

User Manual – Getting Started Guide

July 25, 2023



Table of Contents

Getting Started Guide	6
CSPM Prerequisites	6
Cloud Account Onboarding	6
AWS	6
AZURE	9
GCP	
CWPP Prerequisites	23
Cluster Onboarding	25
Asset Inventory	
Cloud Assets	
Cloud Workload	35
Misconfigurations	
Where to find misconfigurations	
Asset Detail Page	
How to group by findings	
How to group by criticality and Status	45
How to create a ticket	
Issues/Vulnerabilities	53
Group findings by source and severity	53
How to group by Findings and severity	54
How to group by Asset and severity	55
How to create automated tickets in Findings and Asset grouping	57
How does registry scan happen?	57
How to interpret Registry scan results	60
What is Risk Based Prioritization?	60
Baseline	

How to a	create a Baseline out of a data source	
How to d	compare 2 baselines	64
Compliand	e	65
How to g	get Compliance for Cloud Assets	65
How to §	get Compliance for Cloud Workload	
App Behav	/ior	
How to i	nterpret network graph	
How to s	see App Behavior Telemetry	70
Runtime P	rotection w/ Policy Management	72
How to u	understand discover policies	72
How to u	understand Hardening policies	75
How to /	Audit application and get alerts for that	
When do	o we say policies are stable?	
What if s	something changes in Application??	
How to p	perform bulk operation on applying policies	
Integrations		
Integrate S	SIEM tools	
Splunk		
Splunk li	ntegration:	
Integrat	ion of Splunk:	
a.	Prerequisites:	
b.	Steps to Integrate:	
AWS Cloud	dwatch	
AWS Clo	udWatch Integration	
Integrat	ion of Amazon CloudWatch:	
a.	Prerequisites	
b.	Steps to Integrate:	

с.	Configuration of Alert Triggers:104
d.	Logs Forwarding:
Rsyslog .	
RSyslo	g Integration
Integra	ation of RSyslog:
a.	Prerequisites:
b.	Steps to Integrate:
Integrate	e Notifications Tools
Slack	
Slack I	ntegration:
Integra	ation of Slack:
a.	Prerequisites:
b.	Steps to Integrate:
Integrate	e Ticketing Tools
Jira Integ	ration
Integra	ation of JIRA:
a.	Prerequisites
JIRA in	tegration for CWPP:
JIRA in	tegration for CSPM:
Freshser	vice
Freshs	ervice Integration:
Integra	ation of Freshservice:
a. F	rerequisites
b.	Steps to Integrate:
Creating	Ticket Configuration
Integrate	e Registries
Regist	y114

	a.	Amazon Elastic Container Registry:	115
	b.	Google Container Registry:	115
	с.	Nexus Registry:	115
	d.	DockerHub Registry:	115
User N	lanage	ement	116
Invit	e folks	s to the workspace	116
Assi	gn RBA	٨C	120
Crea	ite Rol	es and Assign Users	121



Getting Started Guide

CSPM Prerequisites

Cloud Account Onboarding

AWS

1. Manual Setup

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

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

	Σ	\$?	Ohio 🔻	GAURA		HRA 🔺
ayout	+ /	Add wi	Accou	int ID:	1997 - 199 3	07 (7)	
			Αςςοι	unt			
			Orga	nization			
vice			Servi	ce Quotas			
			Billin	g Dashboai	rd		
			Secu	rity credent	ials		
			Settii	ngs			
						Sign	out





- 2. From AccuKnox SaaS UI (Access Key Method)
 - Click settings -> Cloud Accounts
 - Click Add account

Dashboard	Cloud Account	ts					
Inventory ~	Search						Add Account
🛦 issues 🗸 🗸	Cloud	Account	Connected	Status	Enabled	Last scanned	Scan
🖥 Compliance 🗸	aws	aws: 199488642388	2023-02-22		29 h		Scan
	aws	aws: 963417633336	2023-02-22		25 h		Scan
© Collectors	aws	aws: 956994857092	2023-02-23		4 h		Scan
Remediation 🗸	aws	aws: 788471067825	2023-02-23		2 h		Scan :
■ Monitors / v Logging v							
E Reports							
Settings							
Cloud Accounts							
Manage Cluster							
User Management							
RBAC	1-4 of 4 < >						Rows per page: 100 +

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



Dashboard	
Inventory	Ť
	ř
Compliance	Ť
Runtime Protection	~
© Collectors	
Remediation	•
Monitors / Logging	•
E Reports	
A Notifications	
Settings	^
Cloud Accounts	
Manage Cluster	
User Manageme	nt
RBAC	

• Select the Labels and Tags

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

	Home $>$ Settings $>$ Cloud Accounts $>$ Add Account		solutions	~ °	Shanmuga 🗸
7 Protection		o o o			
🗈 Remediation 🗸		Cloud Account Label & Tag Set Up Details Connectivity			
Monitors / Logging ~		Label* 🛞			
🖹 Reports		ADITYA			
Notifications		Tag 💿			
🕸 Settings 🖍		aditya 🗸			
Cloud Accounts					
Manage Cluster		Back Cancel Next			
User Management					
RBAC					
Integrations					
Labels					
Tags					

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



Home > Settings > Cloud Account > Add Account			solutions ~	🖒 Shanmuga 🗸
	Cloud Account Lat Details	el & Tag Set Up Connectivity		
I Monitors / →	Access Key ID*			
E Reports	shanmuga+solutions@accuknox	com		
Notifications	Secret Access Key*	Show steps		
Settings A		Θ		
Cloud Accounts	Region*	Select All		
Manage Cluster	ap-south-1	eu-north-1		
User Management	eu-west-3	eu-west-2 ap-northeast-3		
RBAC	ap-northeast-2	ap-northeast-1		
Integrations	ca-central-1 ap-southeast-1	ap-southeast-2		
Labels	eu-central-1	us-east-1		
Tags	us-west-2			
Groups				
	Back	Cancel		
🕞 Log Out				

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

	Home > Settings > Clou	id Accounts				solutions	~ \	Shanmuga 🗸
7 Protection Y	Orașele							
Remediation 🗸	Search						Add Account	-
■ Monitors / Logging ~	Cloud	Account	Connected	Status	Enabled	Last scanned	Scan	
은 Reports	aws	aws: 172721035794	2023-07-10	-	10 days ago	2023-07-10	Scan	:
Notifications	aws	aws: 750567562417	2023-07-05		15 days ago	2023-07-20	Scan	:
💠 Settings 🖍		gcp: priyashan-390305	2023-07-10	-	10 days ago	-	Scan	:
Cloud Accounts		azure: 7e851ea0-b37b-4664-af56-	€ 2023-07-10		9 days ago	2023-07-20	Scan	:
Manage Cluster								
User Management								

AZURE

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

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



All Services (34) Documentation (99+)	Reso	urces (0) Resource Groups (0) Marketplace (0)	
Azure Active Directory (0)			
ervices		See all)
App registrations		App proxy	r
App Services		🎸 Function App	
E Event Grid Partner Registrations		Application gateways	
App Configuration		Application groups	
ocumentation		See all	
egistering applications	C ⁷	ALM Accelerator App Registrations - considerations when designi	ł
mplement app registration - Training	ď	Share gallery images using an app registration - Azure Virtual Ma	ł
emove limits on creating app registrations - Microsoft Entra	ď	Tutorial: Register a Single-page application with the Microsoft ide	ł
egister your app with the Azure AD v2.0 endpoint - Microsoft	Gr	Configure required Azure AD Graph permissions for an app regist	
Continue searching in Azure Active Directory			
arching all subscriptions		₽ Give feedback	

• Here click on New registration

Home > App registra	tions 🖈					
+ New registration	Endpoints	🤌 Troubleshooting	🖒 Refresh	↓ Download	🐼 Preview features	🔗 Got feedback?
 Starting June 30t and Microsoft Gr 	h, 2020 we will no l aph. <u>Learn more</u>	onger add any new feati	ures to Azure Act	tive Directory Auth	entication Library (ADAL) and Azure AD Graph. We will c
All applications	Owned applicati	ons Deleted appl	ications			
Start typing a dis	play name or app	lication (client) ID to fil	lter these r	+ _▼ Add fil	ters	
7 applications found Display name 1						

• Name your application, remember this name as it will be used again later, For the rest keep the default settings.



Home > App registration	ons >
Register an a _l	pplication
Name	
he user-facing display na	ame for this application (this can be changed later).
Accuknox-may-2023	\checkmark
Supported account t	ypes
Who can use this applicat	tion or access this API?
 Accounts in this orga 	anizational directory only (Default Directory only - Single tenant)
Accounts in any orga	anizational directory (Any Azure AD directory - Multitenant)
Accounts in any orga	snizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
Personal Microsoft a	ccounts only
lelp me choose	
Redirect URI (optiona	al)
Ve'll return the authentic hanged later, but a value	ation response to this URI after successfully authenticating the user. Providing this now is optional and it can be is required for most authentication scenarios.
Select a platform	e.o. https://example.com/auth
ocicer a plationin	·
Register an app you're wo	orking on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.
By proceeding, you agree	e 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'

splay name : <u>Accuknox-may-2023</u>		Client credentials	: Add a certificate or secret
plication (client) ID : 0aaaf206-7336-		Redirect URIs	: Add a Redirect URI
oject ID : e3dcd617-e4b3-		Application ID URI	: Add an Application ID URI
rectory (tenant) ID : 57650de0-d901-		Managed application in I.	: Accuknox-may-2023
pported account types : My organization only			
ectory (tenant) ID : 576500e0-0901- pported account types : <u>My organization only</u> Welcome to the new and improved App registr	ons. Looking to learn how it's changed from App registrations (Le	Managed application in l.	: <u>Accuknox-may-2023</u>

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



P Search	« R Got feedback?				
Overview					
Quickstart	Got a second to give us	some feedback? \rightarrow			
Integration assistant					
anage	Credentials enable confidenti scheme). For a higher level of	al applications to identify themselves t fassurance, we recommend using a cer	o the authentication service wi tificate (instead of a client sec	hen receiving tokens at a web addressable location (ret) as a credential.	using an HTTPS
Branding & properties					
Authentication		radificates secrets and federated condan	als can be found in the tabs belo	na l	
Certificates & secrets	Copromoti registration			479-	
Token configuration	Certificates (0) Client	secrets (1) Federated credentials	(0)		
API permissions	A correct strings that the seal	instian upor to remus its identity when	majartina a takan Also can b	a referred to an available paraved	
Expose an API	w secret suring that the appr	ication uses to prove its mentity when	requesting a token. Also can o	e reveneu to as approation passivoru.	
App roles	+ New client secret				
Owners	Description	Expires	Value 🛈	Copied scret ID	
Roles and administrators	may-2023	5/8/2025	zXd8Q~	- [15] 72e13faf-	0
Manifest					

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

$ \mathcal{P} $ subscriptions	×				
All Services (8) Marketplace (5) Documentat Azure Active Directory (0)	tion (99+) Resources (0) Resource Groups (0)				
Subscriptions	📧 Event Grid				
Billing subscriptions	🖾 Management groups				
Event Grid Subscriptions	Service Bus				
3 🚯 Quotas	间 Resource groups				
1 Marketplace					
SharpCloud Subscriptions	Barracuda WAF Add On Subscriptions				
e 🖄 HARP Connect	💪 UIB UnificationEngine® WhatsApp Business Platform Subscrip :s				
🖄 Medialine Managed Service in Subscriptions					
Documentation	See all				

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



≡ Micr	osoft Azure		𝒫 Search resour	rces, services, and docs	(G+/)
Home >					
Subscri Default Directo	otions 🖈 … y				
+ Add	Manage Policies 📒 View Requests 👁 Vie	ew eligible subscriptions			
P Search for	any field Subscriptions == global filter	r My role == all	Status == all	+ _▼ Add filter	
Subscription	name 1	¢↓	Му	role ↑↓	
Microsoft A	zure Sponsorship f3f782a3-		Owr	ner	

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

₽ Search «	+ Add ↓ Download ro	ole assignments ≡≡ Edit columns 🔘 Refresh 🛛 🗙 Remove 📄 🎘 Feedback
Overview	Add role assignment	ete Palas Dany assignmente Classis administrators
Activity log	Add co-administrator	Classic administrators
Access control (IAM)	Add custom role	permissions. You can use the built-in roles or you can create your own custom roles. Learn more 🖉
Tags		× Type : All Category : All
Diagnose and solve problems		
Security	Showing 0 of 412 roles	
Events	Name ↑↓	Description ↑↓
lling	No results.	
Invoices		
Payment methods		
Partner information		
ttings		
Programmatic deployment		
Resource groups		

• Search for "Security Reader" Job function Role, select it and press next



Home > Subscriptions > Microsoft Azure Sponsorship Acc	sess control (IAM) >
Add role assignment	
Role Members Review + assign	
A role definition is a collection of permissions. You can use the b	uilt-in roles or you can create your own custom roles. Learn more 🕫
Assignment type	
Job function roles Privileged administrator roles	
Grant access to Azure resources based on job function, such as	: the ability to create virtual machines.
♀ security reader	× Type : All Category : All
Name $\uparrow \downarrow$	Description ↑↓
Security Detonation Chamber Reader	Allowed to query submission info and files from Security Detonation Chamber
Security Reader	Security Reader Role
< Previous Page 1 v of 1 Next >	

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

Add role assig	gnment	
Role Members	Review + assign	
Selected role	Security Reader	
Assign access to Members	 User, group, or service principal Managed identity +<u>Select members</u> 	
Description	Name No members selected Optional	Object ID

Getting Started Guide



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



From AccuKnox SaaS UI

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

- Home > Settings > Cloud Accounts solutions 0 ACCUKNOX Protection Search Add Account Remediation Monitors / Cloud Account Connected Status Enabled Last scanned Scan aws aws: 172721035794 2023-07-10 10 days ago 2023-07-10 Scan E Reports aws aws: 750567562417 2023-07-05 2023-07-20 Scan . 15 days ago A Notifications 0 2023-07-10 Scan gcp: priyashan-390305 . 10 days ago Settings azure: 7e851ea0-b37b-4664-af56-€ 2023-07-10 2023-07-20 Scan -9 days ago Cloud Accounts Manage Cluster User Management
- Go to settings-> Cloud Account and click on Add Account

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

Shanmuga v



	Home $>$ Settings $>$ Cloud Accounts $>$ Add Account			solutions	ۍ ۲	Shanmuga 🗸
7 Protection Y		0	- 2 3			
Remediation ~		Cloud Account Details	Label & Tag Set Up Connectivity			
■ Monitors / ✓ Logging		Cloud Account Type *				
🖹 Reports		Microsoft Azure	~			
A Notifications						
🕸 Settings 🖍			Cancel Next			
Cloud Accounts						
Manage Cluster						
User Management						
RBAC						

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

	Home $>$ Settings $>$ Cloud Accounts $>$ Add Account		solutions - 🏷 Shanmuga -
7 Protection		Ø Ø 3	
Remediation 🗸		Cloud Account Label & Tag Set Up Details Connectivity	
■ Monitors / Logging ~		Label* 💿	
🖹 Reports		CHIRAGAZURE ~	
A Notifications		Tag 🕲	
🕸 Settings 🖍		azure-guru ~	
Cloud Accounts			
Manage Cluster		Back Cancel Next	
User Management			
RBAC			
Integrations			



• 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

	Home > Settings > Cloud Accounts > Add Account	knoxdemo ~ Q
I	Ø — Ø — Ø	
Remediation ~	Cloud Label & Tag Set Up Account Connectivity	
Monitors / V Logging V	Details	
E Reports	Application ID* Show sh	aps
Notifications	0aaaf206-7	
🕸 Settings 🖍	Key Value* Show sh	aps
Cloud Accounts	zXd8Q~oG	
Manage Cluster	Subscription ID* Show str	eps
User Management	f3f782a3-	
RBAC	Directory ID1 Show d	
Integrations	57650de0-	- cut
Labels		
Tags	Back Cannot Connect	
Groups		
Ticket Template		
🕞 Log Out		

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

	Home > Settings > Close	ud Accounts				solutions	Shan	muga 🗸
Protection								
Remediation ~	Search						Add Account	
■ Monitors / Logging ✓	Cloud	Account	Connected	Status	Enabled	Last scanned	Scan	
E Reports	aws	aws: 172721035794	2023-07-10		10 days ago	2023-07-10	Scan	
Notifications	aws	aws: 750567562417	2023-07-05	-	15 days ago	2023-07-20	Scan	
💠 Settings 🖍	<u></u>	gcp: priyashan-390305	2023-07-10	-	10 days ago		Scan	
Cloud Accounts		azure: 7e851ea0-b37b-466	4-af56-€ 2023-07-10		9 days ago	2023-07-20	Scan	
Manage Cluster								
User Management								

GCP

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



\equiv	Google Cloud	♣ k8s-wp-pr
θ	IAM & Admin	IAM
+2	IAM	PERM
Θ	Identity & Organization	Perr
3	Policy Troubleshooter	These
Ę	Policy Analyzer	
	Organization Policies	VI
음	Service Accounts	=
	Workload Identity Federat	
•	Labels	
	Tags	
-	Settings	
\$	Manage Resources	
Ē	Release Notes	
<1		

• Click on "Create Service Account".



≡	Google Cloud	•	IAM				×	Q Search	►	¢ (?)	:	(
0	IAM & Admin	Service accourt	ts + CREATE SERVIC	E ACCOUNT	🗑 DELETE	+2 MANAGE ACCESS	C REFRESH		🗩 HELP /	ASSISTANT	۵۱	EARN
+ <u>+</u> 0	IAM Identity & Organization	Service account A service account rep Organization policies	nts for project " resents a Google Cloud service identi can be used to secure service accourt	" ty, such as code run nts and block risky s	nning on Comput	e Engine VMs, App Engine a eatures, such as automatic	apps, or systems ru IAM Grants, key cre	nning outside Goo ation/upload, or t	ogle. <u>Learn more</u> he creation of se	about service a	accounts entirely.	<u>ه.</u> [ک Learn
Ę	Policy Analyzer Organization Policies	Filter Enter	count organization policies.							(m
연	Service Accounts	Email		Status	Name ↑	Description	Key ID Key cr	eation date	OAuth 2 Client II) 🕜	Actio	ons
•	Workload Identity Federat	<u>compute</u>	@developer.gserviceaccount.com	·	Engine default service account		keys				•	
	Tags											
**	Settings											
¢ E	Manage Resources Release Notes											

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

8 1/	IAM & Admin			_ ·	-	9		
~		÷	Create service account		P	B HELP /	ASSISTANT	
+ <u>e</u> IA	IAM	0	Service account details					
\varTheta Id	Identity & Organization		Accuknox					
A P	Policy Troubleshooter		Display name for this service account					
B P	Policy Analyzer		service account ID * X C					
0	Organization Policies							
🖻 S	Service Accounts		Service account description					
II: W	Workload Identity Federat		Describe what this service account will do					
۹ La	Labels							
▶ Та	Tags		CREATE AND CONTINUE					
± S	Settinas		Grant this service account access to project					
¢ M	Manage Resources	2	(optional)					
E R	Release Notes	3	Grant users access to this service account (optional)					
<1		DO	e cancel					



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

Ĩ	You have ₹7,701.33 remainir	ng credit and may be c	izible for a discount once w	ou'va usad all of your aradita			
≡	Google Cloud	& k8s-wp-priy	= Finter Type to Inter			×	Q Search
0	IAM & Admin	← (Network Management	Roles Browser			
+•	IAM	🗢 S	Ops Config Monitoring	Editor			
Θ	Identity & Organization		Organization Policy	Owner Viewer			
2	Policy Troubleshooter	2	Other				
	Policy Analyzer	G	Project		mission to		
	Organization Policies	C	Proximity Beacon		2		
ᅄ	Service Accounts		MANAGE ROLES		i		
(#I)	Workload Identity Federat						

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

≡	Google Cloud	•	IAM			×	Q Search	>-	¢	?	:
θ	IAM & Admin	AccuKnox							ļ	E HELP	ASSISTANT
+ <u>e</u>	IAM	DETAILS PERMISSI	ONS KEYS	METRICS LOGS							
Θ	Identity & Organization	Keys									
٩	Policy Troubleshooter	A Service account	t keys could pose a secur	ity risk if compromised. We recom	mend you avoid downloading servic	e accour	nt keys and inste	ad use the <u>Wo</u>	rkload I	dentity F	ederation
E,	Policy Analyzer	E. Tou can lean	E. Tou can ream more about the best way to autoenticate service accounts on Google Cloud nete E.								
	Organization Policies	Add a new key pair or uploa	Add a new key pair or upload a public key certificate from an existing key pair.								
역	Service Accounts	Block service account key on Learn more about setting on	reation using organization rganization policies for se	on policies 🖄. ervice accounts 🖄							
	Workload Identity Federat	ADD KEY 👻									
•	Labels	Create new key	Key creation date	Key expiration date							
	Tags	Upload existing key									
12	Settings										
	Manage Resources										

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

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





2. From AccuKnox SaaS UI

• Click settings -> Cloud Accounts

Click Add account

	Home > Settings > Cloud Account	its					Customer Usecases 🗸 🗘	Ý
🛋 issues 🗸 🗸								
🕯 Compliance 🗸	Search						Add Account +)
	Cloud	Account	Connected	Status	Enabled	Last scanned	Scan	
Remediation ~	aws	aws:	2023-04-12		a month ago		Scan	
Monitors /		azure:	2023-04-21		18 days ago		Scan	
C Reports	aws	aws:	2023-05-04		5 days ago	2023-05-08	Scan	
	aws	aws:	2023-04-11		a month ago	2023-05-08	Scan	
Settings	aws	aws:	2023-05-08		21 hours ago	2023-05-08	Scan	
Cloud Accounts								
Manage Cluster								
User Management								
RBAC								
Integrations	Total Count: 5						Rows per page: 20 👻 < 📋 >	
Labels								
🕞 Log Out								



• Select the Cloud Account type to GCP and Click Next

	Home > Settings > Cloud Accounts > Add Account		Customer Usecases ~	٥
▲ issues		0 0 0		
🖬 Compliance 🗸		Cloud Label & Tag Set Up Account Connectivity Details		
f Runtime Protection		Cloud Account Type *		
Remediation 🗸		Google Cloud Platform (GCP)		
E Monitors / ~				
E Reports		Cancel Next		
A Notifications				
🔹 Settings 🖍				
Cloud Accounts				
Manage Cluster				
User Management				
RBAC				
Integrations				
Labels				
Tane				
🕒 Log Out				

• Select the Labels and Tags and click Next

		· · · · · · · · · · · · · · · · · · ·
ACCUKNOX Home > Settings > Cloud Accounts > Add Account		Customer Usecases 🗸
▲ Issues ~	o o o	
alt Compliance ∽	Cloud Label & Tag Set Up Account Connectivity Details	
+ Runtime -	Label 7	
Remediation v	KNOX GKE V	
e Monitors / ↓	Tag 🕲	
E Reports	gke-val-tag ~	
Q Notifications		
Settings	Back Cancel Next	
Cloud Accounts		
Manage Cluster		
User Management		
RBAC		
Integrations		
Labels		
G→ Log Out		

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

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



	Home > Settings > Cloud Accounts > Add Account	Customer Usecases 🗸
▲ Issues ~	Cloud Label & Tag Set Up Account Connectivity Details	
f Runtime Protection	Show steps	Steps to get Drag and Drop
Remediation ~	Project ID	1. Log into your Google Cloud console and navigate to
Monitors /	Client Email	IAM Admin > Service Accounts. 2. Click on "Create Service Account". 3. Enter "AccuKnox" in the "Service account name",
E Reports	Enter Your Client Email	then enter 'Accuknox API Access' in the description. 4. Click on Continue. 5. Select the role: Project > Viewer and click Continue.
A Notifications	Private Key	 Click on "Create Key". Leave the default JSON selected and click "Create".
Settings	("type") "pervice_account", "transiec_taf" '	 Save the provided JSON file Copy the value of JSON in private key field box
Cloud Accounts	Sauluate, Janu 145, 1930058-03305155032058-234-0484596-E-34E-4725	
Manage Cluster		
User Management	Back Cancel Connect	
RBAC		
Integrations		
Labels		
🕞 Log Out		

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

• Check Settings \rightarrow Cloud Accounts. You will see your cloud account is added successfully.

	Home > Settings > Clos	id Accounts				solutions	ب	Shanmuga
 Protection 	Course							
Remediation 🗸	Search						Add Accou	m +
■ Monitors / v Logging v	Cloud	Account	Connected	Status	Enabled	Last scanned	Scan	
E Reports	aws	aws: 172721035794	2023-07-10		10 days ago	2023-07-10	Scan	:
Notifications	aws	aws: 750567562417	2023-07-05	-	15 days ago	2023-07-20	Scan	:
🔹 Settings 🖍	۵	gcp: priyashan-390305	2023-07-10	-	10 days ago		Scan	:
Cloud Accounts		azure: 7e851ea0-b37b-4664	-af56-€ 2023-07-10		9 days ago	2023-07-20	Scan	:
Manage Cluster								
User Management								

CWPP Prerequisites

Minimum Resource required

Deployments	Resource usage	Port	Connection Type
KubeArmor	CPU: 200 m, Memory: 200 Mi	-	-
Agents Operator	CPU: 50 m, Memory: 50 Mi	8081	Inbound/Outbound
Discovery Engine	CPU: 100 m, Memory: 100 Mi	-	-



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

• These ports need to be allowed through the firewall.



Cluster Onboarding

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

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

	Home >		customer ~ Q test ~
	CNAPP Dashboard	select	Cluster v Refresh 🗘 🚺 Last 2 days 🗸
	Image Risk Assessment	Image Security Issues	Runtime Policies Assessment
▲ Issues ✓			
I Compliance V	No Graph data avanable!	No Graph data avanable:	No Graph data available:
Protection	Top 5 Pods with Highest Egress and Ingress connections	Top 10 Namespace Specific Alerts	Remediations
Monitors / Logging ~		No Graph data available!	No Graph data availablet
E Reports	No Graph data available!		
Notifications	Puntime Alerte: Network Process File	Top 10 Alerts by Policy	Compliance Alerte
- Log Out	Runtime Alerts: Network, Process, File	TOP TO ALERTS BY POIICY	Compliance Alerts

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



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



	Home > Settings > Manage Cluster > Onboard	customer	۰ ۵	test 🗸
	Cluster Onboarding			
■ Monitors / Logging ~	Enter Cluster Name			
E Reports	gke-cluster			
A Notifications	Back Save & Next			
🔹 Settings 🖍				
Cloud Accounts				
Manage Cluster				
User Management				
RBAC				
→ Log Out				

Step 4: Onboarded Cluster without AccuKnox agents:

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

	Home $>$ Inventory $>$ Cloud Workloads				customer	~	٥	test ~
Dashboard	K8s Cluster	Clusters		Last 7 days	✓ C off	· · ·	Onboard Clust	ter
Inventory A	Search Kubernetes Cluster					LIST	GRAPH	•
Assets	→ 🔘 gke-cluster (0) 💿							
Cloud Workloads								
Imports			gke-cluster					
Explorer								
Baselines								
🔺 Issues 🗸 🗸								
🖬 Compliance 🗸								
		+						
<u> </u>		-						
G→ Log Out								

Step 5: Installing KubeArmor and AccuKnox agents:

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

Step 5.1: KubeArmor Installation:

KubeArmor:



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

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

KubeArmor differs from seccomp-based profiles, wherein KubeArmor allows to dynamically set the restrictions on the pod. With seccomp, the restrictions must be placed during the pod startup and cannot be changed later. KubeArmor leverages Linux Security Modules (LSMs) to enforce policies at runtime.

	Home $>$ Settings $>$ Manage Cluster $>$ Age	ants	customer	· () test ~
E Reports					
Notifications	List of Agents	1. KubeArmor			
🛱 Settings 🔺	KubeArmor	Installation Guide			
		Description			
Manage Cluster	Accultor Agents	This agent is used to apply system level policies			
User Management		Download and install karmor CLI			
RBAC		curl -sfL http://get.kubearmor.io/ sudo sh -sb /usr/local/bin		Сору 🖻	C
Integrations		Install KubeArmor			
Labels		karmor install		Сору 🖥	
Tags		2 Accuknox Agents			_
Groups		Installation Guide			
Ticket Template					
G→ Log Out			Back	Next	

KubeArmor is installed using the following commands:

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





Step 5.2: AccuKnox-Agents installation:

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

AccuKnox Agents:

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

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

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

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

	Home $>$ Settings $>$ Manage Cluster $>$ Ag	ents	customer	~	٥	test 🗸
Notifications	List of Agents	The AccuKnox agent is a K8s operator that installs the following agents:				
🗘 Settings 🖍	KubeArmor	 Reeder-service: It collects KubeArmor feeds. Shared-informer-agent: This agent authenticates with your cluster and colle entities like nodes, pods, and namespaces. 	ects information reg	arding		
Cloud Accounts	Accuknox Agents	- Policy-enforcement-agent: This agent authenticates with your cluster and e	nforces labels and	policies.		
Manage Cluster		 Discovery Engine: Discovery Engine discovers the security posture for your the policy set required to put the workload in least-permissive mode. The engineering 	workloads and auto gine leverages the ri)-discove ich visibil	ity	
User Management		provided by KubeArmor to auto discover systems and network security postu	res.			- I
RBAC		The agent-operator also manages the agents' resource limits. The operator is agents based on the size of the cluster. If the cluster size changes, i.e., new n	in charge of spawn odes are added or	ing the existing		
Integrations		nodes are deleted, then the operator scales up or down the resources accord	ingly.			
Labels				Сору 🖺		
Tags		helm repo add accuknox-agents https://accuknox-agents-dev:h47Sh4taE helm repo update	s@artifactory.accuk	n		
Groups		neim upgradeinstali agents-operator accuknox-agents/agents-operator set props.tenant_id="399" \ set props.workspace_id="399" \	./			
Ticket Template						
⊖ Log Out			Back	Nex	t	



AccuKnox Agents can be installed using the following command:



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

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

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

ACCUKNOX

	Home > Inventory > Cloud Workloads		customer ~ Q test ~
	K8s Cluster	Clusters > Pods	S Last 7 days ▼ C off ∨ Onboard Cluster
Baselines	Search	T Filter	LIST GRAPH
🛦 Issues 🗸 🗸	Kubernetes Cluster → ake-cluster (53)	(
🛍 Compliance 🗸		accutror-agents 01/o 1	Note-space (Delta)
		agents-operatio-6f886456 19-httd2 0 discovery-engine-56c8779 6ff-ahttg5 0	entropy and the second
📑 Remediation 🗸		sande-informer-agent-o7 reeder-service-to-442c7bb 9idd99i-Imygom8intzk policy-enforcement-agent -Secoolsford-agent	get-metter sport p20v kubasmor taxas Biochester Bioc
Monitors / Logging ~			calco-robe-s2wel calco-robe-s288 knowedroty-send-s2bcd Rearcal-spin-og Robe-sing b-mass-spin-reductive b-mass-spin-chapter knowedroty send-s2bcd Rearcal-spin-og b-mass-spin-reductive b-mass-spin-chapter knowedroty b-chapter knowedroty b-
Reports			kubeumor-2m2k gen-entrice-agent-fixege socialisto- kubeumor-2m2k gen-entrice-agent-fixege kubeumor-2m2k geges-colariti
A Notifications			Nuber dre vultosaler-956 calco-type-vertical-au 1987c-altin 0 tocale-668//129-1994 0 tocal-6658 calco-type-vertical-au
Settings ~		-	budersmort story may be also a set of the se
Ch Lon Out			pdcsi-node-t445z konnect/kty-agen-54bc6 fluentbit-gke-j82vj calico-typha-56995 18ocb-mxcdp pbtd4

Asset Inventory

Cloud Assets

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



• First navigate to the Assets screen under Inventory:





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

buck	et		Filter by I v	Filter by t 🗸	Filter by g V	ilter by a 🗸	Filter by d 🗸	Ct
	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da	Asset type	Data typ
	newbucketdirty	ADITYA	0	0/0		2023-07-10	s3bucket	4
	production-blog-awsgoa	ADITYA	0	0/0		2023-07-10	s3bucket	5
	dev-blog-awsgoat-buck	ADITYA	0	0/0		2023-07-10	s3bucket	5
	do-not-delete-awsgoat	ADITYA	0	0/0		2023-07-10	s3bucket	5
	thisisthebucket2	ADITYA	0	0/0	1	2023-07-10	s3bucket	5
	config-bucket-7505675	ADITYA	0	0/0		2023-07-10	s3bucket	4

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

Sear	ch	Filter by I	. v Fi	ilter by t v	Filter by g v	aws X ^		Filter by d 🗸	G
	Asset	Label	Targets	Baseline	Total Vulnerabilities	azuresubscriptior	da	Asset type	Data typ
	project-vpc	AWS100723	0	0/0		awslambda gcpproject	10	awsvpc	0
	vpc-069ee98298179beff	ADITYA	0	0/0		azurenetworkinte azurenetworksec	10	awsvpc	0
	AWS_GOAT_VPC	ADITYA	0	0/0		awsvpc	10	awsvpc	0
	vpc-0ac830ca18c12037a	AWS100723	0	0/0		host s3bucket	10	awsvpc	0
	vpc-01c32594e0ea8b87d	ADITYA	0	0/0		awsiamrole 2023-07-	10	awsvpc	0





• How to group assets

Г

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

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

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

					A	dd to Group
Search	Filter by I 🗸	Filter by t v	Filter by g 🗸	Filter by a 🗸	Filter by d 🗸	C ₀

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

Add to group	×
Choose the type of group:	
New group It allows you to create a new group	
O Existing group It allows you to edit an existing group	
Close	Next



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

Add to Group	×
Group	~
Back	Save

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

Sear	ch		Filter by I V	Filter by t v	test X ^	Filter by a v	Filter by d 🗸	C _t
	Asset	Label	Targets	Baseline	aws-1 's	Last Scan da	Asset type	Data typ
	public.ecr.aws/k9v9d5v		0	2/0	aws-2 aws-3	2023-05-22	container	2
	public.ecr.aws/k9v9d5v		0	1/0	aws-4 aws11	2023-06-14	container	3
	public.ecr.aws/k9v9d5v		0	1/0	test	2023-06-09	container	2
	accuknox-ui-softaculous	CHIRAGAZUR	E 0	0/0	azureresourcegro testdemo	2023-07-20	azureresource	0
	public.ecr.aws/k9v9d5v		0	1/0	samplecidwise 594 36 280	2023-05-27	container	3

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



Searc	ch		AWS X ^	Filter by t v	Filter by g v	Filter by a Y	ilter by d 🗸	C _t
	Asset	Label	ADITYA	ts Baseline	Total Vulnerabilities	Last Scan da	Asset type	Data typ
	project-vpc	AWS100723	AWS100723 AWSSTAGE	0/0		2023-07-10	awsvpc	0
	172721035794:us-east-1	AWS100723	CGJUNE15 CHIRAGAZURE	0/1		2023-07-10	securityhubaı	0
	AWSServiceRoleForAma	AWS100723	DEMOAZURE14	0/0		2023-07-10	awsiamrole	0
	172721035794:eu-north-1	AWS100723	GCP100723 GURUAZURE	0/0		2023-07-10	cloudsploitau	0
	project-subnet-public2	AWS100723	MSAZUREGURUN U	0/0		2023-07-10	awssubnet	0
	default	AWS100723	0	0/0		2023-07-10	awssecurityg	0
	AWS-accu-user	AWS100723	0	0/0		2023-07-10	awsiamuser	1

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

Cloud Workload

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





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

K8s Cluster	Clusters				Last 7 days 🗸	C off v	Onboard Cluster
Search						LIST	GRAPH
→ (a) aks-demo-	Cluster Name	Nodes	Pods	Active Policies	Alerts	Location	Network
→ ⁽⁶⁾ democluster (55) 0	aks-demo-prod	3	50	0	0		View Traffi
	democluster	4	55	0	0		View Traffi

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

K8s Cluster	Clusters		Last 7 days 🗸	C off ~ Onboar	rd Cluster
- Kubernetes Cluster					
→ @ aks-demo- prod (50) 183.7k					_
→ 💿 democluster (55) 💿		183.7k		AKS-DEMO-PROD	\times
		aks-d + Add Policies	a a	NO OF NODES	3
		+ Add Label		NO OF PODS	50
		View Pods View Nodes		NO OF POLICIES	
		View Policies		LOCATION	

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


Clusters > Pods	▲ Last 7 days ★	C off ~ Onboard Cluster
T Filter		LIST GRAPH
conjur Dinfo 0 conjur-conjur-oss-698fbf 6cd5-kb62v conjur-postgres-0	default Info vault-0 vault-0 vault-agent-injector-687 78b4555-5hq5g	dvwa Dinfo o dvwa-mysql-fb6b455f4-tfh kr dvwa-web-7f9b95f z

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

Clusters > Pods > Containers	♦ Last 7 days ♥ Onboard Cluster
	LIST GRAPH
	CONJUR-OSS ×
conjur-oss	IMAGE docker.io/cyberark/conjur:lat est
Conjur nginx	PORT 8080
	SERVICE conjur-conjur-oss

• Notice the Hierarchical structure above: Clusters > Pods > Containers. Clicking on any of them allows navigation through the different screens.

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



Clusters > Nodes		Last 7 days	C off ~ Onboard C	Cluster RAPH
	(3)		AKS-AGENTPOOL-16128849- VMSS000002	×
aks-age	ntpool-16128849-v aks-agentr mss000001 ms + Add	Policies 📖 a	LABELS	22
	aks-agentpool-16128849-v mss000000	Label I	NO OF PODS	17
			NO OF POLICIES	
			CONTAINERS	25
			ALERTS	
			LOCATION	

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

H Dashboard	Polic	cies					
🗉 Inventory 🗸	K8s	aks-demo-prod × × ×	Namespace	~ Po	olicy Type 🛛 🗸	Status	~
🔺 Issues 🗸 🗸							
ulu Compliance 🗸	Searc	ch					
All (249) Discovered (49) Hardening (195) Custom (5)							
CWPP Dashboard		Policy Name	Category	Status	Clusters	Namespace	Selector Labels
App Behavior		Ksp-vault-protect (v1) KubeArmor	Custom	 Inactive 	aks-demo-prod	default	None
Policies		harden-wordpress-pkg-mngr-exec (v KubeArmor	5 Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress
🗄 Remediation 🗸		harden-wordpress-file-integrity-monit KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress



Misconfigurations

Where to find misconfigurations

Asset Detail Page

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

\leftrightarrow \rightarrow C \triangleq app.dem	o.accuknox.com/inventory/asse	ts						• Q 🖻 🖈	😕 🕮 🖈 🗖 🔕
	Cloud	Hosts App	web/	API Cont	ainers Clusters				
Tashboard	388	13 0	0	4:	23 0				
Inventory A									
Assets	Asset Count by Sca	an	Ass	set Types by	Date	F	indings by D	ate	
Cloud Workloads	750 -		9				18K 13.5K-		
Imports	250 -						9K- 4.5K-		
Explorer	07/06/23		07/20/23	07/06/23		07/20/23	07/06/23		07/20/23
Baselines	Asset Count by Scan			Asset Types by Da	te		Findings by Da	te	
🔺 Issues 🗸 🗸									
🛍 Compliance 🗸	Search		Filter by	label ~ Filte	r by target v Filter by	group v Filter	by asset 🗸	Filter by data 👻	C ₀
Runtime Protection	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan date	Asset type	Data types	Monitors
Protection	public.ecr.aws/k9v9	d5v	0	1/0	29 50 6 9	2023-05-26	container	3	0
Remediation V	public.ecr.aws/k9v9	d5v	0	2/0		2023-05-22	container	2	0
Monitors / Logging	accuknoxuser/knox-	regi	0	1/0	190 140 51 64	2023-06-14	container	3	0
🖹 Reports	public.ecr.aws/k9v9	d5v	0	1/0	15 10	2023-06-14	container	3	0
	public.ecr.aws/k9v9	d5v	0	1/0		2023-06-09	container	2	0
🕒 Log Out	default	CHIRAGAZURE	0	0/0		2023-07-20	azuresubnet	1	0

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

	Home > Inventory > Assets > Details				solutions 🗸 🏷 Shanmuga 🗸
Dashboard	Asset details			Vulnerabilities	Compliance
Inventory ~	Asset Name: Label:	public.ecr.aws/k9v9d5v2/nginxinc:11	9-alpine	Critical	Failed Passed
Assets	Type: Last Seen:	container Friday, May 26, 2023 13:49 PM		Medium	
Cloud Workloads	0 3	0	0 0		
Imports	Tickets Group:	s Audit Files	Monitors Linked Assets		
Explorer					
Baselines	Explorer				
🔺 Issues 🗸 🗸	Search				
🖥 Compliance 🗸	Ticket Configuration v	Filter by			G 🖫 🔶 🗶 C
Runtime Protection	Last seen D	ata Type Tickets	OS	Monitors	
Remediation 🗸	2023-05-26 h	istory_metadata 0		1	
■ Monitors / v Logging v	2023-05-26 h	istory_metadata 0		1	
E Reports	2023-05-26 h	istory_metadata 0		1	
🕞 Log Out	Total Count: 20	·····			Rows per page: 20 👻 🤇 1 🗲



Scroll down for the Findings

ACCORNOX	Last seen Data Type Tickets OS Monitors	
Dashboard	□ 2023-05-28 bistory metadata 0 1	
Inventory A		
Accete	2023-05-26 history_metadata 0 1	
	2023-05-26 history_metadata 0 1	
Cloud Workloads		
Imports	Total Count: 20	Rows per page: 20 👻 < 1 >
Explorer		
Baselines	Findings	7
🔺 Issues 🗸 🗸	Search	
🖬 Compliance 🗸	Ticket Configuration v Group by v Data Type v Risk Factor v	
Runtime Protostion	Ignored v Status v Tickets v Exploit Available v	0 1 2 4 0 0
Protection	Last seen	
Remediation ~		
Monitors /	Last seen Risk Factor Finding Status Ignored Exploit Avail Tickets Data Type	
Logging	2023-05-26 Medium busybox: incorrect handling of a special Active False False 0 trivy	
🖺 Reports	2023-05-28 Medium curl Metalink download sends credentis Active False False 0 trivy	
A Notifications		
'	2023-05-26 Medium curt: auth/cookie leak on redirect: (curti@ Active False False 0 trivy	
🕞 Log Out		
	Total Count: 94	Rows per page: 20 - < 1 2 3 4 5 >

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

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

ACCORNOX	Vulnerabilities	Data type	~ bucket	x ^				
Dashboard	Risk factor	Ign	production- awsgoat-bu	blog- icket-	Status		1	Ficke 1
🗐 Inventory 🗸 🗸	Risk factor	~	Ignored 7505675624	417 ~	Status		•	Tic
	Group	Sci	an 750567562	icket- 417				
🔺 Issues 🖍	Group	~	Scan do-not-dele	ete- ~				
Vulnerabilities			awsgoat-sta files- 7505675624	ate-				
Registry Scan	Edit		thisisthebu	cket2				
Risk-based Prioritization			config-buck 7505675624	xet- 417				
🛯 Compliance 🗸	Search							
✔ Runtime Protection ✔	Ticket Configuration ~	Group by	~			Ø	(t)	0
Remediation 🗸	Last seen Find	ing			Status	Tickets	Ignored	
Monitors /	2023-07-10 Bloc	k public access setti	ngs are disabled for t	he S3 bucket	Active		False	

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



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

Sear	ch		Filter by I 🗸	Filter by t \checkmark	Filter by g V	s3b X ^	Filter by d \vee	C _t
	Asset	Label	Targets	Baseline	Total Vulnerabilities	azuresubscriptior da	Asset type	Data typ
	newbucketdirty	ADITYA	0	0/0		awslambda gcpproject	s3bucket	4
	production-blog-awsgoa	ADITYA	0	0/0		azurenetworkinte. azurenetworksec	s3bucket	5
	dev-blog-awsgoat-buck	ADITYA	0	0/0		awsvpc 10	s3bucket	5
	do-not-delete-awsgoat	ADITYA	0	0/0		s3bucket	s3bucket	5
	thisisthebucket2	ADITYA	0	0/0	1	awsiamrole 2023-07-10	s3bucket	5
	config-bucket-7505675	ADITYA	0	0/0		2023-07-10	s3bucket	4

Step 2 : Select all and Add to a group by clicking the Add to group button:

								Add to Group
Sear	ch		Filter by I V	Filter by t \vee	Filter by g v	s3b X ~	Filter by d \vee	Ct
\checkmark	Asset	Label	Targets	Baseline	Total Vulnerabilities	Last Scan da	Asset type	Data typ
	newbucketdirty	ADITYA	0	0/0		2023-07-10	s3bucket	4
	production-blog-awsgoa	ADITYA	0	0/0		2023-07-10	s3bucket	5
	dev-blog-awsgoat-buck	ADITYA	0	0/0		2023-07-10	s3bucket	5
	do-not-delete-awsgoat	ADITYA	0	0/0		2023-07-10	s3bucket	5
	thisisthebucket2	ADITYA	0	0/0	1	2023-07-10	s3bucket	5
	config-bucket-7505675	ADITYA	0	0/0		2023-07-10	s3bucket	4

Step 3: Click on Save

AccuKnox	itani - Safiragi - Araigi						solutions	~ D	Shanmuga -
* Protection *	Groups								
🖬 Remediation 🖂	Search						Dealers	nur + Dala	œ I
⊯ Monitors/ v	Name Name	Tickets	Assots	Findings	Esseine) Date	Time	Monitors	
🖹 Reports	🔲 ans-1					2023-06-09	07.00 PM	0	
A Notifications			Create group		×	Invelid Date	Invalid Date		
O Settings			Name*			Invisited Data	Invalid Data		
Cloud Accounts	□ ans-4		\$3-new			www.itd Date	Invalled Date		
Manage Cluster	Item D		Assets*	all manufaque manuface i manufacer -		Invalid Date	myseld Date		
User Management RBAC	tost 🗌		production-blog-awsgoat-b config-bucket-7505675624	ocket * thisisthebucket2	× ×	2023-07-25	07:51 AM		
Integrations	🗋 atomesourcegrosp		ao-nor-delete-awsgoor-tra	e-nes		2023-07-20	07-51 AM		
Labels	🔲 testilena		Cancel		Save	2023-05-22	SA SEPA		
Tags	asopiecizatas		6	73 789 234 8	50.	2023-07-29	07:51.464		
Greeps	at porter					2023-07-10	02-D): PM		
Content Template	Total Count 10							n per paga 20 + (



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



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



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

▲ Issues	~							_	
Vulnerabilities									
Registry Scan		S	Search						
Risk-based Prioritization			Ticket Configur	ation ~ As	sset X ~		C Co	⊘ ♦ ⋮	Ĵ.
d Compliance	~		Group ids	Last seen	Finding	Status	Tickets	Ignored	Data Type
Runtime Protection	~		1	2023-07-10	Block public access settings are disabled for the S3 buck	ket Active		False	securityhub
Remediation	~								
Monitors /									

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

Accet Turney 62Bug	kot	Status	Activo	~
Asset Type: S3Buc	ket	Status.	Active	Ť
Port: N/A		Ignored:	False	
		Tickets:	0	⊼
		Severity:	High	~
		Ticket Conf	figuration	ч Œ
			Save	
Description	Tool Output	Solution		References
All bucket-level bucket. Access	block public access to the bucket is cont access control lists	settings were dis rolled by accoun	sabled for t-level blo bucket's t	the S3 ock public

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

How to group by findings

1. Goto Issues tab, click on Vulnerabilities section



	Home > Issues	Vational	oitics											buloe	ions	×.	٥	User
Deshboard	Vulner	abilitie	BS Data	type =	Ass	et v									54	lect Config	1.2	€
	Risk factor				ig.	nored			Status				Ticke	96 - ⁻				
an a	Risk fact	þi		2		Ignored		×.	Status			×.	Ts	keta				*
▲ Issues ~	Group				50	lan												
Vulnerabilities	Group					Scan												
Registry Scan	_	-														C		
Risk-based Prioritization	£di															L	Reset	
🕯 Compliance 🗸	Canta																	
+ Runtime Protection *	Ticket C	en Figuradi	01 - 10	Houp by	-								Ø	6	3 @	Eh	.1.	0
Remediation v																	-	
Monitors /	Last of	en :	Finding				Status	Tick	th	Ignored	Data Type	Exploit	hvail	Asset				
Logging	2023-	7-20	segfaulting C	OB read; (Rati	n/u5@0.1-	1ubuntu1.18.04)	Attive			False	trivy	False		Jayjersan	leg			
Reports	2023-	7-20	seglauting C	008 need: 11km	ucuransw5	@61-1uburitu138.04)	Active			False	trivy	Faise		(ay)ersar	/my			
A Notifications	2023-4	7-20	heap-based	buffer overflow	er in Jaco	aptoinfo() in captoinfo.c	Active			False	trivy	False)ayjersar	ing_			
G+ Log Out	2023-	7-20	Possible DoS	translating AS	SN1 objec	ildertifiers: (Result1@11.	Active			False	trivy	False		jay)ersan	tmy			

2. Navigate to *Group by* filter.

	Home > issues > Vulnerabilities	solutions v Q. User v
E Dashboard	Vulnerabilities Data type Asset	Select Config 🗸 🗭
🗉 Inventory 🗸	Risk factor Ignored Status	Tickets
A 1	Risk factor v Ignored v Status	v Tickets v
Lissues ^	Group Scan	
Vulnerabilities	Group v Scan v	
Registry Scan		
Risk-based Prioritization	Edit	Reset
li Compliance v	Search	
Runtime Protection ~	Ticket Configuration v Group by v	0 to 0 🖉 🖬 t 0
🗉 Remediation 🗸		
Monitors /	Last seen Finding Status Tickets Ignored Data Type	Exploit Avail Asset
Logging	2023-07-20 segfaulting OOB read: (libtinfo5@8.1-lubuntu1.18.04) Active False trivy	False jayjersan/my
Reports	2023-07-20 segfaulting OOB read: (libncursesw5@61-1ubuntu118.04) Active False trivy	False jayjersan/my
Notifications	2023-07-20 heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: Active False trivy	False jayjersan/my
🕞 Log Out	2023-07-20 Possible DoS translating ASN1 object identifiers: (Ibssl11@i1.L. Active False trivy	False jayjersan/my
	2022-07-20 Local years can trional equivity-relevant memory contraction Active Ealer Triou	Ealea isularean/mu

Click on it and choose *Findings*

	Home > issues > Wehrenbilles	solutions v Q User v
Dashboard	Vulnerabilities Data type v Asset v	Select Config v
🗉 Inventory 🗸	Risk factor Ignored Status	Tickets
	Risk factor v Ignored v Status	v Tickets v
A Issues	Group Scan	
Vulnerabilities	Group v Scan v	
Registry Scan		
Risk-based Prioritization	Edit	Reset
III Compliance ~	Search	
Protection	Ticket Configuration v Group by A	0 1 4 0 0 0
Remediation ~	Status	
Monitors /	Last seen Finding Data Type Status Tickets Ignored Data Type	Exploit Avail Asset
Logging	2023-07-20 segfaulti Areat Areat Areat	False jayjersan/my
Reports	2023-07-20 segfaulting uous reas: noncurseswoig6.1-1ubuntu1.18.04) Active False trivy	False jayjersan/my
Notifications	2023-07-20 heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: Active False trivy	False jayjersan/my
🕒 Log Out	2023-07-20 Possible DoS translating ASN.1 object identifiers: (Rossi1.1@1.1 Active False trivy	False jayjersan/my
	2002 A7 20 Lood users on trianer constitut relevant moments corruntion. Active Edica False	Ealan lasianaa las



Now, you can see that similar findings are grouped. On clicking the arrow button in

the findings list, you will be able to view all the assets it is found in

-	Risk factor		- Ignored	~ Status		*) [Tickets	~
ACCUKNOX	Group		Scan					
Deshboard	Group		v Scan	¥				
liventory v	Leit							Reset
Lissues A								
Vulnerabilities	Faurth							
Registry Scan	operun							
Risk-based Prioritization	Ticket Config	ration -	inding X +			e	60	* G ± 0
Compliance v	Group ids	Last seen	Finding	Status Tickets	Ignored	Data Type	Exploit Avail	Asset
Buntime	0 1	2023-06-09	2060: (binutitu@2.30-93.el6)	Active	False	trivy	False	projectaccuk
Protection	□ 7D	2023-06-01	A ode execution vulnerability exists in the Statement B	linding Active	False	trivy	False	rajvanshijui
Remediation v	D 1	2023-06-09	Are Spectre-BHB mitigation for AmpereOne: (Inux-libc-	-dev@ Active	False	trivy	False	public.ecca
Monitons / v	• D	2023-05-22	A enial of service issue in a26027 driver in drivers/med	fia/us Active	False	trivy	False	public.ecca
Reports		2023-08-09	A enial of service issue in ap8027 driver in drivers/med	Salus Active	False	trivy	False	accuknosuse
Notifications			Recental of service issue in a26027 driver in drivers/med	Salus Active	False	trivy	False	fre20234/dx
		2023-08-15	A denial of service issue in a26027 driver in drivers/med	Salus Active	False	trivy	False	accuknoxuse
Log Out		2023-06-14	A denial of service issue in a25027 driver in drivers/med	Salus Active	False	trivy	False	public.ect.a
		2023-06-14	A denial of service issue in az8027 driver in drivers/med	Salus Active	Fatue	trivy	False	accuknowuse

How to group by criticality and Status

1. Goto Inventory tab, click on Assets section

	Home > Inventory > Asse	ts		solutions	✓ ↓ User ↓
- Dashboard	Assets				07/06/23 - 07/20/23
Inventory					
Assets	Cloud	Hosts	Apps	Web/API	Containers
Cloud Workloads	388	13	0	0	423
Imports					
Explorer	Clusters				
Baselines	0				
🔺 Issues 🗸 🗸	0				
🏜 Compliance 🗸	Asset Count k	oy Scan	Asset Types by [Date Findi	ngs by Date
Runtime			· I		1.11.1.1

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

	Asset Count by Scan Asse	et Types by Date	Findings by Date
Dashboard	750- 9- 500- 6-		13.5К- 9К-
Inventory			4.5K-
Assets	07/06/23 07/20/2: 07/0 ■ Asset Count by Scan ■ A	06/23 07/20/2: sset Types by Date	07/06/23 07/20/2: Findings by Date
Cloud Workloads			
Imports	Search	F v F v F v	F v F v Co
Explorer	Asset Label	Targets I	Baseline Total Vulnerabilit
Baselines			
🔺 Issues 🗸 🗸	accuknoxuser/knox-regi	0	1/0 413 271 639
🖥 Compliance 🗸	public.ecr.aws/k9v9d5v	0	1/0 15 10
Runtime	buntu:22.10	0 :	2/0 595 38 291
Protection	public.ecr.aws/k9v9d5v	0	2/0 396 311 629
Remediation 🗸	public.ecr.aws/k9v9d5v	0	1/0 397 310 629

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

Asset Name: public ecraws/Adv/d5/2/Inginanc:110-Jpine Orical	
Asset Name: public.ec.aws/k9/0d5/2/(ginxinc:13)-apine Critical Criticae Criticae Criticae Criticae Criticae Criticae Criticae Cri	
labet restord	
Assets Last Searc Friday, May 26, 2023 13:49 PM	
Cloud Workloads 0 3 0 0 0 0	
Imports Tickets Groups Audit Files Monitors Linked Assets	
Explorer	
Baselines Explorer	
▲ Issues Search	
Compliance Ticket Configuration Filter by Filter by	
Runtime Protection Last seen Data Type Tickets OS Monitors	
Remediation Colored at a 0 1	
Monitors / Logging 2023-05-26 history_metadata 0 1	
Reports 2023-05-26 history_metadata 0 1	
Contract Count: 20 Rows per page: 20 v K 1	>

	Home > Inventory > Assets > Details	solutions v) User -
Deshboard	Asset details Asset Name public act average Monte 2230	Vulnerabilities Compliance	•
Inventory ^	Label	Medum Passed	
Assets	Last Scerc Priday, June 9, 2023 18:43 PM		
Cloud Workloads	0 1 0 0 0		
Imports	Tickets Groups Audit Files Monitors Linked Assets		
Explorer			
Baselines	Explorer		
▲ Issues 🗸	Search		
A Compliance 🗸	Ticket Configuration v Filter by v	G 🖪 🔷 1	C
Runtime Protection	Last seen Data Type Tickets OS	Monitors	
Remediation ~	2023-06-09 history_metadata 0	1	
Monitors / Logging ~	2023-06-09 history_metadata 0	1	
Reports	2023-06-09 metadata 0 linux	0	
A Notifications	Total Countr 7	Braze new newsr. 98 -	
🗘 Settings 🗸 🗸	tean search, z	nows heli ballet i son A 🛛 🖌	
🕞 Log Out	Findings		7
	Search		

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

	2023-05-26 history_metadata 0 1
	2023-05-26 history_metadata 0 1
Dashboard	
■ Inventory ^	Total Count: 33 Rows per page: 20 🗸 < 1 2 🗲
Assets	
Cloud Workloads	Findings
Imports	Search
Explorer	Ticket Configuration - Finding X - Data Type - Risk Factor A
Baselines	Ignored v Status v Tickets v Unknown
🔺 Issues 🗸 🗸	Last soon
🎝 Compliance 🗸	Medium Last seen Risk Factor Finding c Exploit Avail Tickets Data Type
# Runtime	Critical
Protection	1 2023-05-28 Medium ARM straight-line speculation vulnerabil Active False False 0 trivy
Remediation ~	1 2023-05-26 Medium ARM straight-line speculation vulnerabili Active False 0 trivy
■ Monitors / ~	1 2023-05-26 Medium ARM straight-line speculation vulnerabili Active False 0 trivy
G→ Log Out	Total Count: 908 Rows per page: 20 🗸 🤇 1 2 3 4 5 48 >

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



Dashboard	No rows
Inventory ^	
Assets	Total Count: 0
Cloud Workloads	
Imports	Findings
Explorer	Search
Baselines	Ticket Configuration v Group by v Data Type v High x v
🛦 Issues 🗸 🗸	Ignored 🗸 Status 🗸 Tickets 🗸 Exploit Available 🗸 🙆 🕼 🗘 🗘
🎝 Compliance 🗸	Last seen
f Runtime Protection	Last seen Risk Factor Finding Status Ignored Exploit Avail Tickets Data Type
Remediation ~	2023-07-10 High CVE-2021-43565 - golang.org/x/crypto Active False False 0 securityhub
■ Monitors / ~	223-07-10 High CVE-2021-33194 - golang.org/x/net Active False False 0 securityhub
🖹 Reports	2023-07-10 High CVE-2023-0288 - libss11.1 Active False False 0 securityhub
🕞 Log Out	Total Comit: 49 Rows per page: 20 v C 1 2 3 >

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

	No rows
Deshboard	
Inventory ^	Teld Crust A
Assets	INTERNAL R
Cloud Workloads	Findings
Imports	Search
Explorer	Ticket Configuration - Platus x A Data Type - High x -
Baselines	Ignored v Status Tickets v Exploit Available v 🖉 Co 🖉 🔂 🗘 🛈
issues v	Last seen
Compliance V	many
Runtime Protection	Last seen Risk Factor Finding Status Ignored Exploit Avail Tickets Data Type
Remediation ~	1 2023-07-10 High CVE-2023-2650 - opensal Accepted Rial False False 0 securityhub
Monitors /	48 2023-07-10 High CVE-2022-42918 - curl Active False False 0 securityhub
-	
🕒 Log Out	Total Count: 2 Rows per page: 20 + C 1 >

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



	Findings
Dashboard	Search
Inventory A	Ticket Confi v Status X v Data Type v Risk Factor v
Assets	Ignored ~ Status ~ Tickets ~ Exploit Avail ~ 🖉 Γ _O 🧷 🔶 🔂 🗘 🛈
Cloud Workloads	Last seen
Imports	
Explorer	Last seen Risk Factor Finding Status Ignored Exploit Avail Tickets
Baselines	1 2023-07-10 High CVE-2023-2650 - openssl Accepted Ris False 0
🔺 Issues 🗸 🗸	□ 167 ▷ 2023-07-10 High CVE-2023-0215 - openssl Active False False 0
🕯 Compliance 🗸	
Runtime Protection	Total Count: 2 Rows per page: 20 + < 1 >

How to create a ticket

Goto Inventory tab, click on Assets section

	Home > Inventory > Asset	ls		solutions	 ✓ ↓ User ↓
- Dashboard	Assets				07/06/23 - 07/20/23
Inventory A					
Assets	Cloud	Hosts	Apps	Web/API	Containers
Cloud Workloads	388	13	0	0	423
Imports					
Explorer	Clusters				
Baselines					
🔺 Issues 🗸 🗸	0				
u Compliance 🗸	Asset Count b	y Scan	Asset Types by D	Date Findir	ngs by Date
▲ Runtime	1000		12	18K	1.11.1.11



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

	Asset Count by Scan	Asset Types by Date	Findings by Date
Dashboard	750- 500-	9- 6-	13.5К- 9К-
Inventory A		3- 0- -	4.5K-
Assets	Asset Count by Scan	07/06/23 07/20/2: ■ Asset Types by Date	07/06/23 07/20/2: Findings by Date
Cloud Workloads Imports	Search	F v F v	Fv Fv Fv G
Explorer	Asset	Label Targets	Baseline Total Vulnerabilit
Baselines			
Issues 🗸	accuknoxuser/knox-regi	0	1/0 413 271 639
🛚 Compliance 🗸 🗸	public.ecr.aws/k9v9d5v	0	1/0 15 10
Runtime	public.ecr.aws/k9v9d5v2/ buntu:22.10	/u0	2/0 595 38 291
Protection	public.ecr.aws/k9v9d5v	0	2/0 396 311 629
Remediation 🗸	public.ecr.aws/k9v9d5v	0	1/0 397 310 629

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

	Home > Inventory > Assets > Details	solutions v Q User v
Deshboard	Asset details	Vulnerabilities Compliance
Inventory ^	Label	Modum Passed
Assets	Type: container Last Seen: Priday, June 9, 2023 18-43 PM	
Cloud Workloads	0 1 0 0 0	
Imports	Tickets Groups Audit Files Monitors Linked Assets	
Explorer		
Baselines	Explorer	
▲ Issues 🗸	Search	
🕯 Compliance 🗸	Ticket Configuration v Filter by v	G G @ 1 @
Runtime Protection	Last seen Data Type Tickets OS	Monitors
Remediation ~	2023-06-09 history_metadata 0	1
■ Monitors / v Logging v	2023-06-09 history,metadata 0	
Reports	2023-06-09 metadata 0 linux	٥
A Notifications		
🗘 Settings 🗸 🗸	Total Count: 7	Rows per page: 20 ¥ < 1 >
🕞 Log Out	Findings	7
	Search	

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



Rows per page: 20 🕶 < 1 2 🔾

	2023-06-09		iisto/y metadata						1							
Total	Count: 7												Roms (iel page	20 ¥	E.
1	indiana															
	nungs															
	bearch															
	Ticket Configura	Son -	Group by	*	Data Type		Risk Factor									
	lgrored	-	Status		Tickets	÷ .	Exploit Availat	At			Ø	6	0	٢	6	Ţ.
	Last seen	0														
	ast seen	Risk Fact	or Finding			Status	Ignored	Exploit Avail	Tickets	Data Typ	pe					
	1023-08-09	Medium	Local use	ers can trig	ger security-relev	an Active	Følse	False	0	stivy						
	023-06-09	Medium	systema	tocal infor	mation leak due to	a vitike	False	False	0	silvy						
	2023-06-09	Medium	deadlock	in systems	d-coredump via a	cri Active	False	False	0	trivy						
-	****															
	196910-12 Pilos															
(] 2023-06-06)	history_metada	fa	0					1						
0	2023-06-05)	history_metada	fla fla	0					1						
C C To	2023-08-09 2023-08-09 tal Count: 7	9	history,metada	ta ta	0					1			Row	is per pag	pe: 20	¥ (
C C To	2023-08-09 2023-06-09 tal Count: 7	9	history,metada history,metada	ta ta	0					1			Row	is per pag	ge: 20	•
С (То	2023-08-05 2023-08-05 tal Count: 7 Findings	2	Nistory_metada	ta ta	0					1			Row	s per pag	ge: 20	•
C C To] 2023-06-06] 2023-06-06 tal Count: 7 Findings	2	history,metadu	ta ta	0					1			Row	s per pag	ge: 20	• <
C C To	2023-06-01 2023-06-01 tal Count: 7 Findings Coardh Ticker Config	aration A	Nistory, metada Nistory, metada Group by	ta ta	0 0 Data Type	~	Risk Factor	· · ·		1			Row	s per pa	ge: 20	
C To	2023-06-06 2023-06-06 tal Count: 7 Findings Ticket Config guru-test-val	aration A	Nistory, metada Nistory, metada Group by Status	6a 6a 	0 0 Data Type Tickets		Risk Factor	v) Iable v)		1	8	- Co	Row	s per pay	ре: 20 СЪ	t
C C Tu	2023-06-06 2023-06-06 tal Count: 7 Findings Casesh Ticket Config guru-test-vali guru-test-vali	eration A	history, metadu history, metadu Group by Status	ta ta	0 0 Data Type Tickets		Risk Factor Exploit Ava	v) latie v)		1	Ø	- Co	Row	s per pay	ge: 20	• (
1	2023-06-05 2023-06-05 tal Count: 7 Findings Ticket Config guru-test-val guru-test-val guru-test-val	d Bration	Nistory, metada Nistory, metada Group by Status	nta nta v v	0 0 Data Type Tickets	↓ ↓ Status	Risk Factor Exploit Ave	v latie v	L. Tickets	1	(2) Tupe	G	Row	s per pay	g≈ 20	• (
	2023-06-06 2023-06-06 tal Count: 7 Findings Gaarab Ticket Config guru-test-vall guru-test-vall guru-inprivals guru-inprivals guru-inprivals 2023-06-06	oration A d cogration Risk Fi	history, metada history, metada Group by Status sctor Findin n Local	ta ta v v g	0 0 0 Data Type Tickets rigger security-re	U Status I Status	Risk Factor Exploit Avai Ignored False	v Itable v Doplott Avai Faise	R_ Tickets	1 1 Data	С	Go	Row	s per pay	ре: 20 Ср	t
	2023-06-06 2023-06-06 2023-06-06 tal Count: 7 Findings Ticket Config guru-test-val guru-test-val guru-itest-val 2023-06-06 2023-06-06	d cration A d cegration Risk Fi Media	Nistory, metada Nistory, metada Group by Status sector Findin n Local	fa fa v g users can t nd: local ini	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Status ievani Active e to s: Active	Risk Factor Exploit Avai Ignored False False	v latite v Exploit Aval Faise	L. Tickets 0 0	1 1 Data trivy	(2) Type	Co.	Row	s per pay	g≈ 20	•

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

d. Choose the *Priority* from the dropdown.

Total Count: 25

🕞 Log Out



	Home \Rightarrow Issues \Rightarrow Vulnerabilities \Rightarrow Create Ticket			solutions	✓ Q User ✓
	C Deals to all				Constant
Dashboard	Eack to all				Create +
	Ticket 1 Ticket 2				
Inventory ~					
	Create ticket				
🔺 Issues 🔷 🔨					
Vulnorabilition	Priority	_			
Vulnerabilities	Medium	·			
Registry Scan	Hinhest				
Risk-based	High				
Prioritization	Medium				
b 0	Low				
Compliance V	Lowest				
& Runtime	Preserviction neutron before 6.4 2022040	19 when used by a setuid applica	ing allows local usars to trigger convity, relevant memory corre	ntion via malformed data i	n a terminfe
' Protection	database file that is found in \$HOME/.ter	minfo or reached via the TERMIN	On TERM environment variable.	ption via mailormed data i	n a terminio
Remediation ~	Synopsis				
	Impacted Assets				
Monitors /		B 1			
cogging	Asset	Port			
Reports	public.ecr.aws/k9v9d5v2/ubuntu:22.10	libncurses6@6.3+20220423-2			
	Blueie Octant				
	Prugin Output				
🕞 Log Out					

- 1. Edit the Ticket Title and Ticket Description, as required.
- 2. Click on the Create button at the top right corner.

	Vulnerabilities > Create Ticket	solutions ~	User v
Dashboard	sket 2		Create +
Inventory	~		
▲ Issues	^ licket		
Vulnerabilities			
Registry Scan			
Risk-based Prioritization	rs can trigger security-relevant		
ttps://app.demo.accuknox.cc	ntion		

You can see the tickets were created successfully.



ACCUKNOX	Home > Inventory >	ଁ	You have success	fully created 2 tickets	×	solutions	~	۵	User v
- Dashboard									
Inventory A									
Assets									
Cloud Workloads									
Imports									
Explorer									
Baselines									
🔺 Issues 🗸 🗸									

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

	bopened: 11 High 1 High 2 High 2 Med 3	13% JIRATEST 25% JIRATEST 38%	openssl: RSA authenticatio × 62 D Kernel: A use-after-free d × 55 D
▲ Issues ~	Cancelled: 0	0%	
uli Compliance 🗸			
f Runtime Protection	Tickets		
E Remediation	Search		Delete Close
Ticket Summary	Type: Label v Type: Dat v Type: Si	at v Type: Con v	Type: Prio V Type: Date
Monitors / Logging	Project name Ticket configuration	Ticket Number	Priority Ticket title
E Reports	JIRAINTEGRATIONTEST guru-test-valid	JIRATEST-262	= Medium Local users can
Notifications	JIRAINTEGRATIONTEST guru-test-valid	JIRATEST-263	— Medium systemd: local i
	JIRAINTEGRATIONTEST guru-inpriyaintegrat	ion JIRATEST-256	- Low ncurses: heap-

Issues/Vulnerabilities

Group findings by source and severity

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

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



	Home > Issues > Vulnerabilities	
Dashboard	Vulnerabilities Data type Asset	
Inventory	Risk factor Ignored Status T	icket
	Risk factor v Ignored v Status v	Tic
▲ Issues ▲	Group Scan	
Vulnerabilities	Group × Scan ×	
Registry Scan		
Risk-based Prioritization	Edit	
🌢 Compliance 🗸	Search	
<pre></pre>	Ticket Configuration	2
Remediation 🗸	Status	
Monitors /	Last seen Finding Data Type Status Tickets Ignored Data Type Exploit Avail	Ass
Logging	2023-07-20 seafaulti Finding Journ ul.18.04) Active False trivy	jayj€
🖹 Reports	Asset 2023-07-20 segfaulting OOB read: (libncursesw5@6.1-1µbuntu1.18.04) Active False trivy False	jayj€
A Notifications	2023-07-20 heap-based buffer overflow in _nc_captoinfo() in captoinfo.c: Active False trivy False	jayje
🔹 Settings 🗸 🗸	2023-07-20 Possible DoS translating ASN.1 object identifiers: (libssl1.1@1.1 Active False trivy False	jayj€

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

AccuKn	ох	Home	> Issues > Vuln	erabilities							
Dashboard		N	/ulnerabili	ties Data ty	pe v	Asset ~					
Inventory	~	R	isk factor			Ignored		s	Status		
▲ Issues	^		Risk factor			lgnored Scan	~		Status		
Vulnerabilities			Informational			Scan	~				
Registry Scan			Low								
Risk-based Prioritization			Medium High Critical								
L Compliance	~										
Runtime Protection	~		Search Ticket Configu	ration ~ Da	ta Type X	•					
Remediation	~										
Monitors /			Group ids	Last seen	Finding		Sta	tus	Tickets	Ignored	Data
Logging	Ť		173 ⊳	2023-07-10	Amazon S3 Blo	ock Public Access was disabled	for S3 bucket t Act	ive		False	secu
🖹 Reports			62752 >	2023-06-09	2060: (binutils	@2.30-93.el8)	Act	ive		False	trivy
A Notifications											
Settings	~										

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.



	iox	Home > Issues > Vulnerabilities				
Dashboard		Vulnerabilities Data type Asset				
Inventory	•	Risk factor Ignored		Status		
		Risk factor ~ Ignored	~	Status		~
▲ Issues	^	Group Scan				
Vulnerabilities		Group ~ Scan	~			
Registry Scan						
Risk-based Prioritization		Edit				
	Ť	Search				
Runtime Protection	~	Ticket Configuration V				
Remediation	•					
Monitors /		Last seen Finding Data Type	Status Tickets	Ignored	Data Type	Exploit Avail
Logging	Ť	2023-06-09 2060: (b Finding	Active	False	trivy	False
🖹 Reports		2023-06-01 A code execution vulnerability exists in the Statement Binding	Active	False	trivy	False
A Notifications		2023-06-09 Add Spectre-BHB mitigation for AmpereOne: (linux-libc-dev@	Active	False	trivy	False
Settings	×	2023-05-22 A denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False

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

	Home $>$ Issues $>$ Vulnerabilities				
Dashboard	Vulnerabilities Data type v Asset v				
🗉 Inventory 🗸 🗸	Risk factor Ignored		Status		
	Risk factor ^ Ignored	~	Status		
🔺 Issues 🖍	Unknown				
Vulnerabilities	Informational Scan	~			
Registry Scan	Low				
Risk-based	Medium				
Prioritization	High				
🌢 Compliance 🗸	United				
	Search				
Runtime Protection	Ticket Configuration V Data Type X V				
Remediation ~					
👝 Monitors /	Group ids Last seen Finding	Status	Tickets	Ignored	Data
Logging	173 D 2023-07-10 Amazon S3 Block Public Access was disabled for S3 bucket t	Active		False	secu
🖹 Reports	□ 62752 > 2023-06-09 2060; (binutiis@2.30-93.el8)	Active		False	trivy
A Notifications					
😫 Settings 🗸 🗸					

How to group by Asset and severity

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



	iome > Issues > Vulnerabilities			
Dashboard	Vulnerabilities Data type	✓ Asset ✓		
≡ Inventory ∽	Risk factor	Ignored	Status	
	Risk factor	✓ Ignored	∽ Status	
	Group	Scan		
Vulnerabilities	Group	∽ Scan	~	
Registry Scan				
Risk-based Prioritization	Edit			
🖥 Compliance 🗸	Search			
	Ticket Configuration 🗸 🕴	^)		
🖪 Remediation 🗸	Status			
— Monitors /	Last seen Finding Data Type	Statu	Is Tickets Ignored	Data T
Logging V	2023-06-09 2060: (bi Asset	Activ	e False	trivy
E Reports	2023-06-01 A code execution vulr	nerability exists in the Statement Binding Activ	e False	trivy
Notifications	2023-06-09 Add Spectre-BHB mit	igation for AmpereOne: (linux-libc-dev@ Active	e False	trivy
🕸 Settings 🗸 🗸	2023-05-22 A denial of service iss	sue in az6027 driver in drivers/media/us Active	e False	trivy
		un in an 0007 duiters in deiters (madia (

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

) ЭХ	Home	> Issues > Vuln	erabilities							
🗄 Dashboard	I	V	ulnerabili	ties Data ty	pe v	Asset ~					
Inventory	~	Ris	sk factor			Ignored			Status		
			Risk factor		^)	Ignored		~	Status		
▲ Issues	^		Unknown			Scan					
Vulnerabilities			Informational			Scan		~			
Registry Scan			Low								
Risk-based			Medium								
Prioritization			High								
Compliance	•		ontical								
		4	Search								
Runtime Protection	~		Ticket Configu	ration × Da	ta Type X	*					
Remediation			fielder oonlige		ia i jpo						
			Group ids	Last seen	Finding			Status	Tickets	Ignored	Data
Monitors / Logging	~	_									
			173 ▷	2023-07-10	Amazon S3 Blo	ck Public Access was disa	bled for S3 bucket t	Active		False	secu
			62752 ⊳	2023-06-09	2060: (binutils)	@2.30-93.el8)		Active		False	trivy
A Notifications											
Settings	~										

How to create automated tickets in Findings and Asset grouping

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

	Risk factor	Ignored	Status			Tickets	
	Risk factor	* Ignored	~ Statu	s	~	Tickets	~
- Dashboard	Group	Scan					
🗉 Inventory 🗸 🗸	Group	Ƴ Scan	~				
▲ Issues	Edit						Reset
Vulnerabilities							
Registry Scan	Search						Create a ticket
Risk-based Prioritization	-test-valid X ^ Finding	X Select ticket			Create ticket	e la l	🤊 💩 🖞 🛈
🎝 Compliance 🗸	-test-valid integration en Fi	continguration	Status	ickets Ignored	Data Type	Exploit Avail	Asset
	□ 6 ▷ 2023-05-22 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	public.ecr.a
Remediation 🗸	I7 ▷ 2023-06-09 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	accuknoxuse
Monitors /	2023-06-15 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	frez0234/dv
Logging	2023-06-15 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	accuknoxuse
🖹 Reports	2023-06-1, Selec	az6027 driver in drivers/media/us	Active	False	trivy	False	public.ecr.a
A Notifications	2023-06-14 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	accuknoxuse
	2023-06-09 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	accuknoxuse
🕸 Settings 🗸 🗸	2023-06-09 A	denial of service issue in az6027 driver in drivers/media/us	Active	False	trivy	False	public.ecr.a

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

How does registry scan happen?

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

Registry Onboarding:

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

ACCUKNOX

	Home \supset Issues \supset Registry Scan		AccuKnox ~ 🗘 Customer ~
Dashboard	Image Scanning Progress	Image Risk Assessment	Image Security Issues
🗐 Inventory 🗸 🗸	Total Registered Images	4 Total Vulnerabilities	3.1k Total Images 1
▲ Issues	4 Scanned Images 0 Failed to Scan	Critical High Medium	315 928 1 1 1 1 1 0 926
Vulnerabilities	0 Images in Queue	Low Negligible	938 15 Total Malware: 0 2 Total Sensitive Data: 0
Registry Scan		No Issue	
Risk-based Prioritization	Findings Scan Queue		
🏜 Compliance 🗸	Search		Add Registry
✔ Runtime Protection ✓	Repositories	Security Issues	Registry Name
◎ Targets	 accuknoxuser/knox-registry 	<u>301</u> 720 673 349 8 ₿ ⁰	a •
Remediation 🗸	 accuknoxuser/knox-registry 	301 720 673 349 8 ₫ ∘	ê •

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

	Home $ ightarrow$ Settings $ ightarrow$ Integrations $ ightarrow$ Registry $ ightarrow$ Add	AccuKnox	۰ ۵	Customer ~
Dashboard	CWPP CSPM Registry S3 Data Source			
Inventory ~				
🔺 Issues 🗸 🗸	Add Registry			
🖥 Compliance 🗸	Registry Name * Enter Registry Name			
✤ Runtime Protection ↔	Description *			
© Targets	Registry Description			
Remediation				
E Monitors / V	Registry Type*			
🖹 Reports	Select Kegistry Type			
A Notifications	Test Connection	Cancel		Save
🔹 Settings 🗸 🗸				

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



ACCUKN	ох	Home > Settings > Integrations > Registry > Add	AccuKnox v Q Customer
Dashboard		CWPP CSPM Registry S3 Data Source	
Inventory	*		
Issues	~	Add Registry	
• • • • • • • • • • • • • • • • • • •		Registry Name *	
Compliance	*	Enter Registry Name	
Runtime Protection	~	Description *	
Targets		Registry Description	
Remediation	*		
Monitors / Logging	~	Registry Type*	
Penorts		Select Registry Type	^)
		Nexus	
Notifications		GCR	
Settings	~	ECR	
		DockerHub	

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

Registry Name *		
my-docker-registry		
Description *		
docker hub registry		
Registry Type*		
DockerHub		~
Username *		
knoxuser		
Password *		
Test Connection	Cancel	Save

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

💿 ΑςςυΚνοχ

Image Scanning Progress • Total Registered Images 4 • 4 Scanned Images • 0 Failed to Scan • 0 Images in Queue	Image Risk Assessment Total Vulnerabilities Critical High Medium Low	 In 3.1k 315 928 926 926 	nage Security Iss Total Images	sues	0 1
Total Registered Images 4 4 Scanned Images 4 0 Failed to Scan 4 0 Images in Queue 4	Total Vulnerabilities Critical High Medium Low	3.1k T 315 928 926	Total Images	1 1	1
 4 Scanned Images 0 Failed to Scan 0 Images in Queue 	Critical High Medium Low	315 928 926	1 1 1	1 1	
	No Issue	938 15 To 0 To	otal Malware: 0 otal Sensitive Data: 0		0
FindingsSearch					
0 0 4 0 Pending In Progress Finished Failed					
Name	Registry Name Status	Qu	Jeued On	Last Progress	

How to interpret Registry scan results

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

	Home $ ightarrow$ Issues $ ightarrow$ Registry Scan		AccuKnox	∽ Q Customer √
- Dashboard	Image Scanning Progress	Image Risk Assessment	Image Securit	y Issues
E Inventory	Total Registered Images	4 Total Vulnerabilities	3.1k Total Images	1
▲ Issues	4 Scanned Images 0 Failed to Scan 0 Images in Queue	Critical High Medium Low	315 928 926 938	1 1 0
Registry Scan		Negligible No Issue	0 Total Sensitive Data	: 0
Risk-based Prioritization	Findings Scan Queue			
🛯 Compliance 🗸	Search			Add Registry
f Runtime Protection	Repositories	Security Issues	Registry Name	
◎ Targets	 accuknoxuser/knox-registry 	301 720 673 349 8	â°	
Remediation 🗸	 accuknoxuser/knox-registry 	<u>301</u> 720 673 349 8 ∯ ∘	ê °	
Monitors /	 accuknoxuser/knox-registry 	315 927 917 926 15	accuknox-registry	
Logging	 accuknoxuser/knox-registry 	315 928 926 938 15 4	accuknox-registry	

What is Risk Based Prioritization?

In this section, users will be given a comprehensive risk analysis that is found in their onboard environment. The risks that are identified are classified as High to critical based on the severity of those



risks. Users will get details about the risks associated with images, and their CVSS scores identified based on which source and severity of the risk.

	Risk Based Prioriti	zation Triv	,	Asset	~			Select Config	~ F
iventory ~	Risk factor	Ignored	Status		Tickets	Group		Scan	
isues ^	Risk Factor 🗸	Ignored	~ Status	~	Tickets	Group	~	Scan	
erabilities									
try Scan	Edit								Reset
based Prioritization		Filter	vulnerabilities b	the context of the	ir environment an	d risk factors			
ompliance ~		T INCO	Vulnerabilities with High a Critical severity	d	Vuinerabilitie "network" att	s with CVSS ack vector			
untime Protection ~	IMPORTANT	(o					IMPORTANT &	
emediation ~		A 1	High to Critica		Networ	k Attack		UNULIT	
Ionitors / Logging 🗸			3.22 K		3.1	1К			
ettings ~	Ticket configuration 🗸	Group by	~				C G	0	Ē Î
	Uulnerability	mage		Severity	Pkg Name	Ins Version	Fix Version		Status
	CVE-2020-12403	vulnerable/log4j-poc:1.0		Critical	libnssl1.1	1.1.1o-r0	1.1.1t-r0		Active 🗸
	CVE-2020-12402	/ulnerable/log4j-poc:1.0		Critical	libnssl1.1	1.1.1o-r0	1.1.1t-r0		Active ~
	CVE-2020-12403								

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

	Policies						CVE-2020-12403 log4j-poc:1.0 (D) ocker Hub)	×
Dashboard	Risk Based Prio	ritization	Data Type	~	Asset	~	CRITICAL	Based on NVD CVSSv3 9.1	Exploit Not Available
Inventory	Risk factor	Ignored		Status		Tickets	5 Mar 1994		
▲ Issues ^	Risk Factor	- Ignored	~	Status	~	Tickets	Status	Ignored	Tickets
Vulnerabilities							Active	False	0 7
Registry Scan	Edit						Severity	Ticket Configuration	ticket
Risk-based Prioritization							Critical v	Select 🗸 🧮	SAVE
			Filter vulner	abilities by the	context of the	eir environme			
II Compliance V			Vulnerabili Critical sev	ities with High and verity		Vul "ne	A flaw was found in the	way CHACHA20-POLY1305 w	as implemented in NSS in
+ Runtime Protection ~	IMPORTANT			•			Versions before 5.55. W	terr using multi-per chac	
Remediation ~			Hig	h to Critical			Installed Resource	libnss3 2:3.26.2-1.1+deb9u1	based on parent vulnerability
Monitors / Logging ~				3.22 K			Fixed Version	2:3.26.2-1.1+deb9u2	
A Cottingo	Group by	e]					Published by NVD	2021-05-27	
🗘 Settings	C. Malescekiller	1		6	-10-1		CVSS Score	NVD CVSSv3 9.1 NVD CVSSv2 6.4	
	vunerability	image		Seve	nty				
	CVE-2020-12403	vulnerable/log4j-po	c:1.0	c	ritical		Remediation	Upgrade package libns: 2:3.26.2-11+deb9u2 or	s3 to version above.
	CVE-2020-12403	vulnerable/log4j-po	c:1.0	c	ritical		Mitigation	N/A	
	CVE-2020-12403	vulnerable/log4j-po	c:1.0	. н	igh		Accept Risk	Aknowledge	
							Scan Details		
[Jacout	1-5 of 5 < >						Image	ravkishu/log4j-poc:1.0 (Docker Hub)
							Operating System	debian 9.8	



Baseline

How to create a Baseline out of a data source

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

To create a baseline, follow these steps:

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

	Home	Compliance > Baselines					solutions	 ✓ Solution ~
Dasnboard		Search		Filter by Pass or Fail 🗸	Filter by Label 🗸	Compare bas	Add basel	ne + Delete 🖃
Inventory ~		Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment
🔺 Issues 🗸 🗸		b nbv	CloudSploit	0	0	420	0/0	
🛍 Compliance 🧥		baseline-aws100723	Security Hub	1	0	0	0/0	
Baselines		Baseline-1	Prowler	0	112	0	0/0	
CSPM Executive Dashboard		mutliHost	Security Hub	0	0	0	0/0	
Runtime Protection		All	Security Hub	0	0	0	0/0	
Remediation V		Industry and regulatory standards	Security Hub	0	0	0	0/0	-
Monitors /		SACCIARS	Security Hub	0	0	0	0/0	-
Logging T	-	test	Security Hub	0	0	0	0/0	
E Reports	_	multicloud-pass	Security Hub	0	0	0	0/0	
A Notifications		manual pasa	occarty rup		-	~		
💠 Settings 🗸 🗸		CIS-1	Security Hub	0	0	0	0/0	
	Total	Count: 15					Row	is per page: 20 - C 1 >

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

	Home > Compliance > Baselines > Create Bas	eline		solutio	ns v 🗘 Solution v
Dashboard	Create Baseline				Save
Inventory ~	Name *	Source *	Label	Result	
▲ Issues 🗸	Manual	CloudSploit	~ AWS100723	X Y Pass	Fail
d Compliance 🔺	Add				
Baselines					Back
CSPM Executive Dashboard					
∳ Runtime Protection ~					
— • • • •					

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



Manual	CloudSploit		X Y Pass
Add			
		×	
	Add		
	Audit file		
	+		
	Select All		
	172 ap-south-2	+	
	172 ap-southeast-4	+	
	172 -eu-central-2	+	

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

	ba	seline-aws1	0723					(Duplicate
Deathbaard	Resu	ult		Expected Value	Tick	et(s) Created		Annotation	
Dashboard	R	esult	~	Expected Value	 ті 	cket(s) Created	~	Annotation	*)
🗉 Inventory 🗸								Edit Fields	Edit Sources
🔺 Issues 🗸 🗸									
止 Compliance 🗸	Data	Assigned Ho	ts Assigned Groups	History					
f Runtime Protection	Se	earch							
Remediation ~	П	icket Configuration	- Group by	*				\oplus \bigcirc	E 🔿 1
Monitors / Logging ·		Result Ta	gs Control	Description Info	Last Comment Tickets	Solution			
🖹 Reports		FAILED Fa	se log metric fil	This control	-	For informati			
A Notifications		FAILED Fa	se the use of th	The root use	-	For informati			
🔹 Settings 🗸 🗸		FAILED Fa	se Config shoul	This AWS co	-	For informati			
		FAILED Fa	se a log metric	Real-time m	-	For informati			
		FAILED Fa	se a log metric	Real-time m		For informati			
		FAILED Fa	se a log metric	Real-time m	-	For informati			
		FAILED Fa	se a log metric	Real-time m	-	For informati			
🕞 Log Out		FAILED Fa	se a log metric	Real-time m		For informati			
		FAILED Fa	se a log metric	Real-time m	-	For informati			

How to compare two baselines

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

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

	Ho	me > Compliance > Ba	aselines				sol	utions 🗸 🖒	Solution ~
Dashboard		Search		Filter by Pass or Fail	Click here		npare baselines 🗼 🗛	ld baseline + Delete	₿
🗉 Inventory 🗸		Name	Source	Asset failed	Asset passed	No data	Tickets	Last comment	
🔺 Issues 🗸 🗸		b nbv	CloudSploit	0	0	420	0/0		
🕯 Compliance 🧄		baseline-aws10	0723 Security Hub	1	0	0	0/0	-	
Baselines		Baselina-1	Select multiple	0	112	0	0/0	-	
CSPM Executive Dashboard		✓ mutliHost	Security Hub	°	0	0	0/0		
f Runtime Protection		All	Security Hub	0	0	0	0/0		
Remediation ~		Industry and reg	gulatory standards Security Hub	0	0	0	0/0		
■ Monitors / v		SACCIARS	Security Hub	0	0	0	0/0		
🖹 Reports		test test	Security Hub	0	0	0	0/0		
Notifications		multicloud-pass	Security Hub	0	o	0	0/0	-	
🔹 Settings 🗸 🗸		CIS-1	Security Hub	0	0	0	0/0		
	T	otal Count: 15						Rows per page: 20 👻 🤇	1 >

The comparison will look like following

Compare			
Finding	baseline-aws100723	Baseline-1	mutliHost
Ensure, a log metric filter and alarm exist for Manage	\checkmark	×	×
A, log metric filter and alarm should exist for usage o	~	×	×
Ensure, a log metric filter and alarm exist for change	~	×	×
Ensure, a log metric filter and alarm exist for AWS Co	~	×	×
Avoid, the use of the root user, Multi region CloudTra	~	×	×
Ensure, a log metric filter and alarm exist for route ta	~	×	×
Ensure, a log metric filter and alarm exist for IAM poli	~	×	×
Ensure, a log metric filter and alarm exist for VPC ch	~	×	×
Ensure, a log metric filter and alarm exist for disablin	~	×	×
Ensure, a log metric filter and alarm exist for change	~	×	×
Total Count: undefined			



Compliance

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

How to get Compliance for Cloud Assets

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



How to get Compliance for Cloud Workload

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

	Home > Runtime Security > CWPP Da	ishboard				solution	ns v 🗘 Solution v
Dashboard	CWPP Dashboard						
🗉 Inventory 🗸 🗸	~	Namespace	~			C 1	min 🗸 🚺 Last 60 days 🗸
🛦 Issues 🗸 🗸	Alerts summary			Complianc	e summary		
🖥 Compliance 🗸	Total Alerts Generated	Total Blocked Alerts		MITRE	NIST	CIS	PCI-DSS
f Runtime Protection	3439 Alerts	Blocked Alerts	2437 Audited Alerts	MITRE	3 NIST	CIS	PCI-DSS
CWPP Dashboard							
App Behavior	Compliance Alerts						
Policies	3						
📑 Remediation 🗸	1.5						
■ Monitors / v Logging v	0.75						
🖹 Reports	NIST MITRE F	CI-DSS CIS T1003	sysrv-hello 🔳 malware 🔳 crypto-mi	ning 🔳 Botnet 🗖 TeamTNT			
Notifications	L						
🕸 Settings 🗸 🗸	Namespace Severity S	Summary		Top 10 Policies	s by Alert Count		
	3			2800-			

App Behavior

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

How to interpret network graph

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

1. Install workload:

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



- 2. Showing App behavior screen in the context of the wordpress-mysql application. To see the Application Behavior user must Navigate to the **Runtime Protection->App Behavior** section. Then click on the Cluster and Namespace and pod from the filters to see the Application Behavior.
- Network Graph: This view gives the graphical representation of Ingress and Egress traffic that are occurring in the Pod. When we click on the connections, we can get a clear view of the traffic type and port details.



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

	ĸ	App Behavior						
- Dashboard		azure-staging ~	wordpress × v m	ysql-6c6 X ~	rated Whitelisted	Application Behavio	List	Graph 🚺 All 🗸
Inventory				Auto Gene	Taled Whiteiisled		u	
▲ Issues	-	File Observability Process	Observability Network Observabi	lity				Show Aggregated View
Compliance	~	Last Update	Process	File Path Accessed	Container	Occurance	Status	I. I
Runtime Protection	~	02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/Ame	er mysql	1	Allow	Details 🗸
CWPP Dashboard		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/Ame	ri mysql	1	Allow	Details 🐱
App Behavior		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/Ame	er mysql	1	Allow	Details 🐱
Policies		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/Ame	er mysql	1	Allow	Details 🐱
Targets		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/Canada/E	a: mysql	1	Allow	Details 🗸
Remediation	~ I	02/17/2023 08:47 AM	/usr/sbin/mysqld	/var/lib/mysql/mysql/proc.MYI	mysql	1	Allow	Details 🐱
Monitors / Logging	~	02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/America/F	te mysql	1	Allow	Details 🗸
Reports		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/GMT	0 mysql	1	Allow	Details 🗸
A Notifications		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/posix/Ame	er mysql	1	Allow	Details 🐱
🔹 Settings		02/17/2023 08:47 AM	/usr/bin/mysql_tzinfo_to_sql	/usr/share/zoneinfo/right/Euro	p mysql	1	Allow	Details 🐱

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

	App Behavior						
Dashboard	azure-staging ~	wordpress × v my	rsql-6c6 × v			List	Graph 🚺 All 🗸
🗉 Inventory 🗸 🗸			A	uto Generated P	Process Observability		
🛆 Issues 🗸 🗸	File Observability Process	Observability Network Observabil	ity				
Compliance 🗸	Last Update	Process	File Path Accessed	Container	Occurance	Status	
Runtime Protection	02/17/2023 08:47 AM	/bin/dash	/usr/sbin/mysqld	mysql	1	Allow	Details 🐱
CWPP Dashboard	02/17/2023 08:47 AM	/bin/bash	/bin/date	mysql	7	Allow	Details 🐱
App Behavior	02/17/2023 09:52 AM	/bin/bash	/bin/ls	mysql	8	Allow	Details 🗸
Policies	02/17/2023 08:47 AM	/bin/bash	/usr/sbin/mysqld	mysql	1	Allow	Details 🗸
) Targets	02/17/2023 08:47 AM	/usr/bin/containerd-shim-runc	· /usr/sbin/mysqld	mysql	1	Allow	Details 🗸
Remediation 🗸	02/17/2023 15:31 PM	/bin/bash	/bin/rm	mysql	1	Allow	Details 🐱
Monitors / 🗸	02/17/2023 08:47 AM	/bin/bash	/bin/sleep	mysql	1	Allow	Details 🐱
) Reports	02/17/2023 08:47 AM	/bin/bash	/bin/sed	mysql	1	Allow	Details 🐱
Notifications	02/17/2023 08:47 AM	/bin/bash	/usr/bin/mysqladmin	mysql	1	Allow	Details 🐱
Settings 🗸	02/17/2023 08:47 AM	/bin/bash	/usr/bin/mysql	mysql	4	Allow	Details 🐱

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

azure-staging	wordpress	. × • m	ysql-6c6 × ∨			List Graph	🔄 🚺 🚺 🔪
			Auto Generated	Network Obse	ervability		
File Observability Pr	ocess Observability	Network Observabil	ity				
File Observability Pr	ocess Observability	Network Observabil	Dest. POD/SVC/IP Port	Container	Occurance	Status	
File Observability Pr Last Update 02/17/2023 08:47 AN	Source Command	Network Observabil	ity Dest. POD/SVC/IP Port pod/wordpress-84dl 3306	Container	Occurance	Status	 Details 🗸

How to see App Behavior Telemetry

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

	Process Observability	Network Observability				how Aggregated Viev
ast Update	Process	File Path Accessed	Container	Occurrence	Status	
06/27/2023 17:51 F	PM /usr/bin/apt	/usr/	mysql	6	Allow	Hide 🔺
ld": "0000000000	000000000000000",					
updated_time": 16	87868467,					
DeploymentName": "",	": "mysql",					
pod_name": "mysc	ql-76ddc6ddc4-h47hv",					
a a ma a a a a a a ll. Il. una a	de re e e euro ell'					
namespace": "wor abels": "app=mys	dpress-mysql", ql",					
namespace": "wor labels": "app=mys source": "/usr/bin/	dpress-mysql", ql", apt", 					
namespace": "worn labels": "app=mys source": "/usr/bin/ container_name": ' container_id": "e10	dpress-mysql", ql", apt", "mysql",)d5edb62ac2daa4eb9a2'	146e2f2cfa87b6a5f30bd3ae20)fc91a2bf4d727747",			
namespace": "wor labels": "app=mys source": "/usr/bin/ container_name": container_id": "e10 ip": "",	dpress-mysql", ql", apt", "mysql",)d5edb62ac2daa4eb9a2' "	146e2f2cfa87b6a5f30bd3ae20)fc91a2bf4d727747",			
namespace": "wor labels": "app=mys source": "/usr/bin/. container_name": container_id": "e10 (p": "", destination": "/usr, destination_label".	dpress-mysql", ql", apt", "mysql", 0d5edb62ac2daa4eb9a2" "", "".	146e2f2cfa87b6a5f30bd3ae20	fc91a2bf4d727747",			
namespace": "worn labels": "app=mys source": "/usr/bin/. container_name": container_id": "e1C0 p": "", destination": "/usr, destination_label": destination_names	dpress-mysql", ql", apt", "mysql",)d5edb62ac2daa4eb9a2' /", ;"", space": "",	146e2f2cfa87b6a5f30bd3ae20	fc91a2bf4d727747",			
namespace": "worn labels": "app=myss source": "/usr/bin/. container_name": container_name": container_id": "e1C "p": "", destination_label": destination_names count": 6, action": "Allow"	dpress-mysql", ql", apt", "mysql",)d5edb62ac2daa4eb9a2' '", "", space": "",	146e2f2cfa87b6a5f30bd3ae20	fc91a2bf4d727747",			



• **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

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 🔨
Id": "6479820c3d	l63aeb2d1f0a112",					
'Id": "6479820c3d 'updated_time": 16	163aeb2d1f0a112", 585684643,					
'Id": "6479820c3d 'updated_time": 16 'cluster_name": "a	163aeb2d1f0a112", 585684643, ks-demo-prod",					
'Id": "6479820c3d 'updated_time": 16 'cluster_name": "a 'DeploymentName	163aeb2d1f0a112", 585684643, ks-demo-prod", ": "mysql", el, 76d66dda4, b47bu",					
"Id": "6479820c3d "updated_time": 16 "cluster_name": "a 'DeploymentName 'pod_name": "mys 'namespace": "woj	163aeb2d1f0a112", 585684643, ks-demo-prod", *": "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql",					
'Id": "6479820c3d 'updated_time": 16 'cluster_name": "a 'DeploymentName 'pod_name": "mys 'namespace": "woi 'labels": "app=mys	I63aeb2d1f0a112", 585684643, ks-demo-prod", s": "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sql",					
'Id": "6479820c3d 'updated_time": 16 'cluster_name": "a 'DeploymentName 'pod_name": "mys 'namespace": "woi 'labels": "app=mys 'source": "/bin/bas	163aeb2d1f0a112", 385684643, ks-demo-prod", ": "mysql", ql-76dc6ddc4-h47hv", rdpress-mysql", sql",					
"Id": "6479820C3d "updated_time": 16 "cluster_name": "a "DeploymentName "pod_name": "mys "namespace": "woi "labels": "app=mys 'source": "/bin/bas 'container_name":	I63aeb2d1f0a112", 85584643, ks-demo-prod", ""mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sql", "mysql",					
'ld": "6479820c3d 'updated_time": 16 'cluster_name": "a 'DeploymentName 'pod_name": "mys 'namespace": "wov 'labels": "app=mys 'source": "/bin/bas 'container_id": "e1 'container_id": "e1 'container_id": "e1	I63aeb2d1f0a112", 85584643, ks-demo-prod", ** "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sql", "mysql", 0d5edb62ac2daa4eb9a	2146e2f2cfa87b6a5f30bd3ae20	Dfc91a2bf4d727747",			
Id": "6479820c3d updated_time": 16 Cluster_name": "6 DeploymentName 'pod_name": "mys 'namespace": "woi Iabels": "app=mys 'source": "/bin/bas 'container_name": "container_id": "e1 'ip": "", 'destination": "/bin	I63aeb2d1f0a112", 85584643, ks-demo-prod", ": "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sql", "mysql", 0d5edb62ac2daa4eb9a. h/sed"	2146e2f2cfa87b6a5f30bd3ae2(Dfc91a2bf4d727747",			
Id": "6479820C3d lupdated_time": 16 cluster_name": "a DeploymentName pod_name": "mys 'namespace": "woi labels": "app=mys 'source": "/bin/bas container_name": 'container_name": 'container_id": "e1 ip": ", 'destination": "/bin /destination_label"	I63aeb2d1f0a112", 85584643, ks-demo-prod", *": "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sh", "mysql", Od5edb62ac2daa4eb9a. 1/sed", *"."	2146e2f2cfa87b6a5f30bd3ae2(Dfc91a2bf4d727747",			
"Id": "6479820c3d 'updated_time": 1d 'cluster_name": "a 'DeploymentName 'pod_name": "moy 'abales": "wop 'abales": "app=mys 'source": "voin'abales" 'container_name": 'container_id": "e1 'ip": "", 'destination_label" 'destination_name	I63aeb2d1f0a112", 385684643, ks-demo-prod", ** "mysql", ql-76ddc6ddc4-h47hv", rdpress-mysql", sh", "mysql", 0d5ed62ac2daa4eb9a h/sed", *****, sinspace": "",	2146e2f2cfa87b6a5f30bd3ae20	Dfc91a2bf4d727747",			

• 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

Y 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	Details 🗸
07/06/2023 15:47	PM /usr/bin/mysql	egress 🖈	svc/wordpress 3306	mysql	2	Allow	Hide 🔺
In Consolver of Market Consolver of Market Consolver of Market Consolver	sb8638674, i": "mysql", qi-76ddc6ddc4-h47hv", rdpress-mysql", imysql", i", imysql", 0d5edb62ac2daa4eb9a ss", : "", ispace": "wordpress-mys	2146e2f2cfa87b6a5f30t sql",	bd3ae20fc91a2bf4d727747",				



Runtime Protection w/ Policy Management

How to understand discover policies

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

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



 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 autodiscovered policies.






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





How to understand Hardening policies

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

- Let us understand by taking a use-case example Disallowing any binaries execution to prevent from RCE Vulnerability
- 1. Select your cluster and namespace from this Policies screen. We will be getting a list of hardening policies for the selected Namespace.

Dashboard		Policies					Create Policy +
Inventory	¥	Workloads	Cluster	Namespace	Policy Type		
▲ Issues	•	K8s ~	Cluster(1) X ~	Namespace(1) X ~	Policy Type v		
Compliance	~						
Runtime Protection	^	Search All (38) Discov	ered (29) Changed (0)	Active (5) Inactive (4)	Pending (0) Ignored (0)	> Ø Ignore	Apply
CWPP Dashboard		-					
App Behavior		Policy Name	Catego	ory Status	Clusters Namespace	Selector Labels	Tags
Policies		KubeArmor	Discov	ered Inactive	azure-staginç wordpress-mysql	app=wordpress	None
Targets		Aarden-word KubeArmor	dpress-trusted-cert-mo Discov	ered Inactive	azure-staginç wordpress-mysql	app=wordpress	None
Remediation	~ i	KubeArmor	dpress-shell-history-mc Discov	ered Inactive	azure-staginç wordpress-mysql	app=wordpress	None
Monitors /	•	L 🛞 harden-word KubeArmor	dpress-k8s-client-tool-f Discov	ered Inactive	azure-staginç wordpress-mysql	app=wordpress	None
		Harden-word KubeArmor	dpress-write-etc-dir Discov	ered Inactive	azure-staginç wordpress-mysql	app=wordpress	None

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



	harden-wordpress-pkg-mngr-exec
<u> </u>	KubeArmorPolicy Updated 17days ago
YAI	ML 🖉 Edit 🗍 Clone 🛓 Download
0	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	namesnace: wordpress-pkg-mngr-exec
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
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: /usc/hin/rom
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: /usc/hin/makenka
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: /spin/yaourt
40	- 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 50	- 51-4
51	- NIST 800-53 SI-4
52	



3. Select this policy and click on the apply option

	Search		Apply
Dashboard	All (38) Discovered (29) Changed (0) Active (5) Inactive (4) Pending (0) Ignored (0) Hardening (0)	Ø Ignore ☐ Delete	() Make Inactive
Inventory ~	Policy Name Category Status Clusters Namespace Selector Labels	Tags	
🔺 Issues 🗸 🗸	barden-wordpress-write-under-bin: KubeArmor biscovered inactive azure-staging wordpress-mysql app=wordpress	None	:
👍 Compliance 🗸	barden-wordpress-trusted-cert-mo Discovered Inactive azure-staging wordpress-mysql app=wordpress	None	:
Runtime Protection	Aarden-wordpress-shell-history-mc Discovered Inactive azure-staging wordpress-mysql app=wordpress	None	:
CWPP Dashboard	Aarden-wordpress-k8s-client-tool-t Discovered Inactive azure-staging wordpress-mysgl app=wordpress	None	:
App Behavior	barden-wordpress-write-etc-dir KubeArmor Discovered Inactive azure-staging wordpress-mysgl app=wordpress	None	:
Policies	Aarden-wordpress-write-under-dev Discovered Inactive azure-staging wordpress-mysql app=wordpress	None	:
Targets	barden-wordpress-file-integrity-mo Discovered Inactive azure-staging wordpress-mysql app=wordpress	None	:
Monitors /	barden-wordpress-cronjob-cfg Discovered Inactive azure-staging wordpress-mysgl app=wordpress	None	:
Logging V	barden-wordpress-nkg-mngr-exec Discovered Inactive azure-staginc wordpress-mysql app=wordpress	None	:
Reports	barden-wordpress-remote-file-cop: KubeArmor biscovered liscovered inactive azure-staging wordpress-mysgl app=wordpress	None	:
A Notifications			

4. After applying policy goes into active state.

	Home > Runtime Security > Policies	AccuKnox ~	Customer ∨
Dashboard	Policies	Crea	te Policy +
Inventory ~	Workloads Cluster Namespace Policy Type	_	
🔺 Issues 🗸 🗸	K8s Cluster(1) X Namespace(1) X Policy Type		
🛍 Compliance 🗸			
f Runtime Protection	Search		Apply
CWPP Dashboard	All (38) Discovered (28) Changed (0) Active (6) Inactive (4) Pending (0) Ignored (0) Hardening (0)	Ignore 🗍 Delete	也 Make Inactive
App Behavior	Policy Name Category Status Clusters Namespace Selector Labels	Tags	
Policies	KubeArmor Applied about a secol Active azure-staging wordpress-mysql app=wordpress	None	:
© Targets	audit-mysq.(y3) Custom KubeArmor Appied7days ago • Active azure-staging wordpress-mysql app=mysql	None	:
Remediation 🗸	the Amore A set of the active ac	None	:
Monitors / Logging ~	the Amore And Amore And Amore A	None	:
E Reports	Image: mysql-audit-policy.(v1) Custom • Inactive azure-staging wordpress-mysql app=mysql	None	:
A Notifications	Ksp-wordpress-block-process.(v2) Custom Applied 10days ago Active azure-stagin; wordpress-mysql app=wordpress	None	:



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

How to Audit application and get alerts for that

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

Ø	ksp-mysql-audit-dir (v3) KubeArmorPolicy © Created a month ago.			×
Ø	The YAML is valid			
YAI	ML	🖍 Edit	Clone	
1	apiVersion: security.kubea	armor.co	om/v1	
2	kind: KubeArmorPolicy			
3	metadata:			
4	name: ksp-mysql-audit-di	ir		
5	namespace: wordpress-mys	sql		
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	<pre>message: mysql-audit-pol</pre>	licy		

- 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 > Ru	ntime Security > Policies					partner	demo
Polic	ies						
K8s	✓ aks-demo-prod × × ✓	wordpress-my	sql × × ×	Policy Type	~	Active ×	x ~
Sear	ch	Audit	based policy is	applied from			
All (1) Discovered (0) Hardening (0)	Accu Custom (1)	Knox SaaS			Ø Ignore	📋 Delete
	Policy Name	Category	Status 💙	Clusters	Namespace	Selector La	abels
	ksp-mysql-audit-dir (v3) KubeArmor	Custom Applied a few seco	Active	aks-demo-prod	wordpress-mys	ql 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.





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



When do we say policies are stable?

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



*	autopol-egress-3275896150 NetworkPolicy © Created 2 months ago.
\sim	The YAML is valid months. This is an example of
YA	ML Stable policy 🛃 Download
0	Discovered / Hardening Policies are not editable. To modify, first clone this policy then convert into custom 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; mysqi
20	- ports:
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 did not get any updates or changes.

What if something changes in Application??

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



	Discovered (Changes Available 2months ago) © Created 2 months ago.	×
Upda	ted 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.



5	8	<pre>path: /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0</pre>
5	9	- fromSource:
6	0	- path: /usr/sbin/apache2
6	1	path: /usr/lib/x86_64-linux-gnu/libuuid.so.1
6	2 -	+ - fromSource:
6	3 -	+ - path: /bin/bash
6	4	<pre>+ path: /root/.bash_history</pre>
6	5	+ - fromSource:
6	6 -	+ - path: /bin/bash
6	7 -	+ path:/dev/pts/0
6	8 -	+ - fromSource:
6	9 -	+ - path: /bin/ls
7	0 -	+ path: /etc/ld.so.cache
7	1 -	+ - fromSource:
7	2 -	+ - path: /bin/ls
7. 7.	2 -	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0</pre>
7: 7: 7:	2 - 3 - 4	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process:</pre>
7: 7: 7: 7: 7:	2 - 3 - 4	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths:</pre>
7: 7: 7: 7: 7: 7: 7:	2 - 3 - 4 5 6	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2</pre>
7: 7: 7: 7: 7: 7: 7: 7:	2 - 3 - 4 5 6 7	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash</pre>
7: 7: 7: 7: 7: 7: 7: 7: 7:	2 - 3 - 4 5 6 7 8	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: path: /usr/sbin/apache2 path: /bin/bash fromSource:</pre>
7: 7: 7: 7: 7: 7: 7: 7: 7: 7: 7:	2 - 3 - 5 - 7 - 9 -	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash - fromSource: - path: /bin/bash</pre>
7: 7: 7: 7: 7: 7: 7: 7: 7: 8:	2 - 3 - 5 6 7 8 9 0	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: path: /usr/sbin/apache2 path: /bin/bash fromSource: path: /bin/bash path: /bin/ping</pre>
7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 9. 8. 8.	2 - 3 - 4 5 6 7 8 9 0 1	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash - fromSource: - path: /bin/bash path: /bin/ping - fromSource:</pre>
7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 8. 8. 8.	2 - 3 - 5 - 6 - 7 - 8 - 9 - 0 - 1 - 2 -	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash - fromSource: - path: /bin/bash path: /bin/ping - fromSource: - path: /bin/bash</pre>
7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 8. 8. 8. 8. 8. 8. 8.	2 - 3 - 5 - 6 - 7 - 8 - 9 - 0 - 1 - 2 - 3 -	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash - fromSource: - path: /bin/bash path: /bin/ping - fromSource: - path: /bin/bash path: /usr/sbin/apache2</pre>
7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7. 7	2 - 3 - 5 - 6 - 7 - 8 - 9 - 0 - 1 - 2 - 3 - - 3 -	<pre>+ - path: /bin/ls + path: /usr/lib/x86_64-linux-gnu/libpcre2-8.so.0 process: matchPaths: - path: /usr/sbin/apache2 - path: /bin/bash - fromSource: - path: /bin/bash path: /bin/ping - fromSource: - path: /bin/bash path: /usr/sbin/apache2 - path: /bin/ping</pre>

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



×

	Discovered (Changes Available 2months ago) Update
Upda	ted 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

- After the user clicks the update, the policy will be updated.
- How to create a custom Policy
- File restriction Policy
- To create a file restriction based custom policy user must navigate to Runtime Protection->Policies section.
- To create the policy user needs to click on the create policy option

🙆 ACCUKNOX

Home > Ru	Intime Security > Policies					partnerdemo	~ 🗘 Partner
Polic	cies						Create Policy +
K8s	aks-demo-prod x X V	Namespace	~) (P	olicy Type 🛛 🗸	Status	~	
Sear	ch						Activate
All (2	249) Discovered (49) Hardening	(195) Custom	(5)			🖉 Ignore 📋 Delete	U Make Inactive
	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
	WbeArmor	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=mysql-malac	None
	With Report Street Report Repo	Discovered	 Inactive 	aks-demo-prod	default	app.kubernetes	+2 V None
	Autopol-egress-3275896150 Kubernetes Network	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	None
_	autopol-ingress-3061100860						

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

Policy Editor Tool									
KubeArmor Policy Network	Policy					1	K8S C	D VM	·
Policy Name *				÷		Uploa optio	ad Yam n		Upload YAML ± Save to Workspace
Enter Policy Name									The created YAML is invalid
Cluster*									1 apiVersion: security.kubearmor.com,
Select Cluster	×).								
Namespace*									
Select Namespace	· · ·	Cre	eating po	o <mark>licy</mark> fror	n editor	tool option	1 -		
Default O Node									
Selector Labels*									
Select Labels	~ .								
Tags									
Select Tags	~) [•]						+ -		
							-		

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

Home $>$ Runtime Security $>$ Policies $>$ Polic	zy Editor		partnerdemo v 🗘 Partner v
Policy Editor Tool			
KubeArmor Policy Network Policy		K8S 🍞 VM	
			Upload YAML 🛓 Save to Workspace 🍙
() mysql-audit-dir wordpress-mysql Cluster: aks-demo-prod Labels: epp-mysql Message: mysql-audit-policy	Rules Drag and Drop the properties below Process + File + Network +	File (1) + X Edit Delete /var/lib/mysql/ IsDirectory IsRecursive	The created YAML is valid apiVersion: security.kubearmor.com kind: KubeArmorPolicy metadata: name: mysql-audit-dir namespace: wordpress-mysql spec: severity: 5
		Unable to view this rule	8 selector: 9 matchLabels: 10 app: mysql
		action Unable to view this rule 	12 matchDirectories: 13 - dir: /var/lib/mysql/ 14 recursive: true 15 action: Audit
		+ - 3	<pre>16 message: mysql-audit-policy 17</pre>

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

ome > R	untime S	Security >	Policies	> Policy	Editor					partnerdemo 🗸 🗘 Partner y
Polic	y Ed	litor T	ool							
KubeAr	mor Po	licy N	letwork	Policy					K8S 🌒 VM	
	32					1	23	2		Upload YAML 2 Save to Workspace 🕼
<pre>{} mys</pre>	ql-audit	t-dir		1	Rules Drag and	Drop the p	roperties belo	ow	File (1) + X	The created YAML is valid
Cluster:	s-mysqi aks	s-demo-proc	d		Proces	S		+	/var/lib/mysql/	1 apiversion: security.kubearmor.com □ ± 2 kind: KubeArmorPolicy
Labels:	ар	pp=mysql			File			+	IsDirectory IsRecursive	3 metadata: 4 name: mysql-audit-dir
Message:	my	sql-audit-po	olicy		Netwo	rk		+		6 spec:
									severity Unable to view this rule	7 severity: 5 8 selector: 9 matchLabels:
									action	10 app: mysql 11 file:
1.4		-							Unable to view this rule	 13 - dir: /var/lib/mysql/ 14 recursive: true
		023		020		1	23	ς.		<pre>15 action: Audit 16 message: mysql-audit-policy 17</pre>
									+	**

• After that policy will be saved to the workspace.



) mys	sql-audit	-dir		1	Rules Drag and I	Drop the pr	operties belo	v	File (1)		() F	dit)	+ Dele	×	The created YAML is valid
luster:	aks	-demo-prod			Process	5		+	/var/li	b/mys	ql/				1 apiVersion: security.kubearmor.com 2 kind: KubeArmorPolicy
abels:	ар	p=mysql			File			+	IsDirec	tory	IsRecursive				3 metadata:
lessage	e: my	sql-audit-poli	су		Network	ć		+							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
												+	-	0	17 message: mysql-audit-policy
				D all											
Create	e Policy -	+		Polic	y is save		orkspace								Eilo Bulo
	,					П									
_ F	Policy Na	ame	Poli	су Туре	Cluster	s V	Names	pace	Workspa	ace	Created	l At	I	_	 In the file section, there are 2 types of match matchPaths and matchDirectories. You can define specific executables using matchPatl or all executables in specific directories using
r	mysql-au	ıdit-dir	Kub	eArmor	aks-de	mo-proc	d wordpi	ess-my	/sc partnerc	demo	07/20/2	023 1	18:2	:	matchDirectories. In each match, there are three options:
- H	ksp-mys	ql-audit-di	r Kub	eArmor	aks-de	mo-proc	d wordpi	ess-my	/sc partnerc	demo	06/15/2	023 2	22:3	:	 ownerOnly: (static action: allow owner only; otherwise block all) If this is enabled, the owners of the executable(s) defined with

- 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

Home > Ru	Intime Security > Policies					partnerdemo	✓
Polic	cies						Create Policy +
K8s	✓ aks-demo-prod × × ✓	Namespace	e v P	olicy Type 🛛 🗸	Status	~	
Sear	ch						Activate
All (2	249) Discovered (49) Hardening	(195) Custom	n (5)			🖉 Ignore 📋 Delete	U Make Inactive
	Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags
	WubeArmor	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=mysql-malac	None
	WubeArmor	Discovered	 Inactive 	aks-demo-prod	default	app.kubernetes	+2 V None
	Autopol-egress-3275896150 Kubernetes Network	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	None
	autopol-ingress-3061100860 Kubernetes Network	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	None



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

e > Runtime Security > Policies > Po	blicy Editor					partnerdemo - Q Partr
olicy Editor Tool						
IbeArmor Policy Network Polic	cy					
Policy Name *						Upload YAML 1 Save to Workspace
Enter Policy Name						8 The created YAML is invalid
Cluster*						1 apiVersion: networking.k8s.io/v1
Select Cluster	× .					
Namespace*						
Select Namespace	· ·					
Selector Labels						
Selector Labels	· ·					
	Save					
				+ -	- 0	
Create Policy +						Policy Metadata

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

Home $>$ Runtime Security $>$ Policies $>$ Polic	y Editor			partnerdemo v 🗘 Partner v
Policy Editor Tool				
KubeArmor Policy Network Policy	_			
. Rules Drag and Drop the properties below		Policy Name* autopol-ingress-paagilbjlwzidtq		Upload YAML 1 Save to Workspace (
Ingress Egress		Cluster*	· ·	1 apiVersion: networking.k8s.io/v1 ☐ 2 kind: NetworkPolicy
. ipBlock	+ .	aks-demo-prod v	· ·	<pre>3 metadata: 4 name: autopol-ingress-paagilbjlwzidtq 5 namecnace: dwwa</pre>
podSelector	+ +	dvwa ~	· · ·	6 spec: 7 ingress:
		Selector Labels app=dvwa-mysql ×	1	 - port: 3306 - port: 3307 1 podtelector:
		tier=backend × × ×	1	2 matchLabels: 3 app: dvwa-mysql 4 tier: backend
		Save	· · · 1 + - : 1	5 policyTypes: 6 - Ingress 7

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

olio	cy Ed	itor To	loc								
204	rmor Poli	iov N	otwork B	oliov							
JEA			etwork P	Jicy							
	Rule	s			•	Policy Name *		۰ ۱			Upload YAML ± Save to Workspace
	Drag a	nd Drop the	properties	below		autopol-ingress-paagilbj	jlwzidtą			0	The created YAML is valid
	h	ngress	Eg	ress		Cluster*				1	apiVersion: networking.k8s.io/v1
	ipBlo	ck		+		aks-demo-prod	~	.		2	metadata:
						Namespace*				4	<pre>name: autopol-ingress-paagilbjlwzidtq namespace: dvwa</pre>
	podS	elector		т		Ramespace				6	spec:
	name	espaceSe	elector	+		dvwa	~			7	ingress: - ports:
	-				4.	Selector Labels				9	- port: 3306
						app=dvwa-mysql ×				10	- port: 3307
						tier=backend ×	× v			11	matchLabels:
				100	2.52				5	13	app: dvwa-mysql
										14	tier: backend
							Save			15	policyTypes:
										10	- Ingress

• After that policy will be saved to the workspace.

	Rules Drag and Drop the	properties be	elow		{} auto	pol-in	gress-paa	gilbjlwz	/) .				Upload YAML ± Update Policy
ю к	Ingress ipBlock	Egre	ess +	* •	Cluster: Namespa	al ce: d	ks-demo-pro vwa app=dywa-my	od		•			•	1 apiVersion: networking.k8s.io/v1 2 kind: NetworkPolicy 3 metadata: 4 name: autopol-ingress-paagilbjlwzidtq
	podSelector namespaceSe	lector	+		Labels:	6	tier=backend) .			·	5 namespace: dvwa 6 spec: 7 ingress: 8 - ports:
					×					•			•	9 - port: 3306 10 - port: 3307 11 podSelector: 12 matchlabels:
				•										13 app: dvwa-mysql 14 tier: backend 15 policyTypes:
											+	-	13	16 - Ingress 17
Cre	ate Policy +		Policy i	s save	d to Work	space								Policy Metadata Mandatory Fields: As with all other Kubernet
	Policy Name	P	olicy Type	Clus	ters	Nam	espace	Worksp	bace	Create	d At			config, a NetworkPolicy needs apiVersion, kin and metadata fields.
	autopol-ingres	s-p Ne	etworkPolicy	/ aks-	demo-prod	dvwa	a	partner	demo	07/20/	2023 1	19:2	:	PodSelector: Each NetworkPolicy includes a podSelector which selects the grouping of pods to which the policy applies. The example policy selects pods with the label "role=db". A empty podSelector selects all pods in the namespace.

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



> Ru	intime Se	curity > Policies					partnerdemo	~ Q	Partnei
Polic	cies							Create Policy	+
K8s	*	aks-demo-prod × × ~	Namespace	~ P	olicy Type 🗸 🗸	Status	~		
								Activate	
Searc	ch							Activate	P
Searo All (2	rch 249)	Discovered (49) Hardening	g (195) Custom ((5)			🖉 Ignore 📋 Delete	Make Inactive	e
Searce All (2	249) Policy	Discovered (49) Hardening Name	g (195) Custom (Category	(5) Status	Clusters	Namespace	⊘ Ignore ☐ Delete Selector Labels	Make Inactive Tags	
Searc	ch 249) Policy	Discovered (49) Hardening Name autopol-system-2096115234 KubeArmor	g (195) Custom (Category Discovered	(5) Status • Inactive	Clusters I	Namespace	 Ignore Delete Selector Labels app=mysql-malac 	U Make Inactive	ine
All (2	ch 249) Policy	Discovered (49) Hardening Name autopol-system-2096115234 KubeArmor autopol-system-1021014936 KubeArmor	g (195) Custom (Category Discovered Discovered	(5) Status • Inactive • Inactive	Clusters	Namespace wordpress-mysql default	 Ignore Delete Selector Labels app=mysql-malac app.kubernetes 		ne
Searc	ch 249) Policy () () () ()	Discovered (49) Hardening Name autopol-system-2096115234 KubeArmor autopol-system-1021014936 KubeArmor autopol-egress-3275896150 Kubernetes Network	g (195) Custom (Category Discovered Discovered Discovered	(5) Status • Inactive • Inactive • Inactive	Clusters	Namespace wordpress-mysql default wordpress-mysql	Ignore Delete Selector Labels app=mysql-malac app.kubernetes app=wordpress	C Make Inactive Tags No +2 No No	e me me

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

Policy						K8S		1
					Upl	oad Yam		Upload YAML 1 Save to Workspace
					opt			S The created YAML is invalid
		<u>.</u>						1 apiVersion: security.kubearmor.com,
~								
1								
~ ·-	Cre	ating po	o <mark>licy</mark> fror	n editor	tool opti	on ·		
~ .						э.		
							•	
			v · · · · · · · · · · · · · · · · · · ·	Creating policy from	Creating policy-from editor	· ·	Upload Yam option Creating policy from editor tool option	Upload Yaml option Creating policy from editor tool option

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

olicy E	ditor 1	Fool	> Policy E	aitor					partnerdemo V V Partne
IbeArmor P	olicy I	Network F	Policy					K8S 🕕 VM	
{} words	press-bloci	<-process		Rule	IS and Drop the	properties below	i	Process (2) + X	Upload YAML 1 Save to Workspace
Cluster:	mysql aks-dem app-wo	o-prod rdpress		Proc	ess		+	/usr/bin/apt	1 apiVersion: security.kubearmor.com
Message:	apt proce	ess block		Netv	vork		+	/usr/bin/apt-get	4 name: wordpress-block-process 5 namespace: wordpress-mysql 6 spec:
								severity Unable to view this rule	7 severity: 3 8 selector: 9 matchLabels:
								action	<pre>10 app: wordpress 11 process: 12 matchPaths:</pre>
								Unable to view this rule	 13 - path: /usr/bin/apt 14 - path: /usr/bin/apt-get 15 action: Block
								+ - 0	16 message: 'apt process block ' 17

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

e)	> Runtime S	Security >	Policies >	Policy Edi	tor					partnerdemo 🗸 🗘 Partne
0	licy Ec	litor 1	lool							
ibe	eArmor Po	olicy I	Network P	Policy					K8S 🌒 VM	
8						2				Upload YAML 1 Save to Workspace
	{} wordp wordpress-	ress-bloci mysql	k-process		Rul	es and Drop the	properties be	Now	Process (2) + X	The created YAML is valid
	Cluster:	aks-dem	o-prod		Pro	Cess		+	/usr/bin/apt	1 apiVersion: security.kubearmor.com 🗋 : 2 kind: KubeArmorPolicy
	Message:	app-wo	ess block		Net	work		+	/usr/bin/apt-get	<pre>3 metadata: 4 name: wordpress-block-process 5 namespace: wordpress-mysal</pre>
	10						1			6 spec: 7 severity: 3
	20	2				2	÷	2	Unable to view this rule	<pre>8 selector: 9 matchLabels: 10 ann: wordpress</pre>
									action	11 process: 12 matchPaths:
						·			Unable to view this rule	 path: /usr/bin/apt path: /usr/bin/apt-get
				27			÷.			15 action: Block 16 message: 'apt process block ' 17
									T - U	<u> </u>

• After that policy will be saved to the workspace.



	C) word	wordpre	ss-block-p	rocess	1	Rules Drag and Drop	the properties	below	Proc	ess (2)	Æd	+ lit) (11 Del	×	Upload YAML 1
	Clus	ter:	aks-demo-p	rod		Process		+	/u	sr/bin/apt				
	Labe	ls:	app=wordpr	css		File		+			Ed	lit) (Total Del	ete)	1 apiVersion: security.kubearmor.com
	Mess	age:	apt process	block		Network		+	/u	sr/bin/apt-ge	et 🤇			3 metadata:
	_				_	Hetholik								4 name: wordpress-block-process
														5 namespace: wordpress-mysq1 6 spec:
					1		1							7 severity: 3
														8 selector:
							1.1							9 matchLabels:
														10 app: wordpress
														12 matchPaths:
1						1	1							13 - path: /usr/bin/apt
														14 - path: /usr/bin/apt-get
														15 action: Block
												.		16 message: apt process block
												т -		· · ·
				Policy S	aved t	o Workspa	ce							
Creat	te Policy	+				Π								Process Rule
_						<u>الج</u>								In the process section, there are 2 types of
	Policy Na	ame	P	olicy Type	Clus	ter	Names	space	Works	space	Created	d At		matches: matchPaths and matchDirectories. You can define specific executables using
	wordpre	ss-bloc	k K	lubeArmor	aks-	demo-prod	wordp	ress-mys	c partn	erdemo	07/20/2	2023 18	:4	directories using matchDirectories. In each match, there are three options:
	mysql-au	ıdit-dir	k	lubeArmor	aks-	demo-prod	wordp	ress-mys	c partn	erdemo	07/20/2	2023 18	:2 🚦	 ownerOnly: (static action: allow owner only; otherwise block all) If this is enabled, the

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

root@mysql-	6c6fcdccf-sk5	x2:/# cd sbin				
root@mysql-	6c6fcdccf-sk5	x2:/sbin# ls				
agetty	dumpe2fs	fsck.ext2	installkernel	mkfs.cramfs	pivot_root	swapoff
badblocks	e2fsck	fsck.ext3	isosize	mkfs.ext2	raw	swapon
blkdiscard	e2image	fsck.ext4	killall5	mkfs.ext3	resize2fs	switch_root
blkid	e2label	fsck.minix	ldconfig	mkfs.ext4	runuser	tune2fs
blockdev	e2undo	fsfreeze	logsave	mkfs.minix	sfdisk	unix_chkpwd
cfdisk	fdisk	fstab-decode	losetup	mkhomedir_helper	shadowconfig	unix_update
chcpu	findfs	fstrim	mke2fs	mkswap	start-stop-daemon	wipefs
ctrlaltdel	fsck	getty	mkfs	pam_tally	sulogin	zramctl
debugfs	fsck.cramfs	hwclock	mkfs.bfs	pam_tally2	swaplabel	
root@mysql-	6c6fcdccf-sk5	x2:/sbin# touc	h mks2			
root@mysql-	6c6fcdccf-sk5	x2:/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@mysal-	6c6fcdccf-sk5	x2:/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.

Dashboard	Policies	Create Policy +
Inventory ~	Workloads Select Policy Type to filter	
🔺 Issues 🗸 🗸	Select Clusters to filter	
🖥 Compliance 🗸	azure-prod + Select Namespace to filter	
Runtime Protection	wordpress-mysql +	
CWPP Dashboard		
App Behavior		
Policies	Search	Apply
Remediation v	All (34) Discovered (6) Changed (0) Active (0) Inactive (34) Pending (9) Ignored > O Ignore Delete () Make Inactive
Monitors /	Policy Name Category Status Clusters Namespace Selector Labels	Tags
	Aarden-wordpress-pkg-mngr-exec. Hardening Inactive azure-prod wordpress-mysql app=wordpress	NIST +4
	□ 🚺 Ksp-mysql-audit-dir_(v2) KubeArmor Custom • Inactive azure-prod wordpress-mysql app≠mysql	None
🕒 Log Out	harden-mvsol-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.

Sear	ch							Activate	
All (4	13)	Discovered (3) Hardening (39) Custom (1)				Olgnore 🔂 Delete	し Make Inactive	
	Policy	Name	Category	Status	Clusters	Namespace	Selector Labels	Tags	
	0	harden-wordpress-shell-history-mod KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	-
	0	<u>harden-wordpress-write-etc-dir</u> KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	NIST_8	00-
	Ø	harden-wordpress-remote-file-copy KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	MITRE	
	Ø	harden-wordpress-write-under-bin-di KubeArmor	^I Hardening	• Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	
	Ø	<u>harden-wordpress-pkg-mngr-exec (v</u> KubeArmor	5 Hardening	• Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	
	Ø	harden-wordpress-file-integrity-monit KubeArmor	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	
	Ø	<u>harden-mysql-file-integrity-monitoring</u> KubeArmor	9. Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=mysql	NIST	
	0	<u>harden-mysql-pkg-mngr-exec</u> KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=mysql	NIST	
	Å	harden-wordpress-trusted-cert-mod	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



Ø	harden-mysql-file-integrity-monitoring X KubeArmorPolicy X © Created 5 days ago. X
YAI	ML 🖉 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	<pre>name: harden-mysql-file-integrity-monitoring</pre>
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	readoniy: true
21 22	_ dir: /hin/
22	readOnly: true
27	recursive: true
25	- dir: /boot/
26	readOnly: true
27	recursive: true
28	message: Detected and prevented compromise to File integri
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	e-integrity-monitoring
namespace:		wordpress-mysql
spec:		
action:		Block
file:		
matchDirecto	ries:	
-	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: Dete	ected and prevente	ed 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_T156	5_data_manipulat	ion



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

Sear	ch							Activate	
All (4	43)	Discovered (3) Hardening (39)	Custom (1)				Ølgnore 🖸 Delete	U Make Inactive	
	Polic	y Name	Category	Status	Clusters	Namespace	Selector Labels	Tags	
	Ø	harden-wordpress-shell-history-mod KubeArmor	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+6
	Ø	harden-wordpress-write-etc-dir KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress_,	NIST_80	00-E
	0	harden-wordpress-remote-file-copy KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	MITRE	
	0	harden-wordpress-write-under-bin-dir KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	++
	۲	harden-wordpress-pkg-mngr-exec.(v5 KubeArmor	Hardening	 Inactive 	aks-demo-prod	wordpress-mysql	app=wordpress,	NIST	++
	(0)	harden-wordpress-file-integrity-monito	Hardening	Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+1
2	0	harden-mysql-file-integrity-monitoring. KubeArmor	Hardening	• Inactive	aks-demo-prod	wordpress-mysql	app=mysql	NIST	+1
	Ø	harden-mysgl-pkg-mngr-exec KubeArmor	Hardening	• Inactive	aks-demo-prod	wordpress-mysql	app=mysql	NIST	++
	()	harden-wordpress-trusted-cert-mod	Hardening	• Inactive	aks-demo-prod	wordpress-mysql	app=wordpress	MITRE	

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

Home	e > Ru	intime Se	curity > Policies				partnerdemo	Y Dartner
F	Polic	cies						Create Policy +
	K8s	~	aks-demo-prod × × ×	wordpress-m	nysql 🗙 🗙	KubeArmor × × ×	Status ~	
	Sear	ch						Activate
	All (4	43)	Discovered (3) Hardening (39)	Custom (1)			🖉 Ignore 📋 Delete	U Make Inactive
		Policy	News					
	_	POlicy	Name	Category	Status	Clusters Namespace	Selector Labels	Tags
		Ø	harden-mysql-file-integrity-monitoring. KubeArmor	Category Hardening Applied a few seco	Active	Clusters Namespace	Selector Labels	NIST +! 5
		() ()	harden-mysql-file-integrity-monitoring, KubeArmor harden-wordpress-shell-history-mod KubeArmor	Category Hardening Applied a few seco Hardening	StatusActiveInactive	Clusters Namespace	Selector Labels	NIST +
		Image: Constraint of the second secon	harden-mysql-file-integrity-monitoring, KubeArmor harden-wordpress-shell-history-mod KubeArmor harden-wordpress-write-etc-dir KubeArmor	Category Hardening Applied a few seco Hardening Hardening	Active Inactive Inactive	Clusters Namespace aks-demo-prod wordpress-m aks-demo-prod wordpress-m aks-demo-prod wordpress-m	Selector Labels ysql app=mysql ysql app=wordpress ysql app=wordpress	Tags NIST +! > NIST +! NIST_800-5
		Image: Control Image:	harden-mysql-file-integrity-monitoring. KubeArmor harden-wordpress-shell-history-mod KubeArmor harden-wordpress-write-etc-dir KubeArmor harden-wordpress-remote-file-copy KubeArmor	Category Hardening Applied a few seco Hardening Hardening Hardening	Status Active Inactive Inactive Inactive Inactive	Clusters Namespace aks-demo-prod wordpress-m aks-demo-prod wordpress-m aks-demo-prod wordpress-m aks-demo-prod wordpress-m	Selector Labels ysql app=mysql ysql app=wordpress ysql app=wordpress	Tags NIST +1 NIST +1 NIST_800-E MITRE

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



root@mysql-	6c6fcdccf-sk5	x2:/sbin# ls				
agetty badblocks blkdiscard blkid blockdev cfdisk chcpu	dumpe2fs e2fsck e2image e2label e2undo fdisk findfs	fsck.ext2 fsck.ext3 fsck.ext4 fsck.minix fsfreeze fstab-decode fstrim	installkernel isosize killall5 ldconfig logsave losetup mke2fs	<pre>mkfs.cramfs mkfs.ext2 mkfs.ext3 mkfs.ext4 mkfs.minix mkhomedir_helper mks2 </pre>	pam_tally2 pivot_root raw resize2fs runuser sfdisk shadowconfig	swaplabel swapoff swapon switch_root tune2fs unix_chkpwd unix_update
ctriaitdei debugfs root@mysql- rm: cannot root@mysql-	+SCK fsck.cramfs 6c6fcdccf-sk5 remove 'mkfs' 6c6fcdccf-sk5	getty hwclock x2:/sbin# rm m : Permission d x2:/sbin#	mkts mkfs.bfs Nkfs lenied	mkswap pam_tally	start-stop-daemon sulogin	wipe t s zramctl

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

	Home $>$ Monitors Logging $>$ Logs	Operation Syscall	Cluster Name azure-prod	Pod Name mysql-6c6fcdccf-sk5×2	
🎝 Compliance 🗸	Logs	Davidant			Copy
	Titer	root: {} 31 items Action: Block			
Remediation 🗸	√Saved Filter	ClusterName: a ContainerID: 8 ContainerImag ContainerNam	azure-prod eacabb1d0da40156354a e: docker.io/library/mysq e: mysql	6abd74c2da6e100c67ff72201192f3efe4706f8e4 :5.6@sha256:20575ecebe6216036d25dab5903	31 808211f1e9ba63dc7825ac20cb975e34cfc
■ Monitors / ^	GMS NS	Data: syscall=5 Enforcer: AppA HostName: aks HostPID: 3521	SYS_UNLINKAT flags= Armor s-amd64nodes-21235576 501	6-vmss000000	
Logs	wordpress-trigger 03	HostPPID: 352 Labels: app=m	1033 wsgl		
Triggers	wordpress-trigger / 03	NamespaceNa Operation: Sys PID: 231 PPID: 224	me: wordpress-mysql call		
Monitors	mysal trigger	ParentProcess	Name: /bin/bash		
🖺 Reports	03	PolicyName: D ProcessName: Resource: mkf	efaultPosture /bin/rm s		
Notifications		Source: /bin/m Timestamp: 16 Type: Matched	sion denied n mkfs 79391357 IPolicy		
🖨 Settings 🗸 🗸	03	UpdatedTime: cluster_id: 176 component_na instanceGroup	2023-03-21T09:35:57.91 9 me: kubearmor : 0	13806Z	
G→ Log Out	03	instanceID: 0 tenant_id: 118 workload: 1			

How to perform bulk operation on applying policies

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

	Home > Runtime Security > Policies partnerdemo ~	Partner ~
Dashboard	Policies	reate Policy +
Inventory ~	K8s v aks-demo-prod x X v wordpress-mysql x X v KubeArmor x X v Status v	
🔺 Issues 🗸 🗸		
🌢 Compliance 🗸	Search	Activate
Runtime Protection	All (43) Discovered (3) Hardening (39) Custom (1)	Make Inactive
CWPP Dashboard	Policy Name Category Status Clusters Namespace Selector Labels	Tags
App Behavior	ksp-mysg-audit-dir.(v3) Custom Applied 20 minutes Active aks-demo-prod wordpress-mysql None	None
Policies	Image: barden-wordpress-pkg-mngr-exec (v5 KubeArmor Hardening • Inactive aks-demo-prod wordpress-mysql app=wordpress	NIST +
Remediation 🗸	harden-wordpress-file-integrity-monito Hardenino • Inactive aks-demo-prod wordpress-mysol app=wordpress	NIST +



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

ne 🗧 Runtime Se	ecurity > Policies					partnerdemo	Y 🗘 Parti
Policies							Create Policy +
K8s ~	aks-demo-prod × × ×	wordpres	s-mysql 🗙 🗙	~ KubeArmo	or × × ~	Status ~	
Applying	g Multiple policies						
Search	Ŷ					=	Activate
All (43)	Discovered (3) Hardening (39) Custom (1)			🖉 Ignore 📋 Delete	U Make Inactive
Policy	y Name	Category	Status	Clusters	Namespace	Selecto ⁻ Labels	Tags
•	<u>ksp-mysql-audit-dir (v3)</u> KubeArmor	Custom	 Inactive 	aks-demo-prod	wordpress-mysql	None	None
☑ 🚷	autopol-system-2096115234 KubeArmor	Discovered	 Inactive 	aks-demo-prod	wordpress-mysql	app=n ysql-malac	None
☑ ()	harden-wordpress-shell-history-mod KubeArmor	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
✓ (⁰)	KubeArmor						

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

ACCUKN	ox	Sear	ch						Activate	
Dashboard		All (4	43) Discovered (3) Hardening (39	Custom (1)				🖉 Ignore 📋 Delete	O Make Inactive	
Inventory	~		Policy Name	Category	Status	Clusters	Namespace	Selector Labels	Tags	
Issues	~		harden-mysgl-file-integrity-monitoring KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=mysql	NIST	+!
Compliance	~		harden-wordpress-remote-file-copy KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=wordpress	MITRE	
Runtime Protection	~		Harden-wordpress-write-etc-dir KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=wordpress	NIST_800	0-5
WPP Dashboard			Harden-wordpress-shell-history-mod KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+1
pp Behavior			WubeArmor	Discovered Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=mysql-malac	None	
olicies			harden-mysql-pkg-mngr-exec KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=mysql	NIST	+/
Remediation	~		harden-wordpress-pkg-mngr-exec.(vf KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+-
Monitors / Logging	~		Marden-wordpress-write-under-bin-dir KubeArmor	Hardening Applied a few seco	Active	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+
• Log Out			harden-wordpress-file-integrity-monito	2 Hardening Applied a few seco	 Active 	aks-demo-prod	wordpress-mysql	app=wordpress	NIST	+!

Integrations

Integrate SIEM tools

- SPLUNK
- AWS Cloud Watch



Rsyslog

Splunk

Splunk Integration:

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

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

Integration of Splunk:

a. Prerequisites:

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

To set up HEC, use instructions in <u>Splunk documentation</u>. 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.

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



	Home > Settings > Integrations > Splunk		
Collectors			
Remediation 🗸	🔤 Splunk		Help 🕥
Monitors /	Integration Name *	Splunk HTTP event collector URL *	
Logging	Enter the Integration Name	https://mysplunkserver.example.com:8086/server/collector	
Reports	la da se		
Notifications	Enter the Index	12345678-1234-1234-5678	
Settings			
Cloud Accounts	Source*	Source Type	
Manage Cluster	Enter the source of Log	Enter the Source Type	
Isor Management			
BAC	Test		Cancel Save
ntegrations			
abels			
ags			
Groups			
icket Template			
+ Log Out			

- 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-xxxxxxxx.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-0xxxxxxx-xxxxx00000
 - Source: Enter the source as http: sh Kafka
 - Source Type: Enter your Source Type here, this can be anything and the same will be attached to the event type forwarded to Splunk. e.g., sh _json
 - Click Test to check the new functionality, You will receive the test message on the configured slack channel. e.g., sh Test Message host = xxxxxx-deployment-xxxxxx-xxx00 source = http:kafka sourcetype = trials
 - Click Save to save the Integration. You can now configure Alert Triggers for Slack Notifications.



AWS CloudWatch

AWS CloudWatch Integration

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

Integration of Amazon CloudWatch:

a. Prerequisites

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

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

	Home $>$ Settings $>$ Integrations $>$ Aws Cloudwatch			
Collectors				
Remediation 🗸	🎩 AWS CloudWatch			Help 🕥
Monitors / Logging	Integration Name*	AWS Access Key () *		
E Reports	Enter a name for integration	Enter the Access key		
A Notifications	AWS Secret Key () *	Region	LogGroup Name*	
🖨 Settings 🖍	Litter the Seciet Key			
Cloud Accounts	Test		c	ancel Save
Manage Cluster				
User Management				
RBAC				
Integrations				
Labels				
Groups				
Ticket Template				
🕞 Log Out				

- Here you will be able to see these entries:
 - Integration Name: Enter the name for the integration. You can set any name.
 - AWS Access Key: Enter your AWS Access Key here.
 - AWS Secret Key: Enter your AWS Secret Key here.
 - Region Name: Enter your AWS Region Name here.

• Once you fill in every field and then click the button this will evaluate whether your integration is working or not.

ACCUKNOX

- Click the Save button.
- c. Configuration of Alert Triggers:
 - On the Logs page, after choosing a specific log filter click on the 'Create Trigger' button.
 - The below fields need to be entered with appropriate data:
 - Name: Enter the name of the trigger. You can set any name without special characters.
 - When to Initiate: The frequency of the trigger as Real Time /.
 - Status: Enter the severity of the trigger.
 - Search Filter Data: The filter log chosen is automatically populated here. This is optional.
 - Predefined queries: The list of predefined queries for this workspace is shown as default.
 - Notification Channel: Select the integration channel that needs to receive logs. This should be AWS CloudWatch. (Note: Channel Integration is done on the previous step)
 - Save: Click on Save for the trigger to get stored in the database.
- d. Logs Forwarding:
 - For each Enabled Trigger, please check the AWS platform to view the logs.
 - Based on Frequency (Real Time / Once in a Day / Week)
 - The Rule Engine matches the real-time logs against the triggers created.

Rsyslog

RSyslog Integration

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

Integration of RSyslog:

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

Note: To deploy the RSyslog server, follow <u>RSyslog Documentation</u>.



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

E Reports			
A Notifications			
💠 Settings 🖍	rsusing Rsyslog		
Cloud Accounts	Integration Name *	Server Address *	Port*
Manage Cluster	Enter a name for integration	Eg., rsyslog.mydomain.com	E.g., 514
User Management	Transport		
RBAC	tcp	~	
Integrations			
Labels	Test		Cancel Save
Tags			
Groups			
Ticket Template			
'			
⊖ Log Out			

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



Integrate Notifications Tools

Slack

Slack

Slack Integration:

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

Integration of Slack:

a. Prerequisites:

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

Note: To generate a Hook URL follow the steps, Webhooks-for-Slack.

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

	Home $>$ Settings $>$ Integrations $>$ Slack		and ground 1. O state
Collectors			
Remediation ~	Slack		Неір 🕥
Monitors /	Integration Name*	Hook URL *	
C Reports	Enter a name for integration	https://hooks.slack.com/services/T000/B000/XXXXXX	<
Notifications	Sender Name *	Title *	Channel Name *
Cattings	Enter the Sender Name	Enter the Title	Enter the Channel Name
Cloud Accounts			
Manage Cluster	Test		Cancel Save
User Management			
RBAC			
Integrations			
Labels			
Tags			
Groups			
Ticket Template			
🕒 Log Out			

- Fill up the following fields:
- Integration Name: Enter the name for the integration. You can set any name. e.g., Container Security Alerts
- Hook URL: Enter your generated slack hook URL here. e.g., https://hooks.slack.com/services/T000/B000/XXXXXXX



- Sender Name: Enter the sender's name here. e.g., AccuKnox User
- Channel Name: Enter your slack channel name here. e.g., livealertsforcontainer
- Click Test to check the new functionality, You will receive the test message on configured slack channel. Test message Please ignore !!
- Click Save to save the Integration. You can now configure Alert Triggers for Slack Notifications.

Integrate Ticketing Tools

- Jira cloud
- fresh service

Jira Integration

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

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



Integration of JIRA:

a. Prerequisites

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

JIRA integration for CWPP:

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

	Home $>$ Settings $>$ Integrations $>$ Jira		
Collectors			
Remediation 🗸	न Jira		Help 🕥
E Monitors /	Integration Name *	Site *	
Reports	Enter a name for integration	https://accuknoxtemporal.atlassian.net/	
Notifications	User Email *	Token *	User Id *
	Usermail.example.com	******	60a7XXXXXXXX068dae49e
Settings A	Project ID *	Issue Summary*	Issue Type
Cloud Accounts	Enter a Project Id	Enter the issue	Select the options V
Wanage Cluster User Management RBAC	Test		Cancel Save
Integrations			
Labels			
Tags			
Groups			
Ticket Template			
🕞 Log Out			

- 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/apitokens. .e.g., kRVxxxxxxxx39
- 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., 5bbxxxxxxx0103780


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

JIRA integration for CSPM:

Steps to Integrate:

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

	Home \rightarrow Settings \rightarrow Integrations \rightarrow CSPM			accuknox-sandbox ~ Q Chirag ~
■ Monitors / Logging ~	CWPP CSPM Registry S3 Data Source			
🖹 Reports	Ticketing Backends			Add connector +
Notifications				
🕸 Settings 🖍		٩	io data available!	
Cloud Accounts			×	
Manage Cluster	4	Add Connector		
User Management	т	ype *		
RBAC	(Jira Cloud	<u>^</u>	
Integrations		Email Backend		
Minions		Jira Server		
Labels		Freshservice		
Tags		ConnectWise		
Groups				
Ticket Template				
🕞 Log Out				

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/apitokens. .e.g., kRVxxxxxxxx39



ACCUKNOX	Home \rightarrow Settings \rightarrow Integrations \rightarrow Cspm \rightarrow Jira Clo	ud				accuknox-sandbox V 🗘 Chirag V
Dashboard	Jira Cloud	Configuration ticket		×		
Inventory ~	Main Name *	Configuration name *			Email*	
🛦 Issues 🗸 🗸	JIRACLD	Default template*				
🏜 Compliance 🗸	Secret*	Default template		• +		
∳ Runtime Protection ~		Project *				
Ollectors	 Is Jira admin Ticket Configuration 	Project Issue type *				Add configuration
📕 Remediation 🗸		Issue type		~		
■ Monitors / Logging ~		Auto maintain tickets Ki	eep syncing closed tickets			Save
🖹 Reports		Remap priority				
Notifications			Priority*			
🕸 Settings 🔷 🔺		Unknown	Priority	~		
Cloud Accounts		Informational	Priority *	,		
Manage Cluster			Priority *			
G→ Log Out		Low	Priority	~		
0			Priority *			

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

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

You can now configure Alert Triggers for JIRA.

Freshservice

Freshservice Integration:

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

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

Integration of Freshservice:

a. Prerequisites

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



- You can find your API key in profile settings in the right-side column.
- b. Steps to Integrate:
- Go to Channel Integration -> CSPM.
- Click on Add the connector and select Freshservice

ACCUKNOX	Home > Settings > Integrations > CSPM		customerdemo v 🖉 Solution v
Remediation 🗸	CWPP CSPM Registry S3 Data S	Source	
■ Monitors / Logging ~	Ticketing Backends		Add connector +
E Reports			
A Notifications		Û	
🌣 Settings 🖍	Jira Cloud JIRATEST	×	
Cloud Accounts	Last sync: 2023-05-02 Connected	Add Connector	
Manage Cluster		Type •	
User Management		type ^	
RBAC		Jira Server	
Integrations		Freshservice	
Labels		ConnectWise	
Tags		Email Backeng	
Groups			
Ticket Template			
G→ Log Out			
Ũ			
	Home > Settings > Integrations > Cspm > Freshse	nvice	customerdemo v Q Solution v
	Home > Settings > Integrations > Cspm > Freshse Freshservice	nice	customerdemo v Q Solution v
ACCUKNOX Remediation ~	Home > Settings > Integrations > Cipm > Freshie Freshservice Main	nice	customerdemo v Q Solution v
ACCUKNOX Remediation Monitors / Logging	Home > Settings > Integrations > Copm > Freshee Freshservice Main Name*	company domain *	customerdemo v 🎝 Solution v Email*
ACCUKNOX Remediation Monitors / Logging Reports	Home > Settings > Integrations > Copm > Freshee Freshservice Main Name*	company domain * https://freshservice.com/	customerdemo v 🗘 Solution v Email*
 ACCUKNOX Remediation Monitors / Monitors / Reports Notifications 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Sacret*	Company domain* https://freshservice.com/	customerdemo v Q Solution v Email*
Accuknox Remediation Monitors / Logging Reports Notifications Settings	Home > Settings > Integrations > Cipm > Freshie Freshservice Main Name* Secret*	Company domain * Company domain * https://freshservice.com/	customerdemo v 🗘 Solution v
 ACCUKNOX Remediation • Monitors / • Monitors / • Reports Notifications Settings ^ Cloud Accounts 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Secret*	Company domain * Company domain * https://freshservice.com/	customerdemo v 🎝 Solution v Email*
ACCUKNOX Remediation Monitors / Logging Notifications Settings Cloud Accounts Manage Cluster	Home > Settings > Integrations > Cipm > Fresher Freshservice Main Name* 	nvice Company domain* https://freshservice.com/	customerdemo v 🄉 Solution v Email*
 ACCUKNOX Remediation • Monitors / • Monitors / • Monitors / • Reports Notifications Settings • Cloud Accounts Manage Cluster User Management 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name * 	nnice Company domain* https://freshservice.com/	Customerdemo v Customerdemo v
 ACCUKNOX Remediation Monitors / Cogging Reports Notifications Notifications Settings Cloud Accounts Manage Cluster User Management RBAC 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Secret*	nnice Company domain* https://freshservice.com/	customerdemo
 ACCUKNOX Remediation ~ Monitors / ~ Monitors / ~ Reports Notfleations Notfleations Settings ^ Cloud Accounts Manage Cluster User Management RBAC Integrations 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Secret*	nnice Company domain* https://freshservice.com/	customerdeno
 ACCUKNOX Remediation • Monitors / • Monitors / • Reports Notifications Settings • Cloud Accounts Manage Cluster User Management RBAC Integrations Labels 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Secret* 	company domain* thtps://freshservice.com/	customerdeno v 🎝 Solution v Email*
 ACCUKNOX Remediation • Monitors / • Monitors / • Reports Notifications Settings • Cloud Accounts Manage Cluster User Management RBAC Integrations Labels Tags 	Home > Settings > Integrations > Capm > Freshee Main Name *	Invice Company domain* Intips://freshservice.com/ Intips://freshservic	customerdeno v Solution v
 ACCUKNOX Remediation • Monitors / • Reports Reports Notifications Settings • Cloud Accounts Manage Cluster User Management RBAC Integrations Labels Tags Groups 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name* Secret*	nnice Company domain* https://freshservice.com/	customerdeno
 ACCUKNOX Remediation ~ Monitors / ~ Monitors / ~ Reports Notifications Notifications Settings ^ Cloud Accounts Manage Cluster User Management RBAC Integrations Labels Tags Groups Ticket Template 	Home > Settings > Integrations > Cipm > Freshee Freshservice Main Name * 	nnice Company domain* https://freshservice.com/	customerdeno

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.

ACCUKNOX	$Home \ > \ Settlings \ > \ Integrations \ > \ Cspm \ > \ Freshserv$	ce		Customer Usecases V Q Customer V
Remediation ~	Freshservice	Configuration ticket	×	
Monitors /	Name *	Configuration name*		Email*
E Reports	FreshserviceINT	Default template *		
△ Notifications	Count	Vulnerability (Group by Finding)	* +	
🔹 Settings 🔷	Succes.	Issue type *		
Cloud Accounts		Software		Add configuration
Manage Cluster	FSTICKET	Auto maintain tickets	rep syncing closed lickets	
User Management		Remap priority		
RBAC			Priority*	_
Integrations		Unknown	Low X ~	Save
Labels		Informational	Priority*	
Tags			Priority*	
Groups		Low	Low × ~	
		Marium	Priority*	
G→ Log Out		WOUNH	Priority*	

Click on the Freshservice ticketing backend to add configuration.

Here Enter the following details:

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

You can now configure Alert Triggers for Freshservice.



Creating Ticket Configuration

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

A Notifications	CWPP CSPM Registry	S3 Data Source			
Settings	Ticketing Backends				Add connector +
Manage Cluster		Ê		Ē	
User Management	Jira Cloud		Jira Cloud		
RBAC	Last sync: 2023-07-20		priya Last sync: 2023-07-20		
Integrations	Connected		Connected		
Labels					

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

Jira Cloud				
Main				
Name*		Service Desk URL*		Email*
priya		https://accu-knox.atlassian.net		shanmuga@accuknox.com
Secret *				
Is Jira admin				
Ticket Configuration				Add configuration
priya-config	Ø	guru-inpriyaintegration	Ø	
Project: JIRAINTEGRATIONTEST Issue type: Bug	Ē	Project: JIRAINTEGRATIONTEST Issue type: Bug	Ē	

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



onfiguration name *		
conf_name		
fault template *		
Default template		^)
Compliance Template		
Datalist Software Template		-
Vulnerability (Group by Finding)		
Issue type		~
] Auto maintain tickets 🔲 Kee	ep syncing closed tickets	
emap priority 🔳		

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

Integrate Registries

Registry

- AccuKnox CSPM tool provides registry scan where the user can onboard their Docker Hub, Nexus, GCR, and ECR registries. Once the registry is onboarded, the scanning of the registry starts automatically in the background. After the scanning is completed, the findings will be populated in the registry scan dashboard.
- To Onboard Registry <u>click here</u>

- a. Amazon Elastic Container Registry:
 - Accuknox CSPM security tool scans images that are present in the onboarded <u>Amazon Elastic</u> <u>Container Registry</u> and identifies any known vulnerabilities and risks associated with those images. These are then categorized based on their severity. Users will be getting a comprehensive view of these risks and vulnerabilities in the dashboard which can be remediated.
- **b.** Google Container Registry:
 - <u>Google Container Registry</u> with images Once onboarded into the AccuKnox SaaS platform, the images are scanned. The risks and vulnerabilities associated with these images are identified and shown in the scan results. The vulnerabilities are classified based on the CVSS Scores.
- c. Nexus Registry:
 - AccuKnox CSPM Security leverages various open-source scanning tools to scan the images present in the onboarded Nexus Repository. It identifies the common vulnerabilities and exploits associated with those images and risks. These Vulnerabilities and risks are classified based on their severity.
- d. DockerHub Registry:
 - <u>DockerHub</u> Repositories can be integrated with AccuKnox SaaS. Once these registries are onboarded, the images are scanned for vulnerabilities and risks. These findings are populated in the dashboard with Critical, High, and low vulnerabilities.



User Management

AccuKnox SaaS provides the ability to authenticate and authorize multiple users to access and utilize the Saas platform. Inside the user management section user can create profiles for other users and these profiles are displayed in the form of a list. From the list, users can View Permissions, Edit, Deactivate, and delete user profiles.

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

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

Invite folks to the workspace

Inviting new users:

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

	Home > Settings > User profiles			' Q institut ~
Dashboard Inventory ~ Issues ~	User profile details First Name*	Last name*	Role*	
III Compliance ~ III Runtime Protection ~ IIII Remediation ~ IIII Monitors / Logging ~ IIII Settings ~	Email*	Groups	Admin Editor Viewer Custom	~
Cloud Accounts Manage Clusters User Management RBAC Manage workspace	resum 122 res(cr) Commun2 + Save	+		Cancel
Integration Labels Tags Groups				
[→ Logout				

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



Dashboard	User Profile Detail			
Inventory ~	First Name*	Last Name*	Role*	
🛦 Issues 🗸 🗸	FirstName	~ LastName	~ Admin	~
ılı Compliance v	E			
+ Runtime Protection ~	Email*	Labels	Groups	
Remediation ~	user@example.com	audit file description	id plugin id audit file descripti	on finding
💷 Monitors / Logging 🗸	MFA	hash network	hash +	
🔹 Settings 🛛 🔿				
Cloud Accounts				
Manage Clusters				
User Management				
RBAC			Can	cel Save
Manage workspace				
Integration				
Labels				
Tags				
Groups				
[→ Logout				

Step 3: After we click save, the new user will be getting a user invite email with username, password, and sign in link to the mentioned email id

Dear FirstName,	
Great going! Welcome to AccuKnox	
Too to be intered to interparticipation	TOXICOTT FIElde TOMIT WITH THE
haten and destining to be the result of the	
below credentials to setup your account	nt
below credentials to setup your accour Email Address : user@accuknox.com	nt
below credentials to setup your accour Email Address : user@accuknox.com Password : A12GbajkRu	nt
below credentials to setup your accour Email Address : user@accuknox.com Password : A12GbajKRu If you did not request, you can safely ig	nt gnore this email.
below credentials to setup your account Email Address : user@accuknox.com Password : A12GbajKRu If you did not request, you can safely is Sincerely,	nt gnore this email.



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

	Sign In
	Email address
	Invictus Innocent
Cloud Native	Password
Easily see & secure cloud assets, workloads,	Invictus Innocent
vulnerabilities and posture.	Forgot Password?

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

		JKNOX	
	Change Pa We are here	assword	
	Old Password *	۲	
	New Password *	٥	
	Confirm Password *	numbers 🗸 8-15 characters	
	Save		
← Back			



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

Setup virtual MFA	Enter MFA Code
device	You need to have an Authentication App to authorise and Proceed Safely
I.Install a Authenticator app on your mobile or computer (example: Google Authenticator App)	Enter Code
2.Use your virtual MFA app and your device camera to scan the QR code	Two-factor authentication code
3. Enter the MFA code	
	Login

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





Assign RBAC

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

	Home > Settings > RBAC		· Q Anadame •
Dashboard	Role Name*		
Inventory			
🛦 Issues 🗸 🗸			
ılı Compliance 🗸 🗸	Permissions	Choose the Permissions	
Funtime Protection ~	Select the Navigation	Search	
🗉 Remediation 🗸 🗸	Full Access	Settings : 2 Inventory : 4	
💷 Monitors / Logging 🗸	Dashboard	Select All	
Settings ^	Inventory	View user's profile	
- Cloud Accounts	Issues	Delete roles in workspace	
Manage Clusters	Runtime Protection	Create new users	
Liser Management	Compliance	Delete users in workspace	
	Remediation	Cancel invites	
Nonoro workensee	Monitors	 Update user's profile 	
Integration	Settings	 Invite users to workspace 	
Labele			
			hack Save
Tags			Dack Save
Groups			
[→ Logout			

💿 ΑςςυΚνοχ

	Home > Settings > RBAC			· Q mailure ·
H Dashboard				
Inventory ~	RBAC			Add Role +
🛦 Issues 🗸 🗸	Role 🌣	Users 🏾	Permissions +	
ll Compliance 🗸 🗸	Admin	7	5	🖺 Clone
Runtime Protection ~		4		5 days
Remediation ~	Editor	4	3	I Cione
Monitors / Logging ~	Viewer	6	1	Clone
Settings ^	Custom	3	2	🖉 Edit 📋 Delete 📋 Clone
Cloud Accounts				
Managa Clusters				
Wanage Clusters				
User Management				
Wanage Clusters User Management RBAC Manage workspace				
Wanage Clusters				
User Manage Clusters RBAC Manage workspace Integration Labels				
User Manage Lusters User Manage workspace Integration Labels Tags				
Wanage Clusters User Management RBAC Manage workspace Integration Labels Tags Groups				
Wanage Clusters User Management RBAC Manage workspace Integration Labels Tags Groups				
User Management RBAC Manage workspace Integration Labels Tags Groups	Page 1 of 16 <			Rows per page: 10 ~

Create Roles and Assign Users

Steps:

• Click on Add Role

	Home \rightarrow Settings \rightarrow Roles			solutions ~ 🗘 Ad
	RBAC			Add role +
Remediation ~				
■ Monitors / ~	Role	Permissions	Users	
🖹 Reports	Editor	90	0	
A Notifications	Policy-creation	1	1	🧪 Edit 📋 Delete
🗢 Settings 🖍	Admin	122	13	
Cloud Accounts	Viewer	40	2	
Manage Cluster	custosample	1	0	🥕 Edit 🧻 Delete
User Management				
RBAC				
Integrations				
Labels				
Tags				
Groups				
Ticket Template	Total Count: 5			Rows per page: 10 👻 < 🚺 >
⊖ Log Out				

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



ACCUKNOX	Home > Settings > Roles > Add		solutions
	Role Name *		
Remediation 🗸	demo-role		
Monitors /	Categories	Choose the permissions	
Logging	Select the Navigation	Search	
Reports		App Behavior: 1 Registry Scan: 1	
Notifications	Full Access	View App Behavior	
Settings A	Policy Management	View Image Scan Details	
	Cluster Management		
Ja Accounts	Alerts and Telemetry		
nage Cluster	App Behavior	View Labels	
r Management	Registry Scan	View Label Entities	
AC	CWPP Label/Tag	View Tags	
egrations	Channel Integrations	Delete Triggers	
ibels	Dashboard	Delete Filters	
igs		Delete Registries	
oups			
cket Template			Back
🗲 Log Out			

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

← → C ■ app.demo.accukn	ox.com/settings/user-profiles/details		아 순 ☆ 🏚
	Home > Settings > User Profiles > Details		solutions ~ 🗘
	User profile details		
Remediation +	Email *	First name *	Last name *
Monitors /			
🖹 Reports	Role*	Labels	Groups
	× ^	+	+
S Notifications	Editor		
🗘 Settings 🔨	Policy-creation		
Cloud Accounts	demo-role Admin		Cancel
Manage Cluster	Viewer		
User Management	custosample		
RBAC			
later stars			
integrations			
Labels			
Tags			
Groups			
Ticket Template			
C Log Out			