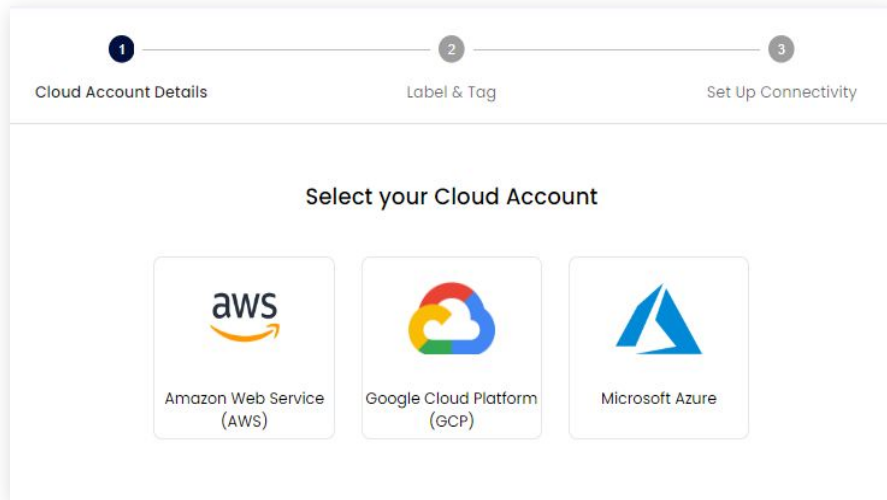




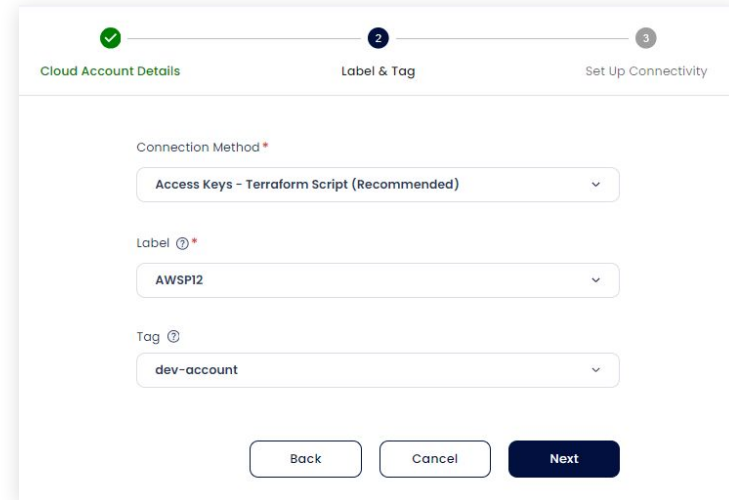
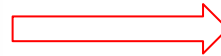
CSPM Playbook



- Choose the Cloud provider (AWS | GCP | Azure)
 - Select AWS
 - Choose connection method -> Access keys
 - Select Label and Tag (It will be used to identify the assets)



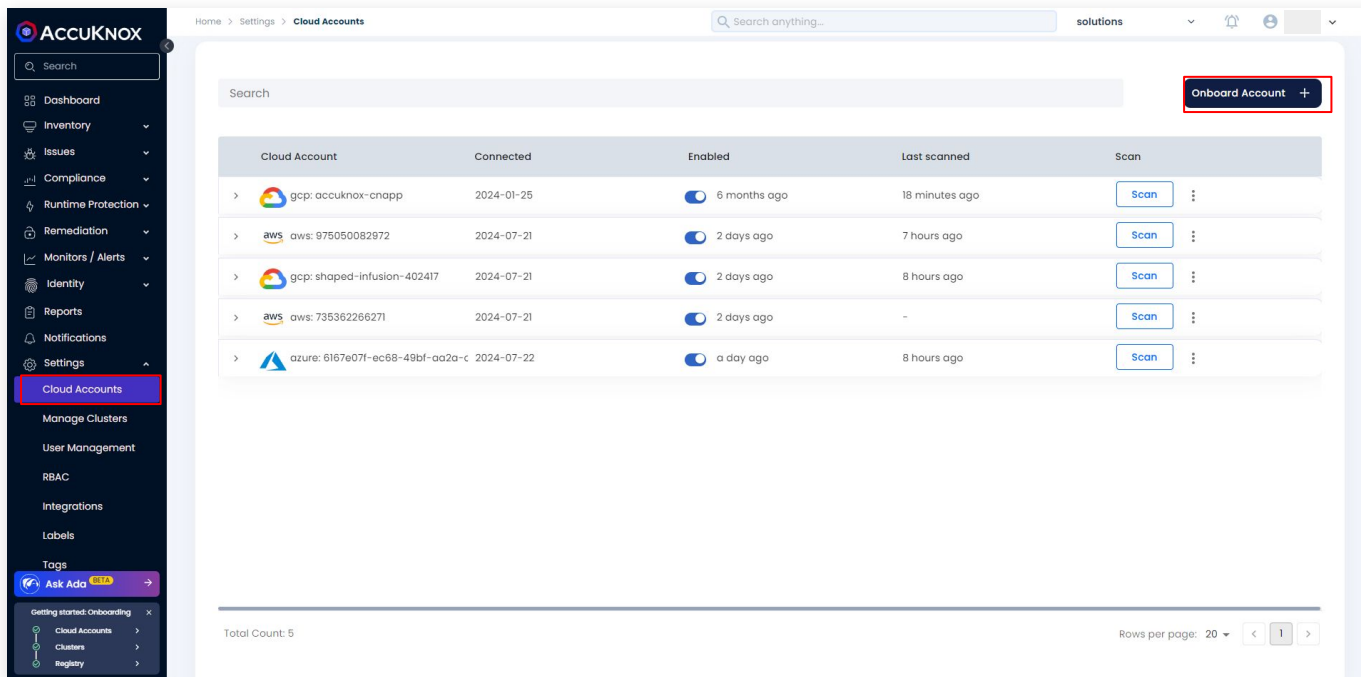
The screenshot shows the first step of the onboarding process, 'Cloud Account Details'. A progress bar at the top indicates three steps: 1. Cloud Account Details (active), 2. Label & Tag, and 3. Set Up Connectivity. Below the progress bar, the heading 'Select your Cloud Account' is centered. Three options are presented in white boxes with rounded corners: Amazon Web Service (AWS) with the AWS logo, Google Cloud Platform (GCP) with the GCP logo, and Microsoft Azure with the Azure logo.



The screenshot shows the second step of the onboarding process, 'Label & Tag'. The progress bar at the top shows step 1 as completed with a green checkmark, step 2 as active, and step 3 as pending. The heading 'Label & Tag' is centered. Below the heading, there are three dropdown menus: 'Connection Method*' with 'Access Keys - Terraform Script (Recommended)' selected, 'Label*' with 'AWSP12' selected, and 'Tag*' with 'dev-account' selected. At the bottom, there are three buttons: 'Back', 'Cancel', and 'Next'.

How to onboard Cloud Account?

- Onboarding Using Terraform Script:
 - Navigate to Settings
 - Click on Cloud accounts
 - Click on Add Account to add a new cloud account



The screenshot shows the ACCUKNOX interface for managing cloud accounts. The left sidebar contains a navigation menu with 'Settings' and 'Cloud Accounts' highlighted. The main content area displays a table of connected cloud accounts with columns for 'Cloud Account', 'Connected', 'Enabled', 'Last scanned', and 'Scan'. An 'Onboard Account +' button is visible in the top right corner of the table area.

Cloud Account	Connected	Enabled	Last scanned	Scan
> gcp: accuknox-cnapp	2024-01-25	6 months ago	18 minutes ago	Scan
> aws: 975050082972	2024-07-21	2 days ago	7 hours ago	Scan
> gcp: shaped-infusion-402417	2024-07-21	2 days ago	8 hours ago	Scan
> aws: 735362266271	2024-07-21	2 days ago	-	Scan
> azure: 6167e071-ec68-49bf-aa2a-c	2024-07-22	a day ago	8 hours ago	Scan

Total Count: 5

Rows per page: 20

- After specifying Label and Tag
 - Click on Next
 - Follow the steps and run the terraform Script to create required keys
 - Get the saved keys from “credentials.txt”
 - Paste the credentials > Select region > Click on Connect

The screenshot displays the AccuKnox onboarding process. On the left is a navigation sidebar with 'Cloud Accounts' highlighted. The main content area shows a progress bar with three steps: 'Cloud Account Details' (completed), 'Label & Tag' (completed), and 'Set Up Connectivity' (current step). Below the progress bar is a section titled 'Terraform script to create the Access Key' with a note and four steps. Step 1: Install Terraform. Step 2: Create a Terraform file with the following script (highlighted in a red box):1 provider "aws" {
2 }
3
4 resource "aws_iam_user" "accuknox" {
5 name = "mj-iam-user"
6 }
7
8 resource "aws_iam_user_policy_attachment" "attach_readonly_policy" {
9 user = aws_iam_user.accuknox.name
10 policy_arn = "arn:aws:iam::aws:policy/ReadOnlyAccess"
11 }
12
13 resource "aws_iam_user_policy_attachment" "attach_security_audit_policy" {
14 user = aws_iam_user.accuknox.name
15 policy_arn = "arn:aws:iam::aws:policy/IAMSecurityAudit"
16 }
17
18 resource "aws_iam_access_key" "accuknox_access_key" {
19 user = aws_iam_user.accuknox.name
20 }
21
22 resource "local_file" "credentials_file" {
23 filename = "credentials.txt"
24 content = <<EOF
25 [default]
26 aws_access_key_id = \${aws_iam_access_key.accuknox_access_key.id}
27 aws_secret_access_key = \${aws_iam_access_key.accuknox_access_key.secret}
28 EOF
29 }Step 3: Run the command: `terraform init && terraform plan && terraform apply`. Step 4: Get the access key and secret key from the file `credentials.txt`. On the right, the 'Set Up Connectivity' form has input fields for 'Access Key ID*' and 'Secret Access Key*', a 'Region*' dropdown menu with a grid of region options, and 'Back', 'Cancel', and 'Connect' buttons. A red box highlights the 'Connect' button with the text 'Click on Connect to Onboard your AWS account'. A red arrow points from the Terraform script box to the 'Connect' button.

Risk Assessment - Cloud Assets View

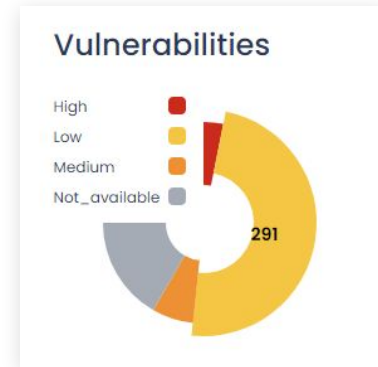
- After Onboarding the cloud account wait for the scan to complete
 - Scan is triggered instantly on account onboarding, but the scan completion might take at-least an hour or more. You will get an email after the successful scan executes.
- Once Scan completed, you should be able to see the cloud assets by navigating to Inventory -> Cloud Assets

The screenshot shows the ACCUKNOX interface for Cloud Assets. The dashboard includes a sidebar with navigation options and a main content area with a search bar and a grid of asset categories. Below the grid is a table of assets with columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. The Findings column is highlighted with a red box, showing counts for each asset.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
<input type="checkbox"/>	10.0.0.167(agent-name)	NessusTest	2024-07-22	Host_Scan_Host	Host_Scan_Host	0	-
<input type="checkbox"/>	6167e07f-ec68-49bf-aa...	AZURE22JULY	2024-07-23	Cloud Account	azure_subscription	0	-
<input type="checkbox"/>	3d64034d-3c3e-4959-...	AZURE22JULY	2024-07-23	Management	azure_tenant	0	-
<input type="checkbox"/>	735362266271	None	-	-	-	0	-
<input type="checkbox"/>	750567562417.dkr.ecr.us...	None	2023-10-17	Container	Container	0	-
<input type="checkbox"/>	788471067825.dkr.ecr.us...	None	2023-10-30	Container	Container	0	-
<input type="checkbox"/>	975050082972	AWS5G	2024-07-23	Cloud Account	aws_account	0	-

Risk Assessment - Asset Detail View

You may further choose to view the misconfigurations associated with a particular Asset from Asset View



Home > Inventory > Cloud Assets > Details

Asset details

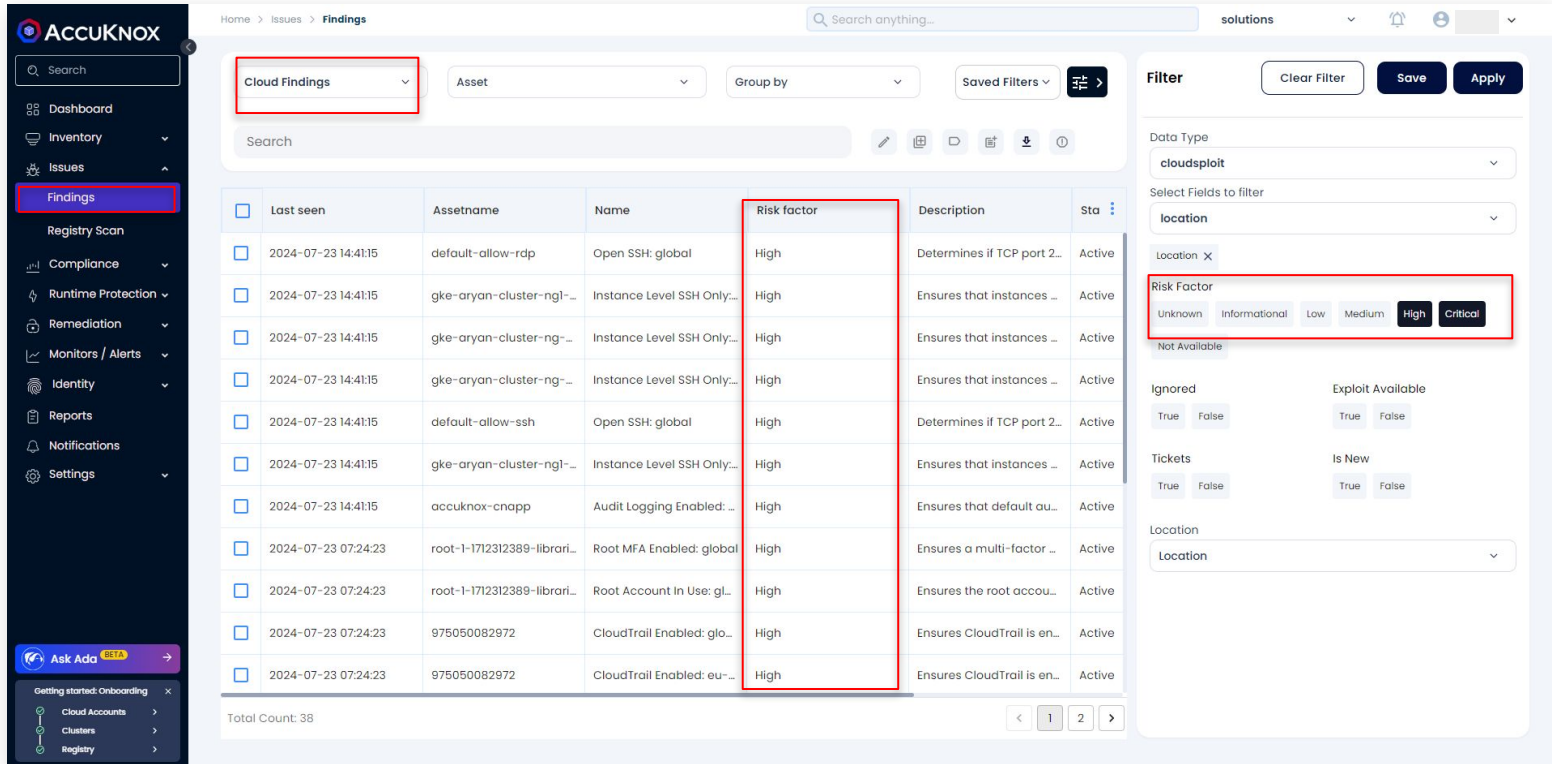
Asset Name: 975050082972
Parent:
Label: AWS5G
Category: Cloud Account
Last Seen: Tuesday, July 23, 2024 07:44 AM
Region: --

0 Tickets

<input type="checkbox"/>	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
<input type="checkbox"/>	2024-07-23	Low	GuardDuty is Enabled: eu-west-2	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Low	VPC Flow Logs Metric Alarm: eu-west-	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Low	Shield Advanced Enabled: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Low	AWS Glue Data Catalog Encryption En	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Low	XRay Encryption Enabled: eu-west-2	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Medium	Password Expiration: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Not_available	Config Service Enabled: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-23	Low	CloudTrail To CloudWatch: eu-west-2	Active	False	False	0	cloudsploit

Risk Assessment - Most Critical Findings

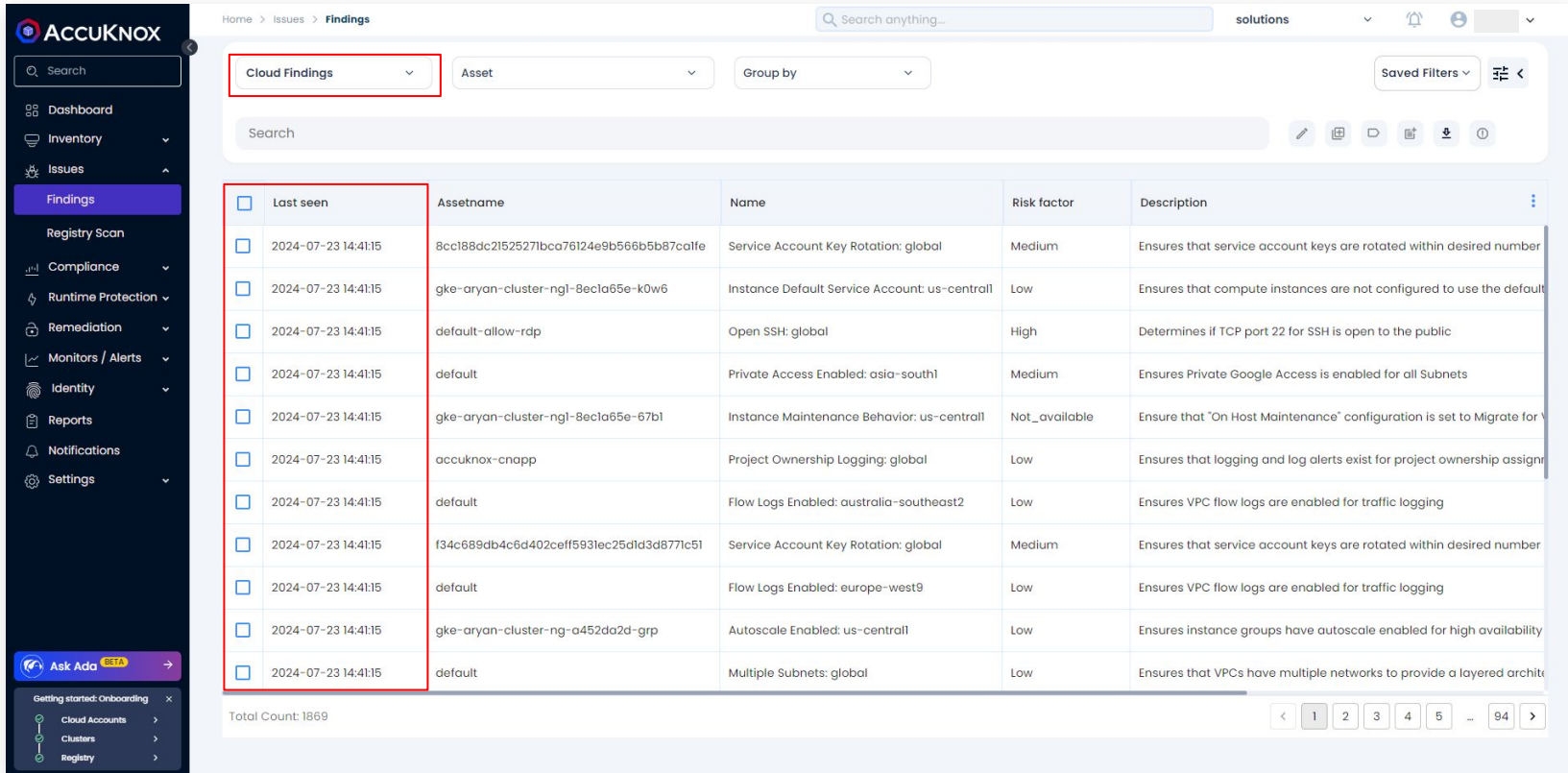
- Find the most *critical findings* across your Cloud Environment
 - Risk Factor = Critical/High



The screenshot displays the AccuKnox Findings interface. The left sidebar contains navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a table of findings with columns: Last seen, Assetname, Name, Risk factor, Description, and Status. The 'Risk factor' column is highlighted in red, showing 'High' for all entries. A filter panel on the right shows 'Risk Factor' set to 'Critical'.

Last seen	Assetname	Name	Risk factor	Description	Status
2024-07-23 14:41:15	default-allow-rdp	Open SSH: global	High	Determines if TCP port 2...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ngl...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ng...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ng...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	default-allow-ssh	Open SSH: global	High	Determines if TCP port 2...	Active
2024-07-23 14:41:15	gke-aryan-cluster-ngl...	Instance Level SSH Only...	High	Ensures that instances ...	Active
2024-07-23 14:41:15	accuknox-cnapp	Audit Logging Enabled: ...	High	Ensures that default au...	Active
2024-07-23 07:24:23	root-1-1712312389-librari...	Root MFA Enabled: global	High	Ensures a multi-factor ...	Active
2024-07-23 07:24:23	root-1-1712312389-librari...	Root Account In Use: gl...	High	Ensures the root accou...	Active
2024-07-23 07:24:23	975050082972	CloudTrail Enabled: glo...	High	Ensures CloudTrail is en...	Active
2024-07-23 07:24:23	975050082972	CloudTrail Enabled: eu...	High	Ensures CloudTrail is en...	Active

- Find the recent most findings



The screenshot displays the AccuKnox interface for finding recent findings. The left sidebar contains navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar is a 'Get started: Onboarding' section with links for Cloud Accounts, Clusters, and Registry.

The main content area shows the 'Findings' page with a search bar and filters. The 'Cloud Findings' filter is highlighted with a red box. Below the filters is a search bar and a table of findings. The table has columns for 'Last seen', 'Assetname', 'Name', 'Risk factor', and 'Description'. The first row of the table is highlighted with a red box. The table shows 10 findings, all dated 2024-07-23 14:41:15. The total count of findings is 1869.

<input type="checkbox"/>	Last seen	Assetname	Name	Risk factor	Description
<input type="checkbox"/>	2024-07-23 14:41:15	8cc188dc21525271bca76124e9b566b5b87ca1fe	Service Account Key Rotation: global	Medium	Ensures that service account keys are rotated within desired number
<input type="checkbox"/>	2024-07-23 14:41:15	gke-aryan-cluster-ngl-8ec1a65e-k0w6	Instance Default Service Account: us-central1	Low	Ensures that compute instances are not configured to use the default
<input type="checkbox"/>	2024-07-23 14:41:15	default-allow-rdp	Open SSH: global	High	Determines if TCP port 22 for SSH is open to the public
<input type="checkbox"/>	2024-07-23 14:41:15	default	Private Access Enabled: asia-south1	Medium	Ensures Private Google Access is enabled for all Subnets
<input type="checkbox"/>	2024-07-23 14:41:15	gke-aryan-cluster-ngl-8ec1a65e-67b1	Instance Maintenance Behavior: us-central1	Not_available	Ensure that "On Host Maintenance" configuration is set to Migrate for
<input type="checkbox"/>	2024-07-23 14:41:15	accuknox-cnapp	Project Ownership Logging: global	Low	Ensures that logging and log alerts exist for project ownership assign
<input type="checkbox"/>	2024-07-23 14:41:15	default	Flow Logs Enabled: australia-southeast2	Low	Ensures VPC flow logs are enabled for traffic logging
<input type="checkbox"/>	2024-07-23 14:41:15	f34c689db4c6d402ceff5931ec25a1d3d8771c51	Service Account Key Rotation: global	Medium	Ensures that service account keys are rotated within desired number
<input type="checkbox"/>	2024-07-23 14:41:15	default	Flow Logs Enabled: europe-west9	Low	Ensures VPC flow logs are enabled for traffic logging
<input type="checkbox"/>	2024-07-23 14:41:15	gke-aryan-cluster-ng-a452da2d-grp	Autoscale Enabled: us-central1	Low	Ensures instance groups have autoscale enabled for high availability
<input type="checkbox"/>	2024-07-23 14:41:15	default	Multiple Subnets: global	Low	Ensures that VPCs have multiple networks to provide a layered archite

Total Count: 1869

- Find the recent most findings
 - group by assets
 - Click on any of the findings

6 issues found across muzammil@accuknox.com
muzammil@accuknox.com

Asset ID	Asset Type	Asset Category	Location
063f0db7-3bb8-497e-aece-d12e90def5e1	aws_iam_user	IAM	global

🕒 **Discovered** about 2 day ago, on 21/07/2024
🕒 **Last detected** on 23/07/2024

Assets ✎ 📄 🗨️ 📄 ⬇️ ⌚

<input type="checkbox"/>	Last seen	Asset	Finding	Risk Factor	Description	Status	Location	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Unauthorized t...	Low	Ensures AWS IAM users t...	Active	global	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Has Tags: glob...	Not_available	Ensure that AWS IAM Us...	Active	global	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Account In Use...	Not_available	Ensure that IAM user ac...	Active	global	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	IAM User Admins: global	Medium	Ensures the number of L...	Active	global	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	Users Password And Ke...	Low	Detects whether users ...	Active	global	
<input type="checkbox"/>	2024-07-23 07:24:23	muzammil@accuknox.c...	No User IAM Policies: glo...	Low	Ensures IAM policies are...	Active	global	

How to Remediate Cloud Misconfigurations?

- Misconfigurations/Findings could be more for a larger infrastructure (Cloud Account) compared to smaller one. The approach should be to attend to the following -
 - Find Most Critical Finding that are unique
 - Find Assets Grouped with associated Findings and filter further based on severity

Search

Ticket Configuration Group by

Misconfiguration list for the Onboarded Cloud Account

<input type="checkbox"/>	Last seen	Finding
<input type="checkbox"/>	2023-09-13	IAM User Has Tags: global
<input type="checkbox"/>	2023-09-13	IAM User Without Permissions: global
<input type="checkbox"/>	2023-09-13	Access Keys Extra: global
<input type="checkbox"/>	2023-09-13	IAM User Account In Use: global
<input type="checkbox"/>	2023-09-13	IAM User Account In Use: global
<input type="checkbox"/>	2023-09-13	IAM User Without Permissions: global
<input type="checkbox"/>	2023-09-13	IAM User Without Permissions: global
<input type="checkbox"/>	2023-09-13	IAM User Unauthorized to Edit: global
<input type="checkbox"/>	2023-09-13	IAM User Has Tags: global
<input type="checkbox"/>	2023-09-13	IAM Username Matches Regex: global
<input type="checkbox"/>	2023-09-13	Access Keys Last Used: global

Total Count: 14219

Search

Ticket Configuration Finding X

<input type="checkbox"/>	Group ids	Last seen	Finding
<input type="checkbox"/>	1	2023-09-13	198.148.116.152 is performing SSH brute force attacks against...
<input type="checkbox"/>	1	2023-09-13	Accelerated Networking Enabled: centralindia
<input type="checkbox"/>	13 >	2023-09-13	Accelerated Networking Enabled: eastus
<input type="checkbox"/>	1	2023-09-13	Accelerated Networking Enabled: eastus2
<input type="checkbox"/>	495 >	2023-09-13	Access Keys Extra: global
<input type="checkbox"/>	439 >	2023-09-13	Access Keys Last Used: global
<input type="checkbox"/>	440 >	2023-09-13	Access Keys Rotated: global
<input type="checkbox"/>	2 >		
<input type="checkbox"/>	2 >		
<input type="checkbox"/>	2 >		
<input type="checkbox"/>	2 >		

Total Count: 2930

Search

Ticket Configuration Asset X

<input type="checkbox"/>	Group ids	Last seen	Finding
<input type="checkbox"/>	43 >	2023-09-12	Open PostgreSQL: us-east-1
<input type="checkbox"/>	5 >	2023-09-13	IAM Role Has Tags: global
<input type="checkbox"/>	14 >	2023-09-13	Users MFA Enabled: global
<input type="checkbox"/>	11 >	2023-09-13	IAM User Account Not In Use: global
<input type="checkbox"/>	11 >	2023-09-13	IAM User Account Not In Use: global
<input type="checkbox"/>	6 >	2023-08-29	EC2 has Tags: us-east-2
<input type="checkbox"/>	11 >	2023-08-22	Access Keys Extra: global
<input type="checkbox"/>	6 >	2023-08-29	EC2 has Tags: us-east-2
<input type="checkbox"/>	2 >	2023-09-08	VPC Subnet Instances Present: us-east-1
<input type="checkbox"/>	6 >	2023-09-12	Trusted Cross Account Roles: global
<input type="checkbox"/>	11 >	2023-09-13	Access Keys Last Used: global

Total Count: 1214

Group by **Findings** for a particular Data-Source (For example - Misconfiguration - Cloudsploit) will showcase **similar findings grouped together** for a resource

So that user don't have to work on same issue twice

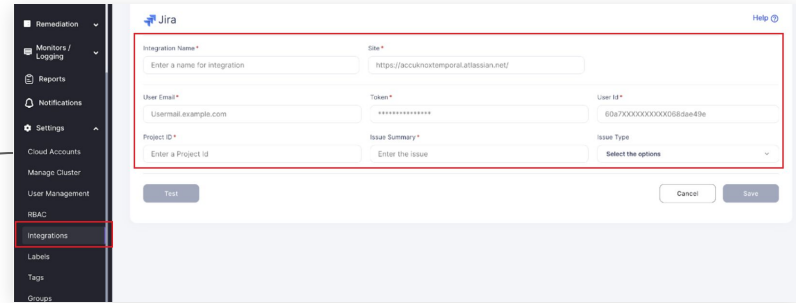
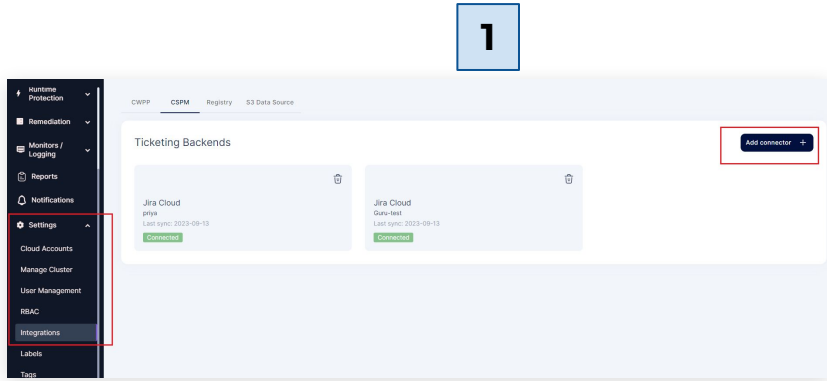
Group by **Assets** for a particular Data-Source (For example - Misconfiguration - Cloudsploit) will showcase **all the issues associated to a particular Asset** such as S3bucket, Host, Container etc.

So that user can focus on Assets of choice

How to set up ticketing tool?

- Setup Ticketing Configuration from Settings >> Integrations >> CSPM

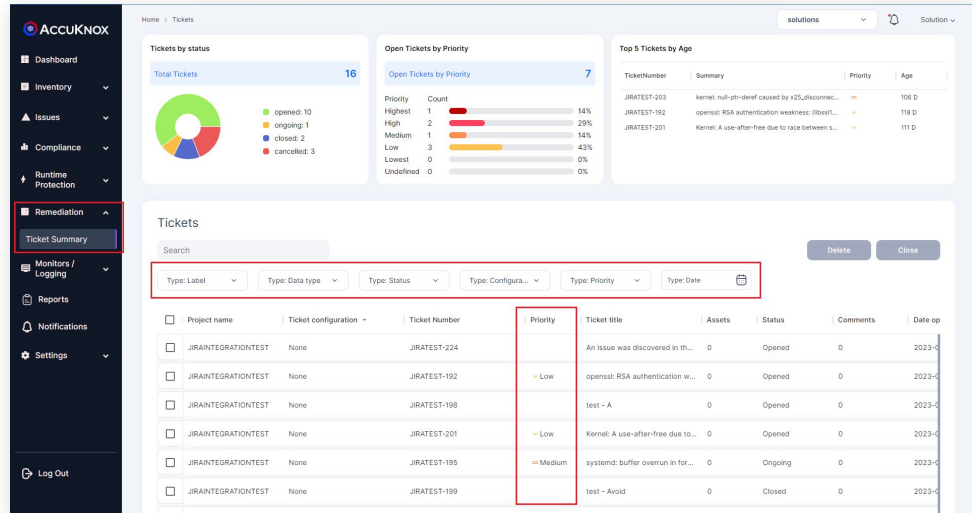
2



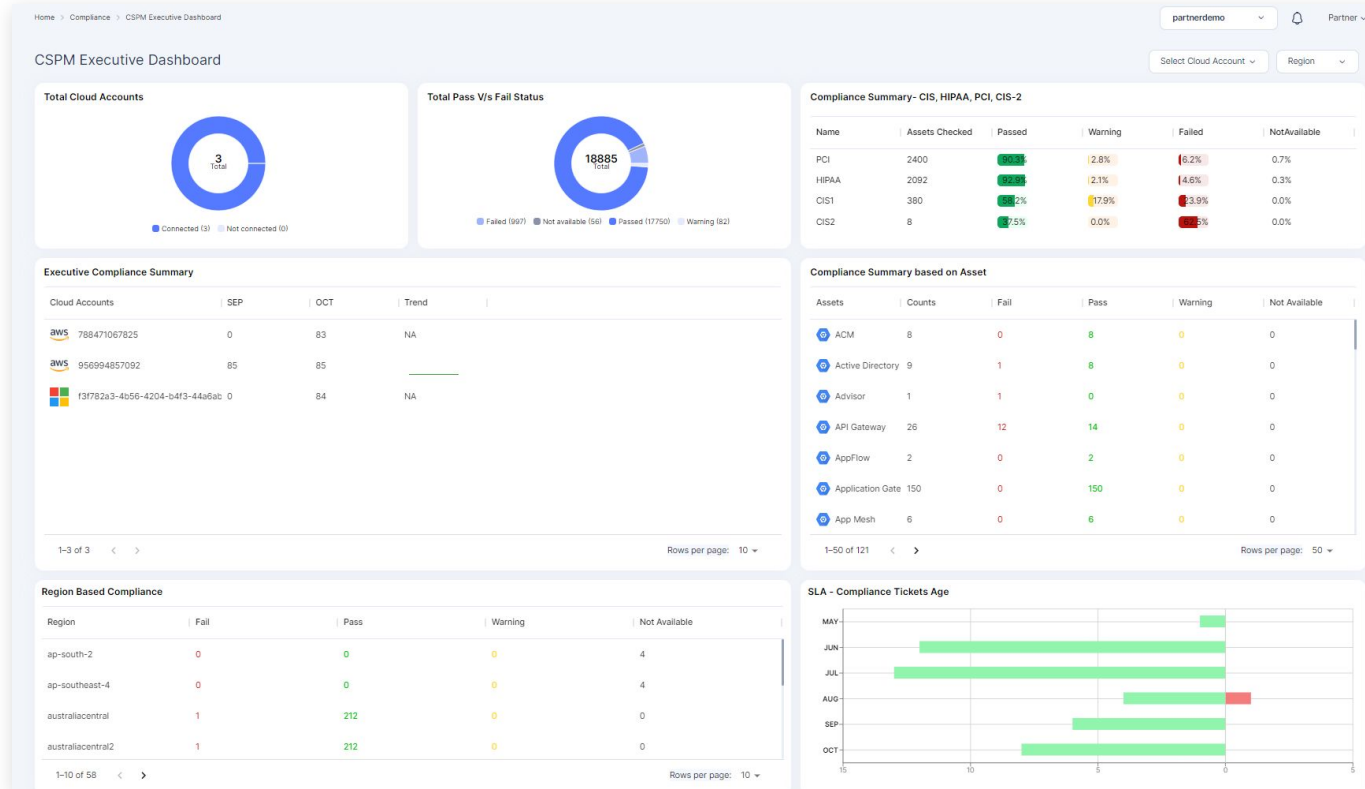
- Then go to the **Remediation >> Ticket Summary** to get Overview of the Issues

3

You need to raise issues from Asset Detail page or Issues >> Vulnerability section to see Ticket Summary



Overview of CSPM Compliance Across Multi Cloud










- To see the compliance summary for the cloud account
 - Click on Cloud Asset Summary
 - Choose the Compliance you want to see from the list

The screenshot shows the ACCUKNOX Compliance Summary interface. The sidebar on the left contains navigation options: Dashboard, Inventory, Issues, Compliance, Baselines, CSPM Executive Dashboard, Cloud Assets Summary (highlighted), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main content area displays a search bar, a dropdown for 'Select Cloud Accounts', and a dropdown for 'Region'. Below this, there are tabs for 'Compliance' and 'Detailed View'. The 'Compliance' tab is active, showing a list of compliance standards and a table of findings. A red box highlights the '33 Compliance found' section, which includes a list of standards and their compliance percentages. The table below shows the details of the findings.

Control	Assets	Description	Compliance	Result
1.10 Ensure multi-factor authentication...	7	Multi-Factor Authentication (MFA) ad...	29 %	5 0 0 2
1.11 Do not setup access keys during in...	7	AWS console defaults to no check box...	29 %	5 0 0 2
1.12 Ensure credentials unused for 45 ...	7	AWS IAM users can access AWS resou...	100 %	0 0 0 7
1.13 Ensure there is only one active ac...	36	Access keys are long-term credential...	86 %	5 0 0 31
1.14 Ensure access keys are rotated ev...	38	Access keys consist of an access key ...	68 %	0 12 0 26
1.15 Ensure IAM Users Receive Permissi...	36	IAM users are granted access to servi...	11 %	0 32 0 4
1.16 Ensure IAM policies that allow full ...	76	IAM policies are the means by which ...	13 %	66 0 0 10
1.17 Ensure a support role has been cr...	0	AWS provides a support center that c...	0 %	1 0 0 0
1.19 Ensure that all the expired SSL/TLS ...	0	To enable HTTPS connections to your ...	100 %	0 0 0 1
1.20 Ensure that IAM Access analyzer L...	0	Enable IAM Access analyzer for IAM p...	0 %	1 0 0 0
1.4 Ensure no root user account acces...	1	The root user account is the most priv...	0 %	1 0 0 0
Total Count: 52				< 1 2 3 >

How to view failed Compliance?

- To see the compliance summary for the Failed results
- Click on Cloud Asset Summary and select any compliance from the compliance list
 - Click on the failed check from the Results
 - You can select filters by Compliance to see specific compliance

Description	Compliance	Result	Detailed View								
Multi-Factor Authentication (MFA) ad...	29 %			Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link	
AWS console defaults to no check box...	29 %		<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
AWS IAM users can access AWS resou...	100 %		<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
Access keys are long-term credential...	86 %		<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
Access keys consist of an access key ...	68 %		<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
IAM users are granted access to servi...	11 %	 failed	<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
IAM policies are the means by which ...	13 %		<input type="checkbox"/>	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...	
			<input type="checkbox"/>	iamRolePolicies	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:iam::123456789012:policy	Role inline ...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...
			<input type="checkbox"/>	iamRolePolicies	arn:aws:iam::123456789012:policy	Role mana...	FAILED	Low	VAIT +20	Ensure that all IAM roles are scoped to spe...	https://docs.aws.amazon.com/IAM/latest/Us...
			Total Count: 66								

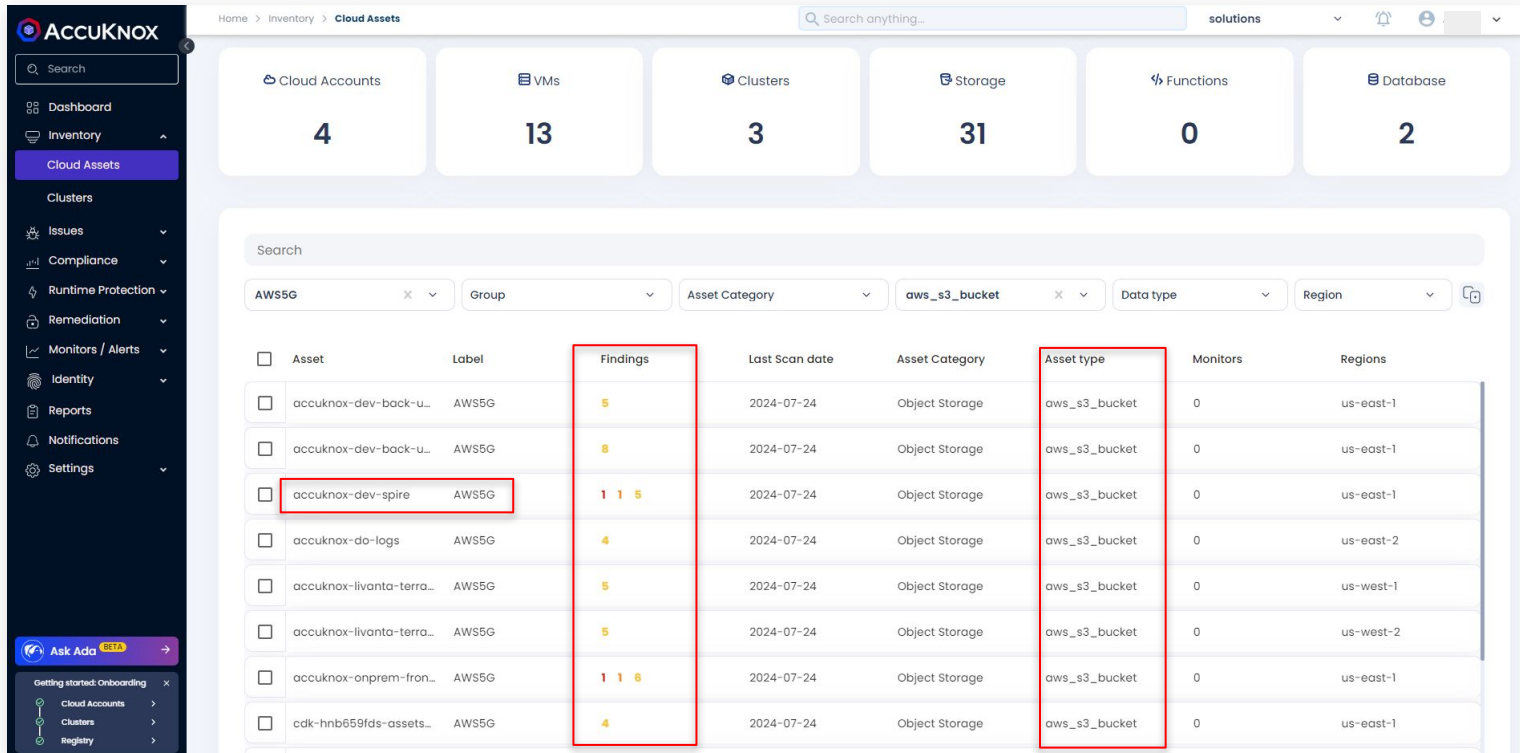


AWS Risk Assessment

Compliance failure and
Misconfiguration

How to identify critical S3-buckets?

- Go to Inventory >> Assets page and Filter for Asset Type as *s3bucket*
- Look for *S3bucket* with count in *Total Vulnerabilities*



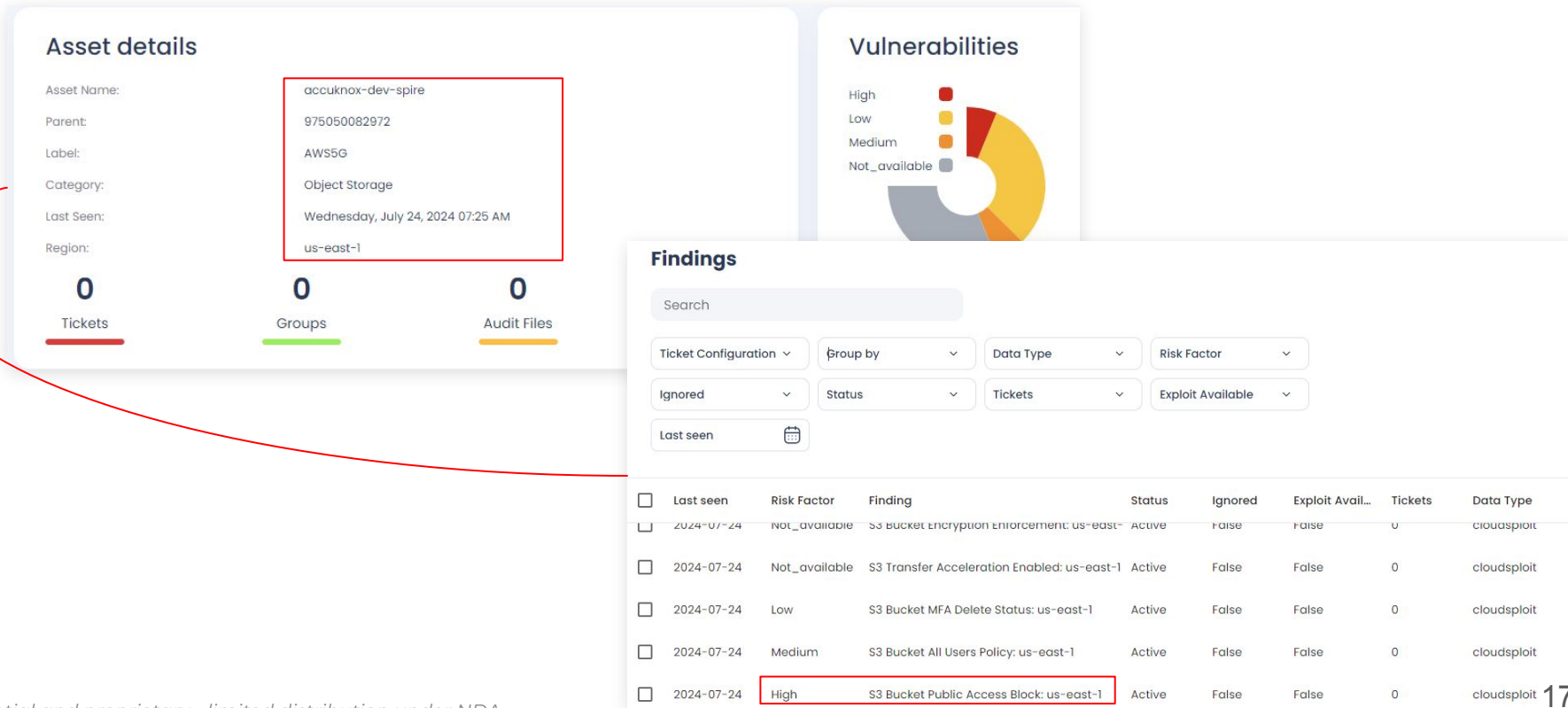
The screenshot displays the ACCUKNOX interface with the following components:

- Navigation Sidebar:** Includes Dashboard, Inventory, Cloud Assets (selected), Clusters, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings.
- Summary Cards:** Cloud Accounts (4), VMs (13), Clusters (3), Storage (31), Functions (0), Database (2).
- Filters:** AWS5G, Group, Asset Category, aws_s3_bucket, Data type, Region.
- Table:** Lists assets with columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
accuknox-dev-back-u...	AWS5G	5	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
accuknox-dev-back-u...	AWS5G	8	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
accuknox-dev-spire	AWS5G	1 1 5	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
accuknox-da-logs	AWS5G	4	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-2
accuknox-livanta-terra...	AWS5G	5	2024-07-24	Object Storage	aws_s3_bucket	0	us-west-1
accuknox-livanta-terra...	AWS5G	5	2024-07-24	Object Storage	aws_s3_bucket	0	us-west-2
accuknox-onprem-fron...	AWS5G	1 1 6	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
cdk-hnb659fds-assets...	AWS5G	4	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1

Identify S3 buckets accessible on public networks

- After Identification of *S3bucket* with misconfiguration
 - Click on the bucket with *misconfiguration*(accuknox-dev-spire) to see the detailed view



The screenshot displays the 'Asset details' and 'Findings' sections of the AccuKnox interface. The 'Asset details' section shows the following information:

- Asset Name: accuknox-dev-spire
- Parent: 975050082972
- Label: AWS5G
- Category: Object Storage
- Last Seen: Wednesday, July 24, 2024 07:25 AM
- Region: us-east-1

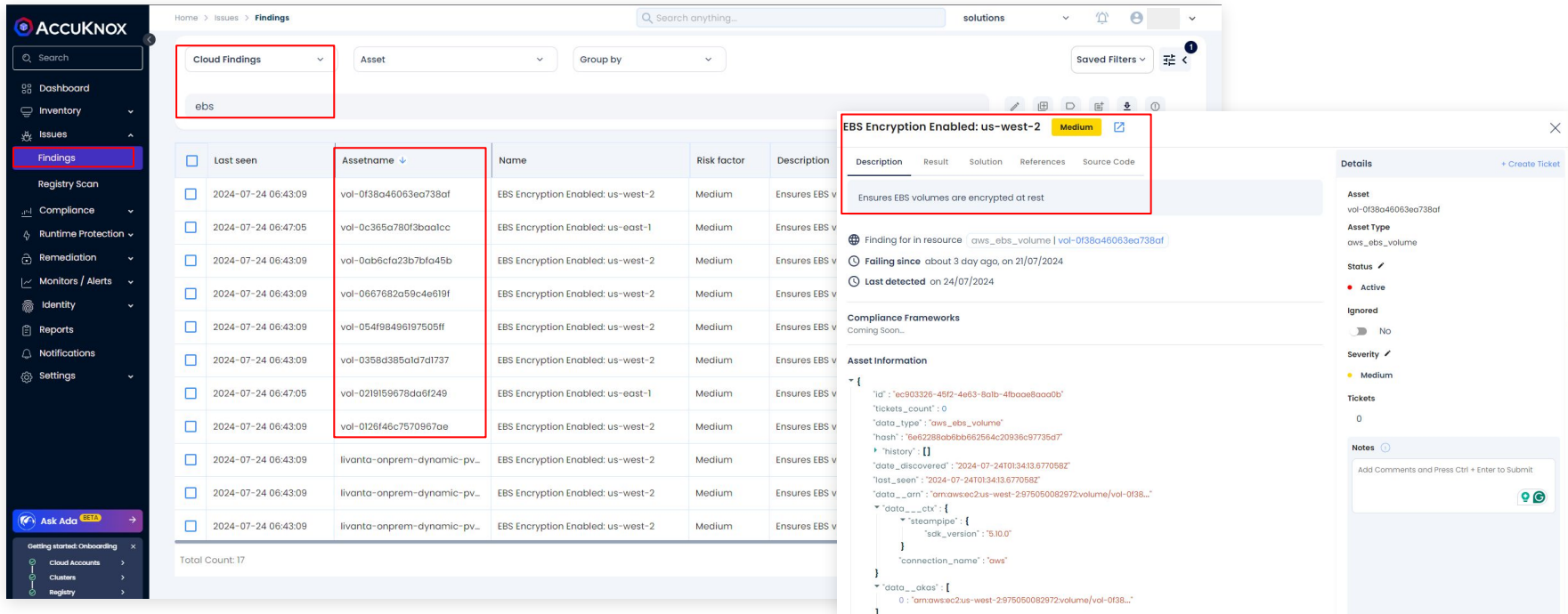
Below the asset details, there are three summary cards: Tickets (0), Groups (0), and Audit Files (0). A red box highlights the asset name and its details. A red arrow points from this box to the 'Findings' table.

The 'Findings' section includes a search bar and several filter dropdowns: Ticket Configuration, Group by, Data Type, Risk Factor, Ignored, Status, Tickets, and Exploit Available. The 'Last seen' filter is set to a calendar icon.

<input type="checkbox"/>	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
<input type="checkbox"/>	2024-07-24	Not_available	S3 bucket encryption Enforcement: us-east-1	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Not_available	S3 Transfer Acceleration Enabled: us-east-1	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Low	S3 Bucket MFA Delete Status: us-east-1	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Medium	S3 Bucket All Users Policy: us-east-1	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	High	S3 Bucket Public Access Block: us-east-1	Active	False	False	0	cloudsploit

How to identify unencrypted EBS Volume?

- To identify the unencrypted EBS Volume associated with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply Cloud Findings in the filter
 - Search for “ebs volume” in the search field



The screenshot displays the AccuKnox Findings interface. The left sidebar shows the navigation menu with 'Findings' selected. The main area shows a list of findings with columns for 'Last seen', 'Assetname', 'Name', 'Risk factor', and 'Description'. A red box highlights the 'Assetname' column, showing various volume IDs. Another red box highlights a specific finding titled 'EBS Encryption Enabled: us-west-2' with a 'Medium' risk level. The detailed view of this finding shows the description 'Ensures EBS volumes are encrypted at rest', the asset name 'vol-0f38a46063ea738af', and the asset type 'aws_aws_volume'. The finding is marked as 'Active' and 'Medium' severity. The details panel also shows the asset's ID and a JSON snippet of the finding's data.

Last seen	Assetname	Name	Risk factor	Description
2024-07-24 06:43:09	vol-0f38a46063ea738af	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:47:05	vol-0c365a780f3baalc	EBS Encryption Enabled: us-east-1	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-0ab6cfa23b7bf45b	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-0667682a59c4e619f	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-054f98496197505ff	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-0358d385a1d7d1737	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:47:05	vol-0219f59678da6f249	EBS Encryption Enabled: us-east-1	Medium	Ensures EBS v
2024-07-24 06:43:09	vol-0126f46c7570967ae	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	livanta-onprem-dynamic-pv...	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	livanta-onprem-dynamic-pv...	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v
2024-07-24 06:43:09	livanta-onprem-dynamic-pv...	EBS Encryption Enabled: us-west-2	Medium	Ensures EBS v

EBS Encryption Enabled: us-west-2 Medium

Description: Ensures EBS volumes are encrypted at rest

Asset: vol-0f38a46063ea738af

Asset Type: aws_aws_volume

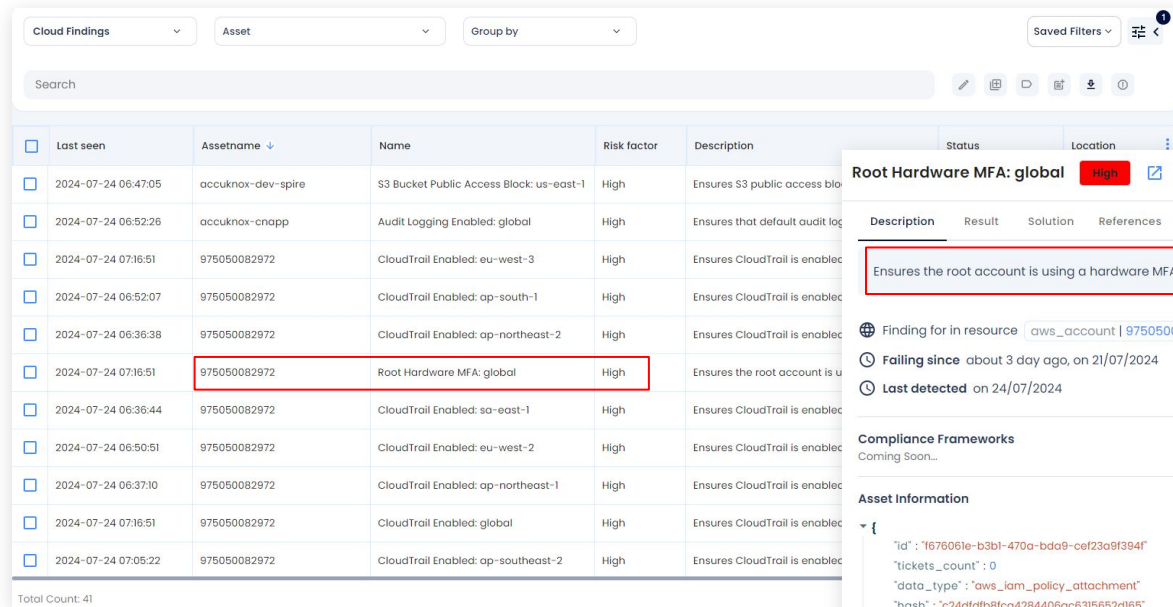
Status: Active

Severity: Medium

```
{
  "id": "ec903328-45f2-4e63-8ab6-4fbaae8aaa0b",
  "tickets_count": 0,
  "data_type": "aws_aws_volume",
  "hash": "6e62288ab6bb662564c20936c97735d7",
  "history": [
    {
      "date_discovered": "2024-07-24T01:34:13.677056Z",
      "last_seen": "2024-07-24T01:34:13.677056Z",
      "data_arn": "arn:aws:ec2:us-west-2:975050082872:volume/vol-0f38..."
    }
  ],
  "data__ctx": {
    "steampipe": {
      "sdk_version": "3.10.0"
    },
    "connection_name": "aws"
  },
  "data__akas": [
    {
      "arn:aws:ec2:us-west-2:975050082872:volume/vol-0f38..."
    }
  ]
}
```

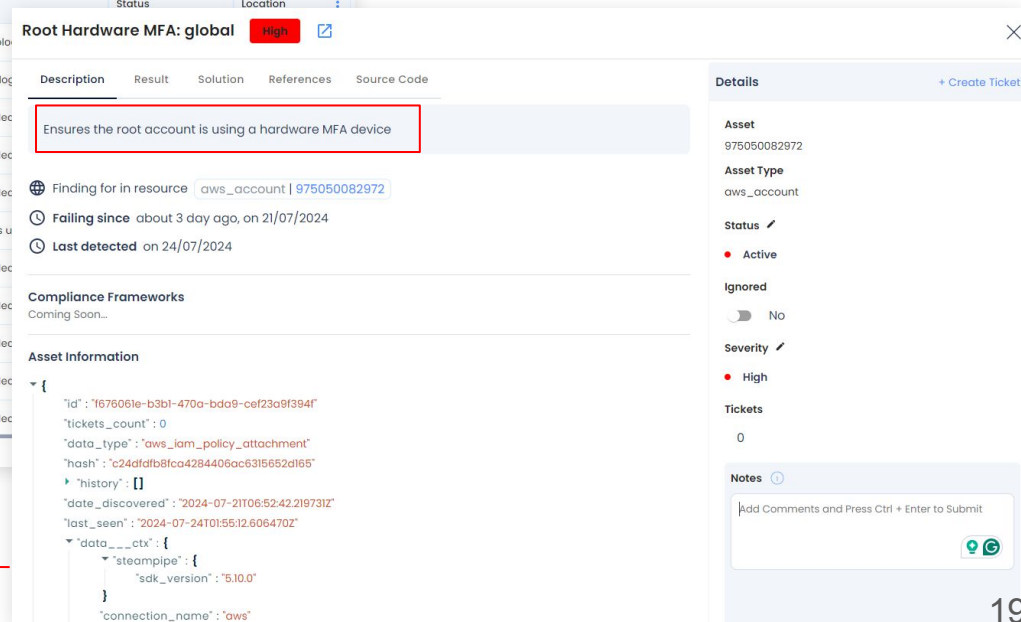
How to identify if root user has enabled MFA?

- To identify if the root user has enabled MFA with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply Cloud Findings in the filter
 - Choose High/Critical Severity



<input type="checkbox"/>	Last seen	Assetname	Name	Risk factor	Description	Status	Location
<input type="checkbox"/>	2024-07-24 06:47:05	accuknox-dev-spire	S3 Bucket Public Access Block: us-east-1	High	Ensures S3 public access blo		
<input type="checkbox"/>	2024-07-24 06:52:26	accuknox-cnapp	Audit Logging Enabled: global	High	Ensures that default audit log		
<input type="checkbox"/>	2024-07-24 07:16:51	975050082972	CloudTrail Enabled: eu-west-3	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 06:52:07	975050082972	CloudTrail Enabled: ap-south-1	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 06:36:38	975050082972	CloudTrail Enabled: ap-northeast-2	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 07:16:51	975050082972	Root Hardware MFA: global	High	Ensures the root account is u		
<input type="checkbox"/>	2024-07-24 06:36:44	975050082972	CloudTrail Enabled: sa-east-1	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 06:50:51	975050082972	CloudTrail Enabled: eu-west-2	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 06:37:10	975050082972	CloudTrail Enabled: ap-northeast-1	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 07:16:51	975050082972	CloudTrail Enabled: global	High	Ensures CloudTrail is enable		
<input type="checkbox"/>	2024-07-24 07:05:22	975050082972	CloudTrail Enabled: ap-southeast-2	High	Ensures CloudTrail is enable		

Total Count: 41



Root Hardware MFA: global High

Description | Result | Solution | References | Source Code

Ensures the root account is using a hardware MFA device

Finding for in resource `aws_account | 975050082972`

Failing since about 3 day ago, on 21/07/2024

Last detected on 24/07/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "f67606le-b3bl-470a-bda9-cel23a9f394f"
  "tickets_count": 0
  "data_type": "aws_iam_policy_attachment"
  "hash": "c24d4dfb8fca4284406ac6315652d165"
  "history": []
  "date_discovered": "2024-07-21T06:52:42.219731Z"
  "last_seen": "2024-07-24T01:55:12.606470Z"
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
  }
  "connection_name": "aws"
}
```

Details [+ Create Ticket](#)

Asset
975050082972

Asset Type
aws_account

Status Active

Ignored No

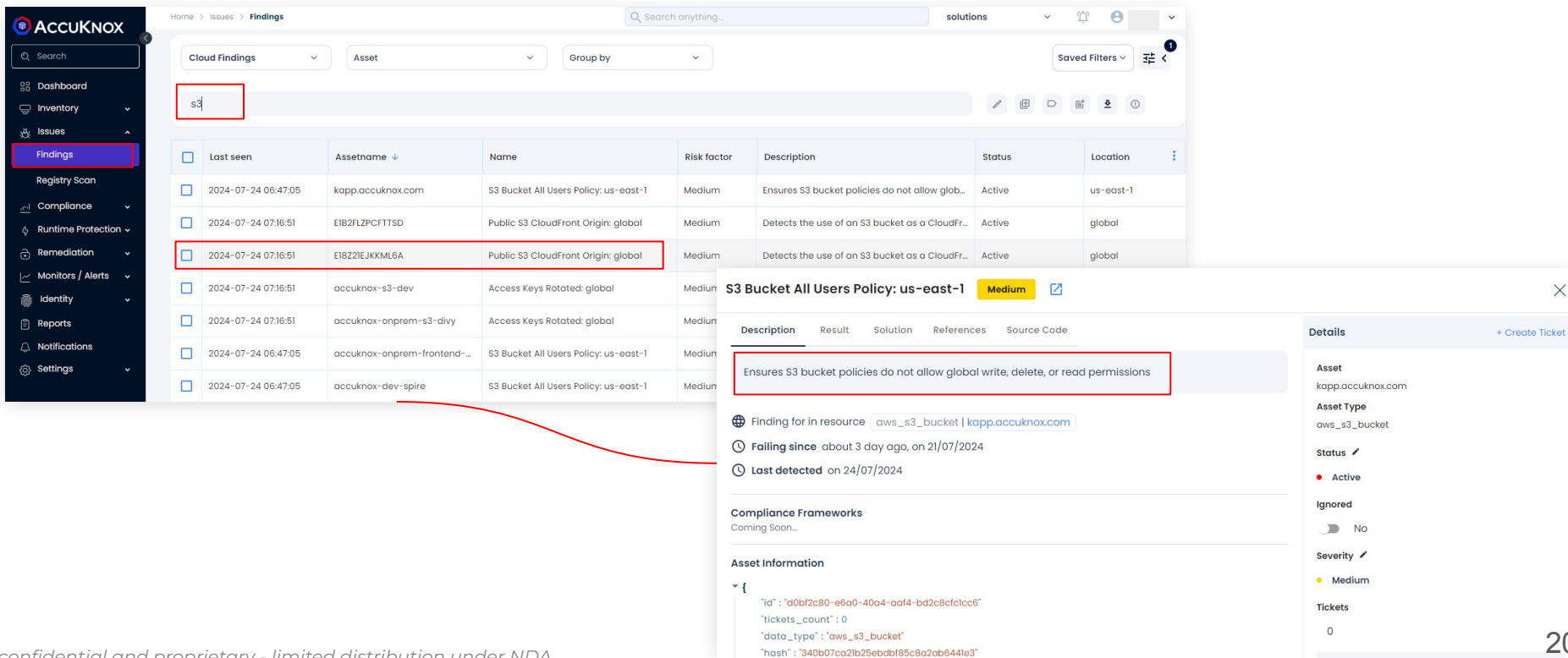
Severity High

Tickets
0

Notes
Add Comments and Press Ctrl + Enter to Submit

How to identify if s3 bucket policy allow global write, delete permission?

- To identify the s3 bucket misconfiguration with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply Cloud Findings in the filter
 - Search for s3



The screenshot displays the ACCUKNOX interface. On the left, a sidebar menu highlights 'Findings'. The main area shows a search for 's3' in the 'Findings' section. A table lists several findings, with one highlighted in red: 'Public S3 CloudFront Origin: global' (Medium risk, Active status). A detailed view of this finding is shown on the right, with a red box highlighting the description: 'Ensures S3 bucket policies do not allow global write, delete, or read permissions'. The detailed view also shows the asset name 'kapp.accuknox.com', the asset type 'aws_s3_bucket', and the status 'Active'.

Last seen	Assetname	Name	Risk factor	Description	Status	Location
2024-07-24 06:47:05	kapp.accuknox.com	S3 Bucket All Users Policy: us-east-1	Medium	Ensures S3 bucket policies do not allow glob...	Active	us-east-1
2024-07-24 07:16:51	E182FLZPCFTTSD	Public S3 CloudFront Origin: global	Medium	Detects the use of an S3 bucket as a CloudFr...	Active	global
2024-07-24 07:16:51	E18Z2IEJKML6A	Public S3 CloudFront Origin: global	Medium	Detects the use of an S3 bucket as a CloudFr...	Active	global
2024-07-24 07:16:51	accuknox-s3-dev	Access Keys Rotated: global	Medium			
2024-07-24 07:16:51	accuknox-onprem-s3-divy	Access Keys Rotated: global	Medium			
2024-07-24 06:47:05	accuknox-onprem-frontend...	S3 Bucket All Users Policy: us-east-1	Medium			
2024-07-24 06:47:05	accuknox-dev-spire	S3 Bucket All Users Policy: us-east-1	Medium			

S3 Bucket All Users Policy: us-east-1 Medium

Description Result Solution References Source Code

Ensures S3 bucket policies do not allow global write, delete, or read permissions

Finding in for resource [aws_s3_bucket | kapp.accuknox.com](#)

Failing since about 3 day ago, on 21/07/2024

Last detected on 24/07/2024

Compliance Frameworks
Coming Soon...

Asset information

```
{
  "id": "a0b12c80-e6a0-40a4-aaf4-bd2c8cfc1cc6"
  "tickets_count": 0
  "data_type": "aws_s3_bucket"
  "hash": "340b07ca21b25ebdb185c8a2cb6441e3"
```

Details [+ Create Ticket](#)

Asset
kapp.accuknox.com

Asset Type
aws_s3_bucket

Status Active

Ignored No

Severity Medium

Tickets
0

How to find Open SSH?

To find the open SSH in the onboarded AWS account

- Navigate to the Issues > Findings
- Search for SSH
- Click on the finding to view the details

Cloud Findings | Asset | Group by

ssh

<input type="checkbox"/>	Last seen	Assetname ↓	Name	Risk factor	Description	Severity	Asset
<input type="checkbox"/>	2024-07-24 07:02:03	rj-gcp	Instance Level SSH Only: us-central1	High	Ensures t		
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-ng-a452d...	Instance Level SSH Only: us-central1	High	Ensures t		
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-ng-a452d...	Instance Level SSH Only: us-central1	High	Ensures t		
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-ngl-8ecla...	Instance Level SSH Only: us-central1	High	Ensures that instances are not configura to...	Active	us-central1
<input type="checkbox"/>	2024-07-24 06:52:26	gke-aryan-cluster-ngl-8ecla...	Instance Level SSH Only: us-central1	High	Ensures that instances are not configura to...	Active	us-central1
<input type="checkbox"/>	2024-07-24 06:47:05	eks-infra-stack-BastionSecuri...	Open SSH: us-east-1	High	Determine if TCP port 22 for SSH is open to th...	Active	us-east-1
<input type="checkbox"/>	2024-07-24 07:02:03	default-allow-ssh	Open SSH: global	High	Determines if TCP port 22 for SSH is open to t...	Active	global
<input type="checkbox"/>	2024-07-24 06:52:26	default-allow-ssh	Open SSH: global	High	Determines if TCP port 22 for SSH is open to t...	Active	global
<input type="checkbox"/>	2024-07-24 06:52:26	default-allow-rdp	Open SSH: global	High	Determines if TCP port 22 for SSH is open to t...	Active	global

Open SSH: us-east-1 High

Description Result Solution References Source Code

Determine if TCP port 22 for SSH is open to the public

Finding in resource: aws_vpc_security_group | eks-infra-stack-BastionSecurityGroupDAB89EBD-3EayCj6s0CT9

Failing since: about 3 day ago, on 21/07/2024

Last detected: on 24/07/2024

Compliance Frameworks: Coming Soon...

Asset Information

```
{
  "id": "8fdc7a95-0443-4454-8166-78d831854135"
  "tickets_count": 0
  "data_type": "aws_vpc_security_group"
  "hash": "c16d65a060efb30443e1847238cecf18"
  "history": []
  "date_discovered": "2024-07-24T01:36:12.894821Z"
  "last_seen": "2024-07-24T01:36:12.894821Z"
  "data_arn": "arn:aws:ec2:us-east-1:975050082972:security-group/..."
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
  }
  "connection_name": "aws"
}
```

Details

Asset: eks-infra-stack-BastionSecurityGroupDAB89EBD-3EayCj6s0CT9

Asset Type: aws_vpc_security_group

Status: Active

Ignored: No

Severity: High

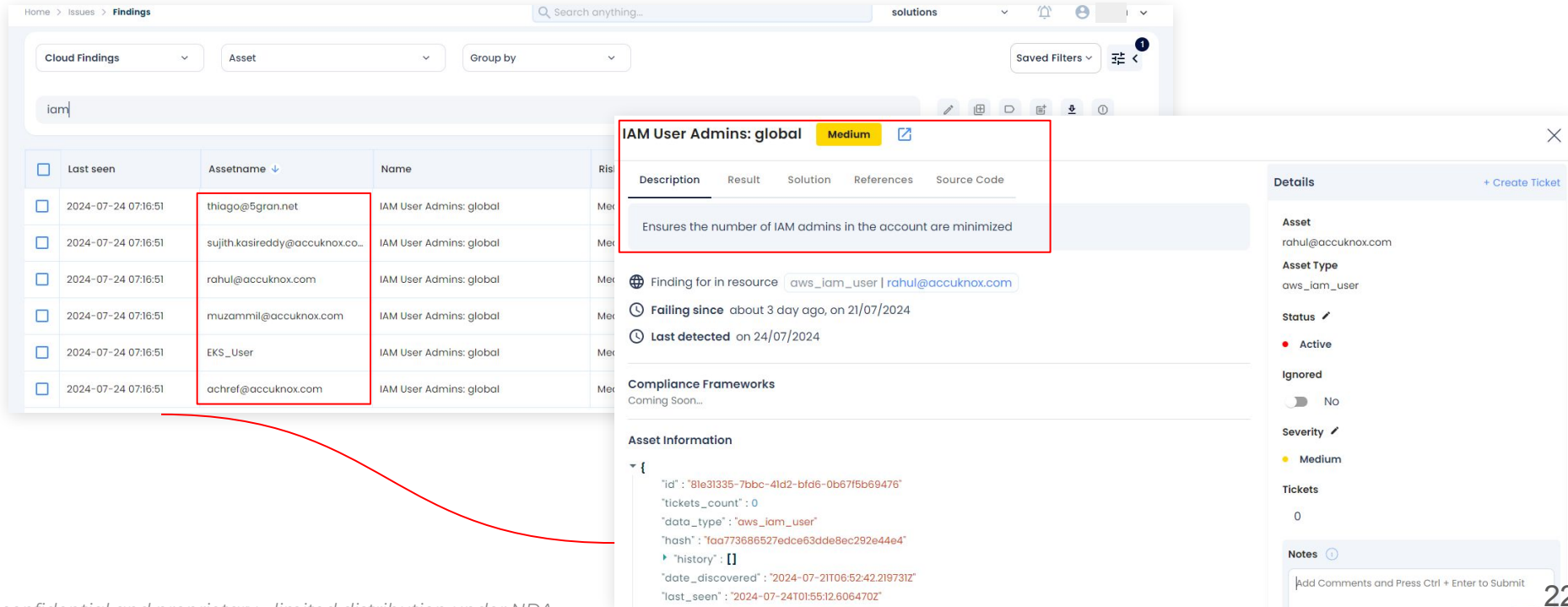
Tickets: 0

Notes: [Add Comments and Press Ctrl + Enter to Submit]

How to Identify IAM related security misconfiguration?

To identify the critical IAM misconfiguration

- Navigate to Issues > Findings
- Search IAM in the search bar
- Click on the findings to view the details



The screenshot displays the Accuknox Findings interface. At the top, there is a search bar with the text 'iam' entered. Below the search bar, a table lists findings. The first finding is highlighted with a red box, showing the asset name 'thiago@5gran.net' and the name 'IAM User Admins: global'. A red arrow points from this finding to a detailed view window.

The detailed view window shows the following information:

- Findings Title:** IAM User Admins: global (Medium severity)
- Description:** Ensures the number of IAM admins in the account are minimized
- Result:** Finding for in resource `aws_iam_user` | [raahul@accuknox.com](#)
- Timeline:** Failing since about 3 day ago, on 21/07/2024; Last detected on 24/07/2024
- Compliance Frameworks:** Coming Soon...
- Asset Information:**

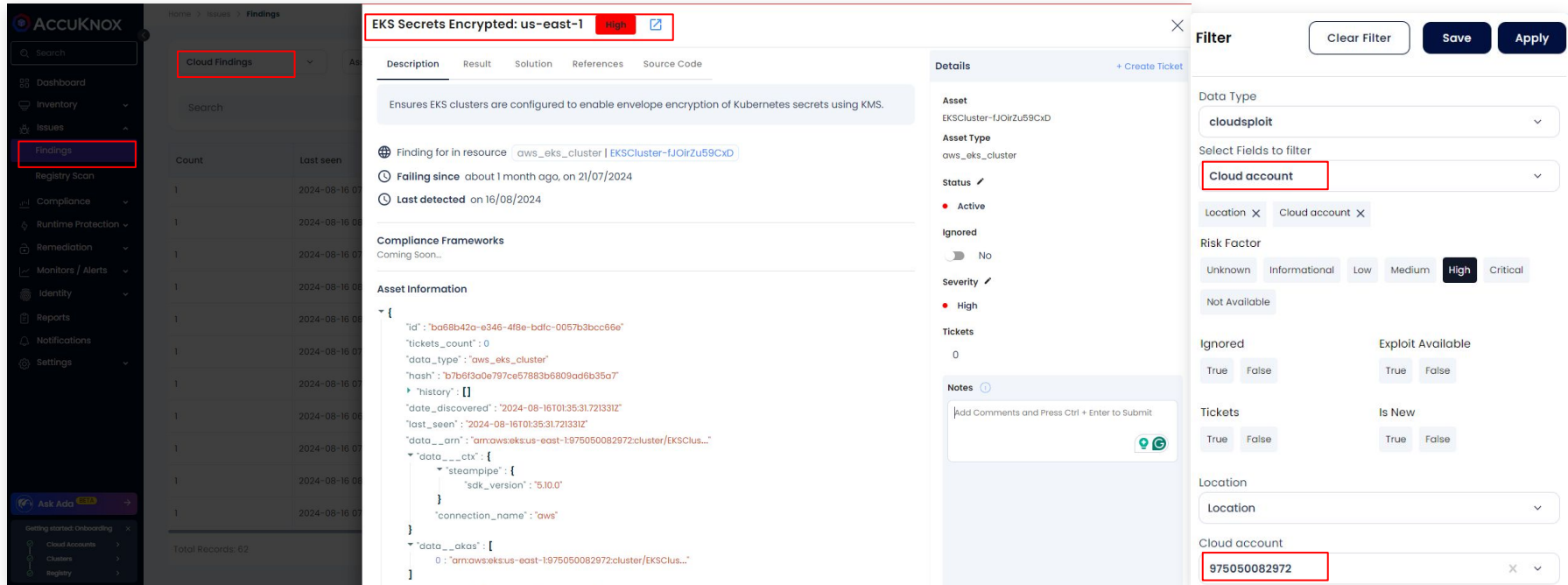
```
{
  "id": "81e31335-7bbc-41d2-bfd6-0b67f5b69476"
  "tickets_count": 0
  "data_type": "aws_iam_user"
  "hash": "f6a773686527edce63dde8ec292e44e4"
  "history": []
  "date_discovered": "2024-07-21T06:52:42.2197312"
  "last_seen": "2024-07-24T01:55:12.6064702"
}
```

The right sidebar shows details for the asset `raahul@accuknox.com`, which is an `aws_iam_user` asset. The status is Active, and the severity is Medium.

How to Identify if encryption is enabled for EKS secrets?

User can identify if encryption is enabled for the EKS secrets by following steps,

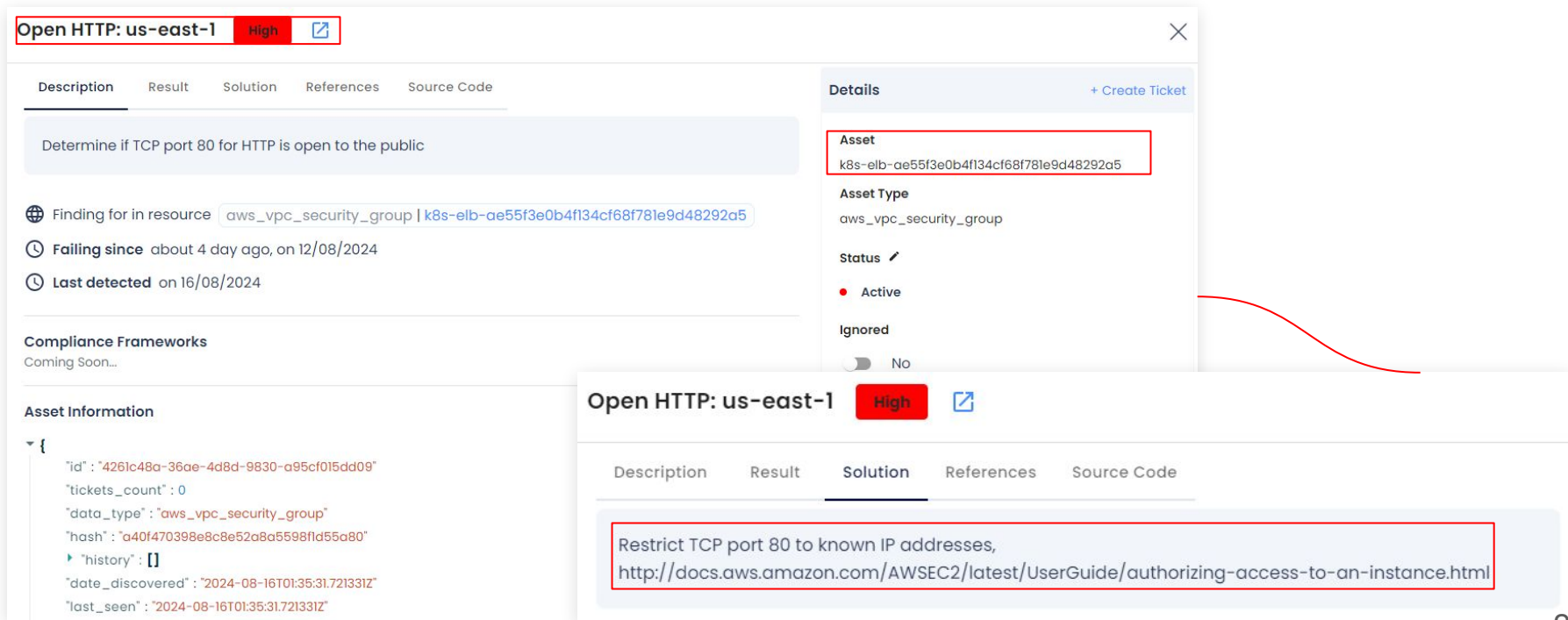
- Select Cloud Findings in findings-type filter
- Add Cloud Account from Select fields to filter, Choose aws cloud in the cloud account filter.
- Also, User can directly search for the Assets/Findings from the Search field
- Then user can click on any findings to get more detailed information with solutions and to create ticket for that particular issue.



The screenshot displays the ACCUKNOX interface. On the left is a dark sidebar with navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a list of findings under the 'Findings' tab, with one finding highlighted: 'EKS Secrets Encrypted: us-east-1' with a 'High' severity. A detailed view of this finding is open, showing a description: 'Ensures EKS clusters are configured to enable envelope encryption of Kubernetes secrets using KMS.' It also shows a finding for resource 'aws_eks_cluster | EKScluster-fJ0irZu59CxD', failing since about 1 month ago, and last detected on 16/08/2024. The 'Asset Information' section shows a JSON object with details like 'id', 'tickets_count', 'data_type', 'hash', 'date_discovered', 'last_seen', 'data_arn', 'data_ctx', and 'data_akas'. A filter panel on the right is active, showing 'Data Type' set to 'cloudsploit', 'Select Fields to filter' set to 'Cloud account', and 'Risk Factor' set to 'High'. The 'Cloud account' filter is set to '975050082972'.

How to identify if Insecure HTTP Port open to public?

- To identify if the HTTP port open to public with the Onboarded Cloud Account:
- User can navigate to Issues -> Findings
 - Apply Cloud Findings in the filter
 - Search for “open HTTP” in the search field



Open HTTP: us-east-1 High

Description Result Solution References Source Code

Determine if TCP port 80 for HTTP is open to the public

Finding for in resource `aws_vpc_security_group | k8s-elb-ae55f3e0b4f134cf68f781e9d48292a5`

Failing since about 4 day ago, on 12/08/2024

Last detected on 16/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "4261c48a-36ae-4d8d-9830-a95cf015dd09"
  "tickets_count": 0
  "data_type": "aws_vpc_security_group"
  "hash": "a40f470398e8c8e52a8a5598fd55a80"
  "history": []
  "date_discovered": "2024-08-16T01:35:31.721331Z"
  "last_seen": "2024-08-16T01:35:31.721331Z"
}
```

Details [+ Create Ticket](#)

Asset
k8s-elb-ae55f3e0b4f134cf68f781e9d48292a5

Asset Type
aws_vpc_security_group

Status ✓

Active

Ignored No

Open HTTP: us-east-1 High

Description Result **Solution** References Source Code

Restrict TCP port 80 to known IP addresses,
<http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

How to identify RDS instances are not deployed in public subnet?

- To identify if the RDS database instances are not deployed with the Onboarded Cloud Account:
- User can navigate to Issues -> Findings
 - Apply Cloud Findings filter.
 - Apply for high risk in cloud findings.

RDS Public Subnet: us-west-2 High [🔗](#)

Description Result Solution References Source Code

Ensures RDS database instances are not deployed in public subnet.

Finding in for in resource `aws_rds_db_instance | livanta-onprem-instance-1`

Failing since about 1 month ago, on 21/07/2024

Last detected about 3 day ago, on 13/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "Id": "0230ea9d-82cb-4437-9e97-686b9c333955"
  "tickets_count": 0
  "data_type": "aws_rds_db_instance"
  "hash": "3e2a9e62f0b0b9c2e0dac6751d12842c"
  "history": []
  "date_discovered": "2024-08-13T01:49:56.293284Z"
  "last_seen": "2024-08-13T01:49:56.293284Z"
  "data_arn": "arn:aws:rds:us-west-2:975050082972:db:livanta-onpr..."
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
  }
  "connection_name": "aws"
}
```

Details [+ Create Ticket](#)

Asset
livanta-onprem-instance-1

Asset Type
aws_rds_db_instance

Status ✓
Active

Ignored
 No

Severity ✓
High

Tickets

Create Ticket

Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page.

`compliancej` X ▼

[Close](#) [Create Ticket](#)

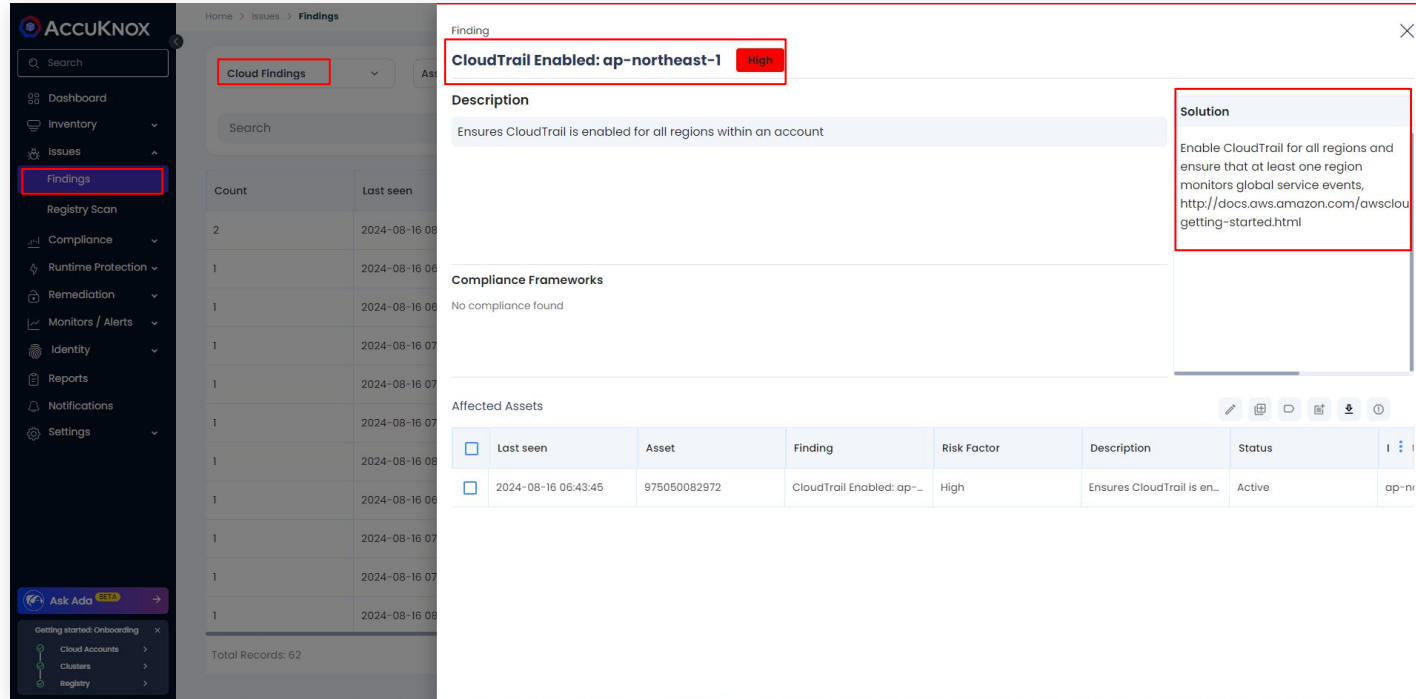
RDS Public Subnet: us-west-2 High [🔗](#)

Description Result **Solution** References Source Code

Replace the subnet groups of rds instance with the private subnets.,
<https://docs.aws.amazon.com/config/latest/developerguide/rds-instance-public-access-check.html>

How to identify if cloud trail is enabled for the cloud account?

- To identify if the cloud trail is enabled for cloud monitoring for an onboarded cloud account:
- User can navigate to Issues -> Findings
 - Apply Cloud Findings filter.
 - Apply for high risk in cloud findings.



The screenshot shows the ACCUKNOX interface with the 'Findings' section selected. A modal window displays a finding titled 'CloudTrail Enabled: ap-northeast-1' with a 'High' risk level. The description states 'Ensures CloudTrail is enabled for all regions within an account'. The solution section provides instructions to enable CloudTrail for all regions and monitor global service events, with a link to the AWS documentation. Below the modal, a table lists affected assets.

Asset	Finding	Risk Factor	Description	Status
2024-08-16 06:43:45	CloudTrail Enabled: ap-...	High	Ensures CloudTrail is en...	Active

Compliance failure for CIS Benchmark

To Identify CIS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot shows the AccuKnox interface for compliance monitoring. The left sidebar contains navigation options, with 'Cloud Assets Summary' highlighted. The main content area displays a list of compliance findings for the asset 'aws 975050082972 | AWS5G'. A table lists 14 CIS benchmark controls, with the 'Compliance' column showing percentages and a bar chart indicating the status of each control. The table is as follows:

Control	Assets	Description	Compliance	Result
1.10 Ensure multi-factor authentication (MFA...	7	Multi-Factor Authentication (MFA) ad...	29 %	5 0 0 2
1.11 Do not setup access keys during initial us...	7	AWS console defaults to no check box...	29 %	5 0 0 2
1.12 Ensure credentials unused for 45 days or...	7	AWS IAM users can access AWS resou...	100 %	0 0 0 7
1.13 Ensure there is only one active access ke...	36	Access keys are long-term credential...	86 %	5 0 0 31
1.14 Ensure access keys are rotated every 90 ...	38	Access keys consist of an access key ...	68 %	0 12 0 26
1.15 Ensure IAM Users Receive Permissions O...	36	IAM users are granted access to servi...	11 %	0 32 0 4
1.16 Ensure IAM policies that allow full "*" ad...	76	IAM policies are the means by which ...	13 %	66 0 0 10
1.17 Ensure a support role has been created t...	0	AWS provides a support center that c...	0 %	1 0 0 0
1.19 Ensure that all the expired SSL/TLS certifi...	0	To enable HTTPS connections to your ...	100 %	0 0 0 1
1.20 Ensure that IAM Access analyzer is enab...	0	Enable IAM Access analyzer for IAM p...	0 %	1 0 0 0
1.4 Ensure no root user account access key ...	1	The root user account is the most priv...	0 %	1 0 0 0

Compliance failure for HIPAA Benchmark



To Identify HIPAA failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot displays the AWS IAM Compliance console for account 975050082972 in the AWS5G region. On the left, a summary shows 28 compliance findings for various benchmarks: FedRamp (56.3% compliant), FERPA (58.0%), FISMA (59.2%), General Data Protec... (24.5%), HIPAA (63.6%), and HITRUST CSF (77.1%). The HIPAA benchmark is highlighted with a red box. The main table lists failed checks, with the 'Result' and 'Severity' columns highlighted in red. The filter panel on the right shows filters for 'control_name' and 'program_name', with 'HIPAA' and '164.312(d) Person or Entity Authentication' selected.

Control	Assets	Description	Compliance	Result
164.312(a)(1) Access Controls	27	Implement technical policies and pro...	100 %	0 0 0 5
164.312(a)(2)(iv) Encryption and Decryption ...	18	Implement a mechanism to encrypt ...	100 %	0 0 0 5
164.312(b) Audit Controls	54	Implement hardware, software, and/...	33 %	6 0 0 3

Plugin	Asset	Message	Result	Severity	Compla...	Recommended Action	Solution Reference Lit...
usersMfaEnab...	arn:aws:iam::975050082972:user:abhi...	User: abhi...	FAILED	Medium	ISMS-P FOR A +20	Enable an MFA device f...	http://docs.aws.amazon...
rootAccessKe...	arn:aws:iam::975050082972:access-key:rootAccessKe...	Access ke...	FAILED	High	KOREAN FINA +19	Remove access keys fo...	http://docs.aws.amazon...
usersMfaEnab...	arn:aws:iam::975050082972:user:rah...	User: rah...	FAILED	Medium	ISMS-P FOR A +20	Enable an MFA device f...	http://docs.aws.amazon...
usersMfaEnab...	arn:aws:iam::975050082972:user:nan...	User: nan...	FAILED	Medium	ISMS-P FOR A +20	Enable an MFA device f...	http://docs.aws.amazon...
usersMfaEnab...	arn:aws:iam::975050082972:user:thia...	User: thia...	FAILED	Medium	ISMS-P FOR A +20	Enable an MFA device f...	http://docs.aws.amazon...
usersMfaEnab...	arn:aws:iam::975050082972:user:sujit...	User: sujit...	FAILED	Medium	ISMS-P FOR A +20	Enable an MFA device f...	http://docs.aws.amazon...
rootAccountIn...	arn:aws:iam::975050082972:root	Root acc...	FAILED	High	AWS WELL-AF +R	Create IAM users with a...	http://docs.aws.amazon...

Compliance failure for ISO 27001 Benchmark



To Identify ISO 27001 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

Compliance Detailed View

28 Compliance found

- ISMS-P for AWS**
Controls: 21, 40.4% Compliant
- ISO 27001**
Controls: 39, 53.6% Compliant
- ISO 27018**
Controls: 6, 78.9% Compliant
- Korean Financial Se...**
Controls: 26, 71.7% Compliant
- LGPD**
Controls: 4, 58.1% Compliant

Control	Assets	Description	Compliance	Result
A.10.1.1 Policy on the Use of Cryptograp...	66	A policy on the use of cryptographic c...	90 %	1 0 0 9
A.10.1.2 Key Management	25	A policy on the use, protection and lif...	100 %	0 0 0 4
A.12.1.2 Change Management	45	Changes to the organization, busines...	93 %	0 3 0 42
A.12.1.3 Capacity Management				
A.12.2.1 Controls Against Malware				
A.12.3.1 Information Backup				
A.12.4.1 Event Logging				
A.12.4.2 Protection of Log Informa...				
A.12.4.3 Administrator and Operat...				
A.12.7.1 Information Systems Audit...				

Compliance Detailed View

Plugin	Asset	Message	Result	Severity	Complia...	Recommended Action	Solution Reference Lir
cloudfrontWaf...	arn:aws:c...	The Clou...	FAILED	Low	MITRE AWS A...+10	1. Enter the WAF service...	https://docs.aws.amazon
guardDutyMa...	None	No Guard...	FAILED	Low	NIST SP 800-1+11	Configure the member ...	https://docs.aws.amazon
cloudfrontWaf...	arn:aws:c...	The Clou...	FAILED	Low	MITRE AWS A...+10	1. Enter the WAF service...	https://docs.aws.amazon
shieldAdvanc...	None	Shield su...	FAILED	Low	HITRUST CSF+11	Enable AWS Shield Adv...	https://docs.aws.amazon
guardDutyEna...	None	GuardDut...	FAILED	Low	HITRUST CSF+14	Enable GuardDuty for a...	https://docs.aws.amazon
shieldEmerge...	None	Shield su...	FAILED	Low	HITRUST CSF+11	Configure emergency c...	https://docs.aws.amazon
shieldProtecti...	None	Shield su...	FAILED	Low	NIST CSF+13	Enable AWS Shield Adv...	https://docs.aws.amazon

Filter Clear Filter Apply

Select Fields to filter

control_name

program_name X control_name X

program_name
ISO 27001 X

control_name
A.12.2.1 Controls Against Malware X

Compliance failure for Mitre AWS Attack Framework

To Identify Mitre framework failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot displays the AWS Compliance console interface. On the left, a sidebar lists various compliance frameworks: LGPD (58.1% Compliant), Mitre AWS Attack Framework (31.9% Compliant), NIST 800-171 (54.7% Compliant), NIST CSF (63.7% Compliant), NIST SP 800-53 (61.5% Compliant), and PCI (67.2% Compliant). The Mitre AWS Attack Framework is highlighted with a red box. The main area shows a table of controls, with a red box around the 'Control' column. A detailed view of the Mitre AWS Attack Framework is shown, listing 14 controls. A red box highlights the 'Result' and 'Severity' columns, showing that all 14 controls have failed with a 'Low' severity. The detailed view table includes columns for Plugin, Asset, Message, Result, Severity, Compliance, Recommended Action, and Solution Reference Link.

Control	Assets	Description	Compliance	Result
Account Manipulation	49	Measures should be put in place to pr...	40 %	6 0 0 4
Brute Force	7	Additio...		
Create Account	25	Account...		
Data from Cloud Storage Object	75	Data in...		
Defacement	2	Disaste...		
Exploit Public-Facing Application	22	Control...		
Impair Defences	132	Necessi...		
Implant Container Image	3	Control...		
Modify Cloud Compute Infrastructure	107	Modific...		
Network Denial of Service	16	Attacke...		
Network Scanning	20	Measur...		
Total Count: 14				

Plugin	Asset	Message	Result	Severity	Complia...	Recommended Action	Solution Reference Lin...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role man...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...
iamRolePolic...	arnaws...	Role has ...	FAILED	Low	VAIT +20	Ensure that all IAM role...	https://docs.aws.amazon...

Compliance failure for NIST 800 compliance

To Identify NIST 800 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

Home > Compliance > Cloud Assets Summary

Search anything...

aws 975050082972 | AWS5G Region

28 Compliance found

- LGPD** (Controls: 4, 58.1% Compliant)
- Mitre AWS Attack Fr...** (Controls: 14, 31.9% Compliant)
- NIST 800-171** (Controls: 10, 54.7% Compliant)
- NIST CSF** (Controls: 38, 63.7% Compliant)
- NIST SP 800-53** (Controls: 13, 61.5% Compliant)
- PCI** (Controls: 8, 67.2% Compliant)

Control	Assets	Description	Compliance	Result
3.12 Security Assessment	0	Implement controls that evaluate ma...	100 %	0 0 0 1
3.13 System and Communications Pro...	130	Monitor, control, and protect commun...	64 %	10 0 0 18
3.14 System and Information Integrity	6	Identify, report, and correct system fla...	50 %	7 0 0 7
3.1 Access Control	131	Limit system access to authorized use...	78 %	20 0 0 72
3.3 Audit and Accountability	58	Create and retain system audit logs a...	57 %	6 0 0 8
3.4 Configuration Management	112	Establish and enforce security config...	95 %	1 0 0 18
3.5 Identification and Authentication	215	Identify system users, processes acti...	45 %	100 47 0 122
3.6 Incident Response	4	Establish an operational incident-han...	50 %	2 0 0 2
3.8 Media Protection	64	Protect (i.e. securely store) system m...	61 %	11 0 0 17
3.9 Personal Security	45	Ensure that organizational systems c...	93 %	0 3 0 42

Total Count: 10

Assistive Remediation For AWS Risks

AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 1)

- Navigate to Issues > Findings
- Select the finding and create a ticket for it

Create Ticket

Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page.

compliancej X v

Close

Create Ticket

Root Hardware MFA: global High [🔗](#)

Description Result Solution References Source Code

Ensures the root account is using a hardware MFA device

Finding for in resource `aws_account | 975050082972`

Failing since about 3 day ago, on 21/07/2024

Last detected on 24/07/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "f676061e-b3b1-470a-bda9-cef23a9f394f"
  "tickets_count": 0
  "data_type": "aws_iam_policy_attachment"
}
```

Details

+ Create Ticket

Asset
975050082972

Asset Type
aws_account

Status [🔗](#)
Active

Ignored [🔗](#)
No

Severity [🔗](#)
High

Tickets
0

Home > Issues > Findings > Create Ticket

Search anything...

Back to all

Create +

Create ticket

Priority
Highest

Ticket Title *
Root Hardware MFA: global

Ticket Description

Description Ensures the root account is using a hardware MFA device

Synopsis

Impacted Assets

Asset	Port
975050082972	global

Solution

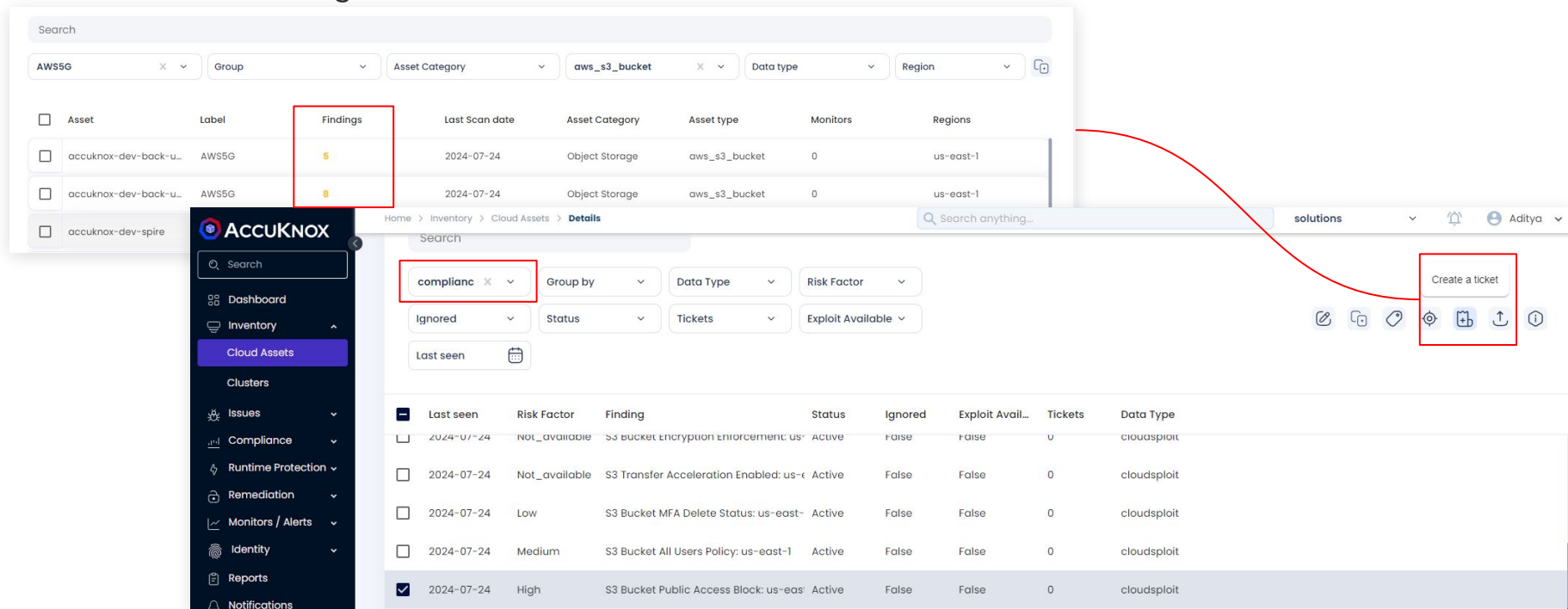
Enable a hardware MFA device for the root account and disable any virtual devices, https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa_enable_physical.html

Plugin Output

FAILED, Root account is not using an MFA device

AccuKnox offers solution reference links to assist with the remediation
To Remediate the findings (Approach 2)

- Navigate to Inventory > Cloud Assets
- Select the finding and create a ticket for it



The screenshot displays the AccuKnox interface. On the left, a sidebar menu is open, highlighting 'Cloud Assets'. The main content area shows a list of findings. A red box highlights the 'Findings' column in the top table. A red arrow points from this box to a 'Create a ticket' button in the bottom table's action column. The bottom table also has a red box around the 'compliance' filter.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions	
<input type="checkbox"/>	accuknox-dev-back-u...	AWS5G	5	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
<input type="checkbox"/>	accuknox-dev-back-u...	AWS5G	8	2024-07-24	Object Storage	aws_s3_bucket	0	us-east-1
<input type="checkbox"/>	accuknox-dev-spire							

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type	
<input type="checkbox"/>	2024-07-24	Not available	S3 Bucket Encryption Enforcement: us-	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Not available	S3 Transfer Acceleration Enabled: us-	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Low	S3 Bucket MFA Delete Status: us-east-	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-07-24	Medium	S3 Bucket All Users Policy: us-east-1	Active	False	False	0	cloudsploit
<input checked="" type="checkbox"/>	2024-07-24	High	S3 Bucket Public Access Block: us-eas-	Active	False	False	0	cloudsploit

Assistive Remediation For AWS Compliance Failure

AccuKnox offers solution reference links to assist with the remediation
To Remediate the findings (Approach 3)

- From the detailed view of Cloud Asset Summary
- Select the failed compliance and create a ticket for it

The screenshot displays the AccuKnox interface. On the left, a navigation sidebar highlights 'Cloud Assets Summary'. The main area shows a table of compliance findings for 'aws-975050082972 | AWS5G' in the 'Region'.

Plugin	Asset	Message	Result
iamRolePolic...	arn:aws:iam::975050082972:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing	Role managed policy allows actions on all resources	FAILED

The detailed view for the failed finding shows:

- Description:** Ensures IAM role policies are properly scoped with specific permissions.
- Message:** Role managed policy allows actions on all resources.
- Solution Reference Link:** https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html
- Recommended Actions:** Ensure that all IAM roles are scoped to specific services and API calls.
- Details:** Includes a '+ Create Ticket' button.
- Asset:** arn:aws:iam::975050082972:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing
- Asset Category:** IAM
- Region:** None
- Result:** FAILED
- Severity:** Low
- Account:** aws-975050082972

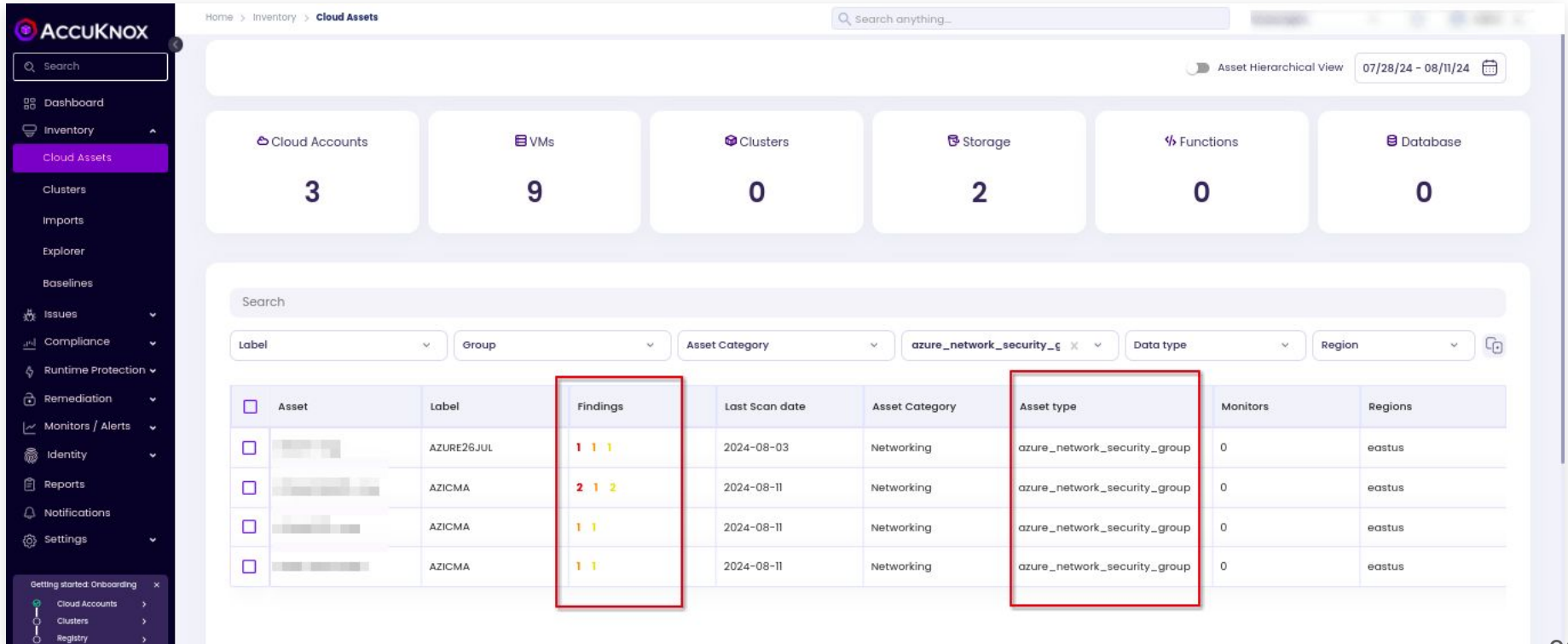


AZURE Misconfigurations

Critical Risks

How to identify all issues in Azure Network security group?

- Go to Inventory >> Assets page and Filter for Asset Type as **azure_network_security_group**
- Look for **Azure Network security group** with count in **Total Vulnerabilities**

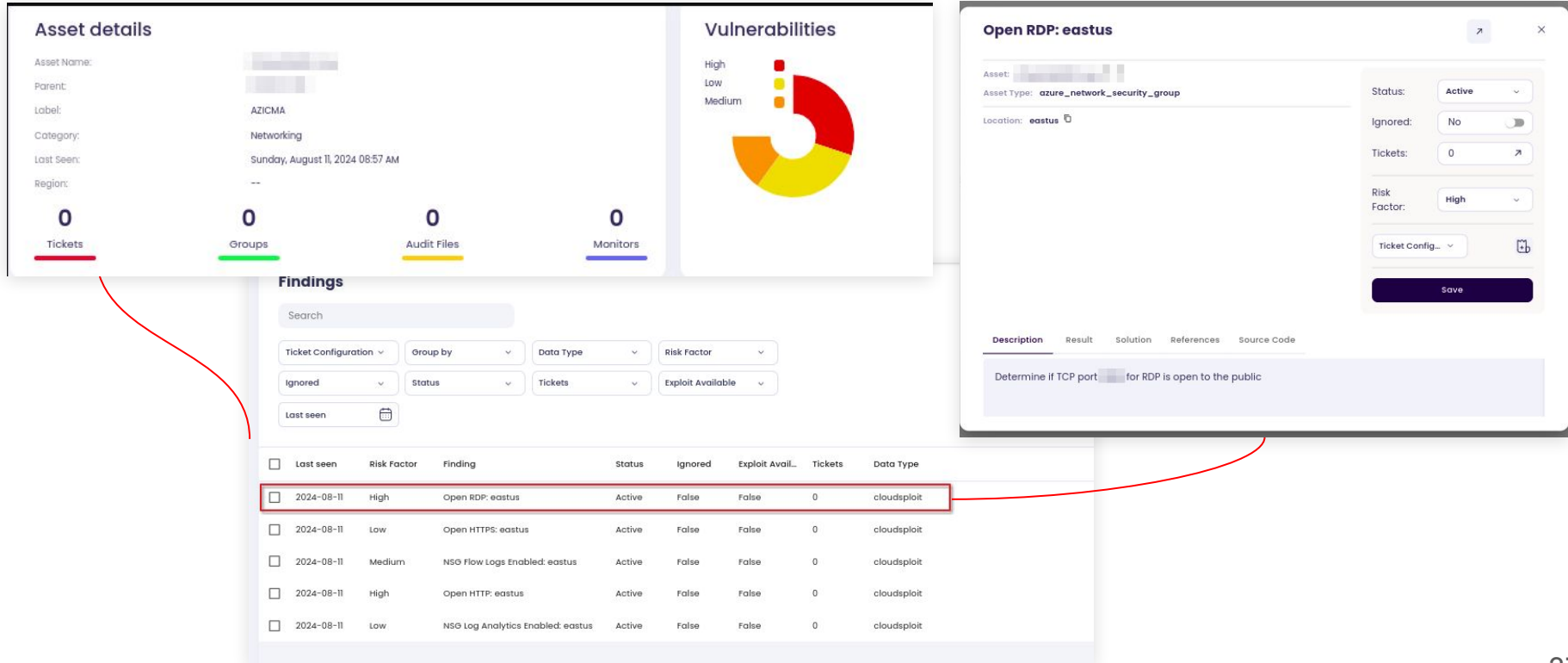


The screenshot shows the ACCUKNOX Cloud Assets dashboard. The top navigation bar includes 'Home > Inventory > Cloud Assets' and a search bar. Below the navigation are six asset category cards: Cloud Accounts (3), VMs (9), Clusters (0), Storage (2), Functions (0), and Database (0). The main content area features a search bar and a filter bar with dropdowns for Label, Group, Asset Category, Data type, and Region. The 'Asset Category' dropdown is set to 'azure_network_security_group'. Below the filters is a table with the following columns: Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. The 'Findings' and 'Asset type' columns are highlighted with red boxes. The table contains four rows of data, all with 'azure_network_security_group' as the asset type.

Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
<input type="checkbox"/>	[REDACTED]	1 1 1	2024-08-03	Networking	azure_network_security_group	0	eastus
<input type="checkbox"/>	[REDACTED]	2 1 2	2024-08-11	Networking	azure_network_security_group	0	eastus
<input type="checkbox"/>	[REDACTED]	1 1	2024-08-11	Networking	azure_network_security_group	0	eastus
<input type="checkbox"/>	[REDACTED]	1 1	2024-08-11	Networking	azure_network_security_group	0	eastus

Identify Azure Network security group issues

- After Identification of **Azure Network security group** with misconfiguration
 - Click on any **misconfiguration** to get the detailed view

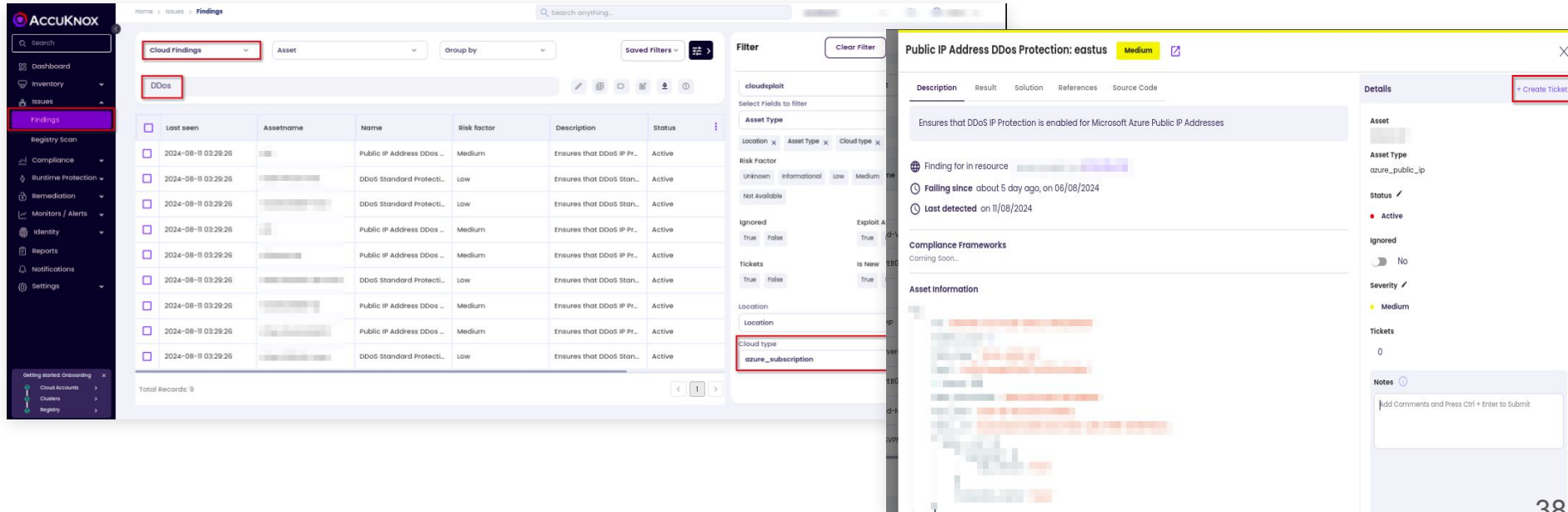


The screenshot displays the AccuKnox interface. On the left, the 'Asset details' panel shows information for an asset named 'AZICMA' in the 'Networking' category, last seen on 'Sunday, August 11, 2024 08:57 AM'. Below this are four metrics: Tickets (0), Groups (0), Audit Files (0), and Monitors (0). The 'Vulnerabilities' section features a donut chart with segments for High (red), Low (yellow), and Medium (orange) risk levels. The main 'Findings' table is filtered by 'Ticket Configuration', 'Group by', 'Data Type', 'Risk Factor', 'Ignored', 'Status', 'Tickets', and 'Exploit Available'. The table lists several findings, with the first one, 'Open RDP: eastus', highlighted in red. A red arrow points from this finding to a detailed view window on the right. This window shows the asset type as 'azure_network_security_group' and location as 'eastus'. It includes controls for Status (Active), Ignored (No), Tickets (0), and Risk Factor (High). The description of the finding is: 'Determine if TCP port [redacted] for RDP is open to the public'.

	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
<input checked="" type="checkbox"/>	2024-08-11	High	Open RDP: eastus	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-11	Low	Open HTTPS: eastus	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-11	Medium	NSO Flow Logs Enabled: eastus	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-11	High	Open HTTP: eastus	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-11	Low	NSO Log Analytics Enabled: eastus	Active	False	False	0	cloudsploit

How to Identify if the DDoS protection is enabled?

- To identify if the DDoS protection is enabled in Azure Public IP Addresses, Please navigate to Issues -> Findings
 - Select **Cloud Findings** in findings-type filter
 - Add Cloud Type from fields to filter, Choose azure_subscription in the cloud type filter.
 - Also, User can directly search for the Assets/Findings from the Search field
 - Then user can click on any findings to get more detailed information with solutions and to create ticket for that particular issue

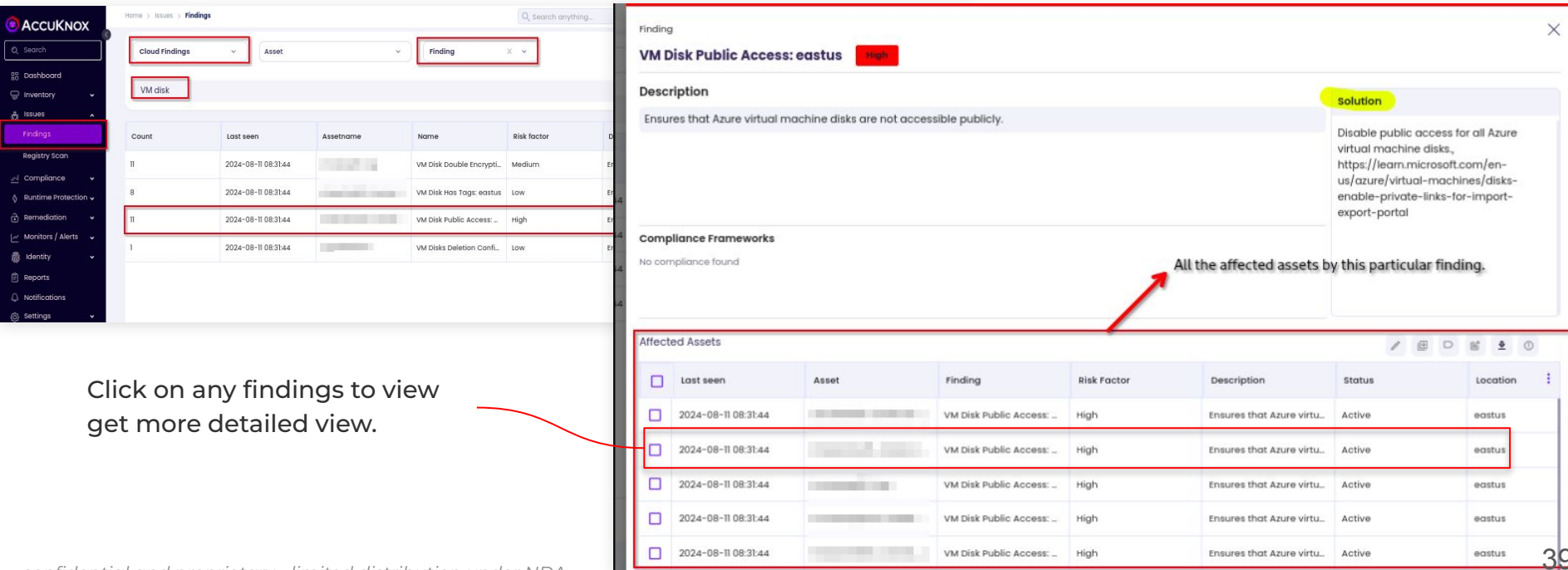


The screenshot displays the AccuKnox interface. On the left, a navigation sidebar includes 'Findings' (highlighted in purple). The main area shows a list of findings filtered by 'Cloud Findings' and 'DDoS'. A table lists findings with columns for 'Last seen', 'Assetname', 'Name', 'Risk factor', 'Description', and 'Status'. The 'Filter' panel on the right shows 'cloudsploit' as the asset type and 'azure_subscription' as the selected cloud type. A detailed view of a finding titled 'Public IP Address DDoS Protection: eastus' (Medium severity) is shown on the right. The description states: 'Ensures that DDoS IP Protection is enabled for Microsoft Azure Public IP Addresses'. The 'Details' panel on the far right includes a '+ Create Ticket' button, asset information (Asset Type: azure_public_ip, Status: Active), and a notes section.

Last seen	Assetname	Name	Risk factor	Description	Status
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	DDoS Standard Protect...	Low	Ensures that DDoS Stan...	Active
2024-08-11 03:29:26	[redacted]	DDoS Standard Protect...	Low	Ensures that DDoS Stan...	Active
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	DDoS Standard Protect...	Low	Ensures that DDoS Stan...	Active
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	Public IP Address DDoS ...	Medium	Ensures that DDoS IP Pr...	Active
2024-08-11 03:29:26	[redacted]	DDoS Standard Protect...	Low	Ensures that DDoS Stan...	Active

How to Identify if the VM Disks are not publicly accessible?

- To identify if the VM Disks are not publicly accessible in Azure Virtual Machine, Please navigate to Issues -> Findings
 - Select **Cloud Findings** in findings-type filter
 - Choose “Findings” in the group by filter
 - Also, User can directly search for the Assets/Findings from the Search field
 - To get more detailed information and ticket creation user can click on that particular findings



The screenshot displays the ACCUKNOX interface. On the left is a navigation sidebar with options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a 'Findings' list with columns for Count, Last seen, Assetname, Name, and Risk factor. One finding is highlighted with a red box. To the right, a detailed view of this finding is shown, including a description, a solution link, and a table of affected assets. A red arrow points from the text 'All the affected assets by this particular finding.' to the 'Affected Assets' table.

Click on any findings to view get more detailed view.

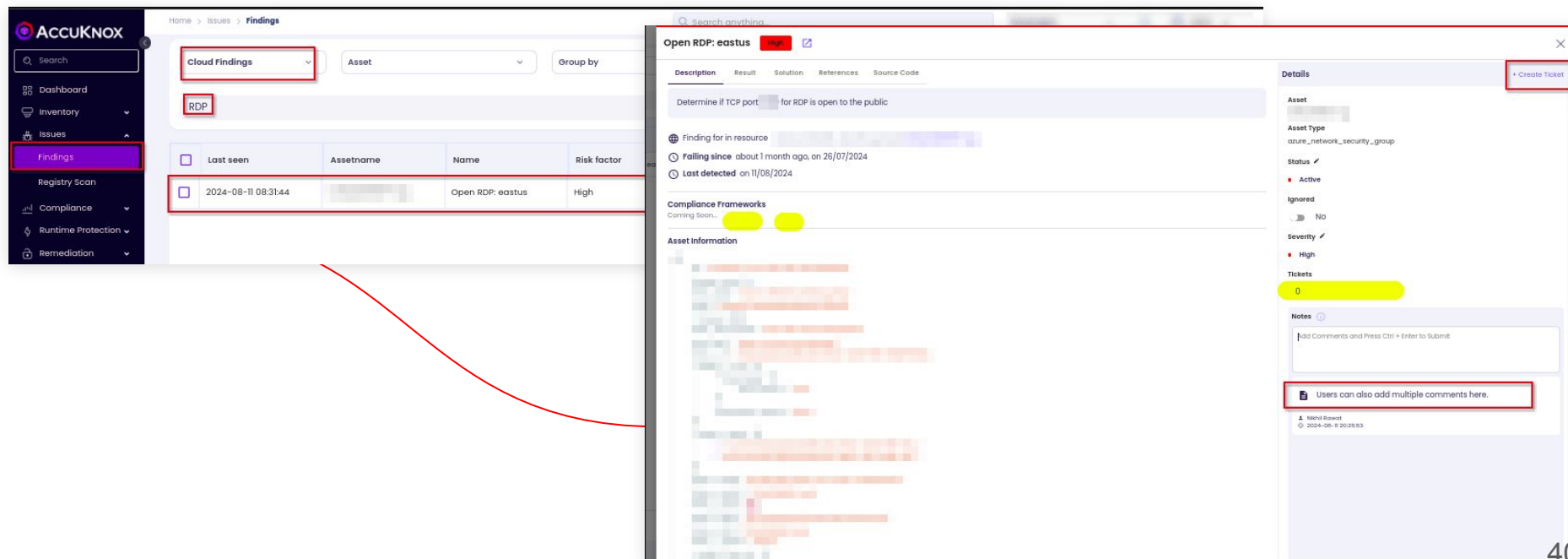
All the affected assets by this particular finding.

Count	Last seen	Assetname	Name	Risk factor
11	2024-08-11 08:31:44	[redacted]	VM Disk Double Encrypt...	Medium
8	2024-08-11 08:31:44	[redacted]	VM Disk Has Tags: eastus	Low
11	2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High
1	2024-08-11 08:31:44	[redacted]	VM Disks Deletion Confl...	Low

Last seen	Asset	Finding	Risk Factor	Description	Status	Location
2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High	Ensures that Azure virtu...	Active	eastus
2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High	Ensures that Azure virtu...	Active	eastus
2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High	Ensures that Azure virtu...	Active	eastus
2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High	Ensures that Azure virtu...	Active	eastus
2024-08-11 08:31:44	[redacted]	VM Disk Public Access: ...	High	Ensures that Azure virtu...	Active	eastus

How to Identify if the RDP Port is Open in Azure Network Security Group?

- To identify if the RDP port is open in Azure Network Security Groups, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.
 - Users can also add notes to a particular finding.



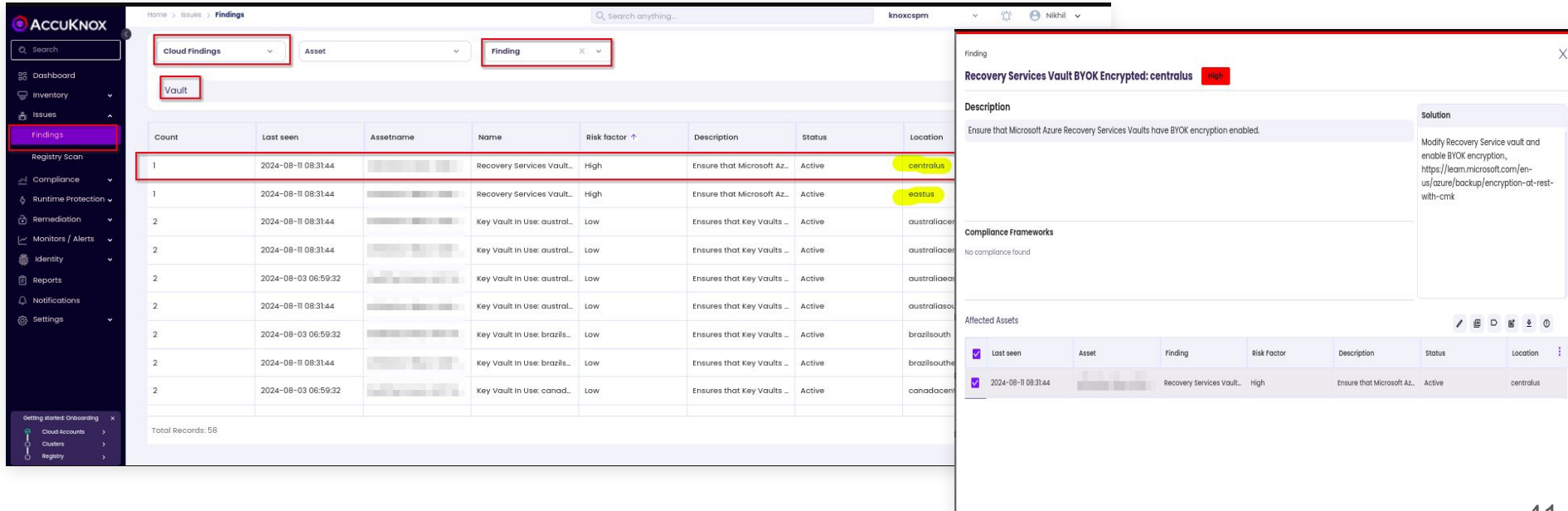
The screenshot displays the ACCUKNOX interface. On the left, a sidebar menu includes 'Findings' (highlighted in purple). The main area shows a 'Findings' view with filters for 'Cloud Findings' and 'RDP'. A table lists findings, with one entry for 'Open RDP: eastus' on '2024-08-11 08:31:44' with a 'High' risk factor. A red line connects this entry to a detailed view of the finding.

The detailed view for 'Open RDP: eastus' shows the following information:

- Description:** Determine if TCP port: [redacted] for RDP is open to the public
- Result:** Finding for in resource [redacted]
- Timeline:** Failing since about 1 month ago, on 26/07/2024; Last detected on 11/08/2024
- Compliance Frameworks:** Coming soon...
- Asset Information:** [redacted]
- Details:** Asset [redacted], Asset Type azure_network_security_group, Status Active, Ignored No, Severity High, Tickets 0.
- Notes:** A text input field with a red box around the instruction: 'Users can also add multiple comments here.'
- Buttons:** '+ Create Ticket' button (highlighted in red).

How to Identify if the Recovery Services Vault is Encrypted with BYOK in Azure?

- To identify if the Recovery Services Vault is encrypted with Bring Your Own Key (BYOK) in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - Choose Findings in the group by filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.



The screenshot displays the ACCUKNOX interface. On the left is a navigation sidebar with 'Findings' highlighted. The main area shows a 'Findings' page with filters for 'Cloud Findings', 'Asset', and 'Finding'. A table lists findings, with the first row highlighted in red. A modal window on the right shows details for the finding 'Recovery Services Vault BYOK Encrypted: centralus' with a 'High' risk level. The modal includes a description, a solution link, and a table of affected assets.

Count	Last seen	Assetname	Name	Risk factor ↑	Description	Status	Location
1	2024-08-11 08:31:44	[redacted]	Recovery Services Vault...	High	Ensure that Microsoft AZ...	Active	centralus
1	2024-08-11 08:31:44	[redacted]	Recovery Services Vault...	High	Ensure that Microsoft AZ...	Active	eastus
2	2024-08-11 08:31:44	[redacted]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiace
2	2024-08-11 08:31:44	[redacted]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiace
2	2024-08-03 06:59:32	[redacted]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiace
2	2024-08-11 08:31:44	[redacted]	Key Vault In Use: austral...	Low	Ensures that Key Vaults ...	Active	australiace
2	2024-08-03 06:59:32	[redacted]	Key Vault In Use: brazil...	Low	Ensures that Key Vaults ...	Active	brazilouth
2	2024-08-11 08:31:44	[redacted]	Key Vault In Use: brazil...	Low	Ensures that Key Vaults ...	Active	brazilouth
2	2024-08-03 06:59:32	[redacted]	Key Vault In Use: canad...	Low	Ensures that Key Vaults ...	Active	canadacenc

Total Records: 58

Finding: Recovery Services Vault BYOK Encrypted: centralus High

Description: Ensure that Microsoft Azure Recovery Services Vaults have BYOK encryption enabled.

Solution: Modify Recovery Service vault and enable BYOK encryption, <https://learn.microsoft.com/en-us/azure/backup/encryption-at-rest-with-cmk>

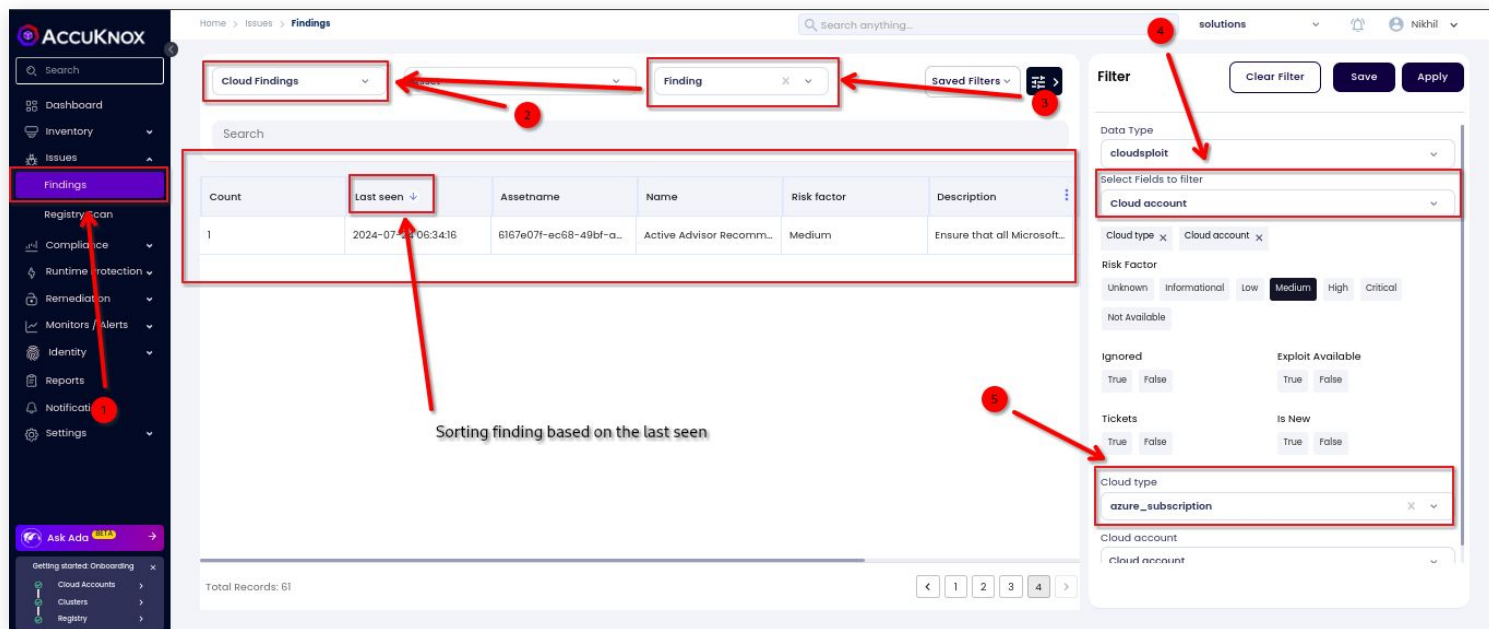
Compliance Frameworks: No compliance found.

Affected Assets:

Last seen	Asset	Finding	Risk Factor	Description	Status	Location
2024-08-11 08:31:44	[redacted]	Recovery Services Vault...	High	Ensure that Microsoft AZ...	Active	centralus

How to Identify if the SQL Server Firewall Rule Alerts Monitor is enabled in Azure?

- To identify if the SQL Server Firewall Rule Alerts Monitor is enabled in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - Choose Findings in the group by filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.
 - User can also sort the findings based on various parameters like last seen, affected assets count etc.

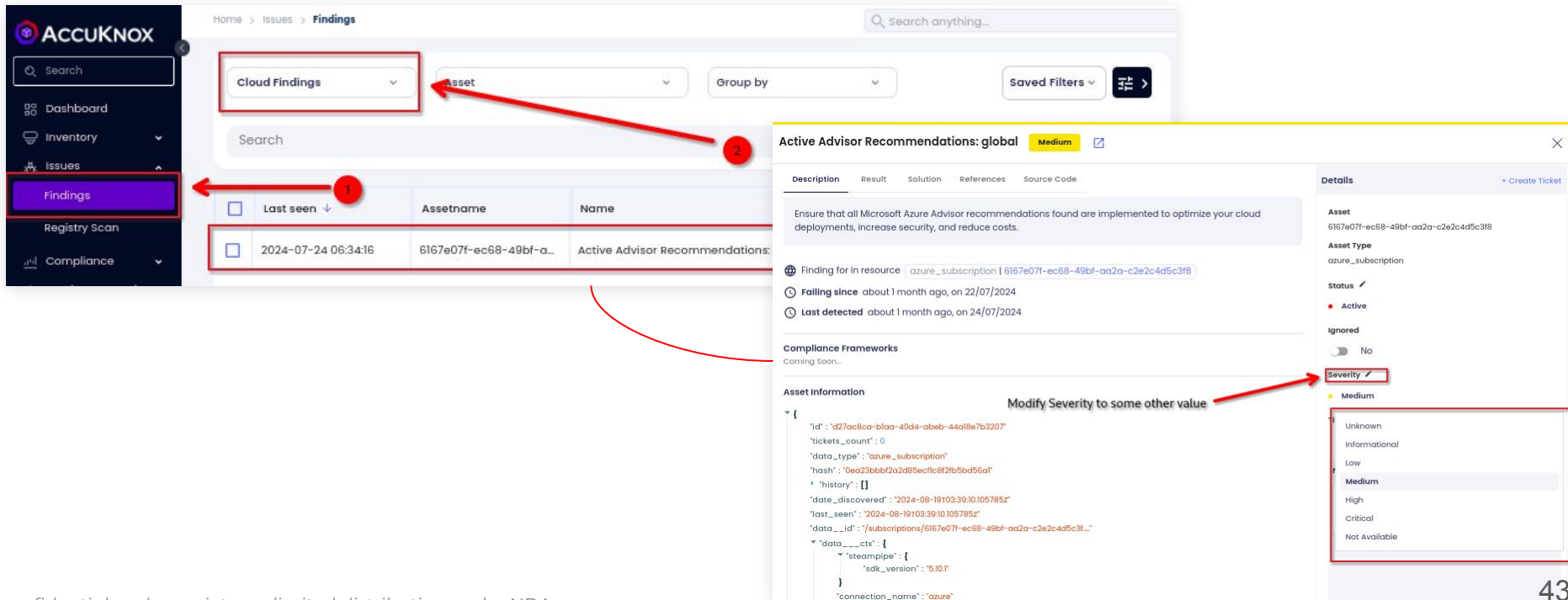


The screenshot shows the ACCUKNOX interface for the 'Findings' section. The left sidebar contains navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, and Notifications. The main area displays a table of findings with columns for Count, Last seen, Assetname, Name, Risk factor, and Description. A red box highlights the 'Last seen' column header, with an arrow pointing to it and the text 'Sorting finding based on the last seen'. The right sidebar shows a 'Filter' panel with various options like Data Type (cloudsploit), Select Fields to filter (Cloud account), Risk Factor (Medium), Ignored, Exploit Available, Tickets, and Its New. Red arrows and boxes highlight specific elements: 'Cloud Findings' in the filter, 'Finding' in the group by filter, 'Last seen' in the table header, and 'Cloud account' in the filter panel. A red circle with the number '1' is placed near the 'Findings' menu item in the sidebar.

Count	Last seen ↓	Assetname	Name	Risk factor	Description
1	2024-07-24T06:34:16	6167e07f-ec68-49bf-a...	Active Advisor Recomm...	Medium	Ensure that all Microsoft...

How to Identify if the Microsoft Azure Advisor recommendations are implemented in Azure?

- To identify if the Microsoft Azure Advisor recommendations are implemented in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.



The screenshot displays the ACCUKNOX interface. On the left is a navigation sidebar with 'Findings' highlighted. The main area shows the 'Findings' page with a filter set to 'Cloud Findings' and an 'Asset' dropdown. A table lists findings, with one entry for 'Active Advisor Recommendations: global' highlighted. A detailed view of this finding is shown on the right, including a description, finding details, and a 'Severity' dropdown menu. Red arrows and circles (1 and 2) indicate the steps described in the text.

Findings Table:

Last seen	Assetname	Name
2024-07-24 06:34:16	6167e07f-ec68-49bf-a...	Active Advisor Recommendations: global

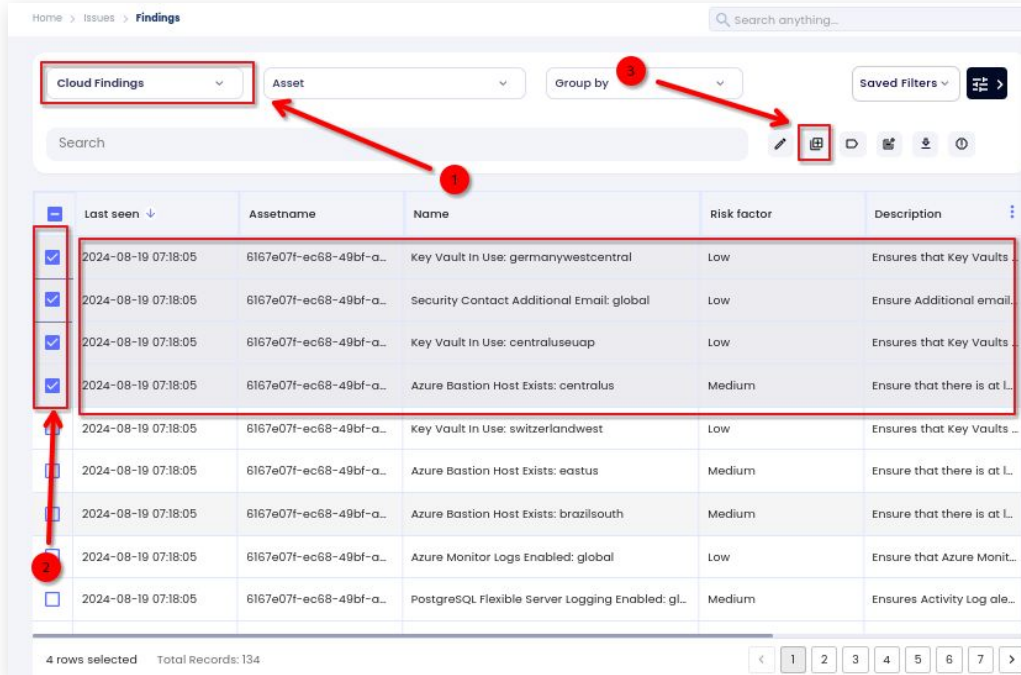
Active Advisor Recommendation Details:

- Description:** Ensure that all Microsoft Azure Advisor recommendations found are implemented to optimize your cloud deployments, increase security, and reduce costs.
- Finding for in resource:** azure_subscription | 6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8
- Falling since:** about 1 month ago, on 22/07/2024
- Last detected:** about 1 month ago, on 24/07/2024
- Severity:** Medium

```
{
  "id": "d27ac8ca-b1aa-40d4-abeb-44a18e7b3207",
  "tickets_count": 0,
  "data_type": "azure_subscription",
  "hash": "0ea23bbb12a2d85ec1c8f21b5bd56a1",
  "history": [],
  "date_discovered": "2024-08-19T03:39:10.105785Z",
  "last_seen": "2024-08-19T03:39:10.105785Z",
  "data_id": "/subscriptions/6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8...",
  "data_ctx": {
    "steampipe": {
      "sdk_version": "5.10.1"
    }
  },
  "connection_name": "azure"
}
```

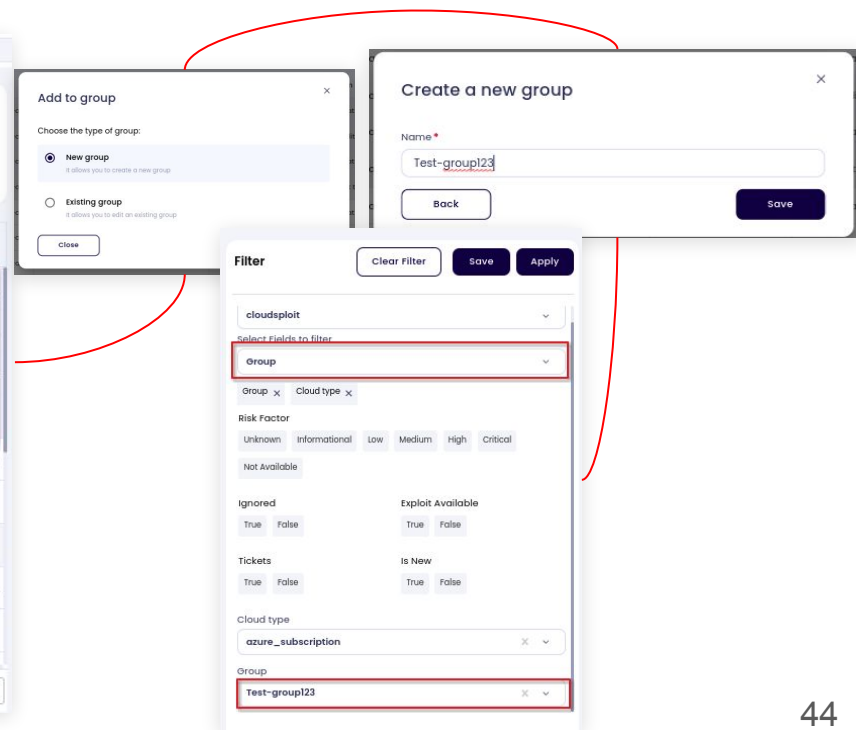
How to Group different findings together in Azure?

- To Group different findings together in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - After getting the specific finding user can select the findings and click on Group to group findings together.
 - Later user cfilter findings based on the created groups too.



The screenshot shows the Azure Findings interface. At the top, there are filters for 'Cloud Findings' (highlighted with a red box), 'Asset', and 'Group by'. A search bar is also present. Below the filters is a table of findings. The first four rows are selected, indicated by blue checkmarks in the leftmost column. A red box highlights these four rows. A red arrow points from the 'Group by' dropdown to a 'Group' button (represented by a grid icon) in the toolbar. Another red arrow points from the 'Group' button to the 'Group by' dropdown. At the bottom left, a red circle highlights the '4 rows selected' status.

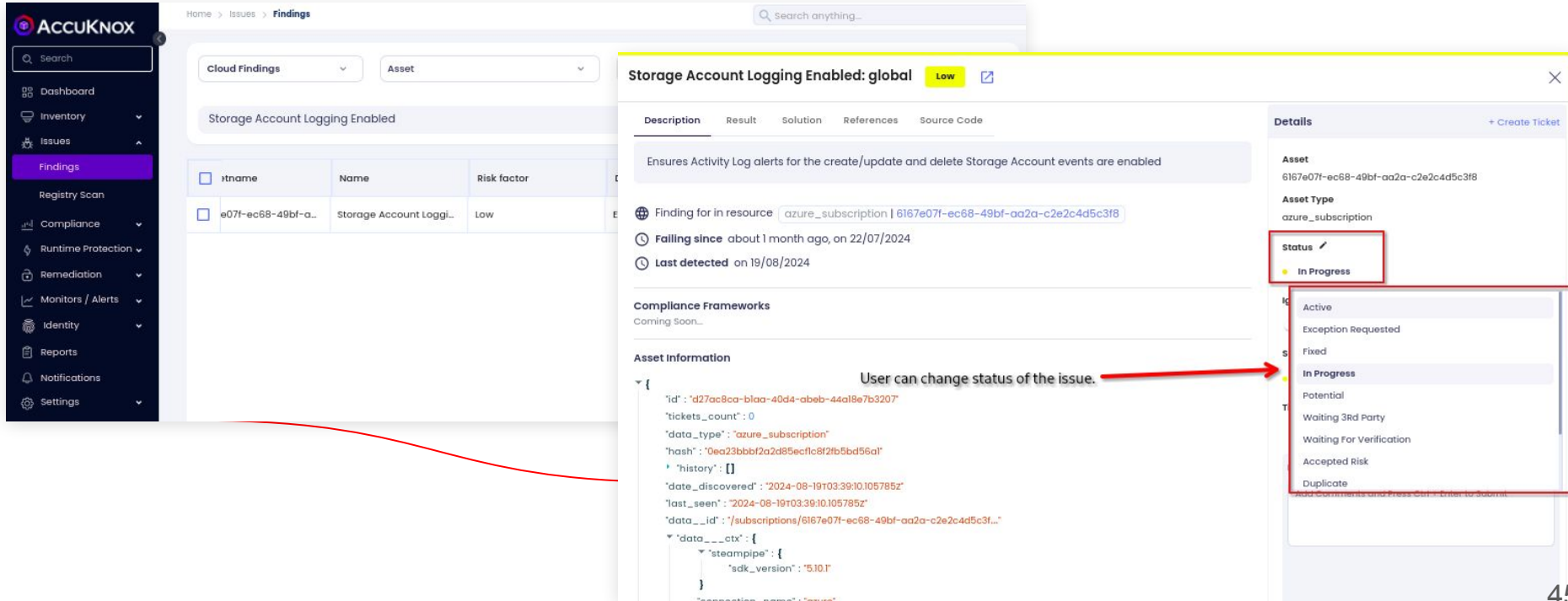
Last seen ↓	Assetname	Name	Risk factor	Description	
<input checked="" type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Key Vault In Use: germanywestcentral	Low	Ensures that Key Vaults ...
<input checked="" type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Security Contact Additional Email: global	Low	Ensure Additional email...
<input checked="" type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Key Vault In Use: centraluseuap	Low	Ensures that Key Vaults ...
<input checked="" type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: centralus	Medium	Ensure that there is at L...
<input type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Key Vault In Use: switzerlandwest	Low	Ensures that Key Vaults ...
<input type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: eastus	Medium	Ensure that there is at L...
<input type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: brazilsouth	Medium	Ensure that there is at L...
<input type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Monitor Logs Enabled: global	Low	Ensure that Azure Monit...
<input type="checkbox"/>	2024-08-19 07:18:05	6167e07f-ec68-49bf-a...	PostgreSQL Flexible Server Logging Enabled: gl...	Medium	Ensures Activity Log ale...



The screenshots show the workflow for creating a group. The 'Add to group' dialog has 'New group' selected. The 'Create a new group' dialog shows the name 'Test-group123'. The 'Filter' dialog shows the 'Group' filter applied, with 'Test-group123' selected in the dropdown.

How to Identify if the Storage Account Logging Enabled in Azure?

- To identify if the Storage Account Logging Enabled in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.



The screenshot displays the ACCUKNOX interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main content area shows a search bar and filters for 'Cloud Findings' and 'Asset'. A table lists findings, with one entry for 'Storage Account Logging Enabled' (ID: e07f-ec68-49bf-a...) and a 'Low' risk factor. A detailed view of this finding is shown, titled 'Storage Account Logging Enabled: global' with a 'Low' severity. The description states: 'Ensures Activity Log alerts for the create/update and delete Storage Account events are enabled'. It includes a resource ID, a 'Failing since' date of 22/07/2024, and a 'Last detected' date of 19/08/2024. A red arrow points to the 'Status' dropdown menu, which is open and shows options: Active, Exception Requested, Fixed, In Progress (selected), Potential, Waiting 3rd Party, Waiting For Verification, Accepted Risk, and Duplicate. A red box highlights the 'Status' dropdown and its options. A red arrow points to the 'In Progress' option with the text 'User can change status of the issue.'

Storage Account Logging Enabled: global Low

Description Result Solution References Source Code

Ensures Activity Log alerts for the create/update and delete Storage Account events are enabled

Finding for in resource `azure_subscription | 6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8`

Failing since about 1 month ago, on 22/07/2024

Last detected on 19/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "d27ac8ca-b1aa-40d4-abeb-44a18e7b3207"
  "tickets_count": 0
  "data_type": "azure_subscription"
  "hash": "0ea23bbbf2a2d85ecf08f2b5bd56a1"
  "history": []
  "date_discovered": "2024-08-19T03:39:10.105785Z"
  "last_seen": "2024-08-19T03:39:10.105785Z"
  "data__id": "/subscriptions/6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8..."
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.1"
    }
  }
  "connection_name": "azure"
}
```

Details [+ Create Ticket](#)

Asset
6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8

Asset Type
azure_subscription

Status [✎](#)

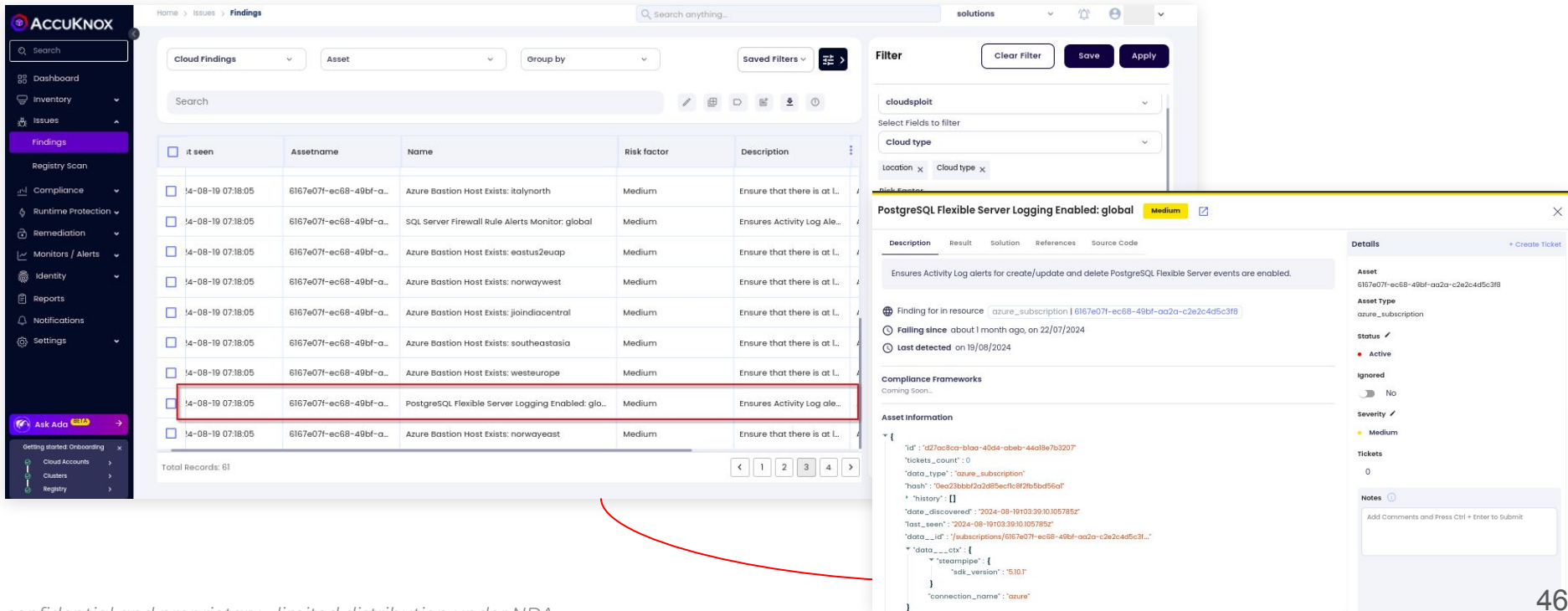
- In Progress
- Active
- Exception Requested
- Fixed
- In Progress
- Potential
- Waiting 3rd Party
- Waiting For Verification
- Accepted Risk
- Duplicate

Add comments and Press Ctrl+Enter to Submit

User can change status of the issue.

How to Identify if the PostgreSQL Flexible Server Logging Enabled in Azure?

- To identify if the postgresQL Flexible Server Logging Enabled in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - You can also directly search for the specific Assets/Findings using the Search field.
 - For more detailed information and to create a ticket, click on the particular finding.



The screenshot displays the AccuKnox interface. On the left is a navigation sidebar with 'Findings' selected. The main area shows a table of findings under the 'Cloud Findings' filter. A red box highlights a finding with the description 'PostgreSQL Flexible Server Logging Enabled: glo...'. A red arrow points from this finding to a detailed view on the right.

it seen	Assetname	Name	Risk factor	Description	
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: italnorth	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	SQL Server Firewall Rule Alerts Monitor: global	Medium	Ensures Activity Log Ale...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: eastus2euap	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: norwaywest	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: jiaidiacentral	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: southeastasia	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: westeurope	Medium	Ensure that there is at L...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	PostgreSQL Flexible Server Logging Enabled: glo...	Medium	Ensures Activity Log ale...
<input type="checkbox"/>	14-08-19 07:18:05	6167e07f-ec68-49bf-a...	Azure Bastion Host Exists: norwayeast	Medium	Ensure that there is at L...

PostgreSQL Flexible Server Logging Enabled: global Medium

Description

Result	Solution	References	Source Code
Ensures Activity Log alerts for create/update and delete PostgreSQL Flexible Server events are enabled.			

Details

Asset
6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8

Asset Type
azure_subscription

Status
Active

Ignored
No

Severity
Medium

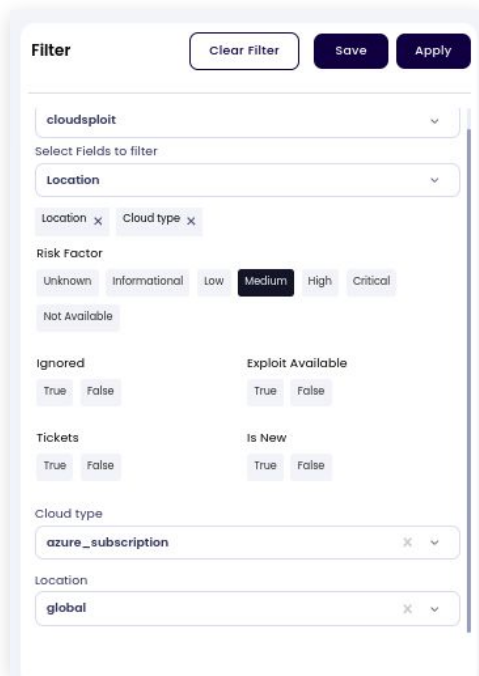
Tickets
0

Notes
Add Comments and Press Ctrl + Enter to Submit

```
{
  "id": "d27a68ca-b1aa-4d54-8beb-44a8e7b3207",
  "tickets_count": 0,
  "data_type": "azure_subscription",
  "hash": "0e023bbb02a2d85ecf8f2b5bd56af",
  "history": [],
  "date_discovered": "2024-08-19T03:30:10.105785Z",
  "last_seen": "2024-08-19T03:30:10.105785Z",
  "data__id": "/subscriptions/6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8...",
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.1",
      "connection_name": "azure"
    }
  }
}
```

How to Identify all the findings within the Global region in Azure?

- To identify all the findings within the Global region in Azure, please navigate to Issues -> Findings.
 - Select **Cloud Findings** in the findings-type filter.
 - In the advanced filter add location, then select Global region in location and apply it.
 - For more detailed information and to create a ticket, click on the particular finding.



Filter Clear Filter Save Apply

cloudsploit

Select Fields to filter

Location

Location x Cloud type x

Risk Factor

Unknown Informational Low **Medium** High Critical

Not Available

Ignored Exploit Available

True False True False

Tickets Is New

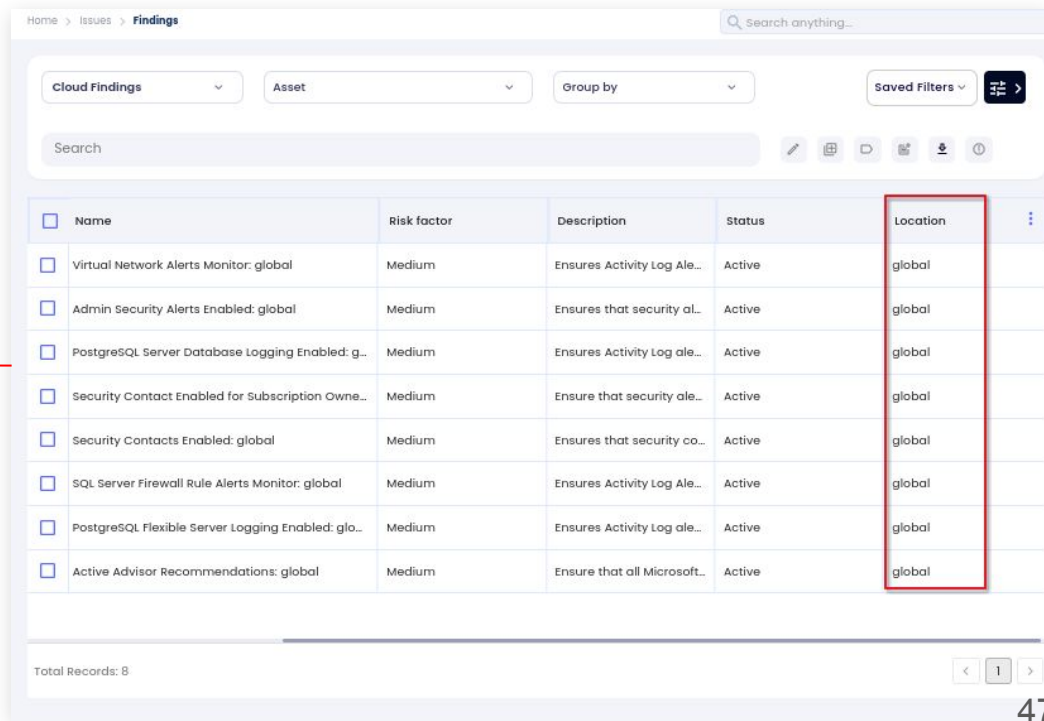
True False True False

Cloud type

azure_subscription x

Location

global x



Home > Issues > Findings

Search anything...

Cloud Findings Asset Group by Saved Filters

Search

<input type="checkbox"/>	Name	Risk factor	Description	Status	Location	
<input type="checkbox"/>	Virtual Network Alerts Monitor: global	Medium	Ensures Activity Log Ale...	Active	global	
<input type="checkbox"/>	Admin Security Alerts Enabled: global	Medium	Ensures that security aL...	Active	global	
<input type="checkbox"/>	PostgreSQL Server Database Logging Enabled: g...	Medium	Ensures Activity Log ale...	Active	global	
<input type="checkbox"/>	Security Contact Enabled for Subscription Owne...	Medium	Ensure that security ale...	Active	global	
<input type="checkbox"/>	Security Contacts Enabled: global	Medium	Ensures that security co...	Active	global	
<input type="checkbox"/>	SQL Server Firewall Rule Alerts Monitor: global	Medium	Ensures Activity Log Ale...	Active	global	
<input type="checkbox"/>	PostgreSQL Flexible Server Logging Enabled: glo...	Medium	Ensures Activity Log ale...	Active	global	
<input type="checkbox"/>	Active Advisor Recommendations: global	Medium	Ensure that all Microsoft...	Active	global	

Total Records: 8

< 1 >

Compliance failure for Azure CIS Benchmark v2.0.0

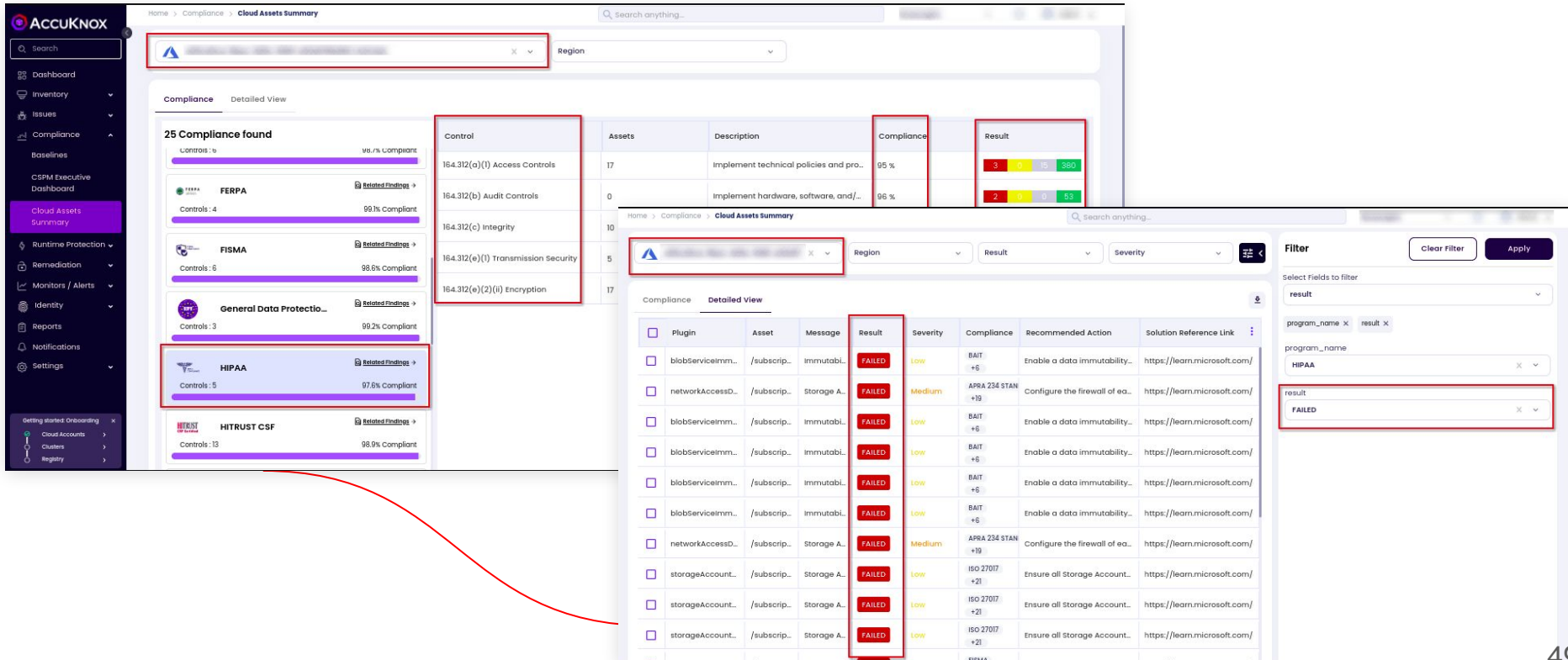
- To Identify CIS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary
- After that choose the cloud account for which you want to assess the compliance posture.

The screenshot shows the AccuKnox Compliance dashboard. The left sidebar contains navigation options: Dashboard, Inventory, Issues, Compliance, CSPM Executive Dashboard, Cloud Assets Summary (highlighted), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main content area is titled 'Compliance Detailed View' and shows a list of compliance standards. The 'Azure CIS Benchmark v2.0.0' standard is highlighted with a red box, showing 77 controls and 98.5% compliance. Below this, a table lists specific control failures, also highlighted with a red box. The table has columns for Control, Assets, Description, Compliance, and Result.

Control	Assets	Description	Compliance	Result
1.23 Ensure That No Custom Subscripti...	0	The principle of least privilege should ...	100 %	0 0 0 1
1.5 Ensure Guest Users Are Reviewed o...	0	Azure AD is extended to include Azure ...	100 %	0 0 0 1
2.1.11 Ensure That Microsoft Defender f...	1	Microsoft Defender for DNS scans all n...	0 %	1 0 0 0
2.1.15 Ensure that Auto provisioning of ...	1	Enable automatic provisioning of the ...	0 %	1 0 0 0
2.1.19 Ensure Additional email address...	0	Microsoft Defender for Cloud emails t...	0 %	1 0 0 0
2.1.5 Ensure That Microsoft Defender f...	1	Turning on Microsoft Defender for SQL...	0 %	1 0 0 0
2.1.7 Ensure That Microsoft Defender fo...	1	Turning on Microsoft Defender for Stor...	0 %	1 0 0 0
2.1.8 Ensure That Microsoft Defender f...	1	Turning on Microsoft Defender for Co...	0 %	1 0 0 0
3.1.1 Ensure Soft Delete is Enabled for A...	5	The Azure Storage blobs contain data...	91 %	5 0 0 52
3.1.5 Ensure the "Minimum TLS version" ...	5	In some cases, Azure Storage sets the...	98 %	1 0 0 56
3.1 Ensure that Secure transfer require...	5	Enable data encryption in transit.	98 %	1 0 0 56

Compliance failure for HIPAA Benchmark v2.0.0

- To Identify HIPAA failed compliance checks > Navigate to Compliance and select Cloud Asset Summary
- After that choose the cloud account for which you want to assess the compliance posture.



The screenshot displays the AccuKnox Compliance Cloud Assets Summary interface. The left sidebar shows navigation options, with 'Cloud Assets Summary' selected. The main content area shows a summary of 25 compliance findings, including FERPA, FISMA, General Data Protection, HIPAA, and HITRUST CSF. The HIPAA section is highlighted, showing 5 controls with 97.6% compliance. A detailed view of the HIPAA controls is shown, listing 17 assets with their respective messages, results, and severities. The results are categorized as FAILED, with severities ranging from Low to Medium. A filter panel on the right shows the 'result' filter set to 'FAILED'.

Control	Assets	Description	Compliance	Result
164.312(a)(1) Access Controls	17	Implement technical policies and pro...	95 %	3 0 15 80
164.312(b) Audit Controls	0	Implement hardware, software, and/...	96 %	2 0 0 98
164.312(c) Integrity	10			
164.312(e)(1) Transmission Security	5			
164.312(e)(2)(i) Encryption	17			

Plugin	Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
networkAccessD...	/subscrip...	Storage A...	FAILED	Medium	APRA 234 STAN +19	Configure the firewall of ea...	https://learn.microsoft.com/
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
blobServiceImm...	/subscrip...	Immutable...	FAILED	Low	BAIT +6	Enable a data immutability...	https://learn.microsoft.com/
networkAccessD...	/subscrip...	Storage A...	FAILED	Medium	APRA 234 STAN +19	Configure the firewall of ea...	https://learn.microsoft.com/
storageAccount...	/subscrip...	Storage A...	FAILED	Low	ISO 27017 +21	Ensure all Storage Account...	https://learn.microsoft.com/
storageAccount...	/subscrip...	Storage A...	FAILED	Low	ISO 27017 +21	Ensure all Storage Account...	https://learn.microsoft.com/
storageAccount...	/subscrip...	Storage A...	FAILED	Low	ISO 27017 +21	Ensure all Storage Account...	https://learn.microsoft.com/

Compliance failure for ISO 27001 Benchmark

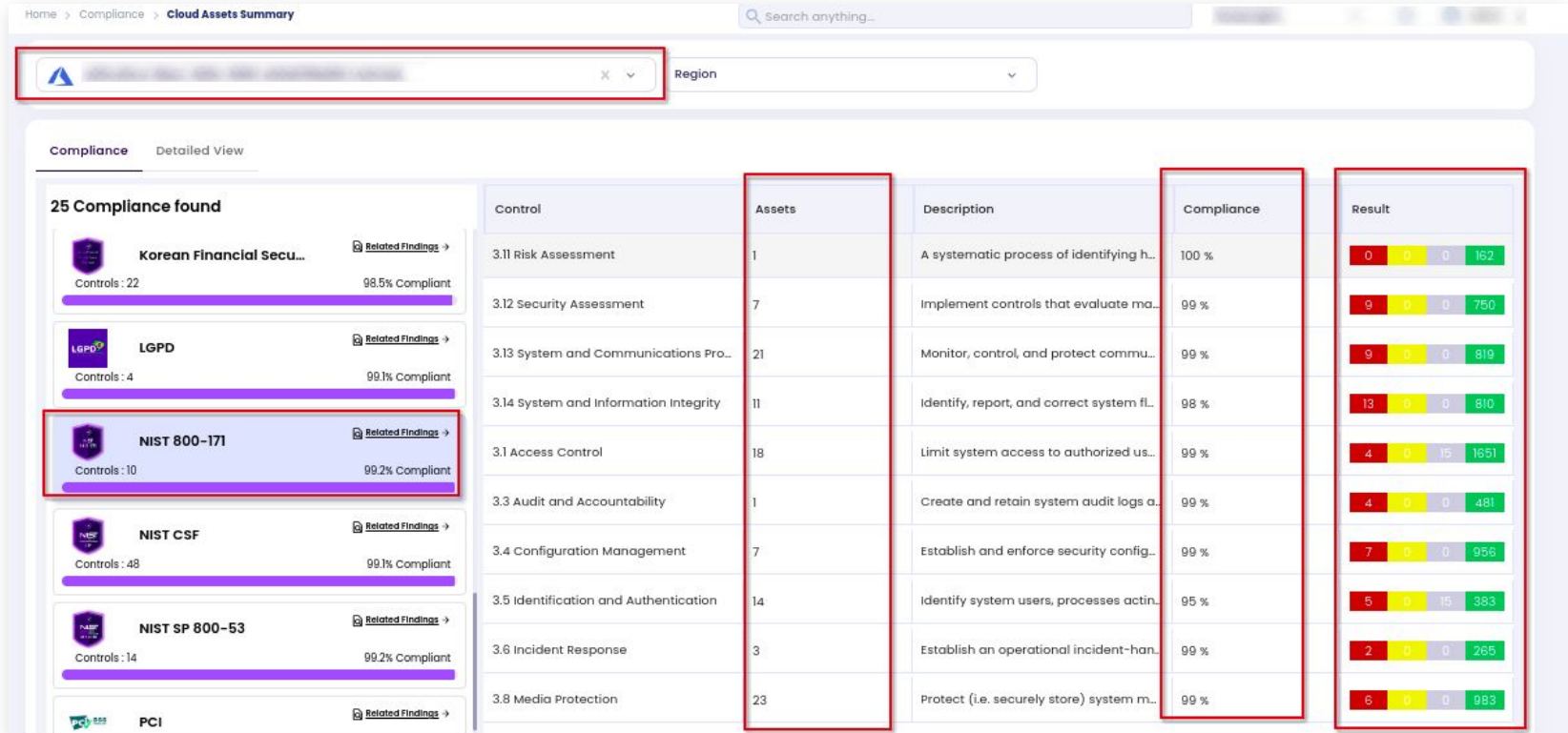
- To Identify ISO 27001 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary
- After that choose the cloud account for which you want to assess the compliance posture.

The screenshot displays the ACCUKNOX Compliance dashboard. On the left, a sidebar lists various compliance frameworks: General Data Protection..., HIPAA, HITRUST CSF, ISO 27001, ISO 27017, and ISO 27018. The ISO 27001 framework is highlighted with a red box, and its 'Related Findings' link is also highlighted. A red arrow points from this link to the 'Detailed View' of the ISO 27001 controls table on the right. The table lists controls such as 'A.10.1.1 Policy on the Use of Cryptograp...', 'A.12.1.3 Capacity Management', and 'A.12.4.3 Administrator and Operator lo...'. A red box highlights the 'Result' column in the table, which shows a summary of 5 failed, 9 passed, 0 not applicable, and 497 compliant assets. A text overlay 'To get more detailed view of controls' is positioned over the table.

Control	Assets	Description	Compliance	Result
A.10.1.1 Policy on the Use of Cryptograp...	17	A policy on the use of cryptographic c...	99 %	5 Failed, 9 Passed, 0 Not Applicable, 497 Compliant
A.12.1.3 Capacity Management	1	The use of resources shall be monitor...	0 %	
A.12.2.1 Controls Against Malware	7	Detection, prevention and recovery c...	100 %	
A.12.4.1 Event Logging	3	Event logs recording user activities, ex...	0 %	
A.12.4.2 Protection of Log Information	0	Logging facilities and log information ...	100 %	
A.12.4.3 Administrator and Operator lo...	0	System administrator and system op...	0 %	
A.12.5.1 Installation of Software on Ope...	0	Procedures shall be implemented to ...	0 %	
A.12.6.1 Management of Systems Audit...	1	Information about technical vulnerab...	100 %	
A.12.6.2 Restrictions on Software Install...	0	Rules governing the installation of sof...	0 %	
A.12.7.1 Information Systems Audit Con...	1	Audit requirements and activities inv...	99 %	

Compliance failure for NIST 800-171 Benchmark

- To Identify NIST 800-171 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary
- After that choose the cloud account for which you want to assess the compliance posture.



The screenshot displays the 'Cloud Assets Summary' page in the AccuKnox interface. The breadcrumb trail is 'Home > Compliance > Cloud Assets Summary'. A search bar is present at the top right. Below the breadcrumb, there is a dropdown menu for selecting a cloud account (highlighted with a red box) and a 'Region' dropdown. The main content area is titled 'Compliance Detailed View' and shows a summary of 25 compliance frameworks found. On the left, a list of frameworks includes Korean Financial Security, LGPD, NIST 800-171 (highlighted with a red box), NIST CSF, NIST SP 800-53, and PCI. The NIST 800-171 entry shows 10 controls and 99.2% compliance. The main table lists specific controls, the number of assets, descriptions, and compliance percentages. The 'Assets' column (highlighted with a red box) shows values ranging from 1 to 23. The 'Compliance' column (highlighted with a red box) shows percentages from 95% to 100%. The 'Result' column (highlighted with a red box) displays a bar chart with counts for 'Pass', 'Fail', 'Warning', and 'Info' statuses, along with a total count. For example, for '3.1 Risk Assessment', there are 0 fails, 0 warnings, 0 info, and 162 passes.

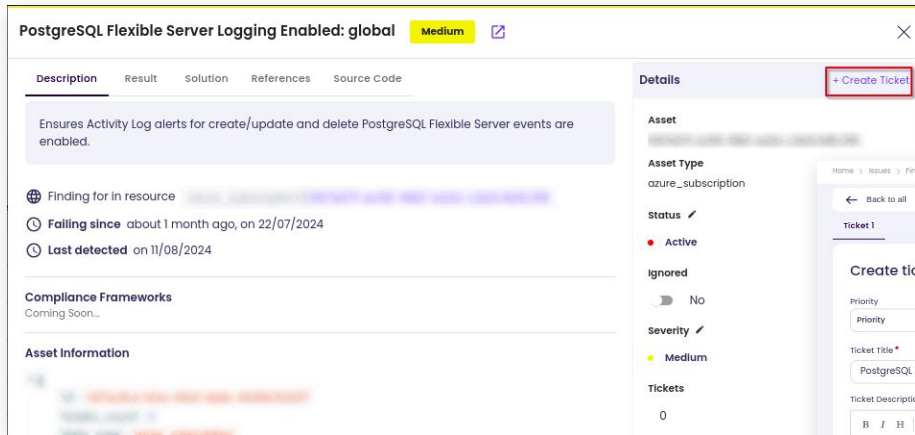
Control	Assets	Description	Compliance	Result
3.1.1 Risk Assessment	1	A systematic process of identifying h...	100 %	0 0 0 162
3.1.2 Security Assessment	7	Implement controls that evaluate ma...	99 %	9 0 0 750
3.1.3 System and Communications Pro...	21	Monitor, control, and protect commu...	99 %	9 0 0 819
3.1.4 System and Information Integrity	11	Identify, report, and correct system fl...	98 %	13 0 0 810
3.1 Access Control	18	Limit system access to authorized us...	99 %	4 0 0 15 1651
3.3 Audit and Accountability	1	Create and retain system audit logs a...	99 %	4 0 0 481
3.4 Configuration Management	7	Establish and enforce security config...	99 %	7 0 0 956
3.5 Identification and Authentication	14	Identify system users, processes actin...	95 %	5 0 0 15 383
3.6 Incident Response	3	Establish an operational incident-han...	99 %	2 0 0 265
3.8 Media Protection	23	Protect (i.e. securely store) system m...	99 %	6 0 0 983

Assistive Remediation For Azure Risks

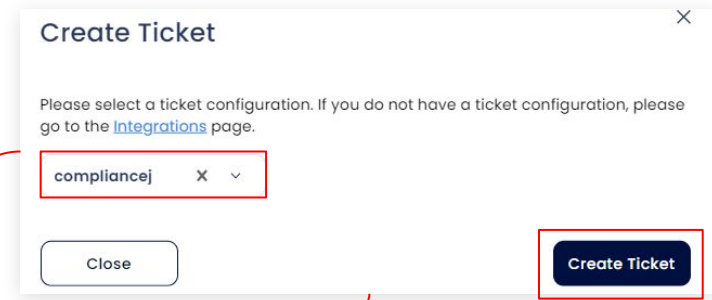
AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 1)

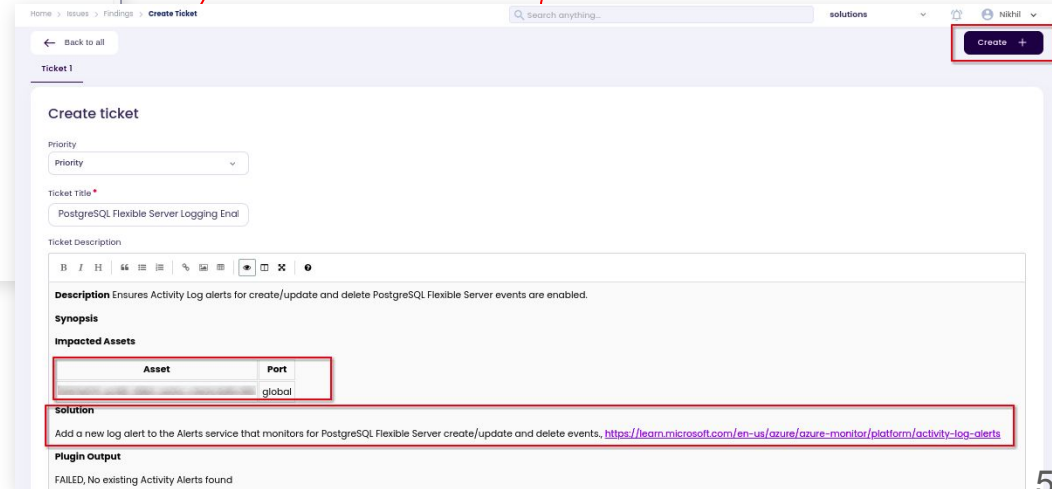
- Navigate to Issues > Findings
- Select the finding and create a ticket for it



The screenshot shows a finding detail page for "PostgreSQL Flexible Server Logging Enabled: global" with a "Medium" severity. The "Details" tab is active, and a red box highlights the "+ Create Ticket" button. The finding description states: "Ensures Activity Log alerts for create/update and delete PostgreSQL Flexible Server events are enabled." It also shows the finding is "Falling since about 1 month ago, on 22/07/2024" and "Last detected on 11/08/2024".



The "Create Ticket" modal dialog is shown. It prompts the user to "Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page." A dropdown menu is open, showing "compliancej" selected. A red box highlights the "Create Ticket" button at the bottom right of the modal.

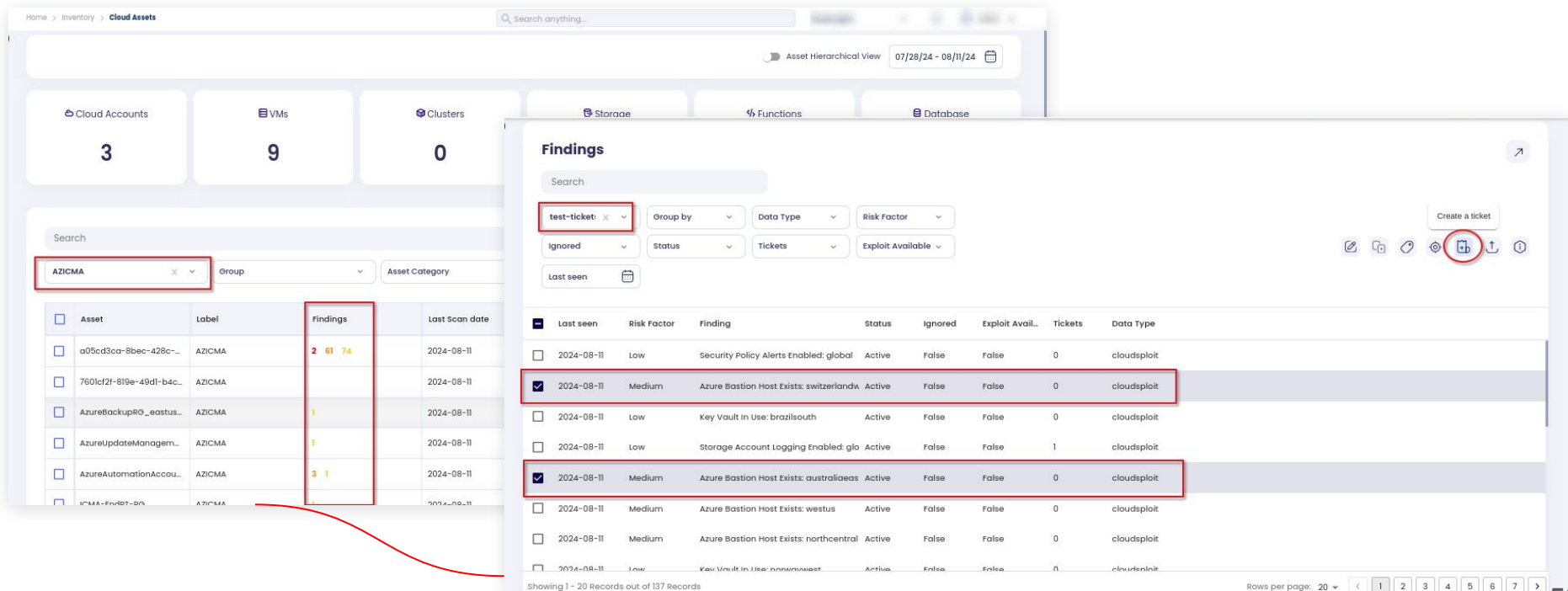


The "Create ticket" form is shown. The "Ticket Title" is "PostgreSQL Flexible Server Logging Enal". The "Ticket Description" field contains the finding description. The "Impacted Assets" table has one entry: "Asset" (redacted) and "Port" (global). A red box highlights the "Asset" field in the table. The "Solution" field contains the text: "Add a new log alert to the Alerts service that monitors for PostgreSQL Flexible Server create/update and delete events, <https://learn.microsoft.com/en-us/azure/azure-monitor/platform/activity-log-alerts>". The "Plugin Output" field shows "FAILED, No existing Activity Alerts found".

Assistive Remediation For Azure Risks

AccuKnox offers solution reference links to assist with the remediation
To Remediate the findings (Approach 2)

- Navigate to Inventory > Cloud Assets
- Select the finding and create a ticket for it



Home > Inventory > Cloud Assets

Asset Hierarchical View 07/28/24 - 08/11/24

Cloud Accounts 3 VMs 9 Clusters 0 Storage Functions Database

Search

AZICMA Group Asset Category

Asset	Label	Findings	Last Scan date
a05cd3ca-8bec-428c...	AZICMA	2 61 74	2024-08-11
7601cf2f-819e-49d1-b4c...	AZICMA		2024-08-11
AzureBackupRO_eastus...	AZICMA	1	2024-08-11
AzureUpdateManagem...	AZICMA	1	2024-08-11
AzureAutomationAccou...	AZICMA	3 1	2024-08-11
ICMA-Prod-BG	AZICMA		2024-08-11

Findings

Search

test-ticket: x Group by Data Type Risk Factor

Ignored Status Tickets Exploit Available

Last seen

Create a ticket

Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
2024-08-11	Low	Security Policy Alerts Enabled: global	Active	False	False	0	cloudsploit
2024-08-11	Medium	Azure Bastion Host Exists: switzerlandv	Active	False	False	0	cloudsploit
2024-08-11	Low	Key Vault in Use: brazilsoth	Active	False	False	0	cloudsploit
2024-08-11	Low	Storage Account Logging Enabled: glo	Active	False	False	1	cloudsploit
2024-08-11	Medium	Azure Bastion Host Exists: australiaeas	Active	False	False	0	cloudsploit
2024-08-11	Medium	Azure Bastion Host Exists: westus	Active	False	False	0	cloudsploit
2024-08-11	Medium	Azure Bastion Host Exists: northcentral	Active	False	False	0	cloudsploit
2024-08-11	Low	Key Vault in Use: newyorkasset	Active	False	False	0	cloudsploit

Showing 1 - 20 Records out of 137 Records

Rows per page: 20

Assistive Remediation For Azure Compliance Failure

AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 3)

- From the detailed view of Cloud Asset Summary
- Select the failed compliance and create a ticket for it

The screenshot displays the AccuKnox interface for managing Azure compliance. The left sidebar contains navigation options such as Dashboard, Inventory, Issues, Compliance, Baselines, CSPM Executive Dashboard, Cloud Assets Summary (highlighted), Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main content area shows a 'Cloud Assets Summary' table with columns for Plugin, Asset, and Message. A specific finding for 'storageAccountsHttps' is highlighted, showing a 'High' severity. The detailed view of this finding includes a description, a message, a solution reference link, and a list of compliance frameworks (including NIST, ISO 27001, HIPAA, etc.). A 'Recommended Actions' panel on the right suggests enabling the HTTPS-only option for all storage accounts, and a '+ Create Ticket' button is visible.

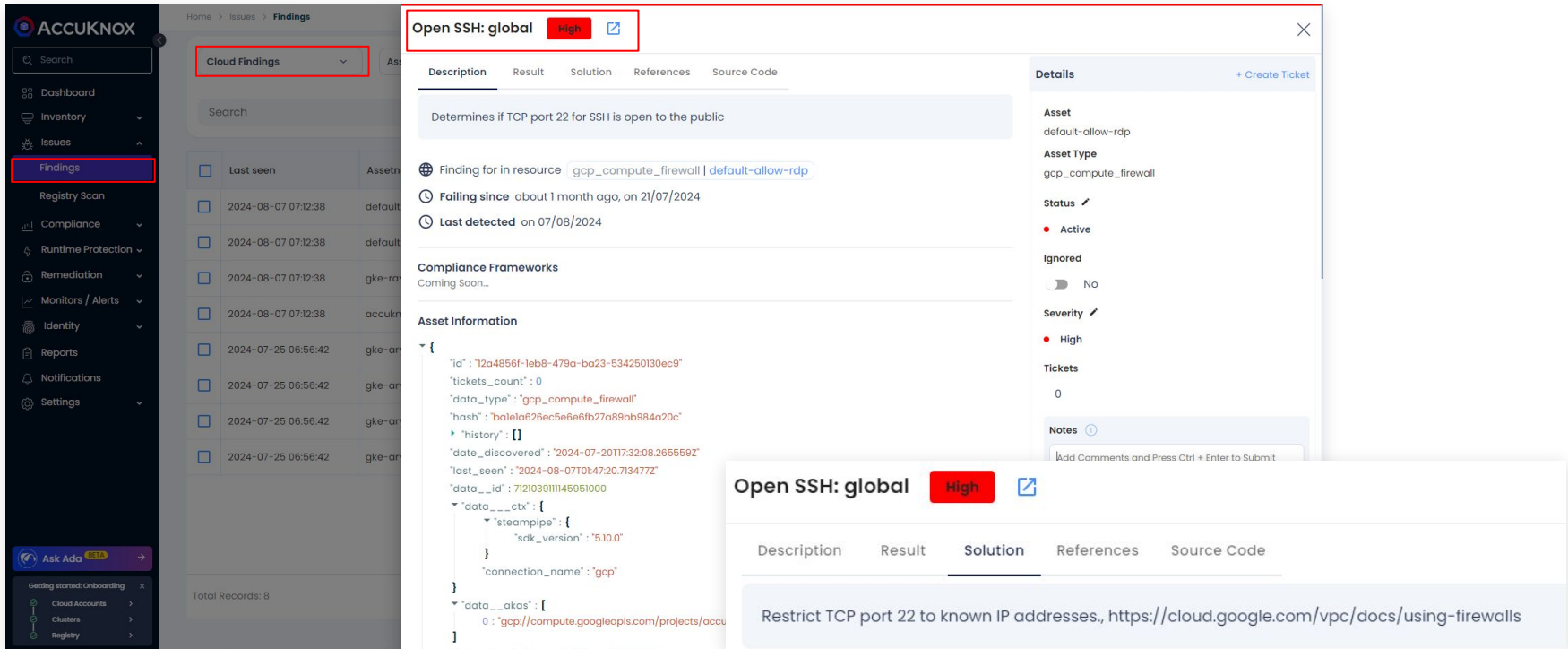


GCP Risk Assessment

Compliance failure and Misconfiguration

How to identify open SSH port?

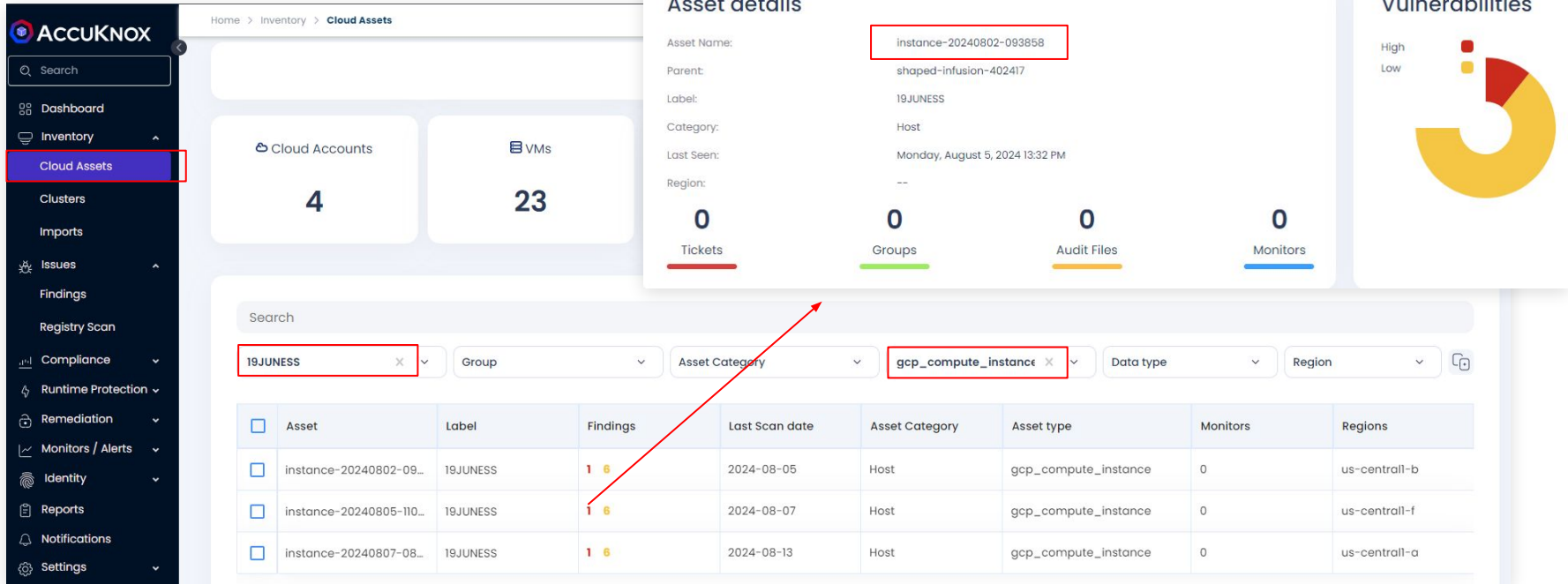
- To identify the if the SSH port open to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply Cloud Findings in the filter
 - Search for “open SSH” in the search field



The screenshot displays the AccuKnox interface. On the left is a dark sidebar with navigation items: Dashboard, Inventory, Issues, Findings (highlighted), Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. At the bottom of the sidebar is a 'Ask Ada' chatbot. The main area shows a breadcrumb path: Home > Issues > Findings. A search bar contains 'Open SSH: global' with a 'High' severity tag and a link icon. Below the search bar is a table of findings with columns for 'Last seen' and 'Assets'. The selected finding is expanded, showing a description: 'Determines if TCP port 22 for SSH is open to the public'. It also shows 'Finding for in resource: gcp_compute_firewall | default-allow-rdp', 'Failing since: about 1 month ago, on 21/07/2024', and 'Last detected: on 07/08/2024'. The 'Compliance Frameworks' section indicates 'Coming Soon...'. The 'Asset Information' section shows a JSON object with details like 'id', 'data_type', 'hash', 'date_discovered', 'last_seen', 'data_id', and 'connection_name'. The 'Severity' is set to 'High'. The 'Solution' section provides a link to Google Cloud documentation: 'Restrict TCP port 22 to known IP addresses., https://cloud.google.com/vpc/docs/using-firewalls'. A 'Details' panel on the right shows asset information, status (Active), and severity (High).

How to identify security issues related to compute instance?

- To identify the compute instance security issues with the Onboarded Cloud Account, Please navigate to Inventory -> Cloud Assets
 - Apply **GCP account label** in the filter
 - Choose **gcp_compute_instance** from the Asset Type filter
 - Click on the findings to view the details



Asset details

Asset Name: instance-20240802-093858
Parent: shaped-infusion-402417
Label: 19JUNESS
Category: Host
Last Seen: Monday, August 5, 2024 13:32 PM
Region: --


0 Tickets 0 Groups 0 Audit Files 0 Monitors

Search: 19JUNESS x Group Asset Category gcp_compute_instance x Data type Region

<input type="checkbox"/>	Asset	Label	Findings	Last Scan date	Asset Category	Asset type	Monitors	Regions
<input type="checkbox"/>	instance-20240802-09...	19JUNESS	1 5	2024-08-05	Host	gcp_compute_instance	0	us-central1-b
<input type="checkbox"/>	instance-20240805-110...	19JUNESS	1 5	2024-08-07	Host	gcp_compute_instance	0	us-central1-f
<input type="checkbox"/>	instance-20240807-08...	19JUNESS	1 5	2024-08-13	Host	gcp_compute_instance	0	us-central1-a

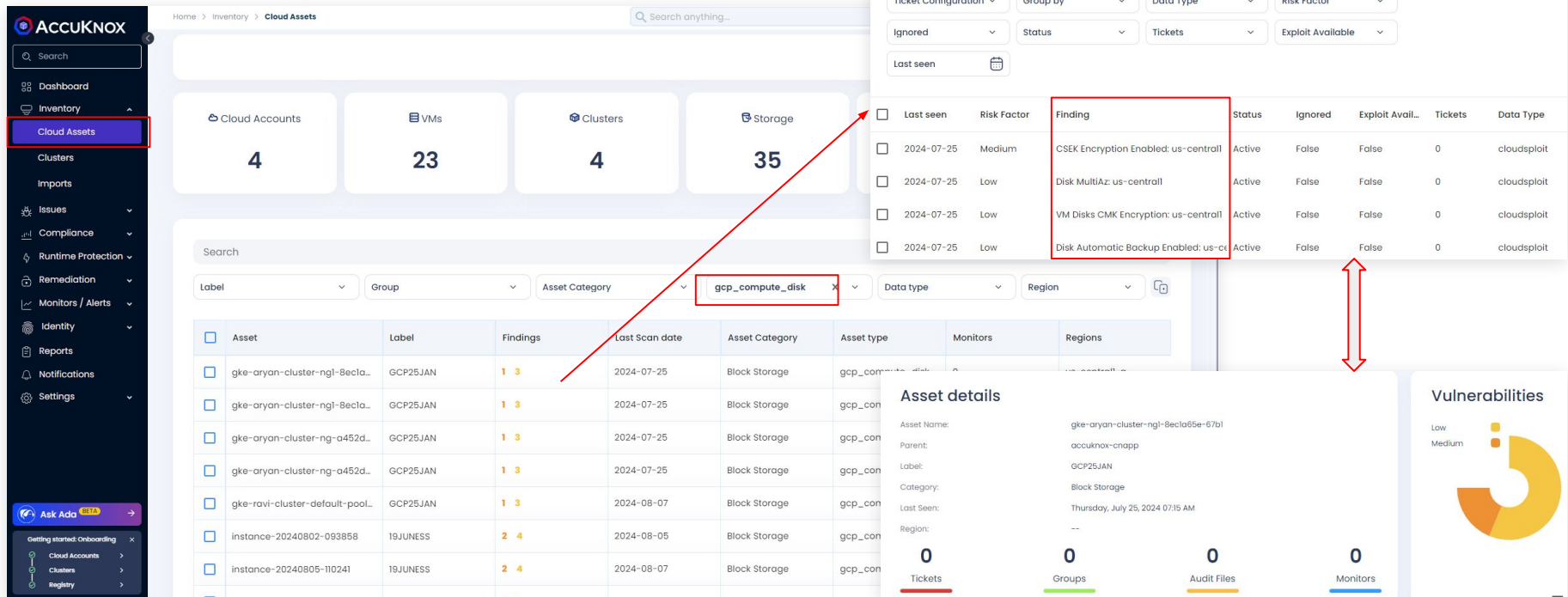
Vulnerabilities

High Low



Identify compute disk security issue for all the onboarded GCP account?

- To identify the compute instance security issues with the Onboarded Cloud Account, Please navigate to Inventory -> Cloud Assets
 - Choose **gcp_compute_disk** from the Asset Type filter
 - Click on the findings to view the details



The screenshot displays the ACCUKNOX interface. On the left is a dark sidebar with navigation options: Dashboard, Inventory (highlighted), Clusters, Imports, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows 'Cloud Assets' with four summary cards: Cloud Accounts (4), VMs (23), Clusters (4), and Storage (35). Below these is a search bar and filters for Label, Group, Asset Category, and Asset type (set to 'gcp_compute_disk'). A table lists assets with columns for Asset, Label, Findings, Last Scan date, Asset Category, Asset type, Monitors, and Regions. A red arrow points from the 'gcp_compute_disk' filter to a 'Findings' modal window. This modal shows a table of findings with columns: Last seen, Risk Factor, Finding, Status, Ignored, Exploit Avail., Tickets, and Data Type. A red box highlights the 'Finding' column. A red double-headed arrow points from the 'Findings' table to an 'Asset details' modal window. This modal shows details for asset 'gke-aryan-cluster-ng1-Becla85e-67bi', including Asset Name, Parent, Label, Category, Last Seen, and Region. At the bottom of the asset details are four summary cards: Tickets (0), Groups (0), Audit Files (0), and Monitors (0). On the right side of the interface, there is a 'Vulnerabilities' section with a donut chart showing 'Low' and 'Medium' risk levels.

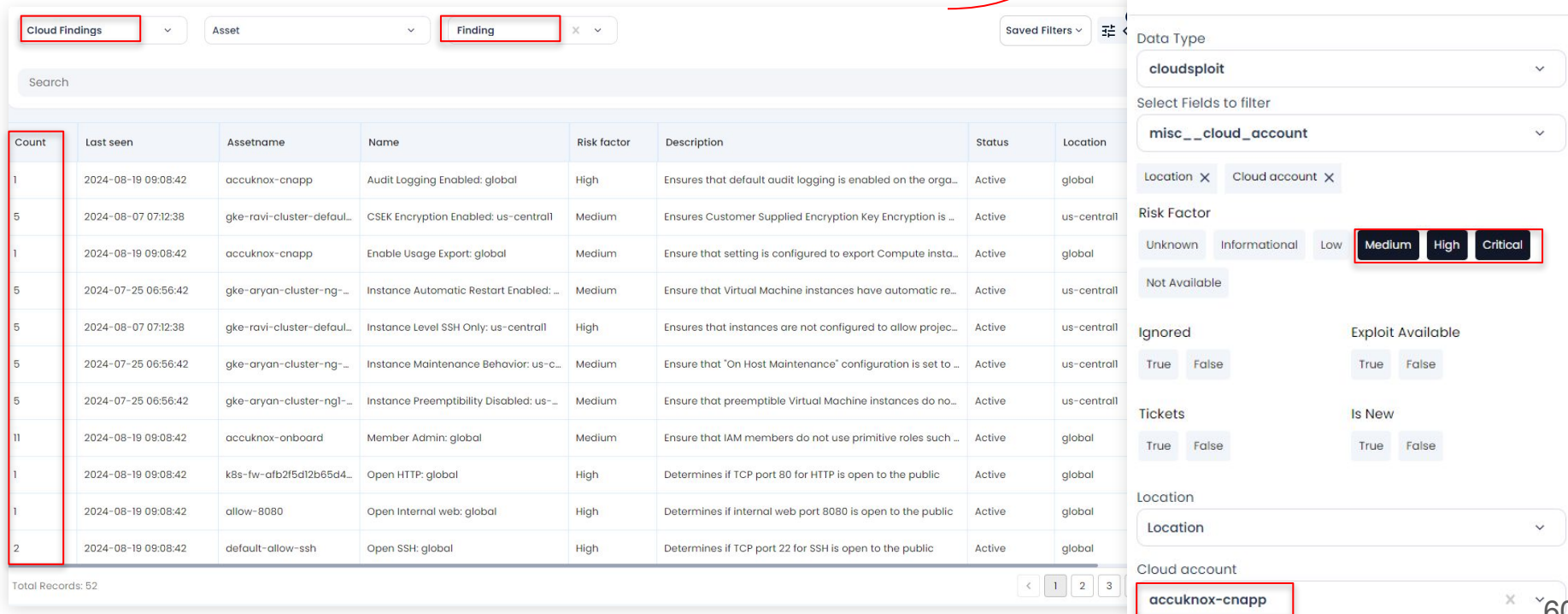
How to identify publicly exposed ports?

- To identify the if all the ports open to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply risk factor as “High”
 - Select the filters by cloud account

The screenshot displays the ACCUKNOX interface. On the left is a sidebar with navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a finding titled "Open All Ports: global" with a severity of "High". The finding description states: "Determines if all ports are open to the public". It includes details such as "Finding for in resource gcp_compute_firewall | aikow-all", "Failing since about 2 day ago, on 05/08/2024", and "Last detected on 07/08/2024". The asset information shows a JSON object with details like "id", "tickets_count", "data_type", "hash", "history", "date_discovered", "last_seen", "data_id", "data__ctx", "steampipe", "sdk_version", "connection_name", "data__akas", and "connection_name". A filter overlay is open on the right, showing "Filter" options. The "Data Type" is set to "cloudsploit", "Select Fields to filter" is "misc__cloud_account", "Risk Factor" is "High", and "Cloud account" is "shaped-infusion-402417".

How to identify unique findings impacting multiple assets?

- To identify the unique findings with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply **cloud account** filter and select severity as **Medium/High/Critical**
 - Apply **Group by findings** filter



The screenshot displays the Accuknox Findings interface. At the top, there are filter dropdowns for 'Cloud Findings', 'Asset', and 'Finding'. Below these is a search bar and a table of findings. The table has columns for Count, Last seen, Assetname, Name, Risk factor, Description, Status, and Location. A red box highlights the first column (Count) and the first row of data. To the right, a 'Filter' panel is open, showing various filter options. A red box highlights the 'Risk Factor' section, specifically the 'Medium', 'High', and 'Critical' buttons. Another red box highlights the 'Cloud account' filter at the bottom of the panel, which is set to 'accuknox-cnapp'. The 'Filter' panel also includes buttons for 'Clear Filter', 'Save', and 'Apply'.

Count	Last seen	Assetname	Name	Risk factor	Description	Status	Location
1	2024-08-19 09:08:42	accuknox-cnapp	Audit Logging Enabled: global	High	Ensures that default audit logging is enabled on the orga...	Active	global
5	2024-08-07 07:12:38	gke-ravi-cluster-defaul...	CSEK Encryption Enabled: us-centrall	Medium	Ensures Customer Supplied Encryption Key Encryption is ...	Active	us-central
1	2024-08-19 09:08:42	accuknox-cnapp	Enable Usage Export: global	Medium	Ensure that setting is configured to export Compute insta...	Active	global
5	2024-07-25 06:56:42	gke-aryan-cluster-ng-...	Instance Automatic Restart Enabled: ...	Medium	Ensure that Virtual Machine instances have automatic re...	Active	us-central
5	2024-08-07 07:12:38	gke-ravi-cluster-defaul...	Instance Level SSH Only: us-centrall	High	Ensures that instances are not configured to allow projec...	Active	us-central
5	2024-07-25 06:56:42	gke-aryan-cluster-ng-...	Instance Maintenance Behavior: us-c...	Medium	Ensure that "On Host Maintenance" configuration is set to ...	Active	us-central
5	2024-07-25 06:56:42	gke-aryan-cluster-ngl-...	Instance Preemptibility Disabled: us-...	Medium	Ensure that preemptible Virtual Machine instances do no...	Active	us-central
11	2024-08-19 09:08:42	accuknox-onboard	Member Admin: global	Medium	Ensure that IAM members do not use primitive roles such ...	Active	global
1	2024-08-19 09:08:42	k8s-fw-alb2f5dl2b65d4...	Open HTTP: global	High	Determines if TCP port 80 for HTTP is open to the public	Active	global
1	2024-08-19 09:08:42	allow-8080	Open Internal web: global	High	Determines if internal web port 8080 is open to the public	Active	global
2	2024-08-19 09:08:42	default-allow-ssh	Open SSH: global	High	Determines if TCP port 22 for SSH is open to the public	Active	global

Total Records: 52

Filter panel details:

- Clear Filter
- Save
- Apply
- Data Type: cloudsploit
- Select Fields to filter: misc__cloud_account
- Location: X Cloud account: X
- Risk Factor: Unknown, Informational, Low, **Medium**, **High**, **Critical**, Not Available
- Ignored: True, False; Exploit Available: True, False
- Tickets: True, False; Is New: True, False
- Location: Location
- Cloud account: **accuknox-cnapp**

How to identify multiple issues impacting single assets?

- To identify the unique findings with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply **Group by Asset** filter

The screenshot shows the ACCUKNOX interface with the 'Findings' section selected in the sidebar. The main view displays a table of findings and a detailed view of a specific asset.

Findings Table:

Count	Last seen	Assetname	Name	Risk
2	2024-08-19 08:23:45	k8s-fw-a211b58e851e94...	Open HTTP: global	High
11	2024-08-19 08:23:45	shaped-infusion-402417	Excessive Firewall Rules: global	Med
1	2024-08-19 08:23:45	API key 2	API Key Rotation: global	Low
2	2024-08-19 08:23:45	default	Private Access Enabled: europe-west2	Med
1	2024-08-19 08:23:45	79312ad245f75b0af32...	Service Account Managed Keys: glob...	Low
6	2024-08-05 13:23:07	instance-20240802-09...	Disk MultiAZ: us-central1	Low
1	2024-08-19 08:23:45	GAR-Testing	Member Admin: global	Med
1	2024-08-19 08:23:45	default	Flow Logs Enabled: us-east1	Low
2	2024-08-19 08:23:45	default	Private Access Enabled: asia-southe...	Med
2	2024-08-19 08:23:45	assetcovGCPdatasetBL...	Dataset Labels Added: global	Low
1	2024-08-19 08:23:45	default-allow-ssh	Open SSH: global	High

Total Records: 109

Asset Details for shaped-infusion-402417:

11 issues found across shaped-infusion-402417

Asset ID	Asset Type	Asset Category
a2790399-c26c-4a8a-b82a-d2f05f92763d	gcp_project	Cloud Account

Location: global

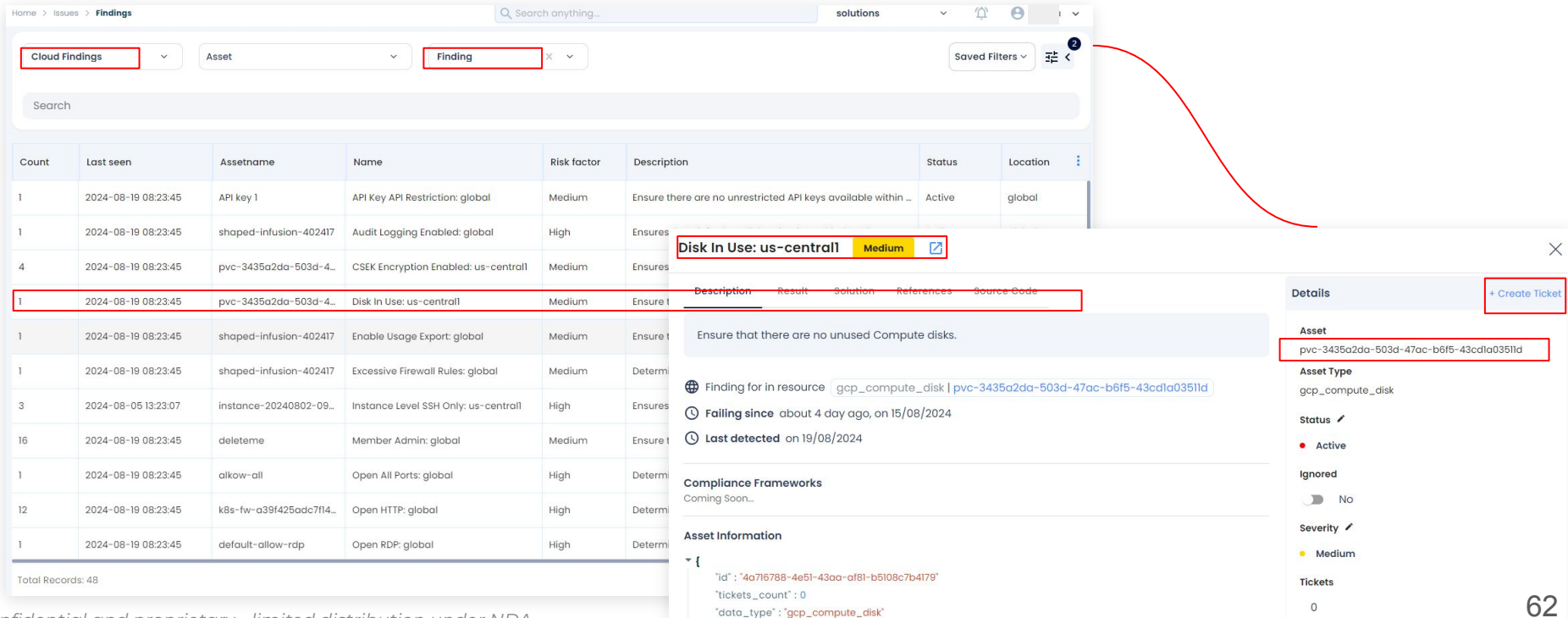
🕒 Discovered about 14 day ago, on 05/08/2024
🕒 Last detected on 19/08/2024

Assets Table:

Last seen	Asset	Finding	Risk Factor	Description	Status	Location
2024-08-19 08:23:45	shaped-infusion-402417	VPC Network Logging: g...	Medium	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	OS Login Enabled: global	Low	Ensures OS login is ena...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Audit Configuration Log...	Low	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Log Sinks Enabled: global	Low	Ensures a log sink is en...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Project Ownership Logg...	Low	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Storage Permissions Lo...	Medium	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Custom Role Logging: g...	Low	Ensures that logging an...	Active	global
2024-08-19 08:23:45	shaped-infusion-402417	Audit Logging Enabled: ...	High	Ensures that default au...	Active	global

How to identify unused disk in the onboarded account?

- To identify the unique findings with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply filter for severity **High/Medium**
 - Search for **Disk** directly or Use **group by findings** filter



The screenshot displays the AccuKnox Findings interface. At the top, there are filter dropdowns for 'Cloud Findings', 'Asset', and 'Finding'. Below these is a search bar and a 'Saved Filters' button. The main area contains a table of findings. One finding is highlighted with a red box: 'Disk In Use: us-central' with a Medium severity. A red arrow points from this finding to a detailed view panel on the right. The detailed view shows the description 'Ensure that there are no unused Compute disks.', the asset ID 'pvc-3435a2da-503d-47ac-b6f5-43cda0351ld', and the status 'Active'. It also shows the last detected time as '19/08/2024' and provides a 'Create Ticket' button.

Count	Last seen	Assetname	Name	Risk factor	Description	Status	Location
1	2024-08-19 08:23:45	API key 1	API Key API Restriction: global	Medium	Ensure there are no unrestricted API keys available within ...	Active	global
1	2024-08-19 08:23:45	shaped-infusion-402417	Audit Logging Enabled: global	High	Ensures		
4	2024-08-19 08:23:45	pvc-3435a2da-503d-4...	CSEK Encryption Enabled: us-central	Medium	Ensures		
1	2024-08-19 08:23:45	pvc-3435a2da-503d-4...	Disk In Use: us-central	Medium	Ensure t		
1	2024-08-19 08:23:45	shaped-infusion-402417	Enable Usage Export: global	Medium	Ensure t		
1	2024-08-19 08:23:45	shaped-infusion-402417	Excessive Firewall Rules: global	Medium	Determ		
3	2024-08-05 13:23:07	instance-20240802-09...	Instance Level SSH Only: us-central	High	Ensures		
16	2024-08-19 08:23:45	deleteme	Member Admin: global	Medium	Ensure t		
1	2024-08-19 08:23:45	alkow-all	Open All Ports: global	High	Determ		
12	2024-08-19 08:23:45	k8s-fw-a39f425adc7f14...	Open HTTP: global	High	Determ		
1	2024-08-19 08:23:45	default-allow-rdp	Open RDP: global	High	Determ		

Total Records: 48

Disk In Use: us-central Medium

Description Result Solution References Source Code

Ensure that there are no unused Compute disks.

Finding for in resource [gcp_compute_disk | pvc-3435a2da-503d-47ac-b6f5-43cda0351ld](#)

Failing since about 4 day ago, on 15/08/2024

Last detected on 19/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "4a716788-4e51-43aa-af81-b5108c7b4179"
  "tickets_count": 0
  "data_type": "gcp_compute_disk"
}
```

Details + Create Ticket

Asset
pvc-3435a2da-503d-47ac-b6f5-43cda0351ld

Asset Type
gcp_compute_disk

Status
Active

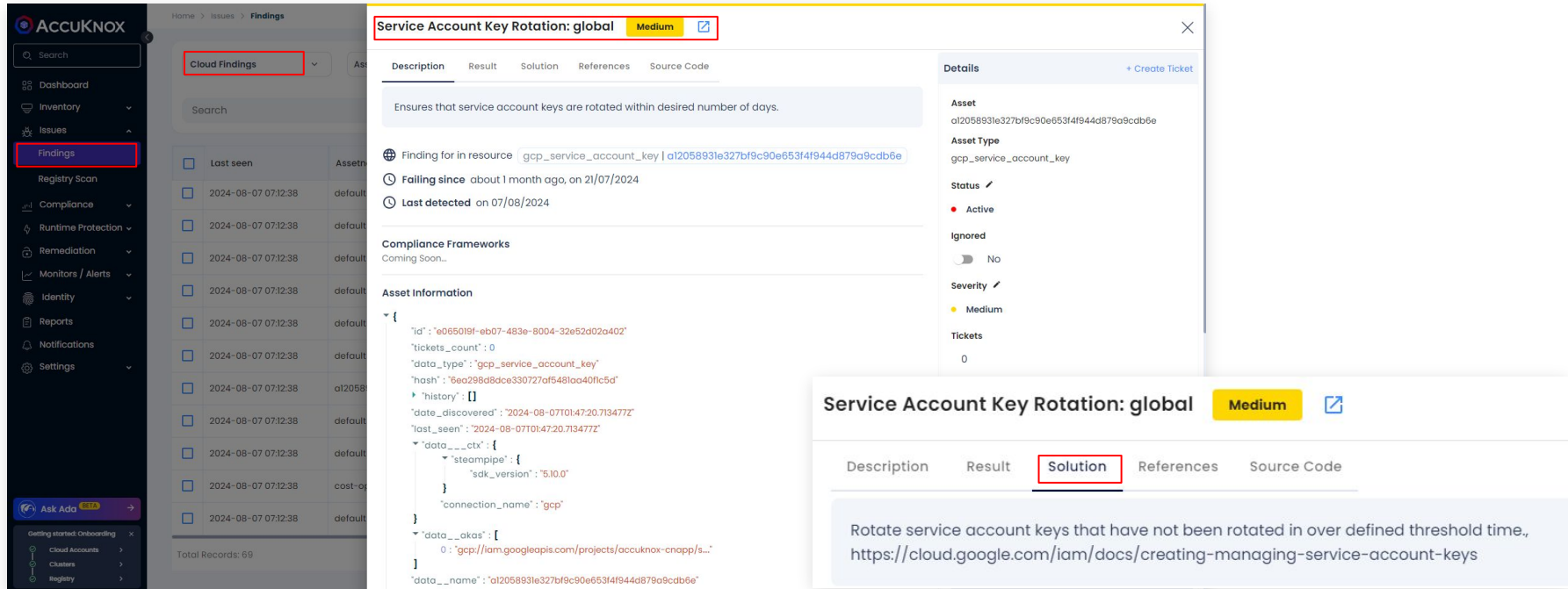
Ignored
No

Severity
Medium

Tickets
0

How to identify if service account keys are exposed?

- To identify the if service account keys are exposed to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply risk factor as “medium”
 - Select the filters by cloud account



Service Account Key Rotation: global Medium

Description Result Solution References Source Code

Ensures that service account keys are rotated within desired number of days.

Finding for in resource `gcp_service_account_key | a12058931e327bf9c90e653f4f944d879a9cabb6e`

Failing since about 1 month ago, on 21/07/2024

Last detected on 07/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "e065019f-eb07-483e-8004-32e52a02a402"
  "tickets_count": 0
  "data_type": "gcp_service_account_key"
  "hash": "6ea296cd8ace330727af54810a40fc5d"
  "history": []
  "date_discovered": "2024-08-07T01:47:20.713477Z"
  "last_seen": "2024-08-07T01:47:20.713477Z"
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
    "connection_name": "gcp"
  }
  "data__akas": [
    0: "gcp://iam.googleapis.com/projects/accuknox-cnapp/s..."
  ]
  "data__name": "a12058931e327bf9c90e653f4f944d879a9cabb6e"
}
```

Details + Create Ticket

Asset
a12058931e327bf9c90e653f4f944d879a9cabb6e

Asset Type
gcp_service_account_key

Status ✓

Active

Ignored
No

Severity ✓

Medium

Tickets
0

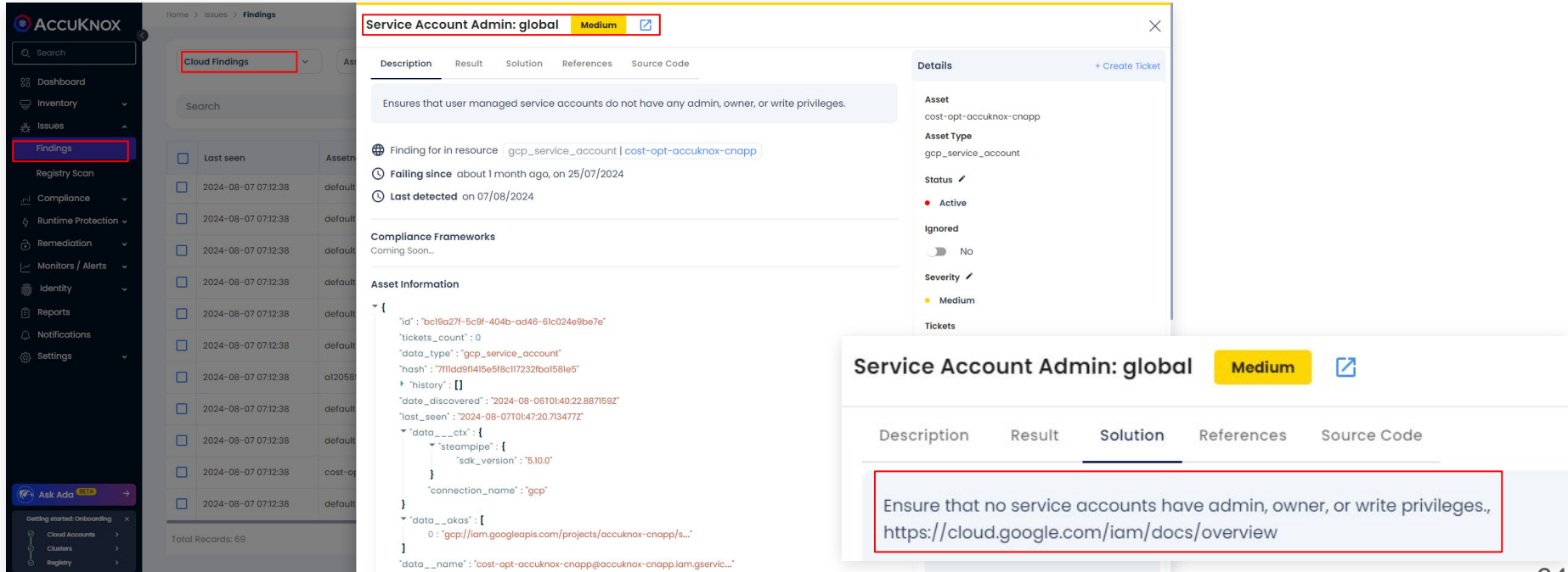
Service Account Key Rotation: global Medium

Description Result **Solution** References Source Code

Rotate service account keys that have not been rotated in over defined threshold time., <https://cloud.google.com/iam/docs/creating-managing-service-account-keys>

How to identify service accounts with admin privilege?

- To identify the if service account keys have admin permissions with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply risk factor as “medium”
 - Select the filters by cloud account



The screenshot displays the ACCUKNOX interface with the following details:

- Navigation:** Home > Issues > Findings. The 'Findings' menu item is highlighted in the left sidebar.
- Filtering:** 'Cloud Findings' is selected in the filter dropdown.
- Findings List:** A table of findings is shown, with the first entry selected. The selected finding is titled 'Service Account Admin: global' with a 'Medium' risk level.
- Findings Details:**
 - Description:** Ensures that user managed service accounts do not have any admin, owner, or write privileges.
 - Asset:** cost-opt-accuknox-cnapp
 - Asset Type:** gcp_service_account
 - Status:** Active
 - Ignored:** No
 - Severity:** Medium
 - Tickets:** + Create Ticket
- Asset Information:**

```
{
  "id": "bcl9a271-5c9f-404b-ad46-61c024e8b67e"
  "tickets_count": 0
  "data_type": "gcp_service_account"
  "hash": "7f11ad9f1415e5f9c11732fba1581e5"
  "history": []
  "date_discovered": "2024-08-06T01:40:22.887159Z"
  "last_seen": "2024-08-07T01:47:20.713477Z"
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
    "connection_name": "gcp"
  }
  "data__akas": [
    0: "gcp://iam.googleapis.com/projects/accuknox-cnapp/s..."
  ]
  "data__name": "cost-opt-accuknox-cnapp@accuknox-cnapp.iam.gservice..."
}
```
- Solution:** A red box highlights the solution link: <https://cloud.google.com/iam/docs/overview>.

How to identify if RDP port exposed to public?

- To identify the if rdp ports since exposed to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Apply **cloud account** filter and select severity as **High/Critical**

Open RDP: global High

Description Result Solution References Source Code

Determines if TCP port 3389 for RDP is open to the public

Details + Create Ticket

Asset
default-allow-rdp

Asset Type
gcp_compute_firewall

Status ✓
• Active

Ignored
No

Severity ✓
• High

Notes
Add Comments and Press Ctrl + Enter to Submit

Asset Information

```
{
  "id": "d6d05414-a13a-4509-9297-abdb3b6d3ce3"
  "tickets_count": 0
  "data_type": "gcp_compute_firewall"
  "hash": "fb8ca25f14b30404cc478702a472e954"
  "history": []
  "date_discovered": "2024-08-05T06:09:25.252622Z"
  "last_seen": "2024-08-13T01:14:22.785067Z"
  "data__id": "5742647272601445000"
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
  }
}
```

Filter Clear Filter Save Apply

Data Type
cloudspot

Select Fields to filter
Cloud account

Location X Cloud account X

Risk Factor
Unknown Informational Low Medium **High** Critical

Tickets
Not Available

Ignored
True False

Exploit Available
True False

Tickets
True False

Is New
True False

Location
Location

Cloud account
shaped-infusion-402417

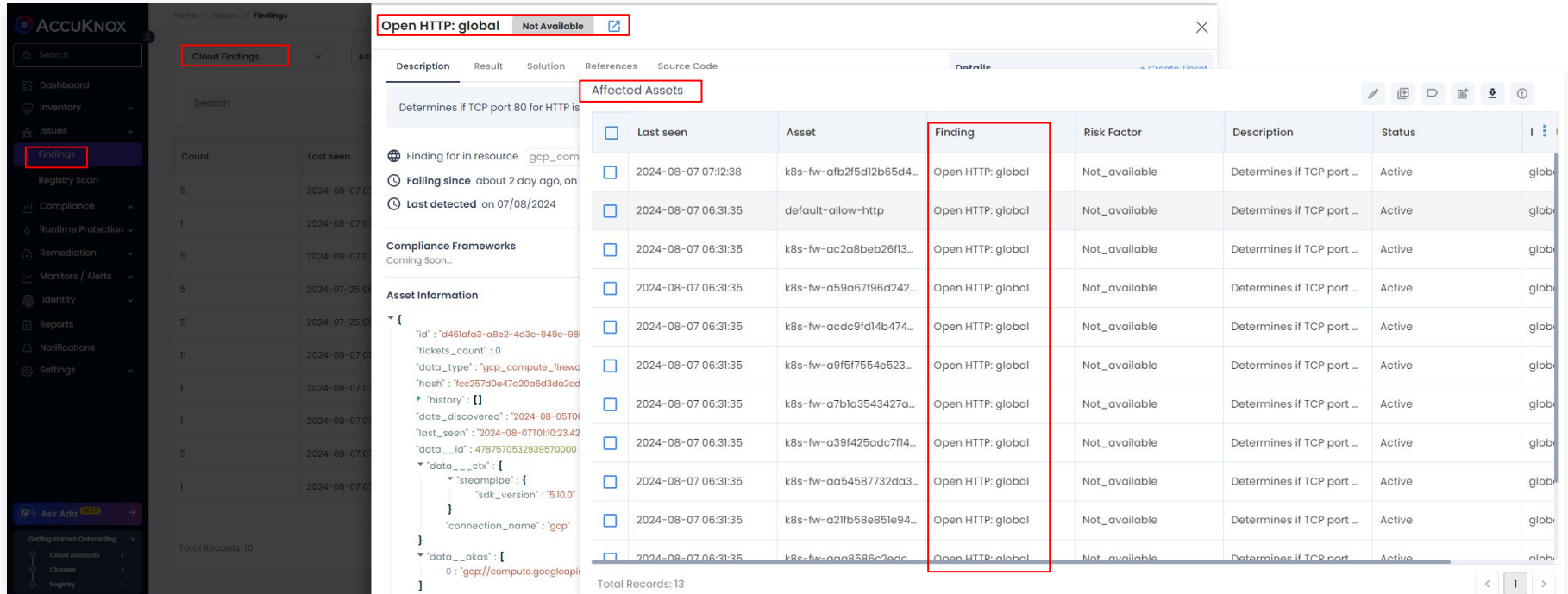
Open RDP: global High

Description Result Solution References Source Code

Restrict TCP port 3389 to known IP addresses., <https://cloud.google.com/vpc/docs/using-firewalls>

How to identify if Insecure HTTP port are exposed to public?

- To identify the if Insecure HTTP port are exposed to public with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Search for “HTTP”

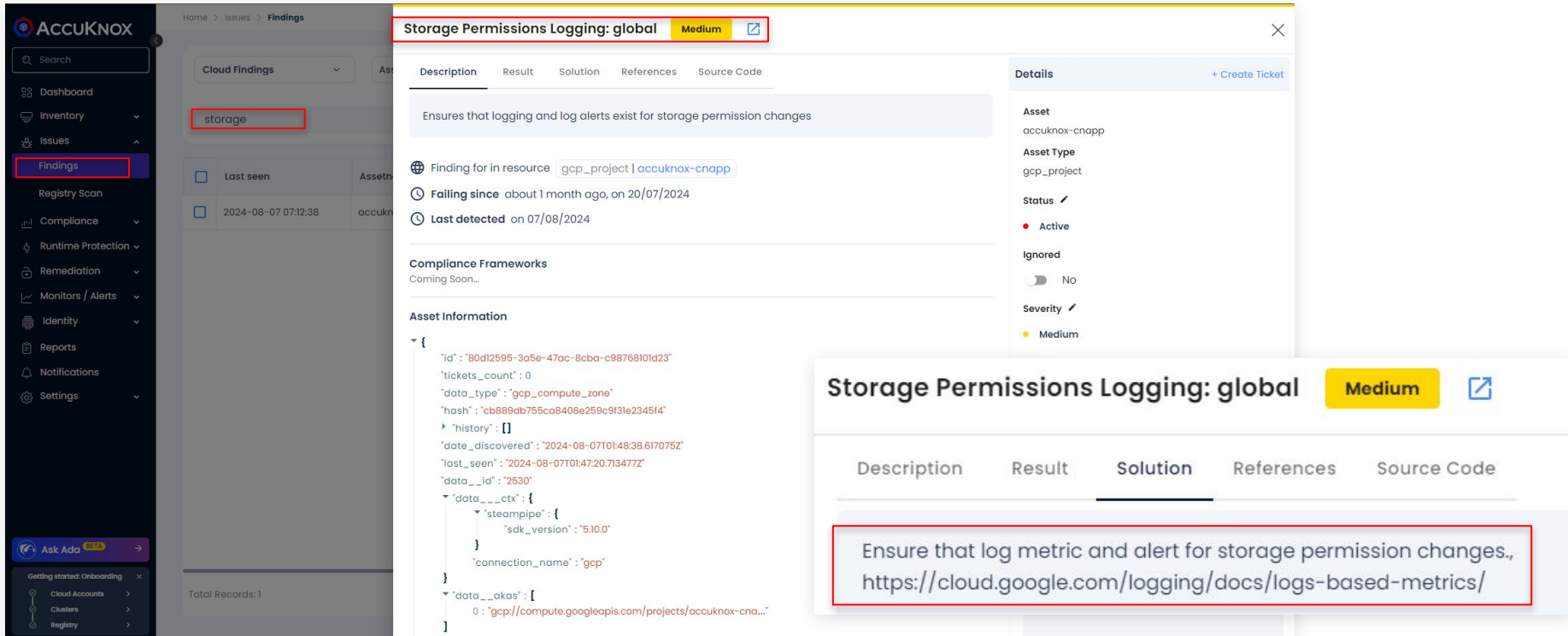


The screenshot displays the ACCUKNOX interface with the following elements:

- Left Sidebar:** Contains navigation menus for Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings.
- Top Filter Bar:** Shows the search criteria: "Open HTTP: global" and "Not Available".
- Table:** A table titled "Affected Assets" with 13 rows. The columns are: Last seen, Asset, Finding, Risk Factor, Description, and Status. The "Finding" column is highlighted with a red box. All findings are "Open HTTP: global" with a "Not_available" risk factor.
- Asset Information:** A detailed view of an asset is shown on the left, including fields like "id", "tickets_count", "data_type", "hash", "history", "date_discovered", "last_seen", "data_id", "data__ctx", "steampipe", "connection_name", and "data__akas".
- Bottom:** A "Total Records: 13" indicator and pagination controls.

How to identify if logging is enabled for storage?

- To identify the if logging is enabled for storage with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Search for “Storage”



The screenshot displays the ACCUKNOX interface with a sidebar on the left containing navigation options like Dashboard, Inventory, Issues, Findings, Registry Scan, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports, Notifications, and Settings. The main area shows a list of findings under 'Cloud Findings' with a search filter set to 'storage'. A specific finding is highlighted, showing details for 'Storage Permissions Logging: global' with a Medium severity level.

Storage Permissions Logging: global Medium

Description Result Solution References Source Code

Ensures that logging and log alerts exist for storage permission changes

Details + Create Ticket

Asset
accuknox-cnapp

Asset Type
gcp_project

Status ✓
Active

Ignored
No

Severity ✓
Medium

Finding in resource | gcp_project | accuknox-cnapp

Failing since about 1 month ago, on 20/07/2024

Last detected on 07/08/2024

Compliance Frameworks
Coming Soon...

Asset Information

```
{
  "id": "80d12595-3a5e-47ac-8cba-c9876810d23"
  "tickets_count": 0
  "data_type": "gcp_compute_zone"
  "hash": "cb889db755ca8408e259c9f31e234514"
  "history": []
  "date_discovered": "2024-08-07T01:48:38.617075Z"
  "last_seen": "2024-08-07T01:47:20.713477Z"
  "data__id": "2530"
  "data__ctx": {
    "steampipe": {
      "sdk_version": "5.10.0"
    }
    "connection_name": "gcp"
  }
  "data__akas": [
    0: "gcp://compute.googleapis.com/projects/accuknox-cna..."
  ]
}
```

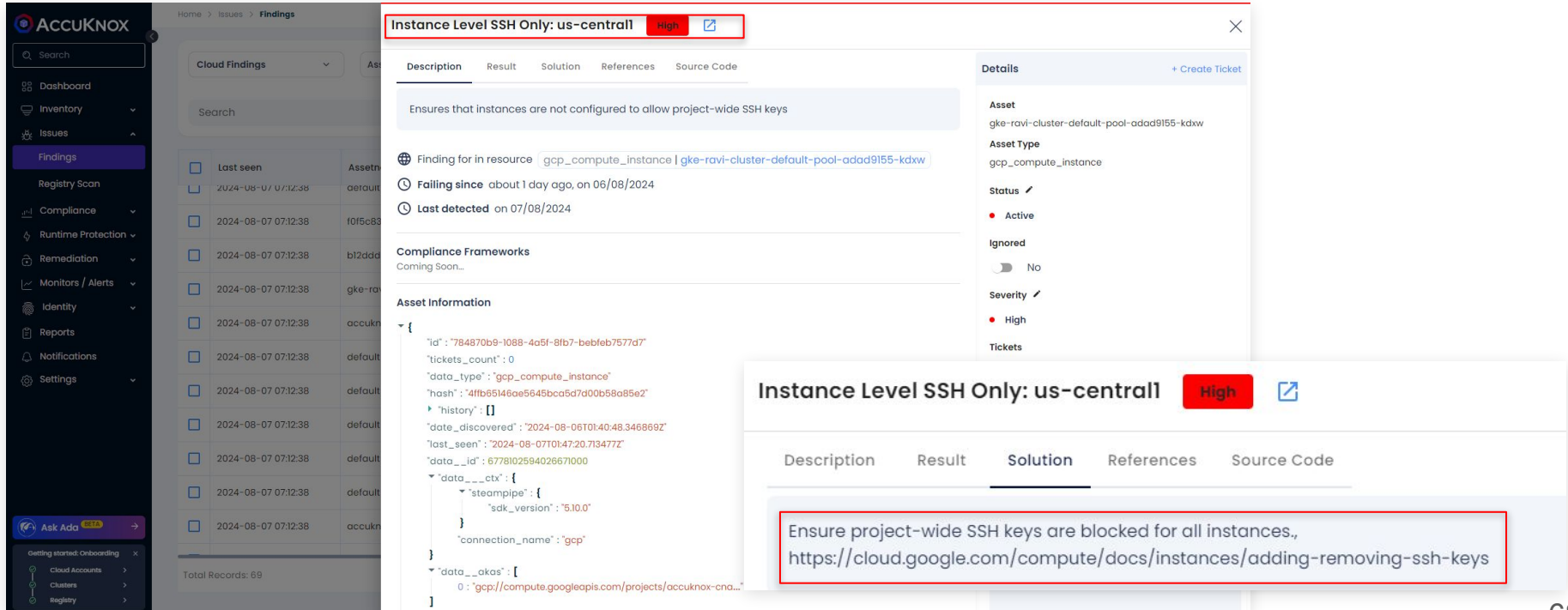
Storage Permissions Logging: global Medium

Description Result Solution References Source Code

Ensure that log metric and alert for storage permission changes.,
<https://cloud.google.com/logging/docs/logs-based-metrics/>

How to identify if instance are allowed project-wide SSH?

- To identify the if instance are allowed to SSH project-wide with the Onboarded Cloud Account, Please navigate to Issues -> Findings
 - Apply **Cloud Findings** in the filter
 - Search for "SSH"



The screenshot displays the ACCUKNOX interface with a finding titled "Instance Level SSH Only: us-central1" highlighted in red. The finding is categorized as "High" severity. The description states: "Ensures that instances are not configured to allow project-wide SSH keys". The asset information shows it is a "gcp_compute_instance" with ID "gke-ravi-cluster-default-pool-adad9155-kdxw". The finding was last detected on 07/08/2024 and has failed since about 1 day ago. The solution provided is a link to the Google Cloud documentation on adding/removing SSH keys: <https://cloud.google.com/compute/docs/instances/adding-removing-ssh-keys>. The interface also shows a table of findings and a sidebar with navigation options.

Compliance failure for CIS Benchmark

To Identify CIS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot shows the AccuKnox interface for the 'Cloud Assets Summary' page. The left sidebar contains navigation options, with 'Cloud Assets Summary' highlighted. The main content area displays a list of compliance findings for various benchmarks, including FISMA, CIS GCP CIS Benchmark, General Data Protec..., HIPAA, and HITRUST CSF. A table provides a detailed view of the CIS GCP CIS Benchmark findings, showing 25 items with columns for Control, Assets, Description, Compliance percentage, and Result. The 'Compliance' column is highlighted with a red box, and the 'Result' column shows a grid of colored indicators (red, yellow, grey, green) representing different compliance statuses.

Control	Assets	Description	Compliance	Result
1.11 Ensure that Separation of duties is ...	0	It is recommended that the principle ...	100 %	0 0 0 1
1.1 Ensure that corporate login creden...	0	Use corporate login credentials inste...	100 %	0 0 0 1
1.4 Ensure that there are only GCP-ma...	57	User managed service accounts shou...	67 %	19 0 0 38
1.5 Ensure that Service Account has n...	4	A service account is a special Google ...	0 %	4 0 0 0
1.6 Ensure that IAM users are not assig...	0	It is recommended to assign the Servi...	100 %	0 0 0 1
1.7 Ensure user-managed/external ke...	19	Service Account keys consist of a key ...	26 %	14 0 0 5
1.8 Ensure that Separation of duties is ...	0	It is recommended that the principle ...	100 %	0 0 0 1
2.10 Ensure that the log metric filter an...	0	It is recommended that a metric filter ...	0 %	1 0 0 0
2.11 Ensure that the log metric filter an...	0	It is recommended that a metric filter ...	100 %	0 0 0 1
2.1 Ensure that Cloud Audit Logging is ...	0	It is recommended that Cloud Audit L...	0 %	1 0 0 0
2.2 Ensure that sinks are configured fo...	0	It is recommended to create a sink th...	0 %	1 0 0 0
Total Records: 48				

Compliance failure for ISO 27001 Benchmark



To Identify ISO 27001 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot displays the AccuKnox Compliance dashboard. On the left, a navigation sidebar includes 'Cloud Assets Summary', which is highlighted with a red box. The main content area shows a 'Cloud Assets Summary' for 'accuknox-cnapp | GCP25JAN' in the 'Region'. It lists 25 compliance findings, with ISO 27001 highlighted in a red box. Below this, a 'Detailed View' table shows various controls, many of which are marked as 'FAILED'. A second table provides details for these failed checks, including the plugin name, asset, message, result, severity, and recommended actions.

Control	Assets	Description	Compliance	Result
A.10.1.1 Policy on the Use of Cryptograp...	1	A policy on the use of cryptographic c...	97 %	1 0 0 35
A.10.1.2 Key Management	0	A policy on the use, protection and lif...	100 %	0 0 0 37

Plugin	Asset	Message	Result	Severity
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
vpcNetworkRouteLogging	None	No log metr...	FAILED	Medium
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
loggingEnabled	projects/ac...	Logging is ...	FAILED	Medium
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLogsEnabled	projects/ac...	The subnet ...	FAILED	Low
flowLoasEnabled	projects/ac...	The subnet ...	FAILED	Low

Compliance failure for PCI DSS Benchmark

To Identify PCI DSS failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot displays the AccuKnox compliance interface. On the left, a 'Compliance' sidebar lists various benchmarks: NIST CSF (81.7% Compliant), NIST SP 800-53 (80.6% Compliant), PCI (95.4% Compliant, highlighted with a red box), and SOC 2 Type II (84.9% Compliant). The main area shows a 'Cloud Assets Summary' table with columns for Control, Assets, Description, Compliance, and Result. A modal window is open over the table, displaying details for a failed check: 'storagePermissionsLogging' (Medium severity). The modal includes a description, a finding for in resource, a message stating 'No log metrics found', a solution reference link, and a list of compliance frameworks and sub-controls. The sub-controls list includes A.12.4.3 ADMINISTRATOR AND OPERATOR LOGS, A.12.4.1 EVENT LOGGING, CLD.13.1.4 ALIGNMENT OF SECURITY MANAGEMENT FOR VIRTUAL AND PHYSICAL NETWORKS, IA - IDENTIFICATION AND AUTHENTICATION, A.16.1.7 COLLECTION OF EVIDENCE, 2.10 ENSURE THAT THE LOG METRIC FILTER AND ALERTS EXIST FOR CLOUD STORAGE IAM PERMISSION CHANGES, A 10.3 CONTROL AND LOGGING OF DATA RESTORATION, DATA PROCESSING RECORDS, and ARTICLE 30 - RECORDS OF PROCESSING ACTIVITIES.

Control	Assets	Description	Compliance	Result
Requirement 10 - Track Access				
Requirement 11 - Test				
Requirement 1 - Firewall				
Requirement 2 - Default				
Requirement 3 - Card				
Requirement 4 - Encr				
Requirement 6 - Secu				
Requirement 7 - Rest				

Plugin	Asset	Message	Result
storagePermiL	None	No log m...	FAILED
projectOwner...	None	No log m...	FAILED
vpcNetworkLo...	None	No log m...	FAILED

storagePermissionsLogging

Medium

Description

Ensures that logging and log alerts exist for storage permission changes

Finding for in resource Category: Logging None

Message

No log metrics found

Solution Reference Link

<https://cloud.google.com/logging/docs/logs-based-metrics/>

Compliance Frameworks

Compliance Sub Controls

- A.12.4.3 ADMINISTRATOR AND OPERATOR LOGS
- ACCESS PERMISSIONS
- INCIDENT MANAGEMENT
- PERFORM CONTINUOUS MONITORING
- RS.AN-3
- A.12.4.1 EVENT LOGGING
- CLD.13.1.4 ALIGNMENT OF SECURITY MANAGEMENT FOR VIRTUAL AND PHYSICAL NETWORKS
- IA - IDENTIFICATION AND AUTHENTICATION
- 164.312(b) AUDIT CONTROLS
- ACCESS CONTROL
- A.16.1.7 COLLECTION OF EVIDENCE
- DE.CM-7
- 2.10 ENSURE THAT THE LOG METRIC FILTER AND ALERTS EXIST FOR CLOUD STORAGE IAM PERMISSION CHANGES
- A 10.3 CONTROL AND LOGGING OF DATA RESTORATION
- 13.1.4 PROVISIONING FUNCTIONS
- DATA PROCESSING RECORDS
- 3.14 SYSTEM AND INFORMATION INTEGRITY
- ARTICLE 30 - RECORDS OF PROCESSING ACTIVITIES
- REQUIREMENT 10 - TRACK ACCESS
- INTERNAL AUDIT

Recommended Actions

Ensure that log metric and alert for storage permission changes.

Details

+ Create Ticket

Asset

None

Asset Category

Category: Logging

Region

None

Result

FAILED

Severity

Medium

Account

accuknox-cnapp

Compliance failure for SOC 2 Benchmark

To Identify SOC 2 failed compliance checks > Navigate to Compliance and select Cloud Asset Summary

The screenshot displays the Accuknox compliance interface. At the top, the account name 'accuknox-cnapp | GCP25JAN' and the region 'Region' are visible. The main dashboard shows a summary of 25 compliance findings, with SOC 2 Type II highlighted as having 10 controls and 84.9% compliance. A detailed view of the SOC 2 Type II findings is shown in a modal window, listing various controls that have failed. The failed controls include 'privateAccessEnabled' (10 instances) and 'osLoginEnabled' (1 instance), all with a severity of Medium or Low. The 'Result' column for these failed items is highlighted with a red box.

Control	Assets	Description	Compliance	Result
A1.1			100%	Compliant
A1.2			100%	Compliant
CC2.1			100%	Compliant
CC5.1			100%	Compliant
CC6.1			100%	Compliant
CC6.2			100%	Compliant
CC6.3			100%	Compliant
CC6.6			100%	Compliant
CC6.7			100%	Compliant
CC7.1			100%	Compliant

Compliance	Plugin	Asset	Message	Result	Severity	Compliance	Recommended Action	Solution Reference Link
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
NIST CSF	<input type="checkbox"/>	privateAccessEnabled	projects/ac... Subnet doe...	FAILED	Medium	NIST CSF +15	1. Enter the VPC Network service. 2. Enter the...	https://cloud.google.com/vpc/docs/configu
LGPD	<input type="checkbox"/>	osLoginEnabled	None OS login is ...	FAILED	Low	LGPD +15	Set enable-oslogin in project-wide metad...	https://cloud.google.com/compute/docs/in

Assistive Remediation For GCP Risks

AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 1)

- Navigate to Issues > Findings
- Select the finding and create a ticket for it

Open SSH: global High 

Description Result Solution References Source Code

Determines if TCP port 22 for SSH is open to the public

Finding for in resource `gcp_compute_firewall` | [default-allow-ssh](#)

Failing since about 1 month ago, on 21/07/2024

Last detected on 07/08/2024

Compliance Frameworks

Coming Soon...

Asset Information

```
{
  "id": "44f30fbb-9515-401c-9c47-1bc6236d61c9"
  "tickets_count": 0
  "data_type": "gcp_compute_firewall"
}
```

Details

+ Create Ticket

Asset

default-allow-ssh

Asset Type

gcp_compute_firewall

Status

Active

Ignored

No

Severity

High

Tickets

0

Create Ticket


Please select a ticket configuration. If you do not have a ticket configuration, please go to the [Integrations](#) page.

compliancej  

Close

Create Ticket

Create ticket

Priority
Priority 

Ticket Title*
Open SSH: global

Ticket Description

B I H       

Description Determines if TCP port 22 for SSH is open to the public

Synopsis

Impacted Assets

Asset	Port
default-allow-ssh	global

Solution

Restrict TCP port 22 to known IP addresses. <https://cloud.google.com/vpc/docs/using-firewalls>

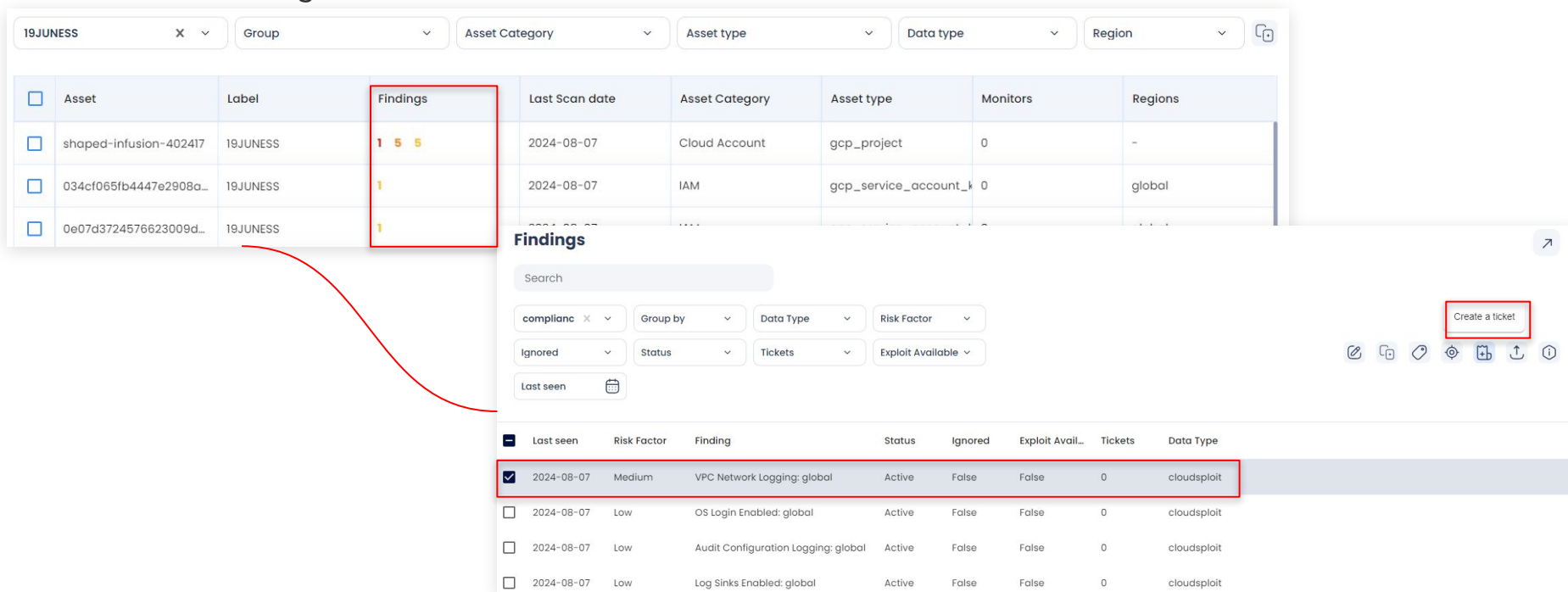
Plugin Output

FAILED, Firewall Rule:(default-allow-ssh) has SSH: TCP port 22 open to 0.0.0.0/0

AccuKnox offers solution reference links to assist with the remediation

To Remediate the findings (Approach 2)

- Navigate to Inventory > Cloud Assets
- Select the finding and create a ticket for it

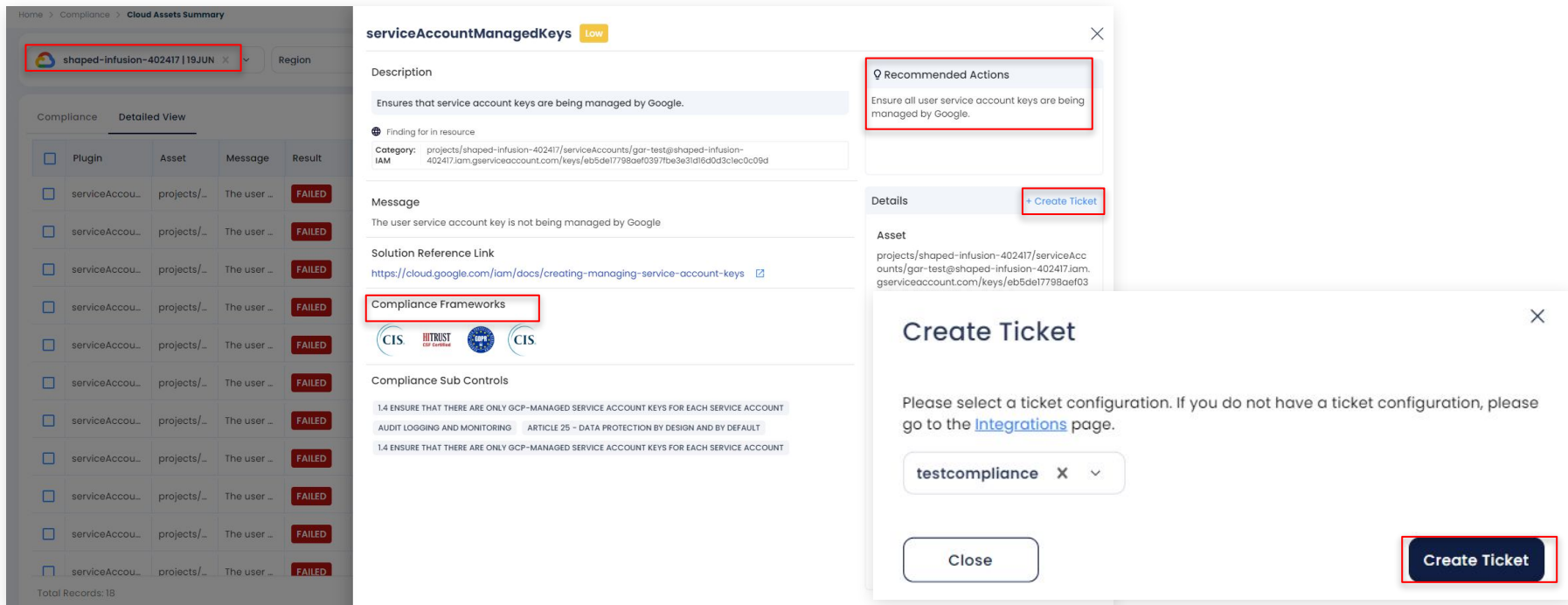


The screenshot displays the AccuKnox interface. At the top, there are filter tabs for '19JUNESS', 'Group', 'Asset Category', 'Asset type', 'Data type', and 'Region'. Below this is a table of assets. A red box highlights the 'Findings' column for the first asset, 'shaped-infusion-402417', which shows '1 5 5' findings. A red arrow points from this box to a detailed 'Findings' view. This view includes a search bar, filter tabs for 'compliance', 'Group by', 'Data Type', and 'Risk Factor', and a 'Create a ticket' button. Below these are icons for edit, copy, share, and other actions. A table of findings is shown, with the first row highlighted in red:

<input type="checkbox"/>	Last seen	Risk Factor	Finding	Status	Ignored	Exploit Avail...	Tickets	Data Type
<input checked="" type="checkbox"/>	2024-08-07	Medium	VPC Network Logging: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-07	Low	OS Login Enabled: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-07	Low	Audit Configuration Logging: global	Active	False	False	0	cloudsploit
<input type="checkbox"/>	2024-08-07	Low	Log Sinks Enabled: global	Active	False	False	0	cloudsploit

AccuKnox offers solution reference links to assist with the remediation
To Remediate the findings (Approach 3)

- From the detailed view of Cloud Asset Summary
- Select the failed compliance and create a ticket for it



The screenshot displays the AccuKnox interface for a compliance failure. On the left, a table lists compliance findings, with the first row highlighted. The main panel shows the detailed view for the finding 'serviceAccountManagedKeys' (Low severity). The description states: 'Ensures that service account keys are being managed by Google.' The message reads: 'The user service account key is not being managed by Google.' A solution reference link is provided: <https://cloud.google.com/iam/docs/creating-managing-service-account-keys>. The 'Compliance Frameworks' section lists CIS, ITRUST, and NIST. The 'Compliance Sub Controls' section includes: '1.4 ENSURE THAT THERE ARE ONLY GCP-MANAGED SERVICE ACCOUNT KEYS FOR EACH SERVICE ACCOUNT AUDIT LOGGING AND MONITORING ARTICLE 25 - DATA PROTECTION BY DESIGN AND BY DEFAULT' and '1.4 ENSURE THAT THERE ARE ONLY GCP-MANAGED SERVICE ACCOUNT KEYS FOR EACH SERVICE ACCOUNT'. A 'Recommended Actions' box suggests: 'Ensure all user service account keys are being managed by Google.' A '+ Create Ticket' button is visible in the 'Details' section. A 'Create Ticket' dialog is open, prompting the user to select a ticket configuration. The 'testcompliance' configuration is selected. The dialog includes 'Close' and 'Create Ticket' buttons.

Plugin	Asset	Message	Result
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED
serviceAcco...	projects/...	The user ...	FAILED

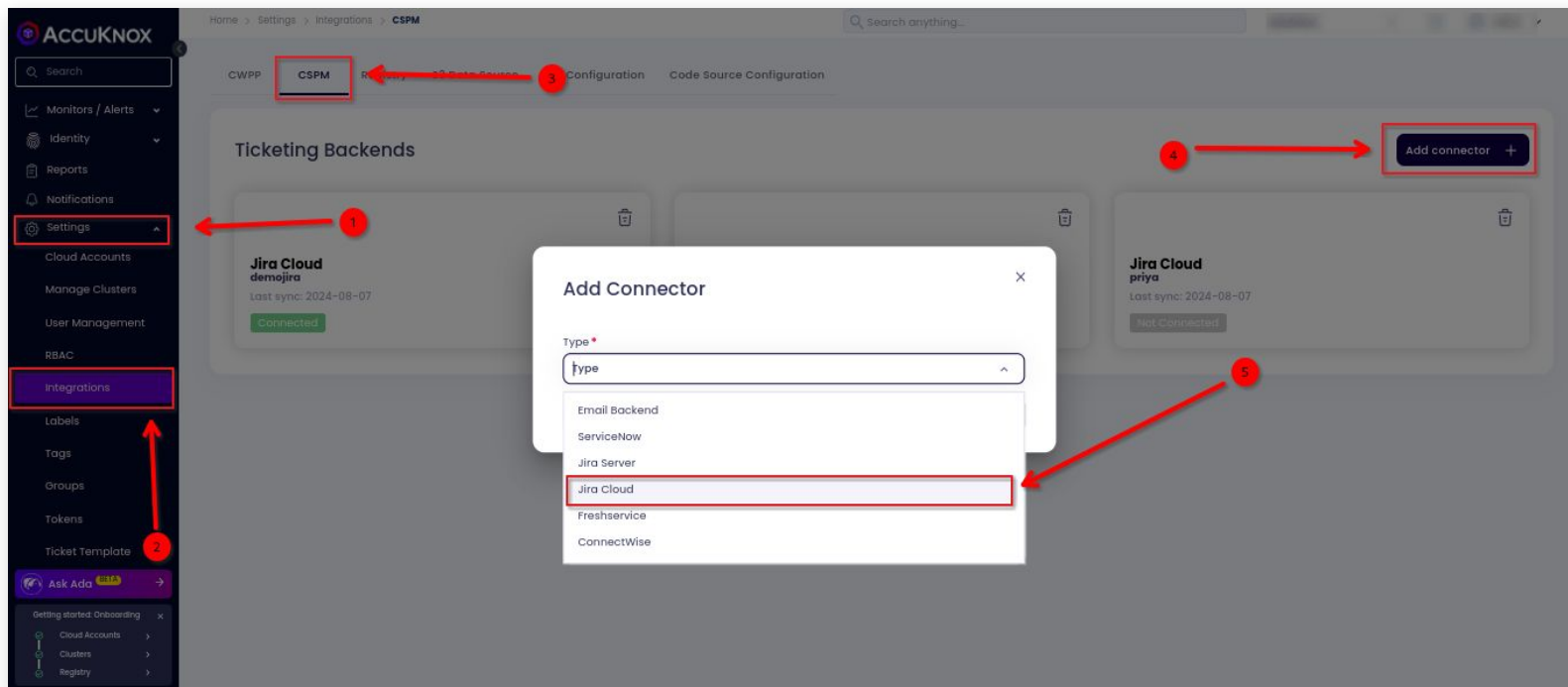


Integrations

How to do CSPM ticketing Integration with Jira Cloud? [1]

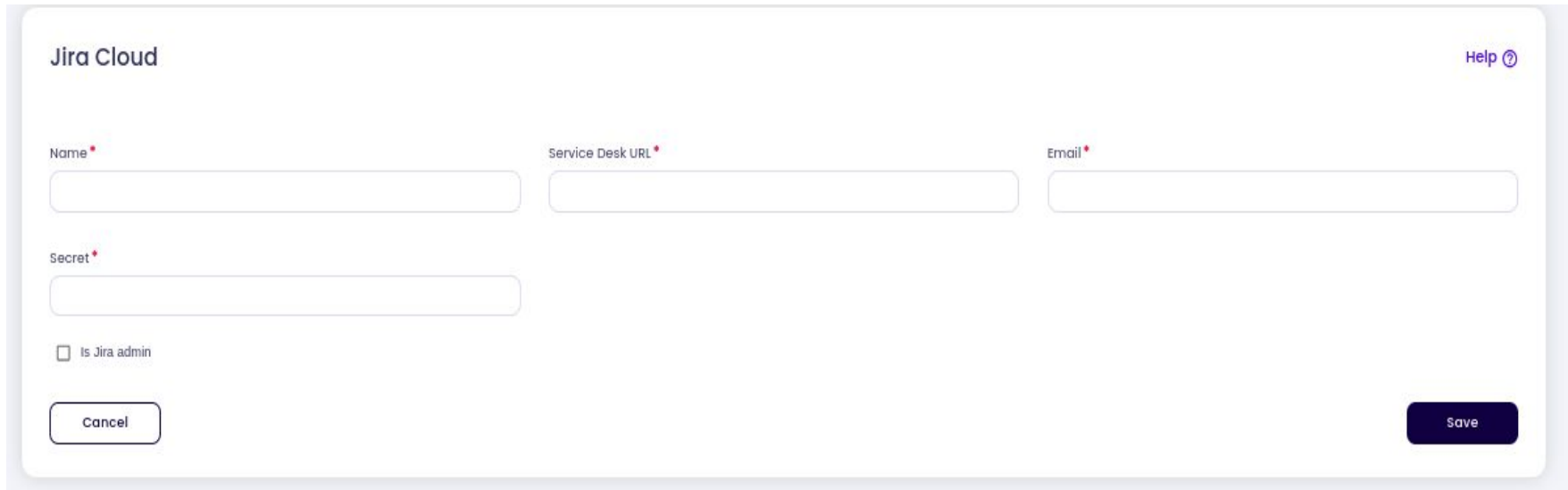
After getting the findings data populated If users want to create tickets for the findings. Then Navigate to Settings->Integrations-> CSPM > Add connector

1. Choose Jira Cloud as the connector and Click Next.



The screenshot shows the AccuKnox CSPM interface. The left sidebar contains a menu with 'Settings' (1) and 'Integrations' (2) highlighted. The main content area shows 'Ticketing Backends' with a 'CSPM' tab (3) selected. A 'Jira Cloud' connector is shown as 'Connected'. An 'Add connector +' button (4) is visible. A modal window titled 'Add Connector' is open, showing a dropdown menu with 'Jira Cloud' (5) selected.

- Fill all the necessary fields and test the connection before saving the integration.
 - a. **Integration Name:** Enter the name for the integration. You can set any name. e.g., Test JIRA
 - b. **Service Desk URL:** Enter the site name of your organisation. e.g., <https://jiratest.atlassian.net/>
 - c. **User Email:** Enter your Jira account email address here.e.g., jira@organisation.com
 - d. **Token:** Enter the generated Token here from <https://id.atlassian.com/manage-profile/security/api-tokens>. e.g., `kRVxxxxxxxxxxxxx39`.
- For more detailed steps refer to the Accuknox help [documentation](#).



Jira Cloud Help

Name

Service Desk URL

Email

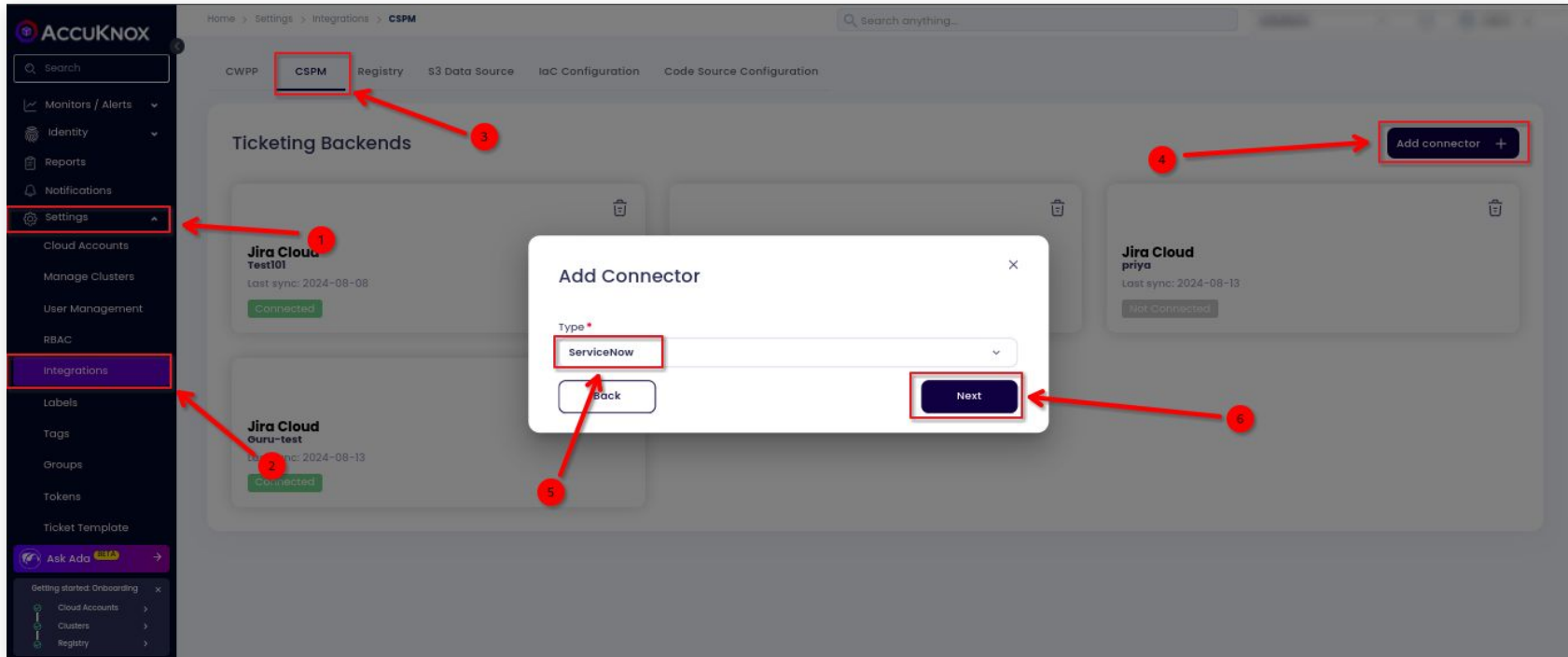
Secret

Is Jira admin

How to do CSPM ticketing Integration with ServiceNow? [1]

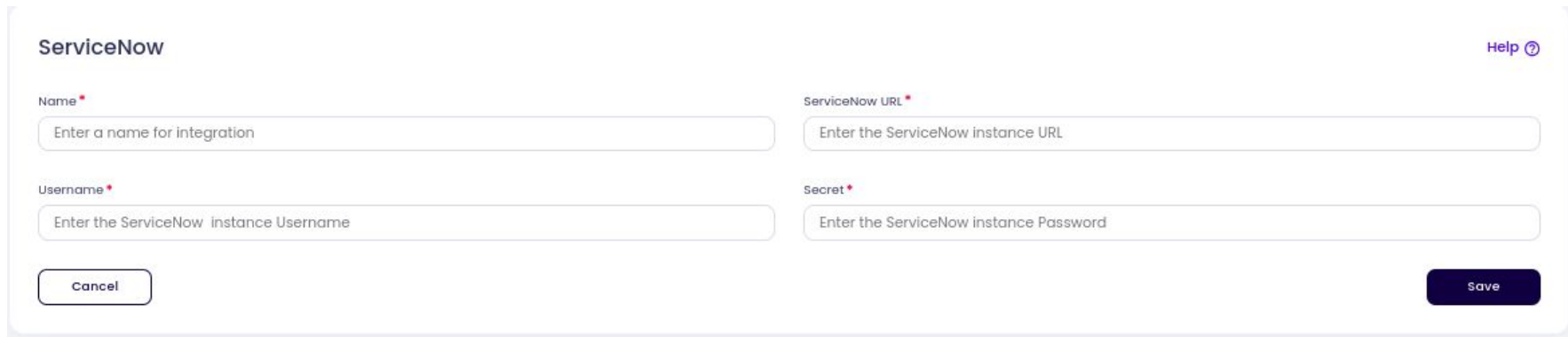
After getting the findings data populated If users want to create tickets for the findings. Then Navigate to Settings->Integrations-> CSPM > Add connector

- Choose ServiceNow as the connector and Click Next.



The screenshot displays the ACCUKNOX user interface. On the left sidebar, the 'Settings' and 'Integrations' menu items are highlighted with red boxes and labeled with '1' and '2' respectively. In the main content area, the 'CSPM' tab is selected and labeled with '3'. Below it, the 'Ticketing Backends' section shows several Jira Cloud connectors. A red arrow labeled '4' points to the 'Add connector +' button. A modal window titled 'Add Connector' is open in the center, showing a dropdown menu with 'ServiceNow' selected (labeled '5') and a 'Next' button (labeled '6').

- Fill all the necessary fields and test the connection before saving the integration.
 - a. **Integration Name:** Enter the name for the integration. You can set any name. e.g.,`MyServiceNow`
 - b. **ServiceNow URL:** The URL of the ServiceNow instance. e.g.,`https://my-instance.service-now.com`
 - c. **Instance Username:** The Username associated with the instance. e.g.,`admin`
 - d. **Secret:** The current password of the instance.
- For more detailed steps refer to the Accuknox help [documentation](#).



The screenshot shows a configuration form titled "ServiceNow" with a "Help" icon in the top right corner. The form contains four input fields arranged in a 2x2 grid:

- Name:** A text input field with the placeholder "Enter a name for integration".
- ServiceNow URL:** A text input field with the placeholder "Enter the ServiceNow instance URL".
- Username:** A text input field with the placeholder "Enter the ServiceNow instance Username".
- Secret:** A text input field with the placeholder "Enter the ServiceNow instance Password".

At the bottom left of the form is a "Cancel" button, and at the bottom right is a dark blue "Save" button.

How to create default template for ticket creation? [1]

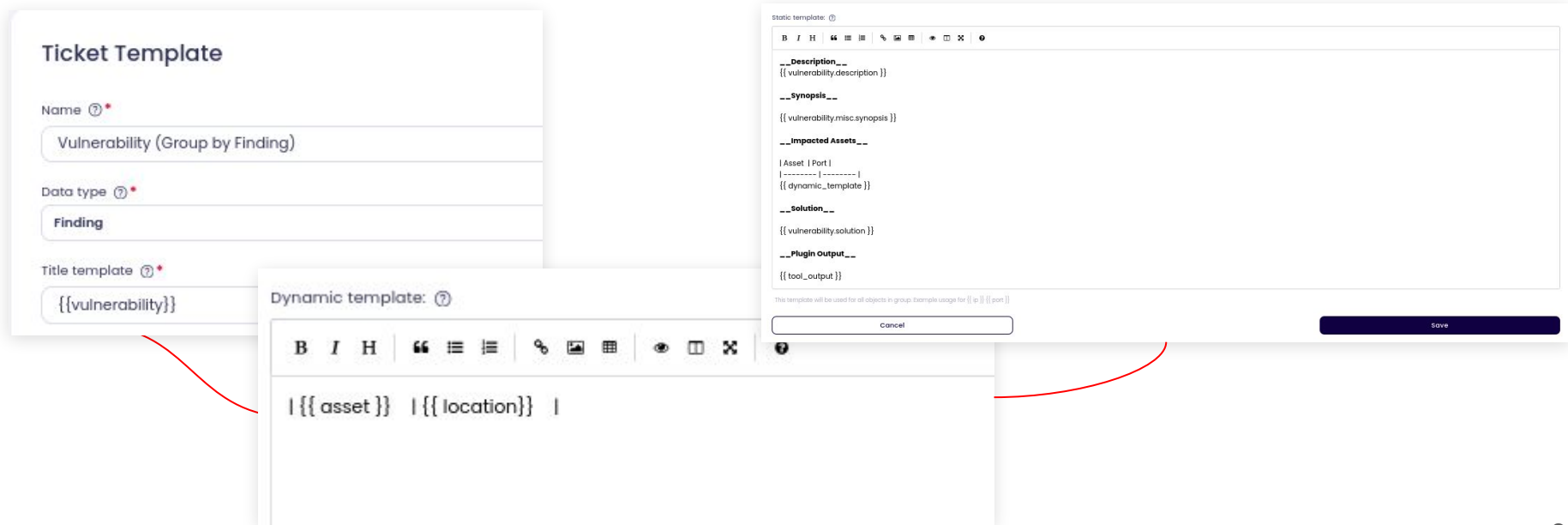
After integrating with a ticketing tool like Jira, ServiceNow etc. User can create default templates for the tickets that they create for that Navigate to Settings->Ticket Template-> Add template

The screenshot displays the ACCUKNOX interface for managing ticket templates. The sidebar on the left contains navigation options, with 'Settings' and 'Ticket Template' highlighted. The main content area shows a table of existing templates and an 'Add template' button. A text box points to the table, stating: "List of all templates that is created by user for different kind of tickets."

Name	Type
<input type="checkbox"/> Datalist Software Template	Data-List
<input type="checkbox"/> Cloud Scan Misconfiguration	Finding
<input type="checkbox"/> IaC Scan Vulnerability	Finding
<input type="checkbox"/> Baseline Template	Control
<input type="checkbox"/> Vulnerability (Group by Finding)	Finding
<input type="checkbox"/> Compliance Template	Control
<input type="checkbox"/> Registry Scan Vulnerability	Finding

How to create default template for ticket creation? [2]

- Fill all the necessary fields and test the connection before saving the integration.
 - a. **Name:** Used for easier access to templates in configurations.
 - b. **Data Type:** Associates the template with a selected data type (e.g., vulnerability) for availability on specific pages.
 - c. **Title Template:** Generates ticket titles in the ticketing system by populating variables.
 - d. **Dynamic Template:** Formats and combines data for multiple objects within a group.
 - e. **Static Template:** Applies consistent data (e.g., solution or description) across a group with similar findings.



The screenshot displays the 'Ticket Template' configuration interface. It includes the following fields and components:

- Name:** Vulnerability (Group by Finding)
- Data type:** Finding
- Title template:** {{{vulnerability}}}
- Dynamic template:** A rich text editor containing the text: | {{{ asset }}} | {{{ location }}} |
- Static template:** A rich text editor containing the following code:

```
__Description__  
{{{ vulnerability.description }}  
  
__Synopsis__  
{{{ vulnerability.misc.synopsis }}  
  
__Impacted Assets__  
| Asset | Port |  
|-----|-----|  
{{{ dynamic_template }}  
  
__Solution__  
{{{ vulnerability.solution }}  
  
__Plugin output__  
{{{ tool_output }}
```

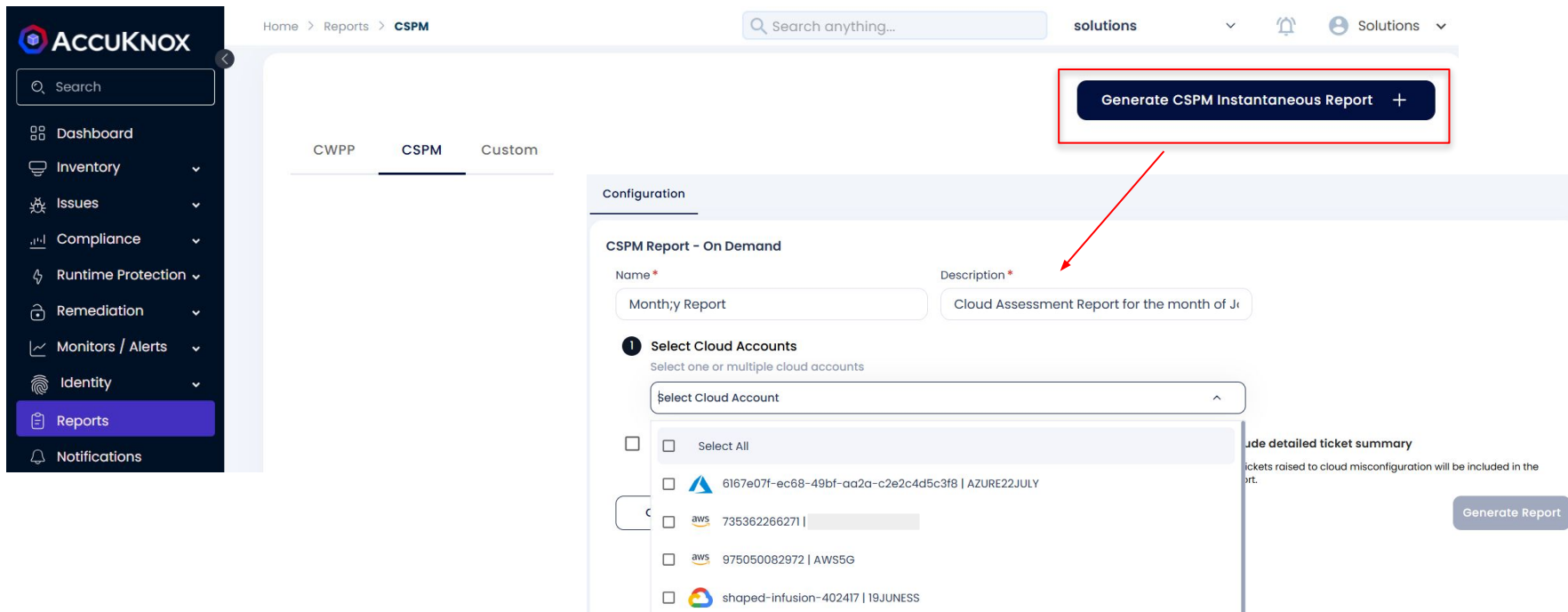
Red lines indicate the flow of information: from the 'Title template' field to the 'Dynamic template' editor, and from the 'Dynamic template' editor to the 'Static template' editor.



Reporting

After getting the findings data populated, a report can be generated for all the misconfigurations or a specific compliance across cloud accounts

- Navigate to Reports -> CSPM & Select Generate CSPM Instantaneous Report
- Specify, Name, Description and Select the Cloud accounts to report on



The screenshot shows the AccuKnox web interface for generating a CSPM report. On the left is a dark sidebar with the AccuKnox logo and a search bar. Below the search bar are menu items: Dashboard, Inventory, Issues, Compliance, Runtime Protection, Remediation, Monitors / Alerts, Identity, Reports (highlighted in purple), and Notifications. The main content area has a breadcrumb trail: Home > Reports > CSPM. A search bar is at the top right. Below the breadcrumb are tabs for CWPP, CSPM (selected), and Custom. A red box highlights a button labeled "Generate CSPM Instantaneous Report +". Below this is a form titled "CSPM Report - On Demand" with fields for "Name*" (containing "Monthly Report") and "Description*" (containing "Cloud Assessment Report for the month of J..."). A section titled "1 Select Cloud Accounts" with the instruction "Select one or multiple cloud accounts" contains a dropdown menu "Select Cloud Account" and a list of cloud accounts with checkboxes: "Select All", "6167e07f-ec68-49bf-aa2a-c2e2c4d5c3f8 | AZURE22JULY", "aws 735362266271 |", "aws 975050082972 | AWS5G", and "shaped-infusion-402417 | 19JUNESS". On the right side of the form, there is a checkbox "Include detailed ticket summary" and a "Generate Report" button.

- Select Compliance Report(Only checks from single framework are included) or Misconfiguration Report
- Include Asset Summary and Ticket Summary as required & click on **Generate Report**

2 Select the Compliance Program

Select the Compliance Program to be included in Report, Compliance Percentage will be calculated for selected programs only

- Compliance Report (Only one compliance selection allowed)**
Compliance report focused on selected Compliance Program with all misconfiguration details will be generated
- Cloud Account Misconfiguration Report**
Select the Compliance Program to be included in Report, Compliance Percentage will be calculated for selected programs only

- Select All
- APRA 234 STANDARD
- AWS CIS Benchmark v1.4.0
- AWS CIS Benchmark v1.5.0
- AWS CIS Benchmark v2.0.0

Include detailed asset summary

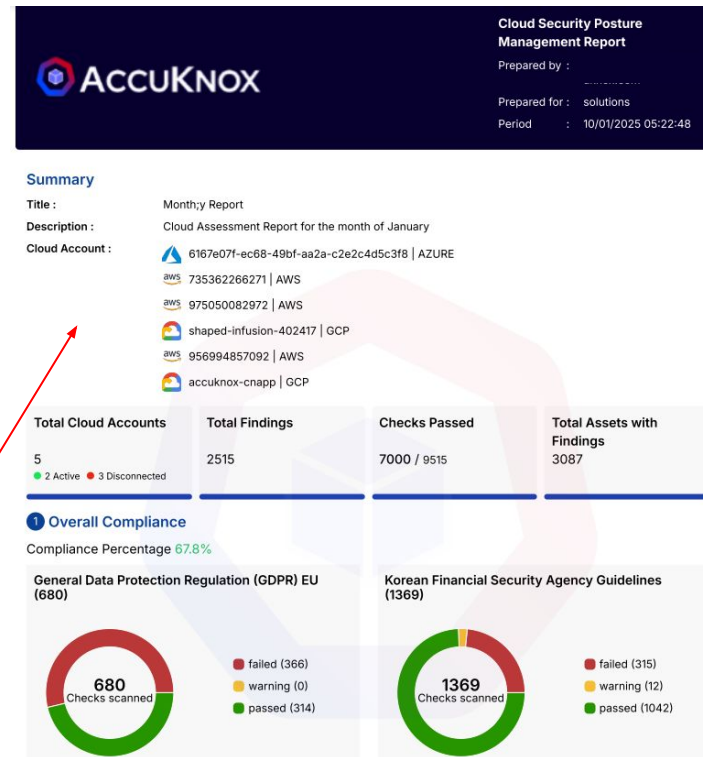
The top 50 misconfigurations will be included. For more details, please check the Cloud Asset Summary Page.

Include detailed ticket summary

All Tickets raised to cloud misconfiguration will be included in the report.

Cancel

Generate Report





CNAPP

(Cloud Native Application
Protection Platform)

