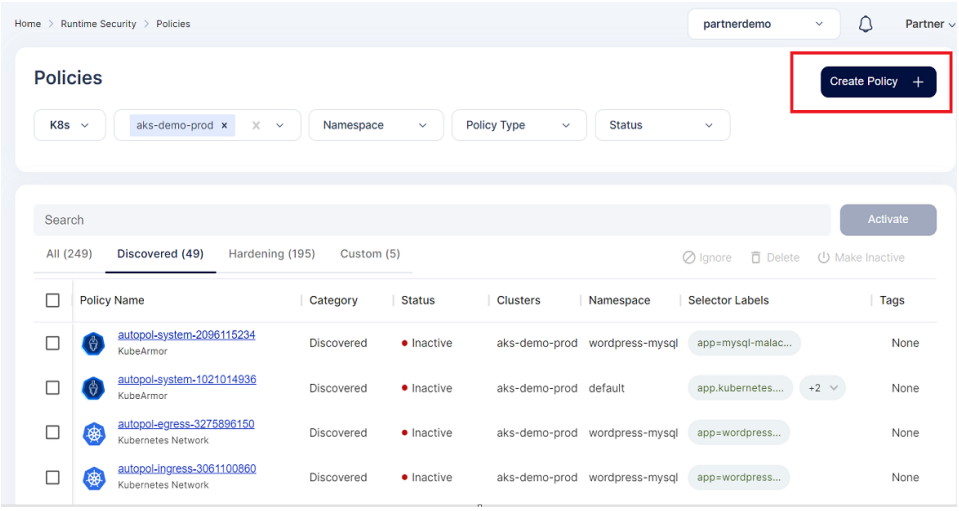
```
58          path: /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0
59        - fromSource:
60          - path: /usr/sbin/apache2
61          path: /usr/lib/x86_64-linux-gnu/libuuid.so.1
62  +     - fromSource:
63  +       - path: /bin/bash
64  +       path: /root/.bash_history
65  +     - fromSource: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

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

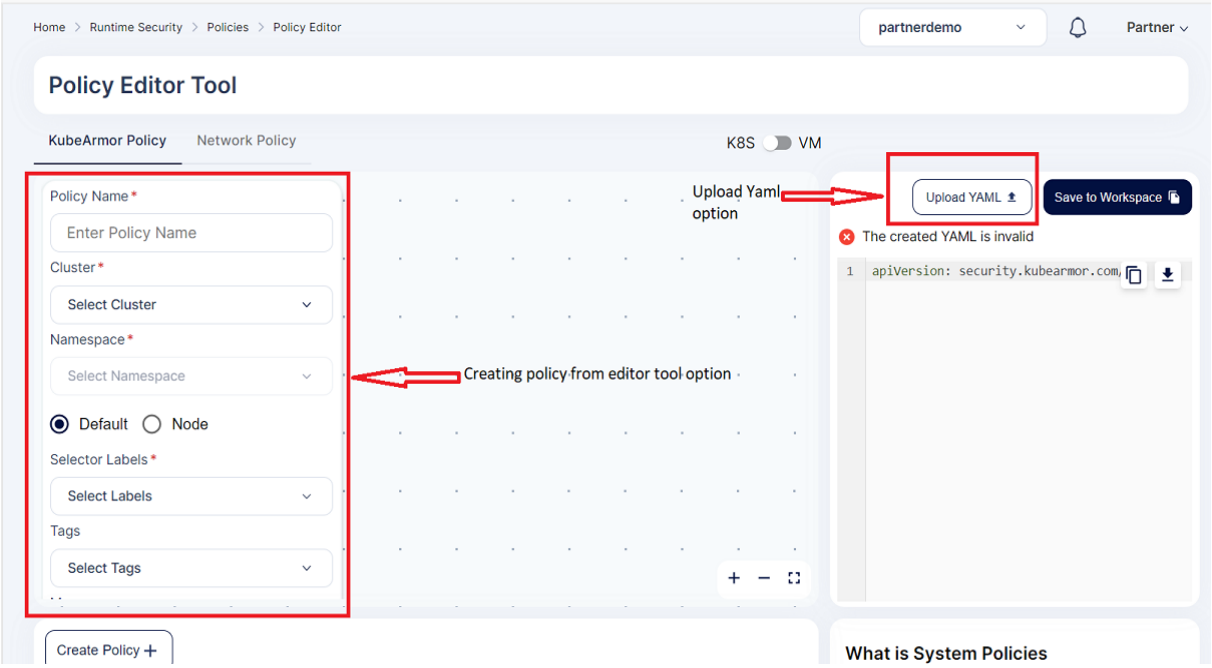


- After the user clicks the update the policy will be updated.

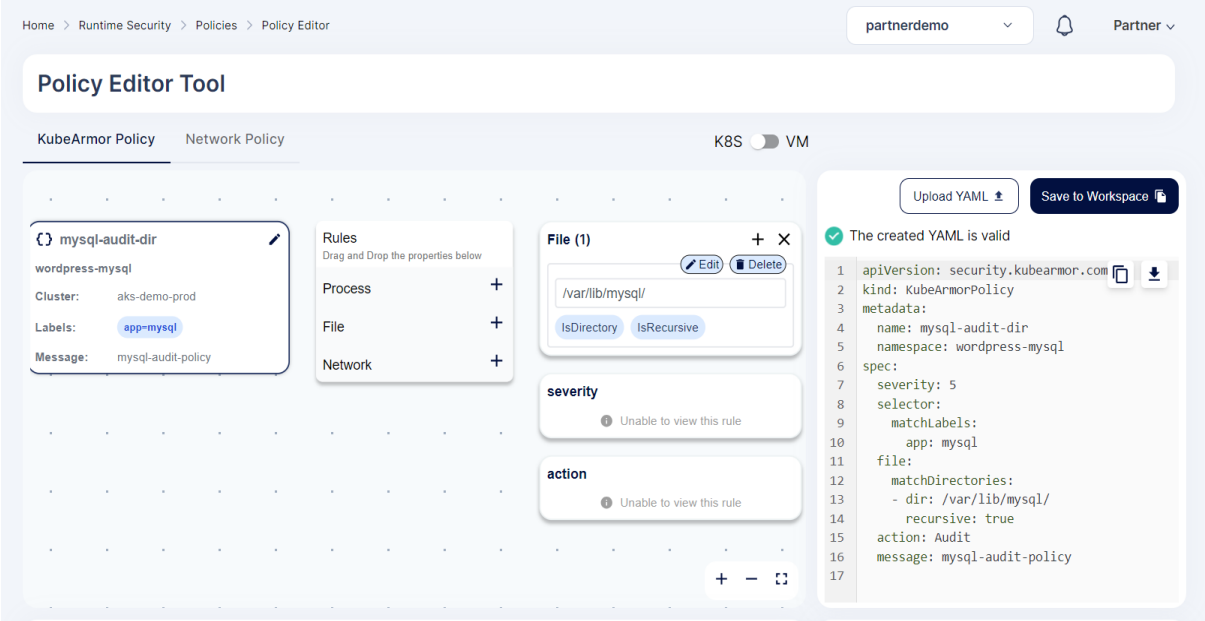
- How to create a custom Policy
  - File restriction Policy
    - To create a file restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
    - To create the policy user needs to click on the create policy option



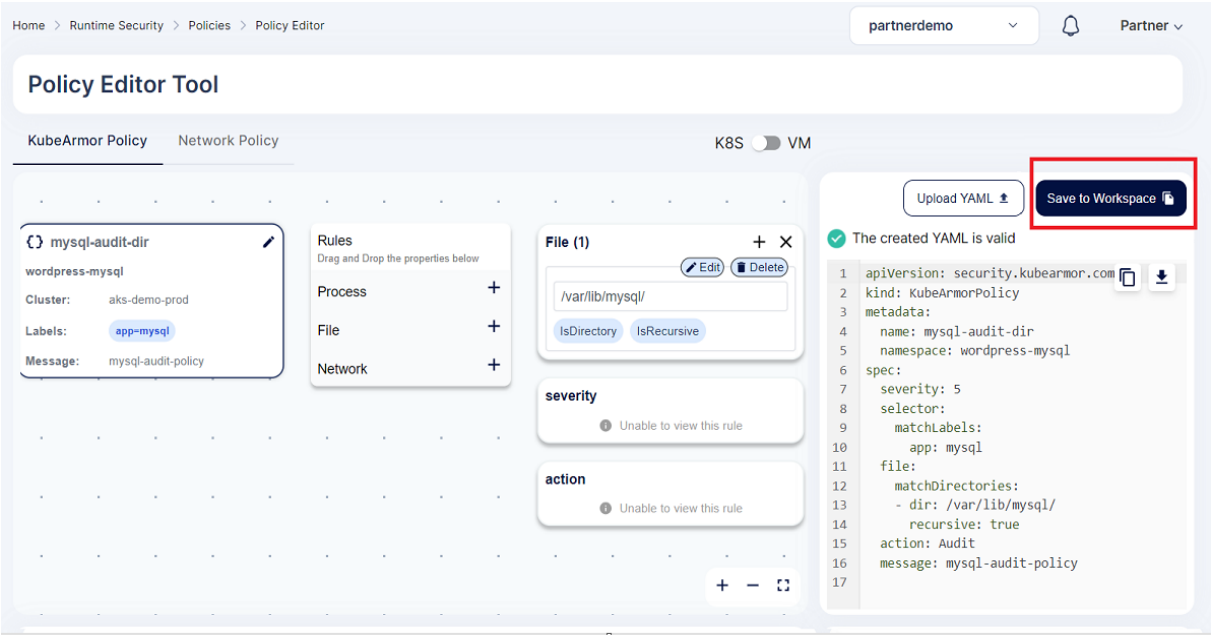
- Now user has two options either to upload the yaml file or to create the policy from policy editor tool



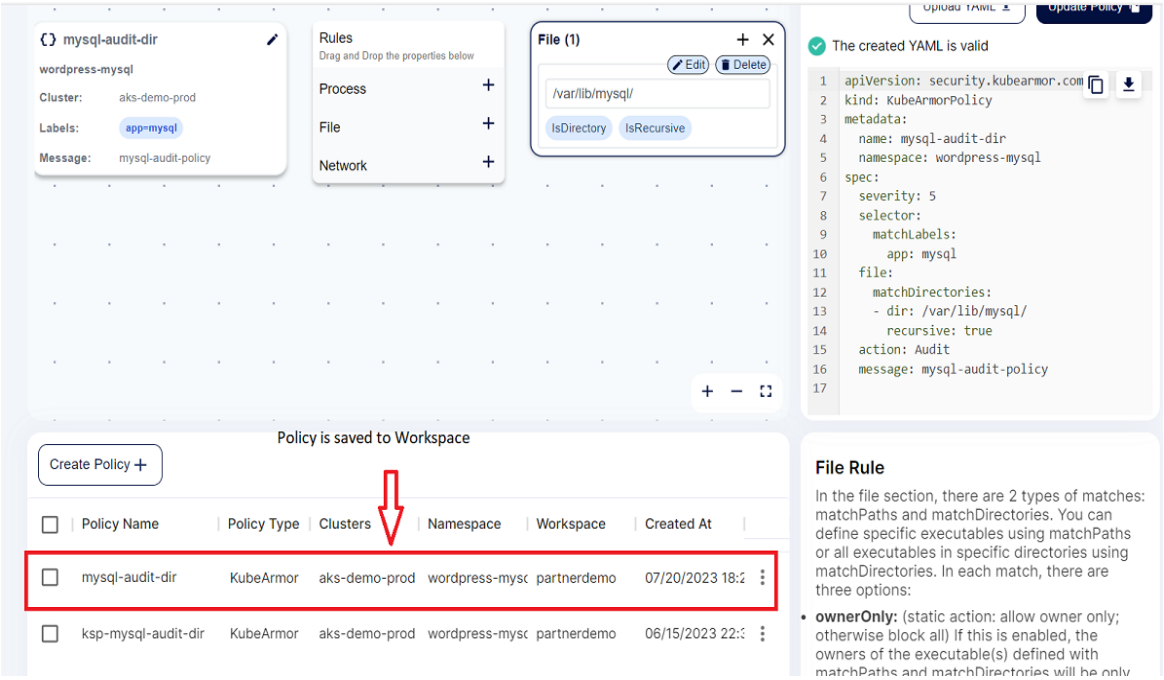
- Now upload the file access policy yaml from your system. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.



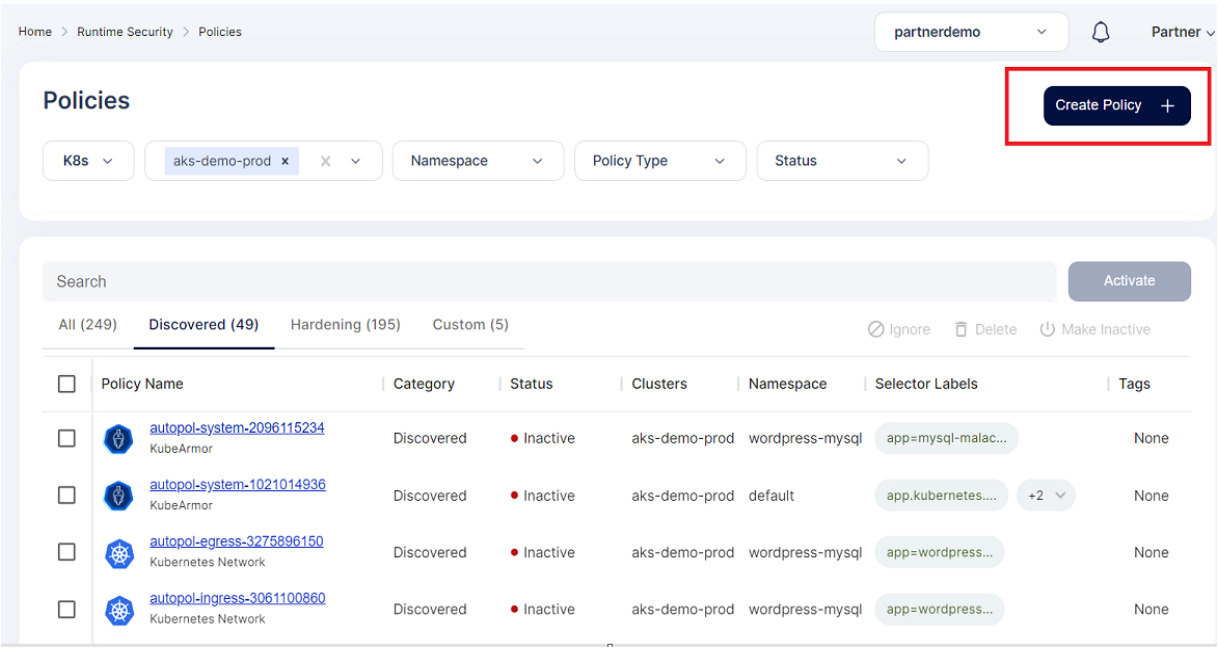
  - Now to save the policy user needs to click the *save to workspace* option



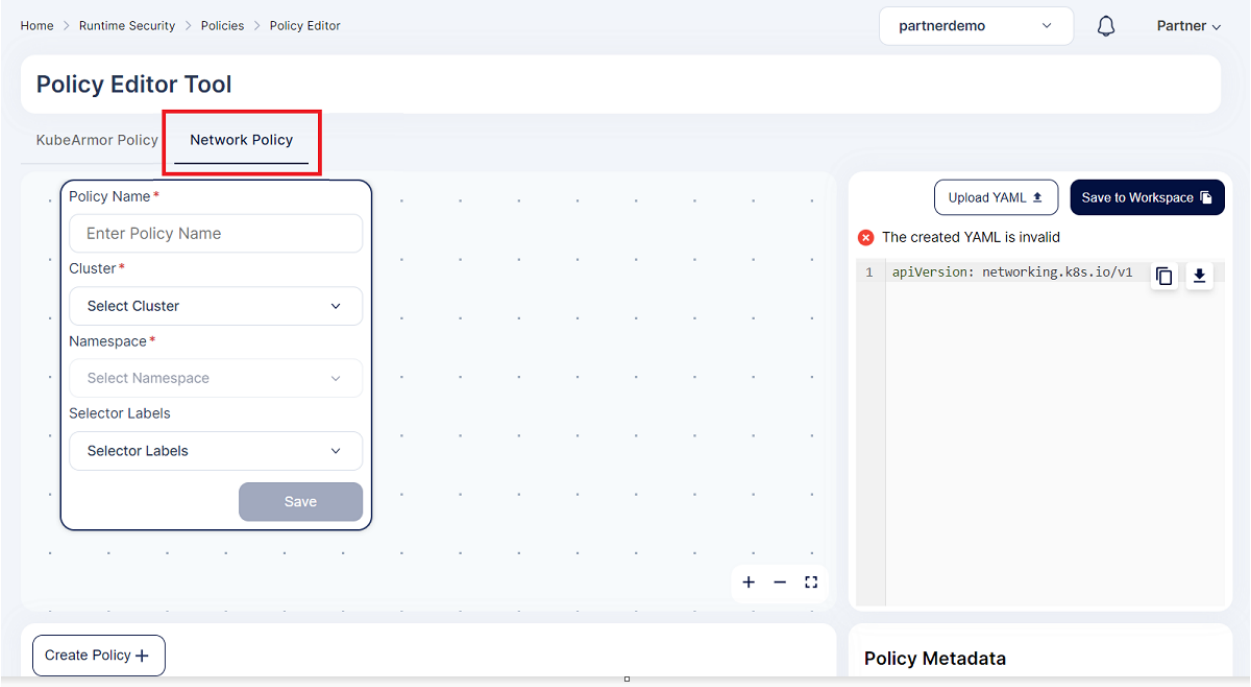
  - After that policy will be saved to the workspace.



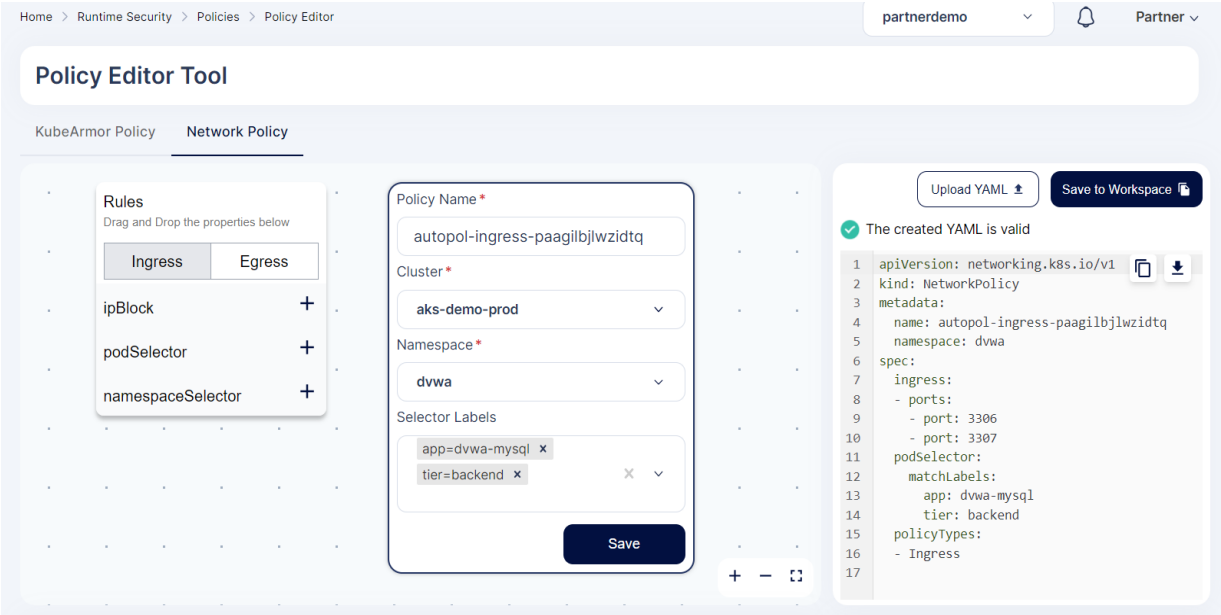
- Network access Policy
  - To create a Network access policy restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
  - To create the policy user needs to click on the create policy option



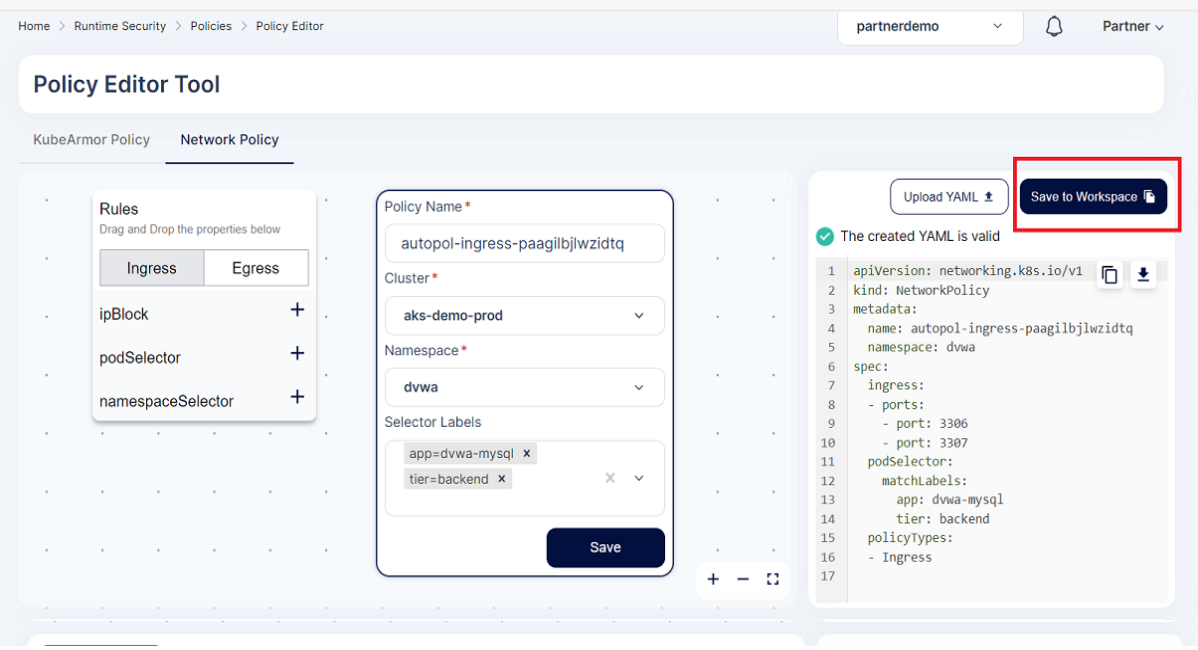
- In this screen for Network Policy creation user needs to select the Network policy editor tool



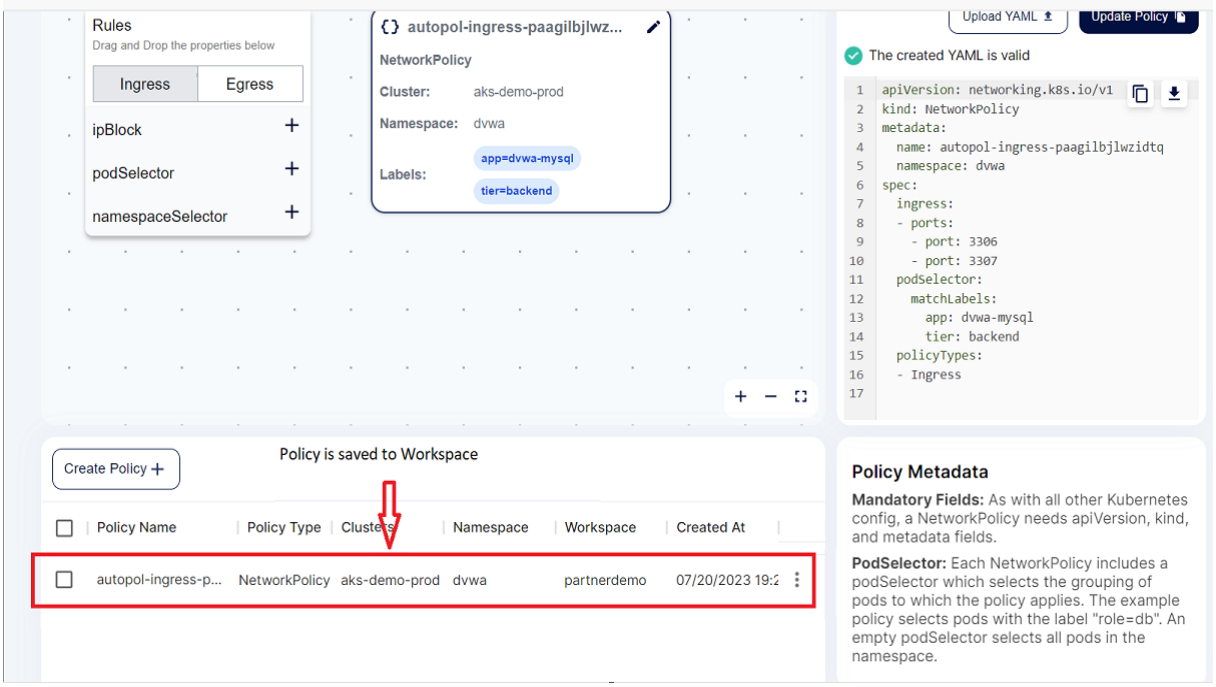
- Now upload the Network policy yaml from your system by clicking the *upload yaml* option. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.



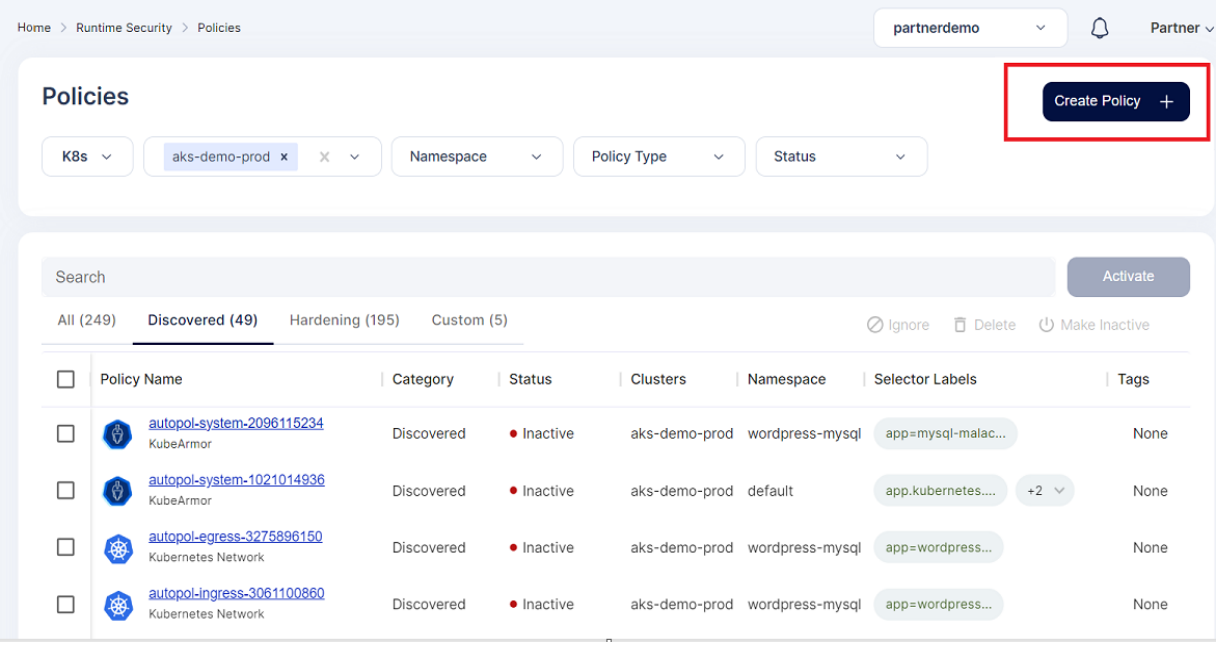
- Now to save the policy user needs to click the *save to workspace* option



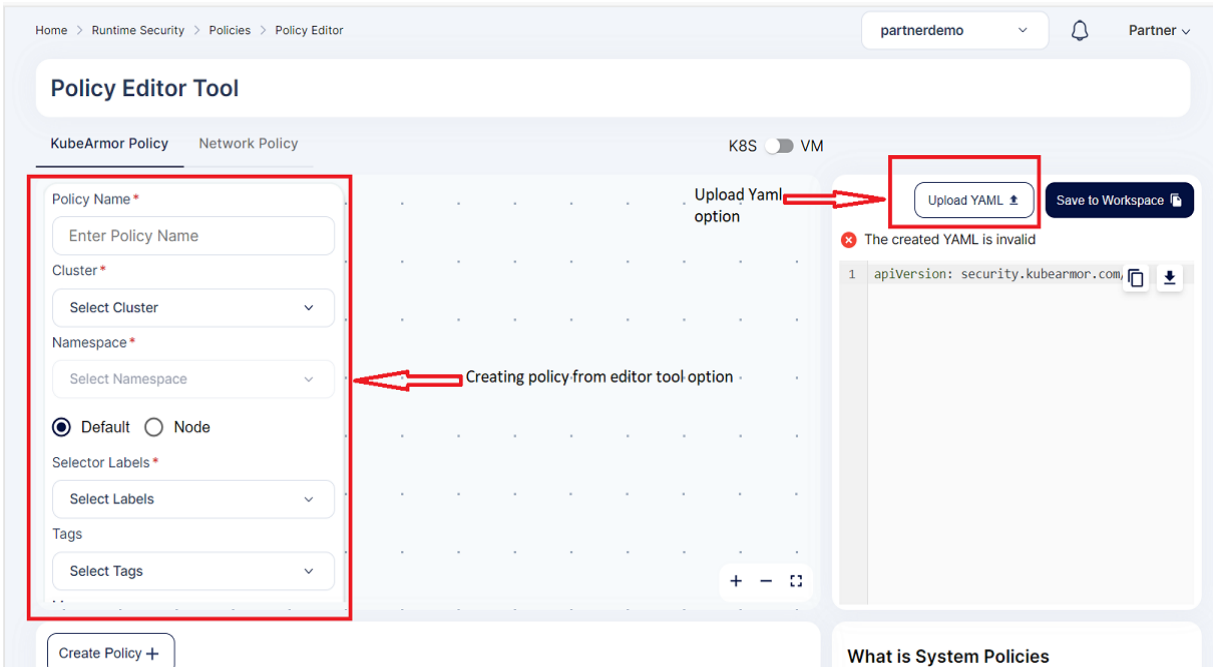
- After that policy will be saved to the workspace.



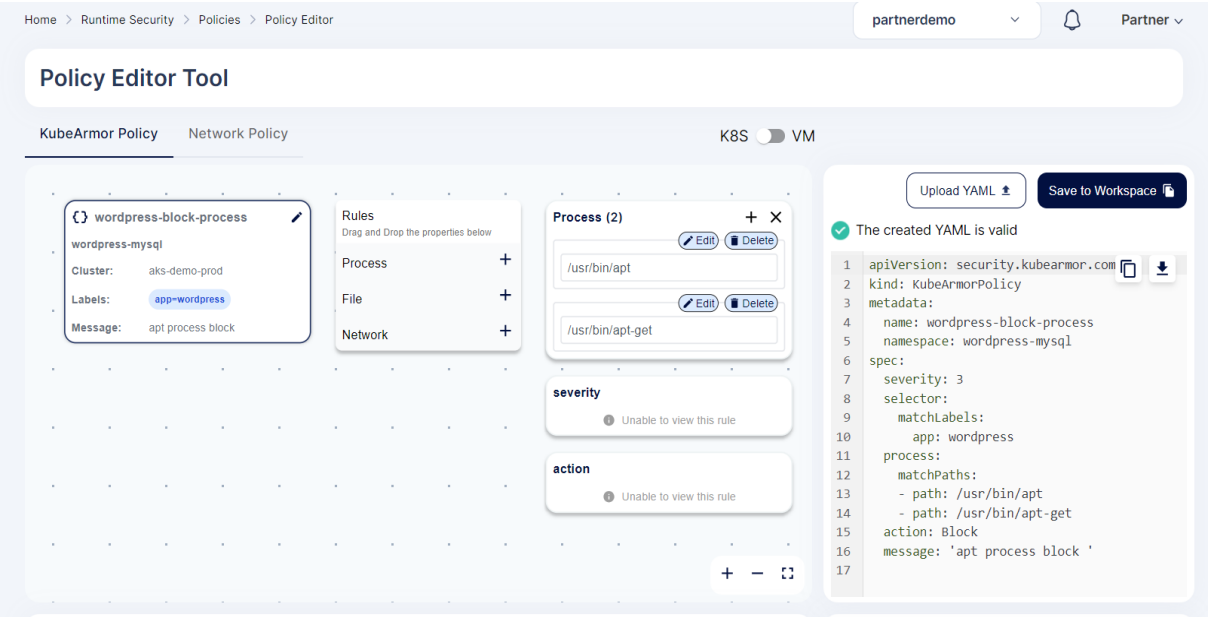
- Process block restriction Policy
  - To create a Process access restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
  - To create the policy user needs to click on the create policy option



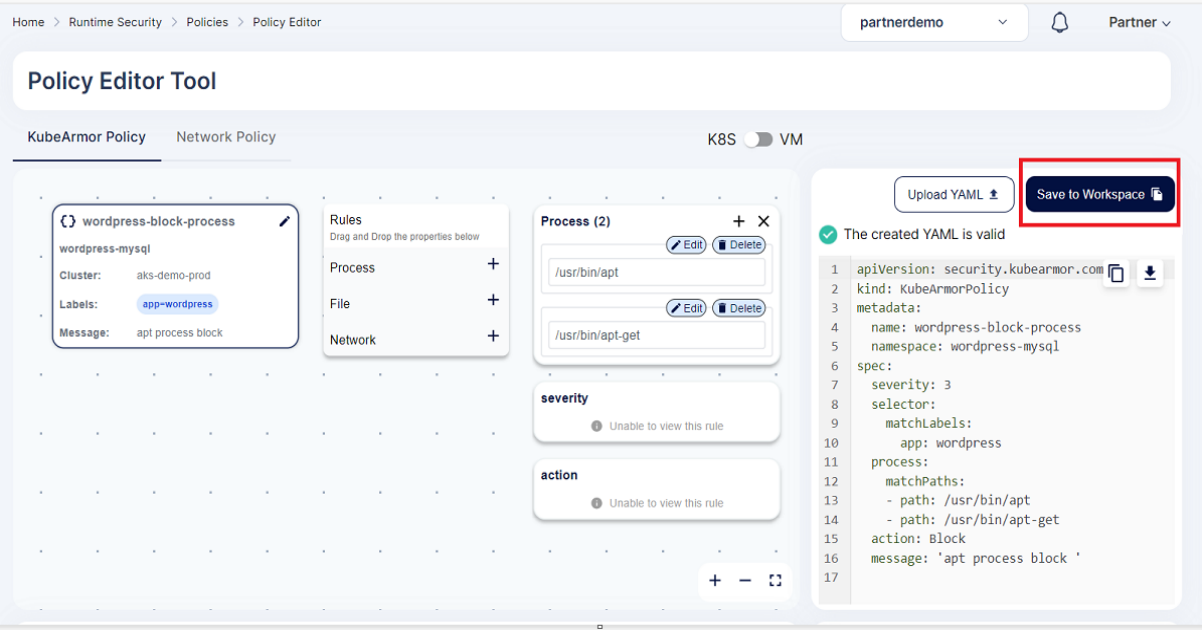
■ Now user has two options either to upload the yaml file or to create the policy from policy editor tool



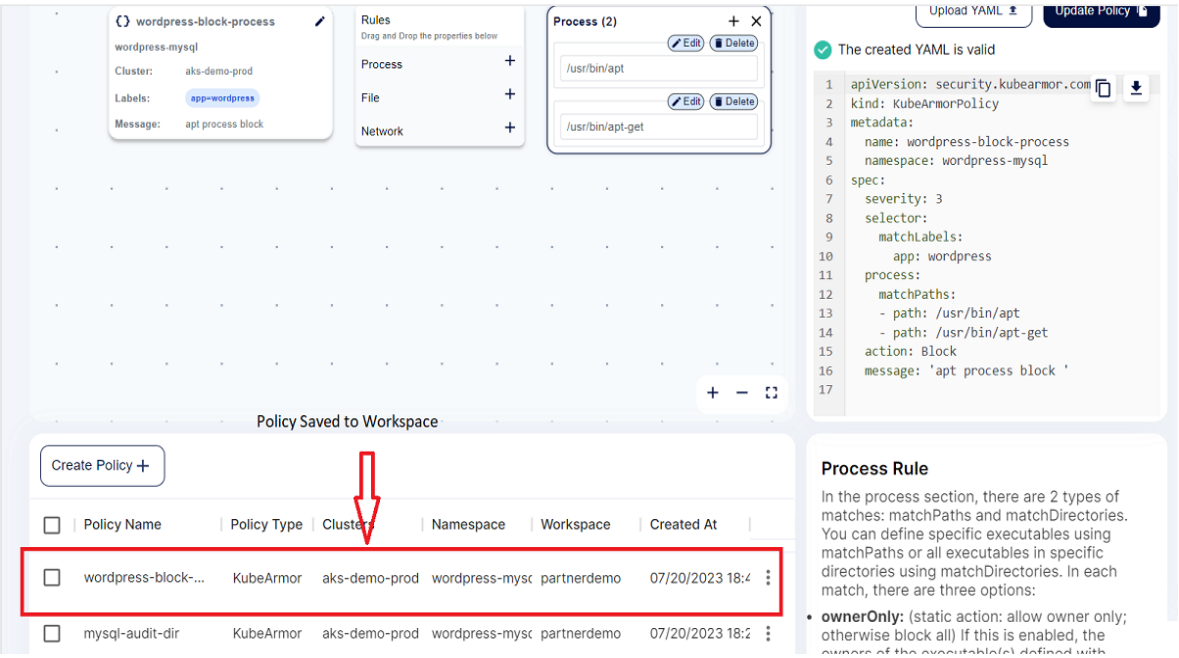
■ Now upload the process block policy yaml from your system. After it is upload some the columns in the left side will be prefilled and user needs to select the cluster and namespace where the policy needs to applied and click save.



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



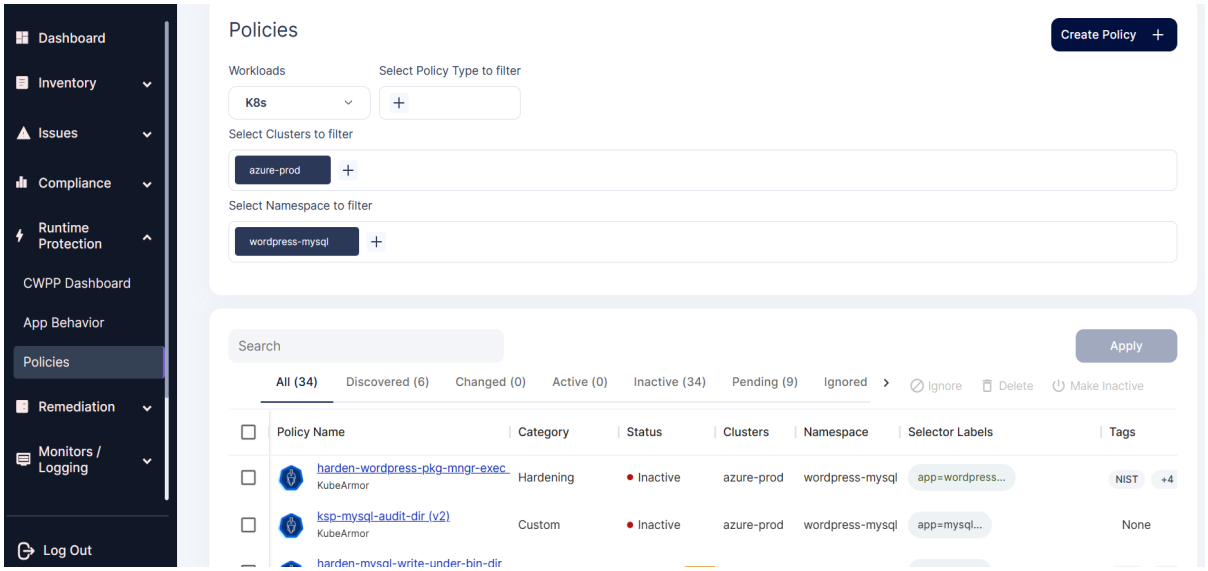
- After that policy will be saved to the workspace.



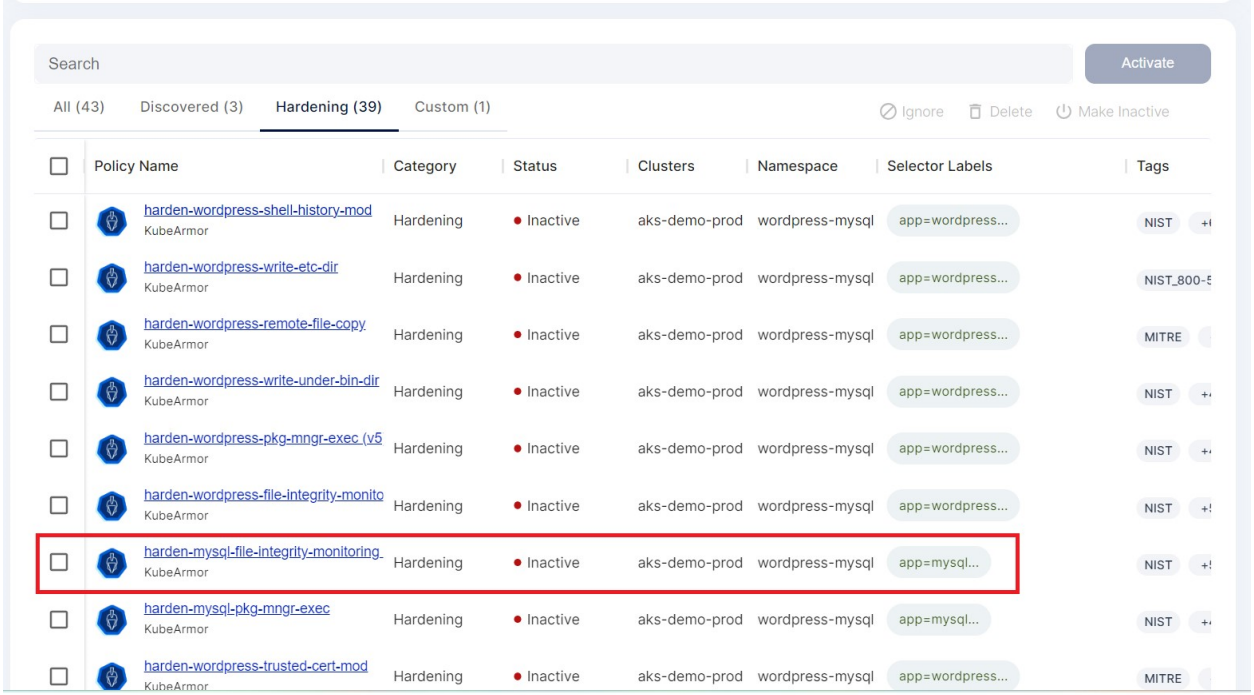
- How to enforce Policies and see anomalies
  - We can apply any of the Auto Discovered, Hardening or custom policies and see the anomalies getting detected using the Monitoring and Logging section.
  - Let us consider the WordPress- MySQL application. In the MySQL application, certain folders will be 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#
```

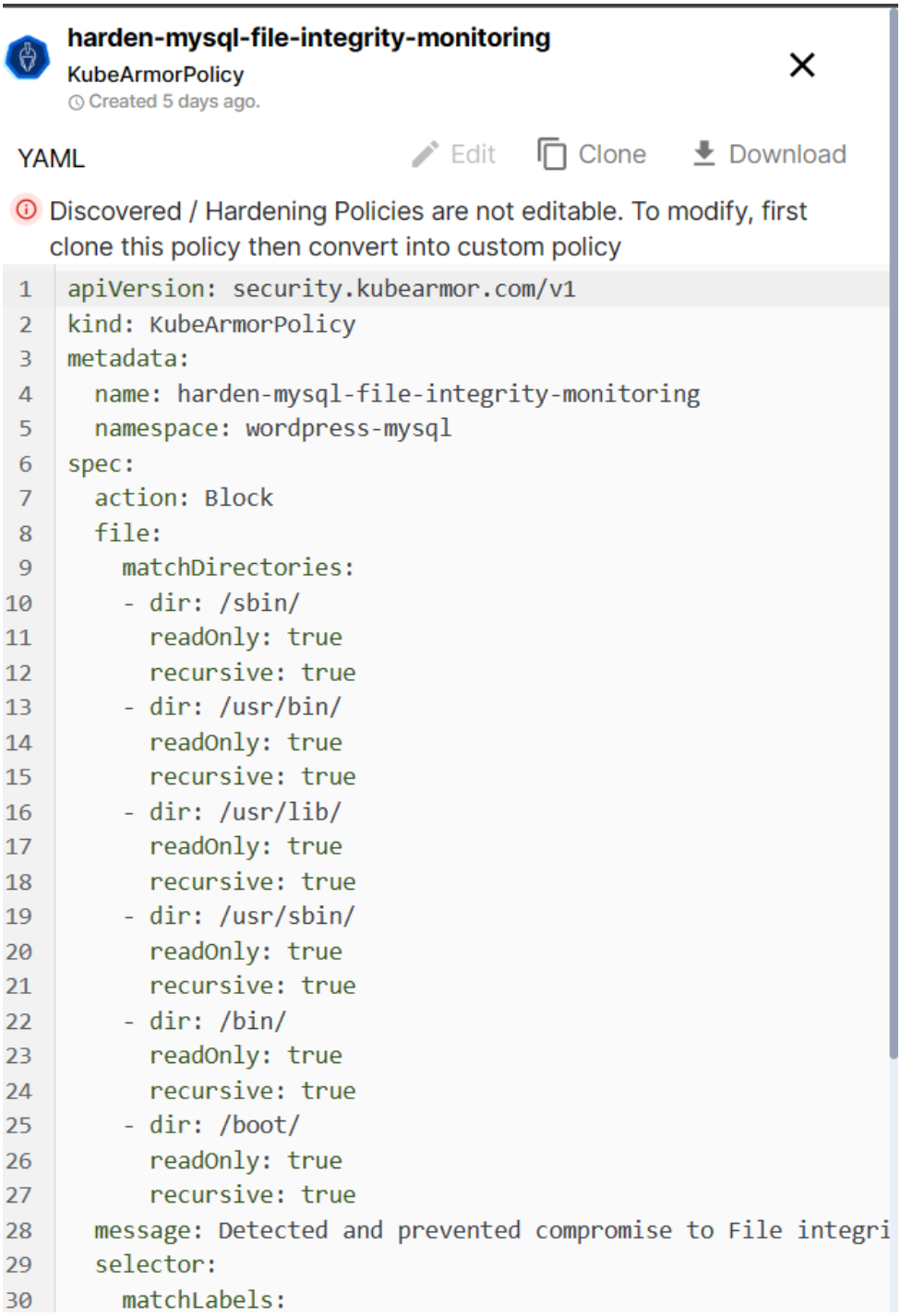
- Now we are going to prevent this using AccuKnox CWPP Solution.
- **Step 1:** Navigate to the Runtime Protection-> Policies and select the cluster and namespace where the WordPress-MySQL application is deployed.



- **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.



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

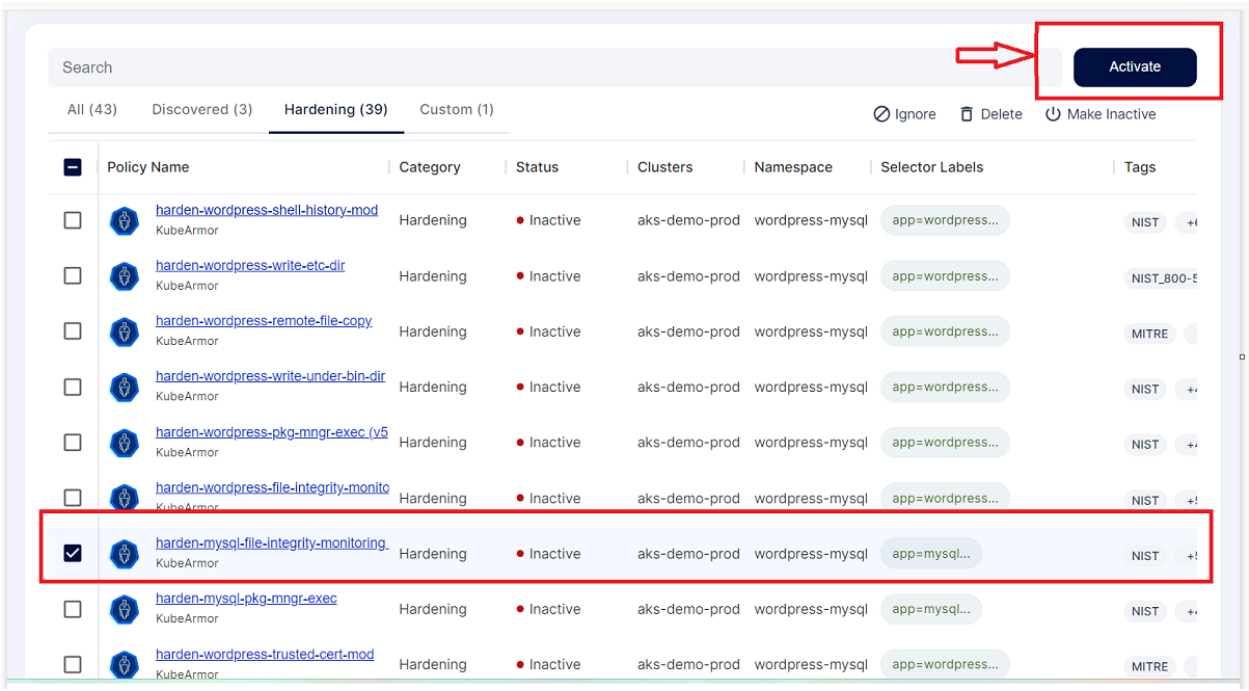


- The policy is allowing users to access the critical folders but it is blocking the write or modify access by whitelisting only read access.

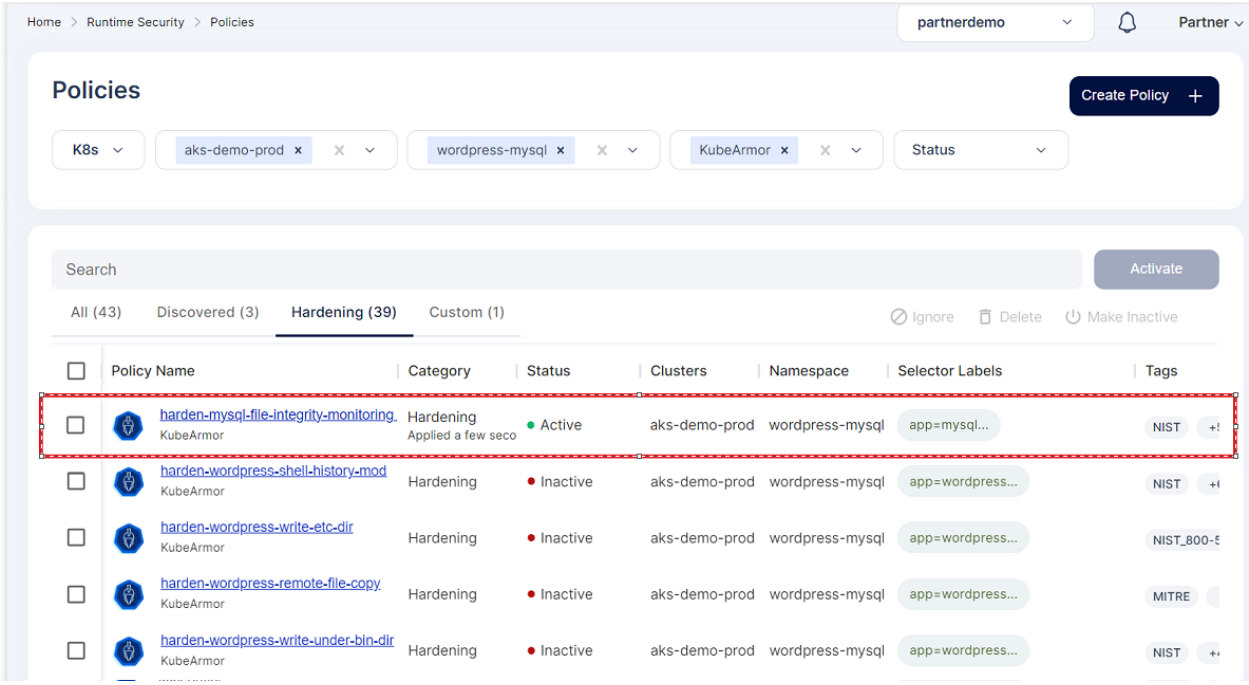
```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
```

```
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



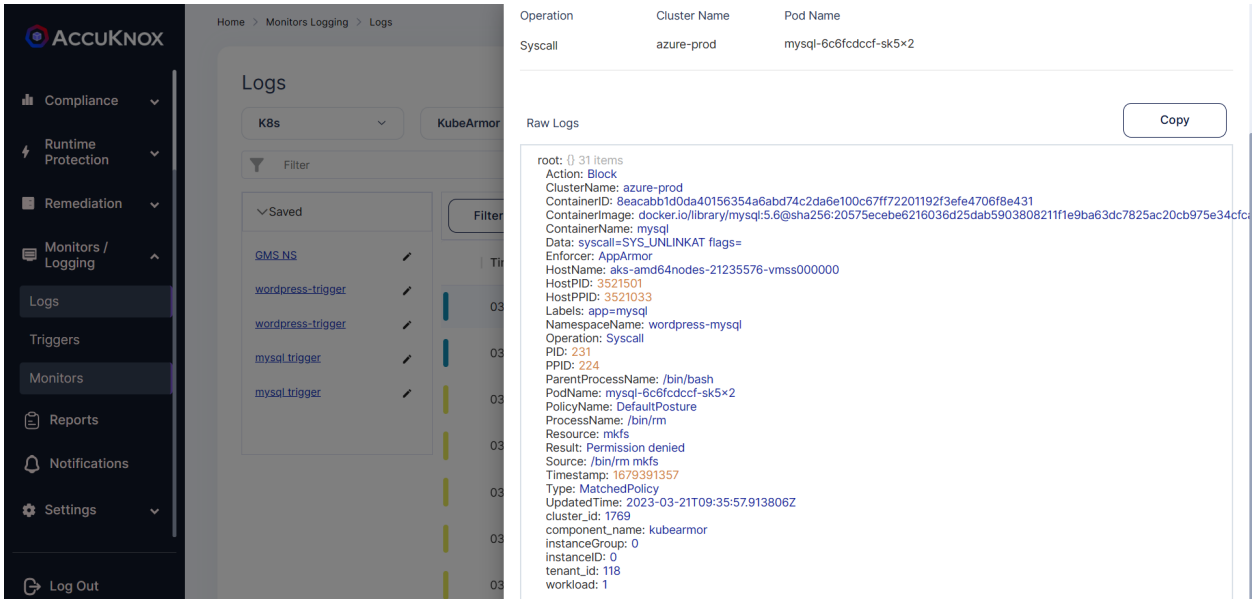
- **Step 5:** Now the policy is active and applied on the cluster



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

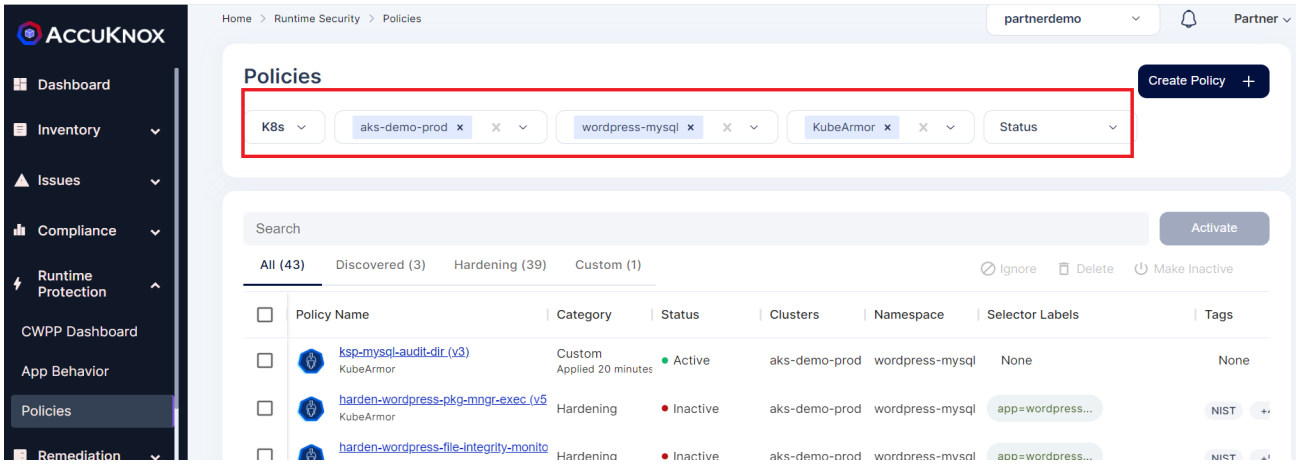
```
root@mysql-6c6fcdccf-sk5x2:/# cd sbin
root@mysql-6c6fcdccf-sk5x2:/sbin# ls
agetty      dumpe2fs     fsck.ext2     installkernel  mkfs.cramfs       pam_tally2         swaplabel
badblocks   e2fsck       fsck.ext3     isosize        mkfs.ext2         pivot_root         swapoff
blkdiscard  e2image      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

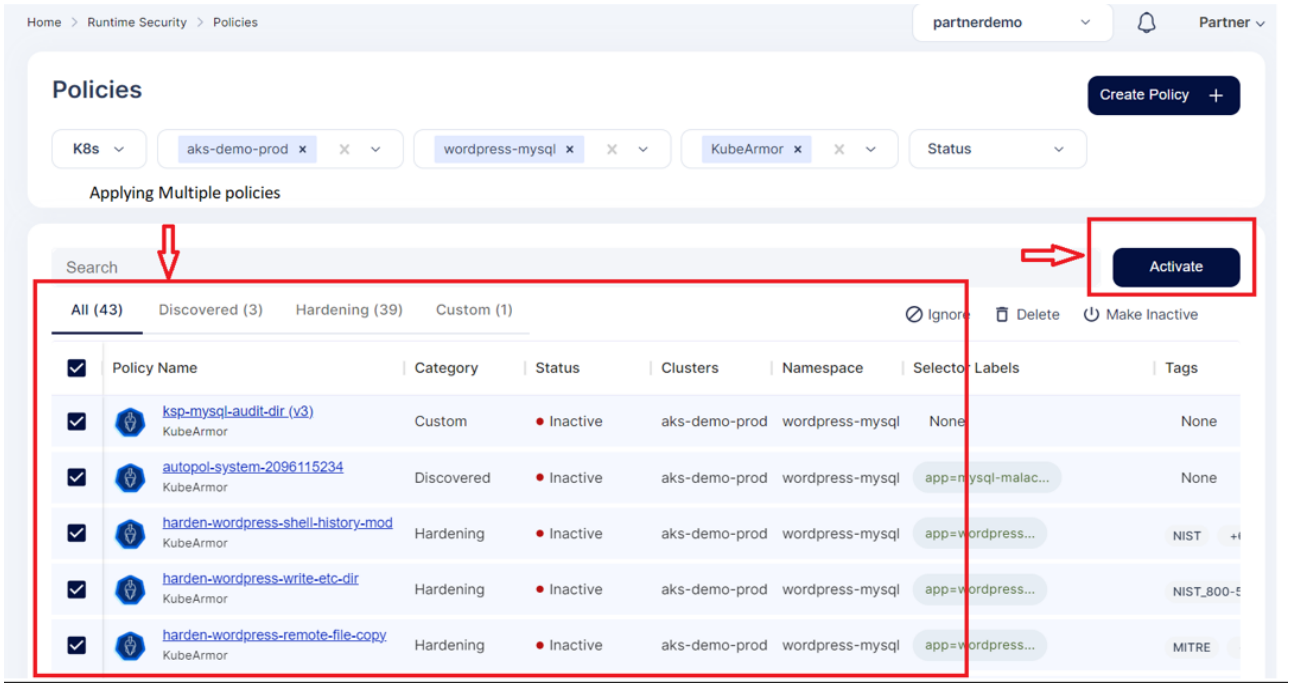


How to perform bulk operation on applying policies

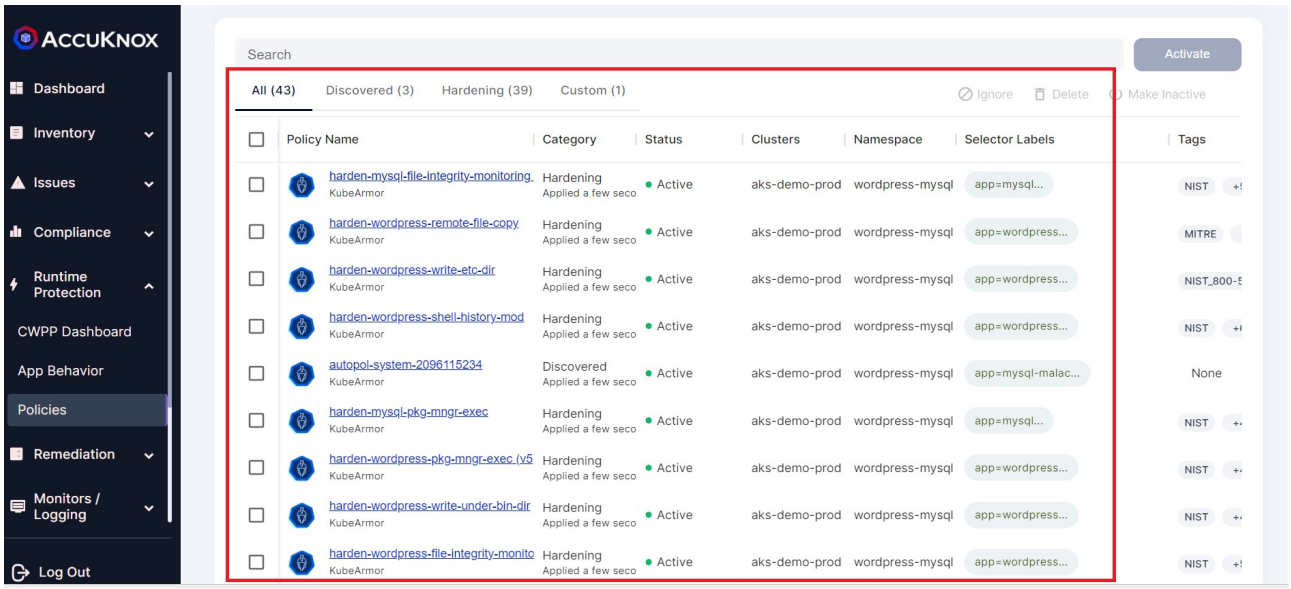
- AccuKnox SaaS supports applying multiple policies at one time. To perform this user must navigate to the *Runtime Protection->Policies* Section.
- From the Filters shown in the Screen user must select the Cluster and Namespace for which they are going to apply multiple policies


ACCUKNOX
Dashboard
Inventory
Issues
Compliance
Runtime Protection
CWPP Dashboard
App Behavior
Policies
Remediation
Home > Runtime Security > Policies
partnerdemo
Partner
Policies
Create Policy
K8s
aks-demo-prod
wordpress-mysql
KubeArmor
Status
Search
Activate
All (43)
Discovered (3)
Hardening (39)
Custom (1)
Ignore
Delete
Make Inactive
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 the all policies from the screen and click Activate button



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



Integrations

1. Integrate SIEM tools

- SPLUNK
- AWS Cloud Watch
- Rsyslog

Splunk

Splunk Integration:

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

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

Integration of Splunk:

a. Prerequisites:

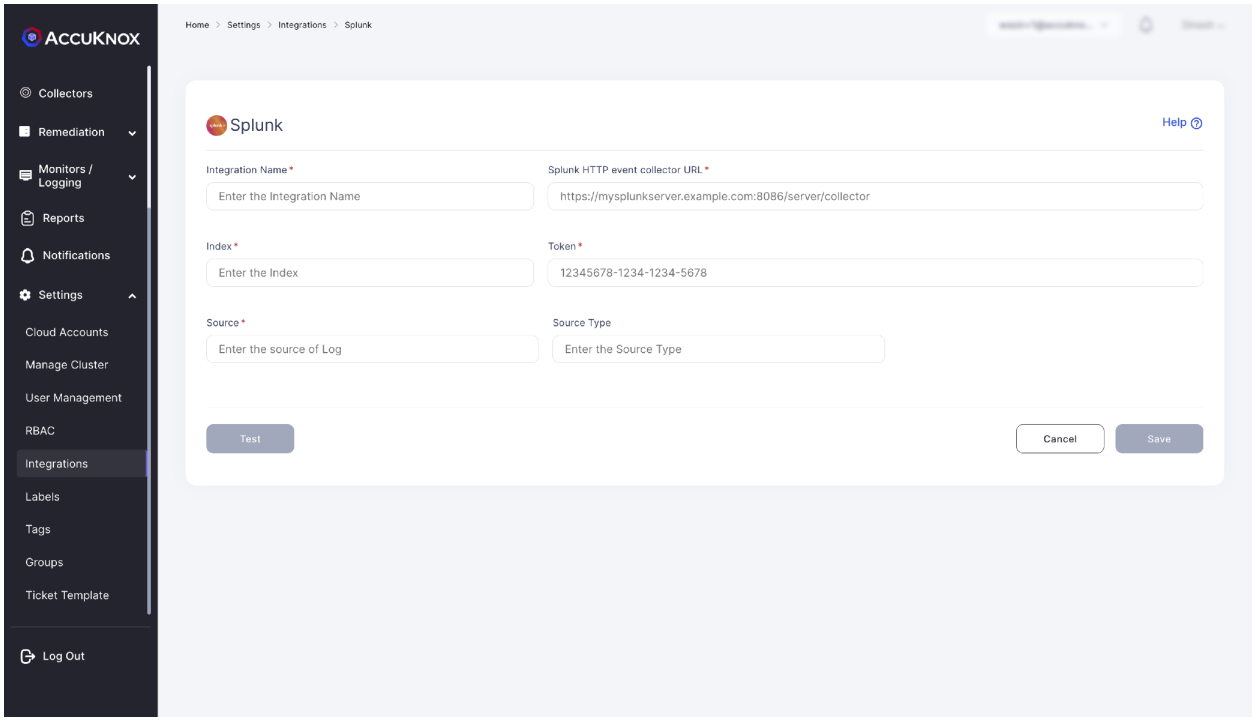
Set up Splunk HTTP Event Collector (HEC) to view alert notifications from AccuKnox in Splunk. Splunk HEC lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols.

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.



- 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.

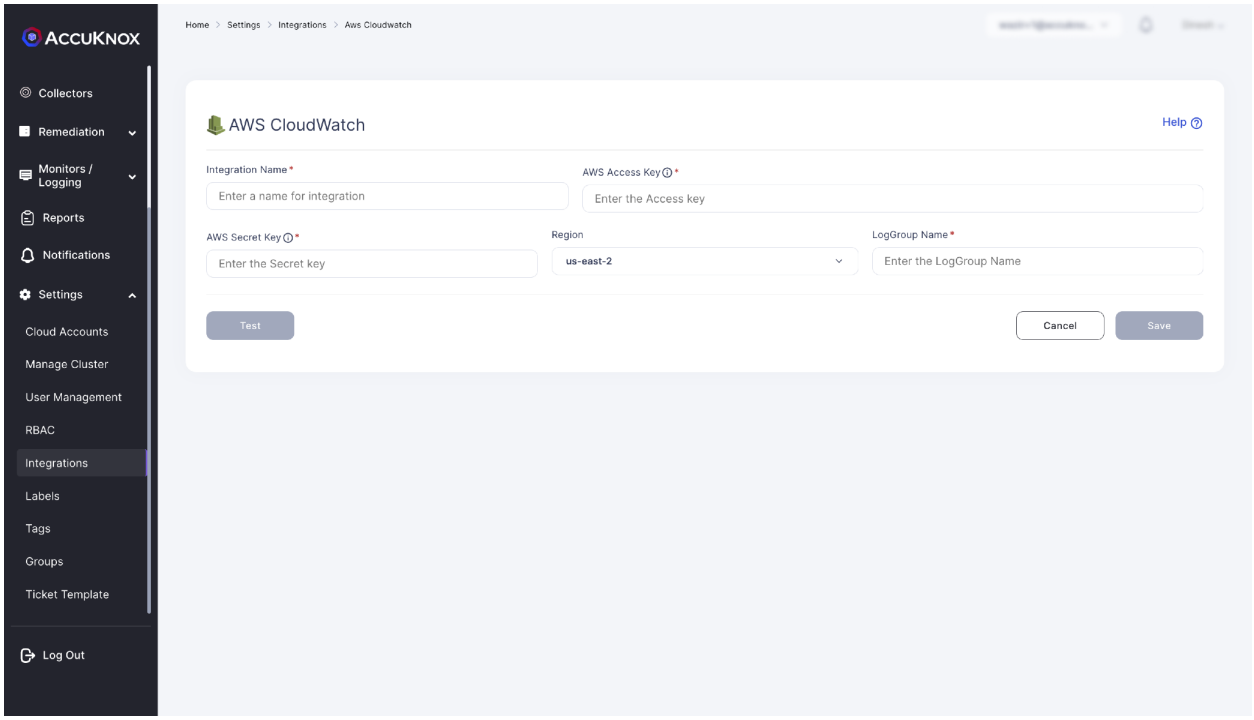
Integration of Amazon CloudWatch:

a. Prerequisites

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

b. Steps to Integrate:

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



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

c. Configuration of Alert Triggers:

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

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

d. Logs Forwarding:

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

Rsyslog

RSyslog Integration

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

Integration of RSyslog:

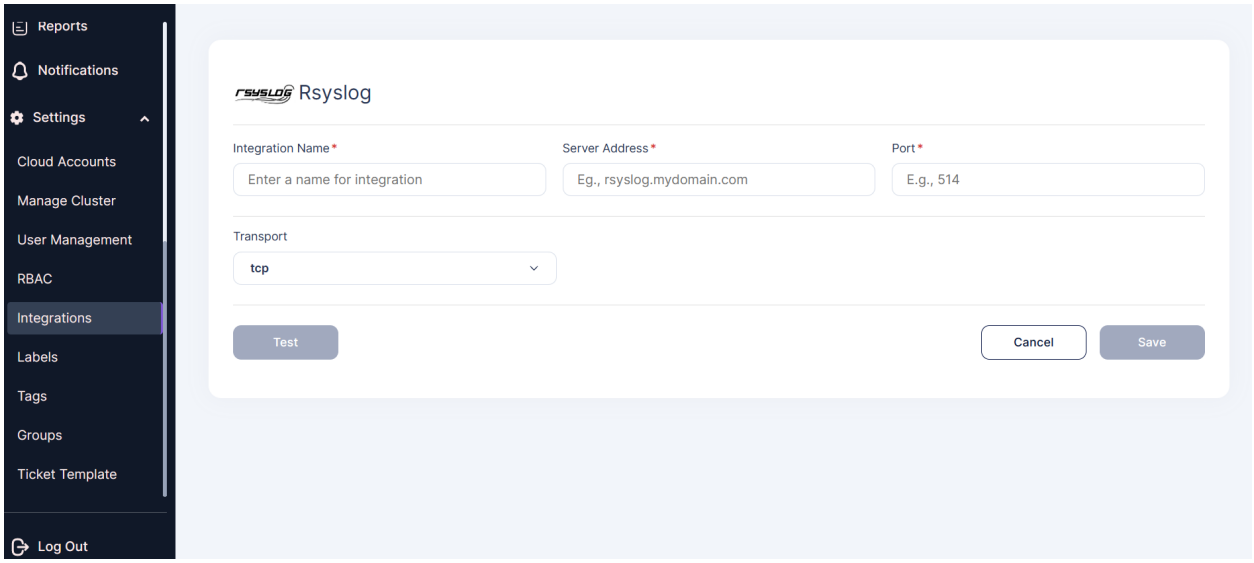
a. Prerequisites:

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

Note: To deploy the RSyslog server, follow RSyslog Documentation.

b. Steps to Integrate:

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



- Fill up the following fields:

- Integration Name: Enter the name for the integration. You can set any name of your choice. e.g., Container Security Alerts
- Server Address: Enter your RSyslog Server address here, IP address or fully qualified domain name (FQDN) of the RSyslog server e.g.,rsyslog.mydomain.com or 35.xx.xx.xx
- Port: The port number to use when sending RSyslog messages (default is UDP on port 514); you must use the same port number. e.g., 514
- Transport: Select UDP, or TCP as the method of communication with the RSyslog server

- Click Test to check the new functionality, You will receive the test message on configured RSyslog Server. -Test message Please ignore !!
- Click Save to save the Integration. You can now configure Alert Triggers for RSyslog Events

2. Integrate Notifications Tools

- Slack

Slack

Slack Integration:

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

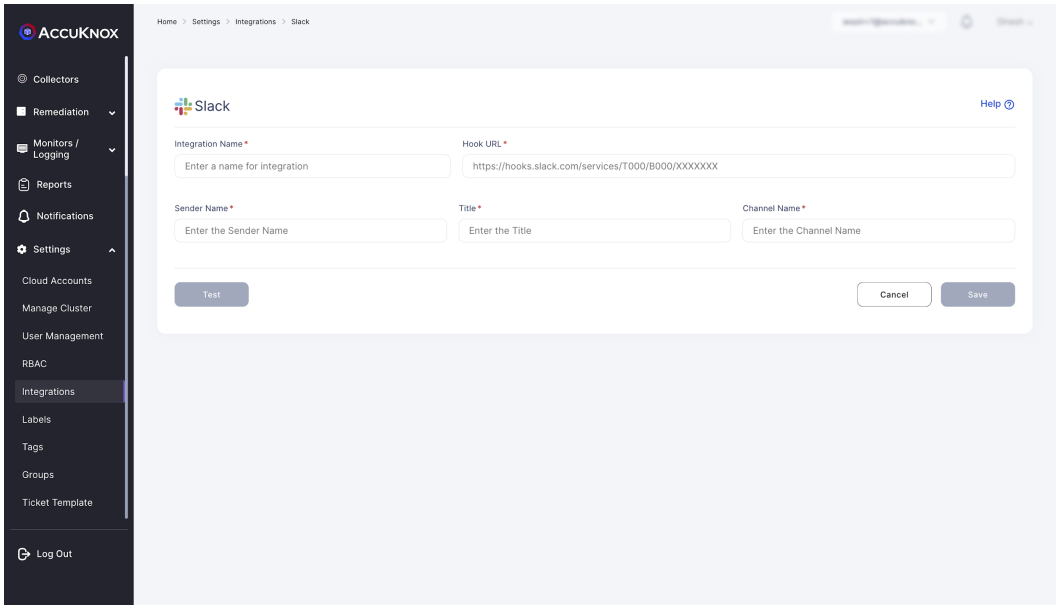
Integration of Slack:

a. Prerequisites:

You need a valid and active account in Slack. After logging into your Slack channel, you must generate a Hook URL.
Note: To generate a Hook URL follow the steps, [Webhooks-for-Slack].

b. Steps to Integrate:

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



- Fill up the following fields:

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

3. Integrate Ticketing Tools

- Jira cloud
- fresh service

Jira Integration

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

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

Integration of JIRA:

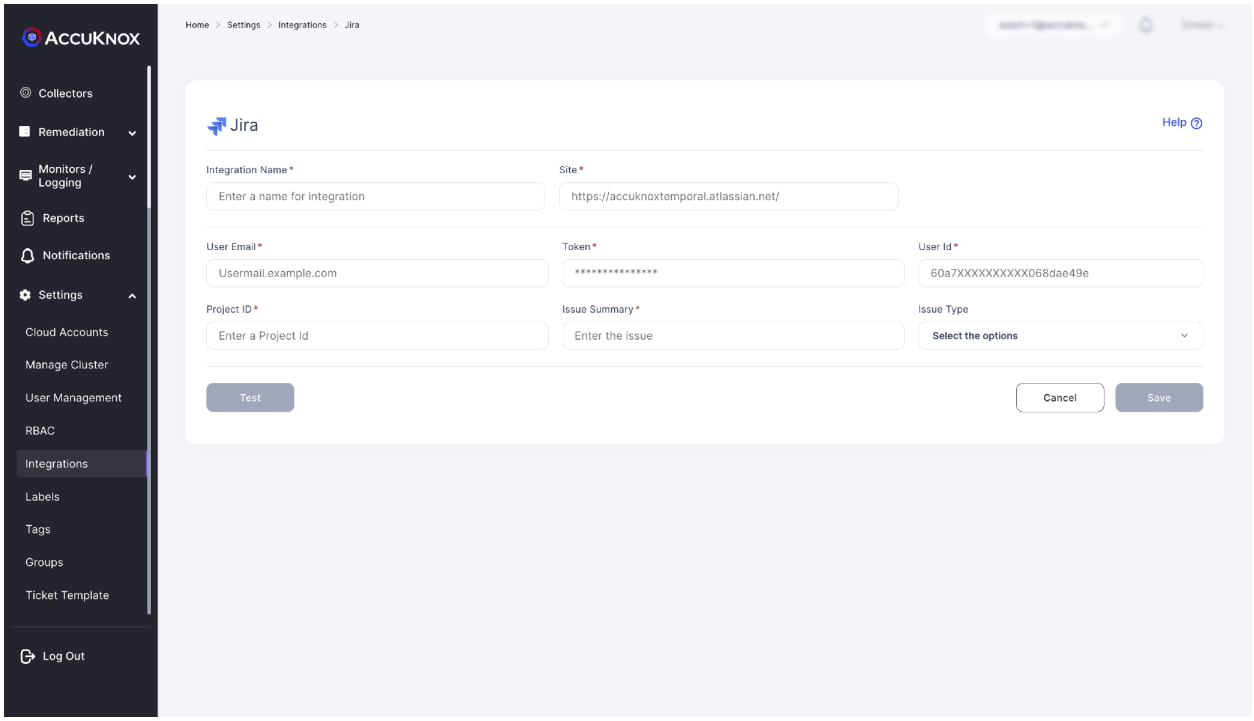
Prerequisites

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

JIRA integration for CWPP:

Steps to Integrate:

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



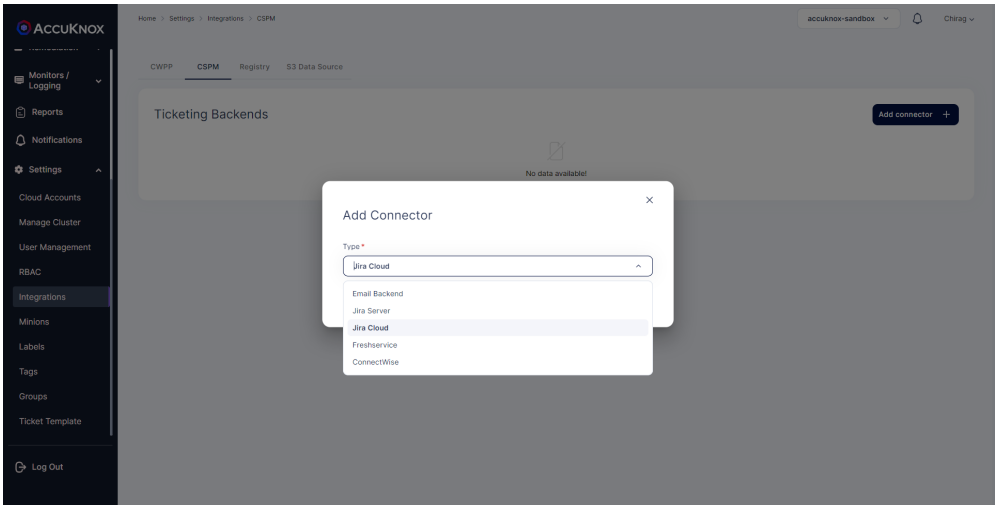
- Enter the following details to configure JIRA.
- Integration Name: Enter the name for the integration. You can set any name. e.g., Test JIRA
- Site: Enter the site name of your organization. e.g., https://jiratest.atlassian.net/

- 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., kRVxxxxxxxxxxxx39
- User ID: Enter your Jira user ID here. You can visit the people section and search your name to see the User ID. For more details check here. e.g., 5bbxxxxxxxxx0103780
- Project ID: Enter your Project key here, each project in an organization starts with some key value and is case-sensitive. Breakdown of a Jira ticket to identify Project ID: https://[JIRA-SITE]/browse/[PROJECT ID]-1414, e.g., DEVSECOPS
- Issue Summary: Enter the summary for the JIRA tickets to be viewed in each JIRA ticket created. e.g., Issues generated from High Severity Incidents on the onboarded cluster.
- Issue Type: You can choose from the dropdown. i.e., Story and Bug
- Click Test to check if the entered details are being validated, If you receive Test Successful, you have entered valid JIRA credentials.
- Click Save to save the Integration.

JIRA integration for CSPM:

Steps to Integrate:

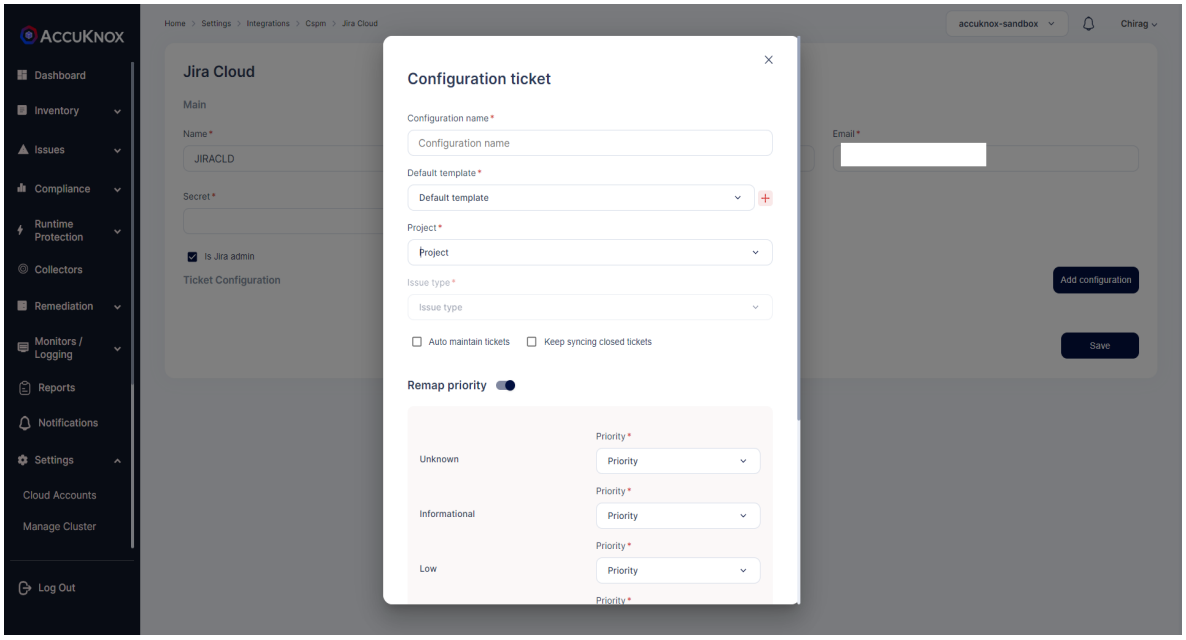
- Go to Channel Integration -> CSPM.
- Click on add the Connector and select JIRA Cloud



Enter the following details to configure JIRA.

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

- Site: Enter the site name of your organization. e.g., https://jiratest.atlassian.net/
- User Email: Enter your Jira account email address here.e.g., jira@organisation.com
- Token: Enter the generated Token here from https://id.atlassian.com/manage-profile/security/api-tokens. .e.g., kRVxxxxxxxxxxxx39



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

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

You can now configure Alert Triggers for JIRA.

Freshservice

Freshservice Integration:

Integrate AccuKnox with Freshservice and receive AccuKnox alert notifications in your Freshservice accounts. With this integration, you can automate the process of generating Freshservice “Problem alerts“ with your existing security workflow.
To set up this integration, you need to coordinate with your Freshservice administrator and gather the inputs needed to enable communication between AccuKnox and Freshservice.

Integration of Freshservice:

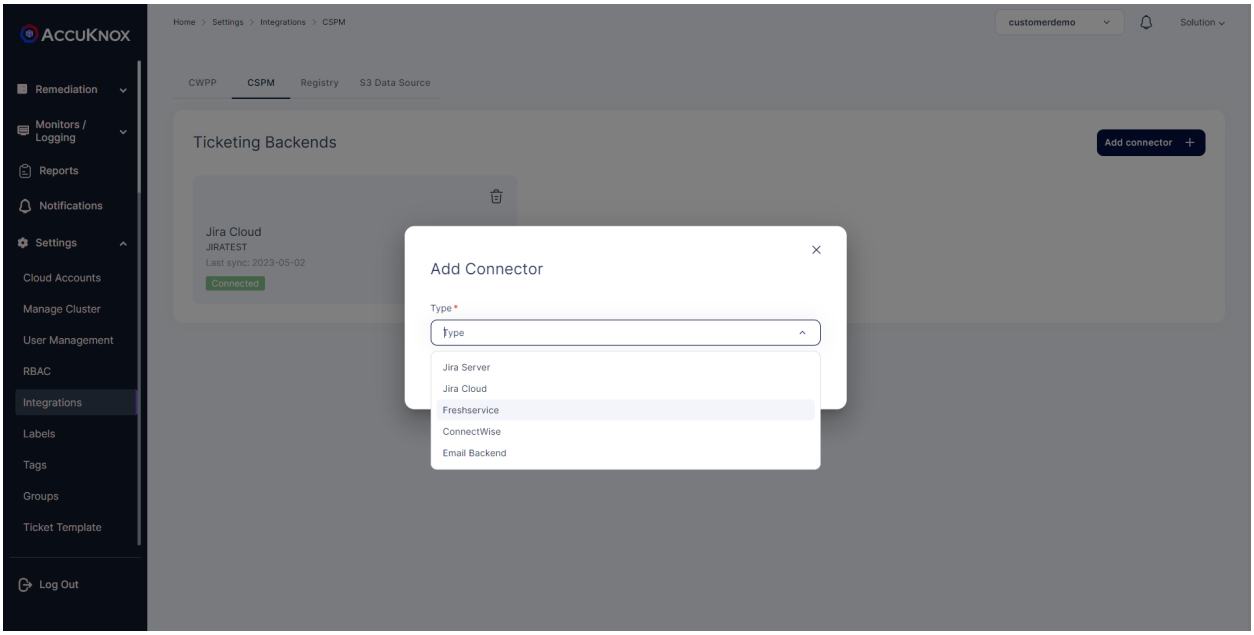
a. Prerequisites

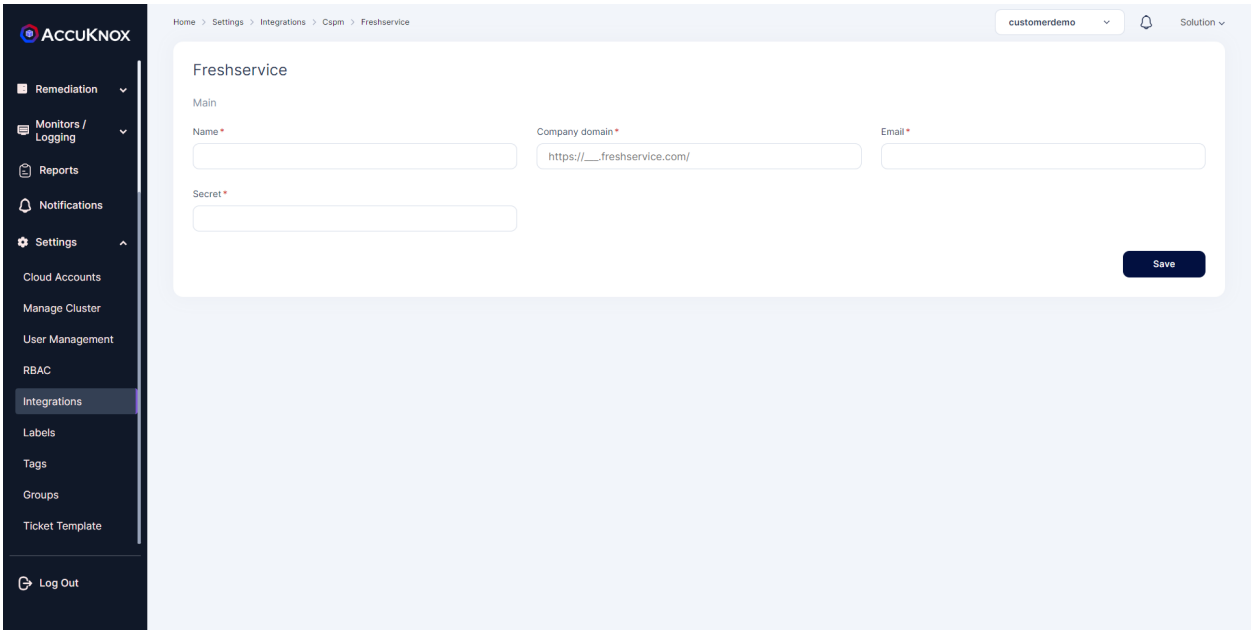
- You need a Company domain, Email & API key (secret) for this integration.
- You can find your API key in profile settings in the right side column.

b. Steps to Integrate:

- Go to Channel Integration -> CSPM.

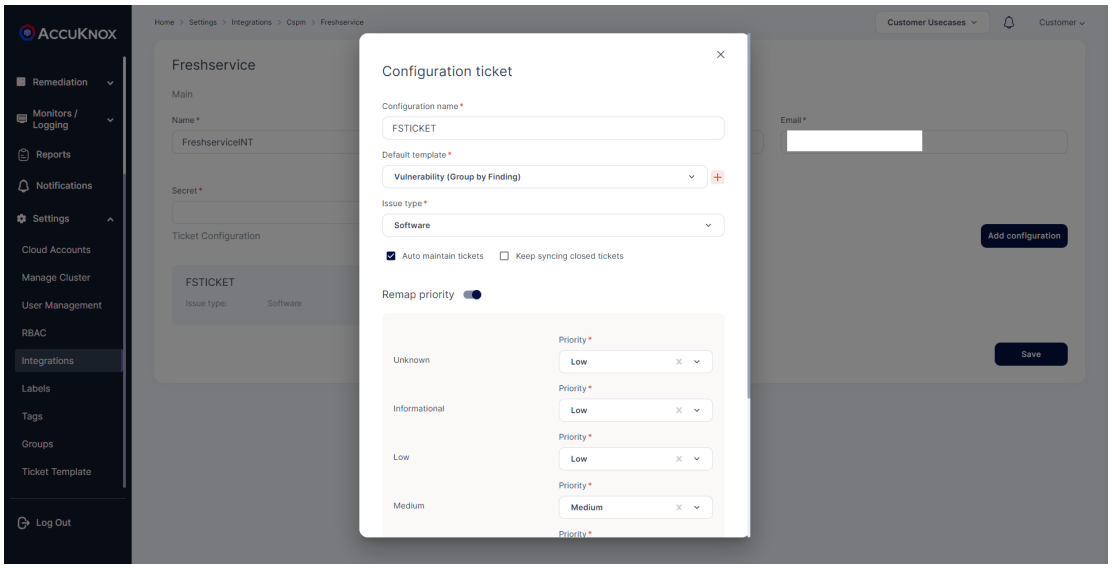
- Click on Add the connector and select Freshservice





Enter the following details to configure Fresh Service.

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



Click on the Freshservice ticketing backend to add configuration.

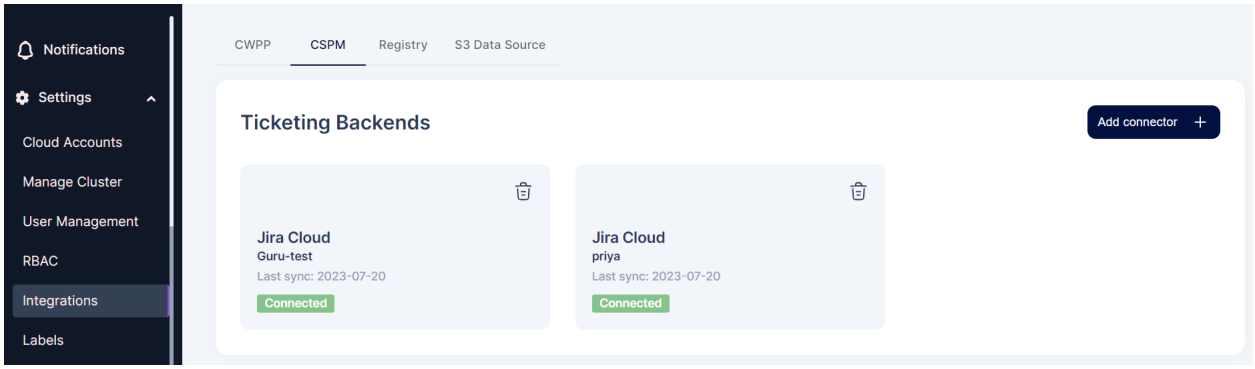
Here Enter the following details:

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

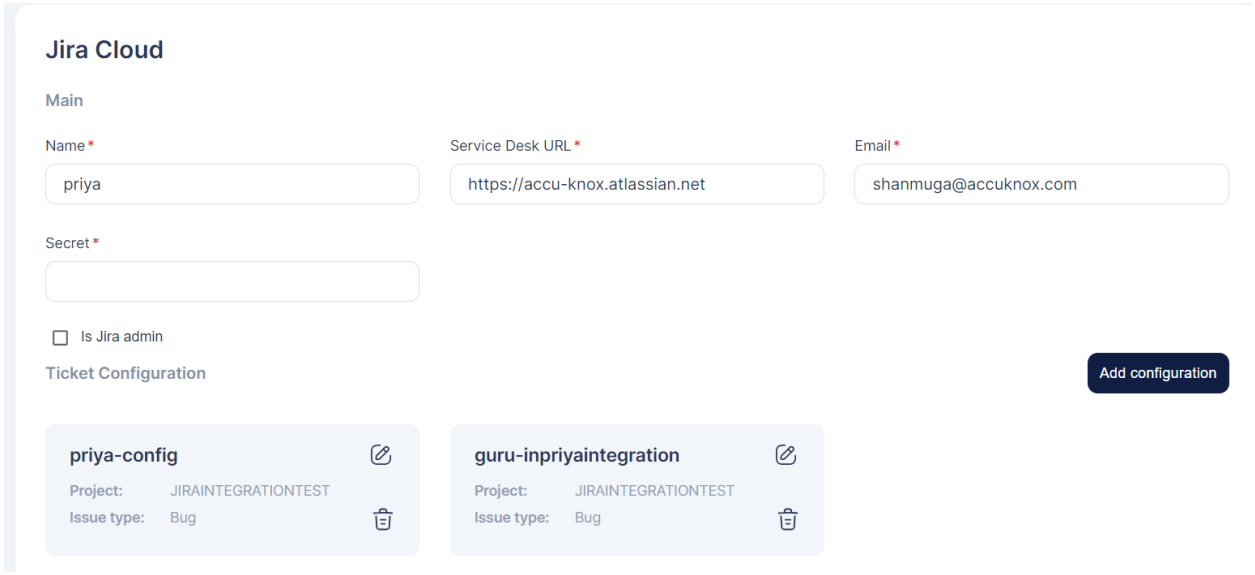
You can now configure Alert Triggers for Freshservice.

Creating Ticket Configuration

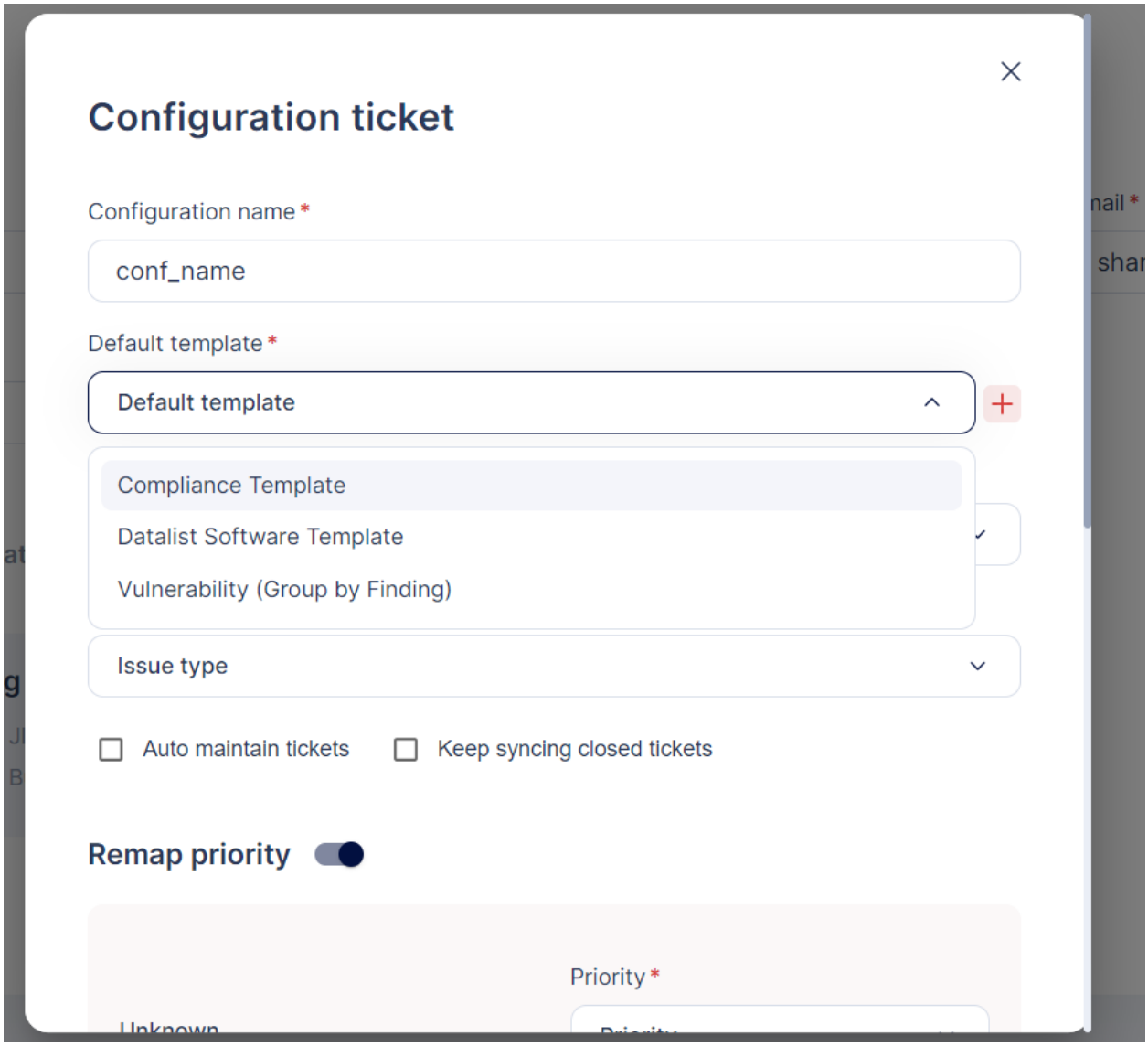
- To create a ticket configuration, navigate to Integrations under Settings and click on the CSPM tab. This will show all the ticketing backends that have been integrated:



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



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



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

4. Integrate Registries

Registry

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

- To Onboard Registry click here

Amazon Elastic Container Registry:

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

Google Container Registry:

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

Nexus Registry:

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

DockerHub Registry:

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

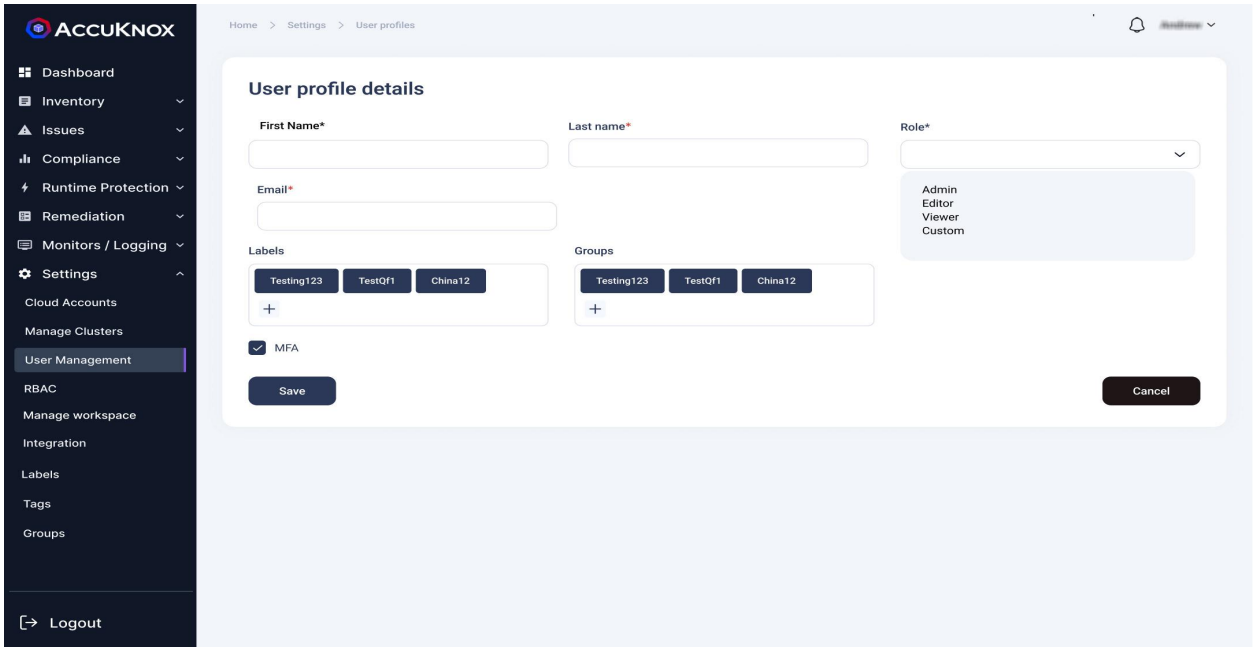
User Management

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

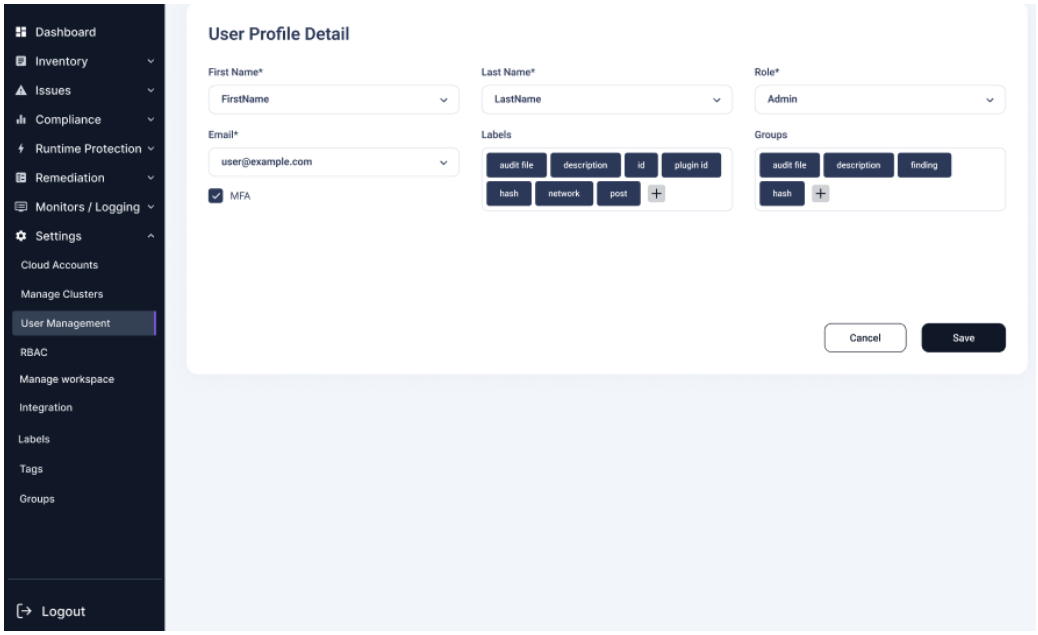
Invite folks to the workspace

Inviting new users:

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

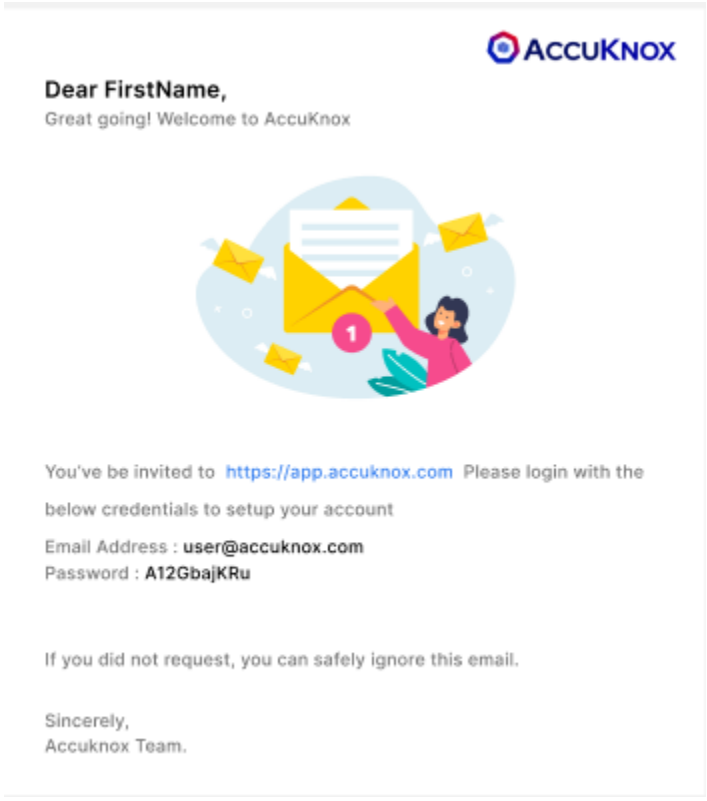


Step 2: Fill in the necessary details for the user invite

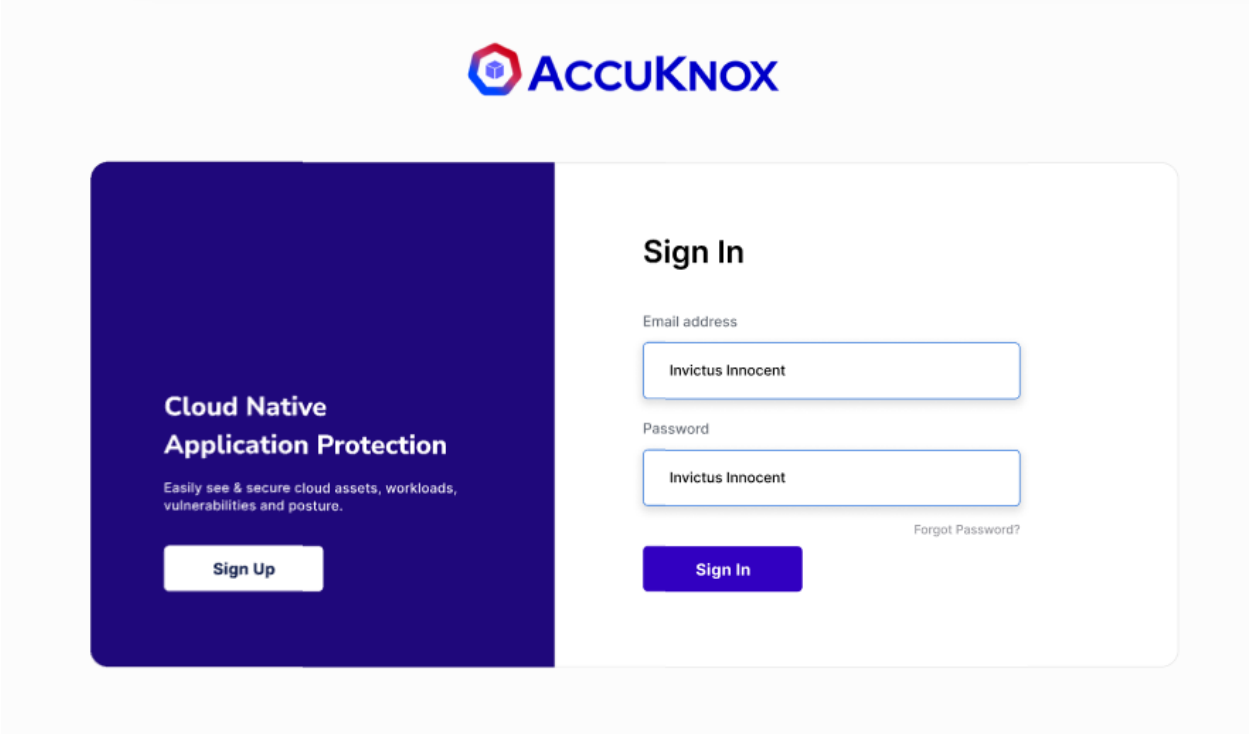


Step 3:

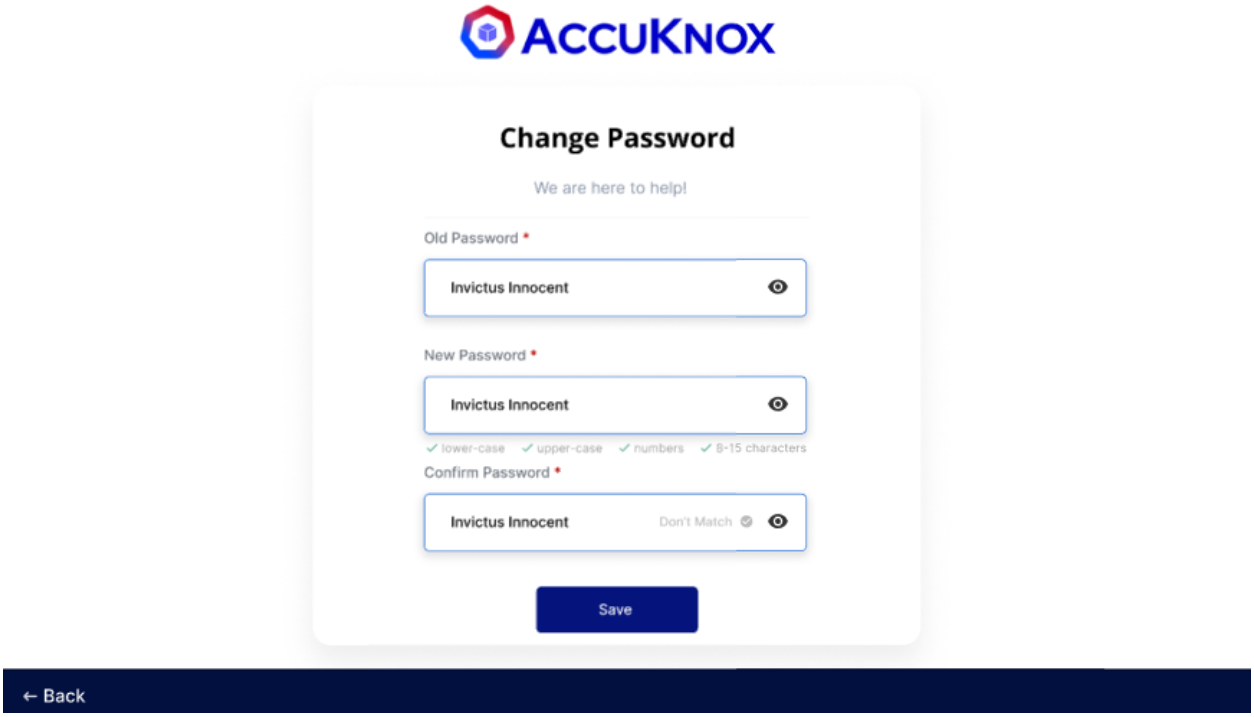
After we click save, the new user will be getting a user invite email with username, password, and sign in link to the mentioned email id



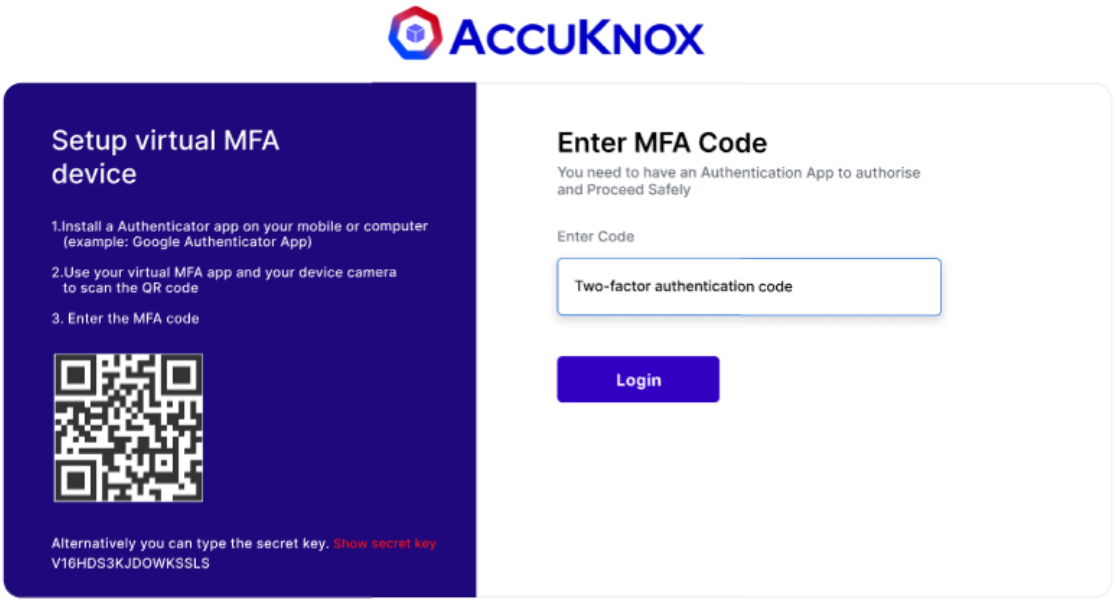
Step 4: The user needs to sign in with the credentials provided in the email.



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



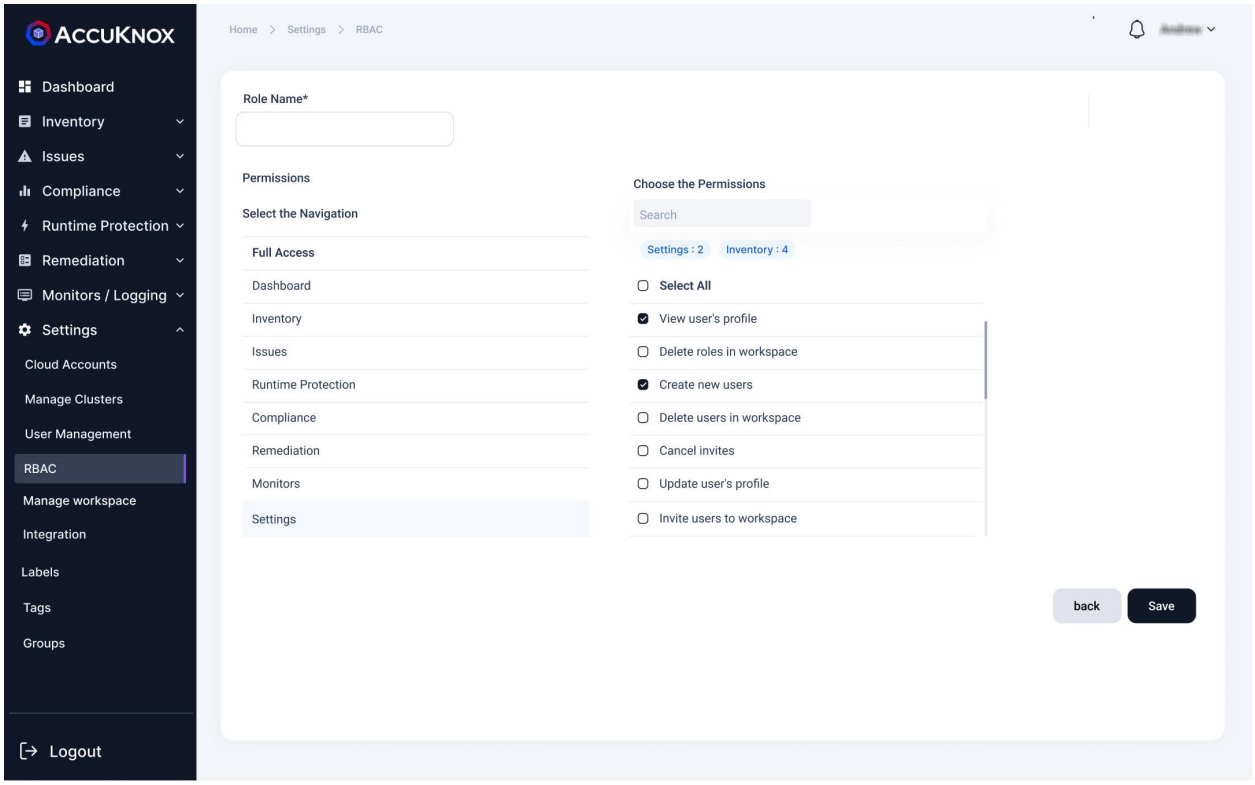
Step 6: Once the password is changed, the user will need to set MFA for his account using any Authenticator Application.

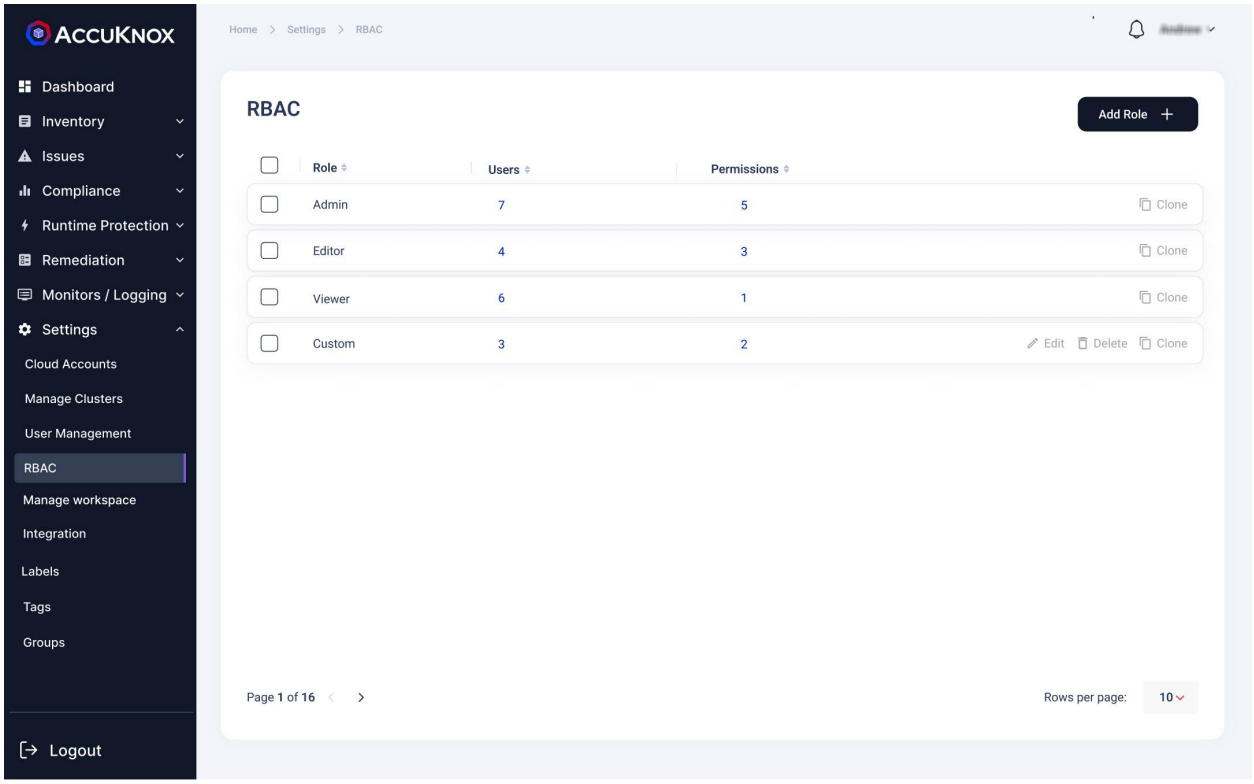


Step 7: After successful login, the user will be directed to the Dashboard screen.

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.

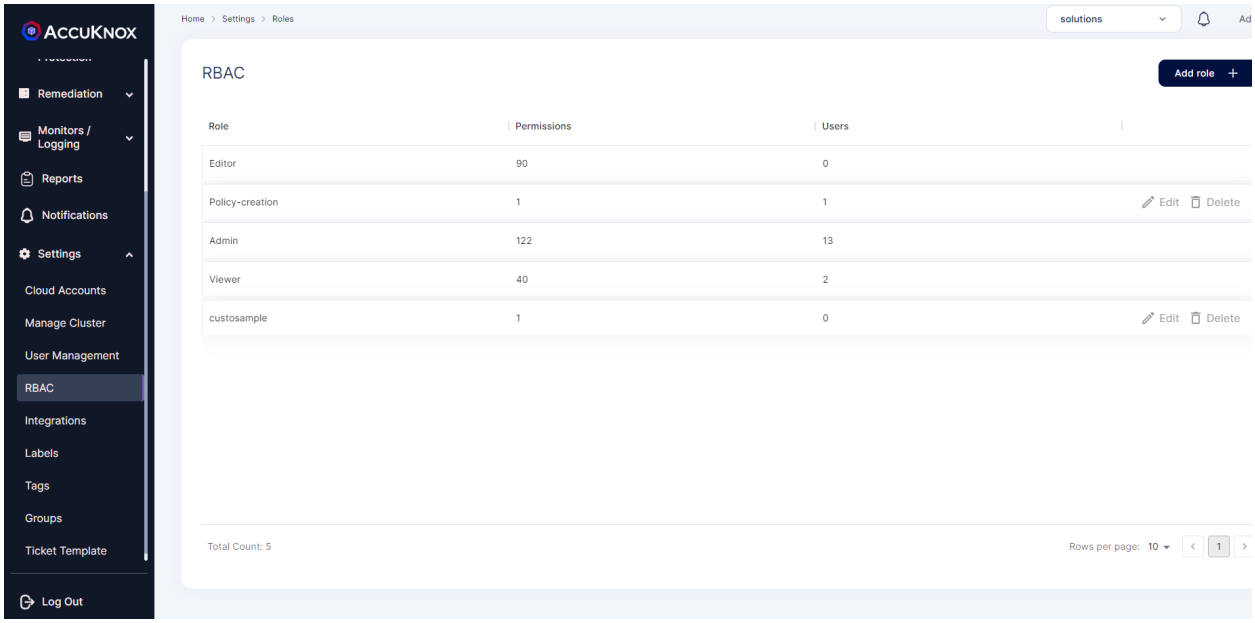




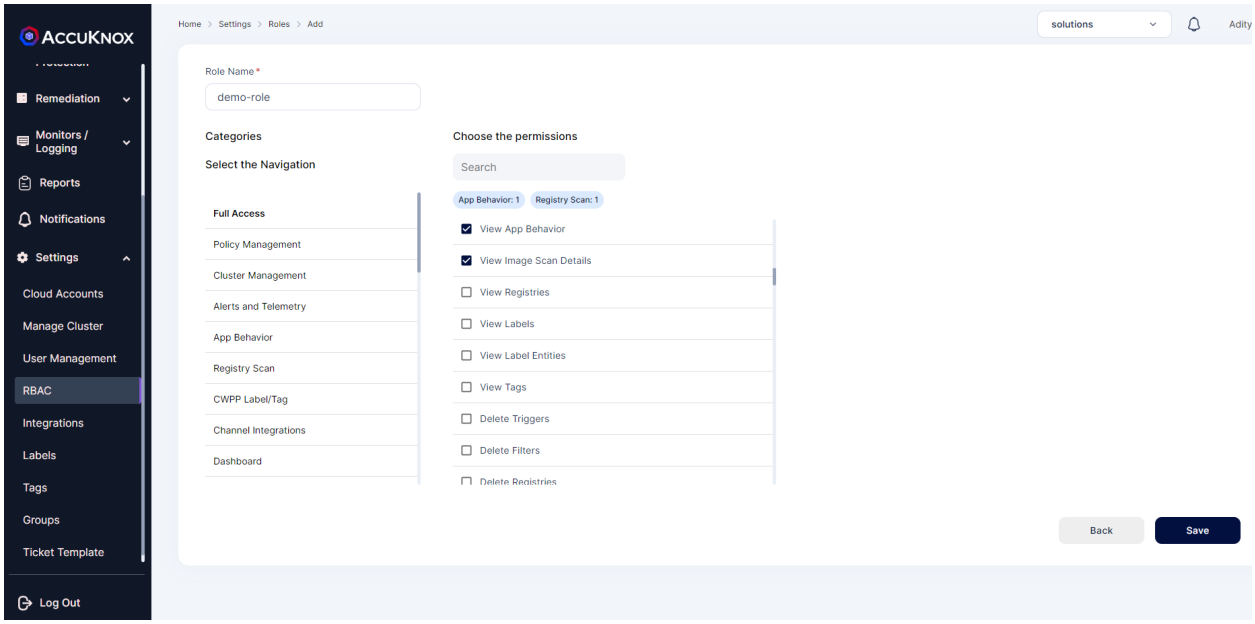
Create Roles and Assign Users

Steps:

- Click on Add Role



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



- 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