



USER MANUAL

Detailed guide to walk you through the
cloud security journey



A large, semi-transparent purple polygonal shape is positioned in the center-right area of the page. It has several sharp edges and points, creating a sense of depth and complexity. Dashed purple lines extend from the vertices of the polygon towards the bottom corners of the page, forming a triangular frame.

Protect every cloud native
application, Protect everywhere

-=AccuKnox Manual=-

Table of Contents

Getting Started Guide	8
1. Assets Count	8
1.1 Cloud	8
1.1.1 AWS	8
1.1.2 Azure	11
1.1.3 GCP	14
1.2 Container Images Counts	16
1.2.1 DockerHub	16
1.2.2 AWS ECR	16
1.2.3 GCR	16
1.2.4 ACR	17
2. CSPM Prerequisites	18
2.1 AWS	18
2.2 AZURE	20
2.3 GCP	29
3. Cloud Onboarding	36
3.1 AWS Onboarding	36
3.2 Azure Onboarding	39
3.3 GCP Onboarding	42
3.4 Cloud Account Deboarding	44
4. CWPP Prerequisites	45
4.1 Minimum Resource required	45
4.2 AccuKnox Agents	45
5. Cluster Onboarding	51
6. Cluster Offboarding	58
7. VM Onboarding with Systemd/Docker Mode	60
7.1 Systemd	60
7.1.1 Container Protection Requirements (Optional)	61
7.1.2 Resource Requirements	61
7.1.3 Network Requirements	62
7.1.4 Onboarding	63
7.1.5 Onboarding Control Plane	64
7.1.6 Onboarding Worker Nodes	65

7.1.7 Deboarding	66
7.2 Docker	67
7.2.1 Resource Requirements	67
7.2.2 Network Requirements	67
7.3 Onboarding	70
7.3.1 Install knoxctl/accuknox-cli	70
7.3.2 Onboarding Control Plane	70
7.3.3 Onboarding Worker Nodes	71
7.4 Deboarding	72
8. Registry Onboarding	73
8.1 Azure Container Registry	73
8.1.1 Steps to generate credentials for onboarding ACR	73
8.1.2 Steps to onboard the registry on AccuKnox SaaS	75
8.2 Harbor Registry	77
8.2.1 Prerequisites for Harbor Registry Onboarding in Accuknox:	77
8.2.2 Steps to Onboard Harbor Registry on Accuknox:	79
8.3 Deboarding a Registry	83
9. AccuKnox CNAPP Dashboard Widgets	84
9.1 CWPP Widgets	84
9.1.1 Top 5 cluster findings Widget	84
9.1.2 Findings by Asset Categories Widget	84
9.1.3 K8S Security Metrics Widgets	85
9.1.4 Workload Alerts Widgets	85
9.1.5 Workloads without any Policy Applied Widget	86
9.1.6 K8s Resource SummaryWidget	86
9.1.7 Cluster Connection Status Widget	87
9.1.8 Workloads without Network Policies Widget	87
9.1.9 Top 5 K8s CIS Findings Widget	88
9.1.10 Block based Policies with Associated Alerts Widget	88
9.2 CSPM	89
9.2.1 Top 3 cloud accounts with failed controls Widget	89
9.2.2 Top 10 risk associated to cloud accounts Widget	89
9.2.3 Findings Trends Widget	90
9.2.4 Cloud Accounts Widget	90
9.2.5 Findings Widget	91
9.3 KIEM	91
9.3.1 Kiem Risk Assessment Widget	91

9.3.2 KIEM Findings by Asset type Widget	92
9.3.3 Top 5 most critical findings Widget	92
9.4 Cloud Misconfiguration Widget	93
Cloud Account Risk Assessment Widget	93
9.5 Container images Widgets	93
9.5.1 Image Severity Distribution Widget	93
9.5.2 Image Risk Assessment Widget	94
9.6 Tickets Widgets	94
Tickets by status Widget	94
10. CSPM (Cloud Security Posture Management)	95
10.1 Asset Inventory	95
10.1.1 How to find a particular asset	95
10.1.2 How to group assets	97
10.1.3 How to search asset by label	100
10.2 Misconfigurations	101
10.2.1 Where to find misconfigurations	101
10.2.2 How to group by Asset and find misconfiguration	102
10.2.3 How to group by Findings	105
10.2.4 How to group by criticality and Status	107
10.2.5 How to create a Ticket	111
10.3 Issues/Findings	116
10.3.1 Group findings by source and severity	116
10.3.2 How to group by Findings and severity	117
10.3.3 How to group by Asset and severity	118
10.4 Baselines	120
10.4.1 How to create a Baseline out of a data source	120
10.4.2 How to compare baselines	122
10.5 Compliance	124
10.5.1 How to get Compliance for Cloud Assets	124
10.6 Remediation - Fix Problems/Create Tickets	126
10.7 CSPM Reports	128
10.8 Rules Engine	130
11. ASPM (Application Security Posture Management)	133
11.1 SAST	133
11.1.1 Integrating SonarQube SAST with AccuKnox in a GitLab CI/CD Pipeline	133
11.1.2 Pre-requisites	133
11.1.3 Steps for Integration	133

11.1.4 Initial CI/CD Pipeline Without AccuKnox Scan	137
11.1.5 CI/CD Pipeline After AccuKnox Integration	137
11.1.6 View Results in AccuKnox SaaS	137
11.2 DAST	139
11.2.1 Gitlab DAST Scan	139
11.2.2 Pre-requisites	139
11.2.3 Steps for Integration	139
11.2.4 Initial CI/CD Pipeline Without AccuKnox Scan	142
11.2.5 CI/CD Pipeline After AccuKnox Scan Integration	142
11.2.6 View Results in AccuKnox SaaS	142
11.3 IaC GitLab Scan	145
11.3.1 Integrating IaC with AccuKnox in a GitLab CI/CD Pipeline	145
11.3.2 Pre-requisites	145
11.3.3 Steps for Integration	145
11.3.4 Initial CI/CD Pipeline Without AccuKnox IaC Scan	149
11.3.5 CI/CD Pipeline After AccuKnox IaC Scan Integration	149
11.3.6 View Results in AccuKnox SaaS	149
11.4 GitLab IaC Scan via Accuknox	152
11.4.1 Prerequisites	152
11.4.2 Configuring Code Source in Accuknox	153
11.4.3 Setting Up IaC Configuration	154
11.4.4 Viewing and Managing IaC Findings on Accuknox	155
11.5 Container Scan Use Case	156
11.5.1 Scenario Before Integrating AccuKnox	156
11.5.2 Scenario After Integrating AccuKnox	157
11.5.3 Remediation and Rescan	159
11.5.4 Steps needed to be taken for integration	160
12. KSPM (Kubernetes Security Posture Management)	165
12.1 CIS Benchmarking Compliance Scan Onboarding	165
12.2 Cluster Misconfiguration Scanning	171
12.2.1 Remediation	173
12.2.2 Vulnerability Management Lifecycle	174
12.3 Kubernetes Identity and Entitlement Management (KIEM)	177
12.3.1. Onboarding Process	177
12.3.2 Install KIEM Agents	177
12.3.3 Post-Onboarding Steps	177
12.3.4 Permissions Overview	178

12.3.5 Key Queries	179
12.3.6 Full-text Search	180
12.3.7 Entity Exploration	181
12.3.8 Interactive Visualization	184
13. CWPP (Cloud Workload Protection Platform)	185
13.1 Cloud Workloads	185
13.1.1 How to find graph view of clusters	185
13.1.2 How to find list view of clusters	185
13.1.3 How to find details on cluster	186
13.1.4 How to get Compliance for Cloud Workload	188
13.2 App Behavior	189
13.2.1 How to interpret network graph	189
13.2.2 How to see App Behavior Telemetry	193
13.3 Runtime Protection w/ Policy Management	195
13.3.1 How to understand discover policies	195
13.3.2 How to understand Hardening policies	198
13.3.3 How to Audit application and get alerts for that	201
13.3.4 When do we say policies are stable?	203
13.3.5 What if something changes in Application?	204
13.3.6 How to create a custom Policy	208
13.3.7 How to enforce Policies and see anomalies	215
13.3.8 How to perform bulk operation on applying policies	222
13.3.9 How to Find Nodes of a VM cluster	224
14. Host Security	226
14.1 Host Scan	226
14.2 Prerequisites for Nessus Integration	226
14.3 Asset Inventory	227
14.4 Vulnerability Management	227
15. Admission Controller Support Using Knoxguard	230
15.1 Introduction	230
15.2 Prerequisite for Knoxguard Admission Controller	231
15.3 Deployment of Knoxguard	232
15.4 Policy Enforcement	233
15.5 Policy Violation and Alerts	235
15.6 Pod Security Admission Controller	236
15.7 Enabling Pod Security Admission (PSA)	237
15.8 PSA Protection Example	240

16. CWPP Report Generation	242
16.1 Regex	242
16.1.1 Rules for Regular Expression	242
16.2 Reports Configuration	244
16.2.1 On Demand Report Configuration	244
16.2.2 Scheduled Report Configuration	245
17. Integrations	248
17.1 Integrate SIEM tools	248
17.1.1 Splunk	248
a. Prerequisites:	249
b. Steps to Integrate:	249
17.1.2 AWS Cloudwatch	251
a. Prerequisites	251
b. Steps to Integrate:	251
c. Configuration of Alert Triggers:	252
d. Logs Forwarding:	253
17.1.3 Azure Sentinel Integration	253
a. Prerequisites:	253
b. Steps to Integrate:	253
17.1.4 Creating webhook using the Azure Logic App	254
a. About the logic app:	254
b. To see Logs in the Sentinel:	254
17.1.5 Rsyslog	254
a. Prerequisites:	254
b. Steps to Integrate:	255
17.2 Integrate Notifications Tools	256
17.2.1 Slack	256
a. Prerequisites:	256
b. Steps to Integrate:	256
17.3 Integrate Ticketing Tools	257
17.3.1 Jira Integration	257
a. Prerequisites	258
b. JIRA integration for CWPP:	258
17.3.2 JIRA integration for CSPM:	259
17.3.3 ServiceNow Integration	262
a. Prerequisites	262
b. Steps for integration	262

17.3.4 Freshservice Integration	262
a. Prerequisites	262
b. Steps to Integrate:	263
17.4 Creating Ticket Configuration	267
17.5 Email Integration	269
18. User Management	271
18.1 Inviting a New User	271
18.2 User Receives Invitation	273
18.3 User Login Options	273
Option A: Traditional Login	273
Option B: Single Sign-On (SSO) with Google	274
18.4 Assign RBAC	275
18.5 Create Roles and Assign Users	276
19. Ticketing Procedures	278
19.1 How to raise an AccuKnox support ticket?	278
19.2 How to track the issue resolution status?	281
20. FAQs	283
20.1 AccuKnox FAQs	283
20.2 Bonus Questions	289
References:	291

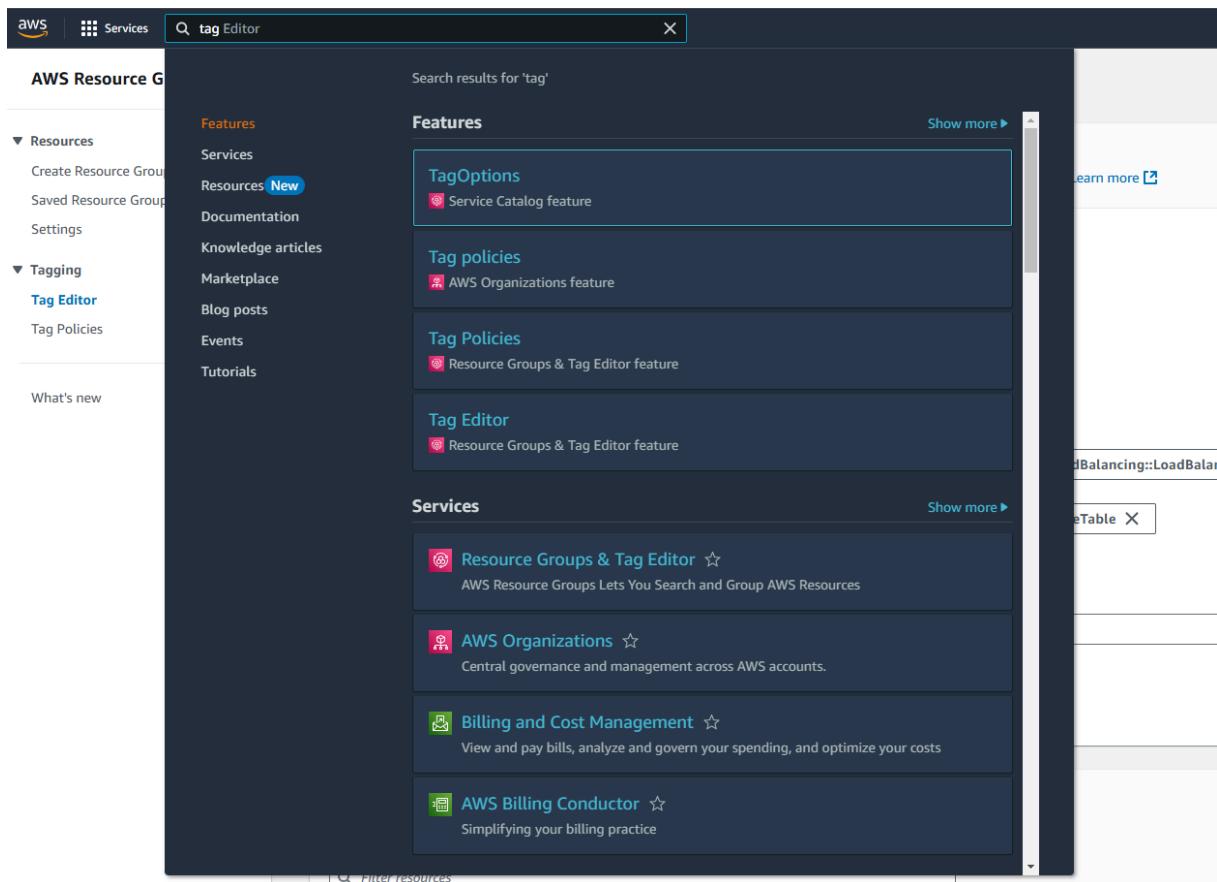
Getting Started Guide

1. Assets Count

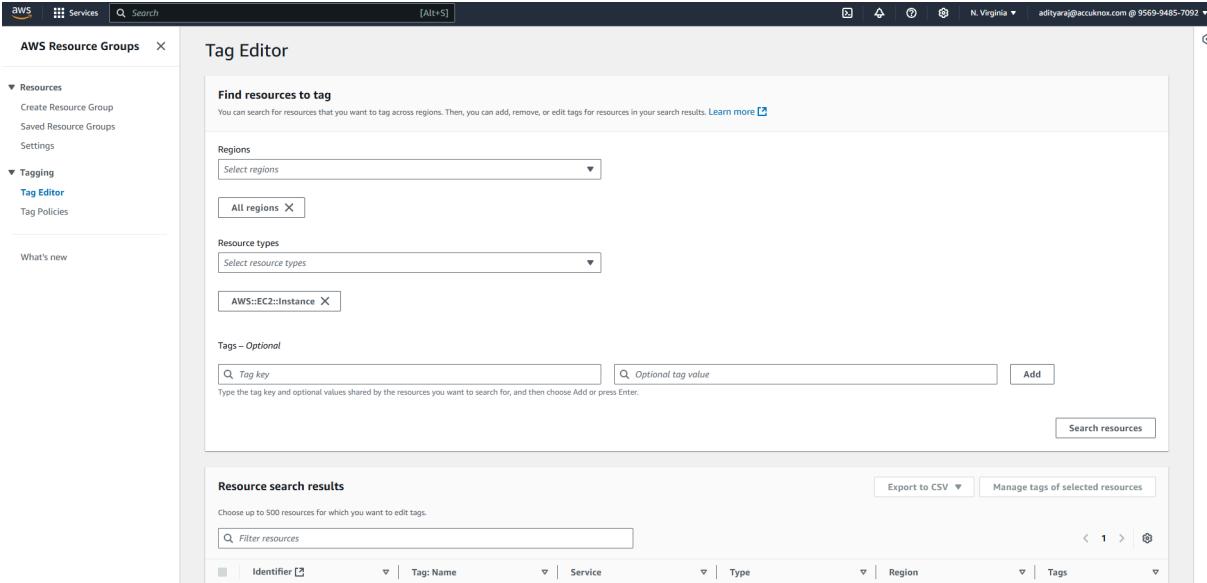
1.1 Cloud

1.1.1 AWS

Step 1: Search for Tag Editor



Step 2: In the tag editor screen, filters can be applied by passing them in the URL



The screenshot shows the AWS Tag Editor interface. On the left, there's a sidebar with 'AWS Resource Groups' and 'Tagging' sections, with 'Tag Editor' selected. Below that are 'What's new' and 'Settings' links. The main area is titled 'Tag Editor' and has a sub-section 'Find resources to tag'. It includes fields for 'Regions' (set to 'All regions') and 'Resource types' (set to 'AWS::EC2::Instance'). A 'Tags - Optional' section allows adding key-value pairs. At the bottom, there's a 'Resource search results' table with columns for Identifier, Tag: Name, Service, Type, Region, and Tags.

Paste the following snippet at the end of the URL in the browser:

```
#query=regions:!('AWS::AllSupported'),resourceTypes:!('AWS::Lambda::Function','AWS::CloudFront::Distribution','AWS::CloudFront::StreamingDistribution','AWS::IAM::InstanceProfile','AWS::IAM::ManagedPolicy','AWS::EC2::VPC','AWS::EC2::Subnet','AWS::EC2::NetworkAcl','AWS::EC2::NetworkInterface','AWS::ElasticLoadBalancingV2::LoadBalancer','AWS::ElasticLoadBalancing::LoadBalancer','AWS::EC2::EIP','AWS::EC2::SecurityGroup','AWS::EC2::RouteTable','AWS::Route53::Domain','AWS::Route53::HealthCheck','AWS::RDS::DBSubnetGroup','AWS::EC2::Instance','AWS::ECS::Cluster','AWS::EKS::Cluster','AWS::ElastiCache::CacheCluster','AWS::ElastiCache::Snapshot','AWS::S3::Bucket','AWS::EC2::Volume','AWS::EC2::Snapshot','AWS::RDS::DBInstance','AWS::RDS::DBCluster'),tagFilters:!(),type:TAG_EDITOR_1_0
```

Eg:

```
https://us-east-1.console.aws.amazon.com/resource-groups/tag-editor/find-resources?region=us-east-1#query=regions:!\('AWS::AllSupported'\),resourceTypes:!\('AWS::Lambda::Function','AWS::CloudFront::Distribution','AWS::CloudFront::StreamingDistribution','AWS::IAM::InstanceProfile','AWS::IAM::ManagedPolicy','AWS::EC2::VPC','AWS::EC2::Subnet','AWS::EC2::NetworkAcl','AWS::EC2::NetworkInterface','AWS::ElasticLoadBalancingV2::LoadBalancer','AWS::ElasticLoadBalancing::LoadBalancer','AWS::EC2::EIP','AWS::EC2::SecurityGroup','AWS::EC2::RouteTable','AWS::Route53::Domain','AWS::Route53::HealthCheck','AWS::RDS::DBSubnetGroup','AWS::EC2::Instance','AWS::ECS::Cluster','AWS::EKS::Cluster','AWS::ElastiCache::CacheCluster','AWS::ElastiCache::Snapshot','AWS::S3::Bucket','AWS::EC2::Volume','AWS::EC2::Snapshot','AWS::RDS::DBInstance','AWS::RDS::DBCluster'\),tagFilters:!\(\),type:TAG\_EDITOR\_1\_0
```

```
able', 'AWS::Route53::Domain', 'AWS::Route53::HealthCheck', 'AWS::RDS::DBSubnetGroup', 'AWS::EC2::Instance', 'AWS::ECS::Cluster', 'AWS::EKS::Cluster', 'AWS::ElastiCache::CacheCluster', 'AWS::ElastiCache::Snapshot', 'AWS::S3::Bucket', 'AWS::EC2::Volume', 'AWS::EC2::Snapshot', 'AWS::RDS::DBInstance', 'AWS::RDS::DBCluster'), tagFilters:!(), type:TAG_EDITOR_1_0
```

Resource types

Select resource types

AWS::Lambda::Function X AWS::CloudFront::Distribution X AWS::CloudFront::StreamingDistribution X AWS::IAM::InstanceProfile X AWS::IAM::ManagedPolicy X

AWS::EC2::VPC X AWS::EC2::Subnet X AWS::EC2::NetworkAcl X AWS::EC2::NetworkInterface X AWS::ElasticLoadBalancingV2::LoadBalancer X

AWS::ElasticLoadBalancing::LoadBalancer X AWS::EC2::EIP X AWS::EC2::SecurityGroup X AWS::EC2::RouteTable X AWS::Route53::Domain X

AWS::Route53::HealthCheck X AWS::RDS::DBSubnetGroup X AWS::EC2::Instance X AWS::ECS::Cluster X AWS::EKS::Cluster X AWS::ElastiCache::CacheCluster X

AWS::ElastiCache::Snapshot X AWS::S3::Bucket X AWS::EC2::Volume X AWS::EC2::Snapshot X AWS::RDS::DBInstance X AWS::RDS::DBCluster X

Tags – Optional

Tag key Tag value Add

Type the tag key and optional values shared by the resources you want to search for, and then choose Add or press Enter.

Search resources

Resource search results (1938)

Choose up to 500 resources for which you want to edit tags.

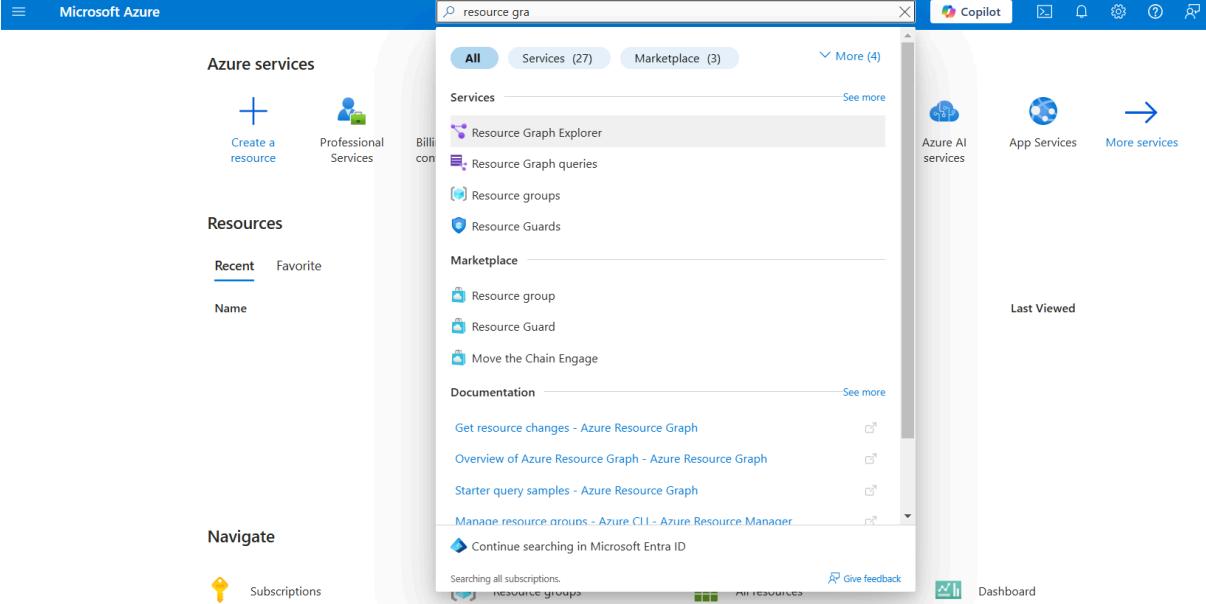
Identifier	Tag: Name	Service	Type	Region	Tags
vpc-00c8ce89bf3cce433	(not tagged)	EC2	VPC	ap-southeast-1	-
vpc-077e684bb6773b467	(not tagged)	EC2	VPC	ap-northeast-3	-

Export 1938 resources to CSV ▾ Manage tags of selected resources

Step 3: Click on Export to CSV.

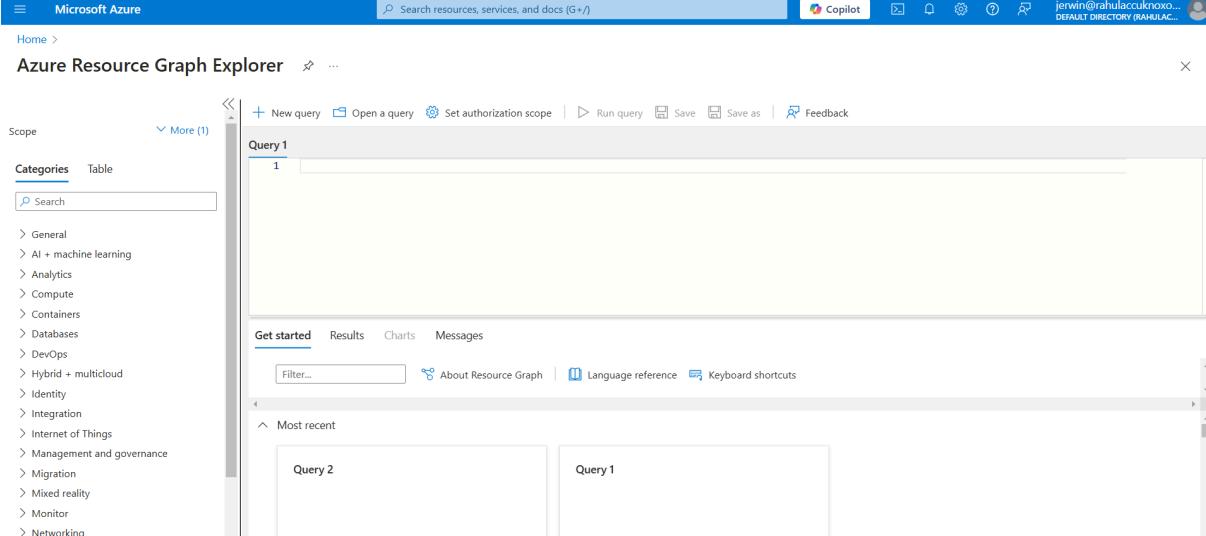
1.1.2 Azure

Step 1: Search for Resource graph explorer



The screenshot shows the Microsoft Azure portal's search interface. The search bar at the top contains the query "resource gra". Below the search bar, there are three main tabs: "All", "Services (27)", and "Marketplace (3)". The "All" tab is selected. The search results are categorized under "Services", "Marketplace", and "Documentation". Under "Services", the "Resource Graph Explorer" is listed as the top result. Other visible items include "Resource Graph queries", "Resource groups", and "Resource Guards". Under "Marketplace", there are links for "Resource group", "Resource Guard", and "Move the Chain Engage". Under "Documentation", there are links for "Get resource changes - Azure Resource Graph", "Overview of Azure Resource Graph - Azure Resource Graph", "Starter query samples - Azure Resource Graph", and "Manage resource groups - Azure CLI - Azure Resource Manager". On the right side of the search results, there are sections for "Azure AI services", "App Services", and "More services". At the bottom of the search results, there is a link to "Continue searching in Microsoft Entra ID".

Step 2: In the resource graph explorer screen, create a new query



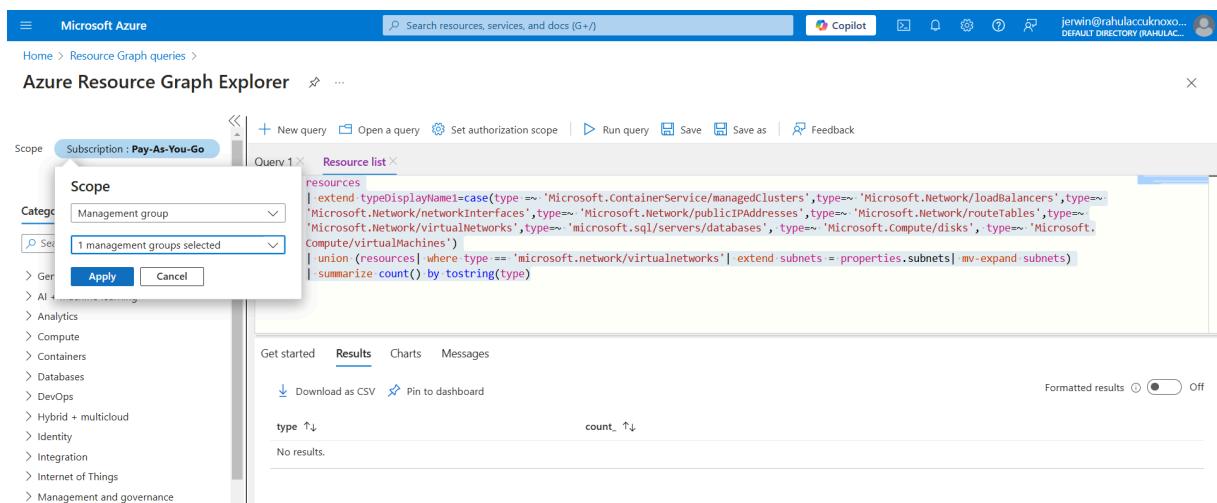
The screenshot shows the Azure Resource Graph Explorer interface. The title bar says "Azure Resource Graph Explorer". The left sidebar has a "Scope" section with "Categories" selected, showing a list of categories like General, AI + machine learning, Analytics, Compute, Containers, Databases, DevOps, Hybrid + multicloud, Identity, Integration, Internet of Things, Management and governance, Migration, Mixed reality, Monitor, and Networking. Below the categories is a search bar. The main area is titled "Query 1" and contains a single digit "1". At the top of the main area are buttons for "+ New query", "Open a query", "Set authorization scope", "Run query", "Save", "Save as", and "Feedback". Below the main query area are tabs for "Get started", "Results", "Charts", and "Messages". The "Results" tab is active. At the bottom of the main area, there is a "Most recent" section showing two previous queries: "Query 2" and "Query 1".

Add the following query to the resource graph explorer:

```
resources
| extend typeDisplayName1=case(type =~
```

```
'Microsoft.ContainerService/managedClusters',type=~
'Microsoft.Network/loadBalancers',type=~
'Microsoft.Network/networkInterfaces',type=~
'Microsoft.Network/publicIPAddresses',type=~
'Microsoft.Network/routeTables',type=~
'Microsoft.Network/virtualNetworks',type=~
'microsoft.sql/servers/databases', type=~ 'Microsoft.Compute/disks',
type=~ 'Microsoft.Compute/virtualMachines')
| union (resources| where type == 'microsoft.network/virtualnetworks'|
extend subnets = properties.subnets| mv-expand subnets)
| summarize count() by tostring(type)
```

Step 3: Click on **More** at the left side and set the scope for the query as required

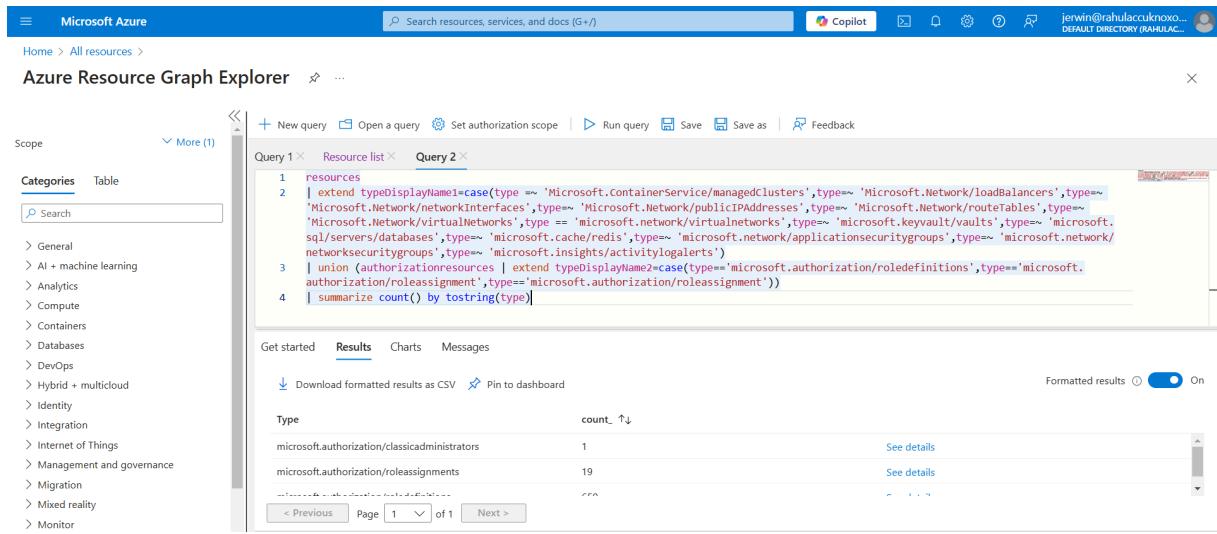


The screenshot shows the Azure Resource Graph Explorer interface. In the top navigation bar, it says "Microsoft Azure" and "Search resources, services, and docs (G+/" followed by user information "jerwin@rahulaccuknoxo.."). Below the navigation is the "Azure Resource Graph Explorer" title bar with a "Scope" dropdown set to "Subscription : Pay-As-You-Go". The main area contains a query editor with the following text:

```
Scope
Subscription : Pay-As-You-Go
Query 1
Resource list
resources
| extend typeDisplayName=case(type =~ 'Microsoft.ContainerService/managedClusters',type=~ 'Microsoft.Network/loadBalancers',type=~ 'Microsoft.Network/networkInterfaces',type=~ 'Microsoft.Network/publicIPAddresses',type=~ 'Microsoft.Network/routeTables',type=~ 'Microsoft.Network/virtualNetworks',type=~ 'microsoft.sql/servers/databases', type=~ 'Microsoft.Compute/disks', type=~ 'Microsoft.Compute/virtualMachines')
| union (resources| where type == 'microsoft.network/virtualnetworks'|
extend subnets = properties.subnets| mv-expand subnets)
| summarize count() by tostring(type)
```

To the left of the query editor is a sidebar titled "Scope" with a dropdown menu set to "Management group" and a sub-menu showing "1 management groups selected". Below this are various category links: AI, Analytics, Compute, Containers, Databases, DevOps, Hybrid + multicloud, Identity, Integration, Internet of Things, and Management and governance. At the bottom of the sidebar is an "Apply" button.

Step 4: Click on run query to view the number of assets by their type



The screenshot shows the Azure Resource Graph Explorer interface. On the left, there's a sidebar with categories like General, AI + machine learning, Analytics, Compute, Containers, Databases, DevOps, Hybrid + multicloud, Identity, Integration, Internet of Things, Management and governance, Migration, Mixed reality, and Monitor. The main area has two tabs: 'Query 1' and 'Query 2'. 'Query 1' contains the following FQL code:

```

1 resources
2 | extend typeDisplayName1=case(type == 'Microsoft.ContainerService/managedClusters',type~ 'Microsoft.Network/loadBalancers',type~ 'Microsoft.Network/networkInterfaces',type~ 'Microsoft.Network/publicIPAddresses',type~ 'Microsoft.Network/routeTables',type~ 'Microsoft.Network/virtualNetworks',type == 'microsoft.network/virtualnetworks',type~ 'microsoft.keyvault/vaults',type~ 'microsoft.sqlservers/databases',type~ 'microsoft.cache/redis',type~ 'microsoft.network/applicationSecurityGroups',type~ 'microsoft.network/networkSecurityGroups',type~ 'microsoft.insights/activityLogs',type~ 'microsoft.authorization/roleAssignments')
3 | union (authorizationresources | extend typeDisplayName2=case(type=='microsoft.authorization/roleDefinitions',type=='microsoft.authorization/roleAssignment',type=='microsoft.authorization/roleAssignment'))
4 | summarize count() by tostring(type)

```

The 'Results' tab is selected, showing a table with one row:

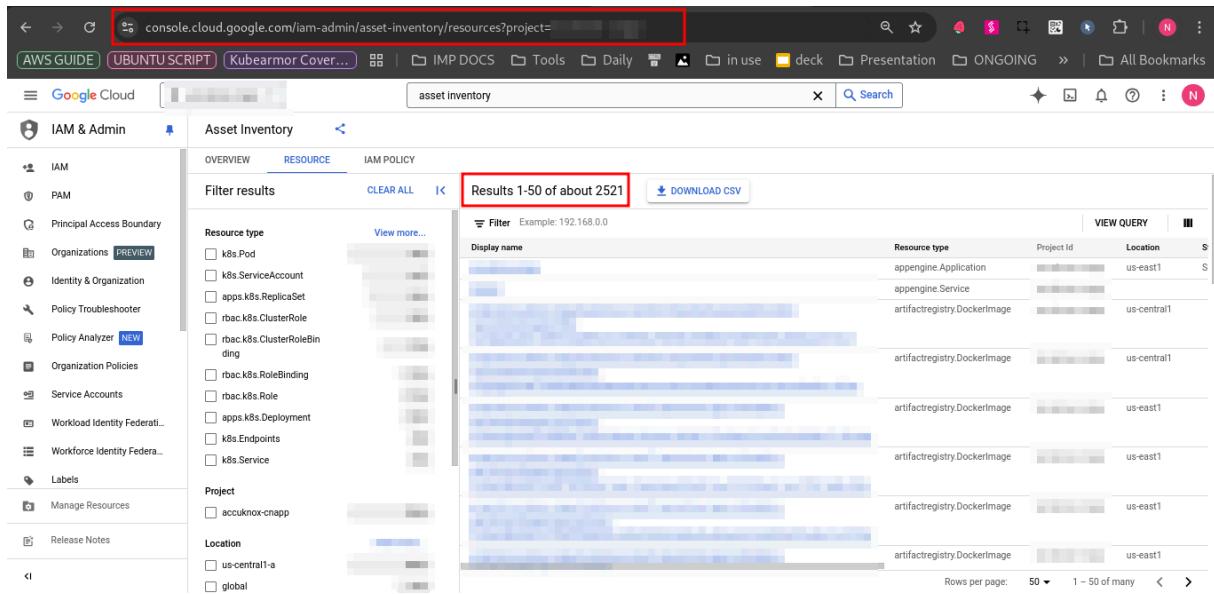
Type	count_ ↑↓	
microsoft.authorization/classicAdministrators	1	See details
microsoft.authorization/roleAssignments	19	See details
...

At the bottom, there are navigation buttons: < Previous, Page 1 of 1, and Next >.

The results can be downloaded as CSV

1.1.3 GCP

Step 1: Navigate to the GCP Asset Inventory (IAM & Admin > Asset Inventory)

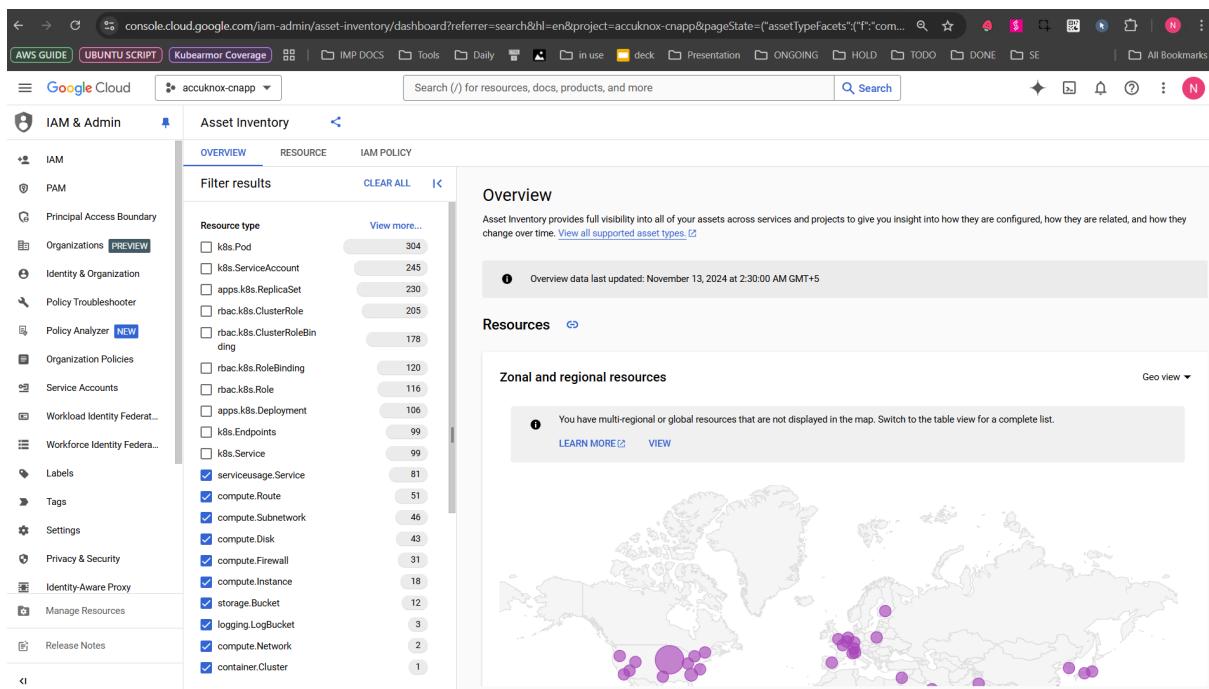


The screenshot shows the Google Cloud IAM & Admin Asset Inventory interface. The URL in the browser is `console.cloud.google.com/iam-admin/asset-inventory/resources/project-[REDACTED]`. The left sidebar is titled "Google Cloud" and includes sections for IAM, PAM, Principal Access Boundary, Organizations (PREVIEW), Identity & Organization, Policy Troubleshooter, Policy Analyzer (NEW), Organization Policies, Service Accounts, Workload Identity Federal..., Workforce Identity Federal..., Labels, Manage Resources, and Release Notes. The main panel is titled "Asset Inventory" and has tabs for OVERVIEW, RESOURCE (which is selected), and IAM POLICY. It includes a "Filter results" section with checkboxes for various resource types like k8s.Pod, k8s.ServiceAccount, etc., and dropdowns for Project, Location, and Resource type. A search bar at the top right contains the text "asset inventory". Below the search bar, it says "Results 1-50 of about 2521" and there is a "DOWNLOAD CSV" button. The main table lists resources with columns for Display name, Resource type, Project Id, Location, and a "View Query" link. The first few rows show artifacts from the accuknox-cnapp project in us-central1, us-east1, and us-central1 locations.

Display name	Resource type	Project Id	Location
[REDACTED]	appengine.Application	[REDACTED]	us-east1
[REDACTED]	appengine.Service	[REDACTED]	us-central1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-central1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-central1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-east1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-east1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-east1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-east1
[REDACTED]	artifactregistry.DockerImage	[REDACTED]	us-east1

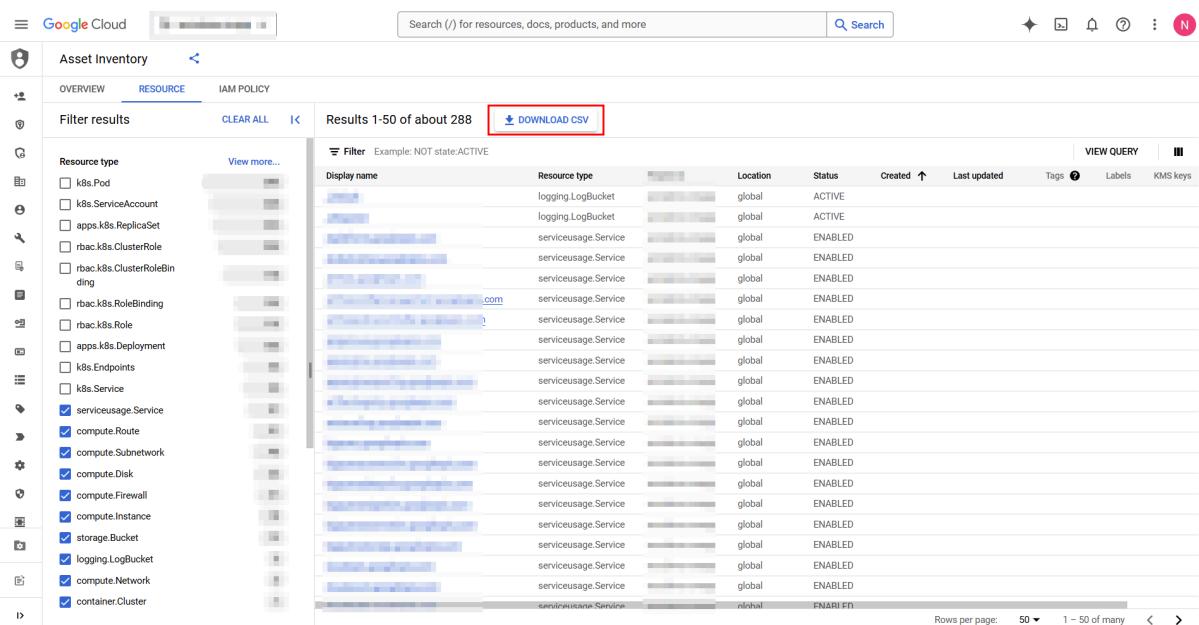
Step 2: Paste this snippet at the end of the url on the Browser to apply the required filters:

```
&pageState={"assetTypeFacets":("f":"compute.googleapis.com%2FSubnetwork,compute.googleapis.com%2FRoute,compute.googleapis.com%2FFirewall,logging.googleapis.com%2FLogBucket,serviceusage.googleapis.com%2FService,compute.googleapis.com%2FDisk,compute.googleapis.com%2FInstance,container.googleapis.com%2FCluster,storage.googleapis.com%2FBucket,compute.googleapis.com%2FNetwork"))}
```



The screenshot shows the Google Cloud Asset Inventory Overview page. On the left, there's a sidebar with various navigation links like IAM & Admin, IAM, PAM, Principal Access Boundary, Organizations, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts, Workload Identity Federation, Workforce Identity Federation, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Manage Resources, and Release Notes. The main area has tabs for OVERVIEW, RESOURCE, and IAM POLICY. Under OVERVIEW, there's a 'Filter results' section with a list of resource types and their counts. The 'serviceusage.Service' type is selected. Below this is an 'Overview' section with a message about full visibility into assets across services and projects. A 'Resources' section follows, featuring a 'Zonal and regional resources' map where purple dots represent global resources. A note says you have multi-regional or global resources that are not displayed in the map. There's also a 'LEARN MORE' and 'VIEW' button.

Note: Sometimes the page might need reload to reflect the filter changes.



This screenshot shows the Google Cloud Asset Inventory RESOURCE page. It displays a table of 288 results. The columns include Display name, Resource type, Location, Status, Created, Last updated, Tags, Labels, and KMS keys. The 'Resource type' column lists various service types like k8s.Pod, k8s.ServiceAccount, etc., with 'serviceusage.Service' being the most common. The 'Status' column shows mostly ACTIVE and ENABLED. The 'Created' and 'Last updated' columns show the timestamp of each resource's creation and last update. The 'Tags' and 'Labels' columns are currently empty. The 'KMS keys' column also shows empty. At the top right of the table, there are buttons for 'VIEW QUERY' and 'CSV'. A red box highlights the 'DOWNLOAD CSV' button. The bottom right of the table shows pagination options for 'Rows per page' (50), '1 - 50 of many', and navigation arrows.

The results can be downloaded as CSV.

1.2 Container Images Counts

1.2.1 DockerHub

To get the count of dockerhub images please use the following command after connecting your dockerhub repository to the commandline using dockerdesktop application.

```
docker images <repository-name>
```

Note: Replace the <repository-name> with your repository name.

1.2.2 AWS ECR

To get the count of the ECR Repository images the users need to connect the AWS account using AWS CLI and use the following command for getting the image count in each repository

```
aws ecr describe-images --repository-name <repository-name> --query "length(imageDetails[])"
```

Note: Replace the <repository-name> with your repository name.

1.2.3 GCR

To get the count of images stored in the GCR registry using the gcloud command line tool use the following command

```
gcloud container images list-tags gcr.io/<PROJECT_ID>/<REPOSITORY_NAME>
--format='get(digest)' | wc -l
```

Note: Replace the <PROJECT_ID> with your Google Cloud project ID and <REPOSITORY_NAME> with the name of the GCR repository you want to count images.

1.2.4 ACR

To get the count of images stored in an Azure Container Registry (ACR) using Azure CLI use the following command

```
az acr repository show-tags --name <ACR_NAME> --repository <REPOSITORY_NAME> --output json --query "length(@)"
```

Note: Replace <ACR_NAME> with the name of your Azure Container Registry and <REPOSITORY_NAME> with the name of the ACR repository you want to count images.

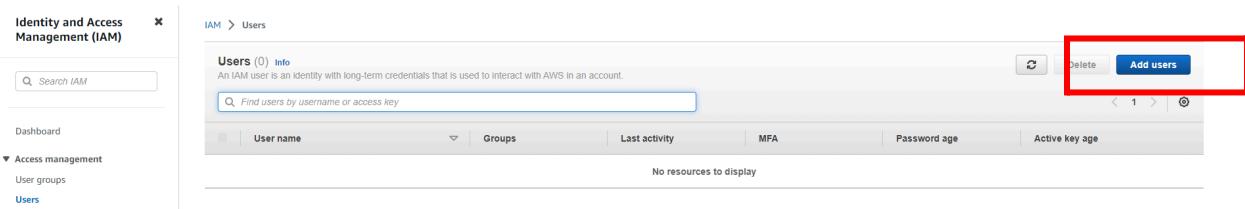
2. CSPM Prerequisites

2.1 AWS

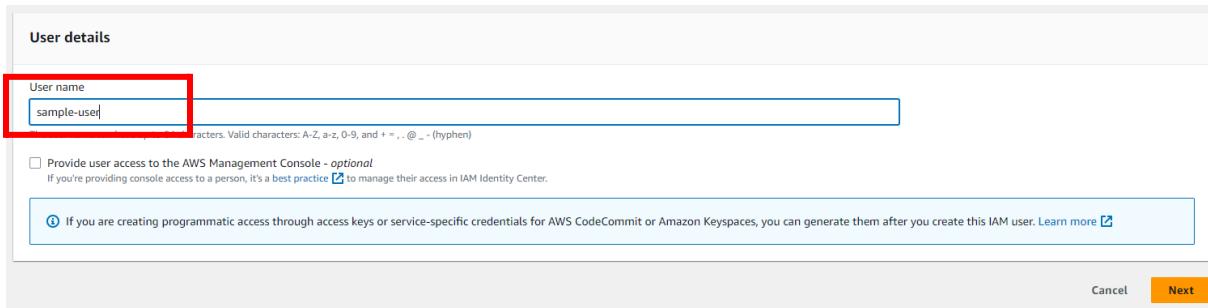
AWS IAM User Creation

Please follow the following steps to provide a user with appropriate read access:

Step 1: Navigate to IAM -> Users and click on Add Users



Step 2: Give a username to identify the user



The screenshot shows the 'User details' step of the IAM user creation wizard. It has fields for 'User name' (containing 'sample-user'), 'Access type' (set to 'Programmatic access'), and 'AWS KMS keys for encryption' (disabled). There are also sections for 'Provide user access to the AWS Management Console' (unchecked) and 'About programmatic access' (with a note about generating access keys after creation). At the bottom are 'Cancel' and 'Next Step' buttons.

Step 3: In the "Set Permissions" screen:

- a. Select "Attach policies directly"
- b. Search "ReadOnly", Filter by Type: "AWS managed - job function" and select the policy

Step 2
Set permissions

Step 3
Review and create

Permissions options

- Add user to group
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

Permissions policies (1/1116)
Choose one or more policies to attach to your new user.

Filter by Type	
<input type="text" value="Q. Readonly"/>	<input type="button" value="X"/>
AWS managed - job function	▼
1 match	
<input checked="" type="checkbox"/> Policy name 	Type
<input checked="" type="checkbox"/>  ReadOnlyAccess	AWS managed - job function
Attached entities 0	

c. Search "SecurityAudit", Filter by Type: "AWS managed - job function" and select the policy

Permissions policies (2/1116)
Choose one or more policies to attach to your new user.

Filter by Type	
<input type="text" value="Q. security"/>	<input type="button" value="X"/>
AWS managed - job function	▼
1 match	
<input checked="" type="checkbox"/> Policy name 	Type
<input checked="" type="checkbox"/>  SecurityAudit	AWS managed - job function
Attached entities 0	

▶ Set permissions boundary - optional

Cancel Previous Next

Step 4: Finish creating the user. Click on the newly created user and create the Access key and Secret Key from the Security Credentials tab to be used in the AccuKnox panel

Permissions Groups Tags **Security credentials** Access Advisor

Console sign-in

Console sign-in link  <https://864316920010.signin.aws.amazon.com/console> Enable console access

Multi-factor authentication (MFA) (0)
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Device type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
<input type="button" value="Assign MFA device"/>			

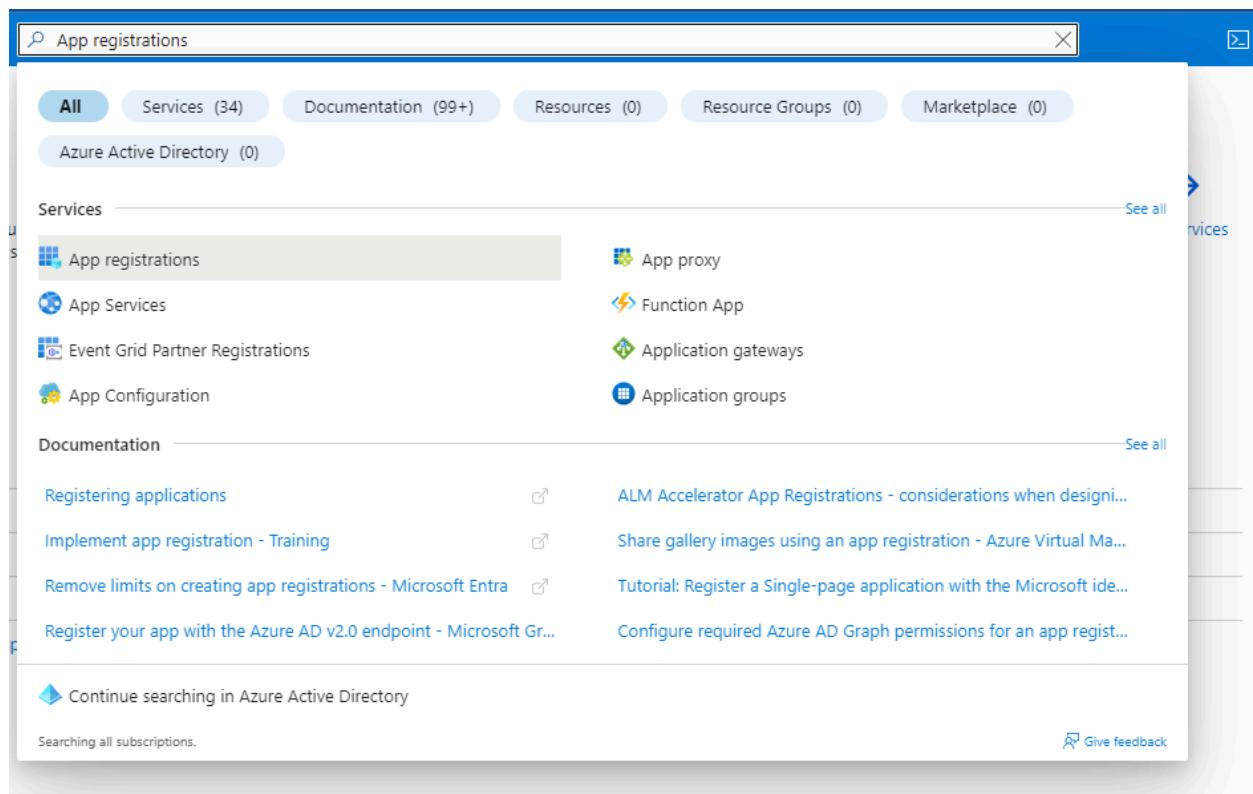
Access keys (0)
Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two access keys (active or inactive) at a time. [Learn more](#)

No access keys
As a best practice, avoid using long-term credentials like access keys. Instead, use tools which provide short term credentials. [Learn more](#)

2.2 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

[Home >](#)

App registrations

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

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

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

7 applications found

Display name ↑↓

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

[Home > App registrations >](#)

Register an application

* Name

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

Accuknox-may-2023

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (Default Directory only - Single tenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant)
 Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
 Personal Microsoft accounts only

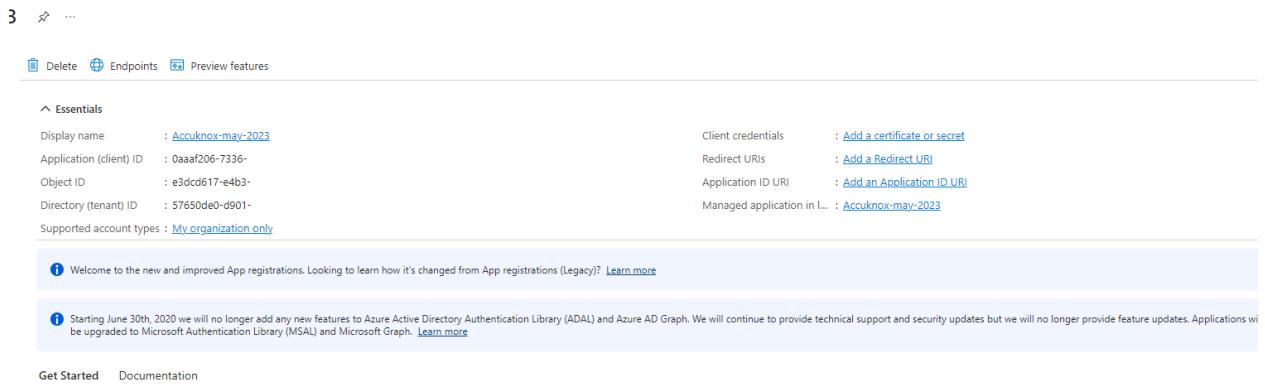
[Help me choose...](#)

Redirect URI (optional)

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

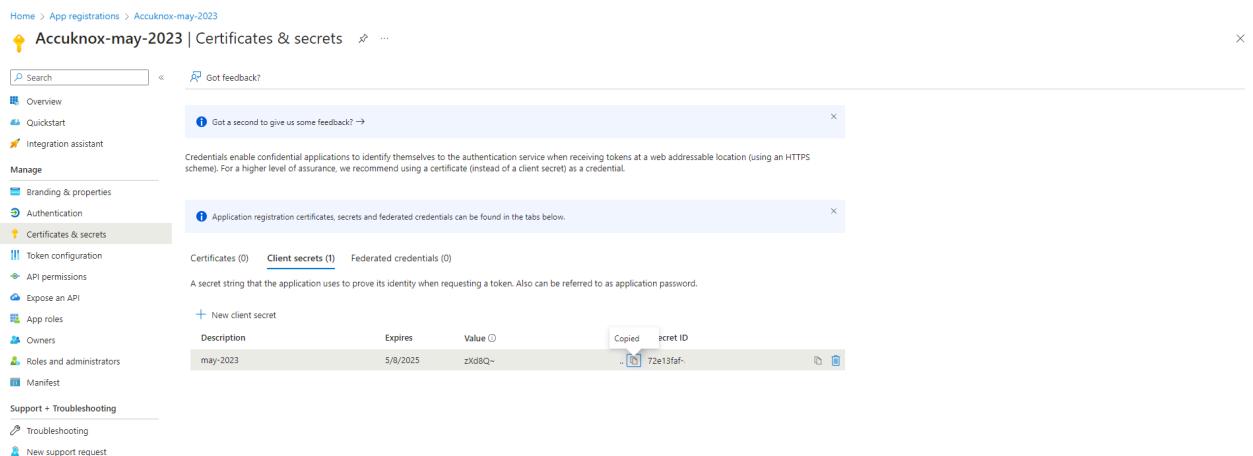
 Select a platform e.g. <https://example.com/auth>Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).By proceeding, you agree to the Microsoft Platform Policies [»](#)[Register](#)

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



The screenshot shows the Azure portal's App registrations section for the application 'Accuknox-may-2023'. The 'Certificates & secrets' tab is active. A single client secret named 'may-2023' is listed with the value 'zxG8Q~' and an expiration date of 5/8/2025.

- Click on a 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.



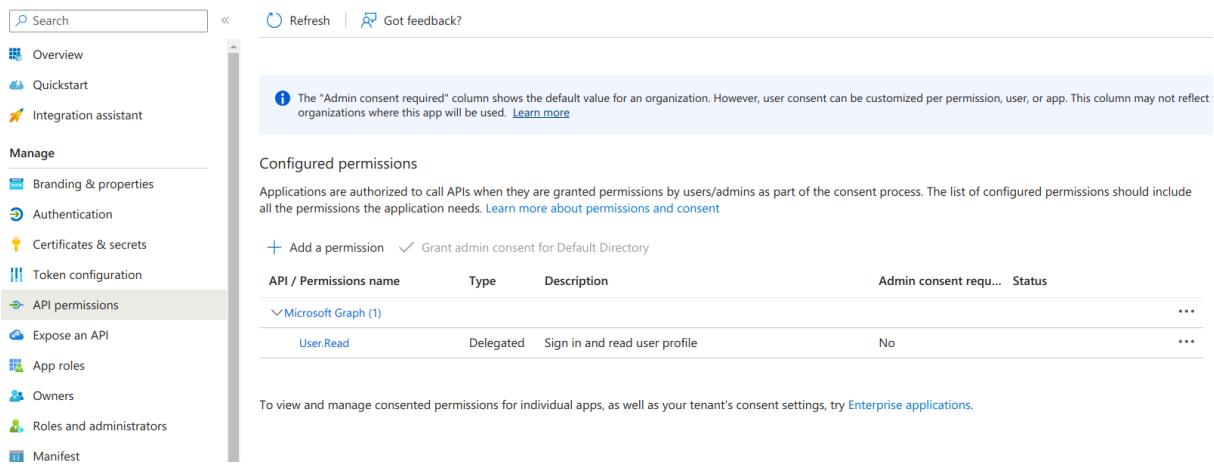
The screenshot shows the 'Certificates & secrets' blade for the application 'Accuknox-may-2023'. The 'Client secrets' tab is selected, displaying a table with one row:

Description	Expires	Value	Actions
may-2023	5/8/2025	zxG8Q~	

- Next, go to the API permissions tab and click on Add a permission

Home > App registrations > Permission-screen

Permission-screen | API permissions



The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect organizations where this app will be used. [Learn more](#)

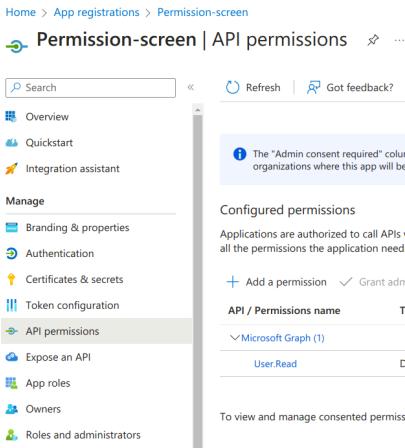
Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name	Type	Description	Admin consent requ...	Status	
Microsoft Graph (1)		User.Read	Delegated	Sign in and read user profile	No

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

- On the screen that appears, click on Microsoft Graph



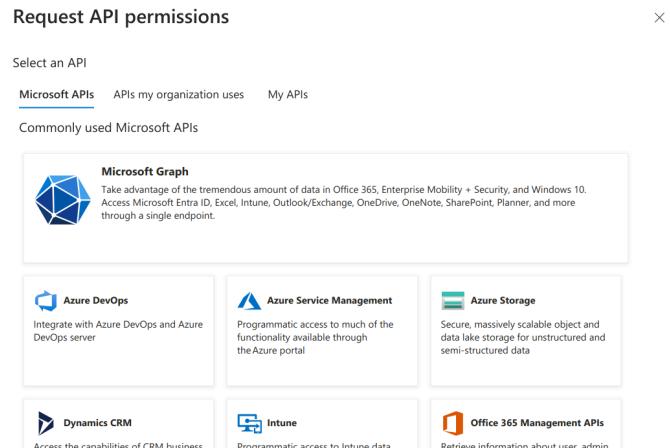
The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect organizations where this app will be used. [Learn more](#)

Configured permissions

Applications are authorized to call APIs when they are granted permission to all the permissions the application needs. [Learn more about permissions and consent](#)

API / Permissions name	Type	Description
Microsoft Graph (1)		User.Read

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).



Request API permissions

Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Microsoft Entra ID, Excel, Intune, Outlook/Exchange, OneDrive, SharePoint, Planner, and more through a single endpoint.

Azure DevOps Integrate with Azure DevOps and Azure DevOps server	Azure Service Management Programmatic access to much of the functionality available through the Azure portal	Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data
Dynamics CRM Access the capabilities of CRM business	Intune Programmatic access to Intune data	Office 365 Management APIs Retrieve information about user, admin,

- Next, select Application Permissions and then search for Directory.Read.All and click on Add permissions

Request API permissions

×

[All APIs](#)

 Microsoft Graph
<https://graph.microsoft.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions [expand all](#)

Permission	Admin consent required
Directory (1)	
<input checked="" type="checkbox"/> Directory.Read.All ⓘ Read directory data	Yes

[Add permissions](#) [Discard](#)

- Select ‘Grant Admin Consent’ for Default Directory and click on ‘Yes’

Microsoft Azure

Home > App registrations > Permission-screen

Permission-screen | API permissions

Grant admin consent confirmation.

Do you want to grant consent for the requested permissions for all accounts in Default Directory? This will update any existing admin consent records this application already has to match what is listed below.

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. [Learn more about permissions and consent](#)

[+ Add a permission](#) [Grant admin consent for Default Directory](#)

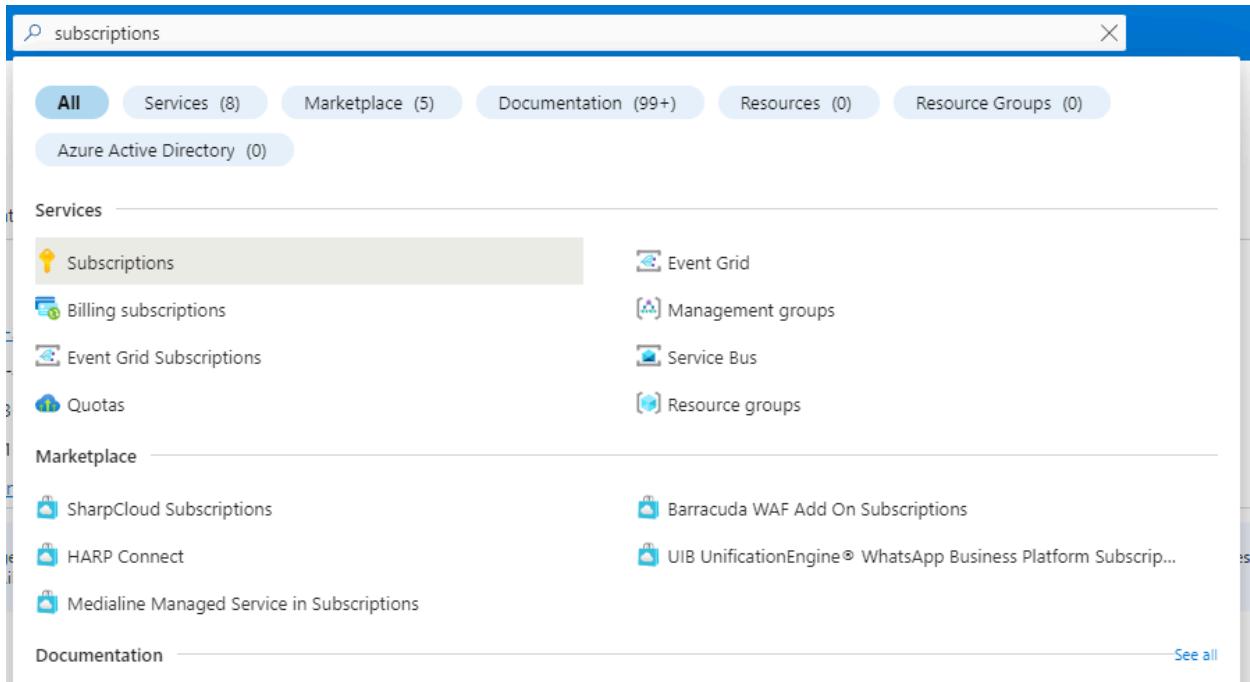
API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (2)				...
Directory.Read.All	Application	Read directory data	Yes	⚠ Not granted for Default... ...
User.Read	Delegated	Sign in and read user profile	No	...

To view and manage consented permissions for individual apps, as well as your tenant's consent settings, try [Enterprise applications](#).

Support + Troubleshooting

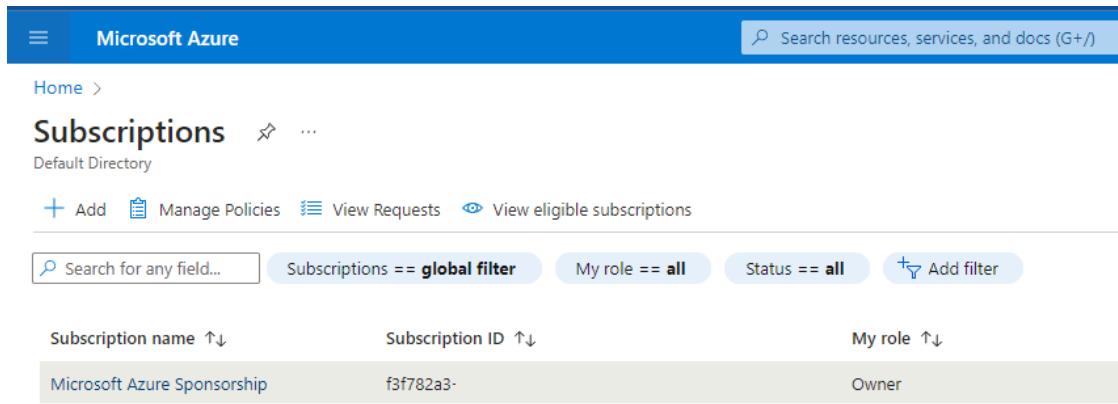
[Troubleshooting](#) [New support request](#)

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



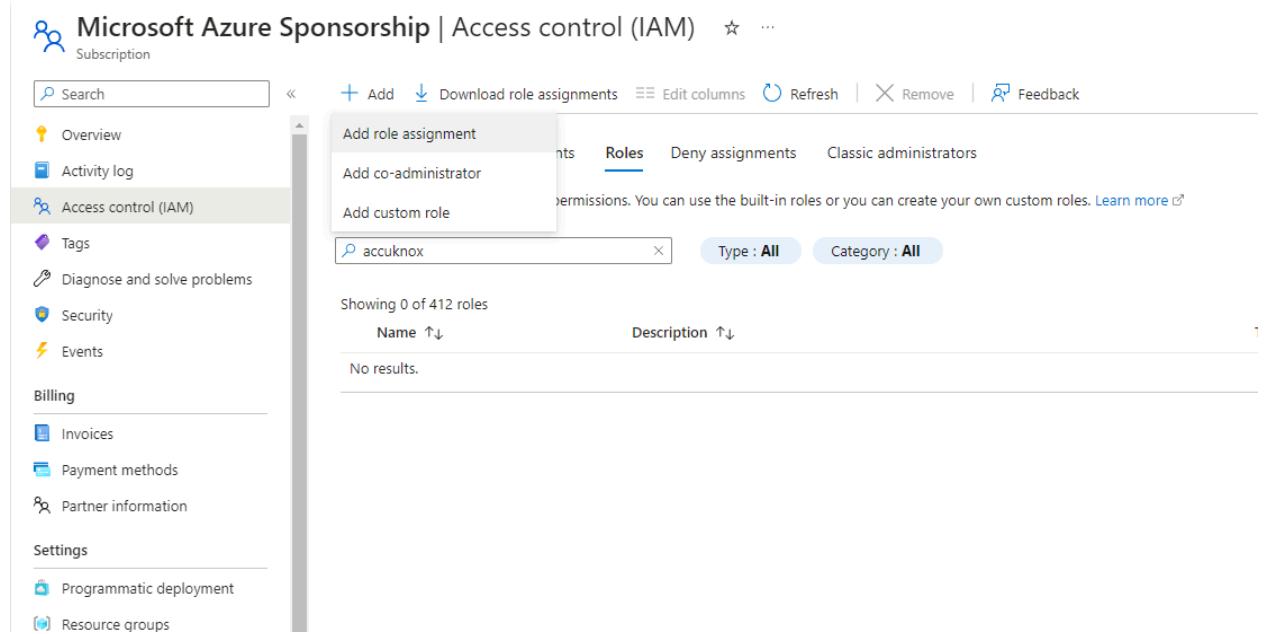
The screenshot shows the Azure portal interface. The search bar at the top contains the text "subscriptions". Below the search bar, there are several filter tabs: All (selected), Services (8), Marketplace (5), Documentation (99+), Resources (0), and Resource Groups (0). Under the "Azure Active Directory (0)" tab, there is a "Services" section with a list of items: Subscriptions (selected), Billing subscriptions, Event Grid Subscriptions, Quotas, Management groups, Service Bus, Resource groups, SharpCloud Subscriptions, HARP Connect, Medialine Managed Service in Subscriptions, Barracuda WAF Add On Subscriptions, UIB UnificationEngine® WhatsApp Business Platform Subscript..., and See all.

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



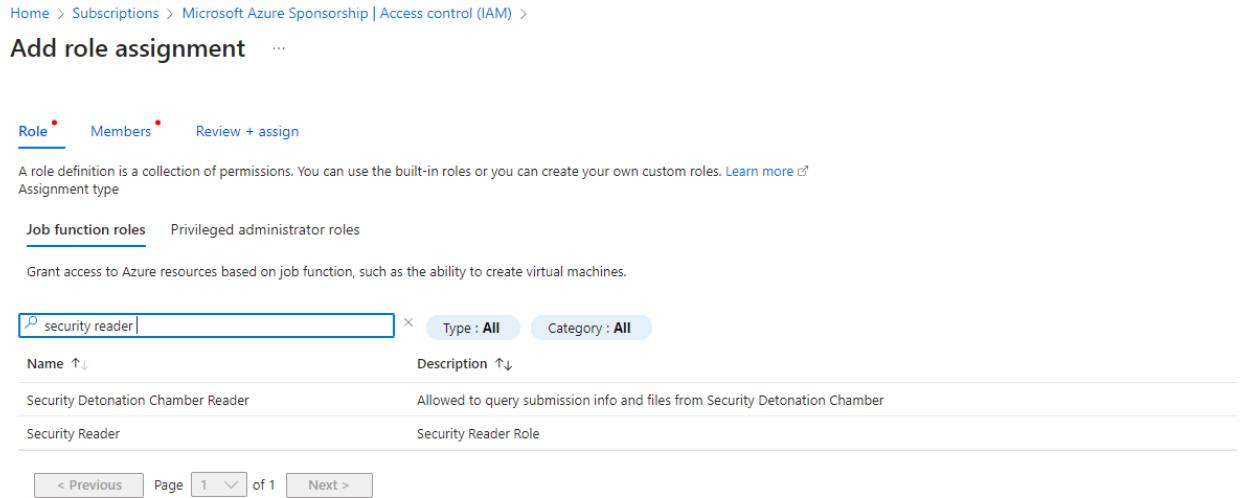
The screenshot shows the Microsoft Azure Subscriptions page. The top navigation bar includes a search bar with the placeholder "Search resources, services, and docs (G+/)". Below the navigation bar, the page title is "Subscriptions" with a back arrow and three dots. A "Default Directory" link is also present. The main content area has a header with "Add", "Manage Policies", "View Requests", and "View eligible subscriptions" buttons. Below this is a search bar with the placeholder "Search for any field..." and several filter buttons: "Subscriptions == global filter", "My role == all", "Status == all", and "Add filter". The main table displays one row for the "Microsoft Azure Sponsorship" subscription, with columns for "Subscription name" (sorted by ascending name), "Subscription ID" (sorted by ascending ID), and "My role" (sorted by descending role). The values for the first row are: Microsoft Azure Sponsorship, f3f782a3, and Owner.

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



The screenshot shows the Microsoft Azure Access control (IAM) Roles page. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Security, Events, Billing, Invoices, Payment methods, Partner information, Settings, Programmatic deployment, and Resource groups. The main area has a search bar with 'accuknox' typed in, and buttons for 'Type : All' and 'Category : All'. A modal window titled 'Add role assignment' is open, showing tabs for 'Add co-administrator', 'Add custom role', and 'Roles'. The 'Roles' tab is selected. Below the modal, the text reads: 'Permissions. You can use the built-in roles or you can create your own custom roles. Learn more'. The search results table has columns for Name and Description, both with ascending/descending arrows. The message 'Showing 0 of 412 roles' is displayed, followed by 'No results.'

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



The screenshot shows the 'Add role assignment' wizard. The top navigation bar includes 'Role *', 'Members *', and 'Review + assign'. Below the search bar, there is a note: 'A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more'. The 'Assignment type' dropdown is set to 'Job function roles'. The description below states: 'Grant access to Azure resources based on job function, such as the ability to create virtual machines.' The search bar contains 'security reader', and the results table has columns for Name and Description, both with ascending/descending arrows. Two items are listed: 'Security Detonation Chamber Reader' (Description: 'Allowed to query submission info and files from Security Detonation Chamber') and 'Security Reader' (Description: 'Security Reader Role'). At the bottom, there are navigation buttons: '< Previous', 'Page 1 of 1', and 'Next >'.

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

Add role assignment ...

Role **Members *** Review + assign

Selected role Security Reader

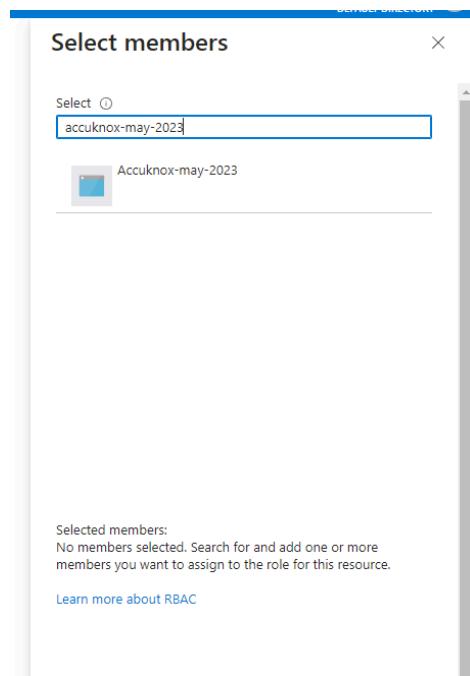
Assign access to User, group, or service principal
 Managed identity

Members [+ Select members](#)

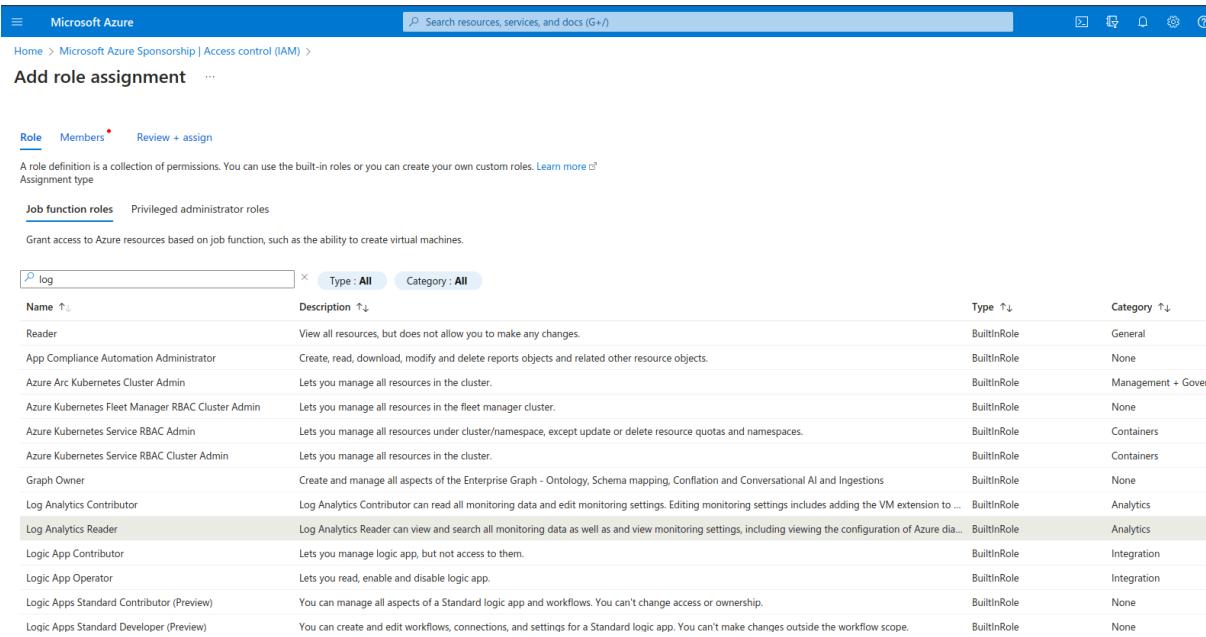
Name	Object ID
No members selected	

Description

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



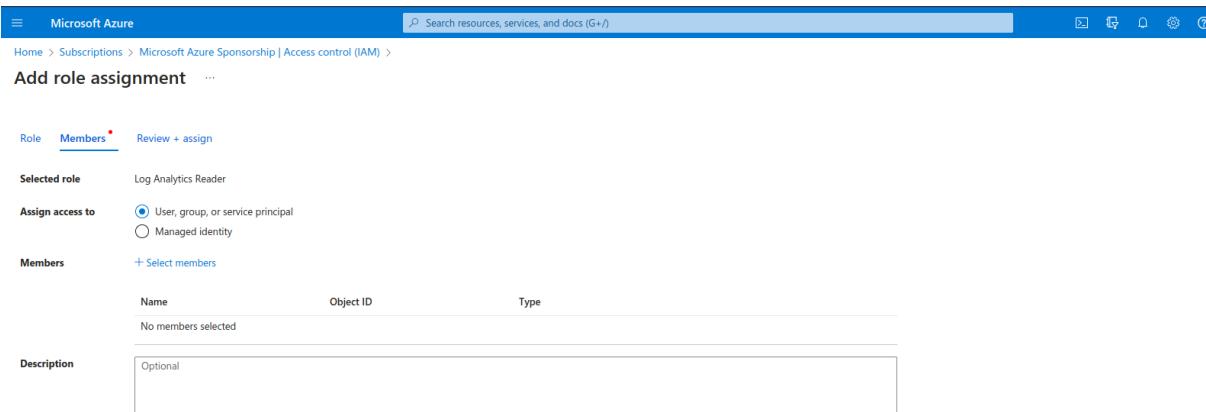
- Similarly, we have to add another role. This time, search for Log Analytics Reader. Select it and click next



The screenshot shows the Microsoft Azure 'Role definition' page. At the top, there are tabs for 'Role', 'Members *' (which is selected), and 'Review + assign'. Below the tabs, a search bar contains the text 'log'. A search result for 'Log Analytics Reader' is highlighted in grey. Other roles listed include Reader, App Compliance Automation Administrator, Azure Arc Kubernetes Cluster Admin, Azure Kubernetes Fleet Manager RBAC Cluster Admin, Azure Kubernetes Service RBAC Admin, Azure Kubernetes Service RBAC Cluster Admin, Graph Owner, Log Analytics Contributor, Logic App Contributor, Logic App Operator, Logic Apps Standard Contributor (Preview), and Logic Apps Standard Developer (Preview). The columns for each role are Name, Description, Type, and Category.

Name	Description	Type	Category
Reader	View all resources, but does not allow you to make any changes.	BuiltinRole	General
App Compliance Automation Administrator	Create, read, download, modify and delete reports objects and related other resource objects.	BuiltinRole	None
Azure Arc Kubernetes Cluster Admin	Lets you manage all resources in the cluster.	BuiltinRole	Management + Govern
Azure Kubernetes Fleet Manager RBAC Cluster Admin	Lets you manage all resources in the fleet manager cluster.	BuiltinRole	None
Azure Kubernetes Service RBAC Admin	Lets you manage all resources under cluster/namespace, except update or delete resource quotas and namespaces.	BuiltinRole	Containers
Azure Kubernetes Service RBAC Cluster Admin	Lets you manage all resources in the cluster.	BuiltinRole	Containers
Graph Owner	Create and manage all aspects of the Enterprise Graph - Ontology, Schema mapping, Conflation and Conversational AI and Ingestions	BuiltinRole	None
Log Analytics Contributor	Log Analytics Contributor can read all monitoring data and edit monitoring settings. Editing monitoring settings includes adding the VM extension to ...	BuiltinRole	Analytics
Log Analytics Reader	Log Analytics Reader can view and search all monitoring data as well as and view monitoring settings, including viewing the configuration of Azure dia...	BuiltinRole	Analytics
Logic App Contributor	Lets you manage logic app, but not access to them.	BuiltinRole	Integration
Logic App Operator	Lets you read, enable and disable logic app.	BuiltinRole	Integration
Logic Apps Standard Contributor (Preview)	You can manage all aspects of a Standard logic app and workflows. You can't change access or ownership.	BuiltinRole	None
Logic Apps Standard Developer (Preview)	You can create and edit workflows, connections, and settings for a Standard logic app. You can't make changes outside the workflow scope.	BuiltinRole	None

- Now, click on select members, select the application that was created similar to the previous role. Finally, click on Review and Assign.



The screenshot shows the Microsoft Azure 'Add role assignment' page. The 'Members' tab is selected. Under 'Selected role', 'Log Analytics Reader' is chosen. Under 'Assign access to', 'User, group, or service principal' is selected. Under 'Members', there is a button '+ Select members'. A table below shows 'No members selected'. There is also a 'Description' field with an optional input area.

Name	Object ID	Type
No members selected		

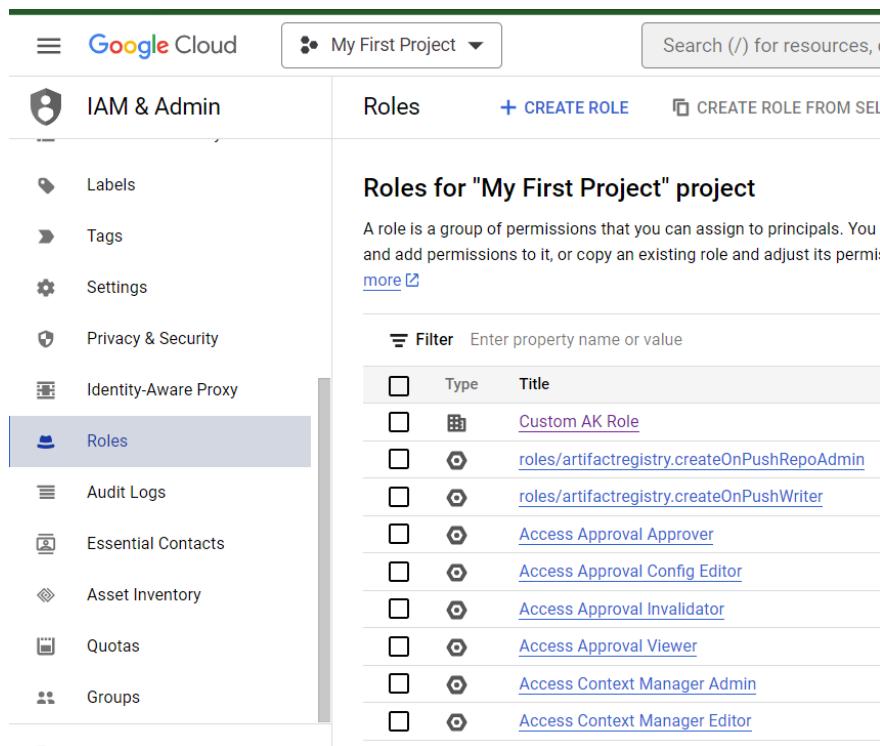
2.3 GCP

Note: Make sure the Below API Library is enabled in your GCP Account for onboarding into AccuKnox SaaS:

1. Compute Engine API
2. Identity and Access Management (IAM) API
3. Cloud Resource Manager API
4. Cloud Functions API
5. KMS API
6. Kubernetes API
7. Cloud SQL Admin API

For GCP there is a requirement for IAM Service Account Access.

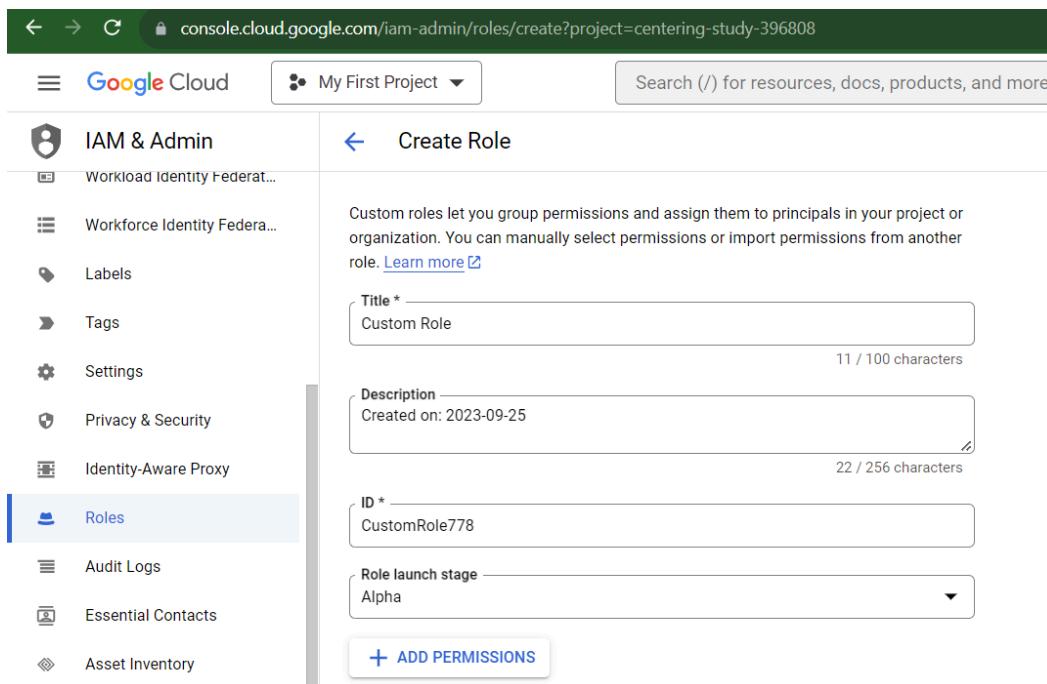
Step 1: Log into your Google Cloud console and navigate to IAM & Admin, choose “Roles” and Click “Create Role”



The screenshot shows the Google Cloud IAM & Admin interface. On the left, a sidebar lists various options: Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles (which is selected and highlighted in grey), Audit Logs, Essential Contacts, Asset Inventory, Quotas, and Groups. The main content area is titled "Roles for 'My First Project' project". It includes a brief description of what a role is and a "more" link. Below this is a "Filter" input field and a table of roles. The table has columns for "Type" (checkboxes) and "Title". The listed roles are:

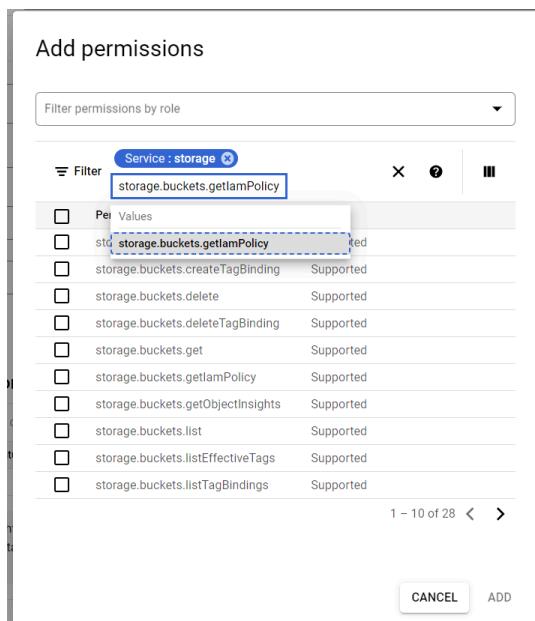
Type	Title
<input type="checkbox"/>	Custom AK Role
<input type="checkbox"/>	roles/artifactregistry.createOnPushRepoAdmin
<input type="checkbox"/>	roles/artifactregistry.createOnPushWriter
<input type="checkbox"/>	Access Approval Approver
<input type="checkbox"/>	Access Approval Config Editor
<input type="checkbox"/>	Access Approval Invalidator
<input type="checkbox"/>	Access Approval Viewer
<input type="checkbox"/>	Access Context Manager Admin
<input type="checkbox"/>	Access Context Manager Editor

Step 2: Name the “Role” and Click “Add Permission”



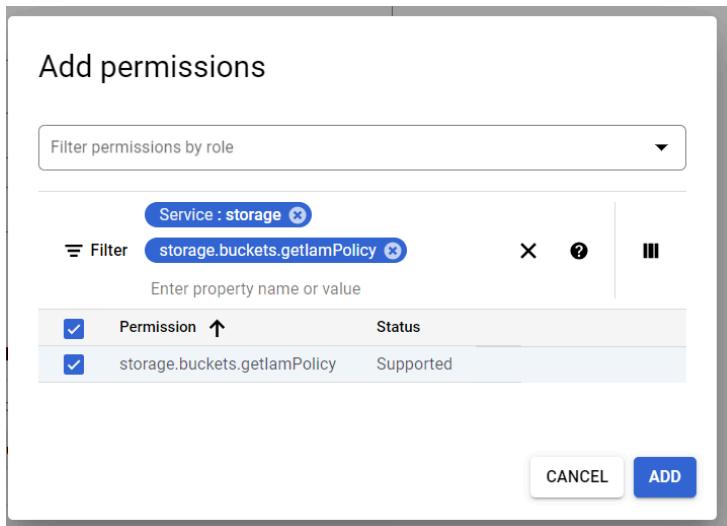
The screenshot shows the Google Cloud IAM & Admin interface. On the left, there's a sidebar with various options like Workload Identity Federation, Workforce Identity Federation, Labels, Tags, Settings, Privacy & Security, Identity-Aware Proxy, Roles (which is selected), Audit Logs, Essential Contacts, and Asset Inventory. The main area is titled 'Create Role'. It has fields for 'Title' (Custom Role), 'Description' (Created on: 2023-09-25), 'ID' (CustomRole778), and 'Role launch stage' (Alpha). At the bottom is a blue button labeled '+ ADD PERMISSIONS'.

Step 3: Use the Service: storage filter, then value as “storage.buckets.getIamPolicy”

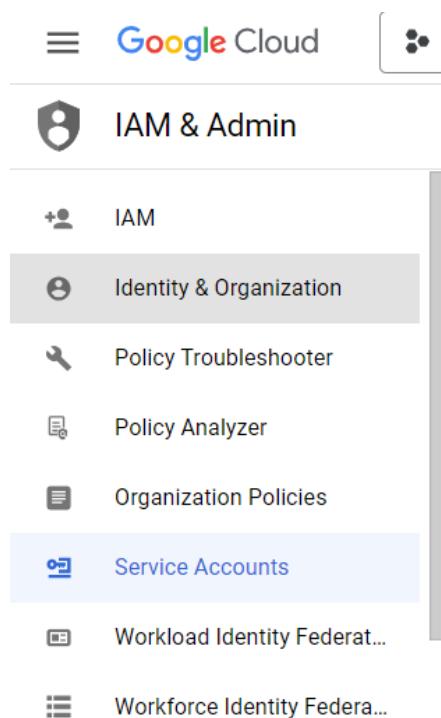


The screenshot shows the 'Add permissions' dialog. A dropdown menu at the top says 'Filter permissions by role'. Below it, a 'Service : storage' dropdown is open, showing a list of permissions. One permission, 'storage.buckets.getIamPolicy', is highlighted with a blue border. At the bottom of the dialog are 'CANCEL' and 'ADD' buttons.

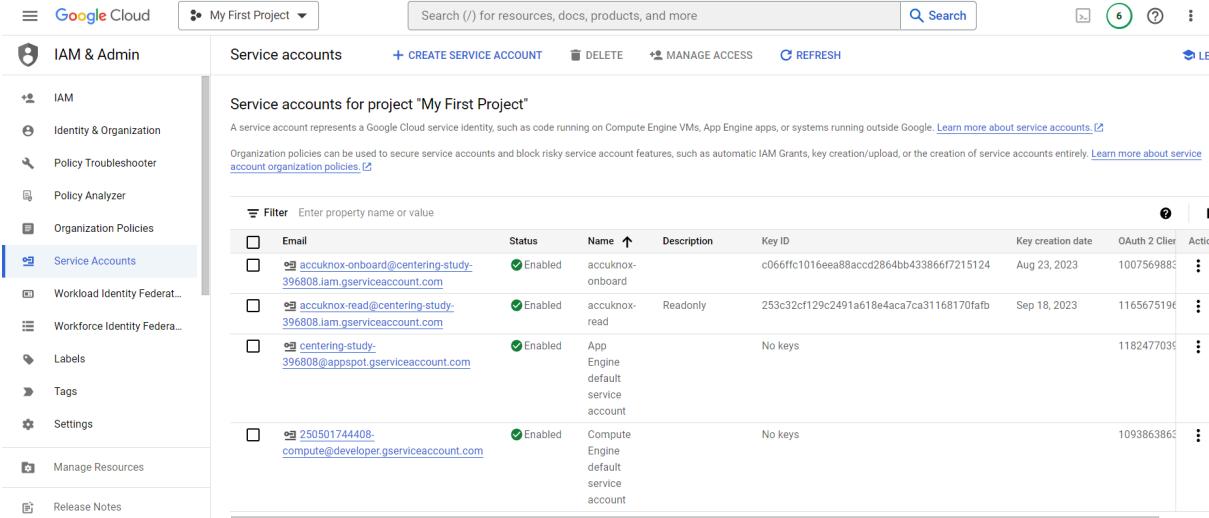
Step 4: Choose the permission and Click “Add” then Click Create in the same page.



Step 5: In the Navigation Panel, navigate to IAM Admin > Service Accounts.



Step 6: Click on "Create Service Account"



The screenshot shows the Google Cloud IAM & Admin Service accounts page for the project "My First Project". The left sidebar is titled "Service Accounts" and lists several other account types like IAM, Identity & Organization, and Policy Troubleshooter. The main area displays a table of existing service accounts:

Email	Status	Name	Description	Key ID	Key creation date	OAuth 2 Client	Action
accuknox-onboard@centering-study-396808.iam.gserviceaccount.com	Enabled	accuknox-onboard		c066fffc1016eea88accd2864bb433866f7215124	Aug 23, 2023	1007569885	⋮
accuknox-read@centering-study-396808.iam.gserviceaccount.com	Enabled	accuknox-read	Readonly	253c32cf129c2491a618e4aca7ca31168170fafb	Sep 18, 2023	1165675196	⋮
centering-study-396808@appspot.gserviceaccount.com	Enabled	App Engine default service account	No keys			1182477035	⋮
250501744408-compute@developer.gserviceaccount.com	Enabled	Compute Engine default service account	No keys			1093863865	⋮

Step 7: Enter any name that you want on Service Account Name.

Step 8: Click on Continue.

1 Service account details

Service account name —

Display name for this service account

Service account ID * X C

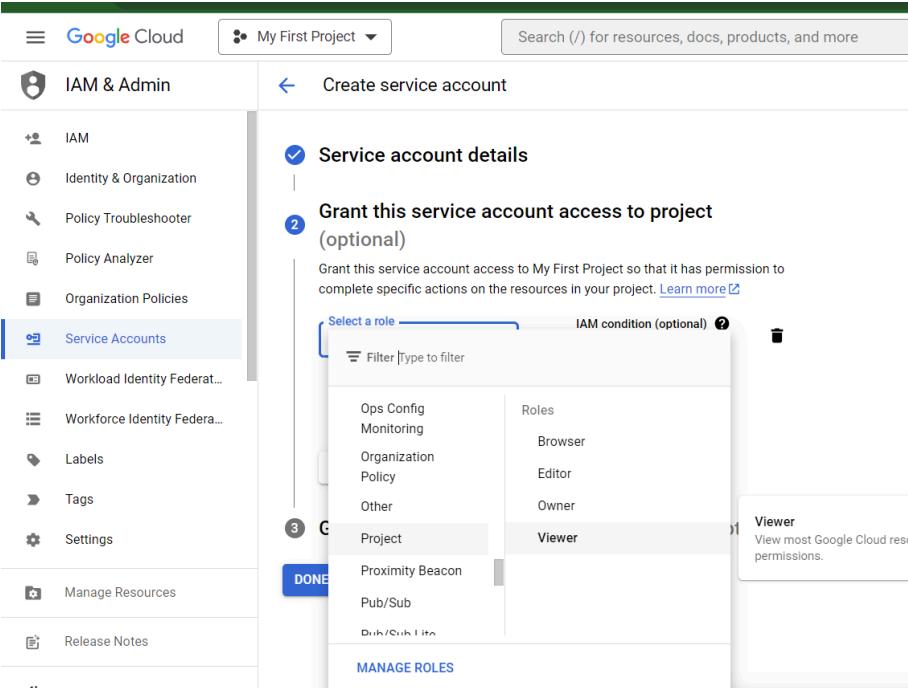
Email address: ak-test@centering-study-396808.iam.gserviceaccount.com ✉

Service account description

Describe what this service account will do

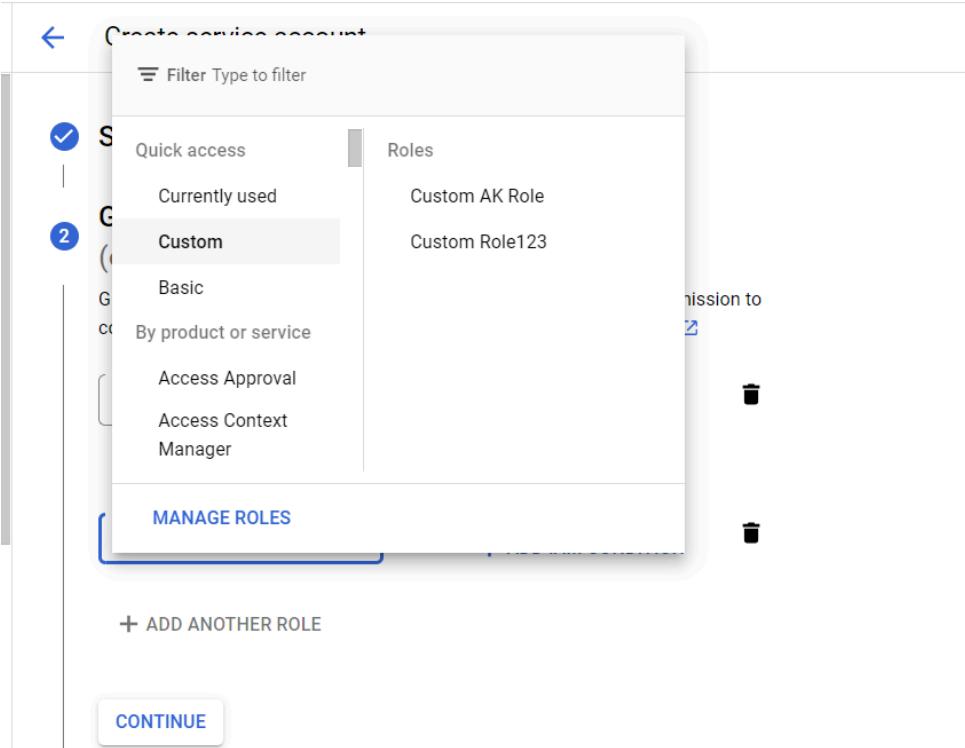
CREATE AND CONTINUE

Step 9: Select the role: Project > Viewer and click Add another Role.



The screenshot shows the Google Cloud IAM & Admin interface. On the left sidebar, under the 'Service Accounts' section, the 'Create service account' option is selected. The main panel displays the 'Service account details' step, which includes a sub-step 'Grant this service account access to project (optional)'. A modal window is open, titled 'Select a role', showing a list of roles. The 'Viewer' role is highlighted, with a tooltip explaining it allows 'View most Google Cloud resources'. Other visible roles include Browser, Editor, Owner, and Project.

Step 10: Click “Add Another Role” Choose “Custom“ Select the created Custom Role.



The screenshot shows the 'Create service account' interface again. The 'Custom' role selection has been completed. The 'MANAGE ROLES' button is highlighted. Below it, there is a '+ ADD ANOTHER ROLE' button and a 'CONTINUE' button at the bottom.

Step 11: Click on “Continue“ and ”Done“

1 Service account details

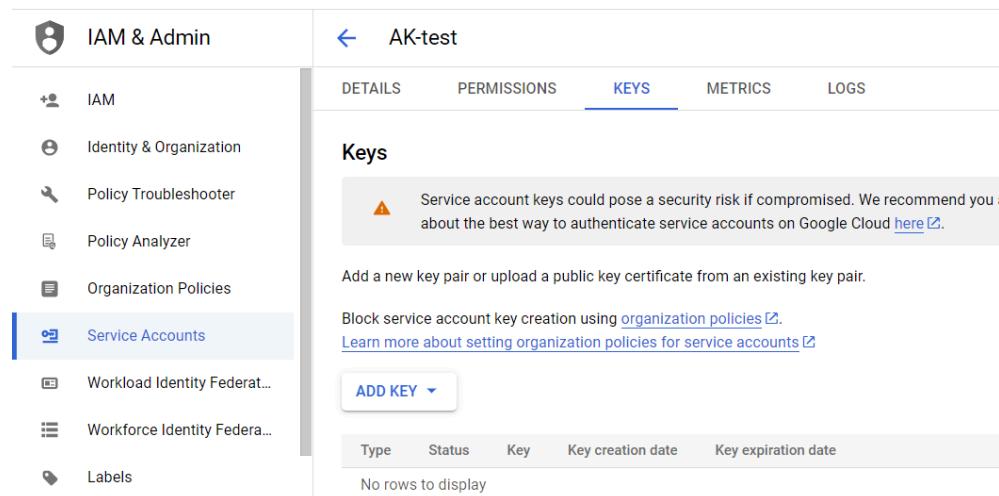
2 Grant this service account access to project (optional)

Grant this service account access to My First Project so that it has permission to complete specific actions on the resources in your project. [Learn more](#)

Role	Viewer	IAM condition (optional) ?	+ ADD IAM CONDITION	
View most Google Cloud resources. See the list of included permissions.				
Role	Custom Role123	IAM condition (optional) ?	+ ADD IAM CONDITION	
Created on: 2023-09-25				
+ ADD ANOTHER ROLE				
CONTINUE				

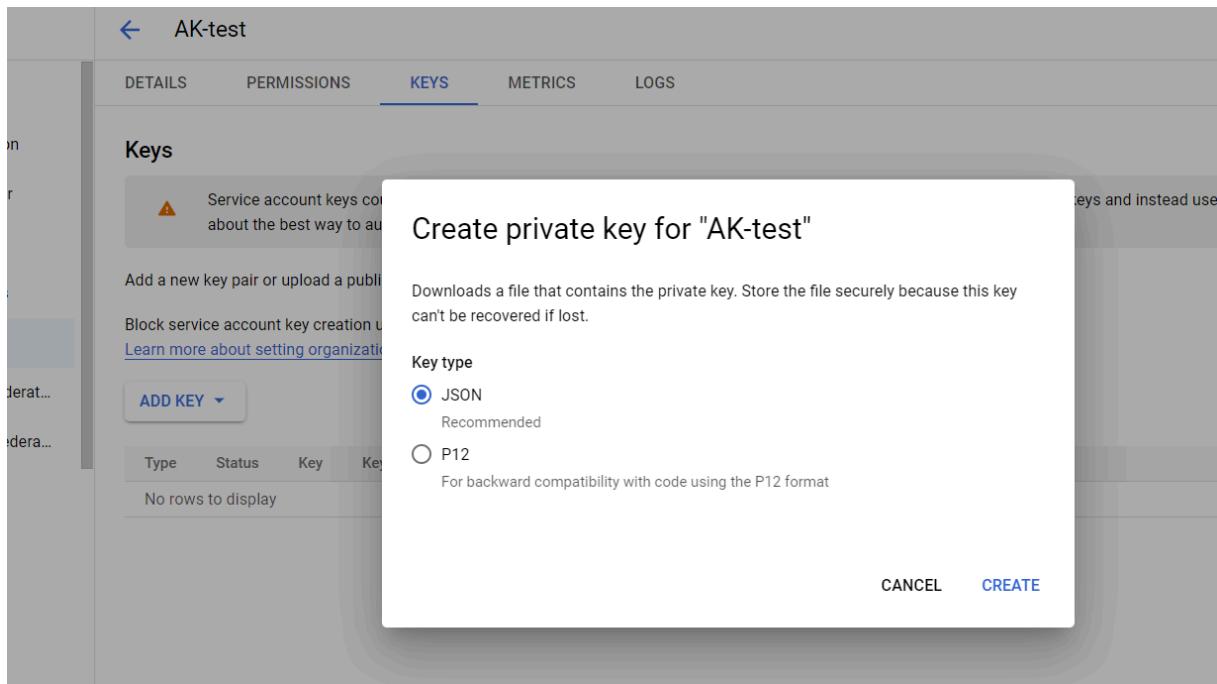
3 Grant users access to this service account (optional)

Step 12: Go to the created Service Account, click on that Service Account navigate to the “Keys“ section.



The screenshot shows the Google Cloud IAM & Admin interface. On the left, there's a sidebar with options like IAM, Identity & Organization, Policy Troubleshooter, Policy Analyzer, Organization Policies, Service Accounts (which is selected), Workload Identity Federation, Workforce Identity Federation, and Labels. The main area is titled "AK-test". It has tabs for DETAILS, PERMISSIONS, KEYS (which is active), METRICS, and LOGS. Under the KEYS tab, there's a warning message: "Service account keys could pose a security risk if compromised. We recommend you learn about the best way to authenticate service accounts on Google Cloud [here](#)". Below that, there's a button to "Add key" and a table with columns for Type, Status, Key, Key creation date, and Key expiration date. The table currently displays "No rows to display".

Step 13: Click the “Add key“ button and “Create new key “ . Chosen Key type should be JSON format.



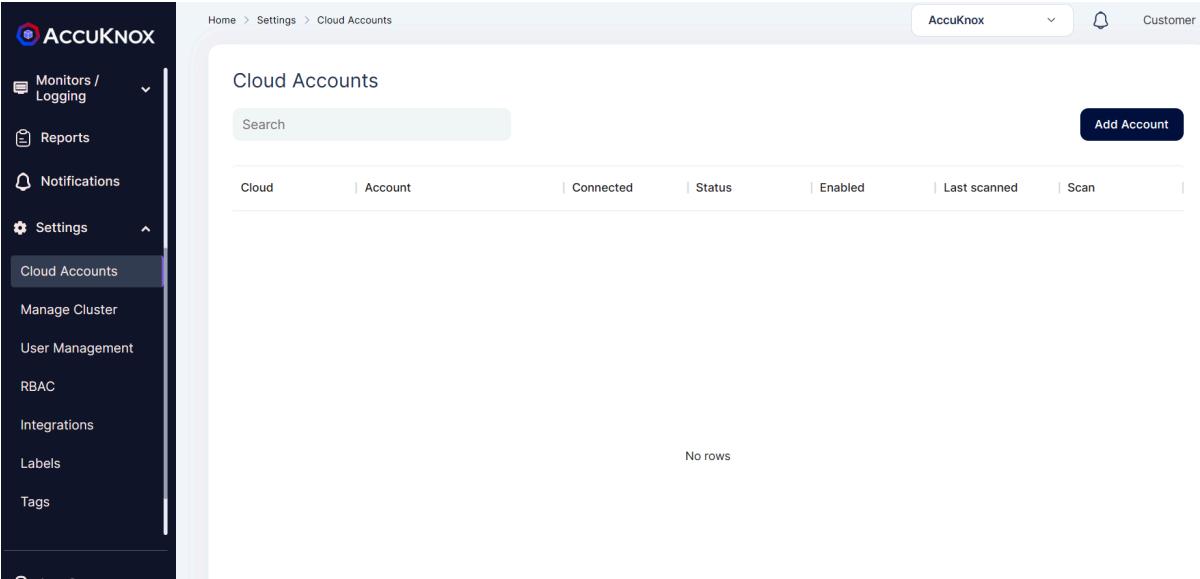
Step 12: Click the “Create“ button it will automatically download the JSON key.

3. Cloud Onboarding

3.1 AWS Onboarding

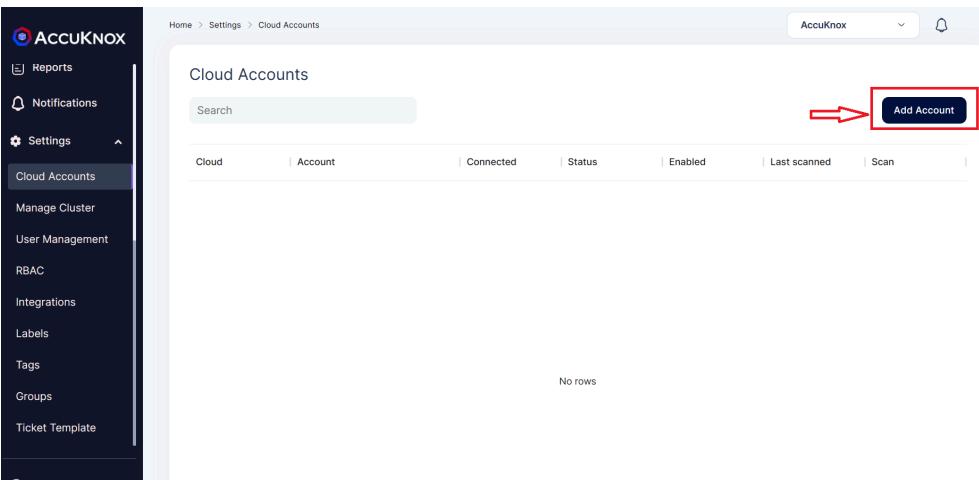
In this example we are onboarding an AWS account using the Access Keys method.

Step 1: To onboard Cloud Account Navigate to *Settings*→*cloud Accounts*



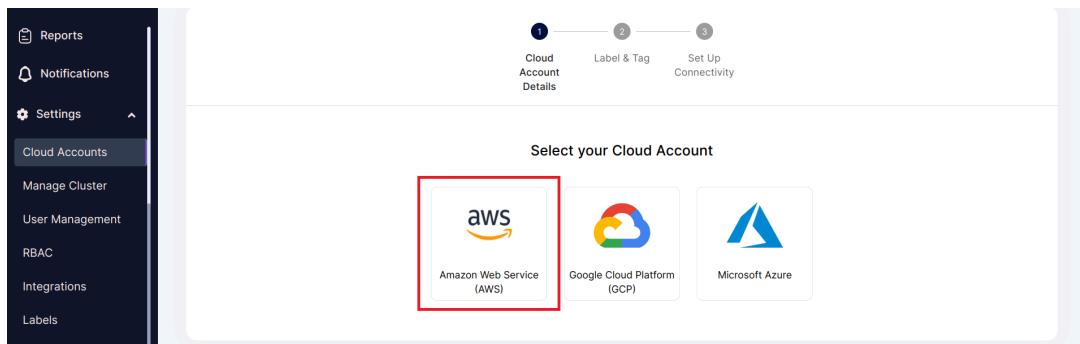
The screenshot shows the AccuKnox web interface. The left sidebar has a dark theme with white text. Under the 'Settings' section, 'Cloud Accounts' is selected and highlighted in purple. The main content area is titled 'Cloud Accounts' and contains a search bar and a table header with columns: Cloud, Account, Connected, Status, Enabled, Last scanned, and Scan. A large blue button labeled 'Add Account' is located in the top right corner of the main content area. The status bar at the bottom of the browser window shows a redacted URL and the number '36'.

Step 2: In the Cloud Account Page select *Add Account* option

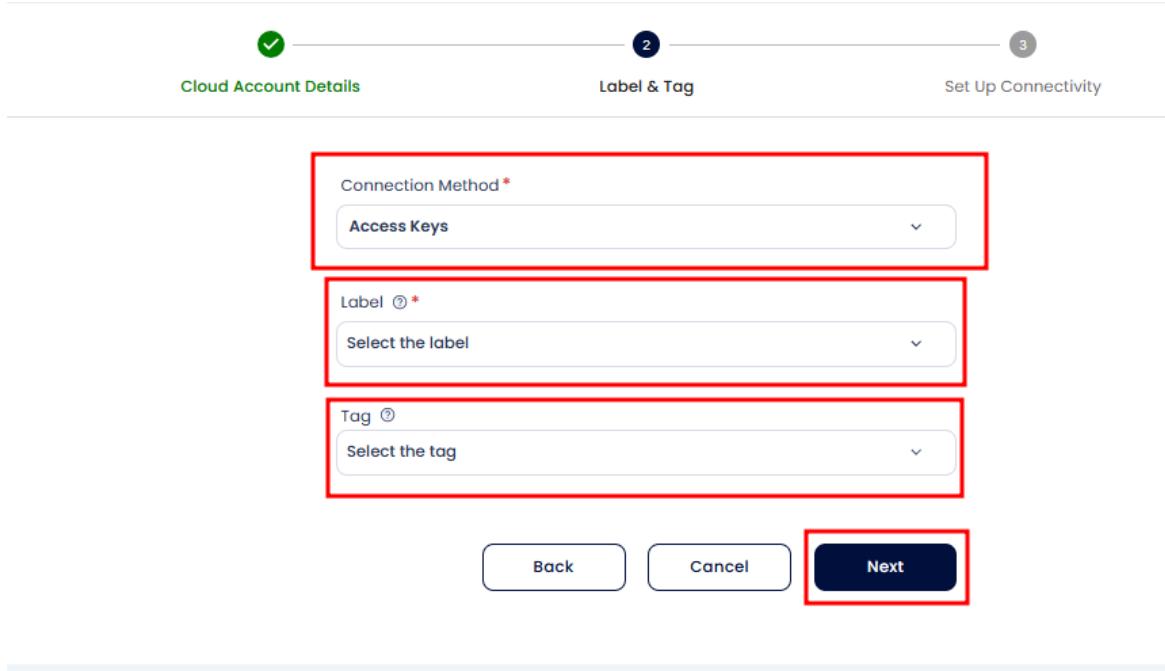


This screenshot is identical to the one above, showing the 'Cloud Accounts' page. However, a red arrow points to the 'Add Account' button, highlighting it as the next step. The rest of the interface and status bar are the same.

Step 3: Select the AWS option

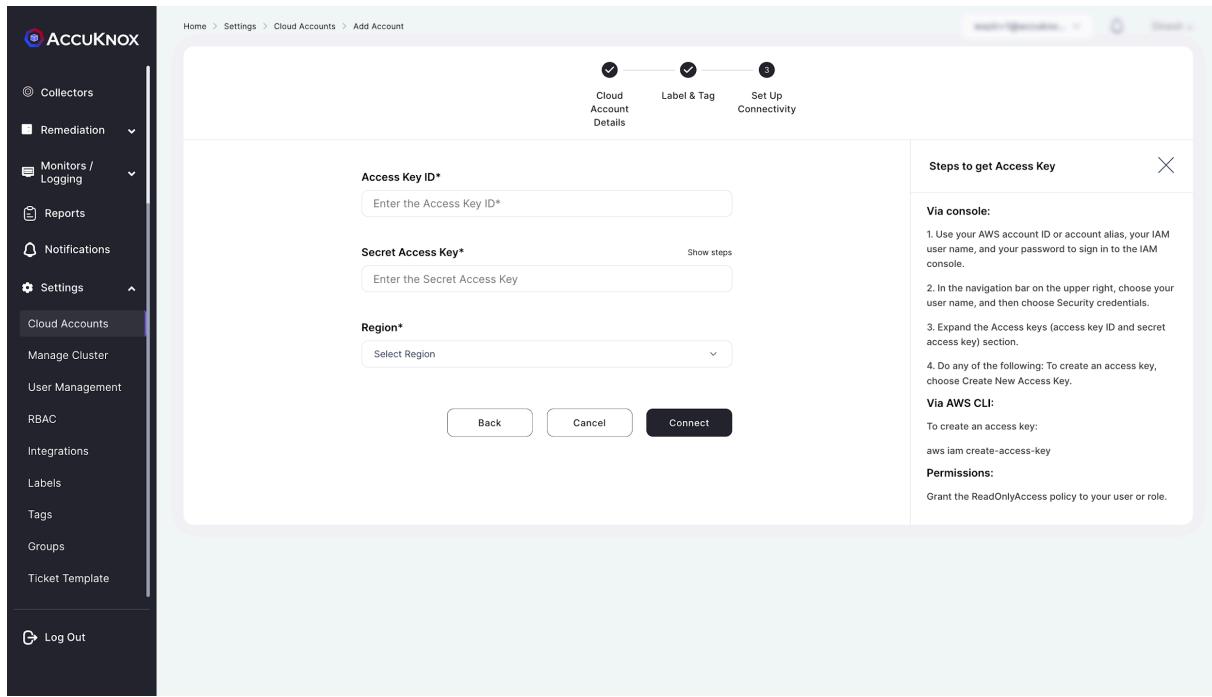


Step 4: In the next Screen select the Connection method, labels and Tags field from the dropdown Menu.

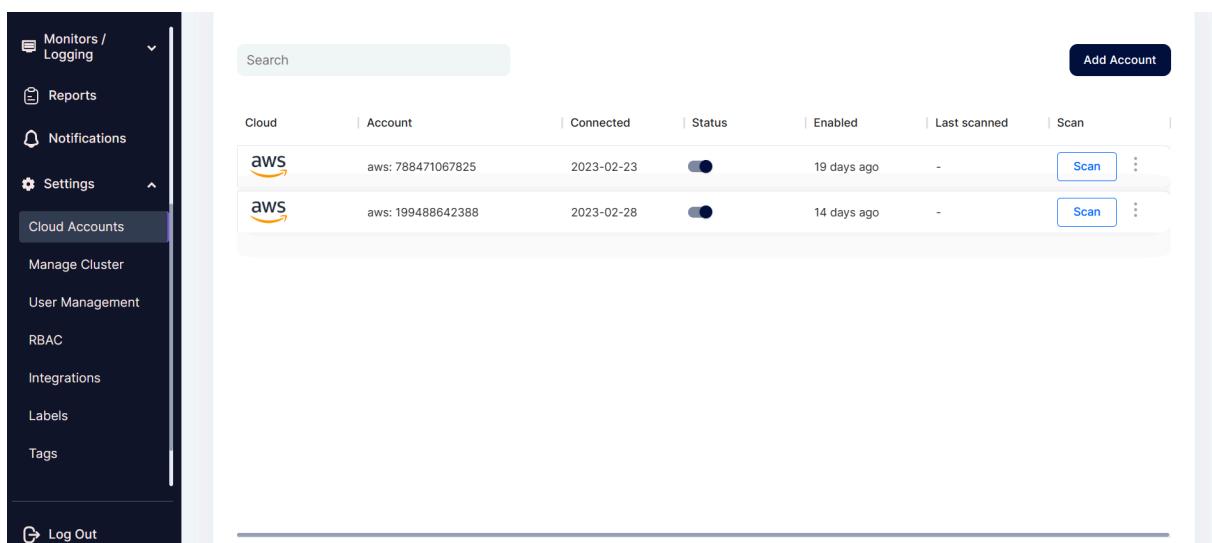


The screenshot shows the 'Cloud Account Details' step of a three-step wizard. The steps are: 1. Cloud Account Details (marked with a green checkmark), 2. Label & Tag (marked with a blue circle), and 3. Set Up Connectivity. The 'Label & Tag' step contains three dropdown menus: 'Connection Method *' (set to 'Access Keys'), 'Label ⓘ *' (set to 'Select the label'), and 'Tag ⓘ' (set to 'Select the tag'). The 'Next' button at the bottom right is highlighted with a red box.

Step 5: After giving labels and Tag in the Next Screen Provide the AWS account's Access Key and Secret Access Key ID and Select the Region of the AWS account.



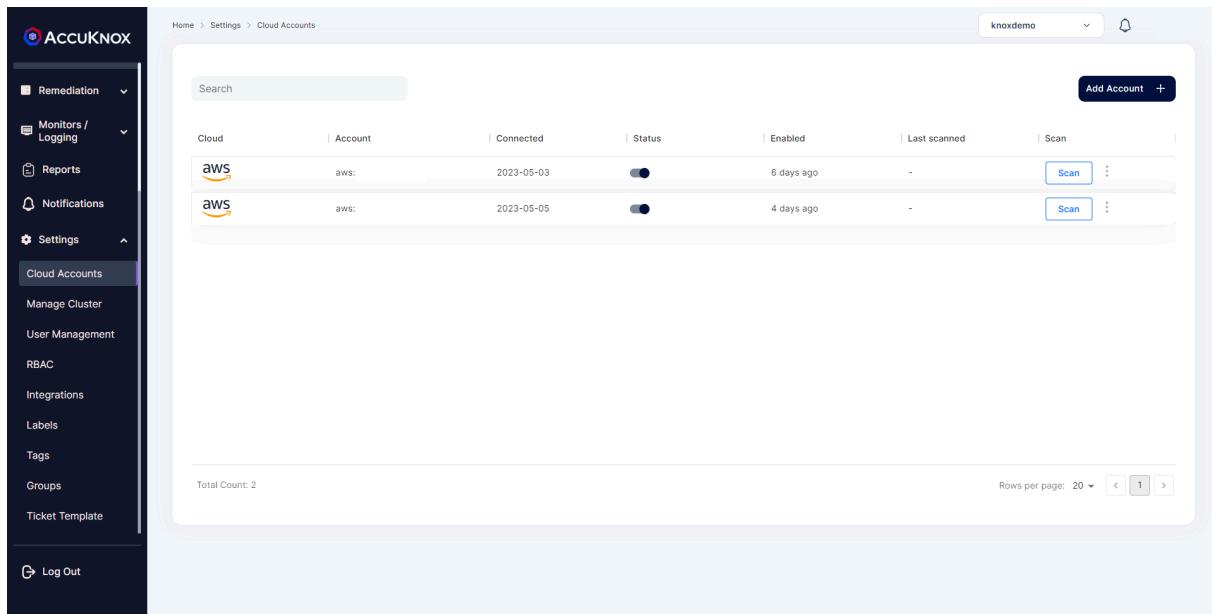
Step 6: AWS account is added to the AccuKnox using Access Key Method. We can see the onboarded cloud account by navigating to Settings→cloud Accounts option.



3.2 Azure Onboarding

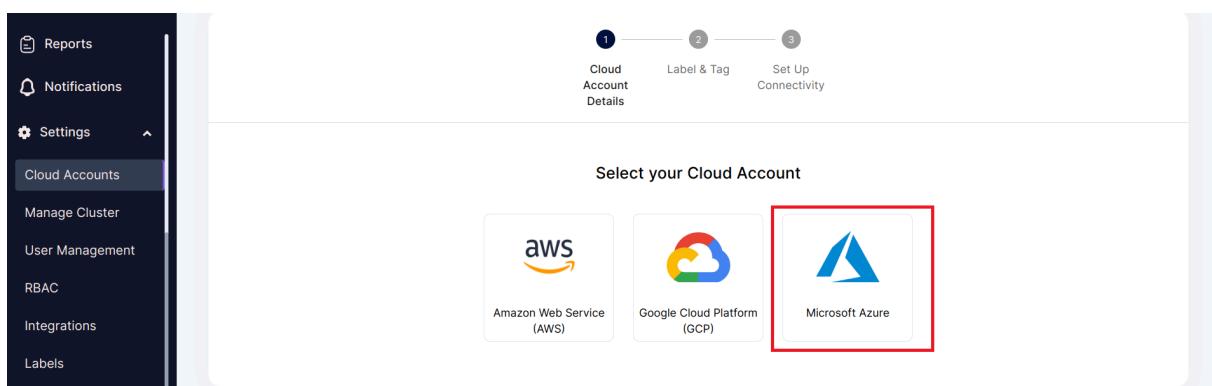
In order to onboard the Azure cloud account onto AccuKnox SaaS Platform.

Step 1: Go to settings→ Cloud Account and click on Add Account



Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aWS	aws:	2023-05-03	●	6 days ago	-	<button>Scan</button>
aWS	aws:	2023-05-05	●	4 days ago	-	<button>Scan</button>

Step 2: Select Microsoft Azure as Cloud Account Type

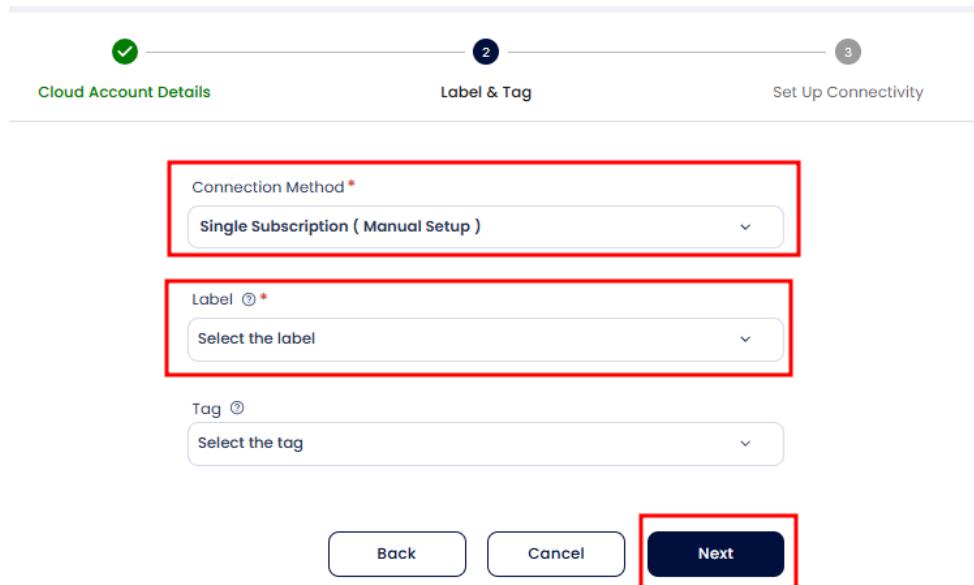


Cloud Account Details

Select your Cloud Account

- Amazon Web Service (AWS)
- Google Cloud Platform (GCP)
- Microsoft Azure

Step 3: Select Connection Method, create label and Tags that will be associated with this Cloud Account



Cloud Account Details 2 3

Label & Tag Set Up Connectivity

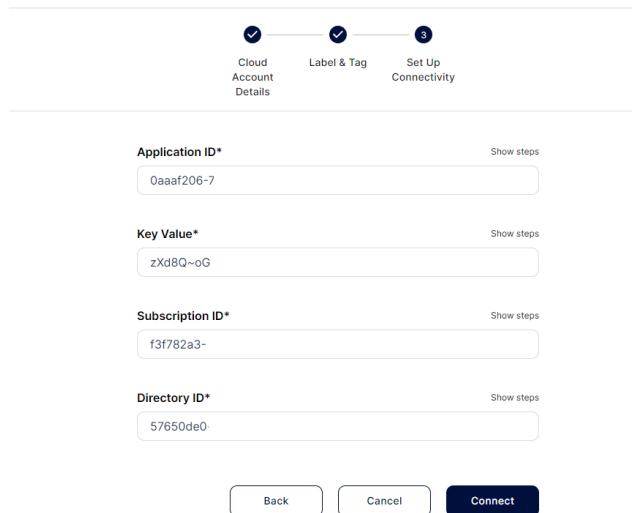
Connection Method*
Single Subscription (Manual Setup)

Label ②*
Select the label

Tag ②
Select the tag

Back Cancel **Next**

Step 4: 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



Cloud Account Details 2 3

Label & Tag Set Up Connectivity

Application ID*
0aaaf206-7

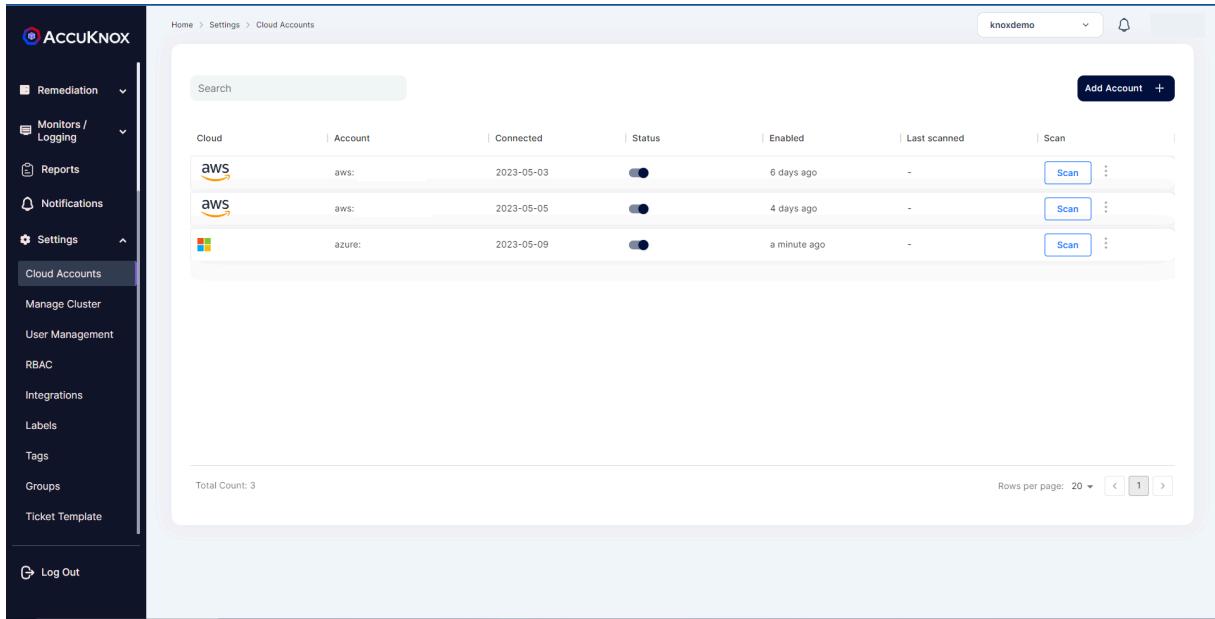
Key Value*
zXd8Q~oG

Subscription ID*
f3f782a3-

Directory ID*
57650de0

Back Cancel **Connect**

Step 5: After successfully connecting your cloud account will show up in the list



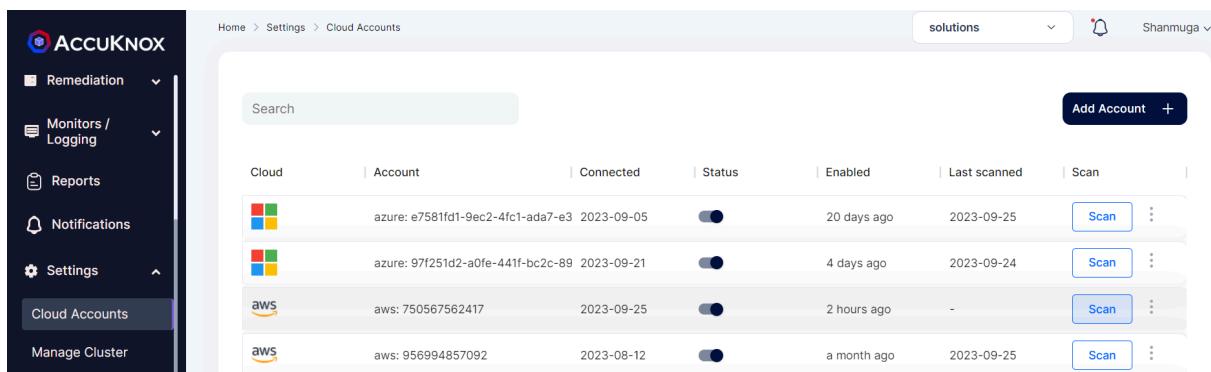
The screenshot shows the ACCUKNOX web interface for managing cloud accounts. The left sidebar includes options like Remediation, Monitors / Logging, Reports, Notifications, Settings (selected), Cloud Accounts (selected), Manage Cluster, User Management, RBAC, Integrations, Labels, Tags, Groups, Ticket Template, and Log Out. The main content area displays a table of connected accounts:

Cloud	Account	Connected	Status	Enabled	Last scanned	Scan	⋮
aws	aws:	2023-05-03	●	6 days ago	-	<button>Scan</button>	⋮
aws	aws:	2023-05-05	●	4 days ago	-	<button>Scan</button>	⋮
azure	azure:	2023-05-09	●	a minute ago	-	<button>Scan</button>	⋮

Total Count: 3 Rows per page: 20 < 1 >

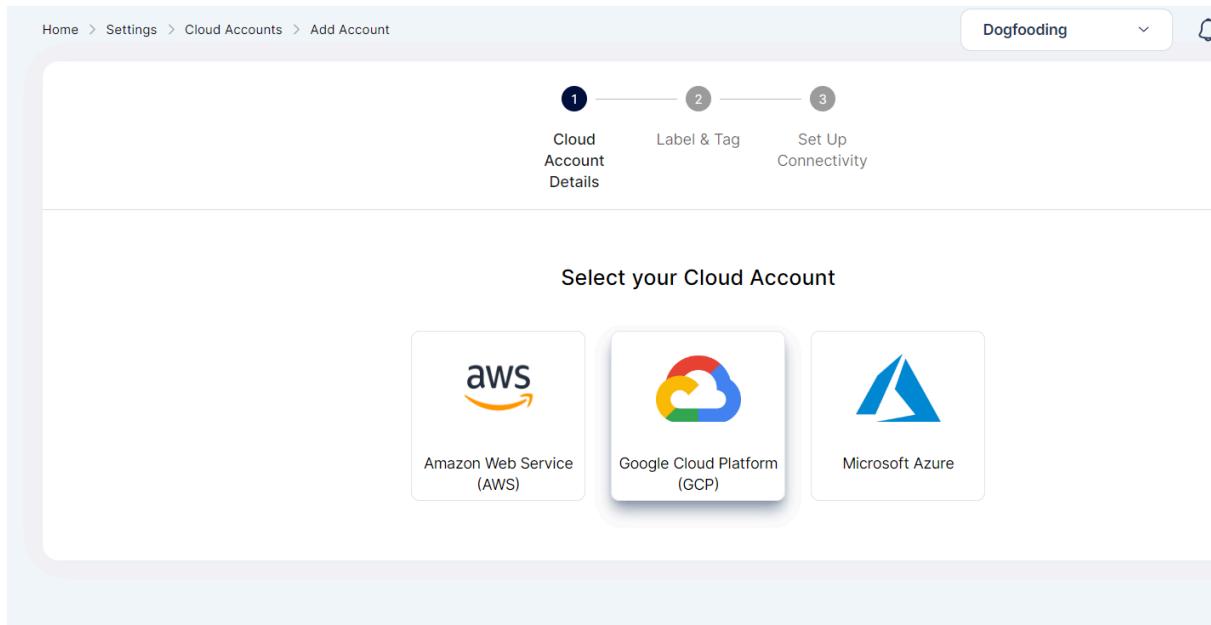
3.3 GCP Onboarding

Step 1: Go to the AccuKnox SaaS. Navigate to the “Settings” → “Cloud Accounts” then “Add Account”.



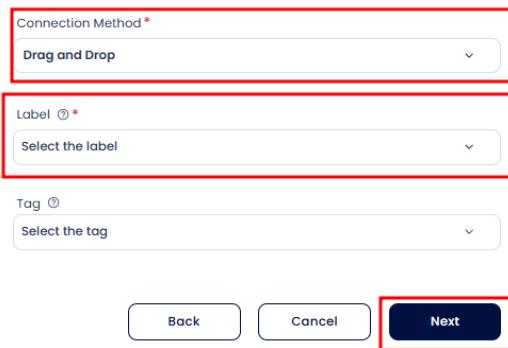
The screenshot shows the AccuKnox SaaS interface. The left sidebar has options like Remediation, Monitors / Logging, Reports, Notifications, Settings (selected), Cloud Accounts (selected), and Manage Cluster. The main area is titled "Cloud Accounts" and shows a table of connected accounts. The columns are Cloud, Account, Connected, Status, Enabled, Last scanned, and Scan. There are four entries: two Azure accounts (e7581fd1-9ec2-4fc1-ada7-e3 and 97f251d2-a0fe-441f-bc2c-89) and two AWS accounts (750567562417 and 956994857092). Each entry has a "Scan" button and a more options menu.

Step 2: Click the “GCP Platform”



The screenshot shows the "Add Account" wizard. The top navigation bar includes "Home", "Settings", "Cloud Accounts", and "Add Account". A dropdown shows "Dogfooding". The main area has a progress bar with three steps: 1. Cloud Account Details (selected), 2. Label & Tag, and 3. Set Up Connectivity. Below the progress bar is a section titled "Select your Cloud Account" with three options: "Amazon Web Service (AWS)", "Google Cloud Platform (GCP)" (highlighted in blue), and "Microsoft Azure".

Step 3: Select a Connection method, Create New Label and Add the Label for identifying the assets inside this account and add a Tag optionally.



Connection Method *

Drag and Drop

Label ⓘ *

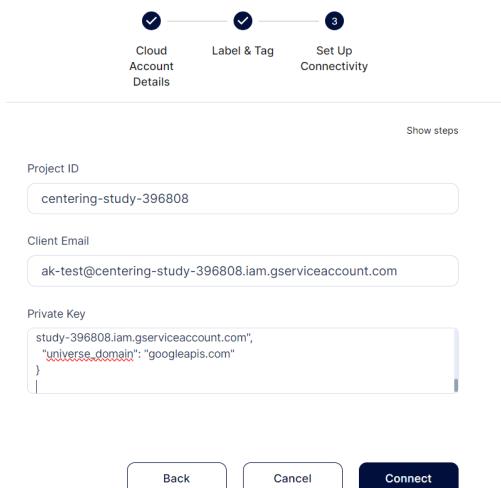
Select the label

Tag ⓘ

Select the tag

Back Cancel Next

Step 4: Enter the “Project ID”, “Client Email”(The Service Account mail ID) and “Private Key” from the downloaded File. Copy paste the entire downloaded file into the ”Private Key” field . Then Click “Connect“



Cloud Account Details

Label & Tag

Set Up Connectivity

Show steps

Project ID

centering-study-396808

Client Email

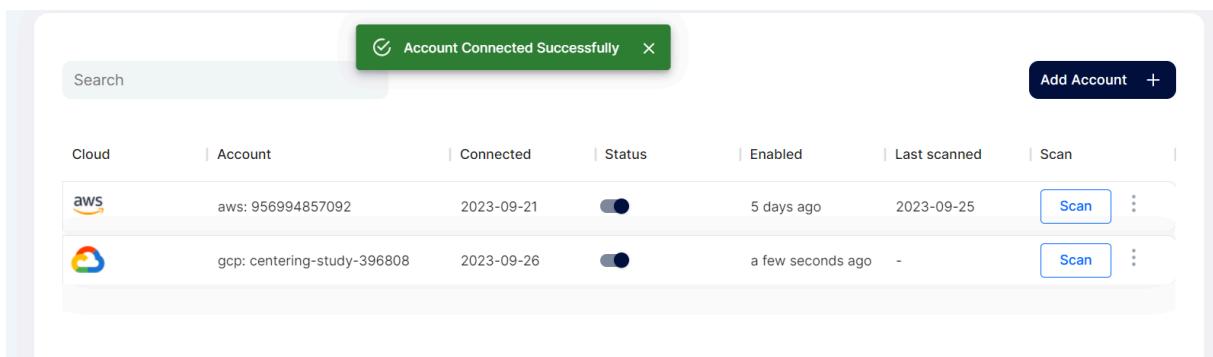
ak-test@centering-study-396808.iam.gserviceaccount.com

Private Key

```
study-396808.iam.gserviceaccount.com",
"universe_domain": "googleapis.com"
}
```

Back Cancel Connect

The cloud account has been onboarded successfully



Search

Account Connected Successfully

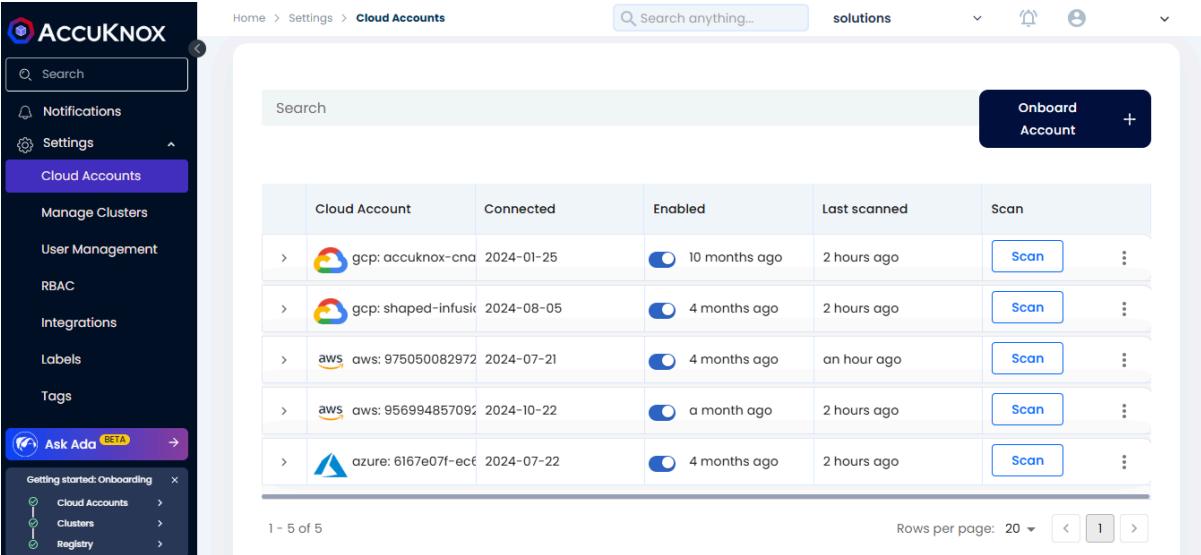
Add Account +

Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
aws	aws: 956994857092	2023-09-21	On	5 days ago	2023-09-25	Scan
gcp	gcp: centering-study-396808	2023-09-26	On	a few seconds ago	-	Scan

3.4 Cloud Account Deboarding

This guide outlines the steps for offboarding a cloud account from AccuKnox SaaS.

Step 1: Login to AccuKnox SaaS and Go to Cloud Accounts under Settings.

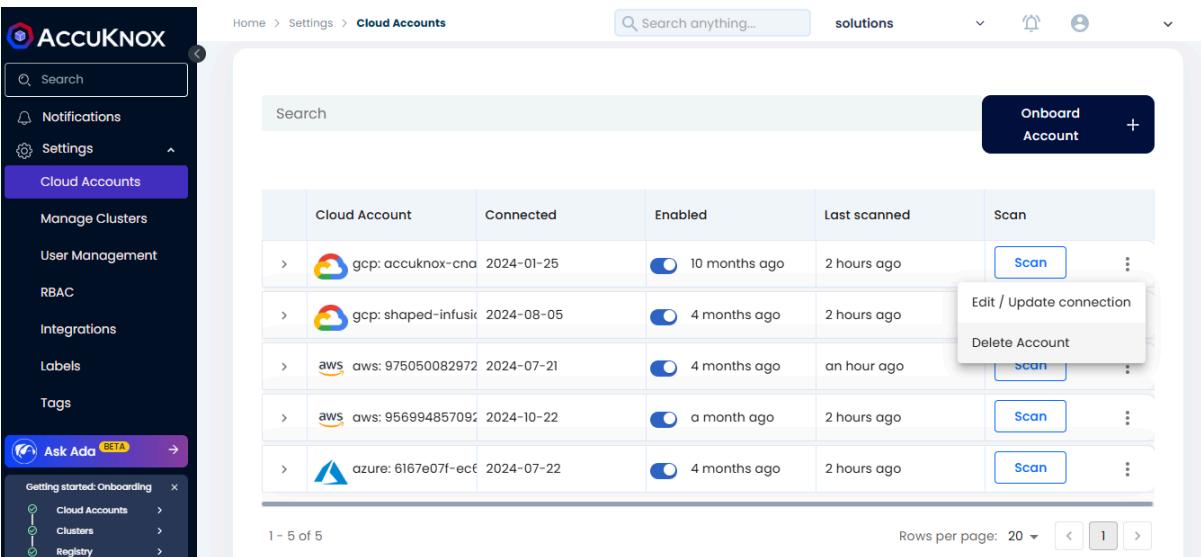


The screenshot shows the AccuKnox SaaS interface. On the left, there is a sidebar with a search bar, notifications, settings, and a 'Cloud Accounts' button which is highlighted in blue. Below that is an 'Ask Ada' button. Under 'Cloud Accounts', there are links for 'Cloud Accounts', 'Clusters', and 'Registry'. The main content area is titled 'Cloud Accounts' and shows a table of connected cloud accounts. The columns are 'Cloud Account', 'Connected', 'Enabled', 'Last scanned', and 'Scan'. There are five entries in the table:

Cloud Account	Connected	Enabled	Last scanned	Scan
> gcp: accuknox-cna	2024-01-25	<input checked="" type="checkbox"/>	10 months ago	2 hours ago
> gcp: shaped-infus	2024-08-05	<input checked="" type="checkbox"/>	4 months ago	2 hours ago
> aws: 975050082972	2024-07-21	<input checked="" type="checkbox"/>	4 months ago	an hour ago
> aws: 956994857092	2024-10-22	<input checked="" type="checkbox"/>	a month ago	2 hours ago
> azure: 6167e07f-ecf	2024-07-22	<input checked="" type="checkbox"/>	4 months ago	2 hours ago

At the bottom right of the table, there is a 'Rows per page:' dropdown set to 20, and a page navigation section showing '1 - 5 of 5'.

Step 2: Select the cloud account and click “Delete” to delete the account from SaaS.



The screenshot shows the same AccuKnox SaaS interface as the previous one, but with a context menu open over the first row of the table. The menu has two options: 'Edit / Update connection' and 'Delete Account'. The rest of the table and interface are identical to the first screenshot.

This will delete the cloud account from AccuKnox SaaS.

4. CWPP Prerequisites

4.1 Minimum Resource required

Deployments	Resource Usage	Ports	Connection Type	AccuKnox Endpoint
KubeArmor	CPU: 200 m, Memory: 200 Mi	-	-	-
Agents Operator	CPU: 50 m, Memory: 50 Mi	8081, 9090	Outbound	*.accuknox.com:8081 --> SPIRE Access *.accuknox.com:9090 --> SPIRE Health Check
Discovery Engine	CPU: 200 m, Memory: 200 Mi	-	-	-
Shared Informer Agent	CPU: 20 m, Memory: 50 Mi	3000	Outbound	*.accuknox.com:3000 --> knox-gateway
Feeder Service	CPU: 50 m, Memory: 100 Mi	3000	Outbound	*.accuknox.com:3000 --> knox-gateway
Policy Enforcement	CPU: 10 m, Memory: 20 Mi	443	Outbound	*.accuknox.com:443 --> Policy Provider Service

These ports need to be allowed through the firewall.

4.2 AccuKnox Agents

We have the agent-based model for CWPP. This offers a balanced approach providing non-intrusive scanning for cloud accounts – not to mention the deep visibility for workloads using eBPF-based agents.

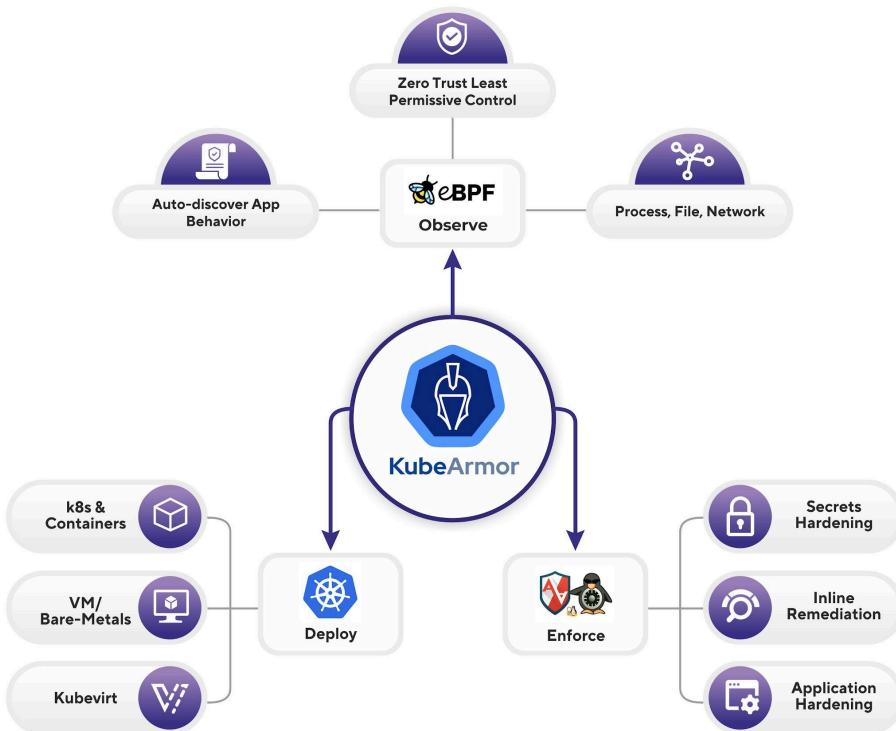
CWPP (Requires Agent)	Protects cloud workloads against Zero-Day Attacks and safeguards against runtime exploits.
Runtime Anomaly Detection	Detects anomalies in application behavior, compliance drift, and attack analysis with detailed context.
Container Forensics Analysis	Helps analyze containers for deep packet-level inspection and understanding of security controls.
Mitigation of Runtime Vulnerabilities	Mitigates exploitable vulnerabilities by applying least permissive security posture.
Protection from Cloud Native Attacks	Essential for safeguarding against sophisticated cloud native attacks that can evade agentless detection.

Note that we also offer an agentless model for CSPM. This is a lightweight, non-intrusive approach that provides deep visibility into cloud accounts without the need for agents. AccuKnox's hybrid approach optimizes cloud security for diverse organizational needs.

Listed below are the various agents that are part of the AccuKnox solution.

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. It operates with Linux security modules LSMs, meaning that it can work on top of any Linux platforms (such as Alpine, Ubuntu, and Container-optimized OS from Google) if Linux security modules (e.g., AppArmor, SELinux, or BPF-LSM) are enabled in the Linux Kernel. KubeArmor will use the appropriate LSMs to enforce the required policies.



KubeArmor allows operators to define security policies and apply them to Kubernetes. Then, KubeArmor will automatically detect the changes in security policies from Kubernetes and enforce them on the corresponding containers and nodes. If there are any violations against security policies, KubeArmor immediately generates alerts with container identities. If operators have any logging systems, it automatically sends the alerts to their systems as well.

2. Feeder Service

The feeder service sends information from the Client Cluster to the AccuKnox SaaS Control Plane. Feeder Service is an agent which runs on every node, collects telemetry/alert events from source systems & messages, and emits them to Messaging Cluster for Storage & Analysis. Ways in which the Feeder service communicates to the central control plane:

- Directly posting messages to Kafka Topic
- List of topics (Each component has a separate topic name) on where the feeder service publishes feeds.
- Posting via a GRPC or REST API Service

All communication between Feeder and Control plane (Kafka, etc) is encrypted using TLS. Feeder Service uses a secret key from Kubernetes secrets to be applied to it when connecting to the control plane. This secret key allows the feeder to talk to the control plane and exchange data for a particular tenant-id/workspace-id. This is an API key that is generated as part of the cluster onboarding. The feeder service will self-assess some metrics and logs and send that information to the Control plane for its own health assessment for one or more components including its own (running on nodes). The Feeder Service makes it simpler to monitor the detailed communication between each entity.

3. Shared Informer Agent

Shared Informer Agent watches all the changes occurring in Kubernetes entities such as Pods, Nodes, Namespaces, Endpoints, and Services.

- Any changes to an entity can be easily tracked by the Shared Informer Agent such as the Creation of an entity, the update of an entity, and if any entity has been deleted and as soon as the changes occur to the entities, the Shared Informer Agent pushes the information to the backend.
- The Shared Informant Agent makes it simpler to track and manage all of the entities that are present in Kubernetes as well as see changes in entities as they occur in real-time.

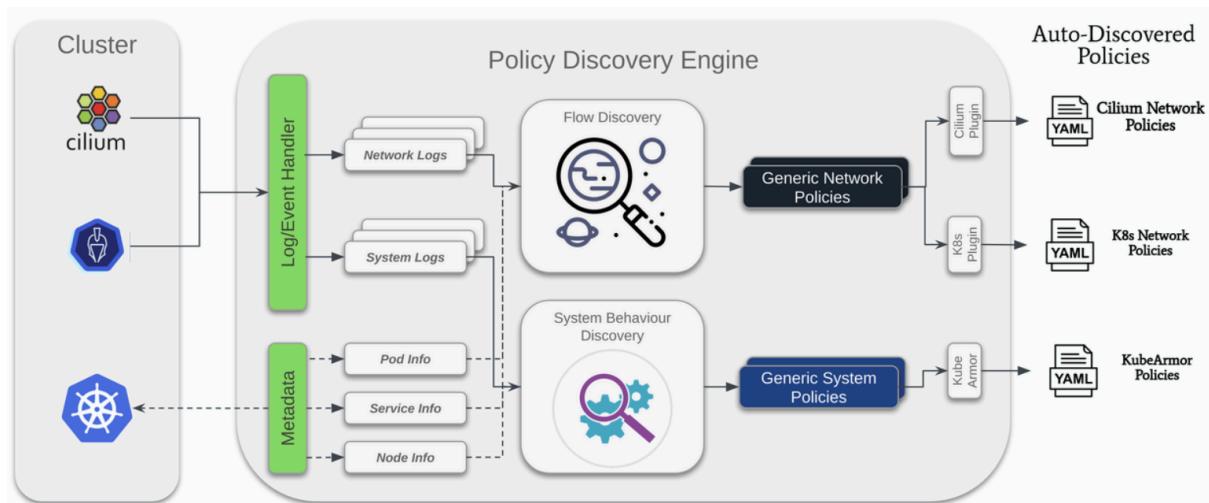
4. Policy Enforcement Agent

AccuKnox's Policy Enforcement Agent enforces the policies by leveraging KubeArmor and Cilium. Policy Enforcement Agent not only keeps the track of the policies but is capable of doing tasks such as applying policies, denying policies, updating policies, and deleting the policies.

- The policy enforcement agent encrypts and decrypts the policies while handing them to and from the policy provider service. It reads the specification of the policies and provides back to the policy provider service.
- All of the changes done to the policy can be tracked granularly with the help of the Policy Enforcement Agent and Policy Gitops Flow which helps with version control and robust management of the security policies.

5. Discovery Engine

AccuKnox policy enforcement engine based on KubeArmor is very flexible and powerful. However, these policy engines must be fed with policies. With 10s or 100s of pods and workloads running in a cluster, it is insanely difficult to handcraft such policies. AccuKnox policy auto-discovery engine leverages the pod visibility provided by KubeArmor to auto-generate network and system policies.



AccuKnox's Runtime security solution is able to provide full visibility into all of these application interactions with the host kernel and provide the ability to filter or restrict specific actions at runtime.

With AccuKnox you can automatically discover the application interaction and network interaction (as described below) in the form of policy as code subsequently these policies can be audited or enforced at runtime giving you the ability to restrict specific behaviors of the application.

For example, you could have a policy that states the following:

- Pod A cannot access the /etc/bin folder
- Pod B cannot initiate ptrace i.e. trace the execution of other processes.
- Pod C cannot communicate to a remote TCP server running on port 5000.

This list can be as exhaustive as you like, and these policies are enforced within the kernel using kernel primitives and technologies as listed below:

Network Security using eBPF

- Network runtime protection in the form of L3, L4, and L7 rules using identity (x509 certificates or K8s labels) for your K8s workloads. In K8s policies, this is implemented as a native K8s networkpolicy object.
- For Virtual Machine workloads, labels are used to provide host-level network policies for L3, L4, and L7.

Application security using Linux Security Modules (LSM) / KubeArmor

- The Linux Security Module (LSM) framework provides a mechanism for various security checks to be hooked by new kernel extensions. It denies access to essential kernel objects, such as files, inodes, task structures, credentials, and inter-process communication objects.
- AccuKnox supports AppArmor, SELinux and BPFLSM as of today for its enforcement engine at runtime.

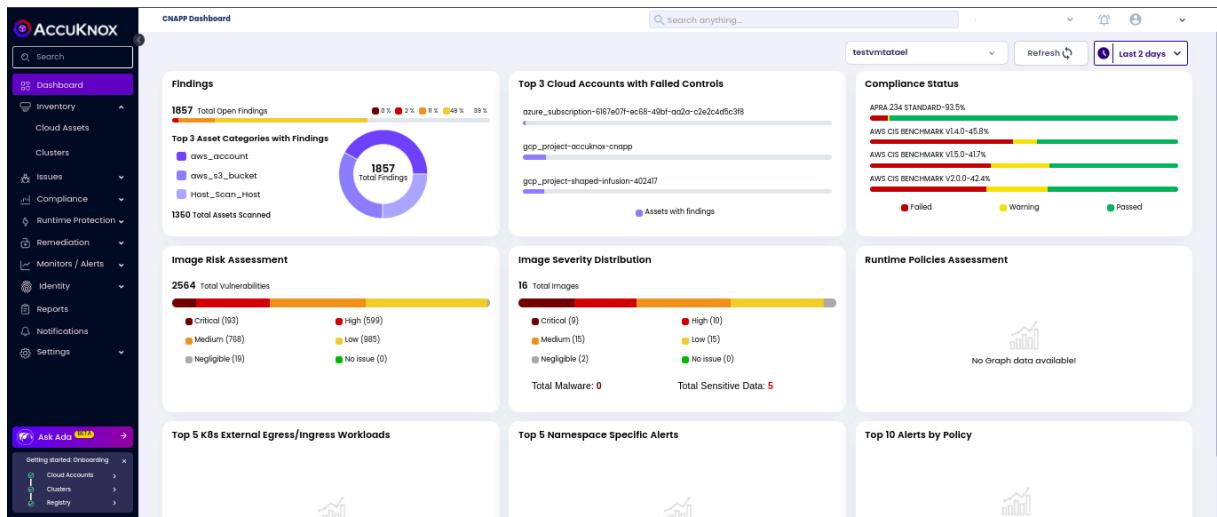
5. Cluster Onboarding

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

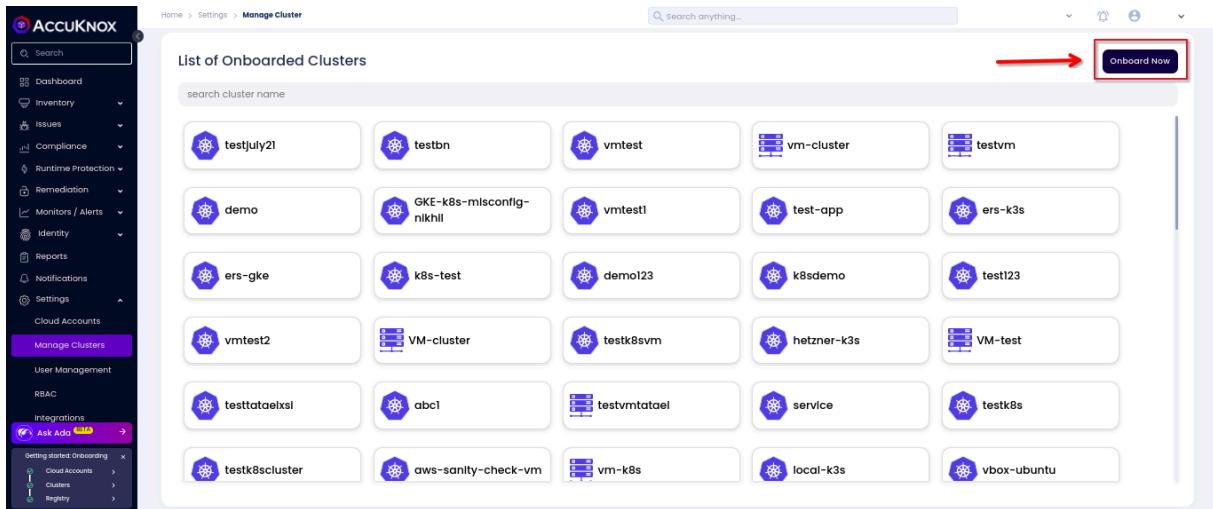
Below shown image is from an k3s cluster running in a local machine with Kali Linux Operating System. We can onboard this cluster by following the steps shown below

```
(Accuknox@kali)-[~]
└$ kubectl get pods
NAME      READY   STATUS    RESTARTS   AGE
nginx-demo 1/1     Running   0          22s
redis-demo 1/1     Running   0          14s
```

Step 1: As a first time user, the management console will show up the CNAPP dashboard without any data mentioned in widgets, since the cloud account and cluster onboarding is not done.

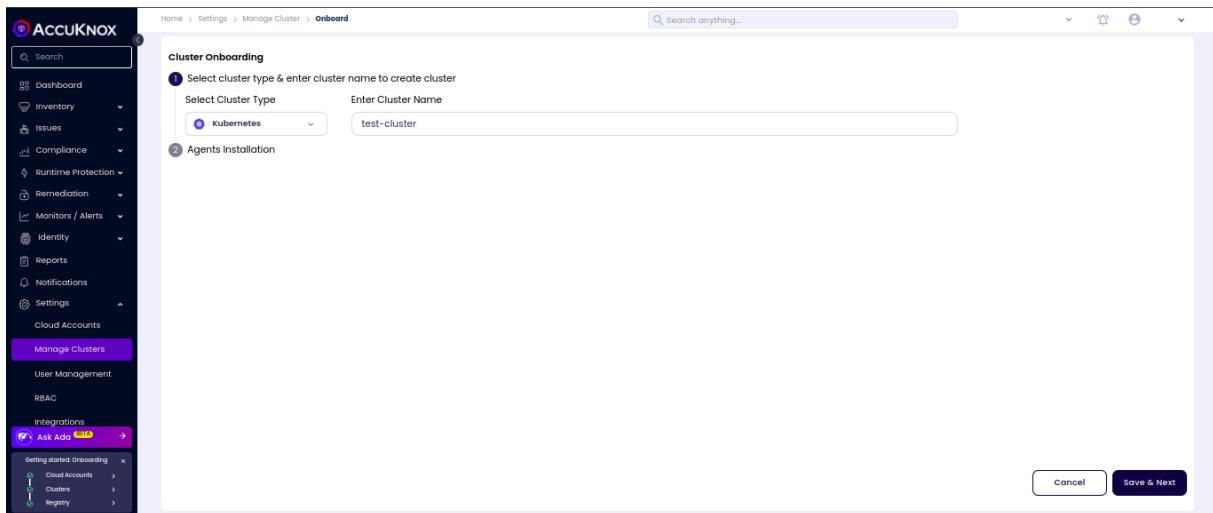


Step 2: Navigate to Manage Cluster from Settings Tab: From this page we can onboard the clusters running in various cloud platforms like GCP,AWS and Azure. We can onboard locally setup clusters using an cloud option. To onboard cluster select onboard now option



The screenshot shows the AccuKnox web interface. On the left is a sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, Settings, Cloud Accounts, Manage Clusters (which is selected), User Management, RBAC, and Integrations. Below these are sections for Getting Started Onboarding (Cloud Accounts, Clusters, Registry) and Ask AccuKnox (with a purple button). The main content area is titled 'List of Onboarded Clusters' and contains a grid of 20 cluster icons with names such as 'testjuly21', 'testbn', 'vmtest', etc. In the top right corner of this section, there is a dark blue button labeled 'Onboard Now' with a red arrow pointing to it.

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



This screenshot shows the 'Cluster Onboarding' step. The sidebar on the left is identical to the previous one. The main area has a title 'Cluster Onboarding' and two steps listed: 1. Select cluster type & enter cluster name to create cluster (with a dropdown for 'Select Cluster Type' set to 'Kubernetes' and an input field for 'Enter Cluster Name' containing 'test-cluster'). Step 2, 'Agents Installation', is shown below. At the bottom right are 'Cancel' and 'Save & Next' buttons.

Step 4: Installing KubeArmor and AccuKnox agents

We are going to install KubeArmor and AccuKnox-agents to connect to the AccuKnox SaaS application. For the agent installation selection click on the Runtime Visibility & Protection.

Step 4.1 KubeArmor Installation

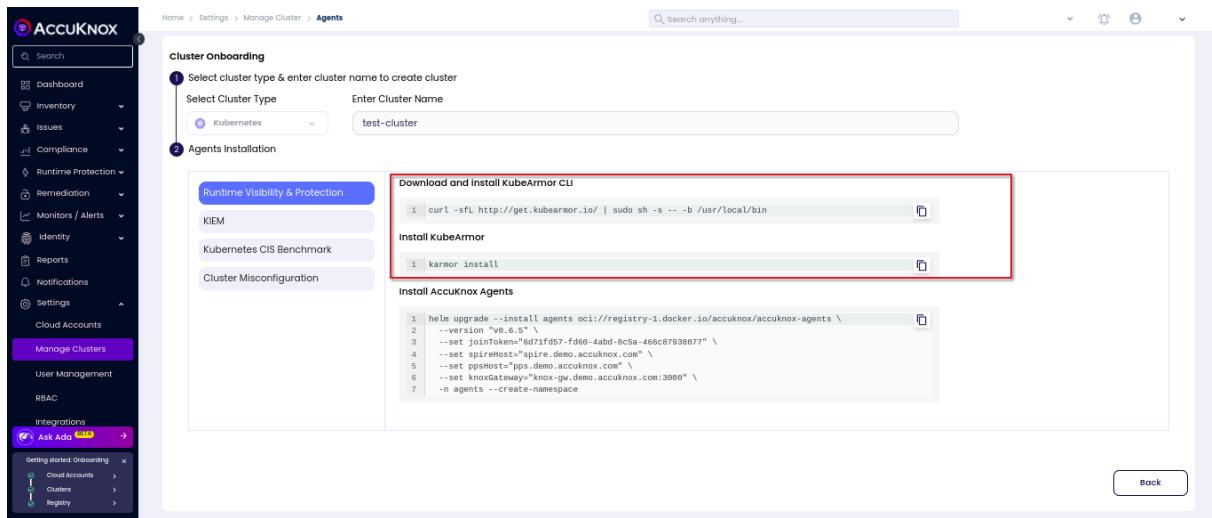
KubeArmor

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.



The screenshot shows the AccuKnox web interface under the 'Agents' section of the 'Manage Cluster' settings. The 'Cluster Onboarding' step is selected. A red box highlights the command-line interface (CLI) area, which contains the following commands:

```

curl -sL http://get.kubearmor.io/ | sudo sh -s -- -b /usr/local/bin
karm install
helm upgrade --install agents oci://registry-1.docker.io/accuknox/accuknox-agents \
--version "v0.6.5" \
--set joinToken="6d71fd57-fd68-4abd-8c5a-466e87938677" \
--set spireHost="spire.demo.accuknox.com" \
--set ppsHost="pps.demo.accuknox.com" \
--set knoxGateway="knox-gw.demo.accuknox.com:3060" \
--n agents --create-namespace

```

KubeArmor is installed using the following commands:

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

Sample Output:

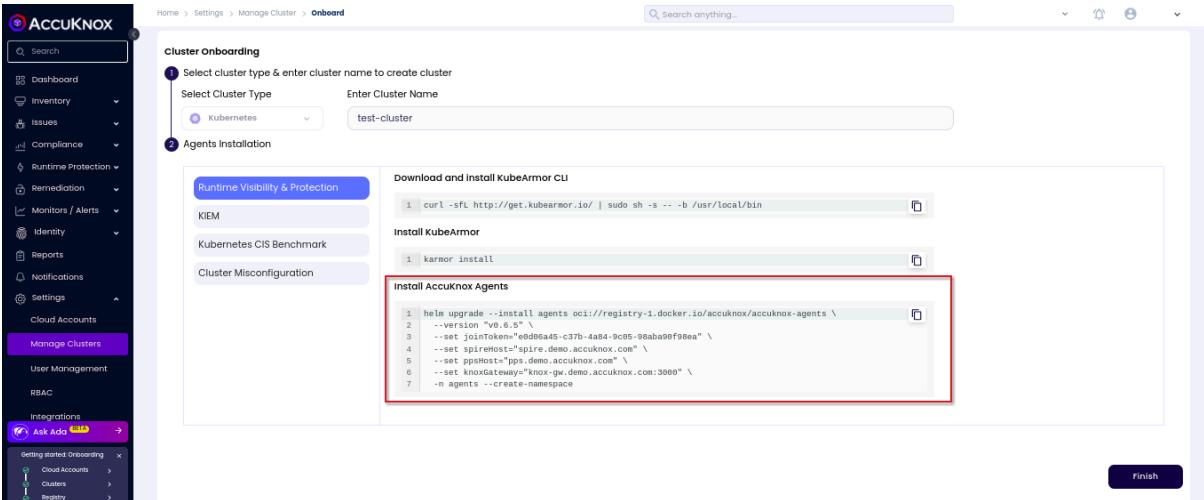
```
(Accuknox㉿kali)-[~]  
└$ curl -sfl http://get.kubearmor.io/ | sudo sh -s -- -b /usr/local/bin  
kubearmor/kubearmor-client info checking GitHub for latest tag  
kubearmor/kubearmor-client info found version: 1.2.3 for  
v1.2.3/linux/amd64  
kubearmor/kubearmor-client info installed /usr/local/bin/karmor  
kubearmor/kubearmor-client info karmor is installed in /usr/local/bin  
kubearmor/kubearmor-client info invoke /usr/local/bin/karmor or move  
karmor to your desired PATH  
  
(Accuknox㉿kali)-[~]  
└$ karmor install  
🛡️ Installed helm release : kubearmor-operator  
😊 KubeArmorConfig updated  
⌚ This may take a couple of minutes  
🎉 KubeArmor Snitch Deployed!  
🎉 KubeArmor Daemonset Deployed!  
Done Checking , ALL Services are running!  
Execution Time : 1m22.006691427s  
VERIFYING KUBEARMOR FUNCTIONALITY (this may take upto a minute)  
|. Verifying KubeArmor functionality (this may take upto a minute)  
🛡️ Your Cluster is Armored Up!  
  
(Accuknox㉿kali)-[~]  
└$
```

Step 4.2: AccuKnox-Agents installation

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

AccuKnox Agents

1. **KubeArmor:** KubeArmor is a cloud-native runtime security enforcement system that restricts the behavior (such as process execution, file access, and networking operation) of containers and nodes at the system level. KubeArmor dynamically set the restrictions on the pod. KubeArmor leverages Linux Security Modules (LSMs) to enforce policies at runtime.
2. **Feeder Service:** It collects the feeds from kubeArmor and relays to the app.
3. **Shared Informer Agent:** It collects information about the cluster like pods, nodes, namespaces etc.,
4. **Policy Discovery Engine:** It discovers the policies using the workload and cluster information that is relayed by a shared informer Agent.



The screenshot shows the AccuKnox web interface under the 'Cluster Onboarding' section. Step 1: 'Select cluster type & enter cluster name to create cluster'. Step 2: 'Agents Installation'. Under 'Runtime Visibility & Protection', there are sections for KIEM, Kubernetes CIS Benchmark, and Cluster Misconfiguration. The 'Install AccuKnox Agents' section contains a command-line interface (CLI) box with a red border around the command:

```
1 helm upgrade --install agents oci://registry-1.docker.io/accuknox/accuknox-agents \
2   --version "v0.6.5" \
3   --set joinToken="*****-*****-*****-*****" \
4   --set spireHost="spire.demo.accuknox.com" \
5   --set ppsHost="pps.demo.accuknox.com" \
6   --set knoxGateway="knox-gw.demo.accuknox.com:3000" \
7   -n agents --create-namespace
```

AccuKnox Agents can be installed using the following command:

```
helm upgrade --install agents
oci://registry-1.docker.io/accuknox/accuknox-agents
--version "v0.6.5"
--set joinToken="*****-*****-*****-*****"
--set spireHost="spire.demo.accuknox.com"
--set ppsHost="pps.demo.accuknox.com"
--set knoxGateway="knox-gw.demo.accuknox.com:3000"
-n agents --create-namespace
```

Sample Output:

```
WARNING: Kubernetes configuration file is group-readable. This is
insecure. Location: /etc/rancher/k3s/k3s.yaml

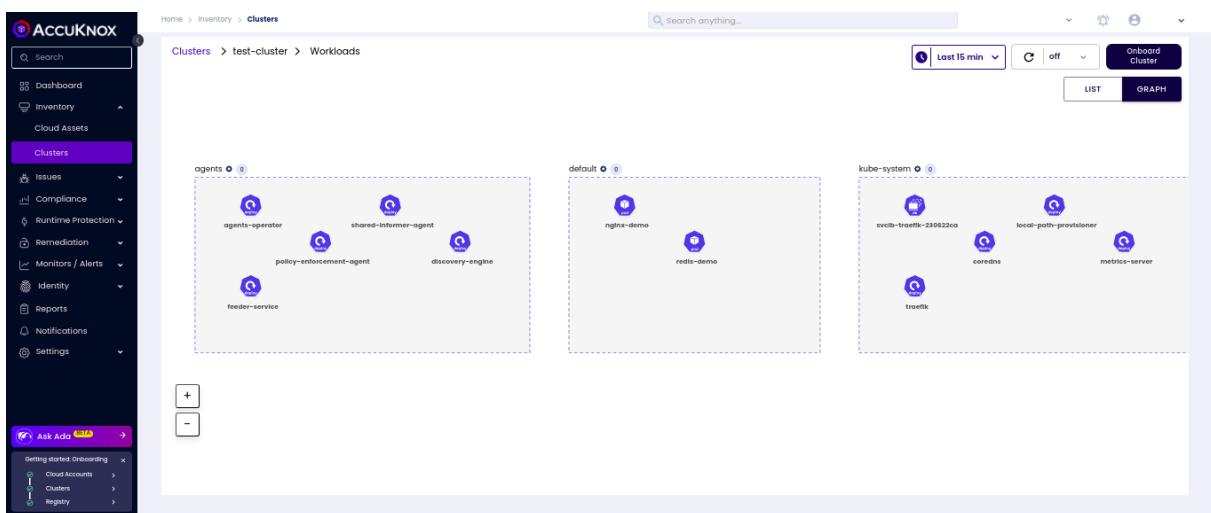
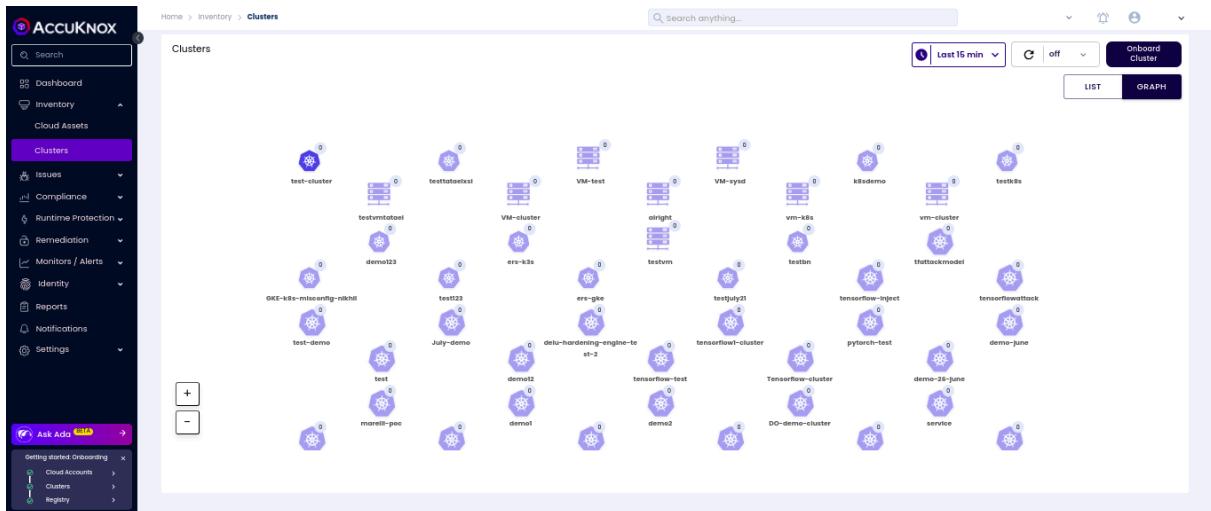
WARNING: Kubernetes configuration file is world-readable. This is
insecure. Location: /etc/rancher/k3s/k3s.yaml
Release "agents" does not exist. Installing it now.
Pulled: registry-1.docker.io/accuknox/accuknox-agents:v0.6.5
Digest:
sha256:420a4dae8225ce1eb201b5468c588eeb71bbf532f9d9f1eafac2281760f61e11
NAME: agents
LAST DEPLOYED: Fri Jul 26 15:23:37 2024
NAMESPACE: agents
STATUS: deployed
REVISION: 1
TEST SUITE: None

(Accuknox㉿kali)-[~]
└$
```

Note: In the above command joinToken is specific to this example and it will vary based on the cluster

Step 5: Onboarded Cluster

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. There all the onboarded clusters will be listed out and all the inactive ones would be grayed out. By double clicking on the active cluster user can get a more detailed view of the cluster.



6. Cluster Offboarding

This guide outlines the steps for offboarding a cluster from AccuKnox SaaS. The process involves uninstalling the agents from the cluster and deleting the cluster from AccuKnox SaaS.

Below, you will find detailed instructions for agent uninstallation from your cluster CLI and deleting the cluster from AccuKnox SaaS. These steps apply to all clusters.

1. Agents Uninstallation

Uninstall AccuKnox agents using the following commands:

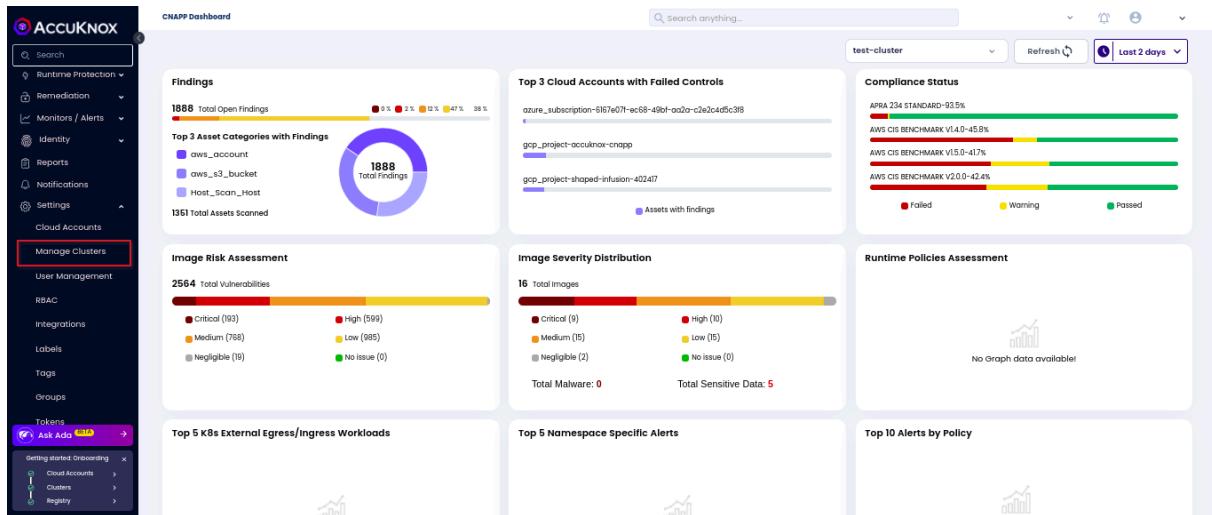
```
helm uninstall agents -n agents && kubectl delete ns agents;
helm uninstall cis-k8s-job;
helm uninstall kiem-job;
helm uninstall k8s-risk-assessment-job
```

2. Sample for Uninstalling Runtime Visibility & Protection agents

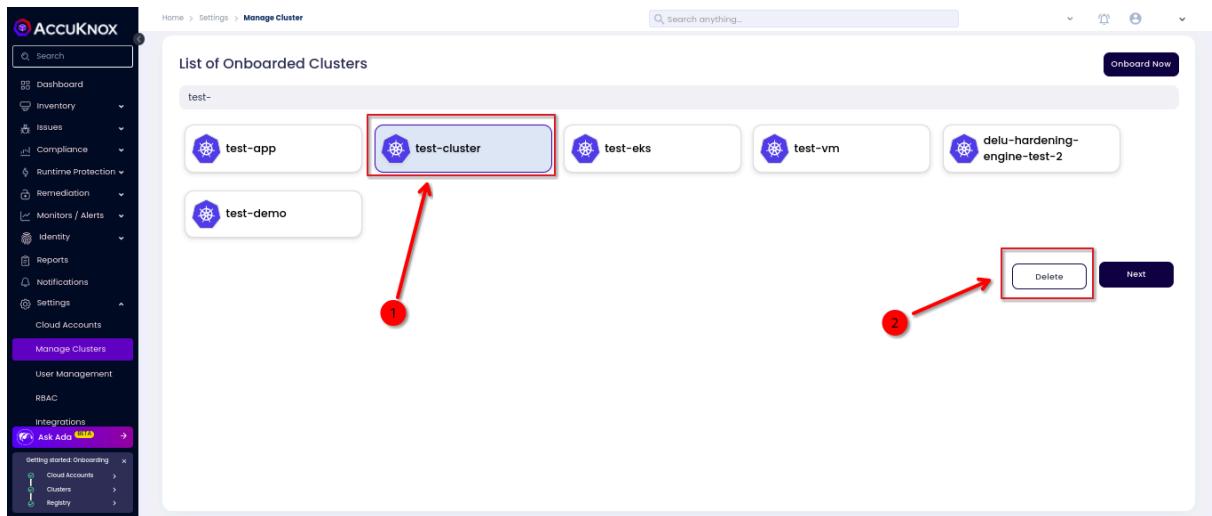
```
(Accuknox㉿kali)-[~]
└─$ helm uninstall agents -n agents && kubectl delete ns agents
WARNING: Kubernetes configuration file is group-readable. This is insecure.
Location: /etc/rancher/k3s/k3s.yaml
WARNING: Kubernetes configuration file is world-readable. This is insecure.
Location: /etc/rancher/k3s/k3s.yaml
release "agents" uninstalled
namespace "agents" deleted
```

3. Cluster Deletion

Step 1: Login to AccuKnox SaaS and Go to Manage Cluster under Settings



Step 2: Select the cluster and click Delete to delete the cluster from SaaS.



This will delete the cluster from AccuKnox SaaS

7. VM Onboarding with Systemd/Docker Mode

7.1 Systemd

Systemd is a core component of modern Linux systems responsible for managing services and processes. It ensures that essential services start automatically during boot, remain running, and restart if they fail. In simple terms, systemd acts like a **controller** that organizes and oversees everything needed to keep the system stable and functional.

Currently, **root/sudo** permissions are needed for onboarding systemd. This is because KubeArmor requires privileges to protect the host and systemd services, packages are currently installed on the root directory.

Only in case of the control plane node, a working RabbitMQ server is required. This can be installed using Docker.

```
# Latest RabbitMQ 3.13
docker run -it --rm --name rabbitmq -p 5672:5672 -p 15672:15672
rabbitmq:3.13-management
```

Alternatively, you can install RabbitMQ using a package manager:

- **Linux, BSD, UNIX:** [Debian](#), [Ubuntu](#) | [RHEL](#), [CentOS Stream](#), [Fedora](#) | [Generic binary build](#) | [Solaris](#)
- **Windows:** [Chocolatey package](#) | [Windows Installer](#) | [Binary build](#)
- **MacOS:** [Homebrew](#) | [Generic binary build](#)
- **Erlang/OTP for RabbitMQ**

BTF support is needed. Any kernel version which has this should work. Check if BTF info is present with the script below:

```
if [ ! -e "/sys/kernel/btf/vmlinux" ]; then
    echo "BTF info not present"
else
    echo "BTF info present"
fi
```

If the script returns "BTF info not present," [BTF support is not available](#), and you should run the script below to build the required files on your system:

```
# Download KubeArmor
git clone https://github.com/kubearmory/KubeArmor/
cd KubeArmor/KubeArmor/packaging
./post-install.sh
```

For detailed instructions specific to SystemD Based Non-BTF Environments, please refer to this [guide](#).

7.1.1 Container Protection Requirements (Optional)

If container protection is needed, a Linux Kernel with **BPF LSM** is desired. Generally, it is present in v5.8+. Here's a guide on enabling BPF LSM: [KubeArmor Getting Started FAQ](#).

If BPF LSM is not available, AppArmor should still work out of the box for host policy application. However, follow the guide [Support for non orchestrated containers](#) for each container.

7.1.2 Resource Requirements

Node Type	CPU	Memory	Disk
Control plane node	2vCPU	4 GB	1 GB

Worker node	2vCPU	2 GB	500 MB
-------------	-------	------	--------

7.1.3 Network Requirements

Connectivity between control plane node and worker nodes is a must. They should either be:

- Part of the same private network (**recommended & secure**)
- Control plane has a public IP (not recommended)

Component	Port	Endpoint	Purpose
Knox-Gateway	3000	knox-gw.<env>.accuknox.com:3000	For Knox-Gateway service
PPS	443	pps.<env>.accuknox.com	For PPS (Policy Provisioning Service)
Spire-Server	8081, 9090	spire.<env>.accuknox.com	For Spire-Server communication
KubeArmor Relay Server	32768	-	For Kubearmor relay server on control plane
Shared Informer Agent	32769	-	For Shared Informer agent on control plane

Policy Enforcement Agent (PEA)	32770	-	For Policy Enforcement Agent on control plane
Hardening Module	32771	-	For Discovery Engine Hardening Module on control plane
VM Worker Nodes	32768-32771	-	For VM worker nodes to connect to the control plane

Check the CWPP documentation for more details on the [network requirements](#).

You can check the connectivity between nodes using curl. Upon a successful connection, the message returned by curl will be:

```
$ curl <control-plane-addr>:32770
curl: (1) Received HTTP/0.9 when not allowed
```

7.1.4 Onboarding

Navigate to the onboarding page (Settings → Manage Cluster → Onboard Now) and choose the "VM" option on the instructions page. Then, provide a name for your cluster. You will be presented with instructions to download accuknox-cli and onboard your cluster.

The following agents will be installed:

1. **Feeder-service** which collects KubeArmor feeds.

2. **Shared-informer-agent** authenticates with your VMs and collects information regarding entities like hosts, containers, and namespaces.
3. **Policy-enforcement-agent** authenticates with your VMs and enforces labels and policies.

Install knoxctl/accuknox-cli

```
curl -sfL https://knoxctl.accuknox.com/install.sh | sudo sh -s --  
-b /usr/bin
```

7.1.5 Onboarding Control Plane

The command may look something like this:

```
$ knoxctl onboard vm cp-node \  
--version "v0.2.10" \  
--join-token="843ef458-cecc-4fb9-b5c7-9f1bf7c34567" \  
--spire-host="spire.dev.accuknox.com" \  
--pps-host="pps.dev.accuknox.com" \  
--knox-gateway="knox-gw.dev.accuknox.com:3000"
```

By default, if Docker is not found, systemd mode of installation would be used. If you want to explicitly onboard using systemd services, add the `--vm-mode=systemd` flag to the above command.

The above command will emit the command to onboard worker nodes. You may also use the `--cp-node-addr` flag to specify the address that other nodes will use to connect with your cluster.

By default, the network created by onboarding commands reserves the subnet 172.20.32.0/27 for the accuknox-net Docker network. If you want to change it for your environment, you can use the `--network-cidr` flag.

7.1.6 Onboarding Worker Nodes

The second command will be for onboarding worker nodes. It may look something like this:

```
knoxctl onboard vm node --cp-node-addr=<control-plane-addr>
```

Example:

```
$ knoxctl onboard vm node --cp-node-addr=192.168.56.106
Pulling kubearmor-init      ... done
Pulling kubearmor           ... done
Pulling kubearmor-vm-adapter ... done
Creating network "accuknox-config_accuknox-net" with the default
driver
Creating kubearmor-init ... done
Creating kubearmor           ... done
Creating kubearmor-vm-adapter ... done
onboard-vm-node.go:41: VM successfully joined with control-plane!
```

If you encounter any issues while onboarding, use the commands below to debug:

```
docker logs spire-agent -f

docker logs shared-informer-agent -f

docker logs kubearmor-init -f

docker logs kubearmor -f
```

7.1.7 Deboarding

Deboard the cluster from SaaS first.

To deboard the worker-vm/Node:

```
knoxctl deboard vm node
```

To deboard the Control-Plane VM:

```
knoxctl deboard vm cp-node
```

Sample Output:

```
$ knoxctl deboard vm cp-node
[+] Running 10/10
✓ Container shared-informer-agent      Removed
✓ Container feeder-service             Removed
✓ Container policy-enforcement-agent  Removed
✓ Container wait-for-it               Removed
✓ Container kubearmor-vm-adapter     Removed
✓ Container kubearmor-relay-server   Removed
✓ Container spire-agent              Removed
✓ Container kubearmor                Removed
✓ Container kubearmor-init           Removed
✓ Network accuknox-config_accuknox-net Removed
```

Please remove any remaining resources at

```
/home/user/.accuknox-config
```

Control plane node deboarded successfully.

After that cleanup the `~/.accuknox-config` directory

```
sudo rm -rf ~/.accuknox-config
```

7.2 Docker

Docker v19.0.3 and Docker Compose v1.27.0+ are required. Follow the latest [Install Docker Engine](#) for downloading. Ensure you also add your user to the docker user group: [Linux post-installation steps for Docker Engine](#).

Linux Kernel v5.8+ with BPF LSM support is needed. See how to [enable BPF LSM](#).

If Linux v5.8+ or BPF LSM is not supported in the given environment, host enforcement will still work out of the box. For protecting containers, new containers will have to be created with special options. See [Support for non orchestrated containers](#) for the same.

7.2.1 Resource Requirements

Node Type	CPU	Memory	Disk
Control plane node	2vCPU	4 GB	24 GB
Worker node	2vCPU	2 GB	12 GB

7.2.2 Network Requirements

Connectivity between control plane node and worker nodes is a must. They should either be:

- Part of the same private network (**recommended & secure**)
- Control plane has a public IP (not recommended)

Ports required on the control plane VM:

Component	Type	Ports	Endpoint	Purpose
Knox-Gateway	Outbound to SaaS	3000	knox-gw.<env>.accuknox.com:3000	For Knox-Gateway service
PPS	Outbound to SaaS	443	pps.<env>.accuknox.com	For PPS (Policy Provisioning Service)
Spire-Server	Outbound to SaaS	8081, 9090	spire.<env>.accuknox.com	For Spire-Server communication
KubeArmor Relay Server	Inbound in CP	32768	-	For KubeArmor relay server on control plane
Shared Informer Agent	Inbound in CP	32769	-	For Shared Informer agent on control plane

Policy Enforcement Agent (PEA)	Inbound in CP	32770	-	For Policy Enforcement Agent on control plane
Hardening Module	Inbound in CP	32771	-	For Discovery Engine Hardening Module on control plane
VM Worker Nodes	Outbound from worker node to CP	32768-32771	-	For VM worker nodes to connect to the control plane

By default, the network created by onboarding commands reserves the subnet 172.20.32.0/27. If you want to change it for your environment, you can use the --network-cidr flag.

You can check the connectivity between nodes using curl. Upon a successful connection, the message returned by curl will be:

```
$ curl <control-plane-addr>:32770
curl: (1) Received HTTP/0.9 when not allowed
```

7.3 Onboarding

Navigate to the onboarding page (Settings → Manage Cluster → Onboard Now) and choose the "VM" option on the instructions page. Then, provide a name for your cluster. You will be presented with instructions to download accuknox-cli and onboard your cluster.

The following agents are installed:

1. **Feeder-service** which collects KubeArmor feeds.
2. **Shared-informer-agent** authenticates with your VMs and collects information regarding entities like hosts, containers, and namespaces.
3. **Policy-enforcement-agent** authenticates with your VMs and enforces labels and policies.

7.3.1 Install knoxctl/accuknox-cli

```
curl -sfL https://knoxctl.accuknox.com/install.sh | sudo sh -s  
-- -b /usr/bin
```

7.3.2 Onboarding Control Plane

The command may look something like this:

```
$ knoxctl onboard vm cp-node \  
--version "v0.2.10" \  
--join-token="843ef458-cecc-4fb9-b5c7-9f1bf7c34567" \  
--spire-host="spire.dev.accuknox.com" \  
--pps-host="pps.dev.accuknox.com" \  
--knox-gateway="knox-gw.dev.accuknox.com:3000"
```

The above command will emit the command to onboard worker nodes. You may also use the --cp-node-addr flag to specify the address that other nodes will use to connect with your cluster.

By default, the network created by onboarding commands reserves the subnet 172.20.32.0/27 for the accuknox-net Docker network. If you want to change it for your environment, you can use the --network-cidr flag.

7.3.3 Onboarding Worker Nodes

The second command will be for onboarding worker nodes. It may look something like this:

```
knoxctl onboard vm node --cp-node-addr=<control-plane-addr>
```

Example:

```
$ knoxctl onboard vm node --cp-node-addr=192.168.56.106
Pulling kubearmor-init      ... done
Pulling kubearmor           ... done
Pulling kubearmor-vm-adapter ... done
Creating network "accuknox-config_accuknox-net" with the default
driver
Creating kubearmor-init ... done
Creating kubearmor          ... done
Creating kubearmor-vm-adapter ... done
onboard-vm-node.go:41: VM successfully joined with control-plane!
```

If you encounter any issues while onboarding, use the commands below to debug:

```
docker logs spire-agent -f
docker logs shared-informer-agent -f
docker logs kubearmor-init -f
docker logs kubearmor -f
```

7.4 Deboarding

Deboard the cluster from SaaS first.

To deboard the worker-vm/Node:

```
knoxctl deboard vm node
```

To deboard the Control-Plane VM:

```
knoxctl deboard vm cp-node
```

Sample Output:

```
$ knoxctl deboard vm cp-node
[+] Running 10/10
✓ Container shared-informer-agent      Removed
✓ Container feeder-service             Removed
✓ Container policy-enforcement-agent  Removed
✓ Container wait-for-it               Removed
✓ Container kubearmor-vm-adapter     Removed
✓ Container kubearmor-relay-server   Removed
✓ Container spire-agent              Removed
✓ Container kubearmor                Removed
✓ Container kubearmor-init           Removed
✓ Network accuknox-config_accuknox-net Removed
Please remove any remaining resources at
/home/user/.accuknox-config
Control plane node deboarded successfully.
```

After that cleanup the `~/.accuknox-config` directory

```
sudo rm -rf ~/.accuknox-config
```

8. Registry Onboarding

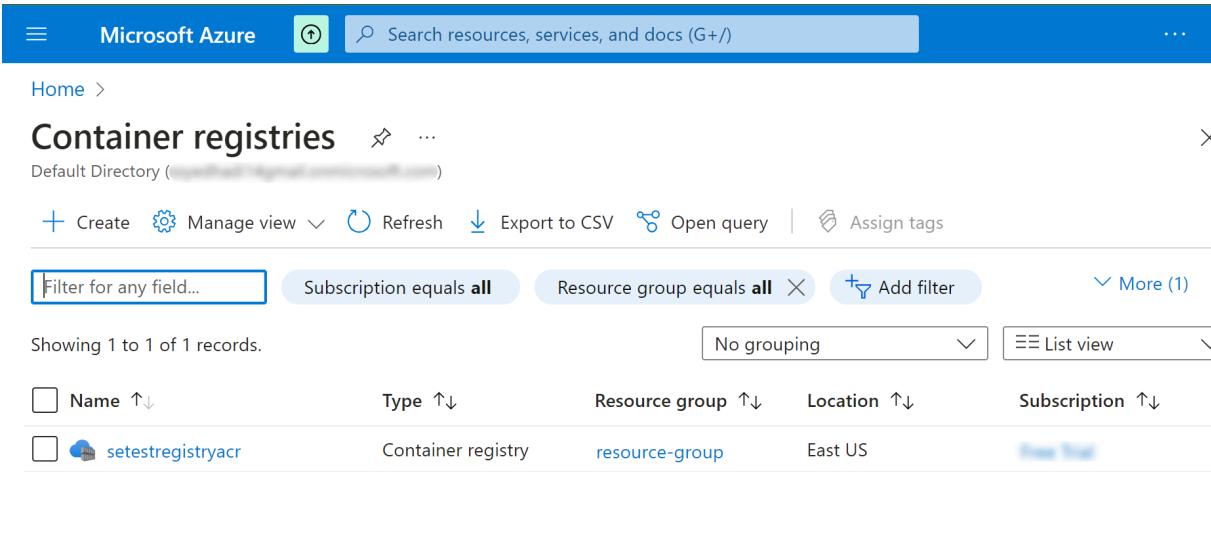
8.1 Azure Container Registry

ACR Onboarding

AccuKnox CSPM security tool scans images that are present in the onboarded Azure Container Registry and has the capability to find the risks and vulnerabilities associated with these images. The risks are identified and shown in the scan results. Users will be getting a comprehensive view of these risks and vulnerabilities in the dashboard along with their remediation.

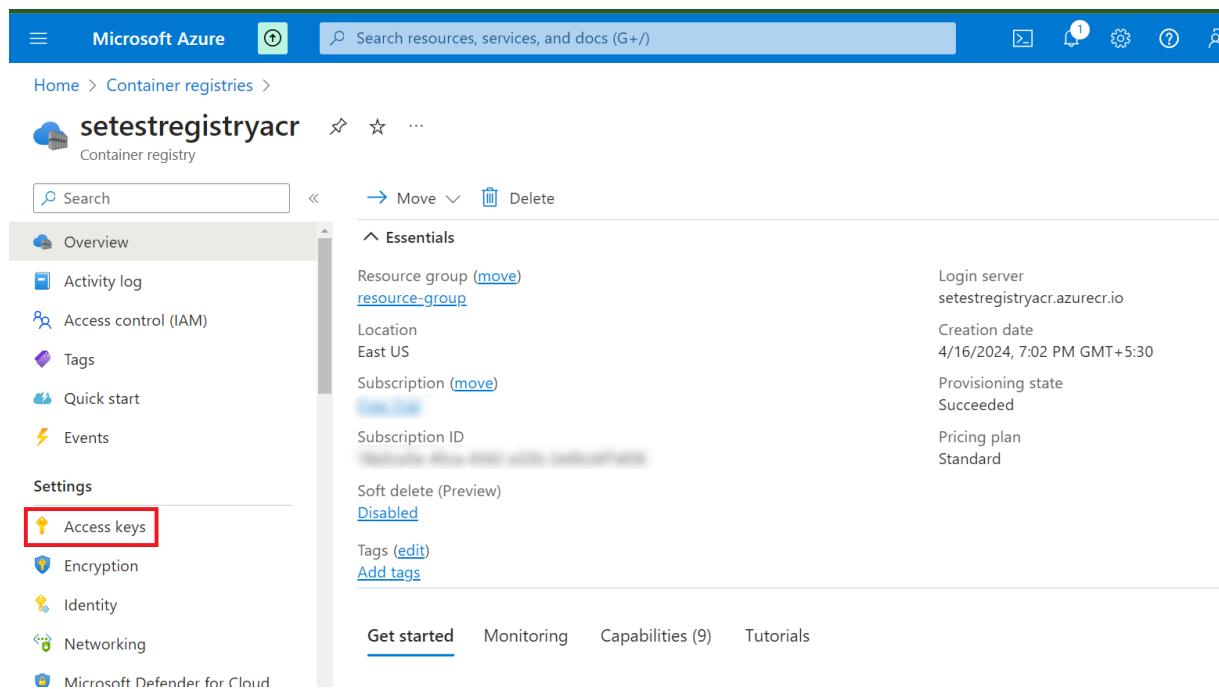
8.1.1 Steps to generate credentials for onboarding ACR

Step 1: Open the Azure Management Console and sign in with your Azure account credentials. Search for the **Container Registry** service in the search bar.



The screenshot shows the Azure portal interface for managing Container registries. At the top, there's a blue header bar with the Microsoft Azure logo, a search bar, and a '...' button. Below it, the main navigation bar includes 'Home >', the current page title 'Container registries', and a '...' button. Underneath, there's a sub-header 'Default Directory ([redacted])'. The main content area has a toolbar with 'Create', 'Manage view', 'Refresh', 'Export to CSV', 'Open query', and 'Assign tags' buttons. Below the toolbar are filter options: 'Filter for any field...', 'Subscription equals all', 'Resource group equals all', 'Add filter', and 'More (1)'. The main table displays one record: 'Showing 1 to 1 of 1 records.' The table has columns for 'Name' (setestregistryacr), 'Type' (Container registry), 'Resource group' (resource-group), 'Location' (East US), and 'Subscription'. There are also sorting arrows for each column. At the bottom, there are navigation icons for back, forward, and search.

Step 2: Click on the name of the registry to be onboarded. In the navigation menu for the container registry, click on **Access Keys** under the Settings section.



setestregistryacr Container registry

Search → Move Delete

Essentials

- Resource group ([move](#)) [resource-group](#)
- Location: East US
- Subscription ([move](#)) [Subscription](#)
- Subscription ID: [REDACTED]
- Creation date: 4/16/2024, 7:02 PM GMT+5:30
- Provisioning state: Succeeded
- Pricing plan: Standard

Soft delete (Preview): [Disabled](#)

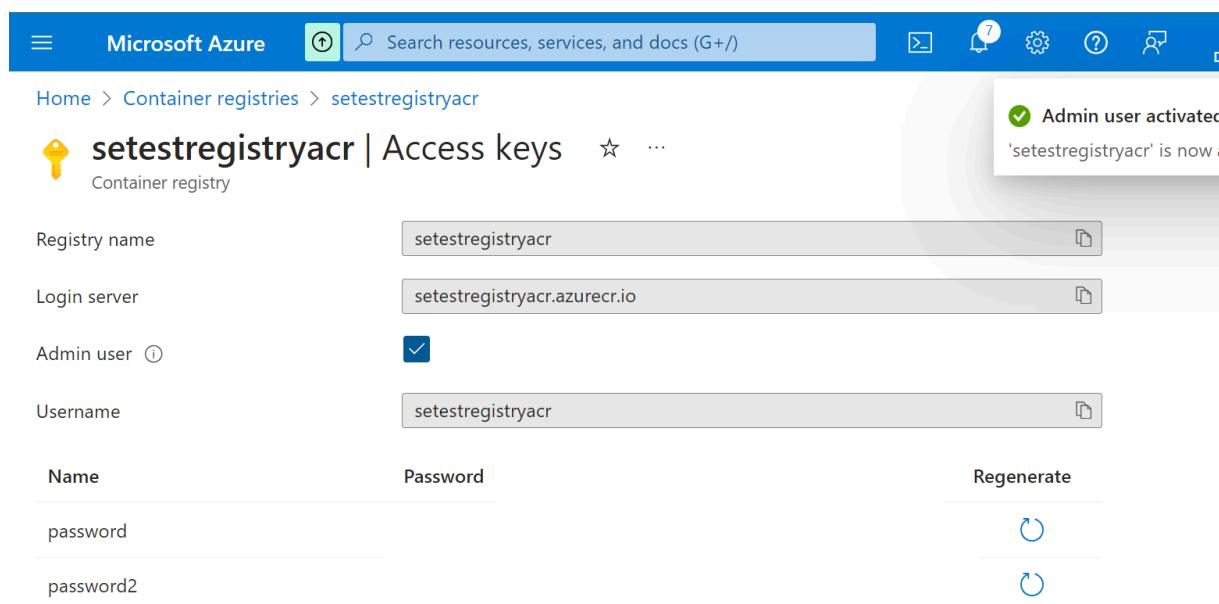
Tags ([edit](#)) [Add tags](#)

Get started Monitoring Capabilities (9) Tutorials

Access keys

Encryption Identity Networking Microsoft Defender for Cloud

Step 3: Click on the **Admin User** checkbox to activate Admin access.



setestregistryacr | Access keys

Registry name: setestregistryacr

Login server: setestregistryacr.azurecr.io

Admin user:

Username: setestregistryacr

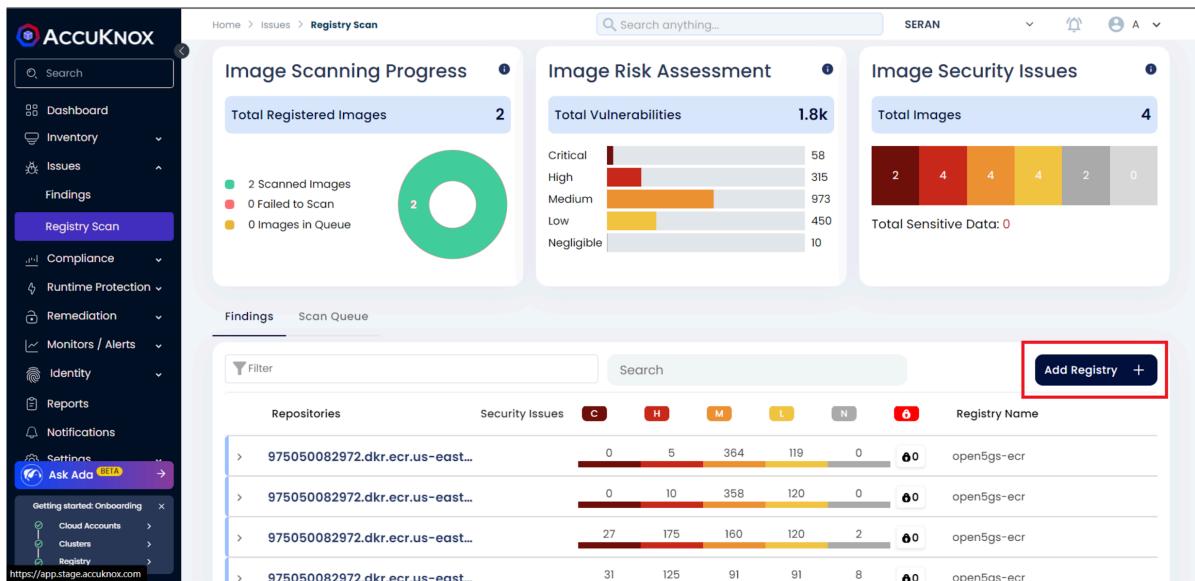
Name	Password	Regenerate
password		
password2		

✓ Admin user activated
'setestregistryacr' is now a fully functional Azure Container Registry.

Copy the generated **Login Server**, **Username** and **Password** for onboarding on AccuKnox SaaS.

8.1.2 Steps to onboard the registry on AccuKnox SaaS

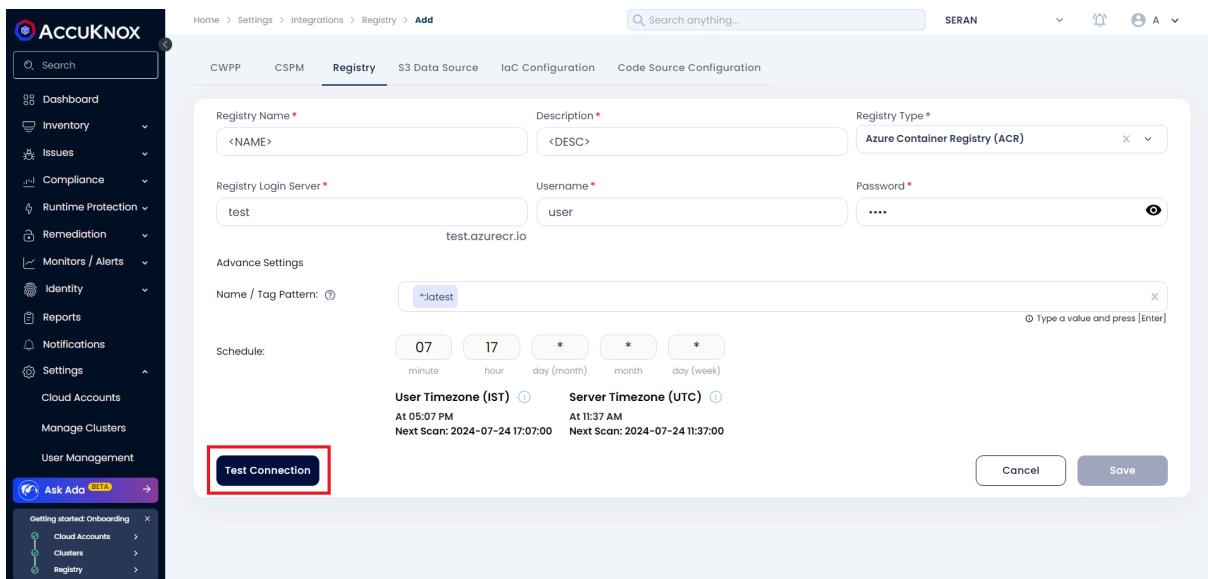
Step 1: Login to the AccuKnox SaaS and Navigate to Issues → Registry Scan. Click on **Add Registry**



The screenshot shows the AccuKnox SaaS interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan (which is selected and highlighted in purple), Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Under Settings, there's an 'Ask Ada' section with a 'Getting started Onboarding' link. The main content area is titled 'Registry Scan' and contains three main sections: 'Image Scanning Progress' (Total Registered Images: 2, 2 Scanned Images, 0 Failed to Scan, 0 Images in Queue), 'Image Risk Assessment' (Total Vulnerabilities: 1.8k, Critical: 58, High: 315, Medium: 973, Low: 450, Negligible: 10), and 'Image Security Issues' (Total Images: 4, 2 Red, 4 Orange, 4 Yellow, 2 Grey, 0 Grey). Below these sections is a table titled 'Findings' showing repositories and their security issues. The last row of the table is highlighted with a red box around the 'Add Registry' button.

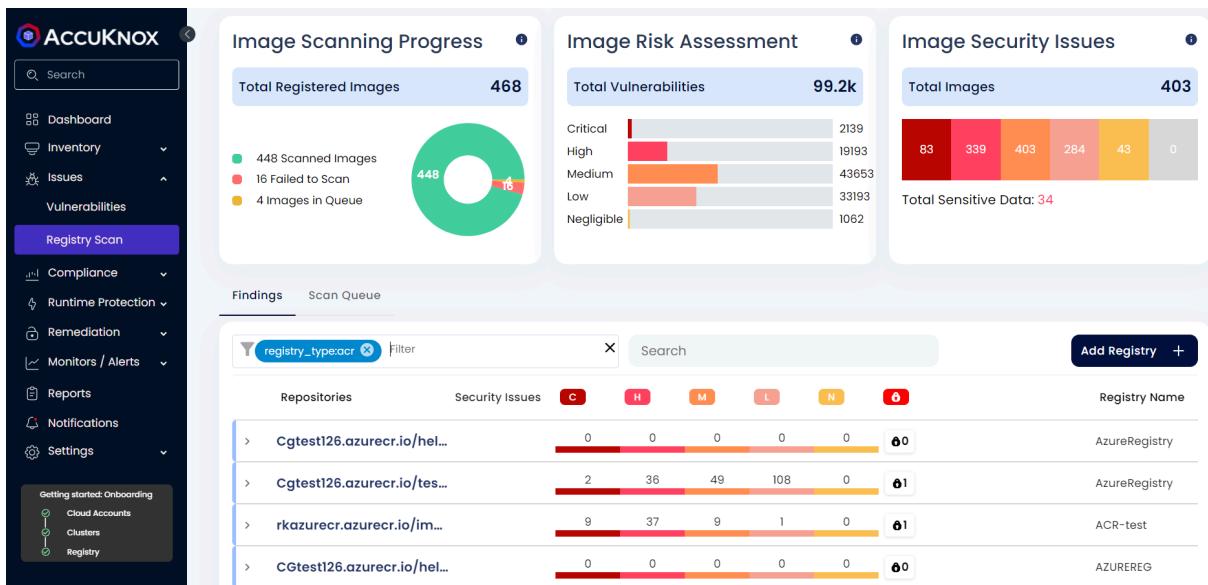
Step 2: Enter any Registry Name and Description. Select Registry Type as ACR and paste the Login Server, Username and Password that was copied.

Click on **Test Connection** and then click on the enabled **Save** button



The screenshot shows the 'Integrations' page with the 'Registry' tab selected. The form fields include 'Registry Name' (placeholder: <NAME>), 'Description' (placeholder: <DESC>), 'Registry Type' (selected: Azure Container Registry (ACR)), 'Registry Login Server' (value: test), 'Username' (value: user), and 'Password' (value: test.azurecr.io). Below these are 'Advance Settings' (Name / Tag Pattern: *latest) and 'Schedule' (07 minute, 17 hour, * day (month), * month, * day (week)). At the bottom are 'User Timezone (IST)' (At 05:07 PM, Next Scan: 2024-07-24 17:07:00) and 'Server Timezone (UTC)' (At 11:37 AM, Next Scan: 2024-07-24 11:37:00). The 'Test Connection' button is highlighted with a red box. At the bottom right are 'Cancel' and 'Save' buttons.

Step 3: A popup appears that the registry is added on successful onboarding.
 Navigate to Issues → Registry Scan to view the scan results. The status of the scan can be checked from the **Scan Queue** tab



8.2 Harbor Registry

Harbor is an open source registry that secures artifacts with policies and role-based access control, ensures images are scanned and free from vulnerabilities, and signs images as trusted.

8.2.1 Prerequisites for Harbor Registry Onboarding in Accuknox:

In Harbor, users and groups are created by the admin.

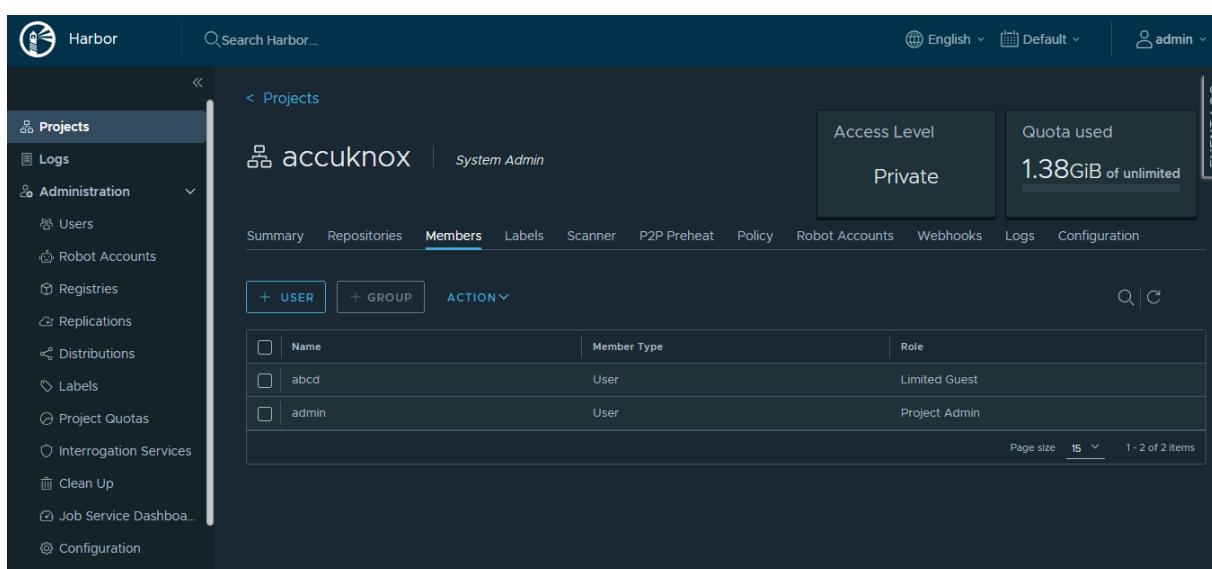
If you have the admin access, then login through those credentials.

To create a new user in Harbor, you can follow the steps mentioned here:

<https://goharbor.io/docs/administration/managing-users/create-users-db/>

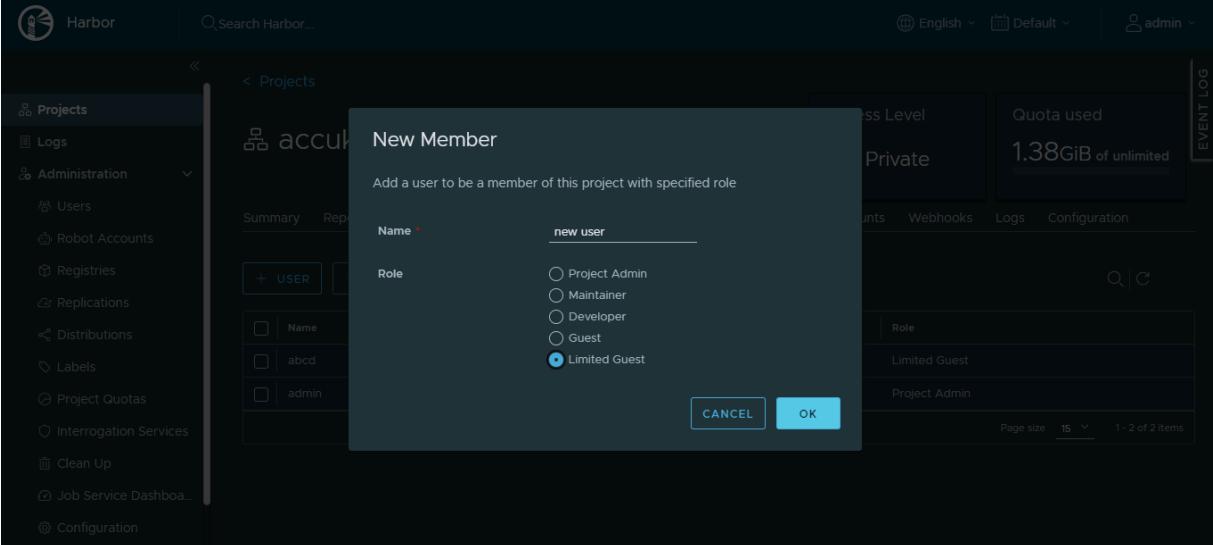
After creating the user, we need to add this user as a member in the Project.

Click on “Projects”, select the Project in which you have to add the user.



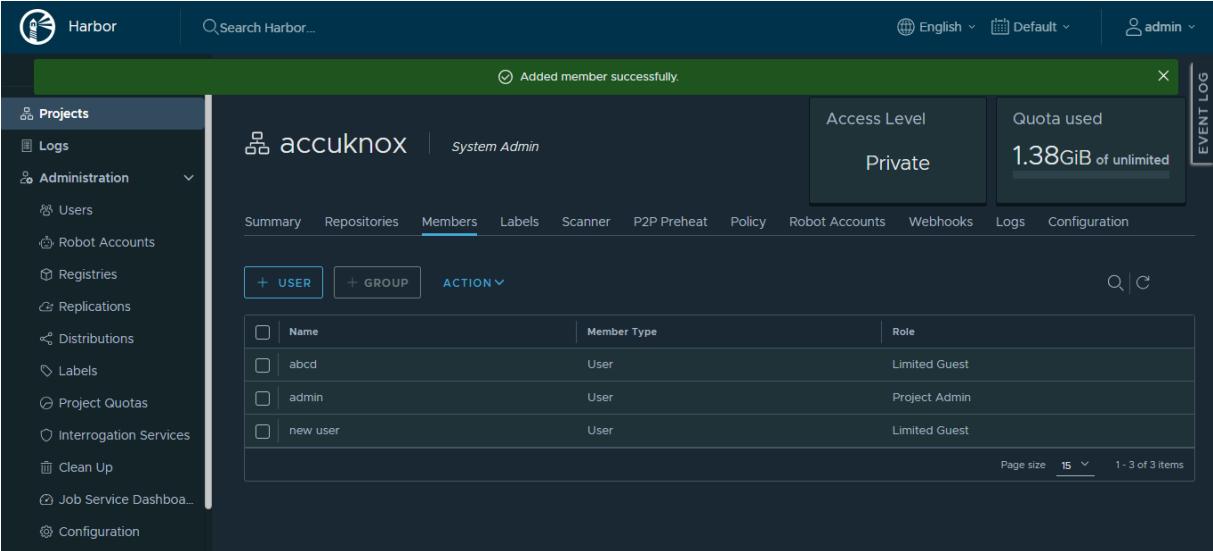
Name	Member Type	Role
abcd	User	Limited Guest
admin	User	Project Admin

Click on the “Members” tab -> +User -> give the user name and select “Limited Guest” role -> ok



The screenshot shows the Harbor UI interface. On the left, there's a sidebar with 'Projects', 'Logs', 'Administration' (expanded), 'Users', 'Robot Accounts', etc. The main area shows a project named 'accuknox'. A modal window titled 'New Member' is open, prompting to add a user to the project. The 'Name' field contains 'new user'. Under 'Role', the 'Limited Guest' option is selected. Other roles like 'Project Admin', 'Maintainer', 'Developer', and 'Guest' are also listed. At the bottom of the modal are 'CANCEL' and 'OK' buttons.

We have now added the member (user) in the Project.



The screenshot shows the Harbor UI after the user 'new user' has been added. A green success message at the top says 'Added member successfully.' The 'Members' tab is selected in the navigation bar. The table below lists the members:

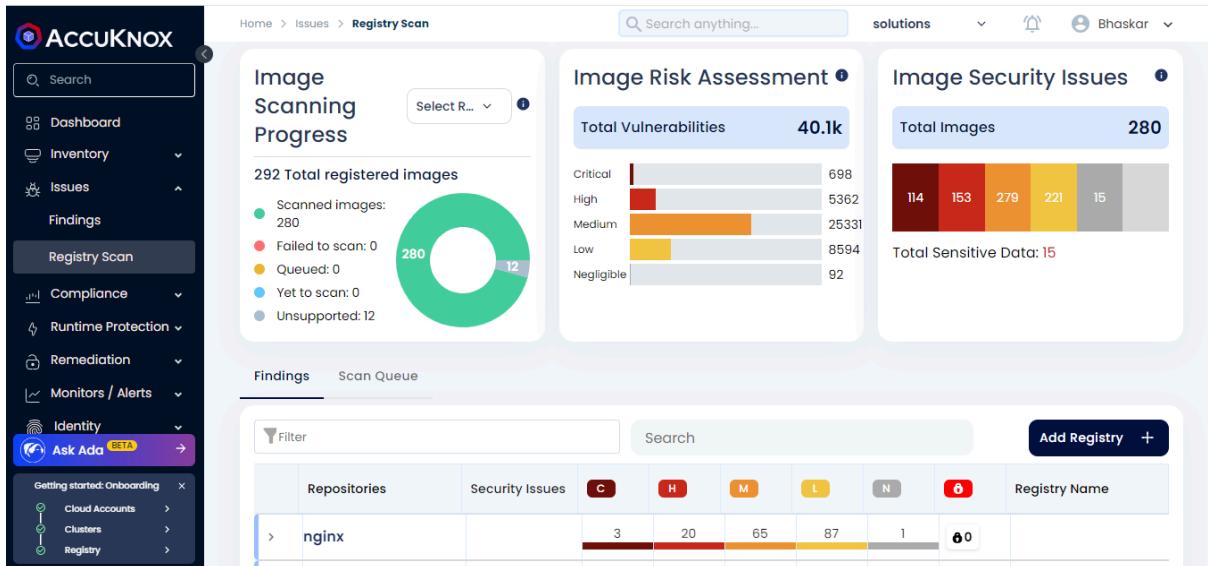
Name	Member Type	Role
abcd	User	Limited Guest
admin	User	Project Admin
new user	User	Limited Guest

Now we can onboard this user in the Accuknox dashboard.

8.2.2 Steps to Onboard Harbor Registry on Accuknox:

In Accuknox dashboard, under Issues, click on “Registry Scan”

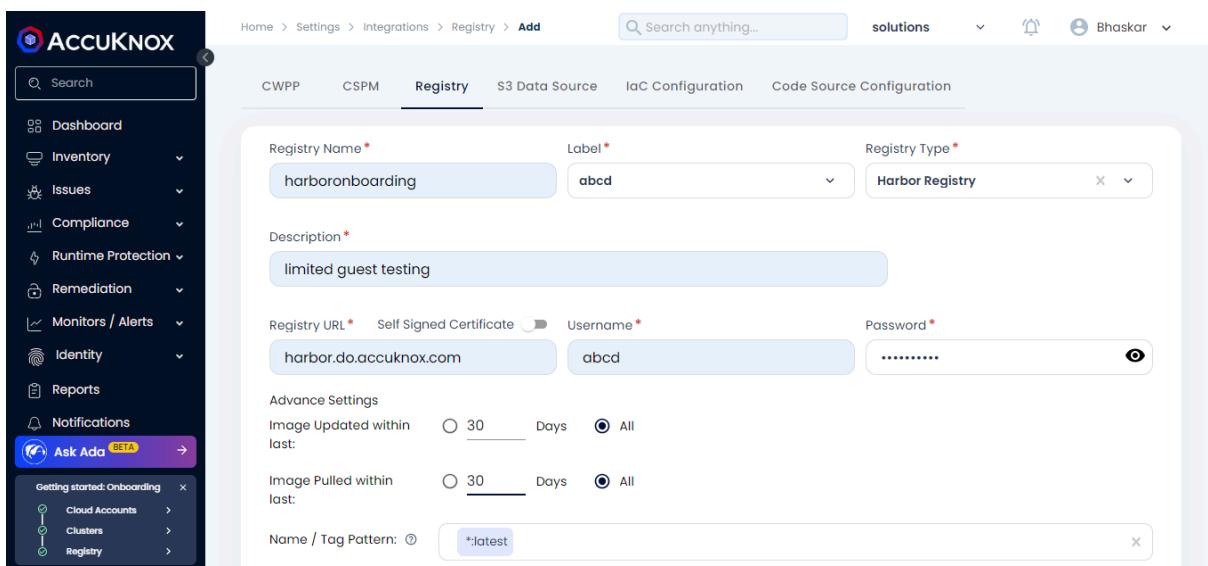
Now, click on “Add Registry”



The screenshot shows the Accuknox dashboard with the 'Issues' menu selected. Under 'Issues', 'Registry Scan' is highlighted. The main area displays the 'Image Risk Assessment' and 'Image Security Issues' sections. The 'Image Risk Assessment' section shows a total of 40.1k vulnerabilities across Critical, High, Medium, Low, and Negligible levels. The 'Image Security Issues' section shows 280 total images with counts for each severity level: Critical (114), High (153), Medium (279), Low (221), and Negligible (15). A large green donut chart indicates 280 registered images with 12 pending scans.

Give the registry name, select Label and select “Harbor Registry” from the Registry type dropdown.

Then, paste the Registry URL and provide the user credentials.



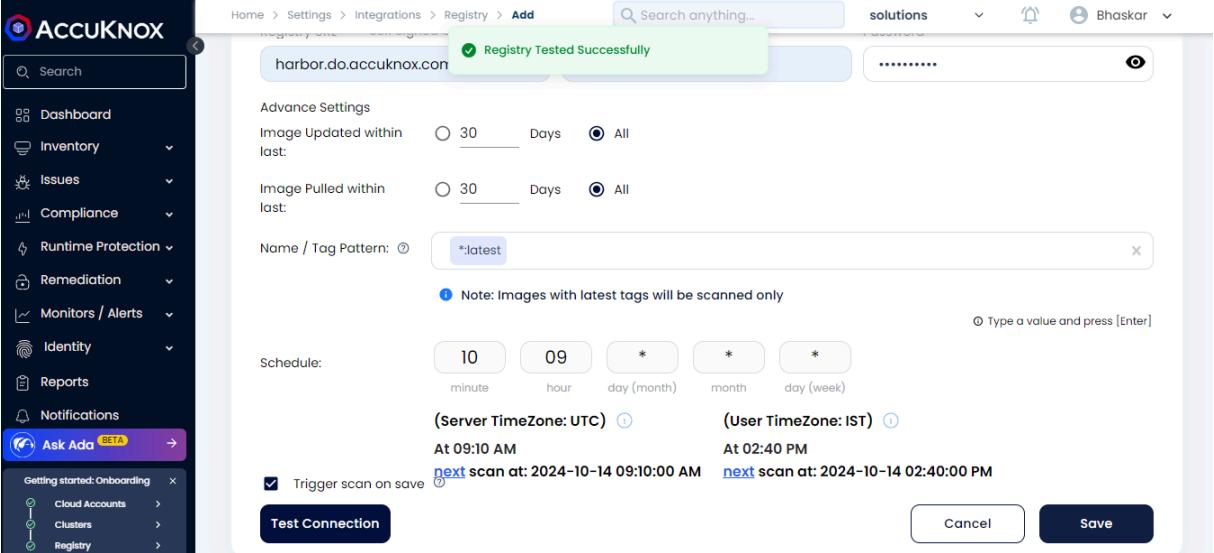
The screenshot shows the 'Integrations' page with the 'Registry' tab selected. It includes tabs for CWPP, CSPM, Registry, S3 Data Source, IaC Configuration, and Code Source Configuration. The 'Registry' tab contains fields for 'Registry Name' (harboronboarding), 'Label' (abcd), 'Registry Type' (Harbor Registry), 'Description' (limited guest testing), 'Registry URL' (harbor.do.accuknox.com), 'Username' (abcd), and 'Password'. Advanced settings allow configuration for image update and pull intervals, and a 'Name / Tag Pattern' field is set to ':latest'.

Provide the Tag pattern, and schedule time for the scanning.

If you need to trigger the scan after saving then click on the “Trigger scan on save” checkbox.

After providing all the information, click on “Test Connection”, it should show “Registry Tested Successfully”.

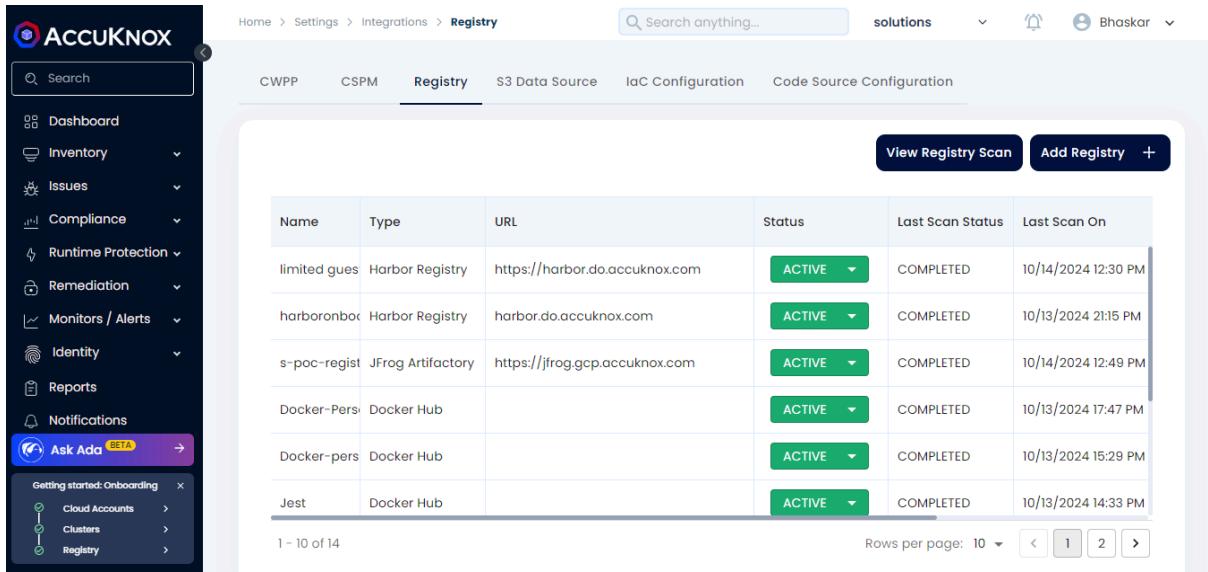
Now, click on Save.



After saving the registry, the scan will start based on the scheduled time.

To see that the scanning is completed or not, go to Settings -> Integrations -> Registry

Here, we can see the list of onboarded registries and their details.



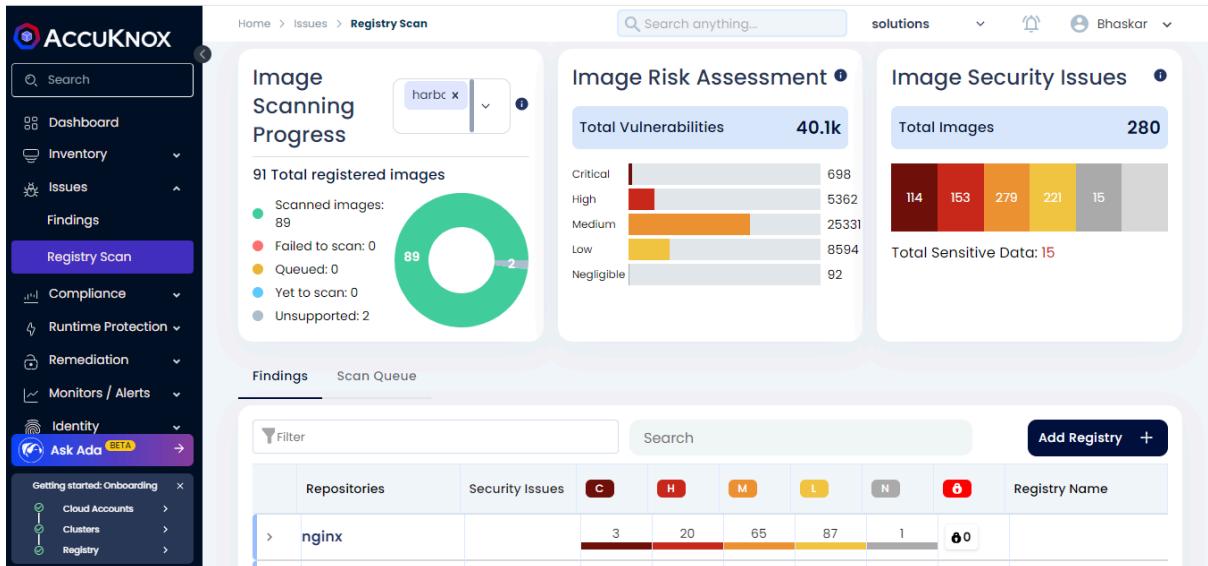
The screenshot shows the AccuKnox interface with the 'Registry' tab selected. A table lists six registries:

Name	Type	URL	Status	Last Scan Status	Last Scan On
limited gues	Harbor Registry	https://harbor.do.accuknox.com	ACTIVE	COMPLETED	10/14/2024 12:30 PM
harboronbo	Harbor Registry	harbor.do.accuknox.com	ACTIVE	COMPLETED	10/13/2024 21:15 PM
s-poc-regist	JFrog Artifactory	https://jfrog.gcp.accuknox.com	ACTIVE	COMPLETED	10/14/2024 12:49 PM
Docker-Perso	Docker Hub		ACTIVE	COMPLETED	10/13/2024 17:47 PM
Docker-perso	Docker Hub		ACTIVE	COMPLETED	10/13/2024 15:29 PM
Jest	Docker Hub		ACTIVE	COMPLETED	10/13/2024 14:33 PM

Rows per page: 10 | < | 1 | 2 | >

Once the scanning is completed, we can see the scan results in the Issues -> Registry Scan

-> Under “Image Scanning Progress” pie chart, select your registry to view the progress.



The screenshot shows the 'Issues > Registry Scan' page. It includes three main sections: 'Image Scanning Progress', 'Image Risk Assessment', and 'Image Security Issues'.

Image Scanning Progress:

- Total registered images: 91
- Scanned images: 89
- Failed to scan: 0
- Queued: 0
- Yet to scan: 0
- Unsupported: 2

Image Risk Assessment:

- Total Vulnerabilities: 40.1k
- Critical: 698
- High: 5362
- Medium: 25331
- Low: 8594
- Negligible: 92

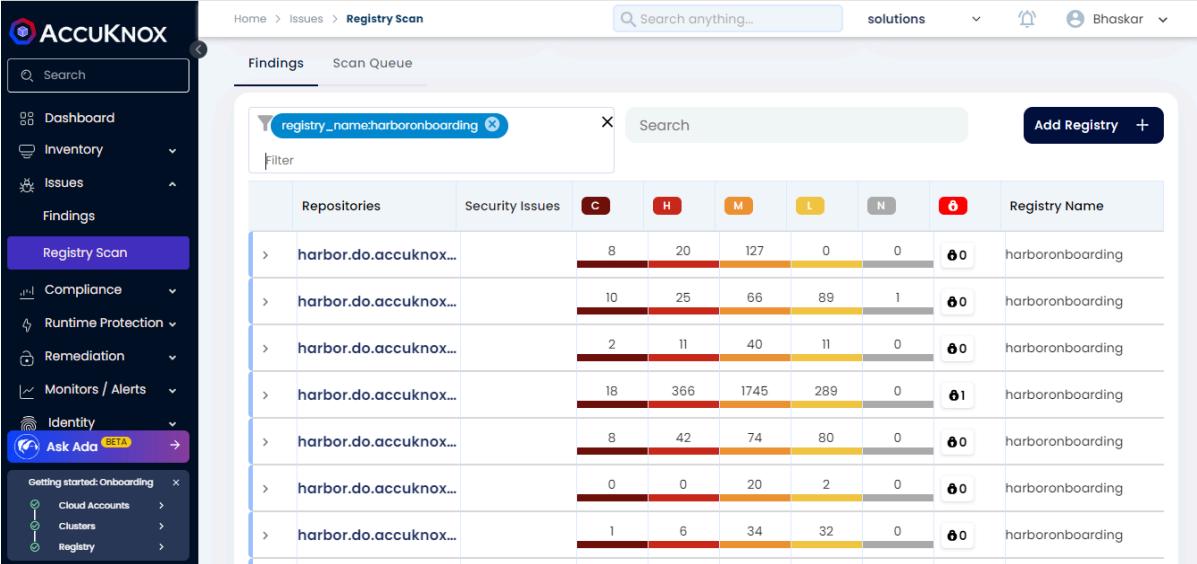
Image Security Issues:

- Total Images: 280
- Findings: 114
- Scan Queue: 153
- Sensitive Data: 279
- Issues: 221
- Unresolved: 15

Repositories:

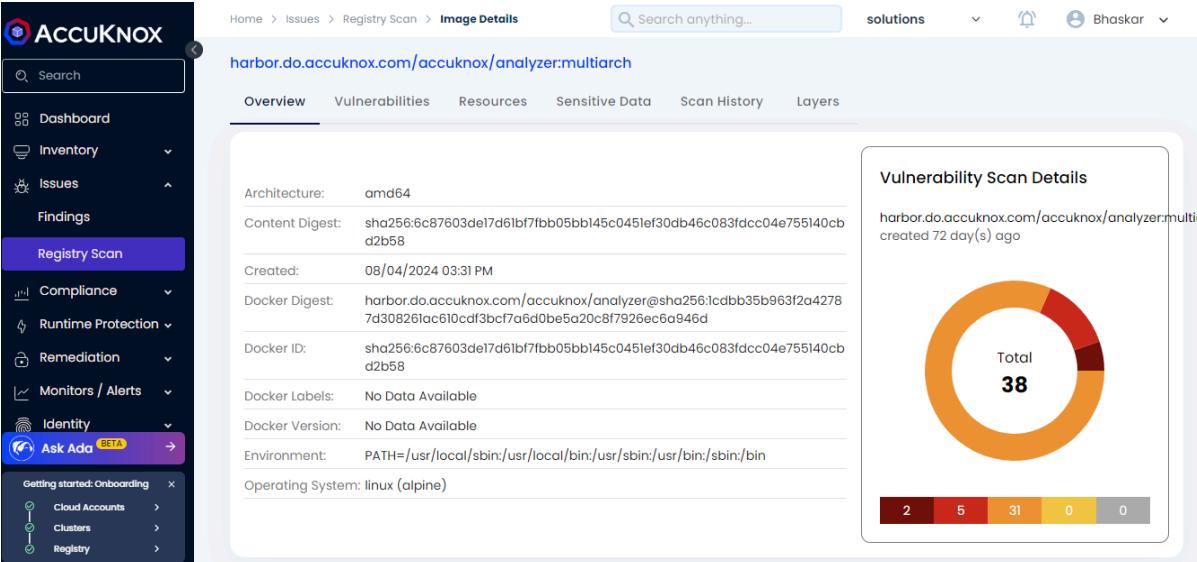
Repositories	Security Issues	C	H	M	L	N	O	Registry Name
nginx	3 20 65 87 1	60						

To view the details of your registry, you can use the filter such as “registry_type”, then select the “harbor” registry or you can also use the filter “registry_name” and provide the name of your registry.



Repositories	Security Issues	C	H	M	L	N	O	Registry Name
harbor.do.accuknox...		8	20	127	0	0	60	harboronboarding
harbor.do.accuknox...		10	25	66	89	1	60	harboronboarding
harbor.do.accuknox...		2	11	40	11	0	60	harboronboarding
harbor.do.accuknox...		18	366	1745	289	0	61	harboronboarding
harbor.do.accuknox...		8	42	74	80	0	60	harboronboarding
harbor.do.accuknox...		0	0	20	2	0	60	harboronboarding
harbor.do.accuknox...		1	6	34	32	0	60	harboronboarding

By clicking on the repositories, we can get more details about the scan results.



Architecture: amd64

Content Digest: sha256:6c87603de17d61bf7fbb05bb145c0451ef30db46c083fdcc04e755140cb
d2b58

Created: 08/04/2024 03:31 PM

Docker Digest: harbor.do.accuknox.com/accuknox/analyzer@sha256:1cd8b35b963f2a4278
7d308261ac610cdf3bcf7a6d0be5a20c8f7926ec6a946d

Docker ID: sha256:6c87603de17d61bf7fbb05bb145c0451ef30db46c083fdcc04e755140cb
d2b58

Docker Labels: No Data Available

Docker Version: No Data Available

Environment: PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

Operating System: linux (alpine)

Vulnerability Scan Details
harbor.do.accuknox.com/accuknox/analyzer:multiarch created 72 day(s) ago

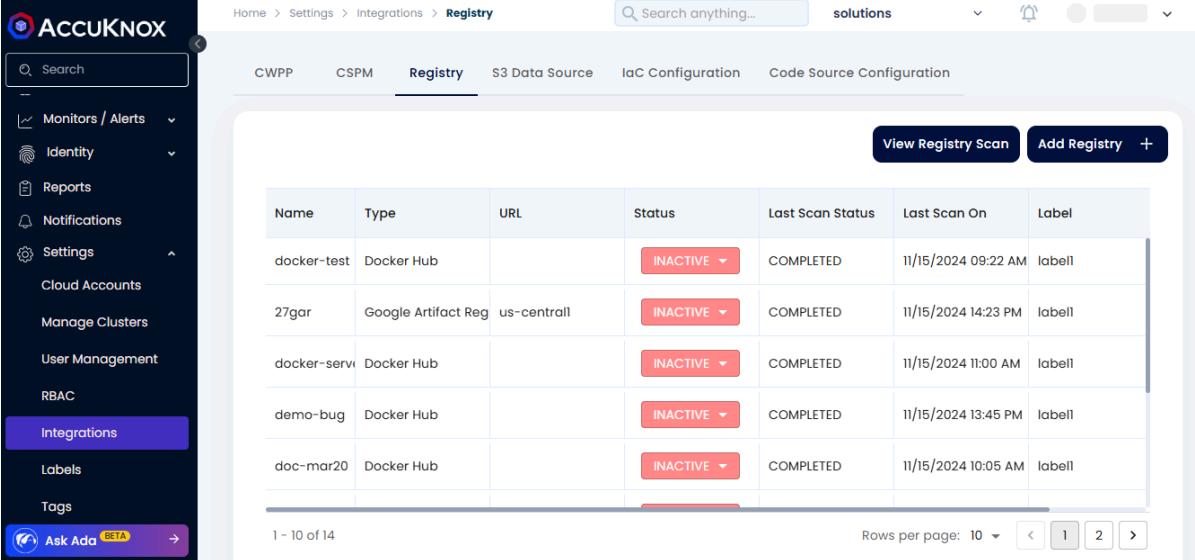
Total 38

2	5	31	0	0
---	---	----	---	---

8.3 Deboarding a Registry

This guide outlines the steps for offboarding a registry from AccuKnox SaaS.

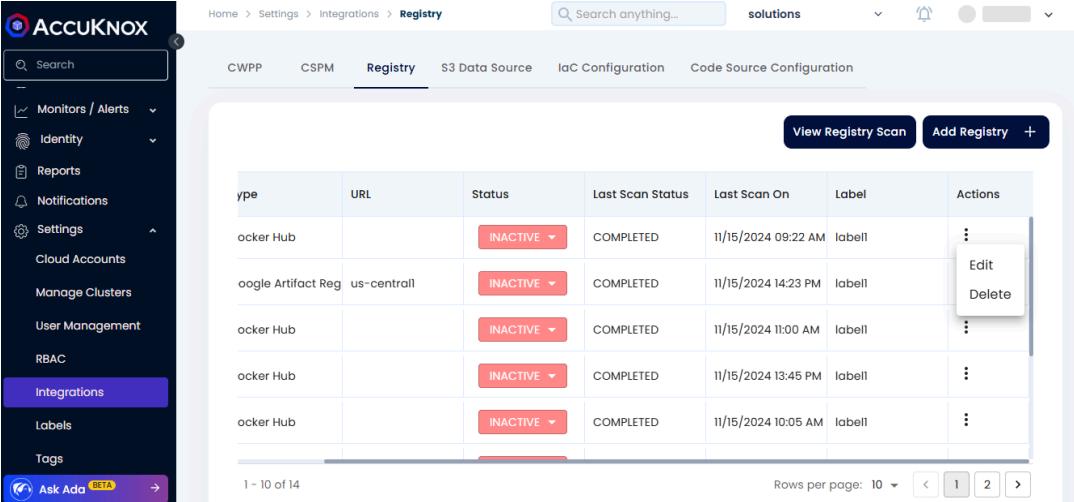
Step 1: Login to AccuKnox SaaS and Go to Settings -> Integrations -> Registry.



The screenshot shows the AccuKnox SaaS interface with the 'Registry' tab selected. The left sidebar has 'Integrations' highlighted. The main table lists five registries:

Name	Type	URL	Status	Last Scan Status	Last Scan On	Label
docker-test	Docker Hub		INACTIVE	COMPLETED	11/15/2024 09:22 AM	label1
27gar	Google Artifact Reg	us-central1	INACTIVE	COMPLETED	11/15/2024 14:23 PM	label2
docker-servi	Docker Hub		INACTIVE	COMPLETED	11/15/2024 11:00 AM	label3
demo-bug	Docker Hub		INACTIVE	COMPLETED	11/15/2024 13:45 PM	label4
doc-mar20	Docker Hub		INACTIVE	COMPLETED	11/15/2024 10:05 AM	label5

Step 2: Scroll to the left and click on the 3 dots of the registry you want to delete and click “Delete”.



The screenshot shows the same Registry page as above, but with a context menu open over the first registry entry. The menu includes 'Edit' and 'Delete' options.

This will delete the Registry from AccuKnox SaaS.

9. AccuKnox CNAPP Dashboard Widgets

9.1 CWPP Widgets

In CWPP, Accuknox has 32 widgets to visualize the findings. Some of them are shown below.

1. Top 5 cluster findings Widget



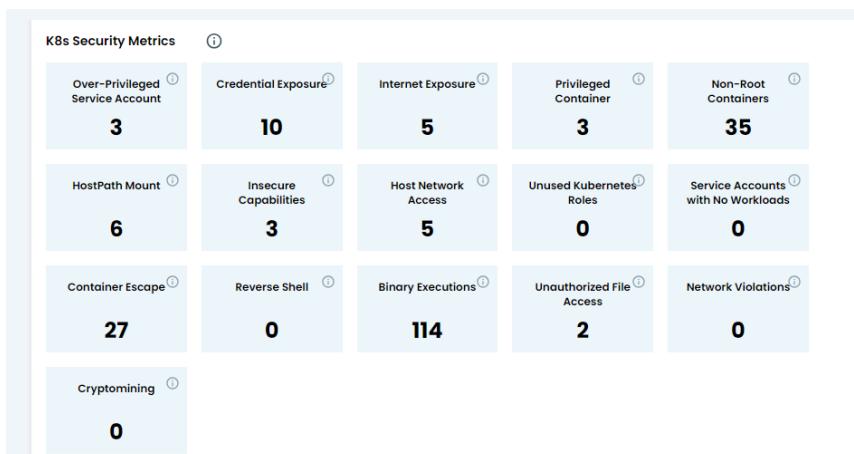
This widget provides an overview of the top findings and the number of affected resources.

2. Findings by Asset Categories Widget



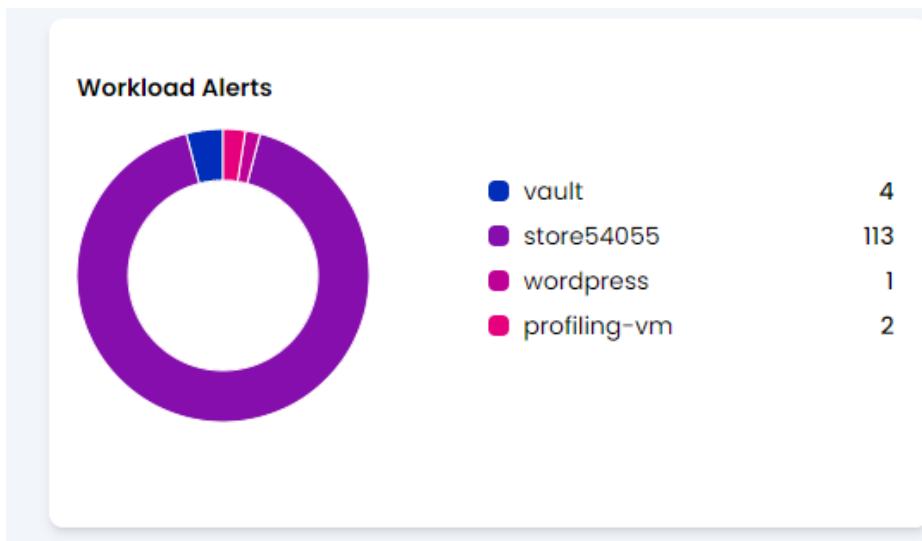
This widget categorizes failed findings by asset type and includes severity details, aiding users in pinpointing which asset categories have severe issues that need immediate attention.

3. K8S Security Metrics Widgets



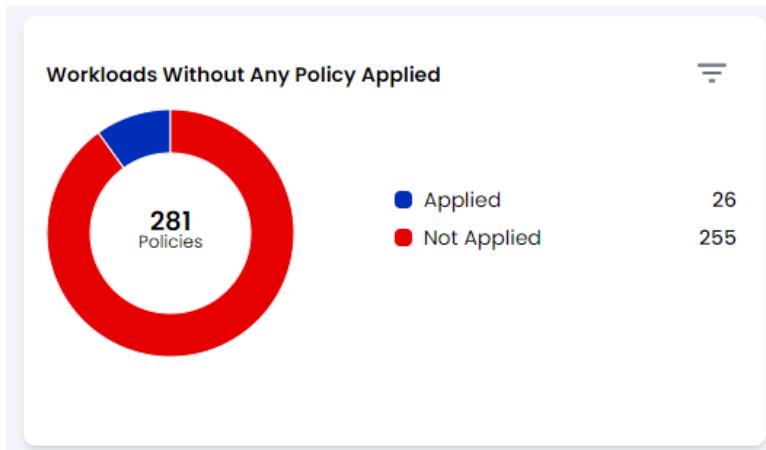
This widget highlights key security metrics related to misconfigurations and vulnerabilities within your Kubernetes clusters, helping to identify and mitigate potential security risks.

4. Workload Alerts Widgets



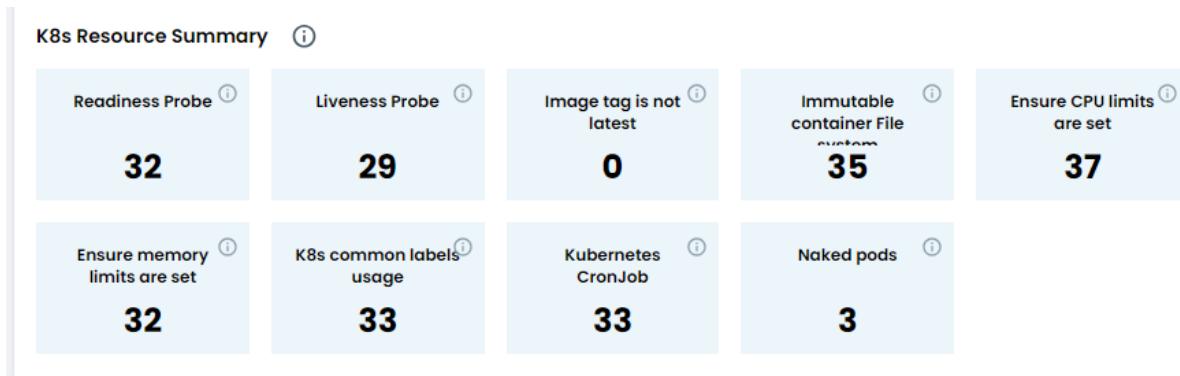
Workload Alerts shows us the alerts generated by each container or VM.

5. Workloads without any Policy Applied Widget



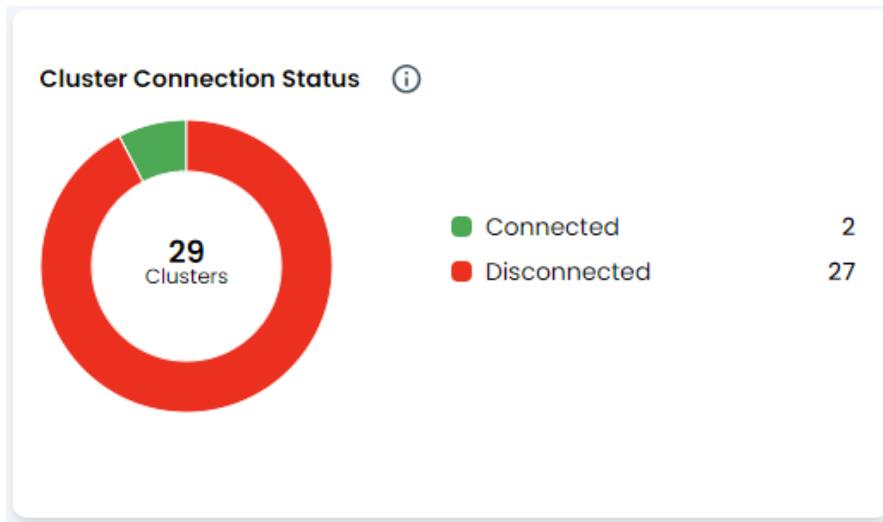
This widget shows us the total number of workloads with policies and the number of workloads policies which do not have a policy applied. The widget allows filtering based on clusters.

6. K8s Resource Summary Widget



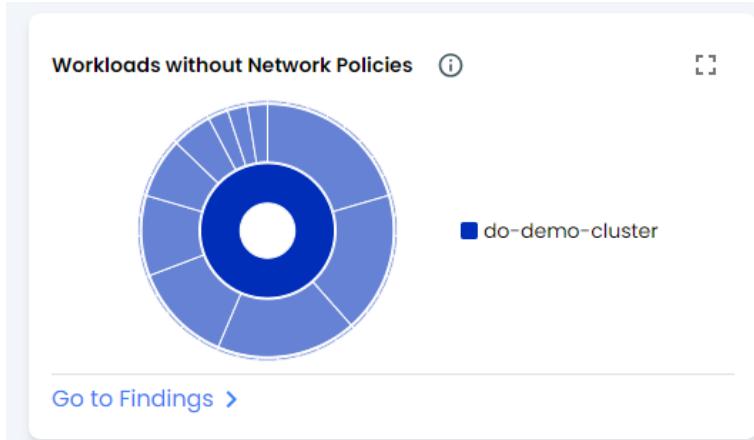
This widget displays key metrics related to resource limits, label usage, health checks, and best practices in your Kubernetes clusters.

7. Cluster Connection Status Widget



This widget will show us the connection status of Clusters which are onboarded.

8. Workloads without Network Policies Widget



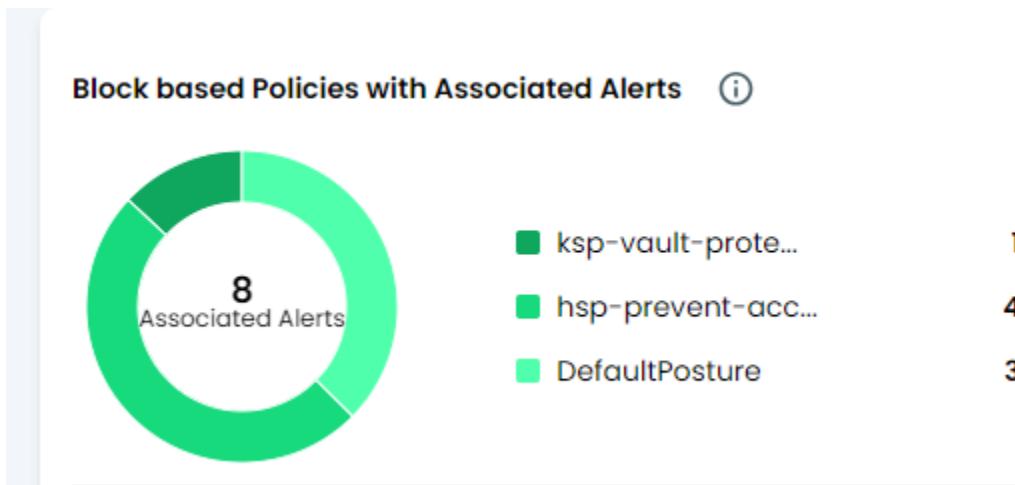
This widget displays the number of workloads that lack network policies. The aim is to help users quickly identify potential security gaps where network policies are not enforced.

9. Top 5 K8s CIS Findings Widget

Finding Name	Assets Impacted
4.2.3: Ensure that the --client-ca-file argument is set ...	1
1.1.19: Ensure that the Kubernetes PKI directory and file ...	1
1.1.13: Ensure that the admin.conf file permissions are s...	1
4.2.2: Ensure that the --authorization-mode argument...	1
4.2.1: Ensure that the --anonymous-auth argument is ...	1

This widget highlights the top 5 CIS benchmark related findings in your Kubernetes clusters, sorted by criticality and affected assets. It helps prioritize remediation to improve cluster security and compliance.

10. Block based Policies with Associated Alerts Widget

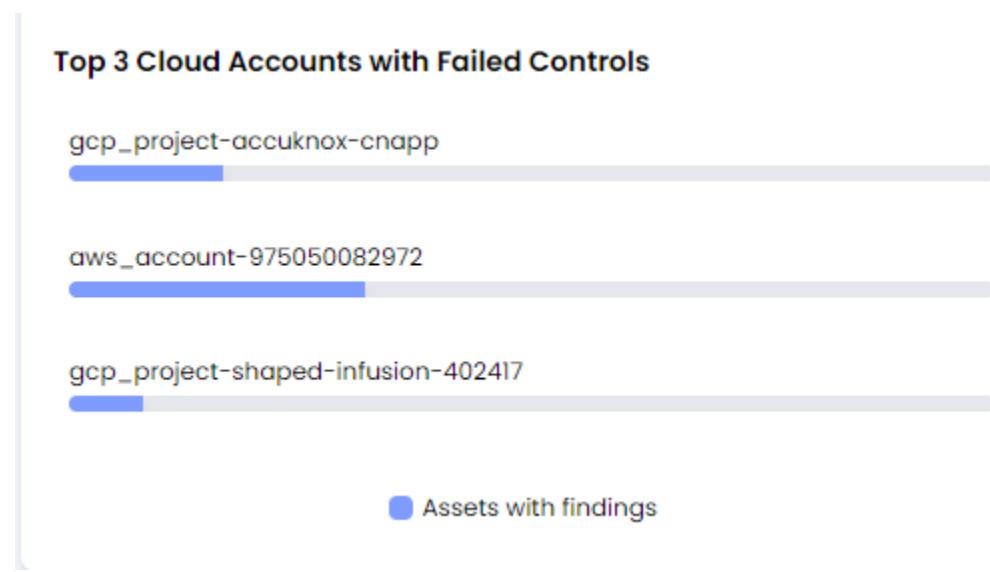


This widget shows all the block based policies which are of high severity and have alerts associated.

9.2 CSPM

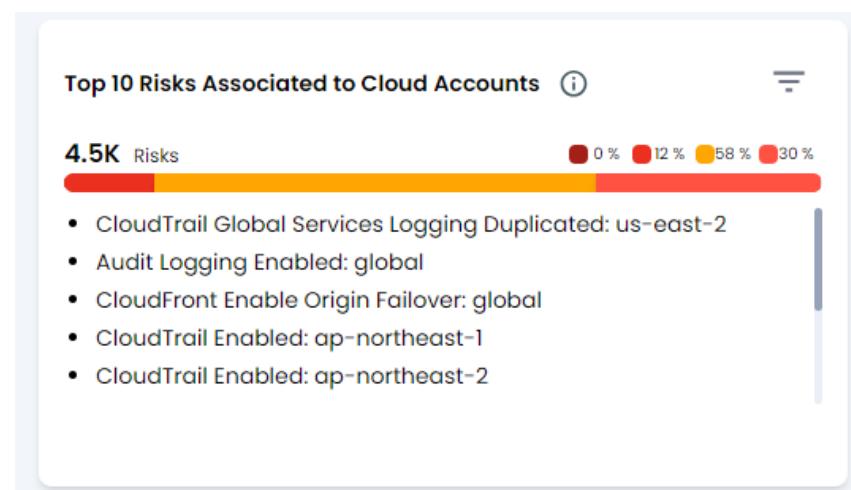
There are 5 widgets under the CSPM section

1. Top 3 cloud accounts with failed controls Widget



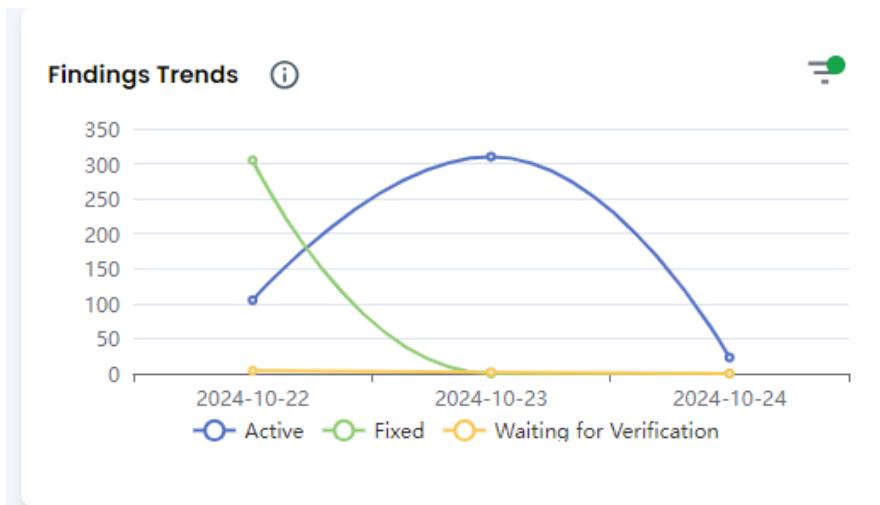
This widget will show the top 3 cloud accounts based on the highest number of failed controls.

2. Top 10 risk associated to cloud accounts Widget



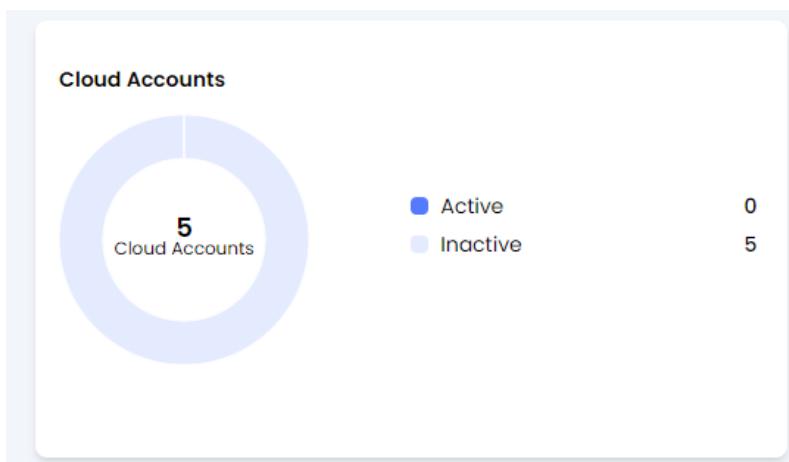
This widget assesses and prioritizes risks associated with IAM policies, S3 bucket, security groups, load balancers, etc... across your cloud accounts.

3. Findings Trends Widget



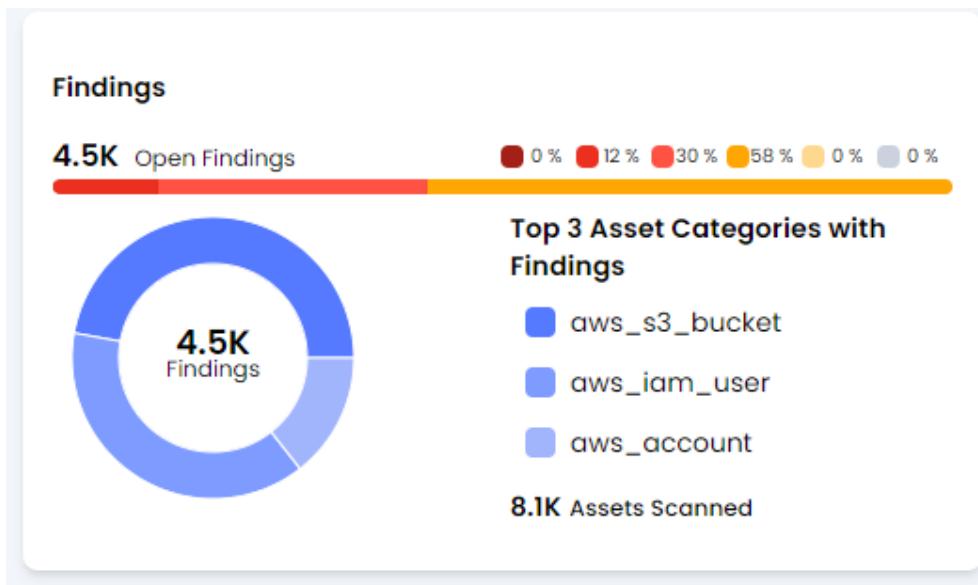
Trend analysis showing the status of findings and their changes over time in the environment.

4. Cloud Accounts Widget



This widget shows the number of cloud accounts on boarded on the AccuKnox platform and the status of their connection, i.e: Active/Inactive.

5. Findings Widget

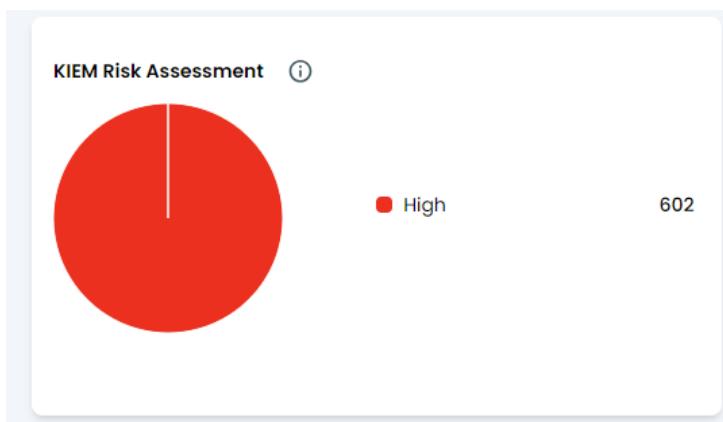


This widget shows us the total number of Findings along with top 3 asset categories that have the highest number of Findings associated with them.

9.3 KIEM

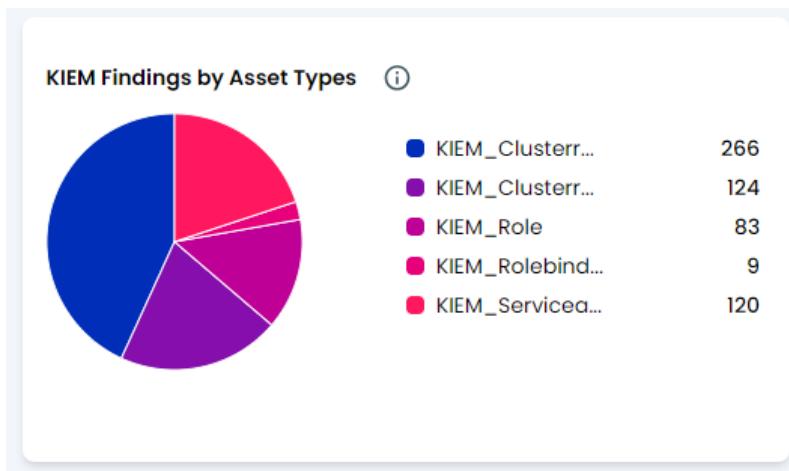
The KIEM section consists of 3 widgets

1. Kiem Risk Assessment Widget



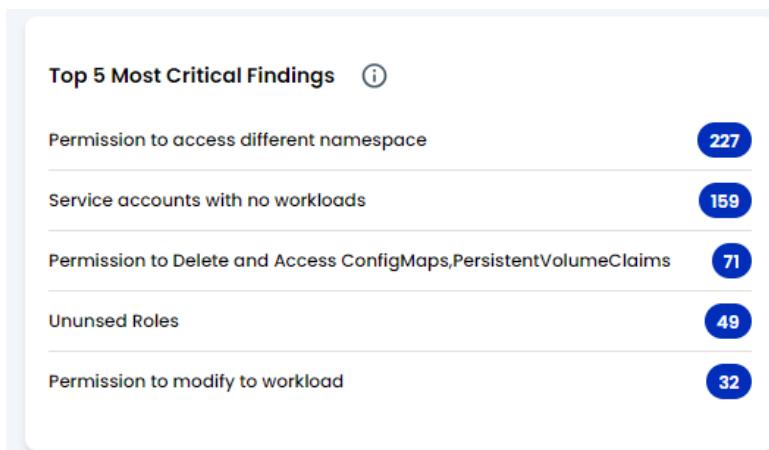
This widget shows us the distribution of KIEM findings by criticality.

2. KIEM Findings by Asset type Widget



This widget shows the distribution of KIEM findings by the type of assets they were identified in.

3. Top 5 most critical findings Widget



This widget shows the most critical findings with the highest number of occurrences or assets affected for prioritization.

9.4 Cloud Misconfiguration Widget

This section currently contains the following widgets

Cloud Account Risk Assessment Widget

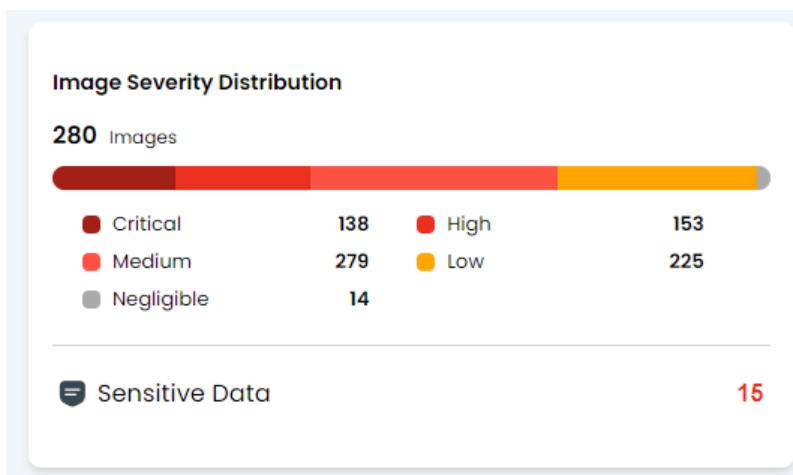


This widget shows the total number of checks that were performed and their result in a pie chart. This can be further filtered to include only the checks for specific cloud accounts.

9.5 Container images Widgets

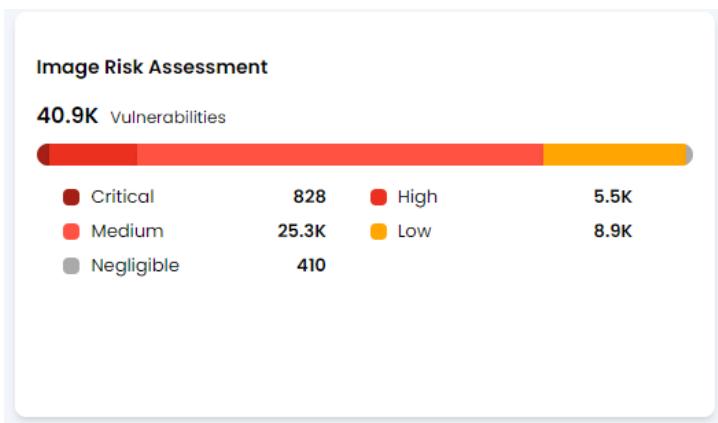
This section consists of two widgets

1. Image Severity Distribution Widget



This widget shows the total number of vulnerable ./images along with the severity level of the vulnerability identified in them. Eg. In the above image, there are 138 ./images identified to contain a critical vulnerability

2. Image Risk Assessment Widget

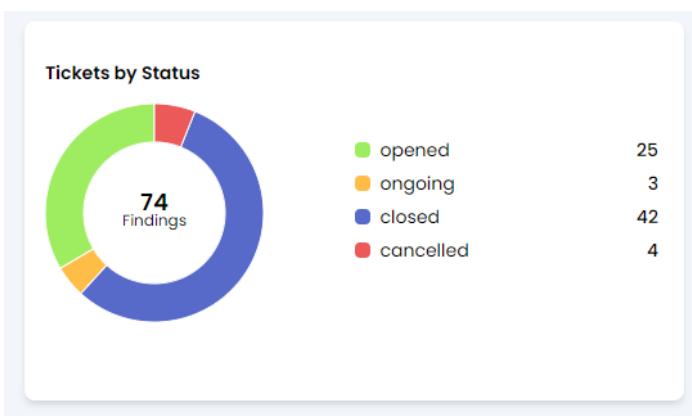


This widget shows the total number of vulnerabilities identified in all the container images along with the severity levels.

9.6 Tickets Widgets

Here, the following widget exists for visualization.

Tickets by status Widget



This widget shows us the total number of tickets generated for the findings along with their current status.

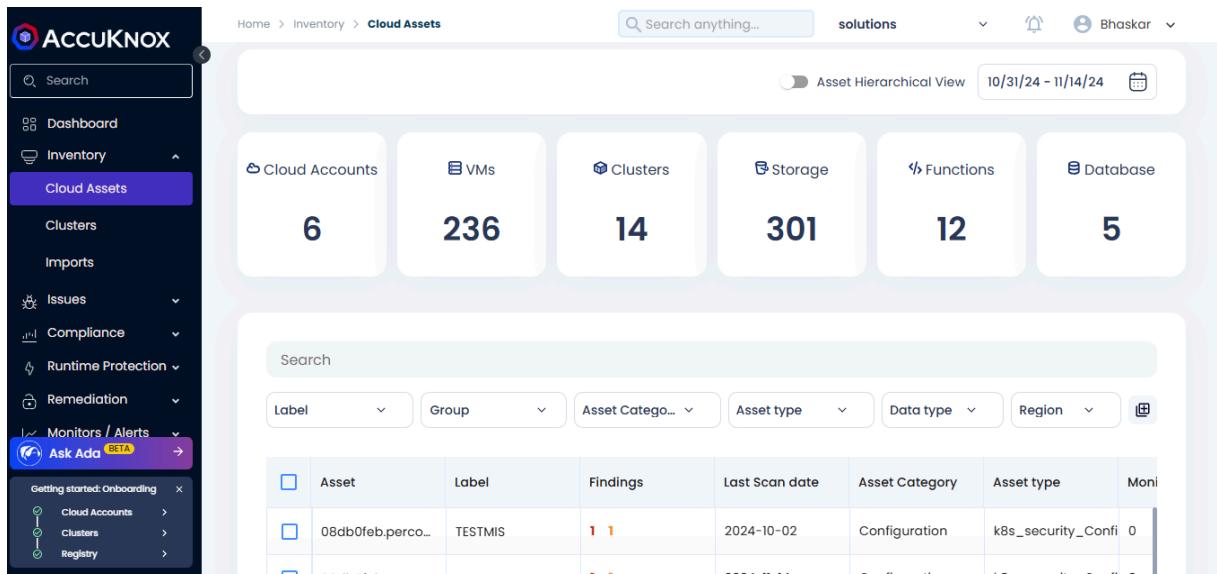
10. CSPM (Cloud Security Posture Management)

10.1 Asset Inventory

Cloud Assets

10.1.1 How to find a particular asset

- First navigate to the Cloud Assets screen under Inventory:



The screenshot shows the AccuKNOX platform's Cloud Assets interface. On the left, a dark sidebar menu is open, with 'Cloud Assets' selected. The main area displays a summary dashboard with counts for various asset types: Cloud Accounts (6), VMs (236), Clusters (14), Storage (301), Functions (12), and Database (5). Below this is a search bar and a table of assets. The table has columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, and Moni. One row is visible, showing an asset labeled '08db0feb.perco...' with a 'TESTMIS' label, 1 finding, scanned on 2024-10-02, categorized as Configuration, and typed as k8s_security_Confi.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Moni
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0

- If the name of the Asset is not known but the Asset type is known, the Filter by "Asset type" can be used to filter the Assets list. The search functionality can also be used on the filtered result:

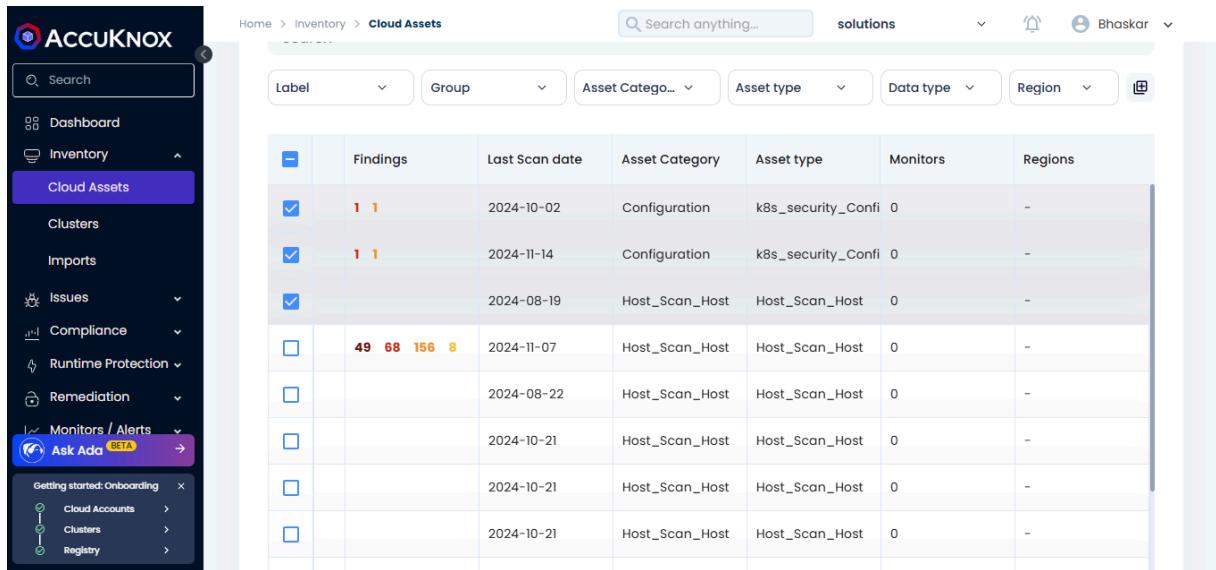
Home > Inventory > Cloud Assets

Search anything... solutions Bhaskar

Label	Group	Asset Catego...	Asset type	Data type	Region
			aws_account		Moni
			null_parent		
			aws_cloudformation_stack		
			aws_ebs_volume		
			aws_ec2_instance		
			aws_ec2_launch_template		
			aws_ec2_load_balancer_listener		
			aws_ec2_network_interface		
			aws_ec2_network_load_balancer		
			2024-08-22	Host_Scan_Host	Host_Scan_Host 0
			173.201.177.205(ip_	Host_Scan_Host	Host_Scan_Host 0
			173.201.185.104(ip_	Host_Scan_Host	Host_Scan_Host 0
			173.231.229.252(v_	Host_Scan_Host	Host_Scan_Host 0

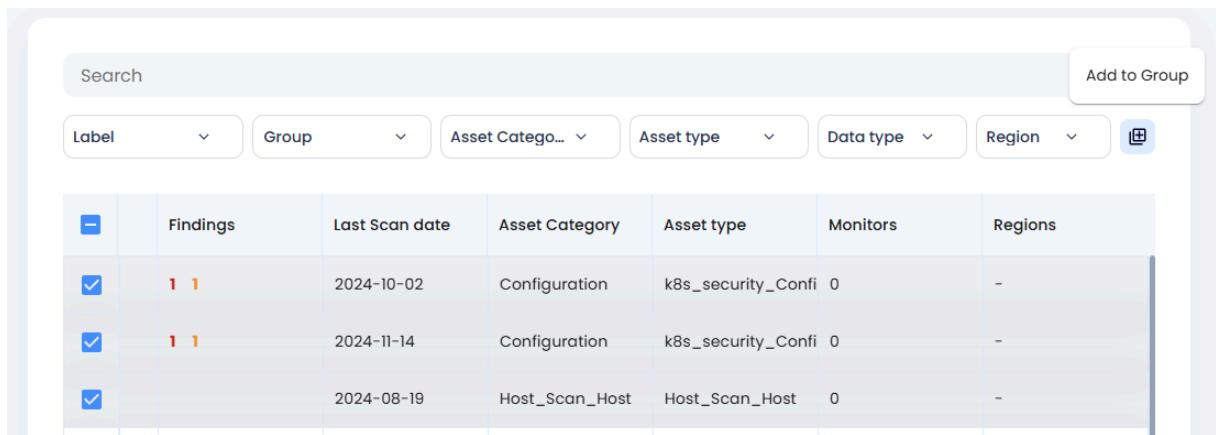
10.1.2 How to group assets

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



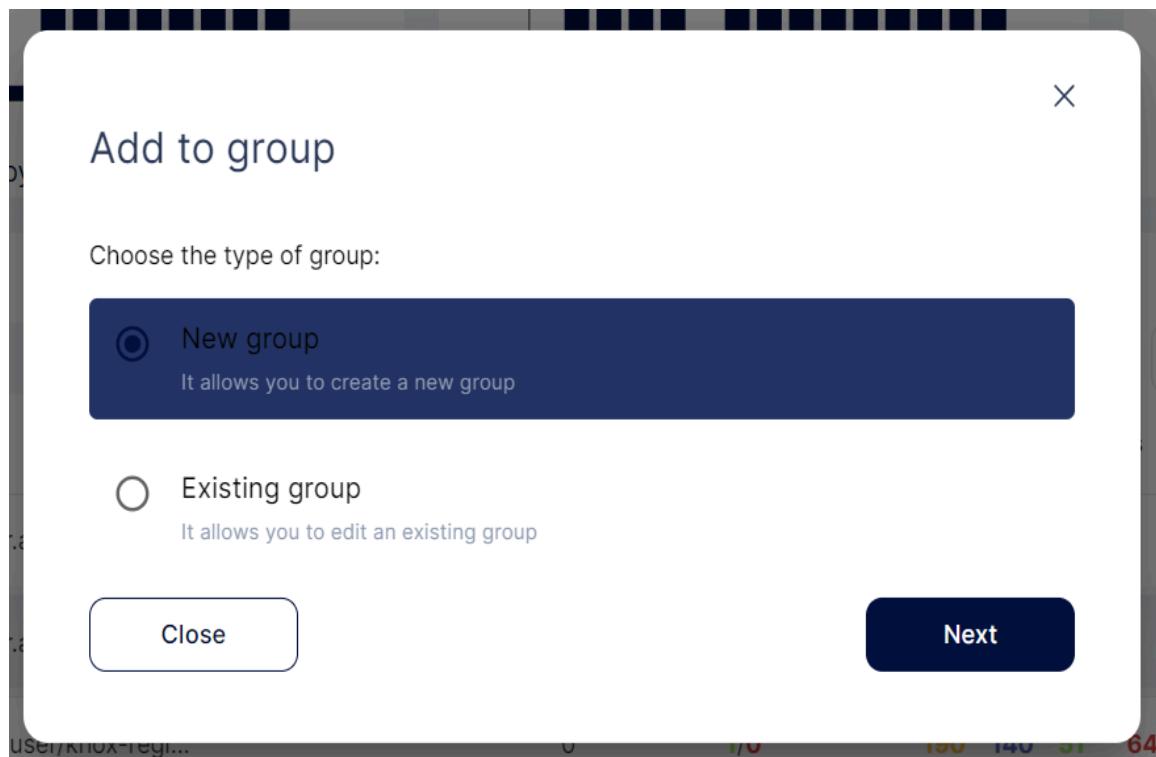
The screenshot shows the AccuKnox Cloud Assets interface. On the left, there's a sidebar with navigation links like Dashboard, Inventory (selected), Cloud Assets (highlighted in purple), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Ada. The main area is titled "Cloud Assets" and shows a table of findings. The table has columns: Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. There are 8 rows of data, with the first three rows having checked checkboxes in the first column. The data includes various scan dates, categories like Configuration and Host_Scan_Host, and asset types like k8s_security_Confi and Host_Scan_Host.

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

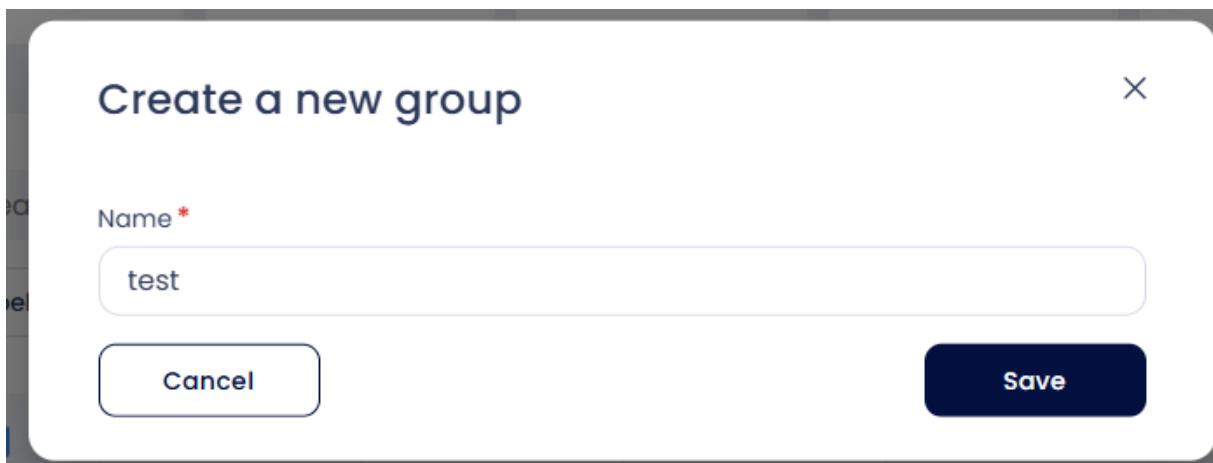


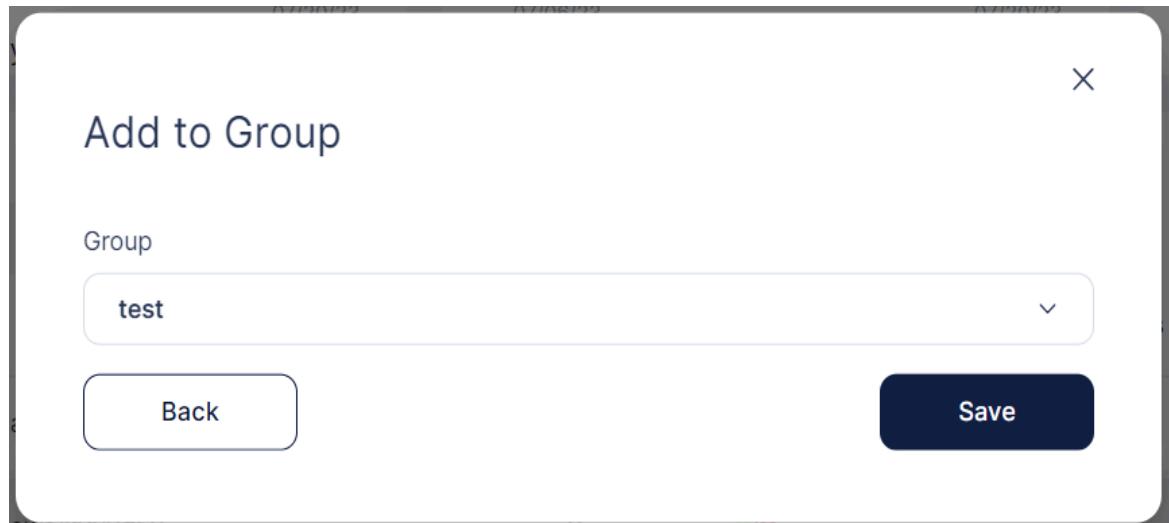
This screenshot shows the same AccuKnox Cloud Assets interface as the previous one, but with a "Add to Group" button visible in the top right corner of the header bar. The rest of the interface and data table remain the same.

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

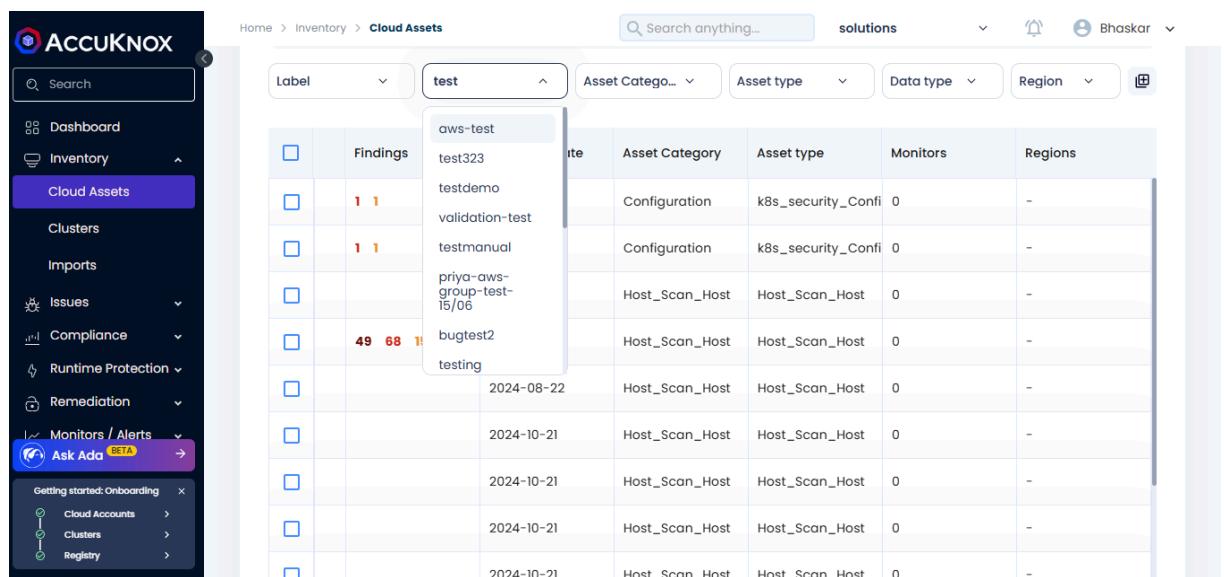


- After entering a name for the group or selecting an existing group, click on Save to finish adding the assets to a group:





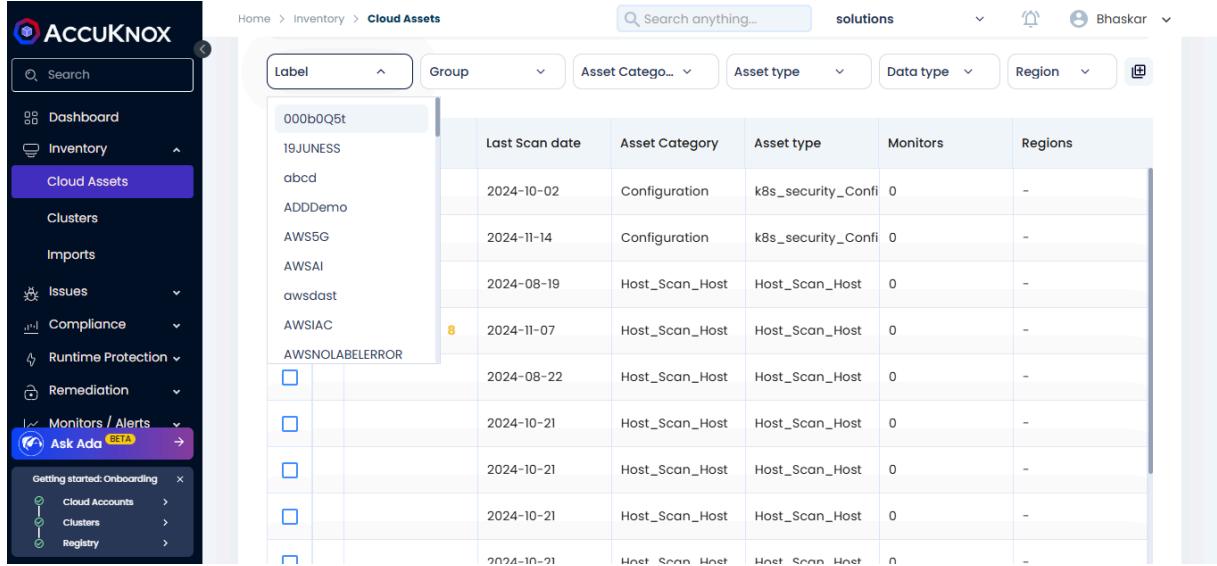
- Now, filtering by group allows us to see only the assets that were added to the group:



Findings	Date	Asset Category	Asset type	Monitors	Regions
1 1	2024-08-22	Configuration	k8s_security_Config	0	-
1 1	2024-10-21	Configuration	k8s_security_Config	0	-
49 68 1	2024-10-21	Host_Scan_Host	Host_Scan_Host	0	-
	2024-10-21	Host_Scan_Host	Host_Scan_Host	0	-
	2024-10-21	Host_Scan_Host	Host_Scan_Host	0	-
	2024-10-21	Host_Scan_Host	Host_Scan_Host	0	-
	2024-10-21	Host_Scan_Host	Host_Scan_Host	0	-

10.1.3 How to search asset by label

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



The screenshot shows the ACCUKNOW platform's Cloud Assets section. On the left is a navigation sidebar with various menu items like Dashboard, Inventory, Cloud Assets (which is selected and highlighted in purple), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Ada (Beta). Below the sidebar is a 'Getting started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main area displays a table of assets under the heading 'Cloud Assets'. The table has columns for Label, Group, Asset Category, Asset type, Monitors, and Regions. A search bar at the top right allows users to 'Search anything...'. The table shows several rows of asset data, with one row currently selected, indicated by a blue border around its cells. The selected row contains the label '000b0Q5t' and the group '19JUNESS'. The other columns show details such as Last Scan date, Asset Category, Asset type, Monitors, and Regions.

Label	Group	Asset Catego...	Asset type	Monitors	Regions
000b0Q5t	19JUNESS				
abcd		Last Scan date	Asset Category	Asset type	Monitors
ADDDemo		2024-10-02	Configuration	k8s_security_Confi	0
AWS5G		2024-11-14	Configuration	k8s_security_Confi	0
AWSAI		2024-08-19	Host_Scan_Host	Host_Scan_Host	0
awsclast		2024-11-07	Host_Scan_Host	Host_Scan_Host	0
AWSIAC	8	2024-08-22	Host_Scan_Host	Host_Scan_Host	0
AWSNOLABELERROR		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
		2024-10-21	Host_Scan_Host	Host_Scan_Host	0

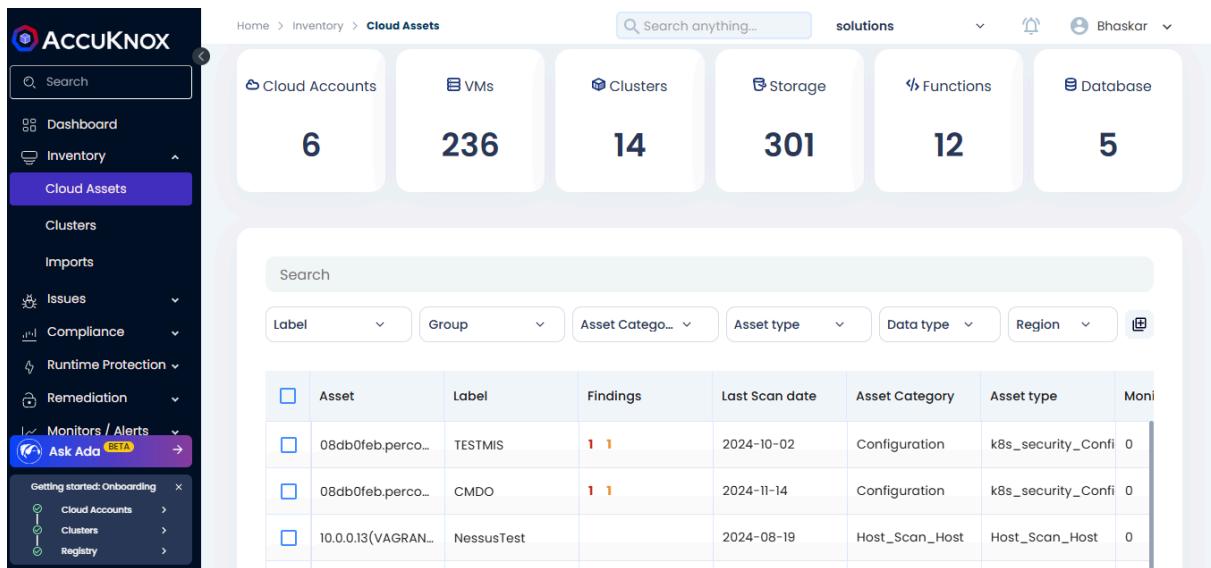
- To further refine the results, we can use the search bar or add additional filters such as Assets.

10.2 Misconfigurations

10.2.1 Where to find misconfigurations

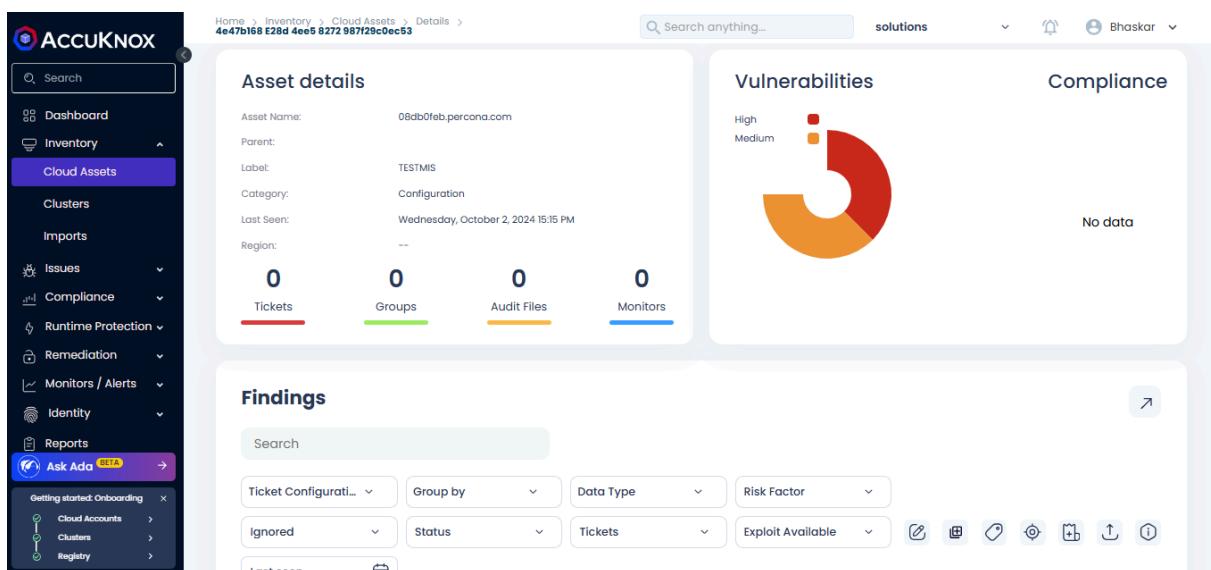
- Cloud Assets Page

Once we have onboarded the Cloud Account, we can navigate to the Inventory → Cloud Assets, here we can see the list of Assets with vulnerabilities.



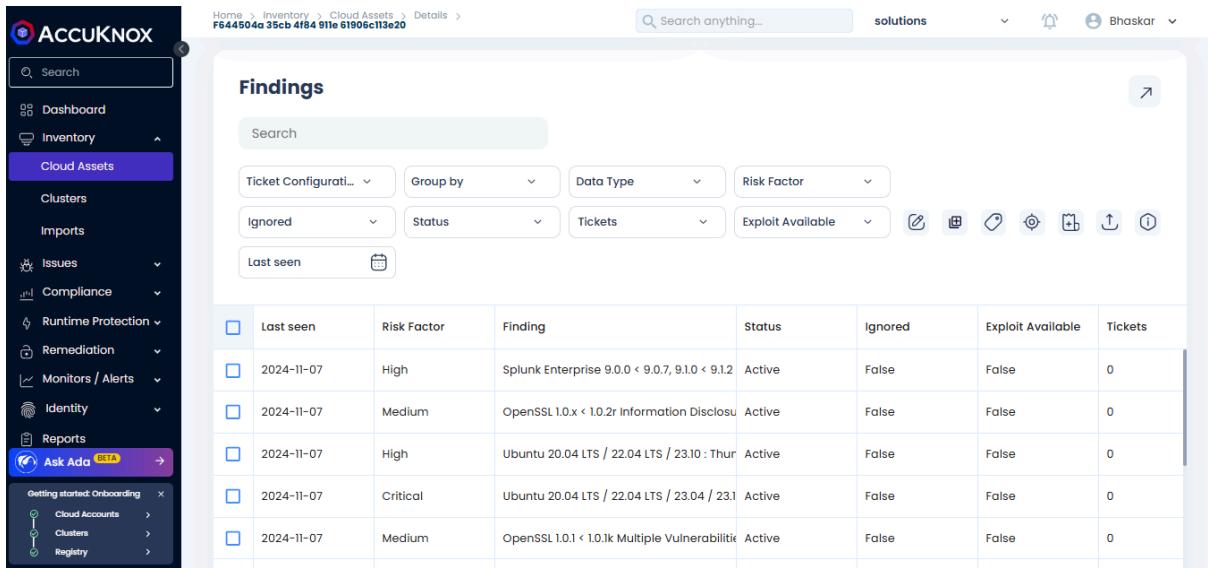
The screenshot shows the AccuKnox interface for Cloud Assets. On the left is a dark sidebar with navigation links like Dashboard, Inventory, Cloud Assets (which is selected), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Ada (Beta). The main area has a header with Home > Inventory > Cloud Assets, a search bar, and user information. Below the header is a summary card with counts for Cloud Accounts (6), VMs (236), Clusters (14), Storage (301), Functions (12), and Database (5). A large table below lists assets with columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, and Monitoring. Three rows are shown: 08db0feb.percona.com (TESTMIS, Configuration, Host_Scan_Host), 08db0feb.percona.com (CMDO, Configuration, Host_Scan_Host), and 10.0.0.13(VAGRAN... (NessusTest, Host_Scan_Host).

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



The screenshot shows the Asset Details page for the asset 08db0feb.percona.com. The sidebar is identical to the previous screenshot. The main area has a breadcrumb path: Home > Inventory > Cloud Assets > Details > 4e47b168 E28d 4ee5 8272 987f29c0ec53. It features three main sections: Asset details (Asset Name: 08db0feb.percona.com, Parent: TESTMIS, Category: Configuration, Last Seen: Wednesday, October 2, 2024 15:15 PM, Region: --), Vulnerabilities (High: 0, Medium: 0, No data), and Compliance (No data). Below these are sections for Findings and a detailed findings table with filters for Ticket Configuration, Group by, Data Type, Risk Factor, Ignored, Status, Tickets, Exploit Available, and various edit and export icons.

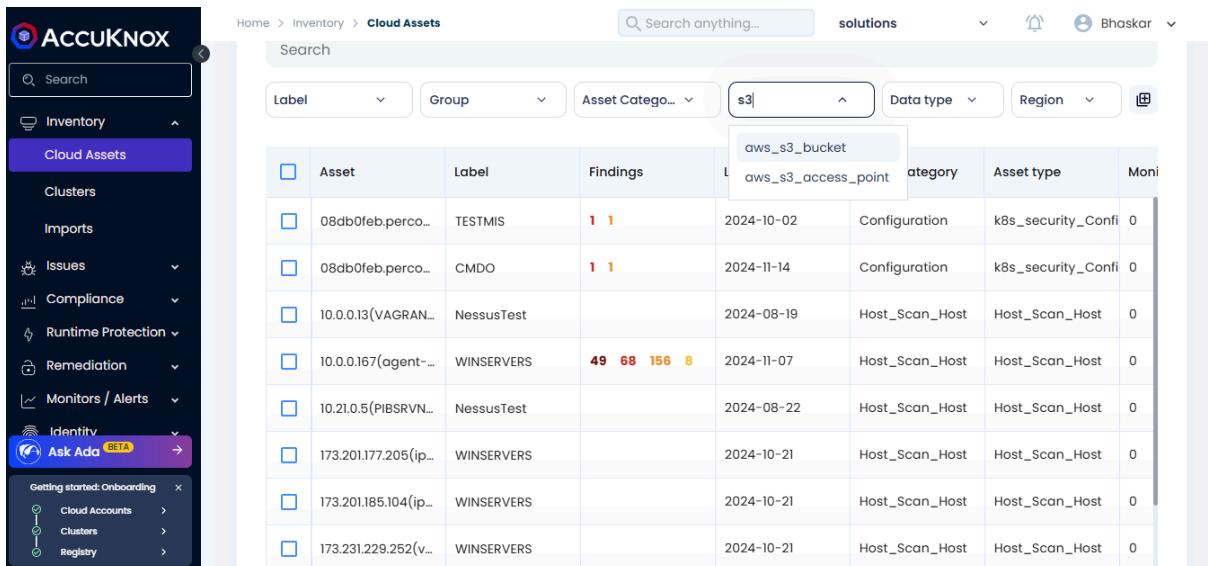
Scroll down for the Findings, here you can see the Risk Factor for the particular Findings.



Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available	Tickets
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.10 < 9.12	Active	False	False	0
2024-11-07	Medium	OpenSSL 1.0.x < 1.0.2r Information Disclosure	Active	False	False	0
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False	0
2024-11-07	Critical	Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.1	Active	False	False	0
2024-11-07	Medium	OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilities	Active	False	False	0

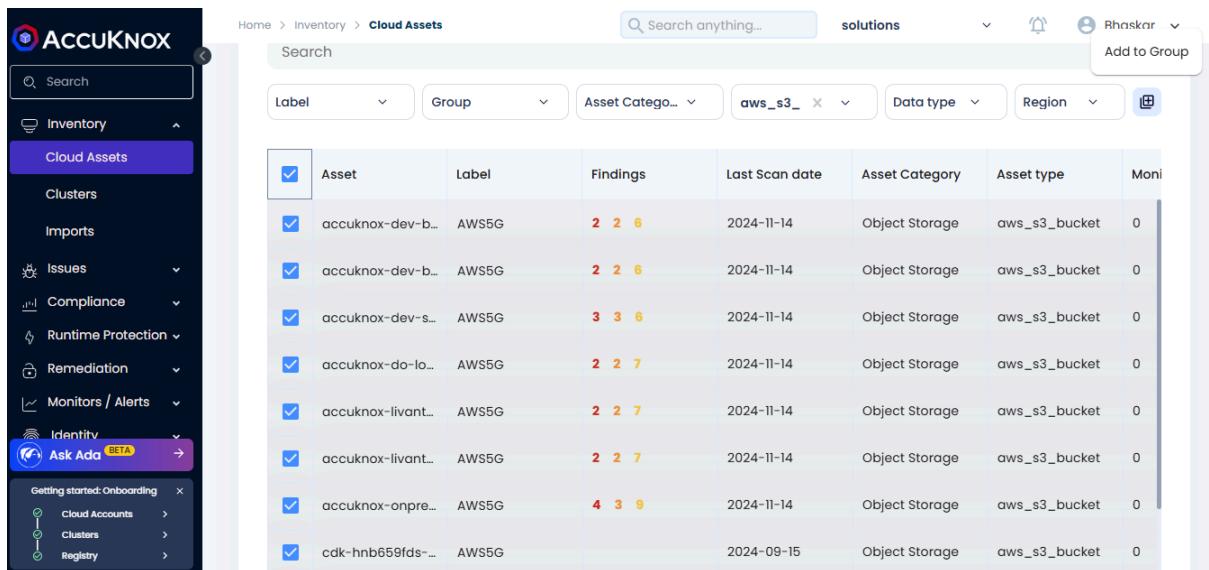
10.2.2 How to group by Asset and find misconfiguration

Step1 : In the Assets screen under Inventory, filter by Assets to view only the particular Asset type (for example s3 bucket)



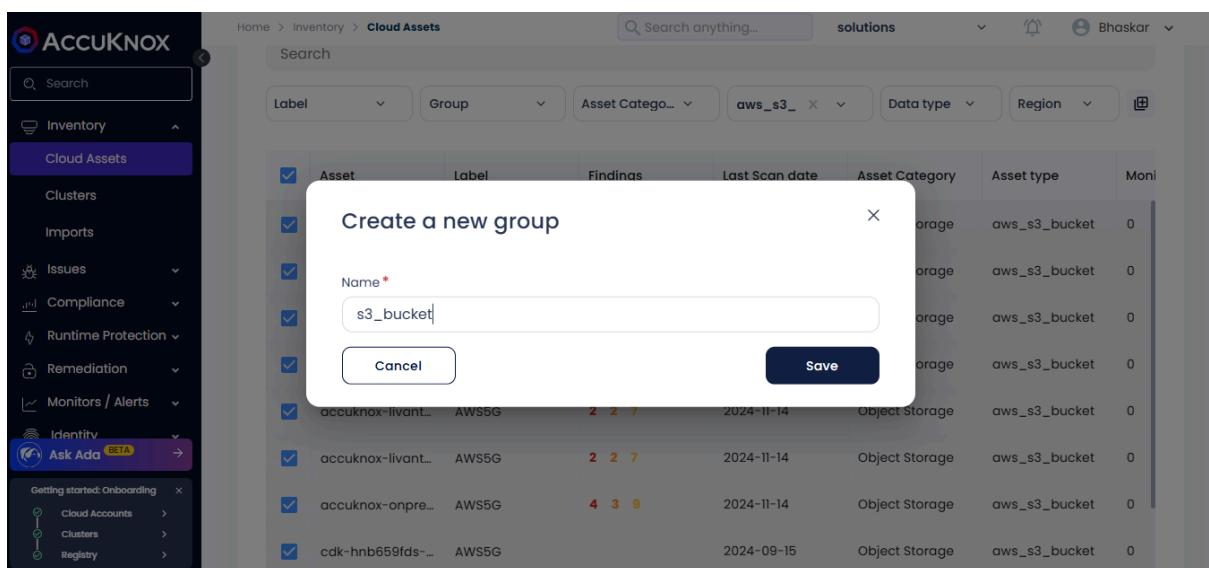
Asset	Label	Findings	Date	Category	Asset type	Mon
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0
08db0feb.perco...	CMDO	1 1	2024-11-14	Configuration	k8s_security_Confi	0
10.0.0.13(VAGRAN...	NessusTest		2024-08-19	Host_Scan_Host	Host_Scan_Host	0
10.0.0.167(agent-...	WINSERVERS	49 68 156 8	2024-11-07	Host_Scan_Host	Host_Scan_Host	0
10.21.0.5(PIBSRVN...	NessusTest		2024-08-22	Host_Scan_Host	Host_Scan_Host	0
173.201.177.205(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.201.185.104(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.231.229.252(v...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0

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



Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
accuknox-dev-b...	AWS5G	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	AWS5G	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-s...	AWS5G	3 3 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-do-lo...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-onpre...	AWS5G	4 3 9	2024-11-14	Object Storage	aws_s3_bucket	0
cdk-hnb659fds-...	AWS5G		2024-09-15	Object Storage	aws_s3_bucket	0

Step3: Click on Save



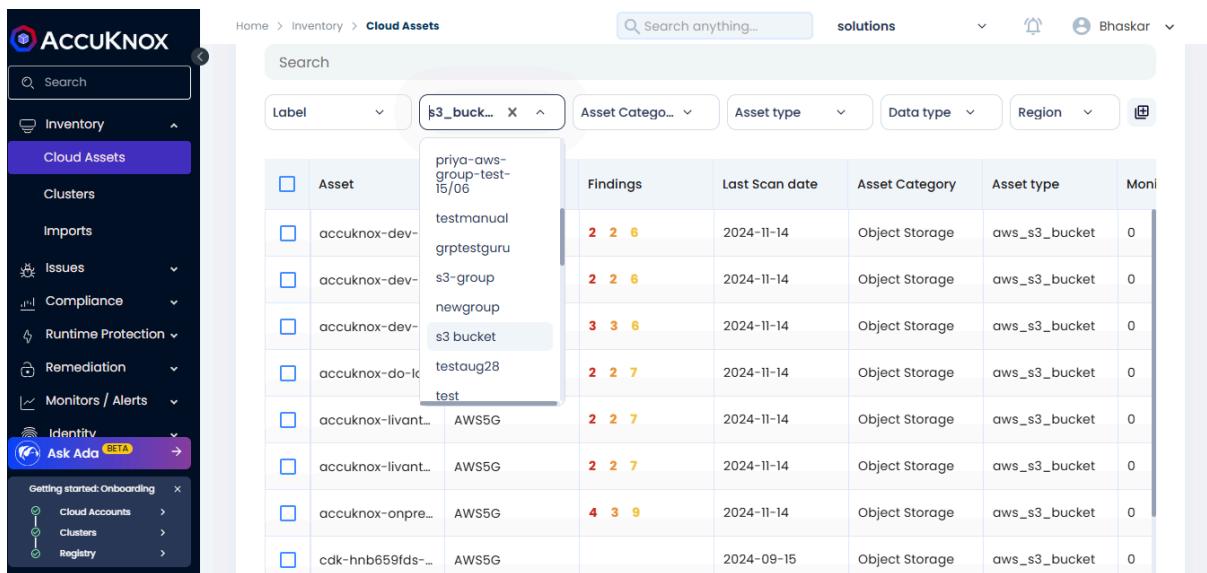
Create a new group

Name *

Cancel Save

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
accuknox-dev-b...	AWS5G	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	AWS5G	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-s...	AWS5G	3 3 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-do-lo...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-onpre...	AWS5G	4 3 9	2024-11-14	Object Storage	aws_s3_bucket	0
cdk-hnb659fds-...	AWS5G		2024-09-15	Object Storage	aws_s3_bucket	0

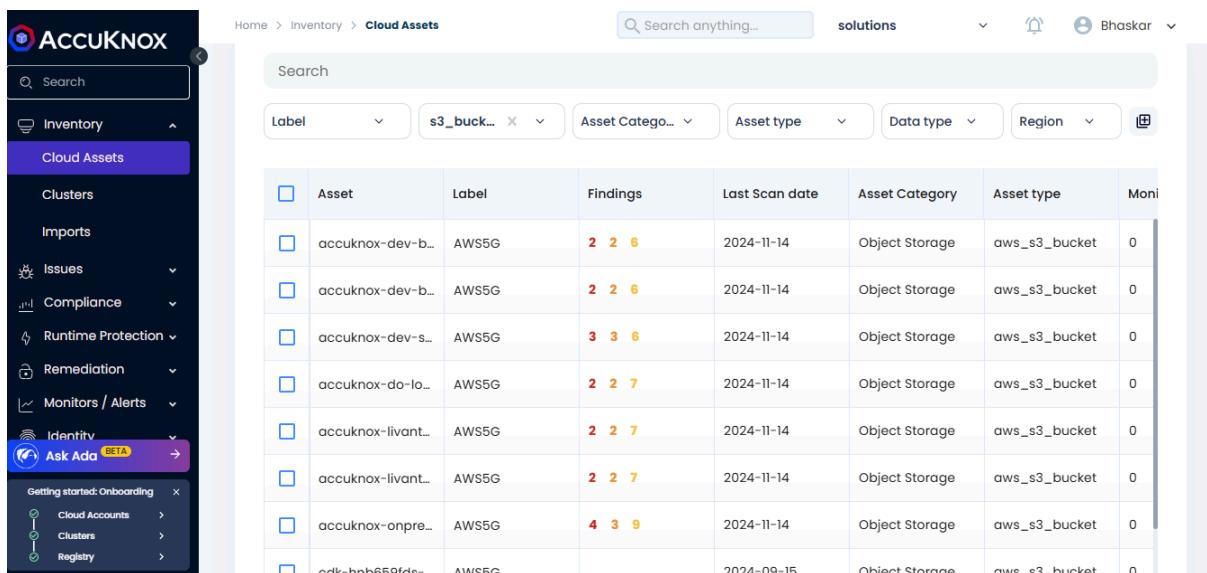
Step 4 : To view the Grouped S3 bucket details, click on Issues -> Cloud Assets, select the group that was created from the drop down:



The screenshot shows the ACCUKNOX platform interface. On the left, there's a sidebar with various navigation options like Inventory, Cloud Assets, Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, and Ask Ada (BETA). The main area is titled "Cloud Assets" and shows a search bar with the query "s3_buck...". Below the search bar is a table with columns: Asset, Label, Findings, Last Scan date, Asset Category, Asset type, and Mon. There are several rows of data, with one row highlighted in blue, indicating it has been selected.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
accuknox-dev-b...	priya-aws-group-test-15/06	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	testmanual	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	grpptestguru	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	s3-group	3 3 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	newgroup	3 3 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-dev-b...	s3 bucket	3 3 6	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-do-lo...	testaug28	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	test	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-livant...	AWS5G	2 2 7	2024-11-14	Object Storage	aws_s3_bucket	0
accuknox-onpre...	AWS5G	4 3 9	2024-11-14	Object Storage	aws_s3_bucket	0
cdk-hnb659fds-...	AWS5G		2024-09-15	Object Storage	aws_s3_bucket	0

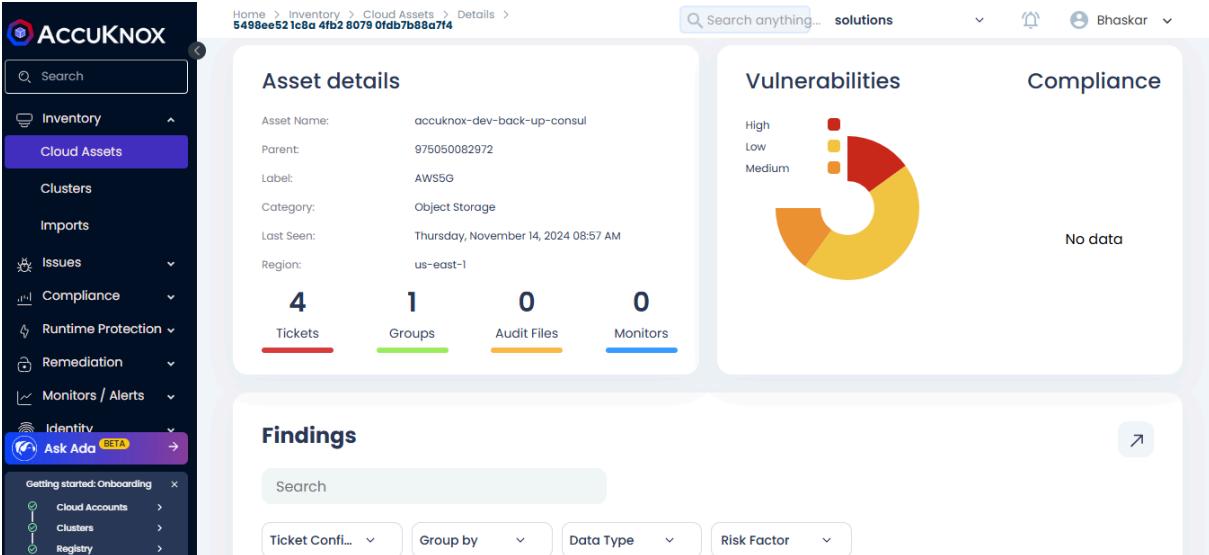
Step 5: Select the Group, the list of s3 buckets with any misconfigurations associated with them can be seen



This screenshot is identical to the one above, showing the ACCUKNOX Cloud Assets page. The search bar contains "s3_buck...". A single row from the previous table is now highlighted in blue, indicating it has been selected for further inspection.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
accuknox-dev-b...	AWS5G	2 2 6	2024-11-14	Object Storage	aws_s3_bucket	0

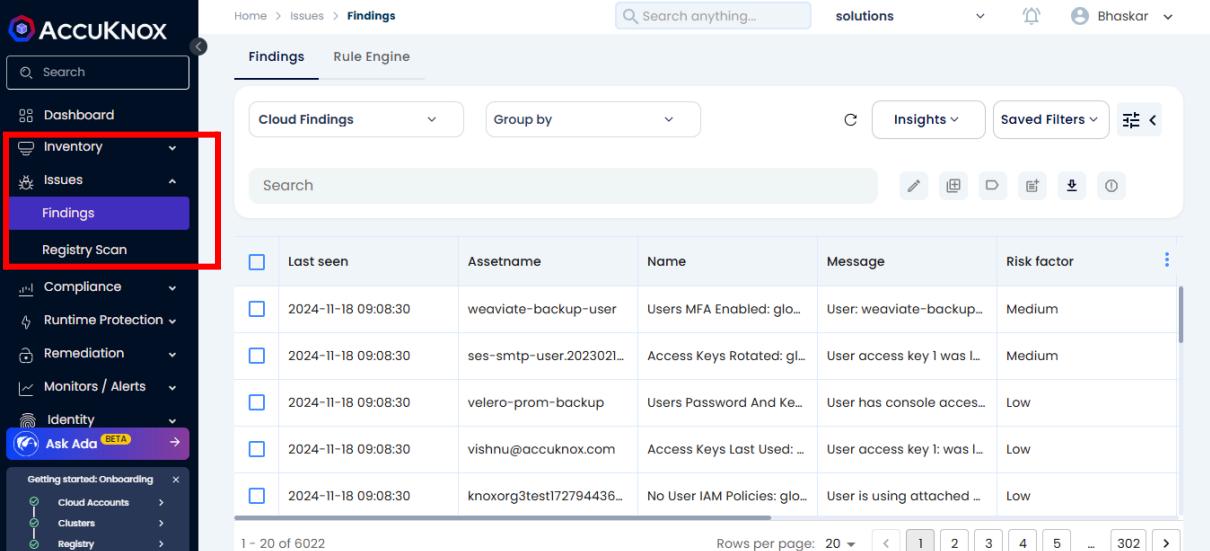
Step 7: Click on any of them to get more details



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

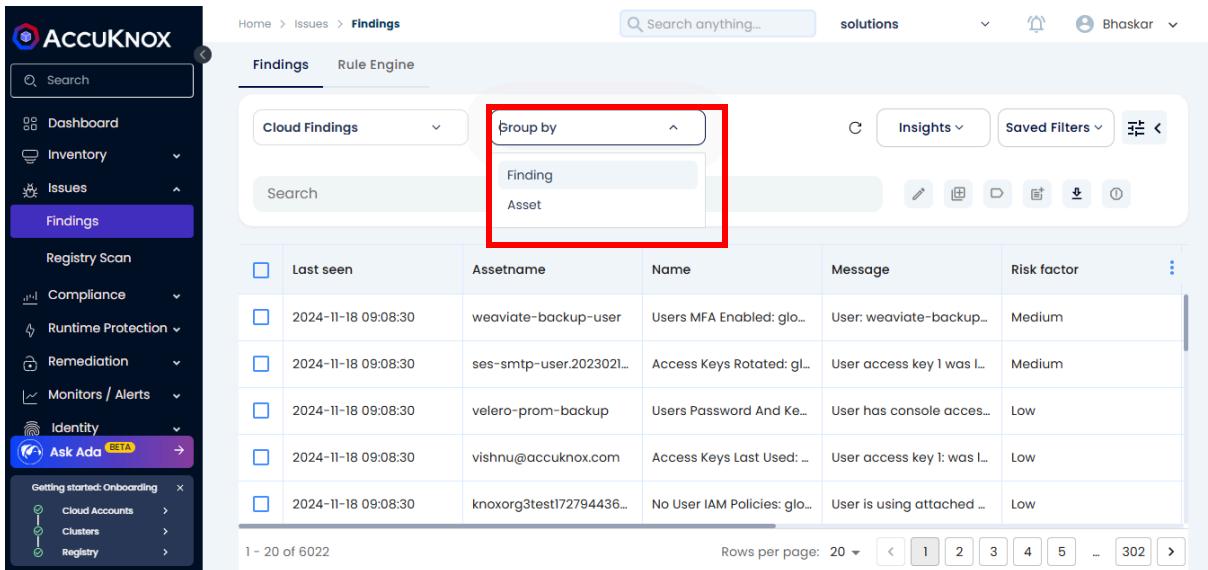
10.2.3 How to group by Findings

1. Go to **Issues** tab, click on **Findings** section



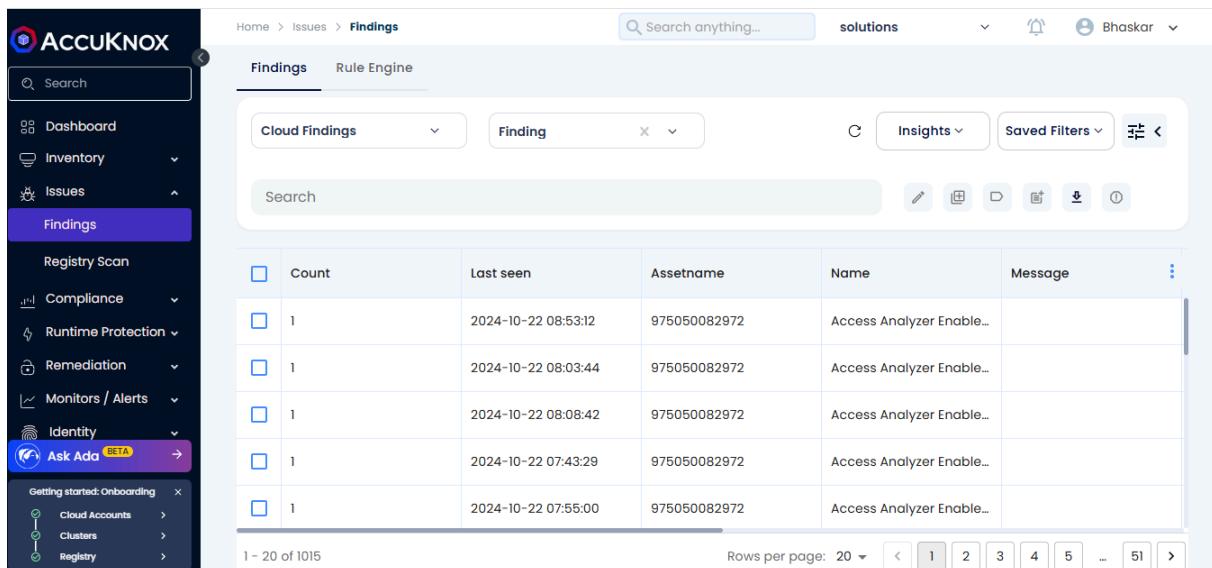
Last seen	Assetname	Name	Message	Risk factor
2024-11-18 09:08:30	weaviate-backup-user	Users MFA Enabled: glo...	User: weaviate-backup...	Medium
2024-11-18 09:08:30	ses-smtp-user.2023021...	Access Keys Rotated: gl...	User access key 1 was l...	Medium
2024-11-18 09:08:30	velero-prom-backup	Users Password And Ke...	User has console acces...	Low
2024-11-18 09:08:30	vishnu@accuknox.com	Access Keys Last Used: ...	User access key 1: was l...	Low
2024-11-18 09:08:30	knoxorg3test172794436...	No User IAM Policies: glo...	User is using attached ...	Low

2. Navigate to **Group by** filter and choose Findings



The screenshot shows the AccuKnox interface with the 'Findings' tab selected in the sidebar. The main area displays a table of findings. Above the table, there is a 'Group by' dropdown menu with two options: 'Finding' and 'Asset'. The 'Finding' option is highlighted with a red box.

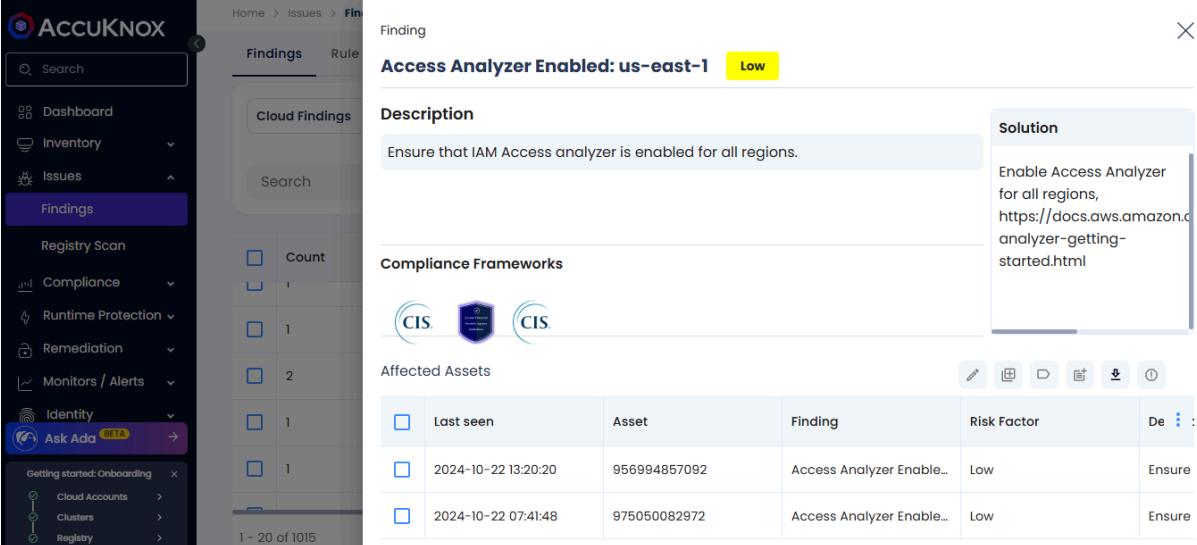
Last seen	Assetname	Name	Message	Risk factor
2024-11-18 09:08:30	weaviate-backup-user	Users MFA Enabled: glo...	User: weaviate-backup...	Medium
2024-11-18 09:08:30	ses-smtp-user.2023021...	Access Keys Rotated: gl...	User access key 1 was l...	Medium
2024-11-18 09:08:30	velero-prom-backup	Users Password And Ke...	User has console acces...	Low
2024-11-18 09:08:30	vishnu@accuknox.com	Access Keys Last Used: ...	User access key 1: was l...	Low
2024-11-18 09:08:30	knoxorg3test172794436...	No User IAM Policies: glo...	User is using attached ...	Low



The screenshot shows the AccuKnox interface with the 'Findings' tab selected in the sidebar. The main area displays a table of findings. Above the table, there is a 'Group by' dropdown menu with two options: 'Cloud Findings' and 'Finding'. The 'Asset' option is selected and highlighted with a red box.

Count	Last seen	Assetname	Name	Message
1	2024-10-22 08:53:12	975050082972	Access Analyzer Enable...	
1	2024-10-22 08:03:44	975050082972	Access Analyzer Enable...	
1	2024-10-22 08:08:42	975050082972	Access Analyzer Enable...	
1	2024-10-22 07:43:29	975050082972	Access Analyzer Enable...	
1	2024-10-22 07:55:00	975050082972	Access Analyzer Enable...	

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



Description

Ensure that IAM Access analyzer is enabled for all regions.

Solution

Enable Access Analyzer for all regions,
<https://docs.aws.amazon.com/analyzer-getting-started.html>

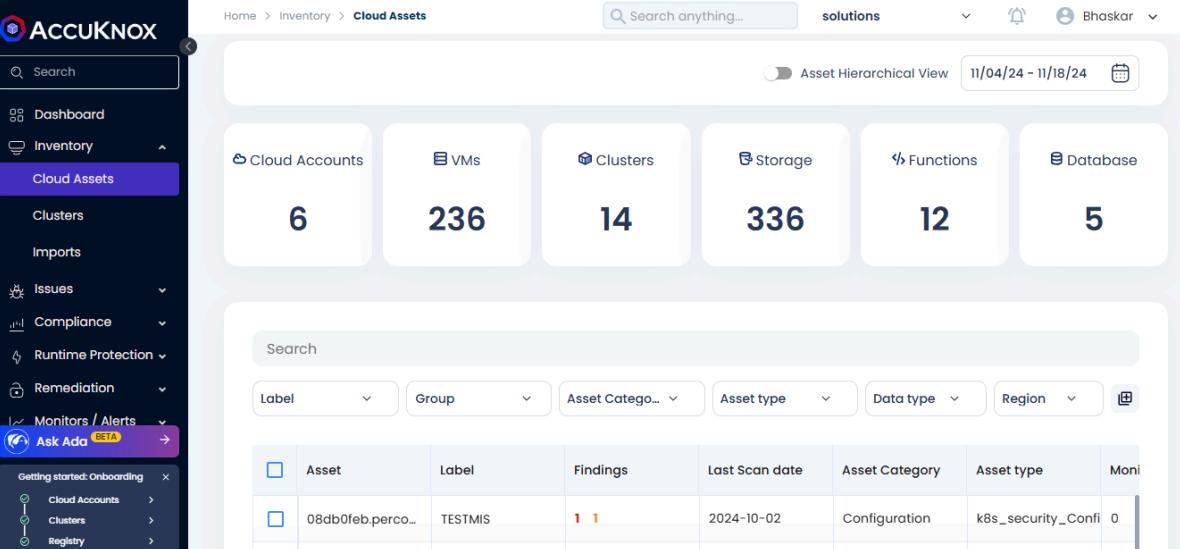
Compliance Frameworks

Affected Assets

Last seen	Asset	Finding	Risk Factor	De
2024-10-22 13:20:20	956994857092	Access Analyzer Enable...	Low	Ensure
2024-10-22 07:41:48	975050082972	Access Analyzer Enable...	Low	Ensure

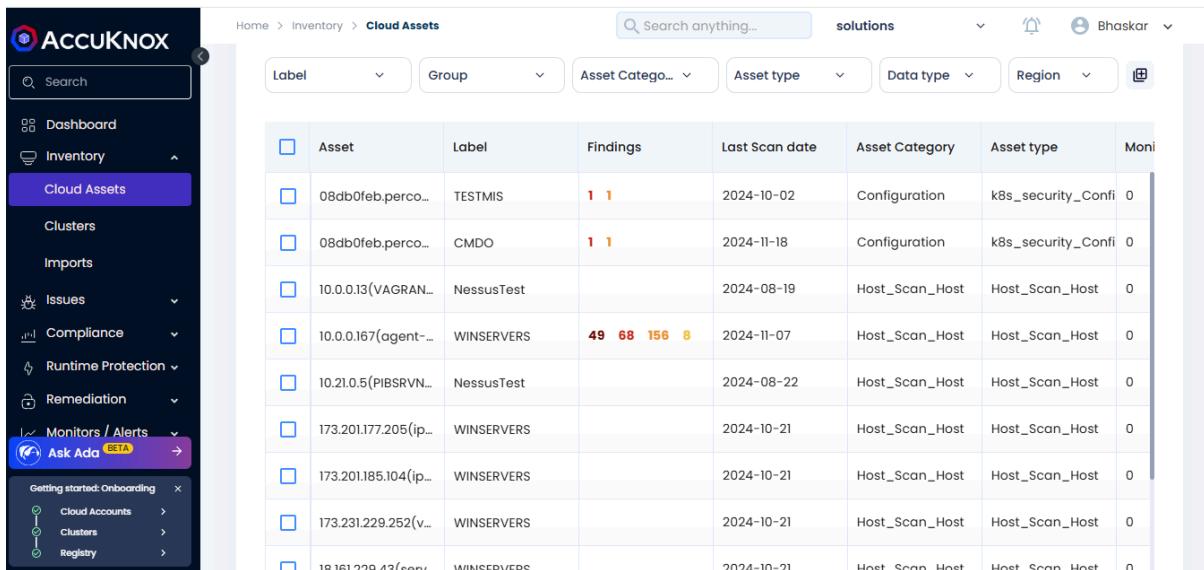
10.2.4 How to group by criticality and Status

1. Goto Inventory tab, click on Cloud Assets section



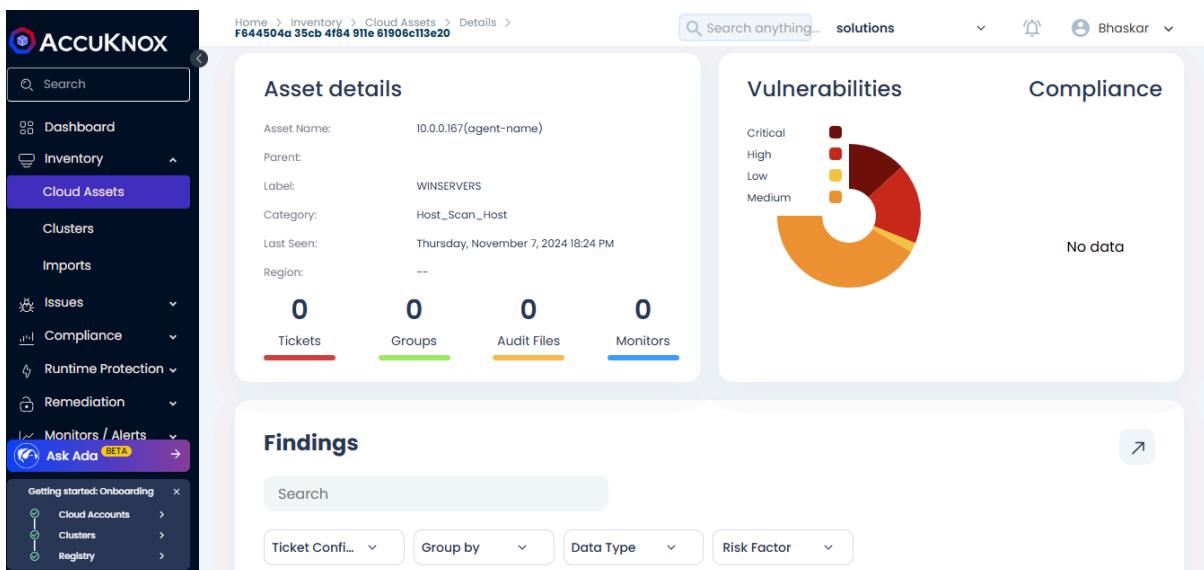
Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Moni
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0

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



Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0
08db0feb.perco...	CMDO	1 1	2024-11-18	Configuration	k8s_security_Confi	0
10.0.0.13(VAGRAN...	NessusTest		2024-08-19	Host_Scan_Host	Host_Scan_Host	0
10.0.0.167(agent-...	WINSERVERS	49 68 156 8	2024-11-07	Host_Scan_Host	Host_Scan_Host	0
10.21.0.5(PIBSRVN...	NessusTest		2024-08-22	Host_Scan_Host	Host_Scan_Host	0
173.201.177.205(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.201.185.104(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.231.229.252(v...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
18.161.229.43(serv...	WINSFRVFRS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0

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



Asset details

Asset Name: 10.0.0.167(agent-name)

Parent:

Label: WINSERVERS

Category: Host_Scan_Host

Last Seen: Thursday, November 7, 2024 18:24 PM

Region: --

0 Tickets **0 Groups** **0 Audit Files** **0 Monitors**

Vulnerabilities

Critical
High
Low
Medium



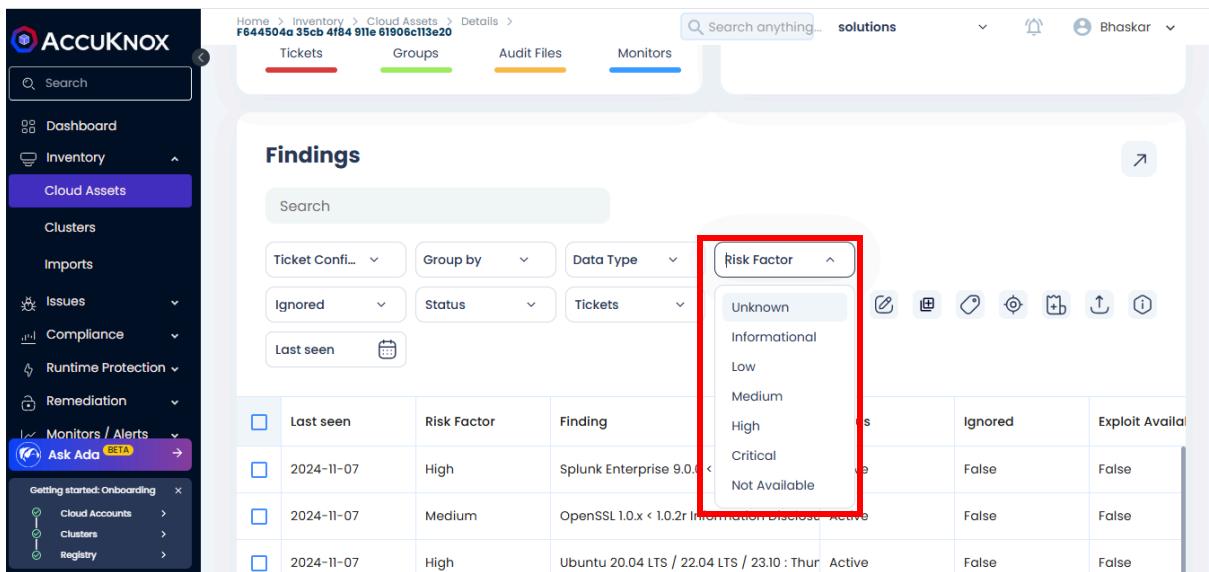
No data

Findings

Search

Ticket Confli... Group by Data Type Risk Factor

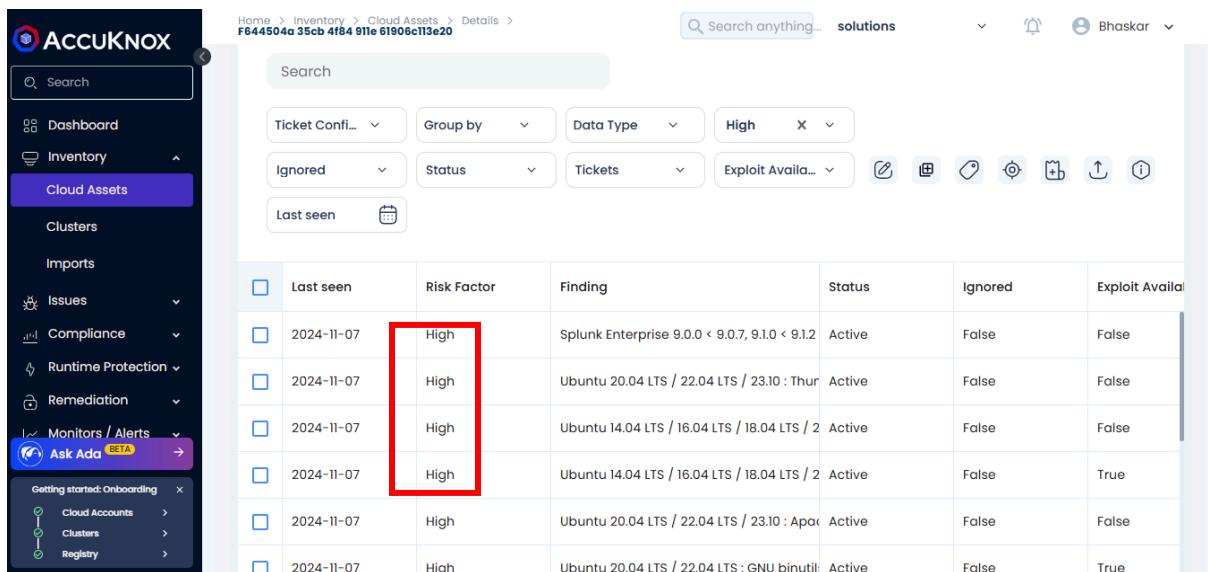
4. Navigate to the **Risk Factor** filter, and choose the severity level.



The screenshot shows the 'Findings' page in the ACCUKNOX interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Cloud Assets, and Monitors / Alerts. The 'Monitors / Alerts' option is currently selected. In the main area, there's a search bar and several filters: 'Ticket Config...', 'Group by', 'Data Type', 'Status', and 'Tickets'. A specific 'Risk Factor' filter is highlighted with a red box. This dropdown menu contains seven items: Unknown, Informational, Low, Medium, High, Critical, and Not Available. Below the filter is a table listing findings with columns for Last seen, Risk Factor, Finding, Status, Ignored, and Exploit Available. The first three rows have 'High' risk factor, while the last two have 'Medium'.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.x < 1.0.2r Information Disclosure	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False
2024-11-07	Medium	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	False
2024-11-07	High	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	True
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils	Active	False	True

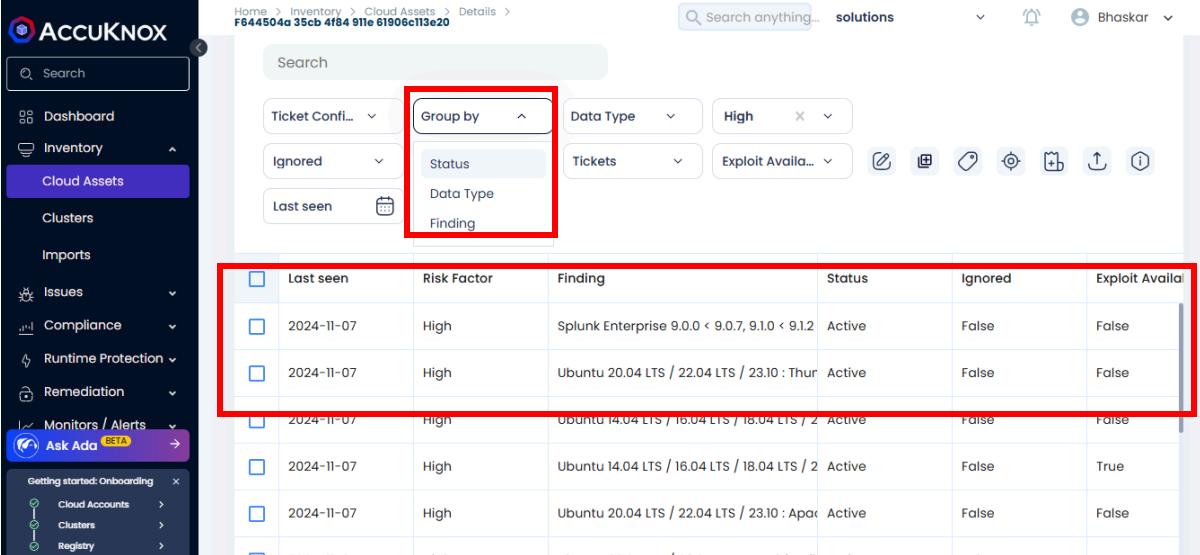
5. Now, you can find the findings as per the criticality level as shown below



This screenshot shows the same 'Findings' page as above, but with a different filter applied. The 'Risk Factor' dropdown now has 'High' selected, indicated by a red box. The table below shows six rows, each with a 'High' risk factor. The columns are identical to the previous table: Last seen, Risk Factor, Finding, Status, Ignored, and Exploit Available.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False
2024-11-07	High	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	False
2024-11-07	High	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	True
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils	Active	False	True

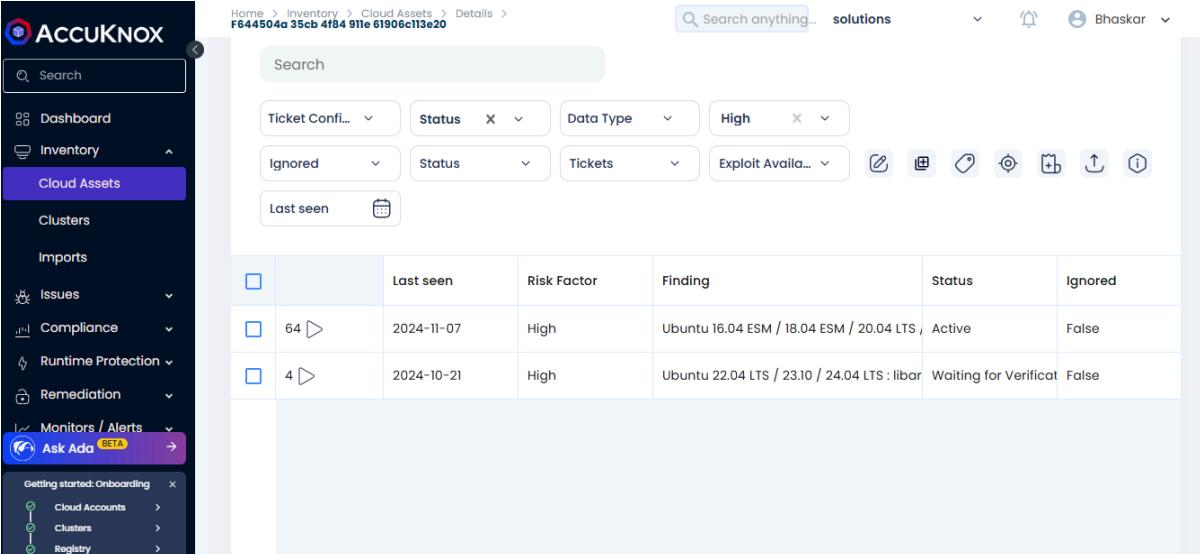
6. Navigate to the **Group by** filter, and choose **Status**.



The screenshot shows the ACCUKNOKX interface for managing cloud assets. On the left, there's a sidebar with navigation links like Dashboard, Inventory, Cloud Assets (which is selected and highlighted in purple), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Add (BETA). The main content area displays a table of findings. At the top of the table, there are several filter and search options: 'Ticket Confli...', 'Ignored', 'Last seen', 'Group by' (with dropdowns for 'Status', 'Tickets', 'Data Type', and 'Finding'), 'Data Type' (set to 'High'), and 'Exploit Availa...'. A red box highlights the 'Group by' section and the first few rows of the table. The table has columns for Last seen, Risk Factor, Finding, Status, Ignored, and Exploit Availa. The data in the table is as follows:

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Availa
2024-II-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2	Active	False	False
2024-II-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False
2024-II-07	High	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	False
2024-II-07	High	Ubuntu 14.04 LTS / 16.04 LTS / 18.04 LTS / 2	Active	False	True
2024-II-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Apache	Active	False	False
2024-II-07	High	Ubuntu 20.04 LTS / 22.04 LTS : GNU binutils	Active	False	True

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

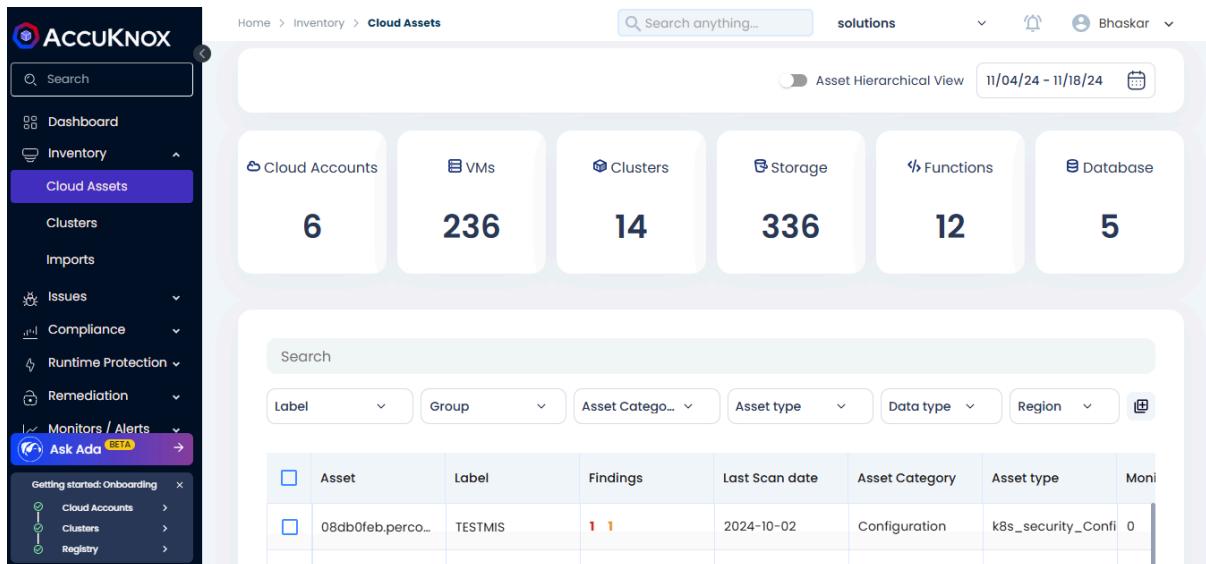


This screenshot shows the same interface as the previous one, but with different filter settings. The 'Group by' dropdown is now set to 'Status'. The table has columns for Last seen, Risk Factor, Finding, Status, and Ignored. The data in the table is as follows:

Last seen	Risk Factor	Finding	Status	Ignored
64 ▶	High	Ubuntu 16.04 ESM / 18.04 ESM / 20.04 LTS	Active	False
4 ▶	High	Ubuntu 22.04 LTS / 23.10 / 24.04 LTS : libcurl	Waiting for Verification	False

10.2.5 How to create a Ticket

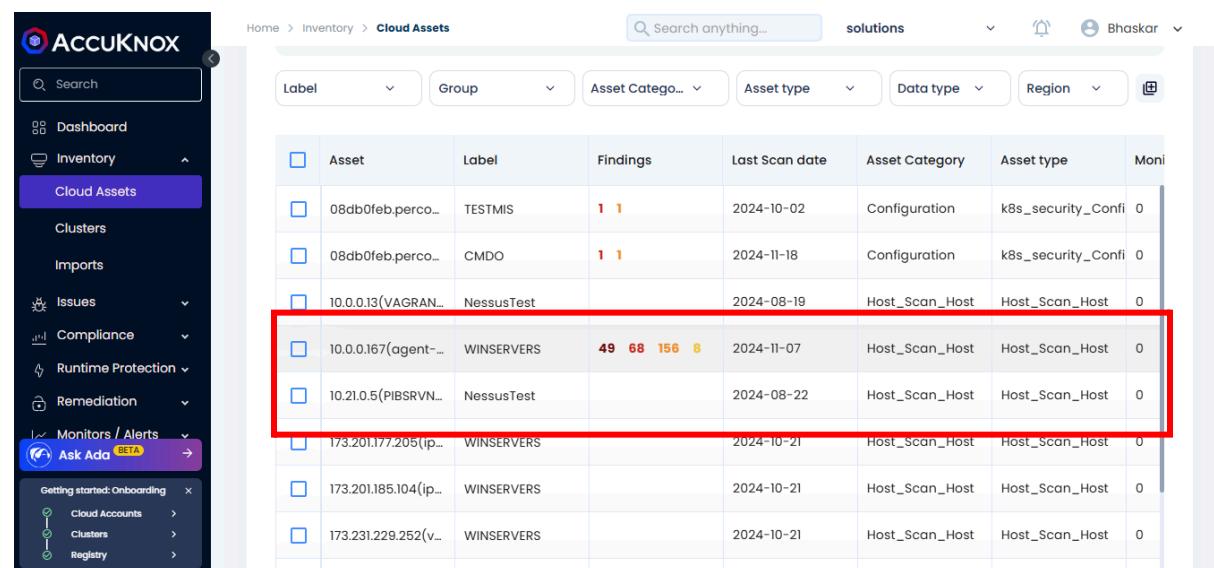
1. Go to Inventory tab, click on Cloud Assets section



The screenshot shows the ACCUKNOX interface with the 'Cloud Assets' section selected in the sidebar. The main area displays a summary dashboard with counts for various asset types. Below the dashboard is a search bar and a table listing assets. One asset row is highlighted.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0

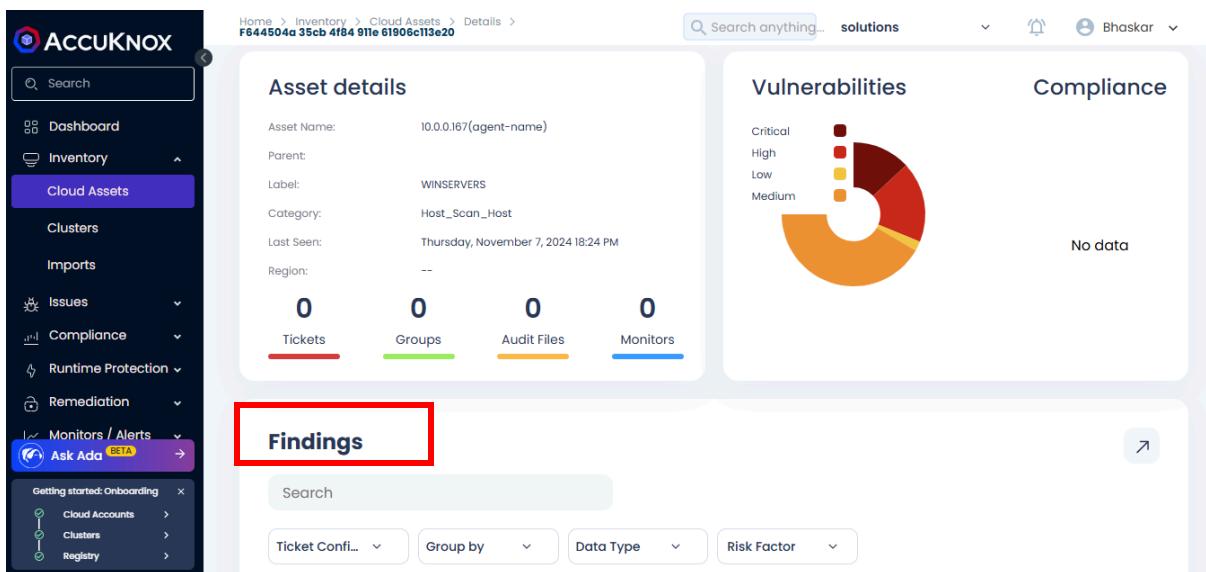
- a. Scroll down and click on the particular asset for which misconfiguration need to be viewed



The screenshot shows the ACCUKNOX interface with the 'Cloud Assets' section selected in the sidebar. The main area displays a list of assets. A specific asset row is highlighted with a red box, indicating it has been selected.

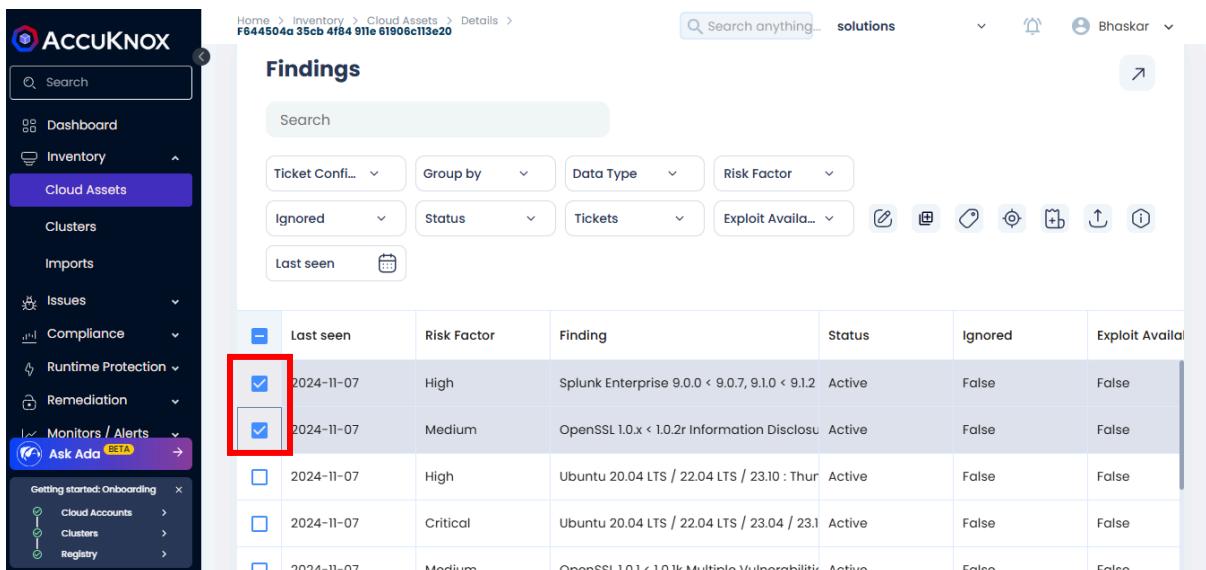
Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0
08db0feb.perco...	CMDO	1 1	2024-11-18	Configuration	k8s_security_Confi	0
10.0.0.13(VAGRAN...	NessusTest		2024-08-19	Host_Scan_Host	Host_Scan_Host	0
10.21.0.5(agent-...	WINSERVERS	49 68 156 8	2024-11-07	Host_Scan_Host	Host_Scan_Host	0
10.21.0.5(PIBSRVN...	NessusTest		2024-08-22	Host_Scan_Host	Host_Scan_Host	0
173.201.177.205(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.201.185.104(ip...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0
173.231.229.252(v...	WINSERVERS		2024-10-21	Host_Scan_Host	Host_Scan_Host	0

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



The screenshot shows the AccuKnox interface for an asset detail view. The left sidebar includes sections like Dashboard, Inventory, Cloud Assets (selected), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Ada. The main content area has tabs for Asset details, Vulnerabilities, and Compliance. The Asset details tab shows asset information such as Name: 10.0.0.167(agent-name), Parent: WINSERVERS, Label: Host_Scan_Host, Category: Host_Scan_Host, Last Seen: Thursday, November 7, 2024 18:24 PM, and Region: --. Below this are four zero-count metrics: Tickets (red), Groups (green), Audit Files (orange), and Monitors (blue). The Vulnerabilities tab features a pie chart showing the distribution of critical, high, low, and medium vulnerabilities. The Compliance tab indicates 'No data'. A prominent red box highlights the 'Findings' tab in the bottom navigation bar, which contains search and filter options (Ticket Config, Group by, Data Type, Risk Factor, Ignored, Status, Tickets, Exploit Available, Last seen).

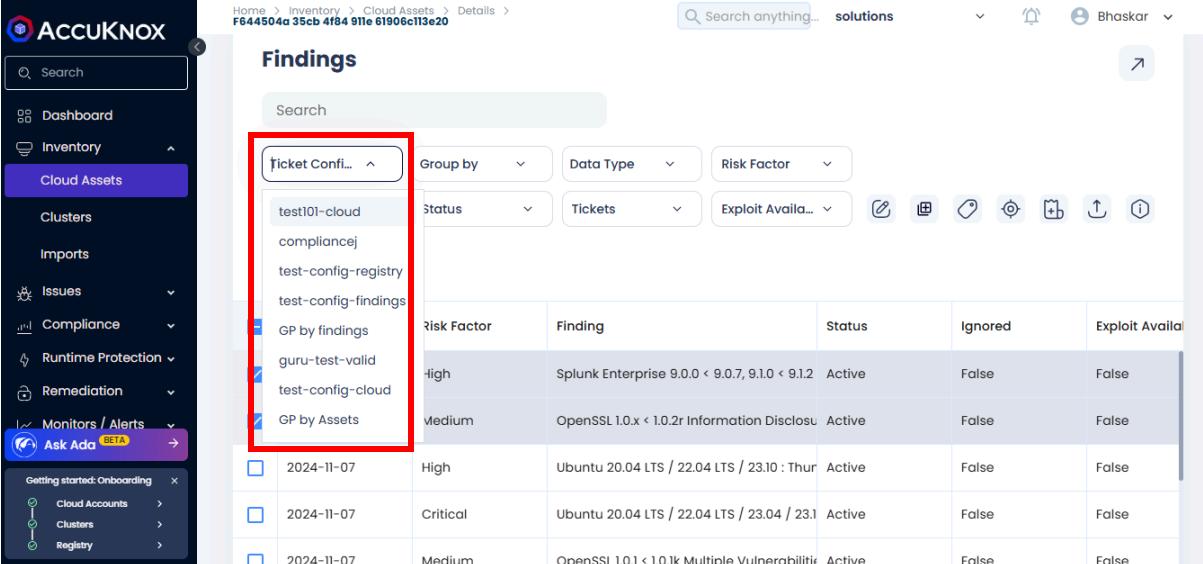
3. Select the check mark behind the ***Findings*** for which ticket needs to be created.



The screenshot shows the AccuKnox Findings page. The left sidebar is identical to the previous screenshot. The main content area displays a table of findings. The first two rows have a red box around them, indicating they are selected. The columns are Last seen, Risk Factor, Finding, Status, Ignored, and Exploit Available. The first finding is for Splunk Enterprise with a High risk factor, last seen on 2024-11-07. The second finding is for OpenSSL 1.0.x with a Medium risk factor, also last seen on 2024-11-07. Both findings are currently Active and Ignored, with False values in the respective columns.

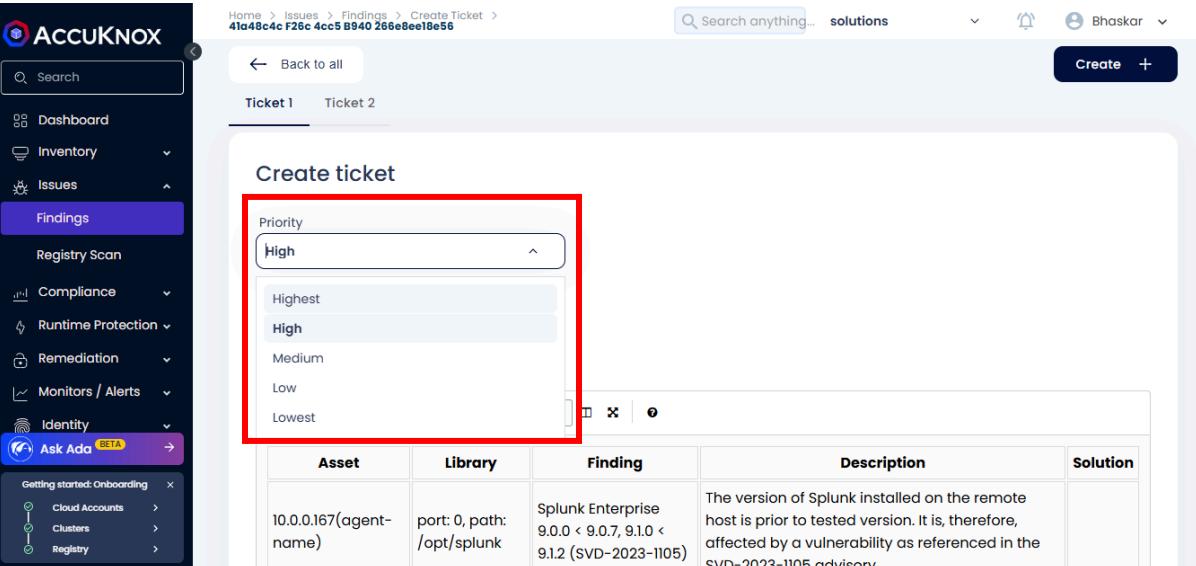
Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.x < 1.0.2r Information Disclosure	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False
2024-11-07	Critical	Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.1	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabiliti	Active	False	False

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



The screenshot shows the AccuKnox interface with the 'Cloud Assets' section selected in the sidebar. The main area is titled 'Findings'. A dropdown menu labeled 'Ticket Config...' is open, listing several options: 'test101-cloud', 'compliancej', 'test-config-registry', 'test-config-findings', 'GP by findings', 'guru-test-valid', 'test-config-cloud', and 'GP by Assets'. The 'GP by Assets' option is highlighted with a red box.

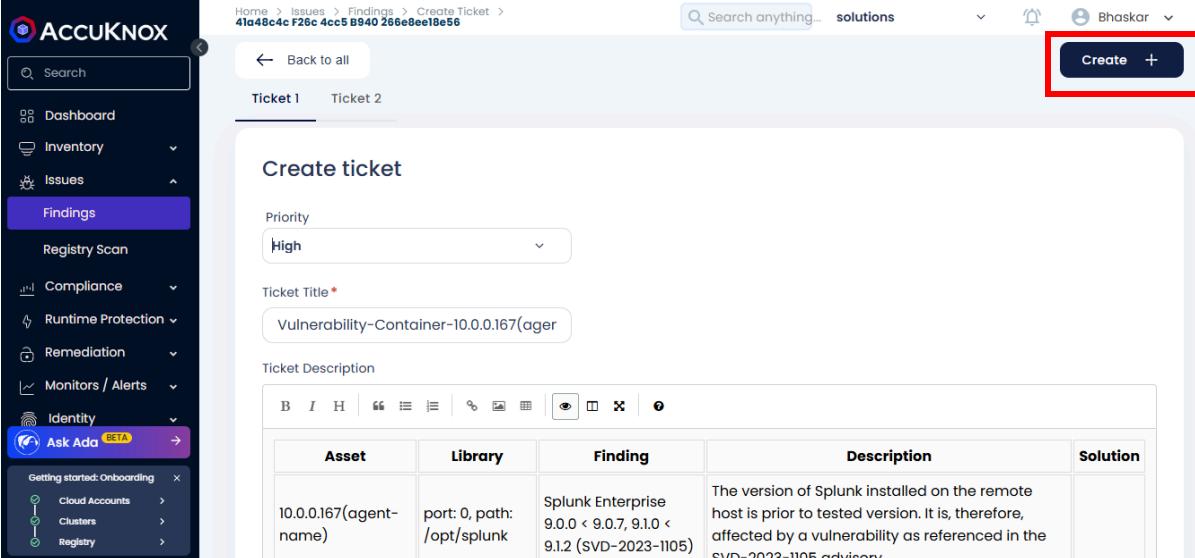
5. Choose the **Priority** from the dropdown.



The screenshot shows the 'Create ticket' page. In the top right corner, there is a 'Create +' button. The main form has two tabs: 'Ticket 1' and 'Ticket 2', with 'Ticket 1' currently active. The 'Priority' field is set to 'High' and is highlighted with a red box. Below it is a dropdown menu with five options: 'Highest', 'High', 'Medium', 'Low', and 'Lowest'. The bottom part of the screen shows a table with columns: Asset, Library, Finding, Description, and Solution. One row is visible, detailing a Splunk Enterprise version vulnerability.

Asset	Library	Finding	Description	Solution
10.0.0.167(agent-name)	port: 0, path: /opt/splunk	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2 (SVD-2023-1105)	The version of Splunk installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the SVD-2023-1105 advisory.	

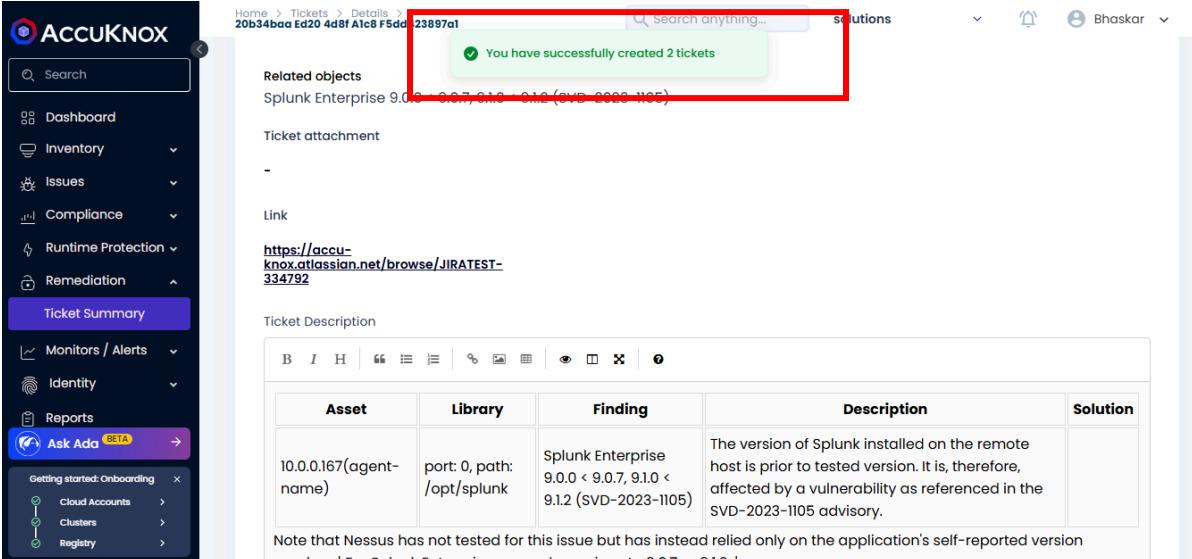
6. Edit the **Ticket Title** and **Ticket Description**, as required.



The screenshot shows the ACCUKNOX interface for creating a ticket. On the left is a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, and Ask Ada. The 'Findings' tab is selected. The main area shows a 'Create ticket' form with fields for Priority (set to High), Ticket Title (Vulnerability-Container-10.0.0.167(ager)), and a rich text editor for Ticket Description. A table below the editor lists an asset (10.0.0.167(agent-name)), library (port: 0, path: /opt/splunk), finding (Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2 (SVD-2023-1105)), description (The version of Splunk installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the SVD-2023-1105 advisory.), and solution (empty). At the top right of the main area is a 'Create +' button, which is highlighted with a red box.

- Click on the **Create** button at the top right corner.

You can see the tickets were created successfully.



The screenshot shows the 'Ticket Summary' section of the ACCUKNOX interface. The sidebar on the left includes 'Ticket Summary' under the 'Remediation' category. The main area displays a ticket detail page with a success message 'You have successfully created 2 tickets' (highlighted with a red box) and a table showing ticket details. The table has columns for Asset (10.0.0.167(agent-name)), Library (port: 0, path: /opt/splunk), Finding (Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2 (SVD-2023-1105)), Description (The version of Splunk installed on the remote host is prior to tested version. It is, therefore, affected by a vulnerability as referenced in the SVD-2023-1105 advisory.), and Solution (empty).

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

Home > Tickets

Search anything... solutions ▾

Tickets by status

Total Tickets **1.4k**



Priority	Count
Highest	1.2k
High	173
Medium	7
Low	8
Lowest	0

Open Tickets by Priority

Open Tickets by Priority **1.4k**

Priority	Count	Percentage
Highest	1.2k	87%
High	173	12%
Medium	7	1%
Low	8	1%
Lowest	0	0%

Top 5 Tickets by Age

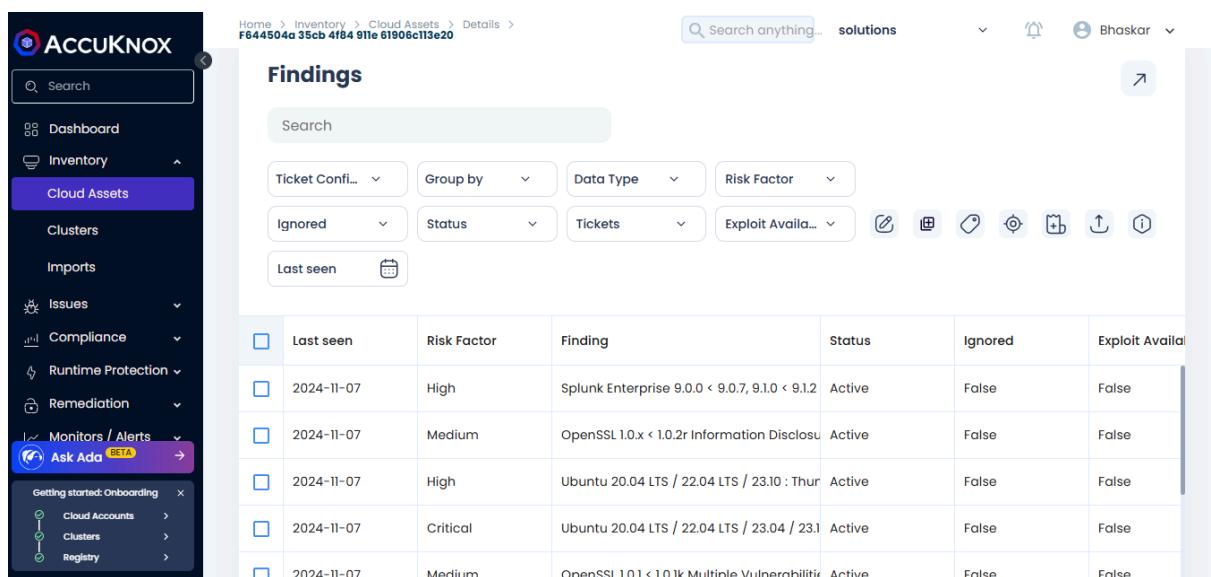
Ticket Number	Summary	Priority	Age
JIRATEST-225	Integer overflow in defineAttribute in xmiparse.c: (expat@2.4.1-r0)	▲	514 D
JIRATEST-226	Local users can trigger security-relevant memory corruption via mal...	▲	514 D
JIRATEST-195	systemd: buffer overrun in format_timespan() function: (libsystemd...	=	549 D
JIRATEST-203	kernel: null-ptr-deref caused by x25_disconnect: (linux-libc-dev@5...	=	537 D
JIRATEST-192	openssl: RSA authentication weakness: (libssl1.1@1.1.1n-0+debian1u4)	▼	550 D

10.3 Issues/Findings

10.3.1 Group findings by source and severity

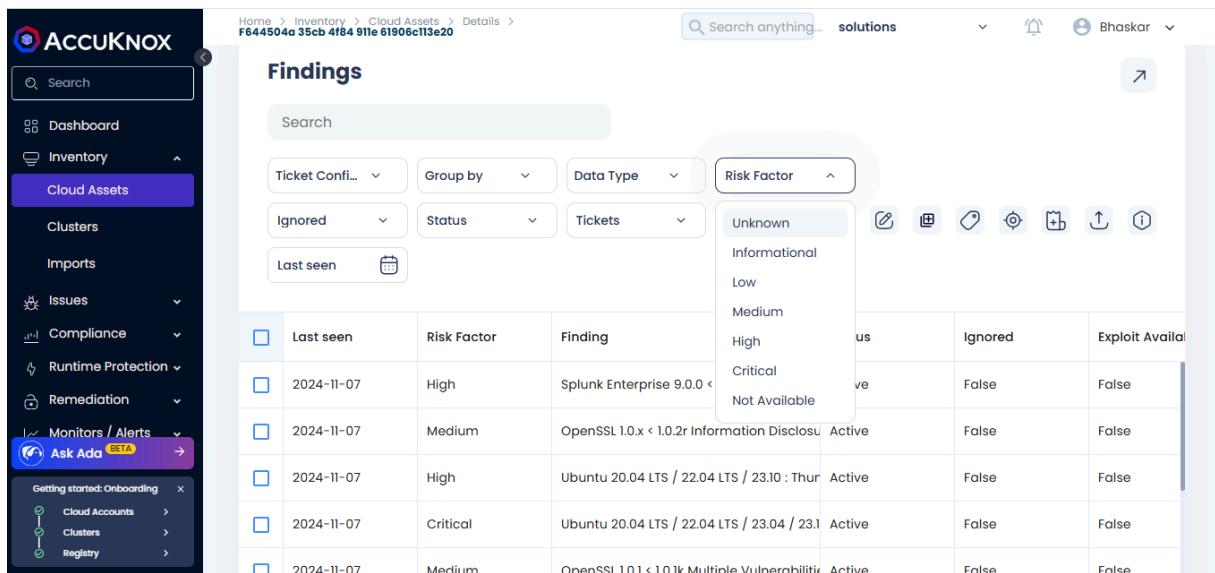
AccuKnox automatically scans assets with the help of various open-source tools. It uses tools like Clair, Trivy, CLOC, Fortify, Snyk, SonarQube, Cloudsploit, Kube Bench, and various other open-source tools for Scanning.

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



Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.7, 9.1.0 < 9.1.2	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.x < 1.0.2r Information Disclosure	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thur	Active	False	False
2024-11-07	Critical	Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.1	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilitie	Active	False	False

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

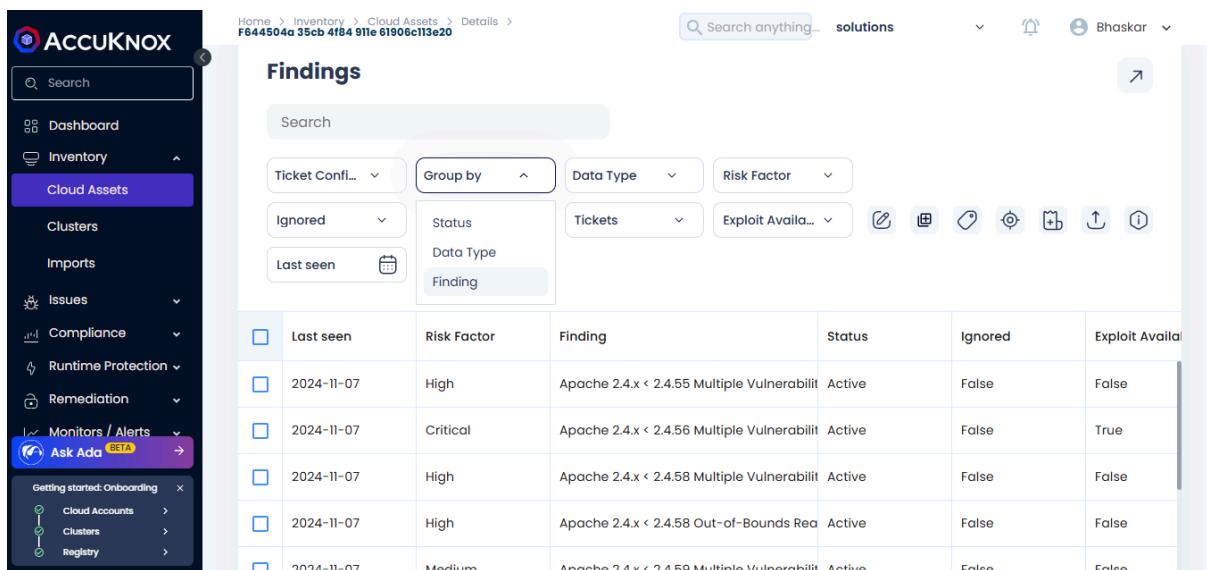


The screenshot shows the AccuKnox interface with the 'Cloud Assets' section selected in the sidebar. The main area displays a table of findings. A modal window is open over the table, specifically targeting the 'Risk Factor' column. The modal lists several risk levels: Unknown, Informational, Low, Medium, High, Critical, and Not Available. Each level has associated icons and a tooltip-like description below it.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Splunk Enterprise 9.0.0 < 9.0.1 Multiple Vulnerabilities	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.x < 1.0.2r Information Disclosure	Active	False	False
2024-11-07	High	Ubuntu 20.04 LTS / 22.04 LTS / 23.10 : Thursday, November 07, 2024	Active	False	False
2024-11-07	Critical	Ubuntu 20.04 LTS / 22.04 LTS / 23.04 / 23.10 : Thursday, November 07, 2024	Active	False	False
2024-11-07	Medium	OpenSSL 1.0.1 < 1.0.1k Multiple Vulnerabilities	Active	False	False

10.3.2 How to group by Findings and severity

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

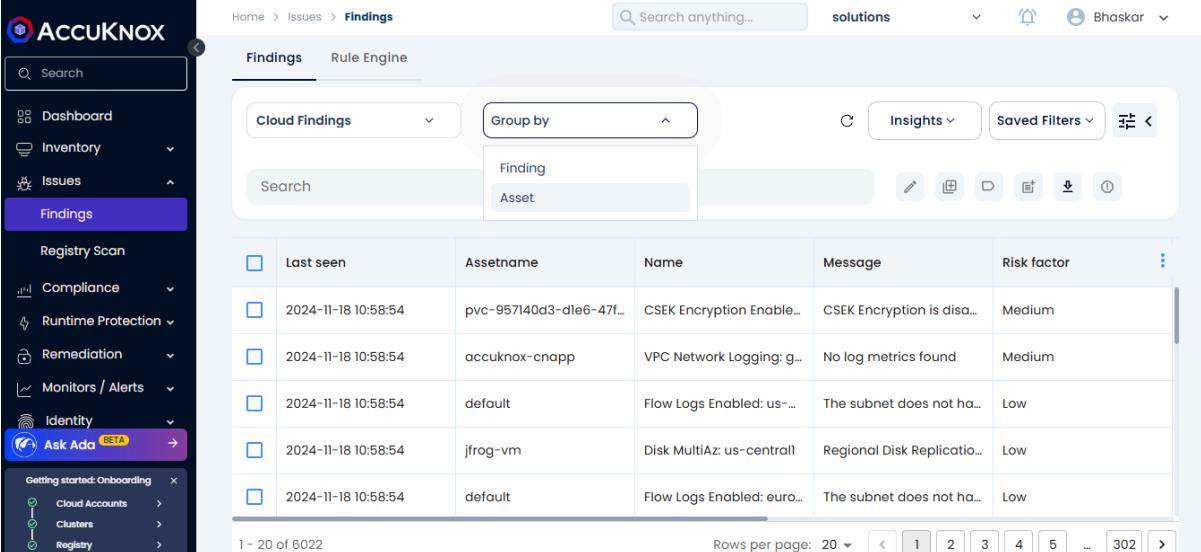


This screenshot is similar to the previous one but shows a different grouping option in the modal. Instead of 'Risk Factor', the 'Data Type' dropdown is selected. The modal lists 'Tickets' and 'Exploit Available' as the available data types.

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Available
2024-11-07	High	Apache 2.4.x < 2.4.55 Multiple Vulnerabilities	Active	False	False
2024-11-07	Critical	Apache 2.4.x < 2.4.56 Multiple Vulnerabilities	Active	False	True
2024-11-07	High	Apache 2.4.x < 2.4.58 Multiple Vulnerabilities	Active	False	False
2024-11-07	High	Apache 2.4.x < 2.4.58 Out-of-Bounds Read	Active	False	False
2024-11-07	Medium	Apache 2.4.x < 2.4.59 Multiple Vulnerabilities	Active	False	False

10.3.3 How to group by Asset and severity

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



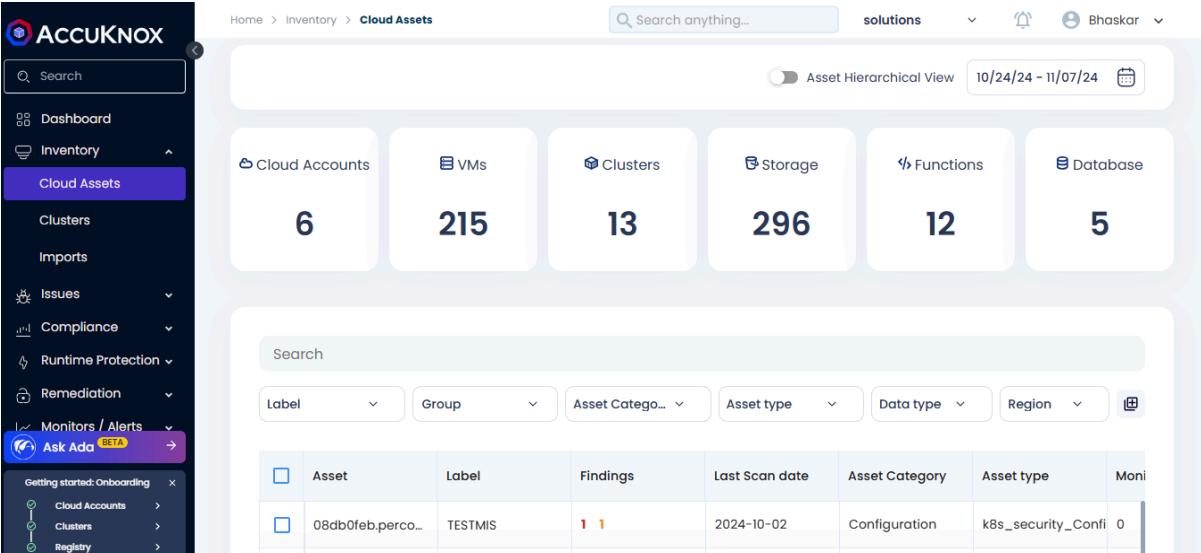
The screenshot shows the AccuKnox interface with the 'Findings' tab selected. The main area displays a table of findings, with the 'Group by' dropdown set to 'Asset'. The table includes columns for Last seen, Assetname, Name, Message, and Risk factor. The data shows various findings across different assets, such as pvc-957140d3-dle6-47f..., accuknox-cnapp, default, and jfrog-vm.

Last seen	Assetname	Name	Message	Risk factor
2024-11-18 10:58:54	pvc-957140d3-dle6-47f...	CSEK Encryption Enable...	CSEK Encryption is disa...	Medium
2024-11-18 10:58:54	accuknox-cnapp	VPC Network Logging: g...	No log metrics found	Medium
2024-11-18 10:58:54	default	Flow Logs Enabled: us-...	The subnet does not ha...	Low
2024-11-18 10:58:54	jfrog-vm	Disk MultiAz: us-centrall	Regional Disk Replicatio...	Low
2024-11-18 10:58:54	default	Flow Logs Enabled: euro...	The subnet does not ha...	Low

9.4 Asset Hierarchical View

In Accuknox Dashboard, under Inventory -> Cloud Assets, Asset Hierarchical View is present.

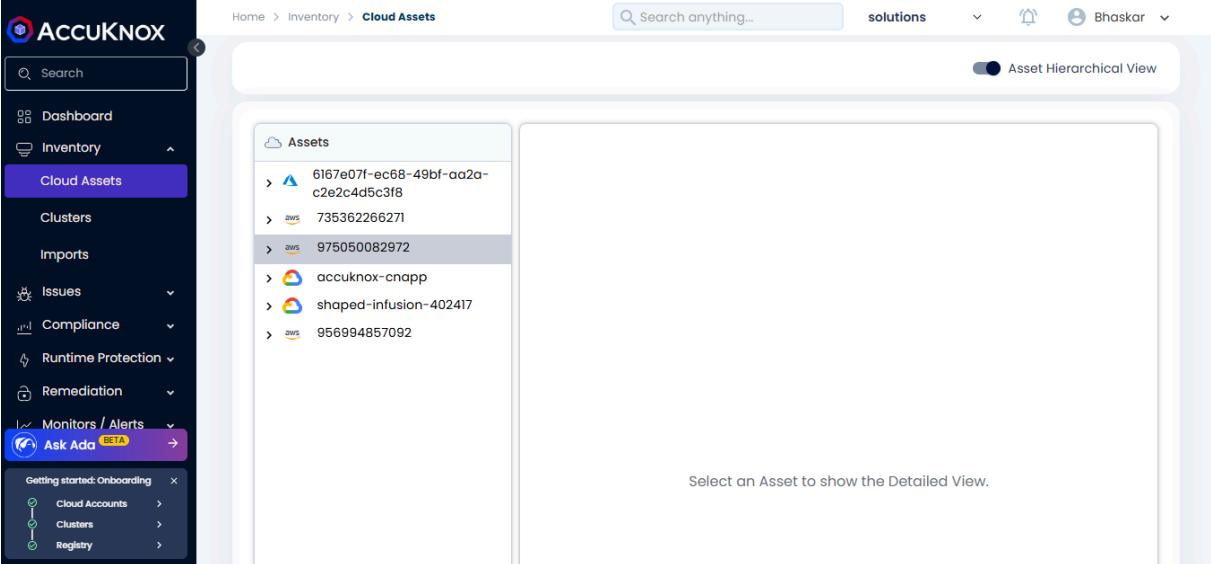
It shows the cloud assets in order.



The screenshot shows the AccuKnox interface with the 'Cloud Assets' tab selected. The top section displays a summary of asset counts: 6 Cloud Accounts, 215 VMs, 13 Clusters, 296 Storage, 12 Functions, and 5 Databases. Below this is a search bar and a table of findings. The table includes columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, and Moni. One row is visible, showing an asset labeled 'TESTMIS' with 1 finding, last scanned on 2024-10-02, and categorized as Configuration.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Moni
08db0feb.perco...	TESTMIS	1 1	2024-10-02	Configuration	k8s_security_Confi	0

Toggle Asset Hierarchical View by clicking on the trigger.



Home > Inventory > Cloud Assets

Search anything...

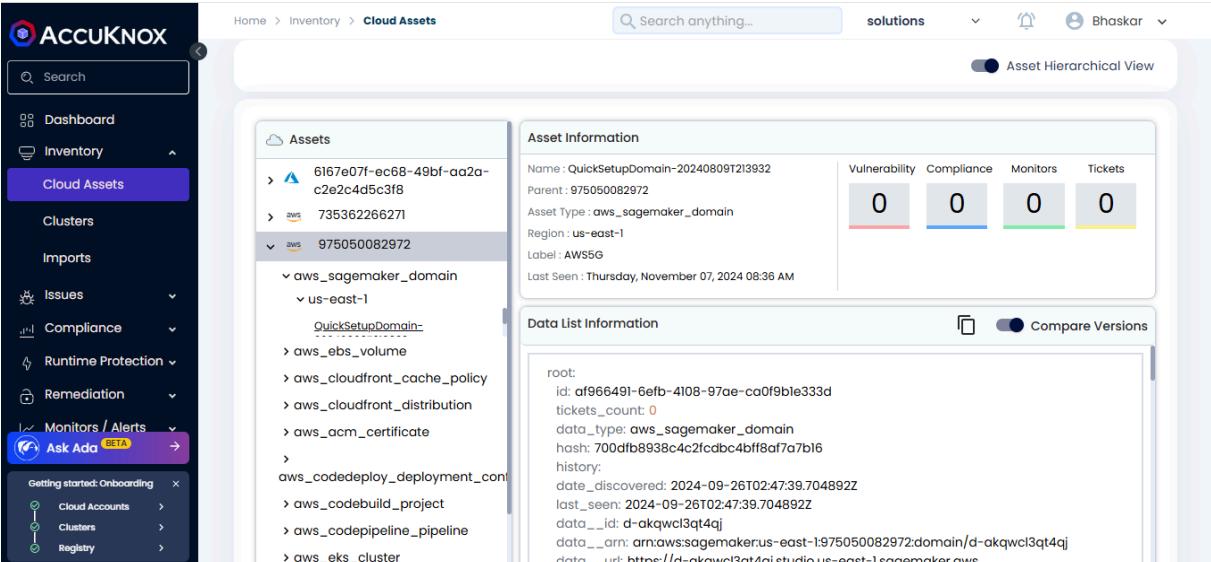
solutions Bhaskar Asset Hierarchical View

Assets

- 6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8
- aws 735362266271
- aws 975050082972
- accuknox-cnapp
- shaped-infusion-402417
- aws 956994857092

Select an Asset to show the Detailed View.

You can click on any of the cloud accounts to get more information about it.



Home > Inventory > Cloud Assets

Search anything...

solutions Bhaskar Asset Hierarchical View

Assets

- 6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8
- aws 735362266271
- aws 975050082972

aws_sagemaker_domain

Asset Information

Name : QuickSetupDomain-20240809T213932
 Parent: 975050082972
 Asset Type: aws_sagemaker_domain
 Region: us-east-1
 Label: AWS5G
 Last Seen: Thursday, November 07, 2024 08:36 AM

Vulnerability	Compliance	Monitors	Tickets
0	0	0	0

Data List Information

```

root:
  id: af966491-6efb-4108-97ae-ca0f9ble333d
  tickets_count: 0
  data_type: aws_sagemaker_domain
  hash: 700dfb8938c4c2fcdbc4bf8af7a7b16
  history:
    date_discovered: 2024-09-26T02:47:39.704892Z
    last_seen: 2024-09-26T02:47:39.704892Z
    data_id: d-akqwl3qt4qj
    data_arn: arn:aws:sagemaker:us-east-1:975050082972:domain/d-akqwl3qt4qj
    data_url: https://d-akqwl3qt4qj.studio.us-east-1.sagemaker.aws
  
```

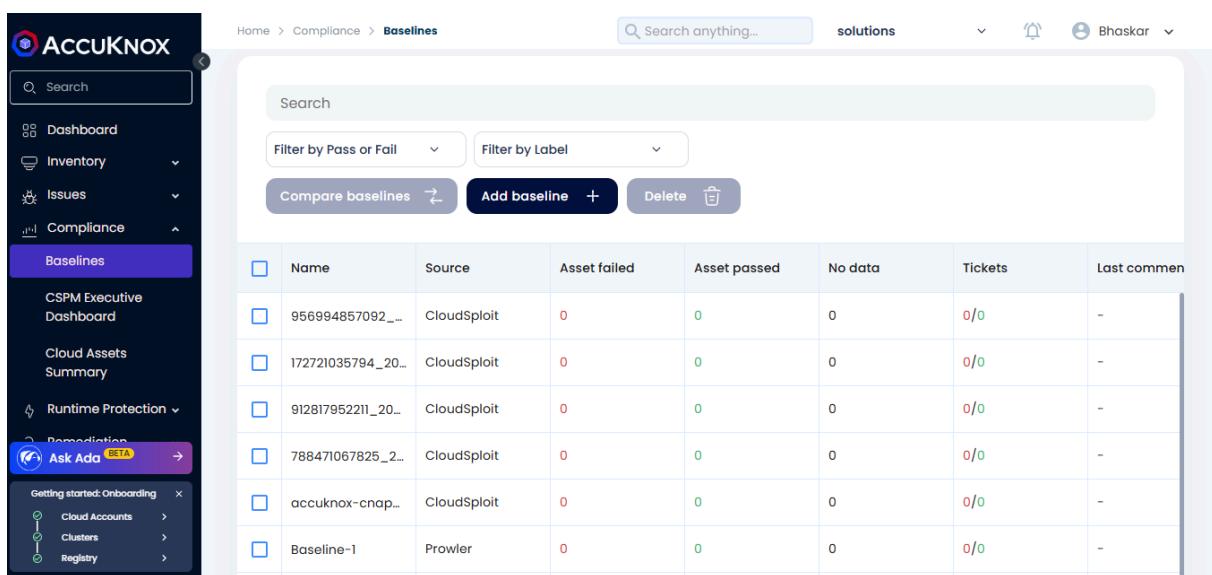
10.4 Baselines

10.4.1 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 can be associated with a specific 'asset' or 'group' of assets. It is a golden benchmark that is used to detect any change in compliance behavior proactively.

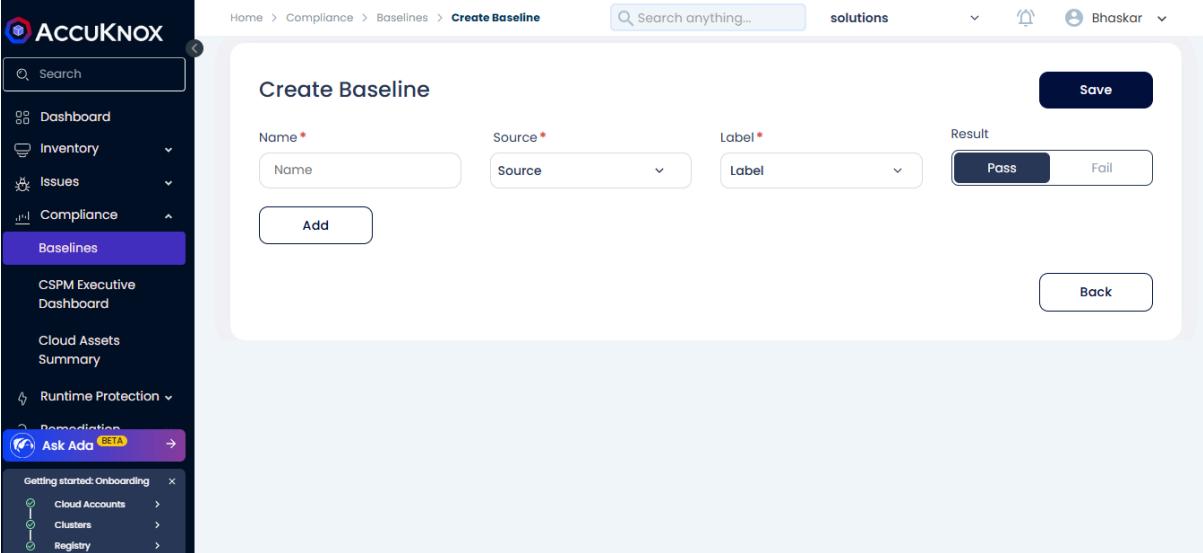
To create a baselines follow these steps:

Step 1: Head to the Baselines page under the Compliance section and click on "Add baseline".

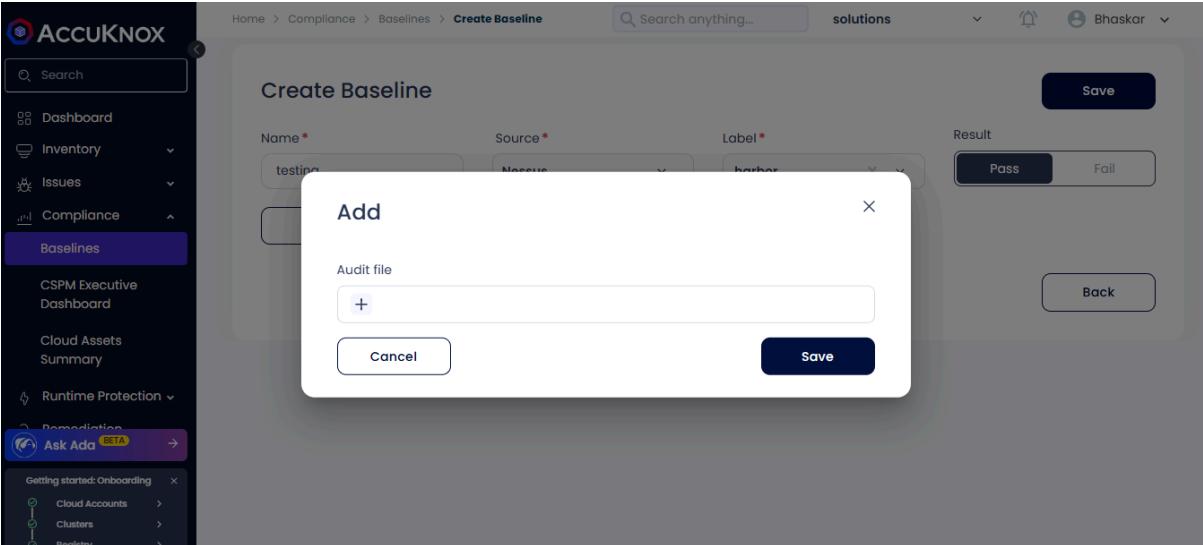


	Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
<input type="checkbox"/>	956994857092_...	CloudSploit	0	0	0	0/0	-
<input type="checkbox"/>	172721035794_20...	CloudSploit	0	0	0	0/0	-
<input type="checkbox"/>	912817952211_20...	CloudSploit	0	0	0	0/0	-
<input type="checkbox"/>	788471067825_2...	CloudSploit	0	0	0	0/0	-
<input type="checkbox"/>	accuknox-cnap...	CloudSploit	0	0	0	0/0	-
<input type="checkbox"/>	Baseline-1	Prowler	0	0	0	0/0	-

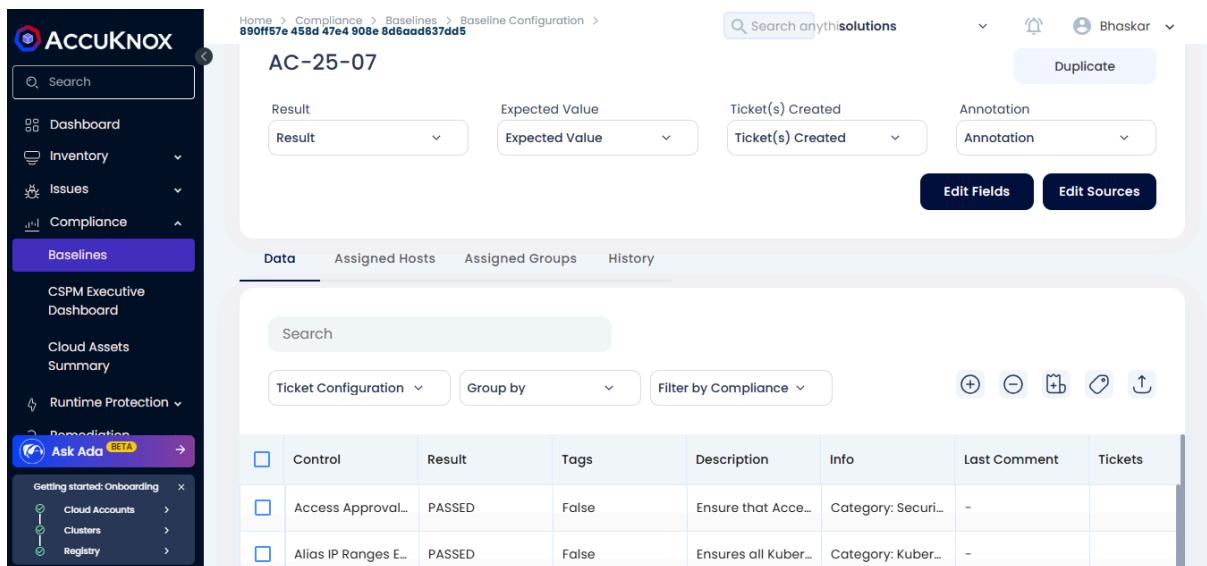
Step 2: Provide a name, select the source and select the Result for your baseline and add a label for your baseline.



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.

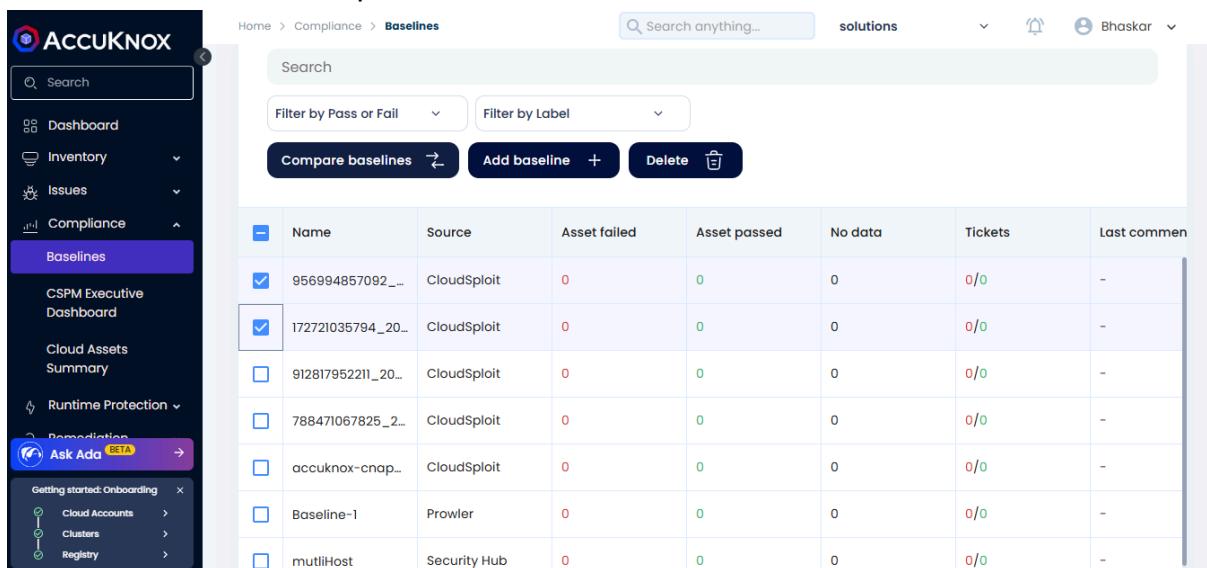


Control	Result	Tags	Description	Info	Last Comment	Tickets
<input type="checkbox"/> Access Approval...	PASSED	False	Ensure that Acce...	Category: Securi...	-	
<input type="checkbox"/> Alias IP Ranges E...	PASSED	False	Ensures all Kuber...	Category: Kuber...	-	

10.4.2 How to compare 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.



Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
956994857092_...	CloudSploit	0	0	0	0/0	-
172721035794_20...	CloudSploit	0	0	0	0/0	-
912817952211_20...	CloudSploit	0	0	0	0/0	-
788471067825_2...	CloudSploit	0	0	0	0/0	-
accuknox-cnap...	CloudSploit	0	0	0	0/0	-
Baseline-1	Prowler	0	0	0	0/0	-
multiHost	Security Hub	0	0	0	0/0	-

The comparison will look like following,

Compare

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

Total Count: undefined

10.5 Compliance

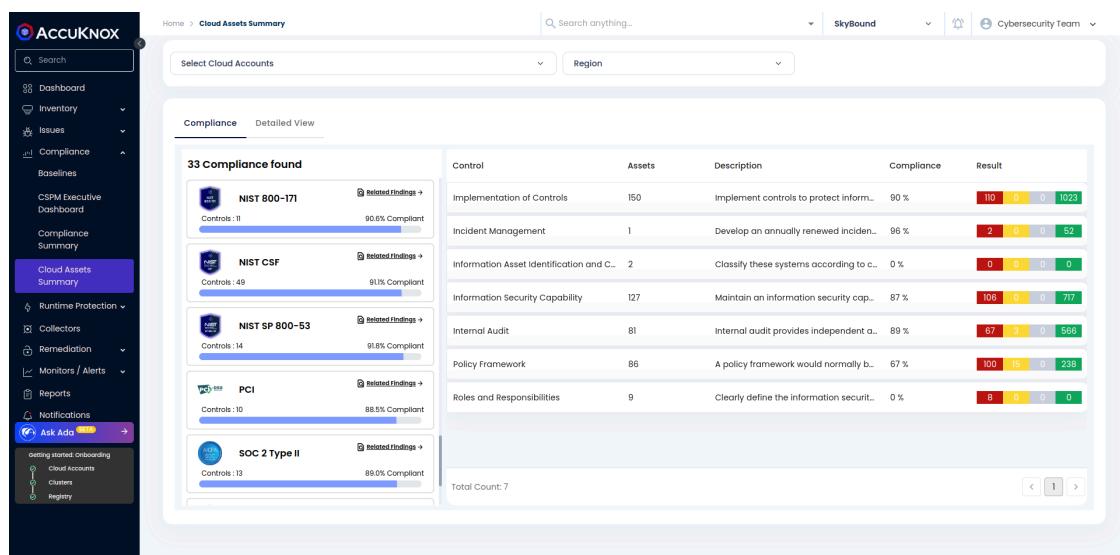
AccuKnox helps you to review your cloud infrastructure health and compliance posture. AccuKnox also helps you to generate reports that contain summary and detailed assessment of vulnerability/findings and compliance risks in your cloud infrastructure or in applications.

10.5.1 How to get Compliance for Cloud Assets

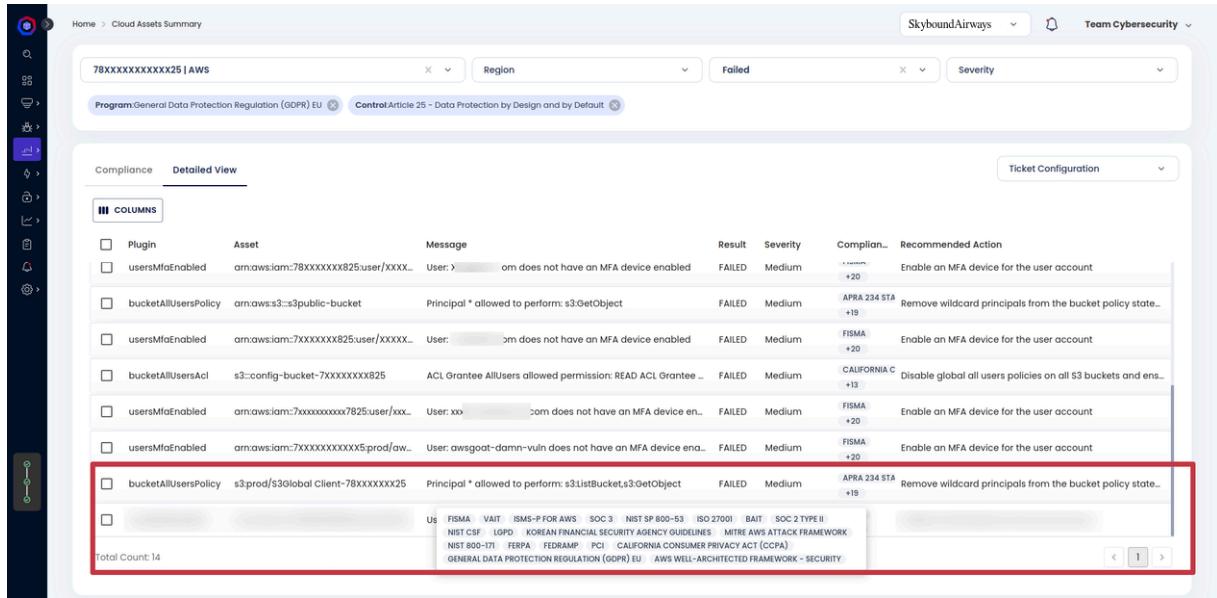
- In order to check for compliance Navigate to **Compliance > Cloud Asset Summary**

Users can click on any Compliance Program or their Sub-control which will navigate to the list of misconfiguration. Further user can filter based on Cloud Account, Region, Severity, Checks, and many more on the **Detailed View Tab**.

- Compliance:** A detailed report that gives you insight into how you score against a framework's requirements and rules.



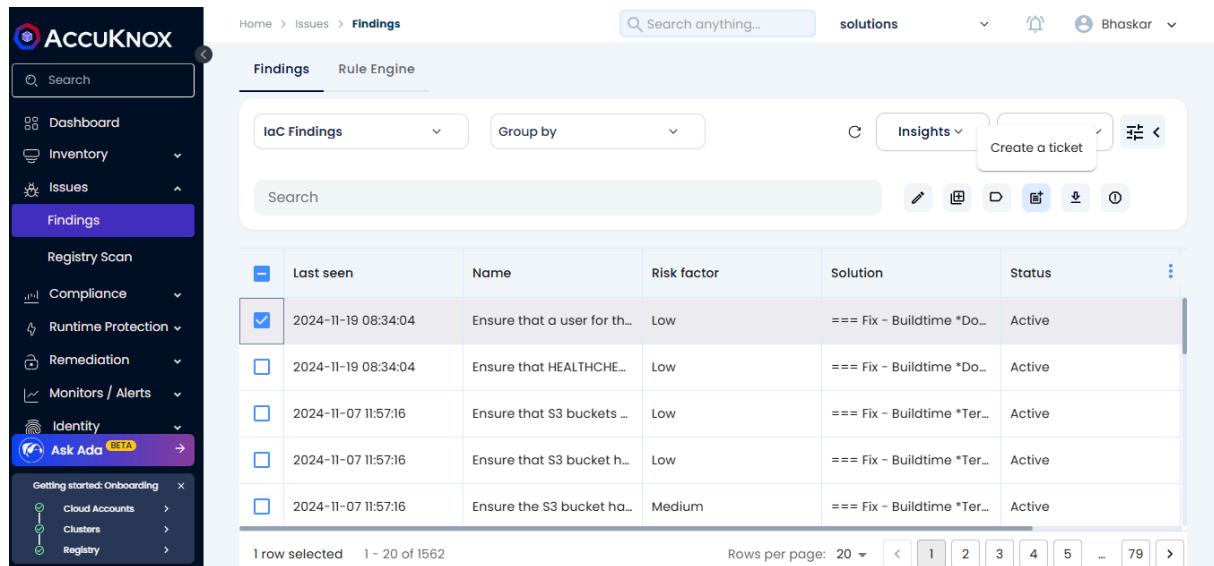
- **Detailed View:** A filtered view of the **Misconfigurations** page that shows resources with misconfigurations for the selected Compliance Program.



The screenshot shows the ACCUKNOX platform's Cloud Assets Summary feature. At the top, there are search filters for 'Region' (set to 'Failed'), 'Severity' (set to 'Medium'), and a dropdown for 'Team Cybersecurity'. Below the filters, a breadcrumb navigation shows 'Home > Cloud Assets Summary'. The main area displays a table titled 'Compliance' with a 'Detailed View' tab selected. The table has columns for 'Plugin', 'Asset', 'Message', 'Result', 'Severity', 'Compliance', and 'Recommended Action'. The 'Message' column contains detailed error descriptions. The 'Compliance' column includes links to various standards like FISMA, NIST SP 800-53, ISO 27001, and SOC 2. A red box highlights a specific row where the 'Asset' is 'bucketAllUsersPolicy' and the 'Message' is 'Principal * allowed to perform: s3:ListBucket,s3:GetObject'. The 'Recommended Action' for this row is 'Remove wildcard principals from the bucket policy state.' At the bottom of the table, it says 'Total Count: 14'.

10.6 Remediation - Fix Problems/Create Tickets

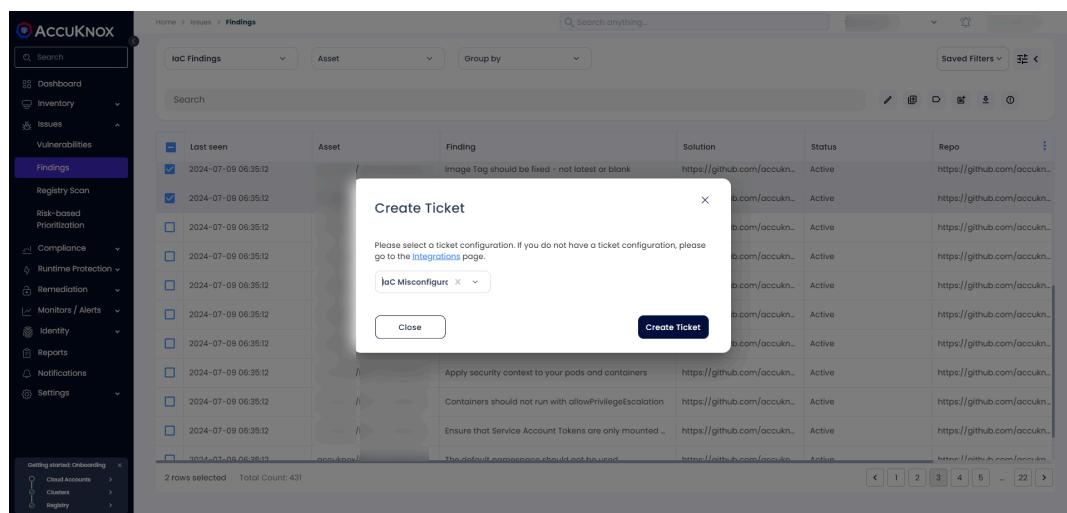
To remediate any findings, users will need to select the finding or group of findings From the Issues→ Findings page and click Create Ticket as shown in the below screenshot.



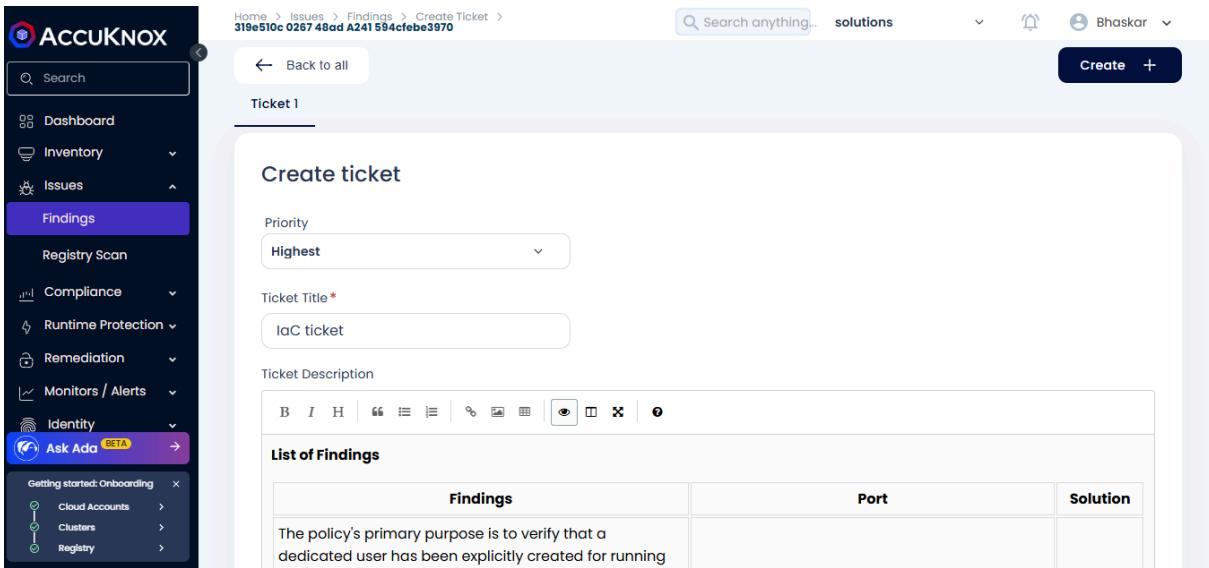
Last seen	Name	Risk factor	Solution	Status
2024-11-19 08:34:04	Ensure that a user for th...	Low	== Fix - Buildtime *Do...	Active
2024-11-19 08:34:04	Ensure that HEALTHCHE...	Low	== Fix - Buildtime *Do...	Active
2024-11-07 11:57:16	Ensure that S3 buckets ...	Low	== Fix - Buildtime *Ter...	Active
2024-11-07 11:57:16	Ensure that S3 bucket h...	Low	== Fix - Buildtime *Ter...	Active
2024-11-07 11:57:16	Ensure the S3 bucket ha...	Medium	== Fix - Buildtime *Ter...	Active

NOTE: Before this users must have integrated their Ticketing backend like Jira Servicenow or connects or Freshservice under Integrations → CSPM section. (Refer to ticketing integrations in Integrations section)

After clicking on the create ticket icon the next page will popup.



Once the user clicks on Create Ticket new page with all the information related to the IaC findings and with a predefined Priority based on the Risk Factor. The user has to click on Create to confirm the ticket creation.



Create ticket

Priority: Highest

Ticket Title: IaC ticket

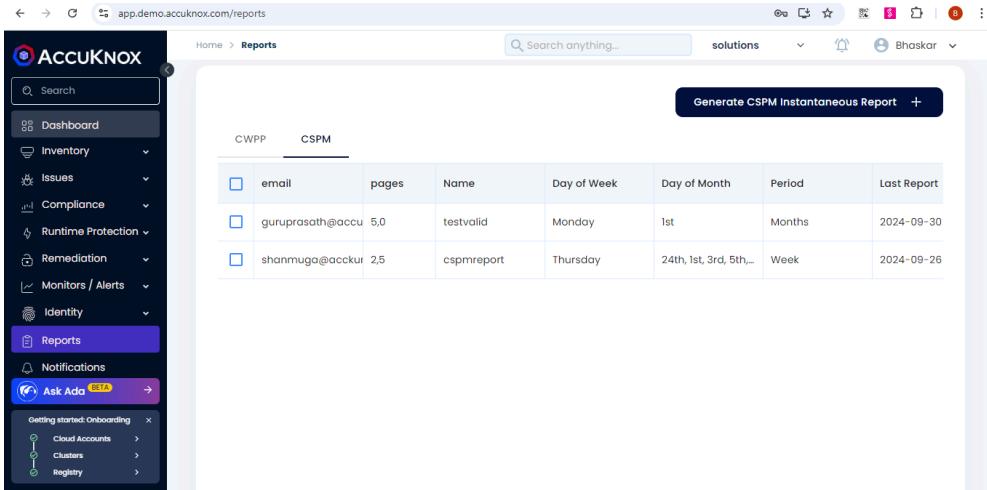
Ticket Description:

List of Findings

Findings	Port	Solution
The policy's primary purpose is to verify that a dedicated user has been explicitly created for running		

10.7 CSPM Reports

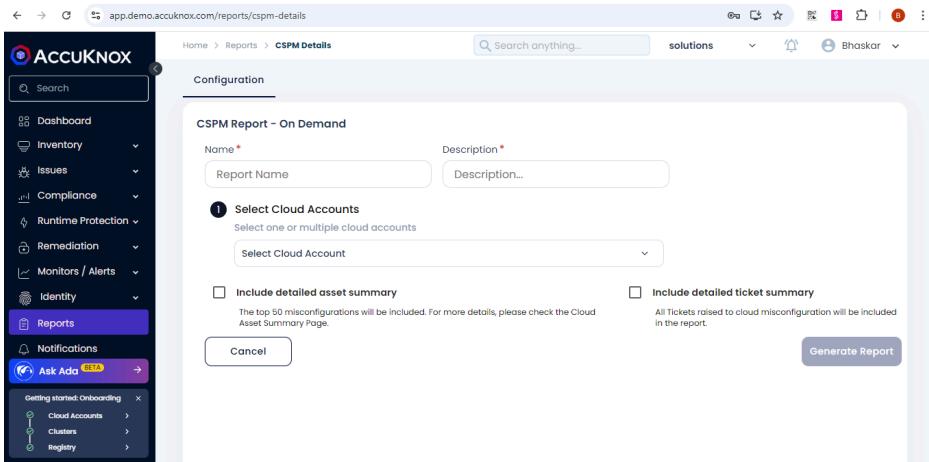
In the Accuknox dashboard, under Settings, go to Reports section, click on the “CSPM” tab, then click on “Generate CSPM Instantaneous Report”.



email	pages	Name	Day of Week	Day of Month	Period	Last Report
guruprasath@accu	5,0	testvalid	Monday	1st	Months	2024-09-30
shanmuga@acc kur	2,5	cspmreport	Thursday	24th, 1st, 3rd, 5th,...	Week	2024-09-26

Now, give the Name, Description and select the Cloud account.

Under the Cloud Account section, we can select multiple cloud accounts.



CSPM Report - On Demand

Name * Report Name

Description * Description...

Select Cloud Accounts
Select one or multiple cloud accounts
 Select Cloud Account

Include detailed asset summary
The top 50 misconfigurations will be included. For more details, please check the Cloud Asset Summary Page.

Include detailed ticket summary
All Tickets raised to cloud misconfiguration will be included in the report.

Cancel Generate Report

After selecting the cloud account, under the Compliance Program, select one of the two:

1. Compliance Report
2. Cloud Account Misconfiguration Report.

Compliance Report:

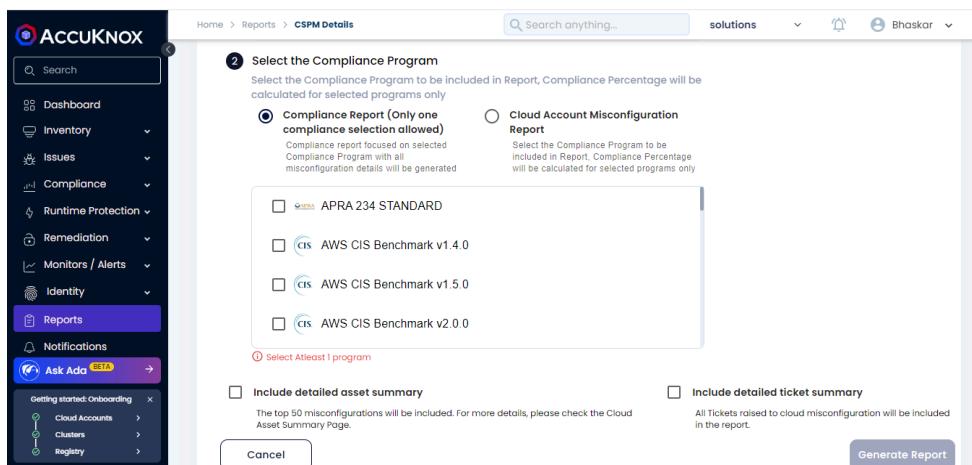
Allows selecting only a single compliance program. The report generated will be focused on the selected compliance program, it will show us all the misconfiguration details.

Cloud Account Misconfiguration Report:

Allows us in selecting more than one compliance program. In this report, the Compliance Percentage will be calculated for selected programs.

After filling the required details, click on “Generate Report”.

You can also select the checkboxes to include the detailed asset summary and detailed ticket summary.



Now we can see that the CSPM Report has been generated.

You can click on the Download icon to download it.

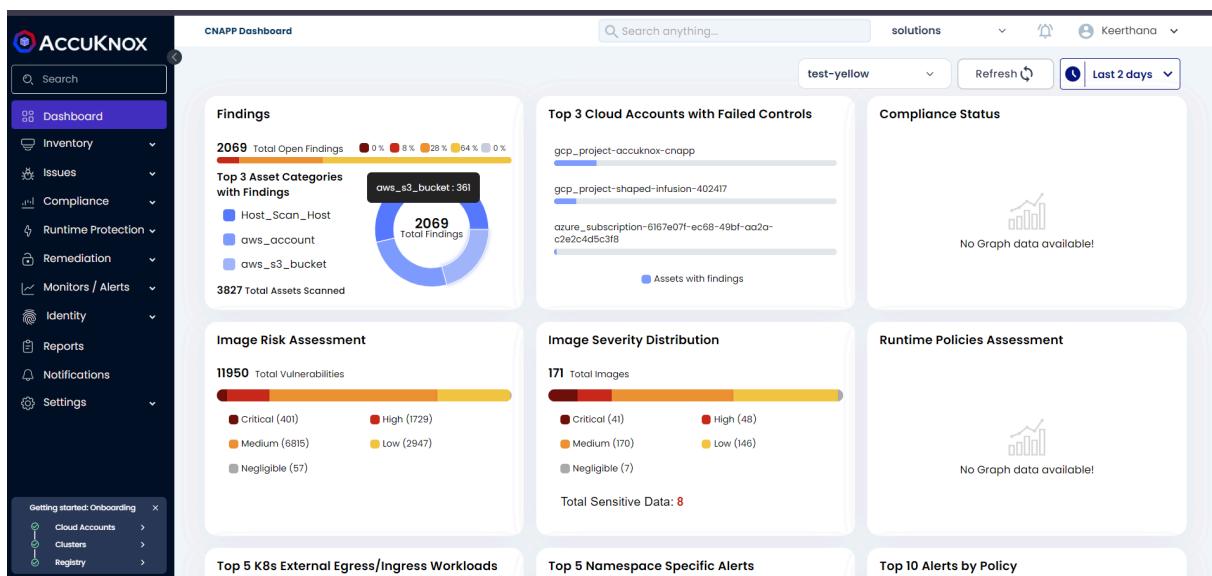
10.8 Rules Engine

The Rules Engine allows users to customize and automate ticket creation by selecting the data type, defining the criticality, and configuring specific ticket settings. This ensures that tickets are created based on the selected criteria, providing more control over the ticketing process.

Automated Ticket Creation using Rules Engine

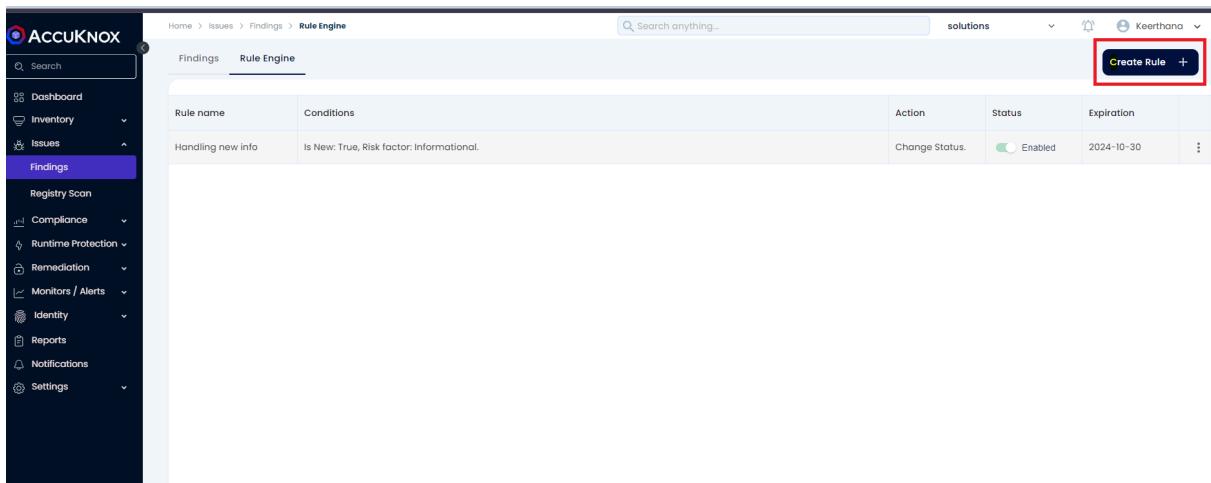
In this section we can find the steps to create a ticket using Rule Engine in the AccuKnox SaaS platform:

Step 1: Log in to app.demo.accuknox.com and navigate to the CNAPP dashboard.



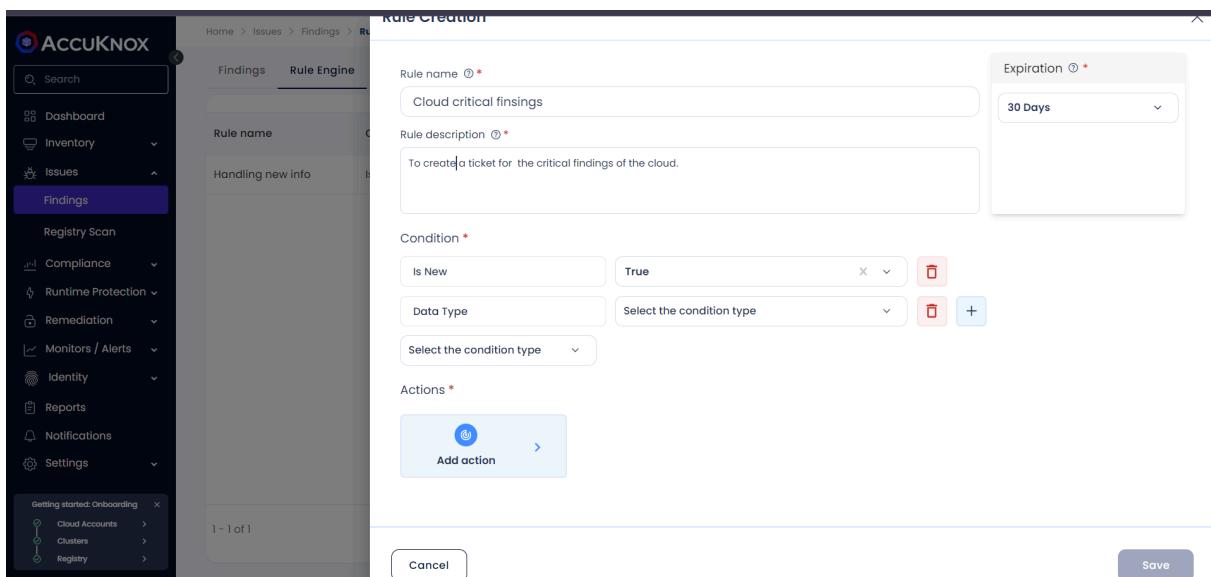
Step 2: Hover over to **Rule Engine** in Findings (Issues>Findings>Rule Engine)

Step 3: Click on **Create Rule** to create an automated rule.

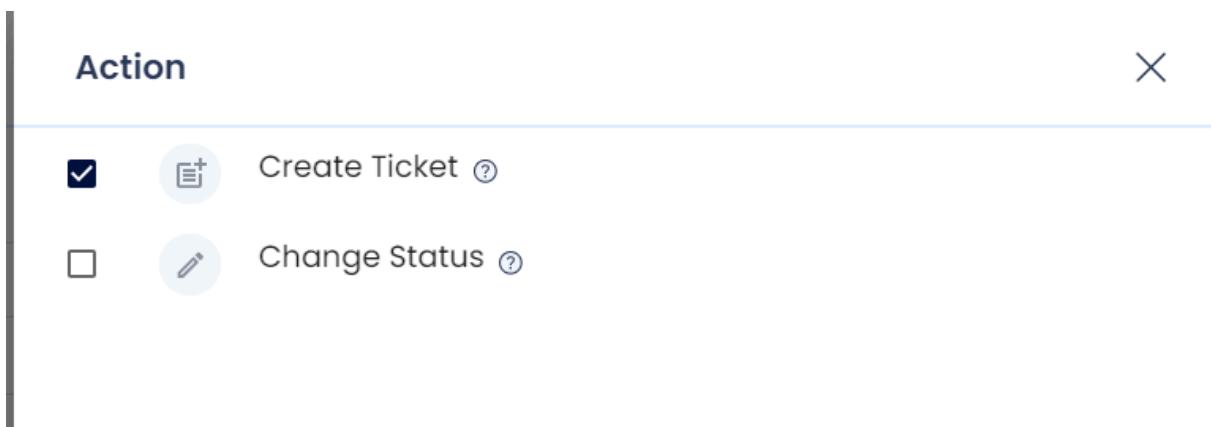


Step 4: Provide the necessary details, including the rule name, rule description, condition type (true or false), and click on "Action" to add the specific action.

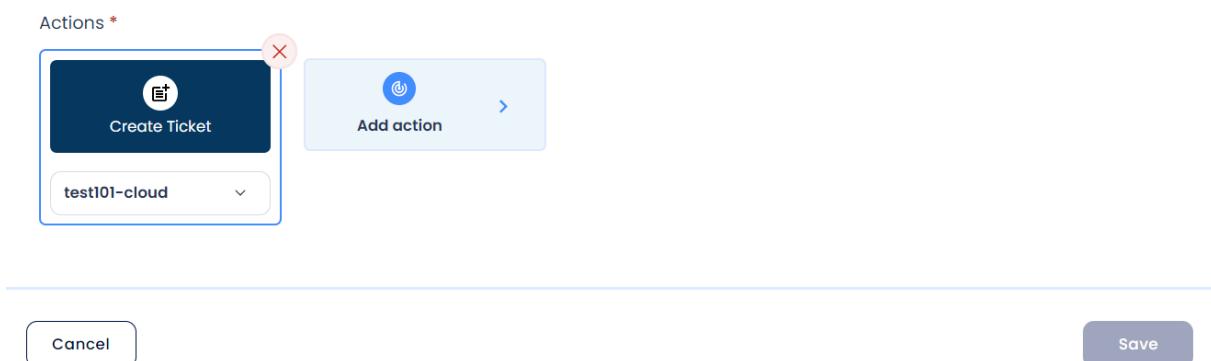
Clicking on the condition type will trigger the action that is required, it is crucial to select the condition type as per the rule created and the description of it.



Step 5: Click on **Create Ticket** to initiate creation of ticket when a finding with a matching the is found.



Step 6: After finalizing the condition, select the ticketing template from the drop down and save it to execute.



Step 7: Users need to create the ticketing configuration via Fresh Service Integration, which helps in automating the process of generating Freshservice “Problem alerts” with the existing security workflow.

11. ASPM (Application Security Posture Management)

This section makes use of Gitlab as an example to demonstrate the ASPM integrations with the CI/CD pipelines. In case a different platform is in use, please refer to the [help docs](#) for customized steps.

11.1 SAST

11.1.1 Integrating SonarQube SAST with AccuKnox in a GitLab CI/CD Pipeline

This guide demonstrates how to incorporate AccuKnox into a CI/CD pipeline using GitLab to enhance security. We'll use SonarQube SAST scanning to identify code vulnerabilities and send the results to AccuKnox for further analysis and remediation.

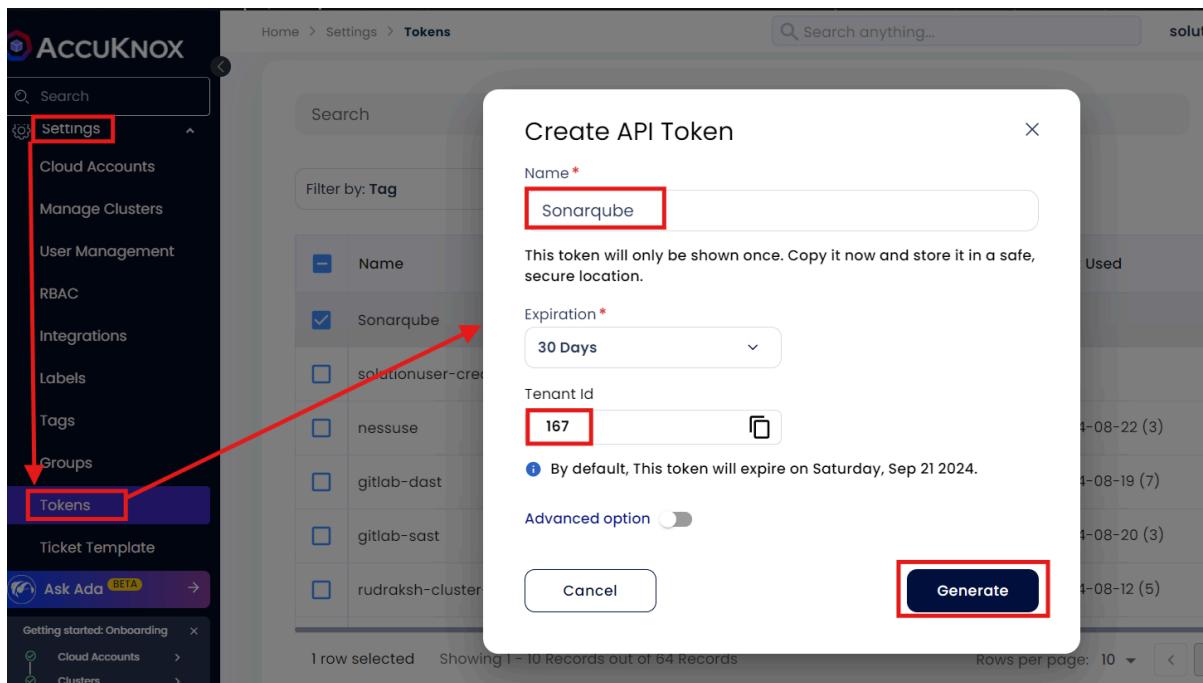
11.1.2 Pre-requisites

- **GitLab Access**
- **AccuKnox UI Access**
- **SonarQube Access**

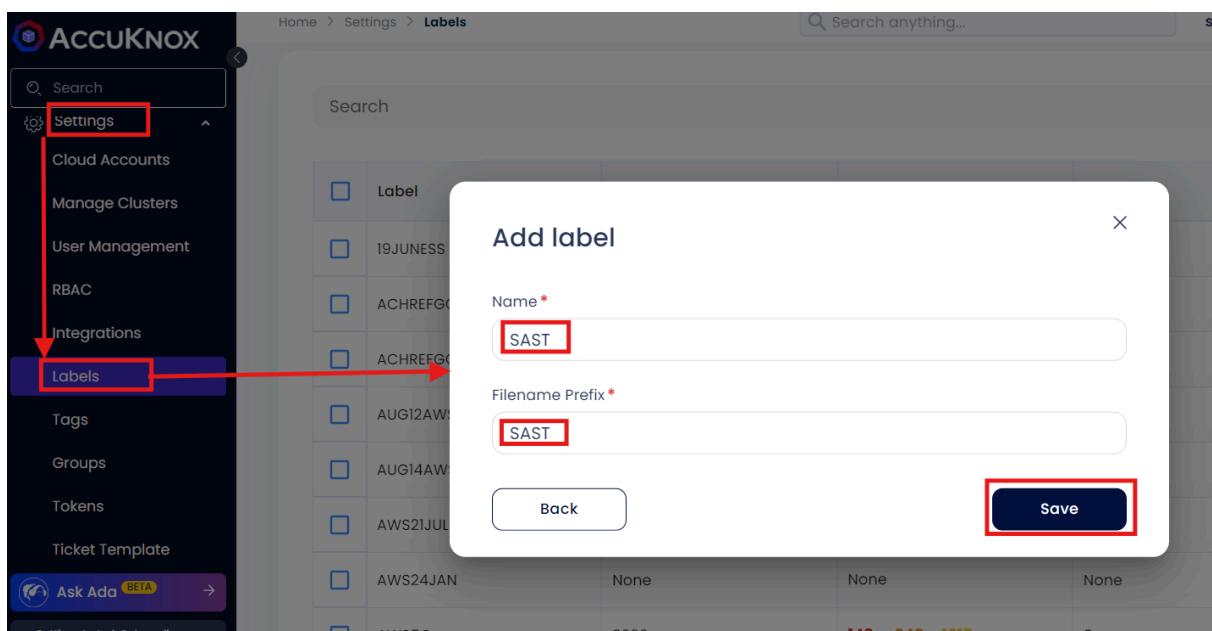
11.1.3 Steps for Integration

Step 1: Log in to AccuKnox

- Navigate to **Settings** and select **Tokens** to create an AccuKnox token for forwarding scan results to SaaS.

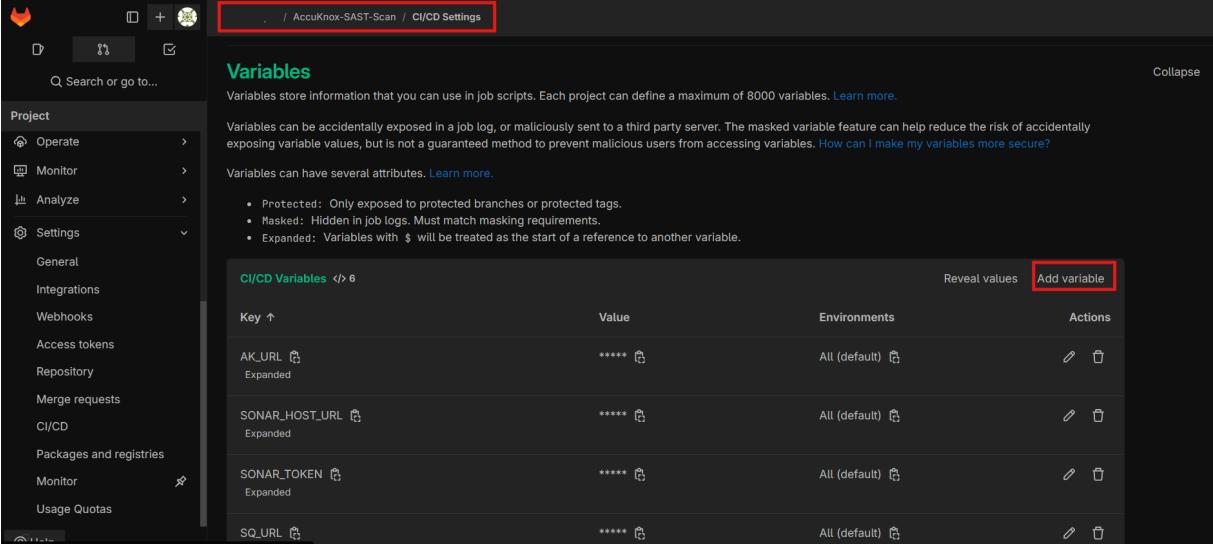


- Go to **AccuKnox > Settings > Labels** and create a label. This label will be used in the GitLab pipeline YAML file.



Step 2: Create GitLab CI/CD Variables

- Copy the AccuKnox token and create a GitLab CI/CD masked variable for it.
- Additionally, create variables for the **tenant ID**, **AccuKnox URL**, **SonarQube token**, and the **SonarQube project URL**.



The screenshot shows the GitLab interface with the path `/ AccuKnox-SAST-Scan / CI/CD Settings`. On the left, there's a sidebar with project settings like Operate, Monitor, Analyze, and Settings. The main area is titled "Variables" and contains information about their usage and security. It lists four CI/CD Variables:

Key ↑	Value	Environments	Actions
AK_URL	*****	All (default)	Edit Delete
SONAR_HOST_URL	*****	All (default)	Edit Delete
SONAR_TOKEN	*****	All (default)	Edit Delete
SQ_URL	*****	All (default)	Edit Delete

Step 3: Set Up GitLab CI/CD Pipeline

Create a new pipeline in your GitLab project with the following YAML configuration:

```

stages:
  - sonarqube-check
  - fetch-report
  - upload-report

sonarqube-check:
  stage: sonarqube-check
  image:
    name: sonarsource/sonar-scanner-cli:latest
    entrypoint: [""]
  variables:
    SONAR_USER_HOME: "${CI_PROJECT_DIR}/.sonar" # Defines the location of the
analysis task cache
    GIT_DEPTH: "0" # Ensures all branches are fetched, required by the analysis
  
```

```

task
cache:
  key: "${CI_JOB_NAME}"
  paths:
    - .sonar/cache
script:
  - sonar-scanner -Dsonar.qualitygate.wait=true || true
allow_failure: true
rules:
  - if: $CI_COMMIT_REF_NAME == 'main' || $CI_PIPELINE_SOURCE == 'merge_request_event'

fetch-report:
  stage: fetch-report
  image: docker:latest
  services:
    - docker:dind
  dependencies:
    - sonarqube-check
  script:
    - |
      docker run --rm \
        -e SQ_URL=$SQ_URL \
        -e SQ_AUTH_TOKEN=$SONAR_TOKEN \
        -e REPORT_PATH=/app/data/ \
        -e SQ_PROJECTS="^gitlab-sast-testing$" \
        -v $PWD:/app/data/ \
        accuknox/sastjob:latest
  artifacts:
    paths:
      - SQ-*.json
    expire_in: 1 hour # Optional: Set expiration time for artifacts

upload-report:
  stage: upload-report
  image: curlimages/curl:latest
  dependencies:
    - fetch-report
  script:
    - |
      for file in `ls -1 SQ-*.json`; do
        curl --location --request POST
        "<https://$AK_URL/api/v1/artifact/?tenant_id=$TENANT_ID&data_type=SQ&save_to_s3=false>" \
          --header "Tenant-Id: $TENANT_ID" \

```

```
--header "Authorization: Bearer $TOKEN" \
--form "file=@\"$file\""
done
```

11.1.4 Initial CI/CD Pipeline Without AccuKnox Scan

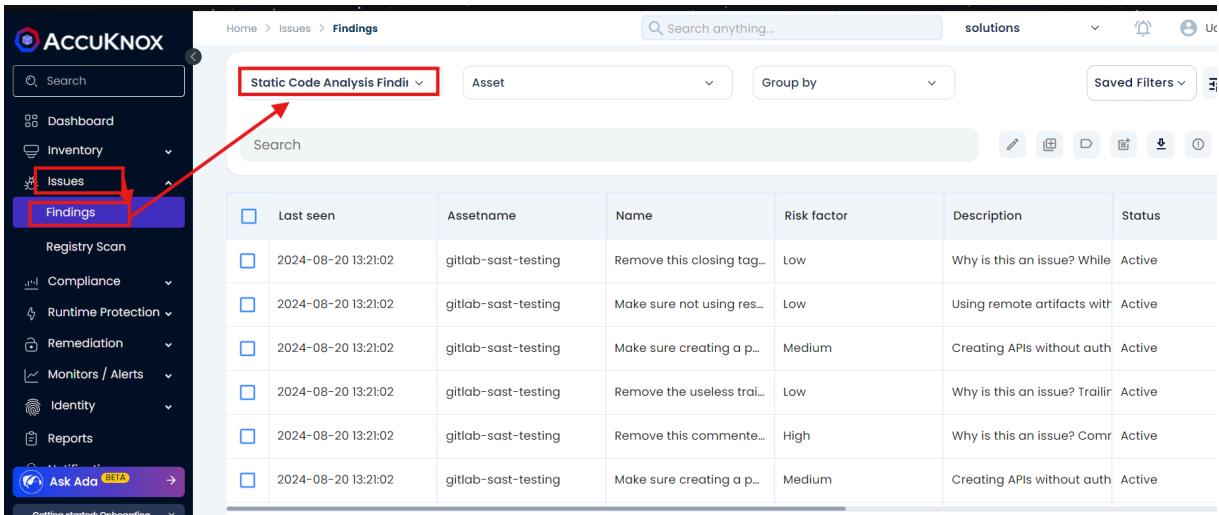
Initially, the CI/CD pipeline does not include the AccuKnox scan. Vulnerabilities in the code could go unnoticed without security checks.

11.1.5 CI/CD Pipeline After AccuKnox Integration

After integrating AccuKnox into the pipeline, pushing changes triggers the SonarQube scan, and results are sent to AccuKnox. AccuKnox helps identify potential code vulnerabilities.

11.1.6 View Results in AccuKnox SaaS

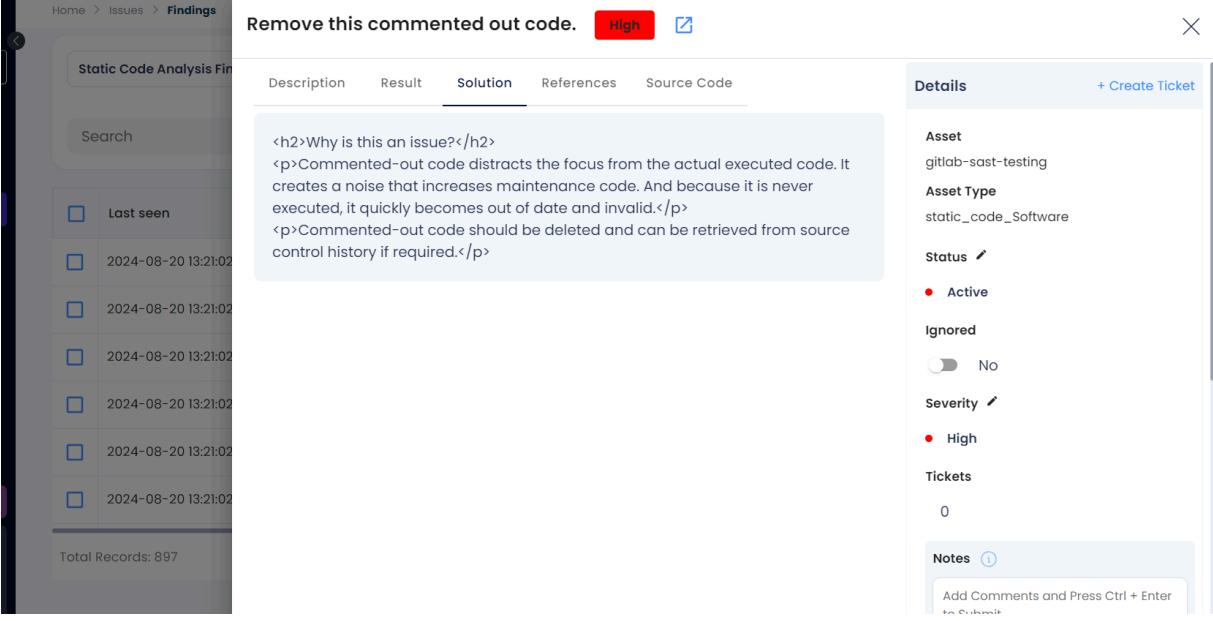
- Access the Dashboard:** After the pipeline completes, navigate to the AccuKnox SaaS dashboard.
- View Findings:** Go to **Issues > Findings** and select **SAST Findings** to see identified vulnerabilities



The screenshot shows the AccuKnox SaaS interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, and Reports. The 'Findings' option is highlighted with a red box and has a red arrow pointing to it. The main content area is titled 'Home > Issues > Findings'. It features a search bar and filters for 'Asset' and 'Group by'. Below is a table of findings:

Last seen	Assetname	Name	Risk factor	Description	Status
2024-08-20 13:21:02	gitlab-sast-testing	Remove this closing tag...	Low	Why is this an issue? While	Active
2024-08-20 13:21:02	gitlab-sast-testing	Make sure not using res...	Low	Using remote artifacts with	Active
2024-08-20 13:21:02	gitlab-sast-testing	Make sure creating a p...	Medium	Creating APIs without auth	Active
2024-08-20 13:21:02	gitlab-sast-testing	Remove the useless tra...	Low	Why is this an issue? Traili	Active
2024-08-20 13:21:02	gitlab-sast-testing	Remove this commente...	High	Why is this an issue? Comme	Active
2024-08-20 13:21:02	gitlab-sast-testing	Make sure creating a p...	Medium	Creating APIs without auth	Active

- Analyze and Fix Vulnerabilities:** Click on a vulnerability to view more details and follow the instructions in the **Solutions** tab.



Description: Remove this commented out code.

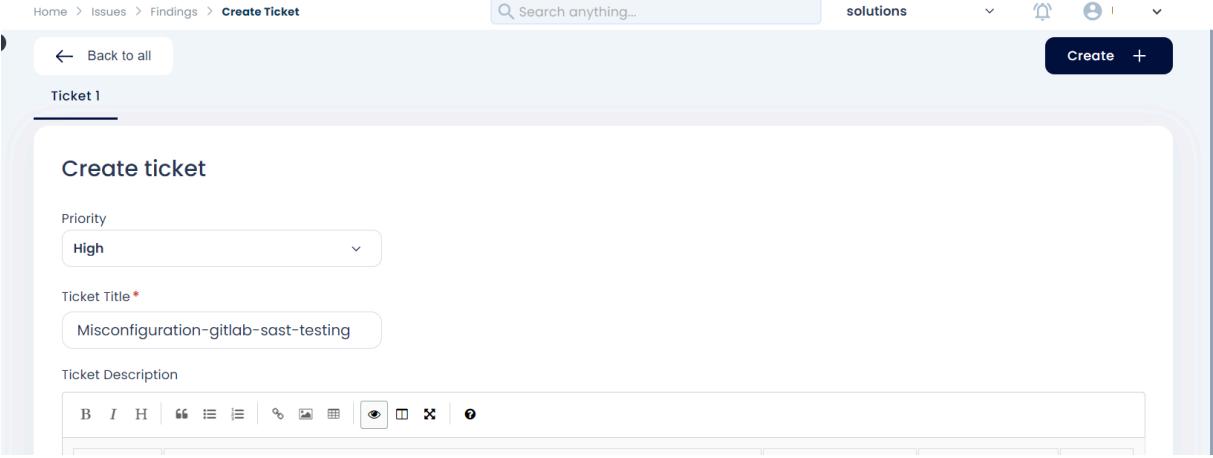
Result: High

Solution:

<h2>Why is this an issue?</h2>
 <p>Commented-out code distracts the focus from the actual executed code. It creates a noise that increases maintenance code. And because it is never executed, it quickly becomes out of date and invalid.</p>
 <p>Commented-out code should be deleted and can be retrieved from source control history if required.</p>

Asset: gitlab-sast-testing
Asset Type: static_code_Software
Status: Active
Severity: High
Tickets: 0

4. **Create a Ticket:** For unresolved vulnerabilities, create a ticket in your issue tracking system.



Ticket 1

Create ticket

Priority: High

Ticket Title *: Misconfiguration-gitlab-sast-testing

Ticket Description

5. **Re-run the Pipeline:** After fixing the vulnerabilities, rerun the GitLab CI/CD pipeline and verify that the issues have been resolved in the AccuKnox dashboard.

11.2 DAST

11.2.1 Gitlab DAST Scan

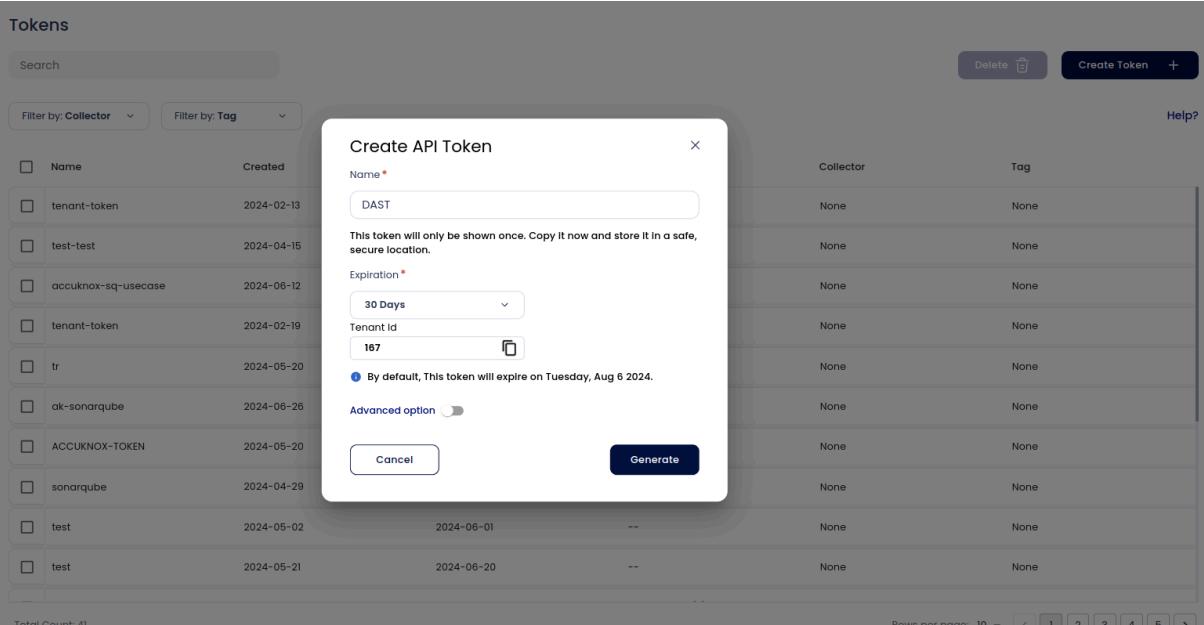
To demonstrate the benefits of incorporating AccuKnox into a CI/CD pipeline using GitLab to enhance security, consider a specific scenario involving a domain with known vulnerabilities. By integrating AccuKnox scanning into the pipeline, we can identify and resolve these security issues.

11.2.2 Pre-requisites

- GitLab Access
- AccuKnox UI access

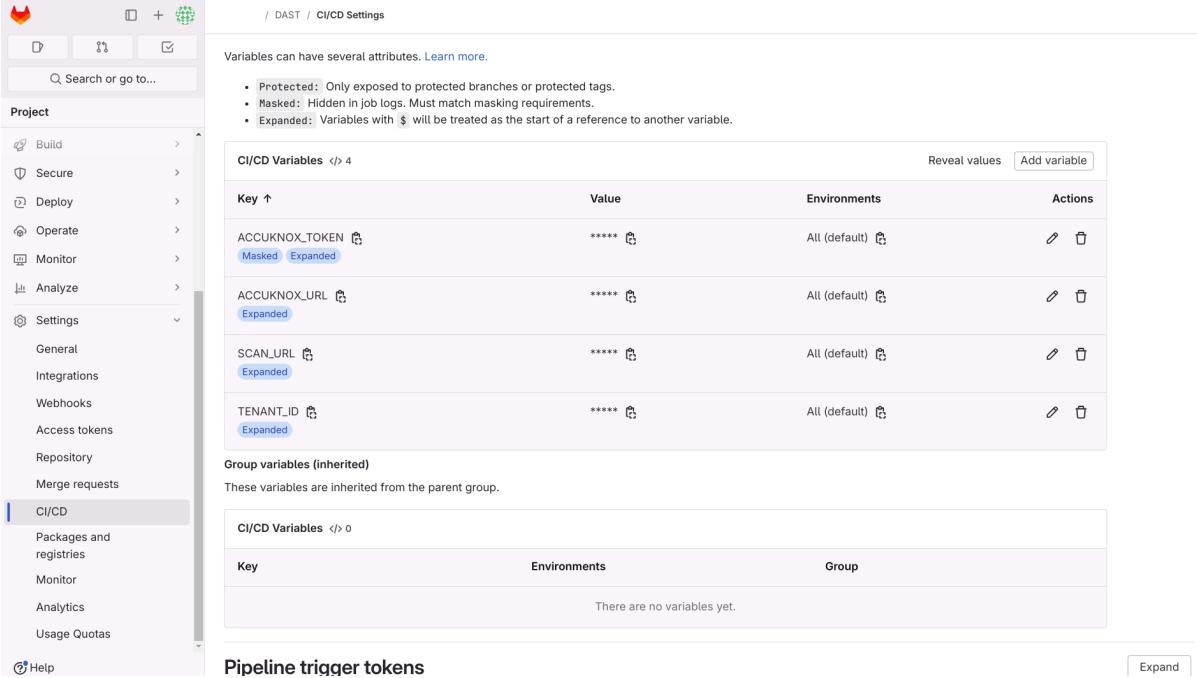
11.2.3 Steps for Integration

Step 1: Log in to AccuKnox Navigate to Settings and select Tokens to create an AccuKnox token for forwarding scan results to SaaS.



The screenshot shows the AccuKnox Tokens management interface. On the left, there is a list of existing tokens with columns for Name, Created, Collector, and Tag. A modal window titled 'Create API Token' is open in the center. It contains fields for 'Name' (set to 'DAST'), 'Expiration' (set to '30 Days'), and 'Tenant Id' (set to '167'). A note below the expiration field states: 'This token will only be shown once. Copy it now and store it in a safe, secure location.' There is also an 'Advanced option' link. At the bottom of the modal are 'Cancel' and 'Generate' buttons. The background shows a grid of token entries with some blurred details.

Step 2: Copy the token and create a GitLab CI/CD masked variable for the token to be used in the pipeline. Also, create variables for the tenant id, AccuKnox URL (cspm.accuknox.com or cspm.demo.accuknox.com), and the target URL that you want to use for DAST.

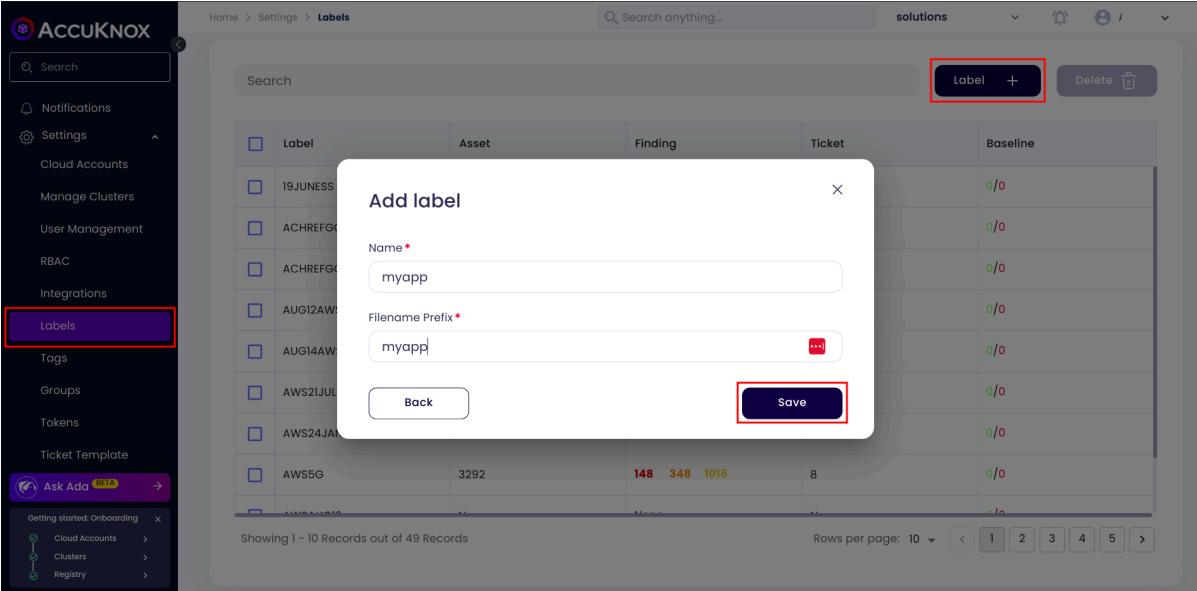


The screenshot shows the AccuKnox interface for managing CI/CD variables. On the left, there's a sidebar with project management options like Build, Secure, Deploy, Operate, Monitor, Analyze, Settings, and CI/CD. The CI/CD section is currently selected. The main area displays a table of CI/CD Variables with four entries:

Key ↑	Value	Environments	Actions
ACCUKNOX_TOKEN	*****	All (default)	
ACCUKNOX_URL	*****	All (default)	
SCAN_URL	*****	All (default)	
TENANT_ID	*****	All (default)	

Below this, there's a section for "Group variables (inherited)" which states "These variables are inherited from the parent group." It shows a table for "CI/CD Variables </> 0" with columns for Key, Environments, and Group, and a note "There are no variables yet."

Step 3: To create a label, navigate to AccuKnox > Settings > Labels, assign a name to your label, click the save button, and then configure it as a GitLab CI/CD variable



The screenshot shows the AccuKnox interface for creating a new label. The left sidebar has a red box around the "Labels" option. The main area shows a list of existing labels and a modal dialog titled "Add label". The dialog contains fields for "Name*" (set to "myapp") and "Filename Prefix*" (set to "myapp"). A "Back" button is at the bottom left, and a large "Save" button is highlighted with a red box at the bottom right. The background shows a grid of labels with various status metrics.



The screenshot shows the AccuKnox CI/CD Variables settings page again. A new variable has been added under the "ACCUKNOX_TOKEN" row, with the key "LABEL" and value "myapp". The "Environments" column shows "All (default)".

Step 4: Set Up GitLab CI/CD Pipeline

Create a new pipeline in your GitLab project with the following YAML configuration:

```
stages:
  - DAST
  - upload-report

DAST:
  stage: DAST
  image: docker:latest
  services:
    - docker:dind
  script:
    - docker run --rm -v $(pwd):/zap/wrk -t zaproxy/zap-stable zap-full-scan.py
      -t $SCAN_URL -J report.json -I
  artifacts:
    paths:
      - report.json

upload-report-to-accuknox:
  stage: upload-report
  image: curlimages/curl:latest
  dependencies:
    - DAST
  script:
    - |
      curl --location --request POST
      "https://$ACCUKNOX_URL/api/v1/artifact/?tenant_id=$TENANT_ID&label_id=$LABEL&data_type=ZAP&save_to_s3=true"
      --header "Tenant-Id: $TENANT_ID" \
      --header "Authorization: Bearer $ACCUKNOX_TOKEN" \
      --form "file=@report.json"
    - echo "Checking for critical vulnerabilities..."
    - |
      if grep -q -i -E "HIGH|CRITICAL" report.json; then
        echo "AccuKnox Scan has halted the deployment because it detected
high/critical vulnerabilities"
        exit 1
      else
        exit 0
      fi
```

11.2.4 Initial CI/CD Pipeline Without AccuKnox Scan

Initially, the CI/CD pipeline does not include the AccuKnox scan. When you push changes to the repository, no security checks are performed, potentially allowing security issues in the application.

11.2.5 CI/CD Pipeline After AccuKnox Scan Integration

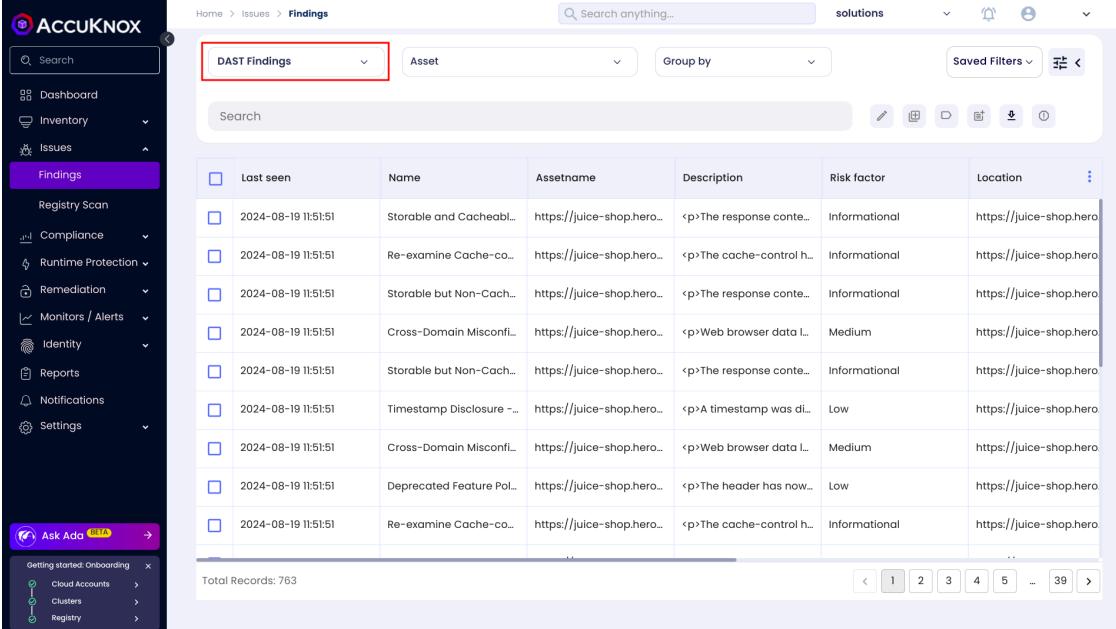
After integrating AccuKnox into your CI/CD pipeline, the next push triggers the CI/CD pipeline. The AccuKnox scan identifies potential vulnerabilities in the application.

```
    7 Preparing environment
    8 Running on runner-jhcjxvh-project-60898060-concurrent-0 via runner-jhcjxvh-s-l-s-amd64-1724328658-fcf2315
      8...
    9 Getting source from Git repository
   10 Fetching changes with git depth set to 20...
   11 Initialized empty Git repository in /builds/affan22/DAST/.git/
   12 Created fresh repository.
   13 Checking out 594f5322 as detached HEAD (ref is main)...
   14 Skipping Git submodules setup
   15 $ git remote set-url origin "${CI_REPOSITORY_URL}"
   16 Downloading artifacts
   17 Downloading artifacts for DAST (7642139528)...
   18 Downloading artifacts from coordinator... ok          host=storage.googleapis.com id=7642139528 responseStat
     us=200 OK token=glcbt-66
   19 Executing "step_script" stage of the job script
   20 Using docker image sha256:65019fbb78d5aa95b9ce0ff1fedffebebebfe33dfbd886c8aeaebd49be8c909407 for curlimages/
     curl:latest with digest curlimages/curl@sha256:8addc281f0ea51517409209f76832b6ddc2cab3264feb1ebbec2a2521ffa
     d24e4 ...
   21 $ curl --location --request POST "https://$ACCUKNOX_URL/api/v1/artifact/?tenant_id=$TENANT_ID&label_id=$LA
     BEL&data_type=ZAP&save_to_s3=false" \ # collapsed multi-line command
   22   % Total    % Received % Xferd  Average Speed   Time   Time   Time  Current
     23             Dload  Upload  Total  Spent   Left  Speed
   24 100 32333  100    39  100 32294     83  68741 --::-- --::-- --::-- 68793
   25 {"detail":"File received successfully"}$ echo "Checking for critical vulnerabilities..."
   26 Checking for critical vulnerabilities...
   27 $ if grep -q -i -E "HIGH|CRITICAL" report.json; then # collapsed multi-line command
   28 AccuKnox Scan has halted the deployment because it detected high/critical vulnerabilities
   29 Cleaning up project directory and file based variables
   30 ERROR: Job failed: exit code 1
```

11.2.6 View Results in AccuKnox SaaS

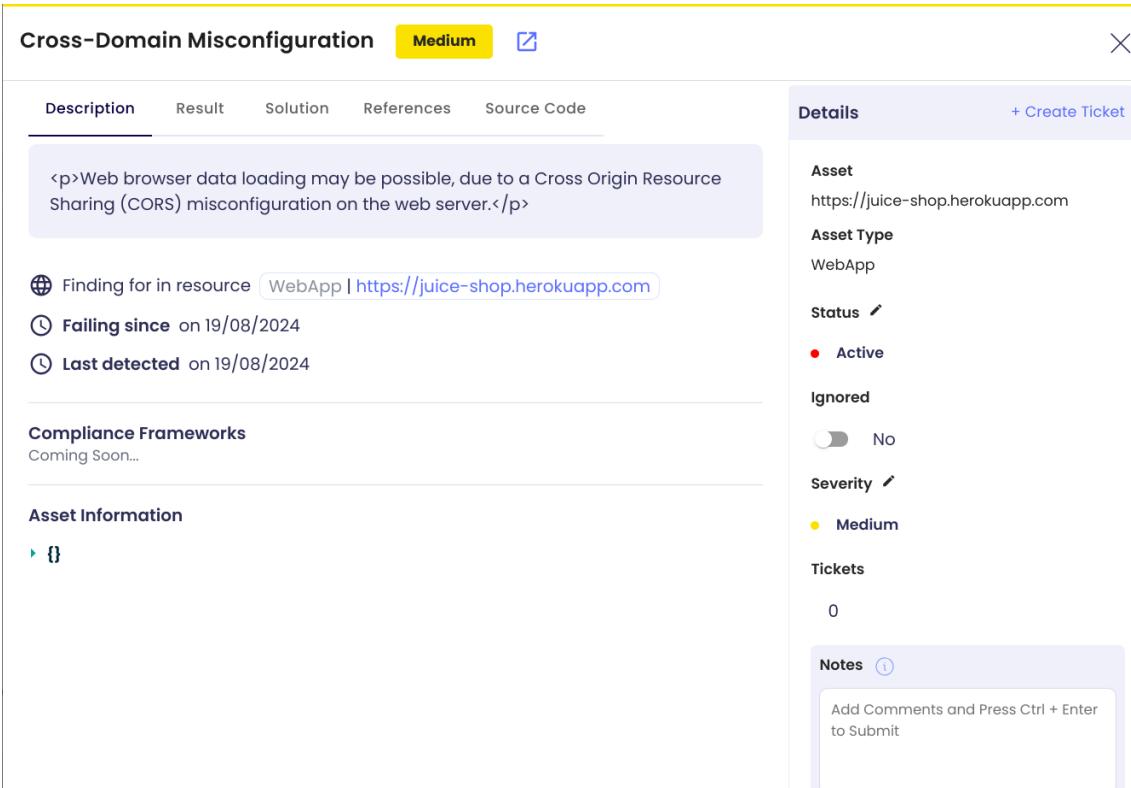
Step 1: After the workflow completes, navigate to the AccuKnox SaaS dashboard.

Step 2: Go to **Issues > Findings** and select **DAST Findings** to see identified vulnerabilities.



The screenshot shows the ACCUKNOX interface. On the left, there's a dark sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which is selected), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below the sidebar, there's a purple 'Ask Ada' button and a 'Getting started: Onboarding' section with Cloud Accounts, Clusters, and Registry. The main area is titled 'DAST Findings'. It has a search bar, filter options for Asset and Group by, and a 'Saved Filters' dropdown. Below the search bar is a table with columns: Last seen, Name, Assetname, Description, Risk factor, and Location. The table contains 8 rows of data, each with a small blue checkbox icon. At the bottom of the table, it says 'Total Records: 763' and has a page navigation bar with buttons for 1 through 39. There are also icons for edit, delete, and refresh.

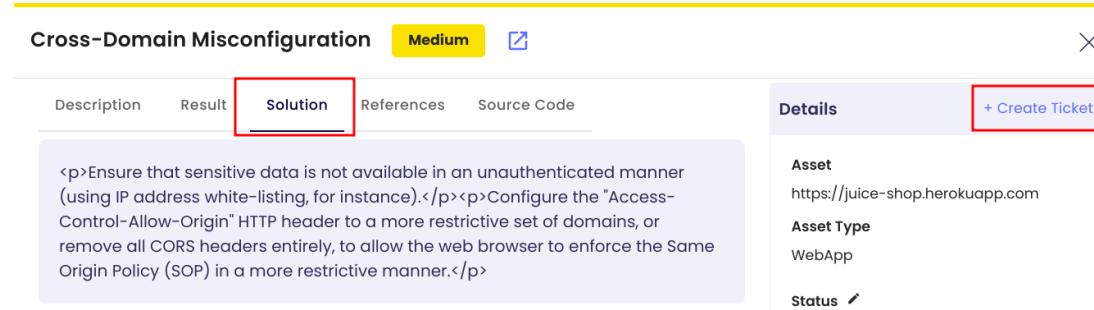
Step 3: Click on a vulnerability to view more details.



This screenshot shows a detailed view of a specific vulnerability. The top header reads 'Cross-Domain Misconfiguration' with a 'Medium' severity level and a 'Details' button. The main content area has tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab contains the following text: '<p>Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.</p>'. Below this, there are three status indicators: a globe icon for 'Finding for in resource' (WebApp | <https://juice-shop.herokuapp.com>), a clock icon for 'Failing since' (on 19/08/2024), and a clock icon for 'Last detected' (on 19/08/2024). The 'Compliance Frameworks' section says 'Coming Soon...'. The 'Asset Information' section has a single item: a green folder icon with an empty list. To the right, there's a 'Details' panel with sections for Asset (https://juice-shop.herokuapp.com), Asset Type (WebApp), Status (Active), Ignored (No), Severity (Medium), Tickets (0), and Notes (an input field with placeholder text: 'Add Comments and Press Ctrl + Enter to Submit').

Step 4: Fix the Vulnerability

Follow the instructions in the Solutions tab to fix the vulnerability (e.g., Cross-Domain Misconfiguration).



Cross-Domain Misconfiguration Medium X

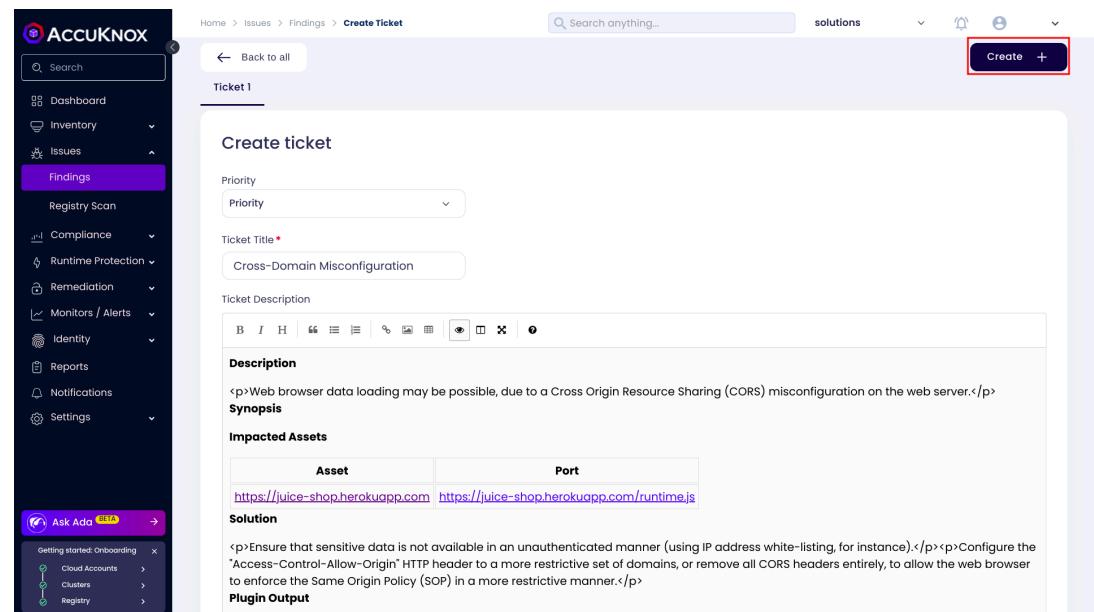
Description	Result	Solution	References	Source Code
<pre><p>Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).</p><p>Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.</p></pre>				

Details + Create Ticket

Asset	https://juice-shop.herokuapp.com
Asset Type	WebApp
Status	✓

Step 5: Create a Ticket for Fixing the Vulnerability

Create a ticket in your issue tracking system to address the identified vulnerability.



Home > Issues > Findings > Create Ticket solutions

Create +

Ticket 1

Create ticket

Priority:

Ticket Title*: Cross-Domain Misconfiguration

Ticket Description

```
<p>Web browser data loading may be possible, due to a Cross Origin Resource Sharing (CORS) misconfiguration on the web server.</p>
```

Synopsis

Impacted Assets

Asset	Port
https://juice-shop.herokuapp.com	https://juice-shop.herokuapp.com/runtime.js

Solution

```
<p>Ensure that sensitive data is not available in an unauthenticated manner (using IP address white-listing, for instance).</p><p>Configure the "Access-Control-Allow-Origin" HTTP header to a more restrictive set of domains, or remove all CORS headers entirely, to allow the web browser to enforce the Same Origin Policy (SOP) in a more restrictive manner.</p>
```

Plugin Output

Step 6: Review Updated Results

- After fixing the vulnerability, rerun the GitLab CI/CD pipeline.
- Navigate to the AccuKnox SaaS dashboard and verify that the vulnerability has been resolved.

11.3 IaC GitLab Scan

11.3.1 Integrating IaC with AccuKnox in a GitLab CI/CD Pipeline

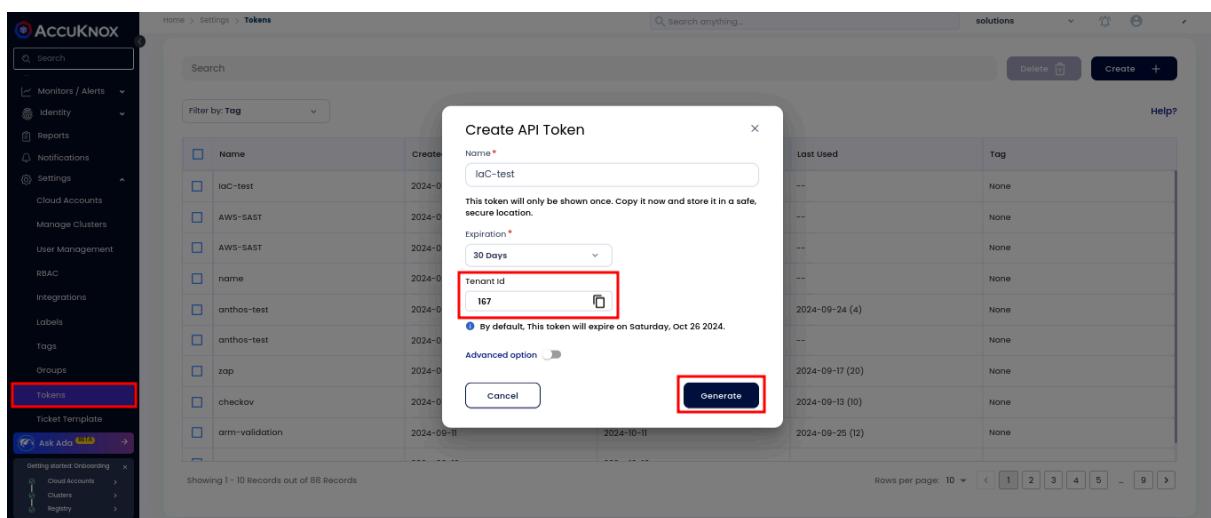
This guide demonstrates how to integrate Infrastructure as Code (IaC) security into a GitLab CI/CD pipeline using AccuKnox. We will implement automated checks to identify configuration vulnerabilities in your IaC templates and send the results to AccuKnox for thorough analysis and remediation. This approach ensures your infrastructure is resilient and aligns with security best practices, effectively minimizing deployment risks.

11.3.2 Pre-requisites

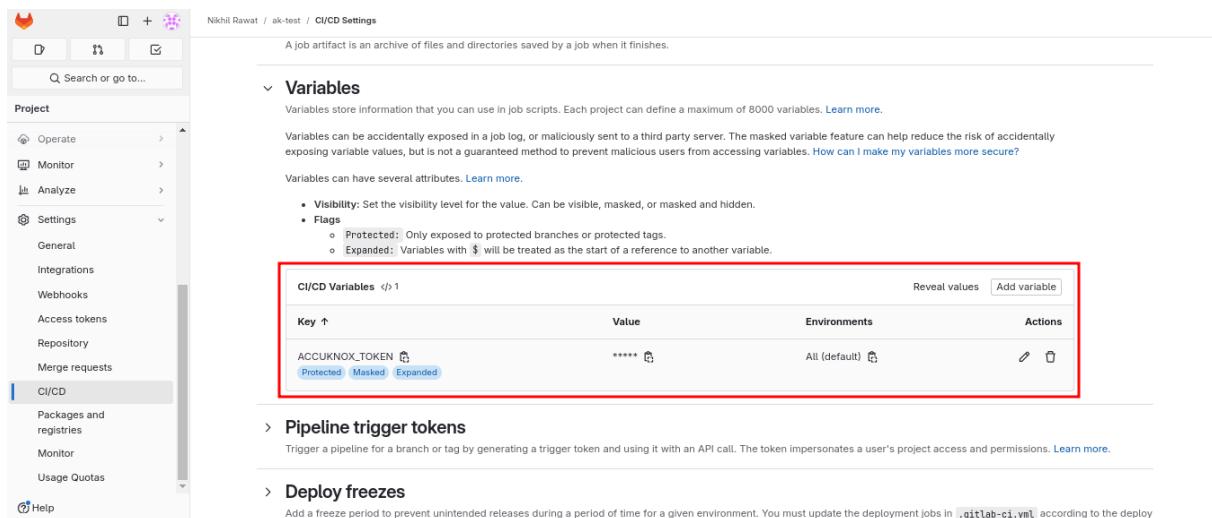
- GitLab Access
- AccuKnox UI Access

11.3.3 Steps for Integration

Step 1: Log in to AccuKnox Navigate to Settings and select Tokens to create a token for forwarding scan results to AccuKnox SaaS. Additionally tenant ID can also be found there which would be helpful for later use.

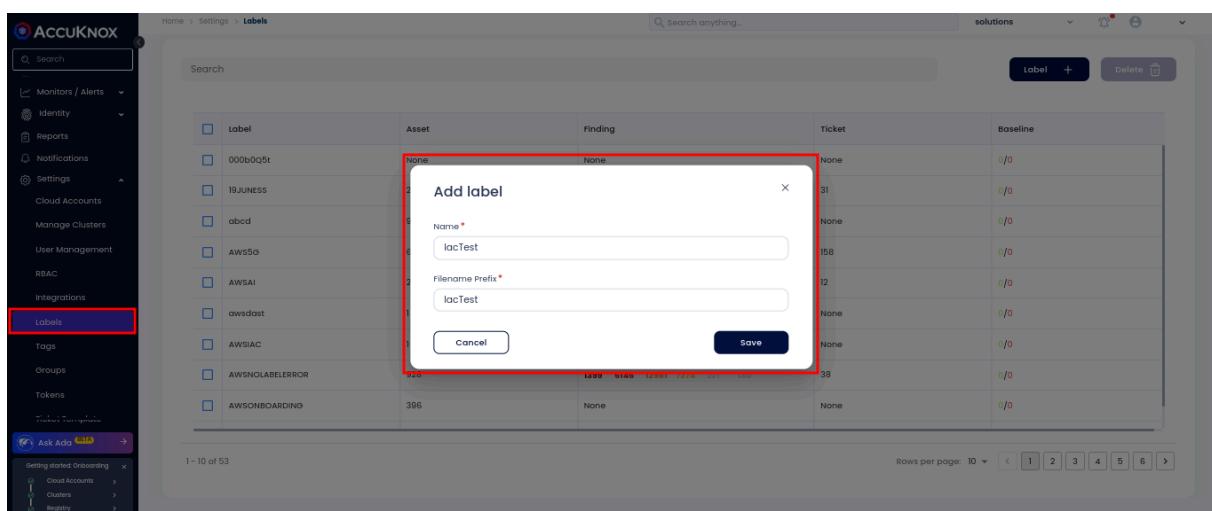


Step 2: Copy the token and create a GitLab CI/CD masked variable for the token to be used in the pipeline.



The screenshot shows the GitLab CI/CD Settings page under the Variables section. A variable named 'ACCUKNOX_TOKEN' is listed with a value of '****'. The 'Protected' and 'Masked' flags are selected, and the 'Expanded' flag is also present. The 'Actions' column contains edit and delete icons.

Step 3: In order to create a label Go to Accuknox > Settings > Labels and create a label, this label is needed to be configured in the pipeline configuration later.



The screenshot shows the AccuKnox Settings Labels page. A new label 'lacTest' is being created, with a 'Name' field containing 'lacTest' and a 'Filename Prefix' field also containing 'lacTest'. The 'Save' button is highlighted.

Step 4: Set Up GitLab CI/CD Pipeline

Create a new pipeline in your GitLab project, and add the following YAML configuration. Update the variables and configurations to match your own project values.

```
stages:
  - scan
  - process
  - deploy
```

```

variables:
  GITLAB_SERVER_URL: 'https://gitlab.com'
  GITLAB_REPOSITORY: 'nikhil120/ak-test' # Update to your GitLab repository
  CSPM_URL: 'cspm.demo.accuknox.com' # Replace with your CSPM endpoint
  TENANT_ID: '000' # Set your unique tenant ID
  ACCUKNOX_API_TOKEN: $ACCUKNOX_API_TOKEN # Ensure this environment variable is set

clone_repo:
  stage: scan
  script:
    - apt-get update
    - apt-get install -y python3 python3-venv python3-pip jq
    - python3 -m venv venv
    - source venv/bin/activate
    - pip install --upgrade pip
    - pip install checkov
    - git clone https://gitlab.com/${GITLAB_REPOSITORY}.git AccuKnox_Iac
    - checkov -d AccuKnox_Iac --output json > checkov_report.json || true
  artifacts:
    paths:
      - checkov_report.json

process_report:
  stage: process
  script:
    - echo "Setting up the environment"
    - apt-get update
    - apt-get install -y python3 python3-venv python3-pip jq
    - echo "Checkov scan complete."
    - ls -al
    - echo "Manipulating JSON report..."
    - |
      # Define repo and branch variables (set these appropriately)
      REPO_LINK="https://gitlab.com/${GITLAB_REPOSITORY}"
      BRANCH_NAME="main" # GitLab predefined variable for branch name

      # Check if the report is empty or not and manipulate JSON
      if [ -s checkov_report.json ]; then
        jq --arg repoLink "$REPO_LINK" --arg branch "$BRANCH_NAME" \
          '. += [{"details": {"repo": $repoLink, "branch": $branch}}]' \
          checkov_report.json > temp.json && \
        mv temp.json checkov_report.json
      else

```

```
echo "[]" > checkov_report.json # Initialize an empty array if the file
is empty
    jq --arg repoLink "$REPO_LINK" --arg branch "$BRANCH_NAME" \
    '. += [{"details": {"repo": $repoLink, "branch": $branch}}]' \
    checkov_report.json > temp.json && \
    mv temp.json checkov_report.json
fi
artifacts:
paths:
- checkov_report.json

push_report:
stage: deploy
image: curlimages/curl:latest
script:
- echo "Uploading checkov_report.json to CSPM endpoint...."
- |
  curl --location --request POST
"https://{$CSPM_URL}/api/v1/artifact/?tenant_id=${TENANT_ID}&data_type=IAC&label
_id=iactest&save_to_s3=false" \
  --header "Tenant-Id: ${TENANT_ID}" \
  --header "Authorization: Bearer ${ACCUKNOX_API_TOKEN}" \
  --form "file=@checkov_report.json"
dependencies:
- process_report
```

Configuration Notes:

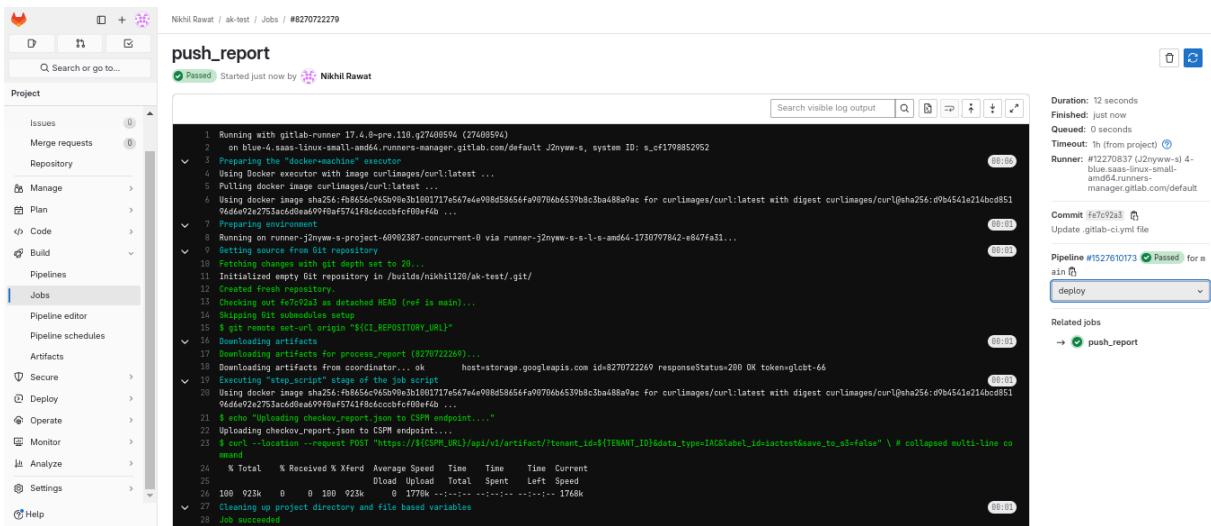
- **GITLAB_REPOSITORY**: Replace this with the path to your GitLab repository in the format `username/repository-name`. Replace with your actual GitLab repository path.
- **CSPM_URL**: Set this to your specific AccuKnox CSPM endpoint URL.
- **TENANT_ID**: Set your tenant ID here.
- **ACCUKNOX_API_TOKEN**: Ensure this variable is stored securely in GitLab CI/CD settings.
- **LABEL_ID**: Customize this label to identify the scan report (e.g. "iac-test"). This label helps categorize and retrieve reports within Accuknox CSPM.

11.3.4 Initial CI/CD Pipeline Without AccuKnox IaC Scan

Initially, the CI/CD pipeline does not include the AccuKnox IaC scan. When changes are pushed to the repository, no infrastructure security checks are performed, potentially allowing misconfigurations or vulnerabilities in the IaC code.

11.3.5 CI/CD Pipeline After AccuKnox IaC Scan Integration

Once the AccuKnox IaC scan is integrated into the CI/CD pipeline, every push triggers an IaC security scan. This scan identifies potential security vulnerabilities or misconfigurations in the infrastructure code, enhancing security prior to deployment. The findings are then sent to the AccuKnox platform.



```

Nikhil Rawat / ak-test / Jobs / #8270722279

push_report
Passed Started just now by Nikhil Rawat

Project
Issues
Merge requests
Repository
Manage
Plan
Code
Build
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Secure
Deploy
Operate
Monitor
Analyze
Settings
Help

Nikhil Rawat / ak-test / Jobs / #8270722279
push_report
Passed Started just now by Nikhil Rawat

Project
Issues
Merge requests
Repository
Manage
Plan
Code
Build
Pipelines
Jobs
Pipeline editor
Pipeline schedules
Artifacts
Secure
Deploy
Operate
Monitor
Analyze
Settings
Help

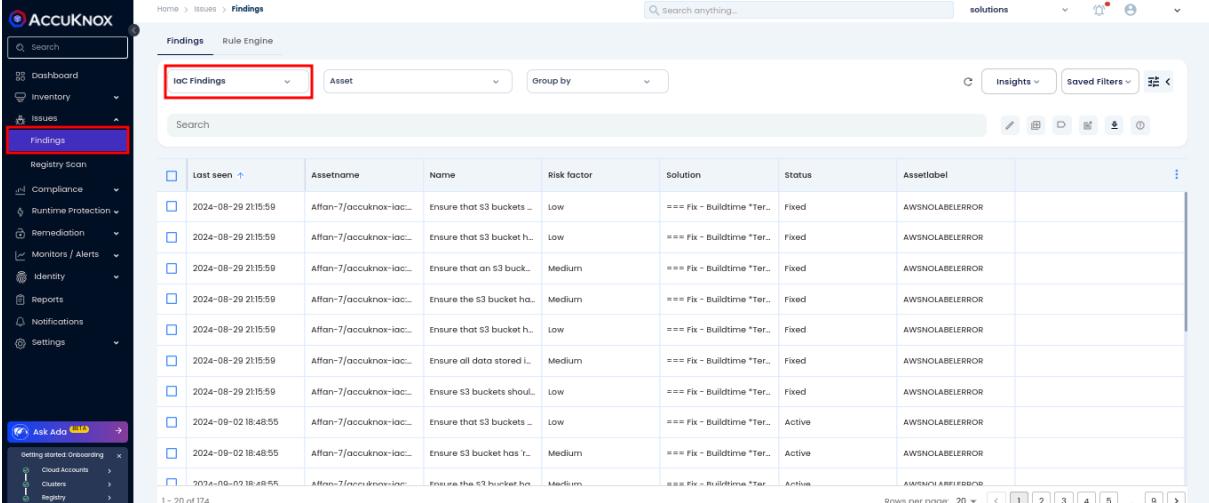
1 Running with gitlab-runner 17.4.0-prerelease.110.g27408594 (27408594)
2 on blue-4.saa...linux-small-and4.runners-manager.gitlab.com/default J2nyww-s, system ID: s_cf1798852952
3 Preparing the "docker-machine" executor
4 Using Docker executor with Image curlimages/curl:latest ...
5 Pulling docker image sha256:fb865ac95d9b8e3b1801717e5a7e4e98bd58656fa08706b6539b8c3ba488a9ac for curlimages/curl:latest with digest curlimages/curl@sha256:d9b4541e214bcd851
6 d6dd092e753a6cd60ea899f08574198cc00fcf0ff0fb ...
7 Preparing environment
8 Running on runner-j2nyww-s-project-60902387-concurrent-0 via runner-j2nyww-s-s-1-s-and64-1730777842-e847fa31...
9 Getting source from Git repository
10 Fetching upstream changes with depth set to 20...
11 Initialized empty Git repository in /builds/nikhil1120/ak-test/.git/
12 Created fresh repository
13 Checking out fe7c92a3 as detached HEAD (ref in main)...
14 Skipping Git submodules setup
15 $ git remote set-url origin "$(CI_REPOSITORY_URL)"
16 Downloading artifacts
17 Downloading artifacts from process_report (8270722269)...
18 Downloading artifacts from coordinator... ok   host=storage.googleapis.com id=8270722269 responseStatus=200 OK token=globt-66
19 Executing "step_script" stage of the job...
20 Using docker image sha256:fb865ac95d9b8e3b1801717e5a7e4e98bd58656fa08706b6539b8c3ba488a9ac for curlimages/curl:latest with digest curlimages/curl@sha256:d9b4541e214bcd851
21 curl -X POST https://$(CSPM_URL)/api/v1/artifact?tenant_id=$(TENANT_ID)&data_type=IaC&label_id=iactest&save_to_s3=false" \ # collapsed multi-line command
22 curl --location --request POST "https://$(CSPM_URL)/api/v1/artifact?tenant_id=$(TENANT_ID)&data_type=IaC&label_id=iactest&save_to_s3=false"
23 Uploading checkov_report.json to CSPM endpoint...
24 curl --location --request POST "https://$(CSPM_URL)/api/v1/artifact?tenant_id=$(TENANT_ID)&data_type=IaC&label_id=iactest&save_to_s3=false"
25 curl --location --request POST "https://$(CSPM_URL)/api/v1/artifact?tenant_id=$(TENANT_ID)&data_type=IaC&label_id=iactest&save_to_s3=false"
26 curl --location --request POST "https://$(CSPM_URL)/api/v1/artifact?tenant_id=$(TENANT_ID)&data_type=IaC&label_id=iactest&save_to_s3=false"
27 Cleaning up project directory and file based variables
28 Job succeeded

Duration: 12 seconds
Finished: just now
Queued: 0 seconds
Timeout: 1h (from project) ⓘ
Runner: #12270837 (J2nyww-s) 4-blue-saa...linux-small-and4.runners-manager.gitlab.com/default
Commit: fe7c92a3 ⓘ
Update: .gitlab-ci.yml file
Pipeline #1527610173 Passed for main ⓘ
deploy
Related jobs
→ push_report
```

11.3.6 View Results in AccuKnox SaaS

Step 1: After the pipeline completes, navigate to the AccuKnox SaaS dashboard.

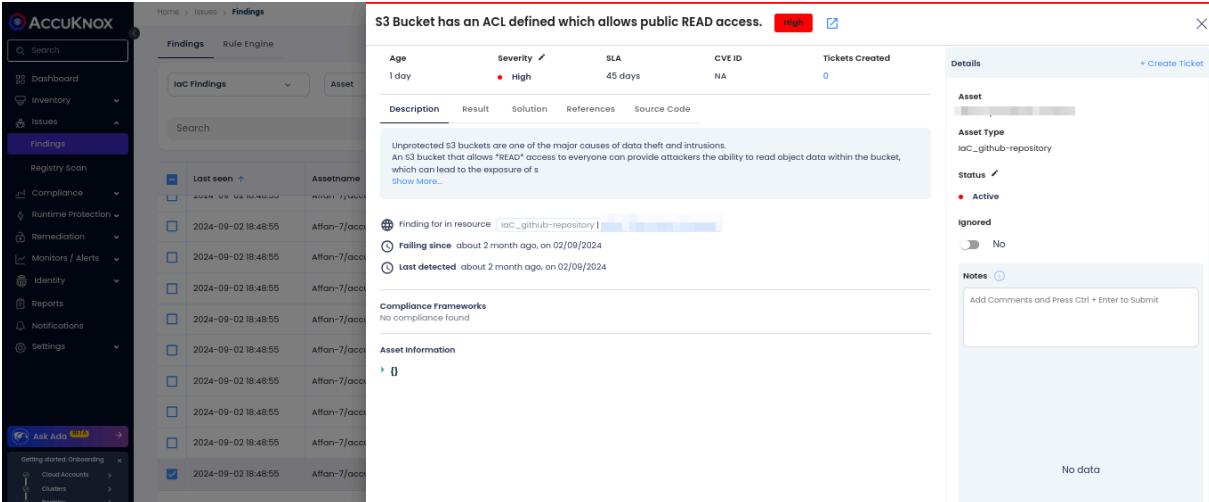
Step 2: Go to **Issues > Findings** and select **IaC Findings** to see identified vulnerabilities.



The screenshot shows the ACCUKNOX interface. On the left, there's a sidebar with navigation links like Dashboard, Inventory, Issues, and Findings. The 'Findings' link is highlighted with a red box. The main content area is titled 'Findings' and shows a table of vulnerabilities. One specific row is highlighted with a red box, detailing an issue with an S3 bucket.

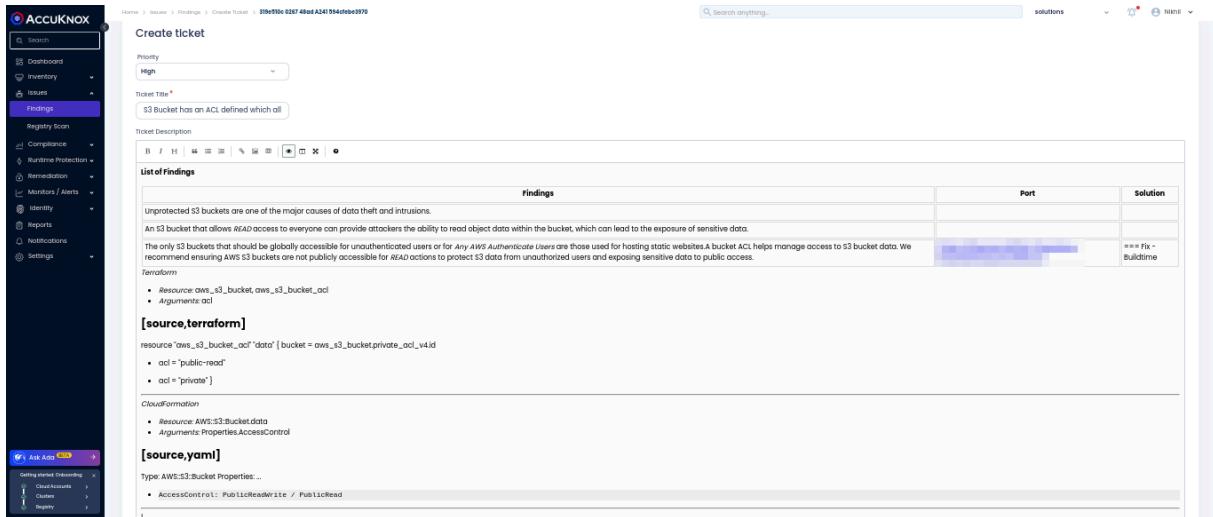
Last seen	Assetname	Name	Risk factor	Solution	Status	Assetlabel
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure that S3 buckets ...	Low	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure that S3 bucket h...	Low	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure that an S3 bucke...	Medium	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure the S3 bucket ha...	Medium	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure that S3 bucket h...	Low	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure all data stored i...	Medium	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-08-29 21:55:59	Affan-7/acuknox-iac...	Ensure S3 buckets shoul...	Low	==== Fix - Buildtime *Ter...	Fixed	AWSNOLABELERROR
2024-09-02 18:48:55	Affan-7/acuknox-iac...	Ensure that S3 buckets ...	Low	==== Fix - Buildtime *Ter...	Active	AWSNOLABELERROR
2024-09-02 18:48:55	Affan-7/acuknox-iac...	Ensure S3 bucket has r...	Medium	==== Fix - Buildtime *Ter...	Active	AWSNOLABELERROR
2024-09-02 18:48:55	Affan-7/acuknox-iac...	Ensure the S3 bucket ha...	Medium	==== Fix - Buildtime *Ter...	Active	AWSNOLABELERROR

Step 3: Click on a vulnerability to view more details and follow the instructions in the Solutions tab.



This screenshot shows a detailed view of a specific finding from the previous table. The finding is about an S3 bucket with public READ access. The severity is listed as 'High'. The right side of the screen shows the 'Details' tab for a ticket, which includes fields for Asset, Asset Type, Status (set to Active), and Notes.

Step 4: For unresolved vulnerabilities, create a ticket in your issue tracking system.



The screenshot shows the AccuKnox interface for creating a ticket. The left sidebar has a dark theme with various navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A central search bar at the top right says "Search anything...". The main area is titled "Create ticket" and includes fields for Priority (High), Ticket Title ("S3 Bucket has an ACL defined which all"), and Ticket Description (with rich text editor). Below this is a "Findings" section with a table header "Findings", "Port", and "solution". A note states: "Unprotected S3 buckets are one of the major causes of data theft and intrusions. An S3 bucket that allows ANY access to everyone can provide attackers the ability to read object data within the bucket, which can lead to the exposure of sensitive data. The only S3 buckets that should be globally accessible are for Any AWS Authenticated Users or for Any AWS IAM User. S3 buckets are used for hosting static websites. A bucket ACL helps manage access to S3 bucket data. We recommend ensuring AWS S3 buckets are not publicly accessible for ANY actions to protect S3 data from unauthorized users and exposing sensitive data to public access." A "Terraform" section shows code for an AWS S3 bucket with acl arguments. A "CloudFormation" section shows a snippet of CloudFormation YAML. At the bottom, there's a "source.yaml" section with a note about AWS::S3::Bucket Properties.

Step 5: After fixing the vulnerabilities, rerun the GitLab CI/CD pipeline and verify that the issues have been resolved in the AccuKnox dashboard.

11.4 GitLab IaC Scan via Accuknox

This guide demonstrates how to secure a CI/CD pipeline in GitLab using Accuknox to enhance security for Infrastructure as Code (IaC). We will identify code vulnerabilities and send the results to AccuKnox for analysis and remediation.

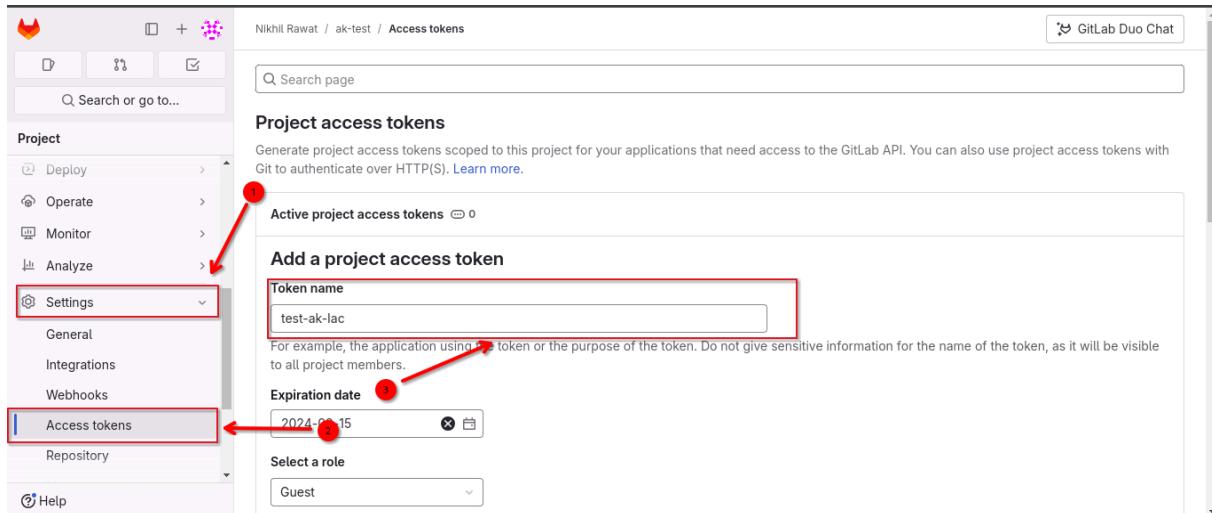
11.4.1 Prerequisites

1. Public Repository:

- You only need the repository URL containing the IaC files.

2. Private Repository:

- Go to your GitLab repository Navigate to Settings > Access Tokens to get the token.



- Add a new token with `read_repository` as the scope and assign the role as `Reporter`

Select a role

Reporter

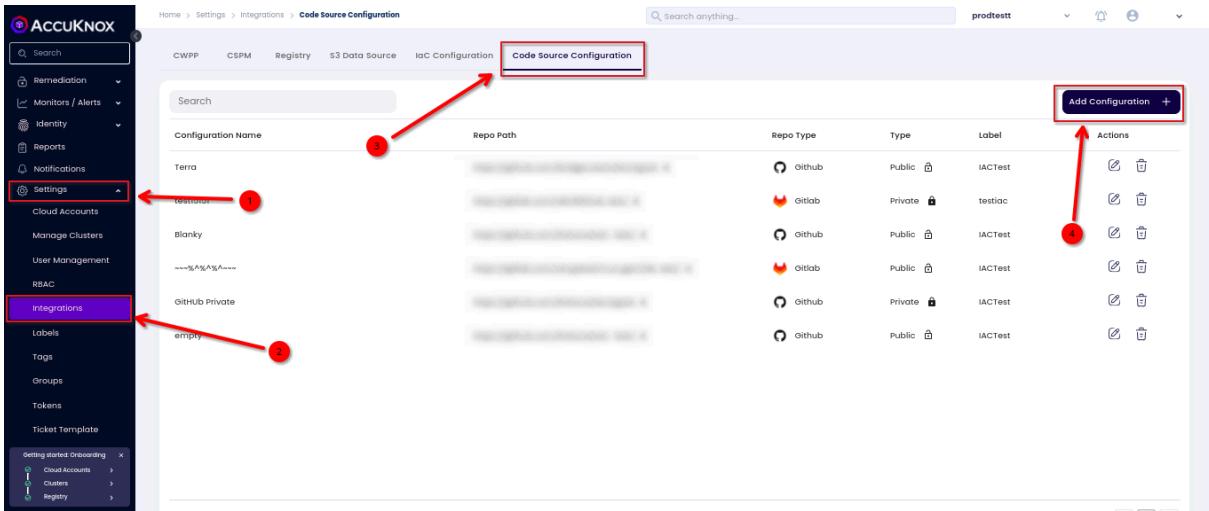
Select scopes

Scopes set the permission levels granted to the token. [Learn more.](#)

<input type="checkbox"/> api	Grants complete read and write access to the scoped project API, including the container registry, the dependency proxy, and the package registry.
<input type="checkbox"/> read_api	Grants read access to the scoped project API, including the Package Registry.
<input type="checkbox"/> create_runner	Grants create access to the runners.
<input type="checkbox"/> manage_runner	Grants access to manage the runners.
<input type="checkbox"/> k8s_proxy	Grants permission to perform Kubernetes API calls using the agent for Kubernetes.
<input checked="" type="checkbox"/> read_repository	Grants read access (pull) to the repository.
<input type="checkbox"/> write_repository	Grants read and write access (pull and push) to the repository.
<input type="checkbox"/> read_registry	

11.4.2 Configuring Code Source in Accuknox

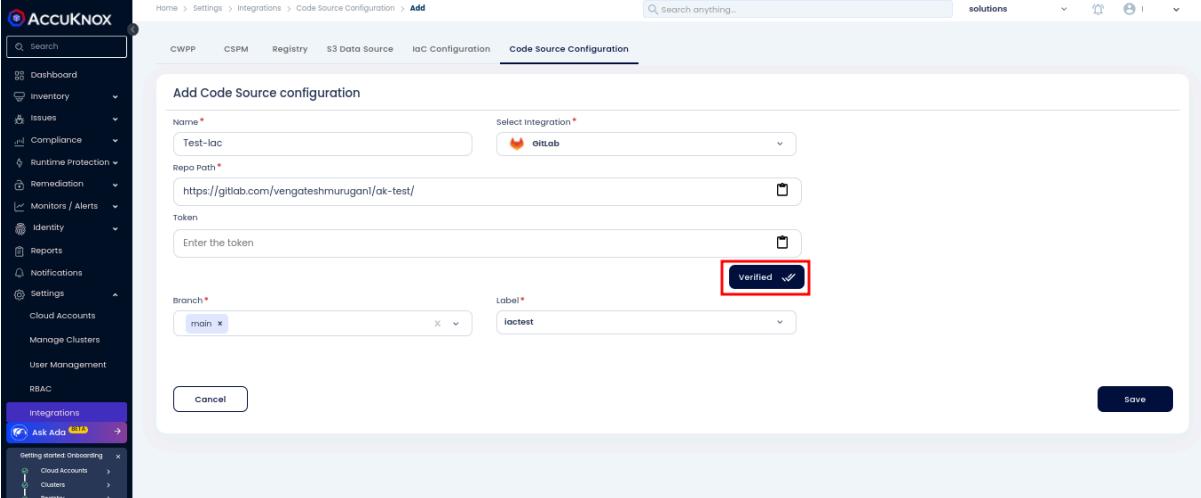
1. Go to Settings > Integration > Code Source Configuration on the Accuknox platform.



Configuration Name	Repo Path	Repo Type	Type	Label	Actions
Terra	https://github.com/testiac/Terra	GitHub	Public	IACTest	
Blanky	https://github.com/testiac/Blanky	GitHub	Private	testiac	
GitHub Private	https://github.com/testiac/GitHub%20Private	GitHub	Public	IACTest	
empty	https://github.com/testiac/empty	GitHub	Private	IACTest	
		GitHub	Public	IACTest	

2. Enter the repository path:
 - **Public Repository:** No token is needed.
 - **Private Repository:** Enter the previously created access token.
3. Click on Test to verify the configuration and ensure there are no errors.
4. Select the branch type and label.

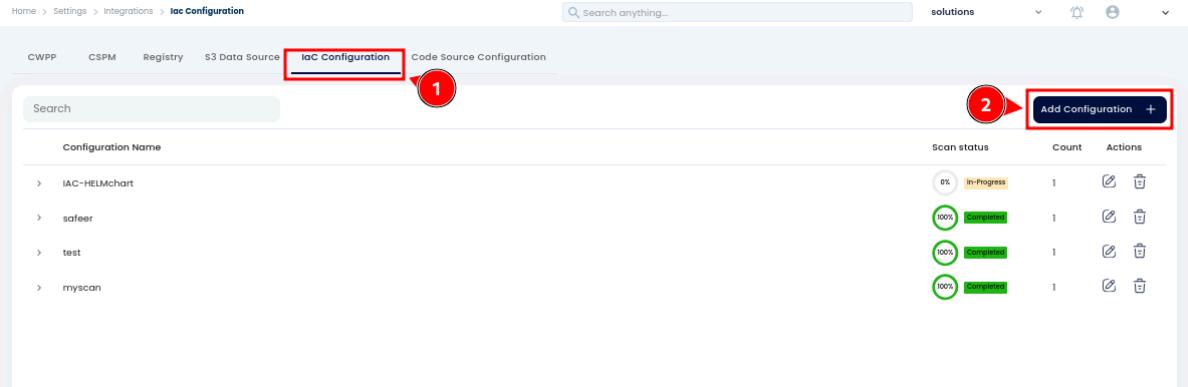
5. Save the configuration.



The screenshot shows the 'Add Code Source configuration' page. The 'Code Source Configuration' tab is active. The 'Name' field contains 'Test-iac'. The 'Select Integration' dropdown is set to 'gitlab'. The 'Repo Path' field shows 'https://gitlab.com/vengateshmrugan/ak-test/'. The 'Token' field has 'Enter the token' placeholder. The 'Branch' field is set to 'main' and the 'Label' field is set to 'iactest'. A 'verified ✓' button is highlighted with a red box. At the bottom right is a 'Save' button.

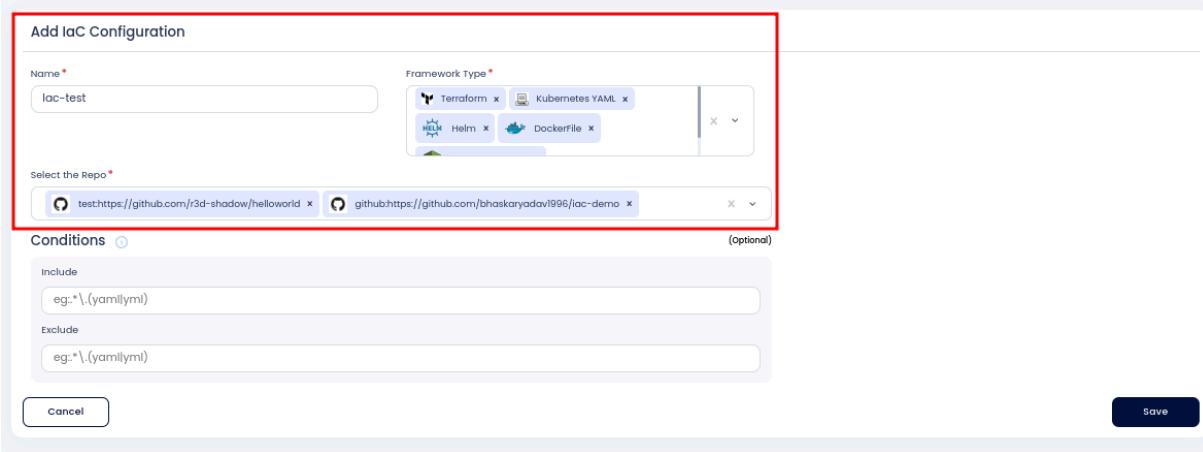
11.4.3 Setting Up IaC Configuration

1. Navigate to the IaC Configuration tab.
2. Click on Add Configuration.



Scan status	Count	Actions	
0% In-Progress	1		
100% Pending	1		
100% Complete	1		
100% Pending	1		

1. Fill in the following details:
 - **Integration Name:** Provide a name for this integration.
 - **Framework Type:** Select the file types you want to scan in the repository (e.g., Terraform, Helm, Dockerfile).
2. Select the repository from the dropdown menu that you previously added.



Add IAC Configuration

Name *

Framework Type *

Select the Repo *

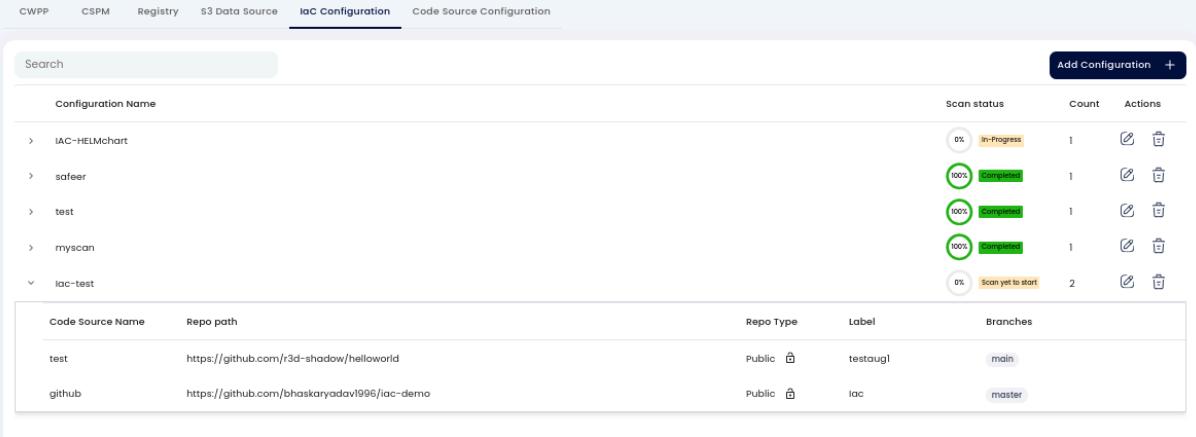
Conditions (optional)

Include: eg: *.yaml|yml

Exclude: eg: *.yaml|yml

Cancel **save**

1. Under the conditions which is an Optional field, you can **include** or **exclude** specific files from the scan.
2. Save the configuration.

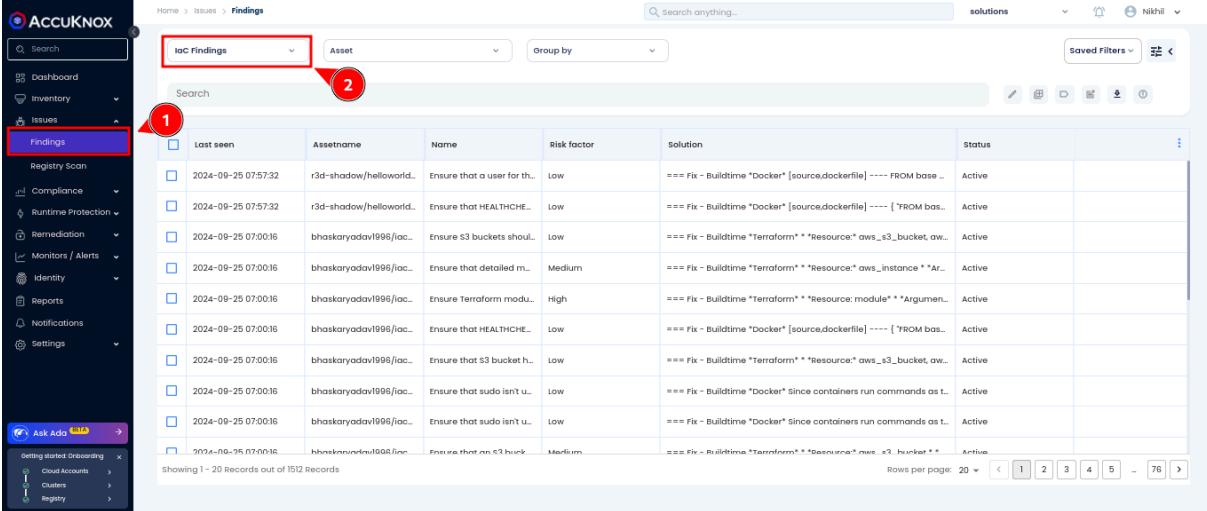


Configuration Name	Scan status	Count	Actions
IAC-HELMchart	0% In-Progress	1	
safeer	100% Complete	1	
test	100% Complete	1	
myscan	100% Complete	1	
iac-test	0% Scan yet to start	2	

Code Source Name	Repo path	Repo Type	Label	Branches
test	https://github.com/r3d-shadow/helloworld	Public	testaugl	main
github	https://github.com/bhaskaryadav1996/iac-demo	Public	iac	master

11.4.4 Viewing and Managing IaC Findings on Accuknox

1. On the Accuknox platform, navigate to Issues > Findings.
2. Select the findings type as IaC Findings.
3. Add the appropriate labels to filter and view the specific IaC findings.



The screenshot shows the AccuKnox platform's user interface. On the left, there's a sidebar with various navigation options like Dashboard, Inventory, Issues, and Settings. The 'Issues' section is expanded, and the 'Findings' tab is selected, highlighted with a red box and circled with a red number '1'. At the top, there's a navigation bar with 'Home > Issues > Findings'. Below the navigation is a search bar with the placeholder 'Search anything...' and a 'Saved Filters' button. The main area is a table titled 'IoC Findings' with columns: Last seen, Assetname, Name, Risk factor, Solution, and Status. There are 1512 records shown, with 1-20 visible on the current page. The table includes several rows of findings related to Docker images and AWS resources.

11.5 Container Scan Use Case

To show how incorporating AccuKnox into a CI/CD pipeline with Gitlab can improve security, let's look at a detailed example involving a Docker image that initially had known vulnerabilities. By running AccuKnox scanning in the pipeline, we can find and fix these vulnerabilities before deploying the image. The following narrative illustrates this process by comparing the situations before and after adding AccuKnox, as seen in the Gitlab jobs log.

11.5.1 Scenario Before Integrating AccuKnox

Context: We started with a Docker image built from a Dockerfile using an outdated base image (`python:alpine`) that contained many known security vulnerabilities. Using this old base image unintentionally introduced many security weaknesses to the Docker image.

Dockerfile Example

```
FROM python:alpine
```

Hypothetical GitLab jobs Log - Pre AccuKnox Scan:

```
Building Docker image...
Image built successfully: your-image:latest
Pushing your-image:latest to Docker Hub...
Image pushed successfully.
```

11.5.2 Scenario After Integrating AccuKnox

Enhancing the GitLab Workflow: We then added a step to our GitLab workflow to run the AccuKnox vulnerability scan on the newly built Docker image.

Updated GitLab Workflow Snippet (Incorporating AccuKnox Scan):

```
build:
  stage: build
  script:
    - echo "Logging into Docker..."
    - echo "$DOCKER_LOGIN_PASSWORD" | docker login -u "$DOCKER_LOGIN_USER"
--password-stdin
    - echo "Building Docker image..."
    - docker build . -t $IMAGE_NAME
    - docker images
    - echo "Running AccuKnox Container Scanner..."
    - docker run --rm -v /var/run/docker.sock:/var/run/docker.sock
$SCAN_IMAGE_NAME image $IMAGE_NAME --format json >> report.json
  artifacts:
    paths:
      - report.json
    expire_in: 1 hour
```

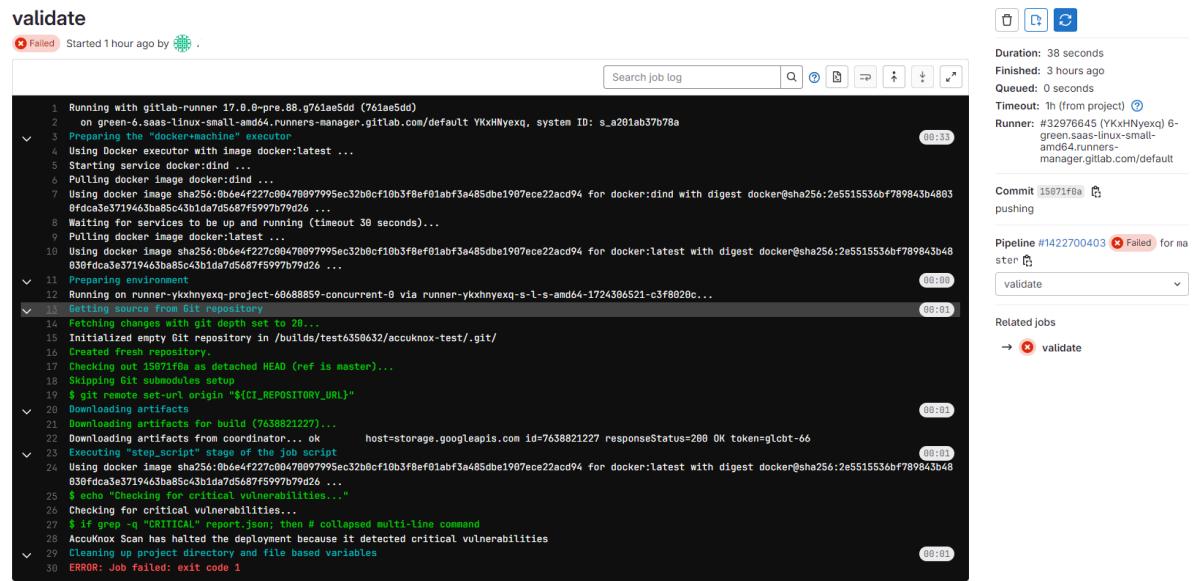
GitLab Jobs Log - Post AccuKnox Integration:

```
Preparing environment
00:00
Running on runner-ykxhnyexq-project-60688859-concurrent-0 via
runner-ykxhnyexq-s-1-s-amd64-1724306521-c3f8020c...
Getting source from Git repository
00:01
Fetching changes with git depth set to 20...
Initialized empty Git repository in /builds/test6350632/accuknox-test/.git/
Created fresh repository.
Checking out 15071f0a as detached HEAD (ref is master)...
Skipping Git submodules setup
$ git remote set-url origin "${CI_REPOSITORY_URL}"
Downloading artifacts
00:01
Downloading artifacts for build (7638821227)...
```

```

Downloading artifacts from coordinator... ok          host=storage.googleapis.com
id=7638821227 responseStatus=200 OK token=glcbt-66
Executing "step_script" stage of the job script
00:01
Using docker image
sha256:0b6e4f227c00470097995ec32b0cf10b3f8ef01abf3a485dbe1907ece22acd94 for
docker:latest with digest
docker@sha256:2e5515536bf789843b48030fdca3e3719463ba85c43b1da7d5687f5997b79d26
...
$ echo "Checking for critical vulnerabilities..."
Checking for critical vulnerabilities...
$ if grep -q "CRITICAL" report.json; then # collapsed multi-line command
AccuKnox Scan has halted the deployment because it detected critical
vulnerabilities
Cleaning up project directory and file based variables
ERROR: Job failed: exit code 1

```



The screenshot shows a GitLab CI pipeline log for a job named 'validate'. The job status is 'Failed' and it started 1 hour ago. The log output is as follows:

```

1 Running with gitlab-runner 17.0.0-pre.88.g76iae5dd (76iae5dd)
2 on green-6.saaS-linux-small-amd64.runners-manager.gitlab.com/default YKxHNyexq, system ID: s_a201ab37b78a
3 Preparing the "Docker+Machine" executor
4 Using Docker executor with image docker:latest ...
5 Starting service docker:dind ...
6 Pulling docker image docker:dind ...
7 Using docker image sha256:0b6e4f227c00470097995ec32b0cf10b3f8ef01abf3a485dbe1907ece22acd94 for docker:dind with digest docker@sha256:2e5515536bf789843b4863
8 Waiting for services to be up and running (timeout 30 seconds)...
9 Pulling docker image docker:latest ...
10 Using docker image sha256:0b6e4f227c00470097995ec32b0cf10b3f8ef01abf3a485dbe1907ece22acd94 for docker:latest with digest docker@sha256:2e5515536bf789843b4863
11 Preparing environment
12 Running on runner-ykxhnnyexq-project-66688859-concurrent-0 via runner-ykxhnnyexq-s-l-s-amd64-1724306521-c3f8020c...
13 Getting source from Git repository
14 Fetching changes with git depth set to 20...
15 Initialized empty Git repository in /builds/test6350632/accuknox-test/.git/
16 Created fresh repository.
17 Checking out 15071ff0 as detached HEAD (ref is master)...
18 Skipping Git submodules setup
19 $ git remote set-url origin "${CI_REPOSITORY_URL}"
20 Downloading artifacts
21 Downloading artifacts for build (7638821227)...
22 Downloading artifacts from coordinator... ok          host=storage.googleapis.com id=7638821227 responseStatus=200 OK token=glcbt-66
23 Executing "step_script" stage of the job script
24 Using docker image sha256:0b6e4f227c00470097995ec32b0cf10b3f8ef01abf3a485dbe1907ece22acd94 for docker:latest with digest docker@sha256:2e5515536bf789843b4863
25 # echo "Checking for critical vulnerabilities...
26 Checking for critical vulnerabilities...
27 $ if grep -q "CRITICAL" report.json; then # collapsed multi-line command
28 AccuKnox Scan has halted the deployment because it detected critical vulnerabilities
29 Cleaning up project directory and file based variables
30 ERROR: Job failed: exit code 1

```

On the right side of the log, there is a summary of the job's execution:

- Duration: 38 seconds
- Finished: 3 hours ago
- Queued: 0 seconds
- Timeout: 1h (from project)
- Runner: #32976645 (YKxHNyexq) 6-green.saaS-linux-small-amd64.runners-manager.gitlab.com/default
- Commit: 15071ff0a pushing
- Pipeline: #1422700403 Failed for master
- Related jobs: validate

AccuKnox carefully analyzed the image and found critical and high-severity vulnerabilities. Based on these findings, the workflow stopped and prevented the vulnerable image from being pushed to the Docker registry.

11.5.3 Remediation and Rescan

Fortifying the Dockerfile: After seeing the vulnerabilities, we updated the Dockerfile to use a newer, more secure base image (`python:alpine` instead, to fix the security issues.

Dockerfile Post-Update:

```
FROM python:alpine# Additional image enhancements and setup
```

GitLab Jobs Log - After Remediation:

Building Docker image...

Image built successfully: your-image:latest

Scanning your-image:latest with AccuKnox...

INF Scanning /path/to/your-image:latest

INF Number of language-specific files: 1

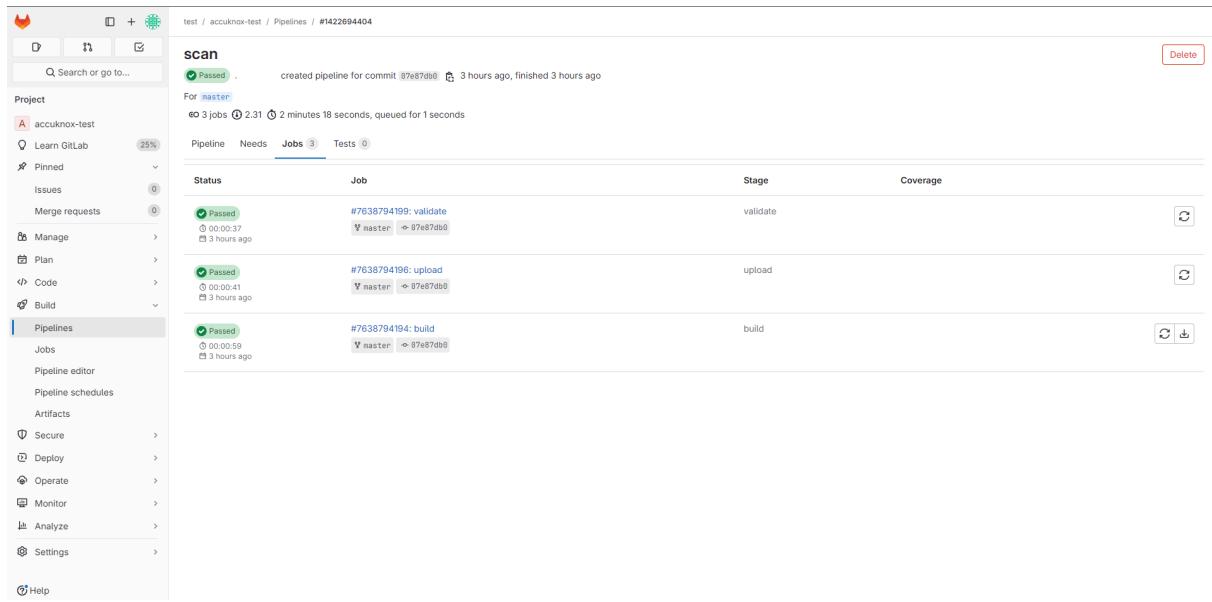
INF No critical vulnerabilities found.

Image scan passed successfully.

Pushing your-image:latest to Docker Hub...

Image pushed successfully.

Once the vulnerabilities were resolved, the AccuKnox scan approved the updated image, allowing it to be safely pushed to the registry. This example clearly shows how important it is to have vulnerability scanning in the pipeline - it prevents insecure images from being deployed to production, ensuring only secure images make it through.



Status	Job	Stage	Coverage
Passed	#7638794199: validate ⌚ 0:00:37 ⌚ 3 hours ago	validate	
Passed	#7638794196: upload ⌚ 0:00:41 ⌚ 3 hours ago	upload	
Passed	#7638794194: build ⌚ 0:00:59 ⌚ 3 hours ago	build	

11.5.4 Steps needed to be taken for integration

Step 1: The user needs to create a GitLab workflow file inside their GitLab repository using the following workflow Template:

```
image: docker:latest # Docker image with Docker installed
```

services:

```
- docker:dind # Docker-in-Docker service for building Docker images
```

variables:

```
IMAGE_NAME: "[tag]/gitlab-pipeline:v1"
SCAN_IMAGE_NAME: "accuknox/accuknox-container-scan"
CSPM_URL: $ACCUKNOX_CSPM_URL
TENANT_ID: $TENANT_ID
DOCKER_LOGIN_USER: $DOCKER_LOGIN_USER
DOCKER_LOGIN_PASSWORD: $DOCKER_LOGIN_PASSWORD
ACCUKNOX_API_TOKEN: $ACCUKNOX_API_TOKEN
```

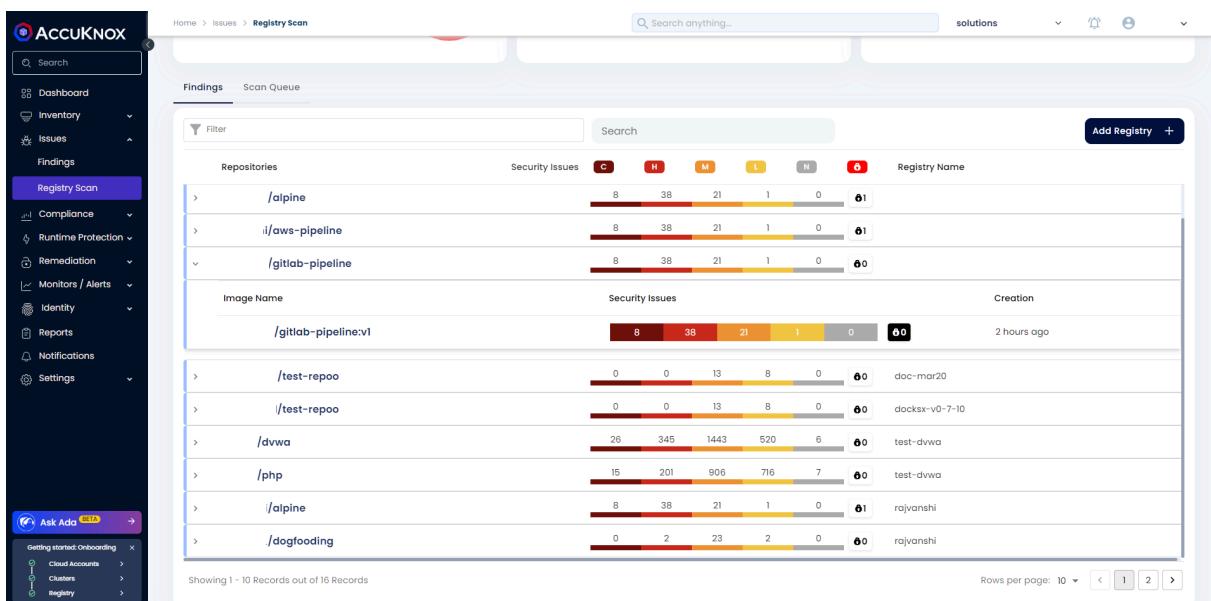
```
stages:
  - build
  - upload
  - validate
build:
  stage: build
  script:
    - echo "Logging into Docker..."
    - echo "$DOCKER_LOGIN_PASSWORD" | docker login -u "$DOCKER_LOGIN_USER"
--password-stdin
    - echo "Building Docker image..."
    - docker build . -t $IMAGE_NAME
    - docker images
    - echo "Running AccuKnox Container Scanner..."
    - docker run --rm -v /var/run/docker.sock:/var/run/docker.sock
$SCAN_IMAGE_NAME image $IMAGE_NAME --format json >> report.json
  artifacts:
    paths:
      - report.json
    expire_in: 1 hour

upload:
  stage: upload
  image: curlimages/curl:latest
  script:
    - echo "Uploading report.json to CSPM endpoint..."
    - |
      curl --location --request POST
"https://{$CSPM_URL}/api/v1/artifact/?tenant_id=${TENANT_ID}&data_type=TR&save_to_s3=false" \
      --header "Tenant-Id: ${TENANT_ID}" \
      --header "Authorization: Bearer ${ACCUKNOX_API_TOKEN}" \
      --form "file=@\"report.json\""
validate:
  stage: validate
  script:
    - echo "Checking for critical vulnerabilities..."
    - |
      if grep -q "CRITICAL" report.json; then
        echo "AccuKnox Scan has halted the deployment because it detected
critical vulnerabilities"
        exit 1
      else
        exit 0
      fi
```

Note: In the above template, the user needs to change some variables, including ACCUKNOX_API_TOKEN, CSPM_URL(cspm.demo|stage|dev.accuknox.com), and TENANT_ID. Values for these variables can be obtained from AccuKnox SaaS.

Step 2: Now, when a user attempts to make any changes to their repository, the workflow will be triggered, performing the necessary steps for scanning and posting the results to AccuKnox SaaS.

Step 3: Once the scan is complete, the user can go into the AccuKnox SaaS and navigate to Issues → RegistryScan where they can find their repository name and select it to see the associated findings

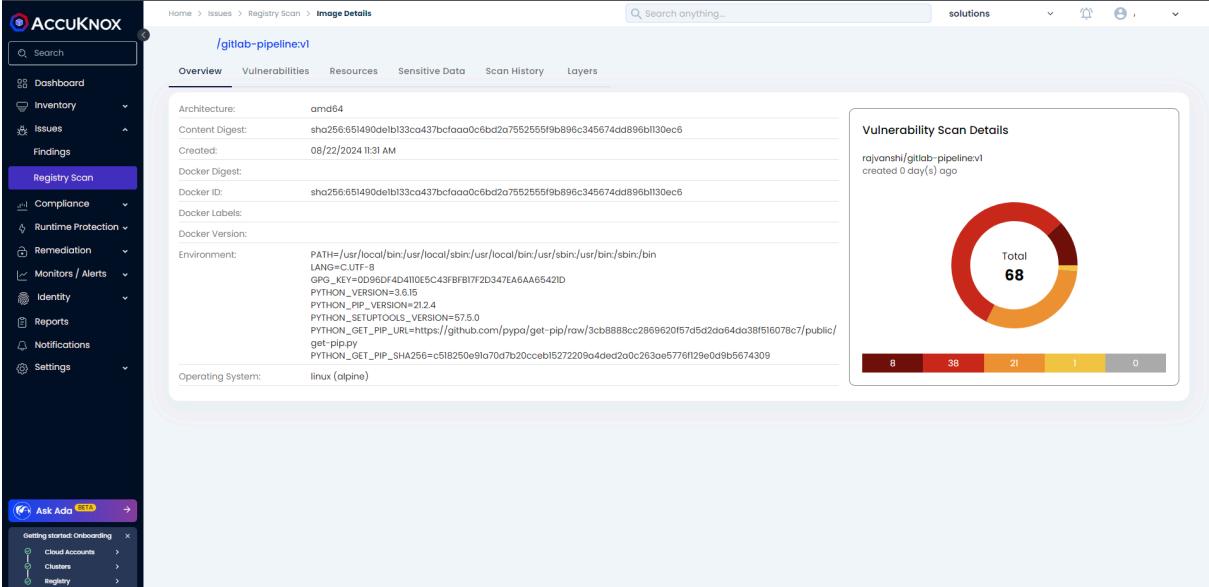


The screenshot shows the AccuKnox SaaS interface with the following details:

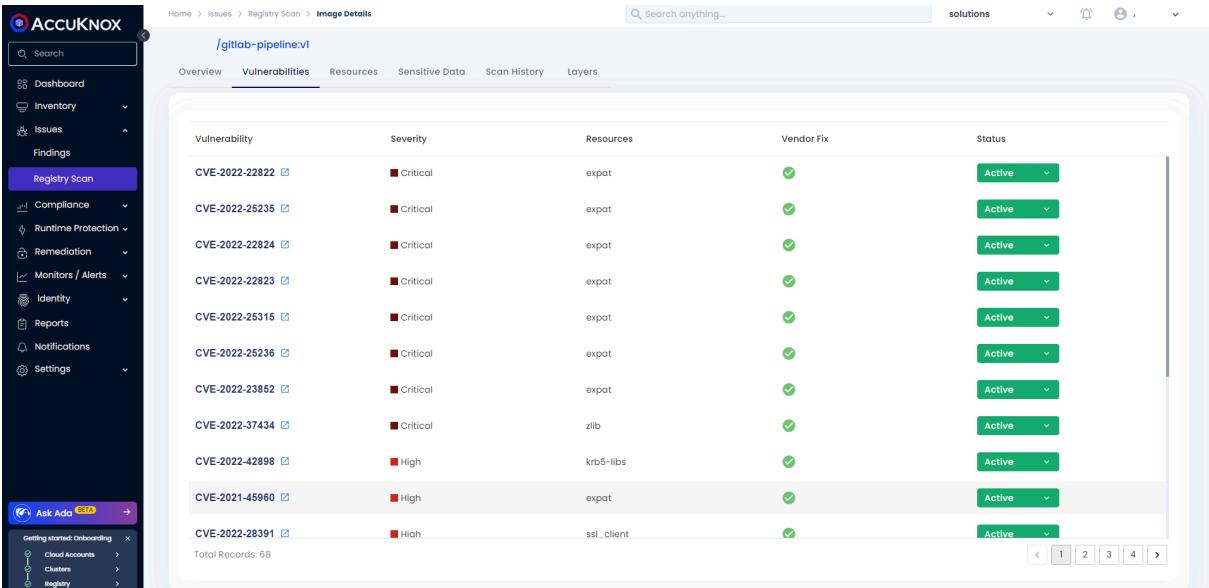
- Left Sidebar:** Includes sections for Dashboard, Inventory, Issues (selected), Findings, Registry Scan (selected), Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A "Getting Started Onboarding" section is also present.
- Top Header:** Home > Issues > Registry Scan. Search bar and solutions dropdown.
- Main Content:** Findings tab selected. A table displays scanned repositories and their findings across various categories (C, H, M, L, N, O).
- Table Headers:** Repositories, Security Issues, Registry Name.
- Table Data:**

Image Name	Security Issues	Creation
/alpine	C: 8, H: 38, M: 21, L: 1, N: 0, O: 61	2 hours ago
ii/aws-pipeline	C: 8, H: 38, M: 21, L: 1, N: 0, O: 61	
/gitlab-pipeline	C: 8, H: 38, M: 21, L: 1, N: 0, O: 60	
/gitlab-pipeline:v1	C: 8, H: 38, M: 21, L: 1, N: 0, O: 60	2 hours ago
/test-repo0	C: 0, H: 0, M: 13, L: 8, N: 0, O: 60	doc-mar20
/test-repo0	C: 0, H: 0, M: 13, L: 8, N: 0, O: 60	docksx-v0-7-10
/dvwa	C: 26, H: 345, M: 1443, L: 520, N: 6, O: 60	test-dvwa
/php	C: 15, H: 201, M: 906, L: 716, N: 7, O: 60	test-dvwa
/alpine	C: 8, H: 38, M: 21, L: 1, N: 0, O: 61	rajvanshi
/dogfooding	C: 0, H: 2, M: 23, L: 2, N: 0, O: 60	rajvanshi
- Bottom:** Rows per page: 10, navigation icons.

Step 4: After clicking on the image name, the user will be able to see the metadata for the image that was built during the workflow execution.

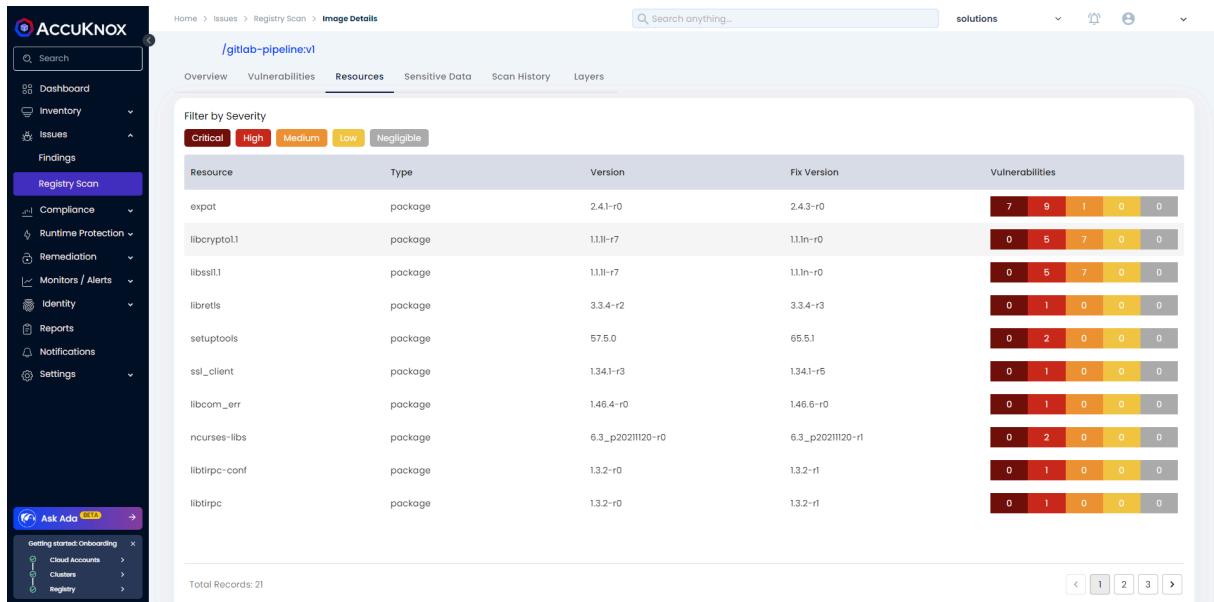


Step 5: In the Vulnerabilities section, the user can see the image-specific vulnerabilities in a list manner that contains relevant information. These findings will also be available in the Issues → Vulnerabilities section where the user can manage these findings with others.



Vulnerability	Severity	Resources	Vendor Fix	Status
CVE-2022-22822	Critical	expat	✓	Active
CVE-2022-25235	Critical	expat	✓	Active
CVE-2022-22824	Critical	expat	✓	Active
CVE-2022-22823	Critical	expat	✓	Active
CVE-2022-25315	Critical	expat	✓	Active
CVE-2022-25236	Critical	expat	✓	Active
CVE-2022-23862	Critical	expat	✓	Active
CVE-2022-37434	Critical	zlib	✓	Active
CVE-2022-42898	High	krb5-libs	✓	Active
CVE-2021-45960	High	expat	✓	Active
CVE-2022-28391	High	ssl_client	✓	Active

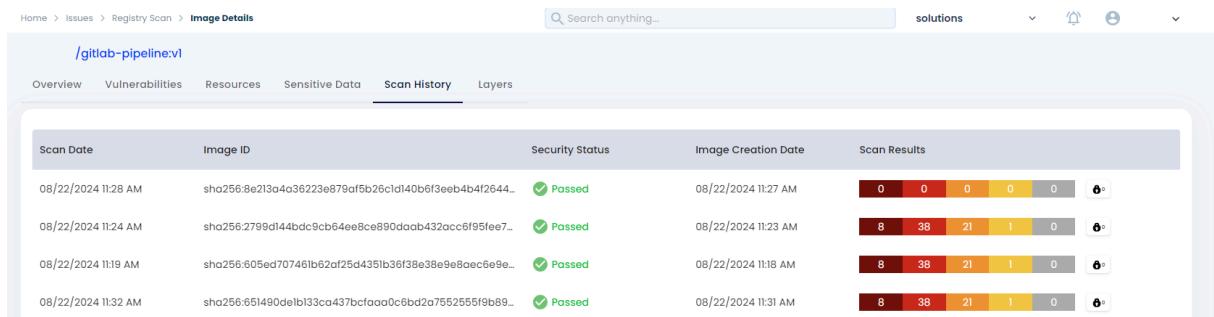
Step 6: The Resources Section contains information about packages and modules that were used to build the code base into a container image.



Resource	Type	Version	Fix Version	Vulnerabilities				
expat	package	2.4.1-r0	2.4.3-r0	7	9	1	0	0
libcryptoki1	package	1.1.11-r7	1.1.11-r0	0	5	7	0	0
libssl1.1	package	1.1.11-r7	1.1.11-r0	0	5	7	0	0
libtiffs	package	3.3.4-r2	3.3.4-r3	0	1	0	0	0
setup-tools	package	57.5.0	65.5.1	0	2	0	0	0
ssl-client	package	1.34.1-r3	1.34.1-r5	0	1	0	0	0
libcom_err	package	1.46.4-r0	1.46.6-r0	0	1	0	0	0
ncurses-libs	package	6.3_p20211120-r0	6.3_p20211120-r1	0	2	0	0	0
libtirpc-conf	package	1.3.2-r0	1.3.2-r1	0	1	0	0	0
libtirpc	package	1.3.2-r0	1.3.2-r1	0	1	0	0	0

Total Records: 21

Step 7: The user can see the scan history of every scan that happened while triggering the workflow.



Scan Date	Image ID	Security Status	Image Creation Date	Scan Results					
08/22/2024 11:28 AM	sha256:8e213a4a36223e079af5b26c1d140b6f3eeb4b4f2644...	Passed	08/22/2024 11:27 AM	0	0	0	0	0	6
08/22/2024 11:24 AM	sha256:2799d144bdc9cb64ee8ce890daab432acc6f95fee7...	Passed	08/22/2024 11:23 AM	8	38	21	1	0	6
08/22/2024 11:19 AM	sha256:605ed707461b62af25d4351b36f38e3be9e8aec6e9e...	Passed	08/22/2024 11:18 AM	8	38	21	1	0	6
08/22/2024 11:32 AM	sha256:651490de1b133ca437bcfaaa0c6bd2a7552555f9b89...	Passed	08/22/2024 11:31 AM	8	38	21	1	0	6

12. KSPM (Kubernetes Security Posture Management)

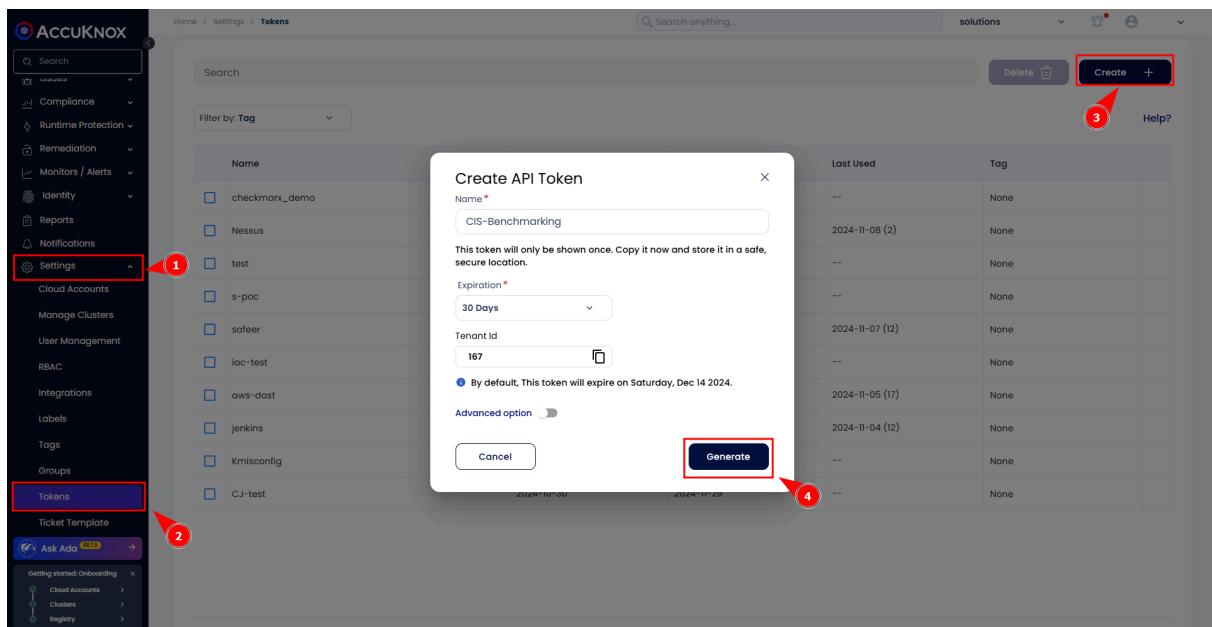
12.1 CIS Benchmarking Compliance Scan Onboarding

This guide details the steps to onboard a Kubernetes cluster to Accuknox SaaS for CIS Benchmarking compliance scanning, enabling you to monitor and improve cluster security in line with CIS standards.

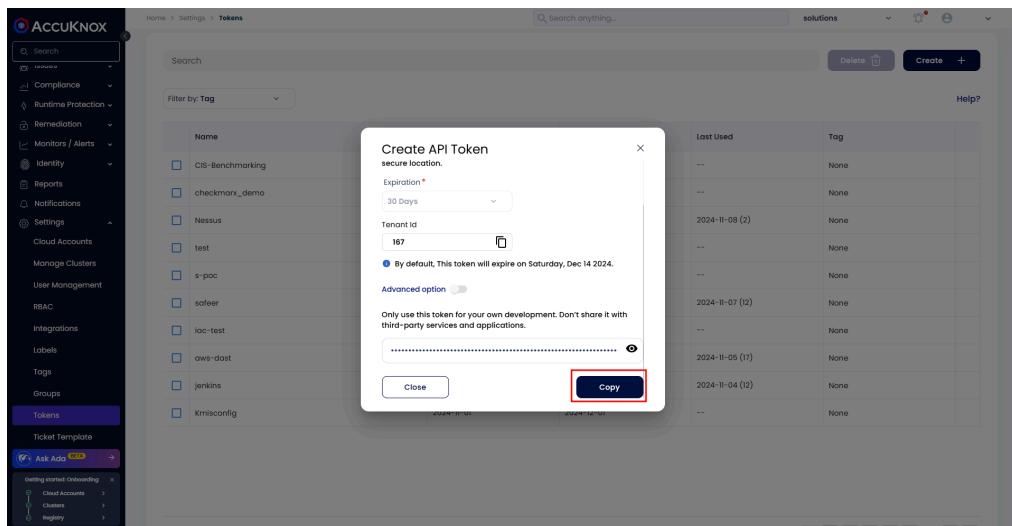
Step 1: Generate an Access Token

To begin, create a token that will authenticate your cluster for scanning. Follow these steps:

1. Navigate to **Settings > Tokens** in the Accuknox platform and Click on the **Create** button, give your token a descriptive name (e.g., "CIS-Compliance-Token"), and click **Generate**.

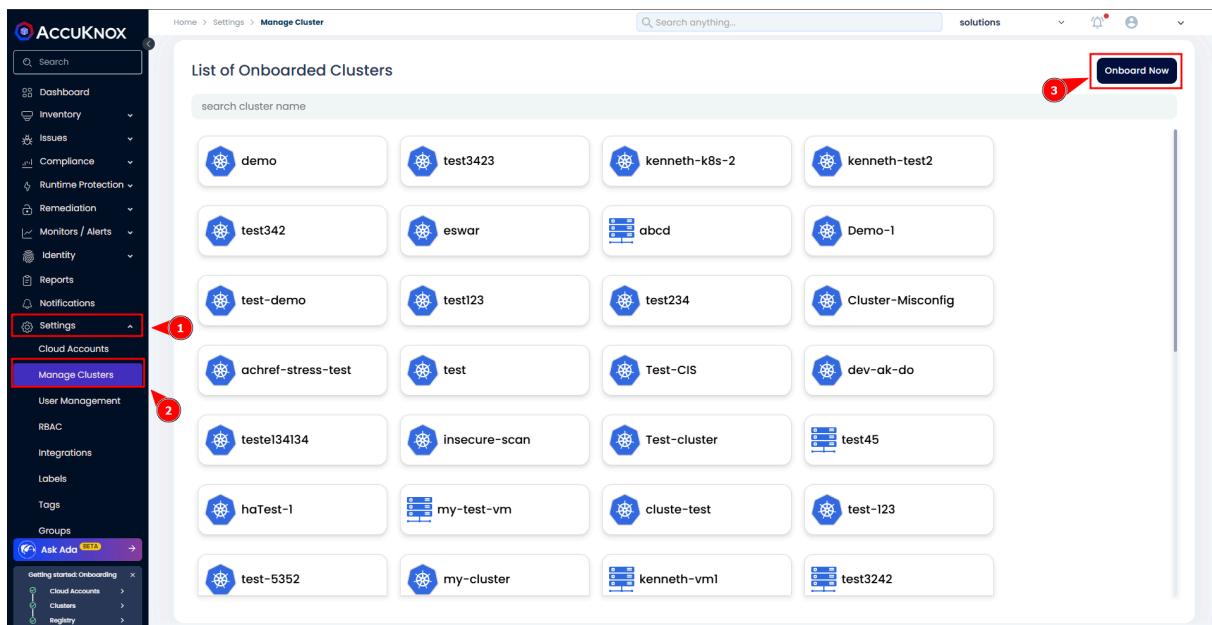


- Once the token is generated, copy it and securely save it for later use.

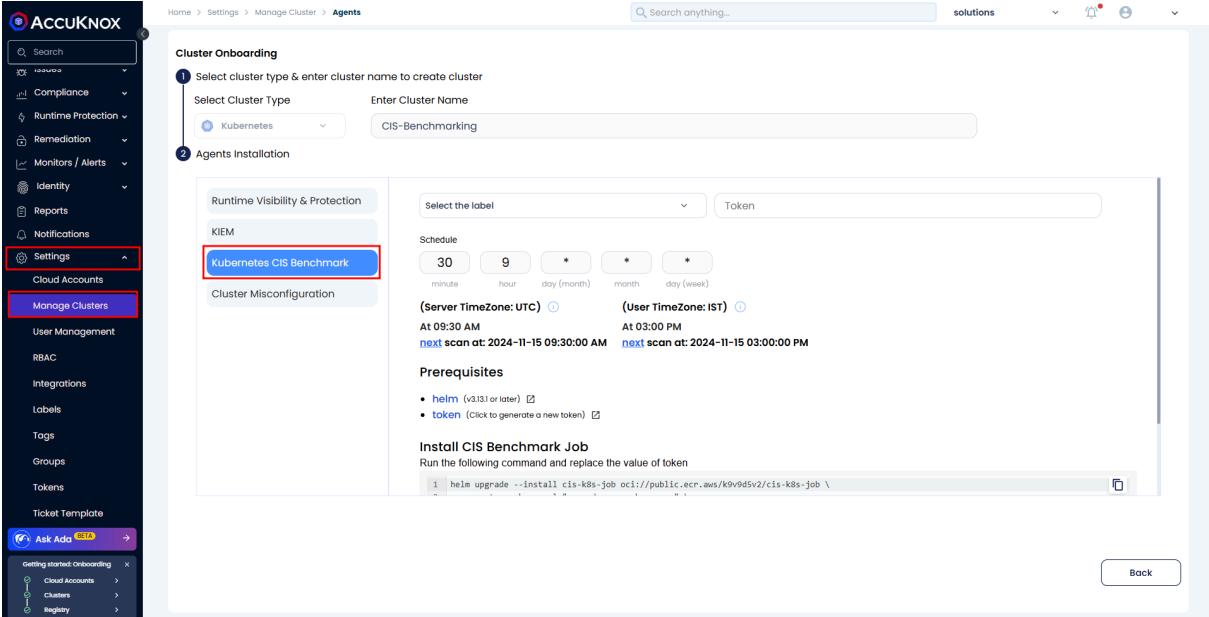


Step 2: Onboard Your Cluster

- Go to **Settings > Manage Clusters** and Click **Onboard Now** or select an existing cluster if you're updating a previously onboarded cluster.

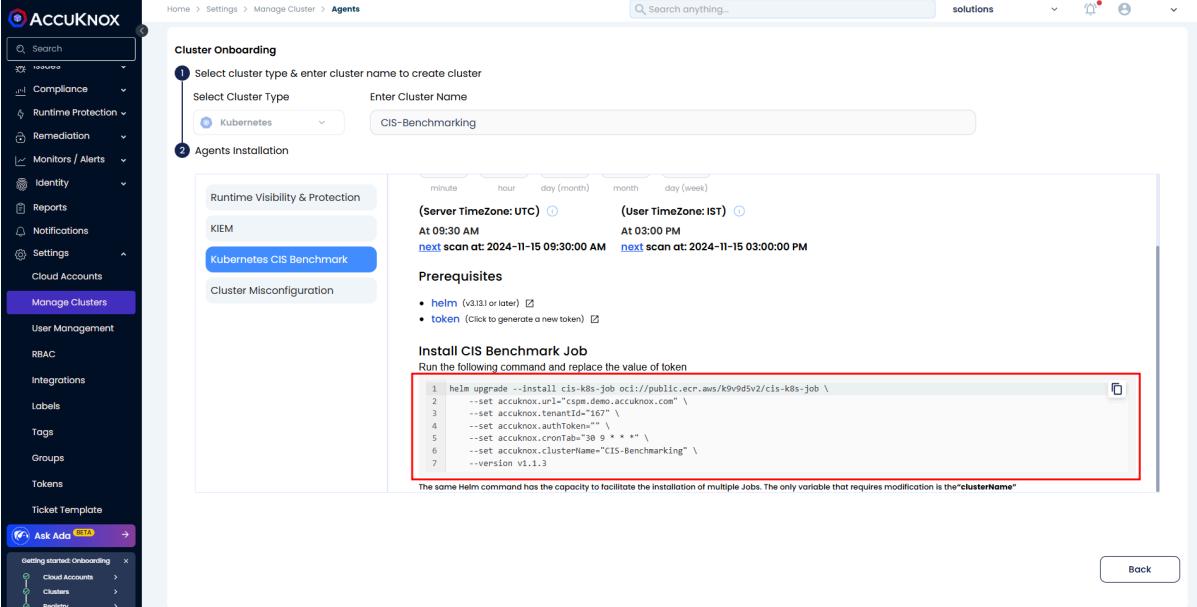


2. Enter a name for your cluster to identify it in Accuknox. From the scan type, choose **CIS Benchmarking**.
3. Select a label for easy identification and paste the token you generated in Step 1. Set a scan schedule based on your requirements. Accuknox will automatically run scans according to the selected schedule



Step 3: Deploy the Scanner Using Helm

1. Scroll down to the **Helm Command** section and copy the provided command.



The screenshot shows the AccuKnox platform's Cluster Onboarding interface. On the left, a sidebar lists various compliance and protection features like Cloud Accounts, Clusters, and Registry. The main panel is titled 'Cluster Onboarding' and 'Agents'. Step 1, 'Select cluster type & enter cluster name to create cluster', shows 'Kubernetes' selected and 'CIS-Benchmarking' entered in the 'Enter Cluster Name' field. Step 2, 'Agents Installation', includes sections for 'Runtime Visibility & Protection' (with KIEM and Kubernetes CIS Benchmark selected), 'Prerequisites' (listing 'helm' and 'token'), and 'Install CIS Benchmark Job'. A red box highlights the terminal command provided:

```

1 helm upgrade --install cis-k8s-job oci://public.ecr.aws/k9v9d5v2/cis-k8s-job \
2   --set accuknox.url="cspm.demo.accuknox.com" \
3   --set accuknox.tenantId="167" \
4   --set accuknox.authToken="" \
5   --set accuknox.cronTab="0 9 * * *" \
6   --set accuknox.clusterName="CIS-Benchmarking" \
7   --version v1.1.3

```

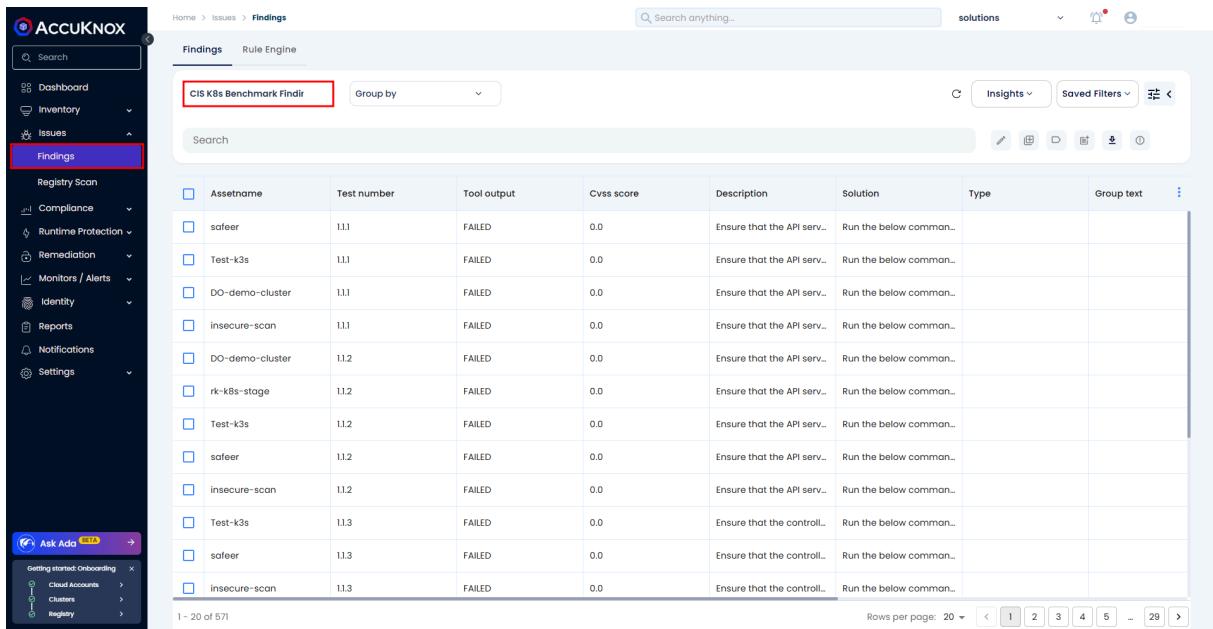
The command is intended for Helm upgrade, setting the URL to the public ECR repository, specifying the tenant ID, and defining a cron tab for the CIS benchmark job. The cluster name is set to 'CIS-Benchmarking'.

2. Run this command in your terminal on a machine that has access to your Kubernetes cluster. The command will schedule the scan for CIS Benchmarking compliance.
3. Once the Helm installation is complete, return to the AccuKnox platform and click **Finish**.

Step 4: View Compliance Findings

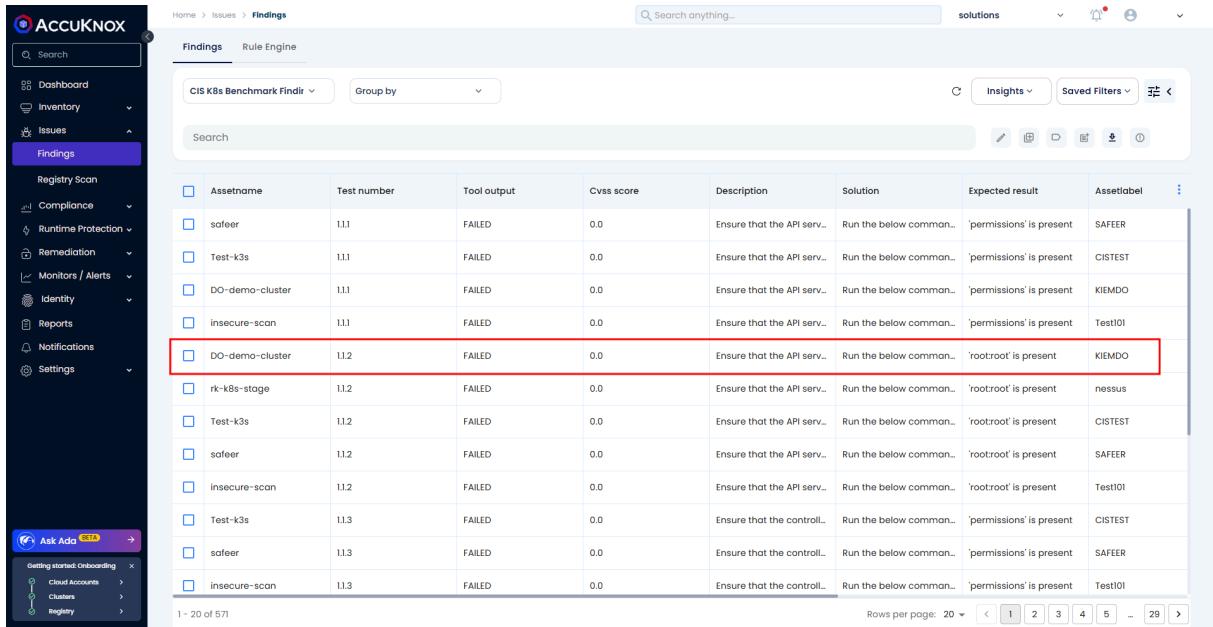
After the initial scan is completed, you can view the compliance results:

1. Go to **Issues > Findings** in AccuKnox.
2. Use the **Findings** dropdown to filter and select CIS k8s Benchmarking finding results.

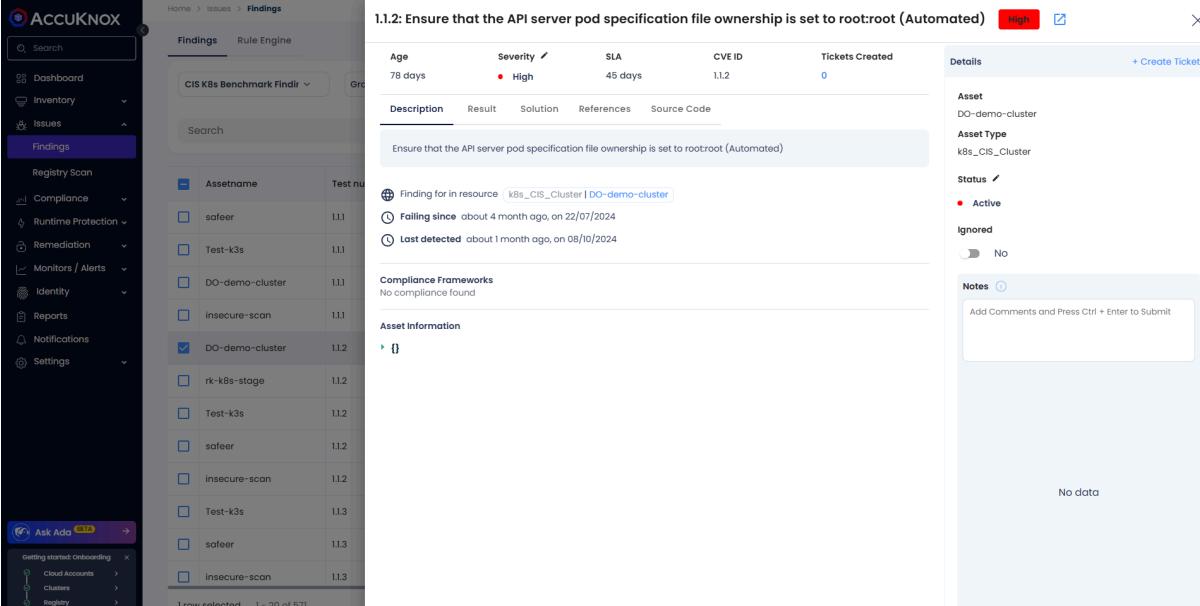


Assetname	Test number	Tool output	CVSS score	Description	Solution	Type	Group text
safeer	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...		
Test-k3s	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...		
DO-demo-cluster	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...		
insecure-scan	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...		
DO-demo-cluster	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...		
rk-k8s-stage	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...		
Test-k3s	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...		
safeer	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...		
insecure-scan	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...		
Test-k3s	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...		
safeer	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...		
insecure-scan	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...		

3. Each result will provide details on specific CIS controls and any non-compliant configurations detected.



Assetname	Test number	Tool output	CVSS score	Description	Solution	Expected result	Assetlabel
safeer	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...	'permissions' is present	SAFEER
Test-k3s	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...	'permissions' is present	CISTEST
DO-demo-cluster	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...	'permissions' is present	KIEMDO
insecure-scan	I.1.1	FAILED	0.0	Ensure that the API serv...	Run the below command...	'permissions' is present	Test101
DO-demo-cluster	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...	'rootroot' is present	KIEMDO
rk-k8s-stage	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...	'rootroot' is present	nessus
Test-k3s	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...	'rootroot' is present	CISTEST
safeer	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...	'rootroot' is present	SAFEER
insecure-scan	I.1.2	FAILED	0.0	Ensure that the API serv...	Run the below command...	'rootroot' is present	Test101
Test-k3s	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...	'permissions' is present	CISTEST
safeer	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...	'permissions' is present	SAFEER
insecure-scan	I.1.3	FAILED	0.0	Ensure that the controll...	Run the below command...	'permissions' is present	Test101



1.1.2: Ensure that the API server pod specification file ownership is set to root:root (Automated)

High  

Age	Severity	SLA	CVE ID	Tickets Created
78 days	High	45 days	1.1.2	0

Description **Result** **Solution** **References** **Source Code**

Ensure that the API server pod specification file ownership is set to root:root (Automated)

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

Failing since: about 4 month ago, on 22/07/2024

Last detected: about 1 month ago, on 08/10/2024

Compliance Frameworks: No compliance found

Asset Information

- DO-demo-cluster
- rk-k8s-stage
- Test-k3s
- safeer
- insecure-scan
- Test-k3s
- safeer
- insecure-scan
- Test-k3s
- safeer
- insecure-scan

1 row selected | 1 - 20 of 571

Asset: DO-demo-cluster
Asset Type: k8s_CIS_Cluster
Status: Active
Ignored: No

Notes  Add Comments and Press Ctrl + Enter to Submit

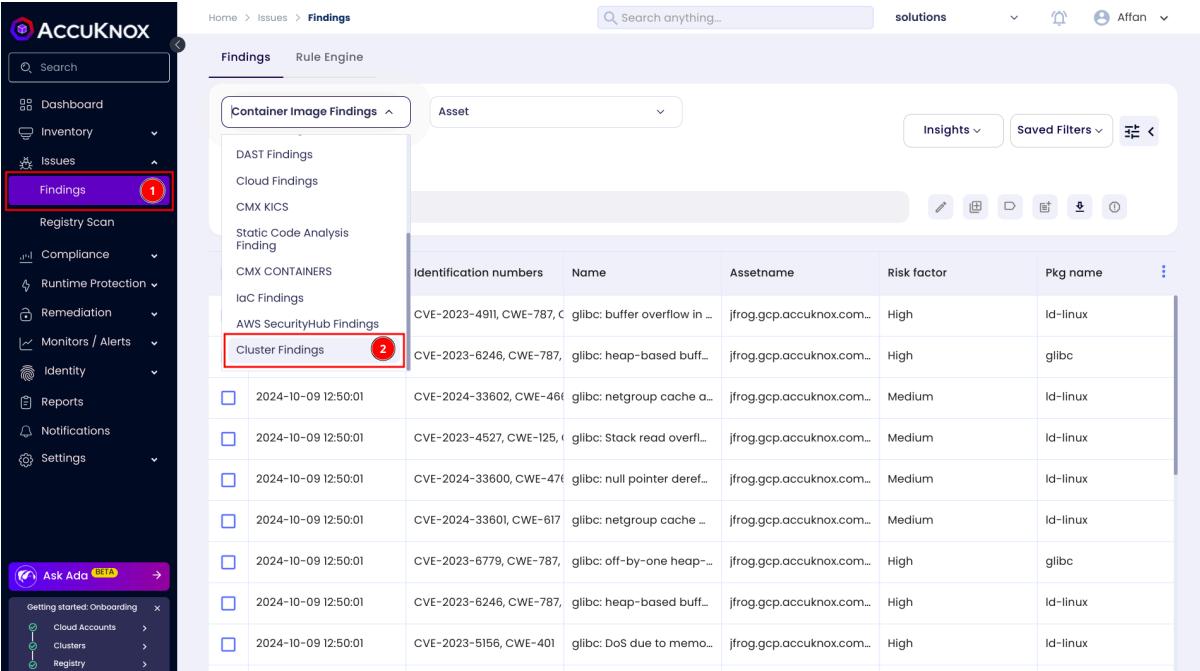
No data

This completes the onboarding process for CIS Benchmarking compliance scanning. You can review findings regularly to maintain and improve your cluster's CIS compliance.

12.2 Cluster Misconfiguration Scanning

Cyber attacks frequently occur due to security misconfigurations in applications and infrastructure. Preventing these vulnerabilities is crucial for maintaining a secure environment. AccuKnox empowers you to identify and remediate security misconfigurations within your Kubernetes clusters, ensuring that your applications and infrastructure are fully protected from potential threats.

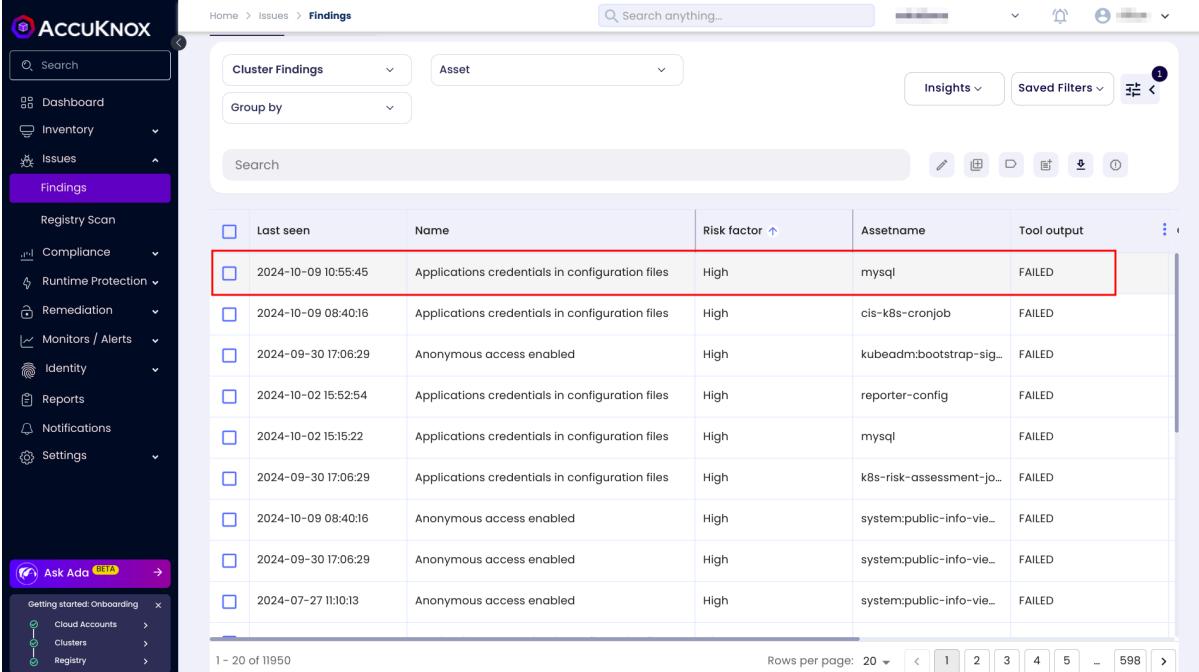
In AccuKnox you can go to findings page and select the cluster findings to list all of the cluster misconfiguration findings.



The screenshot shows the AccuKnox web interface. On the left, there's a dark sidebar with various navigation options like Dashboard, Inventory, Issues, Findings (which has a red box around it and a red number '1' in a circle), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. Below this is an 'Ask Ada' button. At the bottom of the sidebar, there's an 'Onboarding' section with Cloud Accounts, Clusters, and Registry. The main content area is titled 'Findings' and shows a table of findings. The table has columns for Identification numbers, Name, Assetname, Risk factor, and Pkg name. There are 10 rows of data, each with a checkbox and some descriptive text. A red box surrounds the 'Cluster Findings' button in the sidebar, and a red number '2' is in a circle next to it.

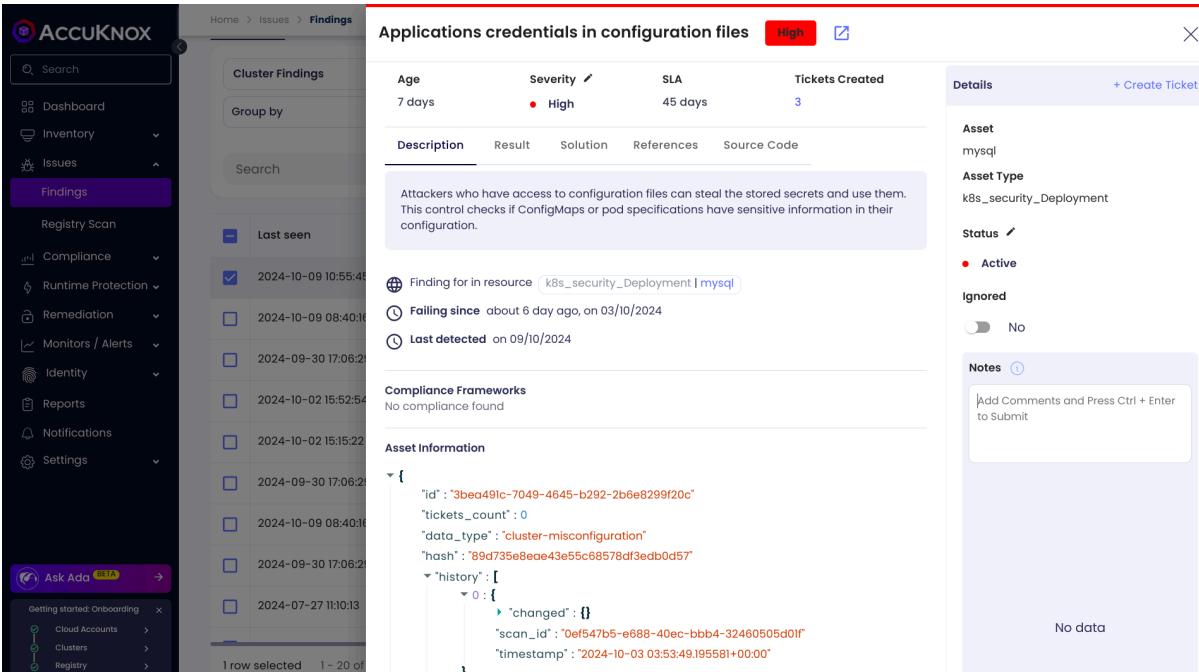
Identification numbers	Name	Assetname	Risk factor	Pkg name
CVE-2023-4911, CWE-787, C	glibc: buffer overflow in ...	jfrog.gcp.accuknox.com...	High	ld-linux
CVE-2023-6246, CWE-787,	glibc: heap-based buff...	jfrog.gcp.accuknox.com...	High	glibc
2024-10-09 12:50:01	CVE-2024-33602, CWE-46	glibc: netgroup cache a...	Medium	ld-linux
2024-10-09 12:50:01	CVE-2023-4527, CWE-125,	glibc: Stack read overfl...	Medium	ld-linux
2024-10-09 12:50:01	CVE-2024-33600, CWE-476	glibc: null pointer deref...	Medium	ld-linux
2024-10-09 12:50:01	CVE-2024-33601, CWE-617	glibc: netgroup cache ...	Medium	ld-linux
2024-10-09 12:50:01	CVE-2023-6779, CWE-787,	glibc: off-by-one heap-...	High	glibc
2024-10-09 12:50:01	CVE-2023-6246, CWE-787,	glibc: heap-based buff...	High	ld-linux
2024-10-09 12:50:01	CVE-2023-5156, CWE-401	glibc: DoS due to memo...	High	ld-linux

You can click on a finding to see more details about it.



The screenshot shows the AccuKnox interface under the 'Findings' section. The left sidebar includes options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A purple 'Ask Ada' button is also present. The main area displays a table of findings with columns: Last seen, Name, Risk factor, Assetname, and Tool output. One row is highlighted with a red border, corresponding to the detailed view shown below.

Last seen	Name	Risk factor	Assetname	Tool output
2024-10-09 10:55:45	Applications credentials in configuration files	High	mysql	FAILED
2024-10-09 08:40:16	Applications credentials in configuration files	High	cis-k8s-cronjob	FAILED
2024-09-30 17:06:29	Anonymous access enabled	High	kubeadm:bootstrap-sig...	FAILED
2024-10-02 15:52:54	Applications credentials in configuration files	High	reporter-config	FAILED
2024-10-02 15:15:22	Applications credentials in configuration files	High	mysql	FAILED
2024-09-30 17:06:29	Applications credentials in configuration files	High	k8s-risk-assessment-jo...	FAILED
2024-10-09 08:40:16	Anonymous access enabled	High	system:public-info-vie...	FAILED
2024-09-30 17:06:29	Anonymous access enabled	High	system:public-info-vie...	FAILED
2024-07-27 11:0:13	Anonymous access enabled	High	system:public-info-vie...	FAILED



The screenshot shows a detailed view of a finding for 'Applications credentials in configuration files' with a severity of High. The left sidebar is identical to the previous screenshot. The right panel provides more context, including the age of the finding (7 days), its status (Failing since about 6 days ago), and the last detected time (09/10/2024). It also lists compliance frameworks (none found) and asset information, which is displayed as a JSON object:

```

{
  "id": "3bea491c-7049-4645-b292-2b6e8299f20c",
  "tickets_count": 0,
  "data_type": "cluster-misconfiguration",
  "hash": "89d735e8eae43e55c68578df3edb0d7",
  "history": [
    {
      "changed": {},
      "scan_id": "0ef547b5-e688-40ec-bbb4-32460505d0f1",
      "timestamp": "2024-10-03 03:53:49.195581+00:00"
    }
  ]
}

```

Here AccuKnox detected the application credentials leaked in the Kubernetes configuration. By clicking on the source code tab you can see that there is a hard coded password in a deployment manifest.

The screenshot shows the AccuKnox platform interface. The left sidebar includes sections for Dashboard, Inventory, Issues (selected), Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A purple banner at the bottom left says "Ask Ada". The main content area has tabs for Home, Issues, and Findings. Under Findings, there are Cluster Findings and Group by options. A search bar is available. The main title is "Applications credentials in configuration files" with a severity of "High". The table has columns: Age (7 days), Severity (High), SLA (45 days), Tickets Created (3), Description, Result, Solution, References, and Source Code (highlighted with a red box). The table lists several findings, with the last one expanded to show its source code. The source code snippet highlights environment variable definitions:

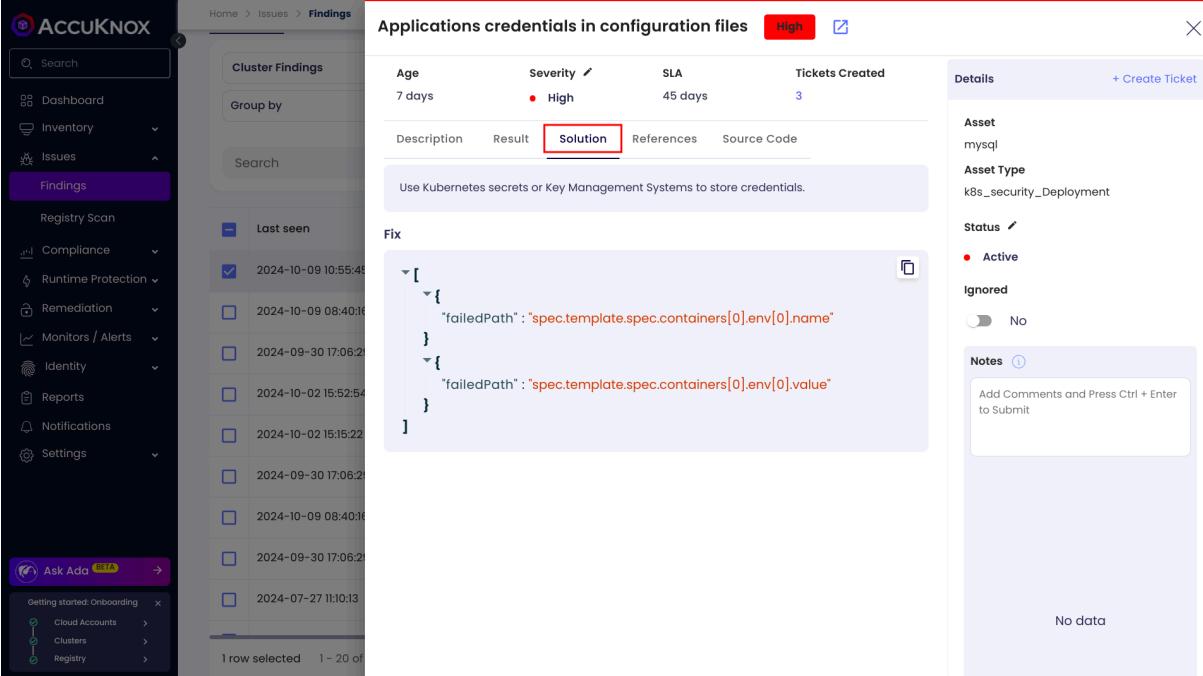
```
1 {
2     "kind": "Deployment",
3     "spec": {
4         "replicas": 1,
5         "selector": {
6             "matchLabels": {
7                 "app": "mysql"
8             }
9         },
10        "strategy": {
11            "type": "RollingUpdate",
12            "rollingUpdate": {
13                "maxSurge": "25%",
14                "maxUnavailable": "25%"
15            }
16        },
17        "template": {
18            "spec": {
19                "dnsPolicy": "ClusterFirst",
20                "containers": [
21                    {
22                        "env": [
23                            {
24                                "name": "MYSQL_ROOT_PASSWORD",
25                                "value": "XXXXXX"
26                            }
27                        ],
28                        "name": "mysql",
29                        "image": "mysql:5.6",
30                        "ports": [
31                            {
32                                "name": "mysql",
33                                "protocol": "TCP",
34                            }
35                        ]
36                    }
37                ]
38            }
39        }
40    }
41}
```

On the right, there are details for the asset: Asset mysql, Asset Type k8s_security_Deployment, Status Active, and Ignored. A note section says "Add Comments and Press Ctrl + Enter to Submit". At the bottom right, it says "No data".

An attacker can use these credentials and access your database. These sort of Kubernetes misconfigurations might get unnoticed by developers or DevOps engineers. By leveraging AccuKnox a user can detect vulnerabilities in time.

12.2.1 Remediation

AccuKnox provides you assistive remediation. Click on the solution tab and you will see what action can be preformed to remediate this issue.



The screenshot shows the AccuKnox interface. On the left is a sidebar with navigation links like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A purple 'Ask Ada' button is also present. The main area shows a 'Findings' view with a red border around the title 'Applications credentials in configuration files'. Inside, there are sections for 'Age' (7 days), 'Severity' (High), 'SLA' (45 days), and 'Tickets Created' (3). Below these are tabs for 'Description', 'Result' (highlighted in red), 'References', and 'Source Code'. A note says 'Use Kubernetes secrets or Key Management Systems to store credentials.' Under the 'Fix' section, there's a code snippet:

```

[{"failedPath": "spec.template.spec.containers[0].env[0].name"}, {"failedPath": "spec.template.spec.containers[0].env[0].value"}]

```

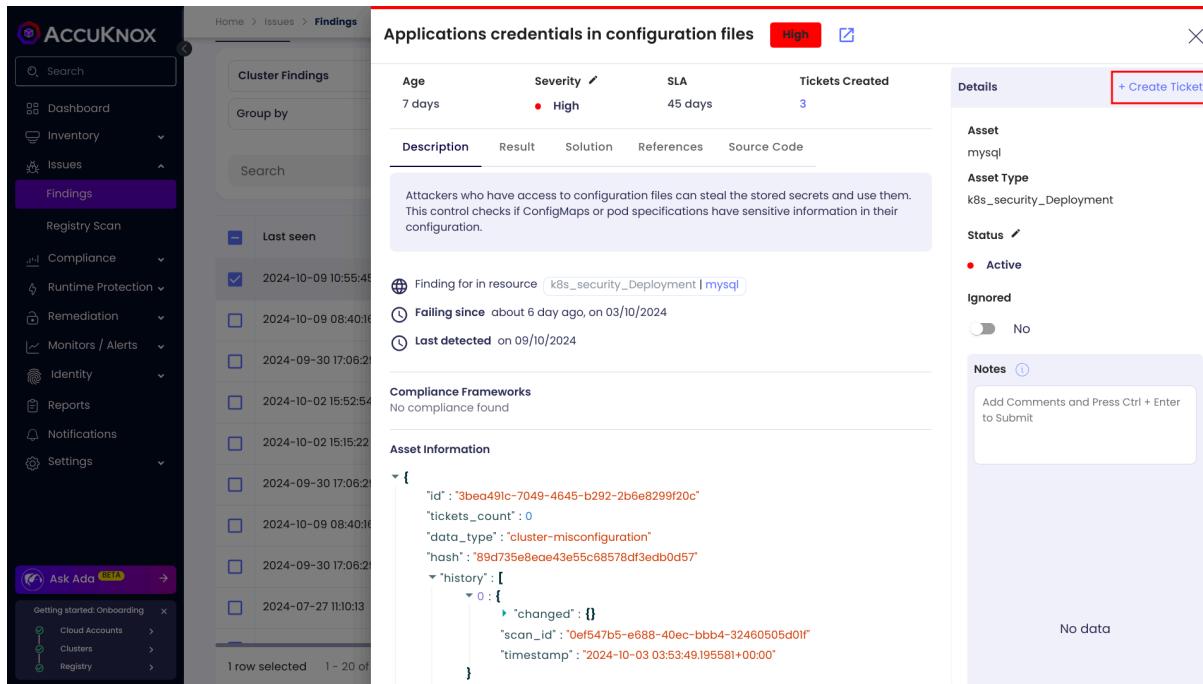
On the right, a 'Details' panel shows fields for 'Asset' (mysql), 'Asset Type' (k8s_security_Deployment), 'Status' (Active), and 'Ignored' (No). A 'Notes' section with a placeholder 'Add Comments and Press Ctrl + Enter to Submit' is also shown. At the bottom right of the main area, it says 'No data'.

12.2.2 Vulnerability Management Lifecycle

You can streamline vulnerability remediation and lifecycle management by creating Jira tickets directly from the AccuKnox UI.

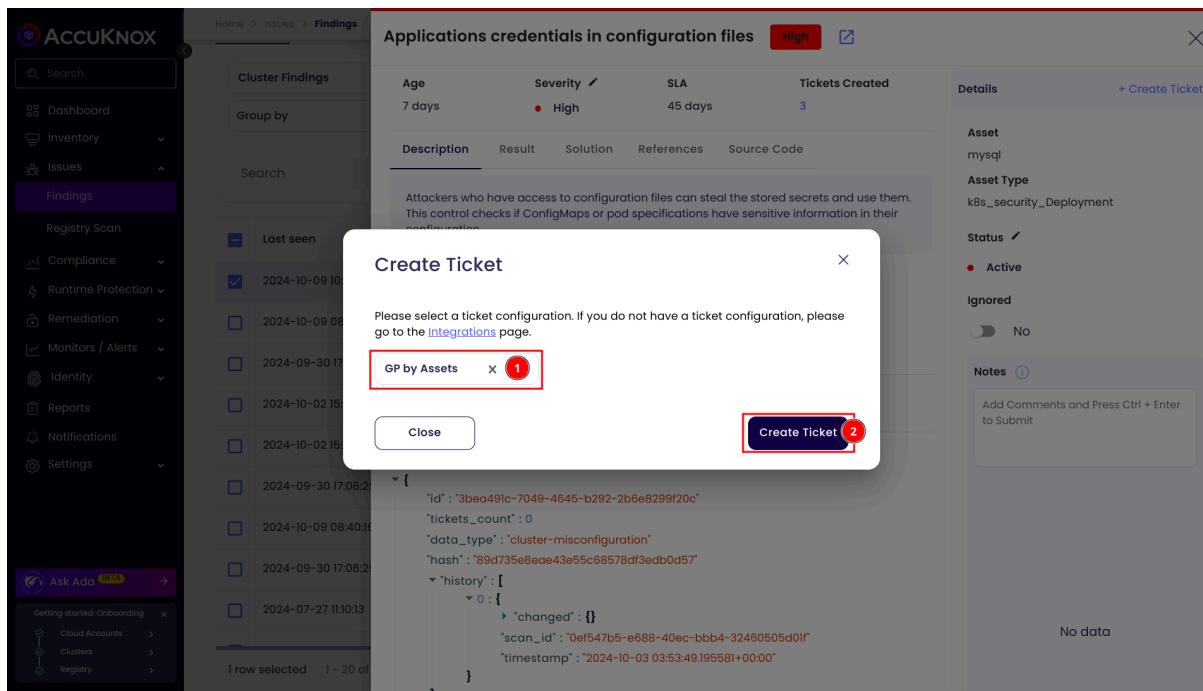
Follow these steps for creating a ticket.

Step 1. Select a vulnerability and click on the create ticket button.



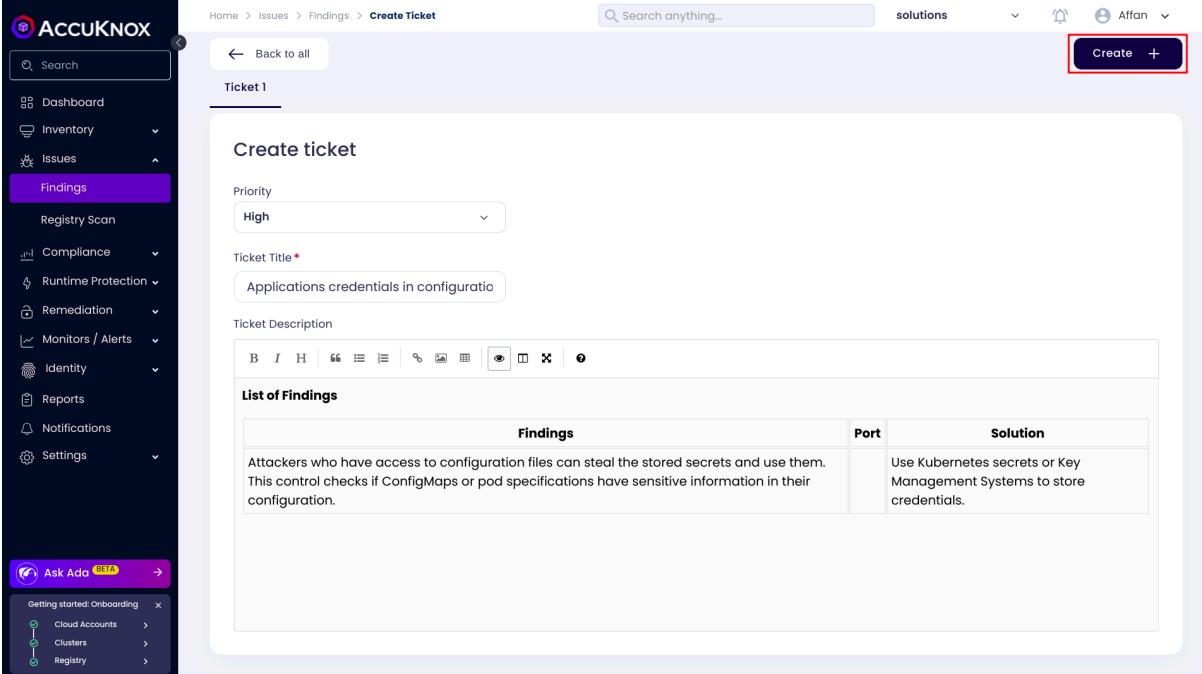
The screenshot shows the AccuKnox interface. On the left is a sidebar with navigation links like Dashboard, Inventory, Issues (selected), Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A central panel displays 'Cluster Findings' with a search bar and a 'Last seen' section showing several log entries from 2024-10-09 to 2024-07-27. Below this is a 'Compliance Frameworks' section stating 'No compliance found'. To the right is a detailed view of a finding titled 'Applications credentials in configuration files' (Severity: High). It includes tabs for Description, Result, Solution, References, and Source Code. The 'Description' tab contains a note about stolen secrets in configuration files. The 'Result' tab lists findings such as 'Finding for resource k8s_security_Deployment | mysql', 'Failing since about 6 day ago, on 03/10/2024', and 'Last detected on 09/10/2024'. The 'Source Code' tab shows a JSON snippet of a configuration file. A 'Details' panel on the right shows asset information for 'mysql' (Asset Type: k8s_security_Deployment, Status: Active, Ignored: No) and a notes section. A red box highlights the '+ Create Ticket' button.

Step 2. Select your ticket configuration and click on the create ticket button.



This screenshot shows the same AccuKnox interface as above, but with a 'Create Ticket' modal open in the foreground. The modal has a title 'Create Ticket' and a message: 'Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page.' It contains two buttons: 'GP by Assets' (marked with a red circle 1) and 'Create Ticket' (marked with a red circle 2). The background shows the same findings list and details panel as the previous screenshot.

Step 3. It will open up a new tab where you can review and modify the ticket details. Once you have reviewed the ticket click on the create button.



Home > Issues > Findings > **Create Ticket**

← Back to all

Ticket 1

Create ticket

Priority: High

Ticket Title*: Applications credentials in configuratio

Ticket Description:

List of Findings

Findings	Port	Solution
Attackers who have access to configuration files can steal the stored secrets and use them. This control checks if ConfigMaps or pod specifications have sensitive information in their configuration.		Use Kubernetes secrets or Key Management Systems to store credentials.

In conclusion, AccuKnox helps you to detect, remediate and manage the lifecycle of Kubernetes security misconfiguration vulnerabilities.

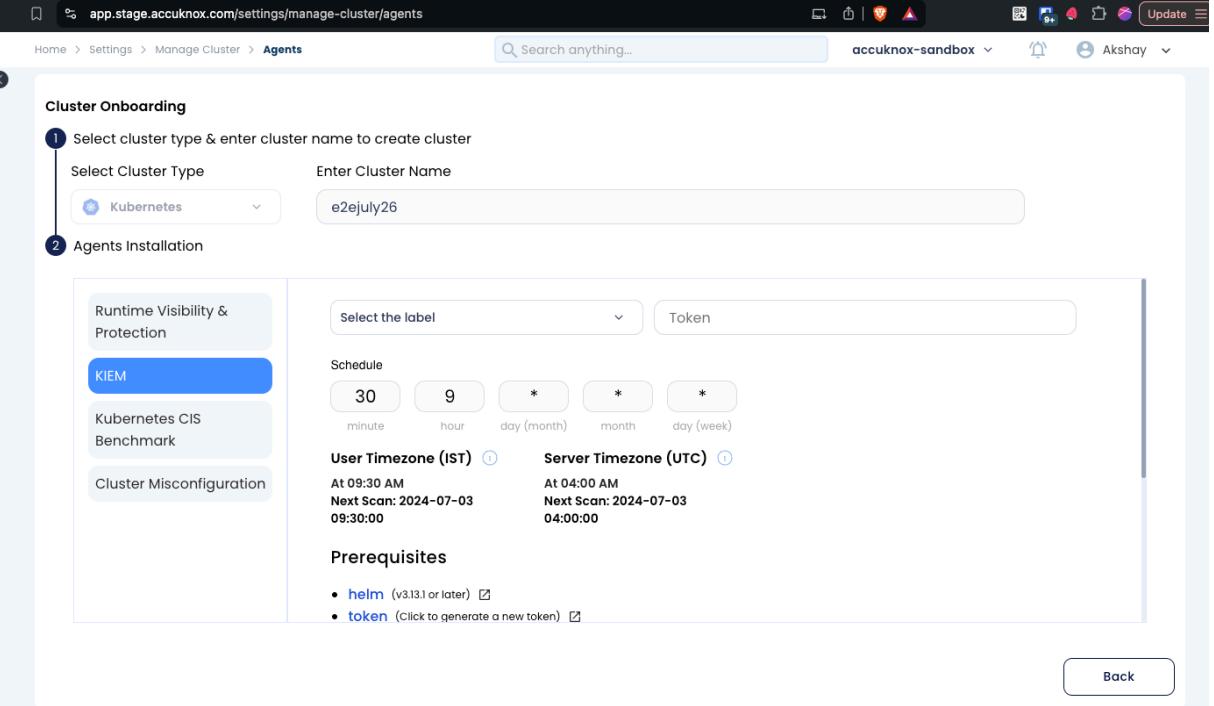
12.3 Kubernetes Identity and Entitlement Management (KIEM)

12.3.1. Onboarding Process

Follow these steps to set up and start using AccuKnox KIEM:

12.3.2 Install KIEM Agents

1. Navigate to the "Manage Cluster" section in your AccuKnox dashboard.
2. Select the target cluster for KIEM installation.
3. Install the KIEM job on the selected cluster.
4. Set up and schedule the cron job for regular scans.



The screenshot shows the 'Cluster Onboarding' page in the AccuKnox dashboard. The URL is app.stage.accuknox.com/settings/manage-cluster/agents. The page title is 'Cluster Onboarding'. Step 1: 'Select cluster type & enter cluster name to create cluster'. Under 'Select Cluster Type', 'Kubernetes' is selected. Under 'Enter Cluster Name', the value 'e2ejuly26' is entered. Step 2: 'Agents Installation'. A sidebar on the left lists 'Runtime Visibility & Protection', 'KIEM' (which is highlighted in blue), 'Kubernetes CIS Benchmark', and 'Cluster Misconfiguration'. The main area shows 'Select the label' dropdown set to 'Token'. The 'Schedule' section shows a cron expression: '30 9 * * *'. Below it, 'User Timezone (IST)' shows 'At 09:30 AM' and 'Next Scan: 2024-07-03 09:30:00'. 'Server Timezone (UTC)' shows 'At 04:00 AM' and 'Next Scan: 2024-07-03 04:00:00'. The 'Prerequisites' section lists 'helm (v3.13.1 or later)' and 'token (Click to generate a new token)'. At the bottom right is a 'Back' button.

12.3.3 Post-Onboarding Steps

After completing the onboarding process:

1. Wait for the initial KIEM cron job to complete its first scan.
2. Once the scan is finished, navigate to the "Identity > KIEM" section in your dashboard.
3. Review the initial findings and adjust configurations as necessary.

12.3.4 Permissions Overview

- Summarizes all permissions in a unified view.
- Rolebinding and workloads are connected to permissions.
- Filter on constraints such as Role, Resource, ApiGroup, Verbs, Rolebinding, Service Accounts, Workload.
- View distilled permission summary for filtered entities.

Cluster: kiem-test | Key Query: Overview | Entity Type: Select from Key Queries | Search for any element: Search... | Filter: List (selected) | Graph

Subject	RoleBinding	Role	Rule	
			Verb	Resource
 service-controller Scope: kube-system	 system:controller:service-controller Scope: cluster_wide	 system:controller:service-controller Scope: cluster_wide	patch, update	services/status
			create, patch, update	events
			get, list, watch	services
			create, patch, update	events
			list, watch	nodes
 ephemeral-volume-controller Scope: kube-system	 system:controller:ephemeral-volume-controller Scope: cluster_wide	 system:controller:ephemeral-volume-controller Scope: cluster_wide	create, patch, update	events
			get, list, watch	pods
			create, patch, update	events
			create, get, list, watch	persistentvolumeclaims
			update	pods/finalizer
 legacy-service-account-token-cleaner	 system:controller:legacy-service-account-token-cleaner	 system:controller:legacy-service-account-token-cleaner	delete, patch	secrets

Current Page: 1 | Prev | Next

Cluster: kiem-test | Key Query: Overview | Entity Type: Select from Key Queries | Search for any element: Search... | Filter: List | Graph

Verb: contains delete | **Resource:** contains secrets | **Search Namespace:** service- | **Apply**

Rule	Verb	Resource
	service-	delete, patch
delete	secrets	
delete, get, list, watch	secrets	

+ Add Query

Current Page: 1 | Prev | Next

12.3.5 Key Queries

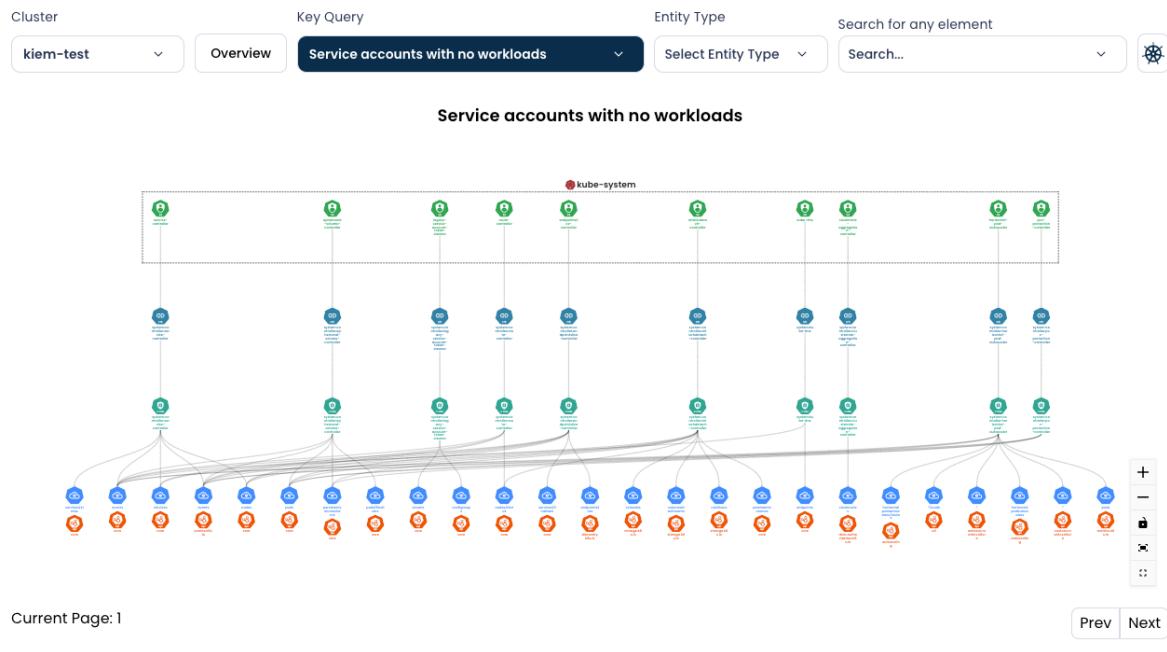
Our KIEM solution includes predefined queries that can detect security risks, misconfigurations, or compliance issues within Kubernetes RBAC configurations.. These prebuilt queries aid in maintaining Kubernetes RBAC configurations with security as a primary factor.

Examples:

- **Identify Service Accounts not connected to any workloads** (indicator of dormant excessive permissions).
- **Identify principals with excessive privileges**. Excessive privileges in Kubernetes can increase the risk of security breaches, as overprivileged users or processes can misuse their access, leading to data breaches, service disruptions, or unauthorized changes in the cluster.
- **Find roles that have permissions to modify workload resources**. Excessive access rights to Kubernetes workload resources can lead to security vulnerabilities, allowing unauthorized access or modifications to critical applications and data, undermining the cluster's security posture.
- **List roles that have read access to Kubernetes secrets**. Kubernetes secrets, often containing sensitive information like passwords, tokens, or encryption keys, can pose a significant security risk if read access to these

roles is compromised, potentially leading to data leakage or unauthorized system access.

- **Identify roles that are not in use.** Unused roles can pose security risks if not regularly audited and cleaned up, potentially accumulating unnecessary permissions or becoming a target for exploitation by attackers.

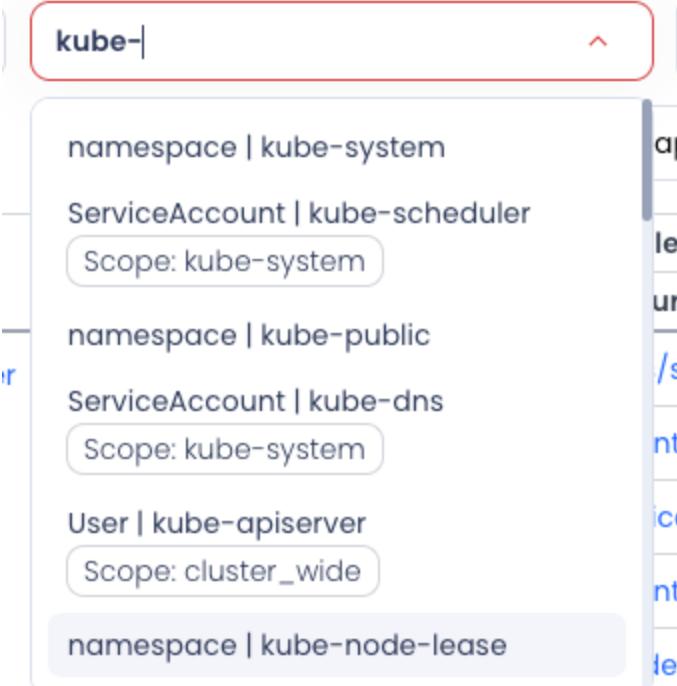


12.3.6 Full-text Search

Search across all RBAC entities:

- ServiceAccounts
- RoleBindings
- Roles And more

Search for any element



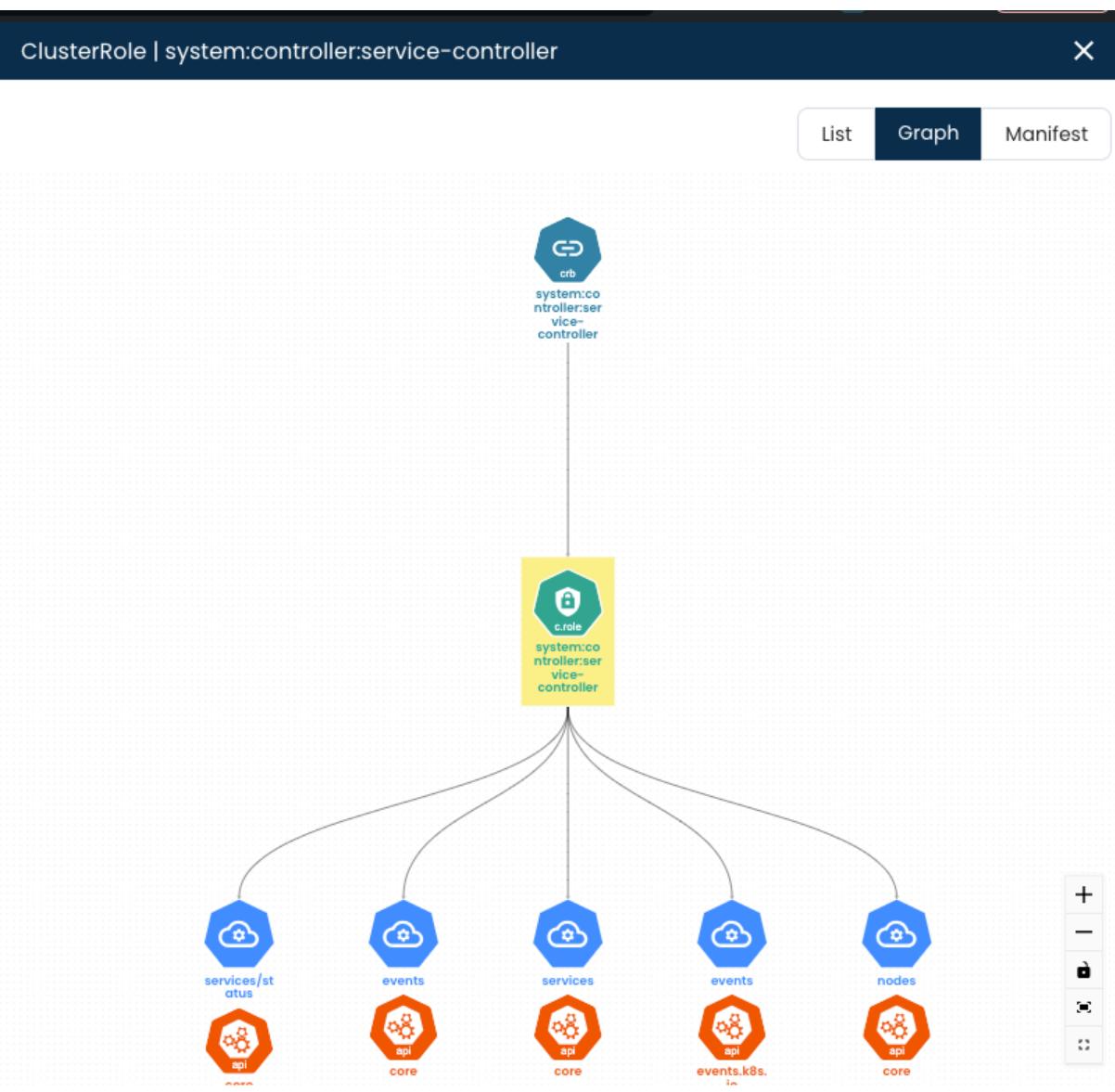
The screenshot shows a search interface with a red border around the search input field. The input field contains the text "kube-". Below the input field is a list of search results:

- namespace | kube-system
- ServiceAccount | kube-scheduler
 - Scope: kube-system
- namespace | kube-public
- ServiceAccount | kube-dns
 - Scope: kube-system
- User | kube-apiserver
 - Scope: cluster_wide
- namespace | kube-node-lease

On the right side of the search results, there is a vertical scroll bar with some blue text visible.

12.3.7 Entity Exploration

- View connections and manifest for select entities.
- Discover excessive permissions.



ClusterRole | system:controller:service-controller

X

List Graph Manifest

```
1 apiVersion: rbac.authorization.k8s.io/v1
2 kind: ClusterRole
3 metadata:
4   name: system:controller:service-controller
5   labels:
6     kubernetes.io/bootstrapping: rbac-defaults
7 rules:
8   - verbs:
9     - get
10    - list
11    - watch
12    apiGroups:
13      - ''
14    resources:
15      - services
16   - verbs:
17     - patch
18     - update
19     apiGroups:
20       - ''
21     resources:
22       - services/status
23   - verbs:
24     - list
25     - watch
26     apiGroups:
27       - ''
28     resources:
29       - nodes
30   - verbs:
31     - create
32     - patch
33     - update
```

- Explore all RBAC entities:
- Service Accounts
- Users
- Groups
- Roles
- RoleBindings

Cluster: kiem-test | Key Query: Overview | Entity Type: ServiceAccount | Search: Search... | List | Graph

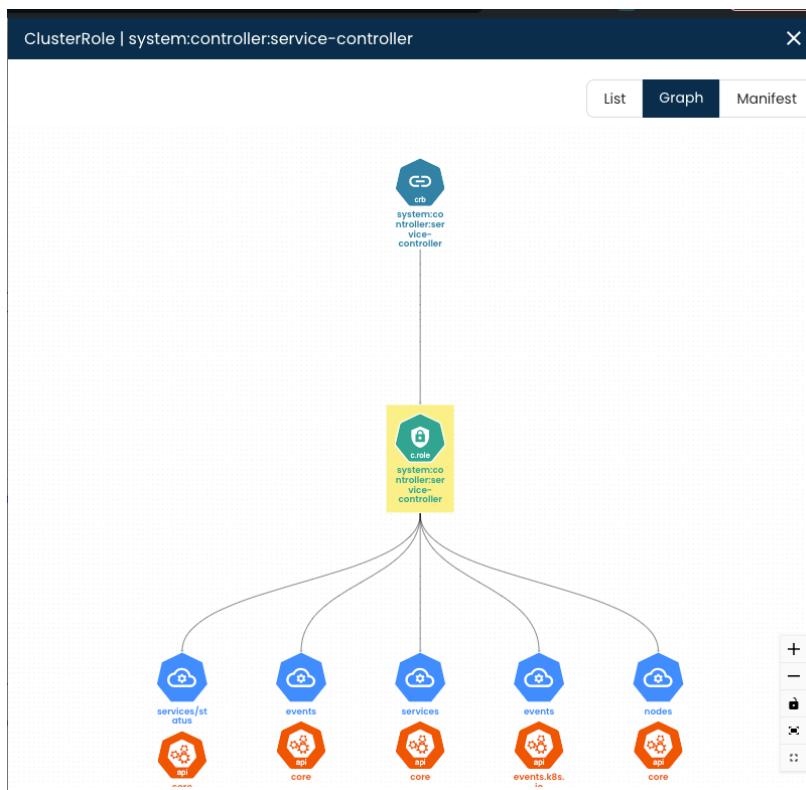
ServiceAccount

Name	Has Role Binding	Mounted By
<code>metrics-server</code> Scope: kube-system	<code>system:metrics-server</code> +1 Scope: cluster_wide	<code>metrics-server-54fd9b65b-prr6n</code> Scope: kube-system
<code>local-path-provisioner-service-account</code> Scope: kube-system	<code>local-path-provisioner-bind</code> Scope: cluster_wide	<code>local-path-provisioner-6c86858495-4cr4k</code> Scope: kube-system
<code>horizontal-pod-autoscaler</code> Scope: kube-system	<code>system:controller:horizontal-pod-autoscaler</code> Scope: cluster_wide	-
<code>pvc-protection-controller</code> Scope: kube-system	<code>system:controller:pvc-protection-controller</code> Scope: cluster_wide	-
<code>replication-controller</code> Scope: kube-system	<code>system:controller:replication-controller</code> Scope: cluster_wide	-
<code>bootstrap-signer</code> Scope: kube-system	<code>system:controller:bootstrap-signer</code> +1	-

Current Page: 1 | Prev | Next

12.3.8 Interactive Visualization

Open any entity and view all its connections by clicking on the link.

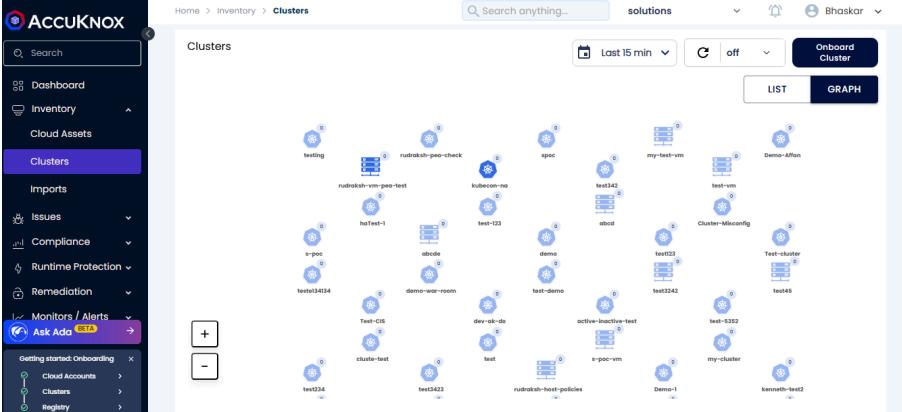


13. CWPP (Cloud Workload Protection Platform)

13.1 Cloud Workloads

13.1.1 How to find graph view of clusters

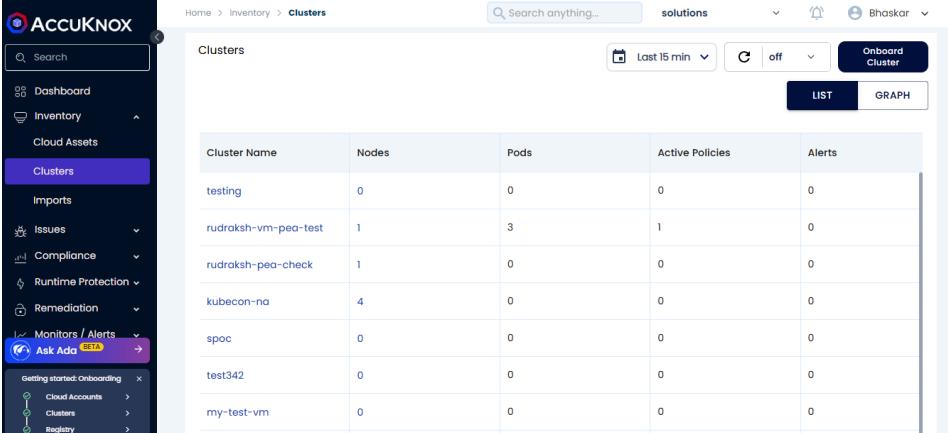
Navigate to Clusters screen under Inventory to view the clusters that have been onboarded:



The screenshot shows the 'Clusters' screen in the AccuKNOX interface. On the left is a sidebar with navigation links like Dashboard, Inventory, Cloud Assets, Clusters (which is selected and highlighted in purple), Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and Ask Ada. The main area is titled 'Clusters' and displays a graph view of various clusters. Each cluster is represented by a node with a blue circle icon and a name like 'testing', 'ruderaksh-pea-test', 'spoc', etc. The graph shows connections between these nodes. At the top right of the main area, there are buttons for 'Last 15 min', 'C off', 'Onboard Cluster', and tabs for 'LIST' (which is currently active) and 'GRAPH'. Below the graph, there are two buttons: a plus sign for adding a cluster and a minus sign for removing one.

13.1.2 How to find list view of clusters

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



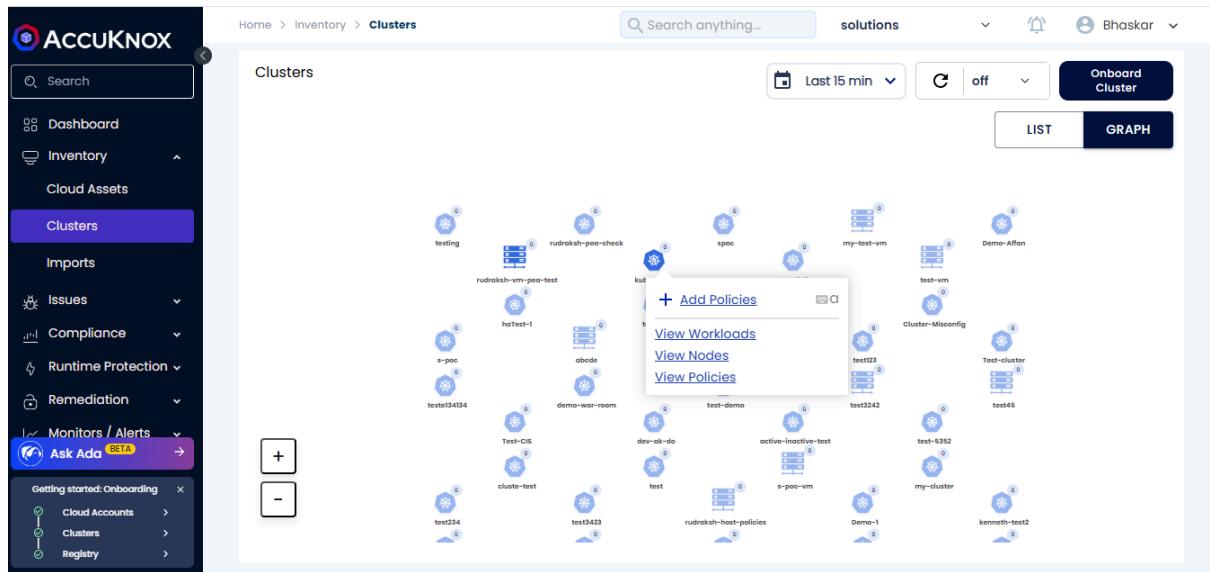
The screenshot shows the same 'Clusters' screen from the previous image, but the 'LIST' tab is now active. The main area now displays a table with columns for Cluster Name, Nodes, Pods, Active Policies, and Alerts. The data rows correspond to the clusters shown in the graph view. The table has 7 rows, each representing a cluster with its respective details.

Cluster Name	Nodes	Pods	Active Policies	Alerts
testing	0	0	0	0
ruderaksh-pea-test	1	3	1	0
ruderaksh-pea-check	1	0	0	0
kubecon-na	4	0	0	0
spoc	0	0	0	0
test342	0	0	0	0
my-test-vm	0	0	0	0

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

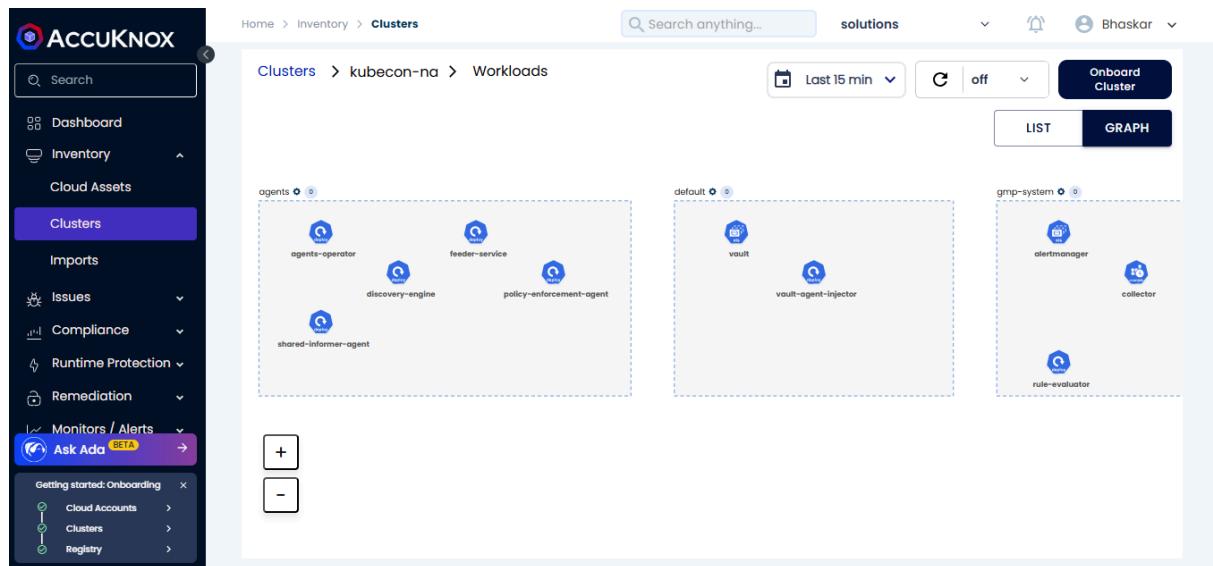
13.1.3 How to find details on cluster

- Clicking on any of the clusters gives more information about the cluster:



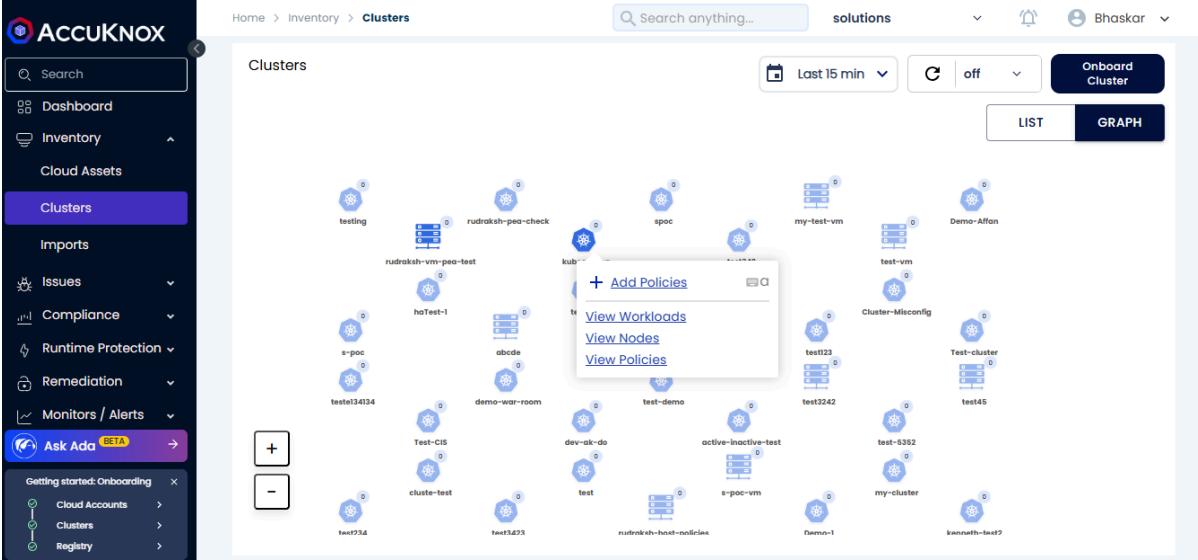
The screenshot shows the ACCUKNOKX interface with the 'Clusters' section selected. A context menu is open over a cluster named 'int'. The menu options are: + Add Policies, View Workloads, View Nodes, and View Policies.

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

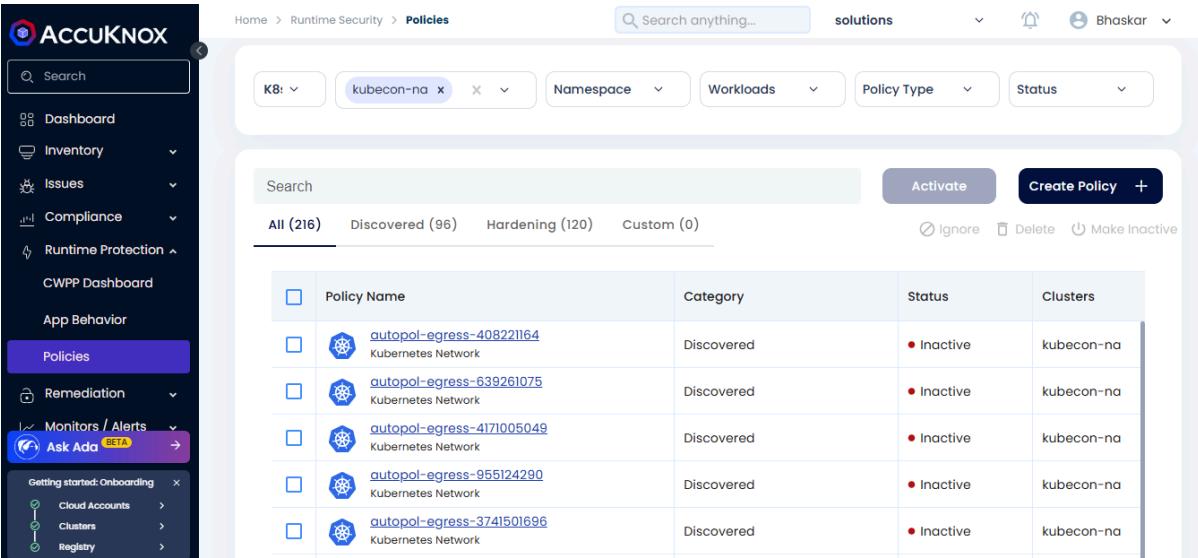


The screenshot shows the ACCUKNOKX interface with the 'Clusters' > 'kubecon-na' > 'Workloads' path selected. The page displays three namespaces: 'agents', 'default', and 'gmp-system', each containing specific pods like agents-operator, feeder-service, etc.

- View Policies can be clicked to jump to the Policies screen to show the policies for the selected cluster or pod. Click on the cluster name and then click on View Policies.



The screenshot shows the ACCUKNOKX platform's Cloud Assets section, specifically the Clusters view. On the left, there's a sidebar with navigation links like Dashboard, Inventory, Cloud Assets (Clusters), Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and an Ask Ada BETA button. The main area displays a grid of cluster names and icons. A context menu is open over the 'kubernetes' cluster, listing 'Add Policies', 'View Workloads', 'View Nodes', and 'View Policies'. The top right features a search bar, a 'solutions' dropdown, a user profile for Bhaskar, and a 'Onboard Cluster' button. Below the search bar are filters for 'Last 15 min', a refresh icon, and a 'LIST' or 'GRAPH' switch.

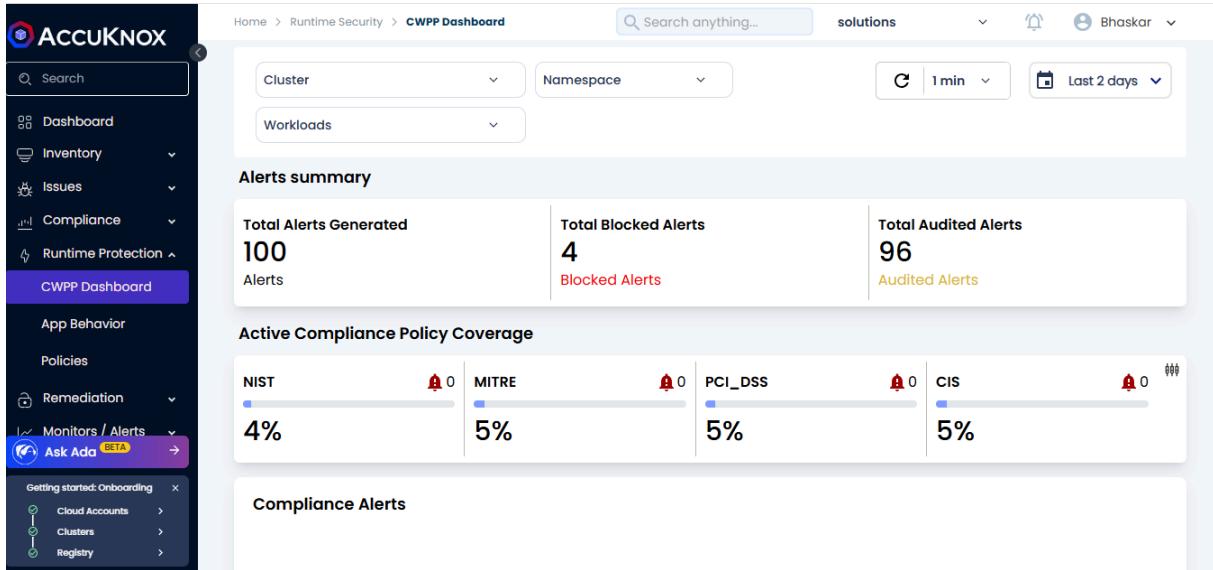


The screenshot shows the ACCUKNOKX platform's Runtime Security section, specifically the Policies view. The left sidebar includes links for Dashboard, Inventory, Issues, Compliance, Runtime Protection, CWPP Dashboard, App Behavior (Policies selected), Remediation, Monitors / Alerts, and an Ask Ada BETA button. The main area features a search bar and several filter buttons: K8s, kubecon-na, Namespace, Workloads, Policy Type, and Status. Below these are buttons for Search, Activate, Create Policy, Ignore, Delete, and Make Inactive. A table lists policies with the following data:

All (216)	Discovered (96)	Hardening (120)	Custom (0)	
<input type="checkbox"/> Autopol-Egress-408221164	Kubernetes Network	Discovered	Inactive	kubecon-na
<input type="checkbox"/> Autopol-Egress-639261075	Kubernetes Network	Discovered	Inactive	kubecon-na
<input type="checkbox"/> Autopol-Egress-4171005049	Kubernetes Network	Discovered	Inactive	kubecon-na
<input type="checkbox"/> Autopol-Egress-955124290	Kubernetes Network	Discovered	Inactive	kubecon-na
<input type="checkbox"/> Autopol-Egress-3741501696	Kubernetes Network	Discovered	Inactive	kubecon-na

13.1.4 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.



The screenshot shows the AccuKnox CWPP Dashboard. On the left is a sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection, CWPP Dashboard (which is selected and highlighted in purple), App Behavior, Policies, Remediation, Monitors / Alerts, and Ask Ada (BETA). Below the sidebar is a "Getting started: Onboarding" section with links for Cloud Accounts, Clusters, and Registry. The main dashboard area has a header with "Home > Runtime Security > CWPP Dashboard", a search bar, and user information for "Bhaskar". It includes filters for "Cluster", "Namespace", "Workloads", and time periods ("1 min" and "Last 2 days"). Below the header is an "Alerts summary" section with three boxes: "Total Alerts Generated 100 Alerts", "Total Blocked Alerts 4 Blocked Alerts", and "Total Audited Alerts 96 Audited Alerts". Underneath is a "Active Compliance Policy Coverage" section with four horizontal progress bars: NIST (4%), MITRE (5%), PCI_DSS (5%), and CIS (5%). Each bar has a red bell icon indicating 0 alerts. At the bottom is a "Compliance Alerts" section which is currently empty.

13.2 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 namespace. Application behavior of the cluster workloads are given in two ways, one is the list view and other is the Graphical view.

13.2.1 How to interpret network graph

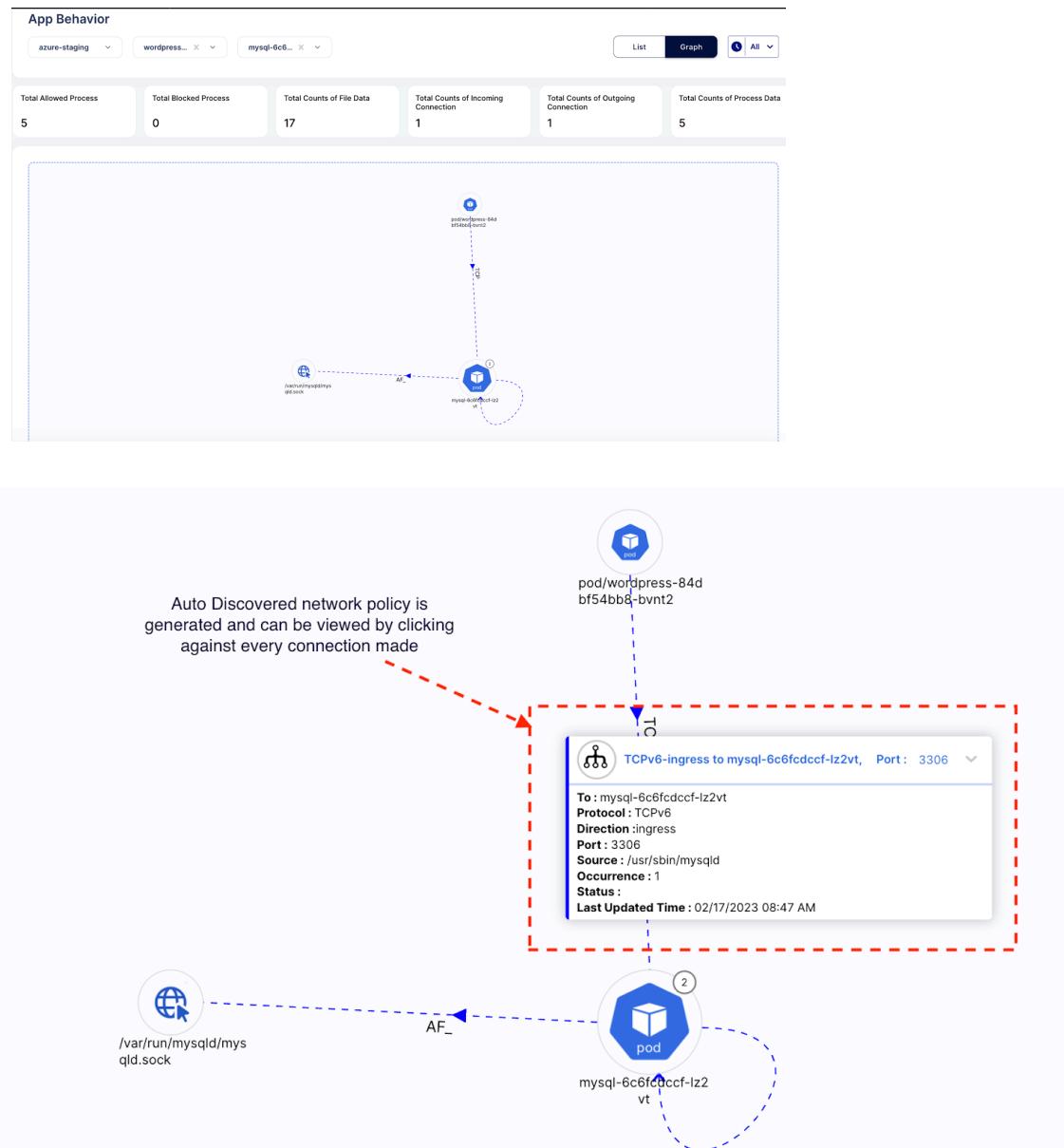
Lets understand this by following use-case example - **Auditing Application Behavior of MySQL application**

1. Install workload:

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

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

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



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

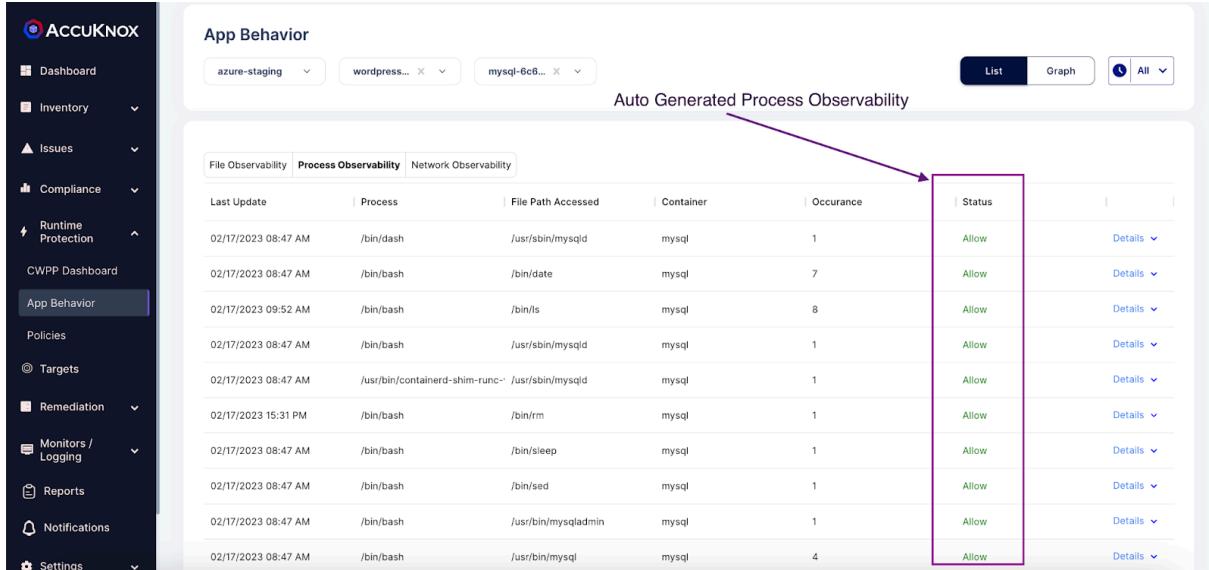
App Behavior

Auto Generated Whitelisted Application Behaviour

Show Aggregated View

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

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



App Behavior

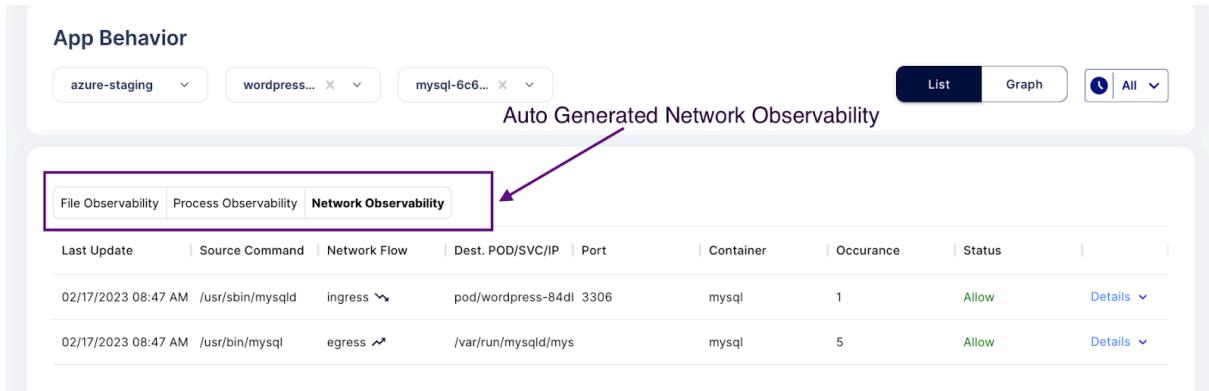
azure-staging wordpress... mysql-6c6...

List Graph All

Auto Generated Process Observability

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

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



App Behavior

azure-staging wordpress... mysql-6c6...

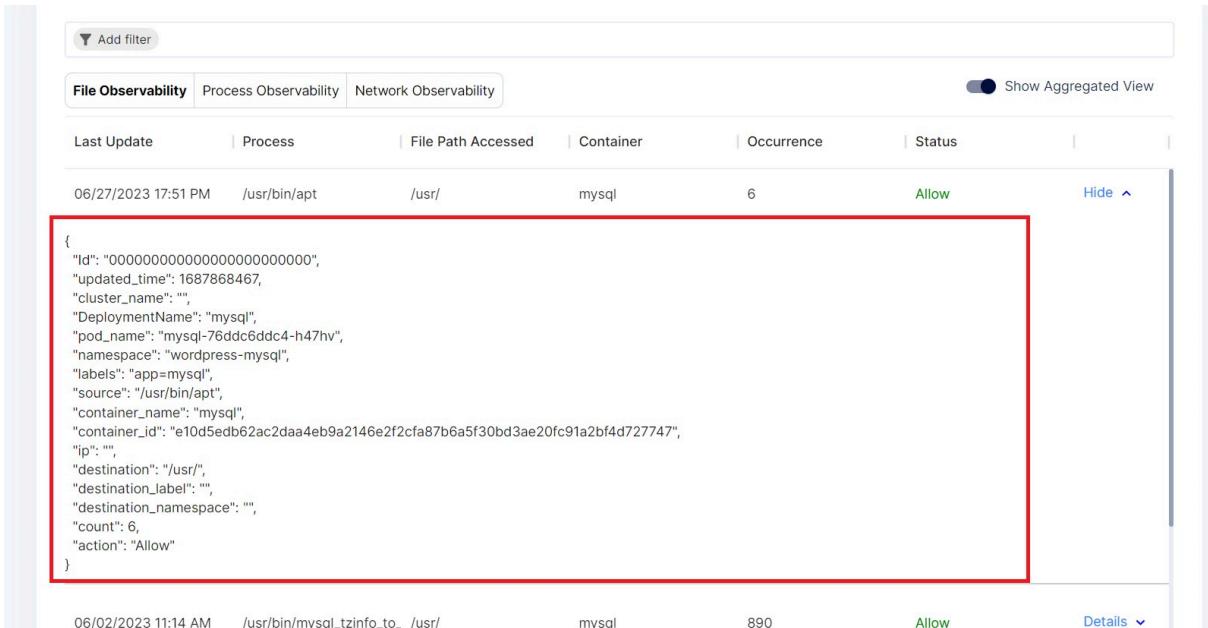
List Graph All

Auto Generated Network Observability

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

13.2.2 How to see App Behavior Telemetry

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



The screenshot shows a list of file access events. One event is highlighted with a red box, showing its detailed JSON structure. The event details are as follows:

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

- **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

▼ Add filter File Observability Process Observability Network Observability							
Last Update	Process	File Path Accessed	Container	Occurrence	Status		
06/02/2023 11:14 AM	/bin/bash	/bin/sed	mysql	1	Allow		Hide ^
<pre>{ "Id": "6479820c3d3aeb2df0a112", "updated_time": 1685684643, "cluster_name": "aks-demo-prod", "DeploymentName": "mysql", "pod_name": "mysql-76ddc6ddc4-h47hv", "namespace": "wordpress-mysql", "labels": "app=mysql", "source": "/bin/bash", "container_name": "mysql", "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747", "ip": "", "destination": "/bin/sed", "destination_label": "", "destination_namespace": "", "count": 1, "action": "Allow" }</pre>							

- 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

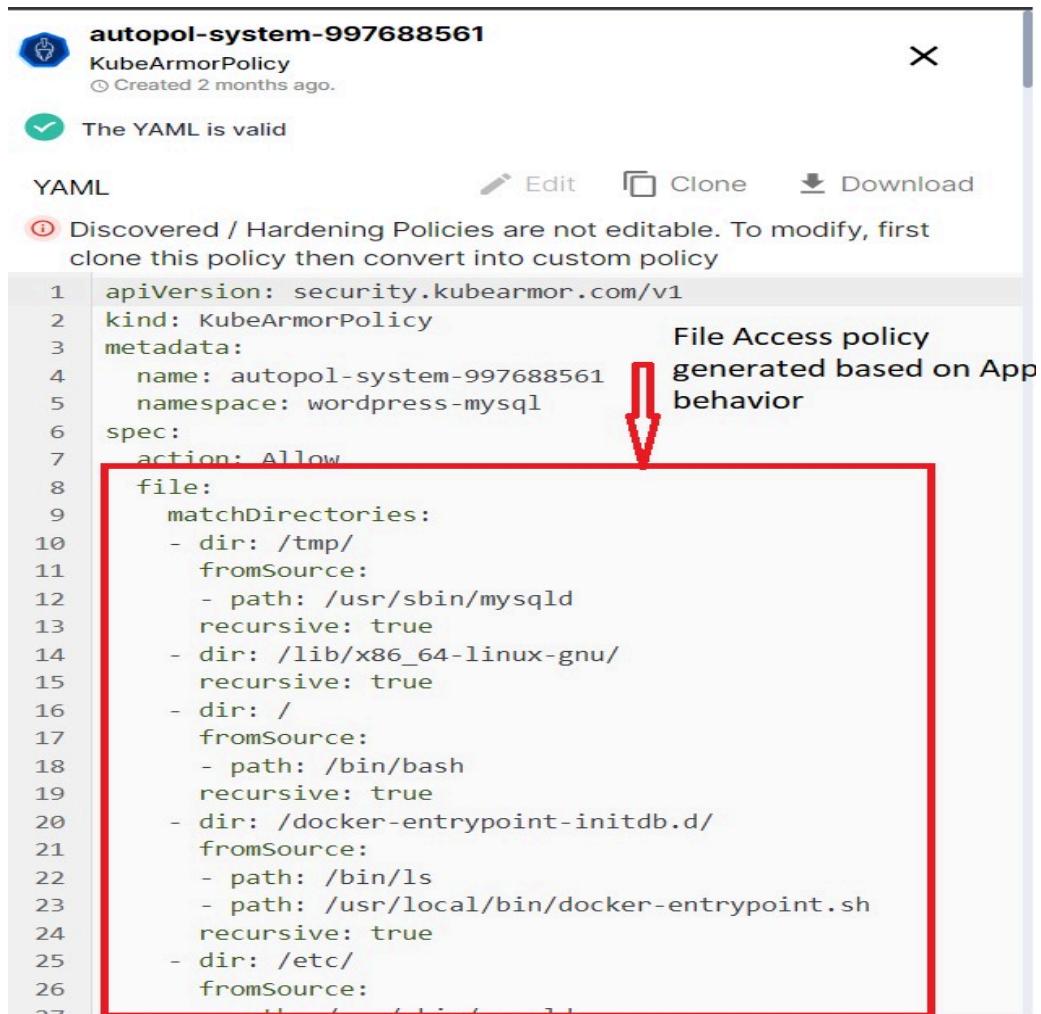
▼ Add filter File Observability Process Observability Network Observability							
Last Update	Source Command	Network Flow	Dest. POD/SVC/IP	Port	Container	Occurrence	Status
06/02/2023 11:14 AM	/usr/bin/mysql	egress ↗	/var/run/mysqld/mysc		mysql	2	Allow
07/06/2023 15:47 PM	/usr/bin/mysql	egress ↗	svc/wordpress	3306	mysql	2	Allow
<pre>{ "Id": "64a69475f181075cb4a563a3", "updated_time": 1688638674, "cluster_name": "", "DeploymentName": "mysql", "pod_name": "mysql-76ddc6ddc4-h47hv", "namespace": "wordpress-mysql", "labels": "app=mysql", "source": "/usr/bin/mysql", "nw_type": "egress", "container_name": "mysql", "container_id": "e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747", "ip": "svc/wordpress", "port": 3306, "protocol": "TCP", "destination": "", "destination_label": "", "destination_namespace": "wordpress-mysql", "count": 2, "action": "Allow" }</pre>							

13.3 Runtime Protection w/ Policy Management

13.3.1 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.



The screenshot shows a KubeArmorPolicy named "autopol-system-997688561" with the status "The YAML is valid". The "YAML" tab is selected, displaying the following code:

```

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

```

A red box highlights the entire "file" section. A red arrow points from this box to the text "File Access policy generated based on App behavior".

- **Process access behavior based policies:** Based on the process that are running in pod, the Auto discovered system policies are generated.

To view that policy user must navigate to *Runtime Protection->policies* section. Then click on the cluster and pod for which we want to see the auto-discovered policies.

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

Process access policy generated based on App Behavior

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

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

Egress policy generated based on the application Behavior

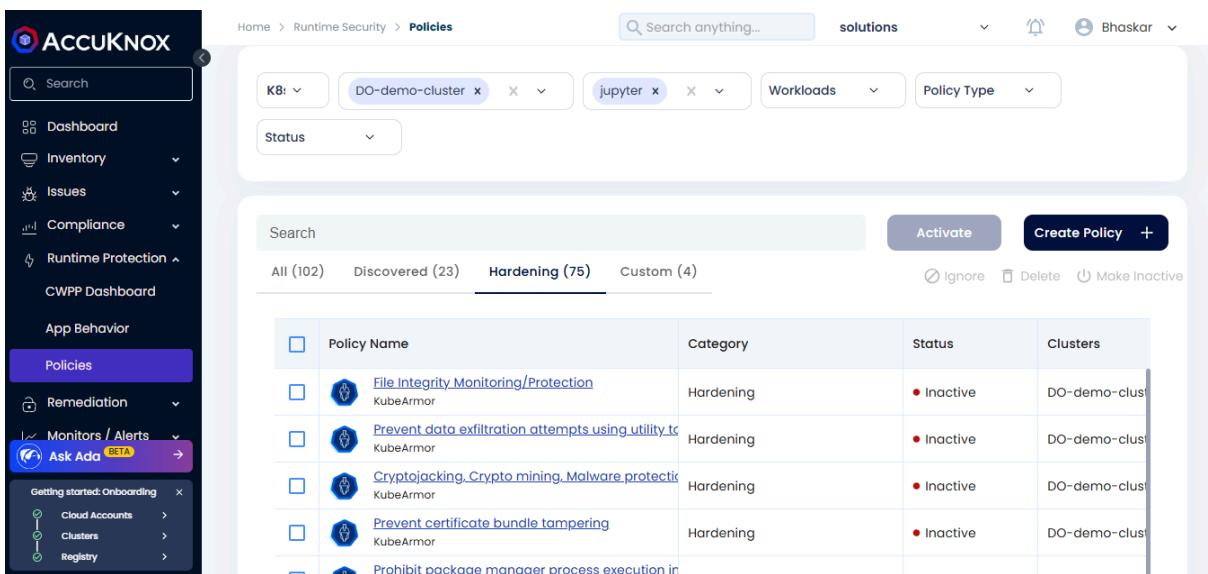


13.3.2 How to understand Hardening policies

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

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

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



The screenshot shows the AccuKnox web interface under the 'Runtime Security' section, specifically the 'Policies' page. The left sidebar has a purple navigation bar with the following items: Dashboard, Inventory, Issues, Compliance (selected), Runtime Protection, CWPP Dashboard, App Behavior (selected), Policies (selected), Remediation, Monitors / Alerts, Ask Ada (BETA), and Getting started: Onboarding (Cloud Accounts, Clusters, Registry). The main content area has a search bar at the top with filters: KB: (dropdown), DO-demo-cluster (selected), jupyter (selected), Workloads (dropdown), Policy Type (dropdown), and Status (dropdown). Below the search bar is a 'Search' input field and a table header with columns: All (102), Discovered (23), Hardening (75) (selected), and Custom (4). To the right of the table are buttons for Activate, Create Policy, Ignore, Delete, and Make Inactive. The table lists seven hardening policies:

<input type="checkbox"/>	Policy Name	Category	Status	Clusters
<input type="checkbox"/>	File Integrity Monitoring/Protection KubeArmor	Hardening	Inactive	DO-demo-clust
<input type="checkbox"/>	Prevent data exfiltration attempts using utility tc KubeArmor	Hardening	Inactive	DO-demo-clust
<input type="checkbox"/>	Cryptojacking, Crypto mining, Malware protection KubeArmor	Hardening	Inactive	DO-demo-clust
<input type="checkbox"/>	Prevent certificate bundle tampering KubeArmor	Hardening	Inactive	DO-demo-clust
<input type="checkbox"/>	Prohibit package manager process execution in ... KubeArmor	Hardening	Inactive	DO-demo-clust

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](#)

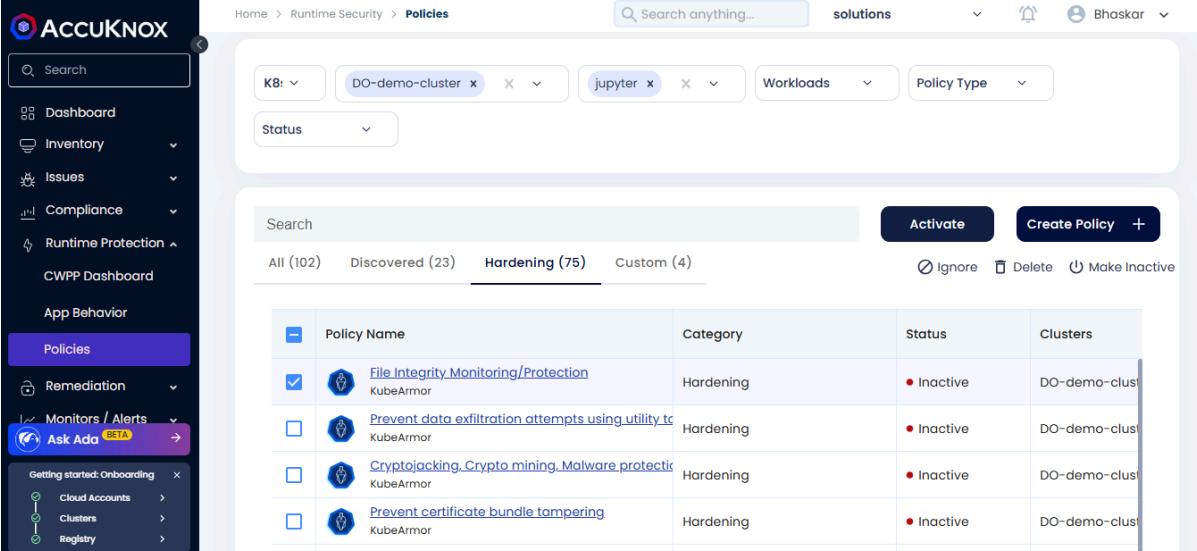
ⓘ Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom policy

```

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

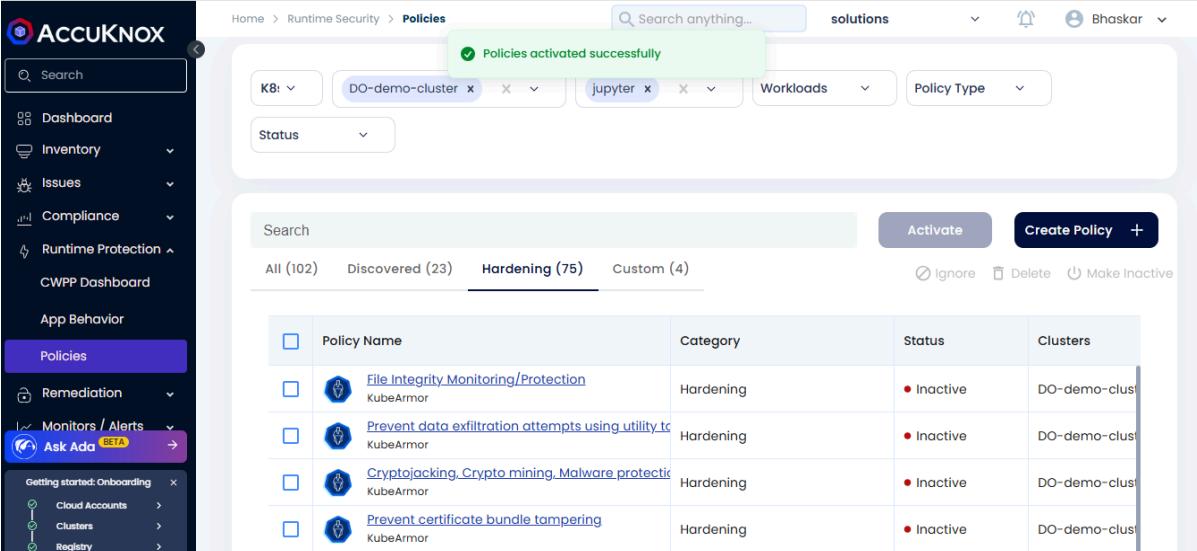
```

3. Select this policy and click on the Activate option.



Policy Name	Category	Status	Clusters
File Integrity Monitoring/Protection KubeArmor	Hardening	Inactive	DO-demo-cluster
Prevent data exfiltration attempts using utility tools KubeArmor	Hardening	Inactive	DO-demo-cluster
Cryptojacking, Crypto mining, Malware protection KubeArmor	Hardening	Inactive	DO-demo-cluster
Prevent certificate bundle tampering KubeArmor	Hardening	Inactive	DO-demo-cluster
Prohibit package manager process execution in			

4. After applying, the policy goes into Active state.



Policy Name	Category	Status	Clusters
File Integrity Monitoring/Protection KubeArmor	Hardening	Active	DO-demo-cluster
Prevent data exfiltration attempts using utility tools KubeArmor	Hardening	Inactive	DO-demo-cluster
Cryptojacking, Crypto mining, Malware protection KubeArmor	Hardening	Inactive	DO-demo-cluster
Prevent certificate bundle tampering KubeArmor	Hardening	Inactive	DO-demo-cluster
Prohibit package manager process execution in			

13.3.3 How to Audit application and get alerts for that

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

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

KubeArmorPolicy
🕒 Created a month ago.

 The YAML is valid

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

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

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

Home > Runtime Security > Policies partnerdemo

Policies

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

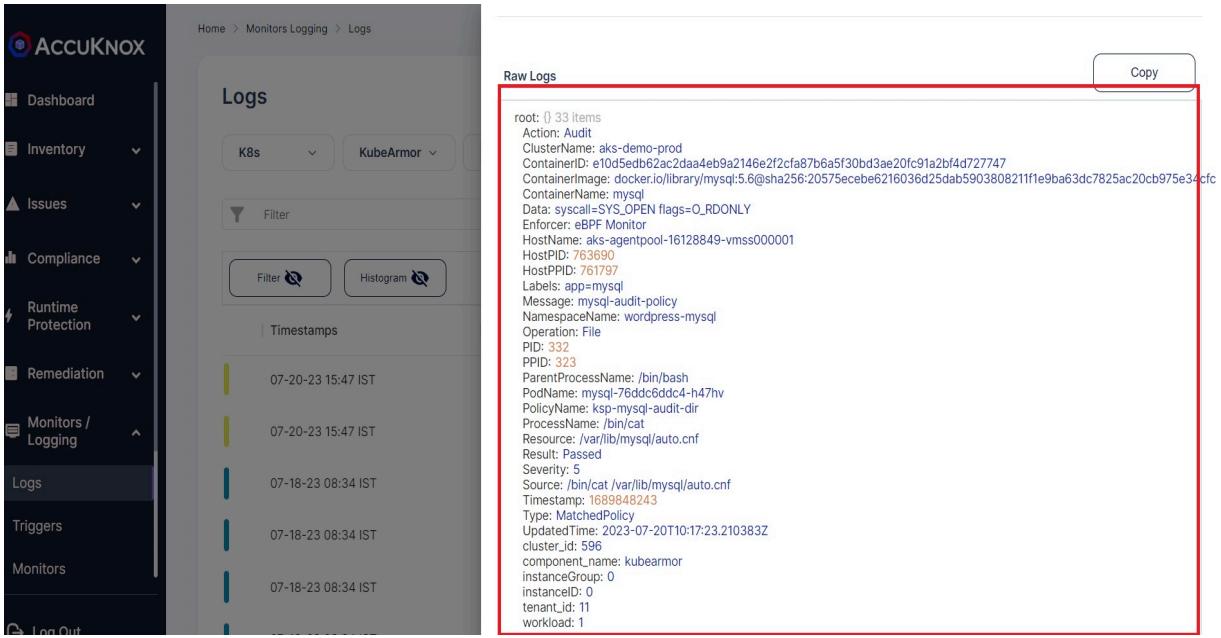
Search Audit based policy is applied from AccuKnox SaaS

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

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

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

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



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

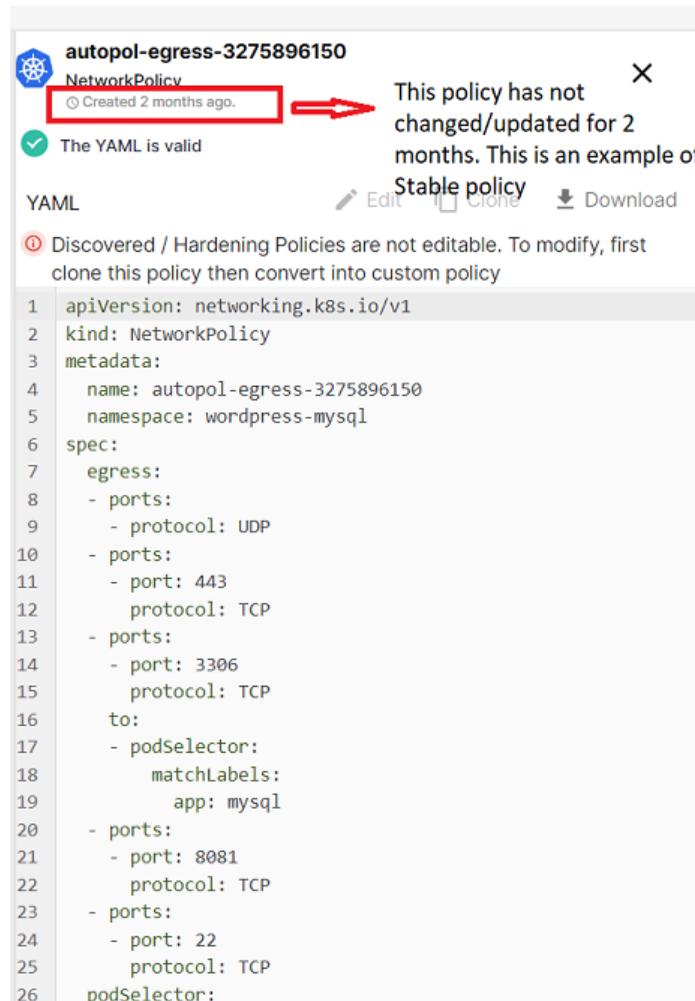
```

root: 33 items
Action: Audit
ClusterName: aks-demo-prod
ContainerID: e10d5edb62ac2daa4eb9a2146e2f2cfa87b6a5f30bd3ae20fc91a2bf4d727747
ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab5903808211fe9ba63dc7825ac20cb975e3...cfc
ContainerName: mysql
Data: syscall=SYS_OPEN flags=O_RDONLY
Enforcer: eBPF Monitor
HostName: aks-agentpool-16128849-vmss000001
HostPID: 763690
HostPPID: 761797
Labels: app=mysql
Message: mysql-audit-policy
NamespaceName: wordpress-mysql
Operation: File
PID: 332
PPID: 323
ParentProcessName: /bin/bash
PodName: mysql-76ddc6ddc4-h47hv
PolicyName: ksp-mysql-audit-dir
ProcessName: /bin/cat
Resource: /var/lib/mysql/auto.cnf
Result: Passed
Severity: 5
Source: /bin/cat /var/lib/mysql/auto.cnf
Timestamp: 1689848243
Type: MatchedPolicy
UpdatedTime: 2023-07-20T10:17:23.210383Z
cluster_id: 596
component_name: kubearmor
instance_group: 0
instance_id: 0
tenant_id: 11
workload: 1

```

13.3.4 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



```

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

```

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

13.3.5 What if something changes in Application?

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

autopol-system-1804736057 (v1)

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

Update X

Updated YAML

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

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

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

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

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

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

Update 

Updated YAML

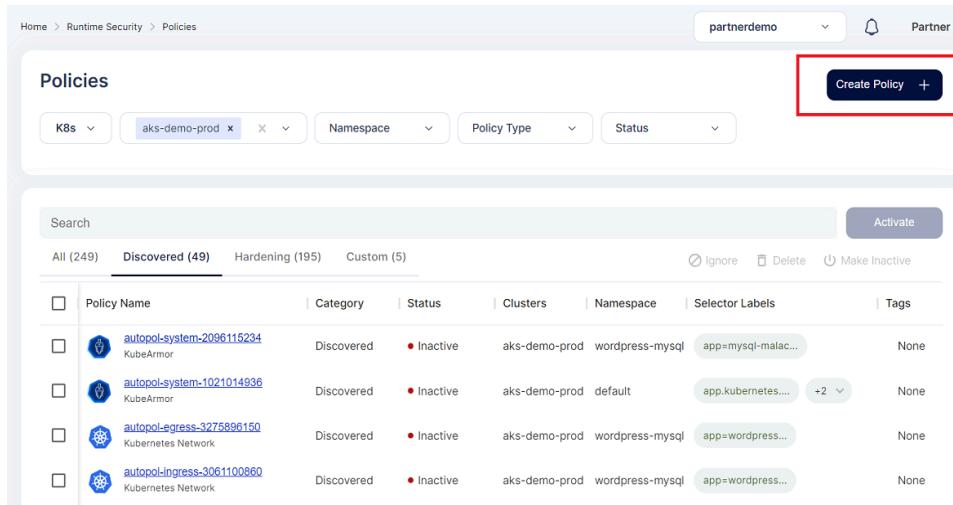
```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: autopol-system-1804736057
5   namespace: dwva
6 spec:
7   action: Allow
8   file:
9     matchDirectories:
10    - dir: /tmp/
11      fromSource:
12        - path: /usr/sbin/apache2
13      recursive: true
14   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

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

13.3.6 How to create a custom Policy

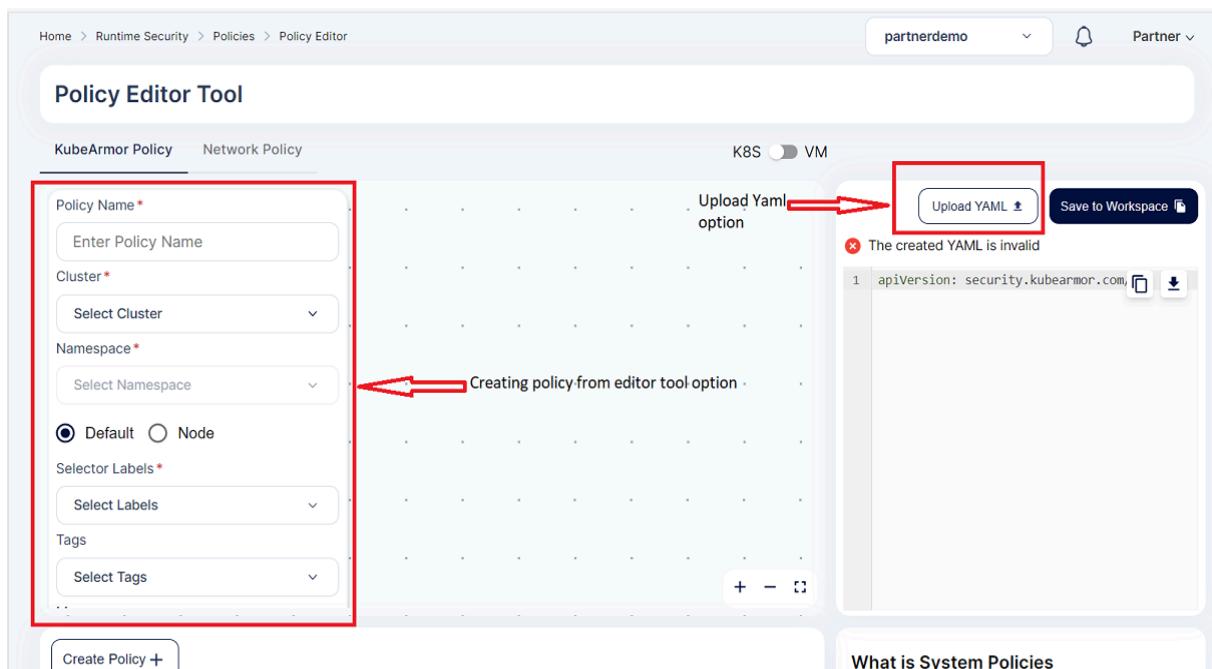
- File restriction Policy

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



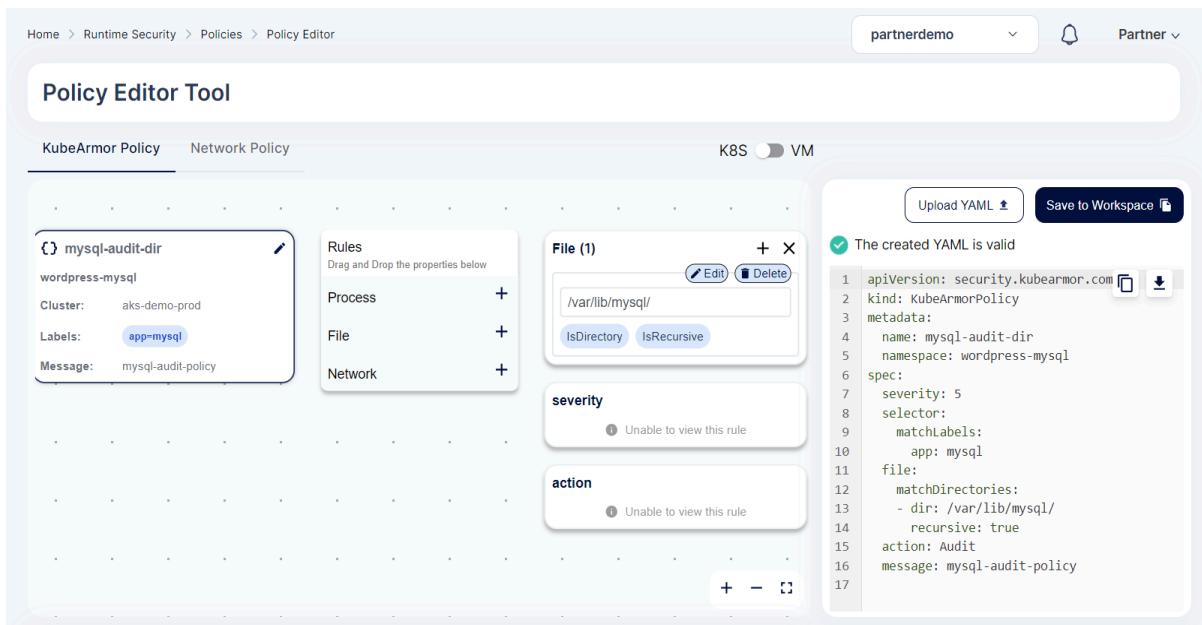
The screenshot shows the 'Policies' page in the AccuKnox interface. At the top right, there is a 'Create Policy' button with a '+' icon, which is highlighted with a red box. Below the header, there are several filter options: 'K8s' dropdown, 'aks-demo-prod' dropdown, 'Namespace' dropdown, 'Policy Type' dropdown, and 'Status' dropdown. A search bar and an 'Activate' button are also present. The main table lists policies categorized by status: 'All (249)', 'Discovered (49)', 'Hardening (195)', and 'Custom (5)'. The columns include 'Policy Name', 'Category', 'Status', 'Clusters', 'Namespace', 'Selector Labels', and 'Tags'. Four policies are listed under 'Discovered': 'autopol-system-2096115234' (KubeArmor), 'autopol-system-1021014936' (KubeArmor), 'autopol-egress-3275896150' (Kubernetes Network), and 'autopol-ingress-3061100860' (Kubernetes Network). Each row shows the policy name, category, status (Inactive), cluster (aks-demo-prod), namespace (wordpress-mysql or default), selector labels (app=mysql-mala..., app.kubernetes..., app=wordpress..., app=wordpress...), and tags (None).

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



The screenshot shows the 'Policy Editor Tool' page. On the left, there are tabs for 'KubeArmor Policy' and 'Network Policy', with 'KubeArmor Policy' selected. The main form area contains fields for 'Policy Name*', 'Cluster*', 'Namespace*', 'Default' (radio button selected), 'Selector Labels*', and 'Tags'. A large red box highlights this entire form area. To the right, there is an 'Upload YAML' option with a red box around it, and a message stating 'The created YAML is invalid'. Below this is a code editor window showing a single line of YAML: 'apiVersion: security.kubearmor.com'. At the bottom left is a 'Create Policy +' button, and at the bottom right is a link 'What is System Policies'.

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

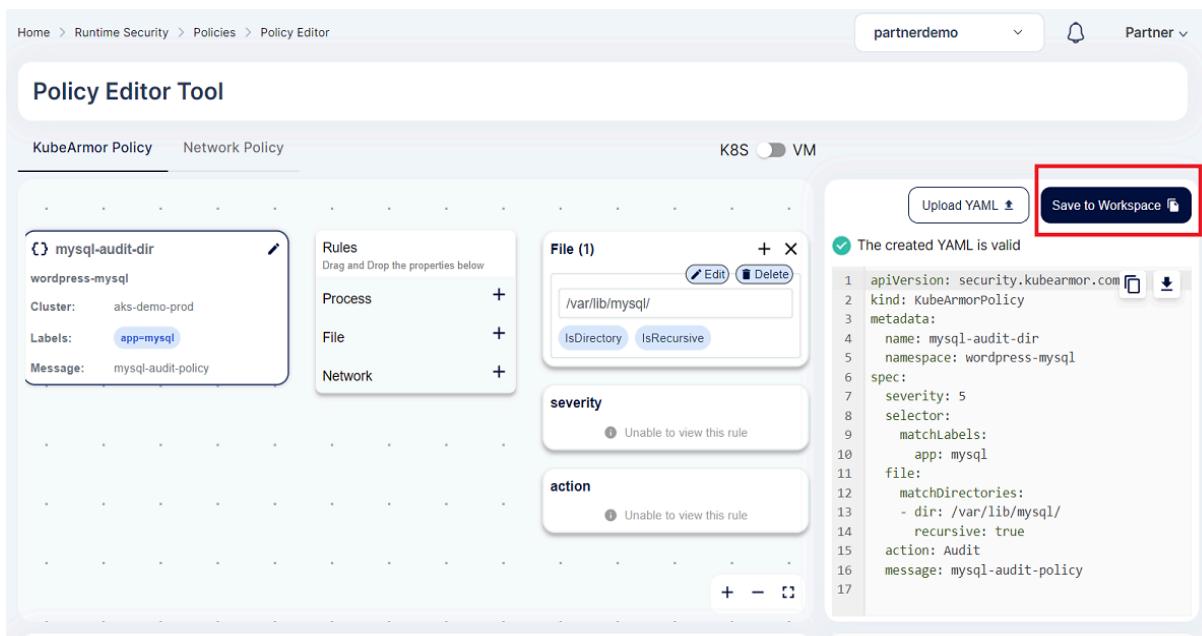


```

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

```

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

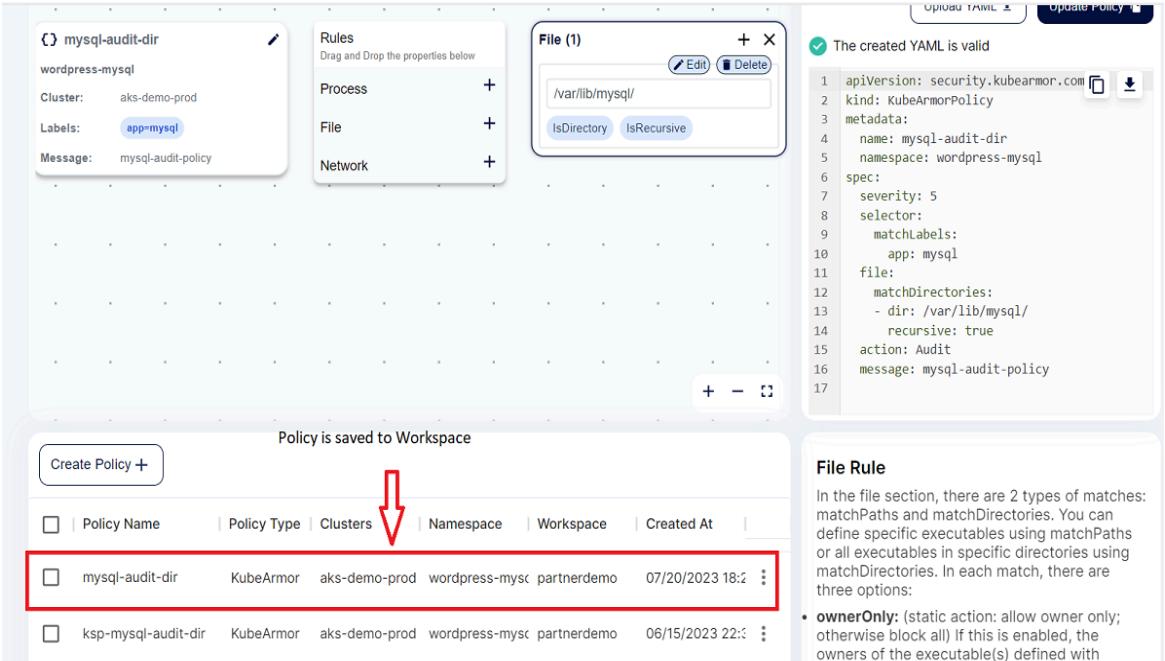


```

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

```

- After that policy will be saved to the workspace.



The screenshot shows the ACCUKNOKX platform's policy creation interface. On the left, there's a sidebar with a policy named "mysql-audit-dir" under "wordpress-mysql". The main area has tabs for "Process", "File", and "Network". Under "File", a rule is defined for "/var/lib/mysql/" with "IsDirectory" and "IsRecursive" selected. To the right, the generated YAML code is displayed:

```

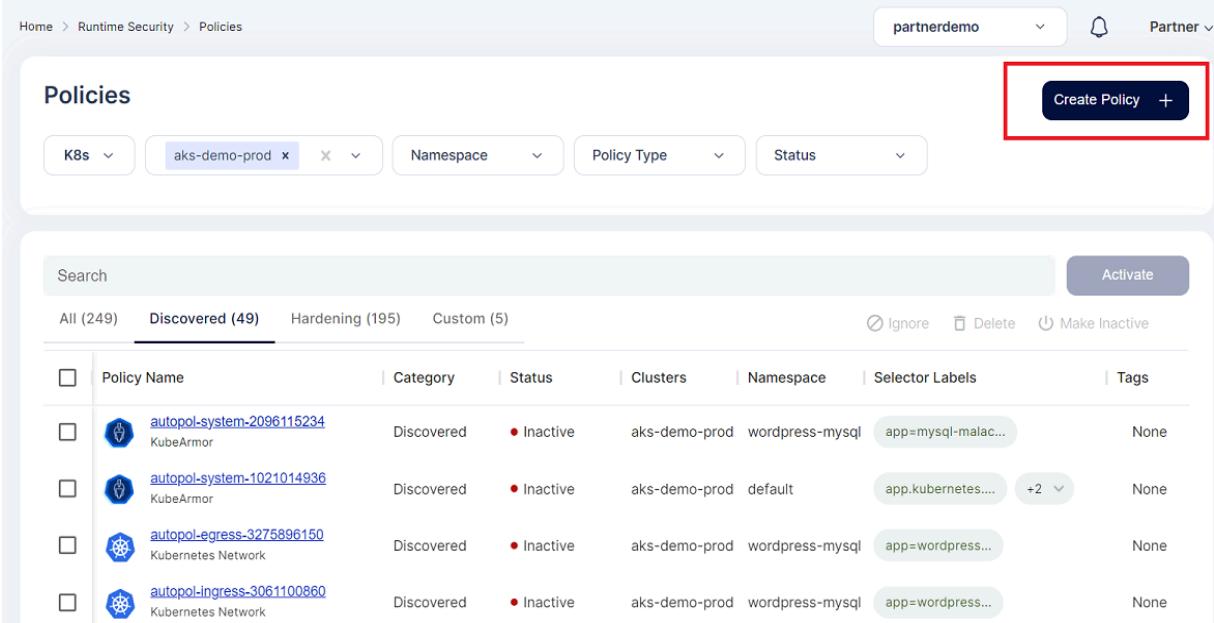
1 apiVersion: security.kubearmor.com
2 kind: KubeArmorPolicy
3 metadata:
4   name: mysql-audit-dir
5   namespace: wordpress-mysql
6 spec:
7   severity: 5
8   selector:
9     matchLabels:
10    app: mysql
11   file:
12     matchDirectories:
13       - dir: /var/lib/mysql/
14         recursive: true
15   action: Audit
16   message: mysql-audit-policy
17

```

Below this, a success message says "The created YAML is valid". At the bottom, a message says "Policy is saved to Workspace" with a red arrow pointing to the "Clusters" tab in the navigation bar. The "mysql-audit-dir" policy is highlighted with a red box.

● Network access Policy

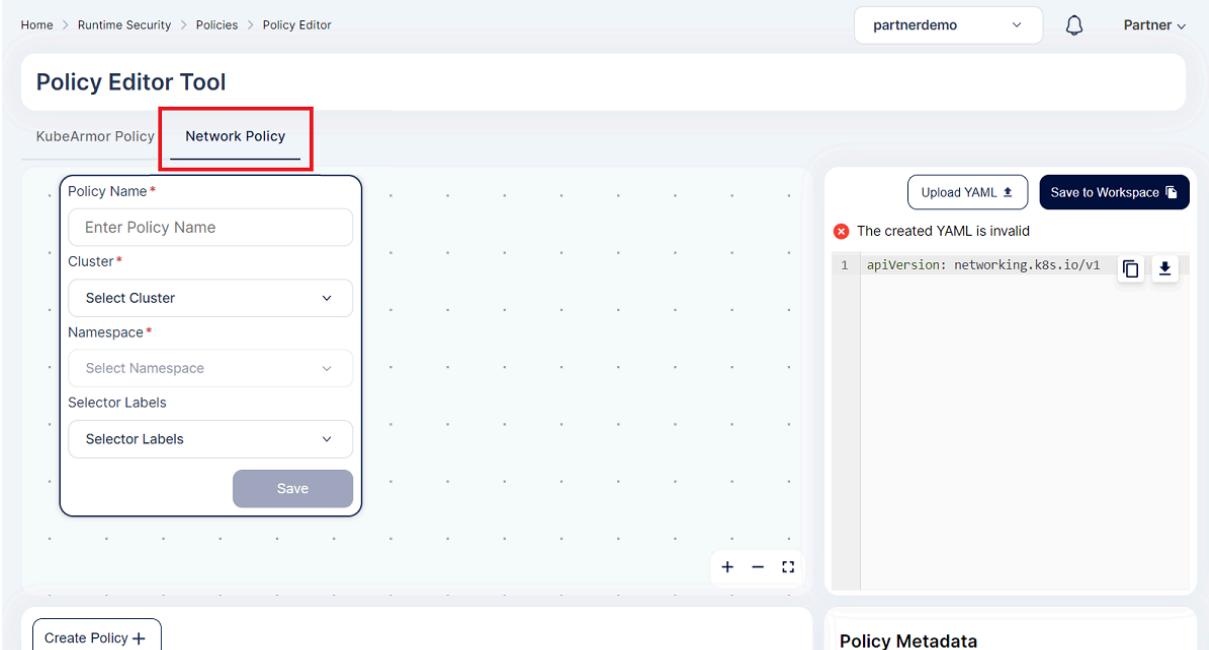
- To create a Network access policy restriction based custom policy user must navigate to *Runtime Protection->Policies* section.
- To create the policy user needs to click on the create policy option



The screenshot shows the ACCUKNOKX Policies page. At the top, there's a search bar and filters for "K8s", "Namespace", "Policy Type", and "Status". A prominent red box highlights the "Create Policy" button. Below this, a table lists policies. The first four rows are highlighted with a red box:

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

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



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

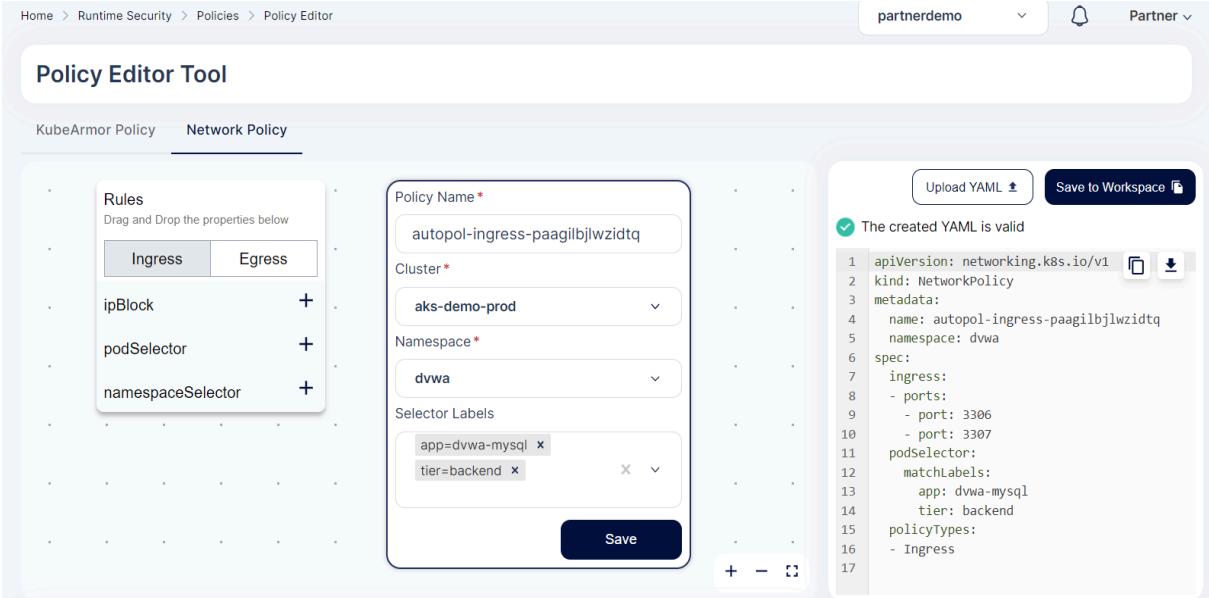
- Policy Name ***: Enter Policy Name
- Cluster ***: Select Cluster
- Namespace ***: Select Namespace
- Selector Labels**: Selector Labels

At the bottom right of the form is a 'Save' button. To the right of the form is a large text area for YAML code. It shows the beginning of a NetworkPolicy YAML file:

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

Below the text area are buttons for 'Upload YAML' and 'Save to Workspace'. A message at the top right says 'The created YAML is invalid'.

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



The screenshot shows the 'Policy Editor Tool' interface with the 'Network Policy' tab selected. On the left, under 'Rules', there are buttons for 'Ingress' and 'Egress', with 'Ingress' currently selected. Below these are three buttons: 'ipBlock', 'podSelector', and 'namespaceSelector', each with a '+' sign to its right.

In the center, there is a form for defining a specific NetworkPolicy:

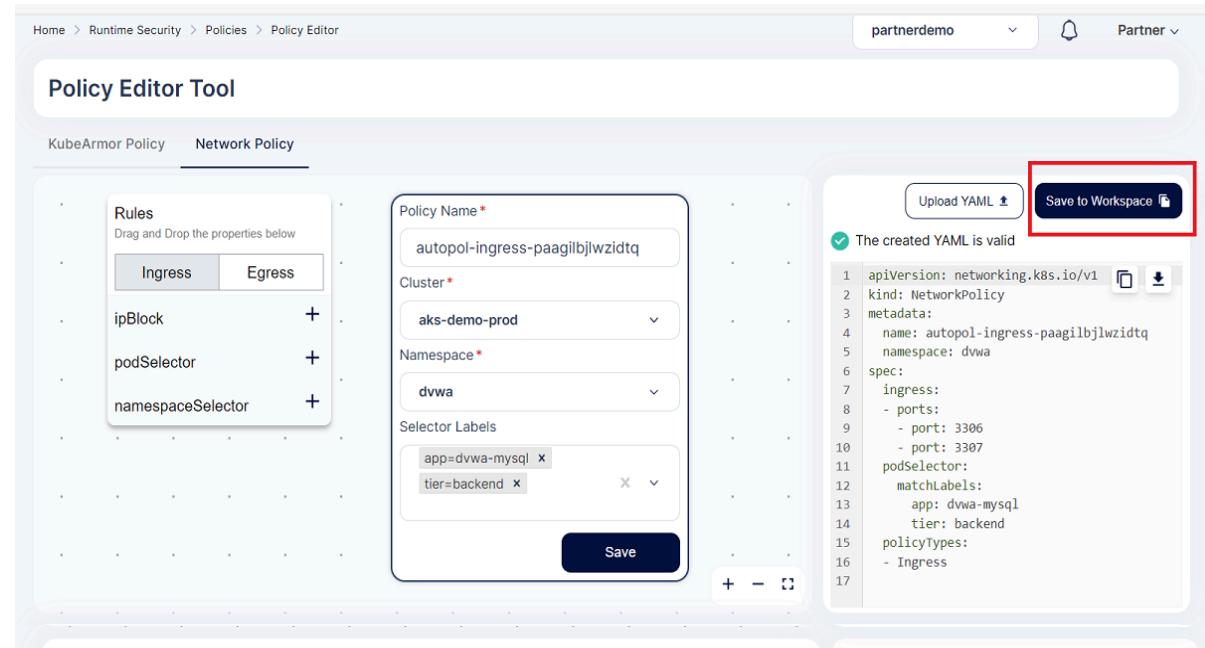
- Policy Name ***: autopol-ingress-paagilbjlwzidtq
- Cluster ***: aks-demo-prod
- Namespace ***: dvwa
- Selector Labels**: app=dvwa-mysql tier=backend

At the bottom right of the form is a 'Save' button. To the right of the form is a large text area for YAML code. It shows a valid NetworkPolicy YAML file:

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

Below the text area are buttons for 'Upload YAML' and 'Save to Workspace'. A message at the top right says 'The created YAML is valid'.

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



The screenshot shows the Policy Editor Tool interface. On the left, there's a sidebar with 'Home', 'Runtime Security', 'Policies', and 'Policy Editor'. The main area is titled 'Policy Editor Tool' and has tabs for 'KubeArmor Policy' and 'Network Policy', with 'Network Policy' selected. In the center, there's a form for creating a NetworkPolicy:

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

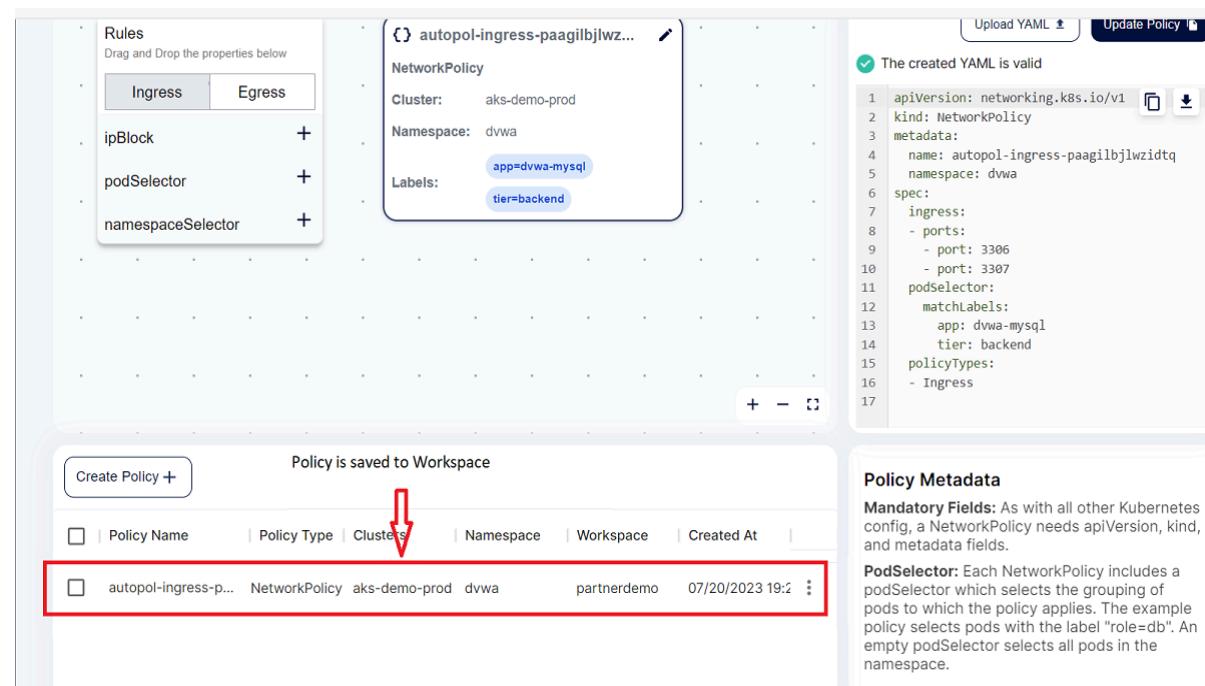
At the bottom right of the form is a 'Save' button. To the right of the form is a code editor window showing the YAML configuration. At the top right of the code editor is a 'Save to Workspace' button, which is highlighted with a red box.

```

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

```

- After that policy will be saved to the workspace.

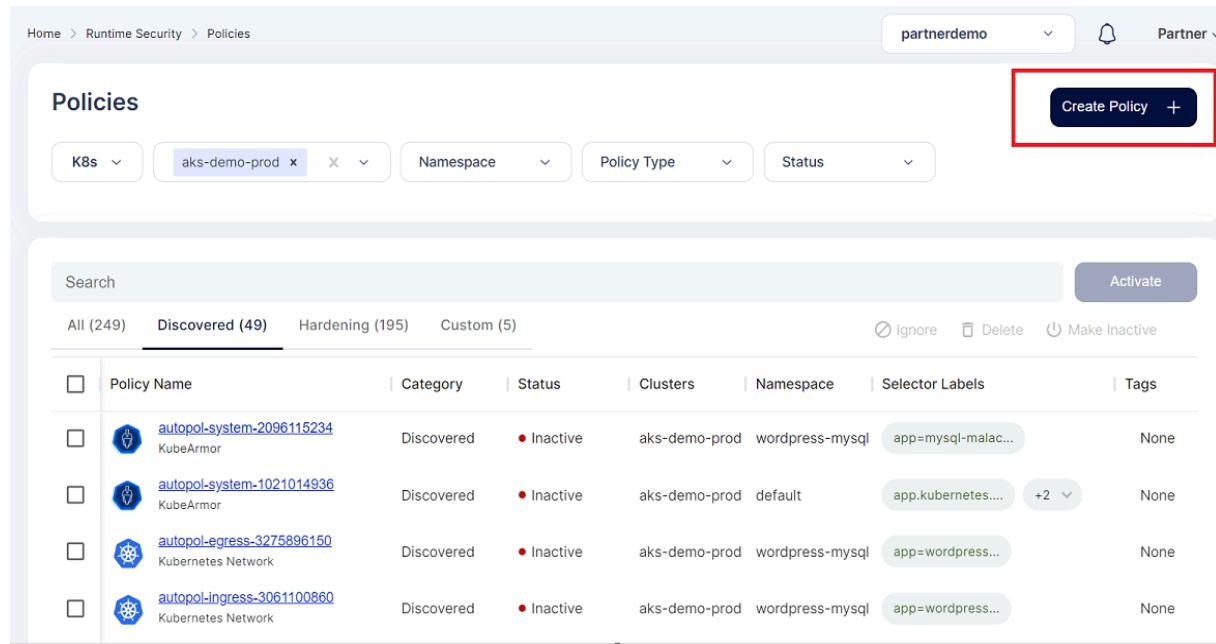


The screenshot shows the Policy Editor Tool after the policy has been saved to the workspace. The interface includes:

- Rules** section with 'Ingress' and 'Egress' buttons.
- NetworkPolicy** details: Cluster: aks-demo-prod, Namespace: dvwa, Labels: app=dvwa-mysql, tier=backend.
- Code Editor** showing the valid YAML configuration.
- Table** showing the saved policy:

	Policy Name	Policy Type	Clusters	Namespace	Workspace	Created At
<input type="checkbox"/>	autopol-ingress-p...	NetworkPolicy	aks-demo-prod	dvwa	partnerdemo	07/20/2023 19:2
- Policy Metadata** section with information about mandatory fields and pod selectors.

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



Policies

Create Policy +

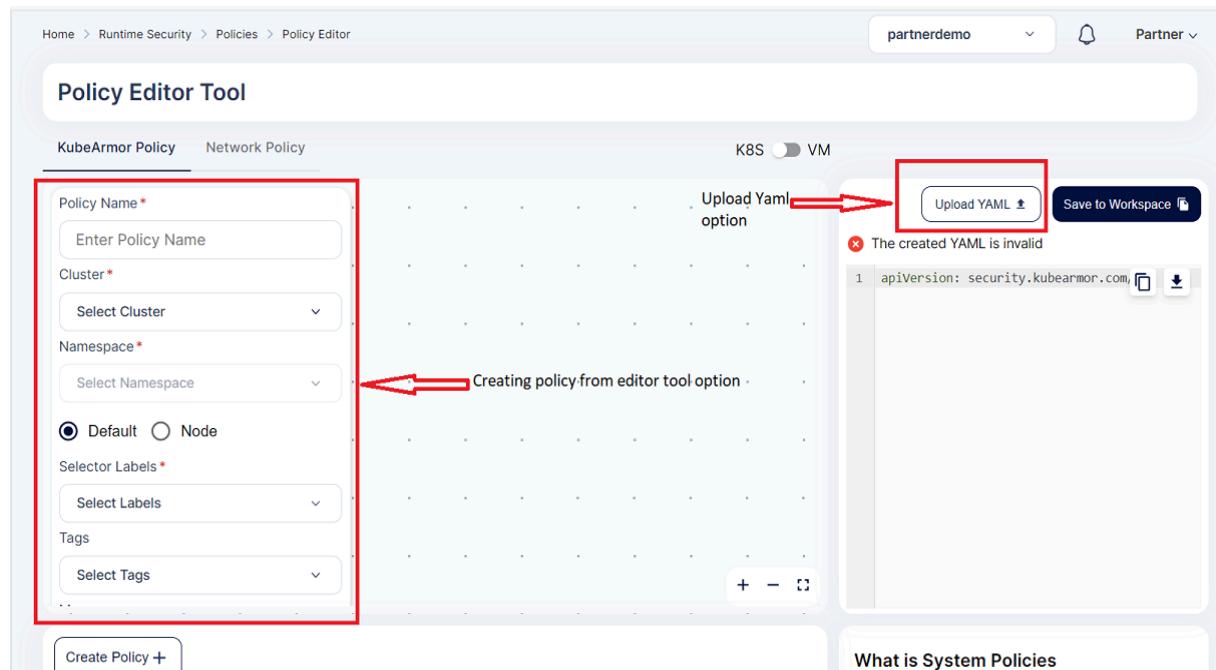
Search

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

Ignore Delete Make Inactive

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

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



Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy

Policy Name* Enter Policy Name

Cluster* Select Cluster

Namespace* Select Namespace

Default Node

Selector Labels* Select Labels

Tags Select Tags

Upload YAML option

Upload YAML Save to Workspace

The created YAML is invalid

Creating policy from editor tool option

apiVersion: security.kubearmor.com,

Create Policy +

What is System Policies

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

Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy K8S VM

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

Rules
 Drag and Drop the properties below

Process (2)

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

severity
Unable to view this rule

action
Unable to view this rule

Upload YAML  **Save to Workspace** 

The created YAML is valid

```

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

```

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

Home > Runtime Security > Policies > Policy Editor

partnerdemo Partner

Policy Editor Tool

KubeArmor Policy Network Policy K8S VM

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

Rules
 Drag and Drop the properties below

Process (2)

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

severity
Unable to view this rule

action
Unable to view this rule

Upload YAML  **Save to Workspace** 

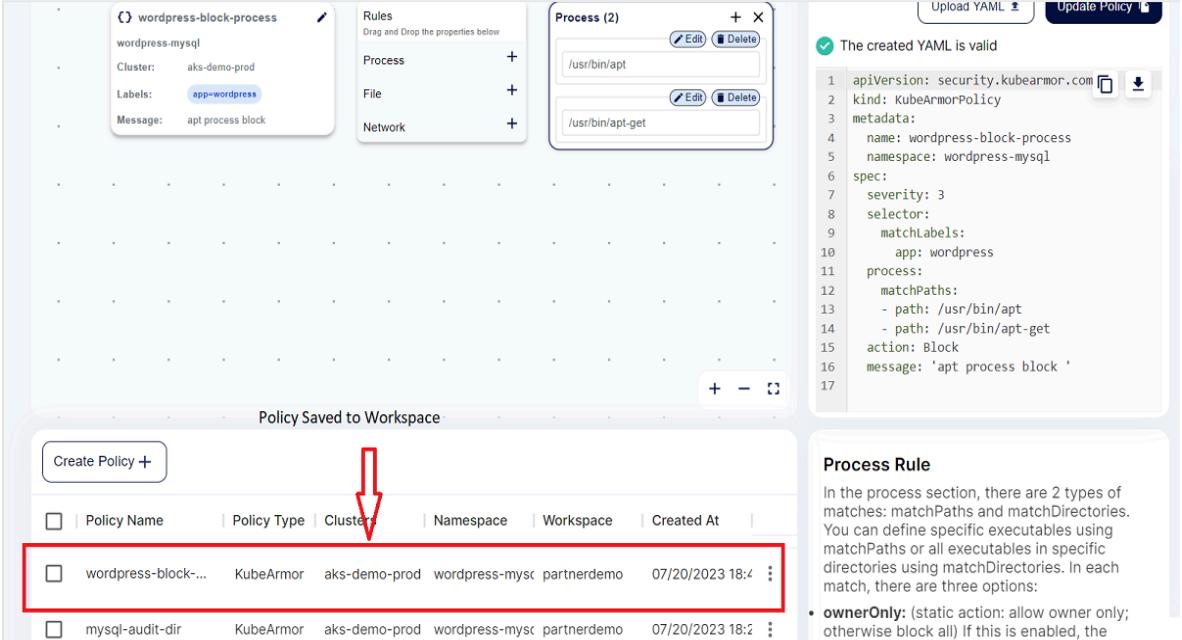
The created YAML is valid

```

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

```

- After that policy will be saved to the workspace.



The screenshot shows the AccuKnox interface for creating and managing security policies. At the top, a policy named "wordpress-block-process" is being edited. It includes fields for Cluster ("aks-demo-prod"), Labels ("app=wordpress"), and Message ("apt process block"). Below this, a "Rules" section allows dragging and dropping properties, with a "Process" rule currently selected. The "Process" rule contains two entries: "/usr/bin/apt" and "/usr/bin/apt-get". To the right, a "YAML" view shows the generated Kubernetes security rule:

```

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

```

A success message indicates "The created YAML is valid". Below the editor, a message says "Policy Saved to Workspace". In the bottom left, a table lists existing policies: "wordpress-block-..." and "mysql-audit-dir". A red box highlights the first row, and a red arrow points from the "Create Policy +" button to the table header. On the right, a "Process Rule" section provides detailed information about the rule structure.

13.3.7 How to enforce Policies and see anomalies

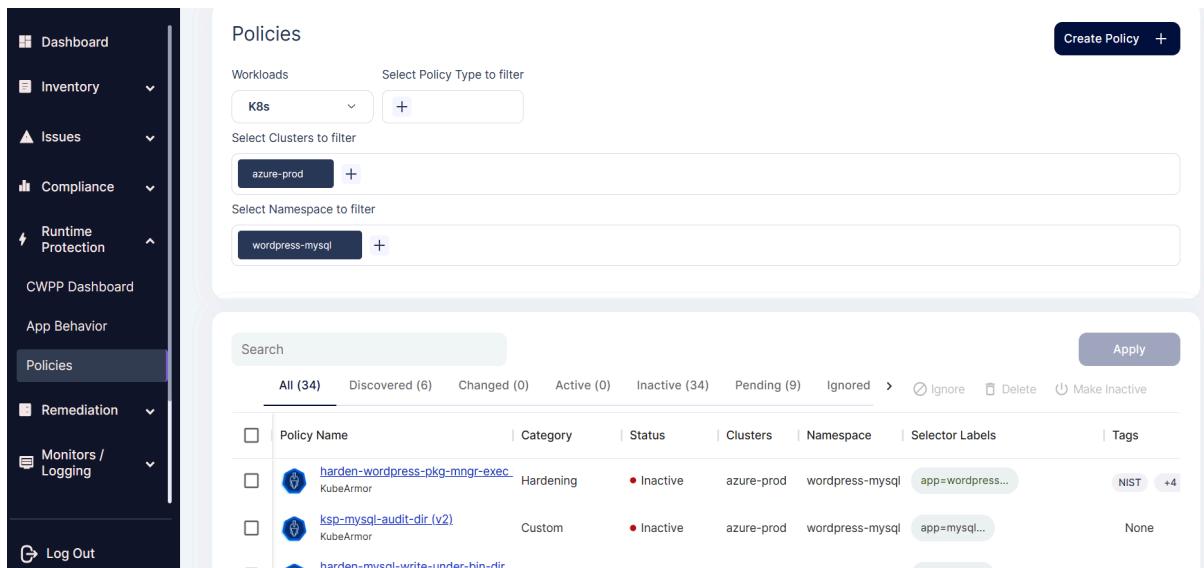
- We can apply any of the Auto Discovered, Hardening or custom policies and see the anomalies getting detected using the Monitoring and Logging section.
- Let us consider the WordPress- MySQL application. In the MySQL application, certain folders will be having certain critical data which can be allowed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

```

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

```

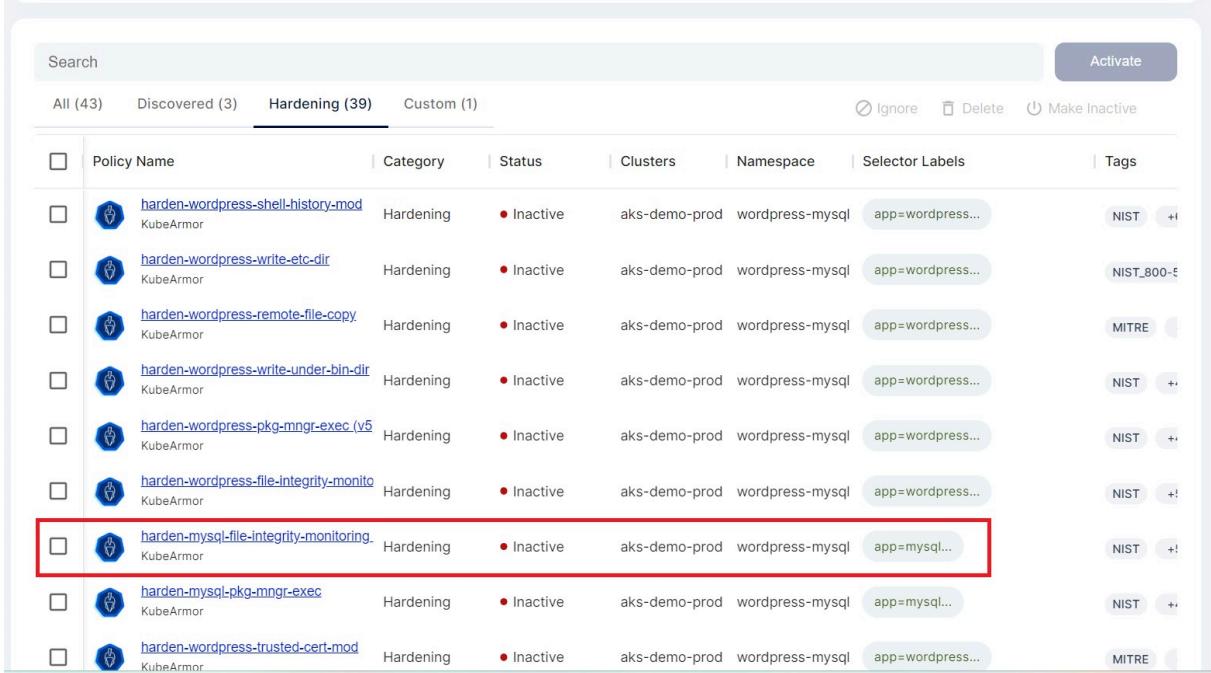
- Now we are going to prevent this using AccuKnox CWPP Solution.
- Step 1:** Navigate to the Runtime Protection-> Policies and select the cluster and namespace where the WordPress-MySQL application is deployed.



The screenshot shows the AccuKnox CWPP interface. On the left, there is a sidebar with navigation links: Dashboard, Inventory, Issues, Compliance, Runtime Protection (selected), CWPP Dashboard, App Behavior, Policies (selected), Remediation, and Monitors / Logging. At the bottom of the sidebar is a Log Out button. The main area is titled "Policies". It has filtering options for Workloads (K8s selected), Clusters (azure-prod selected), and Namespace (wordpress-mysql selected). Below these filters is a search bar and a table of policies. The table has columns: All (34), Discovered (6), Changed (0), Active (0), Inactive (34), Pending (9), Ignored, and buttons for Ignore, Delete, and Make Inactive. The table lists three policies:

	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
<input type="checkbox"/>	harden-wordpress-pkg-mngr-exec_	Hardening	Inactive	azure-prod	wordpress-mysql	app=wordpress...	NIST +4
<input type="checkbox"/>	ksp-mysql-audit-dir (v2)	Custom	Inactive	azure-prod	wordpress-mysql	app=mysql...	None
<input type="checkbox"/>	harden-mysql-write-under-bin-dir						

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



Search								Activate
	All (43)	Discovered (3)	Hardening (39)	Custom (1)	<input type="checkbox"/> Ignore	<input type="checkbox"/> Delete	<input type="checkbox"/> Make Inactive	
	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags	
<input type="checkbox"/>	harden-wordpress-shell-history-mod KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST	
<input type="checkbox"/>	harden-wordpress-write-etc-dir KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST_800-5	
<input type="checkbox"/>	harden-wordpress-remote-file-copy KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE	
<input type="checkbox"/>	harden-wordpress-write-under-bin-dir KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST	
<input type="checkbox"/>	harden-wordpress-pkg-mngr-exec (v5) KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST	
<input type="checkbox"/>	harden-wordpress-file-integrity-monitoring KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	NIST	
<input type="checkbox"/>	harden-mysql-file-integrity-monitoring KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=mysql...	NIST	
<input type="checkbox"/>	harden-mysql-pkg-mngr-exec KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=mysql...	NIST	
<input type="checkbox"/>	harden-wordpress-trusted-cert-mod KubeArmor	Hardening	● Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...	MITRE	

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

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

KubeArmorPolicy
Created 5 days ago.

[YAML](#)  Edit  Clone  Download

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

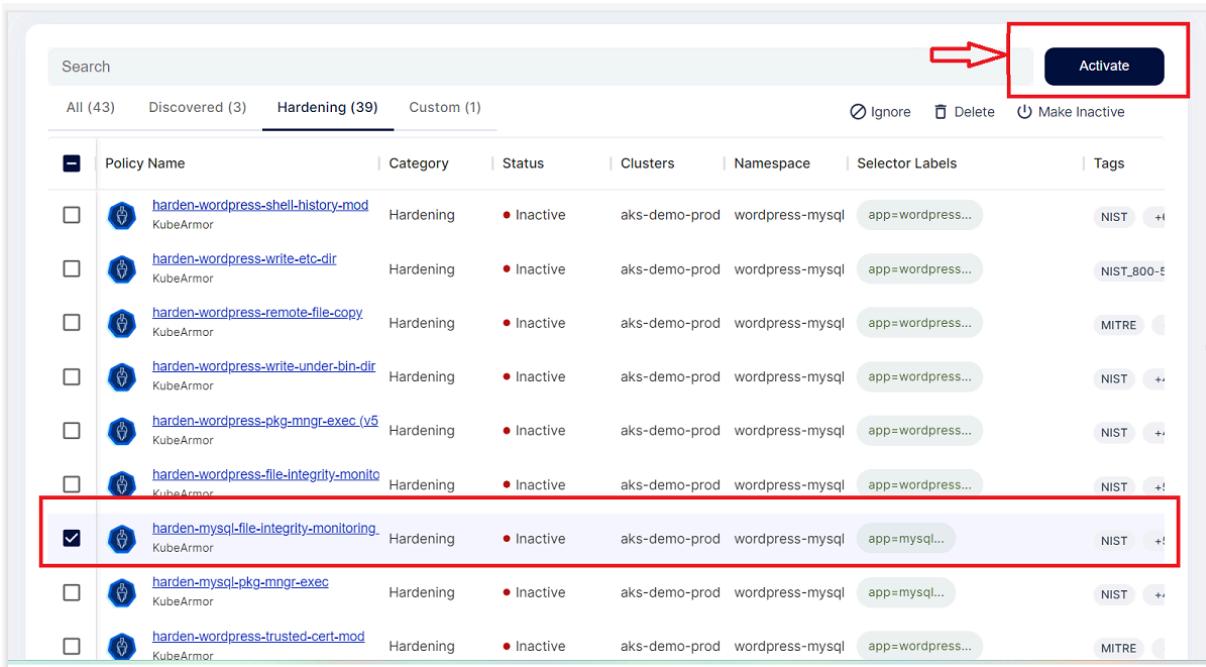
```
1 apiVersion: security.kubearmor.com/v1
2 kind: KubeArmorPolicy
3 metadata:
4   name: harden-mysql-file-integrity-monitoring
5   namespace: wordpress-mysql
6 spec:
7   action: Block
8   file:
9     matchDirectories:
10    - dir: /sbin/
11      readOnly: true
12      recursive: true
13    - dir: /usr/bin/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

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

```
apiVersion: security.kubearmor.com/v1
kind: KubeArmorPolicy
metadata:
  name: harden-mysql-file-integrity-monitoring
  namespace: wordpress-mysql
spec:
  action: Block
  file:
    matchDirectories:
      - dir: /sbin/
        readOnly: true
        recursive: true
      - dir: /usr/bin/
        readOnly: true
        recursive: true
      - dir: /usr/lib/
        readOnly: true
        recursive: true
      - dir: /usr/sbin/
        readOnly: true
        recursive: true
      - dir: /bin/
        readOnly: true
        recursive: true
      - dir: /boot/
        readOnly: true
        recursive: true
    message: Detected and prevented compromise
    to File integrity
  selector:
    matchLabels:
      app: mysql
      severity: 1
    tags:
      - NIST
      - NIST_800-53_AU-2
      - NIST_800-53_SI-4
      - MITRE
```

- MITRE_T1036_masquerading
- MITRE_T1565_data_manipulation

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



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

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

Home > Runtime Security > Policies

partnerdemo

Create Policy +

K8s aks-demo-prod wordpress-mysql KubeArmor Status

Search

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

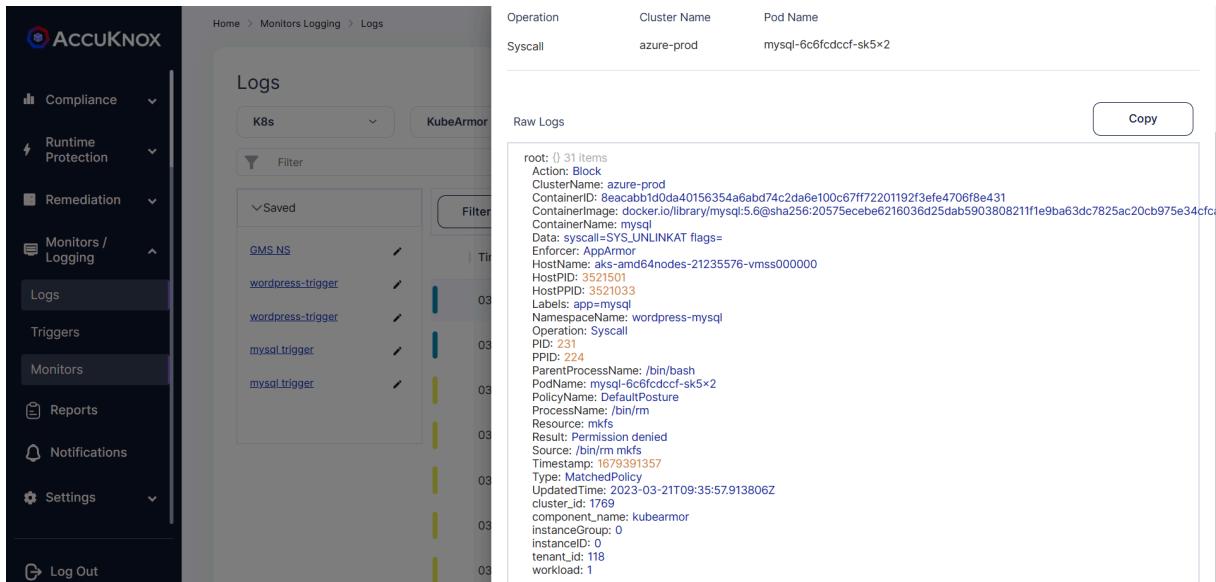
Ignore Delete Make Inactive

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

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

```
root@mysql-6c6fdcccf-sk5x2:/# cd sbin
root@mysql-6c6fdcccf-sk5x2:/sbin# ls
agetty    dumpe2fs   fsck.ext2   installkernel  mkfs.cramfs      pam_tally2      swaplabel
badblocks e2fsck     fsck.ext3   isosize        mkfs.ext2       pivot_root    swapoff
blkdiscard e2image   fsck.ext4   killall5     mkfs.ext3       raw          swapon
blkid     e2label   fsck.minix  ldconfig      mkfs.ext4       resize2fs    switch_root
blockdev e2undo   fsfreeze    logsave       mkfs.minix     runuser      tune2fs
cfdisk    fdisk     fstab-decode losetup      mkhomedir_helper sfdisk      unix_chkpwd
chcpu     findfs    fstrim     mke2fs       mks2          shadowconfig unix_update
ctrlaltdel fsck     getty      mkfs         mkswap        start-stop-daemon wipefs
debugfs   fsck.cramfs hwclock   mkfs.bfs    pam_tally    sulogin      zramctl
root@mysql-6c6fdcccf-sk5x2:/sbin# rm mkfs
rm: cannot remove 'mkfs': Permission denied
root@mysql-6c6fdcccf-sk5x2:/sbin#
```

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



The screenshot shows the AccuKnox SaaS interface for monitoring logs. The left sidebar has a dark theme with categories like Compliance, Runtime Protection, Remediation, Monitors / Logging (selected), Logs, Triggers, Monitors, Reports, Notifications, Settings, and Log Out. The main area shows a breadcrumb path: Home > Monitors Logging > Logs. The title is "Logs" with filters for K8s and KubeArmor. A table header includes Operation, Cluster Name, and Pod Name. A row for "Syscall" shows the cluster name as "azure-prod" and the pod name as "mysql-6c6fcddcf-sk5x2". Below this is a section titled "Raw Logs" with a "Copy" button, displaying log entries for a MySQL pod. One entry is highlighted:

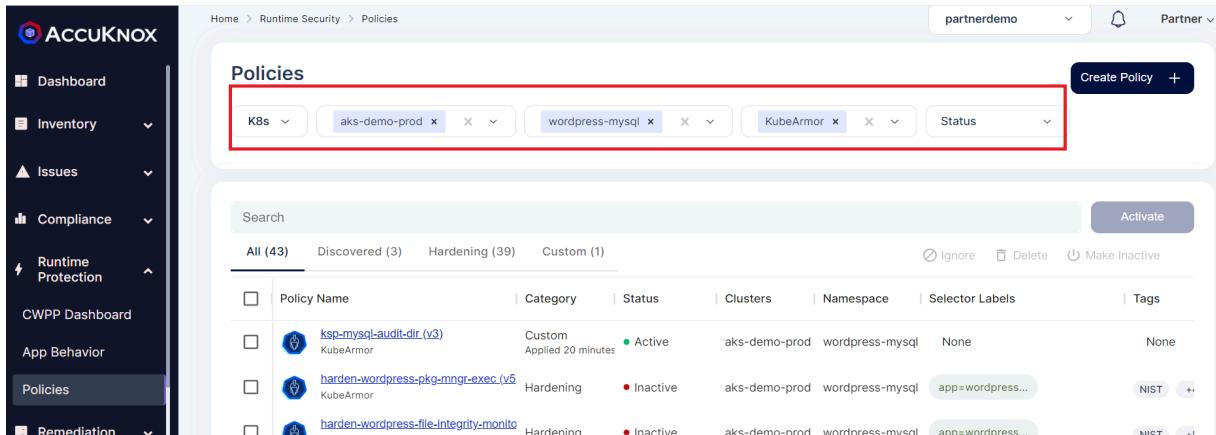
```

root: {} 31 items
Action: Block
ClusterName: azure-prod
ContainerID: 8eacabb1d0da40156354a6abd74c2da6e100c67ff72201192f3efe4706f8e431
ContainerImage: docker.io/library/mysql:5.6@sha256:20575ecebe6216036d25dab5903808211fe9ba63dc7825ac20cb975e34cf
ContainerName: mysql
Data: syscall=SYS_UNLINK flags=
Enforcer: AppArmor
HostName: aks-amd64nodes-21235576-vmss000000
HostPID: 3521501
HostPPID: 3521033
Label: app=mysql
NamespaceName: wordpress-mysql
Operation: Syscall
PID: 231
PPID: 224
ParentProcessName: /bin/bash
PodName: mysql-6c6fcddcf-sk5x2
PolicyName: DefaultPosture
ProcessName: /bin/mrm
Resource: mdfs
Result: Permission denied
Source: /bin/mrm mdfs
Timestamp: 1679391357
Type: MatchedPolicy
UpdatedTime: 2023-03-21T09:35:57.913806Z
cluster_id: 1769
component_name: kubearmor
instance_group: 0
instance_id: 0
tenant_id: 118
workload: 1

```

13.3.8 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



The screenshot shows the AccuKnox SaaS interface for managing policies. The left sidebar has a dark theme with categories like Dashboard, Inventory, Issues, Compliance, Runtime Protection (selected), CWPP Dashboard, App Behavior, Policies (selected), and Remediation. The main area shows a breadcrumb path: Home > Runtime Security > Policies. The title is "Policies" with a "Create Policy" button. A red box highlights the filter bar, which includes dropdowns for K8s, aks-demo-prod, wordpress-mysql, KubeArmor, and Status. Below this is a search bar and a table header with columns: All (43), Discovered (3), Hardening (39), Custom (1), Activate, Ignore, Delete, and Make Inactive. The table lists three policies:

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

Home > Runtime Security > Policies

partnerdemo Partner

Policies

K8s aks-demo-prod wordpress-mysql KubeArmor Status

Applying Multiple policies

Search

All (43)	Discovered (3)	Hardening (39)	Custom (1)	Ignore	Delete	Make Inactive
<input checked="" type="checkbox"/> ksp-mysql-audit-dir (v3)	KubeArmor	Custom	Inactive	aks-demo-prod	wordpress-mysql	None
<input checked="" type="checkbox"/> autopol-system-2096115234	KubeArmor	Discovered	Inactive	aks-demo-prod	wordpress-mysql	app=mysql-malac...
<input checked="" type="checkbox"/> harden-wordpress-shell-history-mod	KubeArmor	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...
<input checked="" type="checkbox"/> harden-wordpress-write-etc-dir	KubeArmor	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...
<input checked="" type="checkbox"/> harden-wordpress-remote-file-copy	KubeArmor	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress...

Activate

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

ACCUKNOX

Dashboard

Inventory

Issues

Compliance

Runtime Protection

CWPP Dashboard

App Behavior

Policies

Remediation

Monitors / Logging

Log Out

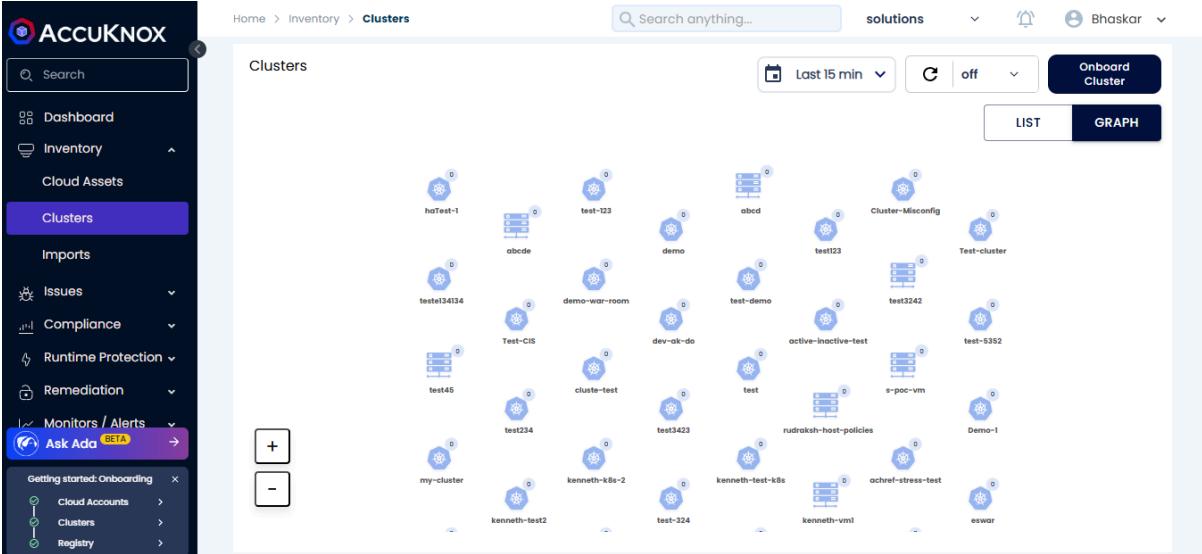
Search

All (43)	Discovered (3)	Hardening (39)	Custom (1)	Ignore	Delete	Make Inactive	
<input type="checkbox"/> harden-mysql-file-integrity-monitoring	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=mysql...
<input type="checkbox"/> harden-wordpress-remote-file-copy	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...
<input type="checkbox"/> harden-wordpress-write-etc-dir	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...
<input type="checkbox"/> harden-wordpress-shell-history-mod	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...
<input type="checkbox"/> autopol-system-2096115234	KubeArmor	Discovered	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=mysql-malac...
<input type="checkbox"/> harden-mysql-pkg-mngr-exec	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=mysql...
<input type="checkbox"/> harden-wordpress-pkg-mngr-exec (v5)	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...
<input type="checkbox"/> harden-wordpress-write-under-bin-dir	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...
<input type="checkbox"/> harden-wordpress-file-integrity-monitor	KubeArmor	Hardening	Applied a few sec	Active	aks-demo-prod	wordpress-mysql	app=wordpress...

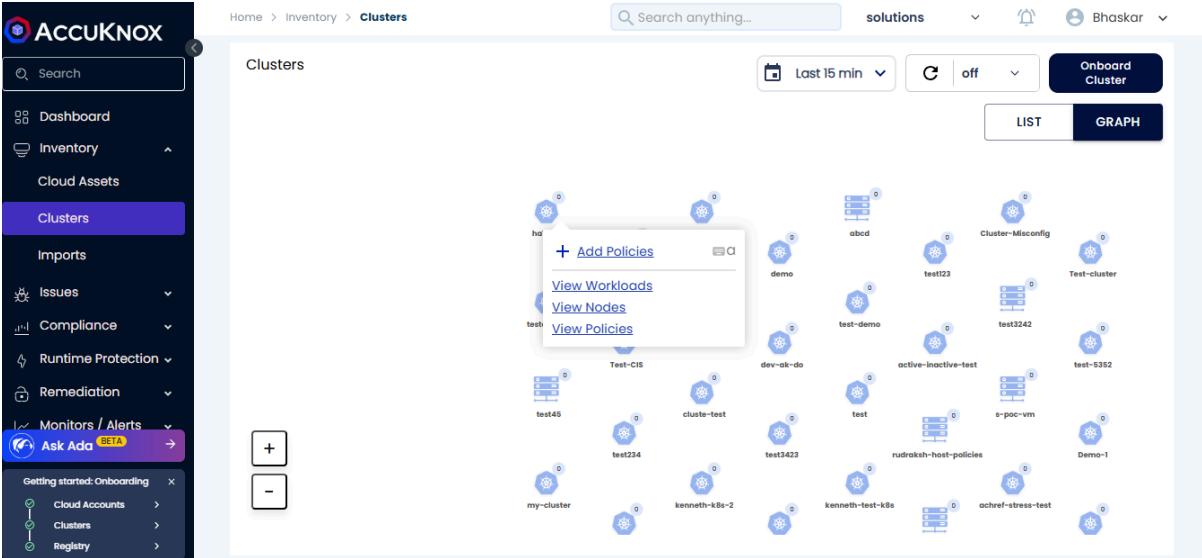
Activate

13.3.9 How to Find Nodes of a VM cluster

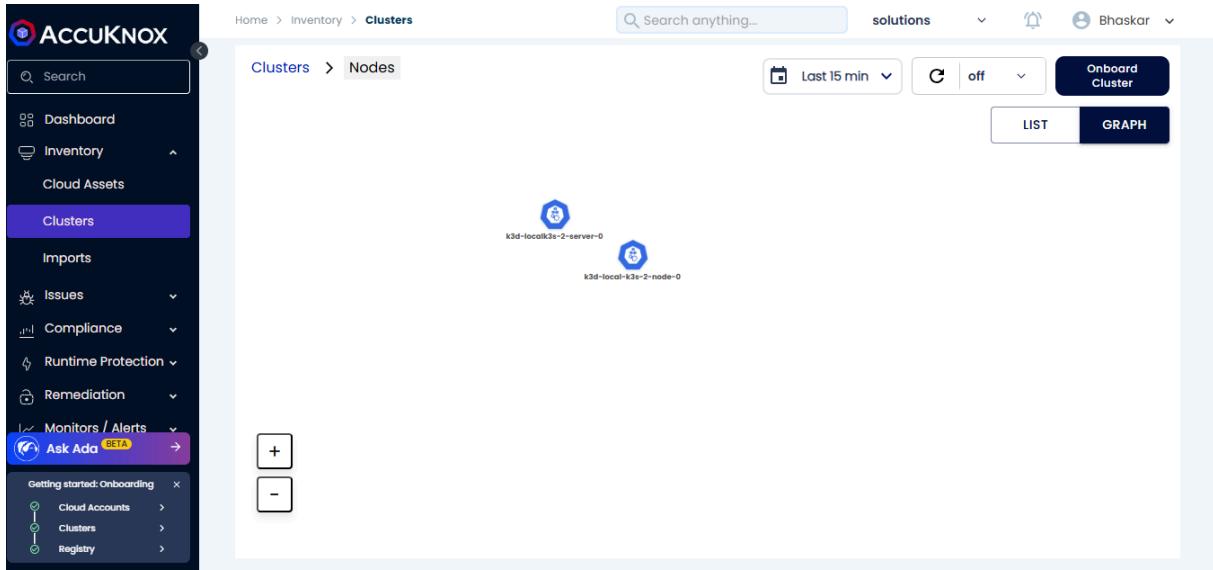
Under Inventory -> Clusters -> you can see the graphical view of all the clusters.



To see nodes of your cluster, click on the cluster name, click on “View Nodes”



You can see the Nodes of that cluster.



The screenshot shows the ACCUKNOK cloud platform interface. The left sidebar has a dark theme with purple highlights for selected items. It includes sections for Dashboard, Inventory (Cloud Assets, Clusters), Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, and an Ask Ada BETA button. A 'Getting started: Onboarding' section lists Cloud Accounts, Clusters, and Registry. The main content area is titled 'Clusters > Nodes'. It features a search bar, a date range selector ('Last 15 min'), a status switch ('off'), and an 'Onboard Cluster' button. Below these are two nodes represented by hexagonal icons with blue outlines: 'k3d-local-k3s-2-server-0' and 'k3d-local-k3s-2-node-0'. At the bottom left of the main area are '+' and '-' buttons.

14. Host Security

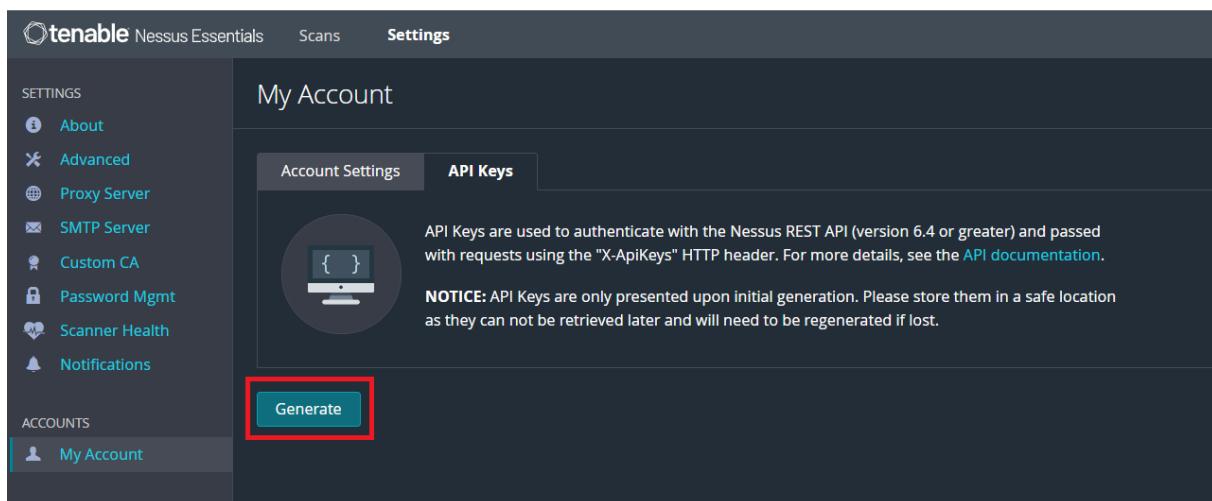
14.1 Host Scan

AccuKnox provides host scanning capabilities through an integration with tools like Nessus, Masscan and Zeek.

14.2 Prerequisites for Nessus Integration

To integrate Nessus with AccuKnox, the Nessus scanner is required to be deployed securely in the target environment with the nessus port accessible by AccuKnox SaaS. To fetch the results from the Nessus deployment, AccuKnox requires the Nessus Deployment URL and the API keys.

To generate the API keys, switch to the **Settings** tab, navigate to **My Account → API keys** and click on **Generate**

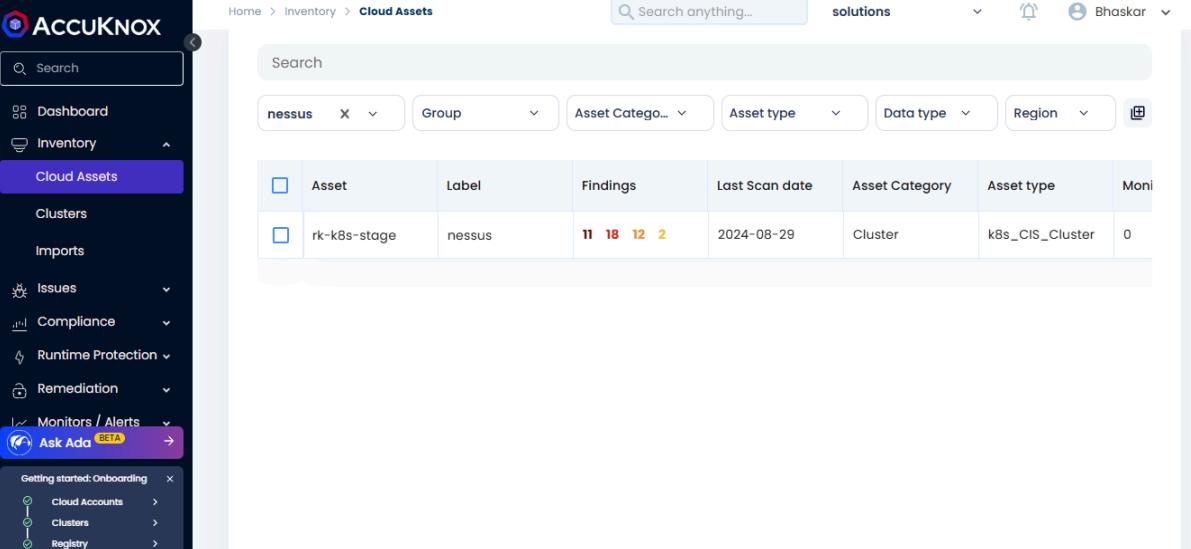


Copy the Access and Secret keys that are generated for the integration.

14.3 Asset Inventory

As Nessus scans all the hosts in the environment, the data is processed to improve the Asset Inventory of AccuKnox with additional data about the Hosts scanned through Nessus.

Step 1: Navigate to Inventory → Cloud Assets



The screenshot shows the AccuKnox interface. On the left, there's a sidebar with navigation links like Dashboard, Inventory (selected), Cloud Assets (selected), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Ask Ada (Beta), and Getting started: Onboarding (Cloud Accounts, Clusters, Registry). The main area is titled "Cloud Assets" and shows a table with one row. The table columns are Asset (checkbox), Label, Findings (containing 11, 18, 12, 2), Last Scan date (2024-08-29), Asset Category (Cluster), Asset type (k8s_CIS_Cluster), and Mon. The asset listed is "rk-k8s-stage" with the label "nessus".

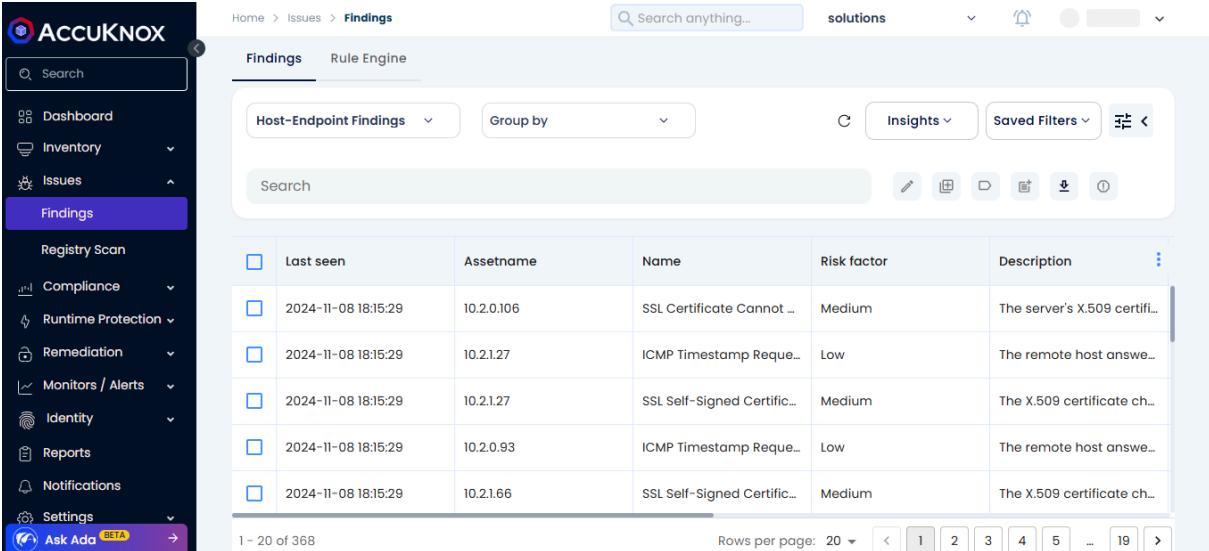
<input type="checkbox"/>	Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Mon
<input type="checkbox"/>	rk-k8s-stage	nessus	11 18 12 2	2024-08-29	Cluster	k8s_CIS_Cluster	0

Step 2: Filter using the **Label** name used for integrating Nessus to view only the assets that were identified using Nessus scanner and their associated findings.

14.4 Vulnerability Management

The vulnerabilities found using Nessus are populated in the AccuKnox SaaS in addition to the findings from other tools for easy management on a single platform.

Step 1: Navigate to Issues → Findings -> select Host-Endpoint Findings from the Findings filter.

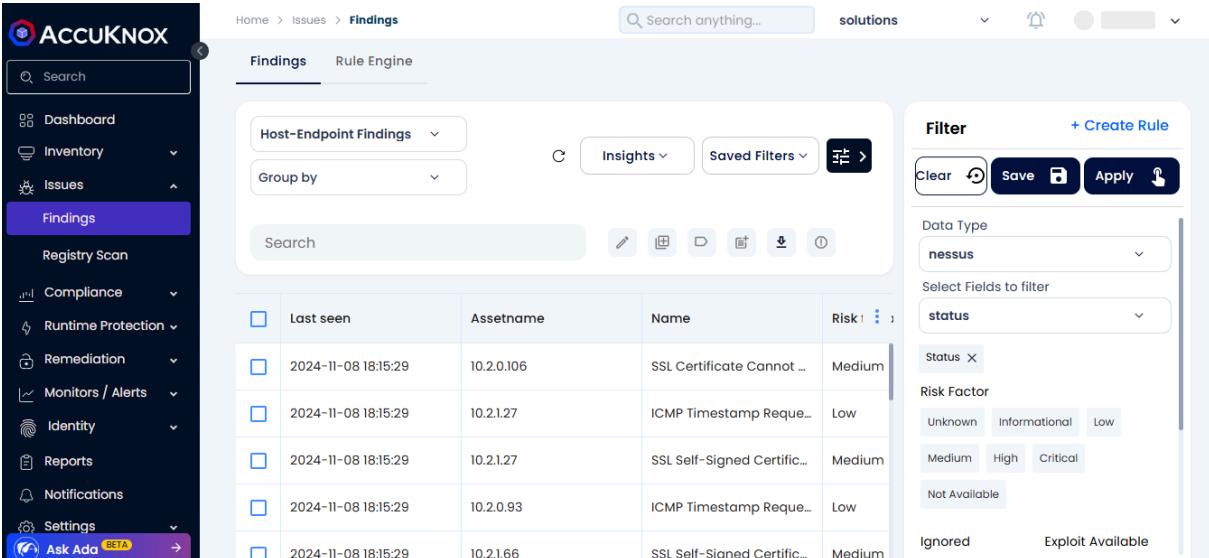


The screenshot shows the AccuKnox interface for viewing findings. The left sidebar has a purple 'Findings' section selected. The main area displays a table of findings with columns: Last seen, Assetname, Name, Risk factor, and Description. The table lists several entries, mostly from 'Host-Endpoint Findings'. A search bar at the top right and a navigation bar with 'Home', 'Issues', and 'Findings' are also visible.

Last seen	Assetname	Name	Risk factor	Description
2024-11-08 18:15:29	10.2.0.106	SSL Certificate Cannot ...	Medium	The server's X.509 certifi...
2024-11-08 18:15:29	10.2.1.27	ICMP Timestamp Reque...	Low	The remote host answe...
2024-11-08 18:15:29	10.2.1.27	SSL Self-Signed Certific...	Medium	The X.509 certificate ch...
2024-11-08 18:15:29	10.2.0.93	ICMP Timestamp Reque...	Low	The remote host answe...
2024-11-08 18:15:29	10.2.1.66	SSL Self-Signed Certific...	Medium	The X.509 certificate ch...

Step 2: To view only the findings from Nessus, choose **Nessus** from the **Data Type** filter.

This will list the issues identified by Nessus such as SSL certificate issues, vulnerable software versions in use, etc...



The screenshot shows the AccuKnox interface with a 'Filter' sidebar open on the right. The 'Data Type' dropdown is set to 'nessus'. Other filter options like 'status', 'Risk Factor', and 'Ignored' are also visible. The main table of findings is identical to the one in the previous screenshot, showing Nessus-related issues.

To learn more about how AccuKnox's advanced Vulnerability Management can be leveraged, refer here

AccuKnox can also leverage other tools such as Masscan and Zeek to provide host scanning. By integrating these tools, AccuKnox will be able to scan the on-premise environment and help in identifying issues on the hosts.

Masscan helps red teamers doing offensive research (penetration testing) as well as blue teamers and IT managers doing defensive research (to find attack vectors within the network).

Zeek is a Network Security Monitor (NSM) to support detection and investigations of suspicious or malicious activity. Zeek also supports a wide range of traffic analysis tasks beyond the security domain, including performance measurement and troubleshooting.

15. Admission Controller Support Using Knoxguard

As Kubernetes adoption continues to surge, securing your clusters becomes critical. Knoxguard, the latest security feature, aims to bolster Kubernetes environment security and compliance through robust policy enforcement. Knoxguard operates independently of any policy engine, offering the flexibility to integrate with your preferred enforcement add on. Currently, Knoxguard supports **Kyverno** as the policy enforcement engine.

15.1 Introduction

Key Features of Knoxguard/Admission Controller

Registry Restrictions

Registry Restrictions allow you to define rules that either restrict or whitelist specific container registries or patterns at the **cluster** and **namespace** levels. This feature ensures that only trusted images are deployed within your Kubernetes clusters, reducing the risk of deploying vulnerable or malicious containers.

Vulnerability Scan Thresholds (Pipeline Feature)

Knoxguard enables you to set thresholds for the maximum number of **critical** or **high-level vulnerabilities** that an image can have. This feature will block the deployment of images with known vulnerabilities, maintaining a high security posture for your applications.

Security Posture Rules

Enforcing security policies like **privileged container restrictions** and **capabilities constraints** helps maintain a secure Kubernetes environment. Knoxguard currently supports **denying privileged mode containers**, with more security rules expected to be added soon.

15.2 Prerequisite for Knoxguard Admission Controller

Before deploying Knoxguard in your Kubernetes environment, ensure the following prerequisite is met:

- **Accuknox Agent Installation:** Install Accuknox Agents on your Kubernetes cluster. These agents facilitate SaaS integration, alerting, and enforcement.

Info

Refer to Cluster On-boarding guide for Accuknox Agents Installation.

Verify the agents' status using the following command:

```
userx@fedora:~$ kubectl get pods -n accuknox-agents
NAME                                         READY   STATUS
RESTARTS          AGE
agents-operator-d8585d594-55s29           1/1    Running   0
72d
discovery-engine-59c69ff787-scrrj         4/4    Running   0
72d
feeder-service-765d8f7d65-d4vq2          1/1    Running   13
(2d21h ago)      4d
policy-enforcement-agent-f5c5f87b-9fw79   1/1    Running   84 (2d21h
ago)      40d
shared-informer-agent-77569db588-c944p     1/1    Running   1090 (2m36s
ago)     40d
```

15.3 Deployment of Knoxguard

Deploy Kyverno:

First, you need to deploy Kyverno, a policy engine for Kubernetes, which Knoxguard utilizes for policy enforcement.

```
helm repo add kyverno https://kyverno.github.io/kyverno/  
helm repo update  
helm install kyverno kyverno/kyverno -n kyverno --create-namespace
```

Step 2: Deploy Knoxguard:

Next, deploy Knoxguard in your Kubernetes cluster. Knoxguard will work in tandem with Kyverno to enforce the defined policies.

```
helm upgrade --install knoxguard oci://public.ecr.aws/k9v9d5v2/knoxguard-chart  
--version=v0 -n knoxguard --create-namespace
```

Verify the deployments:

```
userx@fedora:~$ kubectl get deployments -n knoxguard  
NAME                           READY   UP-TO-DATE   AVAILABLE   AGE  
accuknox-knoxguard-controller-manager   1/1     1           1           16s  
userx@fedora:~$ kubectl get pods -n kyverno  
NAME                           READY   STATUS    RESTARTS   AGE  
kyverno-admission-controller-78d5464dbc-p2248   1/1     Running   1 (49m ago)  52m  
kyverno-background-controller-5f96748b4c-mrcxm   1/1     Running   0 52m  
kyverno-cleanup-admission-reports-28796130-mzg8t   0/1     Completed  0 4m2s  
kyverno-cleanup-cluster-admission-reports-28796130-9nkb7   0/1     Completed  0 4m2s
```

kyverno-cleanup-cluster-ephemeral-reports-28796130-drsmn	0/1	Completed	0
4m2s			
kyverno-cleanup-controller-7b5fb595d6-x57g7	1/1	Running	0
52m			
kyverno-cleanup-ephemeral-reports-28796130-mxnkx	0/1	Completed	0
4m2s			
kyverno-reports-controller-76cd67fb8d-v66wm (49m ago)	1/1	Running	1
52m			

15.4 Policy Enforcement

Once Knoxguard is deployed, you can start enforcing policies within your cluster. This involves Creating, uploading and activating your custom admission policies.

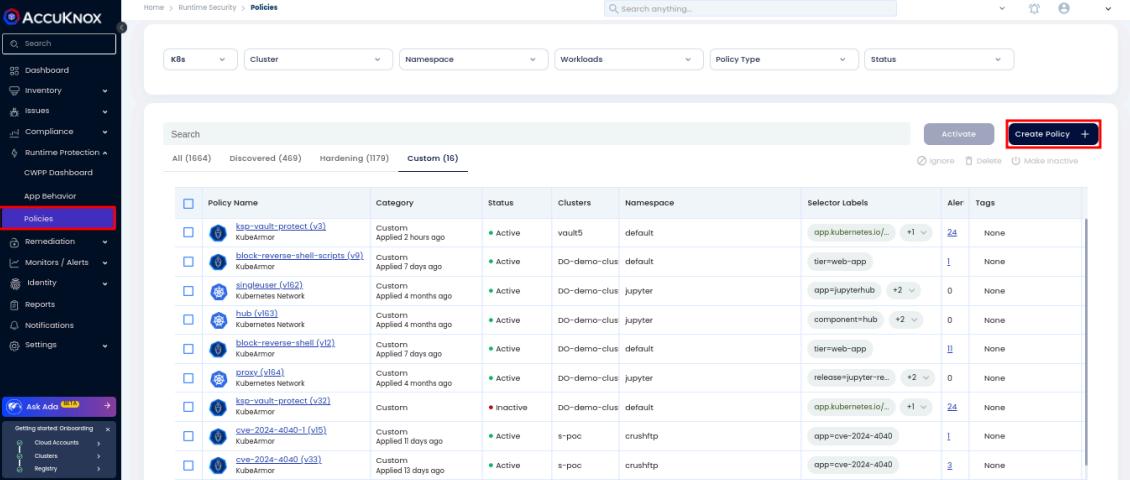
To enforce the admission policy, follow these steps with example:

1. **Define the Admission Policy:** Create an **AdmissionPolicy** resource based on the requirement. Below is the configuration to block privileged pod admission in the default namespace:

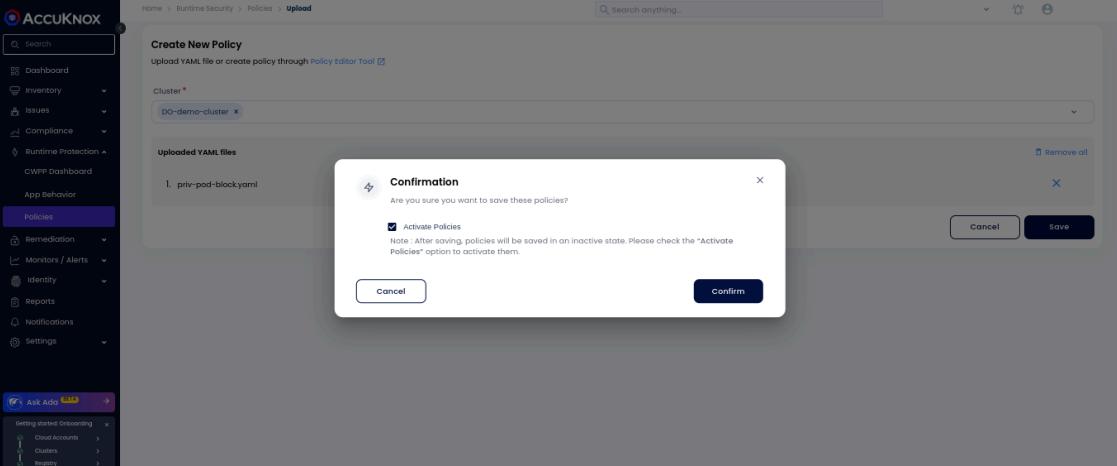
```
apiVersion: admission.accuknox.com/v1
kind: AdmissionPolicy
metadata:
  labels:
    app.kubernetes.io/name: admission-controller
    app.kubernetes.io/managed-by: kustomize
  name: test-priv-pod-policy
spec:
  denyPrivilegedPod:
    action: Block
    targetNamespaces:
      - default
```

1. Upload and Activate Admission Policies:

Use the upload YAML feature to upload your custom admission policies by clicking on Create Policy. This allows you to define and enforce policies specific to your security requirements.



The screenshot shows the ACCUKNOW platform's Runtime Security section, specifically the Policies page. On the left, there is a sidebar with various navigation options like Dashboard, Inventory, Issues, Compliance, Runtime Protection, App Behavior, Policies (which is selected and highlighted in purple), Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. A central search bar at the top has a placeholder 'Search anything...'. Below it are several dropdown filters: K8s, Cluster, Namespace, Workloads, Policy Type, and Status. A main table lists 16 policies, with columns for Policy Name, Category, Status, Clusters, Namespace, Selector Labels, Alert, and Tags. Some policies are marked as Active (green dot) and others as Inactive (red dot). The 'Create Policy +' button is highlighted with a red box in the top right corner of the table header.



This screenshot shows the 'Create New Policy' dialog box. It includes fields for 'Cluster' (set to 'DO-demo-cluster') and 'Uploaded YAML files' (with a file named 'priv-pod-block.yaml' listed). A confirmation dialog box is overlaid on the main screen, asking 'Are you sure you want to save these policies?' with a checkbox for 'Activate Policies'. The background shows the same ACCUKNOW interface as the previous screenshot, with the 'Policies' tab selected.

After uploading and activating the policy, you can verify its status with the following command:

```
userx@fedora:~$ kubectl get admissionpolicy
NAME          READY   MESSAGE
OWNED_PPLICIES
test-priv-pod-policy  True    clusterpolicy has been updated successfully
["knoxguard-privilege-pod-test-priv-pod-policy"]
```

15.5 Policy Violation and Alerts

In the event of a policy violation, Accuknox provides detailed alerts to help you understand and mitigate security issues.

First, attempt to deploy a privileged pod using the following configuration:

```
apiVersion: v1
kind: Pod
metadata:
  name: test-privileged
  namespace: default
spec:
  containers:
  - name: nginx
    image: nginx:latest
    securityContext:
      privileged: true # Should be blocked
```

Upon execution, you will receive an error message indicating that the request has been denied due to policy enforcement.

```
userx@fedora:~$ kubectl apply -f privpod.yaml
Error from server: error when creating "privpod.yaml": admission webhook
"validate.kyverno.svc-fail" denied the request:

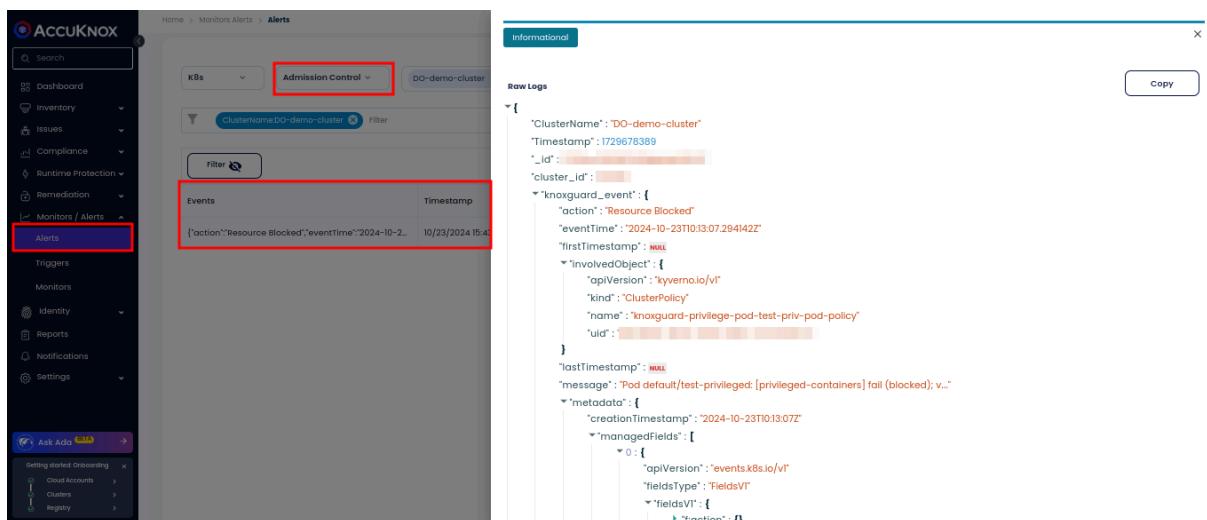
resource Pod/default/test-privileged was blocked due to the following policies

knoxguard-privilege-pod-test-priv-pod-policy:
  privileged-containers: "validation error: Privileged mode is disallowed. The
fields
  spec.containers[].securityContext.privileged,\n\t\t\ttspec.initContainers[].sec
  urityContext.privileged,
  and spec.ephemeralContainers[*].securityContext.privileged must be unset or
  set
  to false. rule privileged-containers failed at path
  /spec/containers/0/securityContext/privileged/"
```

Navigate to **Monitors > Alerts** in the AccuKnox dashboard. Change the alert type to **Admission Controller** to view alerts related to admission policy violations. The system provides comprehensive logging to help you quickly identify and address any security concerns.

Info

These logs can be forwarded to SIEM tools or notification tools by setting up triggers for improved security monitoring. Refer to the guide here for more details.



The screenshot shows the AccuKnox dashboard with the 'Monitors > Alerts' page selected. The 'Admission Control' filter is applied, and a log entry is displayed in the 'Raw Logs' panel. The log entry details a resource being blocked due to a cluster policy violation.

```

{
  "ClusterName": "DO-demo-cluster",
  "Timestamp": "1729678389",
  "Id": "redacted",
  "cluster_id": "redacted",
  "knoguard_event": {
    "action": "Resource Blocked",
    "eventTime": "2024-10-23T10:13:07.294142Z",
    "firstTimestamp": "null",
    "involvedObject": {
      "apiVersion": "kyverno.io/v1",
      "kind": "ClusterPolicy",
      "name": "knoguard-privileged-pod-test-priv-pod-policy",
      "uid": "redacted"
    },
    "lastTimestamp": "null",
    "message": "Pod default/test-privileged: [privileged-containers] fail (blocked); v_",
    "metadata": {
      "creationTimestamp": "2024-10-23T10:13:07Z"
    },
    "managedFields": [
      {
        "apiVersion": "events.k8s.io/v1",
        "fieldsType": "FieldsV1",
        "fieldsV1": {
          "action": "redacted"
        }
      }
    ]
  }
}

```

15.6 Pod Security Admission Controller

Pod Security Admission (PSA) enforces security standards on a Pod's Security Context and related fields based on three levels defined by the Pod Security Standards:

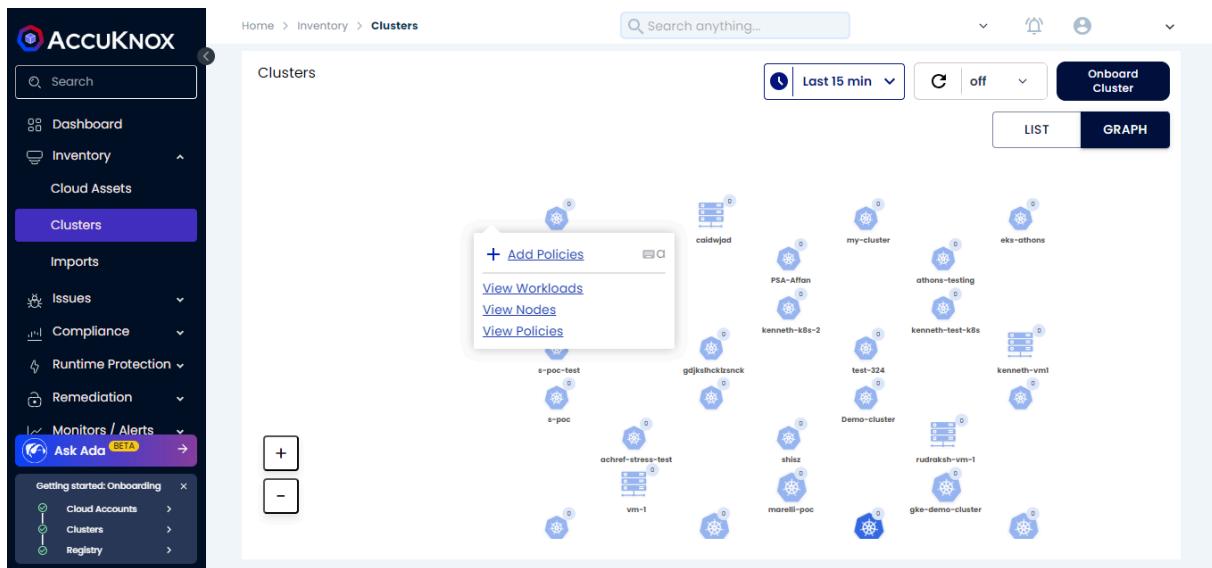
1. **Privileged**: Unrestricted policy, allows known privilege escalations.
2. **Baseline**: Minimally restrictive policy, allows default (minimally specified) Pod configuration.
3. **Restricted**: Heavily restricted policy, adhering to current Pod hardening best practices.

PSA can be enabled in two modes:

1. **Enforce**: Policy violations will cause the pod to be rejected.
2. **Audit**: Policy violations will trigger an alert but still allow the pod.

15.7 Enabling Pod Security Admission (PSA)

Navigate to **Inventory → Clusters** and click on the cluster, then select **View Workloads**.



1. Click on the **cog icon** next to the namespace.

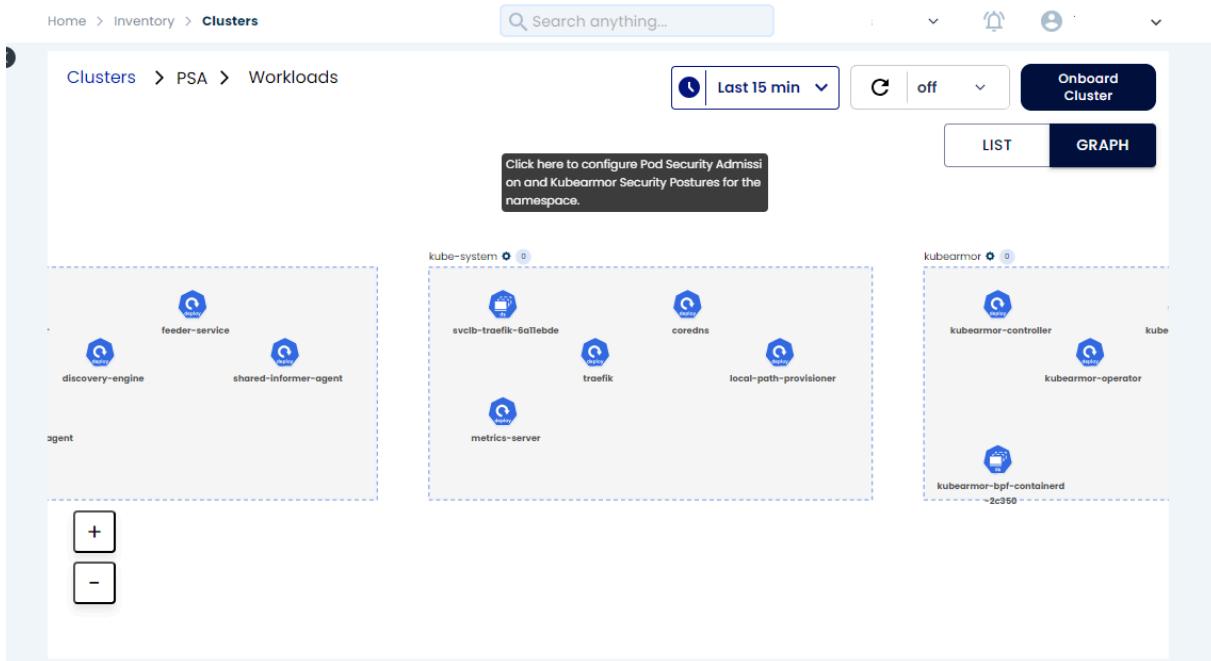
Home > Inventory > Clusters

Clusters > PSA > Workloads

Last 15 min | off | Onboard Cluster

LIST GRAPH

Click here to configure Pod Security Admission and Kubearmor Security Postures for the namespace.



2. Select the desired **PSA Level** and click **Save**.

Home > Inventory > Clusters

Clusters > PSA > Workloads

kube-system

KubeArmor Security Posture

Process File * Network *

Audit Audit

Reset Save

Pod Security Admission

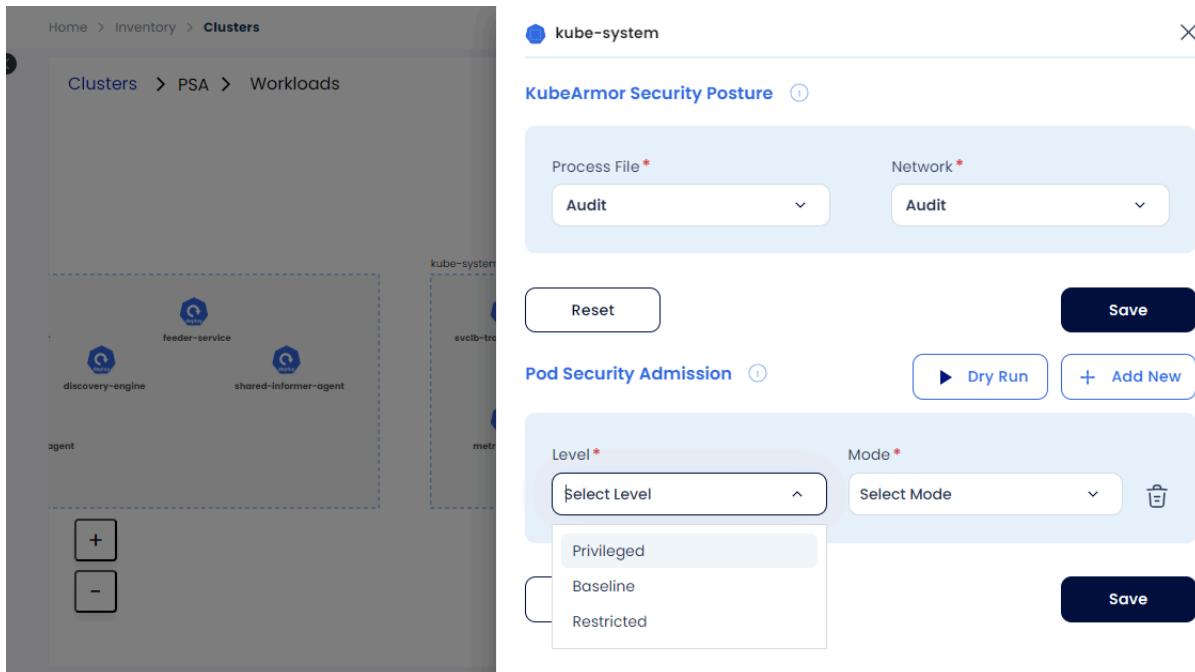
Dry Run Add New

Level * Mode *

Select Level Select Mode

Privileged Baseline Restricted

Save



3. Select the desired **Mode** for PSA.

kube-system X

KubeArmor Security Posture ⓘ

Process File * Network *

Audit Audit

Reset Save

Pod Security Admission ⓘ

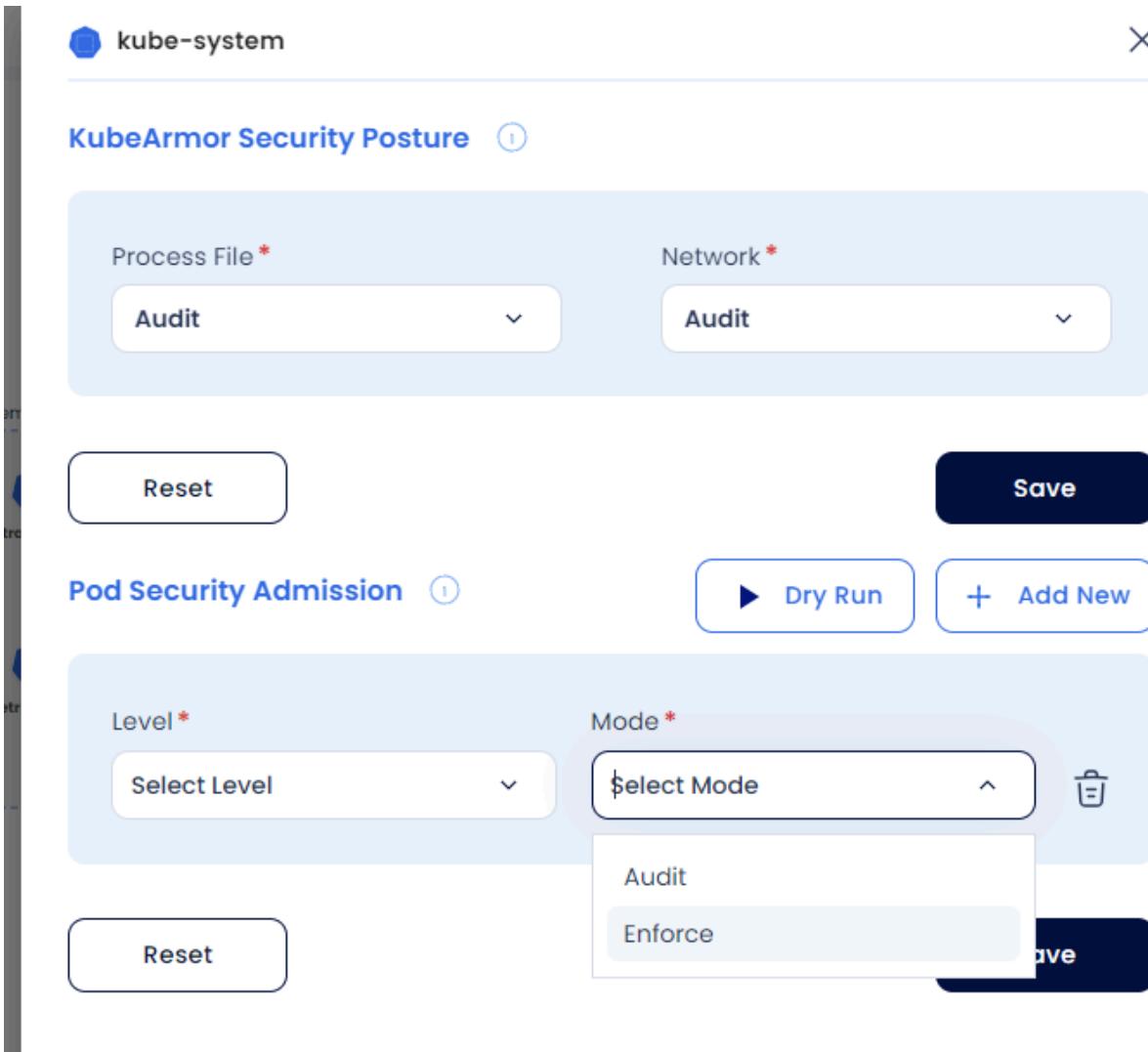
Dry Run Add New

Level * Mode *

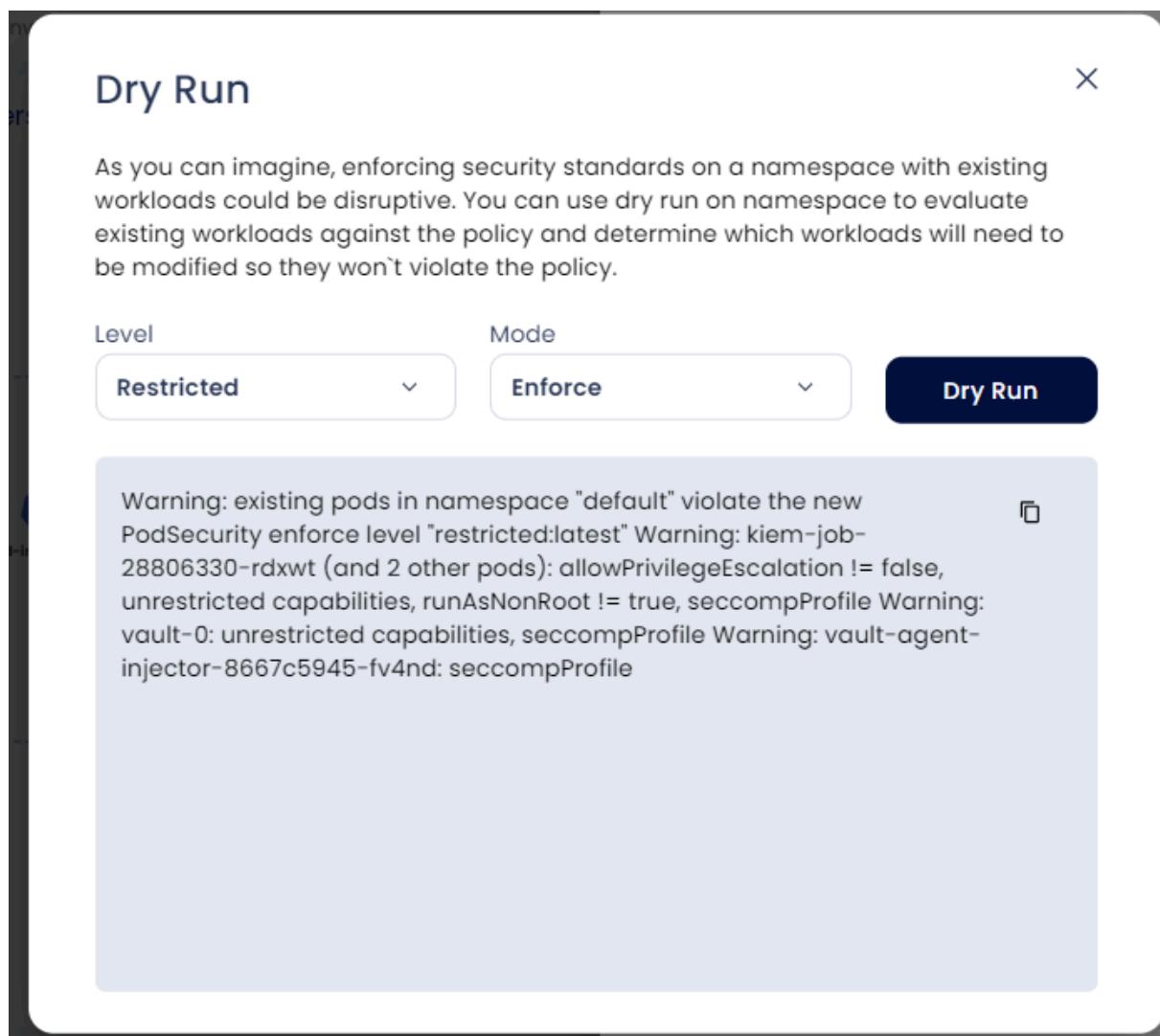
Select Level Select Mode

Audit Enforce

Reset Save



4. If using **Enforce** mode, click on **Dry Run** to preview potential effects before applying.



The **Dry Run** mode allows users to confirm potential effects of the PSA. Once reviewed and acceptable, click **Save** to apply the PSA.

15.8 PSA Protection Example

After setting PSA to enforce the **restricted** level, attempt to run a privileged Pod in the cluster:

```
root@demo:~# kubectl run nginx --image=nginx
```

An error will be returned as shown below:

```
Error from server (Forbidden): pods "nginx" is forbidden: violates PodSecurity
"restricted:latest": allowPrivilegeEscalation != false (container "nginx" must
set securityContext.allowPrivilegeEscalation=false), unrestricted capabilities
(container "nginx" must set securityContext.capabilities.drop=["ALL"]),
runAsNonRoot != true (pod or container "nginx" must set
securityContext.runAsNonRoot=true), seccompProfile (pod or container "nginx"
must set securityContext.seccompProfile.type to "RuntimeDefault" or "Localhost")
```

Since the **restricted** PSA label was applied to the namespace, attempting to create a pod with excessive privileges results in this error, successfully preventing the privileged pod from running.

16. CWPP Report Generation

Understand the Regex to Select the Cluster Name and Namespace

The CWPP report generation utilizes regular expressions (regex) to specify and filter cluster names and namespaces. The syntax for regex follows a particular pattern to ensure accurate selection.

16.1 Regex

Regex Syntax Format: Cluster Name Selection / Namespace Selection

16.1.1 Rules for Regular Expression

Excluding

- To exclude a specific cluster or namespace, prefix it with a hyphen (-).

NOTE

To exclude any cluster or namespace, it must be included in the selection first.

Select all

- Use an asterisk (*) to select all clusters or namespaces.

Delimiter

- A forward slash (/) is used to delimit the cluster name selection from the namespace selection.

Examples

- cluster1/ns1: Include only namespace ns1 from cluster cluster1.

- cluster1/*: Include all namespaces from cluster cluster1.
- cluster1/ns*: Include namespaces starting with ns from cluster cluster1.
- -cluster1/ns3: Exclude namespace ns3 from cluster cluster1.
- */ns1: Include namespace ns1 from all clusters.
- */*: Include all namespaces from all clusters.

16.2 Reports Configuration

Reports can be configured in two ways: On Demand and Scheduled.

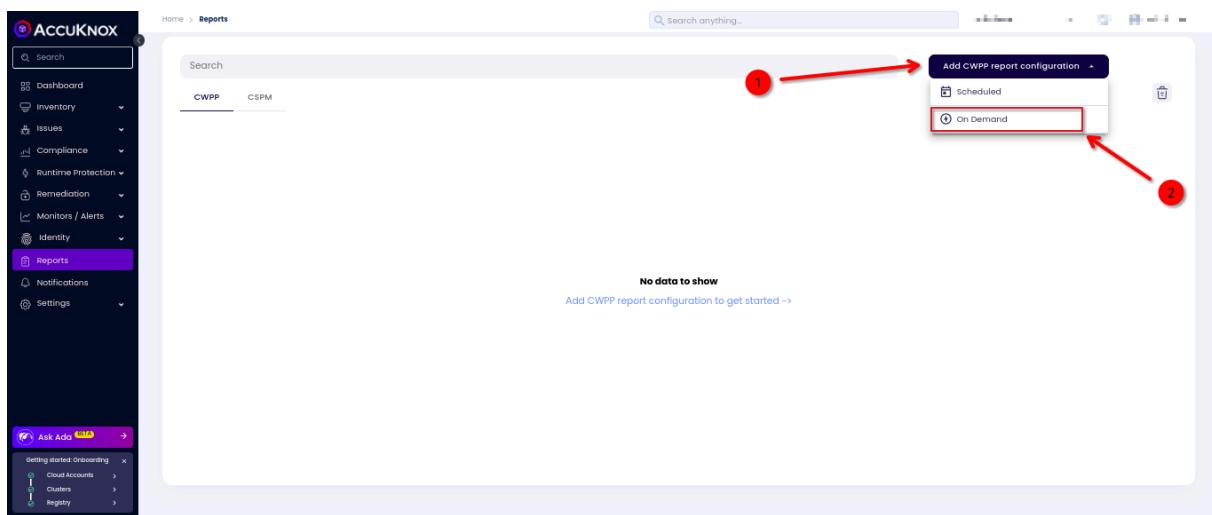
16.2.1 On Demand Report Configuration

In On Demand Report, you can generate the report for the clusters shortly after the configuration is completed.

To generate On Demand reports:

Step 1: Add CWPP Report Configuration

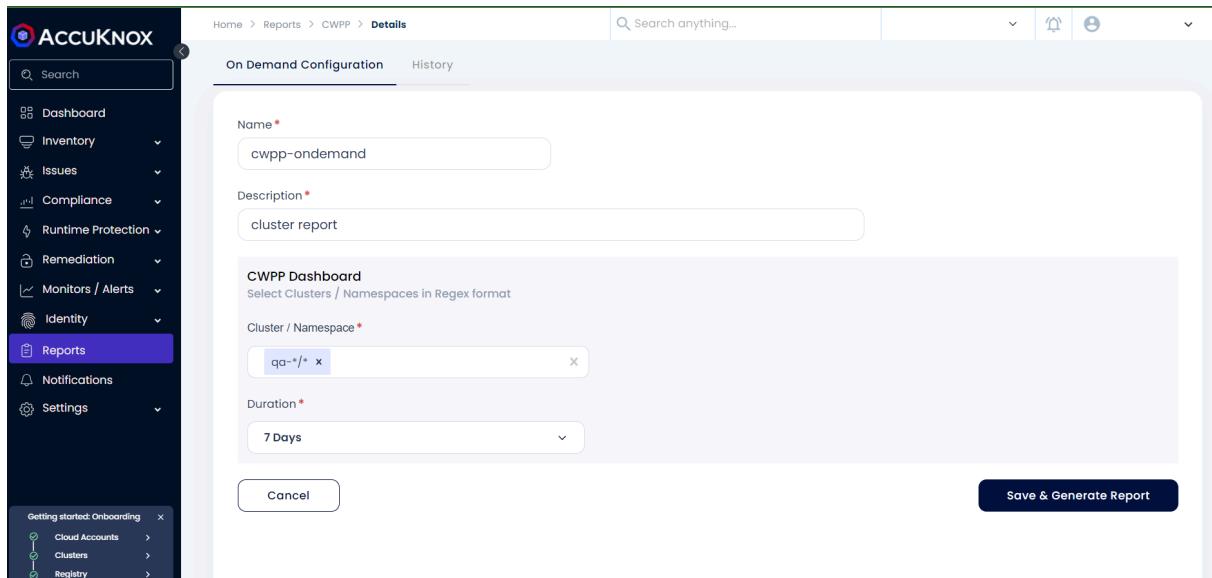
- Go to the Reports section in AccuKnox SaaS.
- Under CWPP Tab, click on “Add CWPP report configuration” and choose “On Demand” from the drop-down menu.



Step 2: In the Configuration user needs to provide the details about Name, Description and Cluster and Namespace.

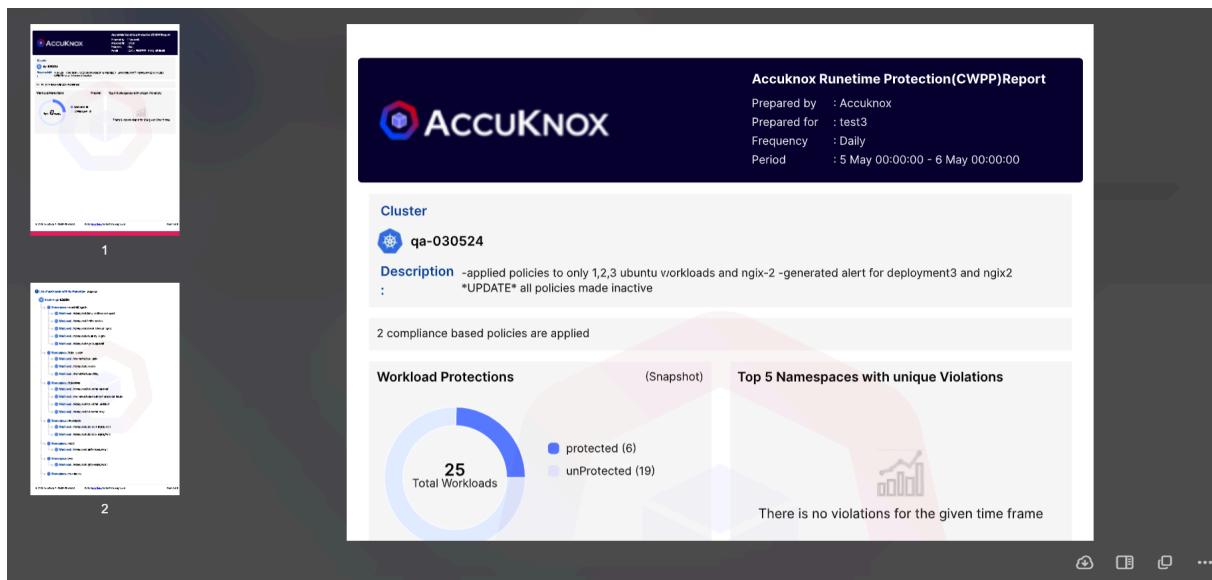
NOTE

The cluster field drop-down will show all the clusters that are active during the report generation.



The screenshot shows the 'On Demand Configuration' section of the AccuKnox interface. The 'Name' field is set to 'cwpp-on-demand'. The 'Description' field contains 'cluster report'. Under 'CWPP Dashboard', the 'Cluster / Namespace' dropdown is set to 'qa-*/*'. The 'Duration' dropdown is set to '7 Days'. At the bottom right is a large blue 'Save & Generate Report' button.

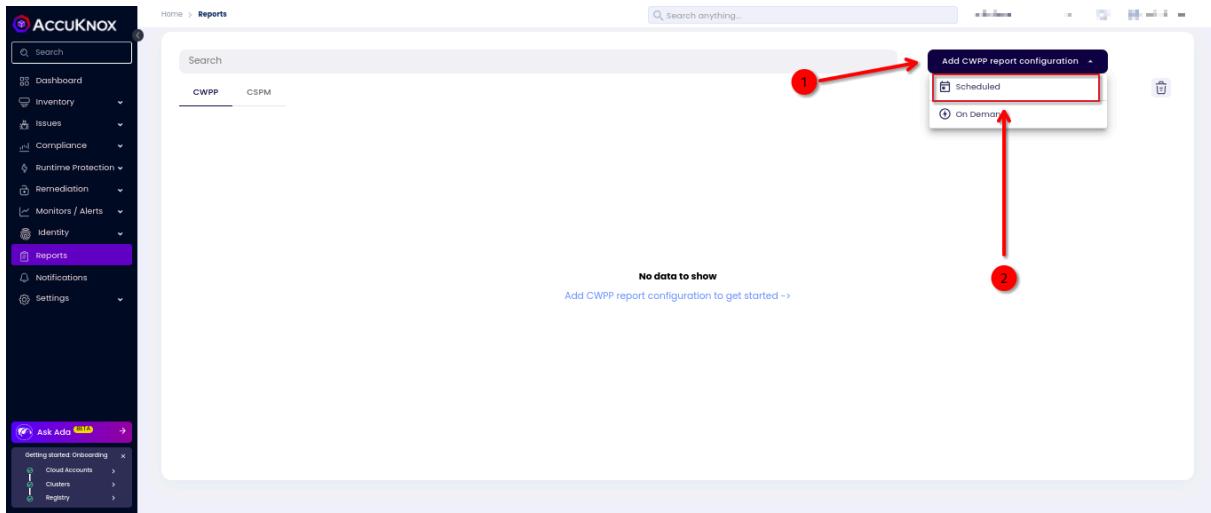
By clicking Save and Generate Report it will generate the report in the PDF format as per the selected duration.



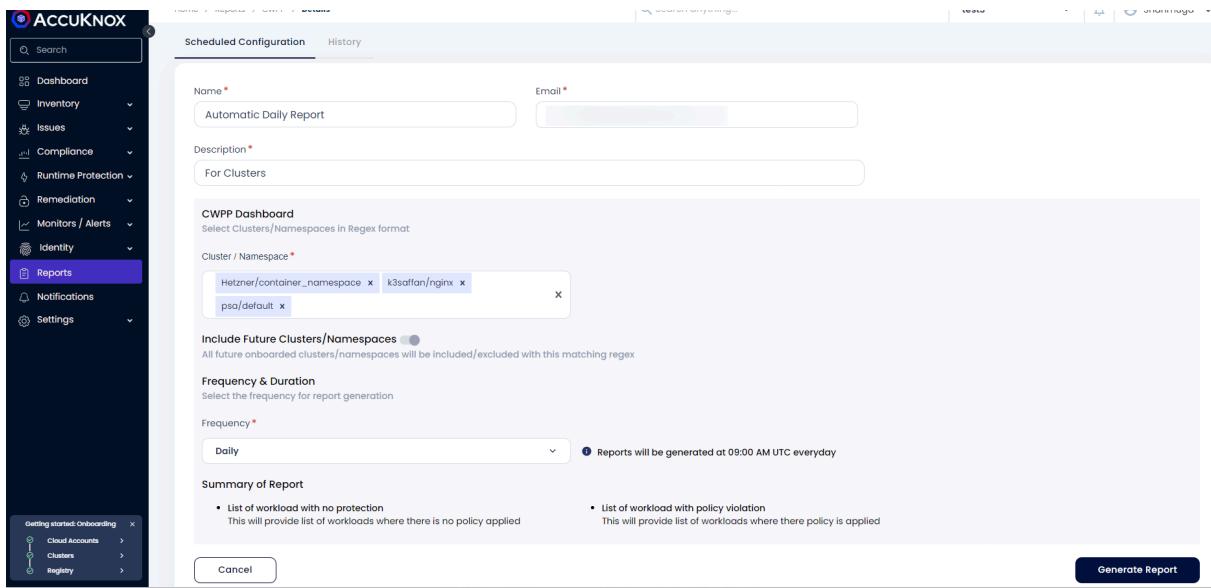
16.2.2 Scheduled Report Configuration

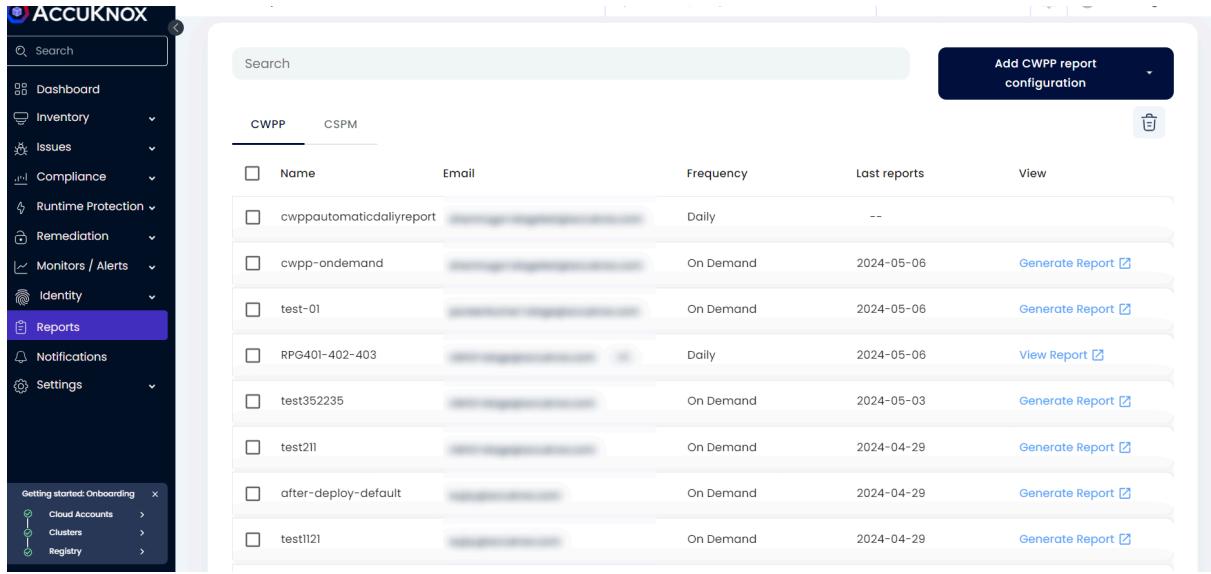
To get the report of the clusters automatically as per the frequency that is chosen .i.e by weekly or by monthly or daily this is the go to way:

Step 1: Add CWPP report configuration as Scheduled and choose the Scheduled option from the drop down.



Step 2: In the Configuration user needs to provide the details about their Name, Email, Selecting the Cluster, Namespace in the regex format and Frequency of the report then click the Generate Report.

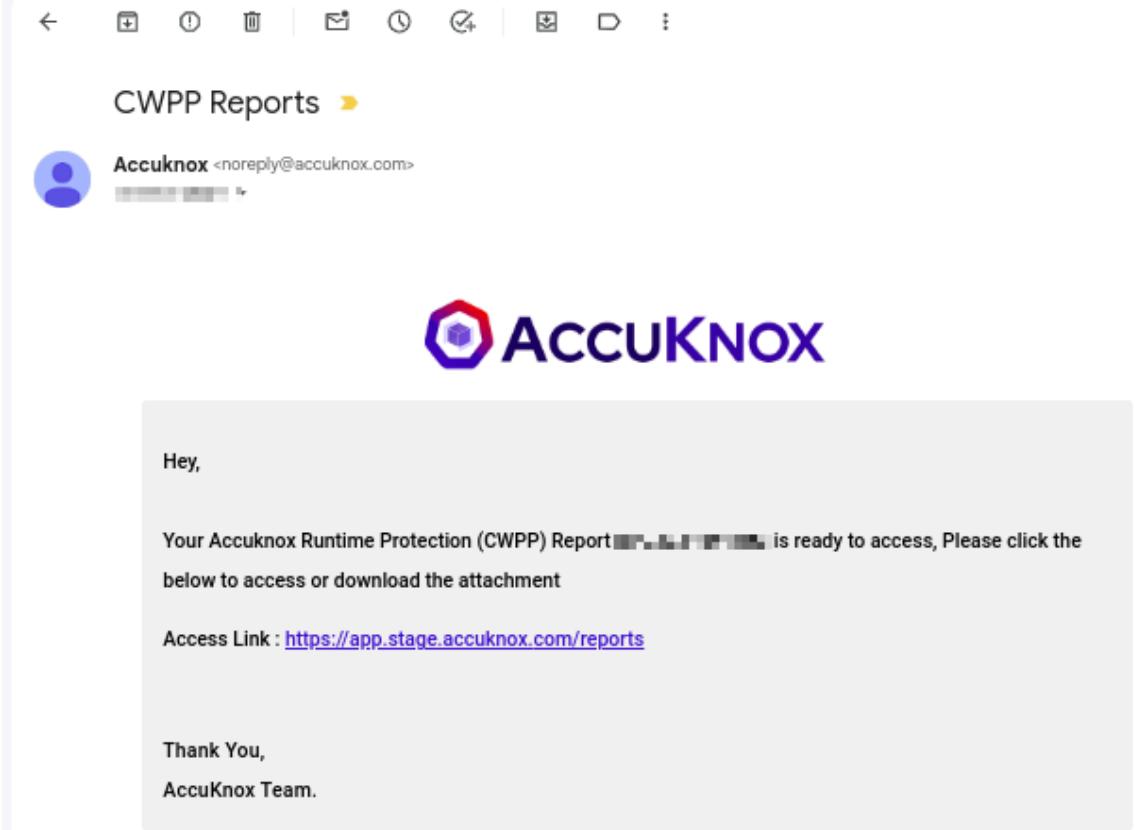




The screenshot shows the ACCUKNOX platform's user interface. On the left, there is a dark sidebar with a search bar at the top and several menu items: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports (which is selected and highlighted in purple), Notifications, and Settings. Below these, there is a "Getting started: Onboarding" section with links for Cloud Accounts, Clusters, and Registry. The main content area has a header with a search bar and a button to "Add CWPP report configuration". It features tabs for "CWPP" and "CSPM", with "CWPP" currently selected. A table lists various reports with columns for Name, Email, Frequency, Last reports, and View. Each row includes a checkbox, the report name, a blurred email address, frequency (Daily or On Demand), the last report date, and a "Generate Report" button. There is also a trash can icon in the top right corner of the main content area.

Name	Email	Frequency	Last reports	View
cwppautomaticdailyreport	[REDACTED]	Daily	--	Generate Report
cwpp-on-demand	[REDACTED]	On Demand	2024-05-06	Generate Report
test-01	[REDACTED]	On Demand	2024-05-06	Generate Report
RPG401-402-403	[REDACTED]	Daily	2024-05-06	View Report
test352235	[REDACTED]	On Demand	2024-05-03	Generate Report
test211	[REDACTED]	On Demand	2024-04-29	Generate Report
after-deploy-default	[REDACTED]	On Demand	2024-04-29	Generate Report
test1121	[REDACTED]	On Demand	2024-04-29	Generate Report

Step 3: After finishing the configuration the report would be scheduled to be sent to you in the email. Users can reconfigure the past configurations by clicking on them to edit the configuration.



The screenshot shows an email interface with a blue header bar containing standard icons like back, forward, and search. Below the header, the subject line "CWPP Reports" is visible, followed by a yellow right-pointing arrow. The sender is listed as "Accuknox <noreply@accuknox.com>" next to a blue circular profile picture. The main body of the email features the AccuKnox logo at the top. The message content includes a greeting "Hey," followed by a note about a runtime protection report being ready to access. It provides a blue hyperlink "Access Link : <https://app.stage.accuknox.com/reports>". At the bottom, it says "Thank You," and "AccuKnox Team."

17. Integrations

17.1 Integrate SIEM tools

- SPLUNK
- AWS Cloud Watch
- Rsyslog

17.1.1 Splunk

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

AccuKnox integrates with Splunk and monitors your assets and sends alerts for resource misconfigurations, compliance violations, network security risks, and

anomalous user activities to Splunk. To forward the events from your workspace you must have Splunk Deployed and HEC URL generated first for Splunk Integration.

a. Prerequisites:

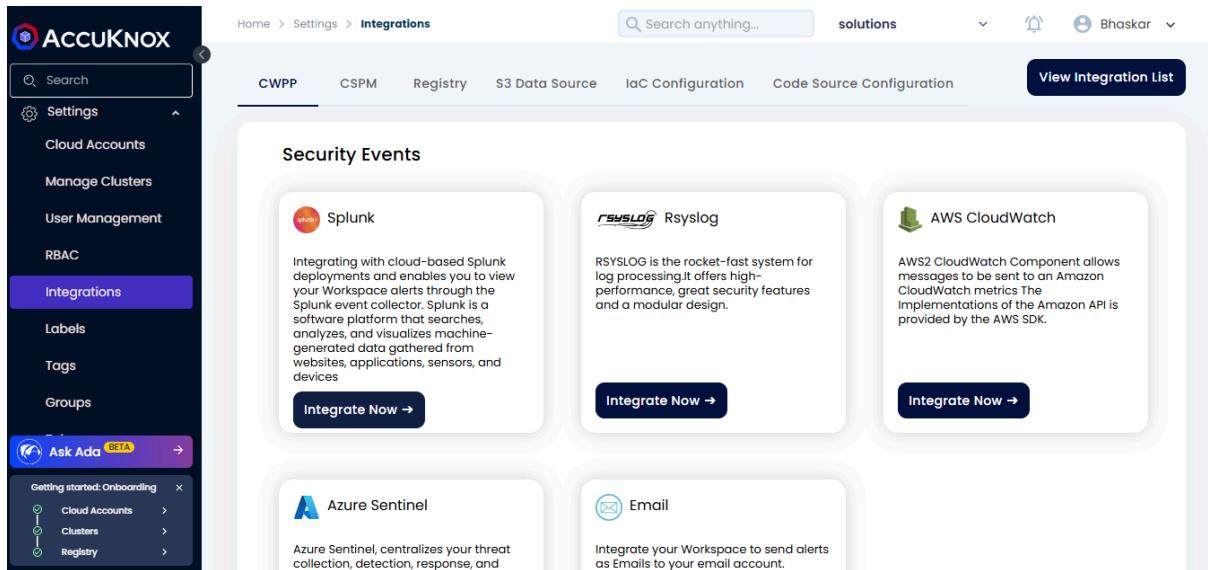
Set up Splunk HTTP Event Collector (HEC) to view alert notifications from AccuKnox in Splunk. Splunk HEC lets you send data and application events to a Splunk deployment over the HTTP and Secure HTTP (HTTPS) protocols.

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.

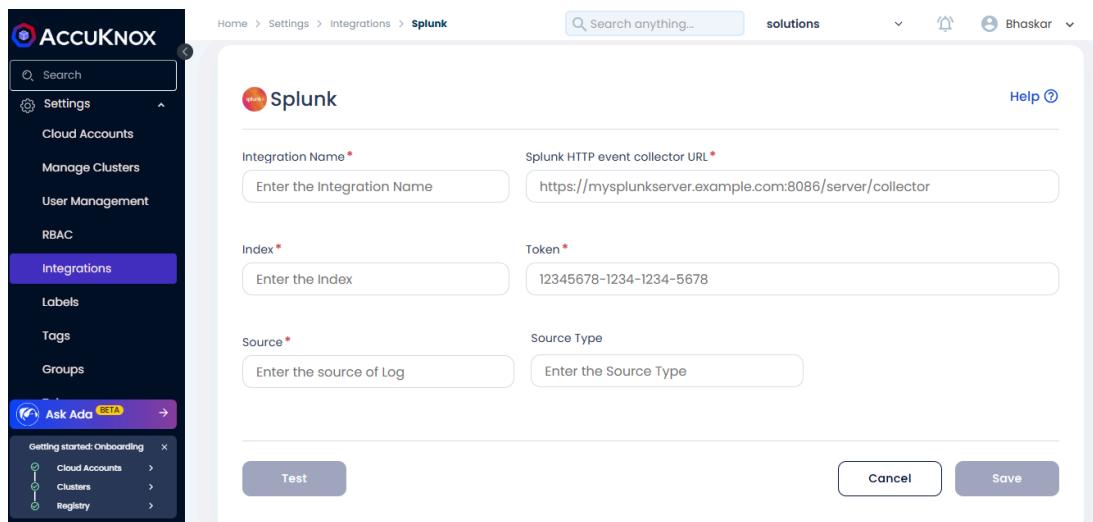
b. Steps to Integrate:

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



The screenshot shows the AccuKnox platform interface. On the left, there's a sidebar with navigation options like 'Search', 'Settings', 'Cloud Accounts', 'Manage Clusters', 'User Management', 'RBAC', 'Integrations' (which is highlighted in purple), 'Labels', 'Tags', and 'Groups'. Below this is a 'Ask Ada' BETA button and a 'Getting started: Onboarding' section with links for 'Cloud Accounts', 'Clusters', and 'Registry'. The main content area is titled 'Integrations' and shows several integration cards:

- Splunk**: Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices. [Integrate Now →](#)
- Rsyslog**: RSYSLOG is the rocket-fast system for log processing. It offers high-performance, great security features and a modular design. [Integrate Now →](#)
- AWS CloudWatch**: AWS CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics. The implementations of the Amazon API is provided by the AWS SDK. [Integrate Now →](#)
- Azure Sentinel**: Azure Sentinel, centralizes your threat collection, detection, response, and investigation. [Integrate Now →](#)
- Email**: Integrate your Workspace to send alerts as Emails to your email account. [Integrate Now →](#)



- 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.

17.1.2 AWS Cloudwatch

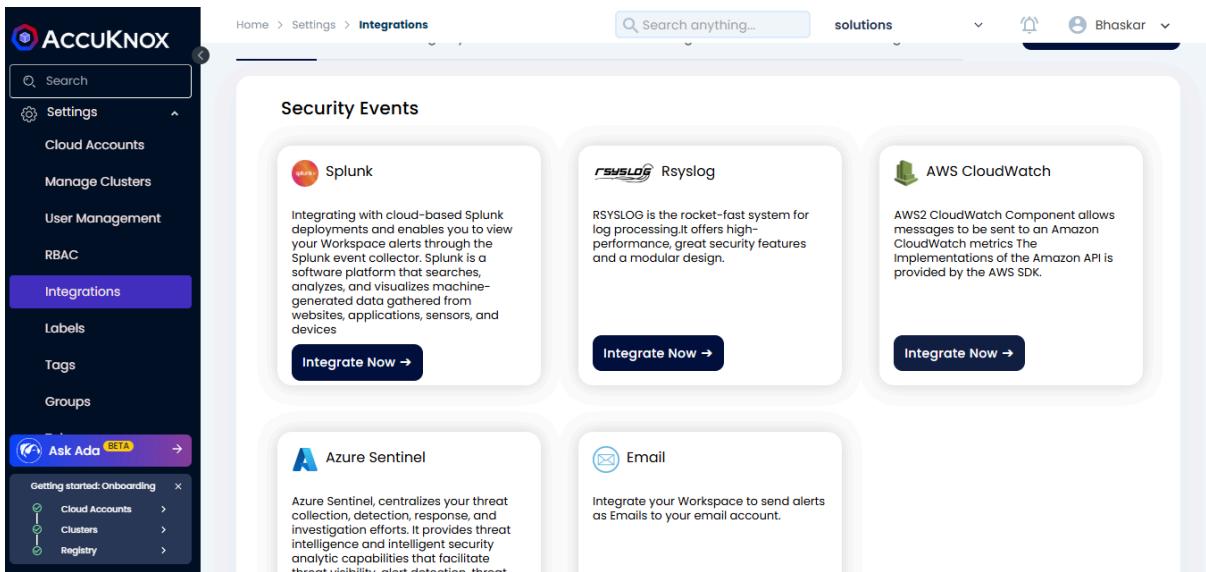
Navigate to Settings->Integrations. Choose "AWS CloudWatch" services and click the Integrate Now button.

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](#)

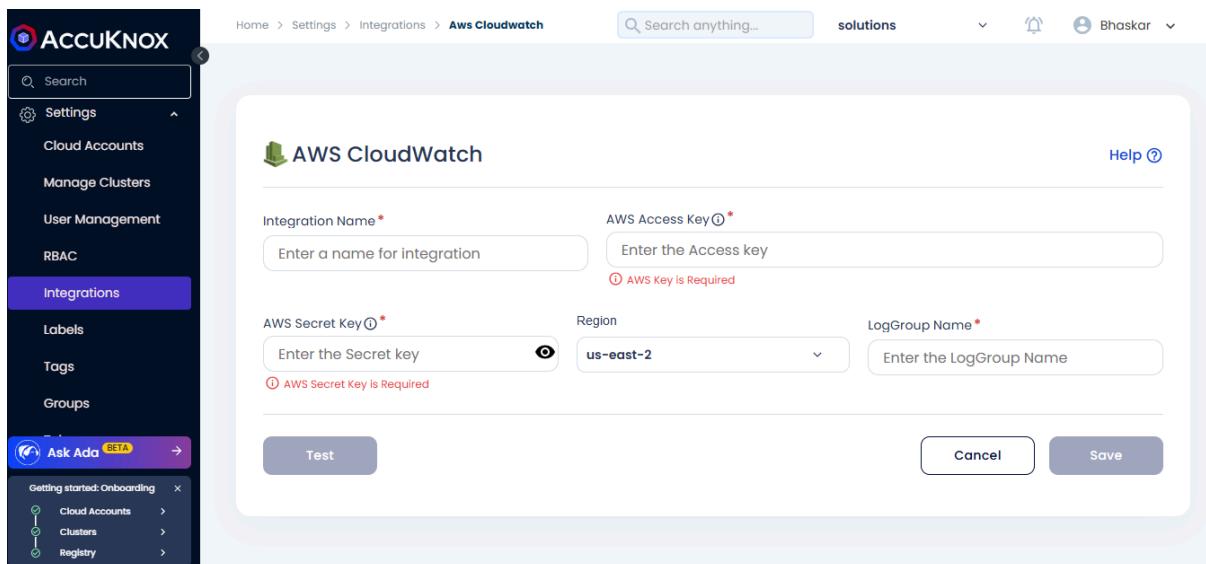
b. Steps to Integrate:

- Go to Settings -> Integration
- Click the Integrate Now button under AWS CloudWatch.



The screenshot shows the ACCUKNOKX platform's integrations page. On the left, there's a sidebar with options like Settings, Cloud Accounts, Manage Clusters, User Management, RBAC, Integrations (which is selected and highlighted in purple), Labels, Tags, Groups, and an Ask Ada BETA button. The main area is titled 'Security Events' and contains five integration cards:

- Splunk**: Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices. [Integrate Now →](#)
- Rsyslog**: Rsyslog is the rocket-fast system for log processing. It offers high-performance, great security features and a modular design. [Integrate Now →](#)
- AWS CloudWatch**: AWS CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics. The implementations of the Amazon API is provided by the AWS SDK. [Integrate Now →](#)
- Azure Sentinel**: Azure Sentinel centralizes your threat collection, detection, response, and investigation efforts. It provides threat intelligence and intelligent security analytic capabilities that facilitate threat visibility, alert detection, threat
- Email**: Integrate your Workspace to send alerts as Emails to your email account. [Integrate Now →](#)



- 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.

17.1.3 Azure Sentinel Integration

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

a. Prerequisites:

- Azure Logic App - Webhook.
- Azure Sentinel Subscription.

b. Steps to Integrate:

- Go to Settings → Integrations → CWPP(Tab).
- Click integrate now on Azure Sentinel.
- 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
 - **Webhook URL:** Enter your Azure Logic App's Webhook URL here. e.g., <https://xyz.xxxx.logic.azure.com:443/workflows/xxxxxx>
 - **Group Name:** You can specify any group name based on your preference, this can be used to filter the events. This works as a key value pair, where key is Group Name and Group Value is the value for the Key Group Name. e.g., K8s Cluster
 - **Group Value:** You can add any value to this group value. e.g., Dev Team Cluster
- Click **Test** to check the new functionality, You will receive the test message on configured Azure Sentinel. -Test message Please ignore !!
- Click **Save** to save the Integration. You can now configure Alert Triggers for Azure Sentinel Events

17.1.4 Creating webhook using the Azure Logic App

a. About the logic app:

Azure Logic Apps is a cloud platform where you can create and run automated workflows with little to no code. Using the visual designer and selecting from prebuilt operations, you can quickly build a workflow that integrates and manages your apps, data, services, and systems. To create a webhook using the logic app.

- **Step 1:** Search for the logic app in the Azure portal.
- **Step 2:** Add the new logic app and fill in the relevant details.
- **Step 3:** After creating the logic it will appear in the logic app dashboard.
- **Step 4:** Open the app and click on the go-to resource button.
- **Step 5:** Select the http request to receive the logs.
- **Step 6:** Click on the new step and click HTTP after that click on the Azure log analytics to receive the alert data.
- **Step 7:** Add the connection name, workspaceID, and workspace key.

You can get the workspace id and key in the log analytics workspace tab.

- **Step 8:** Click on the Integration and click on the Agents tab.
- **Step 9:** Click on the Azure log analytics data collector and click the JSON request body as the body and log name.

After the setup is done you will receive a webhook URL.

b. To see Logs in the Sentinel:

- **Step 1:** Open Microsoft Sentinel in the portal.
- **Step 2:** Click on the integrations.
- **Step 3:** Click on the logs tab and go to custom logs and select the time range and click on run the query to get the logs.

17.1.5 RSyslog

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

a. Prerequisites:

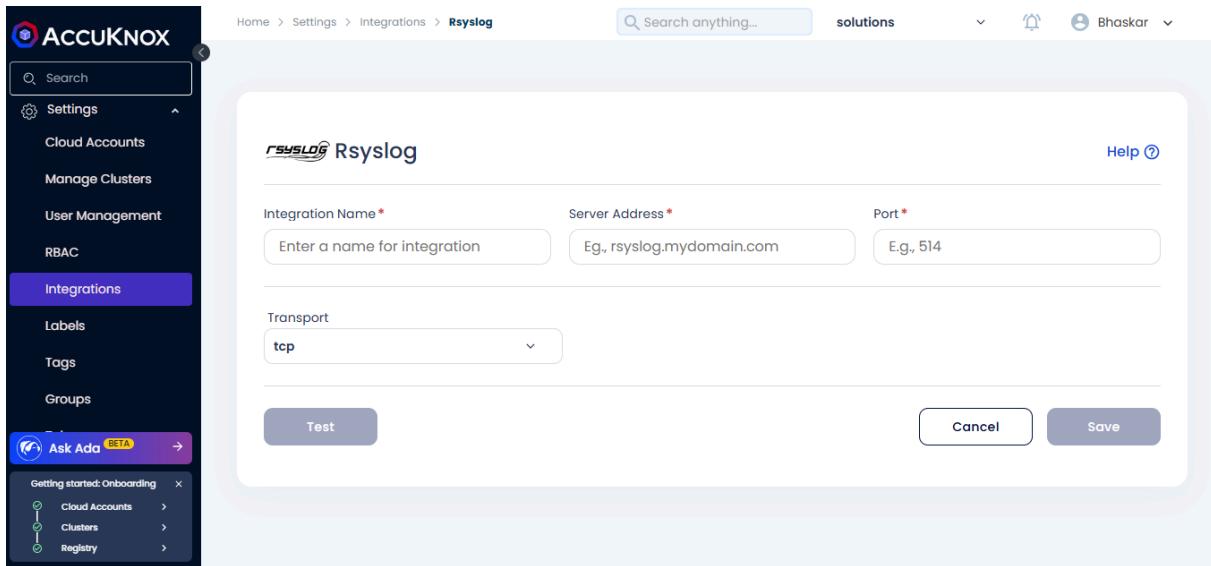
- A running RSyslog server.

- 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.
- 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

17.2 Integrate Notifications Tools

17.2.1 Slack

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

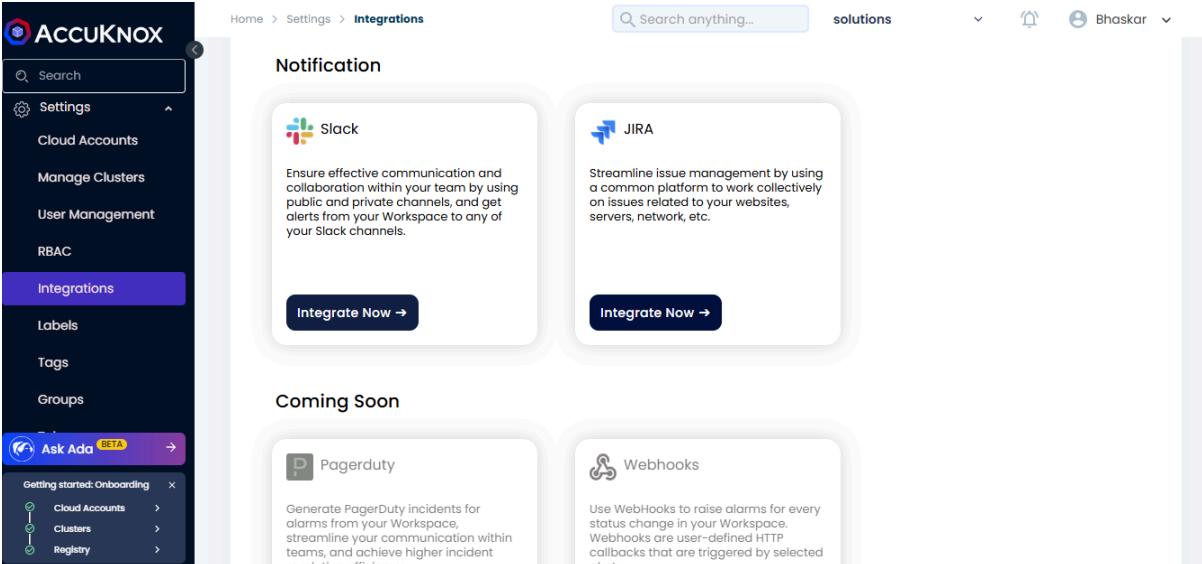
a. Prerequisites:

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

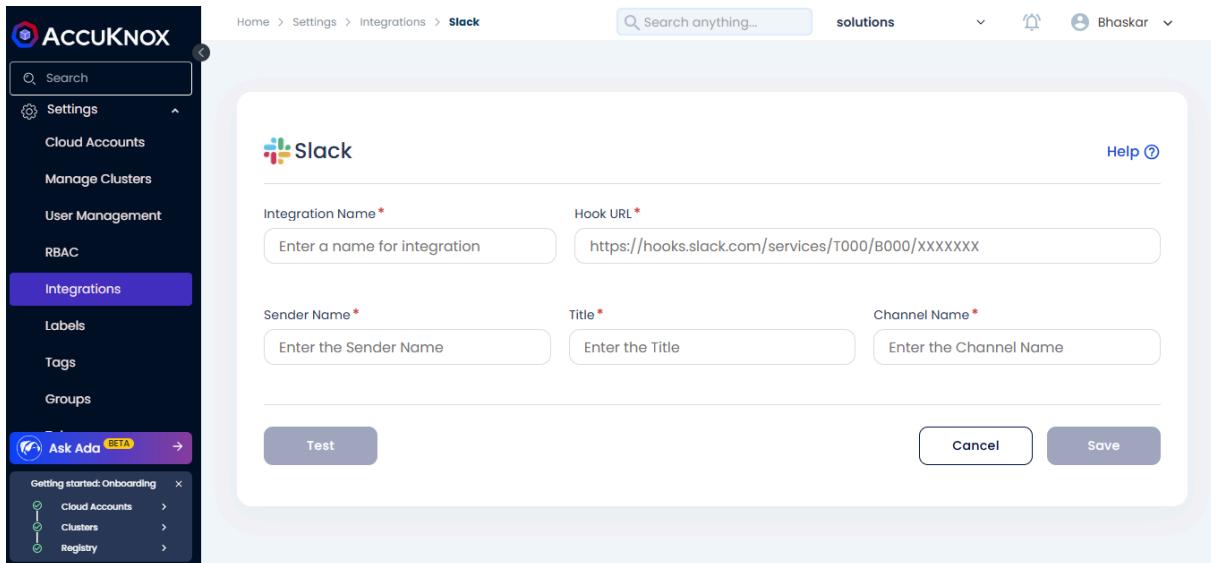
Note: To generate a Hook URL follow the steps, [Webhooks-for-Slack](#).

b. Steps to Integrate:

- Go to Settings -> Integration.
- Click “Integrate Now” under Slack.



The screenshot shows the ACCUKNOKX platform's interface. On the left, there is a sidebar with various navigation options: Settings, Cloud Accounts, Manage Clusters, User Management, RBAC, Integrations (which is currently selected and highlighted in purple), Labels, Tags, Groups, and Ask Ada (BETA). Below the sidebar, there is a "Getting started: Onboarding" section with three items: Cloud Accounts, Clusters, and Registry. The main content area is titled "Notification" and contains four cards: "Slack", "JIRA", "Coming Soon", and "Webhooks". The "Slack" card is the most prominent, featuring its logo and a brief description: "Ensure effective communication and collaboration within your team by using public and private channels, and get alerts from your Workspace to any of your Slack channels." It has a blue "Integrate Now →" button. The "JIRA" card also has a blue "Integrate Now →" button. The "Coming Soon" and "Webhooks" cards are partially visible below them.



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

17.3 Integrate Ticketing Tools

17.3.1 Jira Integration

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

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

Integration of JIRA:

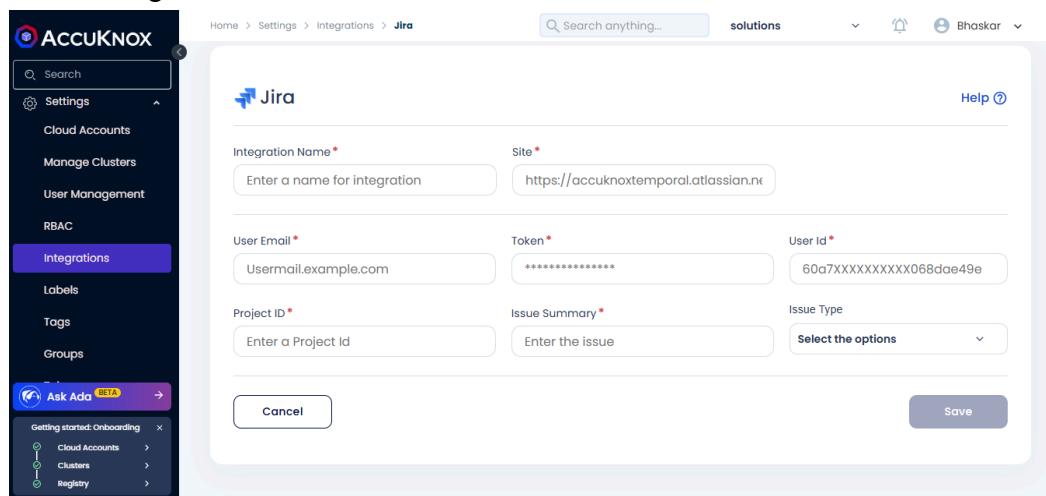
a. Prerequisites

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

b. JIRA integration for CWPP:

Steps to Integrate:

- Go to Settings -> Integration.
- Click “Integrate Now” under JIRA



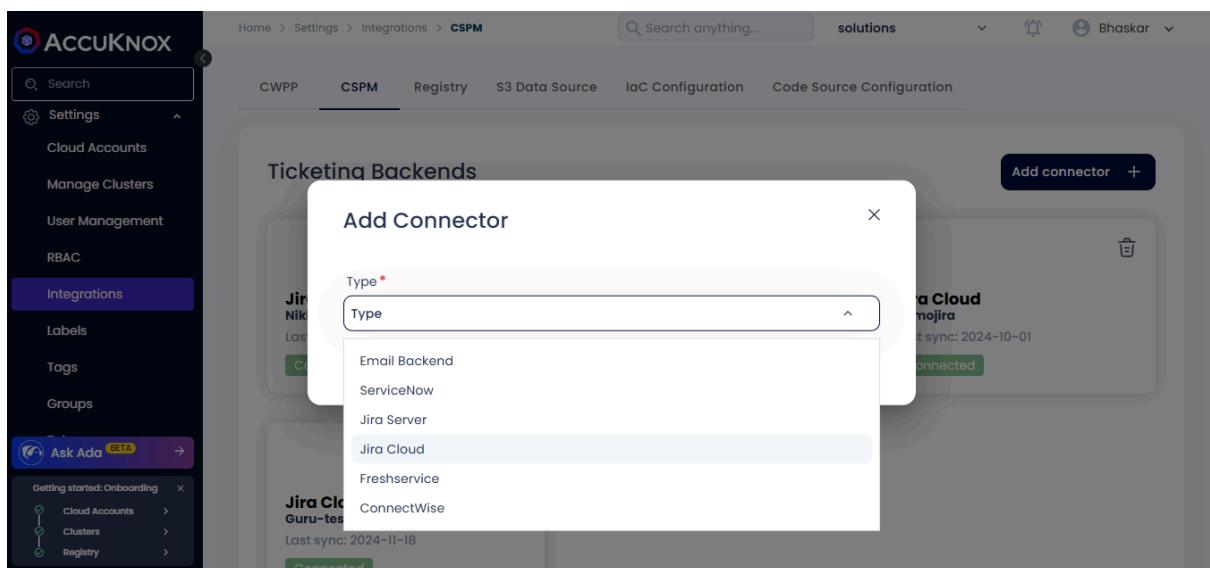
- Enter the following details to configure JIRA.
- Integration Name: Enter the name for the integration. You can set any name. e.g., Test JIRA
- Site: Enter the site name of your organization. e.g., <https://jiratest.atlassian.net/>
- User Email: Enter your Jira account email address here.e.g., jira@organisation.com

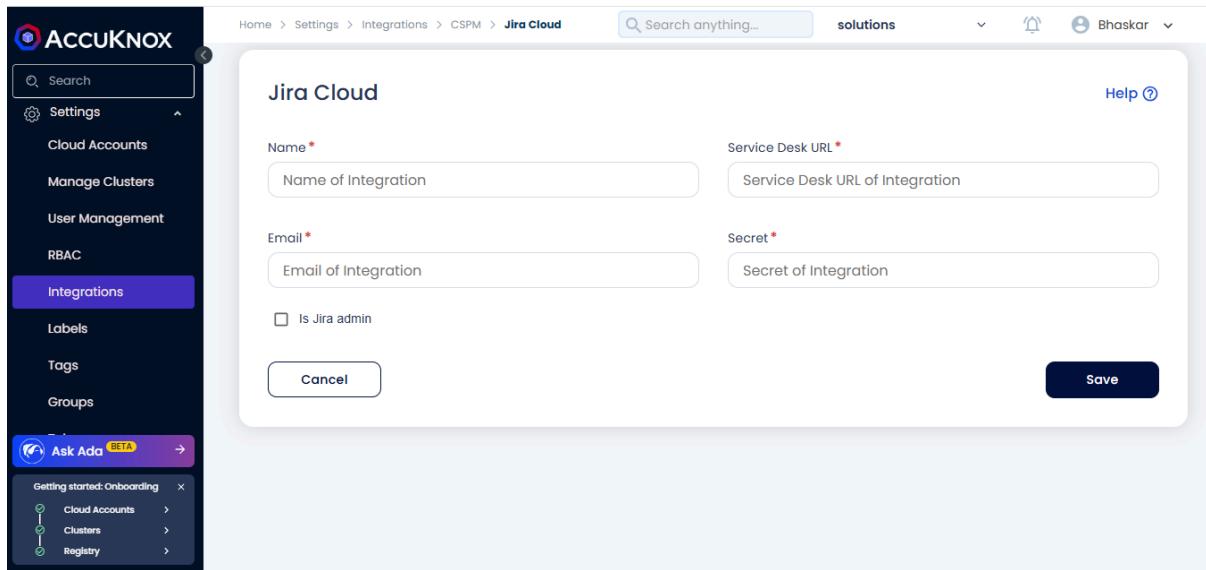
- Token: Enter the generated Token here from <https://id.atlassian.com/manage-profile/security/api-tokens>. e.g., kRVxxxxxxxxxxxxxx39
- User ID: Enter your Jira user ID here. You can visit the people section and search your name to see the User ID. For more details check here. e.g., 5bbxxxxxxxxx0103780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

17.3.2 JIRA integration for CSPM:

Steps to Integrate:

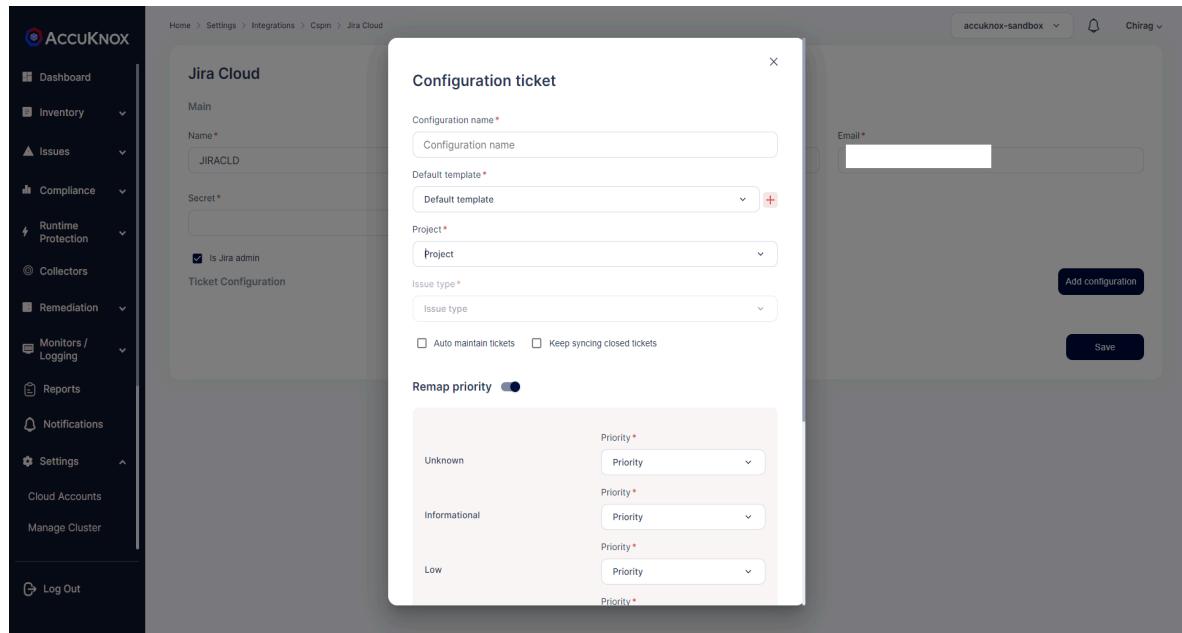
- Go to Channel Integration -> CSPM.
- Click on “Add connector” and select JIRA Cloud





Enter the following details to configure JIRA.

- **Integration Name:** Enter the name for the integration. You can set any name.
e.g., Test JIRA
- **Site:** Enter the site name of your organization. e.g.,
<https://jiratest.atlassian.net/>
- **User Email:** Enter your Jira account email address here.e.g.,
jira@organisation.com
- **Token:** Enter the generated Token here from
<https://id.atlassian.com/manage-profile/security/api-tokens>. .e.g.,
kRVxxxxxxxxxxxxxx39



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

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

You can now configure Alert Triggers for JIRA.

17.3.3 ServiceNow Integration

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

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

a. Prerequisites

- The ServiceNow Integration requires the following: Instance URL, Instance Username and Instance Password.
 - Please refer to the ServiceNow Documentation for how to create an instance and obtain the required credentials.

b. Steps for integration

- Navigate to Settings → Integrations → CSPM tab
- Click on Add Connector and select ServiceNow, click on Next.

17.3.4 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.

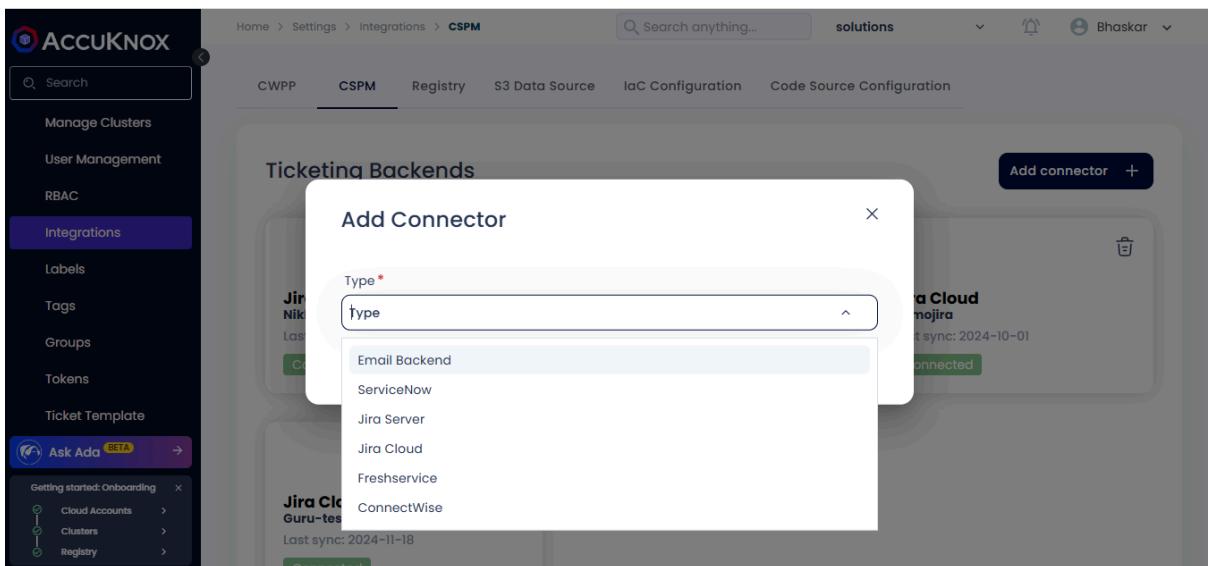
To set up this integration, you need to coordinate with your Freshservice administrator and gather the inputs needed to enable communication between AccuKnox and Freshservice.

a. Prerequisites

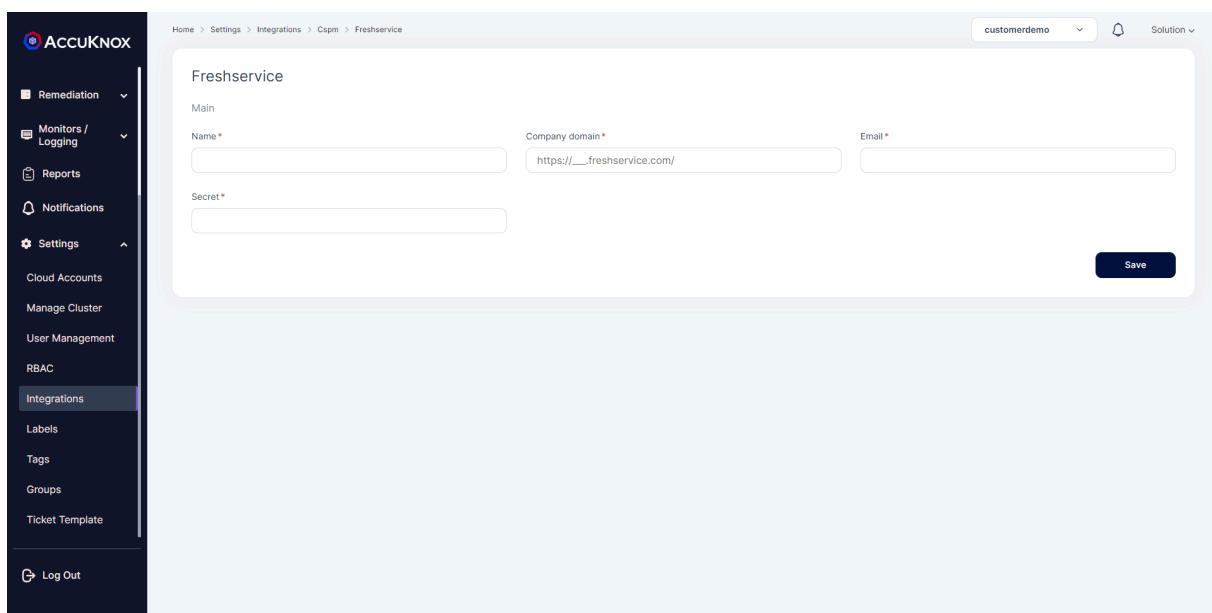
- You need a Company domain, Email & API key (secret) for this integration.
- You can find your API key in profile settings in the right side column.

b. Steps to Integrate:

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



The screenshot shows the AccuKNOX web interface. On the left, there's a sidebar with various navigation options like 'Manage Clusters', 'User Management', 'RBAC', and 'Integrations'. The 'Integrations' option is currently selected. In the main area, under 'Ticketing Backends', there's a list of connectors including Jira Cloud, Freshservice, and ConnectWise. A modal window titled 'Add Connector' is open, showing a dropdown menu for 'Type*' where 'Email Backend' is selected. Other options listed in the dropdown are ServiceNow, Jira Server, Jira Cloud, and Freshservice.

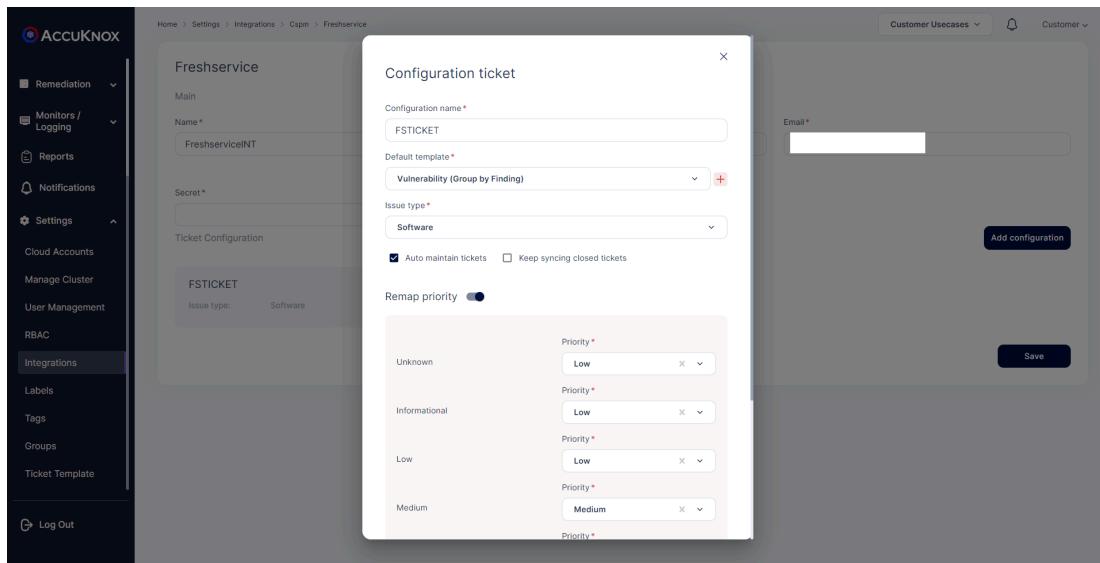


The screenshot shows the 'Freshservice' configuration page within the AccuKNOX interface. The left sidebar has 'Integrations' selected. The main form is titled 'Freshservice' and contains a 'Main' section with fields for 'Name*', 'Company domain*', 'Email*', and 'Secret*'. A 'Save' button is at the bottom right. The URL in the browser bar is 'Home > Settings > Integrations > Cspm > 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.

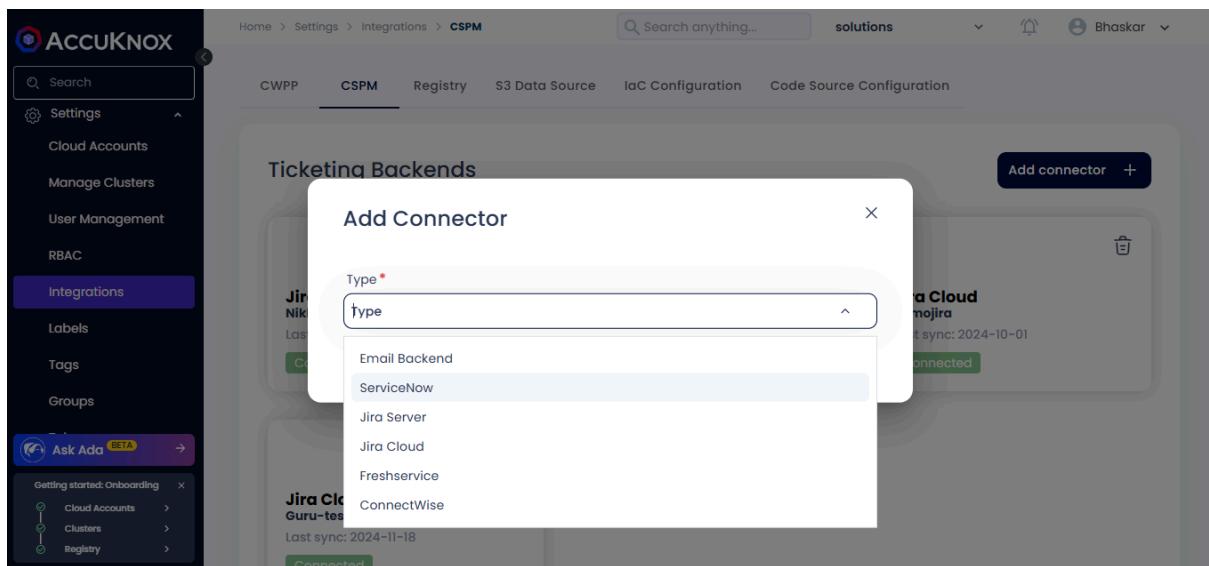


Click on the Freshservice ticketing backend to add configuration.

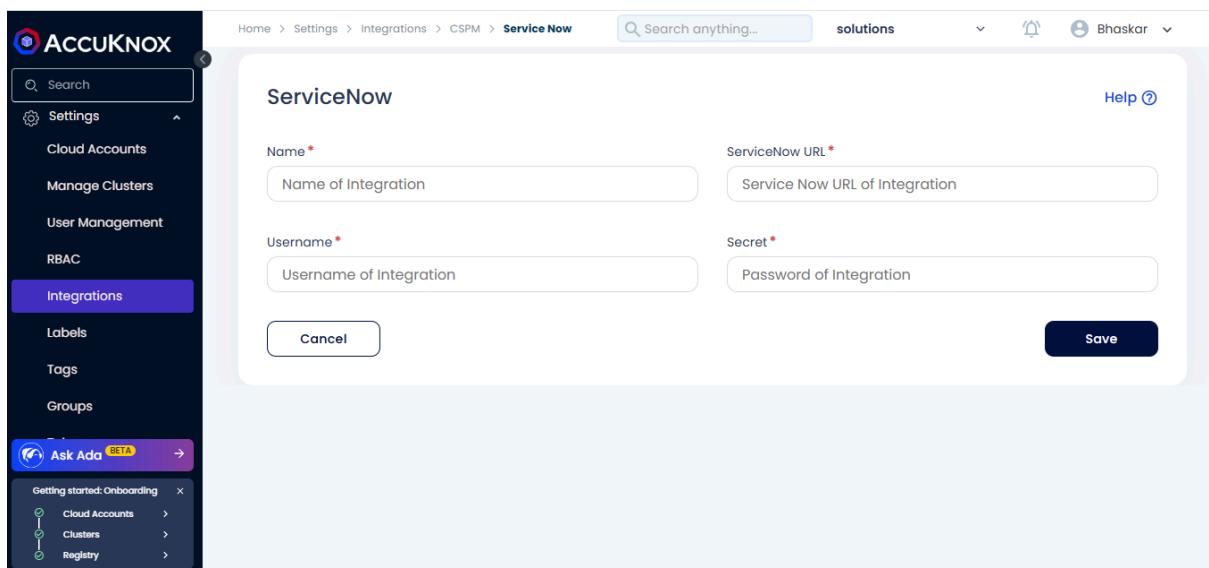
Here Enter the following details:

- 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.

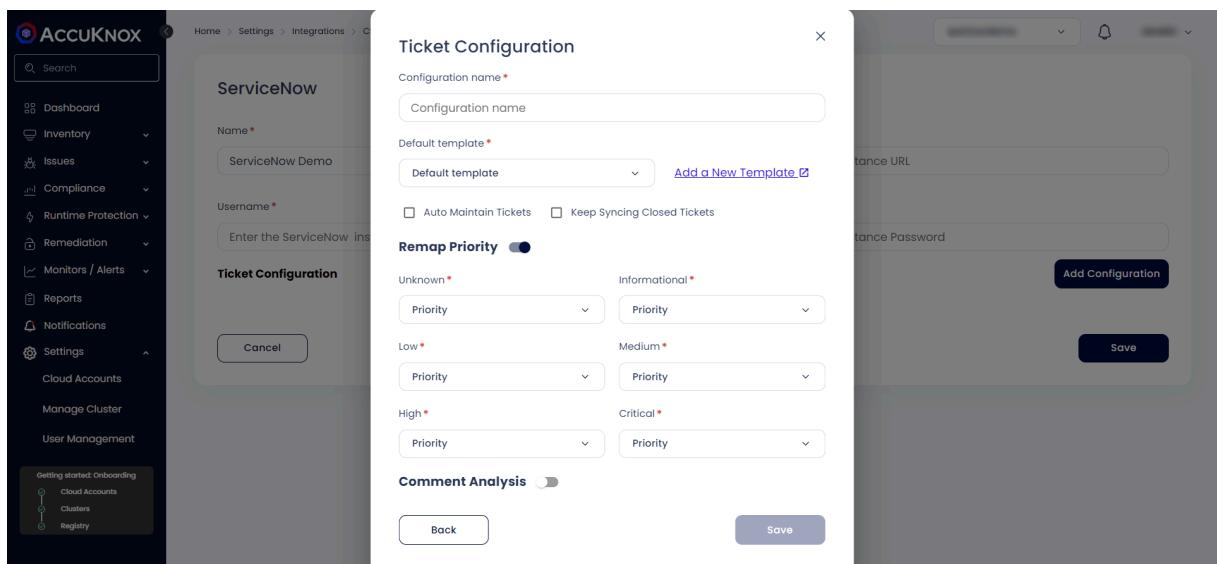


- Enter the following details to configure the ServiceNow Integration:
 - **Integration Name:** Enter the name for the integration. You can set any name. e.g., MyServiceNow
 - **ServiceNow Instance URL:** The URL of the ServiceNow instance. e.g., https://my-instance.service-now.com
 - **Instance Username:** The Username associated with the instance. e.g., admin
 - **Secret:** The current password of the instance.



- Click on the ServiceNow ticketing backend

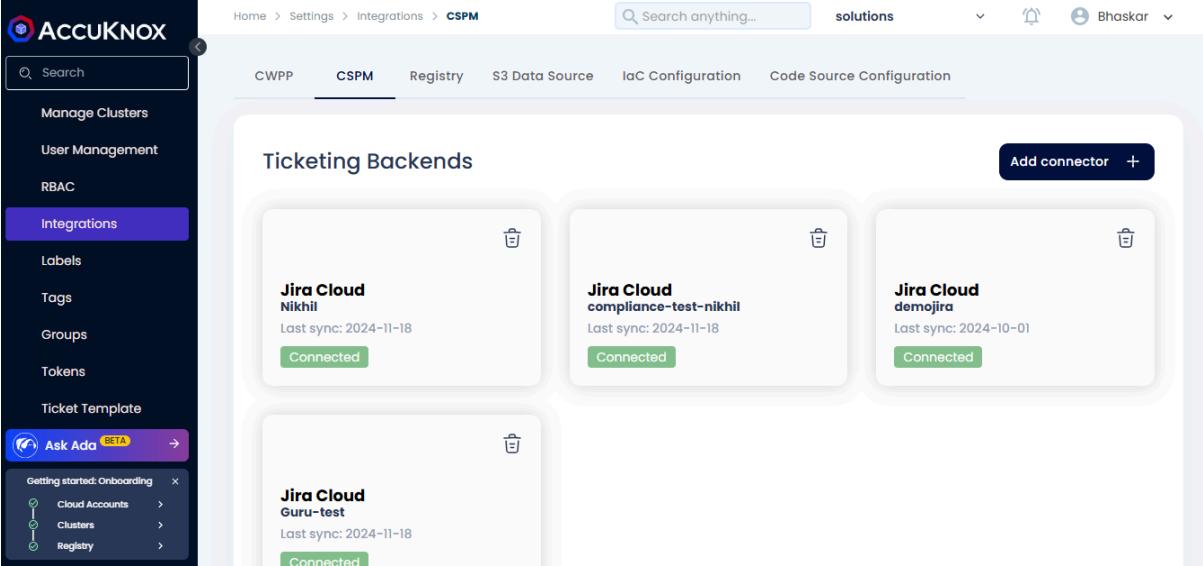
- Click on Add Configuration and enter the following details:
 - **Configuration name:** this name will be displayed under ticket configuration while creating tickets.
 - **Default template:** to specify the of data that this configuration will be used for making tickets.
 - **Issue Type:** You can choose from the dropdown.
 - Fill the priority mapping according to your choice and press **Save**.



You can now create tickets on ServiceNow through the ticketing configuration.

17.4 Creating Ticket Configuration

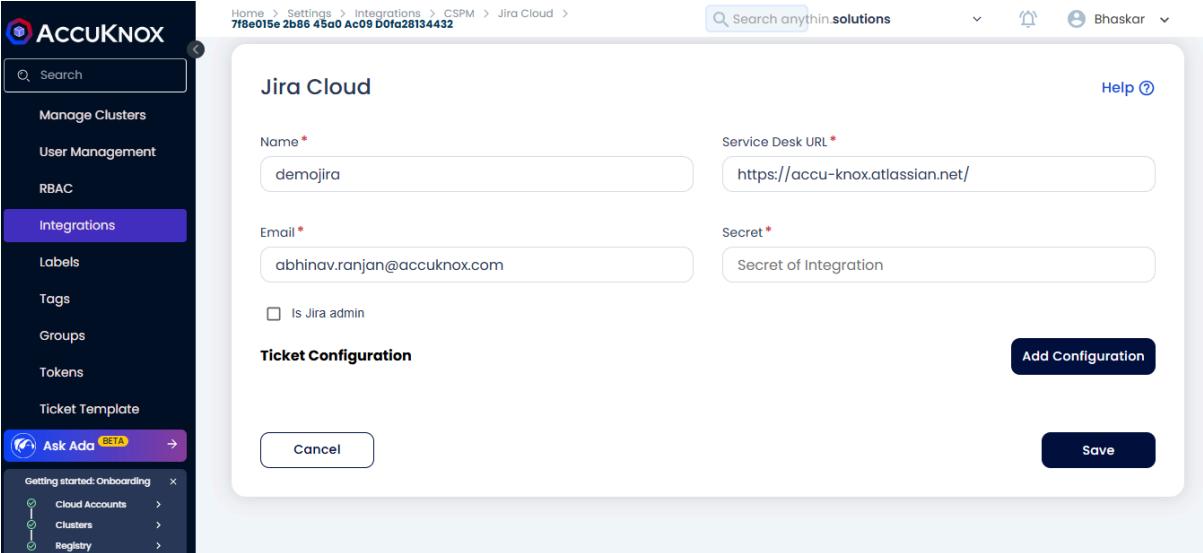
- To create a ticket configuration, navigate to Integrations under Settings and click on the CSPM tab. This will show all the ticketing backends that have been integrated:



The screenshot shows the AccuKnox interface with the navigation path: Home > Settings > Integrations > CSPM. The left sidebar has a dark theme with purple highlights for the 'Integrations' section. The main content area is titled 'Ticketing Backends' and lists four entries, each with a trash icon and a 'Connected' button:

- Jira Cloud Nikhil (Last sync: 2024-11-18)
- Jira Cloud compliance-test-nikhil (Last sync: 2024-11-18)
- Jira Cloud demojira (Last sync: 2024-10-01)
- Jira Cloud Guru-test (Last sync: 2024-11-18)

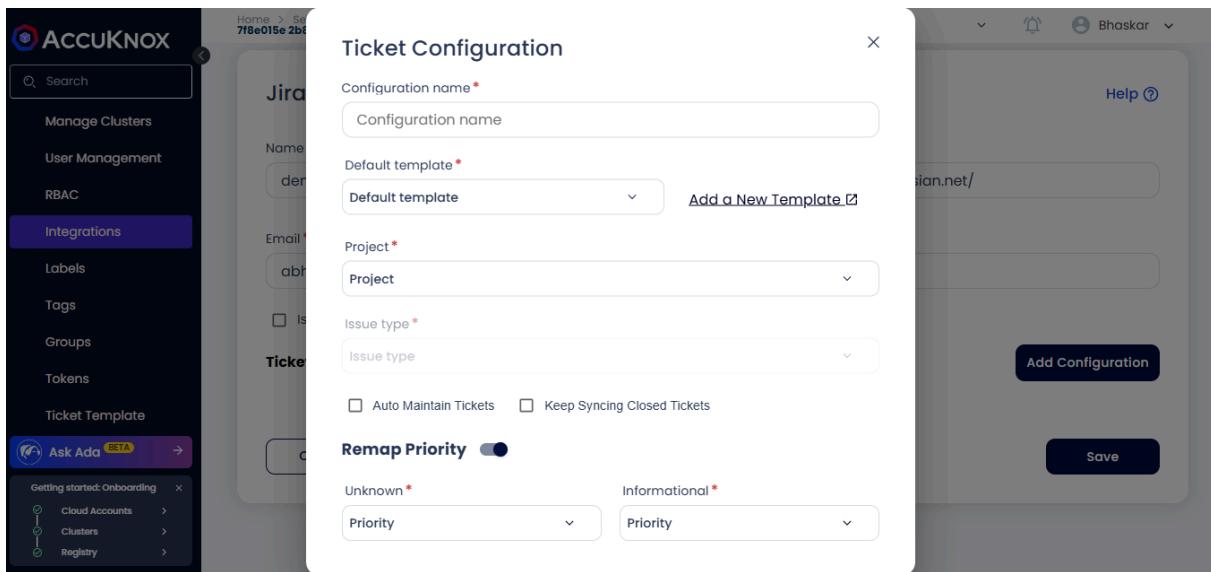
- Click on one of the integrated Ticketing backends and click on Add Configuration button in the subsequent screen:



The screenshot shows the 'Jira Cloud' configuration screen. The path in the top bar is Home > Settings > Integrations > CSPM > Jira Cloud > 7f0e015e 2b86 45a0 Ac09 D0fa28134432. The left sidebar shows the 'Integrations' section. The main form has fields for Name (demojira), Service Desk URL (https://accu-knox.atlassian.net/), Email (abhinav.ranjan@accuknox.com), and Secret (Secret of Integration). There is a checkbox for 'Is Jira admin'. At the bottom are 'Cancel', 'Save', and 'Add Configuration' buttons.

- 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.

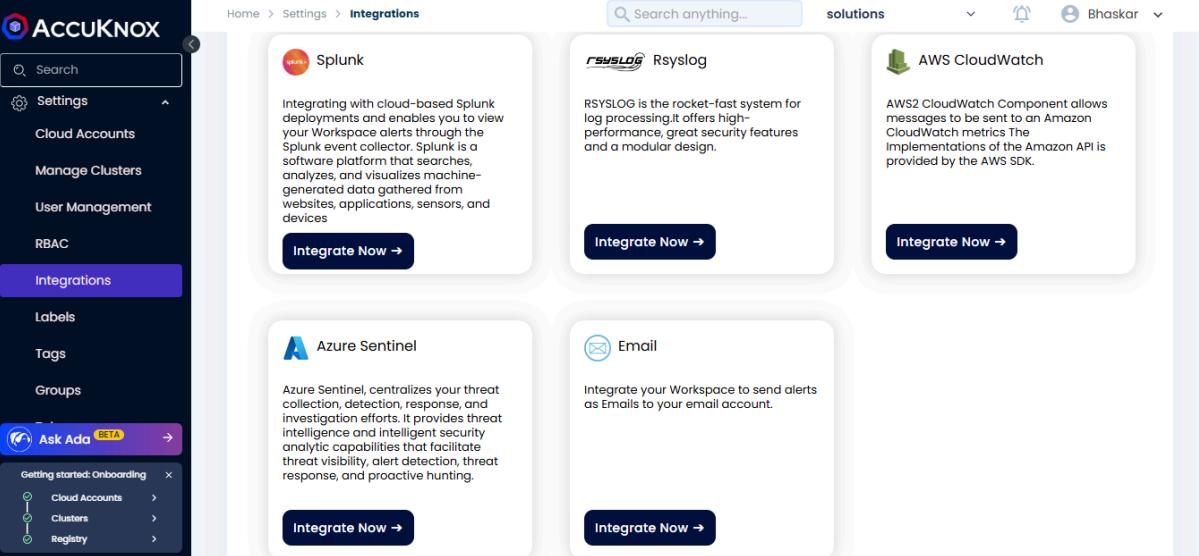


- Enter the relevant data in the remaining fields and click on Save. The ticket configuration is created successfully

17.5 Email Integration

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

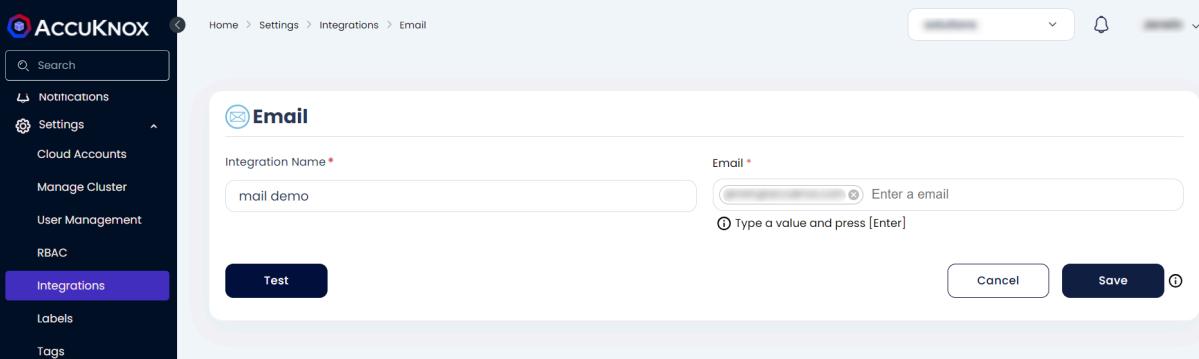
- Navigate to Settings → Integrations → CWPP tab
- Click on the **Integrate Now** button under Email.



The screenshot shows the AccuKnox Settings page with the Integrations tab selected. On the right, there are five integration cards:

- Splunk**: Integrating with cloud-based Splunk deployments and enables you to view your Workspace alerts through the Splunk event collector. Splunk is a software platform that searches, analyzes, and visualizes machine-generated data gathered from websites, applications, sensors, and devices. **Integrate Now →**
- Rsyslog**: RSYSLOG is the rocket-fast system for log processing. It offers high-performance, great security features and a modular design. **Integrate Now →**
- AWS CloudWatch**: AWS CloudWatch Component allows messages to be sent to an Amazon CloudWatch metrics. The implementations of the Amazon API is provided by the AWS SDK. **Integrate Now →**
- Azure Sentinel**: Azure Sentinel centralizes your threat collection, detection, response, and investigation efforts. It provides threat intelligence and intelligent security analytic capabilities that facilitate threat visibility, alert detection, threat response, and proactive hunting. **Integrate Now →**
- Email**: Integrate your Workspace to send alerts as Emails to your email account. **Integrate Now →**

- Fill the following fields:
 - **Integration Name**: Enter the name for the integration. You can set any name. e.g., Container Security Alerts
 - **Email**: Enter the Email that will receive the notification and press ENTER. You can specify multiple email addresses in this field by pressing ENTER after each email address.
e.g., demo@organization.com



The screenshot shows the AccuKnox Integrations > Email configuration page. The left sidebar shows the navigation path: Home > Settings > Integrations > Email. The main form is titled "Email" and contains the following fields:

- Integration Name ***: mail demo
- Email ***: (Type a value and press [Enter])

At the bottom are two buttons: **Test** and **Save**.

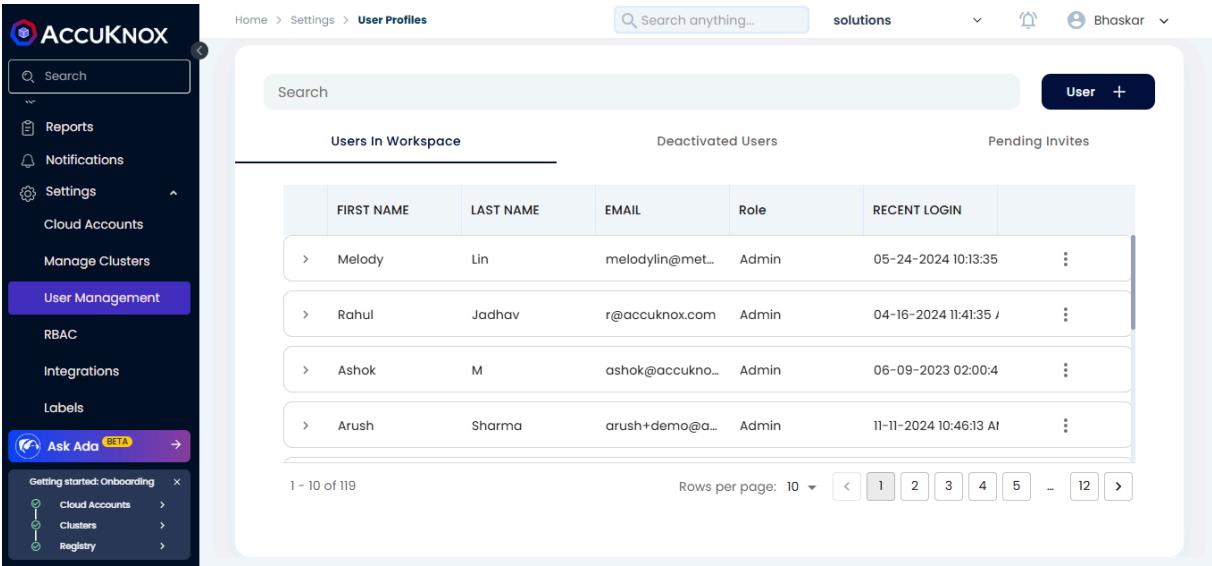
- Click **Test** to check the new functionality, You will receive a test mail on the specified mail addresses with subject "Test email"
- Click **Save** to save the Integration. You can now configure Alert Triggers for Email Notifications.

18. 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.

18.1 Inviting a New User

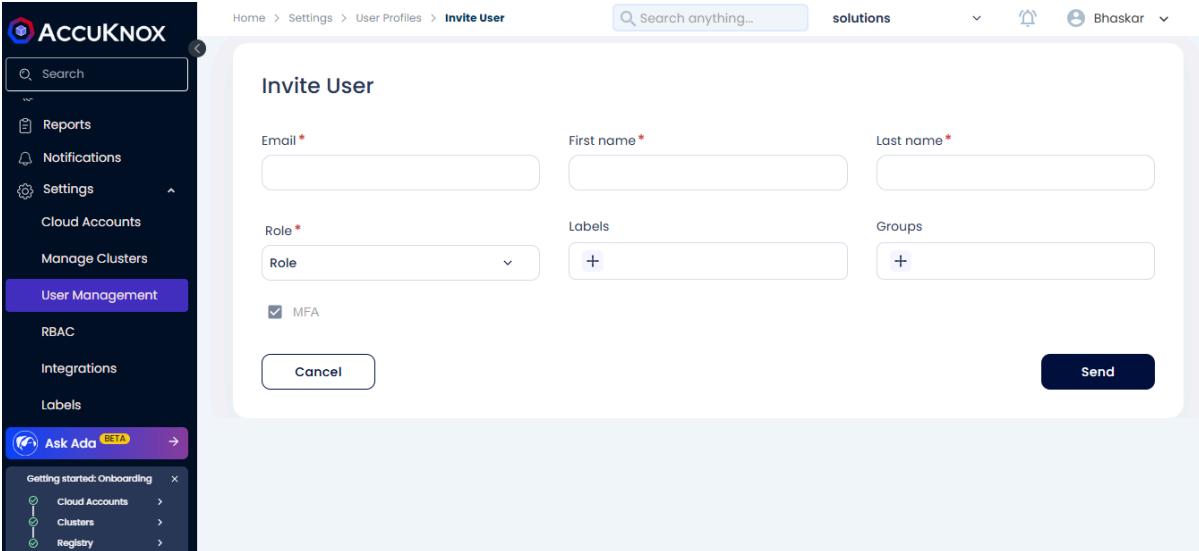
Log in to your AccuKnox dashboard. Navigate to "User Management" in the left sidebar menu. Click the "User +" button in the top right corner of the Users page.



The screenshot shows the AccuKnox dashboard with the "User Management" section selected in the sidebar. The main page displays a list of users in the workspace, with columns for FIRST NAME, LAST NAME, EMAIL, Role, and RECENT LOGIN. The list includes four users: Melody, Rahul, Ashok, and Arush. At the bottom of the list, it shows "1 - 10 of 119" and a "Rows per page: 10" dropdown with page navigation buttons from 1 to 12.

	FIRST NAME	LAST NAME	EMAIL	Role	RECENT LOGIN	
>	Melody	Lin	melodylin@met...	Admin	05-24-2024 10:13:35	⋮
>	Rahul	Jadhav	r@accuknox.com	Admin	04-16-2024 11:41:35 /	⋮
>	Ashok	M	ashok@accukno...	Admin	06-09-2023 02:00:4	⋮
>	Arush	Sharma	arush+demo@a...	Admin	11-11-2024 10:46:13 AI	⋮

In the "Invite User" form, fill out the following details and hit Send.



Invite User

Email*

First name*

Last name*

Role*

Labels

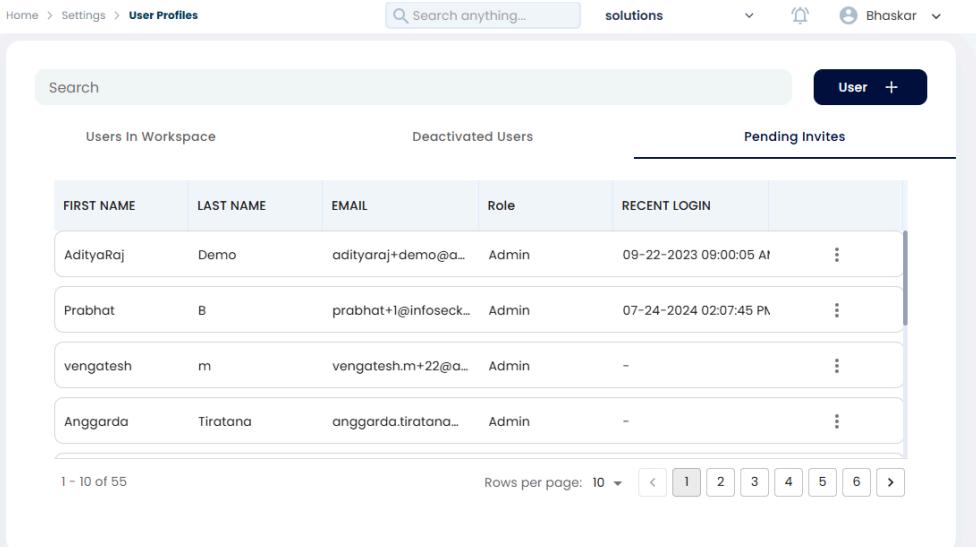
Groups

MFA

Cancel **Send**

Note

You can view pending invitations in the "Pending Invites" tab on the Users page. You can resend or revoke invitations from this tab. Viewing all permissions of a user is possible via the main tab.



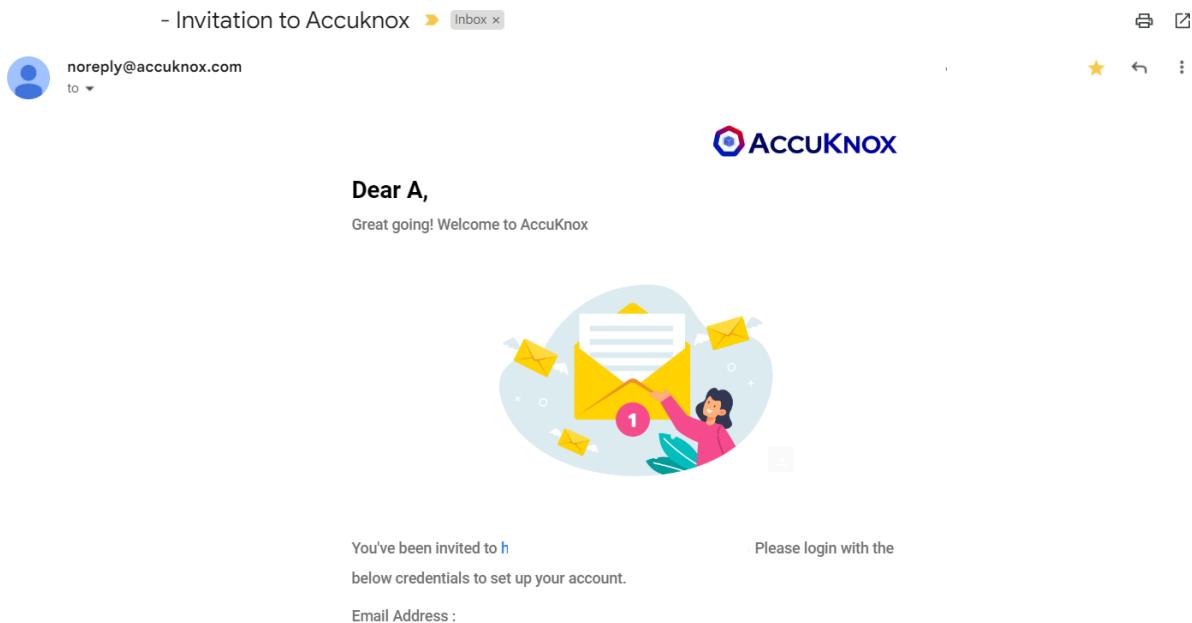
FIRST NAME	LAST NAME	EMAIL	ROLE	RECENT LOGIN
AdityaRaj	Demo	adityaraj+demo@...	Admin	09-22-2023 09:00:05 AM
Prabhat	B	prabhat+l@infoseck...	Admin	07-24-2024 02:07:45 PM
vengatesh	m	vengatesh.m+22@...	Admin	-
Anggarda	Tiratana	anggarda.tiratana...	Admin	-

1 – 10 of 55

Rows per page: 10 < 1 2 3 4 5 6 >

18.2 User Receives Invitation

The invited user will receive a link on their mail to accept the invitation and set up their account if they haven't already done so.



18.3 User Login Options

Users can log in to AccuKnox using two methods:

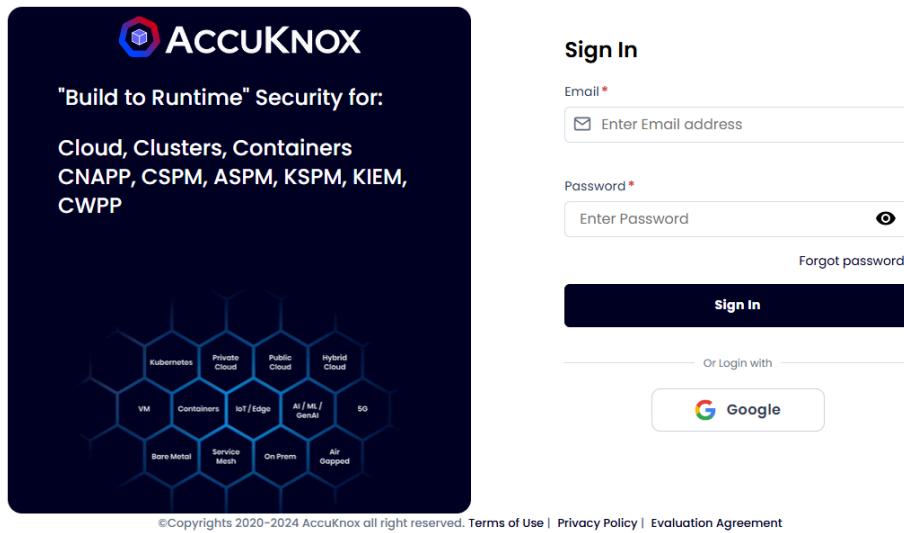
Option A: Traditional Login

1. Go to the AccuKnox login page.
2. Enter the email address and password.
3. Click "Sign In".

Note

This requires you to use the MFA (multi-factor authentication) code if it was enabled during the invitation process. MFA is required for every sign-in attempt.

Option B: Single Sign-On (SSO) with Google



1. Go to the AccuKnox login page.
2. Look for "Or login with" at the bottom of the form.
3. Click on the "Google" button.
4. If not already signed in to Google, enter Google account credentials.
5. Grant any necessary permissions for AccuKnox.

Note

If you are already signed in to Google, you will be automatically logged in to AccuKnox. No need for MFA in this case.

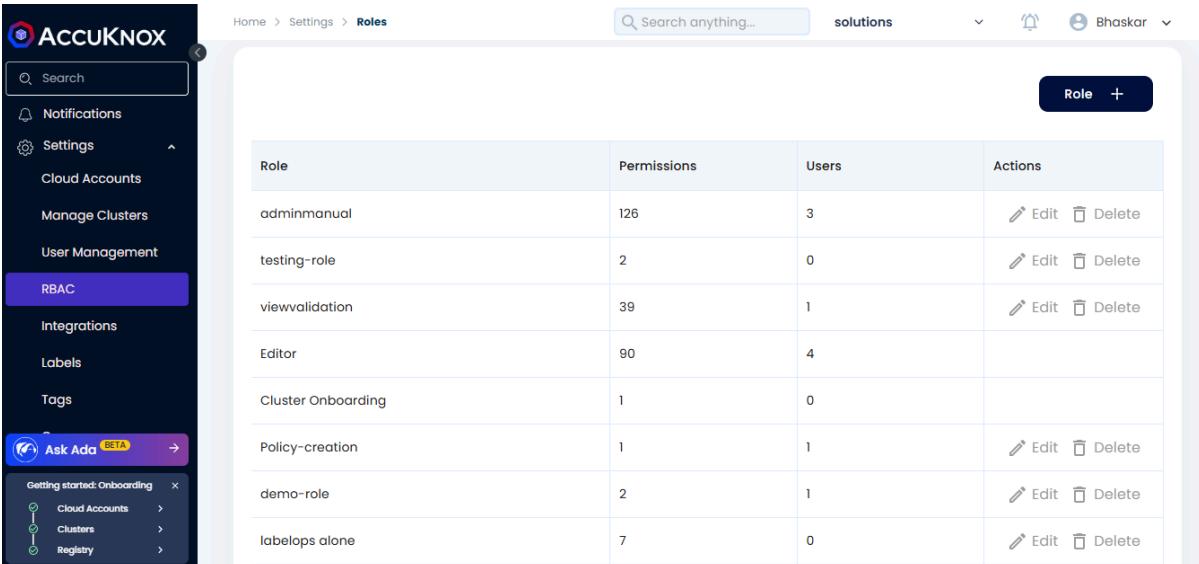
3. Notes

- SSO is currently only supported for Google accounts.
- Users must be invited with their Gmail address to use Google SSO.
- For the best experience, use the same email address for invitation and login.
- If you encounter any issues, contact your AccuKnox administrator or support team.

- Emails with + modifiers (e.g., test+stable@gmail.com or example+solutions@gmail.com) are not supported for SSO. Please use a base email address.

18.4 Assign RBAC

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

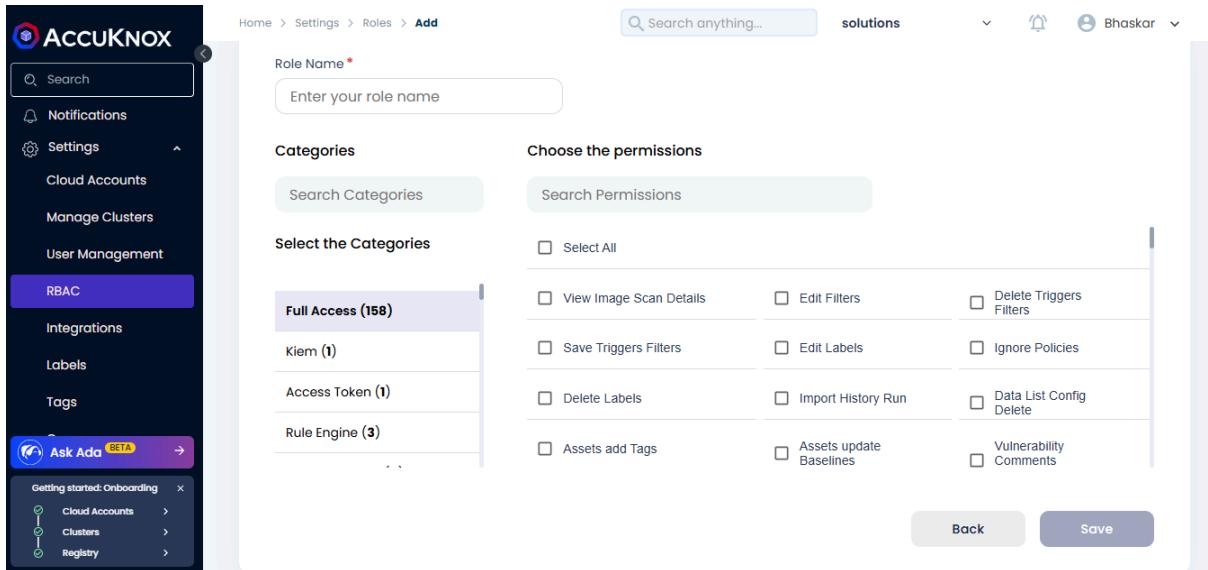


Role	Permissions	Users	Actions
adminmanual	126	3	Edit Delete
testing-role	2	0	Edit Delete
viewvalidation	39	1	Edit Delete
Editor	90	4	
Cluster Onboarding	1	0	
Policy-creation	1	1	Edit Delete
demo-role	2	1	Edit Delete
labelops alone	7	0	Edit Delete

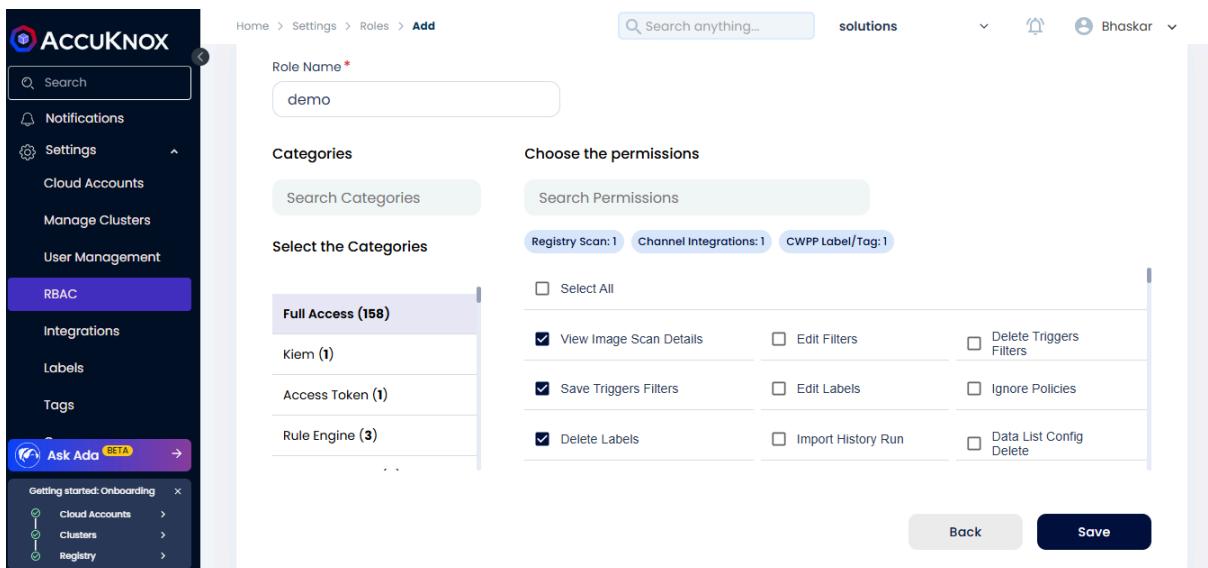
18.5 Create Roles and Assign Users

Steps:

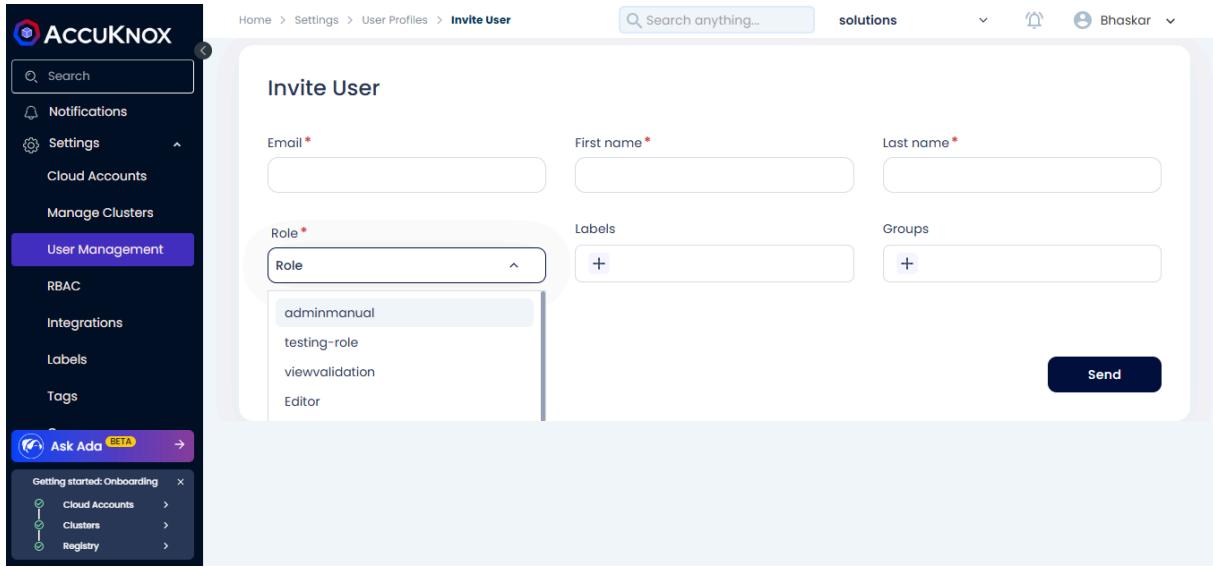
- Click on Add Role



- 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 to the new user with custom role and permission



The screenshot shows the ACCUKNOK User Management interface, specifically the 'Invite User' page. The left sidebar has a dark theme with purple highlights for 'User Management'. The main form is titled 'Invite User' and includes fields for Email*, First name*, Last name*, Role*, Labels, and Groups. A dropdown menu for 'Role' lists 'adminmanual' (selected), 'testing-role', 'viewvalidation', and 'Editor'. A 'Send' button is at the bottom right. The top navigation bar shows 'Home > Settings > User Profiles > Invite User'. The top right corner shows 'solutions' and a user profile for 'Bhaskar'.

Invite User

Email *

First name *

Last name *

Role *

Labels

Groups

Role

- adminmanual
- testing-role
- viewvalidation
- Editor

Send

19. Ticketing Procedures

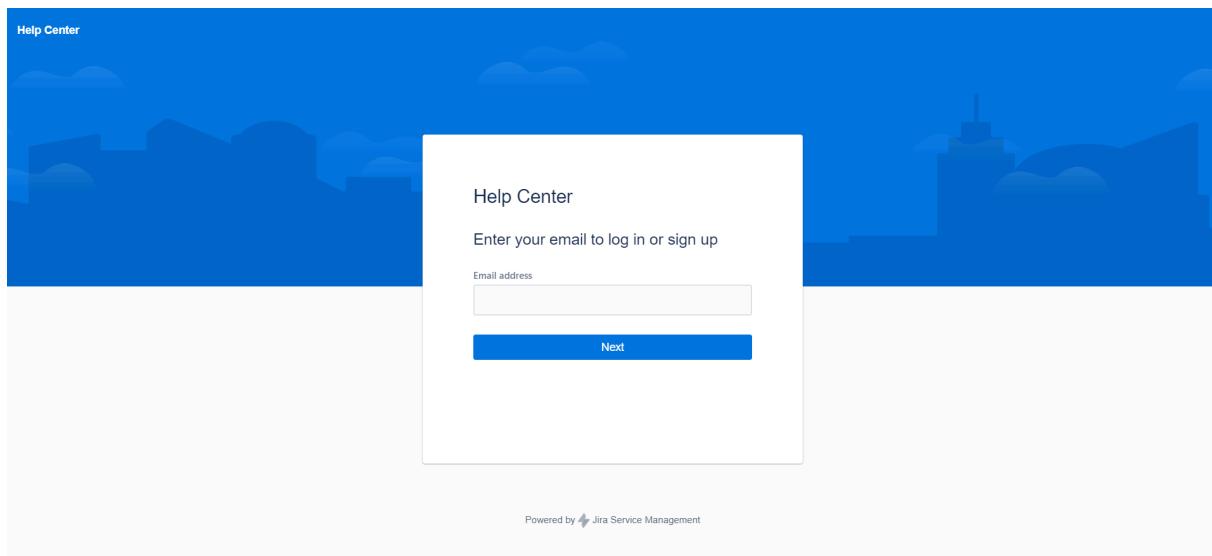
By following these steps, you can quickly and effectively raise a Jira ITSM support ticket for major platform issues, ensuring that your problem is addressed promptly and efficiently.

19.1 How to raise an AccuKnox support ticket?

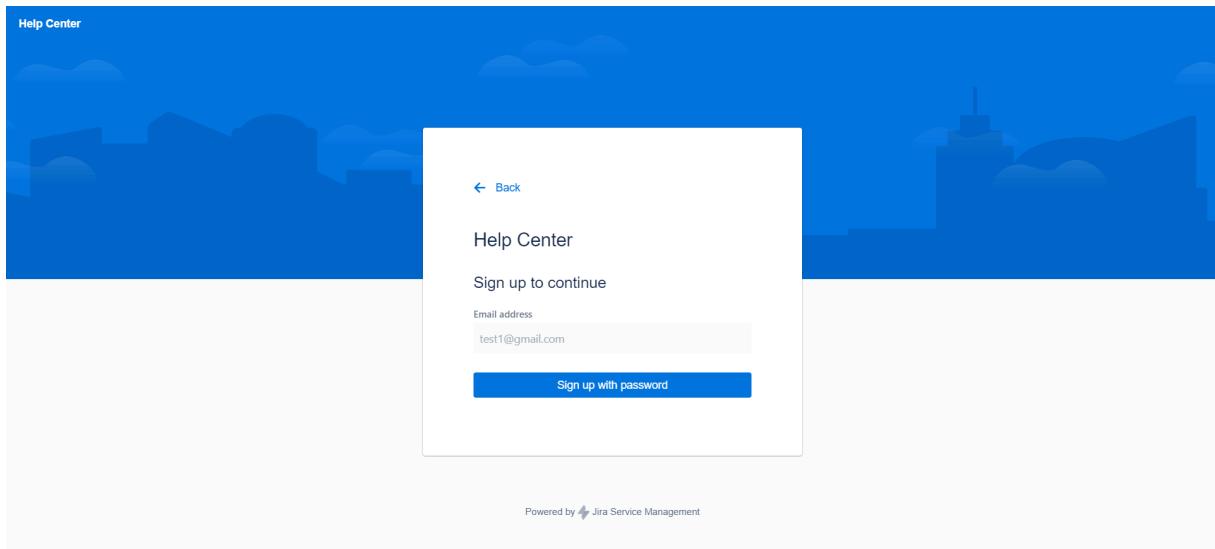
Step 1: Please click the following URL for raising the ticket:

<https://accu-knox.atlassian.net/servicedesk/customer/portal/1>

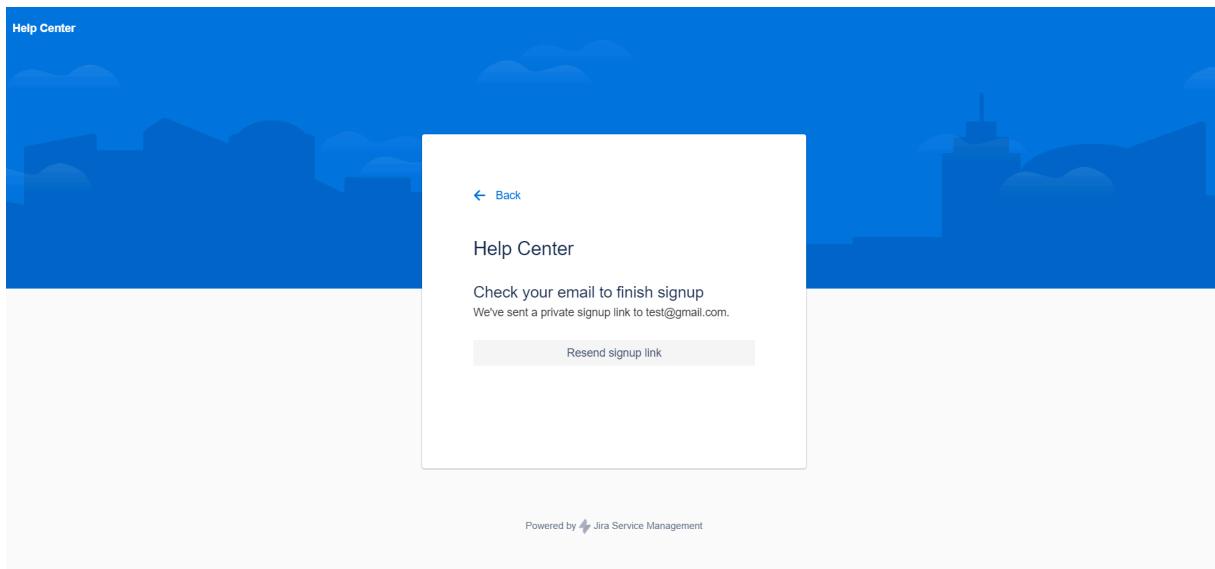
Step 2: The page will ask for you to input the mail ID for signup



Step 3: After giving the email ID and selecting next will ask the user to sign in with a password

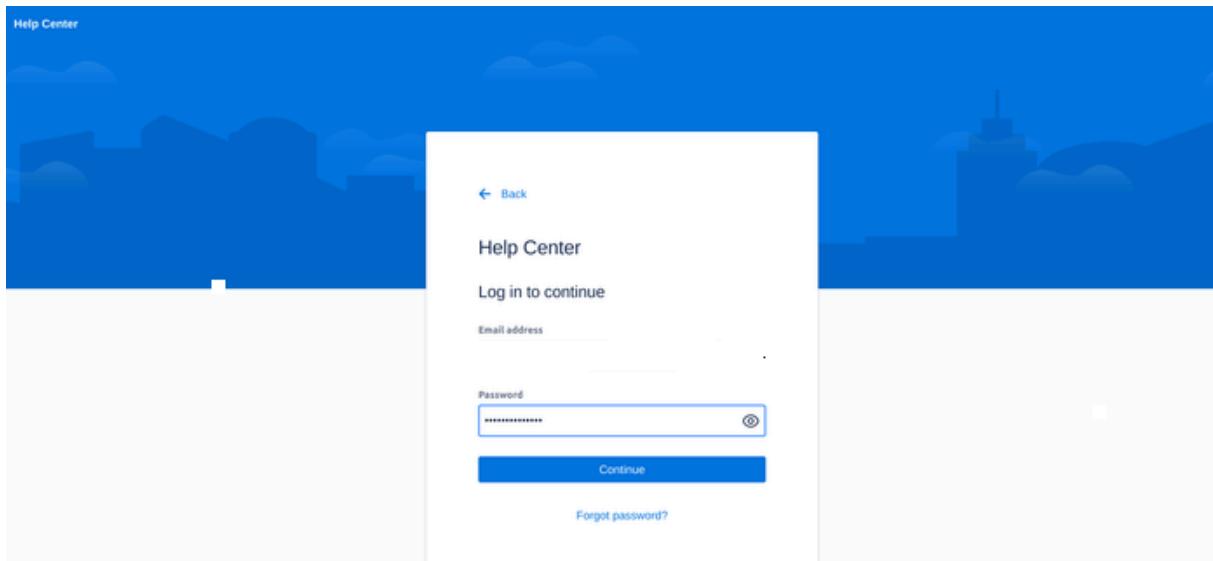


Step 4: Once users click the sign up with password, they will get an email for setting the password to the registered email id.

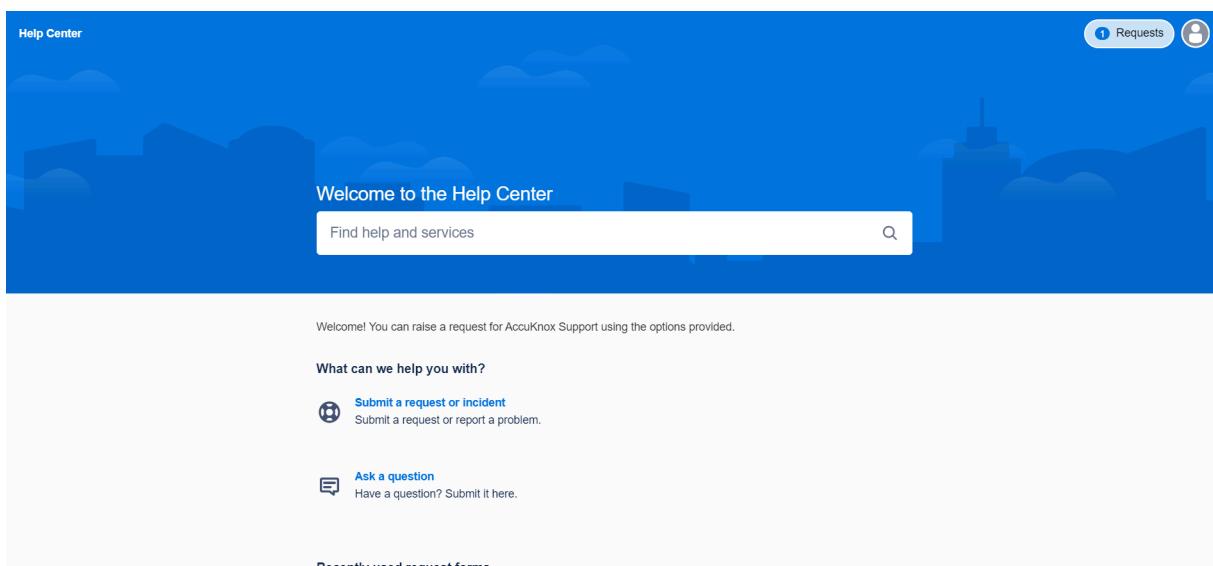


Step 5: After clicking the link and setting up the password and username login into the customer portal again

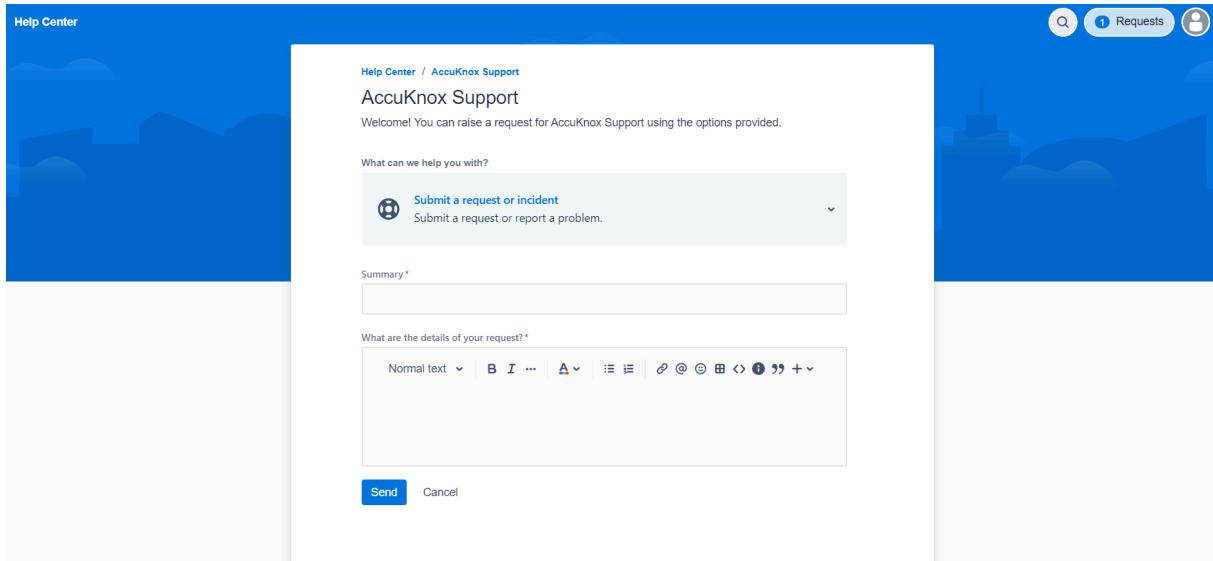
<https://accu-knox.atlassian.net/servicedesk/customer/portal/1>



Step 6: Click on the Submit a request or incident option to create the issue



Step 7: To create an issue fill out this form and click send. Once it is clicked, the issue is created, and you will get a confirmation email to your registered email ID.

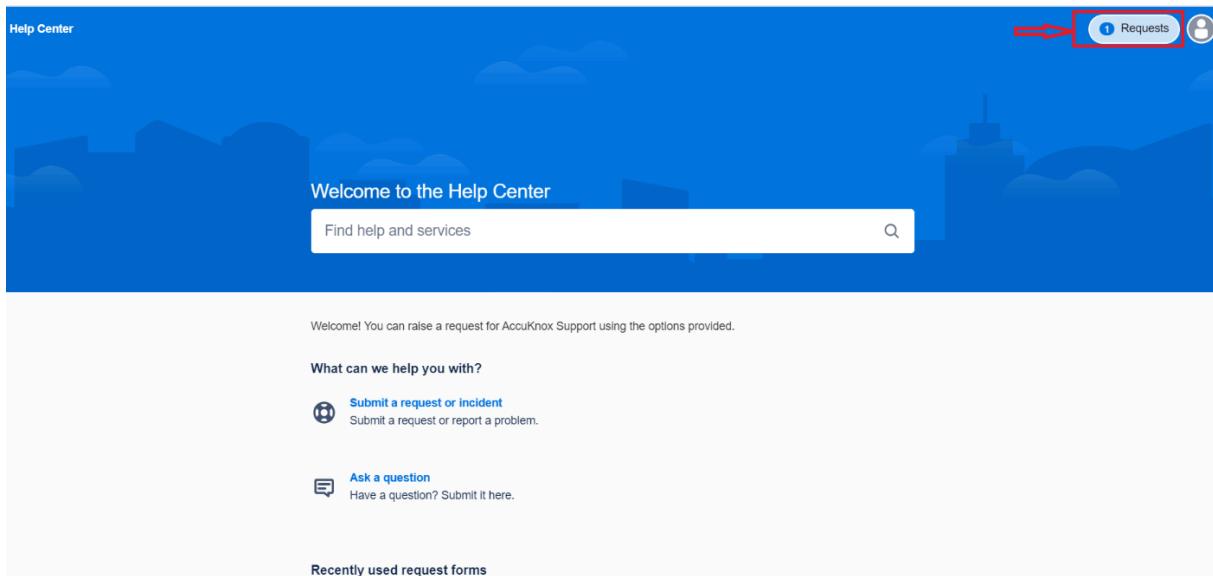


The screenshot shows the 'AccuKnox Support' page within the 'Help Center'. At the top, there's a navigation bar with a search icon, a 'Requests' button (which is highlighted with a red box and an arrow), and a user profile icon. Below the navigation, the page title is 'AccuKnox Support' and a sub-page title is 'Help Center / AccuKnox Support'. A welcome message says, 'Welcome! You can raise a request for AccuKnox Support using the options provided.' There's a dropdown menu titled 'What can we help you with?' containing 'Submit a request or incident' (which is also highlighted with a red box and an arrow) and 'Ask a question'. Below this is a 'Summary' field with a placeholder 'Type your message here...' and a rich text editor toolbar. At the bottom of the form are 'Send' and 'Cancel' buttons.

19.2 How to track the issue resolution status?

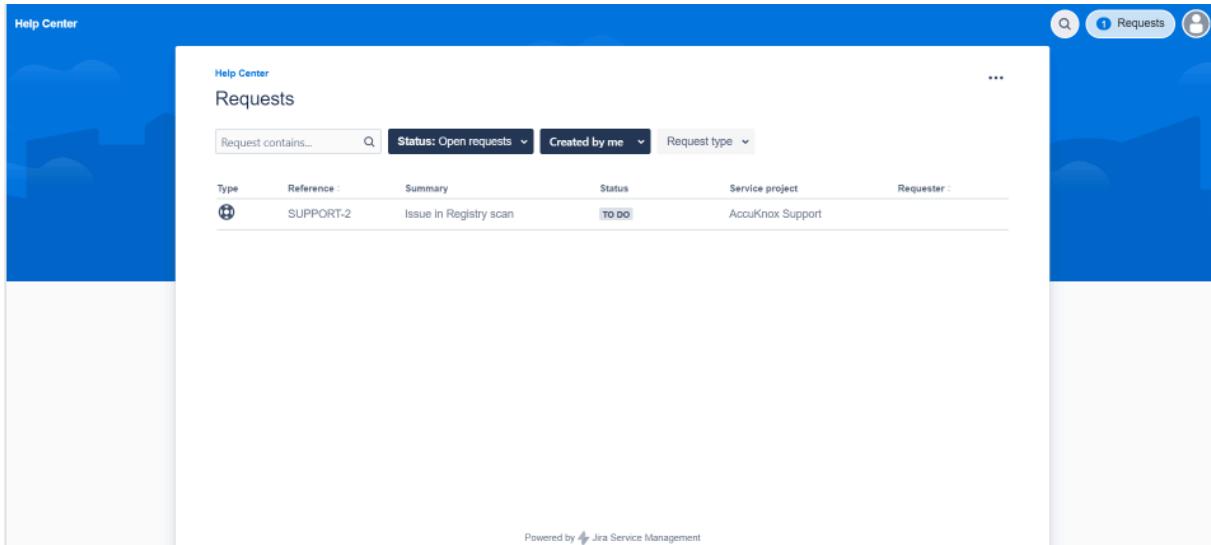
To track the issue raised by the user they can log into the customer service portal using the link <https://accu-knox.atlassian.net/servicedesk/customer/portal/1>

Step 1: Click on the requests section in the top left corner of the screen



The screenshot shows the 'Help Center' homepage. At the top right, there's a red box with an arrow pointing to the 'Requests' button in the top navigation bar. The main content area has a blue background with a city skyline illustration. It features a 'Welcome to the Help Center' message, a search bar with a magnifying glass icon, and a 'Find help and services' input field. Below this is a message: 'Welcome! You can raise a request for AccuKnox Support using the options provided.' There are two main sections: 'What can we help you with?' which includes 'Submit a request or incident' (highlighted with a red box and an arrow) and 'Ask a question', and 'Recently used request forms'.

Step 2: Here you will find the list of issues created by the user and their status



The screenshot shows the 'Help Center' interface with a 'Requests' section. At the top, there are search and filter options: 'Request contains...' with a magnifying glass icon, 'Status: Open requests' (selected), 'Created by me', and 'Request type'. Below these are three buttons: '...', '...', and '...'. The main area displays a table with one row of data:

Type	Reference	Summary	Status	Service project	Requester
	SUPPORT-2	Issue in Registry scan	TO DO	AccuKnox Support	

At the bottom of the page, it says 'Powered by Jira Service Management'.

20. FAQs

20.1 AccuKnox FAQs

1. Does AccuKnox CNAPP support only agent-based scanning or does it support agentless scanning ?

For CSPM, AccuKnox supports agentless scanning for Public Cloud Infrastructure. For Infrastructure behind a firewall or Private Cloud, AccuKnoxCSPM leverages open source based agent to manage remote nodes for Automated reporting, Error log Delivery, Microservice Monitoring, User Shell Activity, Resource Monitoring.

For CWPP, AccuKnox leverage open source CNCF sandbox project KubeArmor for scanning and in-line mitigation from known attacks. Together we provide a complete static and runtime security for a variety of workloads whether they are on Public/Private Cloud, VM, Baremetal or pure-containerized workload. Thus we require agents to be installed to support scanning the workloads.

2. What is the differentiation of AccuKnox in Static Security?

In the Static Security solution, unlike other CSPM tools, AccuKnox provides flexibility to integrate a variety of open source and commercial security scanning tools through built-in parsers to provide you a composite security posture of your infrastructure. We also correlate and normalize results from a variety of security scanning tools and provide detailed results of vulnerabilities across infrastructure.

3. How does AccuKnox help to achieve static security?

AccuKnox Cloud Security Posture Management (CSPM) tool scans the Cloud Account to assess Vulnerabilities, Misconfigurations that are present in the cloud infrastructure based on security best practices & benchmarks. AccuKnox also enables you to handle Vulnerabilities with the ability to mark false positives, Waiting for 3rd party or Accepted risk and many more, so that you get to act on findings that are remediable and containing the SLA. We also give comprehensive compliance reports based on various security governance for third party assessment operators (3PAO) auditing.

4. How does AccuKnox help to achieve Runtime security?

AccuKnox's Cloud Workload Protection Platform (CWPP) achieves runtime security by leveraging CNCF sandbox project, KubeArmor, which is a cloud-native runtime security enforcement system by AccuKnox that restricts and have more granular control over the application behavior such as process execution, file access, and networking operation of containers and nodes at the system level.

5. What is the differentiation of AccuKnox in Runtime Security?

AccuKnox leverages KubeArmor, which is a cloud-native runtime security enforcement system that leverages Linux Security Modules to secure the workloads. LSMs are really powerful but they weren't built with modern workloads including Containers and Orchestrators in mind. Hence, eBPF has provided us with the ability to extend capabilities and BPF LSM provide us with the ability to load our custom programs with

decision-making into the kernel seamlessly helping us protect modern workloads. Therefore, KubeArmor helps to enforce security posture wherein any malicious attacks will be stopped before execution, known as in-line mitigation (mentioned by Forrester report)

6. What does KubeArmor leverage for enforcement and what are its advantages?

KubeArmor leverages best of breed Linux Security Modules (LSMs) such as AppArmor, BPF-LSM, and SELinux for inline mitigation to reduce the attack surface of the pod/container/VM. LSMs have several advantages over any other techniques. By using LSMs, KubeArmor does not have to disturb pods/containers and also doesn't require change at host or CRI level to apply security policies.

KubeArmor deploys as a non-privileged daemonset with certain capabilities that allows it to monitor other pods/containers and host. A given cluster can have multiple nodes utilizing different LSMs so KubeArmor abstracts away the complexities of the LSMs and provides an easy way for policy enforcement.

7. What are the integration tools and registries that are supported by AccuKnox?

AccuKnox can integrate multiple Cloud Account, Registries, SIEM platform, Ticketing or Notifications Tools and the list is ever growing. AccuKnox is pretty flexible to support the progression of the list with the customer's request as our roadmap item. Some of the supported today are as follows:

- Security Events/SIEM : Splunk, Rsyslog, AWS CloudWatch, Elastic Search, Webhooks, Azure Sentinel
- Notification Tools: Slack, Jira, PagerDuty, Emails
- Ticketing Tools: Jira, FreshService, Connectwise, Zendesk
- Registries: Nexus, ECR, GCR, DockerHub, ACR, Harbor

8. How AccuKnox helps in Policy Version Control for Runtime Security?

AccuKnox enables DevSecOps teams to embed security policies as code into their GitOps workflow. This provides a unified, collaborative view of the policies and enables them to be shipped and deployed along with the applications they are protecting. Hence, utilizing Gitops based policy version control, it will be easy to enforce changes to policies and keep track of versions in case of audit or rollback requirement alongwith approval mechanisms.

9. How AccuKnox helps to achieve Microsegmentation?

AccuKnox CWPP provides micro-segmentation at the lowest possible granularity level which is also a smallest execution unit in Kubernetes i.e. Pods. We will help you to identify process execution request from the pods, network connections the pods are trying to make internally or externally and files-system the pods are accessing. By observing the behavior of a particular pod and restricting that behavior so that it functions according to the expected flow of process/events/traffic, one can develop a least permissive security posture from creating a whitelisting policies and auditing/denying everything else.

10. How AccuKnox helps to recommend Auto-Discovered Policies?

AccuKnox CWPP solution provide Discovery Engine agent that assesses the security posture of your workloads and auto-discovers the policy-set required to put the workload in least-permissive mode. We also provide Shared Informer Agent which collects information about cluster like pods, nodes, namespaces etc. The Policy Discovery Engine discovers the policies using the workload and cluster information that is relayed by Shared Informer Agent.

11. What are Hardening Policies?

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 that are based on industry-leading 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.

12. What is Network Segmentation?

In Kubernetes, the network policy resource is a set of network traffic rules that are applied to a group of pods in a Kubernetes cluster. The network policy specifies how a pod is allowed to communicate with others. Network policy controllers (running as pods in the Kubernetes cluster) convert the requirements and restrictions of the network policies that are retrieved from the Kubernetes API into the network infrastructure.

13. How AccuKnox helps to implement Zero Trust?

By implementing a zero trust posture with KubeArmor, organizations can increase their security posture and reduce the risk of unauthorized access or activity within their Kubernetes clusters. This can help to protect sensitive data, prevent system breaches, and maintain the integrity of the cluster. KubeArmor supports allow-based policies which result in specific actions to be allowed and denying/auditing everything else. For example, a specific pod/container might only invoke a set of binaries at runtime. As part of allow-based rules you can specify the set of processes that are allowed and everything else is either audited or denied based on the default security posture.

14. Does KubeArmor only support Kubernetes or it can support on-prem deployments like legacy VM, pure containerized workload as well?

KubeArmor supports following types of workloads:

- K8s orchestrated workloads: Workloads deployed as k8s orchestrated containers. In this case, KubeArmor is deployed as a k8s daemonset. Note, KubeArmor supports policy enforcement on both k8s-pods (KubeArmorPolicy) as well as k8s-nodes (KubeArmorHostPolicy).
- VM/Bare-Metals workloads: Workloads deployed on Virtual Machines or Bare Metal i.e. workloads directly operating as host processes. In this case, KubeArmor is deployed in systemd mode.

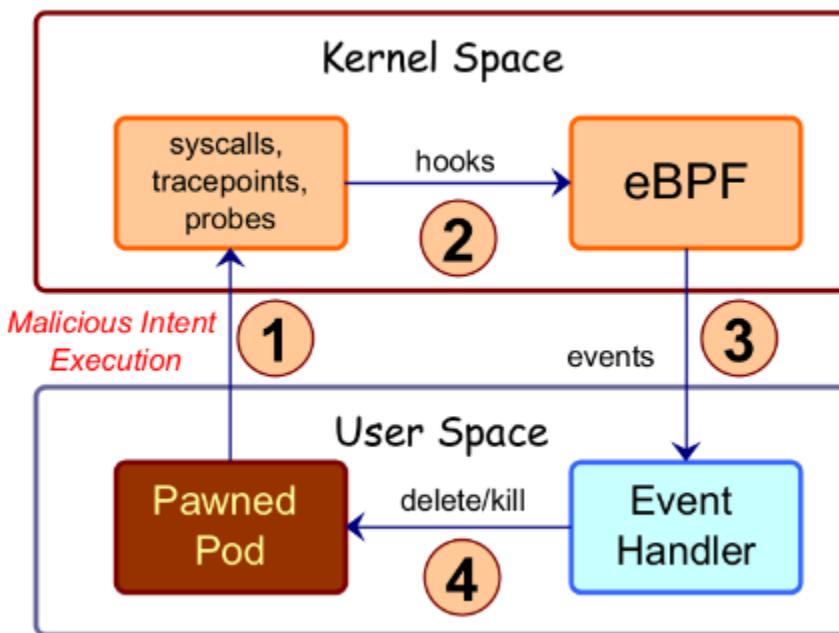
15. How AccuKnox helps achieve protection for Edge, 5G workloads?

With edge computing shifting towards containerized workloads and in few cases to orchestrated kubernetes workloads, it becomes important to have a security solution which can not only provide enforcement into different forms of deployment but can also provide real-time container-rich observability. KubeArmor

supporting un-orCHEstrated containers, k8s workloads and bare metal VMs makes it an ideal universal engine. Its kernel-level runtime security enforcement and container aware observability brings the best of both worlds..

16. What is the difference between Post-attack mitigation and in-line mitigation and which is better?

Post-exploit Mitigation works by killing the suspicious process in response to an alert indicating malicious intent. In this case attacker will be allowed to execute its binary and could possibly disable the security controls, access logs, etc to circumvent the attack detection. By the time the malicious process is killed, it might have already deleted, encrypted, or transmitted the sensitive contents.



Inline Mitigation on the other hand prevents the malicious attack at the time of happening itself. It doesn't allow the attack to happen by protecting the environment with security policy or firewall. AccuKnox's open source tool KubeArmor provides Inline Mitigation. KubeArmor uses inline mitigation to reduce the attack surface of pod/container/VM. KubeArmor leverages best of breed Linux Security Modules (LSMs) such as AppArmor, BPF-LSM, and SELinux (only for host protection) for inline mitigation

17. What are the platforms and environments that AccuKnox supports?

AccuKnox supports the following environments: + SaaS + PaaS + IaaS

AccuKnox supports the following cloud platforms: + AWS + GCP + Azure

AccuKnox support for the different platforms are as follows: + Kubernetes - Fully supported + Linux - Supported distributions + Serverless - Fargate and ECS supported, others are on roadmap + Windows - On roadmap

18.What role does AccuKnox Agents play in runtime-security?

AccuKnox Enterprise version consists of various agents such as

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.

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

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

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

19. Does AccuKnox provide auto discovery of assets and workloads?

Yes, AccuKnox can auto discover assets in the cloud by leveraging the cloud native tools.

For workloads, AccuKnox agents will provide the visibility data.

20. Can AccuKnox help in Monitoring?

- With Accuknox, you can create monitors for assets or group of assets to get alerts for changes observed in their Metadata (software version etc)
- Our Drift detection capability is inherently doing monitoring of the compliance checks (pass/fail) that have changed between scans.
- We collect alerts and telemetry generated by Kubearmor and cillum. These alerts are part of our CWPP offering. These alerts are generated for the events that have violated/complied with a policy.
- For these alerts you can have notification enabled as well through channels like Slack, email etc.

21. Do I need to enable native security services for AWS to get data into Accuknox?

AccuKnox only requires an IAM role to be created with read only access to be able to get data from AWS. Security Hub and Macie can be optionally enabled for AccuKnox to gather richer telemetry data with more context.

22. What are the Hypervisors or Virtualized Environments that are supported by AccuKnox?

AccuKnox technology does not integrate at the VM virtualization layer. AccuKnox tech integrates at the operating system layer and ensures that the right hardening/enforcement for process executions, network access, and file access is in place. Thus AccuKnox can operate on any virtualization tech provided that the underlying VM uses Linux as its operating system.

23. What is the differentiation of AccuKnox in ASPM Security?

In the ASPM Security solution, unlike other tools, AccuKnox provides flexibility to integrate a variety of open source and commercial security scanning tools through built-in parsers to provide you a composite security posture of your infrastructure. This is mainly done for the following two context:

- Remove dependencies and scoped results from one tool
- Bring in contextual understanding of vulnerabilities and prioritization based on that

Further on this, We also correlate and normalize results from a variety of security scanning tools and provide detailed results of vulnerabilities across infrastructure.

20.2 Bonus Questions

1. What are the modules supported by AccuKnox CNAPP currently?

- CSPM
- ASPM
- DevSecOps security in CI/CD pipeline
- CWPP
- Container Images Scanning
- CDR (Cloud Detection or Response) or CDM (Continuous Diagnostic & Mitigation)

2. What are all the compliance frameworks that AccuKnox is covering?

AccuKnox's CNAPP tool checks for compliance and governance from various benchmarks like STIG, CIS, NIST CSF, HIPAA, MITRE, SOC2, ISO 27001.

3. Does Inline remediation slowdown the process?

LSMs are already enabled in the environment and use host based LSM security. Since the attacker usually has direct access to the pod, AccuKnox uses Inline remediation to stop the processes before executing. Therefore, inline remediation does not slow down the process

4. What does AccuKnox measure, while doing security posture observation and how does it help in securing using policies?

- Compliance Frameworks (MITRE, CIS, NIST) for hardening workloads are used to create hardening policies
- Understanding the Application behaviour using LSMs enables creation of behavioural policies
- Hardening policies are block based policies
- Behavioural policies are allow based policies
- An example of policies is FIM (File Integrity Monitoring) policy

5. Do you have any standard hardening rules onboarded and will the hardening policy show what is getting blocked?

Yes, it can show up in terms of Application Behaviour & Logs

6. What is the deployment architecture?

- Applications -
 - For Kubernetes - Daemonset
 - For Containers, VM - Systemd mode
- Infrastructure -
 - Public Cloud - Agentless (API Scan) for SaaS based usage
 - On-Prem or Datacenter - On-prem deployment using Helm-charts

7. Where is AccuKnox SAAS is located?

Currently it is located in US region

8. Is there a support for CIEM?

It is a part of the roadmap, like IOT edge, 5G Security

9. What will happen to my application running on a VM?

You get hardening policies via AccuKnox enforcement engine KubeArmor

10. What is AccuKnox's licensing model?

If it is an end customer - SLA

If it is a MSSP model, it is a revenue share

11. How do you work with resellers and partnership models?

We have a 100% partner aligned go to market approach. to this goal, we provide our partners the following
+ Free training, certification + Joint marketing + Lead sharing

12. Current AccuKnox's marketplace listing?

AccuKnox is currently listed on

- VMWare
- AWS
- Azure
- RedHat Openshift

We are in the process of listing on

- GCP
- Oracle

13. Who are current AccuKnox's partners and resellers?

- We have a global partnership with TCS
- We have a reseller partnership with Ambisure

References:

<https://help.accuknox.com/introduction/home/>

<https://kubearmor.io/>

<https://docs.kubearmor.io/kubearmor>

Featured by



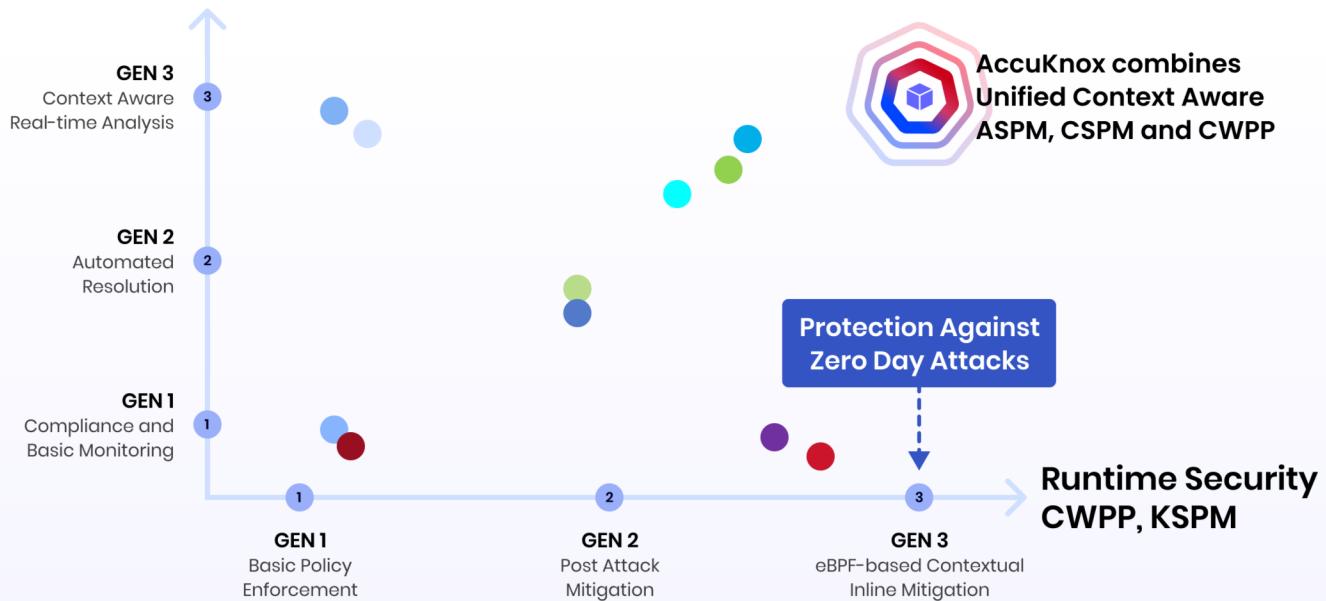
ORACLE

Gartner



LF EDGE

Static Security ASPM, CSPM



Extra 30 Days Free Trial



* No strings attached, Limited period offer!



Scan for Demo

About AccuKnox

AccuKnox is a Zero Trust CNAPP Cloud Security protects Public clouds, Private clouds, Kubernetes, VMs, Bare metals, IoT Edge, and 5G security.



ACCUKNOX®

[linkedin.com/accuknox](https://www.linkedin.com/accuknox)

@AccuKnox